VIVOTEK

AW-GTS-287A

10G L2+ Managed Fiber Switch

User Manual

© 2017, Manufacture Corporation. All rights reserved. All brand and product names are trademarks or registered trademarks of their respective companies

About This Manual

Copyright

Copyright © 2017 VIVOTEK Inc. All rights reserved.
The products and programs described in this User's Manual are licensed products of VIVOTEK Inc., This User's Manual contains proprietary information protected by copyright, and this User's Manual and all accompanying hardware, software and documentation are copyrighted. No parts of this User's manual may be copied, photocopied, reproduced, translated or reduced to any electronic medium or machine-readable from by any means by electronic or mechanical. Including photocopying, recording, or information storage and retrieval systems, for any purpose other than the purchaser's personal use, and without the prior express written permission of VIVOTEK Inc.

Purpose

This manual gives specific information on how to operate and use the management functions of the AW-GTS-287A

Audience

The 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 web management (HTTP/HTTPs).

Table of Contents

Revision History ..... *ix*

INTRODUCTION **1**

CHAPTER 1 OPERATION OF WEB-BASED MANAGEMENT **2**

CHAPTER 2 CONFIGURATION **8**

2-1 SYSTEM 8
2-1.1 Information *8*
2-1.2 IP *7*
2-1.3 NTP *11*
2-1.4 Time *11*
2-1.5 Log *14*
2-2 GREEN ETHERNET 16
2-2.1 Port Power Savings *16*
2-3 PORTS CONFIGURATION 18
2-3.1 Ports *18*
2-3.2 Ports Description *21*
2-4 DHCP 22
2-4.1 Server *22*
2-4.1.1 Mode 22
2-4.1.2 Excluded IP 25
2-4.1.3 Pool 27
2-4.2 Snooping *29*
2-4.3 Relay *31*
2-5 SECURITY 33
2-5.1 Switch *33*
2-5.1.1 Users 33
2-5.1.2 Privilege Level 35
2-5.1.3 Auth Method 37
2-5.1.4 Access Management 39
2-5.1.5 SNMP 41
2-5.1.5.1 System 41
2-5.1.5.2 Trap 43
2-5.1.5.3 Communities 47
2-5.1.5.4 Users 49
2-5.1.5.5 Groups 52
2-5.1.5.6 Views 54
2-5.1.5.7 Access 56
2-5.1.5.8 Trap Event Severity 58
2-5.1.6 RMON 60
2-5.1.6.1 Statistics 60
2-5.1.6.2 History 62
2-5.1.6.3 Alarm 64
2-5.1.6.4 Event 67
2-5.2 Network *69*
2-5.2.1 Limit Control 69
2-5.2.2 NAS 72
2-5.2.3 ACL 81
2-5.2.3.1 Ports 81
2-5.2.3.2 Rate Limiters 83
2-5.2.3.3 Access Control List 84
2-5.2.4 IP Source Guard 97
2-5.2.4.1 Configuration 97
2-5.2.4.2 Static Table 99

2-5.2.5 ARP Inspection 101
2-5.2.5.1 Port Configuration 101
2-5.2.5.2 VLAN Configuration 103
2-5.2.5.3 Static Table 105
2-5.2.5.4 Dynamic Table 107
2-5.3 AAA 109
2-5.3.1 RADIUS 109
2-5.3.2 TACACS+ 112
2-6 AGGREGATION 114
2-6.1 Static 114
2-6.2 LACP 116
2-7 LOOP PROTECTION 118
2-8 SPANNING TREE 120
2-8.1 Bridge Setting 120
2-8.2 MSTI Mapping 123
2-8.3 MSTI Priorities 125
2-8.4 CIST Ports 127
2-8.5 MSTI Ports 130
2-9 IPMC PROFILE 132
2-9.1 Profile Table 132
2-9.2 Address Entry 135
2-10 MVR 137
2-11 IPMC 140
2-11.1 IGMP Snooping 140
2-11.1.1 Basic Configuration 140
2-11.1.2 VLAN Configuration 143
2-11.1.3 Port Filtering Profile 146
2-11.2 MLD Snooping 148
2-11.2.1 Basic Configuration 148
2-11.2.2 VLAN Configuration 151
2-11.2.3 Port Filtering Profile 154
2-12 LLDP 155
2-12.1 LLDP 155
2-12.2 LLDP-MED 159
2-14 MAC TABLE 166
2-15 VLANS 169
2-16 PRIVATE VLANS 173
2-16.1 Membership 173
2-16.2 Port Isolation 175
2-17 VCL 177
2-17.1 MAC-based VLAN 177
2-17.2 Protocol-based VLAN 179
2-17.2.1 Protocol to Group 179
2-17.2.2 Group to VLAN 182
2-17.3 IP Subnet-based VLAN 184
2-18 VOICE VLAN 186
2-18.1 Configuration 186
2-18.2 OUI 190
2-19 QOS 192
2-19.1 Port Classification 192
2-19.2 Port Policing 194
2-19.3 Port Schedulers 196
2-19.4 Port Shaping 199
2-19.5 Port Tag Remarking 202

2-19.6 Port DSCP *205*
2-19.7 DSCP-Based QoS *207*
2-19.8 DSCP Translation *209*
2-19.9 DSCP Classification *211*
2-19.10 QoS Control List *213*
2-19.11 Storm Control *217*
2-20 MIRRORING 219
2-21 UPNP 221
2-22 GVRP 223
2-22.1 Global Config *223*
2-22.2 Port Config *225*
2-23 SFLOW 227
2-24 SMTP 230

CHAPTER 3 MONITOR 232

3-1 SYSTEM 232
3-1.1 Information *232*
3-1.2 IP Status *235*
3-1.3 Log *237*
3-1.4 Detailed Log *238*
3-1.5 Overview *240*
3-2 GREEN ETHERNET 242
3-2.1 Port Power Savings *242*
3-3 PORTS 243
3-3.1 Traffic Overview *243*
3-3.2 Qos Statistics *245*
3-3.3 QCL Status *246*
3-3.4 Detailed Statistics *248*
3-3.5 SFP Detail Info *252*
3-4 DHCP 254
3-4.1 Server *254*
3-4.1.1 Statistics 254
3-4.1.2 Binding 257
3-4.1.3 Declined IP 259
3-4.2 Snooping Table *260*
3-4.3 Relay Statistics *262*
3-4.4 Detailed Statistics *264*
3-5 SECURITY 266
3-5.1 Access Management Statistics *266*
3-5.2 Network *268*
3-5.2.1 Port Security 268
3-5.2.1.1 Switch 268
3-5.2.1.2 Port 270
3-5.2.2 NAS 272
3-5.2.2.1 Switch 272
3-5.2.2.2 Port 274
3-5.2.3 ACL Status 277
3-5.2.4 ARP Inspection 279
3-5.2.5 IP Source Guard 281
3-5.3 AAA *282*
3-5.3.1 RADIUS Overview 282
3-5.3.2 RADIUS Details 284
3-5.4 Switch *286*
3-5.4.1 RMON 286

3-5.4.1.1 Statistics 286
3-5.4.1.2 History 289
3-5.4.1.3 Alarm 291
3-5.4.1.4 Event 293
3-6 LACP 295
3-6.1 System Status 295
3-6.2 Port Status 297
3-6.3 Port Statistics 299
3-7 LOOP PROTECTION 300
3-8 SPANNING TREE 302
3-8.1 Bridge Status 302
3-8.2 Port Status 304
3-8.3 Port Statistics 305
3-9 MVR 307
3-9.1 Statistics 307
3-9.2 MVR Channels Groups 309
3-9.3 MVR SFM Information 311
3-10 IPMC 313
3-10.1 IGMP Snooping 313
3-10.1.1 Status 313
3-10.1.2 Group Information 315
3-10.1.3 IPv4 SFM Information 317
3-10.2 MLD Snooping 319
3-10.2.1 Status 319
3-10.2.2 Group Information 321
3-10.2.3 IPv6 SFM Information 323
3-11 LLDP 325
3-11.1 Neighbour 325
3-11.2 LLDP-MED Neighbour 327
3-11.3 PoE 331
3-11.4 EEE 333
3-11.5 Port Statistics 335
3-12 POE 338
3-13 MAC TABLE 340
3-14 VLANS 342
3-14.1 Membership 342
3-14.2 Port 344
3-15 VCL 346
3-15.1 MAC-based VLAN 346
3-15.2 Protocol-based VLAN 347
3-15.2.1 Protocol to Group 347
3-15.2.2 Group to VLAN 349
3-15.3 IP Subnet-based VLAN 350
3-16 SFLOW 351

CHAPTER 4 DIAGNOSTICS 354

4-1 PING 354
4-2 PING6 356
4-3 CABLE DIAGNOSTICS 358
4-4 TRACEROUTE 360

CHAPTER 5 MAINTENANCE 362

5-1 RESTART DEVICE 362
5-2 REBOOT SCHEDULE 364

5-3 FACTORY DEFAULTS 365
5-4 FIRMWARE 366
5-4.1 Firmware upgrade 366
5-4.2 Firmware Selection 368
5-5 CONFIGURATION 370
5-5.1 Save startup-config 370
5-5.2 Download 372
5-5.3 Upload 373
5-5.4 Activate 374
5-5.5 Delete 375
5-6 SERVER REPORT 376

CHAPTER 6 SURVEILLANCE 377

6-1 INTRODUCTION 377
6-2 MANAGEMENT 378
6-2.1 SURVEILLANCE MODE 378
6-2.2 DEVICE LIST 379
6-3.2 CAMERA CONFIGURE 383
Config Export 383
Config Import 383

CHAPTER 7 SURVEILLANCE – GRAPHICAL MONITORING 386

7-1 Topology View 386
7-2 Floor View 395
7-3 MAP VIEW 398

CHAPTER 8 SURVEILLANCE - MAINTENANCE 400

8-1 FLOOR IMAGE 400
8-2 DIAGNOSTICS 401

Revision History

Release	Date	Revision
V1.00	2017/03/06	A1
V2.00	2018/01/20	A2

Introduction

Overview

VIVOTEK's AW-GTS-287A L2 Plus Managed Switch is a next-generation Fiber Switch offering a full suite of L2 Plus features and additional 1G/10G SFP+ uplink connections. The AW-GTS-287A L2 Plus includes advanced L3 features such as Static Route that delivers a better cost-performance ratio and a lower total cost of ownership in both Enterprise networks and backbone via fiber or copper connections. With high Gigabit port densities and Gigabit SFP, 1G/10G SFP+ support, the GTS-287A switch can act as either a departmental access layer or as an aggregation switch to form a multilevel network. Service providers can take advantage of the high SFP density to structure the aggregation of Fiber to the Building (FTTB) networks that can be extended to subscribers' sites. The AW-GTS-287A can be programmed for a number of advanced switch management functions, such as dynamic port link aggregation, Q-in-Q VLAN, Multiple Spanning Tree Protocol (MSTP), Layer 2/4 QoS, bandwidth control, IGMP/MLD snooping, GARP VLAN Registration Protocol (GVRP) and sFlow. Through link-aggregation of supporting ports, the AW-GTS-287A allows the operation of a high-speed trunk to combine with multiple ports. It enables a maximum of 14 trunk groups, with up to 16 ports in each group, and also supports connection fail-over. The AW-GTS-287A is also specially equipped with one 100~240V AC power supply unit and one 24~72V DC power supply unit to provide enhanced reliability and enable scalable redundant power supply installation. The continuous power system is designed to fulfill the specific demands of high tech facilities requiring the highest power integrity and stability. The AW-GTS-287A also features Graphic View, such as Topology/Map view for controlling and understanding network structure and device situation, and Google Map integration to view system situation status for outdoor applications.

Overview of this User Guide

- Chapter 1 "Operation of Web-based Management"
- Chapter 2 "Configuration"
- Chapter 3 "Monitor"
- Chapter 4 "Diagnostics"
- Chapter 5 "Maintenance"

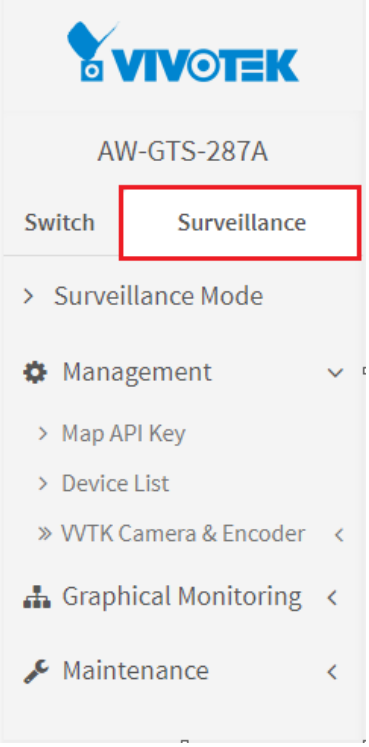
NOTE:

For users who use this switch in a surveillance application, you can go directly to Chapter 6 through Chapter 8 for information directly related to surveillance deployments.

Chapter 1 Operation of Web-based Management

IMPORTANT:

1. It is recommended to use **Chrome or Edge** to open a web interface with the switch.
2. This switch is specifically designed for surveillance applications. It comes with an integrated Surveillance interface for ease of configuration. The Surveillance interface is accessed through a tabbed menu, and the configuration changes made in its window have a higher priority than those in the Switch configuration menus.



3. You should save the configuration changes made on the Surveillance menus before leaving the web page. Otherwise, your configuration changes will be lost. The save button is located on the upper right corner of the screen.

Initial Configuration

This chapter instructs you how to configure and manage the AW-GTS-287A through the web interface. With this facility, you can easily access and monitor through any one port of the switch all the status of the switch, including MIBs status, each port activity, Spanning tree status, port aggregation status, multicast traffic, VLAN and priority status, even illegal access record and so on.
The default values of the AW-GTS-287A listed in the table below:

IP Address	DHCP client
Username	admin
Password	admin

You can use VIVOTEK's Shepherd to locate the switch. After the AW-GTS-287A has been finished network configuration, you can access the web interface by typing the static IP that you configure. For instance, type **http://192.168.1.1** in the address row in a browser, it will show the following screen and ask you input username and password in order to login and access authentication.

The default username is **"admin"** and password is **admin**. For the first time to use, please enter the default username and password, and then click the **<Login>** button. The login process now is completed. In this login menu, you have to input the complete username and password respectively, the AW-GTS-287A will not give you a shortcut to username automatically. This looks inconvenient, but safer.

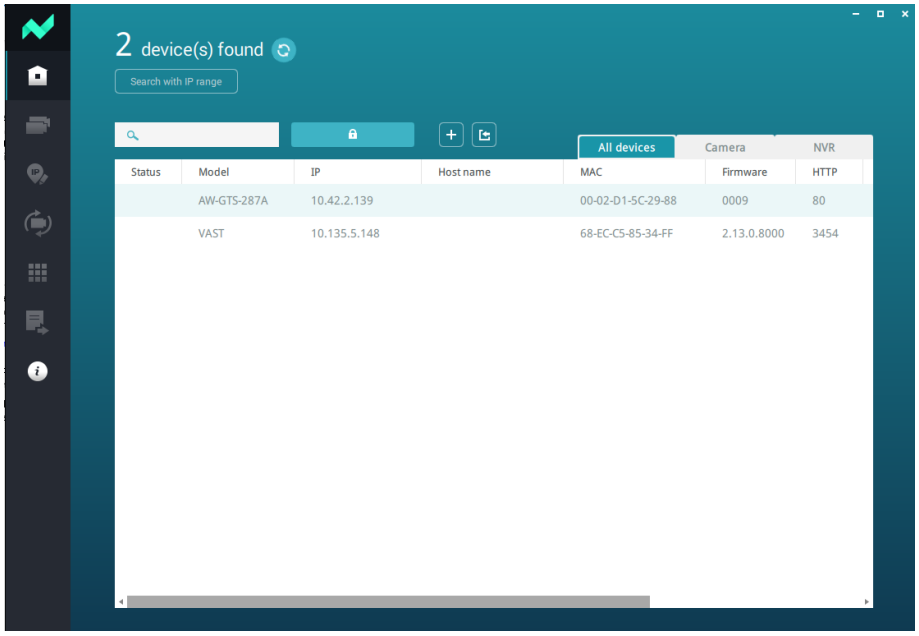
In the AW-GTS-287A, allowed two or more users using administrator's identity to manage this switch, which administrator to do the last setting, it will be an available configuration to effect the system.

NOTE:
When you login the Switch WEB/CLI to manager. You must first type the Username of the admin. Password was blank, so when you type after the end Username, please press enter. Management page to enter WEB/CLI.

When you login AW-GTS-287A switch Web UI management, you can use both ipv4 ipv6 login to manage

To optimize the display effect, we recommend you use Microsoft IE 6.0 above, Netscape V7.1 above or Firefox V1.00 above and have the resolution 1024x768. The switch supported neutral web browser interface

You can find the switch using VIVOTEK's Shepherd. If network address conflicts occur, use this utility to locate the switch.



If you double-click on the entry found on the Shepherd, web browser will be opened.

NOTE:
The Switch **default ip is DHCP client.**

NOTE:

The switch and all cameras attached must be configured in the same subnet. Otherwise, the Surveillance-related functions will not apply. You can let the switch be a DHCP client (listening to a DHCP server for IP assignment), or enable its onboard DHCP server.

Figure 1: The login page

Chapter 2 Configuration

This chapter describes the entire basic configuration tasks which includes the System Information and any manage of the Switch (e.g. Time, Account, IP, Syslog and NTP.)

2-1 System

You can identify the system by configuring the contact information, name, and location of the switch.

2-1.1 Information

The switch system's contact information is provided here.

Web interface

To configure System Information in the web interface:

1. Click Configuration, System and Information.
2. Write System Contact, System Name, System Location information in this page.
3. Click Apply

Figure 2-1.1: System Information

Parameter description:

- **System Contact :**

  The textual identification of the contact person for this managed node, together with information on how to contact this person. The allowed string length is 0 to 128, and the allowed content is the ASCII characters from 32 to 126.

- **System name :**

  An administratively assigned name for this managed node. By convention, this is the node's fully-qualified domain name. A domain name is a text string drawn from the alphabet (A-Za-z), digits (0-9), minus sign (-). No space characters are permitted as part of a name. The first character must be an alpha character. And the first or last character must not be a minus sign. The allowed string length is 0 to 128.

- **System Location :**

  The physical location of this node(e.g., telephone closet, 3rd floor). The allowed string length is 0 to 128, and the allowed content is the ASCII characters from 32 to 126.

Buttons

- **Apply :**

  Click to save changes.

- **Reset :**

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

2-1.2 IP

The IPv4 address for the switch could 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

Configure IP basic settings, control IP interfaces and IP routes.

The maximum number of interfaces supported is 8 and the maximum number of routes is 32.

Web Interface

To configure an IP address in the web interface:

1. Click Configuration, System and IP.
2. Click Add Interface then you can create new Interface on the switch.
3. Click Add Route then you can create new Route on the switch.
4. Click Apply.

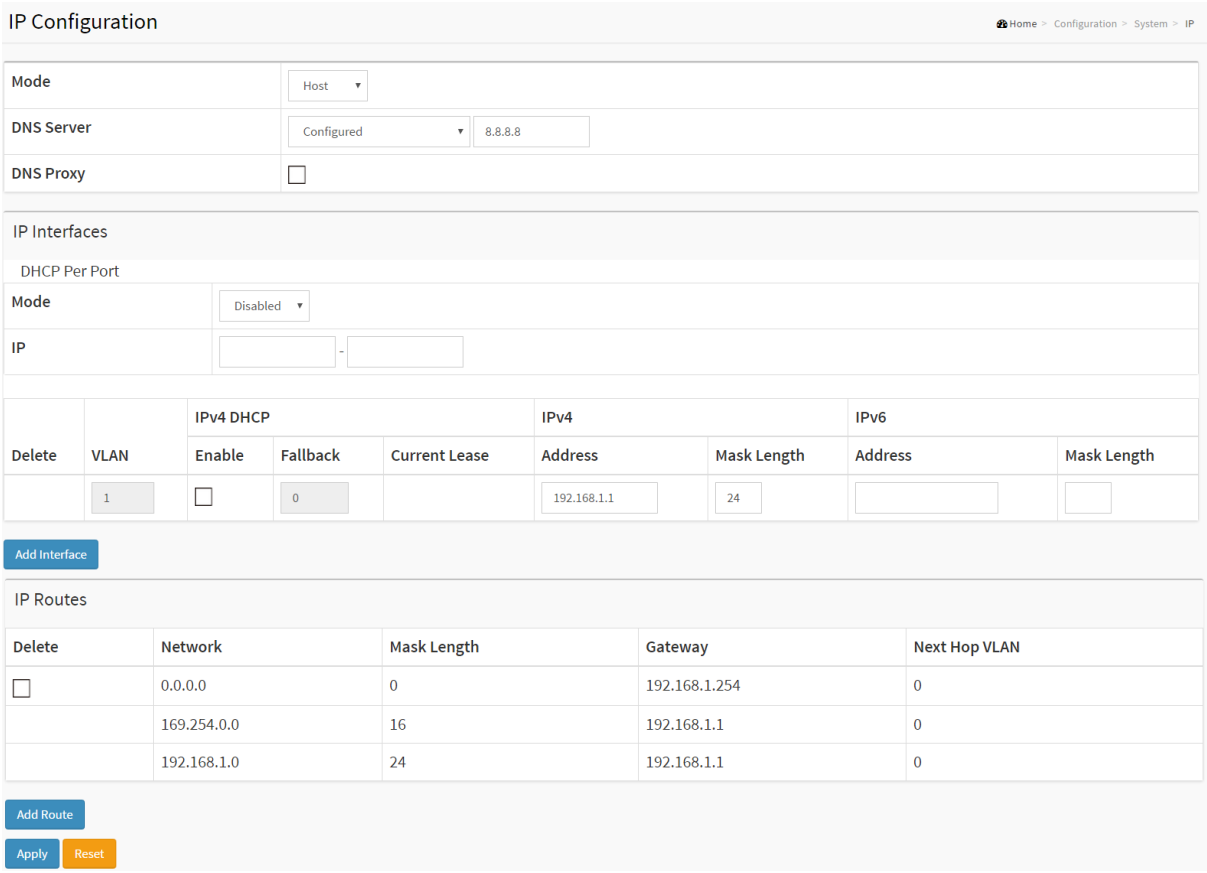


Figure2-1.2: The IP configuration

Parameter description:

IP Configuration

- **Mode :**

  Configure whether the IP stack should act as a Host or a Router. In Host mode, IP traffic between interfaces will not be routed. In Router mode traffic is routed between all interfaces.

- **DNS Server :**

  This setting controls the DNS name resolution done by the switch. The following modes are supported:

  - From any DHCP interfaces:
    The first DNS server offered from a DHCP lease to a DHCP-enabled interface will be used.
  - No DNS server:
    No DNS server will be used.
  - Configured:
    Explicitly provide the IP address of the DNS Server in dotted decimal notation.
  - From this DHCP interface
    Specify from which DHCP-enabled interface a provided DNS server should be preferred.

- **DNS Proxy :**

  When DNS proxy is enabled, system will relay DNS requests to the currently configured DNS server, and reply as a DNS resolver to the client devices on the network.

IP Interfaces

- **DHCP Per Port Mode :**

  Enable/Disable DHCP per port.

- **DHCP Per Port IP :**

  Define the IP range for DHCP per port.

- **Delete :**

  Select this option to delete an existing IP interface.

- **VLAN :**

  The VLAN associated with the IP interface. Only ports in this VLAN will be able to access the IP interface. This field is only available for input when creating a new interface.

- **IPv4 DHCP Enabled :**

  Enable the DHCP client by checking this box. If this option is enabled, the system will configure the IPv4 address and mask of the interface using the DHCP protocol. The DHCP client will announce the configured System Name as hostname to provide DNS lookup.

- **IPv4 DHCP Fallback Timeout :**

  The number of seconds for trying to obtain a DHCP lease. After this period expires, a configured IPv4 address will be used as IPv4 interface address. A value of zero disables the fallback mechanism, such that DHCP will keep retrying until a valid lease is obtained. Legal values are 0 to 4294967295 seconds.

- **IPv4 DHCP Current Lease :**

  For DHCP interfaces with an active lease, this column show the current interface address, as provided by the DHCP server.

- **IPv4 Address :**

  The IPv4 address of the interface in dotted decimal notation.
  If DHCP is enabled, this field is not used. The field may also be left blank if IPv4 operation on the interface is not desired.

- **IPv4 Mask Length :**

  The IPv4 network mask, in number of bits (prefix length). Valid values are between 0 and 30 bits for a IPv4 address.
  If DHCP is enabled, this field is not used. The field may also be left blank if IPv4 operation on the interface is not desired.

- **IPv6 Address :**

  The IPv6 address of the interface. A IPv6 address is in 128-bit records represented as eight fields of up to four hexadecimal digits with a colon separating each field (:). For example, fe80::215:c5ff:fe03:4dc7. The symbol :: is a special syntax that can be used as a shorthand way of representing multiple 16-bit groups of contiguous zeros; but it can appear only once. It can also represent a legally valid IPv4 address. For example, ::192.1.2.34.
  The field may be left blank if IPv6 operation on the interface is not desired.

- **IPv6 Mask Length :**

  The IPv6 network mask, in number of bits (prefix length). Valid values are between 1 and 128 bits for a IPv6 address.
  The field may be left blank if IPv6 operation on the interface is not desired.

IP Routes

- **Delete :**

  Select this option to delete an existing IP route.

- **Network :**

  The destination IP network or host address of this route. Valid format is dotted decimal notationor a valid IPv6 notation. A default route can use the value 0.0.0.0or IPv6 :: notation.

- **Mask Length :**

  The destination IP network or host mask, in number of bits (prefix length). It defines how much of a network address that must match, in order to qualify for this route. Valid values are between 0 and 32 bits respectively 128 for IPv6 routes. Only a default route will have a mask length of 0 (as it will match anything).

- **Gateway :**

  The IP address of the IP gateway. Valid format is dotted decimal notationor a valid IPv6 notation. Gateway and Network must be of the same type.

- **Next Hop VLAN (Only for IPv6) :**

  The VLAN ID (VID) of the specific IPv6 interface associated with the gateway.
  The given VID ranges from 1 to 4094 and will be effective only when the corresponding IPv6 interface is valid.
  If the IPv6 gateway address is link-local, it must specify the next hop VLAN for the gateway.
  If the IPv6 gateway address is not link-local, system ignores the next hop VLAN for the gateway.

Buttons

- **Add Interface :**

  Click to add a new IP interface. A maximum of 8 interfaces is supported.

- **Add Route :**

  Click to add a new IP route. A maximum of 32 routes is supported.

- **Apply :**

  Click to save changes.

- **Reset :**

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

2-1.3 NTP

NTP is Network Time Protocol and 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's processing.

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 able to get the correct time. The switch supports configurable time zone from –12 to +13 step 1 hour.

Default Time zone: +8 Hrs.

Web Interface

To configure NTP in the web interface:

1. Click Configuration, System and NTP.
2. Specify the Time parameter in manual parameters.
3. Click Apply.

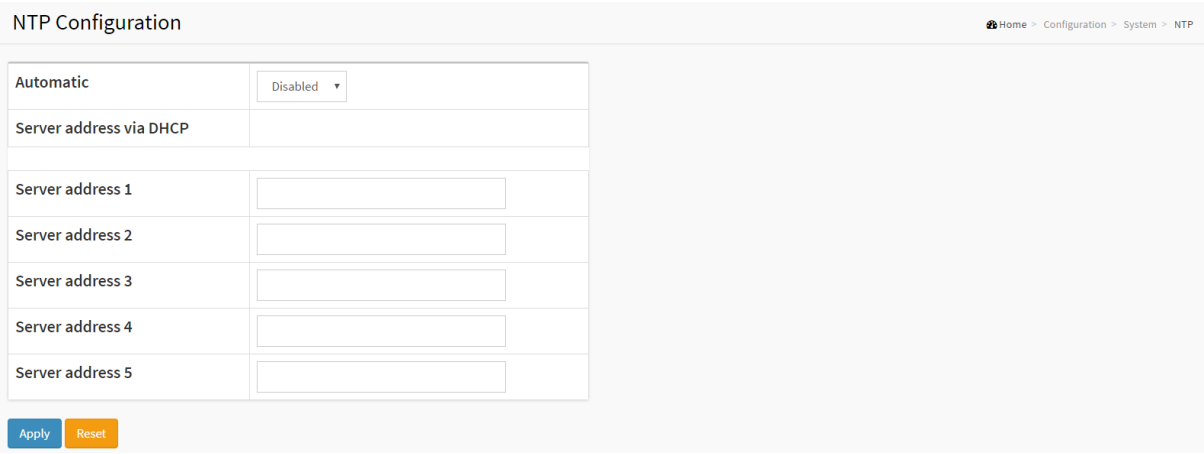


Figure 2-1.3: The NTP configuration

Parameter description:

- **Automatic :**

  Indicates the Automatic mode operation. Possible modes are:
  Enabled: NTP servers available from the DHCP.
  Disabled: NTP servers available from the config.

- **Server address via DHCP :**

  Specify a list of IP addresses indicating NTP servers available to the client.

- **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

- **Apply :**

  Click to save changes.

- **Reset :**

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

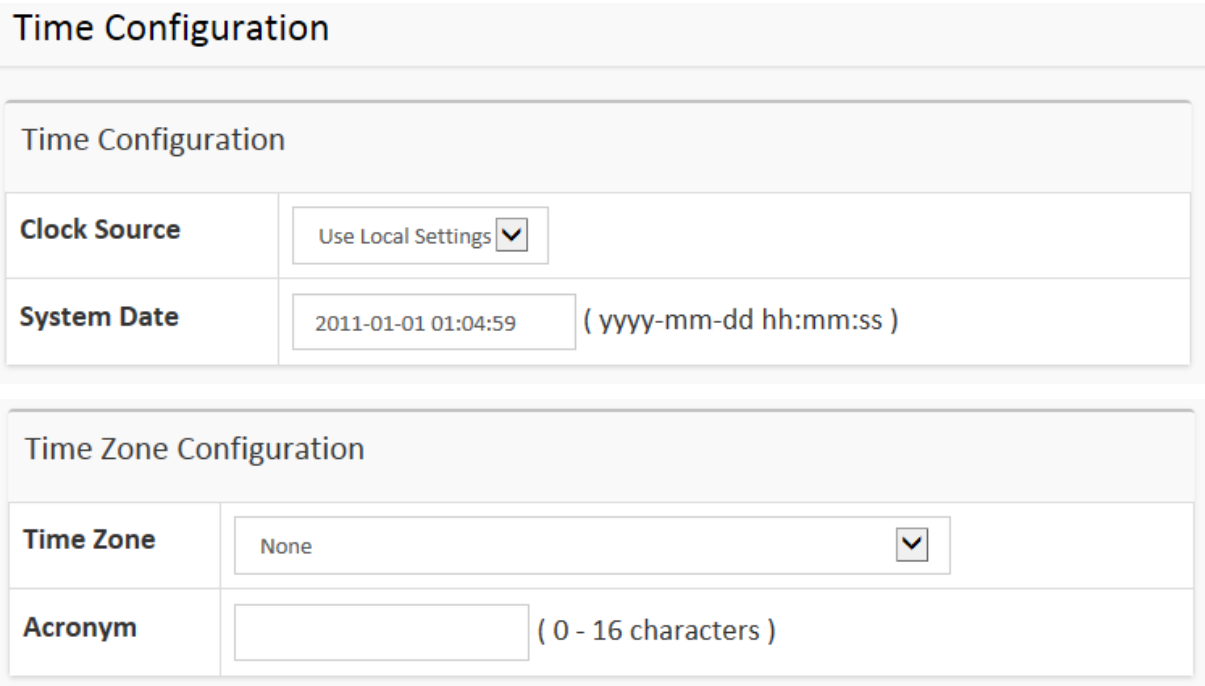
2-1.4 Time

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” and “Minute” within the valid value range indicated in each item.

Web Interface

To configure Time in the web interface:

1. Click Configuration, System and Time.
2. Specify the Time parameter.
3. Click Apply.



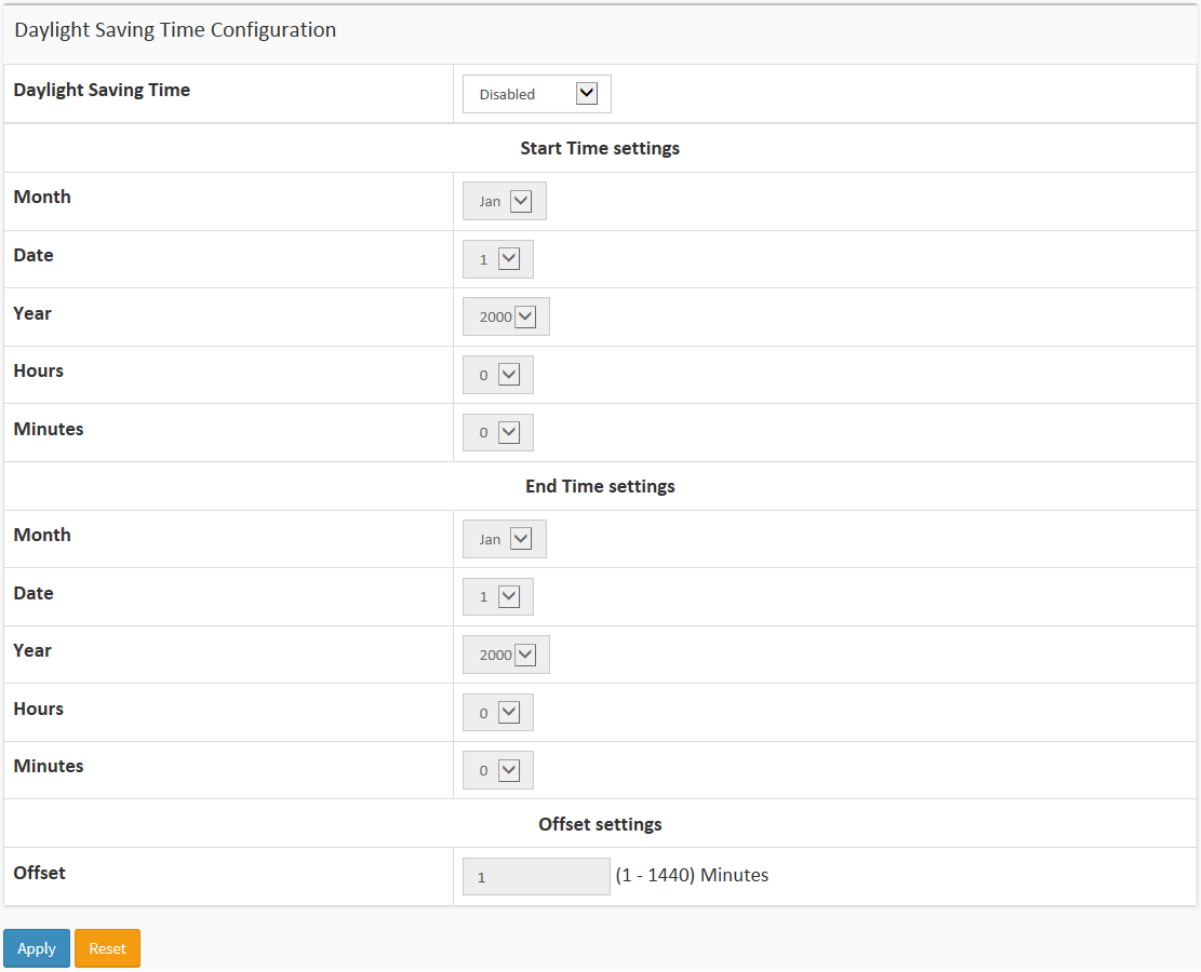


Figure 2-1.4: The time configuration

Parameter description:

Time Configuration

- **Clock Source :**

  There are two modes for configuring how the Clock Source from. Select "Use Local Settings" : Clock Source from Local Time. Select "Use NTP Server" : Clock Source from NTP Server.

- **System Date :**

  Show the current time of the system. The year of system date limits between 2011 and 2037.

Time Zone Configuration

- **Time Zone :**

  Lists various Time Zones worldwide. Select appropriate Time Zone from the drop down and click Apply to set.

- **Acronym :**

  User can set the acronym of the time zone. This is a User configurable acronym to identify the time zone. (Range: Up to 16 characters)

Daylight Saving Time Configuration

- **Daylight Saving Time :**

This is used to set the clock forward or backward according to the configurations set below for a defined Daylight Saving Time duration. Select 'Disable' to disable the Daylight Saving Time configuration. Select 'Recurring' and configure the Daylight Saving Time duration to repeat the configuration every year. Select 'Non-Recurring' and configure the Daylight Saving Time duration for single time configuration. (Default: Disabled).

Recurring Configuration

- **Start time settings :**

  Week - Select the starting week number.

  Day - Select the starting day.

  Month - Select the starting month.

  Hours - Select the starting hour.

  Minutes - Select the starting minute.

- **End time settings :**

  Week - Select the ending week number.

  Day - Select the ending day.

  Month - Select the ending month.

  Hours - Select the ending hour.

  Minutes - Select the ending minute.

- **Offset settings :**

  Offset - Enter the number of minutes to add during Daylight Saving Time. (Range: 1 to 1440)

NOTE: The under "Start Time Settings" and "End Time Settings" was displayed what you set on the "Start Time Settings" and "End Time Settings" field information.

Buttons

- **Apply :**

  Click to save changes.

- **Reset :**

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

2-1.5 Log

The log 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.

Web Interface

To configure log configuration in the web interface:

1. Click Configuration, System and log.
2. Specify the Server Address.
3. Evoke the Syslog to enable it.
4. Click Apply.

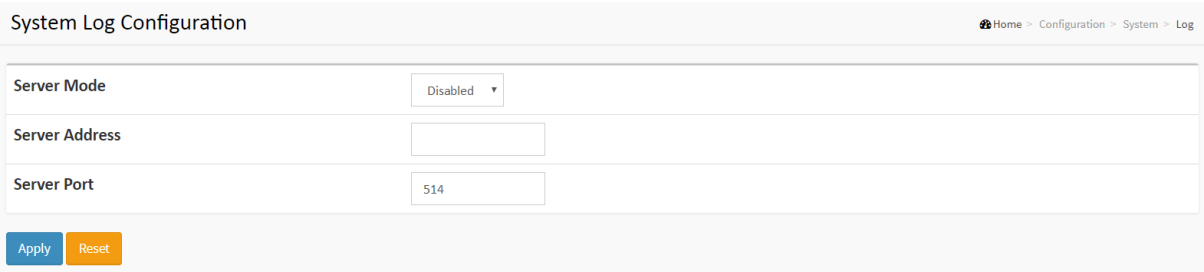


Figure2-1.5: The System Log configuration

Parameter description:

- **Server Mode :**

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

  Enabled: Enable server mode operation.

  Disabled: Disable server mode operation.

- **Server Address :**

  Indicates the IPv4 hosts address of syslog server. If the switch provide DNS feature, it also can be a host name.

- **Server Port :**

  Indicates the service port of syslog server. The port range is 1-65535.

Buttons

- **Apply :**

  Click to save changes.

- **Reset :**

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

2-2 Green Ethernet

2-2.1 Port Power Savings

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

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 wakeup time information using the LLDP protocol.

EEE works for ports in auto-negotiation mode, where the port is negotiated to either 1G or 100 Mbit full duplex mode.

For ports that are not EEE-capable the corresponding EEE checkboxes are grayed out and thus impossible to enable EEE for.

When a port is powered down for saving power, outgoing traffic is stored in a buffer until the port is powered up again. Because there are some overhead in turning the port down and up, more power can be saved if the traffic can be buffered up until a large burst of traffic can be transmitted. Buffering traffic will give some latency in the traffic.

Web Interface

To configure a Port Power Saving Configuration in the web interface:

1. Click Configuration, Green Ethernet and Port Power Savings.
2. Evoke to enable or disable the ActiPHY, PerfectReach, EEE and EEE Urgent Queues.
3. Click Apply.

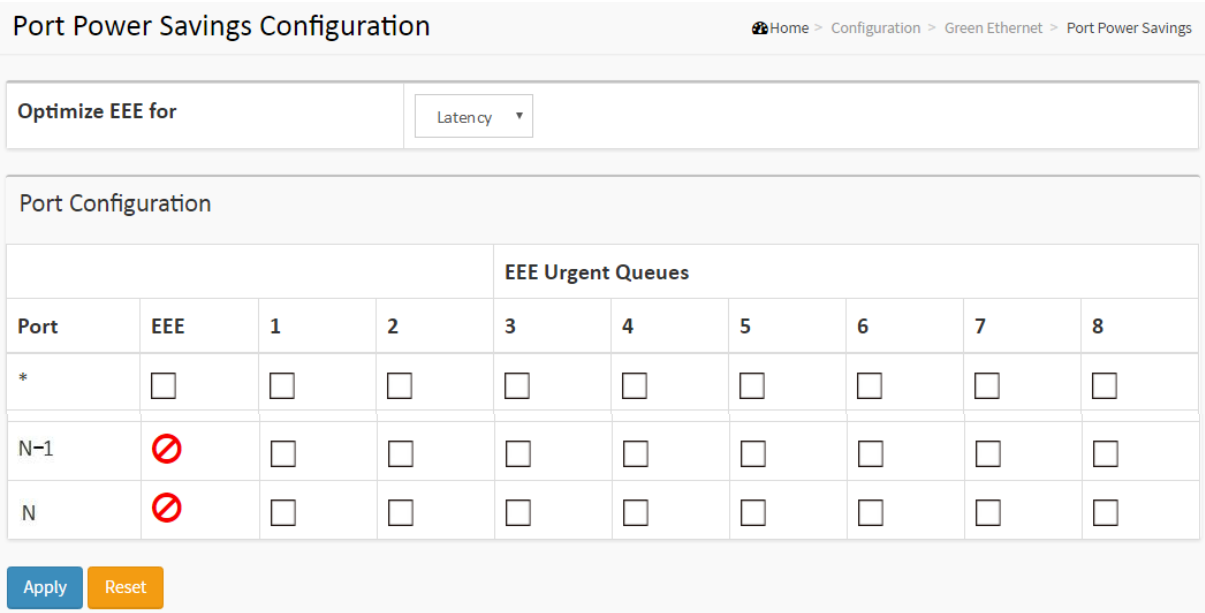


Figure 2-2.1: The Port Power Saving Configuration

Parameter description:

Optimize EEE for :

The switch can be set to optimize EEE for either best power saving or least traffic latency.

- **Port :**

  The switch port number of the logical port.

- **EEE :**

  Controls whether EEE is enabled for this switch port.

  For maximizing power savings, the circuit isn't started at once transmit data is ready for a port, but is instead queued until a burst of data is ready to be transmitted. This will give some traffic latency.

  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.

- **EEE Urgent Queues :**

  Queues set will activate transmission of frames as soon as data is available. Otherwise the queue will postpone transmission until a burst of frames can be transmitted.

Buttons

- **Apply :**

  Click to save changes.

- **Reset :**

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

2-3 Ports Configuration

The section describes 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.

2-3.1 Ports

This page displays current port configurations. Ports can also be configured here.

Web Interface

To configure a Current Port Configuration in the web interface:

1. Click Configuration, Ports Configuration and Ports.
2. Specify the Speed Configured, Flow Control, Maximum Frame size.
3. Click Apply.

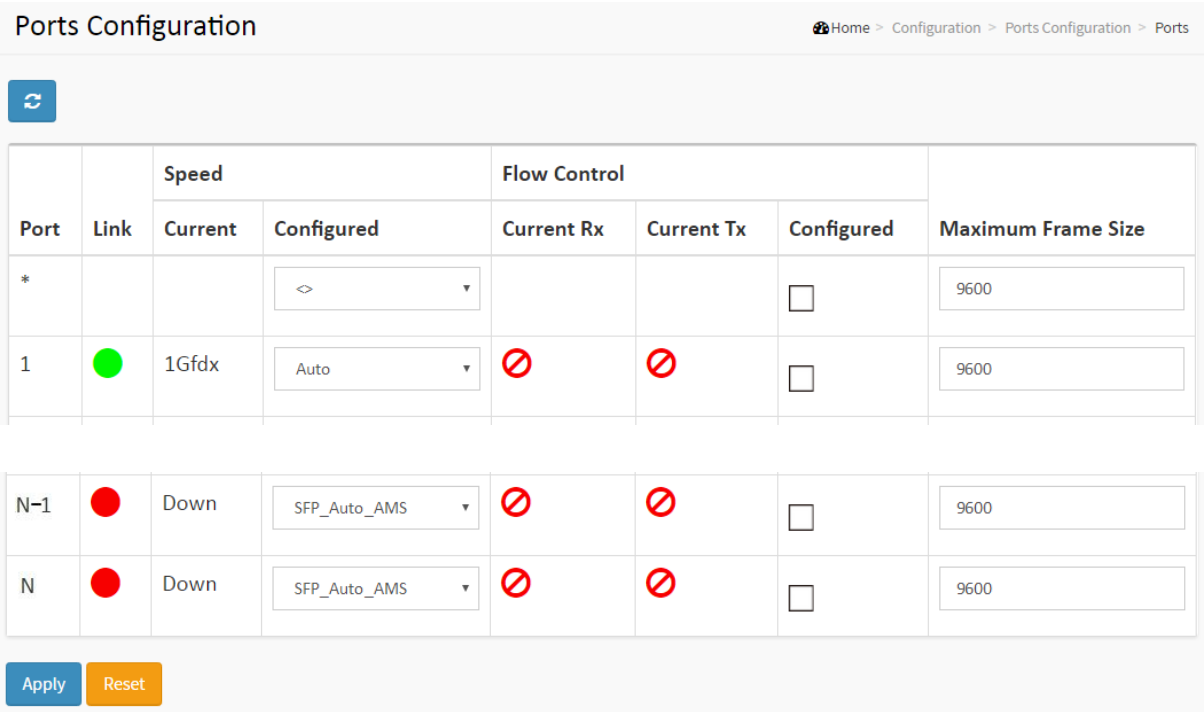


Figure 2-3.1: The Port Configuration

Parameter description:

- **Port :**

  This is the logical port number for this row.

- **Link :**

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

- **Current Link Speed :**

Provides the current link speed of the port.

- **Configured Link Speed :**

  Selects any available link speed for the given switch port. Only speeds supported by the specific port is shown. Possible speeds are:

  Disabled - Disables the switch port operation.

  Auto - Port auto negotiating speed with the link partner and selects the highest speed that is compatible with the link partner.

  10Mbps HDX - Forces the cu port in 10Mbps half-duplex mode.

  10Mbps FDX - Forces the cu port in 10Mbps full duplex mode.

  100Mbps HDX - Forces the cu port in 100Mbps half-duplex mode.

  100Mbps FDX - Forces the cu port in 100Mbps full duplex mode.

  1Gbps FDX - Forces the port in 1Gbps full duplex

  2.5Gbps FDX - Forces the Serdes port in 2.5Gbps full duplex mode.

  SFP_Auto_AMS - Automatically determines the speed of the SFP.

  NOTE: There is no standardized way to do SFP auto detect, so here it is done by reading the SFP rom. Due to the missing standardized way of doing SFP auto detect some SFPs might not be detectable. The port is set in AMS mode. Cu port is set in Auto mode.

  100-FX - SFP port in 100-FX speed. Cu port disabled.

  100-FX_AMS - Port in AMS mode. SFP port in 100-FX speed. Cu port in Auto mode.

  1000-X - SFP port in 1000-X speed. Cu port disabled.

  1000-X_AMS - Port in AMS mode. SFP port in 1000-X speed. Cu port in Auto mode. Ports in AMS mode with 1000-X speed has Cu port preferred. Ports in AMS mode with 100-FX speed has fiber port preferred.

- **Flow Control :**

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

  Check the configured column to use flow control. This setting is related to the setting for Configured Link Speed.

- **Maximum Frame Size :**

  Enter the maximum frame size allowed for the switch port, including FCS.

Buttons

- **Apply :**

  Click to save changes.

- **Reset :**

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

- **Upper left icon (Refresh) :**

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

2-3.2 Ports Description

The section describes 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

Web Interface

To configure a Port Description in the web interface:

1. Click Configuration, Port Configuration and 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 Apply.

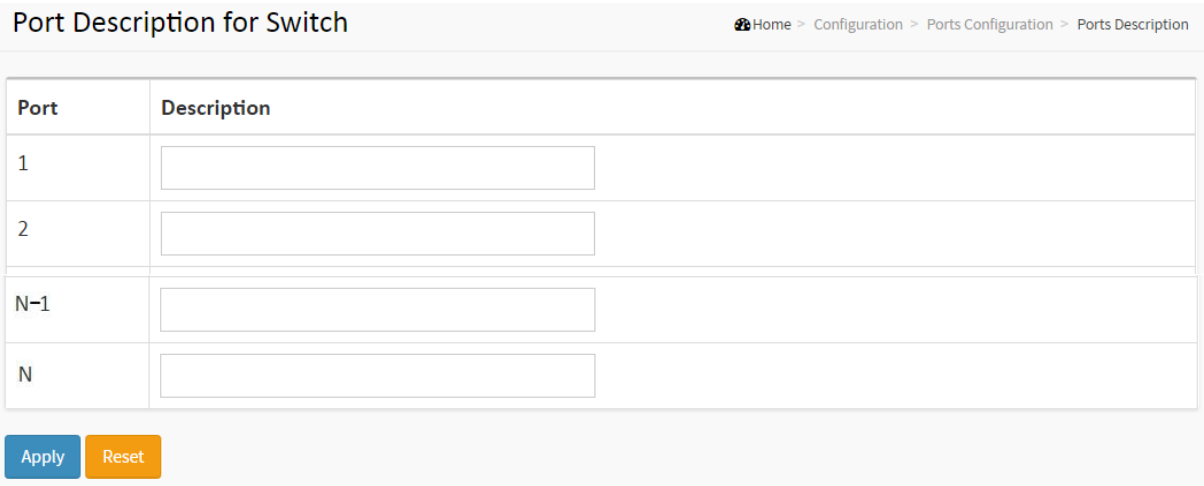


Figure 2-3.2: The Port Configuration

Parameter description:

- **Port :**

  This is the logical port number for this row.

- **Description :**

  Enter up to 47 characters to be descriptive name for identifies this port.

Buttons

- **Apply :**

  Click to save changes.

- **Reset :**

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

2-4 DHCP

The section describes to configure the DHCP Snooping parameters of the switch. The DHCP Snooping can prevent attackers from adding their own DHCP servers to the network.

2-4.1 Server

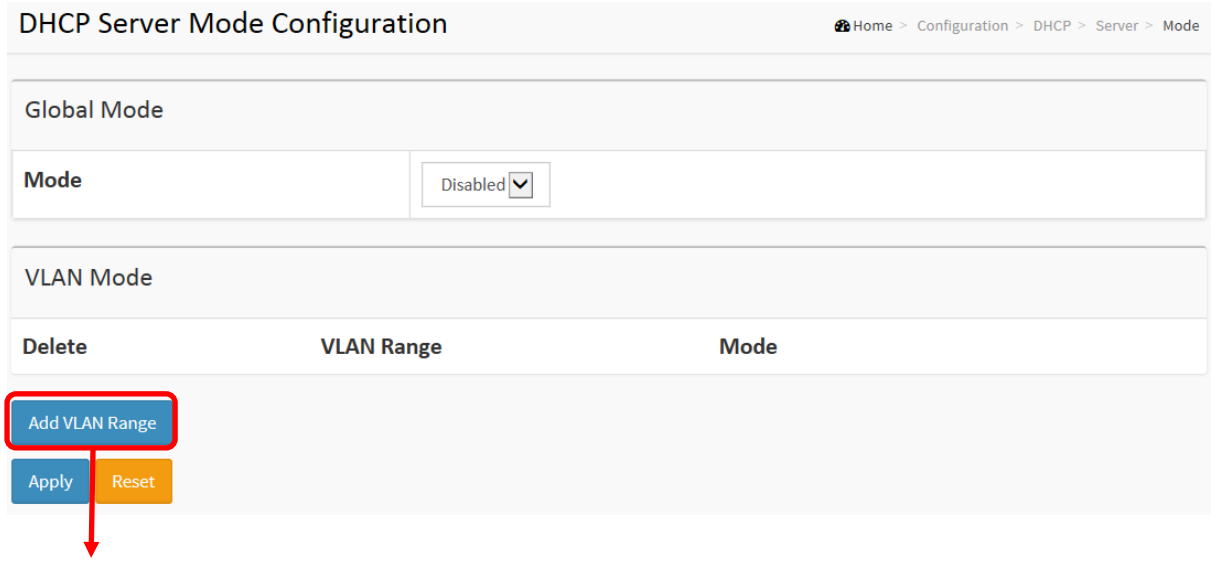
2-4.1.1 Mode

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

Web Interface

To configure DHCP server mode in the web interface:

1. Click Configuration, DHCP, Server and Mode.
2. Select "Enabled" in the Global Mode of DHCP Server Mode Configuration.
3. Add Vlan range.
4. Click Apply.



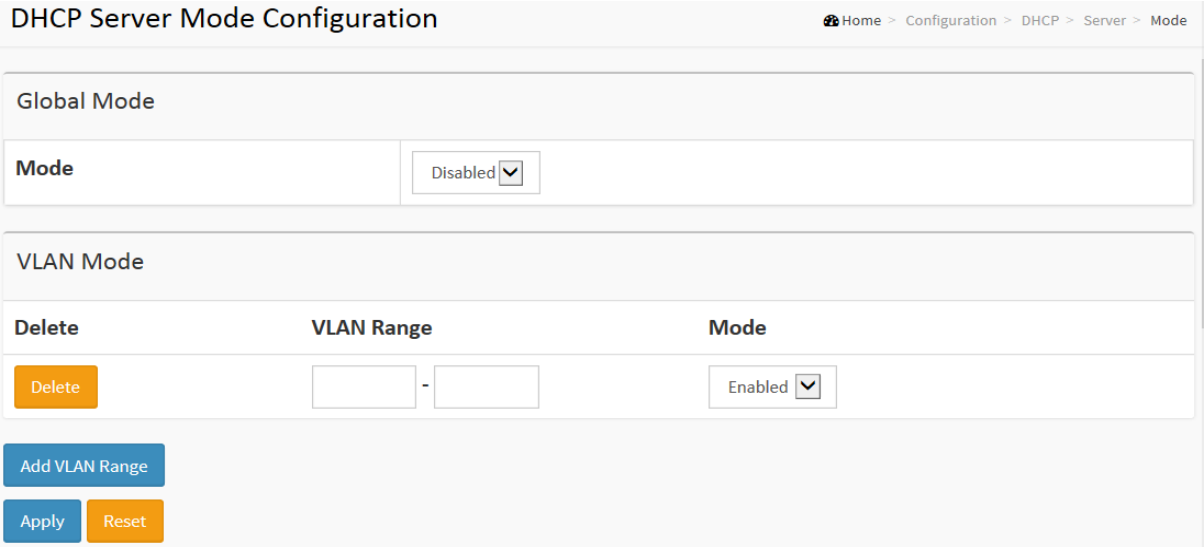


Figure 2-4.1.1: The DHCP server Mode

Parameter description:

- **Mode :**

  Configure the operation mode per system. Possible modes are:
  Enable: Enable DHCP server per system.
  Disable: Disable DHCP server pre system.

- **VLAN Range :**

  Indicate the VLAN range in which DHCP server is enabled or disabled. The first VLAN ID must be smaller than or equal to the second VLAN ID. BUT, if the VLAN range contains only 1 VLAN ID, then you can just input it into either one of the first and second VLAN ID or both.

  On the other hand, if you want to disable existed VLAN range, then you can follow the steps.

  1. press "ADD VLAN Range" to add a new VLAN range.

  2. Input the VLAN range that you want to disable.

  3. Choose Mode to be disabled.

  4. Press Apply to apply the change.

  Then, you will see the disabled VLAN range is removed from the DHCP Server mode configuration page.

- **Mode :**

  Indicate the operation mode per VLAN. Possible modes are:
  Enable: Enable DHCP server per VLAN.
  Disable: Disable DHCP server pre VLAN.

Buttons

- **Delete :**

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

- **Add VLAN Range :**

  Click to add a new VLAN range.

- **Apply :**

  Click to save changes.

- **Reset :**

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

2-4.1.2 Excluded IP

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

Web Interface

To configure DHCP server excluded IP in the web interface:

1. Click Configuration, DHCP, Server and Excluded IP.
2. Click Add IP Range then you can create new IP Range on the switch.
3. Click Apply.

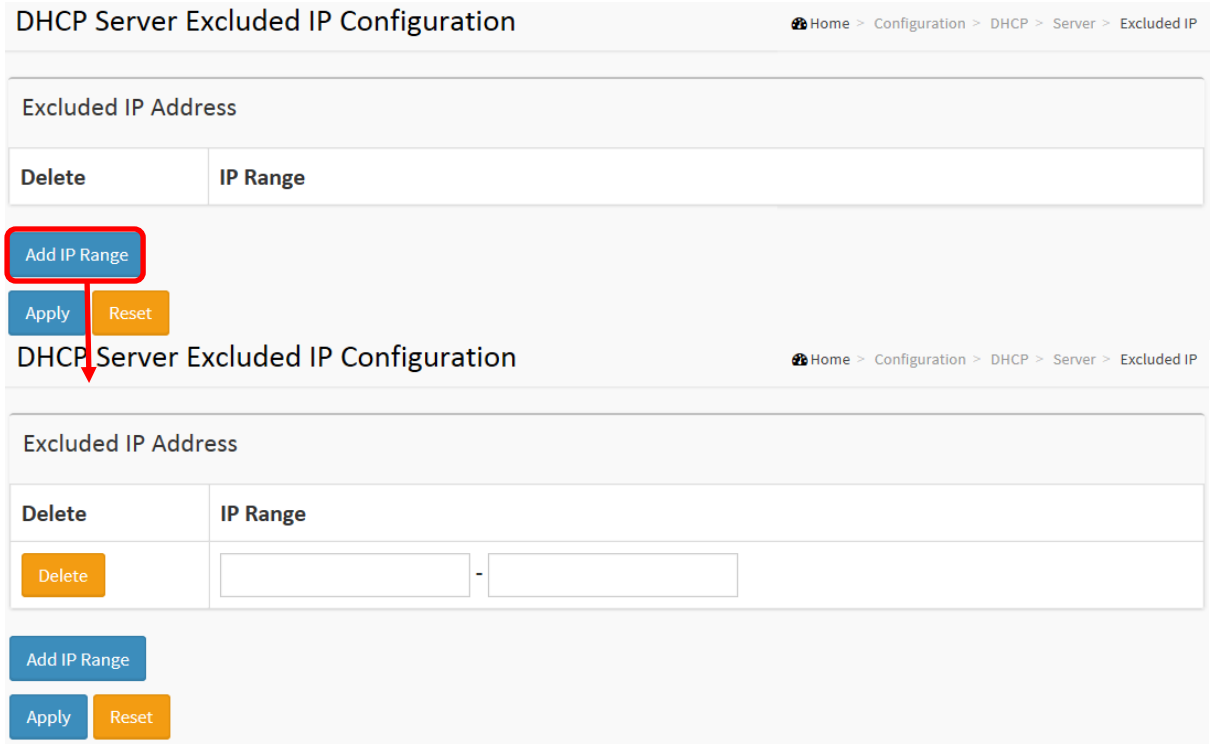


Figure 2-4.1.2: The DHCP server excluded IP

Parameter description:

- **IP Range :**

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

Buttons

- **Delete :**

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

- **Add IP Range :**

  Click to add a new excluded IP range.

- **Apply :**

  Click to save changes.

- **Reset :**

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

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

Web Interface

To configure DHCP server pool in the web interface:

1. Click Configuration, DHCP, Server and Pool.
2. Click Add New Pool then you can create new Pool on the switch.
3. Click Apply.

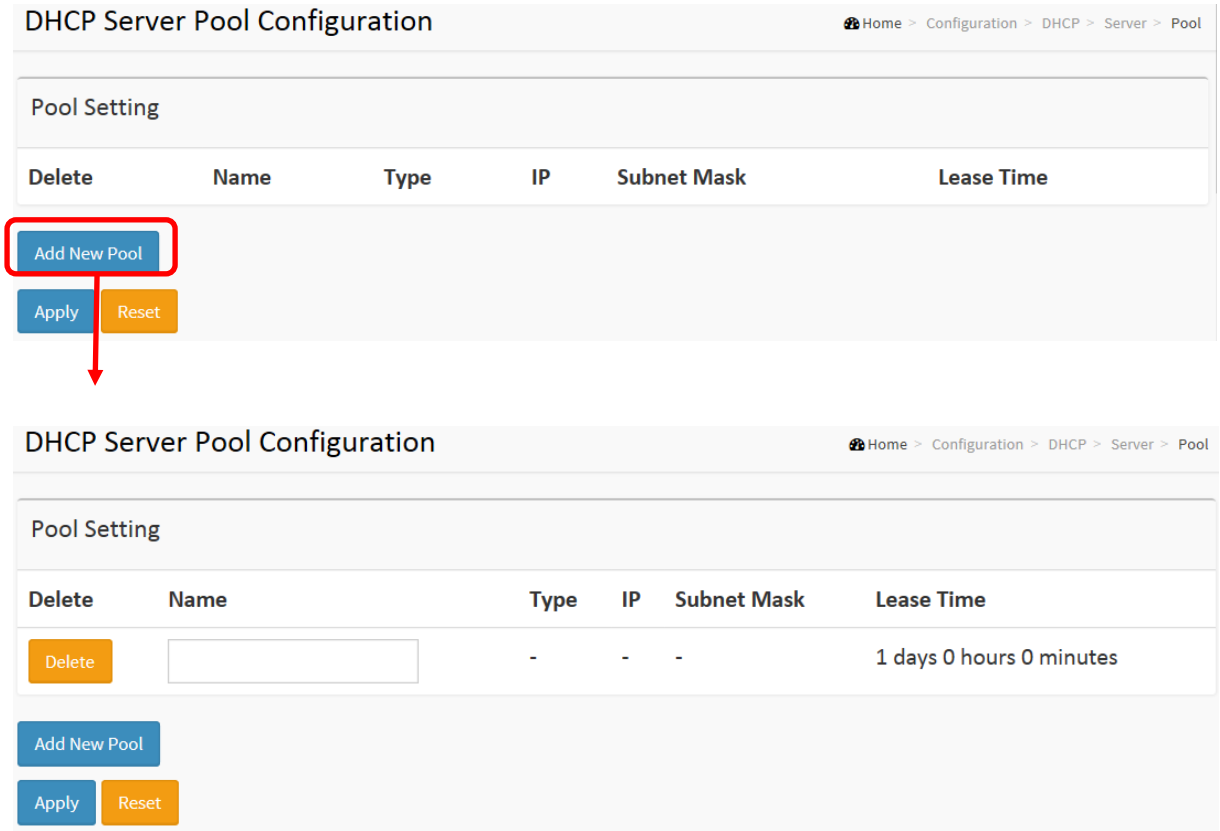


Figure 2-4.1.3: The DHCP server pool

Parameter description:

Pool Setting

Add or delete pools.

Adding a pool and giving a name is to create a new pool with "default" configuration. If you want to configure all settings including type, IP subnet mask and lease time, you can click the pool name to go into the configuration page.

- **Name :**

  Configure the pool name that accepts all printable characters, except white space. If you want to configure the detail settings, you can click the pool name to go into the configuration page.

- **Type :**

  Display which type of the pool is.

  Network: the pool defines a pool of IP addresses to service more than one DHCP client.

  Host: the pool services for a specific DHCP client identified by client identifier or hardware address.

  If "-" is displayed, it means not defined.

- **IP :**

  Display network number of the DHCP address pool.

  If "-" is displayed, it means not defined.

- **Subnet Mask :**

  Display subnet mask of the DHCP address pool.

  If "-" is displayed, it means not defined.

- **Lease Time :**

  Display lease time of the pool.

Buttons

- **Delete :**

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

- **Add New Pool :**

  Click to add a new DHCP pool.

- **Apply :**

  Click to save changes.

- **Reset :**

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

2-4.2 Snooping

DHCP Snooping is used to block intruder on the untrusted ports of the switch device when it tries to intervene by injecting a bogus DHCP reply packet to a legitimate conversation between the DHCP client and server.

The section describes to configure the DHCP Snooping parameters of the switch. The DHCP Snooping can prevent attackers from adding their own DHCP servers to the network.

Web Interface

To configure DHCP snooping in the web interface:

1. Click Configuration, DHCP and Snooping.
2. Select "Enabled" in the Mode of DHCP Snooping Configuration.
3. Select "Trusted" of the specific port in the Mode of Port Mode Configuration.
4. Click Apply.

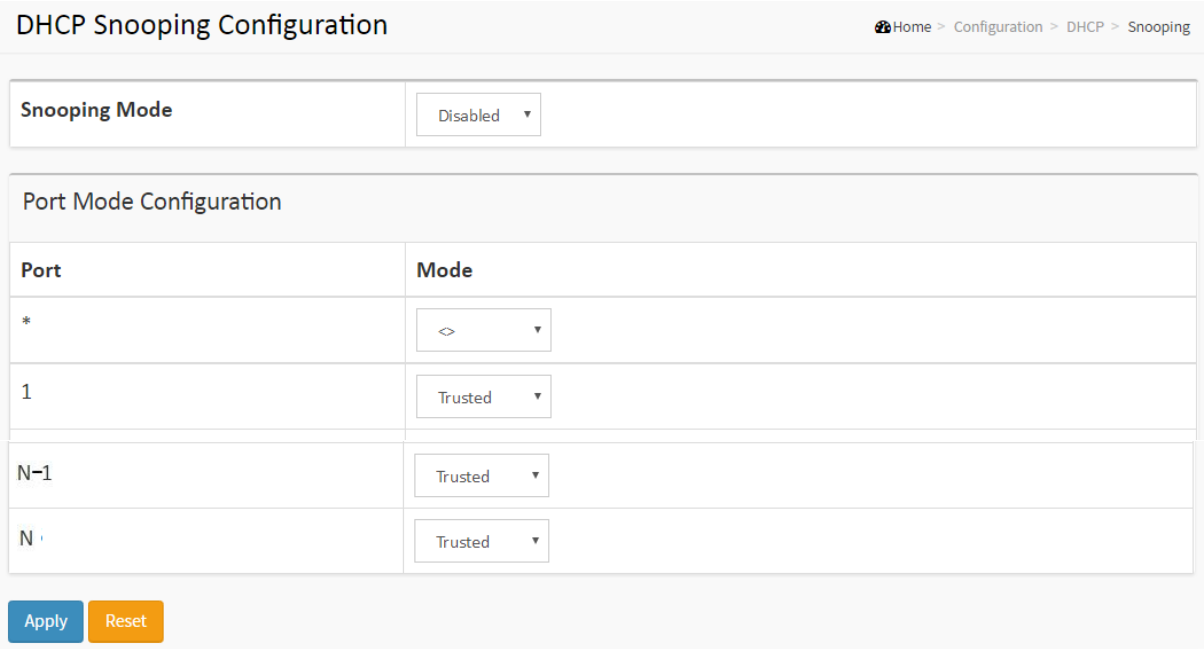


Figure 2-4.2: The DHCP Snooping Configuration

Parameter description:

- **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 Configuration**

  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

- **Apply :**

  Click to save changes.

- **Reset :**

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

2-4.3 Relay

A DHCP relay agent is used to forward and to transfer DHCP messages between the clients and the server when they are not in the same subnet domain. It stores the incoming interface IP address in the GIADDR field of the DHCP packet. The DHCP server can use the value of GIADDR field to determine the assigned subnet. For such condition, please make sure the switch configuration of VLAN interface IP address and PVID(Port VLAN ID) correctly.

Web Interface

To configure DHCP Relay in the web interface:

1. Click Configuration, DHCP and Relay
2. Specify the Relay Mode, Relay server, Relay Information Mode, Relay Information police.
3. Click Apply.

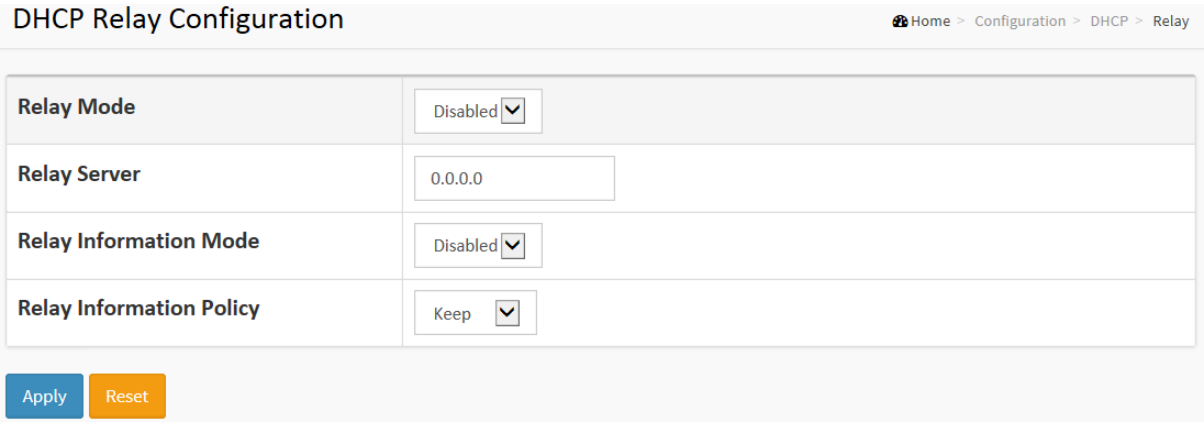


Figure 2-4.3: The DHCP Relay Configuration

Parameter description:

- **Relay Mode :**

  Indicates the DHCP relay mode operation.

  Possible modes are:

  Enabled: Enable DHCP relay mode operation. When DHCP relay mode operation is enabled, the agent forwards and transfers DHCP messages between the clients and the server when they are not in the same subnet domain. And the DHCP broadcast message won't be flooded for security considerations.

  Disabled: Disable DHCP relay mode operation.

- **Relay Server :**

  Indicates the DHCP relay server IP address.

- **Relay Information Mode :**

  Indicates the DHCP relay information mode option operation. The option 82 circuit ID format as "[vlan_id][module_id][port_no]". The first four characters represent the VLAN ID, the fifth and sixth characters are the module ID(in standalone device it always equal 0, in stackable device it means switch ID), and the last two characters are the port number. For example, "00030108" means the DHCP message receive form VLAN ID 3, switch ID 1, port

No 8. And the option 82 remote ID value is equal the switch MAC address.

Possible modes are:

Enabled: Enable DHCP relay information mode operation. When DHCP relay information mode operation is enabled, the agent inserts specific information (option 82) into a DHCP message when forwarding to DHCP server and removes it from a DHCP message when transferring to DHCP client. It only works when DHCP relay operation mode is enabled.

Disabled: Disable DHCP relay information mode operation.

- **Relay Information Policy :**

  Indicates the DHCP relay information option policy. When DHCP relay information mode operation is enabled, if the agent receives a DHCP message that already contains relay agent information it will enforce the policy. The 'Replace' policy is invalid when relay information mode is disabled. Possible policies are:
  Replace: Replace the original relay information when a DHCP message that already contains it is received.
  Keep: Keep the original relay information when a DHCP message that already contains it is received.
  Drop: Drop the package when a DHCP message that already contains relay information is received.

Buttons

- **Apply :**

  Click to save changes.

- **Reset :**

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

2-5 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.

2-5.1 Switch

2-5.1.1 Users

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

Web Interface

To configure User in the web interface:

1. Click Configuration, Security, Switch and Users.
2. Click Add new user
3. Specify the User Name parameter.
4. Click Apply.

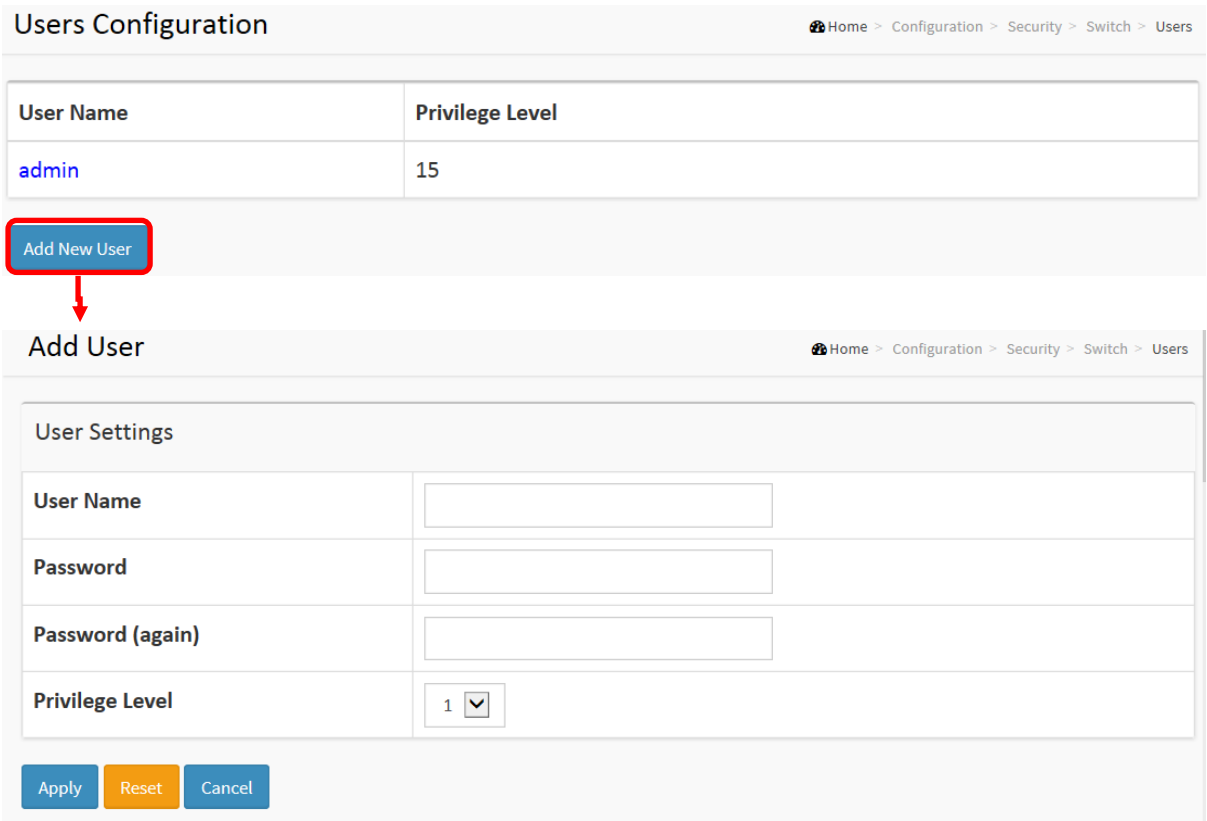


Figure 2-5.1.1: The Users configuration

Parameter description:

- **User Name :**

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

- **Password :**

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

- **Password (again) :**

  To type the password again. You must type the same password again in the field.

- **Privilege Level :**

  The privilege level of the user. The allowed range is 1 to 15. If the privilege level value is 15, it can access all groups, i.e. that is granted the fully control of the device. But others value 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.

Buttons

- **Apply :**

  Click to save changes.

- **Reset :**

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

- **Cancel :**

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

- **Delete User :**

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

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 Ports Private VLANs QoS SMTP SNMP Security Spanning Tree System Trap Event VCL VLANs Voice VLAN Privilege Levels from 1 to 15 .

Web Interface

To configure Privilege Level in the web interface:

1. Click Configuration, Security, Switch and Privilege Level.
2. Specify the Privilege parameter.
3. Click Apply.

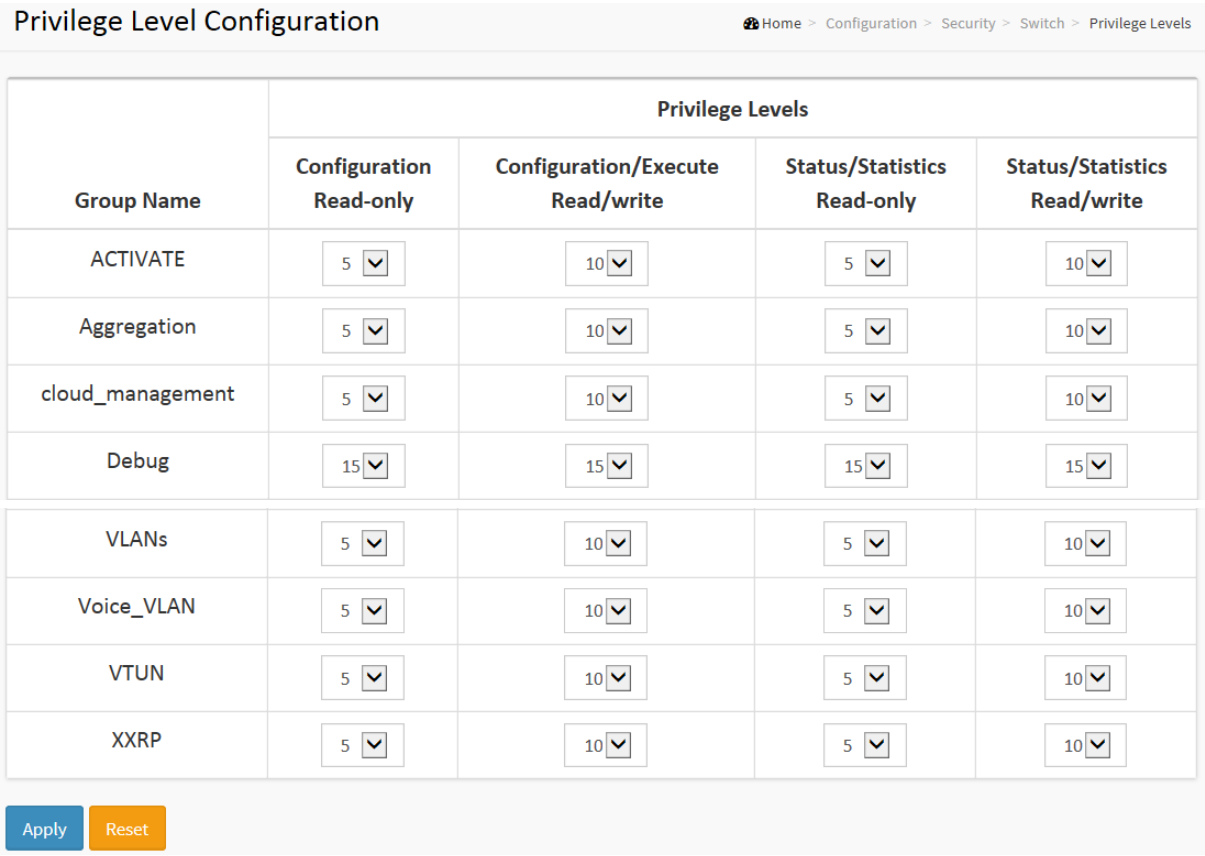


Figure2-5.1.2: The Privilege Level configuration

Parameter description:

- **Group Name :**

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

  System: Contact, Name, Location, Timezone, Daylight Saving Time, Log.

  Security: Authentication, System Access Management, Port (contains Dot1x port, MAC based and the MAC Address Limit), ACL, HTTPS, SSH, ARP Inspection, IP source guard.

IP: Everything except 'ping'.

Port: Everything except 'VeriPHY'.

Diagnostics: 'ping' and 'VeriPHY'.

Maintenance: CLI- System Reboot, System Restore Default, System Password, Configuration Save, Configuration Load and Firmware Load. Web- Users, Privilege Levels and everything in Maintenance.

Debug: Only present in CLI.

- **Privilege Levels :**

  Every group has an authorization Privilege level for the following sub groups: configuration read-only, configuration/execute read-write, status/statistics read-only, and status/statistics read-write (e.g. for clearing of statistics). User Privilege should be same or greater than the authorization Privilege level to have the access to that group.

Buttons

- **Apply :**

  Click to save changes.

- **Reset :**

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

This page shows how to configure a user with authenticated when he logs into the switch via one of the management client interfaces.

Web Interface

To configure an Authentication Method Configuration in the web interface:

1. Click Configuration, Security, Switch and Auth Method.
2. Specify the Client (console, telent, ssh, http, https) which you want to monitor.
3. Specify the Authentication Method (none,local, radius, tacacs+)
4. Specify service port.
5. Click Apply.

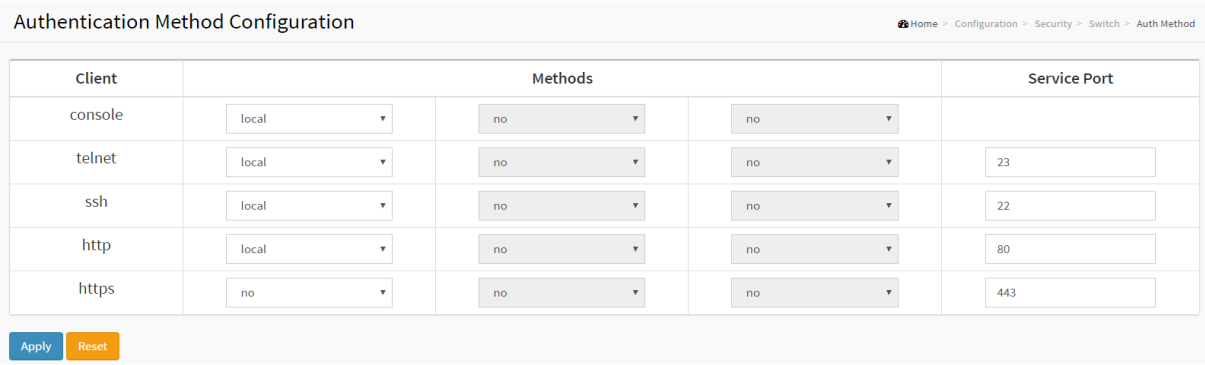


Figure 2-5.1.3: The Authentication Method Configuration

Parameter description:

- **Client :**

  The management client for which the configuration below applies.

- **Authentication Method :**

  Authentication Method can be set to one of the following 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.

