User`s Manual

Cross-48/HPoE (II)

CROSS-48/HPOE (II) rev.2
GUI User Guide

52-Ports L2+ Managed GbE PoE+ Switch

Release A1

About This Manual

Copyright

The products and programs described in this User Guide are licensed products of Manufacture Technology, 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 Manufacture Technology.

.

Purpose

This GUI user guide gives specific information on how to operate and use the management functions of the CROSS-48/HPOE (II) via HTTP/HTTPs 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

Manufacture Technology 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

Revision History

Release	Date	Revision
Initial Release	2018/09/10	A1

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 CROSS-48/HPOE (II) 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 CROSS-48/HPOE (II) are the next generation Industrial L2+ managed GbE PoE+ switch from Manufacture, 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.

CROSS-48/HPOE (II) L2+ Managed GbE PoE+ Switch provide 52 ports in a single device; the specification is highlighted as follows.

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

Overview of this User Guide

- Chapter 1 “Operation of Web-based Management”
- Chapter 2 “System”
- Chapter 3 “Port Management”
- Chapter 4 “PoE Management”
- Chapter 5 “VLAN Management”
- Chapter 6 “Quality of Service”
- Chapter 7 “Spanning tree”
- Chapter 8 “MAC Address Tables”
- Chapter 9 “Multicast”
- Chapter 10 “DHCP”
- Chapter 11 “Security”
- Chapter 12 “Access Control”
- Chapter 13 “SNMP”
- Chapter 14 “MEP”
- Chapter 15 “ERPS”
- Chapter 16 “PTP”
- Chapter 17 “Event Notification”
- Chapter 18 “Diagnostics”
- Chapter 19 “Maintenance”

Ordering information

- Variable N=52
- Variable Y=48

Chapter 1 Operation of Web-based Management

Initial Configuration

This chapter instructs you how to configure and manage the CROSS-48/HPOE (II) 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 MIBs status, each port activity, Spanning tree status, port aggregation status, multicast traffic, VLAN and priority status, even illegal access record and so on.

The default values of the CROSS-48/HPOE (II) are listed in the table below:

IP Address	192.168.1.1
Subnet Mask	255.255.255.0
Default Gateway	192.168.1.254
Username	Admin
Password	1234

After the CROSS-48/HPOE (II) has been finished configuration it interface, you can browse it. For instance, type **http://192.168.1.1** in the address row in a browser, it will show the following screen and ask you inputting username and password in order to login and access authentication.

The default username is **"Admin"** and password is **1234**. 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 CROSS-48/HPOE (II) will not give you a shortcut to username automatically. This looks inconvenient, but safer.

In the CROSS-48/HPOE (II), allowed two or more users using administrator's identity to manage this switch, which administrator to do the last setting, it will be an available configuration to effect the system.

NOTE:

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

When you login CROSS-48/HPOE (II) series switch Web UI management, you can use both ipv4 ipv6 login to manage

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

NOTE:

AS CROSS-48/HPOE (II) the function enable dhcp, so If you do not have DHCP server to provide ip addresses to the switch, the Switch **default ip 192.168.1.1**

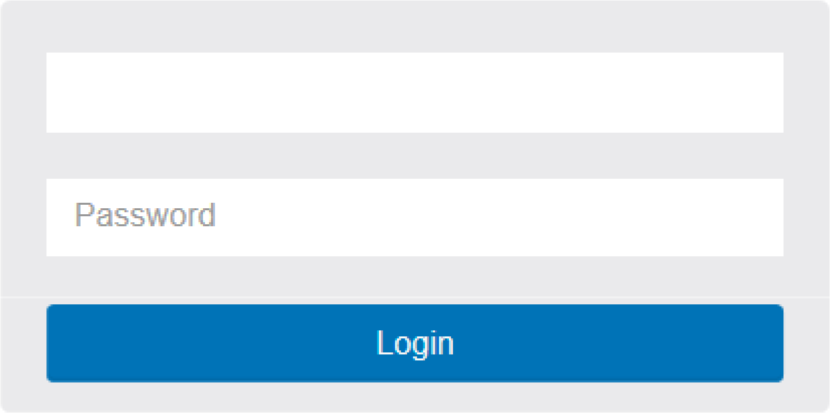


Figure 1: The login page

Chapter 2 System

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

2-1 System Information

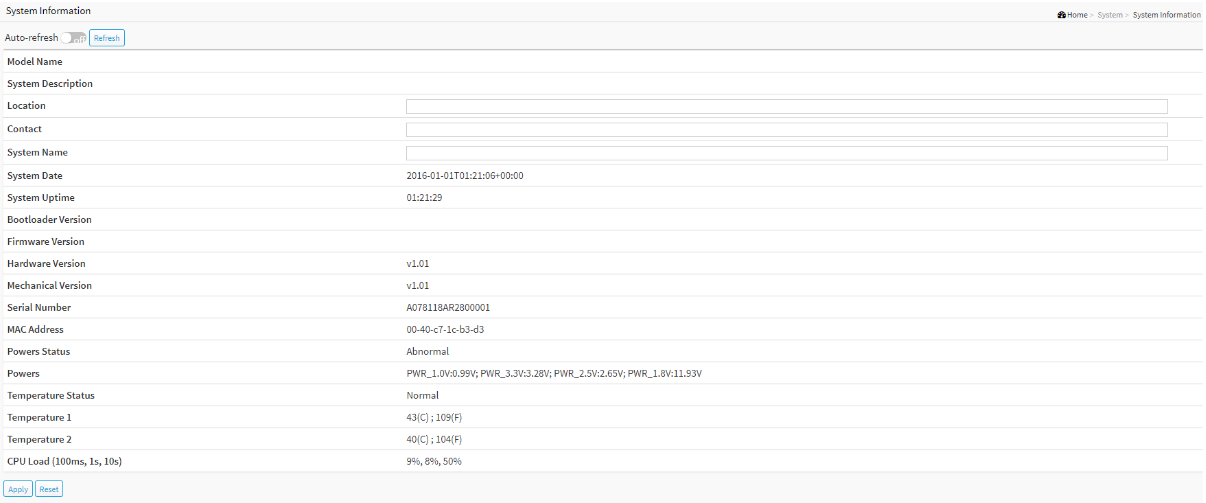
You can identify the system by configuring system name, location and the contact of the switch.

The switch system's contact information is provided here.

Web interface

To configure System Information in the web interface:

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



System Information

Home > System > System Information

Auto-refresh ○off Refresh

Model Name	
System Description	
Location	
Contact	
System Name	
System Date	2016-01-01T01:21:06+00:00
System Uptime	01:21:29
Bootloader Version	
Firmware Version	
Hardware Version	v1.01
Mechanical Version	v1.01
Serial Number	A078118AR2800001
MAC Address	00-40-c7-1c-b3-d3
Powers Status	Abnormal
Powers	PWR_1.0V:0.99V; PWR_3.3V:3.28V; PWR_2.5V:2.65V; PWR_1.8V:11.93V
Temperature Status	Normal
Temperature 1	43(C) ; 109(F)
Temperature 2	40(C) ; 104(F)
CPU Load (100ms, 1s, 10s)	9%, 8%, 50%

Apply Reset

Figure 2-1: System Information

Parameter description:

- **Model Name :**

  Displays the factory defined model name for identification purpose.

- **System Description :**

  Displays the system description.

- **Location :**

  The system location configured in Configuration | System | Information | System Location.

- **Contact :**

  The system contact configured in Configuration | System | Information | System Contact.

- **System name :**

  Displays the user-defined system name that configured in System | System Information | Configuration | System Name.

- **System Date :**

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

- **System Uptime :**

  The period of time the device has been operational.

- **Bootloader Version :**

  Displays the current boot loader version number.

- **Firmware Version :**

  The software version of this switch.

- **Hardware Version :**

  Displays the hardware version of the device.

- **Mechanical Version :**

  Displays the mechanical version of the device.

- **Series Number :**

  The serial number of this switch.

- **MAC Address :**

  The MAC Address of this switch.

- **Powers Status :**

  Displays the powers status of the system.

- **Powers :**

  Displays the powers of the system.

- **Temperature Status :**

  Displays the temperature status of the system.

- **Temperature 1 :**

  Displays the temperature 1 of the system.

- **Temperature 2 :**

  Displays the temperature 2 of the system.

- **CPU Load (100ms, 1s, 10s) :**

  Displays the cpu loading(100ms, 1s, 10s) of the system.

Buttons

- **Apply :**

  Click to save changes.

- **Reset :**

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

- **Refresh :**

Click to refresh the page immediately.

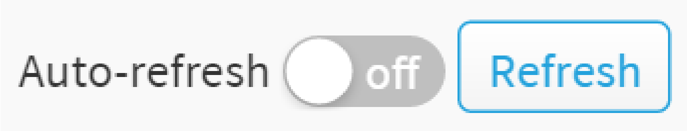


Figure 2-1: The System Information buttons

- **Auto-refresh :**

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

2-2 IP Address

2-2.1 Settings

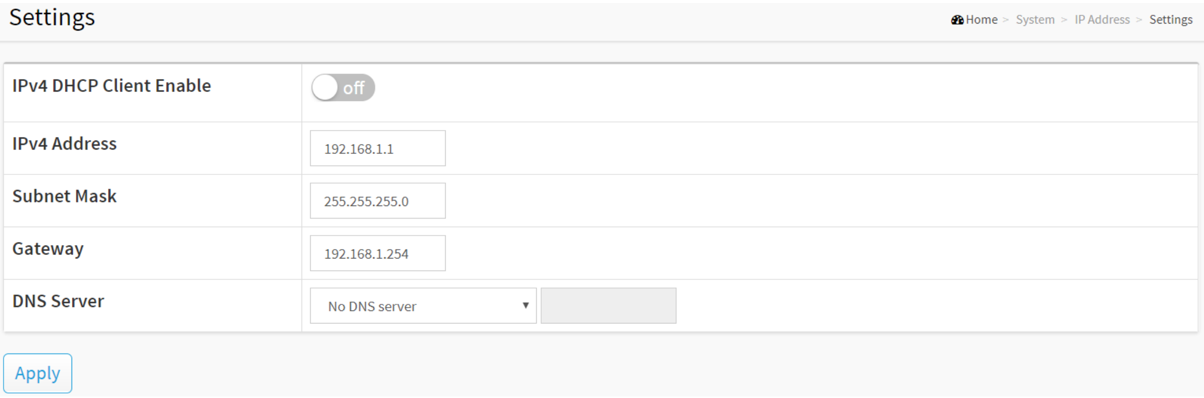
The IPv4 address for the switch could be obtained via DHCP Server for VLAN 1. To manually configure an address, you need to change the switch's default settings to values that are compatible with your network. You may also need to establish a default gateway between the switch and management stations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

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

Web Interface

To configure an IP Settings in the web interface:

1. Click System, IP Address and Settings.
2. Enable or Disable the IPv4 DHCP Client.
3. Specify the IPv4 Address, Subnet Mask, Gateway.
4. Select DNS Server.
5. Click Apply



Settings

IPv4 DHCP Client Enable	off
IPv4 Address	192.168.1.1
Subnet Mask	255.255.255.0
Gateway	192.168.1.254
DNS Server	No DNS server

Figure 2-2.1: The IP settings

Parameter description:

- **IPv4 DHCP Client Enable :**

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

- **IPv4 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 :**

  The IPv4 network mask, in number of bits (prefix length). Valid values are between 0 and 30 bits for a IPv4 address.
  If DHCP is enabled, this field configures the fallback address network mask. The field may be left blank if IPv4 operation on the interface is not desired - or no DHCP fallback address is desired.

- **Gateway :**

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

- **DNS Server :**

  This setting controls the DNS name resolution done by the switch.
  There are four servers available for configuration, and the index of the server presents the preference (less index has higher priority) in doing DNS name resolution.
  The following modes are supported:

  - No DNS server

    No DNS server will be used.

  - Configured IPv4

    Explicitly provide the valid IPv4 unicast address of the DNS Server in dotted decimal notation.
    Make sure the configured DNS server could be reachable (e.g. via PING) for activating DNS service.

  - Configured IPv6

    Explicitly provide the valid IPv6 unicast (except linklocal) address of the DNS Server.
    Make sure the configured DNS server could be reachable (e.g. via PING6) for activating DNS service.

  - From any DHCPv4 interfaces

    The first DNS server offered from a DHCPv4 lease to a DHCPv4-enabled interface will be used.

  - From this DHCPv4 interface

    Specify from which DHCPv4-enabled interface a provided DNS server should be preferred.

  - From any DHCPv6 interfaces

    The first DNS server offered from a DHCPv6 lease to a DHCPv6-enabled interface will be used.

  - From this DHCPv6 interface

    Specify from which DHCPv6-enabled interface a provided DNS server should be preferred.

Buttons

- **Apply :**

  Click to save changes.

2-2.2 Advanced Settings

Configure the switch-managed IP information on this page

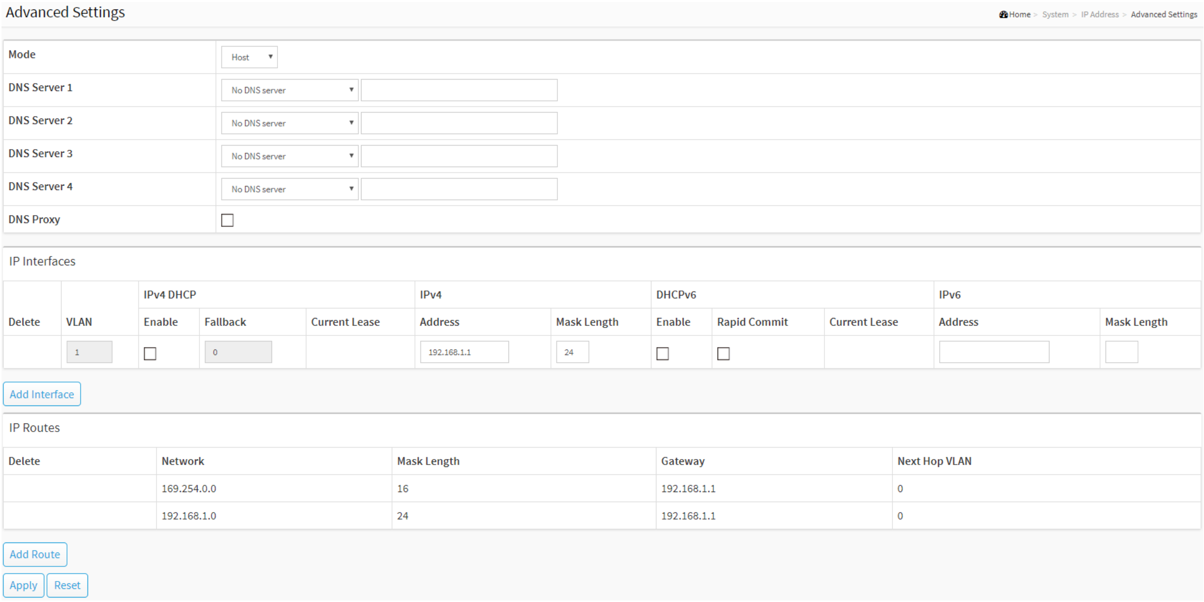
Configure IP basic settings, control IP interfaces and IP routes.

The maximum number of interfaces supported is 128 and the maximum number of routes is 128.

Web Interface

To configure an Advanced Settings in the web interface:

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



Advanced Settings

Mode	Host ▾
DNS Server 1	No DNS server ▾
DNS Server 2	No DNS server ▾
DNS Server 3	No DNS server ▾
DNS Server 4	No DNS server ▾
DNS Proxy	□

IP Interfaces

		IPv4 DHCP			IPv4		DHCPv6			IPv6	
Delete	VLAN	Enable	Fallback	Current Lease	Address	Mask Length	Enable	Rapid Commit	Current Lease	Address	Mask Length
	1	□	0		192.168.1.1	24	□	□			

IP Routes

Delete	Network	Mask Length	Gateway	Next Hop VLAN
	169.254.0.0	16	192.168.1.1	0
	192.168.1.0	24	192.168.1.1	0

Figure 2-2.2: The advanced IP settings

Parameter description:

Basic Setting

- **Mode :**

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

- **DNS Server :**

  This setting controls the DNS name resolution done by the switch. There are four servers available for configuration, and the index of the server presents the preference (less index has higher priority) in doing DNS name resolution. The following modes are supported:

  - No DNS server

    No DNS server will be used.

  - Configured IPv4

    Explicitly provide the valid IPv4 unicast address of the DNS Server in dotted decimal notation.
    Make sure the configured DNS server could be reachable (e.g. via PING) for activating DNS service.

  - Configured IPv6

    Explicitly provide the valid IPv6 unicast (except linklocal) address of the DNS Server.
    Make sure the configured DNS server could be reachable (e.g. via PING6) for activating

DNS service.

- From any DHCPv4 interfaces

  The first DNS server offered from a DHCPv4 lease to a DHCPv4-enabled interface will be used.

- From this DHCPv4 interface

  Specify from which DHCPv4-enabled interface a provided DNS server should be preferred.

- From any DHCPv6 interfaces

  The first DNS server offered from a DHCPv6 lease to a DHCPv6-enabled interface will be used.

- From this DHCPv6 interface

  Specify from which DHCPv6-enabled interface a provided DNS server should be preferred.

- **DNS Proxy :**

  When DNS proxy is enabled, system will relay DNS requests to the currently configured DNS server, and reply as a DNS resolver to the client devices on the network. Only IPv4 DNS proxy is now supported.

IP Interfaces

- **Delete :**

  Select this option to delete an existing IP interface.

- **VLAN :**

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

- **IPv4 DHCP Enabled :**

  Enable the DHCP client by checking this box. If this option is enabled, the system will configure the IPv4 address and mask of the interface using the DHCP protocol.

- **IPv4 DHCP Fallback Timeout :**

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

- **IPv4 DHCP Current Lease :**

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

- **IPv4 Address :**

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

- **IPv4 Mask Length :**

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

- **DHCPv6 Enable**

Enable the DHCPv6 client by checking this box. If this option is enabled, the system will configure the IPv6 address of the interface using the DHCPv6 protocol.

- **DHCPv6 Rapid Commit**

  Enable the DHCPv6 Rapid-Commit option by checking this box. If this option is enabled, the DHCPv6 client terminates the waiting process as soon as a Reply message with a Rapid Commit option is received.
  This option is only manageable when DHCPv6 client is enabled.

- **DHCPv6 Current Lease**

  For DHCPv6 interface with an active lease, this column shows the interface address provided by the DHCPv6 server.

- **IPv6 Address :**

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

- **IPv6 Mask Length :**

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

IP Routes

- **Delete :**

  Select this option to delete an existing IP route.

- **Network :**

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

- **Mask Length :**

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

- **Gateway :**

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

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

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

Buttons

- **Add Interface :**

  Click to add a new IP interface. A maximum of 128 interfaces is supported.

- **Add Route :**

  Click to add a new IP route. A maximum of 128 routes is supported.

- **Apply :**

  Click to save changes.

- **Reset :**

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

2-2.3 Status

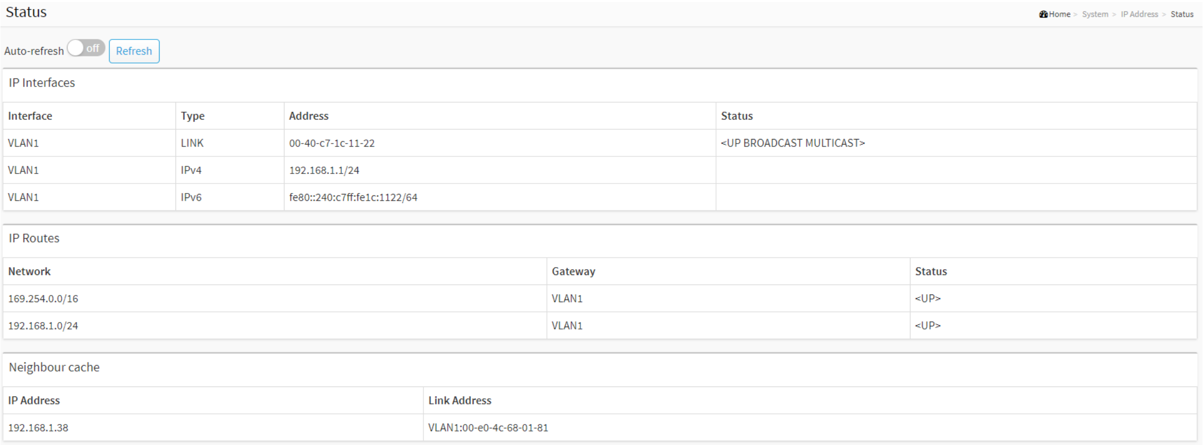
2-2.3.1 IP Status

This page displays the status of the IP protocol layer. The status is defined by the IP interfaces, the IP routes and the neighbour cache (ARP cache) status.

Web Interface

To display the log configuration in the web interface:

1. Click System, IP Address, Status and IP Status.
2. Display the IP Configuration information.



Status

IP Interfaces

Interface	Type	Address	Status
VLAN1	LINK	00-40-c7-1c-11-22	<UP BROADCAST MULTICAST>
VLAN1	IPv4	192.168.1.1/24	
VLAN1	IPv6	fe80::240:c7ff:fe1c:1122/64	

IP Routes

Network	Gateway	Status
169.254.0.0/16	VLAN1	<UP>
192.168.1.0/24	VLAN1	<UP>

Neighbour cache

IP Address	Link Address
192.168.1.38	VLAN1:00-e0-4c-68-01-81

Figure 2-2.3.1: The IP Status

Parameter description:

IP Interfaces

- **Interface :**

  Show the name of the interface.

- **Type :**

  Show the address type of the entry. This may be LINK or IPv4.

- **Address :**

  Show the current address of the interface (of the given type).

- **Status :**

  Show the status flags of the interface (and/or address).

IP Routes

- **Network :**

  Show the destination IP network or host address of this route.

- **Gateway :**

  Show the gateway address of this route.

- **Status :**

  Show the status flags of the route.

Neighbour cache

- **IP Address :**

  Show the IP address of the entry.

- **Link Address :**

  Show the Link (MAC) address for which a binding to the IP address given exist.

Buttons

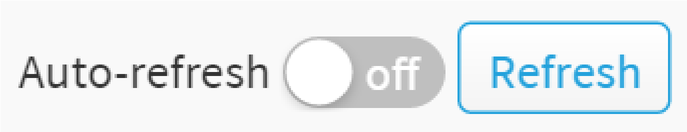


Figure 2-2.3.1: The IP Status buttons

- **Auto-refresh :**

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

- **Refresh :**

  Click to refresh the page immediately.

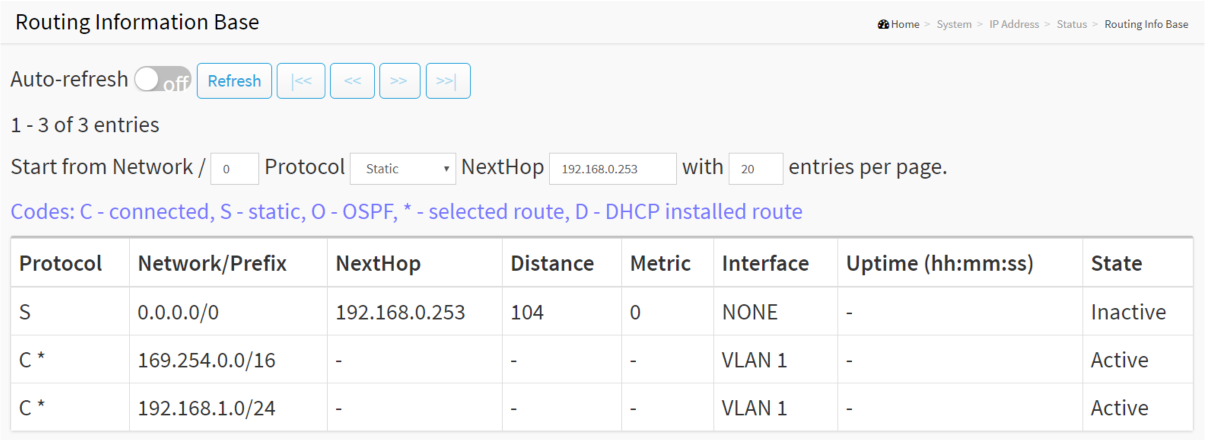
2-2.3.2 Routing Info Base

Each page shows up to 999 table entries, selected through the "entries per page" input field. When first visited, the web page will show the beginning entries of this table.

Web Interface

To display the log configuration in the web interface:

1. Click System, IP Addres, Status and Routing Info Base.
2. Display the Routing Info Base information.



Routing Information Base

1 - 3 of 3 entries

Start from Network / 0 Protocol Static NextHop 192.168.0.253 with 20 entries per page.

Codes: C - connected, S - static, O - OSPF, * - selected route, D - DHCP installed route

Protocol	Network/Prefix	NextHop	Distance	Metric	Interface	Uptime (hh:mm:ss)	State
S	0.0.0.0/0	192.168.0.253	104	0	NONE	-	Inactive
C *	169.254.0.0/16	-	-	-	VLAN 1	-	Active
C *	192.168.1.0/24	-	-	-	VLAN 1	-	Active

Figure 2-2.3.2: The Routing Information Base

Parameter description:

- **Start from ID :**

  Input field allow the user to change the starting point in this table.

- **Protocol :**

  The protocol of the route.
  DHCP: The route is created by DHCP.
  Connected: The destination network is connected directly.
  Static: The route is created by user.
  OSPF: The route is created by OSPF.

- **Network/Prefix**

  Network and prefix (example 10.0.0.0/16) of the given route entry.

- **NextHop**

  The IP address of nexthop. Value '0.0.0.0' indicates the link is directly connected.

- **Distance**

  The distance of the route.

- **Metric**

  The metric of the route.

- **Interface**

  The interface where the ip packet is outgoing.

- **Uptime (hh:ss:mm)**

The time till the route is created. The unit is second.

- **State**

  Indicate if the destination network is reachable or not.

Buttons

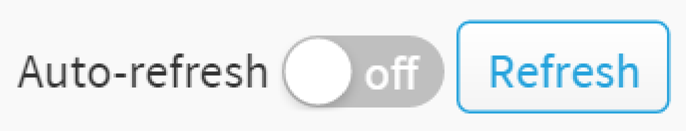


Figure 2-2.3.1: The IP Status buttons

- **Auto-refresh :**

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

- **Refresh :**

  Click to refresh the page immediately.

- **First Page :**

  Updates the system log entries, turn to the first page.

- **Next Page :**

  Updates the system log entries, turn to the next page.

- **First Entry :**

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

- **Next Entry :**

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

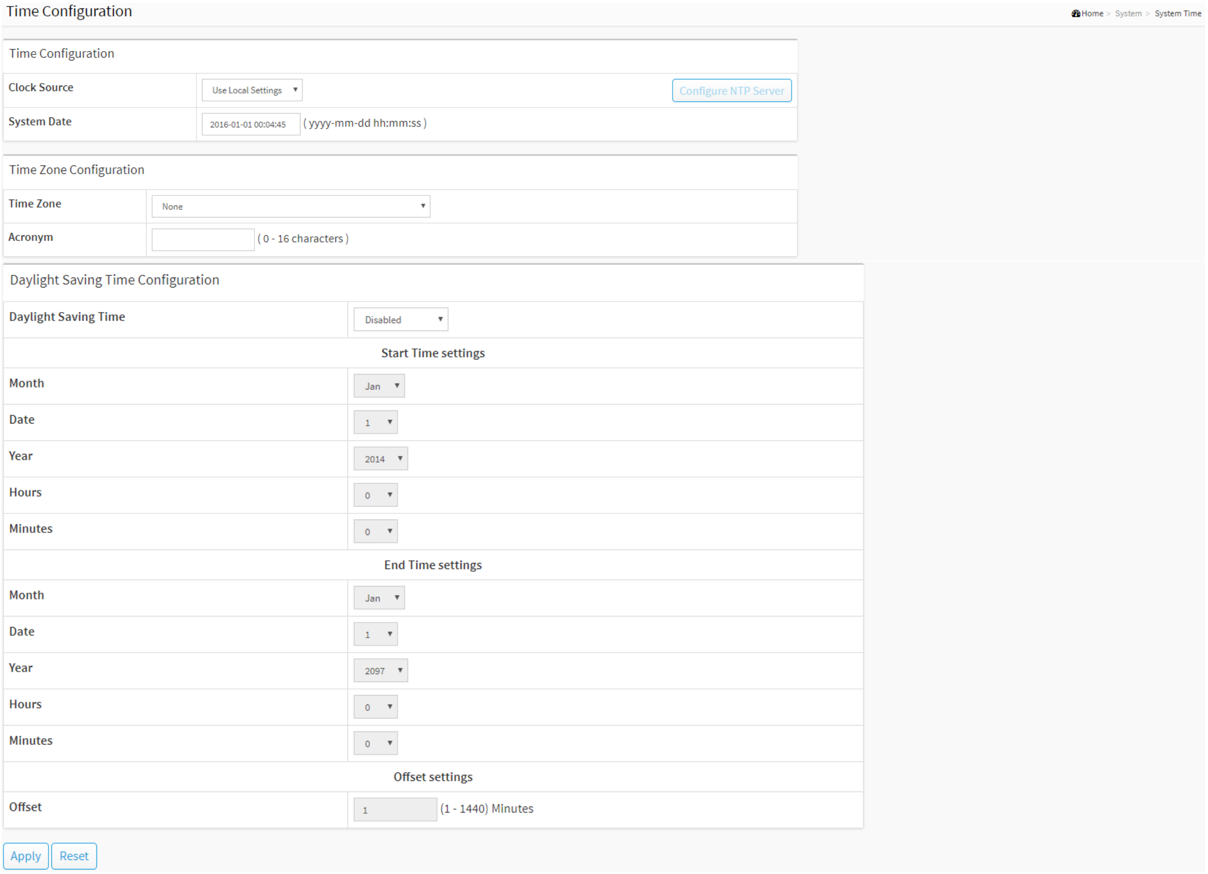
2-3 System Time

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

Web Interface

To configure Time in the web interface:

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



Time Configuration

Time Configuration	
Clock Source	Use Local Settings
System Date	2016-01-01 00:04:45 (yyyy-mm-dd hh:mm:ss)

Time Zone Configuration	
Time Zone	None
Acronym	(0 - 16 characters)

Daylight Saving Time Configuration	
Daylight Saving Time	Disabled
Start Time settings	
Month	Jan
Date	1
Year	2014
Hours	0
Minutes	0
End Time settings	
Month	Jan
Date	1
Year	2097
Hours	0
Minutes	0
Offset settings	
Offset	1 (1 - 1440) Minutes

Figure 2-3: The time configuration

Parameter description:

Time Configuration

- **Clock Source :**

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

- **System Date :**

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

Time Zone Configuration

- **Time Zone :**

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

- **Acronym :**

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

Daylight Saving Time Configuration

- **Daylight Saving Time :**

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

- **Start time settings :**

  Week - Select the starting week number.

  Day - Select the starting day.

  Month - Select the starting month.

  Hours - Select the starting hour.

  Minutes - Select the starting minute.

- **End time settings :**

  Week - Select the ending week number.

  Day - Select the ending day.

  Month - Select the ending month.

  Hours - Select the ending hour.

  Minutes - Select the starting minute.

- **Offset settings :**

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

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

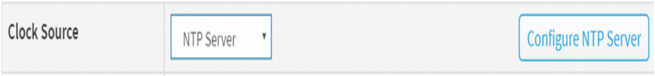
Buttons

- **Apply :**

  Click to save changes.

- **Reset :**

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

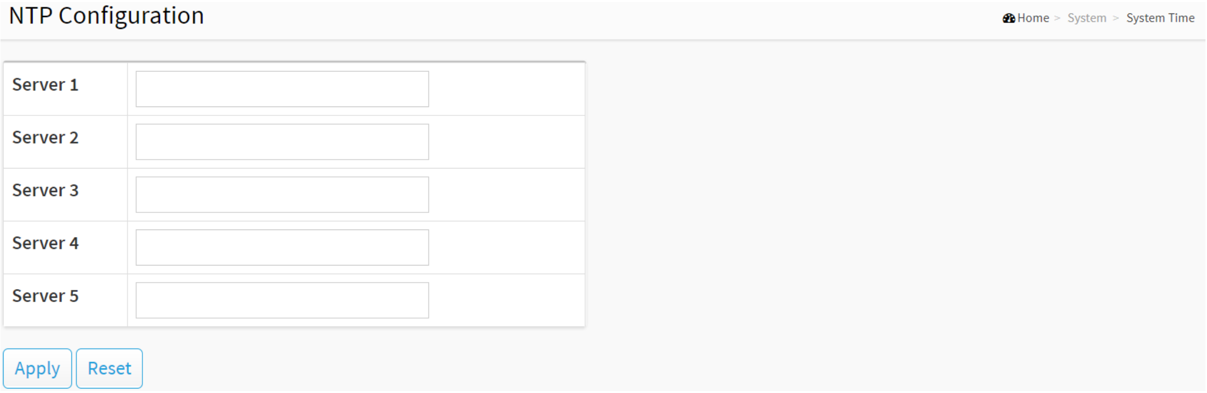


Clock Source: NTP Server

Figure 2-3: The Configure NTP Server button

- **Configure NTP Server :**

  Click to configure NTP server, When Clock Source select from NTP Server.



NTP Configuration

Server 1	
Server 2	
Server 3	
Server 4	
Server 5	

Figure 2-3: The SNTP configuration

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

Time Zone is an offset time of GMT. You have to select the time zone first and then perform time sync via NTP because the switch will combine this time zone offset and updated NTP time to come out the local time, otherwise, you will not able to get the correct time. The switch supports configurable time zone from –12 to +13 step 1 hour.

Default Time zone: +8 Hrs.

Parameter description :

- **Server 1 to 5 :**

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

Buttons

These buttons are displayed on the SNTP page:

- **Apply :**

  Click to save changes.

- **Reset :**

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

2-4 LLDP

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

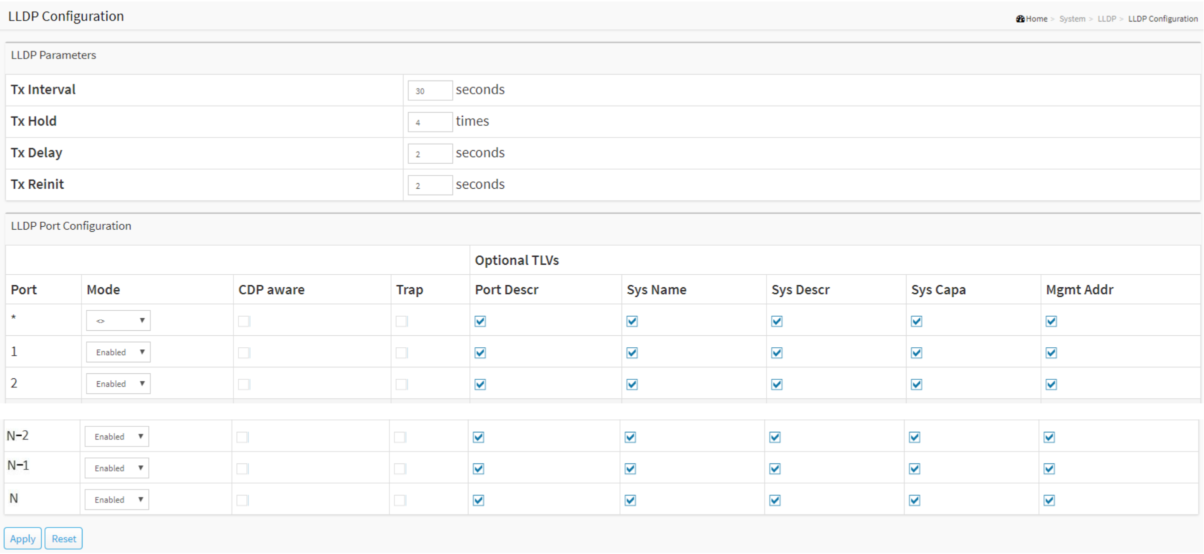
2-4.1 LLDP Configuration

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 LLDP:

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



LLDP Configuration

LLDP Parameters

Tx Interval	30 seconds
Tx Hold	4 times
Tx Delay	2 seconds
Tx Reinit	2 seconds

LLDP Port Configuration

				Optional TLVs				
Port	**Mode**	**CDP aware**	**Trap**	**Port Descr**	**Sys Name**	**Sys Descr**	**Sys Capa**	**Mgmt Addr**
*	<> ▼	□	□	☑	☑	☑	☑	☑
1	Enabled ▼	□	□	☑	☑	☑	☑	☑
2	Enabled ▼	□	□	☑	☑	☑	☑	☑
N-2	Enabled ▼	□	□	☑	☑	☑	☑	☑
N-1	Enabled ▼	□	□	☑	☑	☑	☑	☑
N	Enabled ▼	□	□	☑	☑	☑	☑	☑

Figure 2-4.1: The LLDP Configuration

Parameter description:

LLDP Parameters

- **Tx Interval :**

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

- **Tx Hold :**

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

- **Tx Delay :**

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

- **Tx Reinit :**

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

LLDP Port Configuration

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

- **Port :**

  The switch port number of the logical LLDP port.

- **Mode :**

  Select LLDP mode.

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

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

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

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

- **CDP Aware :**

  Select CDP awareness.

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

  Only CDP TLVs that can be mapped to a corresponding field in the LLDP neighbors' table are decoded. All other TLVs are discarded (Unrecognized CDP TLVs and discarded CDP frames are not shown in the LLDP statistics.). CDP TLVs are mapped onto LLDP neighbors' table as shown below.

  CDP TLV "Device ID" is mapped to the LLDP "Chassis ID" field.

  CDP TLV "Address" is mapped to the LLDP "Management Address" field. The CDP address TLV can contain multiple addresses, but only the first address is shown in the LLDP neighbors' table.

  CDP TLV "Port ID" is mapped to the LLDP "Port ID" field.

  CDP TLV "Version and Platform" is mapped to the LLDP "System Description" field.

  Both the CDP and LLDP support "system capabilities", but the CDP capabilities cover capabilities that are not part of the LLDP. These capabilities are shown as "others" in the LLDP neighbors' table.

If all ports have CDP awareness disabled the switch forwards CDP frames received from neighbor devices. If at least one port has CDP awareness enabled all CDP frames are terminated by the switch.

> **NOTE:** When CDP awareness on a port is disabled the CDP information isn't removed immediately, but gets when the hold time is exceeded.

- **Trap :**

  LLDP trapping notifies events such as newly-detectedneighboring devices and link malfunctions.

- **Port Descr :**

  Optional TLV: When checked the "port description" is included in LLDP information transmitted.

- **Sys Name :**

  Optional TLV: When checked the "system name" is included in LLDP information transmitted.

- **Sys Descr :**

  Optional TLV: When checked the "system description" is included in LLDP information transmitted.

- **Sys Capa :**

  Optional TLV: When checked the "system capability" is included in LLDP information transmitted.

- **Mgmt Addr :**

  Optional TLV: When checked the "management address" is included in LLDP information transmitted.

Buttons

- **Apply :**

  Click to save changes.

- **Reset :**

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

2-4.2 LLDP-MED Configuration

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

Auto-discovery of LAN policies (such as VLAN, Layer 2 Priority and Differentiated services (Diffserv) settings) enabling plug and play networking.

Device location discovery to allow creation of location databases and, in the case of Voice over Internet Protocol (VoIP), Enhanced 911 services.

Extended and automated power management of Power over Ethernet (PoE) end points.

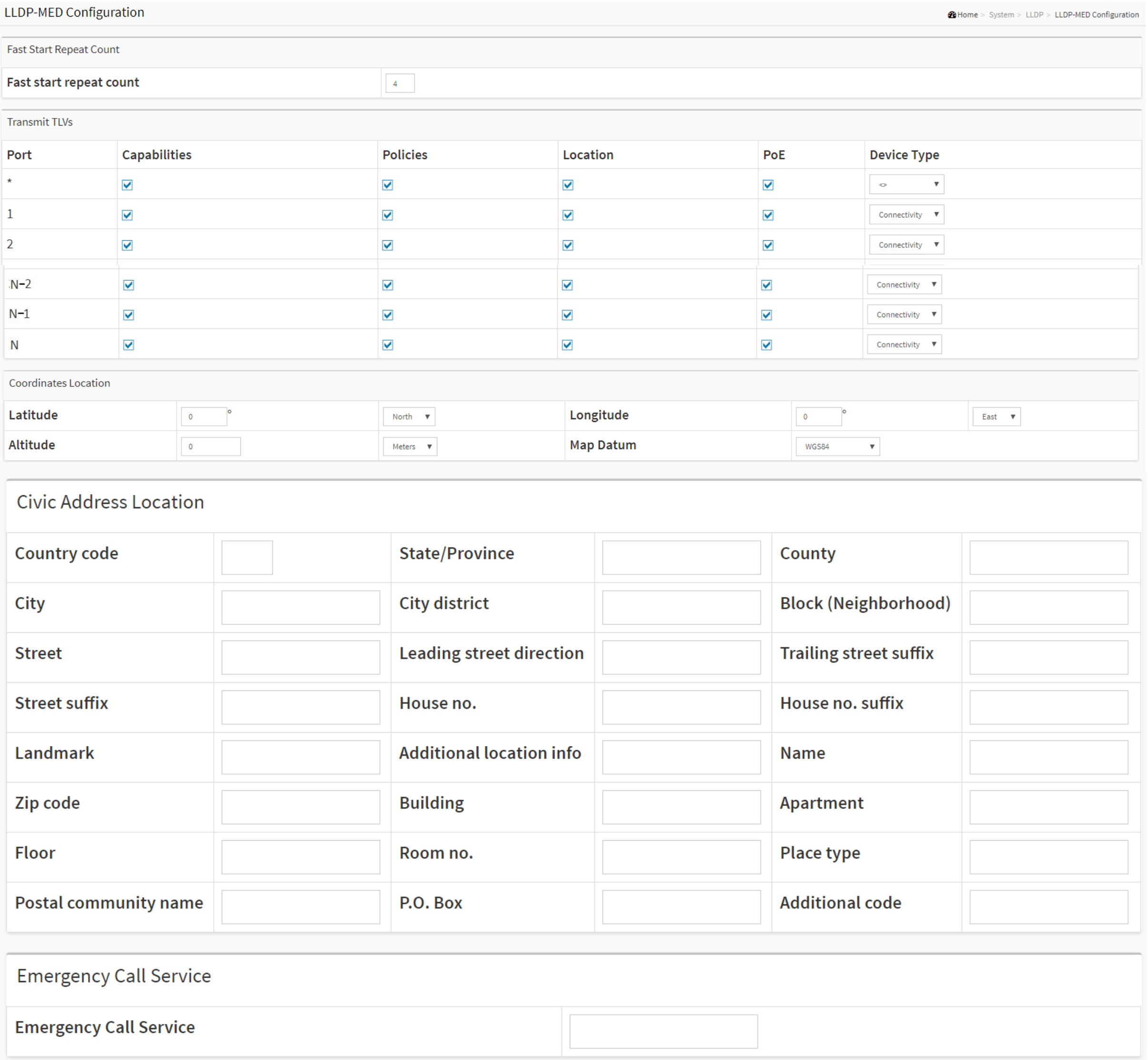
Inventory management, allowing network administrators to track their network devices, and determine their characteristics (manufacturer, software and hardware versions, and serial or asset number).

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

Web Interface

To configure LLDP-MED:

1. Click System, LLDP and LLDP-MED Configuration.
2. Modify Fast start repeat count parameter, default is 4.
3. Modify Transmit TLVs parameters.
4. Modify Coordinates Location parameters.
5. Fill Civic Address Location parameters.
6. Fill Emergency Call Service parameters.
7. Add new policy.
8. Click Apply, will show following Policy Port Configuration.
9. Select Policy ID for each port.
10. Click Apply.



LLDP-MED Configuration

Home > System > LLDP > LLDP-MED Configuration

Fast Start Repeat Count

Fast start repeat count	4

Transmit TLVs

Port	Capabilities	Policies	Location	PoE	Device Type
*	☑	☑	☑	☑	<> ▾
1	☑	☑	☑	☑	Connectivity ▾
2	☑	☑	☑	☑	Connectivity ▾
N−2	☑	☑	☑	☑	Connectivity ▾
N−1	☑	☑	☑	☑	Connectivity ▾
N	☑	☑	☑	☑	Connectivity ▾

Coordinates Location

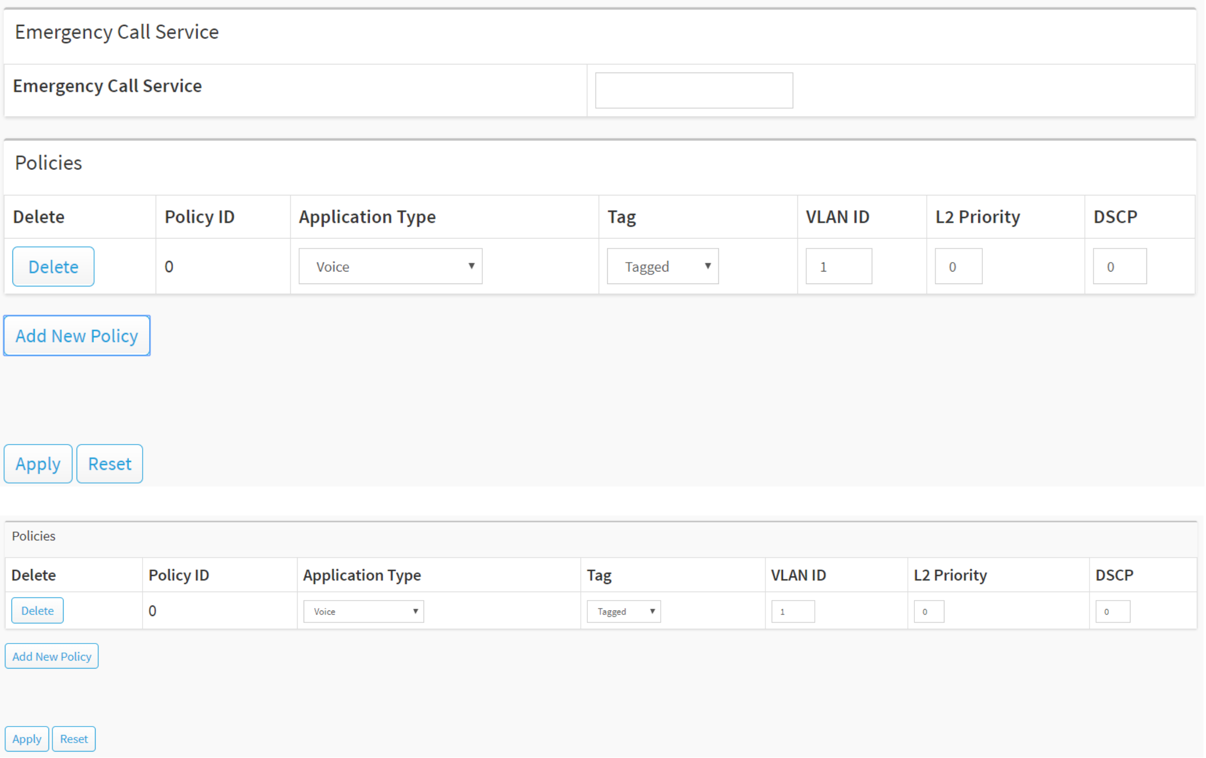
Latitude	0 °	North ▾	**Longitude**	0 °	East ▾
Altitude	0	Meters ▾	**Map Datum**	WGS84 ▾	

Civic Address Location

Country code		**State/Province**		**County**	
City		**City district**		**Block (Neighborhood)**	
Street		**Leading street direction**		**Trailing street suffix**	
Street suffix		**House no.**		**House no. suffix**	
Landmark		**Additional location info**		**Name**	
Zip code		**Building**		**Apartment**	
Floor		**Room no.**		**Place type**	
Postal community name		**P.O. Box**		**Additional code**	

Emergency Call Service

Emergency Call Service	



Emergency Call Service

Emergency Call Service	

Policies

Delete	Policy ID	Application Type	Tag	VLAN ID	L2 Priority	DSCP
Delete	0	Voice	Tagged	1	0	0

Policies

Delete	Policy ID	Application Type	Tag	VLAN ID	L2 Priority	DSCP
Delete	0	Voice	Tagged	1	0	0

Figure 2-4.2: The LLDP-MED Configuration

Parameter description :

Fast start repeat count

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

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

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

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

Transmit TLVs

- **Port :**

The interface name to which the configuration applies.

- **Capabilities :**

  When checked the switch's capabilities is included in LLDP-MEDinformation transmitted.

- **Policies :**

  When checked the configured policies for the interface is included in LLDP-MED information transmitted.

- **Location :**

  When checked the configured location information for the switch is included in LLDP-MED information transmitted.

- **PoE :**

  When checked the configured PoE (Power Over Ethernet) information for the interface is included in LLDP-MED information transmitted.

- **Device Type :**

  Any LLDP-MED Device is operating as a specific type of LLDP-MED Device, which may be either a Network Connectivity Device or a specific Class of Endpoint Device, as defined below.

  A Network Connectivity Device is a LLDP-MED Device that provides access to the IEEE 802 based LAN infrastructure for LLDP-MED Endpoint Devices

  An LLDP-MED Network Connectivity Device is a LAN access device based on any of the following technologies :

  1. LAN Switch/Router

  2. IEEE 802.1 Bridge

  3. IEEE 802.3 Repeater (included for historical reasons)

  4. IEEE 802.11 Wireless Access Point

  5. Any device that supports the IEEE 802.1AB and MED extensions that can relay IEEE 802 frames via any method.

  An Endpoint Device a LLDP-MED Device that sits at the network edge and provides some aspect of IP communications service, based on IEEE 802 LAN technology.

  The main difference between a Network Connectivity Device and an Endpoint Device is that only an Endpoint Device can start the LLDP-MED information exchange.

  Even though a switch always should be a Network ConnectivityDevice, it is possible to configure it to act as an Endpoint Device, and thereby start the LLDP-MED information exchange (In the case where two Network Connectivity Devices are connected together)

Coordinates Location

- **Latitude :**

  Latitude SHOULD be normalized to within 0-90 degrees with a maximum of 4 digits.

  It is possible to specify the direction to either North of the equator or South of the equator.

- **Longitude :**

  Longitude SHOULD be normalized to within 0-180 degrees with a maximum of 5 digits.

  It is possible to specify the direction to either East of the prime meridian or West of the prime meridian.

- **Altitude :**

  Altitude SHOULD be normalized to within -32767 to 32767 with a maximum of 4 digits.

It is possible to select between two altitude types (floors or meters).

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

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

- **Map Datum :**

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

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

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

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

Civic Address Location

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

- **Country code :**

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

- **State/Province :**

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

- **County :**

  County, parish, gun (Japan), district.

- **City :**

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

- **City district :**

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

- **Block (Neighbourhood) :**

  Neighbourhood, block.

- **Street :**

  Street - Example: Poppelvej.

- **Leading street direction :**

  Leading street direction - Example: N.

- **Trailing street suffix :**

  Trailing street suffix - Example: SW.

- **Street suffix :**

  Street suffix - Example: Ave, Platz.

- **House no. :**

  House number - Example: 21.

- **House no. suffix :**

House number suffix - Example: A, 1/2.

- **Landmark :**

  Landmark or vanity address - Example: Columbia University.

- **Additional location info :**

  Additional location info - Example: South Wing.

- **Name :**

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

- **Zip code :**

  Postal/zip code - Example: 2791.

- **Building :**

  Building (structure) - Example: Low Library.

- **Apartment :**

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

- **Floor :**

  Floor - Example: 4.

- **Room no. :**

  Room number - Example: 450F.

- **Place type :**

  Place type - Example: Office.

- **Postal community name :**

  Postal community name - Example: Leonia.

- **P.O. Box :**

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

- **Additional code :**

  Additional code - Example: 1320300003.

Emergency Call Service:

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

- **Emergency Call Service :**

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

Policies

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

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

The network policy attributes advertised are:

1. Layer 2 VLAN ID (IEEE 802.1Q-2003)

2. Layer 2 priority value (IEEE 802.1D-2004)

3. Layer 3 Diffserv code point (DSCP) value (IETF RFC 2474)

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

1. Voice

2. Guest Voice

3. Softphone Voice

4. Video Conferencing

5. Streaming Video

6. Control / Signalling (conditionally support a separate network policy for the media types above)

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

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

- **Delete :**

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

- **Policy ID :**

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

- **Application Type :**

  Intended use of the application types:

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

  2. Voice Signalling (conditional) - for use in network topologies that require a different policy for the voice signalling than for the voice media. This application type should not be advertised if all the same network policies apply as those advertised in the Voice application policy.

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

  4. Guest Voice Signalling (conditional) - for use in network topologies that require a different policy for the guest voice signalling than for the guest voice media. This application type should not be advertised if all the same network policies apply as those advertised in the Guest Voice application policy.

  5. Softphone Voice - for use by softphone applications on typical data centric devices, such as PCs or laptops. This class of endpoints frequently does not support multiple VLANs, if at all, and are typically configured to use an 'untagged' VLAN or a single 'tagged' data specific VLAN. When a network policy is defined for use with an 'untagged' VLAN (see Tagged flag below), then the L2 priority field is ignored and only the DSCP value has relevance.

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

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

8. Video Signalling (conditional) - for use in network topologies that require a separate policy for the video signalling than for the video media. This application type should not be advertised if all the same network policies apply as those advertised in the Video Conferencing application policy.

- **Tag :**

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

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

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

- **VLAN ID :**

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

- **L2 Priority :**

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

- **DSCP :**

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

Buttons

- **Adding New Policy :**

Click to add a new policy. Specify the Application type, Tag, VLAN ID, L2 Priority and DSCP for the new policy. Click "Apply".

- **Apply :**

Click to save changes.

- **Reset :**

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

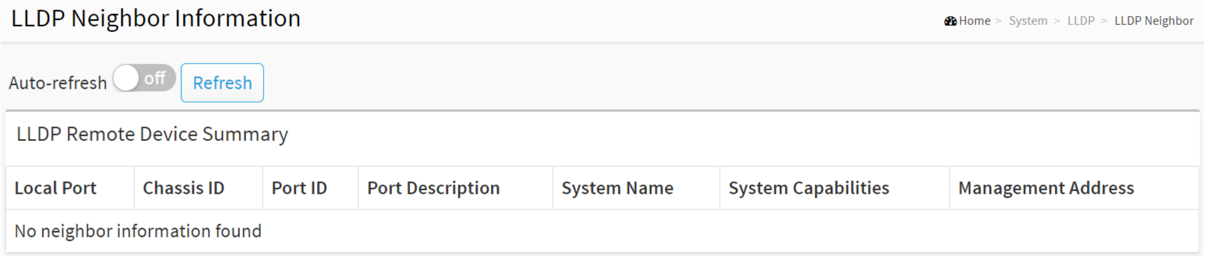
2-4.3 LLDP Neighbour

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

Web Interface

To show LLDP neighbours:

1. Click System, LLDP and LLDP Neighbour.
2. Click Refresh for manual update web screen.
3. Click Auto-refresh for auto-update web screen.



LLDP Neighbor Information

LLDP Remote Device Summary

Local Port	Chassis ID	Port ID	Port Description	System Name	System Capabilities	Management Address
No neighbor information found						

Figure 2-4.3: The LLDP Neighbour information

NOTE: If there is no device that supports LLDP in your network then the table will show "No LLDP neighbour information found".

Parameter description:

- **Local Port :**

  The port on which the LLDP frame was received.

- **Chassis ID :**

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

- **Port ID :**

  The Remote Port ID is the identification of the neighbour port.

- **Port Description :**

  Port Description is the port description advertised by the neighbour unit.

- **System Name :**

  System Name is the name advertised by the neighbour unit.

- **System Capabilities :**

  System Capabilities describes the neighbour unit's capabilities. The possible capabilities are:

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

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

- **System Description**

Displays the system description.

- **Management Address :**

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

Buttons

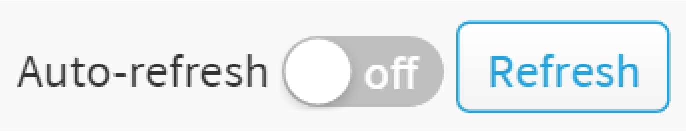


Figure 2-4.3: The LLDP Neighbor buttons

- **Auto-refresh :**

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

- **Refresh :**

  Click to refresh the page immediately.

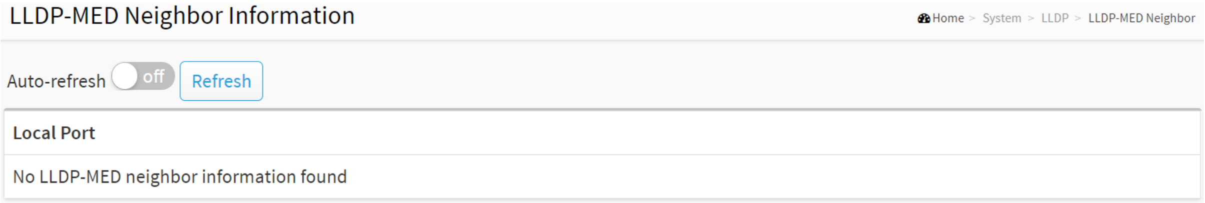
2-4.4 LLDP-MED Neighbour

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

Web Interface

To show LLDP-MED neighbor:

1. Click System, LLDP and LLDP-MED Neighbour.
2. Click Refresh for manual update web screen.
3. Click Auto-refresh for auto-update web screen.



LLDP-MED Neighbor Information

Local Port
No LLDP-MED neighbor information found

Figure 2-4.4: The LLDP-MED Neighbour information

NOTE: If there is no device that supports LLDP-MED in your network then the table will show "No LLDP-MED neighbour information found".

Parameter description

- **Port :**

  The port on which the LLDP frame was received.

- **Device Type :**

  LLDP-MED Devices are comprised of two primary Device Types: Network Connectivity

Devices and Endpoint Devices.

- **LLDP-MED Network Connectivity Device Definition**

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

1. LAN Switch/Router

2. IEEE 802.1 Bridge

3. IEEE 802.3 Repeater (included for historical reasons)

4. IEEE 802.11 Wireless Access Point

5. Any device that supports the IEEE 802.1AB and MED extensions defined by TIA-1057 and can relay IEEE 802 frames via any method.

- **LLDP-MED Endpoint Device Definition :**

LLDP-MED Endpoint Devices, as defined in TIA-1057, are located at the IEEE 802 LAN network edge, and participate in IP communication service using the LLDP-MED framework.

Within the LLDP-MED Endpoint Device category, the LLDP-MED scheme is broken into further Endpoint Device Classes, as defined in the following.

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

- **LLDP-MED Generic Endpoint (Class I) :**

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

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

- **LLDP-MED Media Endpoint (Class II) :**

The LLDP-MED Media Endpoint (Class II) definition is applicable to all endpoint products that have IP media capabilities however may or may not be associated with a particular end user. Capabilities include all of the capabilities defined for the previous Generic Endpoint Class (Class I), and are extended to include aspects related to media streaming. Example product categories expected to adhere to this class include (but are not limited to) Voice / Media Gateways, Conference Bridges, Media Servers, and similar.

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

- **LLDP-MED Communication Endpoint (Class III) :**

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

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

- **LLDP-MED Capabilities :**

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

  1. LLDP-MED capabilities

  2. Network Policy

  3. Location Identification

  4. Extended Power via MDI - PSE

  5. Extended Power via MDI - PD

  6. Inventory

  7. Reserved

- **Application Type :**

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

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

  2. Voice Signalling - for use in network topologies that require a different policy for the voice signalling than for the voice media.

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

  4. Guest Voice Signalling - for use in network topologies that require a different policy for the guest voice signalling than for the guest voice media.

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

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

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

  8. Video Signalling - for use in network topologies that require a separate policy for the video signalling than for the video media.

- **Policy :**

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

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

  Defined: The network policy is defined.

- **TAG :**

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

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

Tagged: The device is using the IEEE 802.1Q tagged frame format.

- **VLAN ID :**

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

- **Priority :**

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

- **DSCP :**

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

- **Auto-negotiation**

  Auto-negotiation identifies if MAC/PHY auto-negotiation is supported by the link partner.

- **Auto-negotiation status**

  Auto-negotiation status identifies if auto-negotiation is currently enabled at the link partner. If **Auto-negotiation** is supported and **Auto-negotiation status** is disabled, the 802.3 PMD operating mode will be determined the operational MAU type field value rather than by auto-negotiation.

- **Auto-negotiation Capabilities**

  Auto-negotiation Capabilities shows the link partners MAC/PHY capabilities.

Buttons

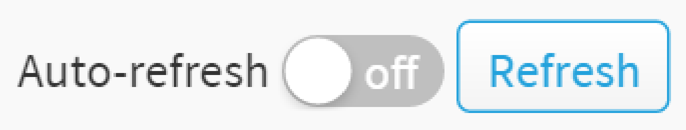


Figure 2-4.4: The LLDP Neighbor buttons

- **Auto-refresh :**

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

- **Refresh :**

  Click to refresh the page immediately.

2-4.5 LLDP Neighbour PoE

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

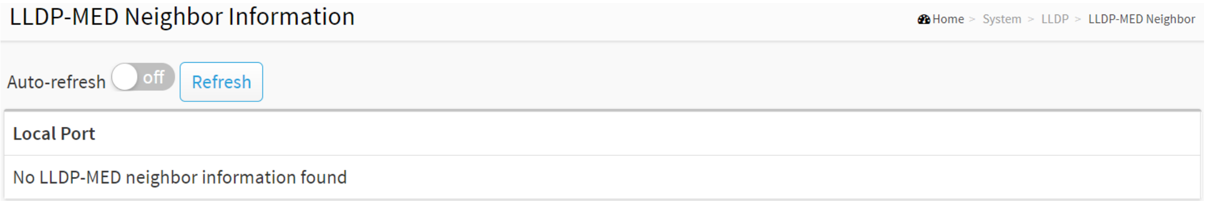
Web Interface

To show LLDP neighbor PoE:

1. Click System, LLDP and LLDP Neighbour PoE.

2. Click Refresh for manual update web screen.

3. Click Auto-refresh for auto-update web screen.


LLDP-MED Neighbor Information

Home > System > LLDP > LLDP-MED Neighbor

Auto-refresh off Refresh

Local Port
No LLDP-MED neighbor information found

Figure 2-4.5: The LLDP Neighbour PoE information

Parameter description

- **Local Port :**

  The interface for this switch on which the LLDP frame was received.

- **Power Type :**

  The Power Type represents whether the device is a Power Sourcing Entity (PSE) or Power Device (PD).

  If the Power Type is unknown it is represented as "Reserved".

- **Power Source :**

  The Power Source represents the power source being utilized by a PSE or PD device.

  If the device is a PSE device it can either run on its Primary Power Source or its Backup Power Source. If it is unknown whether the PSE device is using its Primary Power Source or its Backup Power Source it is indicated as "Unknown"

  If the device is a PD device it can either run on its local power supply or it can use the PSE as power source. It can also use both its local power supply and the PSE.

  If it is unknown what power supply the PD device is using it is indicated as "Unknown"

- **Power Priority :**

  Power Power Priority represents the priority of the PD device, or the power priority associated with the PSE type device's interface that is sourcing the power. There are three levels of power priority. The three levels are: Critical, High and Low.

  If the power priority is unknown it is indicated as "Unknown"

- **Maximum Power :**

  The Maximum Power Value contains a numerical value that indicates the maximum power in watts required by a PD device from a PSE device, or the minimum power a PSE device is capable of sourcing over a maximum length cable based on its current configuration.

  The maximum allowed value is 102.3 W. If the device indicates value higher than 102.3 W, it is represented as "reserved"

Buttons

Figure 2-4.5: The LLDP Neighbor PoE buttons

- **Auto-refresh :**

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

- **Refresh :**

Click to refresh the page immediately.

2-4.6 LLDP Neighbour EEE

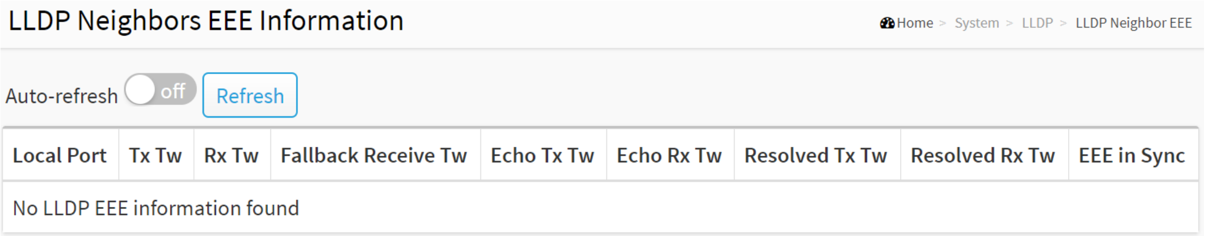
By using EEE power savings can be achieved at the expense of traffic latency. This latency occurs due to that the circuits EEE turn off to save power, need time to boot up before sending traffic over the link. This time is called "wakeup time". To achieve minimal latency, devices can use LLDP to exchange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

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

Web Interface

To show LLDP neighbor EEE:

1. Click System, LLDP and LLDP Neighbour EEE.
2. Click Refresh for manual update web screen.
3. Click Auto-refresh for auto-update web screen.



LLDP Neighbors EEE Information

Local Port	Tx Tw	Rx Tw	Fallback Receive Tw	Echo Tx Tw	Echo Rx Tw	Resolved Tx Tw	Resolved Rx Tw	EEE in Sync
No LLDP EEE information found								

Figure 2-4.6: The LLDP Neighbour EEE information

Parameter description

- **Local Port :**

  The interface at which LLDP frames are received or transmitted.

- **Tx Tw :**

  The link partner's maximum time that transmit path can hold-off sending data after deassertion of LPI.

- **Rx Tw :**

  The link partner's time that receiver would like the transmitter to hold-off to allow time for the receiver to wake from sleep.

- **Fallback Receive Tw :**

  The link partner's fallback receive Tw.

  A receiving link partner may inform the transmitter of an alternate desired Tw_sys_tx. Since a receiving link partner is likely to have discrete levels for savings, this provides the transmitter with additional information that it may use for a more efficient allocation. Systems that do not implement this option default the value to be the same as that of the Receive Tw_sys_tx.

- **Echo Tx Tw :**

  The link partner's Echo Tx Tw value.

  The respective echo values shall be defined as the local link partners reflection (echo) of the remote link partners respective values. When a local link partner receives its echoed values from the remote link partner it can determine whether or not the remote link partner has received, registered and processed its most recent values. For example, if the local link partner receives echoed parameters that do not match the values in its local MIB, then the local link partner infers that the remote link partners request was based on stale information.

- **Echo Rx Tw :**

  The link partner's Echo Rx Tw value.

- **Resolved Tx Tw :**

  The resolved Tx Tw for this link. Note : NOT the link partner

  The resolved value that is the actual "tx wakeup time " used for this link (based on EEE information exchanged via LLDP).

- **Resolved Rx Tw :**

  The resolved Rx Tw for this link. Note : NOT the link partner

  The resolved value that is the actual "tx wakeup time " used for this link (based on EEE information exchanged via LLDP).

- **EEE in Sync :**

  Shows whether the switch and the link partner have agreed on wake times.

  Red - Switch and link partner have not agreed on wakeup times.

  Green - Switch and link partner have agreed on wakeup times.

Buttons

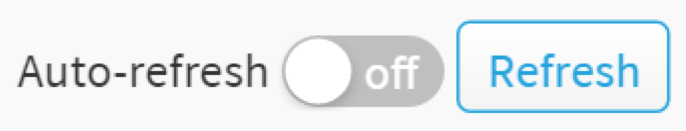


Figure 2-4.6: The LLDP Neighbor EEE buttons

- **Auto-refresh :**

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

- **Refresh :**

  Click to refresh the page immediately.

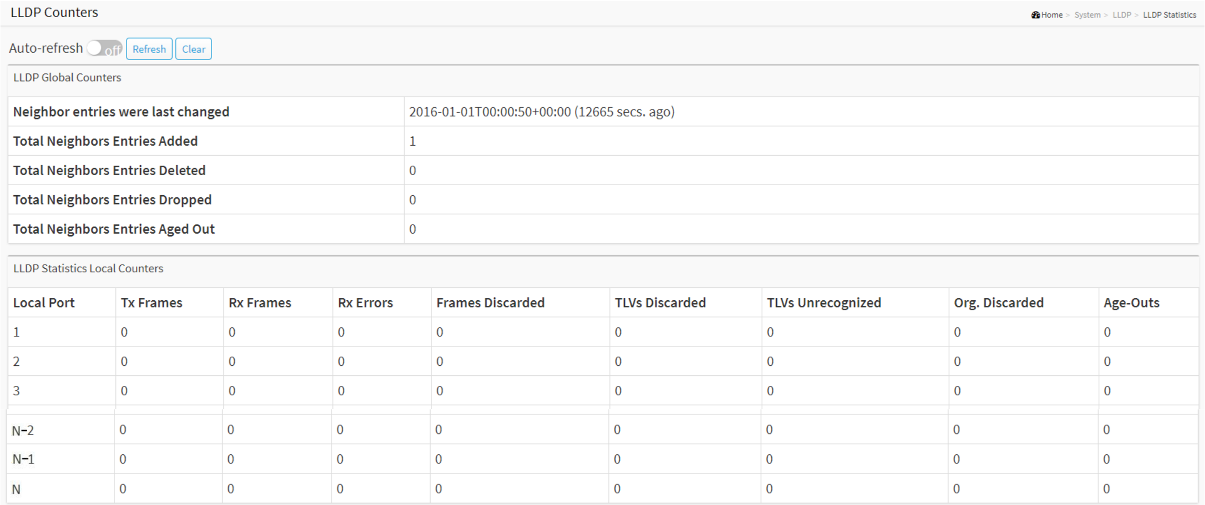
2-4.7 LLDP Statistics

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

Web Interface

To show LLDP Statistics:

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



LLDP Counters

LLDP Global Counters

Neighbor entries were last changed	2016-01-01T00:00:50+00:00 (12665 secs. ago)
Total Neighbors Entries Added	1
Total Neighbors Entries Deleted	0
Total Neighbors Entries Dropped	0
Total Neighbors Entries Aged Out	0

LLDP Statistics Local Counters

Local Port	Tx Frames	Rx Frames	Rx Errors	Frames Discarded	TLVs Discarded	TLVs Unrecognized	Org. Discarded	Age-Outs
1	0	0	0	0	0	0	0	0
2	0	0	0	0	0	0	0	0
3	0	0	0	0	0	0	0	0
N-2	0	0	0	0	0	0	0	0
N-1	0	0	0	0	0	0	0	0
N	0	0	0	0	0	0	0	0

Figure 2-4.7: The LLDP Statistics information

Parameter description:

Global Counters

- **Neighbour entries were last changed at :**

  It also shows the time when the last entry was last deleted or added. It also shows the time elapsed since the last change was detected.

- **Total Neighbours Entries Added :**

  Shows the number of new entries added since switch reboot.

- **Total Neighbours Entries Deleted :**

  Shows the number of new entries deleted since switch reboot.

- **Total Neighbours Entries Dropped :**

  Shows the number of LLDP frames dropped due to the entry table being full.

- **Total Neighbours Entries Aged Out :**

  Shows the number of entries deleted due to Time-To-Live expiring.

Local Counters

The displayed table contains a row for each port. The columns hold the following information:

- **Local Port :**

  The port on which LLDP frames are received or transmitted.

- **Tx Frames :**

  The number of LLDP frames transmitted on the port.

- **Rx Frames :**

  The number of LLDP frames received on the port.

- **Rx Errors :**

  The number of received LLDP frames containing some kind of error.

- **Frames Discarded :**

  If an LLDP frame is received on a port, and the switch's internal table has run full, the LLDP frame is counted and discarded. This situation is known as "Too Many Neighbours" in the LLDP standard. LLDP frames require a new entry in the table when the Chassis ID or Remote Port ID is not already contained within the table. Entries are removed from the table when a given port's link is down, an LLDP shutdown frame is received, or when the entry ages out.

- **TLVs Discarded :**

  Each LLDP frame can contain multiple pieces of information, known as TLVs (TLV is short for "Type Length Value"). If a TLV is malformed, it is counted and discarded.

- **TLVs Unrecognized :**

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

- **Org. Discarded :**

  The number of organizationally received TLVs.

- **Age-Outs :**

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

Buttons

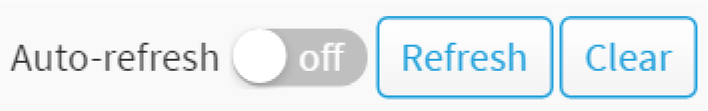


Figure 2-4.7: The LLDP Statistics information buttons

- **Auto-refresh :**

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

- **Refresh :**

  Click to refresh the page.

- **Clear :**

  Clears the counters for the selected port.

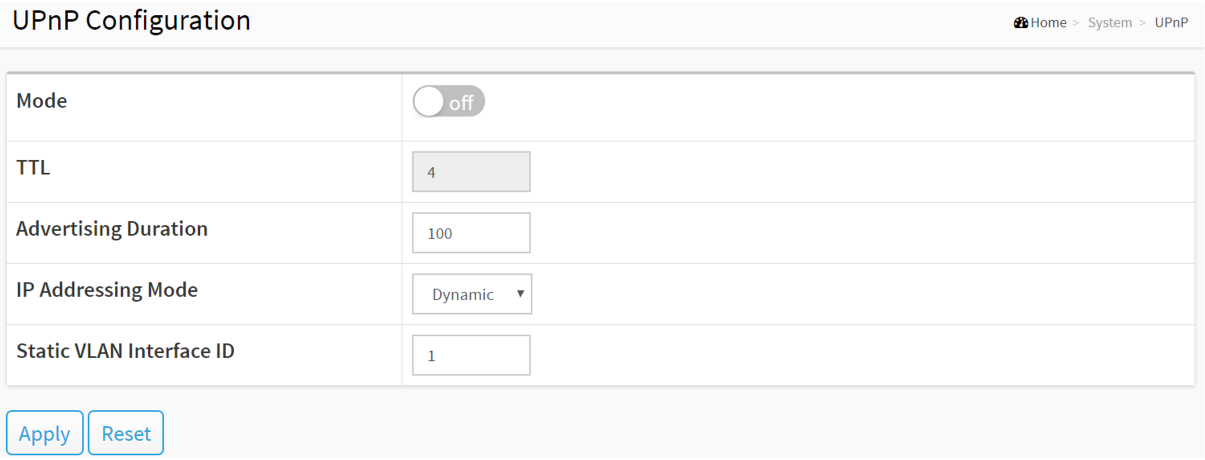
2-5 UPnP

UPnP is an acronym for Universal Plug and Play. The goals of UPnP are to allow devices to connect seamlessly and to simplify the implementation of networks in the home (data sharing, communications, and entertainment) and in corporate environments for simplified installation of computer components

Web Interface

To configure the UPnP Configuration in the web interface:

1. Click System and UPnP
2. Scroll to select the mode to enable or disable
3. Specify the parameters in each blank field.
4. Click the Apply to save the setting
5. If you want to cancel the setting then you need to click the Reset button. It will revert to previously saved values



UPnP Configuration

Mode	off
TTL	4
Advertising Duration	100
IP Addressing Mode	Dynamic ▾
Static VLAN Interface ID	1

Figure 2-5: The UPnP Configuration

Parameter description:

These parameters are displayed on the UPnP Configuration page:

- **Mode :**

  Indicates the UPnP operation mode. Possible modes are:
  on: Enable UPnP mode operation.
  off: Disable UPnP mode operation.
  When the mode is enabled, two ACEs are added automatically to trap UPNP related packets to CPU. The ACEs are automatically removed when the mode is disabled.

- **TTL :**

  The TTL value is used by UPnP to send SSDP advertisement messages. Valid values are in the range 1 to 255.

- **Advertising Duration :**

  The duration, carried in SSDP packets, is used to inform a control point or control points how often it or they should receive an SSDP advertisement message from this switch. If a control point does not receive any message within the duration, it will think that the switch no longer exists. Due to the unreliable nature of UDP, in the standard it is recommended that such refreshing of advertisements to be done at less than one-half of the advertising duration. In the implementation, the switch sends SSDP messages periodically at the interval one-half of the advertising duration minus 30 seconds. Valid values are in the range 100 to 86400.

- **IP Addressing Mode**

  IP addressing mode provides two ways to determine IP address assignment: **Dynamic**: Default selection for UPnP. UPnP module helps users choosing the IP address of the switch device. It finds the first available system IP address. **Static**: User specifies the IP interface VLAN for choosing the IP address of the switch device.

- **Static VLAN Interface ID**

  The index of the specific IP VLAN interface. It will only be applied when IP Addressing Mode is static. Valid configurable values ranges from 1 to 4095. Default value is 1.

Buttons

- **Apply :**

  Click to save changes.

- **Reset :**

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

2-6 OSPF

2-6.1 Configuration

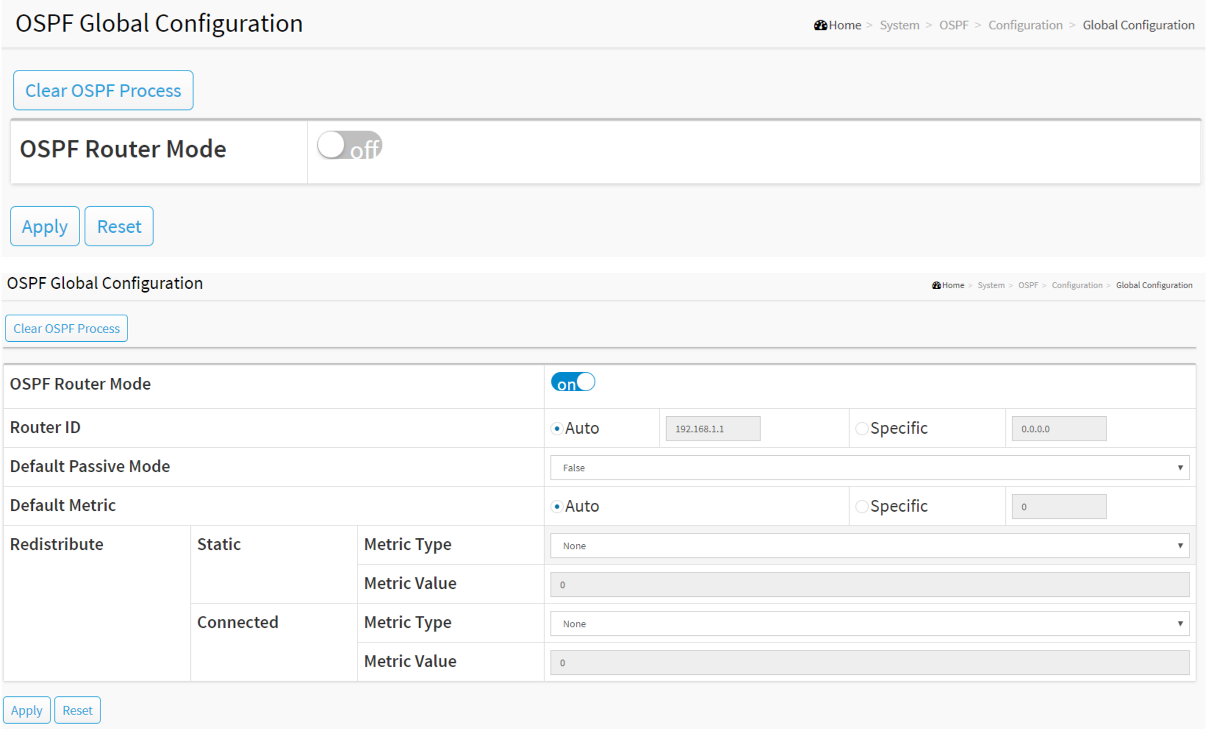
2-6.1.1 Global Configuration

This is OSPF router configuration table. It is a general group to configure the OSPF common router parameters.

Web Interface

To configure OSPF:

1. Click System ,OSPF, Configuration and Global Configuration.
2. Turn on or turn of OSPF Router Mode.
3. Click Apply.
4. Click Clear OSPF Process to reset OSPF



OSPF Global Configuration

Home > System > OSPF > Configuration > Global Configuration

Clear OSPF Process

OSPF Router Mode	off

Apply Reset

OSPF Global Configuration

Home > System > OSPF > Configuration > Global Configuration

Clear OSPF Process

OSPF Router Mode			on			
Router ID			● Auto	192.168.1.1	○ Specific	0.0.0.0
Default Passive Mode			False			
Default Metric			● Auto		○ Specific	0
Redistribute	Static	Metric Type	None			
		Metric Value	0			
	Connected	Metric Type	None			
		Metric Value	0			

Apply Reset

Figure 2-6.1.1: The Global Configuration

Parameter description:

- **OSPF Router Mode :**

  Enable/Disable the OSPF router mode.

- **Router ID :**

  The OSPF Router ID in IPv4 address format(A.B.C.D). When the router's OSPF Router ID is changed, if there is one or more fully adjacent neighbors in current OSPF area, the new router ID will take effect after restart OSPF process. Notice that the router ID should be unique in the Autonomous System and value '0.0.0.0' is invalid since it is reserved for the default algorithm. Auto: The default algorithm will choose the largest IP address assigned to the router. Specific: User specified router ID.

- **Default Passive Mode :**

  Configure all interfaces as passive-interface by default.When an interface is configured as a passive-interface, the OSFP routing updates sending is suppressed, therefore the interface does not establish adjacencies (No OSPF Hellos). The subnet of all interfaces (both passive and active) is advertised by the OSPF router.

- **Default Metric :**

  User specified default metric value for the OSPF routing protocol. The field is significant only when the arugment 'IsSpecificDefMetric' is TRUE. Auto: The default metric is calculated automatically based on the routing protocols.Specific: User specified default metric.

- **Static Redistribute Metric Type :**

  The OSPF redistributed metric type for the connected interfaces. None: The static routes are not redistributed. Specified Metric Value: User specified metric for the static routes. External Type 1: External Type 1 of the static routes. External Type 2: External Type 2 of the static routes.

- **Static Redistribute Metric Value :**

  User specified metric value for the connected interfaces. The field is significant only when the arugment 'ConnectedRedistMetricType' is configured as 'metricTypeSpecified'. The allowed range is 0 to 1677214.

- **Connected Redistribute Metric Type :**

  The OSPF redistributed metric type for the static routes. None: The connected interfaces are not redistributed. Specified Metric Value: User specified metric for the connected interfaces routes. External Type 1: External Type 1 of the connected interfaces routes. External Type 2: External Type 2 of the connected interfaces routes.

- **Connected Redistribute Metric Value :**

  User specified metric value for the static routes.The field is significant only when the arugment 'StaticRedistMetricType' is configured as 'metricTypeSpecified'. The allowed range is 0 to 1677214.

Buttons

- **Clear OSPF Process :**

  Click to reset the current OSPF process.

- **Apply :**

  Click to save changes.

- **Reset :**

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

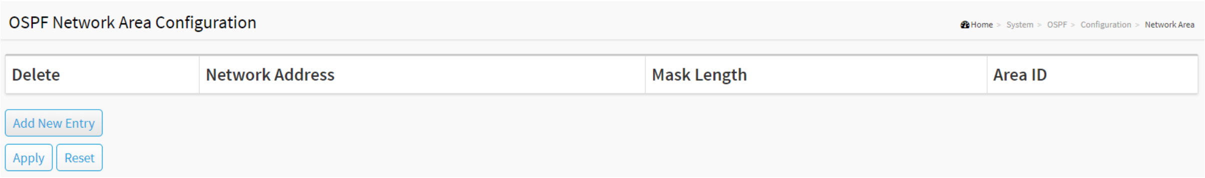
2-6.1.2 Network Area

This is OSPF area configuration table. It is used to specify the OSPF enabled interface(s). When OSPF is enabled on the specific interface(s), the router can provide the network information to the other OSPF routers via those interfaces.

Web Interface

To configure OSPF Network Area Configuration:

1. Click System ,OSPF, Configuration and Network Area.
2. Click Add New Entry.
3. Specify the Network Address, Mask Length and Area ID.
4. Click Apply.



OSPF Network Area Configuration

Delete	Network Address	Mask Length	Area ID

Figure 2-6.1.2: The Network Area

Parameter description:

- **OSPF Router Mode :**

  Enable/Disable the OSPF router mode.

- **Router ID :**

  The OSPF Router ID in IPv4 address format(A.B.C.D). When the router's OSPF Router ID is changed, if there is one or more fully adjacent neighbors in current OSPF area, the new router ID will take effect after restart OSPF process. Notice that the router ID should be unique in the Autonomous System and value '0.0.0.0' is invalid since it is reserved for the default algorithm. Auto: The default algorithm will choose the largest IP address assigned to the router. Specific: User specified router ID.

- **Network Address :**

  IPv4 network address.

- **Mask Length :**

  IPv4 network mask length.

- **Area ID :**

  The OSPF area ID.

Buttons

- **Add New Entry :**

  Click to add new entry.

- **Apply :**

  Click to save changes.

- **Reset :**

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

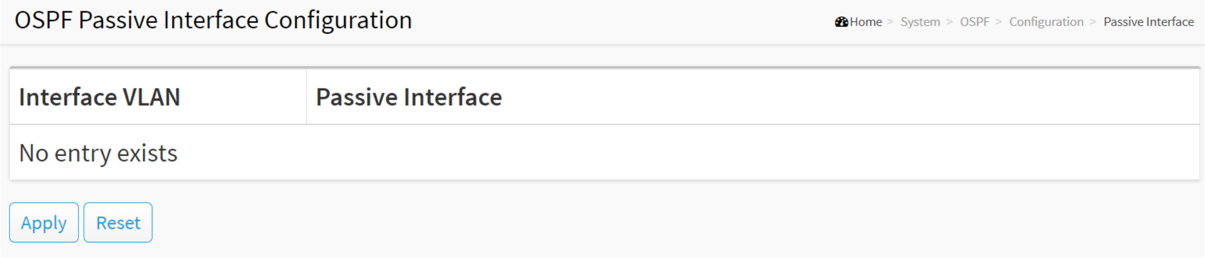
2-6.1.3 Passive Interface

This is OSPF router interface configuration table.

Web Interface

To configure OSPF Passive Interface Configuration:

1. Click System ,OSPF, Configuration and Passive Interface.
2. Specify the Interface VLAN and Passive Interface.
3. Click Apply.



OSPF Passive Interface Configuration

Interface VLAN	Passive Interface
No entry exists	

Figure 2-6.1.3: The Passive Interface

Parameter description:

- **Interface :**

  Interface identification.

- **Passive Interface :**

  Enable the interface as OSPF passive-interface.

Buttons

- **Apply :**

  Click to save changes.

- **Reset :**

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

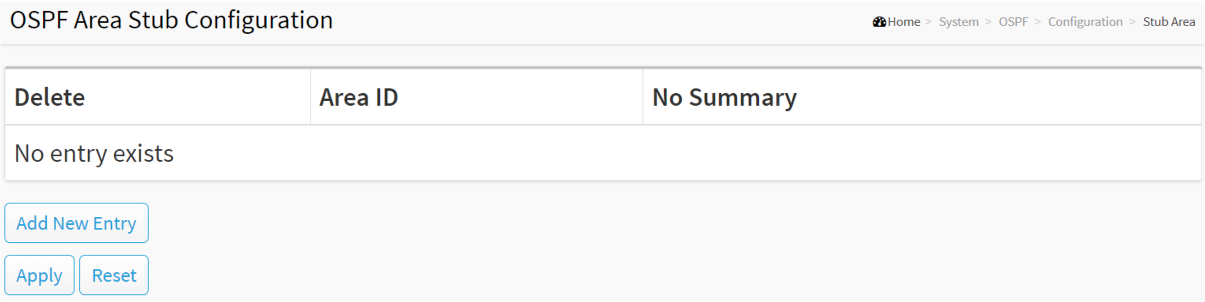
2-6.1.4 Stub Area

This is OSPF stub area configuration table. The configuration is used to reduce the link-state database size and therefore the memory and CPU requirement by forbidding some LSAs.

