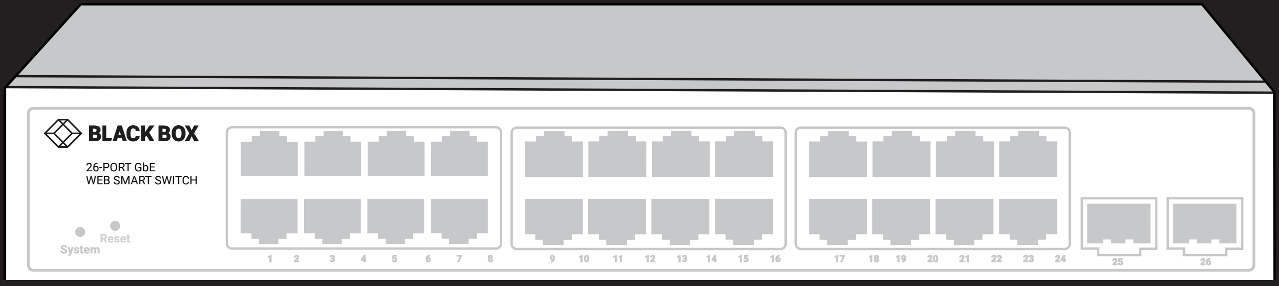
WEB GUI USER MANUAL

LGB2118A-R2, LGB2126A

GBE WEB SMART SWITCHES

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



BLACK BOX

TABLE OF CONTENTS

TABLE OF CONTENTS

TABLE OF CONTENTS

TABLE OF CONTENTS

TABLE OF CONTENTS

DEFAULT SETTINGS

The switch's default values are listed below:

IP Address: 192.168.1.1

Subnet Mask: 255.255.255.0

Default Gateway: 192.168.1.254

Username: admin

Password: <none> (Just press the Enter key.)

ABOUT THIS MANUAL

This GUI user guide gives specific information on how to operate and use the management functions of the LGB2118A-R2 or LGB2126A via HTTP/HTTPs web browser.

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).

RELATED PUBLICATIONS/REVISION HISTORY

RELATED PUBLICATIONS

The following publications give specific information on how to operate and use the management functions of the switch:

- Installation & Getting Started Guide
- CLI User Guide

To download the guides from blackbox.com:

1. Go to www.blackbox.com
2. Enter the part number in the search box (for example, LGB2118A-R2 or LGB2126A).
3. Click on the product in the "Products" page.
4. Click on the "Support" tab on the product page and select the document you wish to download.

REVISION HISTORY

Current manual version: Revision A2, 11/17/2017

INTRODUCTION

OVERVIEW

This User Guide explains how to install and connect your network system and configure and monitor the LGB2118A-R2 or LGB2126A through the web via its serial interface and Ethernet ports. Detailed explanations of hardware and software functions are shown as well as examples of web-based interface operation.

The LGB2118A-R2 or LGB2126A switch provides a reliable infrastructure for your business network. These switches deliver intelligent features that improve the availability of your critical business applications, protect your sensitive information, and optimize your network bandwidth to deliver information and applications more effectively. Each switch provides the ideal combination of affordability and capabilities for entry level networking, including small business or enterprise applications, and helps you create a more efficient, better-connected workforce.

LGB2118A-R2 or LGB2126A Web Managed Switches provide 18 or 26 ports in a single device.

- 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 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 802.1d (STP), 802.1w (RSTP) and 802.1s (MSTP)
- Support LACP and static link aggregation
- Support Q-in-Q double tag VLAN

MANUAL STRUCTURE

- Chapter 1: Operation of Web-based Management
- Chapter 2: First Time Wizard
- Chapter 3: System
- Chapter 4: Port 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: Event Notification
- Chapter 15: Diagnostics
- Chapter 16: Maintenance

CHAPTER 1: OPERATION OF WEB-BASED MANAGEMENT

INITIAL CONFIGURATION

This chapter explains how to configure and manage the LGB2118A-R2 or LGB2126A through the web user interface. With this facility, you can easily access and monitor, through any one port of the switch, 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 switch's default values are listed below:

IP Address: 192.168.1.1

Subnet Mask: 255.255.255.0

Default Gateway: 192.168.1.254

Username: admin

Password: <none> (Just press the Enter key.)

After the LGB2118A-R2 or LGB2126A has finishes configuring its interface, you can browse it. For instance, type http://192.168.1.1 in the address row in a browser, and it will show the following screen and ask you to input username and password to login and access authentication.

The default username is "admin" and password is empty. For first-time use, enter the default username and password, and then click the <Login> button. The login process now is completed. In this login menu, you have to input the complete username and password respectively, the LGB2118A-R2 or LGB2126A will not give you a shortcut to username automatically. This looks inconvenient, but safer.

The LGB2118A-R2 or LGB2126A allows two or more users using administrator's identity to manage this switch, the administrator who does the last setting will be the available configuration in the system.

NOTE: When you log in to the Switch web page to manage the switch, you must first type the Username of the admin. The password was blank, so after you type the Username, just press enter. You will see the management page.

When you log in to LGB2118A-R2 or LGB2126A series switch Web UI management interface, you can use both ipv4 ipv6.

To optimize the display effect, we recommend you use Microsoft IE 6.0 above, Netscape V7.1 above or Firefox V1.00 above with a resolution of 1024 x 768. The switch supports a neutral web browser interface.

NOTE: The LGB2118A-R2 or LGB2126A has the function dhcp enabled, so If you do not have a DHCP server to provide ip addresses to the switch, use the Switch default ip 192.168.1.1

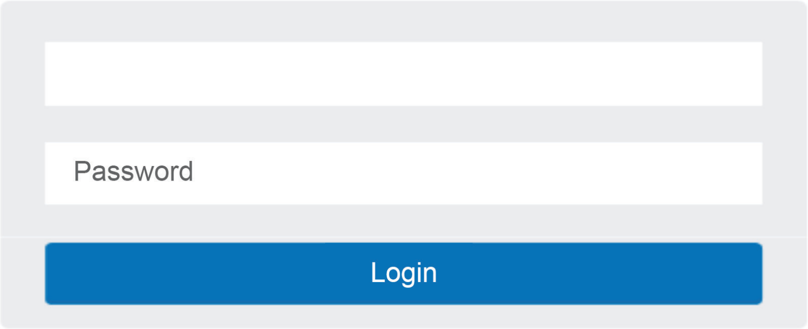


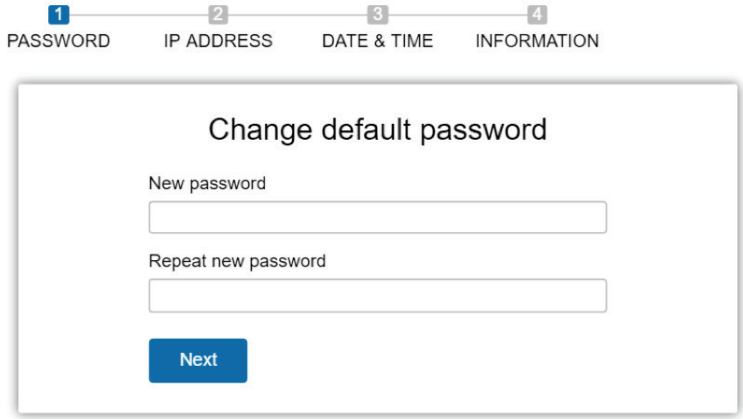
FIGURE 1-1. LOGIN SCREEN

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

Follow the procedure below:

Step 1: Change the default password

Configure the new password and enter it again, then press Next.



Change default password

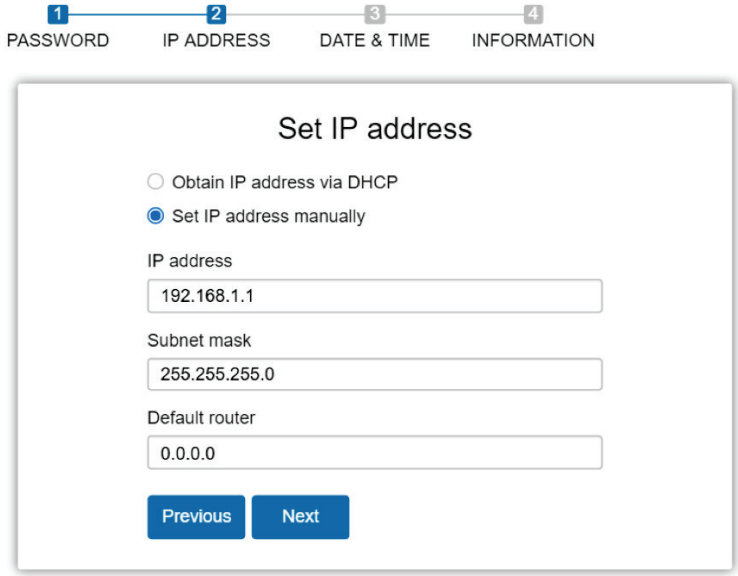
New password

Repeat new password

FIGURE 2-1. CHANGE DEFAULT PASSWORD SCREEN

Step 2: Set the IP address

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



Set IP address

○ Obtain IP address via DHCP

● Set IP address manually

IP address: 192.168.1.1

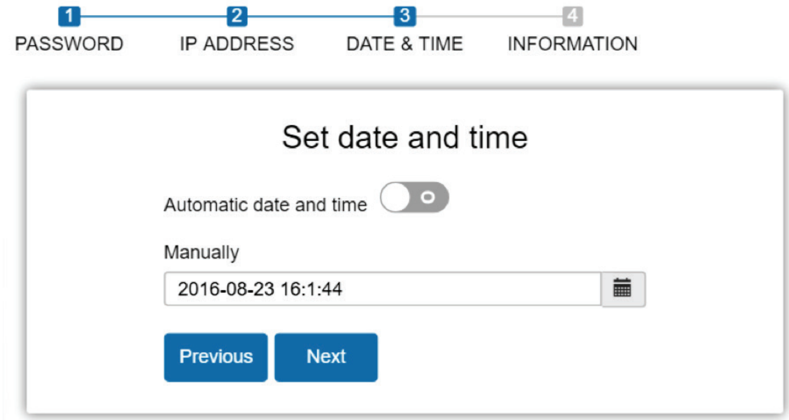
Subnet mask: 255.255.255.0

Default router: 0.0.0.0

FIGURE 2-2. CHANGE IP ADDRESS SCREEN

Step 3: Set the date and time

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



Set date and time

Automatic date and time

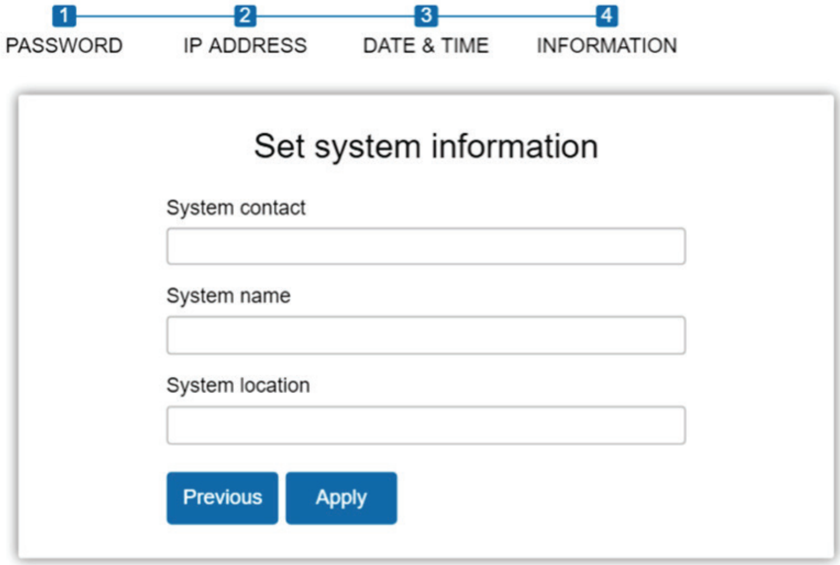
Manually

2016-08-23 16:1:44

FIGURE 2-3. SET DATE AND TIME SCREEN

Step 4: Set the system information

You can set some system information for this device, such as "System contact", "System name", "System location".



Set system information

System contact

System name

System location

FIGURE 2-4. SET SYSTEM INFORMATION SCREEN

CHAPTER 3: SYSTEM

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

3.1 SYSTEM INFORMATION

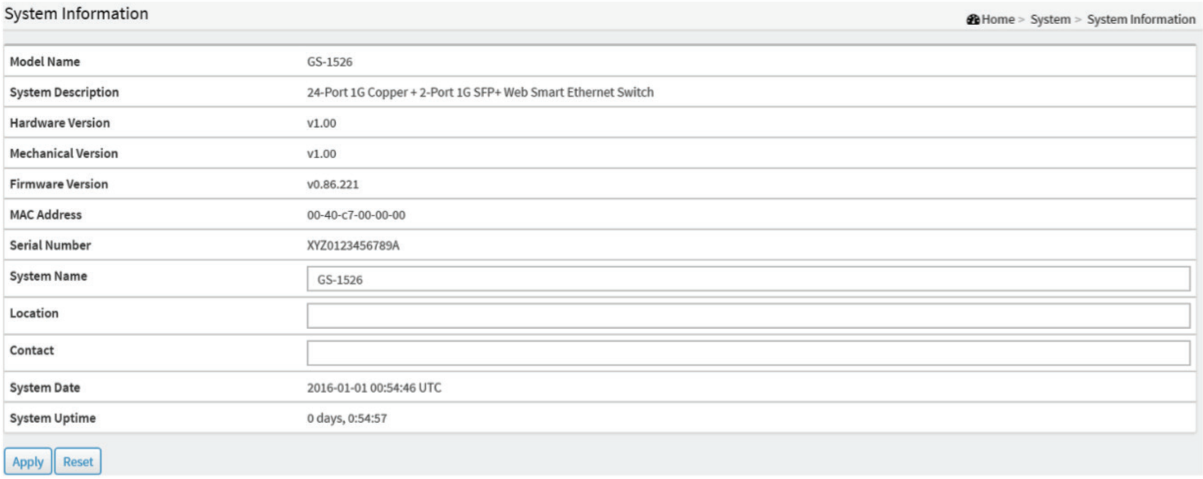
You can identify the system by configuring the contact information, name, and location of the switch.

The switch's contact information is provided here.

WEB INTERFACE

To configure System Information in the web interface:

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



System Information

Model Name	GS-1526
System Description	24-Port 1G Copper + 2-Port 1G SFP+ Web Smart Ethernet Switch
Hardware Version	v1.00
Mechanical Version	v1.00
Firmware Version	v0.86.221
MAC Address	00-40-c7-00-00-00
Serial Number	XYZ0123456789A
System Name	GS-1526
Location	
Contact	
System Date	2016-01-01 00:54:46 UTC
System Uptime	0 days, 0:54:57

FIGURE 3-1. SYSTEM INFORMATION SCREEN

PARAMETER DESCRIPTION

- Model Name: Displays the factory defined model name for identification purposes.
- System Description: Displays the system description.
- Hardware-Mechanical Version: The hardware and mechanical version of this switch.
- Firmware Version: The software version of this switch.
- MAC Address: The MAC Address of this switch.
- Series Number: The serial number of this switch.
- System name: An administratively assigned name for this managed node. By convention, this is the node's fully-qualified domain name. A domain name is a text string drawn from the alphabet (A-Z, a-z), digits (0-9), minus sign (-). No space characters are permitted as part of a name. The first character must be an alpha character, and the first or last character must not be a minus sign. The allowed string length is 0 to 128.
- Location: The physical location of this node (e.g., telephone closet, 3rd floor). The allowed string length is 0 to 128, and the allowed content is the ASCII characters from 32 to 1.

- Contact: The textual identification of the contact person for this managed node, together with information on how to contact this person. The allowed string length is 0 to 128, and the allowed content is the ASCII characters from 32 to 126.
- System Date: The current (GMT) system time and date. The system time is obtained through the Timing server running on the switch, if any.
- System Uptime: The period of time the device has been operational.

Buttons

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

3.2 IP ADDRESS

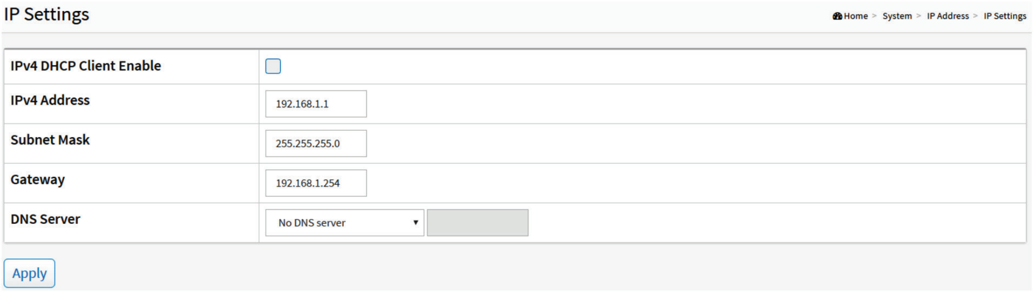
The IPv4 address for the switch can be obtained via DHCP Server for VLAN 1. To manually configure an address, you need to change the switch's default settings to values that are compatible with your network. You may also need to establish a default gateway between the switch and management stations that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

3.3 IP SETTINGS

WEB INTERFACE

To configure the IP settings in the web interface:

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



IP Settings

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

FIGURE 3-2. IP SETTINGS SCREEN

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: User IP subnet mask of the entry.

- Gateway: The IP address of the IP gateway. The 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. The following modes are supported:

  - No DNS server: No DNS server will be used.

  - Configured: Explicitly provide the IP address of the DNS Server in dotted decimal notation.

  - From this DHCP interface: Specify from which DHCP-enabled interface a provided DNS server should be preferred.

  - From any DHCP interfaces: The first DNS server offered from a DHCP lease to a DHCP-enabled interface will be used.

Buttons

- Apply: Click to save changes.

3.3.1 ADVANCED IP SETTINGS

Configure the switch-managed IP information on this page.

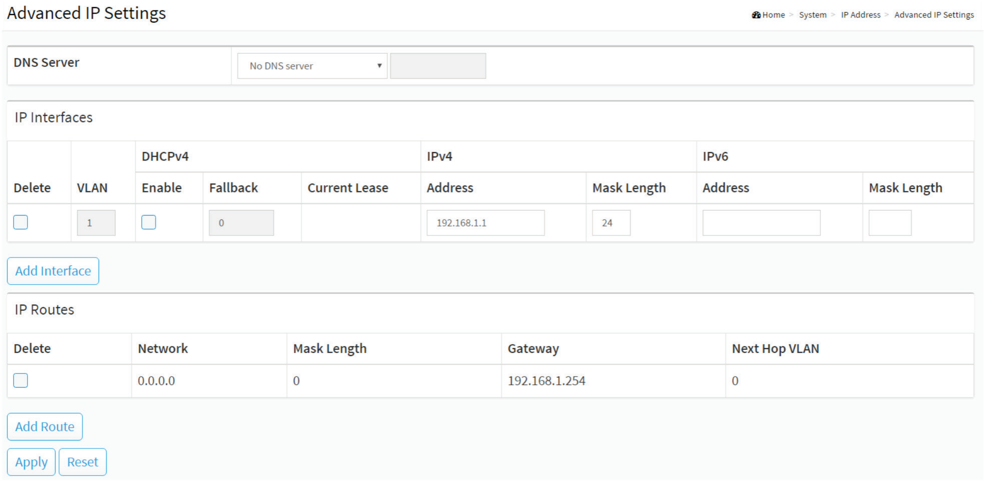
Configure IP basic settings, control IP interfaces and IP routes.

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

WEB INTERFACE

To configure an Advanced IP Settings in the web interface:

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



Advanced IP Settings

Home > System > IP Address > Advanced IP Settings

DNS Server	No DNS server ▾

IP Interfaces

		DHCPv4			IPv4		IPv6	
Delete	VLAN	Enable	Fallback	Current Lease	Address	Mask Length	Address	Mask Length
□	1	□	0		192.168.1.1	24		

IP Routes

Delete	Network	Mask Length	Gateway	Next Hop VLAN
□	0.0.0.0	0	192.168.1.254	0

FIGURE 3-3.ADVANCED IP SETTINGS SCREEN

PARAMETER DESCRIPTION

IP Configuration

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

  - No DNS server: No DNS server will be used.

  - Configured: Explicitly provide the IP address of the DNS Server in dotted decimal notation.

  - From this DHCP interface: Specify from which DHCP-enabled interface a provided DNS server should be preferred.

  - From any DHCP interfaces: The first DNS server offered from a DHCP lease to a DHCP-enabled interface will be used.

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 a new interface.
- IPv4 DHCP Enabled: Enable the DHCP client by checking this box. If this option is enabled, the system will configure the IPv4 address and mask of the interface using the DHCP protocol. The DHCP client will announce the configured System Name as hostname to provide DNS lookup.
- IPv4 DHCP Fallback Timeout: The number of seconds for trying to obtain a DHCP lease. After this period expires, a configured IPv4 address will be used as IPv4 interface address. A value of zero disables the fallback mechanism, so 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 shows the current interface address, as provided by the DHCP server.
- IPv4 Address: The IPv4 address of the interface in dotted decimal notation.
- If DHCP is enabled, this field is not used. The field may also be left blank if IPv4 operation on the interface is not desired.
- IPv4 Mask: The IPv4 network mask, in number of bits (prefix length). Valid values are between 0 and 30 bits for a IPv4 address.
- If DHCP is enabled, this field is not used. The field may also be left blank if IPv4 operation on the interface is not desired.
- IPv6 Address: The IPv6 address of the interface. An IPv6 address is in 128-bit records represented as eight fields of up to four hexadecimal digits with a colon separating each field (:). For example, fe80::215:c5ff:fe03:4dc7. The symbol :: is a special syntax that can be used as a shorthand way of representing multiple 16-bit groups of contiguous zeros; but it can appear only once. It can also represent a legally valid IPv4 address. For example, ::192.1.2.34. The field may be left blank if IPv6 operation on the interface is not desired.
- IPv6 Mask: The IPv6 network mask, in number of bits (prefix length). Valid values are between 1 and 128 bits for a IPv6 address. The field may be left blank if IPv6 operation on the interface is not desired.

IP Routes

- Delete: Select this option to delete an existing IP route.
- Network: The destination IP network or host address of this route. A 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 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. A valid format is dotted decimal notation or a valid IPv6 notation. Gateway and Network must be of the same type.

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

Buttons

- Add Interface: Click to add a new IP interface. A maximum of 8 interfaces is supported.
- Add Route: Click to add a new IP route. A maximum of 8 routes is supported.
- Apply: Click to save changes.
- Reset: Click to undo any changes made locally and revert to previously saved values.

3.3.2 STATUS

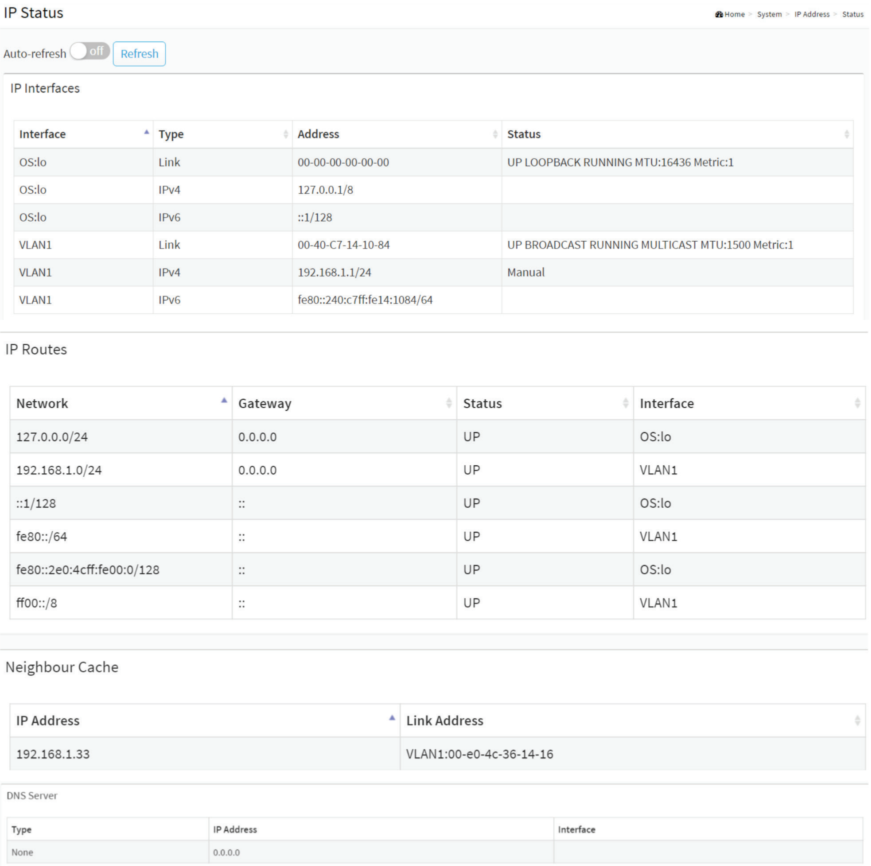
This page displays the status of the IP protocol layer. The status is defined by the IP interfaces, the IP routes and the neighbor cache (ARP cache) status.

WEB INTERFACE

To display the log configuration in the web interface:

1. Click System, IP Address and Status.

2. Display the IP Configuration information.



IP Status

IP Interfaces

Interface	Type	Address	Status
OS:lo	Link	00-00-00-00-00-00	UP LOOPBACK RUNNING MTU:16436 Metric:1
OS:lo	IPv4	127.0.0.1/8	
OS:lo	IPv6	::1/128	
VLAN1	Link	00-40-C7-14-10-84	UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
VLAN1	IPv4	192.168.1.1/24	Manual
VLAN1	IPv6	fe80::240:c7ff:fe14:1084/64	

IP Routes

Network	Gateway	Status	Interface
127.0.0.0/24	0.0.0.0	UP	OS:lo
192.168.1.0/24	0.0.0.0	UP	VLAN1
::1/128	::	UP	OS:lo
fe80::/64	::	UP	VLAN1
fe80::2e0:4cff:fe00:0/128	::	UP	OS:lo
ff00::/8	::	UP	VLAN1

Neighbour Cache

IP Address	Link Address
192.168.1.33	VLAN1:00-e0-4c-36-14-16

DNS Server

Type	IP Address	Interface
None	0.0.0.0	

FIGURE 3-4. IP STATUS SCREEN

PARAMETER DESCRIPTION

IP Interfaces

- Interface: Show the name of the interface.
- Type: Show the address type of the entry. This may be LINK or IPv4.
- Address: Show the current address of the interface (of the given type).
- Status: Show the status flags of the interface (and/or address).

IP Routes

- Network: Show the destination IP network or host address of this route.
- Gateway: Show the gateway address of this route.
- Status: Show the status flags of the route.
- Interface: Show the name of the interface.

Neighbor cache

- IP Address: Show the IP address of the entry.
- Link Address: Show the Link (MAC) address for which a binding to the IP address given exists.

DNS Server

- Type: Show the address type of the entry. This may be LINK or IPv4.
- IP Address: Show the current address of the interface (of the given type).
- Interface: Show the name of the interface.

Buttons

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

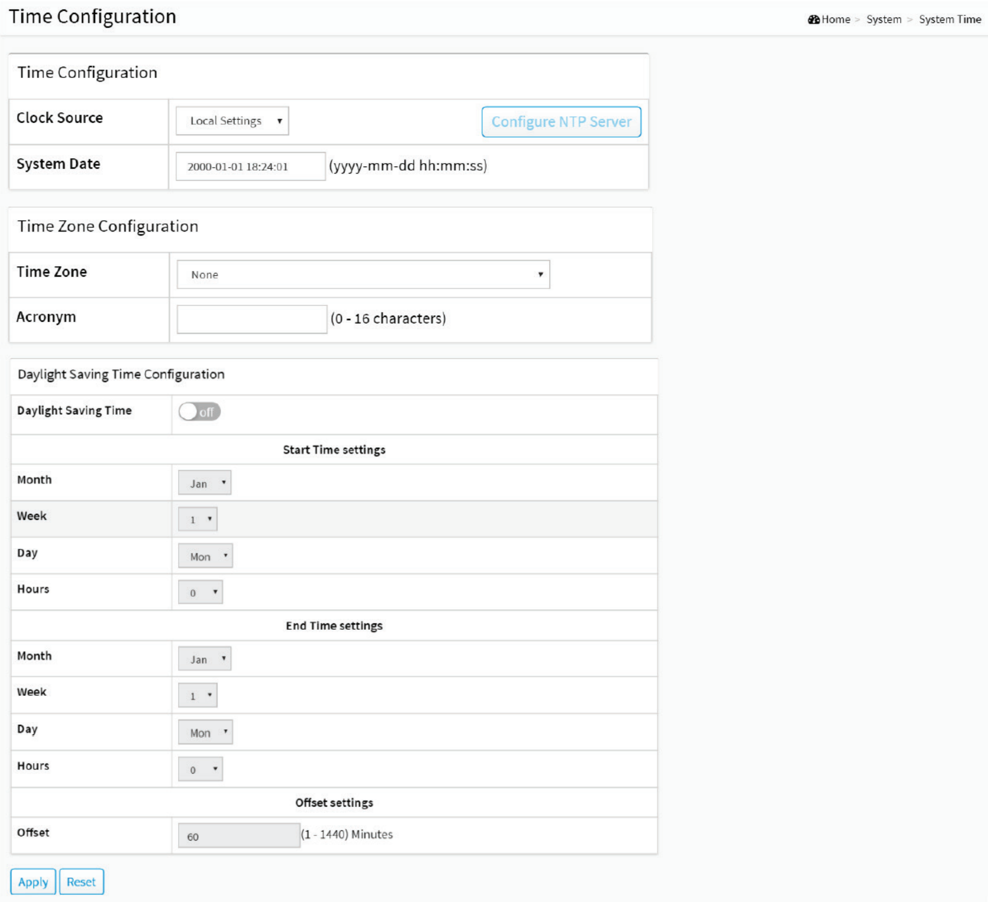
3.4 SYSTEM TIME

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

WEB INTERFACE

To configure Time in the web interface:

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



Time Configuration

Time Configuration	
Clock Source	Local Settings ▾ Configure NTP Server
System Date	2000-01-01 18:24:01 (yyyy-mm-dd hh:mm:ss)

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

Daylight Saving Time Configuration	
Daylight Saving Time	off
Start Time settings	
Month	Jan ▾
Week	1 ▾
Day	Mon ▾
Hours	0 ▾
End Time settings	
Month	Jan ▾
Week	1 ▾
Day	Mon ▾
Hours	0 ▾
Offset settings	
Offset	60 (1 - 1440) Minutes

FIGURE 3-5. TIME CONFIGURATION SCREEN

PARAMETER DESCRIPTION

Time Configuration

- Clock Source: There are two modes for configuring where the Clock Source is 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 is between 2000 and 2037.

Time Zone Configuration

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

Daylight Saving Time Configuration

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

Recurring Configuration

- Start time settings:
  - Week - Select the starting week number.
  - Day - Select the starting day.
  - Month - Select the starting month.
  - Hours - Select the starting hour.
- End time settings:
  - Week - Select the ending week number.
  - Day - Select the ending day.
  - Month - Select the ending month.
  - Hours - Select the ending hour.

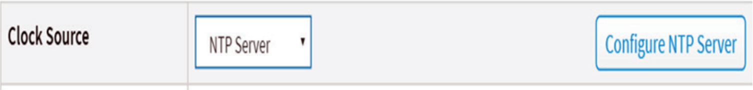
Offset settings:

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

NOTE: Under "Start Time Settings" and "End Time Settings" displays what you set in the "Start Time Settings" and "End Time Settings" field information.

Buttons

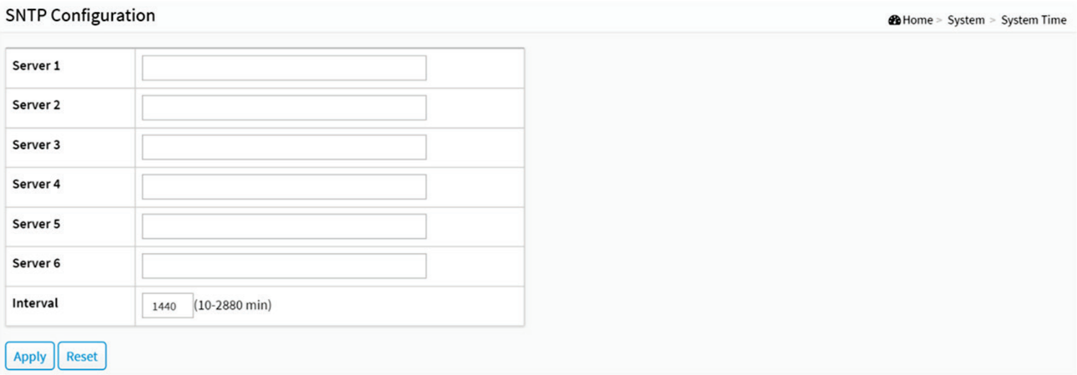
- Apply: Click to save changes.
- Reset: Click to undo any changes made locally and revert to previously saved values.



Clock Source	NTP Server ▾	Configure NTP Server

FIGURE 3-6. CONFIGURE NTP SERVER BUTTON

- Configure NTP Server: Click to configure NTP server when Clock Source is selected from NTP Server.



SNTP Configuration

Home > System > System Time

Server 1	
Server 2	
Server 3	
Server 4	
Server 5	
Server 6	
Interval	1440 (10-2880 min)

FIGURE 3-7. SNTP CONFIGURATION

NTP is Network Time Protocol and is used to sync the network time based Greenwich Mean Time (GMT). If you use the NTP mode and select a built-in NTP time server or manually specify a user-defined NTP server as well as Time Zone, the switch will sync the time shortly after pressing the <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 result in the local time; otherwise, you will not able to get the correct time. The switch supports a configurable time zone from -12 to +13 step 1 hour.

Default Time zone: +8 Hrs.

Parameter description:

- Server 1 to 6: 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'.
- Interval: You can specify the time interval in seconds after which a time check and, in case of deviation, a resynchronization of the internal device clock against the specified timeserver via Network Time Protocol(NTP) should be performed.

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.

3.5 LLDP

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

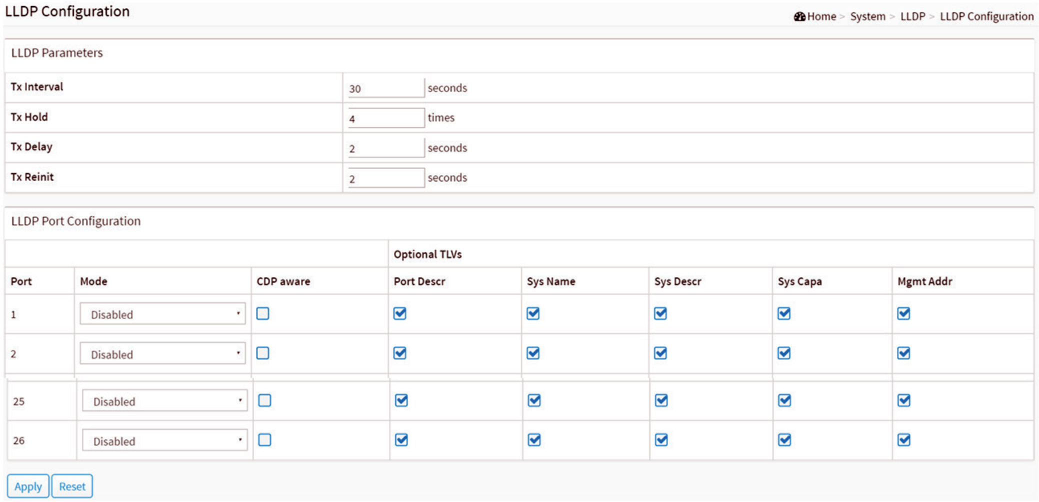
3.5.1 LLDP CONFIGURATION

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

WEB INTERFACE

To configure LLDP:

1. Click 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

Home > System > LLDP > 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	Port Descr	Sys Name	Sys Descr	Sys Capa	Mgmt Addr
1	Disabled	□	☑	☑	☑	☑	☑
2	Disabled	□	☑	☑	☑	☑	☑
25	Disabled	□	☑	☑	☑	☑	☑
26	Disabled	□	☑	☑	☑	☑	☑

FIGURE 3-8. LLDP CONFIGURATION SCREEN

PARAMETER DESCRIPTION

LLDP Parameters

- Tx Interval: The switch periodically transmits LLDP frames to its neighbors for the network discovery information to be up-to-date. The interval between each LLDP frame is determined by the Tx Interval value. Valid values are restricted to 5–32768 seconds.
- Tx Hold: Each LLDP frame contains information about how long the information in the LLDP frame will be considered valid. The LLDP information valid period is set to Tx Hold multiplied by Tx Interval seconds. Valid values are restricted to 2–10 times.
- Tx Delay: If a 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 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.
  - 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 is removed when the hold time is exceeded.

- Port Descr: Optional TLV: When checked, the "port description" is included in LLDP information transmitted.
- Sys Name: Optional TLV: When checked, the "system name" is included in LLDP information transmitted.
- Sys Descr: Optional TLV: When checked, the "system description" is included in LLDP information transmitted.
- Sys Capa: Optional TLV: When checked, the "system capability" is included in LLDP information transmitted.
- Mgmt Addr: Optional TLV: When checked, the "management address" is included in LLDP information transmitted.

