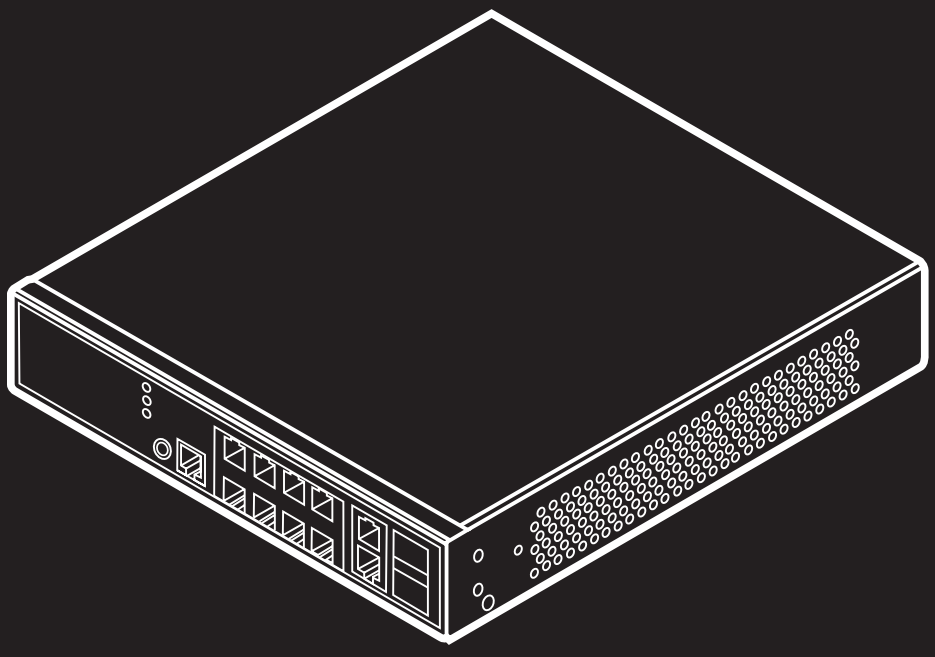
USER MANUAL

LGB1110A, LGB1126A-R2

# GIGABIT MANAGED ENET SWITCH

24/7 TECHNICAL SUPPORT AT 1.877.877.2269 OR VISIT BLACKBOX.COM



BLACK BOX®

# TABLE OF CONTENTS

# TABLE OF CONTENTS

# TABLE OF CONTENTS

# TABLE OF CONTENTS

# TABLE OF CONTENTS

## REVISION HISTORY

RELEASE: V6.38

# CHAPTER 1: INTRODUCTION

## 1.1 OVERVIEW

This user's manual explains how to install and connect your network system and configure and monitor the Gigabit Managed Ethernet Switch through the web via an RJ-45 serial interface and Ethernet ports.

The Gigabit Managed Ethernet Switch provides a reliable infrastructure for your business network. These switches deliver the intelligent features you need to improve the availability of your critical business applications, protect your sensitive information, and optimize your network bandwidth. The switches are ideal for entry-level networking, including small business and enterprise applications.

## 1.2 AVAILABLE MODELS

Three Gigabit Managed Ethernet Switch models are available:

- Gigabit Managed Ethernet Switch - 10-Ports (LGB1110A)
- Gigabit Managed Ethernet Switch - 26-Ports (LGB1126A-R2)

## 1.3 FEATURES

All Gigabit Managed Ethernet Switch provide these functions:

- L2+ features provide better manageability, security, QoS, and performance.
- IPv4/IPv6 dual stack management
- SSH/SSL secured management
- SNMP v1/v2c/v3
- RMON groups 1,2,3,9
- sFlow
- IGMP v1/v2/v3 Snooping
- MLD v1/v2 Snooping
- RADIUS and TACACS+ authentication
- IP Source Guard
- DHCP Relay (Option 82)
- DHCP Snooping
- ACL and QCL for traffic filtering
- 802.1d (STP), 802.1w (RSTP) and 802.1s (MSTP)
- LACP and static link aggregation
- Q-in-Q double tag VLAN
- GVRP dynamic VLAN

# CHAPTER 2: OPERATION OF WEB-BASED MANAGEMENT

## 2.1 INITIAL CONFIGURATION

This chapter instructs you how to configure and manage the Gigabit Managed Ethernet Switch through the web user interface. It enables you to easily access and monitor, through any one port of the switch, MIBs status, each port activity, Spanning tree status, port aggregation status, multicast traffic, VLAN and priority status, illegal access records, and so on.

THE DEFAULT VALUES OF THE GIGABIT MANAGED ETHERNET SWITCH ARE LISTED BELOW:

- IP Address: 192.168.1.1
- Subnet Mask: 255.255.255.0
- Default Gateway: 192.168.1.254
- Username: admin
- Password: <blank>

After the Gigabit Managed Ethernet Switch finishes configuring the IT interface, you can browse it. For instance, type http://192.168.1.1 in the address row in a browser, and it will show the following screen and ask you to input the username and password to login and access authentication.

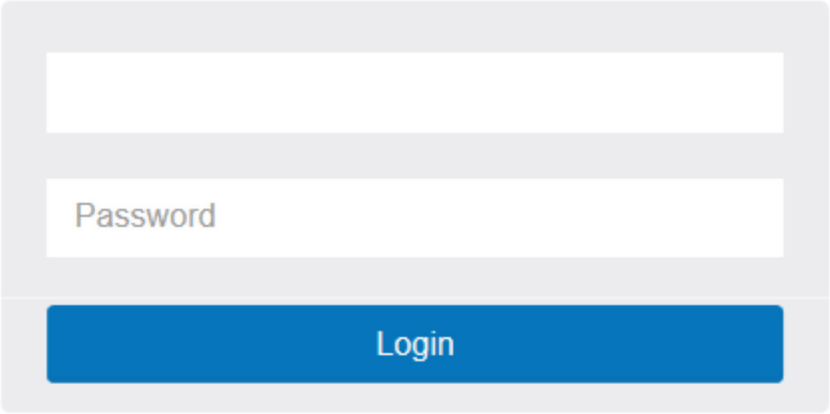



FIGURE 2-1. LOGIN SCREEN

The default username is “admin” and password is <blank>. For first-time use, enter the default username and password, and then click the <Login> button. The login process now is completed. In this login menu, input the complete username and password respectively, the Gigabit Managed Ethernet Switch will not give you a shortcut to username automatically. This looks inconvenient, but safer.

In the Gigabit Managed Ethernet Switch, two or more users can use the administrator’s identity to manage this switch.

**NOTE**: When you log in to the Switch Web/CLI, you must first type the username (admin). Password is blank, so after you type admin, just press enter in the management page to enter the Web/CLI.

When you log in to the Gigabit Managed Ethernet Switch series switch Web UI management, you can use both ipv4 and ipv6 login.

To optimize the display, we recommend that you use Microsoft IE 6.0 or above, Netscape V7.1 or above or Firefox V1.00 above with resolution of 1024 x 768 or above.

# CHAPTER 2: OPERATION OF WEB-BASED MANAGEMENT

**NOTE**: The Gigabit Managed Ethernet Switch enables DHCP, so If you do not have a DHCP server to provide ip addresses to the switch, use the Switch default ip 192.168.1.1

# CHAPTER 3: SYSTEM CONFIGURATION

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

## 3.1 SYSTEM

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

### 3.1.1 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. Type in System Contact, System Name, and System Location information in this page.
3. Click Apply.


FIGURE 3-1. SYSTEM INFORMATION SCREEN

**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 includes 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-Z, a-z), digits (0-9), and minus sign (-). No space characters are permitted as part of a name. The first character must be an alpha character. And the first or last character must not be a minus sign. The allowed string length is 0 to 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 ASCII characters from 32 to 126.

## 3.1.2 IP

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

Configure the switch-managed IP information on this page.

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, 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.

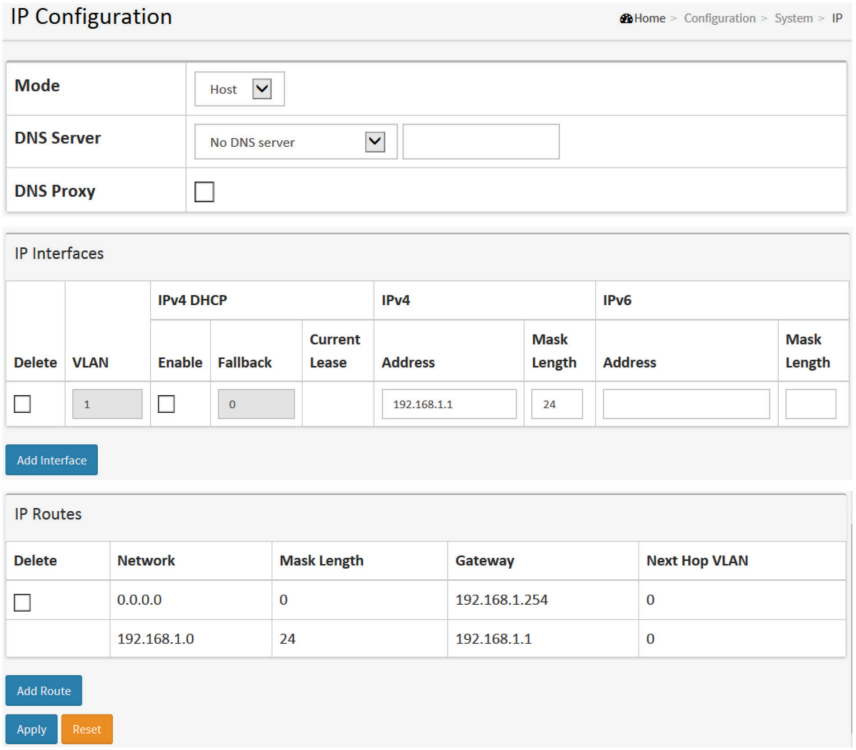



FIGURE 3-2. IP CONFIGURATION SCREEN

**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 set for 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, the 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**

- 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 an 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 the switch will try 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, so DHCP will keep retrying until a valid lease is obtained. Legal values are 0 to 4294967295 seconds.
- IPv4 DHCP Current Lease: For DHCP interfaces with an active lease, this column shows the current interface address, as provided by the DHCP server.
- IPv4 Address: The IPv4 address of the interface in dotted decimal notation. If DHCP is enabled, this field is not used. The field may also be left blank if IPv4 operation on the interface is not desired.
- IPv4 Mask: The IPv4 network mask, in number of bits (prefix length). Valid values are between 0 and 30 bits for a IPv4 address. If DHCP is enabled, this field 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. An IPv6 address is in 128-bit records represented as eight fields of up to four hexadecimal digits with a colon separating each field (:). For example, fe80::215:c5ff:fe03:4dc7. The symbol :: is a special syntax that can be used as a shorthand way of representing multiple 16-bit groups of contiguous zeros; but it can appear only once. 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: 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 notation or a valid IPv6 notation. A default route can use the value 0.0.0.0or IPv6 :: notation.
- Mask Length: The destination IP network or host mask, in number of bits (prefix length). It defines how much of a network address that must match, in order to qualify for this route. Valid values are between 0 and 32 bits, respectively, 128 for IPv6 routes. Only a default route will have a mask length of 0 (as it will match anything).
- Gateway: The IP address of the IP gateway. Valid format is dotted decimal notation, or 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, the 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.

## 3.1.3 NTP

NTP is Network Time Protocol and is used to sync the network time based Greenwich Mean Time (GMT). If you 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 shortly 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 result as 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, NTP.
2. Specify the Time parameter in manual parameters.
3. Click Apply.

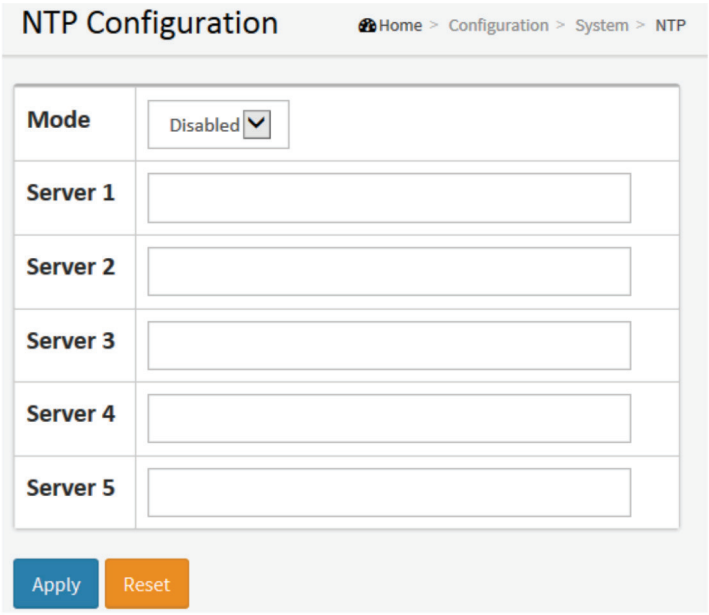



FIGURE 3-3. NTP CONFIGURATION SCREEN

**Parameter description:**

- Mode: Indicates the NTP mode operation. Possible modes are:
- Enabled: Enable NTP client mode operation.
- Disabled: Disable NTP client mode operation.
- 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: These buttons are displayed on the NTP page:

- Apply – Click to save changes.

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

## 3.1.4 TIME

The switch provides manual and automatic ways to set the system time via NTP. Manual setting is simple—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.

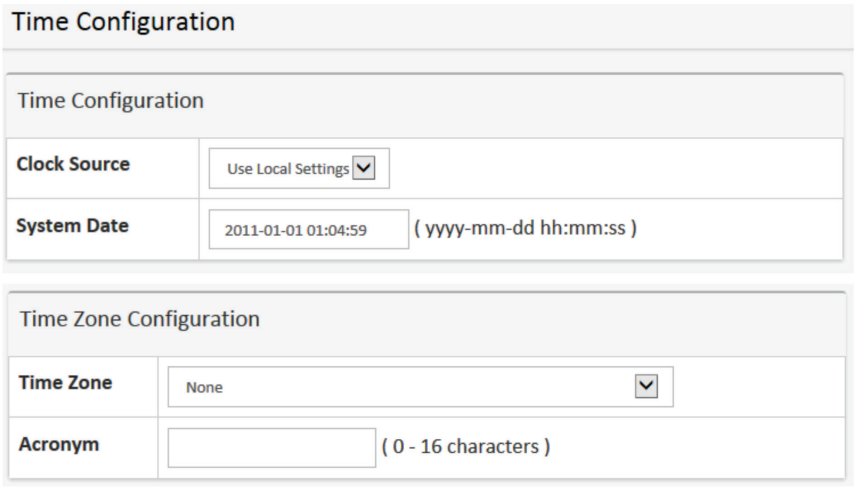



FIGURE 3-4. TIME CONFIGURATION SCREEN

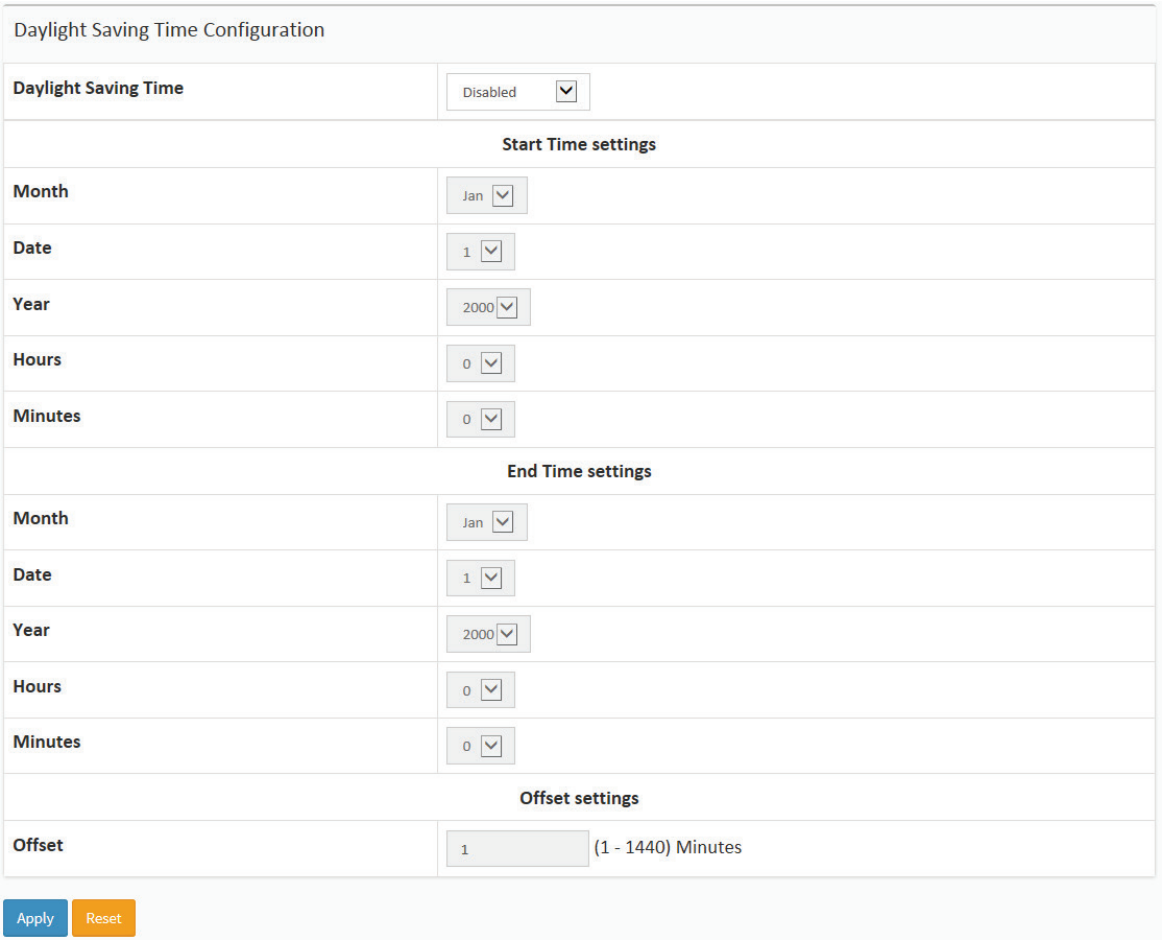



FIGURE 3-5. DAYLIGHT SAVINGS TIME CONFIGURATION SCREEN

**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 system year is a value between 2011 and 2037.

**Time Zone Configuration**

- Time Zone: Lists various Time Zones worldwide. Select the appropriate Time Zone from the drop-down box and click Apply to set.
- Acronym: The user can set the acronym of the time zone. This acronym identifies the time zone. (Range: Up to 16 characters)

**Daylight Savings Time Configuration**

- Daylight Savings Time: Use this to set the clock forward or backward according to the configurations set below for a defined Daylight Savings Time duration. Select "Disable" to disable the Daylight Savings Time configuration. Select "Recurring" and configure the Daylight Savings Time duration to repeat the configuration every year. Select "Non-Recurring" and configure the Daylight Saving Time duration for a 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**: "Start Time Settings" and "End Time Settings" display what you set in the "Start Time Settings" and "End Time Settings" fields.

- Buttons: These buttons are displayed on the NTP page:

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

## 3.1.5 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 as 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 syslog parameters, including the IP Address of the Syslog server and Port number.
3. Select the Syslog to enable it.
4. Click Apply.

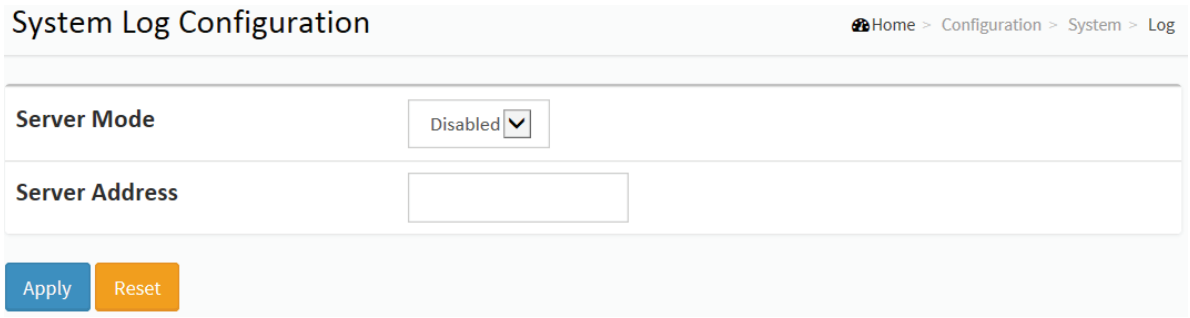



FIGURE 3-6. SYSTEM LOG CONFIGURATION SCREEN

**Parameter description:**

- Server Mode: Indicates the server mode operation. When the mode operation is enabled, the syslog message will be sent out to the syslog server. The syslog protocol is based on UDP communication and received on UDP port 514. The syslog server will not send acknowledgments back to the sender since UDP is a connectionless protocol and it does not provide acknowledgments. The syslog packet will always be sent ou,t 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 the syslog server. If the switch provides a DNS feature, it also can be a host name.

• Syslog Level: Indicates what kind of message will be sent to a syslog server. Possible modes are:

- Info: Send information, warnings, and errors.
- Warning: Send warnings and errors.
- Error: Send errors.

- Buttons: These buttons are displayed on the NTP page:

- Apply – Click to save changes.

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

## 3.2 GREEN ETHERNET

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

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 µs for 1-Gbit links and 30 µs for other link speeds. EEE devices must agree upon the value of the wakeup time to make sure that both the receiving and transmitting devices have 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; so you cannot enable EEE for these ports.

When a port is powered down to save power, outgoing traffic is stored in a buffer until the port is powered up again. Because there is some overhead in powering the port off and on, more power can be saved if the traffic can be buffered 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.
2. Enable or disable the ActiPHY, PerfectReach, EEE, and EEE Urgent Queues.
3. Click Apply.

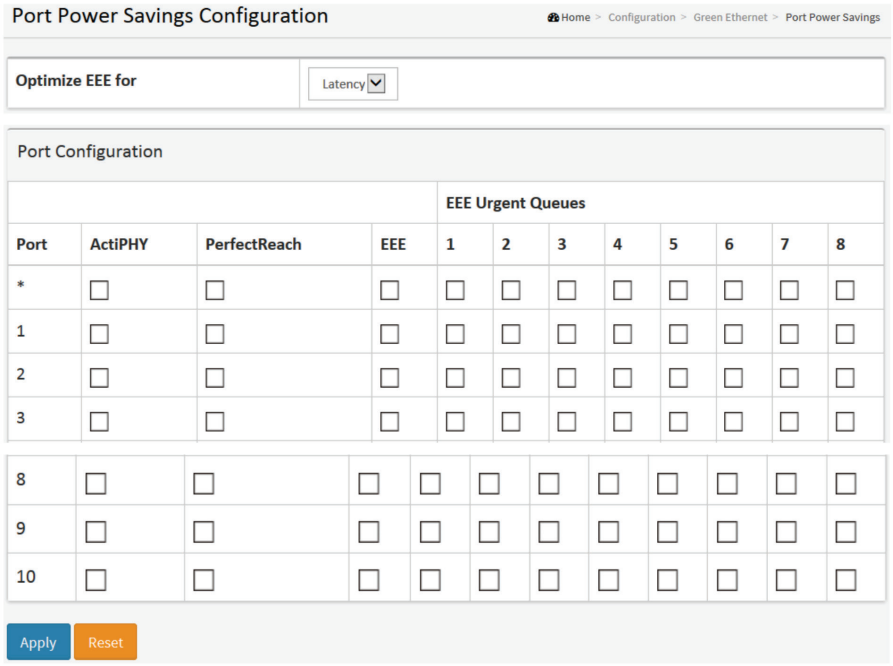



FIGURE 3-7. PORT POWER SAVING CONFIGURATION SCREEN

**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.
- ActiPHY: Link down power savings enabled. ActiPHY works by lowering the power for a port when there is no link. The port is powered up for a short moment to determine if cable is inserted.
- PerfectReach: Cable length power savings enabled. PerfectReach works by determining the cable length and lowering the power for ports with short cables.
- EEE: Controls whether EEE is enabled for this switch port.

To maximize power savings, the circuit isn't started 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, you can 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 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.

## 3.3 PORTS CONFIGURATION

The section describes how to configure the detailed port parameters of the switch. You can use Port configure to enable or disable a switch port. Monitor the ports content or status in the function.

### 3.3.1 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, Excessive Collision mode, and Power Control.
3. Click Apply.

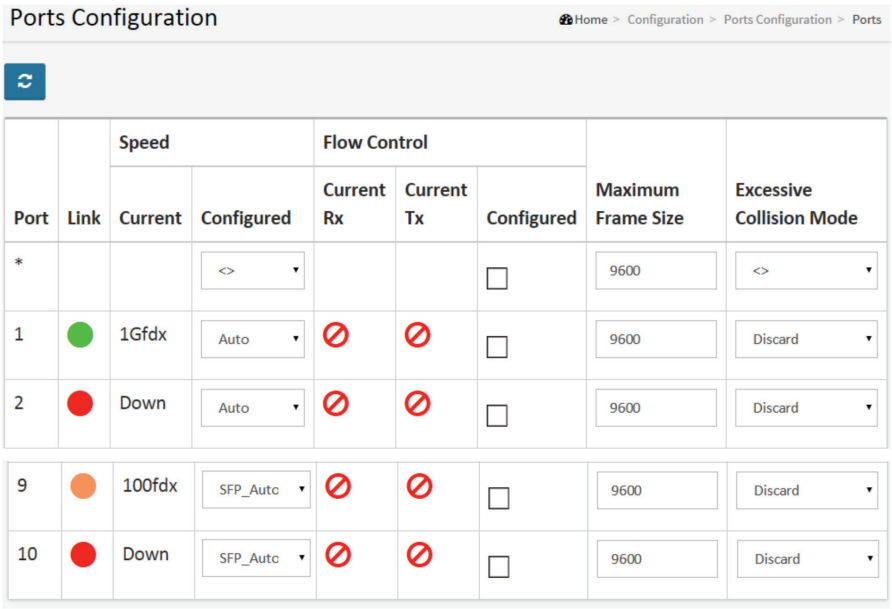



FIGURE 3-8. PORT CONFIGURATION SCREEN

**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 are shown. Possible speeds are:

- Disabled - Disables the switch port operation.

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

- 10-Mbps HDX - Forces the copper port to 10-Mbps half- duplex mode.
- 10-Mbps FDX - Forces the copper port to 10-Mbps full-duplex mode.
- 100-Mbps HDX - Forces the copper port to 100-Mbps half-duplex mode.
- 100-Mbps FDX - Forces the copper port to 100-Mbps full-duplex mode.
- 1-Gbps FDX - Forces the port in 1-Gbps full-duplex mode.
- 2.5-Gbps FDX - Forces the port to 2.5-Gbps 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. SFP auto detect for some SFPs may not work. The port is set in AMS mode. The copper port is set in Auto mode.

- 100-FX - The SFP port is in 100-FX speed. The copper port is disabled.
- 100-FX_AMS - Port in AMS mode. The SFP port is in 100-FX speed. The copper port is in Auto mode.
- 1000-X - The SFP port is in 1000-X speed. The copper port is disabled.
- 1000-X_AMS - Port in AMS mode. The SFP port is in 1000-X speed. The copper port is in Auto mode. Ports in AMS mode with 1000-X speed have the copper port preferred. Ports in AMS mode with 100-FX speed have the 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.

◆ Excessive Collision Mode: Configure the port transmit collision behavior.

- Discard: Discard frame after 16 collisions (default).
- Restart: Restart the backoff algorithm after 16 collisions.

◆ Buttons:

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

◆ Upper right icon (Refresh): Click the icon to  for refresh the Port link Status manually.

## 3.3.2 PORTS DESCRIPTION

The section describes how to configure the Port's alias or any descriptions for the Port Identity. The user must provide 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, then Port Description.
2. Specify a detailed Port alias or an alphanumeric string describing the full name and version for the system's hardware type, software version, and networking application.
3. Click Apply.

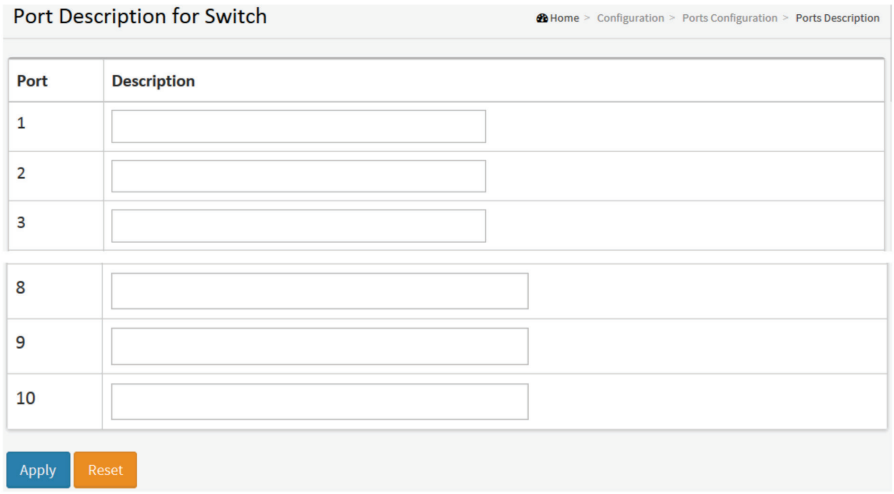



FIGURE 3-9. PORT CONFIGURATION SCREEN

**Parameter description:**

- Port: This is the logical port number for this row.
- Description: Enter up to 47 characters for the name that identifies this port.
- Buttons:

- Apply – Click to save changes.

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

## 3.4 DHCP

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

### 3.4.1 SERVER

#### 3.4.1.1 MODE

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

#### WEB INTERFACE

To configure a DHCP server mode in the web interface:

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

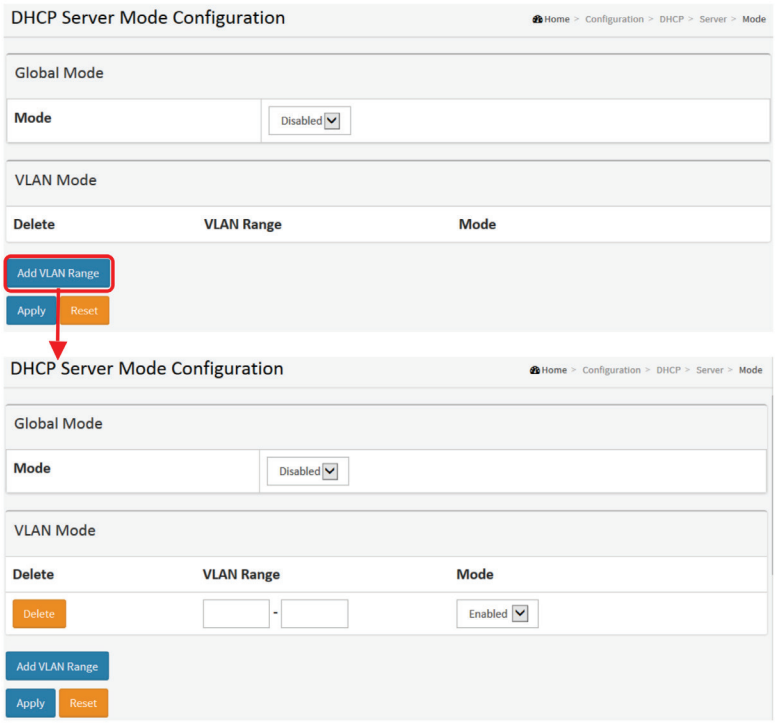



FIGURE 3-10. DHCP SERVER MODE SCREEN

**Parameter description:**

- Mode: Configure the operation mode per system. Possible modes are:

- Enabled: Enable DHCP server per system.

- Disabled: Disable DHCP server pre system.

- VLAN Range: Indicate the VLAN range in which the 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 fields or both.

On the other hand, if you want to disable an existing VLAN range, follow these 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: Indicates the operation mode per VLAN. Possible modes are:

- Enabled: Enable DHCP server per VLAN.

- Disabled: Disable DHCP server pre VLAN.

- Buttons:

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

- Apply – Click to save changes.

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

### 3.4.1.2 EXCLUDED IP

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

### WEB INTERFACE

To configure a DHCP server excluded IP in the web interface:

1. Click Configuration, DHCP, Server, Excluded IP.

2. Click Add IP Range, then you can create a new IP Range on the switch.

3. Click Apply.

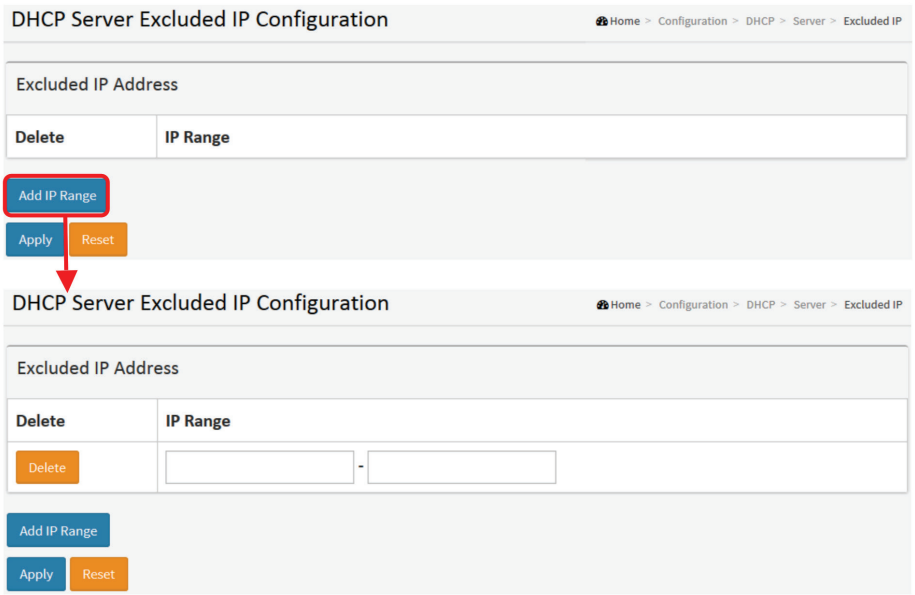



FIGURE 3-11. DHCP SERVER EXCLUDED IP SCREEN

**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 fields or both.
- Buttons:

- 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.

### 3.4.1.3 POOL

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

### WEB INTERFACE

To configure a DHCP server pool in the web interface:

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

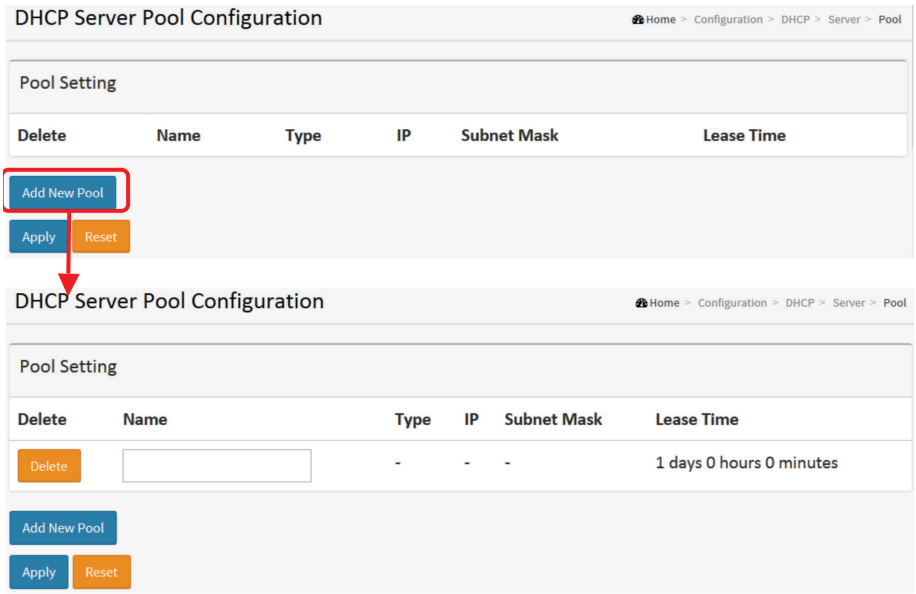



FIGURE 3-12. DHCP SERVER POOL SCREEN

**Parameter description:**

Pool Setting: Add or delete pools. Add a pool and give a name to create a new pool with the ”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 detailed settings, you can click the pool name to go into the configuration page.
- Type: Display the type of pool.

- Network: Defines a pool of IP addresses to service more than one DHCP client.
- Host: Defines services for a specific DHCP client identified by a client identifier or hardware address. If “-” is displayed, the services are not defined.

- IP: Display the network number of the DHCP address pool. If “-” is displayed, the network number is not defined.
- Subnet Mask: Displays the subnet mask of the DHCP address pool. If “-” is displayed, the subnet mask is not defined.
- Lease Time: Displays the lease time of the pool.
- Buttons:

- 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.

## 3.4.2 SNOOPING

DHCP Snooping blocks intruders on the untrusted ports of the switch when they try to intervene by injecting a bogus DHCP reply packet to a legitimate conversation between the DHCP client and server.

The section describes how to configure the DHCP Snooping parameters of the switch. 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, Snooping.
2. Select "Enabled" in the DHCP Snooping Configuration mode.
3. Select "Trusted" for the specific port in the Port Mode Configuration.
4. Click Apply.

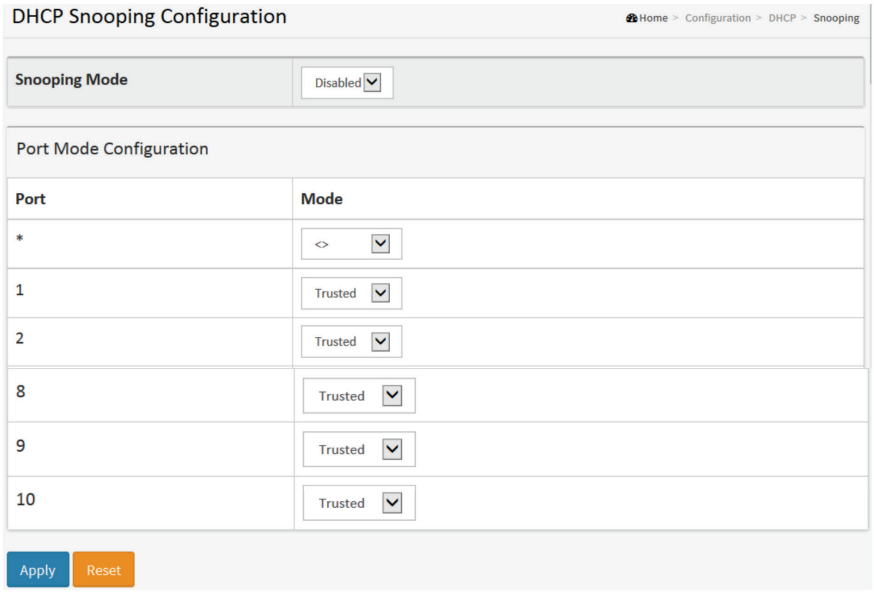



FIGURE 3-13. DHCP SNOOPING CONFIGURATION SCREEN

**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 a trusted source of the DHCP messages.

- Untrusted: Configures the port as an 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.

## 3.4.3 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 the GIADDR field to determine the assigned subnet. Be sure to configure the VLAN interface IP address and PVID (Port VLAN ID) correctly.

### WEB INTERFACE

To configure DHCP Relay in the web interface:

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

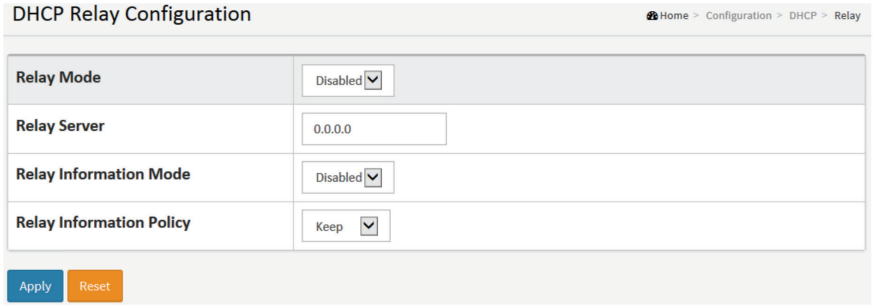



FIGURE 3-14. DHCP RELAY CONFIGURATION SCREEN

**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's IP address.

- Relay Information Mode: Indicates the DHCP relay information mode option operation. The option 82 circuit ID is formatted 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 a standalone device it always equal 0, in a stackable device it is the switch ID), and the last two characters are the port number. For example, "00030108" means the DHCP message is received from VLAN ID 3, switch ID 1, port No 8. The Option 82 remote ID value equals 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.

## 3.5 SECURITY

This section shows you how 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.

### 3.5.1 SWITCH

#### 3.5.1.1 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, Users.
2. Click Add new user.
3. Specify the User Name parameter.
4. Click Apply.

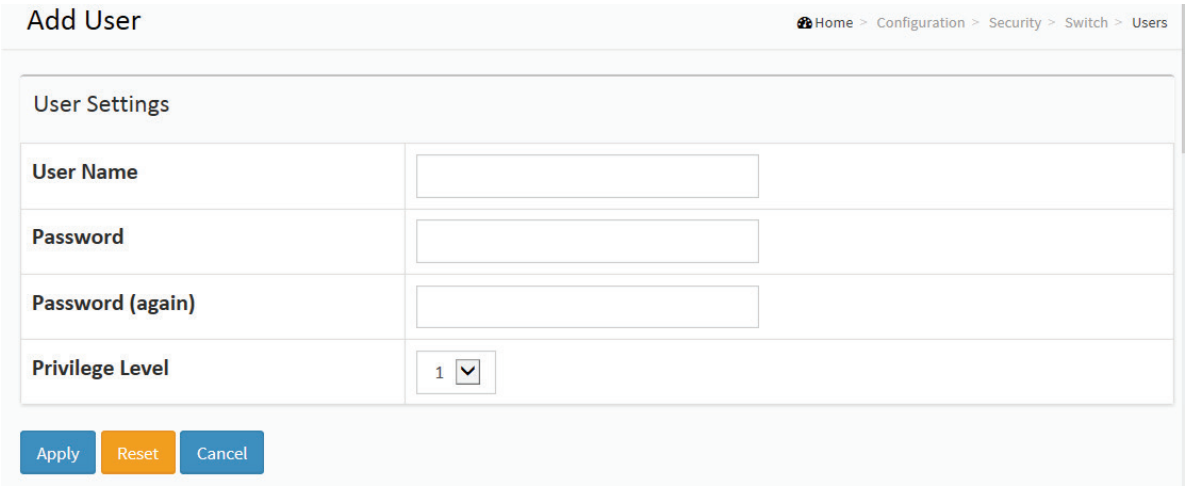



FIGURE 3-15. USERS CONFIGURATION SCREEN

**Parameter description:**

- User Name: The name identifying the user. This is also a link to Add/Edit User.
- Password: Type the password. The allowed string length is 0 to 255, and the allowed content is the ASCII characters from 32 to 126.
- Password (again): Type the password again. You must type the same password again in the field.
- Privilege Level: The privilege level of the user. The allowed range is 1 to 15. If the privilege level value is 15, the user can access all groups for full control of the device. Other values need to refer to each group privilege level. A user's privilege level should be same or greater than the group privilege level to have the access of that group. By default settings, most groups with privilege level 5 have read-only access, and groups with privilege level 10 have read-write access. System maintenance users (software upload, factory defaults and etc.) need user privilege level 15. Use privilege level 15 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).

### 3.5.1.2 PRIVILEGE LEVEL

This page provides an overview of the privilege levels. The switch enables the user to 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 System, Account, Privilege Level.
2. Specify the Privilege parameter.
3. Click Apply.

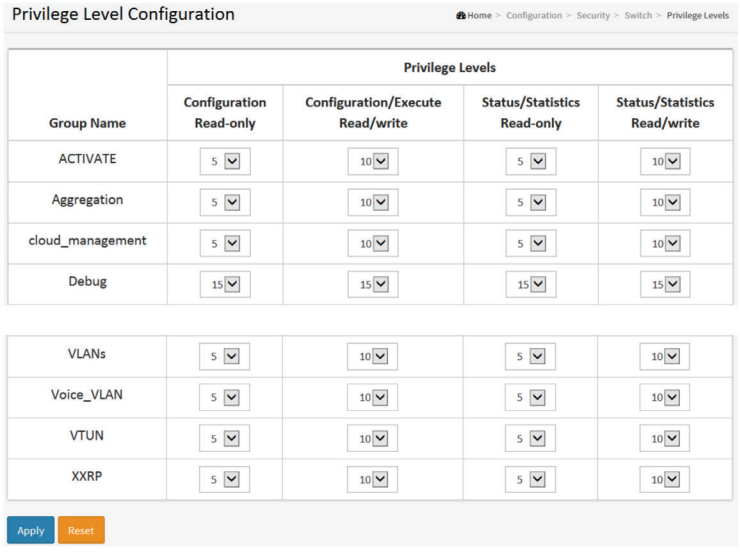



FIGURE 3-16. PRIVILEGE LEVEL CONFIGURATION SCREEN

**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 contain more than one. The following description defines these privilege level groups in detail:

- 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, status/statistics read-write (e.g. to clear statistics). User Privilege should be the same or greater than the authorization Privilege level to have access to that group.
- Buttons:

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

### 3.5.1.3 AUTHENTICATION METHOD

This page shows how to configure a user as 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. Specify the Client (console, telent, ssh, web) that you want to monitor.
2. Specify the Authentication Method (none, local, radius, tacacs+)
3. Check Fallback.
4. Click Apply.

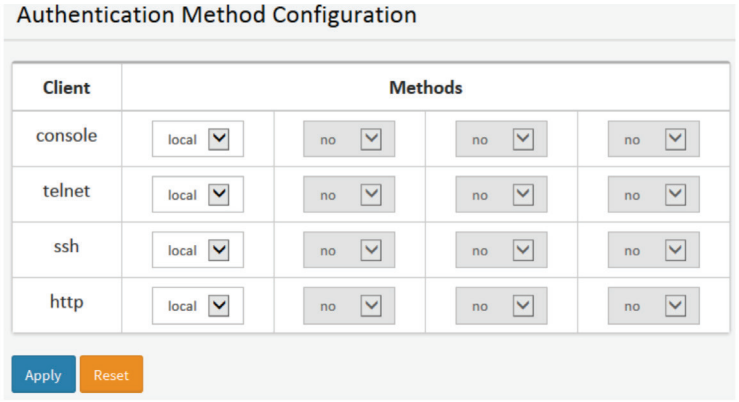



FIGURE 3-17. AUTHENTICATION METHOD CONFIGURATION SCREEN

**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 involve remote servers are timed out if the remote servers are offline. In this case, the switch tries the next method. The switch tries each method from left to right and continues until a method either approves or rejects a user. If a remote server is used for primary authentication, we recommend that you 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.

- Buttons:

- Apply – Click to save changes.

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

### 3.5.1.4 SSH

This section shows you how to use SSH (Secure SHell) to securely access the Switch. SSH is a secure communication protocol that combines authentication and data encryption to provide secure encrypted communication.

### WEB INTERFACE

To configure an SSH Configuration in the web interface:

1. Select "Enabled" in the SSH Configuration Mode field.
2. Click Apply.

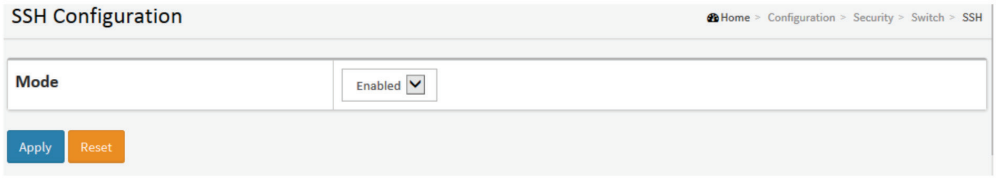



FIGURE 3-18. SSH CONFIGURATION SCREEN

Parameter description:

- Mode: Indicates the SSH mode operation. Possible modes are:

- Enabled: Enable SSH mode operation.

- Disabled: Disable SSH mode operation.

- Buttons:

- Apply – Click to save changes.

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

### 3.5.1.5 HTTPS

This section shows you how to use HTTPS to securely access the Switch. HTTPS is a secure communication protocol that combines authentication and data encryption to provide secure encrypted communication via the browser.

### WEB INTERFACE

To set HTTPS Configuration in the web interface:

1. Select “Enabled” in the HTTPS Configuration Mode field.
2. Select “Enabled” in the Automatic Redirect of HTTPS Configuration field.
3. Click Apply.

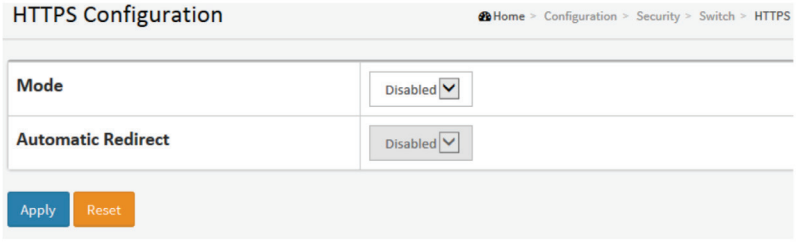



FIGURE 3-19. HTTPS CONFIGURATION SCREEN

Parameter description:

- Mode: Indicates the HTTPS mode operation. Possible modes are:

- Enabled: Enable HTTPS mode operation.

- Disabled: Disable HTTPS mode operation.

- Automatic Redirect: Indicates the HTTPS redirect mode operation. Automatically redirect web browser to HTTPS when HTTPS mode is enabled. Possible modes are:

- Enabled: Enable HTTPS redirect mode operation.

- Disabled: Disable HTTPS redirect mode operation.

### 3.5.1.6 ACCESS MANAGEMENT

This section shows you how to configure the switch's access management table HTTP/HTTPS, SNMP, and TELNET/SSH settings. You can manage the Switch over an Ethernet LAN, or over the Internet.

### WEB INTERFACE

To configure Access Management in the web interface:

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

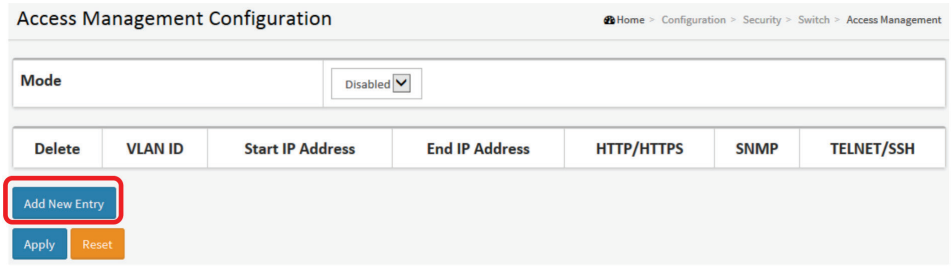



FIGURE 3-20. ACCESS MANAGEMENT CONFIGURATION SCREEN

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.
- Delete: Check to delete the entry. It will be deleted during the next save.
- 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 the 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 the TELNET/SSH interface if the host IP address matches the IP address range provided in the entry.
- Buttons:

- Add New Entry – Click to add a new access management entry.

- Apply – Click to save changes.

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

### 3.5.1.7 SNMP

Any Network Management System (NMS) running the Simple Network Management Protocol (SNMP) can manage the Managed devices equipped with an 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. An SNMP agent is running on the switch to respond to the request issued by the SNMP manager.

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

### SYSTEM

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

### WEB INTERFACE

To configure the SNMP System in the web interface:

1. Click SNMP, System.
2. Select Enable or Disable in the SNMP State field to enable or disable the SNMP function.
3. Specify the Engine ID.
4. Click Apply.

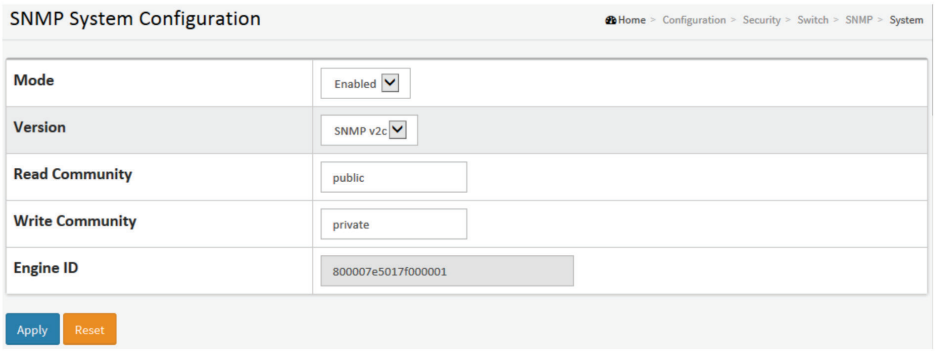



FIGURE 3-21. SNMP SYSTEM CONFIGURATION SCREEN

**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 an SNMP agent. The allowed string length is 0 to 255, and the allowed content is the ASCII characters from 33 to 126.

The field is applicable only when the SNMP version is SNMPv1 or SNMPv2c. If the SNMP version is SNMPv3, the community string will be associated with SNMPv3 communities table. This provides more flexibility to configure security name than an 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: This indicates the community write access string to permit access to an SNMP agent. The allowed string length is 0 to 255, and the allowed content is the ASCII characters from 33 to 126.

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

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

## TRAP

Configure SNMP trap on this page.

**Global Settings**

Configure SNMP trap on this page.

## WEB INTERFACE

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

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

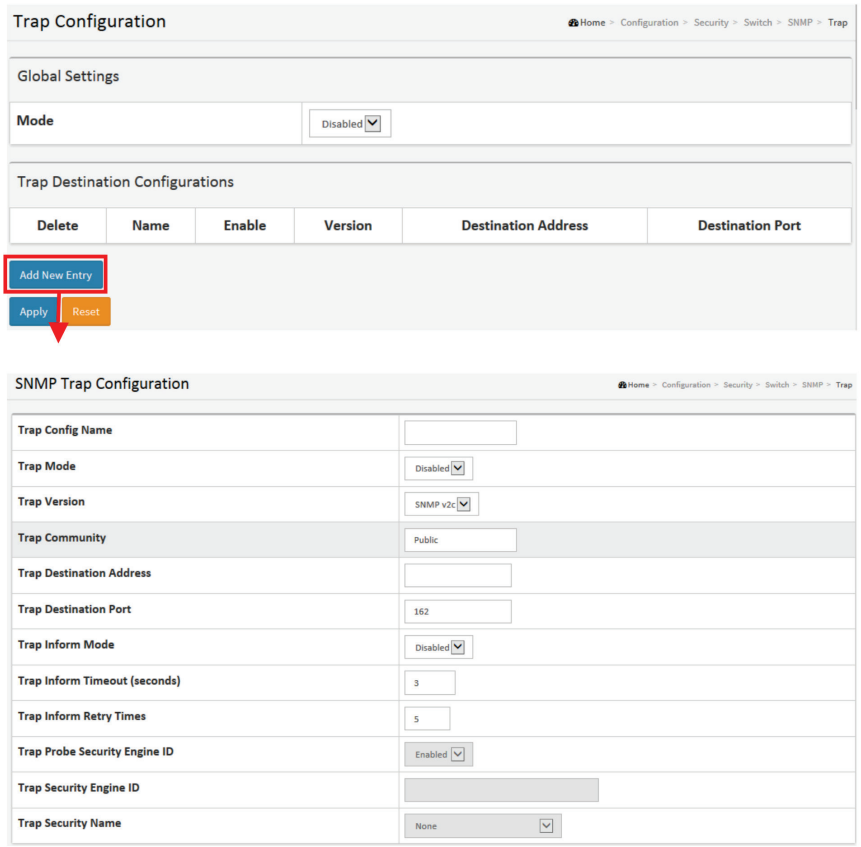



FIGURE 3-22. SNMP TRAP CONFIGURATION SCREEN

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

• Destination Address: Indicates the SNMP trap destination address. It allows a valid IP address in dotted decimal notation ('x.y.z.w').

It also allows a valid hostname. A valid hostname is a string drawn from the alphabet (A-Z, a-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.

It indicates the SNMP trap destination IPv6 address. The IPv6 address is in 128-bit records represented as eight fields of up to four hexadecimal digits with a colon separating each field (:). For example, 'fe80::215:c5ff:fe03:4dc7'. The symbol '::' is a special syntax that can be used as a shorthand way of representing multiple 16-bit groups of contiguous zeros; but it can 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. An SNMP Agent will send an 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.