Web Interface

To configure OSPF Stub Area Configuration:

1. Click System ,OSPF, Configuration and Stub Area.
2. Specify the Area ID and No Summary.
3. Click Apply.


OSPF Area Stub Configuration

Home > System > OSPF > Configuration > Stub Area

Delete	Area ID	No Summary
No entry exists		

Figure 2-6.1.4: The Stub Area

Parameter description:

- **Interface :**

  Interface identification.

- **Passive Interface :**

  Enable the interface as OSPF passive-interface.

- **Area ID :**

  The OSPF area ID.

- **No Summary :**

  The value is true means the area is a totally stub area, which summary-LSAs(Type-3) except for the default route and AS-external-LSAs(Type-5) are blocked. The value is false means the area is a stub area, which summary-LSAs(Type-3) except for the default route are blocked.

Buttons

- **Add New Entry :**

  Click to add new entry.

- **Apply :**

  Click to save changes.

- **Reset :**

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

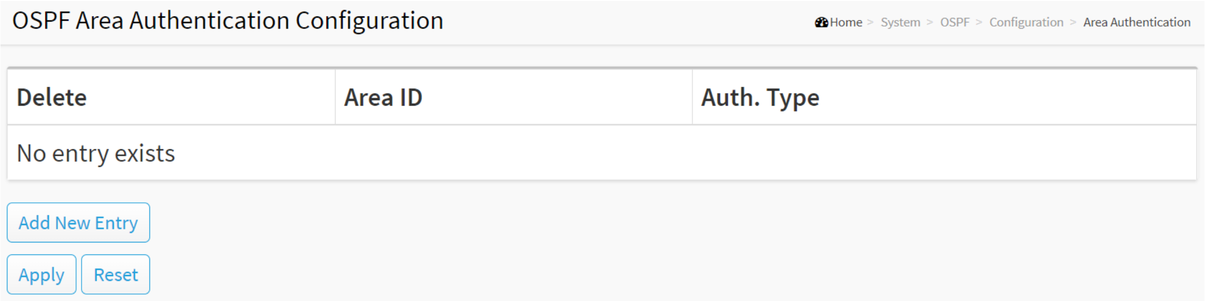
2-6.1.5 Area Authentication

This is OSPF area authentication configuration table. It is used to applied the authentication to all the interfaces belong to the area.

Web Interface

To configure OSPF Area Authentication Configuration:

1. Click System ,OSPF, Configuration and Area Authentication.
2. Specify the Area ID and Auth. Type.
3. Click Apply.


OSPF Area Authentication Configuration

Delete	Area ID	Auth. Type
No entry exists		

Figure 2-6.1.5: The Area Authenticaiton

Parameter description:

- **Area ID :**

  The OSPF area ID.

- **Auth. Type :**

  The authentication type on an area is applied to all the interfaces belong to that area. The authentication type on an IP interface or a virtual link overrides the authentication type on an area and is useful if different interfaces in the same area use different authentication types.
  Specify the authenticaton type.
  Simple Password: Simple password authentication.
  Message Digest: MD5 digest authentication.

Buttons

- **Add New Entry :**

  Click to add new entry.

- **Apply :**

  Click to save changes.

- **Reset :**

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

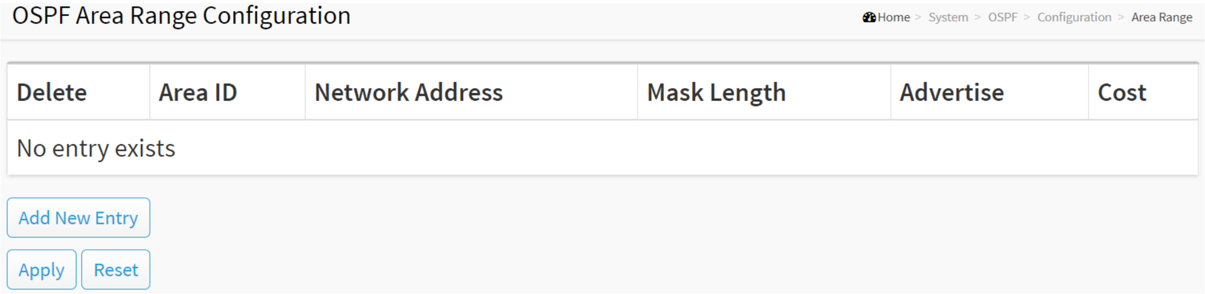
2-6.1.6 Area Range

This is OSPF area range configuration table. It is used to summarize the intra area paths from a specific address range in one summary-LSA(Type-3) and advertised to other areas or configure the address range status as 'DoNotAdvertise' which the summary-LSA(Type-3) is suppressed. The area range configuration is used for Area Border Routers (ABRs) and only router-LSAs(Type-1) and network-LSAs (Type-2) can be summarized. The AS-external-LSAs(Type-5) cannot be summarized because the scope is OSPF autonomous system (AS). The AS-external-LSAs(Type-7) cannot be summarized because the feature is not supported yet.

Web Interface

To configure OSPF Area Range Configuration:

1. Click System ,OSPF, Configuration and Area Range.
2. Specify the Area ID, Network Address, Mask Length, Advertise and Cost.
3. Click Apply.



OSPF Area Range Configuration

Delete	Area ID	Network Address	Mask Length	Advertise	Cost
No entry exists					

Figure 2-6.1.6: The Area Range

Parameter description:

- **Area ID :**

  The OSPF area ID.

- **Network Address :**

  IPv4 network address.

- **Mask Length :**

  IPv4 network mask length.

- **Advertised :**

  When the value is true, it summarizes intra area paths from the address range in one summary-LSA(Type-3) and advertised to other areas. Otherwise, the intra area paths from the address range are not advertised to other areas.

- **Auto/Specific :**

  When 'Auto' is selected, the cost value is set to 0 automatically and isn't allowed to be configured.

- **Cost :**

  User specified cost (or metric) for this summary route. It is allowed to be configured only when 'Specific' is selected and the allowed range is 0 to 65535.. The allowed range is 1 to 16777215 and the default setting is 'auto cost' mode.

Buttons

- **Add New Entry :**

  Click to add new entry.

- **Apply :**

  Click to save changes.

- **Reset :**

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

2-6.1.7 Interface

This is interface configuration parameter table.

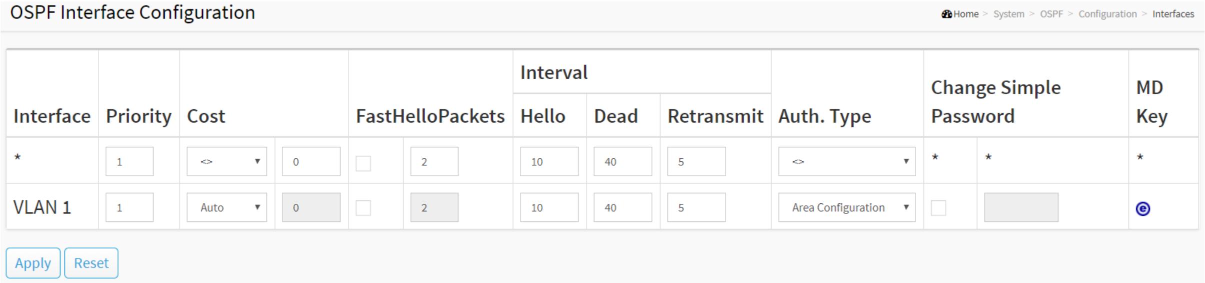
Web Interface

To configure OSPF Interface Configuration:

1. Click System ,OSPF, Configuration and Interface.

2. Specify the Priority, Cost, FastHelloRackets, Interval, Auth. Type, Change Simple Password and MD key.

3. Click Apply.



OSPF Interface Configuration

						Interval						
Interface	Priority	Cost		FastHelloPackets		Hello	Dead	Retransmit	Auth. Type	Change Simple Password		MD Key
*	1	<> ▾	0	□	2	10	40	5	<> ▾	*	*	*
VLAN 1	1	Auto ▾	0	□	2	10	40	5	Area Configuration ▾	□		ⓔ

Figure 2-6.1.7: The Interface

Parameter description:

- **Area ID :**

  The OSPF area ID.

- **Interface :**

  Interface identification.

- **Priority :**

  User specified router priority for the interface. The allowed range is 0 to 255 and the default value is 1.

- **Cost :**

  User specified cost for this interface. It's link state metric for the interface. The field is significant only when 'IsSpecificCost' is TRUE. The allowed range is 1 to 65535 and the default setting is 'auto cost' mode.

- **FastHelloPackets :**

  How many Hello packets will be sent per second. The allowed range is 1 to 10 and the default setting is disabled.

- **Hello Interval :**

  How many Hello packets will be sent per second. The allowed range is 1 to 65535 and the default value is 10 (seconds).

- **Dead Interval :**

  The time interval (in seconds) between hello packets. The allowed range is 1 to 65535 and the default value is 40 (seconds).

- **Retransmit Interval :**

  The time interval (in seconds) between link-state advertisement(LSA) retransmissions for adjacencies. The allowed range is 1 to 65535 and the default value is 5 (seconds).

- **Auth. Type :**

  The authentication type.
  Simple Password: It's using a plain text authentication. A password must be configured, but the password can be read by sniffer the packets.
  Message Digest: It's message-digest algorithm 5 (MD5) authentication. Keying material must also be configured. This is the most secure method.
  Null Authentication: No authentication.
  Area Configuration: Refer to Area authentication setting.

- **Change Simple Password :**

It is used to change the simple password (fill with plain text). The allowed input length is 1 to 8.

- **MD Key :**

  Click the icon to edit the message digest key for the entry.

Buttons

- **Apply :**

  Click to save changes.

- **Reset :**

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

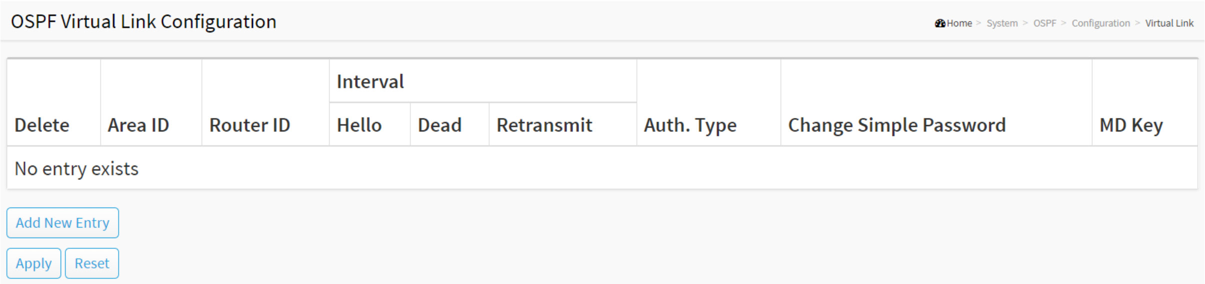
2-6.1.8 Virtual Link

This is OSPF virtual link configuration table. The virtual link is established between 2 ABRs to overcome that all the areas have to be connected directly to the backbone area.

Web Interface

To configure OSPF Virtual Link Configuration:

1. Click System ,OSPF, Configuration and Virtual Link.
2. Specify the Area ID, Router ID, Interal, Auth. Type, Changes Simple Password and MD key.
3. Click Apply.



OSPF Virtual Link Configuration

			Interval					
Delete	Area ID	Router ID	Hello	Dead	Retransmit	Auth. Type	Change Simple Password	MD Key
No entry exists								

Figure 2-6.1.8: The Virtual Link

Parameter description:

- **Area ID :**

  The OSPF area ID.

- **Router ID :**

  OSPF router ID.

- **Hello Interval :**

  The time interval (in seconds) between hello packets. The allowed range is 1 to 65535 and the default value is 10 (seconds).

- **Dead Interval :**

  The number of seconds to wait until the neighbour is decalred to be dead. The allowed range is 1 to 65535 and the default value is 40 (seconds).

- **Retransmit Interval :**

  The time interval (in seconds) between link-state advertisement(LSA) retransmissions for adjacencies. The allowed range is 1 to 65535 and the default value is 5 (seconds).

- **Auth. Type :**

  The authentication type on an area.
  Simple Password: It's using a plain text authentication. A password must be configured, but the password can be read by sniffer the packets.
  Message Digest: It's message-digest algorithm 5 (MD5) authentication. Keying material must also be configured. This is the most secure method.
  Null Authentication: No authentication.
  Area Configuration: Refer to Area authentication setting.

- **Change Simple Password :**

  It is used to change the simple password (fill with plain text). The allowed input length is 1 to 8.

- **MD Key :**

  Click the icon to edit the message digest key for the entry.

Buttons

- **Add New Entry :**

  Click to add new entry.

- **Apply :**

  Click to save changes.

- **Reset :**

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

2-6.2 Status

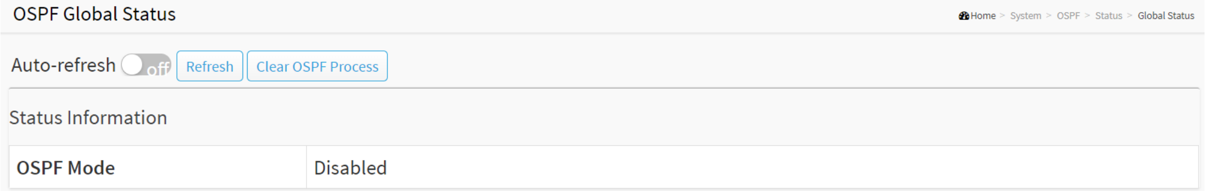
2-6.2.1 Global Status

This is OSPF router status table. It is used to provide the OSPF router status information.

Web Interface

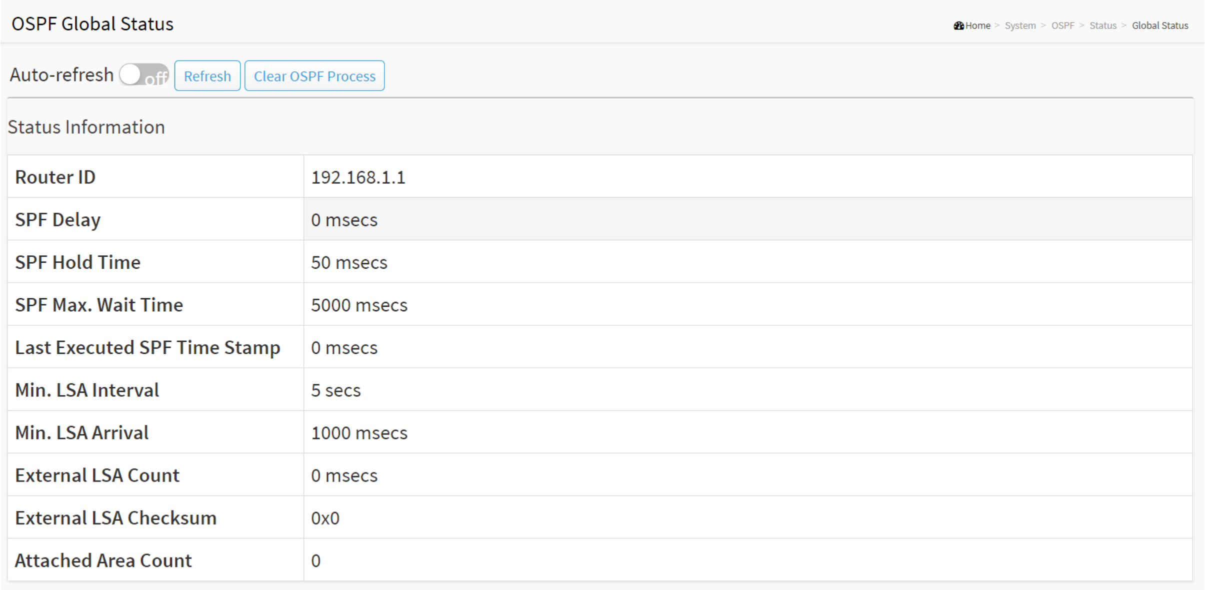
To display the OSPF Global Status:

1. Click System ,OSPF, Status and Global Status.
2. Display the OSPF Global Status.



Status Information

OSPF Mode	Disabled



Status Information

Router ID	192.168.1.1
SPF Delay	0 msecs
SPF Hold Time	50 msecs
SPF Max. Wait Time	5000 msecs
Last Executed SPF Time Stamp	0 msecs
Min. LSA Interval	5 secs
Min. LSA Arrival	1000 msecs
External LSA Count	0 msecs
External LSA Checksum	0x0
Attached Area Count	0

Figure 2-6.2.1: The Global Status

Parameter description:

- **Area ID :**

  The OSPF area ID.

- **Router ID :**

  OSPF router ID.

- **SPF Delay :**

  Delay time (in seconds)of SPF calculations.

- **SPF Hold Time :**

  Minimum hold time (in milliseconds) between consecutive SPF calculations.

- **SPF Max. Wait Time :**

Maximum wait time (in milliseconds) between consecutive SPF calculations.

- **Last Executed SPF Time Stamp :**

  Time (in milliseconds) that has passed between the start of the SPF algorithm execution and the current time.

- **Min. LSA Interval :**

  Minimum interval (in seconds) between link-state advertisements.

- **Min. LSA Arrival :**

  Maximum arrival time (in milliseconds) of link-state advertisements.

- **External LSA Count :**

  Number of external link-state advertisements.

- **External LSA Checksum :**

  Number of external link-state checksum.

- **Attached Area Count :**

  Number of areas attached for the router.

Buttons

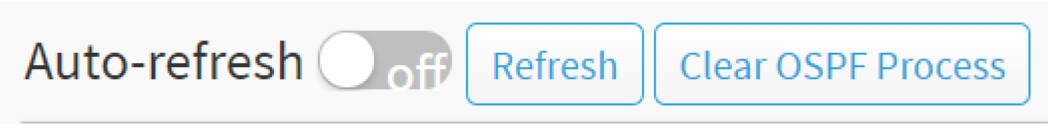


Figure 2-6.2.1: The Global Status buttons

- **Auto-refresh :**

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

- **Refresh :**

  Click to refresh the page.

- **Clear OSPF Process :**

  Click to reset the current OSPF process.

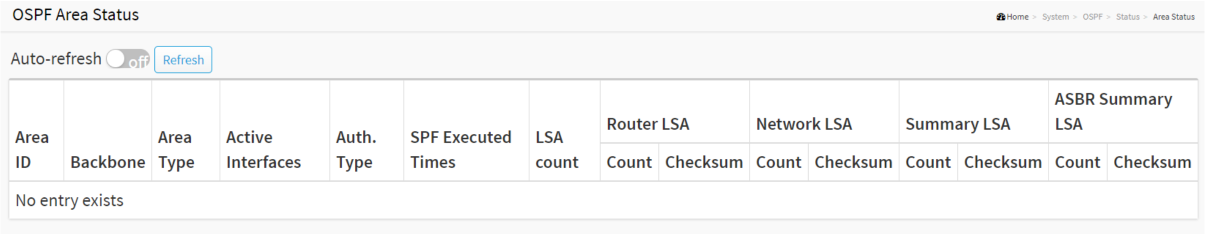
2-6.2.2 Area Status

This is OSPF network area status table. It is used to provide the OSPF network area status information.

Web Interface

To display the OSPF Area Status:

1. Click System ,OSPF, Status and Area Status.
2. Display the OSPF Area Status.



Area ID	Backbone	Area Type	Active Interfaces	Auth. Type	SPF Executed Times	LSA count	Router LSA		Network LSA		Summary LSA		ASBR Summary LSA	
							Count	Checksum	Count	Checksum	Count	Checksum	Count	Checksum
No entry exists														

Figure 2-6.2.2: The Area Status

Parameter description:

- **Area ID :**

  The Area ID.

- **Backbone :**

  Indicate if it's backbone area or not.

- **Area Type :**

  The area type.

- **Active Interfaces :**

  Number of active interfaces attached in the area.

- **Auth. Type :**

  The authentication type in the area.

- **SPF Executed Times :**

  Number of times SPF algorithm has been executed for the particular area.

- **LSA Count :**

  Number of the total LSAs for the particular area.

- **Router LSA Count :**

  Number of the router-LSAs(Type-1) of a given type for the particular area.

- **Router LSA Checksum :**

  The router-LSAs(Type-1) checksum.

- **Network LSA Count :**

  Number of the network-LSAs(Type-2) of a given type for the particular area.

- **Network LSA Checksum :**

  The network-LSAs(Type-2) checksum.

- **Summary LSA Count :**

  Number of the summary-LSAs(Type-3) of a given type for the particular area.

- **Summary LSA Checksum :**

  The the summary-LSAs(Type-3) checksum.

- **ASBR Summary LSA Count :**

  Number of the ASBR-summary-LSAs(Type-4) of a given type for the particular area.

- **ASBR Summary LSA Checksum :**

  The the ASBR-summary-LSAs(Type-4) checksum.

Buttons

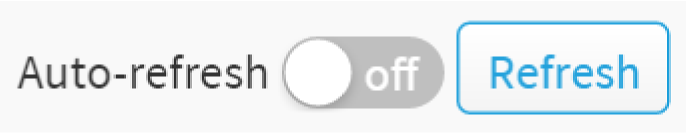


Figure 2-6.2.2: The OSPF Area Status.

- **Auto-refresh :**

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

- **Refresh :**

  Click to refresh the page immediately.

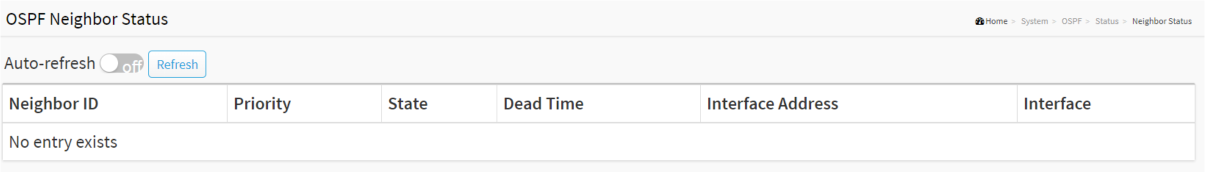
2-6.2.3 Neighbor Status

This is OSPF IPv4 neighbor status table. It is used to provide the OSPF neighbor status information.

Web Interface

To display the OSPF Neighbor Status:

1. Click System ,OSPF, Status and Neighbor Status.
2. Display the OSPF Neighbor Status.



OSPF Neighbor Status

Neighbor ID	Priority	State	Dead Time	Interface Address	Interface
No entry exists					

Figure 2-6.2.3: The Neighbor Status

Parameter description:

- **Area ID :**

  The Area ID.

- **Backbone :**

  Indicate if it's backbone area or not.

- **Neighbor ID :**

  The Neighbor ID.

- **Priority :**

  The priority of OSPF neighbor. It indicates the priority of the neighbor router. This item is used when selecting the DR for the network. The router with the highest priority becomes the DR.

- **State :**

  The state of OSPF neighbor. It indicates the functional state of the neighbor router.

- **Dead Time :**

  Dead timer. It indicates the amount of time remaining that the router waits to receive an OSPF hello packet from the neighbor before declaring the neighbor down.

- **Interface Address :**

  The IP address.

- **Interface :**

  The network interface.

Buttons

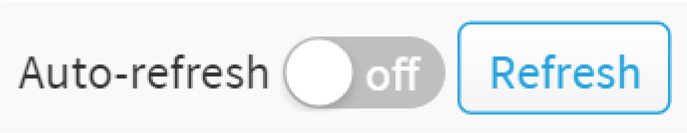


Figure 2-6.2.3: The OSPF Neighbor Status.

- **Auto-refresh :**

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

- **Refresh :**

  Click to refresh the page immediately.

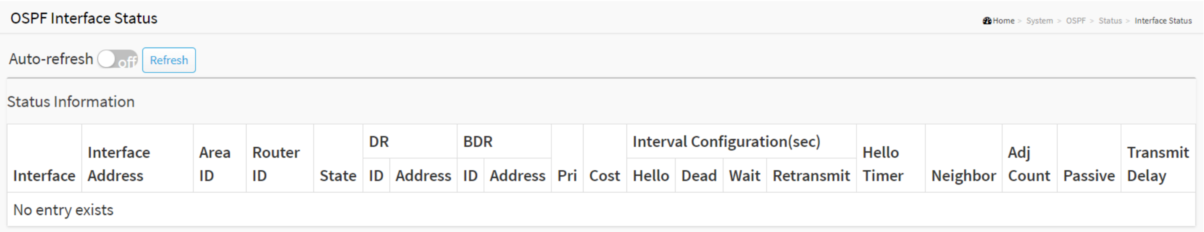
2-6.2.4 Interface Status

This is OSPF IPv4 neighbor status table. It is used to provide the OSPF neighbor status information.

Web Interface

To display the OSPF Interface Status:

1. Click System ,OSPF, Status and Interface Status.
2. Display the OSPF Interface Status.



OSPF Interface Status

Status Information

	Interface	Area	Router		DR		BDR				Interval Configuration(sec)				Hello		Adj		Transmit
Interface	Address	ID	ID	State	ID	Address	ID	Address	Pri	Cost	Hello	Dead	Wait	Retransmit	Timer	Neighbor	Count	Passive	Delay
No entry exists																			

Figure 2-6.2.3: The Interface Status

Parameter description:

- **Area ID :**

  The Area ID.

- **Interface :**

  Interface identification.

- **Interface Address :**

  IPv4 network address.

- **Area ID :**

  The OSPF area ID.

- **Router ID :**

  The OSPF router ID.

- **State :**

  The state of the link.

- **DR ID :**

  The router ID of DR.

- **DR Address :**

  The IP address of DR.

- **BDR ID :**

  The router ID of BDR.

- **BDR Address :**

  The IP address of BDR.

- **Priority :**

  The OSPF priority. It helps determine the DR and BDR on the network to which this interface is connected.

- **Cost :**

  The cost of the interface.

- **Hello :**

  Hello timer. A time interval that a router sends an OSPF hello packet.

- **Dead :**

  Dead timer. Dead timer is a time interval to wait before declaring a neighbor dead. The unit of time is the second.

- **Wait :**

  This interval is used in Wait Timer. Wait timer is a single shot timer that causes the interface to exit waiting and select a DR on the network. Wait Time interval is the same as Dead time interval.

- **Retransmit :**

  Retransmit timer. A time interval to wait before retransmitting a database description packet when it has not been acknowledged.

- **Hello Timer :**

  Hello due timer. An OSPF hello packet will be sent on this interface after this due time.

- **Nbr Count :**

  Neighbor count. This is the number of OSPF neighbors discovered on this interface.

- **Adjacent Nbr Count :**

  Adjacent neighbor count. This is the number of routers running OSPF that are fully adjacent with this router.

- **Passive :**

  Indicate if the interface is passive interface.

- **Transmit Delay :**

  The estimated time to transmit a link-state update packet on the interface.

Buttons

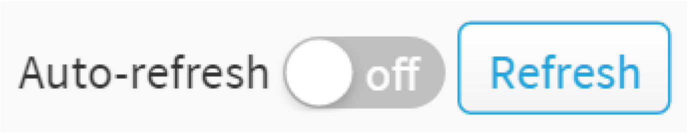


Figure 2-6.2.3: The OSPF Neighbor Status.

- **Auto-refresh :**

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

- **Refresh :**

  Click to refresh the page immediately.

Chapter 3 Port Management

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.

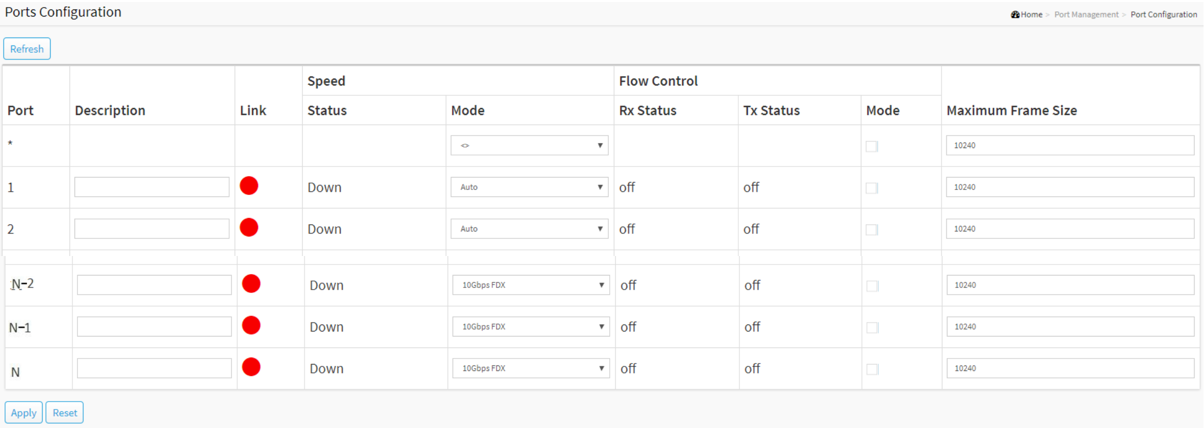
3-1 Port Configuration

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

Web Interface

To configure a Current Port Configuration in the web interface:

1. Click Port Management and Port Configuration.
2. Specify the detail Port alias or description an alphanumeric string describing the full name and version identification for the system's hardware type, software version, and networking application.
3. Specify the Speed Configured, Flow Control, Maximum Frame Size.
4. Click Apply.



Ports Configuration

Port	Description	Link	Speed		Flow Control			Maximum Frame Size
			Status	Mode	Rx Status	Tx Status	Mode	
*				<>			□	10240
1		●	Down	Auto	off	off	□	10240
2		●	Down	Auto	off	off	□	10240
N-2		●	Down	10Gbps FDX	off	off	□	10240
N-1		●	Down	10Gbps FDX	off	off	□	10240
N		●	Down	10Gbps FDX	off	off	□	10240

Figure 3-1: The Port Configuration

Parameter description:

- **Port :**

  This is the logical port number for this row.

- **Description :**

  Enter up to 63 characters to be descriptive name for identifies this port.

- **Link :**

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

- **Current Link Speed Status:**

  Provides the current link speed of the port.

- **Configured Link Speed :**

  Selects any available link speed for the given switch port. Only speeds supported by the specific port is shown. Possible speeds are:
  Disabled - Disables the switch port operation.
  Auto - Port auto negotiating speed with the link partner and selects the highest speed that is compatible with the link partner.
  10Mbps HDX - Forces the cu port in 10Mbps half duplex mode.
  10Mbps FDX - Forces the cu port in 10Mbps full duplex mode.
  100Mbps HDX - Forces the cu port in 100Mbps half duplex mode.
  100Mbps FDX - Forces the cu port in 100Mbps full duplex mode.
  1Gbps FDX - Forces the port in 1Gbps full duplexFlow Control :

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

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

- **Maximum Frame Size**

  Enter the maximum frame size allowed for the switch port, including FCS. The range is 1518-10240 bytes.

Buttons

- **Refresh :**

  You can click them for refresh the Port link Status by manual

- **Apply :**

  Click to save changes.

- **Reset :**

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

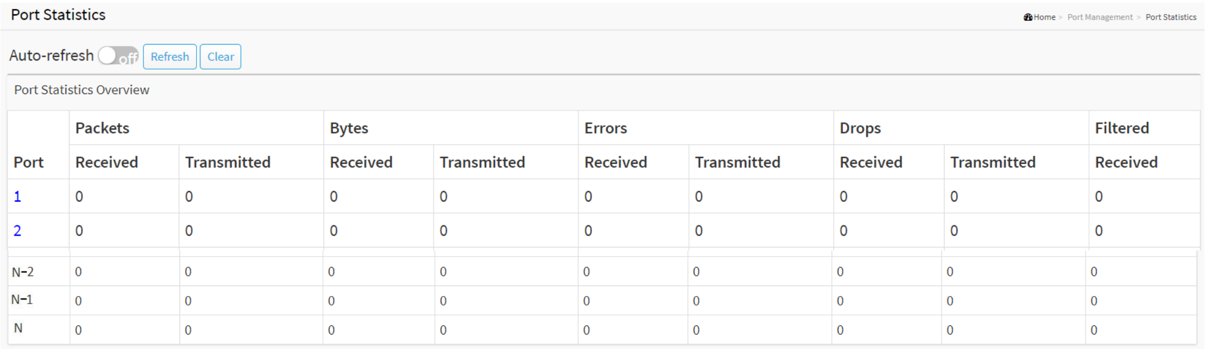
3-2 Port Statistics

The section describes to the Port statistics information and provides overview of general traffic statistics for all switch ports.

Web Interface

To Display the Port Statistics Overview in the web interface:

1. Click Port Management and Port Statistics.
2. If you want to auto-refresh then you need to evoke the “Auto-refresh”.
3. Click “ Refresh“ to refresh the port statistics or clear all information when you click “ Clear”.
4. If you want to see the detail of port statistic then you need to click that port.



Port Statistics

Home > Port Management > Port Statistics

Port Statistics Overview

	Packets		Bytes		Errors		Drops		Filtered
Port	Received	Transmitted	Received	Transmitted	Received	Transmitted	Received	Transmitted	Received
1	0	0	0	0	0	0	0	0	0
2	0	0	0	0	0	0	0	0	0
N-2	0	0	0	0	0	0	0	0	0
N-1	0	0	0	0	0	0	0	0	0
N	0	0	0	0	0	0	0	0	0

Figure 3-2: The Port Statistics Overview

Parameter description:

- **Port :**

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

- **Packets :**

  The number of received and transmitted packets per port.

- **Bytes :**

  The number of received and transmitted bytes per port.

- **Errors :**

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

- **Drops :**

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

- **Filtered**

  The number of received frames filtered by the forwarding process.

Buttons

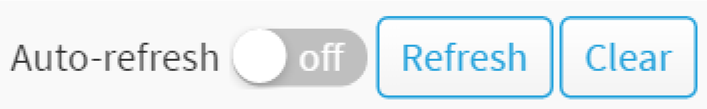


Figure 3-2: The Port Statistics Overview buttons

- **Auto-refresh :**

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

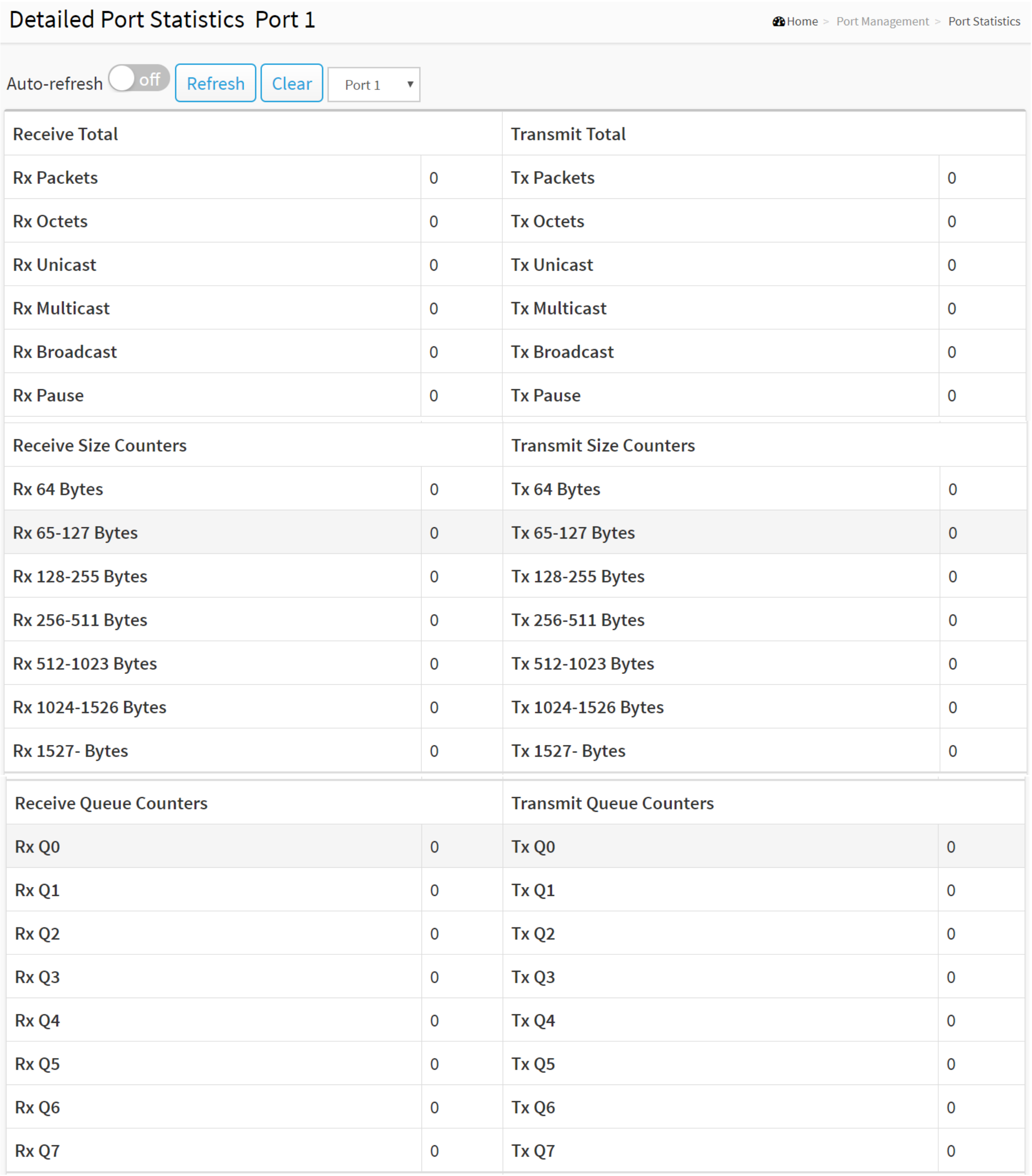
- **Refresh :**

  Click to refresh the page.

- **Clear :**

  Clears the counters for all ports.

If you want to see the detail of port statistic then you need to click that port. The displayed counters are the totals for receive and transmit, the size counters for receive and transmit, and the error counters for receive and transmit.

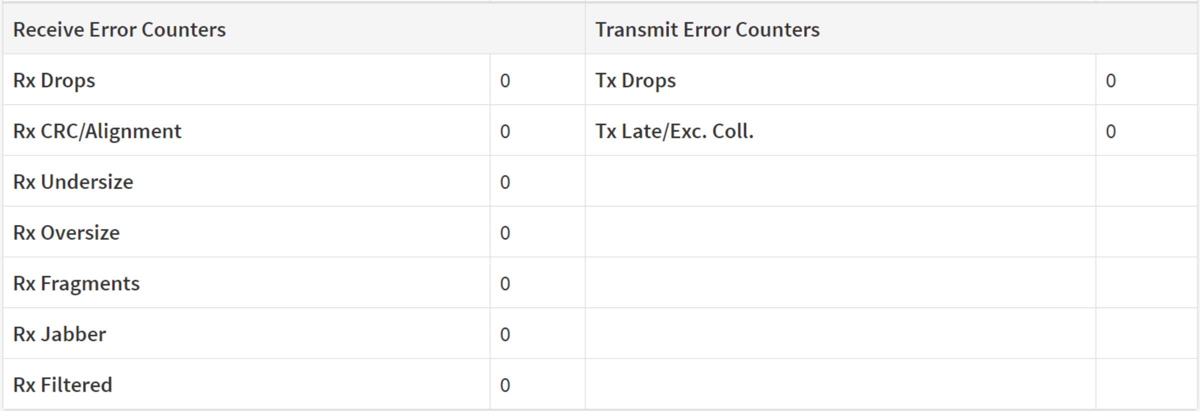


Detailed Port Statistics Port 1

Receive Total		Transmit Total	
Rx Packets	0	Tx Packets	0
Rx Octets	0	Tx Octets	0
Rx Unicast	0	Tx Unicast	0
Rx Multicast	0	Tx Multicast	0
Rx Broadcast	0	Tx Broadcast	0
Rx Pause	0	Tx Pause	0

Receive Size Counters		Transmit Size Counters	
Rx 64 Bytes	0	Tx 64 Bytes	0
Rx 65-127 Bytes	0	Tx 65-127 Bytes	0
Rx 128-255 Bytes	0	Tx 128-255 Bytes	0
Rx 256-511 Bytes	0	Tx 256-511 Bytes	0
Rx 512-1023 Bytes	0	Tx 512-1023 Bytes	0
Rx 1024-1526 Bytes	0	Tx 1024-1526 Bytes	0
Rx 1527- Bytes	0	Tx 1527- Bytes	0

Receive Queue Counters		Transmit Queue Counters	
Rx Q0	0	Tx Q0	0
Rx Q1	0	Tx Q1	0
Rx Q2	0	Tx Q2	0
Rx Q3	0	Tx Q3	0
Rx Q4	0	Tx Q4	0
Rx Q5	0	Tx Q5	0
Rx Q6	0	Tx Q6	0
Rx Q7	0	Tx Q7	0



Receive Error Counters		Transmit Error Counters	
Rx Drops	0	Tx Drops	0
Rx CRC/Alignment	0	Tx Late/Exc. Coll.	0
Rx Undersize	0		
Rx Oversize	0		
Rx Fragments	0		
Rx Jabber	0		
Rx Filtered	0		

Figure 3-2: The Detailed Port Statistics

Parameter description:

- **Upper left scroll bar:**

  To scroll which port to display the Port statistics with “Port-1”, “Port-2”, ...

Receive Total and Transmit Total

- **Rx and Tx Packets :**

  The number of received and transmitted (good and bad) packets.

- **Rx and Tx Octets :**

  The number of received and transmitted (good and bad) bytes. Includes FCS, but excludes framing bits.

- **Rx and Tx Unicast :**

  The number of received and transmitted (good and bad) unicast packets.

- **Rx and Tx Multicast :**

  The number of received and transmitted (good and bad) multicast packets.

- **Rx and Tx Broadcast :**

  The number of received and transmitted (good and bad) broadcast packets.

- **Rx and Tx Pause :**

  A count of the MAC Control frames received or transmitted on this port that have an opcode indicating a PAUSE operation.

Receive and Transmit Size Counters

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

Receive Error Counters

- **Rx Drops :**

  The number of frames dropped due to lack of receive buffers or egress congestion.

- **Rx CRC/Alignment :**

  The number of frames received with CRC or alignment errors.

- **Rx Undersize :**

  The number of short 1 frames received with valid CRC.

- **Rx Oversize :**

The number of long 2 frames received with valid CRC.

- **Rx Fragments :**

  The number of short 1 frames received with invalid CRC.

- **Rx Jabber :**

  The number of long 2 frames received with invalid CRC. .

Transmit Error Counters

- **Tx Drops :**

  The number of frames dropped due to output buffer congestion.

- **Tx Late/Exc. Coll. :**

  The number of frames dropped due to excessive or late collisions.

- **Tx Oversize :**

  The number of frames dropped due to frame oversize.

Buttons

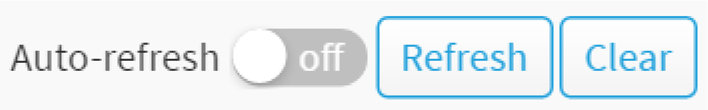


Figure 3-2: The Detailed Port Statistics buttons

- **Auto-refresh :**

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

- **Refresh :**

  Click to refresh the page.

- **Clear :**

  Clears the counters for the selected port.

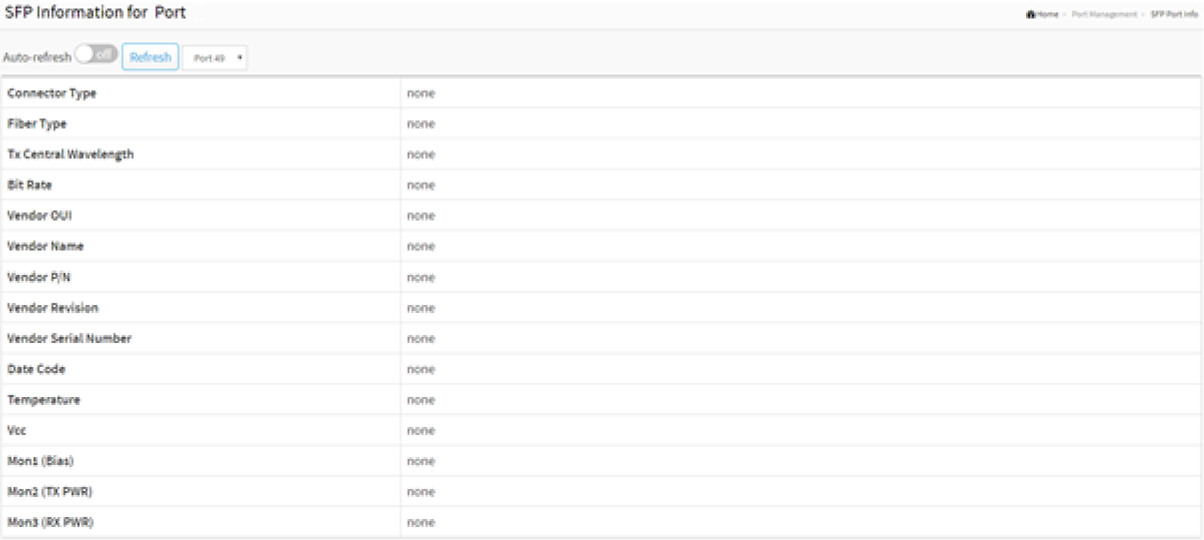
3-3 SFP Port Info

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 the SFP information in the web interface:

1. Click Port Management and SFP Port Info.
2. To display the SFP Information.



SFP Information for Port

Connector Type	none
Fiber Type	none
Tx Central Wavelength	none
Bit Rate	none
Vendor OUI	none
Vendor Name	none
Vendor P/N	none
Vendor Revision	none
Vendor Serial Number	none
Date Code	none
Temperature	none
Vcc	none
Mon1 (Bias)	none
Mon2 (TX PWR)	none
Mon3 (RX PWR)	none

Figure 3-3: The SFP Port Information

Parameter description:

- **Upper left scroll bar:**

  To scroll which port to display the Port statistics.

- **Connector Type:**

  Display the connector type, for instance, UTP, SC, ST, LC and so on.

- **Fiber Type:**

  Display the fiber mode, for instance, Multi-Mode, Single-Mode.

- **Tx Central Wavelength:**

  Display the fiber optical transmitting central wavelength, for instance, 850nm, 1310nm, 1550nm and so on.

- **Bit Rate:**

  Displays the nominal bit rate of the transceiver.

- **Vendor OUI:**

  Display the Manufacturer's OUI code which is assigned by IEEE.

- **Vendor Name:**

  Display the company name of the module manufacturer.

- **Vendor P/N:**

  Display the product name of the naming by module manufacturer.

- **Vendor Rev (Revision):**

  Display the module revision.

- **Vendor SN (Serial Number):**

  Show the serial number assigned by the manufacturer.

- **Date Code:**

  Show the date this SFP module was made.

- **Temperature:**

  Show the current temperature of SFP module.

- **Vcc:**

  Show the working DC voltage of SFP module.

- **Mon1(Bias) mA:**

  Show the Bias current of SFP module.

- **Mon2(TX PWR):**

  Show the transmit power of SFP module.

- **Mon3(RX PWR):**

  Show the receiver power of SFP module.

Buttons

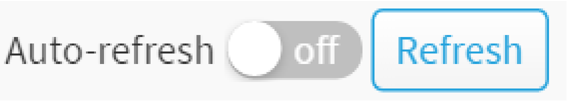


Figure 3-3: The SFP Port Information buttons

- **Auto-refresh :**

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

- **Refresh :**

  Click to refresh the page.

3-4 Energy Efficient Ethernet

EEE is an abbreviation for Energy Efficient Ethernet defined in IEEE 802.3az.

This page allows the user to inspect and configure the current EEE port settings.

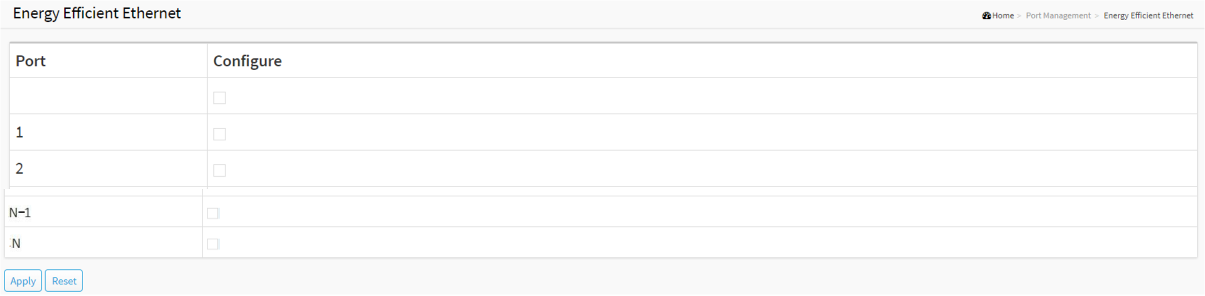
EEE is a power saving option that reduces the power usage when there is very low traffic utilization (or no traffic).

EEE works by powering down circuits when there is no traffic. When a port gets data to be transmitted all circuits are powered up. The time it takes to power up the circuits is named wakeup time. The default wakeup time is 17 us for 1Gbit links and 30 us for other link speeds. EEE devices must agree upon the value of the wakeup time in order to make sure that both the receiving and transmitting device has all circuits powered up when traffic is transmitted. The devices can exchange information about the devices wakeup time using the LLDP protocol.

Web Interface

To configure an Energy Efficient Ethernet in the web interface:

1. Click Port Management and Energy Efficient Ethernet.
2. Select enable or disable Energy Efficient Ethernet by the port.
3. Click the apply to save the setting.
4. If you want to cancel the setting then you need to click the Reset button. It will revert to previously saved values.



Energy Efficient Ethernet

Port	Configure
	□
1	□
2	□
N-1	□
N	□

Figure 4-4: The Energy Efficient Ethernet Configuration

Parameter description:

- **Port :**

  The switch port number of the logical EEE port.

- **Configure :**

  Controls whether EEE is enabled for this switch port.

Buttons

- **Apply :**

  Click to save changes.

- **Reset :**

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

3-5 Link *Aggregation*

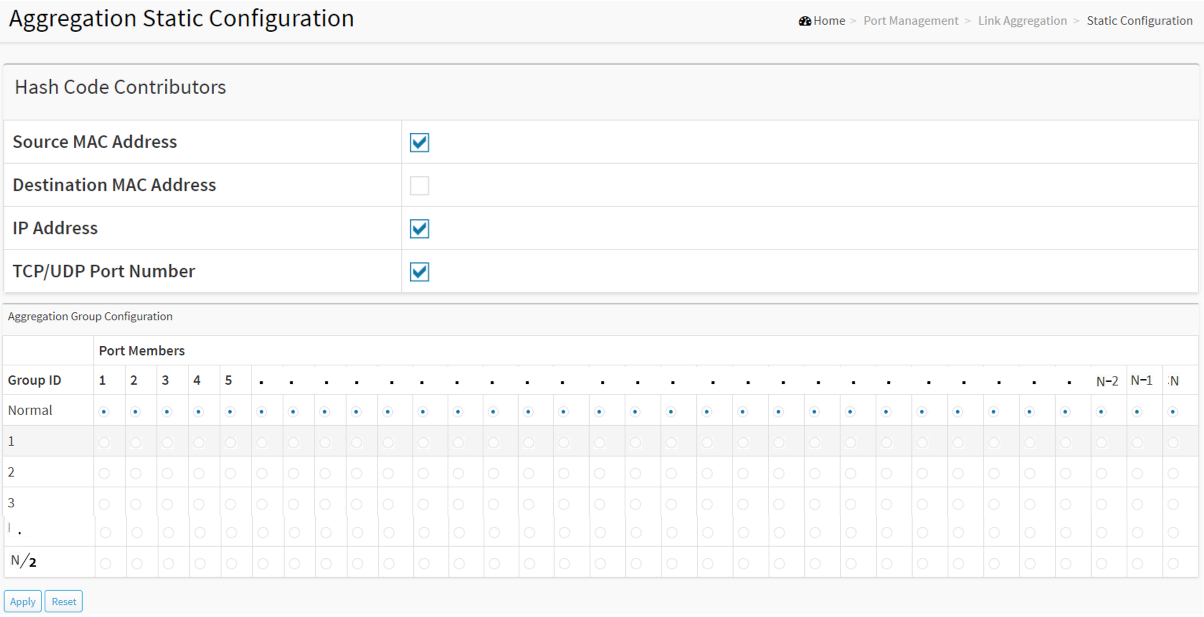
3-5.1 Static Configuration

This page is used to configure the Aggregation hash mode and the aggregation group.

Web Interface

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

1. Click Port Management, Link Aggregation and Static Configuration.
2. Evoke to enable or disable the aggregation mode function.
3. Evoke Aggregation Group ID and Port members.
4. Click Apply to save the setting.
5. If you want to cancel the setting then you need to click the reset button. It will revert to previously saved values.



Aggregation Static Configuration

Home > Port Management > Link Aggregation > Static Configuration

Hash Code Contributors

Source MAC Address	☑
Destination MAC Address	□
IP Address	☑
TCP/UDP Port Number	☑

Aggregation Group Configuration

	Port Members																															
Group ID	1	2	3	4	5	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	N-2	N-1	N
Normal	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●
1	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○
2	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○
3	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○
| .	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○
N/2	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○

Figure 3-5.1: The Static Configuration

Parameter description :

Hash Code Contributors

- **Source MAC Address :**

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

- **Destination MAC Address :**

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

- **IP Address :**

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

- **TCP/UDP Port Number :**

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

Aggregation Group Configuration

- **Group ID :**

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

- **Port Members :**

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

Buttons

- **Apply :**

  Click to save changes.

- **Reset :**

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

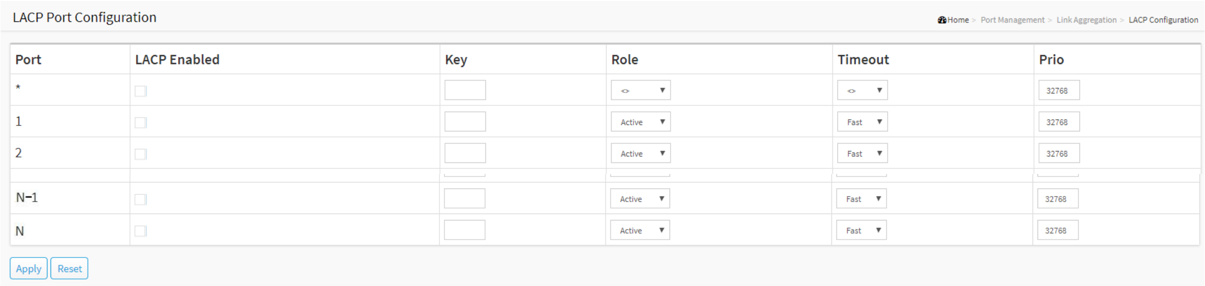
3-5.2 LACP Configuration

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

Web Interface

To configure the LACP Port Configuration in the web interface:

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



LACP Port Configuration

Home > Port Management > Link Aggregation > LACP Configuration

Port	LACP Enabled	Key	Role	Timeout	Prio
*	□		<> ▼	<> ▼	32768
1	□		Active ▼	Fast ▼	32768
2	□		Active ▼	Fast ▼	32768
N-1	□		Active ▼	Fast ▼	32768
N	□		Active ▼	Fast ▼	32768

Figure 3-5.2: The Lacp Configuration

Parameter description:

- **Port :**

  The switch port number.

- **LACP Enabled :**

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

- **Key :**

  The Key value incurred by the port, range 1-65535 . The Auto setting will set the key as appropriate by the physical link speed, 10Mb = 1, 100Mb = 2, 1Gb = 3. Using the Specific setting, a user-defined value can be entered. Ports with the same Key value can participate in the same aggregation group, while ports with different keys cannot.

- **Role :**

  The Role shows the LACP activity status. The Active will transmit LACP packets each second, while Passive will wait for a LACP packet from a partner (speak if spoken to).

- **Timeout :**

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

- **Prio :**

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

Buttons

- **Apply :**

  Click to save changes.

- **Reset :**

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

3-5.3 System Status

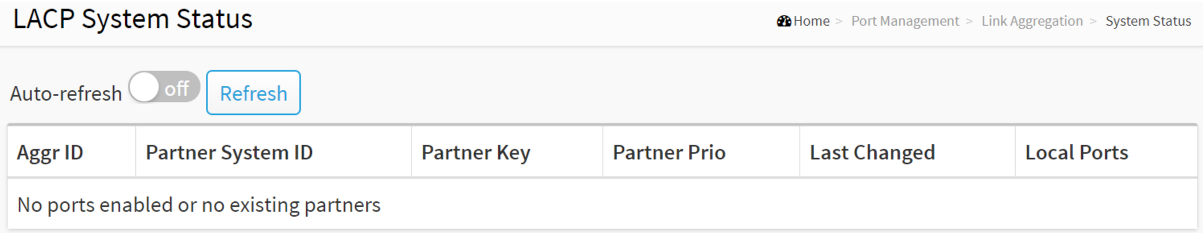
This section describes that when you complete to set LACP function on the switch then it provides a status overview for all LACP instances

Web Interface

To display the LACP System status in the web interface:

Click Port Management, Link Aggregation and System Status.
Checked “Auto-refresh”.

1. Click “Refresh” to refresh the port detailed statistics.



Aggr ID	Partner System ID	Partner Key	Partner Prio	Last Changed	Local Ports
No ports enabled or no existing partners					

Figure 3-5.3: The LACP System Status

Parameter description:

- **Aggr ID :**

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

- **Partner System ID :**

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

- **Partner Key :**

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

- **Partner Prio**

  The priority that the partner has assigned to this aggregation ID.

- **Last changed :**

  The time since this aggregation changed.

- **Local Ports :**

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

Buttons

Figure 3-5.3: The LACP System Status buttons

- **Auto-refresh :**

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

- **Refresh :**

  Click to refresh the page.

3-5.4 Internal Status

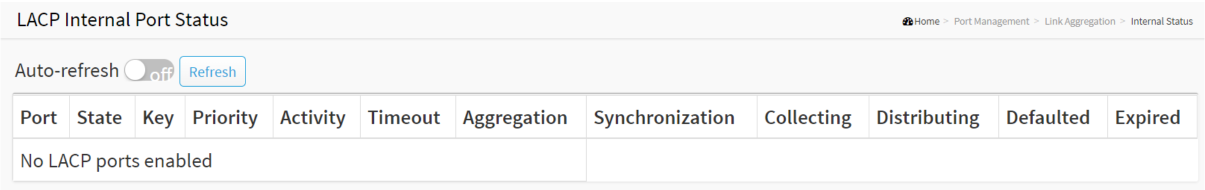
This page provides a status overview for the LACPinternal (i.e. local system) status for all ports. Only ports that are part of an LACP group are shown. For details on the shown parameters please refer to IEEE 801.AX-2014.

Web Interface

To display the LACP Internal System status in the web interface:

Click Port Management, Link Aggregation and Internal Status.
Checked “Auto-refresh”.

1. Click “Refresh” to refresh the port detailed statistics.



LACP Internal Port Status

Home > Port Management > Link Aggregation > Internal Status

Port	State	Key	Priority	Activity	Timeout	Aggregation	Synchronization	Collecting	Distributing	Defaulted	Expired
No LACP ports enabled											

Figure 3-5.4: The LACP Internal Status

Parameter description:

- **Port :**

  The switch port number.

- **State :**

  The current port state:

  Down: The port is not active.

  Active: The port is in active state.

  Standby: The port is in standby state.

- **Key :**

  The key assigned to this port. Only ports with the same key can aggregate together.

- **Priority :**

  The priority assigned to this aggregation group.

- **Activity :**

  The LACP mode of the group (Active or Passive).

- **Timeout :**

  The timeout mode configured for the port (Fast or Slow).

- **Aggregation :**

  Show whether the system considers this link to be "aggregateable"; i.e., a potential candidate for aggregation.

- **Synchronization :**

  Show whether the system considers this link to be "IN_SYNC"; i.e., it has been allocated to the correct LAG, the group has been associated with a compatible Aggregator, and the identity of the LAG is consistent with the System ID and operational Key information transmitted.

- **Collecting :**

  Show if collection of incoming frames on this link is enabled.

- **Distributing :**

  Show if distribution of outgoing frames on this link is enabled.

- **Defaulted :**

  Show if the Actor's Receive machine is using Defaulted operational Partner information.

- **Expired :**

  Show if that the Actor's Receive machine is in the EXPIRED state.

Buttons

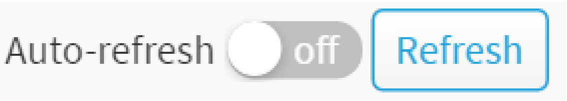


Figure 3-5.4: The LACP Internal Status buttons

- **Auto-refresh :**

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

- **Refresh :**

  Click to refresh the page.

3-5.5 Neighbor Status

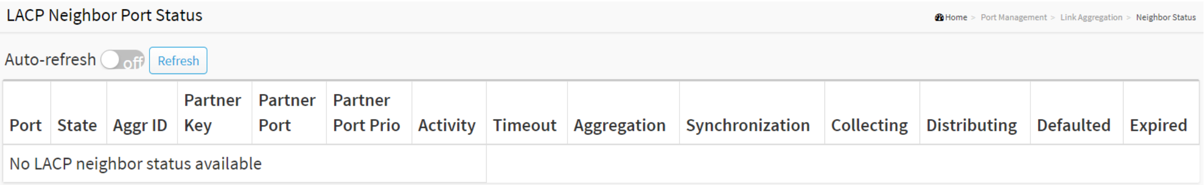
This page provides a status overview for the LACPneighbor status for all ports. Only ports that are part of an LACP group are shown. For details on the shown parameters please refer to IEEE 801.AX-2014.X

Web Interface

To display the LACP Neighbor Port status in the web interface:

Click Port Management, Link Aggregation and Neighbor Status.
Checked “Auto-refresh”.

1. Click “Refresh” to refresh the port detailed statistics.



LACP Neighbor Port Status

Port	State	Aggr ID	Partner Key	Partner Port	Partner Port Prio	Activity	Timeout	Aggregation	Synchronization	Collecting	Distributing	Defaulted	Expired
No LACP neighbor status available													

Figure 3-5.5: The LACP Neighbor Port Status

Parameter description:

- **Aggr ID :**

  The aggregation group ID which the port is assigned to.

- **Port :**

  The switch port number.

- **State :**

  The current port state:

  Down: The port is not active.

  Active: The port is in active state.

  Standby: The port is in standby state.

- **Partner Key**

  The key assigned to this port by the partner.

- **Partner Port**

  The partner port number associated with this link.

- **Partner Port Priority**

  The priority assigned to this partner port .

- **Activity :**

  The LACP mode of the group (Active or Passive).

- **Timeout :**

The timeout mode configured for the port (Fast or Slow).

- **Aggregation :**

  Show whether the system considers this link to be "aggregateable"; i.e., a potential candidate for aggregation.

- **Synchronization :**

  Show whether the system considers this link to be "IN_SYNC"; i.e., it has been allocated to the correct LAG, the group has been associated with a compatible Aggregator, and the identity of the LAG is consistent with the System ID and operational Key information transmitted.

- **Collecting :**

  Show if collection of incoming frames on this link is enabled.

- **Distributing :**

  Show if distribution of outgoing frames on this link is enabled.

- **Defaulted :**

  Show if the Actor's Receive machine is using Defaulted operational Partner information.

- **Expired :**

  Show if that the Actor's Receive machine is in the EXPIRED state.

Buttons

Figure 3-5.5: The LACP Neighbor Port Status buttons

- **Auto-refresh :**

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

- **Refresh :**

  Click to refresh the page.

3-5.6 Port Status

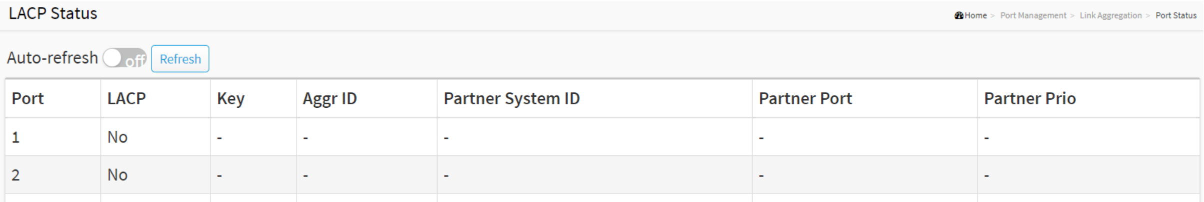
This section describes that when you complete to set LACP function on the switch then it provides a Port Status overview for all LACP instances

Web Interface

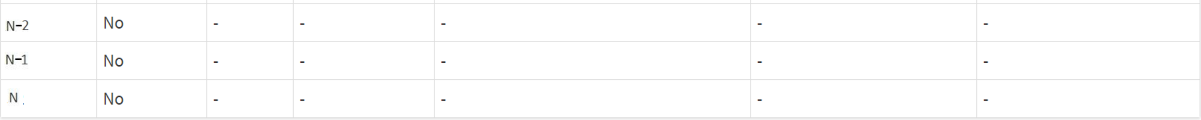
To display the LACP Port status in the web interface:

Click Port Management, Link Aggregation and Port Status.
If you want to auto-refresh the information then you need to evoke the “Auto-refresh”.

1. Click “Refresh” to refresh the LACP Port Status.



Port	LACP	Key	Aggr ID	Partner System ID	Partner Port	Partner Prio
1	No	-	-	-	-	-
2	No	-	-	-	-	-



N-2	No	-	-	-	-	-
N-1	No	-	-	-	-	-
N	No	-	-	-	-	-

Figure 3-5.6: The LACP Status

Parameter description:

- **Port :**

  The switch port number.

- **LACP :**

  'Yes' means that LACP is enabled and the port link is up. 'No' means that LACP is not enabled or that the port link is down. 'Backup' means that the port could not join the aggregation group but will join if other port leaves. Meanwhile it's LACP status is disabled.

- **Key :**

  The key assigned to this port. Only ports with the same key can aggregate together.

- **Aggr ID :**

  The Aggregation ID assigned to this aggregation group. IDs 1 and 2 are GLAGs while IDs 3-14 are LLAGs.

- **Partner System ID :**

  The partner's System ID (MAC address).

- **Partner Port :**

  The partner's port number connected to this port.

- **Partner Prio:**

  The partner's port priority.

Buttons

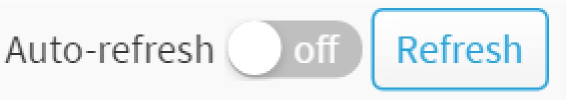


Figure 3-5.4: The Port Status buttons

- **Auto-refresh :**

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

- **Refresh :**

  Click to refresh the page.

3-6 Loop Protection

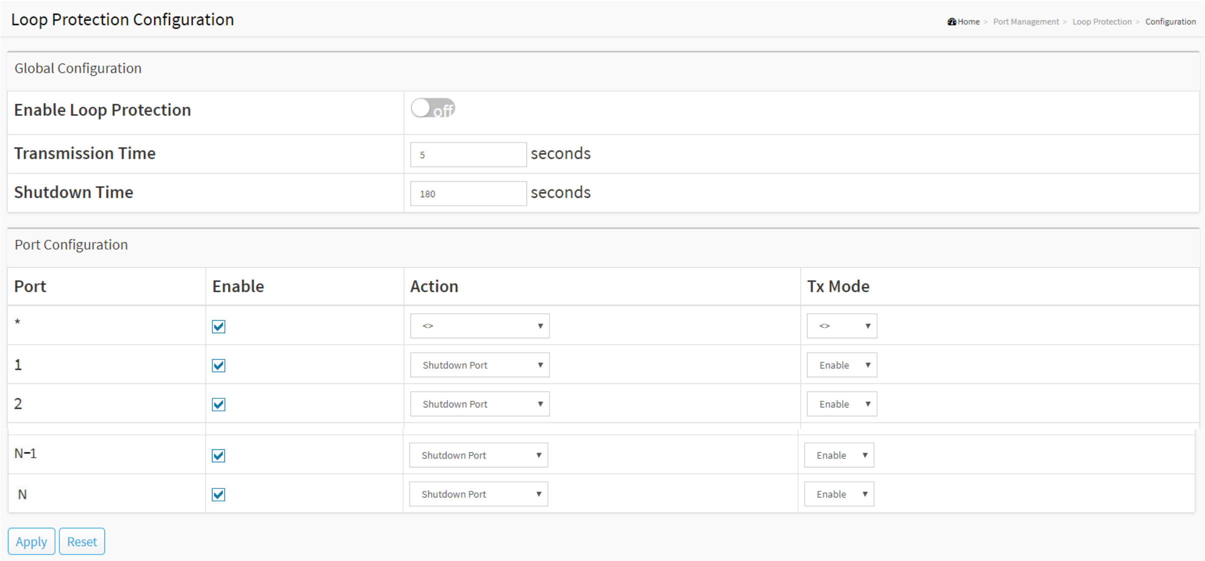
3-6.1 Configuration

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

Web Interface

To configure the Loop Protection parameters in the web interface:

1. Click Port Management, Loop Protection and Configuration.
2. Evoke to select enable or disable the port loop Protection.
3. Click the apply to save the setting.
4. If you want to cancel the setting then you need to click the Reset button. It will revert to previously saved values.



Loop Protection Configuration

Global Configuration

Enable Loop Protection	off
Transmission Time	5 seconds
Shutdown Time	180 seconds

Port Configuration

Port	Enable	Action	Tx Mode
*	☑	<>	<>
1	☑	Shutdown Port	Enable
2	☑	Shutdown Port	Enable
N-1	☑	Shutdown Port	Enable
N	☑	Shutdown Port	Enable

Figure 3-6.1: The Loop Protection Configuration

Parameter description :

Global Configuration

- **Enable Loop Protection :**

  Controls whether loop protections is enabled (as a whole).

- **Transmission Time :**

  The interval between each loop protection PDU sent on each port. Valid values are 1 to 10 seconds.

- **Shutdown Time :**

  The period (in seconds) for which a port will be kept disabled in the event of a loop is detected (and the port action shuts down the port). Valid values are 10 to 604800 seconds (7 days).

Port Configuration

- **Port :**

  The switch port number of the port.

- **Enable :**

  Controls whether loop protection is enabled on this switch port

- **Action:**

  Configures the action performed when a loop is detected on a port. Valid values are Shutdown Port, Shutdown Port and Log or Log Only.

- **Tx Mode :**

Controls whether the port is actively generating loop protection PDU's, or whether it is just passively looking for looped PDU's.

Buttons

- **Apply :**

  Click to save changes.

- **Reset :**

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

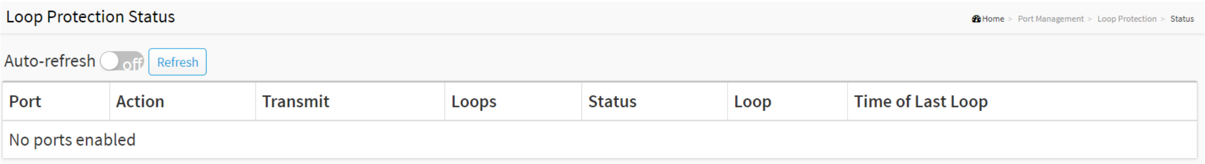
3-6.2 Status

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

Web Interface

To display the Loop Protection status in the web interface:

1. Click Port Management, Loop Protection and Status.
2. If you want to auto-refresh the information then you need to evoke the “Auto refresh”.
3. Click “Refresh” to refresh the Loop Protection Status.



Loop Protection Status

Home > Port Management > Loop Protection > Status

Auto-refresh off Refresh

Port	Action	Transmit	Loops	Status	Loop	Time of Last Loop
No ports enabled						

Figure 3-6.2: Loop Protection Status

Parameter description:

- **Port**

  The switch port number of the logical port.

- **Action**

  The currently configured port action.

- **Transmit**

  The currently configured port transmit mode.

- **Loops**

  The number of loops detected on this port.

- **Status**

  The current loop protection status of the port.

- **Loop**

  Whether a loop is currently detected on the port.

- **Time of Last Loop**

  The time of the last loop event detected.

Buttons

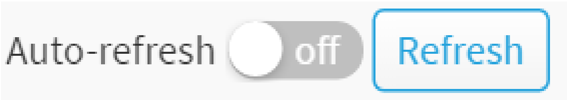


Figure 3-6.2: Loop Protection Status buttons

- **Auto-refresh :**

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

- **Refresh :**

  Click to refresh the page immediately.

3-7 UDLD

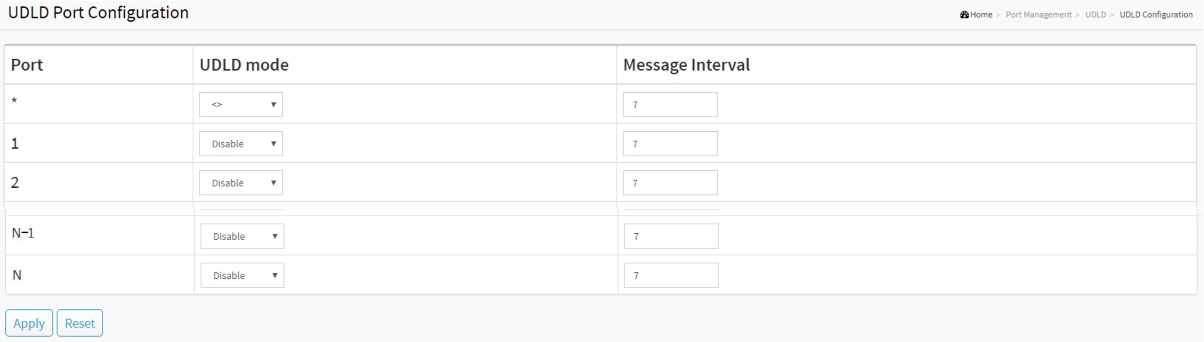
3-7.1 UDLD Configuration

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

Web Interface

To configure the UDLD parameters in the web interface:

1. Click Port Management, UDLD and UDLD Configuration.
2. Evoke to select enable or disable the port UDLD.
3. Specify the Message Interval.
4. Click the apply to save the setting.
5. If you want to cancel the setting then you need to click the Reset button. It will revert to previously saved values.



UDLD Port Configuration

Port	UDLD mode	Message Interval
*	<>	7
1	Disable	7
2	Disable	7
N-1	Disable	7
N	Disable	7

Figure 3-7.1: The UDLD Configuration

Parameter description :

- **Port :**

  Port number of the switch.

- **UDLD Mode :**

  Configures the UDLD mode on a port. Valid values are Disable, Normal and Aggressive. Default mode is Disable.

  Disable: In disabled mode, UDLD functionality doesn't exists on port.

  Normal: In normal mode, if the link state of the port was determined to be unidirectional, it will not affect the port state.

  Aggressive: In aggressive mode, unidirectional detected ports will get shutdown. To bring back the ports up, need to disable UDLDon that port.

- **Message Interval :**

  Configures the period of time between UDLD probe messages on ports that are in the advertisement phase and are determined to be bidirectional. The range is from 7 to 90 seconds(Default value is 7 seconds)(Currently default time interval is supported, due to lack of detailed information in RFC 5171).

Buttons

- **Apply :**

  Click to save changes.

- **Reset :**

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

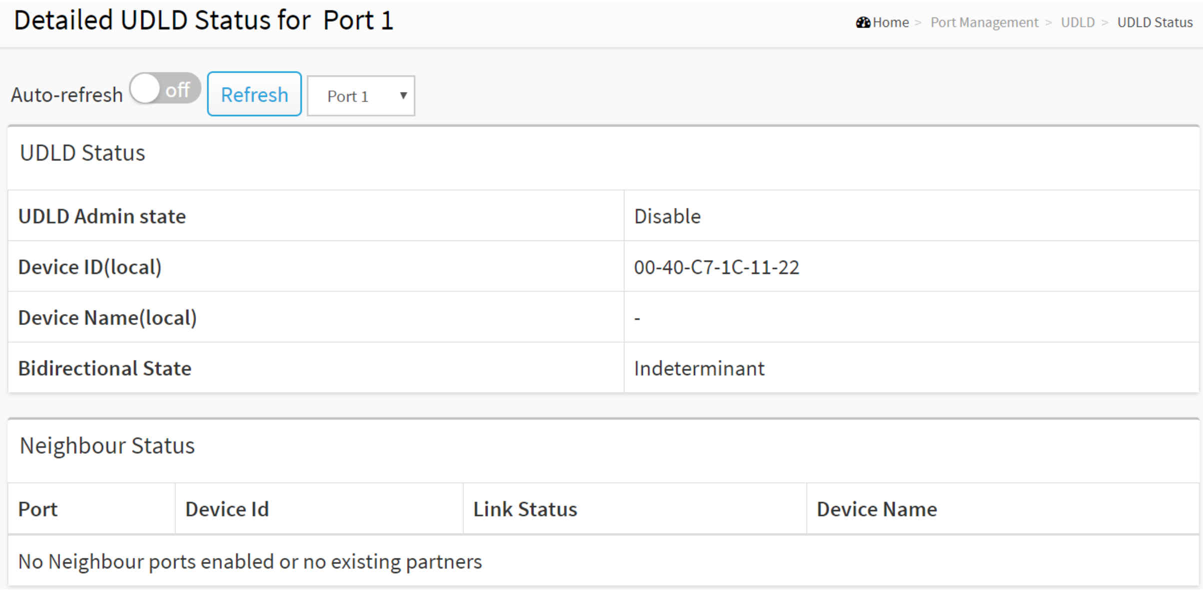
3-7.2 UDLD Status

This page displays the UDLD status of the ports

Web Interface

To display the Loop Protection status in the web interface:

1. Click Port Management, UDLD and UDLD Status.
2. Select port that you want to display the UDLD Status.
3. If you want to auto-refresh the information then you need to evoke the “Auto refresh”.
4. Click “Refresh” to refresh the Loop Protection Status.



Detailed UDLD Status for Port 1

UDLD Status

UDLD Admin state	Disable
Device ID(local)	00-40-C7-1C-11-22
Device Name(local)	-
Bidirectional State	Indeterminant

Neighbour Status

Port	Device Id	Link Status	Device Name
No Neighbour ports enabled or no existing partners			

Figure 3-7.2: UDLD Status

Parameter description :

UDLD port status

- **UDLD Admin State :**

  The current port state of the logical port, Enabled if any of state(Normal,Aggressive) is Enabled.

  Device ID(local): The ID of Device.

  Device Name(local): Name of the Device.

  Bidirectional State: The current state of the port.

Neighbour Status

- **Port :**

  The current port of neighbour device.

- **Device ID :**

  The current ID of neighbour device.

- **Link Status :**

The current link status of neighbour port.

- **Device Name :**

  Name of the Neighbour Device.

Buttons

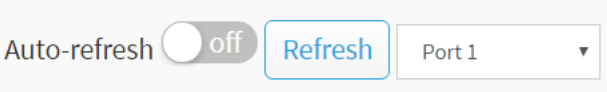


Figure 3-7.2: UDLD Status buttons

- **Auto-refresh :**

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

- **Refresh :**

  Click to refresh the page immediately.

- **Port 1 :**

  Select port that you want to display the DHCP Detailed Statistics.

Chapter 4 PoE Management

PoE is an acronym for Power over Ethernet. Power over Ethernet is used to transmit electrical power, to remote devices over standard Ethernet cable. It could for example be used for powering IP telephones, wireless LAN access points and other equipment, where it would be difficult or expensive to connect the equipment to main power supply.

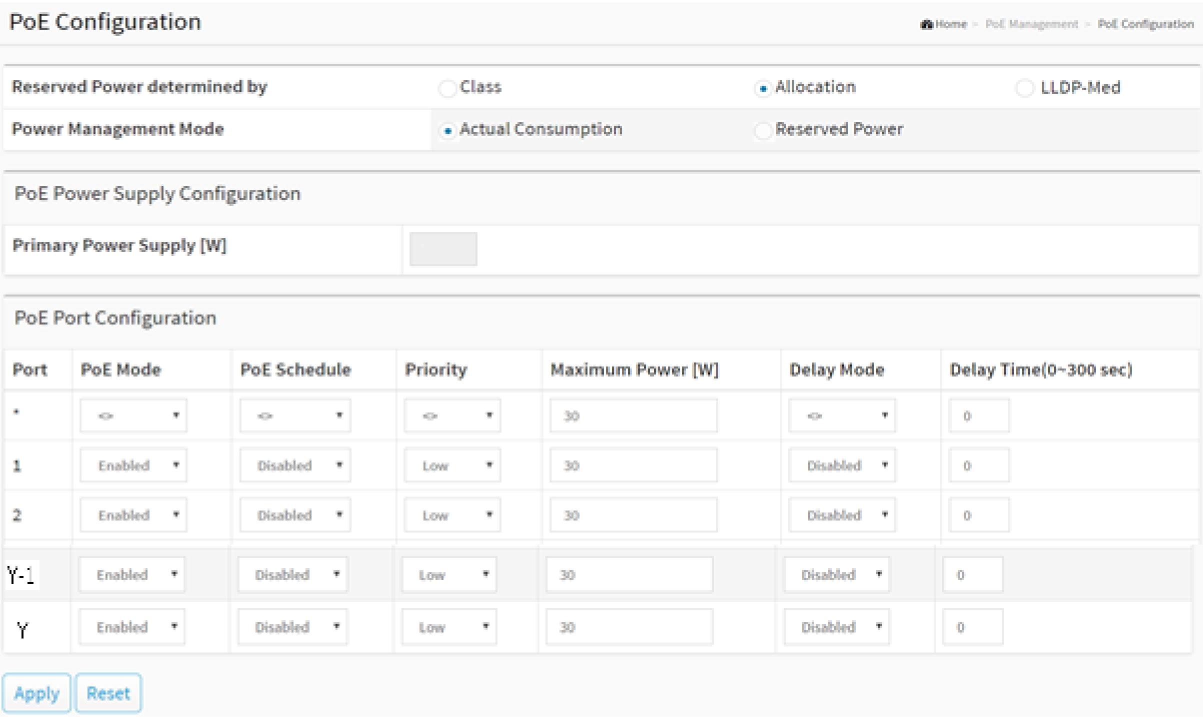
4-1 PoE Configuration

This page allows the user to inspect and configure the current PoE port settings and show all PoE Supply W.

Web Interface

To configure Power over Ethernet in the web interface:

1. Click PoE Management and PoE Configuration.
2. Specify the Reserved Power determined .
3. Specify the PoE or PoE+ Mode, PoE Schedule, Priority, Maximum Power(W), Delay Mode and Delay Time.
4. Click Apply to save the configuration.
5. If you want to cancel the setting then you need to click the Reset button. It will revert to previously saved values.



PoE Configuration

Reserved Power determined by	○ Class	● Allocation	○ LLDP-Med
Power Management Mode	● Actual Consumption	○ Reserved Power	

PoE Power Supply Configuration

Primary Power Supply [W]	

PoE Port Configuration

Port	PoE Mode	PoE Schedule	Priority	Maximum Power [W]	Delay Mode	Delay Time(0~300 sec)
*	<>	<>	<>	30	<>	0
1	Enabled	Disabled	Low	30	Disabled	0
2	Enabled	Disabled	Low	30	Disabled	0
Y-1	Enabled	Disabled	Low	30	Disabled	0
Y	Enabled	Disabled	Low	30	Disabled	0

Figure 4-1: PoE Configuration

Parameter description:

Power Over Ethernet Configuration

- **Reserved Power determined by :**

  There are three modes for configuring how the ports/PDs may reserve power.

  1. Allocated mode: In this mode the user allocates the amount of power that each port may reserve. The allocated/reserved power for each port/PD is specified in the Maximum Power fields.

  2. Class mode: In this mode each port automatically determines how much power to reserve according to the class the connected PD belongs to, and reserves the power accordingly. Four different port classes exist and one for 4, 7, 15.4 or 30 Watts.

  In this mode the Maximum Power fields have no effect.

  3. LLDP-MED mode: This mode is similar to the Class mode expect that each port determine the amount power it reserves by exchanging PoE information using the LLDP protocol and reserves power accordingly. If no LLDP information is available for a port, the port will reserve power using the class mode

  In this mode the Maximum Power fields have no effect

  For all modes: If a port uses more power than the reserved power for the port, the port is shut down.

- **Power Management Mode :**

  There are 2 modes for configuring when to shut down the ports:

  1. Actual Consumption: In this mode the ports are shut down when the actual power consumption for all ports exceeds the amount of power that the power supply can deliver or if the actual power consumption for a given port exceeds the reserved power for that port. The ports are shut down according to the ports priority. If two ports have the same priority the port with the highest port number is shut down.

  2. Reserved Power: In this mode the ports are shut down when total reserved powered exceeds the amount of power that the power supply can deliver. In this mode the port power is not turned on if the PD requests more power than available from the power supply.

PoE Power Supply Configuration

- **Primary Power Supply [W] :**

  To display watts for the primary power supply.

PoE Port Configuration

- **Port :**

  This is the logical port number for this row.

- **PoE Mode :**

  The PoE Mode represents the PoE operating mode for the port. Enable or Disable PoE.

- **PoE Schedule :**

  Disable or Select the PoE Schedule profile.

- **Priority :**

  The Priority represents the ports priority. There are three levels of power priority named Low, High and Critical.

  The priority is used in the case where the remote devices requires more power than the power supply can deliver. In this case the port with the lowest priority will be turn off starting from the port with the highest port number.

- **Maximum Power [W] :**

  The Maximum Power value contains a numerical value that indicates the maximum power in watts that can be delivered to a remote device.

  The maximum allowed value is 30 W.

- **Delay Mode :**

  Turn on / off the power delay function.
  Enabled: Enable POE Power Delay.
  Disabled: Disable POE Power Delay.

- **Delay Time(0~300sec) :**

  When rebooting, the PoE port will start to provide power to the PD when it out of delay time. default: 0, range: 0-300 sec.

Buttons

- **Apply :**

  Click to save changes.

- **Reset :**

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

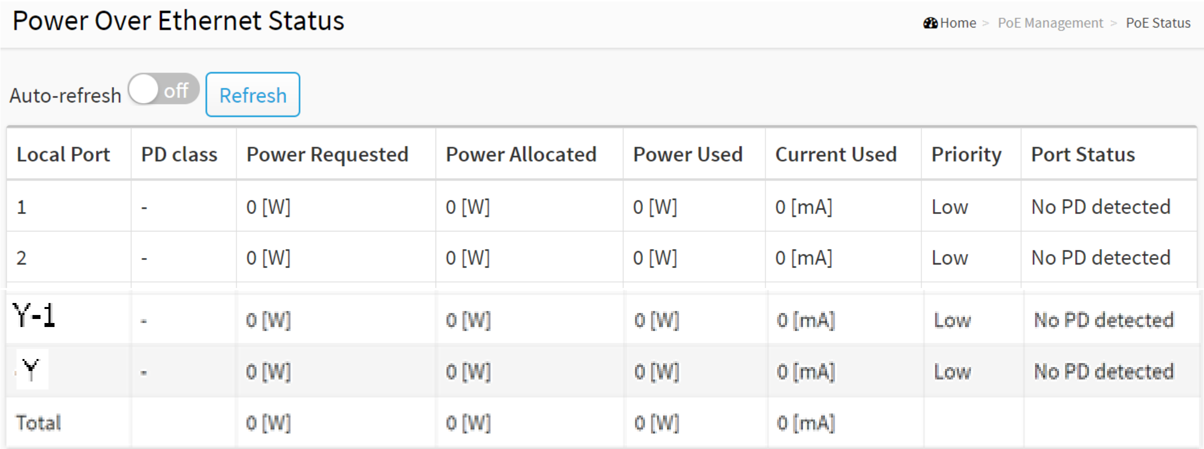
4-2 PoE Status

This page allows the user to inspect the current status for all PoE ports.