Buttons

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

3.5.2 LLDP MED CONFIGURATION

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

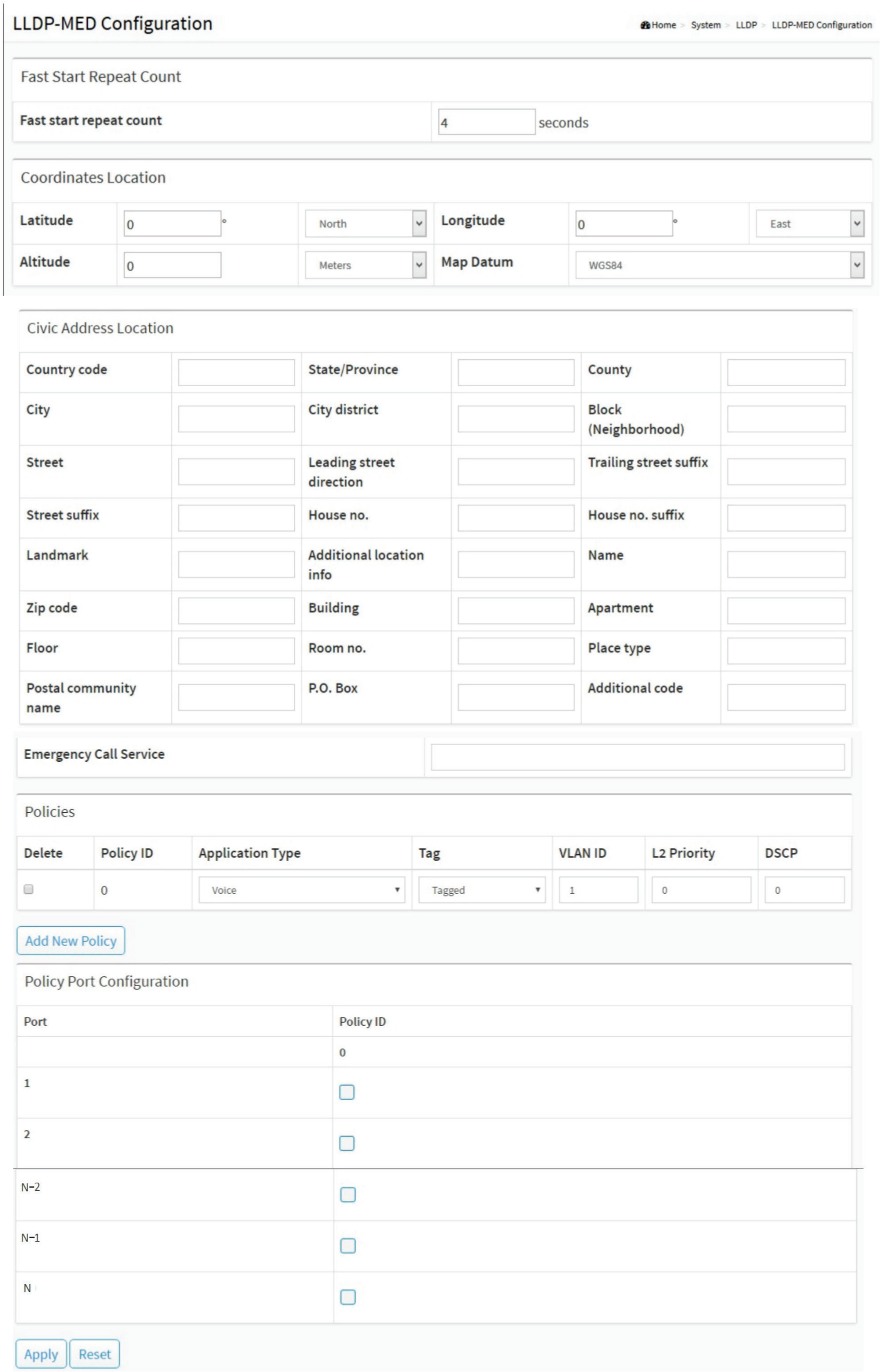
- Auto-discovery of LAN policies (such as VLAN, Layer 2 Priority and Differentiated services (Diffserv) settings) enabling plug and play networking.
- Device location discovery to allow creation of location databases and, in the case of Voice over Internet Protocol (VoIP), Enhanced 911 services.
- Inventory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

This page allows you to configure the LLDP-MED. This function applies to VoIP devices that 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 Coordinates Location parameters.
4. Fill Civic Address Location parameters.
5. Add new policy.
6. Click Apply; this will show the following Policy Port Configuration.
7. Select Policy ID for each port.
8. Click Apply.



LLDP-MED Configuration

Home > System > LLDP > LLDP-MED Configuration

Fast Start Repeat Count

Fast start repeat count	4 seconds

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	

Policies

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

Add New Policy

Policy Port Configuration

Port	Policy ID
	0
1	□
2	□
N-2	□
N-1	□
N	□

Apply Reset

FIGURE 3-9. 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 that are specifically relevant to particular endpoint types (for example, only advertise the voice network policy to permitted voice-capable devices), both in order to conserve the limited LLDPU space and to reduce security and system integrity issues that can come with inappropriate knowledge of the network policy.

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

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

NOTE: The LLDP-MED and the LLDP-MED Fast Start mechanism is only intended to run on links between LLDP-MED Network Connectivity Devices and Endpoint Devices, so it does not apply to links between LAN infrastructure elements, including Network Connectivity Devices, or other types of links.

Coordinates Location

- Latitude: Latitude SHOULD be normalized to within 0-90 degrees with a maximum of 4 digits. You can specify the direction to either North of the equator or South of the equator.
- Longitude: Longitude SHOULD be normalized to within 0-180 degrees with a maximum of 5 digits. You can specify the direction to either East of the prime meridian or West of the prime meridian.
- Altitude: Altitude SHOULD be normalized to within -32767 to 32767 with a maximum of 4 digits. You can select between two altitude types (floors or meters).
- Meters: Representing meters of Altitude defined by the vertical datum specified.
- Floors: Representing altitude in a form more relevant in buildings that have different floor-to-floor dimensions. An altitude = 0.0 is meaningful even outside a building, and represents ground level at the given latitude and longitude. Inside a building, 0.0 represents the floor level associated with ground level at the main entrance.
- Map Datum: The Map Datum is used for the coordinates given in these options:
  - WGS84: (Geographical 3D) - World Geodesic System 1984, CRS Code 4327, and Prime Meridian Name: Greenwich.
  - NAD83/NAVD88: North American Datum 1983, CRS Code 4269, Prime Meridian Name: Greenwich; the associated vertical datum is the North American Vertical Datum of 1988 (NAVD88). This datum pair is to be used when referencing locations on land, not near tidal water (which would use Datum = NAD83/MLLW).
  - NAD83/MLLW: North American Datum 1983, CRS Code 4269, Prime Meridian Name: Greenwich; the associated vertical datum is Mean Lower Low Water (MLLW). This datum pair is to be used when referencing locations on water/sea/ocean.

Civic Address Location:

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

- Country code: The two-letter ISO 3166 country code in capital ASCII letters - Example: DK, DE or US.
- State: National subdivisions (state, canton, region, province, prefecture).
- County: County, parish, gun (Japan), district.
- City: City, township, shi (Japan) - Example: Copenhagen.
- City district: City division, borough, city district, ward, chou (Japan).
- Block (Neighborhood): Neighborhood, block.

- Street: Street - Example: Poppelvej.
- Leading street direction: Leading street direction - Example: N.
- Trailing street suffix: Trailing street suffix - Example: SW.
- Street suffix: Street suffix - Example: Ave, Platz.
- House no.: House number - Example: 21.
- House no. suffix: House number suffix - Example: A, 1/2.
- Landmark: Landmark or vanity address - Example: Columbia University.
- Additional location info: Additional location info - Example: South Wing.
- Name: Name (residence and office occupant) - Example: Flemming Jahn.
- Zip code: Postal/zip code - Example: 2791.
- Building: Building (structure) - Example: Low Library.
- Apartment: Unit (Apartment, suite) - Example: Apt 42.
- Floor: Floor - Example: 4.
- Room no.: Room number - Example: 450F.
- Place type: Place type - Example: Office.
- Postal community name: Postal community name - Example: Leonia.
- P.O. Box: Post office box (P.O. BOX) - Example: 12345.
- Additional code: Additional code - Example: 1320300003.
- Emergency Call Service: Emergency Call Service (e.g. E911 and others), such as defined by TIA or NENA.
- Emergency Call Service: Emergency Call Service ELIN identifier data format is defined to carry the ELIN identifier as used during emergency call setup to a traditional CAMA or ISDN trunk-based PSAP. This format consists of a numerical digit string, corresponding to the ELIN to be used for emergency calling.

Policies

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

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

The network policy attributes advertised are:

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

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

1. Voice
2. Guest Voice
3. Softphone Voice
4. Video Conferencing
5. Streaming Video
6. Control / 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 Signaling (conditional) - for use in network topologies that require a different policy for the voice signaling than for the voice media. This application type should not be advertised if all the same network policies apply as those advertised in the Voice application policy.

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

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

  5. Softphone Voice - for use by softphone applications on typical data centric devices, such as PCs or laptops. This class of endpoints frequently does not support multiple VLANs, if at all, and is typically configured to use an ‘untagged’ VLAN or a single ‘tagged’ data specific VLAN. When a network policy is defined for use with an ‘untagged’ VLAN (see Tagged flag below), then the L2 priority field is ignored and only the DSCP value 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 Signaling (conditional) - for use in network topologies that require a separate policy for the video signaling than for the video media. This application type should not be advertised if all the same network policies apply as those advertised in the Video Conferencing application policy.

- Tag: Tag indicating whether the specified application type is using a ‘tagged’ or an ‘untagged’ VLAN.

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

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

- VLAN ID: VLAN identifier (VID) for the port as defined in IEEE 802.1Q-2003.
- L2 Priority: L2 Priority is the Layer 2 priority to be used for the specified application type. L2 Priority may specify one of eight priority levels (0 through 7), as defined by IEEE 802.1D-2004. A value of 0 represents use of the default priority as defined in IEEE 802.1D-2004.
- DSCP: DSCP value to be used to provide Diffserv node 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.

- Port Policies Configuration: Every port may advertise a unique set of network policies or different attributes for the same network policies, based on the authenticated user identity or port configuration.
- Port: The port number to which the configuration applies.
- Policy Id: The set of policies that will apply to a given port. The set of policies is selected by check marking the checkboxes that corresponds to the policies.

Buttons

- Adding a new policy: Click to add a new policy. Specify the Application type, Tag, VLAN ID, L2 Priority and DSCP for the new policy. Click "Apply".
- Apply: Click to save changes.
- Reset: Click to undo any changes made locally and revert to previously saved values.

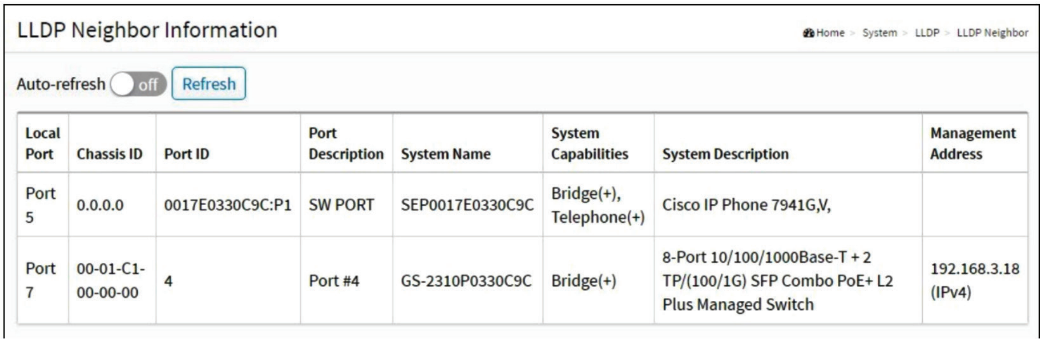
3.5.3 LLDP NEIGHBOR

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

WEB INTERFACE

To show LLDP neighbors:

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


LLDP Neighbor Information
Home > System > LLDP > LLDP Neighbor
Auto-refresh
off
Refresh

Local Port	Chassis ID	Port ID	Port Description	System Name	System Capabilities	System Description	Management Address
Port 5	0.0.0.0	0017E0330C9C:P1	SW PORT	SEP0017E0330C9C	Bridge(+), Telephone(+)	Cisco IP Phone 7941G,V,	
Port 7	00-01-C1-00-00-00	4	Port #4	GS-2310P0330C9C	Bridge(+)	8-Port 10/100/1000Base-T + 2 TP/(100/1G) SFP Combo PoE+ L2 Plus Managed Switch	192.168.3.18 (IPv4)

FIGURE 3-10. LLDP NEIGHBOR INFORMATION

PARAMETER DESCRIPTION

- Local Port: The port on which the LLDP frame was received.
- Chassis ID: The Chassis ID is the identification of the neighbor's LLDP frames.
- Port ID: The Remote Port ID is the identification of the neighbor port.
- Port Description: Port Description is the port description advertised by the neighbor unit.
- System Name: System Name is the name advertised by the neighbor unit.

- System Capabilities: System Capabilities describes the neighbor unit’s capabilities. The possible capabilities are:

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

  When a capability is enabled, the capability is followed by (+). If the capability is disabled, the capability is followed by (-).
- System Description: Displays the system description.
- Management Address: Management Address is the neighbor unit’s address that is used for higher layer entities to assist discovery by the network management. This could, for instance, hold the neighbor’s IP address.

Buttons

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

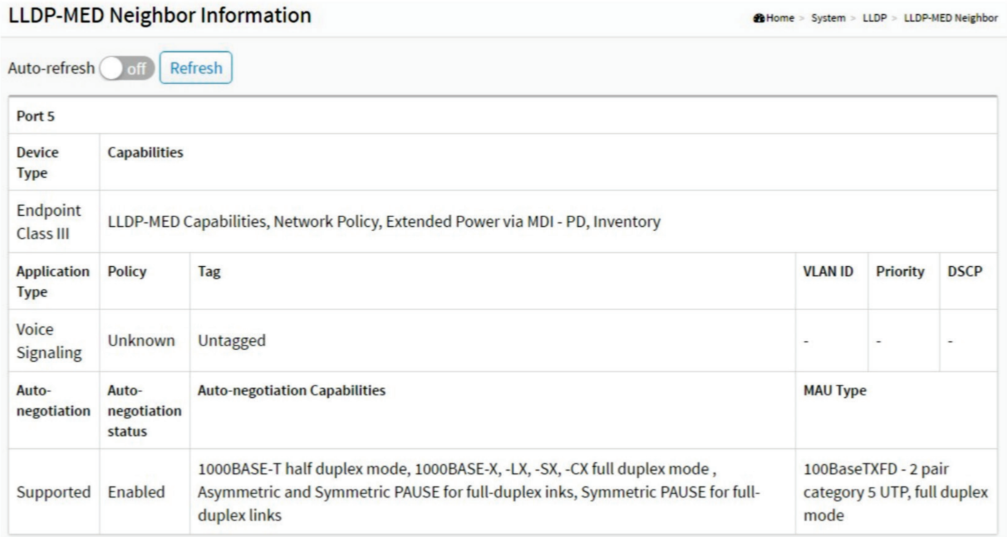
3.5.4 LLDP-MED NEIGHBOR

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

WEB INTERFACE

To show LLDP-MED neighbor:

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



LLDP-MED Neighbor Information

Port 5					
Device Type	**Capabilities**				
Endpoint Class III	LLDP-MED Capabilities, Network Policy, Extended Power via MDI - PD, Inventory				
Application Type	**Policy**	**Tag**	**VLAN ID**	**Priority**	**DSCP**
Voice Signaling	Unknown	Untagged	-	-	-
Auto-negotiation	**Auto-negotiation status**	**Auto-negotiation Capabilities**	**MAU Type**		
Supported	Enabled	1000BASE-T half duplex mode, 1000BASE-X, -LX, -SX, -CX full duplex mode , Asymmetric and Symmetric PAUSE for full-duplex inks, Symmetric PAUSE for full-duplex links	100BaseTXFD - 2 pair category 5 UTP, full duplex mode		

FIGURE 3-11. LLDP-MED NEIGHBOR INFORMATION

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

PARAMETER DESCRIPTION

- Port: The port on which the LLDP frame was received.
- Device Type: LLDP-MED Devices are comprised of two primary Device Types: Network Connectivity Devices and Endpoint Devices.
- LLDP-MED Network Connectivity Device Definition

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

  1. LAN Switch/Router

  2. IEEE 802.1 Bridge

  3. IEEE 802.3 Repeater (included for historical reasons)

  4. IEEE 802.11 Wireless Access Point

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

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

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

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

- LLDP-MED Generic Endpoint (Class I): The LLDP-MED Generic Endpoint (Class I) definition is applicable to all endpoint products that require the base LLDP discovery services defined in TIA-1057, but 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 next.

  1. Voice - for use by dedicated IP Telephony handsets and other similar appliances supporting interactive voice services. These devices are typically deployed on a separate VLAN for ease of deployment and enhanced security by isolation from data applications.
  2. Voice Signaling - for use in network topologies that require a different policy for the voice signaling than for the voice media.
  3. Guest Voice - to support a separate limited feature-set voice service for guest users and visitors with their own IP Telephony handsets and other similar appliances supporting interactive voice services.
  4. Guest Voice Signaling - for use in network topologies that require a different policy for the guest voice signaling than for the guest voice media.
  5. Softphone Voice - for use by softphone applications on typical data centric devices, such as PCs or laptops.
  6. Video Conferencing - for use by dedicated Video Conferencing equipment and other similar appliances supporting real-time interactive video/audio services.

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

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

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

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

  - Defined: The network policy is defined.

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

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

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

- VLAN ID: VLAN ID is the VLAN identifier (VID) for the port as defined in IEEE 802.1Q-2003. A value of 1 through 4094 is used to define a valid VLAN ID. A value of 0 (Priority Tagged) is used if the device is using priority tagged frames as defined by IEEE 802.1Q-2003, meaning that only the IEEE 802.1D priority level is significant and the default PVID of the ingress port is used instead.
- Priority: Priority is the Layer 2 priority to be used for the specified application type. One of the eight priority levels (0 through 7).
- DSCP: DSCP is the DSCP value to be used to provide Diffserv node behavior for the specified application type as defined in IETF RFC 2474. Contain one of 64 code point values (0 through 63).
- Auto-negotiation: Auto-negotiation identifies if MAC/PHY auto-negotiation is supported by the link partner.
- Auto-negotiation status: Auto-negotiation status identifies if auto-negotiation is currently enabled at the link partner. If Auto-negotiation is supported and Auto-negotiation status is disabled, the 802.3 PMD operating mode will be determined the operational MAU type field value rather than by auto-negotiation.
- Auto-negotiation Capabilities: Auto-negotiation Capabilities shows the link partners MAC/PHY capabilities.

Buttons

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

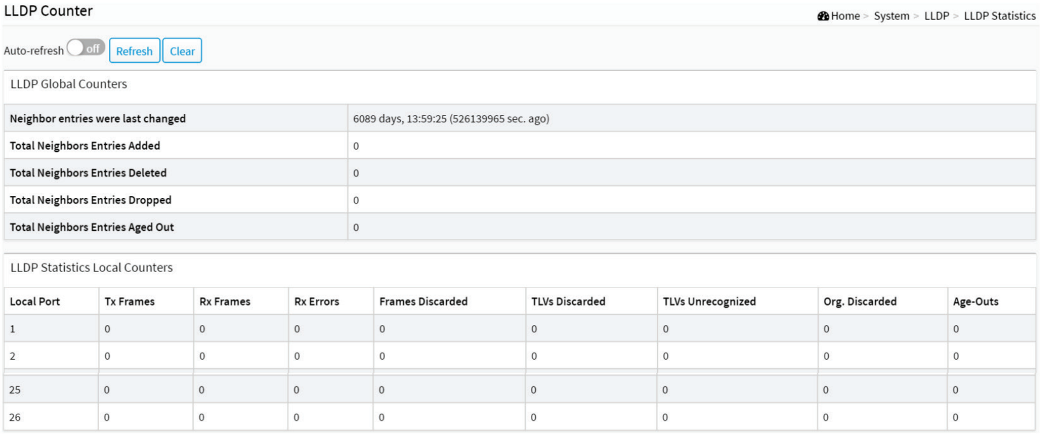
3.5.5 LLDP STATISTICS

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 Counter

LLDP Global Counters

Neighbor entries were last changed	6089 days, 13:59:25 (526139965 sec. ago)
Total Neighbors Entries Added	0
Total Neighbors Entries Deleted	0
Total Neighbors Entries Dropped	0
Total Neighbors Entries Aged Out	0

LLDP Statistics Local Counters

Local Port	Tx Frames	Rx Frames	Rx Errors	Frames Discarded	TLVs Discarded	TLVs Unrecognized	Org. Discarded	Age-Outs
1	0	0	0	0	0	0	0	0
2	0	0	0	0	0	0	0	0
25	0	0	0	0	0	0	0	0
26	0	0	0	0	0	0	0	0

FIGURE 3-12. LLDP STATISTICS INFORMATION

Global Counters

- Neighbor 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 Neighbors Entries Added: Shows the number of new entries added since switch reboot.
- Total Neighbors Entries Deleted: Shows the number of new entries deleted since switch reboot.
- Total Neighbors Entries Dropped: Shows the number of LLDP frames dropped due to the entry table being full.
- Total Neighbors Entries Aged Out: Shows the number of entries deleted due to Time-To-Live expiring.

Local Counters

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

- Local Port: The port on which LLDP frames are received or transmitted.
- Tx Frames: The number of LLDP frames transmitted on the port.
- Rx Frames: The number of LLDP frames received on the port.
- Rx Errors: The number of received LLDP frames containing some kind of error.
- Frames Discarded: If an LLDP frame is received on a port, and the switch's internal table has run full, the LLDP frame is counted and discarded. This situation is known as "Too Many Neighbors" in the LLDP standard. LLDP frames require a new entry in the table when the Chassis ID or Remote Port ID is not already contained within the table. Entries are removed from the table when a given port's link is down, an LLDP shutdown frame is received, or when the entry ages out.
- TLVs Discarded: Each LLDP frame can contain multiple pieces of information, known as TLVs (TLV is short for "Type Length Value"). If a TLV is malformed, it is counted and discarded.
- TLVs Unrecognized: The number of well-formed TLVs, but with an unknown type value.
- Org. Discarded: The number of organizationally received TLVs.
- Age-Outs: Each LLDP frame contains information about how long the LLDP information is valid (age-out time). If no new LLDP frame is received within the age out time, the LLDP information is removed, and the Age-Out counter is incremented.

Buttons

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

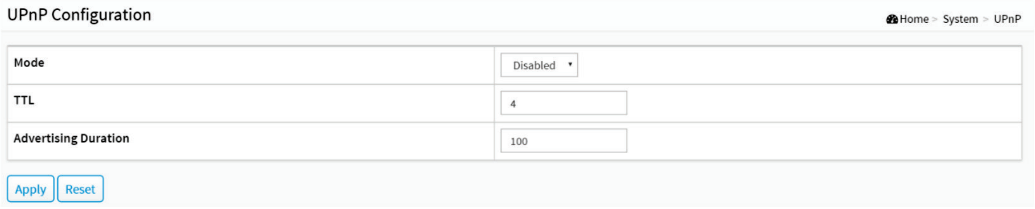
3.6 UPNP

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



UPnP Configuration

Mode	Disabled
TTL	4
Advertising Duration	100

FIGURE 3-13. UPNP CONFIGURATION SCREEN

PARAMETER DESCRIPTION

These parameters are displayed on the UPnP Configuration page:

- Mode: Indicates the UPnP operation mode. Possible modes are:
- Enabled: Enable UPnP mode operation.
- Disabled: Disable UPnP mode operation.
- Interface VLAN: Configure the interface VLAN that is used by UPnP. Allowed VLAN are in the range 1 through 4095, default being 1.
- 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 we recommend that such refreshing of advertisements be done at less than one-half of the advertising duration. In the implementation, the switch sends SSDP messages periodically at the interval one-half of the advertising duration minus 30 seconds. Valid values are in the range 100 to 86400.

Buttons

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

CHAPTER 4: PORT MANAGEMENT

This section describes how to configure the Port detail parameters of the switch. You can use the Port configure function to enable or disable the Port of the switch and monitor the port's content or status.

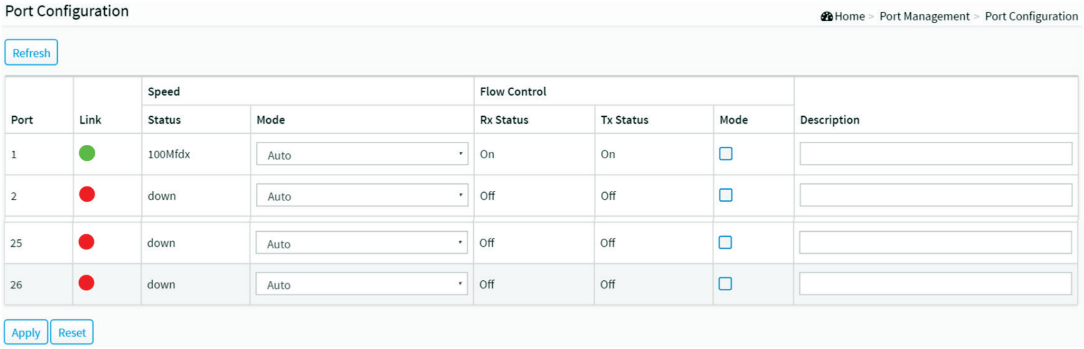
4.1 PORT CONFIGURATION

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 Speed Configured, Flow Control.
3. 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.
4. Click Apply.



Port Configuration

		Speed		Flow Control			
Port	Link	Status	Mode	Rx Status	Tx Status	Mode	Description
1	🟢	100Mfdx	Auto	On	On	□	
2	🔴	down	Auto	Off	Off	□	
25	🔴	down	Auto	Off	Off	□	
26	🔴	down	Auto	Off	Off	□	

FIGURE 4-1. PORT CONFIGURATION SCREEN

PARAMETER DESCRIPTION

- Port: This is the logical port number for this row.
- Link: The current link state is displayed graphically. Green indicates that the link is up and red that it is down.
- Current Link Speed: Provides the current link speed of the port.
- Configured Link Speed: Selects any available link speed for the given switch port. Only speeds supported by the specific port are shown. Possible speeds are:

Disabled - Disables the switch port operation.

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

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

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

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

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

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

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

SFP_Auto_AMS - Automatically determines the speed of the SFP.

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

100-FX - SFP port in 100-FX speed. The copper port is disabled.

100-FX_AMS - Port in AMS mode. The SFP port is running at 100-FX speed. The copper port is n Auto mode.

1000-X - SFP port is running at 1000-X speed. The copper port is disabled.

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

- Flow Control: When Auto Speed is selected on a port, this section indicates the flow control capability that is advertised to the link partner. When a fixed-speed setting is selected, that is what is used. The Current Rx column indicates whether pause frames on the port are obeyed, and the Current Tx column indicates whether pause frames on the port are transmitted. The Rx and Tx settings are determined by the result of the last Auto-Negotiation.
- Check the configured column to use flow control. This setting is related to the setting for Configured Link Speed.
- Description: Enter up to 63 characters to be the descriptive name that identifies this port.

Buttons

- Refresh: Click to refresh the Port link Status manually.
- Apply: Click to save changes.
- Reset: Click to undo any changes made locally and revert to previously saved values.

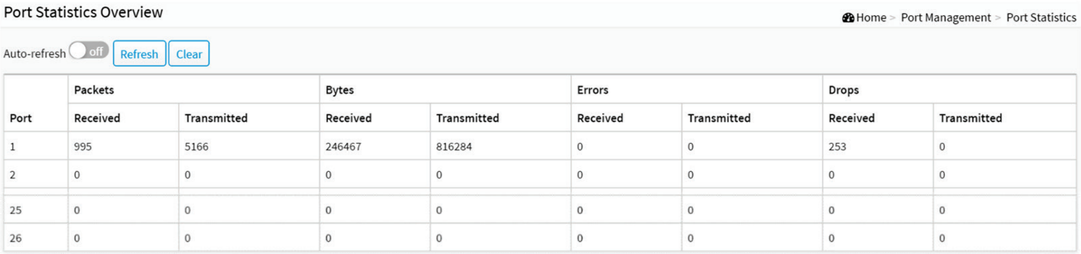
4.2 PORT STATISTICS

This section describes how to display the Port statistics information and provides an overview of general traffic statistics for all switch ports.

WEB INTERFACE

To Display the Port Statistics Overview in the web interface:

1. Click 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 details of the port statistics, then you need to click that port.



	Packets		Bytes		Errors		Drops	
Port	Received	Transmitted	Received	Transmitted	Received	Transmitted	Received	Transmitted
1	995	5166	246467	816284	0	0	253	0
2	0	0	0	0	0	0	0	0
25	0	0	0	0	0	0	0	0
26	0	0	0	0	0	0	0	0

FIGURE 4-2. PORT STATISTICS OVERVIEW

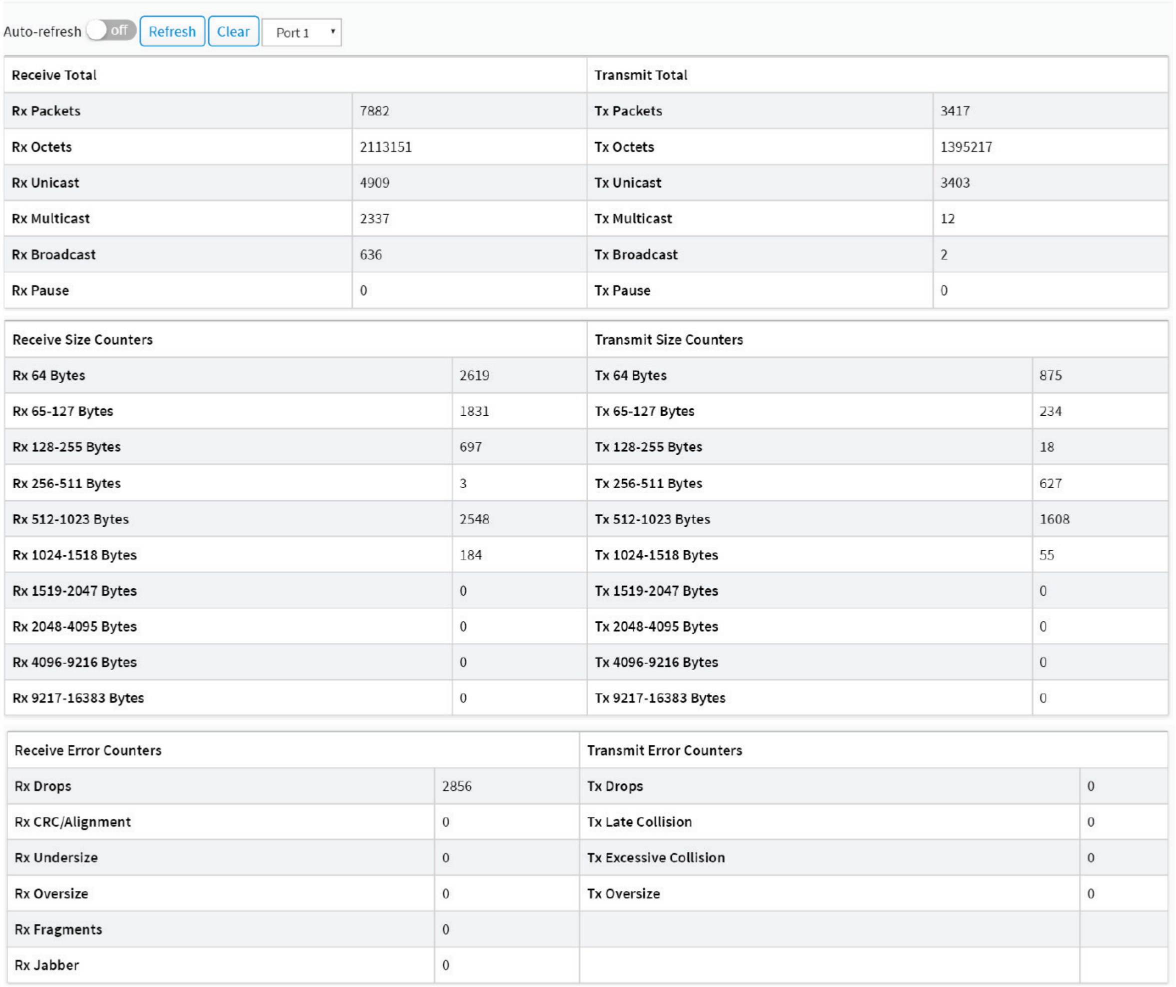
PARAMETER DESCRIPTION

- 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.

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 details of the port statistics, 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.



Receive Total		Transmit Total	
Rx Packets	7882	Tx Packets	3417
Rx Octets	2113151	Tx Octets	1395217
Rx Unicast	4909	Tx Unicast	3403
Rx Multicast	2337	Tx Multicast	12
Rx Broadcast	636	Tx Broadcast	2
Rx Pause	0	Tx Pause	0

Receive Size Counters		Transmit Size Counters	
Rx 64 Bytes	2619	Tx 64 Bytes	875
Rx 65-127 Bytes	1831	Tx 65-127 Bytes	234
Rx 128-255 Bytes	697	Tx 128-255 Bytes	18
Rx 256-511 Bytes	3	Tx 256-511 Bytes	627
Rx 512-1023 Bytes	2548	Tx 512-1023 Bytes	1608
Rx 1024-1518 Bytes	184	Tx 1024-1518 Bytes	55
Rx 1519-2047 Bytes	0	Tx 1519-2047 Bytes	0
Rx 2048-4095 Bytes	0	Tx 2048-4095 Bytes	0
Rx 4096-9216 Bytes	0	Tx 4096-9216 Bytes	0
Rx 9217-16383 Bytes	0	Tx 9217-16383 Bytes	0

Receive Error Counters		Transmit Error Counters	
Rx Drops	2856	Tx Drops	0
Rx CRC/Alignment	0	Tx Late Collision	0
Rx Undersize	0	Tx Excessive Collision	0
Rx Oversize	0	Tx Oversize	0
Rx Fragments	0		
Rx Jabber	0		

FIGURE 4-3. DETAILED PORT STATISTICS

PARAMETER DESCRIPTION

- Upper left scroll bar: Scroll to the 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

- 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.

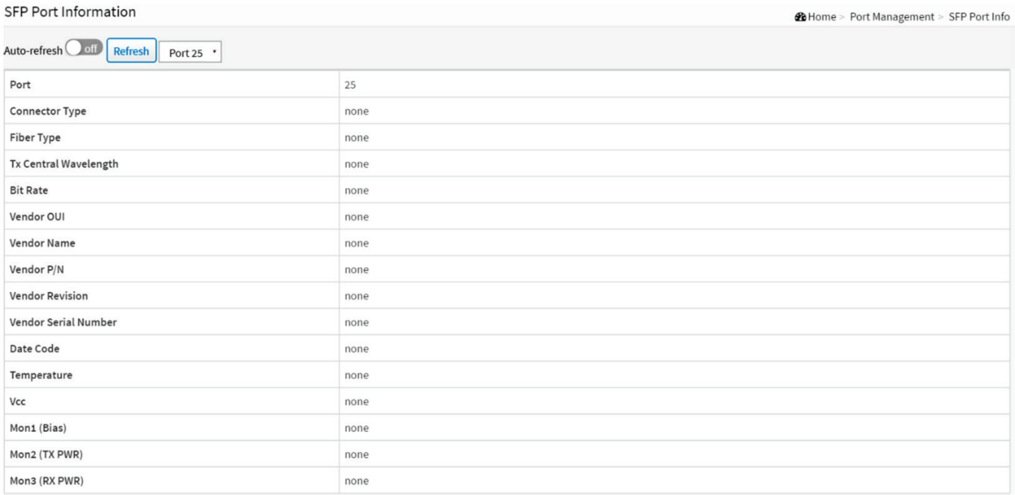
4.3 SFP PORT INFO

This section describes how the switch displays the SFP module detail information connected 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. The SFP Information displays.



Port	25
Connector Type	none
Fiber Type	none
Tx Central Wavelength	none
Bit Rate	none
Vendor OUI	none
Vendor Name	none
Vendor P/N	none
Vendor Revision	none
Vendor Serial Number	none
Date Code	none
Temperature	none
Vcc	none
Mon1 (Bias)	none
Mon2 (TX PWR)	none
Mon3 (RX PWR)	none

FIGURE 4-4. SFP PORT INFORMATION SCREEN

PARAMETER DESCRIPTION

- Upper left scroll bar: To scroll which port to display the Port statistics.
- Connector Type: Displays the connector type, for instance, UTP, SC, ST, LC and so on.
- Fiber Type: Displays the fiber mode, for instance, Multi-Mode, Single-Mode.
- Tx Central Wavelength: Displays the fiber optical transmitting central wavelength, for instance, 850 nm, 1310 nm, 1550 nm, and so on.
- Bit Rate: Displays the nominal bit rate of the transceiver.
- Vendor OUI: Displays the Manufacturer's OUI code, which is assigned by IEEE.
- Vendor Name: Displays the company name of the module manufacturer.
- Vendor P/N: Displays the product name of the naming by module manufacturer.
- Vendor Rev (Revision): Displays the module revision.
- Vendor SN (Serial Number): Shows the serial number assigned by the manufacturer.
- Date Code: Shows the date this SFP module was made.
- Temperature: Shows the current temperature of the SFP module.
- Vcc: Shows the working DC voltage of the SFP module.
- Mon1(Bias) mA: Shows the Bias current of the SFP module.
- Mon2(TX PWR): Shows the transmit power of the SFP module.
- Mon3(RX PWR): Shows the receiver power of the SFP module.

Buttons

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

4.4 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.

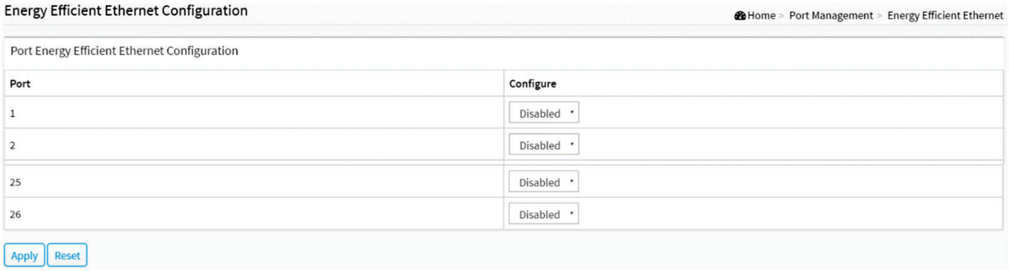
EEE is a power saving option that reduces the power usage when there is very low traffic utilization (or no traffic).

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 1 Gbit links and 30 μs for other link speeds. EEE devices must agree upon the value of the wakeup time to make sure that both the receiving and transmitting device have 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 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 Configuration

Home > Port Management > Energy Efficient Ethernet

Port Energy Efficient Ethernet Configuration

Port	Configure
1	Disabled
2	Disabled
25	Disabled
26	Disabled

FIGURE 4-5. ENERGY EFFICIENT ETHERNET CONFIGURATION SCREEN

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.

