C70-00F-02

L2 PRO PoE Switches

GUI User's Manual

About This Manual

Copyright

.

Purpose

This GUI user guide gives specific information on how to operate and use the management functions of the C70 Series via HTTP web browser

Audience

The Manual is intended for use by network administrators who are responsible for operating and maintaining network equipment; consequently, it assumes a basic working knowledge of general switch functions, the Internet Protocol (IP), and Hypertext Transfer Protocol (HTTP).

CONVENTIONS

The following conventions are used throughout this manual to show information.

WARRANTY

See the Customer Support/ Warranty booklet included with the product. A copy of the specific warranty terms applicable to your Manufacture products and replacement parts can be obtained from your Manufacture Sales and Service Office authorized dealer.

Disclaimer

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

Revision History

Release note	Date	Revision
Initial Release	2026/03/31	

Table of Contents

Overview

In this User Guide, it will not only tell you how to install and connect your network system but configure and monitor the C70 Series through the web by (RJ-45) serial interface and Ethernet ports step-by-step. Many explanations in detail of hardware and software functions are shown as well as the examples of the operation for web-based interface.

The C70 Series are L2 PRO PoE switches from AETEK INC., is a portfolio of affordable managed switches that provides a reliable infrastructure for your business network. These switches deliver more intelligent features you need to improve the availability of your critical business applications, protect your sensitive information, and optimize your network bandwidth to deliver information and applications more effectively. It provides the ideal combination of affordability and capabilities for entry level networking includes small business or enterprise application and helps you create a more efficient, better-connected workforce.

C70 Series is L2 PRO PoE Switches; the specification is highlighted as follows.

Features

- **Layer 2 Switch**
  - 802.1d (STP), 802.1w (RSTP), 802.1s (MSTP)
  - Loop protection
  - SNMP
  - QoS
  - VLAN
  - LACP
  - DHCP Server

Chapter 1 Operation of Web-based Management

Initial Configuration

This chapter instructs you how to configure and manage the C70 Series through the web user interface. With this facility, you can easily access and monitor through any one port of the switch all the status of the switch, including, each port activity, Spanning tree status, port aggregation status, VLAN and priority status, and so on.

The default values of the C70 Series are listed in the table below:

IP Address	192.168.1.1
Subnet Mask	255.255.255.0
Default Gateway	192.168.1.254
User Name	admin
Password	admin

After the C70 Series have been finished configuring the interface, you can browse it at re-login page. In the IP address bar of a browser, it will show the following screen and ask you to input username and password in order to login and access authentication.

The default username is **"admin"** and password is "**admin"**. For the first time to use, please enter the default username and password, and then click the **<Login>** button. The login process now is completed. In this login menu, you have to input the complete username and password respectively, the C70 Series will not give you a shortcut to username automatically. This looks inconvenient, but safer.

In the C70 Series, allowed two or more users using administrator's identity to manage this switch, which administrator to do the last setting, it will be an available configuration to effect the system.

NOTE:
To optimize the display effect, we recommend you to use Google Chrome,, Firefox, Microsoft Edge and have the resolution 1024x768. The switch supported neutral web browser interfaces

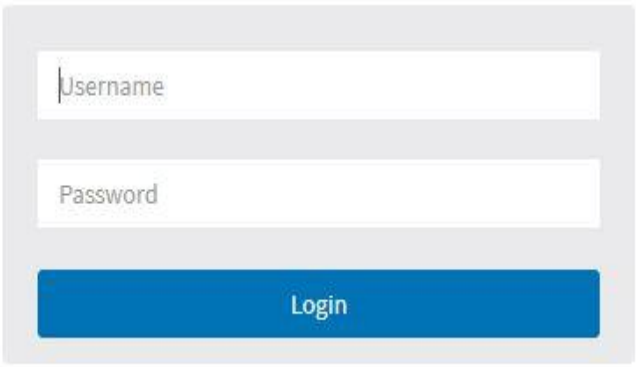


Figure 1: The login page

Chapter 2 FIRST TIME WIZARD

When the first time you use this device, you can configure some basic settings, such as password, IP address, date & time, system information.

According to the following procedure:

Step1: Change default password

Configure new password and enter it again.

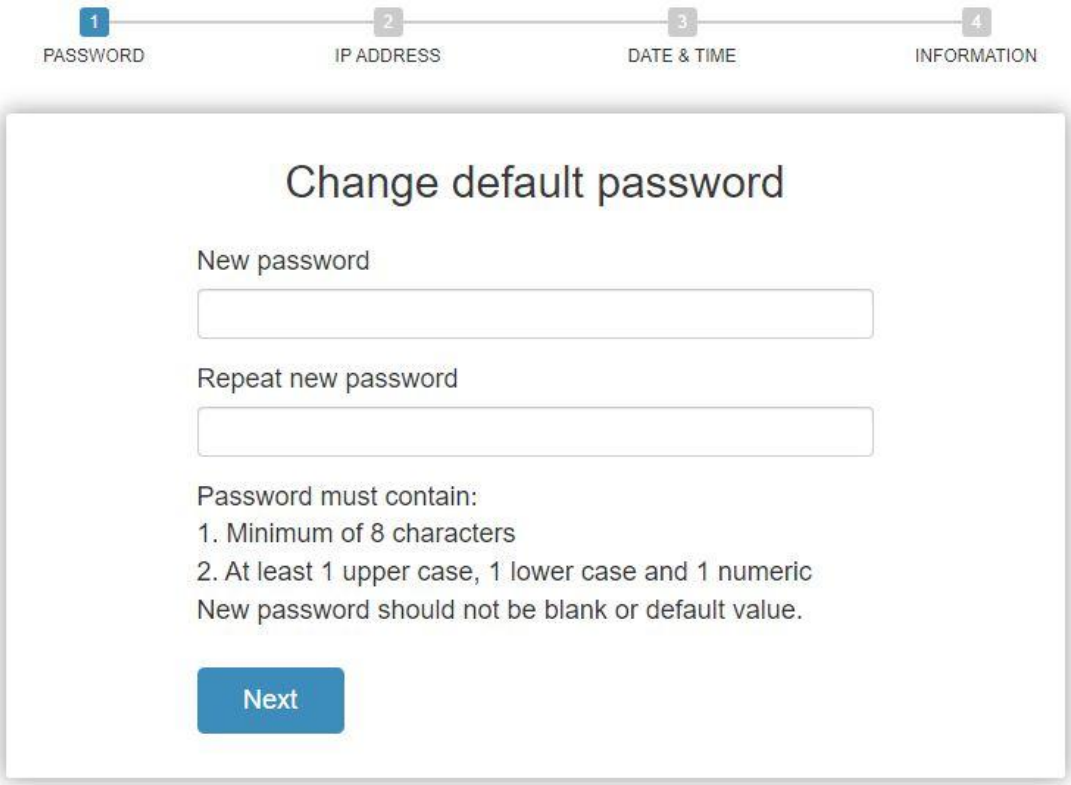


Figure 2-0: Change default password

Step2: Set IP address

Select "obtain IP address via DHCP" or "Set IP address manually" to set IP address.

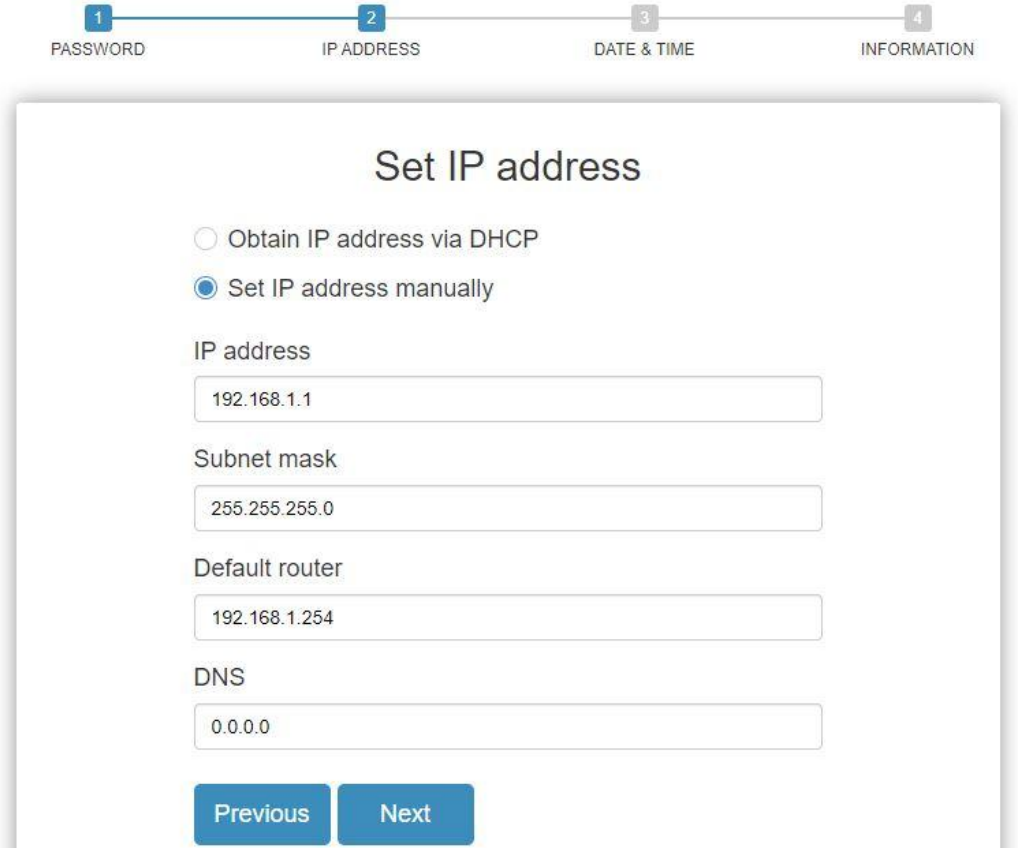


Figure 2-1: Set IP address

Step3: Set date and time

Enable "Automatic data and time" or select manually to set date and time.

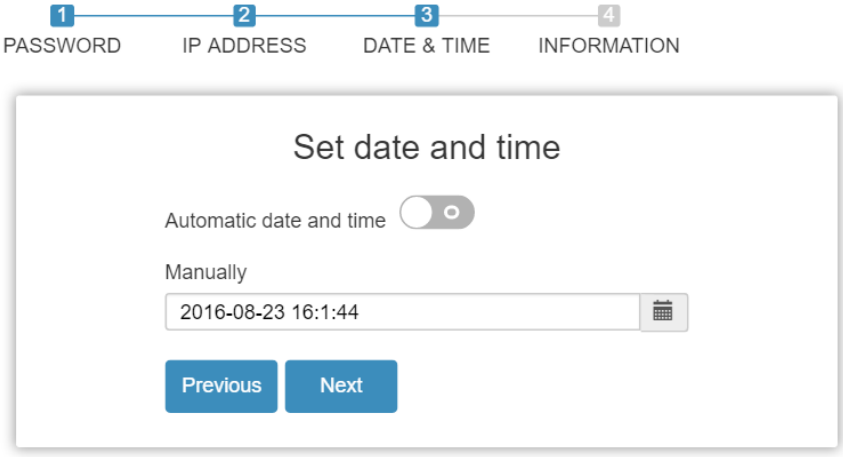


Figure 2-2: Set date and time

Step4: Set system information

You can set some system information to this device, such as “System contact”, “System name”, “System location”.

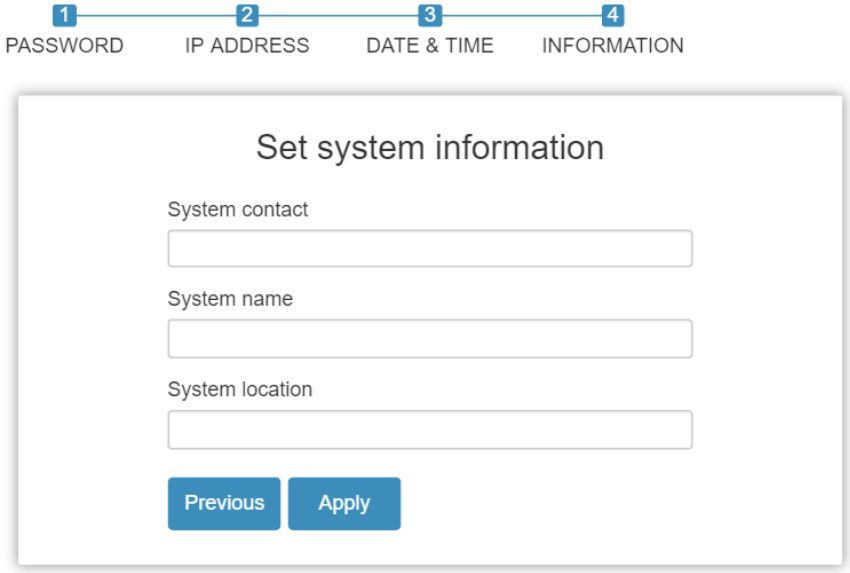


Figure 2-3: Set system information

Chapter 3 SYSTEM

AETEK PoE Managed switch software provides rich functionality for switches in your networks. This guide describes how to use Web-based management interface (Web UI) to configure AETEK managed switch software features.
The Web UI supports all frequently used web browsers listed below:

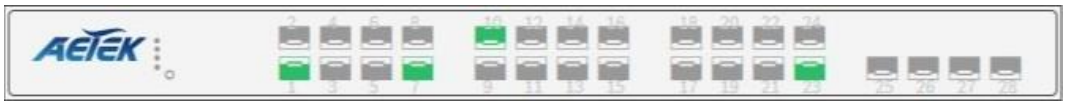


Figure 3-0: Port Information

In the Web UI, the left column shows the configuration menu. The top row shows the switch's current linking status described below.

- Orange : The LAN port is powered on and is connected with 10/100M linking speed powered device.
- Green : The LAN port is powered on and is connected with 1000M linking speed powered device
- Gray : The LAN port is NOT connected with any device.

On the top-right part, it shows useful functions for users to save the system configuration, log out the system. The rest of the screen area displays the configuration settings.

3-1 System Information

You can identify the system by configuring system name, location and the contact of the switch. The switch system's contact information is provided here.

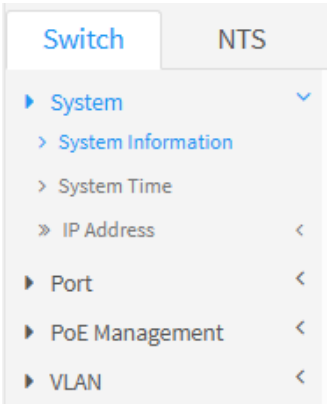


Figure 3-1: System

Web interface

To configure System Information in the web interface:

1. Click System -> System Information.
2. Input System Name, Location and Contact information in this page.
3. Click Apply.

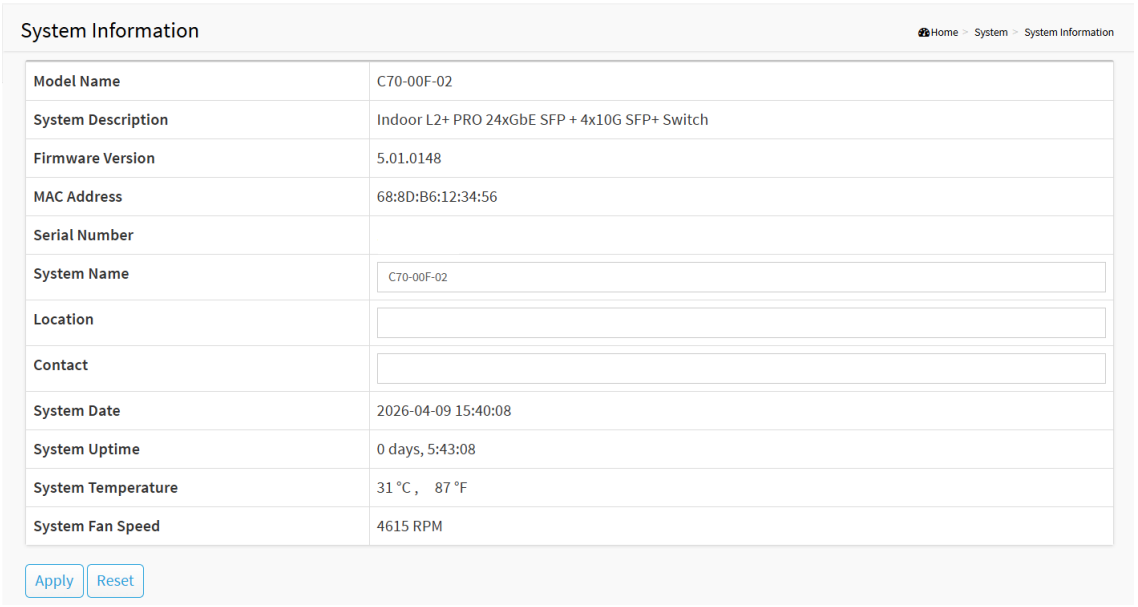


Figure 3-1: System Information

Parameter Description:

- **Model Name**

  Displays the factory defined model name for identification purpose.

- **System Description**

  Displays the system description.

- **Firmware Version**

  The software version of this switch.

- **MAC Address**

  Base MAC address of the switch.

- **Serial Number**

  The unique identification code assigned to the device.

- **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), 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.

- **Location**

  The physical location of this node(e.g., telephone closet, 3rd floor). The allowed string length is 0 to 128, and the allowed content is the ASCII characters from 1 to 32.

- **Contact**

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

- **System 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 operated.

3-2 System Time

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

Web interface

To configure System Time in the web interface:

1. Click System -> System Time.
2. Specify the Time parameter.
3. Click Apply.

NOTE:
Each time when you click apply, it will set new date to system. If **Clock Source** is "Local Setting" and **Daylight Saving Time** is "On", the **System Date** should be manual to "Standard Time" to avoid time configuration shift.

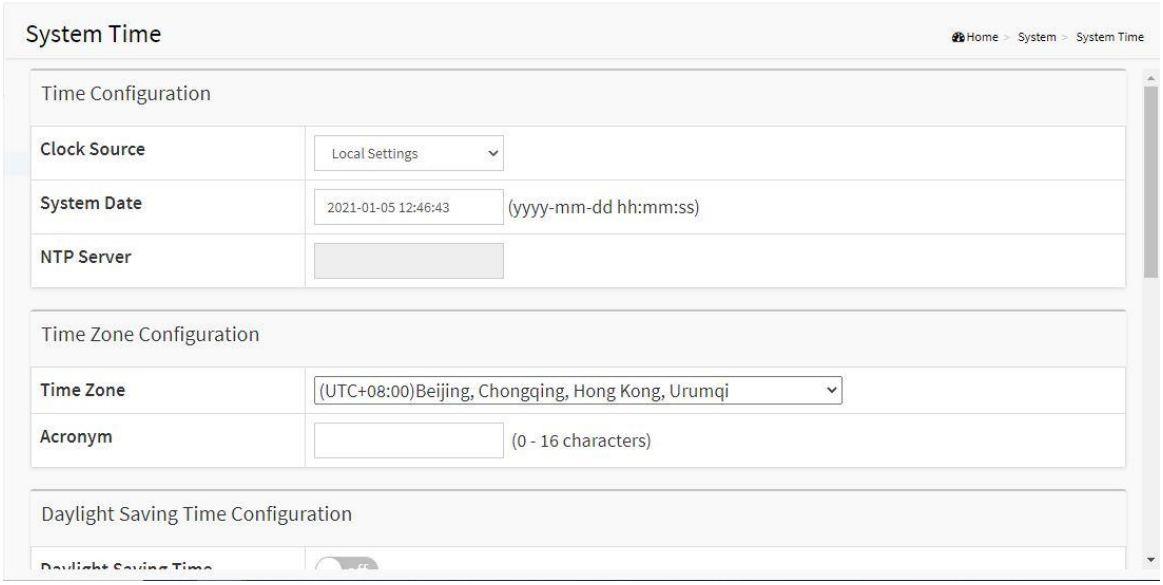


Figure 3-2: System Time

Parameter Description:

- **Time Configuration**

  You can input Year, Month, Day, Hour, Minute and Second manually, and to enable/disable obtaining system time through the time server.

- **Time Zone**

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

- **Daylight Saving Time**

  To enable/disable daylight saving time function.

- **Start Time Settings**

  Month - Select the starting month.

  Day - Select the starting day.

  Hours - Select the starting hour.

- **End Time Settings**

  Month - Select the ending month.

  Day - Select the ending day.

  Hours - Select the ending hour.

- **Offset**

  The number of minutes to be added by Daylight Saving Time. (Range: 1 to 720 minutes)

3-3 IP Address Settings

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

3-3-1 Interface IPv4 Settings

To configure an IPv4 Settings in the web interface:

Web Interface

1. Click System -> IP Address -> Interface IPv4 Settings
2. Click Add New Entry.
3. In VLAN, enter the VLAN ID (1-4094).
4. Enter the IPv4 Address and Mask Length.
5. Click Apply.

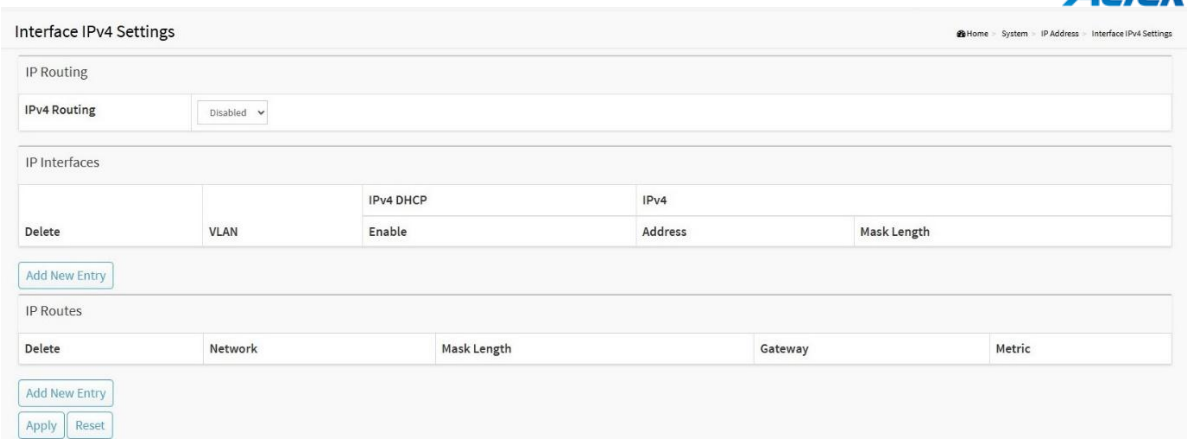


Figure 3-3-1: Interface IPv4 Settings

Parameter Description:

- **IPv4 Routing**

  Enables or Disables the IPv4 routing capability on the device.

- **Delete**

  To delete the entry, select the checkbox and click Apply button to remove it from the list.

- **VLAN**

  Specifies the VLAN ID associated with this IP interface. Only ports in this VLAN can access the interface. This field is editable only when adding a new entry. Valid range: 1–4094.

- **IPv4 DHCP**

  Enables or Disables the DHCP client for the interface. 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 System Name as the hostname for DNS lookup.

- **IPv4 Address**

  The IPv4 address of the interface in dotted-decimal notation (e.g., 192.168.30.1).

  Must be a valid host address within the subnet (i.e., not the network or broadcast address).

- **IPv4 Mask Length**

  The subnet prefix length in bits for the IPv4 address. Valid values: 1–30 (e.g., 24 = 255.255.255.0).

- **Network**

  The destination IPv4 network address in dotted decimal notation.

- **Gateway**

  The IPv4 address of the next-hop router (gateway) used to reach the destination network.

- **Metric**

  The IPv4 routing metric.

- **Add New Entry[Button]**

  Click to create a new configuration entry. Specify and configure the new entry.

- **Apply[Button]**

  Click to apply changes.

- **Reset[Button]**

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

3-3-2 Interface IPv6 Settings

To configure an IPv6 Settings in the web interface:

Web Interface

1. Click System -> IP Address -> Interface IPv6 Settings
2. Click Add New Entry.
3. In VLAN, enter the VLAN ID (1-4094).
4. Enter the IPv6 Address and Mask Length.
5. Click Apply.

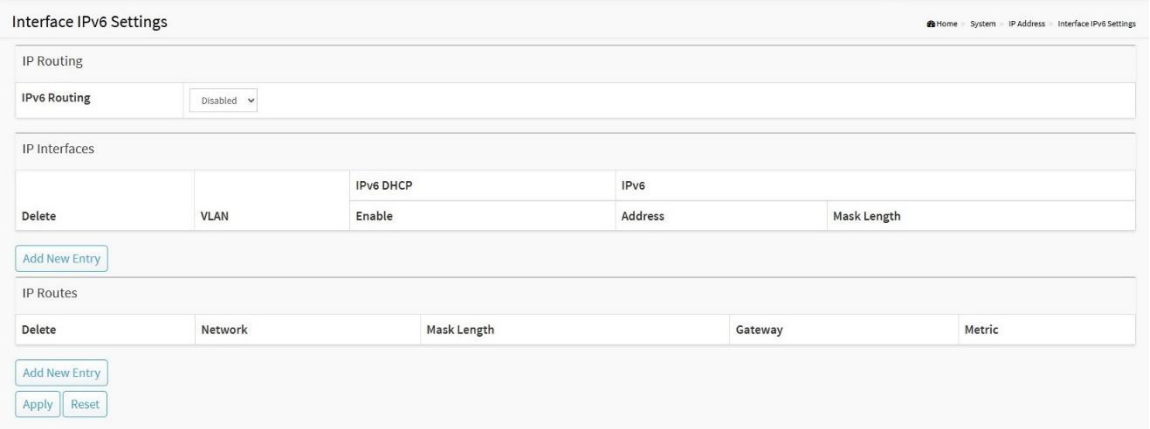


Figure 3-3-2: Interface IPv6 Settings

Parameter Description:

- **IPv6 Routing**

  Enables or Disables the IPv6 routing capability on the device.

- **Delete**

  To delete the entry, select the checkbox and click Apply button to remove it from the list.

- **VLAN**

  Specifies the VLAN ID associated with this IP interface. Only ports in this VLAN can access the interface. This field is editable only when adding a new entry. Valid range: 1–4094.

- **IPv6 DHCP**

  Enables or Disables the DHCP client for the interface. If this option is enabled, the system will configure the IPv6 address and mask of the interface using the DHCP protocol. The DHCP client will announce the System Name as the hostname for DNS lookup.

- **IPv6 Address**

  The IPv6 address of the interface in colon-hexadecimal notation. Must be a valid host address within the subnet.

- **IPv6 Mask Length**

  The subnet prefix length in bits for the IPv6 address. Valid values: 0–128.

- **Network**

  The destination IPv6 network address in colon-hexadecimal notation.

- **Gateway**

  The IPv6 address of the next-hop router (gateway) used to reach the destination network.

- **Metric**

  The IPv6 routing metric.

- **Add New Entry[Button]**

  Click to create a new configuration entry. Specify and configure the new entry. Then click "Apply" button.

- **Apply[Button]**

  Click to apply changes.

- **Reset[Button]**

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

3-3-3 Management IP Settings

Web Interface

To configure an IP Settings in the web interface:

1. Click System -> IP Address -> Management IP Settings
2. Enable or Disable the IPv4 DHCP Client.
3. Specify the IPv4 Address, Subnet Mask and Gateway.
4. Input IPv4 DNS Server if desired.
5. Click Apply.

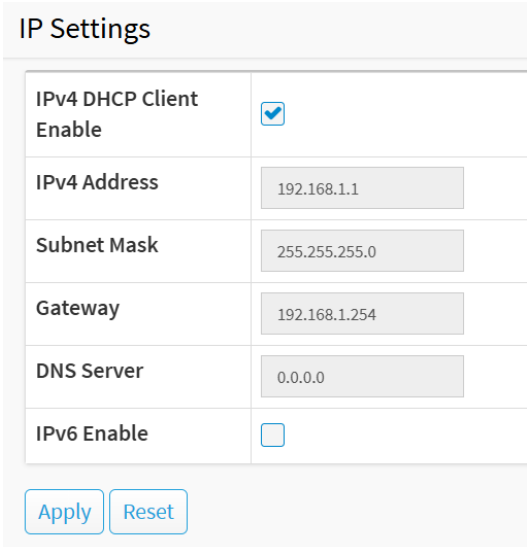


Figure 3-3-3: Management IP Settings

Parameter Description:

- **DHCP Client Enable**

Enable the DHCP client by clicking this checkbox. 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 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.

- **Subnet Mask**

  User IP subnet mask of the entry.

- **Default Gateway**

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

- **DNS Server**

  This setting controls the DNS name resolution done by the switch.

- **IPv6 Enable**

  Enables or disables the IPv6 DHCP client. When enabled, the switch automatically obtains its IPv6 address and configuration through DHCPv6.

3-3-4 Link Local IP Settings

The Link Local IP settings allow you to select a specific interface to configure its IPv4 Link-Local IP address for local network communication. This enables the device to communicate with other nodes on the same network segment when a DHCP server is unavailable.

Web Interface

To configure the Link Local IP Settings in the web interface:

1. Click System -> IP Address -> Link Local IP Settings
2. Select the specific interface.
3. Click Apply.

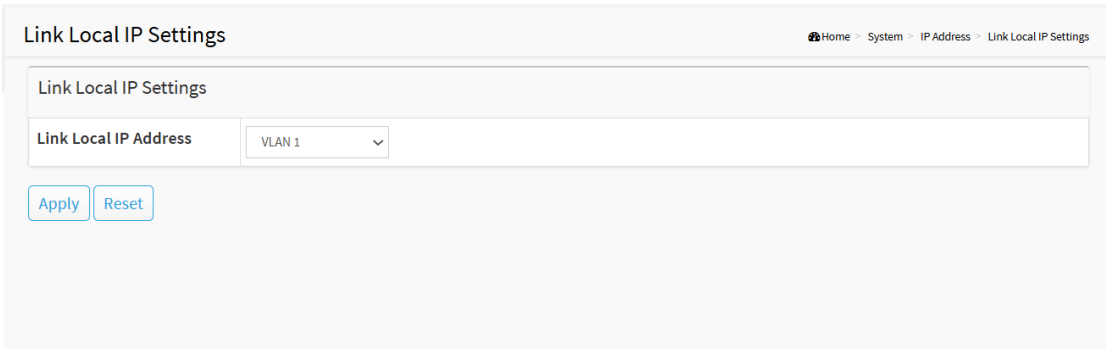


Figure 3-3-4: Link Local IP Settings

Parameter Description:

- **Link Local IP Address**

  Select the specific interface (e.g., VLAN) from the drop-down list to enable the Link-Local IP functionality on that interface.