Web Interface

To Display PoE Status in the web interface:

1. Click PoE Management and PoE Status
2. Scroll "Auto-refresh" to on/off.
3. Click "Refresh" to refresh the port detailed statistics.



Power Over Ethernet Status

Local Port	PD class	Power Requested	Power Allocated	Power Used	Current Used	Priority	Port Status
1	-	0 [W]	0 [W]	0 [W]	0 [mA]	Low	No PD detected
2	-	0 [W]	0 [W]	0 [W]	0 [mA]	Low	No PD detected
Y-1	-	0 [W]	0 [W]	0 [W]	0 [mA]	Low	No PD detected
Y	-	0 [W]	0 [W]	0 [W]	0 [mA]	Low	No PD detected
Total		0 [W]	0 [W]	0 [W]	0 [mA]		

Figure 4-2: The PoE Status

Parameter description:

- **Local Port :**

  This is the logical port number for this row.

- **PD Class :**

  Each PD is classified according to a class that defines the maximum power the PD will use. The PD Class shows the PDs class.

  Five Classes are defined:

  Class 0: Max. power 15.4 W

  Class 1: Max. power 4.0 W

  Class 2: Max. power 7.0 W

  Class 3: Max. power 15.4 W

  Class 4: Max. power 30.0 W

- **Power Requested**

  The Power Requested shows the requested amount of power the PD wants to be reserved.

- **Power Allocated :**

  The Power Allocated shows the amount of power the switch has allocated for the PD.

- **Power Used :**

  The Power Used shows how much power the PD currently is using.

- **Current Used :**

  The Power Used shows how much current the PD currently is using.

- **Priority :**

  The Priority shows the port's priority configured by the user.

- **Port Status :**

  The Port Status shows the port's status. The status can be one of the following values:

  PoE not available - No PoE chip found - PoE not supported for the port.

  PoE turned OFF - PoE disabled : PoE is disabled by user.

  PoE turned OFF - Power budget exceeded - The total requested or used power by the PDs exceeds the maximum power the Power Supply can deliver, and port(s) with the lowest priority is/are powered down.

  No PD detected - No PD detected for the port.

  PoE turned OFF - PD overload - The PD has requested or used more power than the port can deliver, and is powered down.

  PoE turned OFF - PD is off.

  Invalid PD - PD detected, but is not working correctly.

Buttons

Figure 4-2: The PoE Status buttons

- **Auto-refresh :**

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

- **Refresh :**

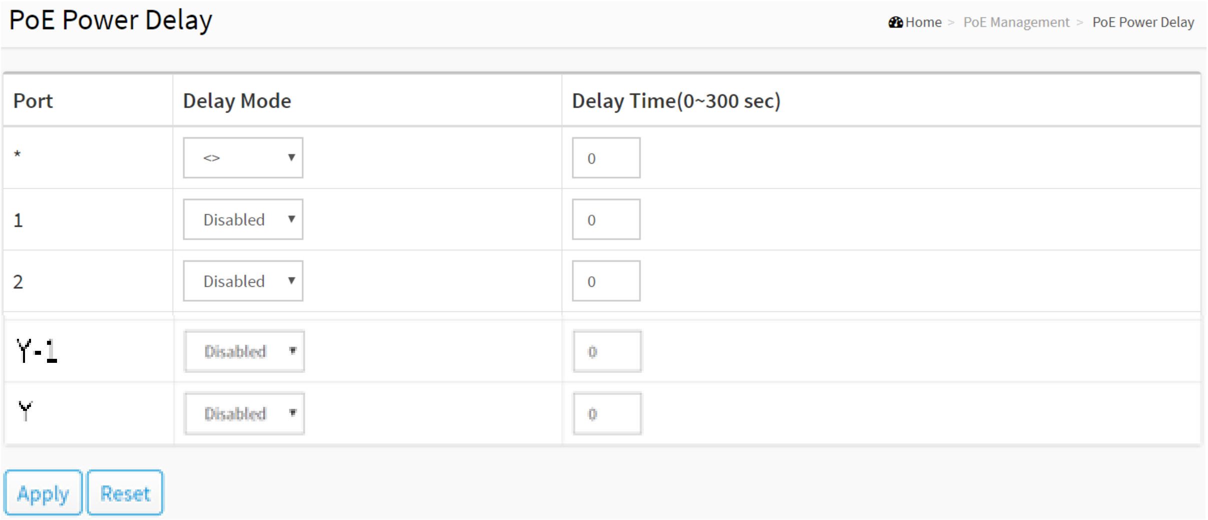
  Click to refresh the page immediately.

4-3 PoE Power Delay

This page allows the user to setting the delay time of power providing after device rebooted.

Web Interface

To Display Power over Ethernet Status in the web interface:
Click PoE Management and PoE Power delay.
Enable the port to the power device.
Specify the power providing delay time when reboot.
Click Apply to apply the change.



PoE Power Delay

Port	Delay Mode	Delay Time(0~300 sec)
*	<>	0
1	Disabled	0
2	Disabled	0
Y-1	Disabled	0
Y	Disabled	0

Figure 4-3: The PoE Power Delay

Parameter description:

- **Port :**

  This is the logical port number for this row.

- **Delay Mode :**

  Turn on / off the power delay function.

  Enabled: Enable POE Power Delay.

  Disabled: Disable POE Power Delay.

- **Delay Time(0~300sec) :**

  When rebooting, the PoE port will start to provide power to the PD when it out of delay time. Default: 0, range: 0-300 sec.

Buttons

- **Apply :**

  Click to save changes.

- **Reset :**

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

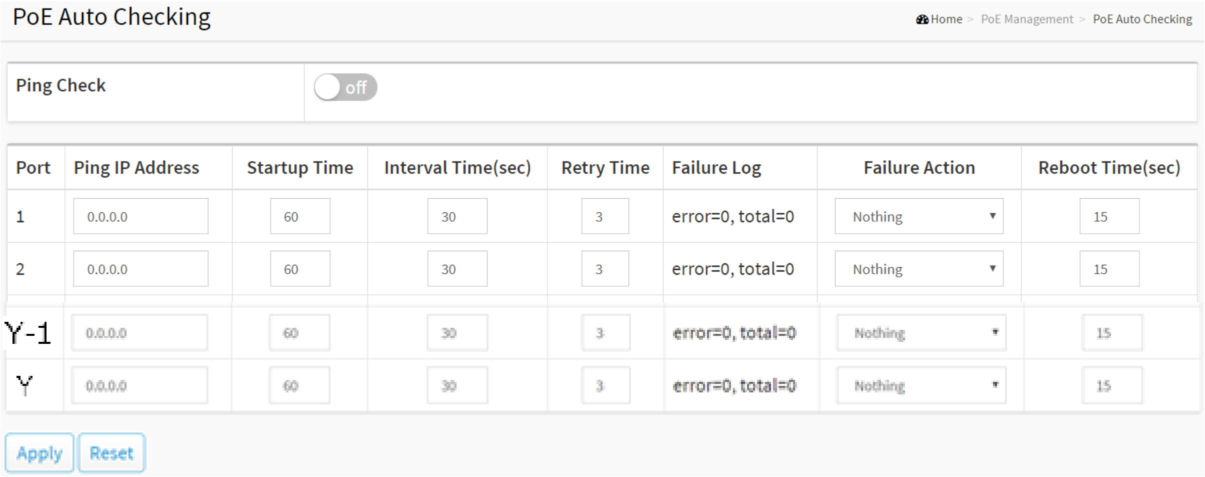
4-4 PoE Auto Checking

This page allows the user to specify the auto detection parameters to check the linking status between PoE ports and PDs. When it detected the fail connect, will reboot remote PD automatically.

Web Interface

To configue Power over Ethernet Auto Checking in the web interface:

1. Click PoE Management and PoE Auto checking.
2. Enable the Ping Check function.
3. Specify the PD's IP address, checking startup time, interval time, retry time, failure action and reboot time.
4. Click Apply to apply the change.



PoE Auto Checking

Ping Check: off

Port	Ping IP Address	Startup Time	Interval Time(sec)	Retry Time	Failure Log	Failure Action	Reboot Time(sec)
1	0.0.0.0	60	30	3	error=0, total=0	Nothing	15
2	0.0.0.0	60	30	3	error=0, total=0	Nothing	15
Y-1	0.0.0.0	60	30	3	error=0, total=0	Nothing	15
Y	0.0.0.0	60	30	3	error=0, total=0	Nothing	15

Figure 4-4: The PoE Auto Checking

Parameter description:

- **Ping Check :**

  Enable Ping Check function can detects the connection between PoE port and power device. Disable will turn off the detection.

- **Port :**

  This is the logical port number for this row.

- **Ping IP Address :**

  The PD's IP Address the system should ping.

- **Startup Time :**

  After startup time, device will enable auto checking. Default: 30, range: 30-60 sec.

- **Interval Time(sec) :**

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

- **Retry Time :**

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

- **Failure Log :**

  Failure loggings counter.

- **Failure Action :**

  The action when the third 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(sec) :**

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

Buttons

- **Apply :**

  Click to save changes.

- **Reset :**

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

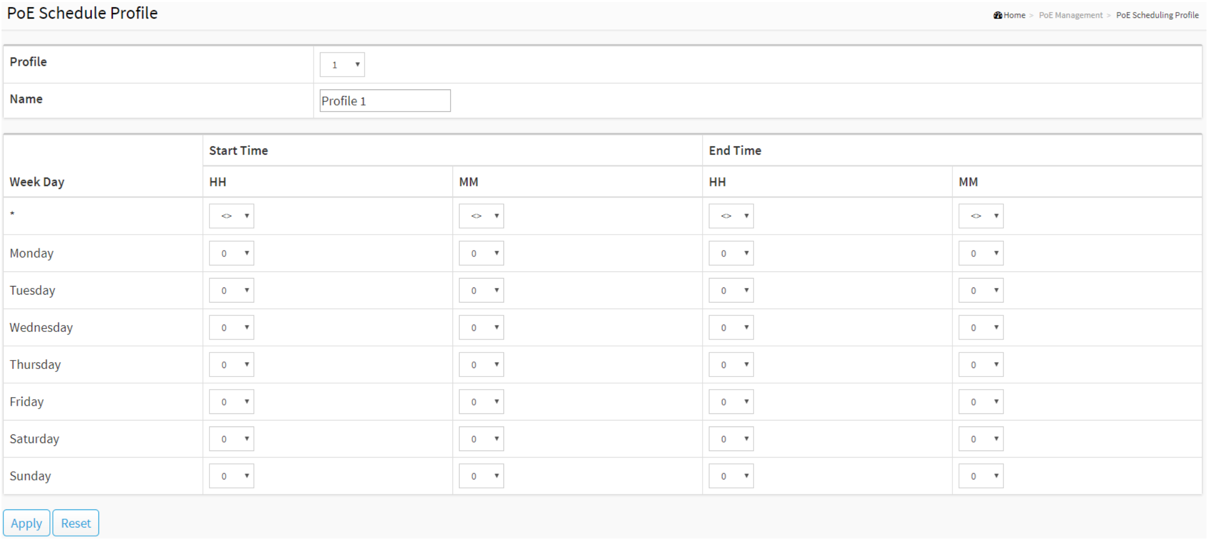
4-5 PoE Scheduleing Profile

This page allows user to define the profile for PoE scheduling.

Web Interface

To configure PoE Schedule Profile in the web interface:

1. Click PoE Management and PoE Scheduling Profile.
2. Select profile number and specify the profile name.
3. Select Week Day and Specify Start Time, End Time.
4. Click Apply to apply the change.



PoE Schedule Profile

Home > PoE Management > PoE Scheduling Profile

Profile	1 ▾
Name	Profile 1

Week Day	Start Time		End Time	
	HH	MM	HH	MM
*	<> ▾	<> ▾	<> ▾	<> ▾
Monday	0 ▾	0 ▾	0 ▾	0 ▾
Tuesday	0 ▾	0 ▾	0 ▾	0 ▾
Wednesday	0 ▾	0 ▾	0 ▾	0 ▾
Thursday	0 ▾	0 ▾	0 ▾	0 ▾
Friday	0 ▾	0 ▾	0 ▾	0 ▾
Saturday	0 ▾	0 ▾	0 ▾	0 ▾
Sunday	0 ▾	0 ▾	0 ▾	0 ▾

Figure 4-5: The PoE Schedule Profile

Parameter description:

- **Profile :**

  The index of profile. There are 16 profiles in the configuration.

- **Name :**

  The name of profile. The default name is "Profile #". User can define the name for identifying the profile.

- **Week Day :**

  The day to schedule PoE.

- **Start Time :**

  The time to start PoE. The time 00:00 means the first second of this day.

- **End Time :**

  The time to stop PoE. The time 00:00 means the last second of this day.

Buttons

- **Apply :**

  Click to save changes.

- **Reset :**

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

Chapter 5 VLAN Management

5-1 VLAN Configuration

To assign a specific VLAN for management purpose. The management VLAN is used to establish an IP connection to the switch from a workstation connected to a port in the VLAN. This connection supports a VSM, SNMP, and Telnet session. By default, the active management VLAN is VLAN 1, but you can designate any VLAN as the management VLAN using the Management VLAN window. Only one management VLAN can be active at a time.

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

Web Interface

To configure VLAN membership configuration in the web interface:

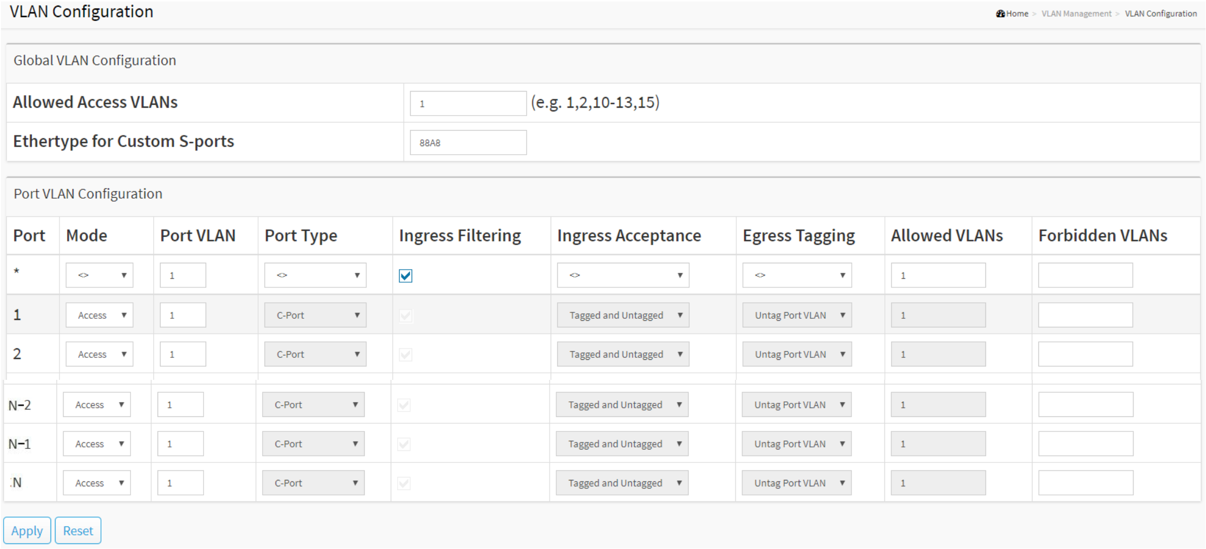
1. Click VLAN Management and VLAN Configuration.

2. Modify Global VLAN Configuration parameter.

3. Scroll the Mode, Port VLAN and Port Type to enable the Port VLAN Configuration parameter.

4. Click the Apply to save the setting.

5. If you want to cancel the setting then you need to click the Reset button. It will revert to previously saved values.



VLAN Configuration

Global VLAN Configuration

Allowed Access VLANs	1 (e.g. 1,2,10-13,15)
Ethertype for Custom S-ports	88A8

Port VLAN Configuration

Port	Mode	Port VLAN	Port Type	Ingress Filtering	Ingress Acceptance	Egress Tagging	Allowed VLANs	Forbidden VLANs
*	<>	1	<>	☑	<>	<>	1	
1	Access	1	C-Port	☑	Tagged and Untagged	Untag Port VLAN	1	
2	Access	1	C-Port	☑	Tagged and Untagged	Untag Port VLAN	1	
N-2	Access	1	C-Port	☑	Tagged and Untagged	Untag Port VLAN	1	
N-1	Access	1	C-Port	☑	Tagged and Untagged	Untag Port VLAN	1	
.N	Access	1	C-Port	☑	Tagged and Untagged	Untag Port VLAN	1	

Figure 5-1: The VLAN Configuration

Parameter description:

Global VLAN Configuration

- **Allowed Access VLANs :**

  This field shows the VLANs that are created on the switch.

  By default, only VLAN 1 exists. More VLANs may be created by using a list syntax where the individual elements are separated by commas. Ranges are specified with a dash separating the lower and upper bound.

  The following example will create VLANs 1, 10, 11, 12, 13, 200, and 300: 1,10-13,200,300. Spaces are allowed in between the delimiters.

- **Ethertype for Custom S-ports :**

  This field specifies the ethertype/TPID (specified in hexadecimal) used for Custom S-ports. The setting is in force for all ports whose Port Type is set to S-Custom-Port.

Port VLAN Configuration

- **Port :**

  This is the logical port number of this row.

- **Mode :**

  The port mode (default is Access) determines the fundamental behavior of the port in question. A port can be in one of three modes as described below. Whenever a particular mode is selected, the remaining fields in that row will be either grayed out or made changeable depending on the mode in question. Grayed out fields show the value that the port will get when the mode is applied.

  Access:
  Access ports are normally used to connect to end stations. Dynamic features like Voice VLAN may add the port to more VLANs behind the scenes. Access ports have the following characteristics:
  • Member of exactly one VLAN, the Port VLAN (a.k.a. Access VLAN), which by default is 1,
  • accepts untagged frames and C-tagged frames,
  • discards all frames that are not classified to the Access VLAN,
  • on egress all frames are transmitted untagged.

  Trunk:
  Trunk ports can carry traffic on multiple VLANs simultaneously, and are normally used to connect to other switches. Trunk ports have the following characteristics:
  • By default, a trunk port is member of all existing VLANs. This may be limited by the use of Allowed VLANs,
  • unless VLAN Trunking is enabled on the port, frames classified to a VLAN that the port is not a member of will be discarded,
  • by default, all frames but frames classified to the Port VLAN (a.k.a. Native VLAN) get tagged on egress. Frames classified to the Port VLAN do not get C-tagged on egress,
  • egress tagging can be changed to tag all frames, in which case only tagged frames are accepted on ingress,
  • VLAN trunking may be enabled.

  Hybrid:
  Hybrid ports resemble trunk ports in many ways, but adds additional port configuration features. In addition to the characteristics described for trunk ports, hybrid ports have these abilities:
  • Can be configured to be VLAN tag unaware, C-tag aware, S-tag aware, or S-custom-tag aware,
  • ingress filtering can be controlled,
  • ingress acceptance of frames and configuration of egress tagging can be configured independently.

- **Port VLAN :**

  Determines the port's VLAN ID (a.k.a. PVID). Allowed VLANs are in the range 1 through 4095, default being 1.
  On ingress, frames get classified to the Port VLAN if the port is configured as VLAN unaware, the frame is untagged, or VLAN awareness is enabled on the port, but the frame is priority tagged (VLAN ID = 0).
  On egress, frames classified to the Port VLAN do not get tagged if Egress Tagging configuration is set to untag Port VLAN.
  The Port VLAN is called an "Access VLAN" for ports in Access mode and Native VLAN for ports in Trunk or Hybrid mode.

- **Port Type :**

  Ports in hybrid mode allow for changing the port type, that is, whether a frame's VLAN tag is used to classify the frame on ingress to a particular VLAN, and if so, which TPID it reacts on. Likewise, on egress, the Port Type determines the TPID of the tag, if a tag is required.

  Unaware:
  On ingress, all frames, whether carrying a VLAN tag or not, get classified to the Port VLAN, and possible tags are not removed on egress.

  C-Port:
  On ingress, frames with a VLAN tag with TPID = 0x8100 get classified to the VLAN ID embedded in the tag. If a frame is untagged or priority tagged, the frame gets classified to the Port VLAN. If frames must be tagged on egress, they will be tagged with a C-tag.

  S-Port:
  On ingress, frames with a VLAN tag with TPID = 0x8100 or 0x88A8 get classified to the VLAN ID embedded in the tag. If a frame is untagged or priority tagged, the frame gets classified to the Port VLAN. If frames must be tagged on egress, they will be tagged with an S-tag.

  S-Custom-Port:
  On ingress, frames with a VLAN tag with a TPID = 0x8100 or equal to the Ethertype configured for Custom-S ports get classified to the VLAN ID embedded in the tag. If a frame is untagged or priority tagged, the frame gets classified to the Port VLAN. If frames must be tagged on egress, they will be tagged with the custom S-tag.

- **Ingress Filtering :**

  Hybrid ports allow for changing ingress filtering. Access and Trunk ports always have ingress filtering enabled.
  If ingress filtering is enabled (checkbox is checked), frames classified to a VLAN that the port is not a member of get discarded.
  If ingress filtering is disabled, frames classified to a VLAN that the port is not a member of are accepted and forwarded to the switch engine. However, the port will never transmit frames classified to VLANs that it is not a member of.

- **Ingress Acceptance :**

  Hybrid ports allow for changing the type of frames that are accepted on ingress.

  Tagged and untagged
  both tagged and untagged frames are accepted.

  Tagged Only
  Only tagged frames are accepted on ingress. Untagged frames are discarded.

Untagged Only
Only untagged frames are accepted on ingress. Tagged frames are discarded.

- **Egress Tagging :**

  Ports in Trunk and Hybrid mode may control the tagging of frames on egress.

  Untag Port VLAN
  Frames classified to the Port VLAN are transmitted untagged. Other frames are transmitted with the relevant tag.

  Tag All
  All frames, whether classified to the Port VLAN or not, are transmitted with a tag.

  Untag All
  All frames, whether classified to the Port VLAN or not, are transmitted without a tag. This option is only available for ports in Hybrid mode.

- **Allowed VLANs :**

  Ports in Trunk and Hybrid mode may control which VLANs they are allowed to become members of. Access ports can only be member of one VLAN, the Access VLAN. The field's syntax is identical to the syntax used in the Existing VLANs field. By default, a port may become member of all possible VLANs, and is therefore set to 1-4095. The field may be left empty, which means that the port will not be member of any of the existing VLANs, but if it is configured for VLAN Trunking it will still be able to carry all unknown VLANs.

- **Forbidden VLANs :**

  A port may be configured to never be member of one or more VLANs. This is particularly useful when dynamic VLAN protocols like MVRP and GVRP must be prevented from dynamically adding ports to VLANs.
  The trick is to mark such VLANs as forbidden on the port in question. The syntax is identical to the syntax used in the Enabled VLANs field.
  By default, the field is left blank, which means that the port may become a member of all possible VLANs.

Buttons

- **Apply :**

  Click to save changes.

- **Reset :**

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

5-2 VLAN Membership

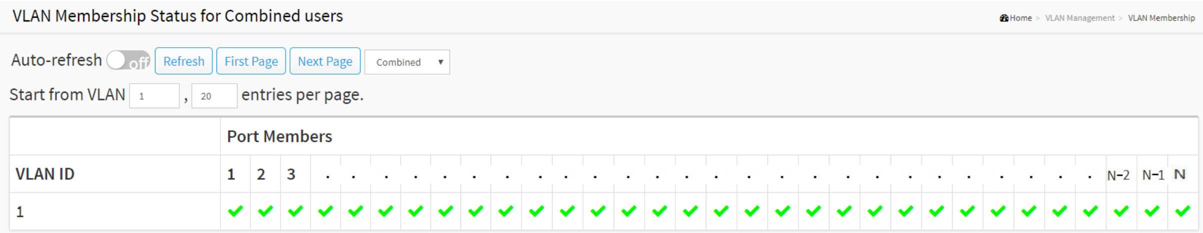
This page provides an overview of membership status of VLAN users.

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

Web Interface

To configure VLAN membership configuration in the web interface:

1. Click VLAN Management and VLAN membership.
2. Scroll the bar to choice which VLANs would like to show up.
3. Click Refresh to update the state.



VLAN Membership Status for Combined users

Combined ▾

Start from VLAN 1 , 20 entries per page.

	Port Members																															
VLAN ID	1	2	3	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	N-2	N-1	N
1	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓

Figure 5-2: The VLAN Membership

Parameter description:

- **VLAN USER :**

  Various internal software modules may use VLAN services to configure VLAN memberships on the fly. The drop-down list on the right allows for selecting between showing VLAN memberships as configured by an administrator (Admin) or as configured by one of these internal software modules. The "Combined" entry will show a combination of the administrator and internal software modules configuration, and basically reflects what is actually configured in hardware.

  VLAN User module uses services of the VLAN management functionality to configure VLAN memberships and VLAN port configurations such as PVID and UVID. Currently we support the following VLAN user types:

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

  GVRP : Adjacent VLAN-aware devices can exchange VLAN information with each other by using Generic VLAN Registration Protocol (GVRP). GVRP is based on the Generic Attribute Registration Protocol (GARP) and propagates VLAN information throughout a bridged network.

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

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

  MSTP : The 802.1s Multiple Spanning Tree protocol (MSTP) uses VLANs to create multiple spanning trees in a network, which significantly improves network resource utilization while maintaining a loop-free environment.

  DMS: Shows DMS VLAN membership status.

VCL : Shows MAC-based VLAN entries configured by various MAC-based VLAN users.

- **VLAN ID :**

  VLAN ID for which the Port members are displayed.

- **Port Members :**

  A row of check boxes for each port is displayed for each VLAN ID. If a port is included in a VLAN, an image U and T will be displayed. Shows egress filtering frame status whether tagged or untagged. Frames classified to the Port VLAN are transmitted tagged(T) or untagged(U).

- **VLAN Membership :**

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

- **Show entries :**

  You can choose how many items you want to show up.

- Admin ▾ **:**

  You can choose the Vlan User.

Buttons

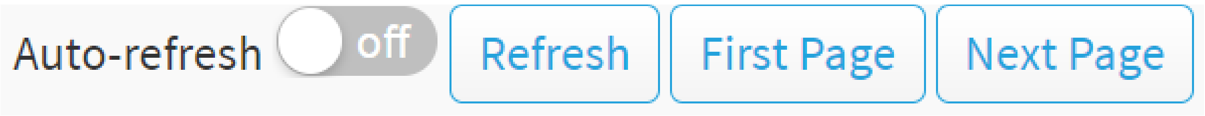


Figure 5-2: The VLAN Membership buttons

- **Auto-refresh :**

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

- **Refresh :**

  Click to refresh the page.

- **First Page :**

  Updates the system log entries, turn to the first page.

- **Next Page :**

  Updates the system log entries, turn to the next page.

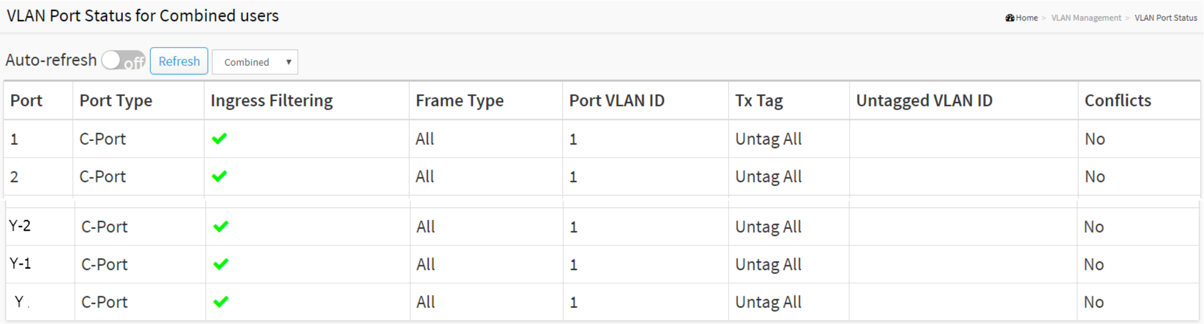
5-3 VLAN Port Status

The function Port Status gathers the information of all VLAN status and reports it by the order of Combined, Admin, NAS, GVRP, MVR, Voice VLAN, MSTP, DMS, VCL.

Web Interface

To Display VLAN Port Status in the web interface:

1. Click VLAN Management and VLAN Port Status.
2. Specify the Combined, Admin, NAS, GVRP, MVR, Voice VLAN, MSTP, DMS, VCL, RMirror.
3. Display Port Status information.



VLAN Port Status for Combined users

Port	Port Type	Ingress Filtering	Frame Type	Port VLAN ID	Tx Tag	Untagged VLAN ID	Conflicts
1	C-Port	✓	All	1	Untag All		No
2	C-Port	✓	All	1	Untag All		No
Y-2	C-Port	✓	All	1	Untag All		No
Y-1	C-Port	✓	All	1	Untag All		No
Y	C-Port	✓	All	1	Untag All		No

Figure 5-3: The VLAN Port Status

Parameter description:

- **VLAN USER :**

  VLAN User module uses services of the VLAN management functionality to configure VLAN memberships and VLAN port configuration such as PVID, UVID. Currently we support following VLAN User types:

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

  GVRP : Adjacent VLAN-aware devices can exchange VLAN information with each other by using Generic VLAN Registration Protocol (GVRP). GVRP is based on the Generic Attribute Registration Protocol (GARP) and propagates VLAN information throughout a bridged network.

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

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

  MSTP : The 802.1s Multiple Spanning Tree protocol (MSTP) uses VLANs to create multiple spanning trees in a network, which significantly improves network resource utilization while maintaining a loop-free environment.

  DMS: Shows DMS VLAN membership status.

  VCL : shows MAC-based VLAN entries configured by various MAC-based VLAN users.

- **Port :**

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

- **Port Type :**

Shows the Port Type. Port type can be any of Unaware, C-port, S-port, Custom S-port.

If Port Type is Unaware, all frames are classified to the Port VLAN ID and tags are not removed. C-port is Customer Port. S-port is Service port. Custom S-port is S-port with Custom TPID.

- **Ingress Filtering :**

  Shows the ingress filtering on a port. This parameter affects VLAN ingress processing. If ingress filtering is enabled and the ingress port is not a member of the classified VLAN, the frame is discarded.

- **Frame Type :**

  Shows whether the port accepts all frames or only tagged frames. This parameter affects VLAN ingress processing. If the port only accepts tagged frames, untagged frames received on that port are discarded.

- **Port VLAN ID :**

  Shows the Port VLAN ID (PVID) that a given user wants the port to have.

  The field is empty if not overridden by the selected user.

- **Tx Tag :**

  Shows egress filtering frame status whether tagged or untagged.

- **Untagged VLAN ID :**

  If Tx Tag is overridden by the selected user and is set to Tag or Untag UVID, then this field will show the VLAN ID the user wants to tag or untag on egress. The field is empty if not overridden by the selected user.

- **Conflicts :**

  Two users may have conflicting requirements to a port's configuration. For instance, one user may require all frames to be tagged on egress while another requires all frames to be untagged on egress. Since both users cannot win, this gives rise to a conflict, which is solved in a prioritized way. The Administrator has the least priority. Other software modules are prioritized according to their position in the drop-down list: The higher in the list, the higher priority. If conflicts exist, it will be displayed as "Yes" for the "Combined" user and the offending software module. The "Combined" user reflects what is actually configured in hardware.

- Admin ▾ **:**

  You can choose the Vlan User.

Buttons

Figure 5-3: The VLAN Port Status buttons

- **Auto-refresh :**

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

- **Refresh :**

  Click to refresh the page.

5-4 MAC-based VLAN

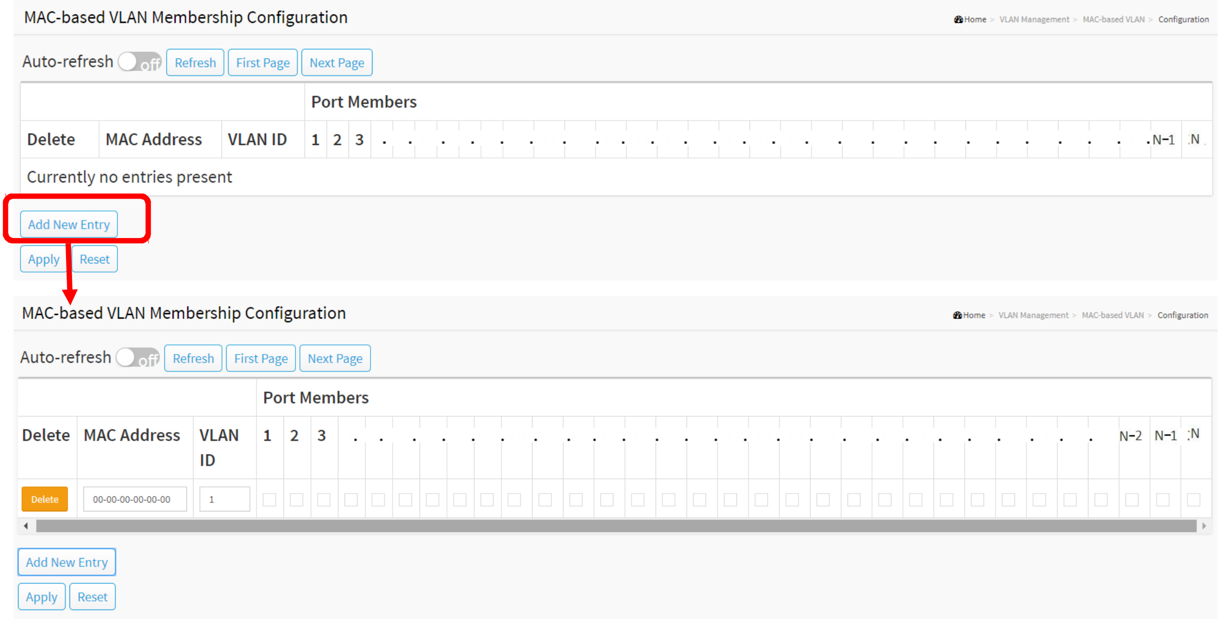
5-4.1 Configuration

The MAC address to VLAN ID mappings can be configured here. This page allows adding and deleting MAC-based VLAN Classification List entries and assigning the entries to different ports.

Web Interface

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

1. Click VLAN Management, MAC-based VLAN and Configuration.
2. Click "Add New Entry".
3. Specify the MAC address and VLAN ID.
4. Click Apply.



MAC-based VLAN Membership Configuration

Home > VLAN Management > MAC-based VLAN > Configuration

Auto-refresh off

			Port Members				
Delete	MAC Address	VLAN ID	1	2	3	. . . N-1	N
Currently no entries present							

MAC-based VLAN Membership Configuration

Home > VLAN Management > MAC-based VLAN > Configuration

Auto-refresh off

			Port Members					
Delete	MAC Address	VLAN ID	1	2	3	. . . N-2	N-1	N
Delete	00-00-00-00-00-00	1	□	□	□	□	□	□

Figure 5-4.1: The MAC-based VLAN Configuration

Parameter description:

- **MAC Address :**

  Indicates the MAC address.

- **VLAN ID :**

  Indicates the VLAN ID.

- **Port Members :**

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

  Buttons

- **Adding New Entry :**

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

- **Delete :**

  To delete a MAC-based VLAN entry, check this box and press apply. The entry will be deleted on the selected switch in the stack.

- **Apply :**

  Click to save changes.

- **Reset :**

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

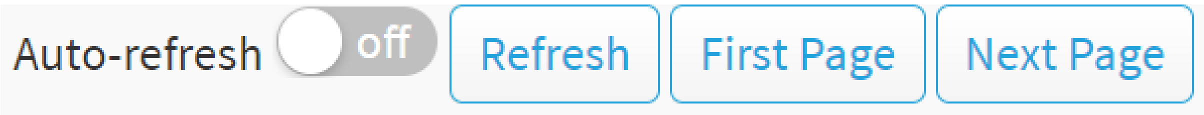


Figure 5-4-1: The MAC-based VLAN Configuration buttons

- **Auto-refresh :**

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

- **Refresh :**

  Click to refresh the page.

- **First Page :**

  Updates the system log entries, turn to the first page.

- **Next Page :**

  Updates the system log entries, turn to the next page.

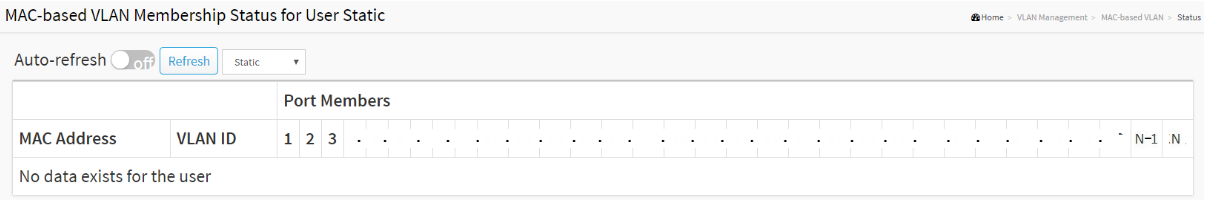
5-4.2 Status

Show the MAC-based VLAN status.

Web Interface

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

1. Click VLAN Management, MAC-based VLAN and Status.
2. If you want to auto-refresh the information then you need to evoke the “Auto-refresh”.
3. Click “Refresh” to refresh the MAC-based VLAN Membership Status.



MAC-based VLAN Membership Status for User Static

Auto-refresh off

		Port Members					
MAC Address	VLAN ID	1	2	3	. . . .	N−1	N
No data exists for the user							

Figure 5-4.2: The MAC-based VLAN Status

Parameter description:

- **MAC Address :**

  Indicates the MAC address.

- **VLAN ID :**

  Indicates the VLAN ID.

- **Port Members :**

  Port members of the MAC-based VLAN entry.

Buttons

Figure 5-4.2: The MAC-based VLAN Status buttons

- **Auto-refresh :**

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

- **Refresh :**

  Click to refresh the page immediately.

5-5 Protocol-based VLAN

This section describe Protocol -based VLAN, The Switch support Protocol include Ethernet LLC SNAP Protocol,

LLC

The Logical Link Control (LLC) data communication protocol layer is the upper sub-layer of the Data Link Layer (which is itself layer 2, just above the Physical Layer) in the seven-layer OSI reference model. It provides multiplexing mechanisms that make it possible for several network protocols (IP, IPX, Decent and Appletalk) to coexist within a multipoint network and to be transported over the same network media, and can also provide flow control and automatic repeat request (ARQ) error management mechanisms.

SNAP

The Subnetwork Access Protocol (SNAP) is a mechanism for multiplexing, on networks using IEEE 802.2 LLC, more protocols than can be distinguished by the 8-bit 802.2 Service Access Point (SAP) fields. SNAP supports identifying protocols by Ethernet type field values; it also supports vendor-private protocol identifier spaces. It is used with IEEE 802.3, IEEE 802.4, IEEE 802.5, IEEE 802.11 and other IEEE 802 physical network layers, as well as with non-IEEE 802 physical network layers such as FDDI that use 802.2 LLC.

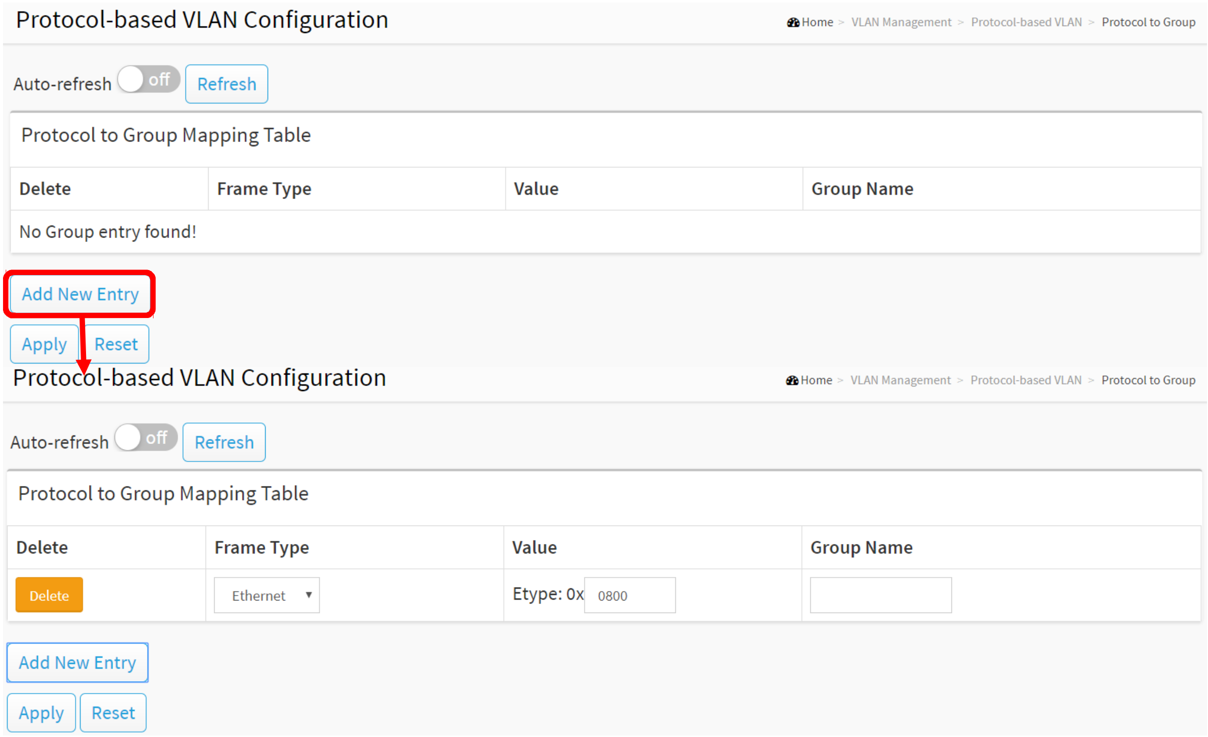
5-5.1 Protocol to Group

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

Web Interface

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

1. Click VLAN Management, Protocol-based VLAN and Protocol to Group.
2. Click “Add New Entry”.
3. Specify the Frame Type, Value and Group Name.
4. Click Apply.



Protocol-based VLAN Configuration

Home > VLAN Management > Protocol-based VLAN > Protocol to Group

Auto-refresh off Refresh

Protocol to Group Mapping Table

Delete	Frame Type	Value	Group Name
No Group entry found!			

Add New Entry

Apply Reset

Protocol-based VLAN Configuration

Home > VLAN Management > Protocol-based VLAN > Protocol to Group

Auto-refresh off Refresh

Protocol to Group Mapping Table

Delete	Frame Type	Value	Group Name
Delete	Ethernet ▾	Etype: 0x 0800	

Add New Entry

Apply Reset

Figure 5-5.1: The Protocol to Group Mapping Table

Parameter description:

- **Frame Type :**

  Frame Type can have one of the following values:

  1. **Ethernet**
  2. **LLC**
  3. **SNAP**

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

- **Value :**

  Valid value that can be entered in this text field depends on the option selected from the the preceding Frame Type selection menu.

  Below is the criteria for three different Frame Types:

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

  2. **For LLC:** Valid value in this case is comprised of two different sub-values.
     a. DSAP: 1-byte long string (0x00-0xff)
     b. SSAP: 1-byte long string (0x00-0xff)

  3. **For SNAP:** Valid value in this case also is comprised of two different sub-values.
     a.OUI: OUI (Organizationally Unique Identifier) is value in format of xx-xx-xx where each pair (xx) in string is a hexadecimal value ranges from 0x00-0xff.
     b. PID: If the OUI is hexadecimal 000000, the protocol ID is the Ethernet type (EtherType) field value for the protocol running on top of SNAP; if the OUI is an OUI for a particular organization, the protocol ID is a value assigned by that organization

to the protocol running on top of SNAP.

- **Group Name :**

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

Buttons

- **Delete :**

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

- **Add New Entry :**

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

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

- **Apply :**

  Click to save changes.

- **Reset :**

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

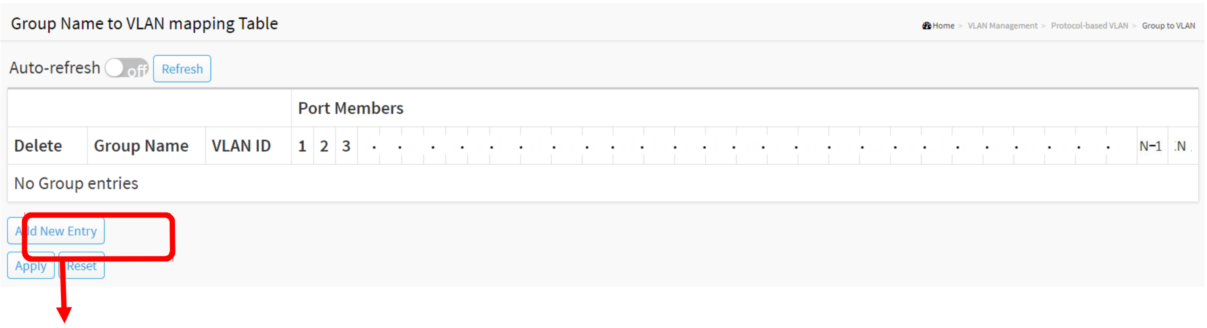
5-5.2 Group to VLAN

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

Web Interface

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

1. Click VLAN Management, Protocol-based VLAN and Group to VLAN.
2. Click “Add New Entry”.
3. Specify the Group Name and VLAN ID.
4. Click Apply.

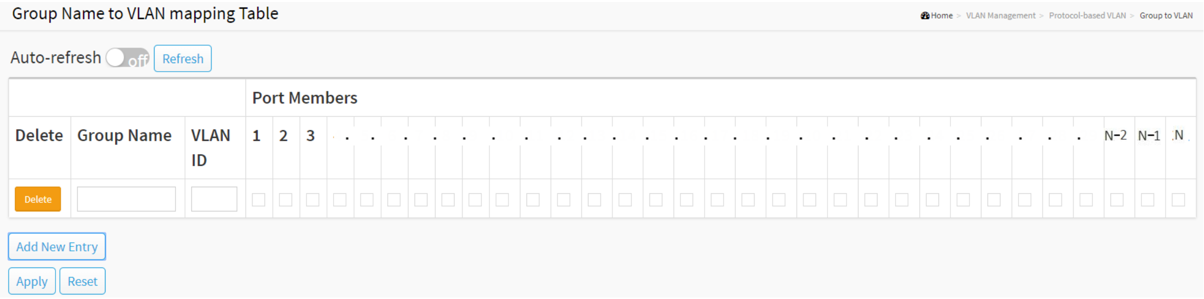


Group Name to VLAN mapping Table

Home > VLAN Management > Protocol-based VLAN > Group to VLAN
Auto-refresh
off
Refresh

			Port Members					
Delete	Group Name	VLAN ID	1	2	3	· · ·	N-1	N
No Group entries								

Add New Entry
Apply
Reset



Group Name to VLAN mapping Table

Home > VLAN Management > Protocol-based VLAN > Group to VLAN
Auto-refresh off
Refresh

			Port Members						
Delete	Group Name	VLAN ID	1	2	3	. . . .	N-2	N-1	N
Delete			□	□	□	□ □	□	□	□

Add New Entry
Apply
Reset

Figure 5-5.2: The Group Name of VLAN Mapping Table

Parameter description:

- **Group Name :**

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

- **VLAN ID :**

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

- **Port Members :**

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

Buttons

- **Delete :**

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

- **Add New Entry :**

  Click to add a new entry in mapping table. An empty row is added to the table, the Group Name, VLAN ID and port members can be configured as needed. Legal values for a VLAN ID are 1 through 4095. The button can be used to undo the addition of new entry.

- **Apply :**

  Click to save changes.

- **Reset :**

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

Figure 5-5.2: The Group to VLAN buttons

- **Auto-refresh :**

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

- **Refresh :**

  Click to refresh the page immediately.

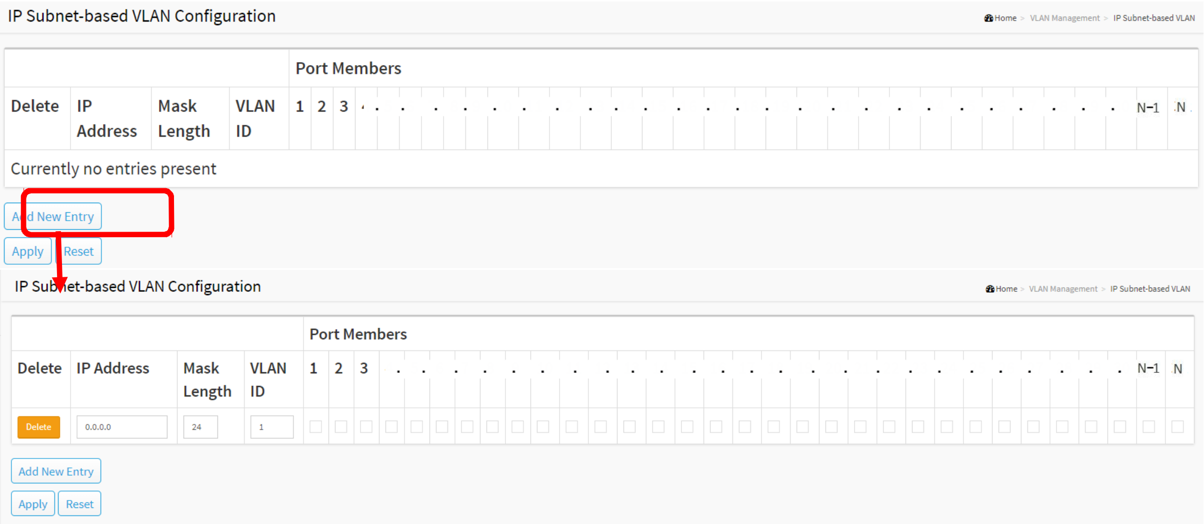
5-6 IP Subnet-based VLAN

The IP subnet-based VLAN entries can be configured here. This page allows for adding, updating and deleting IP subnet-based VLAN entries.

Web Interface

To configure IP subnet-based VLAN Membership to configured in the web interface:

1. Click VLAN Management and IP Subnet-based VLAN.
2. Click "Add New Entry".
3. Specify IP Address, Mask Length, VLAN ID.
4. Click Apply.



IP Subnet-based VLAN Configuration

Home > VLAN Management > IP Subnet-based VLAN

				Port Members					
Delete	IP Address	Mask Length	VLAN ID	1	2	3	. . .	N-1	N
Currently no entries present									

Add New Entry
Apply
Reset

IP Subnet-based VLAN Configuration

Home > VLAN Management > IP Subnet-based VLAN

				Port Members					
Delete	IP Address	Mask Length	VLAN ID	1	2	3	. . .	N-1	N
Delete	0.0.0.0	24	1	□	□	□	□	□	□

Add New Entry
Apply
Reset

Figure 5-6: IP Subnet-based VLAN Membership Configuration

Parameter description:

- **IP Address :**

  Indicates the IP address.

- **Mask Length :**

  Indicates the network mask length.

- **VLAN ID :**

  Indicates the VLAN ID. VLAN ID can be changed for the existing entries.

- **Port Members :**

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

Buttons

- **Delete :**

  To delete a IP subnet-based VLAN entry, check this box and press save. The entry will be deleted on the selected switch in the stack.

- **Add New Entry :**

  Click “Add New Entry” to add a new IP subnet-based VLAN entry. An empty row is added to the table, and the IP subnet-based VLAN entry can be configured as needed. Any IP address/mask can be configured for the IP subnet-based VLAN entry. Legal values for a VLAN ID are 1 through 4095.

  The IP subnet-based VLAN entry is enabled on the selected stack switch unit when you click on "Save". The “Delete” button can be used to undo the addition of new IP subnet-based VLANs. The maximum possible IP subnet-based VLAN entries are limited to 128.

- **Apply :**

  Click to save changes.

- **Reset :**

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

5-7 GVRP

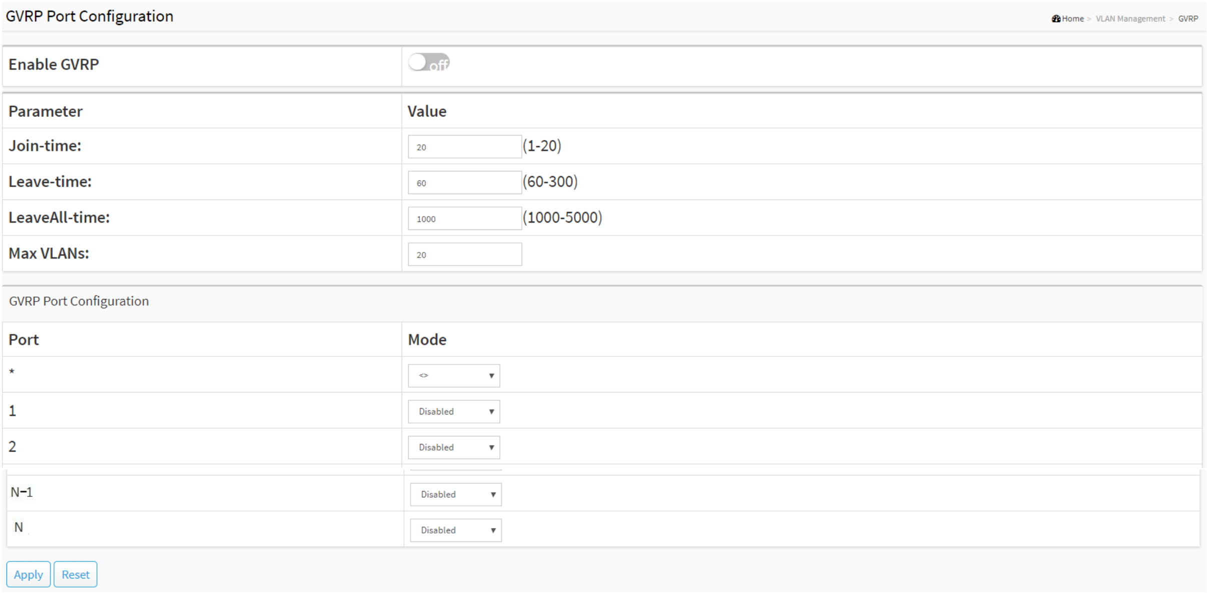
The Generic Attribute Registration Protocol (GARP) provides a generic framework whereby devices in a bridged LAN, e.g. end stations and switches, can register and de-register attribute values, such as VLAN Identifiers, with each other. In doing so, the attributes are propagated to devices in the bridged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

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

Web Interface

To configure the GVRP in the web interface:

1. Click VLAN Management and GVRP.
2. Evoke to enable or disable the GVRP.
3. Specify Join-time, Leave-time, Leave All-time, Max VLANs.
4. Evoke to enable or disable the Mode.
5. Click apply to save the setting.
6. If you want to cancel the setting then you need to click the Reset button. It will revert to previously saved values.



GVRP Port Configuration

Enable GVRP	off

Parameter	Value
Join-time:	20 (1-20)
Leave-time:	60 (60-300)
LeaveAll-time:	1000 (1000-5000)
Max VLANs:	20

GVRP Port Configuration

Port	Mode
*	<>
1	Disabled
2	Disabled
N-1	Disabled
N	Disabled

Figure 5-7: The GVRP Configuration

Parameter description:

- **Enable GVRP globally :**

The GVRP feature is enabled by setting the check mark in the checkbox named Enable GVRP.

- **GVRP protocol timers :**

  Join-time is a value in the range 1-20 in the units of centi seconds, i.e. in units of one hundredth of a second. The default is 20.

  Leave-time is a value in the range 60-300 in the units of centi seconds, i.e. in units of one hundredth of a second. The default is 60.

  Leave All-time is a value in the range 1000-5000 in the units of centi seconds, i.e. in units of one hundredth of a second. The default is 1000.

- **Max VLANs :**

  When GVRP is enabled a maximum number of VLANs supported by GVRP is specified. By default this number is 20. This number can only be changed when GVRP is turned off.

- **Port :**

  The Port column shows the list of ports.

- **Mode :**

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

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

Buttons

- **Apply :**

  Click to save changes.

- **Reset :**

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

5-8 Private VLAN

The Private VLAN membership configurations for the switch can be monitored and modified here. Private VLANs can be added or deleted here. Port members of each Private VLAN can be added or removed here.

Private VLANs are based on the source port mask, and there are no connections to VLANs. This means that VLAN IDs and Private VLAN IDs can be identical.

A port must be a member of both a VLAN and a Private VLAN to be able to forward packets. By default, all ports are VLAN unaware and members of VLAN 1 and Private VLAN 1.

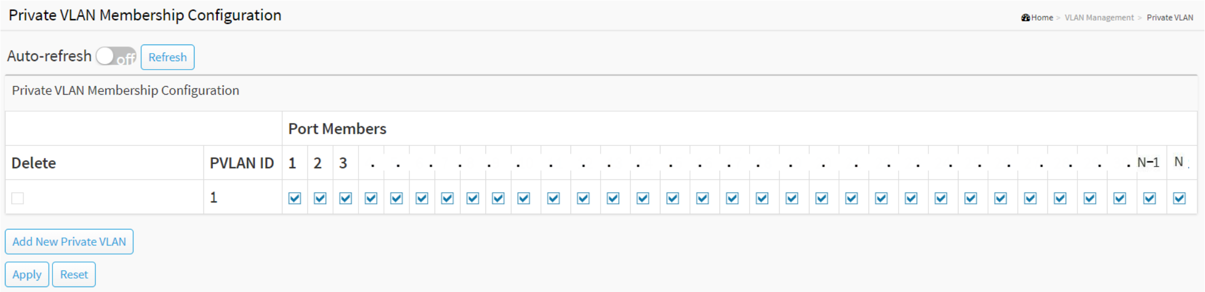
A VLAN unaware port can only be a member of one VLAN, but it can be a member of multiple Private VLANs.

VLAN Priority : Voice VLAN > MAC based VLAN > Protocol based VLAN > Tag based VLAN

Web Interface

To configure Port Isolation configuration in the web interface:

1. Click VLAN Management and Private VLAN.
2. Configure the Private VLAN membership configurations for the switch.
3. Click Apply.



Private VLAN Membership Configuration

Private VLAN Membership Configuration

		Port Members																															
Delete	PVLAN ID	1	2	3	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	N-1	N
□	1	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑

Figure 5-8: The Private VLAN Configuration

Parameter description:

- **Delete :**

  To delete a private VLAN entry, check this box. The entry will be deleted during the next apply.

- **Private VLAN ID :**

  Indicates the ID of this particular private VLAN.

- **Port Members :**

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

- **Add New Private VLAN :**

  Click to add a new private VLAN ID. An empty row is added to the table, and the private VLAN can be configured as needed. The allowed range for a private VLAN ID is the same as the switch port number range. Any values outside this range are not accepted, and a warning message appears. Click "OK" to discard the incorrect entry, or click "Cancel" to return to the editing and make a correction.

The Private VLAN is enabled when you click "Apply".

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

Buttons

- **Apply :**

  Click to save changes.

- **Reset :**

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

5-9 Port Isolation

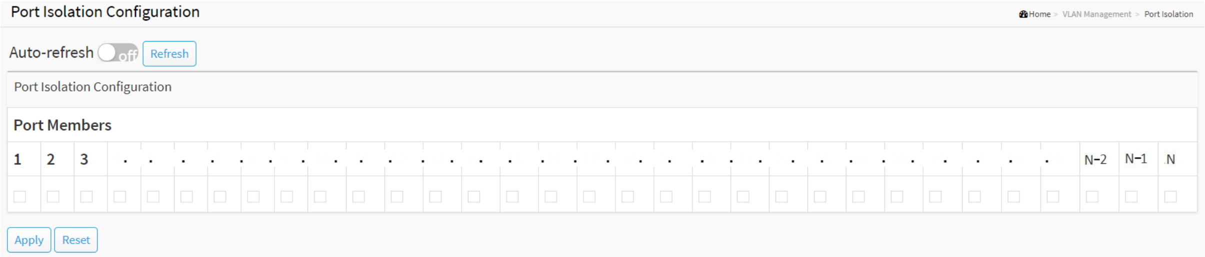
Port Isolation provides for an apparatus and method to isolate ports on layer 2 switches on the same VLAN to restrict traffic flow. The apparatus comprises a switch having said plurality of ports, each port configured as a protected port or a non-protected port. An address table memory stores an address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

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

Web Interface

To configure Port Isolation configuration in the web interface:

1. Click VLAN Management and Port Isolation.
2. Evoke which port want to enable Port Isolation
3. Click Apply.



Port Isolation Configuration

Port Isolation Configuration

Port Members

1 2 3 . . . . N-2 N-1 N

□ □

Figure 5-9: The Port Isolation Configuration

Parameter description:

- **Port Numbers :**

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

Buttons

- **Apply :**

  Click to save changes.

- **Reset :**

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

5-10 Voice VLAN

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

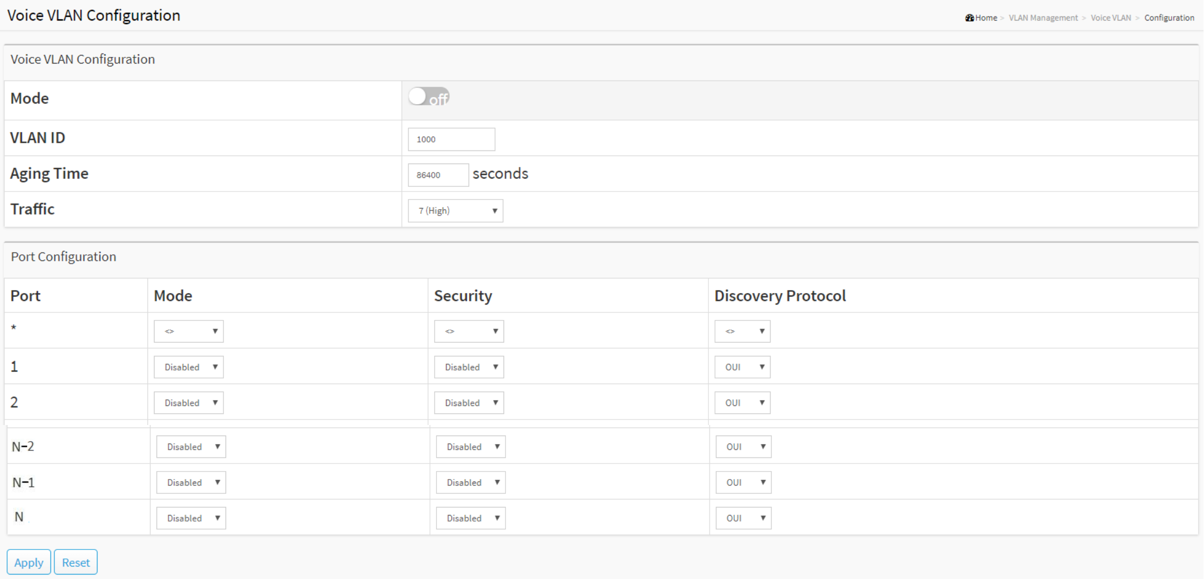
5-10.1 Configuration

The Voice VLAN feature enables voice traffic forwarding on the Voice VLAN, then the switch can classify and schedule network traffic. It is recommended that there be two VLANs on a port - one for voice, one for data. Before connecting the IP device to the switch, the IP phone should configure the voice VLAN ID correctly. It should be configured through its own GUI.

Web Interface

To configure Voice VLAN in the web interface:

1. Click VLAN Management, Voice VLAN and Configuration.
2. Select "on" in the Voice VLAN Configuration.
3. Specify VLAN ID, Aging Time and Traffic Class.
4. Select Port Members in the Voice VLAN Configuration.
5. Specify (Mode, Security, Discovery Protocol) in the Port Configuration.
6. Click the Apply to save the setting.
7. If you want to cancel the setting then you need to click the Reset button. It will revert to previously saved values.



Voice VLAN Configuration

Home > VLAN Management > Voice VLAN > Configuration

Voice VLAN Configuration

Mode	off
VLAN ID	1000
Aging Time	86400 seconds
Traffic	7 (High)

Port Configuration

Port	Mode	Security	Discovery Protocol
*	<>	<>	<>
1	Disabled	Disabled	OUI
2	Disabled	Disabled	OUI
N-2	Disabled	Disabled	OUI
N-1	Disabled	Disabled	OUI
N	Disabled	Disabled	OUI

Figure 5-10.1: The Voice VLAN Configuration

Parameter description:

- **Mode :**

  Indicates the Voice VLAN mode operation. We must disable MSTP feature before we enable Voice VLAN. It can avoid the conflict of ingress filtering. Possible modes are:

  on: Enable Voice VLAN mode operation.

  off: Disable Voice VLAN mode operation.

- **VLAN ID :**

  Indicates the Voice VLAN ID. It should be a unique VLAN ID in the system and cannot equal each port PVID. It is a conflict in configuration if the value equals management VID, MVR VID, PVID etc. The allowed range is 1 to 4095.

- **Aging Time :**

  Indicates the Voice VLAN secure learning aging time. The allowed range is 10 to 10000000 seconds. It is used when security mode or auto detect mode is enabled. In other cases, it will be based on hardware aging time. The actual aging time will be situated between the [age_time; 2 * age_time] interval.

- **Traffic :**

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

- **Port :**

  The switch port number of the Voice VLAN port.

- **Port Mode :**

  Indicates the Voice VLAN port mode. Possible port modes are:

  Disabled: Disjoin from Voice VLAN.

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

  Forced: Force join to Voice VLAN.

  This field will be read only if STP feature is enabled. And the STP port mode will be readonly if this field be set to the mode other than Disabled.

- **Port Security :**

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

  Enabled: Enable Voice VLAN security mode operation.

  Disabled: Disable Voice VLAN security mode operation.

- **Port Discovery Protocol**

  Indicates the Voice VLAN port discovery protocol. It will only work when auto detect mode is enabled. We should enable LLDP feature before configuring discovery protocol to "LLDP" or "Both". Changing the discovery protocol to "OUI" or "LLDP" will restart auto detect process. Possible discovery protocols are:

  OUI: Detect telephony device by OUI address.

  LLDP: Detect telephony device by LLDP.

  Both: Both OUI and LLDP.

Buttons

- **Apply :**

  Click to save changes.

- **Reset :**

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

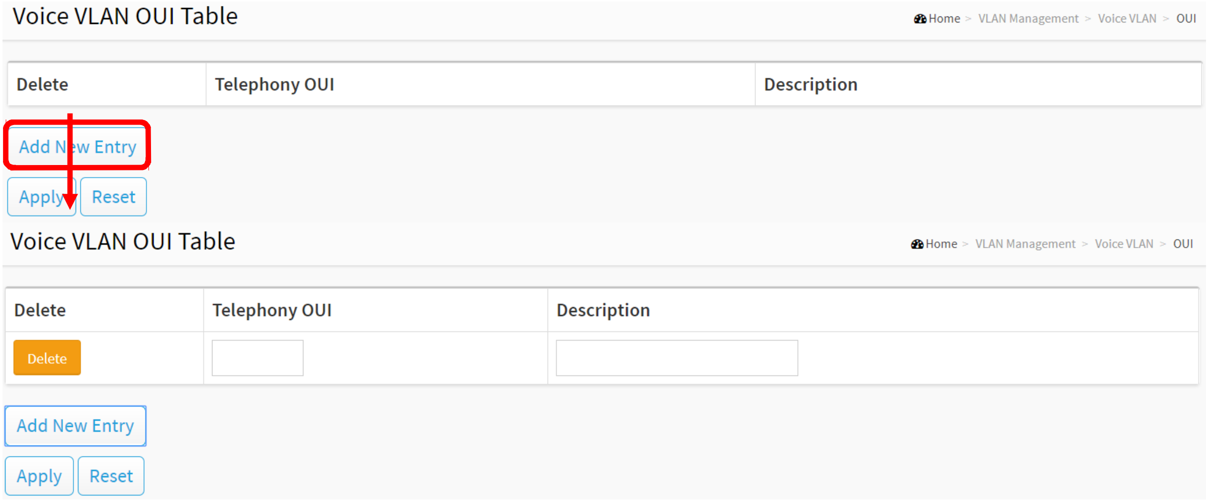
5-10.2 OUI

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

Web Interface

To configure Voice VLAN OUI Table in the web interface:

1. Click VLAN Management, Voice VLAN and OUI
2. Select "Add new entry", "delete" in the Voice VLAN OUI table.
3. Specify Telephony OUI, Description.
4. Click Apply.



Voice VLAN OUI Table

Home > VLAN Management > Voice VLAN > OUI

Delete	Telephony OUI	Description

Voice VLAN OUI Table

Home > VLAN Management > Voice VLAN > OUI

Delete	Telephony OUI	Description
Delete		

Figure 5-10.2: The Voice VLAN OUI Table

Parameter description:

- **Delete :**

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

- **Telephony OUI :**

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

- **Description :**

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

- **Add New entry :**

  Click to add a new entry in Voice VLAN OUI table. An empty row is added to the table, the Telephony OUI, Description.

Buttons

- **Apply :**

  Click to save changes.

- **Reset :**

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

Chapter 6 Quality of Service

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

High flexibility in the classification of incoming frames to a QoS class. The QoS classification looks for information up to Layer 4, including IPv4 and IPv6 DSCP, IPv4 TCP/UDP port numbers, and user priority of tagged frames. This QoS classification mechanism is implemented in a QoS control list (QCL). The QoS class assigned to a frame is used throughout the device for providing queuing, scheduling, and congestion control guarantees to the frame according to what was configured for that specific QoS class.

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

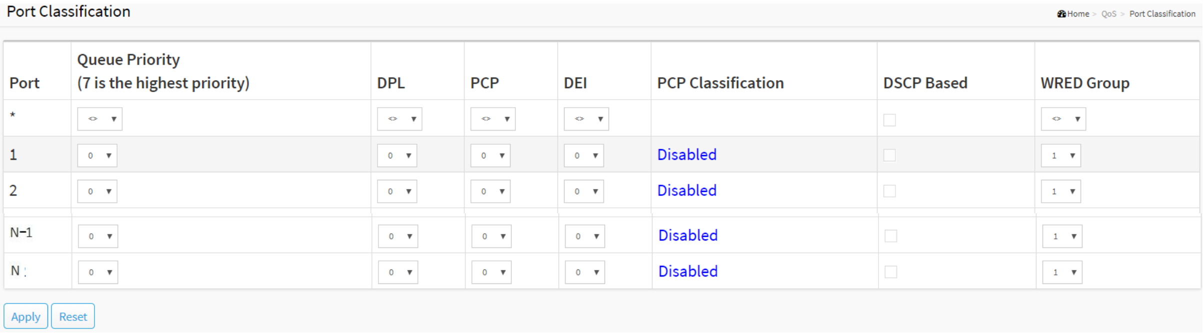
6-1 Port Classification

The section allows you to configure the basic QoS Ingress Classification settings for all switch ports.

Web Interface

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

1. Click Quality of Service and Port Classification.
2. Scroll to select QoS Ingress Port parameters.
3. Click the Apply to save the setting.
4. If you want to cancel the setting then you need to click the Reset button. It will revert to previously saved values.
5. Click “PCP Classification “to next page “Port PCP Classification”.



Port Classification

Port	Queue Priority (7 is the highest priority)	DPL	PCP	DEI	PCP Classification	DSCP Based	WRED Group
*	<> ▾	<> ▾	<> ▾	<> ▾		□	<> ▾
1	0 ▾	0 ▾	0 ▾	0 ▾	Disabled	□	1 ▾
2	0 ▾	0 ▾	0 ▾	0 ▾	Disabled	□	1 ▾
N-1	0 ▾	0 ▾	0 ▾	0 ▾	Disabled	□	1 ▾
N :	0 ▾	0 ▾	0 ▾	0 ▾	Disabled	□	1 ▾

Figure 6-1: The QoS Ingress Port Classification

Parameter description:

- **Port :**

  The port number for which the configuration below applies.

- **Queue Priority :**

  Controls the default CoS value.

  All frames are classified to a CoS. There is a one to one mapping between CoS, queue and priority. A CoS of 0 (zero) has the lowest priority.

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

  The classified CoS can be overruled by a QCL entry.

  Note: If the default CoS has been dynamically changed, then the actual default CoS is shown in parentheses after the configured default CoS.

- **DPL :**

  Controls the default drop precedence level.

  All frames are classified to a drop precedence level.

  If the port is VLAN aware, the frame is tagged and Tag Class. is enabled, then the frame is classified to a DPL that is mapped from the PCP and DEI value in the tag. Otherwise the frame is classified to the default DPL.

  The classified DPL can be overruled by a QCL entry.

- **PCP :**

  Controls the default PCP value.

  All frames are classified to a PCP value.

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

- **DEI :**

  Controls the default DEI value.

  All frames are classified to a DEI value.

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

- **DSCP Based :**

  Click to Enable DSCP Based QoS Ingress Port Classification.

- **WRED Group :**

  Controls the WRED group membership.

Buttons

- **Apply :**

  Click to save changes.

- **Reset :**

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

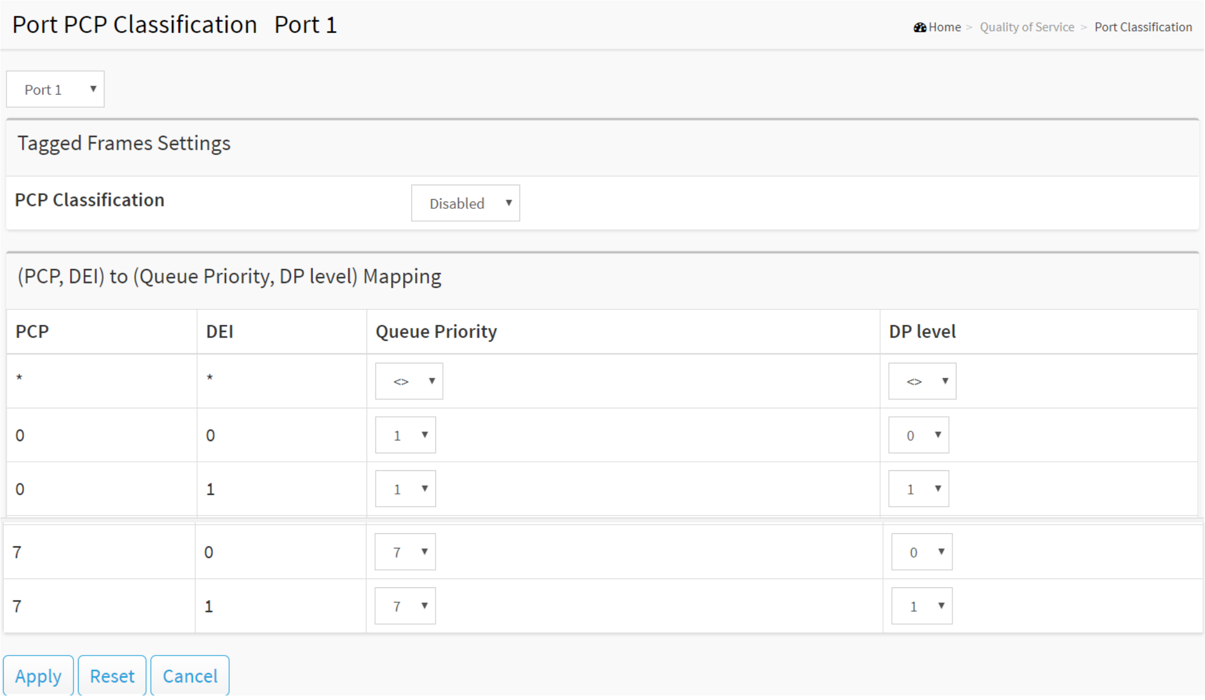
- **PCP Classification :**

  Shows the classification mode for tagged frames on this port. **Disabled:** Use default CoS and DPL for tagged frames.

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

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

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



Port PCP Classification Port 1

Tagged Frames Settings

PCP Classification	Disabled

(PCP, DEI) to (Queue Priority, DP level) Mapping

PCP	DEI	Queue Priority	DP level
*	*	<>	<>
0	0	1	0
0	1	1	1
7	0	7	0
7	1	7	1

Figure 6-1: The Port PCP Classification

Parameter description:

- **PCP Classification**

  Controls the classification mode for tagged frames on this port. **Disabled:** Use default CoS and DPL for tagged frames. **Enabled:** Use mapped versions of PCP and DEI for tagged frames.

- **(PCP, DEI) to (Queue Priority, DPL level) Mapping**

  Controls the mapping of the classified (PCP, DEI) to (Queue Priority, DPL level) values when Tag Classification is set to Enabled.

Buttons

- **Apply :**

  Click to save changes.

- **Reset :**

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

- **Cancel :**

  Click to undo any changes made locally and return to the previous page.

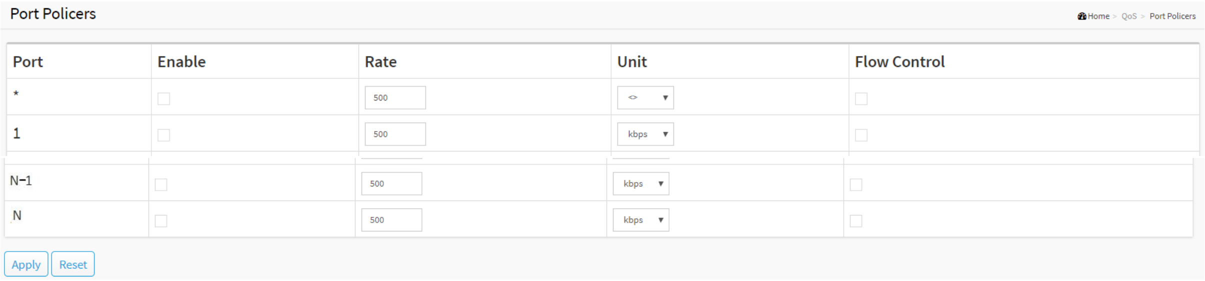
6-2 Port Policers

This section provides an overview of QoS Ingress Port Policers for all switch ports The Port Policing is useful in constraining traffic flows and marking frames above specific rates. Policing is primarily useful for data flows and voice or video flows because voice and video usually maintains a steady rate of traffic

Web Interface

To configure the QoS Port Policers in the web interface:

1. Click Quality of Service and Port Policers.
2. Click which port need to enable the QoS Ingress Port Policers, and configue the Rate limit condition.
3. Scroll to select the column Rate and Unit.
4. Click Apply to save the configuration.
5. If you want to cancel the setting then you need to click the Reset button. It will revert to previously saved values.



Port Policers

Port	Enable	Rate	Unit	Flow Control
*	□	500	<> ▾	□
1	□	500	kbps ▾	□
N−1	□	500	kbps ▾	□
N	□	500	kbps ▾	□

Figure 6-2: The QoS Ingress Port Policers Configuration

Parameter description:

- **Port :**

  The logical port for the settings contained in the same row. Click on the port number in order to configure the schedulers.

- **Enabled :**

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

- **Rate :**

  To set the Rate limit value for this port, the default is 1000000.

- **Unit :**

  Controls the unit of measure for the port policer rate as kbps, Mbps, fps or kfps.

- **Flow Control :**

  If flow control is enabled and the port is in flow control mode, then pause frames are sent instead of discarding frames.

Buttons

- **Apply :**

  Click to save changes.

- **Reset :**

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

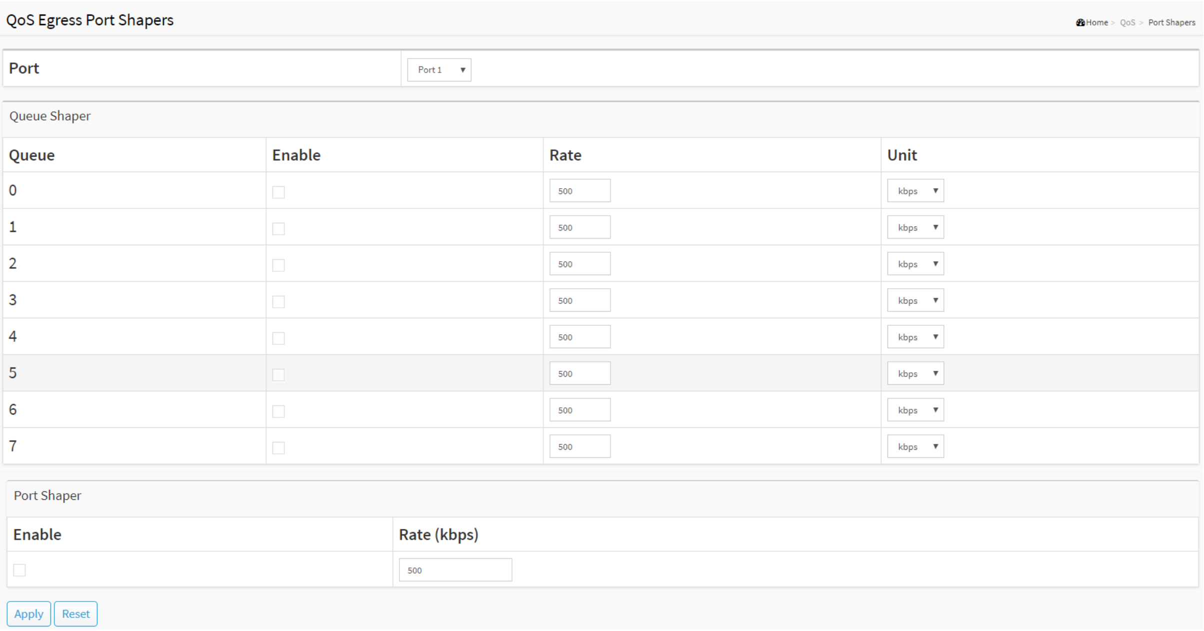
6-3 Port Shapers

This section provides an overview of QoS Egress Port Shapers for all switch ports. Others the user could get all detail information of the ports belong to the currently selected stack unit, as reflected by the page header.

Web Interface

To configure the QoS Port Shapers in the web interface:

1. Click Quality of Service and Port Shapers.
2. Click the Port and display the Qos Egress Port Shapers.
3. Scroll the Port and Scheduler Mode and specify the Queue Shaper parameter.
4. Click the Apply to save the setting.
5. If you want to cancel the setting then you need to click the Reset button. It will revert to previously saved values.



QoS Egress Port Shapers

Home > QoS > Port Shapers

Port	Port 1 ▾

Queue Shaper

Queue	Enable	Rate	Unit
0	□	500	kbps ▾
1	□	500	kbps ▾
2	□	500	kbps ▾
3	□	500	kbps ▾
4	□	500	kbps ▾
5	□	500	kbps ▾
6	□	500	kbps ▾
7	□	500	kbps ▾

Port Shaper

Enable	Rate (kbps)
□	500

Figure 6-3: The QoS Egress Port Shaper

Parameter description:

- **Port :**

  The logical port for the settings contained in the same row. Click on the port number in order to configure the shapers.

- **Shapers – Qn :**

  Shows disabled or actual queue shaper rate - e.g. "800 Mbps".

- **Shapers – Port :**

  Shows disabled or actual port shaper rate - e.g. "800 Mbps".

- **Scheduler Mode :**

  Controls how many of the queues are scheduled as strict and how many are scheduled as weighted on this switch port.

- **Queue Shaper Enable :**

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

- **Queue Shaper Rate :**

  Controls the rate for the queue shaper. This value is restricted to 100-13107100 when "Unit" is kbps, and 1-13107 when "Unit" is Mbps.The rate is internally rounded up to the nearest value supported by the queue shaper.

- **Queue Shaper Unit :**

  Controls the unit of measure for the queue shaper rate as kbps or Mbps.

- **Queue Shaper Rate-type :**

  The rate type of the queue shaper. The allowed values are:
  Line: Specify that this shaper operates on line rate.
  Data: Specify that this shaper operates on data rate.

- **Queue Scheduler Weight :**

  Controls the weight for this queue. This value is restricted to 1-100. This parameter is only shown if "Scheduler Mode" is set to "Weighted".

- **Queue Scheduler Percent :**

  Shows the weight in percent for this queue. This parameter is only shown if "Scheduler Mode" is set to "Weighted".

- **Port Shaper Enable :**

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

- **Port Shaper Rate :**

  Controls the rate for the port shaper. This value is restricted to 100-13107100 when "Unit" is kbps, and 1-13107 when "Unit" is Mbps.The rate is internally rounded up to the nearest value supported by the port shaper.

- **Port Shaper Unit :**

  Controls the unit of measure for the port shaper rate as kbps or Mbps.

- **Port Shaper Rate-type :**

  The rate type of the port shaper. The allowed values are:
  Line: Specify that this shaper operates on line rate.
  Data: Specify that this shaper operates on data rate.

Buttons

- **Apply :**

  Click to save changes.

- **Reset :**

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

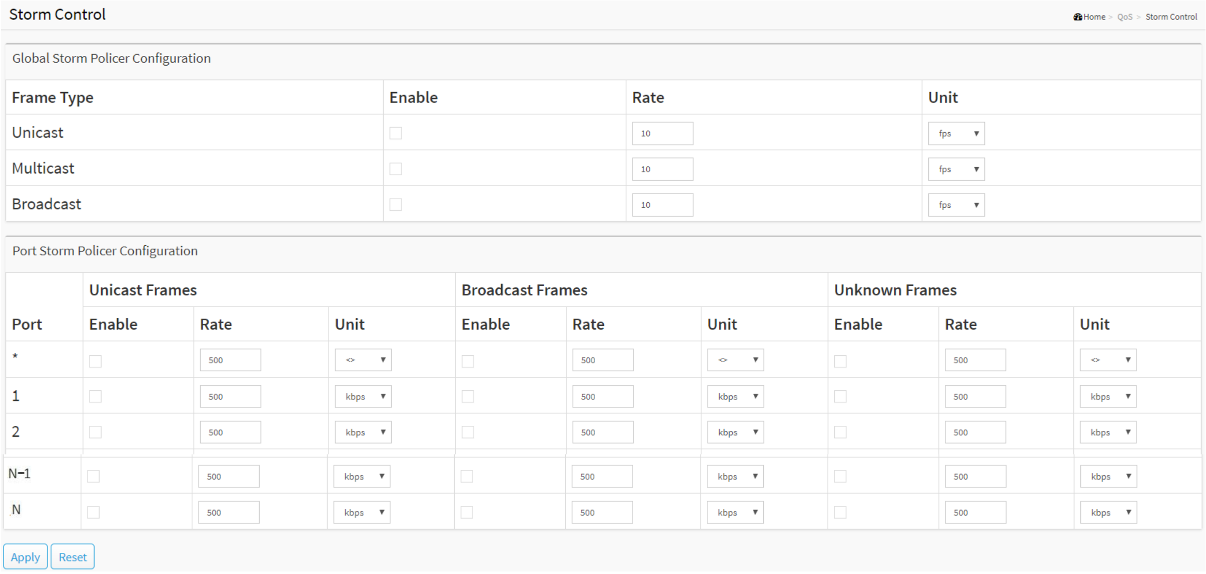
6-4 Storm Control

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

Web Interface

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

1. Click Quality of Service and Storm Control.
2. Evoke to select the frame type to enable storm control.
3. Scroll to set the Rate Parameters and Unit.
4. Click which port need to enable, and configure the Rate limit condition.
5. Click the Apply to save the setting.
6. If you want to cancel the setting then you need to click the Reset button. It will revert to previously saved values.