4.5 LINK AGGREGATION

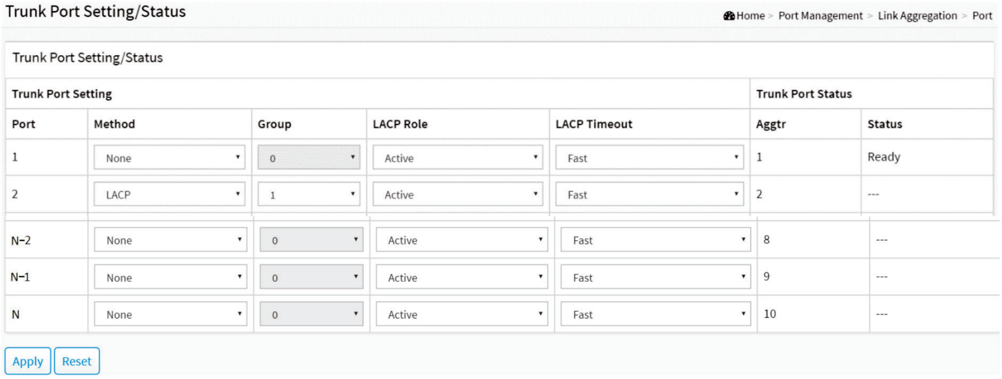
4.5.1 PORT

This section describes the Port setting/status that is used to configure the trunk property of each and every port in the switch system.

WEB INTERFACE

To configure the trunk property of each and every port in the web interface:

1. Click Port Management, Link Aggregation and port.
2. Specify the Method, Group, LACP Role and LACP Timeout.
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.



Trunk Port Setting/Status

Trunk Port Setting/Status

Trunk Port Setting					Trunk Port Status	
Port	Method	Group	LACP Role	LACP Timeout	Aggtr	Status
1	None	0	Active	Fast	1	Ready
2	LACP	1	Active	Fast	2	---
N-2	None	0	Active	Fast	8	---
N-1	None	0	Active	Fast	9	---
N	None	0	Active	Fast	10	---

FIGURE 4-6. TRUNK PORT SETTING/STATUS

PARAMETER DESCRIPTION

- Port: The logical port for the settings contained in the same row.
- Method: This determines the method a port uses to aggregate with other ports.
  - None: A port that does not want to aggregate with any other port should choose this default setting.
  - LACP: A port uses LACP as its trunk method to get aggregated with other ports also using LACP.
  - Static: A port uses Static Trunk as its trunk method to get aggregated with other ports also using Static Trunk.
- Group: Ports choosing the same trunking method other than "None" must be assigned a unique Group number to declare that they want to aggregate with each other.
- LACP Role: This field is only referenced when a port's trunking method is LACP.
  - Active: An Active LACP port begins to send LACPDU to its link partner right after the LACP protocol entity started to take control of this port.
  - Passive: A Passive LACP port will not actively send LACPDU out before it receives an LACPDU from its link partner.
- LACP Timeout: The Timeout controls the period between BPDU transmissions.
  - Fast: It will transmit LACP packets each second.
  - Slow: It will wait for 30 seconds before sending an LACP packet.

- Aggtr: Aggtr is an abbreviation of “aggregator”. Every port is also an aggregator, and its own aggregator ID is the same as its own Port No. We can regard an aggregator as a representative of a trunking group. Ports with same Group ID and using same trunking method will have the opportunity to aggregate to a particular aggregator port. This aggregator port is usually the port with the smallest Port No. within the trunking group.
- Status: This field represents the trunking status of a port that uses a trunking method other than “None”. It also represents the management link status of a port that uses the “None” trunking method. “---“ means “not ready”

Buttons

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

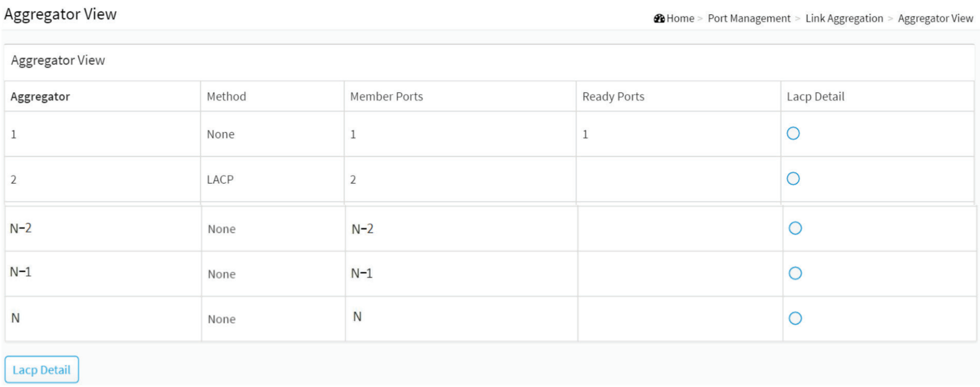
4.5.2 AGGREGATOR VIEW

Display the current port trunking information from the aggregator point of view.

WEB INTERFACE

To see the LACP detail in the web interface:

1. Click Port Management, Link Aggregation and Aggregator View.
2. Click LACP Detail.



Aggregator View

Home > Port Management > Link Aggregation > Aggregator View

Aggregator View

Aggregator	Method	Member Ports	Ready Ports	Lacp Detail
1	None	1	1	○
2	LACP	2		○
N-2	None	N-2		○
N-1	None	N-1		○
N	None	N		○

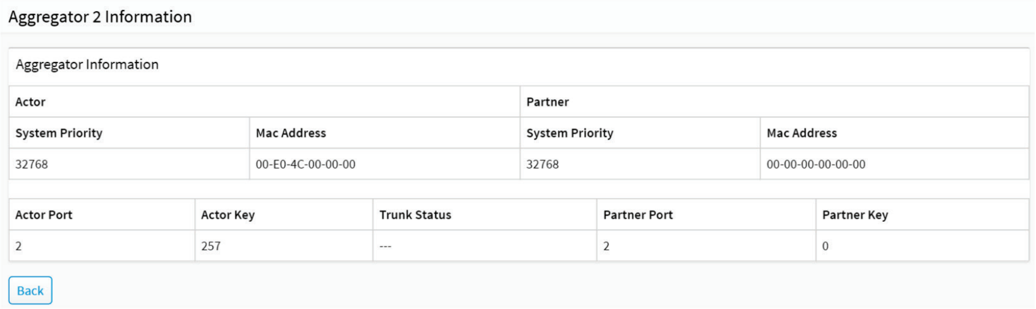
FIGURE 4-7. THE AGGREGATOR VIEW

PARAMETER DESCRIPTION

- Aggregator: It shows the aggregator ID of every port. In fact, every port is also an aggregator, and its own aggregator ID is the same as its own Port No.
- Method: Shows the method a port uses to aggregate with other ports.
- Member Ports: Shows all member ports of an aggregator (port).
- Ready Ports: Shows only the ready member ports within an aggregator (port).
- Lacp Detail: You can select the port that you want to see the LACP Detail.

Buttons

- Lacp Detail: Click this button, then you will see the aggregator information. Details will be described in the next screen.



Aggregator 2 Information

Aggregator Information

Actor		Partner	
System Priority	Mac Address	System Priority	Mac Address
32768	00-E0-4C-00-00-00	32768	00-00-00-00-00-00

Actor Port	Actor Key	Trunk Status	Partner Port	Partner Key
2	257	---	2	0

FIGURE 4-8. THE LACP DETAIL

PARAMETER DESCRIPTION

Actor

- System Priority: Shows the System Priority part of the aggregation Actor. (1-65535)
- Mac Address: The system ID of the aggregation Actor.
- Actor Port: The actor's port number connected to this port.
- Actor Key: The Key that the actor has assigned to this aggregation ID.

Partner

- System Priority: Shows the System Priority part of the aggregation partner. (1-65535)
- Mac Address: The system ID of the aggregation partner.
- Partner Port: The partner's port number connected to this port.
- Partner Key: The Key that the partner has assigned to this aggregation ID.
- Trunk Status: This field represents the trunking status of a port that uses a trunking method other than "None". It also represents the management link status of a port that uses the "None" trunking method. "---" means "not ready"

Button

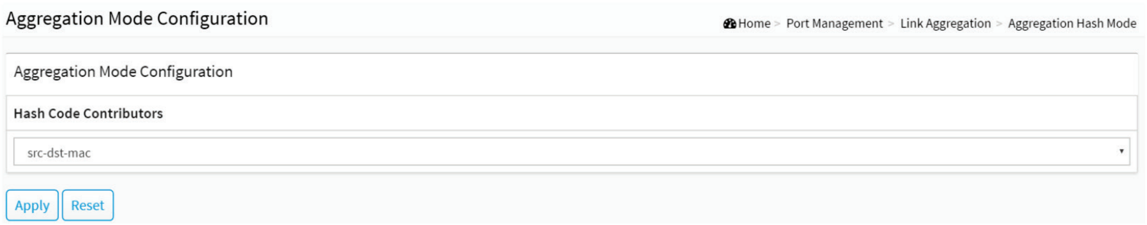
- Back: Click to undo any changes made locally and return to the Users.

4.5.3 AGGREGATION HASH MODE

WEB INTERFACE

To configure the Aggregation hash mode in the web interface:

1. Click Port Management, Link Aggregation and Aggregator Hash Mode.
2. Click Hash Code Contributors to select the mode.
3. Click apply to save the setting.
4. If you want to cancel the setting, then you need to click the Reset button. It will revert to previously saved values.


Aggregation Mode Configuration

Aggregation Mode Configuration

Hash Code Contributors: src-dst-mac

Home > Port Management > Link Aggregation > Aggregation Hash Mode
Apply
Reset

FIGURE 4-9.AGGREGATION HASH MODE

PARAMETER DESCRIPTION

Hash Code Contributors

- src-mac: 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.
- dst-mac: 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: 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.
- src-dst-mac: Source MAC Address + Destination MAC Address.
- src-ip: Source IP Address.
- dst-ip: Destination IP Address.
- src-dst-ip: Source IP Address + Destination IP Address.

Buttons

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

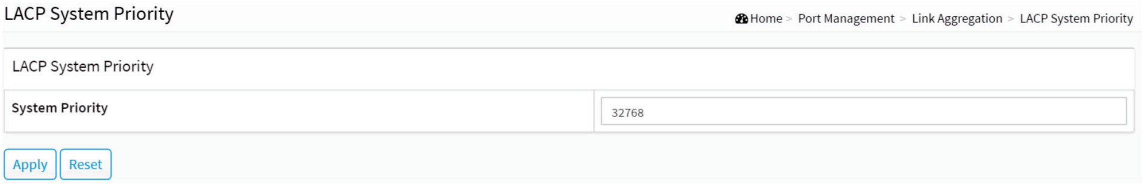
4.5.4 LACP SYSTEM PRIORITY

It is used to set the priority part of the LACP system ID. LACP will only aggregate together the ports whose peer link partners are all on a single system. Each system that supports LACP will be assigned a globally unique System Identifier for this purpose. A system ID is a 64-bit field comprising a 48-bit MAC Address and 16-bit priority value. The System Priority can be set by the user. Its range is from 1 to 65535. Default: 32768

WEB INTERFACE

To configure the LACP System Priority in the web interface:

1. Click Port Management, Link Aggregation and LACP System Priority.
2. Specify the LACP System Priority.
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.



LACP System Priority

Home > Port Management > Link Aggregation > LACP System Priority

LACP System Priority

System Priority	32768

FIGURE 4-10.LACP SYSTEM PRIORITY

PARAMETER DESCRIPTION

- System Priority: 1-65535. Show the System Priority part of a system ID.

Buttons

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

4.6 LOOP PROTECTION

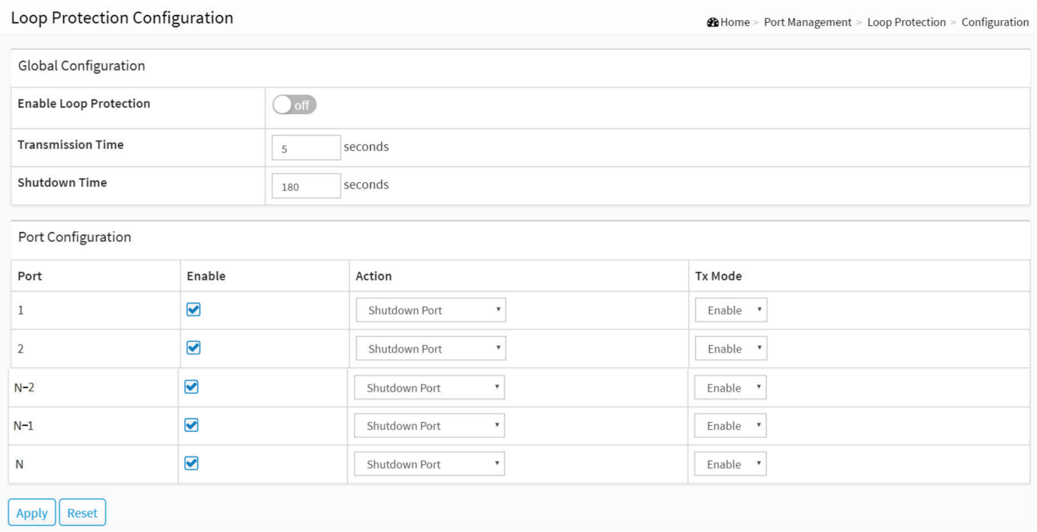
4.6.1 CONFIGURATION

The loop Protection is used to detect the presence of traffic. When the switch receives a packet's (looping detection frame) MAC address the same as oneself from a port, Loop Protection occurs. The port will be locked when it receives the looping Protection frames. If you want to resume the locked port, find out the looping path and remove the looping path, then 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. Select enable or disable the port loop Protection.
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.



Loop Protection Configuration

Home > Port Management > 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-2	☑	Shutdown Port	Enable
N-1	☑	Shutdown Port	Enable
N	☑	Shutdown Port	Enable

FIGURE 4-11. LOOP PROTECTION CONFIGURATION SCREEN

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 if 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.

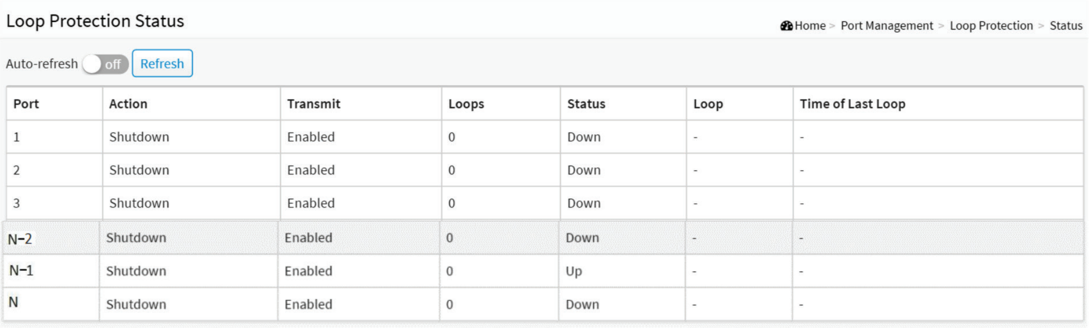
4.6.2 STATUS

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

WEB INTERFACE

To display the Loop Protection status in the web interface:

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



Port	Action	Transmit	Loops	Status	Loop	Time of Last Loop
1	Shutdown	Enabled	0	Down	-	-
2	Shutdown	Enabled	0	Down	-	-
3	Shutdown	Enabled	0	Down	-	-
N-2	Shutdown	Enabled	0	Down	-	-
N-1	Shutdown	Enabled	0	Up	-	-
N	Shutdown	Enabled	0	Down	-	-

FIGURE 4-12. LOOP PROTECTION STATUS SCREEN

PARAMETER DESCRIPTION

Parameter description:

- Port: The switch port number of the logical port.
- Action: The currently configured port action.
- Transmit: The currently configured port transmit mode.
- Loops: The number of loops detected on this port.
- Status: The current loop protection status of the port.
- Loop: Whether a loop is currently detected on the port.
- Time of Last Loop: The time of the last loop event detected.

Buttons

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

5.1 VLAN CONFIGURATION

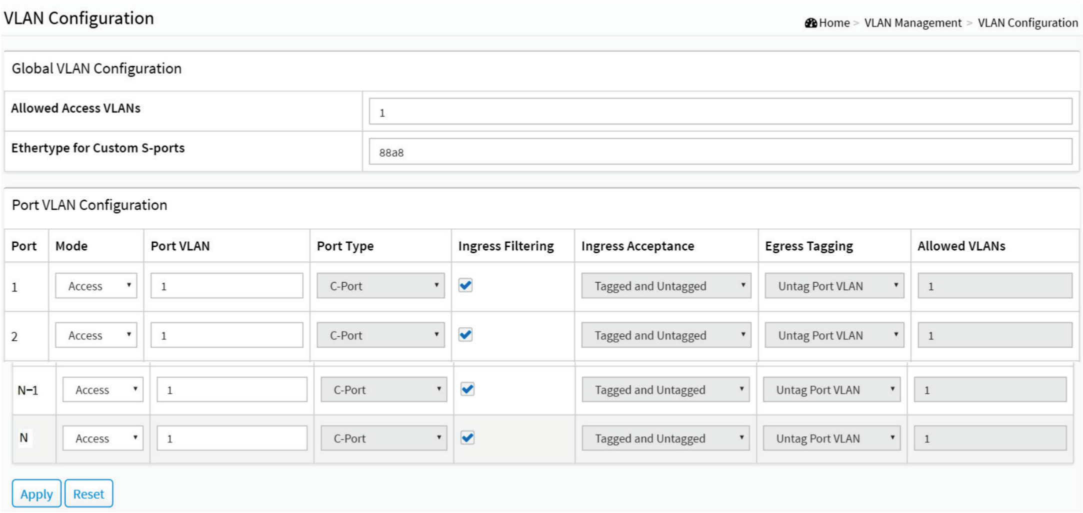
This section explains how to assign a specific VLAN for management purposes. The management VLAN is used to establish an IP connection to the switch from a workstation connected to a port in the VLAN. This connection supports a VSM, SNMP, and Telnet session. By default, the active management VLAN is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

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

WEB INTERFACE

To configure VLAN membership in the web interface:

1. Click VLAN Management and VLAN Configuration.
2. Specify Existing VLANs, Ether type for Custom S-ports.
3. Click Apply.



VLAN Configuration

Home > VLAN Management > VLAN Configuration

Global VLAN Configuration

Allowed Access VLANs	1
Ethertype for Custom S-ports	88a8

Port VLAN Configuration

Port	Mode	Port VLAN	Port Type	Ingress Filtering	Ingress Acceptance	Egress Tagging	Allowed VLANs
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–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. VLAN CONFIGURATION SCREEN

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 add additional port configuration features. In addition to the characteristics described for trunk ports, hybrid ports have these abilities:

- Can be configured to be VLAN tag unaware, C-tag aware, S-tag aware, or S-custom-tag aware,
- ingress filtering can be controlled,
- ingress acceptance of frames and configuration of egress tagging can be configured independently.

- Port VLAN: Determines the port’s VLAN ID (a.k.a. PVID). Allowed VLANs are in the range 1 through 4095, default being 1.

On ingress, frames get classified to the Port VLAN if the port is configured as VLAN unaware, the frame is untagged, or VLAN awareness is enabled on the port, but the frame is priority tagged (VLAN ID = 0).

On egress, frames classified to the Port VLAN do not get tagged if Egress Tagging configuration is set to untag Port VLAN.

The Port VLAN is called an “Access VLAN” for ports in Access mode and Native VLAN for ports in Trunk or Hybrid mode.

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

Unaware:

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

C-Port:

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

S-Port:

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

S-Custom-Port:

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

- Ingress Filtering: Hybrid ports allow for changing ingress filtering. Access and Trunk ports always have ingress filtering enabled.

If ingress filtering is enabled (checkbox is checked), frames classified to a VLAN that the port is not a member of get discarded.

If ingress filtering is disabled, frames classified to a VLAN that the port is not a member of are accepted and forwarded to the switch engine. However, the port will never transmit frames classified to VLANs that it is not a member of.

- VLAN Trunking: Trunk and Hybrid ports allow for enabling VLAN trunking.

When VLAN trunking is enabled, frames classified to unknown VLANs are accepted on the port whether ingress filtering is enabled or not.

This is useful in scenarios where a cloud of intermediary switches must bridge VLANs that haven't been created. By configuring the ports that connect the cloud of switches as trunking ports, they can seamlessly carry those VLANs from one end to the other.

- Ingress Acceptance: Hybrid ports allow for changing the type of frames that are accepted on ingress.

Tagged and untagged

Both tagged and untagged frames are accepted.

Tagged Only

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

Untagged Only

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

- Egress Tagging: Ports in Trunk and Hybrid mode may control the tagging of frames on egress.

Untag Port VLAN

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

Tag All

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

Untag All

All frames, whether classified to the Port VLAN or not, are transmitted without a tag.

This option is only available for ports in Hybrid mode.

- Allowed VLANs: Ports in Trunk and Hybrid mode may control which VLANs they are allowed to become members of. Access ports can only be member of one VLAN, the Access VLAN.

  The field's syntax is identical to the syntax used in the Existing VLANs field. By default, a port may become a 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.

Buttons

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

5.2 VLAN MEMBERSHIP

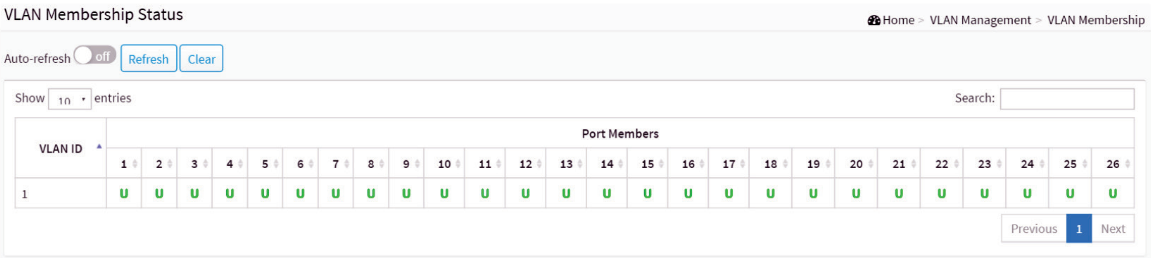
This page provides an overview of membership status of VLAN users.

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 to choose which VLANs you want to show.
3. Click Refresh to update the state.



VLAN Membership Status

VLAN ID	Port Members																									
	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
1	U	U	U	U	U	U	U	U	U	U	U	U	U	U	U	U	U	U	U	U	U	U	U	U	U	U

FIGURE 5-2. VLAN MEMBERSHIP SCREEN

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 use 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 and will be displayed. It shows egress filtering frame status whether tagged or untagged. Frames classified to the Port VLAN are transmitted tagged( ) or untagged( ).
- VLAN Membership: The VLAN Membership Status Page will 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 will show this information for all the VLAN Users, and this is by default. VLAN membership allows the frames classified to the VLAN ID to be forwarded on the respective VLAN member ports.
- Show entries: You can choose how many items you want to show up.
- Admin drop-down box: You can choose the Vlan User.
- Search: You can search for the information that you want to see.

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.
- Next: Updates the system log entries, turns to the next page.
- Previous: Updates the system log entries, turns to the previous page.

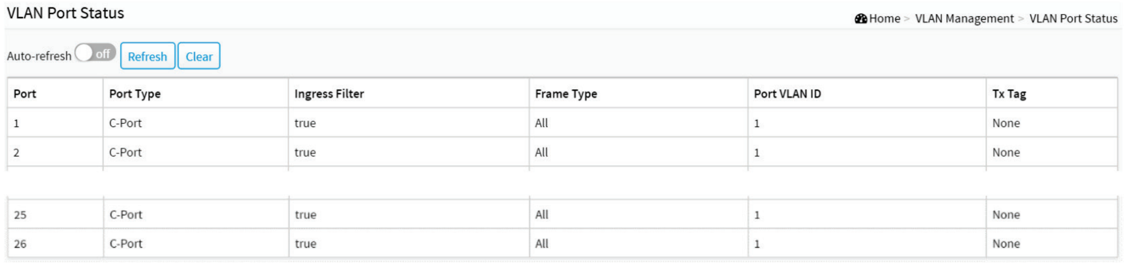
5.3 VLAN PORT STATUS

The Port Status function gathers the information of all VLAN status and reports it in order: 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.
3. Display Port Status information.



Port	Port Type	Ingress Filter	Frame Type	Port VLAN ID	Tx Tag
1	C-Port	true	All	1	None
2	C-Port	true	All	1	None
25	C-Port	true	All	1	None
26	C-Port	true	All	1	None

FIGURE 5-3. VLAN PORT STATUS SCREEN

PARAMETER DESCRIPTION

- VLAN USER: The VLAN User module uses services of the VLAN management functionality to configure VLAN memberships and VLAN port configuration such as PVID, UVID. The switch supports 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 use 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 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.
- Admin drop-down box: You can choose the Vlan User.

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.

5.4 VLAN SELECTIVE QINQ CONFIGURATION

A Q-in-Q VLAN tunnel enables a service provider to segregate the traffic of different customers in their infrastructure, while still giving the customer a full range of VLANs for their internal use by adding a second 802.1Q tag to an already tagged frame.

WEB INTERFACE

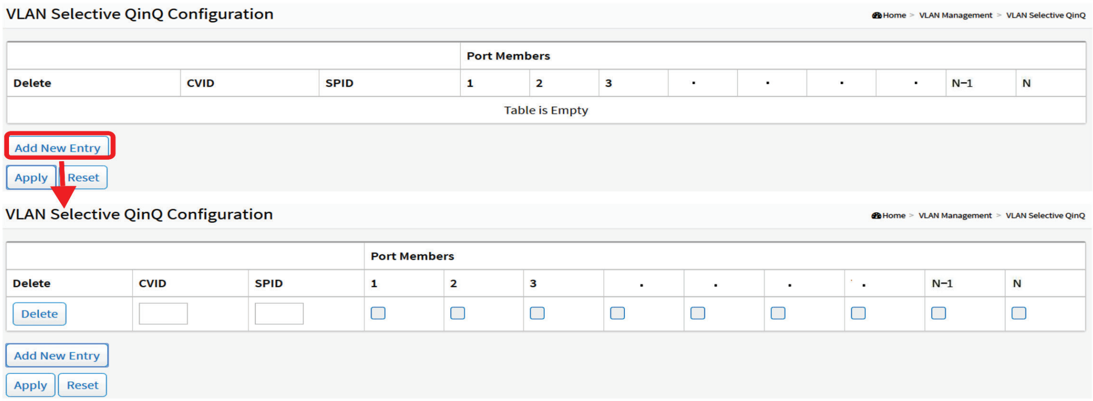
To configure VLAN selective QinQ in the web interface:

1. Click VLAN Management and VLAN Selective QinQ Configuration.

2. Click “Add New Entry”.

3. Specify CVID, SPID, Port Members.

4. Click Apply.



VLAN Selective QinQ Configuration

Home > VLAN Management > VLAN Selective QinQ

			Port Members								
Delete	CVID	SPID	1	2	3	·	·	·	·	N–1	N
Table is Empty											

Add New Entry
Apply
Reset

VLAN Selective QinQ Configuration

Home > VLAN Management > VLAN Selective QinQ

			Port Members								
Delete	CVID	SPID	1	2	3	·	·	·	·	N–1	N
Delete			□	□	□	□	□	□	□	□	□

Add New Entry
Apply
Reset

FIGURE 5-4. VLAN SELECTIVE QINQ SCREEN

PARAMETER DESCRIPTION

- CVID: 1-4095, The customer VLAN ID List to which the tagged packets will be added.
- SPID: 1-4095, This configures the VLAN to join the Service Providers VLAN as a tagged member.
- Port Members: Checkmarks indicate which ports are members of the entry. Check or uncheck as needed to modify the entry.

Buttons

- Delete: To delete a QinQ configuration entry, check this box. The entry will be deleted during the next Save.
- Add New Entry: Click to add a new QinQ configuration.
- Apply: Click to save changes.
- Reset: Click to undo any changes made locally and revert to previously saved values.

5.5 MAC-BASED VLAN

5.5.1 CONFIGURATION

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

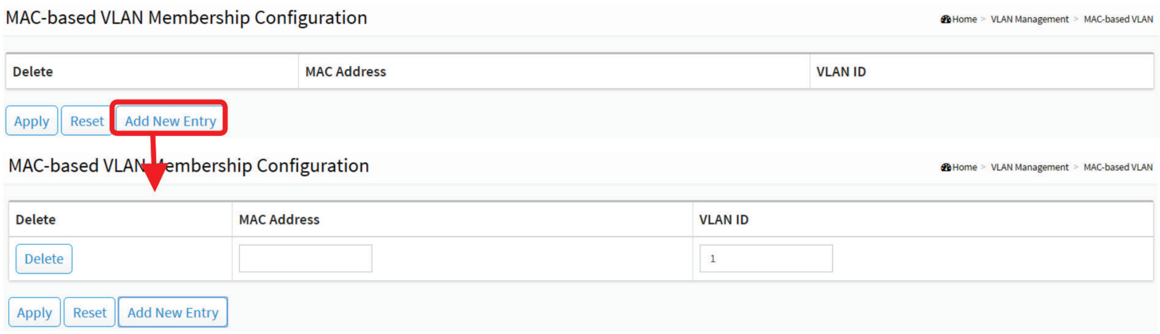
The most common way of grouping VLAN members is by port, hence the name port-based VLAN. Typically, the device adds the same VLAN tag to untagged packets that are received through the same port. Later on, these packets can be forwarded in the same VLAN. Port-based VLAN is easy to configure, and applies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

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

WEB INTERFACE

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

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


Home > VLAN Management > MAC-based VLAN
Apply
Reset
Add New Entry
Home > VLAN Management > MAC-based VLAN
Delete
Apply
Reset
Add New Entry

MAC-based VLAN Membership Configuration

Delete	MAC Address	VLAN ID

MAC-based VLAN Membership Configuration

Delete	MAC Address	VLAN ID
Delete		1

FIGURE 5-5. MAC-BASED VLAN CONFIGURATION SCREEN

PARAMETER DESCRIPTION

- MAC Address: Indicates the MAC address.
- VLAN ID: Indicates the VLAN ID.

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

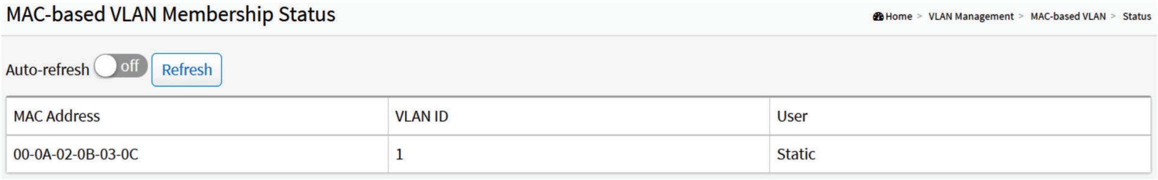
5.5.2 STATUS

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 select "Auto-refresh".
3. Click "Refresh" to refresh the MAC-based VLAN Membership Status.



MAC-based VLAN Membership Status

MAC Address	VLAN ID	User
00-0A-02-0B-03-0C	1	Static

FIGURE 5-6. MAC-BASED VLAN MEMBERSHIP STATUS SCREEN

PARAMETER DESCRIPTION

- MAC Address: Indicates the MAC address.
- VLAN ID: Indicates the VLAN ID.
- User: Indicates the user.

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 PROTOCOL-BASED VLAN

This section describes Protocol -based VLAN. The switch supports Ethernet LLC and SNAP protocols.

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.

5.6.1 PROTOCOL TO GROUP

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

WEB INTERFACE

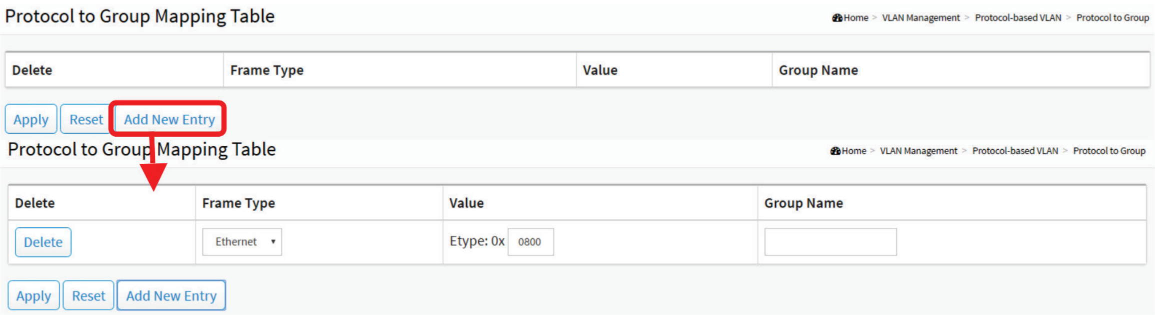
To configure Protocol -based VLAN configuration in the web interface:

1. Click VLAN Management, Protocol-based VLAN and Protocol to Group.

2. Click “Add New Entry”.

3. Specify the Ethernet LLC SNAP Protocol, Value and Group Name.

4. Click Apply.



Protocol to Group Mapping Table

Delete	Frame Type	Value	Group Name

Home > VLAN Management > Protocol-based VLAN > Protocol to Group
Apply
Reset
Add New Entry

Protocol to Group Mapping Table

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

Home > VLAN Management > Protocol-based VLAN > Protocol to Group
Apply
Reset
Add New Entry

FIGURE 5-7. 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, a valid value of the following text field will vary depending on the new frame type you selected.

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

  Below is the criteria for three different Frame Types:

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

  2. For LLC: A 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: A valid value in this case also is comprised of two different sub-values.

  a.OUI: OUI (Organizationally Unique Identifier) is a value in the format of xx-xx-xx where each pair (xx) in string is a hexadecimal value ranging 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.
- Adding 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.

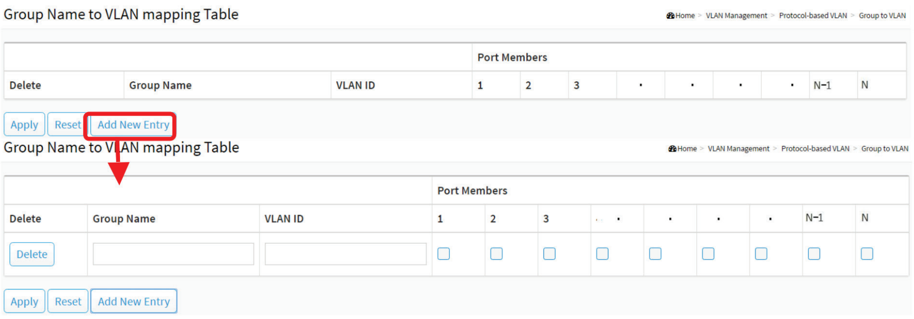
5.6.2 GROUP TO VLAN

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 a Group Name to VLAN mapping table in the web interface:

1. Click VLAN Management, Protocol-based VLAN and Group to Group.
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

			Port Members								
Delete	Group Name	VLAN ID	1	2	3	·	·	·	·	N−1	N

Apply
Reset
Add New Entry

Group Name to VLAN mapping Table

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

			Port Members								
Delete	Group Name	VLAN ID	1	2	3	·	·	·	·	N−1	N
Delete			□	□	□	□	□	□	□	□	□

Apply
Reset
Add New Entry

FIGURE 5-8. 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.
- Adding 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 a new entry.
- Apply: Click to save changes.
- Reset: Click to undo any changes made locally and revert to previously saved values.

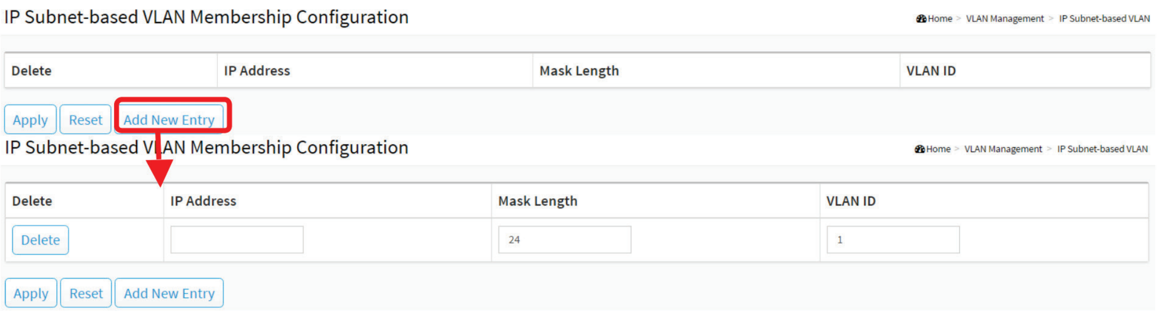
5.7 IP SUBNET-BASED VLAN

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 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 Membership Configuration

Home > VLAN Management > IP Subnet-based VLAN

Delete	IP Address	Mask Length	VLAN ID

Apply Reset Add New Entry

IP Subnet-based VLAN Membership Configuration

Home > VLAN Management > IP Subnet-based VLAN

Delete	IP Address	Mask Length	VLAN ID
Delete		24	1

Apply Reset Add New Entry

FIGURE 5-9. 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.

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.
- Adding 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.

5.8 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.

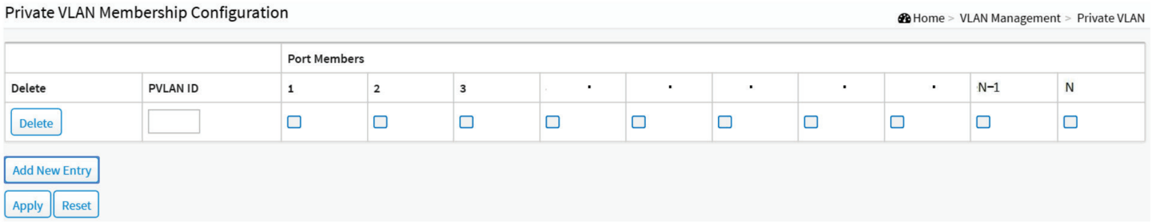
A VLAN unaware port can only be a member of one VLAN, but it can be a member of multiple Private VLANs.