## COMMUNITIES

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

## WEB INTEFACE

To display the configure SNMP Communities in the web interface:

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


FIGURE 3-23. SNMPV1/V2 COMMUNITIES SECURITY CONFIGURATION SCREEN

**Parameter description:**

- Delete: Check to delete the entry. It will be deleted during the next save.
- Community: Indicates the community access string to permit access to SNMPv3 agent. The allowed string length is 1 to 32, and the allowed content is ASCII characters from 33 to 126. The community string will be treated as a security name and map an 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 a source mask.
- Source Mask: Indicates the SNMP access source address mask

## USERS

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

## WEB INTERFACE

To display the configure SNMP Users in the web interface:

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

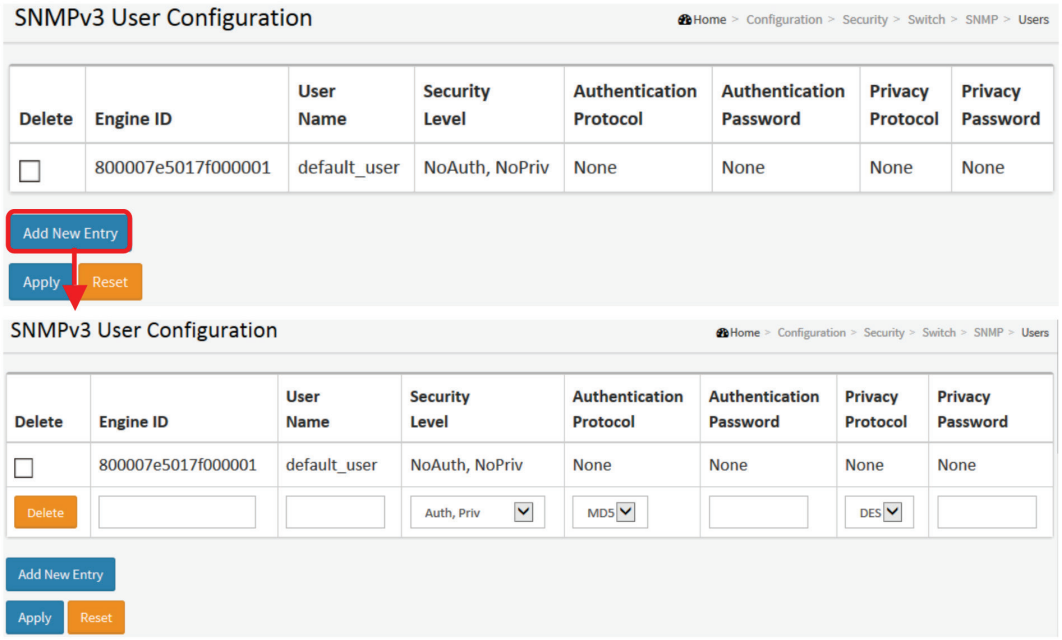



FIGURE 3-24. SNMP USERS CONFIGURATION SCREEN

Parameter description:

- Delete: Check to delete the entry. It will be deleted during the next save.
- Engine ID: An octet string identifying the engine ID that this entry should belong to. The string must contain an even number (in hexadecimal format) with the 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 the user engine ID equals the system engine ID, then it is a local user; otherwise it's a 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 the security level cannot be modified if an entry already exists. First, make sure 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 the MD5 authentication protocol.
- SHA: An optional flag to indicate that this user uses the SHA authentication protocol.

The value of the security level cannot be modified if an entry already exists. First, make sure 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 the 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.

## GROUP

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

## WEB INTERFACE

To display the configure SNMP Groups in the web interface:

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

Figure 2-5.1.7.5: The SNMP Groups Configuration

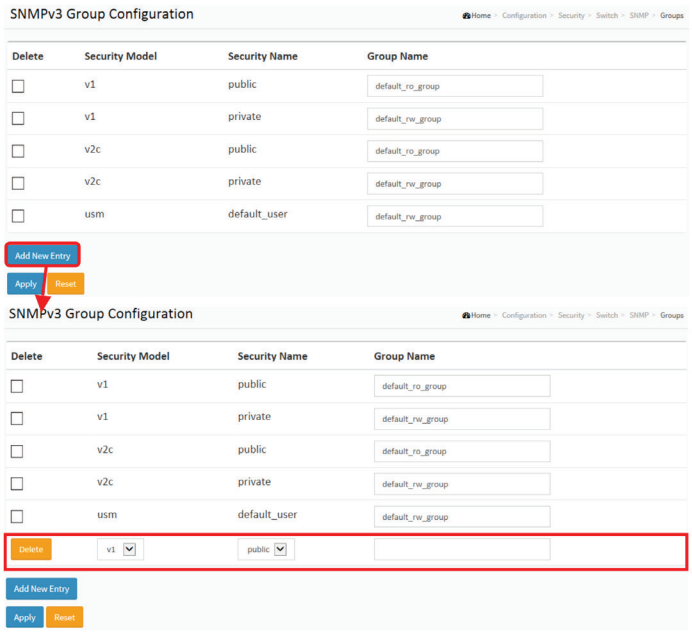



FIGURE 3-25. SNMP GROUPS CONFIGURATION SCREEN

Parameter description:

- Delete: Check to delete the entry. It will be deleted during the next save.
- Security Model: Indicates the security model that this entry should belong to. Possible security models are:

- v1: Reserved for SNMPv1.

- v2c: Reserved for SNMPv2c.

- usm: User-based Security Model (USM).

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

## VIEWS

The function is used to configure the SNMPv3 view. The Entry index keys are OID Subtree and View Name. To create a new view account, check the <Add new view> button, 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 display the configure SNMP views in the web interface:

1. Click SNMP, Views.
2. Click Add new View.
3. Specify the SNMP View parameters.
4. Click Apply.
5. If you want to modify or clear the setting, then click Reset.

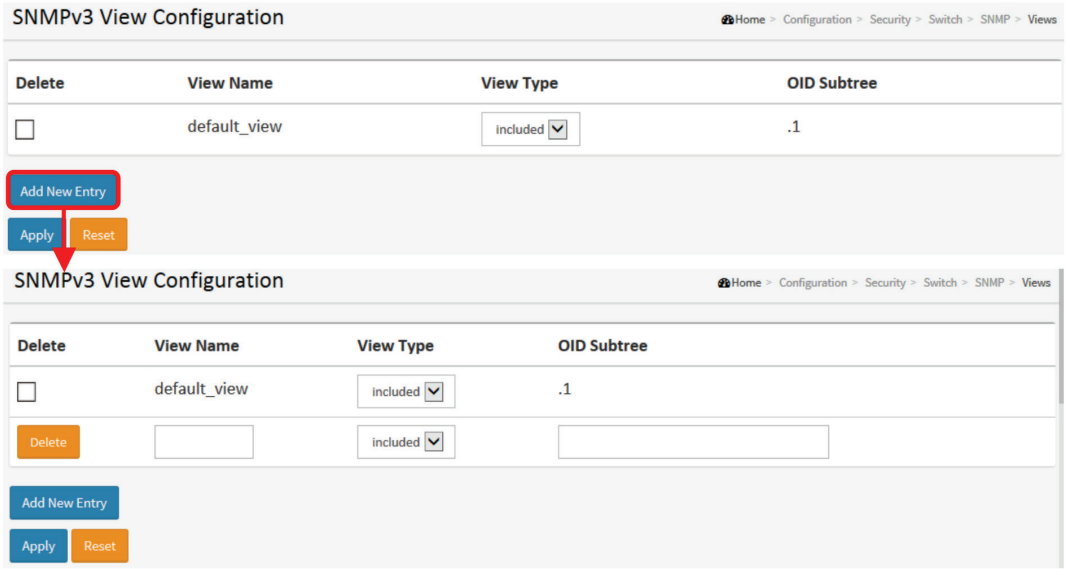



FIGURE 3-26. SNMP VIEWS CONFIGURATION SCREEN

Parameter description:

- Delete: Check to delete the entry. It will be deleted during the next save.
- View Name: A string identifying the view name that this entry should belong to. The allowed string length is 1 to 32, and the allowed content is 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 its 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(*).

## 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 display the configure SNMP Access in the web interface:

1. Click SNMP, 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.

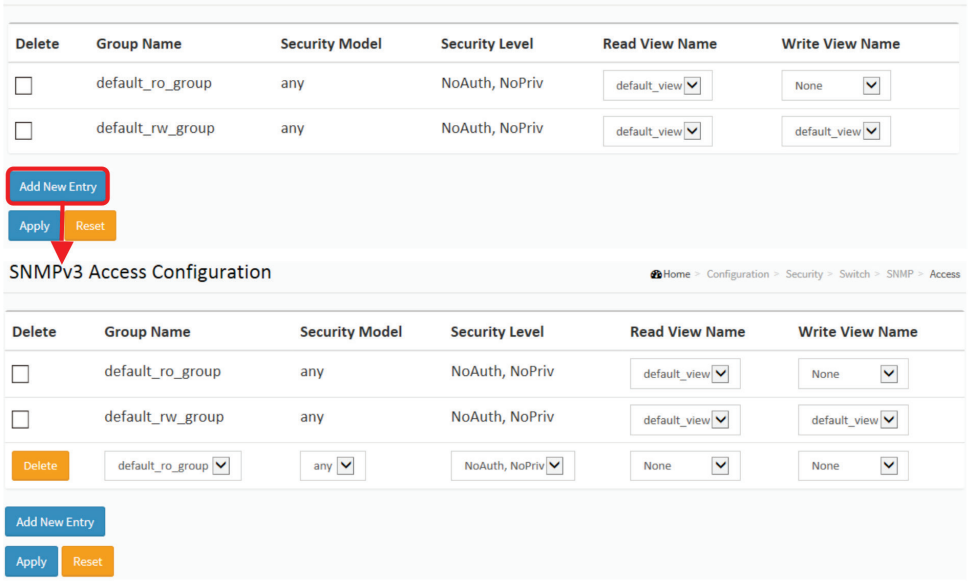



FIGURE 3-27. SNMP ACCESSES CONFIGURATION SCREEN

**Parameter description:**

- Delete: Check to delete the entry. It will be deleted during the next save.
- Group Name: A string identifying the group name that this entry should belong to. The allowed string length is 1 to 32, and the allowed content is 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.

## TRAP EVENT SEVERITY

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

## WEB INTERFACE

To display the configure Trap Event Severity in the web interface:

1. Click SNMP, Trap Event Severity.
2. Scroll to select the Group name and Severity Level.
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.

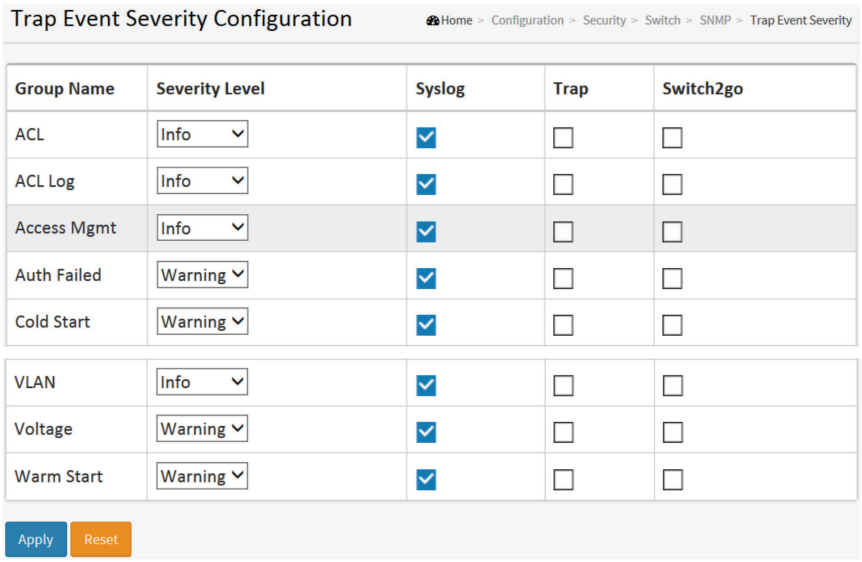



FIGURE 3-28. TRAP EVENT SEVERITY CONFIGURATION SCREEN

Parameter description:

- Group Name: The name identifying the severity group.

- Severity Level: Every group has a severity level. The following level types are supported:

<0> Information: Information messages.

<1> Warning: Warning conditions.

<2> Error: Error conditions.

- Syslog: Enable - Select this Group Name in Syslog.
- Trap: Enable - Select this Group Name in Trap.
- SMTP: Enable - Select this Group Name in SMTP.

### 3.5.1.8 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.

### STATISTICS

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

### WEB INTERFACE

To display the configure RMON configuration in the web interface:

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

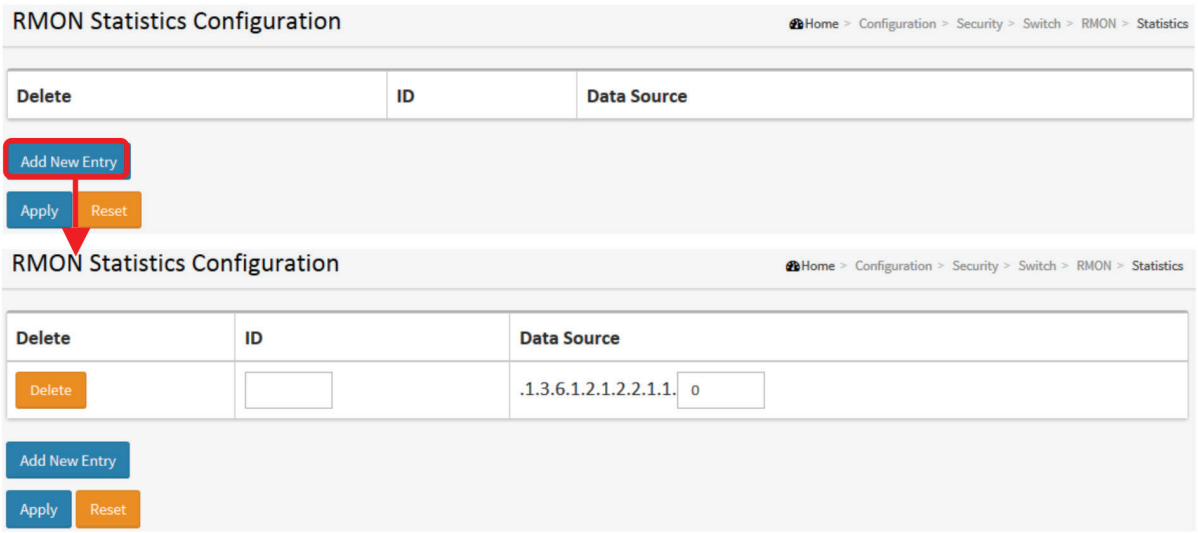



FIGURE 3-29. RMON Statics Configuration screen

**Parameter description:**

These parameters are displayed on the RMON Statistics Configuration page:

- Delete: Check to delete the entry. It will be deleted during the next save.
- ID: Indicates the index of the entry. The range is from 1 to 65535.
- Data Source: Indicates the port ID which wants to be monitored. If in stacking switch, the value must add 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 will be saved in the RMON.

## HISTORY

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

## WEB INTERFACE

To display the configure RMON History in the web interface:

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

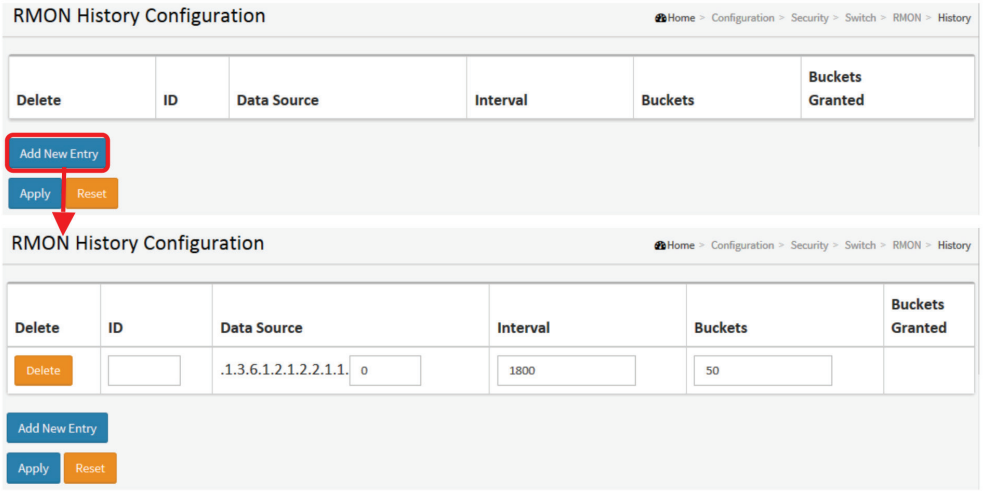



FIGURE 3-30. RMON HISTORY CONFIGURATION SCREEN

**Parameter description:**

These parameters are displayed on the RMON History Configuration page:

- Delete: Check to delete the entry. It will be deleted during the next save.
- ID: Indicates the index of the entry. The range is from 1 to 65535.
- Data Source: Indicates the port ID to be monitored. If a 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 with this History control entry stored in RMON. The range is from 1 to 3600; default value is 50.

• Buckets Granted: The number of data saved in the RMON.

## RMON

Configure the 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 RMON, Alarm.
2. Click Add New Entry.
3. Specify the ID parameters.
4. Click Apply.

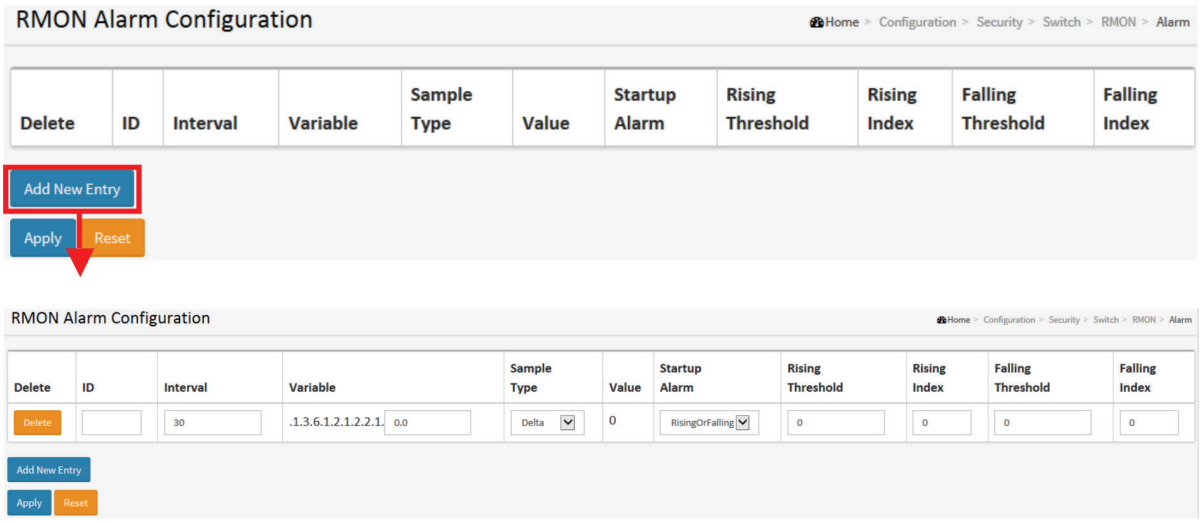



FIGURE 3-31. RMON ALARM CONFIGURATION SCREEN

Parameter description:

These parameters are displayed on the RMON Alarm Configuration page:

- Delete: Check to delete the entry. It will be deleted during the next save.
- ID: Indicates the index of the entry. The range is from 1 to 65535.
- Interval: Indicates the interval in seconds for sampling and comparing the rising and falling threshold. The range is from 1 to 2^31-1.
- Variable: Indicates the particular variable to be sampled, the possible variables are:

- InOctets: The total number of octets received on the interface, including framing characters.
- InUcastPkts: The number of unicast packets delivered to a higher-layer protocol.
- InNUcastPkts: The number of broadcast and multicast packets delivered to a higher-layer protocol.
- InDiscards: The number of inbound packets that are discarded even when the packets are normal.
- InErrors: The number of inbound packets that contained errors preventing them from being delivered to a higher-layer protocol.
- InUnknownProtos: the number of the inbound packets that were discarded because of an unknown or unsupported protocol.
- OutOctets: The number of octets transmitted out of the interface , including framing characters.
- OutUcastPkts: The number of unicast packets that request to transmit.

- OutNUcastPkts: The number of broadcast and multicast packets that request to transmit.
- OutDiscards: The number of outbound packets that are discarded even when the packets is normal.
- OutErrors: The number of outbound packets that could not be transmitted because of errors.
- OutQLen: The length of the output packet queue (in packets).

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

- Absolute: Get the sample directly.
- Delta: Calculate the difference between samples (default).

◆ Value: The value of the statistic during the last sampling period.

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

- 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).

## 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 RMON, Event.
2. Click Add New Entry.
3. Specify the ID parameters.
4. Click Apply.

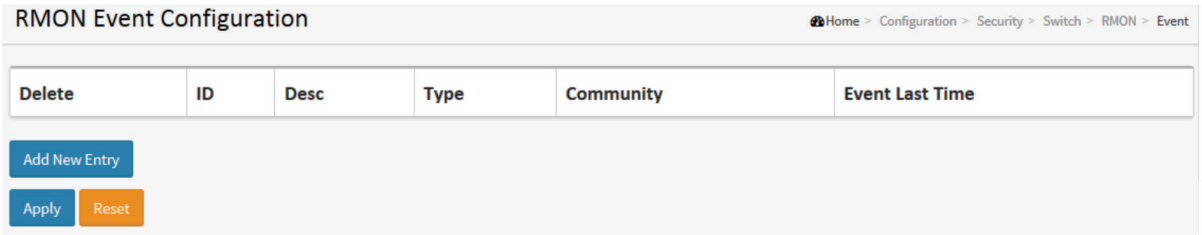



FIGURE 3-32. RMON EVENT CONFIGURATION SCREEN

**Parameter description:**

These parameters are displayed on the RMON History Configuration page:

- Delete: Check to delete the entry. It will be deleted during the next save.
- ID: Indicates the index of the entry. The range is from 1 to 65535.
- Desc: Indicates this event; the string length is from 0 to 127; default is a null string.

Type: Indicates the notification of the event; the possible types are:

- none: No SNMP log is created, no SNMP trap is sent.
- log: Create SNMP log entry when the event is triggered.
- snmptrap: Send SNMP trap when the event is triggered.
- logandtrap: Create SNMP log entry and send SNMP trap when the event is triggered.

- Community: Specify the community when a 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.

## 3.5.2 NETWORK

### 3.5.2.1 LIMIT CONTROL

This section shows you to 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 Limit Control in the web interface:

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

To configure Limit Control Port in the web interface:

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

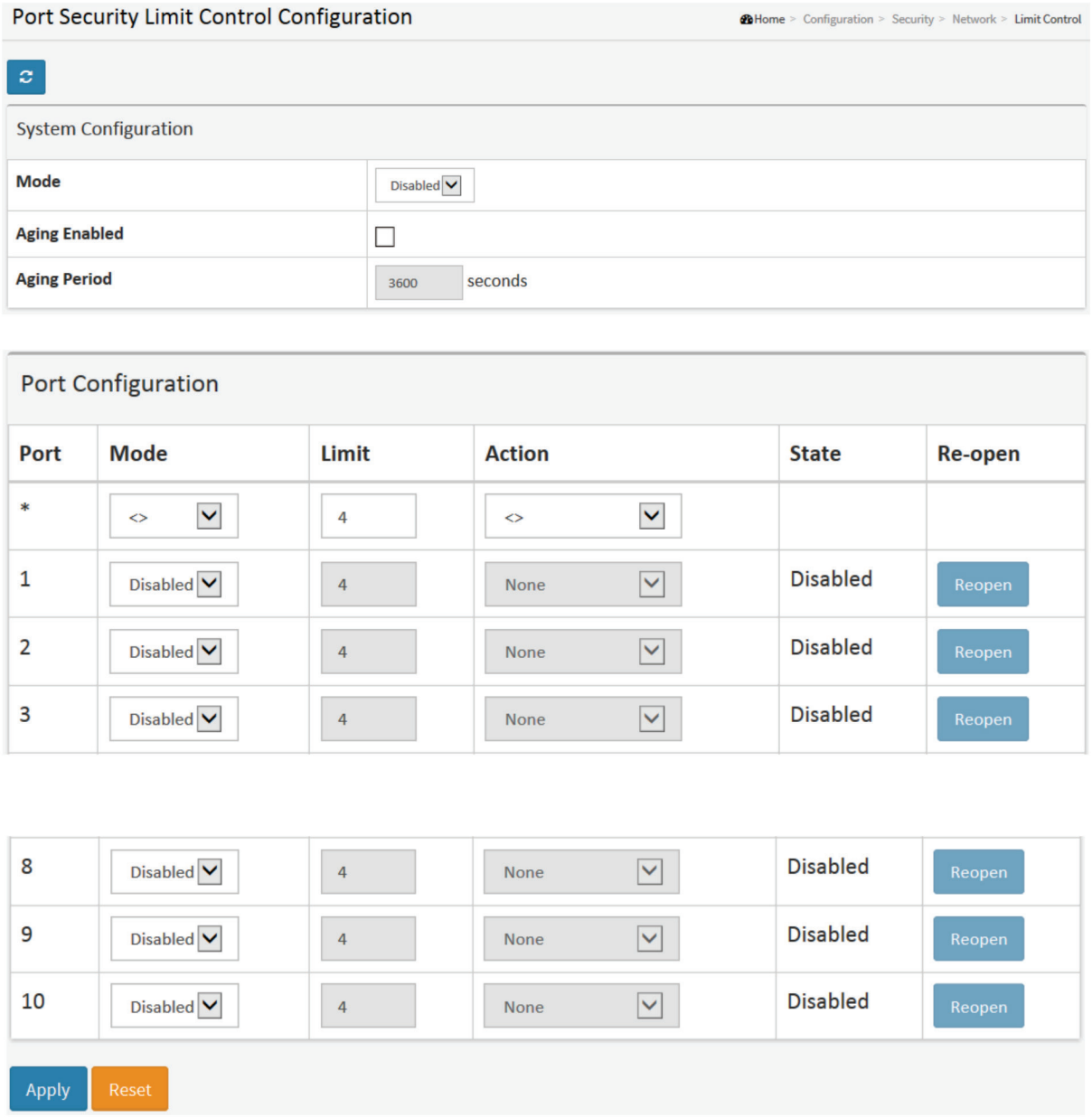



FIGURE 3-33. PORT SECURITY LIMIT CONTROL CONFIGURATION SCREEN

**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 for 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 starts 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. 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 are 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 is exceeded.

- Shutdown: If Limit + 1 MAC addresses are 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 are seen on the port, both the "Trap" and the "Shutdown" actions described above will be taken.

- State: This column shows the current state of the port as seen from the Limit Control's point of view. The state takes one of four values:

- Disabled: Limit Control is either globally disabled or disabled on the port.

- Ready: The limit is not yet reached. This can be shown for all actions.

- Limit Reached: Indicates that the limit is reached on this port. This state can only be shown if Action is set to None or Trap.
- Shutdown: Indicates that the port is shut down by the Limit Control module. This state can only be shown if Action is set to Shutdown or Trap & Shutdown.

◆ 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 Shutdown in the Action section.

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

◆ Upper right icon (Refresh): You can click on this icon to refresh the Port Security information manually.

◆ Buttons:

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

### 3.5.2.2 NAS

The section describes how 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. Select “Enabled” in the Network Access Server Configuration Mode.
2. Check Reauthentication Enabled.
3. Set Reauthentication Period (Default is 3600 seconds).
4. Set EAPOL Timeout (Default is 30 seconds).
5. Set Aging Period (Default is 300 seconds).
6. Set Hold Time (Default is 10 seconds).
7. Check RADIUS-Assigned QoS Enabled.
8. Check RADIUS-Assigned VLAN Enabled.
9. Check Guest VLAN Enabled.
10. Specify Guest VLAN ID.
11. Specify Max. Reauth. Count.
12. Check Allow Guest VLAN if EAPOL Seen.
13. Click Apply.

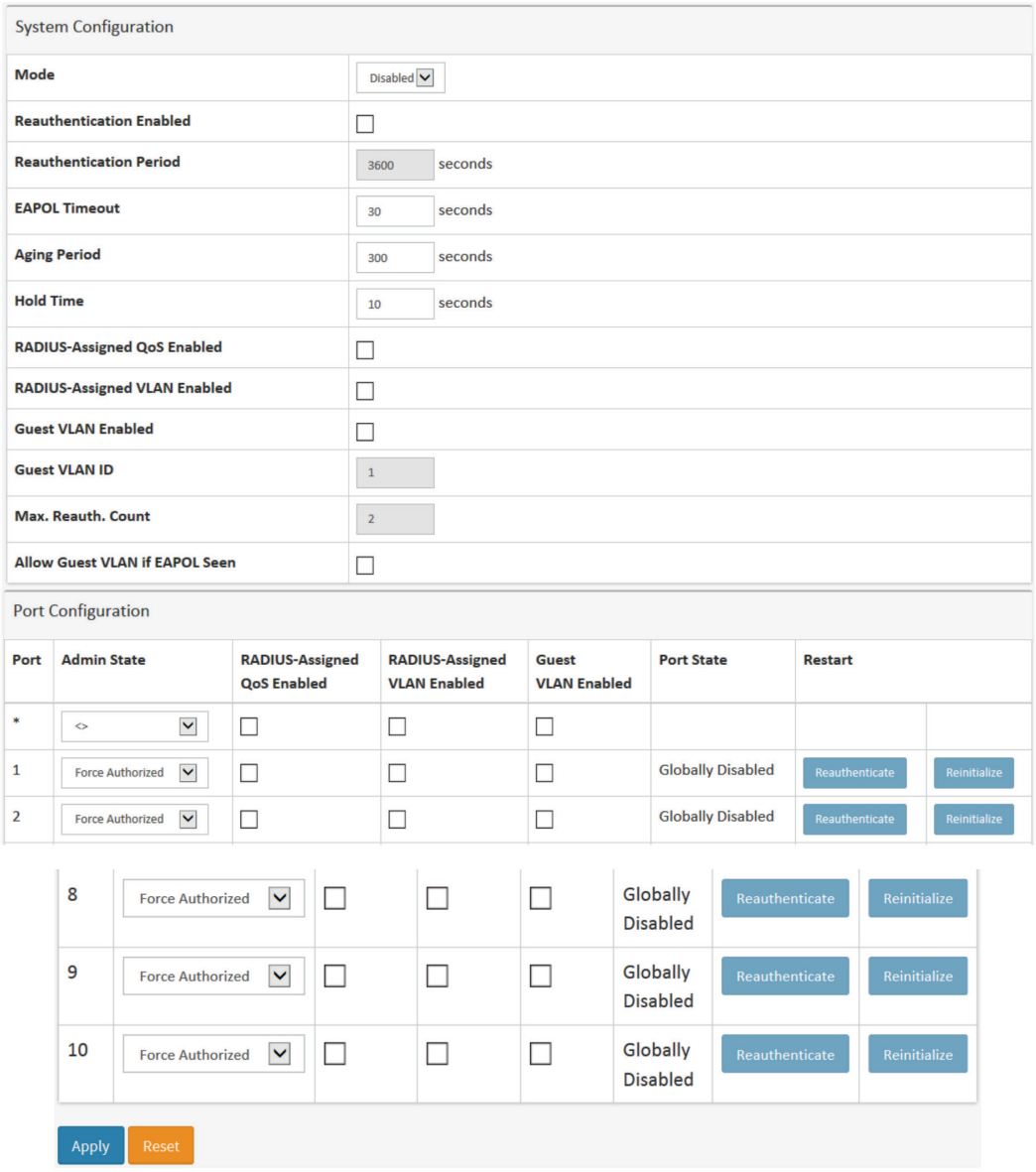



FIGURE 3-34. NETWORK ACCESS SERVER CONFIGURATION SCREEN

**Parameter description:**

- Mode: Indicates if NAS is globally enabled or disabled on the switch. If globally disabled, all ports are allowed to forward 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 range from 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 function 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 reauthentication, which will fail. But if reauthentication is not enabled, the only way to free resources is by aging the entries.

For ports in MAC-based Auth. mode, reauthentication doesn't cause direct communication between the switch and the client, so this will not detect whether the client is still attached or not, and the only way to free any resources is to age the entry.

- Hold Time: This setting applies to the following modes, i.e. modes using the Port Security functionality to secure MAC addresses:

- Single 802.1X

- Multi 802.1X

- MAC-Based Auth.

If a client is denied access—either because the RADIUS server denies the client access or because the RADIUS server request times out (according to the timeout specified on the "Configuration Security AAA" page)—the client is put on hold in the Unauthorized state. The hold timer does not count during an ongoing 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 port's ditto setting determines whether RADIUS-assigned QoS Class is enabled on that port. When unchecked, RADIUS-server assigned QoS Class is disabled on all ports.

- RADIUS-Assigned VLAN Enabled: RADIUS-assigned VLAN provides a means to centrally control the VLAN on which a successfully authenticated supplicant is placed on the switch. Incoming traffic will be classified to and switched on the RADIUS-assigned VLAN. The RADIUS server must be configured to transmit special RADIUS attributes to take advantage of this feature (see RADIUS-Assigned VLAN Enabled 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 port's ditto setting determines whether RADIUS-assigned VLAN is enabled on that port. When unchecked, RADIUS-server assigned VLAN is disabled on all ports.

- Guest VLAN Enabled: A Guest VLAN is a special VLAN —typically with limited network access—on which 802.1X-unaware clients are placed after a network administrator-defined timeout. The switch follows a set of rules for entering and leaving the Guest VLAN as listed below.

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

- Guest VLAN ID: This is the value that a port's Port VLAN ID is set to if a port is moved into the Guest VLAN. It is only changeable if the Guest VLAN option is globally enabled. Valid values are in the range [1; 4095].
- Max. Reauth. Count: The number of times the switch transmits an EAPOL Request Identity frame without response before considering entering the Guest VLAN is adjusted with this setting. The value can only be changed if the Guest VLAN option is globally enabled. Valid values are in the range [1; 255].
- Allow Guest VLAN if EAPOL Seen: The switch remembers if an EAPOL frame has been received on the port for the lifetime of the port. Once the switch considers whether to enter the Guest VLAN, it will first check if this option is enabled or disabled. If disabled (unchecked, default), the switch will only enter the Guest VLAN if an EAPOL frame has not been received on the port for the lifetime of the port. If enabled (checked), the switch will consider entering the Guest VLAN even if an EAPOL frame has been received on the port for the lifetime of the port. The value can only be changed if the Guest VLAN option is globally enabled.
- Port Configuration: The table has one row for each port on the selected switch and a number of columns.
- Port: The port number for which the configuration below applies.
- Admin State: If NAS is globally enabled, this selection controls the port's authentication mode. Several 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 back-end servers are enabled and that the server timeout is configured to X seconds (using the AAA configuration page), and suppose that the first server in the list is currently down (but not considered dead).

If the supplicant retransmits EAPOL Start frames at a rate faster than X seconds, then it will never get authenticated, because the switch will cancel ongoing back-end 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 back-end authentication server request from the switch. This scenario will loop forever. So, 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 piggyback 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 piggyback 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 immediately reverts to the original VLAN ID (which may be changed by the administrator in the meantime without affecting the RADIUS-assigned).

This option is only available for single-client modes, i.e.

- Port-based 802.1X
- Single 802.1X

For troubleshooting VLAN assignments, use the "Monitor VLANs VLAN Membership and VLAN Port" pages. These pages show which modules have (temporarily) overridden the current Port VLAN configuration.

RADIUS attributes used in identifying a VLAN ID:

RFC2868 and RFC3580 form the basis for the attributes used in identifying a VLAN ID in an Access-Accept packet. The following criteria are used:

- The Tunnel-Medium-Type, Tunnel-Type, and Tunnel-Private-Group-ID attributes must all be present at least once in the Access-Accept packet.
- The switch looks for the first set of these attributes that have the same Tag value and fulfill the following requirements (if Tag == 0 is used, the Tunnel-Private-Group-ID does not need to include a Tag):
  - Value of Tunnel-Medium-Type must be set to "IEEE-802" (ordinal 6).
  - Value of Tunnel-Type must be set to "VLAN" (ordinal 13).
  - Value of Tunnel-Private-Group-ID must be a string of ASCII chars in the range 0 – 9, which is interpreted as a decimal string representing the VLAN ID. Leading "0"s are discarded. The final value must be in the range [1; 4095].
- Guest VLAN Enabled: When Guest VLAN is both globally enabled and enabled (checked) for a given port, the switch considers moving the port into the Guest VLAN according to the rules outlined below.

This option is only available for EAPOL-based modes, i.e.:

- Port-based 802.1X
- Single 802.1X
- Multi 802.1X

For troubleshooting VLAN assignments, use the "Monitor—>VLAN—>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 meantime, the switch considers entering the Guest VLAN. The interval between transmission of EAPOL Request Identity frames is configured with EAPOL Timeout. If Allow Guest VLAN if EAPOL Seen is enabled, the port will now be placed in the Guest VLAN. If disabled, the switch will first check its history to see if an EAPOL frame has previously been received on the port (this history is cleared if the port link goes down or the port's Admin State is changed), and if not, the port will be placed in the Guest VLAN. Otherwise, it will not move to the Guest VLAN, but continue transmitting EAPOL Request Identity frames at the rate given by EAPOL Timeout.

Once in the Guest VLAN, the port is considered authenticated, and all attached clients on the port are allowed access on this VLAN. The switch will not transmit an EAPOL Success frame when entering the Guest VLAN.

While in the Guest VLAN, the switch monitors the link for EAPOL frames, and if one such frame is received, the switch immediately takes the port out of the Guest VLAN and starts authenticating the supplicant according to the port mode. If an EAPOL frame is received, the port will never be able to go back into the Guest VLAN if "Allow Guest VLAN if EAPOL Seen" is disabled.

- Port State: The current state of the port. It can be 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 in single-supplicant mode and the supplicant is authorized.

- Unauthorized: The port is in Force Unauthorized or a in single-supplicant mode and the supplicant is not successfully authorized by the RADIUS server.

- X Auth/Y Unauth: The port is in a multi-supplicant mode. Currently X clients are authorized and Y are unauthorized.

- Restart: Two buttons are available for each row. The buttons are only enabled when authentication is globally enabled and the port's Admin State is in an EAPOL-based or MAC-based mode.

Clicking these buttons will not cause settings changed on the page to take effect.

Reauthenticate: Schedules a reauthentication whenever the quiet-period of the port runs out (EAPOL-based authentication). For MAC-based authentication, reauthentication will be attempted immediately.

The button only affects successfully authenticated clients on the port and will not cause the clients to be temporarily unauthorized.

Reinitialize: Forces a reinitialization of the clients on the port and thereby a reauthentication immediately. The clients will transfer to the unauthorized state while the reauthentication is in progress.

- Buttons:

- Apply – Click to save changes.

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

• Upper right icon (Refresh): Click this icon to refresh the NAS Configuration manually.

### 3.5.2.3 ACL

The L2+ Managed 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, 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.

Ports

The section describes how to configure the ACL parameters (ACE) for 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, ACL, then Ports.

2. Scroll to the specific parameter value to select the correct value for port ACL setting.

3. Click save to save the setting.

4. If you want to cancel the setting, click the reset button. It will revert to previously saved values.

5. After you finish the configuration, then you can see the port Counter. Click refresh to update the counter or click Clear to clear the information.

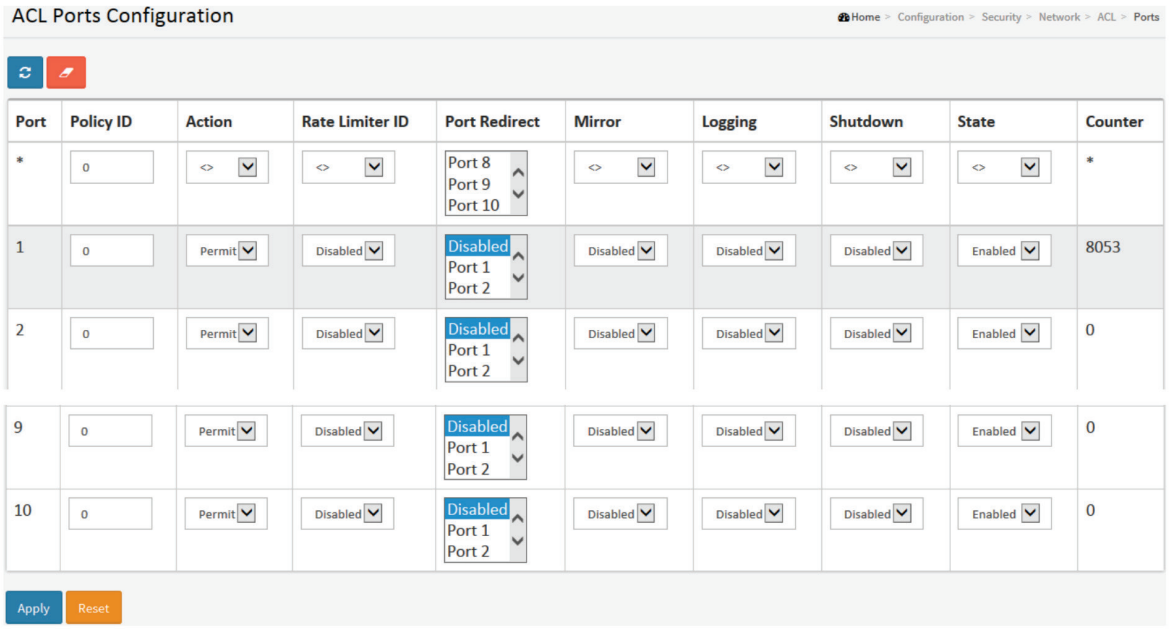



FIGURE 3-35. ACL PORTS CONFIGURATION SCREEN

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

- Enabled: Frames received on the port are mirrored.

- Disabled: Frames received on the port are not mirrored.

The default value is "Disabled."

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

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

- Disabled: Frames received on the port are not logged.

The default value is "Disabled."

**NOTE**: The System Log memory size and logging rate is limited.

- Shutdown: Specify the port shutdown operation. The allowed values are:

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

- Disabled: Port shutdown is disabled.

The default value is "Disabled."

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

- Enabled: Reopen ports by changing the volatile port configuration of the ACL user module.

- Disabled: Close ports by changing the volatile port configuration of the ACL user module.

The default value is "Enabled."

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

- Apply – Click to save changes.

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

- Upper right icon (Refresh, clear): Click on these icons to refresh the ACL Port Configuration or clear it manually.

## RATE LIMITERS

This section describes how to configure the switch's ACL Rate Limiter parameters. The Rate Limiter Level ranges from 1 to 16 pps or kbps.

## WEB INTERFACE

To configure ACL Rate Limiter in the web interface:

1. Click Configuration, ACL, then Rate Limiter.
2. Specify the Rate field and the range from 0 to 3276700.
3. Scroll the Unit with pps or kbps.
4. Click Apply to save the setting.
5. To cancel the setting, click the reset button. It will revert to previously saved values.

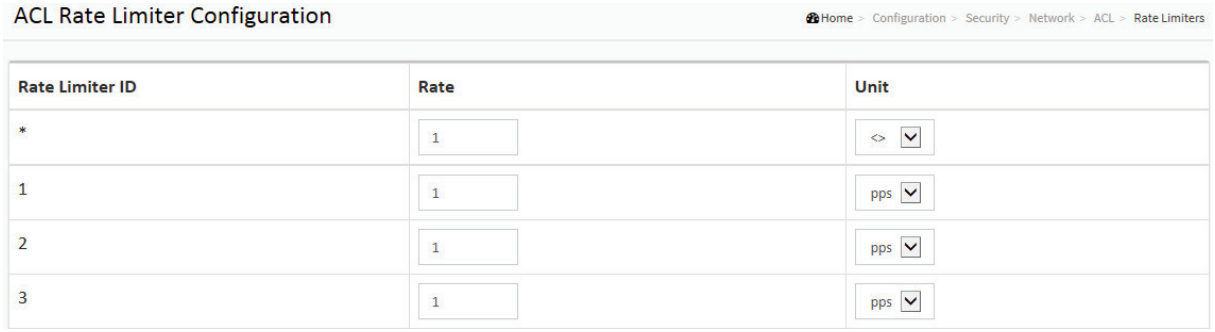



FIGURE 3-36. ACL RATE LIMITER CONFIGURATION SCREEN

Parameter description:

- Rate Limiter ID: The rate limiter ID for the settings contained in the same row.
- Rate: The allowed values are: 0–3276700 in pps or 0, 100, 200, 300, ..., 1000000 in kbps.
- Unit: Specify the rate unit. The allowed values are:

- pps: packets per second.

- kbps: Kbits per second.

- Buttons:

- Apply – Click to save changes.

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

## 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, and the order sequence cannot be changed when the priority is highest.

## WEB INTERFACE

To configure Access Control List in the web interface:

1. Click Configuration, ACL, then Configuration.

2. Click the "+" button to add a new ACL, or use the other ACL modification buttons to specify the editing action (i.e., edit, delete, or moving the relative position of entry in the list).

3. Specify the ACE parameter.

4. Click save to save the setting.

5. To cancel the setting, click the reset button. It will revert to previously saved values.

6. When editing an entry on the ACE Configuration page, note that the Items displayed depend on various selections, such as Frame Type and IP Protocol Type. Specify the relevant criteria to be matched for this rule, and set the actions to take when a rule is matched (such as Rate Limiter, Port Copy, Logging, and Shutdown).

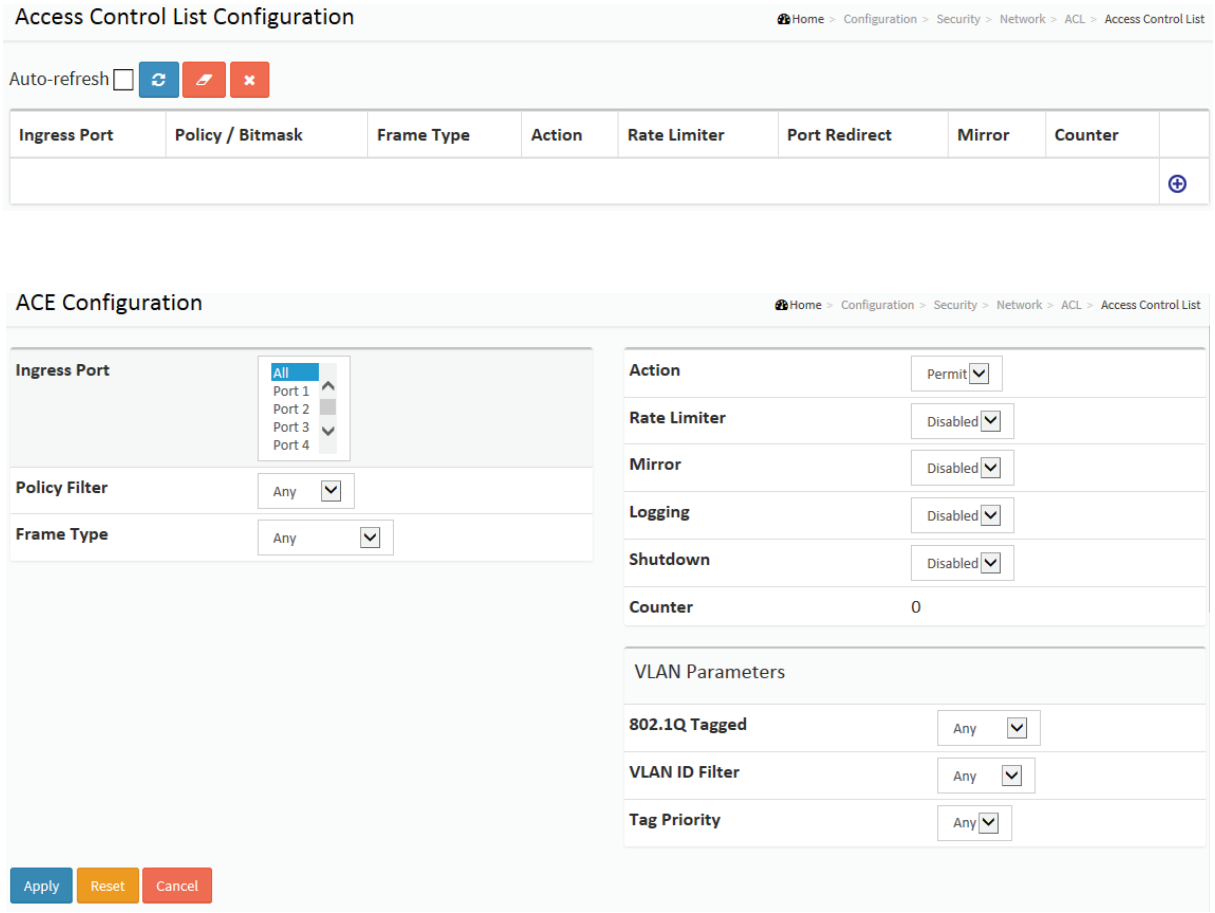



FIGURE 3-37. ACCESS CONTROL LIST CONFIGURATION SCREEN

**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**: 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 Copy: Indicates the port copy operation of the ACE. Frames matching the ACE are copied to the port number. The allowed values are Disabled or a specific port number. When Disabled is displayed, the port copy operation is disabled.
- Mirror: Specify the mirror operation of this port. The allowed values are:

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

- Logging: Indicates the logging operation of the ACE. Possible values are:

- Enabled: Frames matching the ACE are stored in the System Log.
- Disabled: Frames matching the ACE are not logged.

**NOTE**: The System Log memory size and logging rate is limited.

- Shutdown: Indicates the port shutdown operation of the ACE. Possible values are:

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

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

**Modification Buttons**

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

+ Inserts a new ACE before the current row.

o Edits the ACE row.

up-arrow Moves the ACE up the list.

down-arrow Moves the ACE down the list.

x Deletes the ACE.

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

**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.

- Buttons:

- Apply – Click to save changes.

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

- Auto-refresh: Select auto-refresh to refresh the information automatically.

- Upper right icon (Refresh, clear, Remove All): Click to refresh the ACL configuration or clear manually. Click remove all to clean up all ACL configurations on the table.

### 3.5.2.4 IP SOURCE GUARD

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

**Configuration**

This section describes how to configure IP Source Guard settings 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. Select "Enabled" in the IP Source Guard Configuration Mode.
2. Select "Enabled" for the specific port in the Port Mode Configuration.
3. Select Maximum Dynamic Clients (0, 1, 2, Unlimited) for the specific port in the Port Mode Configuration.
4. Click Apply.

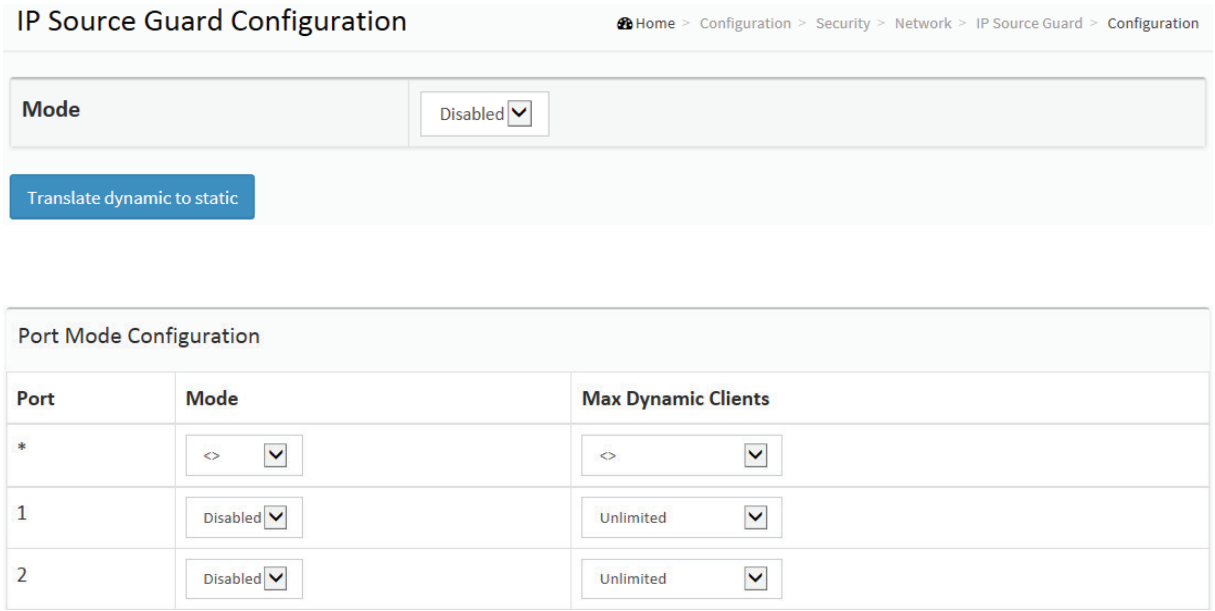



FIGURE 3-38. IP SOURCE GUARD CONFIGURATION SCREEN

**Parameter description:**

- IP Source Guard Configuration Mode: 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 as enabled on which ports. Only when both Global Mode and Port Mode on a given port are enabled will IP Source Guard be enabled on this given port.
- Max Dynamic Clients: Specify the maximum number of dynamic clients that can be learned on a given port. This value can be 0, 1, 2, or unlimited. If the port mode is enabled and the value of max dynamic client is equal to 0, only IP packets that match static entries on the specific port are forwarded.

## STATIC TABLE

The section describes how to configure the Static IP Source Guard Table switch parameters. Use the Static IP Source Guard Table to manage the entries.

## WEB INTERFACE

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

1. Click “Add new entry.”
2. Specify the Port, VLAN ID, IP Address, and MAC address in the entry.
3. Click Apply.

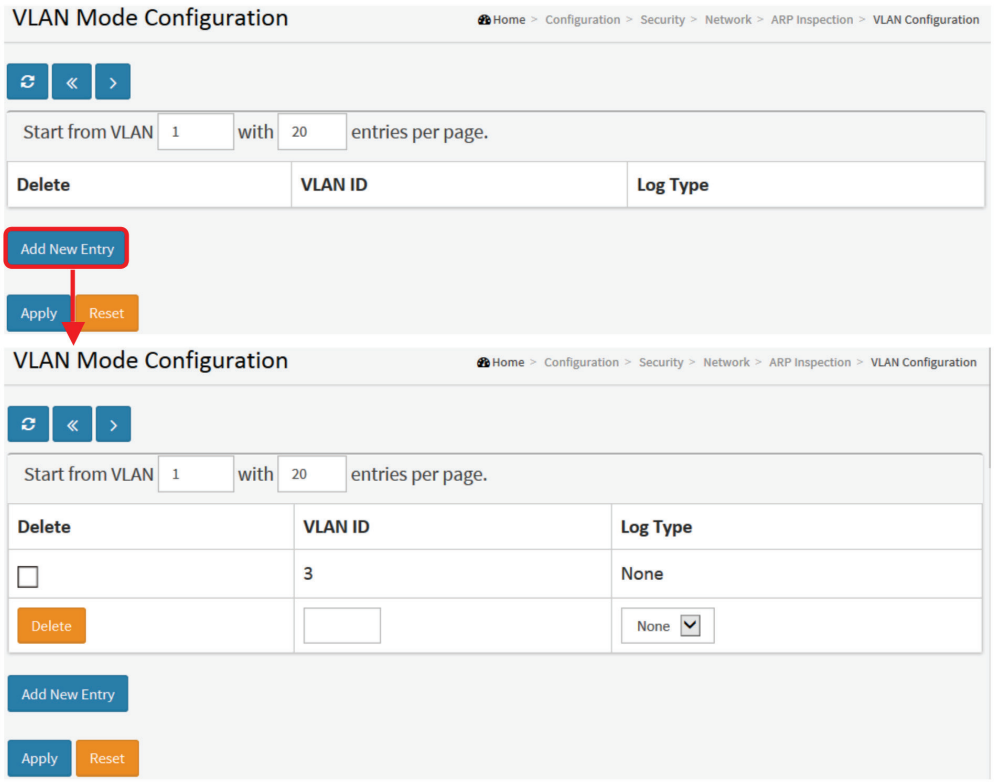



FIGURE 3-39. STATIC IP SOURCE GUARD TABLE SCREEN

**Parameter description:**

- Delete: Check to delete the entry. It will be deleted during the next save.
- Port: The logical port for the settings.
- VLAN ID: The vlan id for the settings.
- IP Address: Allowed Source IP address.
- MAC address: Allowed Source MAC address.
- Adding new entry: Click to add a new entry to the Static IP Source Guard table. Specify the Port, VLAN ID, IP address, and IP Mask for the new entry. Click “Save.”

- Buttons:

- Apply – Click to save changes.

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

### 3.5.2.5 ARP INSPECTION

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

### CONFIGURATION

This section describes how to configure ARP Inspection settings.

- Mode (Enabled and Disabled)
- Port (Enabled and Disabled)

### WEB INTERFACE

To configure an ARP Inspection Configuration in the web interface:

1. Select “Enabled” in the ARP Inspection Configuration Mode.
2. Select “Enabled” for the specific port in the Port Mode Configuration.
3. Click Apply.