Storm Control

Global Storm Policer Configuration

Frame Type	Enable	Rate	Unit
Unicast	□	10	fps ▾
Multicast	□	10	fps ▾
Broadcast	□	10	fps ▾

Port Storm Policer Configuration

	Unicast Frames			Broadcast Frames			Unknown Frames		
Port	Enable	Rate	Unit	Enable	Rate	Unit	Enable	Rate	Unit
*	□	500	<> ▾	□	500	<> ▾	□	500	<> ▾
1	□	500	kbps ▾	□	500	kbps ▾	□	500	kbps ▾
2	□	500	kbps ▾	□	500	kbps ▾	□	500	kbps ▾
N-1	□	500	kbps ▾	□	500	kbps ▾	□	500	kbps ▾
N	□	500	kbps ▾	□	500	kbps ▾	□	500	kbps ▾

Figure 6-4: The Storm Control Configuration

Parameter description:

Global Storm Policer Configuration

Global storm policers for the switch are configured on this page.

There is a unicast storm policer, multicast storm policer, and a broadcast storm policer. These only affect flooded frames, i.e. frames with a (VLAN ID, DMAC) pair not present in the MAC Address table.

- **Frame Type :**

  The frame type for which the configuration below applies.

- **Enable :**

  Enable or disable the global storm policer for the given frame type.

- **Rate :**

  Controls the rate for the global storm policer. This value is restricted to 10-13128147 when "Unit" is fps or kbps, and 1-13128 when "Unit" is kfps or Mbps. The rate is internally rounded up to the nearest value supported by the global storm policer. Supported rates are divisible by 10 fps or 25 kbps.

- **Unit :**

  Controls the unit of measure for the global storm policer rate as fps, kfps, kbps or Mbps.

Port Storm Policer Configuration Help

Port storm policers for all switch ports are configured on this page.

There is a storm policer for known and unknown unicast frames, known and unknown broadcast frames and unknown (flooded) unicast, multicast and broadcast frames.

- **Port :**

  The port number for which the configuration below applies.

- **Enable :**

  Enable or disable the storm policer for this switch port.

- **Rate :**

  Controls the rate for the port storm policer. This value is restricted to 10-13128147 when "Unit" is fps or kbps, and 1-13128 when "Unit" is kfps or Mbps. The rate is internally rounded up to the nearest value supported by the port storm policer. Supported rates are divisible by 10 fps or 25 kbps.

- **Unit :**

  Controls the unit of measure for the port storm policer rate as fps, kfps, kbps or Mbps.

Buttons

- **Apply :**

  Click to save changes.

- **Reset :**

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

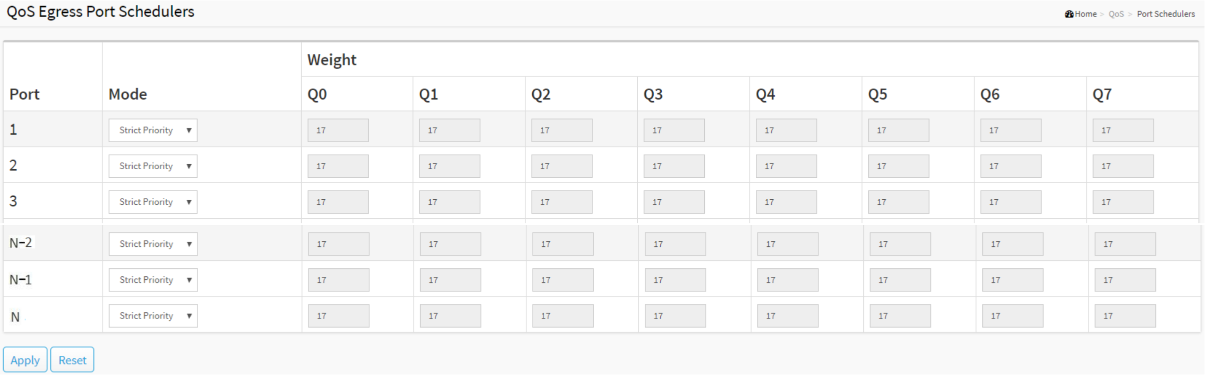
6-5 Port Scheduler

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

Web Interface

To configure the QoS Port Schedulers in the web interface:

1. Click Quality of Service and Port Scheduler.
2. Click the Port and display the QoS Egress Port Schedulers
3. Scroll Port and Scheduler Mode, specify the Queue Shaper parameter.
4. Click the Apply to save the setting.
5. If you want to cancel the setting then you need to click the Reset button. It will revert to previously saved values.



QoS Egress Port Schedulers

		Weight							
Port	Mode	Q0	Q1	Q2	Q3	Q4	Q5	Q6	Q7
1	Strict Priority ▾	17	17	17	17	17	17	17	17
2	Strict Priority ▾	17	17	17	17	17	17	17	17
3	Strict Priority ▾	17	17	17	17	17	17	17	17
N-2	Strict Priority ▾	17	17	17	17	17	17	17	17
N-1	Strict Priority ▾	17	17	17	17	17	17	17	17
N	Strict Priority ▾	17	17	17	17	17	17	17	17

Figure 6-5: The QoS Egress Port Schedules

Parameter description:

- **Port :**

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

- **Mode**

  Shows the scheduling mode for this port.

- **Qn**

  Shows the weight for this queue and port.

- **Scheduler Mode**

  Controls how many of the queues are scheduled as strict and how many are scheduled as weighted on this switch port.

- **Queue Shaper Enable**

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

- **Queue Shaper Rate**

  Controls the rate for the queue shaper. This value is restricted to 100-13107100 when "Unit" is kbps, and 1-13107 when "Unit" is Mbps.The rate is internally rounded up to the nearest value supported by the queue shaper.

- **Queue Shaper Unit**

Controls the unit of measure for the queue shaper rate as kbps or Mbps.

- **Queue Shaper Rate-type**

  The rate type of the queue shaper. The allowed values are:
  Line: Specify that this shaper operates on line rate.
  Data: Specify that this shaper operates on data rate.

- **Queue Scheduler Weight**

  Controls the weight for this queue. This value is restricted to 1-100. This parameter is only shown if "Scheduler Mode" is set to "Weighted".

- **Queue Scheduler Percent**

  Shows the weight in percent for this queue. This parameter is only shown if "Scheduler Mode" is set to "Weighted".

- **Port Shaper Enable**

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

- **Port Shaper Rate**

  Controls the rate for the port shaper. This value is restricted to 100-13107100 when "Unit" is kbps, and 1-13107 when "Unit" is Mbps.The rate is internally rounded up to the nearest value supported by the port shaper.

- **Port Shaper Unit**

  Controls the unit of measure for the port shaper rate as kbps or Mbps.

- **Port Shaper Rate-type**

  The rate type of the port shaper. The allowed values are:
  Line: Specify that this shaper operates on line rate.
  Data: Specify that this shaper operates on data rate.

Buttons

- **Apply :**

  Click to save changes.

- **Reset :**

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

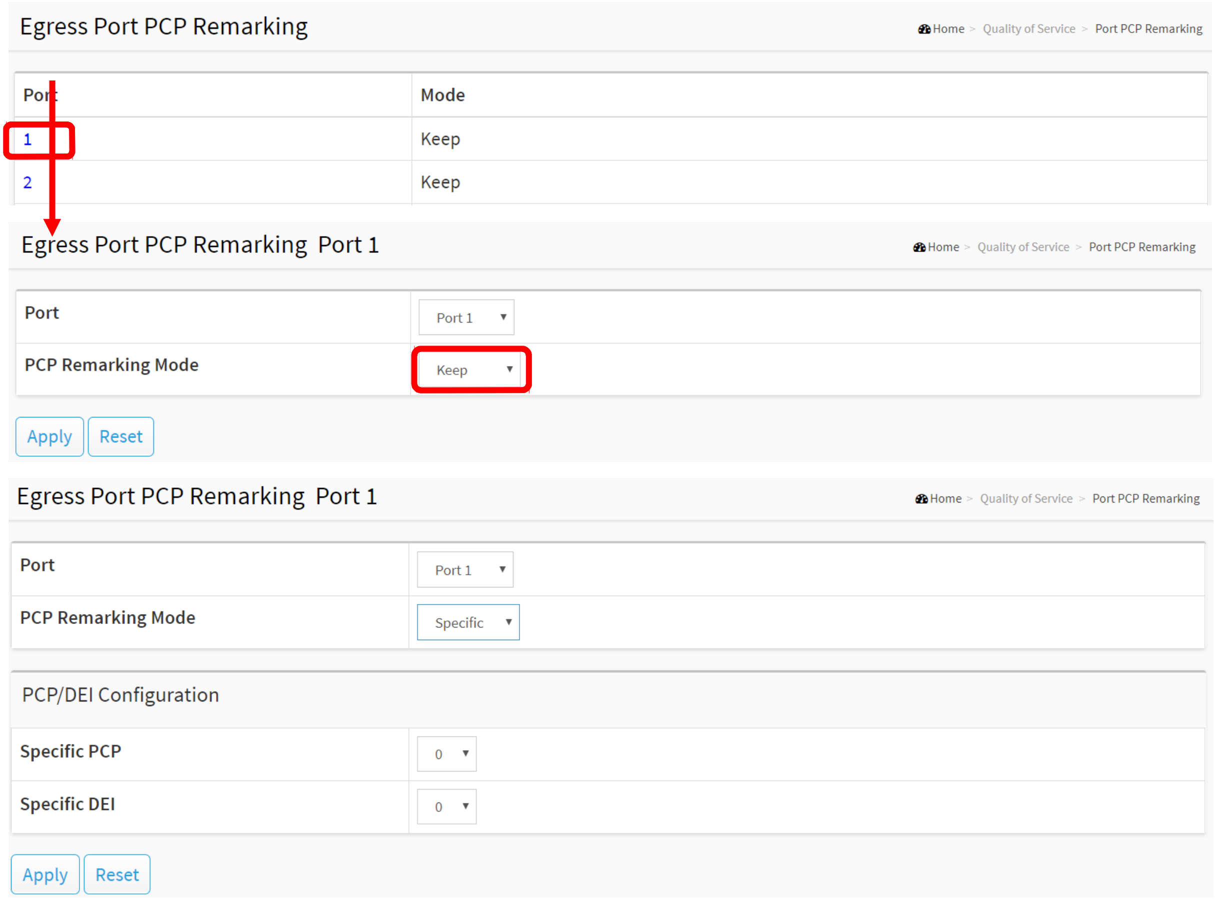
6-6 Port PCP Remarking

The Section provides user to get an overview of QoS Egress Port PCP Remarking for all switch ports. Others the ports belong to the currently selected stack unit, as reflected by the page header. .

Web Interface

To configure the QoS Port PCP Remarking in the web interface:

1. Click Quality of Service and Port PCP Remarking.
2. Click the Port and display the QoS Port PCP Remarking.
3. Scroll the Port and PCP Remarking Mode and specify the Queue Shaper parameter.
4. Click the Apply to save the setting.
5. If you want to cancel the setting then you need to click the Reset button. It will revert to previously saved values.



Egress Port PCP Remarking

Home > Quality of Service > Port PCP Remarking

Port	Mode
1	Keep
2	Keep

Egress Port PCP Remarking Port 1

Home > Quality of Service > Port PCP Remarking

Port	Port 1 ▾
PCP Remarking Mode	Keep ▾

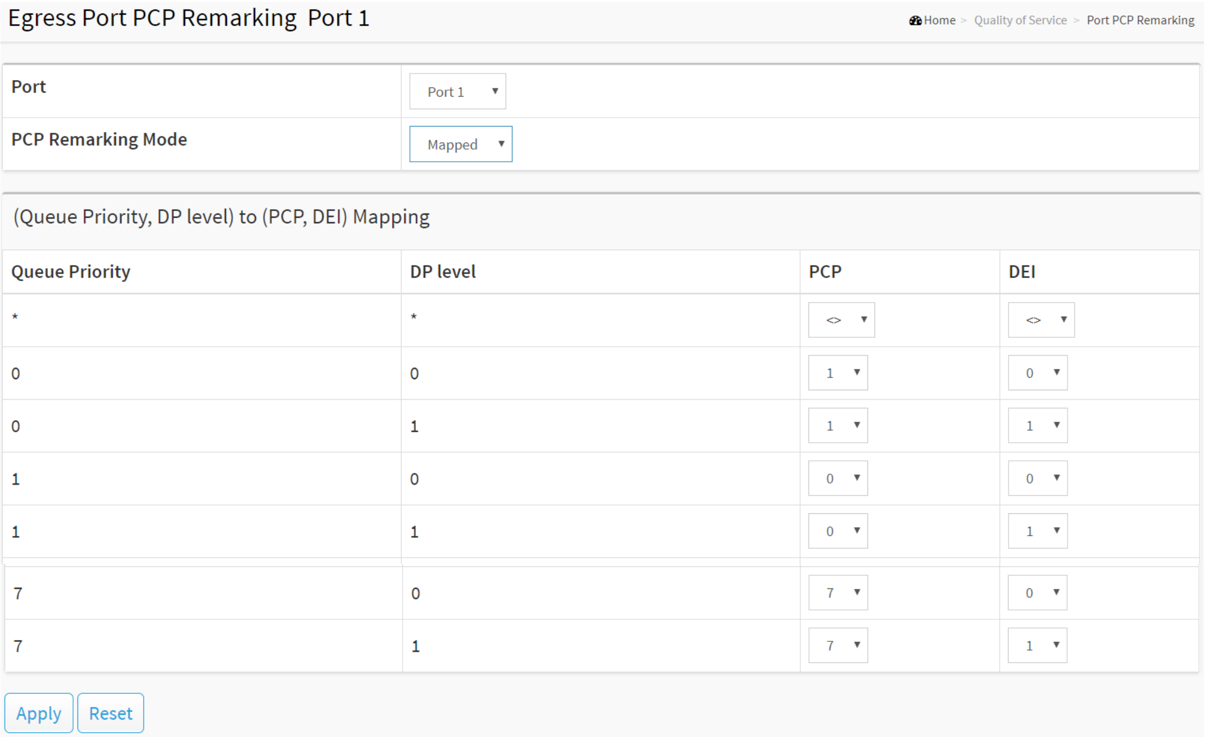
Egress Port PCP Remarking Port 1

Home > Quality of Service > Port PCP Remarking

Port	Port 1 ▾
PCP Remarking Mode	Specific ▾

PCP/DEI Configuration

Specific PCP	0 ▾
Specific DEI	0 ▾



Egress Port PCP Remarking Port 1

Port	Port 1 ▾
PCP Remarking Mode	Mapped ▾

(Queue Priority, DP level) to (PCP, DEI) Mapping

Queue Priority	DP level	PCP	DEI
*	*	<> ▾	<> ▾
0	0	1 ▾	0 ▾
0	1	1 ▾	1 ▾
1	0	0 ▾	0 ▾
1	1	0 ▾	1 ▾
7	0	7 ▾	0 ▾
7	1	7 ▾	1 ▾

Figure 6-6: The Port PCP Remarking

Parameter description:

- **Port :**

  The logical port for the settings contained in the same row.
  Click on the port number in order to configure PCP remarking.

- **Mode :**

  Shows the PCP remarking mode for this port.
  Keep: Use classified PCP/DEI values.
  Specific: Use default PCP/DEI values.
  Mapped: Use mapped versions of CoS and DPL.

- **PCP/DEI Configuration :**

  Controls the default PCP and DEI values used when the mode is set to Default.

- **(QoS class, DP level) to (PCP, DEI) Mapping :**

  Controls the mapping of the classified (QoS class, DP level) to (PCP, DEI) values when the mode is set to Mapped.

Buttons

- **Apply :**

  Click to save changes.

- **Reset :**

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

6-7 DSCP

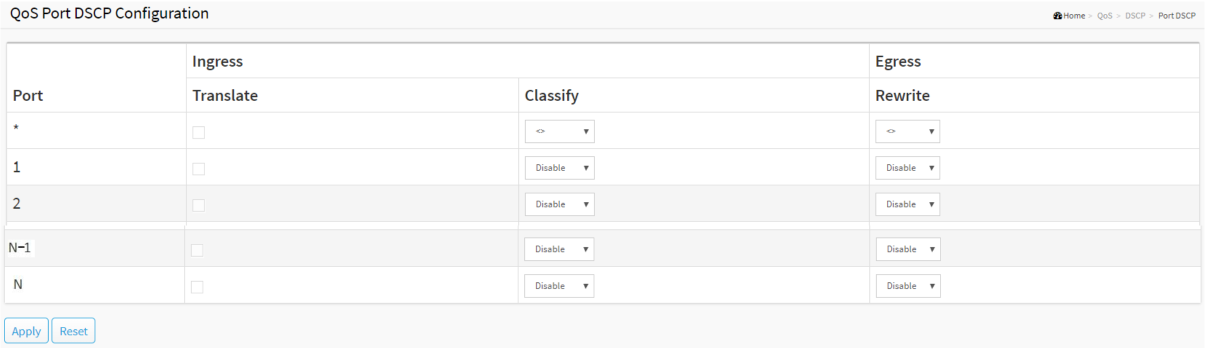
6-7.1 Port DSCP

The section will teach user to set the QoS Port DSCP configuration that was allowed you to configure the basic QoS Port DSCP Configuration settings for all switch ports. Others the settings relate to the currently selected stack unit, as reflected by the page header.

Web Interface

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

1. Click Quality of Service, DSCP and Port DSCP.
2. Evoke to enable or disable the Ingress Translate and Scroll the Classify parameter.
3. Scroll to select Egress Rewrite parameters
4. Click the apply to save the setting
5. If you want to cancel the setting then you need to click the Reset button. It will revert to previously saved values



QoS Port DSCP Configuration

	Ingress		Egress
Port	Translate	Classify	Rewrite
*	□	<> ▾	<> ▾
1	□	Disable ▾	Disable ▾
2	□	Disable ▾	Disable ▾
N-1	□	Disable ▾	Disable ▾
N	□	Disable ▾	Disable ▾

Figure 6-7.1: The QoS Port DSCP Configuration

Parameter description:

- **Port :**

  The Port column shows the list of ports for which you can configure dscp ingress and egress settings.

- **Ingress :**

  In Ingress settings you can change ingress translation and classification settings for individual ports.

  There are two configuration parameters available in Ingress:

  1. Translate: To Enable the Ingress Translation click the checkbox
  2. Classify: Classification for a port have 4 different values

  Disable: No Ingress DSCP Classification.

  DSCP=0: Classify if incoming (or translated if enabled) DSCP is 0.

  Selected: Classify only selected DSCP for which classification is enabled as specified in DSCP Translation window for the specific DSCP.

  All: Classify all DSCP.

- **Egress :**

Port Egress Rewriting can be one of below parameters

Disable: No Egress rewrite.

Enable: Rewrite enable without remapped.

Remap: DSCP from analyzer is remapped and frame is remarked with remapped DSCP value.

Buttons

- **Apply :**

  Click to save changes.

- **Reset :**

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

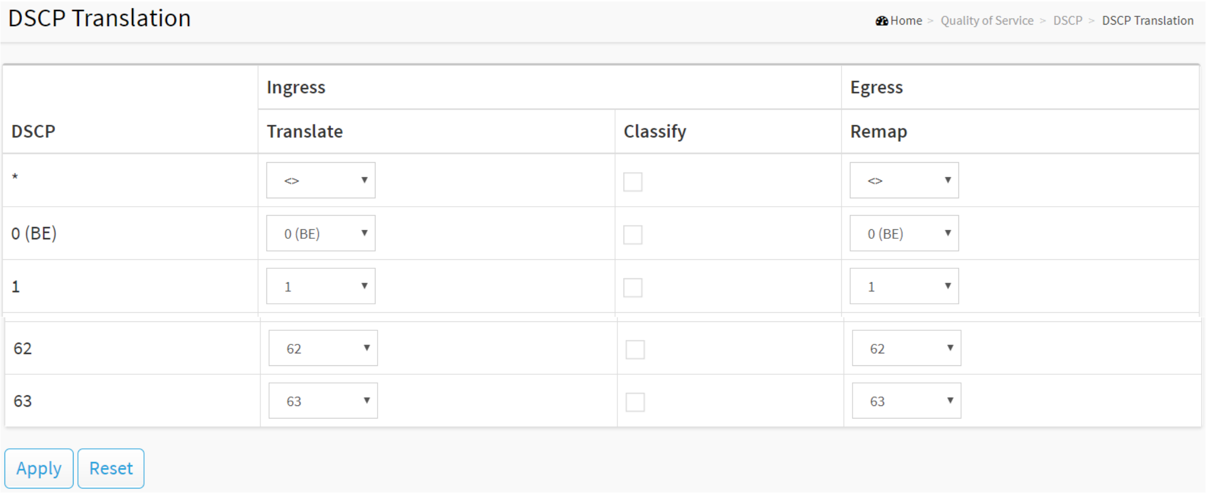
6-7.2 DSCP Translation

The section describes the switch allows you to configure the basic QoS DSCP Translation settings for all switches. DSCP translation can be done in Ingress or Egress.

Web Interface

To configure the DSCP Translation parameters in the web interface:

1. Click Quality of Service, DSCP and DSCP Translation.
2. Scroll to set the Ingress Translate and Egress Remap Parameters.
3. Evoke to enable or disable Classify.
4. Click the apply to save the setting.
5. If you want to cancel the setting then you need to click the Reset button. It will revert to previously saved values.



DSCP Translation

	Ingress		Egress
DSCP	Translate	Classify	Remap
*	<>	□	<>
0 (BE)	0 (BE)	□	0 (BE)
1	1	□	1
62	62	□	62
63	63	□	63

Figure 6-7.2: The DSCP Translation Configuration

Parameter description:

- **DSCP :**

  Maximum number of supported DSCP values are 64 and valid DSCP value ranges from 0 to 63.

- **Ingress :**

  Ingress side DSCP can be first translated to new DSCP before using the DSCP for QoS class and DPL map.

  There are two configuration parameters for DSCP Translation –

  Translate: DSCP at Ingress side can be translated to any of (0-63) DSCP values.

  Classify: Click to enable Classification at Ingress side.

- **Egress :**

  Select the DSCP value from select menu to which you want to remap. DSCP value ranges form 0 to 63.

Buttons

- **Apply :**

  Click to save changes.

- **Reset :**

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

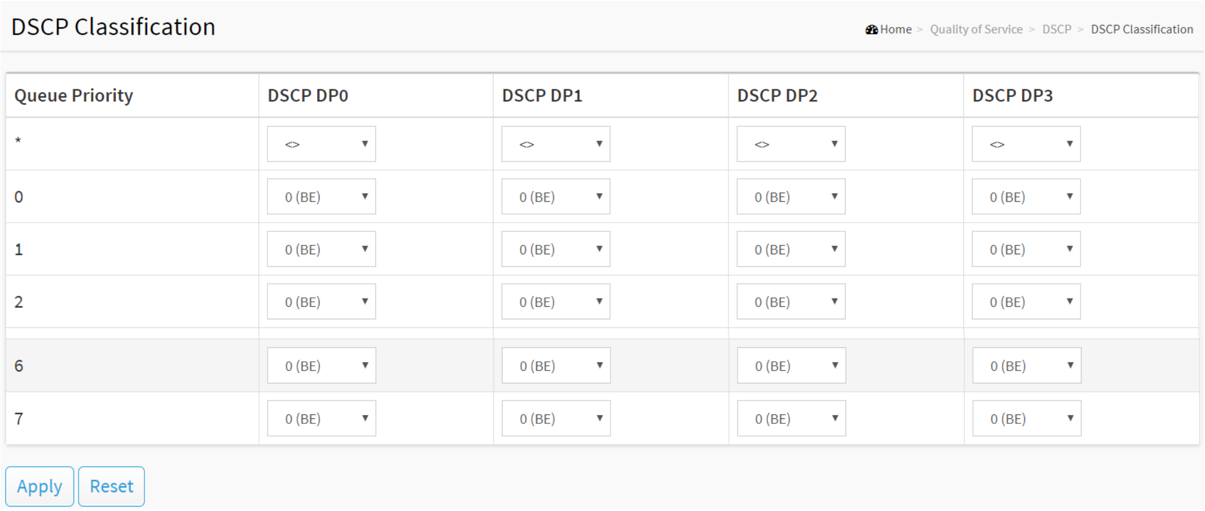
6-7.3 DSCP Classification

The section describes to teach user to configure and allows you to map DSCP value to a QoS Class and DPL value. Others the settings relate to the currently selected stack unit, as reflected by the page header.

Web Interface

To configure the DSCP Classification parameters in the web interface:

1. Click Quality of Service, DSCP and DSCP Translation
2. Scroll to set the DSCP Parameters
3. Click the apply to save the setting
4. If you want to cancel the setting then you need to click the Reset button. It will revert to previously saved values



DSCP Classification

Queue Priority	DSCP DP0	DSCP DP1	DSCP DP2	DSCP DP3
*	<>	<>	<>	<>
0	0 (BE)	0 (BE)	0 (BE)	0 (BE)
1	0 (BE)	0 (BE)	0 (BE)	0 (BE)
2	0 (BE)	0 (BE)	0 (BE)	0 (BE)
6	0 (BE)	0 (BE)	0 (BE)	0 (BE)
7	0 (BE)	0 (BE)	0 (BE)	0 (BE)

Figure 6-7.3: The DSCP Classification Configuration

Parameter description:

- **Queue Priority :**

  Actual Class of Service.

- **DSCP DP0 :**

  Select the classified DSCP value (0-63) for Drop Precedence Level 0.

- **DSCP DP1 :**

  Select the classified DSCP value (0-63) for Drop Precedence Level 1.

- **DSCP DP2 :**

  Select the classified DSCP value (0-63) for Drop Precedence Level 2.

- **DSCP DP3 :**

  Select the classified DSCP value (0-63) for Drop Precedence Level 3.

Buttons

- **Apply :**

  Click to save changes.

- **Reset :**

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

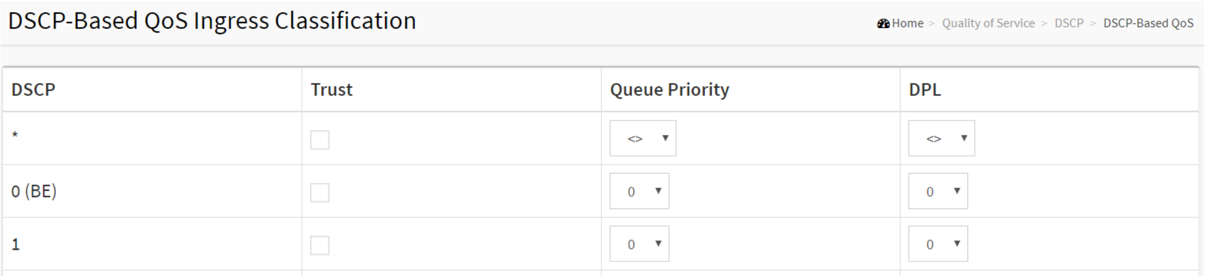
6-7.4 DSCP-Based QoS

The section will teach user to configure the DSCP-Based QoS mode that This page allows you to configure the basic QoS DSCP based QoS Ingress Classification settings for all switches.

Web Interface

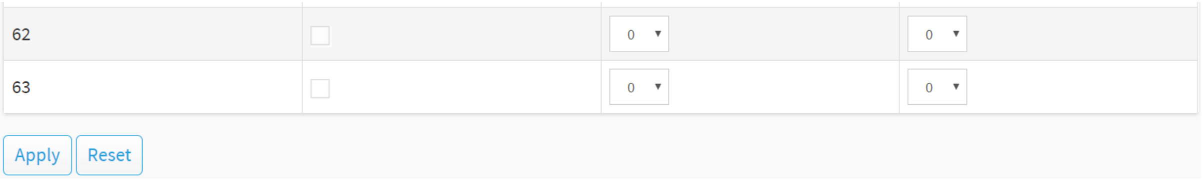
To configure the DSCP –Based QoS Ingress Classification parameters in the web interface:

1. Click Quality of Service, DSCP and DSCP-Based QoS.
2. Evoke to enable or disable the DSCP for Trust.
3. Scroll to select Queue Priority and DPL parameters.
4. Click the save to save the setting.
5. If you want to cancel the setting then you need to click the Reset button. It will revert to previously saved values.



DSCP-Based QoS Ingress Classification

DSCP	Trust	Queue Priority	DPL
*	□	<>	<>
0 (BE)	□	0	0
1	□	0	0



62	□	0 ▾	0 ▾
63	□	0 ▾	0 ▾

Figure 6-7.4: The DSCP-Based QoS Ingress Classification Configuration

Parameter description:

- **DSCP :**

  Maximum number of support ed DSCP values are 64.

- **Trust :**

  Click to check if the DSCP value is trusted.

- **Queue Priority :**

  Queue Priority value can be any between 0 and 7. 7 is the highest.

- **DPL :**

  Drop Precedence Level (0-3)

Buttons

- **Apply :**

  Click to save changes.

- **Reset :**

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

6-8 QoS Control List

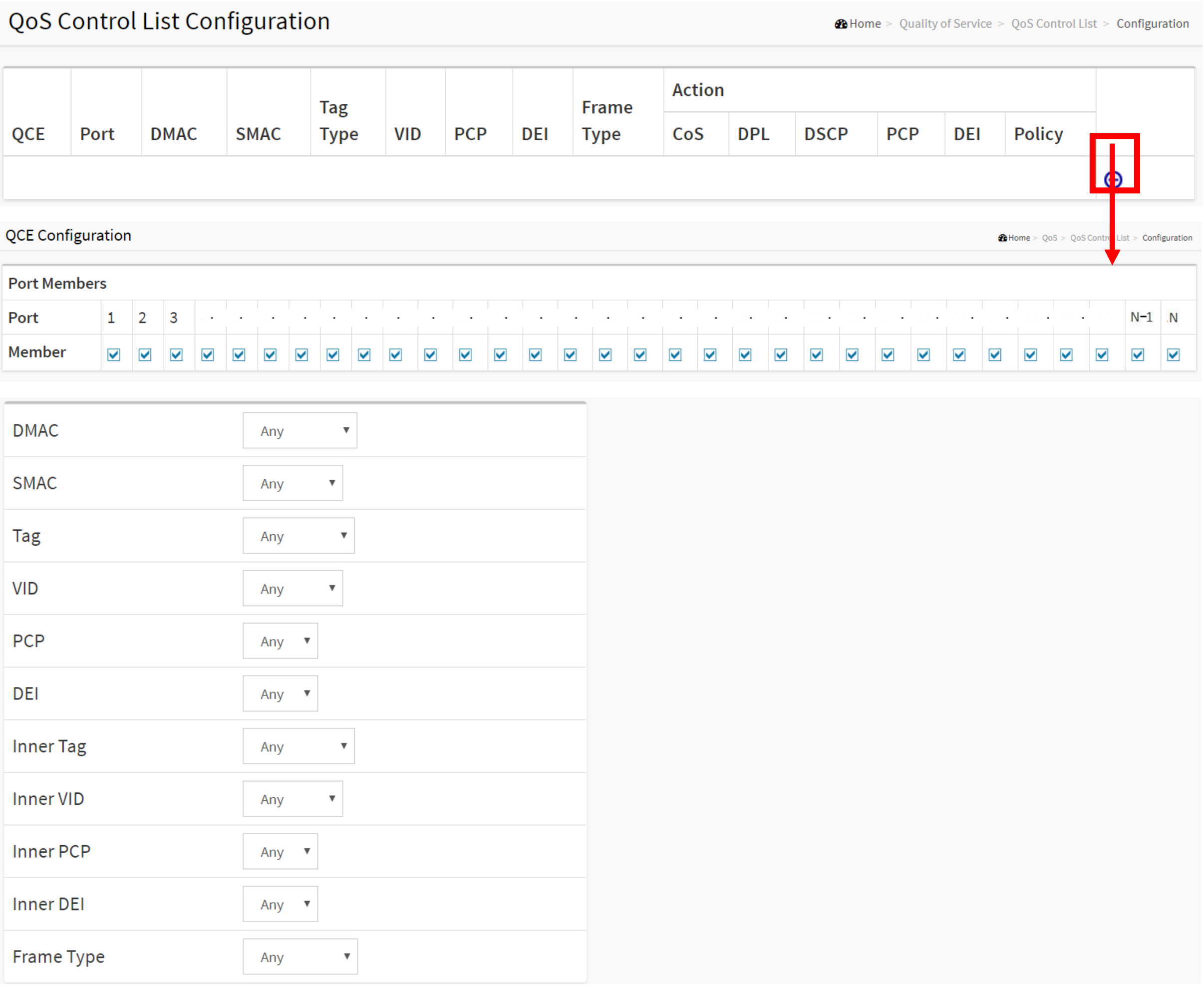
6-8.1 Configuration

The section shows the QoS Control List (QCL), which is made up of the QCEs. Each row describes a QCE that is defined. The maximum number of QCEs is 256 on each switch. Click on the lowest plus sign to add a new QCE to the list.

Web Interface

To configure the QoS Control List parameters in the web interface:

1. Click Quality of Service, QoS Contol List and Configuration.
2. Click the ⊕ to add a new QoS Control List.
3. Scroll all parameters and evoke the Port Member to join the QCE rules.
4. Click the apply to save the setting.
5. If you want to cancel the setting then you need to click the Reset button. It will revert to previously saved values.



QoS Control List Configuration

Home > Quality of Service > QoS Control List > Configuration

				Tag				Frame	Action						
QCE	Port	DMAC	SMAC	Type	VID	PCP	DEI	Type	CoS	DPL	DSCP	PCP	DEI	Policy	
															⊕

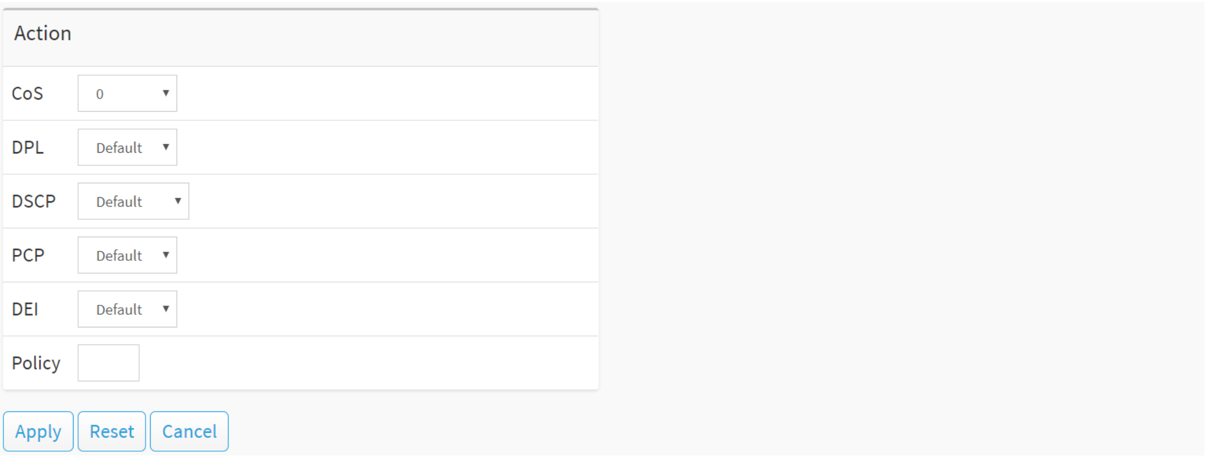
QCE Configuration

Home > QoS > QoS Control List > Configuration

Port Members

Port	1	2	3	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	N-1	N
Member	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑

DMAC	Any ▾
SMAC	Any ▾
Tag	Any ▾
VID	Any ▾
PCP	Any ▾
DEI	Any ▾
Inner Tag	Any ▾
Inner VID	Any ▾
Inner PCP	Any ▾
Inner DEI	Any ▾
Frame Type	Any ▾



Action

CoS	0
DPL	Default
DSCP	Default
PCP	Default
DEI	Default
Policy	

Figure 6-8.1: The QoS Control List Configuration

Parameter description:

- **QCE :**

  Indicates the index of QCE.

- **Port :**

  Indicates the list of ports configured with the QCE.

- **DMAC :**

  Indicates the destination MAC address. Possible values are:

  Any: Match any DMAC.

  Unicast: Match unicast DMAC.

  Multicast: Match multicast DMAC.

  Broadcast: Match broadcast DMAC.

  <MAC>: Match specific DMAC.

  The default value is 'Any'.

- **SMAC :**

  Match specific source MAC address or 'Any'.

  If a port is configured to match on DMAC/DIP, this field indicates the DMAC.

- **Tag Type :**

  Indicates tag type. Possible values are:
  Any: Match tagged and untagged frames.
  Untagged: Match untagged frames.
  Tagged: Match tagged frames.
  C-Tagged: Match C-tagged frames.
  S-Tagged: Match S-tagged frames.
  The default value is 'Any'.

- **VID :**

  Indicates (VLAN ID), either a specific VID or range of VIDs. VID can be in the range 1-4095 or 'Any'

- **PCP :**

  Priority Code Point: Valid values of PCP are specific (0, 1, 2, 3, 4, 5, 6, 7) or range(0-1, 2-3, 4-5, 6-7, 0-3, 4-7) or 'Any'.

- **DEI :**

Drop Eligible Indicator: Valid value of DEI are 0, 1 or 'Any'.

- **Frame Type :**

  Indicates the type of frame to look for incoming frames. Possible frame types are:

  Any: The QCE will match all frame type.

  Ethernet: Only Ethernet frames (with Ether Type 0x600-0xFFFF) are allowed.

  LLC: Only (LLC) frames are allowed.

  SNAP: Only (SNAP) frames are allowed

  IPv4: The QCE will match only IPV4 frames.

  IPv6: The QCE will match only IPV6 frames.

- **Action :**

  Indicates the classification action taken on ingress frame if parameters configured are matched with the frame's content.
  Possible actions are:
  CoS: Classify Class of Service.
  DPL: Classify Drop Precedence Level.
  DSCP: Classify DSCP value.
  PCP: Classify PCP value.
  DEI: Classify DEI value.
  Policy: Classify ACL Policy number.

- **Modification Buttons :**

  You can modify each QCE (QoS Control Entry) in the table using the following buttons:

  ⊕: Inserts a new QCE before the current row.

  ⓔ: Edits the QCE.

  ↑: Moves the QCE up the list.

  ↓: Moves the QCE down the list.

  ⊗: Deletes the QCE.

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

- **Port Members :**

  Check the checkbox button to include the port in the QCL entry. By default all ports are included.

- **Key Parameters :**

  Key configuration is described as below:

  DMAC Destination MAC address: Possible values are 'Unicast', 'Multicast', 'Broadcast', 'Specific' (xx-xx-xx-xx-xx-xx) or 'Any'.
  SMAC Source MAC address: xx-xx-xx-xx-xx-xx or 'Any'.
  Tag Value of Tag field can be 'Untagged', 'Tagged', 'C-Tagged', 'S-Tagged' or 'Any'.
  VID Valid value of VLAN ID can be any value in the range 1-4095 or 'Any'; user can enter either a specific value or a range of VIDs.
  PCP Valid value PCP are specific (0, 1, 2, 3, 4, 5, 6, 7) or range (0-1, 2-3, 4-5, 6-7, 0-3, 4-7) or 'Any'.
  DEI Valid value of DEI can be '0', '1' or 'Any'.
  Inner Tag Value of Inner Tag field can be 'Untagged', 'Tagged', 'C-Tagged', 'S-Tagged' or 'Any'.
  Inner VID Valid value of Inner VLAN ID can be any value in the range 1-4095 or 'Any'; user

can enter either a specific value or a range of VIDs.
Inner PCP Valid value of Inner PCP are specific (0, 1, 2, 3, 4, 5, 6, 7) or range (0-1, 2-3, 4-5, 6-7, 0-3, 4-7) or 'Any'.
Inner DEI Valid value of Inner DEI can be '0', '1' or 'Any'.
Frame Type Frame Type can have any of the following values:

Any

EtherType

LLC

SNAP

IPv4

IPv6

Note: All frame types are explained below.

- **Any :**

  Allow all types of frames.

- **EtherType :**

  Ether Type Valid Ether Type can be 0x600-0xFFFF excluding 0x800(IPv4) and 0x86DD(IPv6) or 'Any'.

- **LLC :**

  DSAP Address Valid DSAP(Destination Service Access Point) can vary from 0x00 to 0xFF or 'Any'.
  SSAP Address Valid SSAP(Source Service Access Point) can vary from 0x00 to 0xFF or 'Any'.
  Control Valid Control field can vary from 0x00 to 0xFF or 'Any'.

- **SNAP :**

  PID Valid PID(a.k.a Ether Type) can be 0x0000-0xFFFF or 'Any'.

- **IPv4 :**

  Protocol IP protocol number: (0-255, 'TCP' or 'UDP') or 'Any'.
  Source IP Specific Source IP address in value/mask format or 'Any'. IP and Mask are in the format x.y.z.w where x, y, z, and w are decimal numbers between 0 and 255. When Mask is converted to a 32-bit binary string and read from left to right, all bits following the first zero must also be zero.
  Destination IP Specific Destination IP address in value/mask format or 'Any'.
  IP Fragment IPv4 frame fragmented option: 'Yes', 'No' or 'Any'.
  DSCP Diffserv Code Point value (DSCP): It can be a specific value, range of values or 'Any'. DSCP values are in the range 0-63 including BE, CS1-CS7, EF or AF11-AF43.
  Sport Source TCP/UDP port:(0-65535) or 'Any', specific or port range applicable for IP protocol UDP/TCP.
  Dport Destination TCP/UDP port:(0-65535) or 'Any', specific or port range applicable for IP protocol UDP/TCP.

- **IPv6 :**

  Protocol IP protocol number: (0-255, 'TCP' or 'UDP') or 'Any'.
  Source IP 32 LS bits of IPv6 source address in value/mask format or 'Any'.
  Destination IP Specific Destination IP address in value/mask format or 'Any'.
  DSCP Diffserv Code Point value (DSCP): It can be a specific value, range of values or 'Any'. DSCP values are in the range 0-63 including BE, CS1-CS7, EF or AF11-AF43.
  Sport Source TCP/UDP port:(0-65535) or 'Any', specific or port range applicable for IP protocol UDP/TCP.
  Dport Destination TCP/UDP port:(0-65535) or 'Any', specific or port range applicable for IP protocol UDP/TCP.

- **Action Parameters :**

  CoS Class of Service: (0-7) or 'Default'.
  DPL Drop Precedence Level: (0-3) or 'Default'.
  DSCP DSCP: (0-63, BE, CS1-CS7, EF or AF11-AF43) or 'Default'.
  PCP PCP: (0-7) or 'Default'. Note: PCP and DEI cannot be set individually.
  DEI DEI: (0-1) or 'Default'.
  Policy ACL Policy number: (0-127) or 'Default' (empty field).

  'Default' means that the default classified value is not modified by this QCE.

Buttons

- **Apply :**

  Click to save changes.

- **Reset :**

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

- **Cancel :**

  Return to the previous page without saving the configuration change.

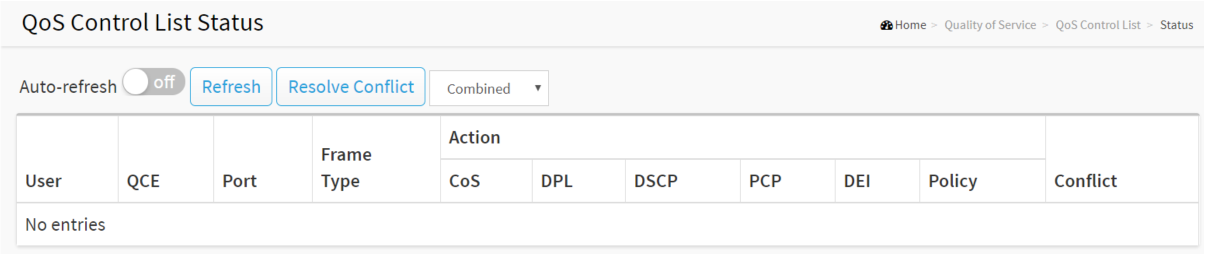
6-8.2 Status

The section will let you know how to configure and shows the QCL status
by different QCL users. Each row describes the QCE that is defined. It is a conflict if a specific QCE is not applied to the hardware due to hardware limitations. The maximum number of QCEs is 256 on each switch.

Web Interface

To display the QoS Control List Status in the web interface:

1. Click Quality of Service, QoS Contol List and Status.
2. If you want to auto-refresh the information then you need to evoke the “Auto-refresh”.
3. Scroll to select the combined, static, Voice VLAN and conflict.
4. To click the “Refresh” to refresh an entry of the MVR Statistics Information.



QoS Control List Status

				Action						
User	QCE	Port	Frame Type	CoS	DPL	DSCP	PCP	DEI	Policy	Conflict
No entries										

Figure 6-8.2: The QoS Control List Status

Parameter description:

- **User :**

  Indicates the QCL user.

- **QCE :**

Indicates the index of QCE.

- **Port :**

  Indicates the list of ports configured with the QCE.

- **Frame Type :**

  Indicates the type of frame. Possible values are:
  Any: Match any frame type.
  Ethernet: Match EtherType frames.
  LLC: Match (LLC) frames.
  SNAP: Match (SNAP) frames.
  IPv4: Match IPv4 frames.
  IPv6: Match IPv6 frames.

- **Action :**

  Indicates the classification action taken on ingress frame if parameters configured are matched with the frame's content.
  Possible actions are:
  CoS: Classify Class of Service.
  DPL: Classify Drop Precedence Level.
  DSCP: Classify DSCP value.
  PCP: Classify PCP value.
  DEI: Classify DEI value.
  Policy: Classify ACL Policy number.
  Ingress Map: Classify Ingress Map ID.

- **Conflict :**

  Displays Conflict status of QCL entries. It may happen that resources required to add a QCE may not available, in that case it shows conflict status as 'Yes', otherwise it is always 'No'. Please note that conflict can be resolved by releasing the H/W resources required to add QCL entry on pressing 'Resolve Conflict' button.

Buttons

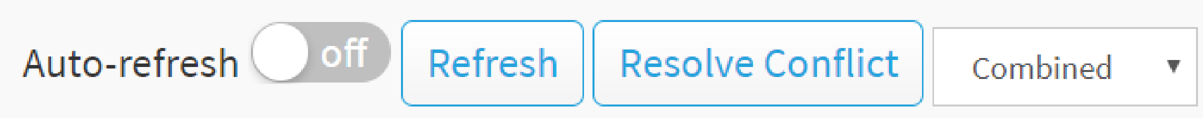


Figure 6-8.2: The QoS Control List Status buttons

- **Auto-refresh :**

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

- **Refresh :**

  Click to refresh the page immediately.

- **Combined :**

  Select the QCL status from this drop down list.

- **Resolve Conflict :**

  Click to release the resources required to add QCL entry, in case the conflict status for any QCL entry is 'yes'.

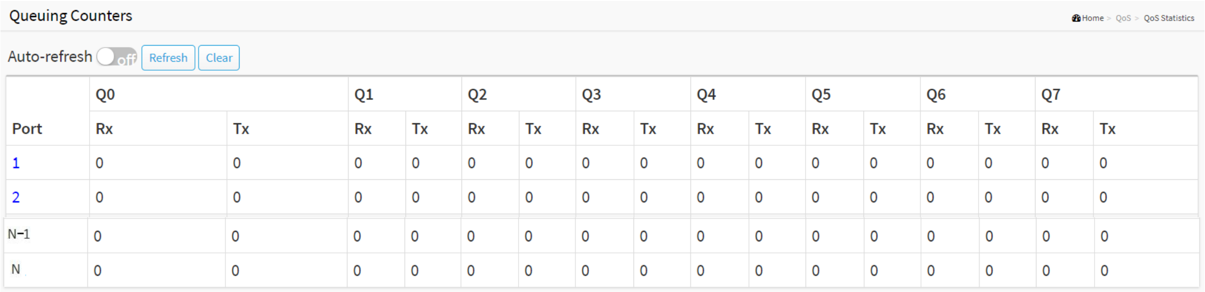
6-9 Qos Statistics

This page provides statistics for the different queues for all switch ports.

Web Interface

To Display the Queuing Counters in the web interface:

1. Click Quality of Service and QoS Statistics
2. If you want to auto-refresh the information then you need to evoke the “Auto-refresh”.
3. Click “Refresh” to refresh the Queuing Counters or clear all information when you click “Clear”.



Queuing Counters

Home > QoS > QoS Statistics

	Q0		Q1		Q2		Q3		Q4		Q5		Q6		Q7	
Port	Rx	Tx	Rx	Tx	Rx	Tx	Rx	Tx	Rx	Tx	Rx	Tx	Rx	Tx	Rx	Tx
1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
2	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
N-1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
N	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0

Figure 6-9: The Queuing Counters Overview

Parameter description:

- **Port :**

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

- **Qn :**

  Qn is the Queue number, There are 8 QoS queues per port. Q0 is the lowest priority queue.

- **Rx/Tx :**

  The number of received and transmitted packets per queue.

Buttons

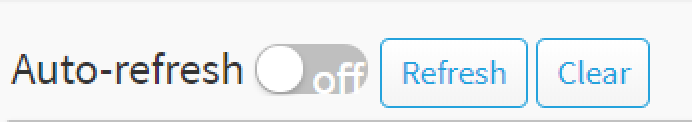


Figure 6-9: The Queuing Counters buttons

- **Auto-refresh :**

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

- **Refresh :**

  Click to refresh the page.

- **Clear :**

  Click to clear the page.

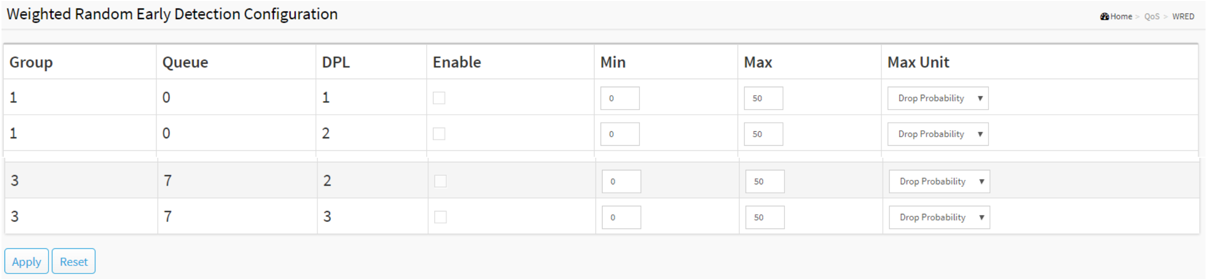
6-10 WRED

This page allows you to configure the Random Early Detection (RED) settings. Through different RED configuration for the queues it is possible to obtain Weighted Random Early Detection (WRED) operation between queues.The settings are global for all ports in the switch.X

Web Interface

To configure and display the Random Early Detection in the web interface:

1. Click Quality of Service and WRED.
2. Scroll all parameters and evoke the Weighted Random Early Detection Configuration.
3. Click the apply to save the setting.
4. If you want to cancel the setting then you need to click the Reset button. It will revert to previously saved values.



Weighted Random Early Detection Configuration

Group	Queue	DPL	Enable	Min	Max	Max Unit
1	0	1	□	0	50	Drop Probability ▾
1	0	2	□	0	50	Drop Probability ▾
3	7	2	□	0	50	Drop Probability ▾
3	7	3	□	0	50	Drop Probability ▾

Figure 6-10: The Weighted Random Early Detection Configuration

Parameter description:

- **Port :**

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

- **Group**

  The WRED group number for which the configuration below applies.

- **Queue**

  The queue number (CoS) for which the configuration below applies.

- **DPL**

  The Drop Precedence Level for which the configuration below applies.

- **Enable**

  Controls whether RED is enabled for this entry.

- **Min**

  Controls the lower RED fill level threshold. If the queue filling level is below this threshold, the drop probability is zero. This value is restricted to 0-100%.

- **Max**

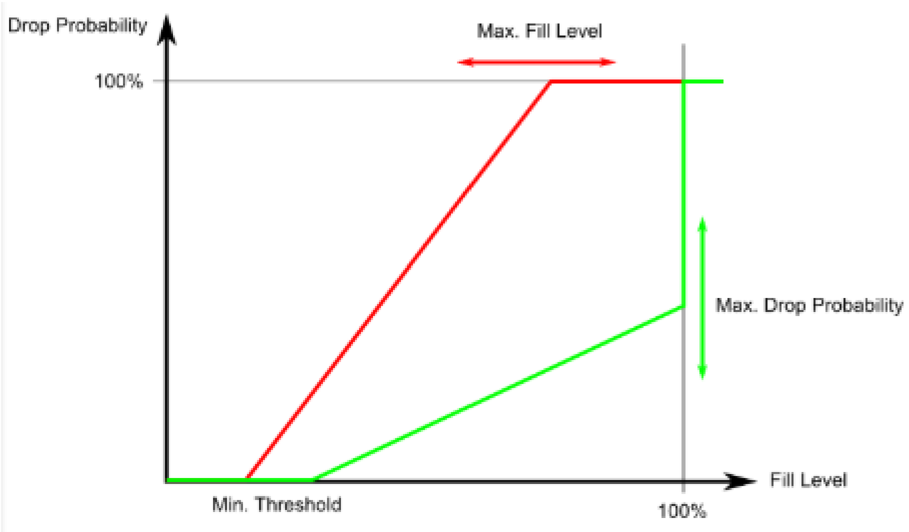
  Controls the upper RED drop probability or fill level threshold for frames marked with Drop Precedence Level > 0 (yellow frames). This value is restricted to 1-100%.

- **Max Unit**

  Selects the unit for Max. Possible values are: **Drop Probability:** Max controls the drop probability just below 100% fill level. **Fill Level:** Max controls the fill level where drop probability reaches 100%.

RED Drop Probability Function

The following illustration shows the drop probability versus fill level function with associated parameters.



Min is the fill level where the queue randomly start dropping frames marked with Drop Precedence Level > 0 (yellow frames).
If Max Unit is 'Drop Probability' (the green line), Max controls the drop probability when the fill level is just below 100%.
If Max Unit is 'Fill Level' (the red line), Max controls the fill level where drop probability reaches 100%. This configuration makes it possible to reserve a portion of the queue exclusively for frames marked with Drop Precedence Level 0 (green frames). The reserved portion is calculated as (100 - Max) %.
Frames marked with Drop Precedence Level 0 (green frames) are never dropped.
The drop probability for frames increases linearly from zero (at Min average queue filling level) to Max Drop Probability or Fill Level.

Buttons

- **Apply :**

  Click to save changes.

- **Refresh :**

  Click to refresh the page.

Chapter 7 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.

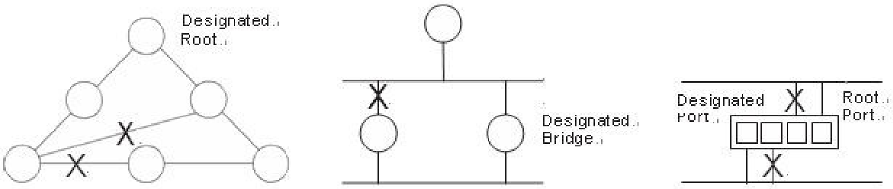


Figure 7: The Spanning Tree Protocol

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.

7-1 STP Configuration

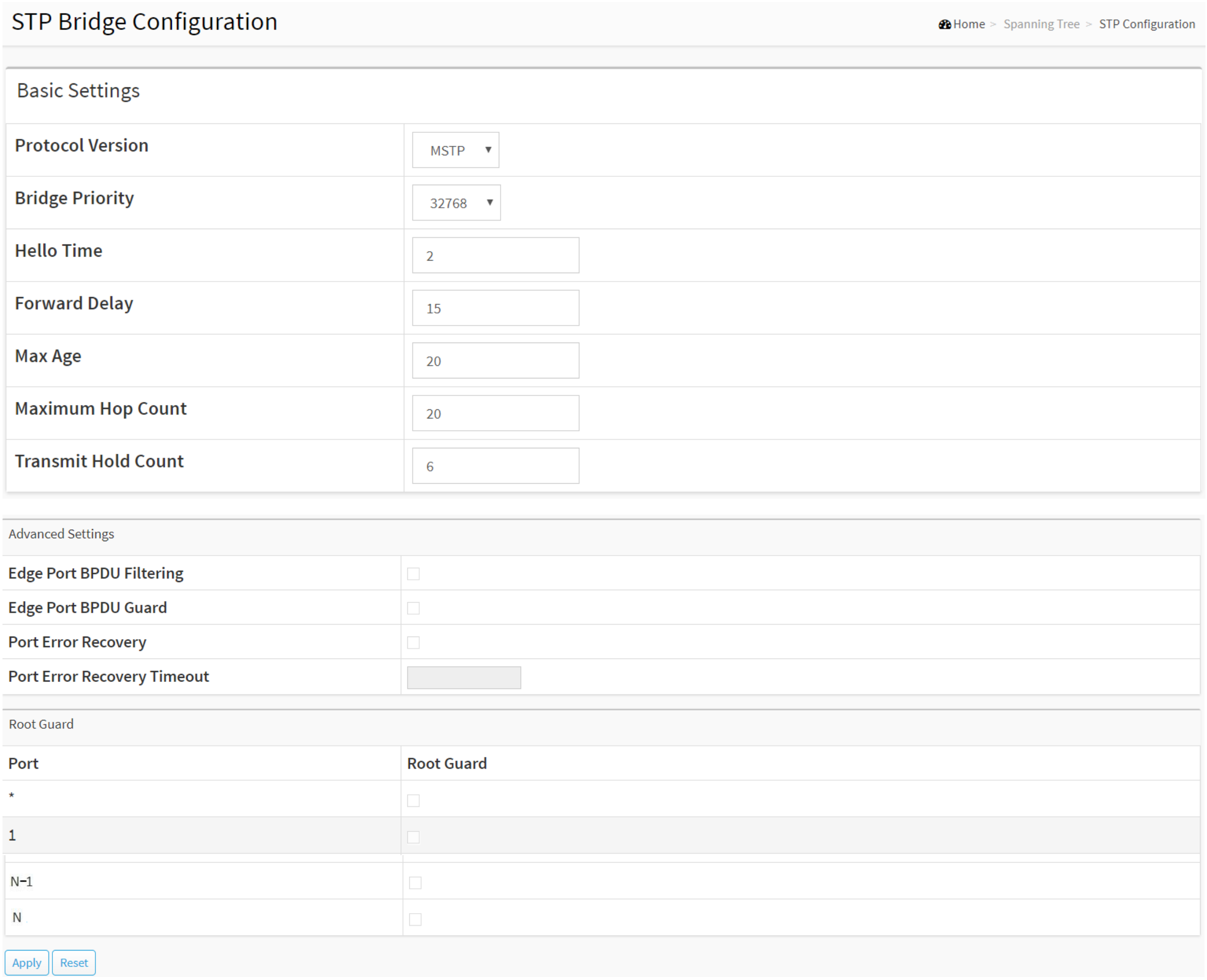
The section describes that you can select enable spanning tree protocol or not, and you can select what protocol version you want.

Web Interface

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

1. Click Spanning Tree and STP Configuration.
2. Scroll to select the parameters and write down available value of parameters in blank field in Basic Settings.
3. Evoke to enable or disable the parameters and write down available value of parameters in blank field in Advanced settings.
4. Click the apply to save the setting.

5. If you want to cancel the setting then you need to click the Reset button. It will revert to previously saved values.



STP Bridge Configuration

Basic Settings

Protocol Version	MSTP ▾
Bridge Priority	32768 ▾
Hello Time	2
Forward Delay	15
Max Age	20
Maximum Hop Count	20
Transmit Hold Count	6

Advanced Settings

Edge Port BPDU Filtering	□
Edge Port BPDU Guard	□
Port Error Recovery	□
Port Error Recovery Timeout	

Root Guard

Port	Root Guard
*	□
1	□
N−1	□
N	□

Figure 7-1: The STP Configuration

Parameter description:

Basic Settings

- **Protocol Version :**

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

- **Bridge Priority :**

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

- **Hello Time :**

  The interval between sending STP BPDU's. Valid values are in the range 1 to 10 seconds, default is 2 seconds.

  Note: Changing this parameter from the default value is not recommended, and may have adverse effects on your network.

- **Forward Delay :**

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

- **Max Age :**

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

- **Maximum Hop Count :**

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

- **Transmit Hold Count :**

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

Advanced Settings

- **Edge Port BPDU Filtering :**

  Control whether a port explicitly configured as Edge will transmit and receive BPDUs.

- **Edge Port BPDU Guard :**

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

- **Port Error Recovery :**

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

- **Port Error Recovery Timeout :**

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

Buttons

- **Apply :**

  Click to save changes.

- **Reset :**

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

7-2 MSTI Configuration

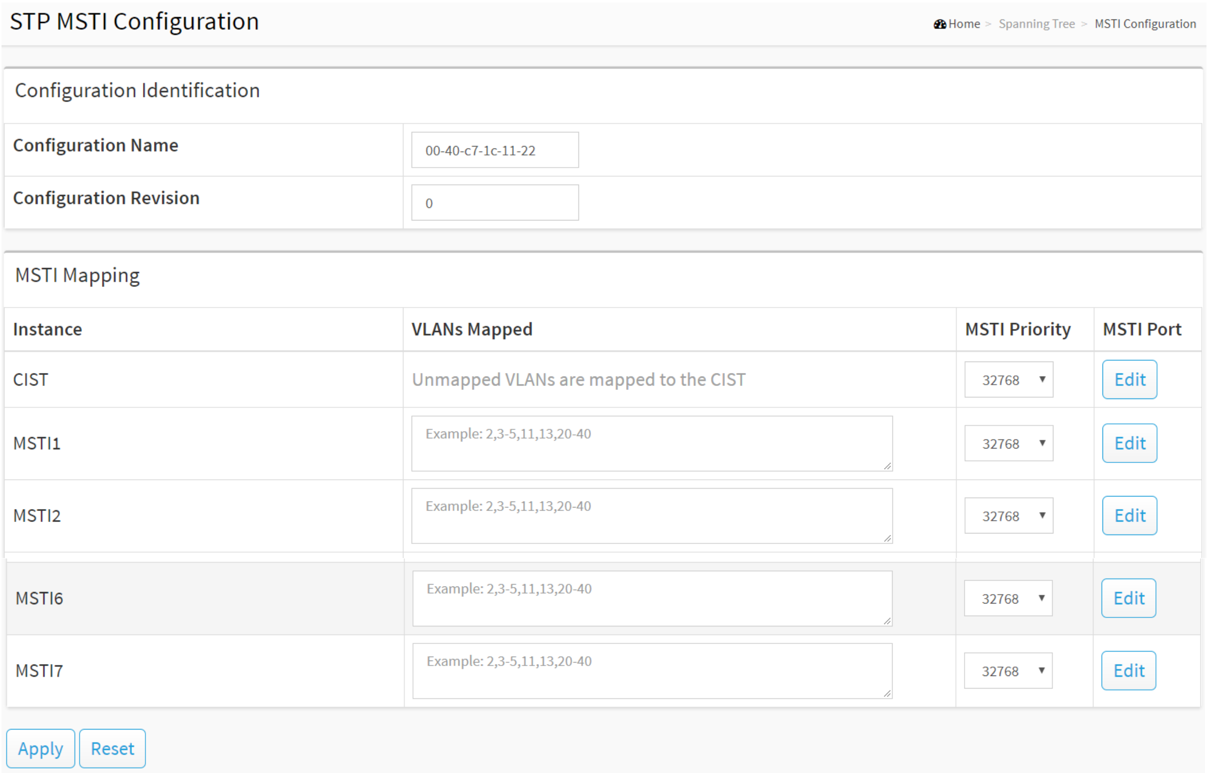
When you implement a Spanning Tree protocol on the switch that the bridge instance. The CIST is not available for explicit mapping, as it will receive the VLANs not explicitly mapped. Due to the reason that you need to set the list of VLANs mapped to the MSTI. The VLANs must be separated with comma and/or space. A VLAN can only be mapped to one MSTI. An unused MSTI should just be left empty. (I.e. not having any VLANs mapped to it.)

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

Web Interface

To configure the Spanning Tree MSTI in the web interface:

1. Click Spanning Tree and MSTI Configuration.
2. Specify the configuration identification parameters in the field. Specify the VLANs Mapped blank field.
3. Click the Apply to save the setting.
4. If you want to cancel the setting then you need to click the Reset button. It will revert to previously saved values.
5. Click Edit to configure the STP CIST Port Configuration.



STP MSTI Configuration

Home > Spanning Tree > MSTI Configuration

Configuration Identification

Configuration Name	00-40-c7-1c-11-22
Configuration Revision	0

MSTI Mapping

Instance	VLANs Mapped	MSTI Priority	MSTI Port
CIST	Unmapped VLANs are mapped to the CIST	32768 ▾	Edit
MSTI1	Example: 2,3-5,11,13,20-40	32768 ▾	Edit
MSTI2	Example: 2,3-5,11,13,20-40	32768 ▾	Edit
MSTI6	Example: 2,3-5,11,13,20-40	32768 ▾	Edit
MSTI7	Example: 2,3-5,11,13,20-40	32768 ▾	Edit

Figure 7-2: The MSTI Configuration

Parameter description:

Configuration Identification

- **Configuration Name :**

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

- **Configuration Revision :**

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

MSTI Mapping

- **Instance :**

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

- **VLANs Mapped :**

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

- **MSTI Priority :**

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

Buttons

- **Apply :**

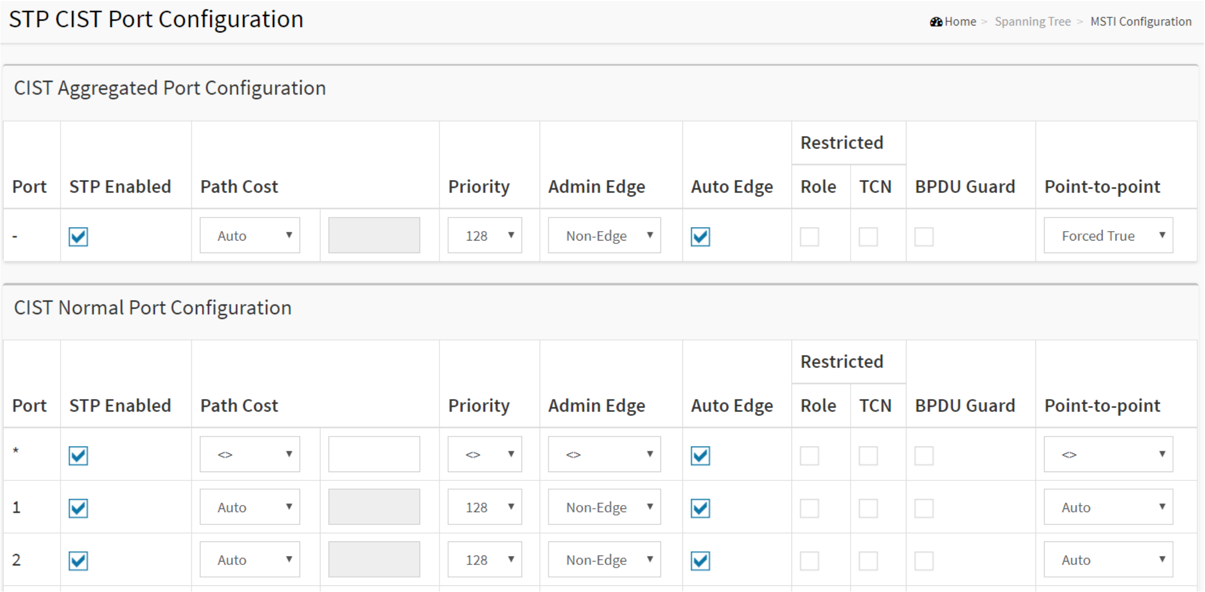
  Click to save changes.

- **Reset :**

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

- **MSTI Port :**

  Click to configure the STP CIST Port Configuration.



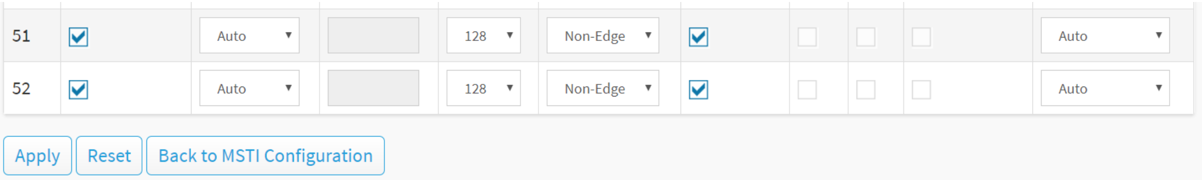
STP CIST Port Configuration

CIST Aggregated Port Configuration

							Restricted			
Port	STP Enabled	Path Cost		Priority	Admin Edge	Auto Edge	Role	TCN	BPDU Guard	Point-to-point
-	☑	Auto ▾		128 ▾	Non-Edge ▾	☑	□	□	□	Forced True ▾

CIST Normal Port Configuration

							Restricted			
Port	STP Enabled	Path Cost		Priority	Admin Edge	Auto Edge	Role	TCN	BPDU Guard	Point-to-point
*	☑	<> ▾		<> ▾	<> ▾	☑	□	□	□	<> ▾
1	☑	Auto ▾		128 ▾	Non-Edge ▾	☑	□	□	□	Auto ▾
2	☑	Auto ▾		128 ▾	Non-Edge ▾	☑	□	□	□	Auto ▾



51	☑	Auto ▾		128 ▾	Non-Edge ▾	☑	□	□	□	Auto ▾
52	☑	Auto ▾		128 ▾	Non-Edge ▾	☑	□	□	□	Auto ▾

Figure 7-2: The STP CIST Port Configuration

Parameter description:

- **Port :**

  The switch port number of the logical STP port.

- **STP Enabled :**

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

- **Path Cost :**

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

- **Priority :**

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

- **AdminEdge :**

  Controls whether the operEdge flag should start as set or cleared. (The initial operEdge state when a port is initialized).

- **AutoEdge :**

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

- **Restricted Role :**

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

- **Restricted TCN :**

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

- **BPDU Guard :**

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

- **Point to Point**

  Controls whether the port connects to a point-to-point LAN rather than to a shared medium. This can be automatically determined, or forced either true or false. Transition to the forwarding state is faster for point-to-point LANs than for shared media.

Buttons

- **Apply :**

  Click to save changes.

- **Reset :**

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

7-3 STP Status

This page provides a status overview of all STP bridge instances.

The displayed table contains a row for each STP bridge instance, where the column displays the following information:

Web Interface

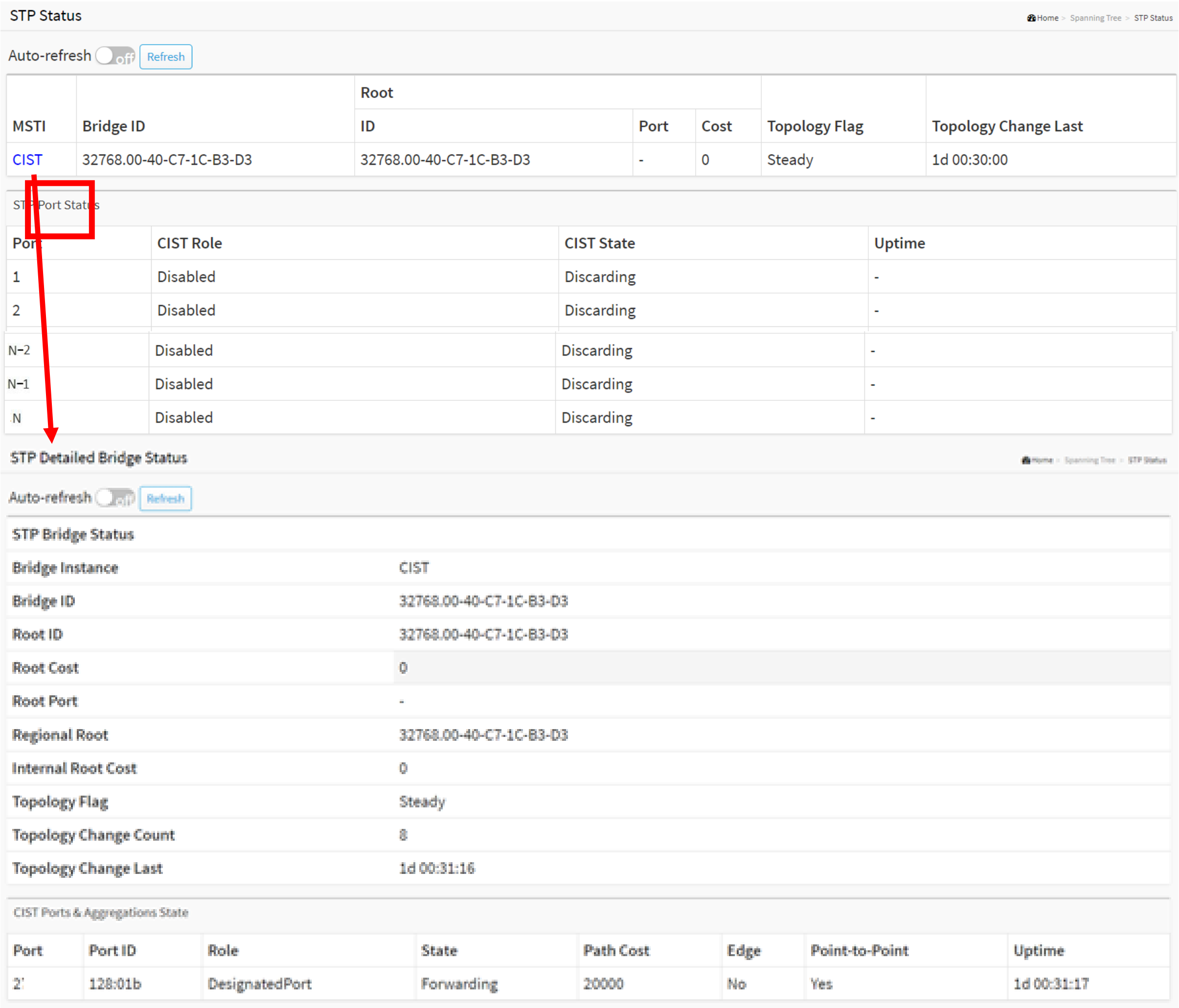
To display the STP Bridges status in the web interface:

Click Spanning Tree and STP Status.

If you want to auto-refresh the information then you need to evoke the “Auto-refresh”.

Click “Refresh” to refresh the STP Bridges.

1. Click “CIST “to next page “STP Detailed Bridge Status”.



STP Status

Home > Spanning Tree > STP Status
Auto-refresh off
Refresh

		Root				
MSTI	Bridge ID	ID	Port	Cost	Topology Flag	Topology Change Last
CIST	32768.00-40-C7-1C-B3-D3	32768.00-40-C7-1C-B3-D3	-	0	Steady	1d 00:30:00

STP Port Status

Port	CIST Role	CIST State	Uptime
1	Disabled	Discarding	-
2	Disabled	Discarding	-
N-2	Disabled	Discarding	-
N-1	Disabled	Discarding	-
N	Disabled	Discarding	-

STP Detailed Bridge Status

Home > Spanning Tree > STP Status
Auto-refresh off
Refresh

STP Bridge Status	
Bridge Instance	CIST
Bridge ID	32768.00-40-C7-1C-B3-D3
Root ID	32768.00-40-C7-1C-B3-D3
Root Cost	0
Root Port	-
Regional Root	32768.00-40-C7-1C-B3-D3
Internal Root Cost	0
Topology Flag	Steady
Topology Change Count	8
Topology Change Last	1d 00:31:16

CIST Ports & Aggregations State

Port	Port ID	Role	State	Path Cost	Edge	Point-to-Point	Uptime
2'	128:01b	DesignatedPort	Forwarding	20000	No	Yes	1d 00:31:17

Figure 7-3: The STP status

Parameter description:

- **MSTI :**

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

- **Bridge ID :**

  The Bridge ID of this Bridge instance.

- **Root ID :**

The Bridge ID of the currently elected root bridge.

- **Root Port :**

  The switch port currently assigned the root port role.

- **Root Cost :**

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

- **Topology Flag :**

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

- **Topology Change Last :**

  The time since last Topology Change occurred.

STP Port Status

- **Port :**

  The switch port number of the logical STP port.

- **CIST Role :**

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

- **CIST State :**

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

- **Uptime :**

  The time since the bridge port was last initialized.

- **CIST :**

  Click to next page "STP Detailed Bridge Status".

STP Bridge Status

- **Bridge Instance :**

  The Bridge instance - CIST, MST1, ...

- **Bridge ID :**

  The Bridge ID of this Bridge instance.

- **Root ID :**

  The Bridge ID of the currently elected root bridge.

- **Root Port :**

  The switch port currently assigned the root port role.

- **Root Cost :**

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

- **Regional Root :**

  The Bridge ID of the currently elected regional root bridge, inside the MSTP region of this bridge. *(For the CIST instance only)*.

- **Internal Root Cost :**

  The Regional Root Path Cost. For the Regional Root Bridge this is zero. For all other CIST instances in the same MSTP region, it is the sum of the Internal Port Path Costs on the least cost path to the Internal Root Bridge. *(For the CIST instance only)*.

- **Topology Flag :**

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

- **Topology Change Count :**

  The number of times where the topology change flag has been set (during a one-second interval).

- **Topology Change Last :**

  The time passed since the Topology Flag was last set.

CIST Ports & Aggregations State

- **Port :**

  The switch port number of the logical STP port.

- **Port ID :**

  The port id as used by the STP protocol. This is the priority part and the logical port index of the bridge port.

- **Role :**

  The current STP port role. The port role can be one of the following **values:** AlternatePortBackupPort RootPort DesignatedPort.

- **State :**

  The current STP port state. The port state can be one of the following **values:** DiscardingLearning Forwarding.

- **Path Cost :**

  The current STP port path cost. This will either be a value computed from the Auto setting, or any explicitly configured value.

- **Edge :**

  The current STP port (operational) Edge Flag. An Edge Port is a switch port to which no Bridges are attached. The flag may be automatically computed or explicitly configured. Each Edge Port transits directly to the Forwarding Port State, since there is no possibility of it participating in a loop.

- **Point-to-Point :**

  The current STP port point-to-point flag. A point-to-point port connects to a non-shared LAN media. The flag may be automatically computed or explicitly configured. The point-to-point properties of a port affect how fast it can transit to STP state.

- **Uptime :**

  The time since the bridge port was last initialized.

Buttons

Figure 7-3: The STP status buttons

- **Auto-refresh :**

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

- **Refresh :**

  Click to refresh the page.

7-4 Port Statistics

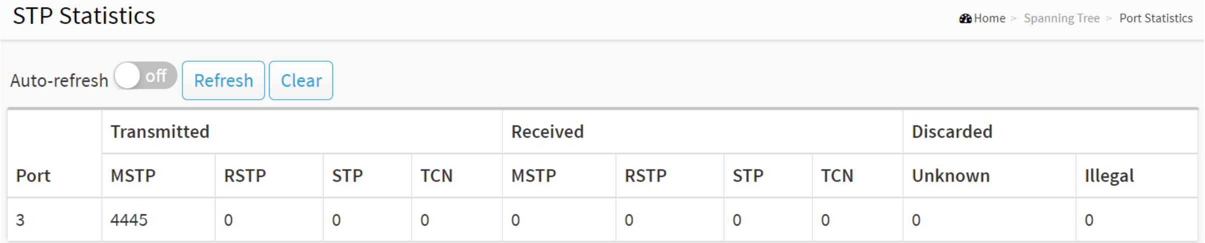
This page displays the STP port statistics counters of bridge ports in the switch.

Web Interface

To display the STP Port Statistic in the web interface:

Click Spanning Tree and Port Statistics.
If you want to auto-refresh the information then you need to evoke the “Auto-refresh”.

1. Click “Refresh” to refresh the STP Bridges.



STP Statistics

	Transmitted				Received				Discarded	
Port	MSTP	RSTP	STP	TCN	MSTP	RSTP	STP	TCN	Unknown	Illegal
3	4445	0	0	0	0	0	0	0	0	0

Figure 7-4: The STP Port Statistics

Parameter description:

- **Port :**

  The switch port number of the logical STP port.

- **MSTP :**

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

- **RSTP :**

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

- **STP :**

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

- **TCN :**

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

- **Discarded Unknown :**

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

- **Discarded Illegal :**

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

Buttons

Figure 7-4: The STP Port Statistics buttons

- **Auto-refresh :**

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

- **Refresh :**

Chapter 8 MAC Address Tables

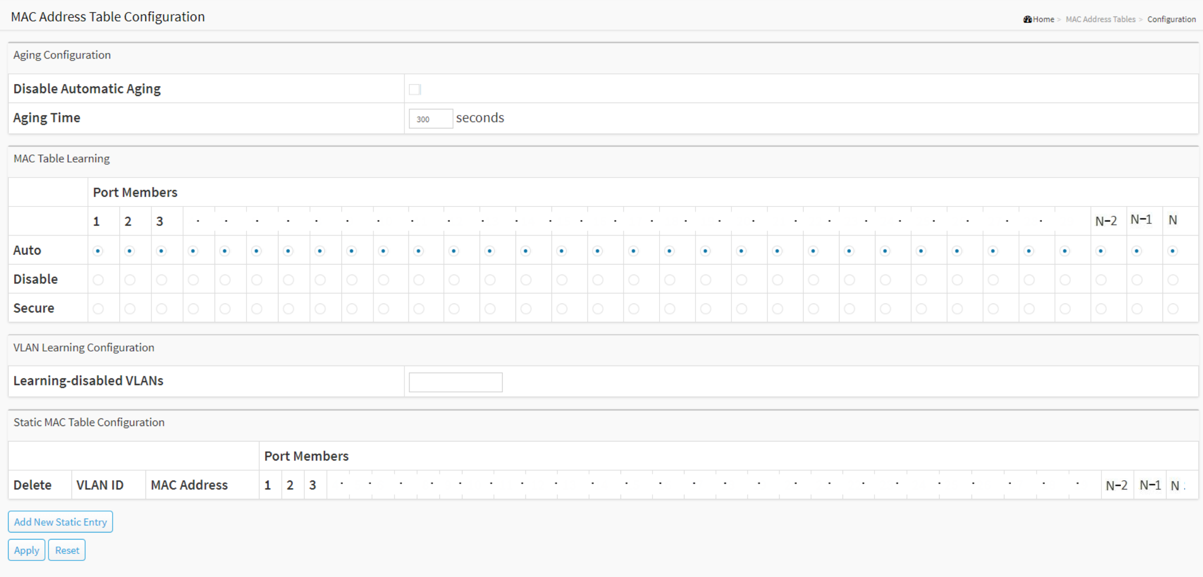
8-1 Configuration

Switching of frames is based upon the DMAC address contained in the frame. The switch builds up a table that maps MAC addresses to switch ports for knowing which ports the frames should go to (based upon the DMAC address in the frame). This table contains both static and dynamic entries. The static entries are configured by the network administrator if the administrator wants to do a fixed mapping between the DMAC address and switch ports.
The frames also contain a MAC address (SMAC address), which shows the MAC address of the equipment sending the frame. The SMAC address is used by the switch to automatically update the MAC table with these dynamic MAC addresses. Dynamic entries are removed from the MAC table if no frame with the corresponding SMAC address have been seen after a configurable age time

Web Interface

To configure MAC Address Table in the web interface:

1. Click MAC Address Tables and Configuration.
2. Specify the Disable Automatic Aging and Aging Time.
3. Specify the Port Members (Auto, Disable, Secure).
4. Specify the Learning-disabled VLANs.
5. Add new Static entry, Specify the VLAN IP and Mac address, Port Members.
6. Click Apply.



MAC Address Table Configuration

Aging Configuration

Disable Automatic Aging	□
Aging Time	300 seconds

MAC Table Learning

	Port Members																															
	1	2	3	·	·	·	·	·	·	·	·	·	·	·	·	·	·	·	·	·	·	·	·	·	·	·	·	·	N-2	N-1	N
Auto	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●
Disable	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○
Secure	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○

VLAN Learning Configuration

Learning-disabled VLANs	

Static MAC Table Configuration

			Port Members																											
Delete	VLAN ID	MAC Address	1	2	3	·	·	·	·	·	·	·	·	·	·	·	·	·	·	·	·	·	·	·	·	·	·	N-2	N-1	N

Figure 8-1: The MAC Address Table Configuration

Parameter description:

Aging Configuration :

By default, dynamic entries are removed from the MAC table after 300 seconds. This removal is also called aging.

Configure aging time by entering a value here in seconds; for example, Age time seconds.

The allowed range is 10 to 1000000 seconds.

Disable the automatic aging of dynamic entries by checking ☑ Disable automatic aging.

MAC Table Learning :

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

- **Auto :**

  Learning is done automatically as soon as a frame with unknown SMAC is received.

- **Disable :**

  No learning is done.

- **Secure :**

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

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

VLAN Learning Configuration

- **Learning-disabled VLANS :**

  This field shows the Learning-disabled VLANs. When a NEW MAC arrives into a learning-disabled VLAN, the MAC won't be learnt. By the default, the field is empty. More VLANs may be created by using a list syntax where the individual elements are separated by commas. Ranges are specified with a dash separating the lower and upper bound. The following example will create VLANs 1, 10, 11, 12, 13, 200, and 300: 1,10-13,200,300. Spaces are allowed in between the delimiters.

Static MAC Table Configuration

The static entries in the MAC table are shown in this table. The static MAC table can contain 128 entries. The maximum of 128 entries is for the whole stack, and not per switch.

- **VLAN ID :**

  The VLAN ID of the entry.

- **MAC Address :**

  The MAC address of the entry.

- **Port Members :**

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

Buttons

- **Add a New Static Entry :**

  Click to add a new entry to the static MAC table. Specify the VLAN ID, MAC address, and port members for the new entry. Click "Apply".

- **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.

8-2 Information

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

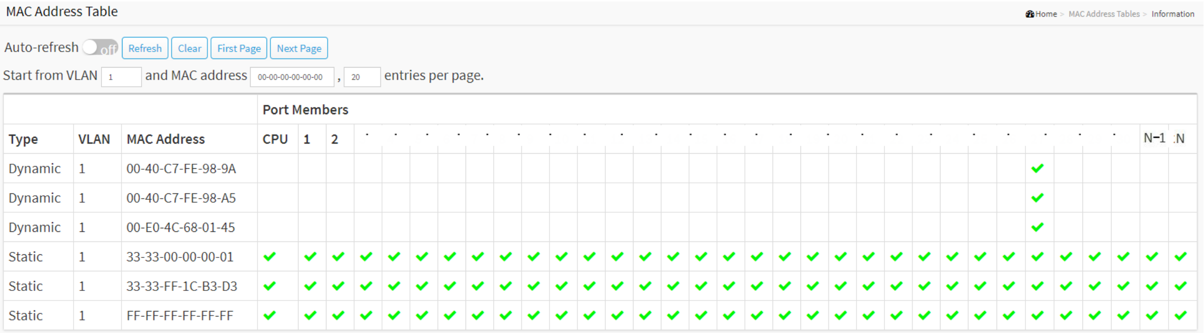
Web Interface

To Display MAC Address Table in the web interface:

1. Click MAC Address Table and Information.

If you want to auto-refresh the information then you need to evoke the “Auto-refresh”.

2. Click “Refresh” to refresh the MAC Address Table.



MAC Address Table

Start from VLAN 1 and MAC address 00-00-00-00-00-00 , 20 entries per page.