Chapter 4 Port

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

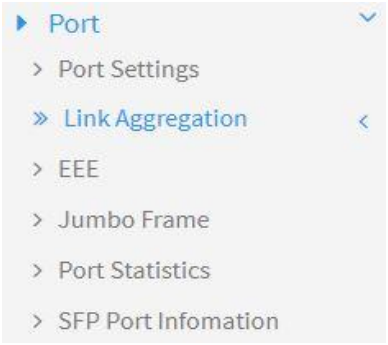


Figure 4-0: Port Setting

4-1 Port Setting

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

Web Interface

To configure a Current Port Configuration in the web interface:

1. Click Port -> Port Setting.
2. Click the port number which you want to configure. (For example: Port 9)
3. Click Edit.
4. Specify the parameters you want to configure.
5. Click Apply.

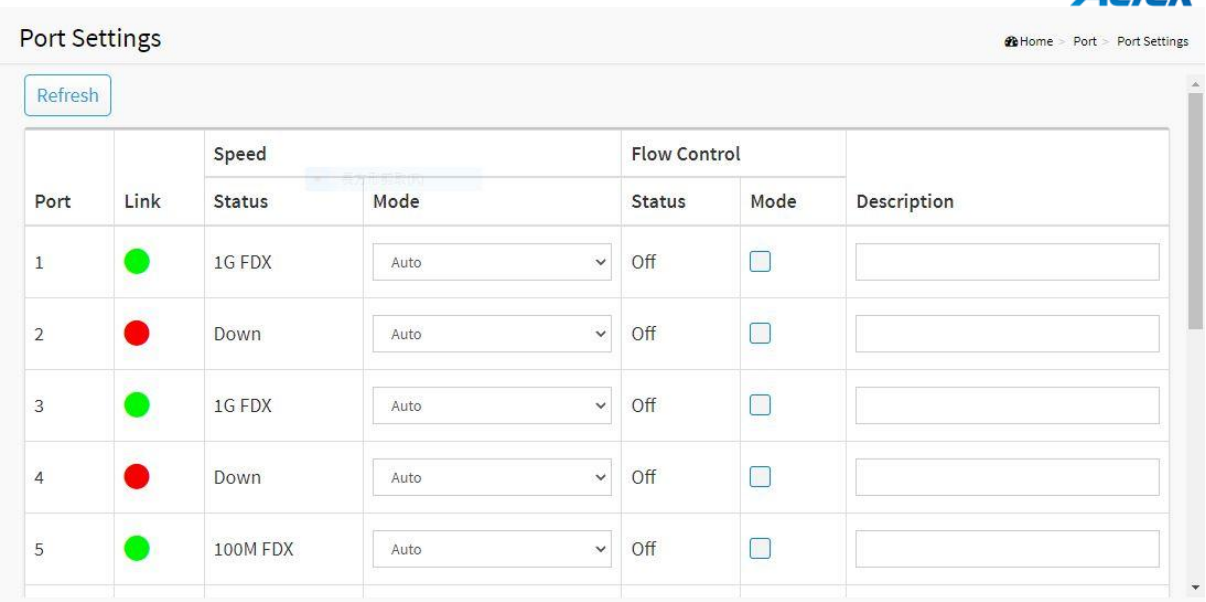


Figure 4-1: Port Setting

4-2 Link Aggregation

4-2-1 Configuration

This page is used to configure port's LACP.

Web Interface

To configure a Current Port's LACP in the web interface:

1. Click Port -> Link Aggregation
2. Specify Link Aggregation Group and the port's LACP method you want to configure. (For example: Port 9)
3. Click Apply.

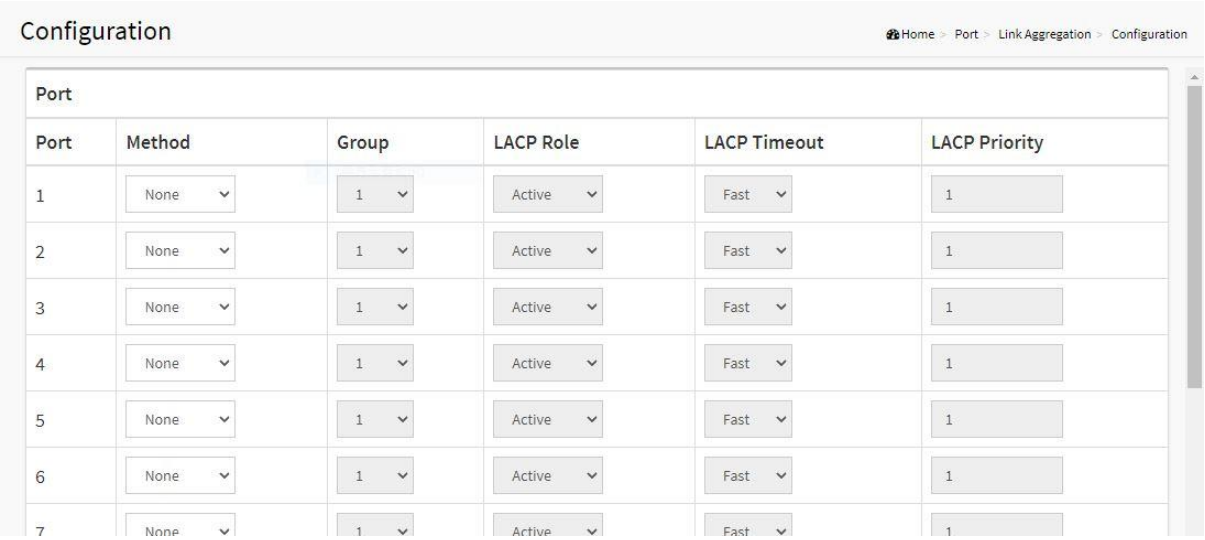


Figure 4-2-1: Link Aggregation

Parameter Description:

- **Method**

  Current port's LACP method.(None/LACP/Static)

4-2-2 Aggregation View

This page is used to show the current port trunking information from the aggregator perspective.

Web Interface

To view the Link Aggregation information in the web interface:

1. Click Port -> Link aggregation -> Link Aggregation View.

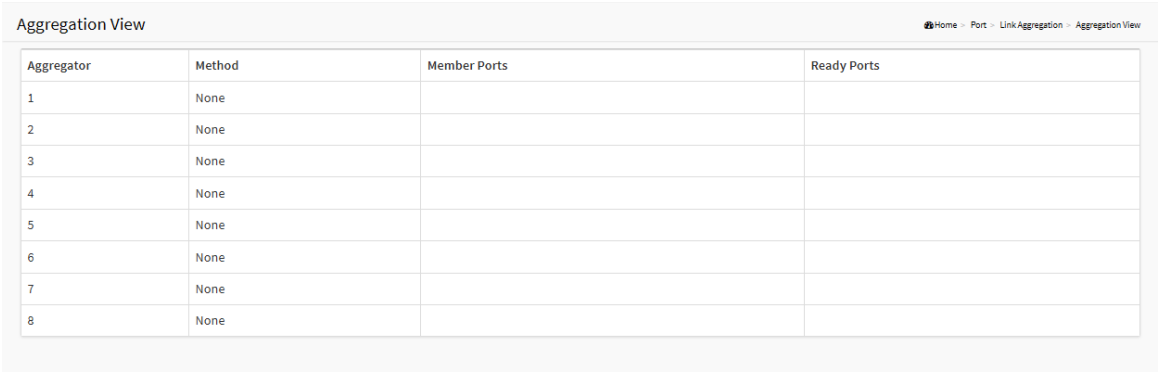


Figure 4-2-2: Link Aggregation View

Parameter Description:

- **Aggregator**

  The aggregator ID for each port; each port acts as its own aggregator, using its port number as the ID.

- **Method**

  The link aggregation method used by the port.

- **Member Ports**

  All ports that are members of the aggregator.

- **Ready Ports**

  Member ports in a ready/operational state within the aggregator.

4-2-3 LACP System Priority

This page is used to configure the LACP System Priority (1–65535; default 32768), the 16-bit field that—together with the switch's MAC address—forms the 64-bit LACP System ID. The System ID identifies the LACP system so ports aggregate only with a single peer system.

Web Interface

To set the System Priority in the web interface:

1. Click Port -> Link aggregation -> LACP System Priority.
2. Specify the parameters you want to configure.
3. Click Apply.

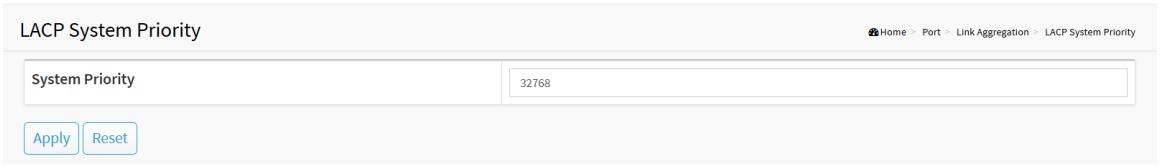


Figure 4-2-3: Link Aggregation Configuration

Parameter Description:

- **System Priority**

  The LACP system priority value.

4-3 EEE(Energy Efficient Ethernet)

This page is used to set current ports' energy configuration.

Web Interface

To configure a Current Port EEE Configuration in the web interface:

1. Click Port -> EEE.
2. Specify the parameters you want to configure.
3. Click Apply.

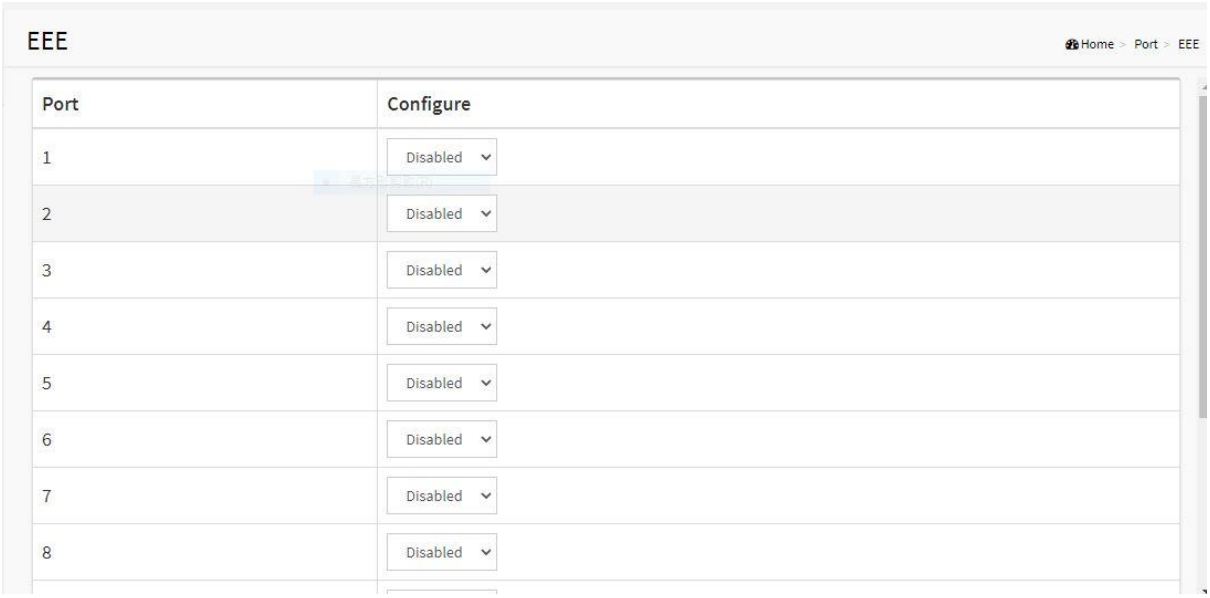


Figure 4-3: Link Aggregation

Parameter Description:

- **Configure**

  To enable/disable EEE function

4-4 Jumbo Frame

This page is used to set jumbo frame function.

Web Interface

To configure jumbo frame function in the web interface:

1. Click Port -> Jumbo Frame.
2. Specify the parameters you want to configure.
3. Click Apply.

Figure 4-4: Jumbo Frame

Parameter Description:

- To enable/disable jumbo frame function.

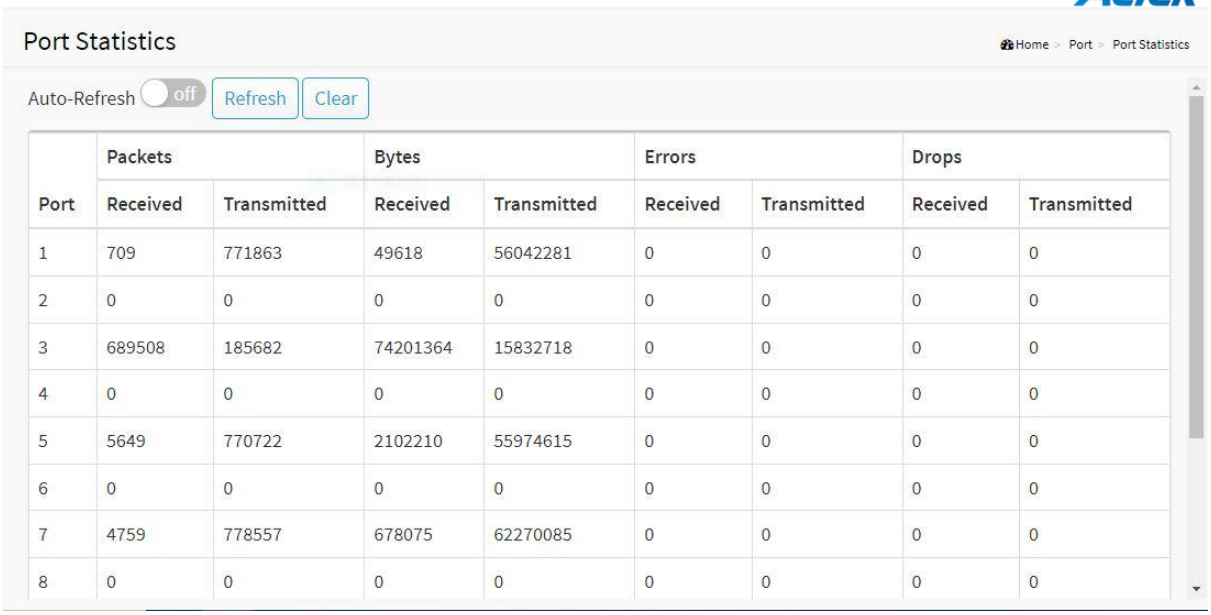
4-5 Port Statistics

The Port Statistics page displays port summary and status information. This page displays standard counters on network traffic from the Interfaces. The port counters would be display in four groups individually.

Web Interface

To display Port Statistics in the web interface:

1. Click Port -> Port Statistics.
2. Check Packets, Bytes , Error and Drops individually to view each port's statistics information.
3. Click "Clear" button will clear counter of current selected port.



Port	Packets		Bytes		Errors		Drops	
	Received	Transmitted	Received	Transmitted	Received	Transmitted	Received	Transmitted
1	709	771863	49618	56042281	0	0	0	0
2	0	0	0	0	0	0	0	0
3	689508	185682	74201364	15832718	0	0	0	0
4	0	0	0	0	0	0	0	0
5	5649	770722	2102210	55974615	0	0	0	0
6	0	0	0	0	0	0	0	0
7	4759	778557	678075	62270085	0	0	0	0
8	0	0	0	0	0	0	0	0

Figure 4-5: Port Statistics

Parameter Description:

- **Refresh[Button]**
  To refresh selected port information.
- **Clear[Button]**

  To clear counter of current selected port.

4-6 SFP Port Information

The section describes that switch could display the SFP module detail information which you connect it to the switch. The information includes: Connector type, Fiber type, wavelength, bit rate and Vendor OUI etc.

Web Interface

To display Port Statistics in the web interface:

1. Click Port -> SFP Port Information

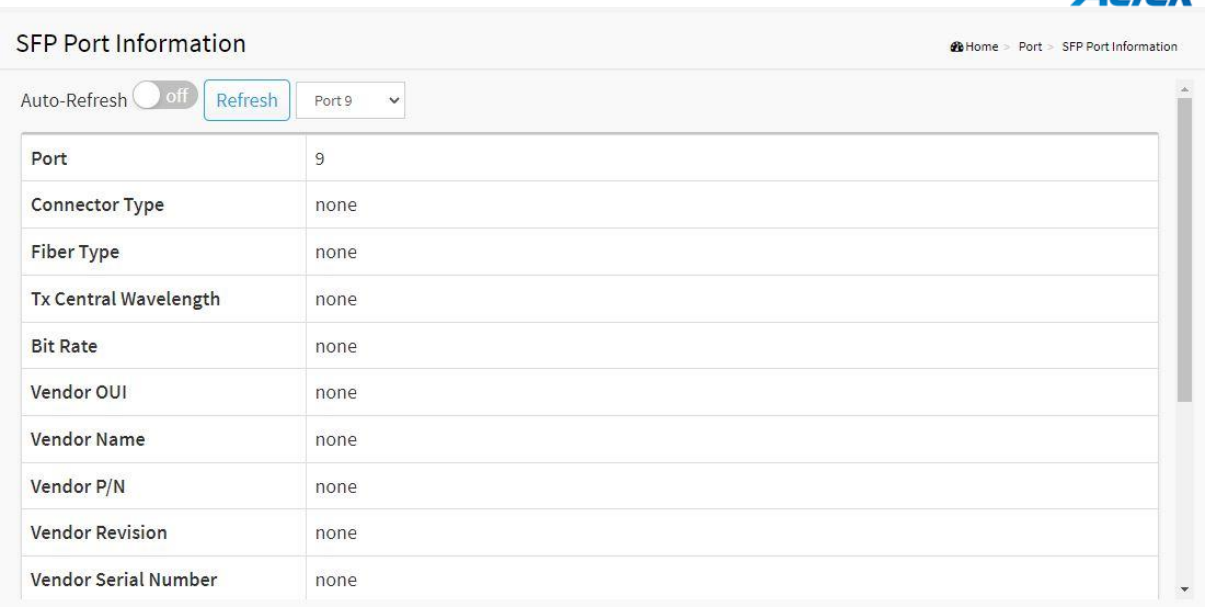


Figure 4-6: SFP Port Information

Parameter Description:

- **Refresh[Button]**
  To refresh selected port information.

Chapter 5 VLAN

A virtual local area network, virtual LAN or VLAN, is a group of hosts with a common set of requirements that communicate as if they were attached to the same broadcast domain, regardless of their physical location. A VLAN has the same attributes as a physical local area network (LAN), but it allows for end stations to be grouped together even if they are not located on the same network switch. VLAN membership can be configured through software instead of physically relocating devices or connections.

5-1 VLAN Configuration

To create new VLANs for management purpose. The management VLAN is used to establish an IP connection to the switch from a workstation connected to a port in the VLAN. By default, the active management VLAN is VLAN 1, but you can designate any VLAN as the management VLAN and 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 create new VLANs the web interface:

1. Click VLAN -> VLAN configuration
2. Input new VLANs.
3. Click Apply.

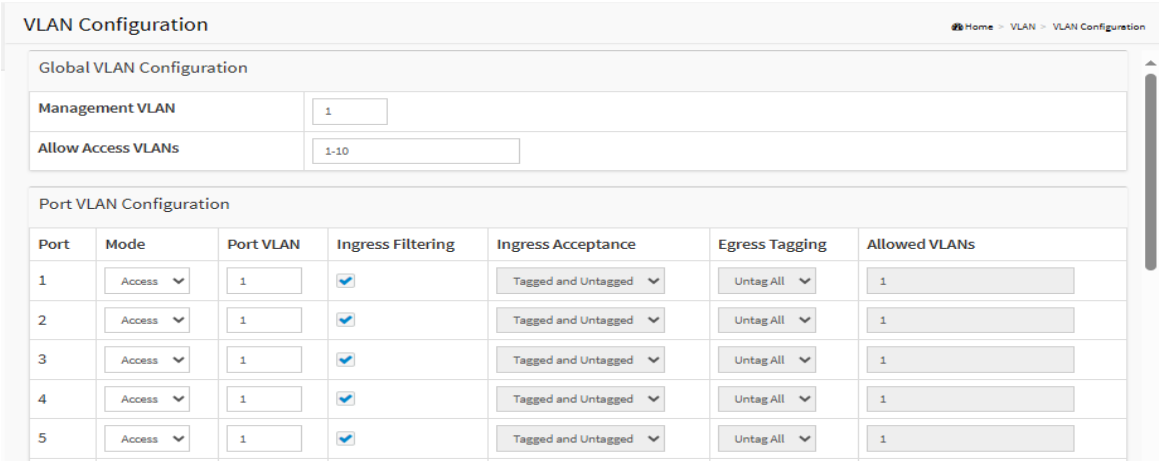


Figure 5-1: VLAN Configuration

Parameter Description:

- **Management VLAN**

  To specify the VLAN ID used for management access.

- **Allow Access VLANs**

  The VLANs list you want to create. Enter the final VLAN list you want.

  e.g. 1 or 1,4,9,11 which means your system has VLAN 1,4,9,11.

5-2 VLAN Membership

This page provides an overview of membership status of VLANs. Users can set ports as untagged or tagged member of VLAN.

Web Interface

To configure VLAN membership configuration in the web interface:

1. Click VLAN -> VLAN Membership.
2. To see the VLAN member for the port(s).
3. Click Apply.

Figure 5-2: VLAN Member

Parameter Description:

- **VLAN ID**

  The VLAN ID list(s).

- **Port Members**

  The port status with VLAN setting.

5-3 Mac-based VLAN

This page provides an overview of MAC-based VLAN membership. Users map source MAC addresses to VLAN IDs so untagged frames are placed into the correct VLAN regardless of the access port (often used with 802.1X).

Web Interface

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

1. Click VLAN -> MAC-based VLAN -> Configuration.
2. Click “Add New Entry”.
3. Specify the parameters which you want to configure.

4. Click Apply.

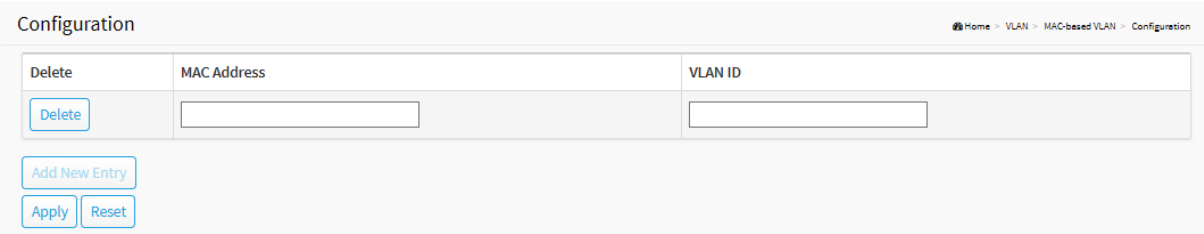


Figure 5-3: MAC-based VLAN Configuration

Parameter Description:

- **Delete**

  To delete the entry.

- **MAC Address**

  The MAC Address associated with VLAN ID.

- **VLAN ID**

  The VLAN ID.

5-4 Protocol-based VLAN

5-4-1 Protocol to Group

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

Web Interface

To configure Protocol to Group configuration in the web interface:

1. Click VLAN -> Protocol-based VLAN -> Protocol to Group.
2. Click “Add New Entry”.
3. Specify the parameters which you want to configure.
4. Click Apply.

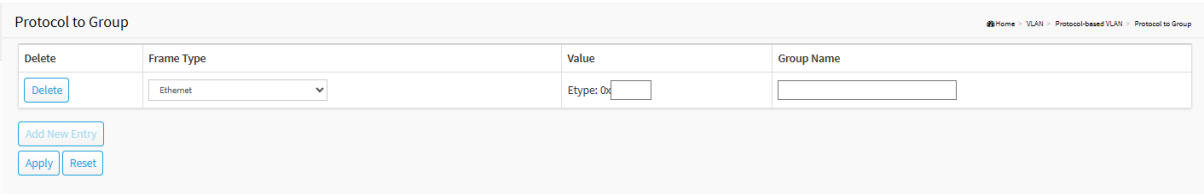


Figure 5-4-1: Protocol to Group VLAN configuration

Parameter Description:

- **Delete**

  To delete a Group Name to VLAN map entry.

- **Frame Type**

  - Ethernet

- LLC

- SNAP

- **Value**

  Frame type value.

- **Group Name**

  A valid Group Name is a unique 16-character long string.

5-4-2 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 configure Group to VLAN configuration in the web interface:

1. Click VLAN -> Protocol-based VLAN -> Group to VLAN.
2. Click "Add New Entry".
3. Specify the parameters which you want to configure.
4. Click Apply.

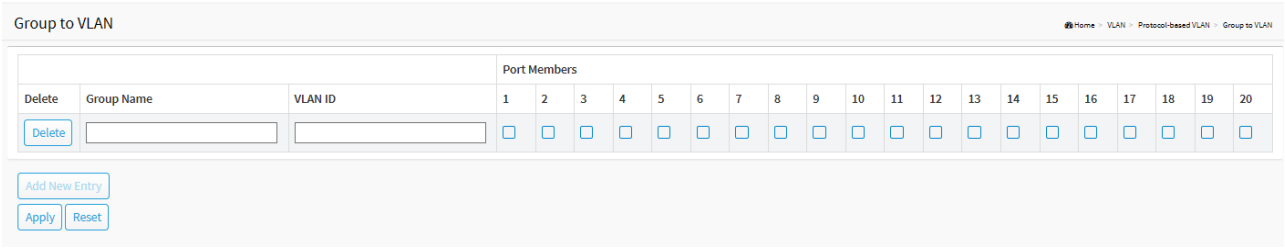


Figure 5-4-2: Group to VLAN configuration

Parameter Description:

- **Delete**

  To delete a Group Name to VLAN map entry.

- **Group Name**

  A valid Group Name is a string of almost 16 characters.

- **VLAN ID**

  Indicates the ID to which Group Name will be mapped. A valid VLAN ID ranges from 1 to 4094.

- **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.

5-5 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.

Web Interface

To configure IP Subnet-based VLAN in the web interface:

1. Click VLAN -> IP Subnet-based VLAN.
2. Click “Add New Entry”.
3. Specify the parameters which you want to configure.
4. Click Apply.

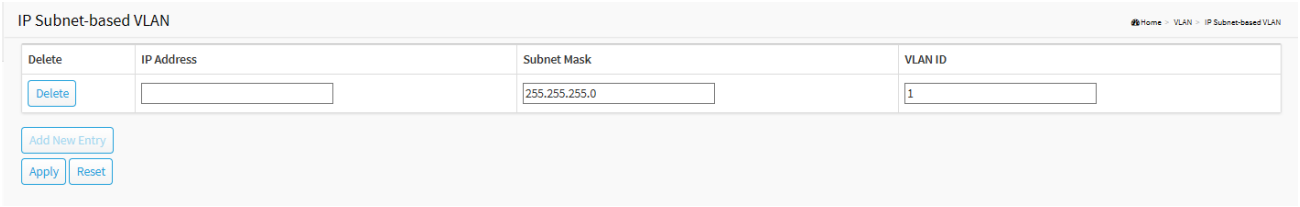


Figure 5-5: IP Subnet-based VLAN configuration

Parameter Description:

- **IP Address**

  Indicates the IP address.

- **Subnet Mask**

  Indicates the network subnet mask.

- **VLAN ID**

  Indicates the VLAN ID.

5-6 Voice VLAN

5-6-1 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.

Web Interface

To configure Voice VLAN in the web interface:

1. Click VLAN -> Voice VLAN -> Configuration.
2. Click “Add New Entry”.
3. Specify the parameters which you want to configure.
4. Click Apply.

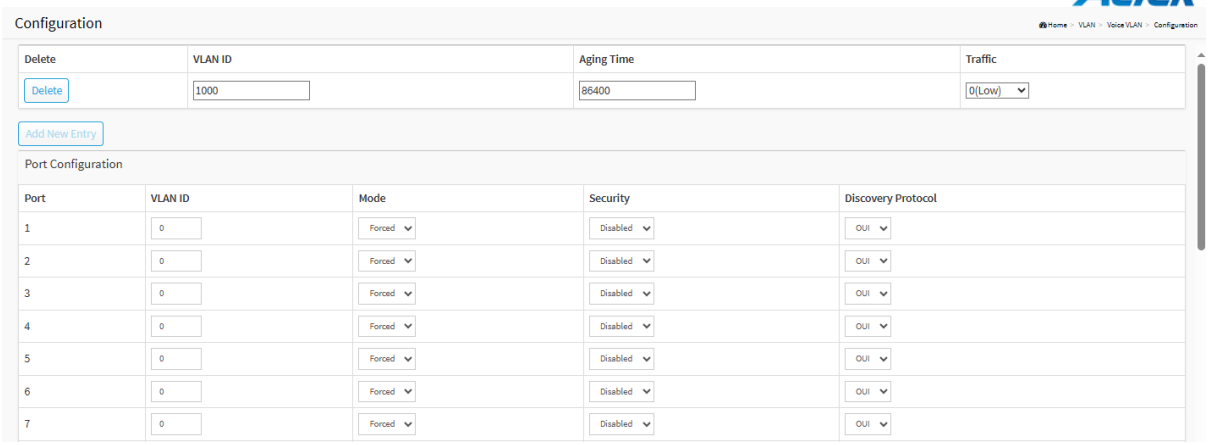


Figure 5-6-1: Voice VLAN Configuration

Parameter Description:

- **VLAN ID**

  The VLAN ID.

- **Aging Time**

  Indicates the Voice VLAN secure learning aging time. The allowed range is 10 to 10000000 seconds.

- **Traffic**

  Indicates the Voice VLAN traffic class. All traffic on the Voice VLAN will apply this class.

- **Mode**

  Indicates the Voice VLAN port mode.

- **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.

- **Discovery Protocol**

  Indicates the Voice VLAN port discovery protocol. It will only work when auto detect mode is enabled.

5-6-2 OUI

This page provides an overview of membership status of VLANs. Users can set ports as untagged or tagged member of VLAN.

Web Interface

To configure VLAN membership configuration in the web interface:

1. Click VLAN -> VLAN Membership.
2. To see the VLAN member for the port(s).
3. Click Apply.

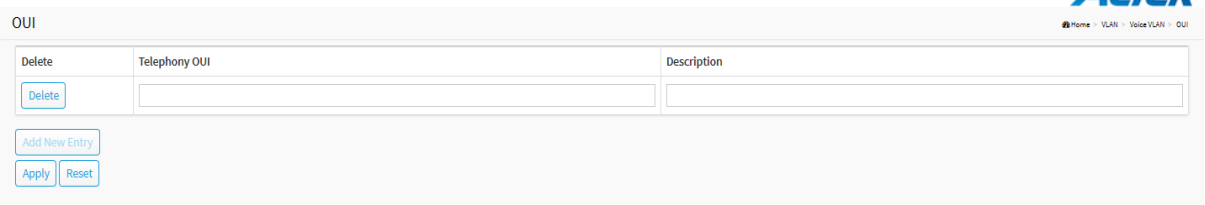


Figure 5-6-2: OUI Configuration

Parameter Description:

- **Telephony OUI**

  A telephony OUI address is a globally unique identifier assigned to a vendor by IEEE. It must be 6 characters long and the input format is "xx:xx:xx" (x is a hexadecimal digit).

