H51-044-30-150
H51-084-30-250
H51-044-90-250

Outdoor L2 PoE Switches

GUI User's Manual

Copyright© AETEK Inc. 2021 | All rights reserved. All brand and product names are trademarks or registered trademarks of their respective companies

About This Manual

Copyright

Copyright © AETEK Inc. 2021 | All rights reserved.

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

.

Purpose

This GUI user guide gives specific information on how to operate and use the management functions of the D51 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.

Table of Contents

.....II

ABOUT THIS MANUAL II

.....1

INTRODUCTION 1

CHAPTER 1 OPERATION OF WEB-BASED MANAGEMENT 2

CHAPTER 2 FIRST TIME WIZARD 3

CHAPTER 3 SYSTEM 6

3-1 SYSTEM INFORMATION 6
3-2 SYSTEM TIME 8
3-3 IP ADDRESS SETTINGS 9
3-4 ACCOUNT / PASSWORD 10
3-5 SNMP 12
3-5.1 Configuration *12*
3-5.2 SNMPv3 .....*14*
3-6 SYSLOG 23
3-6.1 SYSLOG CONFIGURATION 23
3-6.2 View Log *24*
3-7 DIGITAL I/O 25
3-7.1 DI TRIGGER DO 25

CHAPTER 4 PORT 27

4-1 PORT SETTING 27
4-2 LINK AGGREGATION 28
4-3 ENERGY EFFICIENT ETHERNET 29
4-4 JUMBO FRAME 29
4-5 PORT STATISTICS 30
4-6 SFP PORT INFORMATION 31

CHAPTER 5 POE MANAGEMENT 33

5-1 POE CONFIGURATION 33
5-2 POE STATUS 34
5-3 POE POWER DELAY 35
5-4 POE AUTO CHECKING 36
5-5 POE SCHEDULING PROFILE 37

CHAPTER 6 VLAN 39

6-1 VLAN CONFIGURATION 39
6-2 VLAN MEMBERSHIP 40

CHAPTER 7 IGMP SNOOPING 41

7-1 PROPERTY 41
7-2 GROUP ADDRESS 42

CHAPTER 8 LLDP 43

8-1 LLDP CONFIGURATION 43
8-2 LLDP NEIGHBOR 45

CHAPTER 9 LOOP PREVENTION 46

9-1 PROPERTY 46

9-2 STATUS 46

CHAPTER 10 SECURITY 48

10-1 MANAGEMENT 48
10-2 PORT ISOLATION 48
10-3 PORT SECURITY 49
10-4 STORM CONTROL 50
10-5 DOS ATTACK PREVENTION 51

CHAPTER 11 QUALITY OF SERVICE 53

11-1 GLOBAL SETTINGS 53
11-2 PORT SETTINGS 54
11-3 PORT POLICING 55
11-4 PORT SHAPER 56
11-5 PORT SCHEDULER 56
11-6 COS/802.1P MAPPING 57
11-7 COS/802.1P REMARKING 58

CHAPTER 12 SPANNING TREE 60

12-1 STATE 60
12-2 REGION CONFIG 61
12-3 INSTANCE VIEW 62

CHAPTER 13 MAC ADDRESS TABLE 68

CHAPTER 14 DHCP 70

14-1 DHCP SERVER 70

CHAPTER 15 DIAGNOSTICS 71

15-1 MIRRORING 71
15-2 PING 72
15-3 LAN CABLE DIAGNOSTICS 73

CHAPTER 16 MAINTENANCE 74

16-1 CONFIGURATION 74
16-1.1 BACKUP / RESTORE 74
16-2 RESTART DEVICE 75
16-3 RESET DEFAULT 76
16-4 FIRMWARE UPGRADE 77
16-5 FIRMWARE SELECTION 77

INTRODUCTION

Overview

In this User Guide, it will not only tell you how to install and connect your network system but configure and monitor the H51 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 H51 Series are Outdoor L2 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.

H51 Series is Outdoor L2 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
- **PoE Management**
  - PoE Per Port On/OFF Control
  - PoE Status
  - PoE Power Delay
  - PoE Auto Checking
  - PoE Scheduling Profile

Chapter 1 Operation of Web-based Management

Initial Configuration

This chapter instructs you how to configure and manage the H51 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 H51 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 H51 Series have been finished configuring the interface, you can browse it. For instance, type 錯誤！超連結參照不正確。 in the 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 H51 Series will not give you a shortcut to username automatically. This looks inconvenient, but safer.

In the H51 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 Microsoft IE 6.0 above, Netscape V7.1 above or Firefox V1.00 above and have the resolution 1024x768. The switch supported neutral web browser interface

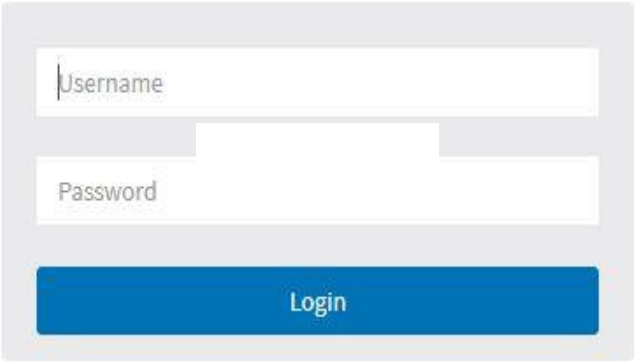


Figure 1: The login page

Chapter 2 FIRST TIME WIZARD

he 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.

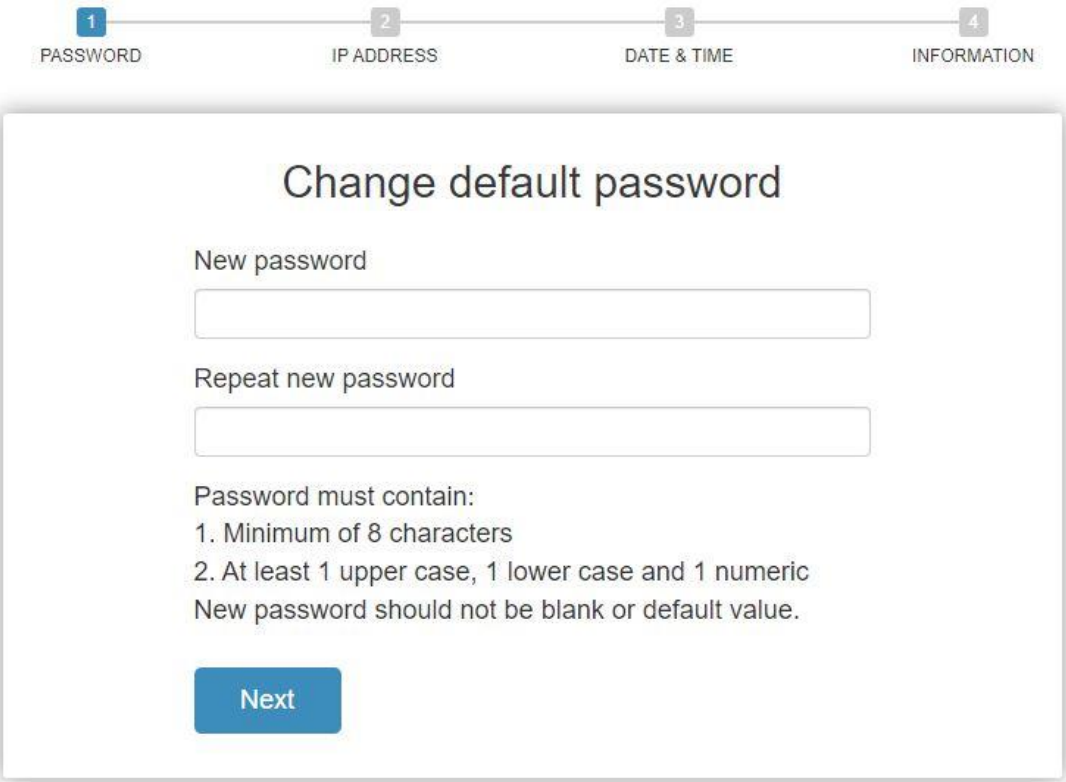


Figure 2: Change default password

Step2: Set IP address

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

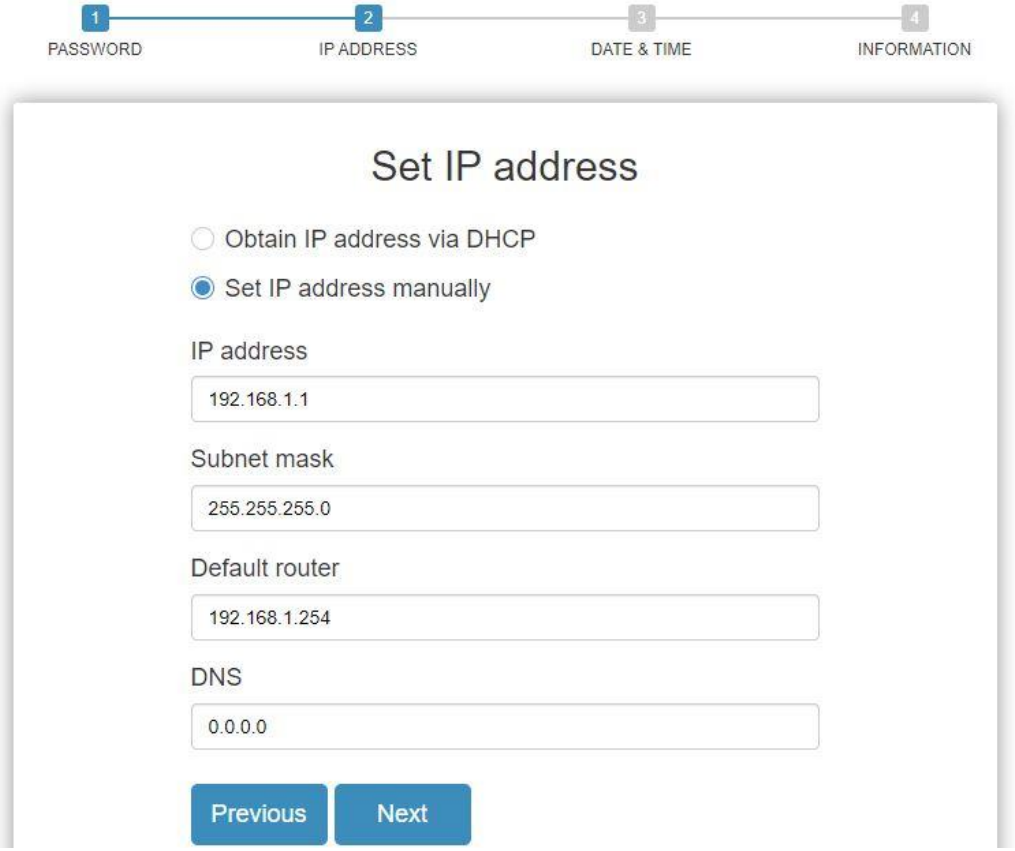


Figure 3: Set IP address

Step3: Set date and time

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

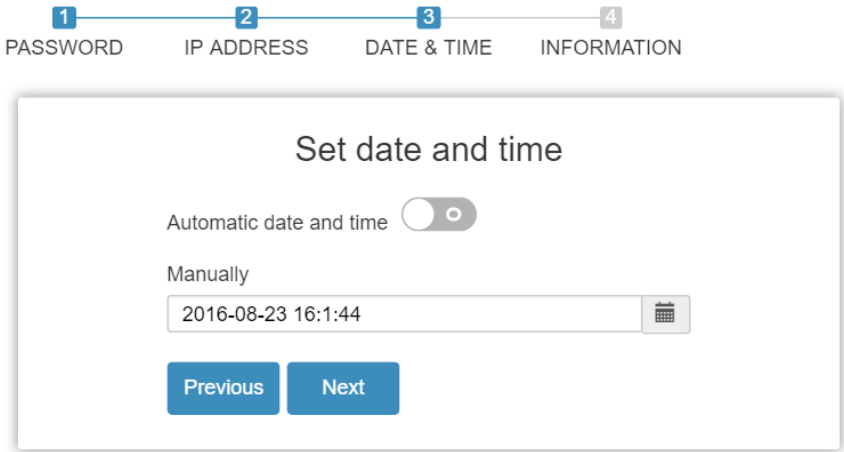


Figure 4: Set date and time

Step4: Set system information

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

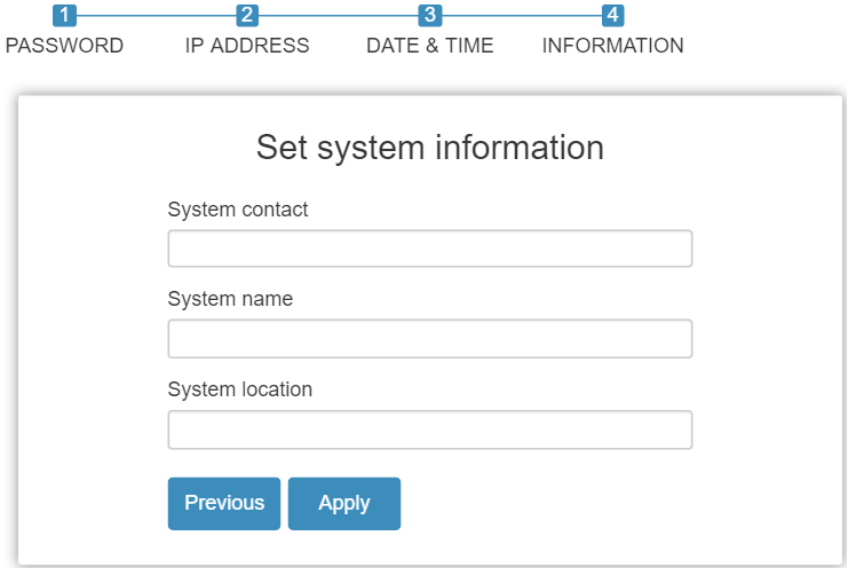


Figure 5: Set system information

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:

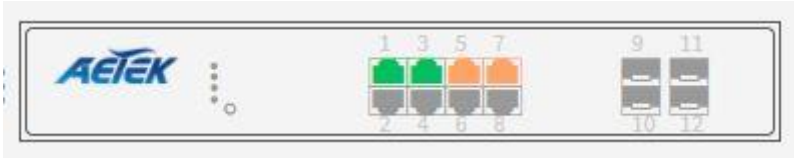


Figure 6: Port Information

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

- Orange circle: The LAN port is powered on and is connected with 10/100M linking speed powered device.
- Green circles: The LAN port is powered on and is connected with 1000M linking speed powered device
- Gray circles: 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.

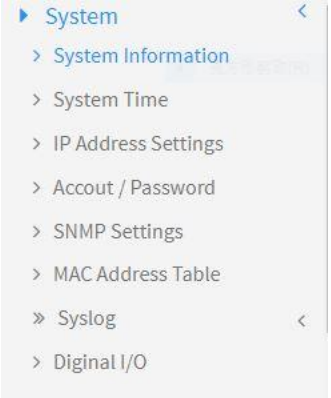


Figure 7: System

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.

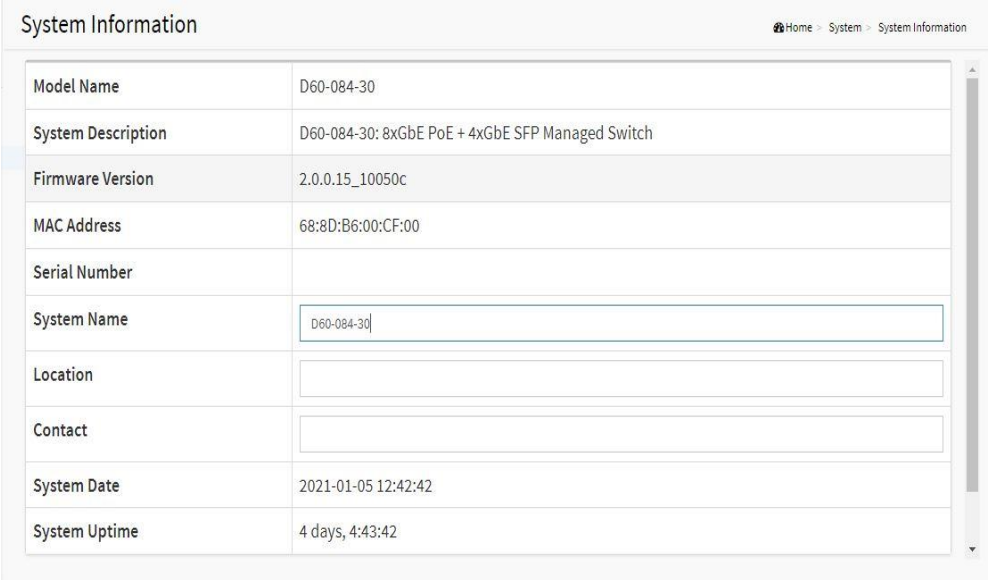


Figure 8: System Information

Parameter Description:

- **Description**

  Displays the system description.

- **Model Name**

  Displays the factory defined model name for identification purpose.

- **MAC Address**

  Base MAC address of the switch.

- **IP Address**

  The IP Address of this switch.

- **Subnet Mask**

  The Subnet Mask IP Address of this switch.

- **Default Gateway**

  The Gateway IP Address of this switch.

- **Firmware Version**

  The software version of this switch.

- **System Time**

  The current (GMT) system time and date. The system time is obtained through the Timing server running on the switch, if any.

- **Uptime**

  The period of time the device has been operated.

- **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.

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.