			Port Members																																
Type	VLAN	MAC Address	CPU	1	2	·	·	·	·	·	·		·	·	·	·		·	·	·	·		·	·	·	·		·	·	·	·		·	N−1	N
Dynamic	1	00-40-C7-FE-98-9A																										✓					
Dynamic	1	00-40-C7-FE-98-A5																										✓					
Dynamic	1	00-E0-4C-68-01-45																										✓					
Static	1	33-33-00-00-00-01	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Static	1	33-33-FF-1C-B3-D3	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Static	1	FF-FF-FF-FF-FF-FF	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓

Figure 8-2: The MAC Address Table Information

Parameter description:

Navigating the MAC Table

Each page shows up to 999 entries from the MAC table, default being 10, selected through the "entries per page" input field. When first visited, the web page will show the first 10 entries from the beginning of the MAC Table. The first displayed will be the one with the lowest VLAN ID and the lowest MAC address found in the MAC Table.

- **Type :**

  Indicates whether the entry is a static or a dynamic entry, 802.1x, DMS.

- **VLAN :**

  The VLAN ID of the entry.

- **MAC address :**

  The MAC address of the entry.

- **Port Members :**

  The ports that are members of the entry.

Buttons

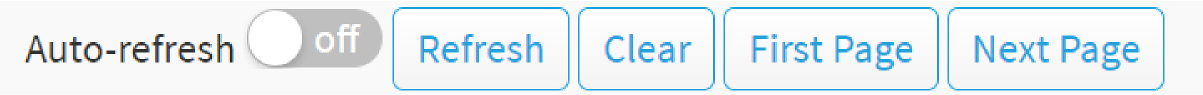


Figure 8-2: The MAC Address Table Information buttons

- **Auto-refresh :**

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

- **Refresh :**

Click to refresh the page.

- **Clear :**

  Click to clear the page.

- **First Page :**

  Updates the system log entries, turn to the first page.

- **Next Page :**

  Updates the system log entries, turn to the next page.

NOTE:
00-40-C7-73-01-29 : your switch MAC address (for IPv4)
33-33-00-00-00-01 : Destination MAC (for IPv6 Router Advertisement) (reference IPv6 RA.JPG)
33-33-00-00-00-02 : Destination MAC (for IPv6 Router Solicitation) (reference IPv6 RS.JPG)
33-33-FF-73-01-29 : Destination MAC (for IPv6 Neighbor Solicitation) (reference IPv6 DAD.JPG)
33-33-FF-A8-01-01: your switch MAC address (for IPv6 global IP)
FF-FF-FF-FF-FF-FF: for Broadcast.

Chapter 9 Multicast

9-1 IGMP Snooping

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

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

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

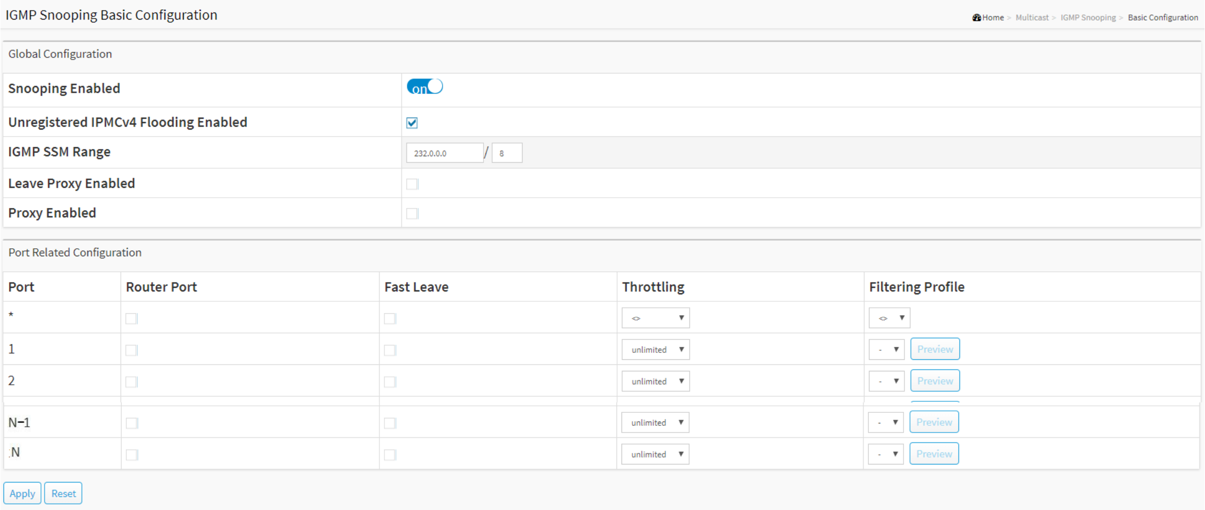
9-1.1 Basic Configuration

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

Web Interface

To configure the IGMP Snooping parameters in the web interface:

1. Click Multicast, IGMP Snooping and Basic Configuration.
2. Evoke to select enable or disable which Global configuration
3. Evoke which port wants to become a Router Port or enable/ disable the Fast Leave function.
4. Scroll to set the Throtting and Profile.
5. Click the Apply to save the setting.
6. If you want to cancel the setting then you need to click the Reset button. It will revert to previously saved values.



IGMP Snooping Basic Configuration

Global Configuration

Snooping Enabled	on
Unregistered IPMCv4 Flooding Enabled	☑
IGMP SSM Range	232.0.0.0 / 8
Leave Proxy Enabled	□
Proxy Enabled	□

Port Related Configuration

Port	Router Port	Fast Leave	Throttling	Filtering Profile
*	□	□	<> ▾	<> ▾
1	□	□	unlimited ▾	- ▾ Preview
2	□	□	unlimited ▾	- ▾ Preview
N-1	□	□	unlimited ▾	- ▾ Preview
N	□	□	unlimited ▾	- ▾ Preview

Figure 9-1.1: The IGMP Snooping Configuration

Parameter description:

Global Configuration

- **Snooping Enabled :**

  Enable the Global IGMP Snooping.

- **Unregistered IPMCv4 Flooding enabled :**

  Enable unregistered IPMCv4 traffic flooding. Unregistered IPMCv4 traffic is so-called unknown multicast.

  After selected, the unregistered multicast stream will be forwarded like normal packets. Once you un-selected it, such stream will be discarded

- **IGMP SSM Range :**

  SSM (Source-Specific Multicast) Range allows the SSM-aware hosts and routers run the SSM service model for the groups in the address range. Format: (IP address/ sub mask)

- **Leave Proxy Enabled**

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

- **Proxy Enabled :**

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

Port Related Configuration

- **Port :**

  It shows the physical Port index of switch.

- **Router Port :**

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

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

- **Fast Leave :**

  Enable the fast leave on the port.

- **Throttling :**

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

- **Profile :**

  Select the profile for this port. Click to preview the page which list the rules associated with the selected profile.

Buttons

- **Apply :**

  Click to save changes.

- **Reset :**

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

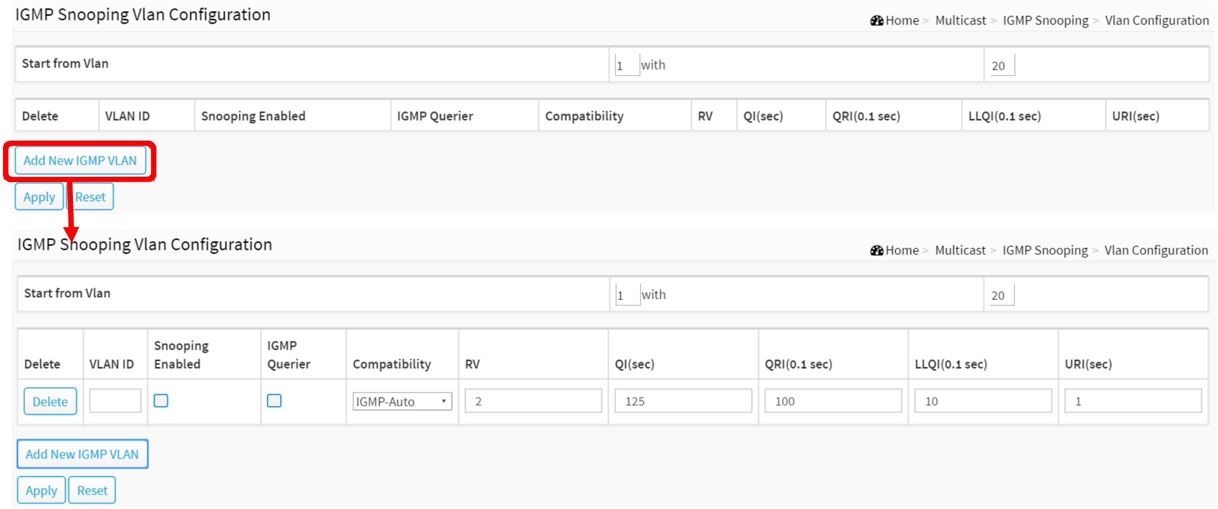
9-1.2 VLAN Configuration

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

Web Interface

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

1. Click Multicast, IGMP Snooping and VLAN Configuration.
2. Click to add new IGMP VLAN.
3. Click the Apply to save the setting
4. If you want to cancel the setting then you need to click the Reset button. It will revert to previously saved values


IGMP Snooping Vlan Configuration
Home > Multicast > IGMP Snooping > Vlan Configuration
Add New IGMP VLAN
Apply
Reset
IGMP Snooping Vlan Configuration
Home > Multicast > IGMP Snooping > Vlan Configuration
Delete
Add New IGMP VLAN
Apply
Reset

Start from Vlan	1	with	20

Delete	VLAN ID	Snooping Enabled	IGMP Querier	Compatibility	RV	QI(sec)	QRI(0.1 sec)	LLQI(0.1 sec)	URI(sec)

Start from Vlan	1	with	20

Delete	VLAN ID	Snooping Enabled	IGMP Querier	Compatibility	RV	QI(sec)	QRI(0.1 sec)	LLQI(0.1 sec)	URI(sec)
Delete		□	□	IGMP-Auto	2	125	100	10	1

Figure 9-1.2: The IGMP Snooping VLAN Configuration

Parameter description:

- **Start from Vlan :**

  You can click them Refreshes the displayed table starting from the "VLAN" input fields.

- **Delete :**

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

- **VLAN ID :**

  It displays the VLAN ID of the entry.

- **Snooping Enabled :**

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

- **IGMP Querier :**

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

- **Compatibility :**

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

- **Rv :**

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

- **QI(sec) :**

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

- **QRI(0.1 sec) :**

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

- **LLQI (0.1 sec) :**

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

- **URI(sec) :**

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

Buttons

- **Apply :**

  Click to save changes.

- **Reset :**

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

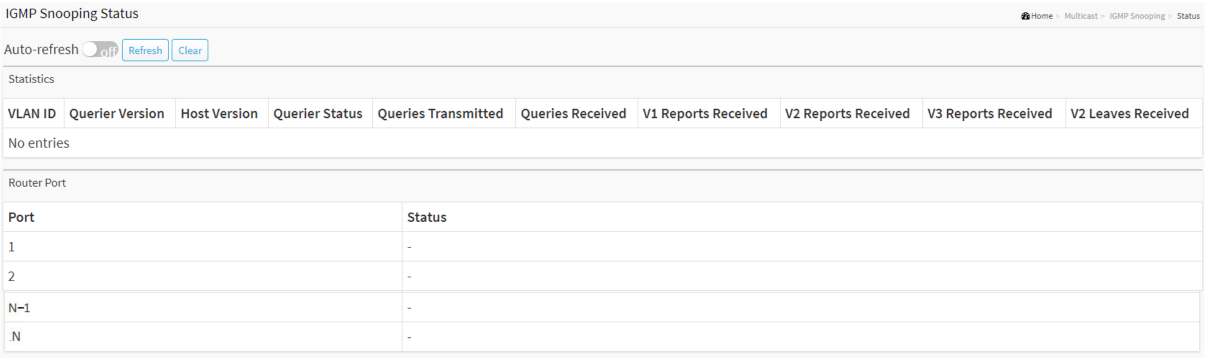
9-1.3 Status

After you complete the IGMP Snooping configuration, then you could to let the switch display the IGMP Snooping Status. The Section provides you to let switch to display the IGMP Snooping detail status.

Web Interface

To display the IGMP Snooping status in the web interface:

1. Click Multicast, IGMP Snooping and Status.
2. If you want to auto-refresh the information then you need to evoke the “Auto-refresh”.
3. Click “Refresh” to refresh the IGMP Snooping Status.



IGMP Snooping Status

Statistics

VLAN ID	Querier Version	Host Version	Querier Status	Queries Transmitted	Queries Received	V1 Reports Received	V2 Reports Received	V3 Reports Received	V2 Leaves Received
No entries									

Router Port

Port	Status
1	-
2	-
N−1	-
.N	-

Figure 9-1.3: The IGMP Snooping Status

Parameter description:

Statistic

- **VLAN ID :**

  The VLAN ID of the entry.

- **Querier Version :**

  Working Querier Version currently.

- **Host Version :**

  Working Host Version currently.

- **Querier Status :**

  Shows the Querier status is "ACTIVE" or "IDLE".

  "DISABLE" denotes the specific interface is administratively disabled.

- **Queries Transmitted :**

  The number of Transmitted Queries.

- **Queries Received :**

  The number of Received Queries.

- **V1 Reports Received :**

  The number of Received V1 Reports.

- **V2 Reports Received :**

  The number of Received V2 Reports.

- **V3 Reports Received :**

  The number of Received V3 Reports.

- **V2 Leaves Received :**

  The number of Received V2 Leaves.

Router Port

Display which ports act as router ports. A router port is a port on the Ethernet switch that leads towards the Layer 3 multicast device or IGMP querier. Static denotes the specific port is configured to be a router port. Dynamic denotes the specific port is learnt to be a router port. Both denote the specific port is configured or learnt to be a router port.

- **Port :**

  Switch port number.

- **Status :**

  Indicate whether specific port is a router port or not.

Buttons

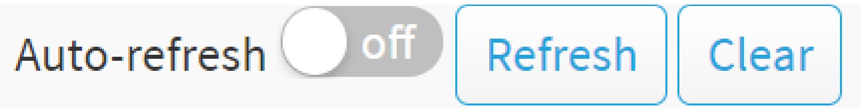


Figure 9-1.3: The IGMP Snooping Status buttons

- **Auto-refresh :**

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

- **Refresh :**

  Click to refresh the page immediately.

- **Clear :**

  Click to clear the page.

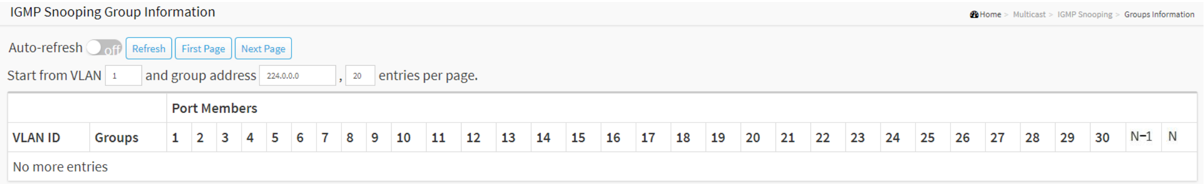
9-1.4 Group Information

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

Web Interface

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

1. Click Multicast, IGMP Snooping and Group Information.
2. Specify how many entries to show in one page.
3. If you want to auto-refresh the information then you need to evoke the “Auto-refresh”.
4. Click “Refresh” to refresh an entry of the IGMP Snooping Groups Information.
5. Click First/Next Page to change page.


IGMP Snooping Group Information
Home > Multicast > IGMP Snooping > Groups Information
Auto-refresh
off
Refresh
First Page
Next Page

Start from VLAN 1 and group address 224.0.0.0 , 20 entries per page.

		Port Members																															
VLAN ID	Groups	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	N−1	N
No more entries																																	

Figure 9-1.4: The IGMP Snooping Groups Information

Parameter description:

Navigating the IGMP Group Table

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

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

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

- **Show entries :**

  You can choose how many items you want to show up.

- **VLAN ID :**

  VLAN ID of the group.

- **Groups :**

  Group address of the group displayed.

- **Port Members :**

  Ports under this group.

Buttons

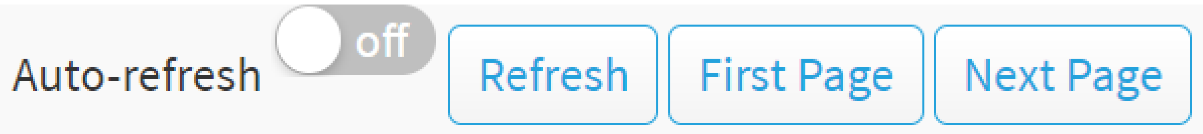


Figure 9-1.4: The IGMP Snooping Groups Information buttons

- **Auto-refresh :**

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

- **Refresh :**

  Click to refresh the page immediately.

- **First Page :**

  Updates the system log entries, turn to the first page.

- **Next Page :**

  Updates the group information entries, turn to the next page.

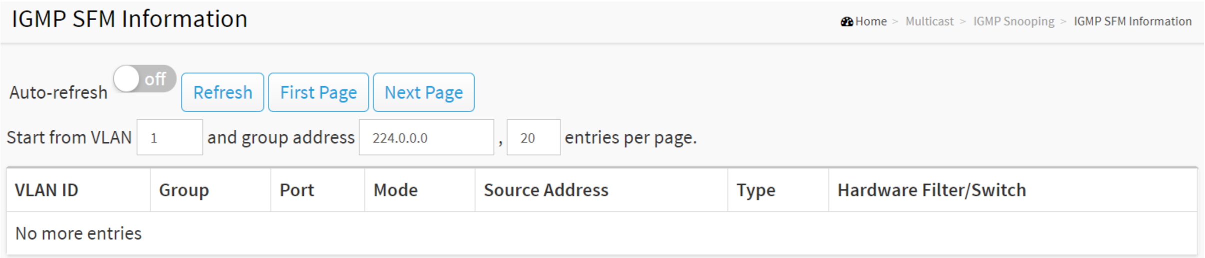
9-1.5 IGMP SFM Information

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

Web Interface

To display the IGMP SFM Information in the web interface:

1. Click Multicast, IGMP Snooping and IGMP SFM Information
2. If you want to auto-refresh the information then you need to evoke the "Auto-refresh".
3. Click "Refresh" to refresh an entry of the IGMP Snooping Groups Information.
4. Click First/Next Page to change page.



IGMP SFM Information

Auto-refresh off

Start from VLAN 1 and group address 224.0.0.0 , 20 entries per page.

VLAN ID	Group	Port	Mode	Source Address	Type	Hardware Filter/Switch
No more entries						

Figure 9-1.5: The IGMP SFM Information

Parameter description:

Navigating the IGMP SFM Information Table

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

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

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

- **Show entries :**

  You can choose how many items you want to show up.

- **VLAN ID :**

  VLAN ID of the group.

- **Group :**

  Group address of the group displayed.

- **Port :**

  Switch port number.

- **Mode :**

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

- **Source Address :**

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

- **Type :**

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

- **Hardware Filter/Switch :**

  Indicates whether data plane destined to the specific group address from the source IPv4 address could be handled by chip or not.

Buttons

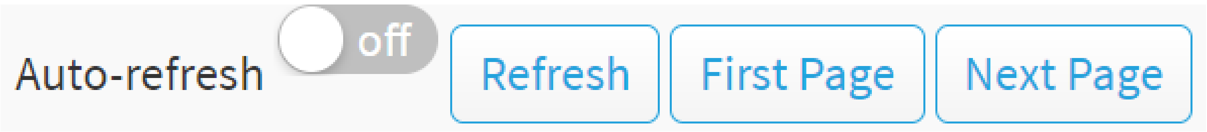


Figure 9-1.5: The IGMP Snooping Groups Information buttons

- **Auto-refresh :**

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

- **Refresh :**

  Click to refresh the page immediately.

- **First Page :**

  Updates the system log entries, turn to the first page.

- **Next Page :**

  Updates the group information entries, turn to the next page.

9-2 MLD Snooping

Curiously enough, a network node that acts as a source of IPv6 multicast traffic is only an indirect participant in MLD snooping—it just provides multicast traffic, and MLD doesn't interact with it. (Note, however, that in an application like desktop conferencing a network node may act as both a source and an MLD host; but MLD interacts with that node only in its role as an MLD host.)

A source node creates multicast traffic by sending packets to a multicast address. In IPv6, addresses with the first eight bits set (that is, "FF" as the first two characters of the address) are multicast addresses, and any node that listens to such an address will receive the traffic sent to that address. Application software running on the source and destination systems cooperates to determine what multicast address to use. (Note that this is a function of the application software, not of MLD.)

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

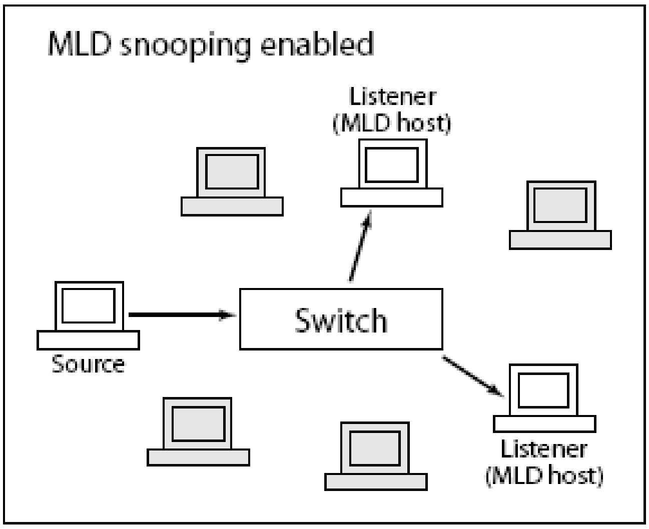


Figure 9-2: The MLD snooping enable

9-2.1 Basic Configuration

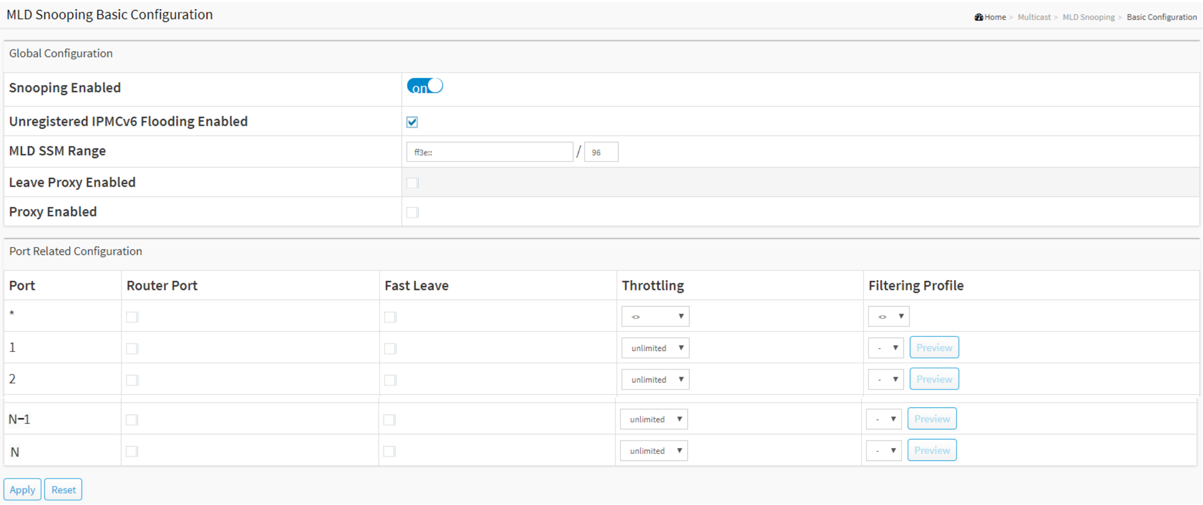
The section will let you understand how to configure the MLD Snooping basic configuration and the parameters.

Web Interface

To configure the MLD Snooping Configuration in the web interface:

1. Click Multicast, MLD Snooping and Basic Configuration.
2. Evoke to on or off the Global configuration parameters.
3. Evoke the port to join Router port and Fast Leave.
4. Scroll to select the Throtting mode with unlimited or 1 to 10.
5. Scroll to set the Profile.
6. Click the apply to save the setting.

7. If you want to cancel the setting then you need to click the Reset button. It will revert to previously saved values.



MLD Snooping Basic Configuration

Home > Multicast > MLD Snooping > Basic Configuration

Global Configuration

Snooping Enabled	on
Unregistered IPMCv6 Flooding Enabled	☑
MLD SSM Range	ff3e:: / 96
Leave Proxy Enabled	□
Proxy Enabled	□

Port Related Configuration

Port	Router Port	Fast Leave	Throttling	Filtering Profile
*	□	□	<> ▾	<> ▾
1	□	□	unlimited ▾	- ▾ Preview
2	□	□	unlimited ▾	- ▾ Preview
N-1	□	□	unlimited ▾	- ▾ Preview
N	□	□	unlimited ▾	- ▾ Preview

Figure 9-2.1: The MLD Snooping Basic Configuration

Parameter description :

Global Configuration

- **Snooping Enabled :**

  Enable the Global MLD Snooping.

- **Unregistered IPMCv6 Flooding enabled :**

  Enable unregistered IPMCv6 traffic flooding.

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

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

- **MLD SSM Range :**

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

- **Leave Proxy Enabled :**

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

- **Proxy Enabled :**

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

Port Related Configuration

- **Router Port :**

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

- **Fast Leave :**

  To evoke to enable the fast leave on the port.

- **Throttling :**

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

- **Filtering Profile :**

  You can select profile when you edit in Multicast Filtering Profile.

Buttons

- **Apply :**

  Click to save changes.

- **Reset :**

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

9-2.2 VLAN Configuration

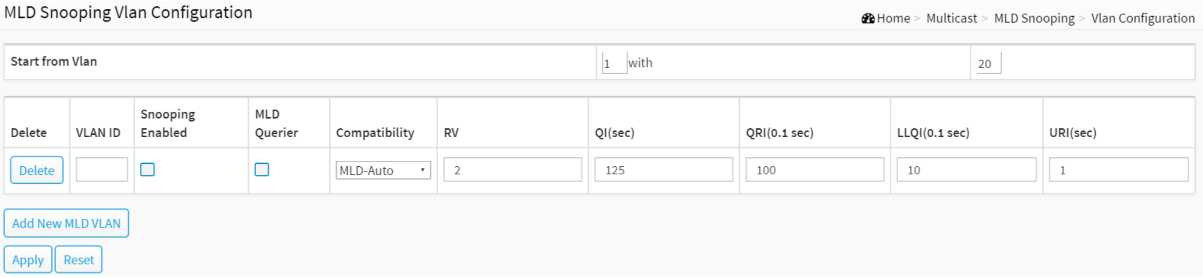
When MLD snooping is enabled on a VLAN, the switch acts to minimize unnecessary multicast traffic. If the switch receives multicast traffic destined for a given multicast address, it forwards that traffic only to ports on the VLAN that have MLD hosts for that address. It drops that traffic for ports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

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

Web Interface

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

1. Click Multicast, MLD Snooping and VLAN Configuration.
2. Click Add New MLD VLAN.
3. Specify the VLAN ID with entries per page.



MLD Snooping Vlan Configuration

Home > Multicast > MLD Snooping > Vlan Configuration

Start from Vlan	1	with	20

Delete	VLAN ID	Snooping Enabled	MLD Querier	Compatibility	RV	QI(sec)	QRI(0.1 sec)	LLQI(0.1 sec)	URI(sec)
Delete		□	□	MLD-Auto	2	125	100	10	1

Figure 9-2.2: The MLD Snooping VLAN Configuration

Parameter description:

- **Delete :**

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

- **VLAN ID :**

  It displays the VLAN ID of the entry.

- **Snooping Enabled :**

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

- **MLD Querier:**

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

- **Compatibility :**

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

- **RV :**

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

- **QI(sec) :**

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

- **QRI(0.1sec) :**

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

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

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

- **URI(sec) :**

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

Buttons

- **Apply :**

  Click to save changes.

- **Reset :**

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

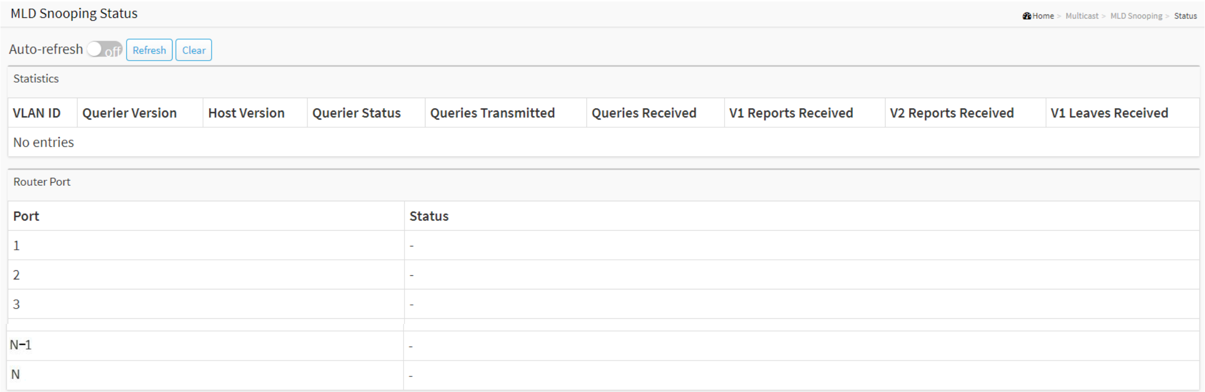
9-2.3 Status

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

Web Interface

To display the MLD Snooping Status in the web interface:

1. Click Multicast, MLD Snooping and Status.
2. If you want to auto-refresh the information then you need to evoke the "Auto-refresh"
3. Click "Refresh" to refresh an entry of the MLD Snooping Status Information.



MLD Snooping Status

Statistics

VLAN ID	Querier Version	Host Version	Querier Status	Queries Transmitted	Queries Received	V1 Reports Received	V2 Reports Received	V1 Leaves Received
No entries								

Router Port

Port	Status
1	-
2	-
3	-
N-1	-
N	-

Figure 9-2.3: The MLD Snooping Status

Parameter description:

- **VLAN ID :**

  The VLAN ID of the entry.

- **Querier Version :**

  Working Querier Version currently.

- **Host Version :**

  Working Host Version currently.

- **Querier Status :**

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

  "DISABLE" denotes the specific interface is administratively disabled.

- **Queries Transmitted :**

  The number of Transmitted Queries.

- **Queries Received :**

  The number of Received Queries.

- **V1 Reports Received :**

  The number of Received V1 Reports.

- **V2 Reports Received :**

  The number of Received V2 Reports.

- **V1 Leaves Received :**

  The number of Received V1 Leaves.

Router Port

Display which ports act as router ports. A router port is a port on the Ethernet switch that leads towards the Layer 3 multicast device or MLD querier.
Static denotes the specific port is configured to be a router port.
Dynamic denotes the specific port is learnt to be a router port.
Both denote the specific port is configured or learnt to be a router port.

- **Port :**

  Switch port number.

- **Status :**

  Indicate whether specific port is a router port or not.

Buttons

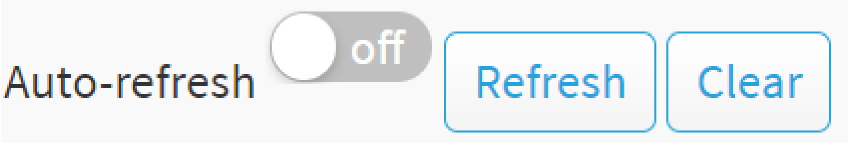


Figure 9-2.3: The MLD Snooping Status buttons

- **Auto-refresh :**

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

- **Refresh :**

  Click to refresh the page immediately.

- **Clear :**

  Clears the counters for the selected port.

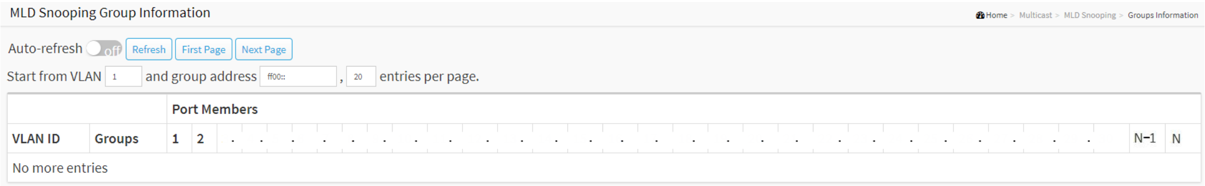
9-2.4 Groups Information

Entries in the MLD Group Table are shown on this page. The MLD Group Table is sorted first by VLAN ID, and then by group.

Web Interface

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

1. Click Multicast, MLD Snooping and Group Information.
2. If you want to auto-refresh the information then you need to evoke the “Auto-refresh”
3. Click “Refresh” to refresh an entry of the MLD Snooping Group Information.
4. Click First/Next Page to change page.



MLD Snooping Group Information

Start from VLAN 1 and group address ff00:: , 20 entries per page.

		Port Members				
VLAN ID	Groups	1	2	. . .	N−1	N
No more entries						

Figure 9-2.4: The MLD Snooping Groups Information

Parameter description:

Navigating the MLD Group Table

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

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

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

- **VLAN ID :**

  VLAN ID of the group.

- **Groups :**

  Group address of the group displayed.

- **Port Members :**

  Ports under this group.

- **Show entries :**

  You can choose how many items you want to show up.

Buttons

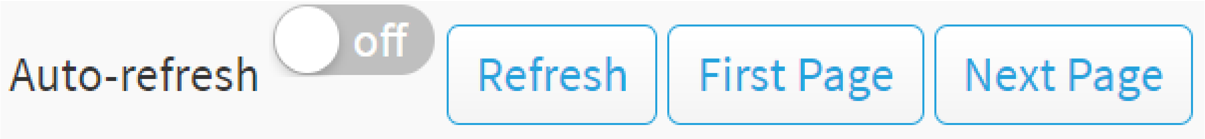


Figure 9-2.4: The MLD Snooping Groups Information buttons

- **Auto-refresh :**

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

- **Refresh :**

  Click to refresh the page immediately.

- **First Page :**
  Updates the system log entries, turn to the first page.

- **Next Page :**

  Updates the group information entries, turn to the next page.

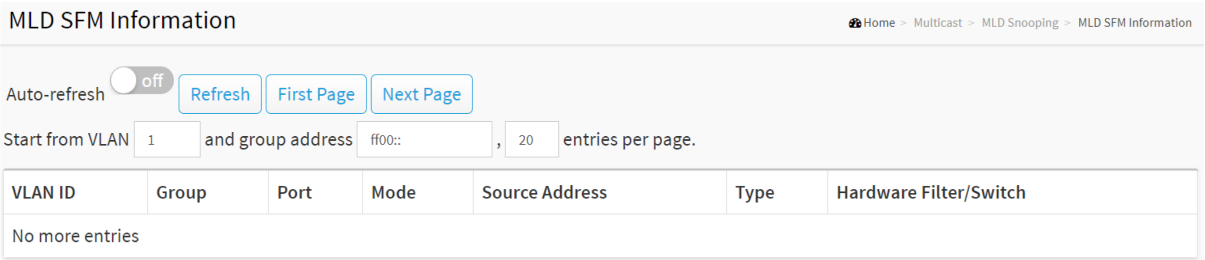
9-2.5 MLD SFM Information

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

Web Interface

To display the MLD SFM Information in the web interface:

1. Click Multicast, MLD Snooping and MLD SFM Information.
2. If you want to auto-refresh the information then you need to evoke the “Auto-refresh”.
3. Click “Refresh” to refresh an entry of the MLD SFM Information.
4. Click First/Next Page to change page.



MLD SFM Information

Home > Multicast > MLD Snooping > MLD SFM Information

Start from VLAN 1 and group address ff00:: , 20 entries per page.

VLAN ID	Group	Port	Mode	Source Address	Type	Hardware Filter/Switch
No more entries						

Figure 9-2.5: The MLD SFM Information

Parameter description:

Navigating the MLD SFM Information Table

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

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

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

- **VLAN ID :**

  VLAN ID of the group.

- **Group :**

  IP Multicast Group address.

- **Port :**

  Switch port number.

- **Mode :**

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

- **Source Address :**

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

- **Type :**

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

- **Hardware Filter/Switch :**

  Indicates whether data plane destined to the specific group address from the source IPv6 address could be handled by chip or not.

Buttons

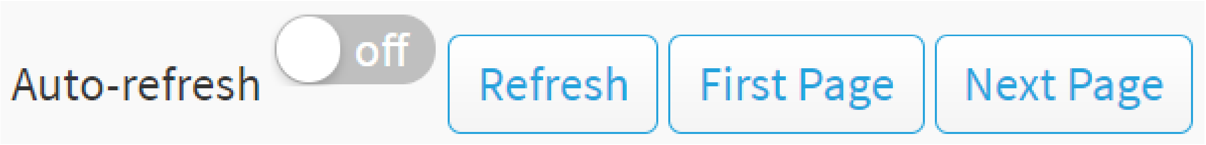


Figure 9-2.5: The MLD SFM Information buttons

- **Auto-refresh :**

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

- **Refresh :**

  Click to refresh the page immediately.

- **First Page :**
  Updates the system log entries, turn to the first page.

- **Next Page :**

  Updates the group information entries, turn to the next page.

9-3 MVR

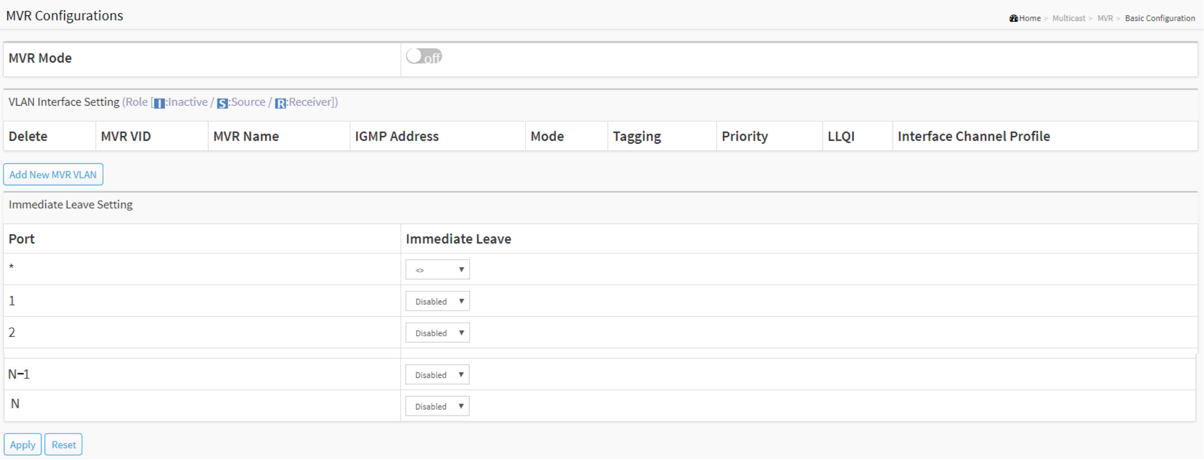
The MVR feature enables multicast traffic forwarding on the Multicast VLAN. In a multicast television application, a PC or a television with a set-top box can receive the multicast stream. Multiple set-top boxes or PCs can be connected to one subscriber port, which is a switch port configured as an MVR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

9-3.1 Basic Configuration

Web Interface

To configure the MVR Configuration in the web interface:

1. Click Multicast, MVR and Basic Configuration.
2. Scroll the MVR mode to enable or disable and Scroll to set all parameters.
3. Click “Add New MVR VLAN”.
4. Specify MVR VID, MVR Name, IGMP Address, Mode, Tagging, Priority, LLQI, Interface Channel Profile.
5. Select which port to Click Immediate Leave.
6. Click the apply to save the setting
7. If you want to cancel the setting then you need to click the Reset button. It will revert to previously saved values



MVR Configurations

MVR Mode	off

VLAN Interface Setting (Role [I:Inactive / S:Source / R:Receiver])

Delete	MVR VID	MVR Name	IGMP Address	Mode	Tagging	Priority	LLQI	Interface Channel Profile

Immediate Leave Setting

Port	Immediate Leave
*	<>
1	Disabled
2	Disabled
N-1	Disabled
N	Disabled

Figure 9-3.1: The MVR Configuration

Parameter description:

- **MVR Mode :**

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

- **MVR VID :**

  Specify the Multicast VLAN ID.

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

- **MVR Name :**

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

- **IGMP Address :**

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

  The default IGMP address is not set (0.0.0.0).

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

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

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

- **Mode :**

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

- **Tagging :**

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

- **Priority :**

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

- **LLQI :**

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

- **Interface Channel Profile :**

  When the MVR VLAN is created, select the profile to expand the corresponding multicast channel settings for the specific MVR VLAN. The file established on Filtering Profile Table.

- **Port :**

  The logical port for the settings.

- **Port Role :**

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

  Inactive: The designated port does not participate MVR operations.

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

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

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

- **Immediate Leave :**

  Enable the fast leave on the port.

Buttons

- **Add New MVR VLAN :**

  Click to add new mvr vlan. Specify MVR VID, MVR Name, IGMP Address, Mode, Tagging, Priority, LLQI, Interface Channel Profile. Click "Apply"

- **Delete :**

  Check to delete the entry. The designated entry 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.

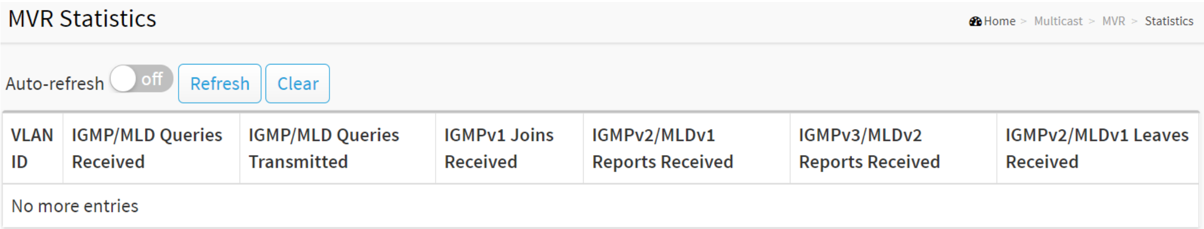
9-3.2 Statistics

The section describes the switch will display the MVR detail Statistics after you had configured MVR on the switch. It provides the detail MVR Statistics Information

Web Interface

To display the MVR Statistics Information in the web interface:

1. Click Multicast, MVR and Statistics.
2. If you want to auto-refresh the information then you need to evoke the “Auto-refresh”.
3. To click the “Refresh” to refresh an entry of the MVR Statistics Information.



VLAN ID	IGMP/MLD Queries Received	IGMP/MLD Queries Transmitted	IGMPv1 Joins Received	IGMPv2/MLDv1 Reports Received	IGMPv3/MLDv2 Reports Received	IGMPv2/MLDv1 Leaves Received
No more entries						

Figure 9-3.2: The MVR Statistics Information

Parameter description:

- **VLAN ID :**

  The Multicast VLAN ID.

- **IGMP/MLD Queries Received :**

  The number of Received Queries for IGMP and MLD, respectively.

- **IGMP/MLD Queries Transmitted :**

  The number of Transmitted Queries for IGMP and MLD, respectively.

- **IGMPv1 Joins Received :**

  The number of Received IGMPv1 Join's.

- **IGMPv2/MLDv1 Report's Received :**

  The number of Received IGMPv2 Join's and MLDv1 Report's, respectively.

- **IGMPv3/MLDv2 Report's Received :**

  The number of Received IGMPv3 Join's and MLDv2 Report's, respectively.

- **IGMPv2/MLDv1 Leave's Received :**

  The number of Received IGMPv2 Leave's and MLDv1 Done's, respectively.

Buttons

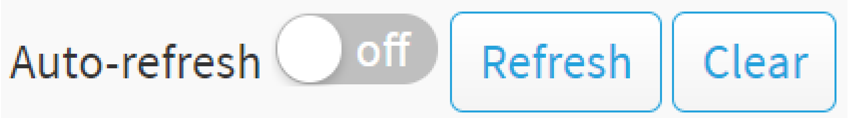


Figure 9-3.2: The MVR Statistics Information buttons

- **Auto-refresh :**

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

- **Refresh :**

  Click to refresh the page immediately.

- **Clear :**

  Clears all Statistics counters.

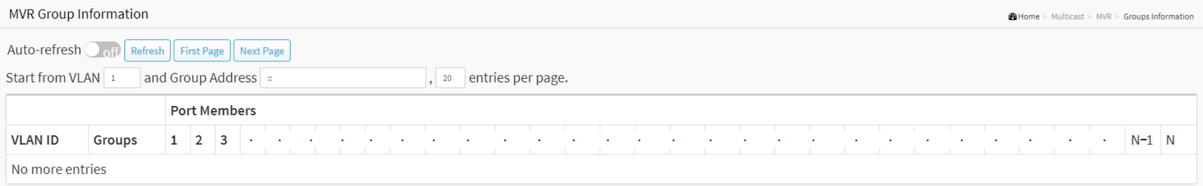
9-3.3 Groups Information

The section describes user could display the MVR Groups detail information on the switch. Entries in the MVR Group Table are shown on this page. The MVR Group Table is sorted first by VLAN ID, and then by group

Web Interface

To display the MVR Groups Information in the web interface:

1. Click Multicast, MVR and Groups Information.
2. If you want to auto-refresh the information then you need to evoke the “Auto-refresh”.
3. To click the “Refresh” to refresh an entry of the MVR Groups Information.
4. Click First/Next Page to change page.



MVR Group Information

Start from VLAN 1 and Group Address :: , 20 entries per page.

		Port Members																														
VLAN ID	Groups	1	2	3	·	·	·	·	·	·	·	·	·	·	·	·	·	·	·	·	·	·	·	·	·	·	·	·	·	·	N−1	N
No more entries																																

Figure 9-3.3: The MVR Groups Information

Parameter description:

Navigating the MVR Channels (Groups) Information Table

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

The "Start from VLAN", and "Group Address" input fields allow the user to select the starting point in the MVR Channels (Groups) Information Table. Clicking the Refresh button will update the displayed table starting from that or the closest next MVR Channels (Groups) Information Table match. In addition, the two input fields will - upon a Refresh button click - assume the value of the first displayed entry, allowing for continuous refresh with the same start address. The Next Page will use the last entry of the currently displayed table as a basis for the next lookup. When the end is reached the text "No more entries" is shown in the displayed table. Use the First Page button to start over.

MVR Channels (Groups) Information Table Columns

- **Show entries :**

  You can choose how many items you want to show up.

- **VLAN ID :**

  VLAN ID of the group.

- **Groups :**

  Group ID of the group displayed.

- **Port Members :**

  Ports under this group.

Buttons

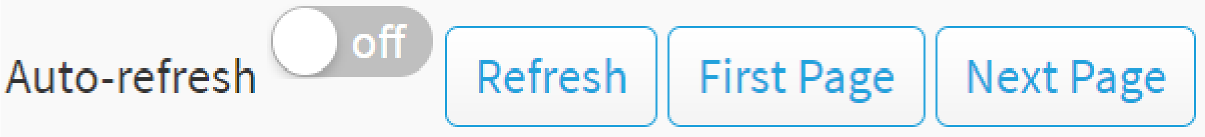


Figure 9-3.3: The MVR Groups Information buttons

- **Auto-refresh :**

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

- **Refresh :**

  Click to refresh the page immediately.

- **First Page :**
  Updates the system log entries, turn to the first page.

- **Next Page :**

  Updates the group information entries, turn to the next page.

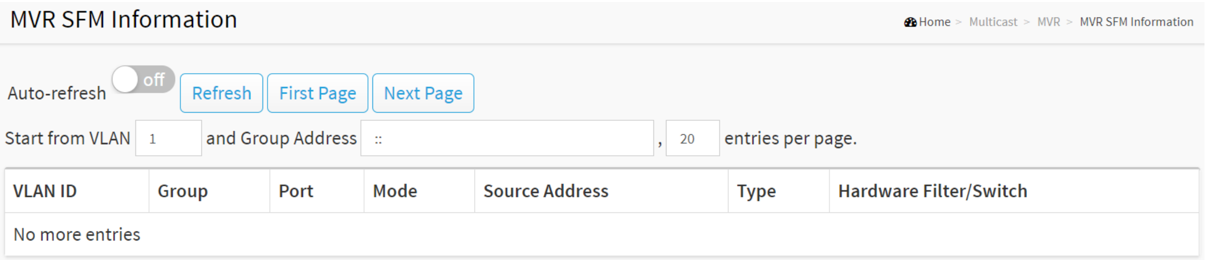
9-3.4 SFM Information

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

Web Interface

To display the MVR SFM Information in the web interface:

1. Click Multicast, MVR and MVR SFM Information.
2. If you want to auto-refresh the information then you need to evoke the “Auto-refresh”.
3. To click the “Refresh” to refresh an entry of the MVR Groups Information.
4. Click First/Next Page to change page.



MVR SFM Information

Start from VLAN 1 and Group Address :: , 20 entries per page.

VLAN ID	Group	Port	Mode	Source Address	Type	Hardware Filter/Switch
No more entries						

Figure 9-3.4: The MVR SFM Information

Parameter description:

Navigating the MVR SFM Information Table

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

MVR SFM Information Table Columns

- **Show entries :**

  You can choose how many items you want to show up.

- **VLAN ID :**

  VLAN ID of the group.

- **Group :**

  IP Multicast Group address.

- **Port :**

  Switch port number.

- **Mode :**

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

- **Source Address :**

  IP Address of the source. Currently, system limits the total number of IP source addresses for filtering to be 128. When there is not any source filtering address, the text "None" is shown in the Source Address field.

- **Type :**

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

- **Hardware Filter/Switch :**

  Indicates whether data plane destined to the specific group address from the source IPv4/IPv6 address could be handled by chip or not.

Buttons

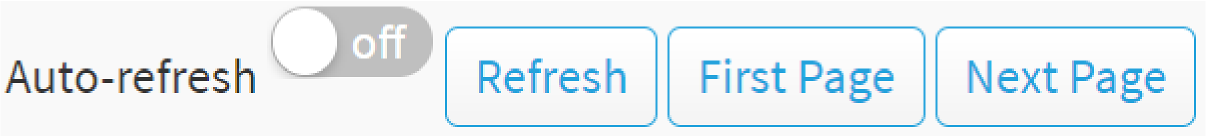


Figure 9-3.4: The MVR SFM Information buttons

- **Auto-refresh :**

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

- **Refresh :**

  Click to refresh the page immediately.

- **First Page :**
  Updates the system log entries, turn to the first page.

- **Next Page :**

  Updates the group information entries, turn to the next page.

9-4 Multicast Filtering Profile

This page provides Multicast Filtering Profile related configurations.

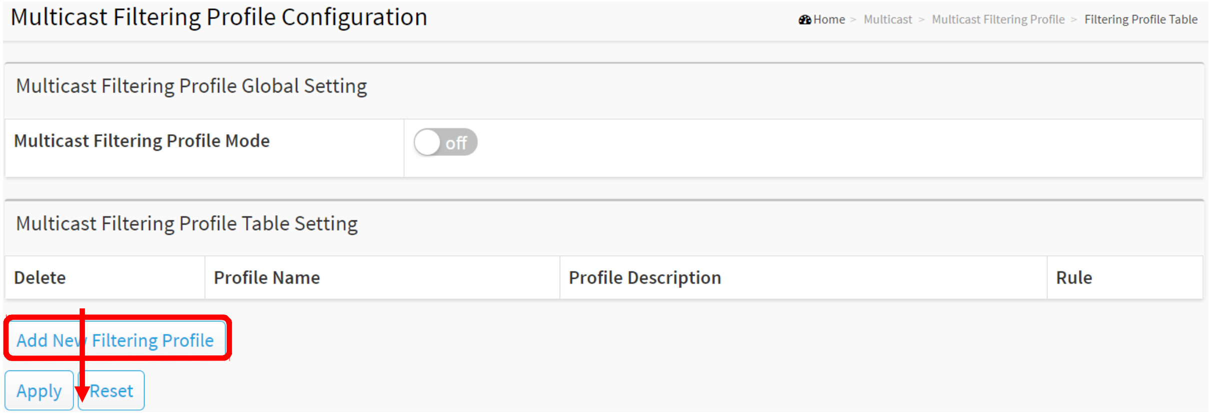
9-4.1 Filtering Profile Table

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

Web Interface

To configure the IPMC Profile Configuration in the web interface:

1. Click Multicast, Multicast Filtering Profile and Filtering Profile Table.
2. Scroll the Multicast Filtering Profile mode to enable or disable.
3. Click "Add New Filtering Profile".
4. Specify Profile Name, Profile Description and Rule.
5. Click the apply to save the setting.
6. If you want to cancel the setting then you need to click the Reset button. It will revert to previously saved values.



Multicast Filtering Profile Configuration

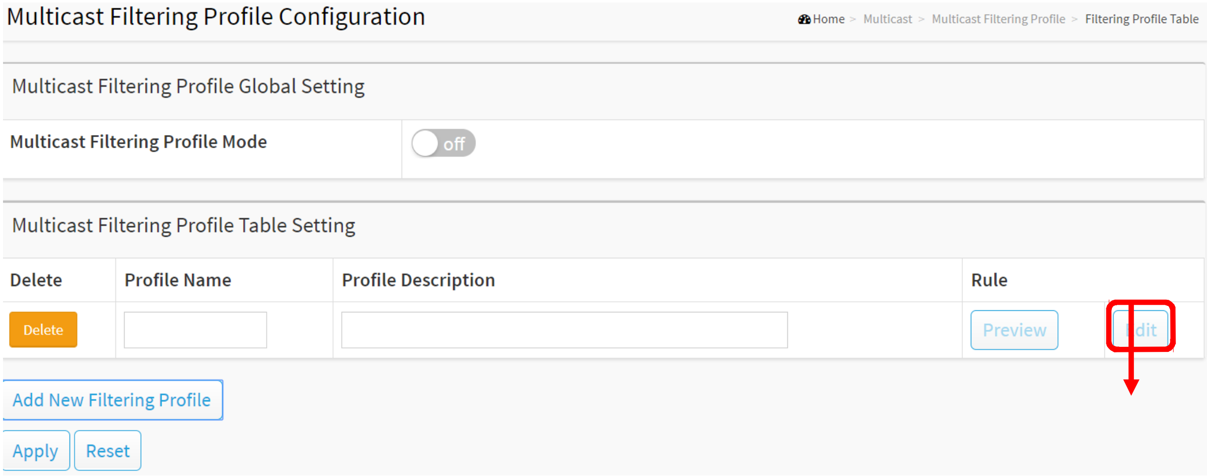
Home > Multicast > Multicast Filtering Profile > Filtering Profile Table

Multicast Filtering Profile Global Setting

Multicast Filtering Profile Mode: off

Multicast Filtering Profile Table Setting

Delete	Profile Name	Profile Description	Rule



Multicast Filtering Profile Configuration

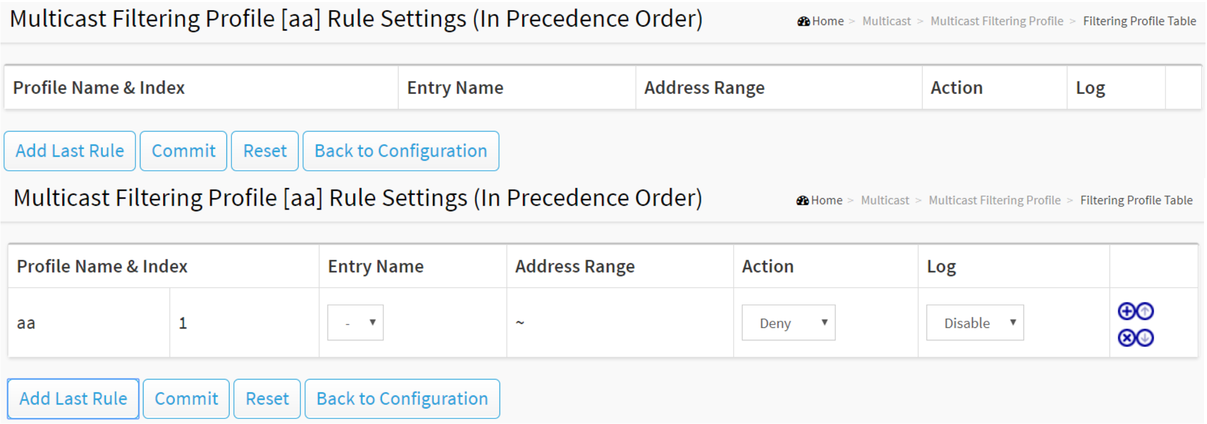
Home > Multicast > Multicast Filtering Profile > Filtering Profile Table

Multicast Filtering Profile Global Setting

Multicast Filtering Profile Mode: off

Multicast Filtering Profile Table Setting

Delete	Profile Name	Profile Description	Rule
Delete			Preview Edit



Multicast Filtering Profile [aa] Rule Settings (In Precedence Order)

Home > Multicast > Multicast Filtering Profile > Filtering Profile Table

Profile Name & Index	Entry Name	Address Range	Action	Log

Add Last Rule
Commit
Reset
Back to Configuration

Multicast Filtering Profile [aa] Rule Settings (In Precedence Order)

Home > Multicast > Multicast Filtering Profile > Filtering Profile Table

Profile Name & Index		Entry Name	Address Range	Action	Log	
aa	1	-	~	Deny	Disable	⊕⊙ ⊗⊙

Add Last Rule
Commit
Reset
Back to Configuration

Figure 9-4.1: The IPMC Profile Configuration

Parameter description:

- **Multicast Filtering Profile Mode :**

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

- **Profile Name :**

  The name used for indexing the profile table.
  Each entry has the unique name which is composed of at maximum 16 alphabetic and numeric characters.

- **Profile Description :**

  Additional description, which is composed of at maximum 64 alphabetic and numeric characters, about the profile.
  No blank or space characters are permitted as part of description. Use "_" or "-" to seperate the description sentence.

- **Rule :**

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

- **Profile Name & Index:**

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

- **Entry Name :**

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

- **Address Range :**

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

- **Action :**

  Indicates the learning action upon receiving the Join/Report frame that has the group address matches the address range of the rule.

Permit: Group address matches the range specified in the rule will be learned.
Deny: Group address matches the range specified in the rule will be dropped.

- **Log :**

  Indicates the logging preference upon receiving the Join/Report frame that has the group address matches the address range of the rule.

  Enable: Corresponding information of the group address, that matches the range specified in the rule, will be logged.
  Disable: Corresponding information of the group address, that matches the range specified in the rule, will not be logged.

- **Rule Management Buttons :**

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

Buttons

- **Add New Filtering Profile :**

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

- **Delete :**

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

- **Apply :**

  Click to save changes.

- **Reset :**

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

- **Add Last Rule :**

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

9-4.2 Filtering Address Entry

This page provides address range settings used in IPMC profile.

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

Web Interface

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

1. Click Multicast, Multicast Filtering Profile and Filtering Address Entry.
2. Click "Add New Address (Range) Entry".
3. Specify Entry Name, Start Address and End Address.
4. Click the apply to save the setting.

5. If you want to cancel the setting then you need to click the Reset button. It will revert to previously saved values.

6. Click “Refresh” to refresh an entry of the MLD Snooping Group Information.

7. Click First Entry/Next Entry to change Entry.

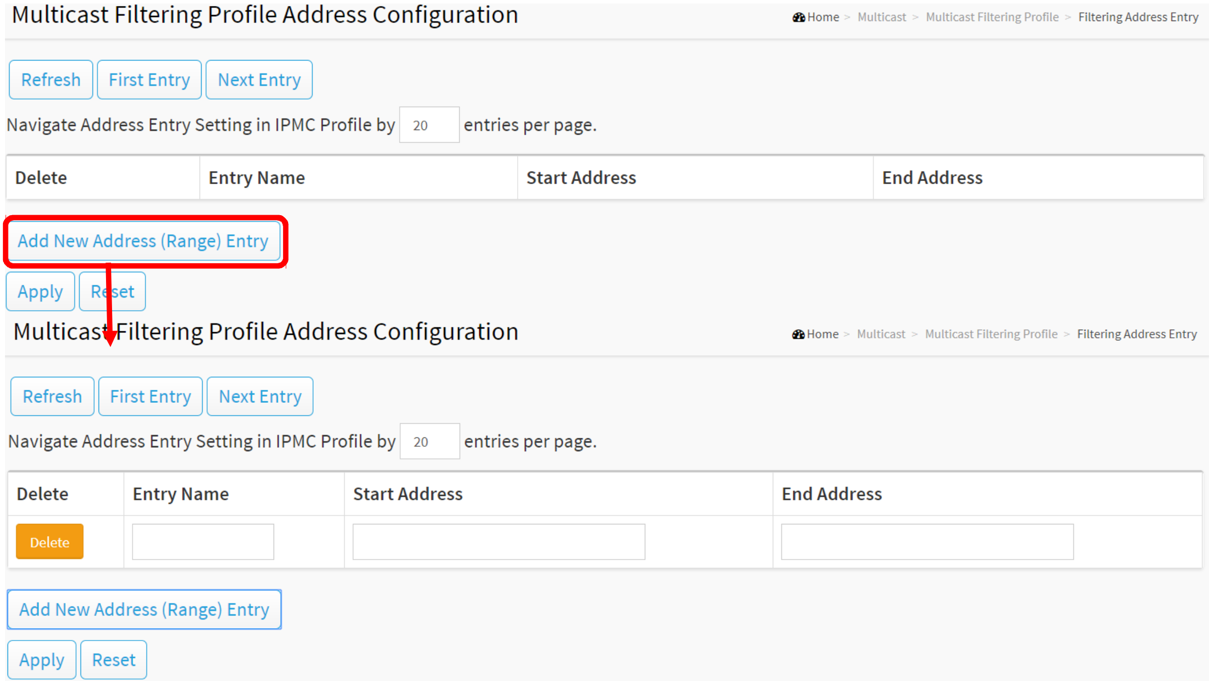

Multicast Filtering Profile Address Configuration
Home > Multicast > Multicast Filtering Profile > Filtering Address Entry
Refresh
First Entry
Next Entry
Navigate Address Entry Setting in IPMC Profile by 20 entries per page.
Delete
Entry Name
Start Address
End Address
Add New Address (Range) Entry
Apply
Reset
Multicast Filtering Profile Address Configuration
Home > Multicast > Multicast Filtering Profile > Filtering Address Entry
Refresh
First Entry
Next Entry
Navigate Address Entry Setting in IPMC Profile by 20 entries per page.
Delete
Entry Name
Start Address
End Address
Delete
Add New Address (Range) Entry
Apply
Reset

Figure 9-4.2: The IPMC Profile Address Configuration

Parameter description:

- **Entry Name :**

  The name used for indexing the address entry table.
  Each entry has the unique name which is composed of at maximum 16 alphabetic and numeric characters.

- **Start Address :**

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

- **End Address :**

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

Buttons

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

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

- **Delete :**

  Check to delete the entry.
  The designated entry 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.

- **First Entry :**

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

- **Next Entry :**

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

Chapter 10 DHCP

The section describes 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.

10-1 Snooping

10-1.1 Configuration

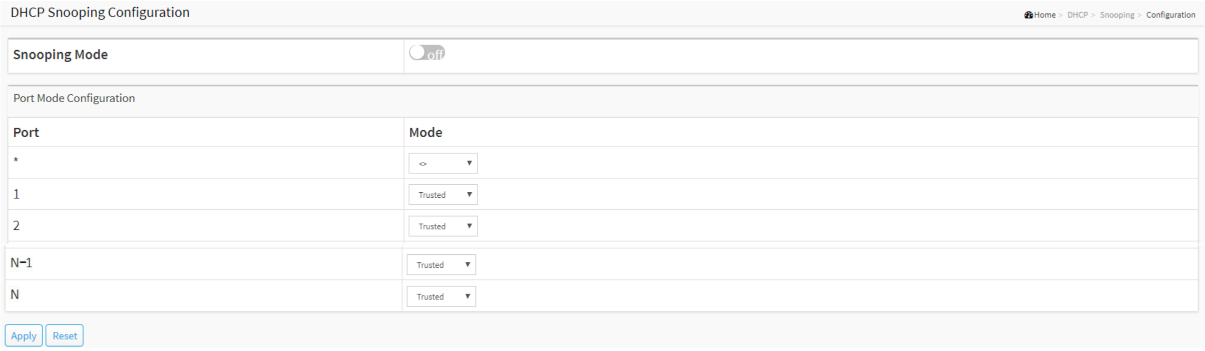
DHCP Snooping is used to block intruder on the untrusted ports of the switch device when it tries to intervene by injecting a bogus DHCP reply packet to a legitimate conversation between the DHCP client and server.

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

Web Interface

To configure DHCP snooping in the web interface:

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



DHCP Snooping Configuration

Snooping Mode	off

Port Mode Configuration

Port	Mode
*	<>
1	Trusted
2	Trusted
N−1	Trusted
N	Trusted

Figure 10-1.1: The DHCP Snooping Configuration

Parameter description:

- **Snooping Mode :**

  Indicates the DHCP snooping mode operation. Possible modes are:

  on: Enable DHCP snooping mode operation. When DHCP snooping mode operation is enabled, the DHCP request messages will be forwarded to trusted ports and only allow reply packets from trusted ports.

  off: Disable DHCP snooping mode operation.

- **Port Mode Configuration**

  Indicates the DHCP snooping port mode. Possible port modes are:

  Trusted: Configures the port as trusted source of the DHCP messages. Trusted port can forward DHCP packets normally.

  Untrusted: Configures the port as untrusted source of the DHCP messages. Untrusted port will discard the packets when it receive DHCP packets.

Buttons

- **Apply :**

  Click to save changes.

- **Reset :**

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

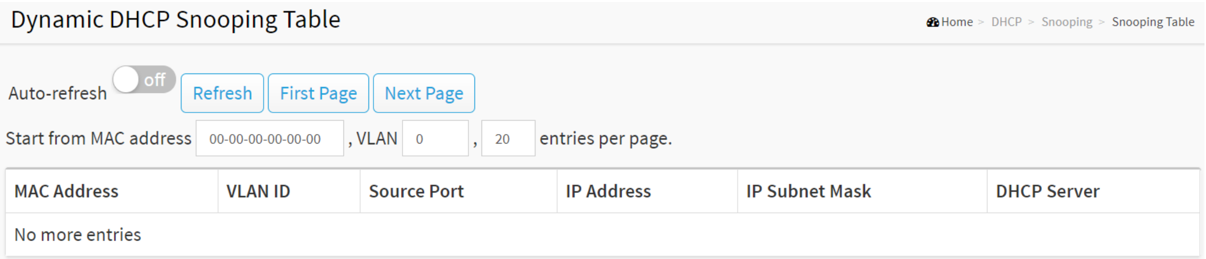
10-1.2 Snooping Table

This page display the dynamic IP assigned information after DHCP Snooping mode is enabled. All DHCP clients obtained the dynamic IP address from the DHCP server will be listed in this table except for local VLAN interface IP addresses. Entries in the Dynamic DHCP snooping Table are shown on this page.

Web Interface

To monitor a DHCP in the web interface:

1. Click DHCP, Snooping and Snooping table.
2. If you want to auto-refresh the information then you need to evoke the "Auto-refresh".
3. To click the "Refresh" to refresh an entry of the MVR Groups Information.
4. Click First/Next Page to change page.



Dynamic DHCP Snooping Table

Home > DHCP > Snooping > Snooping Table

Auto-refresh off Refresh First Page Next Page

Start from MAC address 00-00-00-00-00-00 , VLAN 0 , 20 entries per page.

MAC Address	VLAN ID	Source Port	IP Address	IP Subnet Mask	DHCP Server
No more entries					

Figure 10-1.2: The DHCP snooping table

Parameter description:

- **Show entries :**

  You can choose how many items you want to show up.

- **MAC Address :**

  User MAC address of the entry.

- **VLAN ID :**

  VLAN-ID in which the DHCP traffic is permitted.

- **Source Port:**

  Switch Port Number for which the entries are displayed.

- **IP Address :**

  User IP address of the entry.

- **IP Subnet Mask :**

  User IP subnet mask of the entry.

- **DHCP Server :**

  DHCP Server address of the entry.

Buttons

Figure 10-1.2: The DHCP snooping table buttons

- **Auto-refresh :**

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

- **Refresh :**

  Click to refresh the page immediately.

- **First Page :**
  Updates the system log entries, turn to the first page.

- **Next Page :**

  Updates the group information entries, turn to the next page.

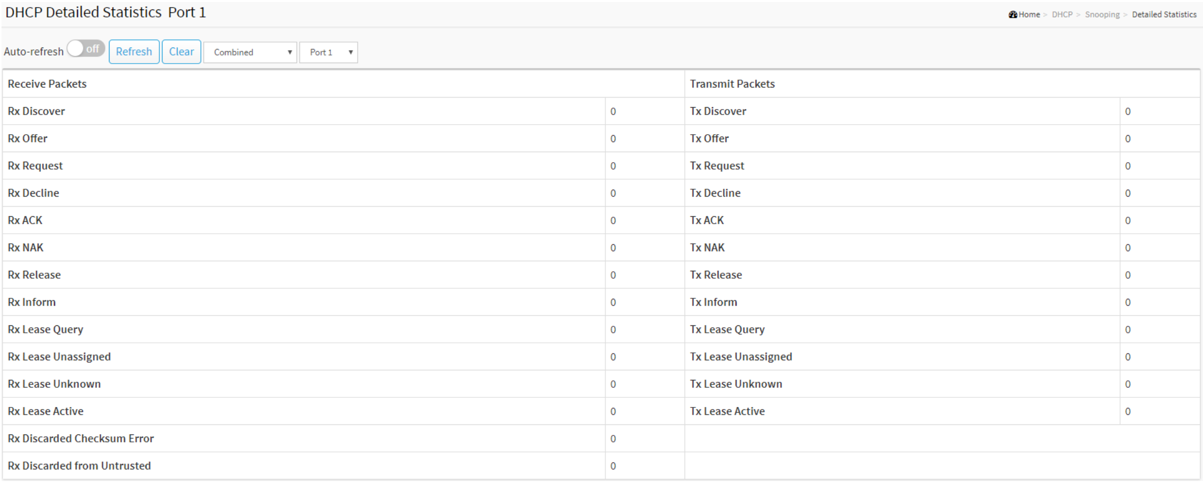
10-1.3 Detailed Statistics

This page provides statistics for DHCP snooping. Notice that the normal forward per-port TX statistics isn't increased if the incoming DHCP packet is done by L3 forwarding mechanism. And clear the statistics on specific port may not take effect on global statistics since it gathers the different layer overview.

Web Interface

To display a DHCP Relay statistics in the web interface:

1. Click DHCP, Snooping and Detailed Statistics.
2. Select port that you want to display the DHCP Detailed Statistics.
3. If you want to auto-refresh the information then you need to evoke the “Auto-refresh”.
4. To click the “Refresh” to refresh an entry of the DHCP Detailed Statistics.



DHCP Detailed Statistics Port 1

Receive Packets		Transmit Packets	
Rx Discover	0	Tx Discover	0
Rx Offer	0	Tx Offer	0
Rx Request	0	Tx Request	0
Rx Decline	0	Tx Decline	0
Rx ACK	0	Tx ACK	0
Rx NAK	0	Tx NAK	0
Rx Release	0	Tx Release	0
Rx Inform	0	Tx Inform	0
Rx Lease Query	0	Tx Lease Query	0
Rx Lease Unassigned	0	Tx Lease Unassigned	0
Rx Lease Unknown	0	Tx Lease Unknown	0
Rx Lease Active	0	Tx Lease Active	0
Rx Discarded Checksum Error	0		
Rx Discarded from Untrusted	0		

Figure 10-1.3: The DHCP Detailed Statistics

Parameter description:

Server Statistics

- **Rx and Tx Discover :**

  The number of discover (option 53 with value 1) packets received and transmitted.

- **Rx and Tx Offer :**

  The number of offer (option 53 with value 2) packets received and transmitted.

- **Rx and Tx Request :**

  The number of request (option 53 with value 3) packets received and transmitted.

- **Rx and Tx Decline :**

  The number of decline (option 53 with value 4) packets received and transmitted.

- **Rx and Tx ACK :**

  The number of ACK (option 53 with value 5) packets received and transmitted.

- **Rx and Tx NAK :**

  The number of NAK (option 53 with value 6) packets received and transmitted.

- **Rx and Tx Release :**

  The number of release (option 53 with value 7) packets received and transmitted.

- **Rx and Tx Inform :**

  The number of inform (option 53 with value 8) packets received and transmitted.

- **Rx and Tx Lease Query :**

  The number of lease query (option 53 with value 10) packets received and transmitted.

- **Rx and Tx Lease Unassigned :**

  The number of lease unassigned (option 53 with value 11) packets received and transmitted.

- **Rx and Tx Lease Unknown :**

  The number of lease unknown (option 53 with value 12) packets received and transmitted. Rx and Tx Lease Active

- **Rx and Tx Lease Active :**

  The number of lease active (option 53 with value 13) packets received and transmitted.

- **Rx Discarded checksum error :**

  The number of discard packet that IP/UDP checksum is error.

- **Rx Discarded from Untrusted :**

  The number of discarded packet that are coming from untrusted port.

Buttons

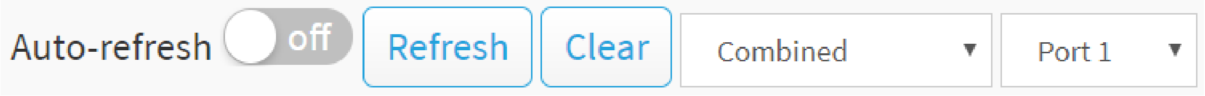


Figure 10-1.3: The DHCP Detailed Statistics buttons

- **Auto-refresh :**

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

- **Refresh :**

  Click to refresh the page immediately.

- **Port 1 :**

  Select port that you want to display the DHCP Detailed Statistics.

10-2 Relay

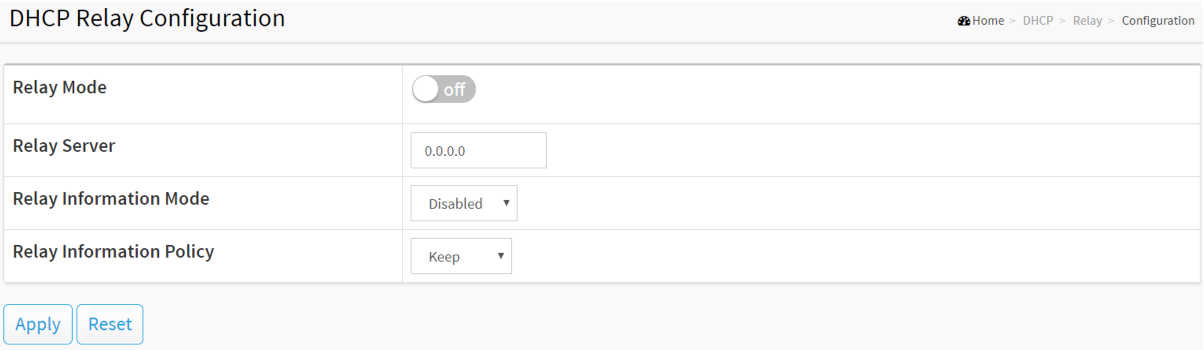
10-2.1 Configuration

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

Web Interface

To configure DHCP Relay in the web interface:

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



DHCP Relay Configuration

Relay Mode	off
Relay Server	0.0.0.0
Relay Information Mode	Disabled
Relay Information Policy	Keep

Figure 10-2.1: The DHCP Relay Configuration

Parameter description:

- **Relay Mode :**

  Indicates the DHCP relay mode operation.

  Possible modes are:

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

  off: Disable DHCP relay mode operation.

- **Relay Server :**

  Indicates the DHCP relay server IP address.

- **Relay Information Mode :**

  Indicates the DHCP relay information mode option operation. The option 82 circuit ID format as "[vlan_id][module_id][port_no]". The first four characters represent the VLAN ID, the fifth and sixth characters are the module ID(in standalone device it always equal 0, in stackable device it means switch ID), and the last two characters are the port number. For example, "00030108" means the DHCP message receive form VLAN ID 3, switch ID 1, port No 8. And the option 82 remote ID value is equal the switch MAC address.

Possible modes are:

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

Disabled: Disable DHCP relay information mode operation.

- **Relay Information Policy :**

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

Buttons

- **Apply :**

  Click to save changes.

- **Reset :**

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

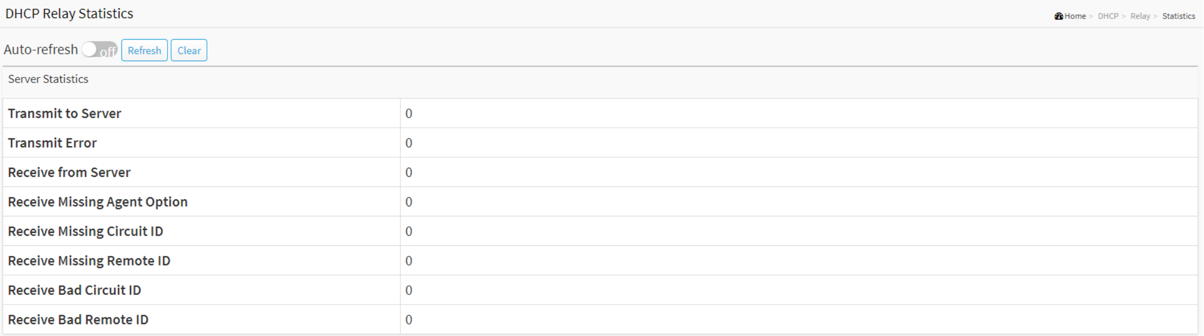
10-2.2 Statistics

This page provides statistics for DHCP relay.

Web Interface

To monitor a DHCP Relay statistics in the web interface:

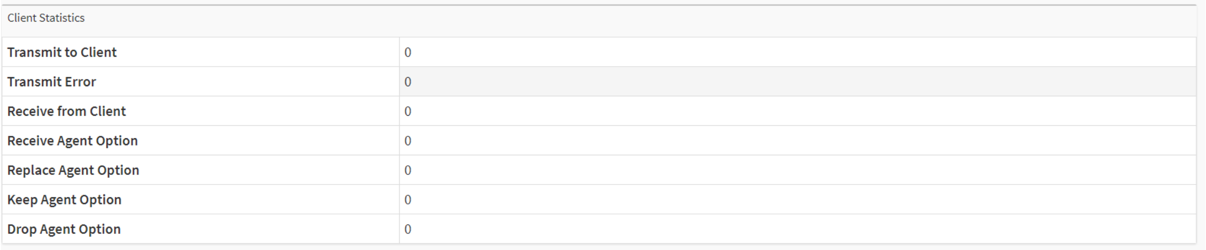
1. Click DHCP, Relay and Statistics.
2. To display DHCP relay statistics.
3. If you want to auto-refresh the information then you need to evoke the “Auto-refresh”.
4. To click the “Refresh” to refresh an entry of the DHCP Detailed Statistics.



DHCP Relay Statistics

Server Statistics

Transmit to Server	0
Transmit Error	0
Receive from Server	0
Receive Missing Agent Option	0
Receive Missing Circuit ID	0
Receive Missing Remote ID	0
Receive Bad Circuit ID	0
Receive Bad Remote ID	0



Client Statistics	
Transmit to Client	0
Transmit Error	0
Receive from Client	0
Receive Agent Option	0
Replace Agent Option	0
Keep Agent Option	0
Drop Agent Option	0

Figure 10-2.2: The DHCP relay statistics

Parameter description:

Server Statistics

- **Transmit to Server :**

  The number of packets that are relayed from client to server.

- **Transmit Error :**

  The number of packets that resulted in errors while being sent to clients.

- **Receive from Server :**

  The number of packets received from server.

- **Receive Missing Agent Option:**

  The number of packets received without agent information options.

- **Receive Missing Circuit ID :**

  The number of packets received with the Circuit ID option missing.

- **Receive Missing Remote ID :**

  The number of packets received with the Remote ID option missing.

- **Receive Bad Circuit ID :**

  The number of packets whose Circuit ID option did not match known circuit ID.

- **Receive Bad Remote ID :**

  The number of packets whose Remote ID option did not match known Remote ID.

Client Statistics

- **Transmit to Client :**

  The number of relayed packets from server to client.

- **Transmit Error :**

  The number of packets that resulted in error while being sent to servers.

- **Receive from Client :**

  The number of received packets from server.

- **Receive Agent Option :**

  The number of received packets with relay agent information option.

- **Replace Agent Option :**

  The number of packets which were replaced with relay agent information option.

- **Keep Agent Option :**

  The number of packets whose relay agent information was retained.

- **Drop Agent Option :**

  The number of packets that were dropped which were received with relay agent information.

Buttons

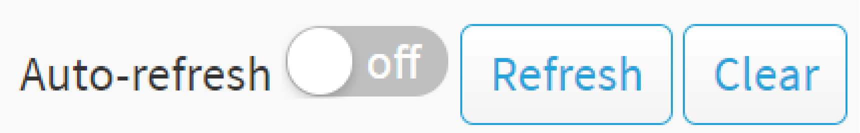


Figure 10-2.2: The DHCP relay statistics buttons

- **Auto-refresh :**

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

- **Refresh :**

  Click to refresh the page immediately.

- **Clear :**

  Clear all statistics.

10-3 Server

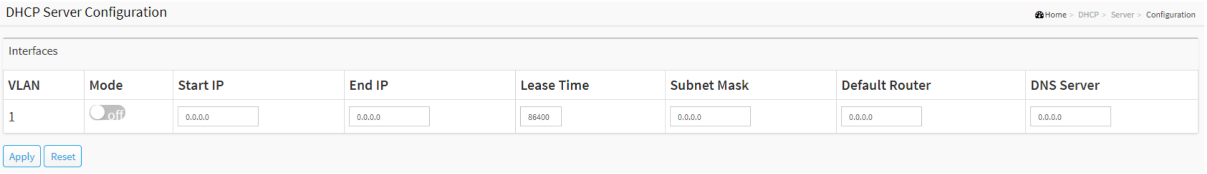
10-3.1 Configuration

This page configures mode to enable/disable DHCP server per system and per VLAN. And configures Start IP and End IP addresses. DHCP server will allocate these IP addresses to DHCP client. And deliver configuration parameters to DHCP client.

Web Interface

To configure DHCP server Configuration in the web interface:

1. Click DHCP, Server and Configurtion.
2. Click "Add Interface".
3. Specify VLAN, Mode, Start IP, End IP, Lease time, Subnet mask, Default router, DNS server.
4. Click Apply.



DHCP Server Configuration

Interfaces

VLAN	Mode	Start IP	End IP	Lease Time	Subnet Mask	Default Router	DNS Server
1	off	0.0.0.0	0.0.0.0	86400	0.0.0.0	0.0.0.0	0.0.0.0

Figure 10-3.1: The DHCP server configuration

Parameter description:

- **VLAN:**

  Configure the VLAN in which DHCP server is enabled or disabled. Allowed VLAN are in the range 1 through 4095

- **Mode :**

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

- **Start IP and End IP :**

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

- **Lease Time :**

  Display lease time of the pool.

- **Subnet Mask :**

  Configure subnet mask of the DHCP address.

- **Default router :**

  Configure the destination IP network or host address of this route.

- **DNS Server :**

  Specify DNS server.

Buttons

- **Delete :**

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

- **Add Interface :**

  Click to add a new DHCP server.

- **Apply :**

  Click to save changes.

- **Reset :**

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

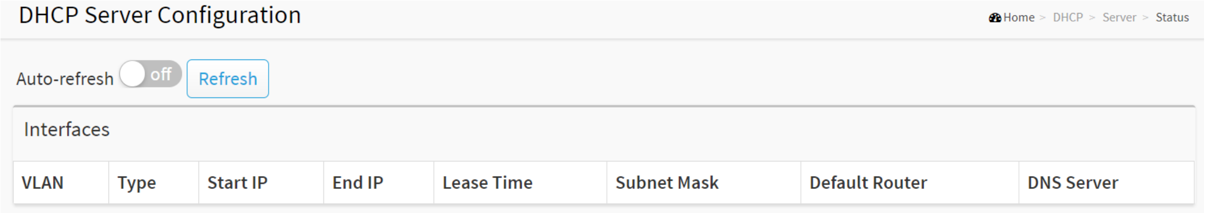
10-3.2 Status

This page displays DHCP server status.

Web Interface

To display DHCP server status in the web interface:

1. Click DHCP, Server and Status.
2. If you want to auto-refresh the information then you need to evoke the "Auto-refresh".
3. To click the "Refresh" to refresh an entry of the DHCP server status.



DHCP Server Configuration

Interfaces

VLAN	Type	Start IP	End IP	Lease Time	Subnet Mask	Default Router	DNS Server

Figure 10-3.2: The DHCP server status

Parameter description:

- **VLAN:**

  The VLAN ID of the entry.

- **Type :**

  Indicate the operation type per VLAN. Possible types are: Static and DMS.

- **Start IP and End IP :**

  Display the Start IP and the End IP.

- **Lease Time :**

  Display lease time of the pool.

- **Subnet Mask :**

  Display subnet mask of the DHCP address.

- **Default router :**

  Display the destination IP network or host address of this route.

- **DNS Server :**

  Display DNS server.

Buttons

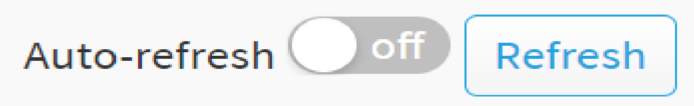


Figure 10-3.2: The DHCP server status buttons

- **Auto-refresh :**

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

- **Refresh :**

  Click to refresh the page immediately.

Chapter 11 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.

11-1 Management

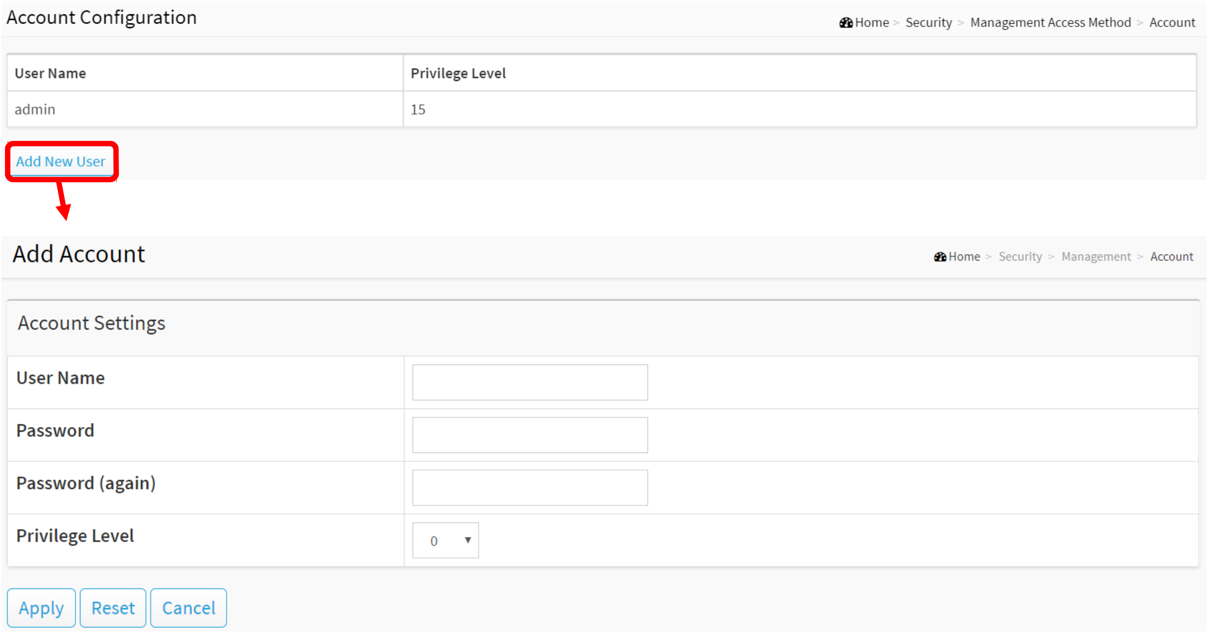
11-1.1 Account

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

Web Interface

To configure User in the web interface:

1. Click Security, Management and Account.
2. Click Add new user
3. Specify the User Name parameter.
4. Click Apply.


Home > Security > Management Access Method > Account
Add New User
Home > Security > Management > Account
Apply
Reset
Cancel

Account Configuration

User Name	Privilege Level
admin	15

Add Account

Account Settings

User Name	
Password	
Password (again)	
Privilege Level	0 ▾

Figure 11-1.1: The Account configuration

Parameter description:

- **User Name :**

  The name identifying the user. The field can be input 31 characters. This is also a link to Add/Edit User.