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

WEB INTERFACE

To configure Port Isolation in the web interface:

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



Private VLAN Membership Configuration

Home > VLAN Management > Private VLAN

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

FIGURE 5-10. 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.
- Adding 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

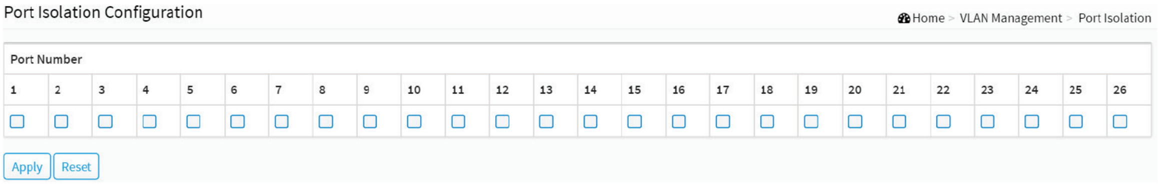
Port Isolation provides for an apparatus and method to isolate ports on layer 2 switches on the same VLAN to restrict traffic flow. The apparatus comprises a switch having said plurality of ports, each port configured as a protected port or a non-protected port. An address table memory stores an address table having a destination address and port number pair. A forwarding map generator generates a forwarding map that 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 ports according 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 in the web interface:

1. Click VLAN Management and Port Isolation.
2. Select the port to enable Port Isolation.
3. Click Apply.



Port Isolation Configuration

Home > VLAN Management > Port Isolation

Port Number

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
□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□

FIGURE 5-11. 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, you can perform QoS-related configuration for voice data, ensuring the transmission priority of voice traffic and voice quality.

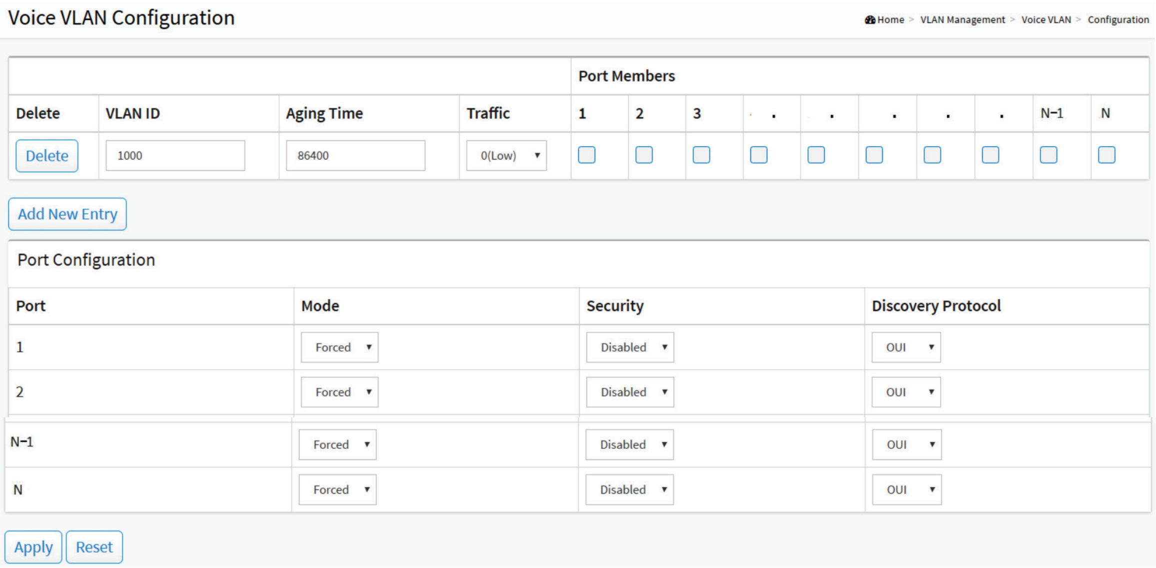
5.10.1 CONFIGURATION

The Voice VLAN feature enables voice traffic forwarding on the Voice VLAN, then the switch can classify and schedule network traffic. We recommend 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. Click "Add New Entry".
3. Select Port Members in the Voice VLAN Configuration.
4. Specify VLAN ID, Aging Time, Traffic.
5. Specify (Mode, Security, Discovery Protocol) in the Port Configuration.
6. Click Apply.



Voice VLAN Configuration

				Port Members									
Delete	VLAN ID	Aging Time	Traffic	1	2	3	.	.	.	.	.	N-1	N
Delete	1000	86400	0(Low)	□	□	□	□	□	□	□	□	□	□

Port Configuration

Port	Mode	Security	Discovery Protocol
1	Forced	Disabled	OUI
2	Forced	Disabled	OUI
N-1	Forced	Disabled	OUI
N	Forced	Disabled	OUI

FIGURE 5-12. VOICE VLAN CONFIGURATION

PARAMETER DESCRIPTION

- Port Members: Indicates the Voice VLAN port mode operation. Disable the MSTP feature before enabling Voice VLAN. This will avoid the conflict of ingress filtering. Select the port for which you want to enable the 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 to this class.

Port Configuration

- Port: The switch port number of the Voice VLAN port.
- Mode: Indicates the Voice VLAN port mode.

When the port mode isn’t disabled, you must disable MSTP feature before you enable Voice VLAN. It can avoid the conflict of ingress filtering.

Possible port modes are:

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

Forced: Force join to Voice VLAN.

- 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.

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

- Add New entry: Click to add a new entry in Voice VLAN configuration.
- Apply: Click to save changes.
- Reset: Click to undo any changes made locally and revert to previously saved values.

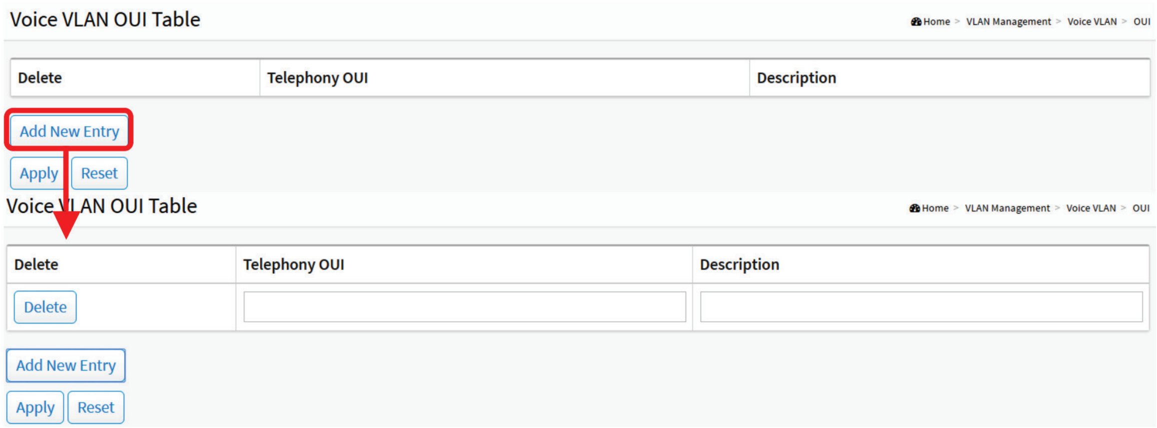
5.10.2 OUI

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

WEB INTERFACE

To configure a 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

Delete	Telephony OUI	Description

Voice VLAN OUI Table

Delete	Telephony OUI	Description
Delete		

Home > VLAN Management > Voice VLAN > OUI
Add New Entry
Apply
Reset
Home > VLAN Management > Voice VLAN > OUI
Add New Entry
Apply
Reset

FIGURE 5-13. 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.

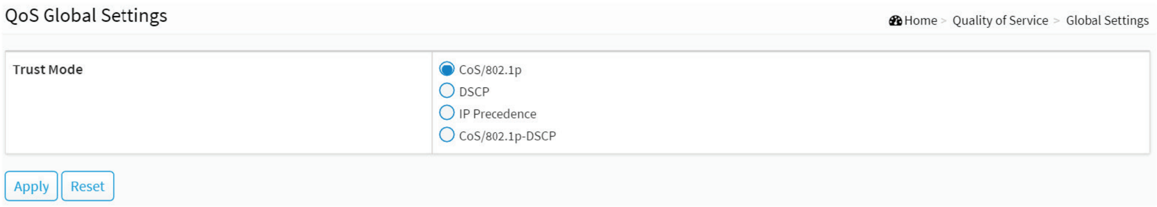
6.1 GLOBAL SETTINGS

Use the Global Settings page to set the trust behavior for QoS basic mode. This configuration is active when the switch is in QoS basic mode. Packets entering a QoS domain are classified at the edge of the QoS domain.

WEB INTERFACE

To configure the Global Settings in the web interface:

1. Click Quality of Service and Global Settings.
2. Select the trust mode when the switch is in QoS basic mode. If a packet CoS level and DSCP tag are mapped to separate queues, the trust mode determines the queue to which the packet is assigned.
3. Click Apply to save the configuration.
4. If you want to cancel the setting, then you need to click the Reset button. It will revert to previously saved values.



QoS Global Settings

Trust Mode
● CoS/802.1p
○ DSCP
○ IP Precedence
○ CoS/802.1p-DSCP

FIGURE 6-1. QOS GLOBAL SETTINGS

PARAMETER DESCRIPTION

Trust Mode

- CoS/802.1p: Traffic is mapped to queues based on the VPT field in the VLAN tag, or based on the per-port default CoS/802.1p value (if there is no VLAN tag on the incoming packet). The actual mapping of the VPT to queue can be configured on the CoS/802.1p to Queue page.
- DSCP: All IP traffic is mapped to queues based on the DSCP field in the IP header. The actual mapping of the DSCP to queue can be configured on the DSCP to Queue page. If traffic is not IP traffic, it is mapped to the best effort queue.
- IP Precedence: Traffic is mapped to queues based on the IP precedence. The actual mapping of the IP precedence to queue can be configured on the IP Precedence to Queue page.
- CoS/802.1p-DSCP: Uses the trust CoS mode for non-IP traffic and trust DSCP mode for IP traffic.

Buttons

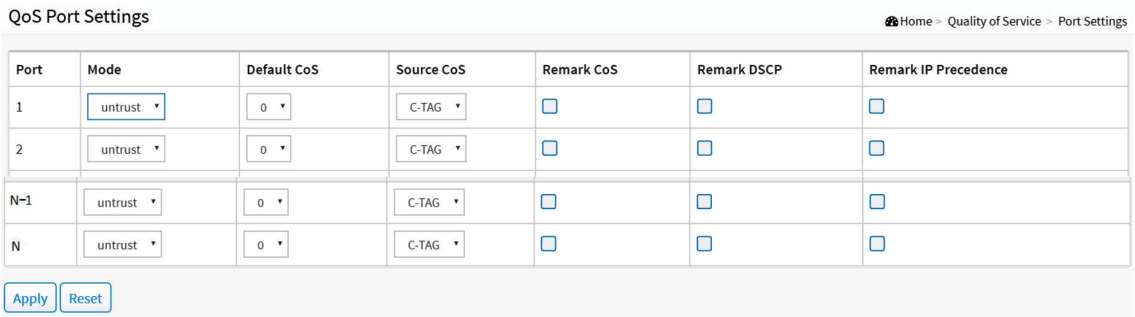
- Apply: Click to save changes.
- Reset: Click to undo any changes made locally and revert to previously saved values.

6.2 PORT SETTINGS

WEB INTERFACE

To configure the QoS Port Setting in the web interface:

1. Click Quality of Service and Port Settings.
2. Select Mode, Default CoS, Source CoS, Remark CoS to each port.
3. Click the port to enable the Remark Cos, Remark DSCP, Remark IP Precedence.
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	Mode	Default CoS	Source CoS	Remark CoS	Remark DSCP	Remark IP Precedence
1	untrust	0	C-TAG	□	□	□
2	untrust	0	C-TAG	□	□	□
N−1	untrust	0	C-TAG	□	□	□
N	untrust	0	C-TAG	□	□	□

FIGURE 6-2. QOS PORT SETTINGS

PARAMETER DESCRIPTION

- Port: The logical port for the settings contained in the same row.
- Mode:

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

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

- Default CoS: Select the default CoS value to be assigned for incoming untagged packets. The range is 0 to 7.
- Source CoS: The CoS value is determined based on C-Tag or S-Tag for incoming tagged packets
- Remark CoS: Click the checkbox to remark the CoS/802.1p priority for egress traffic on this port.
- Remark DSCP: Click the checkbox to remark the DSCP value for egress traffic on this port.
- Remark IP Precedence: Click the checkbox to remark the IP precedence for egress traffic on this port.

NOTE: The CoS/802.1p priority and IP Precedence, or the CoS/802.1p priority and DSCP value can be remarked simultaneously for egress traffic on a port, but the DSCP value and IP Precedence cannot be remarked simultaneously.

Buttons

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

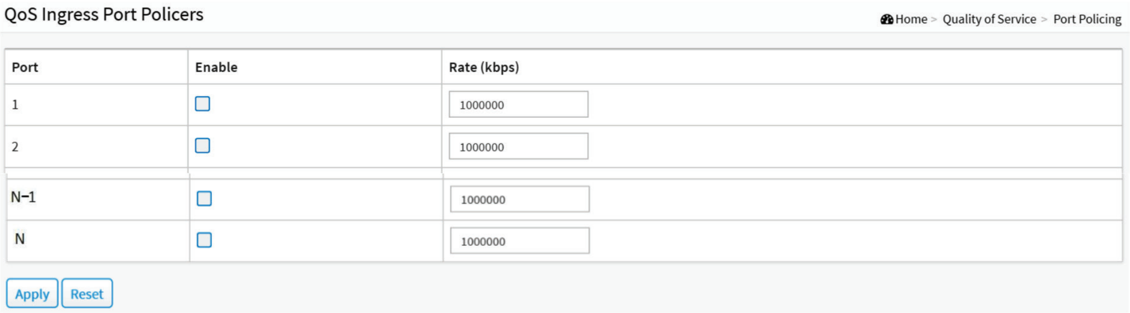
6.3 PORT POLICING

This section provides an overview of QoS Ingress Port Policers for all switch ports 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 Policing.
2. Click the port need to enable the QoS Ingress Port Policers, and configure the Rate limit condition.
3. Click Apply to save the configuration.
4. If you want to cancel the setting, click the Reset button. It will revert to previously saved values.



QoS Ingress Port Policers

Port	Enable	Rate (kbps)
1	□	1000000
2	□	1000000
N-1	□	1000000
N	□	1000000

FIGURE 6-3. QOS INGRESS PORT POLICERS CONFIGURATION

PARAMETER DESCRIPTION

- Port: The logical port for the settings contained in the same row. Click on the port number to configure the schedulers.
- Enabled: Enable the QoS Ingress Port Policers function for a port.
- Rate: Set the Rate limit value for this port, the default is 1000000.

Buttons

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

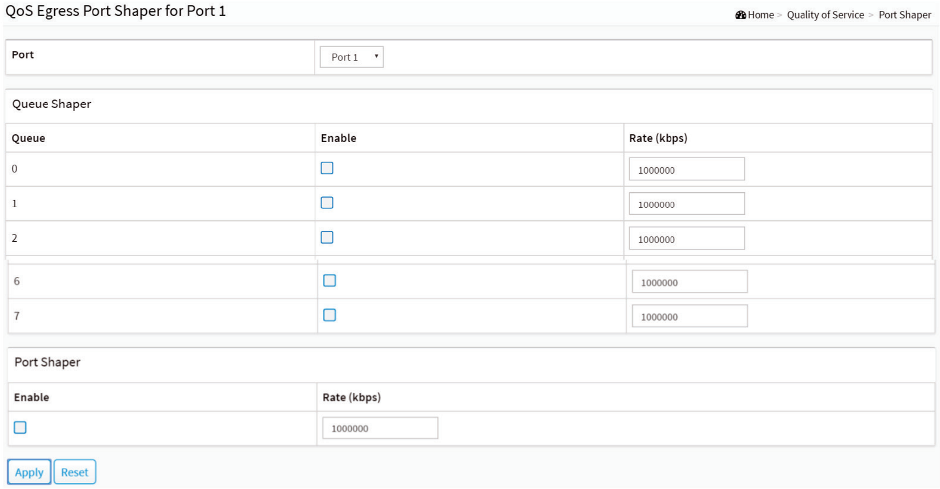
6.4 PORT SHAPER

This section provides an overview of QoS Egress Port Shapers for all switch ports. Users can get detailed information for the ports that belong to the currently selected stack unit.

WEB INTERFACE

To configure the QoS Port Shapers in the web interface:

1. Click Quality of Service and Port Shaper.
2. Select the port to configure QoS Egress Port Shaper.
3. Click the port to enable, and configure the Rate limit condition.
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.



QoS Egress Port Shaper for Port 1

Port	Port 1

Queue Shaper

Queue	Enable	Rate (kbps)
0	□	1000000
1	□	1000000
2	□	1000000
6	□	1000000
7	□	1000000

Port Shaper

Enable	Rate (kbps)
□	1000000

FIGURE 6-4. QOS EGRESS PORT SHAPER

PARAMETER DESCRIPTION

- Port: The logical port for the settings contained in the same row. Click on the port number i to configure the shapers.

Queue Shaper

- Queue: The queue number of the queue shaper on this switch port.
- Enable: Controls whether the queue shaper is enabled for this queue on this switch port.
- Rate(kbps): Controls the rate for the queue shaper. The default value is 1000000.

Port Shaper

- Enable: Controls whether the port shaper is enabled for this switch port.
- Rate(kbps): Controls the rate for the port shaper. The default value is 1000000.

Buttons

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

6.5 STORM CONTROL

This section shows users how 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

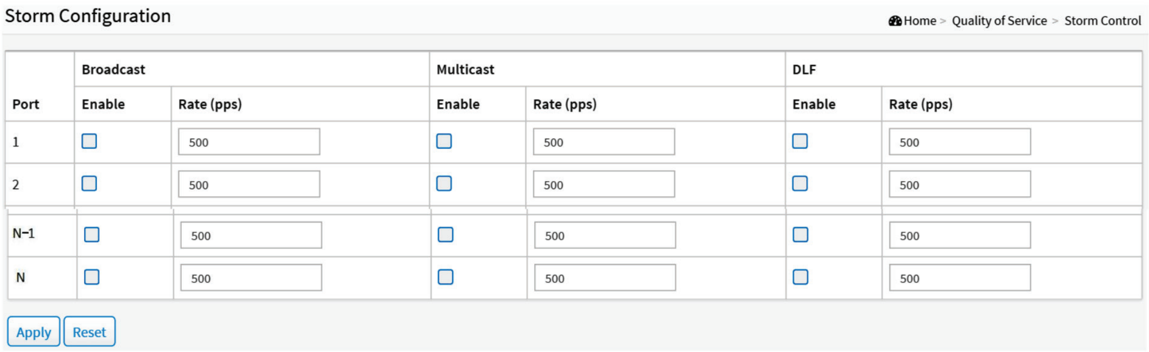
To configure the Storm Control Configuration parameters in the web interface:

1. Click Quality of Service and Storm Control.

2. Click which port need to enable, and configure the Rate limit condition.

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.



Storm Configuration

	Broadcast		Multicast		DLF	
Port	Enable	Rate (pps)	Enable	Rate (pps)	Enable	Rate (pps)
1	□	500	□	500	□	500
2	□	500	□	500	□	500
N-1	□	500	□	500	□	500
N	□	500	□	500	□	500

FIGURE 6-5. STORM CONTROL CONFIGURATION

PARAMETER DESCRIPTION

- Port: The logical port for the settings contained in the same row. Click on the port number to configure the storm control.
- Frame Type: The settings in a particular row apply to the frame type listed here: Broadcast, Multicast or DLF (destination lookup failure).
- Enable: Enable or disable the storm control status for the given frame type.
- Rate: The rate unit is packets per second (pps). Valid values are: 0–262143 (pps). The 1 kpps is actually 1002.1 pps.

Buttons

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

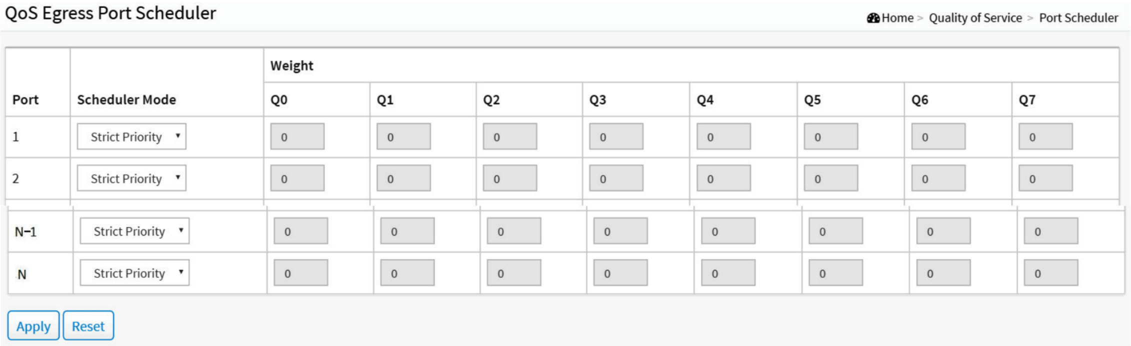
6.6 PORT SCHEDULER

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. Select Scheduler Mode for each port.
3. If you select WRR or WFQ, you can configure weight.
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.



QoS Egress Port Scheduler

		Weight							
Port	Scheduler Mode	Q0	Q1	Q2	Q3	Q4	Q5	Q6	Q7
1	Strict Priority	0	0	0	0	0	0	0	0
2	Strict Priority	0	0	0	0	0	0	0	0
N-1	Strict Priority	0	0	0	0	0	0	0	0
N	Strict Priority	0	0	0	0	0	0	0	0

FIGURE 6-6. QOS EGRESS PORT SCHEDULES

PARAMETER DESCRIPTION

- Port: The logical port for the settings contained in the same row.
- Scheduler Mode: Controls whether the scheduler mode is “Strict Priority”, “WRR” or “WFQ” on this switch port.
- Weight: Controls the weight for this queue. The default value is “0”. This value is restricted to 0-127. This parameter is only shown if “Scheduler Mode” is set to “Weighted”.

Buttons

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

6.7 COS/802.1P MAPPING

Use the CoS/802.1p to Queue page to map 802.1p priorities to egress queues. The CoS/802.1p to Queue table determines the egress queues of the incoming packets based on the 802.1p priority in their VLAN tags. For incoming untagged packets, the 802.1p priority will be the default CoS/802.1p priority assigned to the ingress ports.

WEB INTERFACE

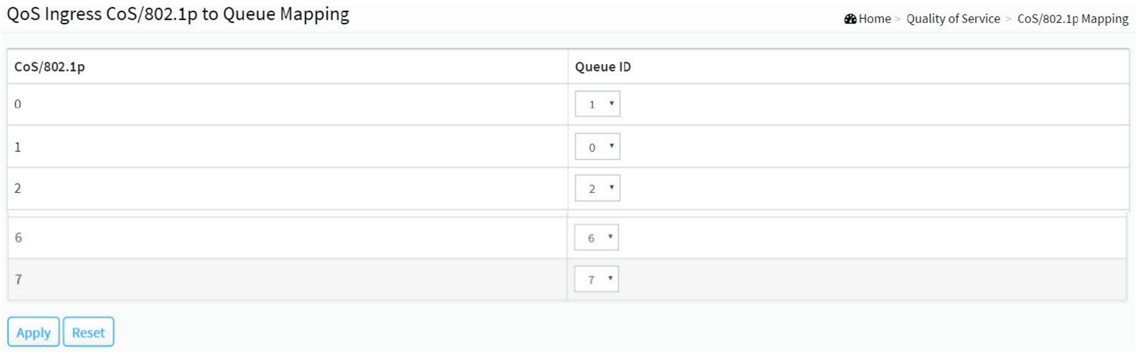
To configure the Cos/802.1p Mapping in the web interface:

1. Click Quality of Service and Cos/802.1p Mapping.

2. Select Queue ID.

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.



QoS Ingress CoS/802.1p to Queue Mapping

CoS/802.1p	Queue ID
0	1
1	0
2	2
6	6
7	7

FIGURE 6-7. QOS INGRESS COS/802.1P TO QUEUE MAPPING

PARAMETER DESCRIPTION

- CoS/802.1p: Displays the 802.1p priority tag values to be assigned to an egress queue, where 0 is the lowest and 7 is the highest priority.
- Queue ID: Select the egress queue to which the 802.1p priority is mapped. Eight egress queues are supported, where Queue 7 is the highest priority egress queue and Queue 0 is the lowest priority egress queue.

Buttons

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

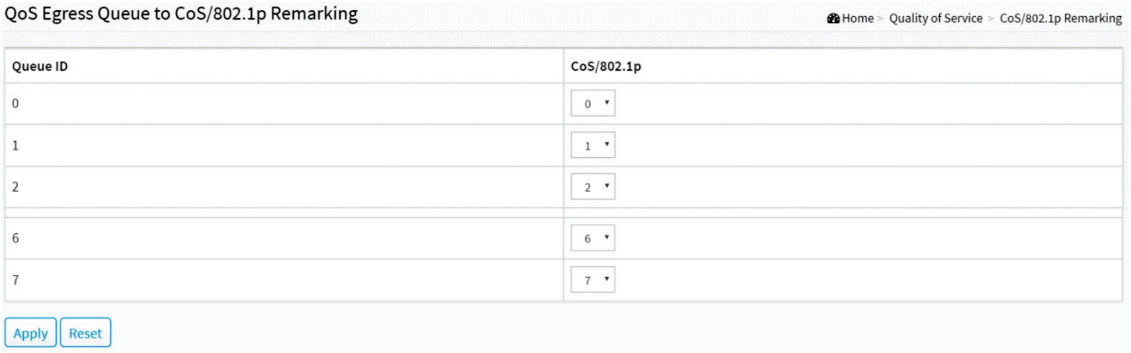
6.8 COS/802.1P REMARKING

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

WEB INTERFACE

To configure the Cos/802.1p Remarking in the web interface:

1. Click Quality of Service and Cos/802.1p Remarking.
2. Select CoS/802.1p.
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.



QoS Egress Queue to CoS/802.1p Remarking

Queue ID	CoS/802.1p
0	0
1	1
2	2
6	6
7	7

FIGURE 6-8. QOS EGRESS QUEUE TO COS/802.1P REMARKING

PARAMETER DESCRIPTION

- Queue ID: Displays the Queue ID, where Queue 7 is the highest priority egress queue and Queue 0 is the lowest priority egress queue.
- CoS/802.1p: For each output queue, select the CoS/802.1p priority to which egress traffic from the queue is remarked.

Buttons

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

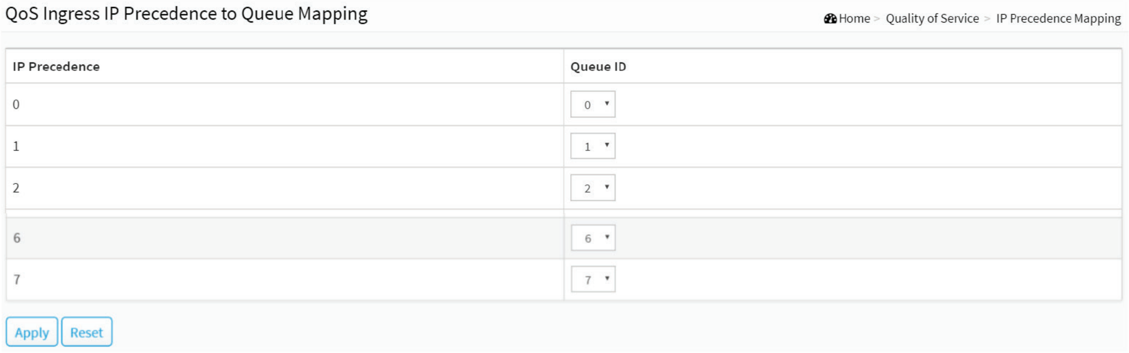
6.9 IP PRECEDENCE MAPPING

This section explains how to map IP precedence to an egress queue.

WEB INTERFACE

To configure the IP Precedence Mapping in the web interface:

1. Click Quality of Service and IP Precedence Mapping.
2. Select Queue ID.
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.



QoS Ingress IP Precedence to Queue Mapping

IP Precedence	Queue ID
0	0
1	1
2	2
6	6
7	7

FIGURE 6-9. QOS INRESS IP PRECEDENCE TO QUEUE MAPPING

PARAMETER DESCRIPTION

- IP Precedence: Displays the IP Precedence priority tag values to be assigned to an egress queue, where 0 is the lowest and 7 is the highest priority.
- Queue ID: Select the egress queue to which the IP precedence priority is mapped. Eight egress queues are supported, where Queue 7 is the highest priority egress queue and Queue 0 is the lowest priority egress queue.

Buttons

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

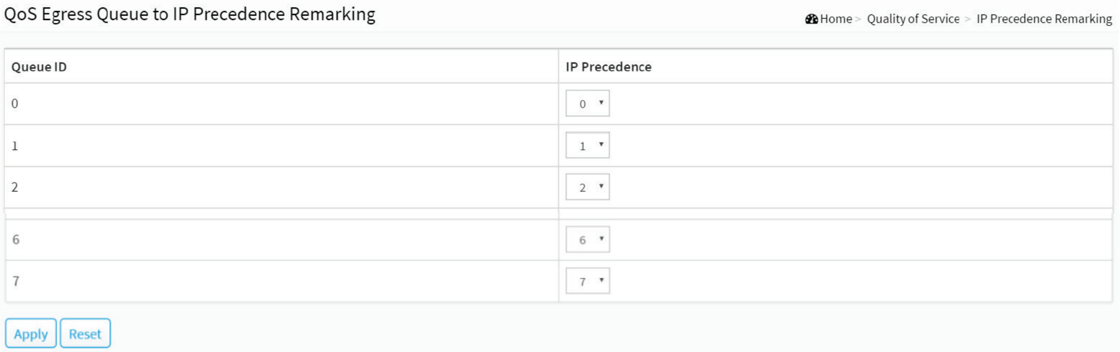
6.10 IP PRECEDENCE REMARKING

This section explains how to map an egress queue to IP precedence.

WEB INTERFACE

To configure the IP Precedence Remarking in the web interface:

1. Click Quality of Service and IP Precedence Remarking.
2. Select IP Precedence.
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.



QoS Egress Queue to IP Precedence Remarking

Queue ID	IP Precedence
0	0
1	1
2	2
6	6
7	7

FIGURE 6-10. QOS ERESS QUEUE TO IP PRECEDENCE REMARKING

PARAMETER DESCRIPTION

- Queue ID: Displays the Queue ID, where Queue 7 is the highest priority egress queue and Queue 0 is the lowest priority egress queue.
- IP Precedence: For each output queue, select the IP Precedence priority to which egress traffic from the queue is remarked.

Buttons

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

6.11 DSCP MAPPING

Use the DSCP to Queue page to map IP DSCP to egress queues. The DSCP to Queue table determines the egress queues of the incoming IP packets based on their DSCP values. The original VLAN Priority Tag (VPT) of the packet is unchanged.

It is possible to achieve the desired QoS in a network by simply changing the DSCP to Queue mapping, the queue schedule method, and bandwidth allocation.

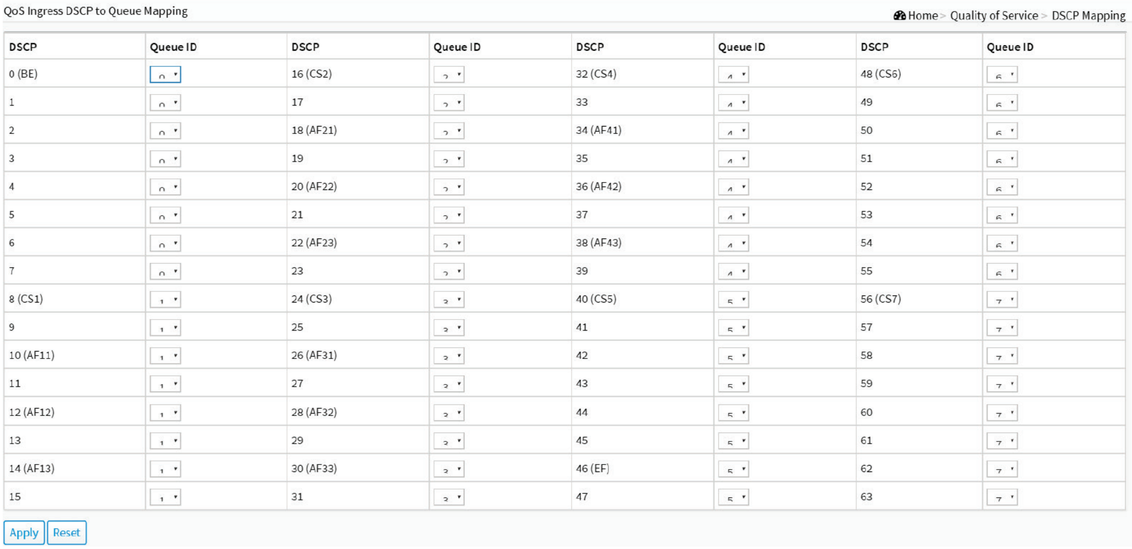
WEB INTERFACE

To configure the DSCP Mapping in the web interface:

1. Click Quality of Service and DSCP Mapping.
2. Select Queue ID.

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.



QoS Ingress DSCP to Queue Mapping

DSCP	Queue ID	DSCP	Queue ID	DSCP	Queue ID	DSCP	Queue ID
0 (BE)	0	16 (CS2)	2	32 (CS4)	4	48 (CS6)	6
1	0	17	2	33	4	49	6
2	0	18 (AF21)	2	34 (AF41)	4	50	6
3	0	19	2	35	4	51	6
4	0	20 (AF22)	2	36 (AF42)	4	52	6
5	0	21	2	37	4	53	6
6	0	22 (AF23)	2	38 (AF43)	4	54	6
7	0	23	2	39	4	55	6
8 (CS1)	1	24 (CS3)	3	40 (CS5)	5	56 (CS7)	7
9	1	25	3	41	5	57	7
10 (AF11)	1	26 (AF31)	3	42	5	58	7
11	1	27	3	43	5	59	7
12 (AF12)	1	28 (AF32)	3	44	5	60	7
13	1	29	3	45	5	61	7
14 (AF13)	1	30 (AF33)	3	46 (EF)	5	62	7
15	1	31	3	47	5	63	7

FIGURE 6-11. QOS INRESS DSCP TO QUEUE MAPPING

PARAMETER DESCRIPTION

- DSCP: Displays the DSCP value in the incoming packet and its associated class.
- Queue ID: Select the traffic forwarding queue from the Output Queue drop-down menu to which the DSCP value is mapped.

Buttons

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

6.12 DSCP REMARKING

Use the Queues to DSCP page to remark DSCP value for egress traffic from each queue.

WEB INTERFACE

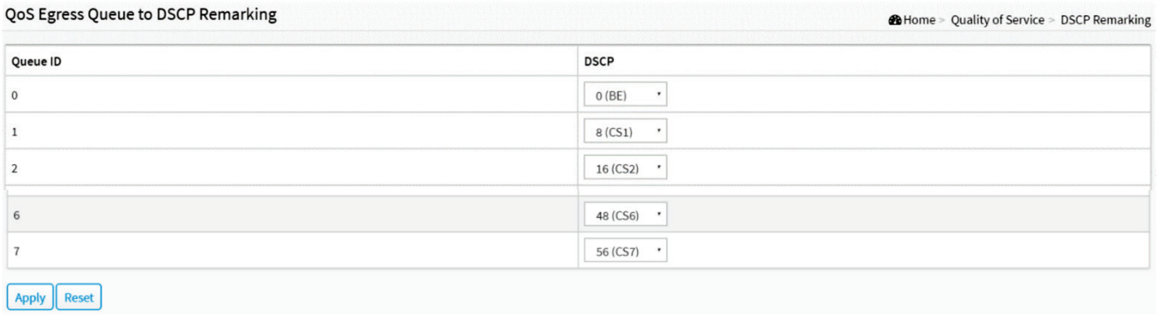
To configure the DSCP Remarking in the web interface:

1. Click Quality of Service and DSCP Remarking.

2. Select DSCP.

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.



QoS Egress Queue to DSCP Remarking

Queue ID	DSCP
0	0 (BE)
1	8 (CS1)
2	16 (CS2)
6	48 (CS6)
7	56 (CS7)

FIGURE 6-12. QOS ERESS QUEUE TO DSCP REMARKING

PARAMETER DESCRIPTION

- Queue ID: Displays the Queue ID, where Queue 7 is the highest priority egress queue and Queue 0 is the lowest priority egress queue.
- DSCP: For each output queue, select the DSCP priority to which egress traffic from the queue is remarked.

Buttons

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

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 that automatically take over when a primary link goes down.

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

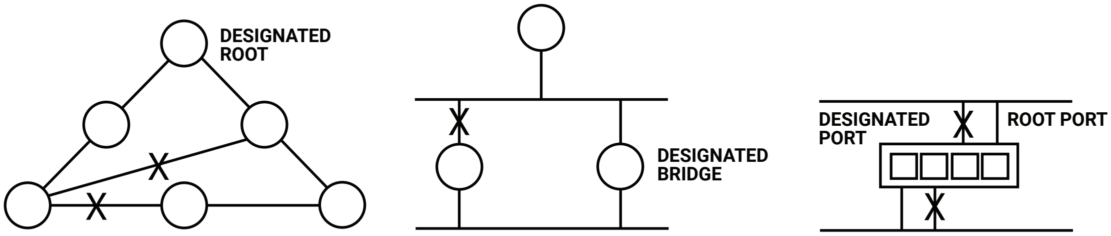


FIGURE 7-1. SPANNING TREE PROTOCOL

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.

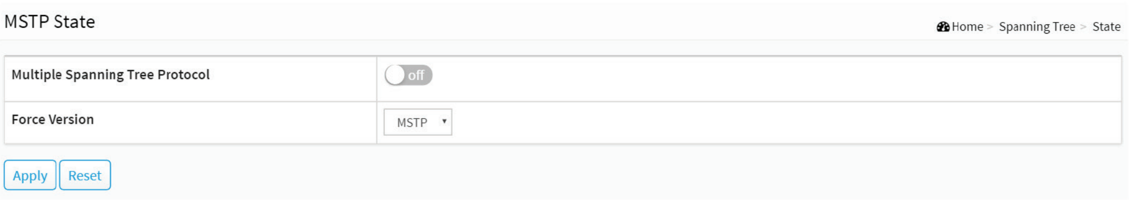
7.1 STATE

This section describes how to select enable spanning tree protocol or not, and how to select the protocol version you want.

WEB INTERFACE

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

1. Click Spanning Tree and state.
2. Enable or disable the Spanning Tree Protocol.
3. Select the Spanning Tree Protocol version.
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.