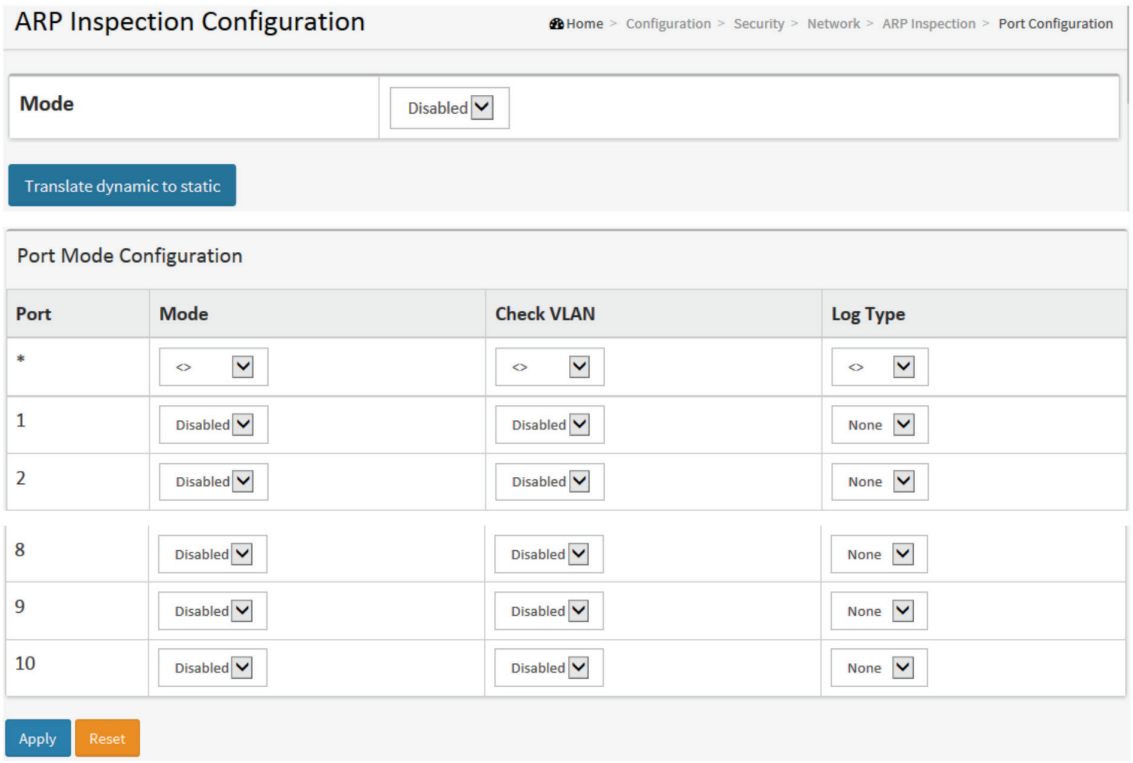



FIGURE 3-40. ARP INSPECTION CONFIGURATION SCREEN

**Parameter description:**

- ARP Inspection Configuration Mode: Enable the Global ARP Inspection or disable the Global ARP Inspection.
- Port Mode Configuration: Specify ARP Inspection as enabled on which ports. Only when both Global Mode and Port Mode on a given port are enabled, will ARP Inspection be 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 “Check VLAN” setting. 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. When the setting of “Check VLAN” is enabled, the log type of ARP Inspection will refer to the VLAN setting. Possible settings of “Check VLAN” are:

- Enabled: Enable check VLAN operation.

- Disabled: Disable check VLAN operation.

Only when the Global Mode and Port Mode on a given port are enabled and the setting of “Check VLAN” is disabled, will the log type of ARP Inspection refer to the port setting. There are four log types:

- None: Log nothing.

- Deny: Log denied entries.

- Permit: Log permitted entries.

- ALL: Log all entries.

- Buttons:

- Apply – Click to save changes.

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

## VLAN MODE CONFIGURATION

Each page shows up to 9999 entries (the default is 20) from the VLAN table 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 switch 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 “Add new entry.”
2. Specify the VLAN ID, Log Type.
3. Click Apply.

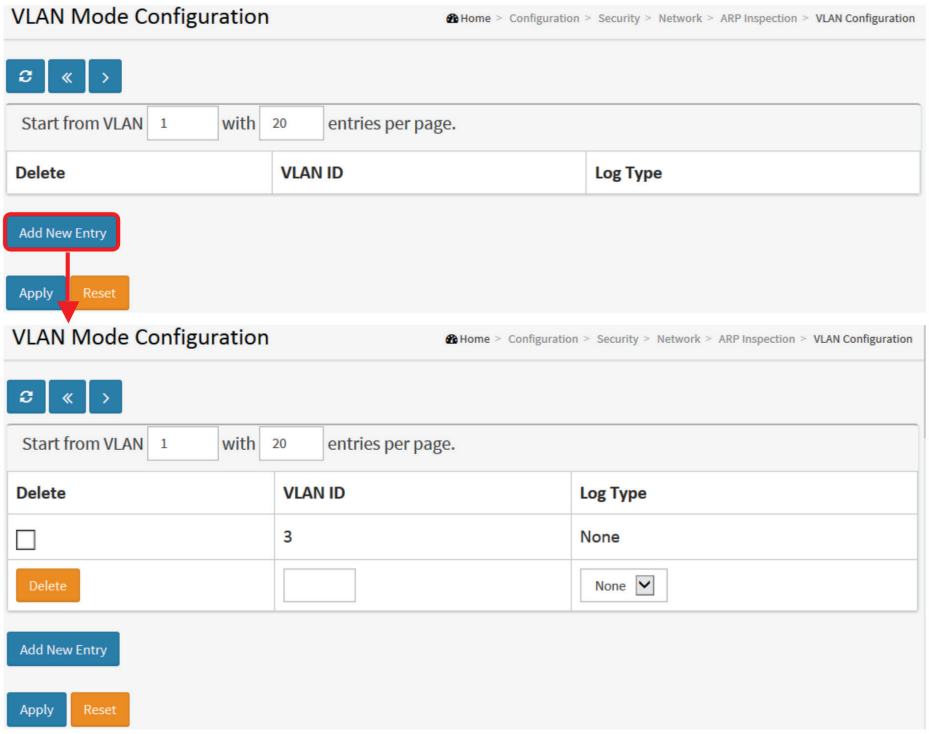



FIGURE 3-41. VLAN MODE CONFIGURATION SCREEN

Parameter description:

- VLAN Mode Configuration: Specify ARP Inspection as 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, will ARP Inspection be 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 a per VLAN setting. Possible types are:

- None: Log nothing.

- Deny: Log denied entries.

- Permit: Log permitted entries.

- ALL: Log all entries.

- Buttons:

- Add New Entry: Click to add a new VLAN to the ARP Inspection VLAN table.

- Apply: Click to save changes.

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

## STATIC TABLE

The section describes how to configure the Static ARP Inspection Table parameters of the switch. You can 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 “Add new entry.”
2. Specify the Port, VLAN ID, IP Address, and MAC address in the entry.
3. Click Apply.

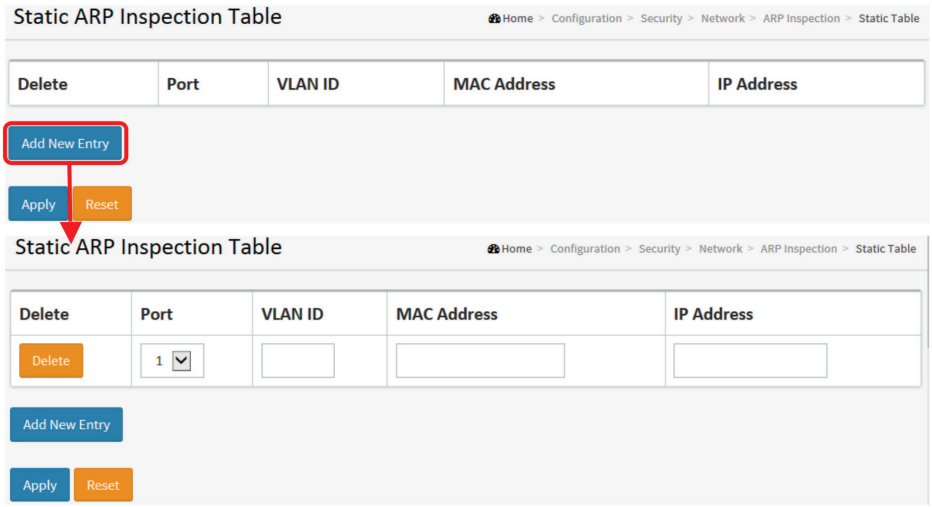



FIGURE 3-42. STATIC ARP INSPECTION TABLE

Parameter description:

- Delete: Check to delete the entry. It will be deleted during the next save.
- Port: The logical port for the settings.
- VLAN ID: The vlan id for the settings.
- MAC Address: The allowed Source MAC address in ARP request packets.
- IP Address: The allowed Source IP address in ARP request packets.
- Adding new entry: Click to add a new entry to the Static ARP Inspection table. Specify the Port, VLAN ID, MAC address, and IP address for the new entry. Click “Save.”
- Buttons:

- Apply – Click to save changes.

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

## 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 (the default is 20) from the Dynamic ARP Inspection table 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 switch 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

You can configure a Dynamic ARP Inspection Table Configuration in the web interface.

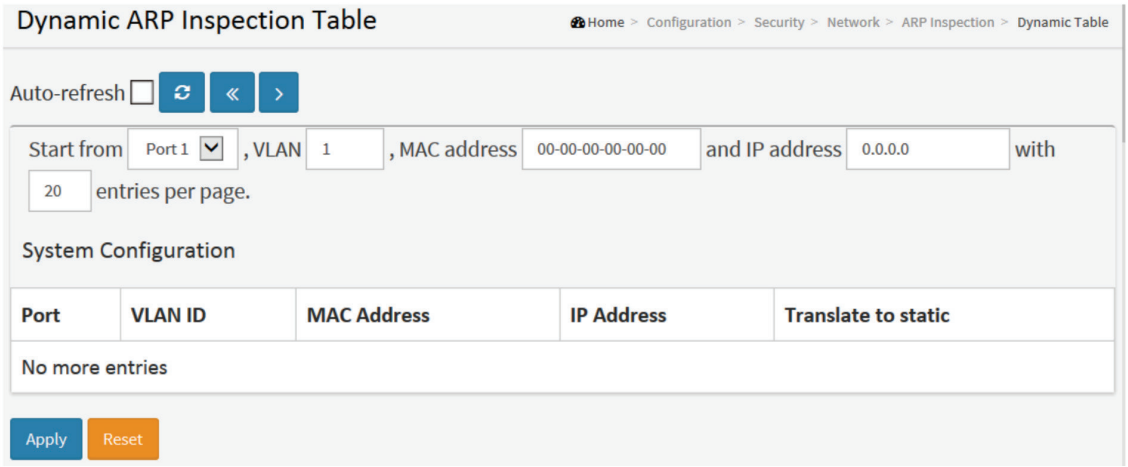



FIGURE 3-43. DYNAMIC ARP INSPECTION TABLE

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.
- 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.

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

<<: 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

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

### 3.5.3.1 RADIUS

**Web Interface**

You can configure a Common Configuration of AAA, RADIUS in the web interface.

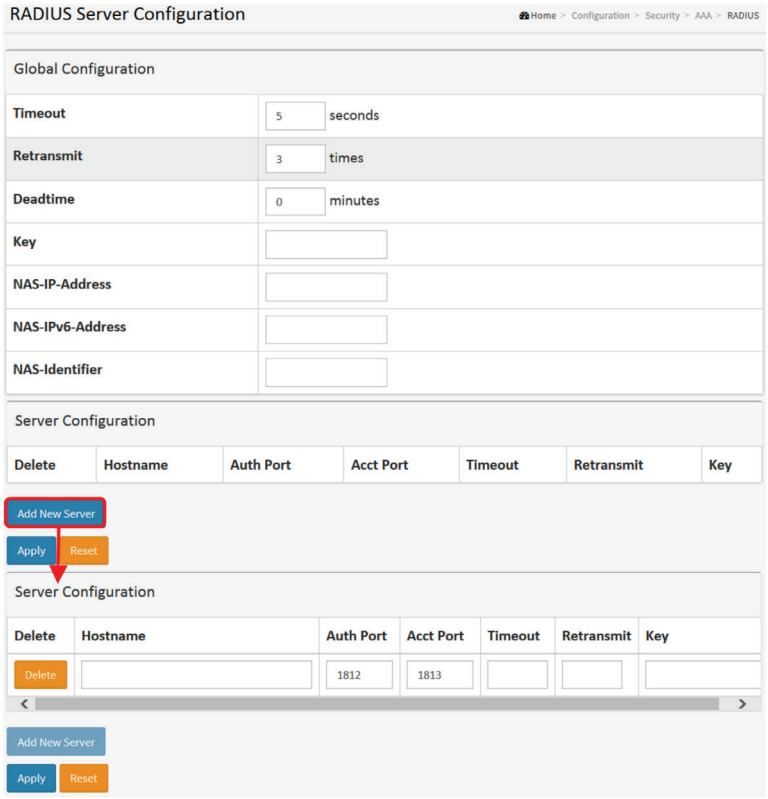



FIGURE 3-44. RADIUS AUTHENTICATION SERVER CONFIGURATION SCREEN

**Parameter description:**

**Global Configuration**

These settings 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.

- Delete: To delete a RADIUS server entry, check this box. The entry will be deleted during the next Save.
- Hostname: The IP address or hostname of the RADIUS server.
- Auth Port: The UDP port to use on the RADIUS server for authentication.
- Acct Port: The UDP port to use on the RADIUS server for accounting.
- Timeout: This optional setting overrides the global timeout value. Leaving it blank will use the global timeout value.
- Retransmit: This optional setting overrides the global retransmit value. Leaving it blank will use the global retransmit value.
- Key: This optional setting overrides the global key. Leaving it blank will use the global key.

Adding a 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.

- Buttons

- Apply: Click to save changes.

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

### 3.5.3.2 TACACS+

## WEB INTERFACE

You can configure a Common Configuration of AAA, TACACS+ in the web interface.

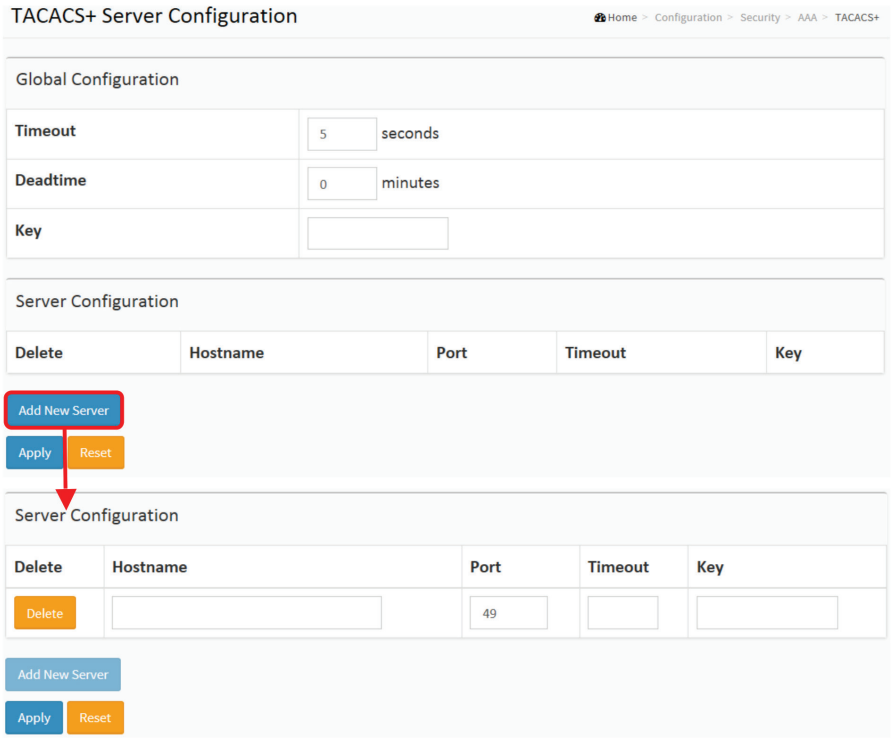



FIGURE 3-45. TACACS+ AUTHENTICATION SERVER CONFIGURATION SCREEN

**Parameter description:**

**Global Configuration**

These settings 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.

**Adding a 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.

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

- Buttons

- Apply: Click to save changes.

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

## 3.6 AGGREGATION

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

### 3.6.1 STATIC

Ports using Static Trunk as their trunk method can choose their unique Static GroupID to form a logical "trunked port." The benefit of using Static Trunk method is that a port can immediately become a member of a trunk group without any handshaking with its peer port. This is also a disadvantage because the peer ports of your static trunk group may not know that they should be aggregated together to form a "logical trunked port." Using Static Trunk on both ends of a link is strongly recommended.

NOTE: Low-speed links will stay in a "not ready" state when using static trunk to aggregate with high speed links.

#### WEB INTERFACE

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

1. Click Configuration, Aggregation, Static and then Aggregation Mode Configuration.

2. Enable or disable the aggregation mode function.

Evoke Aggregation Group ID and Port members.

3. Click save to save the setting.

4. To cancel the setting, click the reset button. It will revert to previously saved values.

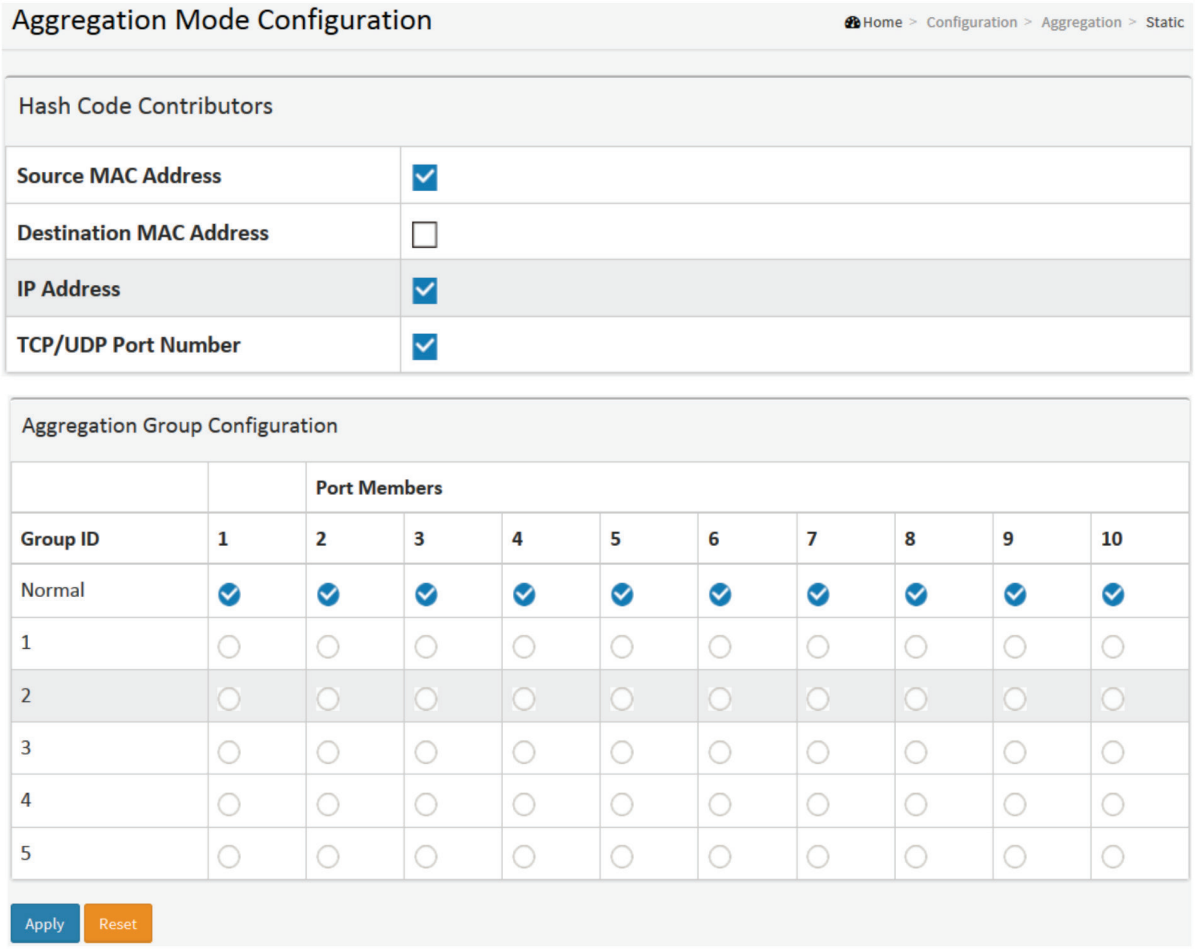



FIGURE 3-46. AGGREGATION MODE CONFIGURATION SCREEN

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

## 3.6.2 LACP

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

### WEB INTERFACE

To configure the Trunk Aggregation LACP parameters in the web interface:

1. Click Configuration, LACP, Configuration.
2. 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 save to save the setting.
6. To cancel the setting, click the reset button. It will revert to previously saved values.

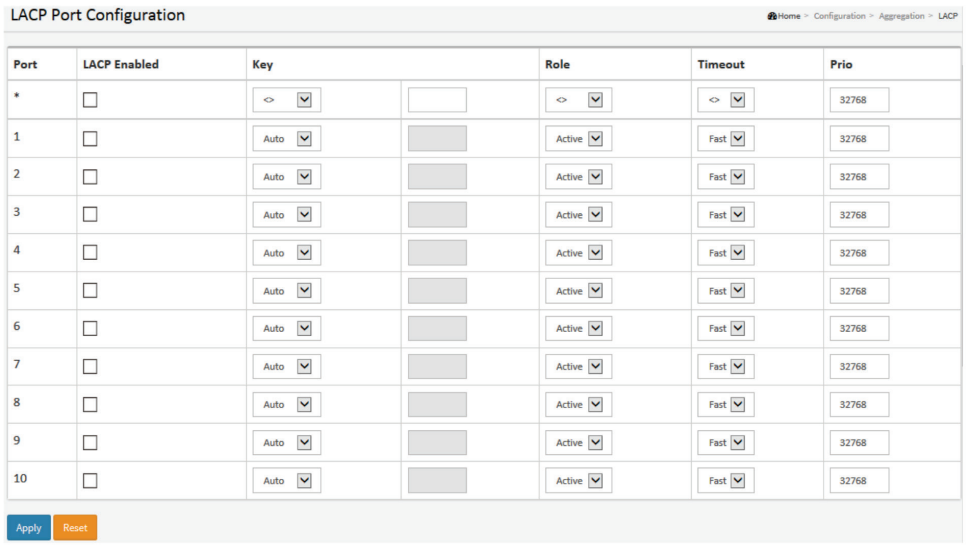



FIGURE 3-47. LACP PORT CONFIGURATION SCREEN

**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, you can enter a user-defined value. Ports with the same Key value can participate in the same aggregation group, while ports with different keys cannot.
- Role: The Role shows the LACP activity status. Active will transmit LACP packets each second, while Passive will wait for a LACP packet from a partner (speak if spoken to).
- Timeout: Timeout controls the period between BPDU transmissions. Fast will transmit LACP packets each second, while Slow will wait for 30 seconds before sending an LACP packet.
- Prio: 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. A 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.

## 3.7 LOOP PROTECTION

Loop Protection is used to detect the presence of traffic. When a switch receives a packet's (looping detection frame) MAC address the same as itself from a port, show Loop Protection happens. The port will be locked when it receives looping Protection frames. If you want to unlock the port, find out the looping path and remove the looping path, then select the locked port and click on "Resume" to turn on the locked port.

### WEB INTERFACE

To configure the Loop Protection parameters in the web interface:

1. Click Configuration, Loop Protection.
2. Enable or disable the port loop Protection.
3. Click save to save the setting.
4. To cancel the setting, click the Reset button. It will revert to previously saved values.

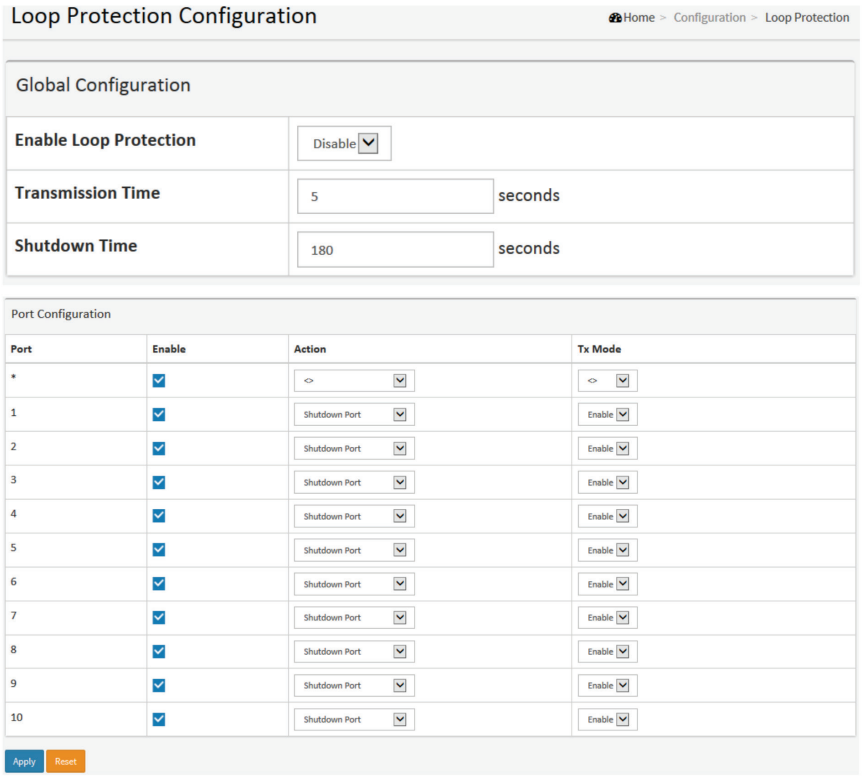



FIGURE 3-48. LOOP PROTECTION CONFIGURATION SCREEN

**Parameter description:**

- Enable Loop Protection: Controls whether loop protection is enabled (as a whole).
- Transmission Time: The interval between each loop protection PDU sent on each port. Valid values are 1 to 10 seconds.
- Shutdown Time: The period (in seconds) for which a port will be kept disabled if a loop is detected (and the port action shuts down the port). Valid values are 0 to 604800 seconds (7 days). A value of zero will keep a port disabled (until next device restart).
- Port No: The switch port number.
- 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 PDUs, or whether it is just passively looking for looped PDUs.
- Buttons:

- Apply – Click to save changes.

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

## 3.8 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 that 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) that 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 that 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.

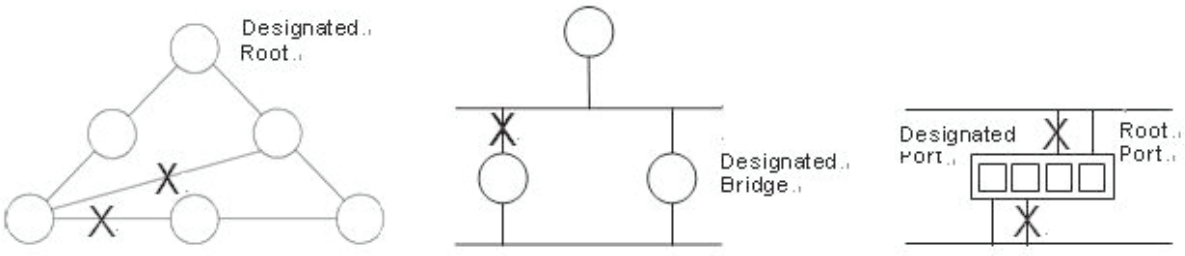



FIGURE 3-49. STP CONFIGURATION

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

## 3.8.1 BRIDGE SETTING

The section describes how to configure the Spanning Tree Bridge and STP System settings. It allows you to configure STP System settings 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. Enable or disable the parameters and write down the available value of parameters in the blank field in Advanced settings.
4. Click apply to save the setting.
5. To cancel the setting, click the Reset button. It will revert to previously saved values.

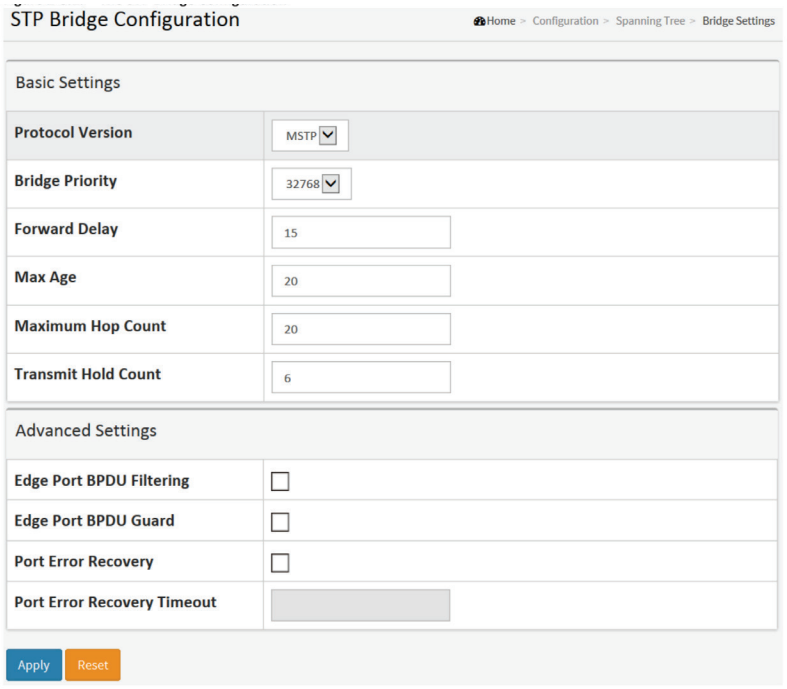



FIGURE 3-50. STP BRIDGE CONFIGURATION SCREEN

**Parameter description:**

**Basic Settings**

- Protocol Version: The STP protocol version setting. Valid values are STP, RSTP, and MSTP.
- Bridge Priority: Controls the bridge priority. Lower numeric values have better priority. The bridge priority plus the MSTI instance number, concatenated with the 6-byte MAC address of the switch forms a Bridge Identifier. For MSTP operation, this is the priority of the CIST. Otherwise, this is the priority of the STP/RSTP bridge.
- Forward Delay: The delay used by STP Bridges to transit Root and Designated Ports to Forwarding (used in STP compatible mode). Valid values are in the range 4 to 30 seconds.

- Max Age: The maximum age of the information transmitted by the Bridge when it is the Root Bridge. Valid values are in the range 6 to 40 seconds, and MaxAge must be <= (FwdDelay-1)*2.
- Maximum Hop Count: This defines the initial value of remaining Hops for MSTI information generated at the boundary of an MSTI region. It defines how many bridges a root bridge can distribute its BPDU information to. Valid values are in the range 6 to 40 hops.
- Transmit Hold Count: The number of BPDU's a bridge port can send per second. When exceeded, transmission of the next BPDU will be delayed. Valid values are in the range 1 to 10 BPDUs 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 when it receives 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.

## 3.8.2 MSTI MAPPING

When you implement a Spanning Tree protocol on the switch as 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 save to save the setting.
4. To cancel the setting, click the Reset button. It will revert to previously saved values.

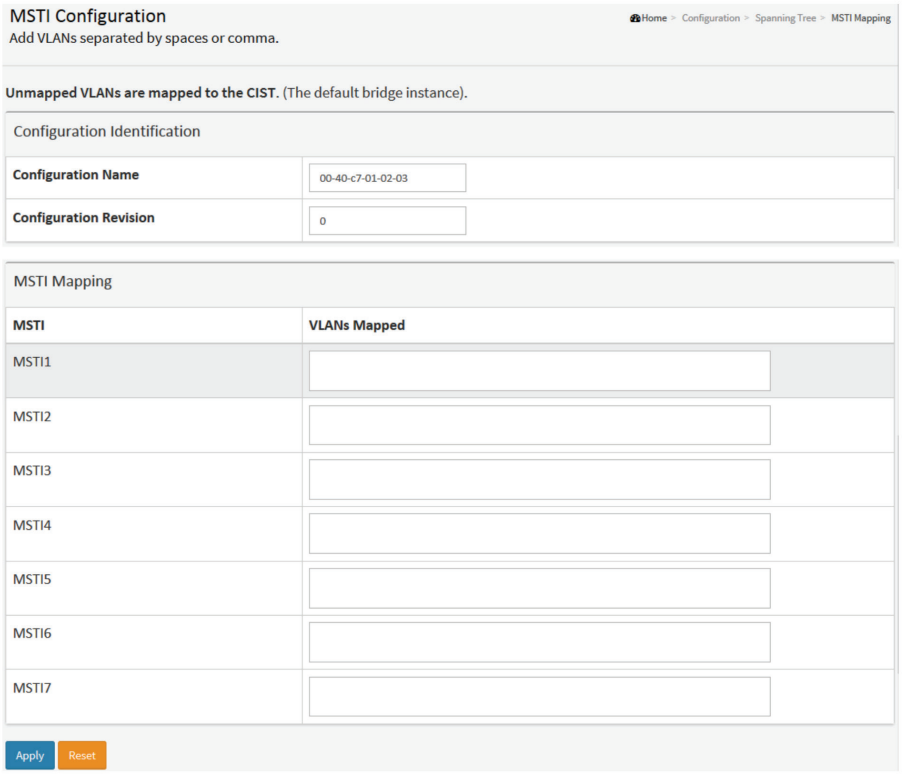



FIGURE 3-51. MSTI CONFIGURATION SCREEN

**Parameter description:**

**Configuration Identification**

- Configuration Name: The name identifying the VLAN to MSTI mapping. Bridges must share the name and revision, as well as the VLAN-to-MSTI mapping configuration in order to share spanning trees for MSTIs (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: The bridge instance. The CIST is not available for explicit mapping, because it will receive the VLANs not explicitly mapped.
- VLANs Mapped: The list of VLANs mapped to the MSTI. The VLANs can be given as a single (xx, xx is 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.

## 3.8.3 MSTI PRIORITIES

When you implement a Spanning Tree protocol on the switch as a bridge instance, the CIST is the default instance which is always active. It 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 how 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 to the Priority; the maximum is 240. The default is 128.
3. Click save to save the setting.
4. To cancel the setting, click the Reset button. It will revert to previously saved values.

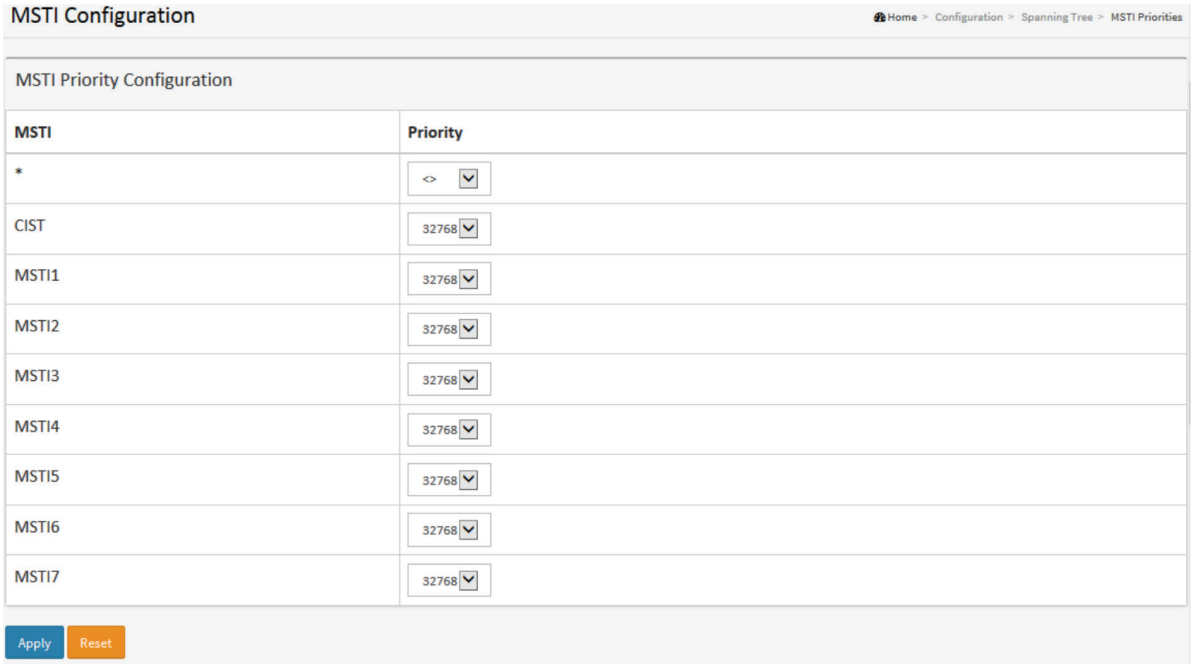



FIGURE 3-52. MSTI CONFIGURATION SCREEN

**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.

## 3.8.4 CIST PORTS

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

### WEB INTERFACE

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

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

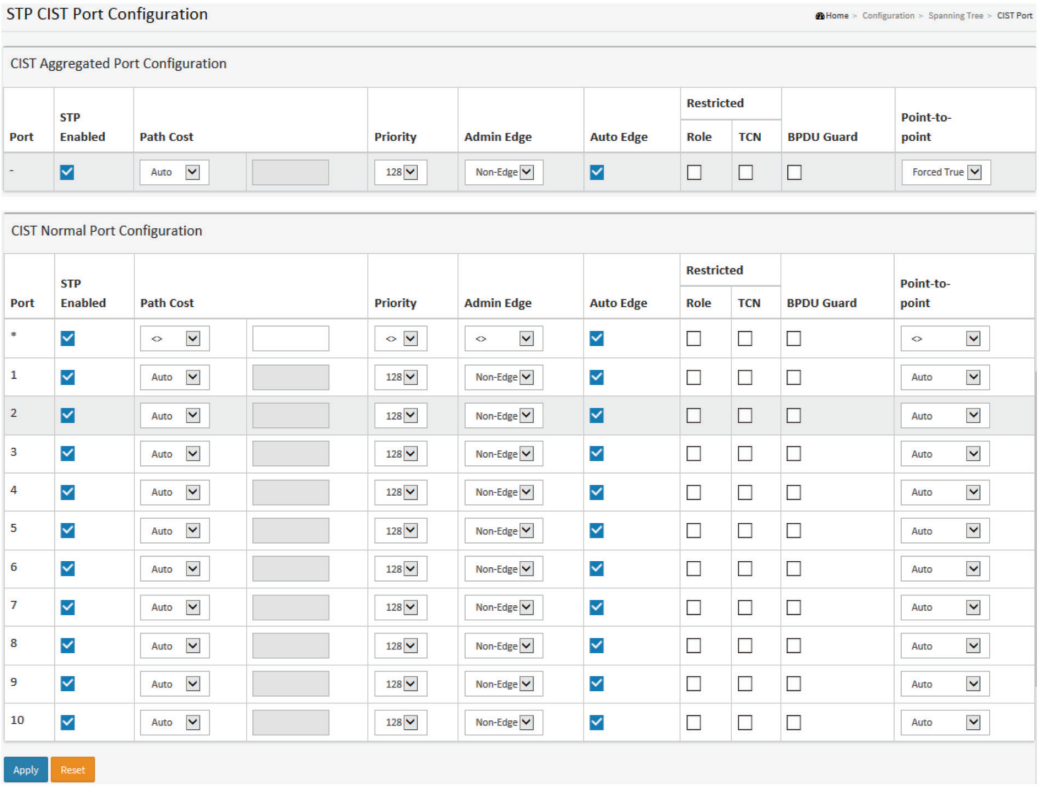



FIGURE 3-53. STP CIST PORT CONFIGURATION SCREEN

**Parameter description:**

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

- Priority: Controls the port priority. This can be used to control priority of ports that have identical port cost.
- 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 (when operEdge is 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. (This is 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 BPDUs are received on the port or not.
- Restricted Role: If enabled, this causes the port not to be selected as the Root Port for the CIST or any MSTI, even if it has the best spanning tree priority vector. Such a port will be selected as an Alternate Port after the Root Port has been selected. If set, it can cause lack of spanning tree connectivity. It can be set by a network administrator to prevent bridges external to a core region of the network influencing the spanning tree active topology, possibly because those bridges are not under the full control of the administrator. This feature is also known as Root Guard.
- Restricted TCN: If enabled, causes the port not to propagate received topology change notifications and topology changes to other ports. If set it can cause temporary loss of connectivity after changes in a spanning 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, this causes the port to disable itself when it receives valid BPDUs. Contrary to the similar bridge setting, the port Edge status does not affect this setting. A port entering error-disabled state caused by 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.

## 3.8.5 MSTI PORTS

The section describes how 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 detailed parameters of the MSTI Ports.
4. Scroll to set all parameters of the MSTI Port configuration.
5. Click save to save the setting.
6. To cancel the setting, click the Reset button. It will revert to previously saved values.

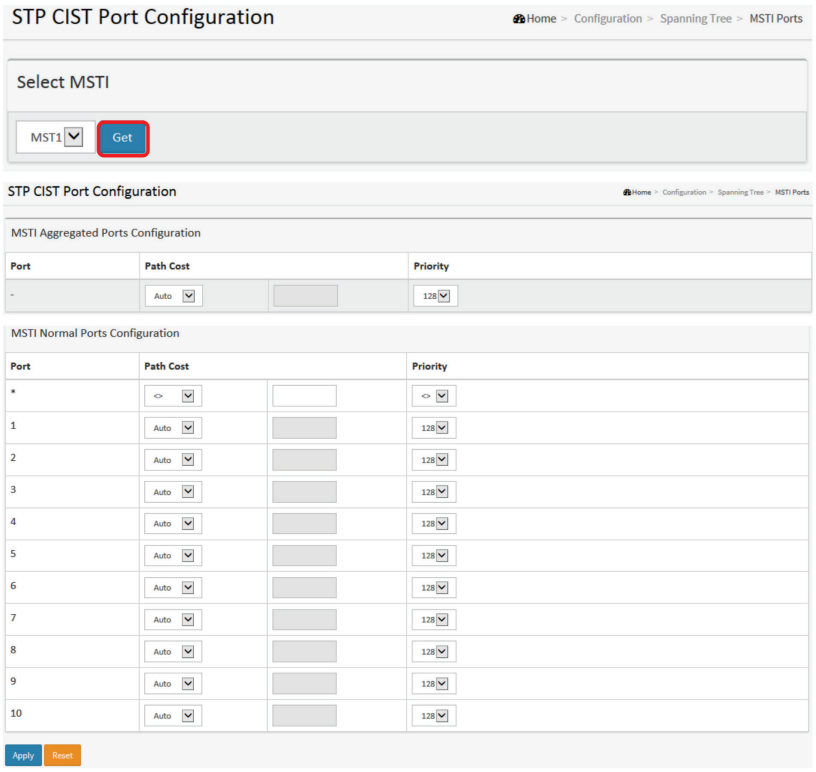



FIGURE 3-54. MSTI PORT CONFIGURATION SCREEN

**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 range from 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.

## 3.9 IPMC PROFILE

This page provides IPMC Profile related configurations.

### 3.9.1 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 of 128 corresponding rules for each.

#### WEB INTERFACE

To configure the IPMC Profile Configuration in the web interface, refer to the next figure.

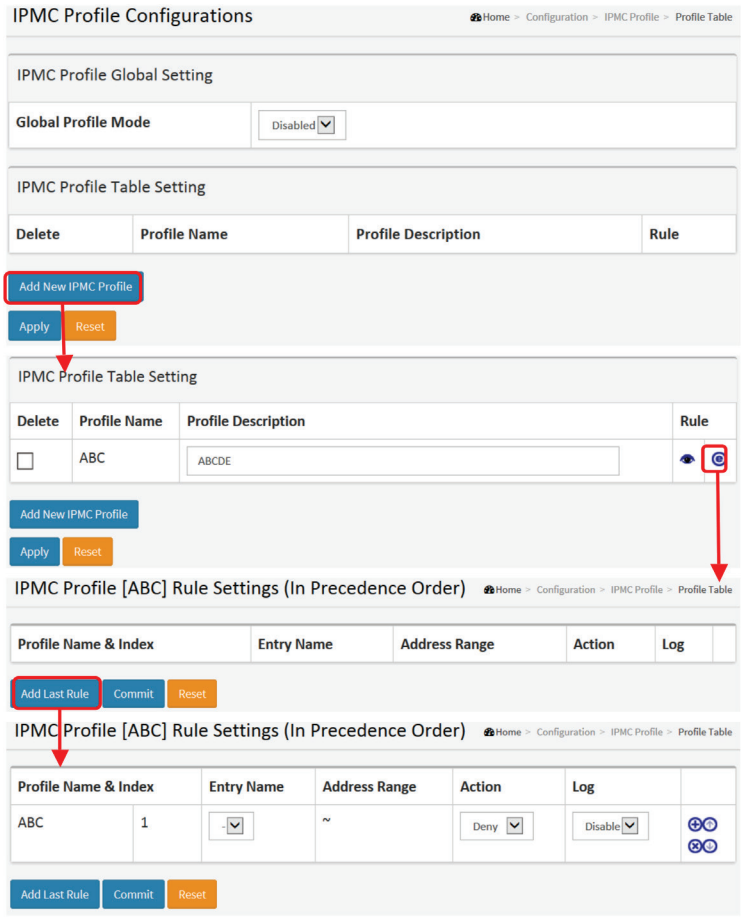



FIGURE 3-55. IPMC PROFILE CONFIGURATION SCREEN

**Parameter description:**

- Port: The switch port number of the corresponding STP CIST (and MSTI) port.
- Global Profile Mode: Enable/Disable the Global IPMC Profile. The 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 composed of at maximum 16 alphabetic and numeric characters. At least one alphabetic character must be present.
- Profile Description: Additional description about the profile, which is composed of at maximum 64 alphabetic and numeric characters. No blank or space characters are permitted as part of the description. Use "_" or "-" to separate the description sentence.
- Rule: When you create the profile, click the edit button to enter the rule setting page for the designated profile. Click the View button to show a summary about the designated profile. You can manage or inspect the rules of the designated profile by using the following buttons:

- eye button: List the rules associated with the designated profile.

- circle e button: Adjust the rules associated with the designated profile.

- Buttons

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

- Apply – Click to save changes.

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

### 3.9.1.1 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 to specify 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 that matches the range specified in the rule will be learned.

- Deny: Group address that 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.

- 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.

x: Delete the current entry of rule.

up-arrow: Moves the current entry of rule up in the list.

down-arrow: Moves the current entry of rule down in the list.

• 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.

## 3.9.2 ADDRESS ENTRY

This page provides address range settings used in the IPMC profile.

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

### WEB INTERFACE

You can configure the IPMC Profile Address Configuration in the web interface.

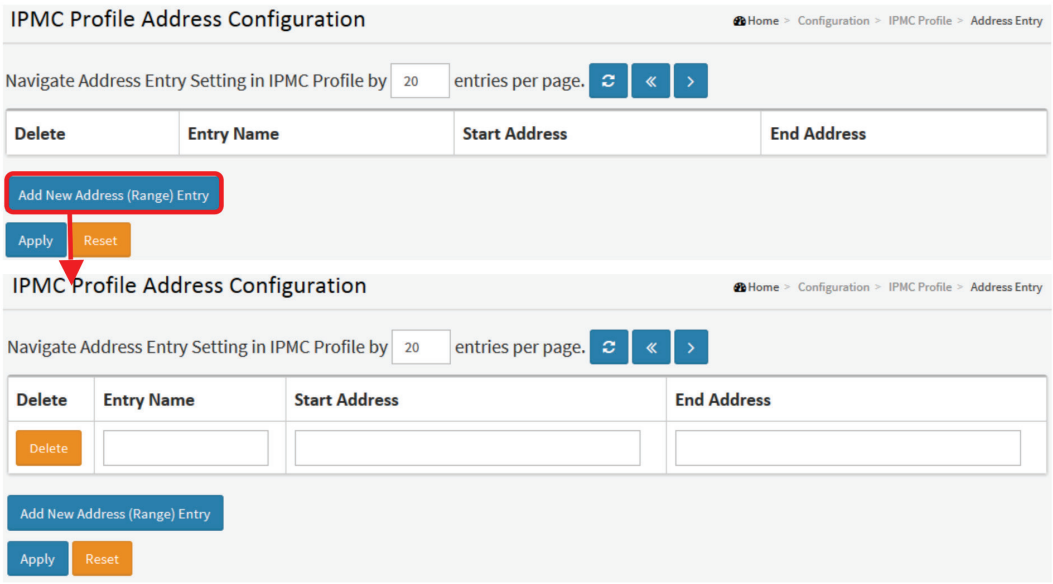



FIGURE 3-56. IPMC PROFILE ADDRESS CONFIGURATION SCREEN

**Parameter description:**

- Delete: Check to delete the entry. The designated entry will be deleted during the next save.
- Entry Name: The name used for indexing the address entry table. Each entry has a unique name composed of at maximum 16 alphabetic and numeric characters. At least one alphabetic character must be present.
- Start Address: The starting IPv4/IPv6 Multicast Group Address that will be used as an address range.
- End Address: The ending IPv4/IPv6 Multicast Group Address that will be used as an address range.
- Buttons:

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

- 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.

<< – 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.

## 3.10 MVR

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

### WEB INTERFACE

To configure the MVR Configuration in the web interface:

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

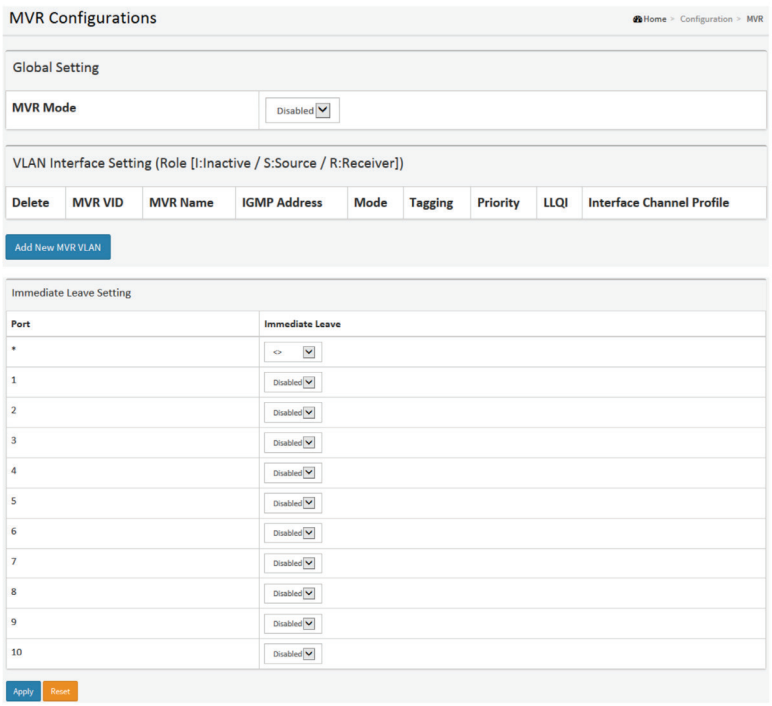



FIGURE 3-57. MVR CONFIGURATION SCREEN

**Parameter description:**

- MVR Mode Enable/Disable the Global MVR. Unregistered Flooding control depends on the current configuration in IGMP/MLD Snooping. We suggest enabling Unregistered Flooding control when the MVR group table is full.
- Delete: Check to delete the entry. The designated entry will be deleted during the next save.
- MVR VID: Specify the Multicast VLAN ID.

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 alphabetic character. 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 a 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, the system uses the IPv4 management address of the IP interface associated with this VLAN.

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

Otherwise, the system uses a predefined 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 a 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 beside the Edit symbol.
- 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 in 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.

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.

## 3.11 IPMC

ICMP is an acronym for Internet Control Message Protocol. It is a protocol that generates the error response for diagnostic or routing purposes. ICMP messages generally contain information about routing difficulties or simple exchanges such as time-stamp or echo transactions.

### 3.11.1 IGMP SNOOPING

The function is used to establish multicast groups to forward multicast packets to the member ports. It prevents wasting bandwidth when IP multicast packets are running over the network. This is because a switch that does not support IGMP or IGMP Snooping cannot tell a multicast packet from a broadcast packet, so it can only treat them all as the broadcast packets. Without IGMP Snooping, a multicast packet is forwarded in the same way as a broadcast packet.

The switch supports IGMP Snooping with query, report and leave functions. This enables a type of packet exchanged between an IP Multicast Router/Switch and an IP Multicast Host to be updated in the Multicast table information 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 IGMP Snooping if the user transmits multicast packets to the multicast group that was not built up in advance. IGMP mode enables the switch to issue an IGMP function to enable IGMP proxy or snooping on the switch, which connects to a router closer to the root of the tree. This interface is the upstream interface. The router on the upstream interface should be running IGMP.

#### 3.11.1.1 BASIC CONFIGURATION

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

#### WEB INTERFACE

To configure the IGMP Snooping parameters in the web interface:

1. Click Configuration, IPMC, IGMP Snooping, Basic Configuration.
2. Select enable or disable Global configuration.
3. Select a port to become a Router Port or enable/ disable the Fast Leave function.
4. Scroll to set the Throttling parameter.
5. Click apply to save the setting.
6. To cancel the setting, click the Reset button. It will revert to previously saved values.

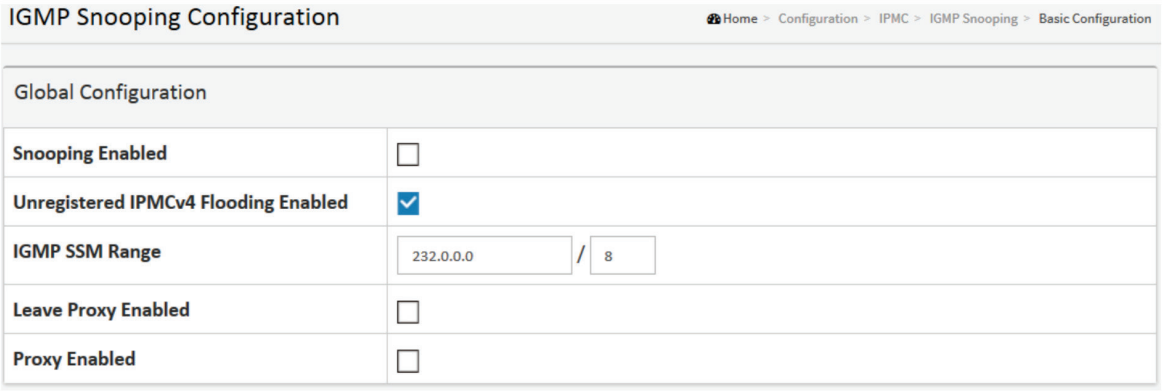



FIGURE 3-58. IGMP SNOOPING CONFIGURATION SCREEN

**Parameter description:**

- Snooping Enabled: Enable the Global IGMP Snooping.
- Unregistered IPMCv4 Flooding enabled: Enable unregistered IPMCv4 traffic flooding.
- IGMP SSM Range: SSM (Source-Specific Multicast) Range allows the SSM-aware hosts and routers to run the SSM service model for the groups in the address range. Format: (IP address/ sub mask)
- Leave Proxy Enable: 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.
- Port: This shows the physical Port index of the switch.
- Router Port: Specify which ports act as router ports. A router port is a port on the Ethernet switch that leads towards the Layer 3 multicast device or IGMP querier.

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

- Fast Leave: Enable fast leave on the port.
- Throttling: Enable to limit the number of multicast groups to which a switch port can belong.

### 3.11.1.2 VLAN CONFIGURATION

This section describes the VLAN configuration setting process integrated with the IGMP Snooping function. Each setting page shows up to 99 entries from the VLAN table, default is 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 entry 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, VLAN Configuration.
2. Enable or disable Snooping , IGMP Querier. Specify the parameters in the blank field.
3. Click refresh to update the data or click << or >> to display the previous entry or next entry.

4. Click save to save the setting.
5. To cancel the setting, click the Reset button. It will revert to previously saved values.

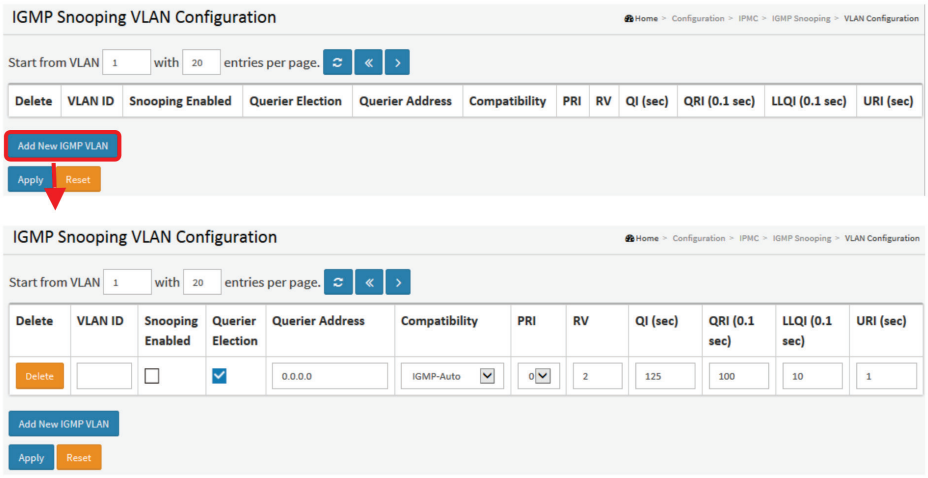



FIGURE 3-59. IGMP SNOOPING VLAN CONFIGURATION SCREEN

Parameter description:

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

- VLAN ID: 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 the IGMP Querier election in the VLAN. Disable to act as an IGMP Non-Querier.
- Querier Address: Define the IPv4 address as the source address used in the IP header for IGMP Querier election.

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

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

Otherwise, the 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, and the default compatibility value is IGMP-Auto.
- PRI: Priority of Interface. This 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.

• Upper right icon (Refresh, |<<, >>): Click to refresh the displayed table starting from the "VLAN" input fields. Or click "|<<" to update the table starting from the first entry in the VLAN table, i.e. the entry with the lowest VLAN ID. Click ">> " to update the table, starting with the entry after the last entry currently displayed.