- **Password :**

To type the password. The field can be input 31 characters, and the allowed content is the ASCII characters from 32 to 126.

- **Password (again) :**

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

- **Privilege Level :**

  The privilege level of the user. The allowed range is 0 to 15. If the privilege level value is 15, it can access all groups, i.e. that is granted the fully control of the device. But others value need to refer to each group privilege level. User's privilege should be same or greater than the group privilege level to have the access of that group. By default setting, most groups privilege level 5 has the read-only access and privilege level 10 has the read-write access. And the system maintenance (software upload, factory defaults and etc.) need user privilege level 15. Generally, the privilege level 15 can be used for an administrator account, privilege level 10 for a standard user account and privilege level 5 for a guest account.

Buttons

- **Apply :**

  Click to save changes.

- **Reset :**

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

- **Cancel :**

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

- **Delete User :**

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

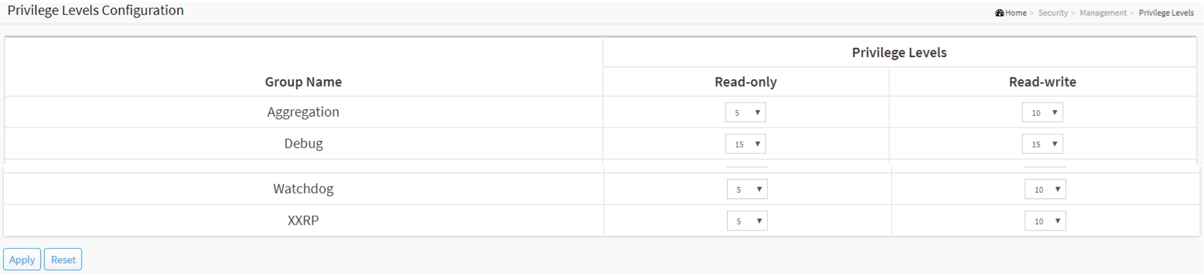
11-1.2 Privilege Levels

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

Web Interface

To configure Privilege Level in the web interface:

1. Click Security, Management and Privilege Levels.
2. Specify the Privilege parameter.
3. Click Apply.



Privilege Levels Configuration

Group Name	Privilege Levels	
	Read-only	Read-write
Aggregation	5 ▾	10 ▾
Debug	15 ▾	15 ▾
Watchdog	5 ▾	10 ▾
XXRP	5 ▾	10 ▾

Figure11-1.2: The Privilege Level configuration

Parameter description:

- **Group Name :**

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

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

- **Privilege Levels :**

  Every group has an authorization Privilege level for the following sub groups: configuration read-only, configuration/execute read-write. User Privilege should be same or greater than the authorization Privilege level to have the access to that group.

Buttons

- **Apply :**

  Click to save changes.

- **Reset :**

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

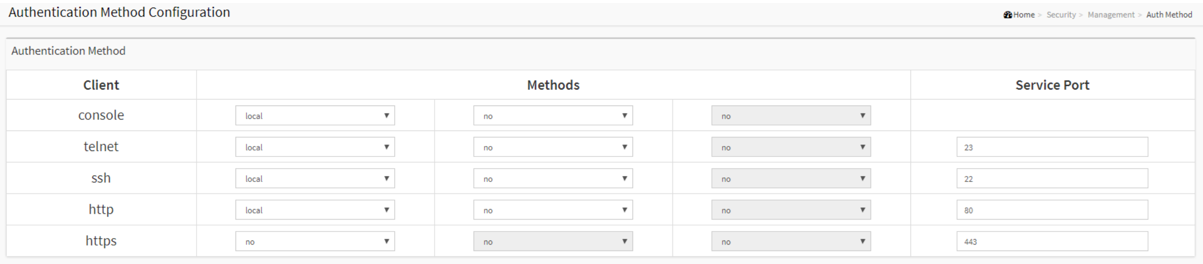
11-1.3 Auth Method

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

Web Interface

To configure an Auth Method Configuration in the web interface:

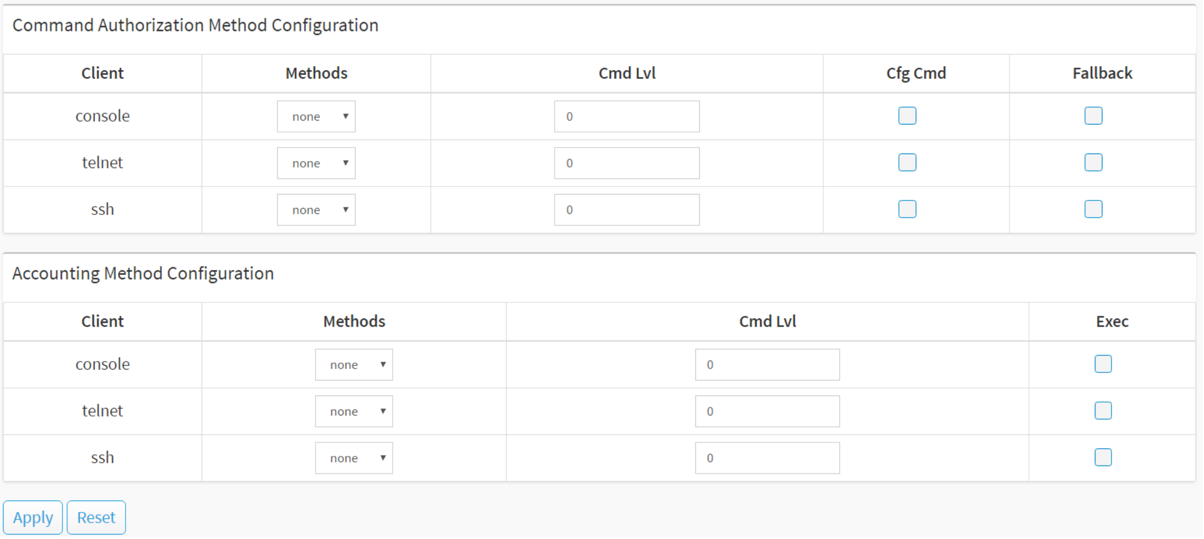
1. Click Security, Management and Auth Method.
2. Specify the Client (console, telent, ssh, web) which you want to monitor.
3. Specify the Methods (none, local, radius, tacacs), Service port, Cmd Lvl, Cfg Cmd, Fallback, Exec.
4. Click Apply.



Authentication Method Configuration

Authentication Method

Client	Methods			Service Port
console	local ▾	no ▾	no ▾	
telnet	local ▾	no ▾	no ▾	23
ssh	local ▾	no ▾	no ▾	22
http	local ▾	no ▾	no ▾	80
https	no ▾	no ▾	no ▾	443



Command Authorization Method Configuration

Client	Methods	Cmd Lvl	Cfg Cmd	Fallback
console	none	0	□	□
telnet	none	0	□	□
ssh	none	0	□	□

Accounting Method Configuration

Client	Methods	Cmd Lvl	Exec
console	none	0	□
telnet	none	0	□
ssh	none	0	□

Figure 11-1.3: The Authentication Method Configuration

Parameter description:

Authentication Method Configuration

- **Client :**

  The management client for which the configuration below applies.

- **Method :**

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

  - none : authentication is disabled and login is not possible.
  - local : use the local user database on the switch for authentication.
  - radius : use a remote RADIUS server for authentication.
  - tacacs : use a remote TACACS server for authentication.

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

- **Service Port :**

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

- **HTTP Redirect :**

  Enable http Automatic Redirect.

Command Authorization Method Configuration

- **Client :**

  The management client for which the configuration below applies.

- **Method :**

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

- none : authorization is disabled and login is not possible.
- tacacs : use a remote TACACS+ server for authorization.

- **Cmd Lvl :**

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

- **Cfg Cmd :**

  Enable or disable the configure command.

- **Fallback :**

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

  Accounting Method Configuration

- **Client :**

  The management client for which the configuration below applies.

- **Method :**

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

  - none : accounting is disabled and login is not possible.
  - tacacs : use a remote TACACS+ server for accounting.

- **Cmd Lvl :**

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

- **Exec :**

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

Buttons

- **Apply :**

  Click to save changes.

- **Reset :**

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

11-1.4 Access Method

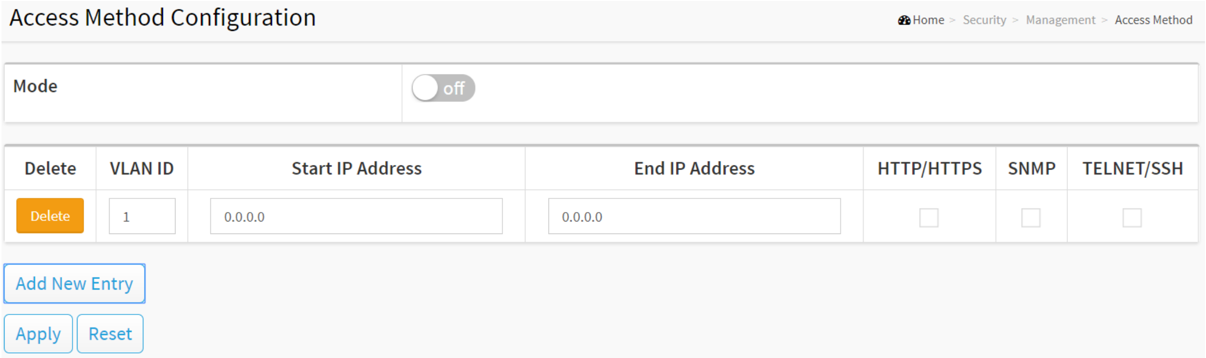
This section shows you to configure access management table of the Switch including HTTP/HTTPS, SNMP, and TELNET/SSH. You can manage the Switch over an Ethernet LAN, or over the Internet.

Web Interface

To configure an Access Method Configuration in the web interface:

1. Click Security, Management and Access Method.
2. Select “on” in the Mode of Access Management Configuration.

3. Click "Add new entry".
4. Specify the VLAN ID, Start IP Address, End IP Address.
5. Checked Access Management method (HTTP/HTTPS, SNMP, and TELNET/SSH) in the entry.
6. Click Apply.



Access Method Configuration

Home > Security > Management > Access Method

Mode	off

Delete	VLAN ID	Start IP Address	End IP Address	HTTP/HTTPS	SNMP	TELNET/SSH
Delete	1	0.0.0.0	0.0.0.0	□	□	□

Figure 11-1.4: The Access Method Configuration

Parameter description:

- **Mode :**

  Indicates the access management mode operation. Possible modes are:

  On : Enable access management mode operation.

  Off : Disable access management mode operation.

- **VLAN ID :**

  Indicates the VLAN ID for the access management entry.

- **Delete :**

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

- **Start IP address :**

  Indicates the start IP unicast address for the access management entry.

- **End IP address :**

  Indicates the end IP unicast address for the access management entry.

- **HTTP/HTTPS :**

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

- **SNMP :**

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

- **TELNET/SSH :**

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

Buttons

- **Add New Entry :**

  Click to add a new access management entry.

- **Apply :**

Click to save changes.

- **Reset :**

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

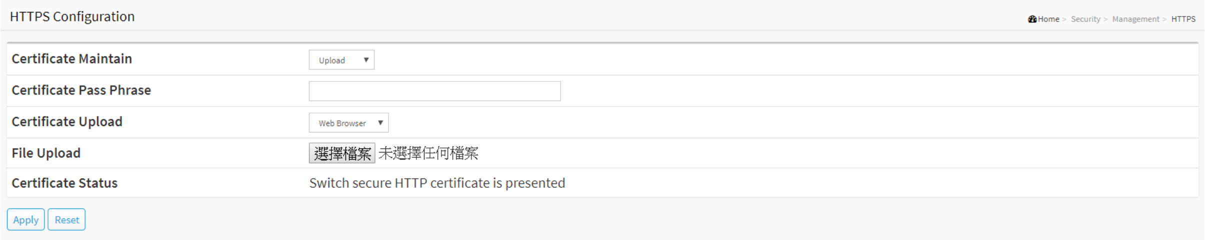
11-1.5 HTTPS

This page allows you to configure the HTTPS settings and maintain the current certificate on the switch.

Web Interface

To configure an Access Management Configuration in the web interface:

1. Click Configuration, Security, Management and HTTPS.
2. Specify the Certificate Maintain, Certificate Pass Phrase, Certificate Upload.
3. Chick Browser to select the file to upload.
4. Click Apply.



HTTPS Configuration

Certificate Maintain	Upload ▾
Certificate Pass Phrase	
Certificate Upload	Web Browser ▾
File Upload	選擇檔案 未選擇任何檔案
Certificate Status	Switch secure HTTP certificate is presented

Figure 11-1.5: The HTTPS Configuration

Parameter description:

- **Certificate Maintain :**

  The operation of certificate maintenance. Possible operations are: **Upload:** Upload a certificate PEM file. Possible methods are: Web Browser or URL. **Generate:** Generate a new self-signed RSA certificate.

- **Certificate Pass Phrase :**

  Enter the pass phrase in this field if your uploading certificate is protected by a specific passphrase.

- **Certificate Upload :**

  Upload a certificate PEM file into the switch. The file should contain the certificate and private key together. If you have two separated files for saving certificate and private key. Use the Linux cat command to combine them into a single PEM file. For example, cat my.cert my.key > my.pem
  Notice that the RSA certificate is recommended since most of the new version of browsers has removed support for DSA in certificate, e.g. Firefox v37 and Chrome v39.
  Possible methods are:
  Web Browser: Upload a certificate via Web browser.
  URL: Upload a certificate via URL, the supported protocols are HTTP, HTTPS, TFTP and FTP.
  The URL format is <protocol>://[<username>[:<password>]@]< host>[:<port>][/<path>]/<file_name>. For example, tftp://10.10.10.10/new_image_path/new_image.dat, http://username:password@10.10.10.10:80/new_image_path/new_image.dat. A valid file name is a text string drawn from alphabet (A-Za-z), digits (0-9), dot (.), hyphen (-), under

score(_). The maximum length is 63 and hyphen must not be first character. The file name content that only contains '.' is not allowed.

- **Certificate Status :**

  Display the current status of certificate on the switch.
  Possible statuses are:
  Switch secure HTTP certificate is presented.
  Switch secure HTTP certificate is not presented.
  Switch secure HTTP certificate is generating ....

Buttons

- **Apply :**

  Click to save changes.

- **Reset :**

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

11-2 802.1X

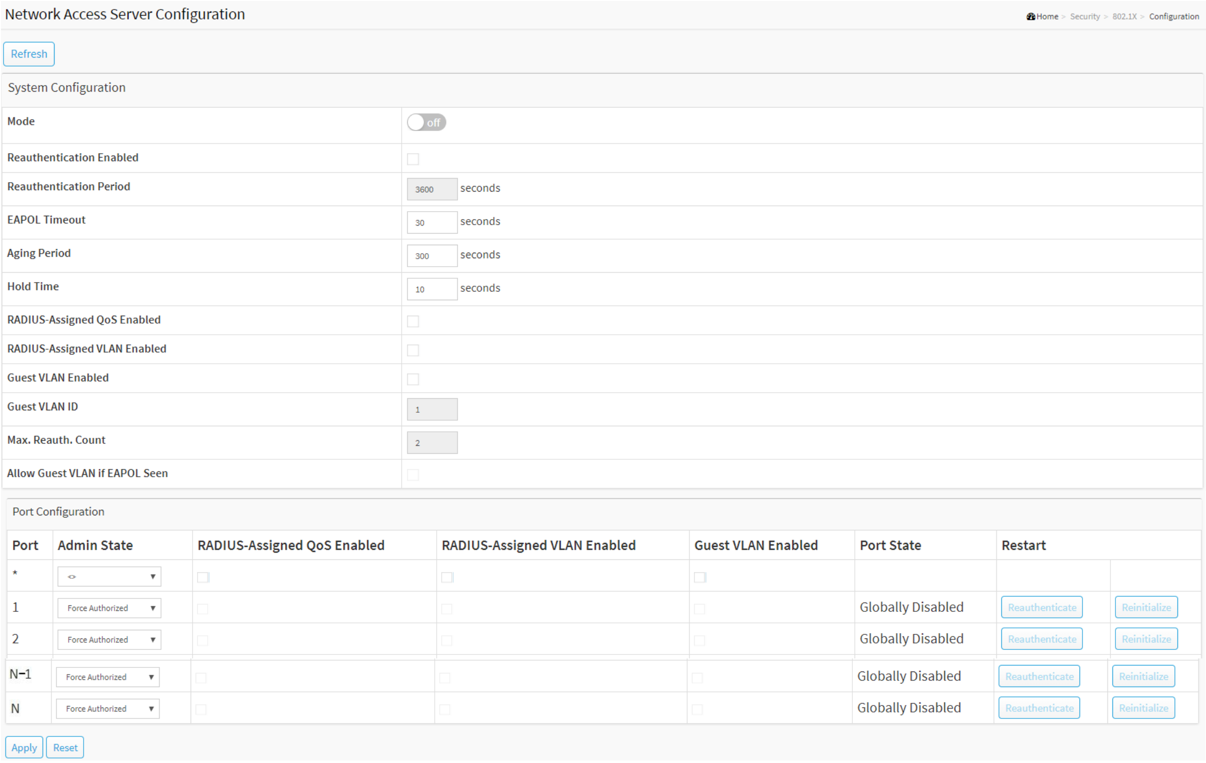
11-2.1 Configuration

The section describes to configure the 802.1X parameters of the switch. The 802.1X can be employed to connect users to a variety of resources including Internet access, conference calls, printing documents on shared printers, or by simply logging on to the Internet.

Web Interface

To configure the IEEE 802.1X in the web interface:

1. Click Security, 802.1X and Configuration.
2. Select "on" in the Mode of IEEE 802.1X Configuration.
3. Checked Reauthentication Enabled.
4. Set Reauthentication Period (Default is 3600 seconds).
5. Set EAPOL Timeout (Default is 30 seconds).
6. Set Aging Period (Default is 300 seconds).
7. Set Hold Time (Default is 10 seconds).
8. Checked RADIUS-Assigned QoS Enabled.
9. Checked RADIUS-Assigned VLAN Enabled.
10. Checked Guest VLAN Enabled.
11. Specify Guest VLAN ID.
12. Specify Max. Reauth. Count.
13. Checked Allow Guest VLAN if EAPOL Seen.
14. Select Admin State and displays Port State.
15. Click the Apply to save the setting.
16. If you want to cancel the setting then you need to click the Reset button. It will revert to previously saved values.


Network Access Server Configuration
Home > Security > 802.1X > Configuration
Refresh

System Configuration

Mode	off
Reauthentication Enabled	□
Reauthentication Period	3600 seconds
EAPOL Timeout	30 seconds
Aging Period	300 seconds
Hold Time	10 seconds
RADIUS-Assigned QoS Enabled	□
RADIUS-Assigned VLAN Enabled	□
Guest VLAN Enabled	□
Guest VLAN ID	1
Max. Reauth. Count	2
Allow Guest VLAN if EAPOL Seen	□

Port Configuration

Port	Admin State	RADIUS-Assigned QoS Enabled	RADIUS-Assigned VLAN Enabled	Guest VLAN Enabled	Port State	Restart	
*	<>	□	□	□			
1	Force Authorized	□	□	□	Globally Disabled	Reauthenticate	Reinitialize
2	Force Authorized	□	□	□	Globally Disabled	Reauthenticate	Reinitialize
N−1	Force Authorized	□	□	□	Globally Disabled	Reauthenticate	Reinitialize
N	Force Authorized	□	□	□	Globally Disabled	Reauthenticate	Reinitialize

Figure 11-2.1: The IEEE 802.1X Configuration

Parameter description:

System Configuration

- **Mode :**

  on or off.

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

- **Reauthentication Enabled :**

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

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

- **Reauthentication Period :**

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

- **EAPOL Timeout :**

  Determines the time for retransmission of Request Identity EAPOL frames.

  Valid values are in the range 1 to 65535 seconds. This has no effect for MAC-based ports.

- **Aging Period :**

  This setting applies to the following modes, i.e. modes using the Port Security functionality to secure MAC addresses:
  • Single 802.1X
  • Multi 802.1X
  • MAC-Based Auth.
  When the NAS module uses the Port Security module to secure MAC addresses, the Port Security module needs to check for activity on the MAC address in question at regular intervals and free resources if no activity is seen within a given period of time. This parameter controls exactly this period and can be set to a number between 10 and 1000000 seconds.
  If reauthentication is enabled and the port is in an 802.1X-based mode, this is not so critical, since supplicants that are no longer attached to the port will get removed upon the next reauthentication, which will fail. But if reauthentication is not enabled, the only way to free resources is by aging the entries.
  For ports in MAC-based Auth. mode, reauthentication doesn't cause direct communication between the switch and the client, so this will not detect whether the client is still attached or not, and the only way to free any resources is to age the entry.

- **Hold Time :**

  This setting applies to the following modes, i.e. modes using the Port Security functionality to secure MAC addresses:
  • Single 802.1X
  • Multi 802.1X
  • MAC-Based Auth.
  If a client is denied access - either because the RADIUS server denies the client access or

because the RADIUS server request times out (according to the timeout specified on the "Configuration→Security→AAA" page) - the client is put on hold in the Unauthorized state. The hold timer does not count during an on-going authentication. In MAC-based Auth. mode, the switch will ignore new frames coming from the client during the hold time.
The Hold Time can be set to a number between 10 and 1000000 seconds.

- **RADIUS-Assigned QoS Enabled :**

  RADIUS-assigned QoS provides a means to centrally control the traffic class to which traffic coming from a successfully authenticated supplicant is assigned on the switch. The RADIUS server must be configured to transmit special RADIUS attributes to take advantage of this feature (see RADIUS-Assigned QoS Enabled below for a detailed description).

  The "RADIUS-Assigned QoS Enabled" checkbox provides a quick way to globally enable/disable RADIUS-server assigned QoS Class functionality. When checked, the individual ports' ditto setting determine whether RADIUS-assigned QoS Class is enabled on that port. When unchecked, RADIUS-server assigned QoS Class is disabled on all ports.

- **RADIUS-Assigned VLAN Enabled :**

  RADIUS-assigned VLAN provides a means to centrally control the VLAN on which a successfully authenticated supplicant is placed on the switch. Incoming traffic will be classified to and switched on the RADIUS-assigned VLAN. The RADIUS server must be configured to transmit special RADIUS attributes to take advantage of this feature (see RADIUS-Assigned VLAN Enabled below for a detailed description).

  The "RADIUS-Assigned VLAN Enabled" checkbox provides a quick way to globally enable/disable RADIUS-server assigned VLAN functionality. When checked, the individual ports' ditto setting determine whether RADIUS-assigned VLAN is enabled on that port. When unchecked, RADIUS-server assigned VLAN is disabled on all ports.

- **Guest VLAN Enabled :**

  A Guest VLAN is a special VLAN - typically with limited network access - on which 802.1X-unaware clients are placed after a network administrator-defined timeout. The switch follows a set of rules for entering and leaving the Guest VLAN as listed below.
  The "Guest VLAN Enabled" checkbox provides a quick way to globally enable/disable Guest VLAN functionality. When checked, the individual ports' ditto setting determines whether the port can be moved into Guest VLAN. When unchecked, the ability to move to the Guest VLAN is disabled on all ports.

- **Guest VLAN ID :**

  This is the value that a port's Port VLAN ID is set to if a port is moved into the Guest VLAN. It is only changeable if the Guest VLAN option is globally enabled.
  Valid values are in the range [1; 4094].

- **Max. Reauth. Count :**

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

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

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

The value can only be changed if the Guest VLAN option is globally enabled.

Port Configuration

- **Port :**

  The port number for which the configuration below applies.

- **Admin State :**

  If 802.1X is globally enabled, this selection controls the port's authentication mode. The following modes are available:

  - **Force Authorized :**

    In this mode, the switch will send one EAPOL Success frame when the port link comes up, and any client on the port will be allowed network access without authentication.

  - **Force Unauthorized :**

    In this mode, the switch will send one EAPOL Failure frame when the port link comes up, and any client on the port will be disallowed network access.

  - **Port-based 802.1X :**

    In the 802.1X-world, the user is called the supplicant, the switch is the authenticator, and the RADIUS server is the authentication server. The authenticator acts as the man-in-the-middle, forwarding requests and responses between the supplicant and the authentication server. Frames sent between the supplicant and the switch are special 802.1X frames, known as EAPOL (EAP Over LANs) frames. EAPOL frames encapsulate EAP PDUs (RFC3748). Frames sent between the switch and the RADIUS server are RADIUS packets. RADIUS packets also encapsulate EAP PDUs together with other attributes like the switch's IP address, name, and the supplicant's port number on the switch. EAP is very flexible, in that it allows for different authentication methods, like MD5-Challenge, PEAP, and TLS. The important thing is that the authenticator (the switch) doesn't need to know which authentication method the supplicant and the authentication server are using, or how many information exchange frames are needed for a particular method. The switch simply encapsulates the EAP part of the frame into the relevant type (EAPOL or RADIUS) and forwards it.

    When authentication is complete, the RADIUS server sends a special packet containing a success or failure indication. Besides forwarding this decision to the supplicant, the switch uses it to open up or block traffic on the switch port connected to the supplicant

> **NOTE:** Suppose two backend servers are enabled and that the server timeout is configured to X seconds (using the AAA configuration page), and suppose that the first server in the list is currently down (but not considered dead).
>
> Now, if the supplicant retransmits EAPOL Start frames at a rate faster than X seconds, then it will never get authenticated, because the switch will cancel on-going backend authentication server requests whenever it receives a new EAPOL Start frame from the supplicant.
>
> And since the server hasn't yet failed (because the X seconds haven't expired), the same server will be contacted upon the next backend authentication server request from the switch. This scenario will loop forever. Therefore, the server timeout should be smaller than the supplicant's EAPOL Start frame retransmission rate.

  - **Single 802.1X :**

    In port-based 802.1X authentication, once a supplicant is successfully authenticated on a port, the whole port is opened for network traffic. This allows other clients connected to the port (for instance through a hub) to piggy-back on the successfully authenticated client and get network access even though they really aren't authenticated. To overcome this security breach, use the Single 802.1X variant. Single 802.1X is really not an IEEE standard, but features many of the same characteristics as does port-based 802.1X. In Single 802.1X, at most one supplicant can get authenticated on the port at a time. Normal EAPOL frames are used in the communication between the supplicant and the switch. If more than one supplicant is connected to a port, the one that comes first when the port's link comes up will be the first one considered. If that supplicant doesn't provide valid credentials within a certain amount of time, another supplicant will get a chance. Once a supplicant is successfully authenticated, only that supplicant will be allowed access. This is the most secure of all the supported modes. In this mode, the Port Security module is used to secure a supplicant's MAC address once successfully authenticated.

- **Multi 802.1X :**

  In port-based 802.1X authentication, once a supplicant is successfully authenticated on a port, the whole port is opened for network traffic. This allows other clients connected to the port (for instance through a hub) to piggy-back on the successfully authenticated client and get network access even though they really aren't authenticated. To overcome this security breach, use the Multi 802.1X variant.

  Multi 802.1X is really not an IEEE standard, but features many of the same characteristics as does port-based 802.1X. Multi 802.1X is - like Single 802.1X - not an IEEE standard, but a variant that features many of the same characteristics. In Multi 802.1X, one or more supplicants can get authenticated on the same port at the same time. Each supplicant is authenticated individually and secured in the MAC table using the Port Security module.

  In Multi 802.1X it is not possible to use the multicast BPDU MAC address as destination MAC address for EAPOL frames sent from the switch towards the supplicant, since that would cause all supplicants attached to the port to reply to requests sent from the switch. Instead, the switch uses the supplicant's MAC address, which is obtained from the first EAPOL Start or EAPOL Response Identity frame sent by the supplicant. An exception to this is when no supplicants are attached. In this case, the switch sends EAPOL Request Identity frames using the BPDU multicast MAC address as destination - to wake up any supplicants that might be on the port.

  The maximum number of supplicants that can be attached to a port can be limited using the Port Security Limit Control functionality.

- **MAC-based Auth.:**

  Unlike port-based 802.1X, MAC-based authentication is not a standard, but merely a best-practices method adopted by the industry. In MAC-based authentication, users are called clients, and the switch acts as the supplicant on behalf of clients. The initial frame (any kind of frame) sent by a client is snooped by the switch, which in turn uses the client's MAC address as both username and password in the subsequent EAP exchange with the RADIUS server. The 6-byte MAC address is converted to a string on the following form "xx-xx-xx-xx-xx-xx", that is, a dash (-) is used as separator between the lower-cased hexadecimal digits. The switch only supports the MD5-Challenge authentication method, so the RADIUS server must be configured accordingly.

  When authentication is complete, the RADIUS server sends a success or failure indication, which in turn causes the switch to open up or block traffic for that particular client, using the Port Security module. Only then will frames from the client be forwarded on the switch. There are no EAPOL frames involved in this authentication, and therefore, MAC-based Authentication has nothing to do with the 802.1X standard.

  The advantage of MAC-based authentication over port-based 802.1X is that several clients can be connected to the same port (e.g. through a 3rd party switch or a hub) and still require individual authentication, and that the clients don't need special supplicant software to authenticate. The advantage of MAC-based authentication over 802.1X-based authentication is that the clients don't need special supplicant software to authenticate. The disadvantage is that MAC addresses can be spoofed by malicious users - equipment whose MAC address is a valid RADIUS user can be used by anyone. Also, only the MD5-Challenge method is supported. The maximum number of clients that can be attached to a port can be limited using the Port Security Limit Control functionality.

- **RADIUS-Assigned QoS Enabled**

When RADIUS-Assigned QoS is both globally enabled and enabled (checked) on a given port, the switch reacts to QoS Class information carried in the RADIUS Access-Accept packet transmitted by the RADIUS server when a supplicant is successfully authenticated. If present and valid, traffic received on the supplicant's port will be classified to the given QoS Class. If (re-)authentication fails or the RADIUS Access-Accept packet no longer carries a QoS Class or it's invalid, or the supplicant is otherwise no longer present on the port, the port's QoS Class is immediately reverted to the original QoS Class (which may be changed by the administrator in the meanwhile without affecting the RADIUS-assigned).
This option is only available for single-client modes, i.e.
• Port-based 802.1X
• Single 802.1X

RADIUS attributes used in identifying a QoS Class:
The User-Priority-Table attribute defined in RFC4675 forms the basis for identifying the QoS Class in an Access-Accept packet.
Only the first occurrence of the attribute in the packet will be considered, and to be valid, it must follow this rule:
• All 8 octets in the attribute's value must be identical and consist of ASCII characters in the range '0' - '7', which translates into the desired QoS Class in the range [0; 7].

- **RADIUS-Assigned VLAN Enabled**

When RADIUS-Assigned VLAN is both globally enabled and enabled (checked) for a given port, the switch reacts to VLAN ID information carried in the RADIUS Access-Accept packet transmitted by the RADIUS server when a supplicant is successfully authenticated. If present and valid, the port's Port VLAN ID will be changed to this VLAN ID, the port will be set to be a member of that VLAN ID, and the port will be forced into VLAN unaware mode. Once assigned, all traffic arriving on the port will be classified and switched on the RADIUS-assigned VLAN ID.
If (re-)authentication fails or the RADIUS Access-Accept packet no longer carries a VLAN ID or it's invalid, or the supplicant is otherwise no longer present on the port, the port's VLAN ID is immediately reverted to the original VLAN ID (which may be changed by the administrator in the meanwhile without affecting the RADIUS-assigned).
This option is only available for single-client modes, i.e.
• Port-based 802.1X
• Single 802.1X
For trouble-shooting VLAN assignments, use the "Monitor→VLANs→VLAN Membership and VLAN Port" pages. These pages show which modules have (temporarily) overridden the current Port VLAN configuration.

RADIUS attributes used in identifying a VLAN ID:
RFC2868 and RFC3580 form the basis for the attributes used in identifying a VLAN ID in an Access-Accept packet. The following criteria are used:
• The Tunnel-Medium-Type, Tunnel-Type, and Tunnel-Private-Group-ID attributes must all be present at least once in the Access-Accept packet.

• The switch looks for the first set of these attributes that have the same Tag value and fulfil the following requirements (if Tag == 0 is used, the Tunnel-Private-Group-ID does not need to include a Tag):
- Value of Tunnel-Medium-Type must be set to "IEEE-802" (ordinal 6).
- Value of Tunnel-Type must be set to "VLAN" (ordinal 13).
- Value of Tunnel-Private-Group-ID must be a string of ASCII chars in the range '0' - '9', which is interpreted as a decimal string representing the VLAN ID. Leading '0's are discarded. The final value must be in the range [1; 4095].

- **Guest VLAN Enabled**

When Guest VLAN is both globally enabled and enabled (checked) for a given port, the switch considers moving the port into the Guest VLAN according to the rules outlined below.
This option is only available for EAPOL-based modes, i.e.:
• Port-based 802.1X
• Single 802.1X
• Multi 802.1X
For trouble-shooting VLAN assignments, use the "Monitor→VLANs→VLAN Membership and VLAN Port" pages. These pages show which modules have (temporarily) overridden the current Port VLAN configuration.
Guest VLAN Operation:
When a Guest VLAN enabled port's link comes up, the switch starts transmitting EAPOL Request Identity frames. If the number of transmissions of such frames exceeds Max. Reauth. Count and no EAPOL frames have been received in the meanwhile, the switch considers entering the Guest VLAN. The interval between transmission of EAPOL Request Identity frames is configured with EAPOL Timeout. If Allow Guest VLAN if EAPOL Seen is enabled, the port will now be placed in the Guest VLAN. If disabled, the switch will first check its history to see if an EAPOL frame has previously been received on the port (this history is cleared if the port link goes down or the port's Admin State is changed), and if not, the port will be placed in the Guest VLAN. Otherwise it will not move to the Guest VLAN, but continue transmitting EAPOL Request Identity frames at the rate given by EAPOL Timeout.
Once in the Guest VLAN, the port is considered authenticated, and all attached clients on the port are allowed access on this VLAN. The switch will not transmit an EAPOL Success frame when entering the Guest VLAN.
While in the Guest VLAN, the switch monitors the link for EAPOL frames, and if one such frame is received, the switch immediately takes the port out of the Guest VLAN and starts authenticating the supplicant according to the port mode. If an EAPOL frame is received, the port will never be able to go back into the Guest VLAN if the "Allow Guest VLAN if EAPOL Seen" is disabled.

- **Port State :**

The current state of the port. It can undertake one of the following values:

Globally Disabled: IEEE 802.1X is globally disabled.

Link Down: IEEE 802.1X is globally enabled, but there is no link on the port.

Authorized: The port is in Force Authorized or a single-supplicant mode and the supplicant is authorized.

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

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

- **Restart :**

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

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

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

The button only has effect for successfully authenticated clients on the port and will not cause the clients to get temporarily unauthorized.

Reinitialize: Forces a re-initialization of the clients on the port and thereby a re-authentication immediately. The clients will transfer to the unauthorized state while the re-authentication is in progress.

Buttons

- **Apply :**

  Click to save changes.

- **Reset :**

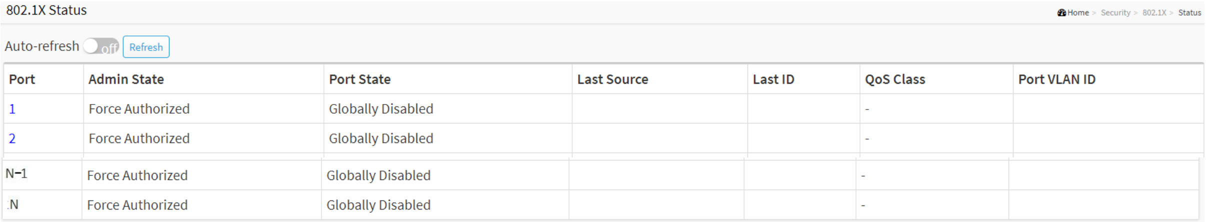
  Click to undo any changes made locally and revert to previously saved values.

11-2.2 Status

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

Web Interface

To displays 802.1X Status in the web interface:
Click Security, IEEE 802.1X and Status.
Checked “Auto-refresh”.
Click “Refresh” to refresh the port detailed statistics.
You can select which port that you want display 802.1X Statistics.



802.1X Status

Port	Admin State	Port State	Last Source	Last ID	QoS Class	Port VLAN ID
1	Force Authorized	Globally Disabled			-	
2	Force Authorized	Globally Disabled			-	
N-1	Force Authorized	Globally Disabled			-	
N	Force Authorized	Globally Disabled			-	

Figure 11-2.2: The IEEE 802.1X Status

Parameter description:

802.1X Status

- **Port :**

  The switch port number. Click to navigate to detail 802.1X statistics for this port.

- **Admin State :**

  The port's current administrative state. Refer to 802.1X Admin State for a description of possible values.

- **Port State :**

The current state of the port. Refer to 802.1X Port State for a description of the individual states.

- **Last Source :**

  The source MAC address carried in the most recently received EAPOL frame for EAPOL-based authentication, and the most recently received frame from a new client for MAC-based authentication.

- **Last ID :**

  The user name (supplicant identity) carried in the most recently received Response Identity EAPOL frame for EAPOL-based authentication, and the source MAC address from the most recently received frame from a new client for MAC-based authentication.

- **QoS Class :**

  QoS Class assigned to the port by the RADIUS server if enabled.

- **Port VLAN ID :**

  The VLAN ID that 802.1X has put the port in. The field is blank, if the Port VLAN ID is not overridden by 802.1X.

  If the VLAN ID is assigned by the RADIUS server, "(RADIUS-assigned)" is appended to the VLAN ID. Read more about RADIUS-assigned VLANs here.

  If the port is moved to the Guest VLAN, "(Guest)" is appended to the VLAN ID. Read more about Guest VLANs here.

Buttons

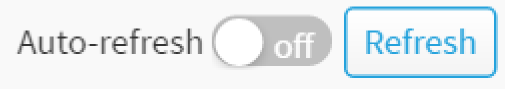


Figure 11-2.2: The IEEE 802.1X Status buttons

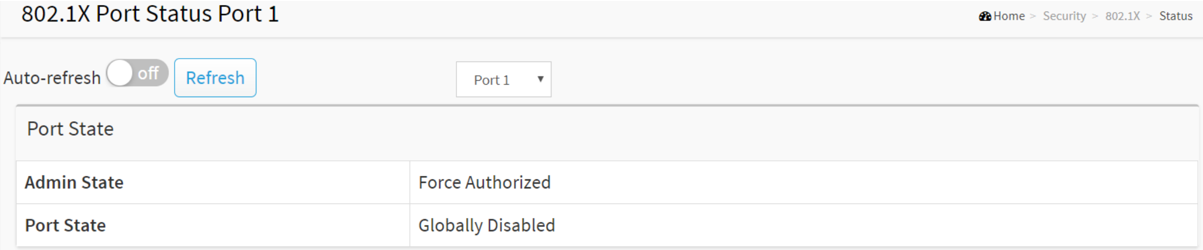
- **Auto-refresh :**

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

- **Refresh :**

  Click to refresh the page immediately.

- **If you select port1 to display 802.1X Statistics.**



802.1X Port Status Port 1

Port State

Admin State	Force Authorized
Port State	Globally Disabled

Figure 11-2.2: The 802.1X Statistics Port 1

Parameter description:

- **Port :**

You can select which port that you want display 802.1X Statistics.

- **Admin State :**

  The port's current administrative state. Refer to 802.1X Admin State for a description of possible values.

- **Port State :**

  The current state of the port. Refer to 802.1X Port State for a description of the individual states.

Buttons

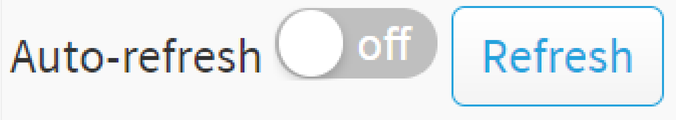


Figure 11-2.2: The IEEE 802.1X Statistics Port buttons

- **Auto-refresh :**

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

- **Refresh :**

  Click to refresh the page.

11-3 IP Source Guard

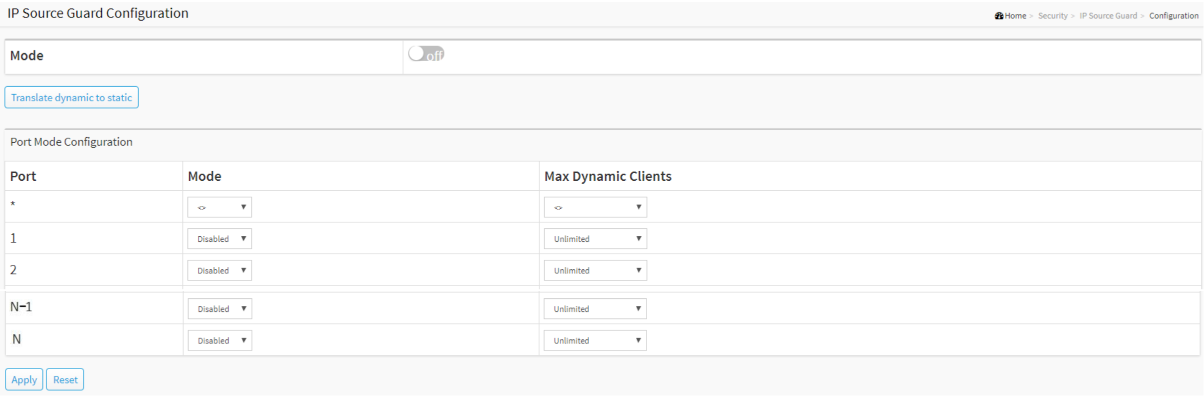
The section describes to configure the IP Source Guard detail parameters of the switch. You could use the IP Source Guard configure to enable or disable with the Port of the switch.

11-3.1 Configuration

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

Web Interface

To configure an IP Source Guard Configuration in the web interface:
Click Security, IP Source Guard and Configuration.
Select "on" in the Mode of IP Source Guard Configuration.
Select "Enabled" of the specific port in the Mode of Port Mode Configuration.
Select Maximum Dynamic Clients (0, 1, 2, Unlimited) of the specific port in the Mode of Port Mode Configuration.
Click Apply.



IP Source Guard Configuration

Home > Security > IP Source Guard > Configuration

Mode	off

Translate dynamic to static

Port Mode Configuration

Port	Mode	Max Dynamic Clients
*	<>	<>
1	Disabled	Unlimited
2	Disabled	Unlimited
N-1	Disabled	Unlimited
N	Disabled	Unlimited

Figure 11-3.1: The IP Source Guard Configuration

Parameter description :

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

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

- **Port Mode Configuration :**

  Specify IP Source Guard is enabled on which ports. Only when both Global Mode and Port Mode on a given port are enabled, IP Source Guard is enabled on this given port.

- **Max Dynamic Clients :**

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

Buttons

- **Apply :**

  Click to save changes.

- **Reset :**

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

- **Translate dynamic to static :**

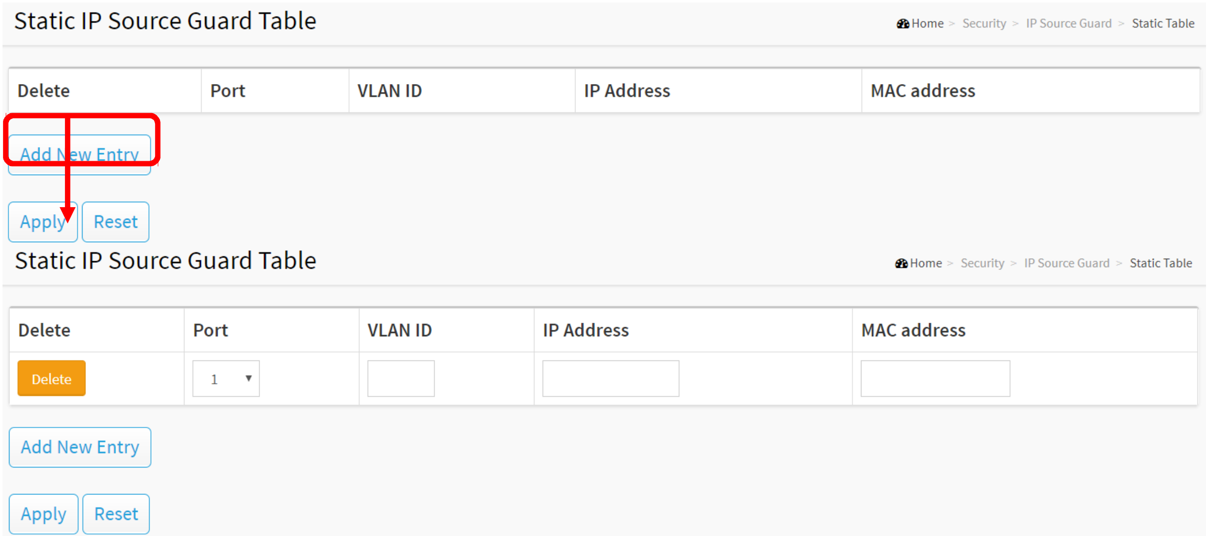
  Click to translate all dynamic entries to static entries.

11-3.2 Static Table

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

Web Interface

To configure a Static IP Source Guard Table Configuration in the web interface:
Click Security, IP Source Guard and Static Table.
Click “Add New Entry”.
Specify the Port, VLAN ID, IP Address, and MAC address in the entry.
Click Apply.



Static IP Source Guard Table

Home > Security > IP Source Guard > Static Table

Delete	Port	VLAN ID	IP Address	MAC address

Static IP Source Guard Table

Home > Security > IP Source Guard > Static Table

Delete	Port	VLAN ID	IP Address	MAC address
Delete	1			

Figure 11-3.2: The Static IP Source Guard Table

Parameter description:

- **Port :**

  The logical port for the settings.

- **VLAN ID :**

  The vlan id for the settings.

- **IP Address :**

  Allowed Source IP address.

- **MAC address :**

  Allowed Source MAC address.

Buttons

- **Add New Entry :**

  Click to add a new entry to the Static IP Source Guard table. Specify the Port, IP address, and MAC address for the new entry. Click "Apply".

- **Delete :**

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

- **Apply :**

Click to save changes.

- **Reset :**

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

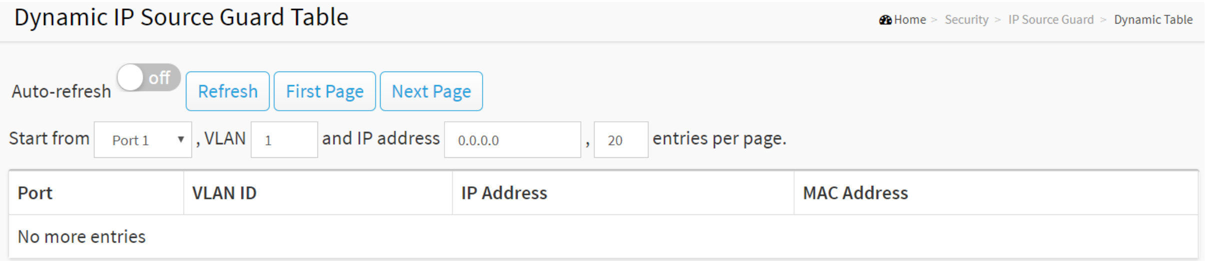
11-3.3 Dynamic Table

Entries in the Dynamic IP Source Guard Table are shown on this page. The Dynamic IP Source Guard Table is sorted first by port, then by IP address, and then by MAC address.

Web Interface

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

1. Click Security, IP Source Guard and Dynamic Table.
2. Checked "Auto-refresh".
3. Click "Refresh" to refresh the port detailed statistics.
4. Click First/Next Page to change page.
5. Specify the Start from port, VLAN, IP Address, and entries per page.



Dynamic IP Source Guard Table

Start from Port 1, VLAN 1 and IP address 0.0.0.0, 20 entries per page.

Port	VLAN ID	IP Address	MAC Address
No more entries			

Figure 11-3.3: The Dynamic IP Source Guard Table

Parameter description:

Navigating the IP Source Guard Table :

Each page shows up to 99 entries from the Dynamic IP Source Guard table, default being 20, selected through the "entries per page" input field. When first visited, the web page will show the first 20 entries from the beginning of the Dynamic IP Source Guard Table. The "Start from port address", "VLAN" and "IP address" input fields allow the user to select the starting point in the Dynamic IP Source Guard Table. Clicking "Refresh" the button will update the displayed table starting from that or the closest next Dynamic IP Source Guard Table match. In addition, the two input fields will - upon a "Refresh" button click - assume the value of the first displayed entry, allowing for continuous refresh with the same start address.

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

- **Port :**

  Switch Port Number for which the entries are displayed.

- **VLAN ID :**

  VLAN-ID in which the IP traffic is permitted.

- **IP Address :**

  User IP address of the entry.

- **MAC Address :**

  Source MAC address.

- **Show entries :**

  You can choose how many items you want to show.

Buttons

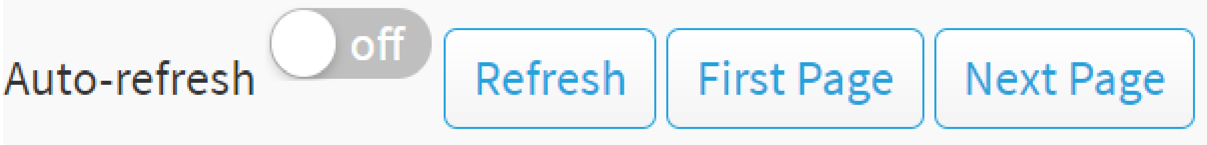


Figure 11-3.3: The Dynamic IP Source Guard Table buttons

- **Auto-refresh :**

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

- **Refresh :**

  Click to refresh the page immediately.

- **First Page :**

  Updates the system log entries, turn to the first page.

- **Next Page :**

  Updates the group information entries, turn to the next page.

11-4 ARP Inspection

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

11-4.1 Configuration

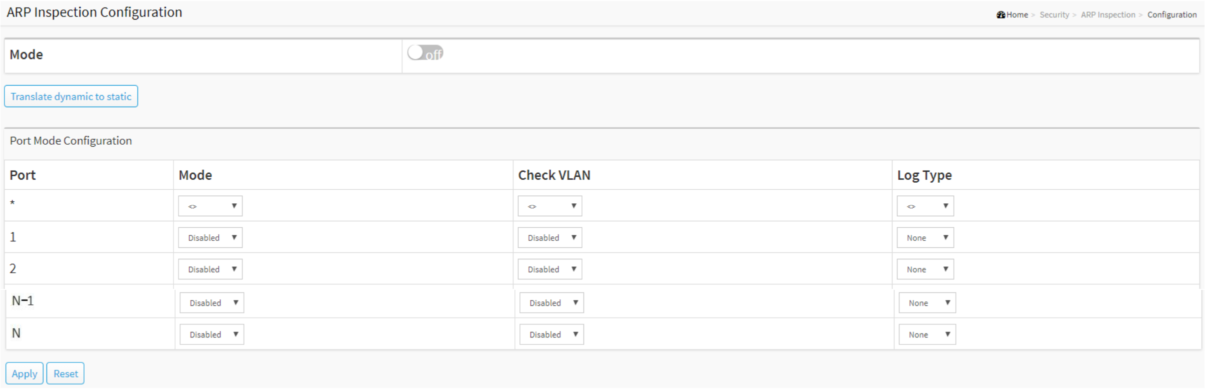
This section describes how to configure ARP Inspection setting including：
Mode (on and off)
Port (Enabled and Disabled)

Web Interface

To configure an ARP Inspection Configuration in the web interface:

1. Click Security, ARP Inspection and Configuration.

Select “on” in the Mode of ARP Inspection Configuration.
Select “Enabled” of the specific port in the Mode of Port Mode Configuration.
Click Apply.



ARP Inspection Configuration

Home > Security > ARP Inspection > Configuration

Mode: off

Translate dynamic to static

Port Mode Configuration

Port	Mode	Check VLAN	Log Type
*	<> ▼	<> ▼	<> ▼
1	Disabled ▼	Disabled ▼	None ▼
2	Disabled ▼	Disabled ▼	None ▼
N-1	Disabled ▼	Disabled ▼	None ▼
N	Disabled ▼	Disabled ▼	None ▼

Apply Reset

Figure 11-4.1: The ARP Inspection Configuration

Parameter description:

- **Mode of ARP Inspection Configuration :**

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

- **Port Mode Configuration :**

  Specify ARP Inspection is enabled on which ports. Only when both Global Mode and Port Mode on a given port are enabled, ARP Inspection is enabled on this given port. Possible modes are:
  Enabled: Enable ARP Inspection operation.
  Disabled: Disable ARP Inspection operation.
  If you want to inspect the VLAN configuration, you have to enable the setting of "Check VLAN". The default setting of "Check VLAN" is disabled. When the setting of "Check VLAN" is disabled, the log type of ARP Inspection will refer to the port setting. And the setting of "Check VLAN" is enabled, the log type of ARP Inspection will refer to the VLAN setting.
  Possible setting of "Check VLAN" are:
  Enabled: Enable check VLAN operation.
  Disabled: Disable check VLAN operation.
  Only the Global Mode and Port Mode on a given port are enabled, and the setting of "Check VLAN" is disabled, the log type of ARP Inspection will refer to the port setting.

There are four log types and possible types are:
None: Log nothing.
Deny: Log denied entries.
Permit: Log permitted entries.
ALL: Log all entries.

- **Check VLAN :**

  If you want to inspect the VLAN configuration, you have to enable the setting of "Check VLAN". The default setting of "Check VLAN" is disabled. When the setting of "Check VLAN" is disabled, the log type of ARP Inspection will refer to the port setting. And the setting of "Check VLAN" is enabled, the log type of ARP Inspection will refer to the VLAN setting.
  Possible setting of "Check VLAN" are:
  Enabled: Enable check VLAN operation.
  Disabled: Disable check VLAN operation.

- **Log Type :**

  Only the Global Mode and Port Mode on a given port are enabled, and the setting of "Check VLAN" is disabled, the log type of ARP Inspection will refer to the port setting.
  There are four log types and possible types are:
  None: Log nothing.
  Deny: Log denied entries.
  Permit: Log permitted entries.
  ALL: Log all entries.

Buttons

- **Apply :**

  Click to save changes.

- **Reset :**

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

- **Translate dynamic to static :**

  Click to translate all dynamic entries to static entries.

11-4.2 VLAN Configuration

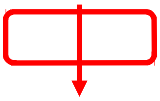
Specify ARP Inspection is enabled on which VLANs

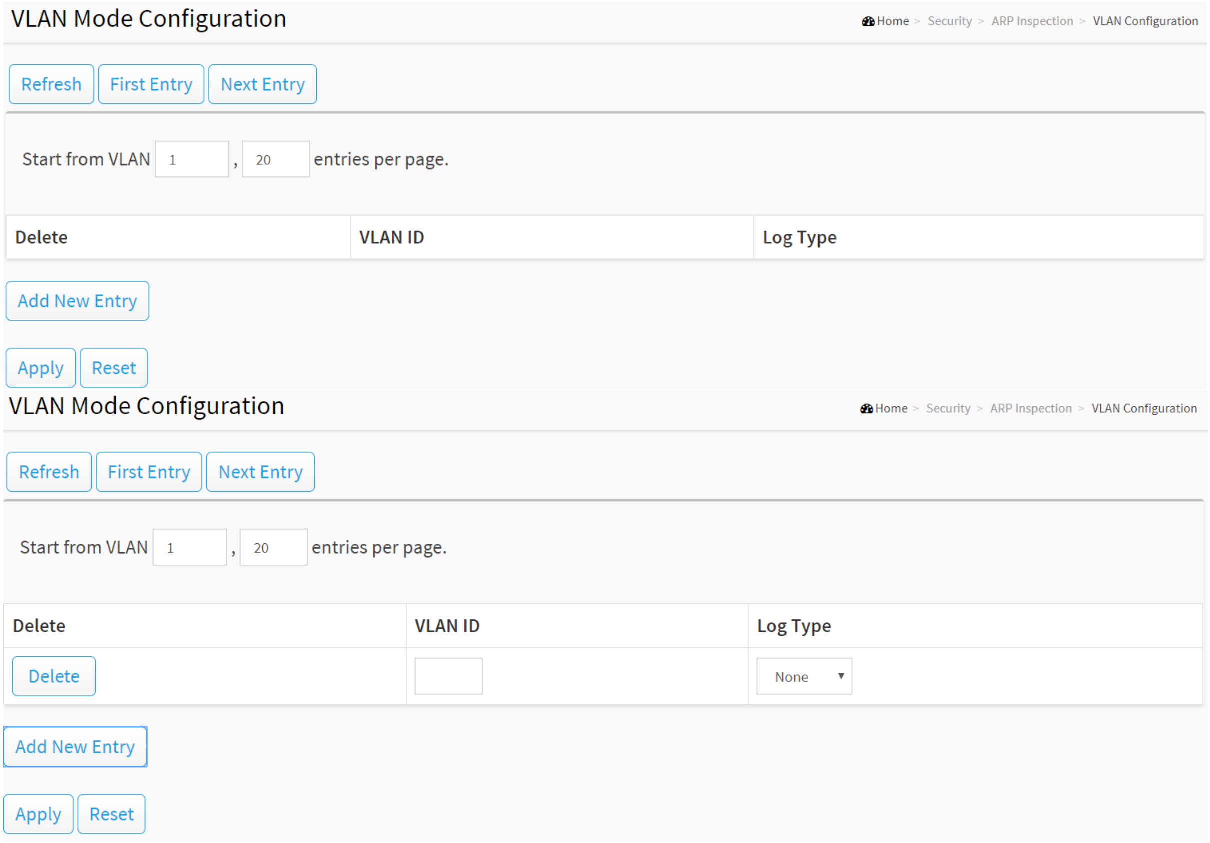
Web Interface

To configure a VLAN Mode Configuration in the web interface:

1. Click Security, ARP Inspection and VLAN Configuration.

Click “Add new entry”.
Specify the VLAN ID, Log Type.
Click Apply.
Click First Entry/Next Entry to change Entry.





VLAN Mode Configuration

Home > Security > ARP Inspection > VLAN Configuration
Refresh
First Entry
Next Entry

Start from VLAN 1 , 20 entries per page.

Delete	VLAN ID	Log Type

Add New Entry
Apply
Reset

VLAN Mode Configuration

Home > Security > ARP Inspection > VLAN Configuration
Refresh
First Entry
Next Entry

Start from VLAN 1 , 20 entries per page.

Delete	VLAN ID	Log Type
Delete		None

Add New Entry
Apply
Reset

Figure 11-4.2: The VLAN Mode Configuration

Parameter description:

- **Navigating the VLAN Configuration**

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

- **VLAN Mode Configuration :**

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

Buttons

- **Add New Entry :**

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

- **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.

- **First Entry :**

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

- **Next Entry :**

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

- **Refresh :**

  Click to refresh the page immediately.

11-4.3 Static Table

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

Web Interface

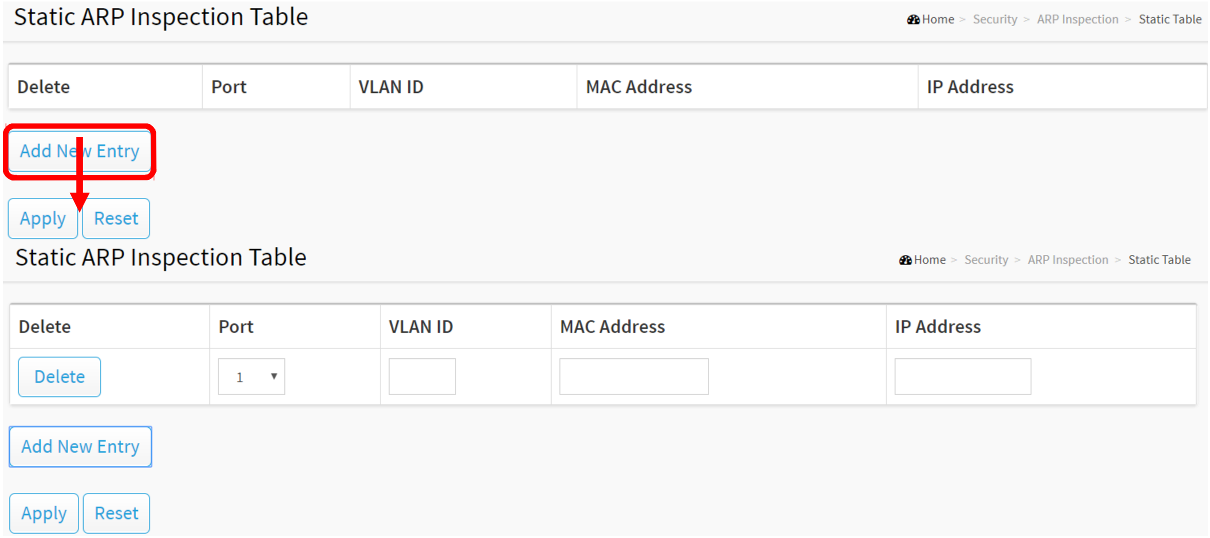
To configure a Static ARP Inspection Table Configuration in the web interface:

Click Security, ARP Inspection and Static Table.

Click “Add new entry”.

Specify the Port, VLAN ID, IP Address, MAC address and IP Address in the entry.

Click Apply.



Static ARP Inspection Table

Home > Security > ARP Inspection > Static Table

Delete	Port	VLAN ID	MAC Address	IP Address

Static ARP Inspection Table

Home > Security > ARP Inspection > Static Table

Delete	Port	VLAN ID	MAC Address	IP Address
Delete	1 ▾			

Figure11-4.3: The Static ARP Inspection Table

Parameter description:

- **Port :**

  The logical port for the settings.

- **VLAN ID :**

  The vlan id for the settings.

- **MAC Address :**

  Allowed Source MAC address in ARP request packets.

- **IP Address :**

  Allowed Source IP address in ARP request packets.

Buttons

- **Add New Entry :**

  Click to add a new entry to the Static ARP Inspection table.

- **Delete :**

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

- **Apply :**

  Click to save changes.

- **Reset :**

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

11-4.4 Dynamic Table

Entries in the Dynamic ARP Inspection Table are shown on this page. The Dynamic ARP Inspection Table contains up to 256 entries, and is sorted first by port, then by VLAN ID, then by MAC address, and then by IP address. All dynamic entries are learning from DHCP Snooping.

Navigating the ARP Inspection Table

Each page shows up to 99 entries from the Dynamic ARP Inspection table, default being 20, selected through the "entries per page" input field. When first visited, the web page will show the first 20 entries from the beginning of the Dynamic ARP Inspection Table.

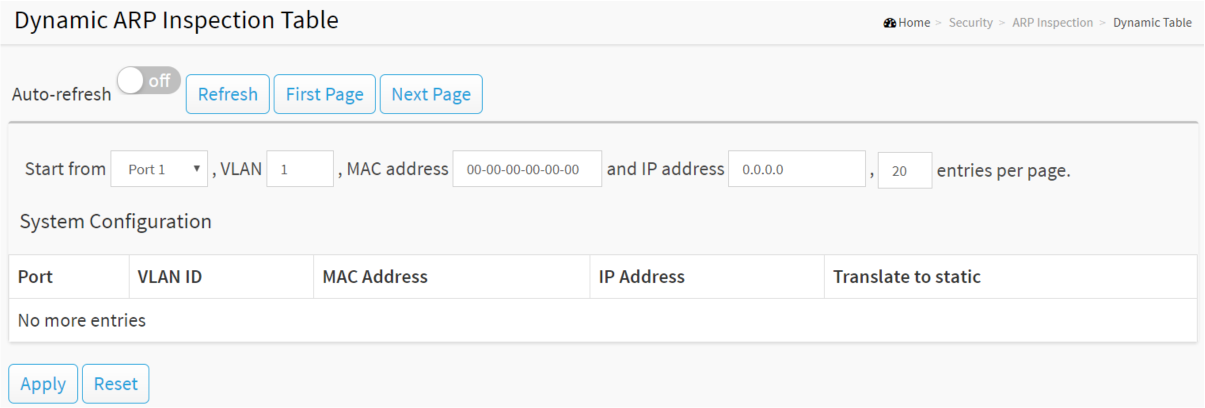
The "Start from port address", "VLAN", "MAC address" and "IP address" input fields allow the user to select the starting point in the Dynamic ARP Inspection Table. Clicking the "Refresh" button will update the displayed table starting from that or the closest next Dynamic ARP Inspection Table match.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

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

Web Interface

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

1. Click Security, ARP Inspection and Dynamic Table.
2. Checked "Auto-refresh".
3. Click "Refresh" to refresh the port detailed statistics.
4. Click First/Next Page to change page.
5. Specify the Start from port, VLAN, MAC Address, IP Address, and entries per page.



Dynamic ARP Inspection Table

Home > Security > ARP Inspection > Dynamic Table

Start from Port 1 , VLAN 1 , MAC address 00-00-00-00-00-00 and IP address 0.0.0.0 , 20 entries per page.

System Configuration

Port	VLAN ID	MAC Address	IP Address	Translate to static
No more entries				

Figure 11-4.4: The Dynamic ARP Inspection Table

Parameter description:

ARP Inspection Table Columns

- **Port :**

  Switch Port Number for which the entries are displayed.

- **VLAN ID :**

  VLAN ID in which the ARP traffic is permitted.

- **MAC Address :**

  User MAC address of the entry.

- **IP Address :**

  User IP address of the entry.

- **Show entries :**

  You can choose how many items you want to show up.

Buttons

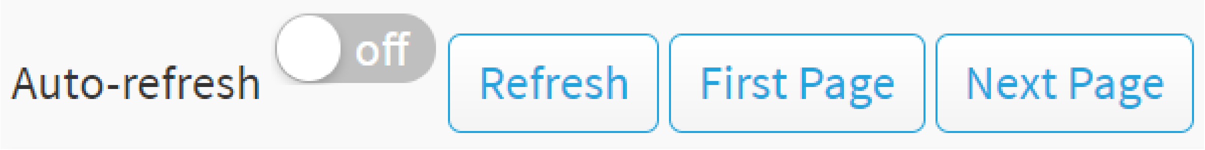


Figure 11-4.4: The Dynamic ARP Inspection Table buttons

- **Auto-refresh :**

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

- **Refresh :**

  Click to refresh the page immediately.

- **First Page :**

  Updates the system log entries, turn to the first page.

- **Next Page :**

  Updates the group information entries, turn to the next page.

11-5 Port Security

11-5.1 Configuration

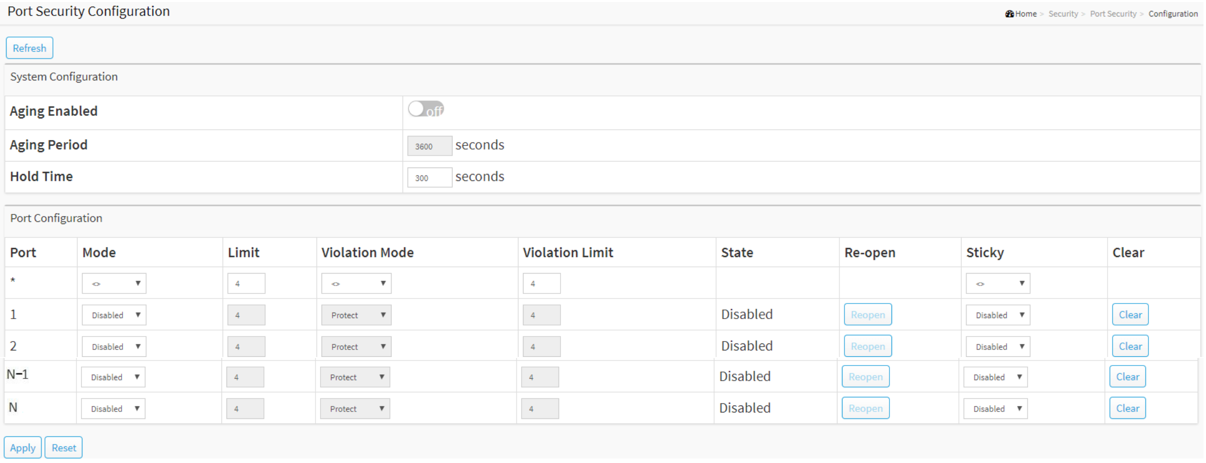
This section shows you to configure the Port Security settings of the Switch. You can use the Port Security feature to restrict input to an interface by limiting and identifying MAC addresses.

Web Interface

To configure a Port Security Configuration in the web interface:

Click Security, Port Security and Configuration.

1. Click to Enable the Aging to specify Aging Period.
2. Set Mode (Enabled, Disabled), Limit, Violation Mode, Violation Limit for each port.
3. Click the Apply to save the setting.
4. If you want to cancel the setting then you need to click the Reset button. It will revert to previously saved values.



Port Security Configuration

System Configuration

Aging Enabled	off
Aging Period	3600 seconds
Hold Time	300 seconds

Port Configuration

Port	Mode	Limit	Violation Mode	Violation Limit	State	Re-open	Sticky	Clear
*	<>	4	<>	4			<>	
1	Disabled	4	Protect	4	Disabled	Reopen	Disabled	Clear
2	Disabled	4	Protect	4	Disabled	Reopen	Disabled	Clear
N-1	Disabled	4	Protect	4	Disabled	Reopen	Disabled	Clear
N	Disabled	4	Protect	4	Disabled	Reopen	Disabled	Clear

Figure 11-5.1: The Port Security Configuration

Parameter description:

System Configuration

- **Aging Enabled :**

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

- **Aging Period :**

If Aging Enabled is checked, then the aging period is controlled with this input. If other modules are using the underlying functionality for securing MAC addresses, they may have other requirements to the aging period. The underlying functionality will use the shorter requested aging period of all modules that have aging enabled. The Aging Period can be set to a number between 10 and 10000000seconds with a default of 3600 seconds.

To understand why aging may be desired, consider the following scenario: Suppose an end-host is connected to a 3rd party switch or hub, which in turn is connected to a port on this switch on which Port Security is enabled. The end-host will be allowed to forward if the limit is not exceeded. Now suppose that the end-host logs off or powers down. If it wasn't for aging, the end-host would still take up resources on this switch and will be allowed to forward. To overcome this situation, enable aging. With aging enabled, a timer is started once the end-host gets secured. When the timer expires, the switch starts looking for frames from the end-host, and if such frames are not seen within the next Aging Period, the end-host is assumed to be disconnected, and the corresponding resources are freed on the switch.

- **Hold Time :**

  The hold time - measured in seconds - is used to determine how long a MAC address is held in the MAC table if it has been found to violate the limit. Valid range is between 10 and 10000000 seconds with a default of 300 seconds. The reason for holding a violating MAC address in the MAC table is primarily to ensure that the same MAC address doesn't give rise to continuous notifications (if notifications on violation count is enabled).

Port Configuration

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

- **Port :**

  The port number to which the configuration below applies.

- **Mode :**

  Controls whether Limit Control is enabled on this port. Both this and the Global Mode must be set to Enabled for Limit Control to be in effect. Notice that other modules may still use the underlying port security features without enabling Limit Control on a given port.

- **Limit :**

  The maximum number of MAC addresses that can be secured on this port. This number cannot exceed 1024. If the limit is exceeded, the corresponding action is taken. The switch is "born" with a total number of MAC addresses from which all ports draw whenever a new MAC address is seen on a Port Security-enabled port. Since all ports draw from the same pool, it may happen that a configured maximum cannot be granted, if the remaining ports have already used all available MAC addresses.

- **Violation Mode :**

  If Limit is reached, the switch can take one of the following actions:
  Protect: Do not allow more than Limit MAC addresses on the port, but take no further action.
  Restrict: If Limit is reached, subsequent MAC addresses on the port will be counted and marked as violating. Such MAC addreses are removed from the MAC table when the hold time expires. At most Violation Limit MAC addresses can be marked as violating at any given time.
  Shutdown: If Limit is reached, one additional MAC address will cause the port to be shut down. This implies that all secured MAC addresses be removed from the port, and no new addresses be learned. There are three ways to re-open the port:
  1) In the "Configuration→Ports" page's "Configured" column, first disable the port, then restore the original mode.
  2) Make a Port Security configuration change on the port.
  3) Boot the switch.

- **Violation Limit**

  The maximum number of MAC addresses that can be marked as violating on this port. This number cannot exceed 1023. Default is 4. It is only used when Violation Mode is Restrict.

- **State :**

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

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

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

Limit Reached: Indicates that the limit is reached on this port. This state can only be shown if Action is set to none or Trap.

Shutdown: Indicates that the port is shut down by the Limit Control module. This state can only be shown if Action is set to Shutdown or Trap & Shutdown.

Buttons

- **Apply :**

  Click to save changes.

- **Reset :**

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

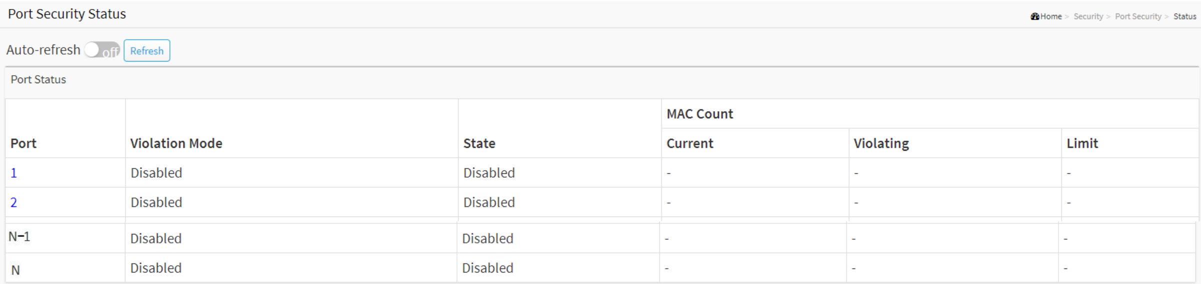
11-5.2 Status

This section shows the Port Security status. Port Security is a module with no direct configuration. Configuration comes indirectly from other modules - the user modules. When a user module has enabled port security on a port, the port is set-up for software-based learning. In this mode, frames from unknown MAC addresses are passed on to the port security module, which in turn asks all user modules whether to allow this new MAC address to forward or block it. For a MAC address to be set in the forwarding state, all enabled user modules must unanimously agree on allowing the MAC address to forward. If only one chooses to block it, it will be blocked until that user module decides otherwise. The status page is divided into two sections - one with a legend of user modules and one with the actual port status.

Web Interface

To displays a Port Security Status in the web interface:
Click Security, Port Security and status.

1. Checked "Auto-refresh".
2. Click "Refresh" to refresh the port detailed statistics.
3. Click the port number to see the status for this particular port.



Port Status

Port	Violation Mode	State	MAC Count		
			Current	Violating	Limit
1	Disabled	Disabled	-	-	-
2	Disabled	Disabled	-	-	-
N-1	Disabled	Disabled	-	-	-
N	Disabled	Disabled	-	-	-

Figure 11-5.2: The Port Security Status

Parameter description:

- **Port :**

  The port number for which the status applies. Click the port number to see the status for this particular port.

- **Violation Mode**

  Shows the configured Violation Mode of the port. It can take one of four values:

Disabled: Port Security is not administratively enabled on this port.
Protect: Port Security is administratively enabled in Protect mode.
Restrict: Port Security is administratively enabled in Restrict mode.
Shutdown: Port Security is administratively enabled in Shutdown mode.

- **State :**

  Shows the current state of the port. It can take one of four values:

  Disabled: No user modules are currently using the Port Security service.

  Ready: The Port Security service is in use by at least one user module, and is awaiting frames from unknown MAC addresses to arrive.

  Limit Reached: The Port Security service is enabled by at least the Limit Control user module, and that module has indicated that the limit is reached and no more MAC addresses should be taken in.

  Shutdown: The Port Security service is enabled by at least the Limit Control user module, and that module has indicated that the limit is exceeded. No MAC addresses can be learned on the port until it is administratively re-opened on the Limit Control configuration Web-page.

- **MAC Count (Current, Violating, Limit)**

  The three columns indicate the number of currently learned MAC addresses (forwarding as well as blocked), the number of violating MAC address (only counting in Restrict mode) and the maximum number of MAC addresses that can be learned on the port, respectively. If no user modules are enabled on the port, the Current column will show a dash (-). If Port Security is not administratively enabled on the port, the Violating and Limit columns will show a dash (-).

Buttons

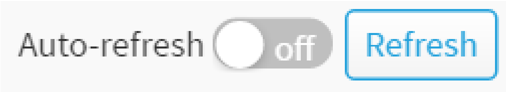


Figure 11-5.2: The Port Security Status buttons

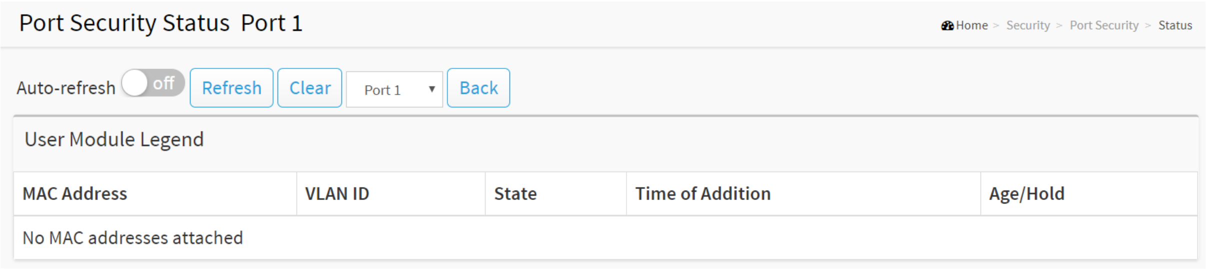
- **Auto-refresh :**

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

- **Refresh :**

  Click to refresh the page immediately.

■ **Click the port number to see the status for this particular port.**


Port Security Status Port 1

User Module Legend

MAC Address	VLAN ID	State	Time of Addition	Age/Hold
No MAC addresses attached				

Figure 11-5.2: The Port Security Status

Parameter description:

- **MAC Address & VLAN ID :**

  The MAC address and VLAN ID that is seen on this port. If no MAC addresses are learned, a single row stating "No MAC addresses attached" is displayed.

- **State :**

  Indicates whether the corresponding MAC address is blocked or forwarding. In the blocked state, it will not be allowed to transmit or receive traffic.

- **Time of Addition :**

  Shows the date and time when this MAC address was first seen on the port.

- **Age/Hold :**

  If at least one user module has decided to block this MAC address, it will stay in the blocked state until the hold time (measured in seconds) expires. If all user modules have decided to allow this MAC address to forward, and aging is enabled, the Port Security module will periodically check that this MAC address still forwards traffic. If the age period (measured in seconds) expires and no frames have been seen, the MAC address will be removed from the MAC table. Otherwise a new age period will begin.

  If aging is disabled or a user module has decided to hold the MAC address indefinitely, a dash (-) will be shown.

Buttons

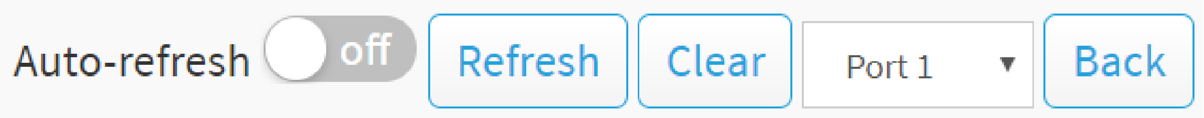


Figure 11-5.2: The Port Security Status Buttons

- **Auto-refresh :**

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

- **Refresh :**

  Click to refresh the page immediately.

- **Clear :**

  Click to remove this particular MAC addresses from MAC table.

- **Port 1 :**

  Select port that you want to display the Port Security Status.

- **Back :**

  Click to go back Port Security Status.

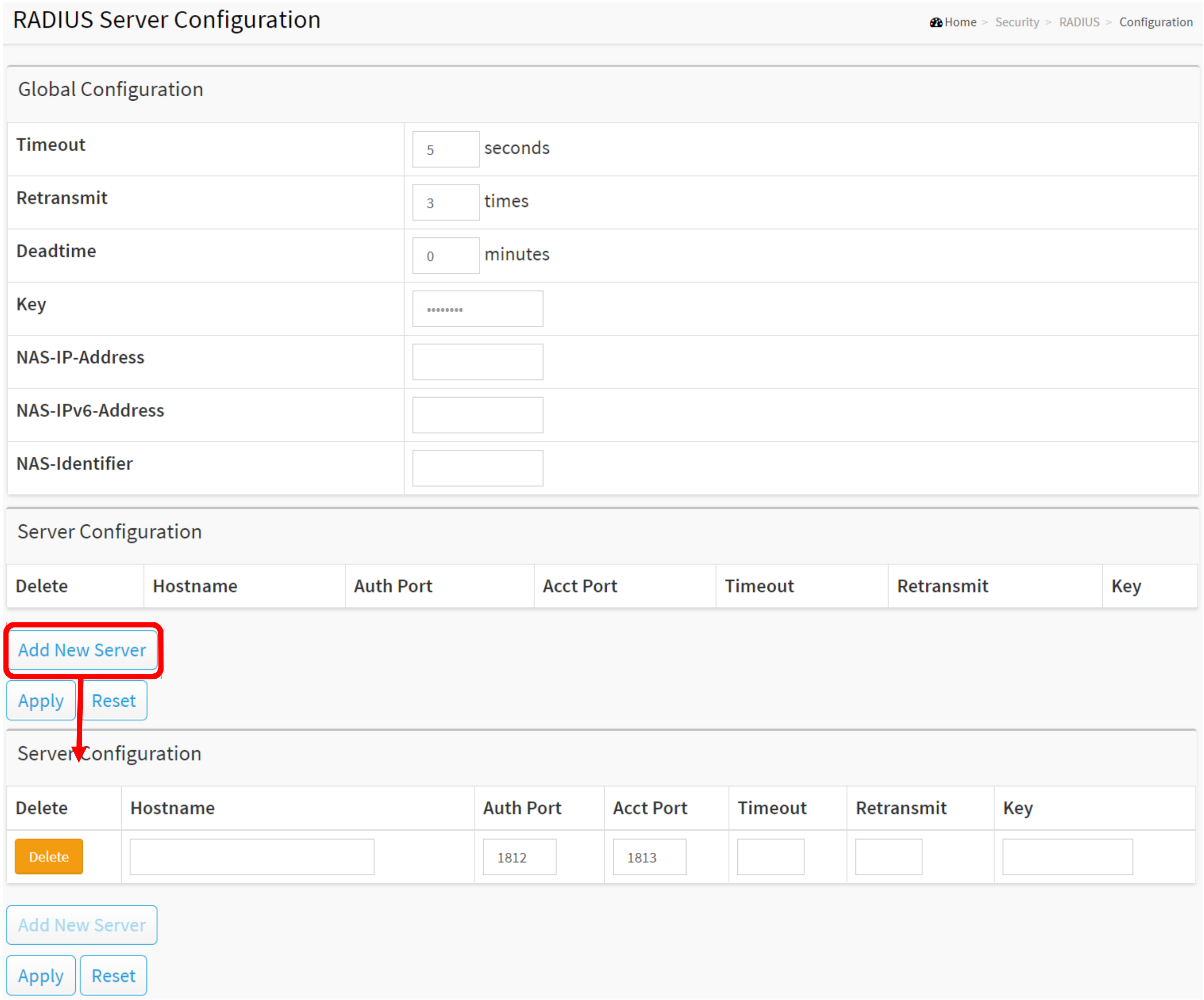
11-6 RADIUS

11-6.1 Configuration

Web Interface

To configure a RADIUS in the web interface:

1. Click Security, RADIUS and Configuration.
2. Set Timeout, Retransmit, Deadtime, Key, NAS-IP-Address, NAS IPv6-Address, NAS-Identifier.
3. Click "Add New Entry".
4. Set Hostname, Auth Port, Acct Port, Timeout, Retransmit, Key.
5. Click the Apply to save the setting.
6. If you want to cancel the setting then you need to click the Reset button. It will revert to previously saved values.



RADIUS Server Configuration

Global Configuration

Timeout	5 seconds
Retransmit	3 times
Deadtime	0 minutes
Key	••••••••
NAS-IP-Address	
NAS-IPv6-Address	
NAS-Identifier	

Server Configuration

Delete	Hostname	Auth Port	Acct Port	Timeout	Retransmit	Key

Server Configuration

Delete	Hostname	Auth Port	Acct Port	Timeout	Retransmit	Key
Delete		1812	1813			

Figure 11-6.1: The RADIUS Configuration

Parameter description:

Global Configuration

These setting are common for all of the RADIUS servers.

- **Timeout :**

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

- **Retransmit :**

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

- **Deadtime :**

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

- **Key :**

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

- **NAS-IP-Address :**

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

- **NAS-IPv6-Address :**

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

- **NAS-Identifier :**

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

Server Configuration

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

- **Hostname :**

  The IP address or hostname of the RADIUS server.

- **Auth Port :**

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

- **Acct Port :**

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

- **Timeout :**

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

- **Retransmit :**

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

- **Key :**

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

Buttons

- **Delete :**

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

- **Add New Entry :**

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

- **Apply :**

  Click to save changes.

- **Reset :**

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

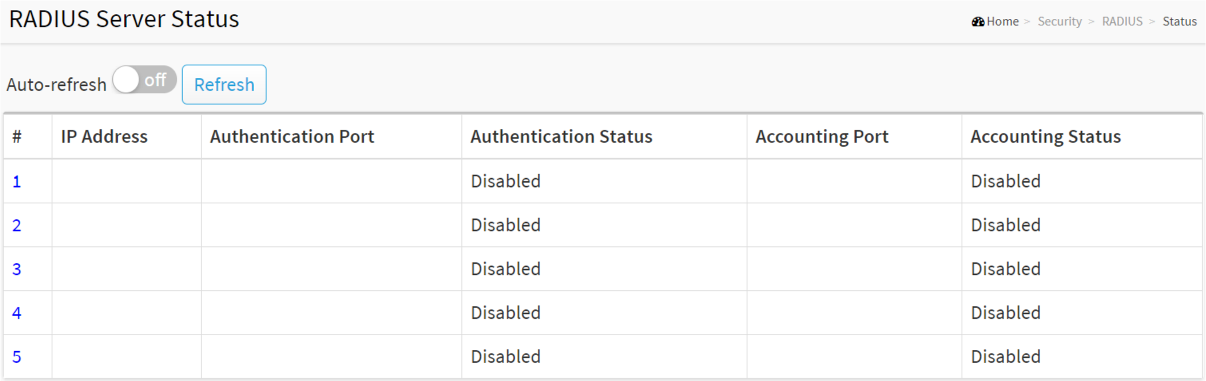
11-6.2 Status

This section shows you an overview/detail of the RADIUS Authentication and Accounting servers' status to ensure the function is workable.