- **Description**

  The description of OUI address. Normally, it describes which vendor telephony device it belongs to. The allowed string length is 0 to 32.

Chapter 6 IGMP Snooping

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

A switch supported IGMP Snooping with the functions of query, report and leave, a type of packet exchanged between IP Multicast Router/Switch and IP Multicast Host, can update the information of the Multicast table when a member (port) joins or leaves an IP Multicast Destination Address. With this function, once a switch receives an IP multicast packet, it will forward the packet to the members who joined in a specified IP multicast group before.

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

6-1 Property

This page sets the property of IGMP Snooping, including State, Immediate Leave and Unknown Multicast.

Web Interface

To configure the property of IGMP Snooping in the web interface:

1. Click IGMP Snooping -> Property.
2. Specify the parameters which you want to configure.
3. Click Apply.

Figure 6-1: Property

Parameter Description:

- **State**

  To enable/disable IGMP Snooping function.(IGMP v2 / IGMP v3)

- **Immediate Leave**

  If set enabled, the multicast traffic would be stopped as soon as an IGMP leave message received on a port

- **Unknown Multicast**

  If set blocked, the unknown multicast received would be dropped; Otherwise, the packets would be flooded

6-2 VLAN Configuration

The section describes the VLAN configuration setting process integrated with IGMP Snooping function.

Web Interface

To set the VLAN configuration in the web interface:

1. Click IGMP Snooping -> VLAN Configuration.
2. Specify the parameters which you want to configure.
3. Click Apply.

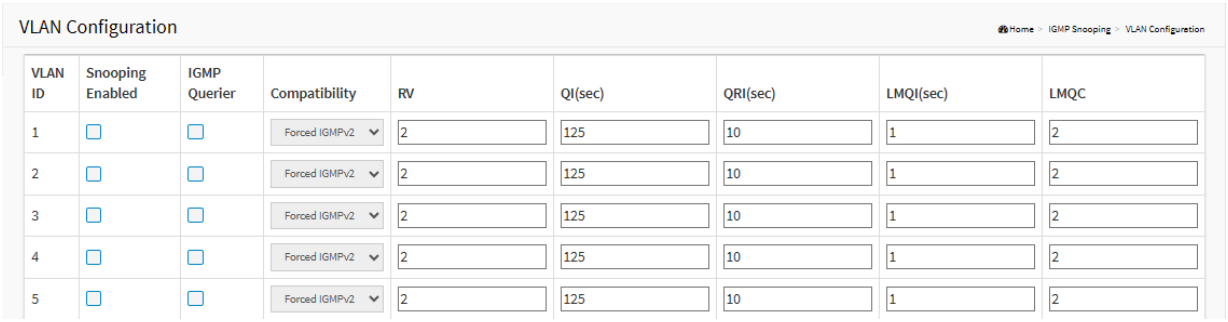


Figure 6-2: VLAN Configuration

Parameter Description:

- **Snooping Enabled**

  Enable the per-VLAN IGMP Snooping.

- **IGMP Querier**

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

- **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 Forced IGMPv2, Forced IGMPv3, default compatibility value is Forced IGMPv2.

- **RV**

  Robustness Variable. The Robustness Variable allows tuning for the expected packet loss on a network. The allowed range is 1 to 7; 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 30 to 18000 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 5 to 20 in seconds; default query response interval is 10 seconds.

- **LMQI**

  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 1 to 25 in seconds; default last member query interval is 1 second.

- **LMQC**

  Last Member Query Count. The Last Member Query Count is the time value represented by the Last Member Query Interval, multiplied by the Last Member Query Count. The allowed range is 1 to 7 in seconds; default last member query interval is 1 second.

6-3 Group Address

This page displays the group address for all port members.

Web Interface

To view the group address in the web interface:

1. Click IGMP Snooping -> Group Address.
2. Click "Clear" to delete the entries.
3. Click "Refresh" to reload the entries.

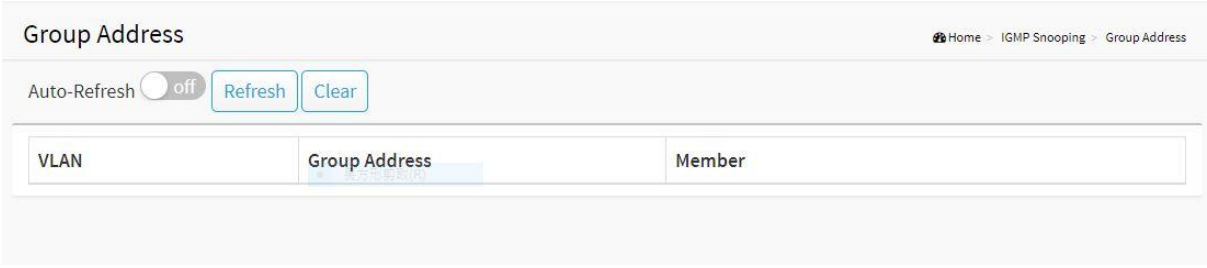


Figure 6-3: Group Address

Parameter Description:

- **VLAN**

  VLAN.

- **Group Address**

  Group Address of IGMP Snooping.

- **Member**

  IGMP Snooping Members.

- **Clear[Button]**

  To delete the entries.

- **Refresh[Button]**

  To reload the entries.

Chapter 7 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.

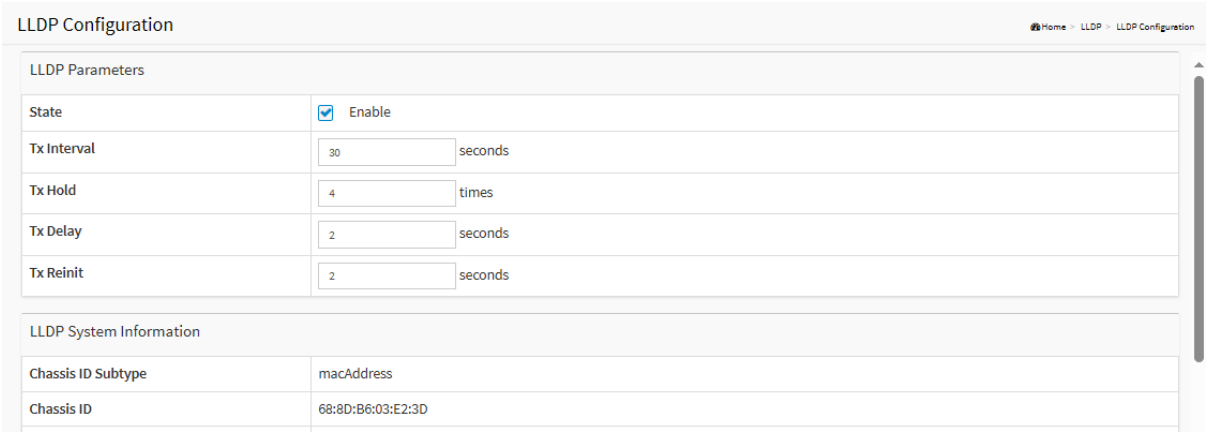
7-1 LLDP Configuration

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

Web Interface

To configure the LLDP settings in the web interface:

1. Click LLDP -> LLDP Configuration.
2. Specify LLDP parameters you want to configure.
3. Click Apply.



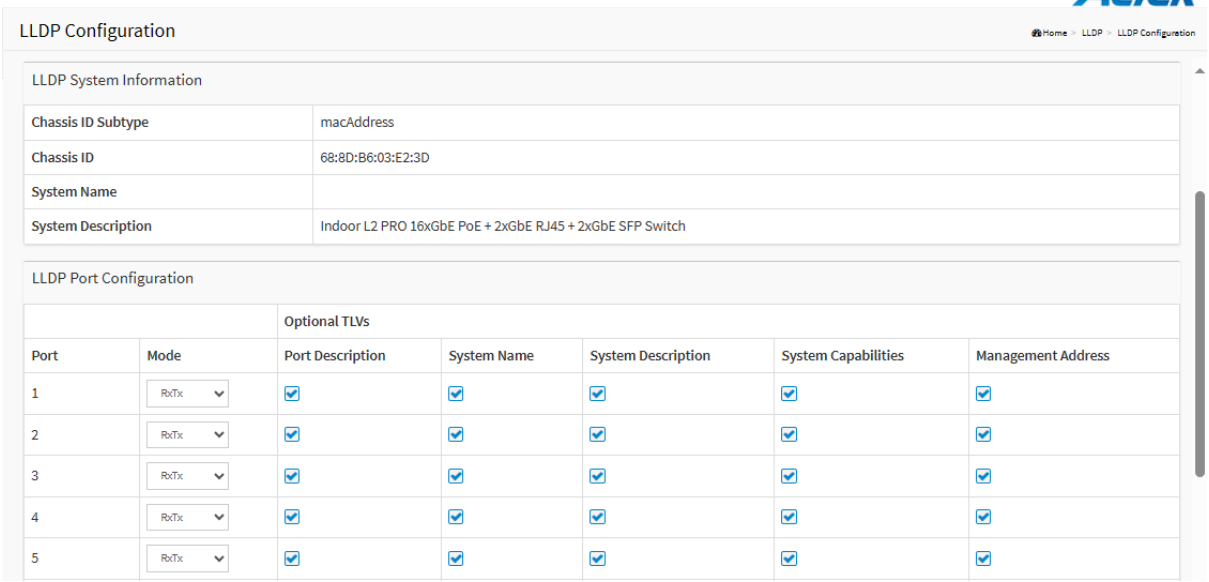


Figure 7-1: LLDP Configuration

Parameter Description:

- **State**

  To enable/disable LLDP function.

- **TX Hold**

  Specify the LLDP packet hold time interval as a multiple of the LLDP timer value. The range is 2 to 10, and the default value is 4.

- **TX Interval**

  Specify how often the software sends LLDP updates in seconds. The range is 5 to 32768 seconds. The default value is 30 seconds.

- **TX Reinit**

  Specify the minimum time in seconds an LLDP port waits before reinitializing LLDP transmission. The range is from 1 to 10 and the default value is 2 seconds.

- **TX Delay**

  Specify the delay in seconds between successive LLDP frame transmissions initiated by value or status changes in the LLDP local systems MIB. The range is from 1 up to 8192 seconds and the default transmission delay is 2 seconds.

- **Chassis ID Subtype**

  Type of chassis ID (for example, MAC address).

- **Chassis ID**

  Identifier of the chassis. Where the chassis ID subtype is a MAC address, the MAC address of the device is displayed.

- **System Name**

  The Name of the device.

- **System Description**

  The Description of the device.

- **Mode**

  Select the LLDP State for the ports.

- **Optional TLVs:**

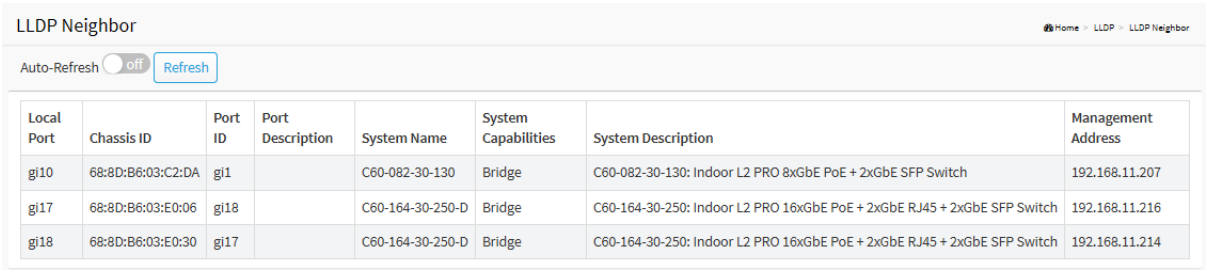
  Select which optional TLVs to include in LLDP information—Port Description, System Name, System Description, System Capabilities, and Management Address; checked items are included.

7-2 LLDP Neighbor

This page is to display LLDP neighborhood status.

Web Interface

To display the LLDP neighborhood status in the web interface, click LLDP -> LLDP Neighbor.



Local Port	Chassis ID	Port ID	Port Description	System Name	System Capabilities	System Description	Management Address
gi10	68:8D:B6:03:C2:DA	gi1		C60-082-30-130	Bridge	C60-082-30-130: Indoor L2 PRO 8xGbE PoE + 2xGbE SFP Switch	192.168.11.207
gi17	68:8D:B6:03:E0:06	gi18		C60-164-30-250-D	Bridge	C60-164-30-250: Indoor L2 PRO 16xGbE PoE + 2xGbE RJ45 + 2xGbE SFP Switch	192.168.11.216
gi18	68:8D:B6:03:E0:30	gi17		C60-164-30-250-D	Bridge	C60-164-30-250: Indoor L2 PRO 16xGbE PoE + 2xGbE RJ45 + 2xGbE SFP Switch	192.168.11.214

Figure 7-2: LLDP Information

Parameter Description:

- **Local Port**

  The normal port of the device.

- **Chassis ID**

  Identifier of the chassis. Where the chassis ID subtype is a MAC address, the MAC address of the device is displayed.

- **Port ID**

  Port identifier.

- **Port Description**

  Displays the LLDP port description advertised by the neighbor device.

- **System Name**

  The Name of the device.

- **System Capabilities**

  Identifies the switch's primary capabilities (bridge, router).

- **System Description**

  The Description of the device.

- **Management Address**

  Specify the management address to be used in LLDP Management Address type, length, and value (TLV) messages. The Management Address TLV typically contains the IPv4 or IPv6 management addresses of the local system. Only out-of-band management addresses must be used for the management-address. Other remote managers can use this address to obtain information related to the local device.

Chapter 8 Loop Prevention

The chapter describes how to prevent loop situation.

8-1 Property

This page is used to configure the loop prevention.

Web Interface

To configure the loop prevention in the web interface:

1. Click Loop Prevention -> Property.
2. Specify the parameter you want to configure.
3. Click Apply.

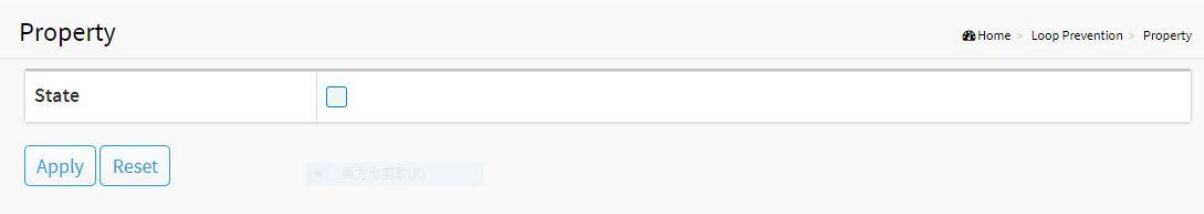


Figure 8-1: Property

Parameter description:

- **State**
  To enable/disable loop prevention function.

8-2 Status

This page is used to display the loop status of ports.

Web Interface

To view the loop status in the web interface, click Loop Prevention -> Status.

Figure 8-2: Status

Chapter 9 Security

This section shows you to configure the Port Security settings of the Switch. You can use the Port Security feature to restrict input to an interface by limiting and identifying MAC addresses.

9-1 Account / Password

This page provides an overview of the current users. Use this page to modify the user name and password.

Web Interface

To configure the Account / Password for multiple user in the web interface:

1. Click Security -> Account / Password.
2. In the Ilde Timeout part, specify the timeout time parameter you want to configure.
3. Click Apply.
4. Click "Add New User".
5. Specify the user name , password and privilege level you want to configure.
6. Click Apply.

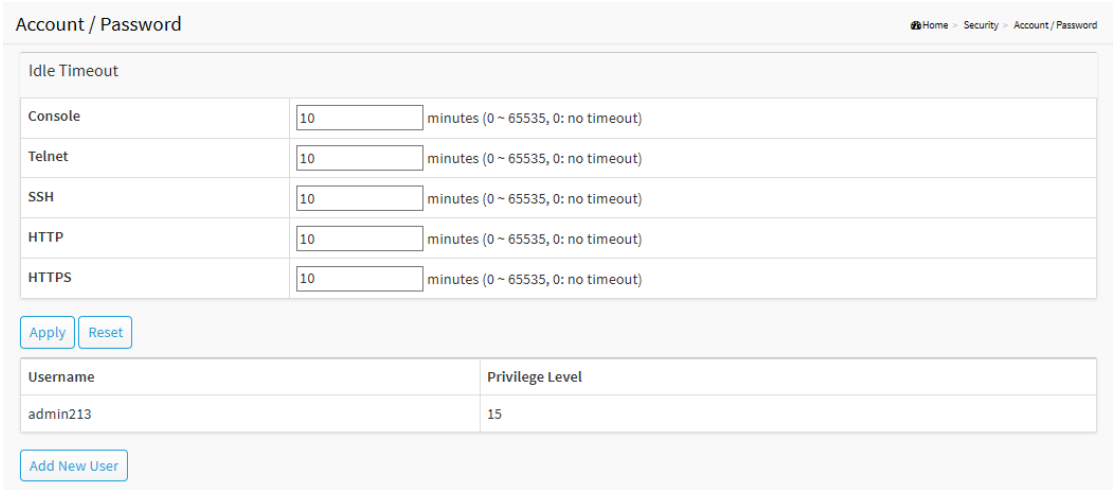


Figure 9-1: Account / Password

Parameter Description:

- **Idle Timeout**

Login idle timeout settings. There are 5 types of login:

- Console
- Telnet
- SSH
- HTTP

- HTTPS.

The range is from 0 to 65535.(0: no timeout) The unit is in minute(s).

- **User Name**

  A string identifying the user name that this entry should belong to. The allowed string length is 1 to 32. The valid user name allows letters, numbers and underscores.

- **Password**

  The password of the user. The allowed string length is 1 to 32 characters. Any printable characters except space is accepted.

- **Privilege Level**

  The privilege level of the user. The allowed range is 0 to 15.

9-2 Privilege Levels

This page provides an overview of the privilege levels.

Web Interface

To configure the Privilege Level function the web interface:

1. Click Security -> Privilege Level.
2. Specify the connection parameter you want to configure.
3. Click Apply.

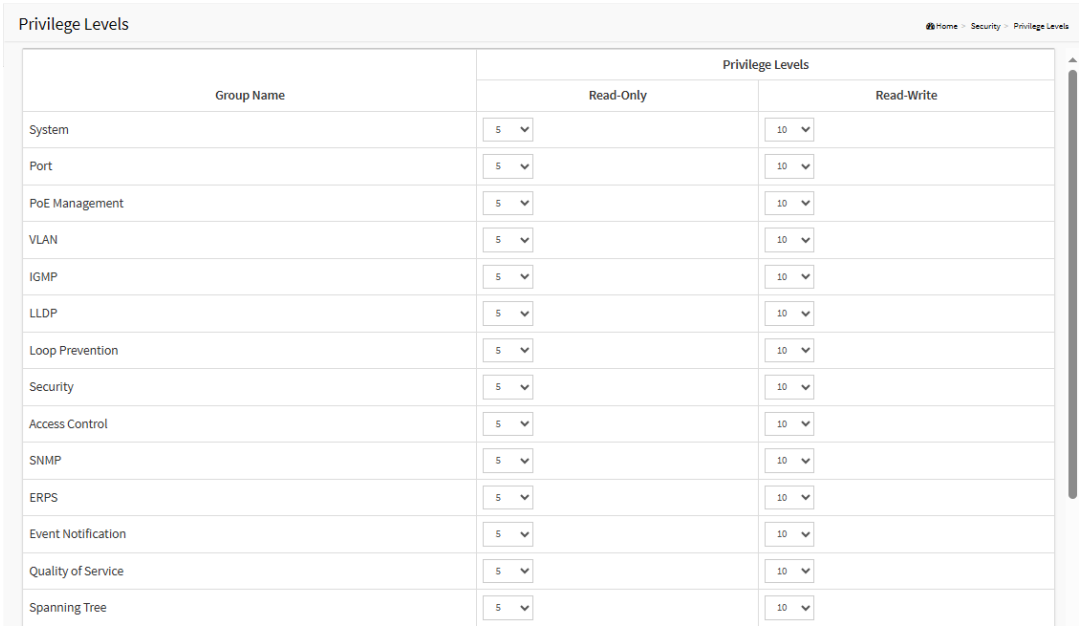


Figure 9-2: Privilege Level

Parameter Description:

- **Group Name**

  The name identifying the privilege group.

■ **Privilege Levels**

Read-Only / Read-Write.

9-3 Auth Method

This page is used to configure the Authentication Method, Command Authorization Method and Accounting Method.

Web Interface

To configure the Auth Method the web interface:

1. Click Security -> Auth Method.
2. Specify the connection parameter you want to configure.
3. Click Apply.

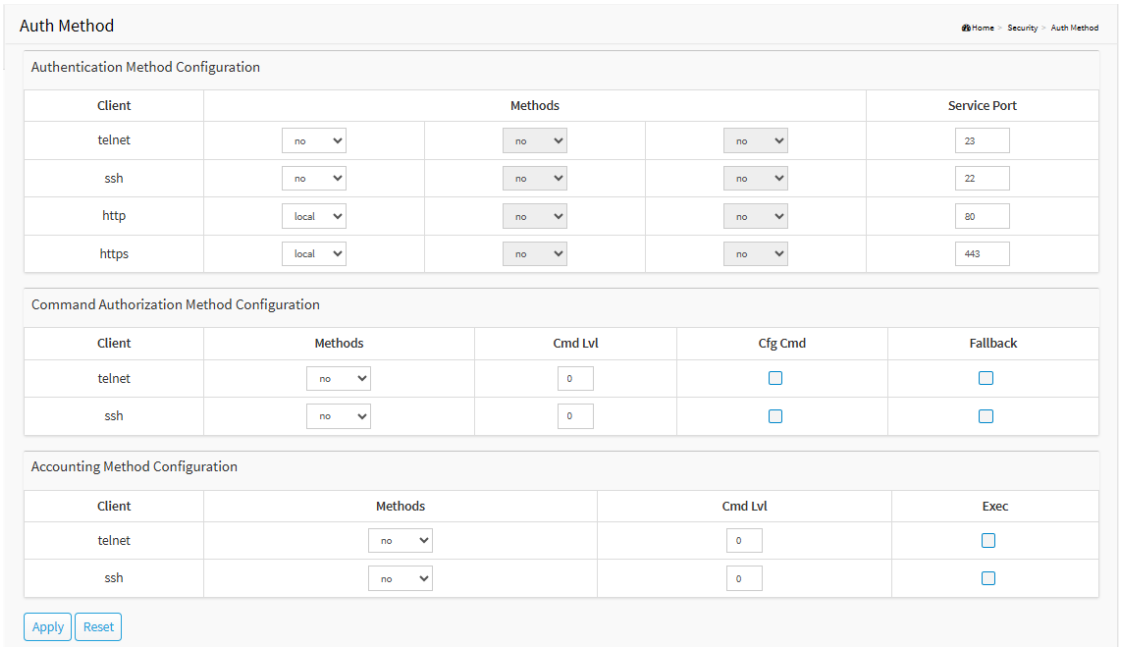


Figure 9-3: Auth Method

Parameter Description:

■ **Client**

The management client for which the configuration applies.

■ **Method**

Authentication Method can be set to one of the following values:

- no : authentication is disabled and login is not possible.
- local : use the local user database on the switch for authentication.
- radius : use a remote RADIUS server for authentication.
- tacacs : use a remote TACACS server for authentication.

- **Service Port**

  The TCP port for each client service. The valid port number is 1 ~ 65535.

- **Cmd Lvl**

  Runs authorization for all commands at the specified privilege level. Specific command level that should be authorized. Valid entries are 0 through 15.

- **Cfg Cmd**

  Enable or disable the configure command.

- **Fallback**

  The local database can act as a fallback method for several functions. This behavior is designed to help you prevent accidental lockout from the security appliance.

- **Exec**

  Runs accounting to determine if the user is allowed to run an EXEC shell. This facility might return user profile information such as auto command information.

9-4 IEEE 802.1X

9-4-1 Configuration

This page is used to configure the 802.1X function.

Web Interface

To configure the 802.1X function the web interface:

1. Click Security -> IEEE 802.1X -> Configuration.
2. Specify the connection parameter you want to configure.
3. Click Apply.

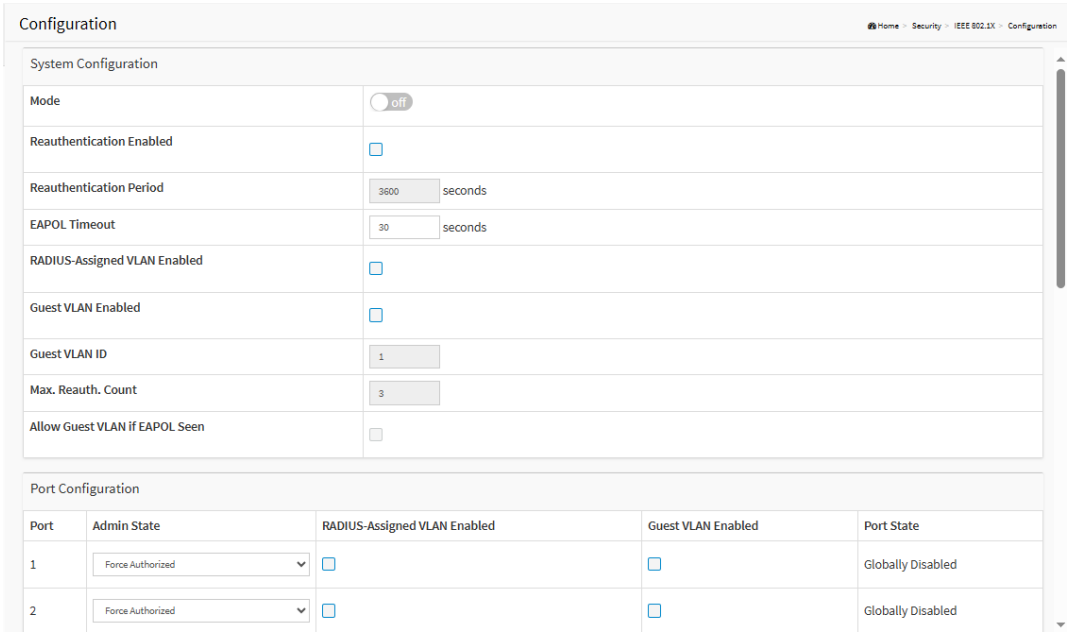


Figure 9-4-1: IEEE 802.1X - Configuration

Parameter Description:

- **Mode**

  on or off. Indicates if IEEE 802.1X is globally enabled or disabled on the switch. If globally disabled, all ports are allowed forwarding of frames.

- **Reauthentication Enabled**

  If checked, successfully authenticated supplicants/clients are reauthenticated after the interval specified by the Reauthentication Period.

- **Reauthentication Period**

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

- **EAPOL Timeout**

  Determines the time for retransmission of Request Identity EAPOL frames. Valid values are in the range 1 to 65535 seconds. This has no effect for MAC-based ports.

- **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.

- **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.

- **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 [1-4094].

- **Max. Reauth. Count**

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

- **Allow Guest VLAN if EAPOL Seen**

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

- **Port**

  The port number for which the configuration below applies.

- **Admin State**

  - Force Authorized
  - Force Unauthorized
  - Port-based 802.1X

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

■ **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.

■ **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

■ **Port State**

- Globally Disabled
- Link Down
- Authorized
- Unauthorized
- X Auth/Y Unauth

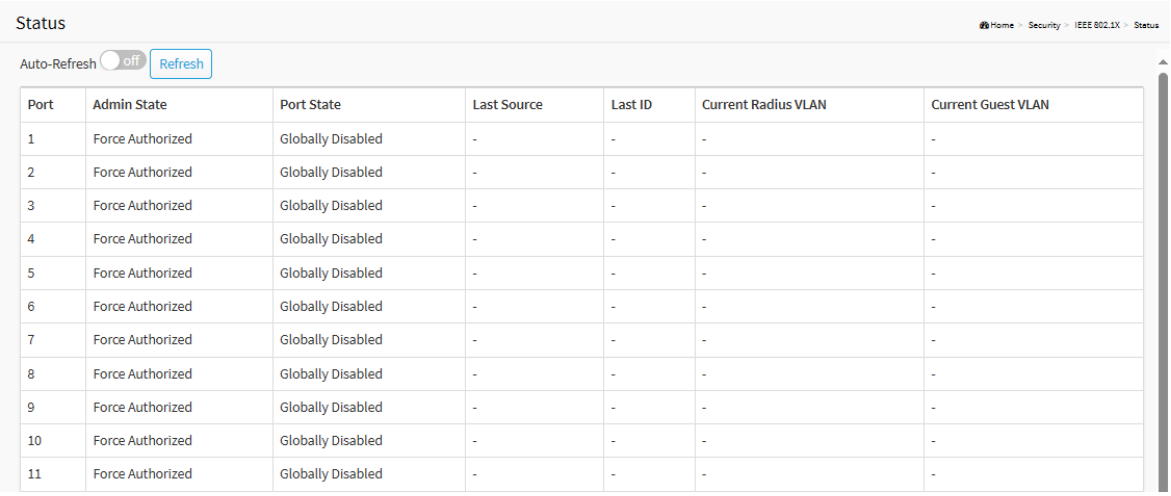
9-4-2 Status

The section describes to show the each port 802.1X status information of the switch. The status includes Admin State, Port State, Last Source, Last ID, Current Radius VLAN and Current Guest VLAN.

Web Interface

To view the IEEE 802.1X configuration the web interface:

1. Click Security -> IEEE 802.1X -> Status.



Port	Admin State	Port State	Last Source	Last ID	Current Radius VLAN	Current Guest VLAN
1	Force Authorized	Globally Disabled	-	-	-	-
2	Force Authorized	Globally Disabled	-	-	-	-
3	Force Authorized	Globally Disabled	-	-	-	-
4	Force Authorized	Globally Disabled	-	-	-	-
5	Force Authorized	Globally Disabled	-	-	-	-
6	Force Authorized	Globally Disabled	-	-	-	-
7	Force Authorized	Globally Disabled	-	-	-	-
8	Force Authorized	Globally Disabled	-	-	-	-
9	Force Authorized	Globally Disabled	-	-	-	-
10	Force Authorized	Globally Disabled	-	-	-	-
11	Force Authorized	Globally Disabled	-	-	-	-

Figure 9-4-2: IEEE 802.1X Status

Parameter Description:

- **Port**

  The switch port number.