MSTP State

Multiple Spanning Tree Protocol	off
Force Version	MSTP

FIGURE 7-2. SPANNING TREE STATE

PARAMETER DESCRIPTION

- Multiple Spanning Tree Protocol: You can select whether to enable spanning tree protocol or not.
- Force Version: The STP protocol version setting. Valid values are STP, RSTP and MSTP.

Buttons

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

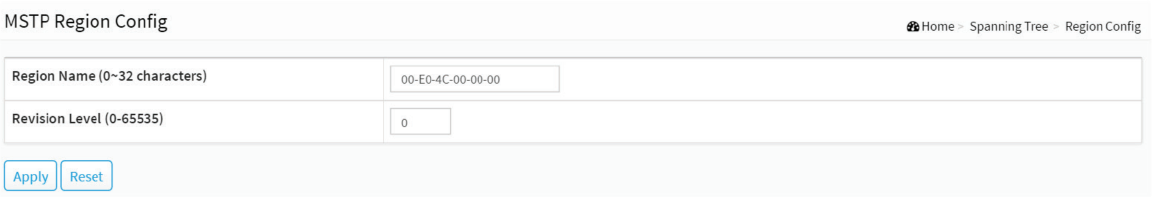
7.2 REGION CONFIG

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

WEB INTERFACE

To configure the Region Config in the web interface:

1. Click Spanning Tree and Region Config.
2. Specify the Region Name and Revision Level.
3. Click Apply to save the setting.
4. If you want to cancel the setting, then you need to click the Reset button. It will revert to previously saved values.



MSTP Region Config

Region Name (0~32 characters)	00-E0-4C-00-00-00
Revision Level (0-65535)	0

FIGURE 7-3. REGION CONFIGURATION

PARAMETER DESCRIIPTION

- Configuration Name: The name identifying the VLAN to MSTI mapping. Bridges must share the name and revision, as well as the VLAN-to-MSTI mapping configuration in order to share spanning trees for 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.

Buttons

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

7.3 INSTANCE VIEW

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

WEB INTERFACE

To configure the MSTP Instance in the web interface:

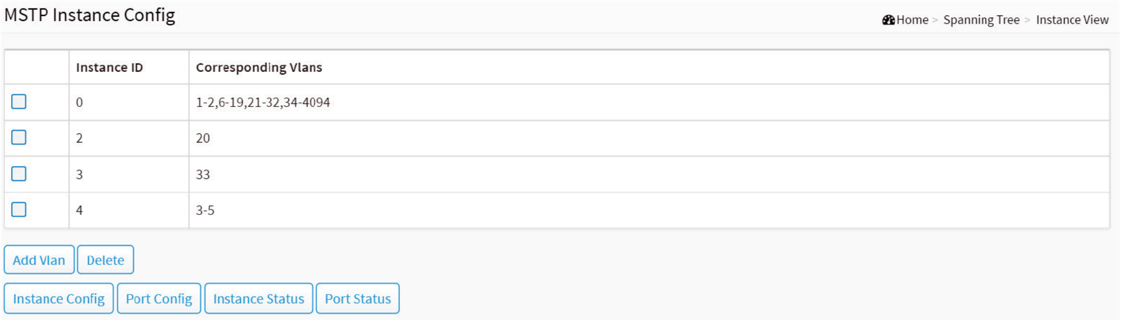
1. Click Spanning Tree and Instance.

2. Click to add vlan.

3. Specify the Instance and Port.

4. Click Instance Status and Port Status to see the details.

5. If you want to cancel the setting, then you need to click Delete.



MSTP Instance Config

	Instance ID	Corresponding Vlans
□	0	1-2,6-19,21-32,34-4094
□	2	20
□	3	33
□	4	3-5

FIGURE 7-4. MSTP INSTANCE CONFIG

PARAMETER DESCRIPTION

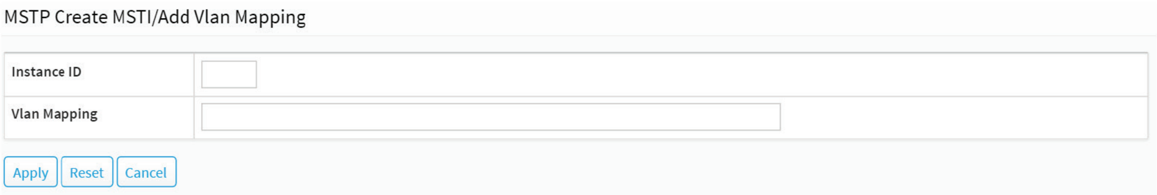
- Instance ID: Every spanning tree instance needs to have a unique instance ID within 0–4094. Instance 0 (CIST) always exists and can not be deleted. Additional spanning instances (MSTIs) can be added or deleted. At least one vlan must be provisioned for an MSTI to declare the need for the MSTI to exist.
- Corresponding Vlans: 1-4094. Multiple vlans can belong to an MSTI. All vlans that are not provisioned through this will be automatically assigned to Instance 0(CIST).

Buttons

- Add Vlan: Add an MSTI and provide its vlan members or modify vlan members for a specific MSTI, you can add up to 63 for a total of 64.
- Delete: Delete an MSTI.
- Instance Config: Provision spanning tree performance parameters per instance.
- Port Config: Provision spanning tree performance parameters per instance per port.
- Instance Status: Show the status report of a particular spanning tree instance.
- Port Status: Show the status report of all ports regarding a specific spanning tree instance.

Please refer to the following introduction:

Add Vlan:



MSTP Create MSTI/Add Vlan Mapping

Instance ID	
Vlan Mapping	

FIGURE 7-5. ADD VLAN

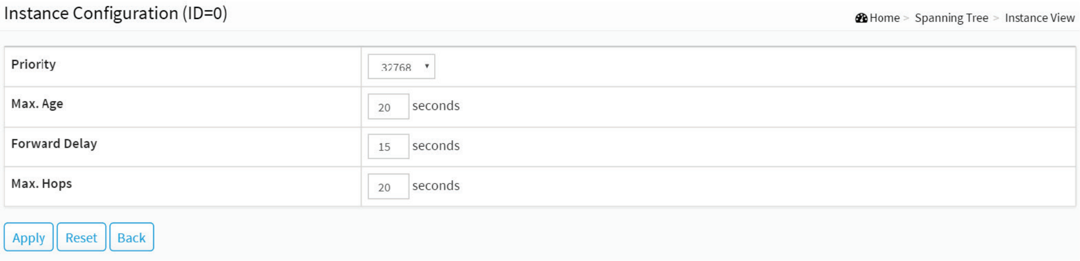
PARAMETER DESCRIIPTION

- Instance ID: The Range is 1-4094.
- Vlan Mapping: 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 have any VLANs mapped to it.) Example: 2,5,20-40.

Buttons

- Apply: Click to save changes.
- Reset: Click to undo any changes made locally and revert to previously saved values.
- Cancel: Click to undo any changes made locally and return to the Users.

Instance Config to Instance 0:



Instance Configuration (ID=0)

Priority	32768
Max. Age	20 seconds
Forward Delay	15 seconds
Max. Hops	20 seconds

FIGURE 7-6. INSTANCE CONFIG TO INSTANCE 0

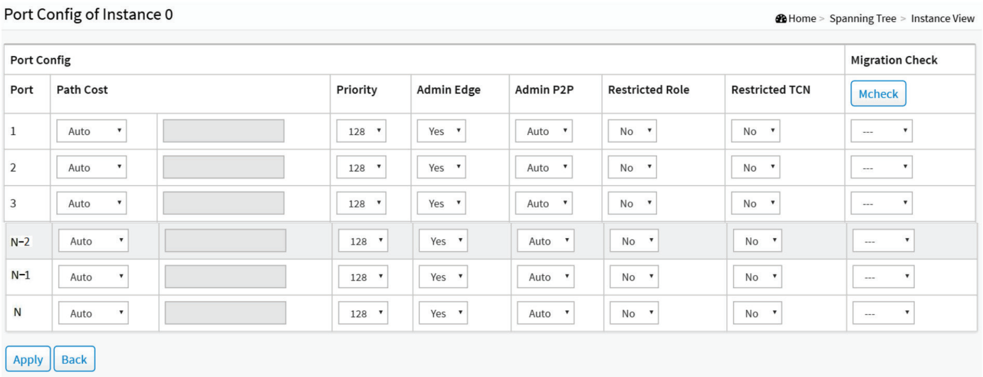
PARAMETER DESCRIPTION

- Priority: The priority parameter used in the CIST (Common and Internal Spanning Tree) connection.
  0/4096/8192/12288/16384/20480/24576/28672/32768/36864/40960/45056/49152/53248/57344/61440
- MAX. Age: 6-40 sec. The same definition as in the RSTP protocol.
- Forward Delay: 4-30 sec. The same definition as in the RSTP protocol.
- MAX. Hops: 6-40 sec. This is a new parameter for the multiple spanning tree protocol. It is used in the internal spanning tree instances. "CIST Remaining Hops" or "MSTI Remaining Hops" in the Spanning tree protocol message would decrease by one when the message is propagated to the neighboring bridge. If the Remaining Hops in a message is zero, the message (BPDU) would be regarded as invalid. Max Hops is used to specify the initial value of the Remaining Hops for Regional Root Bridge (Either CIST Regional Root or MSTI Regional Root).

Buttons

- Apply: Click to save changes.
- Reset: Click to undo any changes made locally and revert to previously saved values.
- Back: Click to undo any changes made locally and return to the Users.

Port Config to Instance 0:



Port Config of Instance 0

Port Config								Migration Check
Port	Path Cost		Priority	Admin Edge	Admin P2P	Restricted Role	Restricted TCN	Mcheck
1	Auto		128	Yes	Auto	No	No	---
2	Auto		128	Yes	Auto	No	No	---
3	Auto		128	Yes	Auto	No	No	---
N-2	Auto		128	Yes	Auto	No	No	---
N-1	Auto		128	Yes	Auto	No	No	---
N	Auto		128	Yes	Auto	No	No	---

FIGURE 7-7. PORT CONFIG TO INSTANCE 0

PARAMETER DESCRIPTION

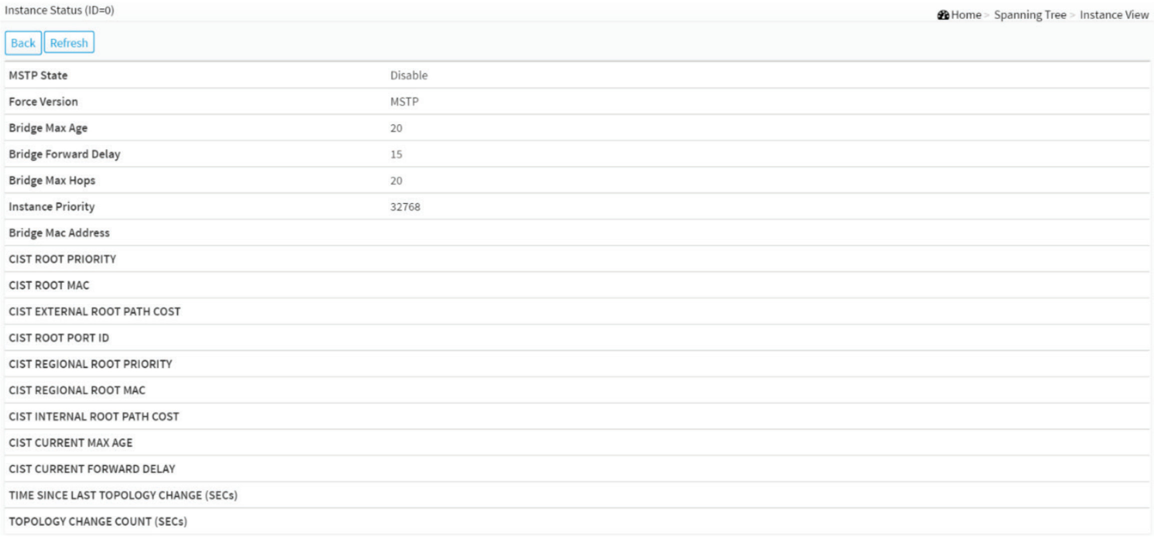
- Port: The logical port for the settings contained in the same row.
- Path Cost: 1–200,000,000: The same definition as in the RSTP specification. But in MSTP, this parameter can be respectively applied to ports of CIST and ports of any MSTI.
- Priority: 0/16/32/48/64/80/96/112/128/144/160/176/192/208/224/240: The same definition as in the RSTP specification. But in MSTP, this parameter can be respectively applied to ports of CIST and ports of any MSTI.
- Admin Edge: Yes/No: The same definition as in the RSTP specification for the CIST ports.
- Admin P2P: Auto/True/False: The same definition as in the RSTP specification for the CIST ports.
- Restricted Role: Yes/No: If "Yes" 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. This parameter is "No" by default. If set, it can cause lack of spanning tree connectivity. It is set by a network administrator to prevent bridges external to a core region of the network from influencing the spanning tree active topology, possibly because those bridges are not under the full control of the administrator.

- Restricted TCN: Yes/No: "Yes" causes the Port not to propagate received topology change notifications and topology changes to other Ports. This parameter is "No" by default. If set it can cause temporary loss of connectivity after changes in a spanning tree's active topology as a result of persistent incorrectly 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 the the network from influencing the spanning tree active topology, possibly because those bridges are not under the full control of the administrator. Or the status of MAC operation for the attached LANs transitions frequently.
- Mcheck: The same definition as in the RSTP specification for the CIST ports.

Buttons

- Apply: Click to save changes.
- Back: Click to undo any changes made locally and return to the Users.

Instance Status to Instance 0:



Instance Status (ID=0)

MSTP State	Disable
Force Version	MSTP
Bridge Max Age	20
Bridge Forward Delay	15
Bridge Max Hops	20
Instance Priority	32768
Bridge Mac Address	
CIST ROOT PRIORITY	
CIST ROOT MAC	
CIST EXTERNAL ROOT PATH COST	
CIST ROOT PORT ID	
CIST REGIONAL ROOT PRIORITY	
CIST REGIONAL ROOT MAC	
CIST INTERNAL ROOT PATH COST	
CIST CURRENT MAX AGE	
CIST CURRENT FORWARD DELAY	
TIME SINCE LAST TOPOLOGY CHANGE (SECs)	
TOPOLOGY CHANGE COUNT (SECs)	

FIGURE 7-8. INSTANCE STATUS TO INSTANCE 0

PARAMETER DESCRIPTION

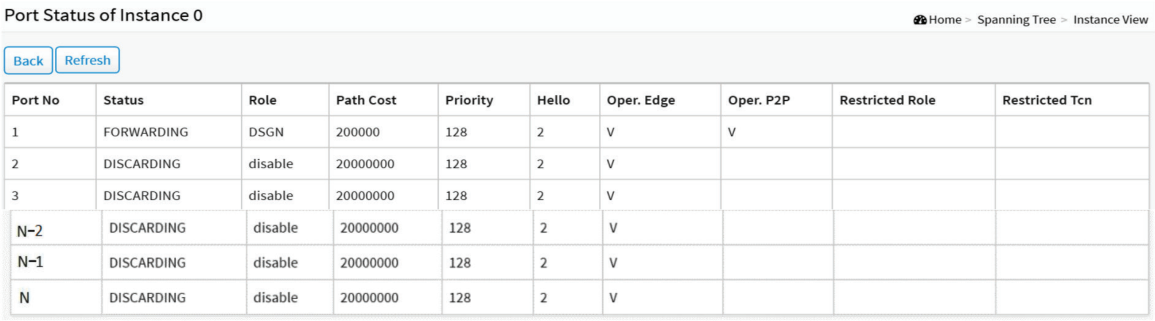
- MSTP State: MSTP protocol is Enable or Disable.
- Force Version: This shows the current spanning tree protocol version configured.
- Bridge Max Age: This shows the Max Age setting of the bridge itself.
- Bridge Forward Delay: This shows the Forward Delay setting of the bridge itself.
- Bridge Max Hops: This shows the Max Hops setting of the bridge itself.
- Instance Priority: Spanning tree priority value for a specific tree instance(CIST or MSTI).
- Bridge Mac Address: The Mac Address of the bridge itself.
- CIST ROOT PRIORITY: Spanning tree priority value of the CIST root bridge.
- CIST ROOT MAC: Mac Address of the CIST root bridge.
- CIST EXTERNAL ROOT PATH COST: Root path cost value from the point of view of the bridge's MST region.

- CIST ROOT PORT ID: The port ID of the bridge's root port. In MSTP, a peer port of a root port may reside in a different MST region or in the same MST region. The first case indicates that the root port's owner is the CIST regional root bridge.
- CIST REGIONAL ROOT PRIORITY: Spanning tree priority value of the CIST regional root bridge. Note that CIST Regional Root bridge is different from CIST Root bridge. One exception is that when a bridge belonging to an MST region happens to be the root bridge of the CST (Common Spanning Tree). An MST Region in the CST can be regarded as a common RSTP bridge. The IST (Internal Spanning Tree) and MSTIs are transparent to bridges outside this region.
- CIST REGIONAL ROOT MAC: Mac Address of the CIST regional root bridge.
- CIST INTERNAL ROOT PATH COST: Root path cost value from the point of view of the bridges inside the IST.
- CIST CURRENT MAX AGE: Max Age of the CIST Root bridge.
- CIST CURRENT FORWARD DELAY: Forward Delay of the CIST Root bridge.
- TIME SINCE LAST TOPOLOGY CHANGE(SECs): Time Since Last Topology Change is the elapsed time in unit of seconds for a bunch of "Topology Change and (or) Topology Change Notification receiving" to occur. When a new series of Topology Changes occur again, this counter will be reset to 0.
- TOPOLOGY CHANGE COUNT(SECs): The per spanning tree instance Topology Change Count expresses the time spent in unit of seconds since the beginning of the Spanning Tree Topology Change to the end of the STP convergence. Once there is no topology change occurring and no more topology change notification received, the Topology Change count will be reset to 0.

Buttons

- Back: Click to undo any changes made locally and return to the Users.
- Refresh: Click to refresh the page.

Port Status to Instance 0:



Port Status of Instance 0

Port No	Status	Role	Path Cost	Priority	Hello	Oper. Edge	Oper. P2P	Restricted Role	Restricted Tcn
1	FORWARDING	DSGN	200000	128	2	V	V		
2	DISCARDING	disable	20000000	128	2	V			
3	DISCARDING	disable	20000000	128	2	V			
N-2	DISCARDING	disable	20000000	128	2	V			
N-1	DISCARDING	disable	20000000	128	2	V			
N	DISCARDING	disable	20000000	128	2	V			

FIGURE 7-9. PORT STATE TO INSTANCE 0

PARAMETER DESCRIPTION

- Port No: The port number to which the configuration applies.
- Status: The forwarding status. Same definition as of the RSTP specification. Possible values are "FORWARDING" , "LEARNING" , "DISCARDING"
- Role: The role that a port plays in the spanning tree topology. Possible values are "disable" (disable port) , "alternate" (alternate port) , "backup" (backup port) , "ROOT" (root port) , "DSGN" (designated port) , "MSTR" (master port). The last 3 are possible port roles for a port to transit to FORWARDING state.
- Path Cost: Display the currently resolved port path cost value for each port in a particular spanning tree instance.
- Priority: Display the port priority value for each port in a particular spanning tree instance.
- Hello: Per port Hello Time display. It takes the following form: Current Hello Time/Hello Time Setting

- Oper. Edge: Whether or not a port is an Edge Port in reality.
- Oper. P2P: Whether or not a port is a Point-to-Point Port in reality.
- Restricted Role: Same as mentioned in “Port Config”
- Restricted Tcn: Same as mentioned in “Port Config”

Buttons

- Back: Click to undo any changes made locally and return to the Users.
- Refresh: Click to refresh the page.

8.1 CONFIGURATION

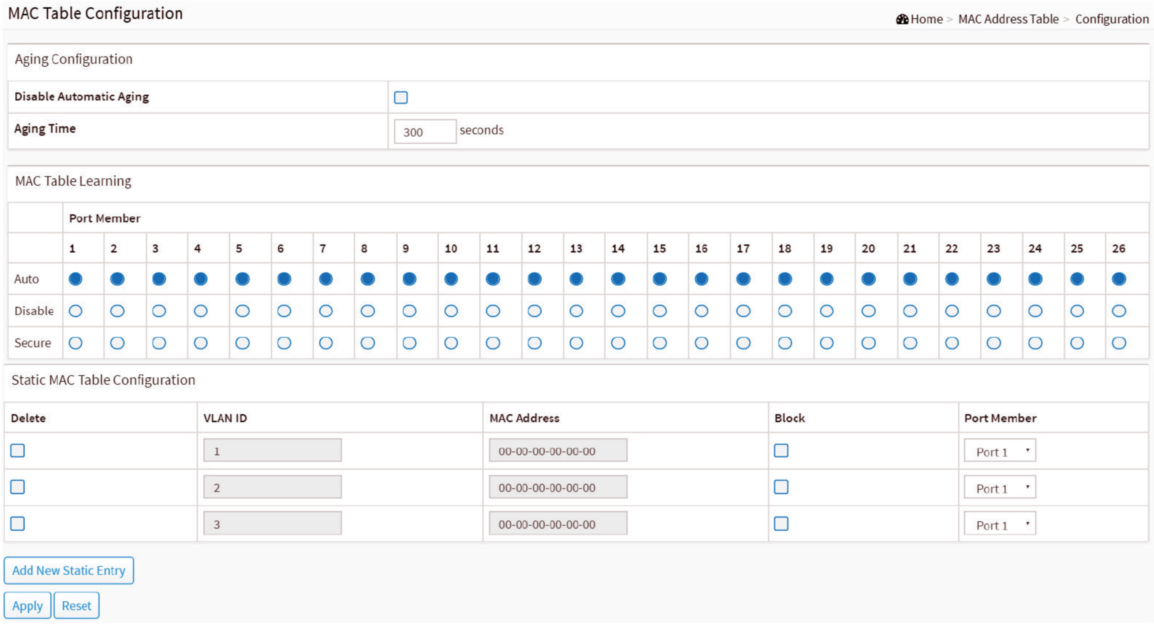
Switching of frames is based upon the DMAC address contained in the frame. The switch builds up a table that maps MAC addresses to switch ports for knowing which ports the frames should go to (based upon the DMAC address in the frame). This table contains both static and dynamic entries. The static entries 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) that shows the MAC address of the equipment sending the frame. The SMAC address is used by the switch to automatically update the MAC table with these dynamic MAC addresses. Dynamic entries are removed from the MAC table if no 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. Add new Static entry, Specify the VLAN IP and Mac address, Port Members, Block.
5. Click Apply.



MAC Table Configuration

Aging Configuration

Disable Automatic Aging	□
Aging Time	300 seconds

MAC Table Learning

	Port Member																									
	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
Auto	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●
Disable	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○
Secure	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○

Static MAC Table Configuration

Delete	VLAN ID	MAC Address	Block	Port Member
□	1	00-00-00-00-00-00	□	Port 1
□	2	00-00-00-00-00-00	□	Port 1
□	3	00-00-00-00-00-00	□	Port 1

FIGURE 8-1. MAC 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 the box next to Disable automatic aging.

- MAC Table Learning: If the learning mode for a given port is grayed out, another module is in control of the mode, so 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.
- Learning: Learning is done automatically as soon as a frame with unknown SMAC is received.
- Disable: No learning is done.
- Secure: Only static MAC entries are learned, all other frames are dropped.

NOTE: Make sure that the link used for managing the switch is added to the Static Mac Table before changing to secure learning mode, otherwise the management link is lost and can only be restored by using another non-secure port or by connecting to the switch via the serial interface.

Static MAC Table Configuration

The static entries in the MAC table are shown in this table. The static MAC table can contain 128 entries. The maximum of 128 entries is for the whole stack, and not per switch.

- Delete: Check to delete the entry. It will be deleted during the next save.
- VLAN ID: The VLAN ID of the entry.
- MAC Address: The MAC address of the entry.
- Block: Click Block if you want block this mac address.
- Port Members: Checkmarks indicate which ports are members of the entry. Check or uncheck as needed to modify the entry.

Buttons

- Adding a New Static Entry: Click to add a new entry to the static MAC table. Specify the VLAN ID, MAC address, and port members for the new entry. Click “Apply”.
- Apply: Click to save changes.
- Reset: Click to undo any changes made locally and revert to previously saved values.

8.2 INFORMATION

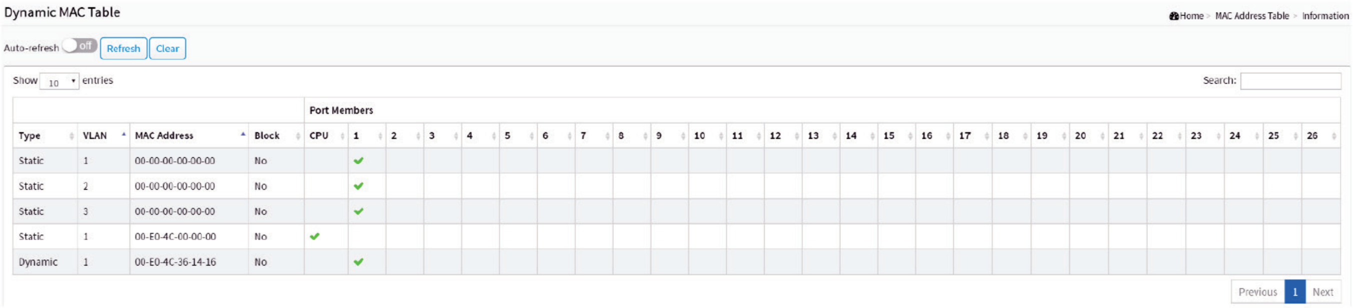
Entries in the MAC Table are shown on this page. The MAC Table contains up to 8192 entries, and is sorted first by VLAN ID, then by MAC address.

WEB INTERFACE

To Display MAC Address Table in the web interface:

1. Click MAC Address Table and Information.
2. Display MAC Address Table.

CHAPTER 8: MAC ADDRESS TABLES



Dynamic MAC Table

Home > MAC Address Table > Information

Auto-refresh off Refresh Clear

Show 10 entries

Search:

				Port Members																										
Type	VLAN	MAC Address	Block	CPU	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
Static	1	00-00-00-00-00-00	No		✓																									
Static	2	00-00-00-00-00-00	No		✓																									
Static	3	00-00-00-00-00-00	No		✓																									
Static	1	00-E0-4C-00-00-00	No	✓																										
Dynamic	1	00-E0-4C-36-14-16	No		✓																									

Previous 1 Next

FIGURE 8-2. MAC ADDRESS TABLE INFORMATION

PARAMETER DESCRIPTION

Navigating the MAC Table

Each page shows up to 999 entries from the MAC table, default is 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.
- Block: Whether the mac address is blocked or not.
- Port Members: The ports that are members of the entry.

Buttons

- Auto-refresh: Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.
- Refresh: Click to refresh the page.
- Clear: Click to clear the page.
- Next: Updates the mac address entries, turns to the next page.
- Previous: Updates the mac address entries, turns to the previous 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

IGMP Snooping is used to establish multicast groups to forward multicasts packet to the member ports without wasting 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 a broadcast packet, so it can only treat them all as broadcast packets. Without IGMP Snooping, the multicast packet forwarding function is the same as for a broadcast packet.

A switch supporting 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 the IGMP function when you enable IGMP proxy or snooping on the switch that 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.

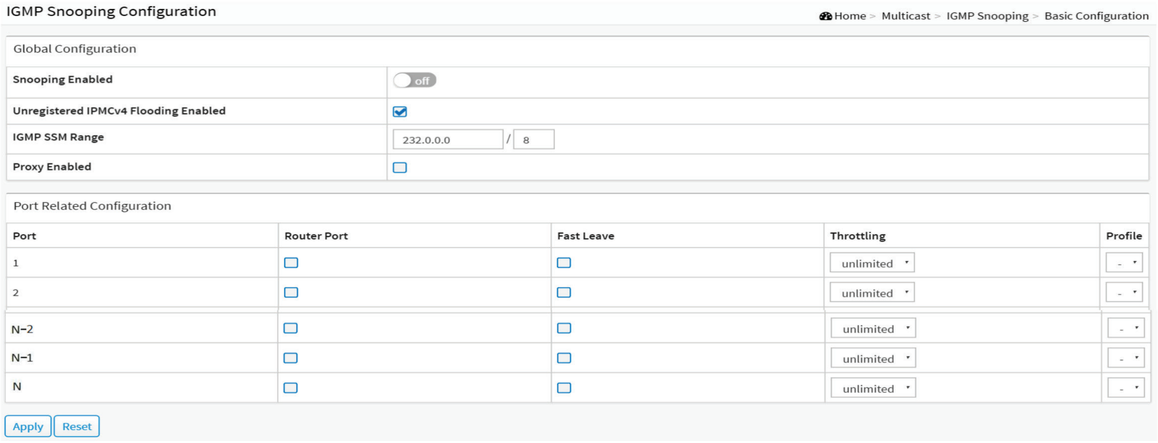
9.1.1 BASIC CONFIGURATION

This section describes how to set the basic IGMP snooping on the switch that 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. Select enable or disable the Global configuration.
3. Select the port to become a Router Port or enable/disable the Fast Leave function.
4. Scroll to set the Throtting and Profile.
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.



IGMP Snooping Configuration

Global Configuration	
Snooping Enabled	off
Unregistered IPMCv4 Flooding Enabled	☑
IGMP SSM Range	232.0.0.0 / 8
Proxy Enabled	□

Port Related Configuration

Port	Router Port	Fast Leave	Throttling	Profile
1	□	□	unlimited	-
2	□	□	unlimited	-
N–2	□	□	unlimited	-
N–1	□	□	unlimited	-
N	□	□	unlimited	-

FIGURE 9-1. IGMP SNOOPING CONFIGURATION

PARAMETER DESCRIPTION

Global Configuration

- Snooping Enabled: Enable 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-select it, the stream will be discarded.
- IGMP SSM Range: SSM (Source-Specific Multicast) Range allows the SSM-aware hosts and routers to run the SSM service model for the groups in the address range. Format: (IP address/ sub mask).
- 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: This 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 fast leave on the port.
- Throttling: Enable to limit the number of multicast groups to which a switch port can belong.
- Profile: You can select the profile to 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.

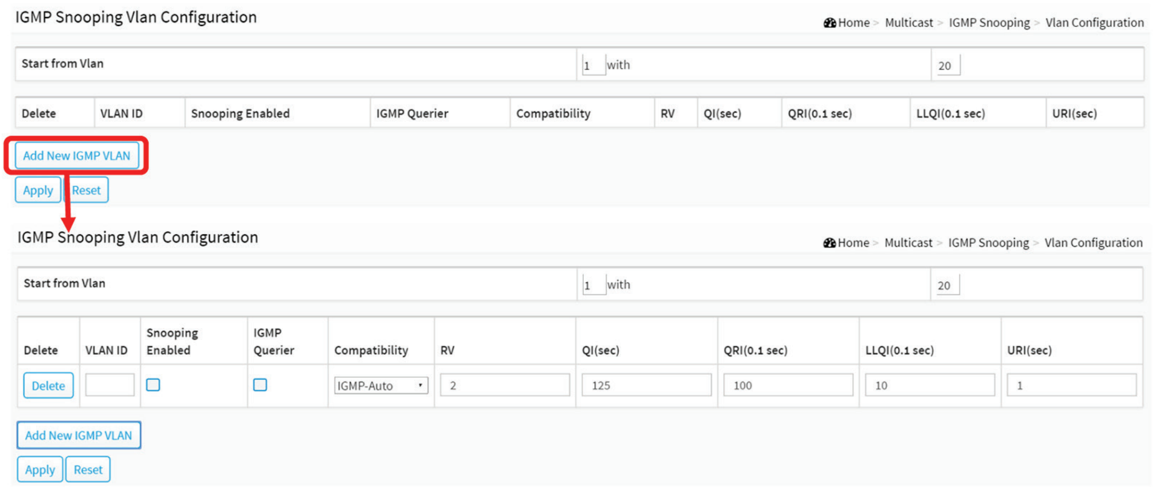
9.1.2 VLAN CONFIGURATION

This section describes the VLAN configuration setting process integrated with the IGMP Snooping function. Each setting page shows up to 99 entries from the VLAN table, default is 20, selected through the “entries per page” input field. When first visited, the web page will show the first 20 entries from the beginning of the VLAN Table. The first displayed 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 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

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)

Add New IGMP VLAN
Apply
Reset

IGMP Snooping Vlan Configuration

Home > Multicast > IGMP Snooping > Vlan Configuration

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

Add New IGMP VLAN
Apply
Reset

FIGURE 9-2. IGMP SNOOPING VLAN CONFIGURATION

PARAMETER DESCRIPTION

- Start from Vlan: 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: Displays the VLAN ID of the entry.
- Snooping Enabled: Enable the per-VLAN IGMP Snooping. 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; the 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; the 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; the 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; the 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; the 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.

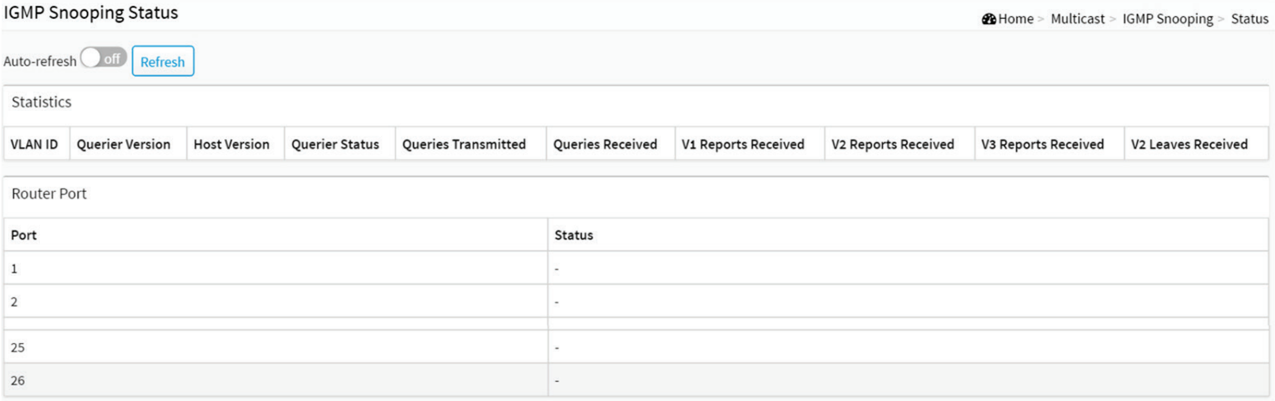
9.1.3 STATUS

After you complete the IGMP Snooping configuration, you can set the switch to display the IGMP Snooping Status. The section explains how 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

Router Port

Port	Status
1	-
2	-
25	-
26	-

FIGURE 9-3. IGMP SNOOPING STATUS

PARAMETER DESCRIPTION

Statistic

- VLAN ID: The VLAN ID of the entry.
- Querier Version: Currently working Querier Version.
- Host Version: Currently working Host Version.
- Querier Status: Shows the Querier status is “ACTIVE” or “IDLE”. “DISABLE” denotes the specific interface is administratively disabled.
- Queries Transmitted: The number of Transmitted Queries.
- Queries Received: The number of Received Queries.
- V1 Reports Received: The number of Received V1 Reports.
- V2 Reports Received: The number of Received V2 Reports.
- V3 Reports Received: The number of Received V3 Reports.
- V2 Leaves Received: The number of Received V2 Leaves.

Router Port

Display the ports that act as router ports. A router port is a port on the Ethernet switch that leads towards the Layer 3 multicast device or IGMP querier. Static denotes the specific port is configured to be a router port. Dynamic denotes the specific port is learned to be a router port. Both denote the specific port is configured and learned to be a router port.

- Port: Switch port number.
- Status: Indicates whether a specific port is a router port or not.

Buttons

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

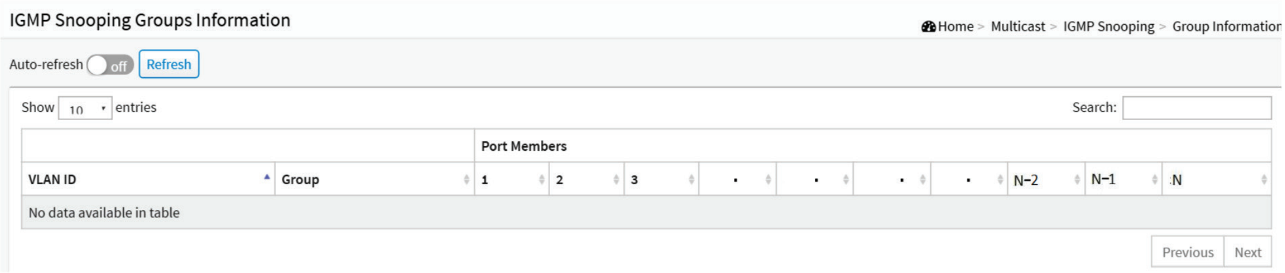
9.1.4 GROUP INFORMATION

After you set the IGMP Snooping function, you can set 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 select “Auto-refresh”.
4. Click “Refresh” to refresh an entry of the IGMP Snooping Groups Information.
5. Click Previous/next to change the page.


IGMP Snooping Groups Information
Home > Multicast > IGMP Snooping > Group Information
Auto-refresh
off
Refresh
Show 10 entries
Search:
Previous
Next

		Port Members									
VLAN ID	Group	1	2	3	•	•	•	•	N–2	N–1	N
No data available in table											

FIGURE 9-4. IGMP SNOOPING GROUPS INFORMATION

PARAMETER DESCRIPTION

Navigating the IGMP Group Table

Each page shows the number of entries from the IGMP Group table, default is 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 IGMP Group Table.

The “Search” input fields allow the user to select the starting point in the IGMP Group Table. It will update the displayed table starting from that or the next closest IGMP Group Table match.

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.

- Search: You can search for the information that you want to see.
- 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

- 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 group information entries, turns to the next page.
- Previous: Updates the group information entries, turns to the previous 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 that belong to the same group are treated as single entry.