### 3.11.1.3 PORT FILTERING PROFILE

The section describes how to set the IGMP Port Group Filtering. With the IGMP filtering feature, an user can exert this type of control. In some network Application environments, such as 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. This 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 Group Configuration in the web interface:

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

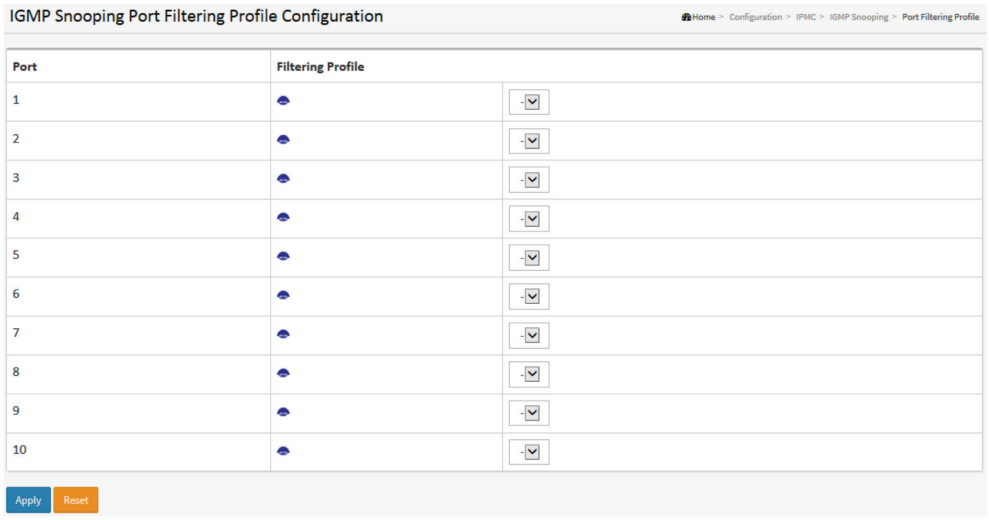



FIGURE 3-60. IGMP SNOOPING PORT GROUP FILTERING PROFILE SCREEN

**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 eye button. It lists 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.

## 3.11.2 MLD SNOOPING

A network node that acts as a source of IPv6 multicast traffic is only an indirect participant in MLD snooping—it just provides multicast traffic, and MLD doesn't interact with it.

**NOTE**: In an application such as 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**: 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.

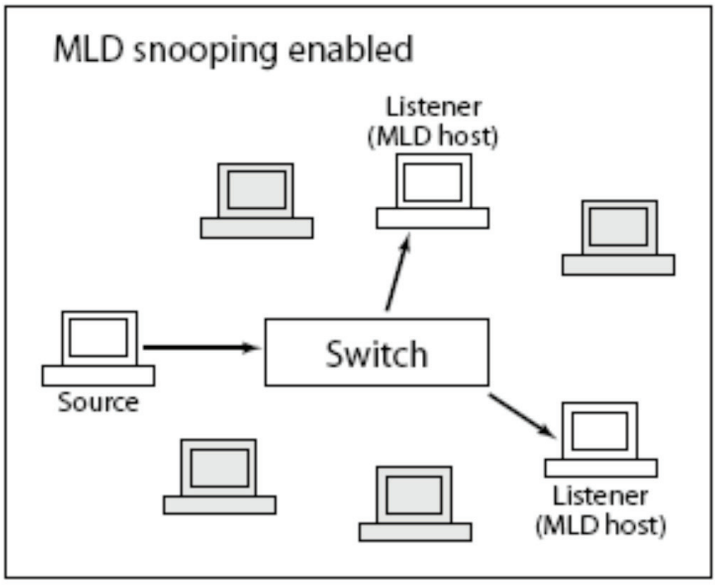



FIGURE 3-61. MLD SNOOPING ENABLED

### 3.11.2.1 BASIC CONFIGURATION

The section explains 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, MLD Snooping, Basic Configuration.
2. Enable or disable the Global configuration parameters. Select the port to join Router port and Fast Leave.
3. Scroll to select the Throttling mode as unlimited or 1 to 10.
4. Click save to save the setting.
5. To cancel the setting, click the Reset button. It will revert to previously saved values.

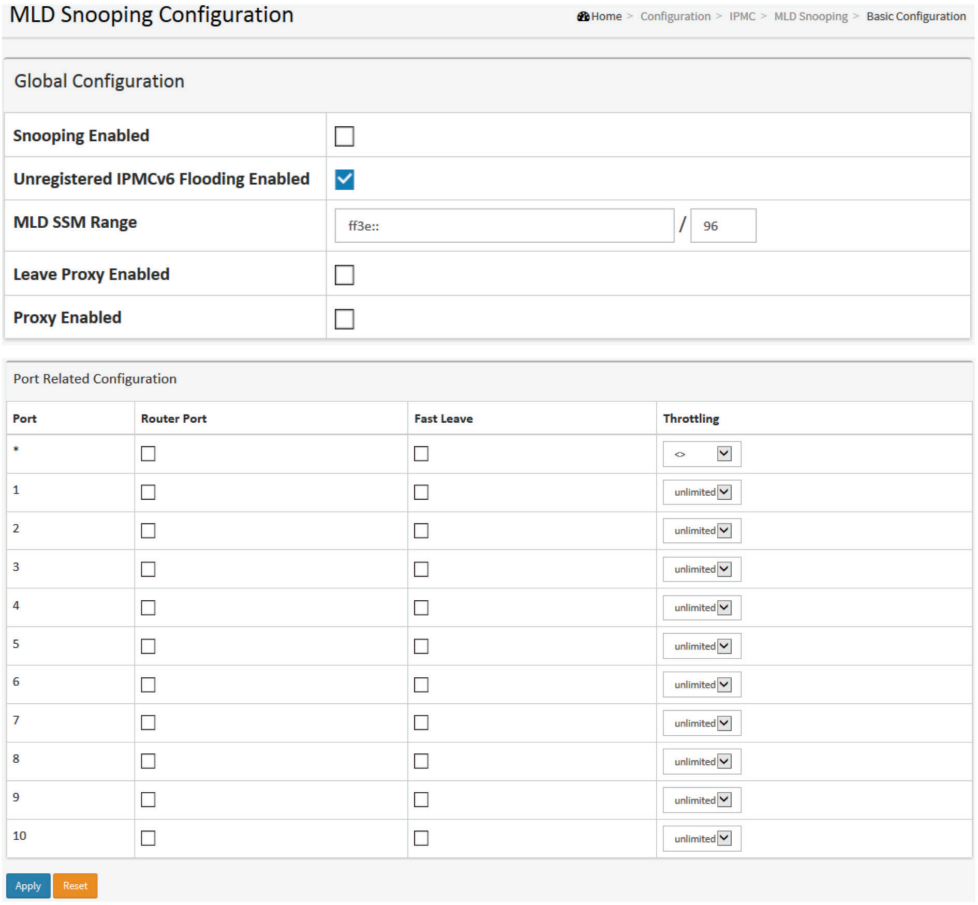



FIGURE 3-62. MLD SNOOPING BASIC CONFIGURATION SCREEN

**Parameter description:**

- Snooping Enabled: Enable 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 to 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: 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.

### 3.11.2.2 VLAN CONFIGURATION

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

The switch 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, 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 the previous or next entry.

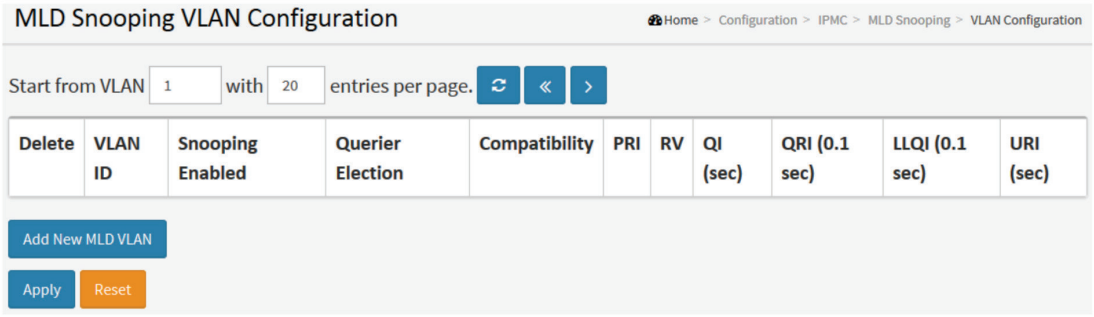



FIGURE 3-63. MLD SNOOPING VLAN CONFIGURATION SCREEN

**Parameter description:**

- Delete: Check to delete the entry. The designated entry will be deleted during the next save.
- VLAN ID: 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 the source address used in IP header for IGMP Querier election.

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

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

Otherwise, the 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. This 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.

- Upper right icon (Refresh, |<<, >>): Click to Refresh the displayed table starting from the "VLAN" input fields. Or click "|<<" to update the table starting from the first entry in the VLAN table, i.e. the entry with the lowest VLAN ID. Click ">> " to update the table, starting with the entry after the last entry currently displayed.

### 3.11.2.3 PORT GROUP FILTERING

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

### WEB INTERFACE

To configure the MLD Snooping Port Group Configuration in the web interface:

1. Click Configuration, IPMC, MLD Snooping, Port Group Filtering Configuration.
2. Click Add new Filtering Group.
3. Specify the Filtering Groups with entries per page.
4. Click Apply to save the setting.
5. To cancel the setting, click the Reset button. It will revert to previously saved values.

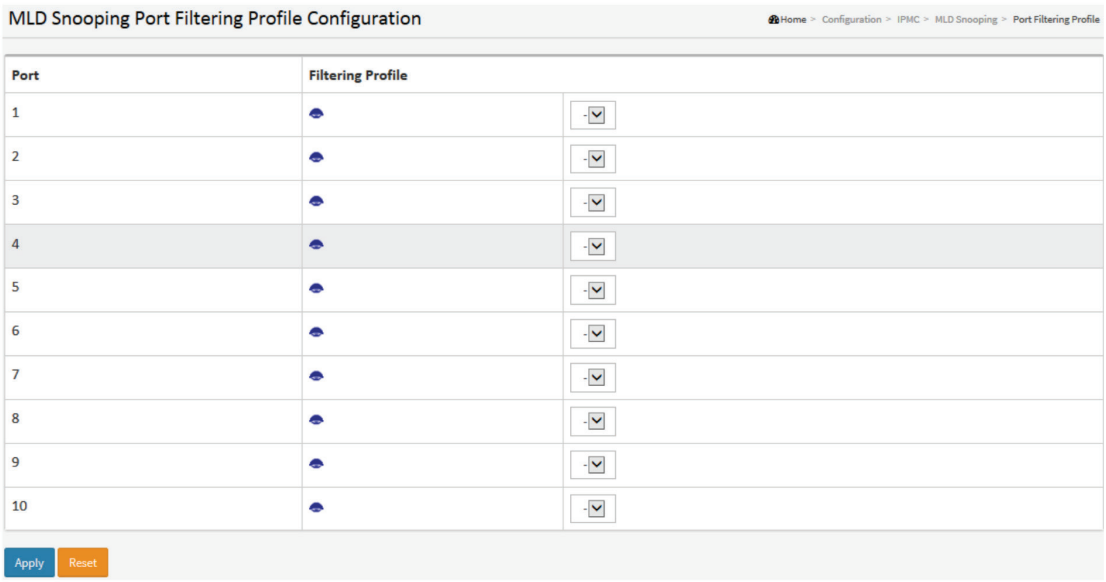



FIGURE 3-64. MLD SNOOPING PORT GROUP FILTERING CONFIGURATION SCREEN

**Parameter description:**

- Port: The logical port for the settings.
- Filtering Profile: Select the IPMC Profile as the filtering condition for the specific port. To show a summary of the designated profile, click the view button.
- Profile Management Button: You can inspect the rules of the designated profile by using the eye 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.

## 3.12 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.

### 3.12.1 LLDP CONFIGURATION

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

#### WEB INTERFACE

To configure LLDP:

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

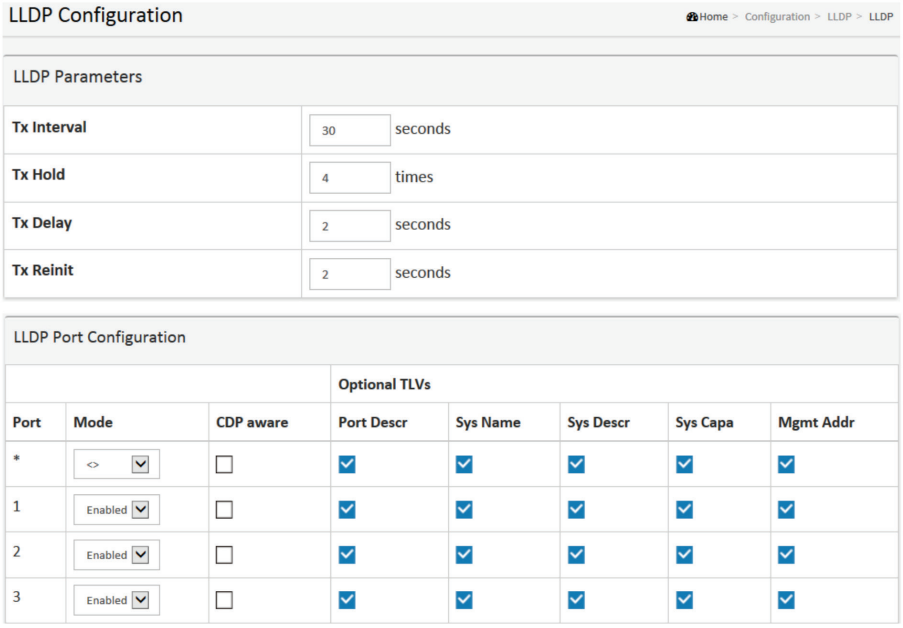



FIGURE 3-65. LLDP CONFIGURATION SCREEN

Parameter description:

LLDP Parameters

- Tx Interval: The switch periodically transmits LLDP frames to its neighbors so the network discovery information is 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 will 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

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

- 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 a 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 "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 is removed 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.

## 3.12.2 LLDP-MED CONFIGURATION

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

- Auto-discovery of LAN policies (such as VLAN, Layer 2 Priority and Differentiated services [Diffserv] settings), enabling plug-and-play networking.
- Device location discovery to allow creation of location databases and, in the case of Voice over Internet Protocol (VoIP), Enhanced 911 services.
- Inventory management, allowing network administrators to track their network devices, and determine their characteristics (manufacturer, software and hardware versions, serial or asset number).
- This page allows you to configure the LLDP-MED. This function applies to VoIP devices which support LLDP-MED.

### WEB INTERFACE

To configure LLDP-MED:

1. Click 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; the switch will show the following Policy Port Configuration.
7. Select Policy ID for each port.
8. Click Apply.

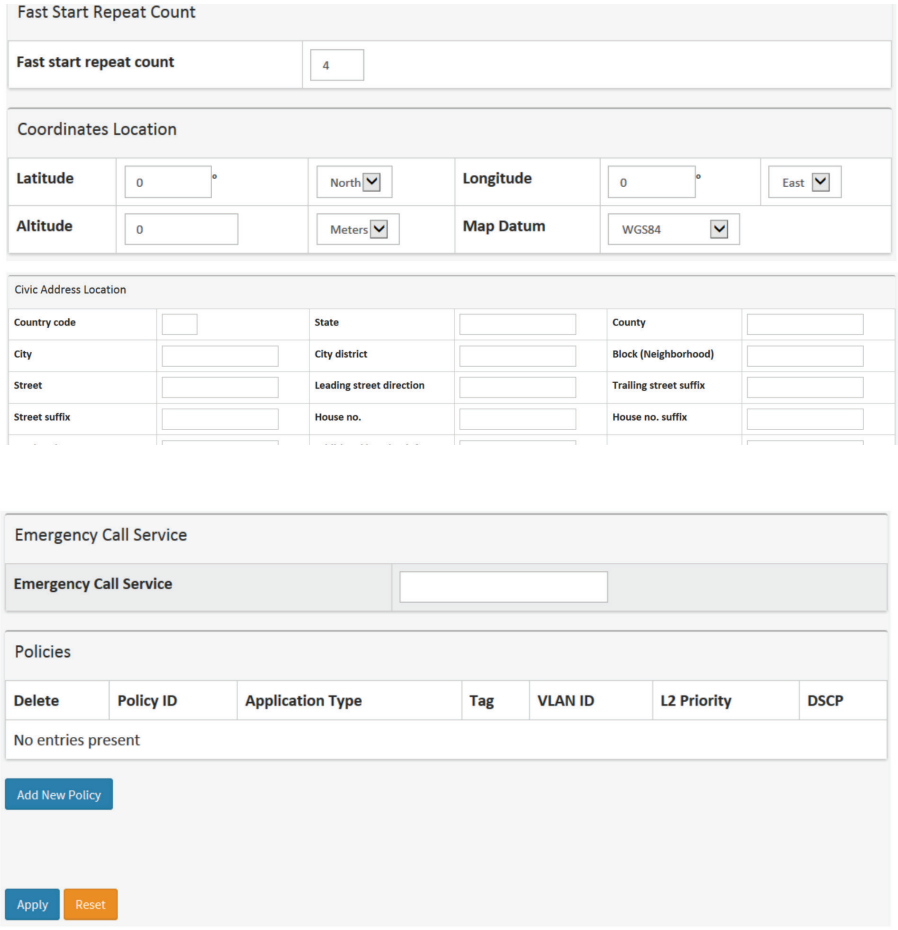



FIGURE 3-66. LLDP-MED CONFIGURATION SCREEN

**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 that 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 to 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, we recommend repeating the fast start transmission multiple times to increase the possibility of the neighbors receiving the LLDP frame. With Fast start repeat count, you can specify the number of times the fast start transmission would be repeated. The recommended value is 4 times, given that 4 LLDP frames with a 1 second interval will be transmitted when an LLDP frame with new information is received.

**NOTE**: The 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 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. You can 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. You can 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. You can 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 that have different floor-to-floor dimensions. An altitude = 0.0 is meaningful even outside a building, and represents ground level at the given latitude and longitude. Inside a building, 0.0 represents the floor level associated with ground level at the main entrance.

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

- WGS84: (Geographical 3D) - World Geodesic System 1984, CRS Code 4327, Prime Meridian Name: Greenwich.
- NAD83/NAVD88: North American Datum 1983, CRS Code 4269, Prime Meridian Name: Greenwich; The associated vertical datum is the North American Vertical Datum of 1988 (NAVD88). This datum pair is to be used when referencing locations on land, not near tidal water (which would use Datum = NAD83/MLLW).
- NAD83/MLLW: North American Datum 1983, CRS Code 4269, Prime Meridian Name: Greenwich; The associated vertical datum is Mean Lower Low Water (MLLW). Use this datum pair 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 (Neighborhood): Neighborhood, block.
- Street: Street—Example: Poppelvej.
- Leading street direction: Leading street direction—Example: N.
- Trailing street suffix: Trailing street suffix—Example: SW.
- Street suffix: Street suffix—Example: Ave, Platz.
- House no.: House number—Example: 21.
- House no. suffix: House number suffix—Example: A, 1/2.
- Landmark: Landmark or vanity address—Example: Columbia University.
- Additional location info: Additional location info—Example: South Wing.
- Name: Name (residence and office occupant)—Example: Flemming Jahn.
- Zip code: Postal/zip code —Example: 2791.
- Building: Building (structure)—Example: Low Library.
- Apartment: Unit (Apartment, suite)—Example: Apt 42.

- Floor: Floor—Example: 4.
- Room no.: Room number—Example: 450F.
- Place type: Place type—Example: Office.
- Postal community name: Postal community name—Example: Leonia.
- P.O. Box: Post office box (P.O. BOX)—Example: 12345.
- Additional code: Additional code—Example: 1320300003.
- Emergency Call Service: Emergency Call Service (e.g. E911 and others), such as defined by TIA or NENA.
- 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 that apply for a set of specific protocol applications on that port. Improper network policy configurations are a very significant issue in VoIP environments that frequently result in voice quality degradation or loss of service.

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

The network policy attributes advertised are:

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

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

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

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

**NOTE**: LLDP-MED is not intended to run on links other than between Network Connectivity Devices and Endpoints, so it does not need to advertise the multitude of network policies that frequently run on an aggregated link interior to the LAN.

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

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

• Application Type: Intended use of the application types:

1. Voice - for use by dedicated IP Telephony handsets and other similar appliances supporting interactive voice services. These devices are typically deployed on a separate VLAN for ease of deployment and enhanced security by isolation from data applications.
2. Voice Signaling (conditional) - for use in network topologies that require a different policy for the voice signaling than for the voice media. This application type should not be advertised if all the same network policies apply as those advertised in the Voice application policy.
3. Guest Voice - support a separate “limited feature-set” voice service for guest users and visitors with their own IP Telephony handsets and other similar appliances supporting interactive voice services.

4. Guest Voice Signaling (conditional) - for use in network topologies that require a different policy for the guest voice signaling than for the guest voice media. This application type should not be advertised if all the same network policies apply as those advertised in the Guest Voice application policy.
5. Softphone Voice - for use by softphone applications on typical data centric devices, such as PCs or laptops. This class of endpoints frequently does not support multiple VLANs, if at all, and is 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 is relevant.
6. Video Conferencing - for use by dedicated Video Conferencing equipment and other similar appliances supporting real-time interactive video/audio services.
7. Streaming Video - for use by broadcast or multicast based video content distribution and other similar applications supporting streaming video services that require specific network policy treatment. Video applications relying on TCP with buffering would not be an intended use of this application type.
8. Video Signaling (conditional) - for use in network topologies that require a separate policy for the video signaling than for the video media. This application type should not be advertised if all the same network policies apply as those advertised in the Video Conferencing application policy.

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

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

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

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

◆ DSCP: DSCP value to be used to provide Diffserv node behavior for the specified application type as defined in IETF RFC 2474. DSCP may contain one of 64 code point values (0 through 63). A value of 0 represents use of the default DSCP value as defined in RFC 2475.

◆ Adding a new policy: Click to add 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 will 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.

## 3.13 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) that 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 frames 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.
2. Specify the Disable Automatic Aging and Aging Time.
3. Click Apply.

**MAC Table Learning**

1. Click configuration.
2. Specify the Port Members (Auto, Disable, Secure).
3. Click Apply.

**Static MAC Table Configuration**

1. Click configuration and Add new Static entry.
2. Specify the VLAN IP and Mac address, Port Members.
3. Click Apply.

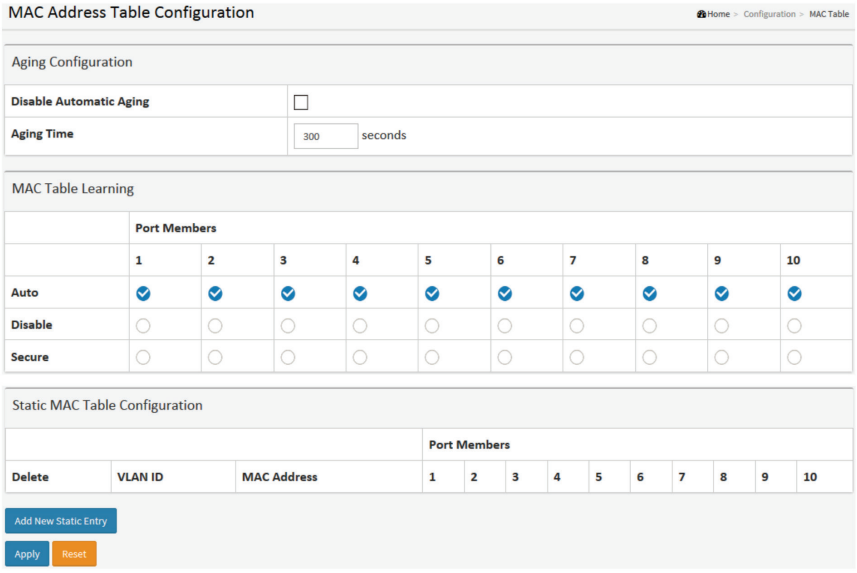



FIGURE 3-67. MAC ADDRESS TABLE CONFIGURATION SCREEN

**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 grayed out, another module is in control of the mode, so that it cannot be changed by the user. An example of such a module is the MAC-Based Authentication under 802.1X. Each port can do learning based upon the following settings:

- Auto: Learning is done automatically as soon as a frame with an 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.

- Delete: Check to delete the entry. It will be deleted during the next save.
- VLAN ID: The VLAN ID of the entry.
- MAC Address: The MAC address of the entry.
- Port Members: Checkmarks indicate which ports are members of the entry. Check or uncheck as needed to modify the entry.
- Adding a New Static Entry: Click to add a new entry to the static MAC table. Specify the VLAN ID, MAC address, and port members for the new entry. Click "Apply."
- Buttons:

- Apply – Click to save changes.

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

## 3.14 VLANS

You can assign a specific VLAN for management purposes. The management VLAN is used to establish an IP connection to the switch from a workstation connected to a port in the VLAN. This connection supports a VSM, SNMP, and Telnet session. By default, the active management VLAN is VLAN 1, but you can designate any VLAN as the management VLAN 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 VLANs.
2. Specify Existing VLANs, Ether type for Custom S-ports.
3. Click Apply.

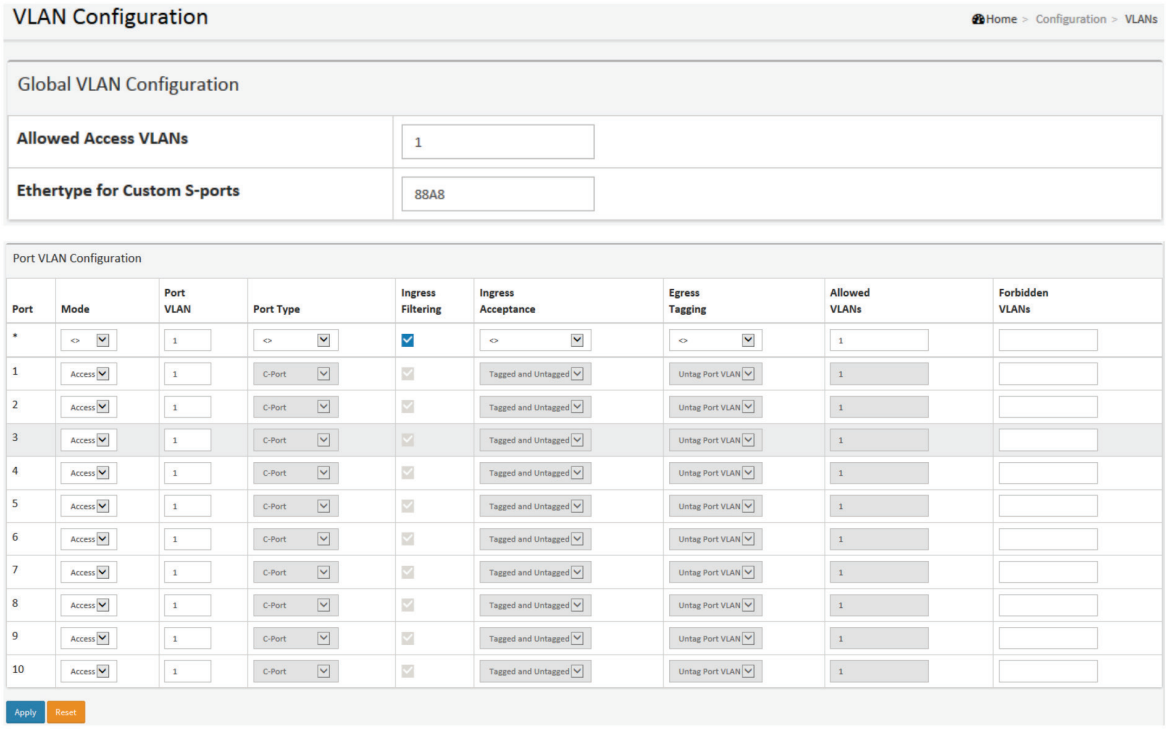



FIGURE 3-68. VLAN CONFIGURATION SCREEN

Parameter description:

Global VLAN Configuration

- Existing VLANs: This field shows the VLANs that are created on the switch.

By default, only VLAN 1 exists. 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 a 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 add additional port configuration features. In addition to the characteristics described for trunk ports, hybrid ports have these abilities: They can be configured to be VLAN tag unaware or, C-tag aware, S-tag aware, or S-custom-tag aware,ingress filtering can be controlled, and 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 is 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 seamlessly 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.

## 3.15 PRIVATE VLANS

In a private VLAN, communication between ports in that private VLAN is not permitted. A VLAN can be configured as a private VLAN.

### 3.15.1 VLAN MEMBERSHIP

The VLAN membership configuration for the selected stack switch unit switch can be monitored and modified here. Up to 4096 VLANs are supported. This page allows for adding and deleting VLANs as well as adding and deleting port members of each VLAN.

#### WEB INTERFACE

To configure VLAN membership configuration in the web interface:

1. Click VLAN membership Configuration.
2. Specify Management VLAN ID. 0–4094
3. Click Apply.

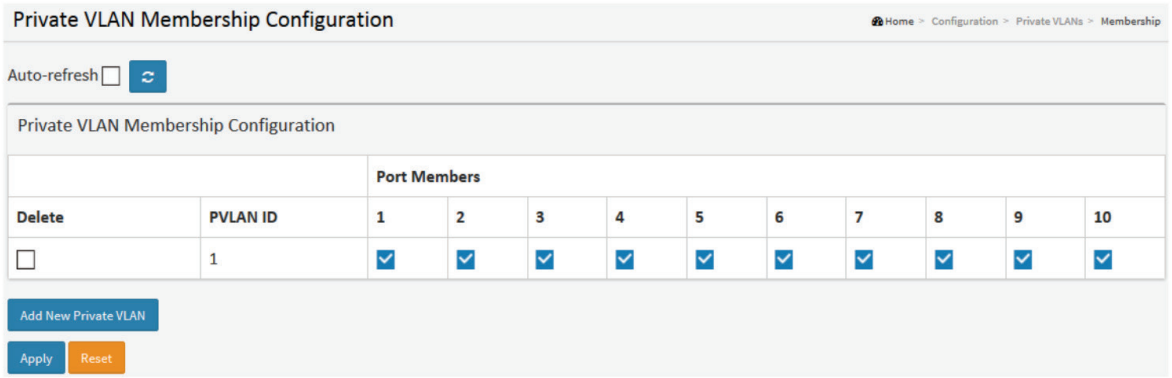



FIGURE 3-69. VLAN MEMBERSHIP CONFIGURATION SCREEN

Parameter description:

- Delete: To delete a private VLAN entry, check this box. The entry will be deleted during the next save.
- PVLAN ID: Indicates the ID of this particular private VLAN.
- Port Members: A row of check boxes for each port is displayed for each VLAN ID. To include a port in a VLAN, check the box. To remove or exclude the port from the VLAN, make sure the box is unchecked. By default, no ports are members, and all boxes are unchecked.
- Adding a New VLAN: Click to add a new VLAN ID. An empty row is added to the table, and the VLAN can be configured as needed. Legal values for a VLAN ID are 1 through 4095.

The VLAN is enabled on the selected stack switch unit when you click on “Save.” The VLAN is thereafter present on the other stack switch units, but with no port members. The check box is greyed out when VLAN is displayed on other stacked switches, but user can add member ports to it.

A VLAN without any port members on any stack unit will be deleted when you click “Save.”

The button can be used to undo the addition of new VLANs.

- Buttons:

- Apply – Click to save changes.

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

## 3.15.2 PORT ISOLATION

Port Isolation provides for an apparatus and method to isolate ports on layer 2 switches on the same VLAN to restrict traffic flow. The apparatus comprises a switch with plurality of ports, each port configured as a protected port or a non-protected port. An address table memory stores an address table having a destination address and port number pair. A forwarding map generator generates a forwarding map which is responsive to a destination address of a data packet. The method for isolating ports on a layer 2 switch comprises configuring each of the ports on the layer 2 switch as a protected port or a non-protected port. A destination address on an data packet is matched with a physical address on the layer 2 switch and a forwarding map is generated for the data packet based upon the destination address on the data packet. The data packet is then sent to the ports identified by the forwarding map generated based upon whether the ingress port was configured as a protected or non-protected port.

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

### WEB INTERFACE

To configure Port Isolation configuration in the web interface:

1. Click Private VLAN, Port Isolation.
2. Select the port for which you want to enable Port Isolation.
3. Click Apply.


FIGURE 3-70. PORT ISOLATION CONFIGURATION SCREEN

**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.

## 3.16 VCL

### 3.16.1 MAC-BASED VLAN

MAC address-based VLAN decides the VLAN for forwarding an untagged frame based on the source MAC address of the frame.

The most common way of grouping VLAN members is by port, hence the name port-based VLAN. Typically, the device adds the same VLAN tag to untagged packets that are received through the same port. Later on, these packets can be forwarded in the same VLAN. Port-based VLAN is easy to configure, and applies to networks where the locations of terminal devices are relatively fixed. As mobile office and wireless network access gain more popularity, the ports that terminal devices use to access the networks are very often non-fixed. A device may access a network through Port A this time, but through Port B the next time. If Port A and Port B belong to different VLANs, the device will be assigned to a different VLAN the next time it accesses the network. As a result, it will not be able to use the resources in the old VLAN. On the other hand, if Port A and Port B belong to the same VLAN, after terminal devices access the network through Port B, they will have access to the same resources as those accessing the network through Port A do, which brings security issues. To provide user access and ensure data security in the meantime, MAC-based VLAN technology is used.

MAC-based VLANs group VLAN members by MAC address. With MAC-based VLAN configured, the device adds a VLAN tag to an untagged frame according to its source MAC address. MAC-based VLANs are mostly used in conjunction with security technologies such as 802.1X to provide secure, flexible network access for terminal devices.

#### WEB INTERFACE

To configure MAC address-based VLAN configuration in the web interface:

1. Click VLC, MAC-based VLAN configuration and add new entry.
2. Specify the MAC address and VLAN ID.
3. Click Apply.

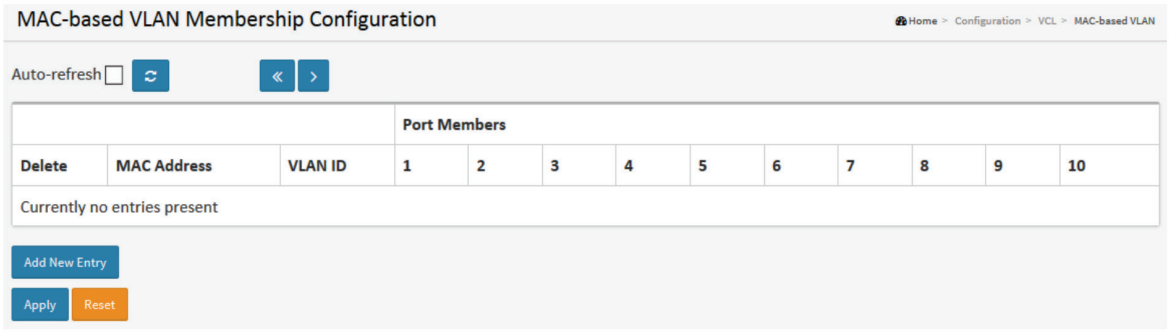



FIGURE 3-71. MAC-BASED VLAN MEMBERSHIP CONFIGURATION SCREEN

**Parameter description:**

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

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

The MAC-based VLAN entry is enabled on the selected stack switch unit when you click on "Save." A MAC-based VLAN without any port members on any stack unit will be deleted when you click "Save."

The button can be used to undo the addition of new MAC-based VLANs.

• Buttons:

- Apply – Click to save changes.

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

## 3.16.2 PORT ISOLATION

This section describes Protocol -based VLAN. The switch supports Ethernet, LLC, and 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, Decnet and Appletalk) to coexist within a multipoint network and to be transported over the same network media, and can also provide flow control and automatic repeat request (ARQ) error management mechanisms.

**SNAP**: The 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.

### 3.16.2.1 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 -based VLAN configuration in the web interface:

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

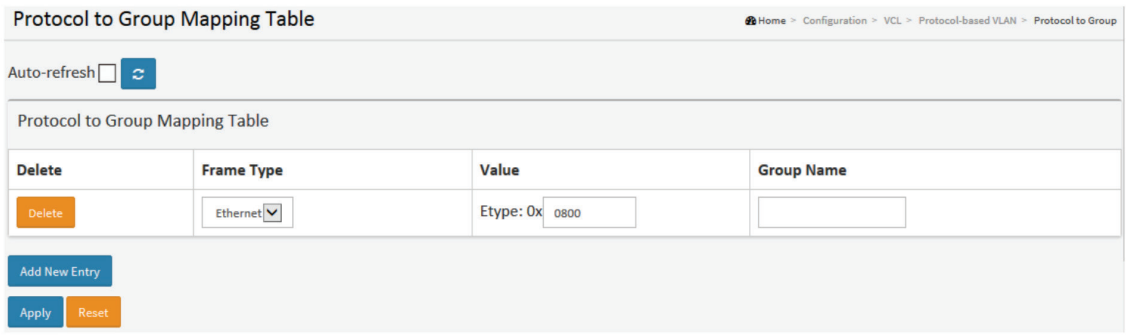



FIGURE 3-72. PROTOCOL TO GROUP MAPPING TABLE

**Parameter description:**

- Delete: To delete a Protocol to Group Name map entry, check this box. The entry will be deleted on the switch during the next Save.
- Frame Type: Frame Type can have one of the following values:

1. Ethernet

2. LLC

3. SNAP

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

- Value: A valid value that can be entered in this text field depends on the option selected from the the preceding Frame Type selection menu.

Below is the criteria for three different Frame Types:

1. For Ethernet: Values in the text field when Ethernet is selected as a Frame Type is called etype. Valid values for etype ranges from 0x0600-0xffff

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 a 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 the value of the OUI field is 00-00-00 then the value of PID will be etype (0x0600-0xffff), and if value of OUI is other than 00-00-00 then a valid value of PID will be any value from 0x0000 to 0xffff.

- Group Name: A valid Group Name is a unique 16-character long string for every entry which consists of a combination of alphabets (a-z or A-Z) and integers (0-9).

**NOTE**: Special characters and underscore(_) are not allowed.

- Adding a New Group to VLAN mapping entry: Click to add a new entry in the 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.
- Buttons:

- Apply – Click to save changes.

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

- Upper right icon (Refresh):

Click to refresh the Protocol Group Mapping information manually.

### 3.16.2.2 GROUP TO VLAN

This section allows you to map an already configured Group Name to a VLAN for the selected stack switch unit switch.

Web Interface

To Display Group Name to VLAN mapping table configured in the web interface:

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

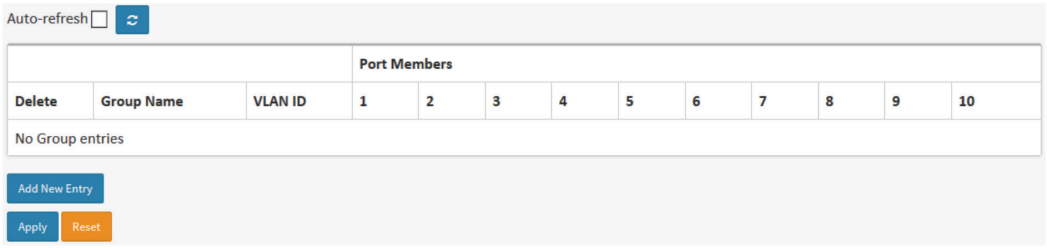



FIGURE 3-73. GROUP NAME OF VLAN MAPPING TABLE

**Parameter description:**

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

- Apply – Click to save changes.

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

- Auto-refresh: Evoke the auto-refresh icon and the device will refresh the information automatically.
- Upper right icon (Refresh): Click to refresh the Protocol Group Mapping information manually.

## 3.16.3 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 Display IP subnet-based VLAN Membership to configured in the web interface:

1. Click VCL, Group Name VLAN configuration, and add new entry.
2. Specify the VCE ID, IP Address, Mask Length, VLAN ID, and select Port Members.
3. Click Apply.

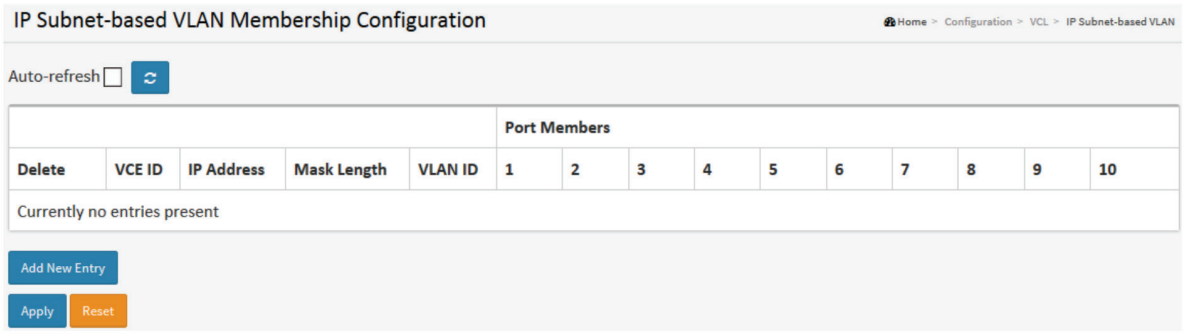



FIGURE 3-74. IP SUBNET-BASED VLAN MEMBERSHIP CONFIGURATION SCREEN

**Parameter description:**

- Delete: To delete a IP subnet-based VLAN entry, check this box and press save. The entry will be deleted on the selected switch in the stack.
- VCE ID: Indicates the index of the entry. It is user configurable. Its value ranges from 0–128. If a VCE ID is 0, the 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, which 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.
- 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.” Use the “Delete” button to undo the addition of new IP subnet-based VLANs. The maximum possible IP subnet-based VLAN entries are limited to 128.

## 3.17 VOICE VLAN

Voice VLAN is VLAN configured specially for voice traffic. By adding the ports with voice devices attached to voice VLAN, we can perform QoS-related configuration for voice data, ensuring the transmission priority of voice traffic and voice quality.

### 3.17.1 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. Select “Enabled” in the Voice VLAN Configuration.
2. Specify VLAN ID, Aging Time, Traffic Class.
3. Specify (Port Mode, Security, Discovery Protocol)

in the Port Configuration.

4. Click Apply.

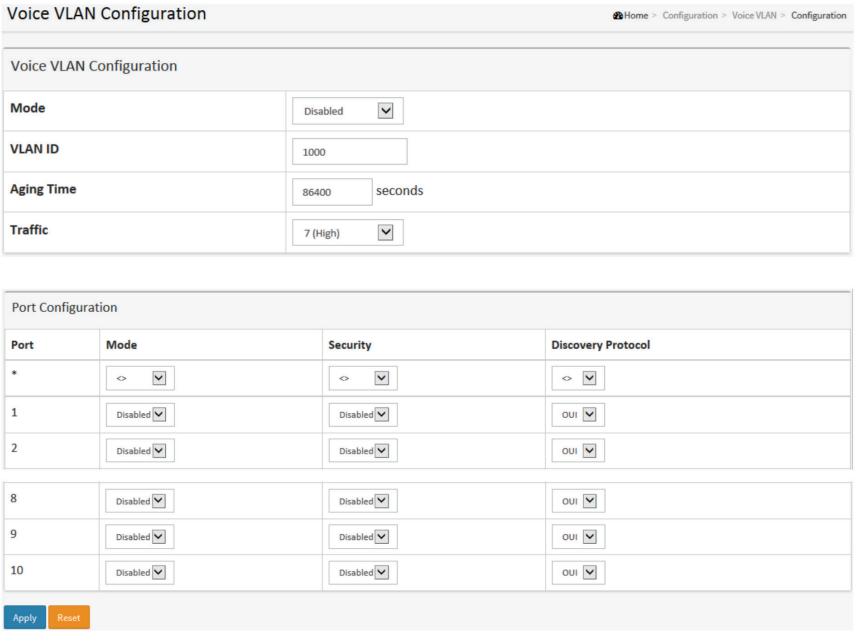



FIGURE 3-75. VOICE VLAN CONFIGURATION SCREEN

**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 Class: Indicates the Voice VLAN traffic class. All traffic on the Voice VLAN will apply to this class.
- Port Mode: Indicates the Voice VLAN port mode.

When the port mode isn't equal disabled, you must disable MSTP feature before you enable Voice VLAN to avoid an ingress filtering conflict.

Possible port modes are:

- Disabled: Disjoin from Voice VLAN.

- Auto: Enable auto detect mode. It detects whether there is VoIP phone attached to the specific port and configures the Voice VLAN members automatically.

- Forced: Force join to Voice VLAN.

- Port Security: Indicates the Voice VLAN port security mode. When the function is enabled, all non-telephonic MAC addresses in the Voice VLAN will be blocked for 10 seconds. Possible port modes are:

- Enabled: Enable Voice VLAN security mode operation.

- Disabled: Disable Voice VLAN security mode operation.

- Port Discovery Protocol: Indicates the Voice VLAN port discovery protocol. It will only work when auto detect mode is enabled. Enable the LLDP feature before configuring discovery protocol to "LLDP" or "Both." Changing the discovery protocol to "OUI" or "LLDP" will restart the 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.

## 3.17.2 OUI

The section describes how to configure the Voice VLAN OUI table. The maximum entry number is 16. Modifying the OUI table will restart auto detection of OUI process.

### WEB INTERFACE

To configure the Voice VLAN OUI Table in the web interface:

1. Select “Add new entry“ in the Voice VLAN OUI table.
2. Specify Telephony OUI, Description.
3. Click Apply.

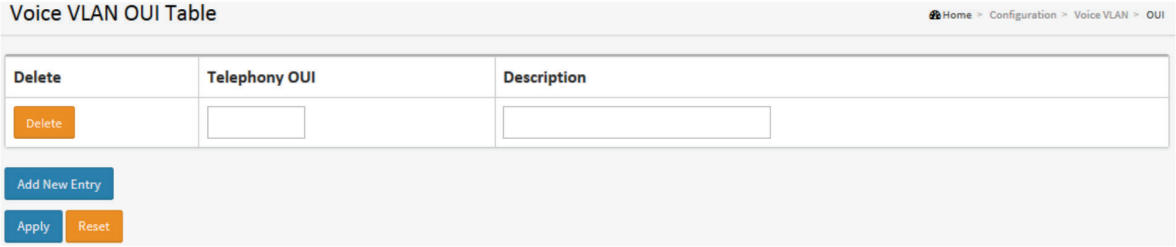



FIGURE 3-76. VOICE VLAN OUI TABLE

**Parameter description:**

- Delete: Check to delete the entry. It will be deleted during the next save.
- Telephony OUI: A telephony OUI address is a globally unique identifier assigned to a vendor by IEEE. It must be 6 characters long and the input format is “xx-xx-xx” (x is a hexadecimal digit).
- Description: The description of an OUI address. Normally, it describes which vendor telephony device it belongs to. The allowed string length is 0 to 32.
- Add New entry: Click to add a new entry in Voice VLAN OUI table. An empty row is added to the table, the Telephony OUI, Description.
- Buttons:

- Apply – Click to save changes.

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

## 3.18 QOS

The switch supports four QoS queues per port with strict or weighted fair queuing scheduling. It supports QoS Control Lists (QCL) for advanced programmable QoS classification, based on IEEE 802.1p, Ethertype, VID, IPv4/IPv6, DSCP, and UDP/TCP ports and ranges.

Classifying incoming frames to a QoS class is highly flexible. 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 supports advanced memory control mechanisms providing excellent performance of all QoS classes under any traffic scenario, including jumbo frame. A super priority queue with dedicated memory and strict highest priority in the arbitration. The ingress super priority queue allows traffic recognized as CPU traffic to be received and queued for transmission to the CPU even when all the QoS class queues are congested.

### 3.18.1 PORT CLASSIFICATION

The section allows you to configure the basic QoS Ingress Classification settings for all switch ports. The settings relate to the currently selected stack unit, as reflected by the page header.

#### WEB INTERFACE

To configure the QoS Port Classification parameters in the web interface:

1. Click Configuration, QoS, Port Classification.
2. Scroll to select QoS class, DP Level, PCP, and DEI parameters.
3. Click save to save the setting.
4. To cancel the setting, click the Reset button. It will revert to previously saved values

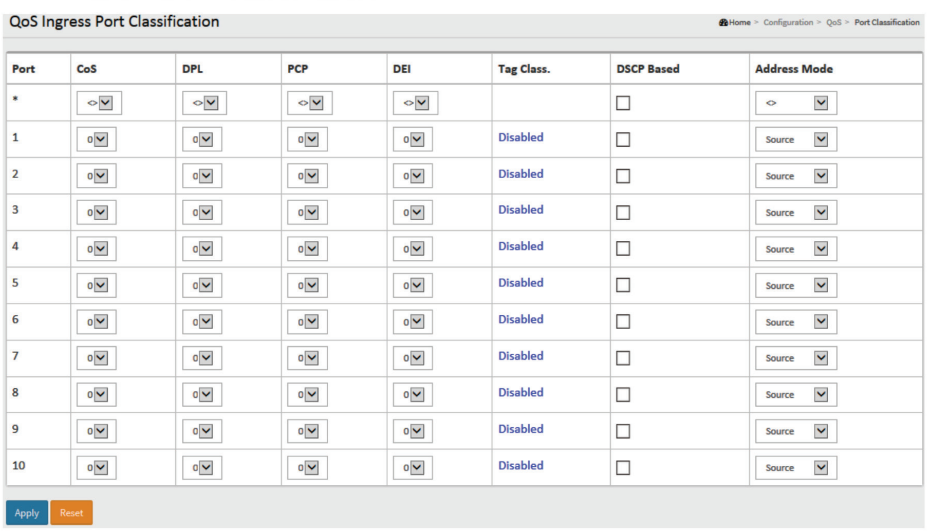



FIGURE 3-77. QOS CONFIGURATION SCREEN

**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, the frame is tagged, and Tag Class. is enabled, then the frame is classified to a CoS that is mapped from the PCP and DEI value in the tag. Otherwise, the frame is classified to the default CoS.

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.

- PCP: Controls the default PCP value.

All frames are classified to a PCP value.

If the port is VLAN aware and the frame is tagged, then the frame is classified to the PCP value in the tag. Otherwise, the frame is classified to the default PCP value.

- DEI: Controls the default DEI value.

All frames are classified to a DEI value.

If the port is VLAN aware and the frame is tagged, then the frame is classified to the DEI value in the tag. Otherwise, the frame is classified to the default DEI value.

- Tag Class.: Shows the classification mode for tagged frames on this port.

- Disabled: Use default QoS class and DP level for tagged frames.

- Enabled: Use mapped versions of PCP and DEI for tagged frames.

Click on the mode in order to configure the mode and/or mapping.

NOTE: This setting has no effect if the port is VLAN unaware. Tagged frames received on VLAN unaware ports are always classified to the default CoS and DPL.

- DSCP Based: Click to Enable DSCP Based QoS Ingress Port Classification.
- Address Mode: The IP/MAC address mode specifying whether the QCL classification must be based on source (SMAC/SIP) or destination (DMAC/DIP) addresses on this port. The allowed values are:

- Source: Enable SMAC/SIP matching.

- Destination: Enable DMAC/DIP matching.

- Buttons:

- Apply – Click to save changes.

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

## 3.18.2 PORT POLICING

This section provides an overview of 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 display the QoS Port Schedulers in the web interface:

1. Click Configuration, QoS, Port Policing.
2. Select which port for which to enable the QoS Ingress Port Policers and type the Rate limit condition.
3.Scroll to select the Rate limit Unit with kbps, Mbps, fps, and kfps.
4. Click Apply to save the configuration.

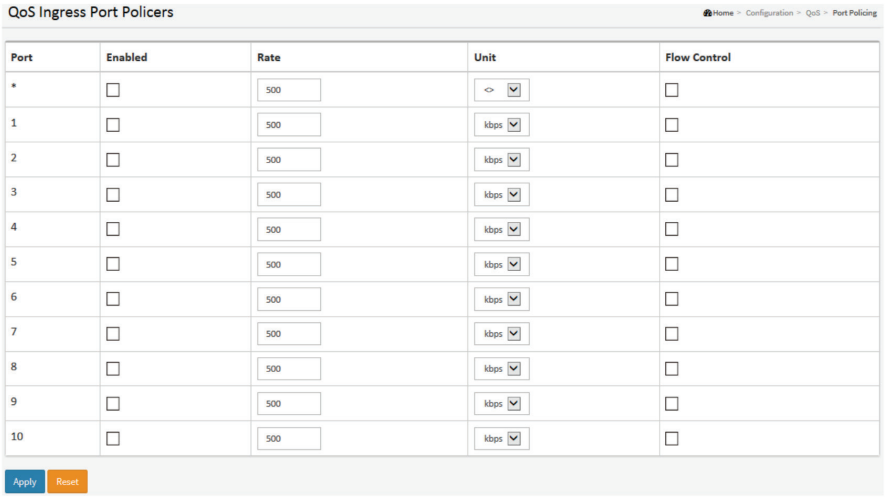



FIGURE 3-78. QOS INGRESS PORT POLICERS CONFIGURATION SCREEN

**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.
- Enabled: Select the Port for which you need to enable the QoS Ingress Port Policers function.
- Rate: Set the Rate limit value for this port, the default is 500.
- Unit: Scroll to select the rate unit from kbps, Mbps, fps and kfps. The default is kbps.
- Flow Control: If flow control is enabled and the port is in flow control mode, then pause frames are sent instead of discarding frames.
- Buttons:

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

## 3.18.3 PORT SCHEDULERS

This section provides an overview of QoS Egress Port Schedulers for all switch ports and the ports belong to the currently selected stack unit, as reflected by the page header.

### WEB INTERFACE

To display the QoS Port Schedulers in the web interface:

1. Click Configuration, QoS, Port Schedulers.
2. Display the QoS Egress Port Schedulers.

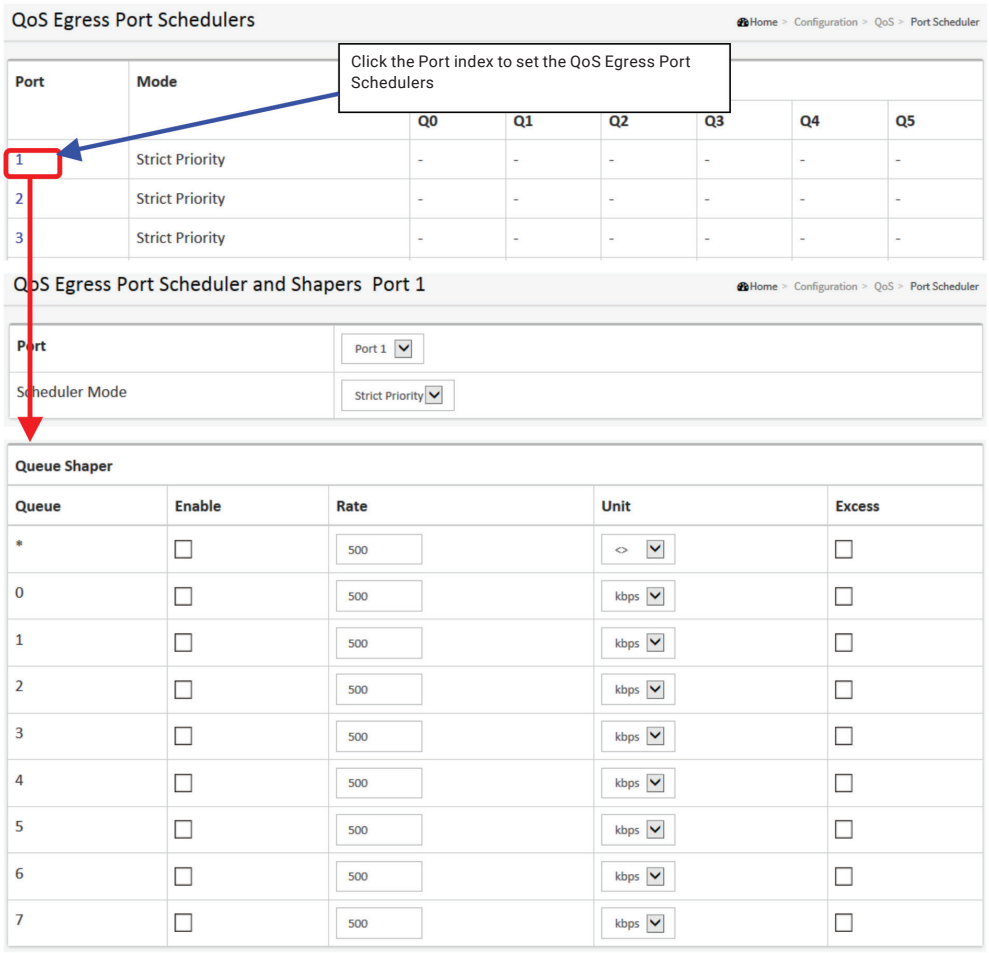



FIGURE 3-79. QOS EGRESS PORT SCHEDULES SCREEN

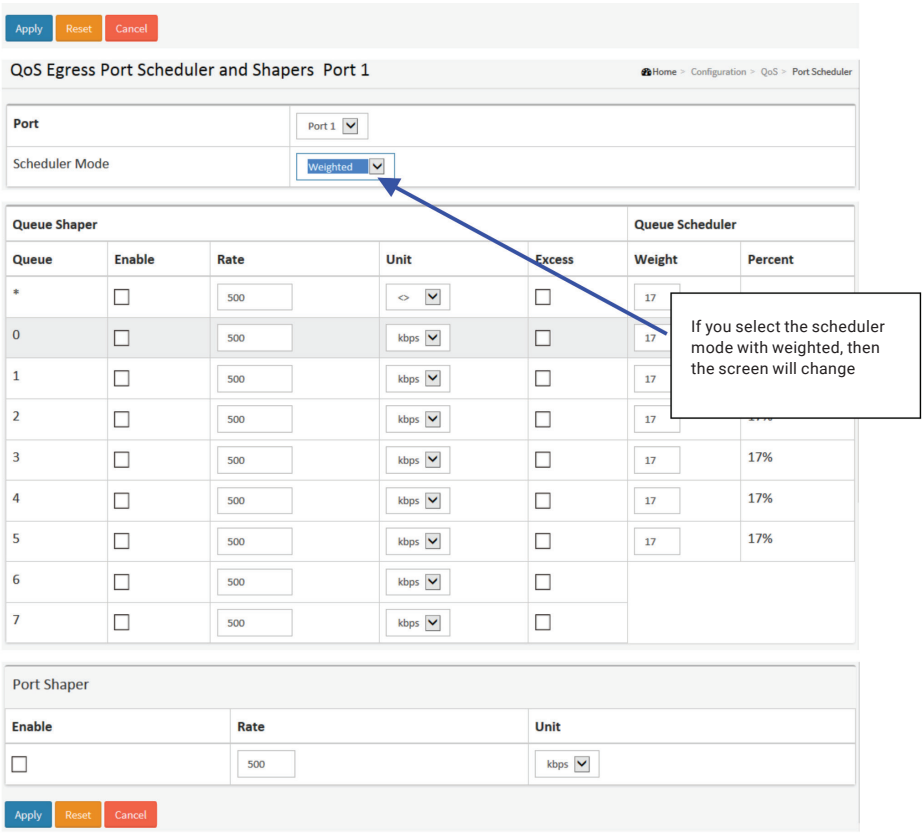



FIGURE 3-80. QOS EGRESS SCHEDULERS AND SHAPERS PORT 1 SCREEN

**Parameter description:**

- Port: The logical port for the settings contained in the same row. Click on the port number to configure the schedulers.
- Mode: Shows the scheduling mode for this port.
- Weight (Qn): Shows the weight for this queue and port.
- Scheduler Mode: Controls whether the scheduler mode is “Strict Priority” or “Weighted” on this switch port.
- Queue Shaper Enable: Controls whether the queue shaper is enabled for this queue on this switch port.
- Queue Shaper Rate: Controls the rate for the queue shaper. The default value is ?. This value is restricted to ?-1000000 when the “Unit” is “kbps”, and it is restricted to 1-? when the “Unit” is “Mbps.
- Queue Shaper Unit: Controls the unit of measure for the queue shaper rate as “kbps” or “Mbps”. The default value is “kbps”.
- Queue Shaper Excess: Controls whether the queue is allowed to use excess bandwidth.
- Queue Scheduler Weight: Controls the weight for this queue. The default value is 17. This value is restricted to 1–100. This parameter is only shown if Scheduler Mode is set to Weighted.
- Queue Scheduler Percent: Shows the weight in percent for this queue. This parameter is only shown if Scheduler Mode is set to Weighted.
- Port Shaper Enable: Controls whether the port shaper is enabled for this switch port.
- Port Shaper Rate: Controls the rate for the port shaper. The default value is ?. This value is restricted to ?–1000000 when the “Unit” is “kbps”, and it is restricted to 1–? 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.