  Methods that involves remote servers are timed out if the remote servers are offline. In this case the next method is tried. Each method is tried from left to right and continues until a method either approves or rejects a user. If a remote server is used for primary authentication it is recommended to configure secondary authentication as 'local'. This will enable the management client to login via the local user database if none of the configured authentication servers are alive.

- **Service Port :**

  The TCP port for each client service. The valid port number is 1 ~ 65534.

Buttons

- **Apply :**

  Click to save changes.

- **Reset :**

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

This section shows you to configure 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.

Web Interface

To configure an Access Management Configuration in the web interface:

1. Click Configuration, Security, Switch and Access Management.
2. Select "Enabled" in the Mode of Access Management Configuration.
3. Click "Add new entry".
4. Specify the Start IP Address, End IP Address.
5. Checked Access Management method (HTTP/HTTPS, SNMP, and TELNET/SSH) in the entry.
6. Click Apply.

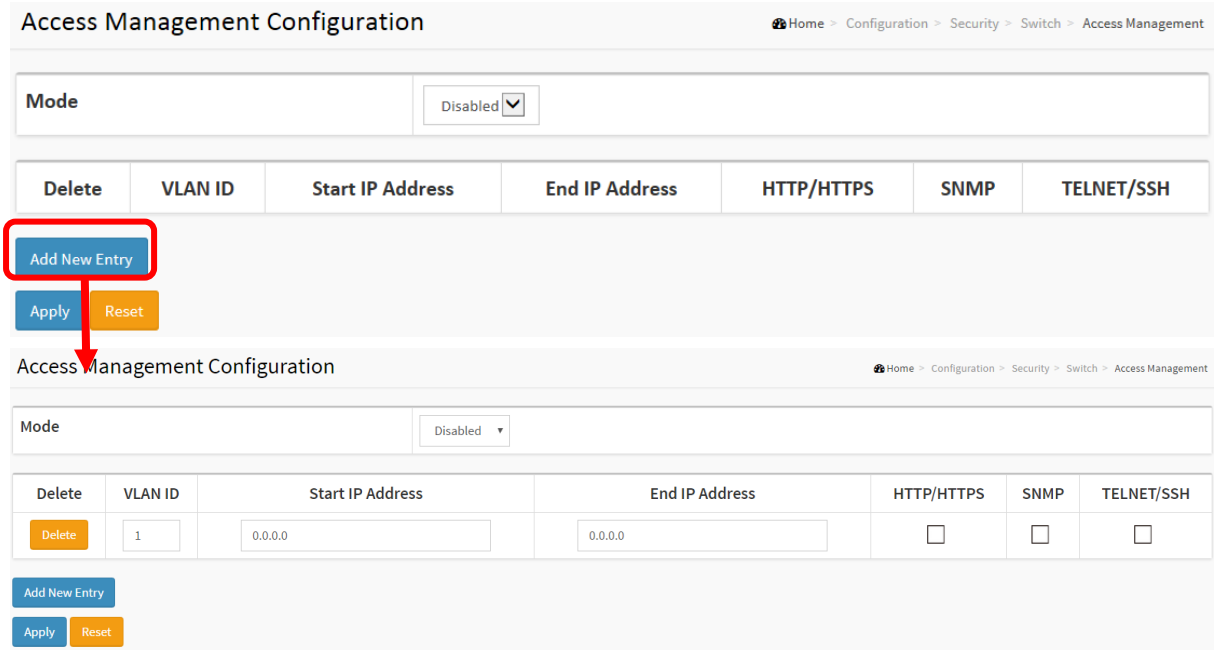


Figure 2-5.1.4: The Access Management Configuration

Parameter description:

- **Mode :**

  Indicates the access management mode operation. Possible modes are:

  Enabled: Enable access management mode operation.

  Disabled: Disable access management mode operation.

- **VLAN ID :**

  Indicates the VLAN ID for the access management entry.

- **Start IP address :**

Indicates the start IP address for the access management entry.

- **End IP address :**

  Indicates the end IP address for the access management entry.

- **HTTP/HTTPS :**

  Indicates that the host can access the switch from HTTP/HTTPS interface if the host IP address matches the IP address range provided in the entry.

- **SNMP :**

  Indicates that the host can access the switch from SNMP interface if the host IP address matches the IP address range provided in the entry.

- **TELNET/SSH :**

  Indicates that the host can access the switch from TELNET/SSH interface if the host IP address matches the IP address range provided in the entry.

Buttons

- **Delete :**

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

- **Add New Entry :**

  Click to add a new access management entry.

- **Apply :**

  Click to save changes.

- **Reset :**

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

2-5.1.5 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.

2-5.1.5.1 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.

Web Interface

To configure the configure SNMP System in the web interface:

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

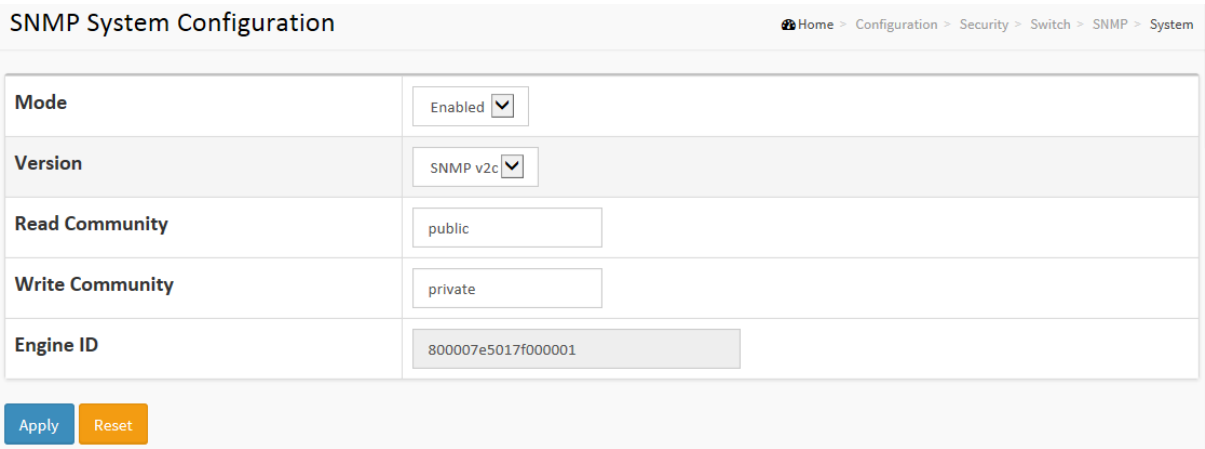


Figure 2-5.1.5.1: The SNMP System Configuration

Parameter description:

- **Mode :**

  Indicates the SNMP mode operation. Possible modes are:

  Enabled: Enable SNMP mode operation.

  Disabled: Disable SNMP mode operation.

- **Version :**

  Indicates the SNMP supported version. Possible versions are:

  SNMP v1: Set SNMP supported version 1.

  SNMP v2c: Set SNMP supported version 2c.

  SNMP v3: Set SNMP supported version 3.

- **Read Community :**

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

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

- **Write Community :**

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

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

- **Engine ID**

  Indicates the SNMPv3 engine ID. The string must contain an even number(in hexadecimal format) with number of digits between 10 and 64, but all-zeros and all-'F's are not allowed. Change of the Engine ID will clear all original local users.

Buttons

- **Apply :**

  Click to save changes.

- **Reset :**

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

2-5.1.5.2 Trap

Configure SNMP trap on this page.

Web Interface

To configure the configure SNMP Trap Configuration in the web interface:

1. Click Configuration, Security, Switch, SNMP and Trap.
2. Click Add New Entry then you can create new SNMP Trap on the switch.
3. Click Apply

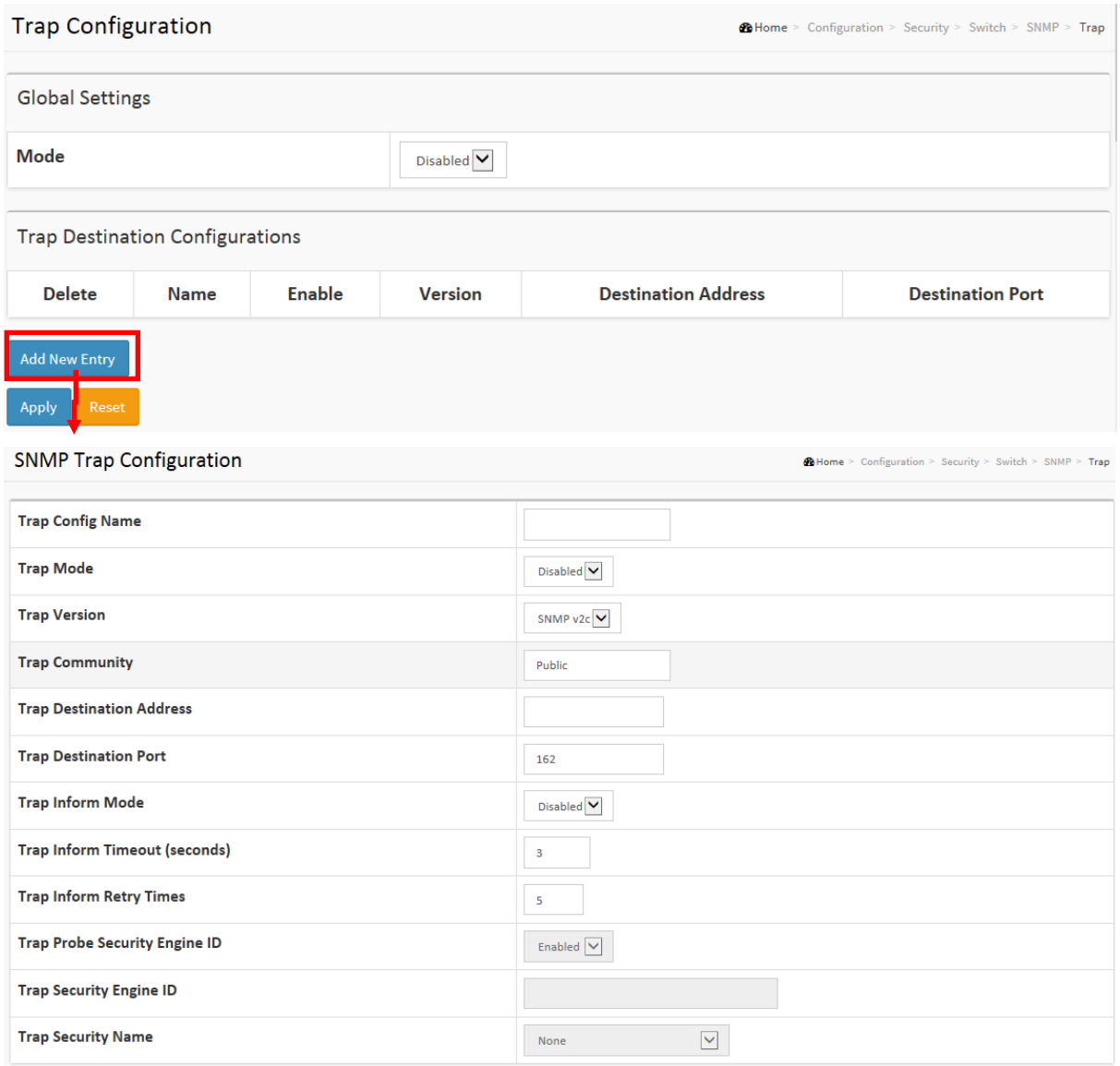


Figure 2-5.1.5.2: The SNMP Trap Configuration

Parameter description:

Global Settings

Configure SNMP trap on this page.

- **Mode :**

  Indicates the trap mode operation. Possible modes are:
  Enabled: Enable SNMP trap mode operation.
  Disabled: Disable SNMP trap mode operation.

Trap Destination Configurations

Configure trap destinations on this page.

- **Name :**

  Indicates the trap Configuration's name. Indicates the trap destination's name.

- **Enable :**

  Indicates the trap destination mode operation. Possible modes are:
  Enabled: Enable SNMP trap mode operation.
  Disabled: Disable SNMP trap mode operation.

- **Version :**

  Indicates the SNMP trap supported version. Possible versions are:
  SNMPv1: Set SNMP trap supported version 1.
  SNMPv2c: Set SNMP trap supported version 2c.

  SNMPv3: Set SNMP trap supported version 3.

- **Destination Address :**

  Indicates the SNMP trap destination address. It allow a valid IP address in dotted decimal notation ('x.y.z.w').

  And it also allow a valid hostname. A valid hostname is a string drawn from the alphabet (A-Za-z), digits (0-9), dot (.), dash (-). Spaces are not allowed, the first character must be an alpha character, and the first and last characters must not be a dot or a dash.

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

- **Destination port :**

  Indicates the SNMP trap destination port. SNMP Agent will send SNMP message via this port, the port range is 1~65535.

SNMP Trap Detailed Configuration

Configure SNMP trap on this page.

- **Trap Config Name :**

  Indicates which trap Configuration's name for configuring. The allowed string length is 1 to 32, and the allowed content is ASCII characters from 33 to 126.

- **Trap Mode :**

  Indicates the trap mode operation. Possible modes are:
  Enabled: Enable SNMP trap mode operation.
  Disabled: Disable SNMP trap mode operation.

- **Trap Mode :**

Indicates the SNMP mode operation. Possible modes are:
Enabled: Enable SNMP mode operation.
Disabled: Disable SNMP mode operation.

- **Trap Version :**

  Indicates the SNMP supported version. Possible versions are:
  SNMP v1: Set SNMP supported version 1.
  SNMP v2c: Set SNMP supported version 2c.
  SNMP v3: Set SNMP supported version 3.

- **Trap Community :**

  Indicates the community access string when sending SNMP trap packet. The allowed string length is 0 to 255, and the allowed content is ASCII characters from 33 to 126.

- **Trap Destination Address :**

  Indicates the SNMP trap destination address. It allow a valid IP address in dotted decimal notation ('x.y.z.w').

  And it also allow a valid hostname. A valid hostname is a string drawn from the alphabet (A-Za-z), digits (0-9), dot (.), dash (-). Spaces are not allowed, the first character must be an alpha character, and the first and last characters must not be a dot or a dash.

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

- **Trap Destination port :**

  Indicates the SNMP trap destination port. SNMP Agent will send SNMP message via this port, the port range is 1~65535.

- **Trap Inform Mode :**

  Indicates the SNMP trap inform mode operation. Possible modes are:
  Enabled: Enable SNMP trap inform mode operation.
  Disabled: Disable SNMP trap inform mode operation.

- **Trap Inform Timeout (seconds) :**

  Indicates the SNMP trap inform timeout. The allowed range is 0 to 2147.

- **Trap Inform Retry Times :**

  Indicates the SNMP trap inform retry times. The allowed range is 0 to 255.

- **Trap Probe Security Engine ID :**

  Indicates the SNMP trap probe security engine ID mode of operation. Possible values are:
  Enabled: Enable SNMP trap probe security engine ID mode of operation.
  Disabled: Disable SNMP trap probe security engine ID mode of operation.

- **Trap Security Engine ID :**

  Indicates the SNMP trap security engine ID. SNMPv3 sends traps and informs using USM for authentication and privacy. A unique engine ID for these traps and informs is needed. When "Trap Probe Security Engine ID" is enabled, the ID will be probed automatically. Otherwise, the ID specified in this field is used. The string must contain an even number(in hexadecimal format) with number of digits between 10 and 64, but all-zeros and all-'F's are not allowed.

- **Trap Security Name :**

  Indicates the SNMP trap security name. SNMPv3 traps and informs using USM for authentication and privacy. A unique security name is needed when traps and informs are enabled.

Buttons

- **Delete :**

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

- **Add New Entry :**

  Click to add a new user.

- **Apply :**

  Click to save changes.

- **Reset :**

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

2-5.1.5.3 Communities

The 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 check <Save>. Max Group Number: 4.

Web Interface

To configure the SNMP Communities in the web interface:

1. Click Configuration, Security, Switch, SNMP and Communities.
2. Click Add new Entry.
3. Specify the SNMP community parameters.
4. Click Apply.
5. If you want to modify or clear the setting then click Reset.

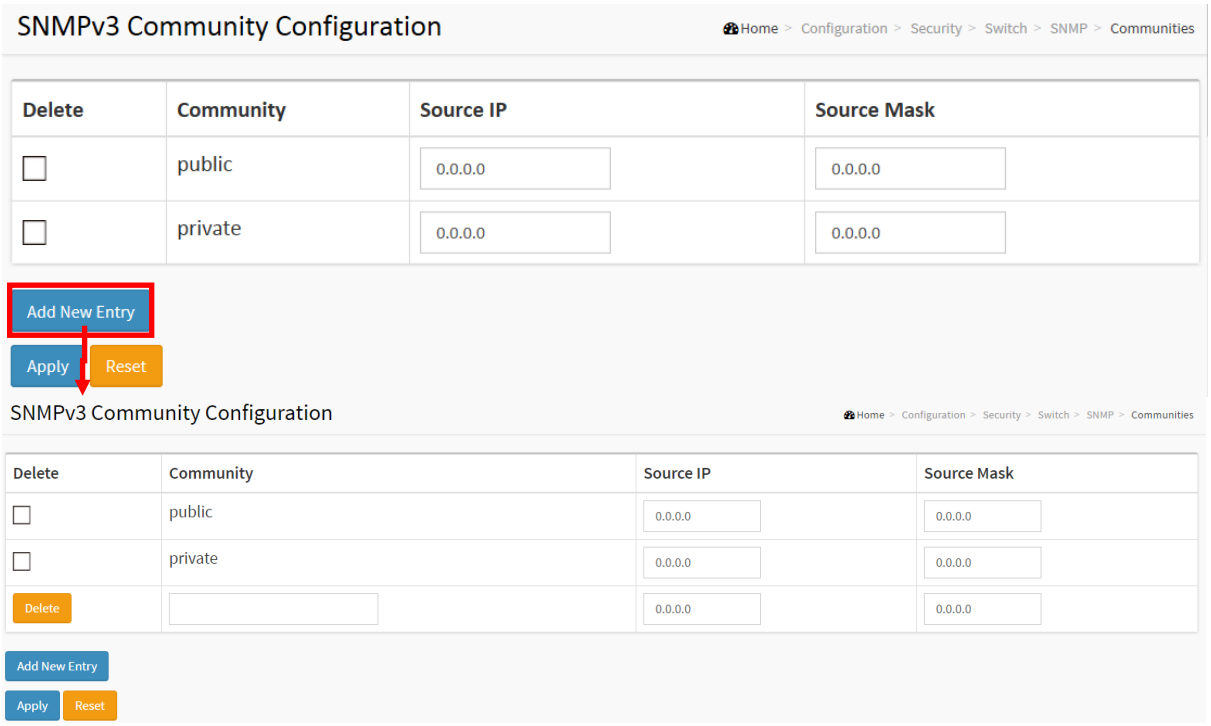


Figure 2-5.1.5.3: The SNMPv1/v2 Communities Security Configuration

Parameter description:

- **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.

- **Source IP :**

  Indicates the SNMP access source address. A particular range of source addresses can be

used to restrict source subnet when combined with source mask.

- **Source Mask :**

  Indicates the SNMP access source address mask

Buttons

- **Delete :**

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

- **Add New Entry :**

  Click to add a new entry.

- **Apply :**

  Click to save changes.

- **Reset :**

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

2-5.1.5.4 Users

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

Web Interface

To configure the SNMP Users in the web interface:

1. Click Configuration, Security, Switch, SNMP and Users.
2. Click Add new Entry.
3. Specify the Privilege parameter.
4. Click Apply.

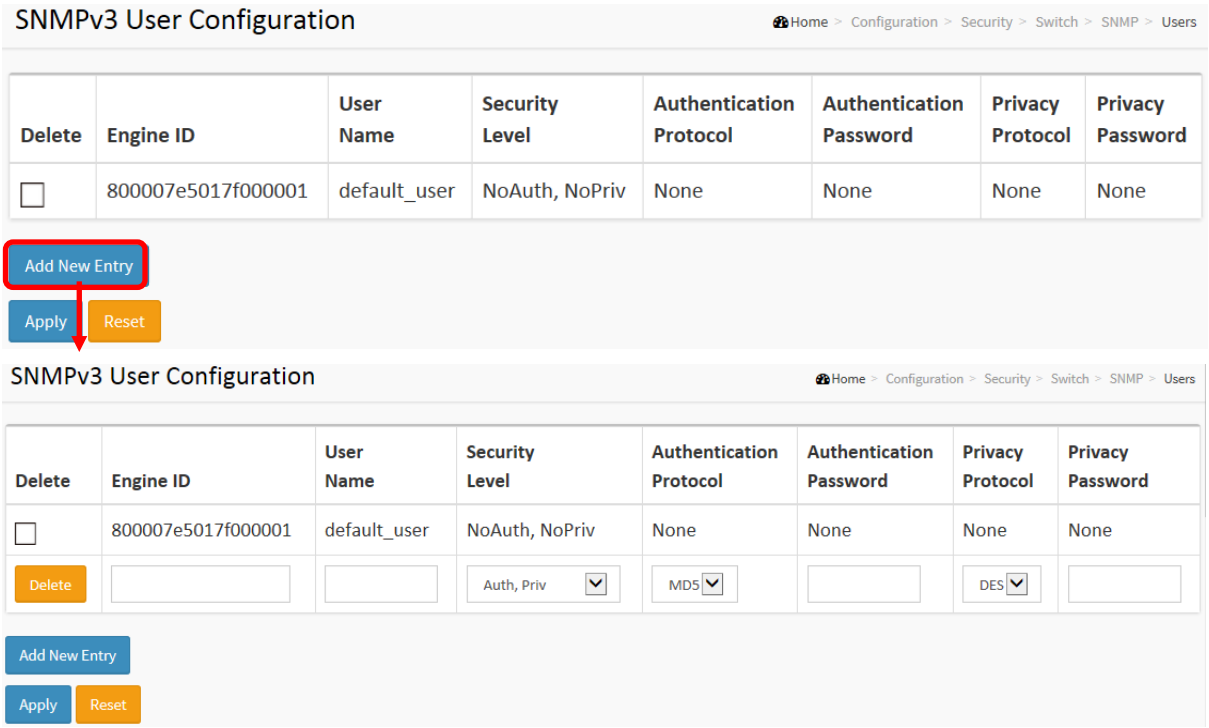


Figure 2-5.1.5.4: The SNMP Users Configuration

Parameter description:

- **Engine ID :**

  An octet string identifying the engine ID that this entry should belong to. The string must contain an even number (in hexadecimal format) with number of digits between 10 and 64, but all-zeros and all-'F's are not allowed. The SNMPv3 architecture uses the User-based Security Model (USM) for message security and the View-based Access Control Model (VACM) for access control. For the USM entry, the usmUserEngineID and usmUserName are the entry's keys. In a simple agent, usmUserEngineID is always that agent's own snmpEngineID value. The value can also take the value of the snmpEngineID of a remote SNMP engine with which this user can communicate. In other words, if user engine ID equal system engine ID then it is local user; otherwise it's remote user.

- **User Name :**

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

- **Security Level :**

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

  NoAuth, NoPriv: 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 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 security level 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 to 32. For SHA authentication protocol, the allowed string length is 8 to 40. The allowed content is ASCII characters from 33 to 126.

- **Privacy Protocol :**

  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, and the allowed content is ASCII characters from 33 to 126.

Buttons

- **Delete :**

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

- **Add New Entry :**

  Click to add a new entry.

- **Apply :**

  Click to save changes.

- **Reset :**

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

2-5.1.5.5 Groups

The function is used to configure SNMPv3 group. The Entry index key are 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.

Web Interface

To configure the SNMP Groups in the web interface:

1. Click Configuration, Security, Switch, SNMP and Groups.
2. Click Add new Entry.
3. Specify the Privilege parameter.
4. Click Apply.

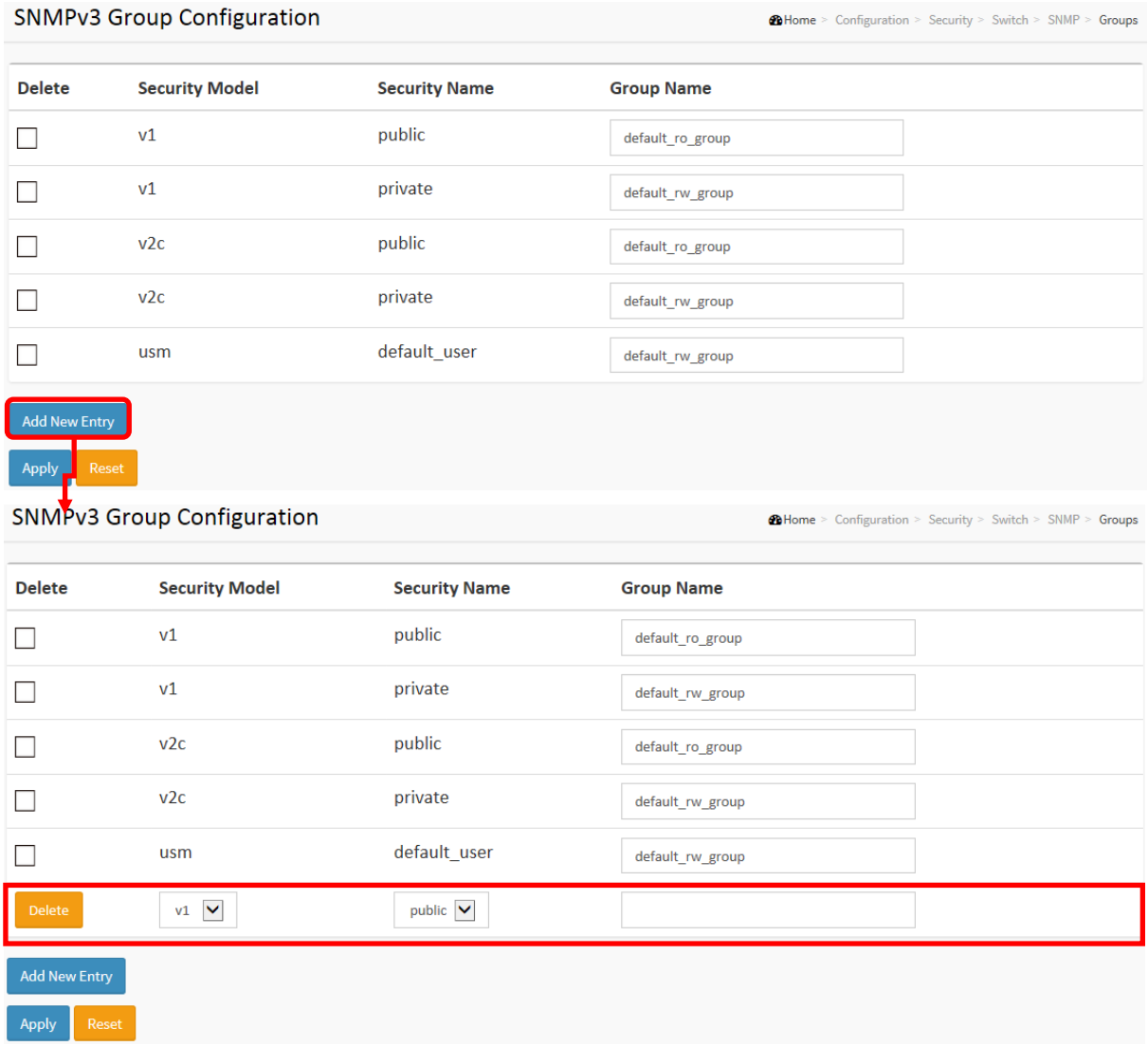


Figure 2-5.1.5.5: The SNMP Groups Configuration

Parameter description:

- **Security Model :**

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

  v1: Reserved for SNMPv1.

  v2c: Reserved for SNMPv2c.

  usm: User-based Security Model (USM).

- **Security Name :**

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

- **Group Name :**

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

Buttons

- **Delete :**

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

- **Add New Entry :**

  Click to add a new entry.

- **Apply :**

  Click to save changes.

- **Reset :**

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

2-5.1.5.6 Views

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

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

Web Interface

To configure the SNMP views in the web interface:

1. Click Configuration, Security, Switch, SNMP and Views.
2. Click Add New Entry.
3. Specify the SNMP View parameters.
4. Click Apply.
5. If you want to modify or clear the setting then click Reset.

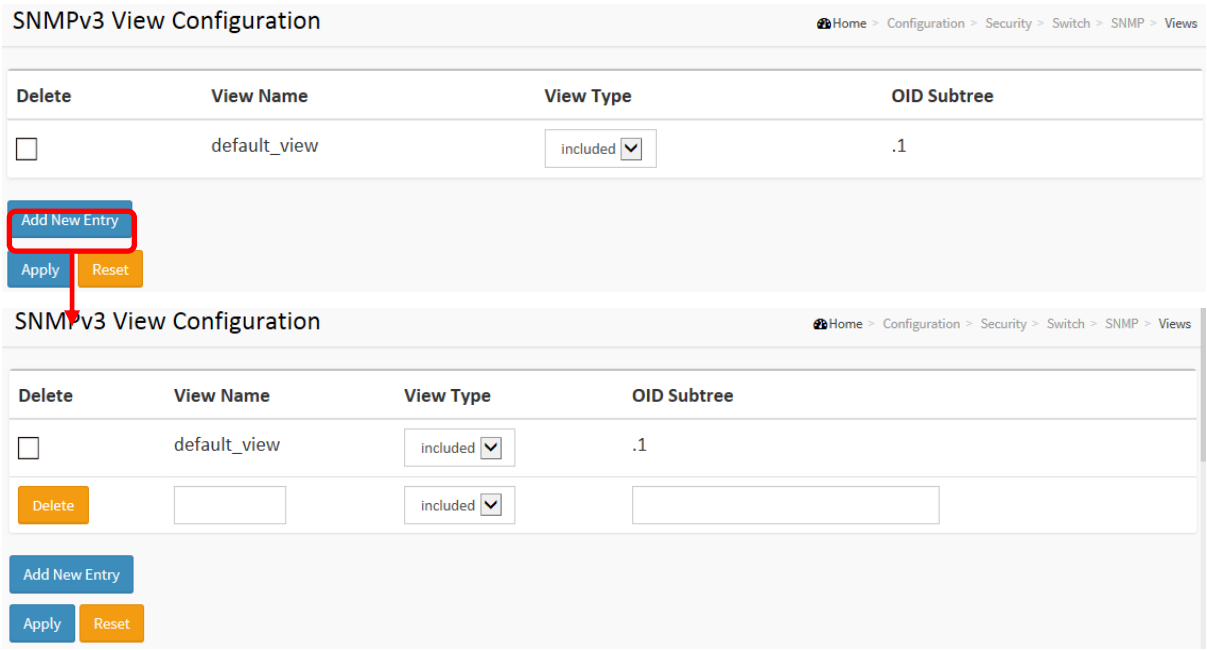


Figure 2-5.1.5.6: The SNMP Views Configuration

Parameter description:

- **View Name :**

  A string identifying the view name that this entry should belong to. The allowed string length is 1 to 32, and the allowed content is ASCII characters from 33 to 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(*).

Buttons

- **Delete :**

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

- **Add New Entry :**

  Click to add a new entry.

- **Apply :**

  Click to save changes.

- **Reset :**

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

2-5.1.5.7 Access

The 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 check <Save>. Max Group Number : 14

Web Interface

To configure the SNMP Access in the web interface:

1. Click Configuration, Security, Switch, SNMP and Accesses.
2. Click Add new Access.
3. Specify the SNMP Access parameters.
4. Click Apply.
5. If you want to modify or clear the setting then click Reset.

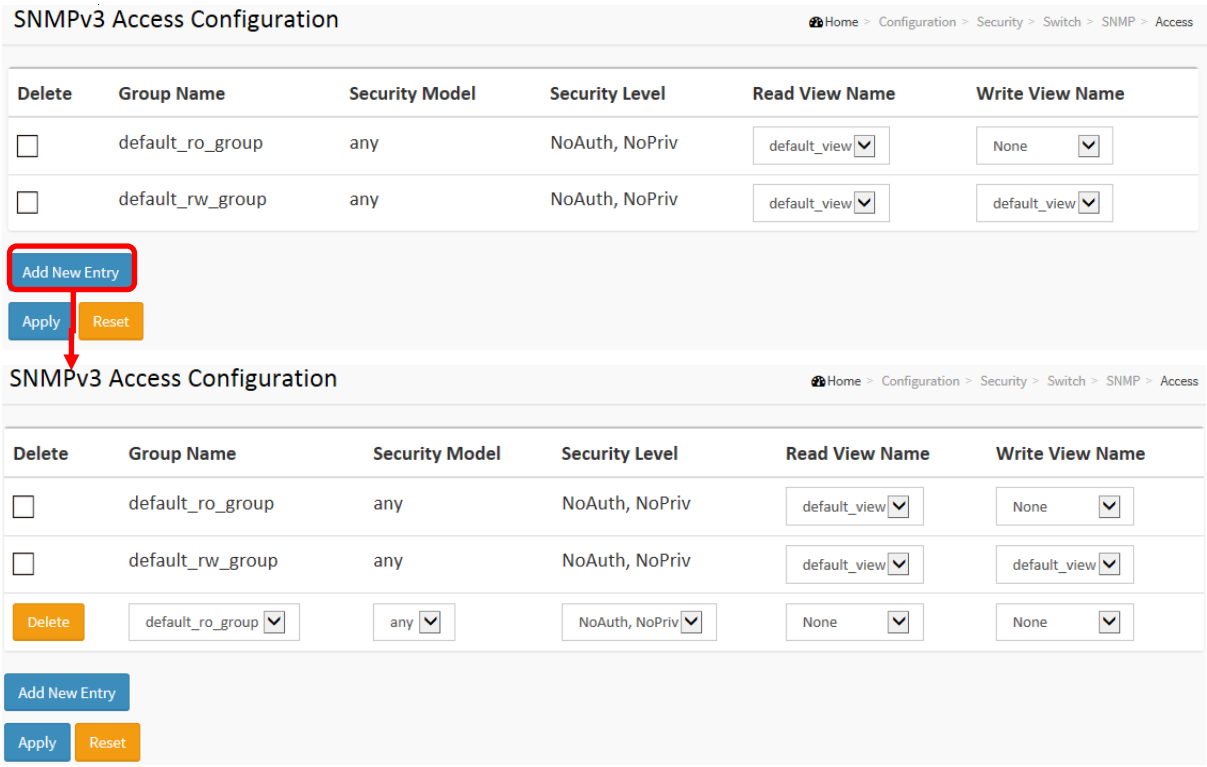


Figure 2-5.1.5.7: The SNMP Accesses Configuration

Parameter description:

- **Group Name :**

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

- **Security Model :**

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

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

v1: Reserved for SNMPv1.

v2c: Reserved for SNMPv2c.

usm: User-based Security Model (USM).

- **Security Level :**

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

  NoAuth, NoPriv: No authentication and no privacy.

  Auth, NoPriv: Authentication and no privacy.

  Auth, Priv: Authentication and privacy.

- **Read View Name :**

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

- **Write View Name :**

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

Buttons

- **Delete :**

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

- **Add New Entry :**

  Click to add a new entry.

- **Apply :**

  Click to save changes.

- **Reset :**

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

2-5.1.5.8 Trap Event Severity

This page displays current trap event severity configurations. Trap event severity can also be configured here.

Web Interface

To configure the Trap Event Severity in the web interface:

1. Click Configuration, Security, Switch, SNMP and Trap Event Severity.
2. Scroll to select the Group name and Severity Level
3. Click the Apply 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

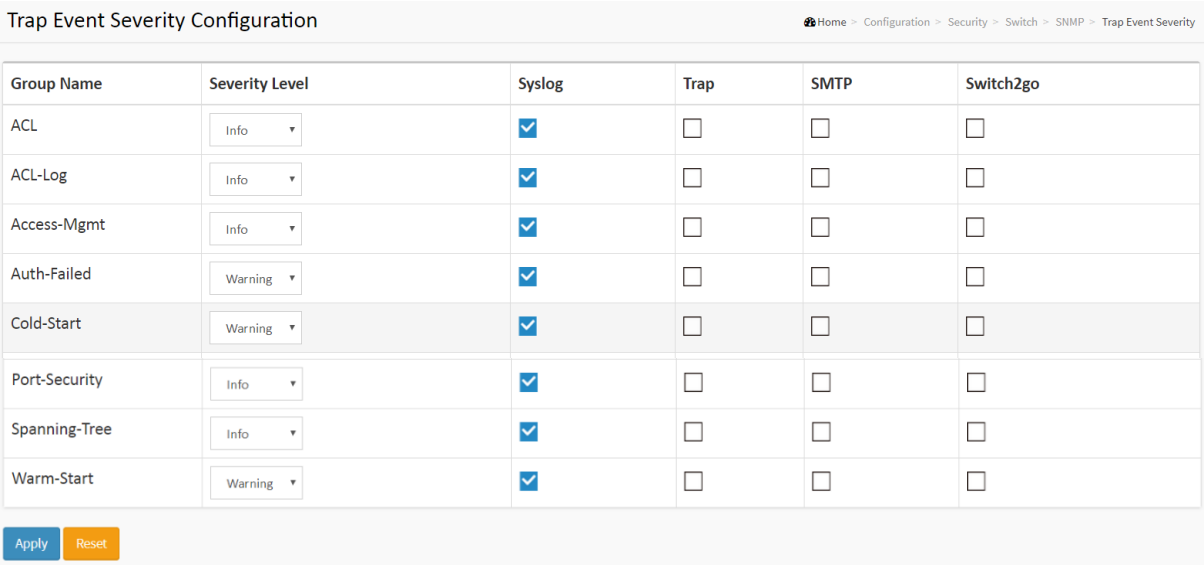


Figure 2-5.1.5.8: The Trap Event Severity Configuration

Parameter description:

- **Group Name :**

  The name identifying the severity group.

- **Severity Level :**

  Every group has an severity level. The following level types are supported:
  <0> Emergency: System is unusable.
  <1> Alert: Action must be taken immediately.
  <2> Critical: Critical conditions.
  <3> Error: Error conditions.
  <4> Warning: Warning conditions.
  <5> Notice: Normal but significant conditions.
  <6> Information: Information messages.
  <7> Debug: Debug-level messages.

- **Syslog :**

Enable - Select this Group Name in Syslog.

- **Trap :**

  Enable - Select this Group Name in Trap.

- **SMTP :**

  Enable - Select this Group Name in SMTP.

Buttons

- **Apply :**

  Click to save changes.

- **Reset :**

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

2-5.1.6 RMON

An RMON implementation typically operates in a client/server model. Monitoring devices contain RMON software agents that collect information and analyze packets. These probes act as servers and the Network Management applications that communicate with them act as clients.

2-5.1.6.1 Statistics

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

Web Interface

To configure the RMON configuration in the web interface:

1. Click Configuration, Security, Switch, RMON and Statistics.
2. Click Add New Entry.
3. Specify the ID parameters.
4. Click Apply.

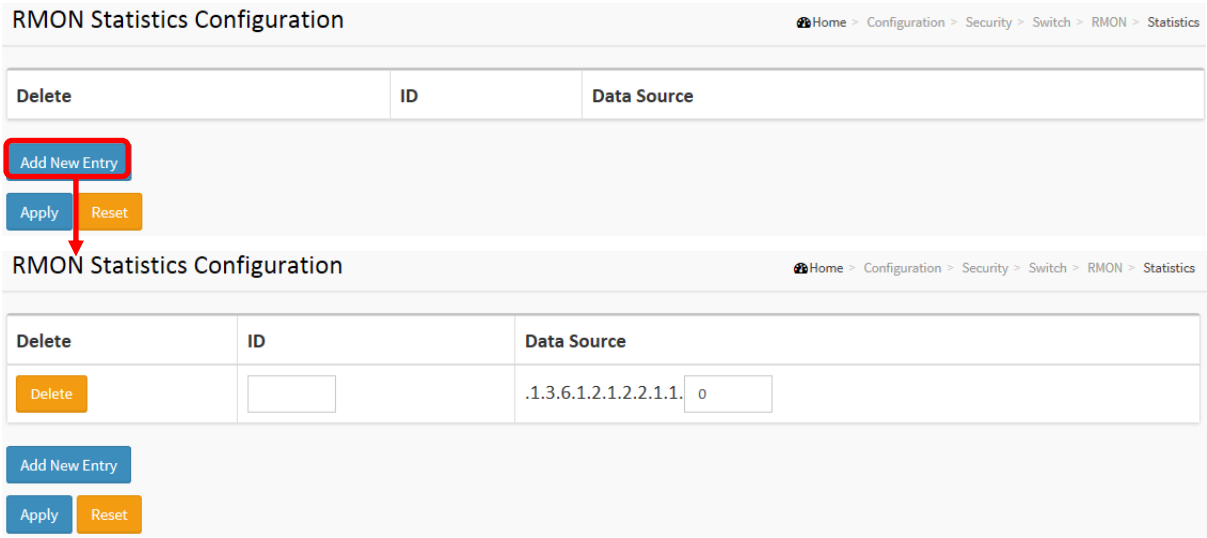


Figure 2-5.1.6.1: The RMON Statistics Configuration

Parameter description:

These parameters are displayed on the RMON Statistics Configuration page:

- **ID :**

  Indicates the index of the entry. The range is from 1 to 65535.

- **Data Source :**

  Indicates the port ID which wants to be monitored. If in stacking switch, the value must add 1000*(switch ID-1), for example, if the port is switch 3 port 5, the value is 2005

Buttons

- **Delete :**

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

- **Add New Entry :**

  Click to add a new entry.

- **Apply :**

  Click to save changes.

- **Reset :**

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

2-5.1.6.2 History

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

Web Interface

the RMON History in the web interface:

1. Click Configuration, Security, Switch, RMON and History.
2. Click Add New Entry.
3. Specify the ID parameters.
4. Click Apply.

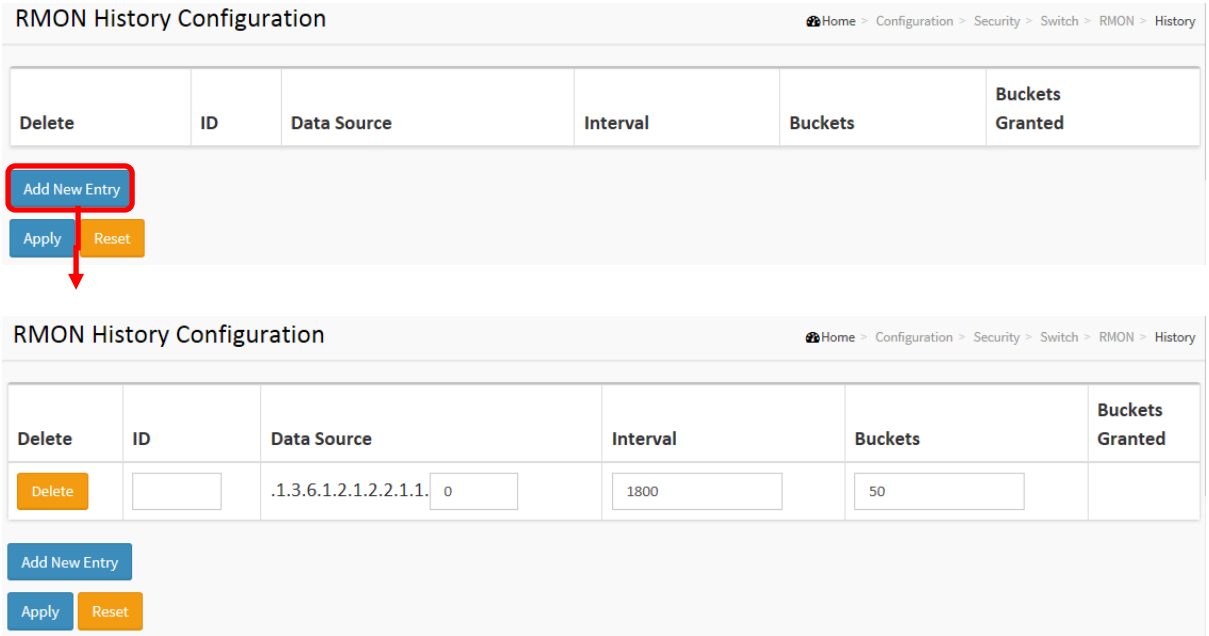


Figure 2-5.1.6.2: The RMON History Configuration

Parameter description:

These parameters are displayed on the RMON History Configuration page:

- **ID :**

  Indicates the index of the entry. The range is from 1 to 65535.

- **Data Source :**

  Indicates the port ID which wants to be monitored. If in stacking switch, the value must add 1000*(switch ID-1), for example, if the port is switch 3 port 5, the value is 2005

- **Interval :**

  Indicates the interval in seconds for sampling the history statistics data. The range is from 1 to 3600, default value is 1800 seconds.

- **Buckets :**

Indicates the maximum data entries associated this History control entry stored in RMON. The range is from 1 to 3600, default value is 50.

- **Buckets Granted :**

  The number of data shall be saved in the RMON.

Buttons

- **Delete :**

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

- **Add New Entry :**

  Click to add a new entry.

- **Apply :**

  Click to save changes.

- **Reset :**

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

2-5.1.6.3 Alarm

Configure RMON Alarm table on this page. The entry index key is **ID.**

Web Interface

To display the configure RMON Alarm in the web interface:

1. Click Configuration, Security, Switch, RMON and Alarm.
2. Click Add New Entry.
3. Specify the ID parameters.
4. Click Apply.

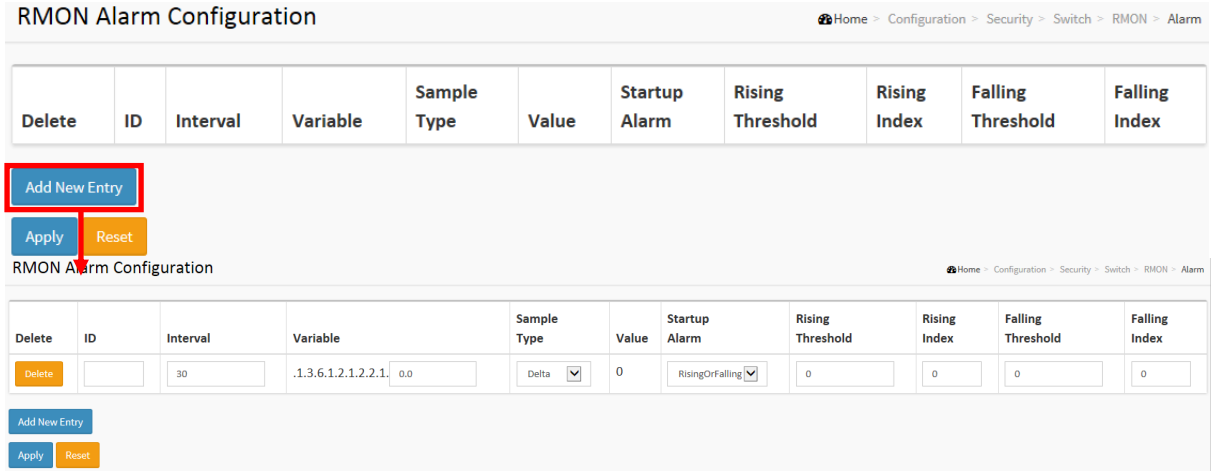


Figure 2-5.1.6.3: The RMON Alarm Configuration

Parameter description:

These parameters are displayed on the RMON Alarm Configuration page:

- **ID :**

  Indicates the index of the entry. The range is from 1 to 65535.

- **Interval :**

  Indicates the interval in seconds for sampling and comparing the rising and falling threshold. The range is from 1 to 2^31-1.

- **Variable :**

  Indicates the particular variable to be sampled, the possible variables are:

  InOctets:
  The total number of octets received on the interface, including framing characters.

  InUcastPkts:
  The number of uni-cast packets delivered to a higher-layer protocol.

  InNUcastPkts:
  The number of broad-cast and multi-cast packets delivered to a higher-layer protocol.

  InDiscards:

The number of inbound packets that are discarded even the packets are normal.

InErrors:
The number of inbound packets that contained errors preventing them from being deliverable to a higher-layer protocol.

InUnknownProtos:
the number of the inbound packets that were discarded because of the unknown or un-support protocol.

OutOctets:
The number of octets transmitted out of the interface , including framing characters.

OutUcastPkts:
The number of uni-cast packets that request to transmit.

OutNUcastPkts:
The number of broad-cast and multi-cast packets that request to transmit.

OutDiscards:
The number of outbound packets that are discarded event the packets is normal.

OutErrors:
The The number of outbound packets that could not be transmitted because of errors.

OutQLen:
The length of the output packet queue (in packets).

- **Sample Type :**

  The method of sampling the selected variable and calculating the value to be compared against the thresholds, possible sample types are:

  Absolute: Get the sample directly.

  Delta: Calculate the difference between samples (default).

- **Value :**

  The value of the statistic during the last sampling period.

- **Startup Alarm :**

  The method of sampling the selected variable and calculating the value to be compared against the thresholds, possible sample types are:

  RisingTrigger alarm when the first value is larger than the rising threshold.

  FallingTrigger alarm when the first value is less than the falling threshold.

  RisingOrFallingTrigger alarm when the first value is larger than the rising threshold or less than the falling threshold (default).

- **Rising Threshold :**

  Rising threshold value (-2147483648-2147483647).

- **Rising Index :**

  Rising event index (1-65535).

- **Falling Threshold :**

  Falling threshold value (-2147483648-2147483647)

- **Falling Index :**

  Falling event index (1-65535).

Buttons

- **Delete :**

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

- **Add New Entry :**

  Click to add a new entry.

- **Apply :**

  Click to save changes.

- **Reset :**

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

2-5.1.6.4 Event

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

Web Interface

To display the configure RMON Event in the web interface:

1. Click Configuration, Security, Switch, RMON and Event.
2. Click Add New Entry.
3. Specify the ID parameters.
4. Click Apply.

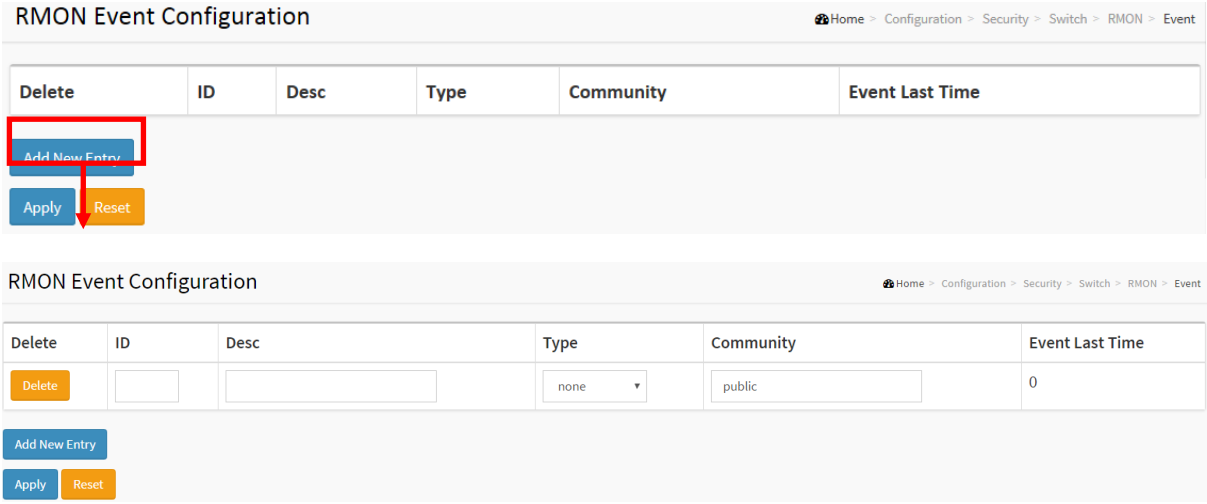


Figure 2-5.1.6.4: The RMON Event Configuration

Parameter description:

These parameters are displayed on the RMON History Configuration page:

- **ID :**

  Indicates the index of the entry. The range is from 1 to 65535.

- **Desc :**

  Indicates this event, the string length is from 0 to 127, default is a null string.

- **Type :**

  Indicates the notification of the event, the possible types are:

  None: No SNMP log is created, no SNMP trap is sent.

  Log: Create SNMP log entry when the event is triggered.

  Snmp trap: Send SNMP trap when the event is triggered.

  Log and trap: Create SNMP log entry and sent SNMP trap when the event is triggered.

- **Community :**

  Specify the community when trap is sent, the string length is from 0 to 127, default is

"public".

- **Event Last Time :**

  Indicates the value of sysUpTime at the time this event entry last generated an event.

Buttons

- **Delete :**

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

- **Add New Entry :**

  Click to add a new entry.

- **Apply :**

  Click to save changes.

- **Reset :**

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

2-5.2 Network

2-5.2.1 Limit Control

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.

Web Interface

To configure a System Configuration of Limit Control in the web interface:

1. Select "Enabled" in the Mode of System Configuration.
2. Checked Aging Enabled.
3. Set Aging Period (Default is 3600 seconds).

To configure a Port Configuration of Limit Control in the web interface:

1. Select "Enabled" in the Mode of Port Configuration.
2. Specify the maximum number of MAC addresses in the Limit of Port Configuration.
3. Set Action (Trap, Shutdown, Trap & Shutdown)
4. Click Apply.

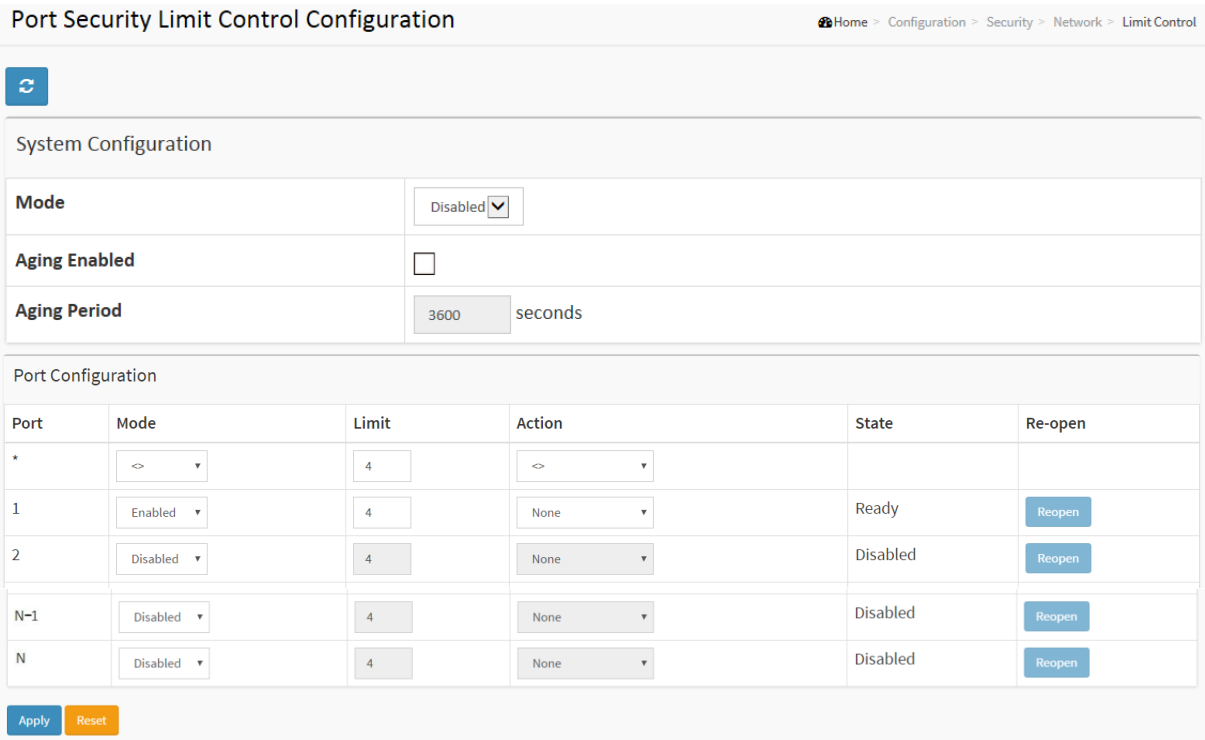


Figure 2-5.2.1: The Port Security Limit Control Configuration

Parameter description:

System Configuration

- **Mode :**

Indicates if Limit Control is globally enabled or disabled on the switch. If globally disabled, other modules may still use the underlying functionality, but limit checks and corresponding actions are disabled.

- **Aging Enabled :**

  If checked, secured MAC addresses are subject to aging as discussed under Aging Period.

- **Aging Period :**

  If Aging Enabled is checked, then the aging period is controlled with this input. If other modules are using the underlying port security for securing MAC addresses, they may have other requirements to the aging period. The underlying port security will use the shorter requested aging period of all modules that use the functionality.

  The Aging Period can be set to a number between 10 and 10,000,000 seconds.

  To understand why aging may be desired, consider the following scenario: Suppose an end-host is connected to a 3rd party switch or hub, which in turn is connected to a port on this switch on which Limit Control is enabled. The end-host will be allowed to forward if the limit is not exceeded. Now suppose that the end-host logs off or powers down. If it 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 shut down or Trap & Shutdown.

- **Re-open Button :**

  If a port is shut down by this module, you may reopen it by clicking this button, which will only be enabled if this is the case. For other methods, refer to shut down in the Action section.

NOTE: That clicking the reopen button causes the page to be refreshed, so non-committed changes will be lost

Buttons

- **Refresh :**

  You can click them for refresh the Port Security information by manual.

- **Apply :**

  Click to save changes.

- **Reset :**

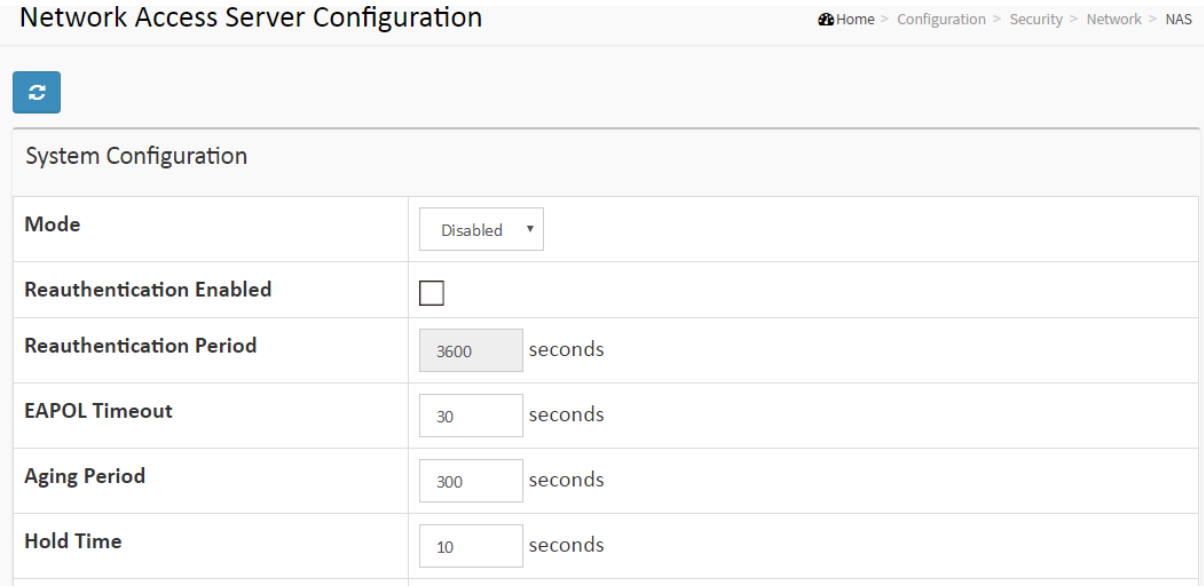
  Click to undo any changes made locally and revert to previously saved values.

The section describes to configure the NAS parameters of the switch. The NAS server can be employed to connect users to a variety of resources including Internet access, conference calls, printing documents on shared printers, or by simply logging on to the Internet.

Web Interface

To configure a Network Access Server in the web interface:

1. Click Configuration, Security, Network and NAS.
2. Select "Enabled" in the Mode of Network Access Server Configuration.
3. Checked Reauthentication Enabled.
4. Set Reauthentication Period (Default is 3600 seconds).
5. Set EAPOL Timeout (Default is 30 seconds).
6. Set Aging Period (Default is 300 seconds).
7. Set Hold Time (Default is 10 seconds).
8. Checked RADIUS-Assigned QoS Enabled.
9. Checked RADIUS-Assigned VLAN Enabled.
10. Checked Guest VLAN Enabled.
11. Specify Guest VLAN ID.
12. Specify Max. Reauth. Count.
13. Checked Allow Guest VLAN if EAPOL Seen.
14. Click Apply.



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
N-1	Force Authorized				Globally Disabled	Reauthenticate	Reinitialize
N	Force Authorized				Globally Disabled	Reauthenticate	Reinitialize

Apply Reset

Figure 2-5.2.2: The Network Access Server Configuration

Parameter description:

System Configuration

- **Mode :**

  Indicates if NAS is globally enabled or disabled on the switch. If globally disabled, all ports are allowed forwarding of frames.

- **Reauthentication Enabled :**

  If checked, successfully authenticated supplicants/clients are reauthenticated after the interval specified by the Reauthentication Period. Reauthentication for 802.1X-enabled ports can be used to detect if a new device is plugged into a switch port or if a supplicant is no longer attached.

  For MAC-based ports, reauthentication is only useful if the RADIUS server configuration has changed. It does not involve communication between the switch and the client, and therefore doesn't imply that a client is still present on a port (see Aging Period below).

- **Reauthentication Period :**

  Determines the period, in seconds, after which a connected client must be reauthenticated. This is only active if the Reauthentication Enabled checkbox is checked. Valid values are in the range 1 to 3600 seconds.

- **EAPOL Timeout :**

  Determines the time for retransmission of Request Identity EAPOL frames.

  Valid values are in the range 1 to 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 a number between 10 and 1000000 seconds.

  If reauthentication is enabled and the port is in an 802.1X-based mode, this is not so critical, since supplicants that are no longer attached to the port will get removed upon the next re-authentication, which will fail. But if re-authentication 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 Un-authorized 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 802.1X-unaware clients are placed after a network administrator-defined timeout. The switch follows a set of rules for entering and leaving the Guest VLAN as listed below.

  The "Guest VLAN Enabled" checkbox provides a quick way to globally enable/disable Guest VLAN functionality. When checked, the individual ports' ditto setting determines whether the port can be moved into Guest VLAN. When unchecked, the ability to move to the Guest VLAN is disabled on all ports.

- **Guest VLAN ID :**

  This is the value that a port's Port VLAN ID is set to if a port is moved into the Guest VLAN. It is only changeable if the Guest VLAN option is globally enabled.
  Valid values are in the range [1; 4095].

- **Max. Reauth. Count :**

  The number of times the switch transmits an EAPOL Request Identity frame without response before considering entering the Guest VLAN is adjusted with this setting. The value can only be changed if the Guest VLAN option is globally enabled.
  Valid values are in the range [1; 255].

- **Allow Guest VLAN if EAPOL Seen :**

  The switch remembers if an EAPOL frame has been received on the port for the life-time of the port. Once the switch considers whether to enter the Guest VLAN, it will first check if this option is enabled or disabled. If disabled (unchecked; default), the switch will only enter the Guest VLAN if an EAPOL frame has not been received on the port for the life-time of the port. If enabled (checked), the switch will consider entering the Guest VLAN even if an EAPOL frame has been received on the port for the life-time of the port.
  The value can only be changed if the Guest VLAN option is globally enabled.

Port Configuration

The table has one row for each port on the selected switch and a number of columns, which are:

- **Port :**

  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 "xx-xx-xx-xx-xx-xx", that is, a dash (-) is used as separator between the lower-cased hexadecimal digits. The switch only supports the MD5-Challenge authentication method, so the RADIUS server must be configured accordingly.

When authentication is complete, the RADIUS server sends a success or failure indication, which in turn causes the switch to open up or block traffic for that particular client, using 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 RFC4675 forms the basis for identifying the QoS Class in an Access-Accept packet.

Only the first occurrence of the attribute in the packet will be considered, and to be valid, it must follow this rule:

• All 8 octets in the attribute's value must be identical and consist of ASCII characters in the range '0' - '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 transmissions 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 re-authentication immediately. The clients will transfer to the unauthorized state while the re-authentication is in progress.

Buttons

- **Refresh :**

  You can click them for refresh the NAS Configuration by manual.

- **Apply :**

  Click to save changes.

- **Reset :**

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

2-5.2.3 ACL

The PSGS-2626GF Series 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 Ether Types. 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, and 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.

2-5.2.3.1 Ports

The section describes how to configure the ACL parameters (ACE) of the each switch port. These parameters will affect frames received on a port unless the frame matches a specific ACE

Web Interface

To configure the ACL Ports Configuration in the web interface:

1. Click Configuration, Security, Network, ACL and 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.

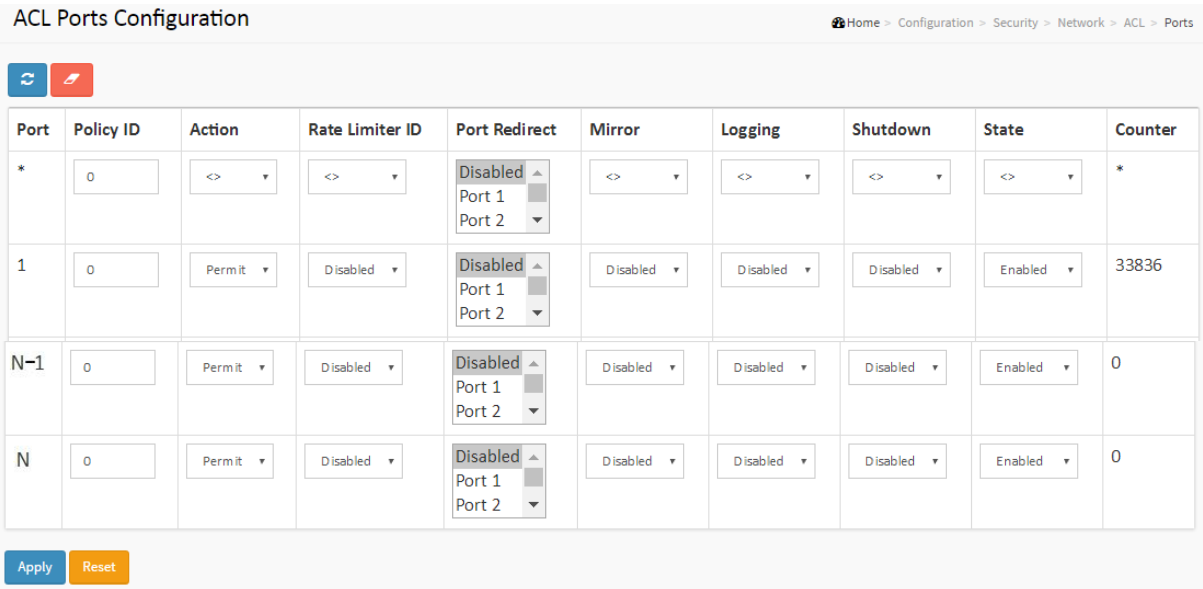


Figure 2-5.2.3.1: The ACL Ports Configuration

Parameter description:

- **Port :**

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

- **Policy ID :**

  Select the policy to apply to this port. The allowed values are 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 Redirect :**

  Select which port frames are redirected on. The allowed values are Disabled or a specific port number and it can't be set when action is permitted. The default value is "Disabled".

- **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".

- **State :**

  Specify the port state of this port. The allowed values are:

  Enabled: To reopen ports by changing the volatile port configuration of the ACL user module.

  Disabled: To close ports by changing the volatile port configuration of the ACL user module.

  The default value is "Enabled"

- **Counter :**

  Counts the number of frames that match this ACE.

Buttons

- **Refresh, clear :**

  You can click them for refresh the ACL Port Configuration or clear them by manual.

- **Apply :**

  Click to save changes.

- **Reset :**

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

2-5.2.3.2 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.

Web Interface

To configure ACL Rate Limiter in the web interface:

1. Click Configuration, Security, Network, ACL and Rate Limiter.
2. To specific the Rate field and the range from 0 to 3276700.
3. Click the Apply 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.

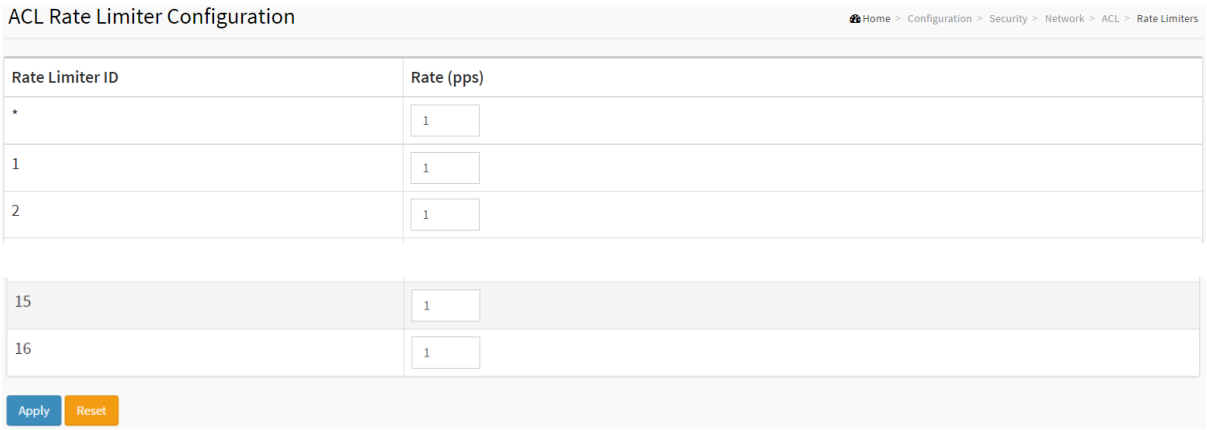


Figure 2-5.2.3.2: The ACL Rate Limiter Configuration

Parameter description:

- **Rate Limiter ID :**

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

- **Rate :**

  The allowed values are: 0-3276700 in pps.

Buttons

- **Apply :**

  Click to save changes.

- **Reset :**

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

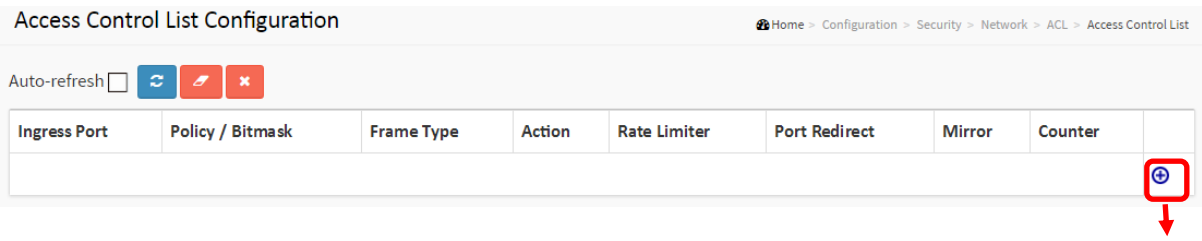
2-5.2.3.3 Access Control List

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 the priority is highest.

Web Interface

1. To configure Access Control List in the web interface:
2. Click Configuration, Security, Network, ACL and Access Control List.
3. 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)
4. To specific the parameter of the ACE
5. Click the save to save the setting
6. If you want to cancel the setting then you need to click the reset button. It will revert to previously saved values.
7. 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).



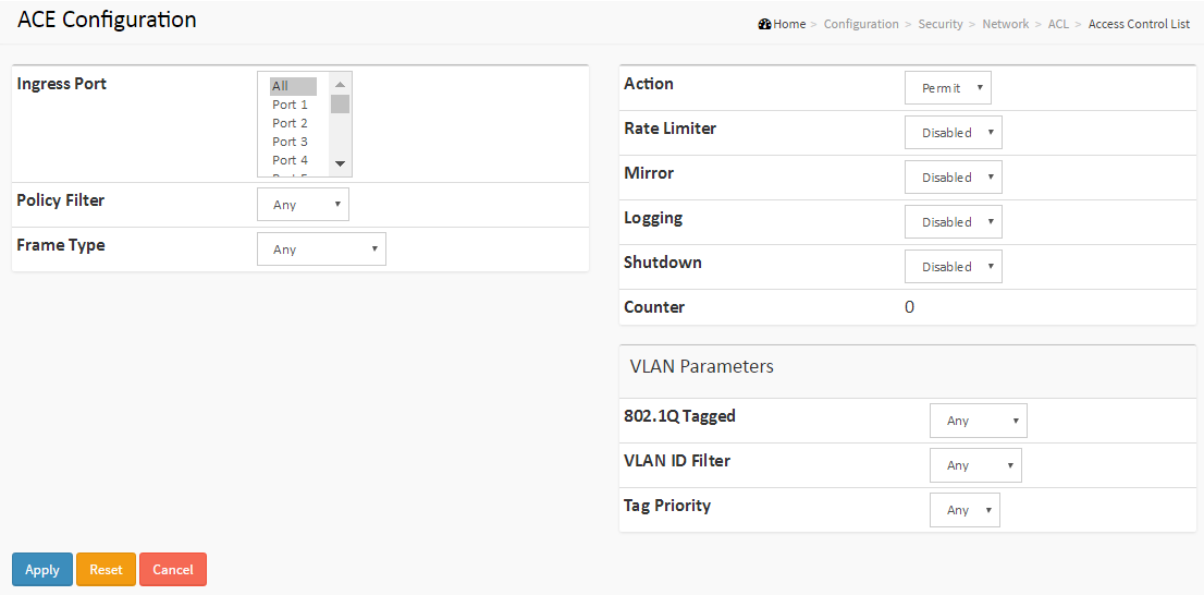


Figure 2-5.2.3.3: The ACL Rate Limiter Configuration

Parameter description:

- **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.

- **Policy / Bitmask :**

  Indicates the policy number and bitmask of the ACE.

- **Frame Type :**

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

  Any: The ACE will match any frame type.

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

  ARP: The ACE will match ARP/RARP frames.

  IPv4: The ACE will match all IPv4 frames.

  IPv4/ICMP: The ACE will match IPv4 frames with ICMP protocol.

  IPv4/UDP: The ACE will match IPv4 frames with UDP protocol.

  IPv4/TCP: The ACE will match IPv4 frames with TCP protocol.

  IPv4/Other: The ACE will match IPv4 frames, which are not ICMP/UDP/TCP.

  IPv6: The ACE will match all IPv6 standard frames.

- **Action :**

  Indicates the forwarding action of the ACE.

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

  Deny: Frames matching the ACE are dropped.

Filter: Frames matching the ACE are filtered.

- **Rate Limiter :**

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

- **Port Redirect :**

  Indicates the port redirect operation of the ACE. Frames matching the ACE are redirected to the port number. The allowed values are Disabled or a specific port number. When Disabled is displayed, the port redirect operation is disabled.

- **Mirror :**

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

  Enabled: Frames received on the port are mirrored.

  Disabled: Frames received on the port are not mirrored.

  The default value is "Disabled".

- **Counter :**

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

- **Modification 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.

ACE Configuration

An ACE consists of several parameters. These parameters vary according to the frame type that you select. First select the ingress port for the ACE, and then select the frame type. Different parameter options are displayed depending on the frame type selected.

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

- **Ingress Port :**

  Select the ingress port for which this ACE applies.
  All: The ACE applies to all port.
  Port n: The ACE applies to this port number, where n is the number of the switch port.

- **Policy Filter :**

  Specify the policy number filter for this ACE.
  Any: No policy filter is specified. (policy filter status is "don't-care".)
  Specific: If you want to filter a specific policy with this ACE, choose this value. Two field for entering an policy value and bitmask appears.

- **Policy Value :**

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

- **Policy Bitmask :**

When "Specific" is selected for the policy filter, you can enter a specific policy bitmask. The allowed range is 0x0 to 0xff. Notice the usage of bitmask, if the binary bit value is "0", it means this bit is "don't-care". The real matched pattern is [policy_value & policy_bitmask]. For example, if the policy value is 3 and the policy bitmask is 0x10(bit 0 is "don't-care" bit), then policy 2 and 3 are applied to this rule.

- **Frame Type :**

  Select the frame type for this ACE. These frame types are mutually exclusive.

  Any: Any frame can match this ACE.

  Ethernet Type: Only Ethernet Type frames can match this ACE. The IEEE 802.3 describes the value of Length/Type Field specifications to be greater than or equal to 1536 decimal (equal to 0600 hexadecimal).

  ARP: Only ARP frames can match this ACE. Notice the ARP frames won't match the ACE with ethernet type.

  IPv4: Only IPv4 frames can match this ACE. Notice the IPv4 frames won't match the ACE with ethernet type.

  IPv6: Only IPv6 frames can match this ACE. Notice the IPv6 frames won't match the ACE with Ethernet type.

- **Action :**

  Specify the action to take with a frame that hits this ACE.

  Permit: The frame that hits this ACE is granted permission for the ACE operation.

  Deny: The frame that hits this ACE is dropped.

  Filter: Frames matching the ACE are filtered.

- **Rate Limiter :**

  Specify the rate limiter in number of base units. The allowed range is 1 to 16. Disabled indicates that the rate limiter operation is disabled.

- **Port Redirect :**

  Frames that hit the ACE are redirected to the port number specified here. The rate limiter will affect these ports. The allowed range is the same as the switch port number range. Disabled indicates that the port redirect operation is disabled and the specific port number of 'Port Redirect' can't be set when action is permitted.

- **Mirror :**

  Specify the mirror operation of this port. Frames matching the ACE are mirrored to the destination mirror port. The rate limiter will not affect frames on the mirror port. The allowed values are:

  Enabled: Frames received on the port are mirrored.

  Disabled: Frames received on the port are not mirrored.

  The default value is "Disabled".

- **Logging :**

  Specify the logging operation of the ACE. Notice that the logging message doesn't include the 4 bytes CRC information. The allowed values are:

  Enabled: Frames matching the ACE are stored in the System Log.

  Disabled: Frames matching the ACE are not logged.

Note: The logging feature only works when the packet length is less than 1518(without VLAN tags) and the System Log memory size and logging rate is limited.

- **Shutdown :**

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

  Enabled: If a frame matches the ACE, the ingress port will be disabled.

  Disabled: Port shut down is disabled for the ACE.

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

- **Counter :**

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

MAC Parameter

- **SMAC Filter :**

  (Only displayed when the frame type is Ethernet Type or ARP.)

  Specify the source MAC filter for this ACE.

  Any: No SMAC filter is specified. (SMAC filter status is "don't-care".)

  Specific: If you want to filter a specific source MAC address with this ACE, choose this value. A field for entering an SMAC value appears.

- **SMAC Value :**

  When "Specific" is selected for the SMAC filter, you can enter a specific source MAC address. The legal format is "xx-xx-xx-xx-xx-xx" or "xx.xx.xx.xx.xx.xx" or "xxxxxxxxxxxx" (x is a hexadecimal digit). A frame that hits this ACE matches this SMAC value.

- **DMAC Filter :**

  Specify the destination MAC filter for this ACE.

  Any: No DMAC filter is specified. (DMAC filter status is "don't-care".)

  MC: Frame must be multicast.

  BC: Frame must be broadcast.

  UC: Frame must be unicast.

  Specific: If you want to filter a specific destination MAC address with this ACE, choose this value. A field for entering a DMAC value appears.

- **DMAC Value :**

  When "Specific" is selected for the DMAC filter, you can enter a specific destination MAC address. The legal format is "xx-xx-xx-xx-xx-xx" or "xx.xx.xx.xx.xx.xx" or "xxxxxxxxxxxx" (x is a hexadecimal digit). A frame that hits this ACE matches this DMAC value.

VLAN Parameters

- **802.1Q Tagged :**

  Specify whether frames can hit the action according to the 802.1Q tagged. The allowed values are:

  Any: Any value is allowed ("don't-care").

  Enabled: Tagged frame only.

  Disabled: Untagged frame only.

The default value is "Any".

- **VLAN ID Filter :**

  Specify the VLAN ID filter for this ACE.

  Any: No VLAN ID filter is specified. (VLAN ID filter status is "don't-care".)

  Specific: If you want to filter a specific VLAN ID with this ACE, choose this value. A field for entering a VLAN ID number appears.

- **VLAN ID :**

  When "Specific" is selected for the VLAN ID filter, you can enter a specific VLAN ID number. The allowed range is 1 to 4095. A frame that hits this ACE matches this VLAN ID value.

- **Tag Priority :**

  Specify the tag priority for this ACE. A frame that hits this ACE matches this tag priority. The allowed number range is 0 to 7 or range 0-1, 2-3, 4-5, 6-7, 0-3 and 4-7. The value Any means that no tag priority is specified (tag priority is "don't-care".)

ARP Parameters

The ARP parameters can be configured when Frame Type "ARP" is selected.

- **ARP/RARP :**

  Specify the available ARP/RARP opcode (OP) flag for this ACE.

  Any: No ARP/RARP OP flag is specified. (OP is "don't-care".)

  ARP: Frame must have ARP opcode set to ARP.

  RARP: Frame must have RARP opcode set to RARP.

  Other: Frame has unknown ARP/RARP Opcode flag.

- **Request/Reply :**

  Specify the available Request/Reply opcode (OP) flag for this ACE.

  Any: No Request/Reply OP flag is specified. (OP is "don't-care".)

  Request: Frame must have ARP Request or RARP Request OP flag set.

  Reply: Frame must have ARP Reply or RARP Reply OP flag.

- **Sender IP Filter :**

  Specify the sender IP filter for this ACE.

  Any: No sender IP filter is specified. (Sender IP filter is "don't-care".)

  Host: Sender IP filter is set to Host. Specify the sender IP address in the SIP Address field that appears.

  Network: Sender IP filter is set to Network. Specify the sender IP address and sender IP mask in the SIP Address and SIP Mask fields that appear.

- **Sender IP Address :**

  When "Host" or "Network" is selected for the sender IP filter, you can enter a specific sender IP address in dotted decimal notation.

- **Sender IP Mask :**

  When "Network" is selected for the sender IP filter, you can enter a specific sender IP mask in dotted decimal notation.

- **Target IP Filter :**

  Specify the target IP filter for this specific ACE.

  Any: No target IP filter is specified. (Target IP filter is "don't-care".)