- **Admin State**

  The port's current administrative state.

- **Port State**

  The current state of the port.

- **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.

- **Current Radius VLAN**

  Current Radius VLAN.

- **Current Guest VLAN**

  Current Guest VLAN.

9-5 RADIUS

9-5-1 Configuration

This page is used to configure the RADIUS Server.

Web Interface

To configure the RADIUS Server the web interface:

1. Click Security -> RADIUS -> Configuration.
2. Specify the connection parameter you want to configure.
3. Click Apply.

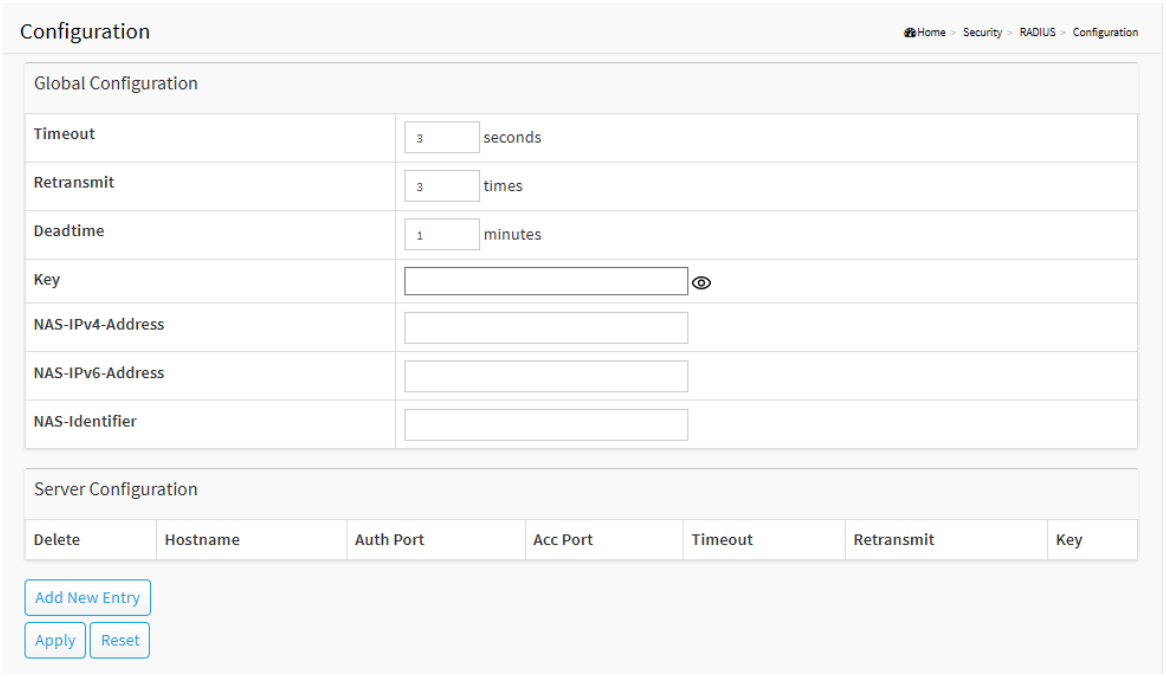


Figure 9-5-1: RADIUS Configuration

Parameter Description:

- **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.

- **Key**

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

- **NAS-IPv4-Address**

  The IPv4 address to be used as attribute 4 in RADIUS Access-Request packets.

- **NAS-IPv6-Address**

  The IPv6 address to be used as attribute 95 in RADIUS Access-Request packets.

- **NAS-Identifier**

  The identifier - up to 255 characters long - to be used as attribute 32 in RADIUS Access-Request packets.

- **Delete**

  To delete a RADIUS server entry, check this box.

- **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.

9-5-2 Status

This page is used to display RADIUS Server status.

Web Interface

To view the RADIUS Server status the web interface:

1. Click Security -> RADIUS -> Status.

Figure 9-5-2: RADIUS Status

Parameter Description:

- **IP Address**

  The IP Address for RADIUS Server.

- **Status**

RADIUS server status.

9-6 TACACS+

This page is used to configure the TACACS+ Server.

Web Interface

To configure the TACACS+ Server the web interface:

1. Click Security -> TACACS+ -> Configuration.
2. Specify the connection parameter you want to configure.
3. Click Apply.

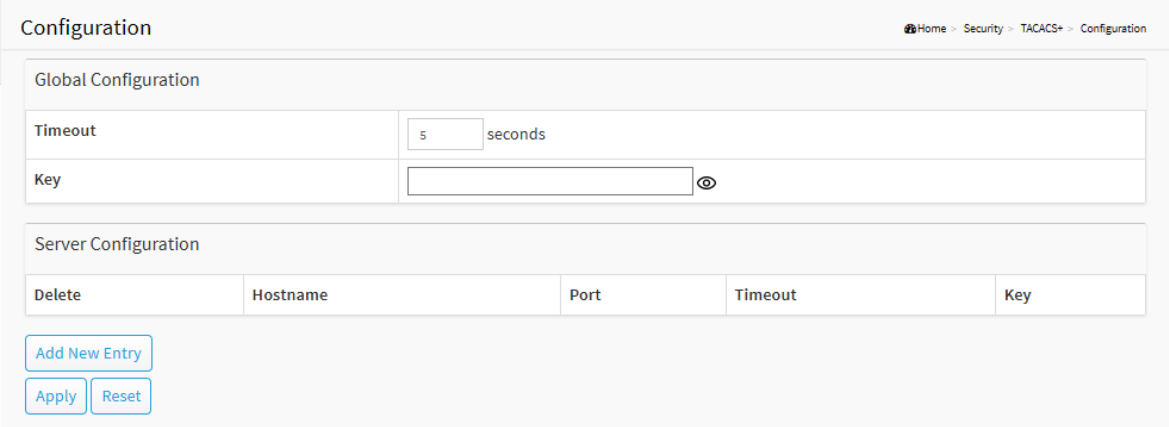


Figure 9-6: TACACS+ Configuration

Parameter Description:

- **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.

- **Key**

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

- **Delete**

  To delete a TACACS+ server entry, check this box.

- **Hostname**

  The IP address or hostname of the TACACS+ server.

- **Port**

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

- **Timeout**

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

- **Key**

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

9-7 Port Isolation

This page is used to configure the Port Isolation function.

Web Interface

To configure the port isolation in the web interface:

1. Click Security -> Port Isolation.
2. Specify the parameter you want to configure.
3. Click Apply.

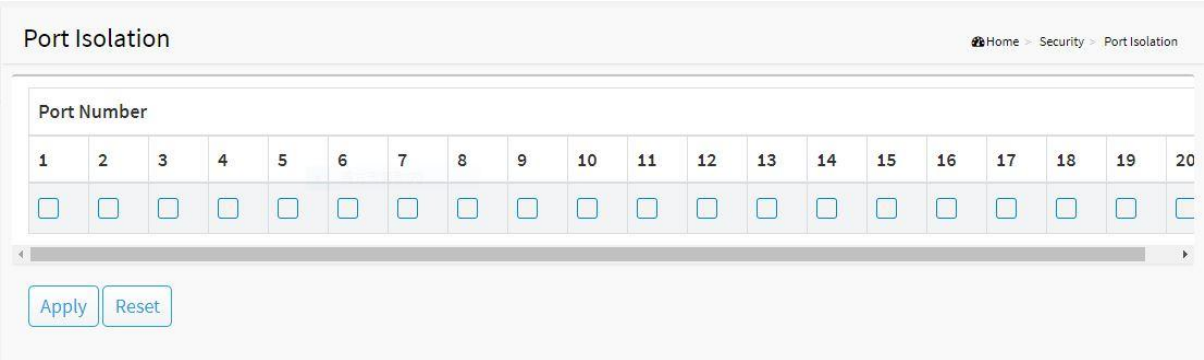


Figure 9-7: Port Isolation

Parameter Description:

- **Port Number**

  Select the port of the device to isolate.

9-8 Port Security

9-8-1 Configuration

This page is used to configure the Port Security function.

Web Interface

To configure the port security in the web interface:

1. Click Security -> Port Security.
2. Specify the parameter you want to configure.
3. Click Apply.

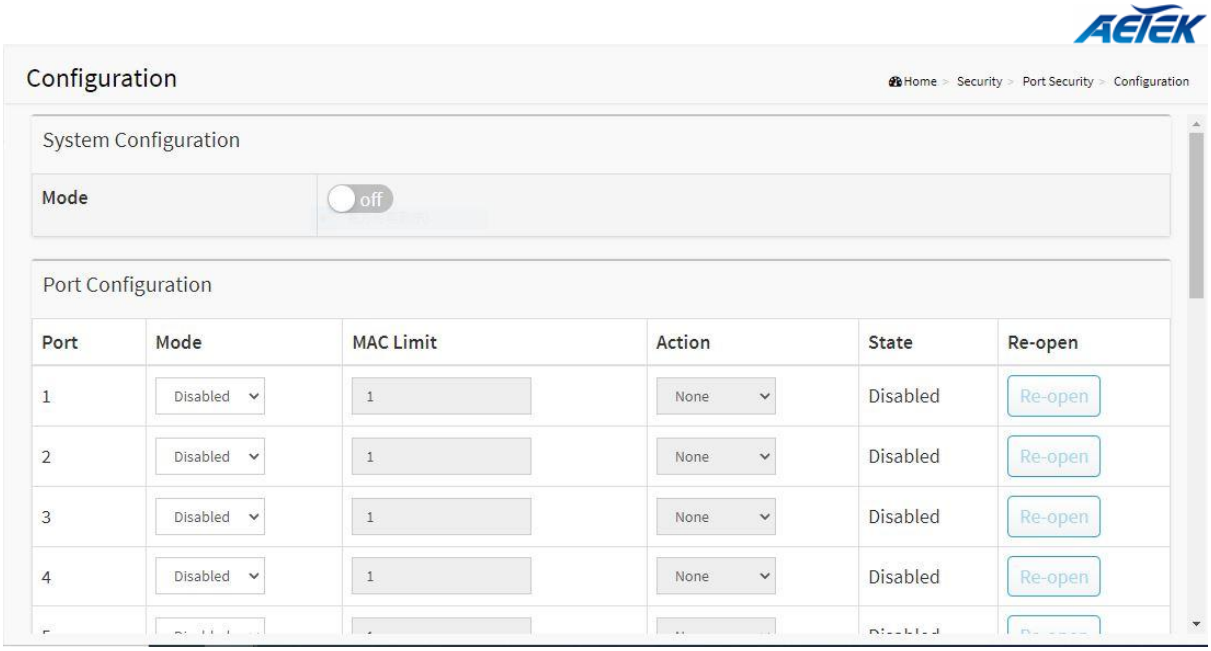


Figure 9-8-1: Port Security

Parameter Description:

- **Port**

  The normal port of the device.

- **Mode**

  The state of the function.

- **MAC Limit**

  The limit number of MAC address.

- **Action**

  The state of the port

- **State**

  The port from the Limit Control's perspective.

  - Disabled
  - Ready
  - Limit Exceeded
  - Shutdown

- **Re-open**

  If a port is shutdown by this module, you may reopen it by clicking this button, which will only be enabled if this is the case.

9-8-2 Status

This page shows the Port Security status, including a legend of user modules and per-port states.

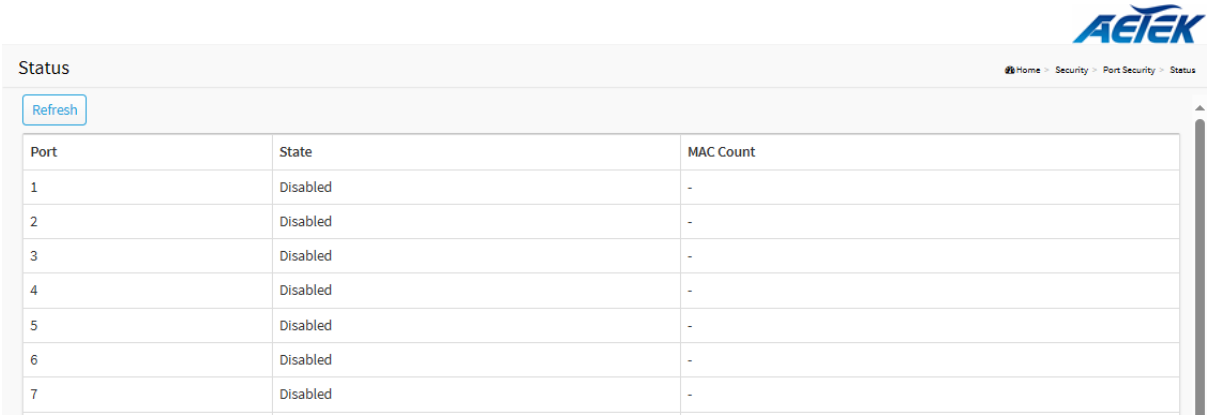


Figure 9-8-2: Port Security Status

Parameter Description:

- **State**

  Shows the port's Port Security state

- **MAC Count**

  The number of currently learned MAC addresses (forwarding and blocked) and the port's learning limit; displays "–" if no user modules are enabled.

9-9 Storm Control

This page is used to configure the storm control function. A traffic storm occurs when packets flood the LAN, creating excessive traffic and degrading network performance. The traffic broadcast and multicast suppression (or storm control) feature prevents LAN ports from being disrupted by a broadcast, multicast and unicast traffic storm on physical interfaces.

Web Interface

To configure the storm control function in the web interface:

1. Click Security -> Storm Control.
2. Specify the parameter you want to configure.
3. Click Apply.

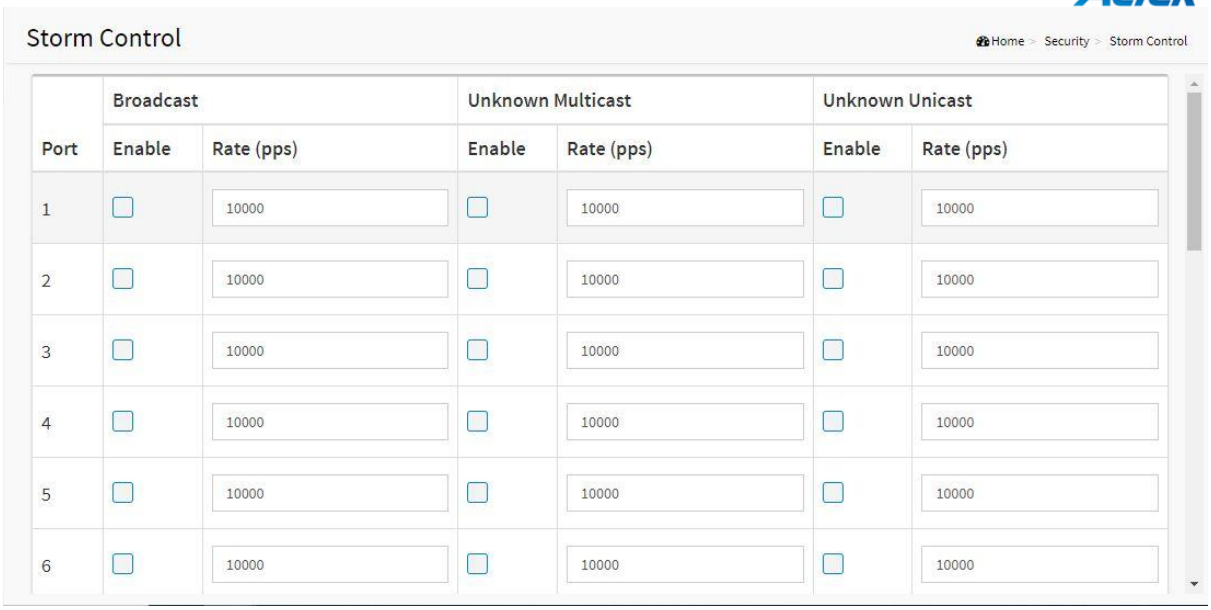


Figure 9-9: Storm Control

Parameter description:

- **Rate**

  The rate for controlling broadcast, multicast and unicast traffic storm on physical interfaces.

- **Enable**

  To enable/disable the function.

9-10 DoS Attack Prevention

This page is used to configure the DoS Attack Prevention function.

Web Interface

To configure the DoS Attack Prevention function in the web interface:

1. Click Security -> DoS Attack Prevention.
2. Specify the parameter you want to configure.
3. Click Apply.

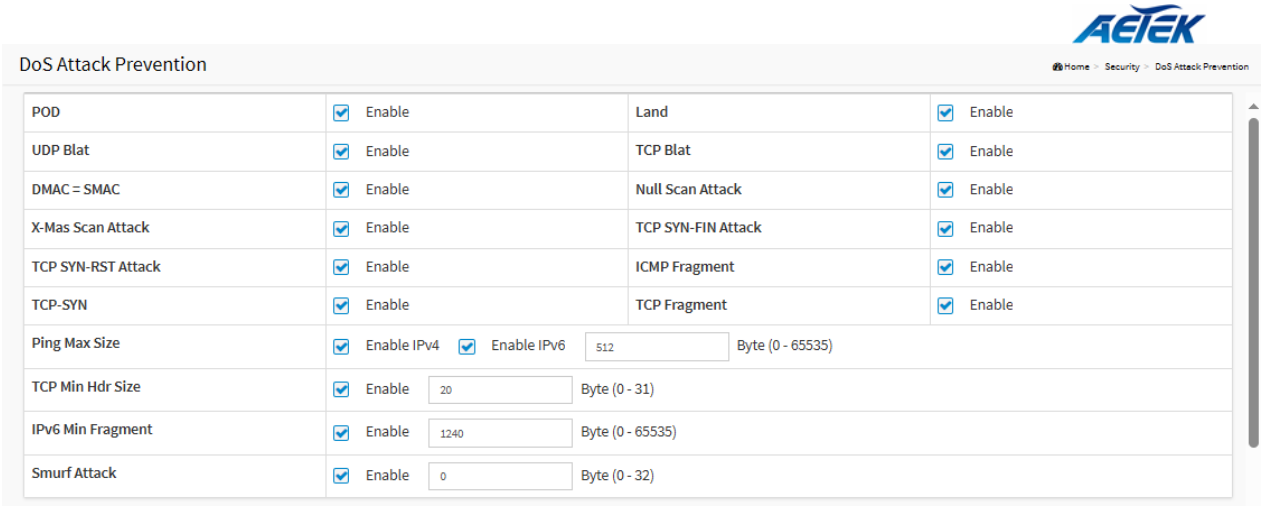


Figure 9-10: DoS Attack Prevention

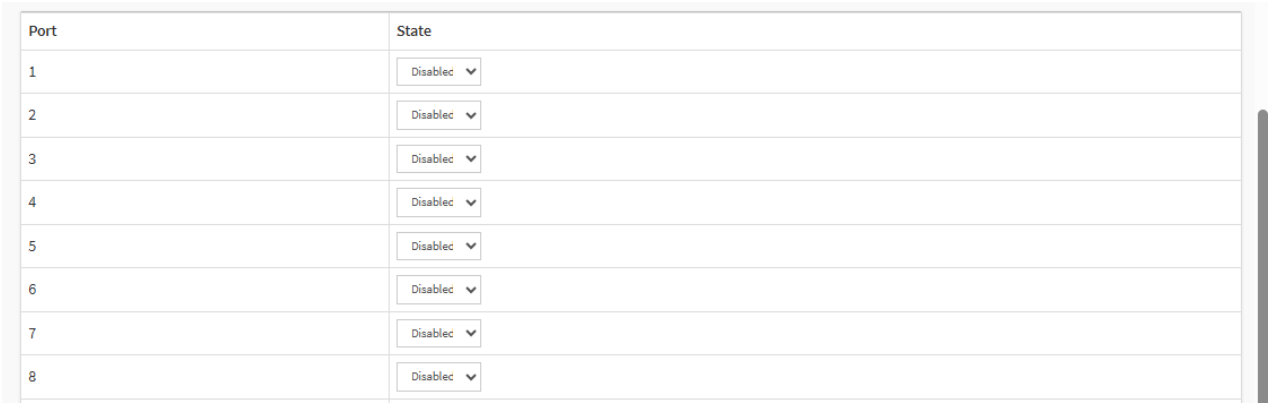


Figure 9-10: DoS Attack Prevention (Detail)

Parameter description:

- **Port**

  The normal port of the device.

- **State**

  To enable/disable the function.

Chapter 10 Access Control

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.

10-1 Create ACL

The page describes how to create Access Control List rule.

Web Interface

To create the ACL rule in the web interface:

1. Click Access Control -> Create ACL.
2. Specify the parameter you want to configure.
3. Click Apply.

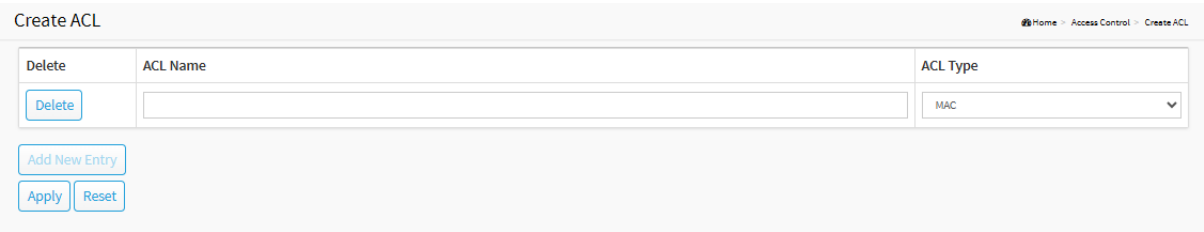


Figure 10-1: Create ACL

Parameter description:

- **Delete**

  To delete the Access Control List.

- **ACL Name**

  The Name of the Access Control List.

- **ACL Type**

  Indicates the type of the ACL. Including MAC and IPv4.

10-2 Create ACE

10-2-1 MAC

The page describes how to configure MAC Access Control Entry rule.

Web Interface

To create the MAC ACE rule in the web interface:

1. Click Access Control -> Create ACE -> MAC.
2. Specify the parameter you want to configure.
3. Click Apply.

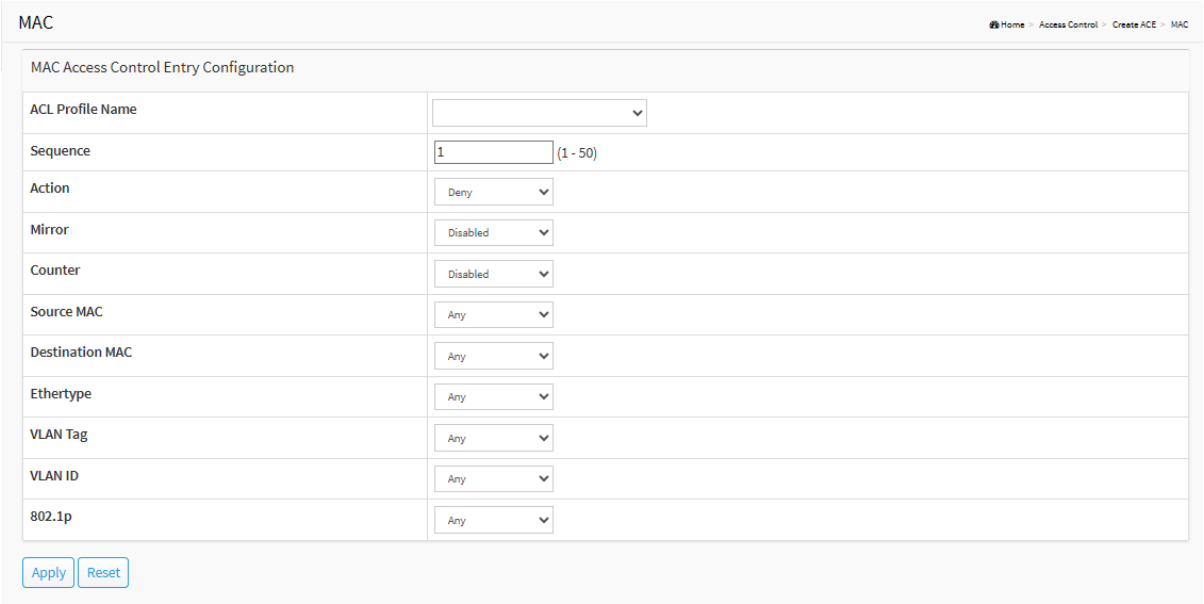


Figure 10-2-1: Create MAC ACE

Parameter description:

- **ACL Profile Name**

  The profile name for the access control list.

- **Sequence**

  Specify sequence of access control entry.

- **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.

  Shutdown: Specify the port shut down operation of the ACE.

- **Mirror**

  Select mirror mode, enable or disable.

- **Mirror Port**

  Select mirror port.

- **Counter**

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

- **Source MAC**

  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 a SMAC value appears.

- **Destination MAC**

  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.

- **EtherType**

  Specify the Ethernet type filter for this ACE.

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

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

- **Ethernet Type Value**

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

- **VLAN Tag**

  Specify the VLAN tagged or untagged for this ACE. The value Any means that no tag is specified (tag is "don't-care".)

- **VLAN ID**

  Specify the VLAN ID filter for this ACE.

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

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

- **802.1p Priority**

  Specify the tag priority for this ACE. A frame that hits this ACE matches this tag priority. The allowed number range is 0 to 7. The value Any means that no tag priority is specified (tag priority is "don't-care".)

The page describes how to configure IPv4 Access Control Entry rule.

Web Interface

To create the MAC ACE rule in the web interface:

1. Click Access Control -> Create ACE -> IPv4.
2. Specify the parameter you want to configure.
3. Click Apply.

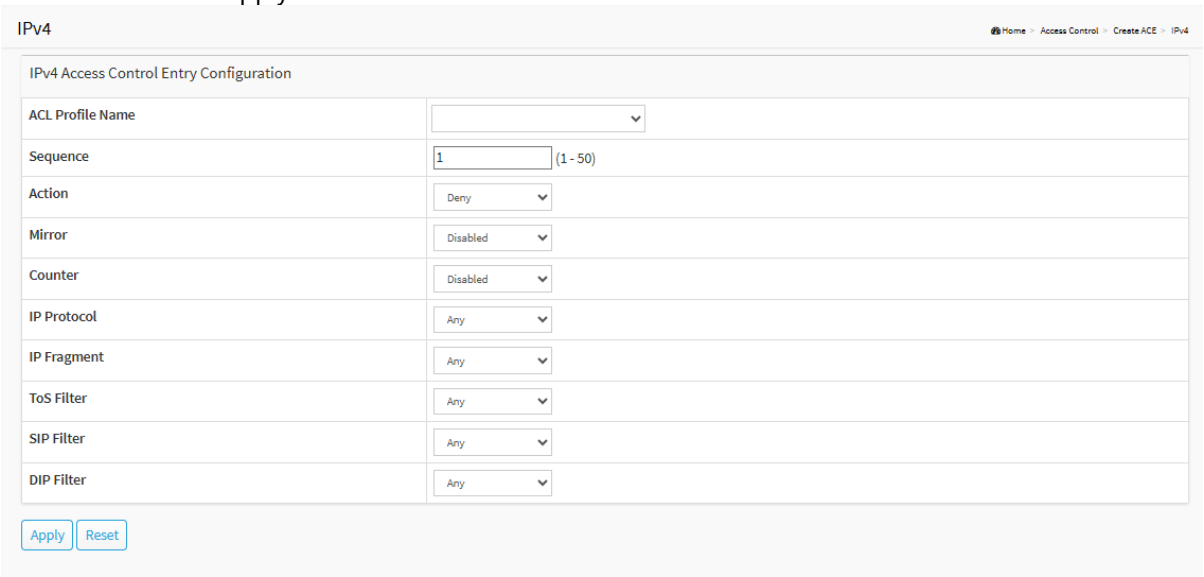


Figure 10-2-2: Create IPv4 ACE

Parameter description:

- **ACL Profile Name**

  The profile name for the access control list.

- **Sequence**

  Specify sequence of access control entry.

- **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.

  Shutdown: Specify the port shut down operation of the ACE.

- **Mirror**

  Select mirror mode, enable or disable.

- **Mirror Port**

  Select mirror port.

- **Counter**

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

- **IP Protocol**

  Specify the IP protocol filter for this ACE.

  Any: The ACE will match any frame type.

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

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

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

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

- **ICMP Type Filter**

  Specify the ICMP type filter for this ACE.

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

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

- **ICMP Type Value**

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

- **ICMP Code Filter**

  Specify the ICMP code filter for this ACE.

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

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

- **ICMP Code Value**

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

- **TCP/UDP Source Port**

  The TCP/UDP source port value. The allowed range is 0 to 65535. A frame that hits this ACE matches this TCP/UDP source port value.

- **TCP/UDP Destination Port**

  The TCP/UDP destination port value. The allowed range is 0 to 65535. A frame that hits this ACE matches this TCP/UDP destination port value.

- **TCP FIN**

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

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

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

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

- **TCP SYN**

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

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

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

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

- **TCP RST**

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

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

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

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

- **TCP PSH**

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

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

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

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

- **TCP ACK**

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

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

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

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

- **TCP URG**

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

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

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

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

- **IP Fragment**

  IPv4 frame fragmented option: 1, 0, any.

- **ToS Filter**

  ToS Filter option: Any, DSCP, IP Precedence.

- **SIP Filter**

  Source IP Filter option: Any, Network.

- **DIP Filter**

  Destination IP Filter option: Any, Network.

10-3 ACE Lists

10-3-1 MAC List

The page shows the MAC Access Control Entries lists.

Web Interface

To display the ACE lists in the web interface:

1. Click Access Control -> ACE Lists -> MAC List.

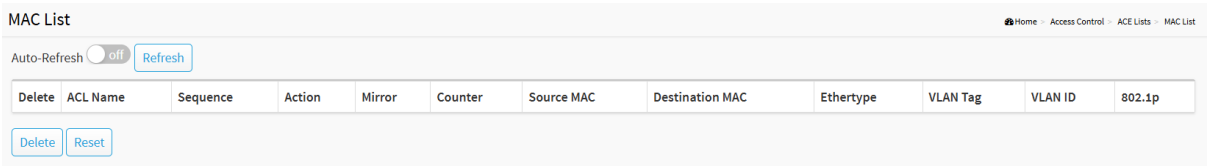


Figure 10-3-1: MAC ACE lists

10-3-2 IPv4 List

The page shows the IP Access Control Entries lists.