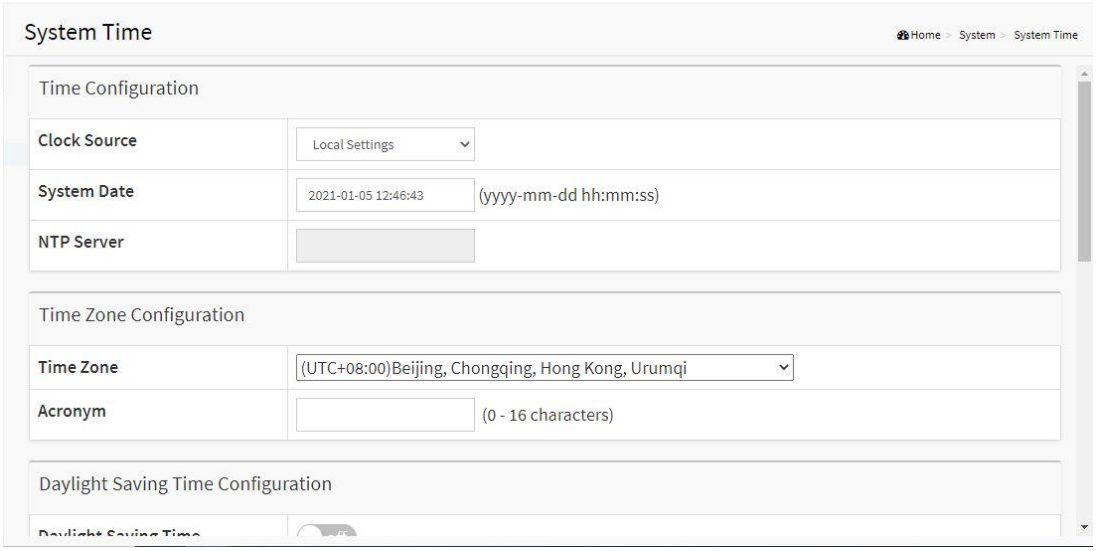


Figure 9: System Time

Parameter Description:

- **Time Configuration**

  You can input Year, Month, Day, Hour, Minute and Second manually, or by clicking "Copy Computer Time" button to get time through PC, 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.

Web Interface

To configure an IP Settings in the web interface:

1. Click System -> IP Address 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.

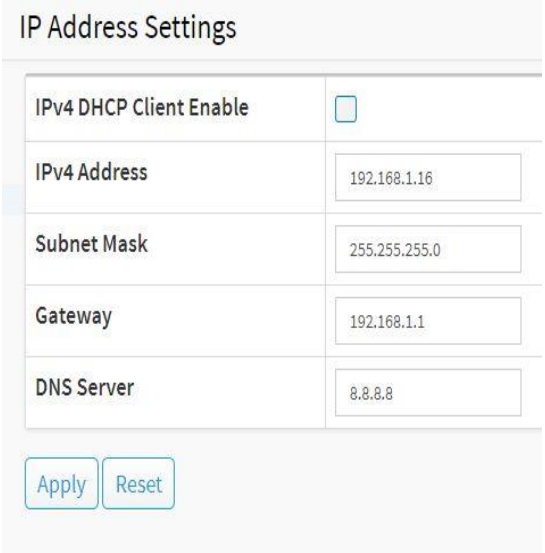


Figure 10: IP Address Setting

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.

3-4 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 User Account in the web interface:

1. Click System -> Account/Password.
2. Specify the User Name.
3. Specify new password and confirm new password.
4. Click Apply.

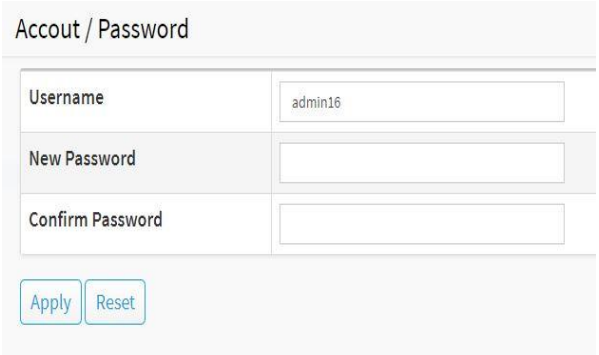


Figure 11: Account / Password

Parameter Description:

- **Username**

  The name identifying the user. The field can be input 32 characters.

- **New Password**

  To type the new password. The field can be input 32 characters.

- **Confirm Password**

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

3-5 SNMP

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

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

3-5.1 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.

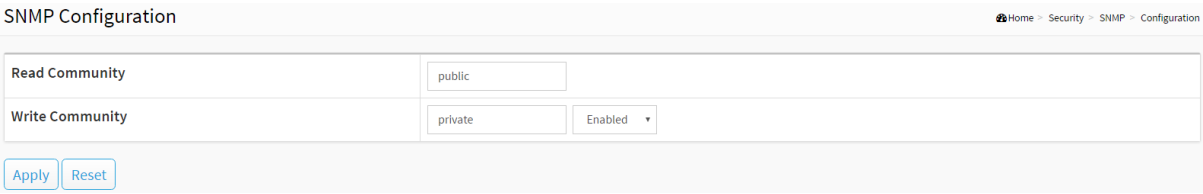


Figure 3-5.1: The SNMP Configuration

Parameter description:

- **Read Community :**

  Indicates the community read access string to permit access to SNMP agent. The allowed string length is 1 to 31, and the allowed content is the ASCII characters from 33 to 126.

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

to restrict source subnet.

- **Write Community :**

  Indicates the community write access string to permit access to SNMP agent. The allowed string length is 1 to 31, and the allowed content is the ASCII characters from 33 to 126.

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

Buttons

- **Apply :**

  Click to save changes.

- **Reset :**

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

3-5.2 SNMPv3

3-5.2.1 Communities

The function is used to configure SNMPv3 communities. The Community is unique. To create a new community account, please check <Add new community> button, and enter the account information then check <Save>. Max Group Number: 6.

Web Interface

To configure the configure SNMP Communities in the web interface:

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

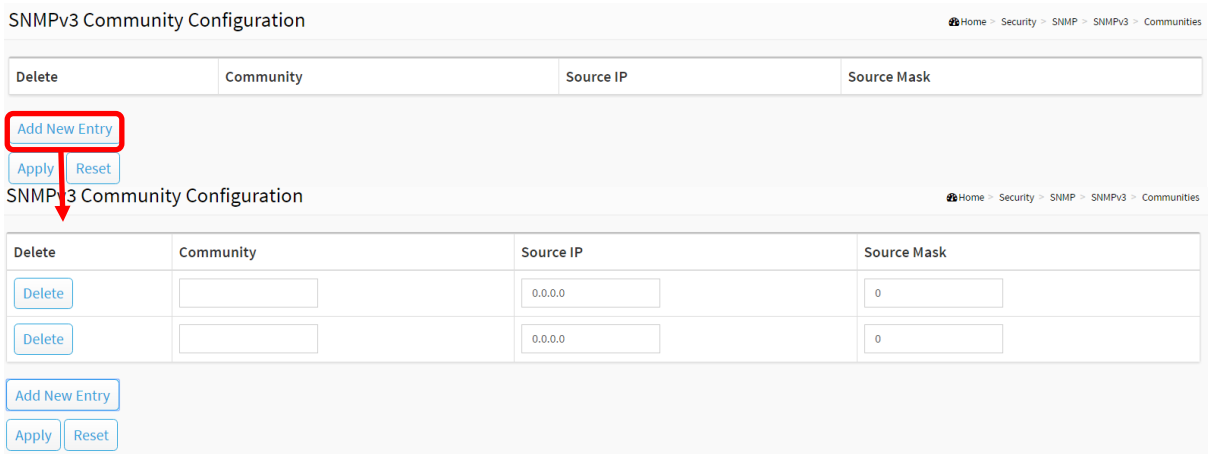


Figure 3-5.2.1: The SNMPv3 Communities Configuration

Parameter description:

- **Community**

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

- **Source IP**

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

- **Source Mask**

  Indicates the SNMP access source address mask

Buttons

- **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.

The function is used to configure SNMPv3 user. The Entry index key is UserName. To create a new UserName account, please check <Add new user> button, and enter the user information then check <Apply>. Max Group Number: 6.

Web Interface

To configure SNMP Users in the web interface:

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

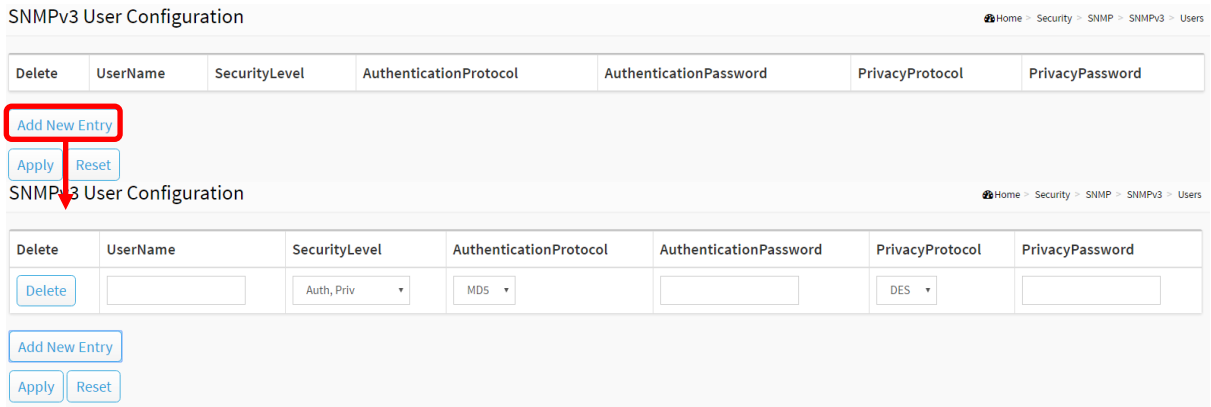


Figure 3-5.2.2: The SNMP Users Configuration

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.

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 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.

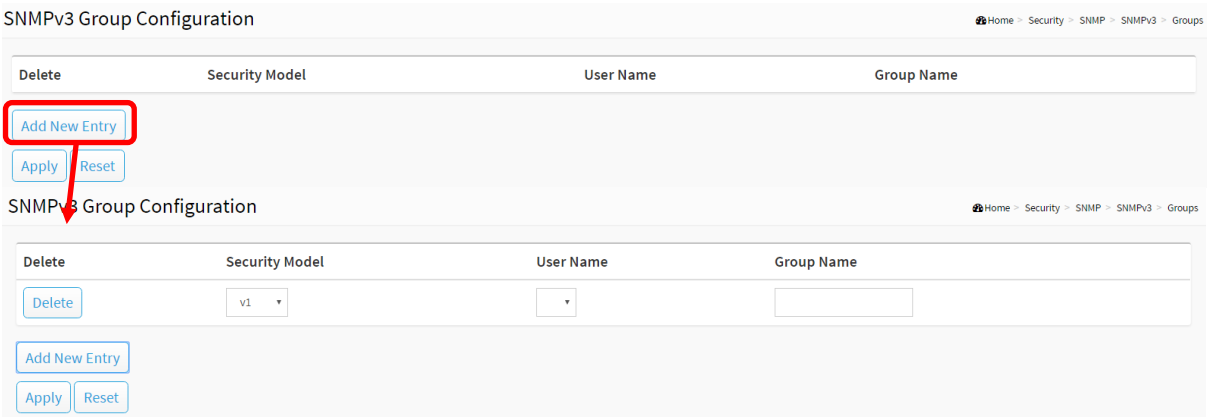


Figure 3-5.2.3: The SNMP Groups Configuration

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).

- **Security Name :**

  A string identifying the security 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.

- **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.

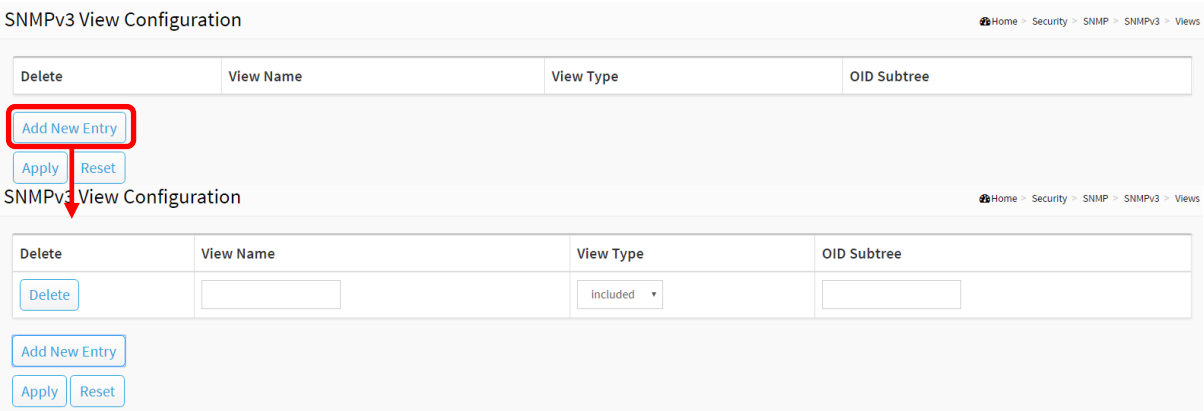


Figure 3-5.2.4: The SNMP Views Configuration

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.

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.

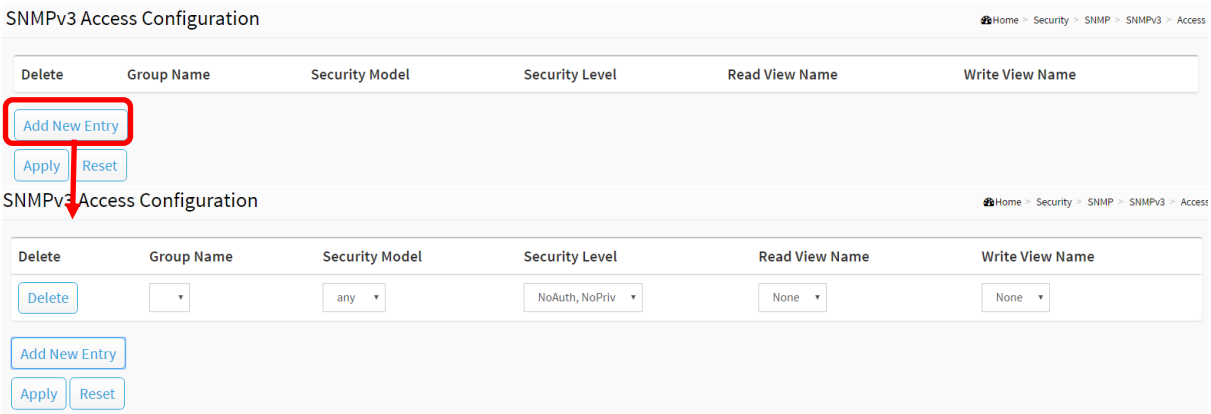


Figure 3-5.2.5: The SNMP Accesses Configuration

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:

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

  v1: Reserved for SNMPv1.

  v2c: Reserved for SNMPv2c.

  usm: User-based Security Model (USM).

- **Security Level :**

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

  NoAuth, NoPriv: No authentication and no privacy.

  Auth, NoPriv: Authentication and no privacy.

  Auth, Priv: Authentication and privacy.

- **Read View Name :**

  The name of the MIB view defining the MIB objects for which this request may request the current values. The allowed string length is 1 to 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.

3-6 SysLog

3-6.1 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 System -> Syslog Configuration.
2. Specify Mode and Server 1(or Server 2) parameters.
3. Click Apply.

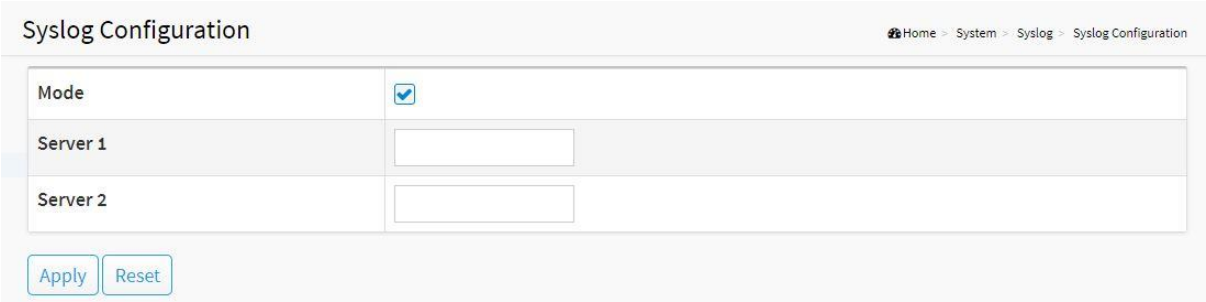


Figure 13: Syslog Configuration

Parameter Description:

- **Mode**

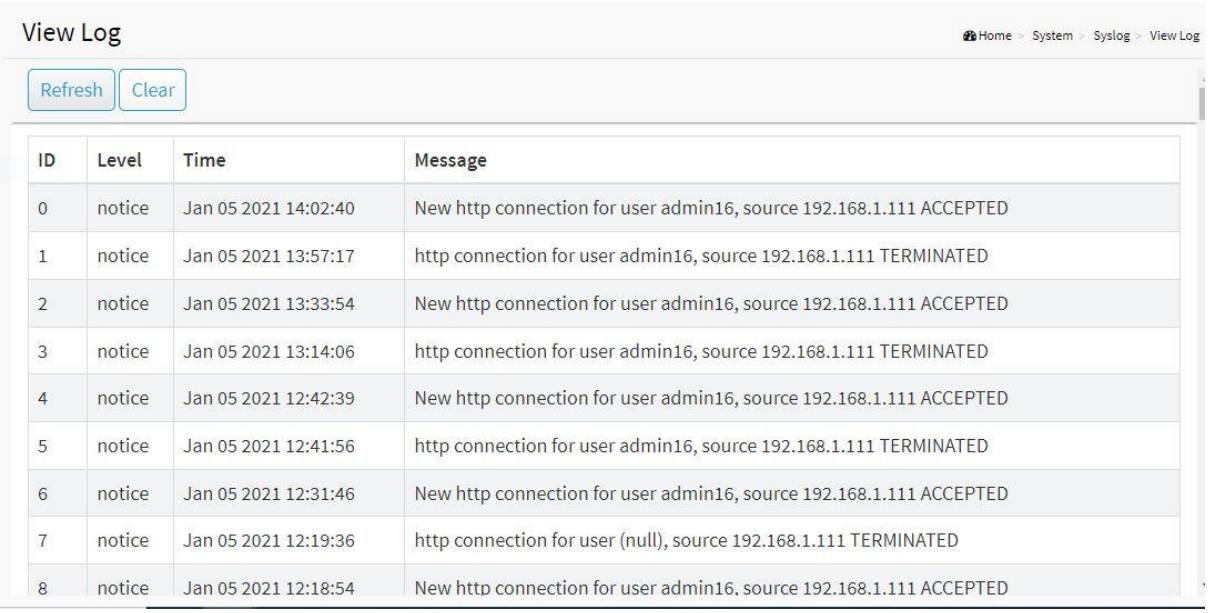
  To enable/disable Syslog function

- **Server1(or Server2)**

  SysLog Server. (IPv4 format)