  Host: Target IP filter is set to Host. Specify the target IP address in the Target IP Address field that appears. Network: Target IP filter is set to Network. Specify the target IP address and target IP mask in the Target IP Address and Target IP Mask fields that appear.

- **Target IP Address :**

  When "Host" or "Network" is selected for the target IP filter, you can enter a specific target IP address in dotted decimal notation.

- **Target IP Mask :**

  When "Network" is selected for the target IP filter, you can enter a specific target IP mask in dotted decimal notation.

- **ARP Sender MAC Match :**

  Specify whether frames can hit the action according to their sender hardware address field (SHA) settings.

  0: ARP frames where SHA is not equal to the SMAC address.

  1: ARP frames where SHA is equal to the SMAC address.

  Any: Any value is allowed ("don't-care").

- **RARP Target MAC Match :**

  Specify whether frames can hit the action according to their target hardware address field (THA) settings.

  0: RARP frames where THA is not equal to the target MAC address.

  1: RARP frames where THA is equal to the target MAC address.

  Any: Any value is allowed ("don't-care").

- **IP/Ethernet Length :**

  Specify whether frames can hit the action according to their ARP/RARP hardware address length (HLN) and protocol address length (PLN) settings.

  0: ARP/RARP frames where the HLN is not equal to Ethernet (0x06) or the (PLN) is not equal to IPv4 (0x04).

  1: ARP/RARP frames where the HLN is equal to Ethernet (0x06) and the (PLN) is equal to IPv4 (0x04).

  Any: Any value is allowed ("don't-care").

- **Ethernet :**

  Specify whether frames can hit the action according to their ARP/RARP hardware address space (HRD) settings.

  0: ARP/RARP frames where the HLD is not equal to Ethernet (1).

  1: ARP/RARP frames where the HLD is equal to Ethernet (1).

  Any: Any value is allowed ("don't-care").

- **IP :**

  Specify whether frames can hit the action according to their ARP/RARP protocol address

space (PRO) settings.

0: ARP/RARP frames where the PRO is not equal to IP (0x800).

1: ARP/RARP frames where the PRO is equal to IP (0x800).

Any: Any value is allowed ("don't-care").

IP Parameters

The IP parameters can be configured when Frame Type "IPv4" is selected.

- **IP Protocol Filter :**

  Specify the IP protocol filter for this ACE.

  Any: No IP protocol filter is specified ("don't-care").

  Specific: If you want to filter a specific IP protocol filter with this ACE, choose this value. A field for entering an IP protocol filter appears.

  ICMP: Select ICMP to filter IPv4 ICMP protocol frames. Extra fields for defining ICMP parameters will appear. These fields are explained later in this help file.

  UDP: Select UDP to filter IPv4 UDP protocol frames. Extra fields for defining UDP parameters will appear. These fields are explained later in this help file.

  TCP: Select TCP to filter IPv4 TCP protocol frames. Extra fields for defining TCP parameters will appear. These fields are explained later in this help file.

- **IP Protocol Value :**

  When "Specific" is selected for the IP protocol value, you can enter a specific value. The allowed range is 0 to 255. A frame that hits this ACE matches this IP protocol value.

- **IP TTL :**

  Specify the Time-to-Live settings for this ACE.

  zero: IPv4 frames with a Time-to-Live field greater than zero must not be able to match this entry.

  non-zero: IPv4 frames with a Time-to-Live field greater than zero must be able to match this entry.

  Any: Any value is allowed ("don't-care").

- **IP Fragment :**

  Specify the fragment offset settings for this ACE. This involves the settings for the More Fragments (MF) bit and the Fragment Offset (FRAG OFFSET) field for an IPv4 frame.

  No: IPv4 frames where the MF bit is set or the FRAG OFFSET field is greater than zero must not be able to match this entry.

  Yes: IPv4 frames where the MF bit is set or the FRAG OFFSET field is greater than zero must be able to match this entry.

  Any: Any value is allowed ("don't-care").

- **IP Option :**

  Specify the options flag setting for this ACE.

  No: IPv4 frames where the options flag is set must not be able to match this entry.

  Yes: IPv4 frames where the options flag is set must be able to match this entry.

  Any: Any value is allowed ("don't-care").

- **SIP Filter :**

  Specify the source IP filter for this ACE.

  Any: No source IP filter is specified. (Source IP filter is "don't-care".)

  Host: Source IP filter is set to Host. Specify the source IP address in the SIP Address field that appears.

  Network: Source IP filter is set to Network. Specify the source IP address and source IP mask in the SIP Address and SIP Mask fields that appear.

- **SIP Address :**

  When "Host" or "Network" is selected for the source IP filter, you can enter a specific SIP address in dotted decimal notation.

- **SIP Mask :**

  When "Network" is selected for the source IP filter, you can enter a specific SIP mask in dotted decimal notation.

- **DIP Filter :**

  Specify the destination IP filter for this ACE.

  Any: No destination IP filter is specified. (Destination IP filter is "don't-care".)

  Host: Destination IP filter is set to Host. Specify the destination IP address in the DIP Address field that appears.

  Network: Destination IP filter is set to Network. Specify the destination IP address and destination IP mask in the DIP Address and DIP Mask fields that appear.

- **DIP Address :**

  When "Host" or "Network" is selected for the destination IP filter, you can enter a specific DIP address in dotted decimal notation.

- **DIP Mask :**

  When "Network" is selected for the destination IP filter, you can enter a specific DIP mask in dotted decimal notation.

IPv6 Parameters

The IPv6 parameters can be configured when Frame Type "IPv6" is selected.

- **Next Header Filter :**

  Specify the IPv6 next header filter for this ACE.

  Any: No IPv6 next header filter is specified ("don't-care").

  Specific: If you want to filter a specific IPv6 next header filter with this ACE, choose this value. A field for entering an IPv6 next header filter appears.

  ICMP: Select ICMP to filter IPv6 ICMP protocol frames. Extra fields for defining ICMP parameters will appear. These fields are explained later in this help file.

  UDP: Select UDP to filter IPv6 UDP protocol frames. Extra fields for defining UDP parameters will appear. These fields are explained later in this help file.

  TCP: Select TCP to filter IPv6 TCP protocol frames. Extra fields for defining TCP parameters will appear. These fields are explained later in this help file.

- **Next Header Value :**

  When "Specific" is selected for the IPv6 next header value, you can enter a specific value.

The allowed range is 0 to 255. A frame that hits this ACE matches this IPv6 protocol value.

- **SIP Filter :**

  Specify the source IPv6 filter for this ACE.

  Any: No source IPv6 filter is specified. (Source IPv6 filter is "don't-care".)

  Specific: Source IPv6 filter is set to Network. Specify the source IPv6 address and source IPv6 mask in the SIP Address fields that appear.

- **SIP Address :**

  When "Specific" is selected for the source IPv6 filter, you can enter a specific SIPv6 address. The field only supported last 32 bits for IPv6 address.

- **SIP BitMask :**

  When "Specific" is selected for the source IPv6 filter, you can enter a specific SIPv6 mask. The field only supported last 32 bits for IPv6 address. Notice the usage of bitmask, if the binary bit value is "0", it means this bit is "don't-care". The real matched pattern is [sipv6_address & sipv6_bitmask] (last 32 bits). For example, if the SIPv6 address is 2001::3 and the SIPv6 bitmask is 0xFFFFFFFE(bit 0 is "don't-care" bit), then SIPv6 address 2001::2 and 2001::3 are applied to this rule.

- **Hop Limit :**

  Specify the hop limit settings for this ACE.

  zero: IPv6 frames with a hop limit field greater than zero must not be able to match this entry.

  non-zero: IPv6 frames with a hop limit field greater than zero must be able to match this entry.

  Any: Any value is allowed ("don't-care").

ICMP Parameters

- **ICMP Type Filter :**

  Specify the ICMP filter for this ACE.

  Any: No ICMP filter is specified (ICMP filter status is "don't-care").

  Specific: If you want to filter a specific ICMP filter with this ACE, you can enter a specific ICMP value. A field for entering an ICMP value appears.

- **ICMP Type Value :**

  When "Specific" is selected for the ICMP filter, you can enter a specific ICMP value. The allowed range is 0 to 255. A frame that hits this ACE matches this ICMP value.

- **ICMP Code Filter :**

  Specify the ICMP code filter for this ACE.

  Any: No ICMP code filter is specified (ICMP code filter status is "don't-care").

  Specific: If you want to filter a specific ICMP code filter with this ACE, you can enter a specific ICMP code value. A field for entering an ICMP code value appears.

- **ICMP Code Value :**

  When "Specific" is selected for the ICMP code filter, you can enter a specific ICMP code value. The allowed range is 0 to 255. A frame that hits this ACE matches this ICMP code value.

TCP/UDP Parameters

- **TCP/UDP Source Filter :**

  Specify the TCP/UDP source filter for this ACE.

  Any: No TCP/UDP source filter is specified (TCP/UDP source filter status is "don't-care").

  Specific: If you want to filter a specific TCP/UDP source filter with this ACE, you can enter a specific TCP/UDP source value. A field for entering a TCP/UDP source value appears.

  Range: If you want to filter a specific TCP/UDP source range filter with this ACE, you can enter a specific TCP/UDP source range value. A field for entering a TCP/UDP source value appears.

- **TCP/UDP Source No. :**

  When "Specific" is selected for the TCP/UDP source filter, you can enter a specific TCP/UDP source value. The allowed range is 0 to 65535. A frame that hits this ACE matches this TCP/UDP source value.

- **TCP/UDP Source Range :**

  When "Range" is selected for the TCP/UDP source filter, you can enter a specific TCP/UDP source range value. The allowed range is 0 to 65535. A frame that hits this ACE matches this TCP/UDP source value.

- **TCP/UDP Destination Filter :**

  Specify the TCP/UDP destination filter for this ACE.

  Any: No TCP/UDP destination filter is specified (TCP/UDP destination filter status is "don't-care").

  Specific: If you want to filter a specific TCP/UDP destination filter with this ACE, you can enter a specific TCP/UDP destination value. A field for entering a TCP/UDP destination value appears.

  Range: If you want to filter a specific range TCP/UDP destination filter with this ACE, you can enter a specific TCP/UDP destination range value. A field for entering a TCP/UDP destination value appears.

- **TCP/UDP Destination Number :**

  When "Specific" is selected for the TCP/UDP destination filter, you can enter a specific TCP/UDP destination value. The allowed range is 0 to 65535. A frame that hits this ACE matches this TCP/UDP destination value.

- **TCP/UDP Destination Range :**

  When "Range" is selected for the TCP/UDP destination filter, you can enter a specific TCP/UDP destination range value. The allowed range is 0 to 65535. A frame that hits this ACE matches this TCP/UDP destination value.

- **TCP FIN :**

  Specify the TCP "No more data from sender" (FIN) value for this ACE.

  0: TCP frames where the FIN field is set must not be able to match this entry.

  1: TCP frames where the FIN field is set must be able to match this entry.

  Any: Any value is allowed ("don't-care").

- **TCP SYN :**

  Specify the TCP "Synchronize sequence numbers" (SYN) value for this ACE.

0: TCP frames where the SYN field is set must not be able to match this entry.

1: TCP frames where the SYN field is set must be able to match this entry.

Any: Any value is allowed ("don't-care").

- **TCP RST :**

  Specify the TCP "Reset the connection" (RST) value for this ACE.

  0: TCP frames where the RST field is set must not be able to match this entry.

  1: TCP frames where the RST field is set must be able to match this entry.

  Any: Any value is allowed ("don't-care").

- **TCP PSH :**

  Specify the TCP "Push Function" (PSH) value for this ACE.

  0: TCP frames where the PSH field is set must not be able to match this entry.

  1: TCP frames where the PSH field is set must be able to match this entry.

  Any: Any value is allowed ("don't-care").

- **TCP ACK :**

  Specify the TCP "Acknowledgment field significant" (ACK) value for this ACE.

  0: TCP frames where the ACK field is set must not be able to match this entry.

  1: TCP frames where the ACK field is set must be able to match this entry.

  Any: Any value is allowed ("don't-care").

- **TCP URG :**

  Specify the TCP "Urgent Pointer field significant" (URG) value for this ACE.

  0: TCP frames where the URG field is set must not be able to match this entry.

  1: TCP frames where the URG field is set must be able to match this entry.

  Any: Any value is allowed ("don't-care").

Ethernet Type Parameters

The Ethernet Type parameters can be configured when Frame Type "Ethernet Type" is selected.

- **EtherType Filter :**

  Specify the Ethernet type filter for this ACE.

  Any: No EtherType filter is specified (EtherType filter status is "don't-care").

  Specific: If you want to filter a specific EtherType filter with this ACE, you can enter a specific EtherType value. A field for entering a EtherType value appears.

- **Ethernet Type Value :**

  When "Specific" is selected for the EtherType filter, you can enter a specific EtherType value. The allowed range is 0x600 to 0xFFFF but excluding 0x800(IPv4), 0x806(ARP) and 0x86DD(IPv6). A frame that hits this ACE matches this EtherType value.

Buttons

- **Apply :**

  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 to refresh the information automatically.

- **Refresh, clear, Remove All :**

  You can click them for refresh the ACL configuration or clear them by manual. Others remove all to clean up all ACL configurations on the table.

- **Cancel :** Return to the previous page.

2-5.2.4 IP Source Guard

The section describes to configure the IP Source Guard detail parameters of the switch. You could use the IP Source Guard configure to enable or disable with the Port of the switch.

2-5.2.4.1 Configuration

This section describes how to configure IP Source Guard setting including:
Mode (Enabled and Disabled)
Maximum Dynamic Clients (0, 1, 2, Unlimited)

Web Interface

To configure an IP Source Guard Configuration in the web interface:

1. Click Configuration, Security, Network, IP Source Guard and Configuration.
2. Select "Enabled" in the Mode of IP Source Guard Configuration.
3. Select "Enabled" of the specific port in the Mode of Port Mode Configuration.
4. Select Maximum Dynamic Clients (0, 1, 2, Unlimited) of the specific port in the Mode of Port Mode Configuration.
5. Click Apply.

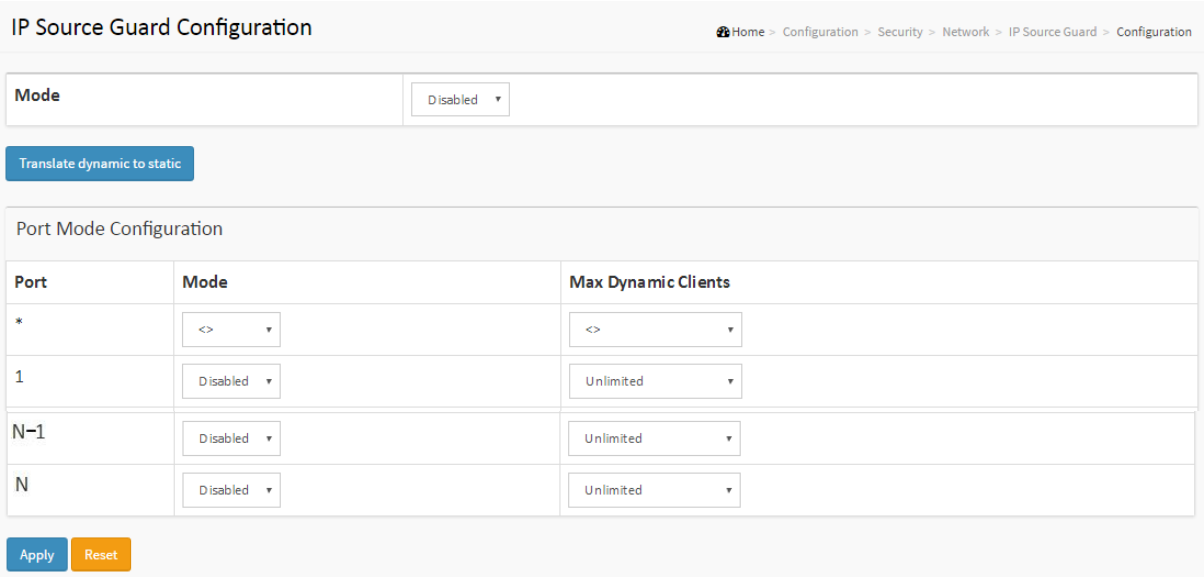


Figure 2-5.2.4.1: The IP Source Guard Configuration

Parameter description:

- **Mode of IP Source Guard Configuration :**

  Enable the Global IP Source Guard or disable the Global IP Source Guard. All configured ACEs will be lost when the mode is enabled.

- **Port Mode Configuration :**

  Specify IP Source Guard is enabled on which ports. Only when both Global Mode and Port

Mode on a given port are enabled, IP Source Guard is enabled on this given port.

- **Max Dynamic Clients :**

  Specify the maximum number of dynamic clients that can be learned on given port. This value can be 0, 1, 2 or unlimited. If the port mode is enabled and the value of max dynamic client is equal to 0, it means only allow the IP packets forwarding that are matched in static entries on the specific port.

Buttons

- **Translate dynamic to static :**

  Click to translate all dynamic entries to static entries.

- **Apply :**

  Click to save changes.

- **Reset :**

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

2-5.2.4.2 Static Table

The section describes to configure the Static IP Source Guard Table parameters of the switch. You could use the Static IP Source Guard Table configure to manage the entries.

Web Interface

To configure a Static IP Source Guard Table Configuration in the web interface:

1. Click Configuration, Security, Network, IP Source Guard and Static Table.
2. Click "Add New Entry".
3. Specify the Port, VLAN ID, IP Address, and MAC address in the entry.
4. Click Apply.

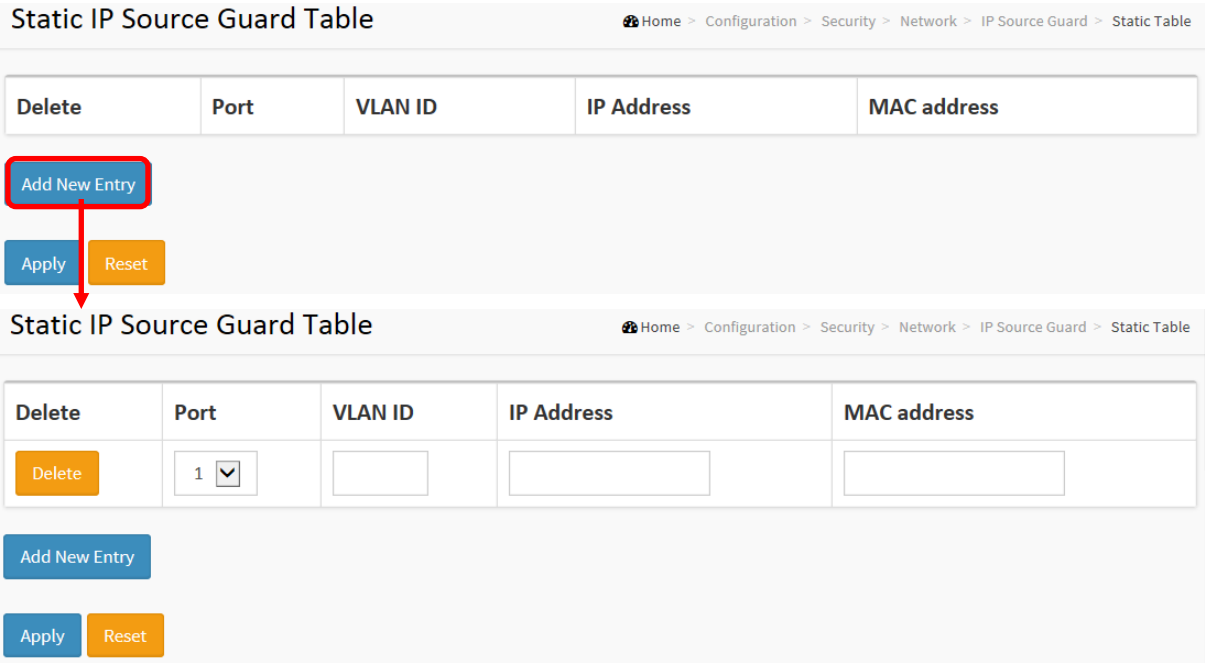


Figure 2-5.2.4.2: The Static IP Source Guard Table

Parameter description:

- **Port :**

  The logical port for the settings.

- **VLAN ID :**

  The VLAN id for the settings.

- **IP Address :**

  Allowed Source IP address.

- **MAC address :**

  Allowed Source MAC address.

Buttons

- **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".

- **Apply :**

  Click to save changes.

- **Reset :**

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

- **Delete :**

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

2-5.2.5 ARP Inspection

The section describes to configure the ARP Inspection parameters of the switch. You could use the ARP Inspection configure to manage the ARP table.

2-5.2.5.1 Port Configuration

This section describes how to configure ARP Inspection setting including:
Mode (Enabled and Disabled)
Port (Enabled and Disabled)

Web Interface

To configure an ARP Inspection Configuration in the web interface:

1. Click Configuration, Security, Network, ARP Inspection and Configuration.
2. Select "Enabled" in the Mode of ARP Inspection Configuration.
3. Select "Enabled" of the specific port in the Mode of Port Mode Configuration.
4. Click Apply.

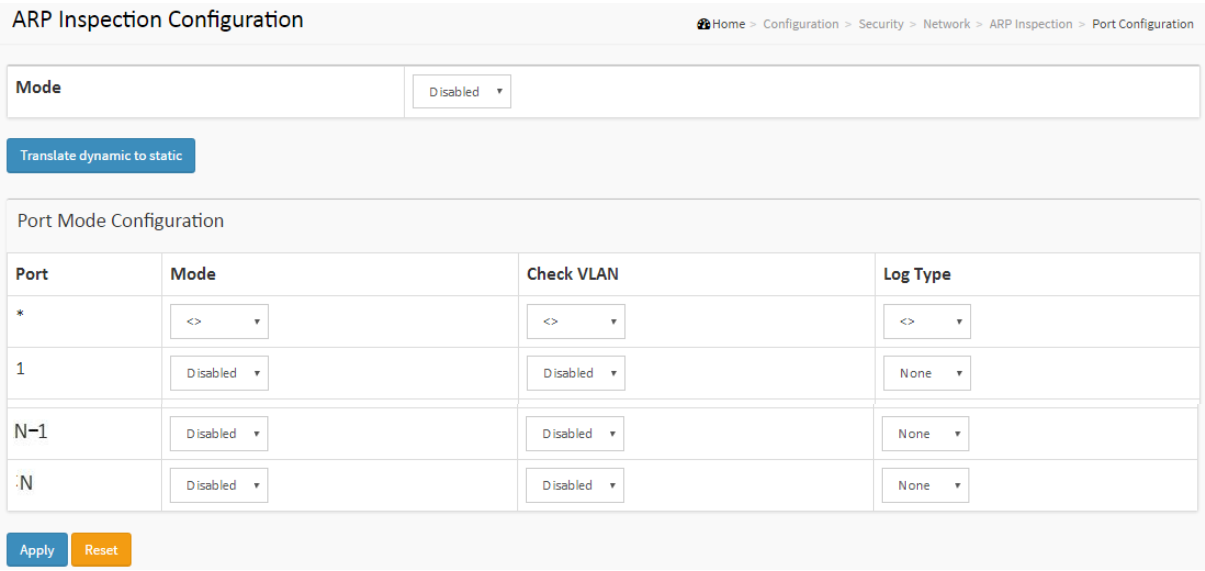


Figure 2-5.2.5.1: The ARP Inspection Configuration.

Parameter description:

- **Mode of ARP Inspection Configuration :**

  Enable the Global ARP Inspection or disable the Global ARP Inspection.

- **Port Mode Configuration :**

  Specify ARP Inspection is enabled on which ports. Only when both Global Mode and Port Mode on a given port are enabled, ARP Inspection is enabled on this given port. Possible modes are:
  Enabled: Enable ARP Inspection operation.

Disabled: Disable ARP Inspection operation.
If you want to inspect the VLAN configuration, you have to enable the setting of "Check VLAN". The default setting of "Check VLAN" is disabled. When the setting of "Check VLAN" is disabled, the log type of ARP Inspection will refer to the port setting. And the setting of "Check VLAN" is enabled, the log type of ARP Inspection will refer to the VLAN setting.
Possible setting of "Check VLAN" are:
Enabled: Enable check VLAN operation.
Disabled: Disable check VLAN operation.
Only the Global Mode and Port Mode on a given port are enabled, and the setting of "Check VLAN" is disabled, the log type of ARP Inspection will refer to the port setting. There are four log types and possible types are:
None: Log nothing.
Deny: Log denied entries.
Permit: Log permitted entries.
ALL: Log all entries.

Buttons

- **Translate dynamic to static :**

  Click to translate all dynamic entries to static entries.

- **Apply :**

  Click to save changes.

- **Reset :**

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

2-5.2.5.2 VLAN Configuration

Each page shows up to 9999 entries from the VLAN table, default being 20, selected through the "entries per page" input field. When first visited, the web page will show the first 20 entries from the beginning of the VLAN Table. The first displayed will be the one with the lowest VLAN ID found in the VLAN Table.
The "VLAN" input fields allow the user to select the starting point in the VLAN Table. Clicking the button will update the displayed table starting from that or the closest next VLAN Table match. The will use the next entry of the currently displayed VLAN entry as a basis for the next lookup. When the end is reached the warning message is shown in the displayed table. Use the button to start over.

Web Interface

To configure a VLAN Mode Configuration in the web interface:

1. Click Configuration, Security, Network, ARP Inspection and VLAN Mode Configuration.
2. Click “Add new entry”.
3. Specify the VLAN ID, Log Type
4. Click Apply.

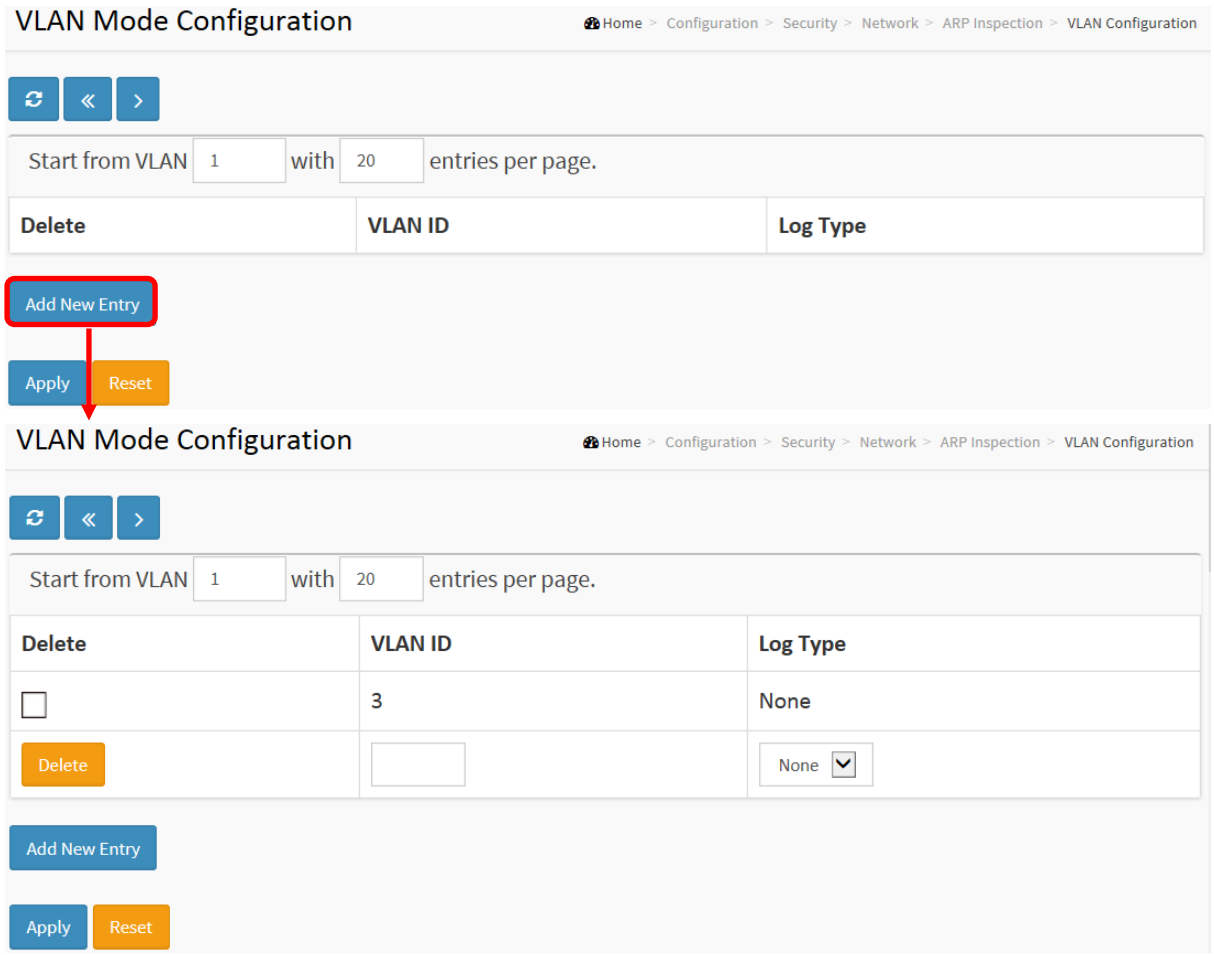


Figure 2-5.2.5.2: The VLAN Mode Configuration

Parameter description:

- **VLAN Mode Configuration :**

  Specify ARP Inspection is enabled on which VLANs. First, you have to enable the port setting on Port mode configuration web page. Only when both Global Mode and Port Mode on a given port are enabled, ARP Inspection is enabled on this given port. Second, you can specify which VLAN will be inspected on VLAN mode configuration web page. The log type also can be configured on per VLAN setting.
  Possible types are:
  None: Log nothing.
  Deny: Log denied entries.
  Permit: Log permitted entries.
  ALL: Log all entries.

Buttons

- **Delete :**

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

- **Apply :**

  Click to save changes.

- **Reset :**

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

- **Add New Entry :**

  Click to add a new VLAN to the ARP Inspection VLAN table.

2-5.2.5.3 Static Table

The section describes to configure the Static ARP Inspection Table parameters of the switch. You could use the Static ARP Inspection Table configure to manage the ARP entries.

Web Interface

To configure a Static ARP Inspection Table Configuration in the web interface:

1. Click Configuration, Security, Network, ARP Inspection and Static Table.
2. Click "Add New Entry".
3. Specify the Port, VLAN ID, IP Address, and MAC address in the entry.
4. Click Apply.

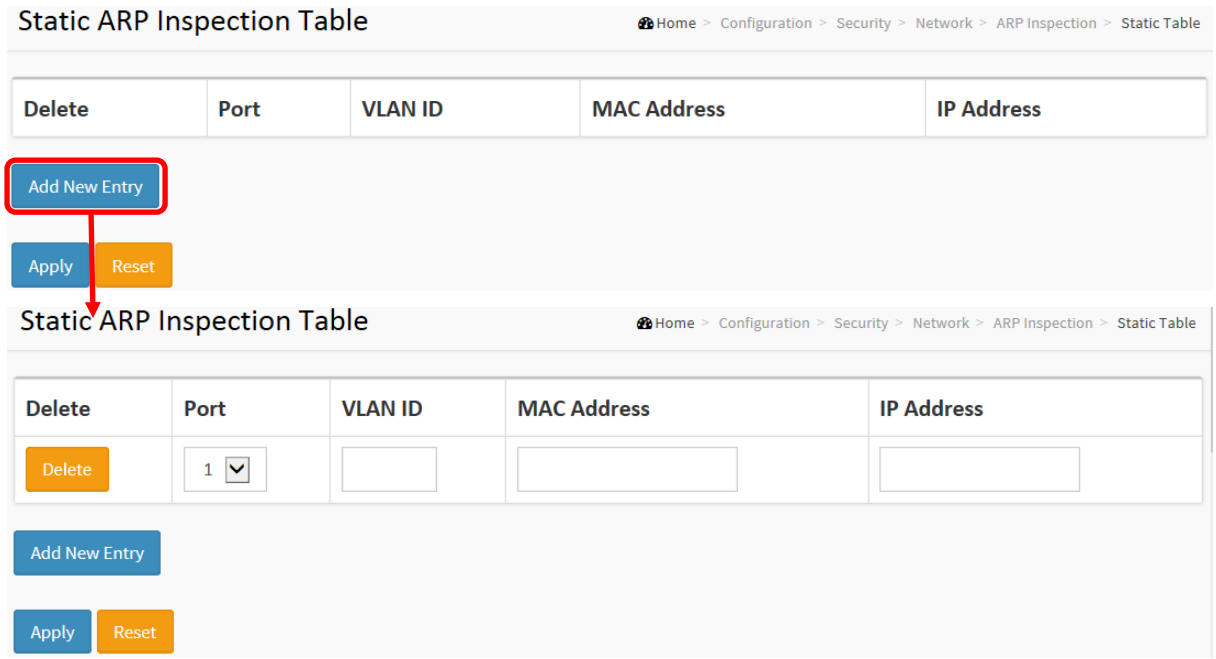


Figure 2-5.2.5.3: The Static ARP Inspection Table

Parameter description:

- **Port :**

  The logical port for the settings.

- **VLAN ID :**

  The vlan id for the settings.

- **MAC Address :**

  Allowed Source MAC address in ARP request packets.

- **IP Address :**

  Allowed Source IP address in ARP request packets.

Buttons

- **Delete :**

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

- **Apply :**

  Click to save changes.

- **Reset :**

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

- **Add New Entry :**

  Click to add a new entry to the Static ARP Inspection table. Specify the Port, VLAN ID, MAC address, and IP address for the new entry. Click "Save".

2-5.2.5.4 Dynamic Table

Entries in the Dynamic ARP Inspection Table are shown on this page. The Dynamic ARP Inspection Table contains up to 1024 entries, and is sorted first by port, then by VLAN ID, then by MAC address, and then by IP address.

Navigating the ARP Inspection Table
Each page shows up to 99 entries from the Dynamic ARP Inspection table, default being 20, selected through the "entries per page" input field. When first visited, the web page will show the first 20 entries from the beginning of the Dynamic ARP Inspection Table.
The "Start from port address", "VLAN", "MAC address" and "IP address" input fields allow the user to select the starting point in the Dynamic ARP Inspection Table. Clicking the button will update the displayed table starting from that or the closest next Dynamic ARP Inspection Table match. In addition, the two input fields will - upon a button click - assume the value of the first displayed entry, allowing for continuous refresh with the same start address.
The will use the last entry of the currently displayed table as a basis for the next lookup. When the end is reached the text "No more entries" is shown in the displayed table. Use the button to start over.

Web Interface

To configure a Dynamic ARP Inspection Table Configuration in the web interface:

1. Click Configuration, Security, Network, ARP Inspection and Dynamic Table.
2. Select “Port” in the Mode of Dynamic ARP Inspection Table.
3. Click Apply.

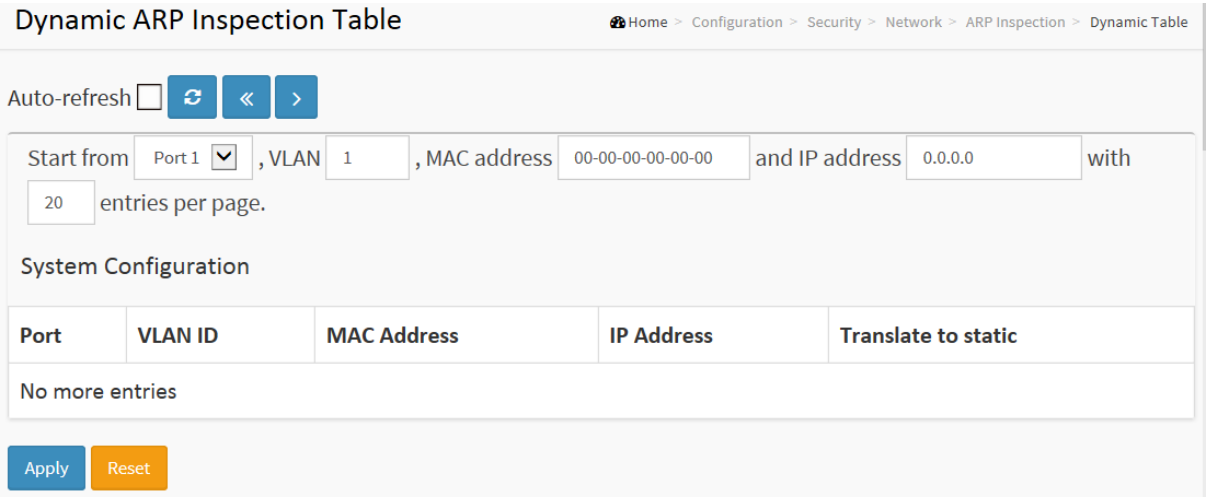


Figure 2-5.2.5.4: The Dynamic ARP Inspection Table

Parameter description:

- **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.

- **Translate to static :**

  Select the checkbox to translate the entry to static entry.

Buttons

- **Apply :**

  Click to save changes.

- **Reset :**

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

- **Auto-refresh :**

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

- **Refresh :**

  Refreshes the displayed table starting from the input fields.

- **Save :**

  Click to save changes.

- **<< :**

  Updates the table starting from the first entry in the Dynamic ARP Inspection Table.

- **>> :**

  Updates the table, starting with the entry after the last entry currently displayed

2-5.3 AAA

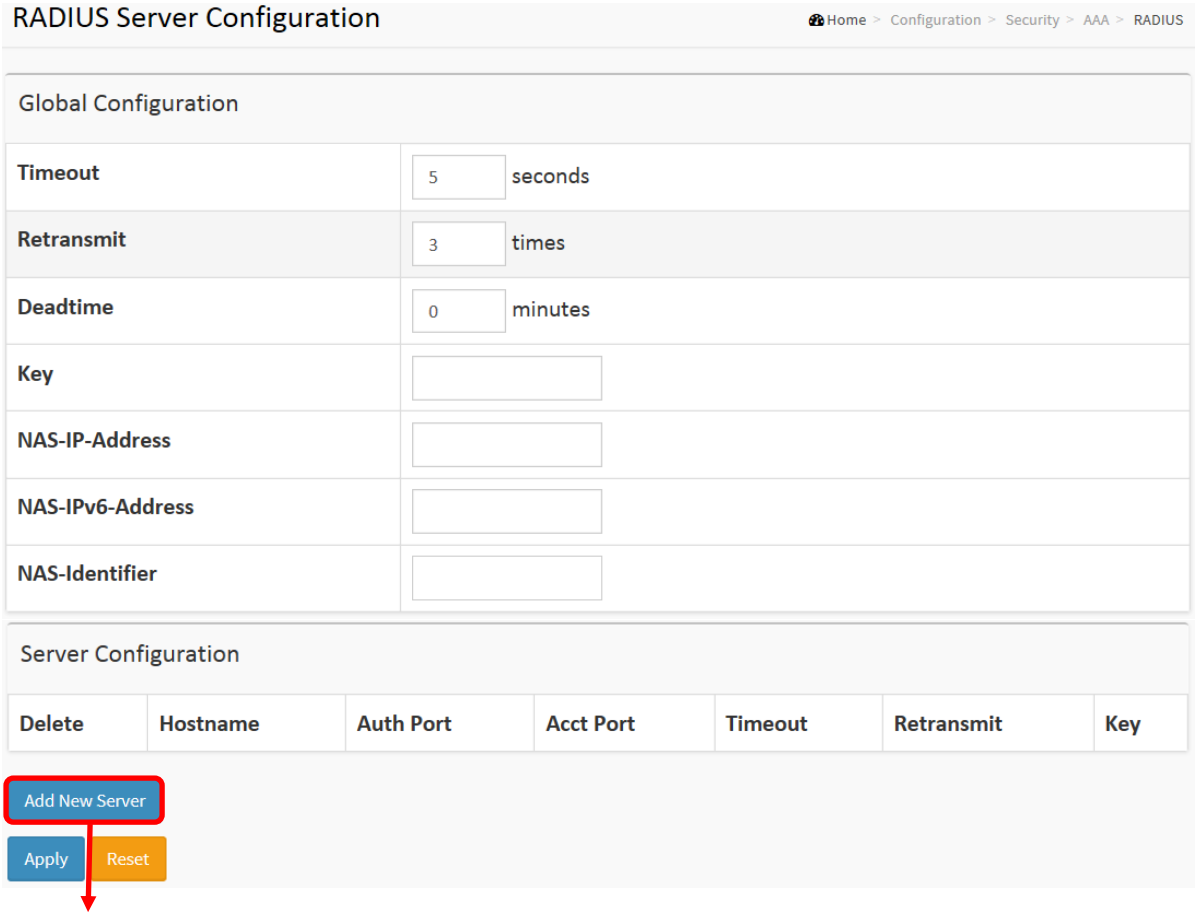
This section shows you to use an AAA (Authentication, Authorization, and Accounting) server to provide access control to your network. The AAA server can be a TACACS+ or RADIUS server to create and manage objects that contain settings for using AAA servers.

2-5.3.1 RADIUS

Web Interface

To configure a Common Configuration of AAA, RADIUS in the web interface:

1. Click Configuration, Security, AAA and RADIUS.
2. Click "Add New Server".
3. Specify the Hostname, Auth Port, Acct Port, Timeout, Retransmit and Key in the server.
4. Click Apply.



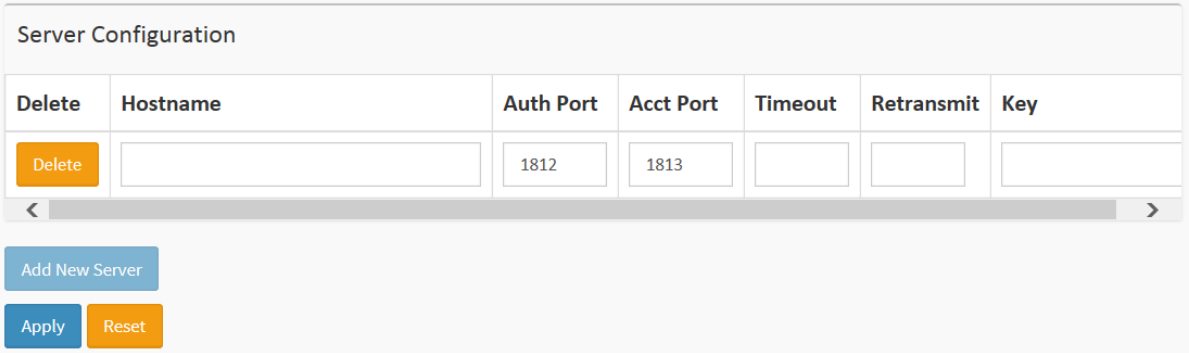


Figure 2-5.3.1: The RADIUS Server Configuration

Parameter description:

Global Configuration

These setting are common for all of the RADIUS servers.

- **Timeout :**

  Timeout is the number of seconds, in the range 1 to 1000, to wait for a reply from a RADIUS server before retransmitting the request.

- **Retransmit :**

  Retransmit is the number of times, in the range 1 to 1000, a RADIUS request is retransmitted to a server that is not responding. If the server has not responded after the last retransmit it is considered to be dead.

- **Deadtime :**

  Deadtime, which can be set to a number between 0 to 1440 minutes, is the period during which the switch will not send new requests to a server that has failed to respond to a previous request. This will stop the switch from continually trying to contact a server that it has already determined as dead.
  Setting the Deadtime to a value greater than 0 (zero) will enable this feature, but only if more than one server has been configured.

- **Key :**

  The secret key - up to 63 characters long - shared between the RADIUS server and the switch.

- **NAS-IP-Address (Attribute 4) :**

  The IPv4 address to be used as attribute 4 in RADIUS Access-Request packets. If this field is left blank, the IP address of the outgoing interface is used.

- **NAS-IPv6-Address (Attribute 95) :**

  The IPv6 address to be used as attribute 95 in RADIUS Access-Request packets. If this field is left blank, the IP address of the outgoing interface is used.

- **NAS-Identifier (Attribute 32) :**

  The identifier - up to 255 characters long - to be used as attribute 32 in RADIUS Access-Request packets. If this field is left blank, the NAS-Identifier is not included in the packet.

Server Configuration

The table has one row for each RADIUS server and a number of columns, which are:

- **Hostname :**

  The IP address or hostname of the RADIUS server.

- **Auth Port :**

  The UDP port to use on the RADIUS server for authentication.

- **Acct Port :**

  The UDP port to use on the RADIUS server for accounting.

- **Timeout :**

  This optional setting overrides the global timeout value. Leaving it blank will use the global timeout value.

- **Retransmit :**

  This optional setting overrides the global retransmit value. Leaving it blank will use the global retransmit value.

- **Key :**

  This optional setting overrides the global key. Leaving it blank will use the global key.

Buttons

- **Delete :**

  This button can be used to undo the addition of the new server.

- **Add New Server :**

  Click to add a new RADIUS server. An empty row is added to the table, and the RADIUS server can be configured as needed. Up to 5 servers are supported.
  The button can be used to undo the addition of the new server.

- **Apply :**

  Click to save changes.

- **Reset :**

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

This page allows you to configure the TACACS+ servers.

Web Interface

To configure the TACACS+ servers in the web interface:

1. Click Configuration, Security, AAA and TACACS+.
2. Click "Add New Server".
3. Specify the Hostname, Port, Timeout and Key in the server.
4. Click Apply.

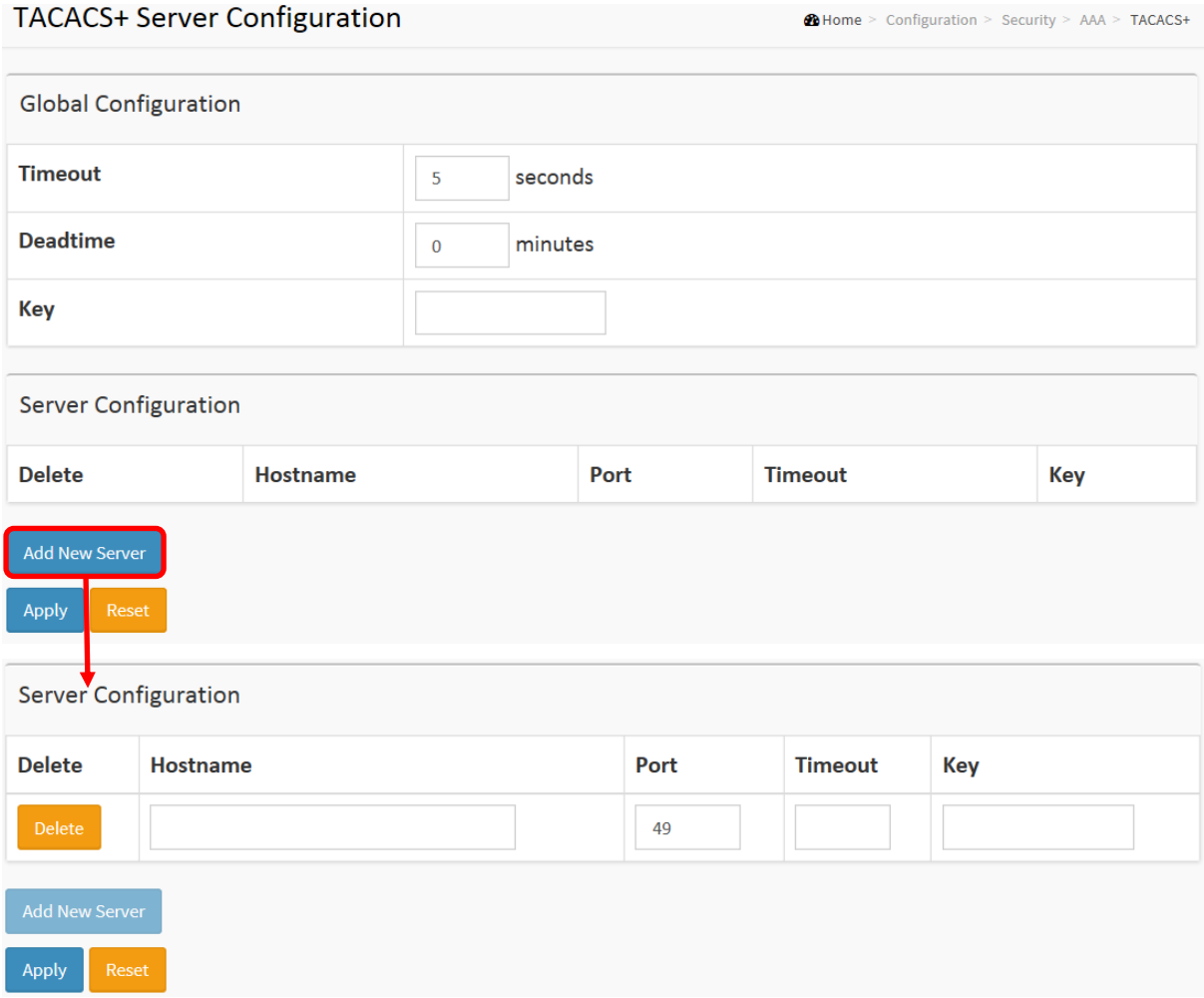


Figure 2-5.3.2: The TACACS+ Server Configuration

Parameter description:

Global Configuration

These setting are common for all of the TACACS+ servers.

- **Timeout :**

Timeout is the number of seconds, in the range 1 to 1000, to wait for a reply from a TACACS+ server before it is considered to be dead.

- **Deadtime :**

  Deadtime, which can be set to a number between 0 to 1440 minutes, is the period during which the switch will not send new requests to a server that has failed to respond to a previous request. This will stop the switch from continually trying to contact a server that it has already determined as dead.
  Setting the Deadtime to a value greater than 0 (zero) will enable this feature, but only if more than one server has been configured.

- **Key :**

  The secret key - up to 63 characters long - shared between the TACACS+ server and the switch.

Server Configuration

The table has one row for each TACACS+ server and a number of columns, which are:

- **Delete :**

  To delete a TACACS+ server entry, check this box. The entry will be deleted during the next Save.

- **Hostname :**

  The IP address or hostname of the TACACS+ server.

- **Port :**

  The TCP port to use on the TACACS+ server for authentication.

- **Timeout :**

  This optional setting overrides the global timeout value. Leaving it blank will use the global timeout value.

- **Key :**

  This optional setting overrides the global key. Leaving it blank will use the global key.

Buttons

- **Delete :**

  This button can be used to undo the addition of the new server.

- **Add New Server :**

  Click to add a new TACACS+ server. An empty row is added to the table, and the TACACS+ server can be configured as needed. Up to 5 servers are supported.

- **Apply :**

  Click to save changes.

- **Reset :**

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

2-6 Aggregation

2-6.1 Static

Web Interface

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

1. Click Configuration, Aggregation and Static.
2. Evoke to enable or disable the aggregation mode function.
3. Evoke Aggregation Group ID and Port members.
4. Click Apply 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.

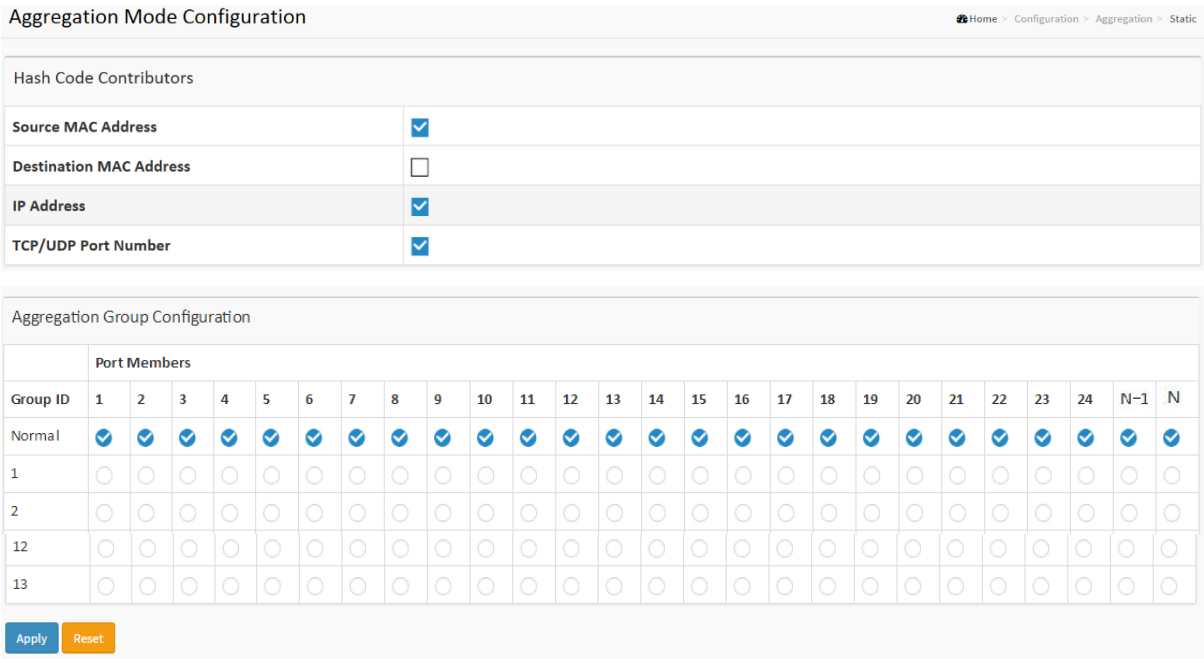


Figure 2-6.1: The Aggregation Mode Configuration

Parameter description:

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

- **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

- **Apply :**

  Click to save changes.

- **Reset :**

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

2-6.2 LACP

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

Web Interface

To configure the LACP Port Configuration in the web interface:

1. Click Configuration, Aggregation and LACP.
2. Evoke to enable or disable the LACP on the port of the switch.
3. Scroll the Key parameter with Auto or Specific. Default is Auto.
4. Scroll the Role with Active or Passive. Default is Active.
5. Click Apply to save the setting.
6. If you want to cancel the setting then you need to click the reset button. It will revert to previously saved values.

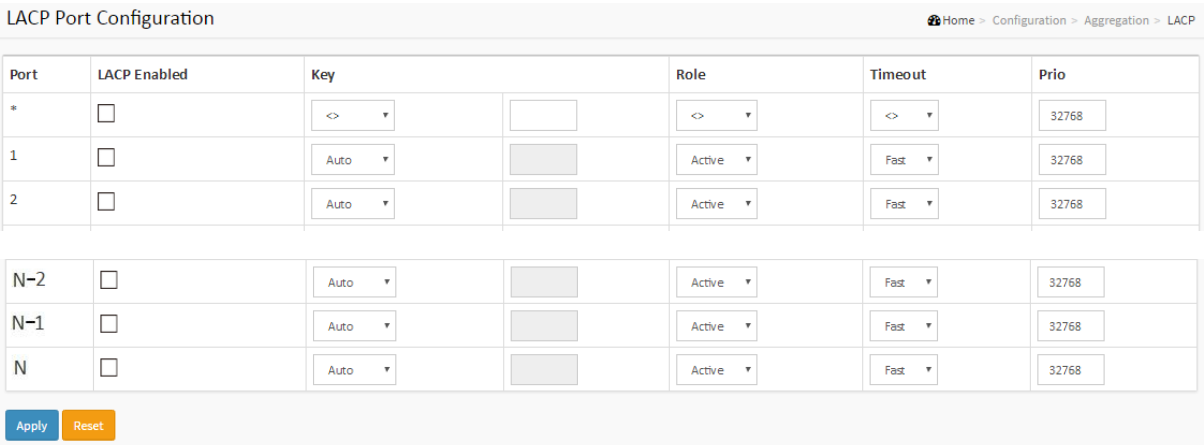


Figure 2-6.2: The LACP Port Configuration

Parameter description:

- **Port :**

  The switch port number.

- **LACP Enabled :**

  Controls whether LACP is enabled on this switch port. LACP will form an aggregation when 2 or more ports are connected to the same partner.

- **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 :**

The Role shows the 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).

- **Timeout :**

  The Timeout controls the period between BPDU transmissions. Fast will transmit LACP packets each second, while Slow will wait for 30 seconds before sending a LACP packet.

- **Prio :**

  The Prio controls the priority of the port. If the LACP partner wants to form a larger group than is supported by this device then this parameter will control which ports will be active and which ports will be in a backup role. Lower number means greater priority.

Buttons

- **Apply :**

  Click to save changes.

- **Reset :**

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

2-7 Loop Protection

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

Web Interface

To configure the Loop Protection parameters in the web interface:

1. Click Configuration, Loop Protection.
2. Evoke to select enable or disable the port loop Protection.
3. Click the Apply 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.

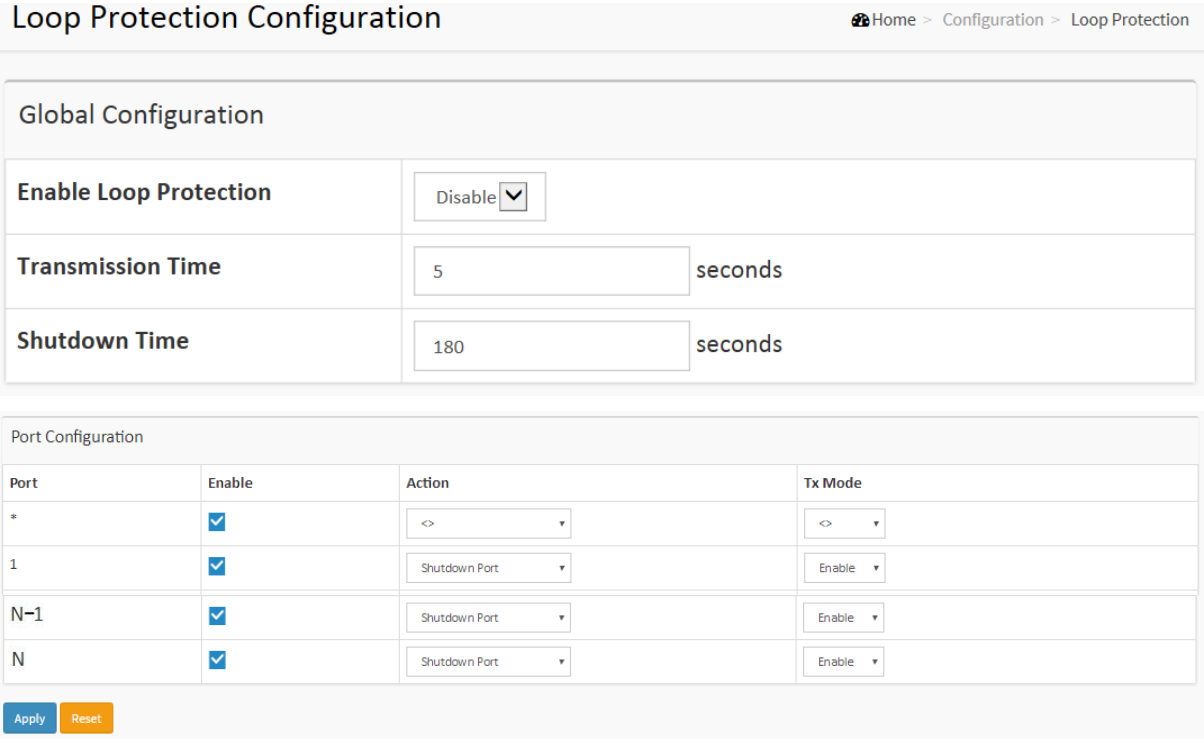


Figure 2-8: The Loop Protection Configuration

Parameter description:

General Settings

- **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 to 10 seconds.

- **Shutdown Time :**

The period (in seconds) for which a port will be kept disabled in the event of a loop is detected (and the port action 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 Configuration

- **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

- **Apply :**

  Click to save changes.

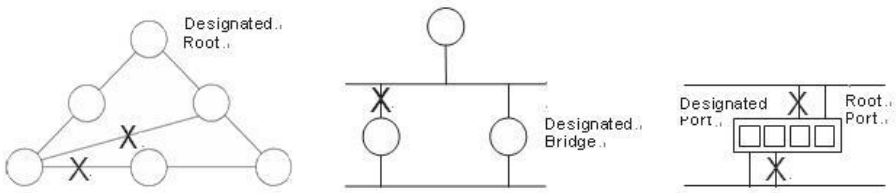
- **Reset :**

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

2-8 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 - 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.

2-8.1 Bridge Setting

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 instance in the switch.

Web Interface

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

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. Evoke to enable or disable the parameters and write down available value of parameters in blank field in Advanced settings.
4. Click the apply 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.

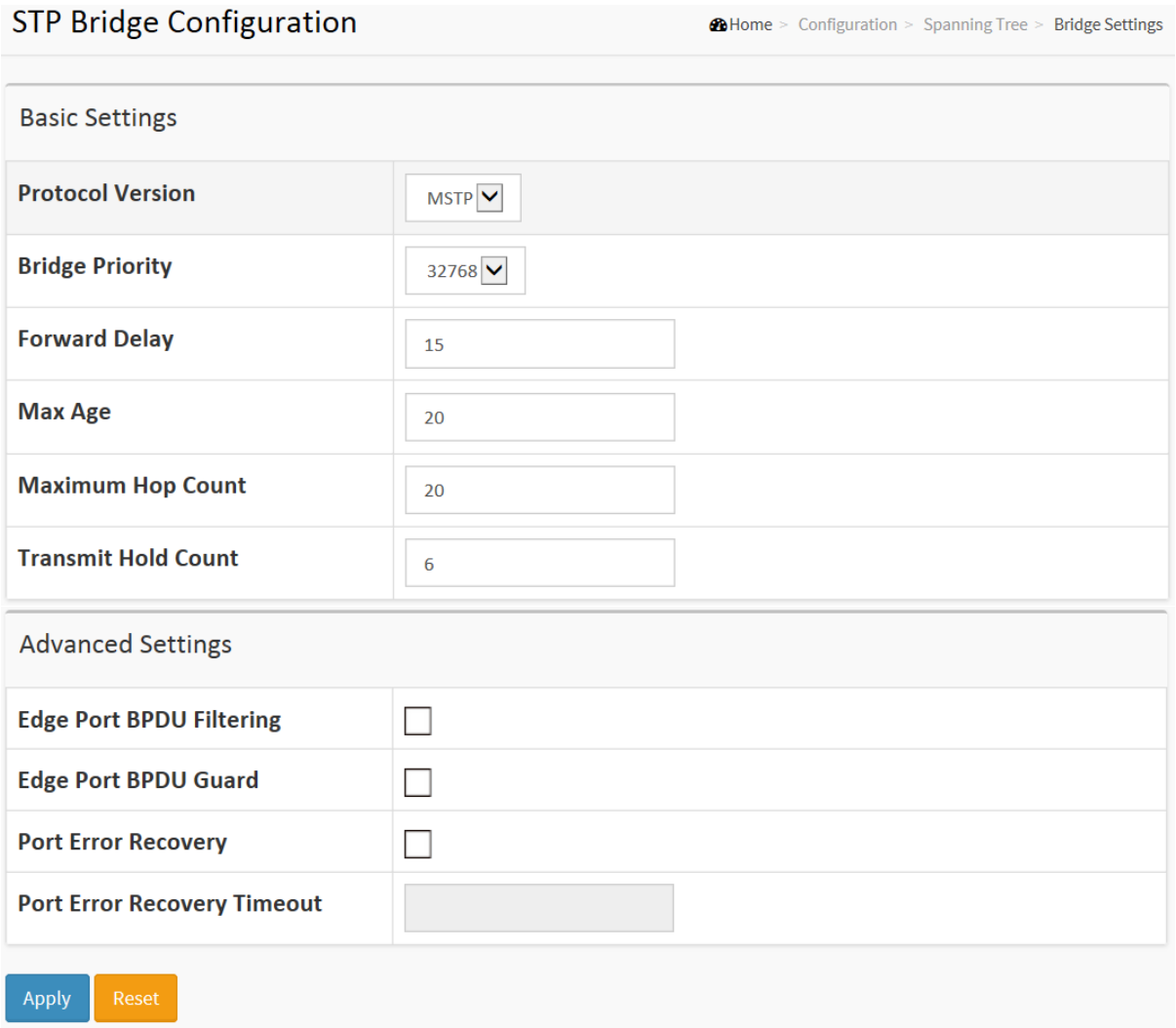


Figure 2-8.1: The STP Bridge Configuration

Parameter description:

Basic Settings

- **Protocol Version :**

  The MSTP / RSTP / STP protocol version setting. Valid values are STP, RSTP and MSTP.

- **Bridge Priority :**

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

- **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

- **Apply :**

  Click to save changes.

- **Reset :**

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

2-8.2 MSTI Mapping

When you implement a 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.

Web Interface

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

1. Click Configuration, Spanning Tree, MSTI Mapping.
2. Specify the configuration identification parameters in the field. Specify the VLANs Mapped blank field.
3. Click the Apply 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.

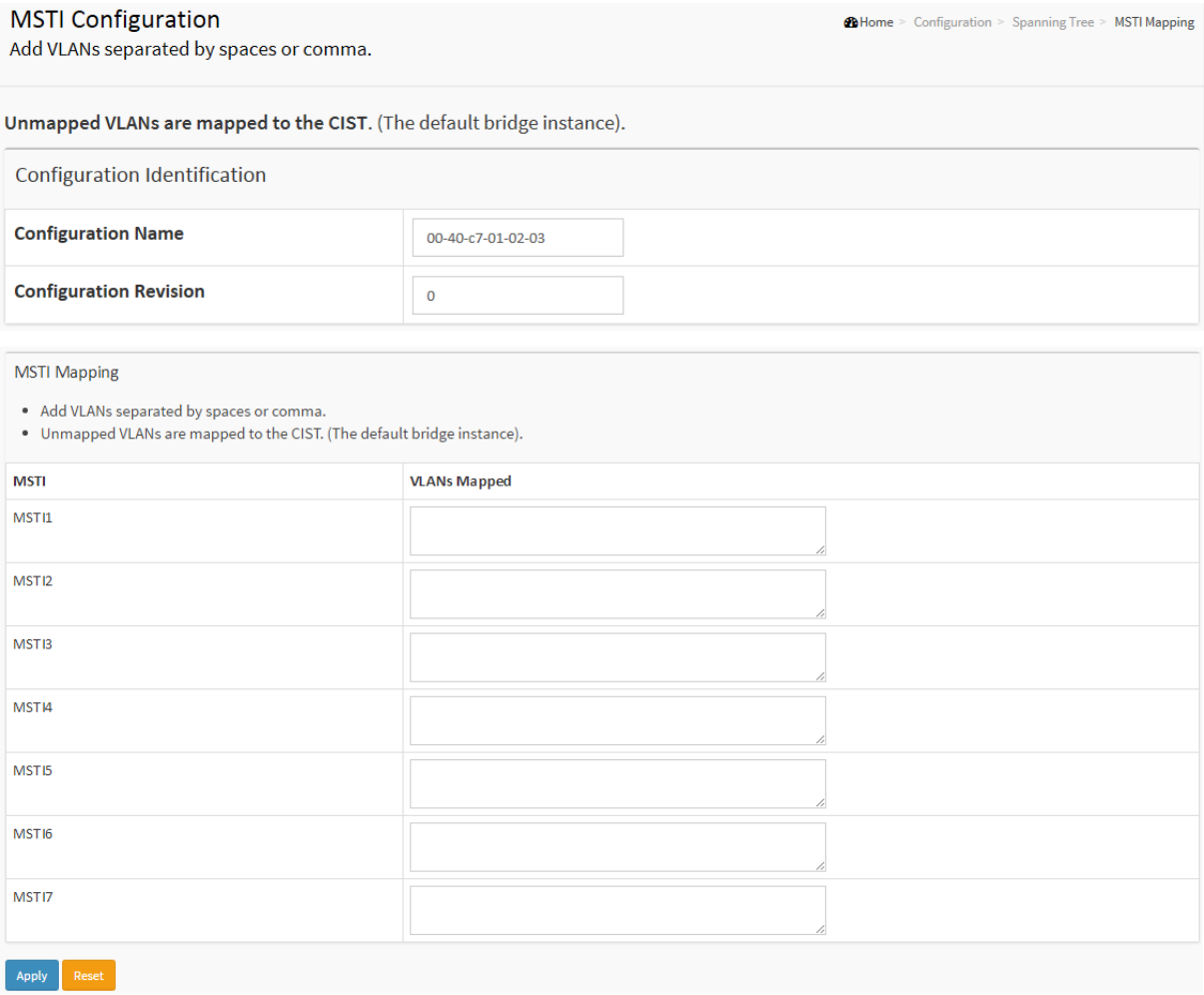


Figure 2-8.2: The MSTI Configuration

Parameter description:

Configuration Identification

- **Configuration Name :**

  The name identifying the VLAN to MSTI mapping. Bridges must share the name and revision (see below), as well as the VLAN-to-MSTI mapping configuration in order to share spanning trees for MSTI's (Intra-region). The name is at most 32 characters.

- **Configuration Revision :**

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

MSTI Mapping

- **MSTI :**

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

- **VLANs Mapped :**

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

Buttons

- **Apply :**

  Click to save changes.

- **Reset :**

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

2-8.3 MSTI Priorities

When you implement a 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

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

Web Interface

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

1. Click Configuration, Spanning Tree, MSTI Priorities.
2. Scroll the Priority.
3. Click the Apply 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.

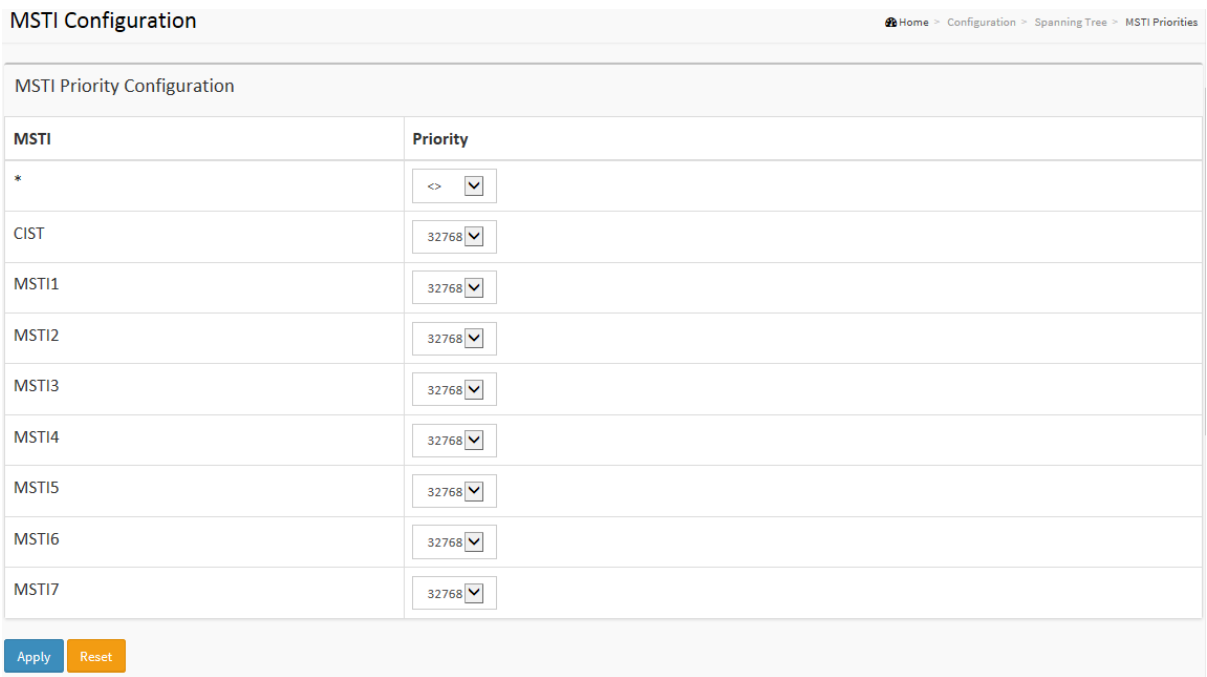


Figure 2-8.3: The MSTI Configuration

Parameter description:

- **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

- **Apply :**

  Click to save changes.

- **Reset :**

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

2-8.4 CIST Ports

When you implement a Spanning Tree protocol on the switch that the bridge instance. You need to configure the CIST Ports. The section describes it allows the user to inspect the current STP CIST port configurations, and possibly change them as well. This page contains settings for physical and aggregated ports.

Web Interface

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

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 apply 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.

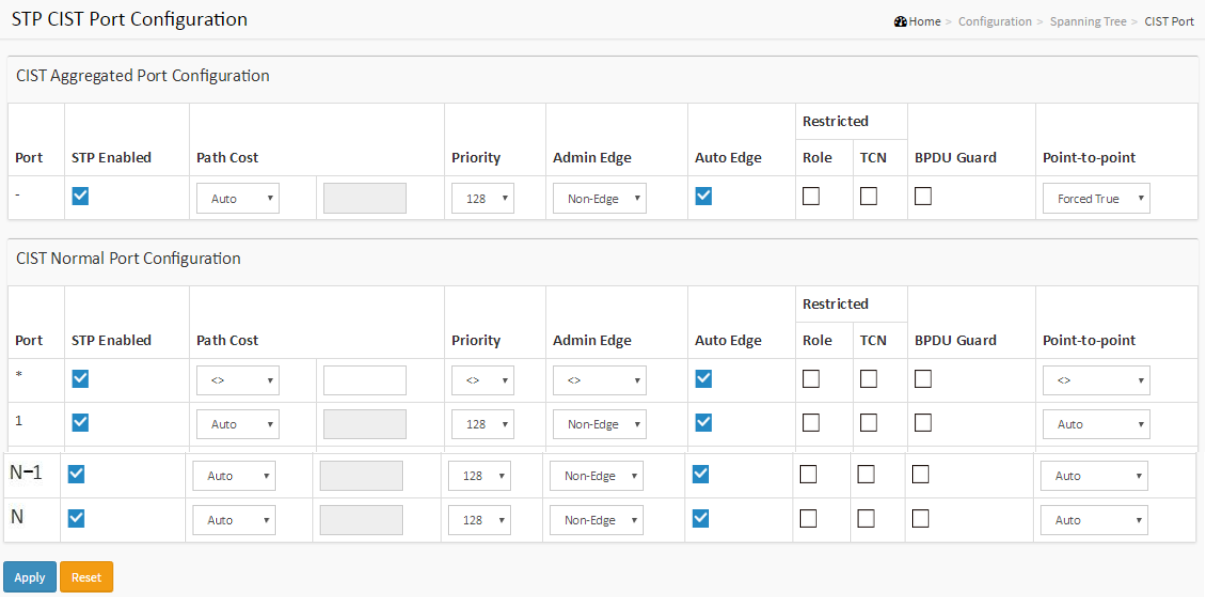


Figure 2-8.4: The STP CIST Port Configuration

Parameter description:

- **Port :**

  The switch port number of the logical STP port.

- **STP Enabled :**

  Controls whether STP is enabled on this switch port. This field will be read only if Voice VLAN feature is enabled. The Voice VLAN port mode will be read only if this field be Enabled.

- **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. Transition to the forwarding state is faster for point-to-point LANs than for shared media.

Buttons

- **Apply :**

  Click to save changes.

- **Reset :**

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

2-8.5 MSTI Ports

The section describes it allows the user to inspect the current STP MSTI port configurations, and possibly change them as well.

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

Web Interface

To configure the Spanning Tree MSTI Port Configuration parameters in the web interface:

1. Click Configuration, Spanning Tree, MSTI Ports
2. Scroll to select the MST1 or other MSTI Port
3. Click Get to set the detail parameters of the MSTI Ports.
4. Scroll to set all parameters of the MSTI Port configuration.
5. Click the save to save the setting
6. If you want to cancel the setting then you need to click the Reset button. It will revert to previously saved values

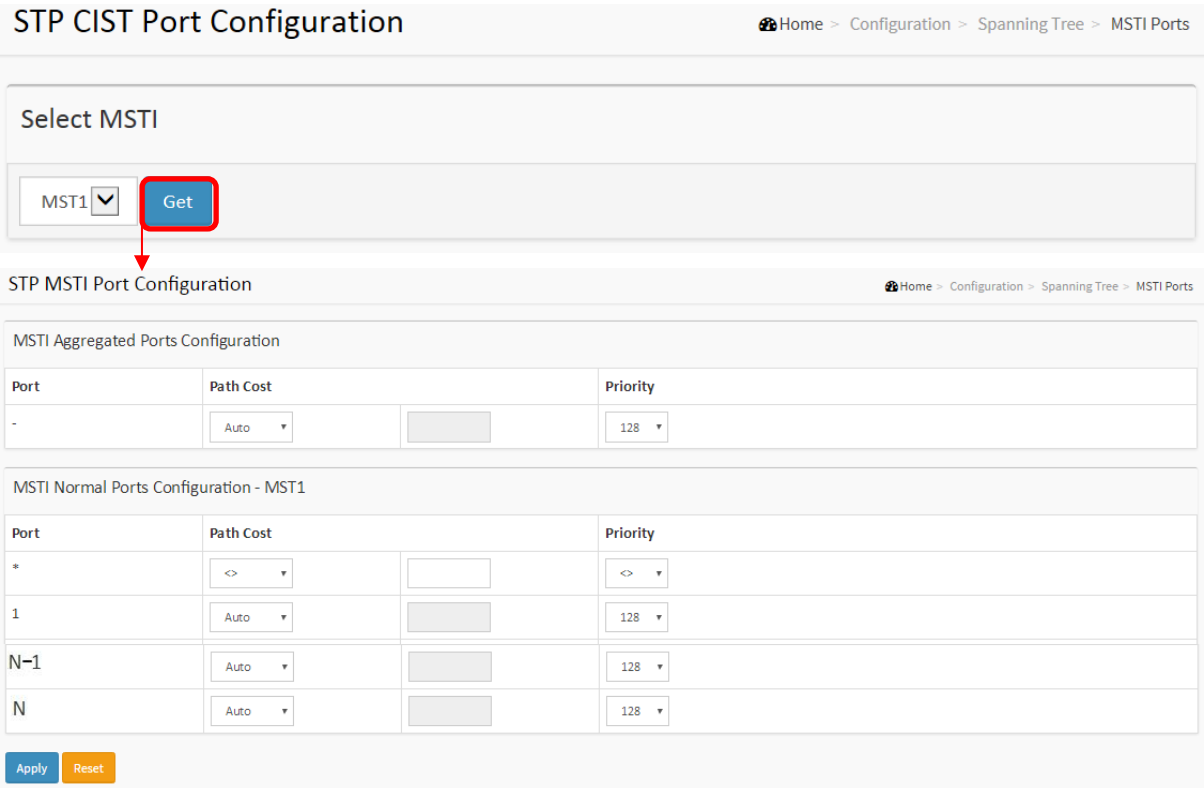


Figure 2-8.5: The MSTI Port Configuration

Parameter description:

- **Port :**

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

- **Path Cost :**

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

- **Priority :**

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

Buttons

- **Apply :**

  Click to save changes.

- **Reset :**

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

2-9 IPMC Profile

This page provides IPMC Profile related configurations.

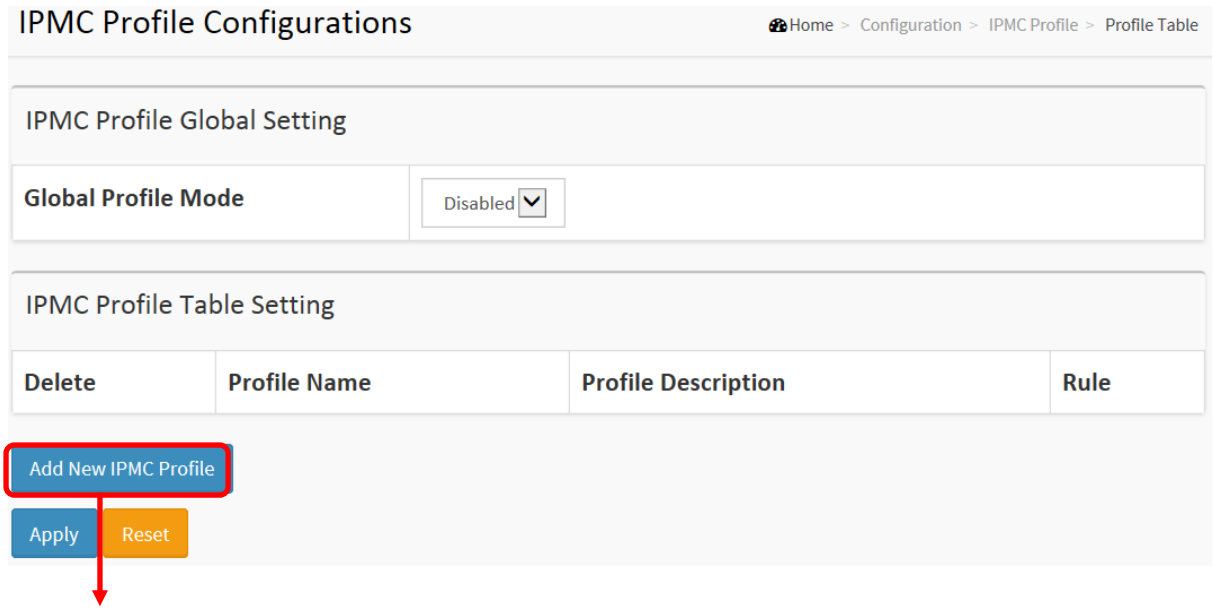
2-9.1 Profile Table

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

Web Interface

To configure the IPMC Profile Configuration in the web interface:

1. Click Configuration, IPMC Profile and Profile Table.
2. Select "Enabled" in the Mode of Global Profile Mode.
3. Click Add New IPMC Profile.
4. Specify the IPMC Profile Table Setting parameters in the field. Specify the Profile Name and Profile Description blank field.
5. Click Apply.
6. Click the button to specify IPMC Profile Rule Settings.
7. Click Add Last Rule and can manage the rules.