Web Interface

To display the ACE lists in the web interface:

1. Click Access Control -> ACE Lists -> IPv4 List.

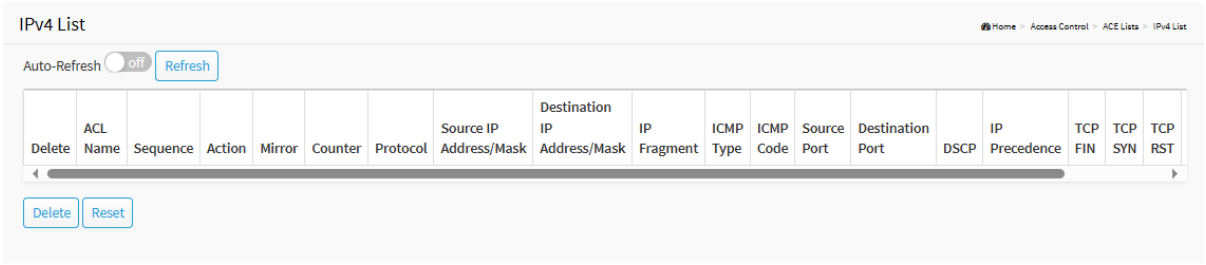


Figure 10-3-2: IPv4 ACE lists

10-4 ACL Binding

The page describes how to configure Access Control List binding. When an ACL is bound to an interface, its ACE rules are applied to packets arriving to that interface.

Web Interface

To configure the ACL binding in the web interface:

1. Click Access Control -> ACE Binding.
2. Specify the parameter you want to configure.
3. Click Apply.

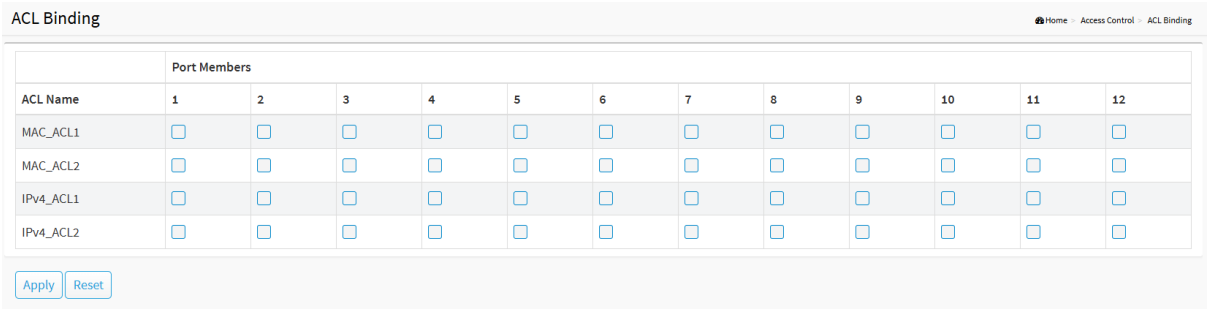


Figure 10-4: ACL Binding

Parameter description:

- **Port**

  The Interface selected for the Access Control List. For each type of interface that was selected, all interfaces of that type are displayed with a list of their current ACLs:

  MAC ACL: ACLs of type MAC that are bound to the interface (if any).

  IPv4 ACL: ACLs of type IPv4 that are bound to the interface (if any).

- **ACL Name**

  Specify the ACL Name for the binding of this Interface.

Chapter 11 SNMP

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

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

11-1 Configuration

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

Web Interface

To configure the configure SNMP System in the web interface:

1. Click Security, SNMP and configuration.
2. Evoke SNMP State to enable or disable the SNMP function.
3. Specify the Read Community, Write Community.
4. Click Apply.

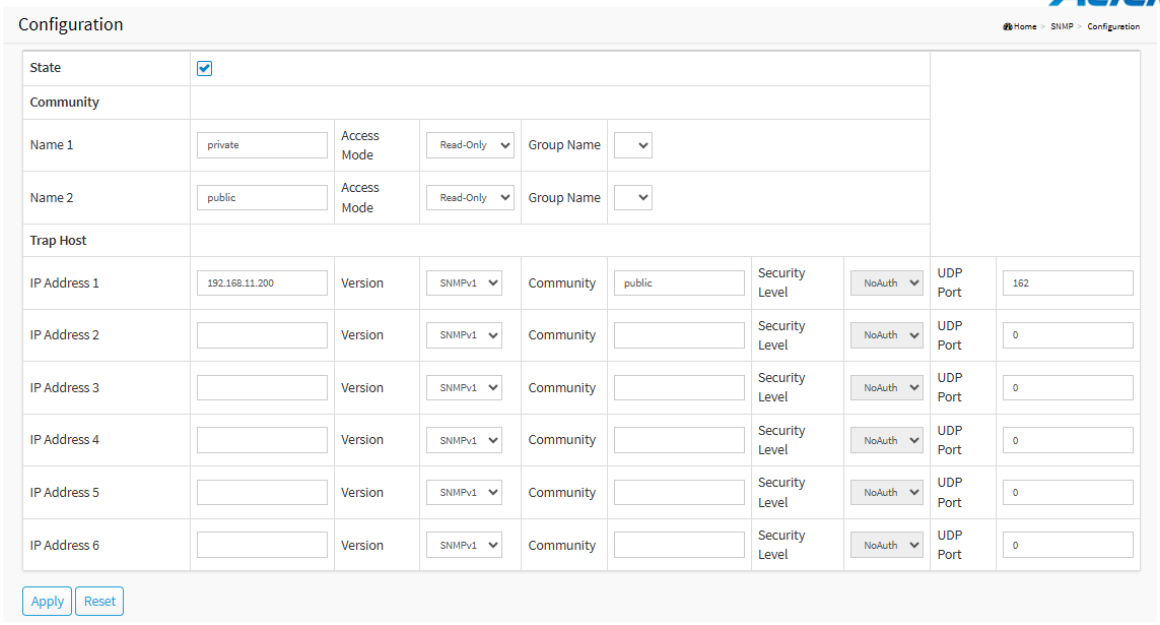


Figure 11-1: The SNMP Configuration

Parameter description:

- **State**

  To enable/disable SNMP function.

- **Community**

  To set the community name and access level.

- **Name 1/2**

  To set the community name.

- **Access Mode**

  Select the access level. Read-Only permits viewing only; Read-Write allows configuration changes.

- **Group Name**

  To assign the community to a group.

- **IP Address**

  To specify the SNMP manager IP address.

- **Version**

  To select the SNMP version (v1/v2/v3).

- **Community**

  To set the community string.

- **Security Level**

  To select the SNMPv3 security level.

- **UDP Port**

  To specify the UDP port.

Buttons:

- **Apply**

  Click to save changes.

- **Reset**

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

11-2 SNMPv3

11-2-1 Communities

The function is used to configure SNMPv3 communities.

Web Interface

To configure the configure SNMP Communities in the web interface:

1. Click Security -> SNMP -> SNMPv3 -> Communities.
2. Select a previously added community string from the list.
3. Click Apply.
4. If you want to modify or clear the setting then click Reset.

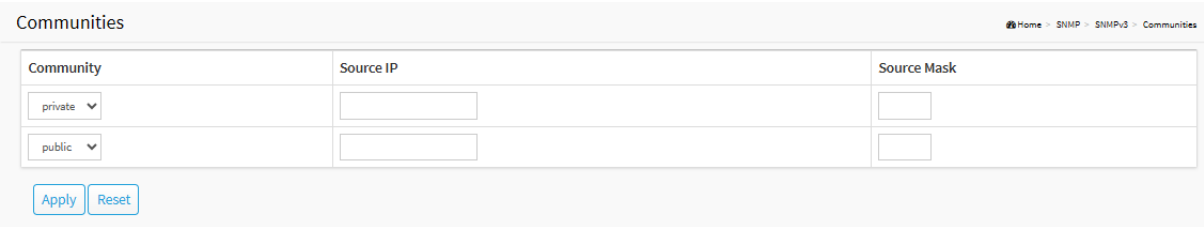


Figure 11-2-1: The SNMPv3 Communities Configuration

Parameter description:

- **Community**

  Indicates the community access string to permit access to SNMPv3 agent.

- **Source IP**

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

- **Source Mask**

  Indicates the SNMP access source address mask

Buttons:

- **Apply**

  Click to save changes.

- **Reset**

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

11-2-2 Users

The function is used to configure SNMPv3 Users.

Web Interface

To configure the configure SNMP Communities in the web interface:

1. Click Security -> SNMP -> SNMPv3 -> Users.
2. Click Add new Entry.
3. Specify the SNMPv3 Users parameter.
4. Click Apply.

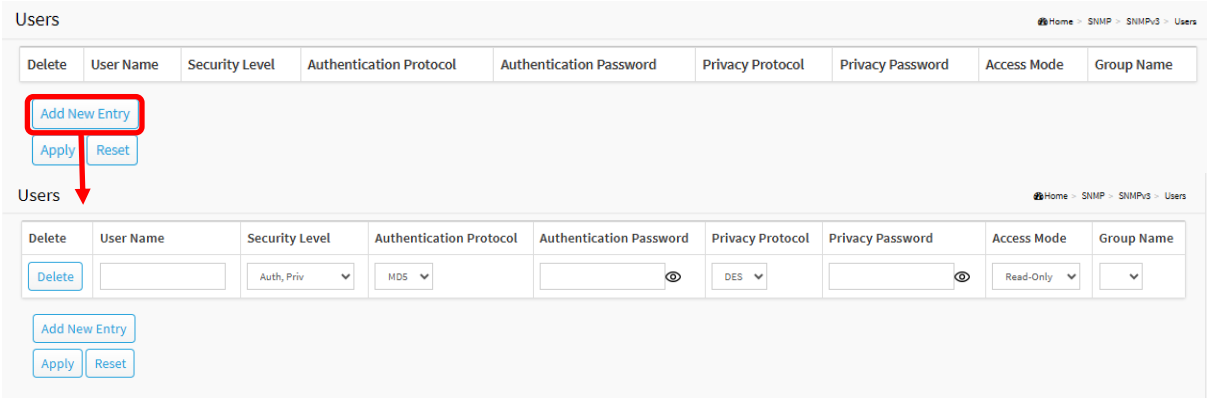


Figure 11-2-2: The SNMPv3 Users Configuration

Parameter description:

- **User Name**

  A string identifying the user name that this entry should belong to. The allowed string length is 1 to 31, and the allowed content is ASCII characters from 33 to 126.

- **Security Level**

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

  NoAuth, NoPriv: No authentication and no privacy.

  Auth, NoPriv: Authentication and no privacy.

  Auth, Priv: Authentication and privacy.

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

- **Authentication Protocol**

  Indicates the authentication protocol that this entry should belong to.

  Possible authentication protocols are:

  MD5: An optional flag to indicate that this user uses MD5 authentication protocol.

  SHA: An optional flag to indicate that this user uses SHA authentication protocol.

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

- **Authentication Password**

  A string identifying the authentication password phrase. For MD5 authentication protocol, the allowed string length is 8 to 39. For SHA authentication protocol, the allowed string length is 8 to 39. 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:

  DES: An optional flag to indicate that this user uses DES authentication protocol.

  AES: An optional flag to indicate that this user uses AES authentication protocol.

- **Privacy Password**

  A string identifying the privacy password phrase. The allowed string length is 8 to 31, and the allowed content is ASCII characters from 33 to 126.

- **Access Mode**

  The access level assigned to the SNMPv3 user, defining permitted operations.

  Read-Only: Allows retrieval operations; no SET or configuration changes.

  Read-Write: Allows retrieval and SET operations on objects permitted by the user's group; configuration changes are allowed.

- **Group Name**

  Assign the user to an SNMPv3 group.

Buttons:

- **Add New Entry**

  Click to add new entry. Specify the name and configure the new entry. Click "Apply".

- **Delete**

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

- **Apply**

  Click to save changes.

- **Reset**

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

11-2-3 Groups

The function is used to configure SNMPv3 group. The Entry index key are Security Model and Security Name. To create a new group account, please check <Add new group> button, and enter the group information then check <Save>. Max Group Number:12.

Web Interface

To configure SNMP Groups in the web interface:

1. Click Security, SNMP, SNMPv3 and Groups.
2. Click Add new entry.
3. Specify the SNMP group parameter.
4. Click Apply.

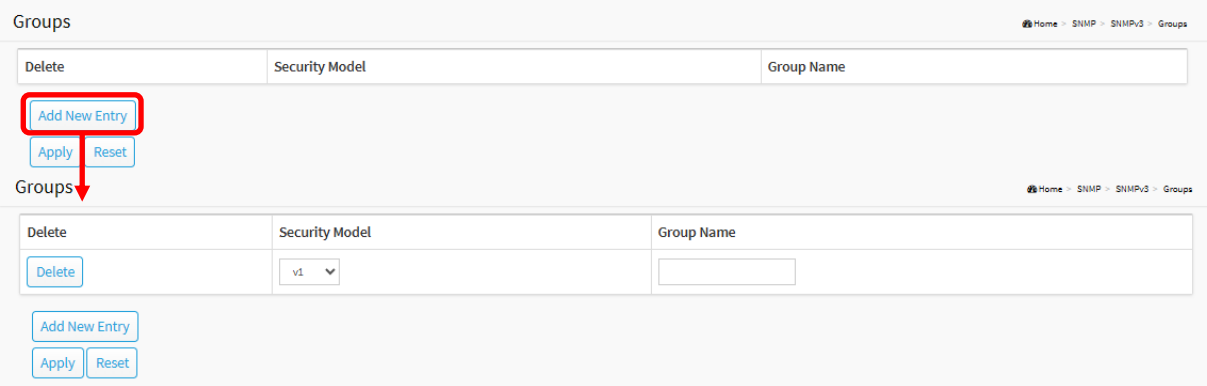


Figure 11-2-3: The SNMP Groups Configuration

Parameter description:

- **Security Model**

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

  v1: Reserved for SNMPv1.

  v2c: Reserved for SNMPv2c.

  usm: User-based Security Model (USM).

- **Group Name**

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

Buttons:

- **Add New Entry**

  Click to add new entry. Specify the name and configure the new entry. Click "Apply".

- **Delete**

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

- **Apply**

  Click to save changes.

- **Reset**

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

The function is used to configure SNMPv3 view. The Entry index keys are OID Subtree and View Name. To create a new view account, please check <Add new view> button, and enter the view information then click <Apply>. Max Group Number: 12.

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

Web Interface

To configure SNMP views in the web interface:

1. Click Security, SNMP, SNMPv3 and Views.
2. Click Add new entry.
3. Specify the SNMP View parameters.
4. Click Apply.
5. If you want to modify or clear the setting then click Reset.

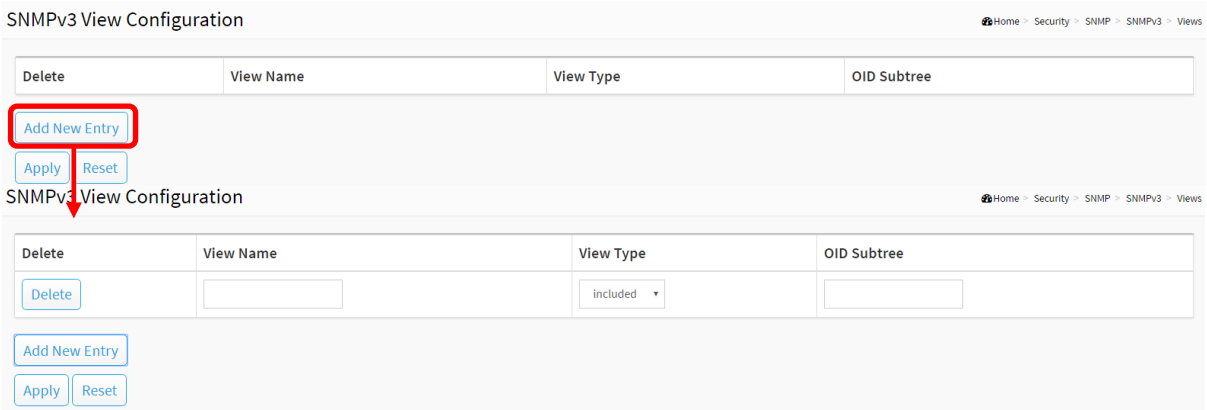


Figure 11-2-4: The SNMP Views Configuration

Parameter description:

- **View Name**

  A string identifying the view name that this entry should belong to. The allowed string length is 1 to 31, and the allowed content is ASCII characters from 33 to 126.

- **View Type**

  Indicates the view type that this entry should belong to. Possible view types are:

  Included: An optional flag to indicate that this view subtree should be included.

  Excluded: An optional flag to indicate that this view subtree should be excluded.

  In general, if a view entry's view type is 'excluded', there should be another view entry existing with view type as 'included' and it's OID subtree should overstep the 'excluded' view entry.

- **OID Subtree**

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

Buttons:

- **Add New Entry**

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

- **Delete**

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

- **Apply**

  Click to save changes.

- **Reset**

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

11-2-5 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 <Apply>. Max Group Number : 12.

Web Interface

To display the configure SNMP Access in the web interface:

1. Click Security, SNMP, SNMPv3 and Accesses.
2. Click Add new entry.
3. Specify the SNMP Access parameters.
4. Click Apply.
5. If you want to modify or clear the setting then click Reset.

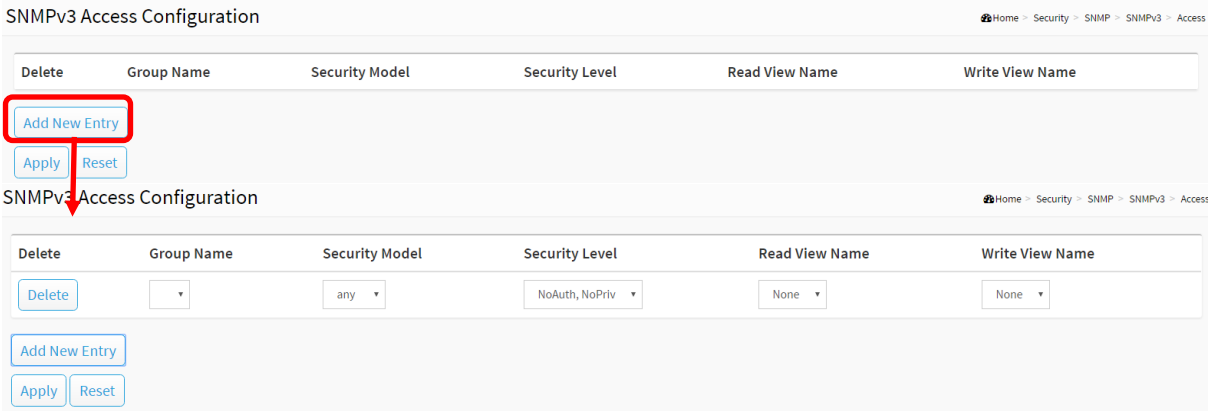


Figure 11-2-5: The SNMP Accesses Configuration

Parameter description:

- **Group Name**

  A string identifying the group name that this entry should belong to. The allowed string length is 1 to 31, 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:

  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 31, 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 31, and the allowed content is ASCII characters from 33 to 126.

Buttons:

- **Add New Entry**

  Click to add new entry. Specify the name and configure the new entry. Click "Apply".

- **Delete**

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

- **Apply**

  Click to save changes.

- **Reset**

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

Chapter 12 Event Notification

12-1 SMTP Settings

Configure SMTP (Simple Mail Transfer Protocol) on this page. Simple Mail Transfer Protocol is the message-exchange standard for the Internet.
The Switch is to be configured as a client of SMTP while the server is a remote device that will receive messages from the switch that alarm events occurred.
Please go to SMTP Setting user interface help page to see the full setting description.

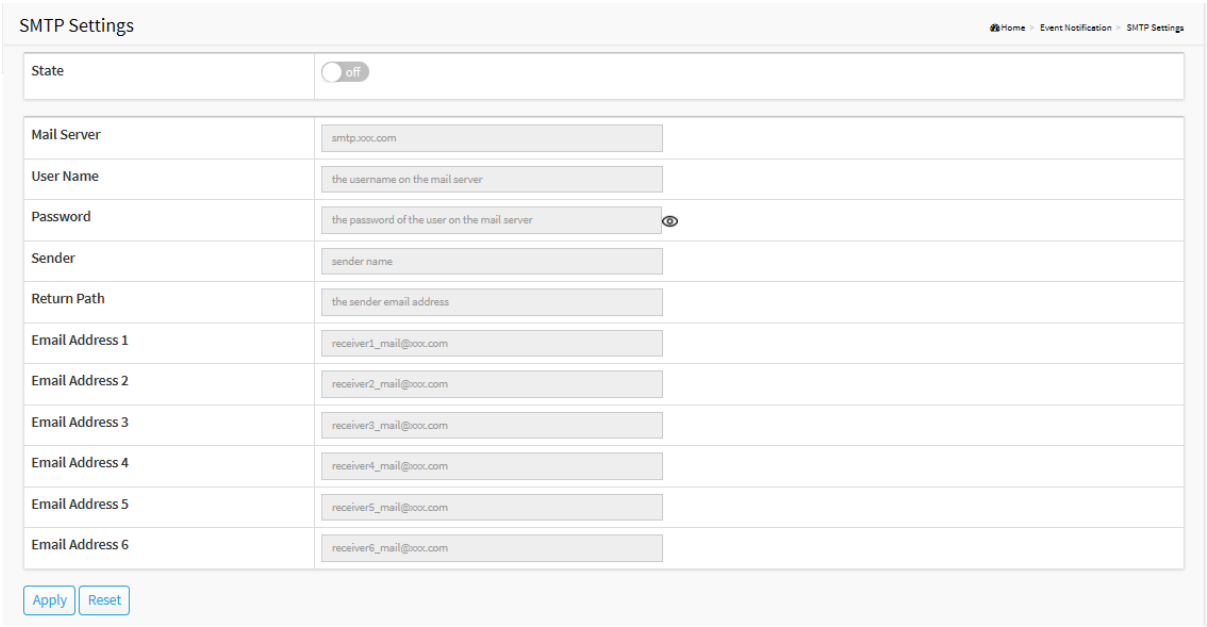


Figure 12-1: SMTP Settings

12-2 Syslog

12-2-1 Syslog Configuration

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

Web Interface

To configure the SysLog Settings in the web interface:

1. Click Syslog -> Syslog Configuration.

2. Specify Mode and Server 1(or Server 2) parameters.
3. Click Apply.

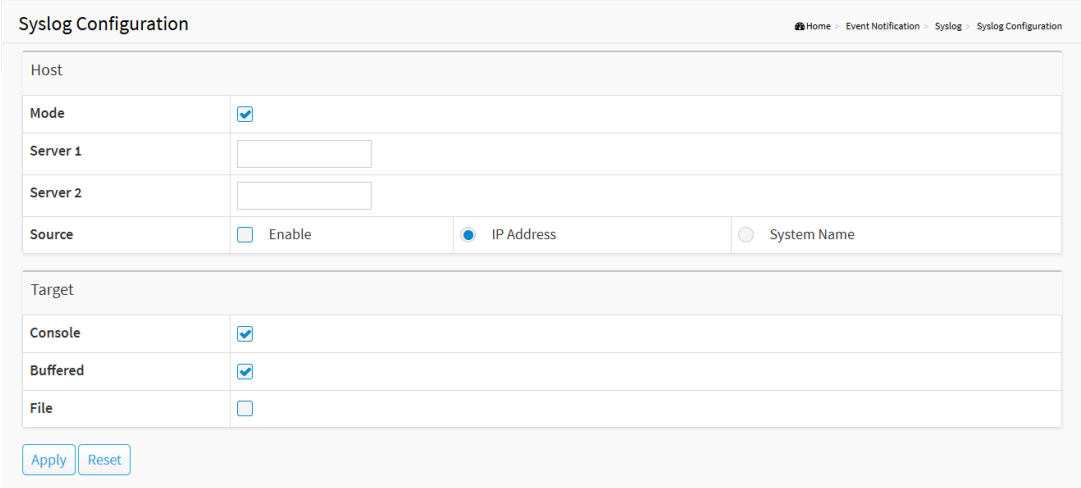


Figure 12-2-1: Syslog Configuration

Parameter Description:

- **Mode**

  To enable/disable Syslog function

- **Server1(or Server2)**

  SysLog Server. (IPv4 format)

- **Source**

  To enable, choose to display either IP or System in the log.

- **Console**

  To enable/disable console logging output (syslog to console).

- **Buffered**

  To enable/disable buffered logging (syslog to RAM).

- **File**

  To enable/disable file logging (syslog to flash).

12-2-2 Buffered Logging

This page provides a buffered log of recent system events for quick review and allows exporting the log to a file.

Web Interface

To view the event in the web interface:

1. Click Syslog -> Buffered Logging.

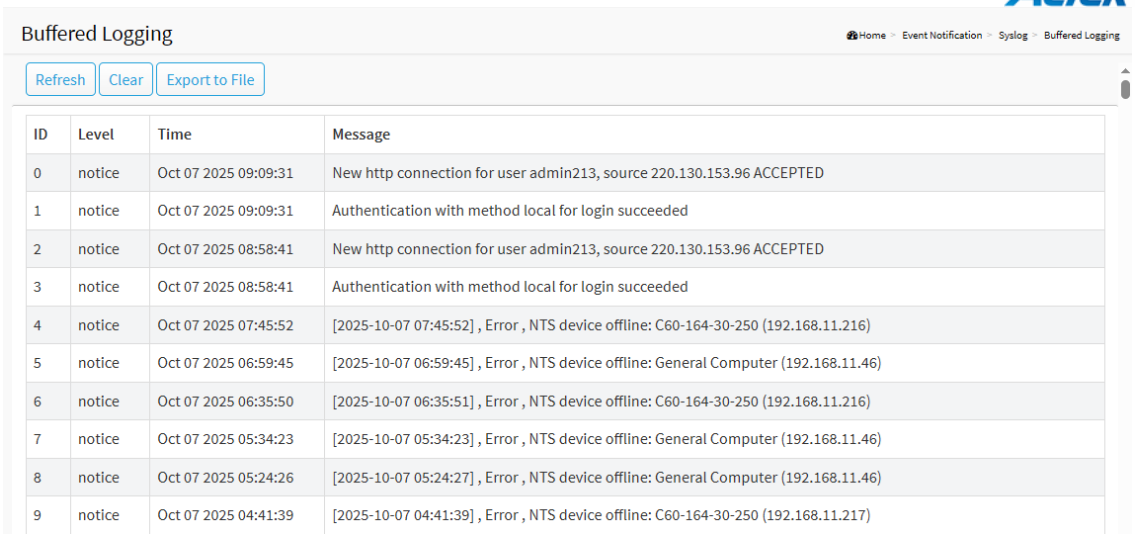


Figure 12-2-2: Buffered Logging

Parameter description:

- **Level**

  The event category.

- **Time**

  Timestamp of the event.

- **Message**

  The text content of the log entry.

Buttons:

- **Refresh**

  Reload the log list.

- **Clear**

  Clear all buffered log messages.

- **Export to file**

  To export logging messages to file.

12-2-3 File Logging

This page displays file log messages saved on the device.

Web Interface

To view the file log in the web interface:

1. Click Syslog -> File Logging.

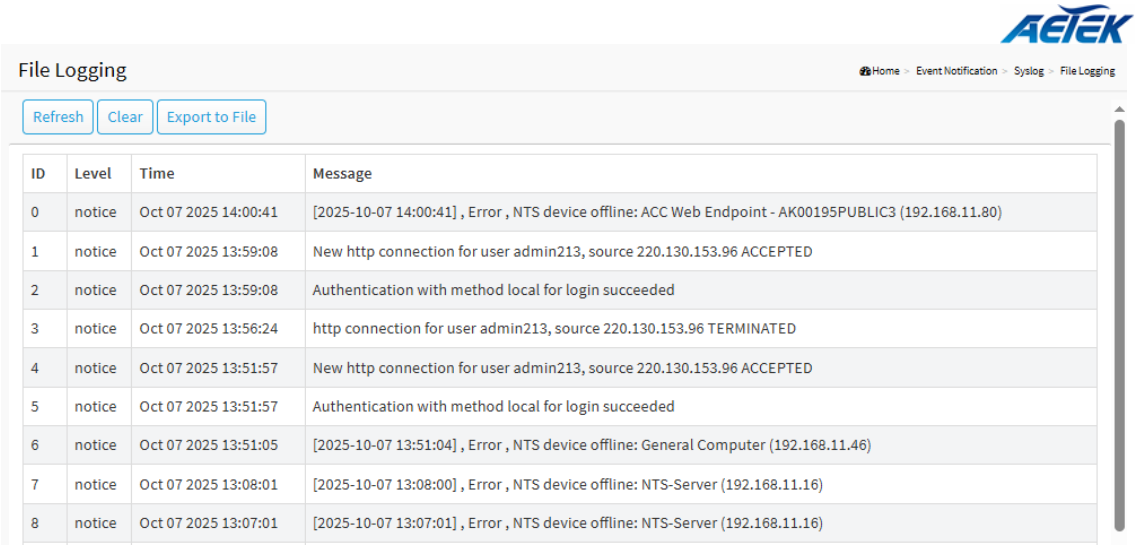


Figure 12-2-3: File Logging

Parameter description:

- **Level**

  The event category.

- **Time**

  Timestamp of the event.

- **Message**

  The text content of the log entry.

Buttons:

- **Refresh**

  Reload the log list.

- **Clear**

  Clear all buffered log messages.

- **Export to file**

  To export logging messages to file.

12-3 Event Configuration

This page displays event configurations for Syslog, SNMP trap and SMTP.

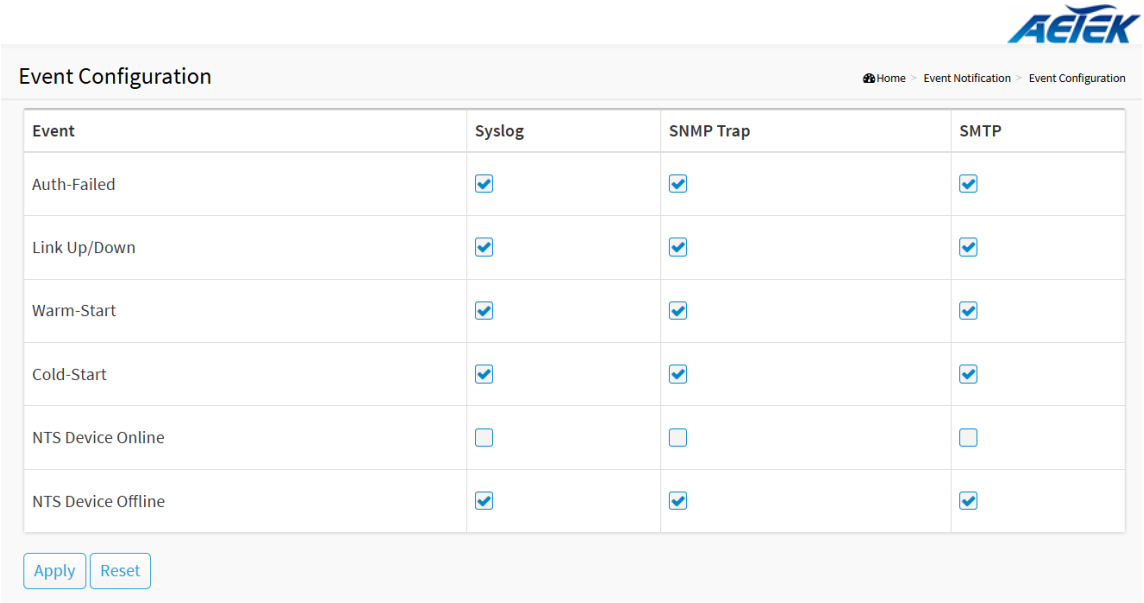


Figure 12-3: Event Configuration

Chapter 13 Quality of Service

Quality of Service refers to traffic prioritization and resource reservation control mechanisms rather than the achieved service quality. Quality of Service is the ability to provide different priority to different applications, users, or data flows, or to guarantee a certain level of performance to a data flow.