3-6.2 View Log

To display Log, click System -> SysLog -> View Log



ID	Level	Time	Message
0	notice	Jan 05 2021 14:02:40	New http connection for user admin16, source 192.168.1.111 ACCEPTED
1	notice	Jan 05 2021 13:57:17	http connection for user admin16, source 192.168.1.111 TERMINATED
2	notice	Jan 05 2021 13:33:54	New http connection for user admin16, source 192.168.1.111 ACCEPTED
3	notice	Jan 05 2021 13:14:06	http connection for user admin16, source 192.168.1.111 TERMINATED
4	notice	Jan 05 2021 12:42:39	New http connection for user admin16, source 192.168.1.111 ACCEPTED
5	notice	Jan 05 2021 12:41:56	http connection for user admin16, source 192.168.1.111 TERMINATED
6	notice	Jan 05 2021 12:31:46	New http connection for user admin16, source 192.168.1.111 ACCEPTED
7	notice	Jan 05 2021 12:19:36	http connection for user (null), source 192.168.1.111 TERMINATED
8	notice	Jan 05 2021 12:18:54	New http connection for user admin16, source 192.168.1.111 ACCEPTED

Figure 14: View log

Parameter Description:

- **Level**

  The log event category

- **Time**

  The log event occurs time

- **Message**

  The log event content

- **Refresh[Button]**

  To reload log events

- **Clear[Button]**

  To clear log events

3-7 Digital I/O

3-7.1 DI Trigger DO

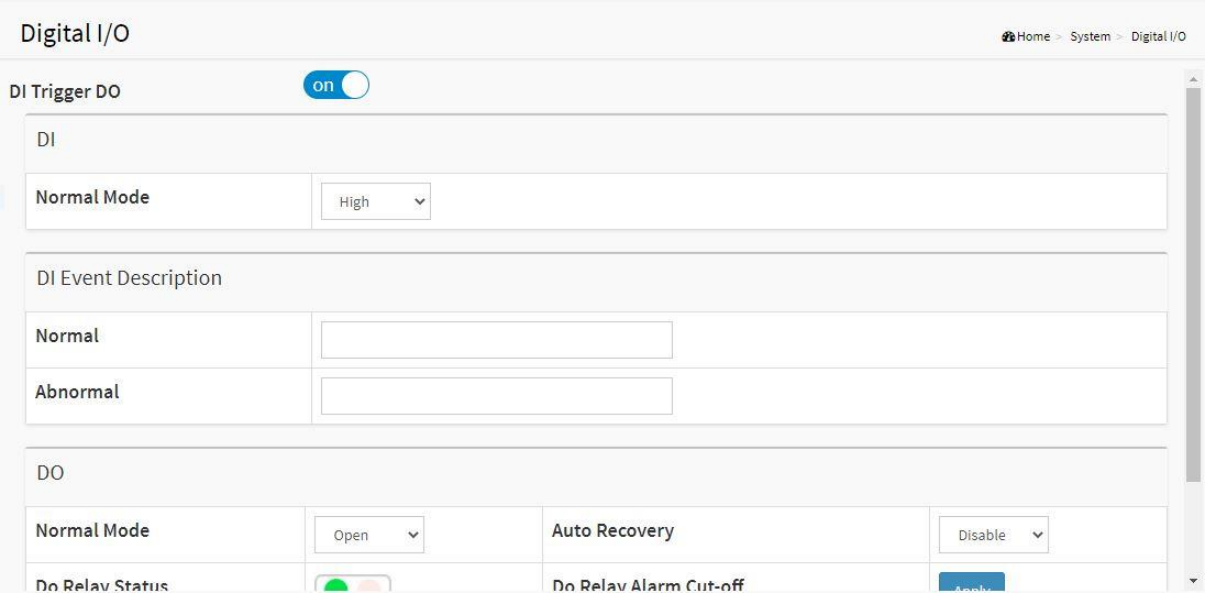


Figure 15: DI Trigger DO

Figure 16: DI without trigger DO

Configure the normal modes of digital input/output (DI/DO).

Web Interface

1. System -> Digital I/O

Parameter Description:

- **DI Trigger DO**

  Set Digital input Trigger digit output.

- **Pulse Duration**

  Set DO pulse duration.

- **DI Trigger DO DO Normal Mode**

  Set the normal mode of the digital output(DO). You can set it to Open or Close.

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

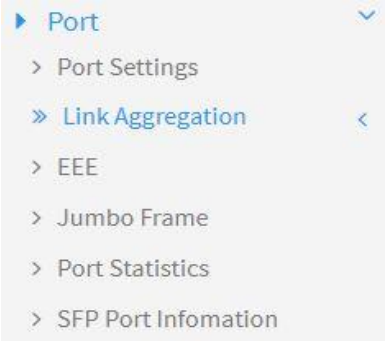


Figure 17: Port Setting

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:

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

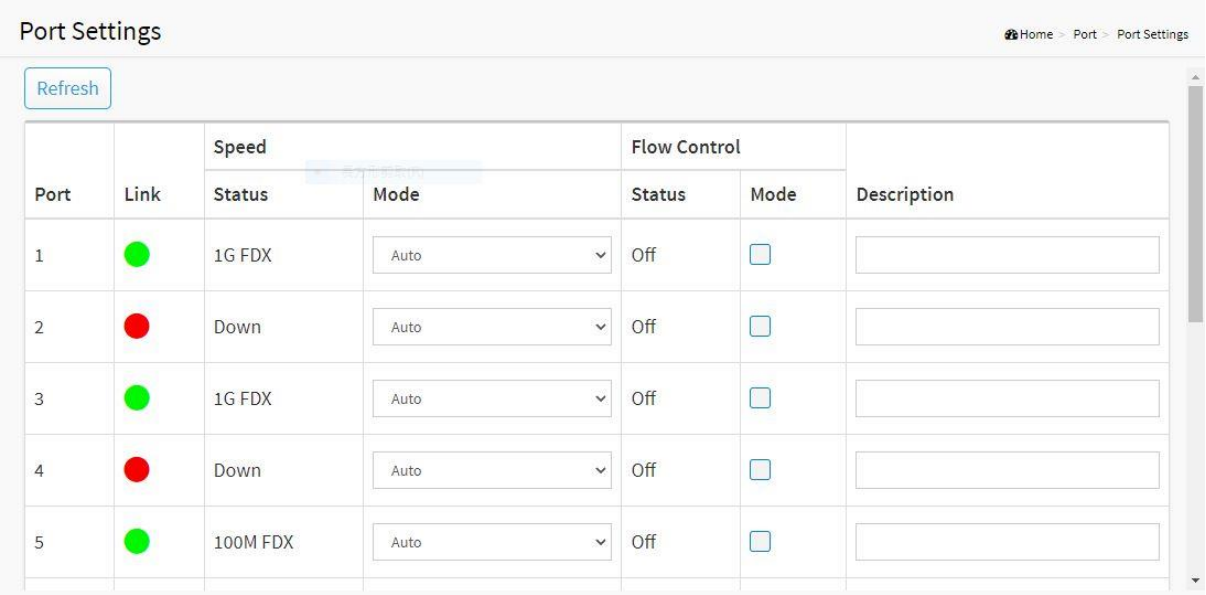


Figure 18: Port Setting

4-2 Link Aggregation

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.

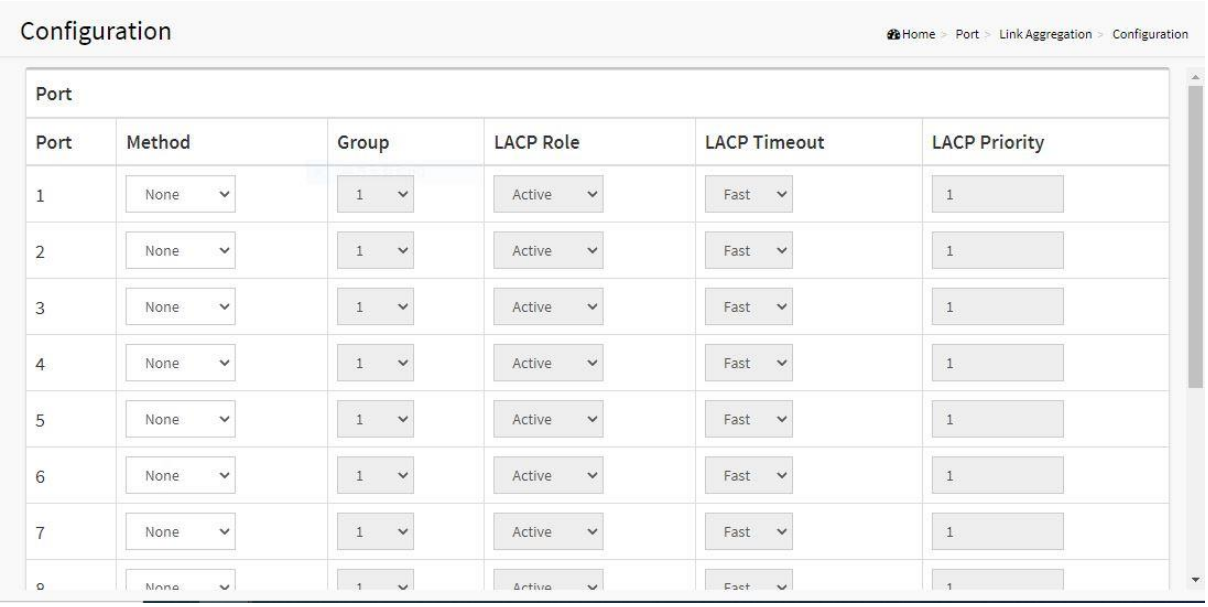


Figure 19: Link Aggregation

Parameter Description:

■ **Method**

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

4-3 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.

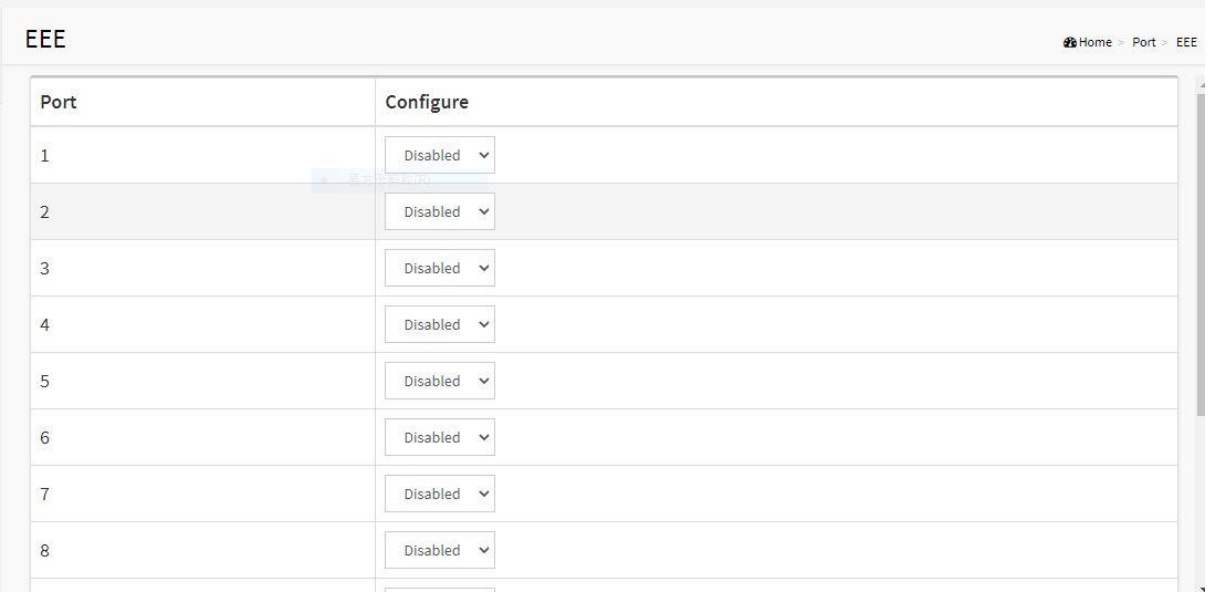


Figure 20: Link Aggregation

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 21: Jumbo Frame

Parameter Description:

- To enable/disable jumbo frame function.

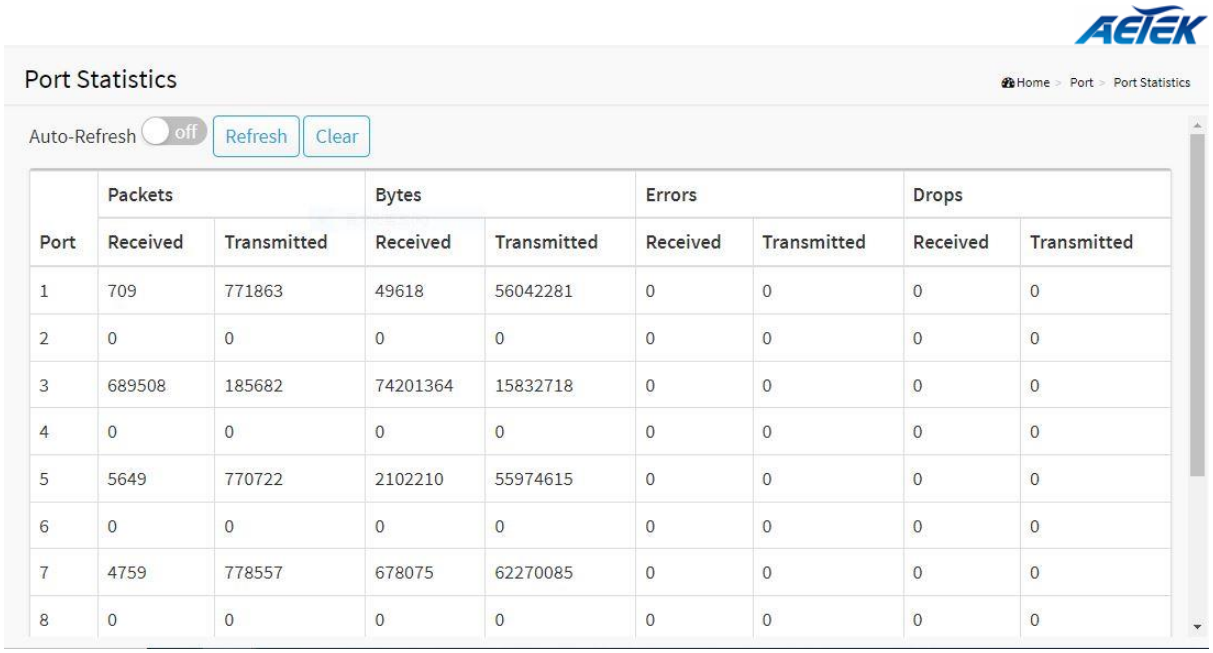
4-5 Port Statistics

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 22: 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:

4. Click Port -> SFP Port Information

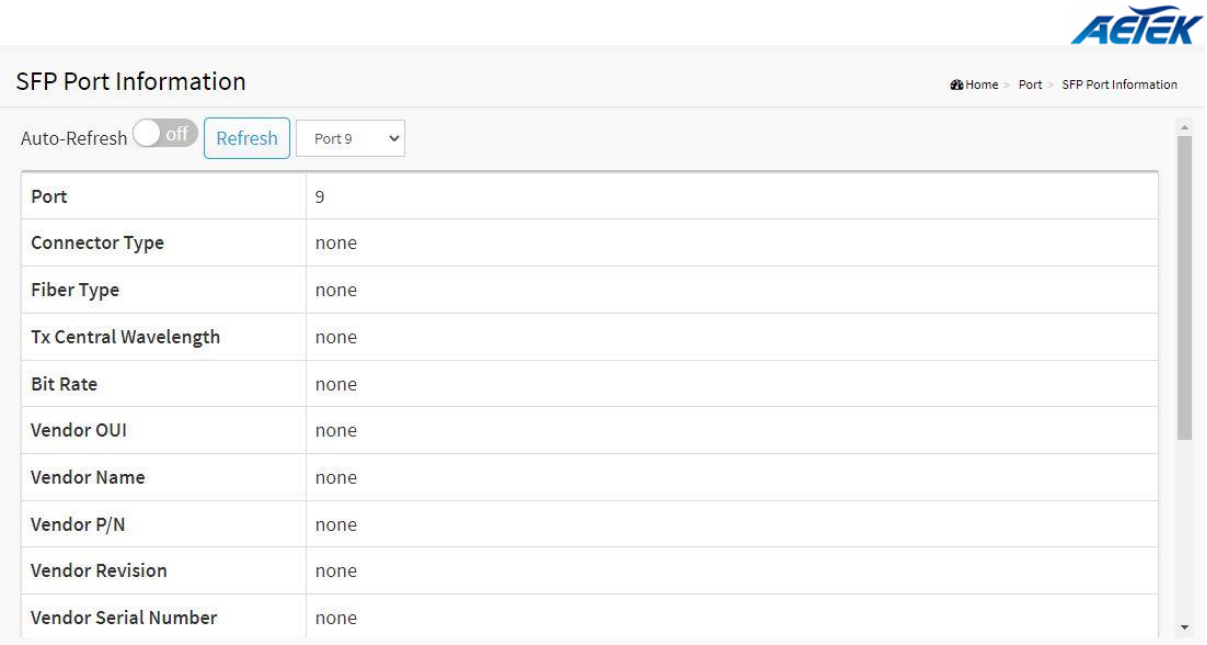


Figure 23: SFP Port Information

Parameter Description:

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

Chapter 5 PoE Management

This chapter describes the PoE management including PoE Configuration, PoE Status, PoE Power Delay, PoE Auto Check and PoE Scheduling Profile.

5-1 PoE Configuration

This page displays current PoE ports' power ON/OFF status and schedule profile. It can also be configured here.