WEB INTERFACE

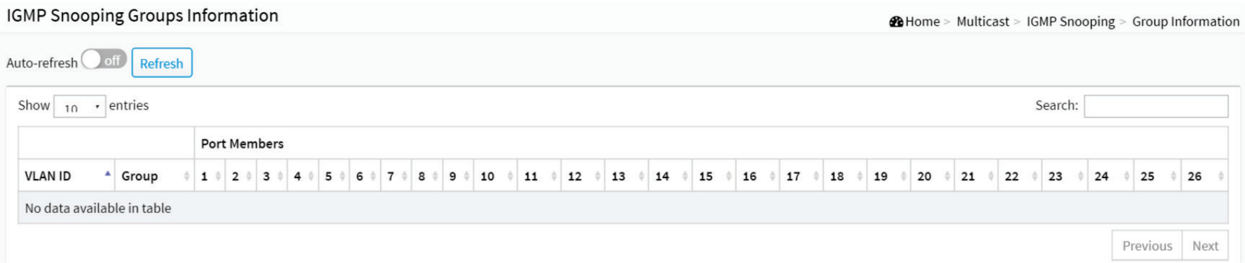
To display the IGMP SFM Information in the web interface:

1. Click Multicast, IGMP Snooping and IGMP SFM Information

2. If you want to auto-refresh the information, then you need to select “Auto-refresh”.

3. Click “Refresh” to refresh an entry of the IGMP Snooping Groups Information.

4. Click Previous/next to change the page.



IGMP Snooping Groups Information

		Port Members																									
VLAN ID	Group	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
No data available in table																											

FIGURE 9-5. IGMP SFM INFORMATION

PARAMETER DESCRIPTION

Navigating the IGMP SFM Information Table

Each page shows the entries from the IGMP SFM Information table, default is 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 IGMP SFM Information Table.

The “Search” input fields allow the user to select the starting point in the IGMP SFM Information Table. It will update the displayed table starting from that or the next closest IGMP SFM Information Table match.

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.

- Search: You can search for the information that you want to see.
- 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 128.
- Type: Indicates the Type. It can be either Allow or Deny.

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 group information entries, turns to the next page.
- Previous: Updates the group information entries, turns to the previous page.

9.2 MLD SNOOPING

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

NOTE: In an application 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: 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.

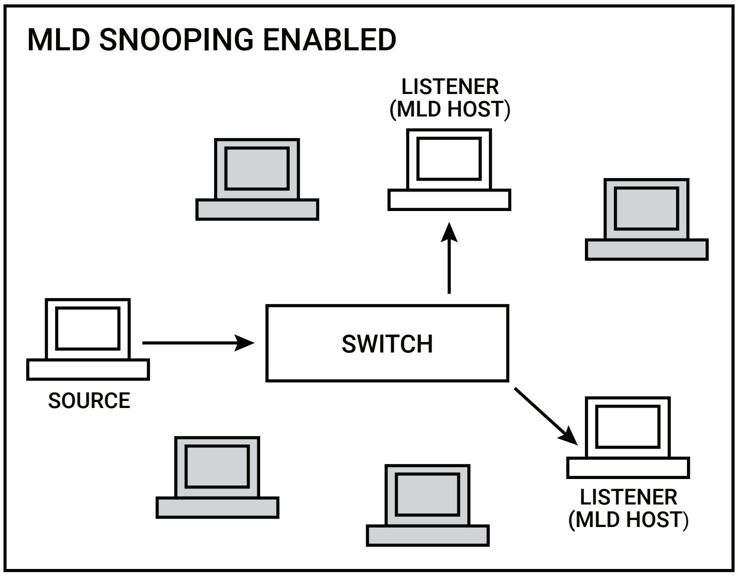


FIGURE 9-6.MLD SNOOPING ENABLE

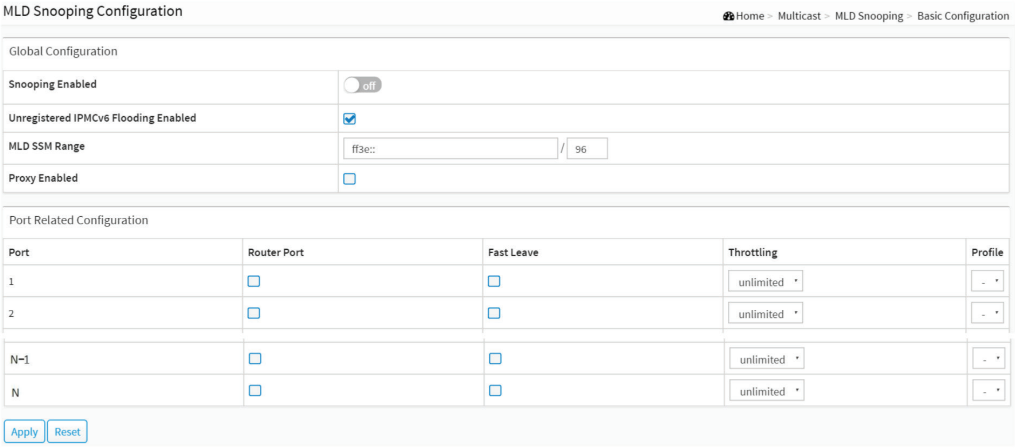
9.2.1 BASIC CONFIGURATION

This section explains how to configure the MLD Snooping basic configuration and the parameters.

WEB INTERFACE

To configure the MLD Snooping Configuration in the web interface:

1. Click Multicast, MLD Snooping and Basic Configuration.
2. Enable or disable the Global configuration parameters.
3. Select the port to join Router port and Fast Leave.
4. Scroll to select the Throtting mode with unlimited or 1 to 10.
5. Click save to save the setting.
6. If you want to cancel the setting, then you need to click the Reset button. It will revert to previously saved values.



MLD Snooping Configuration

Home > Multicast > MLD Snooping > Basic Configuration

Global Configuration

Snooping Enabled	off
Unregistered IPMCv6 Flooding Enabled	☑
MLD SSM Range	ff3e:: / 96
Proxy Enabled	□

Port Related Configuration

Port	Router Port	Fast Leave	Throttling	Profile
1	□	□	unlimited	-
2	□	□	unlimited	-
N-1	□	□	unlimited	-
N	□	□	unlimited	-

FIGURE 9-7. MLD SNOOPING BASIC CONFIGURATION

PARAMETER DESCRIPTION

Global Configuration

- Snooping Enabled: Enable Global MLD Snooping.
- Unregistered IPMCv6 Flooding enabled: Enable unregistered IPMCv6 traffic flooding.

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

  When MLD Snooping is disabled, unregistered IPMCv6 traffic flooding is always active in spite of this setting.
- MLD SSM Range: SSM (Source-Specific Multicast) Range allows the SSM-aware hosts and routers to run the SSM service model for the groups in the address (Using IPv6 Address) range.
- 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: Select to enable fast leave on the port.
- Throttling: Enable to limit the number of multicast groups to which a switch port can belong.
- 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

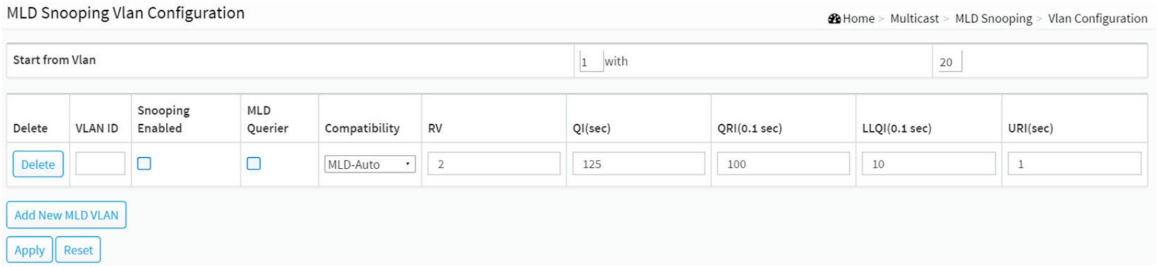
When MLD snooping is enabled on a VLAN, the switch acts to minimize unnecessary multicast traffic. If the switch receives multicast traffic destined for a given multicast address, it forwards that traffic only to ports on the VLAN that have MLD hosts for that address. It drops that traffic for ports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

The switch will use the last entry of the currently displayed entry as a basis for the next lookup. When the end is reached, the text “No more entries” is shown in the displayed table. Use the button to start over.

WEB INTERFACE

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

1. Click 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 9-8. 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. 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; the 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; the 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; the 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; the 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; the 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.

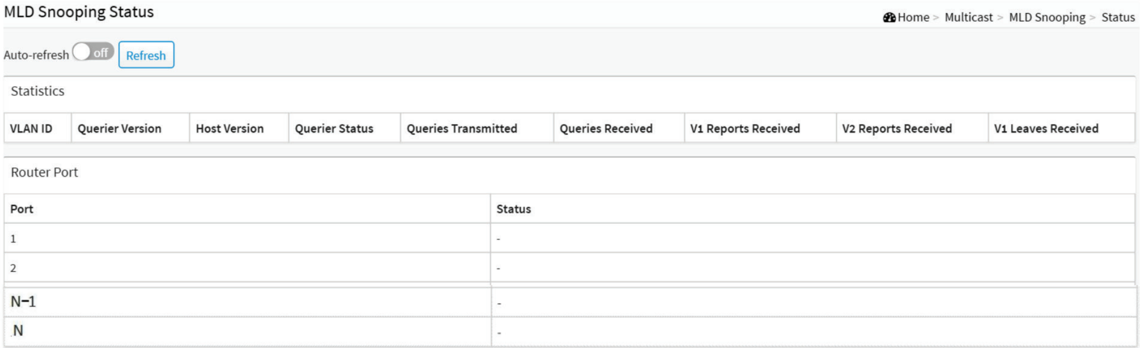
9.2.3 STATUS

This section describes how to display the MLD Snooping Status and detail information.

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 select "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

Router Port

Port	Status
1	-
2	-
N-1	-
N	-

FIGURE 9-9. MLD SNOOPING STATUS

PARAMETER DESCRIPTION

- VLAN ID: The VLAN ID of the entry.
- Querier Version: Currently working Querier Version.
- Host Version: Currently working Host Version.
- Querier Status: Show the Querier status is "ACTIVE" or "IDLE". "DISABLE" denotes the specific interface is administratively disabled.
- Queries Transmitted: The number of Transmitted Queries.

- Queries Received: The number of Received Queries.
- V1 Reports Received: The number of Received V1 Reports.
- V2 Reports Received: The number of Received V2 Reports.
- V1 Leaves Received: The number of Received V1 Leaves.
- Router Port: Display which ports act as router ports. A router port is a port on the Ethernet switch that leads towards the Layer 3 multicast device or MLD querier.

  Static denotes the specific port is configured to be a router port.

  Dynamic denotes the specific port is learned to be a router port.

  Both denote the specific port is configured and learned to be a router port.
- Port: Switch port number.
- Status: Indicate whether a specific port is a router port or not.

Buttons

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

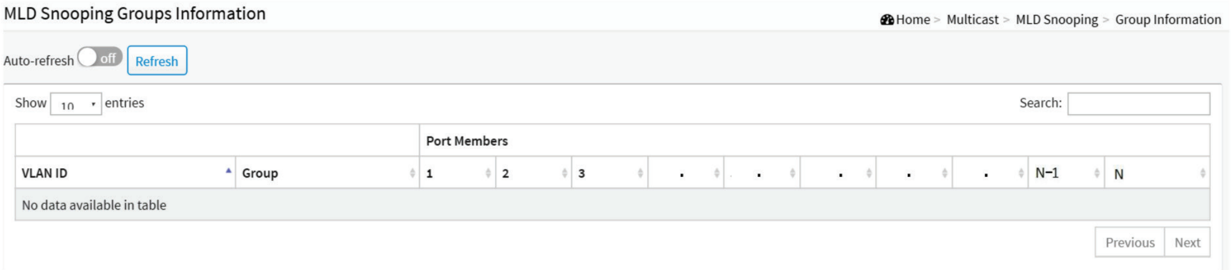
9.2.4 GROUPS INFORMATION

This section describes how to get the MLD Snooping Groups Information. The "Search" input fields allow the user to select the starting point in the MLD Group Table.

WEB INTERFACE

To display the MLD Snooping Group information in the web interface:

1. Click Multicast, MLD Snooping and Group Information.
2. If you want to auto-refresh the information, then you need to select "Auto-refresh."
3. Click "Refresh" to refresh an entry of the MLD Snooping Group Information.



MLD Snooping Groups Information

		Port Members									
VLAN ID	Group	1	2	3	.	.	.	.	.	N−1	N
No data available in table											

FIGURE 9-10. MLD SNOOPING GROUPS INFORMATION

PARAMETER DESCRIPTION

Navigating the MLD Group Table

Each page shows the entries from the MLD Group table, default is 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 MLD Group Table.

The “Search “ input fields allow the user to select the starting point in the MLD Group Table. It will update the displayed table starting from that or the closest next MLD Group Table match. The switch will use the last entry of the currently displayed table as a basis for the next lookup. When the end is reached, the text “No more entries” is shown in the displayed table. Use the button to start over.

- 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

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

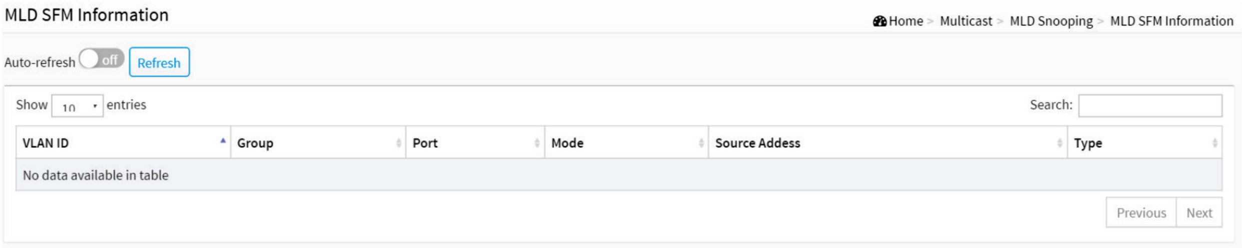
9.2.5 MLD SFM INFORMATION

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 that 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 select “Auto-refresh”.
3. Click “Refresh” to refresh an entry of the MLD SFM Information.



MLD SFM Information

Home > Multicast > MLD Snooping > MLD SFM Information

Auto-refresh off Refresh

Show 10 entries Search:

VLAN ID	Group	Port	Mode	Source Addess	Type
No data available in table					

Previous Next

FIGURE 9-11. MLD SFM INFORMATION

PARAMETER DESCRIPTION

Navigating the MLD SFM Information Table

Each page shows the entries from the MLD SFM Information table, default is 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 MLD SFM Information Table.

The “Search “ input fields allow the user to select the starting point in the MLD SFM Information Table. It will update the displayed table starting from that or the next closest MLD SFM Information Table match.

The switch will use the last entry of the currently displayed table as a basis for the next lookup. When the end is reached, the text “No more entries” is shown in the displayed table. Use the button to start over.

- 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 128.
- Type: Indicates the Type. It can be either Allow or Deny.
- Show entries: You can choose how many items you want to show.

Buttons

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

9.3 MVR

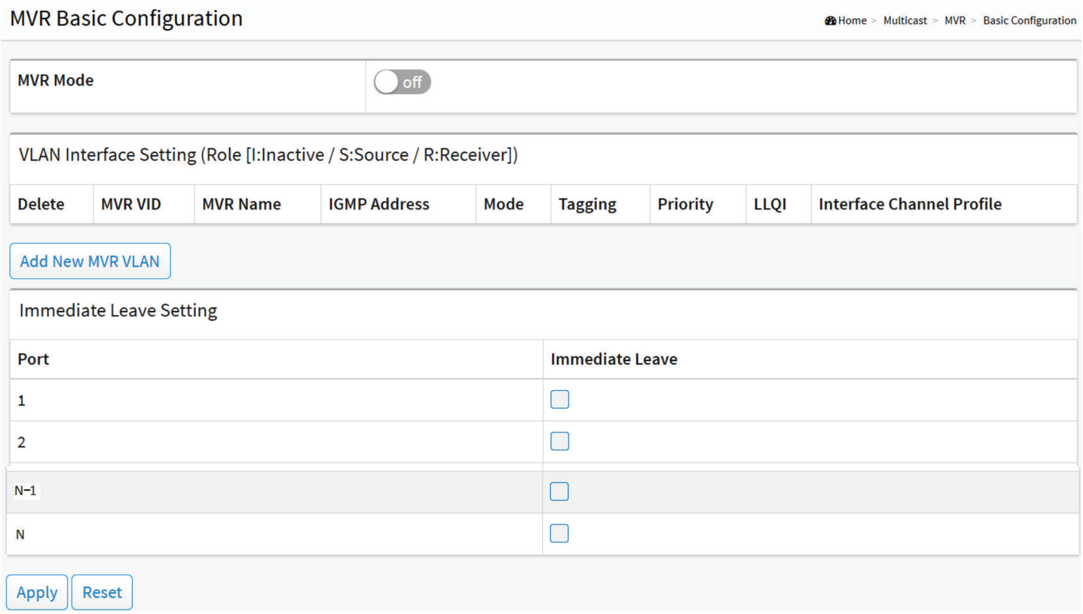
The MVR feature enables multicast traffic forwarding on the Multicast VLAN. In a multicast television application, a PC or a television with a set-top box can receive the multicast stream. Multiple set-top boxes or PCs can be connected to one subscriber port, which is a switch port configured as an MVR 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.
3. Click “Add New MVR VLAN”.
4. Specify MVR VID, MVR Name, IGMP Address, Mode, Tagging, Priority, LLQI, Interface Channel Profile.
5. Select the port to Click Immediate Leave.
6. Click 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 Basic Configuration

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	□
2	□
N-1	□
N	□

FIGURE 9-12. MVR CONFIGURATION

PARAMETER DESCRIPTION

- MVR Mode: Enable/Disable the Global MVR.

  The Unregistered Flooding control depends on the current configuration in IGMP/MLD Snooping. We suggest that you enable Unregistered Flooding control when the MVR group table is full.

- MVR VID: Specify the Multicast VLAN ID.

  CAUTION: We do not recommend overlapping MVR source ports with management VLAN ports.

- MVR Name: MVR Name is an optional attribute to indicate the name of the specific MVR VLAN. The 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, the 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 is established in the 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 in MVR operations.

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

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

  CAUTION: We do not recommend overlapping MVR source ports 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 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.

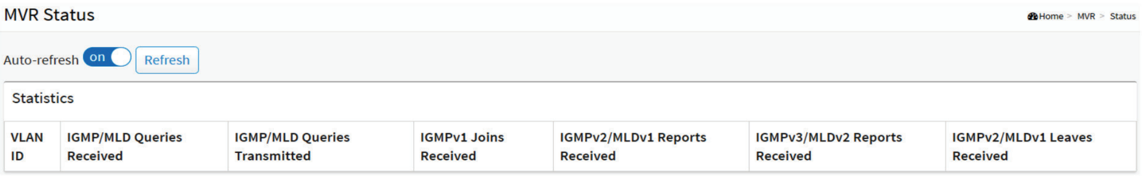
9.3.2 STATUS

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

WEB INTERFACE

To display the MVR Statistics Information in the web interface:

1. Click Multicast, MVR and Status.
2. If you want to auto-refresh the information, then you need to select "Auto-refresh".
3. Click "Refresh" to refresh an entry of the MVR Statistics Information.



MVR Status

Statistics

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

FIGURE 9-13. 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

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

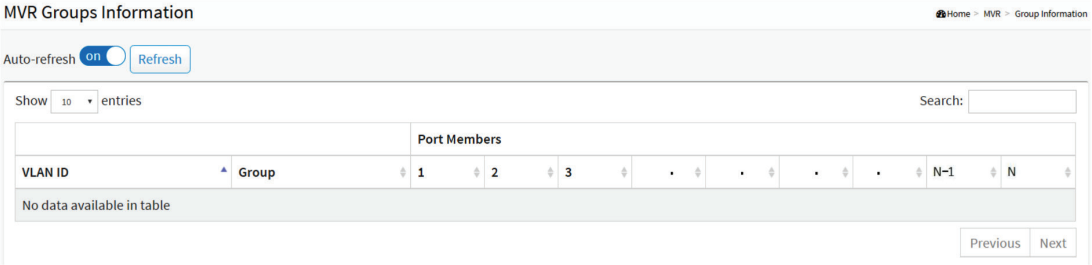
9.3.3 MVR GROUPS INFORMATION

This section describes how to display the MVR Groups detail information on the switch. Entries in the MVR Group Table are shown on this page. The MVR Group Table is sorted first by VLAN ID, and then by group.

WEB INTERFACE

To display the MVR Groups Information in the web interface:

1. Click Multicast, MVR Groups Information.
2. If you want to auto-refresh the information, then you need to select "Auto-refresh".
3. Click "Refresh" to refresh an entry of the MVR Groups Information.
4. Click Previous/next to change the page.



		Port Members								
VLAN ID	Group	1	2	3	·	·	·	·	N-1	N
No data available in table										

FIGURE 9-14. MVR GROUPS INFORMATION

PARAMETER DESCRIPTION

Navigating the MVR Channels (Groups) Information Table

Each page shows the entries from the MVR Group table, default is 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 MVR Channels (Groups) Information Table.

The “Search” input fields allow the user to select the starting point in the MVR Channels (Groups) Information Table. It will update the displayed table starting from that or the closest next MVR Channels (Groups) Information Table match.

The switch will use the last entry of the currently displayed table as a basis for the next lookup. When the end is reached, the text “No more entries” is shown in the displayed table. Use the button to start over.

MVR Channels (Groups) Information Table Columns

- Show entries: You can choose how many items you want to show.
- Search: You can search for the information that you want to see.
- VLAN ID: VLAN ID of the group.
- Groups: Group ID of the group displayed.
- Port Members: Ports under this group.

Buttons

- Auto-refresh: Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.
- Refresh: Click to refresh the page immediately.
- Next: Updates the system log entries, turns to the next page.
- Previous: Updates the system log entries, turns to the previous page.

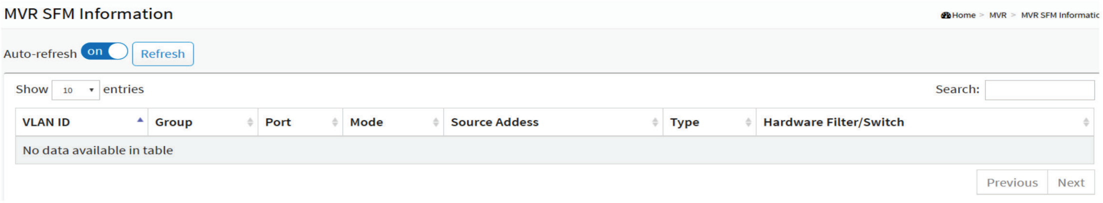
9.3.4 MVR SFM INFORMATION

The MVR SFM (Source-Filtered Multicast) Information Table also contains the SSM (Source-Specific Multicast) information. This table is sorted first by VLAN ID, then by group, and then by Port. Different source addresses that belong to the same group are treated as a 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 select “Auto-refresh”.
3. Click “Refresh” to refresh an entry of the MVR Groups Information.
4. Click Previous/next to change the page.



MVR SFM Information

Home > MVR > MVR SFM Informatic

Auto-refresh on Refresh

Show 10 entries

Search:

VLAN ID	Group	Port	Mode	Source Addess	Type	Hardware Filter/Switch
No data available in table						

Previous Next

FIGURE 9-X. MVR SFM INFORMATION

PARAMETER DESCRIPTION

Navigating the MVR SFM Information Table

Each page shows the entries from the MVR SFM Information Table, default is 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 MVR SFM Information Table.

The “Search “ input fields allow the user to select the starting point in the MVR SFM Information Table. It will update the displayed table starting from that or the closest next MVR SFM Information Table match.

The switch will use the last entry of the currently displayed table as a basis for the next lookup. When the end is reached, the text “No more entries” is shown in the displayed table. Use the button to start over.

MVR SFM Information Table Columns

- Show entries: You can choose how many items you want to show up.
- Search: You can search for the information that you want to see.
- 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, the system limits the total number of IP source addresses for filtering to 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 or not the data plane destined to the specific group address from the source IPv4/IPv6 address can be handled by the chip.

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, turns to the next page.
- Previous: Updates the system log entries, turns to the previous page.

9.4 MULTICAST FILTERING PROFILE

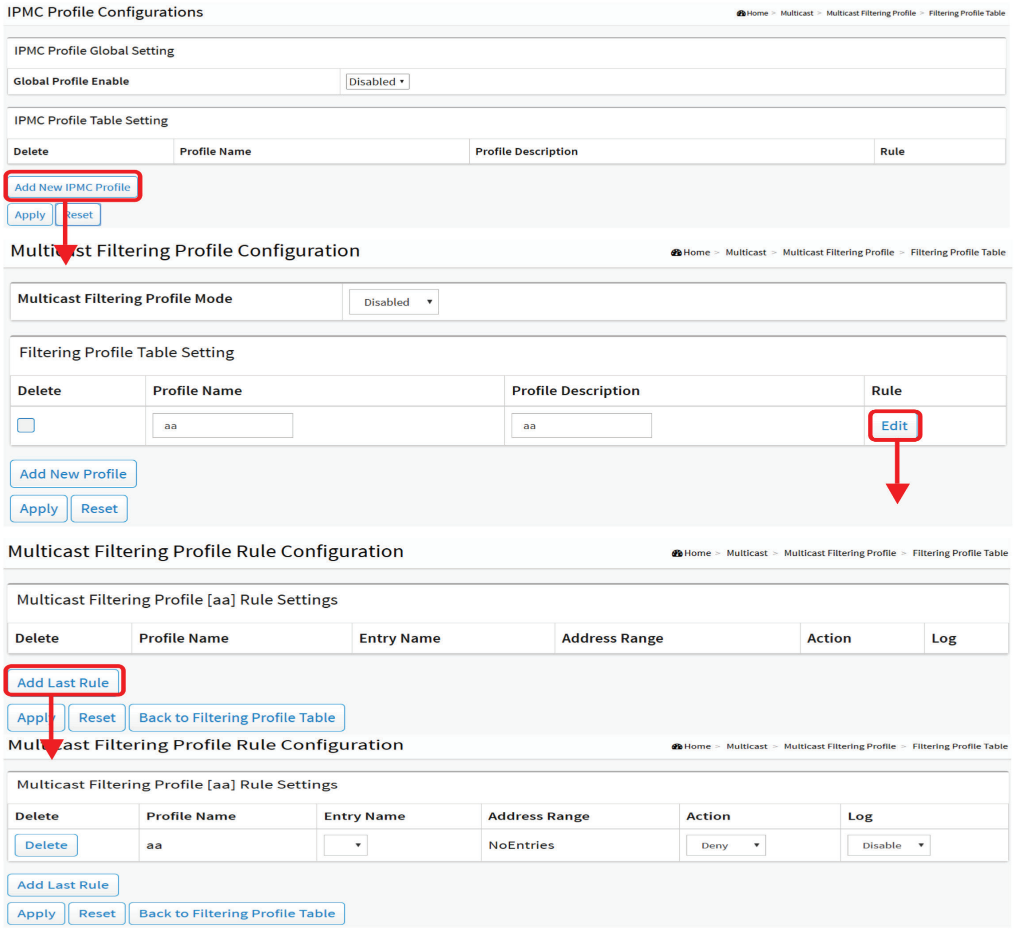
This page provides Multicast Filtering Profile related configurations.

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:



IPMC Profile Configurations

Home > Multicast > Multicast Filtering Profile > Filtering Profile Table

IPMC Profile Global Setting

Global Profile Enable	Disabled

IPMC Profile Table Setting

Delete	Profile Name	Profile Description	Rule

Add New IPMC Profile

Apply Reset

Multicast Filtering Profile Configuration

Home > Multicast > Multicast Filtering Profile > Filtering Profile Table

Multicast Filtering Profile Mode	Disabled

Filtering Profile Table Setting

Delete	Profile Name	Profile Description	Rule
□	aa	aa	Edit

Add New Profile

Apply Reset

Multicast Filtering Profile Rule Configuration

Home > Multicast > Multicast Filtering Profile > Filtering Profile Table

Multicast Filtering Profile [aa] Rule Settings

Delete	Profile Name	Entry Name	Address Range	Action	Log

Add Last Rule

Apply Reset Back to Filtering Profile Table

Multicast Filtering Profile Rule Configuration

Home > Multicast > Multicast Filtering Profile > Filtering Profile Table

Multicast Filtering Profile [aa] Rule Settings

Delete	Profile Name	Entry Name	Address Range	Action	Log
Delete	aa		NoEntries	Deny	Disable

Add Last Rule

Apply Reset Back to Filtering Profile Table

FIGURE 9-15. IPMC PROFILE CONFIGURATION

PARAMETER DESCRIPTION

- Global Profile Mode: Enable/Disable the Global IPMC Profile. The system starts to do filtering based on profile settings only when the global profile mode is enabled.
- 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 separate the description sentence.
- Rule: When the profile is created, click the edit button to enter the rule setting page of the designated profile. A 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:

  - View : List the rules associated with the designated profile.
  - Edit : Adjust the rules associated with the designated profile.
- Profile Name: The name of the designated profile to be associated. This field is not editable.
- Entry Name: The name used in specifying the address range used for this rule. Only the existing profile address entries will be chosen in the selected box. This field is not allowed to be selected as none ("-") while the Rule Settings Table is committed.
- Address Range: The corresponding address range of the selected profile entry. This field is not editable and will be adjusted automatically according to the selected profile entry.
- Action: Indicates the learning action upon receiving the Join/Report frame that has the group address matches the address range of the rule.
- Permit: Group address matches the range specified in the rule will be learned.
- Deny: Group address matches the range specified in the rule will be dropped.
- Log: Indicates the logging preference upon receiving the Join/Report frame that has the group address matches the address range of the rule.

  - Enable: Corresponding information of the group address, that matches the range specified in the rule, will be logged.
  - Disable: Corresponding information of the group address, that matches the range specified in the rule, will not be logged.

Buttons

- Add New IPMC 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".
- Back to Filtering Profile Table: Click to undo any changes made locally and return to the Filtering Profile Table.
- Reset: Click to undo any changes made locally and revert to previously saved values.

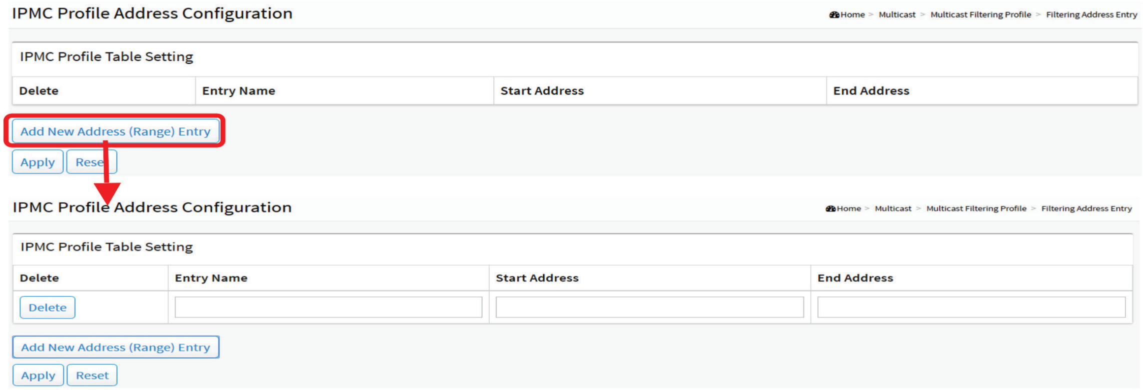
9.4.2 FILTERING ADDRESS ENTRY

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:



IPMC Profile Address Configuration

Home > Multicast > Multicast Filtering Profile > Filtering Address Entry

IPMC Profile Table Setting

Delete	Entry Name	Start Address	End Address

IPMC Profile Address Configuration

Home > Multicast > Multicast Filtering Profile > Filtering Address Entry

IPMC Profile Table Setting

Delete	Entry Name	Start Address	End Address
Delete			

FIGURE 9-16. 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 a 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.

CHAPTER 10: DHCP

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

10.1 SNOOPING

10.1.1 CONFIGURATION

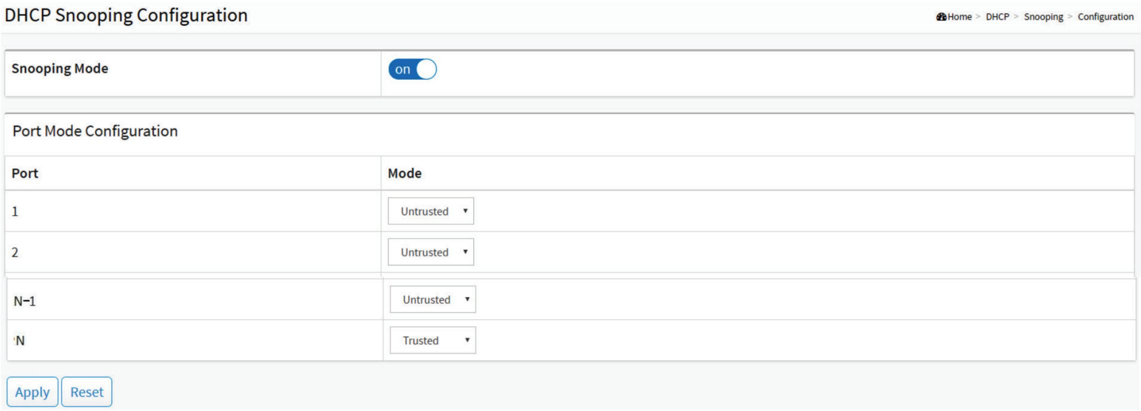
DHCP Snooping is used to block an intruder on the untrusted ports of the switch device when it tries to intervene by injecting a bogus DHCP reply packet to a legitimate conversation between the DHCP client and server.

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

WEB INTERFACE

To configure DHCP snooping in the web interface:

1. Click DHCP, Snooping and Configuration.
2. Select “on” in the Mode of DHCP Snooping Configuration.
3. Select “Trusted” for the specific port in the Mode of Port Mode Configuration.
4. Click Apply.



DHCP Snooping Configuration

Snooping Mode	on

Port Mode Configuration

Port	Mode
1	Untrusted
2	Untrusted
N-1	Untrusted
'N	Trusted

FIGURE 10-1. 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 a trusted source of the DHCP messages. A Trusted port can forward DHCP packets normally.
  - Untrusted: Configures the port as an untrusted source of the DHCP messages. An Untrusted port will discard the packets when it receives DHCP packets.

Buttons

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

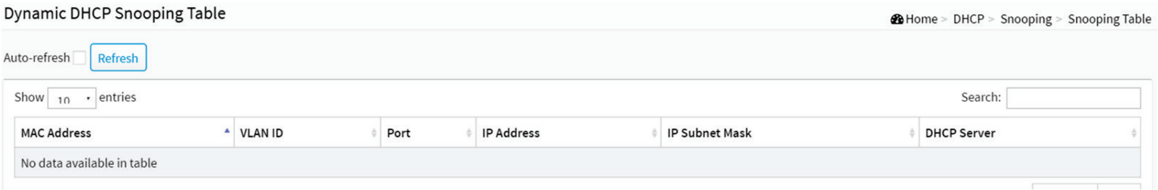
10.1.2 SNOOPING TABLE

This page displays the dynamic IP assigned information after DHCP Snooping mode is enabled. All DHCP clients that obtained the dynamic IP address from the DHCP server will be listed in this table except for local VLAN interface IP addresses. Entries in the Dynamic DHCP snooping Table are shown on this page.

WEB INTERFACE

To monitor a DHCP in the web interface:

1. Click DHCP, Snooping and Snooping table.



Dynamic DHCP Snooping Table

Home > DHCP > Snooping > Snooping Table

Auto-refresh □ Refresh

Show 10 entries

Search:

MAC Address	VLAN ID	Port	IP Address	IP Subnet Mask	DHCP Server
No data available in table					

FIGURE 10-2. DHCP SNOOPING TABLE

PARAMETER DESCRIPTION

- Show entries: You can choose how many items you want to show up.
- Search: You can search for the information that you want to see.
- MAC Address: User MAC address of the entry.
- VLAN ID: VLAN-ID in which the DHCP traffic is permitted.
- 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

- 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, turns to the next page.
- Previous: Updates the system log entries, turns to the previous page.

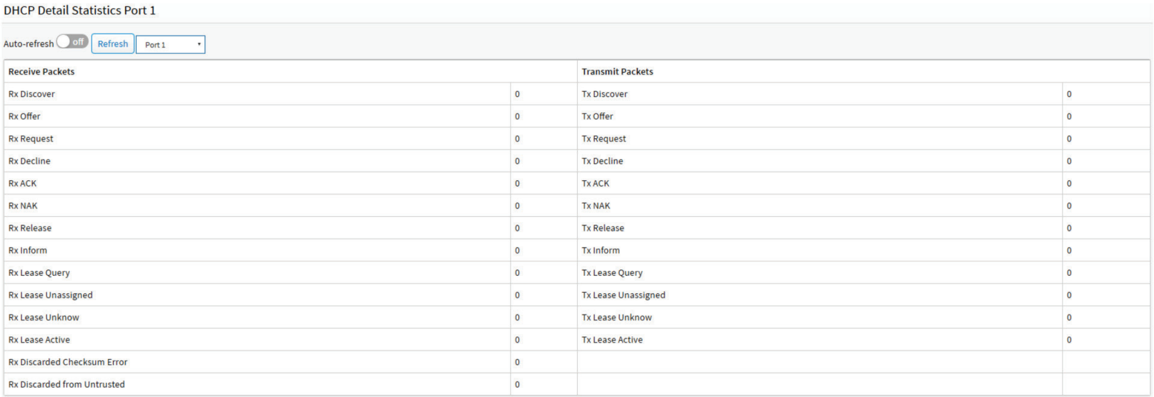
10.1.3 DETAILED STATISTICS

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. Clearing the statistics on specific port may not take effect on global statistics since it gathers the different layer overview.

WEB INTERFACE

To display DHCP Relay statistics in the web interface:

1. Click DHCP, Snooping and Detailed Statistics.
2. Select the port for which you want to display the DHCP Detailed Statistics.
3. If you want to auto-refresh the information, then you need to select "Auto-refresh".
4. Click "Refresh" to refresh an entry of the DHCP Detailed Statistics.



DHCP Detail 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 Unknow	0	Tx Lease Unknow	0
Rx Lease Active	0	Tx Lease Active	0
Rx Discarded Checksum Error	0		
Rx Discarded from Untrusted	0		

FIGURE 10-3. 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 discarded packets with IP/UDP checksum error.
- Rx Discarded from Untrusted: The number of discarded packet that are coming from an untrusted port.