## 3.18.4 PORT SHAPING

This section provides an overview of QoS Egress Port Shapers for all switch ports. Otherwise, the user can get all detailed information to the ports belonging to the currently selected stack unit, as reflected by the page header.

### WEB INTERFACE

To display the QoS Port Shapers in the web interface:

1. Click Configuration, QoS, Port Shapers.

2. Display the QoS Egress Port Shapers.

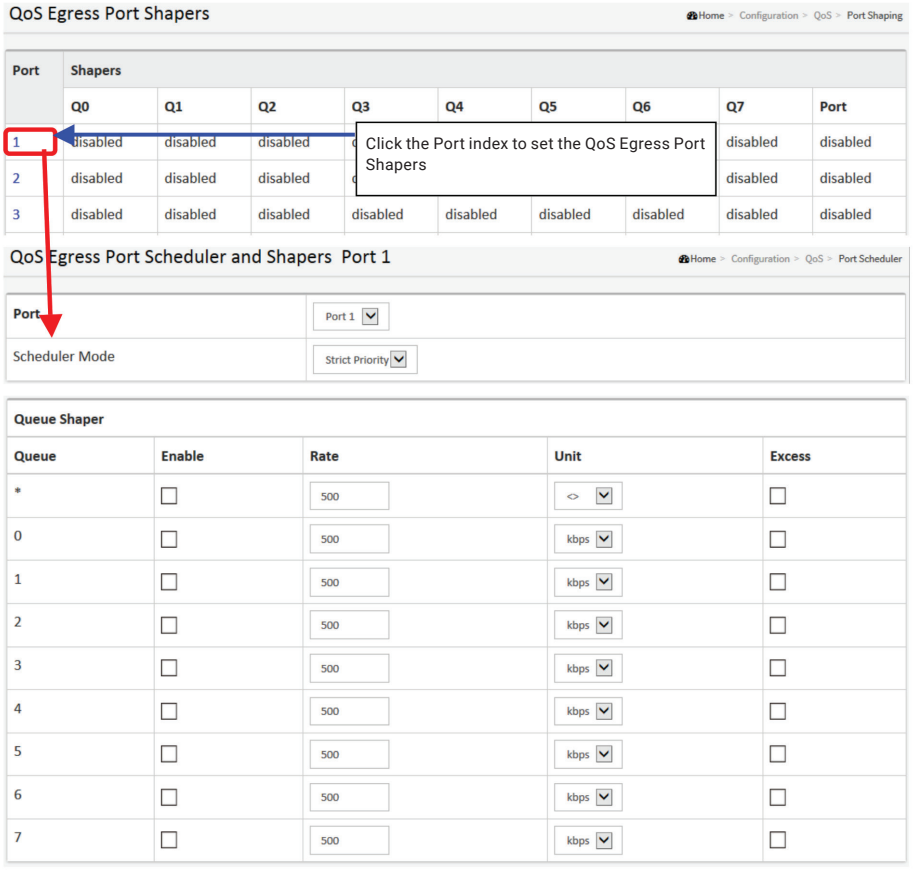



FIGURE 3-81. QOS EGRESS PORT SHAPERS SCREEN

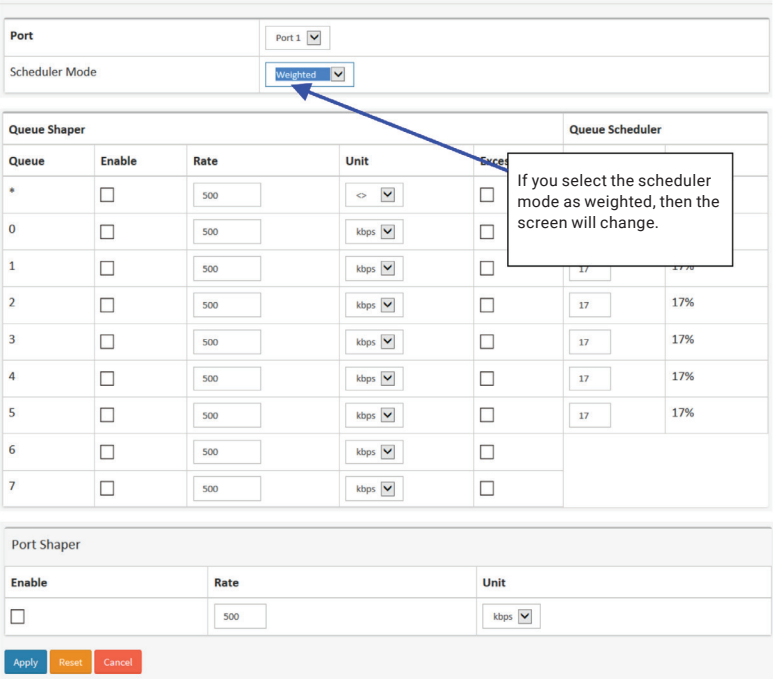



FIGURE 3-82. QOS EGRESS PORT SHAPERS PORT 1 SCREEN

**Parameter description:**

- Port: The logical port for the settings contained in the same row. Click on the port number to configure the shapers.
- Mode: Shows the scheduling mode for this port.
- Shapers (Qn): Shows "disabled" or actual queue shaper rate—e.g. 800 Mbps.
- Scheduler Mode: Controls whether the scheduler mode is "Strict Priority" or "Weighted" on this switch port.
- Queue Shaper Enable: Controls whether the queue shaper is enabled for this queue on this switch port.
- Queue Shaper Rate: Controls the rate for the queue shaper. The default value is ?. This value is restricted to ?–1000000 when the "Unit" is "kbps", and it is restricted to 1–? when the "Unit" is "Mbps."
- Queue Shaper Unit: Controls the unit of measure for the queue shaper rate as "kbps" or "Mbps". The default value is "kbps".
- Queue Shaper Excess: Controls whether the queue is allowed to use excess bandwidth.
- Queue Scheduler Weight: Controls the weight for this queue. The default value is 17. This value is restricted to 1–100. This parameter is only shown if Scheduler Mode is set to Weighted.
- Queue Scheduler Percent: Shows the weight in percent for this queue. This parameter is only shown if Scheduler Mode is set to Weighted.
- Port Shaper Enable: Controls whether the port shaper is enabled for this switch port.
- Port Shaper Rate: Controls the rate for the port shaper. The default value is ?. This value is restricted to ?–1000000 when the "Unit" is "kbps," and it is restricted to 1–? 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.

## 3.18.5 PORT TAG REMARKING

The section provides an overview of QoS Egress Port Tag Remarking for all switch ports. Otherwise, the ports belong to the currently selected stack unit, as reflected by the page header.

### WEB INTERFACE

To display the QoS Port Tag Remarking in the web interface:

1. Click Configuration, QoS, Port Tag Remarking.

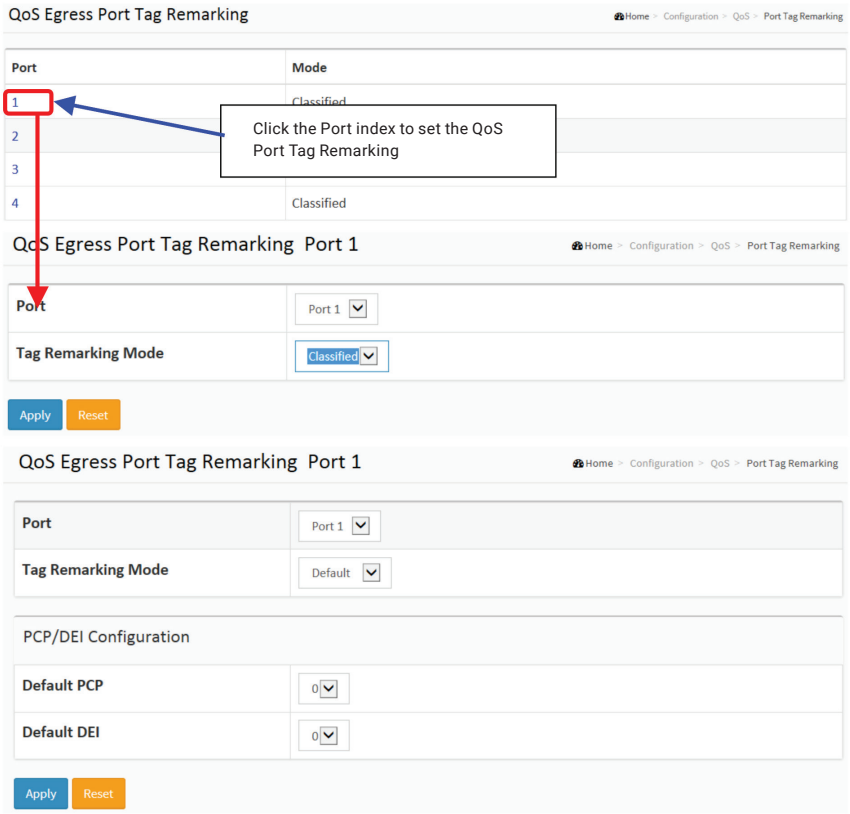



FIGURE 3-83. PORT TAG REMARKING SCREEN

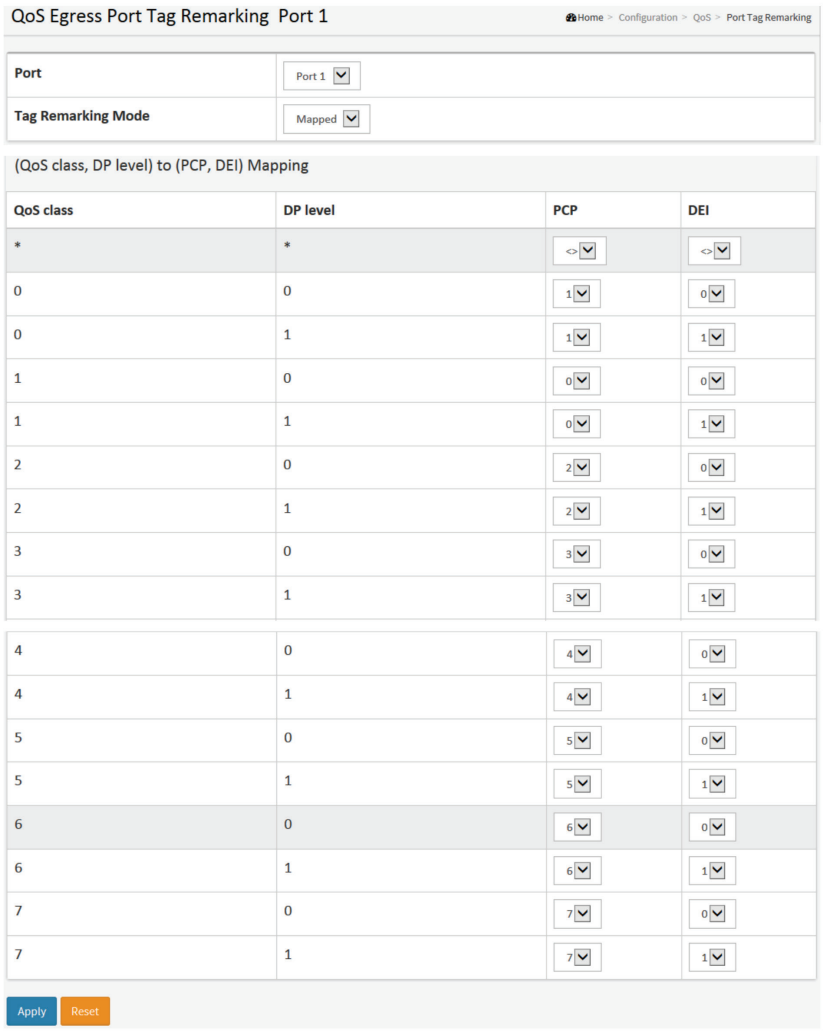



FIGURE 3-84. QOS EGRESS PORT TAG REMARKING PORT 1 SCREEN

**Parameter description:**

- 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 cancel the changes.

## 3.18.6 PORT DSCP

The section will explain how to set the QoS Port DSCP configuration that allowed you to configure the basic QoS Port DSCP Configuration settings for all switch ports. Otherwise, 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, Port DSCP.
2. Enable or disable the Ingress Translate and Scroll to the Classify Parameter configuration.
3. Scroll to select Egress Rewrite parameters.
4. Click save to save the setting.
5. To cancel the setting, click the Reset button. It will revert to previously saved values.

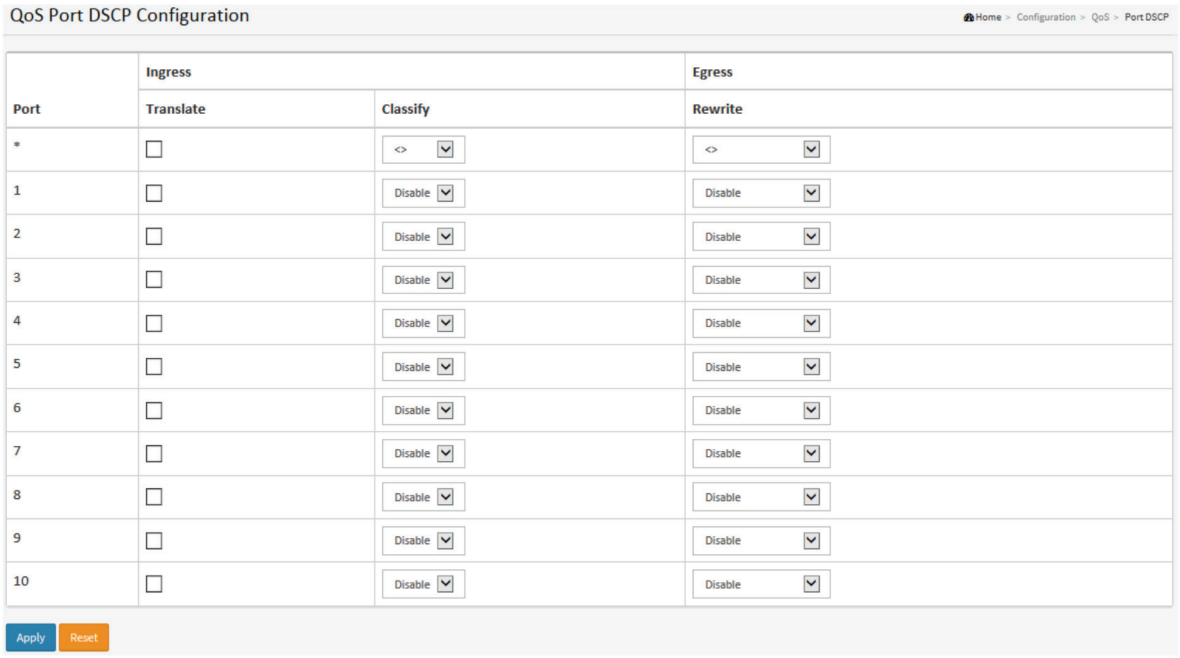



FIGURE 3-85. QOS PORT DSCP CONFIGURATION SCREEN

**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 the 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 the remapped DSCP value.

- Buttons:

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

- Auto-refresh: Select the auto-refresh icon and the device will refresh the information automatically.
- Upper right icon (Refresh): Click this icon to refresh the QoS Port DSCP information manually.

## 3.18.7 DSCP-BASED QOS

The section explains how to configure the DSCP-Based QoS mode. 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, DSCP-Based QoS
2. Enable or disable the DSCP for Trust.
3. Scroll to select QoS Class and DPL parameters.
4. Click save to save the setting.
5. To cancel the setting, click the Reset button. It will revert to previously saved values

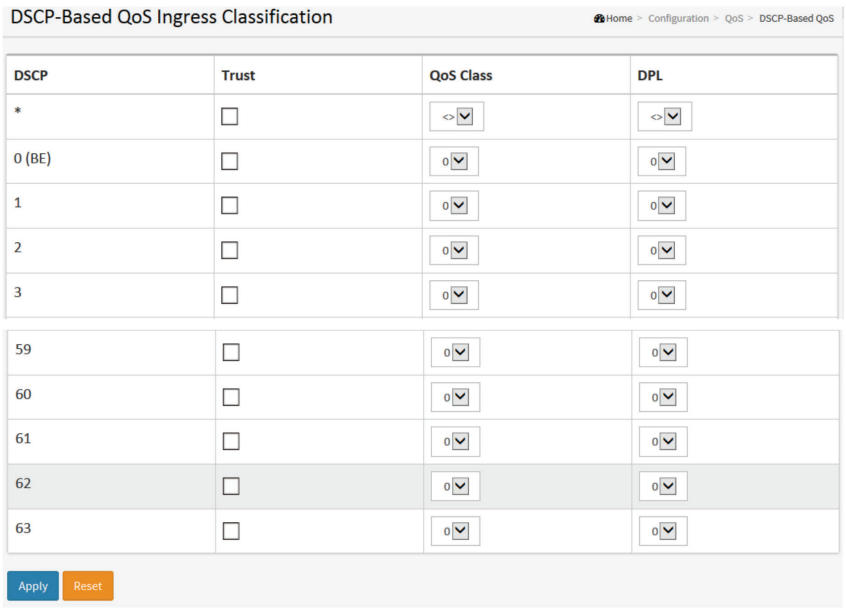



FIGURE 3-86. DSCP-BASED QOS INGRESS CLASSIFICATION CONFIGURATION SCREEN

Parameter description:

- DSCP: Maximum number of supported DSCP values are 64.
- Trust: Click to check if the DSCP value is trusted.
- QoS Class: QoS Class value can be 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.

- Auto-refresh: Select the auto-refresh icon and the device will refresh the information automatically.
- Upper right icon (Refresh): Click to refresh the DSCP-Based QoS Ingress Classification information manually.

## 3.18.8 DSCP TRANSLATION

The section describes how 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, DSCP Translation.
2. Scroll to set the Ingress Translate and Egress Remap DP0 and Remap DP1 Parameters.
3. Enable or disable Classify.
4. Click save to save the setting.
5. To cancel the setting, click the Reset button. It will revert to previously saved values.

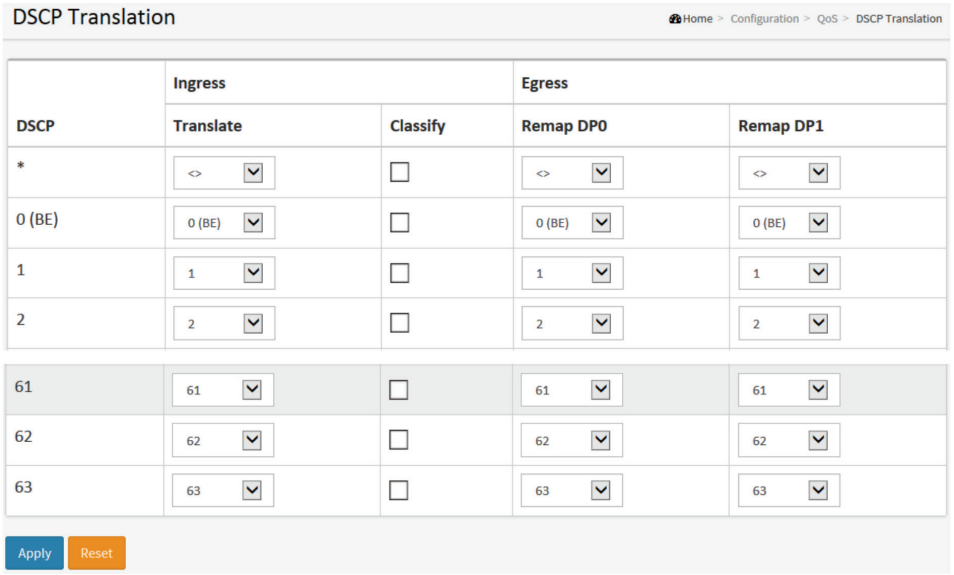



FIGURE 3-87. DSCP TRANSLATION CONFIGURATION SCREEN

**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 the Ingress side.

- Egress: There are the following configurable parameters for Egress side.

1. Remap DP0: Select the DSCP value you want to remap from. DSCP values range from 0 to 63.
2. Remap DP1: Select the DSCP value from select menu to which you want to remap. DSCP values range from 0 to 63.

- Remap: Select the DSCP value from the menu to which you want to remap. DSCP values range from 0 to 63.

- Buttons:

- Apply – Click to save changes.

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

- Auto-refresh: Select the auto-refresh icon and the device will refresh the information automatically.
- Upper right icon (Refresh): Click to refresh the DSCP Translation information manually.

## 3.18.9 DSCP CLASSIFICATION

The section describes how to configure and map a DSCP value to a QoS Class and DPL value. 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, DSCP Translation.
2. Scroll to set the DSCP Parameters.
3. Click save to save the setting.
4. To cancel the setting, click the Reset button. It will revert to previously saved values.

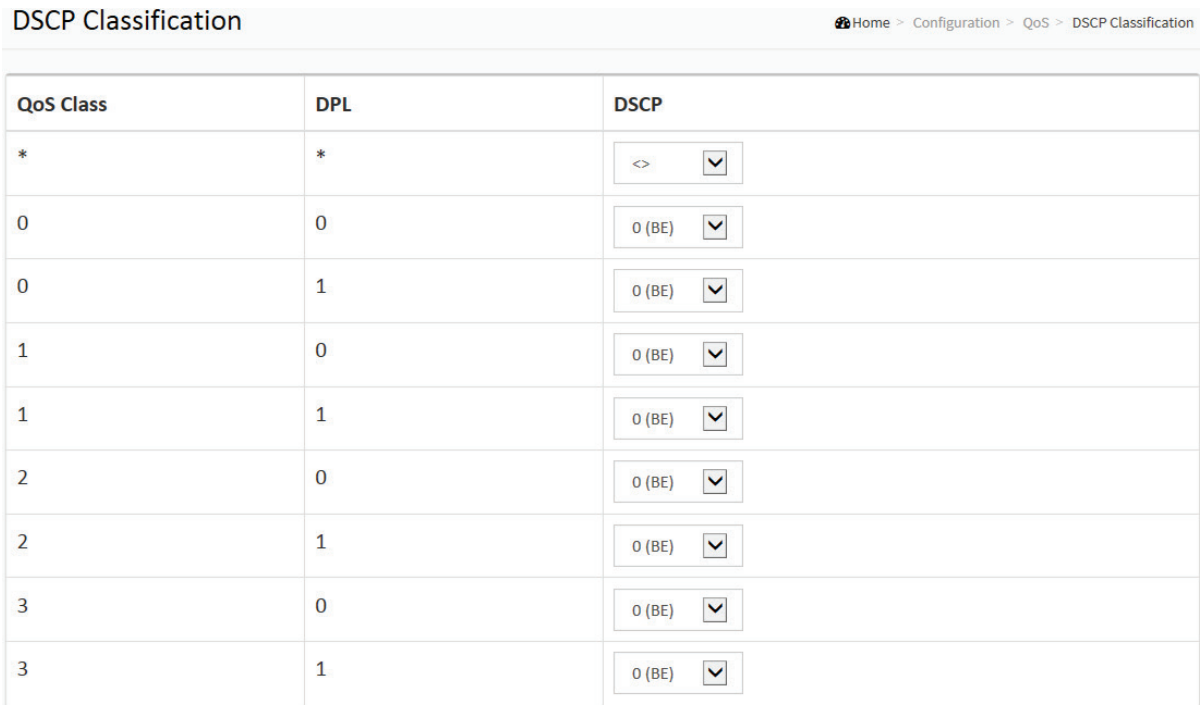



FIGURE 3-88. DSCP CLASSIFICATION CONFIGURATION SCREEN

**Parameter description:**

- QoS Class: Available QoS Class values range from 0 to 7. QoS Class (0–7) can be mapped to parameters.
- DPL: Drop Precedence Level (0-1) can be configured for all available QoS Classes.
- DSCP: Select DSCP value (0–63) from the DSCP menu to map DSCP to the corresponding QoS Class and DPL value.
- Buttons:

- Apply – Click to save changes.

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

- Auto-refresh: Select the auto-refresh icon and the device will refresh the information automatically.
- Upper right icon (Refresh): Click to refresh the DSCP Translation information manually.

## 3.18.10 DSCP CLASSIFICATION

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, QoS Control List.
2. Click the + sign to add a new QoS Control List.
3. Scroll all parameters and enable the Port Member to join the QCE rules.
4. Click save to save the setting.
5. To cancel the setting, click the Reset button. It will revert to previously saved values.

FIGURE 3-89. QOS CONTROL LIST CONFIGURATION SCREEN

**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 values 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 aningress 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.

circle e: Edits the QCE.

up-arrow: Moves the QCE up the list.

down-arrow: Moves the QCE down the list.

x: Deletes the QCE.

+: The lowest plus sign adds a new entry at the bottom of the QCE listings.

- Port Members: Check the checkbox button to make any port a member of the QCL entry. By default, all ports will be checked.
- Key Parameters: Key configuration are described next.

- Tag Value of Tag field can be 'Any', 'Untag' or 'Tag'

- VID Valid value of VLAN ID can be any value in the range 1–4095 or 'Any'; user can enter either a specific value or a range of VIDs

- 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 values of DEI can be any of values between 0, 1 or 'Any'

- SMAC Source MAC address: 24 MS bits (OUI) or 'Any'

- DMAC Type Destination MAC type: possible values are unicast (UC), multicast (MC), broadcast (BC) or 'Any'

- Frame Type: Frame Type can have any of the following values.

1. Any
2. Ethernet
3. LLC
4. SNAP
5. IPv4
6. IPv6

Frame type descriptions are listed below.

1. Any : Allow all types of frames.

2. Ethernet : Ethernet Type: Valid ethernet types can have values 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): This can be a specific value or 'Any'. DSCP values are in the range 0–63, including BE, CS1-CS7, EF or AF11-AF43 .

P 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): This can be a 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)
- Buttons:

- Apply – Click to save changes.

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

## 3.18.11 STORM CONTROL

This section explains how to configure the Storm control for the switch. There is a unicast storm rate control, multicast storm rate control, and a broadcast storm rate control. These only affect flooded frames, i.e. frames with a (VLAN ID, DMAC) pair not present on the MAC Address table. The configuration indicates the permitted packet rate for unicast, multicast, or broadcast traffic across the switch.

### WEB INTERFACE

To configure the Storm Control Configuration parameters in the web interface:

1. Click Configuration, QoS, Storm Control Configuration.
2. Select the frame type to enable storm control.
3. Scroll to set the Rate Parameters.
4. Click save to save the setting.
5. To cancel the setting, click the Reset button. It will revert to previously saved values.

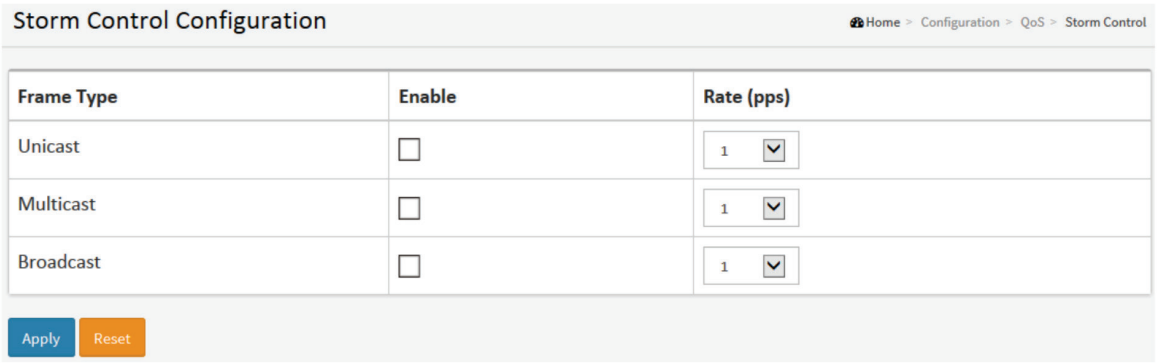



FIGURE 3-90. STORM CONTROL CONFIGURATION SCREEN

**Parameter description:**

- Frame Type: The settings in a particular row apply to the frame type listed here: Unicast, Multicast, or Broadcast.
- Enable: Enable or disable the storm control status for the given frame type.
- Rate: The rate unit is packets per second (pps). Valid values are: 1, 2, 4, 8, 16, 32, 64, 128, 256, 512, 1K, 2K, 4K, 8K, 16K, 32K, 64K, 128K, 256K, 512K or 1024K. , 1024K, 2048K, 4096K, 8192K, 16384K or 32768K. , 1024K, 2048K, 4096K, 8192K, 16384K or 32768K.

**NOTE**: The 1 kpps is actually 1002.1 pps.

- Buttons:

- Apply – Click to save changes.

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

## 3.19 MIRROR

You can mirror traffic from any source port to a target port for real-time analysis. You can then attach a logic analyzer or RMON probe to the target port and study the traffic crossing the source port in a completely unobtrusive manner.

Mirror Configuration monitors the traffic of the network. For example, we assume that Port A and Port B are Monitoring Port and Monitored Port respectively, thus, the traffic received by Port B will be copied to Port A for monitoring.

### WEB INTERFACE

To configure the Mirror in the web interface:

1. Click Configuration, Mirroring.
2. Scroll to select the Port to mirror on which port.
3. Scroll to disabled, enable, TX Only, and RX Only to set the Port mirror mode.
4. Click save to save the setting.
5. To cancel the setting. click the Reset button. It will revert to previously saved values.

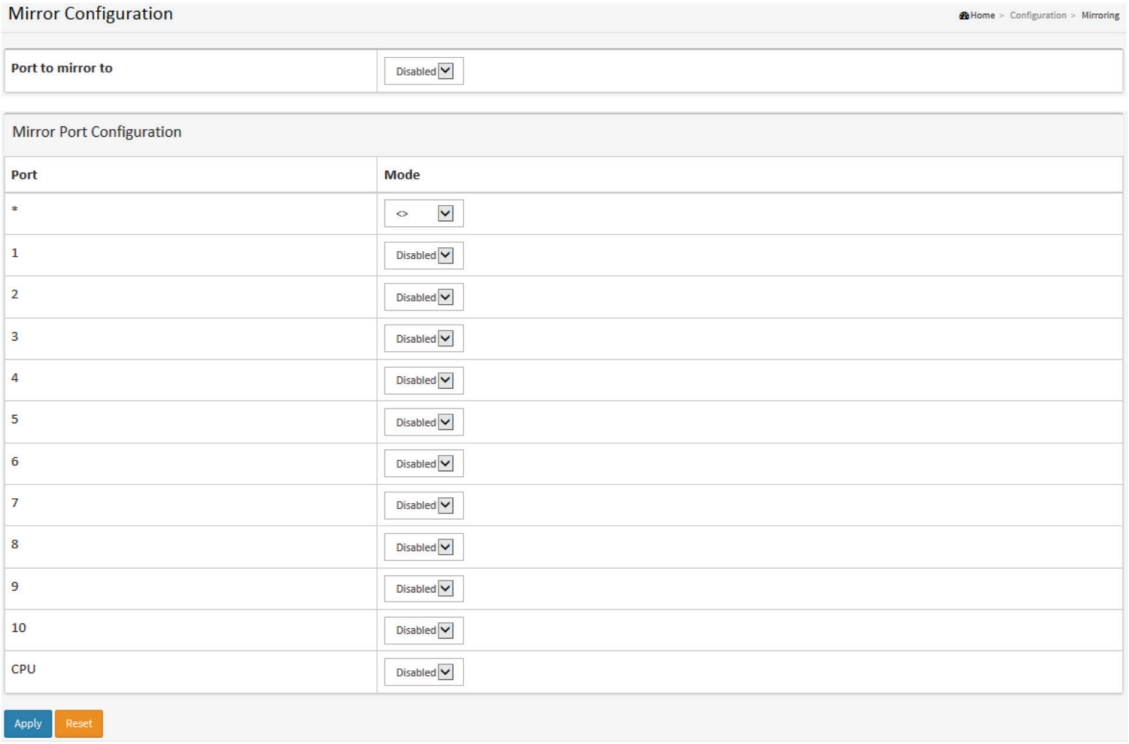



FIGURE 3-91. MIRROR CONFIGURATION SCREEN

**Parameter description:**

- Port to mirror on: Port to mirror is also known as the mirror port. Frames from ports that have either source (rx) or destination (tx) mirroring enabled are mirrored on this port. Disabled disables mirroring.

**Mirror Port Configuration**

- Port: The logical port for the settings contained in the same row.
- Mode: Select mirror mode.
- Rx only: Frames received on this port are mirrored on the mirror port. Frames transmitted are not mirrored.
- Tx only: Frames transmitted on this port are mirrored on the mirror port. Frames received are not mirrored.
- Disabled: Neither frames transmitted nor frames received are mirrored.
- Enabled: Frames received and frames transmitted are mirrored on the mirror port.

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

- Buttons:

- Apply – Click to save changes.

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

## 3.20 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, UPnP.
2. Scroll to select the mode to enable or disable.
3. Specify the parameters in each blank field.
4. Click save to save the setting.
5. To cancel the setting, click the Reset button. It will revert to previously saved values.

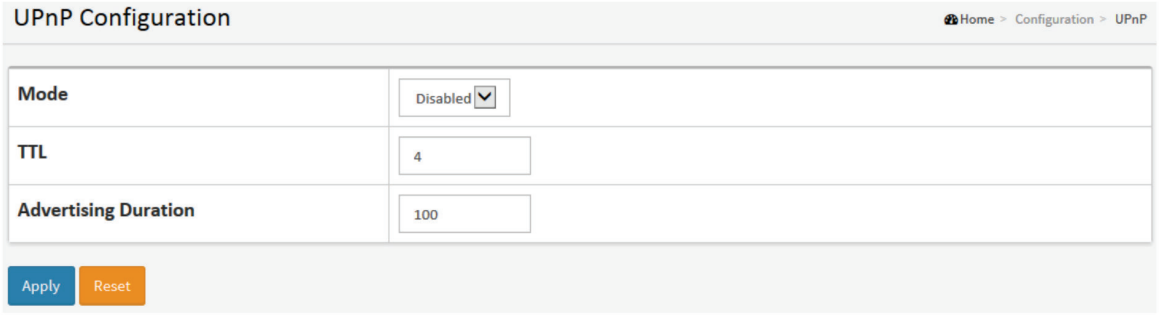



FIGURE 3-92. UPNP CONFIGURATION SCREEN

**Parameter description:**

These parameters are displayed on the UPnP Configuration page:

- 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. Because of the unreliable nature of UDP, in the standard it is recommended that 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.

## 3.21 GVRP

The Generic Attribute Registration Protocol (GARP) provides a generic framework in which devices in a bridged LAN, e.g. end stations and switches, can register and de-register attribute values, such as VLAN Identifiers, with each other. In doing so, the attributes are propagated to devices in the bridged LAN, and these devices form a “reachability” tree that is a subset of an active topology. GARP defines the architecture, rules of operation, state machines, and variables for the registration and de-registration of attribute values.

A GARP participation in a switch or an end station consists of a GARP application component, and a GARP Information Declaration (GID) component associated with each port or the switch. The propagation of information between GARP participants for the same application in a bridge is carried out by the GARP Information Propagation (GIP) component. Protocol exchanges take place between GARP participants by means of LLC Type 1 services, using the group MAC address and PDU format defined for the GARP application concerned.

### 3.21.1 GLOBAL CONFG

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.

You can also store up to two other files and apply them to running-config, thereby switching configuration.

## WEB INTERFACE

To configure the GVRP in the web interface:

1. Click Configuration, GVRP, Global Config.
2. Specify Join-time, Leave-time, Leave All-time, Max VLANs.
3. Click Apply.

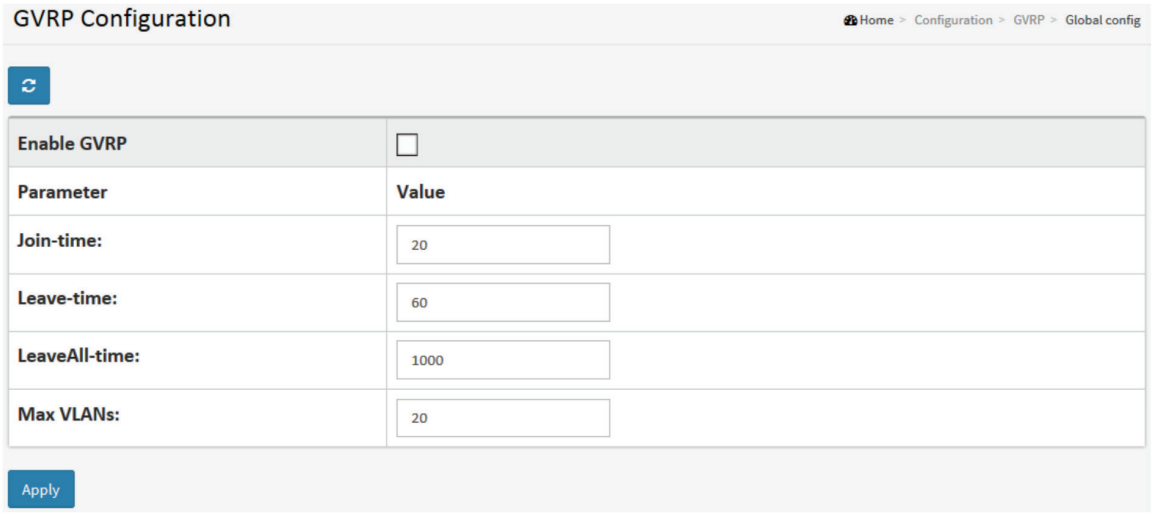



FIGURE 3-93. GVRP CONFIGURATION SCREEN

**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 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 units of centi seconds, i.e. in units of one hundredth of a second.The default is 60.

LeaveAll-time is a value in the range 1000-5000 in 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.

## 3.21.2 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 sFlow Agent in the web interface:

1. Click Configuration, GVRP, Port Config.
2. Specify Port, mode.
3. Click Apply.

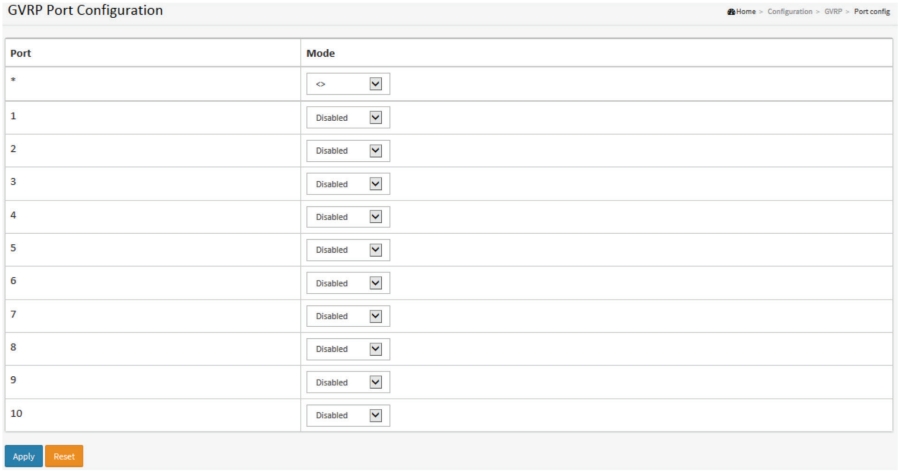



FIGURE 3-94. GVRP CONFIGURATION SCREEN

**Parameter description:**

- GVRP Mode

This configuration is to enable/disable GVRP Mode on a particular port locally.

- Disable: Select to Disable GVRP mode on this port.
- Enable: Select to Enable GVRP mode on this port.

## 3.22 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 saved to non-volatile memory, which means that a reboot or master change will disable sFlow sampling.

### WEB INTERFACE

To configure the sFlow Agent in the web interface:

1. Click Configuration, sFlow.
2. Set the parameters.
3. Click save to save the setting.
4. To cancel the setting, click the Reset button. It will revert to previously saved values.

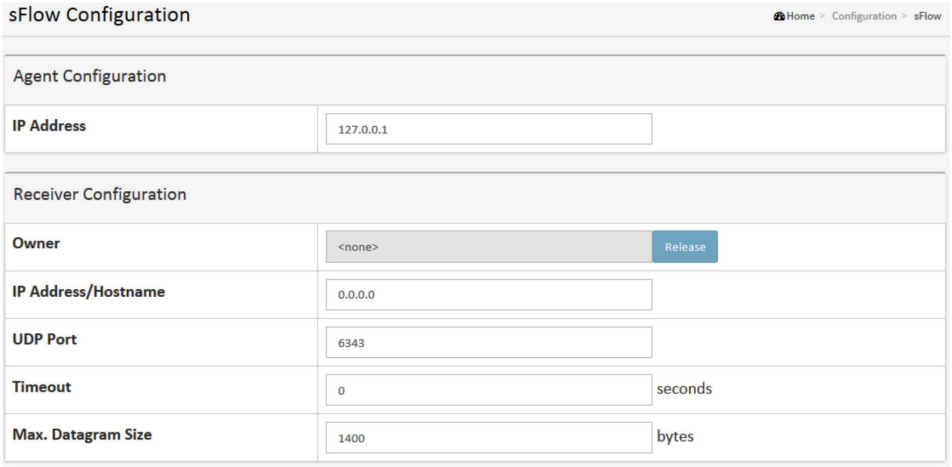



FIGURE 3-95. SFLOW CONFIGURATION SCREEN

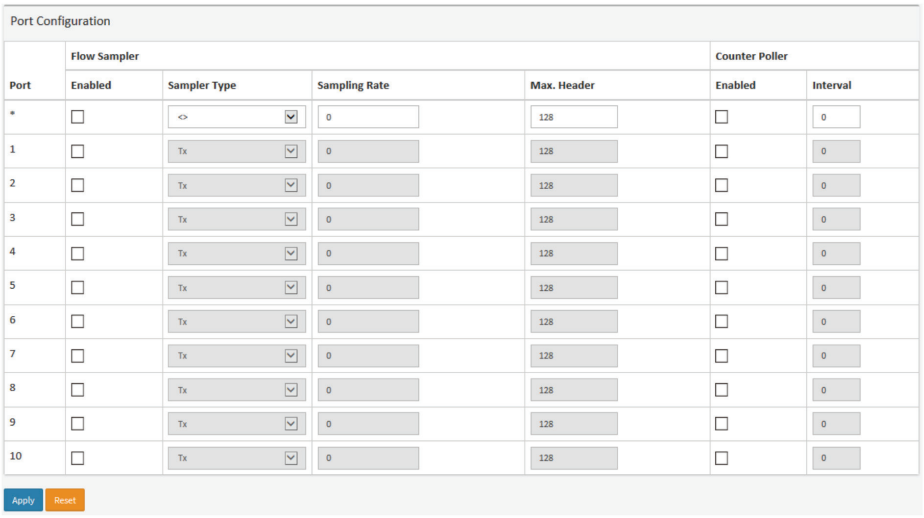



FIGURE 3-96. PORT CONFIGURATION SCREEN

**Parameter description:**

**Agent Configuration**

- IP Address: The IP address is used as an 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: sFlow can be configured in two ways: through local management using the Web or CLI interface or through SNMP. This read-only field shows the owner of the current sFlow configuration and assumes values as follows"
- If sFlow is currently unconfigured/unclaimed, Owner contains <none>.
- If sFlow is currently configured through Web or CLI, Owner contains <Configured through local management>.
- If sFlow is currently configured through SNMP, Owner contains a string identifying the sFlow receiver.

If sFlow is configured through SNMP, all controls—except for the Release-button—are disabled to avoid inadvertent reconfiguration.

The button allows for releasing the current owner and disable sFlow sampling. The button is disabled if sFlow is currently unclaimed. If configured through SNMP, the release must be confirmed (a confirmation request will appear).

- IP Address/Hostname: The IP address or hostname of the sFlow receiver. Both IPv4 and IPv6 addresses are supported.
- UDP Port: The UDP port on which the sFlow receiver listens to sFlow datagrams. If set to 0 (zero), the default port (6343) is used.
- Timeout: The number of seconds remaining before sampling stops and the current sFlow owner is released. While active, the current time left can be updated with a click on the Refresh-button. If locally managed, the timeout can be changed on the fly without affecting any other settings.
- 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 of 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.

## 3.23 SWITCH2GO

### 3.23.1 SWITCH2GO SETTING

Configure Switch2go management and link setting.

#### WEB INTERFACE

To configure Switch2go setting in the web interface:

1. Click Configuration, Switch2go, and and Switch2go setting.
2. Set the parameters.
3. Click Apply.

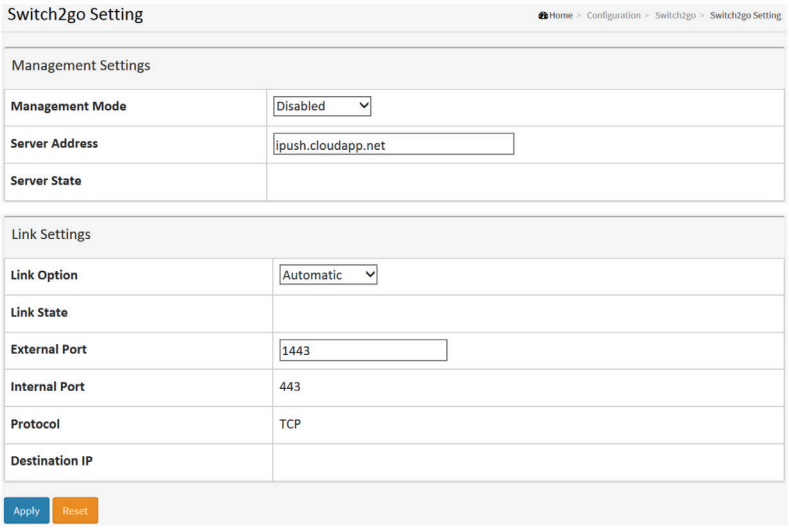



FIGURE 3-97. SWITCH2GO SETTING SCREEN

**Parameter description:**

- Management mode: Indicates the Management mode operation. When the mode operation is enabled, the message will send out to (or get from) the server. The protocol is based on TCP communication and received on TCP port 443 and the server will send acknowledgments/information back to the sender since TCP is a connection-oriented protocol. Possible modes are:

- Enabled: Enable Switch2go Management mode operation.

- Disabled: Disable Switch2go Management mode operation.

- Server Address: Indicates the IPv4 host address of the server. If the switch provides the DNS feature, it also can be a host name.
- Server State: Report network information between the Switch and Server.
- Link Option: Indicates the Link Option operation.

When the Link Option is Automatic, enabling applications access the services provided by an UPnP “Internet Gateway Device (IGN)” present on the network.

When the Link Option is Manual, you should set Setting External Port and Your IGN/NAT’s Port Forward function manually.

When Link function is working successfully, Mobile(s) can access this NAT by Internet.

Possible modes are:

- Automatic: Link Option is Automatic.

- Manual: Link Option is Manual.

- Link State: Report network information between the Switch and the Internet Gateway Device (IGN).
- External Port: When the Link Option is Manual, you should Set the External Port manually.
- Internal Port: Information about the Switch Client's Internal Port.
- Protocol: Information about the Switch Client's Protocol.
- Destination IP: Information about the Client's Destination IP.

## 3.23.2 USER LINK MANAGEMENT

Configure User Link Management on this page.

### WEB INTERFACE

To configure User Link Management in the web interface:

1.Click Configuration, Switch2go, and and User Link Management.

2. Set the parameters.

3. Click Get Activity Code.

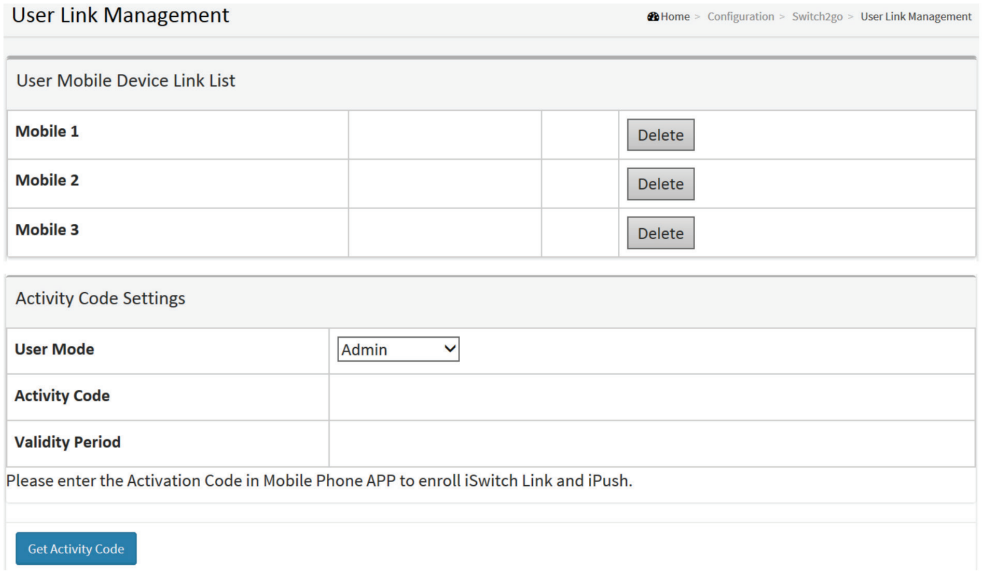



FIGURE 3-98. USER LINK MANAGEMENT SCREEN

**Parameter description:**

- Mobile 1–3: Information about the mobile devices that can access this switch.
- User Mode: Assign This Activity Code Privilege Level.
- Activity Code: The Activity Code to register the mobile device to the Switch2go Setting Server.
- Validity Period: The expiration time of the Activity Code.
- Get Activity Code : Click to Get Activity Code and enter the Activation Code in Mobile Phone APP to enroll iSwitch and iPush.

## 3.23.3 PORT NAME SERVICE

This page displays the current port name and role.

### WEB INTERFACE

To configure Port Name Service in the web interface:

1. Click Configuration, Switch2go and and Port Name Servic
2. Specify the detail Port Name and set the Role.
3. Click Apply.

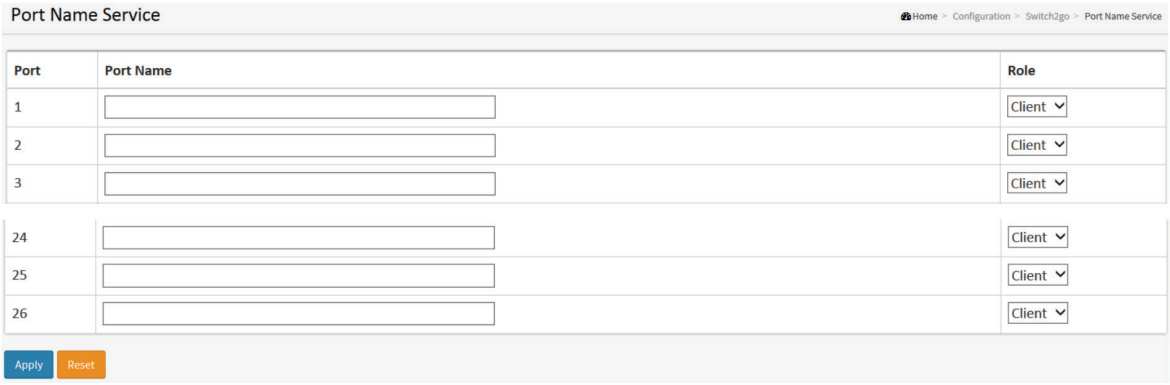



FIGURE 3-99. USER LINK MANAGEMENT SCREEN

Parameter description:

- Port: This is the logical port number for this row.
- Port Name: Enter up to 47 characters to be a descriptive name that identifies this port.
- Role: Selects any available role for the given switch port. Possible roles are:

- Server - Assign this as a Server Port.

- Client - Assign this as a Client Port.

## 3.24 SMTP CONFIGURATION

The function is used to set an Alarm trap for the SMTP server to send you an 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 Apply to save the setting.
5. To cancel the setting, click the Reset button. It will revert to previously saved values.

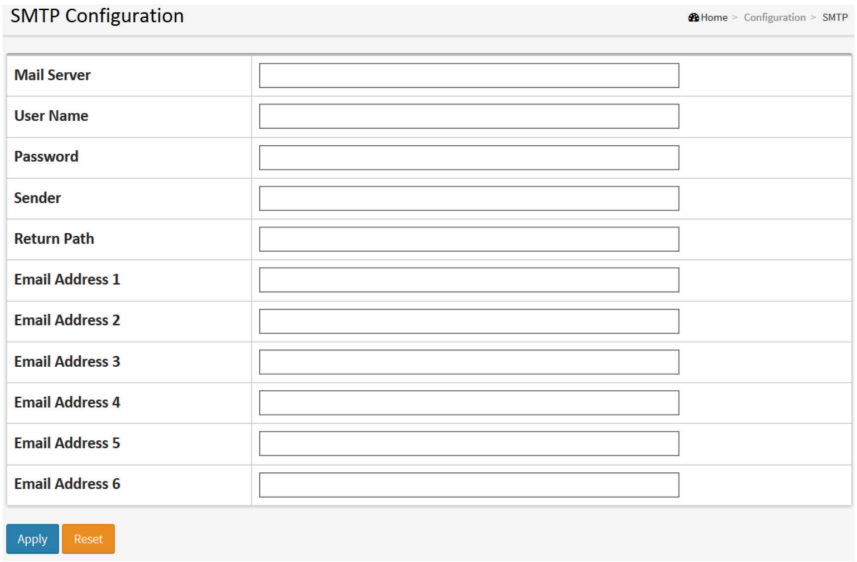



FIGURE 3-100. SMTP CONFIGURATION SCREEN

Parameter description:

These parameters are displayed on the SMTP Configuration page:

- Mail Server: The IP address or hostname of the mail server. The IP address is expressed in dotted decimal notation. This will be the device that sends out the mail for you.
- User name: Specify the username on the mail server.
- Password: Specify the password on the mail server.
- Sender : Specify the sender name of the alarm mail.
- Return-Path: Specify the sender email address of the alarm mail. This address will be the “from” address on the email message.
- Email Address 1-6: Email address that will 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 4: MONITOR

This chapter describes all of the basic network statistics, including Ports, Layer 2 network protocol (e.g. NAS, ACL, DHCP, AAA, and RMON etc.) and any switch settings.

## 4.1 SYSTEM

After you login, the switch shows you the system information. This page is the 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”, and “Device Port”. With this information, you will know the software version used, MAC address, serial number, how many ports are good and so on. This is helpful if the switch malfunctions.

### 4.1.1 INFORMATION

The switch system information is provided here.

#### WEB INTERFACE

To configure 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 button.

System Information

Home > Monitor > System > Information

| | |
|---|---|
| Model Name | |
| System Description | |
| Location | |
| Contact | |
| System Name | |
| System Date | 2011-01-01T02:10:49+00:00 |
| System Uptime | 02:10:49 |
| Bootloader Version | v1.17 |
| Firmware Version | v6.06 2014-11-21 |
| Hardware Version | v1.01 |
| Mechanical Version | v1.01 |
| Serial Number | A053114AR4800002 |
| MAC Address | 00-40-c7-1c-a8-93 |
| Memory | Total=93573 KBytes, Free=83321 KBytes, Max=83321 KBytes |
| FLASH | 0x40000000-0x41ffffff, 512 x 0x10000 blocks |

FIGURE 4-1. SYSTEM INFORMATION SCREEN

Parameter description:

- Model Name: Displays the factory defined model name for identification purposes.
- 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.
- Platform Name: Displays the user-defined system name 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 operating.
- Bootloader Version: Displays the current boot loader version number.
- Firmware Version: The software version of this switch.
- Hardware-Mechanical Version: The hardware and mechanical version of this switch.
- Series Number: The serial number of this switch.
- MAC Address: The MAC Address of this switch.
- Memory: Displays the memory size of the system.
- FLASH: Displays the flash size of the system.