Web Interface

To configure a PoE port's power in the web interface:

1. Click PoE Management -> PoE Configuration.
2. Specify the parameters which you want to configure.
3. Click Apply.

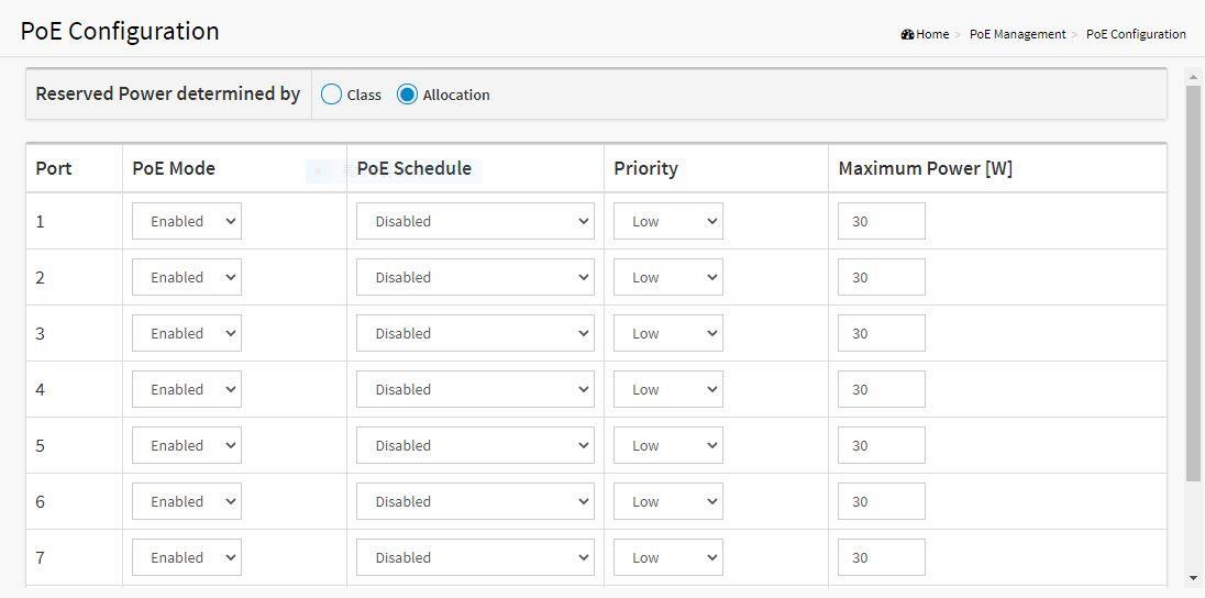


Figure 24: PoE Configuration

Parameter Description:

- **PoE Mode**

(1) Model-30 setting:

To enable/disable port's power

(2) Model-90 setting:

802.3 BT PoE (90W): Enables PoE IEEE 802.3bt 90W mode.

POH (90W): Enables PoH 90W mode.

Disable : Disable PoE.

- **PoE Schedule**

  To set port's schedule profile. (profile 1 to 10, disabled means no schedule profile)

- **Priority**

  To set port's priority.

- **Maximum Power(W)**

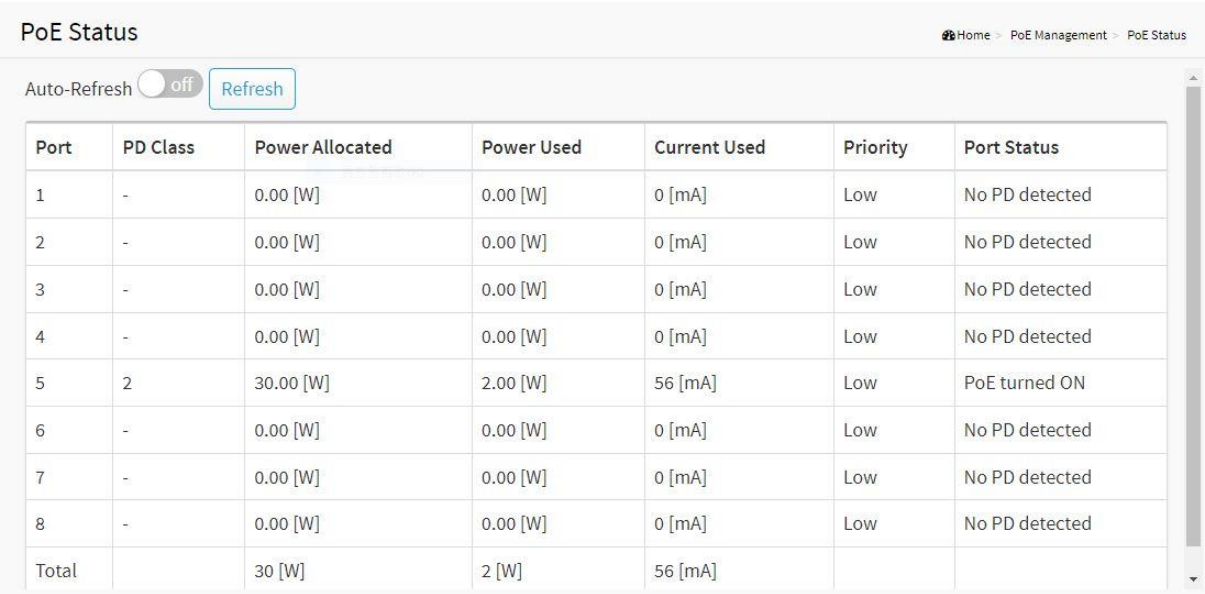
  To set port's power.

5-2 PoE Status

This page displays current ports' power status.

Web Interface

To display PoE port's power information in the web interface, click PoE Management -> PoE Status.



Port	PD Class	Power Allocated	Power Used	Current Used	Priority	Port Status
1	-	0.00 [W]	0.00 [W]	0 [mA]	Low	No PD detected
2	-	0.00 [W]	0.00 [W]	0 [mA]	Low	No PD detected
3	-	0.00 [W]	0.00 [W]	0 [mA]	Low	No PD detected
4	-	0.00 [W]	0.00 [W]	0 [mA]	Low	No PD detected
5	2	30.00 [W]	2.00 [W]	56 [mA]	Low	PoE turned ON
6	-	0.00 [W]	0.00 [W]	0 [mA]	Low	No PD detected
7	-	0.00 [W]	0.00 [W]	0 [mA]	Low	No PD detected
8	-	0.00 [W]	0.00 [W]	0 [mA]	Low	No PD detected
Total		30 [W]	2 [W]	56 [mA]		

Figure 25: PoE Status

Parameter Description:

- **Auto Refresh**

  To refresh web page automatically every 10 seconds.

- **Port**

  The port number.

- **PD Class**

  The IEEE802.3af/at/bt defined power classification.

Class0: 0.44~12.95 W

Class1: 0.44~3.84 W

Class2: 3.84W~6.49 W

Class3: 6.49～12.95 W

Class4: 12.95～25.5 W

Class5: 40 W

Class6: 51 W

Class7: 62 W

Class8: 71 W

- **Power Allocated**

  The port's PoE can used maximum

- **Power Used**

  The port's PoE used power.

- **Current Used**

  The port's PoE used current.

- **Priority**

  The port's PoE priority.

- **Port Status**

  The port's PoE Status.

5-3 PoE Power Delay

This page displays current PoE ports' power delay function. It can also be configured here.

Web Interface

To configure a port power delay function in the web interface:

1. Click PoE Management -> PoE Power Delay.
2. Specify the parameters which you want to configure.
3. Click Apply.

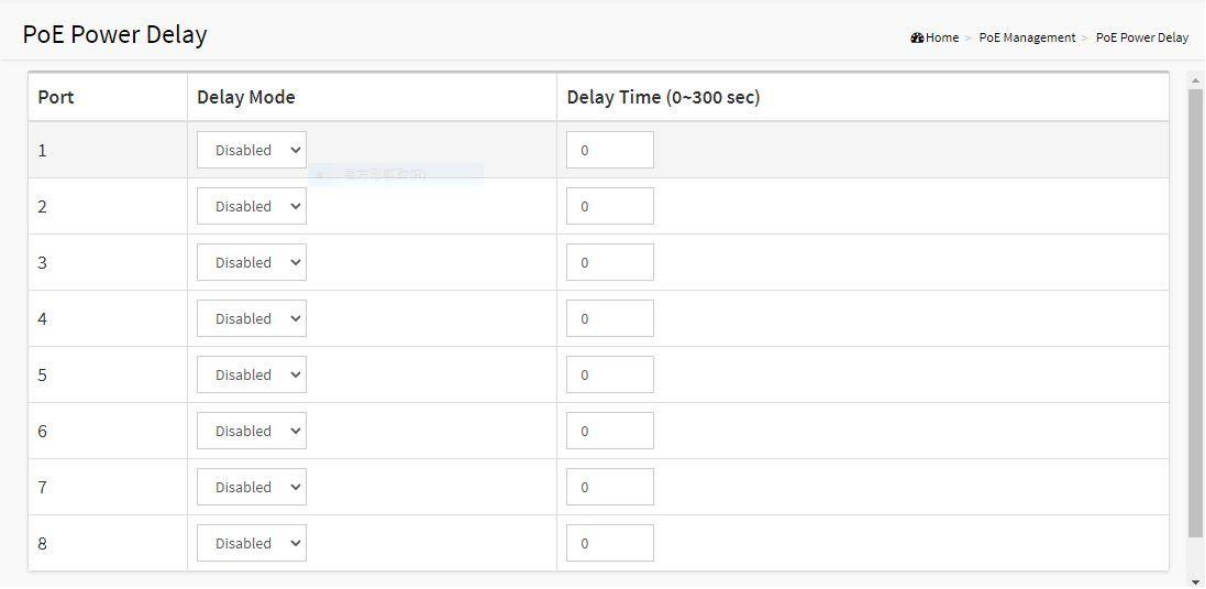


Figure 26: PoE Power Delay

Parameter Description:

- **Delay Mode**

  To enable/disable power delay function

- **Delay Time**

  To set port's power delay time. (0 ~ 300 seconds)

5-4 PoE Auto Checking

This page displays current PoE ports' power auto checking function. It can also be configured here.

Web Interface

To configure a port power auto checking function in the web interface:

1. Click PoE Management -> PoE Auto Checking.
2. Specify the parameters which you want to configure.
3. Click Apply.

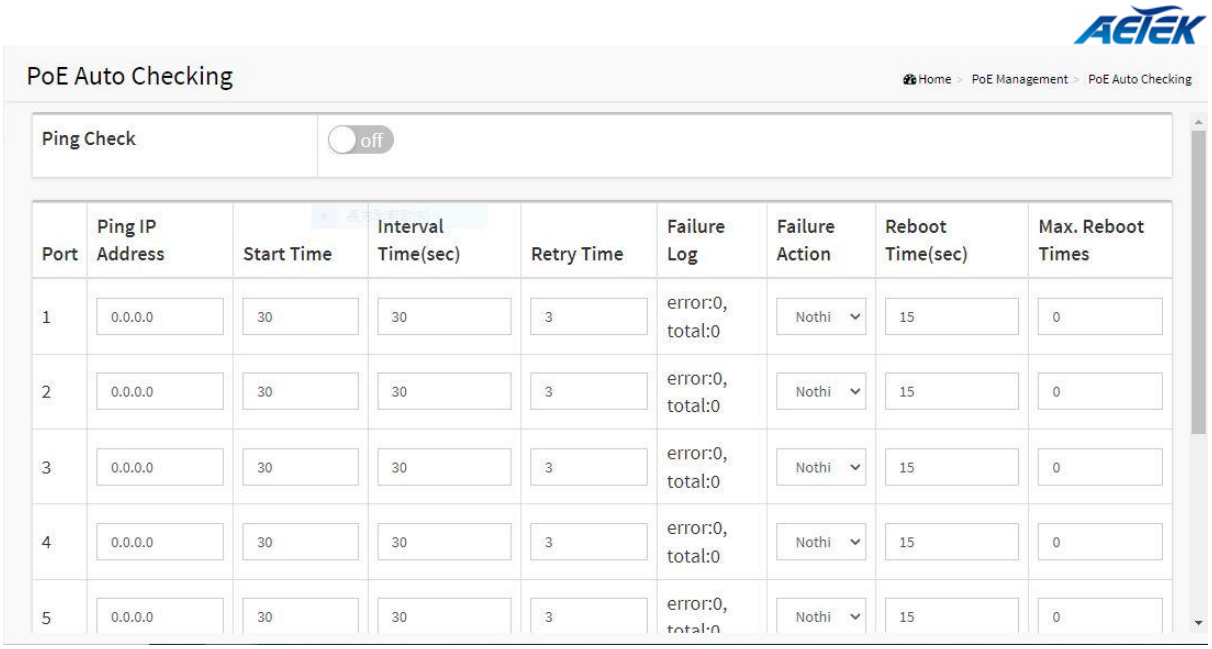


Figure 27: Power Auto Check

Parameter Description:

- **Ping IP Address**

  The PD's IP Address used to test its connectivity.

- **Start Time**

  After Startup Time, PoE auto checking function will be started. Default: 30, range: 30-60 seconds.

- **Interval Time**

  Device will send checking message to PD each interval time. Default: 30, range: 10-120 seconds.

- **Retry Time**

  When PoE port can't ping the PD, it will retry to send detection again. When reaching the retry time, it will trigger failure action. Default: 3, range: 1-5.

- **Failure Log**

  Failure loggings counter.

- **Failure Action**

  The action when reaching the retry time fail detection.

  Nothing: Keep Ping the remote PD but does nothing further.

  Reboot: Cut off the power of the PoE port, make PD rebooted.

- **Reboot Time**

  When PD has been rebooted, the PoE port restored power after the Reboot Time. Default: 15, range: 3-120 sec.

5-5 PoE Scheduling Profile

This page displays current PoE ports' power schedule profile function. It can also be configured here.

Web Interface

To configure power scheduling profile in the web interface:

1. Click PoE Management -> PoE Scheduling Profile.
2. Specify the parameters which you want to configure.
3. Click Apply.

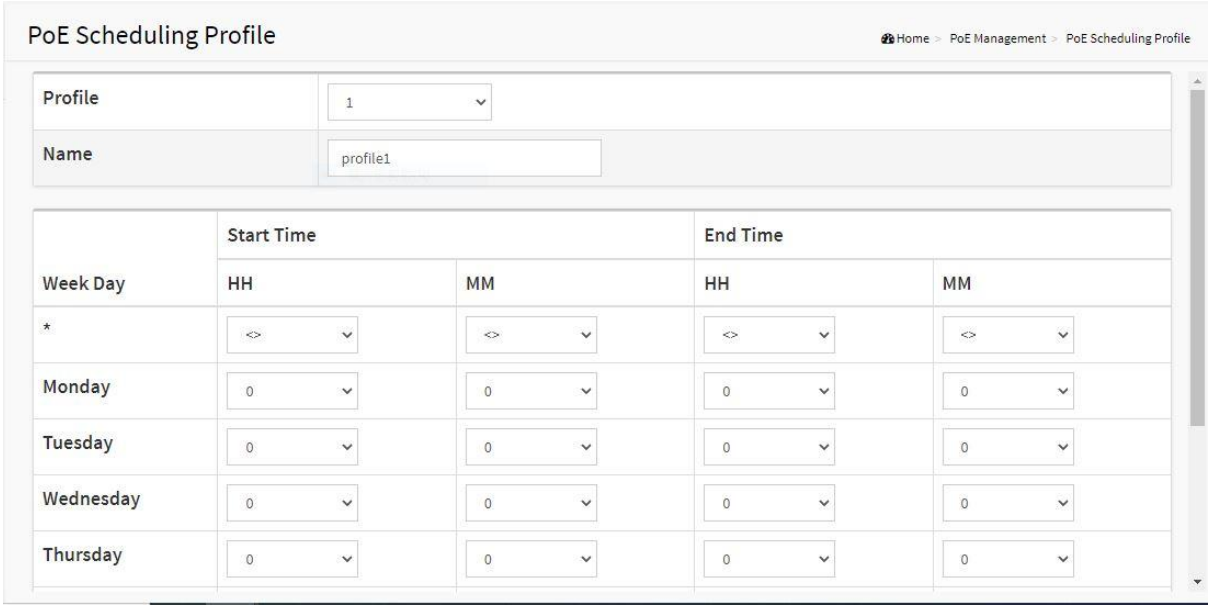


Figure 28: PoE Scheduling Profile

Parameter Description:

- **Profile**

  The profile number. (1-10)

- **Name**

  The profile name.

- **Start Time <HH>**

  The starting hour time.

- **Start Time <MM>**

  The starting minute time.

- **End Time <HH>**

  The ending hour time.

- **End Time <MM>**

  The ending minute time.

Chapter 6 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.

6-1 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.

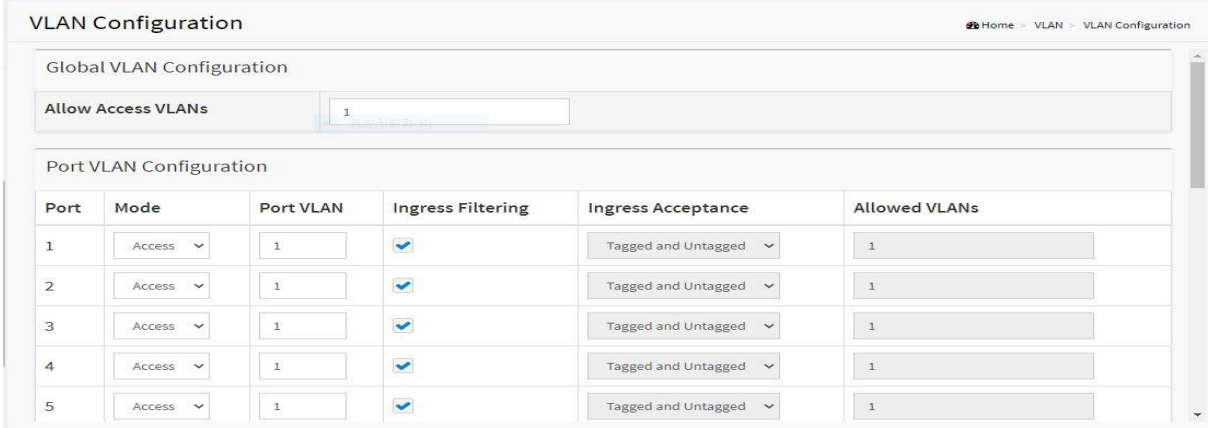


Figure 29: VLAN Configuration

Parameter Description:

- **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.

6-2 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 30: VLAN Member

Parameter Description:

- **VLAN ID**

  The VLAN ID list(s).

- **Port Members**

  The port status with VLAN setting.

Chapter 7 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.

7-1 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.