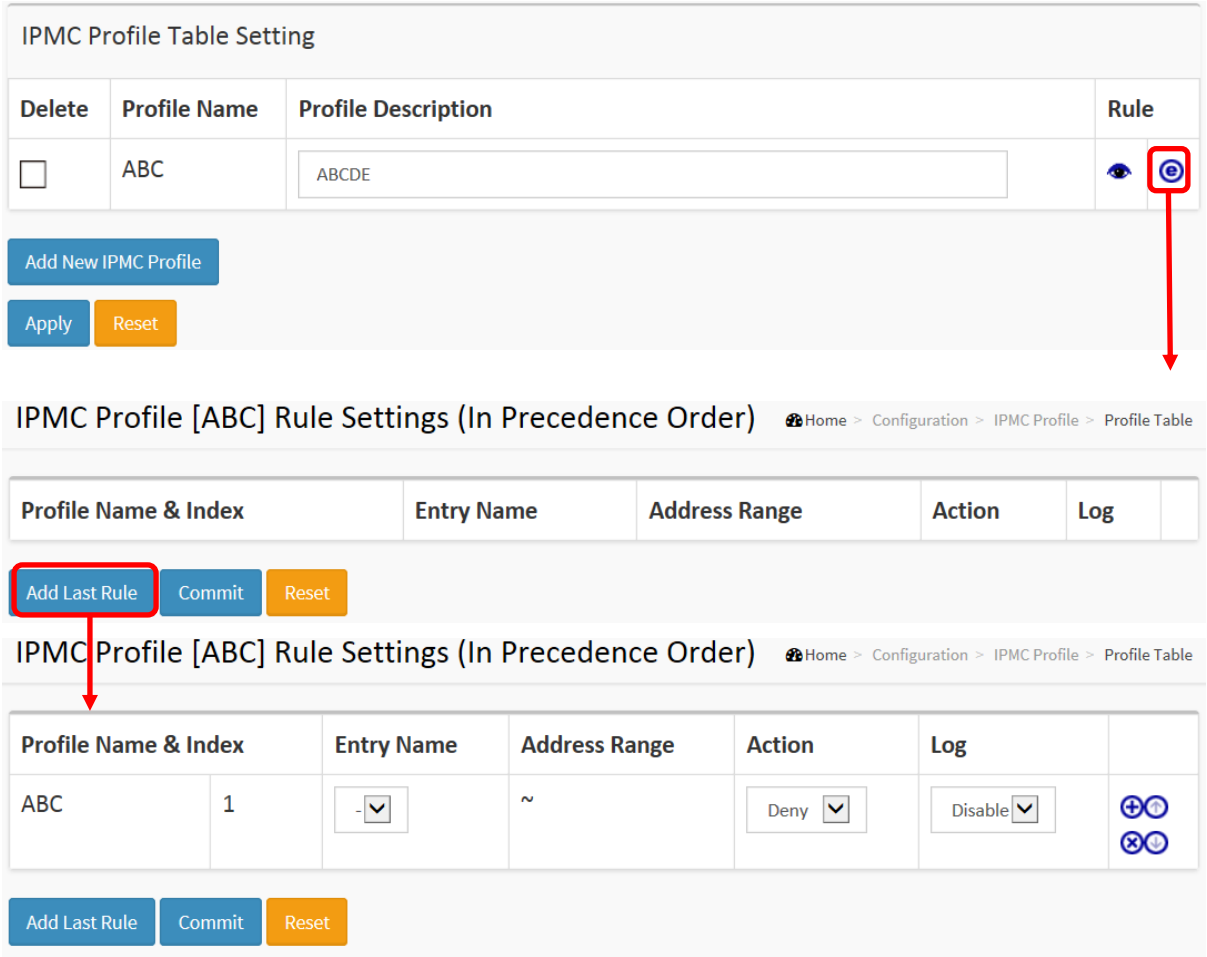


Figure 2-9.1: The IPMC Profile Configuration

Parameter description:

- **Global Profile Mode :**

  Enable/Disable the Global IPMC Profile.
  System starts to do filtering based on profile settings only when the global profile mode is enabled.

- **Delete :**

  Check to delete the entry.
  The designated entry will be deleted during the next save.

- **Profile Name :**

  The name used for indexing the profile table.

  Each entry has the unique name which is composed of at maximum 16 alphabetic and numeric characters. At least one alphabet must be present.

- **Profile Description :**

  Additional description, which is composed of at maximum 64 alphabetic and numeric characters, about the profile.

  No blank or space characters are permitted as part of description. Use "_" or "-" to separate the description sentence.

Buttons

- **Apply :**

Click to save changes.

- **Reset :**

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

- **Add New IPMC Profile :**

  Click to add new IPMC profile. Specify the name and configure the new entry. Click "Save".

- **Rule :**

  When the profile is created, click the edit button to enter the rule setting page of the designated profile. Summary about the designated profile will be shown by clicking the view button. You can manage or inspect the rules of the designated profile by using the following buttons:

  : List the rules associated with the designated profile.

  : Adjust the rules associated with the designated profile.

IPMC Profile Rule Settings Table

This page provides the filtering rule settings for a specific IPMC profile. It displays the configured rule entries in precedence order. First rule entry has highest priority in lookup, while the last rule entry has lowest priority in lookup.

- **Profile Name :**

  The name of the designated profile to be associated. This field is not editable.

- **Entry Name :**

  The name used in specifying the address range used for this rule.
  Only the existing profile address entries will be chosen in the selected box. This field is not allowed to be selected as none ("-") while the Rule Settings Table is committed.

- **Address Range :**

  The corresponding address range of the selected profile entry. This field is not editable and will be adjusted automatically according to the selected profile entry.

- **Action :**

  Indicates the learning action upon receiving the Join/Report frame that has the group address matches the address range of the rule.
  Permit: Group address matches the range specified in the rule will be learned.
  Deny: Group address matches the range specified in the rule will be dropped.

- **Log :**

  Indicates the logging preference upon receiving the Join/Report frame that has the group address matches the address range of the rule.
  Enable: Corresponding information of the group address, that matches the range specified in the rule, will be logged.
  Disable: Corresponding information of the group address, that matches the range specified in the rule, will not be logged.

Buttons

- **Add Last Rule**

  Click to add a new rule in the end of the specific profile's rule list. Specify the address entry and configure the new entry. Click "Commit"

- **Commit**

  Click to commit rule changes for the designated profile.

- **Reset**

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

- **Rule Management Buttons :**

  You can manage rules and the corresponding precedence order by using the following buttons:
  ⊕: Insert a new rule before the current entry of rule.
  ⊗: Delete the current entry of rule.
  ⬆: Moves the current entry of rule up in the list.
  ⬇: Moves the current entry of rule down in the list.

2-9.2 Address Entry

This page provides address range settings used in IPMC profile.

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

Web Interface

To configure the IPMC Profile Address Configuration in the web interface:

1. Click Configuration, IPMC Profile and Address Entry.
2. Click Add New Address (Range) Entry.
3. Specify the IPMC Profile Address Configuration parameters in the field. Specify the Entry Name and Start Address and End Address blank field.
4. Click Apply.

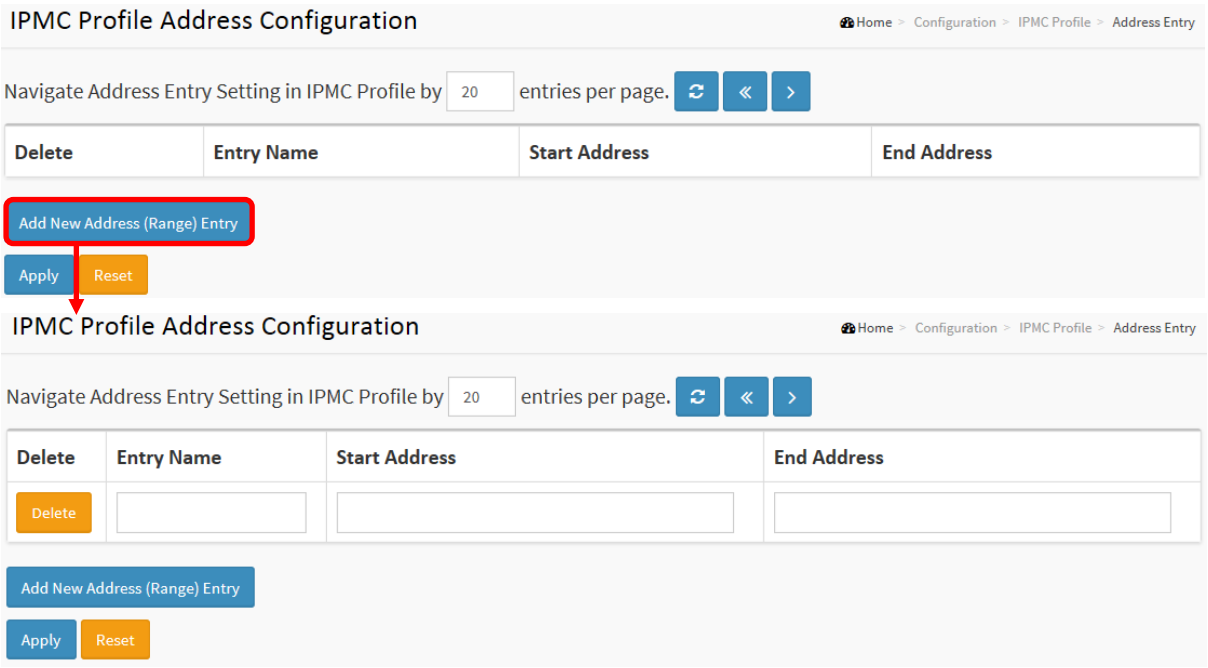


Figure 2-9.2: The IPMC Profile Address Configuration

Parameter description:

- **Entry Name :**

  The name used for indexing the address entry table.
  Each entry has the unique name which is composed of at maximun 16 alphabetic and numeric characters. At least one alphabet must be present.

- **Start Address :**

  The starting IPv4/IPv6 Multicast Group Address that will be used as an address range.

- **End Address :**

  The ending IPv4/IPv6 Multicast Group Address that will be used as an address range.

Buttons

- **Apply :**

  Click to save changes.

- **Reset :**

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

- **Delete :**

  Check to delete the entry.
  The designated entry will be deleted during the next save.

- **Add New Address (Range) Entry :**

  Click to add new address range. Specify the name and configure the addresses. Click "Save"

- **Refresh :**

  Refreshes the displayed table starting from the input fields.

- **< < :**

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

- **> > :**

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

2-10 MVR

The MVR feature enables multicast traffic forwarding on the Multicast VLANs.

In a multicast television application, a PC or a network television or a set-top box can receive the multicast stream. Multiple set-top boxes or PCs can be connected to one subscriber port, which is a switch port configured as an MVR receiver port. When a subscriber selects a channel, the set-top box or PC sends an IGMP/MLD report message to Switch A to join the appropriate multicast group address. Uplink ports that send and receive multicast data to and from the multicast VLAN are called MVR source ports.

It is allowed to create at maximum 4 MVR VLANs with corresponding channel profile for each Multicast VLAN.

The channel profile is defined by the IPMC Profile which provides the filtering conditions.

Web Interface

To configure the MVR Configuration in the web interface:

1. Click Configuration, MVR.
2. Scroll the MVR mode to enable or disable and Scroll to set all parameters.
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.

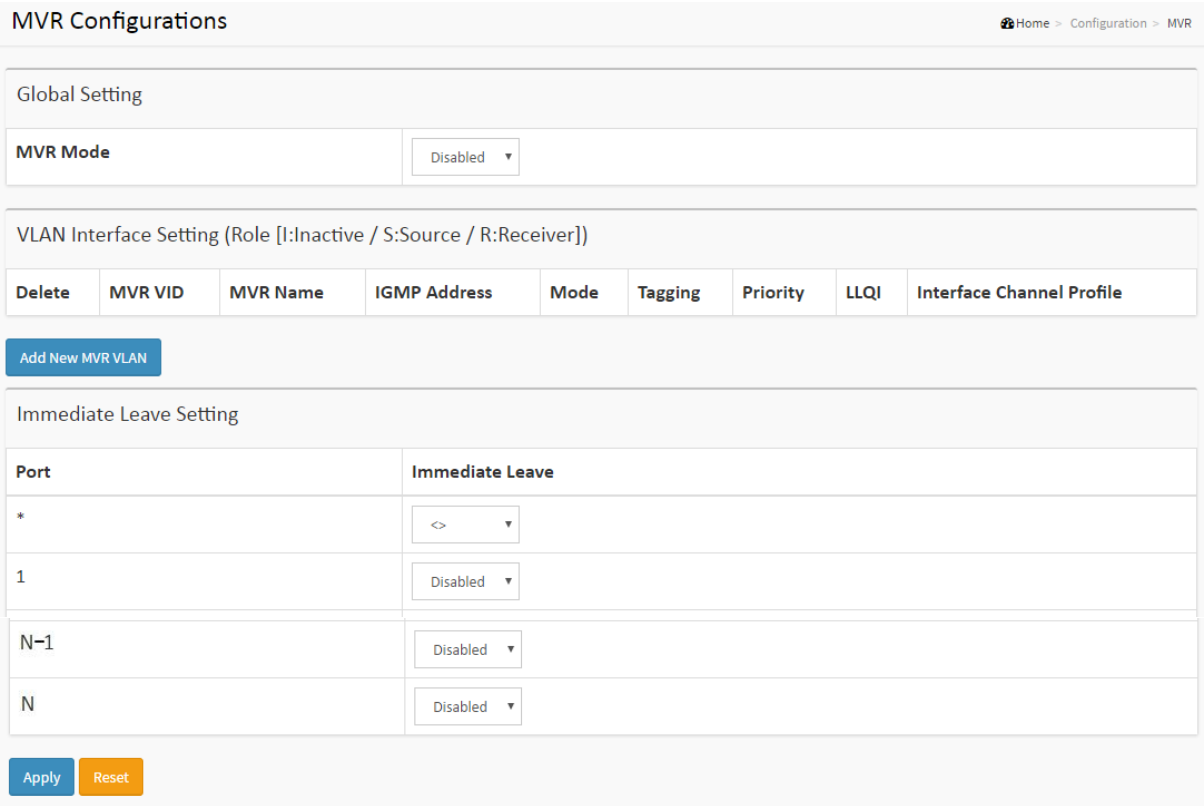


Figure 2-10: The MVR Configuration

Parameter description:

- **MVR Mode :**

  Enable/Disable the Global MVR.
  The Unregistered Flooding control depends on the current configuration in IGMP/MLD Snooping. It is suggested to enable Unregistered Flooding control when the MVR group table is full.

- **MVR VID :**

  Specify the Multicast VLAN ID.
  Be Caution: MVR source ports are not recommended to be overlapped with management VLAN ports.

- **MVR Name :**

  MVR Name is an optional attribute to indicate the name of the specific MVR VLAN. Maximum length of the MVR VLAN Name string is 32. MVR VLAN Name can only contain alphabets or numbers. When the optional MVR VLAN name is given, it should contain at least one alphabet. MVR VLAN name can be edited for the existing MVR VLAN entries or it can be added to the new entries.

- **IGMP Address :**

  Define the IPv4 address as source address used in IP header for IGMP control frames.

  The default IGMP address is not set (0.0.0.0).

  When the IGMP address is not set, system uses IPv4 management address of the IP interface associated with this VLAN.

  When the IPv4 management address is not set, system uses the first available IPv4 management address.

  Otherwise, system uses a pre-defined value. By default, this value will be 192.0.2.1.

- **Mode :**

  Specify the MVR mode of operation. In Dynamic mode, MVR allows dynamic MVR membership reports on source ports. In Compatible mode, MVR membership reports are forbidden on source ports. The default is Dynamic mode.

- **Tagging :**

  Specify whether the traversed IGMP/MLD control frames will be sent as Untagged or Tagged with MVR VID. The default is tagged.

- **Priority :**

  Specify how the traversed IGMP/MLD control frames will be sent in prioritized manner. The default Priority is 0.

- **LLQI :**

  Define the maximum time to wait for IGMP/MLD report memberships on a receiver port before removing the port from multicast group membership. The value is in units of tenths of a seconds. The range is from 0 to 31744. The default LLQI is 5 tenths or one-half second.

- **Interface Channel Setting :**

  When the MVR VLAN is created, click the Edit symbol to expand the corresponding multicast channel settings for the specific MVR VLAN. Summary about the Interface Channel Setting (of the MVR VLAN) will be shown besides the Edit symbol.

- **Profile Management Button :**

You can inspect the rules of the designated profile by using the following button:

Navigate: List the rules associated with the designated profile.

- **Port :**

  The logical port for the settings.

- **Port Role :**

  Configure an MVR port of the designated MVR VLAN as one of the following roles.

  Inactive: The designated port does not participate MVR operations.

  Source: Configure uplink ports that receive and send multicast data as source ports. Subscribers cannot be directly connected to source ports.

  Receiver: Configure a port as a receiver port if it is a subscriber port and should only receive multicast data. It does not receive data unless it becomes a member of the multicast group by issuing IGMP/MLD messages.

  Be Caution: MVR source ports are not recommended to be overlapped with management VLAN ports. Select the port role by clicking the Role symbol to switch the setting. I indicates Inactive; S indicates Source; R indicates Receiver. The default Role is Inactive.

- **Immediate Leave :**

  Enable the fast leave on the port.

Buttons

- **Apply :**

  Click to save changes.

- **Reset :**

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

- **Delete :**

  Check to delete the entry.
  The designated entry will be deleted during the next save.

- **Add New MVR VLAN :**

  Click to add new MVR VLAN. Specify the VID and configure the new entry. Click "Apply".

2-11 IPMC

2-11.1 IGMP Snooping

The 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 should be running IGMP.

It can support up to 1024 multicast groups.

2-11.1.1 Basic Configuration

This page provides IGMP Snooping related configuration.

Web Interface

To configure the IGMP Snooping Configuration in the web interface:

1. Click Configuration, IPMC, IGMP Snooping, Basic Configuration.
2. Evoke to select enable or disable the parameter in the Global Configuration and Port Related Configuration Mode.
3. Click the Apply 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.

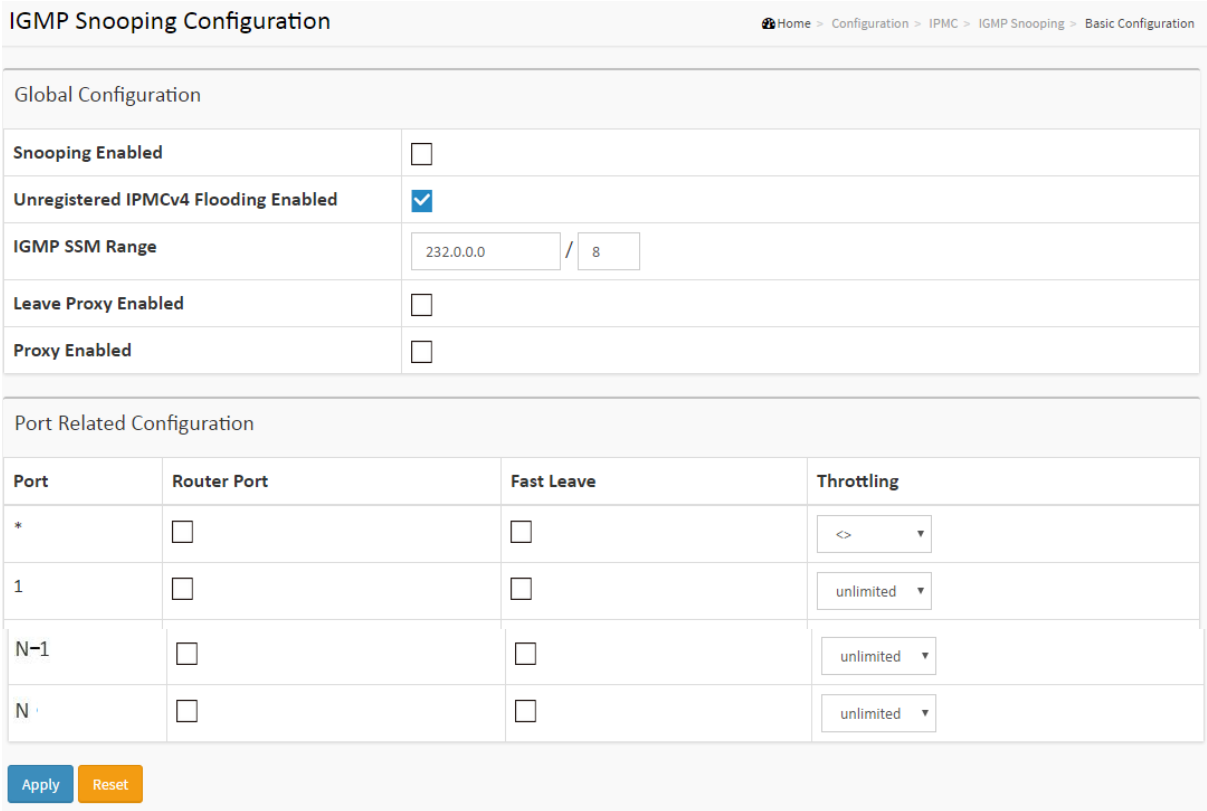


Figure 2-11.1.1: The IGMP Snooping Configuration.

Parameter description:

- **Snooping Enabled :**

  Enable the Global IGMP Snooping.

- **Unregistered IPMCv4 Flooding Enabled :**

  Enable unregistered IPMCv4 traffic flooding.

  The flooding control takes effect only when IGMP Snooping is enabled.

  When IGMP Snooping is disabled, unregistered IPMCv4 traffic flooding is always active in spite of this setting.

- **IGMP SSM Range :**

  SSM (Source-Specific Multicast) Range allows the SSM-aware hosts and routers run the SSM service model for the groups in the address range.

- **Leave Proxy Enabled :**

  Enable IGMP Leave Proxy. This feature can be used to avoid forwarding unnecessary leave messages to the router side.

- **Proxy Enabled :**

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

- **Router Port :**

  Specify which ports act as router ports. A router port is a port on the Ethernet switch that leads towards the Layer 3 multicast device or IGMP querier.

  If an aggregation member port is selected as a router port, the whole aggregation will act as

a router port.

- **Fast Leave :**

  Enable the fast leave on the port.

- **Throttling :**

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

Buttons

- **Apply :**

  Click to save changes.

- **Reset :**

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

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

Web Interface

To configure the IGMP Snooping VLAN Configuration in the web interface:

1. Click Configuration, IPMC, IGMP Snooping and VLAN Configuration.
2. Click Add New IGMP VLAN.
3. Evoke to select enable or disable Snooping, Querier Address. Specify the parameters in the blank field.
4. Click the refresh to update the data or click << or > to display previous entry or next entry.
5. Click the Apply to save the setting
6. If you want to cancel the setting then you need to click the Reset button. It will revert to previously saved values

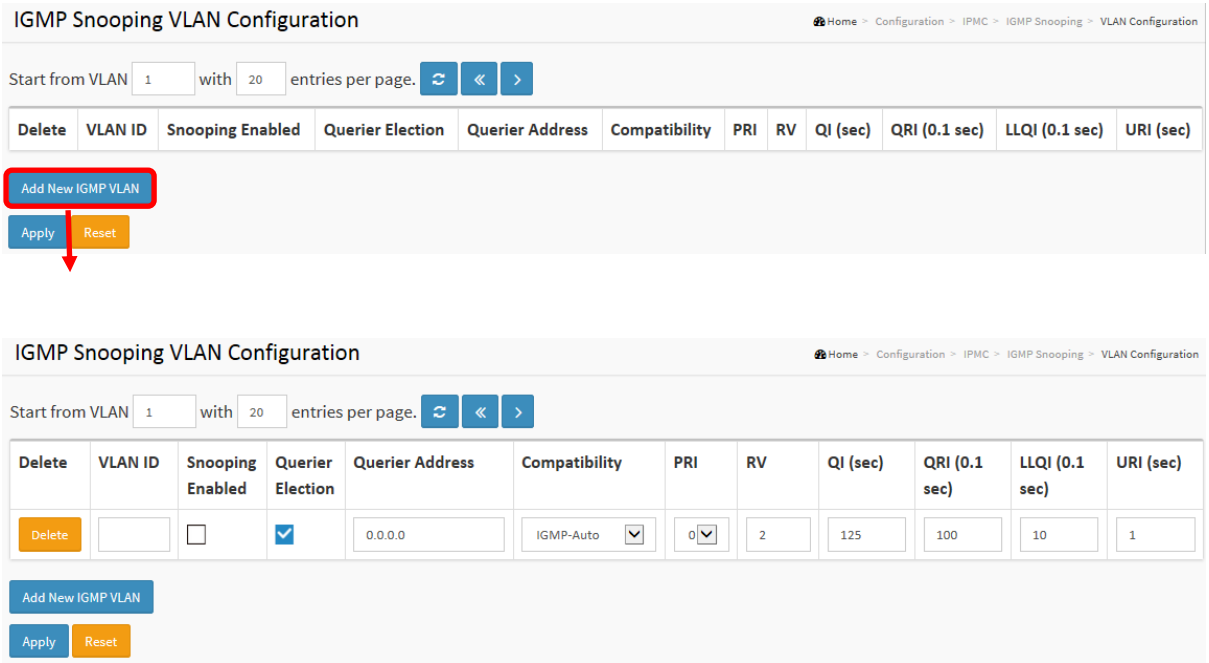


Figure 2-11.1.2: The IGMP Snooping VLAN Configuration.

Parameter description:

- **VLAN ID :**

  It displays the VLAN ID of the entry.

- **IGMP Snooping Enabled :**

Enable the per-VLAN IGMP Snooping. Only up to 32 VLANs can be selected. .

- **Querier Election :**

  Enable to join IGMP Querier election in the VLAN. Disable to act as an IGMP Non-Querier.

- **Querier Address :**

  Define the IPv4 address as source address used in IP header for IGMP Querier election.

  When the Querier address is not set, system uses IPv4 management address of the IP interface associated with this VLAN.

  When the IPv4 management address is not set, system uses the first available IPv4 management address.

  Otherwise, system uses a pre-defined value. By default, this value will be 192.0.2.1.

- **Compatibility :**

  Compatibility is maintained by hosts and routers taking appropriate actions depending on the versions of IGMP operating on hosts and routers within a network. The allowed selection is IGMP-Auto, Forced IGMPv1, Forced IGMPv2, Forced IGMPv3, default compatibility value is IGMP-Auto.

- **PRI :**

  Priority of Interface.

  It indicates the IGMP control frame priority level generated by the system. These values can be used to prioritize different classes of traffic.

  The allowed range is 0 (best effort) to 7 (highest), default interface priority value is 0.

- **RV :**

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

- **QI :**

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

- **QRI :**

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

- **LLQI (LMQI for IGMP) :**

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

- **URI :**

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

Buttons

- **Apply :**

  Click to save changes.

- **Reset :**

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

- **Delete :**

  Check to delete the entry. The designated entry will be deleted during the next save.

- **Add New IGMP VLAN :**

  Click to add new IGMP VLAN. Specify the VID and configure the new entry. Click "Apply". The specific IGMP VLAN starts working after the corresponding static VLAN is also created..

- **Refresh :**

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

- **<< :**

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

- **> :**

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

The section describes how to set the IGMP Port Group Filtering with the IGMP filtering feature, a user can exert this type of control. In some network Application environments, as like the metropolitan or multiple-dwelling unit (MDU) installations, a user might want to control the multicast groups to which a user on a switch port can belong. It allows the user to 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.

Web Interface

To configure the IGMP Snooping Port Filtering Profile Configuration in the web interface:

1. Click Configuration, IPMC, IGMP Snooping and Port Filtering Profile.
2. Scroll the Port to enable the Port Group Filtering. Specify the Filtering Groups in the blank field.
3. Click the apply 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.

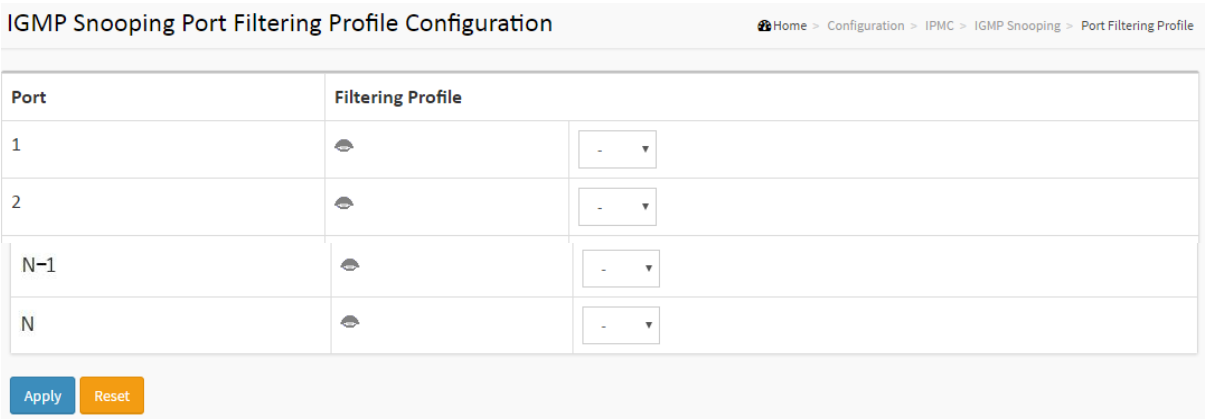


Figure 2-11.1.3: The IGMP Snooping Port Group Filtering Profile.

Parameter description:

- **Port :**

  The logical port for the settings.

- **Filtering Profile :**

Select the IPMC Profile as the filtering condition for the specific port. Summary about the designated profile will be shown by clicking the view button.

- **Profile Management Button :**

  You can inspect the rules of the designated profile by using the following button:

  : List the rules associated with the designated profile.

Buttons

- **Apply :**

  Click to save changes.

- **Reset :**

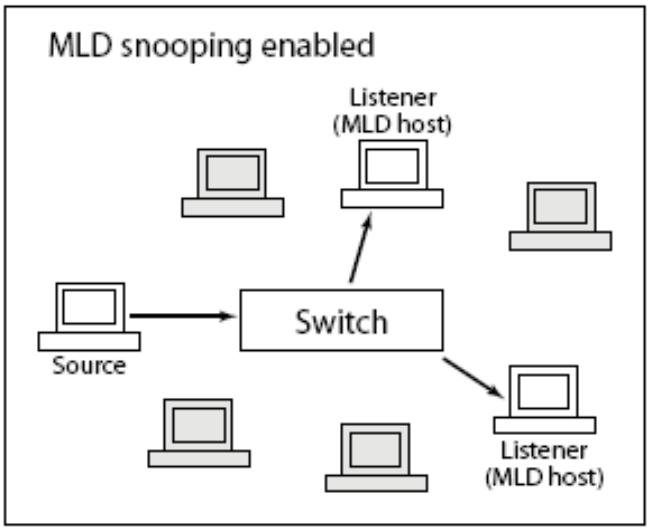
  Click to undo any changes made locally and revert to previously saved values.

2-11.2 MLD Snooping

Curiously enough, 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



2-11.2.1 Basic Configuration

The section will let you understand how to configure the MLD Snooping basic configuration and the parameters.

Web Interface

To configure the MLD Snooping Configuration in the web interface:

1. Click Configuration, IPMC, MLD Snooping and Basic Configuration.
2. Evoke to enable or disable the Global configuration parameters. Evoke the port to join Router port and Fast Leave.
3. Scroll to select the Throttling mode with unlimited or 1 to 10.
4. Click apply 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.

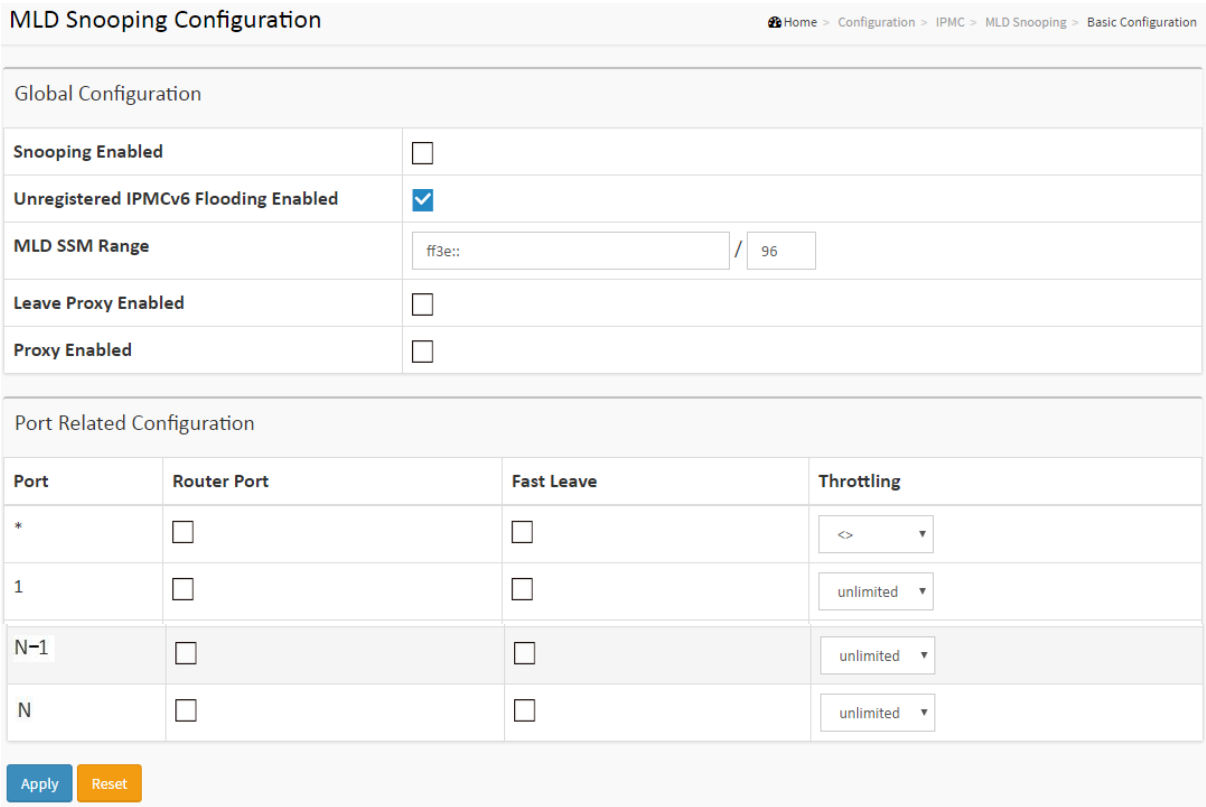


Figure 2-11.2.1: The MLD Snooping Configuration.

Parameter description:

- **Snooping Enabled :**

  Enable the Global MLD Snooping.

- **Unregistered IPMCv6 Flooding enabled :**

  Enable unregistered IPMCv6 traffic flooding.

  The flooding control takes effect only when MLD Snooping is enabled.

  When MLD Snooping is disabled, unregistered IPMCv6 traffic flooding is always active in spite of this setting.

- **MLD SSM Range :**

  SSM (Source-Specific Multicast) Range allows the SSM-aware hosts and routers run the SSM service model for the groups in the address (Using IPv6 Address) range.

- **Leave Proxy Enabled :**

  Enable MLD Leave Proxy. This feature can be used to avoid forwarding unnecessary leave messages to the router side.

- **Proxy Enabled :**

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

- **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

- **Apply :**

  Click to save changes.

- **Reset :**

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

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.

Web Interface

To configure the MLD Snooping VLAN Configuration in the web interface:

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

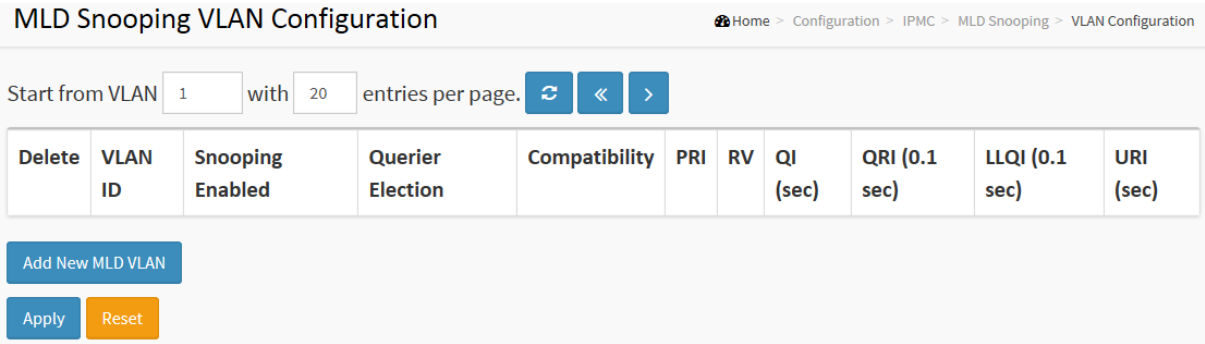


Figure 2-11.2.2: The MLD Snooping VLAN Configuration.

Parameter description:

- **VLAN ID :**

  It displays the VLAN ID of the entry.

- **MLD Snooping Enabled :**

  Enable the per-VLAN MLD Snooping. Up to 32 VLANs can be selected for MLD Snooping.

- **Querier Election :**

  Enable to join MLD Querier election in the VLAN. Disable to act as a MLD Non-Querier.

- **Compatibility :**

  Compatibility is maintained by hosts and routers taking appropriate actions depending on the versions of MLD operating on hosts and routers within a network.

  The allowed selection is MLD-Auto, Forced MLDv1, default compatibility value is MLD-Auto.

- **PRI :**

  Priority of Interface.

It indicates the MLD control frame priority level generated by the system. These values can be used to prioritize different classes of traffic.

The allowed range is 0 (best effort) to 7 (highest), default interface priority value is 0.

- **RV :**

  Robustness Variable.

  The Robustness Variable allows tuning for the expected packet loss on a link.

  The allowed range is 1 to 255, default robustness variable value is 2.

- **QI :**

  Query Interval.

  The Query Interval is the interval between General Queries sent by the Querier.

  The allowed range is 1 to 31744 seconds, default query interval is 125 seconds.

- **QRI :**

  Query Response Interval.

  The Maximum Response Delay used to calculate the Maximum Response Code inserted into the periodic General Queries.

  The allowed range is 0 to 31744 in tenths of seconds, default query response interval is 100 in tenths of seconds (10 seconds).

- **LLQI :**

  Last Listener Query Interval.

  The Last Listener Query Interval is the Maximum Response Delay used to calculate the Maximum Response Code inserted into Multicast Address Specific Queries sent in response to Version 1 Multicast Listener Done messages. It is also the Maximum Response Delay used to calculate the Maximum Response Code inserted into Multicast Address and Source Specific Query messages.

  The allowed range is 0 to 31744 in tenths of seconds, default last listener query interval is 10 in tenths of seconds (1 second).

- **URI :**

  Unsolicited Report Interval.

  The Unsolicited Report Interval is the time between repetitions of a node's initial report of interest in a multicast address.

  The allowed range is 0 to 31744 seconds, default unsolicited report interval is 1 second.

Buttons

- **Apply :**

  Click to save changes.

- **Reset :**

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

- **Delete :**

  Check to delete the entry. The designated entry will be deleted during the next save.

- **Add New MLD VLAN :**

  Click to add new MLD VLAN. Specify the VID and configure the new entry. Click "Apply". The

specific MLD VLAN starts working after the corresponding static VLAN is also created.

- **Refresh :**

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

- **<< :**

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

- **> :**

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

The section describes that you could to set the Port Group Filtering in the MLD Snooping function. On the UI that you could add new filtering group and safety policy.

Web Interface

To configure the Port Filtering Profile in the web interface:

1. Click Configuration, IPMC, MLD Snooping and Port Filtering Profile.
2. Scroll the Port to enable the Port Group Filtering. Specify the Filtering Groups in the blank field.
3. Click the Apply 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.

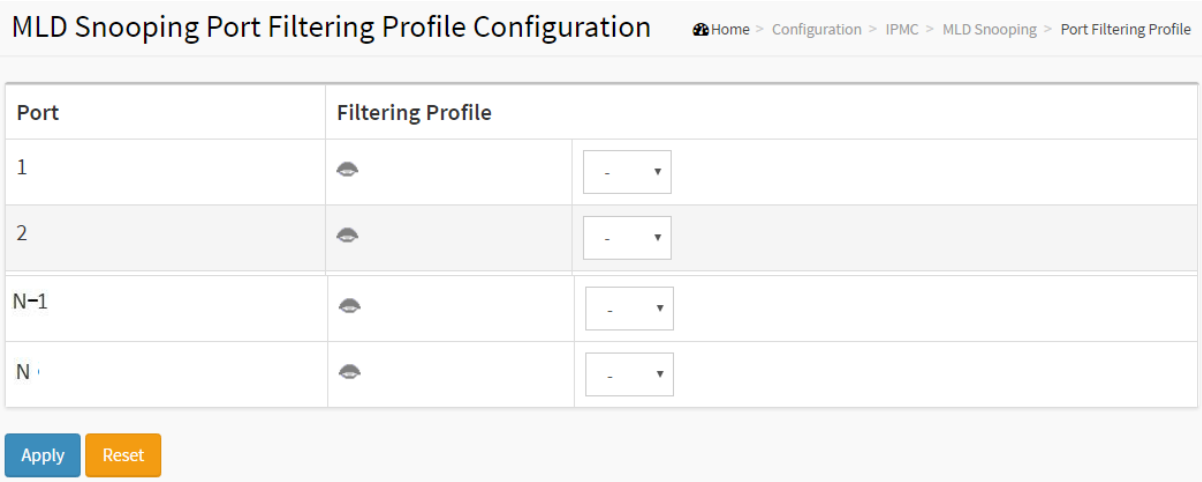


Figure 2-11.2.3: The MLD Snooping Port Group Filtering Configuration

Parameter description:

- **Port :**

  The logical port for the settings.

- **Filtering Profile :**

  Select the IPMC Profile as the filtering condition for the specific port. Summary about the designated profile will be shown by clicking the view button.

Buttons

- **Apply :**

  Click to save changes.

- **Reset :**

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

- **Profile Management Button :**

  You can inspect the rules of the designated profile by using the following button:

: List the rules associated with the designated profile.

2-12 LLDP

The switch supports the LLDP. For current information on your switch model, The Link Layer Discovery Protocol (LLDP) provides a standards-based method for enabling switches to advertise themselves to adjacent devices and to learn about adjacent LLDP devices. The Link Layer Discovery Protocol (LLDP) is a vendor-neutral Link Layer protocol in the Internet Protocol Suite used by network devices for advertising their identity, capabilities, and neighbors on a IEEE 802 local area network, principally wired Ethernet. The protocol is formally referred to by the IEEE as Station and Media Access Control Connectivity Discovery specified in standards document IEEE 802.1AB.

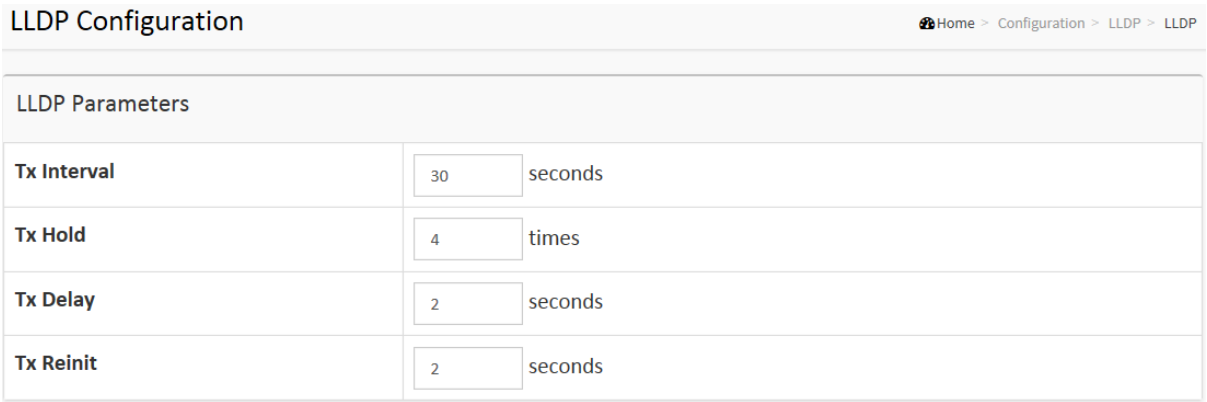
2-12.1 LLDP

You can per port to do the LLDP configuration and the detail parameters, the settings will take effect immediately. This page allows the user to inspect and configure the current LLDP port settings.

Web Interface

To configure the LLDP in the web interface:

1. Click Configuration, LLDP and LLDP.
2. Modify LLDP 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 the Apply to save the setting.
6. If you want to cancel the setting then you need to click the Reset button. It will revert to previously saved values.



LLDP Port Configuration

			Optional TLVs				
Port	Mode	CDP aware	Port Descr	Sys Name	Sys Descr	Sys Capa	Mgmt Addr
*	<>	☐	☑	☑	☑	☑	☑
1	Enabled	☐	☑	☑	☑	☑	☑
N-1	Enabled	☐	☑	☑	☑	☑	☑
N	Enabled	☐	☑	☑	☑	☑	☑

Apply Reset

Figure 2-12.1: The LLDP Configuration

Parameter description:

LLDP Parameters

- **Tx Interval :**

  The switch periodically transmits LLDP frames to its neighbours for having the network discovery information up-to-date. The interval between each LLDP frame is determined by the Tx Interval value. Valid values are restricted to 5 - 32768 seconds.

- **Tx Hold :**

  Each LLDP frame contains information about how long the information in the LLDP frame shall be considered valid. The LLDP information valid period is set to Tx Hold multiplied by Tx Interval seconds. Valid values are restricted to 2 - 10 times.

- **Tx Delay :**

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

- **Tx Reinit :**

  When a port is disabled, 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

- **Apply :**

  Click to save changes.

- **Reset :**

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

2-12.2 LLDP-MED

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.

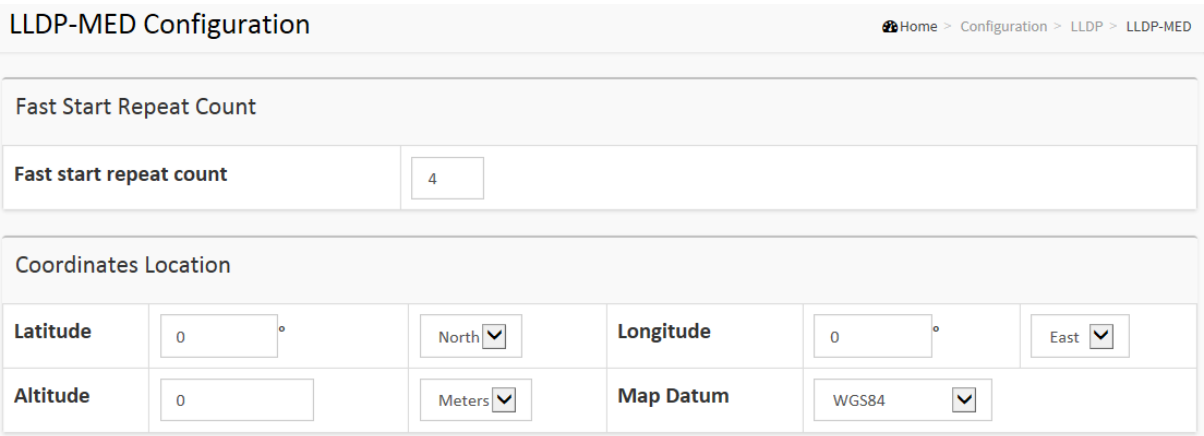
Inventory management, allowing network administrators to track their network devices, and determine their characteristics (manufacturer, software and hardware versions, and serial or asset number).

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

Web Interface

To configure the LLDP-MED in the web interface:

1. Click Configuration, LLDP and LLDP-MED Configuration.
2. Modify Fast start repeat count parameter, default is 4
3. Modify Coordinates Location parameters
4. Fill Civic Address Location parameters
5. Add new policy
6. Click Apply, will show following Policy Port Configuration
7. Select Policy ID for each port
8. Click the Apply to save the setting.
9. If you want to cancel the setting then you need to click the Reset button. It will revert to previously saved values.



Civic Address Location

Country code		State		County	
City		City district		Block (Neighborhood)	
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

Delete	Policy ID	Application Type	Tag	VLAN ID	L2 Priority	DSCP
No entries present						

Add New Policy

Apply Reset

Figure 2-12.2: The LLDP-MED Configuration

Parameter description:

Fast start repeat count

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

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

Because there is a risk of an LLDP frame being lost during transmission between neighbors, it is recommended to repeat the fast start transmission multiple times to increase the

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

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

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, and 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 / Signalling (conditionally support a separate network policy for the media types above)

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

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

- **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 Signalling (conditional) - for use in network topologies that require a different policy for the voice signalling than for the voice media. This application type should not be advertised if all the same network policies apply as those advertised in the Voice application policy.

  3. Guest Voice - 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 Signalling (conditional) - for use in network topologies that require a different policy for the guest voice signalling than for the guest voice media. This application type should not be advertised if all the same network policies apply as those advertised in the Guest Voice application policy.

  5. Softphone Voice - 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 Signalling (conditional) - for use in network topologies that require a separate policy for the video signalling than for the video media. This application type should not be advertised if all the same network policies apply as those advertised in the Video Conferencing application policy.

- **Tag :**

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

  Untagged 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 behaviour for the specified application type as defined in IETF RFC 2474. DSCP may contain one of 64 code point values (0 through 63). A value of 0 represents use of the default DSCP value as defined in RFC 2475.

- **Adding a new policy :**

  Click to add a new policy. Specify the Application type, Tag, VLAN ID, L2 Priority and DSCP for the new policy. 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 check marking the checkboxes that corresponds to the policies.

Buttons

- **Apply :**

  Click to save changes.

- **Reset :**

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

- **Delete**

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

2-14 MAC Table

Switching of frames is based upon the DMAC address contained in the frame. The switch builds up a table that maps MAC addresses to switch ports for knowing which ports the frames should go to (based upon the DMAC address in the frame). This table contains both static and dynamic entries. The static entries are configured by the network administrator if the administrator wants to do a fixed mapping between the DMAC address and switch ports.
The frames also contain a MAC address (SMAC address), which shows the MAC address of the equipment sending the frame. The SMAC address is used by the switch to automatically update the MAC table with these dynamic MAC addresses. Dynamic entries are removed from the MAC table if no frame with the corresponding SMAC address have been seen after a configurable age time

Web Interface

To configure MAC Address Table in the web interface:

Aging Configuration

1. Click configuration and MAC Table.
2. Specify the Disable Automatic Aging and Aging Time.
3. Click the Apply 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.

MAC Table Learning

1. Click configuration and MAC Table.
2. Specify the Port Members (Auto, Disable, Secure).
3. Click the Apply 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.

Static MAC Table Configuration

1. Click configuration, MAC Table and Add new Static entry.
2. Specify the VLAN IP and Mac address, Port Members.
3. Click the Apply 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.

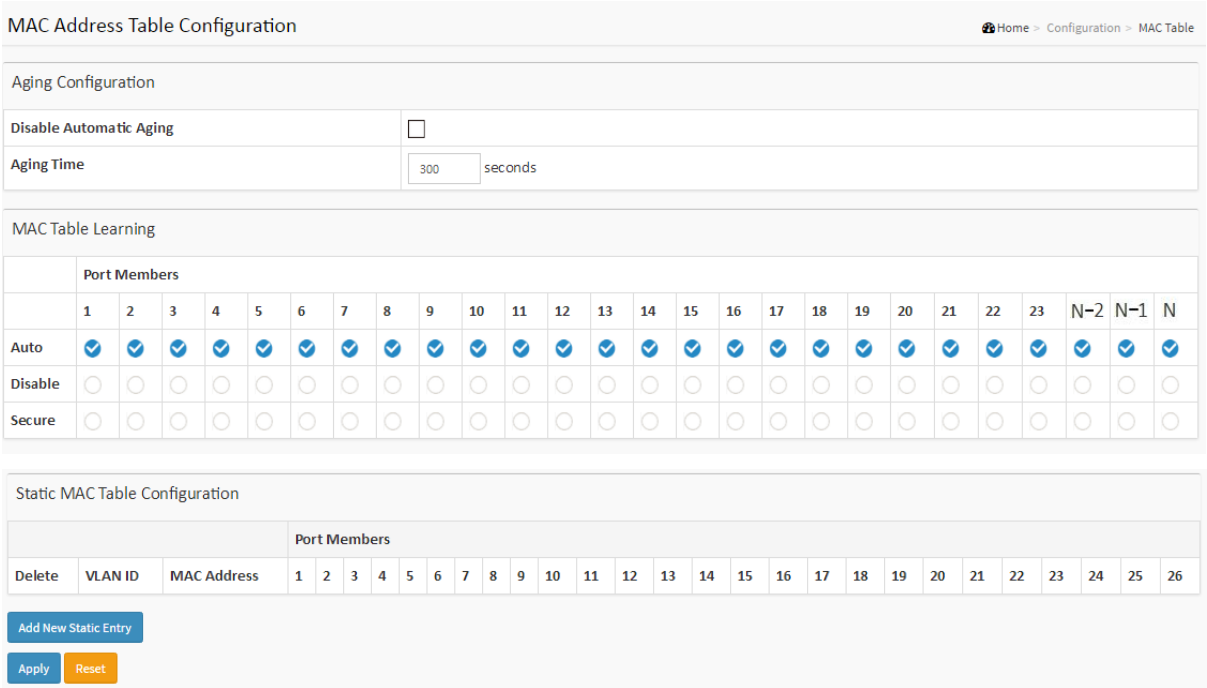


Figure 2-14: The MAC Address Table Configuration

Parameter description:

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 64 entries. The maximum of 64 entries is for the whole stack, and not per switch.

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

- **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.

Buttons

- **Adding a New Static Entry :**

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

- **Apply :**

  Click to save changes.

- **Reset :**

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

- **Delete :**

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

2-15 VLANs

To assign a specific VLAN for management purpose. The management VLAN is used to establish an IP connection to the switch from a workstation connected to a port in the VLAN. This connection supports a VSM, SNMP, and Telnet session. By default, the active management VLAN is VLAN 1, but you can designate any VLAN as the management VLAN using the Management VLAN window. Only one management VLAN can be active at a time.

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

Web Interface

To configure VLAN membership configuration in the web interface:

1. Click Configuration and VLANS.
2. Modify Global VLAN Configuration parameter.
3. Scroll the Mode, Port VLAN and Port Type to enable the Port VLAN Configuration parameter.
4. Click the Apply 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.

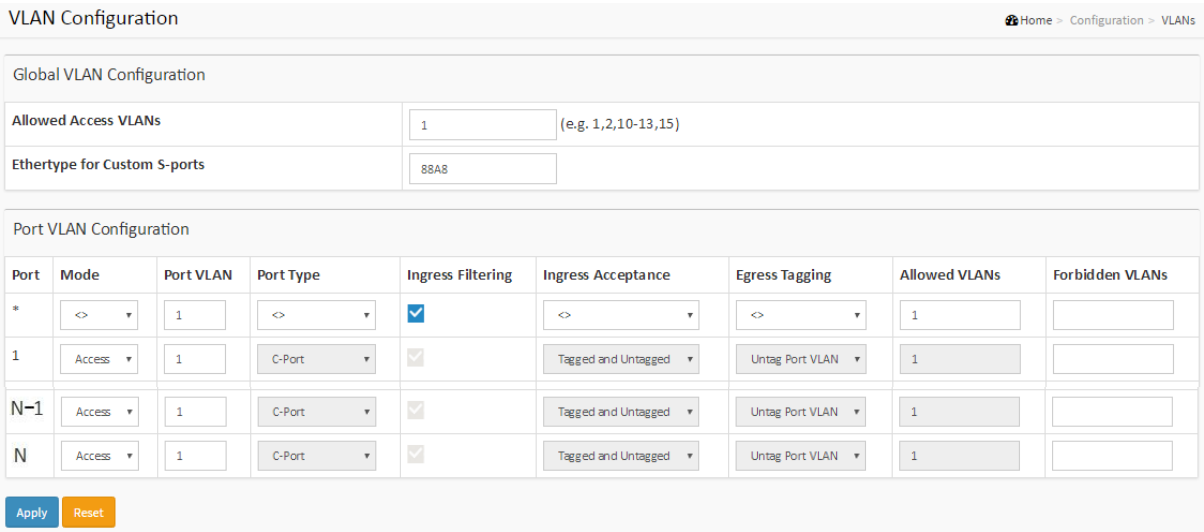


Figure 2-15.1: The VLAN Configuration

Parameter description:

Global VLAN Configuration

- **Allowed Access VLANs :**

  This field shows the allowed Access VLANs, i.e. it only affects ports configured as Access ports. Ports in other modes are members of all VLANs specified in the Allowed VLANs field. By default, only VLAN 1 is enabled. More VLANs may be created by using a list syntax where

the individual elements are separated by commas. Ranges are specified with a dash separating the lower and upper bound.

The following example will create VLANs 1, 10, 11, 12, 13, 200, and 300: 1,10-13,200,300. Spaces are allowed in between the delimiters.

- **Ethertype for Custom S-ports :**

  This field specifies the ethertype/TPID (specified in hexadecimal) used for Custom S-ports. The setting is in force for all ports whose Port Type is set to S-Custom-Port.

Port VLAN Configuration

- **Port :**

  This is the logical port number of this row.

- **Mode :**

  The port mode (default is Access) determines the fundamental behavior of the port in question. A port can be in one of three modes as described below.
  Whenever a particular mode is selected, the remaining fields in that row will be either grayed out or made changeable depending on the mode in question.
  Grayed out fields show the value that the port will get when the mode is applied.
  Access:
  Access ports are normally used to connect to end stations. Dynamic features like Voice VLAN may add the port to more VLANs behind the scenes. Access ports have the following characteristics:
  • Member of exactly one VLAN, the Port VLAN (a.k.a. Access VLAN), which by default is 1,
  • accepts untagged frames and C-tagged frames,
  • discards all frames that are not classified to the Access VLAN,
  • on egress all frames are transmitted untagged.
  Trunk:
  Trunk ports can carry traffic on multiple VLANs simultaneously, and are normally used to connect to other switches. Trunk ports have the following characteristics:
  • By default, a trunk port is member of all existing VLANs. This may be limited by the use of Allowed VLANs,
  • unless VLAN Trunking is enabled on the port, frames classified to a VLAN that the port is not a member of will be discarded,
  • by default, all frames but frames classified to the Port VLAN (a.k.a. Native VLAN) get tagged on egress. Frames classified to the Port VLAN do not get C-tagged on egress,
  • egress tagging can be changed to tag all frames, in which case only tagged frames are accepted on ingress,
  • VLAN trunking may be enabled.
  Hybrid:
  Hybrid ports resemble trunk ports in many ways, but adds additional port configuration features. In addition to the characteristics described for trunk ports, hybrid ports have these abilities:
  • Can be configured to be VLAN tag unaware, C-tag aware, S-tag aware, or S-custom-tag aware,
  • ingress filtering can be controlled,
  • ingress acceptance of frames and configuration of egress tagging can be configured independently.

- **Port VLAN :**

  Determines the port's VLAN ID (a.k.a. PVID). Allowed VLANs are in the range 1 through 4095, default being 1.
  On ingress, frames get classified to the Port VLAN if the port is configured as VLAN unaware,

the frame is untagged, or VLAN awareness is enabled on the port, but the frame is priority tagged (VLAN ID = 0).
On egress, frames classified to the Port VLAN do not get tagged if Egress Tagging configuration is set to untag Port VLAN.
The Port VLAN is called an "Access VLAN" for ports in Access mode and Native VLAN for ports in Trunk or Hybrid mode.

- **Port Type :**

  Ports in hybrid mode allow for changing the port type, that is, whether a frame's VLAN tag is used to classify the frame on ingress to a particular VLAN, and if so, which TPID it reacts on. Likewise, on egress, the Port Type determines the TPID of the tag, if a tag is required.
  Unaware:
  On ingress, all frames, whether carrying a VLAN tag or not, get classified to the Port VLAN, and possible tags are not removed on egress.
  C-Port:
  On ingress, frames with a VLAN tag with TPID = 0x8100 get classified to the VLAN ID embedded in the tag. If a frame is untagged or priority tagged, the frame gets classified to the Port VLAN. If frames must be tagged on egress, they will be tagged with a C-tag.
  S-Port:
  On ingress, frames with a VLAN tag with TPID = 0x8100 or 0x88A8 get classified to the VLAN ID embedded in the tag. If a frame is untagged or priority tagged, the frame gets classified to the Port VLAN. If frames must be tagged on egress, they will be tagged with an S-tag.
  S-Custom-Port:
  On ingress, frames with a VLAN tag with a TPID = 0x8100 or equal to the Ethertype configured for Custom-S ports get classified to the VLAN ID embedded in the tag. If a frame is untagged or priority tagged, the frame gets classified to the Port VLAN. If frames must be tagged on egress, they will be tagged with the custom S-tag.

- **Ingress Filtering :**

  Hybrid ports allow for changing ingress filtering. Access and Trunk ports always have ingress filtering enabled.
  If ingress filtering is enabled (checkbox is checked), frames classified to a VLAN that the port is not a member of get discarded.
  If ingress filtering is disabled, frames classified to a VLAN that the port is not a member of are accepted and forwarded to the switch engine. However, the port will never transmit frames classified to VLANs that it is not a member of.

- **VLAN Trunking :**

  Trunk and Hybrid ports allow for enabling VLAN trunking.
  When VLAN trunking is enabled, frames classified to unknown VLANs are accepted on the port whether ingress filtering is enabled or not.
  This is useful in scenarios where a cloud of intermediary switches must bridge VLANs that haven't been created. By configuring the ports that connect the cloud of switches as trunking ports, they can seemlessly carry those VLANs from one end to the other.

- **Ingress Acceptance :**

  Hybrid ports allow for changing the type of frames that are accepted on ingress.
  Tagged and untagged
  both tagged and untagged frames are accepted.
  Tagged Only
  Only tagged frames are accepted on ingress. Untagged frames are discarded.
  Untagged Only
  Only untagged frames are accepted on ingress. Tagged frames are discarded.

- **Egress Tagging :**

  Ports in Trunk and Hybrid mode may control the tagging of frames on egress.
  Untag Port VLAN
  Frames classified to the Port VLAN are transmitted untagged. Other frames are transmitted with the relevant tag.
  Tag All
  All frames, whether classified to the Port VLAN or not, are transmitted with a tag.
  Untag All
  All frames, whether classified to the Port VLAN or not, are transmitted without a tag.
  This option is only available for ports in Hybrid mode.

- **Allowed VLANs :**

  Ports in Trunk and Hybrid mode may control which VLANs they are allowed to become members of. Access ports can only be member of one VLAN, the Access VLAN.
  The field's syntax is identical to the syntax used in the Existing VLANs field. By default, a port may become member of all possible VLANs, and is therefore set to 1-4095.
  The field may be left empty, which means that the port will not be member of any of the existing VLANs, but if it is configured for VLAN Trunking it will still be able to carry all unknown VLANs.

- **Forbidden VLANs :**

  A port may be configured to never be member of one or more VLANs. This is particularly useful when dynamic VLAN protocols like MVRP and GVRP must be prevented from dynamically adding ports to VLANs.
  The trick is to mark such VLANs as forbidden on the port in question. The syntax is identical to the syntax used in the Existing VLANs field.
  By default, the field is left blank, which means that the port may become a member of all possible VLANs.

Buttons

- **Apply :**

  Click to save changes.

- **Reset :**

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

2-16 Private VLANs

2-16.1 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.

Web Interface

To configure Private VLAN Membership Configuration in the web interface:

1. Click Configuration, Private VLAN and Membership.
2. Evoke Private VLAN Membership Configuration.
3. Click the Apply 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.

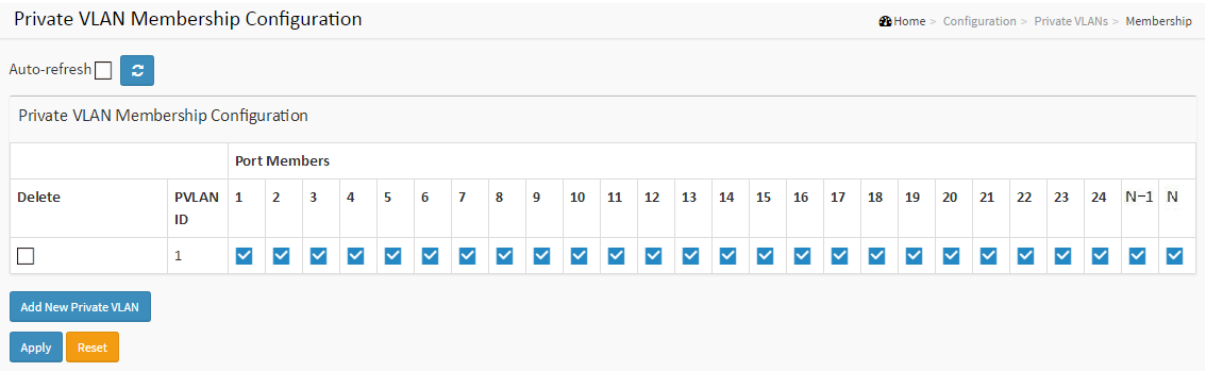


Figure 2-16.1: The Private VLAN Membership Configuration

Parameter description:

- **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.

Buttons

- **Apply :**

  Click to save changes.

- **Reset :**

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

- **Auto-refresh :**

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

- **Refresh :**

  Click to refresh the page immediately.

- **Delete :**

  To delete a private VLAN entry, check this box. The entry will be deleted during the next save.

- **Adding a New Private VLAN :**

  Click Add New Private VLAN to add a new private VLAN ID. An empty row is added to the table, and the private VLAN can be configured as needed. The allowed range for a private VLAN ID is the same as the switch port number range. Any values outside this range are not accepted, and a warning message appears. Click "OK" to discard the incorrect entry, or click "Cancel" to return to the editing and make a correction.
  The Private VLAN is enabled when you click "Save".
  The Delete button can be used to undo the addition of new Private VLANs.

2-16.2 Port Isolation

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.

Web Interface

To configure Port Isolation Configuration in the web interface:

1. Click Configuration, Private VLAN and Port Isolation.
2. Evoke Port Isolation Configuration.
3. Click the Apply 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.

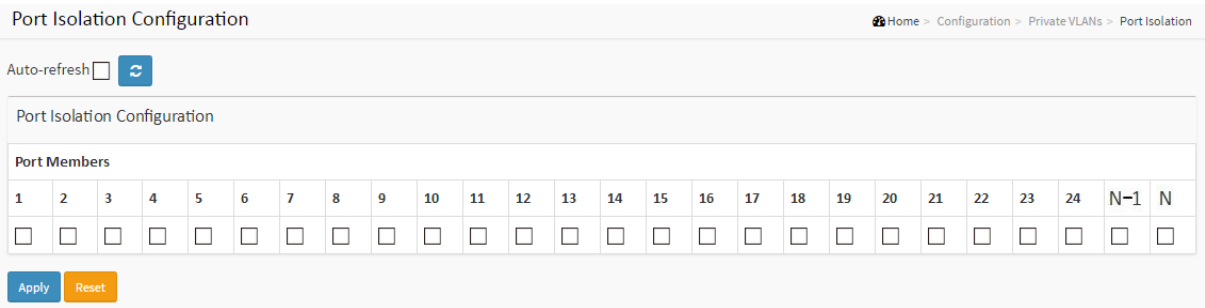


Figure 2-16.2: The Port Isolation Configuration

Parameter description:

- **Port Members :**

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

Buttons

- **Apply :**

  Click to save changes.

- **Reset :**

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

- **Auto-refresh** :

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

- **Refresh :**

  Click to refresh the page immediately.

2-17 VCL

2-17.1 MAC-based VLAN

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

Web Interface

To configure MAC-based VLAN Membership Configuration in the web interface:

1. Click Configuration, VLC and MAC-based VLAN configuration.
2. Specify the MAC address and VLAN ID.
3. Click the Apply 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.

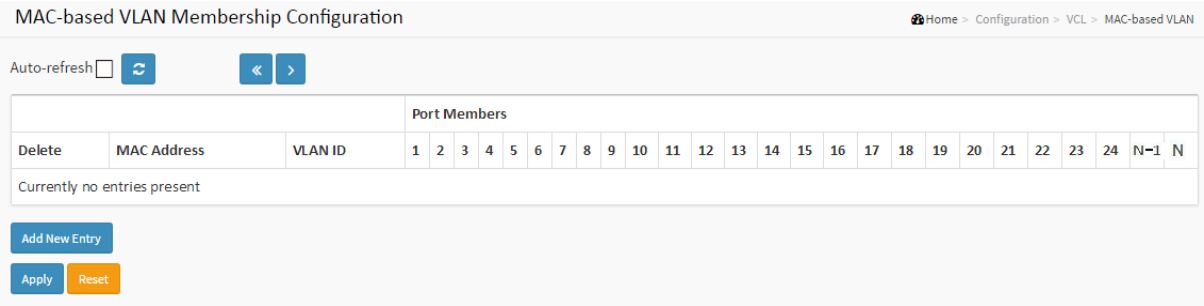


Figure 2-17.1: The MAC-based VLAN Membership Configuration

Parameter description:

- **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.

Buttons

- **Apply :**

  Click to save changes.

- **Reset :**

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

- **Delete :**

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

- **Adding a New MAC-based VLAN :**

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

  The MAC-based VLAN entry is enabled when you click on "Apply". A MAC-based VLAN without any port members will be deleted when you click "Apply".

  The Delete button can be used to undo the addition of new MAC-based VLANs. The

- **Auto-refresh** ☐ **:**

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

- **Refresh :**

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

- **<< :**

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

- **> :**

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

2-17.2 Protocol-based VLAN

This section describe Protocol -based VLAN, The Switch support Protocol include Ethernet LLC SNAP Protocol,

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, Decent 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 Subnetwork Access Protocol (SNAP) is a mechanism for multiplexing, on networks using IEEE 802.2 LLC, more protocols than can be distinguished by the 8-bit 802.2 Service Access Point (SAP) fields. SNAP supports identifying protocols by Ethernet type field values; it also supports vendor-private protocol identifier 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.

2-17.2.1 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 stack switch unit switch.

Web Interface

To configure Protocol to Group Mapping Table configuration in the web interface:

1. Click Configuration, VLC, Protocol-based VLAN configuration and Protocol to Group.
2. Specify the Protocol to Group Mapping Table.
3. Click the Apply 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.

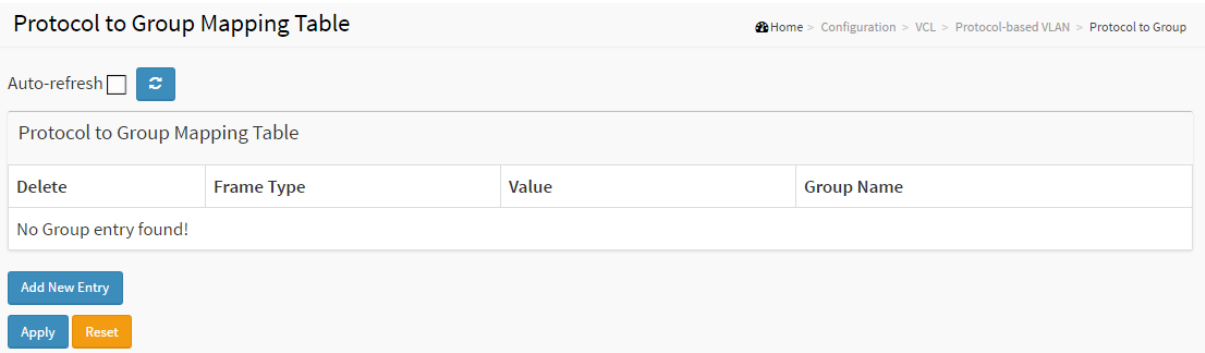


Figure 2-17.2.1: The Protocol to Group Mapping Table

Parameter description:

- **Frame Type :**

  Frame Type can have one of the following values:

  1. Ethernet
  2. LLC
  3. SNAP

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

- **Value :**

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

  For Ethernet: Values in the text field when Ethernet is selected as a Frame Type is called etype. Valid values for etype ranges from 0x0600-0xffff

  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)

  For SNAP: Valid value in this case also is comprised of two different sub-values.

  a. OUI: OUI (Organizationally Unique Identifier) is value in format of xx-xx-xx where each pair (xx) in string is a hexadecimal value ranges from 0x00-0xff.

  b. PID: If the OUI is hexadecimal 000000, the protocol ID is the Ethernet type (EtherType) field value for the protocol running on top of SNAP; if the OUI is an OUI for a particular organization, the protocol ID is a value assigned by that organization to the protocol running on top of SNAP.In other words, if value of OUI field is 00-00-00 then value of PID will be etype (0x0600-0xffff) and if value of OUI is other than 00-00-00 then valid value of PID will be any value from 0x0000 to 0xffff.

- **Group Name :**

  A valid Group Name is a unique 16-character long string for every entry which consists of a combination of alphabets (a-z or A-Z) and integers (0-9).

  NOTE: Special character and underscore (_) are not allowed.

Buttons

- **Apply :**

  Click to save changes.

- **Reset :**

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

- **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.

- **Adding a New Group to VLAN mapping entry :**

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

  The button can be used to undo the addition of new entry.

- **Auto-refresh :**

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

- **Refresh :**

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

2-17.2.2 Group to VLAN

This page allows you to map already configured Group Name to a VLAN for the switch.

Web Interface

To configure Group Name to VLAN mapping Table in the web interface:

1. Click Configuration, VLC, Protocol-based VLAN and Group to VLAN.
2. Specify the Group Name to VLAN Mapping Table.
3. Click the Apply 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.

Figure 2-17.2.2: The Group Name to VLAN mapping Table

Parameter description:

- **Group Name :**

  A valid Group Name is a string at the 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 pre-used 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.

Buttons

- **Apply :**

  Click to save changes.

- **Reset :**

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

- **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

- **Adding a New Group to VLAN mapping entry :**

  Click Add New Entry to add a new entry in mapping table. An empty row is added to the table, the Group Name, VLAN ID and port members can be configured as needed. Legal values for a VLAN ID are 1 through 4095.

  The Delete button can be used to undo the addition of new entry. The maximum possible Group to VLAN mappings are limited to 64.

- **Auto-refresh :**

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

- **Refresh :**

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

2-17.3 IP Subnet-based VLAN

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

Web Interface

To configure IP Subnet-based VLAN Membership Configuration in the web interface:

1. Click Configuration, VLC and IP Subnet-based VLAN.
2. Click Add New Entry.
3. Specify the IP Subnet-based VLAN Membership Configuration.
4. Click the Apply 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.

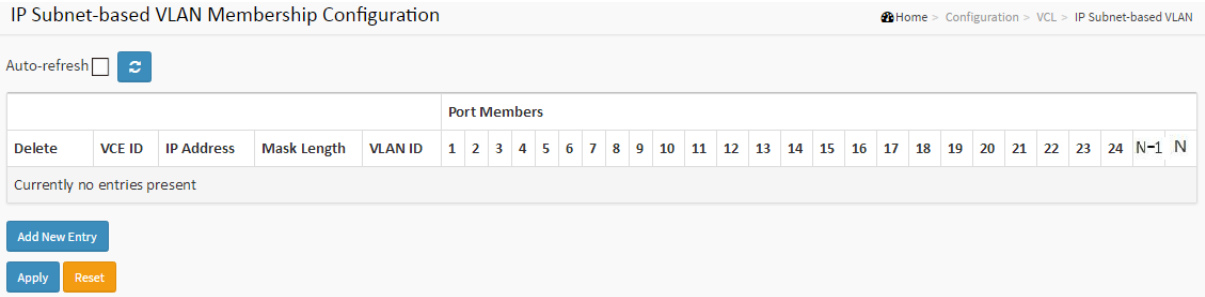


Figure 2-17.3: IP Subnet-based VLAN Membership Configuration

Parameter description:

- **VCE ID :**

  Indicates the index of the entry. It is user configurable. Its value ranges from 0-128. If a VCE ID is 0, application will auto-generate the VCE ID for that entry. Deletion and lookup of IP subnet-based VLAN are based on VCE ID.

- **IP Address :**

  Indicates the IP address.

- **Mask Length :**

  Indicates the network mask length.

- **VLAN ID :**

  Indicates the VLAN ID. VLAN ID can be changed for the existing entries.

- **Port Members :**

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

Buttons

- **Apply :**

  Click to save changes.

- **Reset :**

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

- **Delete :**

  To delete an IP subnet-based VLAN entry, check this box and press save. The entry will be deleted on the selected switch in the stack.

- **Adding a New IP subnet-based VLAN**

  Click “Add New Entry” to add a new IP subnet-based VLAN entry. An empty row is added to the table, and the IP subnet-based VLAN entry can be configured as needed. Any IP address/mask can be configured for the IP subnet-based VLAN entry. Legal values for a VLAN ID are 1 through 4095.

  The IP subnet-based VLAN entry is enabled on the selected stack switch unit when you click on "Save". The “Delete” button can be used to undo the addition of new IP subnet-based VLANs. The maximum possible IP subnet-based VLAN entries are limited to 128.

- **Auto-refresh :**

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

- **Refresh :**

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

2-18 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.

2-18.1 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.

Web Interface

To configure Voice VLAN in the web interface:

1. Click Configuration, Voice VLAN and Configuration.
2. Select "Enabled" in the Voice VLAN Configuration.
3. Specify VLAN ID, Aging Time and Traffic Class.
4. Specify the Port Configuration.
5. Click the Apply to save the setting.
6. If you want to cancel the setting then you need to click the Reset button. It will revert to previously saved values.

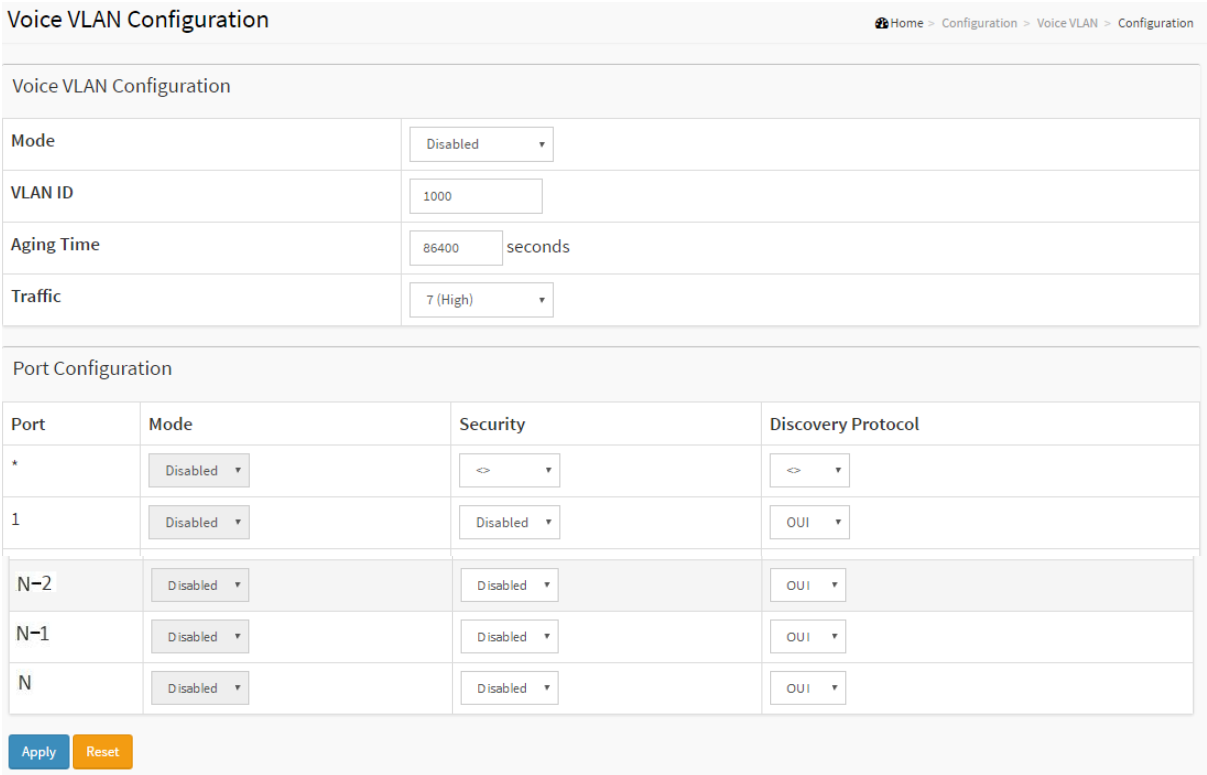


Figure 2-18.1: The Voice VLAN Configuration

Parameter description:

- **Mode :**

  Indicates the Voice VLAN mode operation. We must disable MSTP feature before we enable Voice VLAN. It can avoid the conflict of ingress filtering. Possible modes are:

  Enabled: Enable Voice VLAN mode operation.

  Disabled: Disable Voice VLAN mode operation.

- **VLAN ID :**

  Indicates the Voice VLAN ID. It should be a unique VLAN ID in the system and cannot equal each port PVID. It is 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 :**

  Indicates the Voice VLAN traffic class. All traffic on the Voice VLAN will apply this class.

- **Port Mode :**

  Indicates the Voice VLAN port mode. Possible port modes are:

  Disabled: Disjoin from Voice VLAN.

  Auto: Enable auto detect mode. It detects whether there is VoIP phone attached to the specific port and configures the Voice VLAN members automatically.

  Forced: Force join to Voice VLAN.

  This field will be read only if STP feature is enabled. And the STP port mode will be readonly if this field be set to the mode other than Disabled.

- **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

- **Apply :**

Click to save changes.

- **Reset :**

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

- **Delete :**

  To delete an IP subnet-based VLAN entry, check this box and press save. The entry will be deleted on the selected switch in the stack.

2-18.2 OUI

Configure VOICE VLAN OUI table on this page. The maximum number of entries is 16. Modifying the OUI table will restart auto detection of OUI process.

Web Interface

To configure Voice VLAN OUI Table in the web interface:

1. Click Configuration, Voice VLAN and OUI.
2. Click Add New Entry.
3. Specify the Voice VLAN OUI Table.
4. Click the Apply 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.