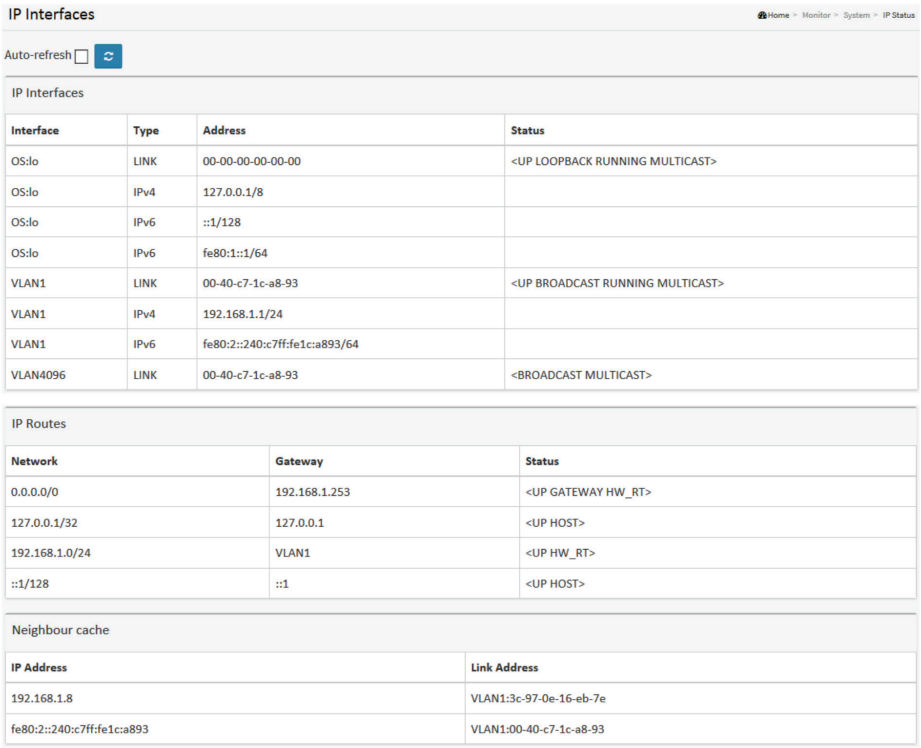
## 4.1.2 IP STATUS

This page displays the status of the IP protocol layer. The status is defined by the IP interfaces, the IP routes, and the neighbor 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 |
|---|---|---|---|
| OS:lo | LINK | 00-00-00-00-00-00 | <UP LOOPBACK RUNNING MULTICAST> |
| OS:lo | IPv4 | 127.0.0.1/8 | |
| OS:lo | IPv6 | ::1/128 | |
| OS:lo | IPv6 | fe80:1::1/64 | |
| VLAN1 | LINK | 00-40-c7-1c-a8-93 | <UP BROADCAST RUNNING MULTICAST> |
| VLAN1 | IPv4 | 192.168.1.1/24 | |
| VLAN1 | IPv6 | fe80:2::240:c7ff:fe1c:a893/64 | |
| VLAN4096 | LINK | 00-40-c7-1c-a8-93 | <BROADCAST MULTICAST> |

IP Routes

| Network | Gateway | Status |
|---|---|---|
| 0.0.0.0/0 | 192.168.1.253 | <UP GATEWAY HW_RT> |
| 127.0.0.1/32 | 127.0.0.1 | <UP HOST> |
| 192.168.1.0/24 | VLAN1 | <UP HW_RT> |
| ::1/128 | ::1 | <UP HOST> |

Neighbour cache

| IP Address | Link Address |
|---|---|
| 192.168.1.8 | VLAN1:3c-97-0e-16-eb-7e |
| fe80:2::240:c7ff:fe1c:a893 | VLAN1:00-40-c7-1c-a8-93 |

FIGURE 4-2. IP STATUS SCREEN

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.

Neighbor 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 exists.

- Buttons:

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

- Refresh: Click to refresh the page immediately.

## 4.1.3 LOG

This section describes the switch's system log information.

### WEB INTERFACE

To display the log configuration in the web interface:

1. Click Monitor, System, and Log.
2. Display the log information.

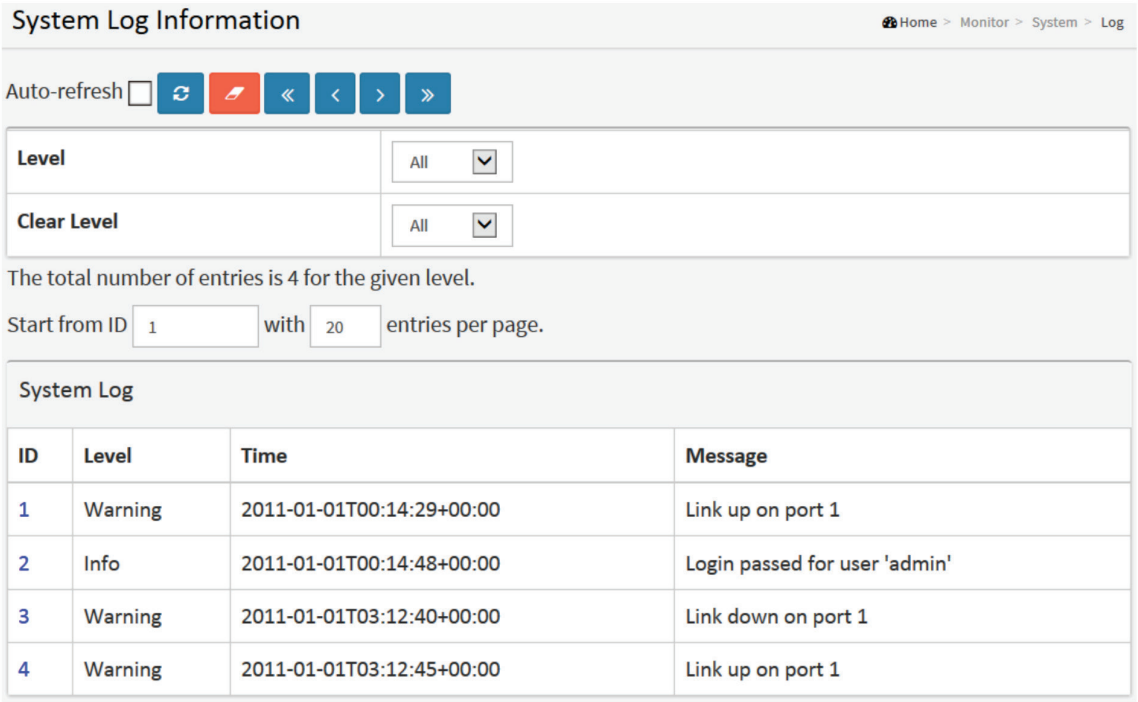



FIGURE 4-3. SYSTEM LOG INFORMATION SCREEN

Parameter description:

- Auto-refresh: Click the auto-refresh icon and the device will refresh the log automatically.
- Level: This is the level of the system log entry. Two types are supported: Warning and Error.

- Warning: Warning level of the system log.

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

- ID: ID (>= 1) of the system log entry.
- Time: This will display the log record by device time. The time of the system log entry.
- Message: This will display the log detail message. The message of the system log entry.
- Buttons:

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

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

- Clear: Clears the selected log entries.

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

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

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

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

## 4.1.4 DETAILED LOG

This section describes that the detailed log information of the switch.

### WEB INTERFACE

To display the detailed log configuration in the web interface:

1. Click Monitor, System, and Detailed Log.
2. Display the log information.

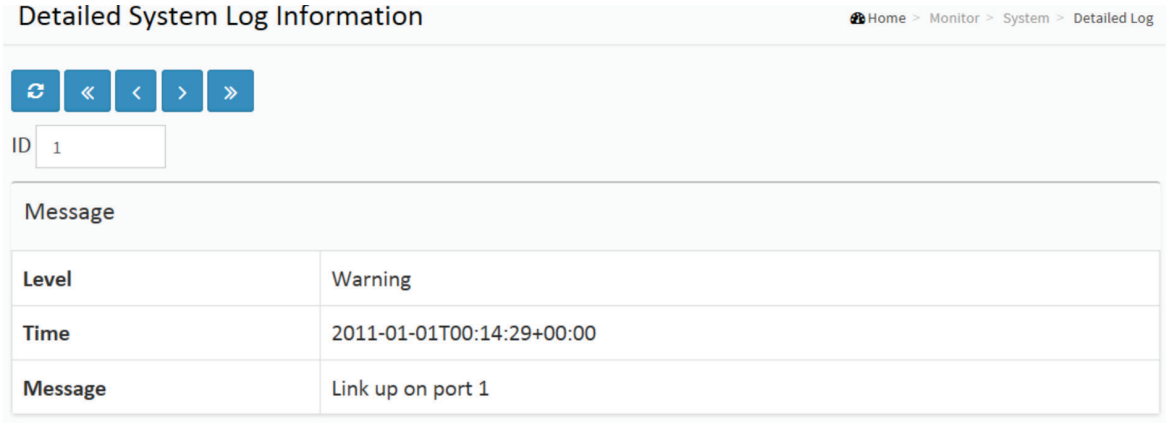



FIGURE 4-4. DETAILED SYSTEM LOG INFORMATION SCREEN

Parameter description:

- ID: The ID (>= 1) of the system log entry.
- Message: The detailed message of the system log entry.
- Upper right icon (Refresh, clear...): Click to refresh the system log or clear manually, go to next/up page or entry.
- Buttons:

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

|<<: Updates the system log entries 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.

## 4.2 GREEN ETHERNET

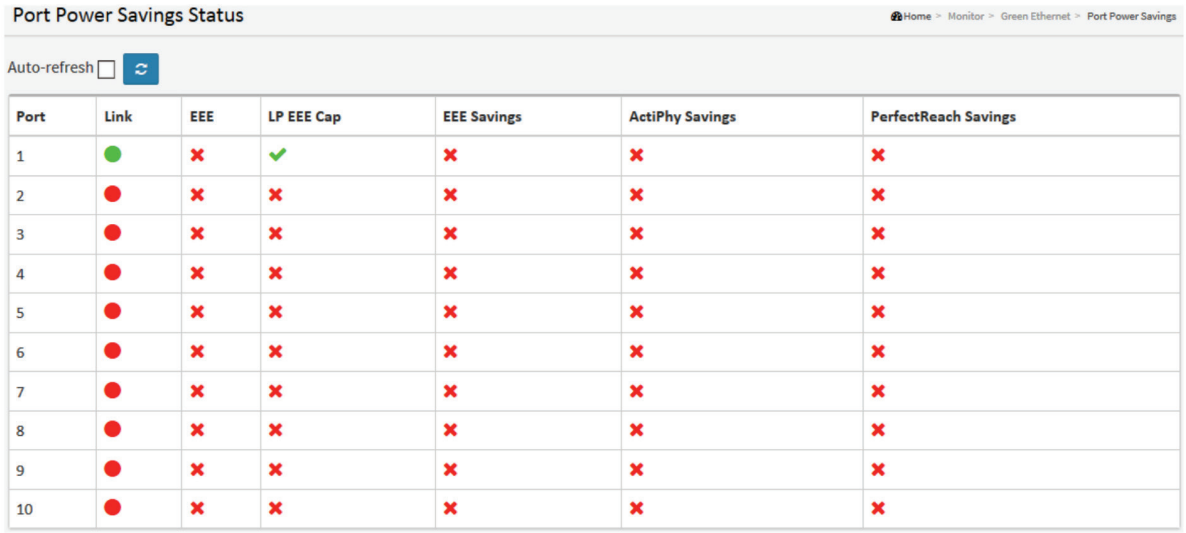
### 4.2.1 DETAILED LOG

This page provides the current status for EEE.

### WEB INTERFACE

To display the power Saving in the web interface:

1. Click Monitor, Port Power Savings.




| Port | Link | EEE | LP EEE Cap | EEE Savings | ActiPhy Savings | PerfectReach Savings |
|---|---|---|---|---|---|---|
| 1 | ● | ✖ | ✔ | ✖ | ✖ | ✖ |
| 2 | ● | ✖ | ✖ | ✖ | ✖ | ✖ |
| 3 | ● | ✖ | ✖ | ✖ | ✖ | ✖ |
| 4 | ● | ✖ | ✖ | ✖ | ✖ | ✖ |
| 5 | ● | ✖ | ✖ | ✖ | ✖ | ✖ |
| 6 | ● | ✖ | ✖ | ✖ | ✖ | ✖ |
| 7 | ● | ✖ | ✖ | ✖ | ✖ | ✖ |
| 8 | ● | ✖ | ✖ | ✖ | ✖ | ✖ |
| 9 | ● | ✖ | ✖ | ✖ | ✖ | ✖ |
| 10 | ● | ✖ | ✖ | ✖ | ✖ | ✖ |

FIGURE 4-5. PORTS STATES SCREEN

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 µsec.
- Actiphy Savings: Shows if the system is currently saving power due to ActiPhy.
- PerfectReach Savings: Shows if the system is currently saving power due to PerfectReach.

## 4.3 PORTS

The section describes how to configure the Port detail parameters of the switch. You can use the Port configure to enable or disable the Port of the switch. Monitor the ports content or status in the function.

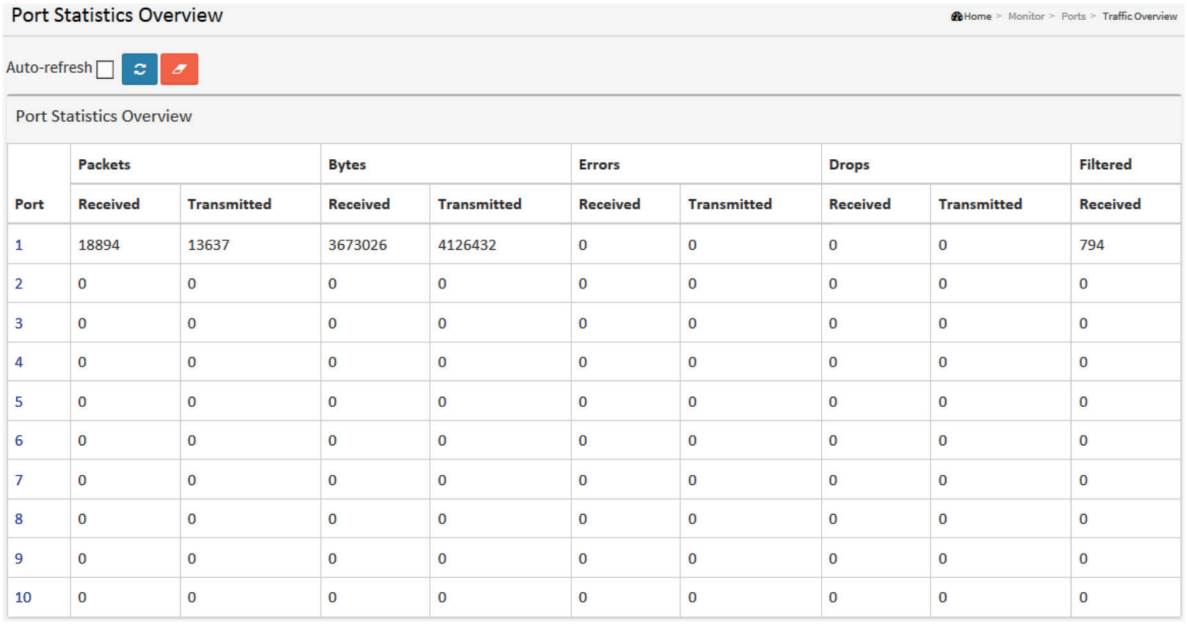
### 4.3.1 TRAFFIC OVERVIEW

The section describes 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, then Traffic Overview.
2. To auto-refresh, click on “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 | 18894 | 13637 | 3673026 | 4126432 | 0 | 0 | 0 | 0 | 794 |
| 2 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 3 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 4 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 5 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 6 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 7 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 8 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 9 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 10 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |

FIGURE 4-6. PORT STATISTICS OVERVIEW SCREEN

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: Clears the counters for all ports.

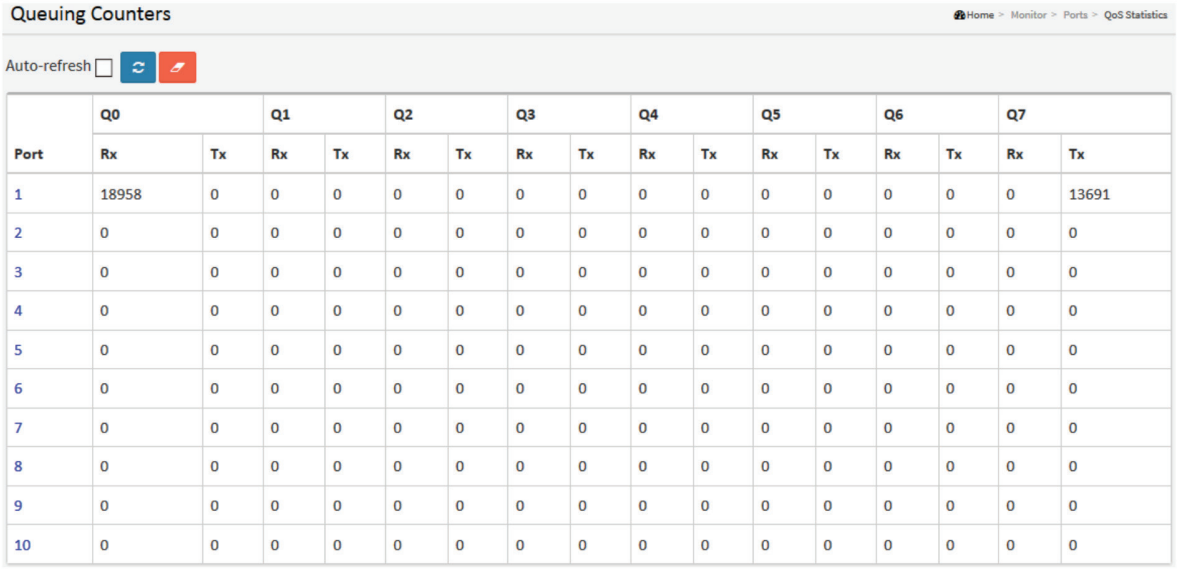
## 4.3.2 QOS STATISTICS

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

### WEB INTERFACE

To Display the Queuing Counters in the web interface:

1. Click Monitor, Ports, then QoS Statistics.
2. To auto-refresh the information, click Auto-refresh.
3. Click Refresh to refresh the Queuing Counters or click Clear to clear all information.




| | 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 | 18958 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 13691 |
| 2 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 3 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 4 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 5 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 6 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 7 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 8 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 9 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 10 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |

FIGURE 4-7. QUEUING COUNTERS OVERVIEW SCREEN

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: Clears the counters for all ports.

## 4.3.3 QCL STATUS

The section explains how to configure and show the QCL status for 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, then QCL Status.
2. To auto-refresh the information, click Auto-Refresh.
3. Scroll to select the combined, static, Voice VLAN, and conflict.
4. Click the" Refresh" to refresh a entry of the MVR Statistics Information.

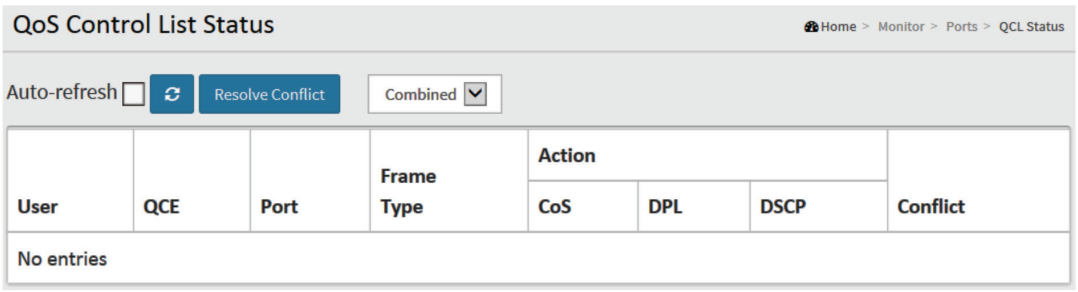



FIGURE 4-8. QOS CONTROL LIST STATUS SCREEN

Parameter description:

- User: Indicates the QCL user.
- QCE#: Indicates the index of QCE.
- Frame Type: Indicates the type of frame to look for incoming frames. Possible frame types are:

- Any: The QCE will match all frame types.
- Ethernet: Only Ethernet frames (with Ether Type 0x600-0xFFFF) are allowed.
- LLC: Only (LLC) frames are allowed
- LLC: Only (SNAP) frames are allowed.
- IPv4: The QCE will match only IPV4 frames.
- IPv6: The QCE will match only IPV6 frames.

• Port: Indicates the list of ports configured with the QCE.

- Action: Indicates the classification action taken on an 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 the DP level will be 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. Resources required to add a QCE may not available; in that case it shows conflict status as Yes, otherwise it is always No.

NOTE: Conflict can be resolved by releasing the H/W resources required to add a QCL entry on pressing the Resolve Conflict button.

- Buttons:

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

- Resolve Conflict: Click to release the resources required to add a QCL entry if conflict status for any QCL entry is yes.

- Refresh: Click to refresh the page.

## 4.3.4 DETAILED STATISTICS

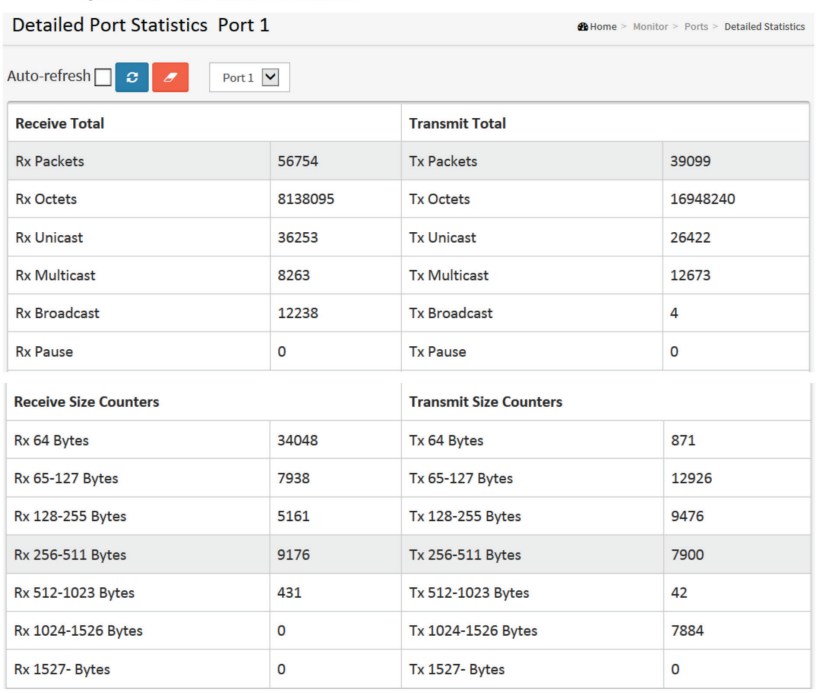
The section describes how to provide detailed traffic statistics for a specific switch port. Use the port select box to select which switch port details to display.

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, then 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".




| 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 |

FIGURE 4-9. DETAILED PORT STATISTICS SCREEN

| 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 4-10. RECEIVE QUEUE COUNTERS SCREEN

Parameter description:

- Auto-refresh: Click Auto-Refresh to refresh the Port Statistics information automatically.
- Upper left scroll bar: To scroll a port to display the Port statistics with “Port-0”, “Port-1...

Receive Total and Transmit Total

- Rx and Tx Packets: The number of received and transmitted (good and bad) packets.
- Rx and Tx Octets: The number of received and transmitted (good and bad) bytes. Includes FCS, but excludes framing bits.
- Rx and Tx Unicast: The number of received and transmitted (good and bad) unicast packets.
- Rx and Tx Multicast: The number of received and transmitted (good and bad) multicast packets.
- Rx and Tx Broadcast: The number of received and transmitted (good and bad) broadcast packets.
- Rx and Tx Pause: A count of the MAC Control frames received or transmitted on this port that have an opcode 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.
- Auto-refresh: Click on Auto-refresh to refresh the Queuing Counters automatically.
- Upper right icon (Refresh, clear): Click to refresh the Port Detail Statistics or clear manually.
- Buttons:

- Auto-refresh: Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.
- Clear: Clears the counters for the selected port.
- Refresh: Click to refresh the page.

## 4.3.5 SFP INFORMATION

The section describes how to display information for the SFP module connected to the switch. The information includes: Connector type, Fiber type, wavelength, baud rate and Vendor OUI etc.

### WEB INTERFACE

To display the SFP information in the web interface:

1. Click Monitor, then SFP Informatio.
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 4-11. SFP INFORMATION OVERVIEW SCREEN

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 optic transmitting central wavelength, for instance, 850 nm, 1310 nm, 1550 nm, and so on.
- Baud Rate: Display the maximum baud rate of the fiber module supported, for instance, 10M, 100M, 1G, and so on.
- Vendor OUI: Display the OUI code assigned by IEEE.
- Vendor Name: Display the company name of the module manufacturer.
- Vendor P/N: Display the module part number.
- Vendor Revision: Display the module revision.
- Vendor 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.

## 4.4 DHCP

### 4.4.1 SERVER

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

#### 4.4.1.1 STATISTICS

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

#### WEB INTERFACE

- Display the DHCP server Statistics Overview in the web interface:
- Click Protocol -based VLAN configuration and add new entry.

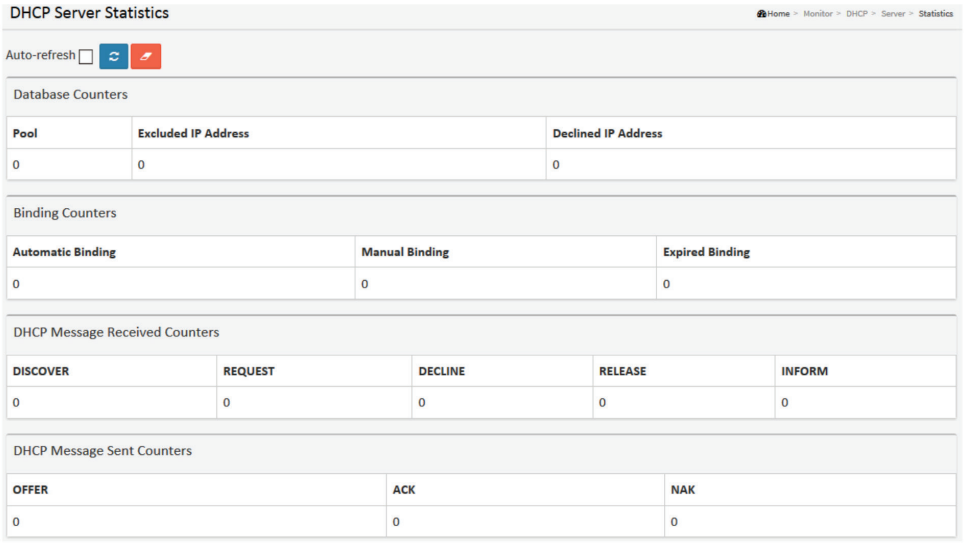



FIGURE 4-12. PROTOCOL TO GROUP MAPPING TABLE SCREEN

Parameter description:

Database Counters

- Pool: Number of pools.
- Excluded IP Address: Number of excluded IP address ranges.
- Declined IP Address: Number of declined IP addresses.

Database Counters

- Automatic Binding: Number of bindings with network-type pools.
- Manual Binding: Number of bindings that an administrator assigns an IP address to a client. The pool is host type.
- Expired Binding: Number of bindings with lease time expired or cleared from Automatic/Manual type bindings.

DHCP Message Received Counters

- DISCOVER: Number of DHCP DISCOVER messages received.
- REQUEST: Number of DHCP REQUEST messages received.
- DECLINE: Number of DHCP DECLINE messages received.
- RELEASE: Number of DHCP RELEASE messages received.
- INFORM: Number of DHCP INFORM messages received.

DHCP Message Sent Counters

- OFFER: Number of DHCP OFFER messages sent.
- ACK: Number of DHCP ACK messages sent.
- NAK: Number of DHCP NAK messages sent.

## 4.4.1.2 BINDING

This page displays bindings generated for DHCP clients.

### WEB INTERFACE

To Display DHCP Server Binding IP in the web interface:

Click DHCP, Server, and Binding.

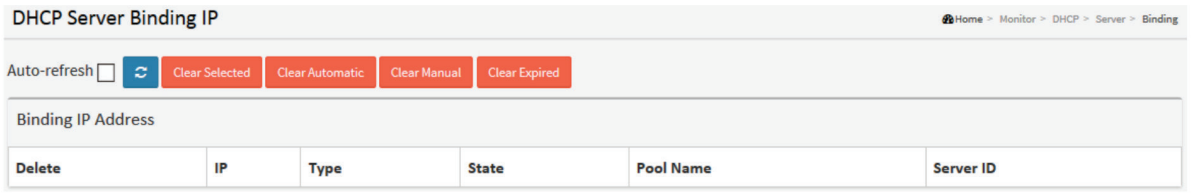



FIGURE 4-13. GROUP NAME OF VLAN MAPPING TABLE

- IP: IP address allocated to DHCP client.
- Type: Type of binding. Possible types are Automatic, Manual, Expired.
- State: State of binding. Possible states are Committed, Allocated, Expired.
- Pool Name: The pool that generates the binding.
- Server ID: Server IP address to service the binding.

### 4.4.1.3 DECLINED IP

This page displays declined IP addresses.

#### WEB INTERFACE

To Display DHCP Server Declined IP in the web interface:

Click DHCP, Server and Declined IP.

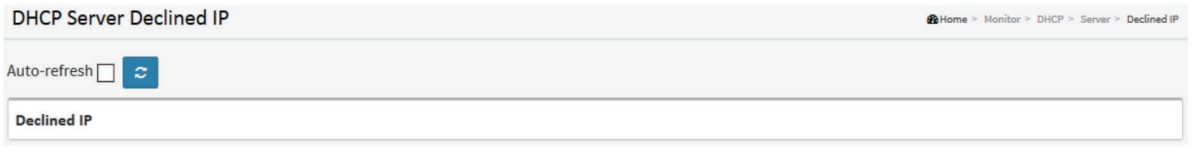



FIGURE 4-14. DECLINED IP SCREEN

Parameter description:

- IP: IP address allocated to DHCP client.
- Type: Type of binding. Possible types are Automatic, Manual, Expired.
- State: State of binding. Possible states are Committed, Allocated, Expired.
- Pool Name: The pool that generates the binding.
- Server ID: Server IP address to service the binding.

### 4.4.2 SNOOPING TABLE

This page displays the dynamic IP assigned information after DHCP Snooping mode is disabled. All DHCP clients that 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 monitor a DHCP in the web interface:

Click Monitor, DHCP, Snooping table

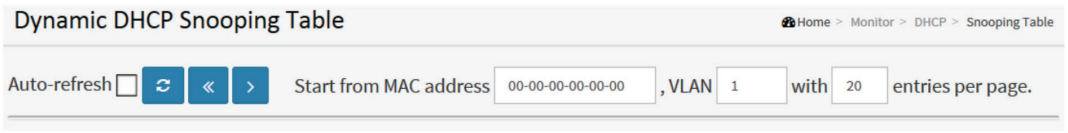



FIGURE 4-15. DHCP SNOOPING TABLE

Parameter description:

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

- IP Address: User IP address of the entry.
- IP Subnet Mask: User IP subnet mask of the entry.
- DHCP Server Address: DHCP Server address of the entry.

## 4.4.3 RELAY STATISTICS

This page provides statistics for DHCP relay.

### WEB INTERFACE

To monitor an DHCP Relay statistics in the web interface: Click Monitor, DHCP, Relay Statistics.

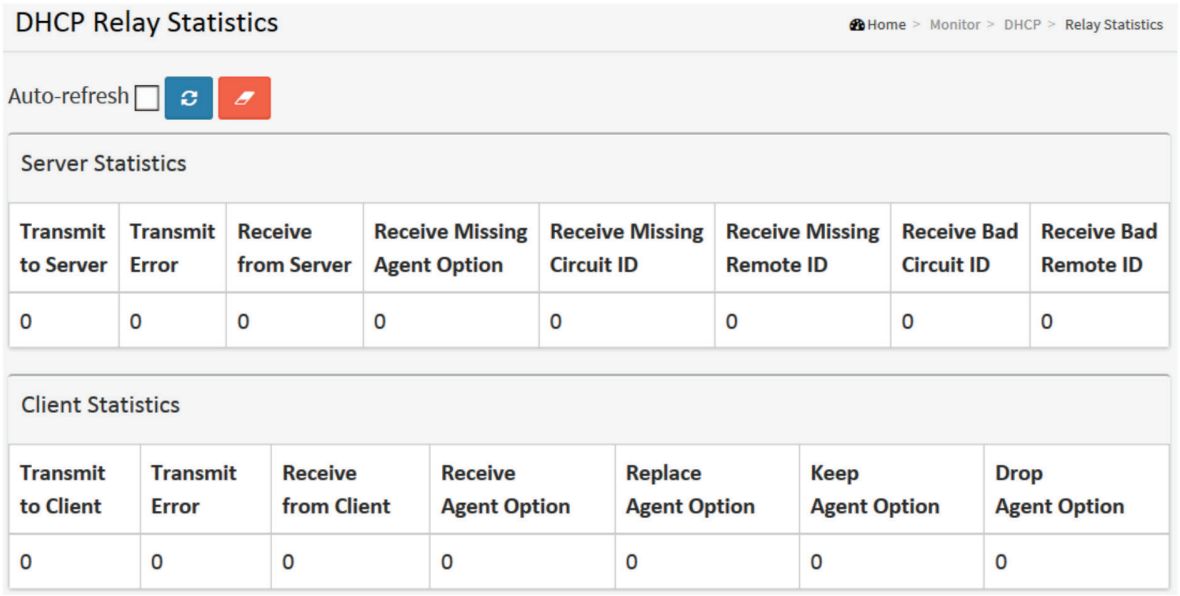



FIGURE 4-16. DHCP RELAY STATISTICS

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 a known circuit ID.
- Receive Bad Remote ID : The number of packets whose Remote ID option did not match a known Remote ID.

Client Statistics

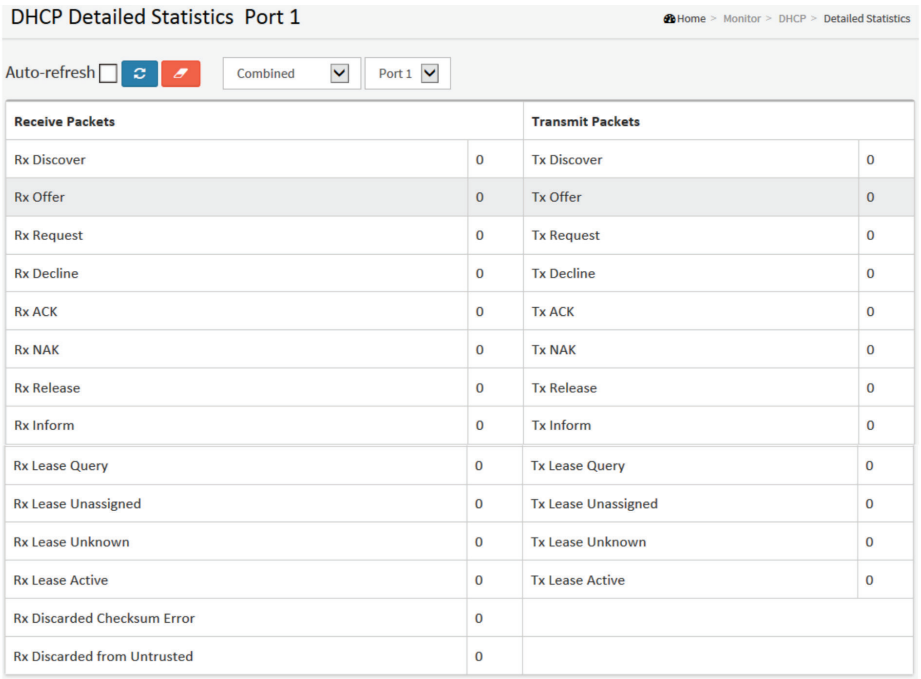
- Transmit to Client: The number of relayed packets from server to client.
- Transmit Error: The number of packets that resulted in an error while being sent to servers.
- Receive from Client: The number of received packets from server.
- Receive Agent Option : The number of received packets with relay agent information option.
- Replace Agent Option : The number of packets that 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 and were received with relay agent information.

## 4.4.4 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 forwarded by L3. Clearing the statistics on a specific port may not take effect on global statistics since it gathers a different layer overview.

### WEB INTERFACE

To monitor a DHCP Relay statistics in the web interface: Click Monitor, DHCP, Detailed Statistics.




| 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 4-17. DHCP DETAILED STATISTICS SCREEN

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: The number of lease active (option 53 with value 13) packets received and transmitted.
- Rx Discarded checksum error:  The number of discarded packets that IP/UDP checksum is error.
- Rx Discarded from Untrusted: The number of discarded packets that are coming from an untrusted port.

## 4.5 SECURITY

### 4.5.1 ACCESS MANAGEMENT STATISTICS

This section shows you detailed statistics of the Access Management including HTTP, HTTPS, SSH. TELNET, ans SSH.

#### WEB INTERFACE

To configure an Assess Management Statistics in the web interface:

1. Click Security, Access Management Statistics.
2. Check Auto-refresh.
3. Click Refresh  to refresh the port detailed statistics or click Clear to clear all information.

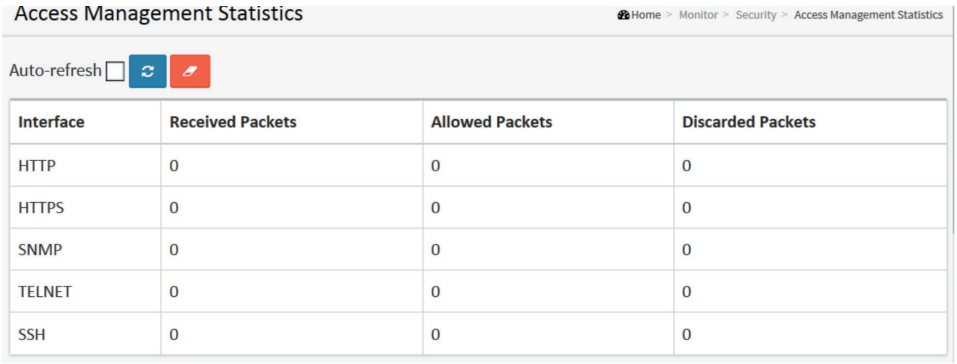



FIGURE 4-18. ACCESS MANAGEMENT STATISTICS SCREEN

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.

- Clear: Clears the counters for the selected port.

- Refresh: Click to refresh the page.

## 4.5.2 NETWORK

### 4.5.2.1 PORT SECURITY

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 configure a Port Security Switch Status Configuration in the web interface:

1.Click Security, Network, Port Security, then Switch.

2. Check Auto-refresh.

3. Click Refresh to refresh the port detailed statistics.

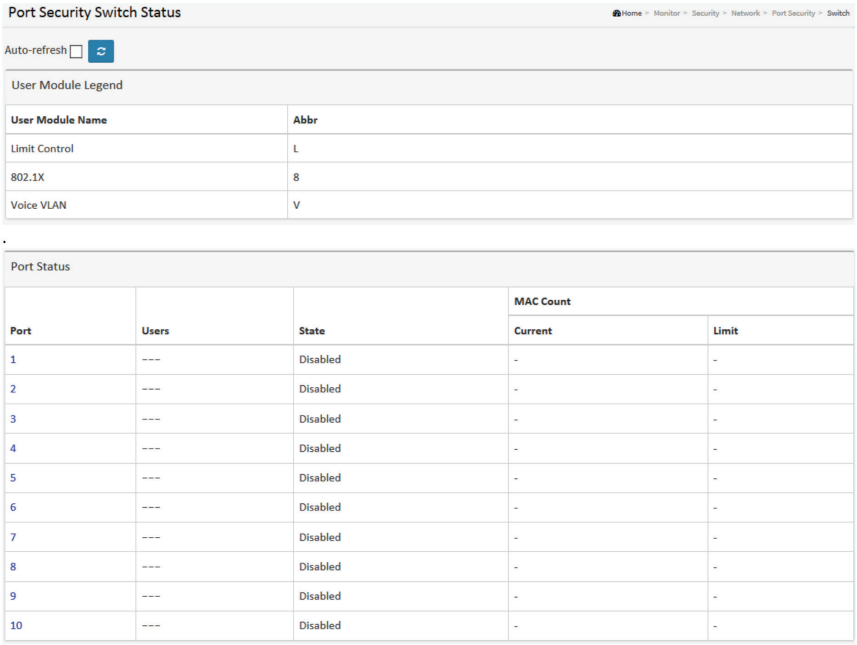



FIGURE 4-19. PORT SECURITY SWITCH STATUS SCREEN

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.
- 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 (-).

If the Limit Control user module is not enabled on the port, the Limit column will show a dash (-).

Indicates the number of currently learned MAC addresses (forwarding as well as blocked) on the port. If no user modules are enabled on the port, a dash (-) will be shown.

- Buttons:

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

- Refresh: Click to refresh the page.

## 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 configure a Port Security Switch Status Configuration in the web interface:

1. Click Security, Network, Port Security, and then Port.
2. Specify the Port that you want to monitor.
3. Check Auto-refresh.
4. Click Refresh to refresh the port detailed statistics.

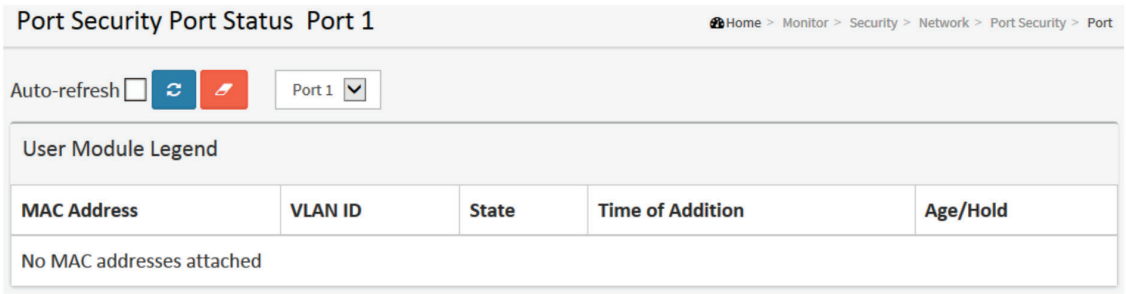



FIGURE 4-20. PORT SECURITY PORT STATUS SCREEN

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 sent, 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.

### 4.5.2.2 NAS

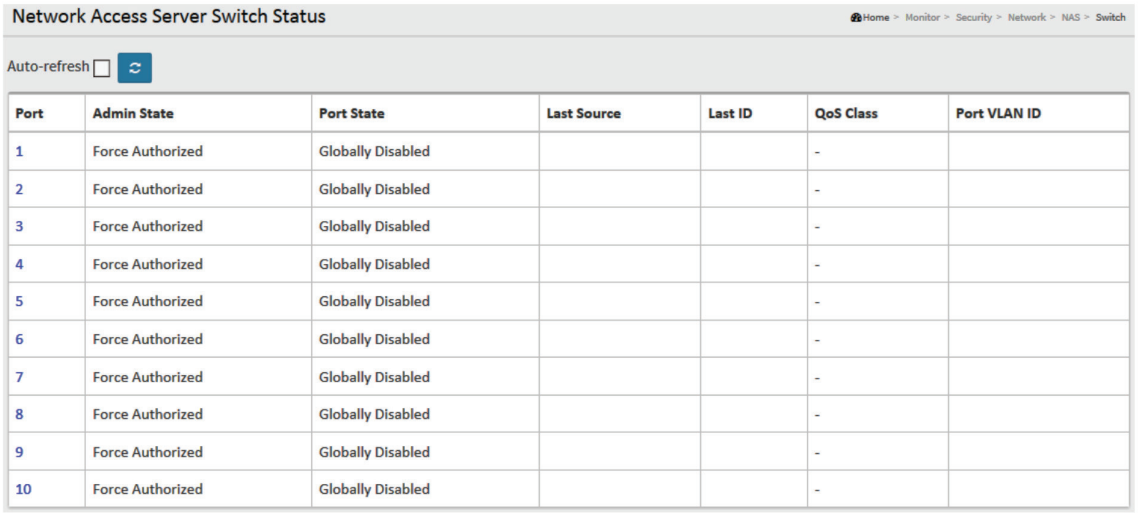
### SWITCH

This section describes how 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 configure a NAS Switch Status Configuration in the web interface:

1. Click Security, Network, NAS, then Port.
2. Check Auto-refresh.
3. Click Refresh  to refresh the port detailed statistics.




| Port | Admin State | Port State | Last Source | Last ID | QoS Class | Port VLAN ID |
|---|---|---|---|---|---|---|
| 1 | Force Authorized | Globally Disabled | | | - | |
| 2 | Force Authorized | Globally Disabled | | | - | |
| 3 | Force Authorized | Globally Disabled | | | - | |
| 4 | Force Authorized | Globally Disabled | | | - | |
| 5 | Force Authorized | Globally Disabled | | | - | |
| 6 | Force Authorized | Globally Disabled | | | - | |
| 7 | Force Authorized | Globally Disabled | | | - | |
| 8 | Force Authorized | Globally Disabled | | | - | |
| 9 | Force Authorized | Globally Disabled | | | - | |
| 10 | Force Authorized | Globally Disabled | | | - | |

FIGURE 4-21. NETWORK ACCESS SERVER SWITCH STATUS SCREEN

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.

- If the port is moved to the Guest VLAN, "(Guest)" is appended to the VLAN ID.

- Buttons:

FIGURE AUTO-REFRESH

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

- Refresh: Click to refresh the page.

## PORT

The section  provides detailed NAS statistics for a specific switch port running EAPOL-based IEEE 802.1X authentication. For MAC-based ports, it shows selected backend server (RADIUS Authentication Server) statistics, only.

## WEB INTERFACE

To configure a NAS Port Status Configuration in the web interface:

1. Click Security, Network, NAS, then Port.
2. Check Auto-refresh.
3. Click Refresh to refresh the port detailed statistics.

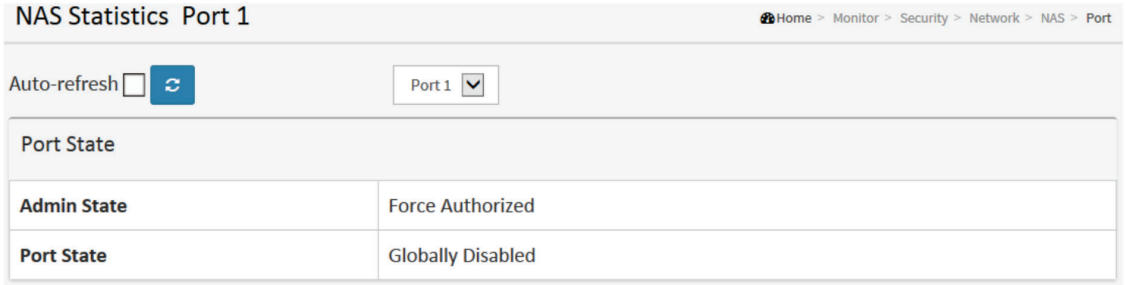



FIGURE 4-22. NAS STATISTICS SCREEN

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.

If the port is moved to the Guest VLAN, "(Guest)" is appended to the VLAN ID.

Port Counters

- EAPOL Counters: These supplicant frame counters are available for the following administrative states:
  - Force Authorized
  - Force Unauthorized
  - Port-based 802.1X
  - Single 802.1X
  - Multi 802.1X
- Backend Server Counters: These backend (RADIUS) frame counters are available for the following administrative states:
  - Port-based 802.1X
  - Single 802.1X
  - Multi 802.1X
  - MAC-based Auth.
- Last Supplicant/Client Info: 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.

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 has 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.

- Clear: This button is available in the following modes:

  • Force Authorized

  • Force Unauthorized

  • Port-based 802.1X

  • Single 802.1X

- Clear All: Click to clear the counters for the selected port.

This button is available in the following modes:

  • Multi 802.1X

  • MAC-based Auth.X

- Clear This: Click to clear both the port counters and all of the attached client's counters. The "Last Client" will not be cleared, however.

This button is available in the following modes:

  • Multi 802.1X

  • MAC-based Auth.X

Click to clear only the currently selected client's counters.

### 4.5.2.3 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 then ACL status.
2. To auto-refresh the information, click Auto-Refresh.
3. Click Refresh to refresh the ACL Status

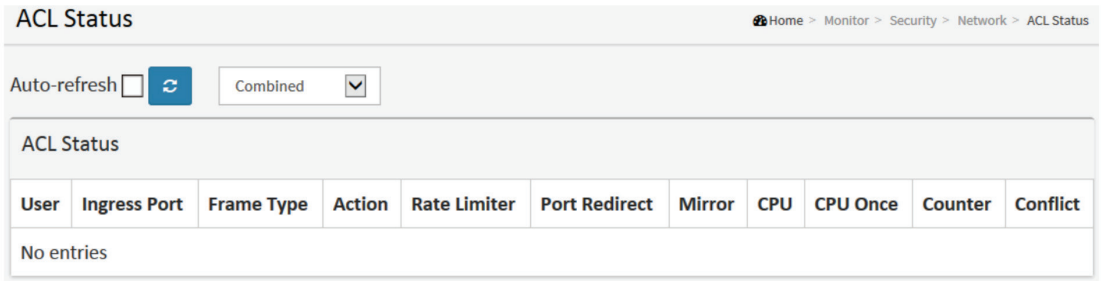



FIGURE 4-23. ACL RATE LIMITER CONFIGURATION SCREEN

Parameter description:

- User: Indicates the ACL user.
- Ingress Port: Indicates the ingress port of the ACE. Possible values are: All and Port.

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

- Enabled: Frames received on the port are mirrored.

- Disabled: Frames received on the port are not mirrored.

The default value is “Disabled”.

- CPU: Forward packet that matched the specific ACE to CPU.
- CPU Once: Forward first packet that matched the specific ACE to CPU.
- Counter: The counter indicates the number of times the ACE was hit by a frame.
- Conflict: Indicates the hardware status of the specific ACE. The specific ACE is not applied to the hardware due to hardware limitations.
- Buttons:

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

- Refresh: Click to refresh the page.

## 4.5.2.4 ARP INSPECTION

The section describes how 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 configure a Dynamic ARP Inspection Table Configuration in the web interface:

1. Click Security, Network, ARP Inspection.
2. Check “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.

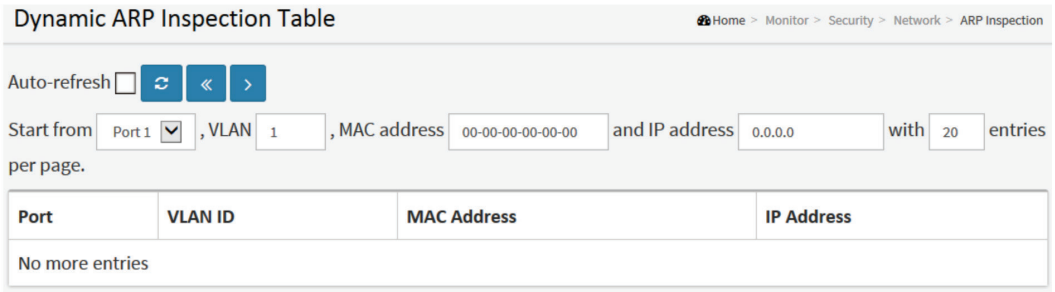



FIGURE 4-24. DYNAMIC ARP INSPECTION TABLE SCREEN

Parameter description:

Navigating the ARP Inspection Table:

Each page shows up to 99 entries from the Dynamic ARP Inspection table, default is 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 switch 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.

- 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 system log entries to the first available entry ID.

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

### 4.5.2.5 IP SOURCE GUARD

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

1. Click Security, Network, IP Source Guard.
2. Check “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.

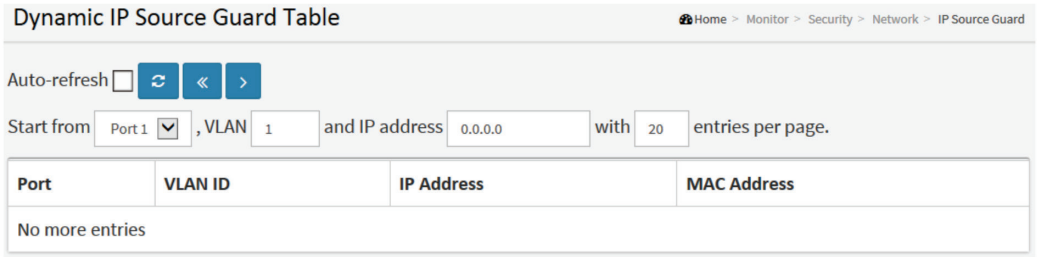



FIGURE 4-25. DYNAMIC IP SOURCE TABLE

Parameter description:

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

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

- Refresh: Click to refresh the page.

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

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

## 4.5.3 AAA

### 4.5.3.1 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 configure a RADIUS Overview Configuration in the web interface:

1. Click Security, AAA, then RADIUS Overview.
2. Check “Auto-refresh.”
3. Click “ Refresh“ to refresh the port detailed statistics.

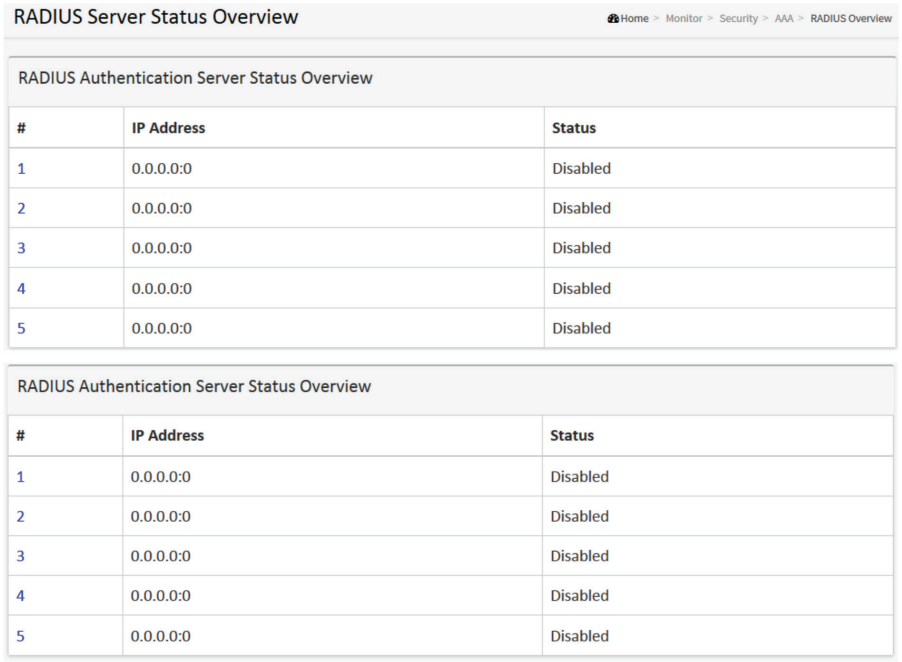



FIGURE 4-26. RADIUS AUTHENTICATION SERVER STATUS OVERVIEW SCREEN

Parameter description:

- #: The RADIUS server number. Click to navigate to detailed statistics for this server.
- IP Address: The IP address and UDP port number (in <IP Address>:<UDP Port> notation) of this server.
- 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.

### 4.5.3.2 RADIUS DETAILS

This section shows you detailed statistics for a particular RADIUS server.

### WEB INTERFACE

To configure a RADIUS Details Configuration in the web interface:

1. Specify Port to check.
2. Click Security, AAA, then RADIUS Overview.
3. Check “Auto-refresh.”
4. Click “ Refresh“ to refresh the port detailed statistics or click “Clear” to clear all information.