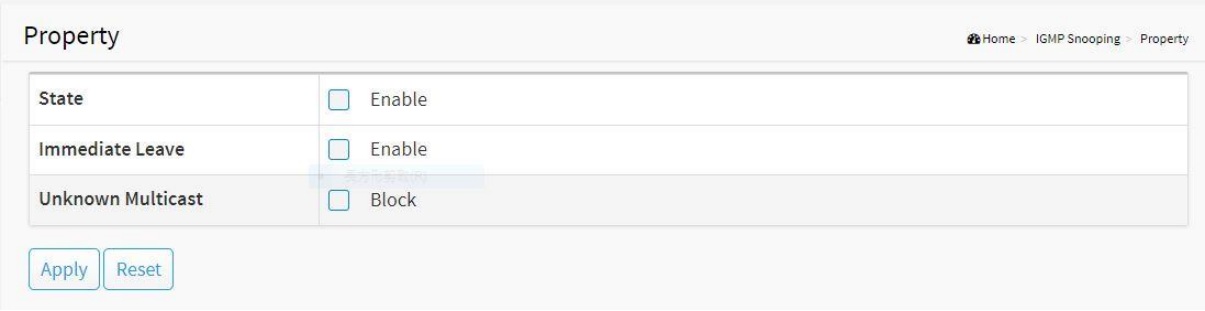


Figure 31: Property

Parameter Description:

- **State**

  To enable/disable IGMP Snooping function.

- **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

7-2 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.

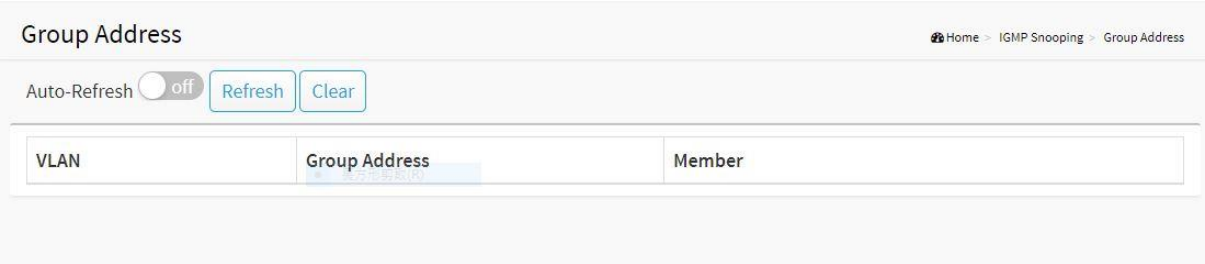


Figure 32: Group Address

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 8 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.

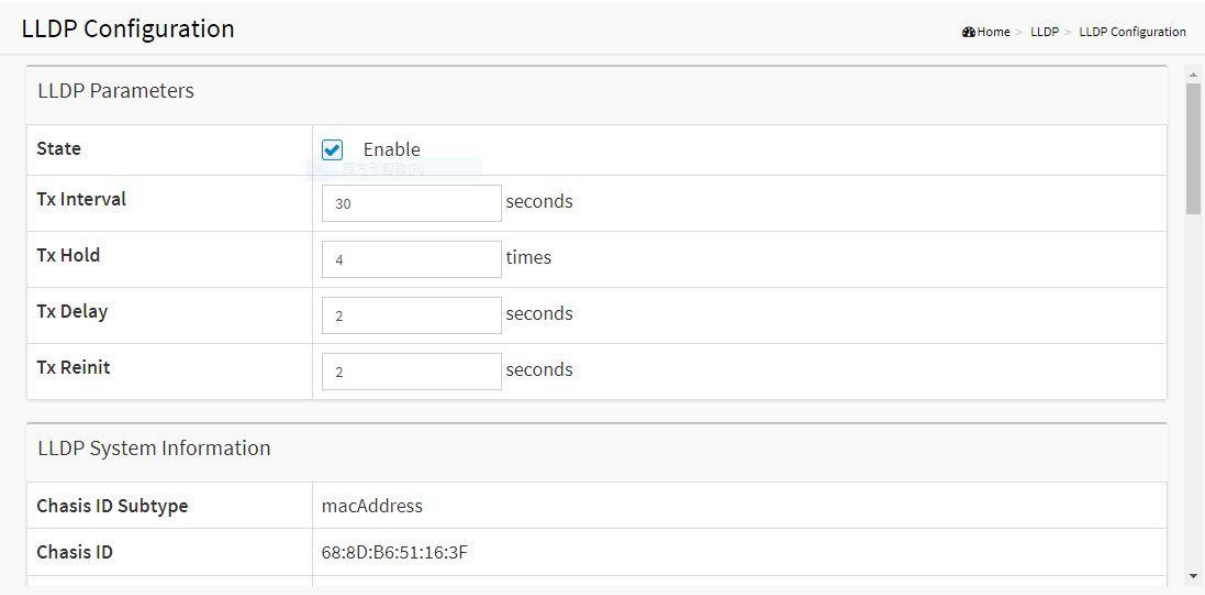
8-1 LLDP Configuration

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.



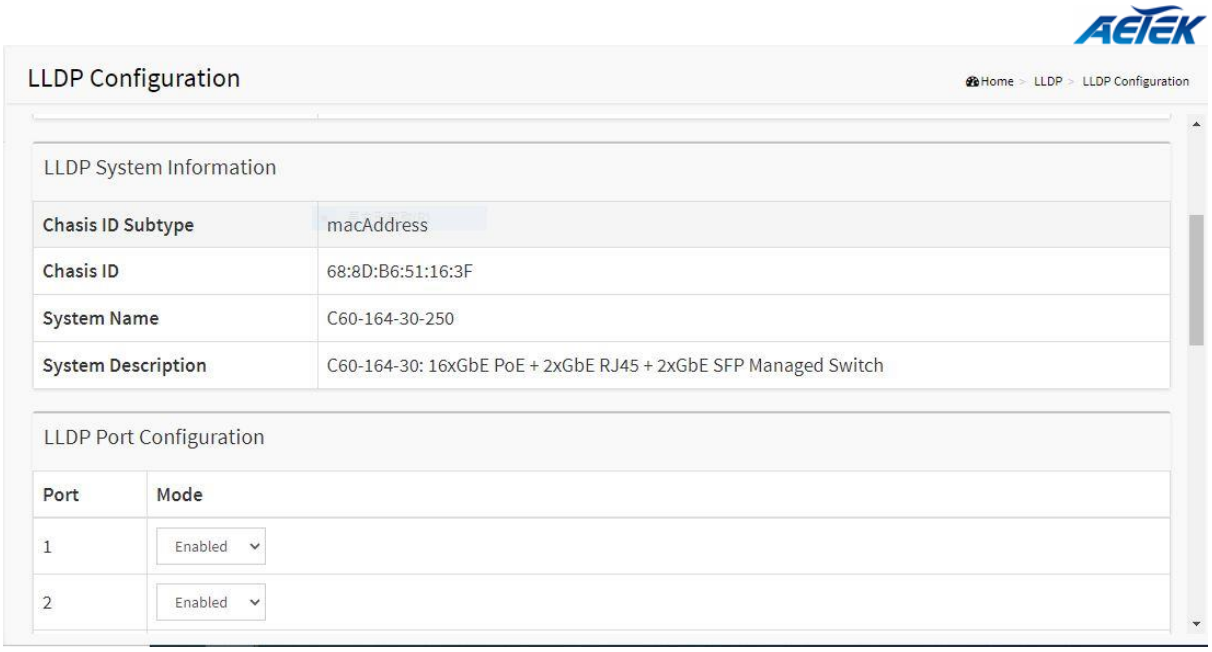


Figure 33: LLDP Configuration

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.

- **LLDP Port Configuration:**

Enable/Disable LLDP State for the ports.

8-2 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.

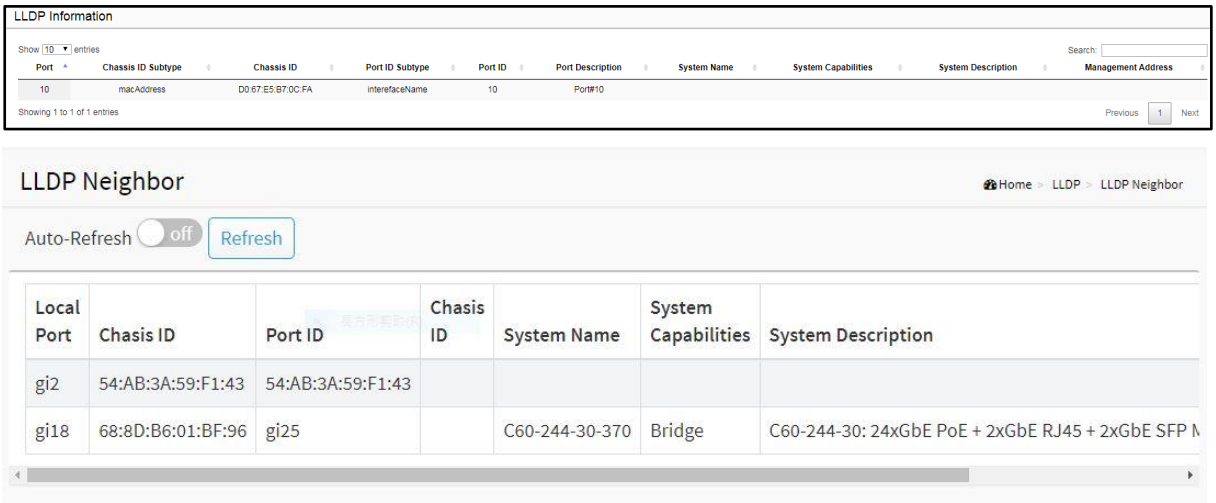


Figure 34: LLDP Information

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.

- **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 9 Loop Prevention

The chapter describes how to prevent loop situation.

9-1 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.

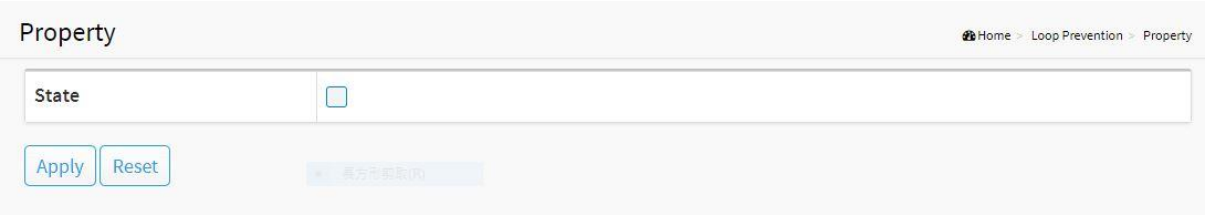


Figure 35: Property

Parameter description:

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

9-2 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.

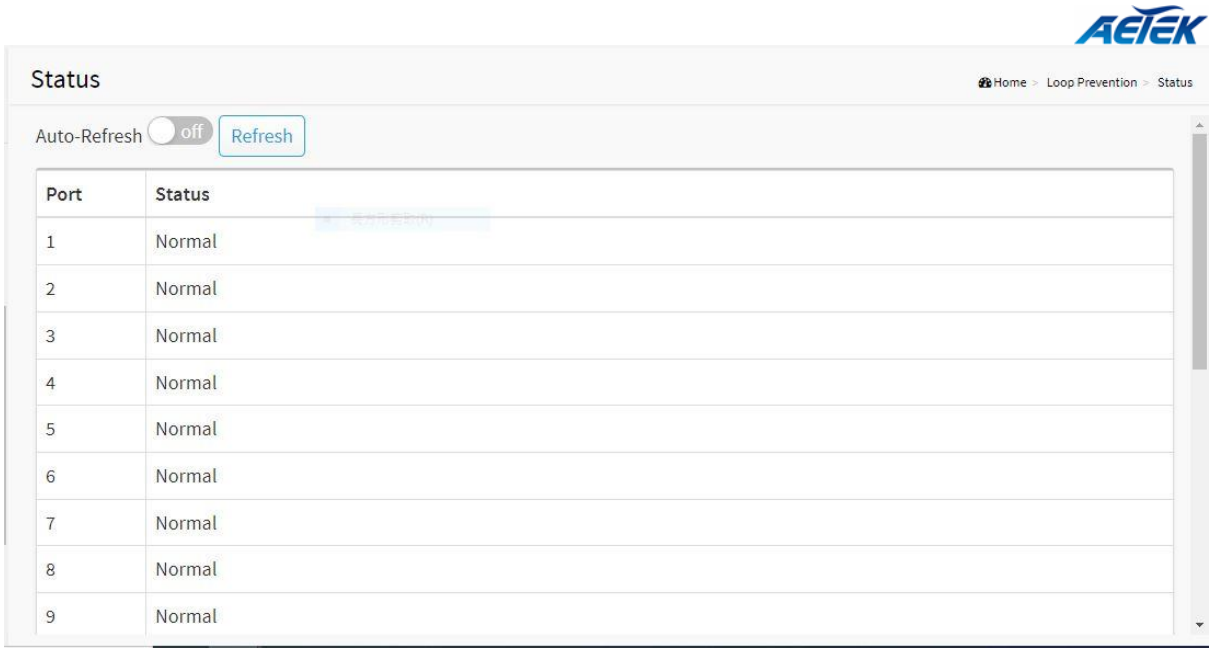


Figure 36: Status

Chapter 10 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.

10-1 Management

This page is used to configure the connect function.

Web Interface

To configure the IP filter function the web interface:

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

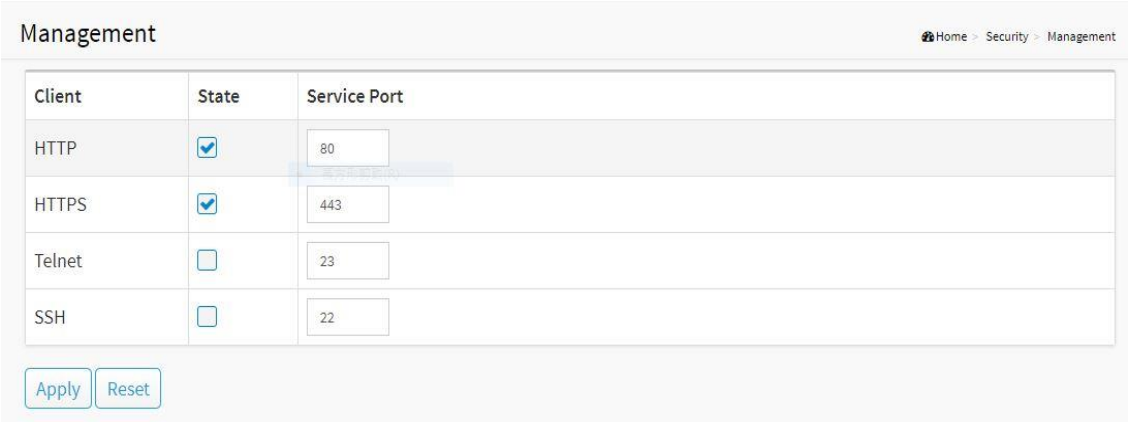


Figure 37: Management

10-2 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.

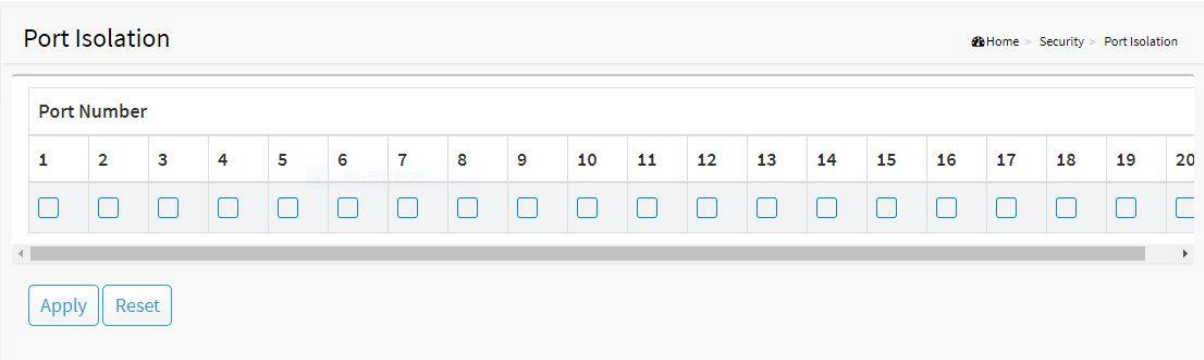


Figure 38: Port Isolation

Parameter Description:

- **Port Number**

  Select the port of the device to isolate.

10-3 Port Security

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.

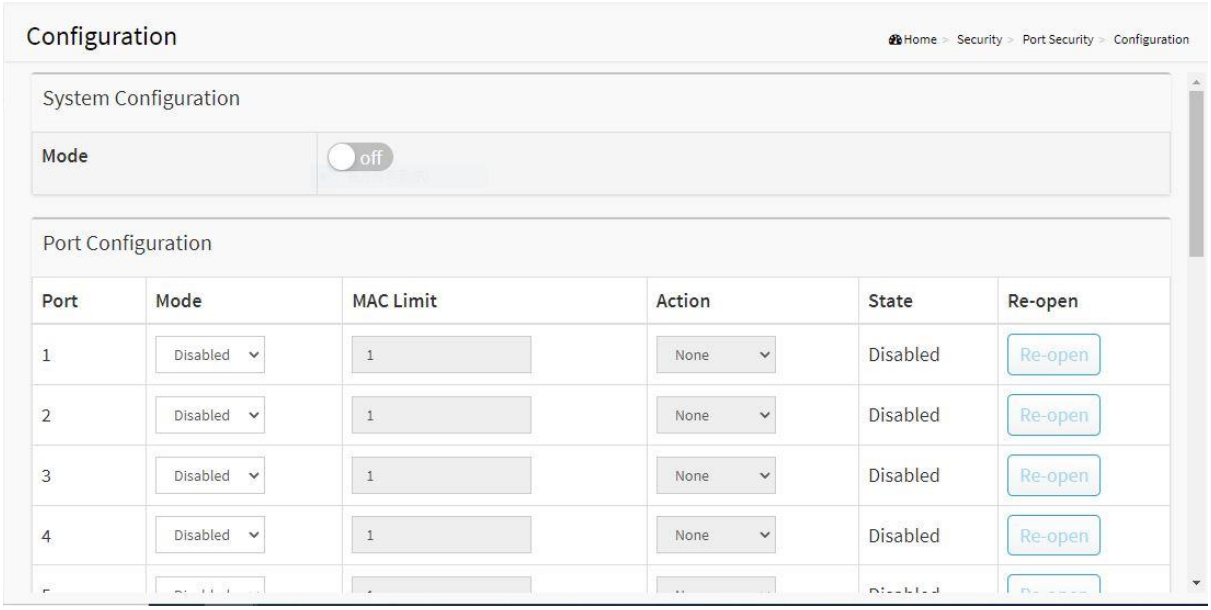


Figure 39: Port Security

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

10-4 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.