Quality of Service is particularly important for the transport of traffic with special requirements. In particular, developers have introduced Voice over IP technology to allow computer networks to become as useful as telephone networks for audio conversations, as well as supporting new applications with even stricter network performance requirements.

13-1 Global Settings

This page is used to configure the QoS mode, including CoS/802.1p, DSCP ,IP Precedence and 802.1p /DSCP.

Web Interface

To configure the QoS mode in the web interface:

1. Click Quality of Service -> Global Setting
2. Specify the parameter you want to configure.
3. Click Apply.

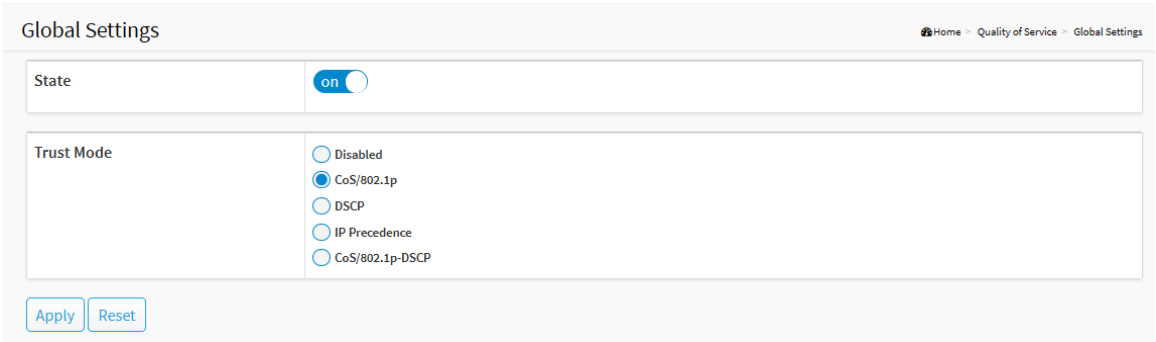


Figure 13-1: Global Setting

Parameter Description:

- **Disable**

  Do not trust any incoming markings.

- **CoS/802.1p**

  Traffic is mapped to queues based on the VPT field in the VLAN tag, or based on the per-port default CoS/802.1p value (if there is no VLAN tag on the incoming packet), the actual mapping of the VPT to queue can be configured on the CoS/802.1p to Queue page.

- **DSCP**

  All IP traffic is mapped to queues based on the DSCP field in the IP header. The actual mapping of the DSCP to queue can be configured on the DSCP to Queue page. If traffic is not IP traffic, it is mapped to the best effort queue.

- **IP Precedence**

  Traffic is mapped to queues based on the IP precedence. The actual mapping of the IP precedence to queue can be configured on the IP Precedence to Queue page.

- **CoS/802.1p-DSCP**

  Differentiated Services Code Point (DSCP) is a priority level that prioritizes the network traffic based on the DSCP queue mapping on the DSCP Settings page.

13-2 Port Settings

Web Interface

To configure the logical port for the setting in the web interface:

1. Click Quality of Service -> Port Setting.
2. Specify the parameter you want to configure.
3. Click Apply.

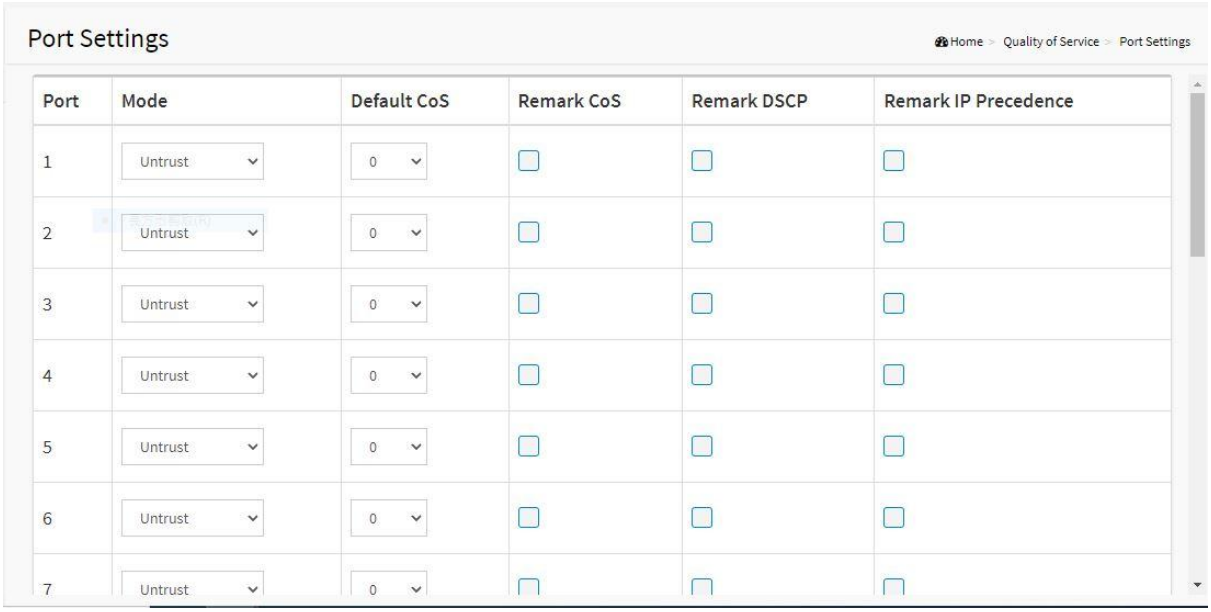


Figure 13-2: Port Setting

Parameter Description:

- **Mode**

  Untrust:

  All ingress traffic on the port is mapped to the best effort queue and no classification/prioritization takes place.

Trust:

Port prioritize ingress traffic is based on the system wide configured trusted mode, which is either CoS/802.1p trusted mode, IP Precedence trusted mode or DSCP trusted mode.

- **Default CoS**

  FIFO, Low, Normal, Medium and High. Select the default CoS value to be assigned for incoming untagged packets. The range is 0 to 7.

- **Remark CoS**

  Click the checkbox to remark the CoS/802.1p priority for egress traffic on this port.

- **Remark DSCP**

  Click the checkbox to remark the DSCP value for egress traffic on this port.

- **Remark IP Precedence**

  Click the checkbox to remark the IP precedence for egress traffic on this port.

13-3 Port Policing

Web Interface

To configure the logical port for the setting in the web interface:

1. Click Quality of Service -> Port Policing.
2. Specify the parameter you want to configure.
3. Click Apply.

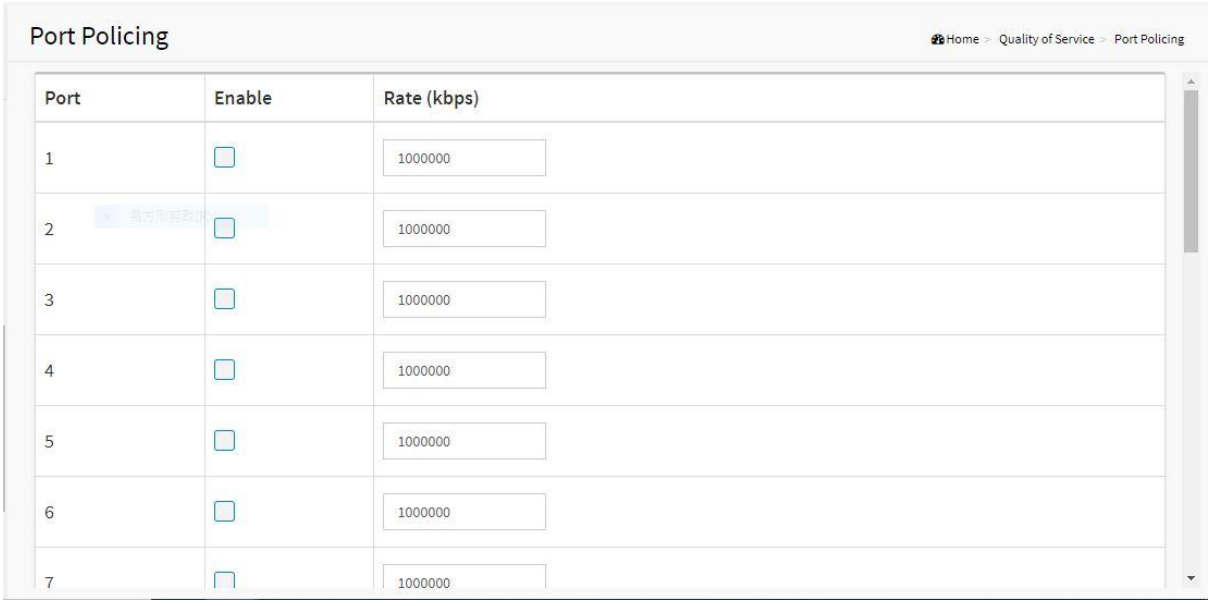


Figure 13-3: Port Policing

Parameter Description:

- **Enable**

  To evoke which Port you need to enable the QoS Ingress Port Policers function.

- **Rate(kbps)**
  To set the Rate limit value for this port, the default is 1000000.

13-4 Port Shaper

Web Interface

To configure the logical port for the setting in the web interface:

1. Click Quality of Service -> Port Shaper.
2. Specify the parameter you want to configure.
3. Click Apply.

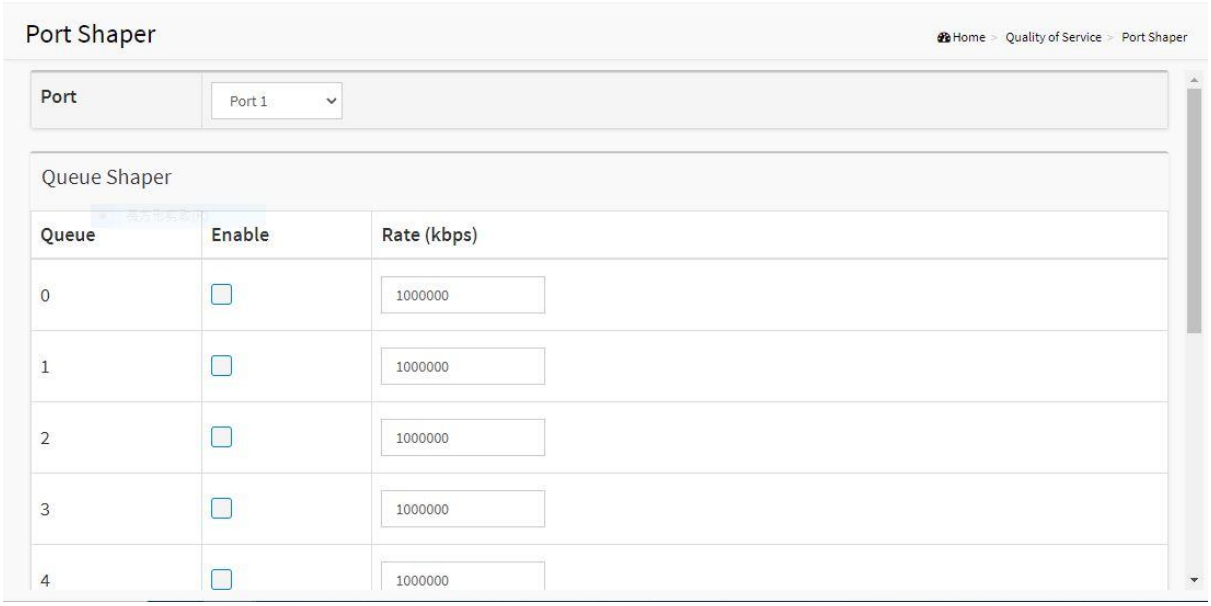


Figure 13-4: Port Shaper

Parameter Description:

- **Enable**

  Controls whether the queue shaper is enabled for this queue on this switch port.

- **Rate(kbps)**
  Controls the rate for the queue shaper. The default value is 1000000.

13-5 Port Scheduler

Web Interface

To configure the logical port for the setting in the web interface:

1. Click Quality of Service -> Port Scheduler.
2. Specify the parameter you want to configure.
3. Click Apply.

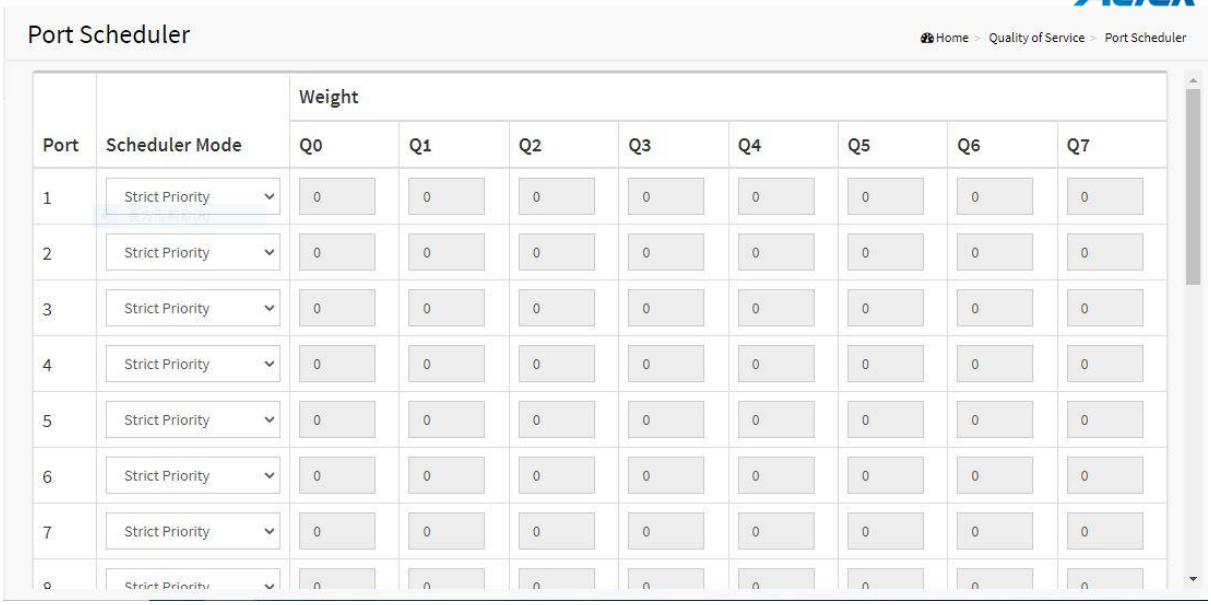


Figure 13-5: Port Scheduler

Parameter Description:

- **Scheduler Mode**

  Controls whether the queue shaper is enabled for this queue on this switch port. Controls whether the scheduler mode is "Strict Priority", "WRR" or "WFQ" on this switch port.

- **Weight**

  Controls the rate for the queue shaper. The default value is 1000000. Controls the weight for this queue. The default value is "0". This value is restricted to 0-127. This parameter is only shown if "Scheduler Mode" is set to "Weighted".

13-6 CoS/802.1p Mapping

This page is used to configure the Class of Service (CoS) which prioritizes the network traffic based on the CoS queue mapping on the CoS Settings.

Web Interface

To configure the CoS in the web interface:

1. Click Quality of Service -> CoS/802.1p Mapping.
2. Specify the parameter you want to configure.
3. Click Apply.

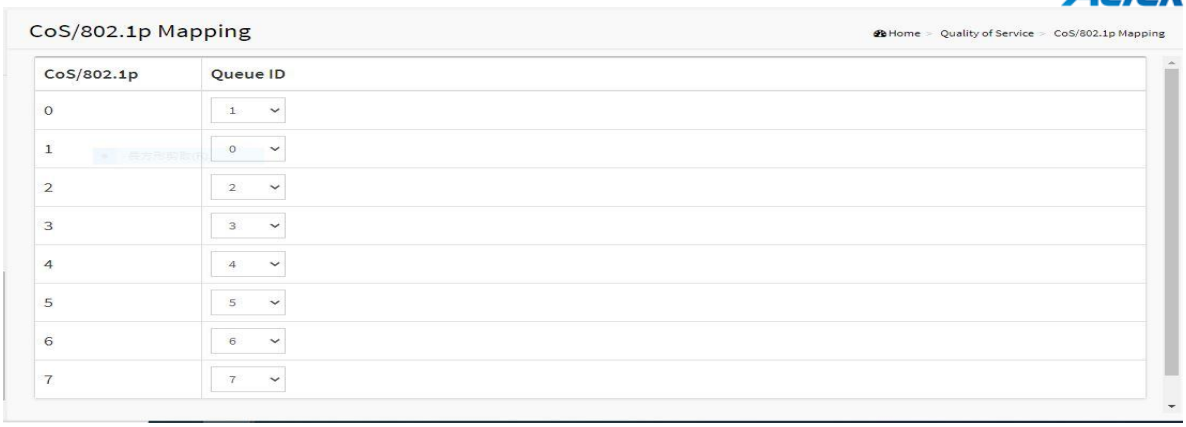


Figure 13-6: CoS/802.1p Mapping

Parameter Description:

- **Queue ID**

  Select the egress queue to which the 802.1p priority is mapped. Eight egress queues are supported, where Queue 7 is the highest priority egress queue and Queue 0 is the lowest priority egress queue.

13-7 CoS/802.1p Remarking

This page is use the Queues to CoS/802.1p page to remark the CoS/802.1p priority for egress traffic from each queue.

Web Interface

To configure the rate limit function in the web interface:

1. Click Quality of Service -> CoS/802.1p remarking
2. Specify the parameter you want to configure.
3. Click Apply.

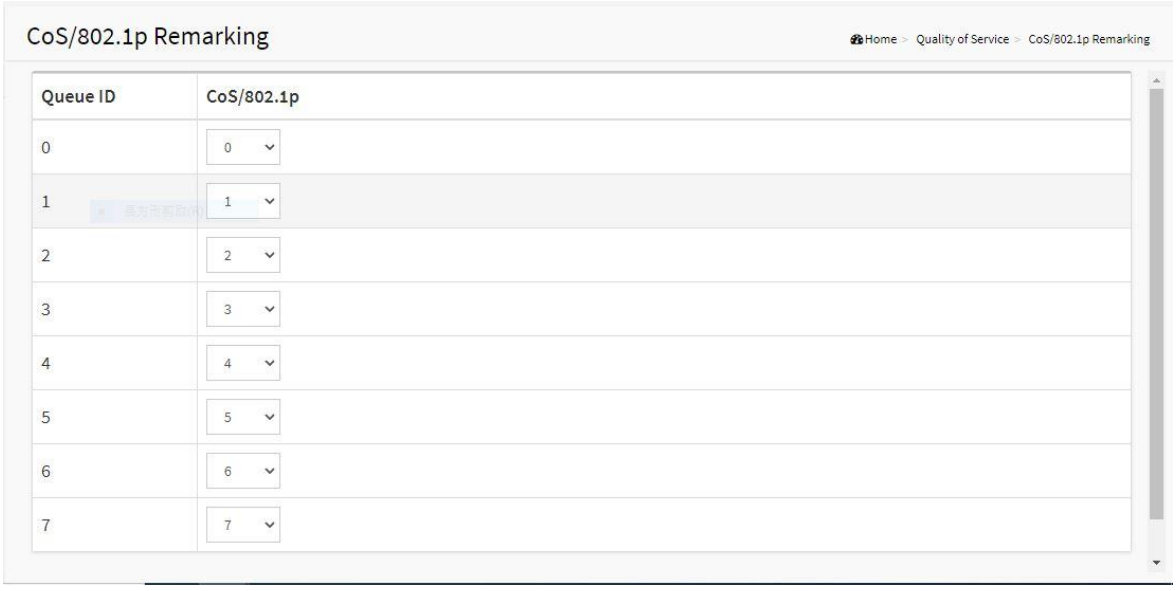


Figure 13-7: CoS/802.1p Remarking

Parameter Description:

- **Queue ID**

  Displays the Queue ID, where Queue 7 is the highest priority egress queue and Queue 0 is the lowest priority egress queue.

- **CoS/802.1p**

  For each output queue, select the CoS/802.1p priority to which egress traffic from the queue is remarked.

13-8 IP Precedence Mapping

This page maps each egress queue to an IP Precedence value (0–7) used to remark outbound traffic.

Web Interface

To configure the rate limit function in the web interface:

1. Click Quality of Service -> IP Precedence Remarking.
2. Specify the parameter you want to configure.
3. Click Apply.

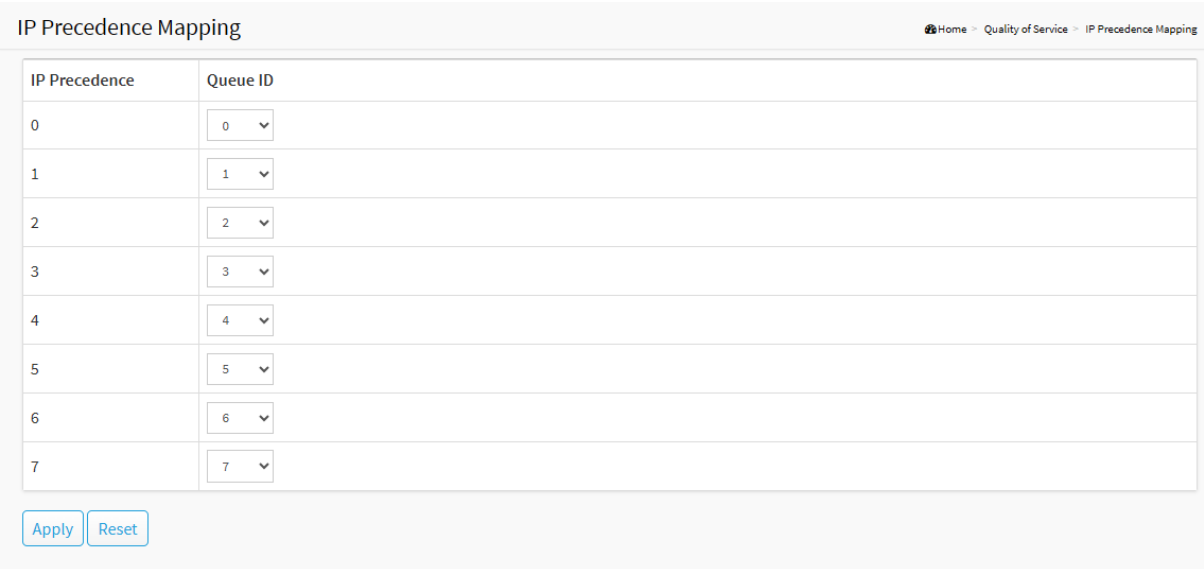


Figure 13-8: IP Precedence Remarking

Parameter Description:

- **IP Precedence**

  Indicates the priority tag value assigned to each egress queue, where 0 represents the lowest and 7 the highest forwarding priority.

- **Queue ID**

  Displays the Queue ID, where Queue 7 is the highest priority egress queue and Queue 0 is the

lowest priority egress queue.

13-9 IP Precedence Remarking

This page is used to map IP Precedence values to egress queues for traffic classification and forwarding priority.

Web Interface

To configure the rate limit function in the web interface:

1. Click Quality of Service -> IP Precedence Remarking.
2. Specify the parameter you want to configure.
3. Click Apply.

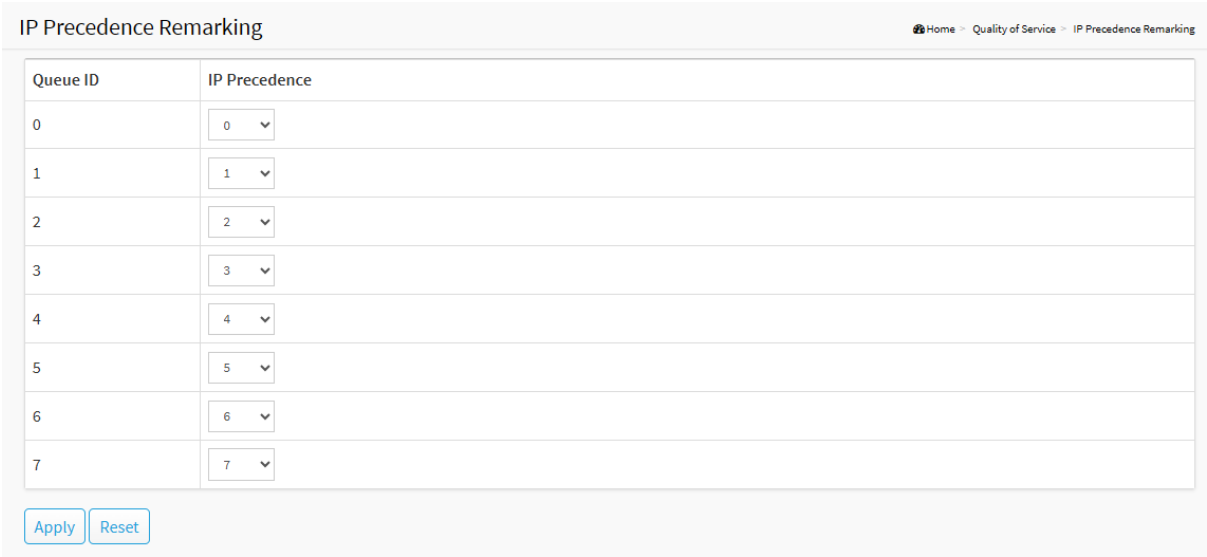


Figure 13-9: IP Precedence Remarking

Parameter Description:

- **Queue ID**

  The egress queue identifier (0–7); 7 is highest priority and 0 is lowest.

- **IP Precedence**

  The remarking value (0–7) applied to traffic leaving the selected queue.

13-10 DSCP Mapping

This page maps IP DSCP values to egress queues for incoming IP packets. The original VLAN Priority Tag (802.1p/CoS) remains unchanged; QoS can be tuned by adjusting this mapping along with queue scheduling and bandwidth allocation.

Web Interface

To configure the rate limit function in the web interface:

1. Click Quality of Service -> DSCP Mapping.
2. Specify the parameter you want to configure.
3. Click Apply.

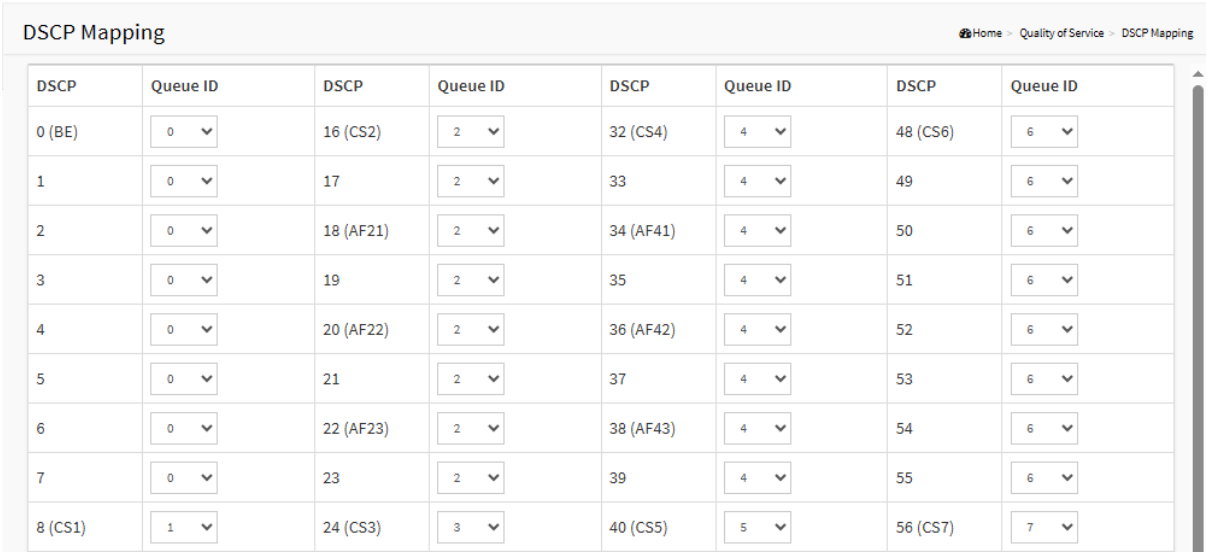


Figure 13-10: DSCP Mapping

Parameter Description:

- **DSCP**
  The DSCP value (0–63) in the incoming IP packet, representing the traffic class for QoS mapping.
- **Queue ID**
  The identifier of the egress queue (0–7) to which packets with the given DSCP value are mapped.

13-11 DSCP Remarking

This page is used to map IP Precedence values to egress queues for traffic classification and forwarding priority.

Web Interface

To configure the rate limit function in the web interface:

1. Click Quality of Service -> DSCP Remarking.
2. Specify the parameter you want to configure.
3. Click Apply.

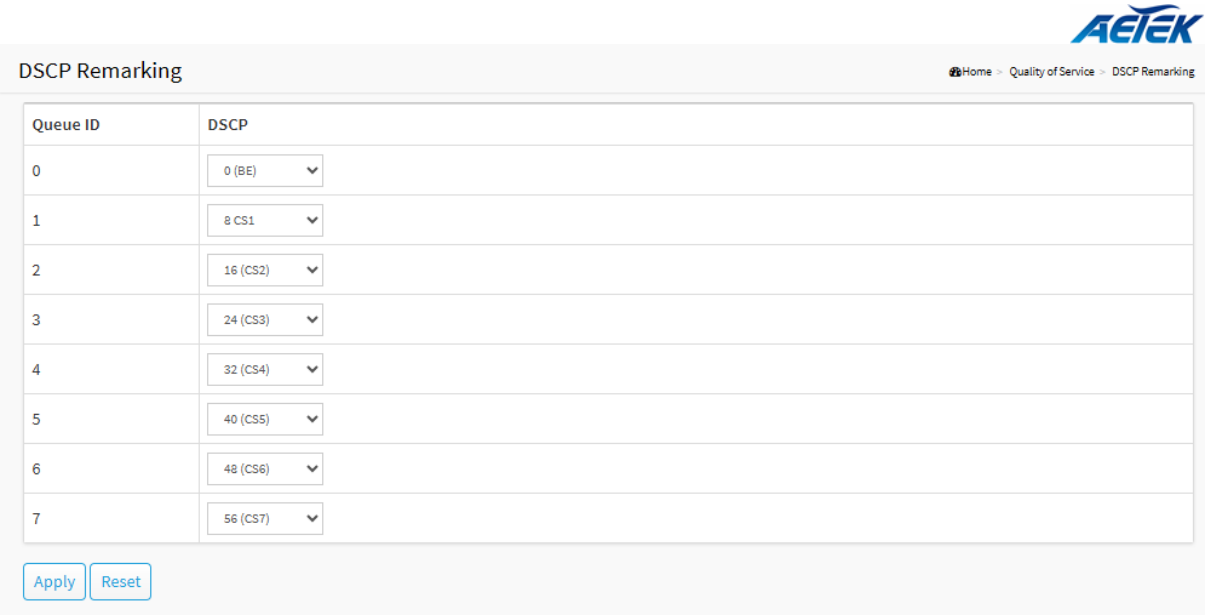


Figure 13-11: DSCP Remarking

Parameter Description:

- **Queue ID**

  The identifier of the egress queue, where Queue 7 represents the highest priority and Queue 0 the lowest.