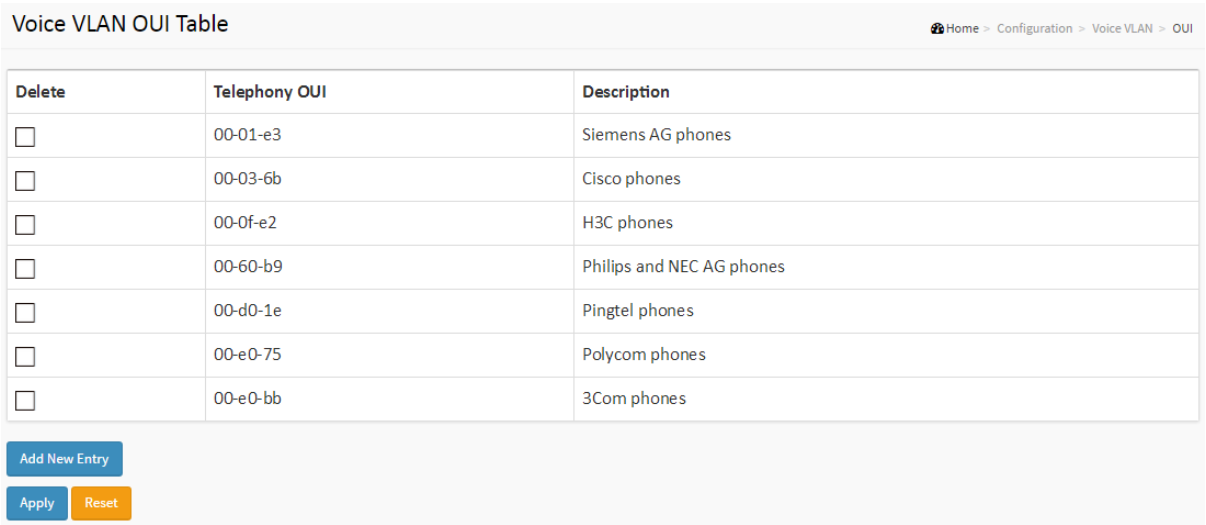


Figure 2-18.2: The Voice VLAN OUI Table

Parameter description:

- **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.

Buttons

- **Apply :**

  Click to save changes.

- **Reset :**

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

- **Delete :**

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

- **Add New entry :**

  Click to add a new access management entry.

2-19 QoS

The switch support four QoS queues per port with strict or weighted fair queuing scheduling. It supports QoS Control Lists (QCL) for advance programmable QoS classification, based on IEEE 802.1p, Ethertype, VID, IPv4/IPv6 DSCP and UDP/TCP ports and ranges.

High flexibility in the classification of incoming frames to a QoS class. The QoS classification looks for information up to Layer 4, including IPv4 and IPv6 DSCP, IPv4 TCP/UDP port numbers, and user priority of tagged frames. This QoS classification mechanism is implemented in a QoS control list (QCL). The QoS class assigned to a frame is used throughout the device for providing queuing, scheduling, and congestion control guarantees to the frame according to what was configured for that specific QoS class.

The switch support advanced memory control mechanisms providing excellent performance of all QoS classes under any traffic scenario, including jumbo frame. A super priority queue with dedicated memory and strict highest priority in the arbitration. The ingress super priority queue allows traffic recognized as CPU traffic to be received and queued for transmission to the CPU even when all the QoS class queues are congested.

2-19.1 Port Classification

The section allows you to configure the basic QoS Ingress Classification settings for all switch ports.

Web Interface

To configure the QoS Ingress Port Classification parameters in the web interface:

1. Click Configuration, QoS and Port Classification.
2. Scroll to select QoS Ingress Port parameters.
3. Click the Apply 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.

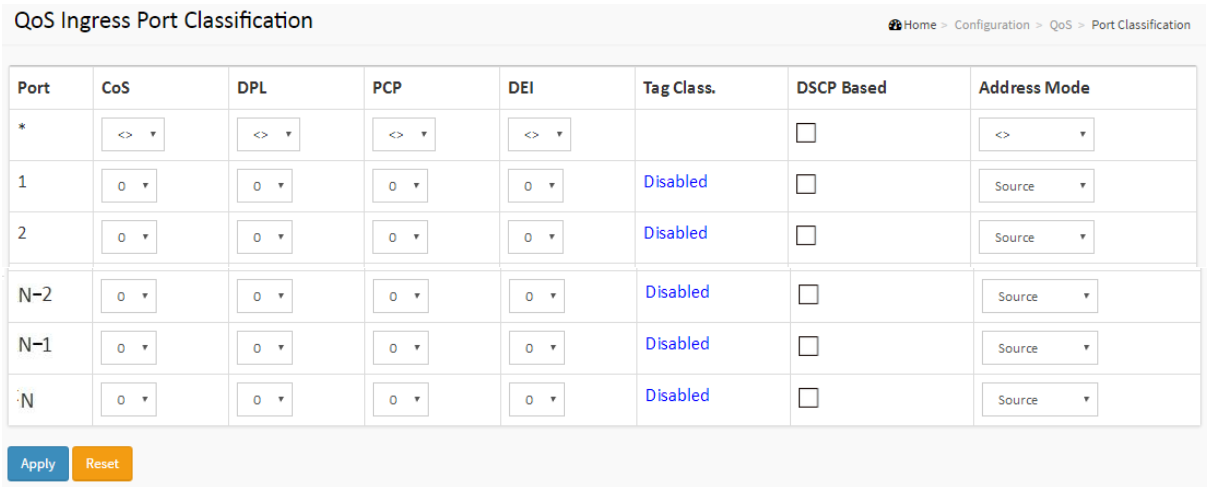


Figure 2-19.1: The QoS Ingress Port Classification

Parameter description:

- **Port :**

  The port number for which the configuration below applies.

- **CoS :**

  Controls the default class of service.

  All frames are classified to a CoS. There is a one to one mapping between CoS, queue and priority. A CoS of 0 (zero) has the lowest priority.

  If the port is VLAN aware and the frame is tagged, then the frame is classified to a CoS that is based on the PCP value in the tag as shown below. Otherwise the frame is classified to the default CoS.

PCP value:	0	1	2	3	4	5	6	7
CoS value:	1	0	2	3	4	5	6	7

  The classified CoS can be overruled by a QCL entry.

  NOTE: If the default CoS has been dynamically changed, then the actual default CoS is shown in parentheses after the configured default CoS.

- **DPL :**

  Controls the default drop precedence level.

  All frames are classified to a drop precedence level.

  If the port is VLAN aware, the frame is tagged and Tag Class. is enabled, then the frame is classified to a DPL that is mapped from the PCP and DEI value in the tag. Otherwise the frame is classified to the default DPL.

  The classified DPL can be overruled by a QCL entry.

- **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.

2-19.2 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

Web Interface

To configure the QoS Ingress Port Policers in the web interface:

1. Click Configuration, QoS and Port Policing
2. Evoke which port need to enable the QoS Ingress Port Policers and type the Rate limit condition.
3. Scroll to select the column Rate and Unit.
4. Click the Apply 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.

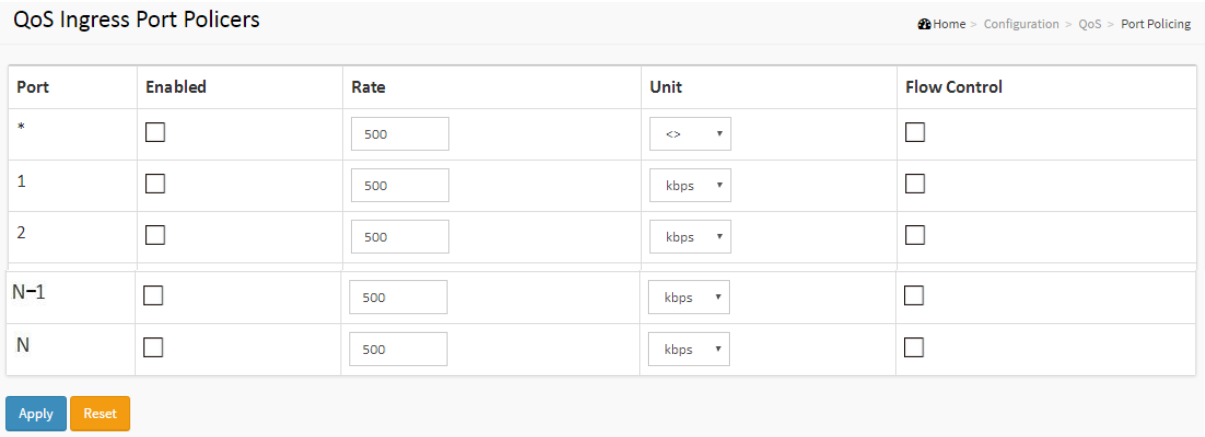


Figure 2-19.2: The QoS Ingress Port Policers

Parameter description:

- **Port :**

  The port number for which the configuration below applies.

- **Enabled :**

  Controls whether the policer is enabled on this switch port.

- **Rate :**

  Controls the rate for the port policer. This value is restricted to 100-13128072 when "Unit" is kbps, 1-13128 when "Unit" is mbps , 1-131071 when "Unit" is fps, and 1-131 when "Unit" is kfps. The rate is internally rounded up to the nearest value supported by the port policer.

- **Unit :**

  Controls the unit of measure for the port policer rate as kbps, Mbps, fps or kfps.

- **Flow Control :**

  If flow control is enabled and the port is in flow control mode, then pause frames are sent instead of discarding frames.

Buttons

- **Apply :**

  Click to save changes.

- **Reset :**

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

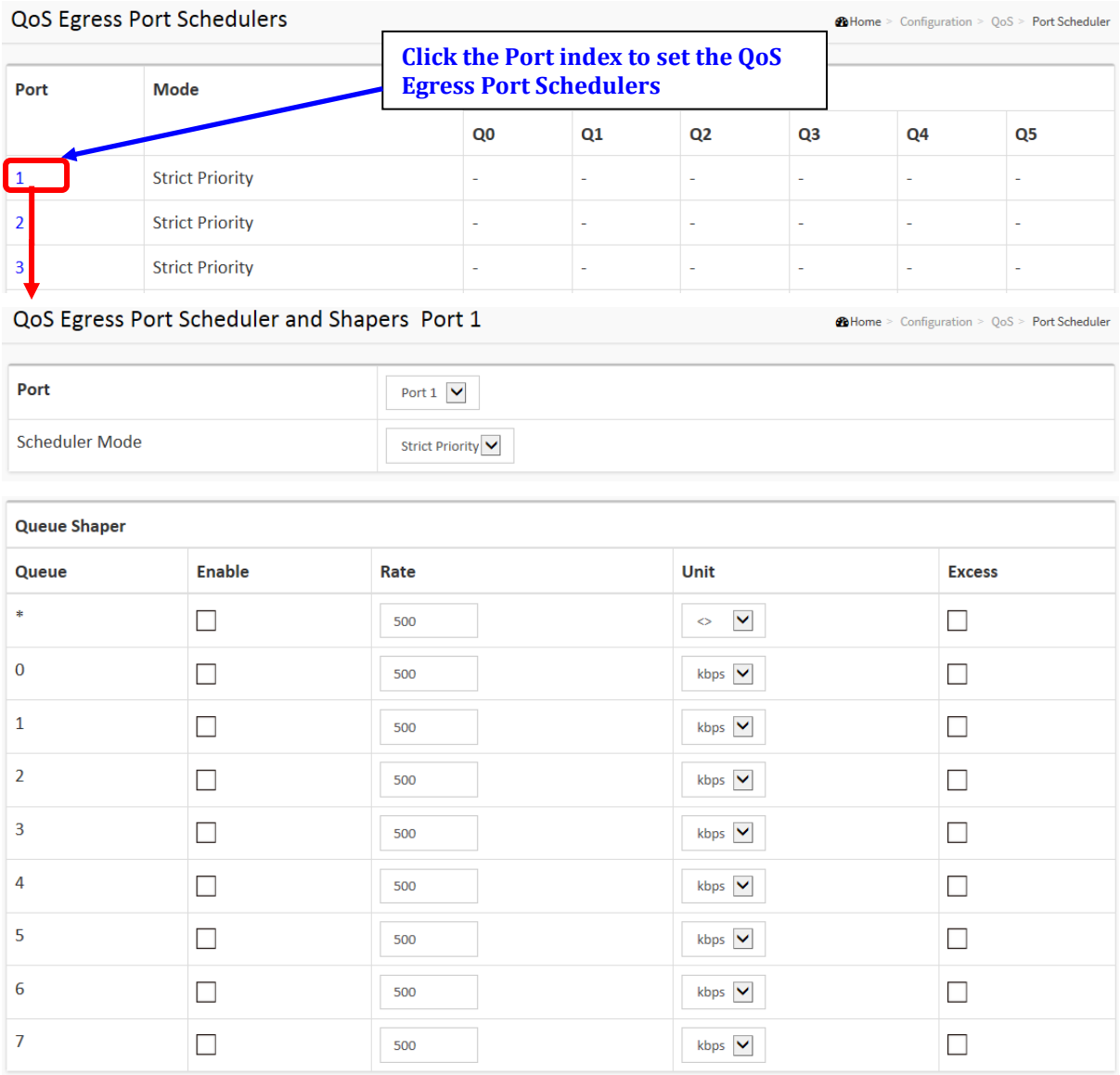
2-19.3 Port Schedulers

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

Web Interface

To configure the QoS Ingress Port Policers in the web interface:

1. Click Configuration, QoS and Port Schedulers.
2. Click the Port and display the QoS Egress Port Schedulers
3. Scroll Port and Scheduler Mode, specify the Queue Shaper parameter.
4. Click the Apply 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.



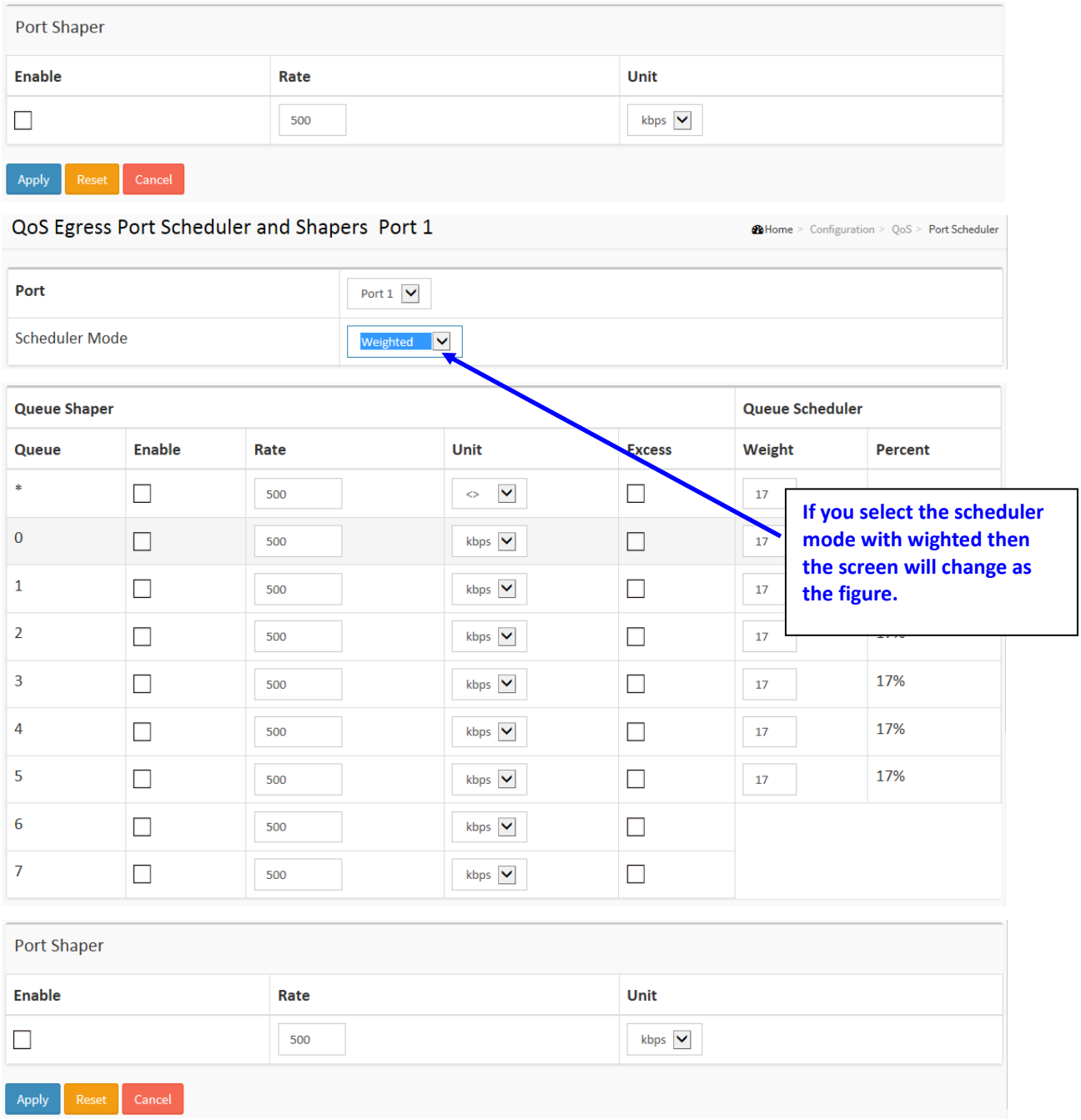


Figure 2-19.3: The QoS Egress Port Schedules

Parameter description:

- **Port :**

  The logical port for the settings contained in the same row. Click on the port number in order to configure the schedulers.

- **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 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".

- **Port Shaper Unit :**

  Controls the unit of measure for the port shaper rate as "kbps" or "Mbps". The default value is "kbps".

Buttons

- **Apply :**

  Click to save changes.

- **Reset :**

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

- **Cancel :**

  Click to undo any changes made locally and return to the previous page.

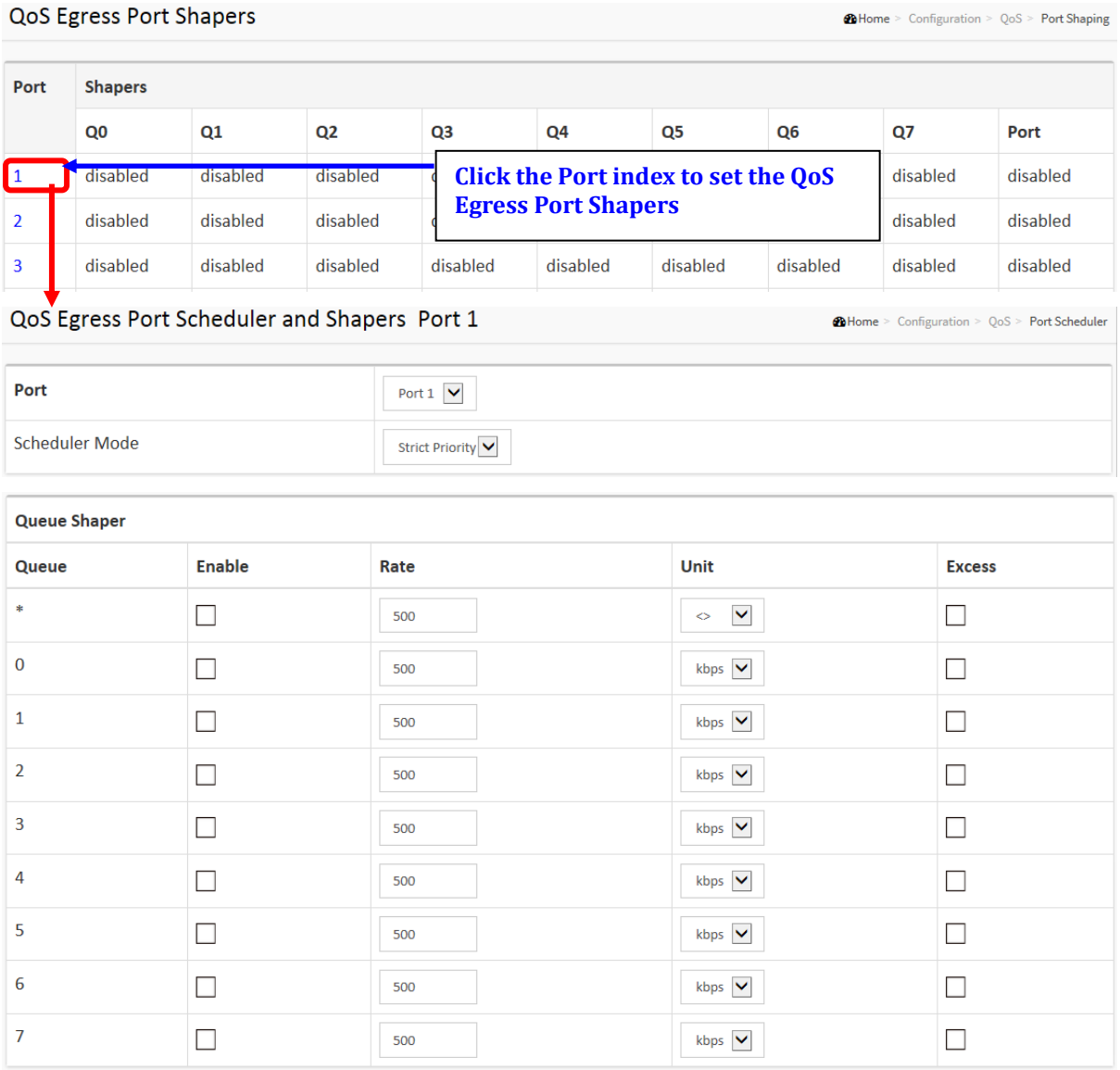
2-19.4 Port Shaping

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

Web Interface

To configure the QoS Egress Port Shapers in the web interface:

1. Click Configuration, QoS and Port Shaping.
2. Click the Port and display the Qos Egress Port Shapers.
3. Scroll the Port and Scheduler Mode and specify the Queue Shaper parameter.
4. Click the Apply 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.



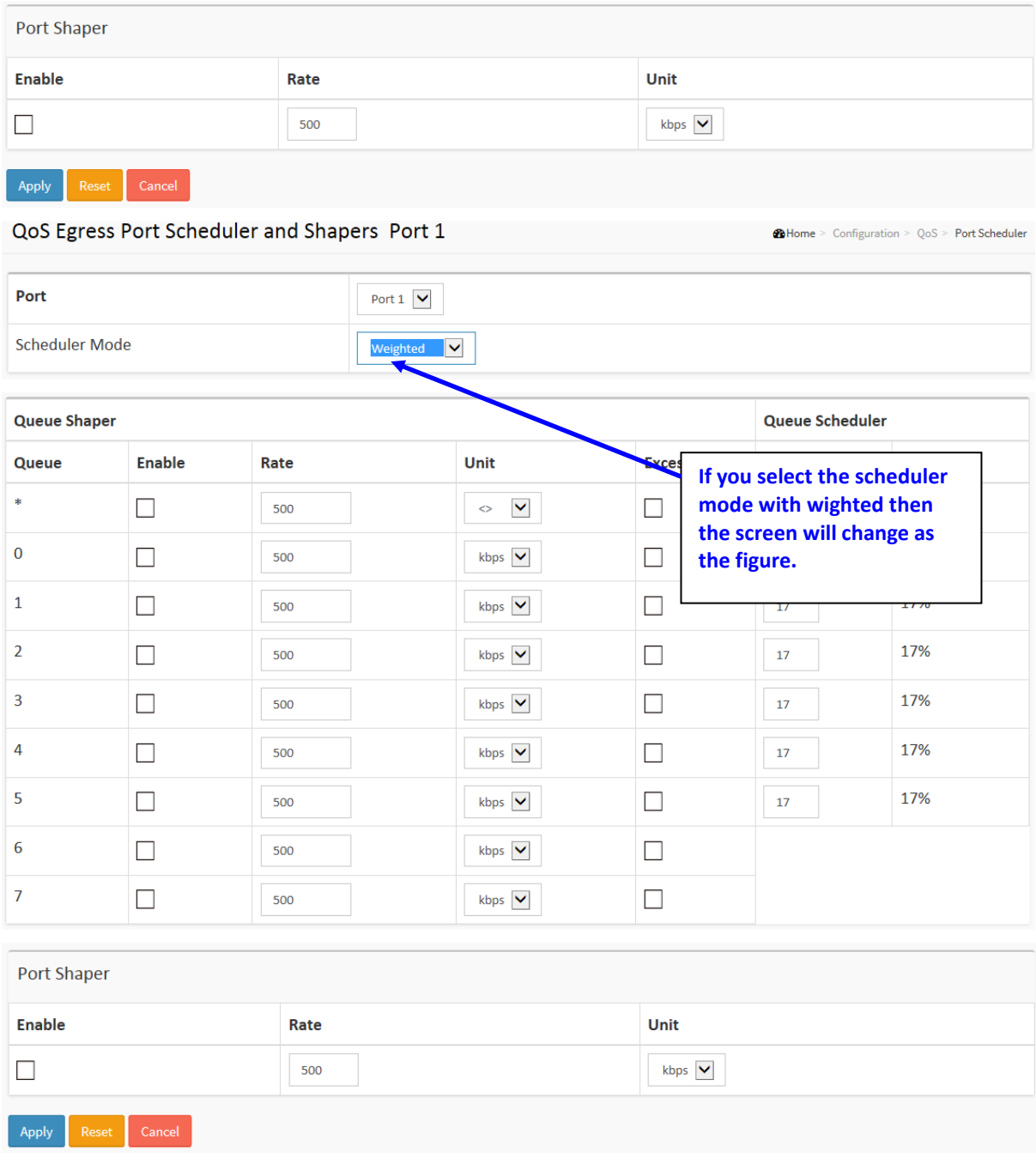


Figure 2-19.4: The QoS Egress Port Shapers

Parameter description:

- **Port :**

  The logical port for the settings contained in the same row. Click on the port number in order to configure the schedulers.

- **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 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".

- **Port Shaper Unit :**

  Controls the unit of measure for the port shaper rate as "kbps" or "Mbps". The default value is "kbps".

Buttons

- **Apply :**

  Click to save changes.

- **Reset :**

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

- **Cancel :**

  Click to undo any changes made locally and return to the previous page.

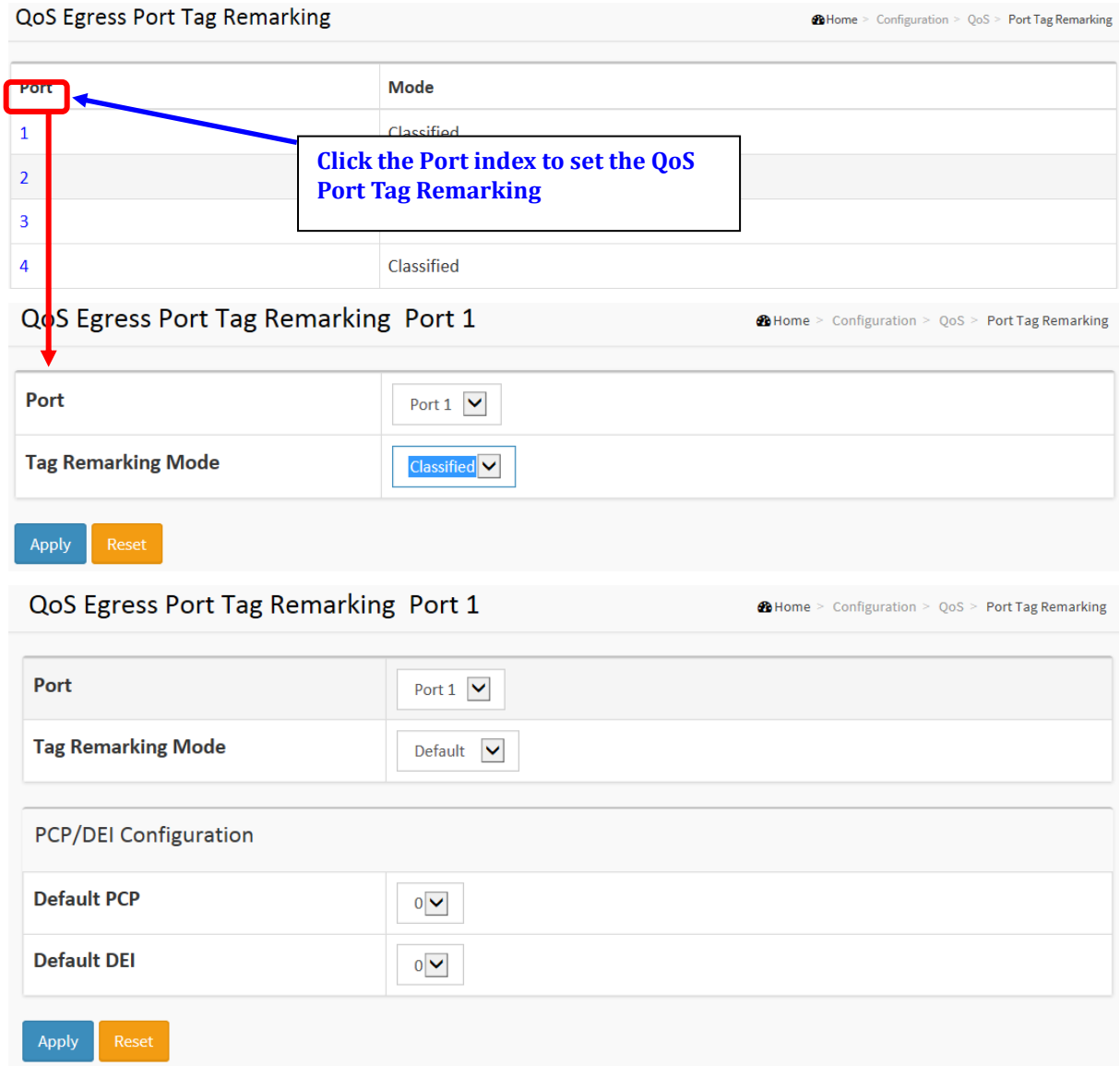
2-19.5 Port Tag Remarking

The Section provides user to get an overview of QoS Egress Port Tag Remarking for all switch ports. Others the ports belong to the currently selected stack unit, as reflected by the page header. .

Web Interface

To configure the QoS Port Tag Remarking in the web interface:

1. Click Configuration, QoS and Port Tag Remarking.
2. Click the Port and display the Qos Port Tag Remarking.
3. Scroll the Port and Tag Remarking Mode and specify the Queue Shaper parameter.
4. Click the Apply 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.



QoS Egress Port Tag Remarking Port 1

Home > Configuration > QoS > Port Tag Remarking

Port	Port 1
Tag Remarking Mode	Mapped

(QoS class, DP level) to (PCP, DEI) Mapping

QoS class	DP level	PCP	DEI
*	*	<>	<>
0	0	1	0
0	1	1	1
1	0	0	0
1	1	0	1
2	0	2	0
2	1	2	1
3	0	3	0
3	1	3	1
4	0	4	0
4	1	4	1
5	0	5	0
5	1	5	1
6	0	6	0
6	1	6	1
7	0	7	0
7	1	7	1

Apply Reset

Figure 2-19.5: The Port Tag Remarking

Parameter description:

- **Port :**

  The logical port for the settings contained in the same row.
  Click on the port number in order to configure tag remarking.

- **Mode :**

  Controls 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.

- **PCP/DEI Configuration :**

  Controls the default PCP and DEI values used when the mode is set to Default.

- **(QoS class, DP level) to (PCP, DEI) Mapping :**

  Controls the mapping of the classified (QoS class, DP level) to (PCP, DEI) values when the mode is set to Mapped.

Buttons

- **Apply :**

  Click to save changes.

- **Reset :**

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

- **Cancel :**

  Click to undo any changes made locally and return to the previous page.

2-19.6 Port DSCP

The section will teach user to set the QoS Port DSCP configuration that was allowed you to configure the basic QoS Port DSCP Configuration settings for all switch ports. Others the settings relate to the currently selected stack unit, as reflected by the page header.

Web Interface

To configure the QoS Port DSCP parameters in the web interface:

1. Click Configuration, QoS and Port DSCP.
2. Evoke to enable or disable the Ingress Translate and Scroll the Classify parameter.
3. Scroll to select Egress Rewrite parameters
4. Click the apply 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

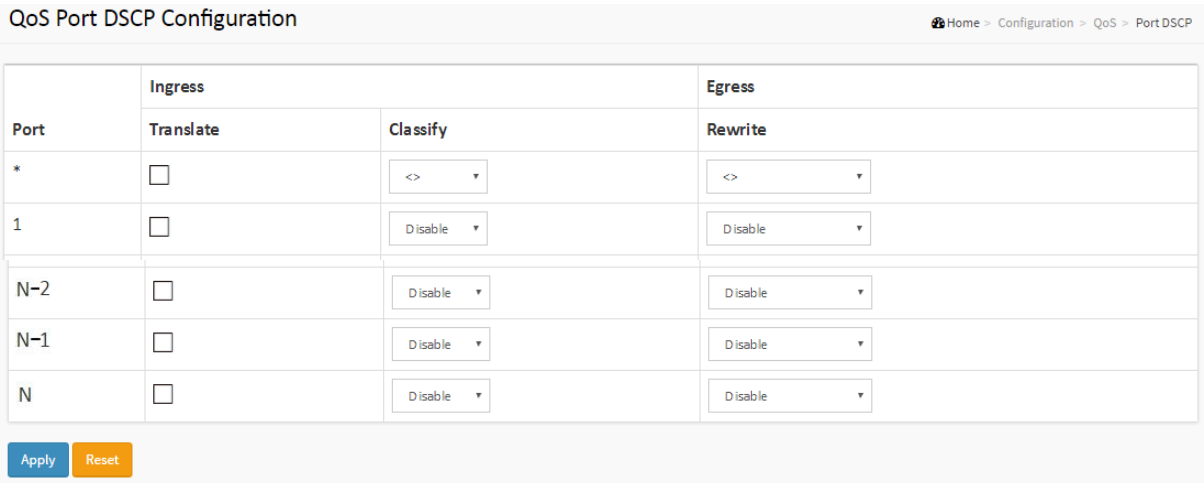


Figure 2-19.6: The QoS Port DSCP Configuration

Parameter description:

- **Port :**

  The Port column shows the list of ports for which you can configure dscp ingress and egress settings.

- **Ingress :**

  In Ingress settings you can change ingress translation and classification settings for individual ports.

  There are two configuration parameters available in Ingress:

  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 below 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.

2-19.7 DSCP-Based QoS

The section will teach user to configure the DSCP-Based QoS mode that This page allows you to configure the basic QoS DSCP based QoS Ingress Classification settings for all switches.

Web Interface

To configure the DSCP –Based QoS Ingress Classification parameters in the web interface:

1. Click Configuration, QoS and DSCP-Based QoS.
2. Evoke to enable or disable the DSCP for Trust
3. Scroll to select QoS Class and DPL parameters
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

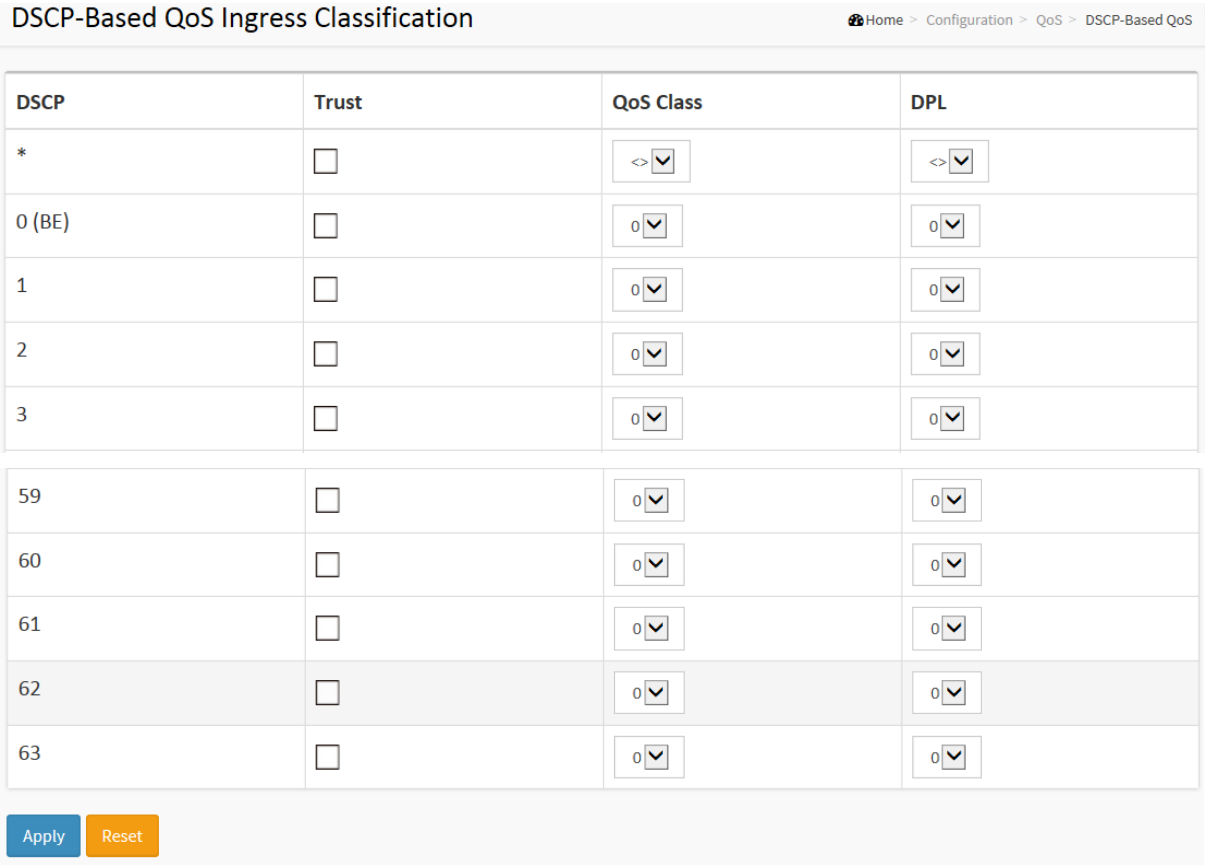


Figure 2-19.7: The DSCP-Based QoS Ingress Classification Configuration

Parameter description:

- **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

- **Apply :**

  Click to save changes.

- **Reset :**

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

2-19.8 DSCP Translation

The section describes the switch allows you to configure the basic QoS DSCP Translation settings for all switches. DSCP translation can be done in Ingress or Egress.

Web Interface

To configure the DSCP Translation parameters in the web interface:

1. Click Configuration, QoS and 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 the apply 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

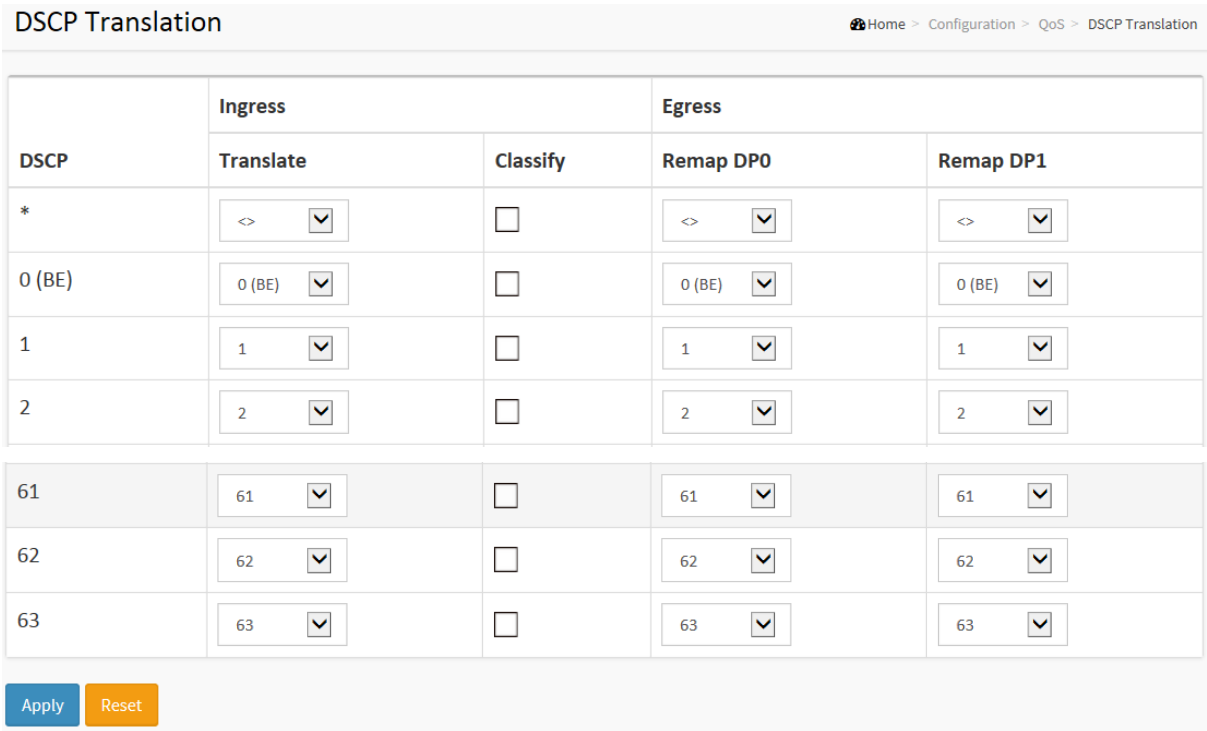


Figure 2-19.8: The DSCP Translation Configuration

Parameter description:

- **DSCP :**

  Maximum number of supported DSCP values are 64 and valid DSCP value ranges from 0 to 63.

- **Ingress :**

  Ingress side DSCP can be first translated to new DSCP before using the DSCP for QoS class and DPL map.

  There are two configuration parameters for DSCP Translation –

1. Translate: DSCP at Ingress side can be translated to any of (0-63) DSCP values.
2. Classify: Click to enable Classification at Ingress side.

- **Egress :**

  There are following configurable parameters for Egress side –

  1. Remap: Select the DSCP value from select menu to which you want to remap. DSCP value ranges from 0 to 63.

- **Remap DP0 :**

  Select the DSCP value from select menu to which you want to remap. DSCP value ranges form 0 to 63.

- **Remap DP1 :**

  Select the DSCP value from select menu to which you want to remap. DSCP value ranges form 0 to 63.

Buttons

- **Apply :**

  Click to save changes.

- **Reset :**

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

2-19.9 DSCP Classification

The section describes to teach user to configure and allows you to map DSCP value to a QoS Class and DPL value. Others the settings relate to the currently selected stack unit, as reflected by the page header.

Web Interface

To configure the DSCP Classification parameters in the web interface:

1. Click Configuration, QoS and DSCP Translation
2. Scroll to set the DSCP Parameters
3. Click the apply 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

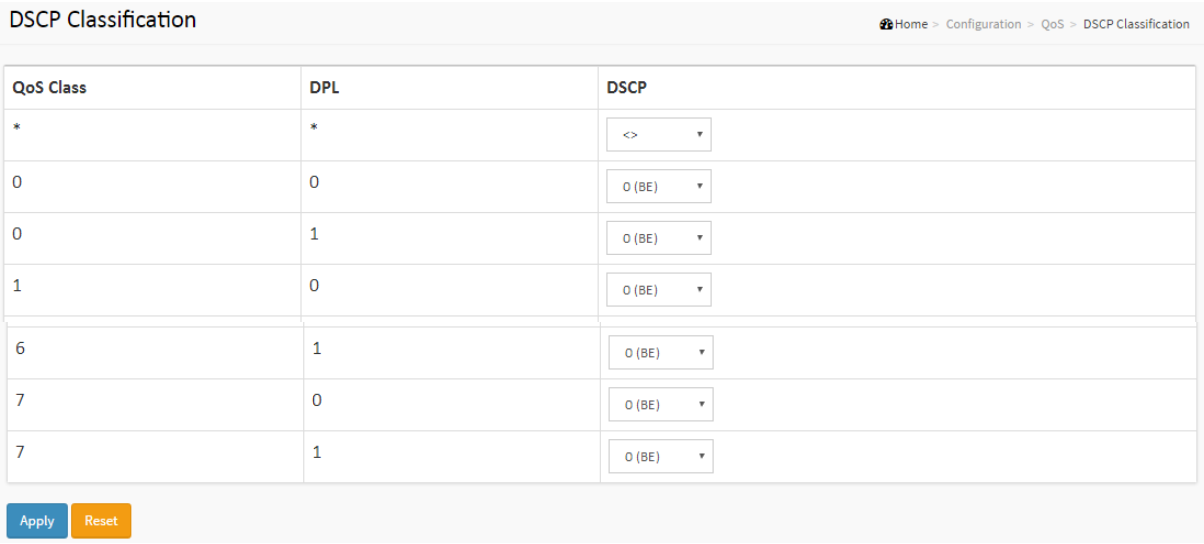


Figure 2-19.9: The DSCP Classification Configuration

Parameter description:

- **QoS Class :**

  Available QoS Class.

- **DPL :**

  Actual Drop Precedence Level.

- **DSCP :**

  Select the classified DSCP value (0-63).

Buttons

- **Apply :**

  Click to save changes.

- **Reset :**

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

2-19.10 QoS Control List

The section shows the QoS Control List (QCL), which is made up of the QCEs. Each row describes a QCE that is defined. The maximum number of QCEs is 256 on each switch. Click on the lowest plus sign to add a new QCE to the list.

Web Interface

To configure the QoS Control List parameters in the web interface:

1. Click Configuration, QoS and QoS Contol List
2. Click the ⊕ to add a new QoS Control List
3. Scroll all parameters and evoke the Port Member to join the QCE rules
4. Click the apply 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

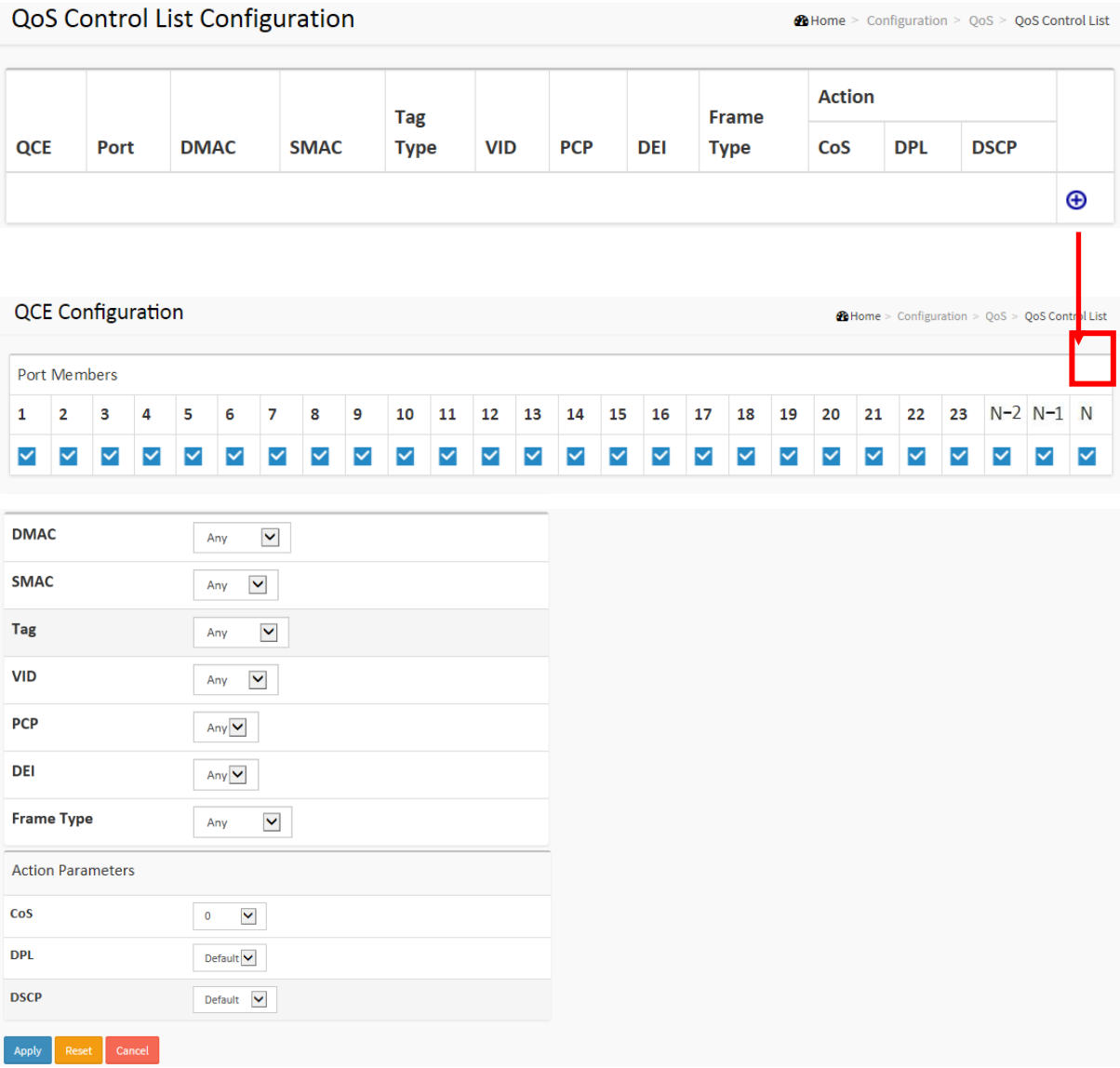


Figure 2-19.10: The QoS Control List Configuration

Parameter description:

- **QCE :**

  Indicates the index of QCE.

- **Port :**

  Indicates the list of ports configured with the QCE.

- **DMAC :**

  Indicates the destination MAC address. Possible values are:

  Any: Match any DMAC.

  Unicast: Match unicast DMAC.

  Multicast: Match multicast DMAC.

  Broadcast: Match broadcast DMAC.

  <MAC>: Match specific DMAC.

  The default value is 'Any'.

- **SMAC :**

  Match specific source MAC address or 'Any'.

  If a port is configured to match on DMAC/DIP, this field indicates the DMAC.

- **Tag Type :**

  Indicates tag type. Possible values are:
  Any: Match tagged and untagged frames.
  Untagged: Match untagged frames.
  Tagged: Match tagged frames.
  C-Tagged: Match C-tagged frames.
  S-Tagged: Match S-tagged frames.
  The default value is 'Any'.

- **VID :**

  Indicates (VLAN ID), either a specific VID or range of VIDs. VID can be in the range 1-4095 or 'Any'

- **PCP :**

  Priority Code Point: Valid values of 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 are 0, 1 or 'Any'.

- **Frame Type :**

  Indicates the type of frame to look for incoming frames. Possible frame types are:

  Any: The QCE will match all frame type.

  Ethernet: Only Ethernet frames (with Ether Type 0x600-0xFFFF) are allowed.

  LLC: Only (LLC) frames are allowed.

  SNAP: Only (SNAP) frames are allowed

  IPv4: The QCE will match only IPV4 frames.

IPv6: The QCE will match only IPV6 frames.

- **Action :**

  Indicates the classification action taken on ingress frame if parameters configured are matched with the frame's content.

  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.

  : 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 are described as below:

  DMAC Destination MAC address: Possible values are 'Unicast', 'Multicast', 'Broadcast' or 'Any'.

  SMAC Source MAC address: xx-xx-xx (24 MS bits OUI) or 'Any'.

  Tag Value of Tag field can be 'Untagged', 'Tagged' or 'Any'.
  VID Valid value of VLAN ID can be any value in the range 1-4095 or 'Any'; user can enter either a specific value or a range of VIDs.
  PCP 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 Valid value of DEI can be '0', '1' or 'Any'.
  Frame Type Frame Type can have any of the following values

  1. Any
  2. Ethernet
  3. LLC
  4. SNAP
  5. IPv4
  6. IPv6

NOTE: All frame types are explained below:
1. Any: 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): It can be specific value, range of value or 'Any'. DSCP values are in the range 0-63 including BE, CS1-CS7, EF or AF11-AF43
Sport Source TCP/UDP port:(0-65535) or 'Any', specific or port range 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) or 'Default'.

  'Default' means that the default classified value is not modified by this QCE.

Buttons

- **Apply :**

  Click to save changes.

- **Reset :**

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

- **Cancel :**

  Return to the previous page without saving the configuration change.

2-19.11 Storm Control

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.

Web Interface

To configure the Storm Control Configuration parameters in the web interface:

1. Click Configuration, QoS and Storm Control.
2. Evoke to select the frame type to enable storm control
3. Scroll to set the Rate Parameters
4. Click the apply 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

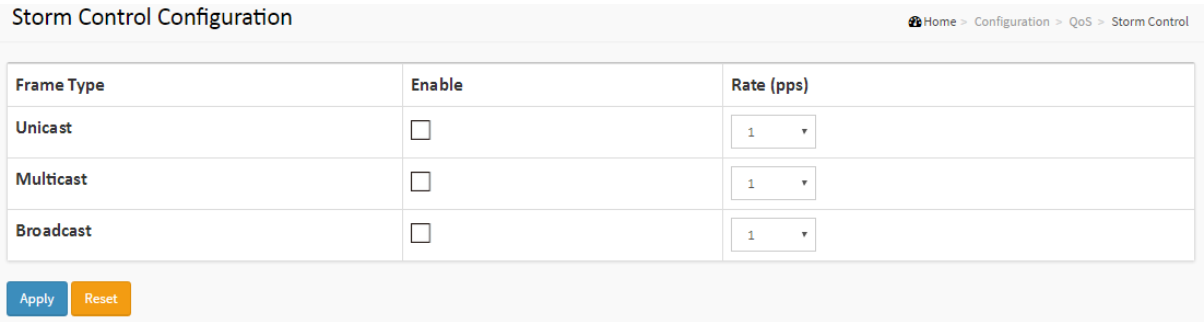


Figure 2-19.11: The Storm Control Configuration

Parameter description:

- **Port :**

  The port number for which the configuration below applies.

- **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.Buttons

- **Apply :**

  Click to save changes.

- **Reset :**

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

2-20 Mirroring

To debug network problems, selected traffic can be copied, or mirrored, on a mirror port where a frame analyzer can be attached to analyze the frame flow.
The traffic to be copied on the mirror port is selected as follows:
All frames received on a given port (also known as ingress or source mirroring).
All frames transmitted on a given port (also known as egress or destination mirroring).

Web Interface

To configure the Mirror in the web interface:

1. Click Configuration and 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 apply 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

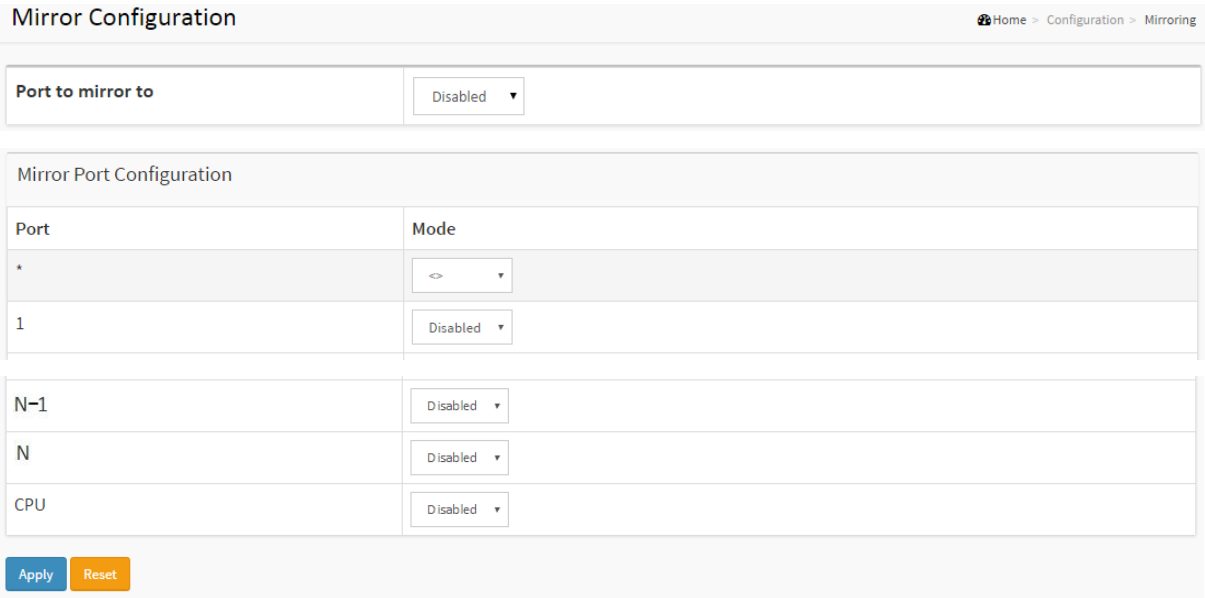


Figure 2-20: The Mirroring Configuration

Parameter description:

Port to mirror on

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

The following table is used for Rx and Tx enabling.

- **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.

2-21 UPnP

UPnP is an acronym for Universal Plug and Play. The goals of UPnP are to allow devices to connect seamlessly and to simplify the implementation of networks in the home (data sharing, communications, and entertainment) and in corporate environments for simplified installation of computer components

Web Interface

To configure the UPnP Configuration in the web interface:

1. Click Configuration and UPnP.
2. Scroll to select the mode to enable or disable.
3. Specify the parameters in each blank field.
4. Click apply 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.

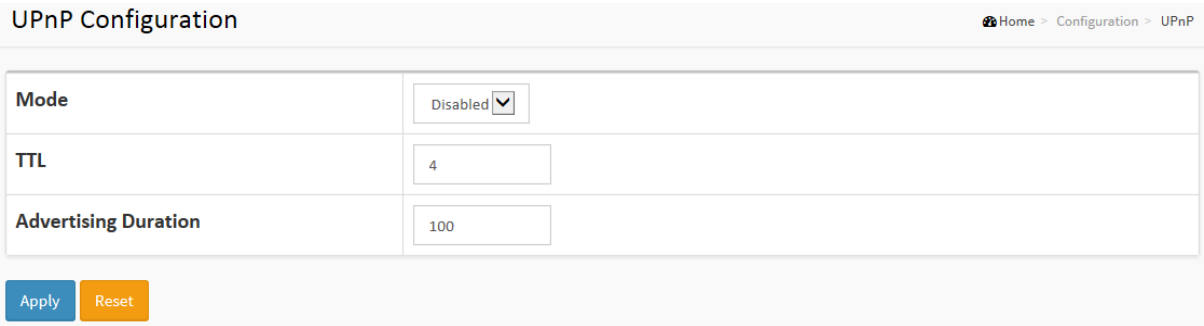


Figure 2-21: The UPnP Configuration

Parameter description:

- **Mode :**

  Indicates the UPnP operation mode. Possible modes are:

  Enabled: Enable UPnP mode operation.

  Disabled: Disable UPnP mode operation.

  When the mode is enabled, two ACEs are added automatically to trap UPNP related packets to CPU. The ACEs are automatically removed when the mode is disabled. .

- **TTL :**

  The TTL value is used by UPnP to send SSDP advertisement messages. Valid values are in the range 1 to 255.

- **Advertising Duration :**

  The duration, carried in SSDP packets, is used to inform a control point or control points how often it or they should receive an SSDP advertisement message from this switch. If a control point does not receive any message within the duration, it will think that the switch no longer exists. Due to the unreliable nature of UDP, in the standard it is recommended

that such refreshing of advertisements to be done at less than one-half of the advertising duration. In the implementation, the switch sends SSDP messages periodically at the interval one-half of the advertising duration minus 30 seconds. Valid values are in the range 100 to 86400.

Buttons

- **Apply :**

  Click to save changes.

- **Reset :**

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

2-22 GVRP

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.

2-22.1 Global Config

This page allows you to configure the basic GVRP Configuration settings for all switch ports.

Web Interface

To configure the GVRP in the web interface:

1. Click Configuration, GVRP and Global Config
2. Evoke to enable or disable the GVRP.
3. Specify Join-time, Leave-time, Leave All-time, Max VLANs
4. Click apply 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.

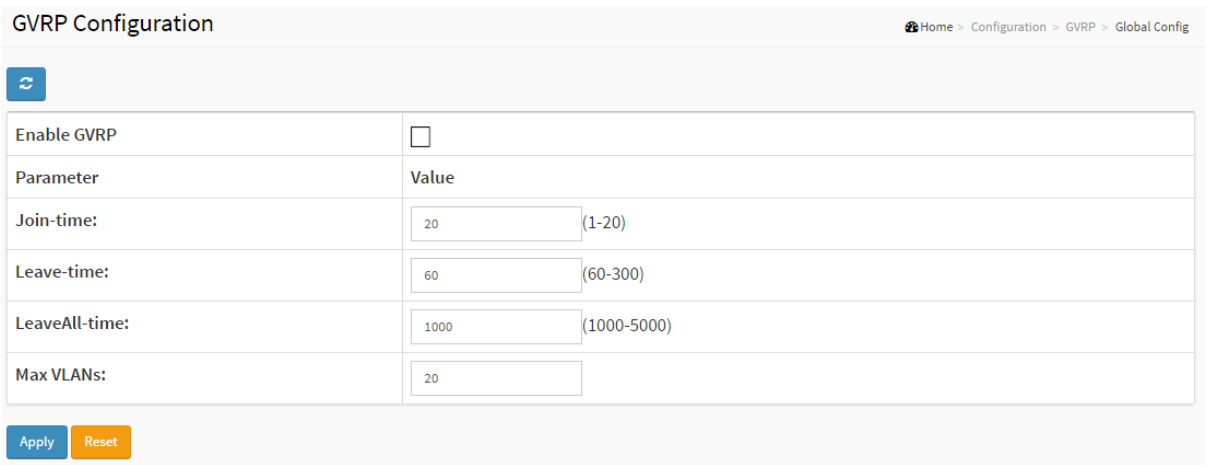


Figure 2-22.1: The GVRP Configuration

Parameter description:

Enable GVRP globally

The GVRP feature is enabled by setting the check mark in the checkbox named Enable GVRP.

GVRP protocol timers

Join-time is a value in the range 1-20 in the units of centi seconds, i.e. in units of one hundredth of a second. The default is 20.

Leave-time is a value in the range 60-300 in the units of centi seconds, i.e. in units of one hundredth of a second. The default is 60.

Leave All-time is a value in the range 1000-5000 in the units of centi seconds, i.e. in units of one hundredth of a second. The default is 1000.

Max number of VLANs

When GVRP is enabled a maximum number of VLANs supported by GVRP is specified. By default this number is 20. This number can only be changed when GVRP is turned off.

Buttons

- **Apply :**

  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 input fields.

2-22.2 Port Config

This page allows you to configure the basic GVRP Configuration settings for all switch ports. The settings relate to the currently selected unit, as reflected by the page header.

Web Interface

To configure the GVRP in the web interface:

1. Click Configuration, GVRP and Port Config
2. Evoke to enable or disable the Mode.
3. Click apply 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.

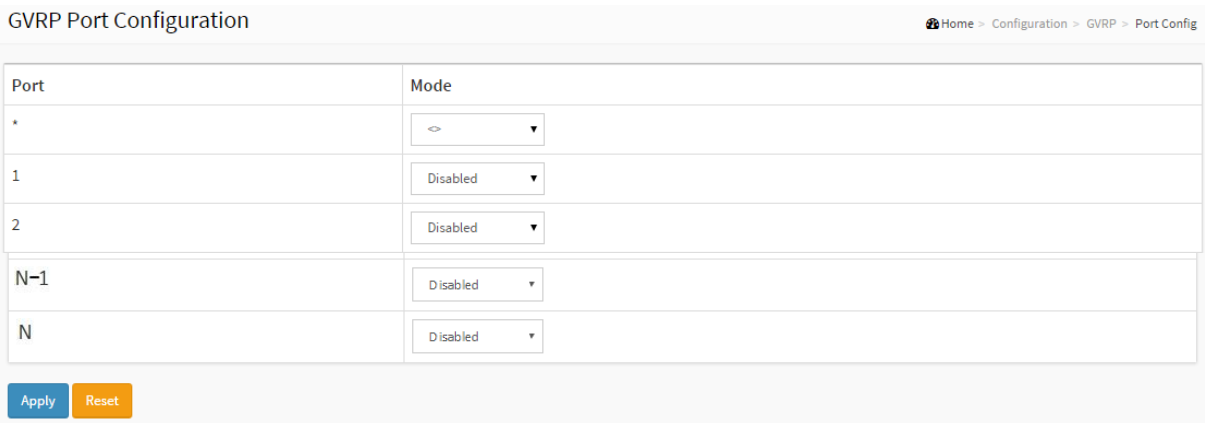


Figure 2-22.2: The GVRP Configuration

Parameter description:

- **Port :**

  The Port column shows the list of ports.

- **Mode :**

  This configuration is to enable/disable GVRP Mode on particular port locally.

  Disable: Select to Disable GVRP mode on this port.
  GVRP Enable: Select to Enable GVRP mode on this port.

Buttons

- **Apply :**

  Click to save changes.

- **Reset :**

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

2-23 sFlow

The sFlow Collector configuration for the switch can be monitored and modified here. The configuration is divided into two parts: Configuration of the sFlow receiver (a.k.a. sFlow collector) and configuration of per-port flow and counter samplers.

sFlow configuration is not persisted to non-volatile memory, which means that a reboot or master change will disable sFlow sampling.

Web Interface

To configure the sFlow in the web interface:

1. Click Configuration and sFlow.
2. Set the parameters.
3. Click apply 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.

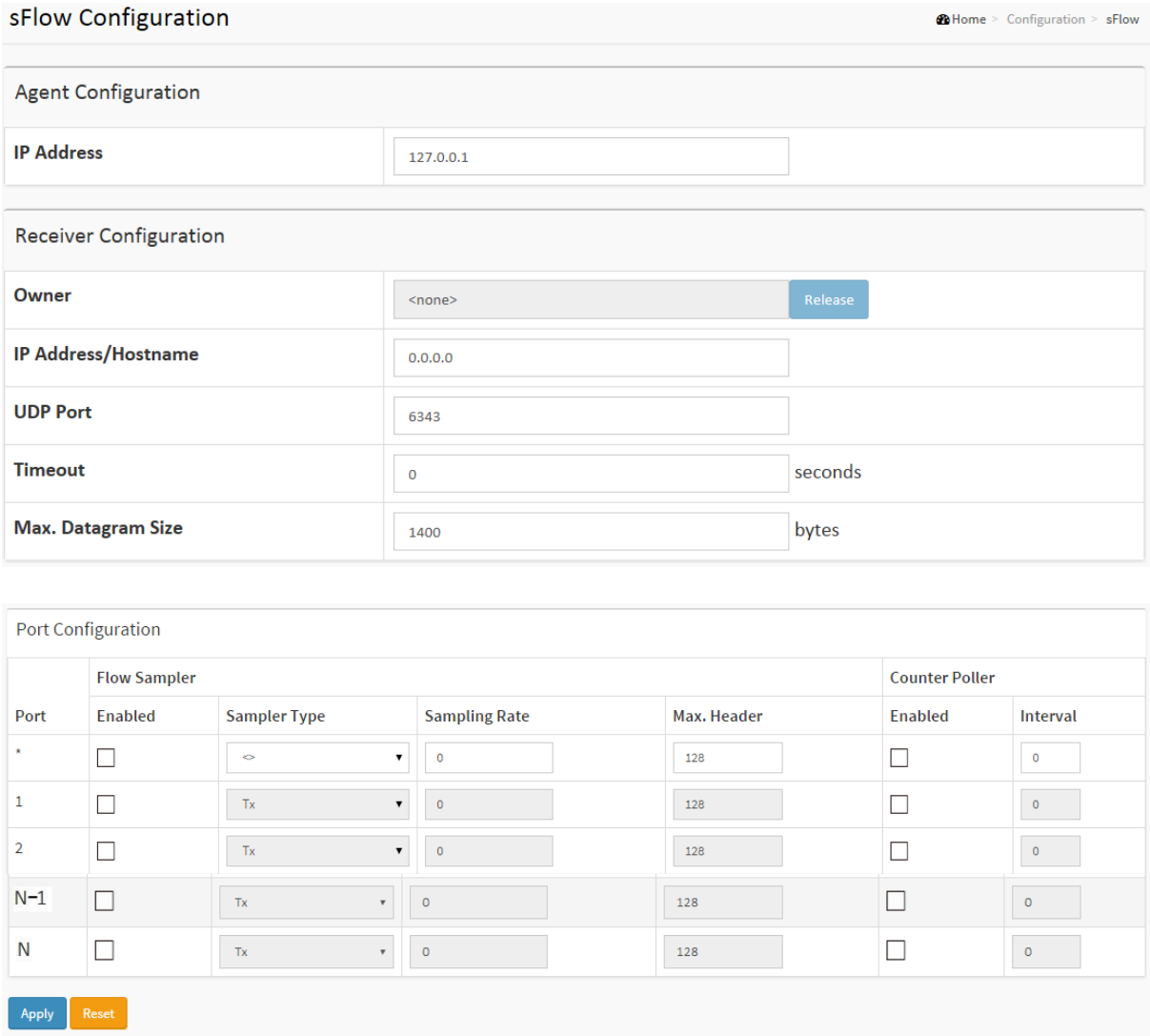


Figure 2-23: The sFlow Configuration

Parameter description:

Agent Configuration

- **IP Address :**

  The IP address used as Agent IP address in sFlow datagrams. It serves as a unique key that will identify this agent over extended periods of time.

  Both IPv4 and IPv6 addresses are supported.

Receiver Configuration

- **Owner :**

  Basically, sFlow can be configured in two ways: Through local management using the Web or CLI interface or through SNMP. This read-only field shows the owner of the current sFlow configuration and assumes values as follows:
  • If sFlow is currently unconfigured/unclaimed, Owner contains <none>.
  • If sFlow is currently configured through Web or CLI, Owner contains <Configured through local management>.
  • If sFlow is currently configured through SNMP, Owner contains a string identifying the sFlow receiver.
  If sFlow is configured through SNMP, all controls - except for the Release-button - are disabled to avoid inadvertent reconfiguration.

  The Release button allows for releasing the current owner and disable sFlow sampling. The button is disabled if sFlow is currently unclaimed. If configured through SNMP, the release must be confirmed (a confirmation request will appear).

- **IP Address/Hostname :**

  The IP address or hostname of the sFlow receiver. Both IPv4 and IPv6 addresses are supported.

- **UDP Port :**

  The UDP port on which the sFlow receiver listens to sFlow datagrams. If set to 0 (zero), the default port (6343) is used.

- **Timeout :**

  The number of seconds remaining before sampling stops and the current sFlow owner is released. While active, the current time left can be updated with a click on the Refresh-button. If locally managed, the timeout can be changed on the fly without affecting any other settings.

- **Max. Datagram Size :**

  The maximum number of data bytes that can be sent in a single sample datagram. This should be set to a value that avoids fragmentation of the sFlow datagrams. Valid range is 200 to 1468 bytes with default being 1400 bytes.

Port Configuration

- **Port :**

  The port number for which the configuration below applies.

- **Flow Sampler Enabled :**

Enables/disables flow sampling on this port.

- **Flow Sampler Sampling Rate :**

  The statistical sampling rate for packet sampling. Set to N to sample on average 1/Nth of the packets transmitted/received on the port.
  Not all sampling rates are achievable. If an unsupported sampling rate is requested, the switch will automatically adjust it to the closest achievable. This will be reported back in this field.

- **Flow Sampler Max. Header :**

  The maximum number of bytes that should be copied from a sampled packet to the sFlow datagram. Valid range is 14 to 200 bytes with default being 128 bytes.
  If the maximum datagram size does not take into account the maximum header size, samples may be dropped.

- **Counter Poller Enabled :**

  Enables/disables counter polling on this port.

- **Counter Poller Interval :**

  With counter polling enabled, this specifies the interval - in seconds - between counter poller samples.

Buttons

- **Apply :**

  Click to save changes.

- **Reset :**

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

- **Release :**

  See description under Owner.

- **Refresh :**

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

2-24 SMTP

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.

Web Interface

To configure the SMTP Configuration in the web interface:

1. Click Configuration, SMTP Configuration
2. Scroll to select the Severity Level
3. Specify the parameters in each blank field.
4. Click the apply 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

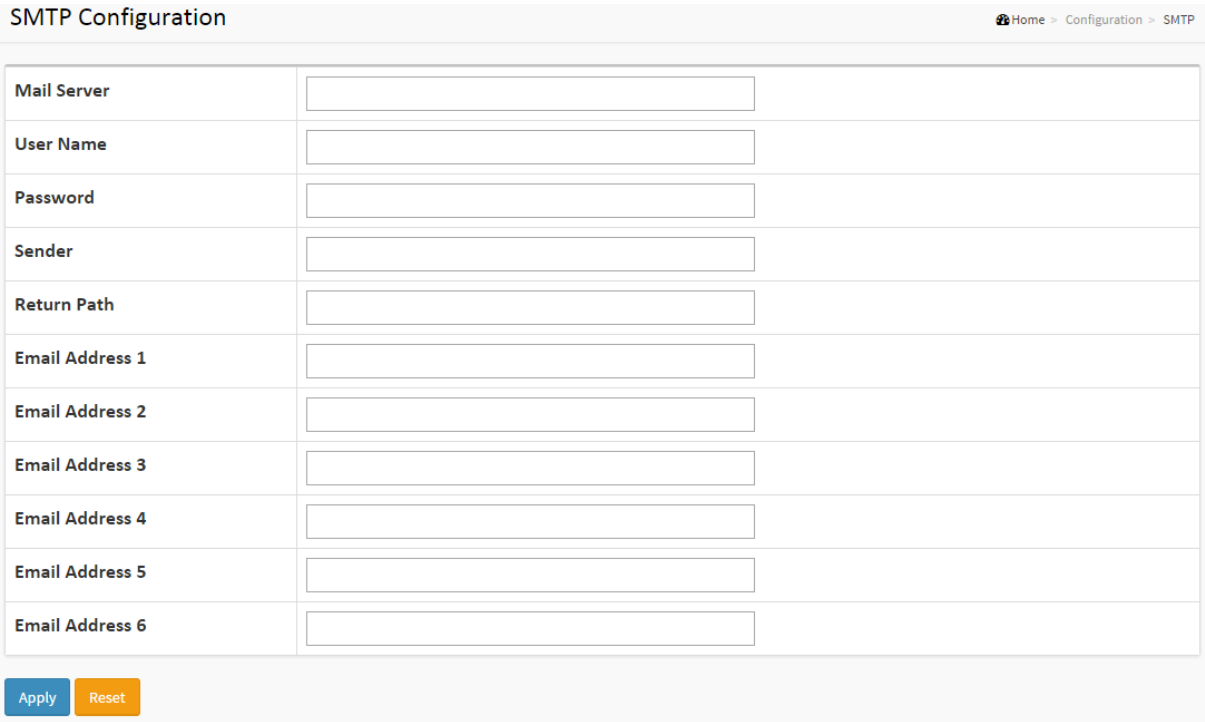


Figure 2-25: The SMTP Configuration

Parameter description:

These parameters are displayed on the SMTP Configuration page:

- **Mail Server :**

  Specify the IP Address of the server transferring your email.

- **User name :**

  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 would like to receive the alarm message.

Buttons

- **Apply :**

  Click to save changes.

- **Reset :**

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

Chapter 3 Monitor

This chapter describes all of the basic network statistics which includes the Ports, Layer 2 network protocol (e.g. NAS, ACL, DHCP, AAA and RMON etc.) and any setting of the Switch.

3-1 System

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", "Location", "System Up Time", "Firmware Version", "Host Mac Address", "Device Port". 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.

3-1.1 Information

The switch system information is provided here.

Web interface

To display System Information in the web interface:

1. Click Monitor, System and Information.
2. Check the contact information for the system administrator as well as the name and location of the switch. Also indicate the local time zone by configuring the appropriate offset.
3. Click the "Refresh"

System Information

Home > Monitor > System > Information

Model Name	
System Description	N-Port L2+ Managed PoE Switch
Location	
Contact	
System Name	
System Date	2011-01-01T00:22:52+00:00
System Uptime	00:22:52
Bootloader Version	v1.15f
Firmware Version	v6.54.2343 2017-01-09
Hardware Version	v1.01
Mechanical Version	v1.01
Serial Number	A055116AR5000001
MAC Address	00-40-c7-1c-a0-f8
Memory	Total=76584 KBytes, Free=52000 KBytes, Max=51433 KBytes
FLASH	0x40000000-0x41fffff, 512 x 0x10000 blocks
CPU Load (100ms, 1s, 10s)	39%, 13%, 9%

Figure 3-1.1: System Information

Parameter description:

- **Model Name :**

  Displays the factory defined model name for identification purpose.

- **System Description :**

  Displays the system description.

- **Location :**

  The system location configured in Configuration | System | Information | System Location.

- **Contact :**

  The system contact configured in Configuration | System | Information | System Contact.

- **System Name :**

  Displays the user-defined system name that configured in System | System Information | Configuration | System Name.

- **System Date :**

  The current (GMT) system time and date. The system time is obtained through the Timing server running on the switch, if any.

- **System Uptime :**

  The period of time the device has been operational.

- **Bootloader Version :**

  Displays the current boot loader version number.

- **Firmware Version :**

  Displays the current firmware version number.

- **Hardware Version :**

Displays the hardware version of the device.

- **Mechanical Version :**

  Displays the mechanical version of the device.

- **Serial Number :**

  Displays the unique serial number that assigned to the device.

- **MAC Address :**

  The MAC Address of this switch.

- **Memory :**

  Displays the memory size of the system.

- **FLASH :**

  Displays the flash size of the system.

- **CPU Load (100ms, 1s, 10s) :**

  Displays the cpu loading (100ms, 1s, 10s) of the system.

3-1.2 IP Status

This page displays the status of the IP protocol layer. The status is defined by the IP interfaces, the IP routes and the neighbour cache (ARP cache) status.

Web Interface

To display the log configuration in the web interface:

1. Click Monitor, System and IP Status.
2. Display the IP address information.

IP Interfaces

Home > Monitor > System > IP Status

Auto-refresh

IP Interfaces

Interface	Type	Address	Status
VLAN1	LINK	00-40-c7-26-24-01	<UP BROADCAST RUNNING MULTICAST>
VLAN1	IPv4	192.168.1.1/24	
VLAN1	IPv4	169.254.0.1/16	
VLAN1	IPv6	fe80::240:c7ff:fe26:2401/64	
VLAN4096	LINK	00-40-c7-26-24-01	<BROADCAST MULTICAST>
VLAN4097	LINK	00-40-c7-26-24-01	<BROADCAST MULTICAST>

IP Routes

Network	Gateway	Status
0.0.0.0/0	192.168.1.254	<UP GATEWAY HW_RT>
127.0.0.0/8	127.0.0.1	<UP>
127.0.0.1/32	127.0.0.1	<UP HOST>
169.254.0.0/16	VLAN1	<UP HW_RT>
192.168.1.0/24	VLAN1	<UP HW_RT>
::1/128	::1	<UP HOST>

Neighbour cache

IP Address	Link Address
192.168.1.1	VLAN1:00-40-c7-26-24-01
192.168.1.123	VLAN1:00-e0-4c-68-01-45
fe80::240:c7ff:fe26:2401	VLAN1:00-40-c7-26-24-01

DNS Server

Type	IP Address	Interface
Static	8.8.8.8	

Figure 3-1.2: The IP Status

Parameter description:

IP Interfaces

- **Interface :**

  Show the name of the interface.

- **Type :**

  Show the address type of the entry. This may be LINK or IPv4.

- **Address :**

  Show the current address of the interface (of the given type).

- **Status :**

  Show the status flags of the interface (and/or address).

IP Routes

- **Network :**

  Show the destination IP network or host address of this route.

- **Gateway :**

  Show the gateway address of this route.

- **Status :**

  Show the status flags of the route.

Neighbour cache

- **IP Address :**

  Show the IP address of the entry.

- **Link Address :**

  Show the Link (MAC) address for which a binding to the IP address given exist.

Buttons

- **Auto-refresh :**

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

- **Refresh :**

  Click to refresh the page immediately.

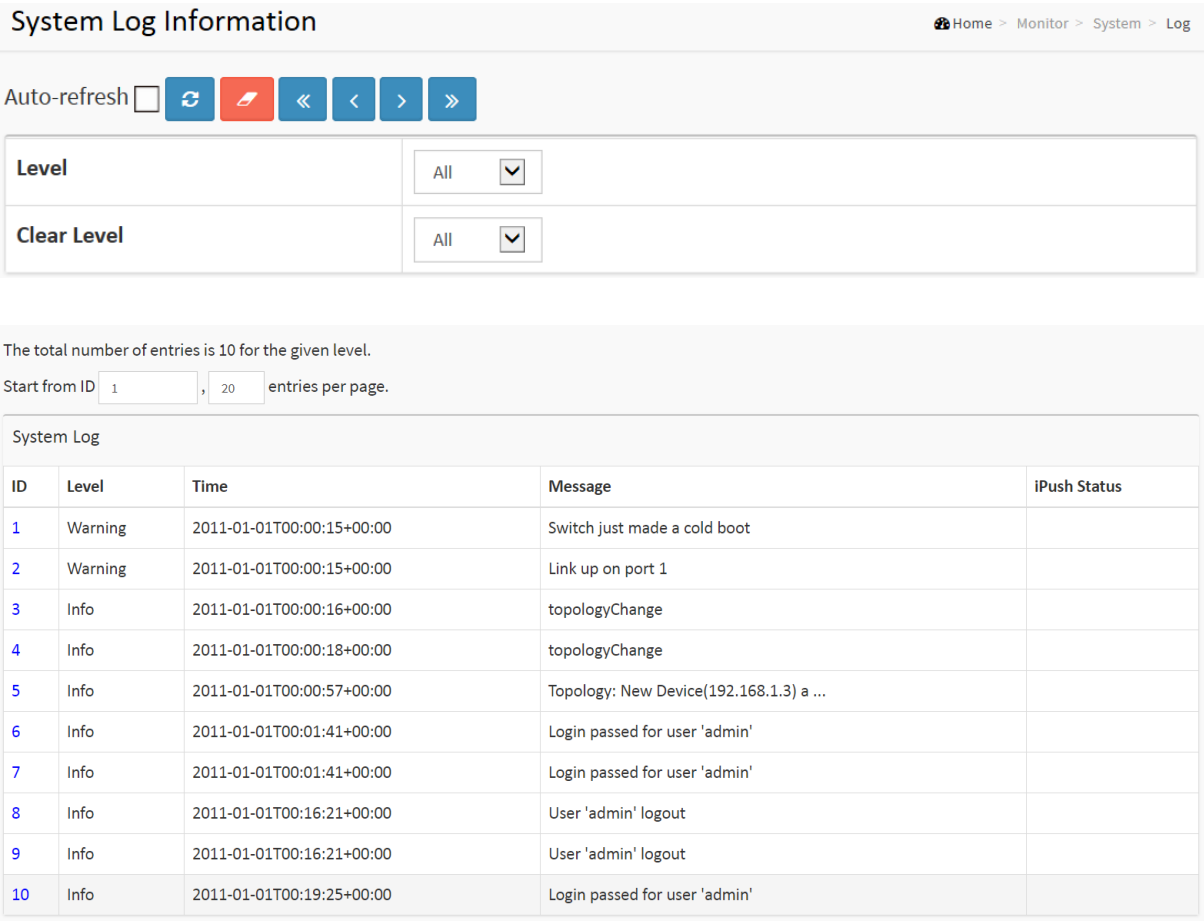
3-1.3 Log

The switch system log information is provided here.