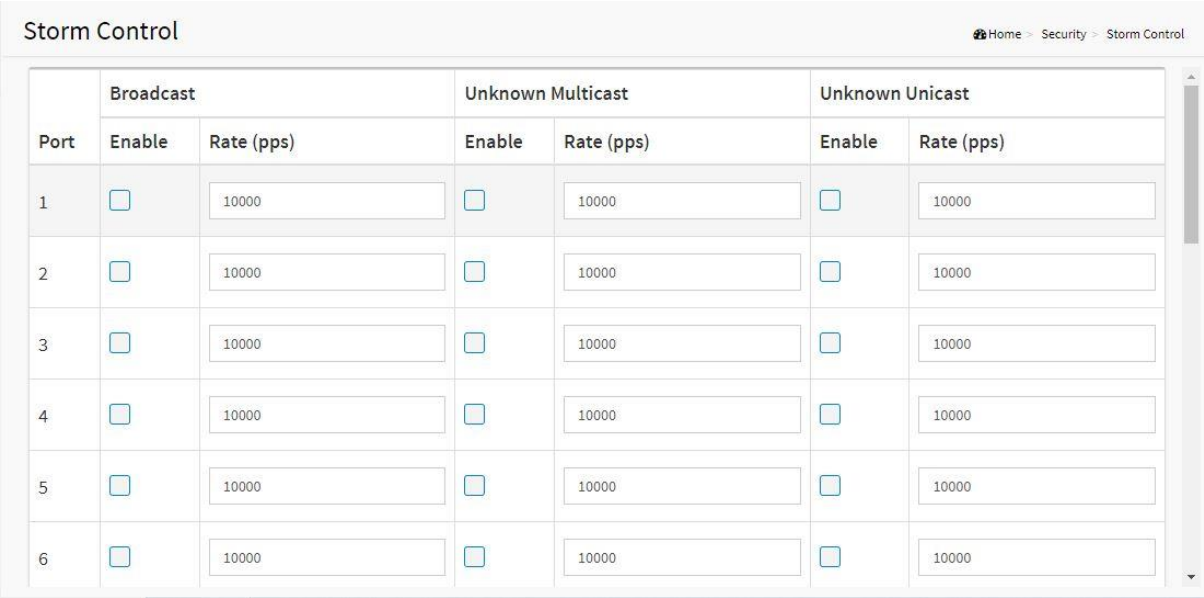


Figure 40: Storm Control

Parameter description:

- **Rate**

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

- **Enable**

  To enable/disable the function.

10-5 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.

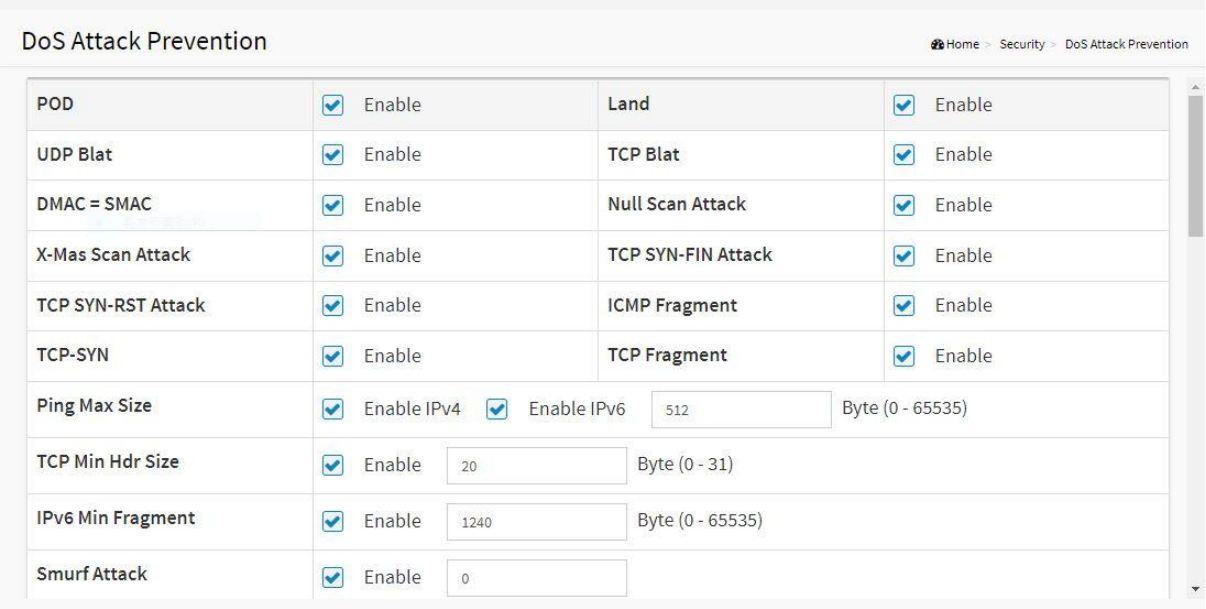


Figure 41: DoS Attack Prevention

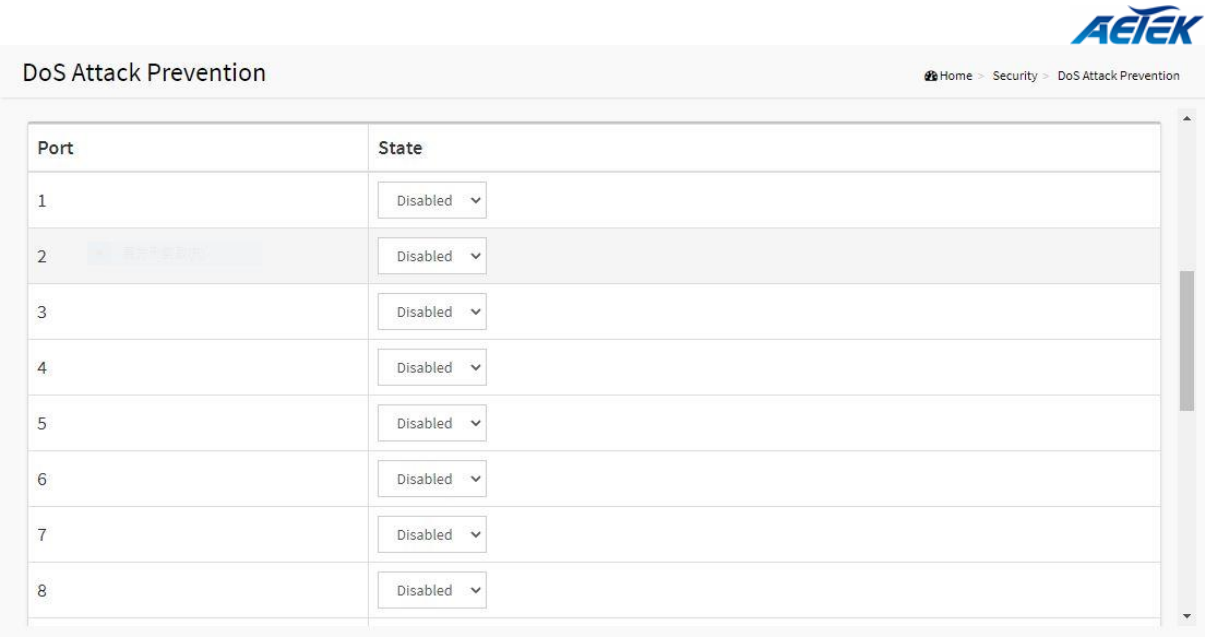


Figure 42: DoS Attack Prevention(Detail)

Parameter description:

- **Port**

  The normal port of the device.

- **State**

  To enable/disable the function.

Chapter 11 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.

11-1 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.

Parameter Description:

- **CoS/802**

  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.

- **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.

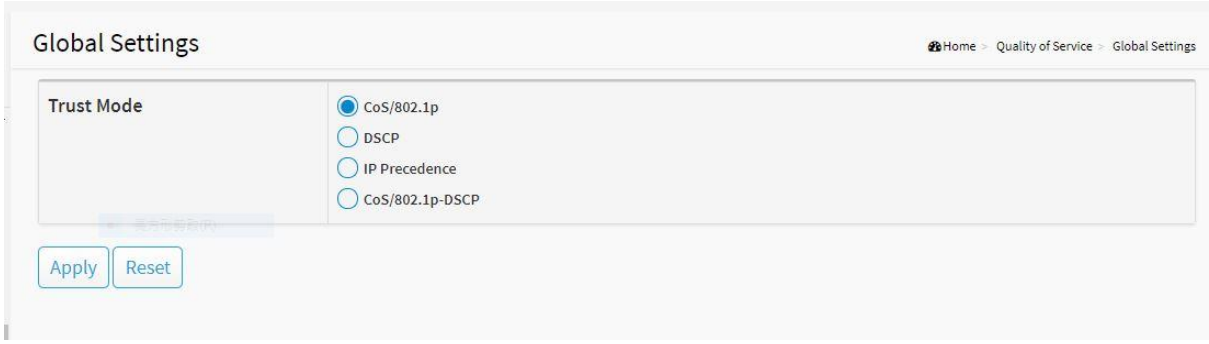


Figure 43: Global Setting

11-2 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.

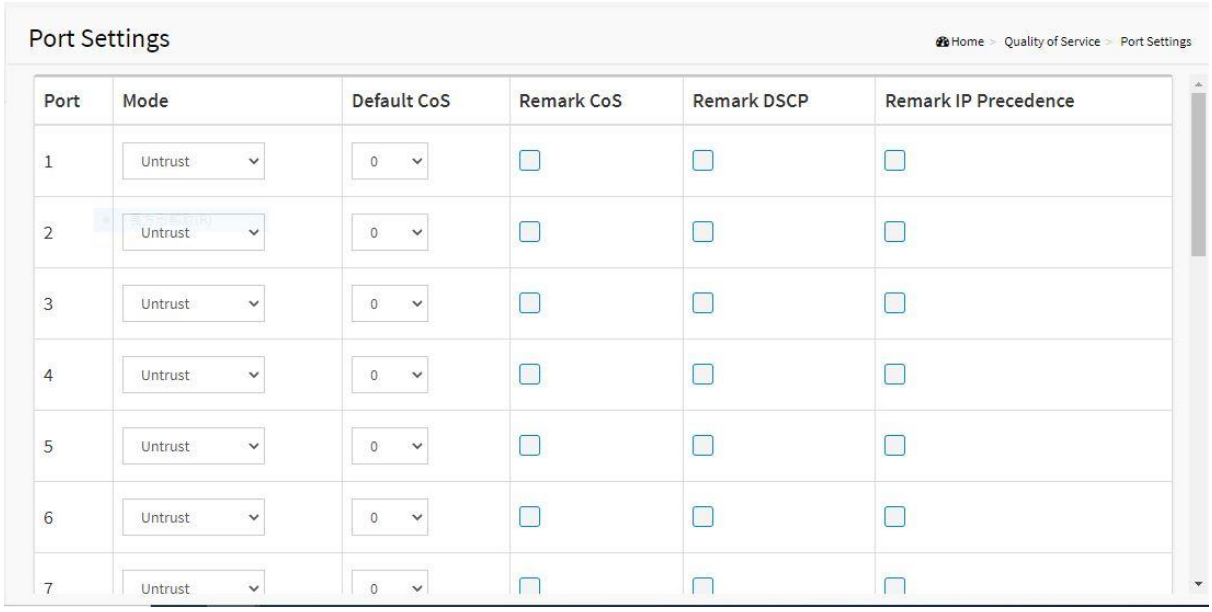


Figure 44: Port Setting

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.
- **Source CoS**
  The CoS value is determined based on C-Tag or S-Tag for incoming tagged packets.
- **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.

11-3 Port Policing

Web Interface

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

4. Click Quality of Service -> Port Policing.
5. Specify the parameter you want to configure.
6. Click Apply.

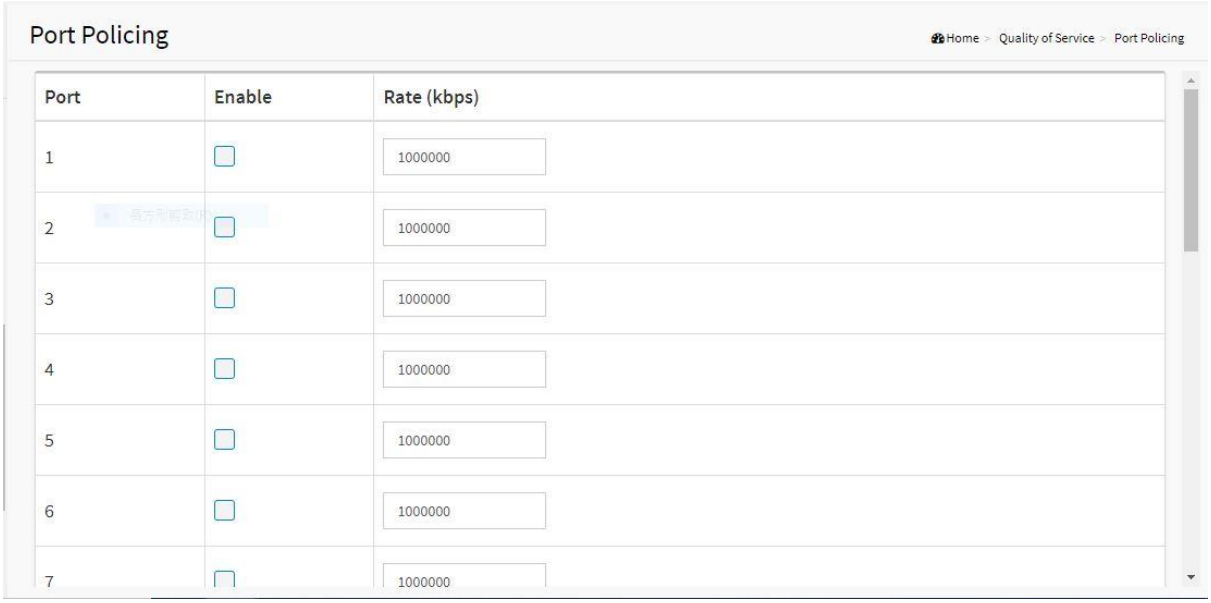


Figure 45: Port Policing

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.

11-4 Port Shaper

Web Interface

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

7. Click Quality of Service -> Port Shaper.
8. Specify the parameter you want to configure.
9. Click Apply.

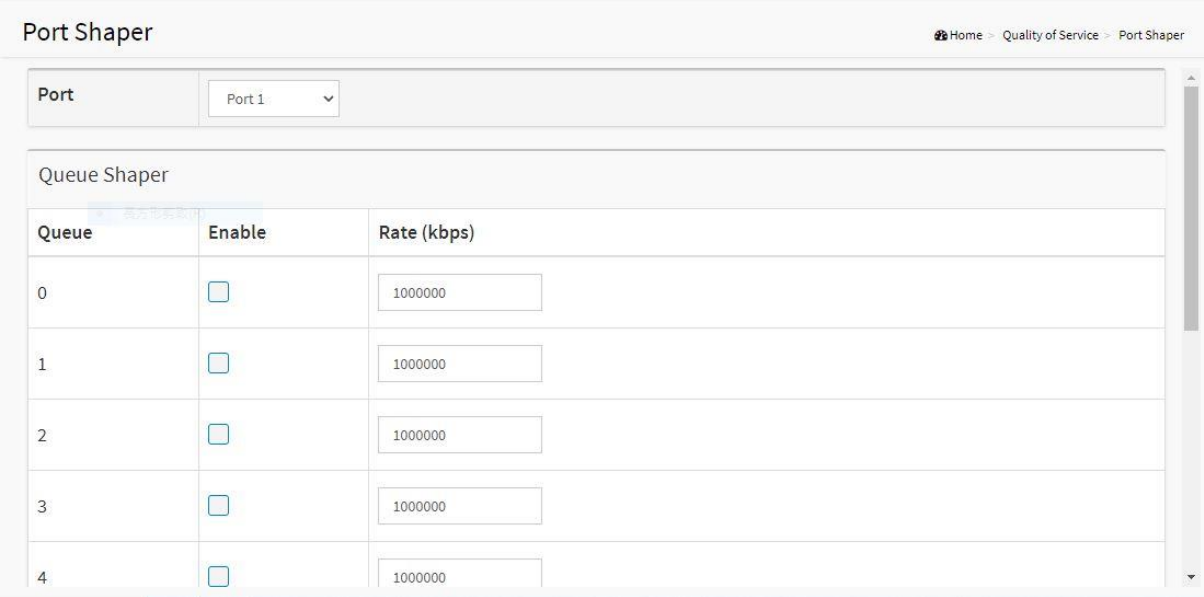


Figure 46: Port Shaper

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.

11-5 Port Scheduler

Web Interface

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

10. Click Quality of Service -> Port Scheduler.
11. Specify the parameter you want to configure.
12. Click Apply.

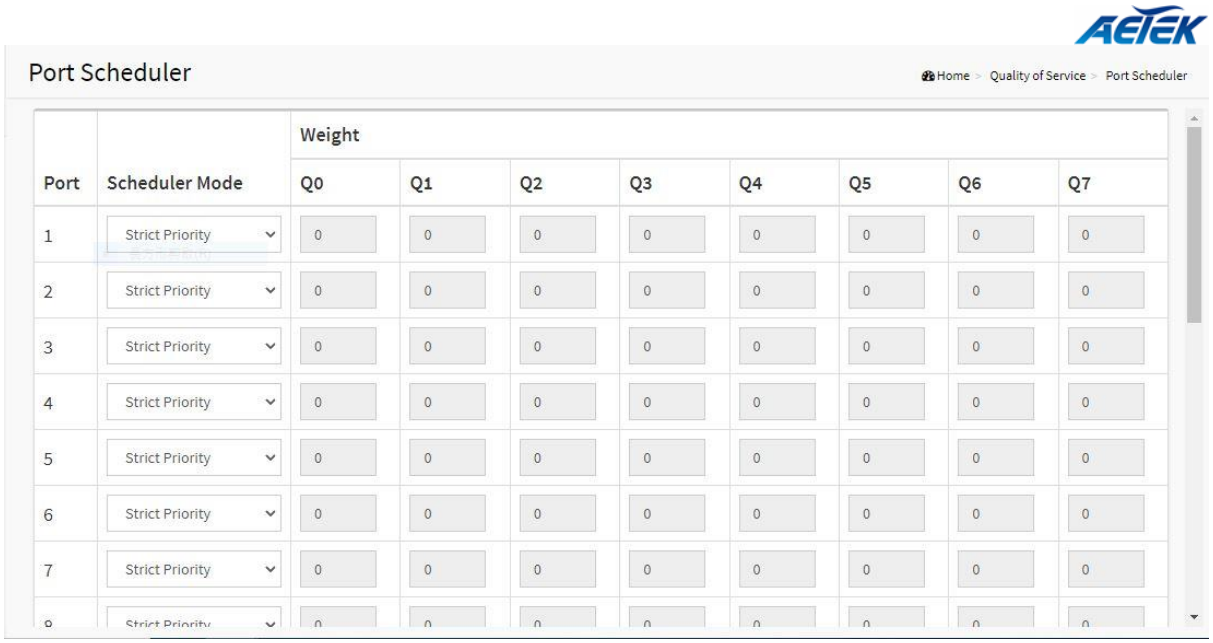


Figure 47: Port Scheduler

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".