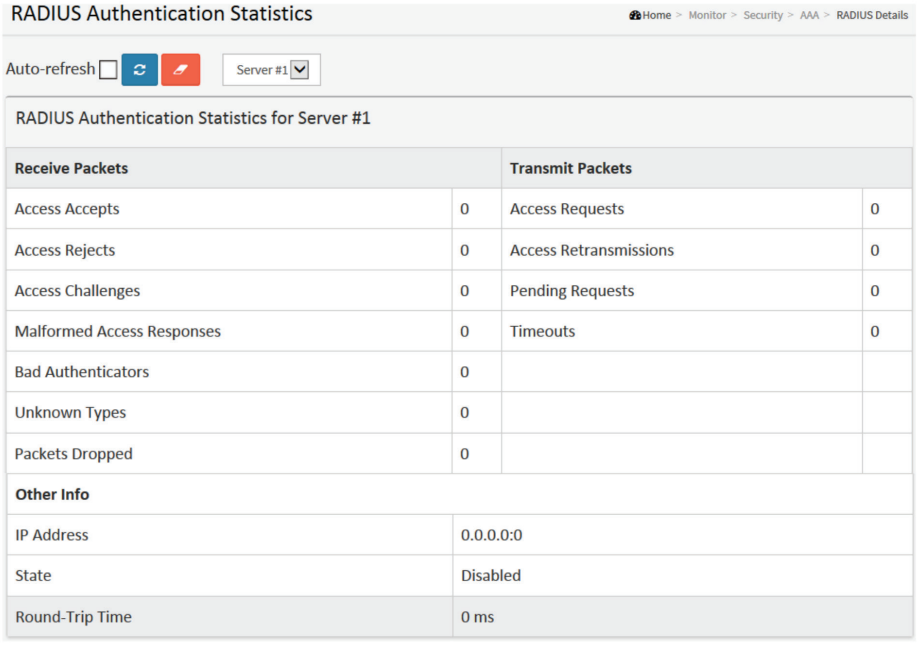



FIGURE 4-27. RADIUS AUTHENTICATION STATISTICS SERVER SCREEN

| RADIUS Accounting Statistics for Server #1 | | | |
|---|---|---|---|
| **Receive Packets** | | **Transmit Packets** | |
| Responses | 0 | Requests | 0 |
| Malformed Responses | 0 | Retransmissions | 0 |
| Bad Authenticators | 0 | Pending Requests | 0 |
| Unknown Types | 0 | Timeouts | 0 |
| Packets Dropped | 0 | | |
| **Other Info** | | | |
| IP Address | 0.0.0.0:0 | | |
| State | Disabled | | |
| Round-Trip Time | 0 ms | | |

FIGURE 4-28. RADIUS ACCOUNTING STATISTICS FOR SERVER #1

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.

TABLE 4-1. RADIUS SIGNAL DESCRIPTIONS

| DIRECTION | NAME | RFC4668 NAME | DESCRIPTION |
|---|---|---|---|
| RX | Access Accepts | radiusAuthClientExtAccessAccepts | The number of RADIUS Access-Accept packets (valid or invalid) received from the server. |
| RX | Access Rejects | radiusAuthClientExtAccessRejects | The number of RADIUS Access-Reject packets (valid or invalid) received from the server. |
| RX | Access Challenges | radiusAuthClientExtAccessChallenges | The number of RADIUS Access-Challenge packets (valid or invalid) received from the server. |
| RX | Malformed Access Responses | radiusAuthClientExtMalformedAccessResponses | The number of malformed RADIUS Access-Response packets received from the server. Malformed packets include packets with an invalid length. Bad authenticators or Message Authenticator attributes or unknown types are not included as malformed access responses. |
| RX | Bad Authenticators | radiusAuthClientExtBadAuthenticators | The number of RADIUS Access-Response packets containing invalid authenticators or Message Authenticator attributes received from the server. |
| RX | Unknown Types | radiusAuthClientExtUnknownTypes | The number of RADIUS packets that were received with unknown types from the server on the authentication port and dropped. |
| RX | Packets Dropped | radiusAuthClientExtPacketsDropped | The number of RADIUS packets that were received from the server on the authentication port and dropped for some other reason. |
| TX | Access Requests | radiusAuthClientExtAccessRequests | The number of RADIUS Access-Request packets sent to the server. This does not include retransmissions. |
| TX | Access Retransmissions | radiusAuthClientExtAccessRetransmissions | The number of RADIUS Access-Request packets retransmitted to the RADIUS authentication server. |
| TX | Pending Requests | radiusAuthClientExtPendingRequests | The number of RADIUS Access-Request packets destined for the server that have not yet timed out or received a response. This variable is incremented when an Access-Request is sent and decremented due to receipt of an Access-Accept, Access-Reject, Access-Challenge, timeout, or retransmission. |
| TX | Timeouts | adiusAuthClientExtTimeouts | The number of authentication timeouts to the server. After a timeout, the client may retry to the same server, send to a different server, or give up. A retry to the same server is counted as a retransmit as well as a timeout. A send to a different server is counted as a Request as well as a timeout. |

Other Info

This section contains information about the state of the server and the latest round-trip time.

TABLE 4-2. OTHER INFO

| NAME | RFC4668 NAME | DESCRIPTION |
|---|---|---|
| IP Address | — | IP address and UDP port for the authentication server in question. |
| State | — | Shows the state of the server. It takes one of the following values:<br>Disabled: The selected server is disabled.<br>Not Ready: The server is enabled, but IP communication is not yet up and running.<br>Ready: The server is enabled, IP communication is up and running, and the RADIUS module is ready to accept access attempts.<br>Dead (X seconds left): Access attempts were made to this server, but it did not reply within the configured timeout. The server has temporarily been disabled, but will get re-enabled when the dead-time expires. The number of seconds left before this occurs is displayed in parentheses. This state is only reachable when more than one server is enabled. |
| Round-Trip Time | radiusAuthClientExtRoundTripTime | The time interval (measured in milliseconds) between the most recent Access-Reply/Access-Challenge and the Access-Request that matched it from the RADIUS authentication server. The granularity of this measurement is 100 ms. A value of 0 ms indicates that there hasn't been round-trip communication with the server yet. |

RADIUS Accounting Statistics

The statistics map closely to those specified in RFC4670 - RADIUS Accounting Client MIB.

Use the server select box to switch between the backend servers to show details for.

Packet Counters

RADIUS accounting server packet counter. There are five receive and four transmit counters.

TABLE 4-3. PACKET COUNTERS

| DIRECTION | NAME | RFC4670 NAME | DESCRIPTION |
|---|---|---|---|
| RX | Responses | radiusAccClientExtResponses | The number of RADIUS packets (valid or invalid) received from the server. |
| RX | Malformed Response | radiusAccClientExtMalformedResponses | The number of malformed RADIUS packets received from the server. Malformed packets include packets with an invalid length. Bad authenticators or unknown types are not included as malformed access responses. |
| RX | Bad Authenticators | radiusAcctClientExtBadAuthenticators | The number of RADIUS packets containing invalid authenticators received from the server. |
| RX | Unknown Types | radiusAccClientExtUnknownTypes | The number of RADIUS packets of unknown types that were received from the server on the accounting port. |
| RX | Packets Dropped | radiusAccClientExtPacketsDropped | The number of RADIUS packets that were received from the server on the accounting port and dropped for some other reason. |
| TX | Requests | radiusAccClientExtRequests | The number of RADIUS packets sent to the server. This does not include retransmissions. |
| TX | Retransmissions | radiusAccClientExtRetransmissions | The number of RADIUS packets retransmitted to the RADIUS accounting server. |
| TX | Pending Requests | radiusAccClientExtPendingRequests | The number of RADIUS packets destined for the server that have not yet timed out or received a response. This variable is incremented when a Request is sent and decremented due to receipt of a Response, timeout, or retransmission. |
| TX | Timeouts | radiusAccClientExtTimeouts | The number of accounting timeouts to the server. After a timeout, the client may retry to the same server, send to a different server, or give up. A retry to the same server is counted as a retransmit as well as a timeout. A send to a different server icounted as a Request as well as a timeout. |

Other Info

This section contains information about the state of the server and the latest round-trip time.

TABLE 4-4. OTHER INFO

| NAME | RFC4668 NAME | DESCRIPTION |
|---|---|---|
| IP Address | — | IP address and UDP port for the authentication server in question. |
| State | — | Shows the state of the server. It takes one of the following values:<br>Disabled: The selected server is disabled.<br>Not Ready: The server is enabled, but IP communication is not yet up and running.<br>Ready: The server is enabled, IP communication is up and running, and the RADIUS module is ready to accept accounting attempts.<br>Dead (X seconds left): Accounting attempts were made to this server, but it did not reply within the configured timeout. The server has temporarily been disabled, but will get re-enabled when the dead-time expires. The number of seconds left before this occurs is displayed in parentheses. This state is only reachable when more than one server is enabled. |
| Round-Trip Time | radiusAccClientExtRoundTripTime | The time interval (measured in milliseconds) between the most recent Response and the Request that matched it from the RADIUS accounting server. The granularity of this measurement is 100 ms. A value of 0 ms indicates that there hasn't been round-trip communication with the server yet. |

- Buttons:

- Auto-refresh – Check this box to enable an automatic refresh of the page at regular intervals.
- Refresh - Click to refresh the page immediately.
- Clear - Clears the counters for the selected server. The "Pending Requests" counter will not be cleared by this operation.

## 4.5.4 SWITCH

### 4.5.4.1 RMON

### STATISTICS

This section provides an overview of RMON Statistics entries. Each page shows up to 99 entries from the Statistics table, default is 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.

The "Start from Control Index" allows the user to select the starting point in the Statistics table. Clicking the button will update the displayed table starting from that or the next closest Statistics table match.

The switch 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 RMON Statistics in the web interface:

1. Specify the Port to check.
2. Click Security, Switch, RMON, then Statistics.
3. Check "Auto-refresh."
4. Click " Refresh" to refresh the port detailed statistics.

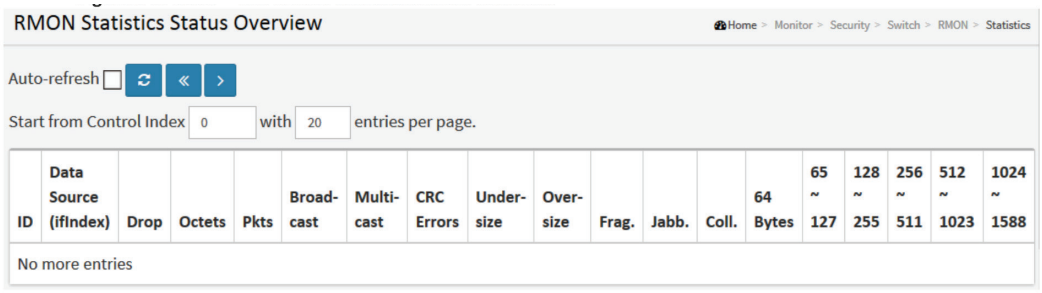



FIGURE 4-29. RMON STATISTICS STATUS OVERVIEW SCREEN

Parameter description:

- ID: Indicates the index of Statistics entry.
- Data Source (ifIndex): The port ID to monitor.
- Drop: The total number of events in which packets were dropped by the probe due to lack of resources.
- Octets: The total number of octets of data (including those in bad packets) received on the network.
- Pkts: The total number of packets (including bad packets, broadcast packets, and multicast packets) received.
- Broadcast: The total number of good packets received that were directed to the broadcast address.
- Multicast: The total number of good packets received that were directed to a multicast address.
- CRC Errors: The total number of packets received that had a length (excluding framing bits, but including FCS octets) of between 64 and 1518 octets, 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 that were less than 64 octets received with invalid CRC.
- Jabb.: The number of frames that were 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: Click to refresh the page immediately.

|<< : 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.

## HISTORY

This section provides an overview of RMON History entries. Each page shows up to 99 entries from the History table, default is 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.

The “Start from History Index and Sample Index” allows the user to select the starting point in the History table.

The “Start from History Index and Sample Index” allows the user to select the starting point in the History table. Clicking the button will update the displayed table starting from that or the next closest History table match.

The switch 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 an RMON history Configuration in the web interface:

1. Specify the Port to check.
2. Click Security, Switch, RMON, then History.
3. Check “Auto-refresh.”
4. Click “ Refresh“ to refresh the port detailed statistics or click “Clear” to clear all information.

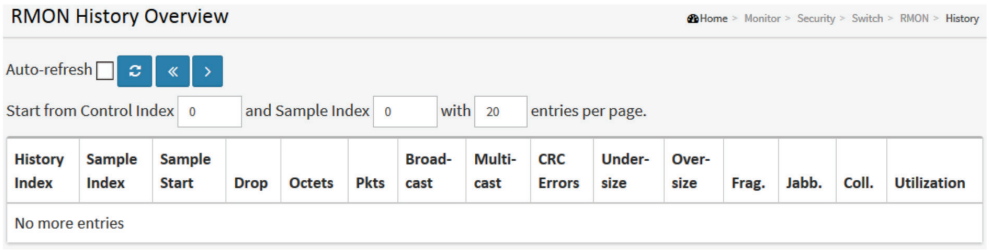



FIGURE 4-30. RMON HISTORY OVERVIEW SCREEN

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 less than 64 octets received with invalid CRC.
- Jabb.: The number of frames 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: Click to refresh the page immediately.

|<< : Updates the table starting from the first entry in the History table, i.e., the entry with the lowest History Index and Sample Index

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

## ALARM

This page provides an overview of RMON Alarm entries. Each page shows up to 99 entries from the Alarm table, default is 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.

The “Start from Control Index” allows the user to select the starting point in the Alarm table.

Clicking the button will update the displayed table starting from that or the next closest Alarm table match.

The switch 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 a RMON Alarm Overview in the web interface:

1. Specify the Port to check.
2. Click Security, Switch, RMON, then Alarm.
3. Check “Auto-refresh.”
4. Click “ Refresh“ to refresh the port detailed statistics.


FIGURE 4-31. RMON ALARM OVERVIEW SCREEN

Parameter description:

- ID: Indicates the index of the 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: Click to refresh the page immediately.

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

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

## EVENT

This page provides an overview of RMON Event table entries. Each page shows up to 99 entries from the Event table, default is 20, selected through the “entries per page” input field. When first visited, the web page will show the first 20 entries from the beginning of the Event table. The first displayed will be the one with the lowest Event Index and Log Index found in the Event table .

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

The switch 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 a RMON Event Overview in the web interface:

1. Click Security, Switch, RMON, then Event.
2. Check “Auto-refresh.”
3. Click “ Refresh“ to refresh the port detailed statistics
4. Specify the Port to check.

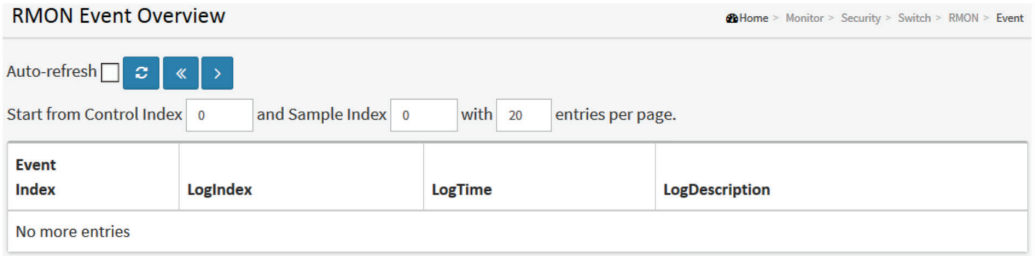



FIGURE 4-32. RMON EVENT OVERVIEW SCREEN

Parameter description:

- Event Index: Indicates the index of the event entry.
- Log Index: Indicates the index of the log entry.
- LogTIme: Indicates the 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: Click to refresh the page immediately.

|<< : Updates the table starting from the first entry in the Event Table, i.e. the entry with the lowest Event Index and Log Index.

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

## 4.6 LACP

### 4.6.1 SYSTEM STATUS

This section describes how 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, System Status.
2. Check “Auto-refresh.”
3. Click “ Refresh“ to refresh the port’s detailed statistics.

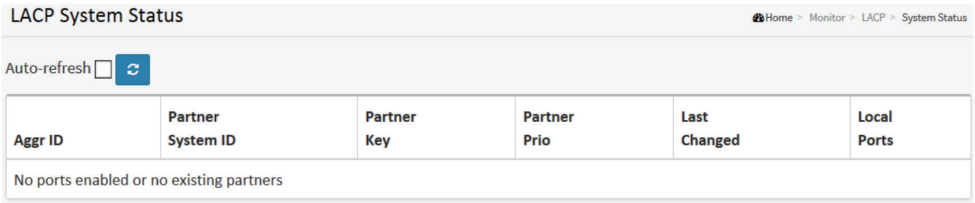



FIGURE 4-33. LACP SYSTEM STATUS SCREEN

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: Click to refresh the page.

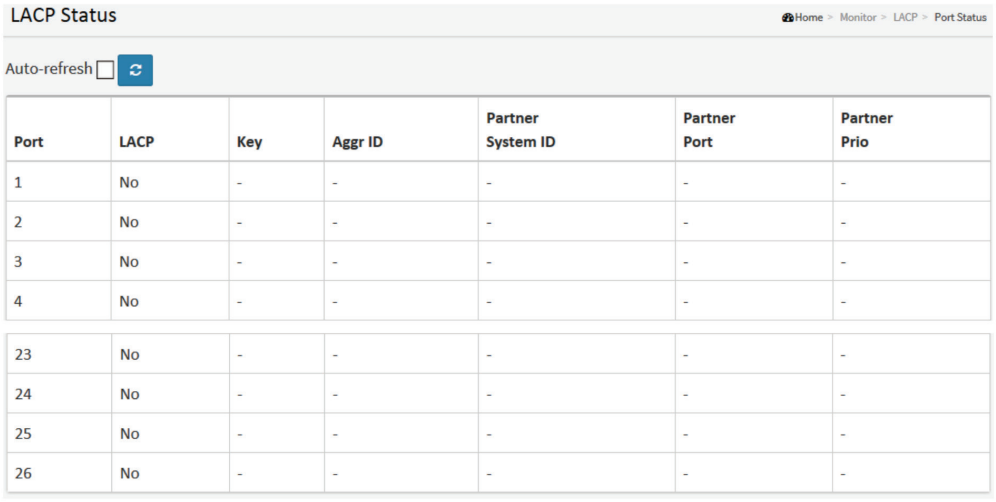
## 4.6.2 PORT STATUS

This section describes how 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, Port Status.
2. To auto-refresh the information, click 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 | - | - | - | - | - |
| 2 | No | - | - | - | - | - |
| 3 | No | - | - | - | - | - |
| 4 | No | - | - | - | - | - |
| 23 | No | - | - | - | - | - |
| 24 | No | - | - | - | - | - |
| 25 | No | - | - | - | - | - |
| 26 | No | - | - | - | - | - |

FIGURE 4-34. LACP STATUS SCREEN

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 its 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: Click to refresh the page.

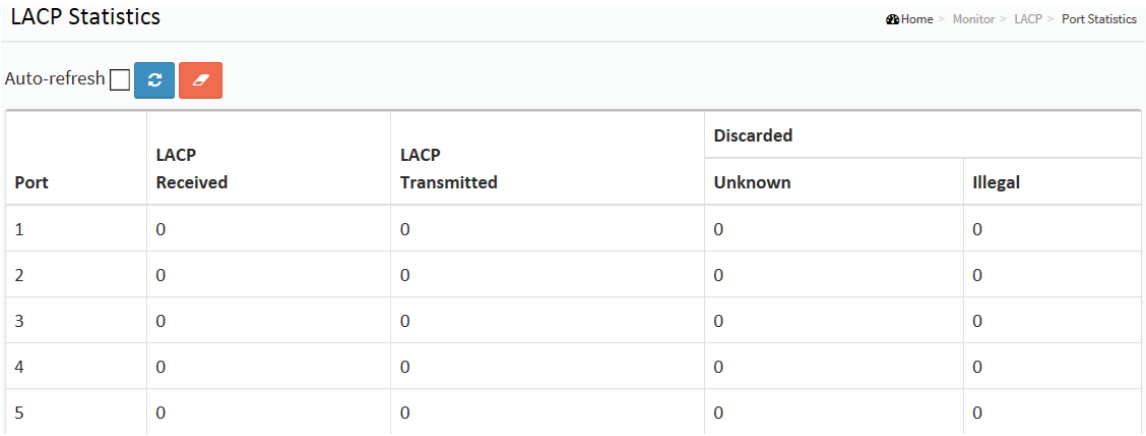
## 4.6.3 PORT STATISTICS

This section describes how 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, Port Statistics.
2. To auto-refresh the information, click “Auto refresh.”
3. Click “ Refresh“ to refresh the LACP Statistics.




| Port | LACP Received | LACP Transmitted | Discarded | |
|---|---|---|---|---|
| | | | Unknown | Illegal |
| 1 | 0 | 0 | 0 | 0 |
| 2 | 0 | 0 | 0 | 0 |
| 3 | 0 | 0 | 0 | 0 |
| 4 | 0 | 0 | 0 | 0 |
| 5 | 0 | 0 | 0 | 0 |

FIGURE 4-35. LACP STATISTICS SCREEN

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.
- Clear: Clears the counters for the selected port.
- Refresh: Click to refresh the page.

## 4.7 LOOP PROTECTION

This section displays the loop protection port status for the ports of the currently selected switch.

### WEB INTERFACE

To display the Loop Protection status in the web interface:

1. Click Monitor, Loop Protection
2. To auto-refresh the information, click “Auto refresh.”
3. Click “ Refresh“ to refresh the LACP Statistics.

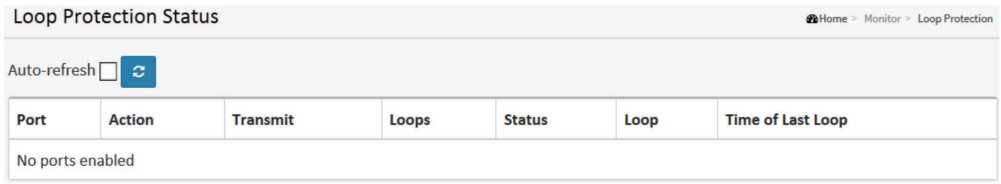



FIGURE 4-36. LOOP PROTECTION STATUS SCREEN

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:

- Refresh: Click to refresh the page immediately.

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

## 4.8 SPANNING TREE

### 4.8.1 BRIDGE STATUS

After you complete the MSTI Port configuration, the switch can display the Bridge Status. This section provides a status overview of all STP bridge instances. The displayed table contains a row for each STP bridge instance, where the column displays the following information.

#### WEB INTERFACE

To display the STP Bridges status in the web interface:

1. Click Monitor, Spanning Tree, STP Bridges.
2. To auto-refresh the information, click Auto-refresh.
3. Click " Refresh"  to refresh the STP Bridges.
4. Click " CIST" to go to the next page "STP Detailed Bridge Status."

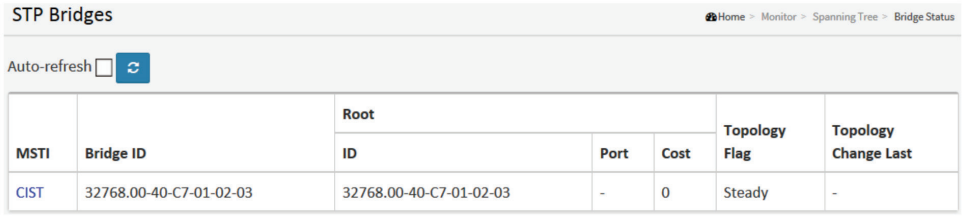



FIGURE 4-37. STP BRIDGES STATUS SCREEN

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 the 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.

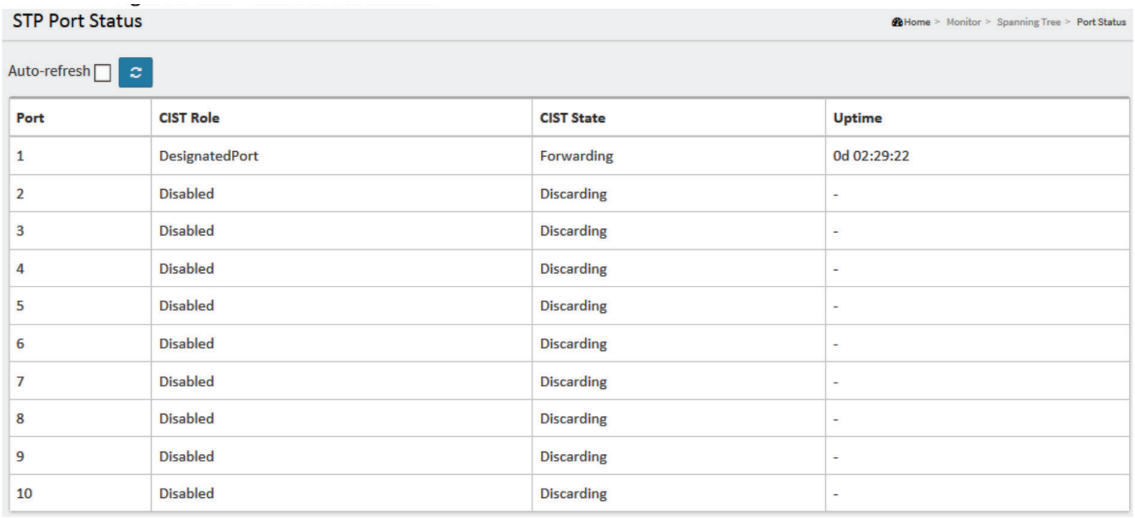
## 4.8.2 PORT STATUS

After you complete the STP configuration, the switch can display the STP Port Status. The explains how 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, STP Port Status
2. To auto-refresh the information, click Auto-refresh.
3. Click " Refresh" to refresh the STP Bridges.




| Port | CIST Role | CIST State | Uptime |
|---|---|---|---|
| 1 | DesignatedPort | Forwarding | 0d 02:29:22 |
| 2 | Disabled | Discarding | - |
| 3 | Disabled | Discarding | - |
| 4 | Disabled | Discarding | - |
| 5 | Disabled | Discarding | - |
| 6 | Disabled | Discarding | - |
| 7 | Disabled | Discarding | - |
| 8 | Disabled | Discarding | - |
| 9 | Disabled | Discarding | - |
| 10 | Disabled | Discarding | - |

FIGURE 4-38. STP PORT STATUS SCREEN

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, or 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, or 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.

## 4.8.3 PORT STATISTICS

After you complete the STP configuration, then the switch can display the STP Statistics. This section explains how 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, Port Statistics.
2. To auto-refresh the information, click Auto-refresh.
3. Click " Refresh" to refresh the STP Bridges.

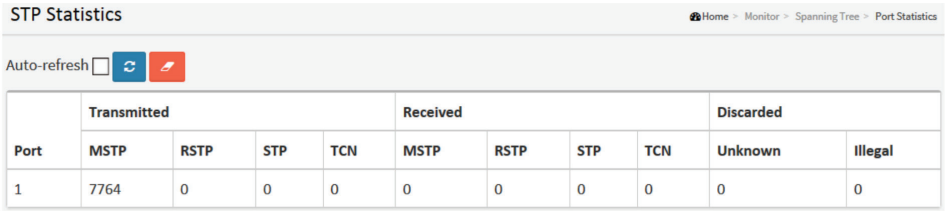



FIGURE 4-39. STP STATISTICS SCREEN

Parameter description:

- Port: The switch port number of the logical STP port.
- MSTP: The number of MSTP Configuration BPDUs 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 BPDUs received/transmitted on the port.
- Discarded Unknown: The number of unknown Spanning Tree BPDUs received (and discarded) on the port.
- Discarded Illegal: The number of illegal Spanning Tree BPDUs received (and discarded) on the port.
- Buttons

- Auto-refresh: Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.
- Clear: Clears the counters for the selected port.
- Refresh: Click to refresh the page.

## 4.9 MVR

### 4.9.1 STATISTICS

The section describes how to display the MVR detail Statistics after you configure MVR on the switch. It provides detailed MVR Statistics Information.

#### WEB INTERFACE

To display the MVR Statistics Information in the web interface:

1. Click Monitor, MVR, Statistics.
2. To auto-refresh the information, click Auto-refresh.
3. Click " Refresh" to refresh an entry of the MVR Statistics Information.

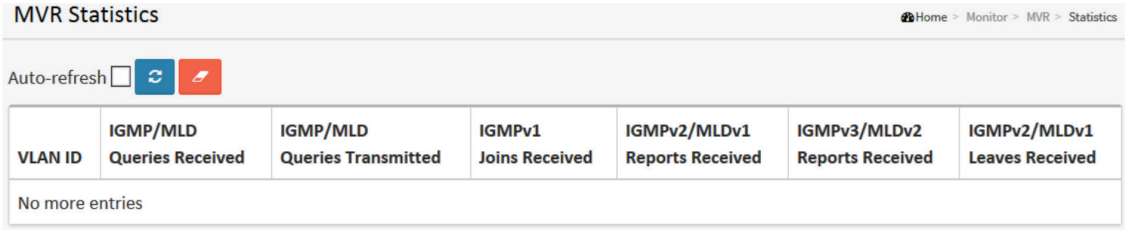



FIGURE 4-40. MVR STATISTICS INFORMATION SCREEN

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 Reports Received The number of Received IGMPv2 Joins and MLDv1 Reports, respectively.
- IGMPv3/MLDv2 Report's Received: The number of Received IGMPv1 Joins and MLDv2 Reports, respectively.
- IGMPv2/MLDv1 Leaves Received: The number of Received IGMPv2 Leaves and MLDv1 Dones, respectively.
- Buttons:

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

- Clear: Clears the counters for the selected port.

- Refresh: Click to refresh the page.

## 4.9.2 MVR CHANNELS GROUPS

The section describes how to 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, Groups Information.
2. To auto-refresh the information, click Auto-refresh.
3. To Click the " Refresh" to refresh a entry of the MVR Groups Information.
4. Click "<< or >> " to move to previous or next entry.

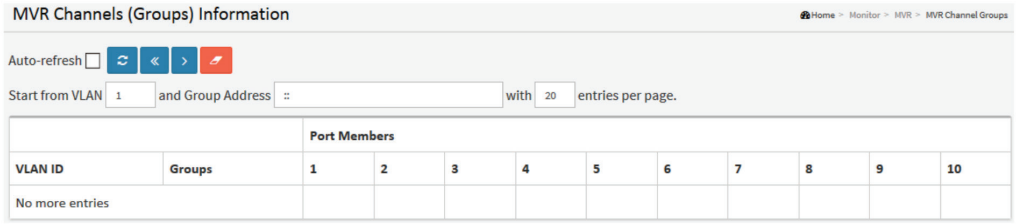



FIGURE 4-41. MVR GROUPS INFORMATION SCREEN

Parameter description:

Navigating the MVR Channels (Groups) Information Table

Each page shows up to 99 entries from the MVR Group table, default is 20, selected through the "entries per page" input field. When first visited, the web page will show the first 20 entries from the beginning of the MVR Channels (Groups) Information Table.

The "Start from VLAN", and "Group Address" input fields allow the user to select the starting point in the MVR Channels (Groups) Information Table. Clicking the button will update the displayed table starting from that or the closest next MVR Channels (Groups) Information Table match. In addition, the two input fields will—upon a button click—assume the value of the first displayed entry, allowing for continuous refresh with the same start address.

The switch 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

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.

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

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

## 4.9.3 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 that 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, MVR SFM Information.
2. To auto-refresh the information, click Auto-refresh.
3. Click " Refresh" to refresh a entry of the MVR Groups Information.
4. Click "<< or >> " to move to previous or next entry.

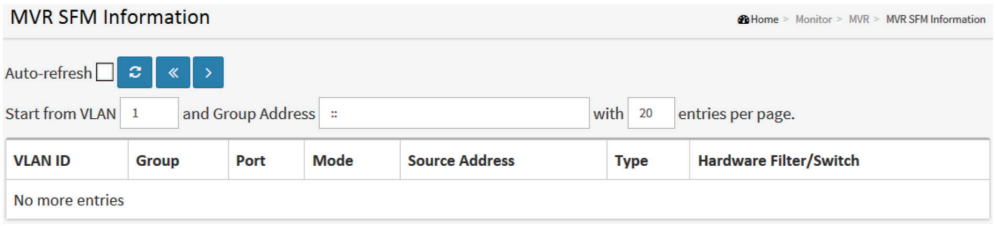



FIGURE 4-42. MVR SFM INFORMATION SCREEN

Parameter description:

Navigating the MVR SFM Information Table

Each page shows up to 99 entries from the MVR SFM Information Table, default is 20, selected through the "entries per page" input field. When first visited, the web page will show the first 20 entries from the beginning of the MVR SFM Information Table.

The "Start from VLAN", and "Group Address" input fields allow the user to select the starting point in the MVR SFM Information Table. Clicking the button will update the displayed table starting from that or the closest next MVR SFM Information Table match. In addition, the two input fields will—upon a button click—assume the value of the first displayed entry, allowing for continuous refresh with the same start address.

The switch 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.

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 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 a data plane destined to the specific group address from the source IPv4/IPv6 address could be handled by the 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.

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

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

## 4.10 IPMC

### 4.10.1 IGMP SNOOPING

#### 4.10.1.1 STATUS

After you complete the IGMP Snooping configuration, the switch can display the IGMP Snooping Status. This section shows how to display the IGMP Snooping detail status.

#### WEB INTERFACE

To display the IGMP Snooping status in the web interface:

1. Click Monitor, IGMP Snooping, Status
2. To auto-refresh the information, click Auto-refresh.
3. Click " Refresh"  to refresh the IGMP Snooping Status.
4. Click " Clear"  to clear the IGMP Snooping Status.

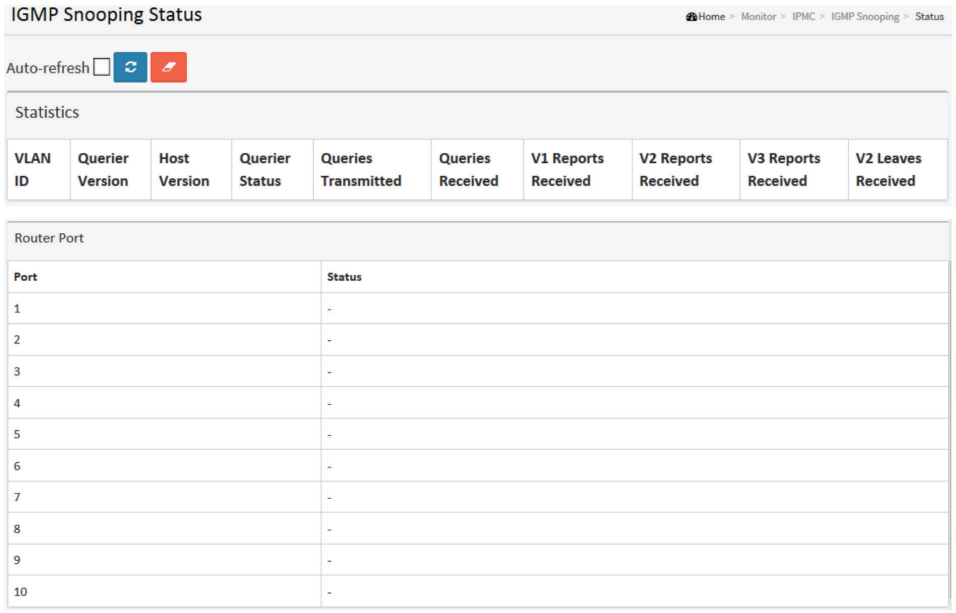



FIGURE 4-43. IGMP SNOOPING STATUS SCREEN

Parameter description:

- VLAN ID: The VLAN ID of the entry.
- Querier Version: Currently Working Querier Version.
- Host Version: Currently Working Host Version.
- Querier Status: Shows the Querier status is ACTIVE or IDLE. DISABLE denotes the specific interface is administratively disabled.
- 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 learned to be a router port.
- Both denotes that the specific port is configured or learned to be a router port.

- Port: Switch port number.
- Status: Indicates 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.
- Clear: Clears the counters for the selected port.
- Refresh: Click to refresh the page.

### 4.10.1.2 GROUP INFORMATION

After you set the IGMP Snooping function, then the switch can 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 switch 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. To auto-refresh the information, click 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.

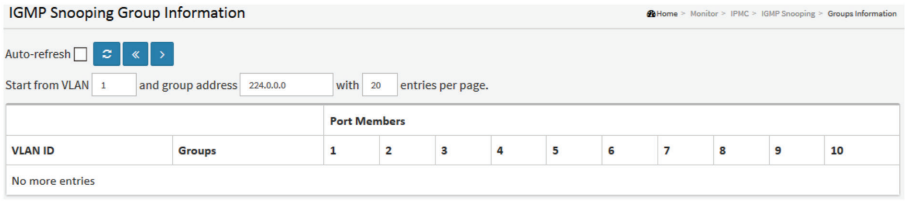



FIGURE 4-44. IGMP SNOOPING GROUPS INFORMATION SCREEN

Parameter description:

Navigating the IGMP Group Table

Each page shows up to 99 entries from the IGMP Group table, default is 20, selected through the “entries per page” input field. When first visited, the web page will show the first 20 entries from the beginning of the IGMP Group Table.

The “Start from VLAN”, and “group” input fields allow the user to select the starting point in the IGMP Group Table. Clicking the button will update the displayed table starting from that or the closest next IGMP Group Table match. In addition, the two input fields will—upon a button click—assume the value of the first displayed entry, allowing for continuous refresh with the same start address.

The switch 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.

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.

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

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

### 4.10.1.3 IPV4 SFM INFORMATION

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 that 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. To auto-refresh the information, click Auto-refresh.
3. Click " Refresh" to refresh a entry of the IPv4 SFM Information.
4. Click "<< or >> " to move to previous or next entry.

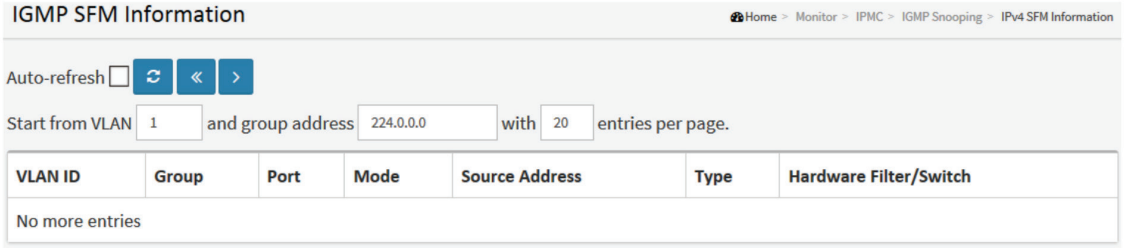



FIGURE 4-45. IPV4 SFM INFORMATION SCREEN

Parameter description:

Navigating the IGMP SFM Information Table

Each page shows up to 99 entries from the IGMP SFM Information table, default is 20, selected through the "entries per page" input field. When first visited, the web page will show the first 20 entries from the beginning of the IGMP SFM Information Table.

The "Start from VLAN", and "group" input fields allow the user to select the starting point in the IGMP SFM Information Table. Clicking the button will update the displayed table starting from that or the closest next IGMP SFM Information Table match. In addition, the two input fields will—upon a button click—assume the value of the first displayed entry, allowing for continuous refresh with the same start address.

The switch 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.

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, the system limits the total number of IP source addresses for filtering to 128.
- Type: Indicates the Type. It can be either Allow or Deny.
- Hardware Filter/Switch: Indicates whether the data plane destined to the specific group address from the source IPv4 address could be handled by the 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.

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

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

## 4.10.2 MLD SNOOPING

### 4.10.2.1 STATUS

The section describes how to complete the MLD Snooping and display the MLD Snooping Status and detailed information. It will help you to find out the detailed information of MLD Snooping status.

### WEB INTERFACE

To display the MLD Snooping Status in the web interface:

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

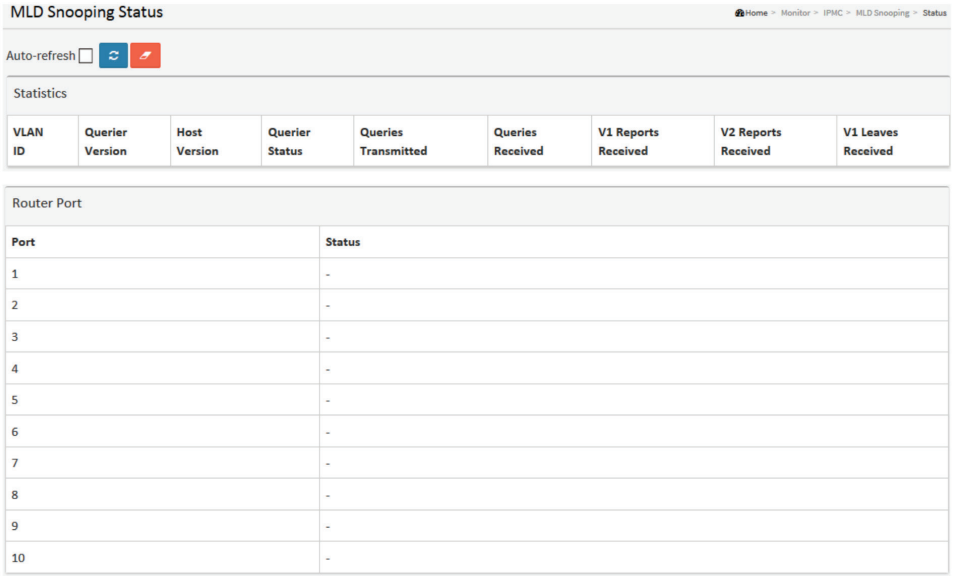



FIGURE 4-46. MLD SNOOPING STATUS SCREEN

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 learned to be a router port.
- Both denotes the specific port is configured or learned to be a router port.

- Port: Switch port number.
- Status: Indicates 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.
- Clear: Clears the counters for the selected port.
- Refresh: Click to refresh the page.

### 4.10.2.2 GROUP INFORMATION

This section describes how to 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, Group Information

2.To auto-refresh the information, click 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.

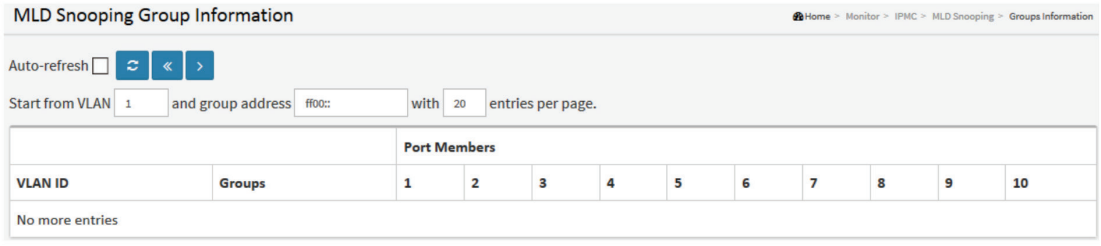



FIGURE 4-47. MLD SNOOPING GROUPS INFORMATION SCREEN

Parameter description:

Navigating the MLD Group Table

Each page shows up to 99 entries from the MLD Group table, default is 20, selected through the “entries per page” input field. When first visited, the web page will show the first 20 entries from the beginning of the MLD Group Table.

The “Start from VLAN”, and “group” input fields allow the user to select the starting point in the MLD Group Table. Clicking the button will update the displayed table starting from that or the closest next MLD Group Table match. In addition, the two input fields will — upon a button click—assume the value of the first displayed entry, allowing for continuous refresh with the same start address.

The switch 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.

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.

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

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

### 4.10.2.3 IPV6 SFM INFORMATION

Entries in the MLD SFM Information Table are shown on this page. The MLD SFM (Source-Filtered Multicast) Information Table also contains the SSM (Source-Specific Multicast) information. This table is sorted first by VLAN ID, then by group, and then by Port. Different source addresses belong to the same group are treated as single entry.

### WEB INTERFACE

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

1. Click Monitor, MLD Snooping, IPv6 SFM Information.
2. To auto-refresh the information, click Auto-refresh.
3. Click “ Refresh“  to refresh a entry of the MLDv2 IPv6 SSM Information.
4. Click “<< or >> “  to move to the previous or next entry.

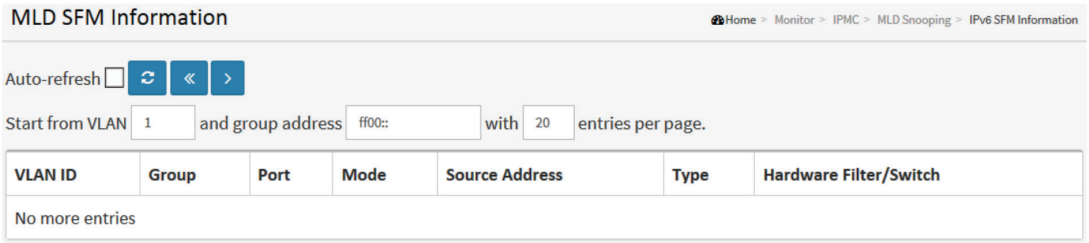



FIGURE 4-48. IPV6 SFM INFORMATION SCREEN

Parameter description:

Navigating the MLD SFM Information Table

Each page shows up to 99 entries from the MLD SFM Information table, default is 20, selected through the “entries per page” input field. When first visited, the web page will show the first 20 entries from the beginning of the MLD SFM Information Table.

The “Start from VLAN”, and “group” input fields allow the user to select the starting point in the MLD SFM Information Table. Clicking the button will update the displayed table starting from that or the closest next MLD SFM Information Table match. In addition, the two input fields will—upon a button click—assume the value of the first displayed entry, allowing for continuous refresh with the same start address.

The switch 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.

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, the system limits the total number of IP source addresses for filtering to 128.
- Type: Indicates the Type. It can be either Allow or Deny.
- Hardware Filter/Switch: Indicates whether the data plane destined to the specific group address from the source IPv6 address could be handled by the 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.

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

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

## 4.11 LLDP

### 4.11.1 NEIGHBOR

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

#### WEB INTERFACE

To show LLDP neighbors:

1. Click Monitor, LLDP, Neighbors.
2. Click Refresh to manually update the web screen.
3. Click Auto-refresh to automatically update the web screen.


FIGURE 4-49. LLDP NEIGHBORS INFORMATION SCREEN

NOTE: If your network without any device supports LLDP, then the table will show "No LLDP neighbor information found."

Parameter description:

- Local Port: The port on which the LLDP frame was received.
- Chassis ID: The Chassis ID identifies the neighbor's LLDP frames.
- Port ID: The Remote Port ID identifies the neighbor port.
- Port Description: Port Description is the port description advertised by the neighbor unit.
- System Name: System Name is the name advertised by the neighbor unit.
- System Capabilities: System Capabilities describes the neighbor unit's capabilities. The possible capabilities are:

1. Other
2. Repeater
3. Bridge
4. WLAN Access Point
5. Router
6. Telephone
7. DOCSIS cable device
8. Station only
9. Reserved

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

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

## 4.11.2 LLDP-MED NEIGHBOR

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

### WEB INTERFACE

To show LLDP-MED neighbor:

1. Click Monitor, LLDP, LLDP-MED Neighbor.
2. Click Refresh to manually update the web screen.
3. Click Auto-refresh to automatically update the web screen.

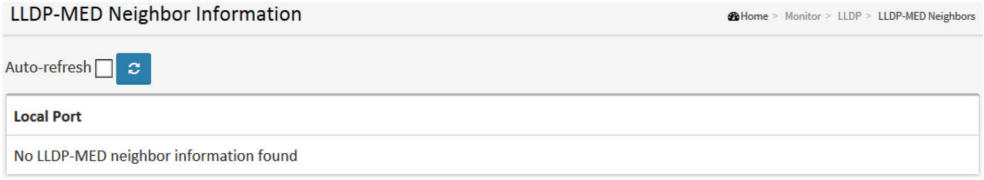



FIGURE 4-50. LLDP-MED NEIGHBORS INFORMATION SCREEN

NOTE: If your network without any device supports LLDP-MED then the table will show “No LLDP-MED neighbor 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, any LLDP-MED Endpoint Device claiming compliance as a Media Endpoint (Class II) will 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 categories.

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 applies 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, and inventory management.

LLDP-MED Capabilities:

LLDP-MED Capabilities describe 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 indicates the primary function of the application(s) defined for this network policy, advertised by an Endpoint or Network Connectivity Device. The possible application types are shown below.

1. Voice—for use by dedicated IP Telephony handsets and other similar appliances supporting interactive voice services. These devices are typically deployed on a separate VLAN for ease of deployment and enhanced security by isolation from data applications.

2. Voice Signaling—for use in network topologies that require a different policy for the voice signaling than for the voice media.

3. Guest Voice—to support a separate limited feature-set voice service for guest users and visitors with their own IP Telephony handsets and other similar appliances supporting interactive voice services.

4. Guest Voice Signaling—for use in network topologies that require a different policy for the guest voice signaling than for the guest voice media.

5. Softphone Voice—for use by softphone applications on typical data centric devices, such as PCs or laptops.

6. Video Conferencing—for use by dedicated Video Conferencing equipment and other similar appliances supporting real-time interactive video/audio services.

7. Streaming Video—for use by broadcast or multicast based video content distribution and other similar applications supporting streaming video services that require specific network policy treatment. Video applications relying on TCP with buffering would not be an intended use of this application type.

8. Video Signaling—for use in network topologies that require a separate policy for the video signaling than for the video media.

- Policy: Policy indicates that an Endpoint Device wants to explicitly advertise that the policy is required by the device. Can be either Defined or Unknown.

- Unknown: The network policy for the specified application type is currently unknown.

- Defined: The network policy is defined.

• TAG: TAG indicates 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. Contains 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 by the operational MAU type field value rather than by auto-negotiation.
- Auto-negotiation Capabilities: Auto-negotiation Capabilities show 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.

## 4.11.3 EEE

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

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

### WEB INTERFACE

To show LLDP EEE neighbors:

1. Click Monitor, LLDP, then click EEE to show discovered EEE devices.
2. Click Refresh to manually update the web screen.
3. Click Auto-refresh to automatically update the web screen.

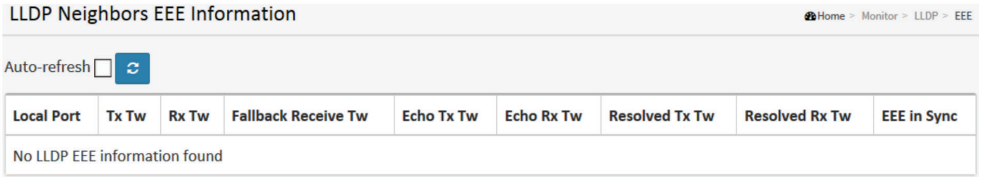



FIGURE 4-51. LLDP NEIGHBORS EEE INFORMATION SCREEN

NOTE: If your network does not have any devices that enable the EEE function, then the table will show “No LLDP EEE information found.”

Parameter description:

- Local Port: The port on which LLDP frames are received or transmitted.
- Tx Tw: The link partner’s maximum time that the transmit path can hold off sending data after reassertion of LPI.
- Rx Tw: The link partner’s time that the 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 will be defined as the local link partner’s reflection (echo) of the remote link partner’s 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 partner’s 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: This is 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: This is 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.

## 4.11.4 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 show LLDP Statistics:

1. Click Monitor, LLDP, then click Port Statistics to show LLDP counters.
2. Click Refresh to manually update the web screen.
3. Click Auto-refresh to automatically update the web screen.
4. Click Clear to clear all counters

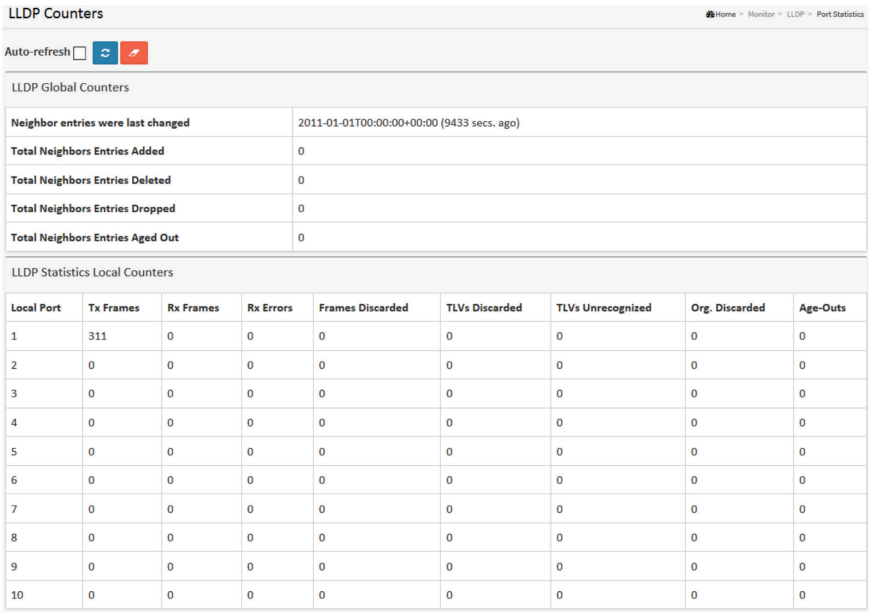



FIGURE 4-52. LLDP PORT STATISTICS INFORMATION SCREEN

Parameter description:

Global Counters

- Neighbor entries were last changed at: It shows the time when the last entry was last deleted or added. It also shows the time elapsed since the last change was detected.
- Total Neighbors Entries Added: Shows the number of new entries added since the switch rebooted.
- Total Neighbors Entries Deleted: Shows the number of new entries deleted since the switch rebooted.
- Total Neighbors Entries Dropped: Shows the number of LLDP frames dropped due to the entry table being full.
- Total Neighbors 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 is full, the LLDP frame is counted and discarded. This situation is known as "Too Many Neighbors" in the LLDP standard. LLDP frames require a new entry in the table when 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 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.
- Clear: Clears the counters for the selected port.
- Refresh: Click to refresh the page.

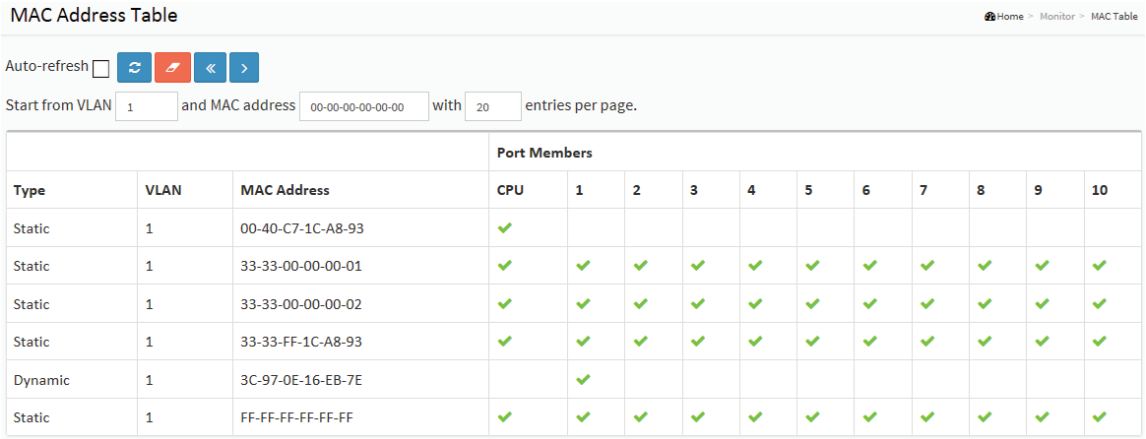
## 4.12 MAC TABLE

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 the MAC Address Table.




| | | | Port Members | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Type | VLAN | MAC Address | CPU | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 |
| Static | 1 | 00-40-C7-1C-A8-93 | ✔ | | | | | | | | | | |
| Static | 1 | 33-33-00-00-00-01 | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ |
| Static | 1 | 33-33-00-00-00-02 | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ |
| Static | 1 | 33-33-FF-1C-A8-93 | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ |
| Dynamic | 1 | 3C-97-0E-16-EB-7E | | ✔ | | | | | | | | | |
| Static | 1 | FF-FF-FF-FF-FF-FF | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ |

FIGURE 4-53. MAC ADDRESS TABLE

Parameter description:

Navigating the MAC Table

Each page shows up to 999 entries from the MAC table, default is 20, selected through the “entries per page” input field. When first visited, the web page will show the first 20 entries from the beginning of the MAC Table. The first displayed will be the one with the lowest VLAN ID and the lowest MAC address found in the MAC Table.

The “Start from MAC address” and “VLAN” input fields allow the user to select the starting point in the MAC Table. Clicking the “Refresh” button will update the displayed table starting from that or the closest next MAC Table match. In addition, the two input fields will—upon a “Refresh” button click—assume the value of the first displayed entry, allowing for continuous refresh with the same start address.

The >> will use the last entry of the currently displayed VLAN/MAC address pairs as a basis for the next lookup. When the end is reached the text “No more entries” is shown in the displayed table. Use the I<< button to start over.

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.
- Clear: Clears the counters for the selected port.
- Refresh: Click to refresh the page.

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

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

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.

## 4.13 VLANS

### 4.13.1 VLAN MEMBERSHIP

This page provides an overview of membership status of VLAN users.

The ports belong to the currently selected stack unit, as reflected by the page header.

### WEB INTERFACE

To configure VLAN membership configuration in the web interface:

1. Click Monitor, VLANs, VLAN membership.
2. Scroll to select which VLANs you want to show up.
3. Click Refresh to update the state.

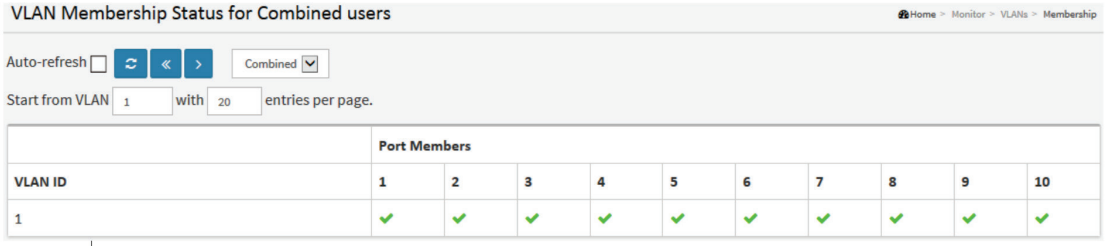



FIGURE 4-54. VLAN MEMBERSHIP STATUS FOR COMBINED USERS SCREEN

Parameter description:

- VLAN USER: VLAN User module uses services of the VLAN management functionality to configure VLAN memberships and VLAN port configurations such as PVID and UVID. Currently the switch supports the 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 de-registration 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 use while maintaining a loop-free environment.