Buttons

- Auto-refresh: Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.
- Refresh: Click to refresh the page immediately.
- Port 1: Select the port for which you want to display the DHCP Detailed Statistics.

10.2 RELAY

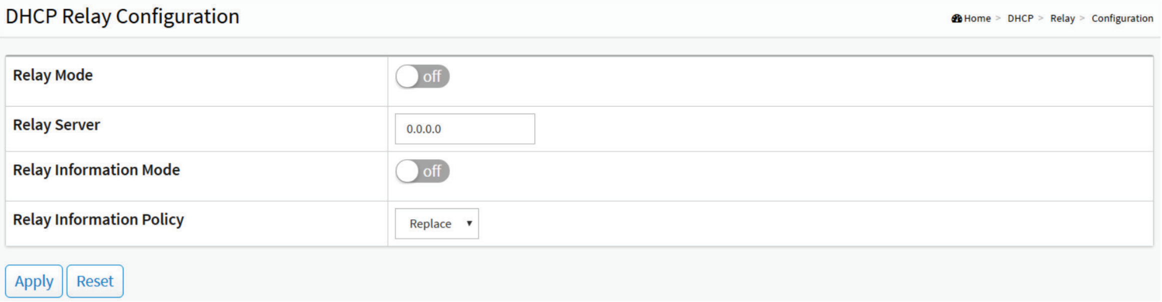
10.2.1 CONFIGURATION

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 this type of condition, make sure to set 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	off
Relay Information Policy	Replace ▾

FIGURE 10-4. 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 is "[vlan_id][module_id][port_no]". The first four characters represent the VLAN ID, the fifth and sixth characters are the module ID (in a standalone device it always equals 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 to 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 a DHCP server and removes it from a DHCP message when transferring to a 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.

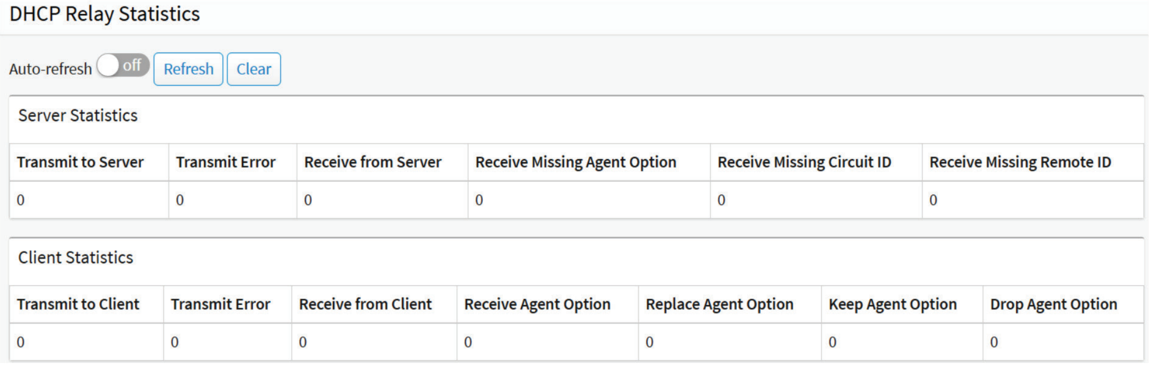
10.2.2 STATISTICS

This page provides statistics for DHCP relay.

WEB INTERFACE

To monitor DHCP Relay statistics in the web interface:

1. Click DHCP, Relay and Relay Statistics.
2. Display DHCP relay statistics.



DHCP Relay Statistics

Server Statistics

Transmit to Server	Transmit Error	Receive from Server	Receive Missing Agent Option	Receive Missing Circuit ID	Receive Missing Remote ID
0	0	0	0	0	0

Client Statistics

Transmit to Client	Transmit Error	Receive from Client	Receive Agent Option	Replace Agent Option	Keep Agent Option	Drop Agent Option
0	0	0	0	0	0	0

FIGURE 10-5. 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 a 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.

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 a client.
- Receive Agent Option: The number of received packets with relay agent information option.
- Replace Agent Option: The number of packets that were replaced with a 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 that were received with relay agent information.

Buttons

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

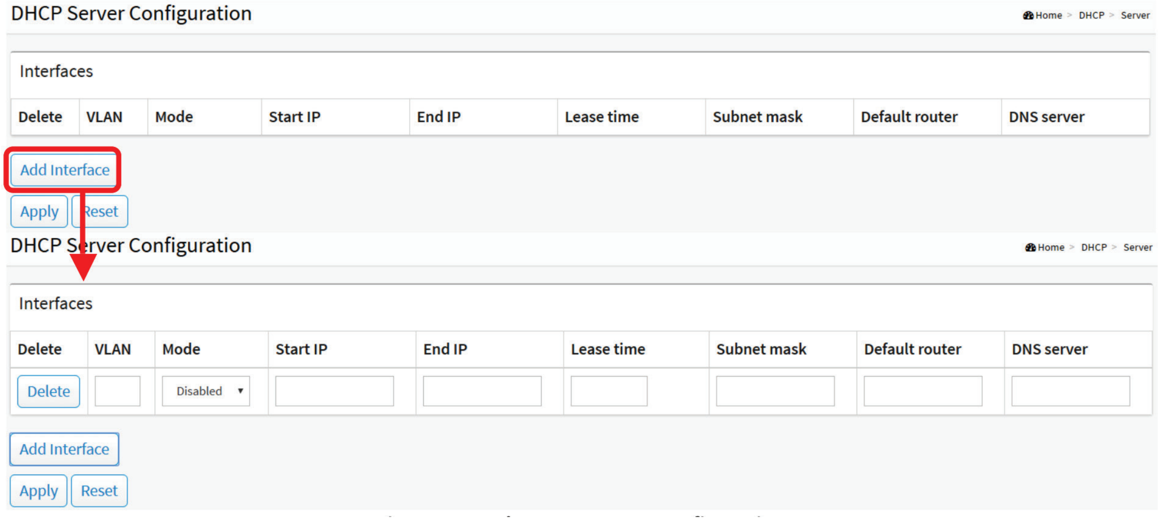
10.3 SERVER

This page configures the mode to enable/disable DHCP server per system and per VLAN. It also configures Start IP and End IP addresses. A DHCP server will allocate these IP addresses to a DHCP client, and deliver configuration parameters to the DHCP client.

WEB INTERFACE

To configure DHCP server Configuration in the web interface:

1. Click DHCP and Server.
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

Delete	VLAN	Mode	Start IP	End IP	Lease time	Subnet mask	Default router	DNS server

DHCP Server Configuration

Interfaces

Delete	VLAN	Mode	Start IP	End IP	Lease time	Subnet mask	Default router	DNS server
Delete		Disabled ▾						

FIGURE 10-6. DHCP SERVER CONFIGURATION

PARAMETER DESCRIPTION

- VLAN: Configure the VLAN in which a 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 the lease time of the pool.
- Subnet Mask: Configure the subnet mask of the DHCP address.
- Default router: Configure the destination IP network or host address of this route.
- DNS Server: Specify a 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.

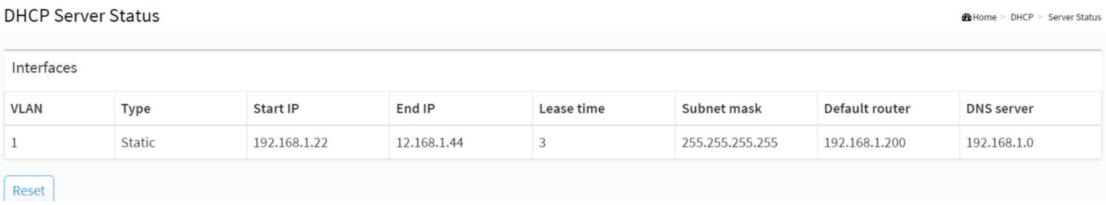
10.4 SERVER STATUS

This page displays DHCP server status.

WEB INTERFACE

To display DHCP server status in the web interface:

1. Click DHCP and Server Status.



DHCP Server Status

Interfaces

VLAN	Type	Start IP	End IP	Lease time	Subnet mask	Default router	DNS server
1	Static	192.168.1.22	12.168.1.44	3	255.255.255.255	192.168.1.200	192.168.1.0

FIGURE 10-7. 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 the lease time of the pool.
- Subnet Mask: Display the subnet mask of the DHCP address.
- Default router: Display the destination IP network or host address of this route.
- DNS Server: Display the DNS server.

Buttons

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

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

11.1 MANAGEMENT

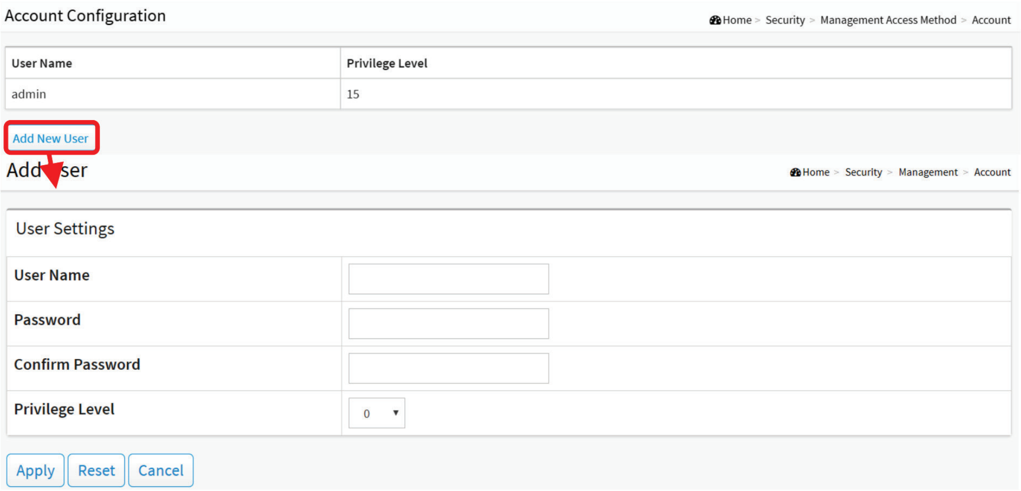
11.1.1 ACCOUNT

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 a 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.



Account Configuration

Home > Security > Management Access Method > Account

User Name	Privilege Level
admin	15

Add User

Home > Security > Management > Account

User Settings

User Name	
Password	
Confirm Password	
Privilege Level	0 ▾

FIGURE 11-1. ACCOUNT CONFIGURATION

PARAMETER DESCRIPTION

- User Name: The name identifying the user. The field can hold up to 31 characters. This is also a link to Add/Edit User.
- Password: Type the password. The field hold up to 31 characters, and the allowed content is the ASCII characters from 32 to 126.
- Password (again): Type the password again. You must type the same password again in the field.
- Privilege Level: The privilege level of the user. The allowed range is 1 to 15. If the privilege level value is 15, it can access all groups, i.e. that it is granted the full control of the device. Other values 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, most groups with privilege level 5 have read-only access and groups with privilege level 10 have read-write access. For system maintenance (software upload, factory defaults and etc.), you need user privilege level 15. Generally, 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).

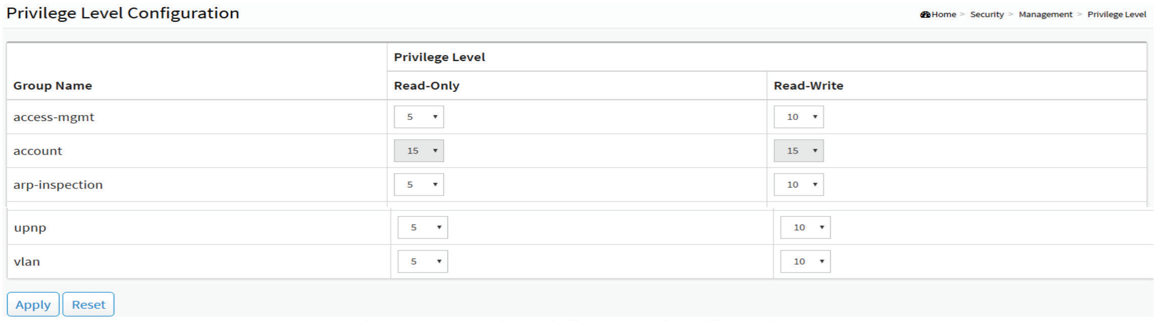
11.1.2 PRIVILEGE LEVELS

This page provides an overview of the privilege levels. The switch provides user set Group Name Privilege Levels from 1 to 15.

WEB INTERFACE

To configure Privilege Level in the web interface:

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



Privilege Level Configuration

	Privilege Level	
Group Name	Read-Only	Read-Write
access-mgmt	5	10
account	15	15
arp-inspection	5	10
upnp	5	10
vlan	5	10

FIGURE 11-2. 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 contain more than one. The following description defines these privilege level groups in detail: 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. The 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.

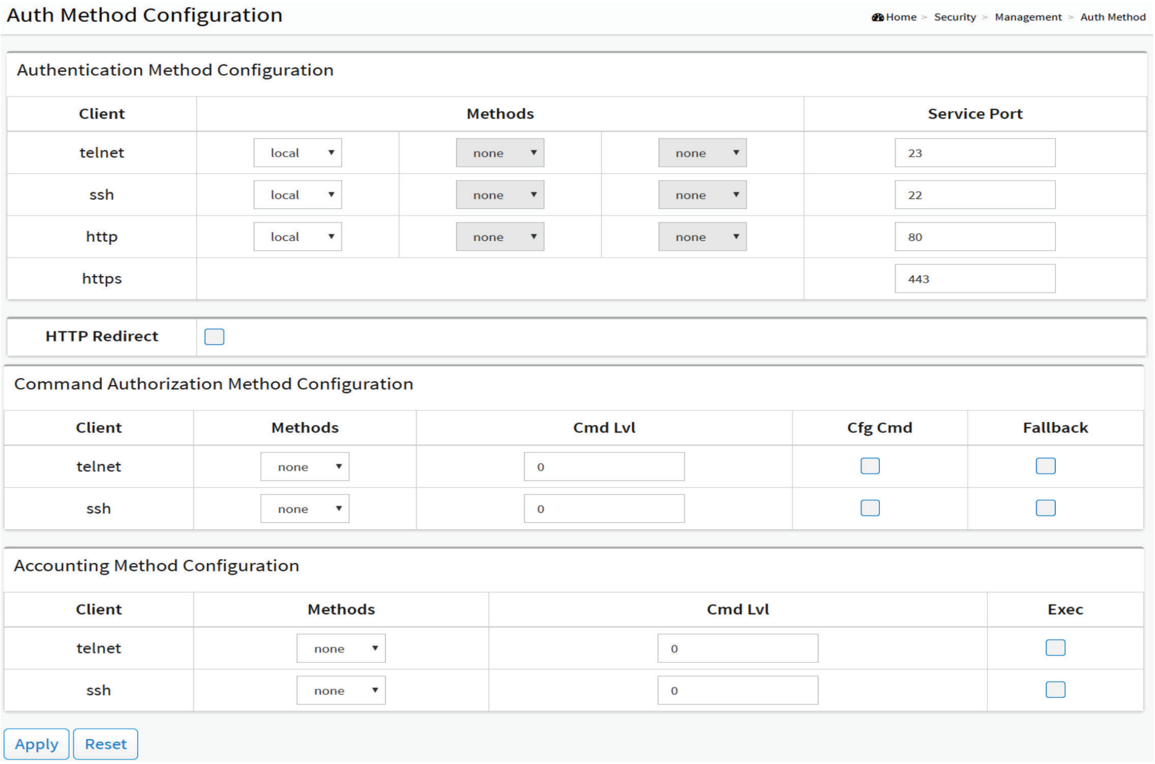
11.1.3 AUTH METHOD

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 (telent, ssh, web) that you want to monitor.
3. Specify the Methods (none, local, radius, tacacs), Service port, Cmd Lvl, Cfg Cmd, Fallback, Exec.
4. Click Apply.



Auth Method Configuration

Authentication Method Configuration

Client	Methods			Service Port
telnet	local	none	none	23
ssh	local	none	none	22
http	local	none	none	80
https				443

HTTP Redirect	□

Command Authorization Method Configuration

Client	Methods	Cmd Lvl	Cfg Cmd	Fallback
telnet	none	0	□	□
ssh	none	0	□	□

Accounting Method Configuration

Client	Methods	Cmd Lvl	Exec
telnet	none	0	□
ssh	none	0	□

FIGURE 11-3. 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 involve 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, we recommend configuring 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. The 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 MANAGEMENT

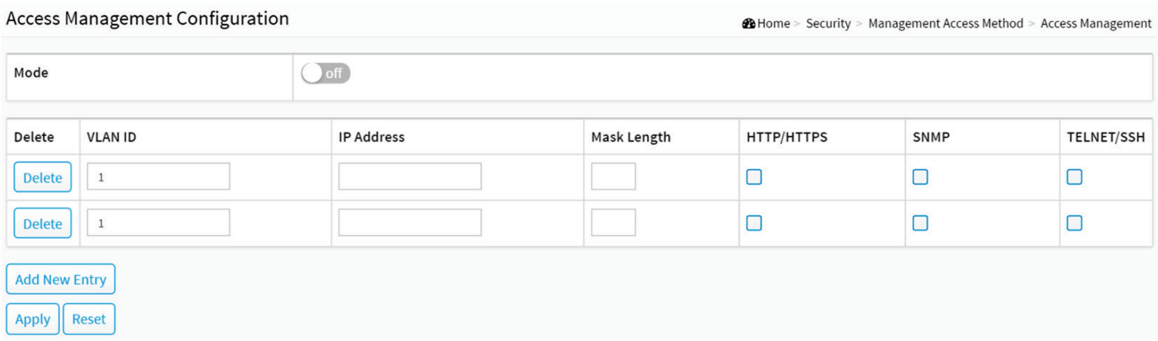
This section shows you how to configure the access management table of the Switch including HTTP/HTTPS, SNMP, and TELNET/SSH. You can manage the Switch over an Ethernet LAN or over the Internet.

WEB INTERFACE

To configure an Access Management Configuration in the web interface:

1. Click Security, Management and Access Management.
2. Select "on" in the Mode of Access Management Configuration.
3. Click "Add new entry".

4. Specify the IP Address, Mask Length.
5. Check the Access Management method (HTTP/HTTPS, SNMP, and TELNET/SSH) in the entry.
6. Click Apply.



Access Management Configuration

Home > Security > Management Access Method > Access Management

Mode	off

Delete	VLAN ID	IP Address	Mask Length	HTTP/HTTPS	SNMP	TELNET/SSH
Delete	1			□	□	□
Delete	1			□	□	□

FIGURE 11-4. ACCESS MANAGEMENT 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.
- IP address: Enter the source IP address.
- Mask Length: Enter the Mask Length.
- 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.

11.2 IEEE 802.1X

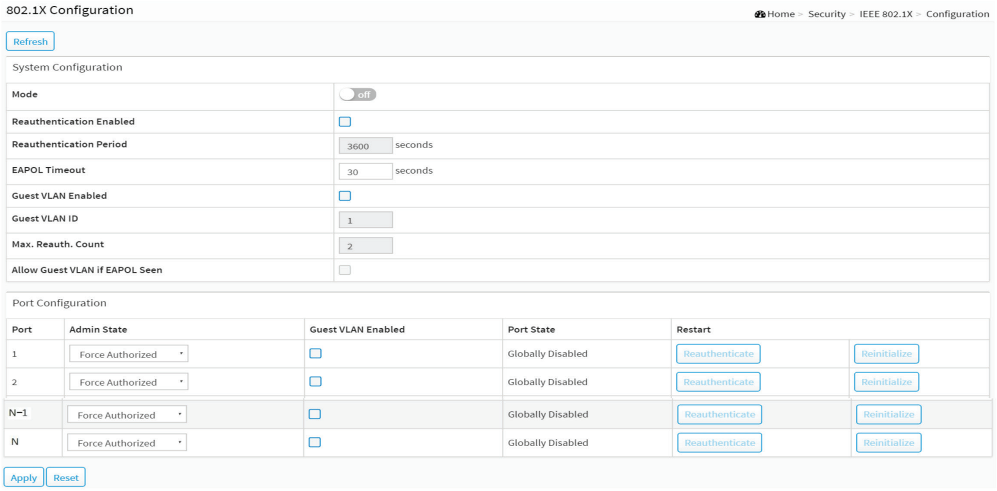
11.2.1 CONFIGURATION

This section describes how 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, IEEE 802.1X and Configuration.
2. Select “on” in the Mode of IEEE 802.1X Configuration.
3. Check Reauthentication Enabled.
4. Set Reauthentication Period (Default is 3600 seconds).
5. Select Admin State and displays Port State.
6. Click 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.


802.1X Configuration

Home > Security > IEEE 802.1X > Configuration

Refresh

System Configuration

Mode	off
Reauthentication Enabled	□
Reauthentication Period	3600 seconds
EAPOL Timeout	30 seconds
Guest VLAN Enabled	□
Guest VLAN ID	1
Max. Reauth. Count	2
Allow Guest VLAN if EAPOL Seen	□

Port Configuration

Port	Admin State	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

Apply Reset

FIGURE 11-5. 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).

- 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.
- 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 a response before considering entering the Guest VLAN is adjusted with this setting. The value can only be changed if the Guest VLAN option is globally enabled. Valid values are in the range [1; 255].

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

Port Configuration

- Port: The port number for which the configuration 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 back-end servers are enabled and that the server timeout is configured to X seconds (using the AAA configuration page), and suppose that the first server in the list is currently down (but not considered dead).

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 back-end authentication server requests whenever it receives a new EAPOL Start frame from the supplicant.

And since the server hasn't yet failed (because the X seconds haven't expired), the same server will be contacted upon the next back-end authentication server request from the switch. This scenario will loop forever. 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.

- Guest VLAN Enabled: When Guest VLAN is both globally enabled and enabled (checked) for a given port, the switch considers moving the port into the Guest VLAN according to the rules outlined below.

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

• Port-based 802.1X

• Single 802.1X

• Multi 802.1X

For troubleshooting VLAN assignments, use the “MonitorVLANs-VLAN Membership and VLAN Port” pages. These pages show which modules have (temporarily) overridden the current Port VLAN configuration.

Guest VLAN Operation:

When a Guest VLAN enabled port’s link comes up, the switch starts transmitting EAPOL Request Identity frames. If the number of transmissions of such frames exceeds Max. Reauth. Count and no EAPOL frames have been received in the meantime, the switch considers entering the Guest VLAN. The interval between transmission of EAPOL Request Identity frames is configured with EAPOL Timeout. If Allow Guest VLAN if EAPOL Seen is enabled, the port will now be placed in the Guest VLAN. If disabled, the switch will first check its history to see if an EAPOL frame has previously been received on the port (this history is cleared if the port link goes down or the port’s Admin State is changed), and if not, the port will be placed in the Guest VLAN. Otherwise, it will not move to the Guest VLAN, but continue transmitting EAPOL Request Identity frames at the rate given by EAPOL Timeout.

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

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

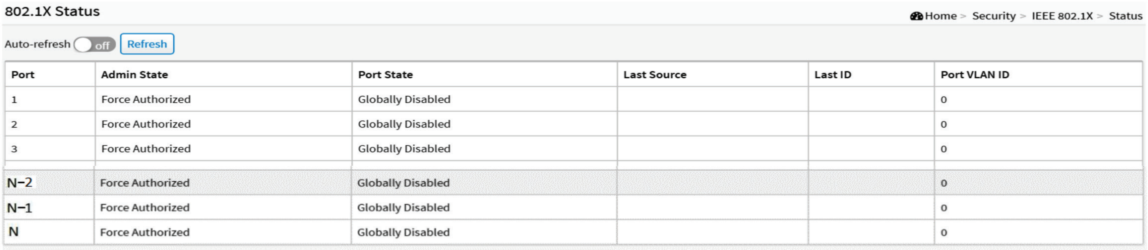
11.2.2 STATUS

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

WEB INTERFACE

To display 802.1X Status in the web interface:

1. Click Security, IEEE 802.1X and Status.
2. Check "Auto-refresh".
3. Click "Refresh" to refresh the detailed port statistics.
4. You can select the port for which you want to display 802.1X Statistics.



Port	Admin State	Port State	Last Source	Last ID	Port VLAN ID
1	Force Authorized	Globally Disabled			0
2	Force Authorized	Globally Disabled			0
3	Force Authorized	Globally Disabled			0
N-2	Force Authorized	Globally Disabled			0
N-1	Force Authorized	Globally Disabled			0
N	Force Authorized	Globally Disabled			0

FIGURE 11-6. IEEE 802.1X STATUS

PARAMETER DESCRIPTION

802.1X Status

- Port: The switch port number. Click to navigate to detailed 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.
- 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.

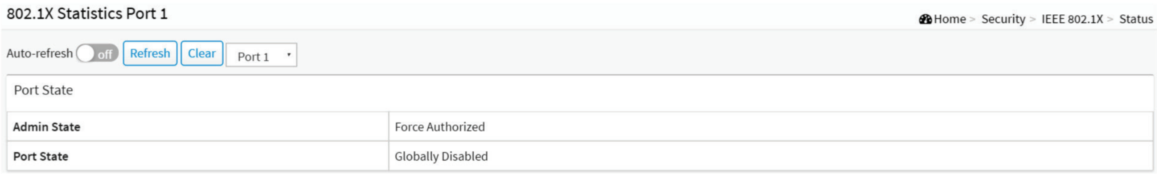
If the VLAN ID is assigned by the RADIUS server, "(RADIUS-assigned)" is appended to the VLAN ID.

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

Buttons

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

You can select port1 to display 802.1X Statistics.



Port State	
Admin State	Force Authorized
Port State	Globally Disabled

FIGURE 11-7. IEEE 802.1X STATISTICS PORT 1

PARAMETER DESCRIPTION

- Port: You can select the port for which 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

- 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.

11.3 IP SOURCE GUARD

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

11.3.1 CONFIGURATION

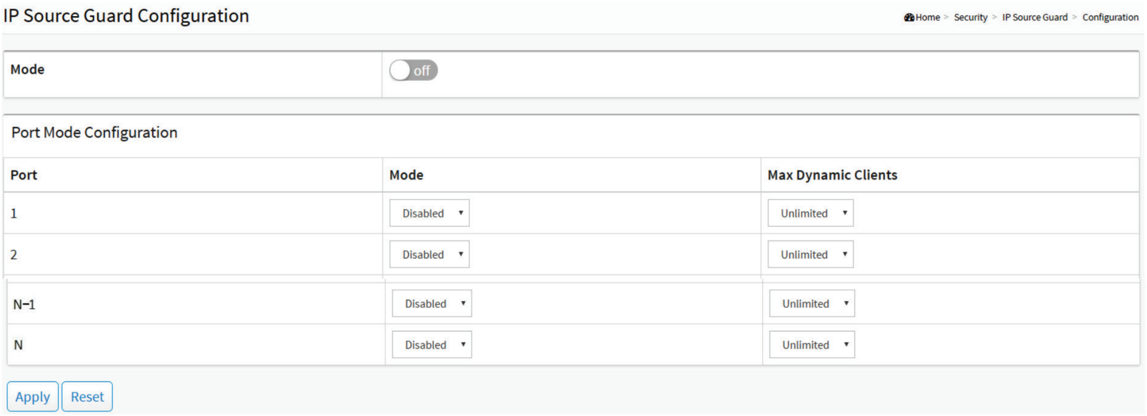
This section describes how to configure IP Source Guard setting including:

- Mode (Enabled and Disabled)
- Maximum Dynamic Clients (0, 1, 2, Unlimited)

WEB INTERFACE

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

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



IP Source Guard Configuration

Mode	off

Port Mode Configuration

Port	Mode	Max Dynamic Clients
1	Disabled	Unlimited
2	Disabled	Unlimited
N-1	Disabled	Unlimited
N	Disabled	Unlimited

FIGURE 11-8. 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 as enabled on selected 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 the IP packets that match static entries on the specific port are forwarded.

Buttons

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

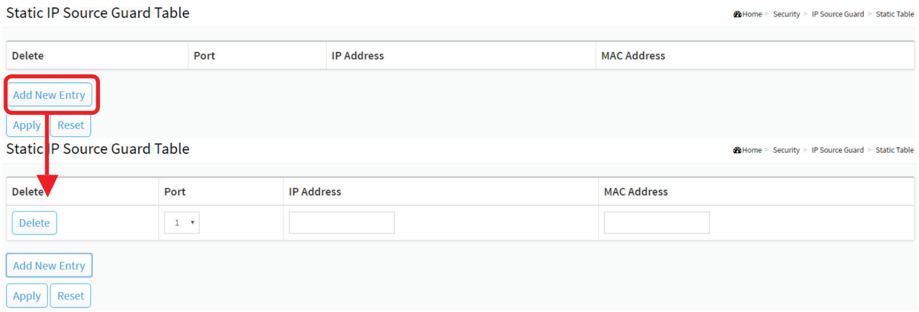
11.3.2 STATIC TABLE

This section describes how to configure the Static IP Source Guard Table parameters of the switch. You can use the Static IP Source Guard Table to manage the entries.

WEB INTERFACE

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

1. Click Security, IP Source Guard and Static Table.
2. Click “Add New Entry”.
3. Specify the Port, IP Address, and MAC address in the entry.
4. Click Apply.


Static IP Source Guard Table

Home > Security > IP Source Guard > Static Table

Delete	Port	IP Address	MAC Address

Static IP Source Guard Table

Home > Security > IP Source Guard > Static Table

Delete	Port	IP Address	MAC Address
Delete	1		

FIGURE 11-9. STATIC IP SOURCE GUARD TABLE

PARAMETER DESCRIPTION

- Port: The logical port 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.

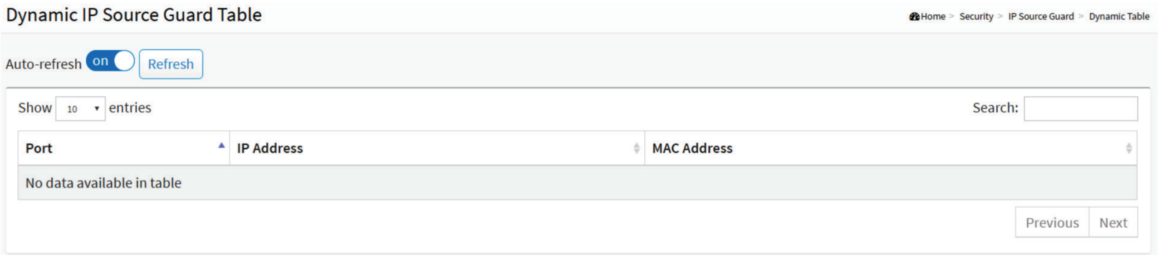
11.3.3 DYNAMIC TABLE

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. Check "Auto-refresh".
3. Click "Refresh" to refresh the detailed port statistics.
4. Specify the Start from port, IP Address, and entries per page.



Dynamic IP Source Guard Table

Home > Security > IP Source Guard > Dynamic Table

Auto-refresh on Refresh

Show 10 entries Search:

Port	IP Address	MAC Address
No data available in table		

Previous Next

FIGURE 11-10. DYNAMIC IP SOURCE GUARD TABLE

PARAMETER DESCRIPTION

- Port: Switch Port Number for which the entries are displayed.
- IP Address: User IP address of the entry.
- MAC Address: Source MAC address.
- 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

- Next: Updates the system log entries, turn to the next page.
- Previous: Updates the system log entries, turn to the previous page.
- Auto-refresh: Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.
- Refresh: Click to refresh the page immediately.

11.4 ARP INSPECTION

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

11.4.1 PORT CONFIGURATION

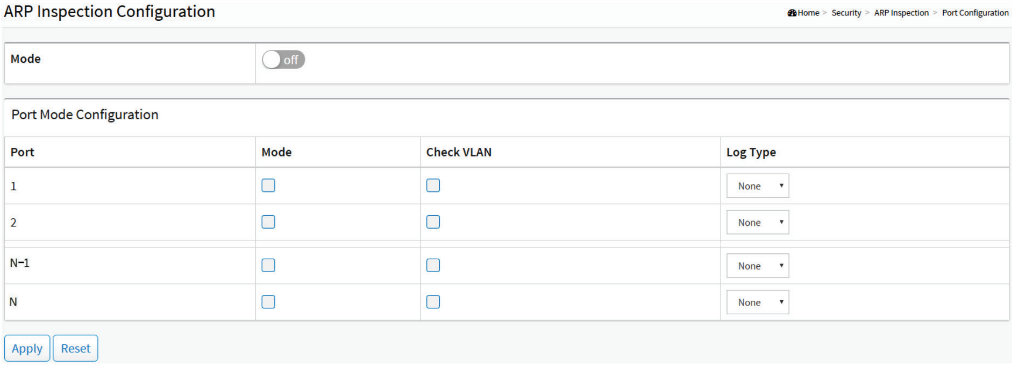
This section describes how to configure ARP Inspection setting including:

- 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 Port Configuration.
2. Select “on” in the Mode of ARP Inspection Configuration.
3. Select “Enable” for the specific port in the Mode of Port Mode Configuration.
4. Click Apply.



ARP Inspection Configuration

Mode	off

Port Mode Configuration

Port	Mode	Check VLAN	Log Type
1	□	□	None
2	□	□	None
N-1	□	□	None
N	□	□	None

FIGURE 11-11. 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 the ports that have ARP Inspection enabled. 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. When 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 when the Global Mode and Port Mode on a given port are enabled, and the setting of "Check VLAN" is disabled, will the log type of ARP Inspection refer to the port setting. There are four log types 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. When 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 when the Global Mode and Port Mode on a given port are enabled, and the setting of "Check VLAN" is disabled, will the log type of ARP Inspection refer to the port setting. There are four log types 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.

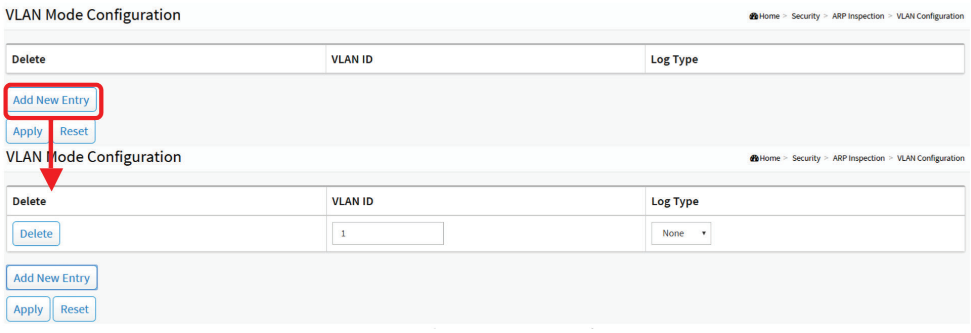
11.4.2 VLAN CONFIGURATION

Specify the VLANs that have ARP Inspection enabled.

WEB INTERFACE

To configure a VLAN Mode Configuration in the web interface:

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



VLAN Mode Configuration

Home > Security > ARP Inspection > VLAN Configuration

Delete	VLAN ID	Log Type

VLAN Mode Configuration

Home > Security > ARP Inspection > VLAN Configuration

Delete	VLAN ID	Log Type
Delete	1	None

FIGURE 11-12. VLAN MODE CONFIGURATION

PARAMETER DESCRIPTION

- VLAN Mode Configuration: Specify ARP Inspection enabled on 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.

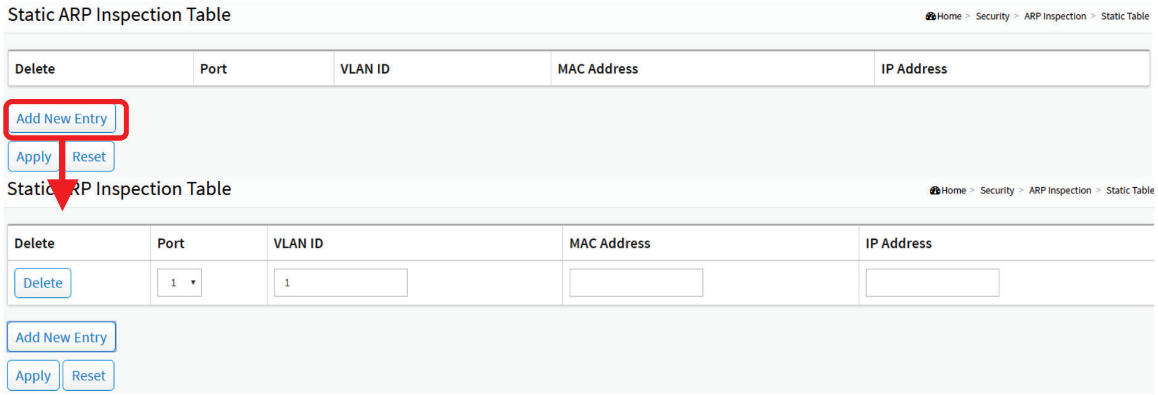
11.4.3 STATIC TABLE

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

WEB INTERFACE

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

1. Click Security, ARP Inspection and Static Table.
2. Click “Add new entry.”
3. Specify the Port, VLAN ID, IP Address, and MAC address in the entry.
4. Click Apply.



Static ARP Inspection Table

Delete	Port	VLAN ID	MAC Address	IP Address

Static ARP Inspection Table

Delete	Port	VLAN ID	MAC Address	IP Address
Delete	1 ▾	1		

Home > Security > ARP Inspection > Static Table
Add New Entry
Apply
Reset
Home > Security > ARP Inspection > Static Table
Add New Entry
Apply
Reset

FIGURE 11-13. 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.
- Adding new entry: Click to add a new entry to the Static ARP Inspection table. Specify the Port, VLAN ID, MAC address, and IP address for the new entry. Click “Apply.”

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.

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 1024 entries, and is sorted first by port, then by VLAN ID, then by MAC address, and then by IP address.

Navigating the ARP Inspection Table

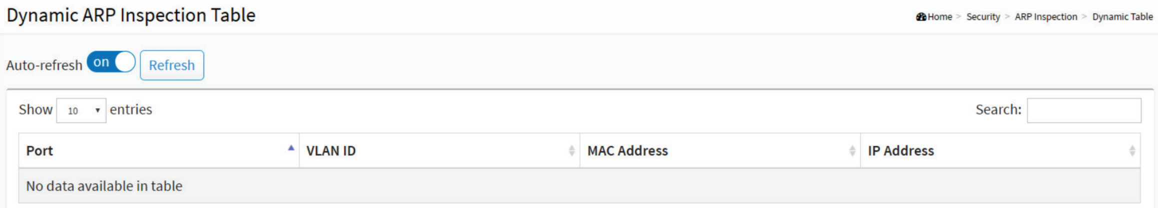
Each page shows many entries from the Dynamic ARP Inspection table, default is 10, selected through the “entries per page” input field. When first visited, the web page will show the first 10 entries from the beginning of the Dynamic ARP Inspection Table.