11-6 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:

13. Click Quality of Service -> CoS/802.1p Mapping.
14. Specify the parameter you want to configure.
15. Click Apply.

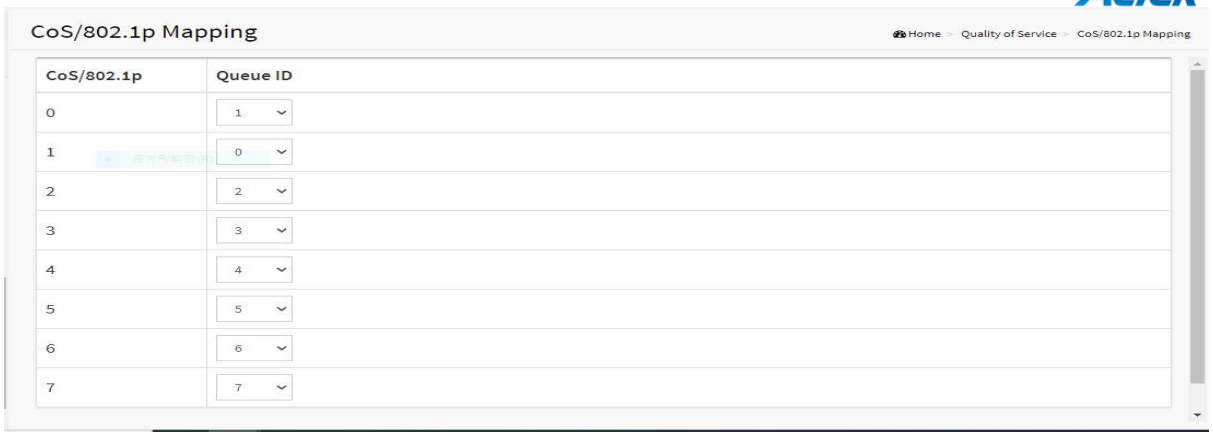


Figure 48: CoS/802.1p Mapping

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.

11-7 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.

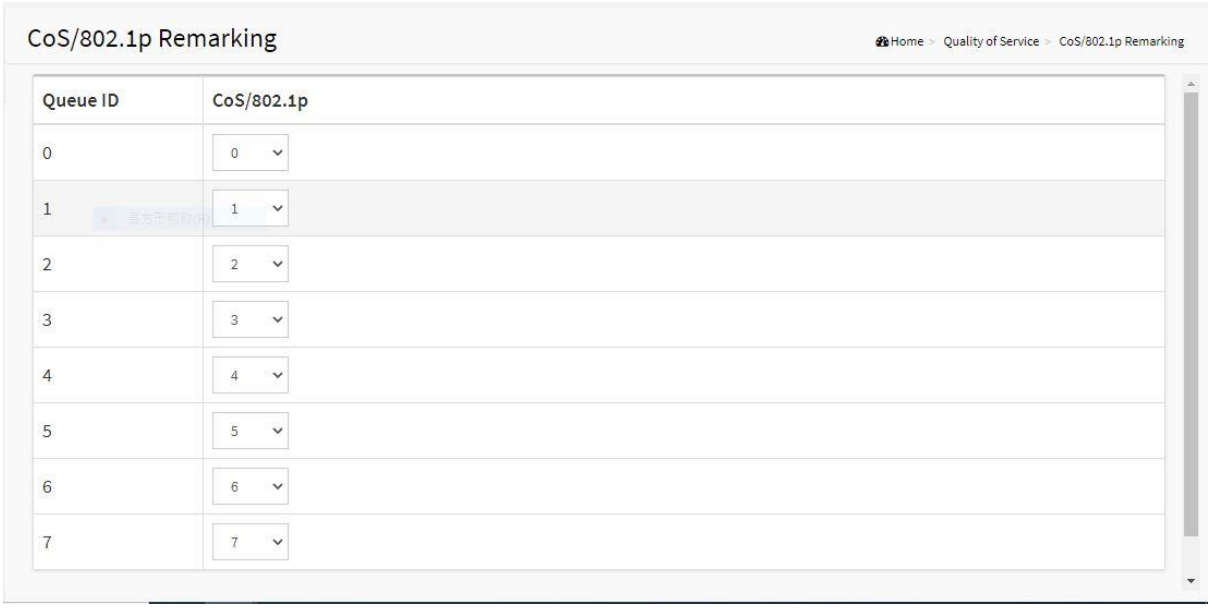


Figure 49 :CoS/802.1p Remarking

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.

Chapter 12 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.

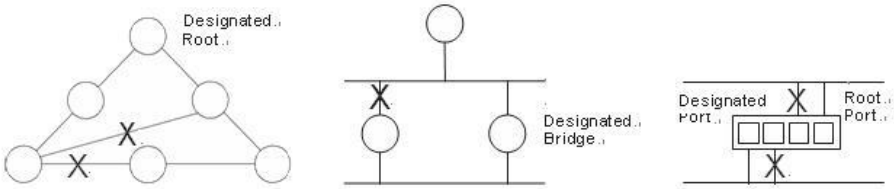


Figure 51: The Spanning Tree Protocol

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.

12-1 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.

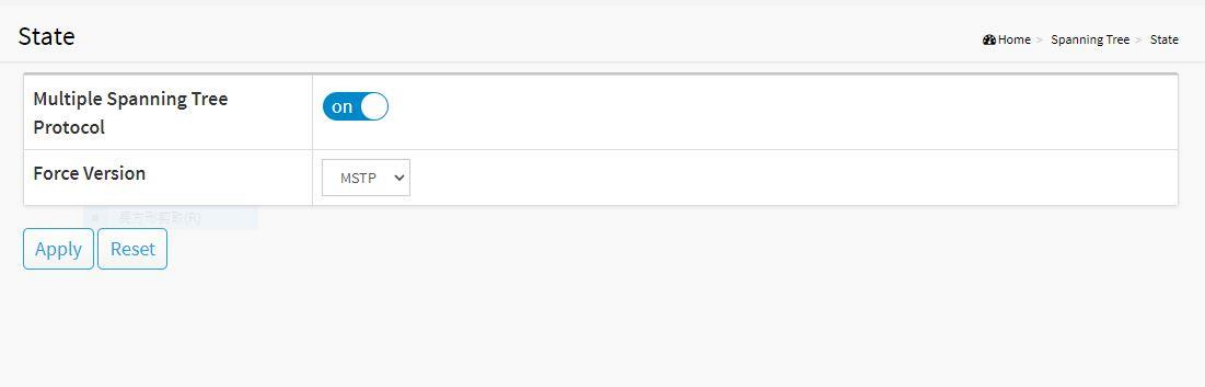


Figure 52: State

Parameter Description:

- **Multiple Spanning Tree Protocol**

  To enable/disable spanning tree protocol.

- **Force Version**

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

12-2 Region Config

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.

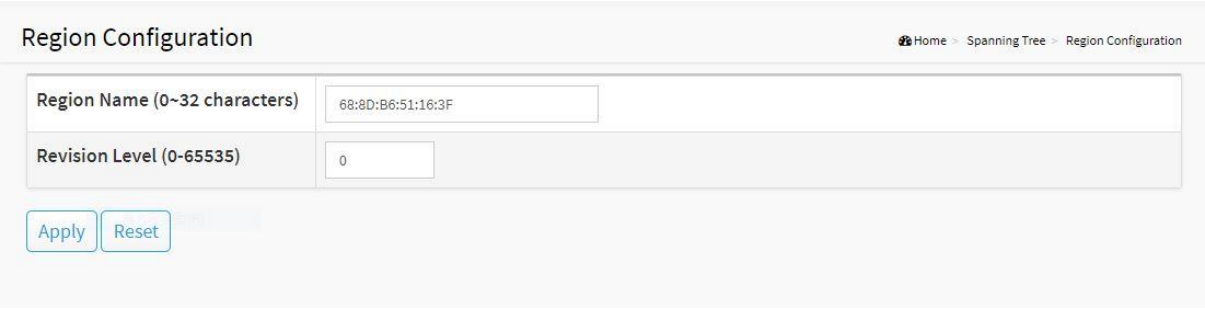


Figure 53: Region Config

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.

12-3 Instance View

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.

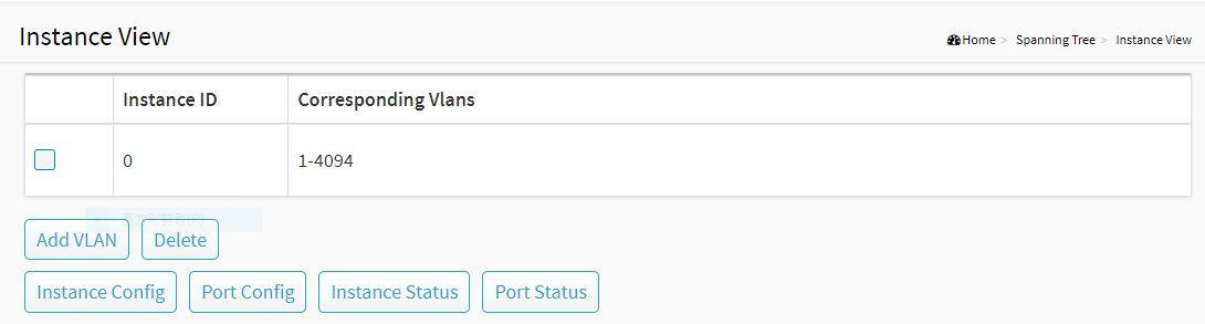


Figure 54: MSTP Instance Config

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

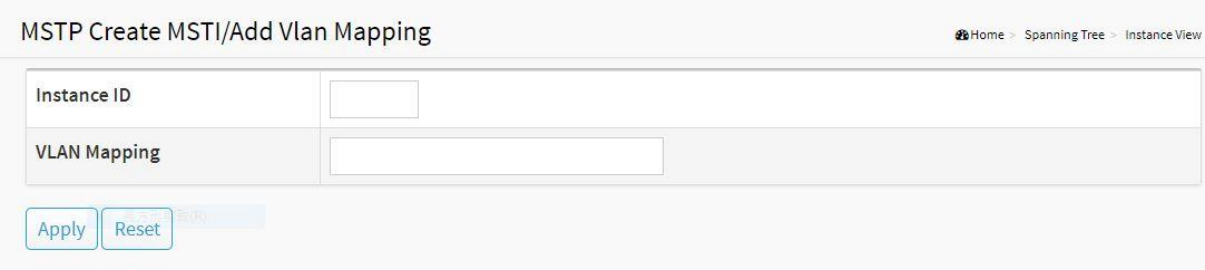


Figure 55: Add VLAN

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)

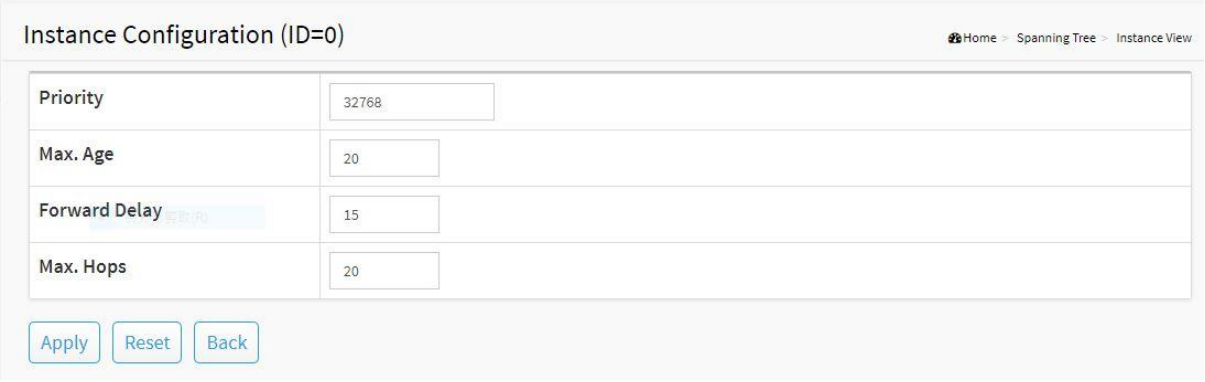


Figure 56: Instance Config (ID 0)

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)

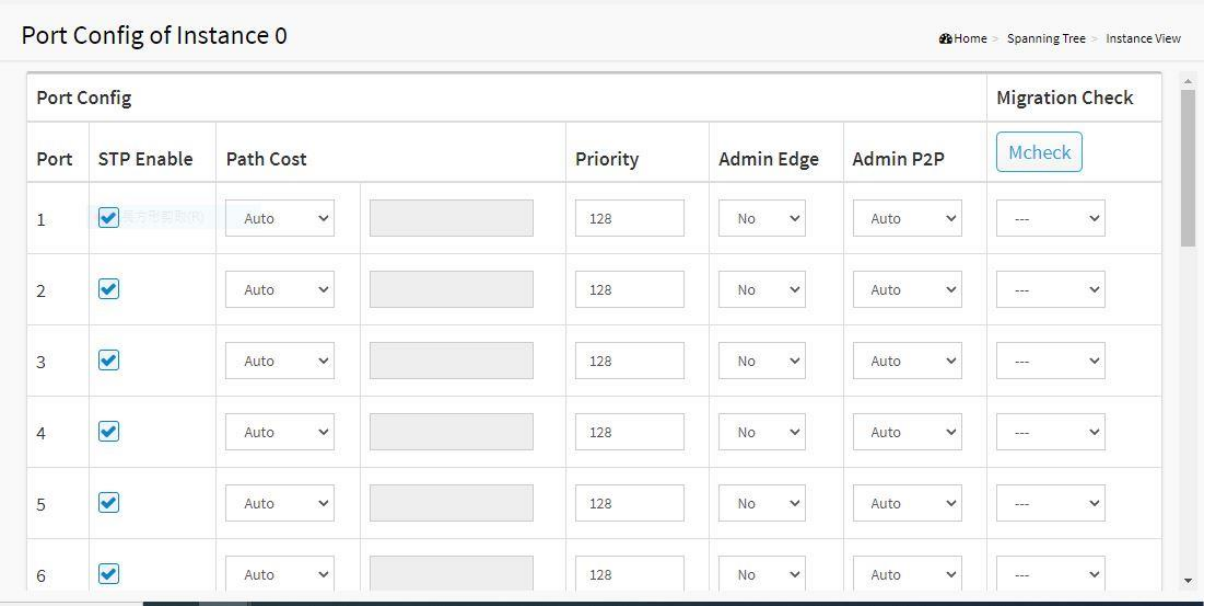


Figure 57: Port Config (ID 0)

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**

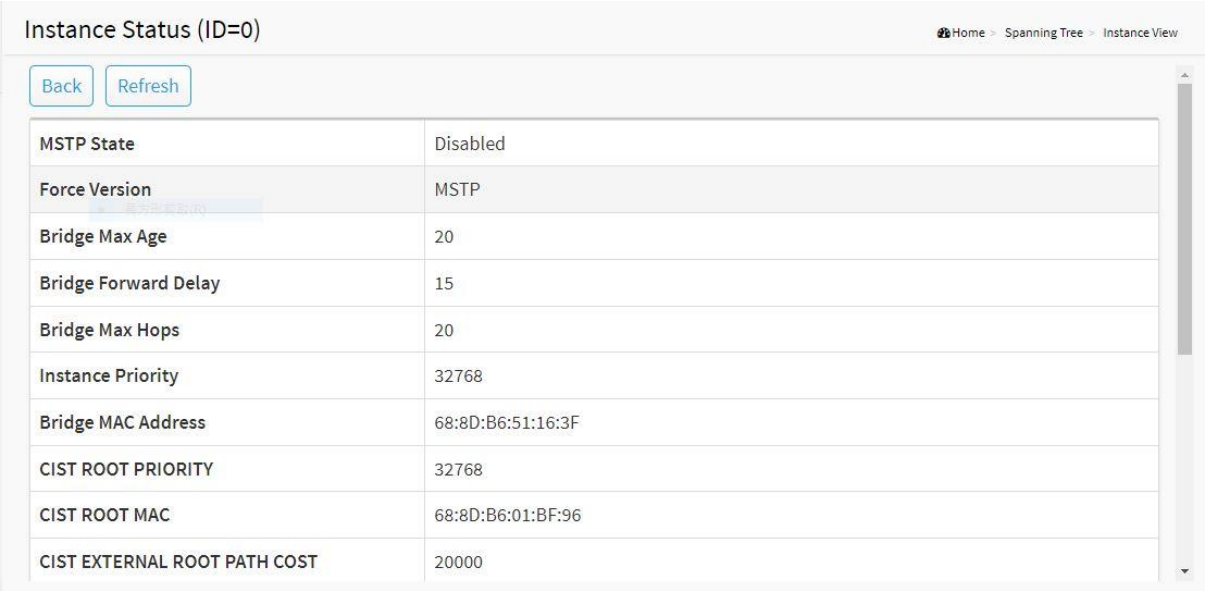
  Auto / True / False

  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)



MSTP State	Disabled
Force Version	MSTP
Bridge Max Age	20
Bridge Forward Delay	15
Bridge Max Hops	20
Instance Priority	32768
Bridge MAC Address	68:8D:B6:51:16:3F
CIST ROOT PRIORITY	32768
CIST ROOT MAC	68:8D:B6:01:BF:96
CIST EXTERNAL ROOT PATH COST	20000

Figure 58: 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.