Web Interface

To display the log configuration in the web interface:

1. Click Monitor, System and Log.
2. Display the system log information.



ID	Level	Time	Message	iPush Status
1	Warning	2011-01-01T00:00:15+00:00	Switch just made a cold boot	
2	Warning	2011-01-01T00:00:15+00:00	Link up on port 1	
3	Info	2011-01-01T00:00:16+00:00	topologyChange	
4	Info	2011-01-01T00:00:18+00:00	topologyChange	
5	Info	2011-01-01T00:00:57+00:00	Topology: New Device(192.168.1.3) a ...	
6	Info	2011-01-01T00:01:41+00:00	Login passed for user 'admin'	
7	Info	2011-01-01T00:01:41+00:00	Login passed for user 'admin'	
8	Info	2011-01-01T00:16:21+00:00	User 'admin' logout	
9	Info	2011-01-01T00:16:21+00:00	User 'admin' logout	
10	Info	2011-01-01T00:19:25+00:00	Login passed for user 'admin'	

Figure 3-1.3: The System Log Information

Parameter description:

- **ID :**

  The identification of the system log entry.

- **Level :**

  The level of the system log entry.

  Emerg: The system log entry is belonged emergency level.

  Alert: The system log entry is belonged alert level.

  Crit: The system log entry is belonged critical level.

Error: The system log entry is belonged error level.

Warning: The system log entry is belonged warning level.

Notice: The system log entry is belonged notice level.

Info: The system log entry is belonged information level.

Debug: The system log entry is belonged debug level.

- **Time :**

  The occurred time of the system log entry.

- **Message :**

  The detail message of the system log entry.

- **iPush Status :**

  The status of sending this syslog to iPush server.

Buttons

- **Auto-refresh :**

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

- **Refresh :**

  Click to refresh the page immediately.

- **Clear :**

  Flushes the selected log entries.

- **:**

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

- **:**

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

- **:**

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

- **:**

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

3-1.4 Detailed Log

The switch system detailed log information is provided here.

Web Interface

To display the detailed log configuration in the web interface:

1. Click Monitor, System and Detailed Log.
2. Display the log information.

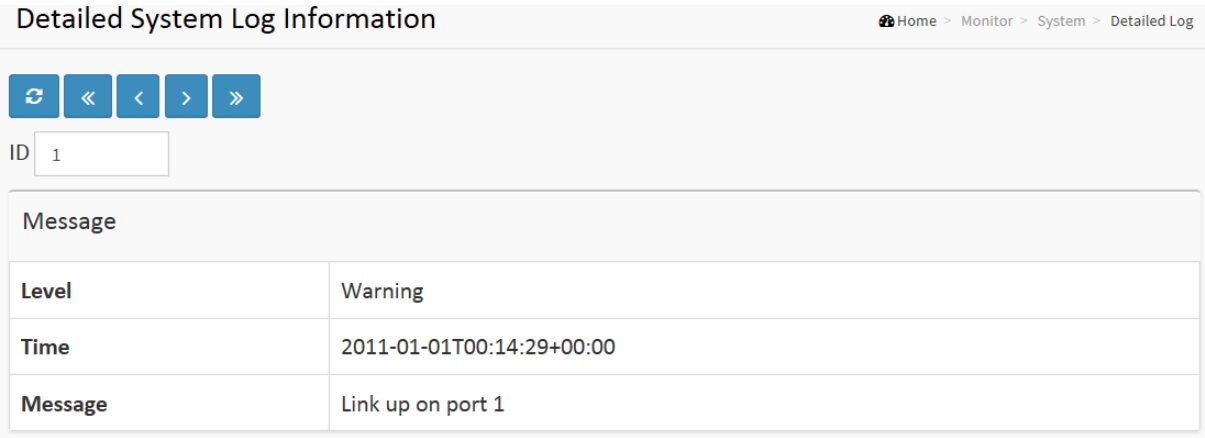


Figure 3-1.4: The Detailed System Log Information

Parameter description:

- **ID :**

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

- **Message :**

  The detailed message of the system log entry.

  Buttons

- **Refresh :**

  Updates the system log entry to the current entry ID.

- **:**

  Updates the system log entry to the first available entry ID.

- **:**

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

- **:**

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

- **:**

  Updates the system log entry to the last available entry ID.

3-1.5 Overview

The switch system overview is provided here.

Web Interface

To display the switch system overview in the web interface:

1. Click Monitor, System and Detailed Log.
2. Display the switch system overview.

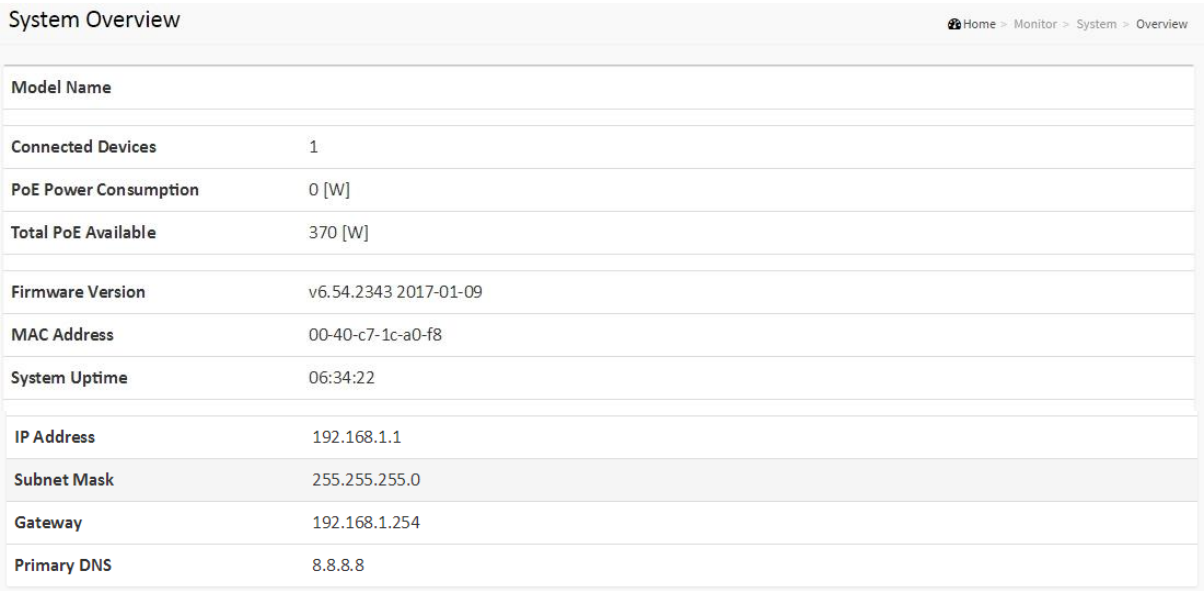


Figure 3-1.5: The System Overview

Parameter description:

- **Model Name :**

  Displays the factory defined model name for identification purpose.

- **Connected Devices :**

  Total of currently connected devices.

- **PoE Power Consumption :**

  Current PoE power consumption.

- **Total PoE Available :**

  Total PoE Budget availability.

- **Firmware Version :**

  Displays the current firmware version number.

- **MAC Address :**

  The MAC Address of this switch.

- **System Uptime :**

  The period of time the device has been operational.

- **IP Address :**

  The IPv4 or IPv6 address of the interface.

- **Subnet Mask :**

  The IPv4 or IPv6 network mask of the interface.

- **Gateway :**

  The IP address of the IP gateway.

- **Primary DNS :**

  The IP address of the DNS Server.

3-2.1 Port Power Savings

This page provides the current status for EEE.

Web Interface

To display the switch system overview in the web interface:

1. Click Monitor, Green Ethernet and Port Power Savings.
2. Display the Port Power Saving Status.

Port Power Savings Status

Home > Monitor > Green Ethernet > Port Power Savings

Auto-refresh

Port	Link	EEE	LP EEE Cap	EEE Savings
1	●	✖	✔	✖
2	●	✖	✖	✖
N-2	●	✖	✖	✖
N-1	●	✖	✖	✖
N	●	✖	✖	✖

Figure 3-2.1: The Port Power Saving Status

Parameter description:

- **Local Port :**

  This is the logical port number for this row.

- **Link :**

  Shows if the link is up for the port (green = link up, red = link down).

- **EEE :**

  Shows if EEE is enabled for the port (reflects the settings at the Port Power Savings configuration page).

- **LP EEE cap :**

  Shows if the link partner is EEE capable.

- **EEE Savings :**

  Shows if the system is currently saving power due to EEE. When EEE is enabled, the system will powered down if no frame has been received or transmitted in 5 uSec.

Buttons

- **Auto-refresh :**

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

- **Refresh :** Click to refresh the page.

3-3 Ports

The section describes 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.

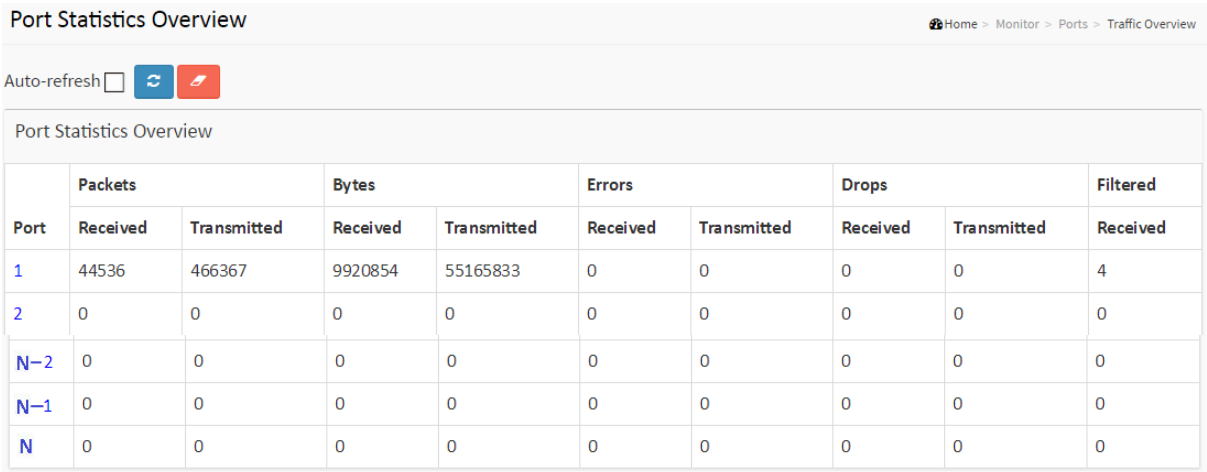
3-3.1 Traffic Overview

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

Web Interface

To Display the Port Statistics Overview in the web interface:

1. Click Monitor, Port and 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".



	Packets		Bytes		Errors		Drops		Filtered
Port	Received	Transmitted	Received	Transmitted	Received	Transmitted	Received	Transmitted	Received
1	44536	466367	9920854	55165833	0	0	0	0	4
2	0	0	0	0	0	0	0	0	0
N−2	0	0	0	0	0	0	0	0	0
N−1	0	0	0	0	0	0	0	0	0
N	0	0	0	0	0	0	0	0	0

Figure 3-3.1: The Port Statistics Overview

Parameter description:

- **Port :**

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

- **Packets :**

  The number of received and transmitted packets per port.

- **Bytes :**

  The number of received and transmitted bytes per port.

- **Errors :**

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

- **Drops :**

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

- **Filtered :**

  The number of received frames filtered by the forwarding

Buttons

- **Auto-refresh :**

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

- **Refresh :**

  Click to refresh the page.

- **Clear :**

  Flushes the selected log entries.

3-3.2 Qos Statistics

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

Web Interface

To Display the Queuing Counters in the web interface:

1. Click Monitor, Ports and QoS Statistics
2. If you want to auto-refresh the information then you need to evoke the "Auto-refresh".
3. Click "Refresh" to refresh the Queuing Counters or clear all information when you click "Clear".

Queuing Counters

Home > Monitor > Ports > QoS Statistics

Auto-refresh

	Q0		Q1		Q2		Q3		Q4		Q5		Q6		Q7	
Port	Rx	Tx	Rx	Tx	Rx	Tx	Rx	Tx	Rx	Tx	Rx	Tx	Rx	Tx	Rx	Tx
1	44725	0	0	0	0	0	0	0	0	0	0	0	0	0	0	467753
2	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
N−2	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
N−1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
N	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0

Figure 3-3.2: The Queuing Counters Overview

Parameter description:

- **Port :**

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

- **Qn :**

  Qn is the Queue number, There are 8 QoS queues per port. Q0 is the lowest priority queue.

- **Rx/Tx :**

  The number of received and transmitted packets per queue.

Buttons

- **Auto-refresh :**

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

- **Refresh :**

  Click to refresh the page.

- **Clear :**

  Flushes the selected log entries.

3-3.3 QCL Status

The section will let you know how to configure and shows the QCL status by different QCL users. Each row describes the QCE that is defined. It is a conflict if a specific QCE is not applied to the hardware due to hardware limitations. The maximum number of QCEs is 256 on each switch.

Web Interface

To display the QoS Control List Status in the web interface:

1. Click Monitor, Ports and QCL Status
2. If you want to auto-refresh the information then you need to evoke the "Auto-refresh".
3. Scroll to select the combined, static, Voice VLAN and conflict.
4. To click the "Refresh" to refresh an entry of the MVR Statistics Information.

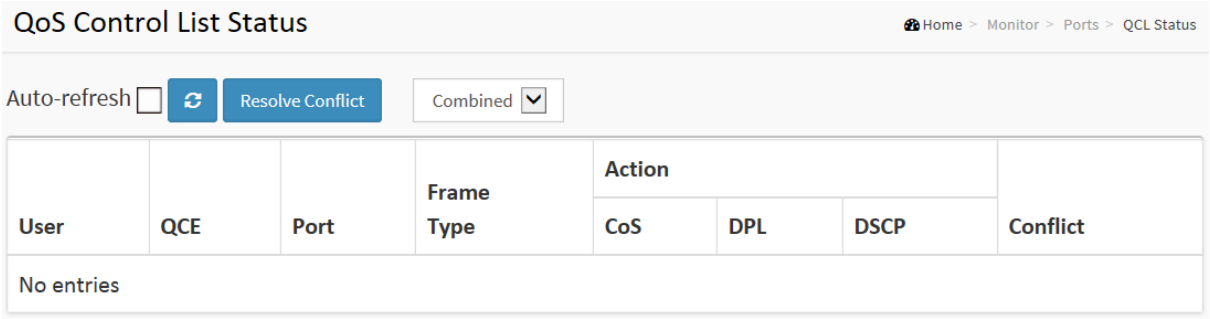


Figure 3-3.3: The QoS Control List Status

Parameter description:

- **User :**

  Indicates the QCL user.

- **QCE :**

  Indicates the index of QCE.

- **Port :**

  Indicates the list of ports configured with the QCE.

- **Frame Type :**

  Indicates the type of frame to look for incoming frames. Possible frame types are:

  Any: The QCE will match all frame 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.

- **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.

- **Conflict :**

  Displays Conflict status of QCL entries. 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 H/W resources required to add QCL entry on pressing 'Resolve Conflict' button.

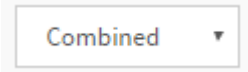
Buttons

- **Auto-refresh :**

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

- **Refresh :**

  Click to refresh the page.

- 

Combined :

  Select the QCL status from this drop down list.

-

Resolve Conflict :

  Click to release the resources required to add QCL entry, in case the conflict status for any QCL entry is 'yes'.

3-3.4 Detailed Statistics

The section describes how to provide 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.

Web Interface

To Display per port detailed Statistics Overview in the web interface:

1. Click Monitor, Ports and Detailed Port Statistics
2. Scroll the Port Index to select which port you want to show the detailed
3. Port statistics overview.
4. If you want to auto-refresh the information then you need to evoke the "Auto-refresh".
5. Click "Refresh" to refresh the port detailed statistics or clear all information when you click "Clear".

Detailed Port Statistics Port 1 Home > Monitor > Ports > Detailed Statistics

Auto-refresh Port 1

Receive Total		Transmit Total	
Rx Packets	56754	Tx Packets	39099
Rx Octets	8138095	Tx Octets	16948240
Rx Unicast	36253	Tx Unicast	26422
Rx Multicast	8263	Tx Multicast	12673
Rx Broadcast	12238	Tx Broadcast	4
Rx Pause	0	Tx Pause	0

Receive Size Counters		Transmit Size Counters	
Rx 64 Bytes	34048	Tx 64 Bytes	871
Rx 65-127 Bytes	7938	Tx 65-127 Bytes	12926
Rx 128-255 Bytes	5161	Tx 128-255 Bytes	9476
Rx 256-511 Bytes	9176	Tx 256-511 Bytes	7900
Rx 512-1023 Bytes	431	Tx 512-1023 Bytes	42
Rx 1024-1526 Bytes	0	Tx 1024-1526 Bytes	7884
Rx 1527- Bytes	0	Tx 1527- Bytes	0

Receive Queue Counters		Transmit Queue Counters	
Rx Q0	56754	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	39099

Receive Error Counters		Transmit Error Counters	
Rx Drops	0	Tx Drops	0
Rx CRC/Alignment	0	Tx Late/Exc. Coll.	0
Rx Undersize	0		
Rx Oversize	0		
Rx Fragments	0		
Rx Jabber	0		
Rx Filtered	4614		

Figure 3-3.4: The Detailed Port Statistics

Parameter description:

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 :**

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

- **Refresh :**

  Click to refresh the page.

- **Clear :**

  Flushes the selected log entries.

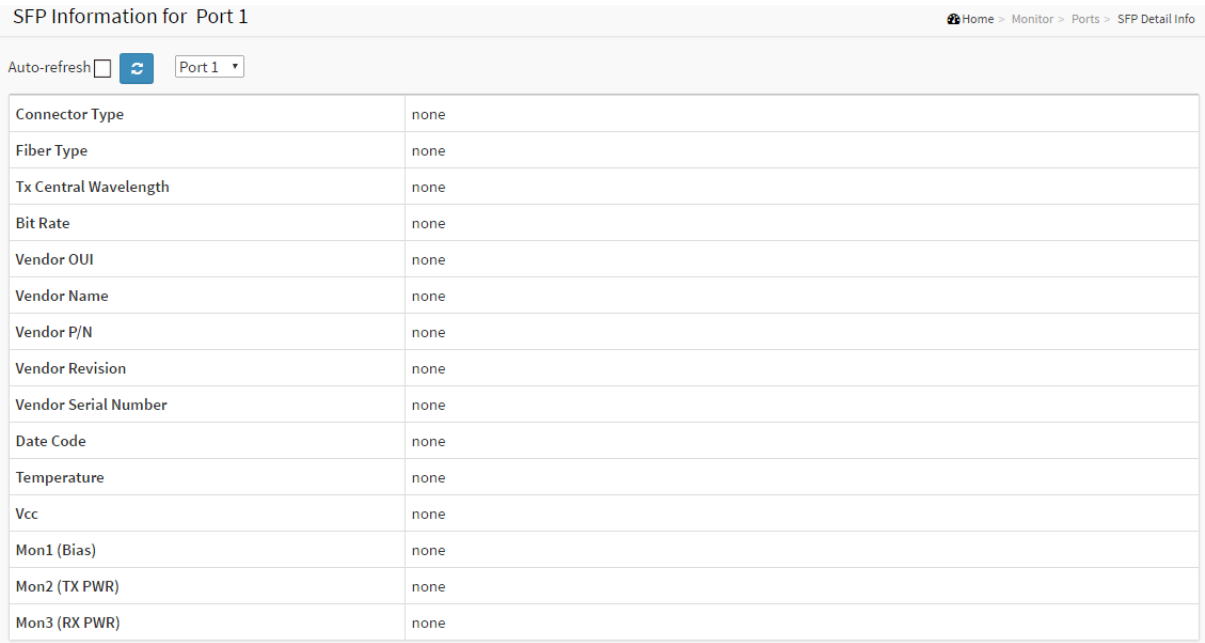
3-3.5 SFP Detail Info

This page displays general SFP information and monitoring information.

Web Interface

To Display the SFP information in the web interface:

1. Click Monitor, Ports and SFP Detail Info.
2. To display the SFP Information.



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

Figure 3-3.5: The SFP Detail Information

Parameter description:

- **Connector Type :**

  Display the connector type, for instance, UTP, SC, ST, LC and so on.

- **Fiber Type :**

  Display the fiber mode, for instance, Multi-Mode, Single-Mode.

- **Tx Central Wavelength :**

  Display the fiber optical transmitting central wavelength, for instance, 850nm, 1310nm, 1550nm and so on.

- **Bit Rate :**

  Displays the nominal bit rate of the transceiver.

- **Vendor OUI :**

  Display the Manufacturer's OUI code which is assigned by IEEE.

- **Vendor Name :**

  Display the company name of the module manufacturer.

- **Vendor P/N :**

  Display the product name of the naming by module manufacturer.

- **Vendor Rev (Revision) :**

  Display the module revision.

- **Vendor SN (Serial Number) :**

  Show the serial number assigned by the manufacturer.

- **Date Code :**

  Show the date this SFP module was made.

- **Temperature :**

  Show the current temperature of SFP module.

- **Vcc :**

  Show the working DC voltage of SFP module.

- **Mon1(Bias) mA :**

  Show the Bias current of SFP module.

- **Mon2(TX PWR) :**

  Show the transmit power of SFP module.

- **Mon3(RX PWR) :**

  Show the receiver power of SFP module.

Buttons

- **Auto-refresh :**

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

- **Refresh :**

  Click to refresh the page.

3-4 DHCP

3-4.1 Server

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

3-4.1.1 Statistics

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

Web Interface

To display the DHCP server Statistics Overview in the web interface:

1. Click DHCP, Server and Statistics.
2. To display the DHCP Server Statistics.

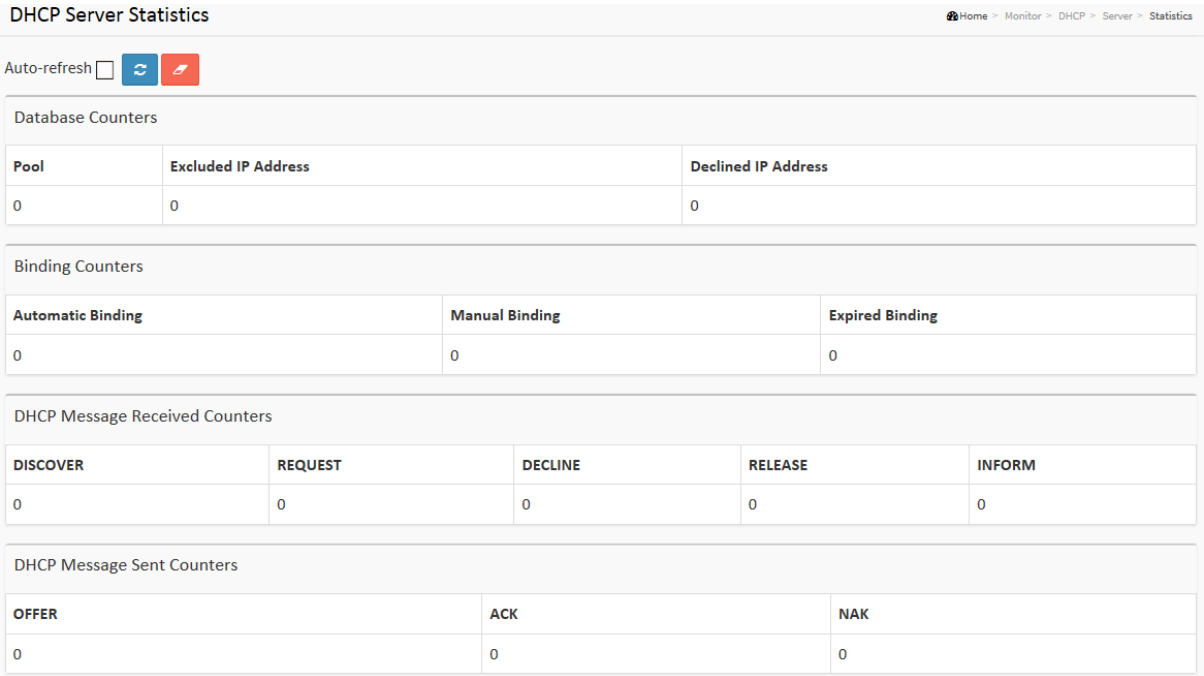


Figure 3-4.1.1: The DHCP Server Statistics

Parameter description:

Database Counters

Display counters of various databases.

- **Pool :**

  Number of pools.

- **Excluded IP Address :**

  Number of excluded IP address ranges.

- **Declined IP Address :**

  Number of sec lined IP addresses.

Binding Counters

Display counters of various databases

- **Automatic Binding :**

  Number of bindings with network-type pools.

- **Manual Binding :**

  Number of bindings that administrator assigns an IP address to a client. That is, the pool is of host type.

- **Expired Binding :**

  Number of bindings that their lease time expired or they are cleared from Automatic/Manual type bindings.

DHCP Message Received Counters

Display counters of DHCP messages received by DHCP server.

- **DISCOVER :**

  Number of DHCP DISCOVER messages received.

- **REQUEST :**

  Number of DHCP REQUEST messages received.

- **DECLINE :**

  Number of DHCP DECLINE messages received.

- **RELEASE :**

  Number of DHCP RELEASE messages received.

- **INFORM :**

  Number of DHCP INFORM messages received.

DHCP Message Sent Counters

Display counters of DHCP messages sent by DHCP server.

- **OFFER :**

  Number of DHCP OFFER messages sent.

- **ACK :**

  Number of DHCP ACK messages sent.

- **NAK :**

  Number of DHCP NAK messages sent.

Buttons

- **Auto-refresh :**

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

- **Refresh :**

  Click to refresh the page.

- **Clear :** Flushes the selected log entries.

This page displays bindings generated for DHCP clients.

Web Interface

To Display DHCP Server Binding IP in the web interface:

1. Click DHCP, Server and Binding.
2. To display the DHCP Server Binding IP.

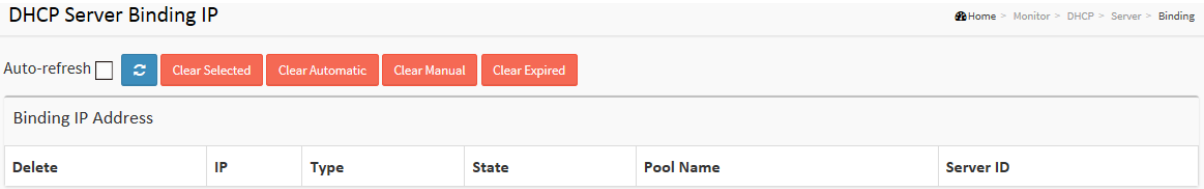


Figure 3-4.1.2: The DHCP Server Binding IP

Parameter description:

Binding IP Address

Display all bindings.

- **IP :**

  IP address allocated to DHCP client.

- **Type :**

  Type of binding. Possible types are Automatic, Manual, and Expired.

- **State :**

  State of binding. Possible states are Committed, Allocated, and Expired.

- **Pool Name :**

  The pool that generates the binding.

- **Server ID :**

  Server IP address to service the binding.

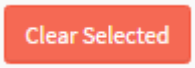
Buttons

- **Auto-refresh :**

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

- **Refresh :**

  Click to refresh the page.

- 

Clear Selected :

  Click to clear selected bindings. If the selected binding is Automatic or Manual, then it is

changed to be Expired. If the selected binding is Expired, then it is freed.

- Clear Automatic **Clear Automatic :**

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

- Clear Manual **Clear Manual :**

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

- Clear Expired **Clear Expired :**

  Click to clear all Expired bindings and free them.

This page displays declined IP addresses.

Web Interface

To Display DHCP Server Declined IP in the web interface:

1. Click DHCP, Server and Declined IP.
2. To display the DHCP Declined IP.

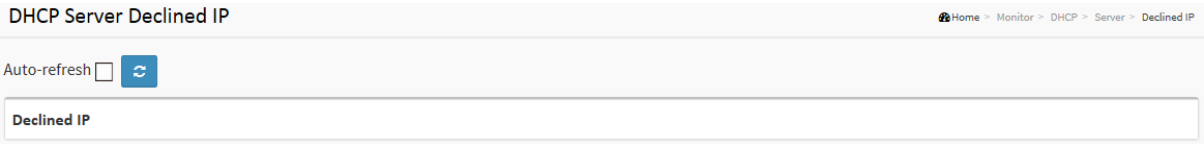


Figure 3-4.1.3: The Declined IP

Parameter description:

Declined IP Addresses

Display IP addresses declined by DHCP clients.

- **Declined IP :**

  List of IP addresses declined.

Buttons

- **Auto-refresh :**

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

- **Refresh :**

  Click to refresh the page.

3-4.2 Snooping Table

This page display the dynamic IP assigned information after DHCP Snooping mode is disabled. All DHCP clients obtained the dynamic IP address from the DHCP server will be listed in this table except for local VLAN interface IP addresses. Entries in the Dynamic DHCP snooping Table are shown on this page.

Web Interface

To display the DHCP in the web interface:

1. Click Monitor, DHCP and Snooping table
2. To display Dynamic DHCP Snooping Table.

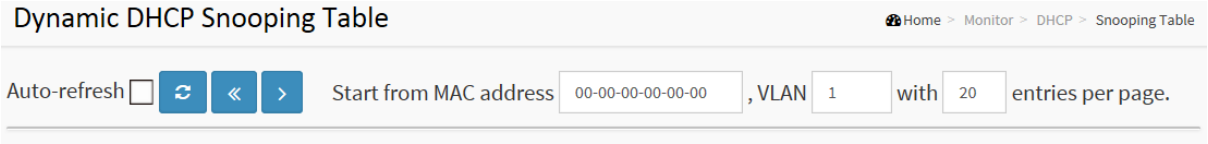


Figure 3-4.2: The DHCP snooping table

Parameter description:

DHCP snooping Table Columns

- **MAC Address :**

  User MAC address of the entry.

- **VLAN ID :**

  VLAN-ID in which the DHCP traffic is permitted.

- **Source Port:**

  Switch Port Number for which the entries are displayed.

- **IP Address :**

  User IP address of the entry.

- **IP Subnet Mask :**

  User IP subnet mask of the entry.

- **DHCP Server Address :**

  DHCP Server address of the entry.

Buttons

- **Auto-refresh :**

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

- **Refresh :**

  Refreshes the displayed table starting from the input fields.

- **:**

Updates the table starting from the first entry in the Dynamic DHCP snooping Table.

- :

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

3-4.3 Relay Statistics

This page provides statistics for DHCP relay.

Web Interface

To monitor a DHCP Relay statistics in the web interface:

1. Click Monitor, DHCP and Relay Statistics
2. To display DHCP relay statistics.

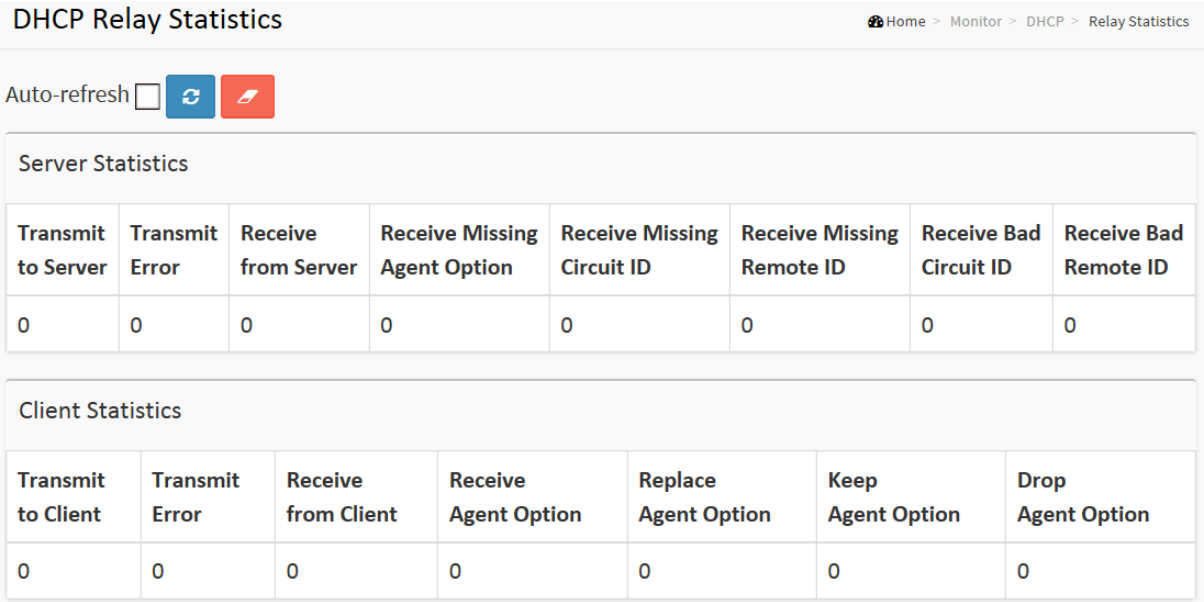


Figure 3-4.3: The DHCP relay statistics

Parameter description:

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 this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.

- **Refresh :**

  Click to refresh the page.

- **Clear :**

  Flushes the selected log entries.

3-4.4 Detailed Statistics

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

Web Interface

To display monitor DHCP Relay statistics in the web interface:

1. Click Monitor, DHCP and Detailed Statistics
2. To display DHCP relay statistics.

DHCP Detailed Statistics Port 1

Home > Monitor > DHCP > Detailed Statistics

Auto-refresh Combined 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
Rx Discarded Checksum Error	0		
Rx Discarded from Untrusted	0		

Figure 3-4.4: The DHCP Detailed Statistics

Parameter description:

Server Statistics

- **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

- **Rx and Tx Lease Active:**

  The number of lease active (option 53 with value 13) packets received and transmitted.

- **Rx Discarded checksum error:**

  The number of discard packet that IP/UDP checksum is error.

- **Rx Discarded from Untrusted:**

  The number of discarded packet that are coming from untrusted port.

Buttons

- **Auto-refresh :**

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

- **Refresh :**

  Click to refresh the page.

- **Clear :**

  Flushes the selected log entries.

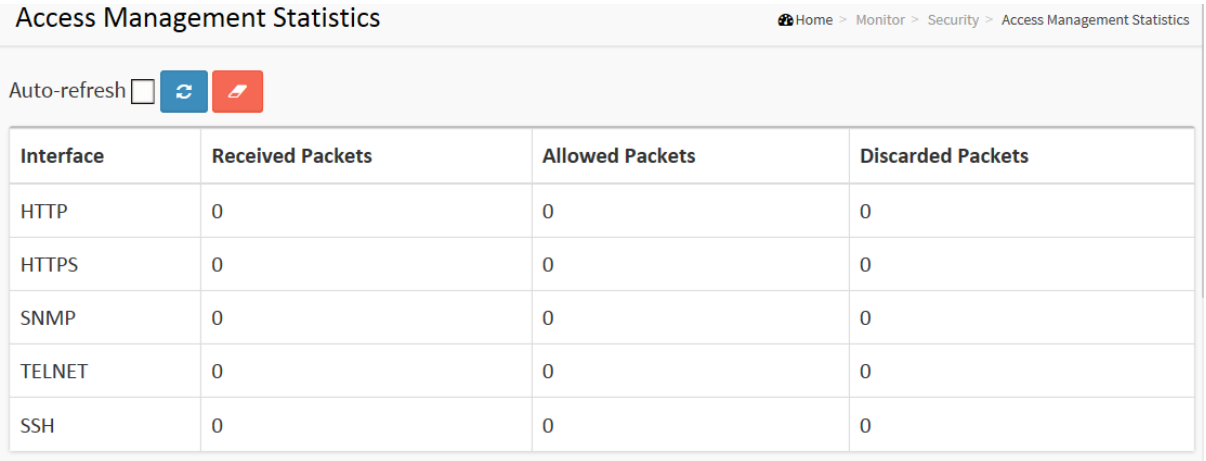
3-5.1 Access Management Statistics

This section shows you a detailed statistics of the Access Management including HTTP, HTTPS, SSH. TELNET, and SSH.

Web Interface

To display the Assess Management Statistics in the web interface:

1. Click Security, Access Management Statistics.
2. Checked "Auto-refresh".
3. Click "Refresh" to refresh the port detailed statistics or clear all information when you click "Clear".



Interface	Received Packets	Allowed Packets	Discarded Packets
HTTP	0	0	0
HTTPS	0	0	0
SNMP	0	0	0
TELNET	0	0	0
SSH	0	0	0

Figure 3-5.1: The Access Management Statistics

Parameter description:

- **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 :**

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

- **Refresh :**

  Click to refresh the page.

- **Clear :**

  Flushes the selected log entries.

3-5.2 Network

3-5.2.1 Port Security

3-5.2.1.1 Switch

This section shows the Port Security status. Port Security is a module with no direct configuration. Configuration comes indirectly from other modules - the user modules. When a user module has enabled port security on a port, the port is set-up for software-based learning. In this mode, frames from unknown MAC addresses are passed on to the port security module, which in turn asks all user modules whether to allow this new MAC address to forward or block it. For a MAC address to be set in the forwarding state, all enabled user modules must unanimously agree on allowing the MAC address to forward. If only one chooses to block it, it will be blocked until that user module decides otherwise. The status page is divided into two sections - one with a legend of user modules and one with the actual port status.

Web Interface

To display the Port Security Switch Status Configuration in the web interface:

1. Click Security, Network, Port Security and Switch
2. Checked "Auto-refresh".
3. Click "Refresh" to refresh the port detailed statistics.

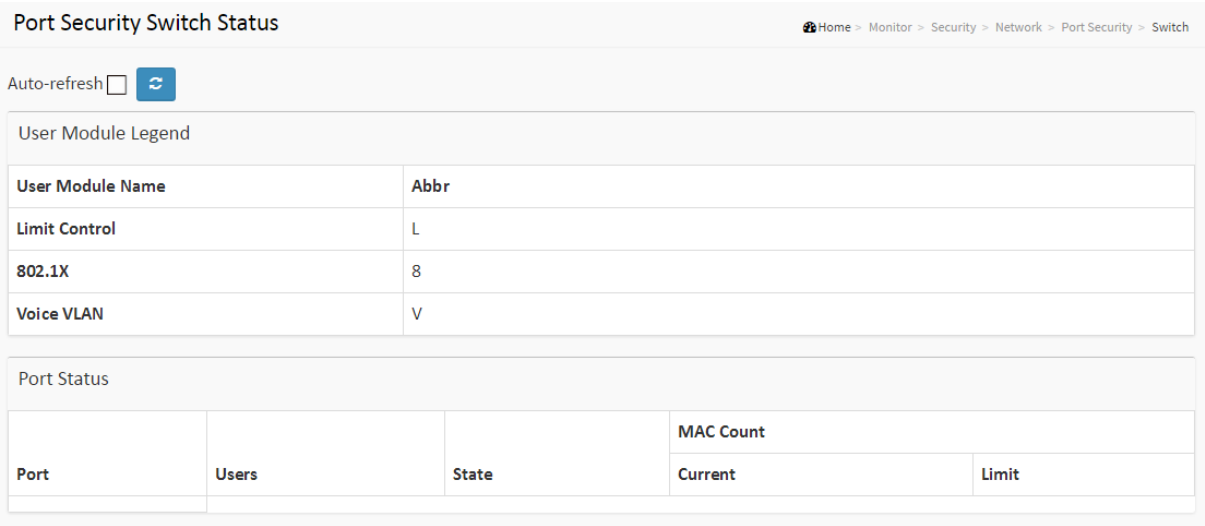


Figure 3-5.2.1.1: The Port Security Switch Status

Parameter description:

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 Web-page.

- **MAC Count (Current, Limit) :**

  The two columns indicate the number of currently learned MAC addresses (forwarding as well as blocked) and the maximum number of MAC addresses that can be learned on the port, respectively.

  If no user modules are enabled on the port, the Current column will show a dash (-).

Buttons

- **Auto-refresh :**

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

- **Refresh :**

  Click to refresh the page.

3-5.2.1.2 Port

This section shows the MAC addresses secured by the Port Security module. Port Security is a module with no direct configuration. Configuration comes indirectly from other modules - the user modules. When a user module has enabled port security on a port, the port is set-up for software-based learning. In this mode, frames from unknown MAC addresses are passed on to the port security module, which in turn asks all user modules whether to allow this new MAC address to forward or block it. For a MAC address to be set in the forwarding state, all enabled user modules must unanimously agree on allowing the MAC address to forward. If only one chooses to block it, it will be blocked until that user module decides otherwise.

Web Interface

To display the Port Security Switch Status Configuration in the web interface:

1. Click Security, Network, Port Security and then Port.
2. Specify the Port which you want to monitor.
3. Checked "Auto-refresh".
4. Click "Refresh" to refresh the port detailed statistics.

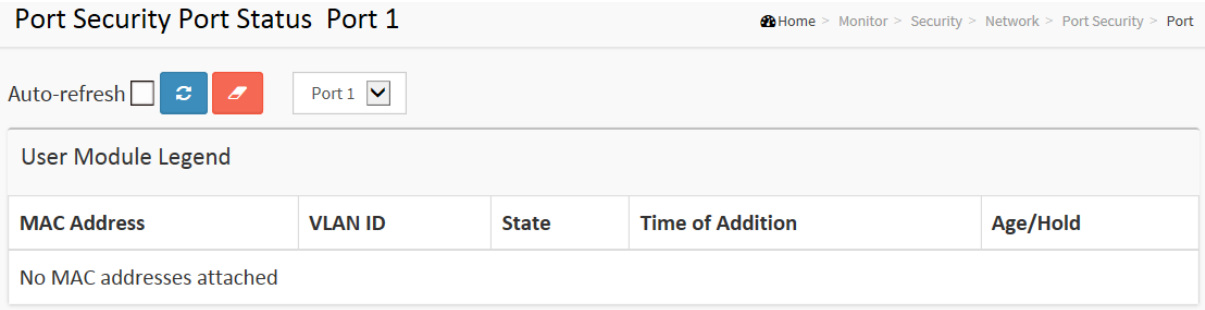


Figure 3-5.2.1.2: The Port Security Port Status

Parameter description:

- **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.

Buttons

- **Auto-refresh :**

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

- **Refresh :**

  Click to refresh the page.

- **Clear :**

  Flushes the selected log entries.

3-5.2.2.1 Switch

The section describes to show the each port NAS status information of the switch. The status includes Admin State Port State, Last Source, Last ID, QoS Class, and Port VLAN ID.

Web Interface

To display the NAS Switch Status Configuration in the web interface:

1. Click Security, Network, NAS and then Port.
2. Checked "Auto-refresh".
3. Click "Refresh" to refresh the port detailed statistics.

Network Access Server Switch Status

Home > Monitor > Security > Network > NAS > Switch

Auto-refresh

Port	Admin State	Port State	Last Source	Last ID	QoS Class	Port VLAN ID
1	Force Authorized	Globally Disabled			-	
2	Force Authorized	Globally Disabled			-	
N−2	Force Authorized	Globally Disabled			-	
N−1	Force Authorized	Globally Disabled			-	
N	Force Authorized	Globally Disabled			-	

Figure 3-5.2.2.1: The Network Access Server Switch Status

Parameter description:

- **Port :**

  The switch port number. Click to navigate to detailed NAS statistics for this port.

- **Admin State :**

  The port's current administrative state. Refer to NAS Admin State for a description of possible values.

- **Port State :**

  The current state of the port. Refer to NAS Port State for a description of the individual states.

- **Last Source :**

  The source MAC address carried in the most recently received EAPOL frame for EAPOL-based authentication, and the most recently received frame from a new client for MAC-based authentication.

- **Last ID :**

  The user name (supplicant identity) carried in the most recently received Response Identity EAPOL frame for EAPOL-based authentication, and the source MAC address from the most

recently received frame from a new client for MAC-based authentication.

- **QoS Class :**

  QoS Class assigned to the port by the RADIUS server if enabled.

- **Port VLAN ID :**

  The VLAN ID that NAS has put the port in. The field is blank, if the Port VLAN ID is not overridden by NAS.

  If the VLAN ID is assigned by the RADIUS server, "(RADIUS-assigned)" is appended to the VLAN ID. Read more about RADIUS-assigned VLANs here.

  If the port is moved to the Guest VLAN, "(Guest)" is appended to the VLAN ID. Read more about Guest VLANs here.

Buttons

- **Auto-refresh :**

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

- **Refresh :**

  Click to refresh the page.

3-5.2.2.2 Port

The section describes to provide detailed NAS statistics for a specific switch port running EAPOL-based IEEE 802.1X authentication. For MAC-based ports, it shows selected backend server (RADIUS Authentication Server) statistics, only.

Web Interface

To display the NAS Port Status Configuration in the web interface:

1. Click Security, Network, NAS and then Port.
2. Checked "Auto-refresh".
3. Click "Refresh" to refresh the port detailed statistics.

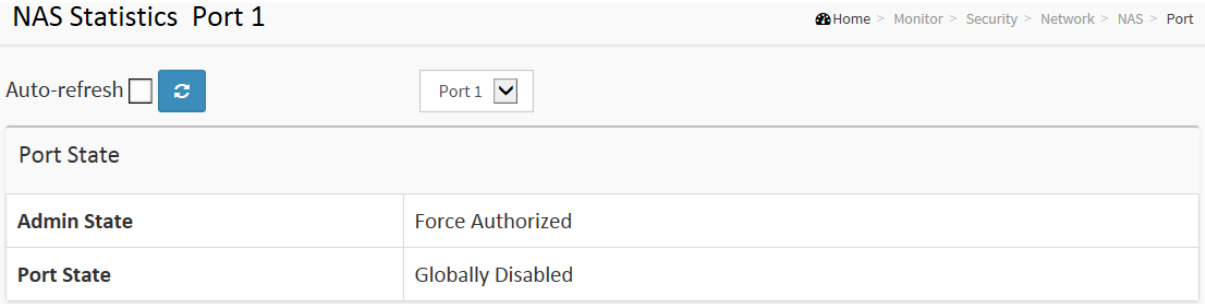


Figure 3-5.2.2.2: The NAS Statistics

Parameter description:

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. Read more about Guest VLANs here.

Port Counters

- **EAPOL Counters :**

  These supplicant frame counters are available for the following administrative states:

  - Force Authorized
  - Force Unauthorized
  - Port-based 802.1X
  - Single 802.1X
  - Multi 802.1X

- **Backend Server Counters :**

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

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

- **Last Supplicant/Client Info :**

  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 MAC-based Auth., this column holds the MAC address of the attached client.

Clicking the link causes the client's Backend Server counters to be shown in the Selected Counters table. If no clients are attached, it shows No clients attached.

- **VLAN ID :**

  This column holds the VLAN ID that the corresponding client is currently secured through the Port Security module.

- **State :**

  The client can either be authenticated or unauthenticated. In the authenticated state, it is allowed to forward frames on the port, and in the unauthenticated state, it is blocked. As long as the backend server hasn't successfully authenticated the client, it is unauthenticated. If an authentication fails for one or the other reason, the client will remain in the unauthenticated state for Hold Time seconds.

- **Last Authentication :**

  Shows the date and time of the last authentication of the client (successful as well as unsuccessful).

Buttons

- **Auto-refresh :**

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

- **Refresh :**

  Click to refresh the page.

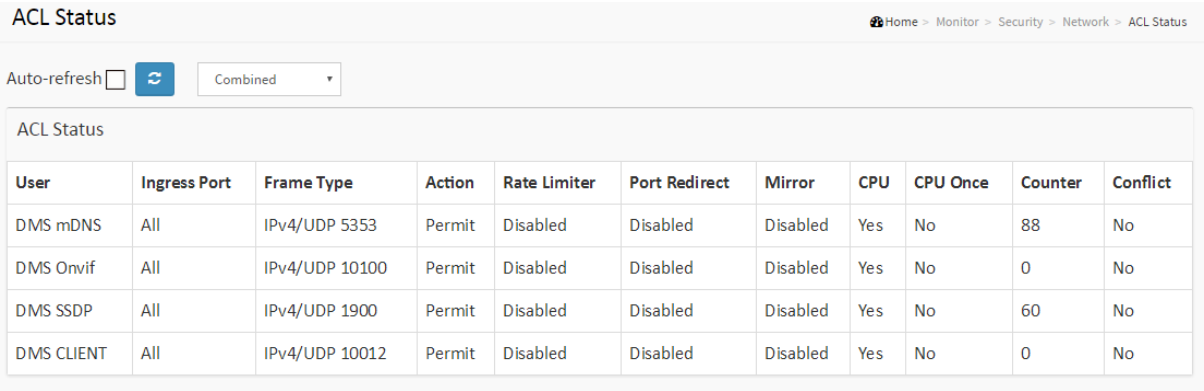
3-5.2.3 ACL Status

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 512 on each switch.

Web Interface

To display the ACL status in the web interface:

1. Click Monitor, Network and ACL status
2. If you want to auto-refresh the information then you need to evoke the "Auto-refresh".
3. Click "Refresh" to refresh the ACL Status



User	Ingress Port	Frame Type	Action	Rate Limiter	Port Redirect	Mirror	CPU	CPU Once	Counter	Conflict
DMS mDNS	All	IPv4/UDP 5353	Permit	Disabled	Disabled	Disabled	Yes	No	88	No
DMS Onvif	All	IPv4/UDP 10100	Permit	Disabled	Disabled	Disabled	Yes	No	0	No
DMS SSDP	All	IPv4/UDP 1900	Permit	Disabled	Disabled	Disabled	Yes	No	60	No
DMS CLIENT	All	IPv4/UDP 10012	Permit	Disabled	Disabled	Disabled	Yes	No	0	No

Figure 3-5.2.3: The ACL Status

Parameter description:

- **User :**

  Indicates the ACL user.

- **Ingress Port :**

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

  All: The ACE will match any ingress port.

  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.

  IPv4: The ACE will match all IPv4 frames.

  IPv4/ICMP: The ACE will match IPv4 frames with ICMP protocol.

IPv4/UDP: The ACE will match IPv4 frames with UDP protocol.

IPv4/TCP: The ACE will match IPv4 frames with TCP protocol.

IPv4/Other: The ACE will match IPv4 frames, which are not ICMP / UDP / TCP.

IPv6: The ACE will match all IPv6 standard frames.

- **Action :**

  Indicates the forwarding action of the ACE.

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

  Deny: Frames matching the ACE are dropped.

  Filter: Frames matching the ACE are filtered.

- **Rate Limiter :**

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

- **Port Redirect :**

  Indicates the port 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.

- **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 :**

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

- **Refresh :**

  Click to refresh the page.

3-5.2.4 ARP Inspection

The section describes to configure the Dynamic ARP Inspection Table 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.

Web Interface

To display the Dynamic ARP Inspection Table Configuration in the web interface:

1. Click Security, Network, ARP Inspection.
2. Checked "Auto-refresh".
3. Click "Refresh" to refresh the port detailed statistics.
4. Specify the Start from port, VLAN ID, MAC Address, IP Address, and entries per page.

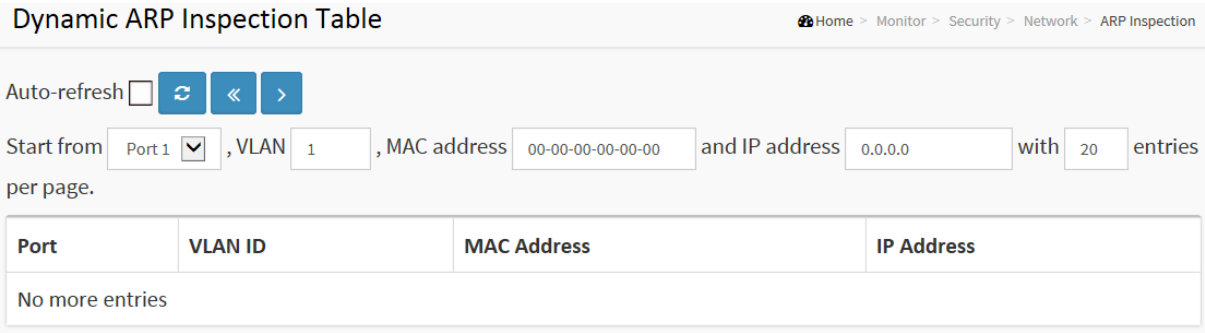


Figure 3-5.2.4: The Dynamic ARP Inspection Table

Parameter description:

ARP Inspection Table Columns

- **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 this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.

- **Refresh :**

  Click to refresh the page.

- « :

  Updates the table starting from the first entry in the Dynamic ARP Inspection Table.

- › :

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

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

Web Interface

To display the Dynamic IP Source Guard Table Configuration in the web interface:

1. Click Security, Network and IP Source Guard.
2. Checked "Auto-refresh".
3. Click "Refresh" to refresh the port detailed statistics.
4. Specify the Start from port, VLAN ID, IP Address, and entries per page.

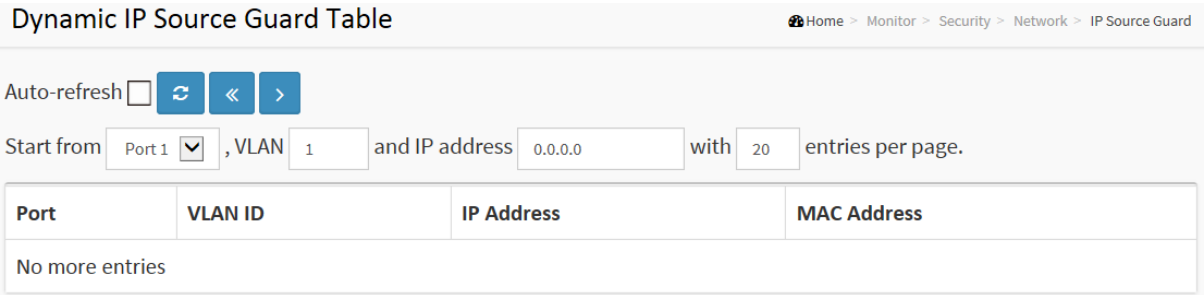


Figure 3-5.2.5: The Dynamic IP Source Table

Parameter description:

IP Source Guard Table Columns

- **Port :**

  Switch Port Number for which the entries are displayed.

- **VLAN ID :**

  VLAN-ID in which the IP traffic is permitted.

- **IP Address :**

  User IP address of the entry.

- **MAC Address :**

  Source MAC address.

Buttons

- **Auto-refresh :**

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

- **Refresh :**

  Click to refresh the page.

- « :

  Updates the table starting from the first entry in the Dynamic ARP Inspection Table.

- › :

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

3-5.3 AAA

3-5.3.1 RADIUS Overview

This section shows you an overview of the RADIUS Authentication and Accounting servers' status to ensure the function is workable.

Web Interface

To display the RADIUS Overview Configuration in the web interface:

1. Click Security, AAA and RADIUS Overview.
2. Checked "Auto-refresh".
3. Click "Refresh" to refresh the port detailed statistics.

RADIUS Server Status Overview

Home > Monitor > Security > AAA > RADIUS Overview

RADIUS Authentication Server Status Overview

#	IP Address	Status
1	0.0.0.0:0	Disabled
2	0.0.0.0:0	Disabled
3	0.0.0.0:0	Disabled
4	0.0.0.0:0	Disabled
5	0.0.0.0:0	Disabled

RADIUS Accounting Server Status Overview

#	IP Address	Status
1	0.0.0.0:0	Disabled
2	0.0.0.0:0	Disabled
3	0.0.0.0:0	Disabled
4	0.0.0.0:0	Disabled
5	0.0.0.0:0	Disabled

Figure 3-5.3.1: The RADIUS Server Status Overview

Parameter description:

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 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.

3-5.3.2 RADIUS Details

This section shows you a detailed statistics for a particular RADIUS server.

Web Interface

To display the RADIUS Details Configuration in the web interface:

1. Specify Port which want to check.
2. Click Security, AAA, RADIUS Overview.
3. Checked "Auto-refresh".
4. Click "Refresh" to refresh the port detailed statistics or clear all information when you click "Clear" & " Fresh".

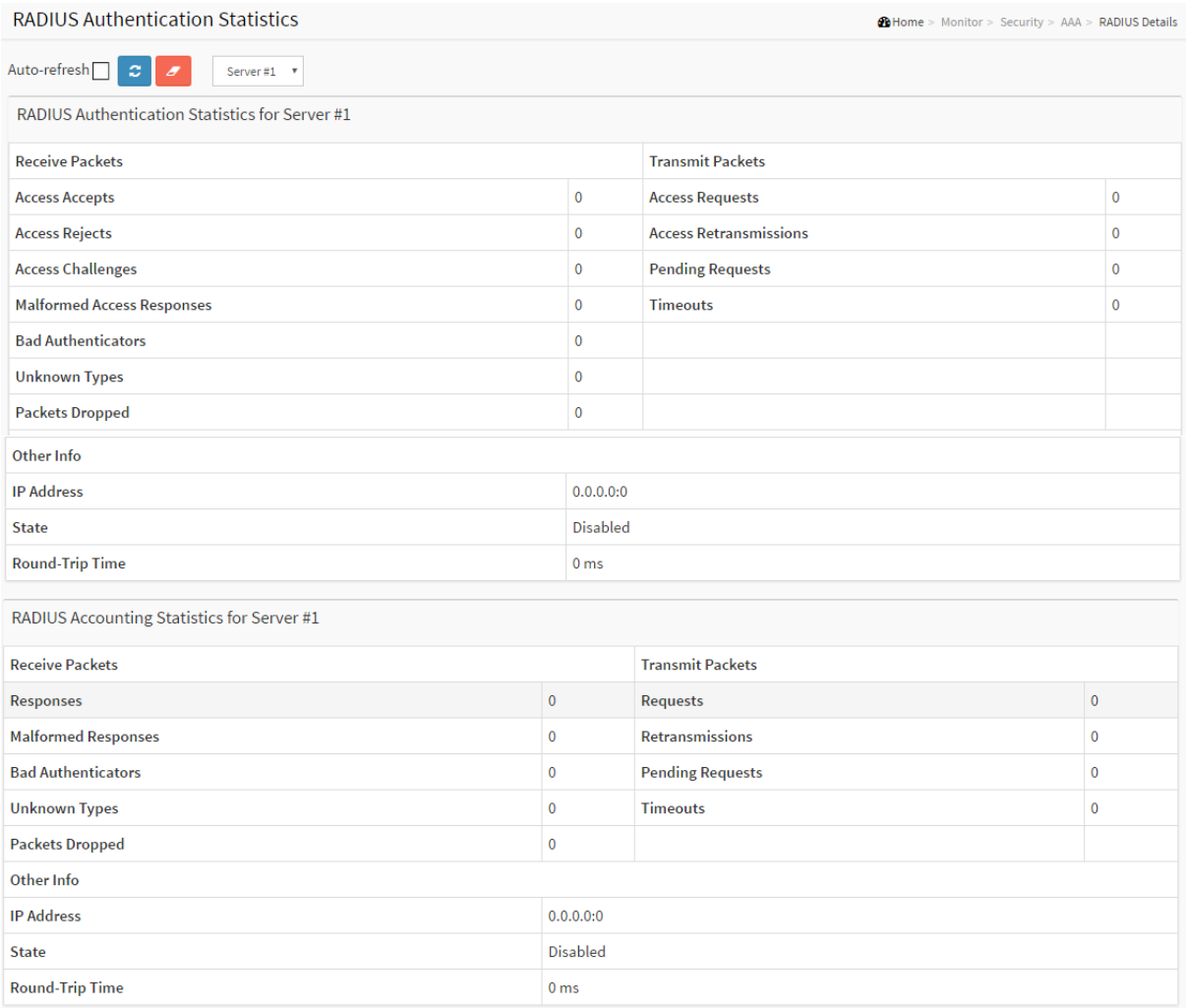


Figure 3-5.3.2: The RADIUS Authentication Statistics Server

Parameter description:

RADIUS Authentication Statistics

The statistics map closely to those specified in RFC4668 - RADIUS Authentication Client MIB.Use the server select box to switch between the backend servers to show details for.

- **Packet Counters :**

  RADIUS authentication server packet counter. There are seven receive and four transmit counters

- **Other Info :**

  This section contains information about the state of the server and the latest round-trip time.

RADIUS Accounting Statistics

The statistics map closely to those specified in RFC4670 - RADIUS Accounting Client MIB.

Use the server select box to switch between the backend servers to show details for.

- **Packet Counters :**

  RADIUS accounting server packet counter. There are five receive and four transmit counters.

- **Other Info :**

  This section contains information about the state of the server and the latest round-trip time.

Buttons

- **Auto-refresh :**

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

- **Refresh :**

  Click to refresh the page.

- **Clear :**

  Clears the counters for the selected server. The "Pending Requests" counter will not be cleared by this operation.

3-5.4 Switch

3-5.4.1 RMON

3-5.4.1.1 Statistics

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

Web Interface

To display the RMON Statistics in the web interface:

1. Click Security, Switch, RMON and Statistics.
2. Specify Port which want to check.
3. Checked "Auto-refresh".
4. Click "Refresh" to refresh the port detailed statistics.

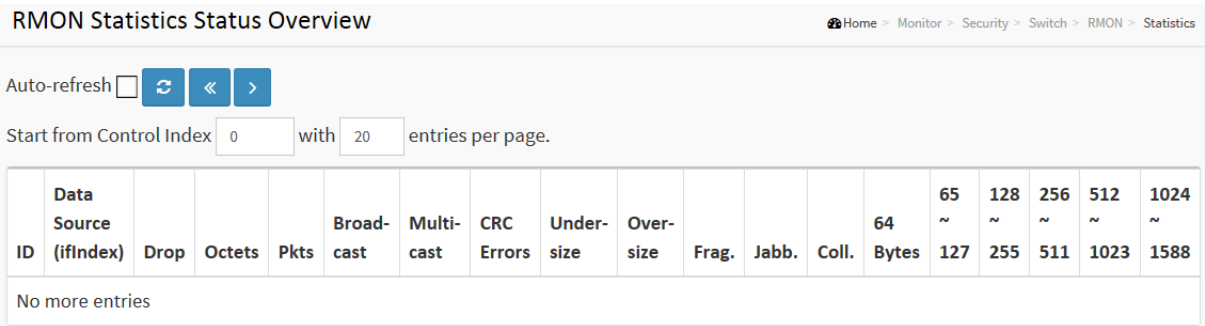


Figure 3-5.4.1.1: The RMON Statistics Status Overview

Parameter description:

- **ID :**

  Indicates the index of Statistics entry.

- **Data Source(if Index) :**

  The port ID which wants to be monitored.

- **Drop :**

  The total number of events in which packets were dropped by the probe due to lack of resources.

- **Octets :**

  The total number of octets of data (including those in bad packets) received on the network.

- **Pkts :**

The total number of packets (including bad packets, broadcast packets, and multicast packets) received.

- **Broad-cast :**

  The total number of good packets received that were directed to the broadcast address.

- **Multi-cast :**

  The total number of good packets received that were directed to a multicast address.

- **CRC Errors :**

  The total number of packets received that had a length (excluding framing bits, but including FCS octets) of between 64 and 1518 octets, inclusive, but had either a bad Frame Check Sequence (FCS) with an integral number of octets (FCS Error) or a bad FCS with a non-integral number of octets (Alignment Error).

- **Under-size :**

  The total number of packets received that were less than 64 octets.

- **Over-size :**

  The total number of packets received that were longer than 1518 octets.

- **Frag. :**

  The number of frames which size is less than 64 octets received with invalid CRC.

- **Jabb. :**

  The number of frames which size is larger than 64 octets received with invalid CRC.

- **Coll. :**

  The best estimate of the total number of collisions on this Ethernet segment.

- **64 :**

  The total number of packets (including bad packets) received that were 64 octets in length.

- **65~127 :**

  The total number of packets (including bad packets) received that were between 65 to 127 octets in length.

- **128~255 :**

  The total number of packets (including bad packets) received that were between 128 to 255 octets in length.

- **256~511 :**

  The total number of packets (including bad packets) received that were between 256 to 511 octets in length.

- **512~1023 :**

  The total number of packets (including bad packets) received that were between 512 to 1023 octets in length.

- **1024~1588 :**

  The total number of packets (including bad packets) received that were between 1024 to 1588 octets in length.

Buttons

- **Auto-refresh :**

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

- **Refresh :**

  Refreshes the displayed table starting from the input fields.

- **:**

  Updates the table starting from the first entry in the Statistics table, i.e. the entry with the lowest ID

- **:**

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

3-5.4.1.2 History

This section provides an overview of RMON History entries. Each page shows up to 99 entries from the History 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 History table. The first displayed will be the one with the lowest History Index and Sample Index found in the History table.

Web Interface

To display the RMON history Configuration in the web interface:

1. Click Security, Switch, RMON and History.
2. Checked "Auto-refresh".
3. Click "Refresh" to refresh the port detailed statistics or clear all information when you click " Clear".

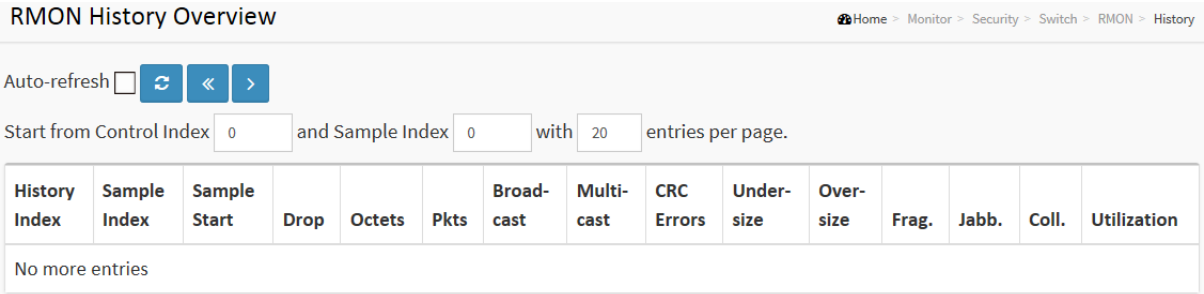


Figure 3-5.4.1.2: RMON History Overview

Parameter description:

- **History Index :**

  Indicates the index of History control entry.

- **Sample Index :**

  Indicates the index of the data entry associated with the control entry.

- **Sample Start :**

  The value of sysUpTime at the start of the interval over which this sample was measured.

- **Drop :**

  The total number of events in which packets were dropped by the probe due to lack of resources.

- **Octets :**

  The total number of octets of data (including those in bad packets) received on the network.

- **Pkts :**

  The total number of packets (including bad packets, broadcast packets, and multicast packets) received.

- **Broadcast :**

The total number of good packets received that were directed to the broadcast address.

- **Multicast :**

  The total number of good packets received that were directed to a multicast address.

- **CRCErrors :**

  The total number of packets received that had a length (excluding framing bits, but including FCS octets) of between 64 and 1518 octets, inclusive, but had either a bad Frame Check Sequence (FCS) with an integral number of octets (FCS Error) or a bad FCS with a non-integral number of octets (Alignment Error).

- **Undersize :**

  The total number of packets received that were less than 64 octets.

- **Oversize :**

  The total number of packets received that were longer than 1518 octets.

- **Frag. :**

  The number of frames which size is less than 64 octets received with invalid CRC.

- **Jabb. :**

  The number of frames which size is larger than 64 octets received with invalid CRC.

- **Coll. :**

  The best estimate of the total number of collisions on this Ethernet segment.

- **Utilization :**

  The best estimate of the mean physical layer network utilization on this interface during this sampling interval, in hundredths of a percent.

Buttons

- **Auto-refresh :**

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

- **Refresh :**

  Refreshes the displayed table starting from the input fields.

- **:**

  Updates the table starting from the first entry in the Statistics table, i.e. the entry with the lowest ID

- **:**

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

3-5.4.1.3 Alarm

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

Web Interface

To display the RMON Alarm Overview in the web interface:

1. Specify Port which wants to check.
2. Click Security, Switch, RMON and Alarm.
3. Checked “Auto-refresh”.
4. Click “Refresh” to refresh the port detailed statistics.

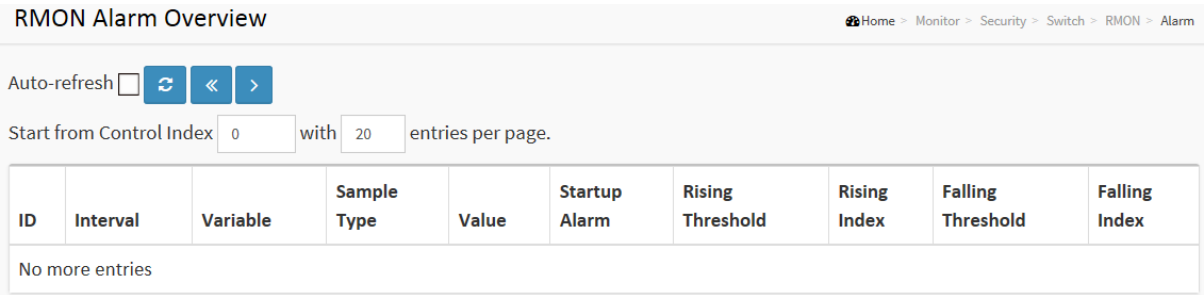


Figure 3-5.4.1.3: RMON Alarm Overview

Parameter description:

- **ID :**

  Indicates the index of Alarm control entry.

- **Interval :**

  Indicates the interval in seconds for sampling and comparing the rising and falling threshold.

- **Variable :**

  Indicates the particular variable to be sampled

- **Sample Type :**

  The method of sampling the selected variable and calculating the value to be compared against the thresholds.

- **Value :**

  The value of the statistic during the last sampling period.

- **Startup Alarm :**

  The alarm that may be sent when this entry is first set to valid.

- **Rising Threshold :**

  Rising threshold value.

- **Rising Index :**

  Rising event index.

- **Falling Threshold :**

  Falling threshold value.

- **Falling Index :**

  Falling event index.

Buttons

- **Auto-refresh :**

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

- **Refresh :**

  Refreshes the displayed table starting from the input fields.

- **:**

  Updates the table starting from the first entry in the Statistics table, i.e. the entry with the lowest ID

- **:**

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

3-5.4.1.4 Event

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

Web Interface

To display the RMON Event Overview in the web interface:

1. Click Security, Switch, RMON and Event.
2. Checked "Auto-refresh".
3. Click " Refresh" to refresh the port detailed statistics
4. Specify Port which wants to check.

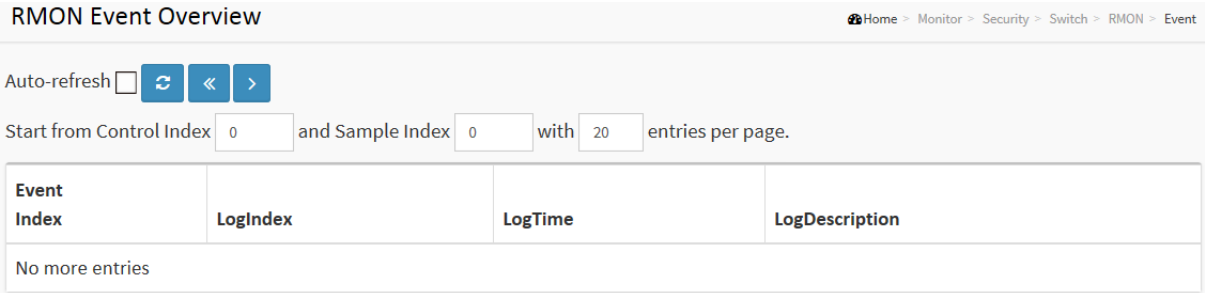


Figure 3-5.4.1.4: RMON Event Overview

Parameter description:

- **Event Index :**

  Indicates the index of the event entry.

- **Log Index :**

  Indicates the index of the log entry.

- **LogTIme :**

  Indicates Event log time

- **LogDescription :**

  Indicates the Event description.

Buttons

- **Auto-refresh :**

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

- **Refresh :**

  Refreshes the displayed table starting from the input fields.

- « :

  Updates the table starting from the first entry in the Statistics table, i.e. the entry with the lowest ID

- › :

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

3-6 LACP

3-6.1 System Status

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

Web Interface

To display the LACP System status in the web interface:

1. Click Monitor, LACP and System Status
2. Checked "Auto-refresh".
3. Click "Refresh" to refresh the port detailed statistics.

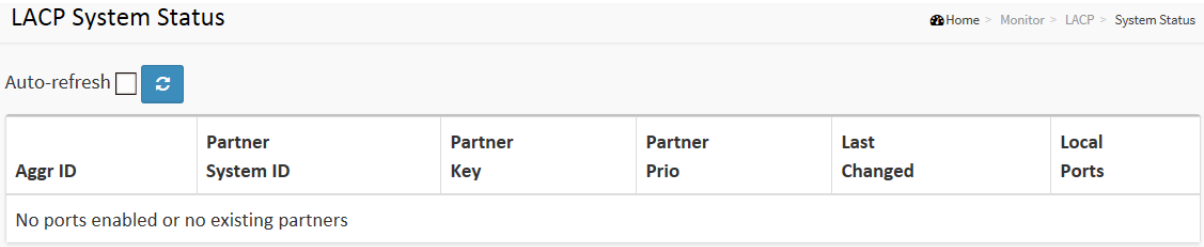


Figure 3-6.1 The LACP System Status

Parameter description:

- **Aggr ID :**

  The Aggregation ID associated with this aggregation instance. For LLAG the id is shown as 'isid: aggr-id' and for GLAGs 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 this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.

- **Refresh :**

  Refreshes the displayed table starting from the input fields.

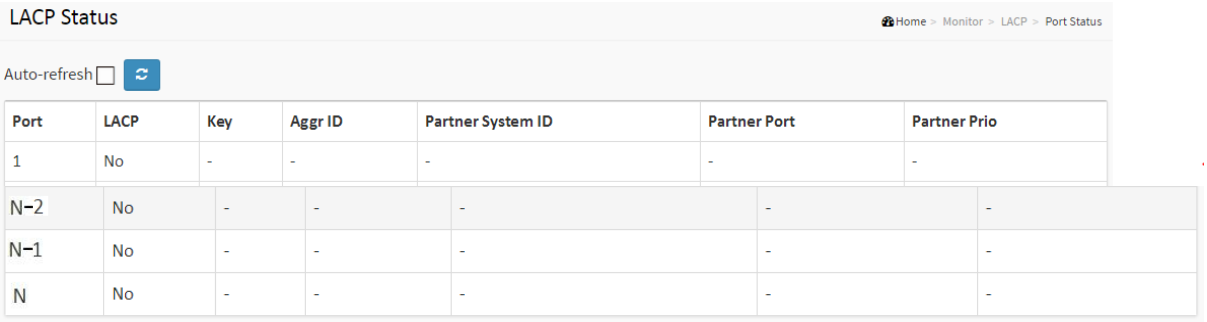
3-6.2 Port Status

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

Web Interface

To display the LACP Port status in the web interface:

1. Click Monitor, LACP and Port Status
2. If you want to auto-refresh the information then you need to evoke the "Auto-refresh".
3. Click "Refresh" to refresh the LACP Port Status.



Port	LACP	Key	Aggr ID	Partner System ID	Partner Port	Partner Prio
1	No	-	-	-	-	-
N-2	No	-	-	-	-	-
N-1	No	-	-	-	-	-
N	No	-	-	-	-	-

Figure 3-6.2: The LACP Status

Parameter description:

- **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.

- **Partner Prio:**

  The partner's port priority.

Buttons

- **Auto-refresh :**

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

- **Refresh :**

  Refreshes the displayed table starting from the input fields.

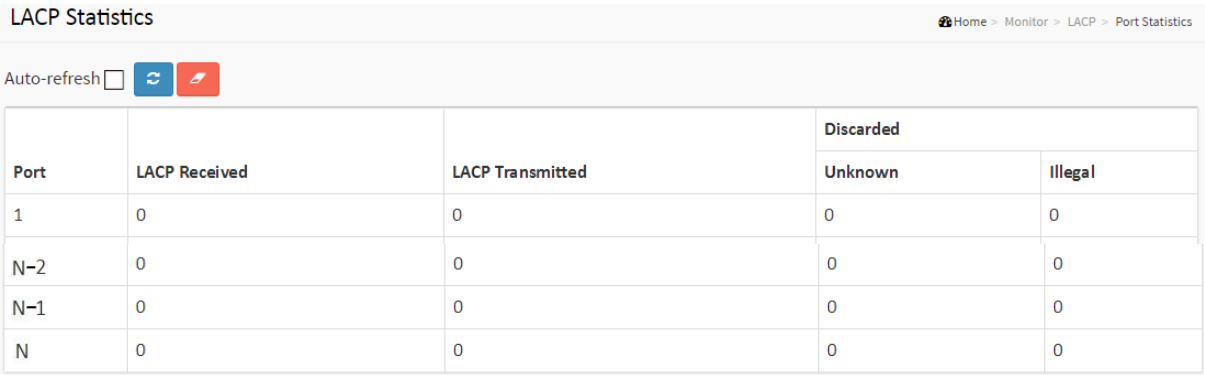
3-6.3 Port Statistics

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

Web Interface

To display the LACP Port status in the web interface:

1. Click Monitor, LACP and Port Statistics
2. If you want to auto-refresh the information then you need to evoke the "Auto refresh".
3. 3. Click "Refresh" to refresh the LACP Statistics.



Port	LACP Received	LACP Transmitted	Discarded	
			Unknown	Illegal
1	0	0	0	0
N-2	0	0	0	0
N-1	0	0	0	0
N	0	0	0	0

Figure 3-6.3: The LACP Statistics

Parameter description:

- **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 :**

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

- **Refresh :**

  Click to refresh the page.

- **Clear :**

  Clears the counters for all ports.

3-7 Loop Protection

This section displays the loop protection port status the ports of the currently selected switch.

Web Interface

To display the Loop Protection status in the web interface:

1. Click Monitor and Loop Protection
2. If you want to auto-refresh the information then you need to evoke the "Auto refresh".
3. Click "Refresh" to refresh the LACP Statistics.

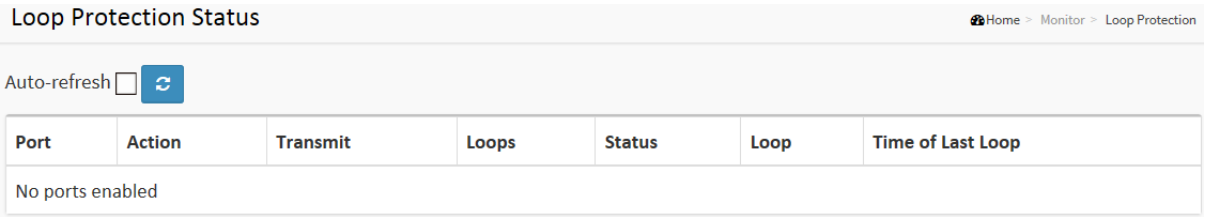


Figure 3-7: Loop Protection Status

Parameter description:

- **Port :**

  The switch port number of the logical port.

- **Action :**

  The currently configured port action.

- **Transmit :**

  The currently configured port transmit mode.

- **Loops :**

  The number of loops detected on this port.

- **Status :**

  The current loop protection status of the port.

- **Loop :**

  Whether a loop is currently detected on the port.

- **Time of Last Loop :**

  The time of the last loop event detected.

Buttons

- **Auto-refresh :**

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

- **Refresh :**

  Click to refresh the page.

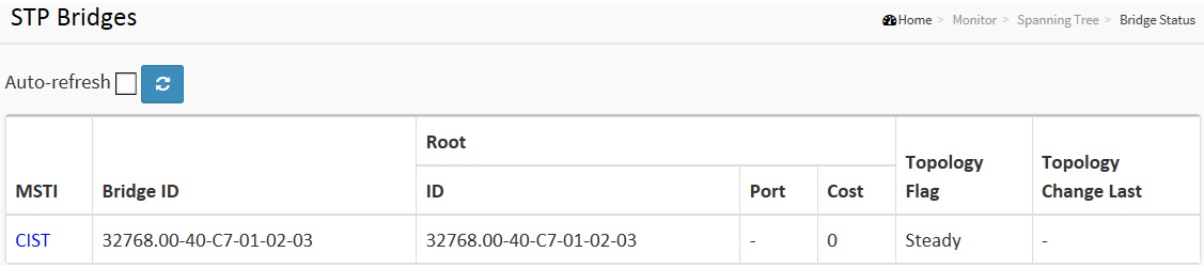
3-8.1 Bridge Status

After you complete the MSTI Port configuration then you could to ask the switch display the Bridge Status. The Section provides a status overview of all STP bridge instances. The displayed table contains a row for each STP bridge instance, where the column displays the following information:

Web Interface

To display the STP Bridges status in the web interface:

1. Click Monitor, Spanning Tree and Bridge Status.
2. If you want to auto-refresh the information then you need to evoke the "Auto-refresh".
3. Click "Refresh" to refresh the STP Bridges.
4. Click "CIST "to next page "STP Detailed Bridge Status".



MSTI	Bridge ID	Root			Topology Flag	Topology Change Last
		ID	Port	Cost		
CIST	32768.00-40-C7-01-02-03	32768.00-40-C7-01-02-03	-	0	Steady	-

Figure 3-8.1: The STP Bridges status

Parameter description:

- **MSTI :**

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

- **Bridge ID :**

  The Bridge ID of this Bridge instance.

- **Root ID :**

  The Bridge ID of the currently elected root bridge.

- **Root Port :**

  The switch port currently assigned the root port role.

- **Root Cost :**

  Root Path Cost. For the Root Bridge 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 this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.