Web Interface

To display a RADIUS Status in the web interface:

1. Click Security, RADIUS and Status.
2. Select server to display the detail statistics for a particular RADIUS



RADIUS Server Status

#	IP Address	Authentication Port	Authentication Status	Accounting Port	Accounting Status
1			Disabled		Disabled
2			Disabled		Disabled
3			Disabled		Disabled
4			Disabled		Disabled
5			Disabled		Disabled

Figure 11-6.2: The RADIUS Server Status Overview

Parameter description:

- **# :**

  The RADIUS server number. Click to navigate to detailed statistics for this server.

- **IP Address :**

  The IP address and UDP port number (in <IP Address>:<UDP Port> notation) of this server.

- **Authentication Port :**

  UDP port number for authentication.

- **Authentication Status :**

The current status of the server. This field takes one of the following values:
Disabled: The server is disabled.
Not Ready: The server is enabled, but IP communication is not yet up and running.
Ready: The server is enabled, IP communication is up and running, and the RADIUS module is ready to accept access attempts.
Dead (X seconds left): Access attempts were made to this server, but it did not reply within the configured timeout. The server has temporarily been disabled, but will get re-enabled when the dead-time expires. The number of seconds left before this occurs is displayed in parentheses. This state is only reachable when more than one server is enabled.

- **Accounting Port :**

UDP port number for accounting.

- **Accounting Status :**

The current status of the server. This field takes one of the following values:
Disabled: The server is disabled.
Not Ready: The server is enabled, but IP communication is not yet up and running.
Ready: The server is enabled, IP communication is up and running, and the RADIUS module is ready to accept access attempts.
Dead (X seconds left): Access attempts were made to this server, but it did not reply within the configured timeout. The server has temporarily been disabled, but will get re-enabled when the dead-time expires. The number of seconds left before this occurs is displayed in parentheses. This state is only reachable when more than one server is enabled.

Buttons

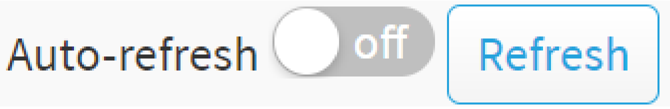


Figure 11-6.2: The RADIUS Server Status Buttons

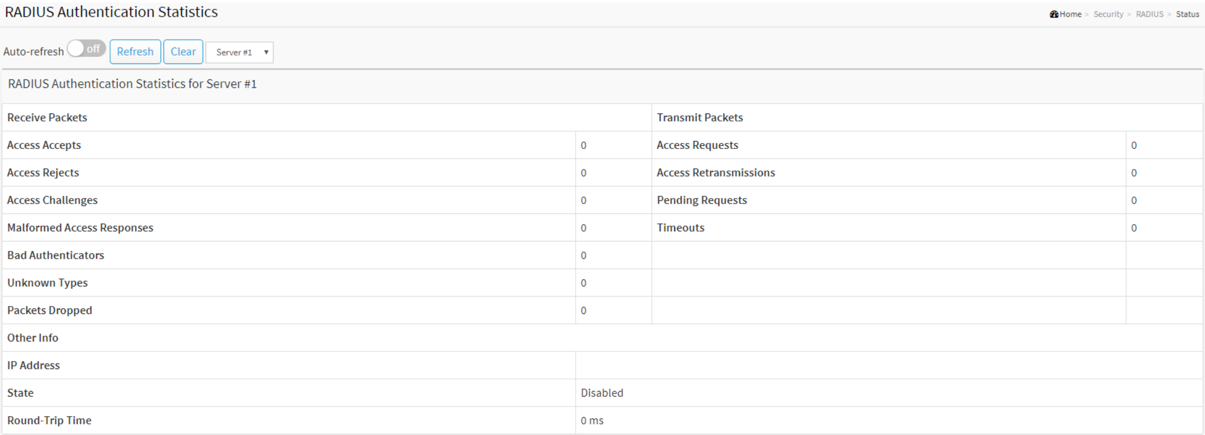
- **Auto-refresh :**

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

- **Refresh :**

Click to refresh the page immediately.

- **If you select Server#1 to display RADIUS Statistics**

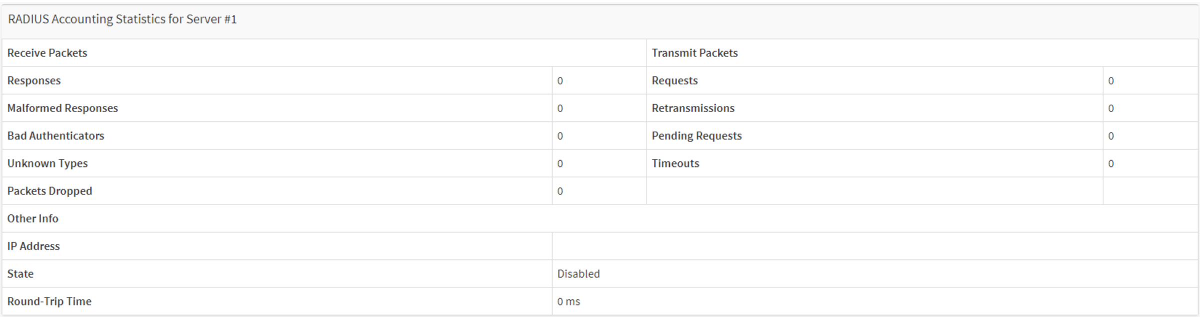


RADIUS Authentication Statistics

RADIUS Authentication Statistics for Server #1

Receive Packets		Transmit Packets	
Access Accepts	0	Access Requests	0
Access Rejects	0	Access Retransmissions	0
Access Challenges	0	Pending Requests	0
Malformed Access Responses	0	Timeouts	0
Bad Authenticators	0		
Unknown Types	0		
Packets Dropped	0		

Other Info	
IP Address	
State	Disabled
Round-Trip Time	0 ms



RADIUS Accounting Statistics for Server #1

Receive Packets		Transmit Packets	
Responses	0	Requests	0
Malformed Responses	0	Retransmissions	0
Bad Authenticators	0	Pending Requests	0
Unknown Types	0	Timeouts	0
Packets Dropped	0		
Other Info			
IP Address			
State	Disabled		
Round-Trip Time	0 ms		

Figure 11-6.2: The RADIUS Statistics for Server

Parameter description:

- **server :**

  You can select which server that you want to display RADIUS.

  RADIUS Authentication Statistics for Server #1

  The statistics map closely to those specified in RFC4668 - RADIUS Authentication Client MIB.
  Use the server select box to switch between the backend servers to show details for.

- **Access Accepts :**

  The number of RADIUS Access-Accept packets (valid or invalid) received from the server.

- **Access Rejects :**

  The number of RADIUS Access-Reject packets (valid or invalid) received from the server.

- **Access Challenges :**

  The number of RADIUS Access-Challenge packets (valid or invalid) received from the server.

- **Malformed Access Responses :**

  The number of malformed RADIUS Access-Response packets received from the server. Malformed packets include packets with an invalid length. Bad authenticators or Message Authenticator attributes or unknown types are not included as malformed access responses.

- **Bad Authenticators :**

  The number of RADIUS Access-Response packets containing invalid authenticators or Message Authenticator attributes received from the server.

- **Unknown Types :**

  The number of RADIUS packets that were received with unknown types from the server on the authentication port and dropped.

- **Packets Dropped :**

  The number of RADIUS packets that were received from the server on the authentication port and dropped for some other reason.

- **Access Requests :**

  The number of RADIUS Access-Request packets sent to the server. This does not include retransmissions.

- **Access Retransmissions :**

  The number of RADIUS Access-Request packets retransmitted to the RADIUS authentication server.

- **Pending Requests :**

The number of RADIUS Access-Request packets destined for the server that have not yet timed out or received a response. This variable is incremented when an Access-Request is sent and decremented due to receipt of an Access-Accept, Access-Reject, Access-Challenge, timeout, or retransmission.

- **Timeouts :**

  The number of authentication timeouts to the server. After a timeout, the client may retry to the same server, send to a different server, or give up. A retry to the same server is counted as a retransmit as well as a timeout. A send to a different server is counted as a Request as well as a timeout.

- **IP Address :**

  IP address and UDP port for the authentication server in question.

- **State :**

  Shows the state of the server. It takes one of the following values:

  - **Disabled :**

    The selected server is disabled.

  - **Not Ready :**

    The server is enabled, but IP communication is not yet up and running.

  - **Ready :**

    The server is enabled, IP communication is up and running, and the RADIUS module is ready to accept access attempts.

  - **Dead (X seconds left) :**

    Access attempts were made to this server, but it did not reply within the configured timeout. The server has temporarily been disabled, but will get re-enabled when the dead-time expires. The number of seconds left before this occurs is displayed in parentheses. This state is only reachable when more than one server is enabled.

- **Round-Trip Time :**

  The time interval (measured in milliseconds) between the most recent Access-Reply/Access-Challenge and the Access-Request that matched it from the RADIUS authentication server. The granularity of this measurement is 100 ms. A value of 0 ms indicates that there hasn't been round-trip communication with the server yet.

RADIUS Accounting Statistics for Server #1

The statistics map closely to those specified in RFC4670 - RADIUS Accounting Client MIB. Use the server select box to switch between the backend servers to show details for.

- **Responses :**

  The number of RADIUS packets (valid or invalid) received from the server.

- **Malformed Responses :**

  The number of malformed RADIUS packets received from the server. Malformed packets include packets with an invalid length. Bad authenticators or unknown types are not included as malformed access responses.

- **Bad Authenticators :**

  The number of RADIUS packets containing invalid authenticators received from the server.

- **Unknown Types :**

  The number of RADIUS packets of unknown types that were received from the server on the accounting port.

- **Packets Dropped :**

  The number of RADIUS packets that were received from the server on the accounting port and dropped for some other reason.

- **Requests :**

  The number of RADIUS packets sent to the server. This does not include retransmissions

- **Retransmissions :**

  The number of RADIUS packets retransmitted to the RADIUS accounting server.

- **Pending Requests :**

  The number of RADIUS packets destined for the server that have not yet timed out or received a response. This variable is incremented when a Request is sent and decremented due to receipt of a Response, timeout, or retransmission.

- **Timeouts :**

  The number of accounting timeouts to the server. After a timeout, the client may retry to the same server, send to a different server, or give up. A retry to the same server is counted as a retransmit as well as a timeout. A send to a different server is counted as a Request as well as a timeout.

- **IP Address :**

  IP address and UDP port for the accounting server in question.

- **State :**

  Shows the state of the server. It takes one of the following values:

  - **Disabled :**

    The selected server is disabled.

  - **Not Ready :**

    The server is enabled, but IP communication is not yet up and running.

  - **Ready :**

    The server is enabled, IP communication is up and running, and the RADIUS module is ready to accept accounting attempts.

  - **Dead (X seconds left) :**

    Accounting attempts were made to this server, but it did not reply within the configured timeout. The server has temporarily been disabled, but will get re-enabled when the dead-time expires. The number of seconds left before this occurs is displayed in parentheses. This state is only reachable when more than one server is enabled.

- **Round-Trip Time :**

  The time interval (measured in milliseconds) between the most recent Response and the Request that matched it from the RADIUS accounting server. The granularity of this measurement is 100 ms. A value of 0 ms indicates that there hasn't been round-trip communication with the server yet.

Buttons

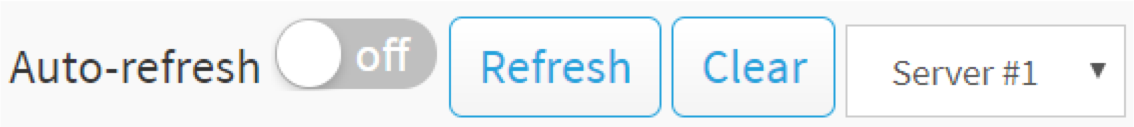


Figure 11-6.2: The RADIUS Server Status for Server Buttons

- **Auto-refresh :**

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

- **Refresh :**

  Click to refresh the page immediately.

- **Clear :**

  Clears the counters for the selected server. The "Pending Requests" counter will not be cleared by this operation.

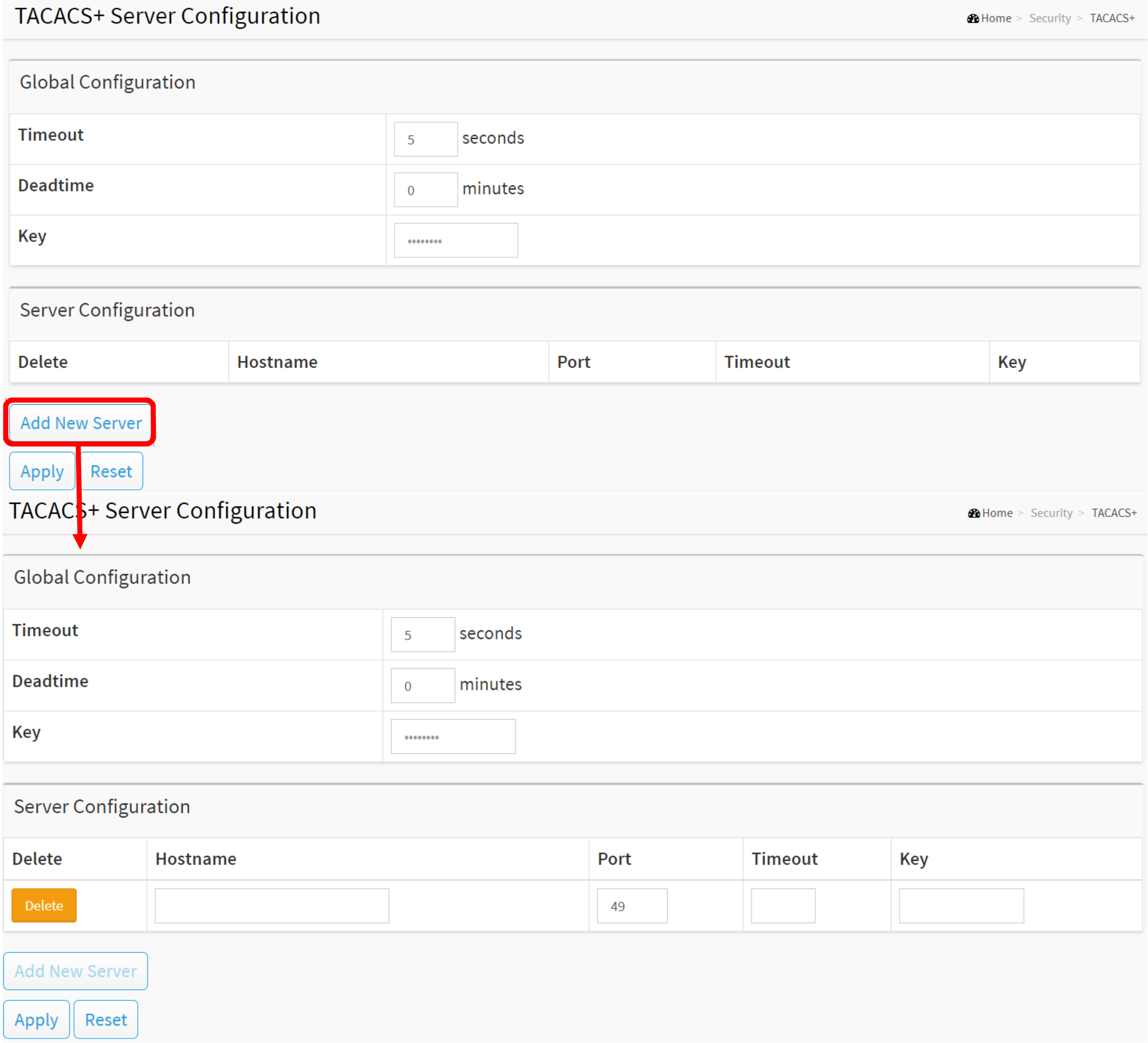
11-7 TACACS+

This page allows you to configure up to 5 TACACS+servers.

Web Interface

To configure the TACACS+ servers in the web interface:

1. Click Security and TACACS+.
2. Click "Add New Entry".
3. Specify the Timeout, Deadtime, Key.
4. Specify the Hostname, Port, Timeout and Key in the server.
5. Click Apply.



TACACS+ Server Configuration

Global Configuration

Timeout	5 seconds
Deadtime	0 minutes
Key	••••••••

Server Configuration

Delete	Hostname	Port	Timeout	Key

TACACS+ Server Configuration

Global Configuration

Timeout	5 seconds
Deadtime	0 minutes
Key	••••••••

Server Configuration

Delete	Hostname	Port	Timeout	Key
Delete		49		

Figure 11-7: The TACACS+ Server Configuration

Parameter description:

Global Configuration

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

- **Timeout :**

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

- **Deadtime :**

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

- **Key :**

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

Server Configuration

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

- **Delete :**

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

- **Hostname :**

  The IP address or hostname of the TACACS+ server.

- **Port :**

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

- **Timeout :**

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

- **Key :**

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

Buttons

- **Delete :**

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

- **Add New Server :**

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

- **Apply :**

  Click to save changes.

- **Reset :**

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

Chapter 12 Access Control

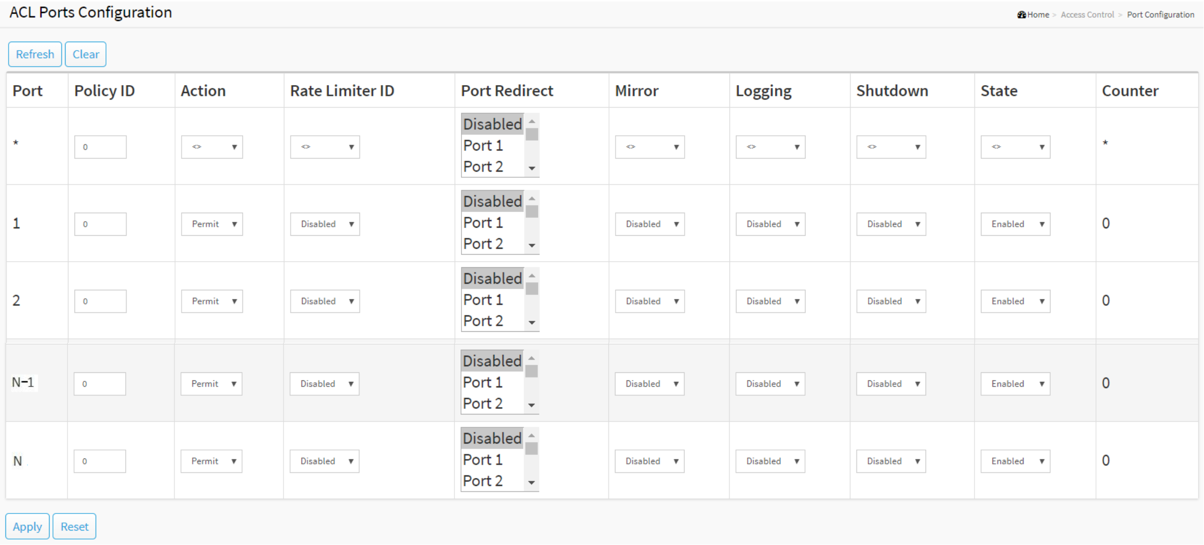
12-1 Ports Configuration

Configure the ACL parameters (ACE) of each switch port. These parameters will affect frames received on a port unless the frame matches a specific ACE.

Web Interface

To configure the ACL Ports Configuration in the web interface:

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



ACL Ports Configuration

Home > Access Control > Port Configuration

Refresh Clear

Port	Policy ID	Action	Rate Limiter ID	Port Redirect	Mirror	Logging	Shutdown	State	Counter
*	0	<>	<>	Disabled Port 1 Port 2	<>	<>	<>	<>	*
1	0	Permit	Disabled	Disabled Port 1 Port 2	Disabled	Disabled	Disabled	Enabled	0
2	0	Permit	Disabled	Disabled Port 1 Port 2	Disabled	Disabled	Disabled	Enabled	0
N-1	0	Permit	Disabled	Disabled Port 1 Port 2	Disabled	Disabled	Disabled	Enabled	0
N	0	Permit	Disabled	Disabled Port 1 Port 2	Disabled	Disabled	Disabled	Enabled	0

Apply Reset

Figure 12-1: The ACL Ports Configuration

Parameter description:

- **Port :**

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

- **Policy ID :**

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

- **Action :**

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

- **Rate Limiter ID :**

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

- **Port Redirect :**

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

- **Mirror**

  Specify the mirror operation of this port. The allowed values are:
  Enabled: Frames received on the port are mirrored.
  Disabled: Frames received on the port are not mirrored.
  The default value is "Disabled".

- **Logging :**

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

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

  Disabled: Frames received on the port are not logged.

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

- **Shutdown :**

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

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

  Disabled: Port shut down is disabled.

  The default value is "Disabled".

- **State :**

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

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

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

  The default value is "Enabled"

- **Counter :**

  Counts the number of frames that match this ACE.

Buttons

- **Refresh, clear :**

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

- **Apply :**

  Click to save changes.

- **Reset :**

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

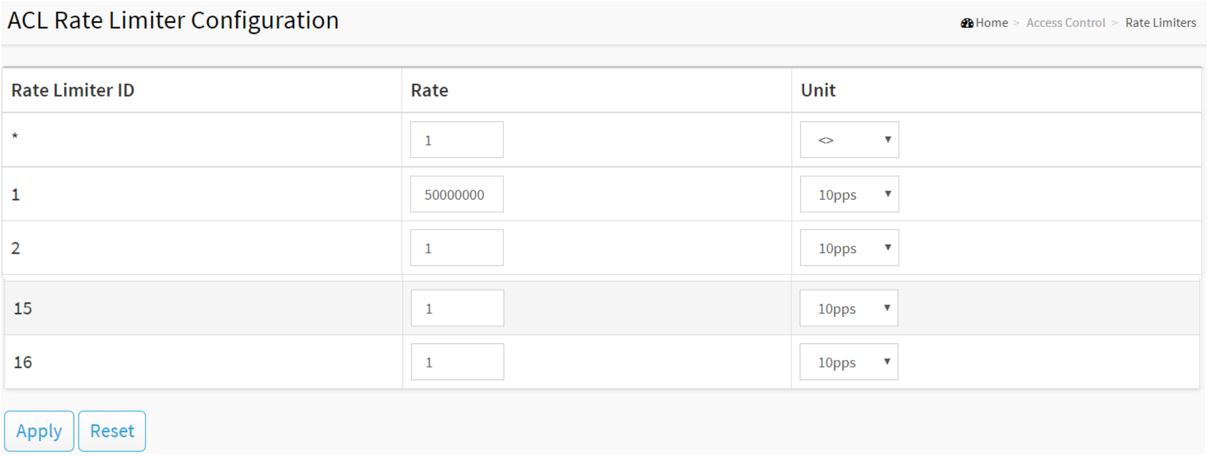
12-2 Rate Limiters

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

Web Interface

To configure ACL Rate Limiter in the web interface:

1. Click Access Control and Rate Limiters.
2. To specific the Rate field, Unit.
3. Click the Apply to save the setting
4. If you want to cancel the setting then you need to click the reset button. It will revert to previously saved values.



ACL Rate Limiter Configuration

Home > Access Control > Rate Limiters

Rate Limiter ID	Rate	Unit
*	1	<>
1	50000000	10pps
2	1	10pps
15	1	10pps
16	1	10pps

Figure 12-2: The ACL Rate Limiter Configuration

Parameter description:

- **Rate Limiter ID :**

  The rate limiter ID for the settings contained in the same row and its range is 1 to 16.

- **Rate :**

  The valid rate is 0, 10, 20, 30, ..., 5000000 in pps

  or 0, 25, 50, 75, ..., 10000000 in kbps.

- **Unit**

  Specify the rate unit. The allowed values are:
  10pps: packets per second.
  25kbps: Kbits per second.

Buttons

- **Apply :**

  Click to save changes.

- **Reset :**

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

12-3 Access Control List

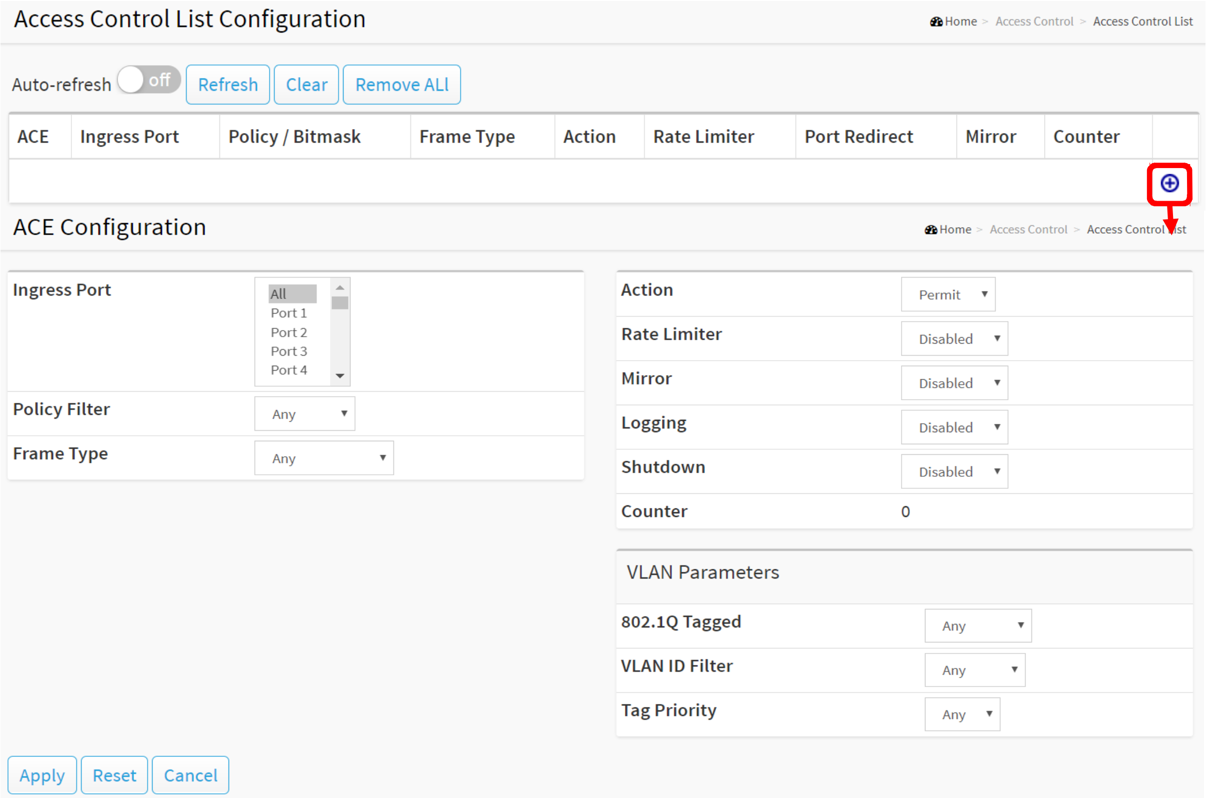
This page shows the Access Control List (ACL), which is made up of the ACEs defined on this switch. Each row describes the ACE that is defined. The maximum number of ACEs is 512 on each switch.

Click on the lowest plus sign to add a new ACE to the list. The reserved ACEs used for internal protocol, cannot be edited or deleted, the order sequence cannot be changed and the priority is highest.

Web Interface

To configure Access Control List in the web interface:

1. Click Access Control and Access Control List.
2. Click the ⊕ button to add a new ACL, or use the other ACL modification buttons to specify the editing action (i.e., edit, delete, or moving the relative position of entry in the list)
3. To specific the parameter of the ACE
4. Click the save to save the setting
5. If you want to cancel the setting then you need to click the reset button. It will revert to previously saved values.
6. When editing an entry on the ACE Configuration page, note that the Items displayed depend on various selections, such as Frame Type and IP Protocol Type. Specify the relevant criteria to be matched for this rule, and set the actions to take when a rule is matched (such as Rate Limiter, Port Copy, Logging, and Shutdown).



Access Control List Configuration

Home > Access Control > Access Control List
Auto-refresh
off
Refresh
Clear
Remove ALL

ACE	Ingress Port	Policy / Bitmask	Frame Type	Action	Rate Limiter	Port Redirect	Mirror	Counter	
									⊕

ACE Configuration

Home > Access Control > Access Control List

Ingress Port	All Port 1 Port 2 Port 3 Port 4
Policy Filter	Any
Frame Type	Any

Action	Permit
Rate Limiter	Disabled
Mirror	Disabled
Logging	Disabled
Shutdown	Disabled
Counter	0

VLAN Parameters

802.1Q Tagged	Any
VLAN ID Filter	Any
Tag Priority	Any

Figure 12-3: The Access Control List Configuration

Parameter description:

- **ACE :**

  Indicates the ACE ID.

- **Ingress Port :**

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

  Any: The ACE will match any ingress port.

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

  Port: The ACE will match a specific ingress port.

- **Policy / Bitmask :**

  Indicates the policy number and bitmask of the ACE.

- **Frame Type :**

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

  Any: The ACE will match any frame type.

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

  ARP: The ACE will match ARP/RARP frames.

  IPv4: The ACE will match all IPv4 frames.

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

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

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

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

  IPv6: The ACE will match all IPv6 standard frames.

- **Action :**

  Indicates the forwarding action of the ACE.

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

  Deny: Frames matching the ACE are dropped.

  Filter: Frames matching the ACE are filtered.

- **Rate Limiter :**

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

- **Port Redirect :**

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

- **Mirror :**

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

  Enabled: Frames received on the port are mirrored.

  Disabled: Frames received on the port are not mirrored.

  The default value is "Disabled".

- **Counter :**

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

- **Modification Buttons :**

  You can modify each ACE (Access Control Entry) in the table using the following buttons:
  ⊕: Inserts a new ACE before the current row.
  ⓔ: Edits the ACE row.
  ⇧: Moves the ACE up the list.
  ⇩: Moves the ACE down the list.
  ⊗: Deletes the ACE.
  ⊕: The lowest plus sign adds a new entry at the bottom of the ACE listings.

ACE Configuration

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

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

- **Ingress Port :**

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

- **Policy Filter :**

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

- **Policy Value :**

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

- **Policy Bitmask :**

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

- **Frame Type :**

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

  Any: Any frame can match this ACE.

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

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

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

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

- **Action :**

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

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

Deny: The frame that hits this ACE is dropped.

Filter: Frames matching the ACE are filtered.

- **Rate Limiter :**

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

- **Port Redirect :**

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

- **Mirror :**

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

  Enabled: Frames received on the port are mirrored.

  Disabled: Frames received on the port are not mirrored.

  The default value is "Disabled".

- **Logging :**

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

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

  Disabled: Frames matching the ACE are not logged.

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

- **Shutdown :**

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

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

  Disabled: Port shut down is disabled for the ACE.

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

- **Counter :**

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

MAC Parameter

- **SMAC Filter :**

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

  Specify the source MAC filter for this ACE.

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

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

- **SMAC Value :**

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

- **DMAC Filter :**

  Specify the destination MAC filter for this ACE.

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

  MC: Frame must be multicast.

  BC: Frame must be broadcast.

  UC: Frame must be unicast.

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

- **DMAC Value :**

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

VLAN Parameters

- **802.1Q Tagged :**

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

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

  Enabled: Tagged frame only.

  Disabled: Untagged frame only.

  The default value is "Any".

- **VLAN ID Filter :**

  Specify the VLAN ID filter for this ACE.

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

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

- **VLAN ID :**

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

- **Tag Priority :**

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

ARP Parameters

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

- **ARP/RARP :**

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

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

  ARP: Frame must have ARP opcode set to ARP.

  RARP: Frame must have RARP opcode set to RARP.

Other: Frame has unknown ARP/RARP Opcode flag.

- **Request/Reply :**

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

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

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

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

- **Sender IP Filter :**

  Specify the sender IP filter for this ACE.

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

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

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

- **Sender IP Address :**

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

- **Sender IP Mask :**

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

- **Target IP Filter :**

  Specify the target IP filter for this specific ACE.

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

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

- **Target IP Address :**

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

- **Target IP Mask :**

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

- **ARP Sender MAC Match :**

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

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

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

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

- **RARP Target MAC Match :**

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

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

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

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

- **IP/Ethernet Length :**

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

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

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

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

- **Ethernet :**

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

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

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

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

- **IP :**

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

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

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

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

IP Parameters

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

- **IP Protocol Filter :**

  Specify the IP protocol filter for this ACE.

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

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

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

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

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

- **IP Protocol Value :**

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

- **IP TTL :**

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

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

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

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

- **IP Fragment :**

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

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

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

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

- **IP Option :**

  Specify the options flag setting for this ACE.

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

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

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

- **SIP Filter :**

  Specify the source IP filter for this ACE.

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

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

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

- **SIP Address :**

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

- **SIP Mask :**

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

- **DIP Filter :**

  Specify the destination IP filter for this ACE.

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

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

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

- **DIP Address :**

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

- **DIP Mask :**

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

IPv6 Parameters

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

- **Next Header Filter :**

  Specify the IPv6 next header filter for this ACE.

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

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

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

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

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

- **Next Header Value :**

  When "Specific" is selected for the IPv6 next header value, you can enter a specific value. The allowed range is 0 to 255. A frame that hits this ACE matches this IPv6 protocol value.

- **SIP Filter :**

  Specify the source IPv6 filter for this ACE.

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

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

- **SIP Address :**

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

- **SIP BitMask :**

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

- **Hop Limit :**

  Specify the hop limit settings for this ACE.

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

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

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

ICMP Parameters

- **ICMP Type Filter :**

  Specify the ICMP filter for this ACE.

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

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

- **ICMP Type Value :**

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

- **ICMP Code Filter :**

  Specify the ICMP code filter for this ACE.

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

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

- **ICMP Code Value :**

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

TCP/UDP Parameters

- **TCP/UDP Source Filter :**

  Specify the TCP/UDP source filter for this ACE.

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

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

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

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

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

- **TCP/UDP Source Range :**

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

- **TCP/UDP Destination Filter :**

  Specify the TCP/UDP destination filter for this ACE.

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

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

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

- **TCP/UDP Destination Number :**

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

- **TCP/UDP Destination Range :**

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

- **TCP FIN :**

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

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

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

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

- **TCP SYN :**

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

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

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

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

- **TCP RST :**

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

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

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

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

- **TCP PSH :**

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

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

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

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

- **TCP ACK :**

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

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

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

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

- **TCP URG :**

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

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

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

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

Ethernet Type Parameters

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

- **EtherType Filter :**

  Specify the Ethernet type filter for this ACE.

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

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

- **Ethernet Type Value :**

  When "Specific" is selected for the EtherType filter, you can enter a specific EtherType value.

The allowed range is 0x600 to 0xFFFF but excluding 0x800(IPv4), 0x806(ARP) and 0x86DD(IPv6). A frame that hits this ACE matches this EtherType value.

Buttons

- **Apply :**

  Click to save changes.

- **Reset :**

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

- **Auto-refresh :**

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

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

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

- **Cancel :**

  Return to the previous page.

12-4 ACL Status

The section describes how to shows the ACL status by different ACL users. Each row describes the ACE that is defined. It is a conflict if a specific ACE is not applied to the hardware due to hardware limitations. The maximum number of ACEs is 512 on each switch.

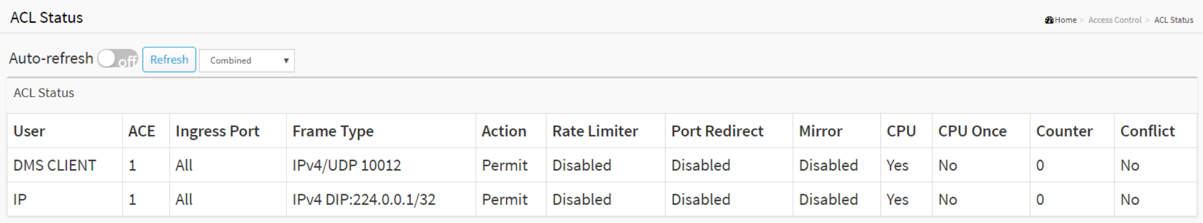
Web Interface

To display the ACL status in the web interface:

Click Access Control and ACL status

If you want to auto-refresh the information then you need to evoke the "Auto-refresh".

1. Click "Refresh" to refresh the ACL Status.



ACL Status

User	ACE	Ingress Port	Frame Type	Action	Rate Limiter	Port Redirect	Mirror	CPU	CPU Once	Counter	Conflict
DMS CLIENT	1	All	IPv4/UDP 10012	Permit	Disabled	Disabled	Disabled	Yes	No	0	No
IP	1	All	IPv4 DIP:224.0.0.1/32	Permit	Disabled	Disabled	Disabled	Yes	No	0	No

Figure 12-4: The ACL Status

Parameter description:

- **User :**

  Indicates the ACL user.

- **ACE :**

  Indicates the ACE ID on local switch.

- **Ingress Port :**

  Indicates the ingress port of the ACE. Possible values are:
  All: The ACE will match all ingress port.
  Port: The ACE will match a specific ingress port.

- **Frame Type :**

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

  Any: The ACE will match any frame type.

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

  ARP: The ACE will match ARP/RARP frames.

  IPv4: The ACE will match all IPv4 frames.

  IPv4: The ACE will match all IPv4 frames.

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

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

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

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

  IPv6: The ACE will match all IPv6 standard frames.

- **Action :**

  Indicates the forwarding action of the ACE.

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

  Deny: Frames matching the ACE are dropped.

  Filter: Frames matching the ACE are filtered.

- **Rate Limiter :**

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

- **Port Redirect :**

  Indicates the port redirect operation of the ACE. Frames matching the ACE are redirected to the port number. The allowed values are Disabled or a specific port number. When Disabled is displayed, the port redirect operation is disabled.

- **Mirror :**

  Specify the mirror operation of this port. The allowed values are:
  Enabled: Frames received on the port are mirrored.
  Disabled: Frames received on the port are not mirrored.
  The default value is "Disabled".

- **CPU :**

  Forward packet that matched the specific ACE to CPU.

- **CPU Once :**

  Forward first packet that matched the specific ACE to CPU.

- **Counter :**

  The counter indicates the number of times the ACE was hit by a frame.

- **Conflict :**

  Indicates the hardware status of the specific ACE. The specific ACE is not applied to the hardware due to hardware limitations.

Buttons

Figure 12-4: The ACL Status Buttons

- **Auto-refresh :**

  Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.

- **Refresh :**

  Click to refresh the page immediately.

Chapter 13 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.

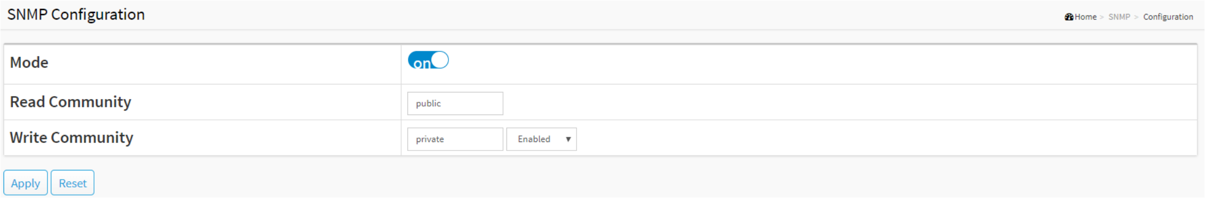
13-1 Configuration

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 SNMP and configuration.
2. Evoke SNMP State to enable or disable the SNMP function.
3. Specify the Read Community, Write Community.
4. Click Apply.



SNMP Configuration

Mode	on
Read Community	public
Write Community	private Enabled ▾

Figure 13-1: The SNMP Configuration

Parameter description:

- **Mode :**

  Indicates the SNMP mode operation. Possible modes are:
  on: Enable SNMP mode operation.
  off: Disable SNMP mode operation.

- **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.

13-2 SNMPv3

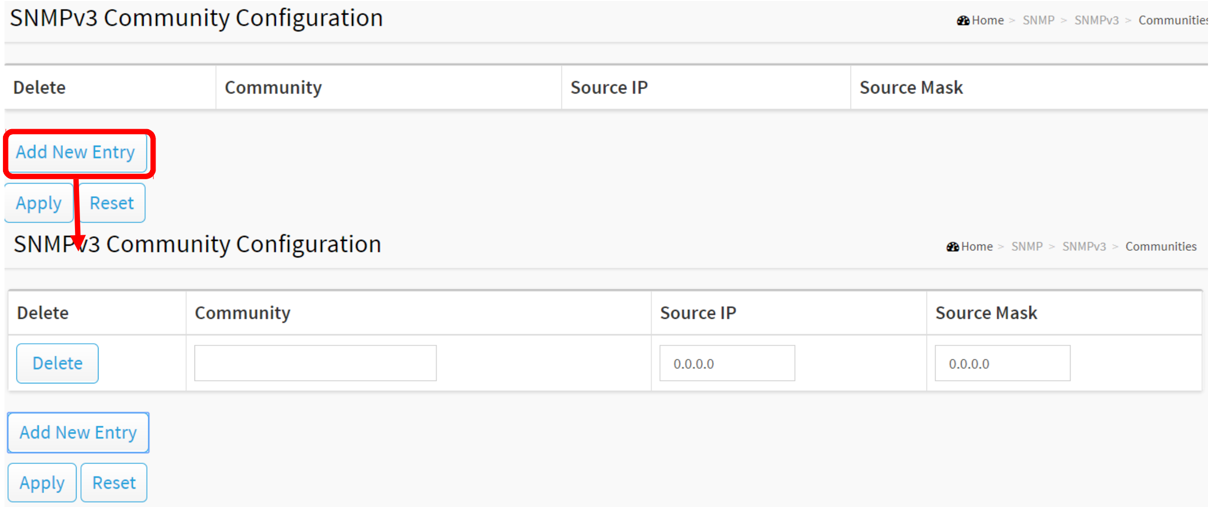
13-2.1 Communities

Configure SNMPv3 community table on this page. The entry index key is Community.

Web Interface

To configure the configure SNMP Communities in the web interface:

1. Click SNMP, SNMPv3 and Communities.
2. Click Add New Entry.
3. Specify the SNMP community parameters.
4. Click Apply.
5. If you want to modify or clear the setting then click Reset.



SNMPv3 Community Configuration

Delete	Community	Source IP	Source Mask

SNMPv3 Community Configuration

Delete	Community	Source IP	Source Mask
Delete		0.0.0.0	0.0.0.0

Home > SNMP > SNMPv3 > Communities
Add New Entry
Apply
Reset
Home > SNMP > SNMPv3 > Communities
Add New Entry
Apply
Reset

Figure 13-2.1: The SNMPv3 Communities Configuration

Parameter description:

- **Community :**

  Indicates the security name to map the community to the SNMP Groups configuration. The allowed string length is 1 to 32, and the allowed content is ASCII characters from 33 to 126.

- **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 IP Prefix :**

  Indicates the SNMP access source address prefix.

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.

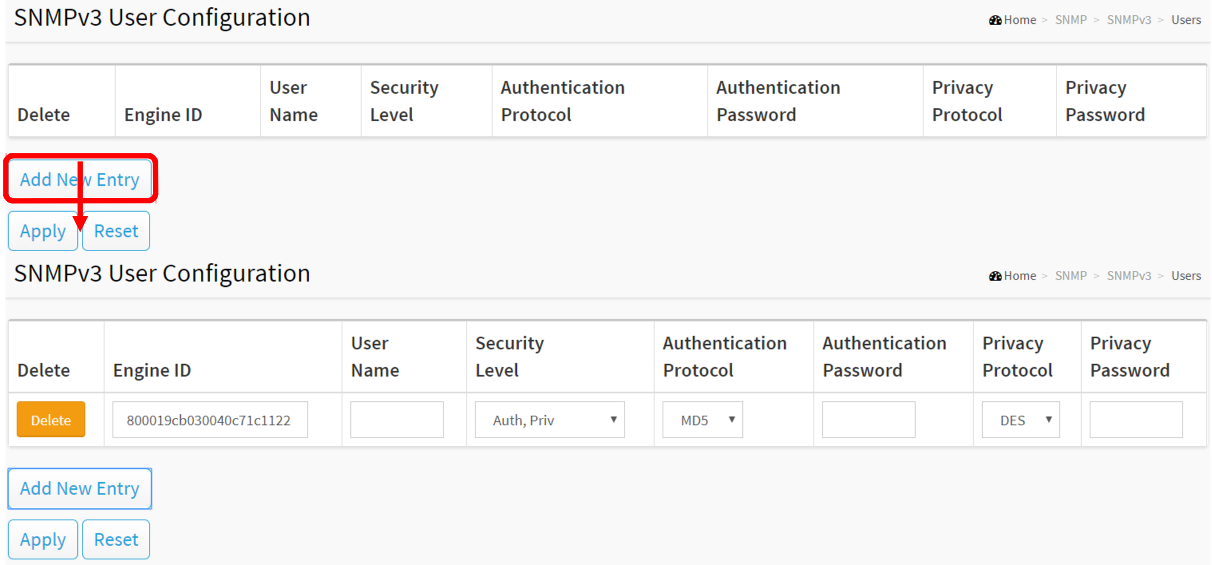
13-2.2 Users

The function is used to configure SNMPv3 user. The Entry index key is UserName. To create a new UserName account, please check <Add new user> button, and enter the user information then check <Apply>. Max Group Number: 6.

Web Interface

To configure SNMP Users in the web interface:

1. Click SNMP, SNMPv3 and Users.
2. Click Add new entry.
3. Specify the SNMPv3 Users parameter.
4. Click Apply.



SNMPv3 User Configuration

Delete	Engine ID	User Name	Security Level	Authentication Protocol	Authentication Password	Privacy Protocol	Privacy Password

SNMPv3 User Configuration

Delete	Engine ID	User Name	Security Level	Authentication Protocol	Authentication Password	Privacy Protocol	Privacy Password
Delete	800019cb030040c71c1122		Auth, Priv	MD5		DES	

Figure 13-2.2: The SNMP Users Configuration

Parameter description:

- **Engine ID :**

  An octet string identifying the engine ID that this entry should belong to. The string must contain an even number(in hexadecimal format) with number of digits between 10 and 64, but all-zeros and all-'F's are not allowed. The SNMPv3 architecture uses the User-based Security Model (USM) for message security and the View-based Access Control Model (VACM) for access control. For the USM entry, the usmUserEngineID and usmUserName are the entry's keys. In a simple agent, usmUserEngineID is always that agent's own snmpEngineID value. The value can also take the value of the snmpEngineID of a remote SNMP engine with which this user can communicate. In other words, if user engine ID equal system engine ID then it is local user; otherwise it's remote user.

- **User Name :**

  A string identifying the user name that this entry should belong to. The allowed string length is 1 to 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.

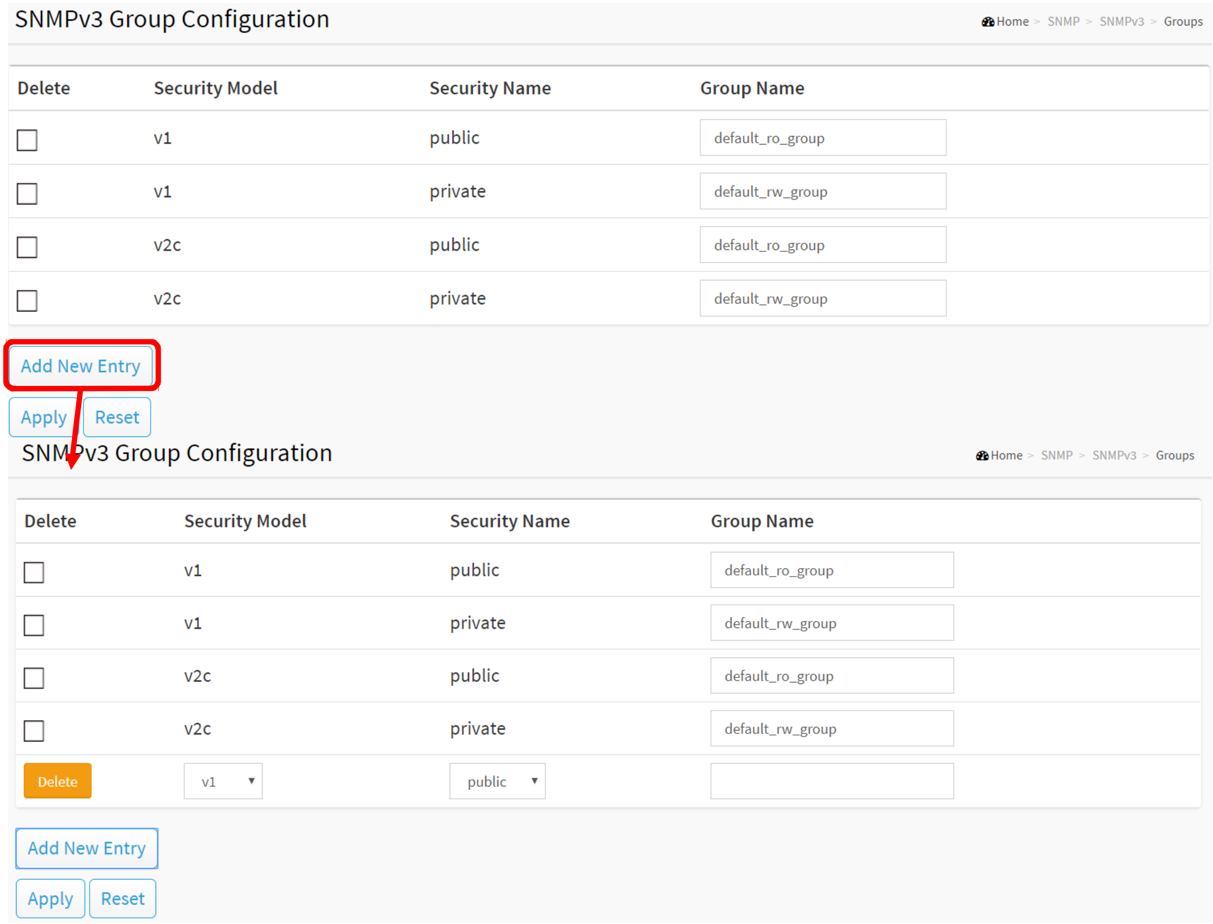
13-2.3 Groups

The function is used to configure SNMPv3 group. The Entry index key are Security Model and Security Name. To create a new group account, please check <Add new group> button, and enter the group information then check <Apply>. Max Group Number:12.

Web Interface

To configure SNMP Groups in the web interface:

1. Click SNMP, SNMPv3 and Groups.
2. Click Add new entry.
3. Specify the SNMP group parameter.
4. Click Apply.



SNMPv3 Group Configuration

Delete	Security Model	Security Name	Group Name
□	v1	public	default_ro_group
□	v1	private	default_rw_group
□	v2c	public	default_ro_group
□	v2c	private	default_rw_group

SNMPv3 Group Configuration

Delete	Security Model	Security Name	Group Name
□	v1	public	default_ro_group
□	v1	private	default_rw_group
□	v2c	public	default_ro_group
□	v2c	private	default_rw_group
Delete	v1	public	

Figure 13-2.3: 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.

13-2.4 Views

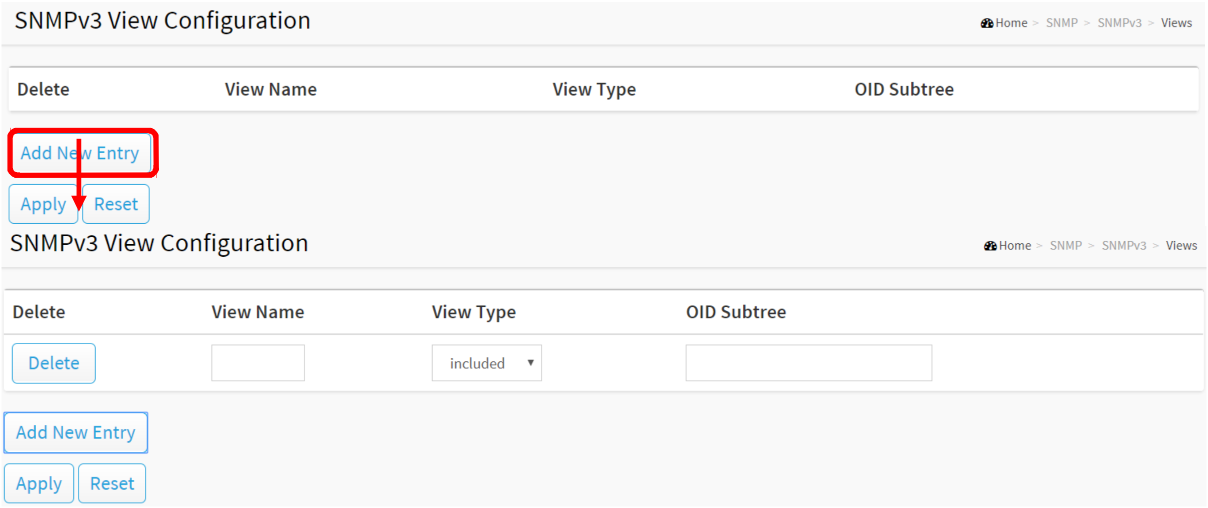
The function is used to configure SNMPv3 view. The Entry index keys are OID Subtree and View Name. To create a new view account, please check <Add new view> button, and enter the view information then click <Apply>. Max Group Number: 12.

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 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.



SNMPv3 View Configuration

Home > SNMP > SNMPv3 > Views

Delete	View Name	View Type	OID Subtree

SNMPv3 View Configuration

Home > SNMP > SNMPv3 > Views

Delete	View Name	View Type	OID Subtree
Delete		included ▾	

Figure 13-2.4: 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 "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.

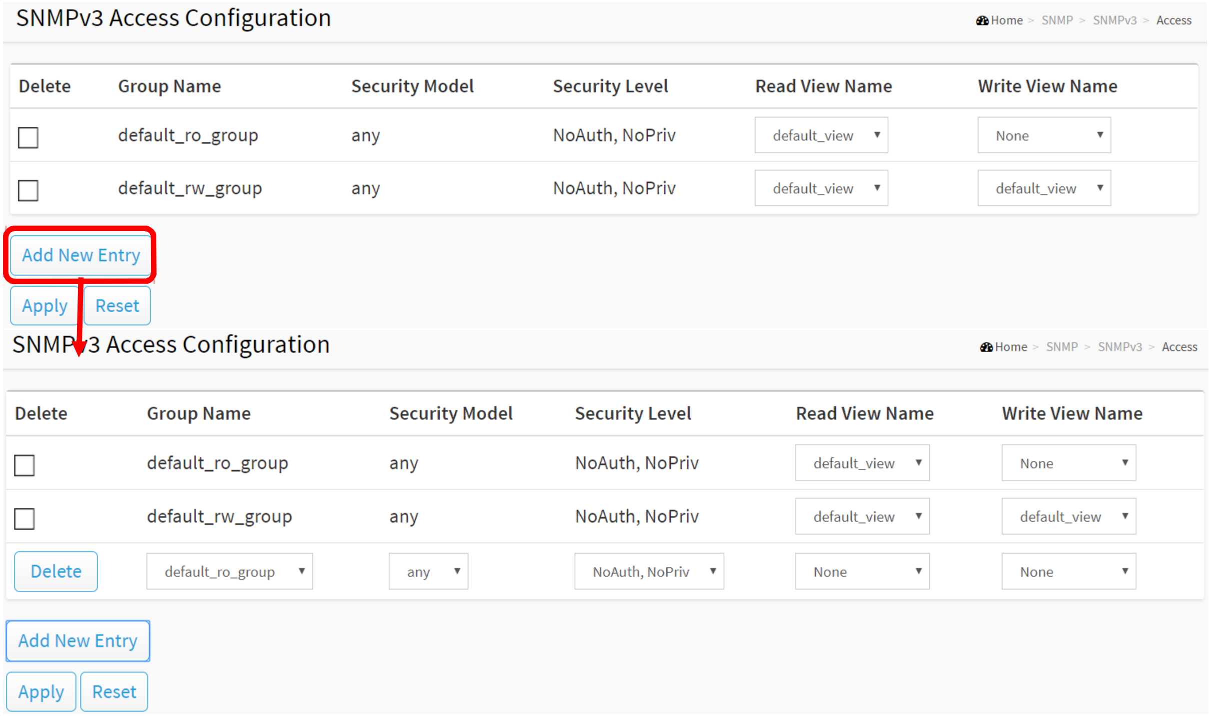
13-2.5 Access

The function is used to configure SNMPv3 accesses. The Entry index key are Group Name, Security Model and Security level. To create a new access account, please check <Add new access> button, and enter the access information then check <Apply>. Max Group Number : 12.

Web Interface

To display the configure SNMP Access in the web interface:

1. Click 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.



SNMPv3 Access Configuration

Delete	Group Name	Security Model	Security Level	Read View Name	Write View Name
□	default_ro_group	any	NoAuth, NoPriv	default_view	None
□	default_rw_group	any	NoAuth, NoPriv	default_view	default_view

SNMPv3 Access Configuration

Delete	Group Name	Security Model	Security Level	Read View Name	Write View Name
□	default_ro_group	any	NoAuth, NoPriv	default_view	None
□	default_rw_group	any	NoAuth, NoPriv	default_view	default_view
Delete	default_ro_group	any	NoAuth, NoPriv	None	None

Figure 13-2.5: 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.

13-3 Statistics

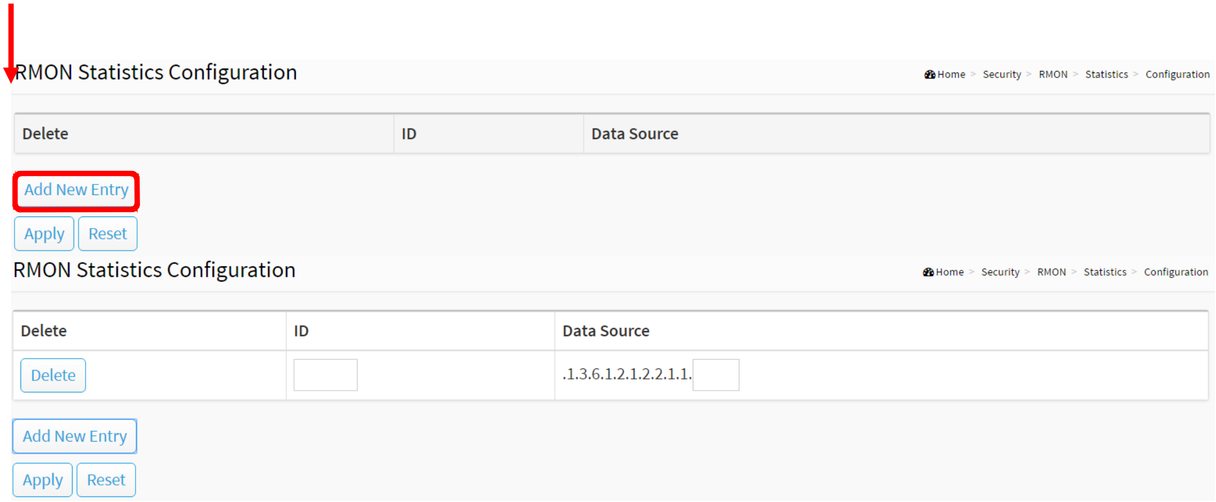
13-3.1 Configuration

Configure RMON Statistics table on this page. The entry index key is **ID.**

Web Interface

To configure the RMON Statistics Configuration in the web interface:

1. Click Security, RMON, Statistics and Configuration.
2. Click Add New Entry.
3. Specify the ID parameters.
4. Click Apply.



RMON Statistics Configuration

Delete	ID	Data Source

RMON Statistics Configuration

Delete	ID	Data Source
Delete		.1.3.6.1.2.1.2.2.1.1.

Home > Security > RMON > Statistics > Configuration
Add New Entry
Apply
Reset
Home > Security > RMON > Statistics > Configuration
Add New Entry
Apply
Reset

Figure 13-3.1: The RMON Statistics Configuration

Parameter description:

These parameters are displayed on the RMON Statistics Configuration page:

- **ID :**

  Indicates the index of the entry. The range is from 1 to 65535.

- **Data Source :**

  Indicates the port ID which wants to be monitored. If in stacking switch, the value must add 1000*(switch ID-1), for example, if the port is switch 3 port 5, the value is 2005

Buttons

- **Delete :**

  Check to delete the entry. It will be deleted during the next save.

- **Add New Entry :**

  Click to add a new entry.

- **Apply :**

  Click to save changes.

- **Reset :**

  Click to undo any changes made locally and revert to previously saved values.

13-3.2 Status

This page provides an overview of RMON Statistics entries. Each page shows up to 99 entries from the Statistics table, default being 20, selected through the "entries per page" input field. When first visited, the web page will show the first 20 entries from the beginning of the Statistics table. The first displayed will be the one with the lowest ID found in the Statistics table.

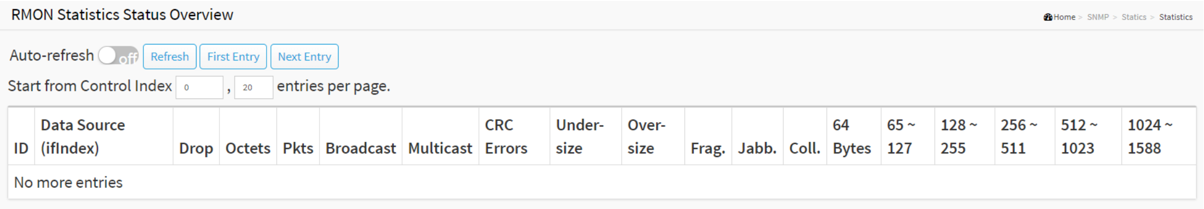
The "Start from Control Index" allows the user to select the starting point in the Statistics table. Clicking the Refresh button will update the displayed table starting from that or the next closest Statistics table match.

The Next Entry will use the last entry of the currently displayed entry as a basis for the next lookup. When the end is reached the text "No more entries" is shown in the displayed table. Use the First Entry button to start over.

Web Interface

To display a RMON Statistics Status in the web interface:

1. Click Security, RMON, Statistics and Status.
2. Specify Port which want to check.
3. Checked "Auto-refresh".
4. Click "Refresh" to refresh the port detailed statistics.



RMON Statistics Status Overview

Start from Control Index 0 , 20 entries per page.

ID	Data Source (ifIndex)	Drop	Octets	Pkts	Broadcast	Multicast	CRC Errors	Under-size	Over-size	Frag.	Jabb.	Coll.	64 Bytes	65 ~ 127	128 ~ 255	256 ~ 511	512 ~ 1023	1024 ~ 1588
No more entries																		

Figure 13-3.2: The RMON Statistics Status

Parameter description:

- **ID :**

  Indicates the index of Statistics entry.

- **Data Source(if Index) :**

  The port ID which wants to be monitored.

- **Drop :**

  The total number of events in which packets were dropped by the probe due to lack of resources.

- **Octets :**

  The total number of octets of data (including those in bad packets) received on the network.

- **Pkts :**

  The total number of packets (including bad packets, broadcast packets, and multicast packets) received.

- **Broadcast :**

  The total number of good packets received that were directed to the broadcast address.

- **Multicast :**

  The total number of good packets received that were directed to a multicast address.

- **CRC Errors :**

  The total number of packets received that had a length (excluding framing bits, but including FCS octets) of between 64 and 1518 octets, inclusive, but had either a bad Frame Check Sequence (FCS) with an integral number of octets (FCS Error) or a bad FCS with a non-integral number of octets (Alignment Error).

- **Under-size :**

  The total number of packets received that were less than 64 octets.

- **Over-size :**

  The total number of packets received that were longer than 1518 octets.

- **Frag. :**

  The number of frames which size is less than 64 octets received with invalid CRC.

- **Jabb. :**

  The number of frames which size is larger than 64 octets received with invalid CRC.

- **Coll. :**

  The best estimate of the total number of collisions on this Ethernet segment.

- **64 Bytes :**

  The total number of packets (including bad packets) received that were 64 octets in length.

- **65~127 :**

  The total number of packets (including bad packets) received that were between 65 to 127 octets in length.

- **128~255 :**

  The total number of packets (including bad packets) received that were between 128 to 255 octets in length.

- **256~511 :**

  The total number of packets (including bad packets) received that were between 256 to 511 octets in length.

- **512~1023 :**

  The total number of packets (including bad packets) received that were between 512 to 1023 octets in length.

- **1024~1588 :**

  The total number of packets (including bad packets) received that were between 1024 to 1588 octets in length.

- **Search :**

  You can search for the information that you want to see.

- **Show entries :**

  You can choose how many items you want to show off.

Buttons

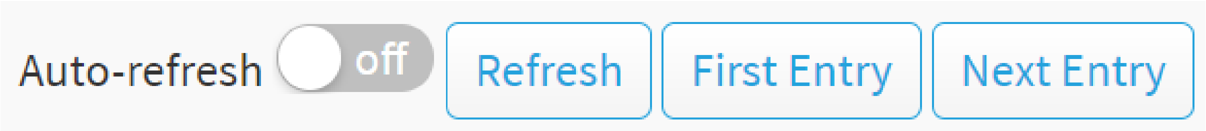


Figure 13-3.2: The RMON Statistics Status buttons

- **Auto-refresh :**

  Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.

- **Refresh :**

  Click to refresh the page immediately.

- **Next :**

  Updates the system log entries, turn to the next page.

- **Previous :**

  Updates the system log entries, turn to the previous page.

13-4 History

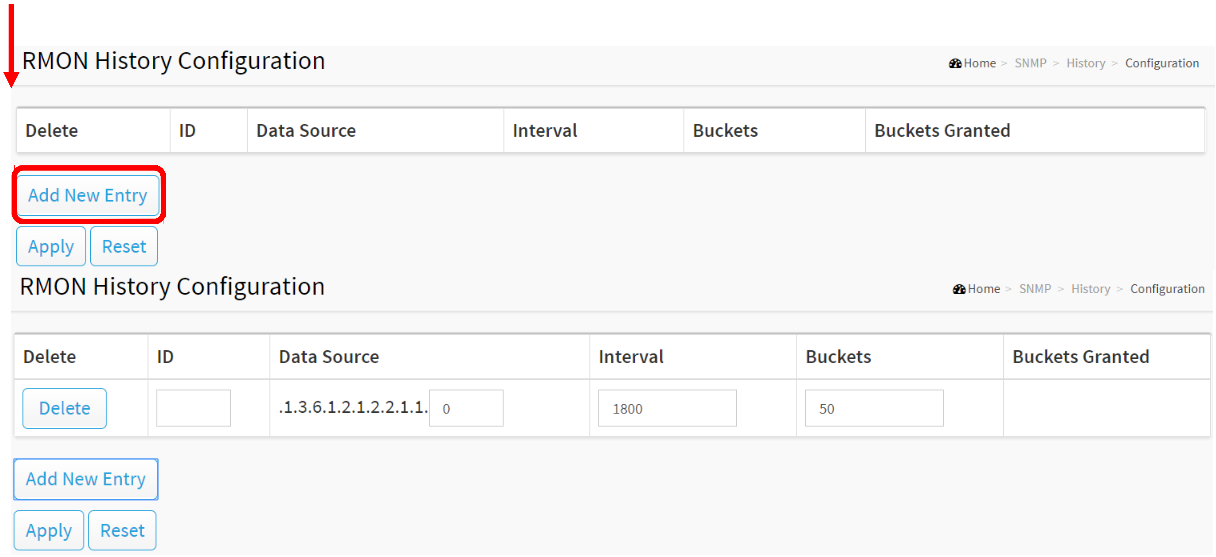
13-4.1 Configuration

Configure RMON History table on this page. The entry index key is **ID.**

Web Interface

To configure the RMON History Configuration in the web interface:

1. Click SNMP, History and Configuration.
2. Click Add New Entry.
3. Specify the ID parameters.
4. Click Apply.



RMON History Configuration

Home > SNMP > History > Configuration

Delete	ID	Data Source	Interval	Buckets	Buckets Granted

Add New Entry

Apply Reset

RMON History Configuration

Home > SNMP > History > Configuration

Delete	ID	Data Source	Interval	Buckets	Buckets Granted
Delete		.1.3.6.1.2.1.2.2.1.1. 0	1800	50	

Add New Entry

Apply Reset

Figure 13-4.1: The RMON History Configuration

Parameter description:

These parameters are displayed on the RMON History Configuration page:

- **ID :**

  Indicates the index of the entry. The range is from 1 to 65535.

- **Data Source :**

  Indicates the port ID which wants to be monitored. If in stacking switch, the value must add 1000*(switch ID-1), for example, if the port is switch 3 port 5, the value is 2005

- **Interval :**

  Indicates the interval in seconds for sampling the history statistics data. The range is from 1 to 3600, default value is 1800 seconds.

- **Buckets :**

  Indicates the maximum data entries associated this History control entry stored in RMON. The range is from 1 to 3600, default value is 50.

- **Buckets Granted :**

  The number of data shall be saved in the RMON.

Buttons

- **Delete :**

  Check to delete the entry. It will be deleted during the next save.

- **Add New Entry :**

  Click to add a new entry.

- **Apply :**

  Click to save changes.

- **Reset :**

  Click to undo any changes made locally and revert to previously saved values.

13-4.2 Status

This page provides an overview of RMON History entries. Each page shows up to 99 entries from the History table, default being 20, selected through the "entries per page" input field. When first visited, the web page will show the first 20 entries from the beginning of the History table. The first displayed will be the one with the lowest History Index and Sample Index found in the History table.

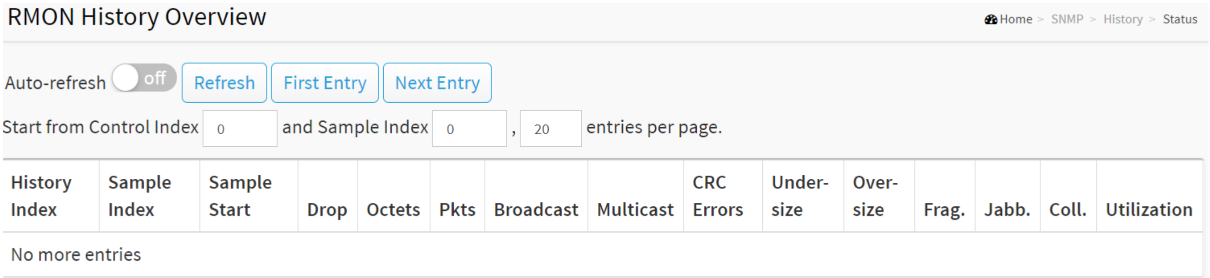
The "Start from History Index and Sample Index" allows the user to select the starting point in the History table. Clicking the Refresh button will update the displayed table starting from that or the next closest History table match.

The Next Entry will use the last entry of the currently displayed entry as a basis for the next lookup. When the end is reached the text "No more entries" is shown in the displayed table. Use the First Entry button to start over.

Web Interface

To display a RMON History Status in the web interface:

1. Click SNMP, History and Status.
2. Checked "Auto-refresh".
3. Click "Refresh" to refresh the port detailed statistics.
4. Click First Entry/Next Entry to change Entry.



RMON History Overview

Auto-refresh off

Start from Control Index 0 and Sample Index 0 , 20 entries per page.

History Index	Sample Index	Sample Start	Drop	Octets	Pkts	Broadcast	Multicast	CRC Errors	Under-size	Over-size	Frag.	Jabb.	Coll.	Utilization
No more entries														

Figure 13-4.2: The RMON History Status

Parameter description:

- **History Index :**

Indicates the index of History control entry.

- **Sample Index :**

  Indicates the index of the data entry associated with the control entry.

- **Sample Start :**

  The value of sysUpTime at the start of the interval over which this sample was measured.

- **Drop :**

  The total number of events in which packets were dropped by the probe due to lack of resources.

- **Octets :**

  The total number of octets of data (including those in bad packets) received on the network.

- **Pkts :**

  The total number of packets (including bad packets, broadcast packets, and multicast packets) received.

- **Broadcast :**

  The total number of good packets received that were directed to the broadcast address.

- **Multicast :**

  The total number of good packets received that were directed to a multicast address.

- **CRC Errors :**

  The total number of packets received that had a length (excluding framing bits, but including FCS octets) of between 64 and 1518 octets, inclusive, but had either a bad Frame Check Sequence (FCS) with an integral number of octets (FCS Error) or a bad FCS with a non-integral number of octets (Alignment Error).

- **Under-size :**

  The total number of packets received that were less than 64 octets.

- **Over-size :**

  The total number of packets received that were longer than 1518 octets.

- **Frag. :**

  The number of frames which size is less than 64 octets received with invalid CRC.

- **Jabb. :**

  The number of frames which size is larger than 64 octets received with invalid CRC.

- **Coll. :**

  The best estimate of the total number of collisions on this Ethernet segment.

- **Utilization :**

  The best estimate of the mean physical layer network utilization on this interface during this sampling interval, in hundredths of a percent.

- **Show entries :**

  You can choose how many items you want to show.

Buttons

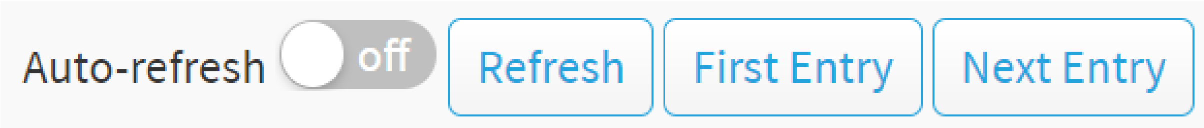


Figure 13-4.2: The RMON History Status buttons

- **Auto-refresh :**

  Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.

- **Refresh :**

  Click to refresh the page immediately.

- **First Entry :**

  Updates the table starting from the first entry in the IPMC Profile Address Configuration.

- **Next Entry :**

  Updates the table, starting with the entry after the last entry currently displayed.

13-5 Alarm

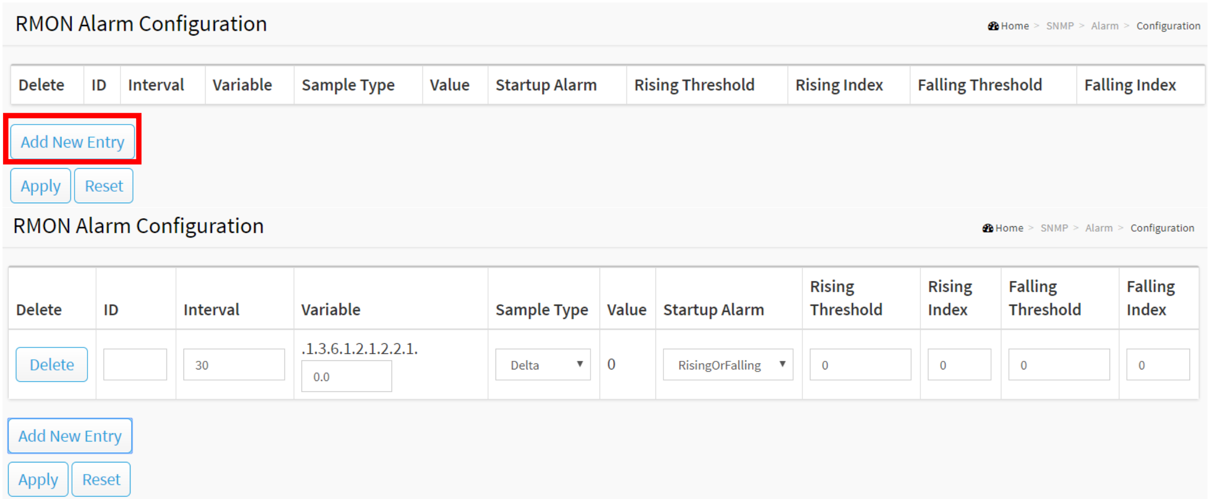
13-5.1 Configuration

Configure RMON Alarm table on this page. The entry index key is **ID.**

Web Interface

To configure the RMON Alarm Configuration in the web interface:

1. Click SNMP, Alarm and Configuration.
2. Click Add New Entry.
3. Specify the ID parameters.
4. Click Apply.



RMON Alarm Configuration

Home > SNMP > Alarm > Configuration

Delete	ID	Interval	Variable	Sample Type	Value	Startup Alarm	Rising Threshold	Rising Index	Falling Threshold	Falling Index

Add New Entry
Apply
Reset

RMON Alarm Configuration

Home > SNMP > Alarm > Configuration

Delete	ID	Interval	Variable	Sample Type	Value	Startup Alarm	Rising Threshold	Rising Index	Falling Threshold	Falling Index
Delete		30	.1.3.6.1.2.1.2.2.1. 0.0	Delta ▾	0	RisingOrFalling ▾	0	0	0	0

Add New Entry
Apply
Reset

Figure 13-5.1: The RMON Alarm Configuration

Parameter description:

These parameters are displayed on the RMON Alarm Configuration page:

- **ID :**

  Indicates the index of the entry. The range is from 1 to 65535.

- **Interval :**

  Indicates the interval in seconds for sampling and comparing the rising and falling threshold. The range is from 1 to 2^31-1.

- **Variable :**

  Indicates the particular variable to be sampled, the possible variables are:

  InOctets:
  The total number of octets received on the interface, including framing characters.

  InUcastPkts:
  The number of uni-cast packets delivered to a higher-layer protocol.

  InNUcastPkts:
  The number of broad-cast and multi-cast packets delivered to a higher-layer protocol.

  InDiscards:
  The number of inbound packets that are discarded even the packets are normal.

InErrors:
The number of inbound packets that contained errors preventing them from being deliverable to a higher-layer protocol.

InUnknownProtos:
the number of the inbound packets that were discarded because of the unknown or un-support protocol.

OutOctets:
The number of octets transmitted out of the interface , including framing characters.

OutUcastPkts:
The number of uni-cast packets that request to transmit.

OutNUcastPkts:
The number of broad-cast and multi-cast packets that request to transmit.

OutDiscards:
The number of outbound packets that are discarded event the packets is normal.

OutErrors:
The The number of outbound packets that could not be transmitted because of errors.

OutQLen:
The length of the output packet queue (in packets).

- **Sample Type :**

  The method of sampling the selected variable and calculating the value to be compared against the thresholds, possible sample types are:

  Absolute: Get the sample directly.

  Delta: Calculate the difference between samples (default).

- **Value :**

  The value of the statistic during the last sampling period.

- **Startup Alarm :**

  The method of sampling the selected variable and calculating the value to be compared against the thresholds, possible sample types are:

  RisingTrigger alarm when the first value is larger than the rising threshold.

  FallingTrigger alarm when the first value is less than the falling threshold.

  RisingOrFallingTrigger alarm when the first value is larger than the rising threshold or less than the falling threshold (default).

- **Rising Threshold :**

  Rising threshold value (-2147483648-2147483647).

- **Rising Index :**

  Rising event index (1-65535).

- **Falling Threshold :**

  Falling threshold value (-2147483648-2147483647)

- **Falling Index :**

  Falling event index (1-65535).

Buttons

- **Delete :**

  Check to delete the entry. It will be deleted during the next save.

- **Add New Entry :**

  Click to add a new entry.

- **Apply :**

  Click to save changes.

- **Reset :**

  Click to undo any changes made locally and revert to previously saved values.

13-5.2 Status

This page provides an overview of RMON Alarm entries. Each page shows up to 99 entries from the Alarm table, default being 20, selected through the "entries per page" input field. When first visited, the web page will show the first 20 entries from the beginning of the Alarm table. The first displayed will be the one with the lowest ID found in the Alarm table.

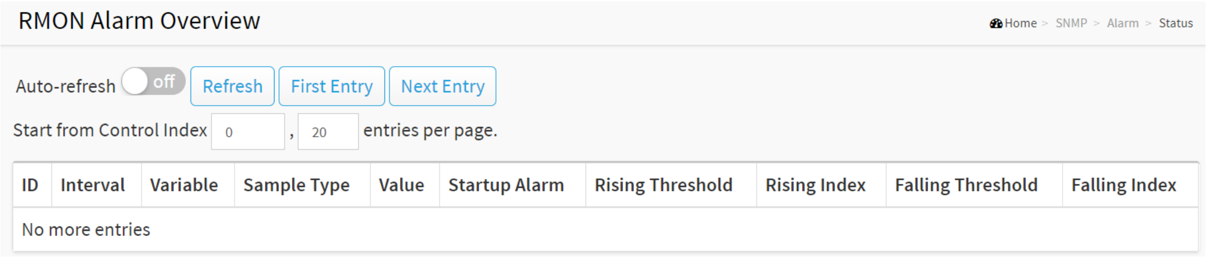
The "Start from Control Index" allows the user to select the starting point in the Alarm table. Clicking the Refresh button will update the displayed table starting from that or the next closest Alarm table match.

The Next Entry will use the last entry of the currently displayed entry as a basis for the next lookup. When the end is reached the text "No more entries" is shown in the displayed table. Use the First Entry button to start over.

Web Interface

To display a RMON Alarm Status in the web interface:

1. Click SNMP, Alarm and Status.
2. Checked "Auto-refresh".
3. Click "Refresh" to refresh the port detailed statistics.
4. Click First Entry/Next Entry to change Entry.



RMON Alarm Overview

Home > SNMP > Alarm > Status

Auto-refresh off Refresh First Entry Next Entry

Start from Control Index 0 , 20 entries per page.

ID	Interval	Variable	Sample Type	Value	Startup Alarm	Rising Threshold	Rising Index	Falling Threshold	Falling Index
No more entries									

Figure 13-5.2: RMON Alarm Status

Parameter description:

- **ID :**

  Indicates the index of Alarm control entry.

- **Interval :**

  Indicates the interval in seconds for sampling and comparing the rising and falling threshold.

- **Variable :**

Indicates the particular variable to be sampled

- **Sample Type :**

  The method of sampling the selected variable and calculating the value to be compared against the thresholds.

- **Value :**

  The value of the statistic during the last sampling period.

- **Startup Alarm :**

  The alarm that may be sent when this entry is first set to valid.

- **Rising Threshold :**

  Rising threshold value.

- **Rising Index :**

  Rising event index.

- **Falling Threshold :**

  Falling threshold value.

- **Falling Index :**

  Falling event index.

- **Show entries :**

  You can choose how many items you want to show off.

Buttons

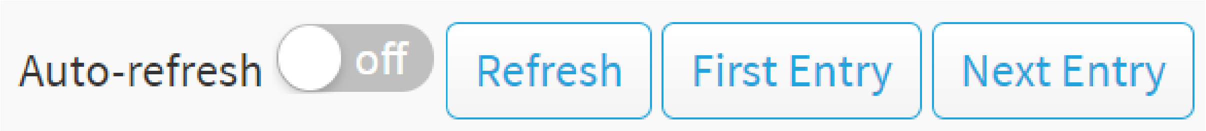


Figure 13-5.2: RMON Alarm Status buttons

- **Auto-refresh :**

  Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.

- **Refresh :**

  Click to refresh the page immediately.

- **First Entry :**

  Updates the table starting from the first entry in the IPMC Profile Address Configuration.

- **Next Entry :**

  Updates the table, starting with the entry after the last entry currently displayed.

13-6 Event

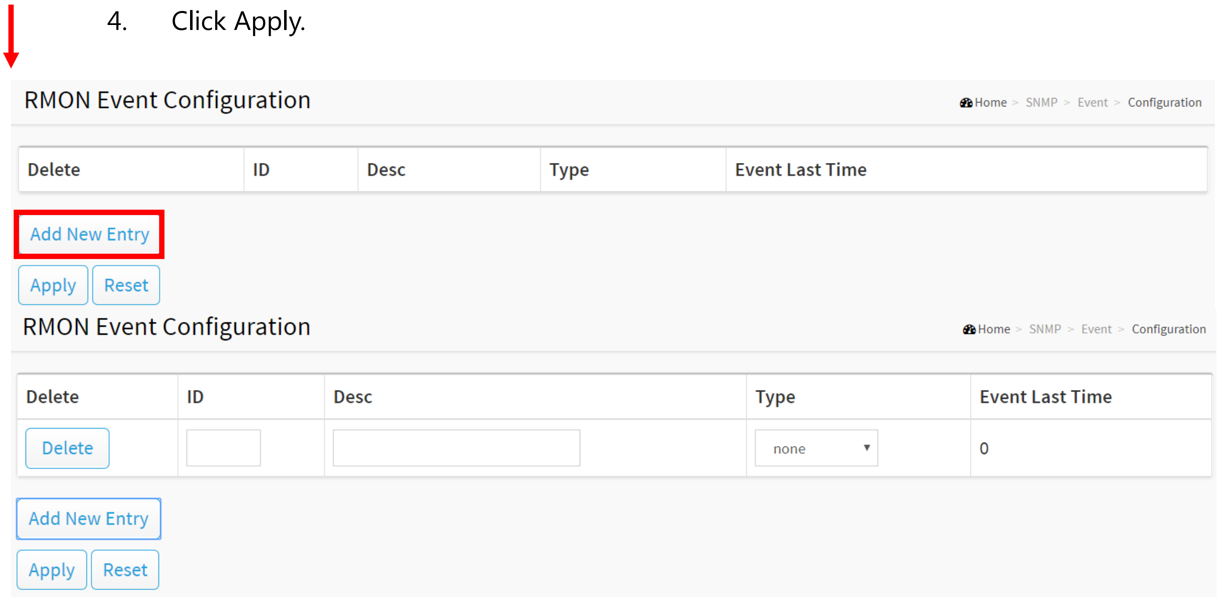
13-6.1 Configuration

Configure RMON Event table on this page. The entry index key is **ID.**

Web Interface

To configure the RMON Event Configuration in the web interface:

1. Click SNMP, Event and Configuration.
2. Click Add New Entry.
3. Specify the ID parameters.
4. Click Apply.



RMON Event Configuration

Home > SNMP > Event > Configuration

Delete	ID	Desc	Type	Event Last Time

Add New Entry
Apply
Reset

RMON Event Configuration

Home > SNMP > Event > Configuration

Delete	ID	Desc	Type	Event Last Time
Delete			none	0

Add New Entry
Apply
Reset

Figure 13-6.1: The RMON Event Configuration

Parameter description:

These parameters are displayed on the RMON History Configuration page:

- **ID :**

  Indicates the index of the entry. The range is from 1 to 65535.

- **Desc :**

  Indicates this event, the string length is from 0 to 127, default is a null string.

- **Type :**

  Indicates the notification of the event, the possible types are:

  None: No SNMP log is created, no SNMP trap is sent.

  Log: Create SNMP log entry when the event is triggered.

  Snmp trap: Send SNMP trap when the event is triggered.

  Log and trap: Create SNMP log entry and sent SNMP trap when the event is triggered.

- **Event Last Time :**

  Indicates the value of sysUpTime at the time this event entry last generated an event.

Buttons

- **Delete :**

  Check to delete the entry. It will be deleted during the next save.

- **Add New Entry :**

  Click to add a new entry.

- **Apply :**

  Click to save changes.

- **Reset :**

  Click to undo any changes made locally and revert to previously saved values.

13-6.2 Status

This page provides an overview of RMON Event table entries. Each page shows up to 99 entries from the Event table, default being 20, selected through the "entries per page" input field. When first visited, the web page will show the first 20 entries from the beginning of the Event table. The first displayed will be the one with the lowest Event Index and Log Index found in the Event table.