Port Status (ID=0)

Port Status of Instance 0

Home > Spanning Tree > Instance View

Back Refresh

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 59: 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**

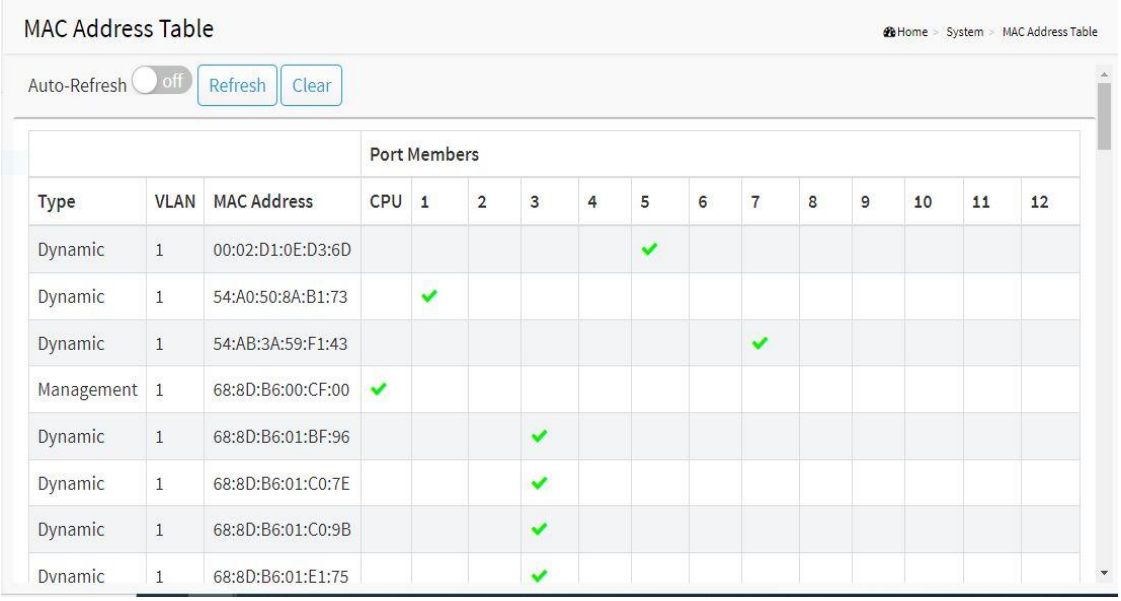
  Whether or not a port is a Point-to-Point Port in reality.

Chapter 13 MAC Address Table

The MAC address table page displays all MAC address entries on the switch including static MAC address created by administrator or auto learned from hardware.

Web Interface

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



			Port Members												
Type	VLAN	MAC Address	CPU	1	2	3	4	5	6	7	8	9	10	11	12
Dynamic	1	00:02:D1:0E:D3:6D						✔							
Dynamic	1	54:A0:50:8A:B1:73		✔											
Dynamic	1	54:AB:3A:59:F1:43								✔					
Management	1	68:8D:B6:00:CF:00	✔												
Dynamic	1	68:8D:B6:01:BF:96				✔									
Dynamic	1	68:8D:B6:01:C0:7E				✔									
Dynamic	1	68:8D:B6:01:C0:9B				✔									
Dynamic	1	68:8D:B6:01:E1:75				✔									

Figure 60: MAC Address Table

Parameter Description:

- **VLAN**

  VLAN ID of the MAC address

- **MAC Address**

  MAC address

- **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.

- **Port**

  Type of Port

  · CPU: DUT's CPU port for management purpose

  · Other: Normal switch port

- **Clear Dynamic[Button]**

  To clear all dynamic entries.

- **Refresh[Button]**

  To retrieve latest MAC address entries shown on this page.

Chapter 14 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.

14-1 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.

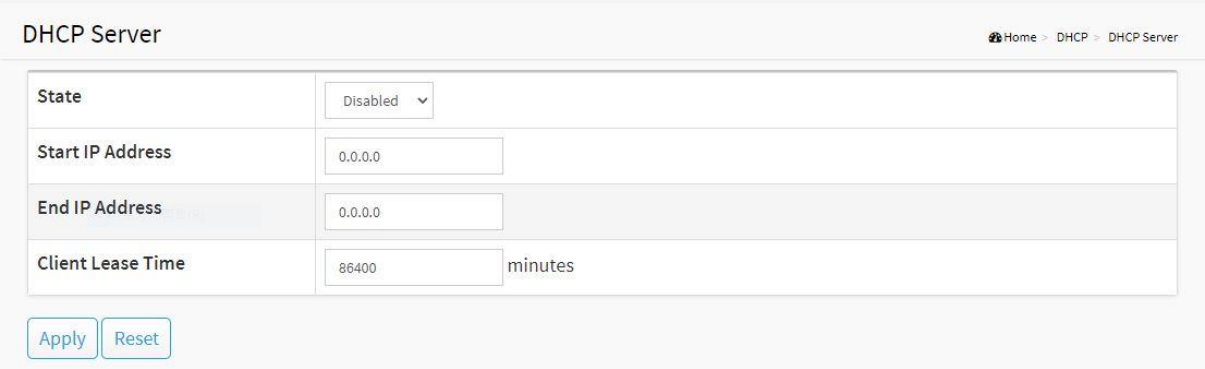


Figure 61: DHCP Server

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 15 Diagnostics

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

15-1 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.

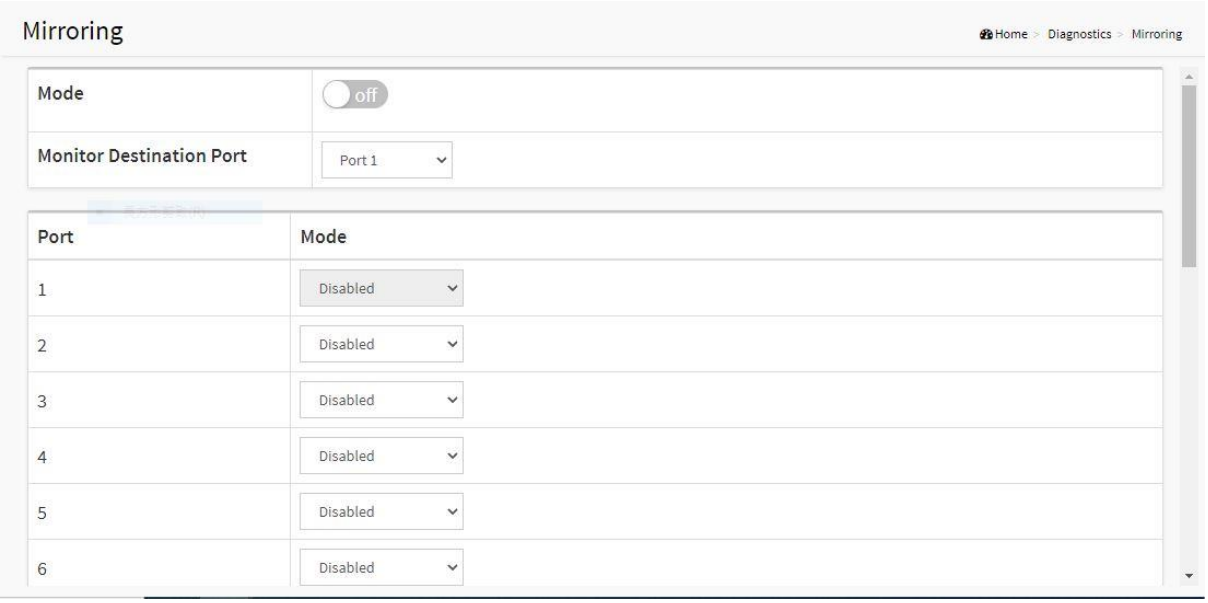


Figure 62: Mirroring

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.

15-2 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.

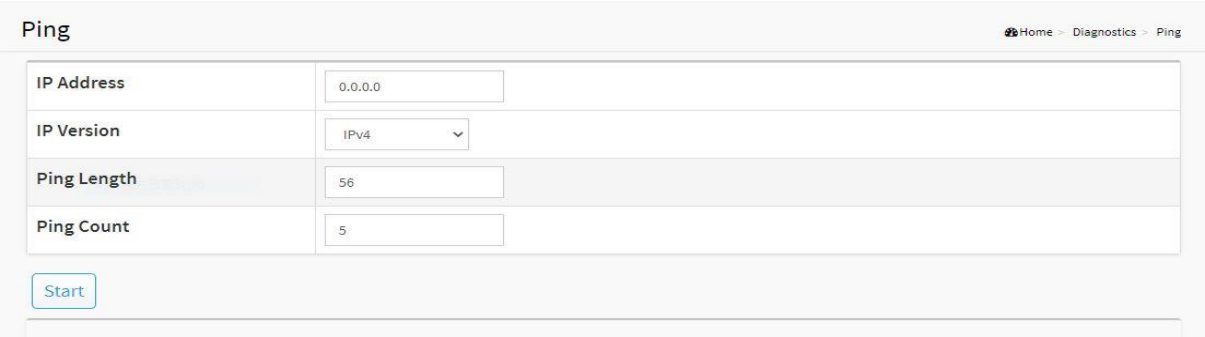


Figure 63: Ping

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.

15-3 LAN Cable Diagnostics

This section shows how to run LAN Cable Diagnostics for copper ports.

Web Interface

To configure a LAN Cable Diagnostics Configuration in the web interface:

1. Click Diagnostics -> Cable Diagnostics.
2. Specify Port which you want to check.
3. Click Cable Test.

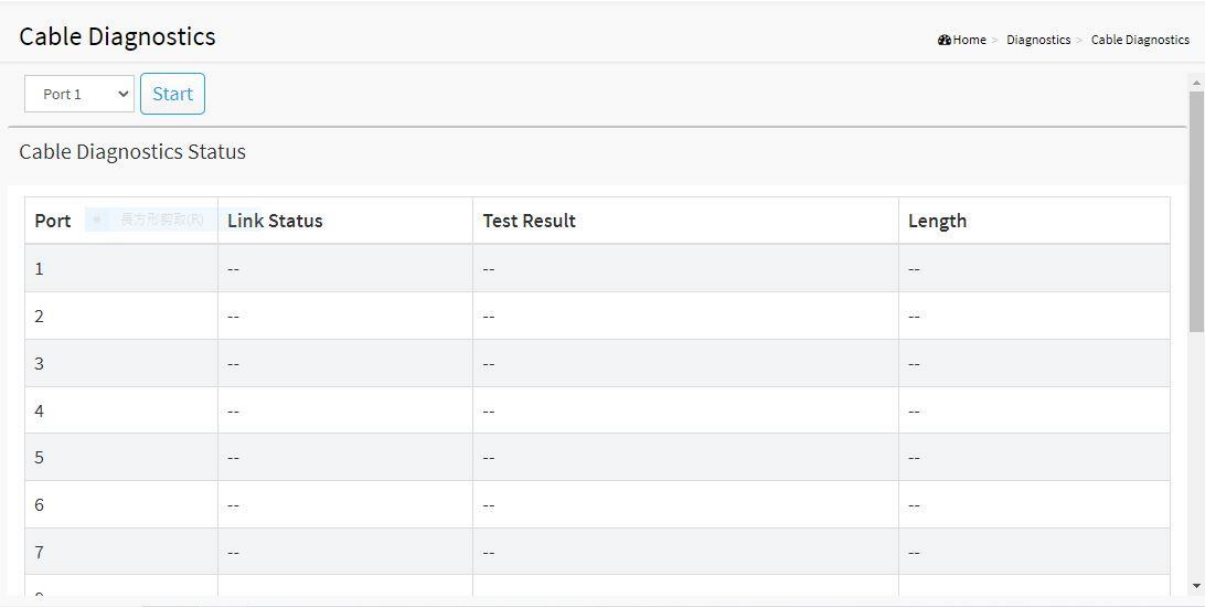


Figure 64: LAN Cable Diagnostics

Parameter Description:

- **Port**

  The port where you are requesting Cable Diagnostics.

- **Result**
  The status of copper test. It include:
  · OK: Correctly terminated pair
  · Short Cable: A short circuit was detected on the twisted pair.
  · Open Cable: Opening pair. One scenario is the cable doesn't plug to the link partner.
  · Impedance mismatch: The normal impedance should be 100Ω, impedance mismatch is detected if the impedance measured is not in the range 70Ω~130Ω.
  · Line Drive: The high impedance is detected. One scenario is the cable plug to a power down link partner.

- **Length**
  Distance in meter from the port to the location on the cable where the fault was discovered.

Chapter 16 Maintenance

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

16-1 Configuration

16-1.1 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.

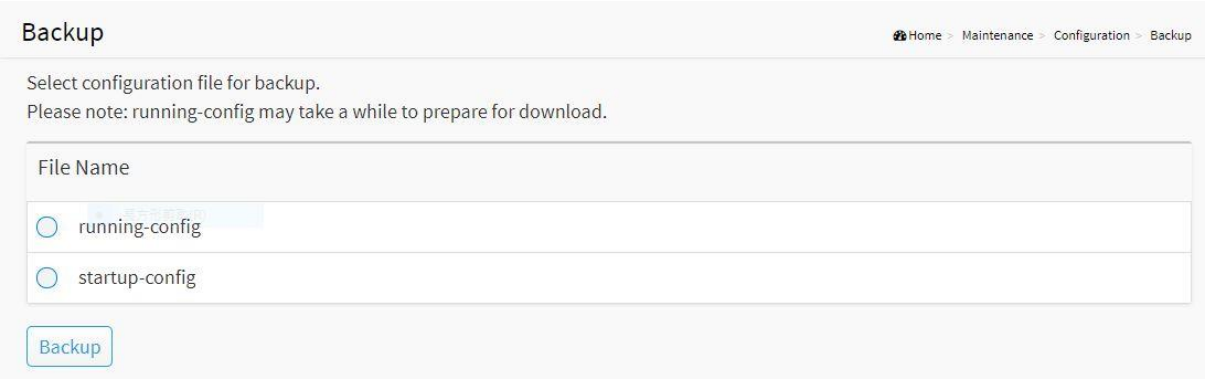


Figure 65: Backup / Restore

Parameter Description:

- **Backup[Button]**

  Set port enable/disable.

- **Restore[Button]**

  Set port enable/disable.

16-2 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.

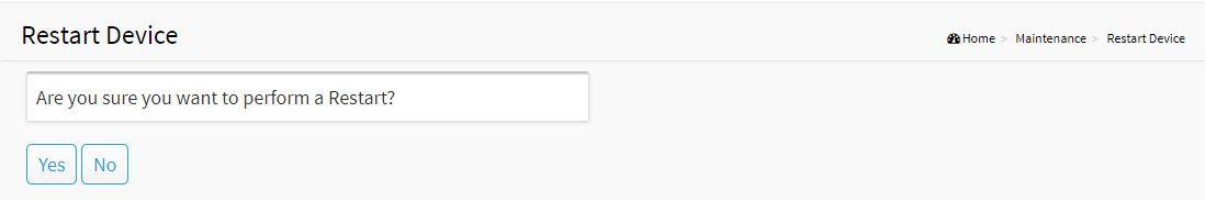


Figure 66: Restart Device

Parameter Description:

- **Yes[Button]**

  To restart device

16-3 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.

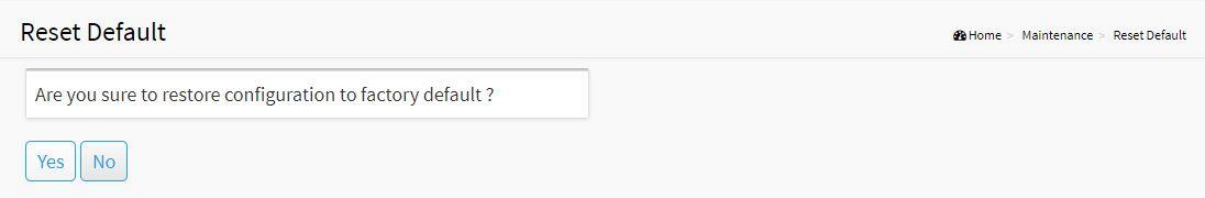


Figure 67: Reset Default

Parameter Description:

- **Yes[Button]**

  To reset the device to factory default value.

16-4 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 68: 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.

16-5 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:

4. Click Maintenance -> Firmware -> Firmware Selection.
5. Choose the firmware version you want to use.
6. Click Activate.

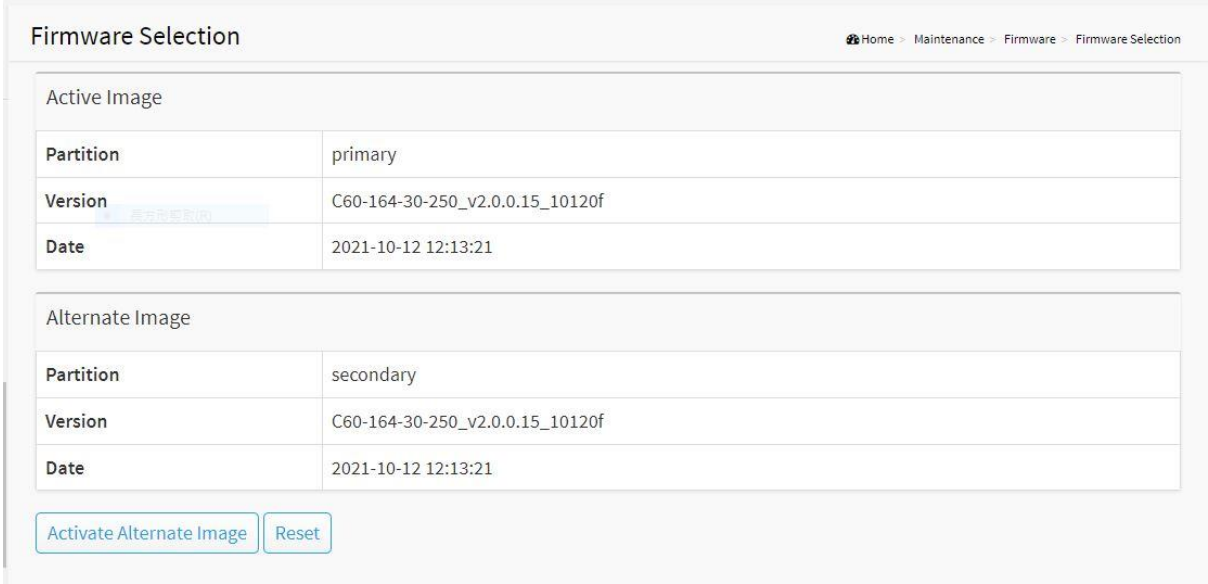


Figure 69: Firmware Upgrade

Parameter Description:

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

  Reset the setting.