- **Refresh :**

  Click to refresh the page.

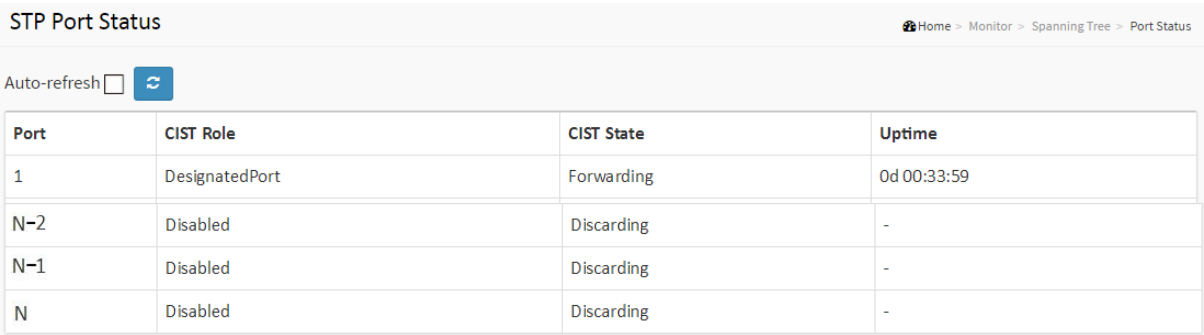
3-8.2 Port Status

After you complete the STP configuration then you could to ask the switch display the STP Port Status. The Section provides you to ask switch to display the STP CIST port status for physical ports of the currently selected switch.

Web Interface

To display the STP Port status in the web interface:

1. Click Monitor, Spanning Tree and Port Status.
2. If you want to auto-refresh the information then you need to evoke the "Auto-refresh".
3. Click "Refresh" to refresh the STP Bridges.



Port	CIST Role	CIST State	Uptime
1	DesignatedPort	Forwarding	0d 00:33:59
N-2	Disabled	Discarding	-
N-1	Disabled	Discarding	-
N	Disabled	Discarding	-

Figure 3-8.2: The STP Port status

Parameter description:

- **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, Backup Port, RootPort, DesignatedPort Disabled.

- **CIST State :**

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

- **Uptime :**

  The time since the bridge port was last initialized.

Buttons

- **Auto-refresh :**

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

- **Refresh :**

  Click to refresh the page.

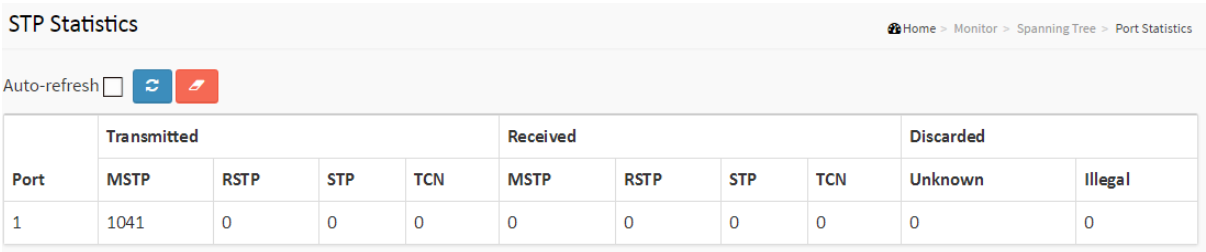
3-8.3 Port Statistics

After you complete the STP configuration then you could to let the switch display the STP Statistics. The Section provides you to ask switch to display the STP Statistics detail counters of bridge ports in the currently selected switch.

Web Interface

To display the STP Port status in the web interface:

1. Click Monitor, Spanning Tree and Port Statistics
2. If you want to auto-refresh the information then you need to evoke the "Auto-refresh".
3. Click "Refresh" to refresh the STP Bridges.



	Transmitted				Received				Discarded	
Port	MSTP	RSTP	STP	TCN	MSTP	RSTP	STP	TCN	Unknown	Illegal
1	1041	0	0	0	0	0	0	0	0	0

Figure 3-8.3: The STP Statistics

Parameter description:

- **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 :**

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

- **Refresh :**

  Click to refresh the page.

- **Clear :**

  Click to reset the counters.

3-9 MVR

3-9.1 Statistics

The section describes the switch will display the MVR detail Statistics after you had configured MVR on the switch. It provides the detail MVR Statistics Information

Web Interface

To display the MVR Statistics Information in the web interface:

1. Click Monitor, MVR and Statistics
2. If you want to auto-refresh the information then you need to evoke the "Auto-refresh".
3. To click the "Refresh" to refresh an entry of the MVR Statistics Information.

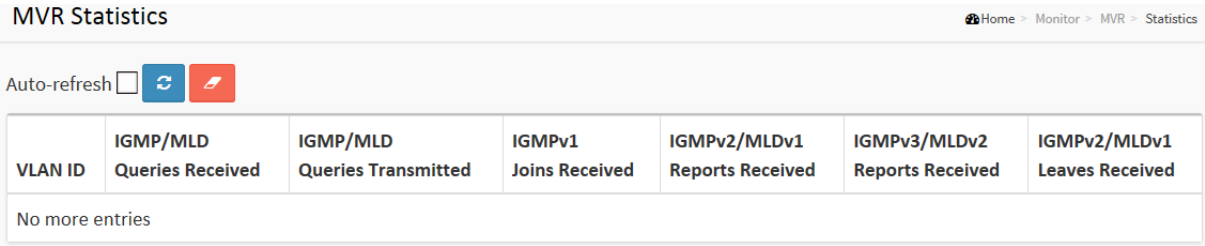


Figure 3-9.1: The MVR Statistics Information

Parameter description:

- **VLAN ID :**

  The Multicast VLAN ID.

- **IGMP/MLD Queries Received :**

  The number of Received Queries for IGMP and MLD, respectively.

- **IGMP/MLD Queries Transmitted :**

  The number of Transmitted Queries for IGMP and MLD, respectively.

- **IGMPv1 Joins Received :**

  The number of Received IGMPv1 Join's.

- **IGMPv2/MLDv1 Report's Received :**

  The number of Received IGMPv2 Join's and MLDv1 Report's, respectively.

- **IGMPv3/MLDv2 Report's Received :**

  The number of Received IGMPv1 Join's and MLDv2 Report's, respectively.

- **IGMPv2/MLDv1 Leave's Received :**

  The number of Received IGMPv2 Leave's and MLDv1 Done's, respectively.

Buttons

- **Auto-refresh :**

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

- **Refresh :**

  Click to refresh the page.

- **Clear :**

  Click to reset the counters

3-9.2 MVR Channels Groups

The section describes user could display 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

Web Interface

To display the MVR Groups Information in the web interface:

1. Click Monitor, MVR and Groups Information
2. If you want to auto-refresh the information then you need to evoke the "Auto-refresh".
3. To click the "Refresh" to refresh an entry of the MVR Groups Information.
4. Click "<< or >> "to move to previous or next entry.

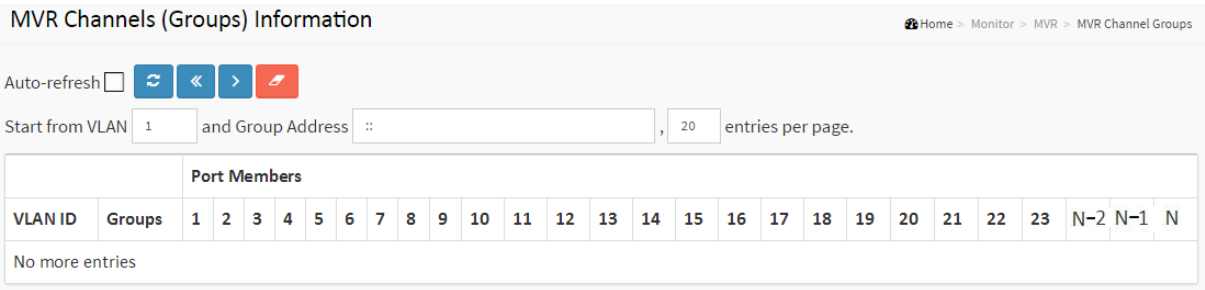


Figure 3-9.2: The MVR Groups Information

Parameter description:

MVR Channels (Groups) Information Table Columns

- **VLAN ID :**

  VLAN ID of the group.

- **Groups :**

  Group ID of the group displayed.

- **Port Members :**

  Ports under this group.

Buttons

- **Auto-refresh :**

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

- **Refresh :**

  Click to refresh the page immediately.

- **Clear :**

Flushes the selected log entries.

- « :

  Updates the table starting from the first entry in the MVR Channels (Groups) Information Table.

- < :

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

3-9.3 MVR SFM Information

The MVR SFM (Source-Filtered Multicast) Information Table also contains the SSM (Source-Specific Multicast) information. This table is sorted first by VLAN ID, then by group, and then by Port. Different source addresses belong to the same group are treated as single entry.

Web Interface

To display the MVR SFM Information in the web interface:

1. Click Monitor, MVR and MVR SFM Information
2. If you want to auto-refresh the information then you need to evoke the "Auto-refresh".
3. To click the "Refresh" to refresh an entry of the MVR Groups Information.
4. Click "<< or >> "to move to previous or next entry.

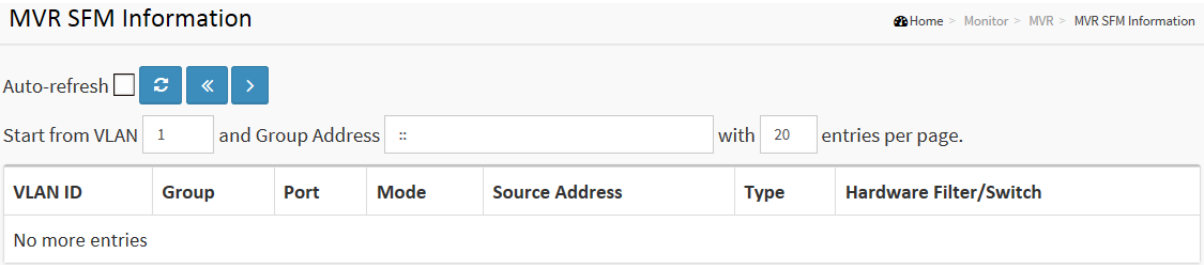


Figure 3-9.2: The MVR SFM Information

Parameter description:

MVR SFM Information Table Columns

- **VLAN ID :**

  VLAN ID of the group.

- **Group :**

  Group address of the group displayed.

- **Port :**

  Switch port number.

- **Mode :**

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

- **Source Address :**

  IP Address of the source. Currently, system limits the total number of IP source addresses for filtering to be 128. When there is no any source filtering address, the text "None" is shown in the Source Address field.

- **Type :**

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

- **Hardware Filter/Switch :**

  Indicates whether data plane destined to the specific group address from the source IPv4/IPv6 address could be handled by chip or not.

Buttons

- **Auto-refresh :**

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

- **Refresh :**

  Click to refresh the page immediately.

- **:**

  Updates the table starting from the first entry in the MVR Channels (Groups) Information Table.

- **:**

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

3-10.1 IGMP Snooping

3-10.1.1 Status

After you complete the IGMP Snooping configuration, then you could to let the switch display the IGMP Snooping Status. The Section provides you to let switch to display the IGMP Snooping detail status.

Web Interface

To display the IGMP Snooping status in the web interface:

1. Click Monitor, IGMP Snooping and Status
2. If you want to auto-refresh the information then you need to evoke the "Auto-refresh".
3. Click "Refresh" to refresh the IGMP Snooping Status.
4. Click "Clear "to clear the IGMP Snooping Status.

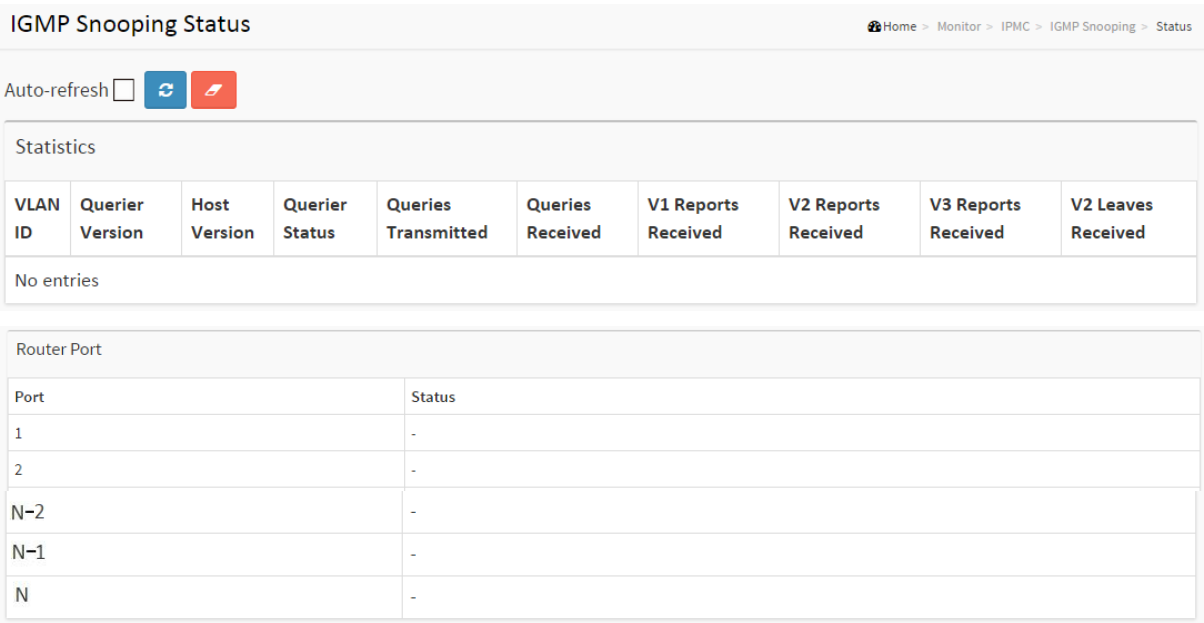


Figure 3-10.1.1: The IGMP Snooping Status.

Parameter description:

- **VLAN ID :**

  The VLAN ID of the entry.

- **Querier Version :**

  Working Querier Version currently.

- **Host Version :**

Working Host Version currently.

- **Querier Status :**

  Shows the Querier status is "ACTIVE" or "IDLE".

  "DISABLE" denotes the specific interface is administratively disabled.

- **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.

- **Router Port :**

  Display which ports act as router ports. A router port is a port on the Ethernet switch that leads towards the Layer 3 multicast device or IGMP querier.
  Static denotes the specific port is configured to be a router port.
  Dynamic denotes the specific port is learnt to be a router port.
  Both denote the specific port is configured or learnt to be a router port.

- **Port :**

  Switch port number.

- **Status :**

  Indicate whether specific port is a router port or not.

Buttons

- **Auto-refresh :**

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

- **Refresh :**

  Click to refresh the page immediately.

- **Clear :**

  Clears all Statistics counters.

After you complete to set the IGMP Snooping function then you could let the switch to display 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.

Web Interface

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

1. Click Monitor, 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 an entry of the IGMP Snooping Groups Information.
4. Click “<< or >> “to move to previous or next entry.

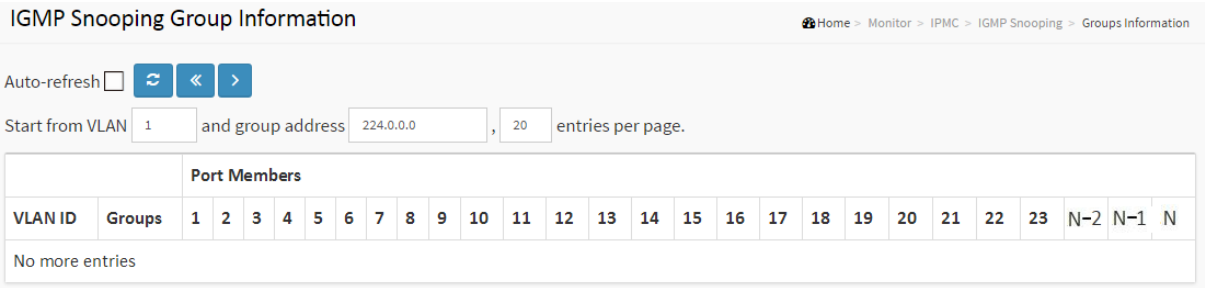


Figure 3-10.1.2: The IGMP Snooping Groups Information.

Parameter description:

IGMP Group Table Columns

- **VLAN ID :**

  VLAN ID of the group.

- **Groups :**

  Group address of the group displayed.

- **Port Members :**

  Ports under this group.

Buttons

- **Auto-refresh :**

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

- **Refresh :**

  Click to refresh the page immediately.

- « :

  Updates the table, starting with the first entry in the IGMP Group Table.

- < :

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

Entries in the IGMP SFM Information Table are shown on this page. The IGMP SFM (Source-Filtered Multicast) Information Table also contains the SSM (Source-Specific Multicast) information. This table is sorted first by VLAN ID, then by group, and then by Port. Different source addresses belong to the same group are treated as single entry.

Web Interface

To display the IPv4 SSM Information in the web interface:

1. Click Monitor, IGMP Snooping, IPv4 SSM Information
2. If you want to auto-refresh the information then you need to evoke the "Auto-refresh".
3. Click "Refresh" to refresh an entry of the IPv4 SFM Information.
4. Click "<< or >> "to move to previous or next entry.

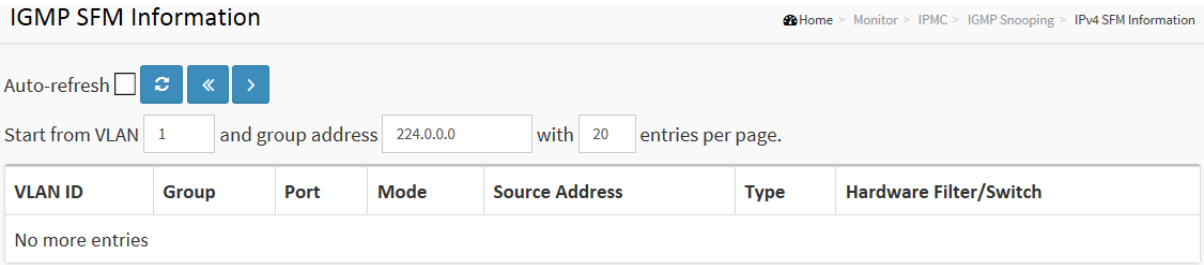


Figure 3-10.1.3: The IPv4 SFM Information.

Parameter description:

IGMP SFM Information Table Columns

- **VLAN ID :**

  VLAN ID of the group.

- **Group :**

  Group address of the group displayed.

- **Port :**

  Switch port number.

- **Mode :**

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

- **Source Address :**

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

- **Type :**

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

- **Hardware Filter/Switch**

  Indicates whether data plane destined to the specific group address from the source IPv4 address could be handled by chip or not.

  Ports under this group.

Buttons

- **Auto-refresh :**

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

- **Refresh :**

  Click to refresh the page immediately.

- **:**

  Updates the table, starting with the first entry in the IGMP Group Table.

- **:**

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

3-10.2 MLD Snooping

3-10.2.1 Status

The section describes when you complete the MLD Snooping and how to display the MLD Snooping Status and detail information. It will help you to find out the detail information of MLD Snooping status.

Web Interface

To display the MLD Snooping Status in the web interface:

1. Click Monitor, MLD Snooping and Status.
2. If you want to auto-refresh the information then you need to evoke the “Auto-refresh”.
3. Click “Refresh” to refresh an entry of the MLD Snooping Status Information.
4. Click “Clear “to clear the MLD Snooping Status.

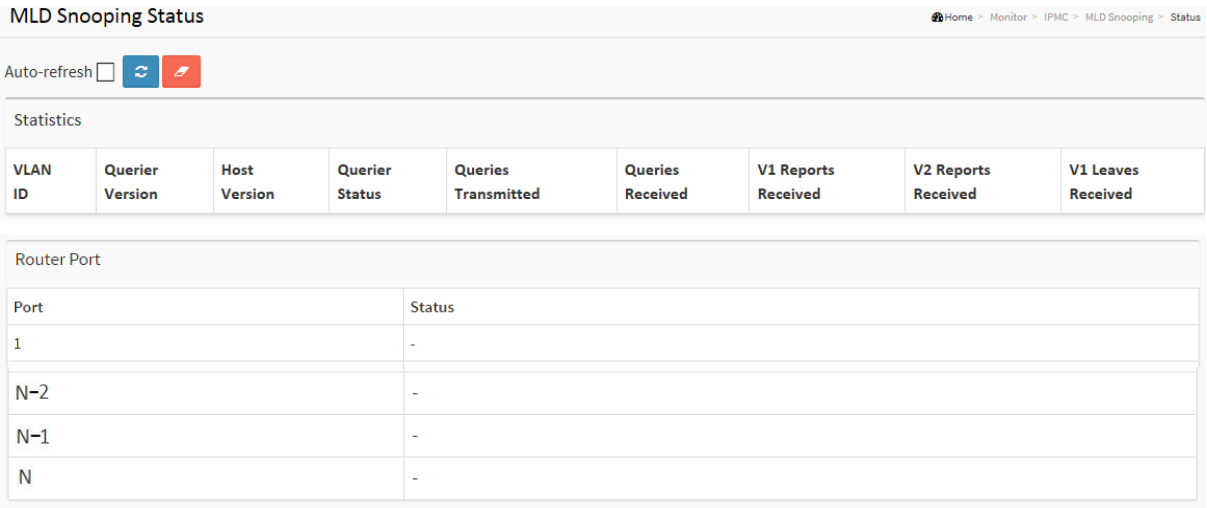


Figure 3-10.2.1: The MLD Snooping Status

Parameter description:

- **VLAN ID :**

  The VLAN ID of the entry.

- **Querier Version :**

  Working Querier Version currently.

- **Host Version :**

  Working Host Version currently.

- **Querier Status :**

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

  "DISABLE" denotes the specific interface is administratively disabled.

- **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.

- **Router Port :**

  Display which ports act as router ports. A router port is a port on the Ethernet switch that leads towards the Layer 3 multicast device or MLD querier.
  Static denotes the specific port is configured to be a router port.
  Dynamic denotes the specific port is learnt to be a router port.
  Both denote the specific port is configured or learnt to be a router port.

- **Port :**

  Switch port number.

- **Status :**

  Indicate whether specific port is a router port or not.

Buttons

- **Auto-refresh :**

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

- **Refresh :**

  Click to refresh the page immediately.

- **Clear :**

  Clears all Statistics counters.

The section describes user could 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

Web Interface

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

1. Click Monitor, MLD Snooping and Group Information
2. If you want to auto-refresh the information then you need to evoke the “Auto-refresh”
3. Click “Refresh” to refresh an entry of the MLD Snooping Group Information.
4. Click “Clear “to clear the MLD Snooping Groups information..

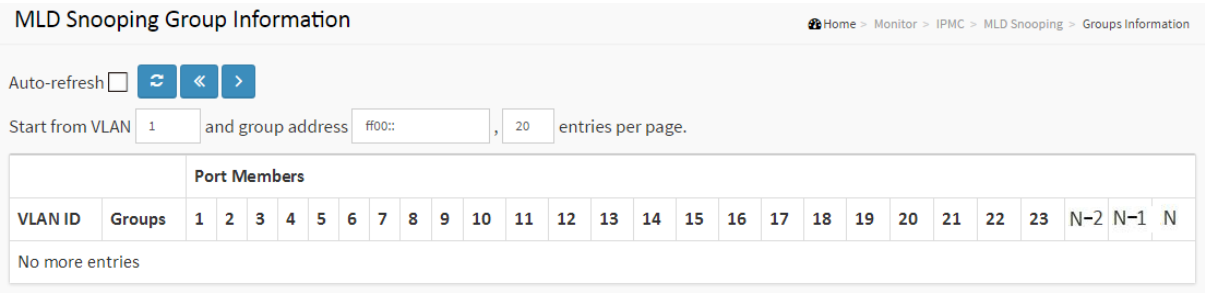


Figure 3-10.2.2: The MLD Snooping Groups Information

Parameter description:

MLD Snooping Information Table Columns

- **VLAN ID :**

  VLAN ID of the group.

- **Groups :**

  Group address of the group displayed.

- **Port Members :**

  Ports under this group.

Buttons

- **Auto-refresh :**

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

- **Refresh :**

  Click to refresh the page immediately.

- **:**

Updates the table, starting with the first entry in the IGMP Group Table.

- :

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

Entries in the MLD SFM Information Table are shown on this page. The MLD SFM (Source-Filtered Multicast) Information Table also contains the SSM (Source-Specific Multicast) information. This table is sorted first by VLAN ID, then by group, and then by Port. Different source addresses belong to the same group are treated as single entry.

Web Interface

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

1. Click Monitor, MLD Snooping and IPv6 SFM Information.
2. If you want to auto-refresh the information then you need to evoke the "Auto-refresh".
3. Click "Refresh" to refresh an entry of the MLDv2 IPv6 SSM Information.
4. Click "<< or >> "to move to previous or next entry.

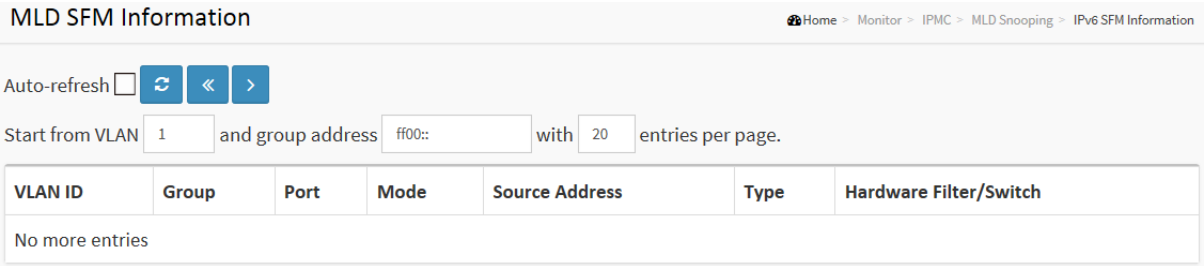


Figure 3-10.2.3: The IPv6 SFM Information

Parameter description:

MLD SFM Information Table Columns

- **VLAN ID :**

  VLAN ID of the group.

- **Group :**

  Group address of the group displayed.

- **Port :**

  Switch port number.

- **Mode :**

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

- **Source Address :**

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

- **Type :**

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

- **Hardware Filter/Switch :**

  Indicates whether data plane destined to the specific group address from the source IPv6 address could be handled by chip or not.

Buttons

- **Auto-refresh :**

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

- **Refresh :**

  Click to refresh the page immediately.

- **:**

  Updates the table, starting with the first entry in the IGMP Group Table.

- **:**

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

3-11 LLDP

3-11.1 Neighbour

This page provides a status overview for all LLDP neighbours. The displayed table contains a row for each port on which an LLDP neighbour is detected. The columns hold the following information

Web Interface

To display the LLDP neighbours:

1. Click Monitor, LLDP and Neighbours.
2. Click Refresh for manual update web screen
3. Click Auto-refresh for auto-update web screen

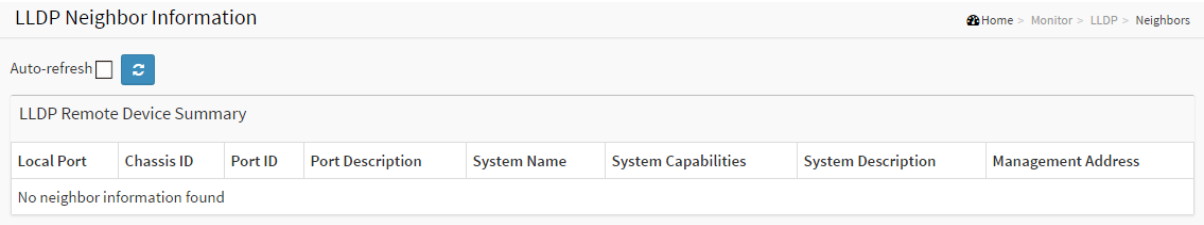


Figure 3-11.1: The LLDP Neighbours information

NOTE: If your network without any device supports LLDP then the table will show "No LLDP neighbour information found".

Parameter description:

- **Local Port :**

  The port on which the LLDP frame was received.

- **Chassis ID :**

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

- **Port ID :**

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

- **Port Description :**

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

- **System Name :**

  System Name is the name advertised by the neighbour unit.

- **System Capabilities :**

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

  1. Other
  2. Repeater

3. Bridge

4. WLAN Access Point

5. Router

6. Telephone

7. DOCSIS cable device

8. Station only

9. Reserved

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

- **Management Address :**

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

Buttons

- **Auto-refresh :**

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

- **Refresh :**

  Click to refresh the page immediately.

3-11.2 LLDP-MED Neighbour

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:

Web Interface

To display the LLDP-MED neighbor:

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

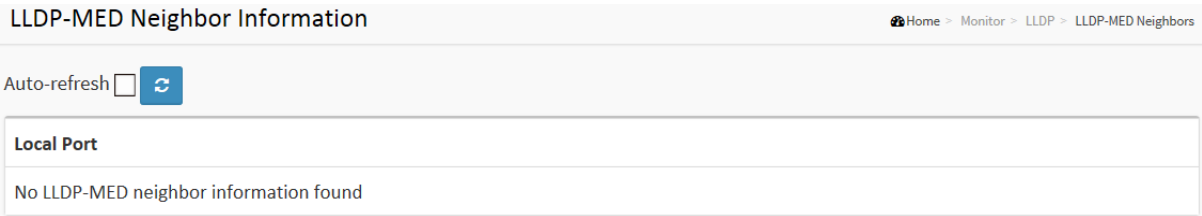


Figure 3-11.2: The LLDP-MED Neighbours information

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

Parameter description:

- **Port :**

  The port on which the LLDP frame was received.

- **Device Type :**

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

  LLDP-MED Network Connectivity Device Definition

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

  1. LAN Switch/Router

  2. IEEE 802.1 Bridge

  3. IEEE 802.3 Repeater (included for historical reasons)

  4. IEEE 802.11 Wireless Access Point

  5. Any device that supports the IEEE 802.1AB and MED extensions defined by TIA-1057 and can relay IEEE 802 frames via any method.

  LLDP-MED Endpoint Device Definition :

  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 Signalling - for use in network topologies that require a different policy for the voice signalling 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 Signalling - for use in network topologies that require a different policy for the guest voice signalling 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 through 7).

- **DSCP :**

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

- **Auto-negotiation :**

  Auto-negotiation identifies if MAC/PHY auto-negotiation is supported by the link partner.

- **Auto-negotiation status :**

  Auto-negotiation status identifies if auto-negotiation is currently enabled at the link partner. If Auto-negotiation is supported and Auto-negotiation status is disabled, the 802.3 PMD operating mode will be determined the operational MAU type field value rather than by auto-negotiation.

- **Auto-negotiation Capabilities :**

  Auto-negotiation Capabilities shows the link partners MAC/PHY capabilities.

Buttons

- **Auto-refresh :**

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

- **Refresh :**

  Click to refresh the page immediately.

3-11.3 PoE

This page allows the user to inspect the current status for all PoE ports. The section show all port Power Over Ethernet Status.

Web Interface

To display the LLDP Neighbor Power Over Ethernet information:

1. Click Monitor ,LLDP, PoE
2. Display Power Over Ethernet Status Information
3. Click Auto-refresh for auto-update web screen

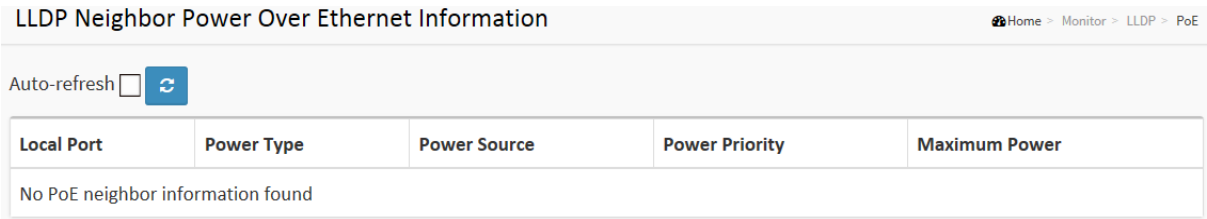


Figure 3-12.3: The LLDP Neighbors EEE information

Parameter description:

- **Local Port :**

  The port for this switch on which the LLDP frame was received.

- **Power Type :**

  The Power Type represents whether the device is a Power Sourcing Entity (PSE) or Power Device (PD).

  If the Power Type is unknown it is represented as "Reserved".

- **Power Source :**

  The Power Source represents the power source being utilized by a PSE or PD device.

  If the device is a PSE device it can either run on its Primary Power Source or its Backup Power Source. If it is unknown whether the PSE device is using its Primary Power Source or its Backup Power Source it is indicated as "Unknown"

  If the device is a PD device it can either run on its local power supply or it can use the PSE as power source. It can also use both its local power supply and the PSE.

  If it is unknown what power supply the PD device is using it is indicated as "Unknown"

- **Power Priority :**

  Power Priority represents the priority of the PD device, or the power priority associated with the PSE type device's port that is sourcing the power. There are three levels of power priority. The three levels are: Critical, High and Low.

  If the power priority is unknown it is indicated as "Unknown"

- **Maximum Power :**

  The Maximum Power Value contains a numerical value that indicates the maximum power in watts required by a PD device from a PSE device, or the minimum power a PSE device is

capable of sourcing over a maximum length cable based on its current configuration.

The maximum allowed value is 102.3 W. If the device indicates value higher than 102.3 W, it is represented as "reserved"

Buttons

- **Auto-refresh :**

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

- **Refresh :**

  Click to refresh the page immediately.

3-11.4 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.

Web Interface

To display the LLDP EEE neighbors:

1. Click Monitor, 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.

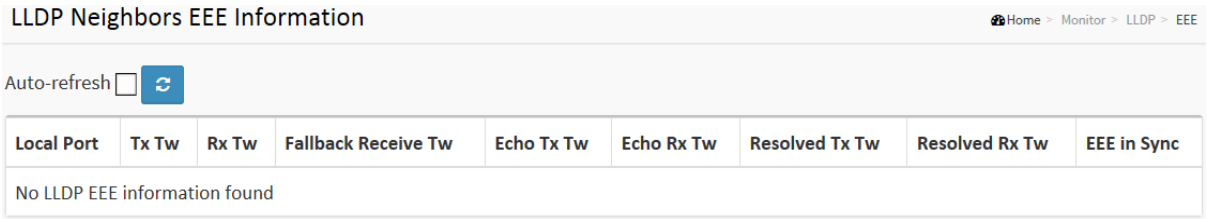


Figure 3-11.4: The LLDP Neighbors EEE information

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

Parameter description:

LLDP Neighbors EEE Information

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

- **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 hold off 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 partner's 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).

- **EEE in Sync :**

  Shows whether the switch and the link partner have agreed on wake times.

  Red - Switch and link partner have not agreed on wakeup times.

  Green - Switch and link partner have agreed on wakeup times.

Buttons

- **Auto-refresh :**

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

- **Refresh :**

  Click to refresh the page immediately.

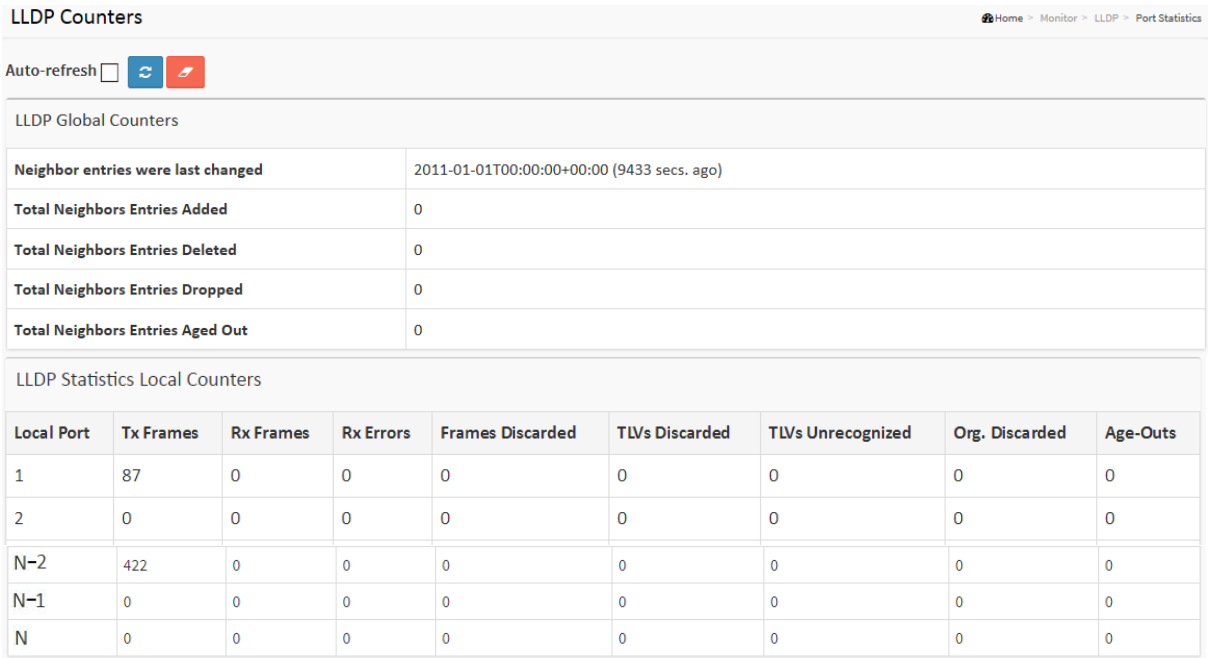
3-11.5 Port Statistics

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

Web Interface

To display the LLDP Statistics:

1. Click Monitor ,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



LLDP Counters

Home > Monitor > LLDP > Port Statistics

Auto-refresh

LLDP Global Counters

Neighbor entries were last changed	2011-01-01T00:00:00+00:00 (9433 secs. ago)
Total Neighbors Entries Added	0
Total Neighbors Entries Deleted	0
Total Neighbors Entries Dropped	0
Total Neighbors Entries Aged Out	0

LLDP Statistics Local Counters

Local Port	Tx Frames	Rx Frames	Rx Errors	Frames Discarded	TLVs Discarded	TLVs Unrecognized	Org. Discarded	Age-Outs
1	87	0	0	0	0	0	0	0
2	0	0	0	0	0	0	0	0
N-2	422	0	0	0	0	0	0	0
N-1	0	0	0	0	0	0	0	0
N	0	0	0	0	0	0	0	0

Figure 3-11.5: The LLDP Port Statistics information

Parameter description:

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

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

- **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 this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.

- **Refresh :**

  Click to refresh the page immediately.

- **Clear :**

Clears the local counters. All counters (including global counters) are cleared upon reboot.

This page allows the user to inspect the current status for all PoE ports.

Web Interface

To Display Power Over Ethernet Statistics in the web interface:

1. Click Monitor, PoE
2. Checked "Auto-refresh".
3. Click "Refresh" to refresh the port detailed statistics.

Power Over Ethernet Status

Home > Monitor > PoE

Auto-refresh

Local Port	PD class	Power Requested	Power Allocated	Power Used	Current Used	Priority	Port Status
1	-	0 [W]	0 [W]	0 [W]	0 [mA]	Low	No PD detected
2	-	0 [W]	0 [W]	0 [W]	0 [mA]	Low	No PD detected
N-3	-	0 [W]	0 [W]	0 [W]	0 [mA]	Low	No PD detected
N-2	-	0 [W]	0 [W]	0 [W]	0 [mA]	Low	No PD detected
Total		0 [W]	0 [W]	0 [W]	0 [mA]		

Figure 3-12: The PoE Statistics

Parameter description:

- **Local Port :**

  This is the logical port number for this row.

- **PD Class :**

  Each PD is classified according to a class that defines the maximum power the PD will use. The PD Class shows the PDs class.

  Five Classes are defined:

  Class 0: Max. power 15.4 W

  Class 1: Max. power 4.0 W

  Class 2: Max. power 7.0 W

  Class 3: Max. power 15.4 W

  Class 4: Max. power 30.0 W

- **Power Requested :**

  The Power Requested shows the requested amount of power the PD wants to be reserved.

- **Power Allocated :**

  The Power Allocated shows the amount of power the switch has allocated for the PD.

- **Power Used :**

  The Power Used shows how much power the PD currently is using.

- **Current Used :**

  The Power Used shows how much current the PD currently is using.

- **Priority :**

  The Priority shows the port's priority configured by the user.

- **Port Status :**

  The Port Status shows the port's status. The status can be one of the following values:

  PoE not available - No PoE chip found - PoE not supported for the port.

  PoE turned OFF - PoE disabled : PoE is disabled by user.

  PoE turned OFF - Power budget exceeded - The total requested or used power by the PDs exceeds the maximum power the Power Supply can deliver, and port(s) with the lowest priority is/are powered down.

  No PD detected - No PD detected for the port.

  PoE turned OFF - PD overload - The PD has requested or used more power than the port can deliver, and is powered down.

  PoE turned OFF - PD is off.

  Invalid PD - PD detected, but is not working correctly.

Buttons

- **Auto-refresh :**

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

- **Refresh :**

  Click to refresh the page immediately.

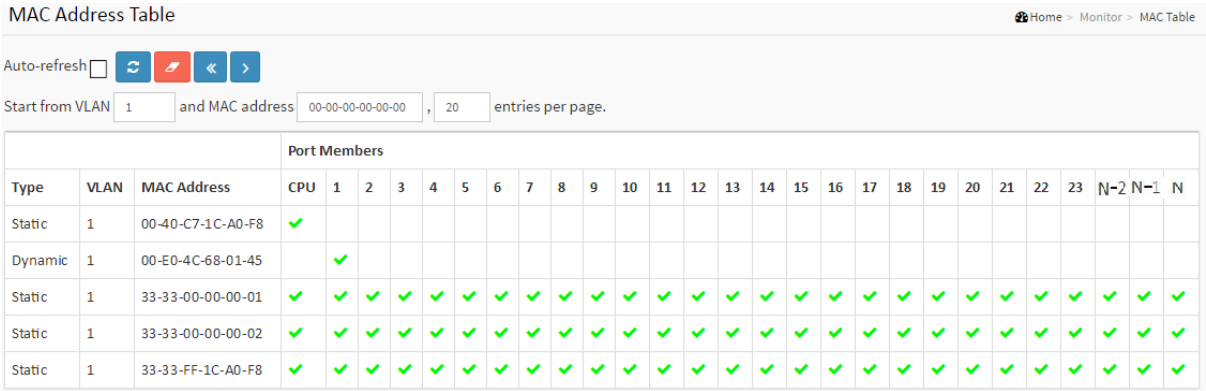
3-13 MAC Table

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

Web Interface

To Display MAC Address Table in the web interface:

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



			Port Members																									
Type	VLAN	MAC Address	CPU	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	N-2	N-1	N
Static	1	00-40-C7-1C-A0-F8	✔																										
Dynamic	1	00-E0-4C-68-01-45		✔																									
Static	1	33-33-00-00-00-01	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔
Static	1	33-33-00-00-00-02	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔
Static	1	33-33-FF-1C-A0-F8	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔

Figure 3-13: The MAC Address Table

Parameter description:

MAC Table Columns

- **Switch (stack only) :**

  The stack unit where the entry is learned.

- **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 this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.

- **Refresh :**

  Refreshes the displayed table starting from the "Start from MAC address" and "VLAN" input

fields.

- **Clear :**

  Flushes the selected log entries.

- **:**

  Updates the table starting from the first entry in the MAC Table, i.e. the entry with the lowest VLAN ID and MAC address

- **:**

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

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.

3-14.1 Membership

This page provides an overview of membership status of VLAN users.

Web Interface

To display the VLAN membership configuration in the web interface:

1. Click Monitor, VLANs and VLAN membership.
2. Scroll the bar to choice which VLANs would like to show up.
3. Click Refresh to update the state.

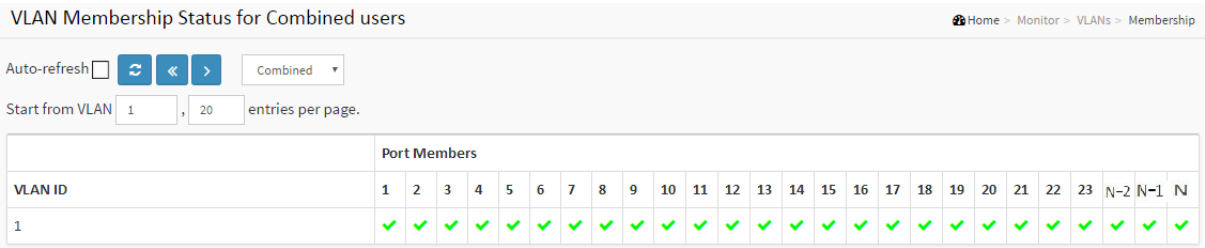


Figure 3-14.1: VLAN Membership Status for Combined users

Parameter description:

- **VLAN USER :**

  Various internal software modules may use VLAN services to configure VLAN memberships on the fly.

  The drop-down list on the right allows for selecting between showing VLAN memberships as configured by an administrator (Admin) or as configured by one of these internal software modules.

  The "Combined" entry will show a combination of the administrator and internal software modules configuration, and basically reflects what is actually configured in hardware.

- **VLAN ID :**

  VLAN ID for which the Port members are displayed.

- **Port Members :**

  A row of check boxes for each port is displayed for each VLAN ID.
  If a port is included in a VLAN, an image ✓ will be displayed.
  If a port is included in a Forbidden port list, an image ✗ will be displayed.
  If a port is included in a Forbidden port list and dynamic VLAN user register VLAN on same Forbidden port, then conflict port will be displayed as ✗c.

- **VLAN Membership**

  The VLAN Membership Status Page shall show the current VLAN port members for all VLANs configured by a selected VLAN User (selection shall be allowed by a Combo Box). When ALL VLAN Users are selected, it shall show this information for all the VLAN Users,

and this is by default. VLAN membership allows the frames classified to the VLAN ID to be forwarded on the respective VLAN member ports.

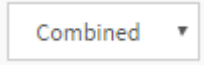
Buttons

- **Auto-refresh :**

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

- **Refresh :**

  Refreshes the displayed table starting from the "Start from MAC address" and "VLAN" input fields.

- 

Combined :

  Select VLAN Users from this drop down list.

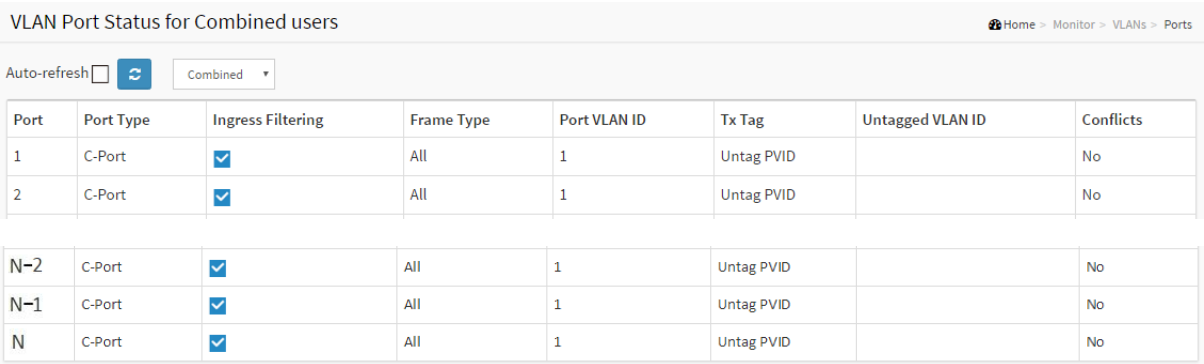
3-14.2 Port

The function Port Status gathers the information of all VLAN status and reports it by the order of Static NAS MVRP MVP Voice VLAN MSTP GVRP Combined.

Web Interface

To Display VLAN Port Status in the web interface:

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



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

Figure 3-14.2: The VLAN Port Status for Static user

Parameter description:

- **VLAN USER :**

  VLAN User module uses services of the VLAN management functionality to configure VLAN memberships and VLAN port configuration such as PVID, UVID. Currently we support following VLAN User types:

  CLI/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.

  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.

- **Port :**

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

- **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.

- **Port VLAN ID :**

  Shows the Port VLAN ID (PVID) that a given user wants the port to have.

  The field is empty if not overridden by the selected user.

- **Tx Tag :**

  Shows egress filtering frame status whether tagged or untagged.

- **UVID :**

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

- **Conflicts :**

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

  Functional Conflicts between features.

  Conflicts due to hardware limitation.

  Direct conflict between user modules.

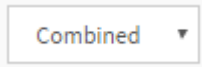
Buttons

- **Auto-refresh :**

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

- **Refresh :**

  Click to refresh the page immediately.

- 

Combined :

  Select VLAN Users from this drop down list.

3-15.1 MAC-based VLAN

This section shows MAC-based VLAN entries configured by various MAC-based VLAN users. Currently we support following VLAN User types:

CLI/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.

Web Interface

To Display MAC-based VLAN configuration in the web interface:

1. Click Monitor and MAC-based VLAN Status.
2. Specify the Static, NAS, Combined.
3. Display MAC-based information.

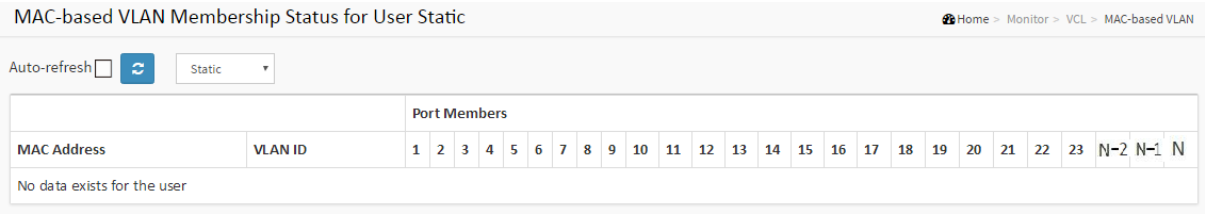


Figure 3-15.1: The MAC-based VLAN Membership Status for User Static

Parameter description:

- **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 :**

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

- **Refresh :**

  Click to refresh the page immediately.

3-15.2 Protocol-based VLAN

3-15.2.1 Protocol to Group

This page shows you the protocols to Group Name (unique for each Group) mapping entries for the switch.

Web Interface

To Display Protocol-based VLAN configuration in the web interface:

1. Click Monitor, VCL and Protocol to Group.
2. Checked "Auto-refresh".
3. Click "Refresh" to refresh the port detailed statistics.

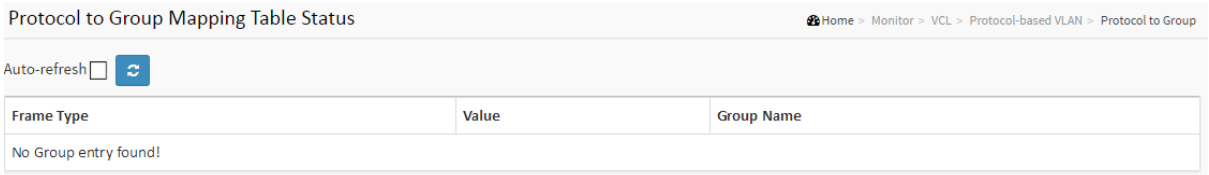


Figure 3-15.2.1: The protocol to Group for Protocol-based VLAN

Parameter description:

- **Frame Type :**

  Frame Type can have one of the following values:

  1. Ethernet
  2. LLC
  3. SNAP

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

- **Value :**

  Valid value that can be entered in this text field depends on the option selected from the preceding Frame Type selection menu.

  Below is the criteria for three different Frame Types:

  1. For Ethernet: Values in the text field when Ethernet is selected as a Frame Type is called etype. Valid values for etype ranges from 0x0600-0xffff

  2. For LLC: Valid value in this case is comprised of two different sub-values.

  a. DSAP: 1-byte long string (0x00-0xff)

  b. SSAP: 1-byte long string (0x00-0xff)

3. For SNAP: Valid value in this case also is comprised of two different sub-values.

a. OUI: OUI (Organizationally Unique Identifier) is value in format of xx-xx-xx where each pair (xx) in string is a hexadecimal value ranges from 0x00-0xff.

b. PID: If the OUI is hexadecimal 000000, the protocol ID is the Ethernet type (EtherType) field value for the protocol running on top of SNAP; if the OUI is an OUI for a particular organization, the protocol ID is a value assigned by that organization to the protocol running on top of SNAP.

In other words, if value of OUI field is 00-00-00 then value of PID will be etype (0x0600-0xffff) and if value of OUI is other than 00-00-00 then valid value of PID will be any value from 0x0000 to 0xffff.

- **Group Name :**

A valid Group Name is a unique 16-character long string for every entry which consists of a combination of alphabets (a-z or A-Z) and integers (0-9).

NOTE:
special character and underscore(_) are not allowed.

Buttons

- **Auto-refresh :**

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

- **Refresh :**

Click to refresh the page immediately.

This page shows you the configured Group Name to a VLAN for the switch.

Web Interface

To Display Group to VLAN configuration in the web interface:

1. Click Monitor, VCL, Group to VLAN.
2. Checked "Auto-refresh".
3. Click "Refresh" to refresh the port detailed statistics.

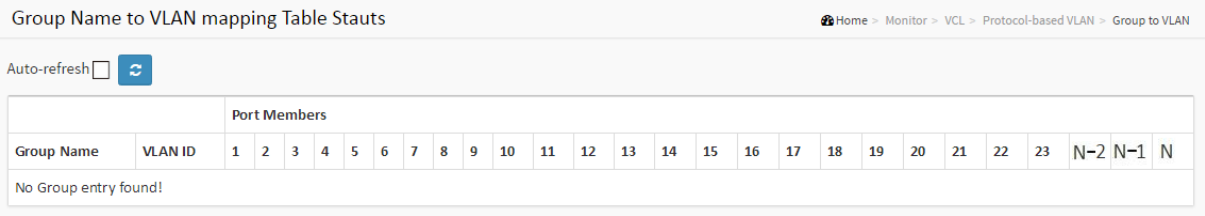


Figure 3-15.2.2: The Group Name to VLAN mapping Table Status

Parameter description:

- **Group Name :**

  A valid Group Name is a string at the 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 pre-used 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.

Buttons

- **Auto-refresh :**

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

- **Refresh :**

  Click to refresh the page immediately.

3-15.3 IP Subnet-based VLAN

The page shows IP subnet-based VLAN entries. This page shows only static entries.

Web Interface

To Display MAC-based VLAN configuration in the web interface:

1. Click Monitor, VCL and IP Subnet-based VLAN.
2. Checked "Auto-refresh".
3. Click "Refresh" to refresh the port detailed statistics.

Figure 3-15.3: The IP Subnet-based VLAN Membership Status

Parameter description:

- **VCE ID :**

  Indicates the index of the entry. It is user configurable. Its value ranges from 0-128. If a VCE ID is 0, application will auto-generate the VCE ID for that entry. Deletion and lookup of IP subnet-based VLAN are based on VCE ID.

- **IP Address :**

  Indicates the IP address.

- **Mask Length :**

  Indicates the network mask length.

- **VLAN ID :**

  Indicates the VLAN ID. VLAN ID can be changed for the existing entries.

- **Port Members :**

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

Buttons

- **Auto-refresh :**

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

- **Refresh :**

  Click to refresh the page immediately.

3-16 sFlow

This session shows receiver and per-port sFlow statistics

Web Interface

To Display port sFlow statistics in the web interface:

1. Click Monitor and sFlow.
2. Display sFlow information.

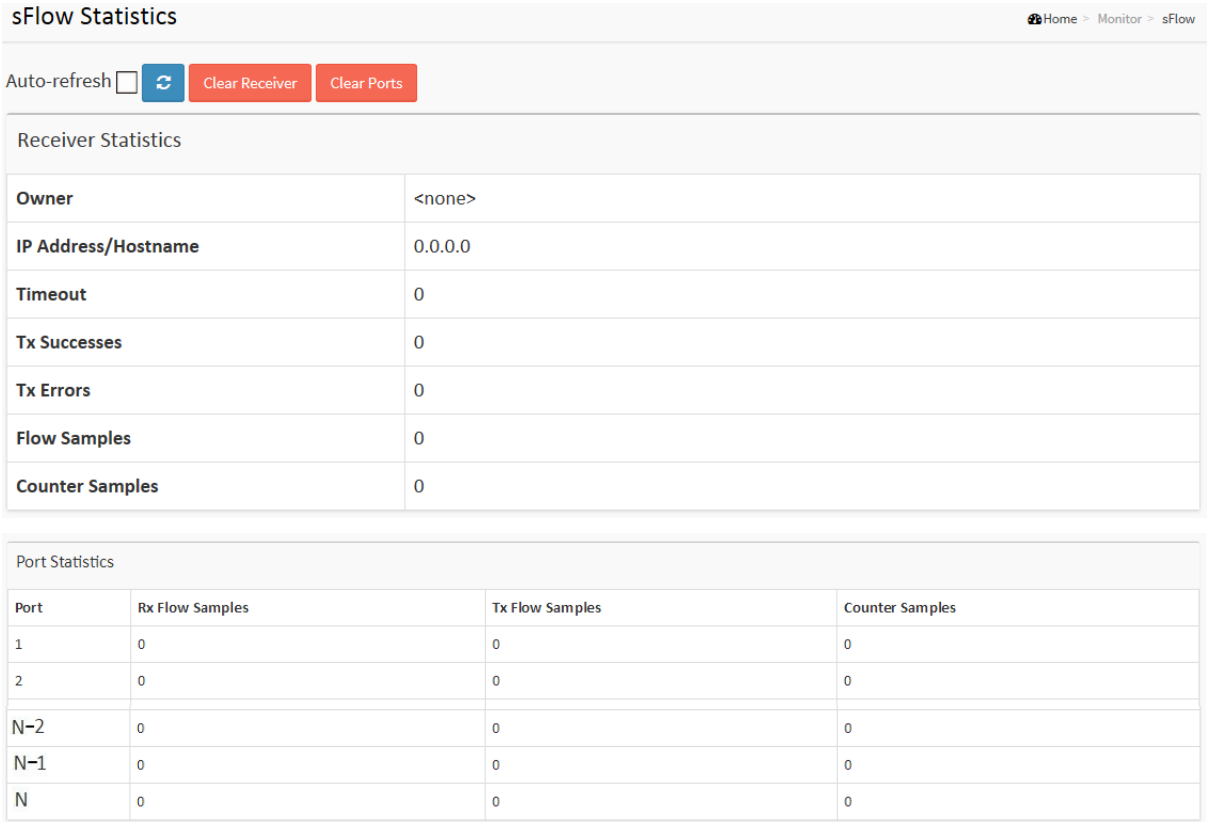


Figure 3-16: The sFlow Statistics

Parameter description:

Receiver Statistics

- **Owner :**

  This field shows the current owner of the sFlow configuration. It assumes one of three values as follows:

  • If sFlow is currently unconfigured/unclaimed, Owner contains <none>.

  • If sFlow is currently configured through Web or CLI, Owner contains <Configured through local management>.

  • If sFlow is currently configured through SNMP, Owner contains a string identifying the

sFlow receiver.`

- **IP Address/Hostname :**

  The IP address or hostname of the sFlow receiver.

- **Timeout :**

  The number of seconds remaining before sampling stops and the current sFlow owner is released.

- **Tx Successes :**

  The number of UDP datagrams successfully sent to the sFlow receiver.

- **Tx Errors :**

  The number of UDP datagrams that has failed transmission.
  The most common source of errors is invalid sFlow receiver IP/hostname configuration. To diagnose, paste the receiver's IP address/hostname into the Ping Web page (Diagnostics → Ping/Ping6).

- **Flow Samples :**

  The total number of flow samples sent to the sFlow receiver.

- **Counter Samples :**

  The total number of counter samples sent to the sFlow receiver.

Port Statistics

- **Port :**

  The port number for which the following statistics applies.

- **Rx and Tx Flow Samples :**

  The number of flow samples sent to the sFlow receiver originating from this port. Here, flow samples are divided into Rx and Tx flow samples, where Rx flow samples contains the number of packets that were sampled upon reception (ingress) on the port and Tx flow samples contains the number of packets that were sampled upon transmission (egress) on the port.

- **Counter Samples :**

  The total number of counter samples sent to the sFlow receiver originating from this port.

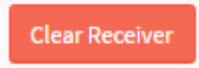
Buttons

- **Auto-refresh :**

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

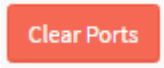
- **Refresh :**

  Click to refresh the page immediately.

- 

Clear Receiver :

  Clears the sFlow receiver counters.

- 

Clear Ports :

  Clears the per-port counters.

Chapter 4 Diagnostics

This chapter provides a set of basic system diagnosis. It let users know that whether the system is health or needs to be fixed. The basic system check includes ICMP Ping, Link OAM, ICMPv6, and VeriPHY Cable Diagnostics.

4-1 Ping

This section allows you to issue ICMP PING packets to troubleshoot IPv6 connectivity issues.

Web Interface

To configure an ICMP PING Configuration in the web interface:

1. Specify ICMP PING IP Address.
2. Specify ICMP PING Size.
3. Click Start.

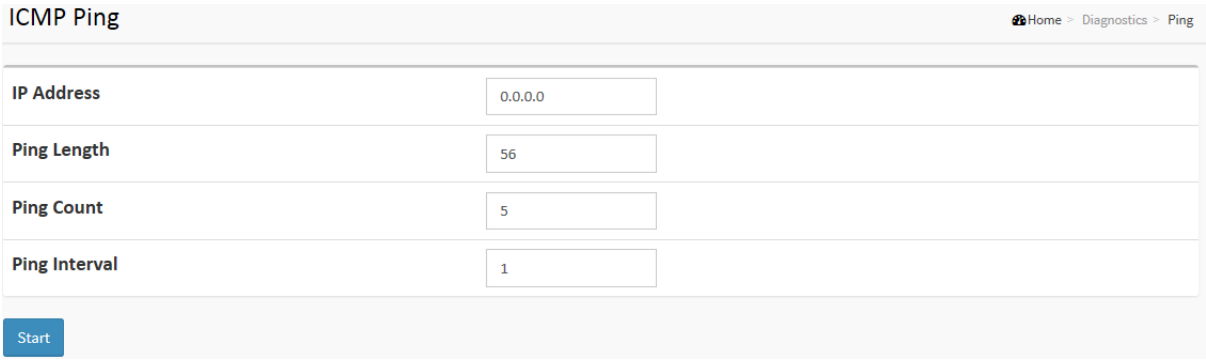


Figure 4-1: The ICMP Ping

Parameter description:

- **IP Address :**

  To set the IP Address of device what you want to ping it.

- **Ping Length :**

  The payload size of the ICMP packet. Values range from 2 bytes to 1452 bytes.

- **Ping Count :**

  The count of the ICMP packet. Values range from 1 time to 60 times.

- **Ping Interval :**

The interval of the ICMP packet. Values range from 0 second to 30 seconds.

Buttons

- **Start :**

  Click the "Start" button then the switch will start to ping the device using ICMP packet size what set on the switch.

  After you press , 5 ICMP packets are transmitted, and the sequence number and roundtrip time are displayed upon reception of a reply. The page refreshes automatically until responses to all packets are received, or until a timeout occurs.

  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

4-2 Ping6

This section allows you to issue ICMPv6 PING packets to troubleshoot IPv6 connectivity issues.

Web Interface

To configure an ICMPv6 PING Configuration in the web interface:

1. Specify ICMPv6 PING IP Address.
2. Specify ICMPv6 PING Size.
3. Click Start.

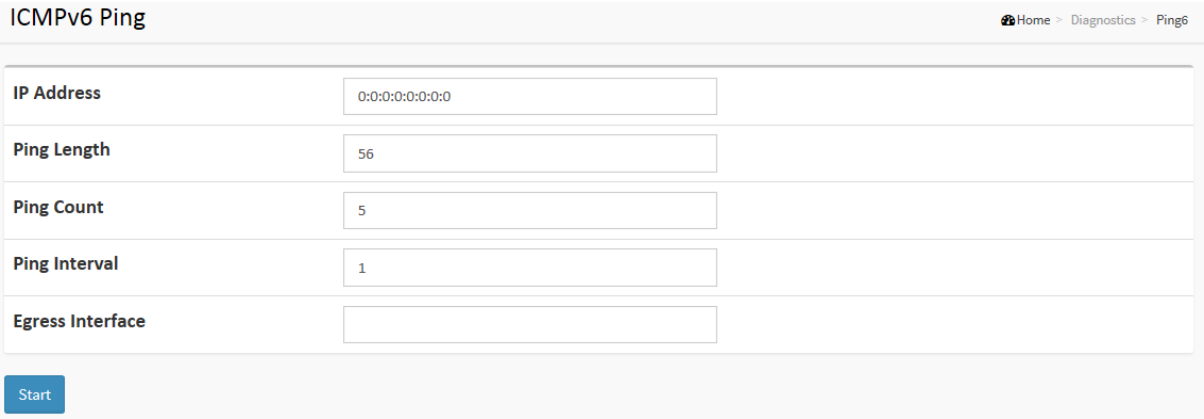


Figure 4-2: The ICMPv6 Ping

Parameter description:

- **IP Address :**

  The destination IP Address with IPv6

- **Ping Length :**

  The payload size of the ICMP packet. Values range from 2 bytes to 1452 bytes.

- **Ping Count :**

  The count of the ICMP packet. Values range from 1 time to 60 times.

- **Ping Interval :**

  The interval of the ICMP packet. Values range from 0 second to 30 seconds.

- **Egress Interface (Only for IPv6) :**

  The VLAN ID (VID) of the specific egress IPv6 interface which ICMP packet goes.
  The given VID ranges from 1 to 4094 and will be effective only when the corresponding IPv6 interface is valid.
  When the egress interface is not given, PING6 finds the best match interface for destination.
  Do not specify egress interface for loopback address.
  Do specify egress interface for link-local or multicast address.

Buttons

- **Start :**

Click the "Start" button then the switch will start to ping the device using ICMPv6 packet size what set on the switch.

After you press, 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.

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

64 bytes from fe80::219:5bff:fe2f:b47: icmp_seq=0, time=10ms

64 bytes from fe80::215:58ff:feed:69dd: icmp_seq=0, time=10ms

64 bytes from fe80::219:5bff:fe2f:b47: icmp_seq=1, time=0ms

64 bytes from fe80::215:58ff:feed:69dd: icmp_seq=1, time=0ms

64 bytes from fe80::219:5bff:fe2f:b47: icmp_seq=2, time=0ms

64 bytes from fe80::215:58ff:feed:69dd: icmp_seq=2, time=0ms

64 bytes from fe80::219:5bff:fe2f:b47: icmp_seq=3, time=0ms

64 bytes from fe80::215:58ff:feed:69dd: icmp_seq=3, time=0ms

64 bytes from fe80::219:5bff:fe2f:b47: icmp_seq=4, time=0ms

64 bytes from fe80::215:58ff:feed:69dd: icmp_seq=4, time=0ms

Sent 5 packets, received 10 OK, 0 bad

You can configure the following properties of the issued ICMP packets:

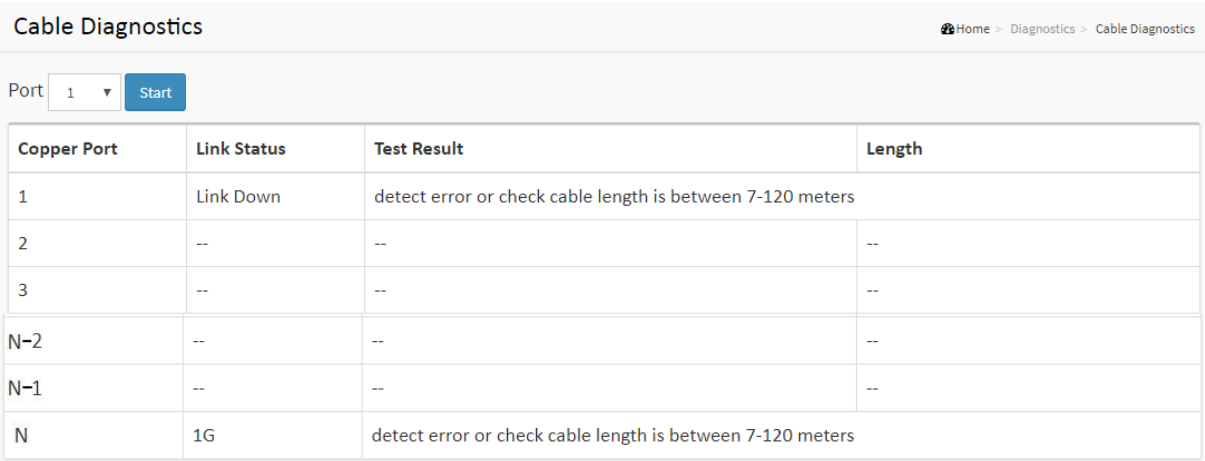
4-3 Cable Diagnostics

This page is used for running the Cable Diagnostics for 10/100 and 1G copper ports. Press to run the diagnostics. This will take approximately 5 seconds. When completed, the page refreshes automatically, and you can view the cable diagnostics results in the cable status table. Note that Cable Diagnostics is only accurate for cables of length 7 - 120 meters with 5-meter accuracy.
10 and 100 Mbps ports will be linked down while running Cable Diagnostics. Therefore, running Cable Diagnostics on a 10 or 100 Mbps management port will cause the switch to stop responding until Cable Diagnostics is complete.

Web Interface

To configure Cable Diagnostics in the web interface:

1. Specify each port cable diagnostics.
2. Click Start.



Copper Port	Link Status	Test Result	Length
1	Link Down	detect error or check cable length is between 7-120 meters	
2	--	--	--
3	--	--	--
N-2	--	--	--
N-1	--	--	--
N	1G	detect error or check cable length is between 7-120 meters	

Figure 4-3: The Cable Diagnostics

Parameter description:

- **Port**

  The port where you are requesting Cable Diagnostics.

- **Copper Port**

  Copper port number.

- **Link Status**

  The status of the cable.

  10M:

  Cable is link up and correct. Speed is 10Mbps

  100M:

  Cable is link up and correct. Speed is 100Mbps

  1G:

Cable is link up and correct. Speed is 1Gbps

Link Down:

Link down or cable is not correct.

- **Test Result**

Test Result of the cable.

OK:

Correctly terminated pair

Abnormal:

Incorrectly terminated pair or link down

- **Length**

The length (in meters) of the cable pair. The resolution is 3 meters. When Link Status is shown as follow, the length has different definition.

1G:

The length is the minimum value of 4-pair.

10M/100M:

The length is the minimum value of 2-pair.

Link Down:

1The length is the minimum value of non-zero of 4-pair.

- **Start :**

Press this button 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 Diagnostics is only accurate for cables of length 7 - 140 meters.

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

4-4 Traceroute

This page allows you to issue ICMP, TCP, or UDP packets to diagnose network connectivity issues.

Web Interface

To configure an ICMPv6 PING Configuration in the web interface:

1. Specify traceroute IP Address.
2. Specify traceroute Size.
3. Click Start.

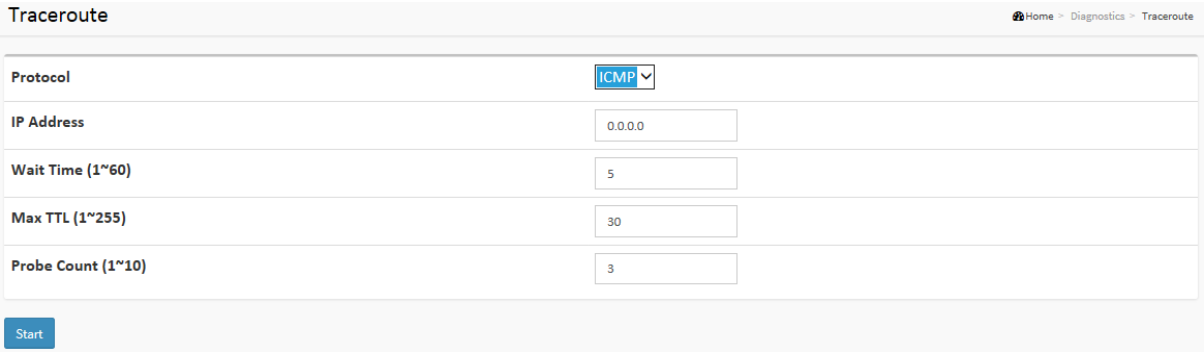


Figure 4-4: The Traceroute

Parameter description:

- **Protocol :**

  The protocol (ICMP, UDP, TCP) packets to send.

- **IP Address :**

  The destination IP Address.

- **Wait Time :**

  Set the time (in seconds) to wait for a response to a probe (default 5.0 sec). Values range from 1 to 60. The payload size of the ICMP packet. Values range from 2 bytes to 1452 bytes.

- **Max TTL :**

  Specifies the maximum number of hops (max time-to-live value) traceroute will probe. Values range from 1 to 255. The default is 30.

- **Probe Count :**

  Sets the number of probe packets per hop. Values range from 1 to 10. The default is 3.

Buttons

- **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, Traceroute sends packets with gradually increasing TTL value, starting with TTL value of 1. The first router receives the packet, decrements the TTL value and drops the packet because it then has TTL value zero. The router sends an ICMP Time Exceeded message back to the source. The next set of packets are given a TTL value of 2, so the first router forwards the packets, but the second router drops them and replies with ICMP Time Exceeded. Proceeding in this way, traceroute uses the returned ICMP Time Exceeded messages to build a list of routers that packets traverse, until the destination is reached and returns an ICMP Echo Reply message.

traceroute to 202.39.253.11 (202.39.253.11), 30 hops max, 40 byte packets
1 192.168.10.254 ae-2-3508.edge4.Atlanta2.Level3.net. (192.168.10.254) 10 ms 10 ms 10 ms
2 59-125-13-254.HINET-IP.hinet.net. (59.125.13.254) 20 ms 20 ms 20 ms
3 h146.s228.ts.hinet.net. (168.95.228.146) 20 ms 10 ms 20 ms
4 tchn-3011.hinet.net. (220.128.16.194) 20 ms TCHN-3112.hinet.net. (220.128.17.142) 20 ms tchn-3011.hinet.net. (220.128.16.202) 20 ms
5 TPDT-3012.hinet.net. (220.128.17.6) 20 ms TPDT-3011.hinet.net. (220.128.16.10) 20 ms TPDT-3012.hinet.net. (220.128.17.6) 40 ms
6 CHCH-3112.hinet.net. (220.128.2.13) 20 ms tchn-3011.hinet.net. (220.128.1.9) 10 ms CHCH-3112.hinet.net. (220.128.2.13) 30 ms
7 211.22.41.237 CHCH-3112.hinet.net. (211.22.41.237) 20 ms 30 ms 30 ms
8 202-39-253-11.HINET-IP.hinet.net. (202.39.253.11) 10 ms 10 ms

You can configure the following properties:

Chapter 5 Maintenance

This chapter describes the entire switch Maintenance configuration tasks to enhance the performance of local network including Restart Device, Firmware upgrade, Save/Restore, Import/Export.

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.

Web Interface

To configure a Restart Device Configuration in the web interface:

1. Chick Restart Device.
2. Click Yes.

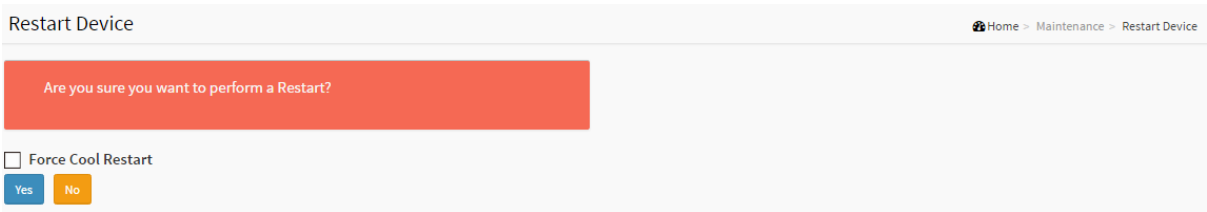


Figure 5-1: Restart Device

Parameter description:

Restart Device :

You can restart the switch on this page. After restart, the switch will boot normally.

Buttons

- **Force Cool Restart :**

  Uncheck "Force Cool Restart" if you want to perform a warm restart of the switch.

  Check "Force Cool Restart" if you want to simulate a power-on (cold restart) of the switch.

WARNING: Forcing a cool restart will affect the traffic going through the switch.

- **Yes :**

  Click to restart device

- **No :**

  Click to return to the Port State page without restarting.

5-2 Reboot Schedule

This page allows user to schedule the time to reboot the switch.

Web Interface

To configure a Reboot Schedule Configuration in the web interface:

1. Chick Maintenance and Reboot Schedule.
2. Click apply to save changes.

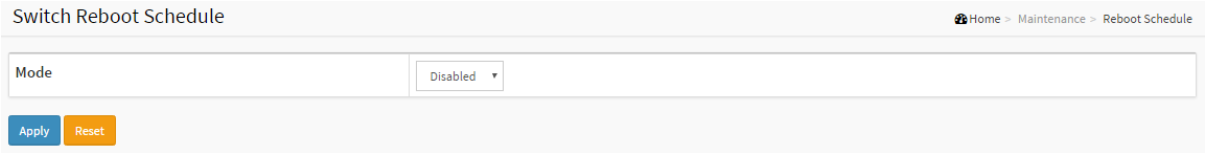


Figure 5-2: Reboot Schedule

Parameter description:

- **Mode :**

  Indicates the reboot scheduling mode operation. Possible modes are:

  Enabled: Enable switch reboot scheduling.

  Disabled: Disable switch reboot scheduling.

- **Week Day :**

  The day to reboot this switch.

- **Reboot Time :**

  The time to reboot the switch.

Buttons

- **Apply :**

  Click to save changes.

- **Reset :**

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

You can reset the configuration of the switch on this page. Only the IP configuration is retained. The new configuration is available immediately, which means that no restart is necessary.

Web Interface

To configure a Factory Defaults Configuration in the web interface:

1. Chick Maintenance and Factory Defaults.
2. Click Yes.

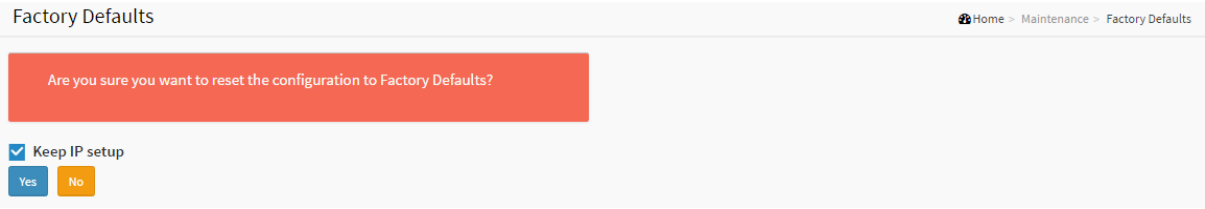


Figure 5-3: The Factory Defaults

Parameter description:

Buttons

- **Keep IP setup :**

  Check "Keep IP setup" if you want to keep current IP setting

- **Yes :**

  Click to reset the configuration to Factory Defaults.

- **No :**

  Click to return to the Port State page without restarting.

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

5-4 Firmware

This section describes how to upgrade Firmware. The Switch can be enhanced with more value-added functions by installing firmware upgrades.

5-4.1 Firmware upgrade

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

Web Interface

To configure a Firmware Upgrade Configuration in the web interface:

1. Chick Browser to select Maintenance/Software in you device.
2. Click Download.

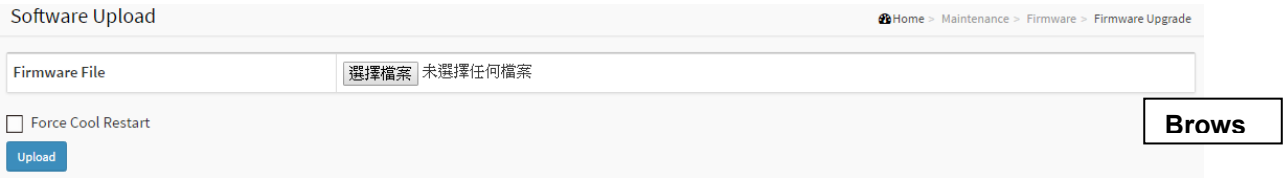


Figure 5-4.1: The firmware Download

Parameter description:

Buttons

- **Force Cool Restart :**

  Uncheck "Force Cool Restart" if you want to perform a warm restart of the switch after the software upload.
  Check "Force Cool Restart" if you want to simulate a power-on (cold restart) of the switch after the software upload.

WARNING: Forcing a cool restart will affect the traffic going through the switch.

- **Browse :**

  Click the “Browse...” button to search the Firmware URL and filename and click “Upload”.

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 all managed

switches restart. 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.

5-4.2 Firmware Selection

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

The web page displays two tables with information about the active and alternate firmware images.

NOTE: In case the active firmware image is the alternate image, only the "Active Image" table is shown. In this case, the Activate Alternate Image button is also disabled.

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.

The firmware version and date information may be empty for older firmware releases. This does not constitute an error.

Web Interface

To configure a Firmware Upgrade Configuration in the web interface:

1. Chick Browser to select Maintenance/Software in you device.
2. Click Image Select.

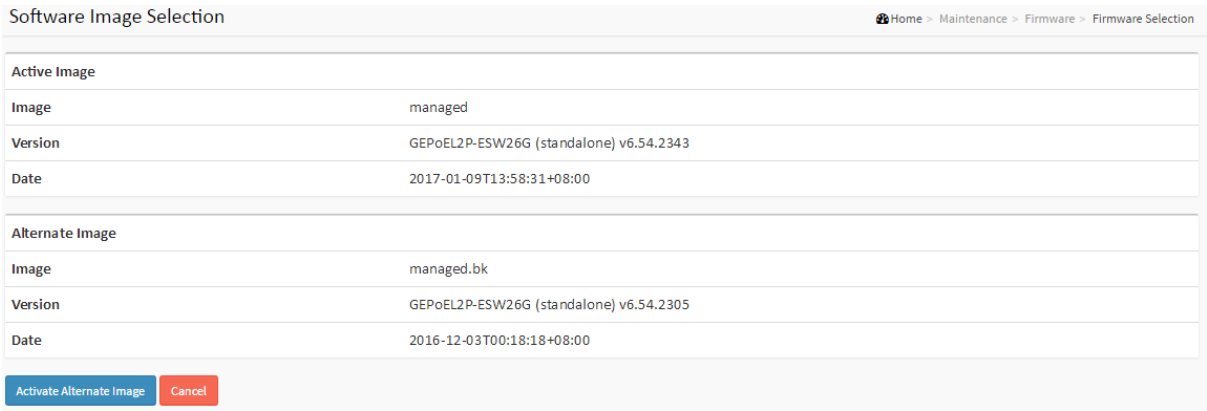


Figure 5-4.2: The Firmware selection

Parameter description:

Image Information

- **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.