- **IP Precedence**

  The DSCP priority value (0–63) assigned to each output queue for remarking egress traffic.

Chapter 14 Spanning Tree

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

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

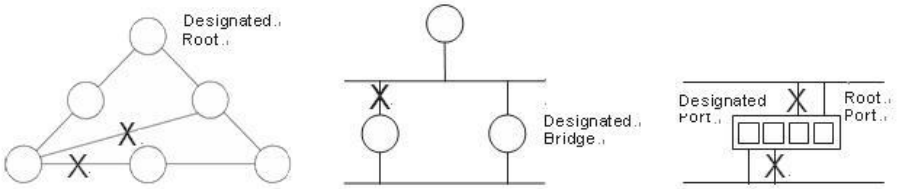


Figure 14-0: The Spanning Tree Protocol

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.

14-1 State

The section describes that you can select enable spanning tree protocol or not, and you can select what protocol version you want.

Web Interface

To configure the Spanning Tree Protocol version in the web interface:

1. Click Spanning Tree -> State.
2. To enable/disable the Spanning Tree Protocol.
3. Select the Spanning Tree Protocol version.
4. Click Apply.

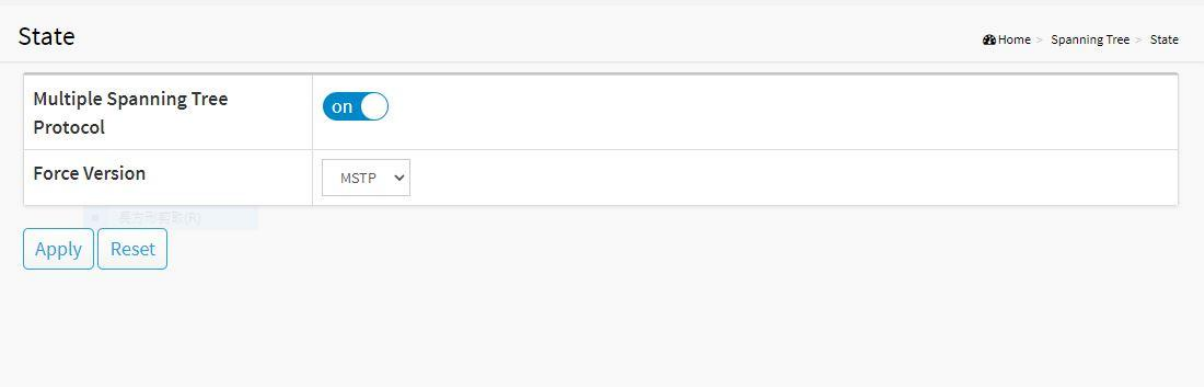


Figure 14-1: State

Parameter Description:

- **Multiple Spanning Tree Protocol**

  To enable/disable spanning tree protocol.

- **Force Version**

  The Spanning Tree protocol version, including STP, RSTP and MSTP.

14-2 Region Configuration

The section describes how to configure the basic identification of a MSTP bridge. Bridges participating in a common MST region must have the same Region Name and Revision Level.

Web Interface

To configure the Region Config in the web interface:

1. Click Spanning Tree -> Region Configuration
2. Specify the Region Name and Revision Level.
3. Click Apply.

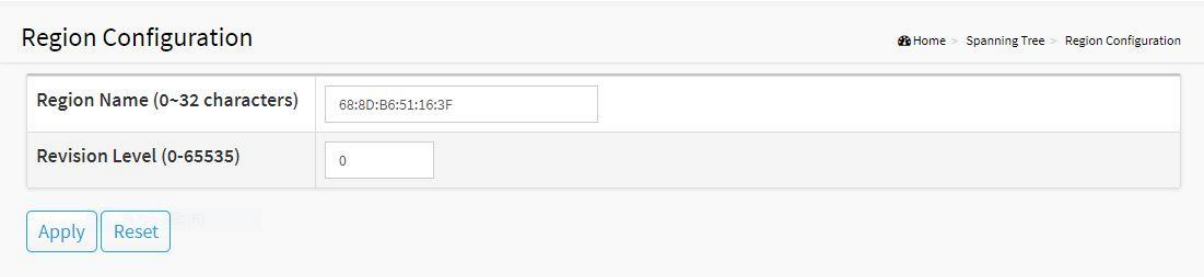


Figure 14-2: Region Config

Parameter Description:

- **Region Name**

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

- **Revision Level**

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

The section describes how to configure the basic identification of a MSTP bridge. Bridges participating in a common MST region must have the same Region Name and Revision Level.

The section providing an MST instance table which include information(vlan membership of a MSTI) of all spanning instances provisioned in the particular MST region which the bridge belongs to. Through this table, additional MSTP configuration data can be applied and MSTP status can be retrieved.

Web Interface

To configure the MSTP Instance in the web interface:

1. Click Spanning Tree -> Instance View.
2. Click Add VLAN.
3. Specify the Instance ID and Vlan Mapping.
4. Click Instance Config, Port Config, Instance Status and Port Status to see the detail.
5. If you want to cancel the setting, click Delete.

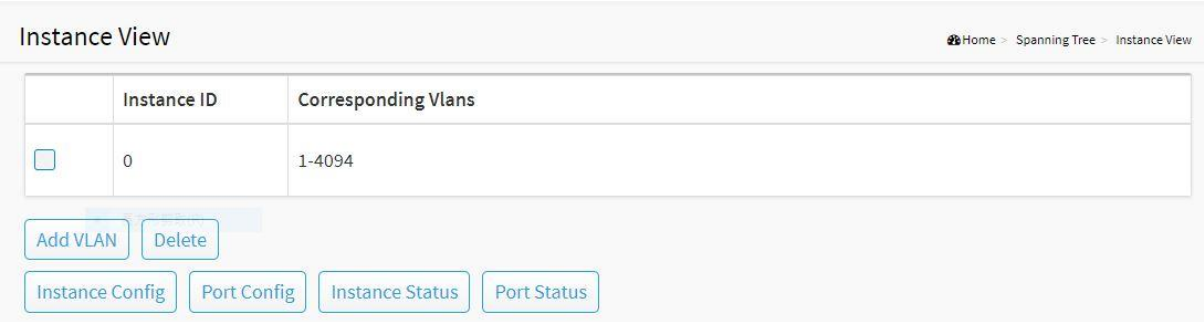


Figure 14-3: MSTP Instance Config

Parameter Description:

- **Instance ID**

  Every spanning tree instance need to have a unique instance ID within 1~15. Instance 0 (CIST) always exists and cannot be deleted. Additional spanning instances (MSTIs) can be added or deleted. At least one vlan must be provisioned for an MSTI to declare the need for the MSTI to be existent.

- **Corresponding VLANs**

  1-4094.

  Multiple vlans can belong to an MSTI. All vlans that are not provisioned through this will be automatically assigned to Instance 0(CIST).

- **Add VLAN[Button]**

  To add an MSTI and provide its vlan members for a specific MSTI, you can add up to 15.

- **Delete[Button]**

  To delete an MSTI.

- **Instance Config[Button]**

  To provision spanning tree performance parameters per instance.

- **Port Config[Button]**

  To provision spanning tree performance parameters per instance per port.

- **Instance Status[Button]**

  To show the status report of a particular spanning tree instance.

- **Port Status[Button]**

  To show the status report of all ports regarding a specific spanning tree instance.

Add VLAN

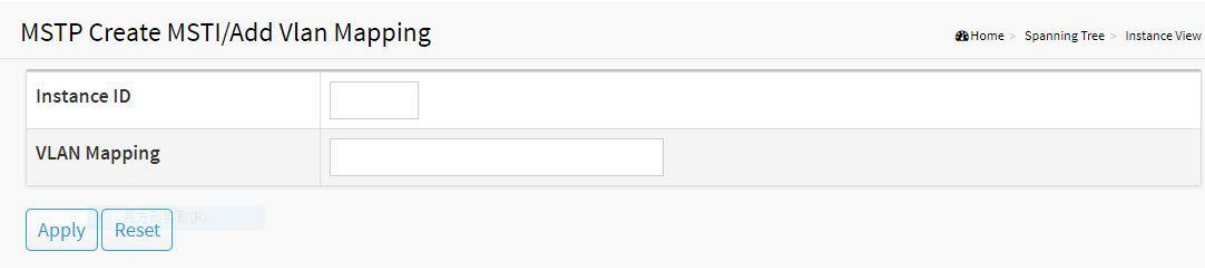


Figure 14-3: Add VLAN

Parameter Description:

- **Instance ID**

  The Range is 1-15

- **Vlan Mapping**

  The list of VLANs mapped to the MSTI. The VLANs can be given as a single (xx, xx must be 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.

Instance Config (ID=0)

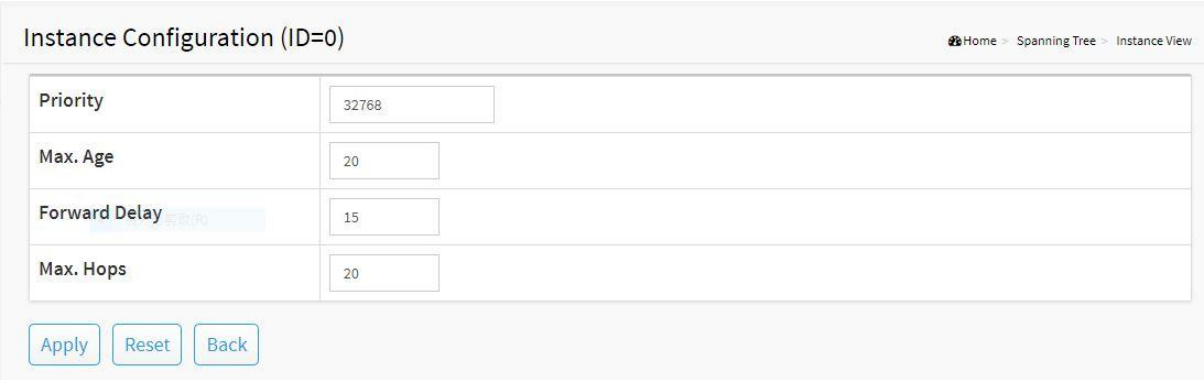


Figure 14-3: Instance Config (ID 0)

Parameter Description:

- **Priority**

  The priority parameter used in the CIST(Common and Internal Spanning Tree) connection.

  0 / 4096 / 8192 / 12288 / 16384 / 20480 / 24576 / 28672 / 32768 / 36864 / 40960 / 45056 / 49152 / 53248 / 57344 / 61440

- **MAX. Age**

  Range: 6-40 sec

  The max age timer controls the maximum length of time that passes before a bridge port saves its configuration BPDU information. This time is 20 sec by default, but you can tune the time to be between 6 and 40 sec.

- **Forward Delay**

  Range: 4-30 sec

  It is the same definition as in the RSTP protocol. The forward delay is the time that is spent in the listening and learning state. This time is equal to 15 sec by default, but you can tune the time to be between 4 and 30 sec.

- **MAX. Hops**

  Range: 1-40 sec

  It's a new parameter for the multiple spanning tree protocol. It is used in the internal spanning tree instances. "CIST Remaining Hops" or "MSTI Remaining Hops" in the Spanning tree protocol message would decreased by one when the message is propagated to the neighboring bridge. If the Remaining Hops in a message is zero, the message (BPDU) would be regarded as invalid. Max Hops is used to specify the initial value of the Remaining Hops for Regional Root Bridge (Either CIST Regional Root or MSTI Regional Root)

Port Config (ID=0)

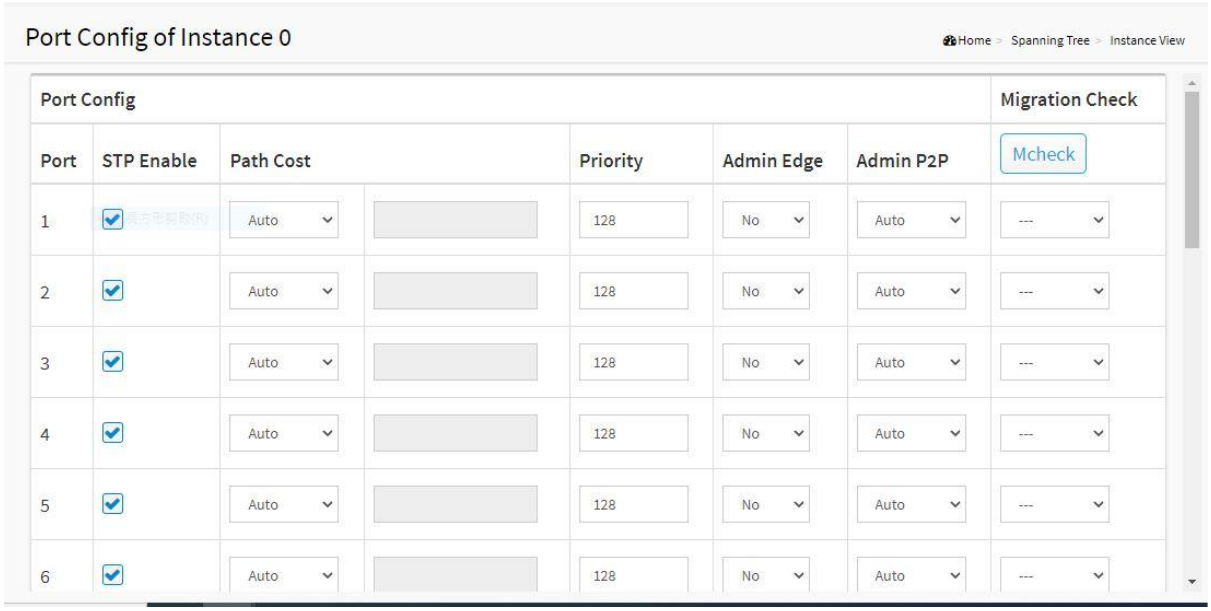


Figure 14-3: Port Config (ID 0)

Parameter Description:

- **Port**

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

- **Path Cost**

  Range: 0-200000000

  It is the same definition as in the RSTP specification. But in MSTP, this parameter can be respectively applied to ports of CIST and ports of any MSTI.

- **Priority**

  0 / 16 / 32 / 48 / 64 / 80 / 96 / 112 / 128 / 144 / 160 / 176 / 192 / 208 / 224 / 240

  It is the same definition as in the RSTP specification. But in MSTP, this parameter can be respectively applied to ports of CIST and ports of any MSTI.

- **Admin Edge**

  Yes / No

  It is the same definition as in the RSTP specification for the CIST ports.

- **Admin P2P**

  Auto / True / False

  It is the same definition as in the RSTP specification for the CIST ports.

- **MCheck**

  It is the same definition as in the RSTP specification for the CIST ports.

Instance Status (ID=0)

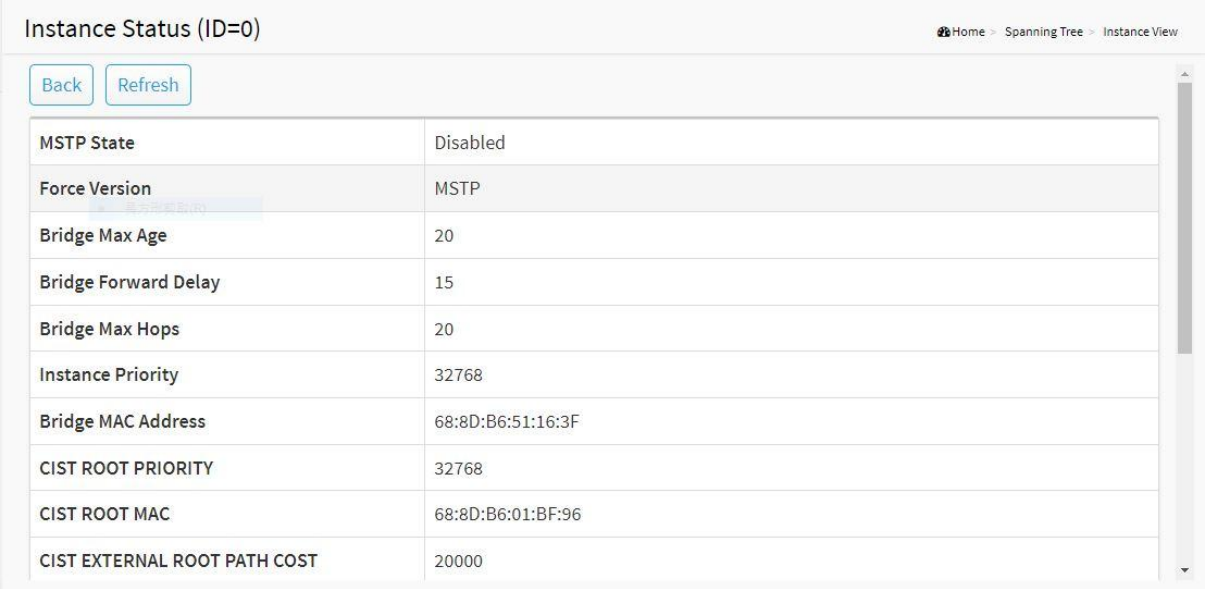


Figure 14-3: Instance Status (ID 0)

Parameter Description:

- **MSTP State**

  MSTP protocol is Enable or Disable.

- **Force Version**

  It shows the current spanning tree protocol version configured.

- **Bridge Max Age**

  It shows the Max Age setting of the bridge itself.

- **Bridge Forward Delay**

  It shows the Forward Delay setting of the bridge itself.

- **Bridge Max Hops**

  It shows the Max Hops setting of the bridge itself.

- **Instance Priority**

  Spanning tree priority value for a specific tree instance(CIST or MSTI)

- **Bridge Mac Address**

  The Mac Address of the bridge itself.

- **CIST ROOT PRIORITY**

  Spanning tree priority value of the CIST root bridge

- **CIST ROOT MAC**

  Mac Address of the CIST root bridge

- **CIST EXTERNAL ROOT PATH COST**

  Root path cost value from the point of view of the bridge's MST region.

- **CIST ROOT PORT ID**

  The port ID of the bridge's root port. In MSTP, peer port of a root port may reside in different MST region or in the same MST region. The first case indicates that the root port's owner is the CIST regional root bridge.

- **CIST REGIONAL ROOT PRIORITY**

  Spanning tree priority value of the CIST regional root bridge. Note that CIST Regional Root bridge is different from CIST Root bridge. One exception is that when a bridge belonging to an MST region happens to be the root bridge of the CST(Common Spanning Tree). An MST Region in the CST can be regarded as a common RSTP bridge. The IST(Internal Spanning Tree) and MSTIs are transparent to bridges outside this region.

- **CIST REGIONAL ROOT MAC**

  Mac Address of the CIST regional root bridge.

- **CIST INTERNAL ROOT PATH COST**

  Root path cost value from the point of view of the bridges inside the IST.

- **CIST CURRENT MAX AGE**

  Max Age of the CIST Root bridge.

- **CIST CURRENT FORWARD DELAY**

  Forward Delay of the CIST Root bridge.

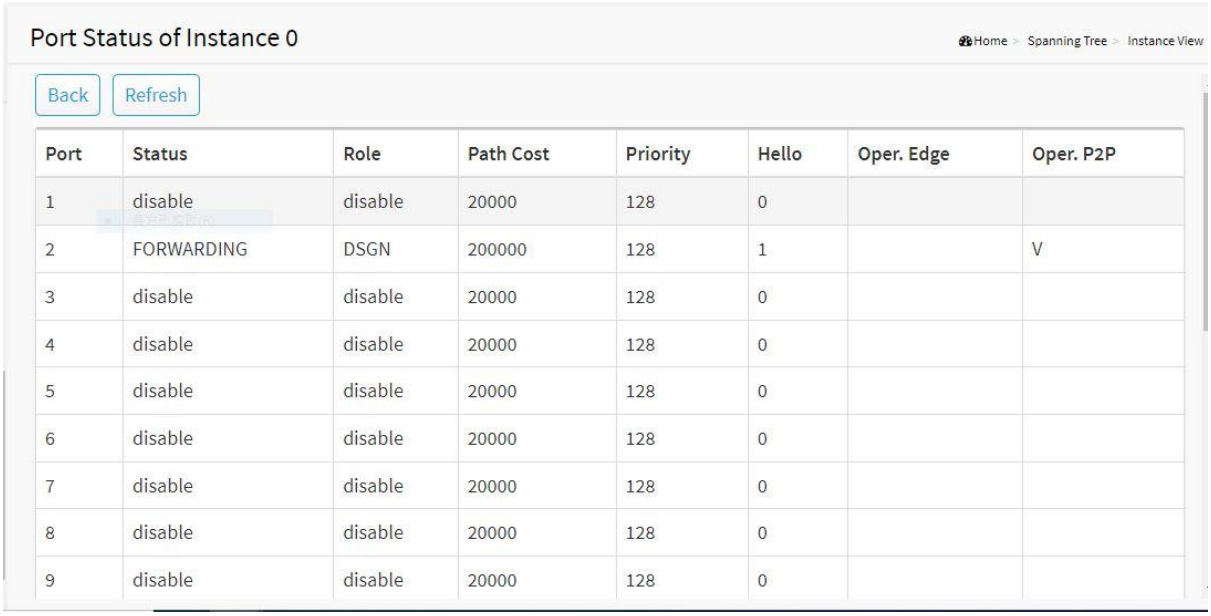
- **TIME SINCE LAST TOPOLOGY CHANGE (SECs)**

  The elapsed time in seconds since the most recent topology change was detected for this STP instance; resets to 0 when a new change occurs.

- **TOPOLOGY CHANGE COUNT (SECs)**

  The time spent in seconds from topology change start to STP convergence; resets to 0 when the event ends.

Port Status (ID=0)



Port	Status	Role	Path Cost	Priority	Hello	Oper. Edge	Oper. P2P
1	disable	disable	20000	128	0		
2	FORWARDING	DSGN	200000	128	1		V
3	disable	disable	20000	128	0		
4	disable	disable	20000	128	0		
5	disable	disable	20000	128	0		
6	disable	disable	20000	128	0		
7	disable	disable	20000	128	0		
8	disable	disable	20000	128	0		
9	disable	disable	20000	128	0		

Figure 14-3: Port Status (ID 0)

Parameter Description:

- **Port No**

  The port number to which the configuration applies.

- **Status**

  The forwarding status. Same definition as of the RSTP specification.

  Possible values are “FORWARDING”, “LEARNING”, “DISCARDING”

- **Role**

  The role that a port plays in the spanning tree topology.

  Possible values are “disable”(disable port) , ”alternate”(alternate port) , “backup”(backup port) , “ROOT”(root port) , “DSGN”(designated port) , “MSTR”(master port). The last 3 are possible port roles for a port to transit to FORWARDING state

- **Path Cost**

  Display currently resolved port path cost value for each port in a particular spanning tree instance.

- **Priority**

  Display port priority value for each port in a particular spanning tree instance.

- **Hello**

  Per port Hello Time display. It takes the following form:

  Current Hello Time/Hello Time Setting

- **Oper. Edge**

  Whether or not a port is an Edge Port in reality.

- **Oper. P2P**

  Whether or not a port is a Point-to-Point Port in reality.

Chapter 15 ERPS

The Switch ERPS (Ethernet Ring Protection Switching) page configures ITU-T G.8032 ring protection on the switch to prevent Layer-2 loops and ensure rapid recovery in a ring topology. ERPS blocks a Ring Protection Link during normal operation and uses R-APS control messages to quickly unblock or restore paths when a failure occurs. Instances can be bound to VLANs, and roles such as RPL Owner and RPL Neighbor are configured per instance on the switch.

16-1 Global Setting

Web Interface

To display MAC Address Table Configuration page, click System -> ERPS -> Global Setting

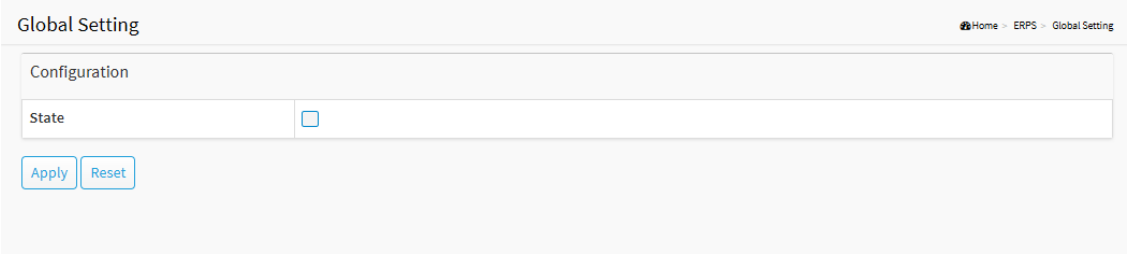


Figure 15-1: ERPS Global Setting

Parameter Description:

- **State**

  To enable/disable the ERPS function.

15-2 VLAN Group Setting

This page is used to configure ERPS VLAN Group settings on the switch. Define a VLAN group name and specify the allowed VLANs for the group.

Web Interface

To configure the VLAN Group Setting in the web interface:

1. Click System -> ERPS -> VLAN Group Setting.
2. Click Add New Entry.
3. Enter the VLAN configuration.
4. Click Apply.

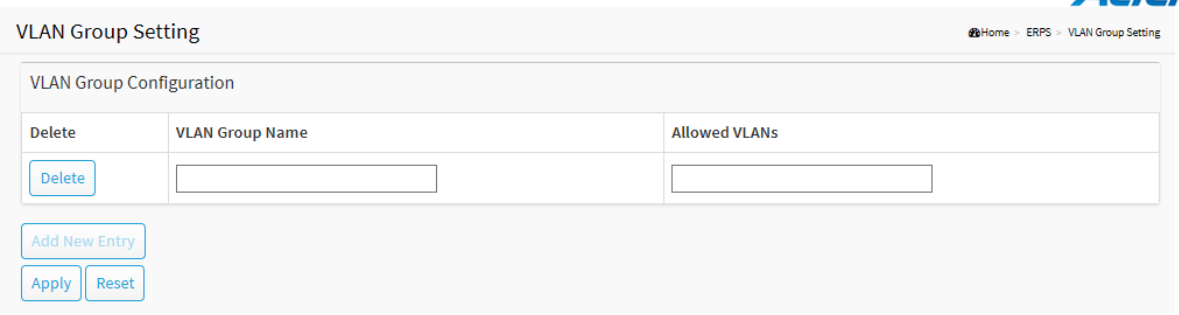


Figure 15-2: VLAN Group Setting

Parameter Description:

- **VLAN Group Name**

  The name assigned to the VLAN group.

- **Allowed VLANs**

  The VLAN IDs permitted within the VLAN group.

15-3 Ring Setting

The Ring Setting page is used to configure ERPS Ring parameters on the switch.

Web Interface

To configure the Ring Setting in the web interface:

1. Click System -> ERPS -> Ring Setting.
2. Click Add New Entry.
3. Enter the VLAN configuration.
4. Click Apply.

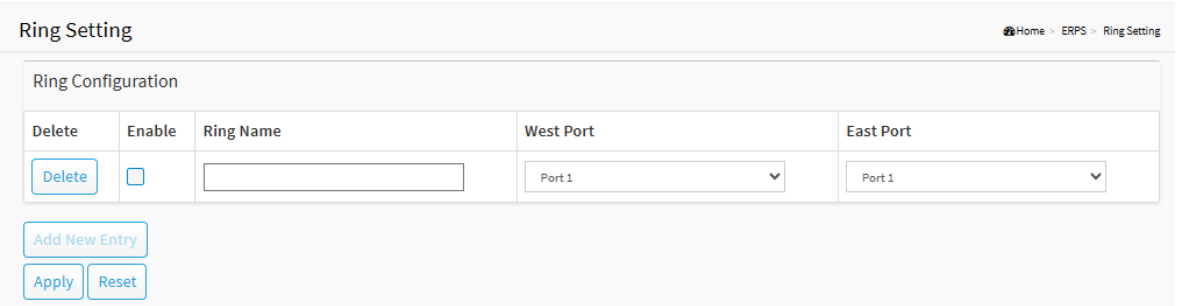


Figure 15-3: Ring Setting

Parameter Description:

- **Enable**

  To enable/disable the administrative state of the ring.

- **Ring Name**

  The name of the ERPS ring.

- **West Port**

  The port designated as the West side of the ring.

- **East Port**

  The port designated as the East side of the ring.

15-4 Instance Setting

The Instance Setting page is used to configure ERPS instance parameters on the switch. It allows enabling or disabling an instance, defining the instance name and ID, specifying the node ID, binding the instance to a physical ring, and setting parameters such as control VLAN, inclusion VLAN, MEG level, node type, and timers.