- 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 a conflict port will be displayed.
- VLAN Membership: The VLAN Membership Status Page will show the current VLAN port members for all VLANs configured by a selected VLAN User (selection will be allowed by a Combo Box). When ALL VLAN Users are selected, it will 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.

Navigating the VLAN Monitor page

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

The “VLAN” input fields allow the user to select the starting point in the VLAN Table. Clicking the “Refresh” button will update the displayed table starting from that or the closest next VLAN Table match. The “ >> ”will use the last entry of the currently displayed VLAN 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.

- Buttons

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

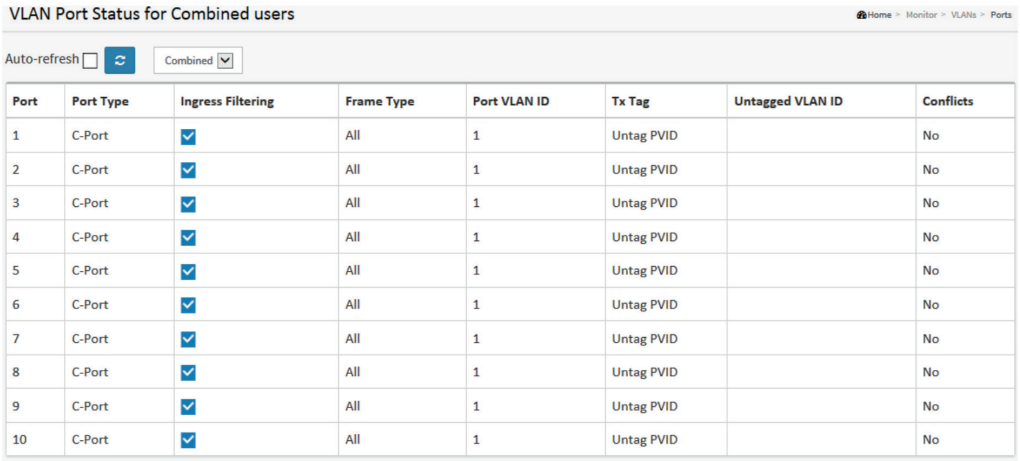
## 4.13.2 VLAN PORT

The function Port Status gathers the information of all VLAN status and reports it by Static NAS, MVRP, MVP, Voice VLAN, MSTP, GVRP Combined.

### WEB INTERFACE

To Display VLAN Port Status in the web interface:

1. Click Monitor, VLAN 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 |
| 3 | C-Port | ☑ | All | 1 | Untag PVID | | No |
| 4 | C-Port | ☑ | All | 1 | Untag PVID | | No |
| 5 | C-Port | ☑ | All | 1 | Untag PVID | | No |
| 6 | C-Port | ☑ | All | 1 | Untag PVID | | No |
| 7 | C-Port | ☑ | All | 1 | Untag PVID | | No |
| 8 | C-Port | ☑ | All | 1 | Untag PVID | | No |
| 9 | C-Port | ☑ | All | 1 | Untag PVID | | No |
| 10 | C-Port | ☑ | All | 1 | Untag PVID | | No |

FIGURE 4-55. VLAN PORT STATUS FOR STATIC USER SCREEN

Parameter description:

VLAN USER

The VLAN User module uses services of the VLAN management functionality to configure VLAN memberships and VLAN port configuration such as PVID, UVID. Currently the switch supports 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 de-registration 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). A Port's UVID determines the packet's behavior at the egress side.
- Conflicts: Shows status of Conflicts whether they exist 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.

## 4.14 VCL

### 4.14.1 MAC-BASED VLAN

This section shows MAC-based VLAN entries configured by various MAC-based VLAN users. Currently the switch supports the 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, MAC-based VLAN Status.
2. Specify Static, NAS, Combined.
3. Display MAC-based information.


FIGURE 4-56. MAC-BASED VLAN MEMBERSHIP STATUS FOR USER STATIC SCREEN

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.

## 4.14.2 PROTOCOL-BASED VLAN

### 4.14.2.1 PROTOCOL TO GROUP

This page shows you the protocols for 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, Protocol to Group.
2. Check “Auto-refresh.”
3. Click “Refresh“ to refresh the port‘s detailed statistics.

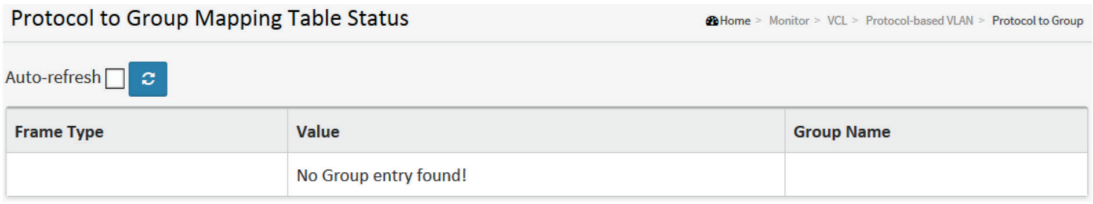



FIGURE 4-57. MAC-BASED VLAN MEMBERSHIP STATUS FOR USER STATIC SCREEN

Parameter description:

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

1. Ethernet

2. LLC

3. SNAP

NOTE: When you change the Frame type field, a valid value of the following text field will vary depending on the new frame type you selected.

- Value: A 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 are 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 the value of the OUI field is 00-00-00 then the value of PID will be etype (0x0600-0xffff) and if value of OUI is other than 00-00-00, then a valid value of PID will be any value from 0x0000 to 0xffff.

- Group Name: A valid Group Name is a unique 16-character long string for every entry that consists of a combination of alphabets (a-z or A-Z) and integers (0-9).

NOTE: Special characters 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.

### 4.14.2.2 GROUP TO VLAN

This page shows you the configured Group Name for 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. Check “Auto-refresh.”

3. Click “Refresh“ to refresh the port detailed statistics.

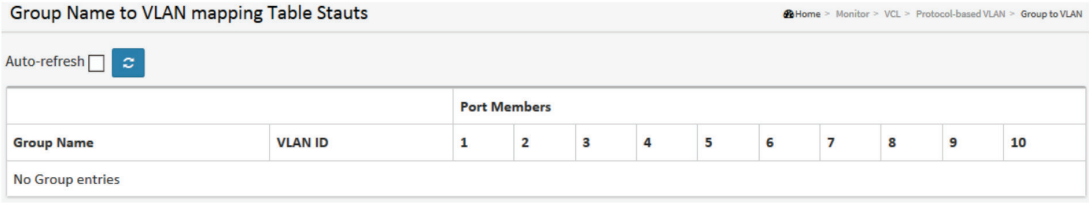



FIGURE 4-58. MAC-BASED VLAN MEMBERSHIP STATUS FOR USER STATIC SCREEN

Parameter description:

- Group Name: A valid Group Name is a string at the most 16 characters which consists of a combination of alphabetic characters (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 the 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.

## 4.14.3 IP SUBNET-BASED VLAN

### 4.14.3.1 PROTOCOL TO GROUP

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, IP Subnet-based VLAN.
2. Check “Auto-refresh.”
3. Click “Refresh“ to refresh the port detailed statistics.

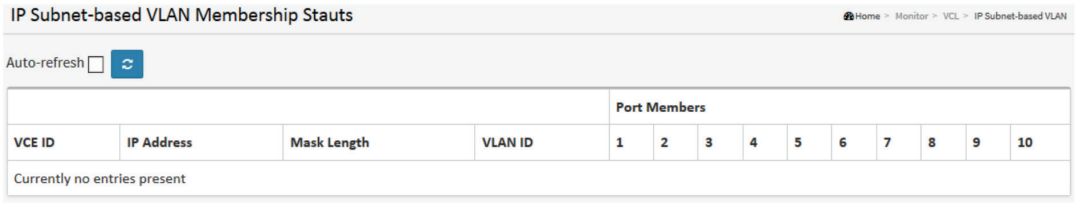



FIGURE 4-59. MAC-BASED VLAN MEMBERSHIP STATUS FOR USER STATIC SCREEN

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, the 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. The 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.

## 4.15 SFLOW

This section shows receiver and per-port sFlow statistics.

### WEB INTERFACE

To Display MAC-based VLAN configuration in the web interface:

1. Click Monitor, sFlow.
2. Display sFlow information.

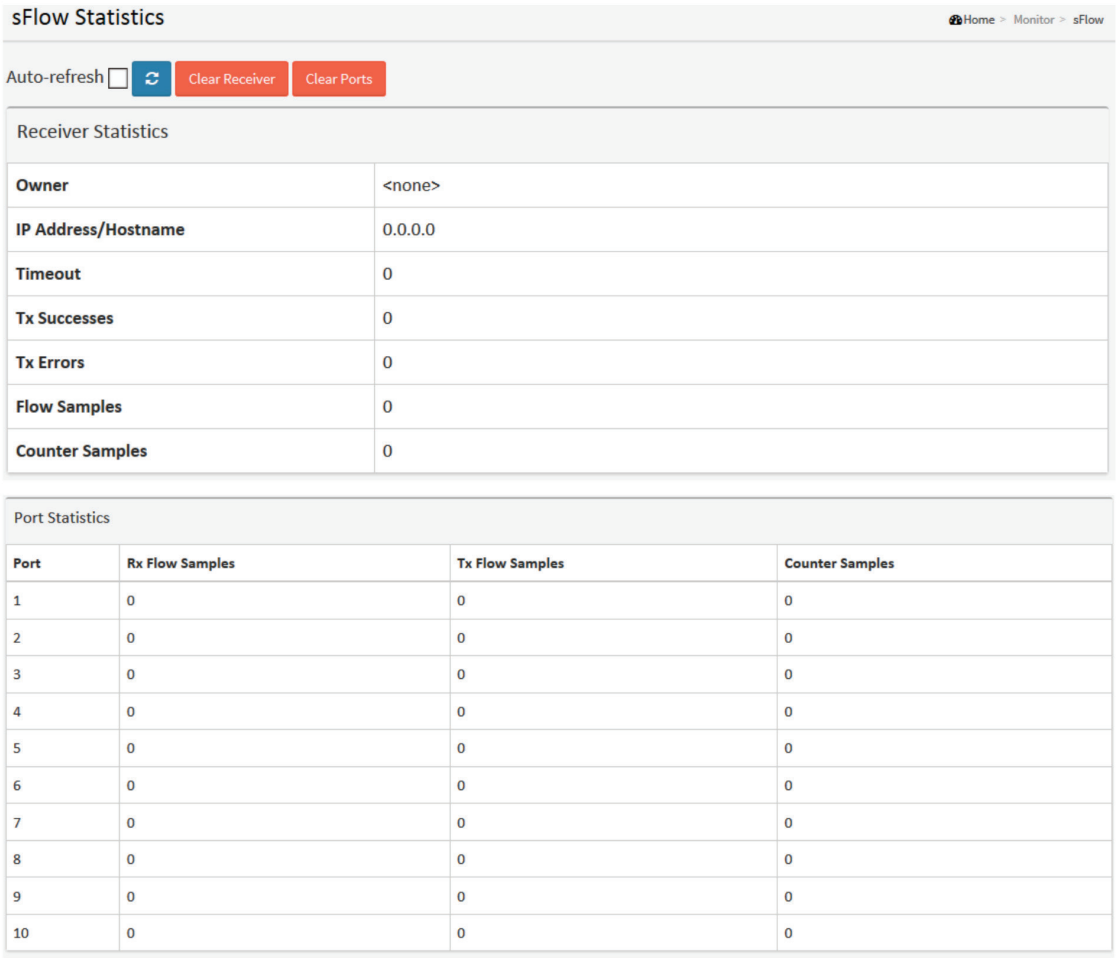



FIGURE 4-60. SFLOW STATISTICS SCREEN

Parameter description:

- Owner: This field shows the current owner of the sFlow configuration. It assumes one of three values as follows:
- If sFlow is currently unconfigured/unclaimed, Owner contains <none>.
- If sFlow is currently configured through Web or CLI, Owner contains <Configured through local management>.
- If sFlow is currently configured through SNMP, Owner contains a string identifying the sFlow receiver.`
- IP Address/Hostname: The IP address or hostname of the sFlow receiver.

- Timeout: The number of seconds remaining before sampling stops and the current sFlow owner is released.
- Tx Successes: The number of UDP datagrams successfully sent to the sFlow receiver.
- Tx Errors: The number of UDP datagrams that has failed transmission. The most common source of errors is invalid sFlow receiver IP/hostname configuration. To diagnose, paste the receiver's IP address/hostname into the Ping Web page (Diagnostics ▯ Ping/Ping6).
- Flow Samples: The total number of flow samples sent to the sFlow receiver.
- Counter Samples: The total number of counter samples sent to the sFlow receiver.

Port Statistics

- Port: The port number for which the following statistics apply.
- Rx and Tx Flow Samples: The number of flow samples sent to the sFlow receiver originating from this port. 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.
- Clear Receiver: Clears the sFlow receiver counters.
- Clear Ports: Clears the per-port counters.

# CHAPTER 5: DIAGNOSTICS

This chapter provides a set of basic system diagnosis. It let users know that whether the system is healthy or needs to be fixed. The basic system check includes ICMP Ping, Link OAM, ICMPv6, and VeriPHY Cable Diagnostics.

## 5.1 PING

This section allows you to issue ICMP PING packets to troubleshoot IPv6 connectivity issues.

### WEB INTERFACE

To configure an ICMP PING Configuration in the web interface:

1. Specify the ICMP PING IP Address.
2. Specify the ICMP PING Size.
3. Click Start.

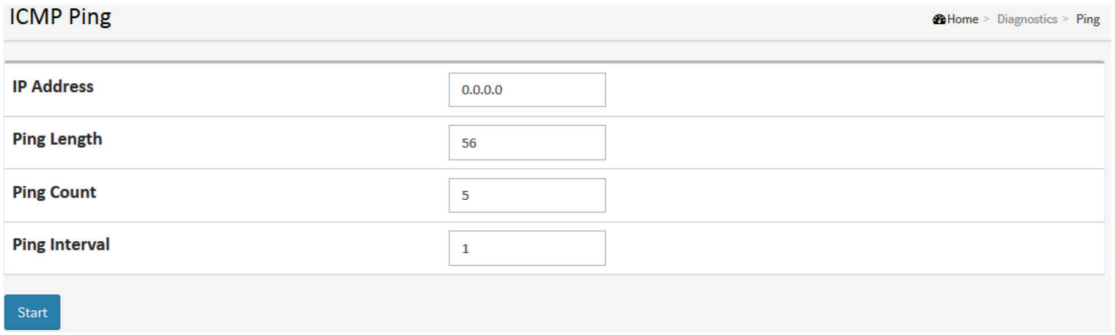



FIGURE 5-1. ICMP PING SCREEN

Parameter description:

- IP Address: To set the IP Address of device that you want to ping.
- 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 to which the 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.

- Start: Click the "Start" button, then the switch will start to ping the device using ICMP packet size that you set on the switch.

After you press Start, 5 ICMP packets are transmitted, and the sequence number and roundtrip time are displayed upon reception of a reply. The page refreshes automatically until responses to all packets are received, or until a timeout occurs.

PING6 server ::10.10.132.20

64 bytes from ::10.10.132.20: icmp_seq=0, time=0ms

64 bytes from ::10.10.132.20: icmp_seq=1, time=0ms

64 bytes from ::10.10.132.20: icmp_seq=2, time=0ms

64 bytes from ::10.10.132.20: icmp_seq=3, time=0ms

64 bytes from ::10.10.132.20: icmp_seq=4, time=0ms

Sent 5 packets, received 5 OK, 0 bad

## 5.2 PING6

This section explains how 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.

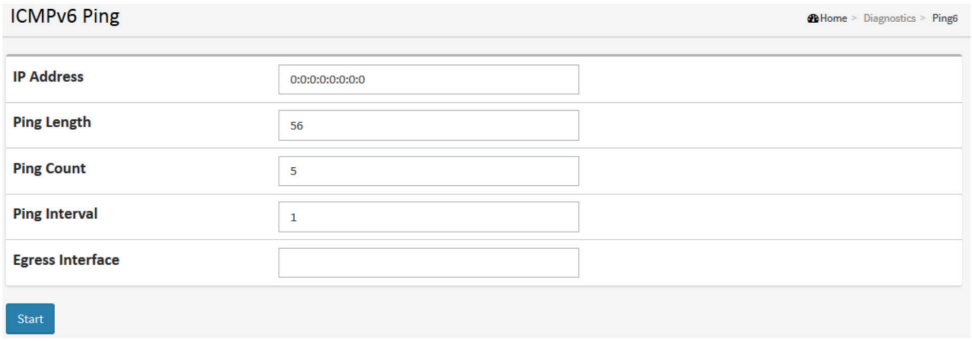



FIGURE 5-2. ICMP6 PING SCREEN

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 to which the 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 an egress interface for a loopback address. Do specify egress interface for a link-local or multicast address.
- Start: Click the "Start" button, then the switch will start to ping the device using ICMPv6 packet size that you set on the switch.

After you press Start, 5 ICMPv6 packets are transmitted, and the sequence number and roundtrip time are displayed when the switch receives a reply. The page refreshes automatically until responses to all packets are received, or until a timeout occurs.

PING server 10.10.132.20

64 bytes from 10.10.132.20: icmp_seq=0, time=0ms

64 bytes from 10.10.132.20: icmp_seq=1, time=0ms

64 bytes from 10.10.132.20: icmp_seq=2, time=0ms

64 bytes from 10.10.132.20: icmp_seq=3, time=0ms

64 bytes from 10.10.132.20: icmp_seq=4, time=0ms

Sent 5 packets, received 5 OK, 0 bad

You can configure the properties of the issued ICMP packets.

## 5.3 VERIPHY

This section explains how to run the VeriPHY Cable Diagnostics. Press 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: VeriPHY is only accurate for cables of length 7–140 meters.10 and 100 Mbps ports will be linked down while running VeriPHY. Running VeriPHY on a 10 or 100 Mbps management port will cause the switch to stop responding until VeriPHY is complete.

### WEB INTERFACE

To configure a VeriPHY Cable Diagnostics Configuration in the web interface:

1. Specify the Port you want to check.

2. Click Start.

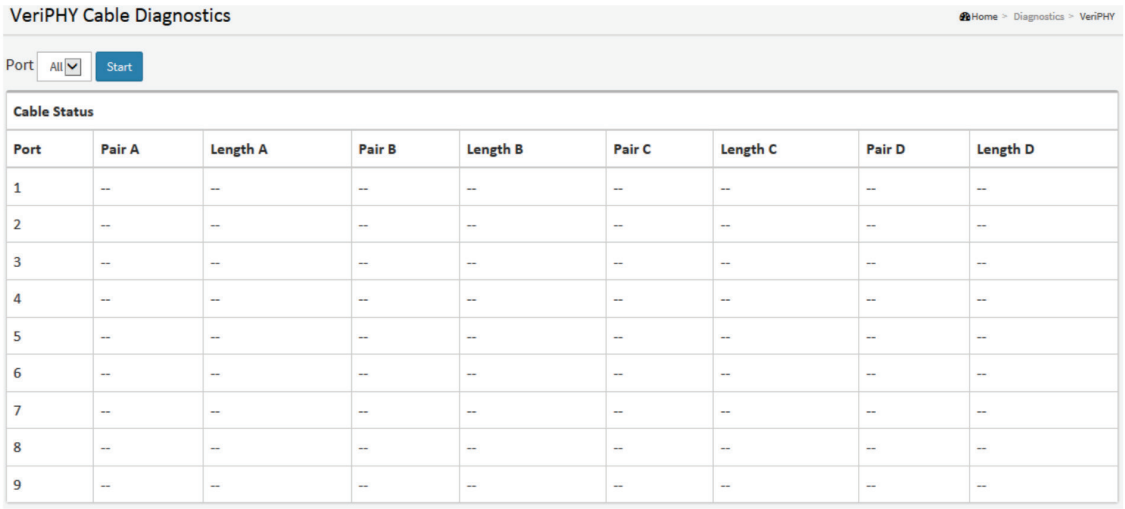



FIGURE 5-3. VERIPHY SCREEN

Parameter description:

- Port: The port for which you are requesting VeriPHY Cable Diagnostics.
- Cable Status:

- Port: Port number.

- Pair: The status of the cable pair.
- Length: The length (in meters) of the cable pair.

## 5.4 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 the traceroute IP Address.
2. Specify the traceroute Size.
3. Click Start.

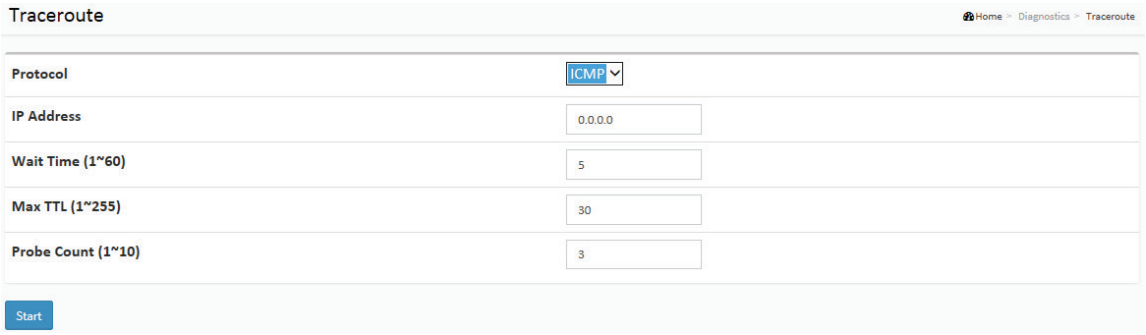



FIGURE 5-4. TRACEROUTE SCREEN

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) that the 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.

# CHAPTER 6: MAINTENANCE

This chapter describes the entire switch Maintenance configuration tasks to enhance the performance of a local network including Restart Device, Firmware upgrade, Save/Restore, and Import/Export.

## 6.1 RESTART DEVICE

This section describes how to restart the switch for any maintenance needs. Any configuration files or scripts that you saved in the switch should still be available afterwards.

### WEB INTERFACE

To configure a Restart Device Configuration in the web interface:

1. Click Restart Device.
2. Click Yes.

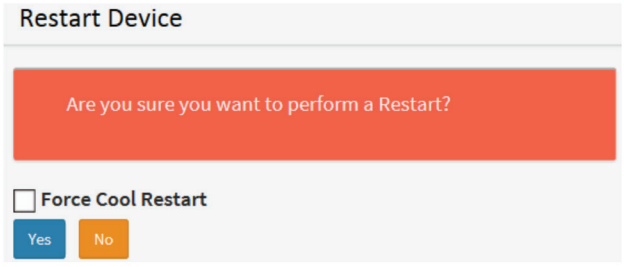



FIGURE 6-1. RESTART DEVICE

**Parameter description:**

- Restart Device: You can restart the switch on this page. After restart, the switch will boot normally.
- Buttons:

- Yes – Click “Yes” then the device will restart.
- No - Click to undo any restart action.

## 6.2 FACTORY DEFAULTS

This section describes how to reset the Switch configuration to Factory Defaults. Any configuration files or scripts will recover to factory default values.

### WEB INTERFACE

To configure a Factory Defaults Configuration in the web interface:

1. Click Factory Defaults.
2. Click Yes.

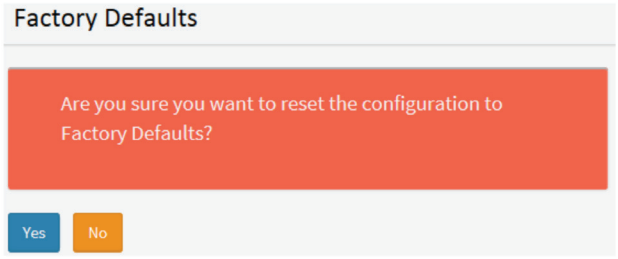



FIGURE 6-2. FACTORY DEFAULTS SCREEN

Parameter description:

- Buttons:

- Yes – Click the “Yes” button to reset the configuration to Factory Defaults.
- No - Click to to return to the Port State page without resetting the configuration.

## 6.3 FIRMWARE

This section describes how to upgrade the Firmware. The switch can be enhanced with more value-added functions by installing firmware upgrades.

### 6.3.1 FIRMWARE UPGRADE

This page enables you to update the firmware controlling the  switch..

#### WEB INTERFACE

To configure a Firmware Upgrade Configuration in the web interface:

1. Click the Browser to select Maintenance/Software in you device.
2. Click Download.


FIGURE 6-3. FIRMWARE DOWNLOAD SCREEN

Parameter description:

- Browse: Click the “Browse...” button to search the Firmware URL and filename.

NOTE: This page enables you to update 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 does not work. 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.

## 6.3.2 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.

NOTES:

1. If the active firmware image is the alternate image, only the "Active Image" table is shown. In this case, the Activate Alternate Image button is also disabled.
2. If the alternate image is active (due to a corruption of the primary image or by manual intervention), uploading a new firmware image to the device will automatically use the primary image slot and activate this.
3. The firmware version and date information may be empty for older firmware releases. This does not generate an error.

### WEB INTERFACE

To configure a Firmware Upgrade Configuration in the web interface:

1. Click Browser to select Maintenance/Software in your device.
2. Click Image Select.

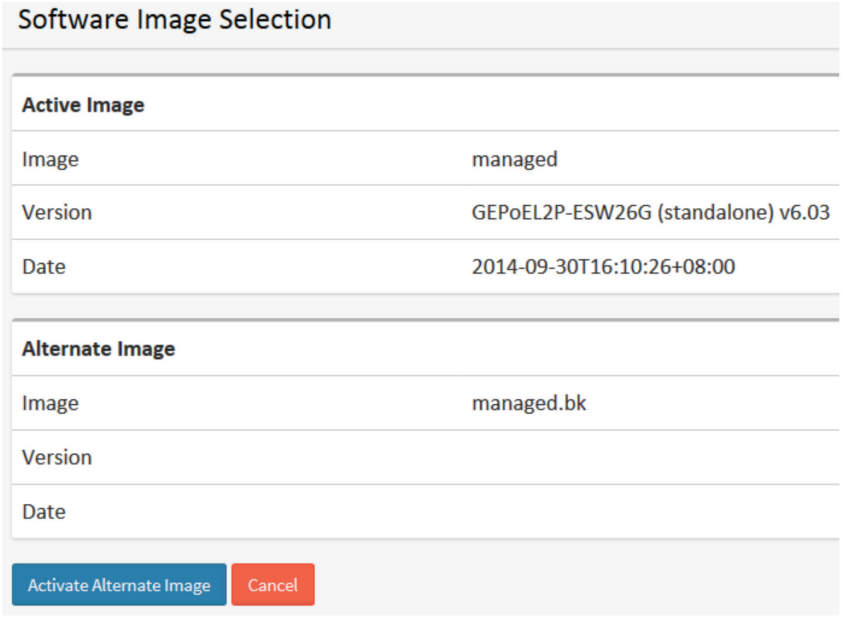



FIGURE 6-4. FIRMWARE SELECTION SCREEN

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 the system state.

- Cancel: Cancel activating the backup image. This navigates away from this page.

## 6.4 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.

You can also store up to two other files and apply them to running-config, thereby switching configuration.

### 6.4.1 SAVE STARTUP-CONFIG

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

#### WEB INTERFACE

To save running configuration in the web interface:

1. Click Browser to select Maintenance/Configuration in you device.
2. Click Apply Startup-Config Select.

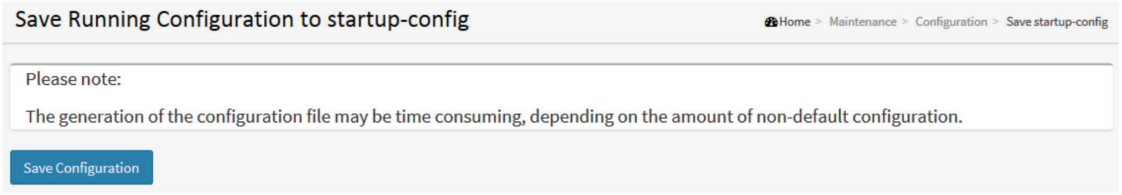



FIGURE 6-5. SAVE STARTUP CONFIGURATION SCREEN

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.

## 6.4.2 UPLOAD

The configuration upload function will back up and save the switch's configuration into the running web browser PC.

You can upload any of the files on the switch to the web browser. Select the file and click Upload running-config. This 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. Click Browser to select Maintenance/Configuration in you device.
2. Click upload Select.

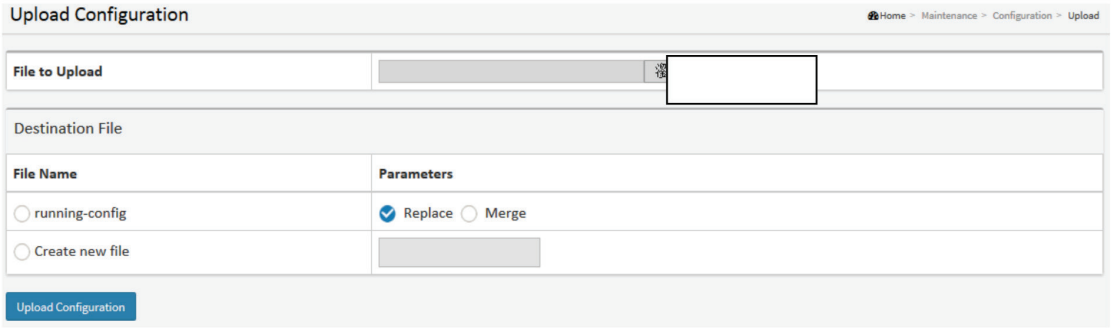



FIGURE 6-6. CONFIGURATION UPLOAD SCREEN

There are three system files:

1. running-config: A virtual file that represents the currently active configuration on the switch. This file is volatile.
2. startup-config: The startup configuration for the switch, read at boot time.
3. default-config: A read-only file with vendor-specific configuration. This file is read when the system is restored to default settings.

Parameter description:

- 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. You can configure the web browser's upload file path to keep the configuration file.

## 6.4.3 DOWNLOAD

This section describes how to export the Switch Configuration for maintenance needs. Any current configuration files will be exported as text format.

You can download a file from the web browser to all the files on the switch, except for default-config, which is read-only.

Select the file to download, select the destination file on the target, then 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), you cannot create new files, but an existing file must be overwritten or another deleted first.

### WEB INTERFACE

To download configuration in the web interface:

1. Click the Browser to select Maintenance/Configuration in you device.
2. Click Download Select.

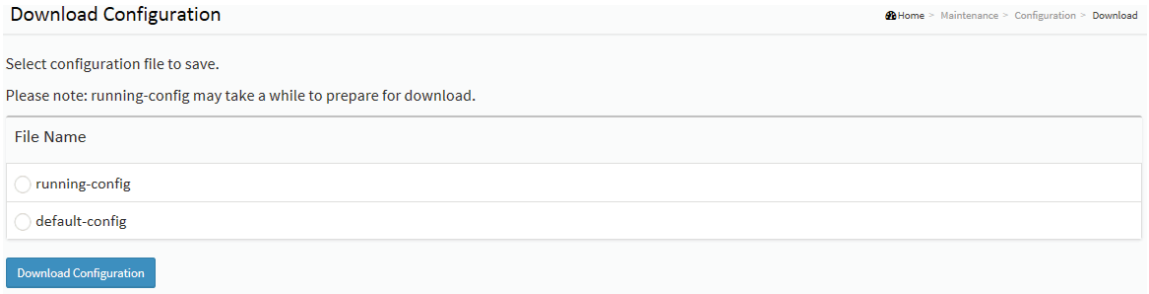



FIGURE 6-7. CONFIGURATION DOWNLOAD SCREEN

Parameter description:

- Browse: Click the “Browse...” button to search the configuration text file and filename.
- Download: Click the “Download” button, then the switch will start to download the configuration from the configuration’s stored location in the PC or Server.

## 6.4.4 ACTIVATE

You can 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. Click the Browser to select Maintenance/Configuration in your device.
2. Click Activate Select.

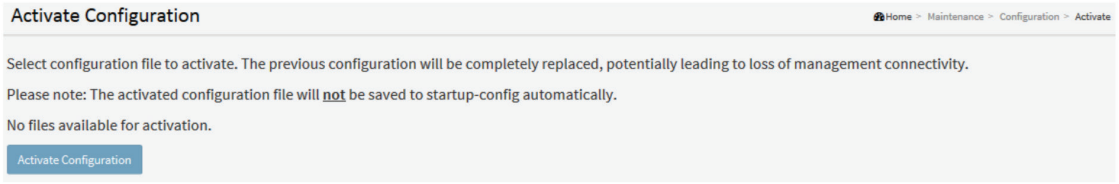



FIGURE 6-8. CONFIGURATION ACTIVATION SCREEN

There are two system files:

1. default-config: A read-only file with vendor-specific configuration. This file is read when the system is restored to default settings.
2. startup-config: The startup configuration for the switch, read at boot time.

Parameter description:

- Buttons:

- Activate Configuration: Click the “Activate” button ,then the default-config or startup-config file will be activated to be the switch’s running configuration.

## 6.4.5 DELETE

You can delete any of the writable files stored in flash, including startup-config. If you do this and the switch is rebooted without saving, this resets the switch to the default configuration.

### WEB INTERFACE

To delete a configuration in the web interface:

1. Click the Browser to select the Maintenance/Configuration in your device.
2. Click Delete Select.

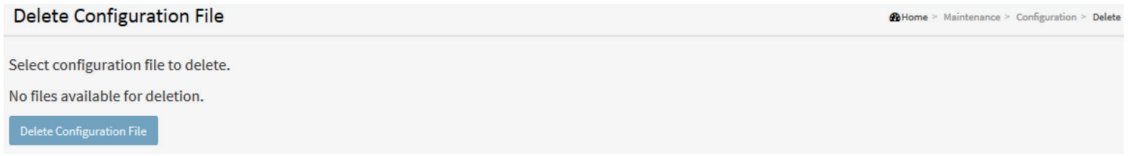



FIGURE 6-9. DELETE CONFIGURATION SCREEN

There is one system file:  startup-config: The startup configuration for the switch, read at boot time.

Parameter description:

- Buttons:

- Delete Configuration: Click the “Delete” button, then the startup-config file will be deleted This resets the switch to the default configuration.

Parameter description:

- Buttons:

- Delete Configuration: Click the “Delete” button, then the startup-config file will be deleted This resets the switch to the default configuration.

## 7.1 INFORMATION

The Information page shows general system information for the switch including its DMS software version, the maximum number of devices it can manage, the MAC Address, and the IP Address.

### WEB INTERFACE

To configure DMS Information in the web interface:

1. Click Management, and Information.
2. Select Enabled or Disabled for the DMS state.
3. Specify the IP Setting.
4. Select Enabled or Disabled for the DHCP server.
5. Click Save to save changes.

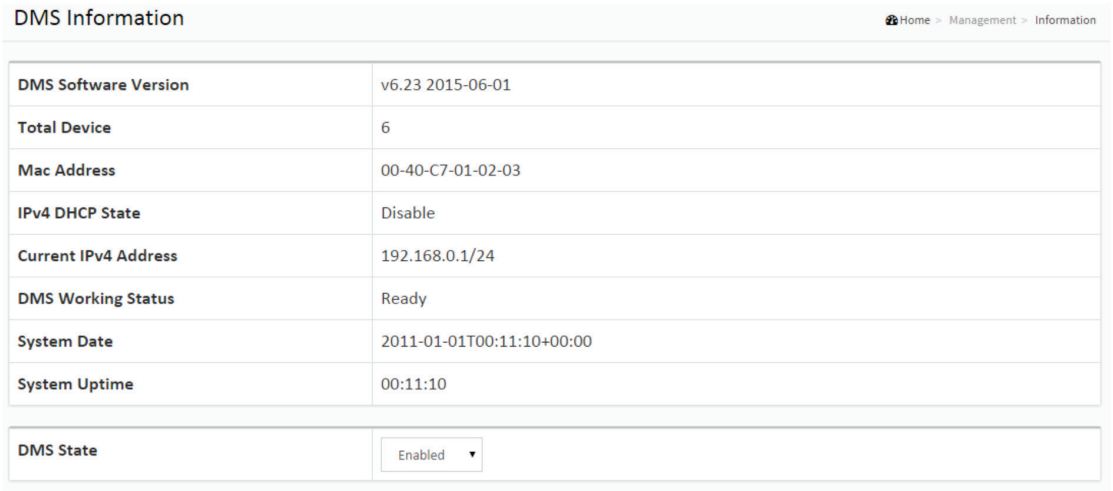



FIGURE 7-1. DMS INFORMATION SCREEN

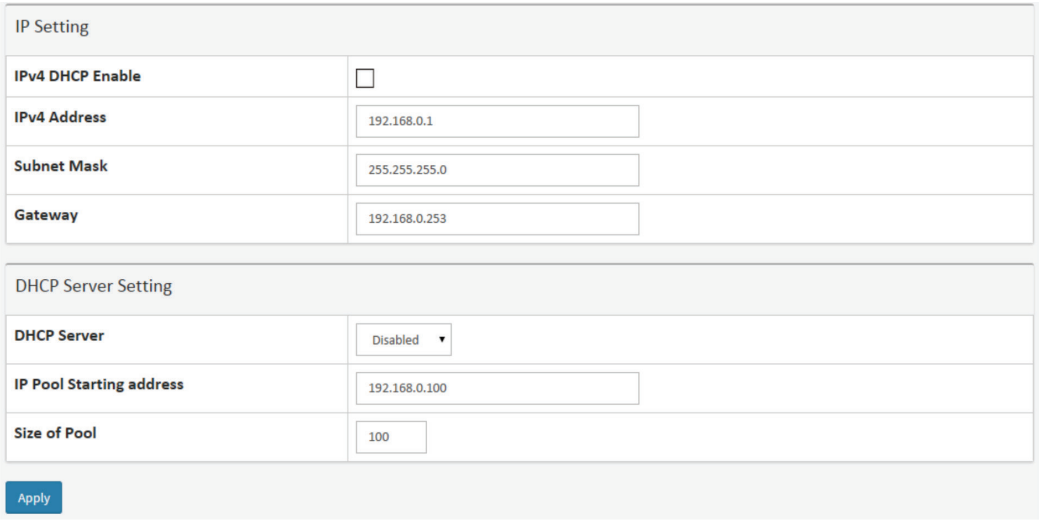



FIGURE 7-2. IP SETTING SCREEN

Parameter description:

- DMS Software Version: Displays the current DMS firmware version number.
- Total Device: Displays the number of devices in the topology.
- MAC Address: The MAC Address of this switch.
- Current IP Address: The current address (IPv4). DMS use switch interface VLAN1.
- DMS State: Enabled or Disabled DMS.
- IP Address: The IPv4 address of the interface VLAN1.
- System name: The IPv4 network mask of the interface VLAN1.

## 7.2 DEVICE LIST

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

### WEB INTERFACE

To configure the Device list in the web interface:

1. Click Management and Device List.
2. Click to refresh the Devices List.
3. Evoke then the device will refresh the information automatically.
4. Click to edit Device Name and Http Port
5. Evoke Off-Line device to remove.
6. Click to save changes

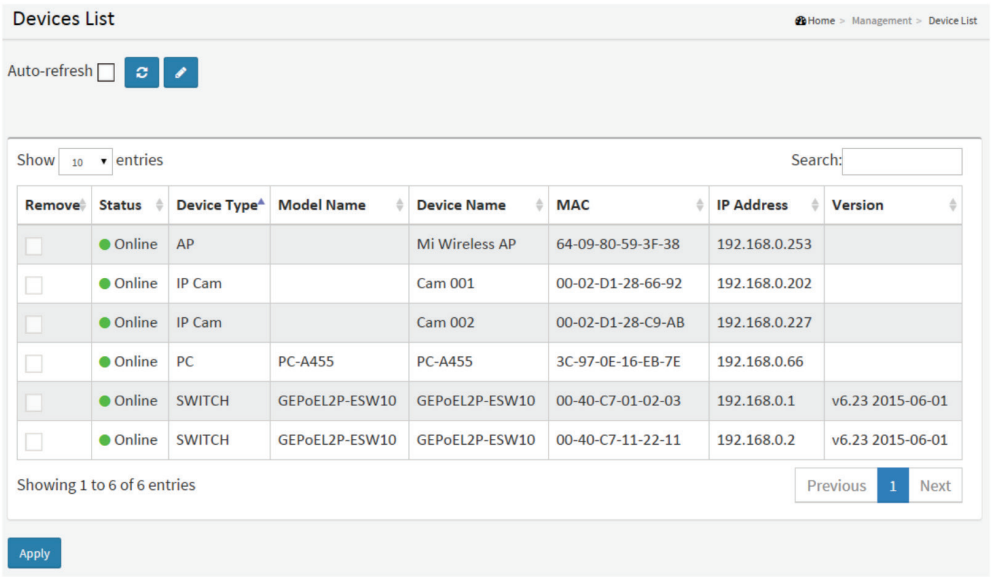



FIGURE 7-3. DEVICE LIST SCREEN

- Parameter description:
- Remove:  Off-Line devices removed from the selected device.
- Status:  Device link state (On/Off Line)
- Model Name:  Device model name
- Device Name:  Device name
- Edit Device Name:  Device name edit (save in flash)
- MAC:  Device mac
- IP Address:  Device IP address, hyperlink re-direct to device website
- Version:  Device firmware version.

# CHAPTER 8: DMS GRAPHIC MONITORING

## 8.1 TOPOLOGY VIEW

In this page, you can see a visual view of the topology in a cluster of networks.

### WEB INTERFACE

To configure DMS Topology View in the web interface:

1. Click Graphical Monitoring, and Topology View.
2. Click to select the display information in Topology View.

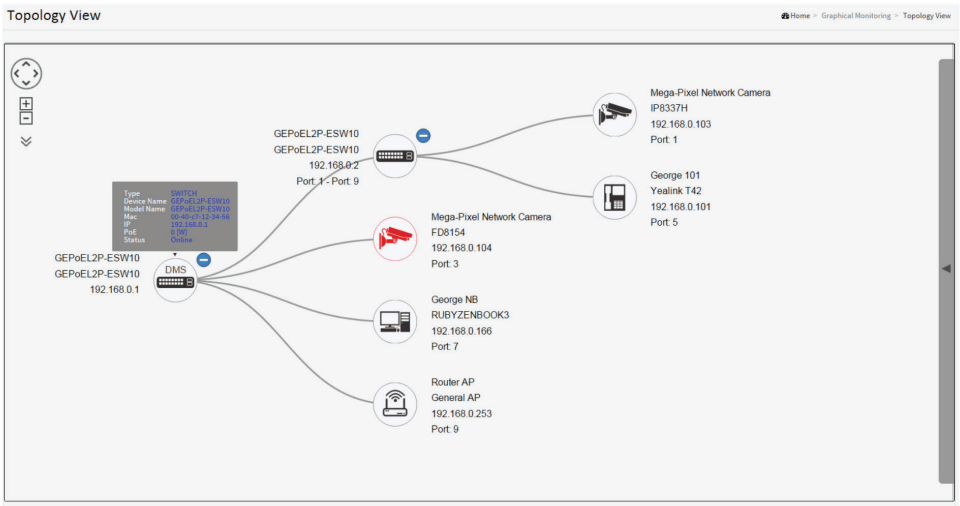



FIGURE 8-1. TOPOLOGY VIEW

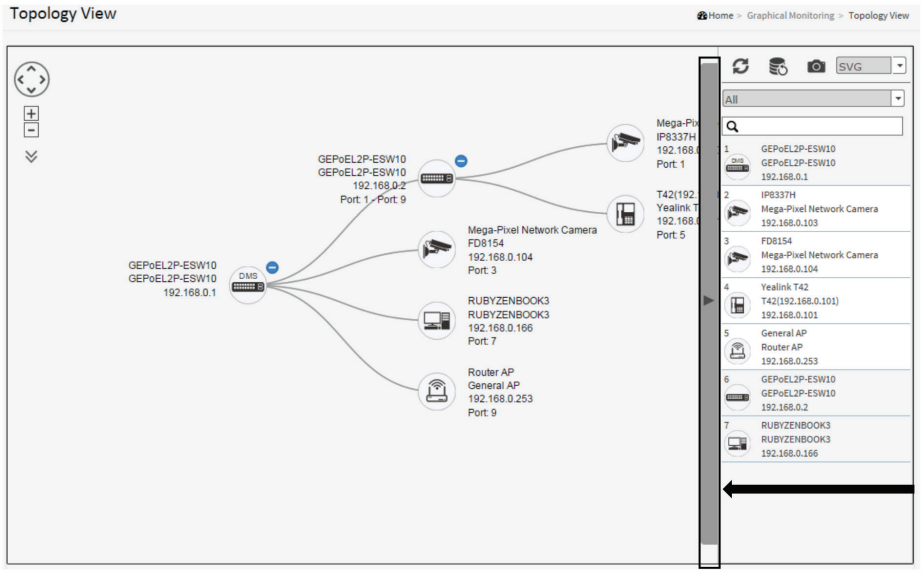



FIGURE 8-2. TOPOLOGY VIEW

# CHAPTER 8: DMS GRAPHIC MONITORING

Parameter description:

• Login: Login to this device.

• Troubleshooting: Move to the troubleshooting page.

• Find my switch: Allows administrators to quickly and easily find the Switch in their cabinet.

• Reboot Device: Reboot the PD device.

• Device Type: Select Device Type for PC, IP phone, IP cam, AP, or other device.

DIAGRAM: Click to refresh the Topology View

DIAGRAM: Click to rescan the Topology View

DIAGRAM: Use the directional pad to scroll up, down, left, or right.

DIAGRAM: Use the slider to zoom in/out. Alternatively, you can use the mouse to navigate by clicking and dragging the left mouse button. Use the mouse wheel to zoom in/out.

DIAGRAM: Save the whole View to SVG, PNG or PDF

DIAGRAM : Select the device category.

DIAGRAM : Search for device by typing IP/MAC address or Model/Device name.

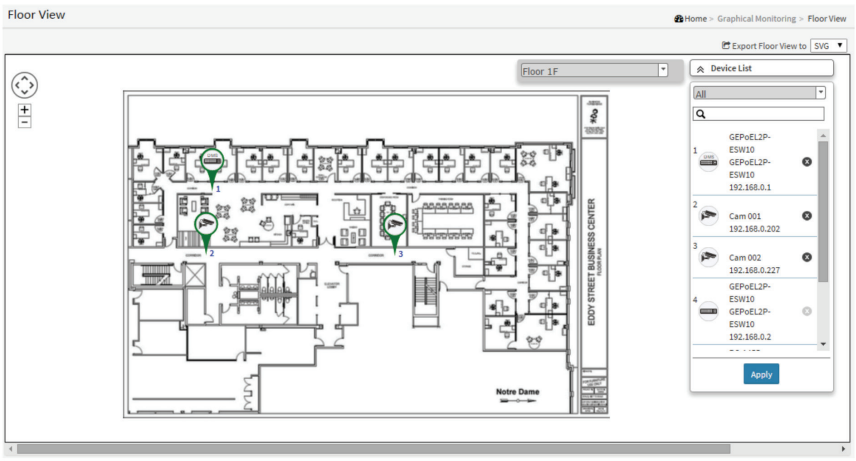
## 8.2 FLOOR VIEW

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.

### WEB INTERFACE

To configure DMS Floor View in the web interface:

1. Click DMS, Graphic Monitoring, Floor Plan and Floor View.




Use the directional pad to scroll up, down, left, or right.

Use the slider to zoom in/out. Alternatively, you can use the mouse to navigate by clicking and dragging the left mouse button. Use the mouse wheel to zoom in/out


Save the whole View to SVG, PNG or PDF


Select the device category.

Search for device by typing IP/MAC address or Model/Device name.

FIGURE 8-3. FLOOR VIEW

## 8.3 MAP VIEW

In this page, you can view a realistic representation of a device in the network. To find one of devices within the network, enter the device name in the search bar. Click “Device List” to hide the “Device List” on the page or show a list of devices.

### WEB INTERFACE

To configure DMS Map View in the web interface:

1. Click DMS, Graphic Monitoring, and Map View.


Use the directional pad to scroll up, down, left, or right.

Use the slider to zoom in/out. Alternatively, you can use the mouse to navigate by clicking and dragging the left mouse button. Use the mouse wheel to zoom in/out


Save the whole View to SVG, PNG or PDF

Select the device category.

Search for device by typing IP/MAC address or Model/Device name.

FIGURE 8-4. MAP VIEW

## 9.1 FLOOR VIEW

In this page, an administrator can add or delete a custom map or floor image.

### WEB INTERFACE

To configure DMS Information in the web interface:

1. Click Maintenance and Floor Image.
2. Click “Browse…” to select Floor image in your device.
3. Click Add.

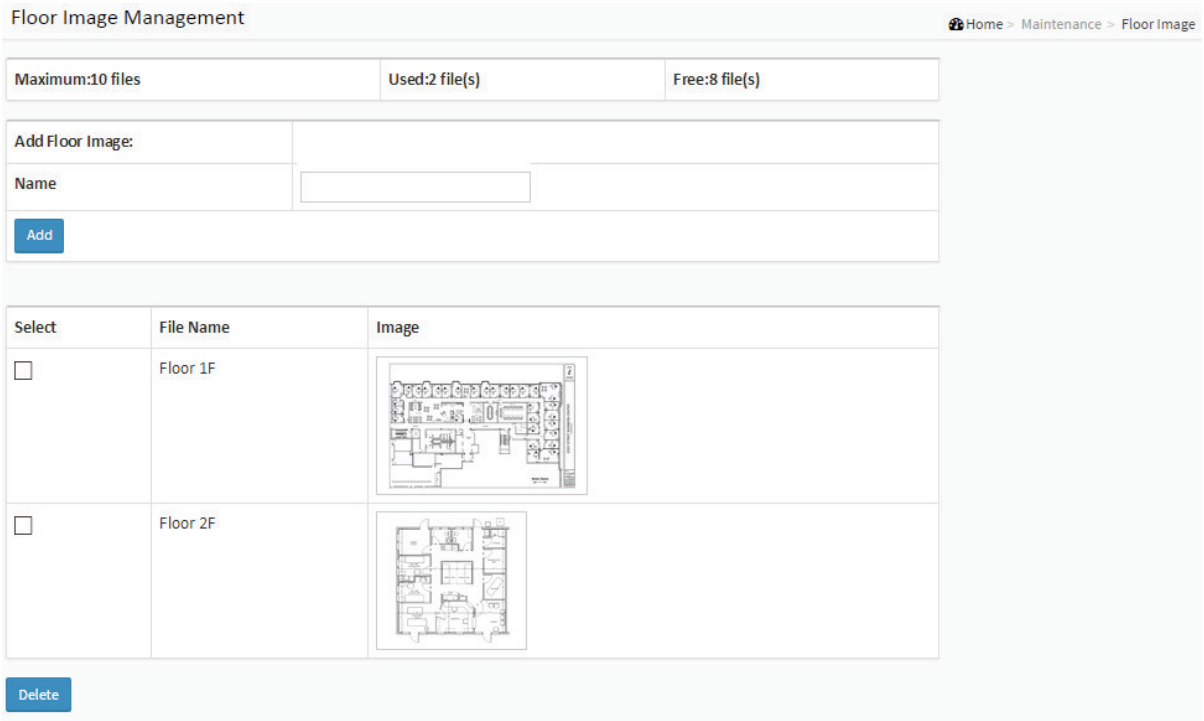



FIGURE 9-1. FLOOR IMAGE

## 9.2 DIAGNOSTICS

In this page, you can diagnose any issue you have with a device connected to the network. This feature is designed primarily for administrators to verify and test the link route between the switch and the device. A diagnostics solution is provided by the system so that administrators can detect where the problem lies.

NOTE: The topology of the network must be saved for this function to work properly.

### WEB INTERFACE

To configure DMS Information in the web interface:

1. Click DMS, Diagnostics, and Device Status.
2. Select the device to start the recover Mechanism.

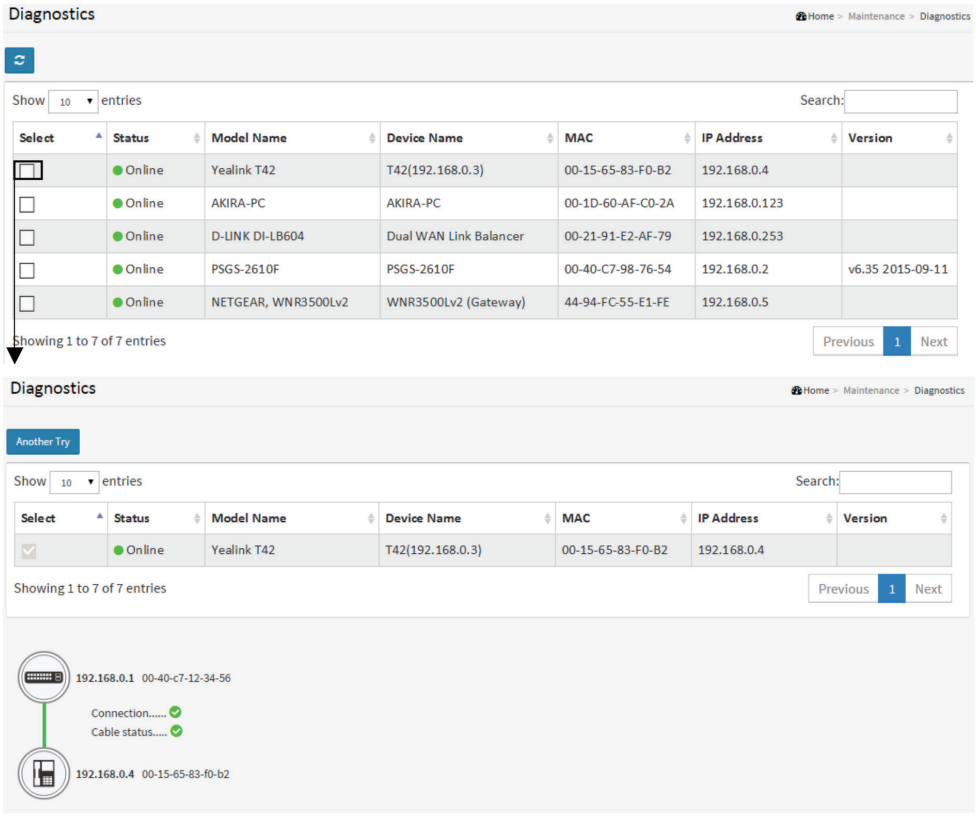



FIGURE 9-2. DEVICE STATUS

## 9.3 TRAFFIC CHART

This page displays a visual chart of network traffic of all the devices managed by DMS switch.

### WEB INTERFACE

To configure DMS Information in the web interface:

1. Click DMS, Monitor, and Traffic.
2. Specify the DMS state, longitude and latitude, IP address, Subnet Mask.
3. Click Apply.

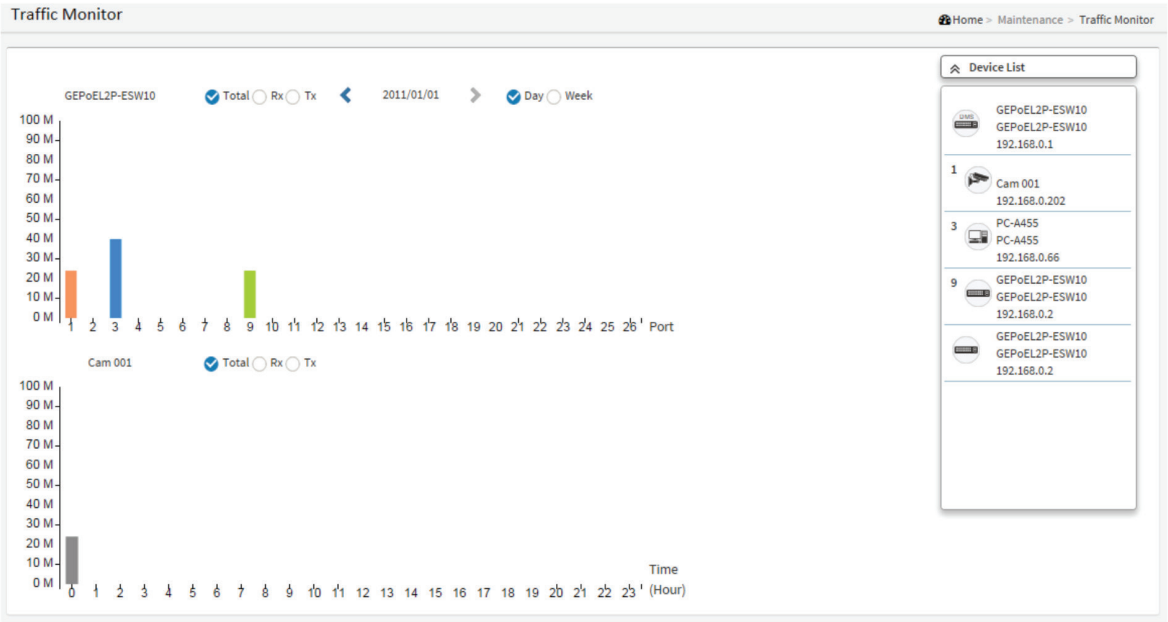



FIGURE 9-3. TRAFFIC CHART

# CHAPTER 10: COMPLIANCE

## 10.1 FCC

### 10.1.1 FCC WARNING

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the Instruction manual, may cause harmful interference to radio communications.

### 10.1.2 FCC CAUTION

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

## 10.2 CE MARK WARNING

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

# NOTES

# NOTES

# NOTES

NEED HELP?
LEAVE THE TECH TO US

# LIVE 24/7 TECHNICAL SUPPORT

**1.877.877.2269**

BLACK BOX®