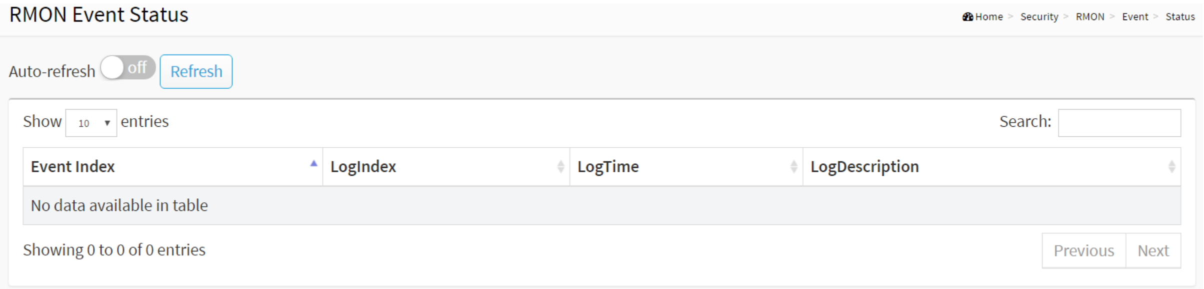
The "Start from Event Index and Log Index" allows the user to select the starting point in the Event table. Clicking the Refresh button will update the displayed table starting from that or the next closest Event table match.

The Next Entry will use the last entry of the currently displayed entry as a basis for the next lookup. When the end is reached the text "No more entries" is shown in the displayed table. Use the First Entry button to start over.

Web Interface

To display a RMON Event Status in the web interface:

1. Click SNMP, Event and Status.
2. Checked "Auto-refresh".
3. Click " Refresh" to refresh the port detailed statistics
4. Click First Entry/Next Entry to change Entry.



RMON Event Status

Home > Security > RMON > Event > Status

Auto-refresh off Refresh

Show 10 entries Search:

Event Index	LogIndex	LogTime	LogDescription
No data available in table			

Showing 0 to 0 of 0 entries

Figure 13-6.2: RMON Event Status

Parameter description:

- **Event Index :**

  Indicates the index of the event entry.

- **Log Index :**

  Indicates the index of the log entry.

- **LogTIme :**

  Indicates Event log time

- **LogDescription :**

  Indicates the Event description.

- **Show entries :**

  You can choose how many items you want to show.

Buttons

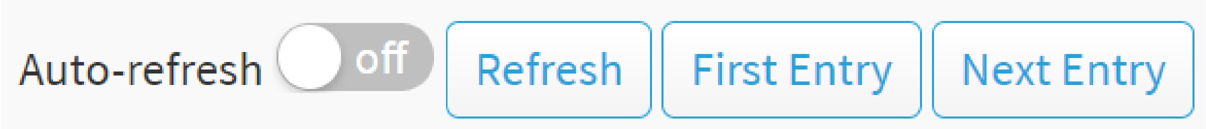


Figure 13-6.2: RMON Event Status buttons

- **Auto-refresh :**

  Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.

- **Refresh :**

  Click to refresh the page immediately.

- **First Entry :**

  Updates the table starting from the first entry in the IPMC Profile Address Configuration.

- **Next Entry :**

  Updates the table, starting with the entry after the last entry currently displayed.

Chapter 14 MEP

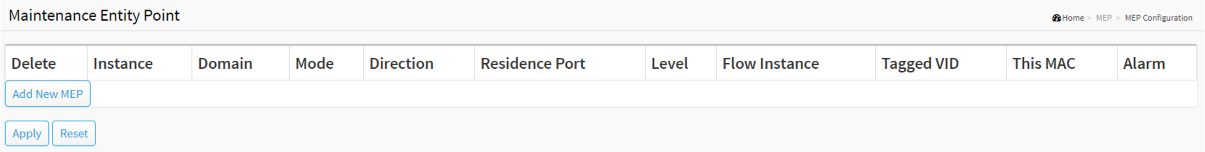
14-1 MEP Configuration

The Maintenance Entity Point instances are configured here.

Web Interface

To configure the MEP parameters in the web interface:

1. Click MEP.
2. Specify the Maintenance Entity Point parameters.
3. Click Apply to apply the change.



Maintenance Entity Point

Home > MEP > MEP Configuration

Delete	Instance	Domain	Mode	Direction	Residence Port	Level	Flow Instance	Tagged VID	This MAC	Alarm

Figure 14-1: The Maintenance Entity Point

Parameter description:

- **Delete :**

  This box is used to mark a MEP for deletion in next Save operation.

- **Instance :**

  The ID of the MEP. Click on the ID of a MEP to enter the configuration page. The range is from 1through 3124.

- **Domain :**

  Port: This is a MEP in the Port Domain.

  VLAN: This is a MEP in the VLAN Domain. 'Flow Instance' is a VLAN. In case of Up-MEP the VLAN must be created

- **Mode :**

  MEP: This is a Maintenance Entity End Point.

  MIP: This is a Maintenance Entity Intermediate Point.

- **Direction :**

  Down: This is a Down MEP - monitoring ingress OAM and traffic on 'Residence Port'.

  Up: This is a Up MEP - monitoring egress OAM and traffic on 'Residence Port'.

- **Residence Port :**

  The port where MEP is monitoring - see 'Direction'. For a EVC MEP the port must be a port in the EVC. For a VLAN MEP the port must be a VLAN member.

- **Level :**

The MEG level of this MEP.

- **Flow Instance :**

  The MEP is related to this flow - See 'Domain'. This is not relevant and not shown in case of Port MEP.

- **Tagged VID :**

  Port MEP: An outer C/S-tag (depending on VLAN Port Type) is added with this VID. Entering '0' means no TAG added.

  EVC MEP: This is not used.

  VLAN MEP: This is not used.

  EVC MIP: On Serval, this is the Subscriber VID that identify the subscriber flow in this EVC where the MIP is active.

- **This MAC :**

  The MAC of this MEP - can be used by other MEP when unicast is selected (Info only).

- **Alarm :**

  There is an active alarm on the MEP or operational state is not "Up".

Buttons

- **Add New MEP :**

  Click to add a new MEP entry.

- **Apply :**

  Click to save changes.

- **Reset :**

  Click to undo any changes made locally and revert to previously saved values.

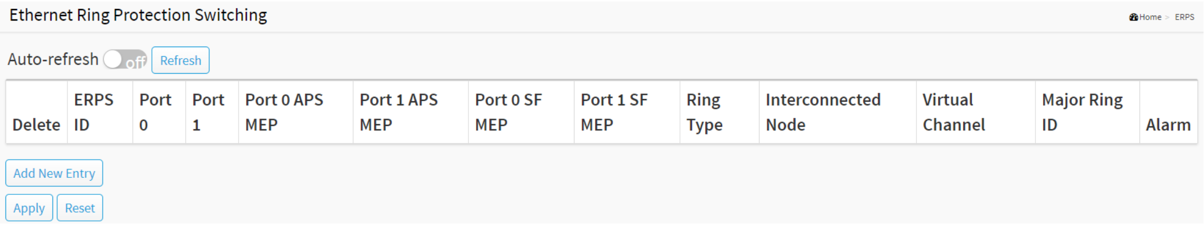
Chapter 15 ERPS

The ERPS instances are configured here.

Web Interface

To configure the Ethernet Ring Protection Switching parameters in the web interface:

1. Click ERPS.
2. Specify the Ethernet Ring Protection Switching parameters.
3. Click Apply to apply the change.



Ethernet Ring Protection Switching

Delete	ERPS ID	Port 0	Port 1	Port 0 APS MEP	Port 1 APS MEP	Port 0 SF MEP	Port 1 SF MEP	Ring Type	Interconnected Node	Virtual Channel	Major Ring ID	Alarm

Figure 15: The Ethernet Ring Protection Switching

Parameter description:

- **Delete :**

  This box is used to mark an EPS for deletion in next save operation.

- **ERPS ID :**

  The ID of the created Protection group, It must be an integer value between 1 and 64. The maximum number of ERPS Protection Groups that can be created are 64. Click on the ID of an Protection group to enter the configuration page.

- **Port 0 :**

  This will create a Port 0 of the switch in the ring.

- **Port 1 :**

  This will create "Port 1" of the switch in the Ring. As interconnected sub-ring will have only one ring port, "Port 1" is configured as "0" for interconnected sub-ring. "0" in this field indicates that no "Port 1" is associated with this instance

- **Port 0 SF MEP :**

  The Port 0 Signal Fail reporting MEP.

- **Port 1 SF MEP :**

  The Port 1 Signal Fail reporting MEP. As only one SF MEP is associated with interconnected sub-ring without virtual channel, it is configured as "0" for such ring instances. "0" in this field indicates that no Port 1 SF MEP is associated with this instance.

- **Port 0 APS MEP :**

  The Port 0 APS PDU handling MEP.

- **Port 1 APS MEP :**

The Port 1 APS PDU handling MEP. As only one APS MEP is associated with interconnected sub-ring without virtual channel, it is configured as "0" for such ring instances. "0" in this field indicates that no Port 1 APS MEP is associated with this instance.

- **Ring Type :**

  Type of Protecting ring. It can be either major ring or sub-ring.

- **Interconnected Node :**

  Interconnected Node indicates that the ring instance is interconnected. Click on the checkbox to configure this. "Yes" indicates it is an interconnected node for this instance. "No" indicates that the configured instance is not interconnected.

- **Virtual Channel :**

  Sub-rings can either have virtual channel or not on the interconnected node. This is configured using "Virtual Channel" checkbox. "Yes" indicates it is a sub-ring with virtual channel. "No" indicates, sub-ring doesn't have virtual channel.

- **Major Ring ID :**

  Major ring group ID for the interconnected sub-ring. It is used to send topology change updates on major ring. If ring is major, this value is same as the protection group ID of this ring.

- **Alarm :**

  There is an active alarm on the ERPS.

Buttons

Figure 15: The Ethernet Ring Protection Switching buttons

- **Auto-refresh :**

  Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.

- **Refresh :**

  Click to refresh the page immediately.

- **Add New Protection Group:**

  Click to add a new Protection group entry.

- **Apply :**

  Click to save changes.

- **Reset :**

  Click to undo any changes made locally and revert to previously saved values.

Chapter 16 PTP

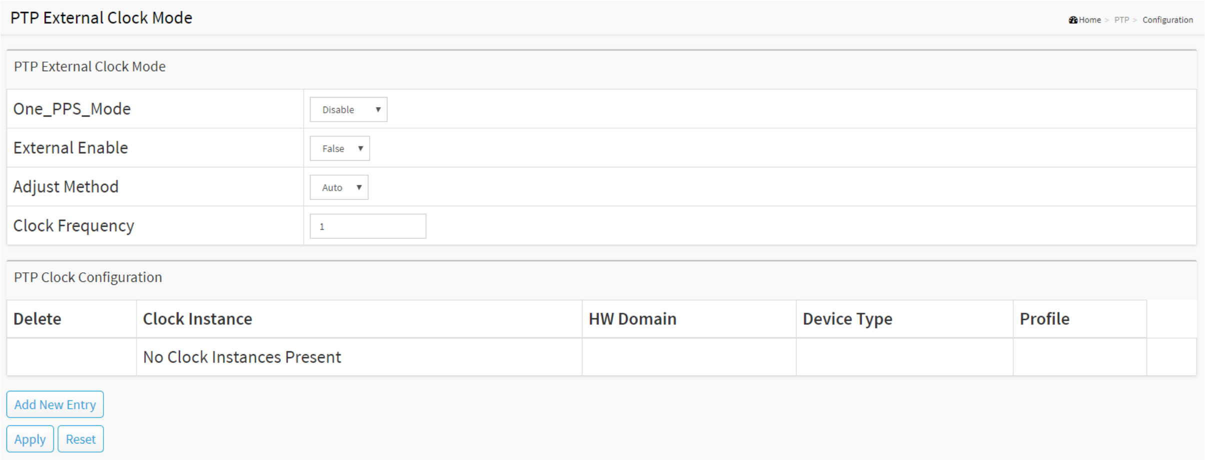
16-1 Configuration

This page allows the user to configure and inspect the current PTP clock settings.

Web Interface

To configure the PTP in the web interface:

1. Click PTP and Configuraiton.
2. Scroll to select the mode to enable or disable
3. Specify the parameters in each blank field.
4. Click the save to save the setting
5. If you want to cancel the setting then you need to click the Reset button. It will revert to previously saved values



PTP External Clock Mode

Home > PTP > Configuration

PTP External Clock Mode

One_PPS_Mode	Disable ▾
External Enable	False ▾
Adjust Method	Auto ▾
Clock Frequency	1

PTP Clock Configuration

Delete	Clock Instance	HW Domain	Device Type	Profile
	No Clock Instances Present			

Figure 16-1: The PTP configuration

Parameter description:

PTP External Clock Configuration

- **One_PPS_Mode :**

  This Selection box will allow you to select the One_pps_mode configuration.

  The following values are possible:

  1. Output : Enable the 1 pps clock output

  2. Input : Enable the 1 pps clock input

  3. Disable : Disable the 1 pps clock in/out-put

- **External Enable :**

  This Selection box will allow you to configure the External Clock output.

  The following values are possible:

1. True : Enable the external clock output

2. False : Disable the external clock output

- **Adjust Method :**

  This Selection box will allow you to configure the Frequency adjustment configuration.

  1. LTC : Select Local Time Counter (LTC) frequency control

  2. Single : Select SyncE DPLL frequency control, if allowed by SyncE

  3. Independent : Select an oscillator independent of SyncE for frequency control, if supported by the HW

  4. Common : Select second DPLL for PTP, Both DPLL have the same (SyncE recovered) clock.

  4. Auto : AUTO Select clock control, based on PTP profile and available HW resources.

- **Clock Frequency :**

  This will allow to set the Clock Frequency.

  The possible range of values are 1 - 25000000 (1 - 25MHz)

PTP Clock Configuration

- **Delete :**

  Check this box and click on 'Save' to delete the clock instance.

- **Clock Instance :**

  Indicates the instance number of a particular Clock Instance [0..3].

  Click on the Clock Instance number to edit the Clock details.

- **HW Domain :**

  Indicates the HW clock domain used by the clock.

- **Device Type :**

  Indicates the Type of the Clock Instance. There are five Device Types.

  1. Ord-Bound - clock's Device Type is Ordinary-Boundary Clock.

  2. P2p Transp - clock's Device Type is Peer to Peer Transparent Clock.

  3. E2e Transp - clock's Device Type is End to End Transparent Clock.

  4. Master Only - clock's Device Type is Master Only.

  5. Slave Only - clock's Device Type is Slave Only.

- **Profile :**

  Indicates the profile used by the clock.

Buttons

- **Add New Entry :**

  Click to add a new clock instance.

- **Apply :**

  Click to save changes.

- **Reset :**

  Click to undo any changes made locally and revert to previously saved values.

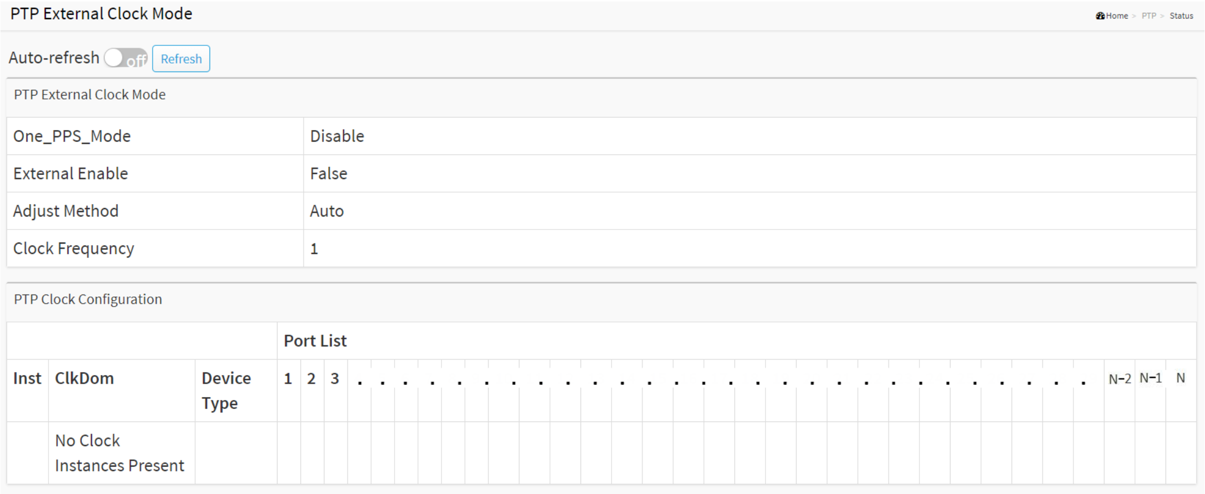
16-2 Status

This page allows the user to inspect the current PTP clock settings.

Web Interface

To display the PTP status in the web interface:

1. Click PTP and Status.
2. Specify the PTP parameters.
3. Click Apply to apply the change.



PTP External Clock Mode

PTP External Clock Mode

One_PPS_Mode	Disable
External Enable	False
Adjust Method	Auto
Clock Frequency	1

PTP Clock Configuration

			Port List						
Inst	ClkDom	Device Type	1	2	3	. . . .	N-2	N-1	N
	No Clock Instances Present								

Figure 16-2: The PTP Status

Parameter description:

PTP External Clock Description

- **One_PPS_Mode :**

  Shows the current One_pps_mode configured.

  Output : Enable the 1 pps clock output

  Input : Enable the 1 pps clock input

  Disable : Disable the 1 pps clock in/out-put

- **External Enable :**

  Shows the current External clock output configuration.

  True : Enable the external clock output

  False : Disable the external clock output

- **Adjust Method :**

  Shows the current Frequency adjustment configuration.

  LTC : Use Local Time Counter (LTC) frequency control

  Single : Use SyncE DPLL frequency control, if allowed by SyncE

  Independent : Use an oscillator independent of SyncE for frequency control, if supported by the HW

  Common : Use second DPLL for PTP, Both DPLL have the same (SyncE recovered) clock.

Auto : AUTO Select clock control, based on PTP profile and available HW resources.

- **Clock Frequency :**

  Shows the current clock frequency used by the External Clock.

  The possible range of values are 1 - 25000000 (1 - 25MHz)

PTP Clock Description

- **Inst :**

  Indicates the Instance of a particular Clock Instance [0..3].

  Click on the Clock Instance number to monitor the Clock details.

- **ClkDom :**

  Indicates the Clock domain used by the Instance of a particular Clock Instance [0..3].

- **Device Type :**

  Indicates the Type of the Clock Instance. There are five Device Types.

  Ord-Bound - Clock's Device Type is Ordinary-Boundary Clock.

  P2p Transp - Clock's Device Type is Peer to Peer Transparent Clock.

  E2e Transp - Clock's Device Type is End to End Transparent Clock.

  Master Only - Clock's Device Type is Master Only.

  Slave Only - Clock's Device Type is Slave Only.

- **Port List :**

  Shows the ports configured for that Clock Instance.

Buttons

Figure 16-2: The PTP buttons

- **Auto-refresh :**

  Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.

- **Refresh :**

  Click to refresh the page immediately.

- **Apply :**

  Click to save changes.

- **Reset :**

  Click to undo any changes made locally and revert to previously saved values.

Chapter 17 Event Notification

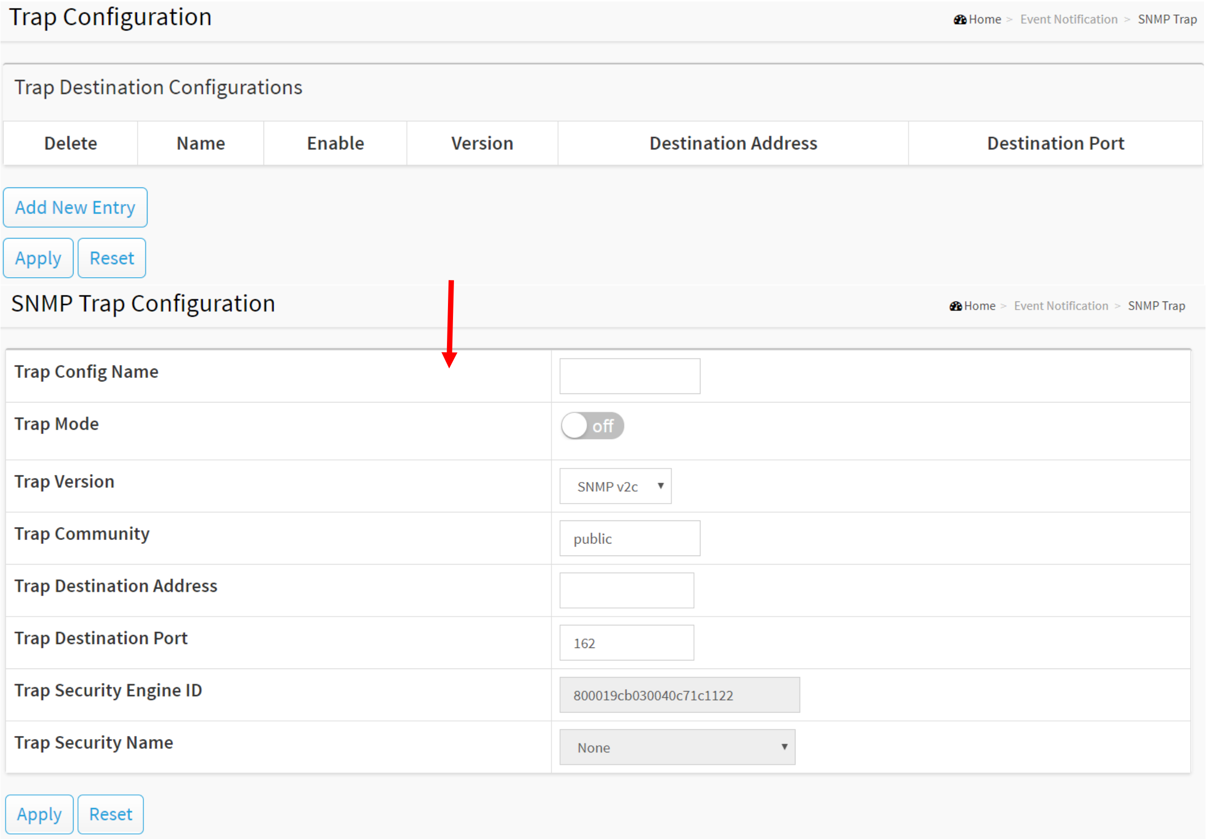
17-1 SNMP Trap

Configure Trap on this page.

Web Interface

To configure SNMP Trap Configuration in the web interface:

1. Click Event Notification and SNMP Trap.
2. Click Add New Entry then you can create new SNMP Trap on the switch.
3. Specify SNMP Trap parameter.
4. Click Apply.



Trap Configuration

Home > Event Notification > SNMP Trap

Trap Destination Configurations

Delete	Name	Enable	Version	Destination Address	Destination Port

Add New Entry
Apply
Reset

SNMP Trap Configuration

Home > Event Notification > SNMP Trap

Trap Config Name	
Trap Mode	off
Trap Version	SNMP v2c
Trap Community	public
Trap Destination Address	
Trap Destination Port	162
Trap Security Engine ID	800019cb030040c71c1122
Trap Security Name	None

Figure 17-1: The SNMP Trap Configuration

Parameter description:

Trap Destination Configurations

- **Name :**

  Indicates the trap Configuration's name. Indicates the trap destination's name.

- **Enable :**

Indicates the trap destination mode operation. Possible modes are:
Enabled: Enable SNMP trap mode operation.
Disabled: Disable SNMP trap mode operation.

- **Version :**

  Indicates the SNMP trap supported version. Possible versions are:
  SNMPv1: Set SNMP trap supported version 1.
  SNMPv2c: Set SNMP trap supported version 2c.
  SNMPv3: Set SNMP trap supported version 3.

- **Destination Address :**

  Indicates the SNMP trap destination address. It allow a valid IP address in dotted decimal notation ('x.y.z.w').

  And it also allow a valid hostname. A valid hostname is a string drawn from the alphabet (A-Za-z), digits (0-9), dot (.), dash (-). Spaces are not allowed, the first character must be an alpha character, and the first and last characters must not be a dot or a dash.

  Indicates the SNMP trap destination IPv6 address. IPv6 address is in 128-bit records represented as eight fields of up to four hexadecimal digits with a colon separating each field (:). For example, 'fe80::215:c5ff:fe03:4dc7'. The symbol '::' is a special syntax that can be used as a shorthand way of representing multiple 16-bit groups of contiguous zeros; but it can appear only once. It can also represent a legally valid IPv4 address. For example, '::192.1.2.34'.

- **Destination port :**

  Indicates the SNMP trap destination port. SNMP Agent will send SNMP message via this port, the port range is 1~65535.

SNMP Trap Configuration

- **Trap Config Name :**

  Indicates which trap Configuration's name for configuring. The allowed string length is 1 to 32, and the allowed content is ASCII characters from 33 to 126.

- **Trap Mode :**

  Indicates the SNMP mode operation. Possible modes are:
  on: Enable SNMP mode operation.
  off: Disable SNMP mode operation.

- **Trap Version :**

  Indicates the SNMP supported version. Possible versions are:
  SNMP v1: Set SNMP supported version 1.
  SNMP v2c: Set SNMP supported version 2c.

  SNMP v3: Set SNMP supported version 3.

- **Trap Community :**

  Indicates the community access string when sending SNMP trap packet. The allowed string length is 0 to 63, and the allowed content is ASCII characters from 33 to 126.

- **Trap Destination Address :**

  Indicates the SNMP trap destination address. It allow a valid IP address in dotted decimal notation ('x.y.z.w').

  And it also allow a valid hostname. A valid hostname is a string drawn from the alphabet (A-Za-z), digits (0-9), dot (.), dash (-). Spaces are not allowed, the first character must be an alpha character, and the first and last characters must not be a dot or a dash.

  Indicates the SNMP trap destination IPv6 address. IPv6 address is in 128-bit records represented as eight fields of up to four hexadecimal digits with a colon separating each field (:). For example, 'fe80::215:c5ff:fe03:4dc7'. The symbol '::' is a special syntax that can be used as a shorthand way of representing multiple 16-bit groups of contiguous zeros; but it can appear only once. It can also represent a legally valid IPv4 address. For example, '::192.1.2.34'.

- **Trap Destination port :**

  Indicates the SNMP trap destination port. SNMP Agent will send SNMP message via this port, the port range is 1~65535.

- **Trap Security Engine ID :**

  Indicates the SNMP trap security engine ID. SNMPv3 sends traps and informs using USM for authentication and privacy. A unique engine ID for these traps and informs is needed. When "Trap Probe Security Engine ID" is enabled, the ID will be probed automatically. Otherwise, the ID specified in this field is used. The string must contain an even number(in hexadecimal format) with number of digits between 10 and 64, but all-zeros and all-'F's are not allowed.

- **Trap Security Name :**

  Indicates the SNMP trap security name. SNMPv3 traps and informs using USM for authentication and privacy. A unique security name is needed when traps and informs are enabled.

Buttons

- **Add New Entry :**

  Click to add a new entry.

- **Apply :**

  Click to save changes.

- **Reset :**

  Click to undo any changes made locally and revert to previously saved values.

17-2 eMail

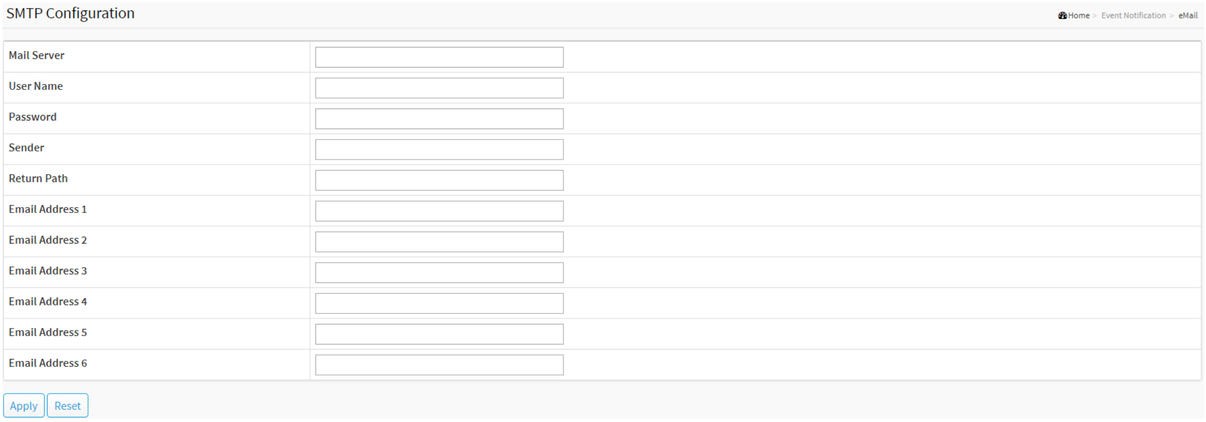
Configure SMTP (Simple Mail Transfer Protocol) on this page. Simple Mail Transfer Protocol is the message-exchange standard for the Internet.

The Switch is to be configured as a client of SMTP while the server is a remote device that will receive messages from the switch that alarm events occurred.

Web Interface

To configure SMTP Configuration in the web interface:

1. Click Event Notification and eMail.
2. Specify SMTP Configuration parameter.
3. Click Apply.



SMTP Configuration

Mail Server	
User Name	
Password	
Sender	
Return Path	
Email Address 1	
Email Address 2	
Email Address 3	
Email Address 4	
Email Address 5	
Email Address 6	

Figure 17-2: The SMTP Configuration

Parameter description:

- **Mail Server :**

  The IP address or hostname of the mail server. IP address is expressed in dotted decimal notation. This will be the device that sends out the mail for you

- **User Name :**

  Specify the username on the mail server.

- **Password :**

  Specify the password of the user on the mail server.

- **Sender :**

  Specify the sender name of the alarm mail.

- **Return Path :**

  Specify the sender email address of the alarm mail. This address will be the "from" address on the email message.

- **Email Address # :**

  Specify the email address of the receiver.

Buttons

- **Apply :**

Click to save changes.

- **Reset :**

  Click to undo any changes made locally and revert to previously saved values.

17-3 Log

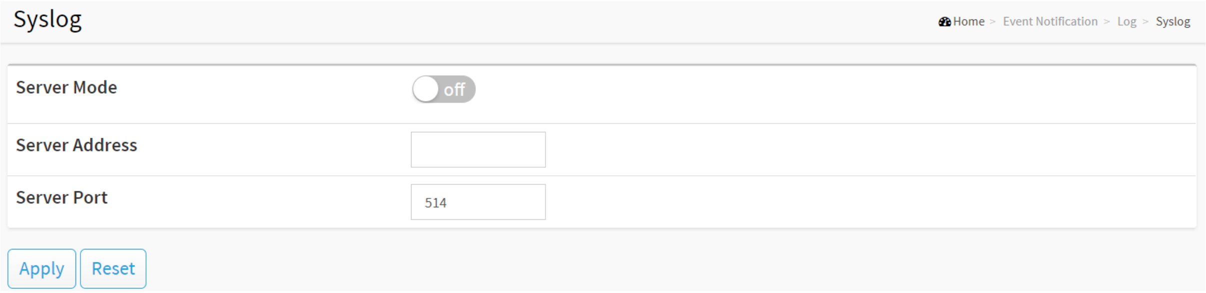
17-3.1 Syslog

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 Syslog Configuration in the web interface:

1. Click Event Notification, Log and Syslog.
2. Evoke the Server Mode to enable it.
3. Specify the syslog parameters include Server Address and Server Port.
4. Click Apply.



Server Mode	off
Server Address	
Server Port	514

Figure 17-3.1: The System Log configuration

Parameter description:

- **Server Mode :**

  Indicates the server mode operation. When the mode operation is enabled, the syslog message will send out to syslog server. The syslog protocol is based on UDP communication and received on UDP port 514 and the syslog server will not send acknowledgments back sender since UDP is a connectionless protocol and it does not provide acknowledgments. The syslog packet will always send out even if the syslog server does not exist. Possible modes are:
  Enabled: Enable server mode operation.
  Disabled: Disable server mode operation.

- **Server Address :**

  Indicates the IPv4 host address of syslog server. If the switch provide DNS feature, it also can be a domain name.

- **Server Port :**

  Indicates the service port of syslog server.

Buttons

- **Apply :**

  Click to save changes.

- **Reset :**

Click to undo any changes made locally and revert to previously saved values.

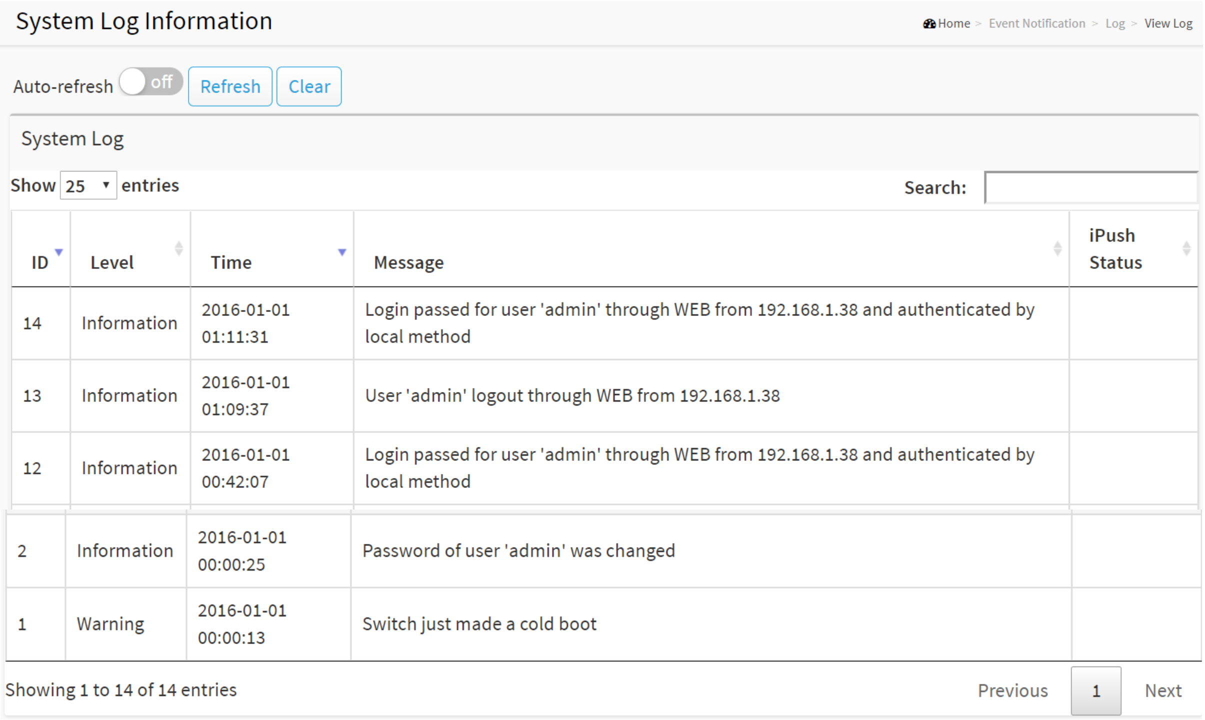
17-3.2 View Log

This section describes that display the system log information of the switch

Web Interface

To display the log Information in the web interface:

1. Click Event Notification, Log and View Log.
2. Display the log information.



ID	Level	Time	Message	iPush Status
14	Information	2016-01-01 01:11:31	Login passed for user 'admin' through WEB from 192.168.1.38 and authenticated by local method	
13	Information	2016-01-01 01:09:37	User 'admin' logout through WEB from 192.168.1.38	
12	Information	2016-01-01 00:42:07	Login passed for user 'admin' through WEB from 192.168.1.38 and authenticated by local method	
2	Information	2016-01-01 00:00:25	Password of user 'admin' was changed	
1	Warning	2016-01-01 00:00:13	Switch just made a cold boot	

Showing 1 to 14 of 14 entries

Figure 17-3.2: The System Log Information

Parameter description:

- **ID :**

  ID (>= 1) of the system log entry.

- **Level :**

  level of the system log entry. The following level types are supported:

  Debug : debug level message.

  Info : informational message.

  Notice : normal, but significant, condition.

  Warning : warning condition.

  Error : error condition.

  Crit : critical condition.

  Alert : action must be taken immediately.

Emerg : system is unusable.

- **Time :**

  It will display the log record by device time. The time of the system log entry.

- **Message :**

  It will display the log detail message. The message of the system log entry.

- **Search :**

  You can search for the information that you want to see.

- **Show entries :**

  You can choose how many items you want to show.

Buttons

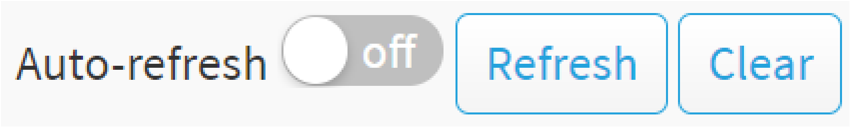


Figure 14-3.2: View Log buttons

- **Auto-refresh :**

  Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.

- **Refresh :**

  Updates the system log entries, starting from the current entry ID.

- **Clear :**

  Clear all the system log entries.

- **Next :**

  Updates the system log entries, turn to the next page.

- **Previous :**

  Updates the system log entries, turn to the previous page.

17-4 Digital I/O

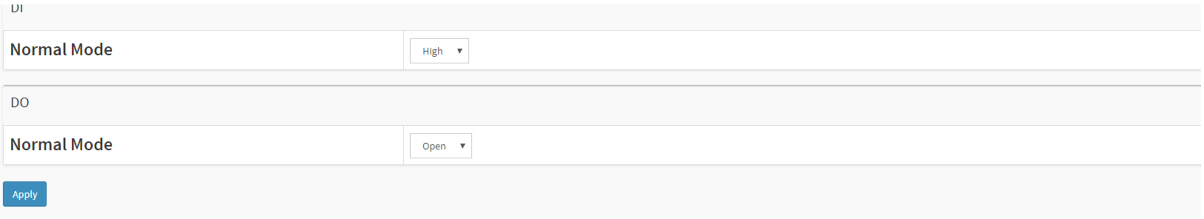
Configure the normal modes of digital input/output (DI/DO).

Web Interface

To configure the digital input/output:

1. Click Event Notification and Digital I/O.
2. Scroll to select the DI/DO Mode.
3. Click the Apply to save the setting.

.



DI

Normal Mode: High

DO

Normal Mode: Open

Figure 17-4: The Digital I/O Configuration

Parameter description:

- **Group Name :**

  The name identifying the severity group.

- **DI Normal Mode**

  Set the normal mode of the digital input(DI). You can set it to High or Low.

- **DO Normal Mode**

  Set the normal mode of the digital output(DO). You can set it to Open or Close.

Buttons

- **Apply :**

  Click to save changes.

17-5 Event Configuration

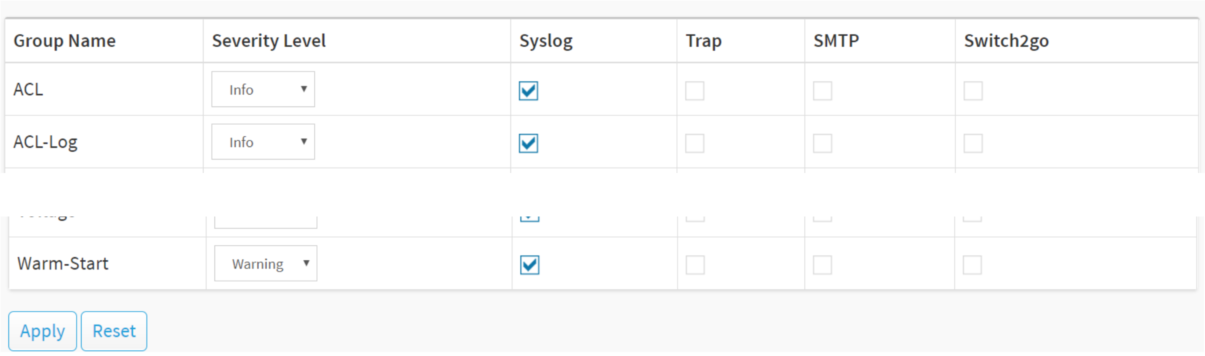
This page displays current trap event severity configurations. Trap event severity can also be configured here.

Web Interface

To display the configure Trap Event Severity in the web interface:

1. Click Event Notification and Event Configuration.
2. Scroll to select the Group name and Severity Level.
3. Click Enable to select different trap event.
4. Click the Apply to save the setting.
5. If you want to cancel the setting then you need to click the Reset button. It will revert to previously saved values.

.



Group Name	Severity Level	Syslog	Trap	SMTP	Switch2go
ACL	Info	☑	□	□	□
ACL-Log	Info	☑	□	□	□
Warm-Start	Warning	☑	□	□	□

Figure 17-5: The Event Severity Configuration

Parameter description:

- **Group Name :**

  The name identifying the severity group.

- **Severity Level :**

  Every group has an severity level. The following level types are supported:
  <0> Emergency: System is unusable.
  <1> Alert: Action must be taken immediately.
  <2> Critical: Critical conditions.
  <3> Error: Error conditions.
  <4> Warning: Warning conditions.
  <5> Notice: Normal but significant conditions.
  <6> Information: Information messages.
  <7> Debug: Debug-level messages.

- **Syslog :**

  Enable - Select this Group Name in Syslog.

- **Trap :**

  Enable - Select this Group Name in Trap.

- **Switch2go :**

  Enable - Select this Group Name in Push Notification.

Buttons

- **Apply :**

  Click to save changes.

- **Reset :**

  Click to undo any changes made locally and revert to previously saved values.

Chapter 18 Diagnostics

This chapter provides a set of basic system diagnosis. These includes Ping, Traceroute, Cable Diagnostics and port mirror.

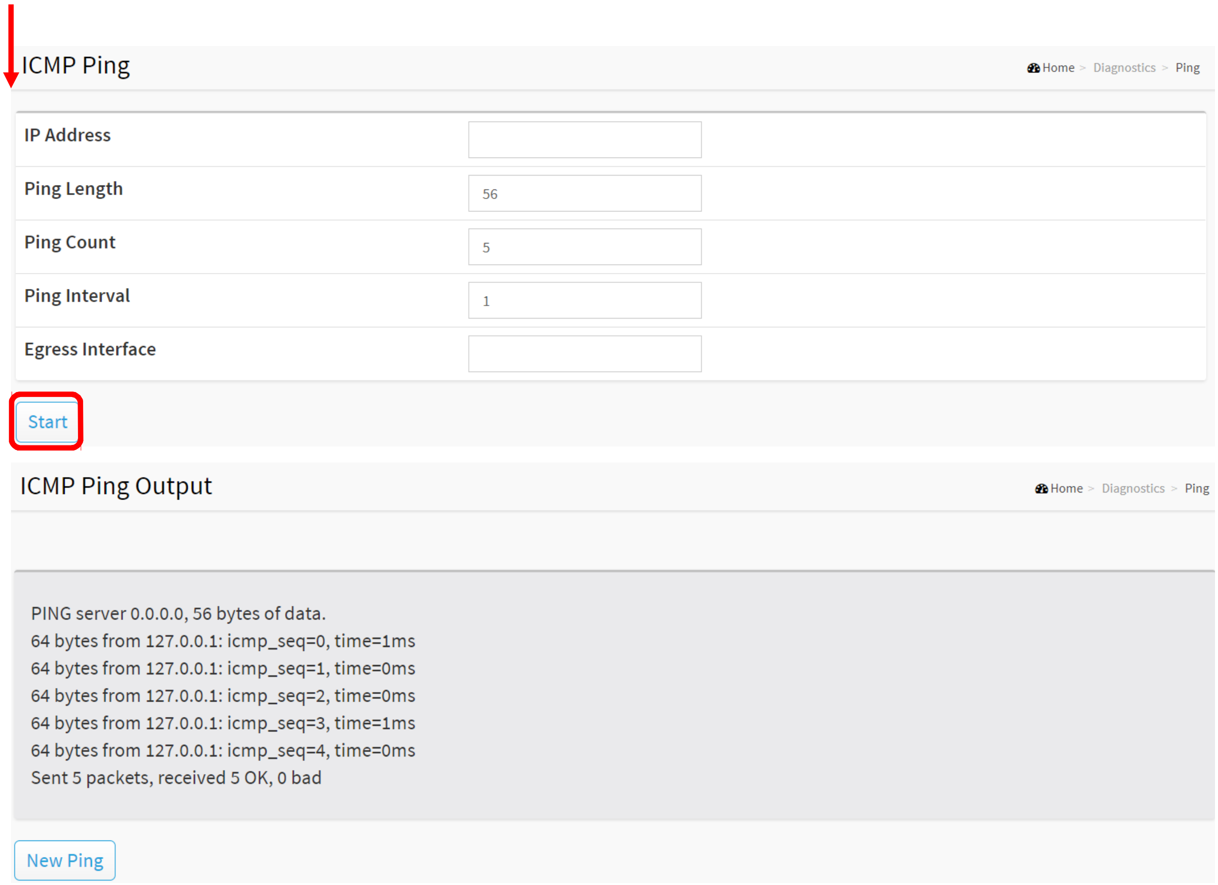
18-1 Ping

This section allows you to issue ICMP Echo packets to troubleshoot Ipv4/6 connectivity issues.

Web Interface

To configure a PING in the web interface:

1. Click Diagnostics and Ping.
2. Specify IP Address, Ping Length, Ping Count, Ping Interval and Egress Interface.
3. Click Start.



IP Address	
Ping Length	56
Ping Count	5
Ping Interval	1
Egress Interface	

```
PING server 0.0.0.0, 56 bytes of data.
64 bytes from 127.0.0.1: icmp_seq=0, time=1ms
64 bytes from 127.0.0.1: icmp_seq=1, time=0ms
64 bytes from 127.0.0.1: icmp_seq=2, time=0ms
64 bytes from 127.0.0.1: icmp_seq=3, time=1ms
64 bytes from 127.0.0.1: icmp_seq=4, time=0ms
Sent 5 packets, received 5 OK, 0 bad
```

Figure 18-1: The ICMP Ping

Parameter description:

- **IP Address :**

To specify the target IP Address of the Ping.

- **Ping Length :**

  The payload size of the ICMP packet. Values range from 2 bytes to 1452 bytes.

- **Ping Count :**

  The count of the ICMP packet. Values range from 1 time to 60 times.

- **Ping Interval :**

  The interval of the ICMP packet. Values range from 0 second to 30seconds.

- **Egress Interface (Only for IPv6) :**

  The VLAN ID (VID) of the specific egress IPv6 interface which ICMP packet goes. The given VID ranges from 1 to 4094 and will be effective only when the corresponding IPv6 interface is valid.
  When the egress interface is not given, PING6 finds the best match interface for destination.
  Do not specify egress interface for loopback address.
  Do specify egress interface for link-local or multicast address.

Buttons

- **Start :**

  Click the “Start” button to start to ping the target IP Address.

- **New Ping :**

  Back to ICMP Ping page.

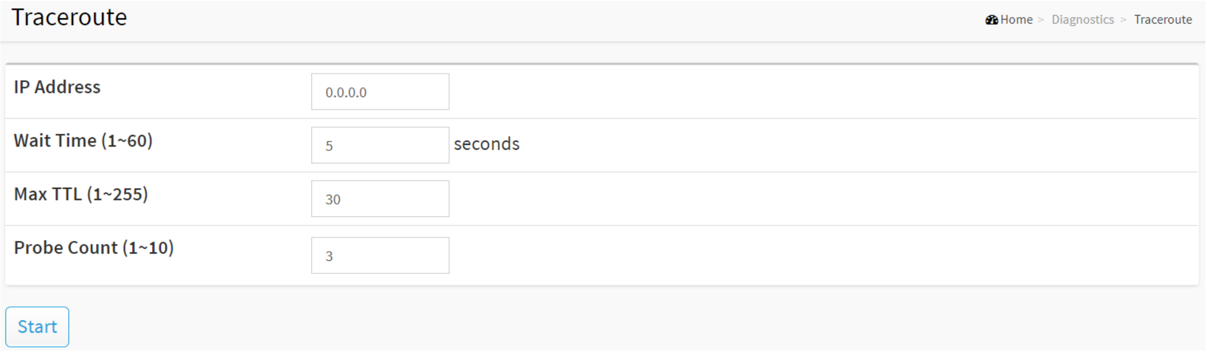
18-2 Traceroute

This page allows you to issue ICMP, TCP, or UDP packets to diagnose network connectivity issues.

Web Interface

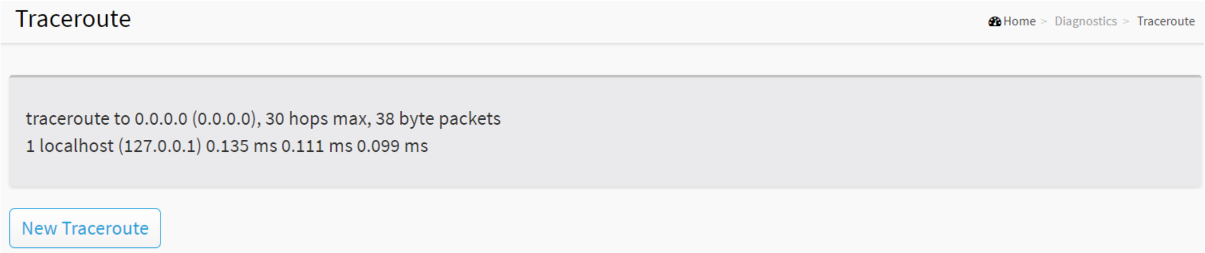
To start a Traceroute in the web interface:
Click Diagnostics and Traceroute.

1. Specify IP Address, Wait Time, Max TTL and Probe Count.
2. Click Start.



Traceroute

IP Address	0.0.0.0	
Wait Time (1~60)	5	seconds
Max TTL (1~255)	30	
Probe Count (1~10)	3	



```
traceroute to 0.0.0.0 (0.0.0.0), 30 hops max, 38 byte packets
1 localhost (127.0.0.1) 0.135 ms 0.111 ms 0.099 ms
```

Figure 18-2: The Traceroute

Parameter description:

- **IP Address :**

  The destination IP Address.

- **Wait Time :**

  Set the time (in seconds) to wait for a response to a probe (default 5.0 sec). Values range from 1 to 60. The payload size of the ICMP packet. Values range from 2 bytes to 1452 bytes.

- **Max TTL :**

  Specifies the maximum number of hops (max time-to-live value) traceroute will probe. Values range from 1 to 255. The default is 30.

- **Probe Count :**

  Sets the number of probe packets per hop. Values range from 1 to 10. The default is 3.

Buttons

- **Start :**

  Click the “Start” button to start to traceroute the target IP Address.

- **New Ping :**

  Back to Traceroute page.

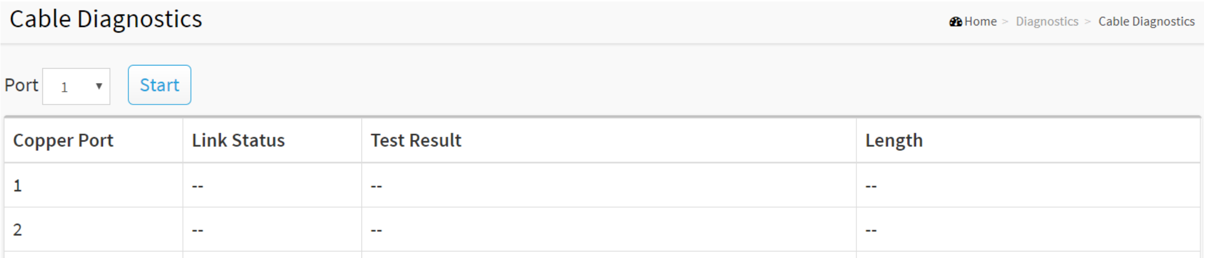
18-3 Cable Diagnostics

This section shows how to run Cable Diagnostics for copper ports.

Web Interface

To configure a Cable Diagnostics Configuration in the web interface:

1. Click Diagnostics and Cable Diagnostics.
2. Specify Port which want to check.
3. Click Start.



Copper Port	Link Status	Test Result	Length
1	--	--	--
2	--	--	--

Figure 18-3: The Cable Diagnostics

Parameter description:

- **Port :**

  The port where you are requesting Cable Diagnostics.

- **Copper Port :**

  Copper port number.

- **Link Status :**

  The status of the cable.

  10M: Cable is link up and correct. Speed is 10Mbps

  100M: Cable is link up and correct. Speed is 100Mbps

  1G: Cable is link up and correct. Speed is 1Gbps

  Link Down: Link down or cable is not correct.

- **Test Result :**

  Test Result of the cable.

  OK: Correctly terminated pair

  Abnormal: Incorrectly terminated pair or link down

- **Length :**

  The length (in meters) of the cable pair. The resolution is 3 meters. When Link Status is shown as follow, the length has different definition.

  1G: The length is the minimum value of 4-pair.

  10M/100M: The length is the minimum value of 2-pair.

  Link Down: The length is the minimum value of non-zero of 4-pair.

Button

- **Start :**

  Start to cable diagnostics the port that you selected.

18-4 Mirroring

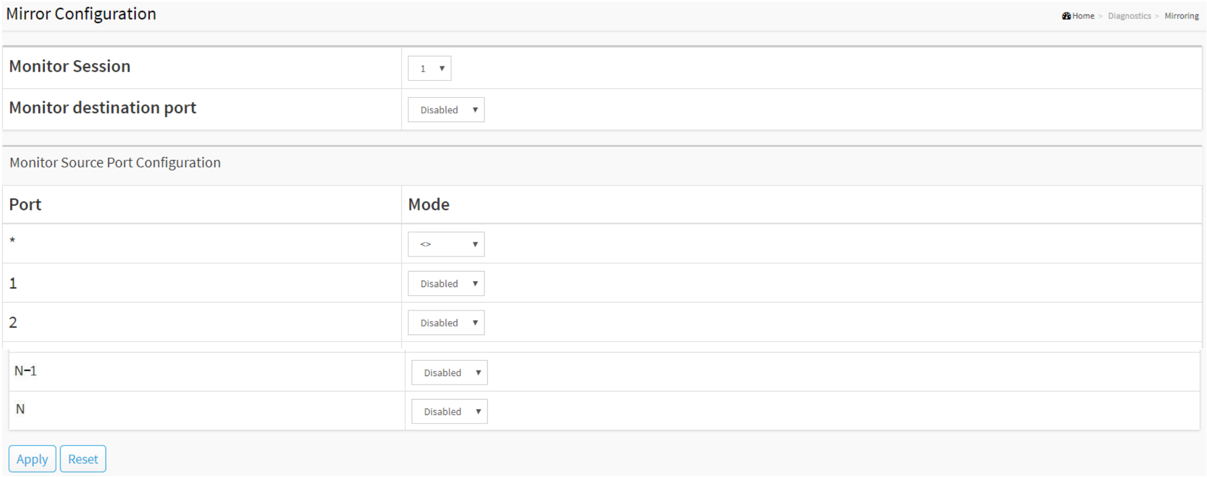
You can mirror traffic from any source port to a target port for real-time analysis. You can then attach a logic analyzer or RMON probe to the target port and study the traffic crossing the source port in a completely unobtrusive manner.

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 the Port Mirror function in the web interface:

1. Click Diagnostics and Mirroring.
2. Select the Monitor Destination Port (Mirror Port).
3. Select mode (disabled, enable, TX Only and RX only) for each monitored port.
4. Click the Apply button to save the setting.
5. If you want to cancel the setting then you need to click the Reset button to revert to previously saved values.



Mirror Configuration

Monitor Session	1 ▾
Monitor destination port	Disabled ▾

Monitor Source Port Configuration

Port	Mode
*	<> ▾
1	Disabled ▾
2	Disabled ▾
N-1	Disabled ▾
N	Disabled ▾

Figure 18-4: The Mirror Configuration

Parameter description:

- **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.

  Mirror Source Port Configuration

  The following table is used for Rx and Tx enabling.

- **Port :**

  The logical port for the settings contained in the same row.

- **Mode :**

  Select mirror mode.

  Rx only : Frames received on this port are mirrored on the mirror port. Frames transmitted are not mirrored.

Tx only : Frames transmitted on this port are mirrored on the mirror port. Frames received are not mirrored.

Disabled : neither frames transmitted nor frames received are mirrored.

Enabled : Frames received and frames transmitted are mirrored on the mirror port.

Buttons

- **Apply :**

  Click to save changes.

- **Reset :**

  Click to undo any changes made locally and revert to previously saved values.

18-5 sFlow

18-5.1 Configuration

The sFlow Collector configuration for the switch can be monitored and modified here. The configuration is divided into two parts: Configuration of the sFlow receiver (a.k.a. sFlow collector) and configuration of per-port flow and counter samplers.

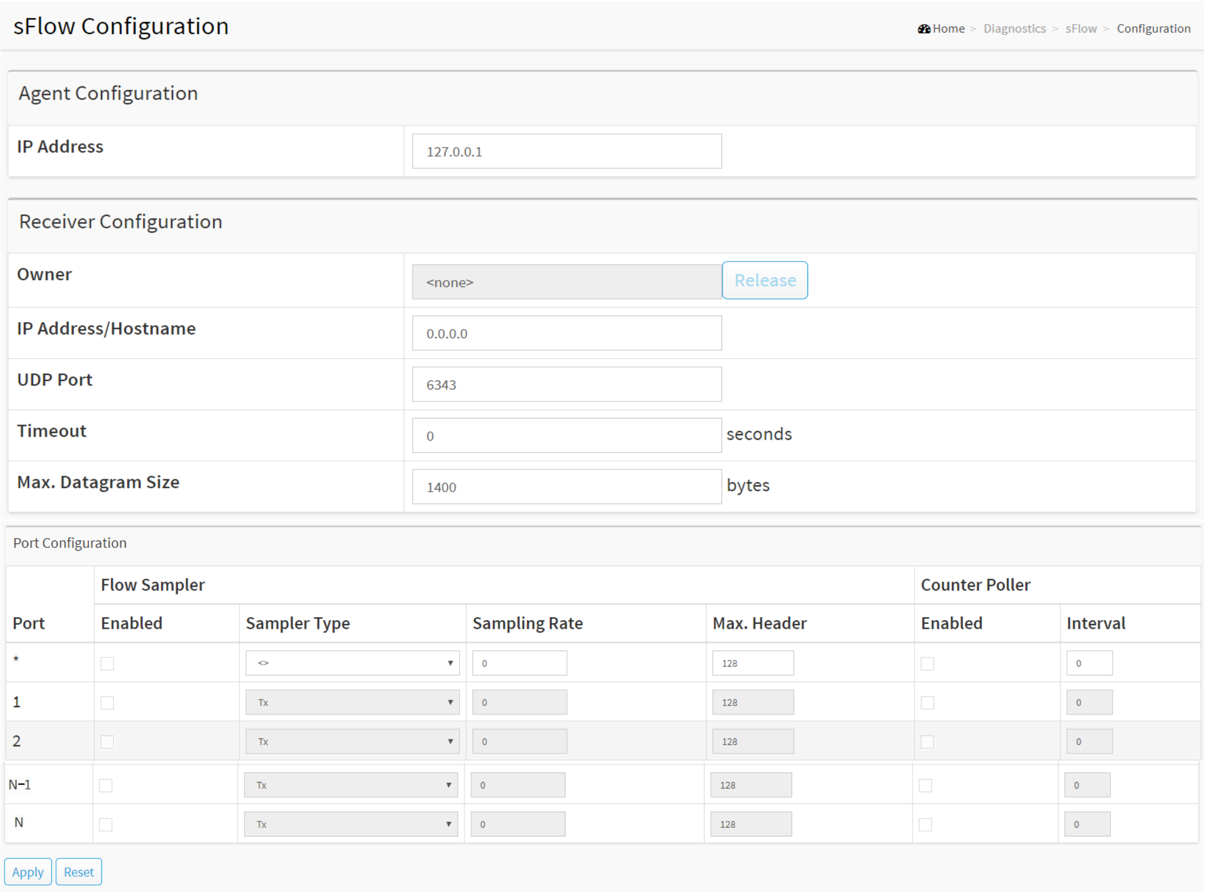
sFlow configuration is not persisted to non-volatile memory, which means that a reboot or master change will disable sFlow sampling.

Web Interface

To configure the sFlow in the web interface:

1. Click Diagnostics, sFlow and Configuration.
2. Set the sFlow parameters.
3. Click apply to save the setting.
4. If you want to cancel the setting then you need to click the Reset button.

It will revert to previously saved values.



sFlow Configuration

Home > Diagnostics > sFlow > Configuration

Agent Configuration

IP Address	127.0.0.1

Receiver Configuration

Owner	<none> Release
IP Address/Hostname	0.0.0.0
UDP Port	6343
Timeout	0 seconds
Max. Datagram Size	1400 bytes

Port Configuration

	Flow Sampler				Counter Poller	
Port	Enabled	Sampler Type	Sampling Rate	Max. Header	Enabled	Interval
*	☐	<>	0	128	☐	0
1	☐	Tx	0	128	☐	0
2	☐	Tx	0	128	☐	0
N-1	☐	Tx	0	128	☐	0
N	☐	Tx	0	128	☐	0

Figure 18-5.1: The sFlow Configuration

Parameter description:

Agent Configuration

- **IP Address :**

The IP address used as Agent IP address in sFlow datagrams. It serves as a unique key that will identify this agent over extended periods of time.

Both IPv4 and IPv6 addresses are supported.

Receiver Configuration

- **Owner :**

  Basically, sFlow can be configured in two ways: Through local management using the Web or CLI interface or through SNMP. This read-only field shows the owner of the current sFlow configuration and assumes values as follows:
  • If sFlow is currently unconfigured/unclaimed, Owner contains <none>.
  • If sFlow is currently configured through Web or CLI, Owner contains <Configured through local management>.
  • If sFlow is currently configured through SNMP, Owner contains a string identifying the sFlow receiver.
  If sFlow is configured through SNMP, all controls - except for the Release-button - are disabled to avoid inadvertent reconfiguration.

  The Release button allows for releasing the current owner and disable sFlow sampling. The button is disabled if sFlow is currently unclaimed. If configured through SNMP, the release must be confirmed (a confirmation request will appear).

- **IP Address/Hostname :**

  The IP address or hostname of the sFlow receiver. Both IPv4 and IPv6 addresses are supported.

- **UDP Port :**

  The UDP port on which the sFlow receiver listens to sFlow datagrams. If set to 0 (zero), the default port (6343) is used.

- **Timeout :**

  The number of seconds remaining before sampling stops and the current sFlow owner is released. While active, the current time left can be updated with a click on the Refresh-button. If locally managed, the timeout can be changed on the fly without affecting any other settings.

- **Max. Datagram Size :**

  The maximum number of data bytes that can be sent in a single sample datagram. This should be set to a value that avoids fragmentation of the sFlow datagrams. Valid range is 200 to 1468 bytes with default being 1400 bytes.

Port Configuration

- **Port :**

  The port number for which the configuration below applies.

- **Flow Sampler Enabled :**

  Enables/disables flow sampling on this port.

- **Flow Sampler Sampling Rate :**

  The statistical sampling rate for packet sampling. Set to N to sample on average 1/Nth of the packets transmitted/received on the port.
  Not all sampling rates are achievable. If an unsupported sampling rate is requested, the switch will automatically adjust it to the closest achievable. This will be reported back in this field.

- **Flow Sampler Max. Header :**

  The maximum number of bytes that should be copied from a sampled packet to the sFlow datagram. Valid range is 14 to 200 bytes with default being 128 bytes.

If the maximum datagram size does not take into account the maximum header size, samples may be dropped.

- **Counter Poller Enabled :**

  Enables/disables counter polling on this port.

- **Counter Poller Interval :**

  With counter polling enabled, this specifies the interval - in seconds - between counter poller samples.

Buttons

- **Apply :**

  Click to save changes.

- **Reset :**

  Click to undo any changes made locally and revert to previously saved values.

- **Release :**

  See description under Owner.

- **Refresh :**

  Click to refresh the page. Note that unsaved changes will be lost.

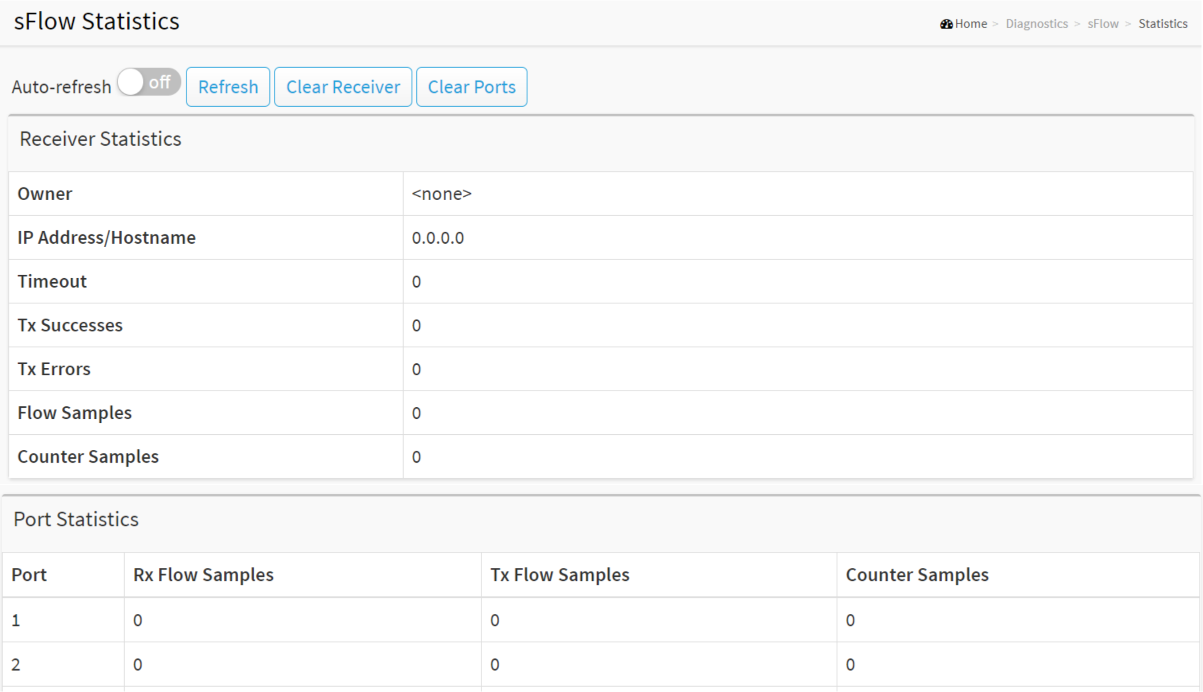
18-5.2 Statistics

This session shows receiver and per-port sFlow statistics

Web Interface

To Display port sFlow statistics in the web interface:
Click Diagnostics, sFlow and statistics.

1. Display sFlow information.

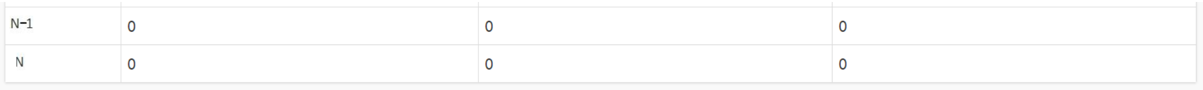


Receiver Statistics

Owner	<none>
IP Address/Hostname	0.0.0.0
Timeout	0
Tx Successes	0
Tx Errors	0
Flow Samples	0
Counter Samples	0

Port Statistics

Port	Rx Flow Samples	Tx Flow Samples	Counter Samples
1	0	0	0
2	0	0	0



N-1	0	0	0
N	0	0	0

Figure 18-5.2: The sFlow Statistics

Parameter description:

Receiver Statistics

- **Owner :**

  This field shows the current owner of the sFlow configuration. It assumes one of three values as follows:

  • If sFlow is currently unconfigured/unclaimed, Owner contains <none>.

  • If sFlow is currently configured through Web or CLI, Owner contains <Configured through local management>.

  • If sFlow is currently configured through SNMP, Owner contains a string identifying the sFlow receiver.`

- **IP Address/Hostname :**

  The IP address or hostname of the sFlow receiver.

- **Timeout :**

  The number of seconds remaining before sampling stops and the current sFlow owner is released.

- **Tx Successes :**

  The number of UDP datagrams successfully sent to the sFlow receiver.

- **Tx Errors :**

  The number of UDP datagrams that has failed transmission.
  The most common source of errors is invalid sFlow receiver IP/hostname configuration. To diagnose, paste the receiver's IP address/hostname into the Ping Web page (Diagnostics → Ping/Ping6).

- **Flow Samples :**

  The total number of flow samples sent to the sFlow receiver.

- **Counter Samples :**

  The total number of counter samples sent to the sFlow receiver.

Port Statistics

- **Port :**

  The port number for which the following statistics applies.

- **Rx and Tx Flow Samples :**

  The number of flow samples sent to the sFlow receiver originating from this port. Here, flow samples are divided into Rx and Tx flow samples, where Rx flow samples contains the number of packets that were sampled upon reception (ingress) on the port and Tx flow samples contains the number of packets that were sampled upon transmission (egress) on the port.

- **Counter Samples :**

  The total number of counter samples sent to the sFlow receiver originating from this port.

Buttons

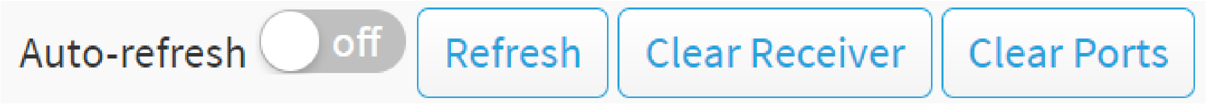


Figure 15-5.2: The sFlow Statistics buttons

- **Auto-refresh :**

  Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.

- **Refresh :**

  Click to refresh the page immediately.

- **Clear Receiver :**

  Clears the sFlow receiver counters.

- **Clear Ports :**

  Clears the per-port counters.

Chapter 19 Maintenance

This chapter describes the entire Maintenance configuration tasks including Save/Backup/Restore/Activate/Delete Restart Device, Factory Defaults, Firmware upgrade.

19-1 Configuration

The switch stores its configuration in a number of files in text format. The files are either virtual (RAM-based) or stored in flash on the switch.

There are three system files:

- running-config: A virtual file that represents the currently active configuration on the switch. This file is volatile.
- startup-config: The startup configuration for the switch, read at boot time.
- default-config: A read-only file with vendor-specific configuration. This file is read when the system is restored to default settings.

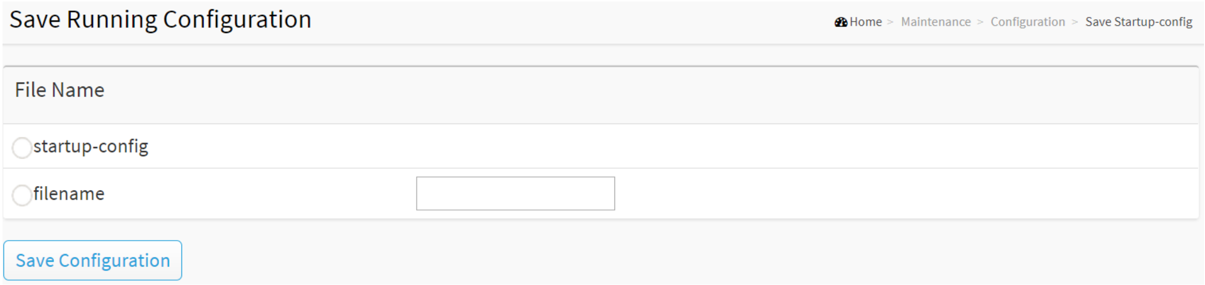
19-1.1 Save startup-config

This copy running-config to startup-config, thereby ensuring that the current active configuration will be used at the next reboot.

Web Interface

To save running configuration in the web interface:

1. Click Maintenance, Configuration and Save startup-config.
2. Click Save Configuration.



Save Running Configuration

File Name

○ startup-config

○ filename

Figure 19-1.1: The Save Startup Configuration

Parameter description:

Button

- **Save Configuration :**

  Click to save configuration, the running configuration will be written to flash memory for system boot up to load this startup configuration file.

19-1.2 Backup

This section describes how to export the Switch Configuration for maintenance needs. Any current configuration files will be exported as text format.

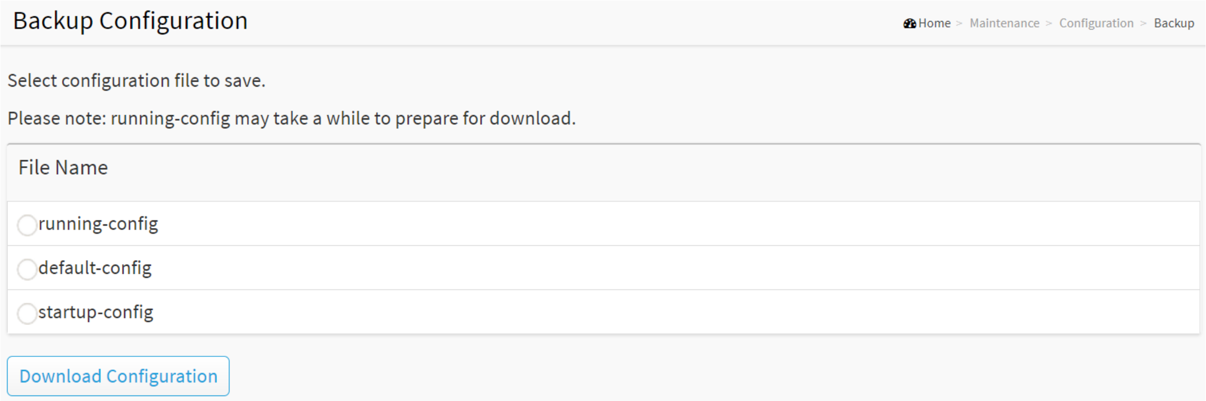
The configuration files on the switch can be backed up and saved on the station running the web browser.

It is possible to transfer any of the files on the switch to the web browser. Select the running-config may take a little while to complete, as the file must be prepared before backup.

Web Interface

To backup configuration in the web interface:

1. Click Maintenance, Configuration and Backup.
2. Click Backup.



Backup Configuration

Select configuration file to save.

Please note: running-config may take a while to prepare for download.

File Name
○running-config
○default-config
○startup-config

Figure 19-1.2: Backup

Parameter description:

- **running-config :**

  A virtual file that represents the currently active configuration on the switch. This file is volatile.

- **startup-config :**

  The startup configuration for the switch, read at boot time.

- **default-config :**

  A read-only file with vendor-specific configuration. This file is read when the system is restored to default settings.

Button

- **Download Configuration :**

  Click the button then the switch will start to transfer the configuration file to your workstation.

19-1.3 Restore

It is possible to import a file from the web browser to all the files on the switch, except default-config, which is read-only.

Select the source file to restore, and select the destination file on the target.

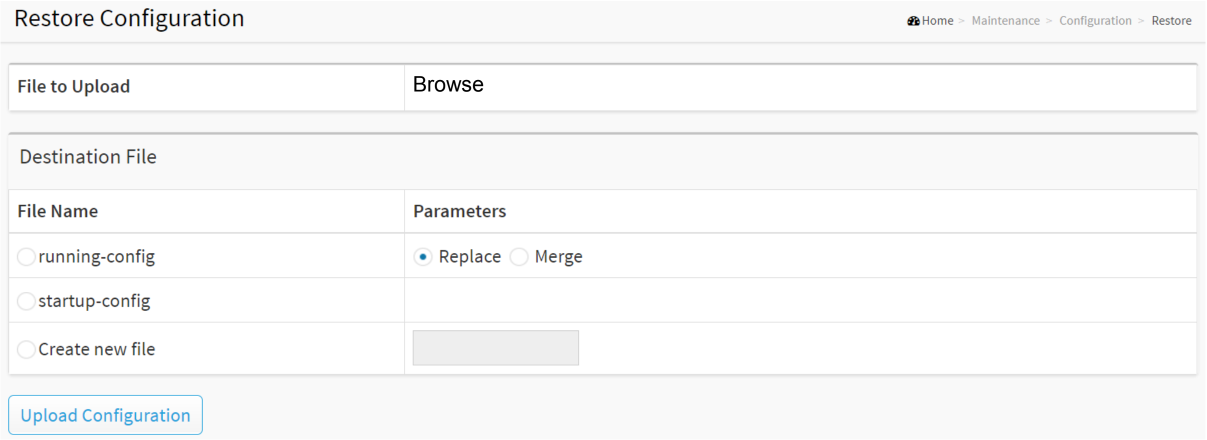
If the destination is running-config, the file will be applied to the switch configuration. This can be done in two ways:

- ■ Replace mode: The current configuration is fully replaced with the configuration specified in the source file.
- ■ Merge mode: The source file configuration is merged into running-config.

Web Interface

To restore configuration in the web interface:

1. Click Maintenance, Configuration and Restore.
2. Click Restore.



Restore Configuration

File to Upload	Browse

Destination File

File Name	Parameters
○ running-config	● Replace ○ Merge
○ startup-config	
○ Create new file	

Upload Configuration

Figure 19-1.3: Restore Config

Parameter description:

- **running-config :**

  A virtual file that represents the currently active configuration on the switch. This file is volatile.

  Replace mode: The current configuration is fully replaced with the configuration in the uploaded file.

Merge mode: The uploaded file is merged into running-config.

- **startup-config :**

  The startup configuration for the switch, read at boot time.

- **Create new file :**

  To create new files.

Parameter description:

Buttons

- **Browse :**

  Click the button to search the configuration text file and filename

- **Upload Configuration :**

  Click the button to start transfer the source file to the destination file.

19-1.4 Activate

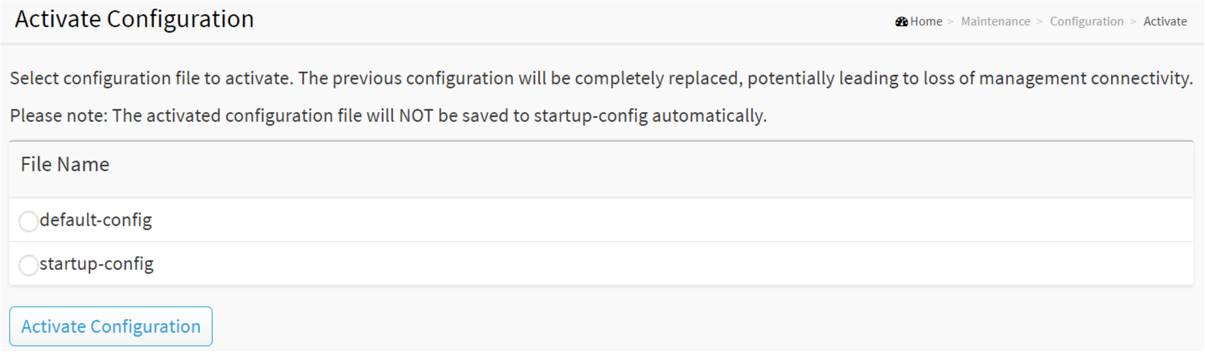
It is possible to activate any of the configuration files present on the switch, except for running-config which represents the currently active configuration.

Select the file to activate and click. This will initiate the process of completely replacing the existing configuration with that of the selected file.

Web Interface

To activate configuration in the web interface:

1. Click Maintenance, Configuration and Activate .
2. Click Activate Select.



Activate Configuration

Select configuration file to activate. The previous configuration will be completely replaced, potentially leading to loss of management connectivity.

Please note: The activated configuration file will NOT be saved to startup-config automatically.

File Name
○ default-config
○ startup-config

Figure 19-1.4: Configuration Activation

Parameter description:

Buttons

- **Activate Configuration :**

  Click the “Activate Configuration” button then the selected file will be activated to be the switch's running configuration.

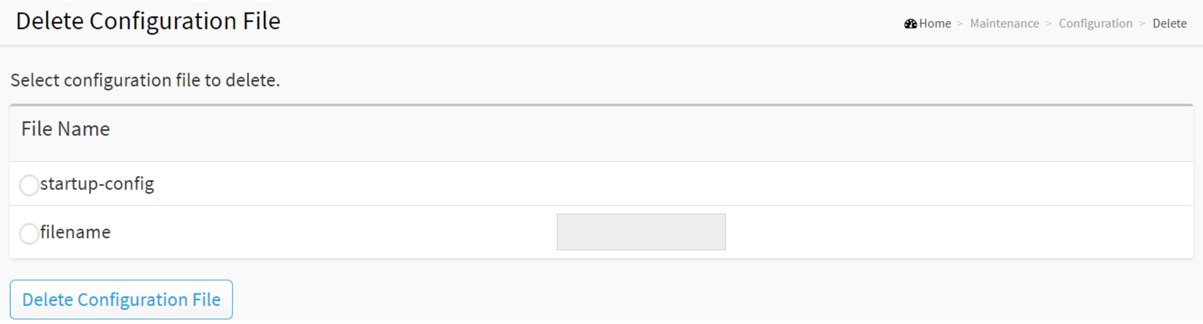
19-1.5 Delete

It is possible to delete any of the writable files stored in flash, including startup-config. If this is done and the switch is rebooted without a prior save operation, this effectively resets the switch to default configuration.

Web Interface

To delete configuration in the web interface:

1. Click Maintenance, Configuration and Delete.
2. Click Delete Select.



Delete Configuration File

Home > Maintenance > Configuration > Delete

Select configuration file to delete.

File Name	
○startup-config	
○filename	

Figure 19-1.5: Delete Configuration

Parameter description:

Buttons

- **Delete Configuration File:**

  Click the “Delete Configuration File” button then the selected file will be deleted.

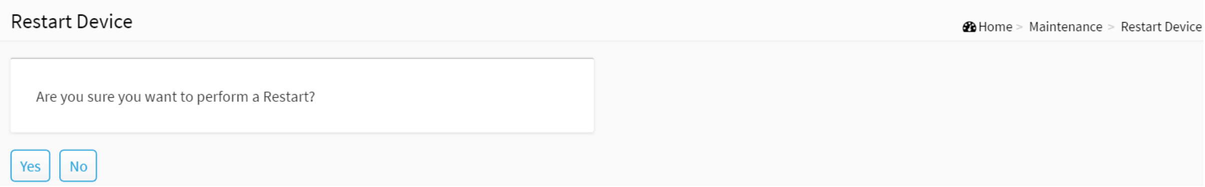
19-2 Restart Device

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 and Restart Device.
2. Click Yes.



Restart Device

Are you sure you want to perform a Restart?

Figure 19-2: Restart Device

Parameter description:

Restart Device :

You can restart the switch on this page. After restart, the switch will boot normally.

Buttons

- **Yes :**

  Click to "Yes" then the device will restart.

- **No :**

  Click to cancel the opeation.

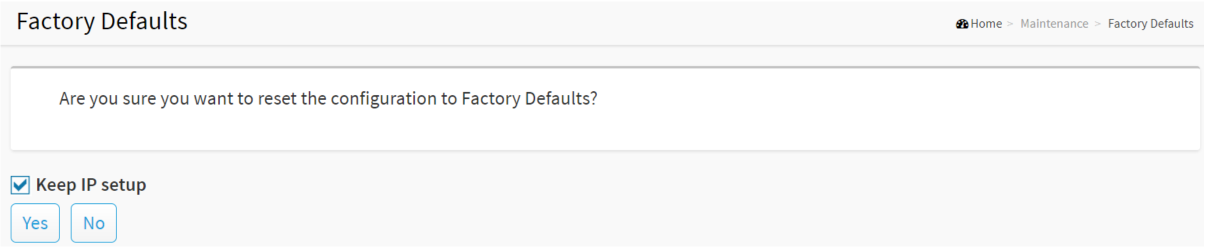
19-3 Factory Defaults

This section describes how to restore the Switch configuration to Factory Defaults.

Web Interface

To restore a Factory Defaults in the web interface:

1. Click Maintenance and Factory Defaults.
2. You can choose if you want to keep ip configuration or not.
3. Click Yes.



Factory Defaults

Home > Maintenance > Factory Defaults

Are you sure you want to reset the configuration to Factory Defaults?

☑ Keep IP setup

Figure 19-3: The Factory Defaults

Parameter description:

Buttons

- **Keep IP Configuration :**

  Choose if you want to keep ip configuration or not.

- **Yes :**

  Click to “Yes” button to reset the configuration to Factory Defaults.

- **No :**

  Click to cancel the operation.

19-4 Firmware

This section describes how to upgrade (or update) Firmware.

19-4.1 Firmware Upgrade

This page facilitates an update of the firmware controlling the switch..

Web Interface

To update firmware of the device in the web interface:

1. Click Maintenance, Firmware and Firmware Upgrade.
2. Click Upload.

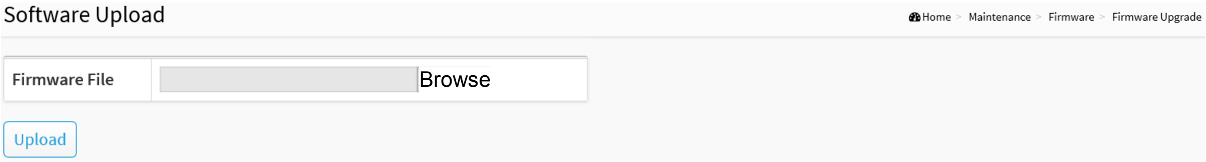


Figure 19-4.1 The firmware upgrade

Parameter description:

- **Browse :**

  Click the "Browse" button to search the Firmware URL and filename.

19-4.2 Firmware Selection

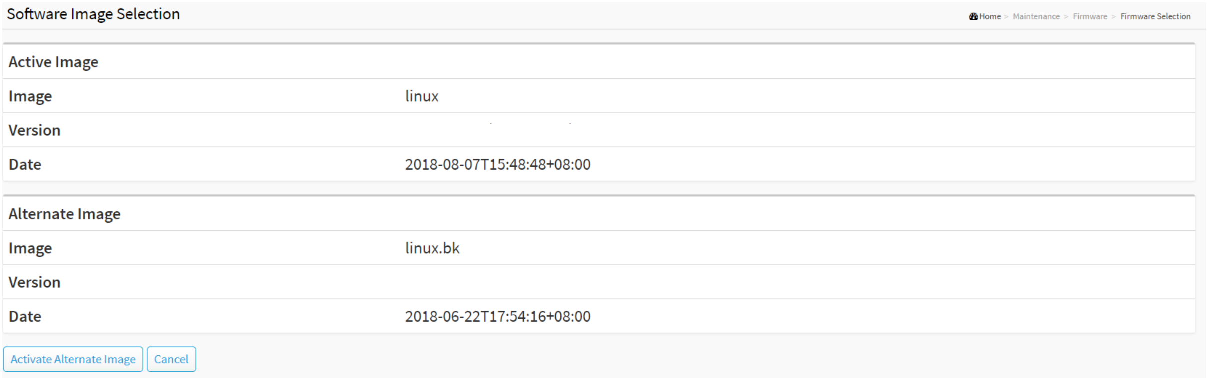
This page provides information about the active and alternate (backup) firmware images in the device, and allows you to activate the alternate image.

The web page displays two tables with information about the active and alternate firmware images.

Web Interface

To show the Firmware information or swap booting firmware in the web interface:

1. Click Maintenance, Firmware and Firmware Selection.
2. Click Activate Alternate Image



Software Image Selection

Active Image	
Image	linux
Version	
Date	2018-08-07T15:48:48+08:00

Alternate Image	
Image	linux.bk
Version	
Date	2018-06-22T17:54:16+08:00

Figure 19-4.2 The Firmware selection

Image Information

- **Image :**

  The file name of the firmware image, from when the image was last updated.

- **Version :**

  The version of the firmware image.

- **Date :**

  The date where the firmware was produced.

Buttons

- **Activate Alternate Image :**

  Click to use the “Activate Alternate Image”. This button may be disabled depending on system state.

- **Cancel :**

  Cancel activating the alternate image. Navigates away from this page.