Web Interface

To configure the Instance Setting in the web interface:

1. Click System -> ERPS -> Instance Setting.
2. Enter the parameters you want to configure.
3. Click Apply.

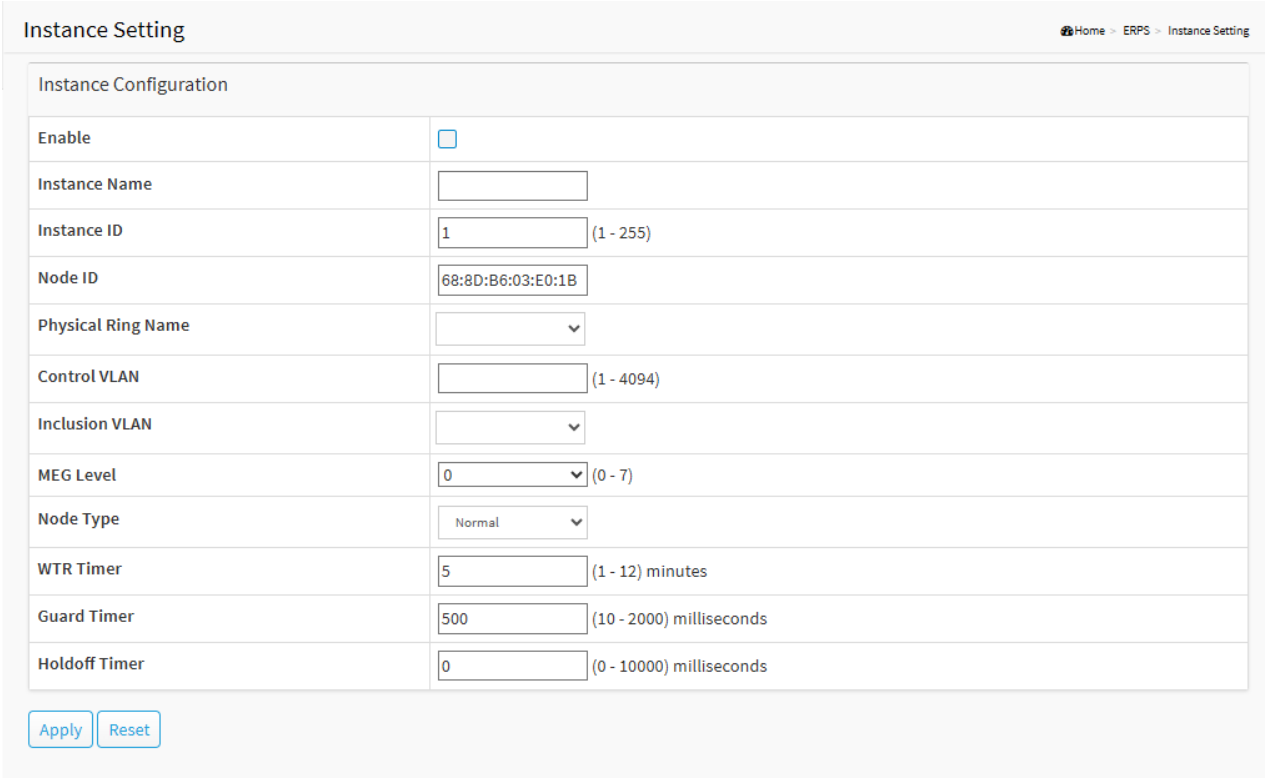


Figure 15-4: Instance Setting

Parameter Description:

- **Enable**

  To enable/disable the administrative state of the ERPS instance.

- **Instance Name**

  The name of the ERPS instance.

- **Instance ID**

  The numeric identifier of the ERPS instance.

- **Node ID**

  The node identifier within the ERPS ring.

- **Physical Ring Name**

  The name of the physical ring associated with the instance.

- **Control VLAN**

  The VLAN ID used for ERPS control messages.

- **Inclusion VLAN**

  The VLANs included in this ERPS instance.

- **MEG Level**

  The Maintenance Entity Group (MEG) level used for OAM monitoring.

- **Node Type**

  The operating role of the node.

- **WTR Timer**

  Wait-to-Restore timer value.

- **Guard Timer**

  Guard timer value to prevent false recovery.

- **Holdoff Timer**

  Holdoff timer value before declaring a failure.

15-5 Instance Information

The page shows the ERPS Instance Information including the operational status, node role, control VLAN, and associated ring details for each configured instance on the switch.

Web Interface

To configure the Instance Setting in the web interface:

1. Click System -> ERPS -> Instance Information.

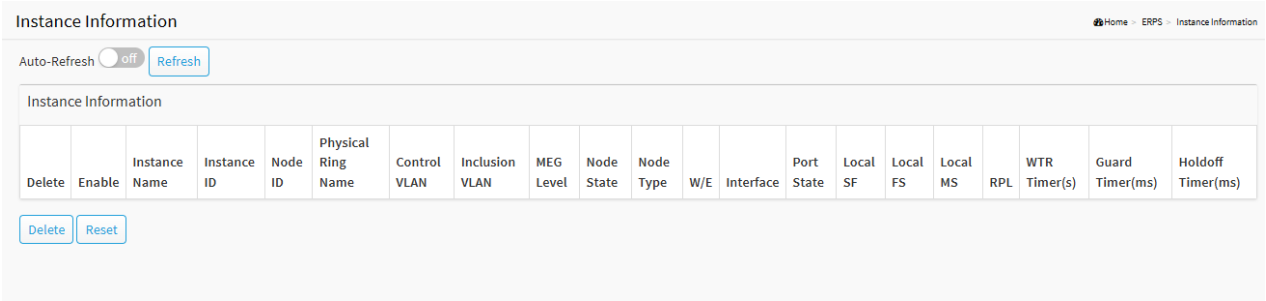


Figure 15-5: Instance Information

Parameter Description:

- **Node State**

  The current operational state of the ERPS instance.

- **W/E**

  Indicates the port direction in the ERPS ring — W (West) or E (East).

- **Interface**

  The physical interface participating in the ERPS ring.

- **Port State**

  The current forwarding status of the port.

- **Local SF**

  The local Signal Failure (SF) condition.

- **Local FS**

  The local Forced Switch (FS) condition.

- **Local MS**

  The local Manual Switch (MS) condition.

- **RPL**

  Indicates whether the port functions as the Ring Protection Link in the ERPS ring.

Chapter 16 MAC Address Table

The MAC Address Table page displays all MAC address entries on the switch, including static addresses manually configured by the administrator and dynamic addresses automatically learned from incoming frames. The switch uses this table to determine the destination port for each frame based on its destination MAC (DMAC) address.

16-1 Configuration

Web Interface

To display MAC Address Table Configuration page, click System -> MAC Address Table -> Configuration

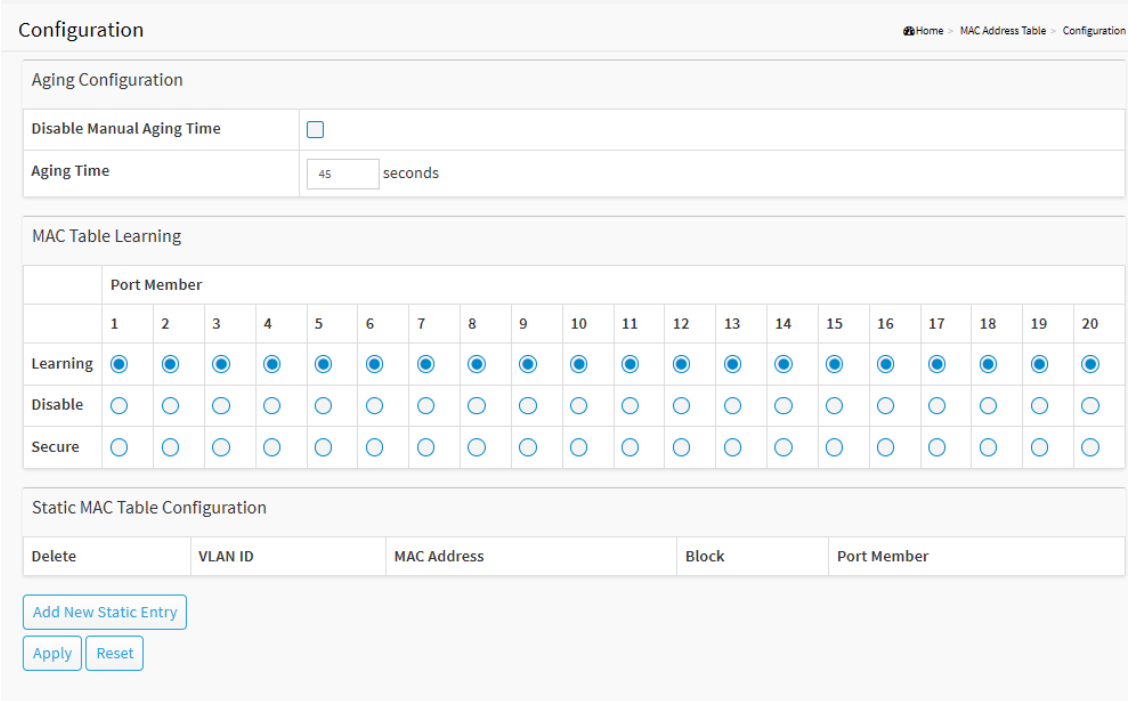


Figure 16-1: MAC Address Table Configuration

Parameter Description:

- **Disable Manual Aging Time**

  To enable/disable the Aging Time field; when disabled, the system uses the default global aging behavior for dynamic entries.

- **Aging Time**

  The MAC aging timer in seconds (10–630) for dynamic entries.

- **Learning**

  Automatic learning of unknown source MAC addresses.

- **Disable**

  No MAC learning is performed.

- **Secure**

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

- **VLAN ID**

  The VLAN identifier associated with the entry.

- **MAC Address**

  The MAC address associated with the entry.

- **Block**

  Blocks traffic for this MAC address when enabled.

- **Port Member**

  The member ports for this entry.

- **Add New Static Entry[Button]**

  To add a static MAC entry by specifying VLAN ID, MAC Address, and Port Members, then click Apply.

- **Apply[Button]**

  To save and apply the current changes.

- **Reset[Button]**

  To revert to the last saved values.

16-2 Information

Web Interface

To display MAC Address Table page, click System -> MAC Address Table -> Information

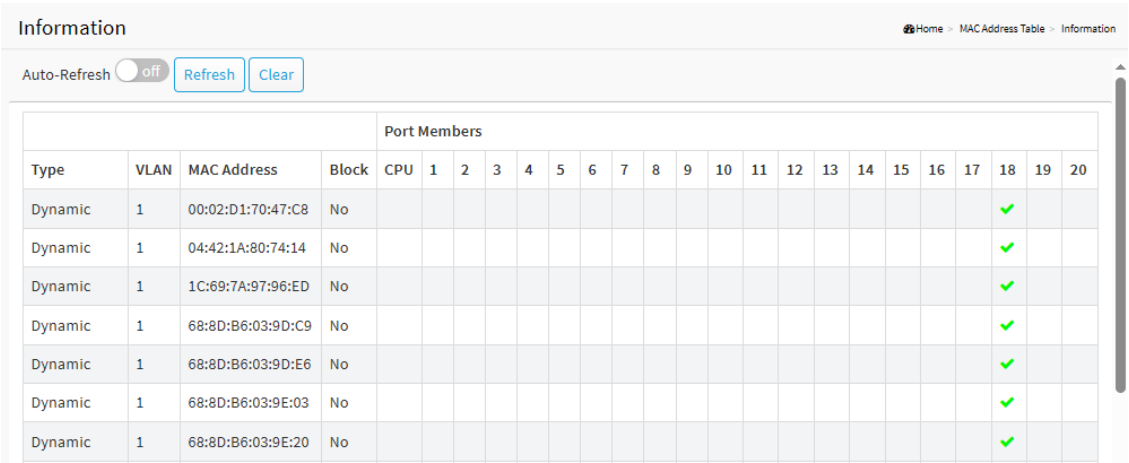


Figure 16-2: MAC Address Table

Parameter Description:

- **Type**

  Type of MAC address

  · Management: DUT's base MAC address for management purpose

- SecureStatic: Manually configured by administrator for port security function.
- SecureDynamic: Dynamically learned by hardware associated with port security. It will be aged out.
- Dynamic: Dynamically learned by hardware, and it will be aged out.

- **VLAN**

  VLAN ID of the MAC address.

- **MAC Address**

  MAC address.

- **Block**

  Whether the MAC address is blocked.

- **Port**

  Type of Port

  - CPU: DUT's CPU port for management purpose
  - Other: Normal switch port

- **Refresh[Button]**

  To retrieve latest MAC address entries shown on this page.

- **Clear[Button]**

  To clear all dynamic entries.

Chapter 17 DHCP

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

17-1 DHCP Server

This page is used to configure the DHCP Server, including State, Start IP/End IP addresses and Client Lease Time. DHCP Server will allocate these IP addresses to DHCP clients. And deliver configuration parameters to DHCP clients.

Web Interface

To configure the DHCP Server in the web interface:

1. Click DHCP -> DHCP Server.
2. Specify the parameter you want to configure.
3. Click Apply.

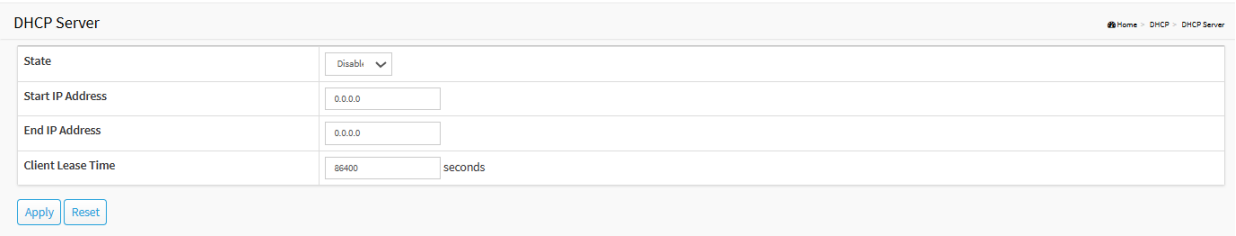


Figure 17-1: DHCP Server

Parameter description:

- **State**

  To enable/disable DHCP Server function.

- **Start IP Address and End IP Address**

  Define the IP range. The Start IP Address must be smaller than or equal to the End IP Address.

- **Client Lease Time**

  Range: 1 - 14400000, 0: infinite

  Display the lease time of the pool.

Chapter 18 Diagnostics

This chapter provides a set of basic system diagnosis, including Mirroring, Ping and LAN Cable Diagnostics.

18-1 Mirroring

This page is used to configure the ports' mirror function. 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 is to monitor 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 port mirroring in the web interface:

1. Click Diagnostics -> Mirroring.
2. Click the Enable checkbox.
3. Select Monitor Destination Port. (Mirror Port)
4. Specify the state of Monitor Source Port.
5. Click Apply.

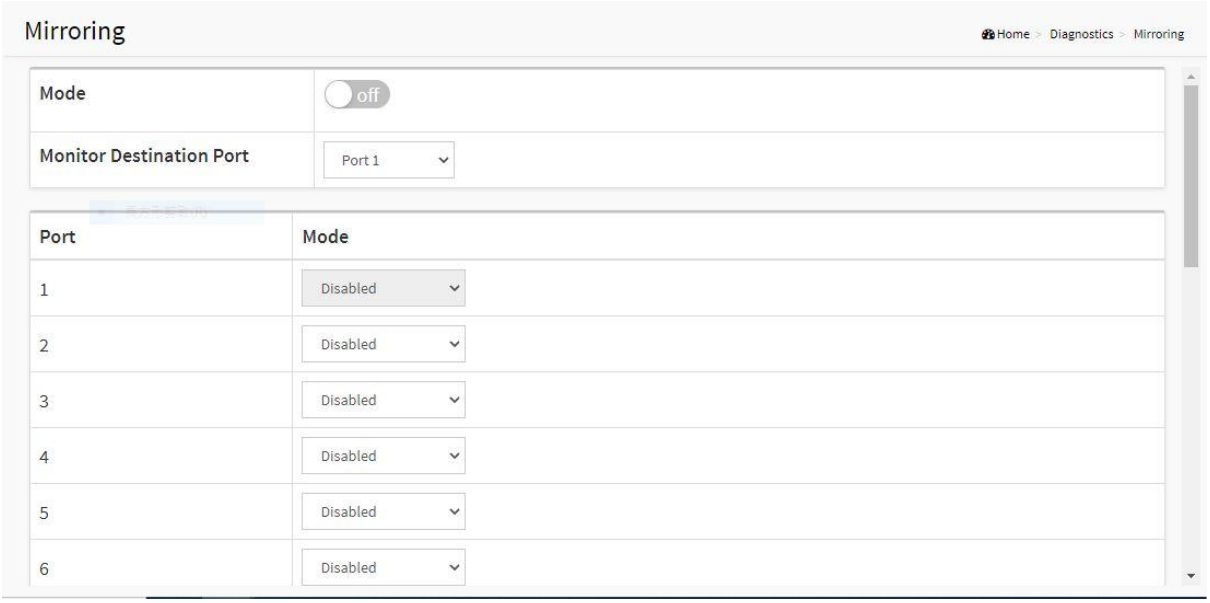


Figure 18-1: Mirroring

Parameter Description:

- **Mode**

  To enable/disable port mirroring function.

- **Monitor Destination Port**

  Port to output the mirrored traffic. Also known as the mirror port. Frames from ports that have either source (rx) or destination (tx) mirroring enabled are mirrored on this port.

- **Monitor Source Port State**

  To enable/disable source port mirroring function:

  - Disabled: neither frames transmitted nor frames received are mirrored.

  - Enabled: Frames received and frames transmitted are mirrored on the mirror port.

18-2 Ping

This section allows you to issue ICMP Echo packets to troubleshoot Ipv4 connectivity issues.

Web Interface

To configure a PING in the web interface:

1. Click Diagnostics -> Ping.
2. Specify IP Address and Ping Count.
3. Click Ping to start.
4. Click Stop to stop.

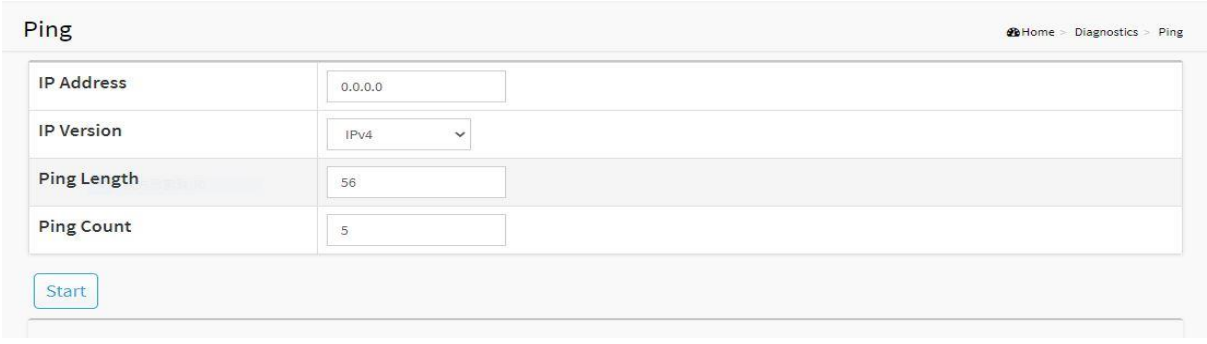


Figure 18-2: Ping

Parameter Description:

- **IP Address**

  To specify the target IP Address of the Ping.

- **IP Version**

  To select the IP Version.

- **Ping Length**

  The payload size of the ICMP packet. Values range from 1 bytes to 1452 bytes.

- **Ping Count**
  The count of the ICMP packet. Values range from 1 time to 60 times.

Chapter 19 NTS Server Agent

This page is used to configure the connection to the NTS Server and define the Sync Configuration Behavior. Use this page to set the NTS Server address, License Key, Sync Interval, and Sync Configuration Behavior.

19-1 Configuration

Web Interface

To configure port mirroring in the web interface:

1. Click NTS Server Agent -> Configuration.
2. Enter the NTS Server IP address.
3. Enter the Sync Interval.
4. Select the Sync Configuration options.
5. Click Apply.

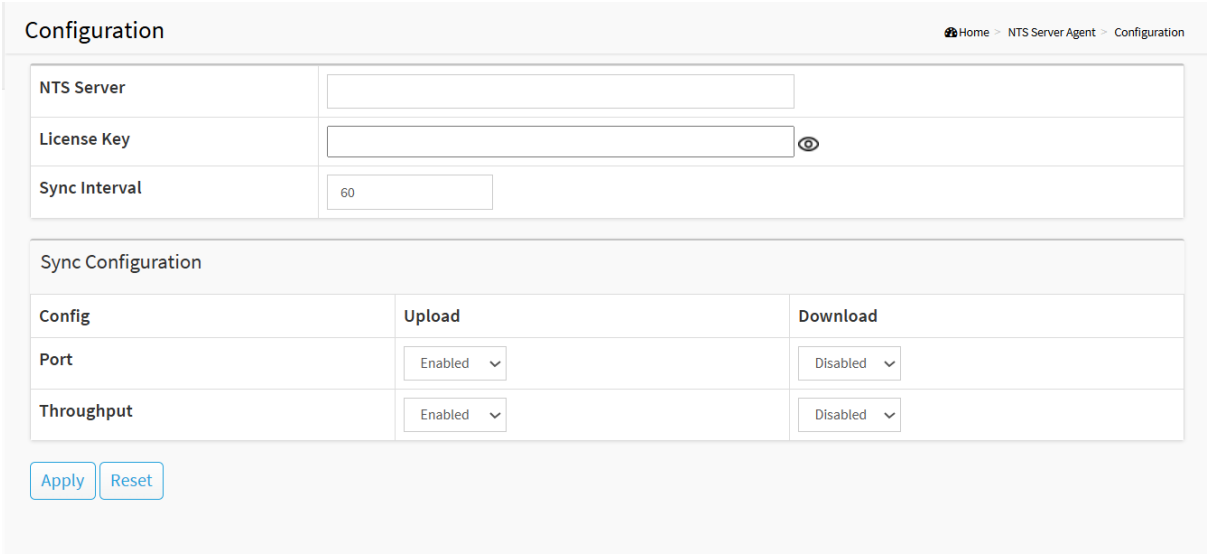


Figure 19-1: NTS Server Agent Configuration

Parameter Description:

- **NTS Server**

  The NTS server address (IPv4 or domain name).

- **License Key**

  The license key is issued by the NTS server.

- **Sync Interval**

The configuration synchronization interval in seconds; the switch uses this single interval for all sync tasks.

- **Sync Configuration**

  Determines whether configuration data is uploaded to or downloaded from the NTS server:

  - Upload Config: When enabled, the switch uploads its configuration to the NTS server; when disabled, no upload occurs.

  - Download Config: When enabled, the switch downloads configuration from the NTS server; when disabled, no download occurs.

Chapter 20 Maintenance

This chapter provides the maintenance of the system. These includes Configuration Import/Export, Restart Device, Reset to default and Firmware Upgrade.

20-1 Configuration

20-1-1 Backup / Restore

This section describes how to import or export the Switch Configuration for maintenance needs. Any current configuration files will be exported as text format, and the configuration files on the switch can be backed up and saved on the station running the web browser.

It is possible to transfer any of the files on the switch to the web browser. Select the configuration file for uploading, as the file must be backup before uploading.

Web Interface

To import or export the current device's configuration in the web interface:

1. Click Maintenance -> Configuration -> Backup / Restore
2. For upload configuration, select the file you want to backup and restore.
3. For backup, click Backup to save the configuration file.

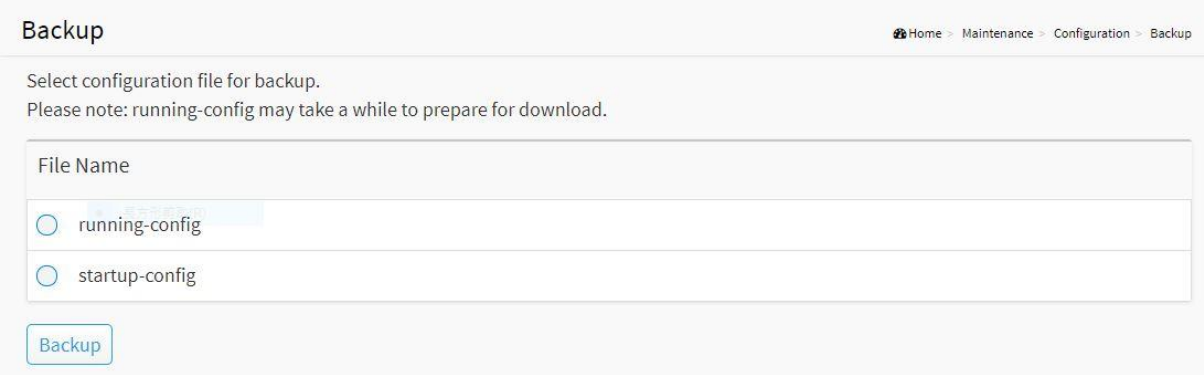


Figure 20-1-1: Backup / Restore

Parameter Description:

- **Backup[Button]**

  Set port enable/disable.

- **Restore[Button]**

  Set port enable/disable.

20-2 Restart Device

This section describes how to restart the device for any maintenance needs. Any configuration files or scripts that you saved in the switch should still be available afterwards.

Web Interface

To Restart Device in the web interface:

1. Click Maintenance -> Restart Device.
2. Click Yes.

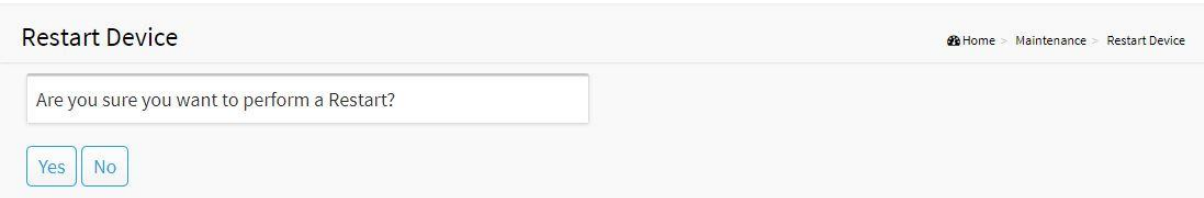


Figure 20-2: Restart Device

Parameter Description:

- **Yes[Button]**

  To restart device

20-3 Reset Default

This section describes how to restore the Switch configuration to factory default value.

Web Interface

To restore to factory default value in the web interface:

1. Click Maintenance -> Reset Default.
2. Click Yes.

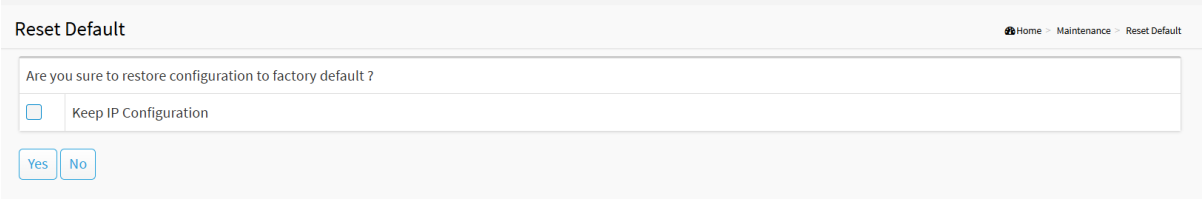


Figure 20-3: Reset Default

Parameter Description:

- **Yes[Button]**

  To reset the device to factory default value.

20-4 Firmware Upgrade

To display firmware upgrade page, you can click 'Maintenance -> Firmware Upgrade'. This page allows user to upgrade firmware image through HTTP.

Web Interface

To update firmware of the device in the web interface:

1. Click Maintenance -> Firmware -> Firmware Upgrade.
2. Choose the firmware you want to upgrade.
3. Click Upload.

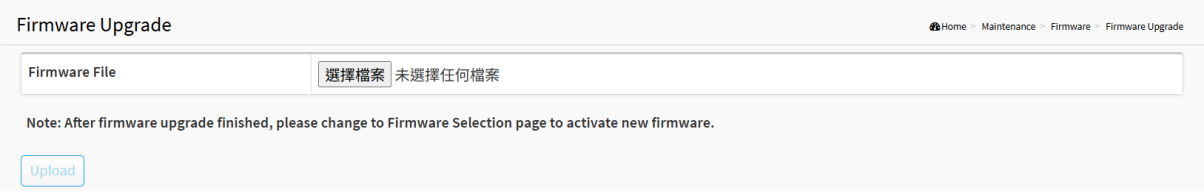


Figure 20-4: Firmware Upgrade

Parameter Description:

- **Firmware File**
  The firmware version which currently runs on this device
- **Upload[Button]**

  Click to perform firmware upgrading.

  Don't turn off the device during the firmware upgrading.

20-5 Firmware Selection

To display firmware upgrade page, you can click 'Maintenance -> Firmware -> Firmware Selection'. This page allows user to select firmware image through UI.

Web Interface

To update firmware of the device in the web interface:

1. Click Maintenance -> Firmware -> Firmware Selection.
2. Choose the firmware version you want to use.
3. Click Activate.

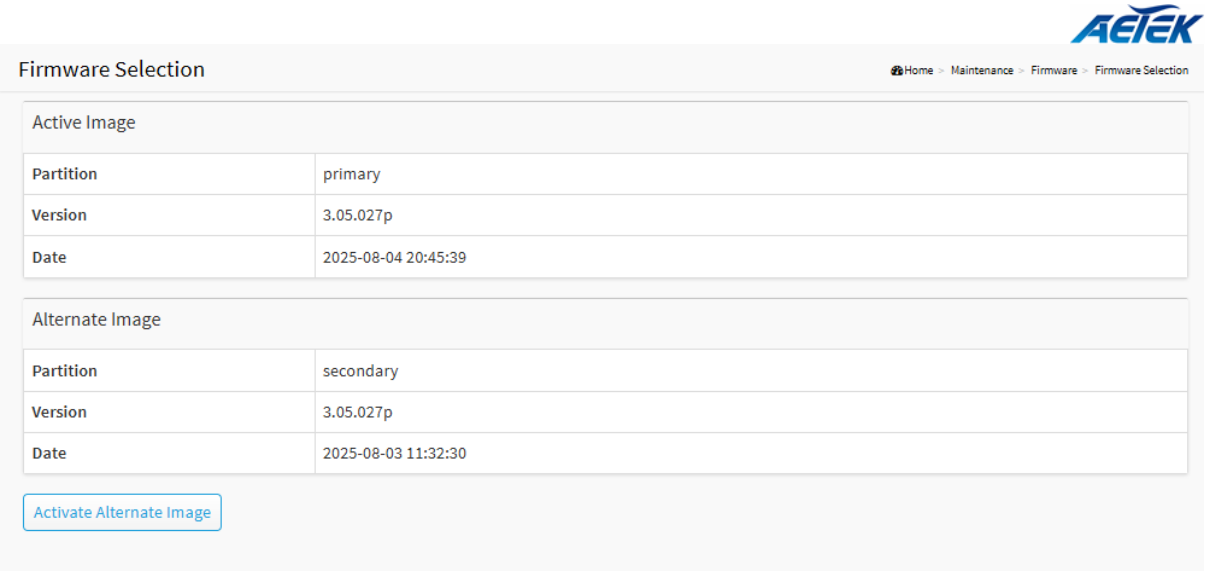


Figure 20-5: Firmware Upgrade

Parameter Description:

- **Activate Alternate Image[Button]**
  The firmware version which would like to activate on this device.