Buttons

- **Activate Alternate Image :**

  Click to use the "Activate Alternate Image". This button may be disabled depending on system state.

- **Cancel :**

  Cancel activating the backup image. Navigates away from this page.

5-5 Configuration

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

There are three system files:

- running-config: A virtual file that represents the currently active configuration on the switch. This file is volatile.
- startup-config: The startup configuration for the switch, read at boot time.
- default-config: A read-only file with vendor-specific configuration. This file is read when the system is restored to default settings.

It is also possible to store up to two other files and apply them to running-config, thereby switching configuration.

5-5.1 Save startup-config

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

Web Interface

To save running configuration in the web interface:

1. Chick Browser to select Maintenance/Configuration in you device.
2. Click Apply Startup-Config Select.

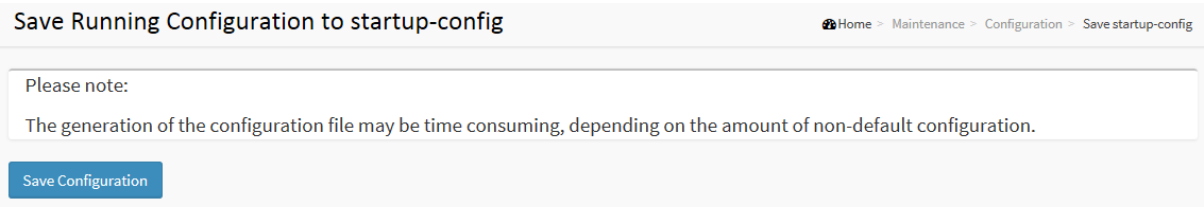


Figure 5-5.1: The Save Startup Configuration

Parameter description:

Buttons

- **Save Configuration:**

  Click to save configuration, the running configuration will be written to flash memory for system boot up to load this startup configuration file.

5-5.2 Download

This section describes to export the Switch Configuration for maintenance needs. Any current configuration files will be exported as text format.

It is possible to download a file from the web browser to all the files on the switch, except default-config, which is read-only.

Select the file to download, select the destination file on the target, and click.

If the destination is running-config, the file will be applied to the switch configuration. This can be done in two ways:

- Replace mode: The current configuration is fully replaced with the configuration in the downloaded file.
- Merge mode: The downloaded file is merged into running-config.

If the file system is full (i.e. contains the three system files mentioned above plus two other files), it is not possible to create new files, but an existing file must be overwritten or another deleted first.

Web Interface

To download configuration in the web interface:

1. Chick Browser to select Maintenance/Configuration in you device.
2. Click Download Select.

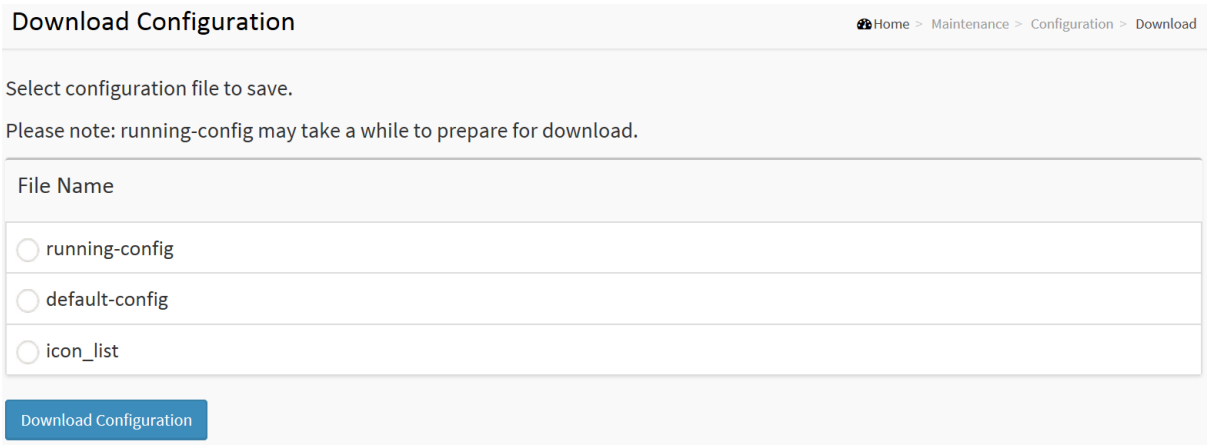


Figure 5-5.2: Configuration Download

Parameter description:

Buttons

- **Download :**

  Click the "Download" button then the switch will start to download the configuration from configuration stored location PC or Server.

5-5.3 Upload

The configuration upload function will be backuped and saved configuration from the switch's configuration into the running web browser PC.

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

Web Interface

To upload configuration in the web interface:

1. Chick Browser to select Maintenance/Configuration in you device.
2. Click upload Select.

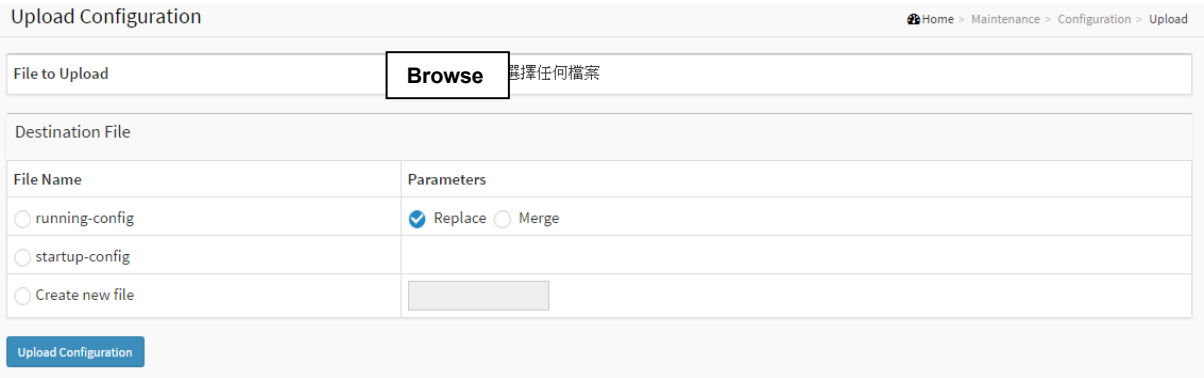


Figure 5-5.3: Configuration upload

Parameter description:

- **running-config :**

  the file will be applied to the switch configuration. This can be done in two ways:

  Replace mode: The current configuration is fully replaced with the configuration in the uploaded file.

  Merge mode: The uploaded file is merged into running-config.

- **startup-config :**

  The startup configuration for the switch, read at boot time.

- **default-config :**

  A read-only file with vendor-specific configuration. This file is read when the system is restored to default settings.

Buttons

- **Upload Configuration :**

  Click the "Upload" button then the running web management PC will start to upload the configuration from the managed switch configuration into the location PC, user can

configure web browser's upload file path to keep configuration file.

5-5.4 Activate

It is possible to activate any of the configuration files present on the switch, except for running-config which represents the currently active configuration.

Select the file to activate and click. This will initiate the process of completely replacing the existing configuration with that of the selected file.

Web Interface

To activate configuration in the web interface:

1. Chick Browser to select Maintenance/Configuration in you device.
2. Click Activate Select.

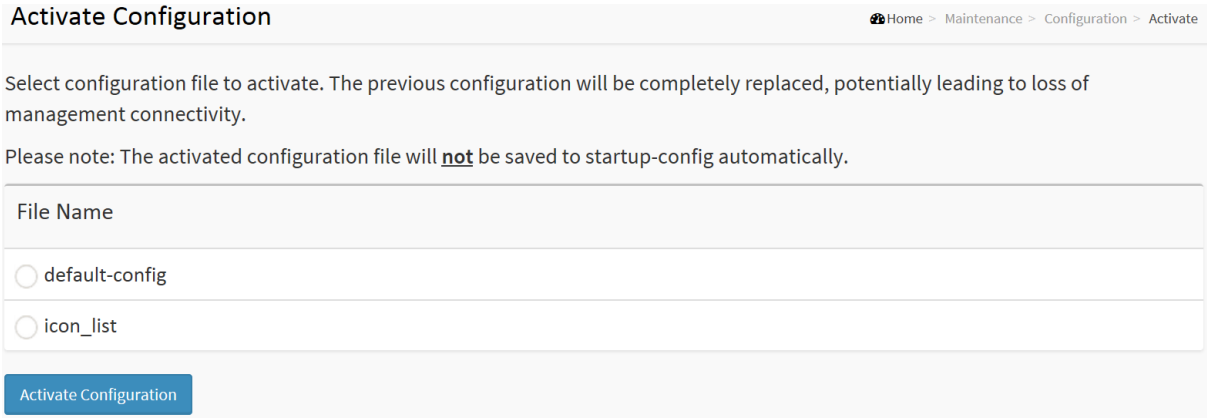


Figure 5-5.4: Configuration Activation

Parameter description:

- **default-config :**

  A read-only file with vendor-specific configuration. This file is read when the system is restored to default settings.

Buttons

- **Activate Configuration :**

  Click the "Activate" button then the default-config or startup-config file will be activated and to be this switch's running configuration.

5-5.5 Delete

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

Web Interface

To delete configuration in the web interface:

1. Chick Browser to select Maintenance/Configuration in you device.
2. Click Delete Select.

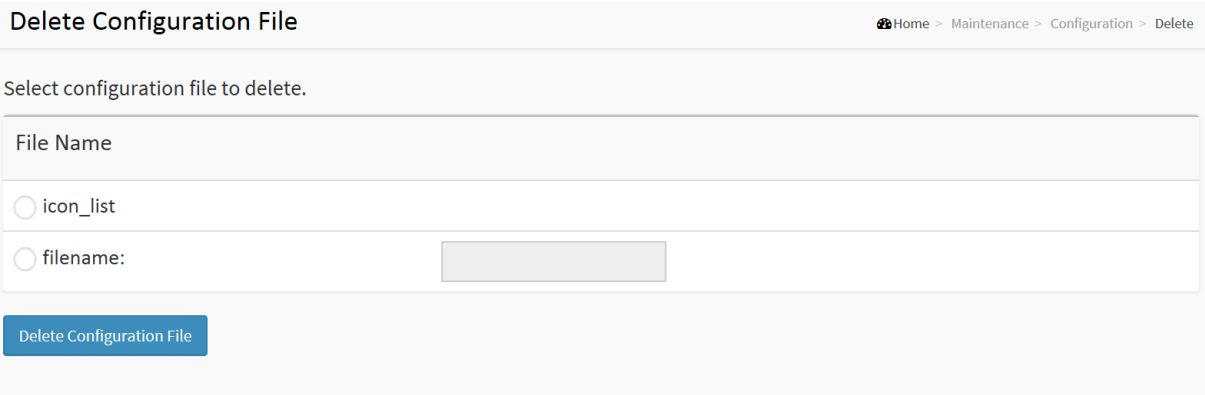


Figure 5-5.5: Delete Configuration

Parameter description:

Buttons

- **Delete Configuration :**

  Click the "Delete" button then the startup-config file will be deleted, this effectively resets the switch to default configuration.

It is possible to download server report file on the switch to the web browser.
Download of server-report may take a little while to complete, as the file must be prepared for download.

Web Interface

To delete configuration in the web interface:

1. Chick Maintenance and Server Report.
2. Click Download Server Report.

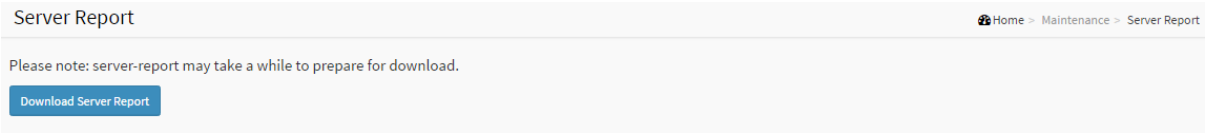


Figure 5-6: Server Report

Parameter description:

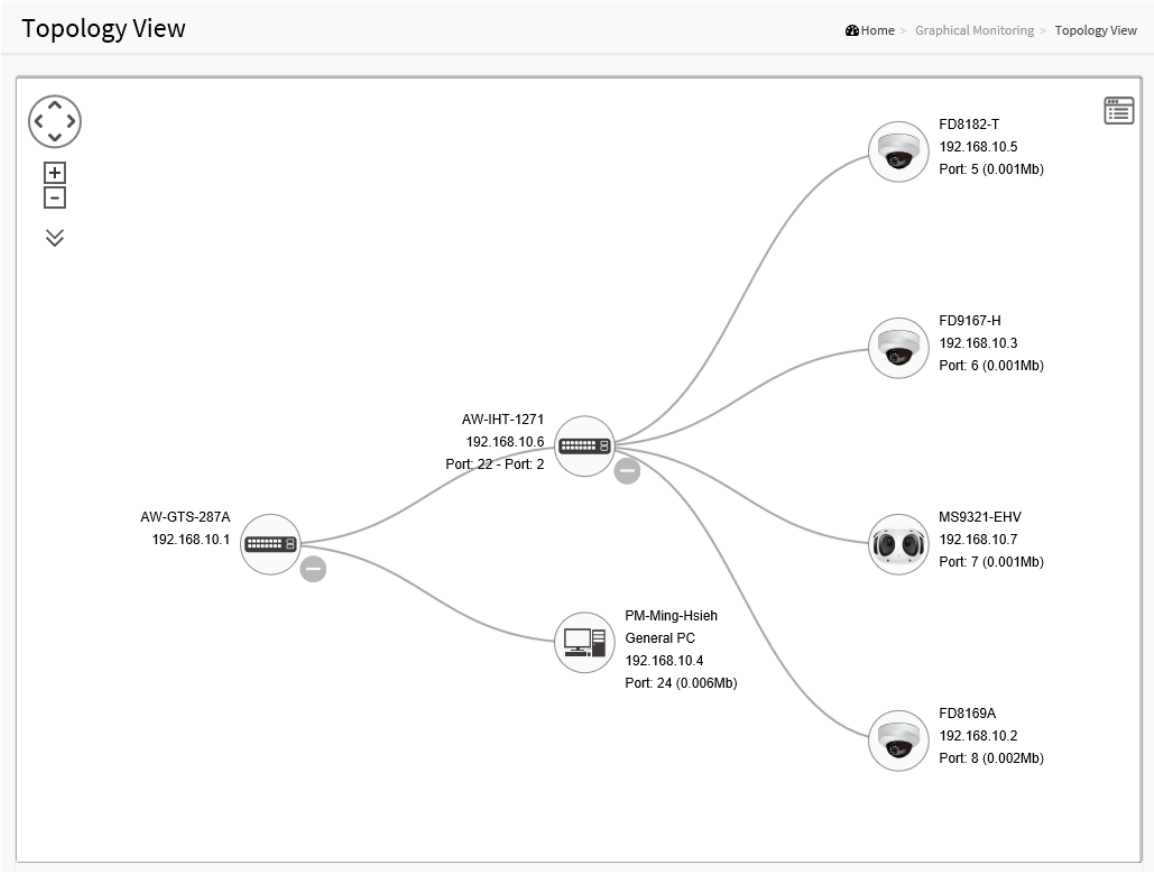
Buttons

- **Download Server Report :**

  Download server report file on the switch to the web browser.

6-1 Surveillance

1. It is recommended to use **IE10** or **IE11** to open a web console with the PoE switch.
2. This PoE switch is specifically designed for surveillance applications. It comes with an integrated Surveillance interface for ease of configuration. The Surveillance interface is accessed through a tabbed menu, and the configuration changes made in its window have a higher priority than those in the Switch configuration menus.



6-1.1 INTRODUCTION (for the Surveillance functions):

1. All devices connected to the switches can be discovered and displayed automatically using standard networking protocols such as LLDP, UPnP, ONVIF, Bonjour, etc.
2. Users can operate the features below via an intuitive web GUI.
   - Power down, remotely, the IP cameras, NVRs, or any PoE devices.
   - Identify where exactly the broken cable is, remotely.
   - Detect abnormal traffic issues on IP cameras/NVR.

- Monitor devices status intuitively, e.g., link up, PoE power, traffic, etc.
- Configure VLAN/QoS intuitively for better solution quality/reliability.

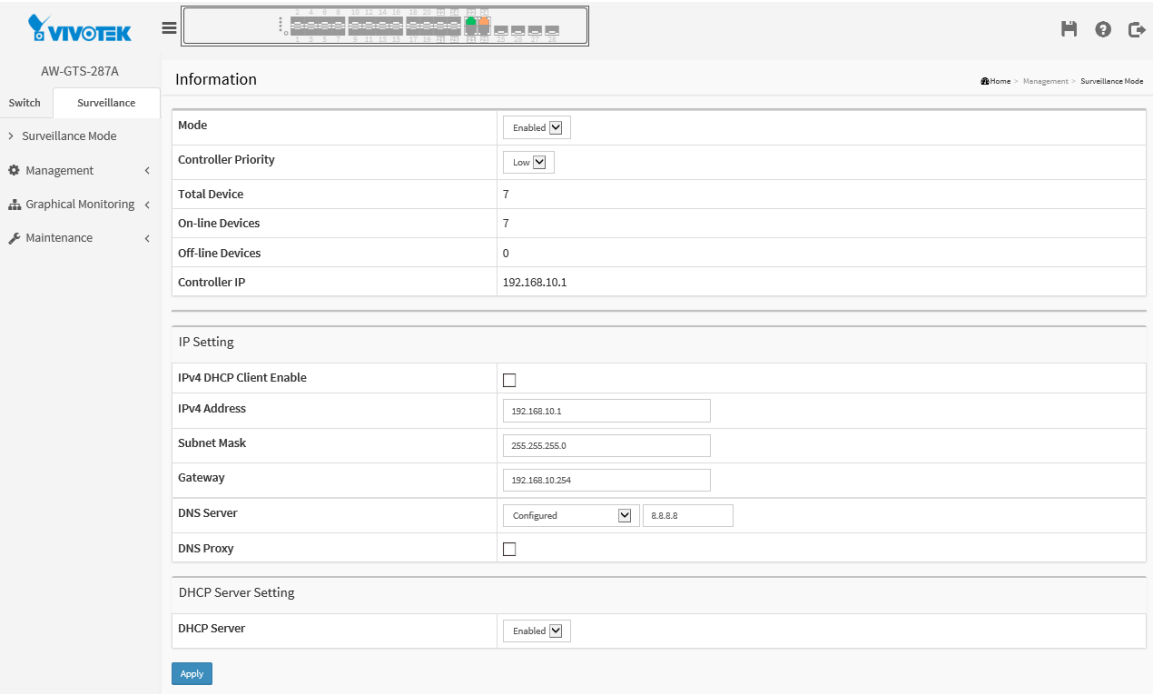
3. The interface supports up to 1000 devices.

The interface is designed to be extremely easy-to-use/manage/install IP Phone, IP Camera, or Wifi-AP for enterprise applications.

User can deploy IP Device through the Topology/ Floor/ Map View to installation location, and through Diagnostics and Traffic Monitor, they may also check link status and monitor throughput as well.

6-2 Management

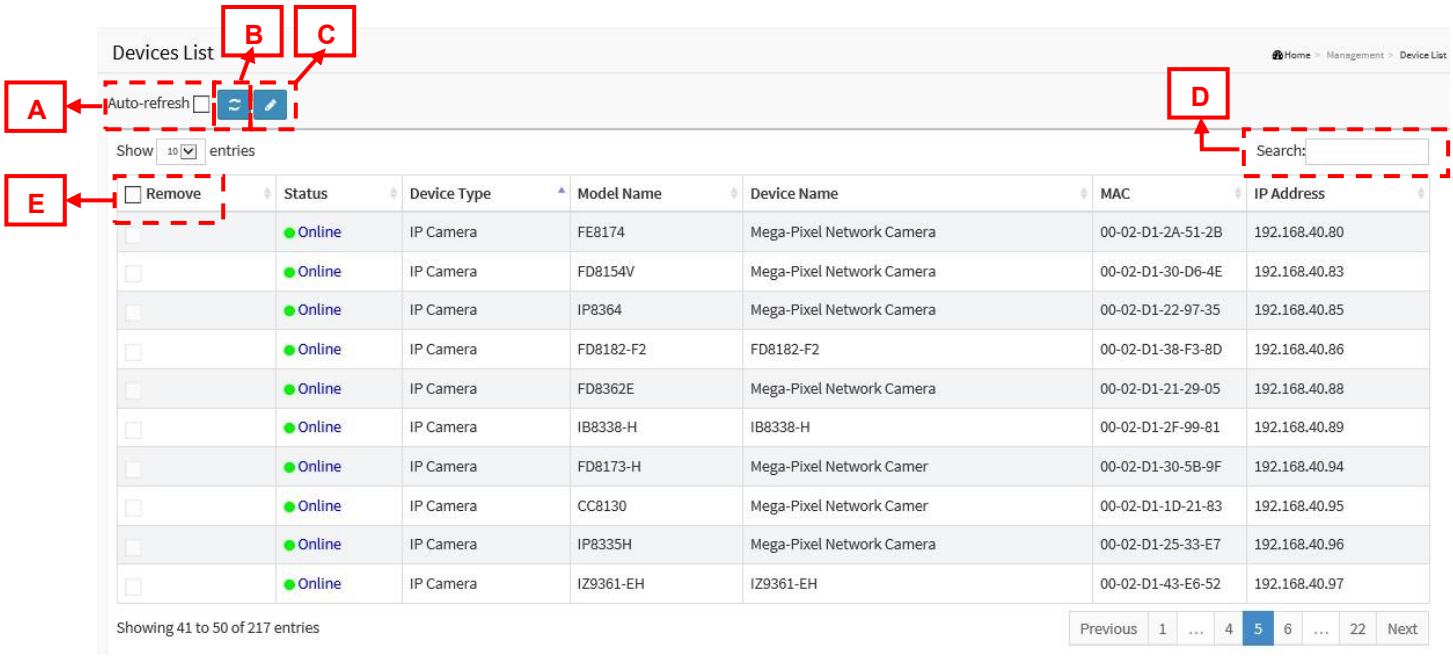
6-2.1 Surveillance Mode



- Surveillance Mode: Enable/ Disable the Surveillance function, or configure the mode with High Priority for Master switch.
- Total Device: Displays how many IP devices are detected and displayed in the topology view.
- On-Line Devices: Displays how many IP devices on-line in the topology view.
- Off-Line Device: Displays how many IP devices are currently off-line in the topology view.
- Controller IP: Displays the Master switch IP (the IP of the PoE switch that you configure surveillance mode as high priority.
- IP Setting: Configure switch network settings.
- DHCP Server Setting: Enable/disable DHCP server.

6-2.2 Device List

It will show all devices and their information which are detected by Surveillance.



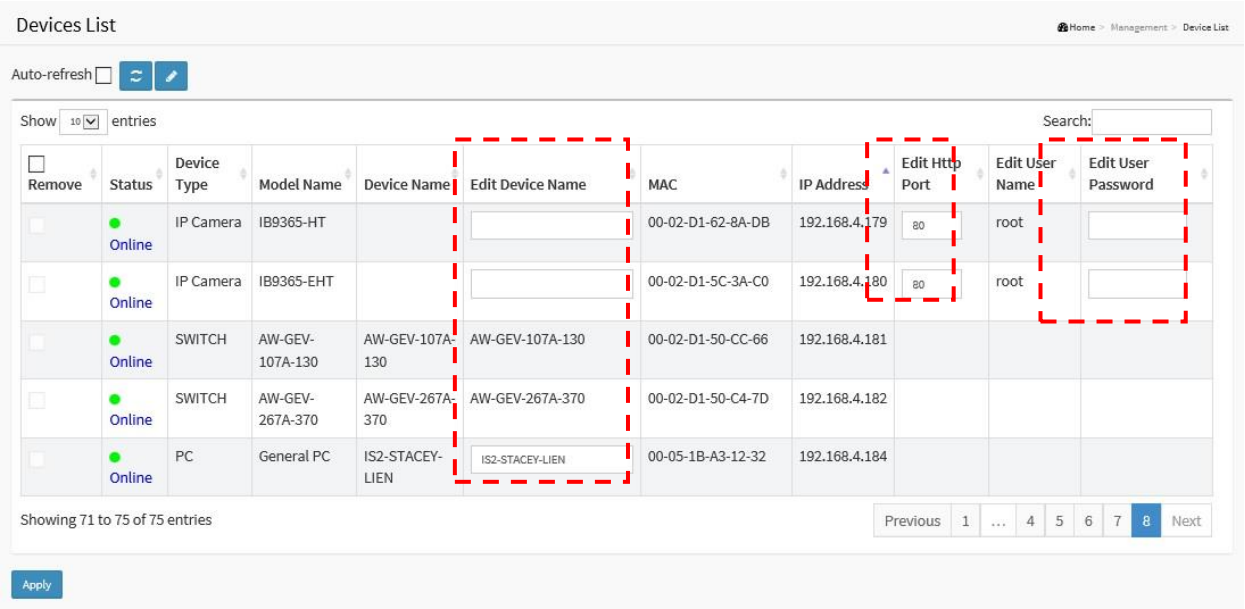
A.

If you want the PoE switch to automatically refresh the information then you need to evoke the "Auto refresh" function.

B.
Click this button to Refresh the status of all devices.

C.
Click this button to Edit Device Name, http Port and camera password.

- User can press the "Edit" button to edit device name and HTTP port for each IP device. This function can also be configured in the Dashboard of Topology view.
- There is no HTTP connection function for Unknown Device and PC type devices, therefore, the UI doesn't provide "Edit HTTP port" function for them.



D. Search: Search devices by keying words with full text search.

E. Remove The Remove function only applies to the Offline devices.

Note:

The device name will not be saved until you click the Apply button. Please do not click on the refresh, auto-refresh or edit buttons before you apply new device name.

6-3 VVTK Camera & Encoder

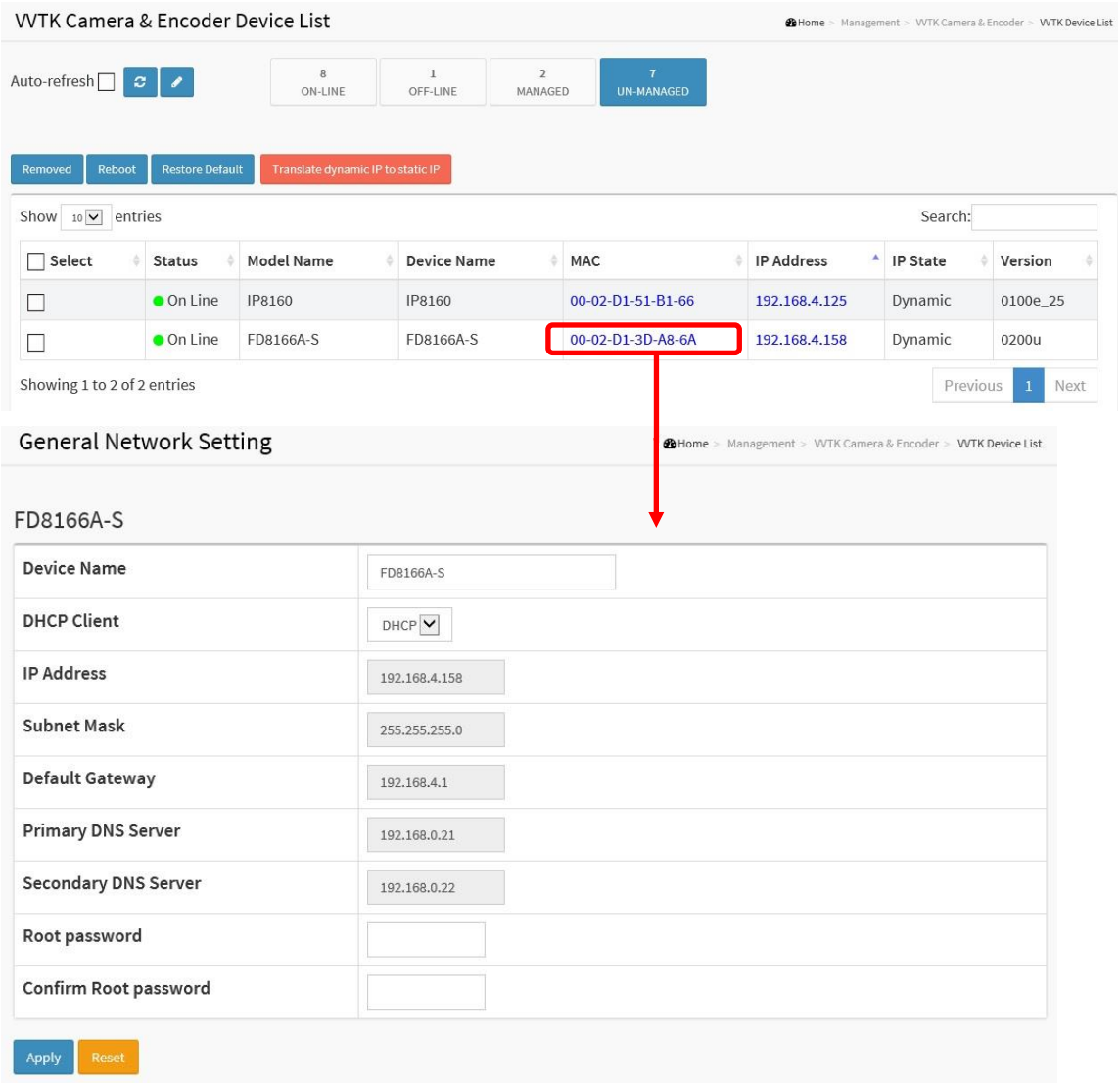
6-3.1 VVTK Device List

This page displays the status of all VIVOTEK IP Cameras and video servers currently connected to your switch as well as all the devices in the network that the switch can access.

Web interface

To configure Surveillance Camera & Encoder in the web interface:

1. Click Surveillance > Management > VVTK Camera & Encoder > VVTK Device List.
2. Click on a device's MAC address to configure the general Network setting.
3. Click on the IP address to opens a web interface of the IP camera (or video server).
4. Click the **Apply** button for the configuration to take effect.



Parameter description:

- **Select:**

  Use the checkbox in the Select column to Remove, Reboot, or restore the Default of a device.

- **Status:**

  Device link state (On/Off Line)

- **Model Name:**

  VIVOTEK Camera & Encoder model name

- **Device Name:**

  VIVOTEK Camera & Encoder device name

- **Edit Device Name:**

  VIVOTEK Camera & Encoder device name edit

- **MAC:**

  Camera & Encoder device MAC address. It is also a hyper-link that opens the device's General Network Setting page.

- **IP Address:**

  Camera & Encoder device IP address. It is also a hyper-link that opens a web Interface.

- **IP State:**

  Dynamic IP or Static IP.

- **Version:**

  VIVOTEK Camera & Encoder device's firmware version

Device Status and Functional Buttons

- **Refresh** :

  Refresh and poll the connection statuses from the connected devices. You may

  also select the Auto-refresh checkbox. The switch will update the connection status by every one second.

- **Edit device name** :

  Click the button. The device Name of IP cameras will become editable. You can then enter a new name in the text box.

- **Remove:**

  Select the checkbox in front of a device, and then click the Remove button to remove a device from the list.

- **Reboot:**

  Select the checkbox in front of a device, and then click the Reboot button to re-start a device. Rebooting a device can sometimes restore an IP camera from a faulty state.

- **Restore Default:**

  Select the checkbox in front of a device, and then click the Restore default button to restore its firmware default.

- **Translate dynamic IP to static IP:**

  By default, VIVOTEK's IP cameras listen to a DHCP server for a dynamic IP. This button sets

their dynamic IPs (that are currently in use) into static IPs. Using a static IP can avoid the change of IPs when devices need to be re-started.

NOTE: The Search function on the Device list page supports search entry by Model Name, MAC address, or IP addresses.

6-3.2 Camera Configure

Config Export

Web interface

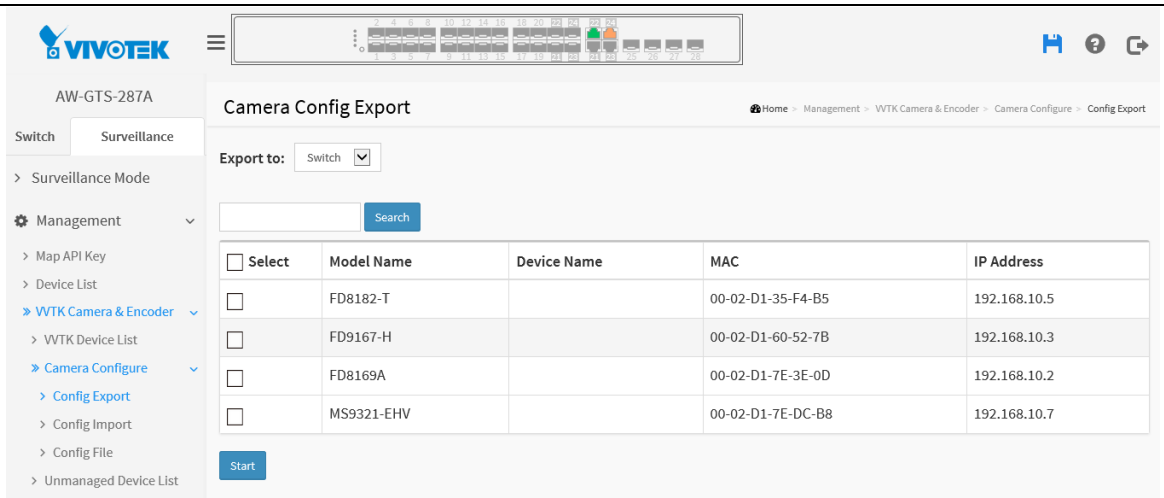
To configure Surveillance Information in the web interface:

1. Click Surveillance > Management > VVTK Camera & Encoder > Camera Configure > Config Export
2. Select the Device to export the configuration file from. You can export IP cameras' configuration profile (128KB in size) to the client computer or to the switch itself. Note that if you choose to export to the switch, you can store up to 39 copies of camera configuration profile.

   The Search box supports filtering find of devices using Model Name, MAC address, or IP addresses.

   IMPORTANT: If you need to export the configuration to a client computer, a TFTP server is required in your network. The configuration profile is transported via a TFTP server.

3. Click Start.



Config Import

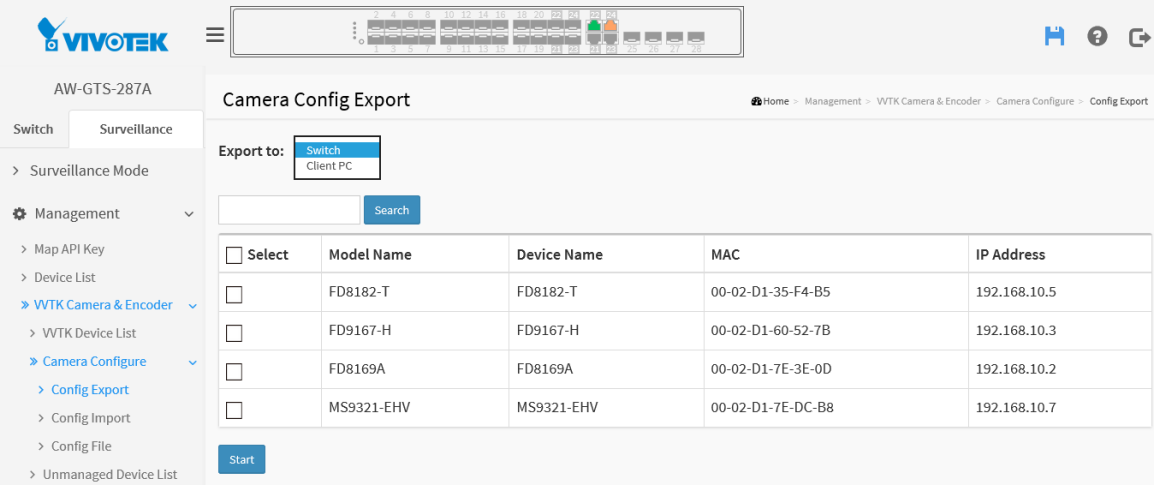
Web interface

To configure Camera config. in the web interface:

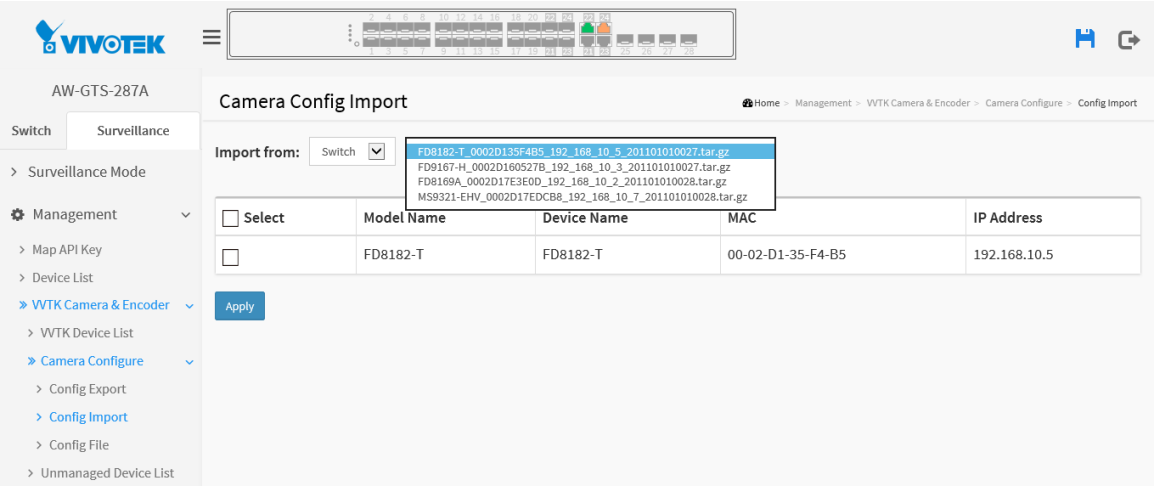
1. Click Surveillance > Management > VVTK Camera & Encoder > Camera Configure >

Config Import.

2. Select the Device to import the configuration file from client PC.
3. Select the IP camera to load the configuration file to, using a single-click on its checkbox.
4. Click the Apply button.



6-3.2 Config import from client PC



6-3.2 Config import from switch

Config Files

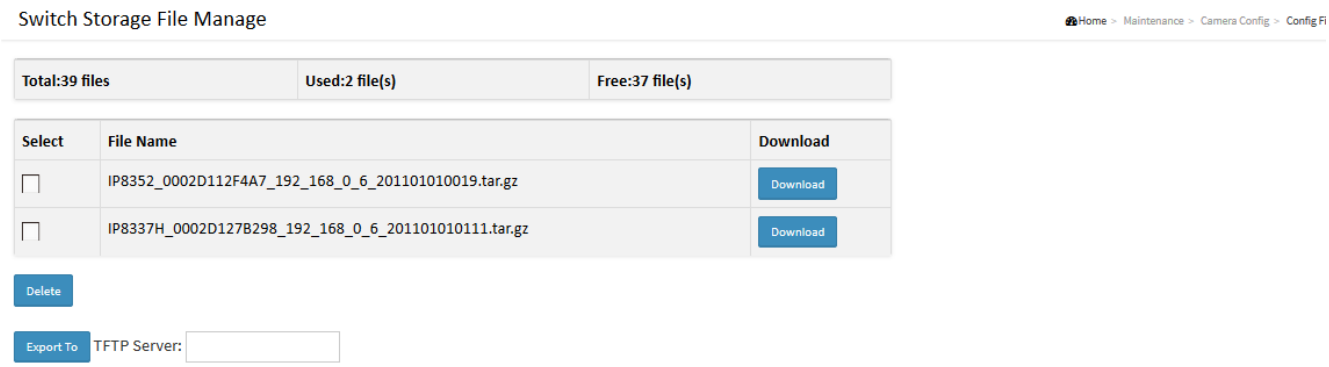
Web interface

To display configuration files currently stored on the switch:

1. Click Surveillance > Management > VVTK Camera & Encoder > Camera Configure > Config File.
2. You can select configuration files and delete these files by selecting their checkboxes, and click the Delete button. Or you may download the configuration file to the client PC using the Download button.
3. You can also export the files to a TFTP server by entering the TFTP address, checking the files to be uploaded, and click the Export To button.

   IMPORTANT: If you need to export the configuration to a client computer, a TFTP server is

required in your network. The configuration file is transported via a TFTP server.



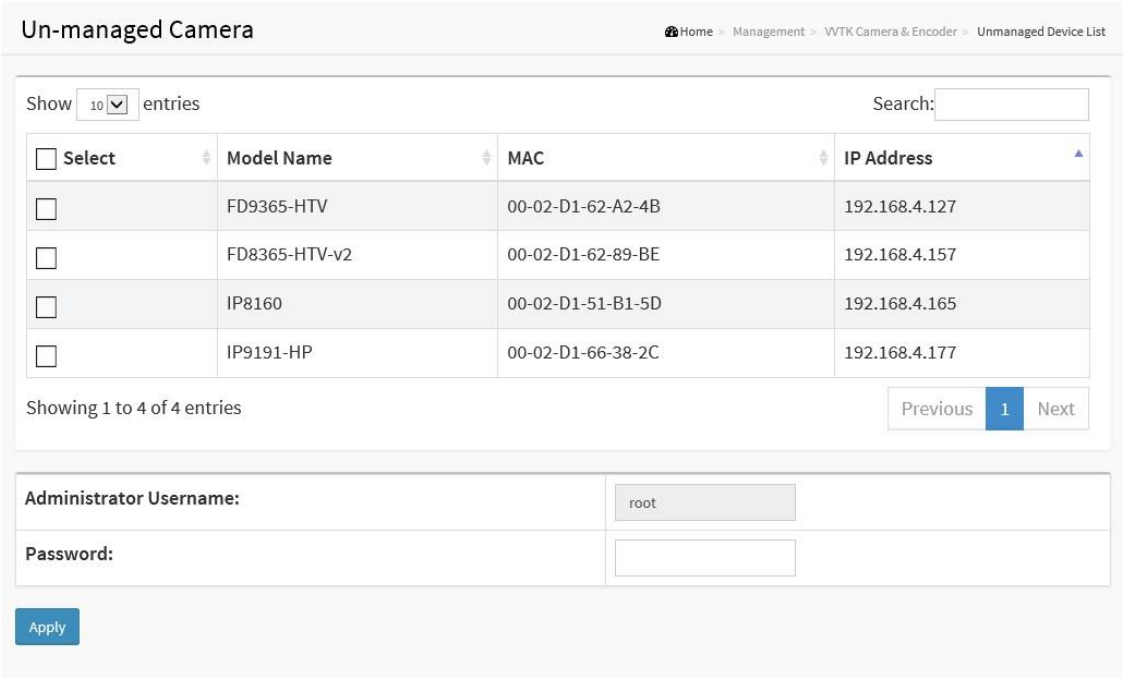
6-4 Unmanaged Device List

An Un-managed VIVOTEK camera is the ones that come with unknown Root password. From this page you can force to change the Root password for batch VIVOTEK cameras. When a new Root password is applied, the unmanaged VIVOTEK cameras will be manageable.

Web interface

To configure Surveillance Un-managed Devices VVTK Camera in the web interface:

1. Click Surveillance > Management > VVTK Camera & Encoder > Unmanaged Device List
2. Enter a Password (blank also applies).
3. Click the Apply button



Parameter description:

- **Administrator Username:**

  Root (system administrator default and cannot be changed).

- **Administrator Password:**

The Root password that will be applied to the selected device(s).

Chapter 7 Surveillance – Graphical Monitoring

7-1 Topology View

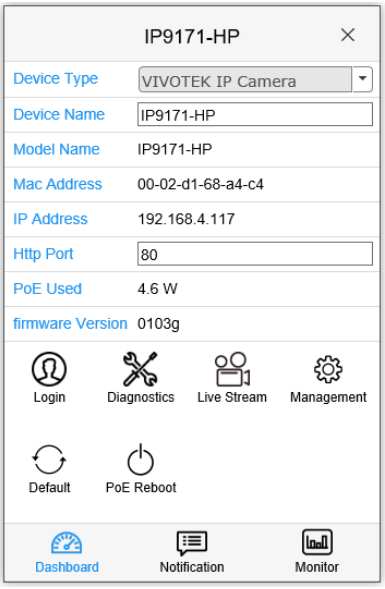
Web interface

To configure Surveillance Topology View in the web interface:

1. Click Surveillance > Graphical Monitoring > Topology View.

2. To reveal details of a device, mouse over a device to display its device name, model name, MAC, IP, and status.

3. You can click on a device to display the quick access menu.



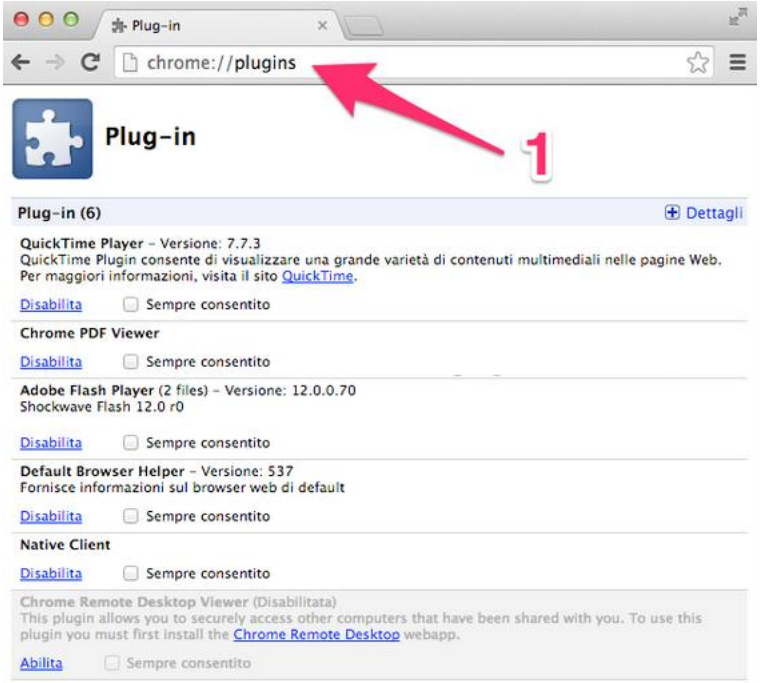
1	Login	Opens the web console with the camera.
2	Diagnostics	Diagnoses the network connectivity with the device.
3	Live Stream	Displays a live stream (stream 1) window. For multi-sensor models, only channel 1 video stream will be displayed.
4	Management	Directs to the camera general network setting page.
5	Default	Restores back to factory default settings.
6	PoE Reboot	Reboots the camera.
7	Notification	Displays event messages from the camera/device.
8	Monitor	Displays the throughput threshold configuration page.

The quick access menu is also available on the Floor View and Google Map.

The Live Stream feature applies in the following browser versions:

	Chrome V39 above	Chrome V38 under	Firefox v39	IE11	IE10	IE9	IE8
WinXP	No	Yes	Yes	--	--	--	No
Win7	No	Yes	Yes	Yes	Yes	No	No
Win8/8.1	No	Yes	Yes	Yes	YEs	No	No

You will also need to enable the QuickTime plug-ins for your browser. For example, try using the chrome://plugins command in your URL address field on Chrome.



4. For example, you can use the Diagnostics function to figure out whether there is a link problem to a device. The switch sends test packets to verify the link connectivity between switch port and camera. This helps when diagnosing cabling problems in your deployments.

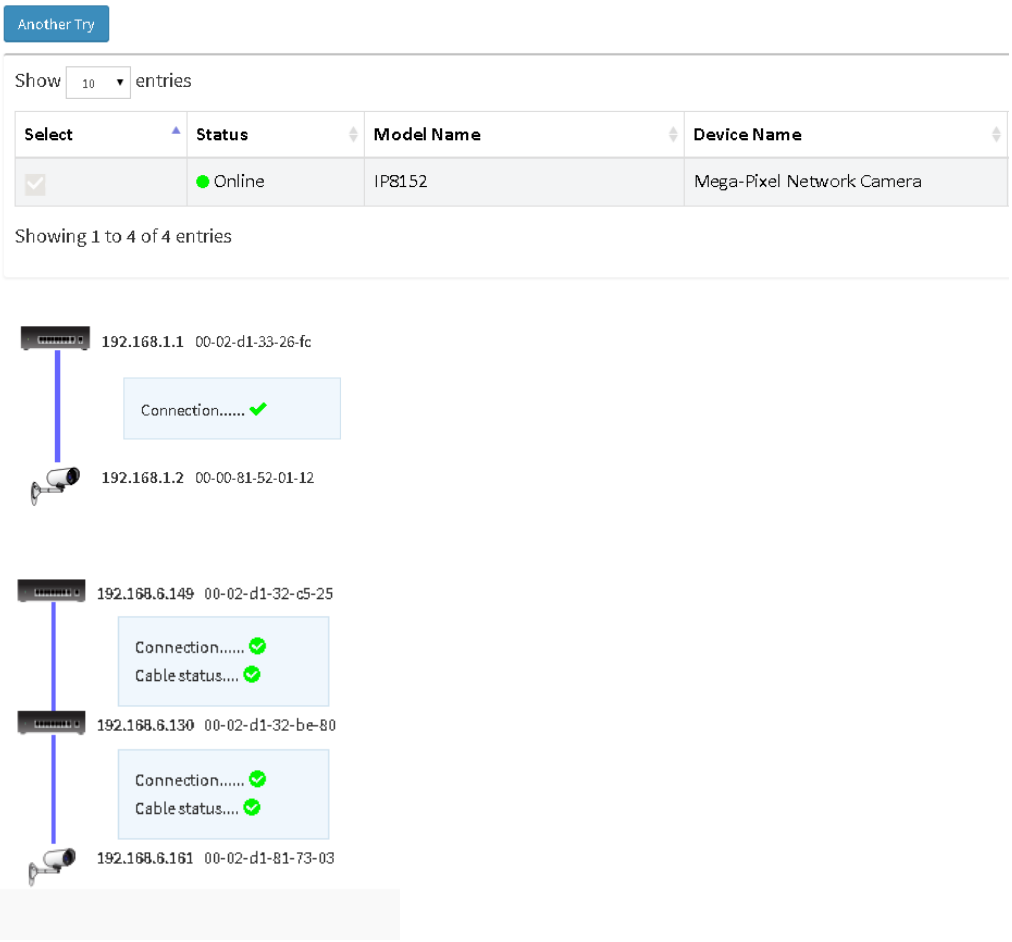
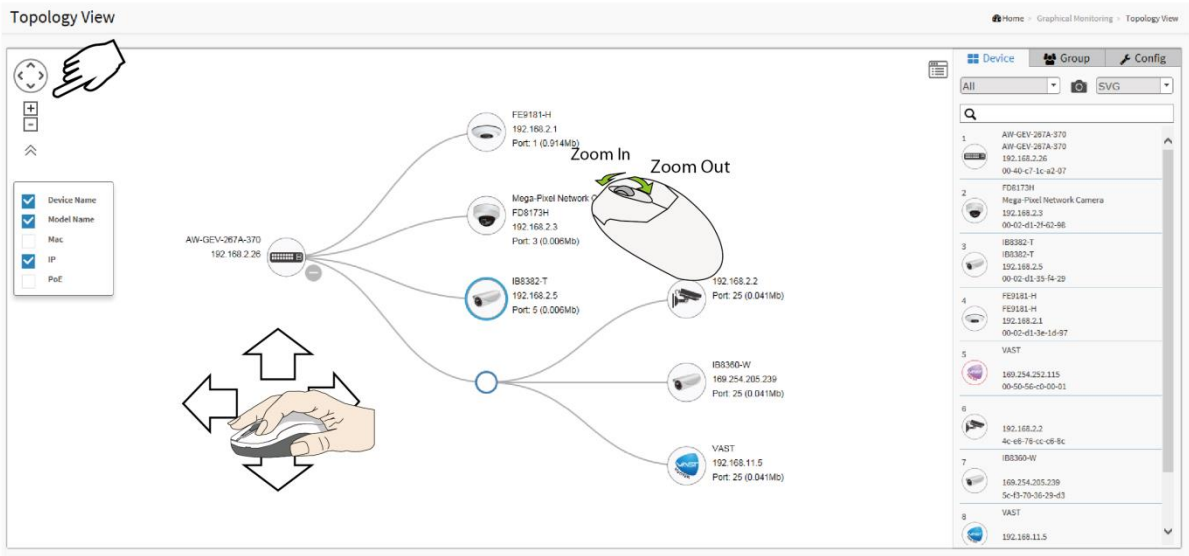


Figure 7-1.1: Topology View

See below for the sample screen and mouse control:

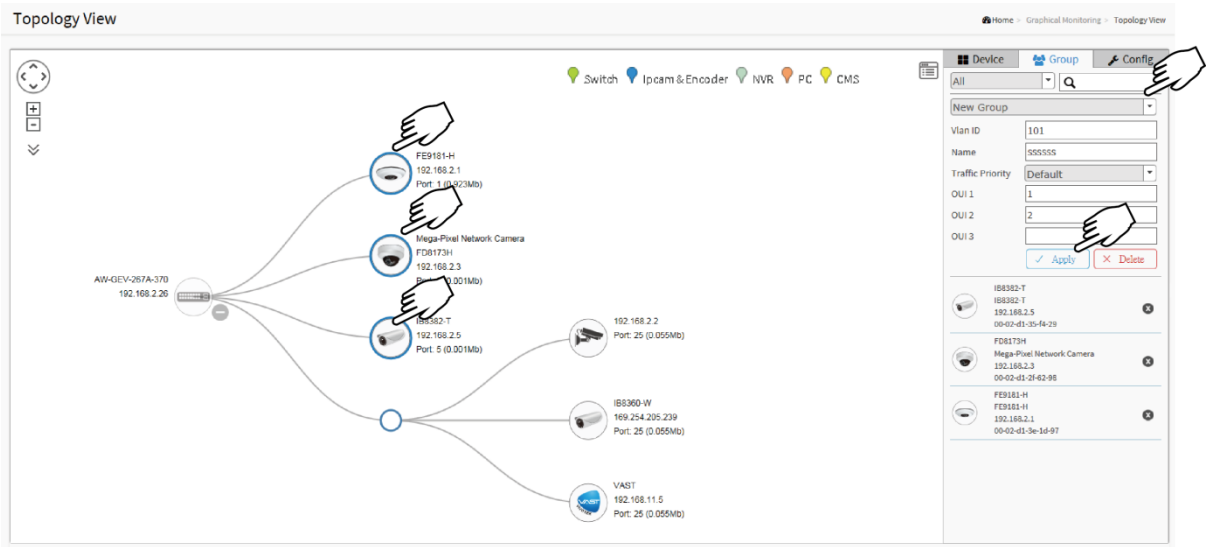


You can also configure VLAN grouping in the Topology View. To configure grouping, proceed with the following:

1. Enable the Grouping mode by selecting the "Group" menu from the Device List menu. Select New Group from the pull-down menu. Single-click IP cameras or servers to include them into group. When configuring an existing group, select an existing group.
2. Select the members you prefer from the topology.
3. Enter a Group name, Description, and a unique VLAN ID. See the previous chapter for details. 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.

   Organizationally Unique Identifiers (OUI) are the first three bytes of a MAC Address, while the last three bytes contain a unique station ID. You can add a specific manufacturer with the OUI. Enter the first 3 octets as the hexadecimal 000000 to specify the device range.
4. When done, click the Apply button for the configuration to take effect. Click the Save button to save your configuration.

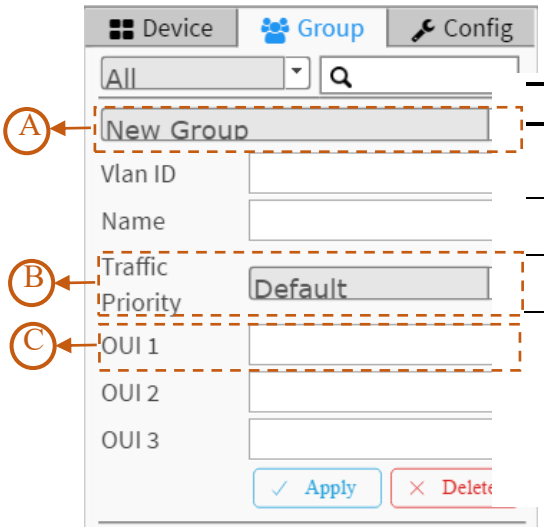
Figure 7-1.2: Configuring Grouping in the Topology View



A VLAN can also span across multiple switches. Select devices on multiple switches to join them into the same VLAN. They will be automatically tagged into a VLAN.

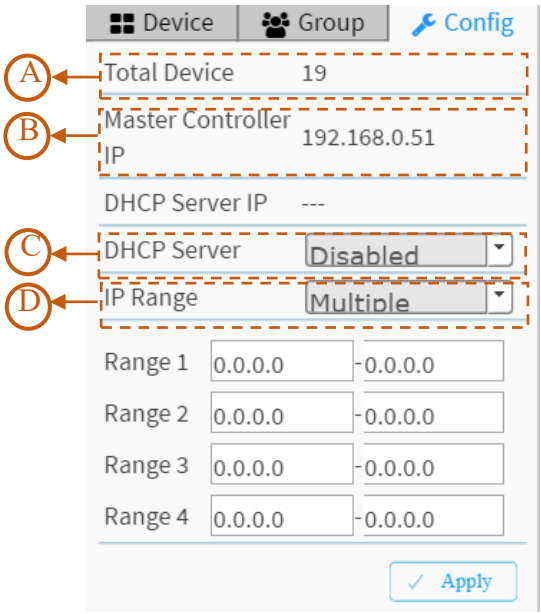
Group Setting Console

- Users can configure VLAN groups for each IP device using the OUI or selecting device icons, and configure traffic priority (0~7) for each VLAN group.
- The configuration uses Mac Based VLAN to isolate groups.
- One IP device only can join one VLAN group.



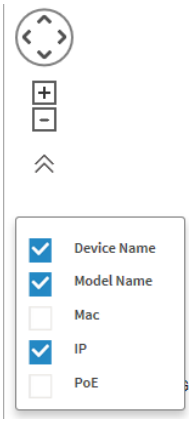
	Function
A.	Group devices by filtering, searching, clicking device icons, or specifying OUI.
B.	Configure traffic priority for the VLAN.
C.	Assign a VLAN ID or Name to the Group.

System Setting Console



	Function
A.	The number of IP devices is displayed here in the topology view.
B.	Displays the IP of the Master PoE switch.
C.	You can enable/disable DHCP server.
D.	- Single Subnet: The Surveillance feature will base on the master switch's IP address. Here the subnet mask is "255.255.255.0". - Multiple Subnet: To provide 4 ranges for manual configuration. In the case, it is recommended to to change the switch's subnet mask to "255.255.0.0." This also avoids IP devices from not being recognized.)

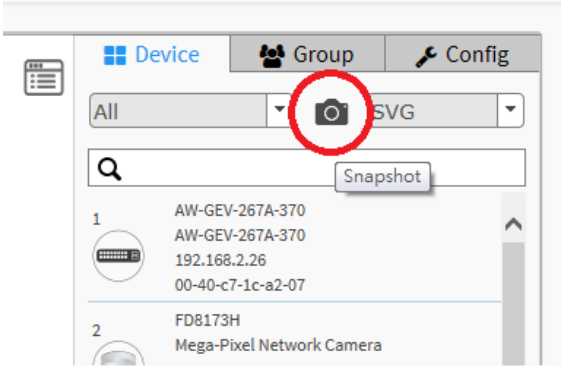
You can use the device menu to select or deselect the types of device information on screen, e.g., MAC address, or Device Name. Note that only 4 types of information can be displayed at one time.



Device picture

- Icon in black: The device is connected. User can select function and check issues.
- Icon in red: Device is not connected. User can diagnose the link status.
- Icons with numbers: It means some events have happened (e.g. Device Off-line, IP Duplicate...etc.) on the IP device, users can click on the device icon to check events in Notification.
- Icon with a question mark: It means the IP device is detected by the Surveillance feature, but the device type can't be recognized. The device is classified as an unknown device type.

An unmanaged device is displayed with a no entry mark. The information for such device will be limited.



You can preserve your configuration by taking a snapshot of your current topology. Note that if using IE browser, you can only export in the SVG format.

- Different device type supports different function:
  - If an IP device is recognized as a Surveillance switch, it will support "Upgrade", "PoE Config," and the "Find Switch" functions.
  - If an IP device is recognized as a PoE device, it will support "PoE Reboot" function in addition to the "Upgrade" and "Find Switch" functions.
- Device Type: This entry appears automatically. If an unknown type is detected, user can still select a device type from a pre-defined list.
- Device Name: Create your own Device Name or alias for easy management such as, 1F_Lobby_Cam1.
- Model Name, MAC Address, IPv4 Address, Subnet Mask, Gateway, PoE Supply and PoE Used are displayed automatically by the Surveillance functions.
- Http Port: A re-assign http port number to the device for better security.
- DHCP Client: Enable or Disable the DHCP client. If this feature is enabled, the system will configure the IPv4 address and network mask of the interface using the DHCP protocol. The DHCP client will announce the configured System Name as hostname to provide DNS lookup.
-

Login: Click the Login Action Icon to log in the device via http for further configuration or status monitoring.
-

Upgrade: Click to upgrade the software version.
-

Find Switch: When this feature is activated, the switch LEDs will all light up and flicker for 15 seconds.
-

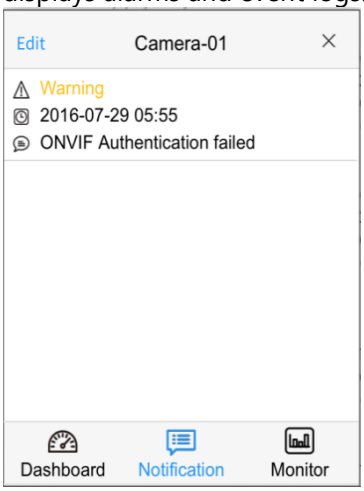
PoE Config: Click it to configure the PoE function, enable/disable PoE Auto Checking or enable/disable PoE mode on a per port basis.
-

PoE Reboot: When necessary, click to reboot the device remotely so as to restore a device back to its normal operation.
-

Streaming: Click to display the video images streaming, if the device supports this feature.
-

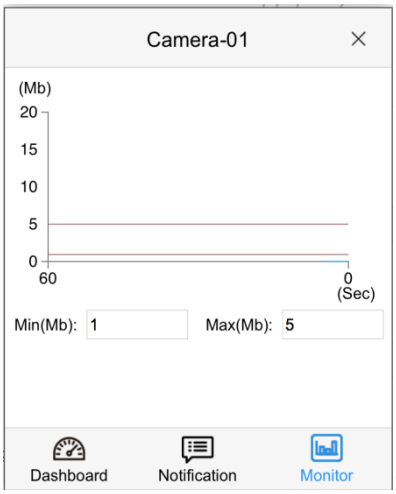
Icon with blank node: When a PoE switch detects more than two IP devices from the same port, the switch can't resolve this IP device's layout, instead, it will display a blank node to present this situation. Users can use the "Parent Node" function to adjust layout on the Dashboard.

Notification Console: This window displays alarms and event logs.

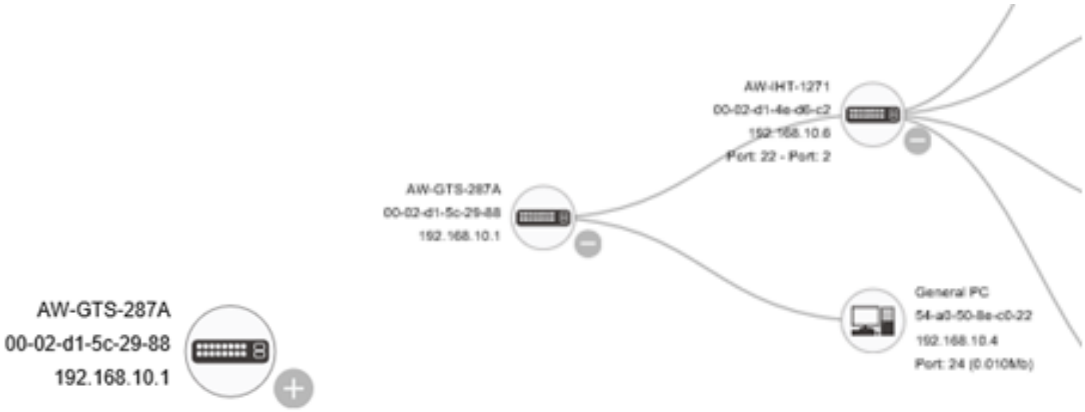


Monitor Console: This window displays the traffics for device health check purpose.

- Except PoE switch, users can configure throughput thresholds for each IP device. Users will receive event notifications when throughput is lower or higher than your configuration.
- If both values are "0", it means the function is disabled.
- The polling interval is 1 second. When the page is closed, the Polling interval will change to 5 seconds.



If you click on switch "**+**" or "**-**", it will retract the subtree infrastructure.



7-2 Floor View

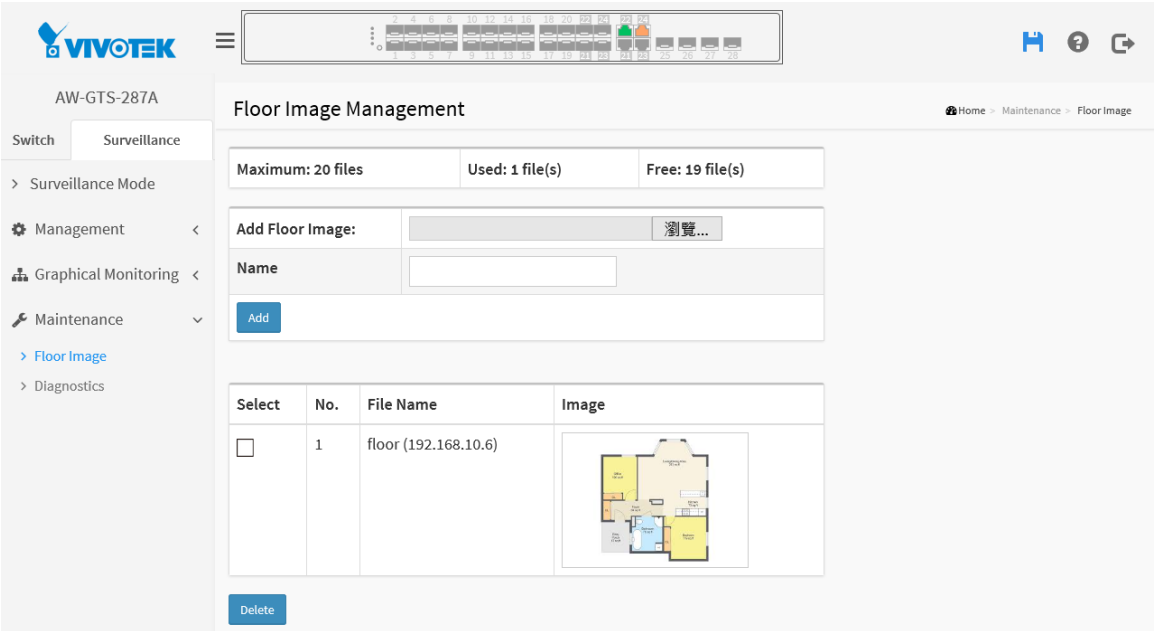
In this page, the administrator can place a device per time onto the custom image, which you have already uploaded, by dragging-and-dropping markers in the device list.

You can upload up to 10 map files in JPG and PNG formats, with the limitation of 512KB in file size each.

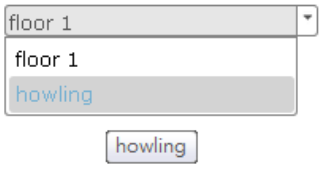
Web interface

To configure the surveillance Floor View in the web interface:

1. Click Surveillance > Graphical Monitoring > Floor View.
2. Select a floor map you uploaded. You can prepare and upload one or multiple floor maps in the Surveillance > Maintenance > Floor Image window.

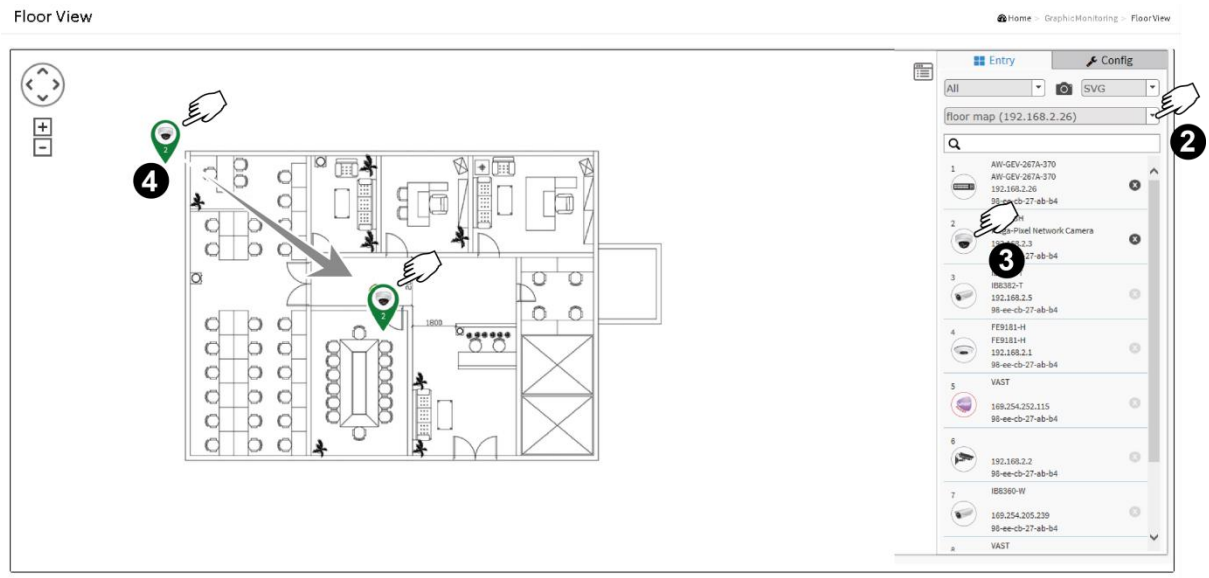


3. You then select a device on the Device List by a single click. A similar bubble icon will appear on screen. Click and drag the icon to a preferred location on the map.
4. Repeat the above process until you finish the map setup, and click the **Apply** button.
5. With multiple maps in your deployment, e.g., different floor or building, select a different floor view from the pull-down menu on top and continue with the configuration.

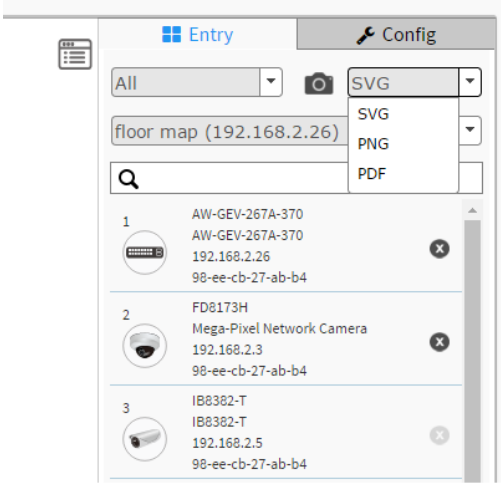


6. Click the Save button to save your configuration.

Figure 7-2.1: Floor View



When the configuration is done, use the **Snapshot** function on the upper right of the screen to export your configuration. The file format can be SVG, PNG, or PDF (Chrome and Firefox).



Note that if using IE browser, you can only export files in the SVG format.

7-3 Map View

On this page, you can view a realistic representation of devices through the Google map. This Map View applies in wide area, outdoor deployments. The preconditions for using this function are:

1. The client computer having a web session with the PoE switch must have an **Internet** connection.

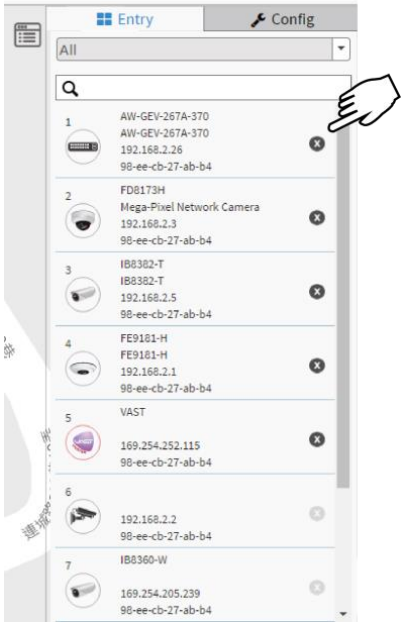
Web interface

To configure Surveillance Map View in the web interface:

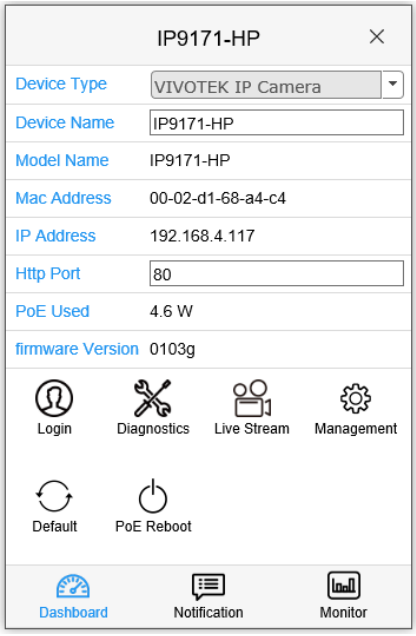
1. Click Surveillance > Graphical Monitoring > Map View.
2. On the Google map, move to your location, and zoom in to a preferred view. To move on the screen, click and hold down your left mouse button to move to a preferred direction. You can also key in the address you have in mind in the Search box, e.g., Sunset Boulevard, Los Angeles, etc. The GPS location of your current position is also supported.
3. Click to select a device. The device will appear on the map.
4. Click and drag the device to a preferred location.
5. Repeat the above process to complete the map setup, and click Apply to finish the configuration.

Figure 7-3.1: Map View

To return to a location you previously visited, simply click on a camera or device (on the Device List) you implanted on the map. The current map view will move back to the location you previously configured. An implanted camera will be indicated by a bubble icon with a dim out color.

To remove a camera from a Google map, click on the camera's cross mark from the Device List, and the camera will disappear from map.	

The quick access menu is also available on the Google Map.



1	Login	Opens the web console with the camera.
2	Diagnostics	Diagnoses the network connectivity with the device.
3	Live Stream	Displays a live stream (stream 1) window. For multi-sensor models, only channel 1 video stream will be displayed.
4	Management	Directs to the camera general network setting page.
5	Default	Restores back to factory default settings.
6	PoE Reboot	Reboots the camera.
7	Notification	Displays event messages from the camera/device.
8	Monitor	Displays the throughput threshold configuration page.

8-1 Floor Image

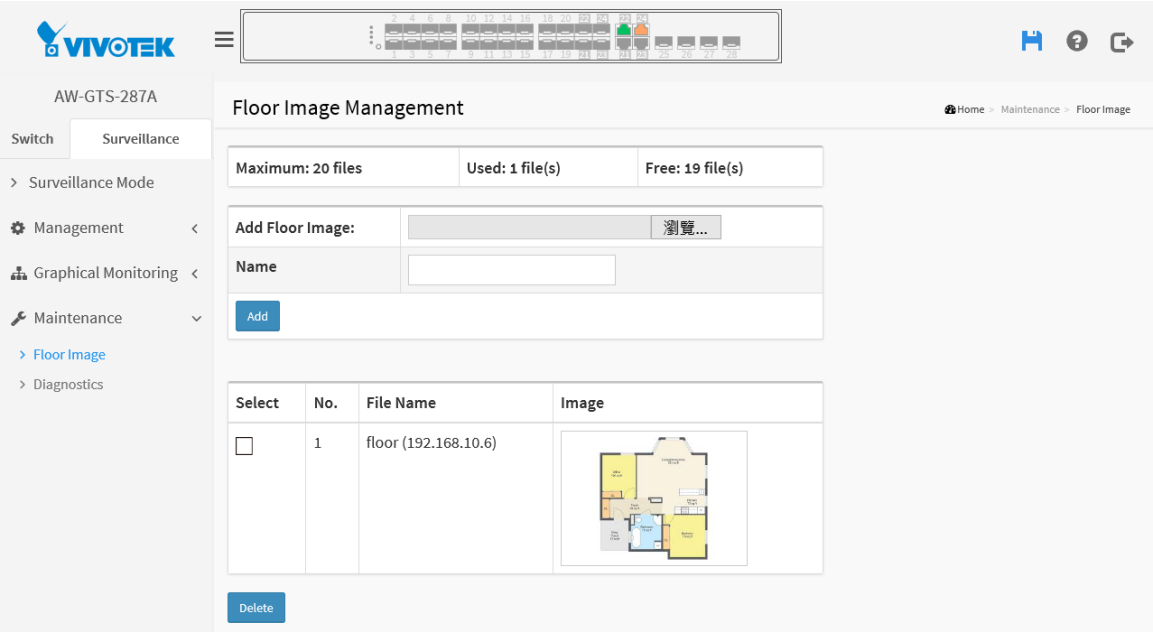
In this page, you can upload or manage floor map images. Due to the limitation of the flash memory, up to 20 JPEG images, each of a max. of 256KB size, can be uploaded to the switch.

Web interface

To configure the Floor Image in the web interface:

1. Click Surveillance > Floor Plan > Floor Image.
2. Click "Browse..." to select Floor image from the client computer. Enter a name for the Name entry.
3. Click Add to upload. When done, a snapshot will be available on screen.
4. If you need to remove an existing floor map, select its checkbox and click Delete to remove.

Figure 8-1.1: Floor Image



8-2 Diagnostics

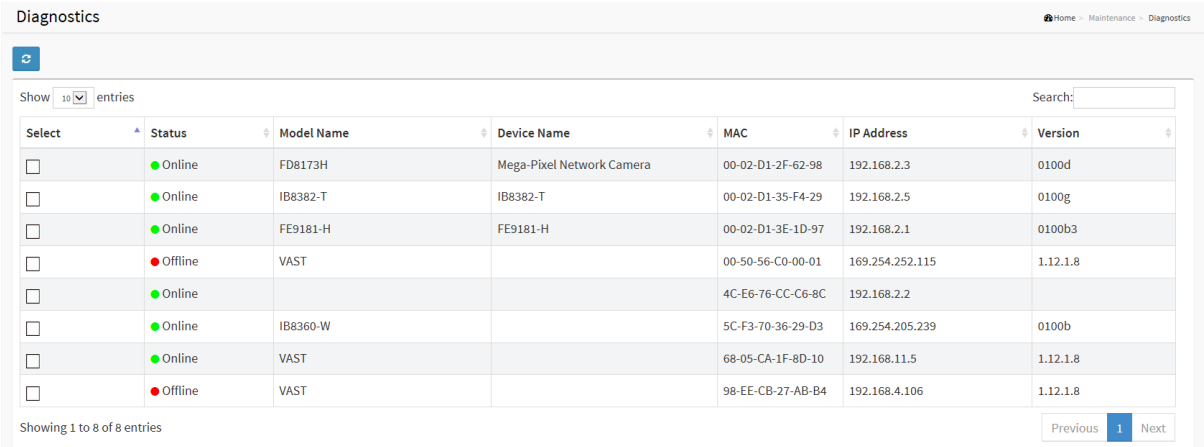
In this page, you can troubleshoot the connection between PoE switch and IP Devices. This feature is designed primarily for administrators to verify and test the link routes between the switch and the IP device. Note that the topology of network needs to be saved for this function to work properly.

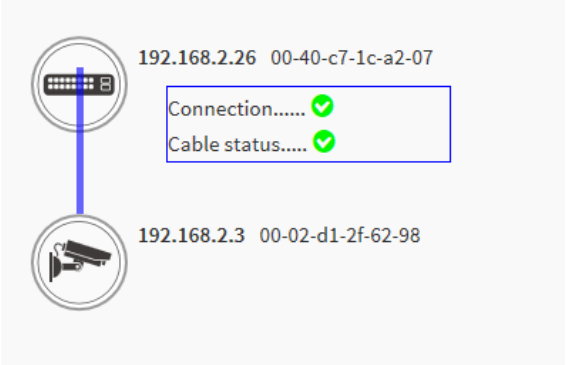
Web interface

To configure Surveillance Information in the web interface:

1. Click Surveillance > Maintenance > and Diagnostics.
2. Select a device's checkbox to start the connectivity test.
3. Click Another Try to go back to the Device Status screen.

Figure 8-2.1: Device Status



Select	Status	Model Name	Device Name	MAC	IP Address	Version
☐	Online	FD8173H	Mega-Pixel Network Camera	00-02-D1-2F-62-98	192.168.2.3	0100d
☐	Online	IB8382-T	IB8382-T	00-02-D1-35-F4-29	192.168.2.5	0100g
☐	Online	FE9181-H	FE9181-H	00-02-D1-3E-1D-97	192.168.2.1	0100b3
☐	Offline	VAST		00-50-56-C0-00-01	169.254.252.115	1.12.1.8
☐	Online			4C-E6-76-CC-C6-8C	192.168.2.2	
☐	Online	IB8360-W		5C-F3-70-36-29-D3	169.254.205.239	0100b
☐	Online	VAST		68-05-CA-1F-8D-10	192.168.11.5	1.12.1.8
☐	Offline	VAST		98-EE-CB-27-AB-B4	192.168.4.106	1.12.1.8

The diagnostics result will immediately displays at the lower screen.