The “Search” input fields allow the user to select the starting point in the Dynamic ARP Inspection Table. It will update the displayed table starting from that or the closest next Dynamic ARP Inspection Table match.

The switch will use the last entry of the currently displayed table as a basis for the next lookup. When the end is reached, the text “No more entries” is shown in the displayed table. Use the button to start over.

WEB INTERFACE

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



Dynamic ARP Inspection Table

Port	VLAN ID	MAC Address	IP Address
No data available in table			

FIGURE 11-14. 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.
- Search: You can search for the information that you want to see.
- Show entries: You can choose how many items you want to show up.

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.

11.5 PORT SECURITY

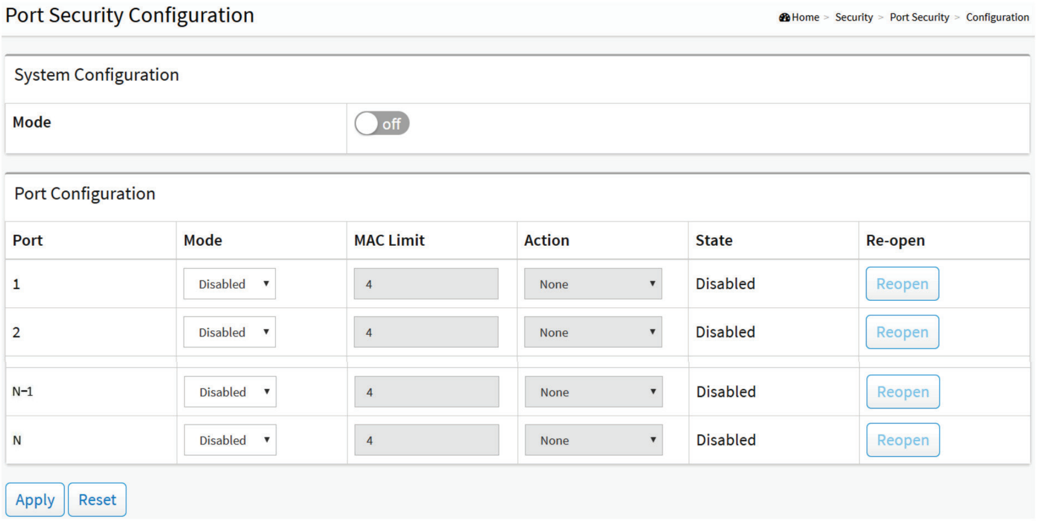
11.5.1 CONFIGURATION

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

WEB INTERFACE

To configure a Port Security Configuration in the web interface:

1. Click Security, Port Security and Configuration.
2. Select "Enabled" in the Mode of System Configuration.
3. Set Mode (Enabled, Disabled), MAC Limit, Action (Trap, Shutdown, Trap & Shutdown) for each port.
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.



Port Security Configuration

System Configuration

Mode	off

Port Configuration

Port	Mode	MAC Limit	Action	State	Re-open
1	Disabled	4	None	Disabled	Reopen
2	Disabled	4	None	Disabled	Reopen
N-1	Disabled	4	None	Disabled	Reopen
N	Disabled	4	None	Disabled	Reopen

FIGURE 11-15. PORT SECURITY CONFIGURATION

PARAMETER DESCRIPTION

System Configuration

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

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.

- MAC Limit: The maximum number of MAC addresses that can be secured on this port. This number cannot exceed 1024. If the limit is exceeded, the corresponding action is taken.

  The switch is "born" with a total number of MAC addresses from which all ports draw whenever a new MAC address is seen on a Port Security-enabled port. Since all ports draw from the same pool, it may happen that a configured maximum cannot be granted, if the remaining ports have already used all available MAC addresses.

- Action: If the Limit is reached, the switch can take one of the following actions:

  None: Do not allow more than Limit MAC addresses on the port, but take no further action.

  Trap: If Limit + 1 MAC addresses is seen on the port, send an SNMP trap. If Aging is disabled, only one SNMP trap will be sent, but with Aging enabled, new SNMP traps will be sent every time the limit gets exceeded.

  Shutdown: If Limit + 1 MAC addresses is seen on the port, shut down the port. This implies that all secured MAC addresses will be removed from the port, and no new address will be learned. Even if the link is physically disconnected and reconnected on the port (by disconnecting the cable), the port will remain shut down. There are three ways to re-open the port:

  1. Boot the switch,

  2. Disable and re-enable Limit Control on the port or the switch,

  3. Click the Reopen button.

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

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

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

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

  Limit Reached: Indicates that the limit is reached on this port. This state can only be shown if Action is set to none or Trap.

  Shutdown: Indicates that the port is shut down by the Limit Control module. This state can only be shown if Action is set to Shutdown or Trap & Shutdown.

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

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

Buttons

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

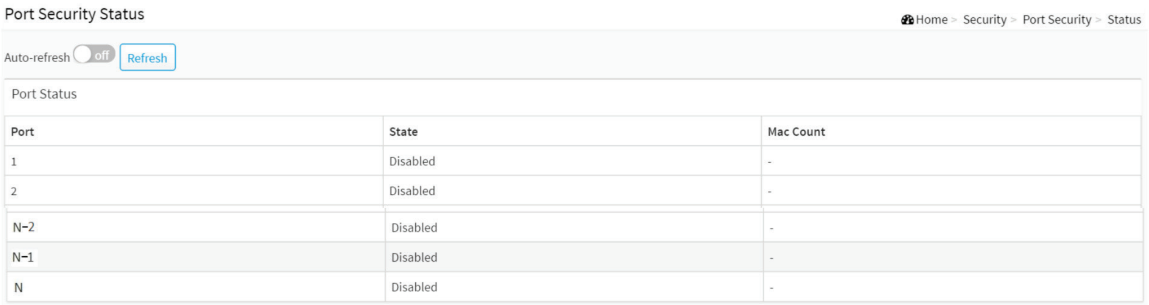
11.5.2 STATUS

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 display a Port Security Status in the web interface:

1. Click Security, Port Security and status.
2. Check “Auto-refresh.”
3. Click “Refresh” to refresh the port detailed statistics.
4. Click the port number to see the status for this particular port.



Port Security Status

Port Status

Port	State	Mac Count
1	Disabled	-
2	Disabled	-
N-2	Disabled	-
N-1	Disabled	-
N	Disabled	-

FIGURE 11-16. 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.
- 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 Learned): The columns indicate the number of currently learned MAC addresses (forwarding as well as blocked) and the number of MAC addresses that can be learned on the port, respectively.

  If no user modules are enabled on the port, the Current column will show a dash (-).

Buttons

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

11.6 RADIUS

11.6.1 CONFIGURATION

WEB INTERFACE

To configure a RADIUS in the web interface:

1. Click Security, RADIUS and Configuration.

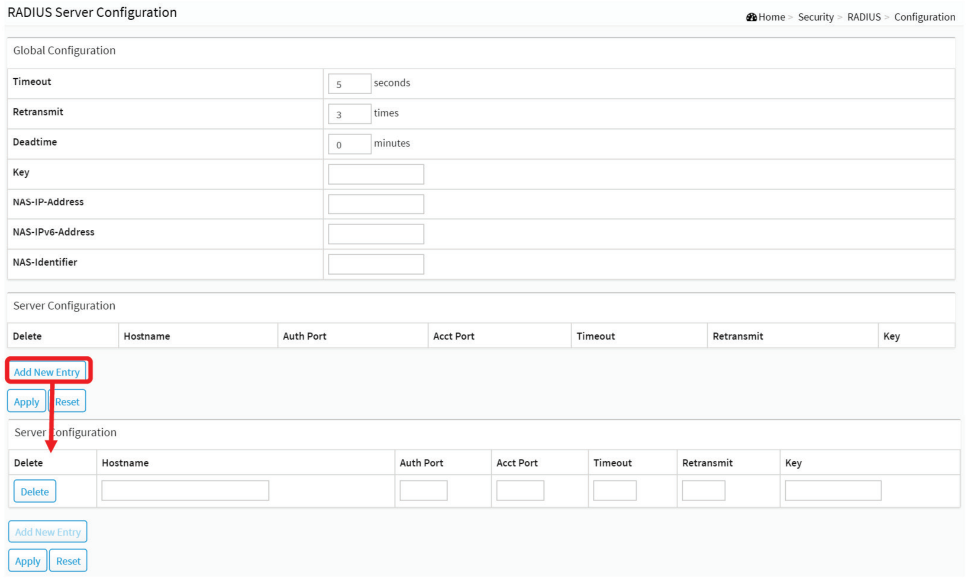
2. Set Timeout, Retransmit, Deadtime, Key, NAS-IP-Address, NAS IPv6-Address, NAS-Identifier.

3. Click "Add New Entry."

4. Set Hostname, Auth Port, Acct Port, Timeout, Retransmit, Key.

5. Click 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						

FIGURE 11-17. RADIUS CONFIGURATION

PARAMETER DESCRIPTION

Global Configuration

These settings are common for all of the RADIUS servers.

- Timeout: Timeout is the number of seconds, in the range 1 to 1000, to wait for a reply from a RADIUS server before retransmitting the request.
- Retransmit: Retransmit is the number of times, in the range 1 to 1000, a RADIUS request is retransmitted to a server that is not responding. If the server has not responded after the last retransmit, it is considered to be dead.
- Deadtime: Deadtime, which can be set to a number between 0 to 1440 minutes, is the period during which the switch will not send new requests to a server that has failed to respond to a previous request. This will stop the switch from continually trying to contact a server that it has already determined as dead. Setting the Deadtime to a value greater than 0 (zero) will enable this feature, but only if more than one server has been configured.

- Key: The secret key—up to 63 characters long—shared between the RADIUS server and the switch.
- NAS-IP-Address: 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:

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

Buttons

- Adding 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

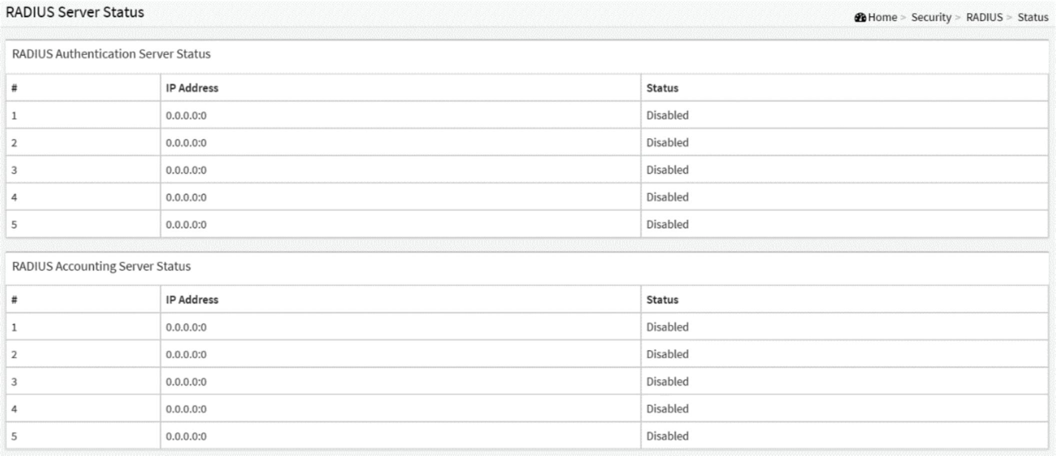
This section shows you an overview/detail of the RADIUS Authentication and Accounting servers' status to ensure the function is workable.

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

RADIUS Authentication Server Status

#	IP Address	Status
1	0.0.0.0:0	Disabled
2	0.0.0.0:0	Disabled
3	0.0.0.0:0	Disabled
4	0.0.0.0:0	Disabled
5	0.0.0.0:0	Disabled

RADIUS Accounting Server Status

#	IP Address	Status
1	0.0.0.0:0	Disabled
2	0.0.0.0:0	Disabled
3	0.0.0.0:0	Disabled
4	0.0.0.0:0	Disabled
5	0.0.0.0:0	Disabled

FIGURE 11-18. RADIUS SERVER STATUS OVERVIEW

PARAMETER DESCRIPTION

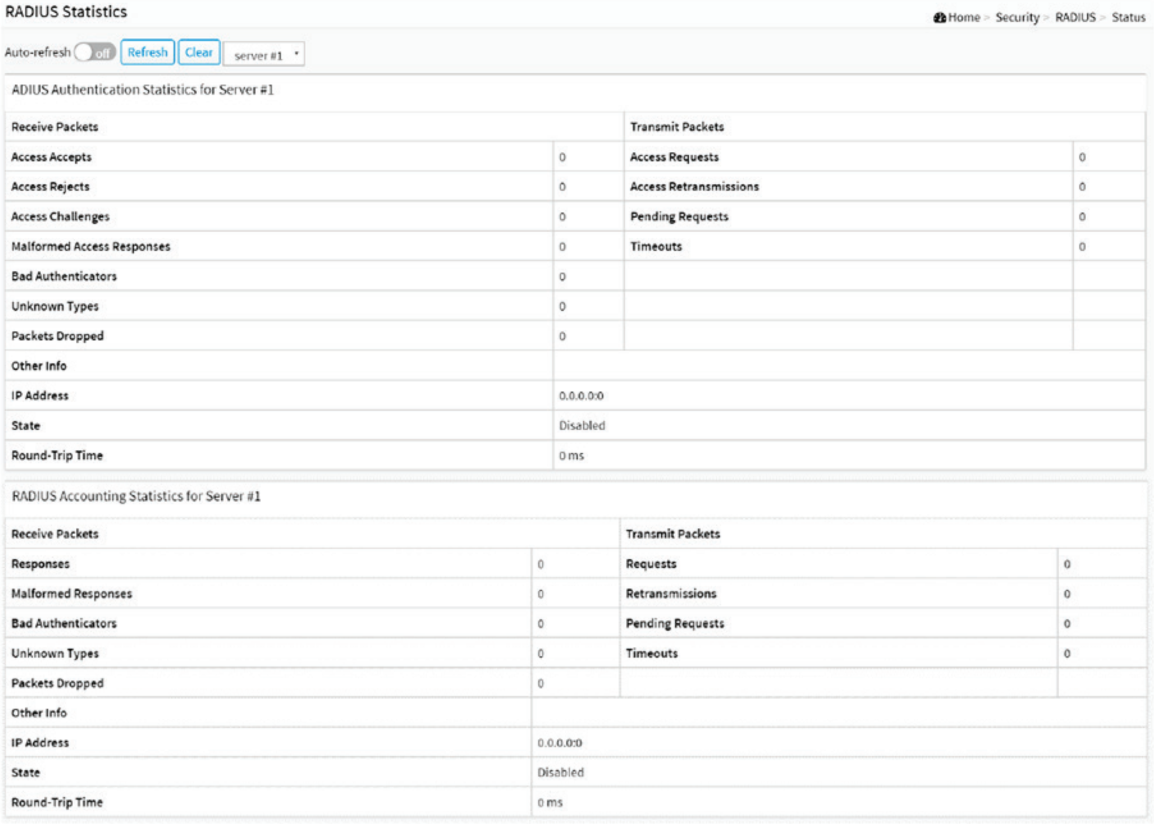
RADIUS Authentication Server Status

- #: The RADIUS server number. Click to navigate to detailed statistics for this server.
- IP Address: The IP address and UDP port number (in <IP Address>:<UDP Port> notation) of this server.
- State: The current state of the server. This field takes one of the following values:
  - Disabled: The server is disabled.
  - Not Ready: The server is enabled, but IP communication is not yet up and running.
  - Ready: The server is enabled, IP communication is up and running, and the RADIUS module is ready to accept access attempts.
  - Dead (X seconds left): Access attempts were made to this server, but it did not reply within the configured timeout. The server has temporarily been disabled, but will get re-enabled when the dead-time expires. The number of seconds left before this occurs is displayed in parentheses. This state is only reachable when more than one server is enabled.

RADIUS Accounting Server Status

- #: The RADIUS server number. Click to navigate to detailed statistics for this server.
- IP Address: The IP address and UDP port number (in <IP Address>:<UDP Port> notation) of this server.
- State: The current state of the server. This field takes one of the following values:
- Disabled: The server is disabled.
- Not Ready: The server is enabled, but IP communication is not yet up and running.
- Ready: The server is enabled, IP communication is up and running, and the RADIUS module is ready to accept accounting attempts.
- Dead (X seconds left): Accounting attempts were made to this server, but it did not reply within the configured timeout. The server has temporarily been disabled, but will get re-enabled when the dead-time expires. The number of seconds left before this occurs is displayed in parentheses. This state is only reachable when more than one server is enabled.

If you select Server#1 to display RADIUS Statistics



RADIUS Statistics

ADIUS 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	0.0.0.0:0		
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	0.0.0.0:0		
State	Disabled		
Round-Trip Time	0 ms		

FIGURE 11-19. RADIUS STATISTICS SERVER

PARAMETER DESCRIPTION

- server: You can select the server for which 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 Accept: 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 when it receives 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.

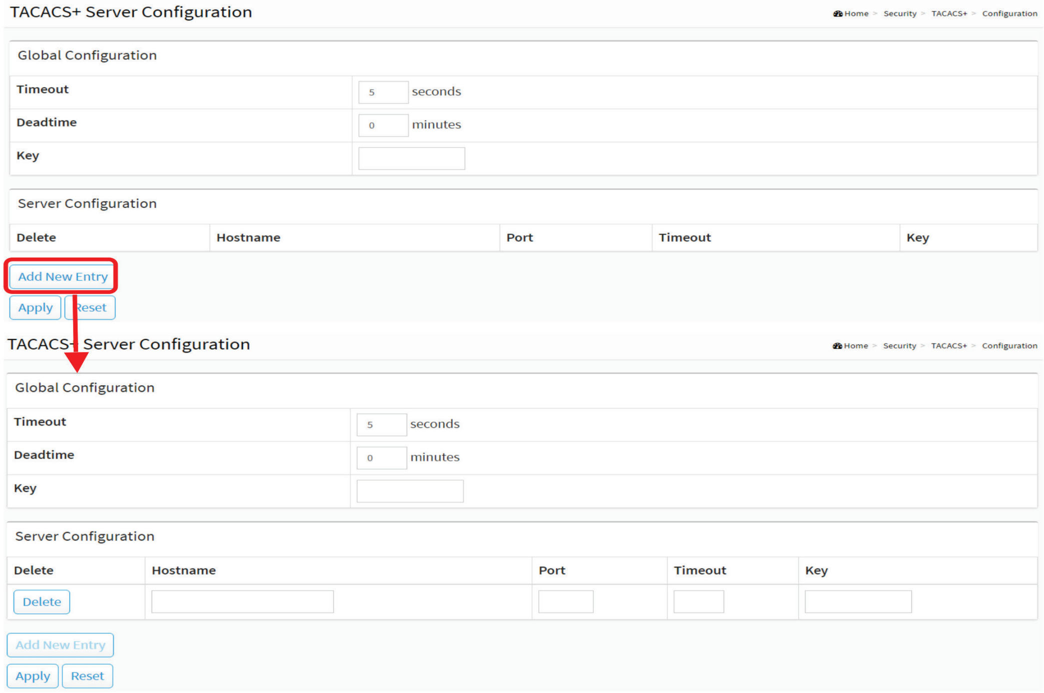
11.7 TACACS+

11.7.1 CONFIGURATION

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

Home > Security > TACACS+ > Configuration

Global Configuration

Timeout	5 seconds
Deadtime	0 minutes
Key	

Server Configuration

Delete	Hostname	Port	Timeout	Key

TACACS+ Server Configuration

Home > Security > TACACS+ > Configuration

Global Configuration

Timeout	5 seconds
Deadtime	0 minutes
Key	

Server Configuration

Delete	Hostname	Port	Timeout	Key
Delete				

FIGURE 11-20. 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.

12.1 ACCESS CONTROL LIST

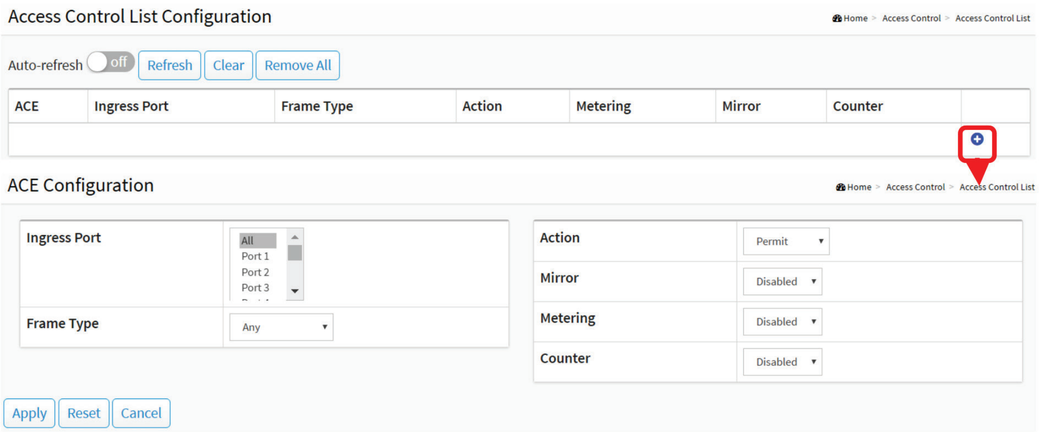
This section describes how to configure Access Control List rule. An Access Control List (ACL) is a sequential list of permit or deny conditions that apply to IP addresses, MAC addresses, or other more specific criteria. This switch tests ingress packets against the conditions in an ACL one by one. A packet will be accepted as soon as it matches a permit rule, or dropped as soon as it matches a deny rule. If no rules match, the frame is accepted. Other actions can also be invoked when a matching packet is found, including rate limiting, copying matching packets to another port or to the system log, or shutting down a port.

This page shows the Access Control List (ACL), which is made up of the ACEs defined on this switch. Each row describes the ACE that is defined. The maximum number of ACEs is 256 on each switch. Click on the lowest plus sign to add a new ACE to the list. The reserved ACEs used for internal protocol cannot be edited or deleted, the order sequence cannot be changed 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 an entry in the list).
3. To specify the parameter of the ACE.
4. Click Apply.
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.



Access Control List Configuration

Home > Access Control > Access Control List
Auto-refresh off
Refresh
Clear
Remove All

ACE	Ingress Port	Frame Type	Action	Metering	Mirror	Counter

ACE Configuration

Home > Access Control > Access Control List

Ingress Port	All Port 1 Port 2 Port 3
Frame Type	Any

Action	Permit
Mirror	Disabled
Metering	Disabled
Counter	Disabled

FIGURE 12-1. ACCESS CONTROL LIST AND ACE CONFIGURATION

PARAMETER DESCRIPTION

- ACE: The ACE number for the Access Control List.
- Ingress Port: Indicates the ingress port of the ACE.
- Frame Type: Indicates the frame type of the ACE. Possible values are:
  - Any: The ACE will match any frame type.
  - Ethernet Type: The ACE will match Ethernet Type frames. Note that an Ethernet Type based ACE will not get matched by IP and ARP frames.
  - IPv4: The ACE will match all IPv4 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.
  - Shutdown: Specify the port shutdown operation of the ACE.
- Metering: Select metering mode, enable or disable.
- Mirror: Select mirror mode, enable or disable.
- 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:

+ button: Inserts a new ACE before the current row.

pen button: Edits the ACE row.

x button: Deletes the ACE.

+ button: 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.

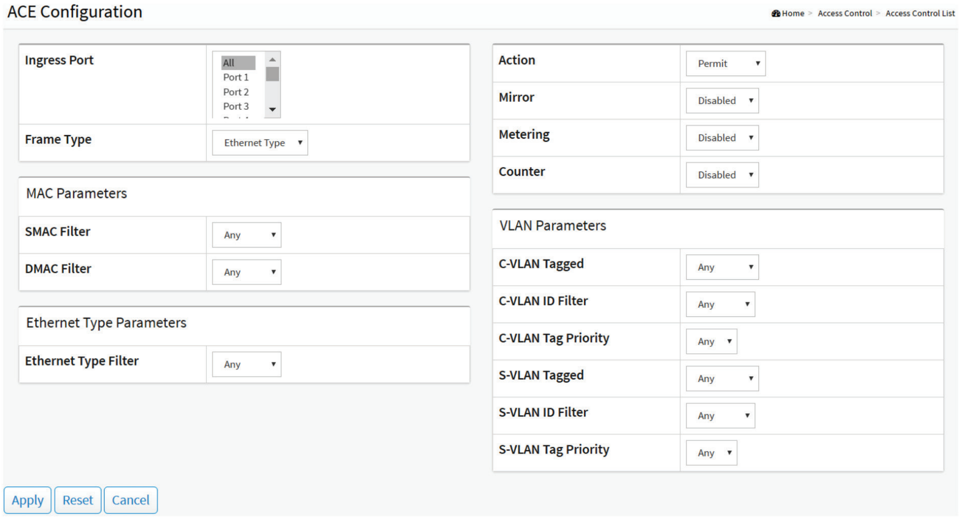
A frame that hits this ACE matches the configuration that is defined here.

- 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.
- 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).
  - IPv4: Only IPv4 frames can match this ACE. Notice the IPv4 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.
  - Shutdown: Specify the port shut down operation of the ACE.

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

- Metering: Select metering mode, enable or disable.
- Mirror: Select mirror mode, enable or disable.
- Counter: The counter indicates the number of times the ACE was hit by a frame.

Select Frame Type to Ethernet Type:



ACE Configuration

Ingress Port	All Port 1 Port 2 Port 3
Frame Type	Ethernet Type

MAC Parameters

SMAC Filter	Any
DMAC Filter	Any

Ethernet Type Parameters

Ethernet Type Filter	Any

Action	Permit
Mirror	Disabled
Metering	Disabled
Counter	Disabled

VLAN Parameters

C-VLAN Tagged	Any
C-VLAN ID Filter	Any
C-VLAN Tag Priority	Any
S-VLAN Tagged	Any
S-VLAN ID Filter	Any
S-VLAN Tag Priority	Any

FIGURE 12-2. ACE CONFIGURATION (SELECT FRAME TYPE TO ETHERNET TYPE)

MAC Parameters

- SMAC Filter: Specify the destination 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 destination MAC address with this ACE, choose this value. A field for entering a SMAC value appears.
- 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.

Ethernet Type Parameters

- Ethernet Type Filter: Specify the destination Ethernet Type filter for this ACE.
  - Any: No Ethernet Type filter is specified. (Ethernet Type filter status is “don’t-care”.)
  - Specific: If you want to filter a specific destination Ethernet Type with this ACE, choose this value. A field for entering a Ethernet Type value appears.

VLAN Parameters

- C-VLAN Tagged: Indicates tag type. Possible values are:

  - Any: Match tagged and untagged frames.

  - Enable: Match C-VLAN Tagged frames.

  - Disable: disable C-VLAN Tagged frames.

- C-VLAN ID Filter: Specify the C-VLAN ID filter for this ACE.

  - Any: No C-VLAN ID filter is specified. (C-VLAN ID filter status is “don’t-care”.)

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

- C-VLAN 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”.)

- S-VLAN Tagged: Indicates tag type. Possible values are:

  - Any: Match tagged and untagged frames.

  - Enable: Match S-VLAN Tagged frames.

  - Disable: disable S-VLAN Tagged frames.

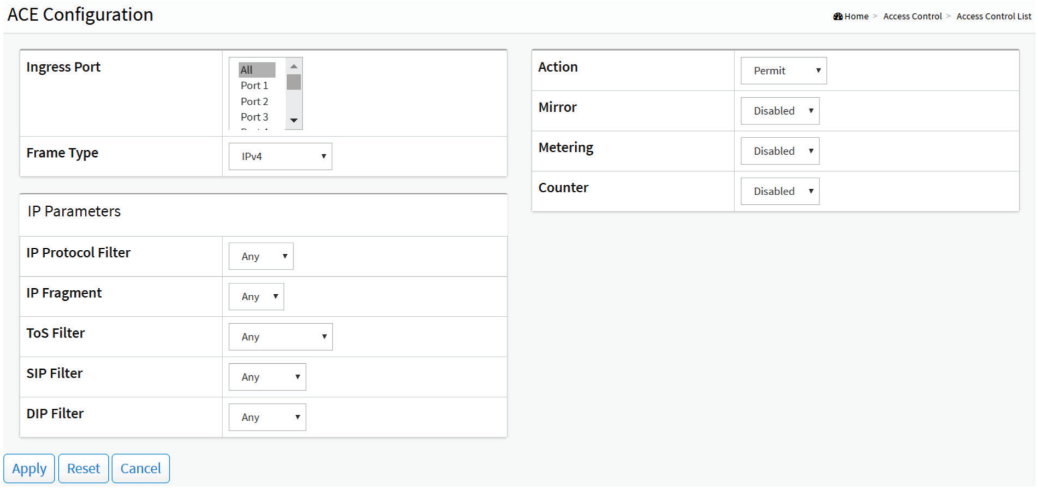
- S-VLAN ID Filter: Specify the S-VLAN ID filter for this ACE.

  - Any: No S-VLAN ID filter is specified. (S-VLAN ID filter status is “don’t-care”.)

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

- S-VLAN 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”.)

Select Frame Type to IPv4:



ACE Configuration

Ingress Port	All Port 1 Port 2 Port 3
Frame Type	IPv4

Action	Permit
Mirror	Disabled
Metering	Disabled
Counter	Disabled

IP Parameters

IP Protocol Filter	Any
IP Fragment	Any
ToS Filter	Any
SIP Filter	Any
DIP Filter	Any

FIGURE 12-3. ACE CONFIGURATION (SELECT FRAME TYPE TO IPV4)

IP Parameters

- IP Protocol Filter:
  - Any: The ACE will match any frame type.
  - ICMP: The ACE will match IPv4 frames with ICMP protocol.
  - UDP: The ACE will match IPv4 frames with UDP protocol.
  - TCP: The ACE will match IPv4 frames with TCP protocol.
  - Other: The ACE will match IPv4 frames, which are not ICMP/UDP/TCP.
- IP Fragment: IP Fragment IPv4 frame fragmented option: yes, no, any.
- ToS Filter: ToS Filter option: Any, DSCP, IP Precedence.
- SIP Filter: SIP Filter option: Any, Host, Network.
- DIP Filter: DIP Filter option: Any, Host, Network

Buttons

- Apply: Click to save changes.
- Reset: Click to undo any changes made locally and revert to previously saved values.
- Auto-refresh: Select auto-refresh to refresh the information automatically.
- Refresh, clear, Remove All: Click to refresh the ACL configuration or clear it by manual. Otherwise, remove all to clean up all ACL configurations on the table.
- Cancel: Return to the previous page.

12.2 ACCESS CONTROL STATUS

This section describes how to shows the Access Control Status for 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 because of hardware limitations. The maximum number of ACEs is 512 on each switch.

WEB INTERFACE

To To display the ACL status in the web interface:

1. Click Access Control and Access Control Status.
2. If you want to auto-refresh the information, then you need to select “Auto-refresh.”
3. Click “Refresh“ to refresh the ACL Status.

PARAMETER DESCRIPTION

- Port: The port number of the access control status.
- State: Shows the current state of the port. It can take one of two values:
  - None: The port is normally used.
  - Shutdown: The port is shut down by ACL rule.
- Re-open Button: To recover the shutdown port that triggered by ACL rule.

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 an SNMP agent, provided that the Management Information Base (MIB) is installed correctly on the managed devices. SNMP is a protocol that is used to govern the transfer of information between an SNMP manager and an agent and traverses the Object Identity (OID) of the management Information Base (MIB), described in the form of SMI syntax. An SNMP agent is running on the switch in response to the request issued by an 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”, the SNMP agent will start up. All supported MIB OIDs, including RMON MIB, can be accessed via the SNMP manager. If the field SNMP is set to “Disable”, the SNMP agent will be de-activated, and 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 an 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. An 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 you complete the setting, click the <Apply> button, and the setting takes effect.

WEB INTERFACE

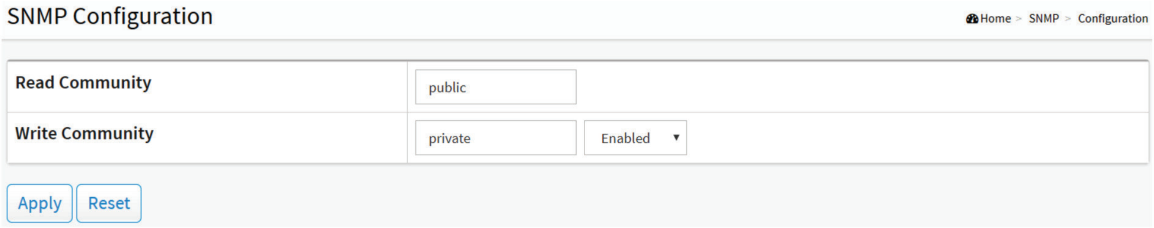
To configure the configure SNMP System in the web interface:

1. Click SNMP and configuration.

2. Select SNMP State to enable or disable the SNMP function.

3. Specify the Read Community, Write Community.

4. Click Apply.



SNMP Configuration

Read Community	public	
Write Community	private	Enabled ▾

FIGURE 13-1. SNMP CONFIGURATION

PARAMETER DESCRIPTION

- Read Community: Indicates the community read access string to permit access to an 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 the 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 a 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 an 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 the SNMP version is SNMPv1 or SNMPv2c. If the SNMP version is SNMPv3, the community string will be associated with an SNMPv3 communities table. It provides more flexibility to configure security name than an SNMPv1 or SNMPv2c community string. In addition to community string, a particular range of source addresses can be used to restrict source subnet.

Buttons

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

13.2 SNMPV3

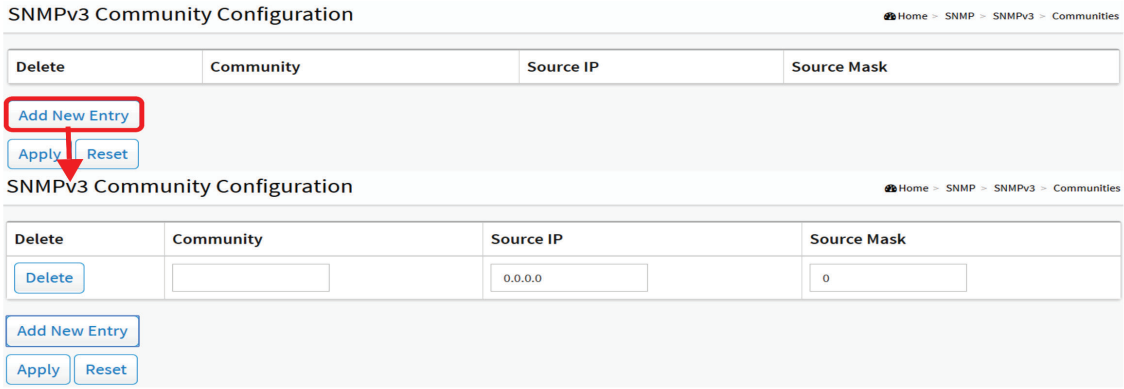
13.2.1 COMMUNITIES

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

WEB INTERFACE

To configure the configure SNMP Communities in the web interface:

1. Click SNMP, SNMPv3 and Communities.
2. Click Add new community.
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

Home > SNMP > SNMPv3 > Communities
Add New Entry
Apply
Reset
Home > SNMP > SNMPv3 > Communities
Add New Entry
Apply
Reset

FIGURE 13-2. SNMPV3 COMMUNITIES CONFIGURATION

PARAMETER DESCRIPTION

- Community: Indicates the community access string to permit access to an SNMPv3 agent. The allowed string length is 1 to 32, and the allowed content is ASCII characters from 33 to 126. The community string will be treated as security name and map a SNMPv1 or SNMPv2c community string.
- Source IP: Indicates the SNMP access source address. A particular range of source addresses can be used to restrict source subnet when combined with source mask.
- Source Mask: Indicates the SNMP access source address mask.

Buttons

- Add New Entry: Click to add a 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.

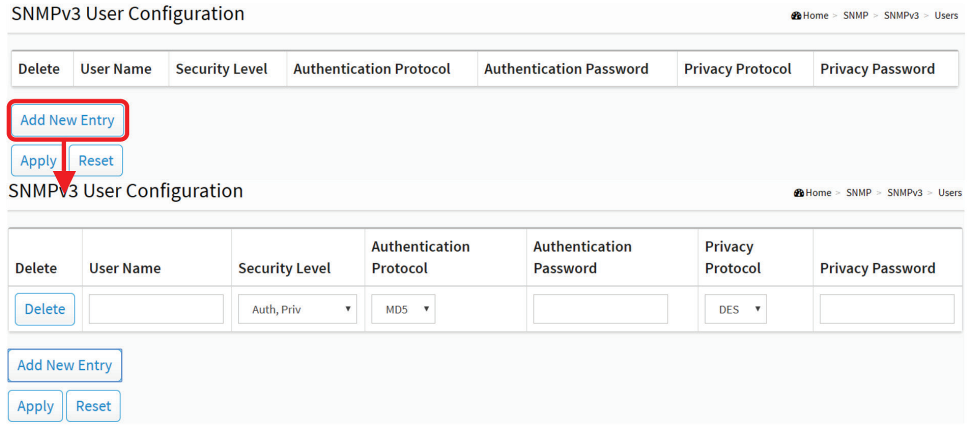
13.2.2 USERS

This function is used to configure SNMPv3 user. The Entry index key is UserName. To create a new UserName account, check the <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	User Name	Security Level	Authentication Protocol	Authentication Password	Privacy Protocol	Privacy Password

SNMPv3 User Configuration

Delete	User Name	Security Level	Authentication Protocol	Authentication Password	Privacy Protocol	Privacy Password
Delete		Auth, Priv	MD5		DES	

FIGURE 13-3. SNMPV3 USERS CONFIGURATION

PARAMETER DESCRIPTION

- User Name: A string identifying the user name that this entry should belong to. The allowed string length is 1 to 31, and the allowed content is ASCII characters from 33 to 126.
- Security Level: Indicates the security model that this entry should belong to. Possible security models are:

  - NoAuth, NoPriv: No authentication and no privacy.

  - Auth, NoPriv: Authentication and no privacy.

  - Auth, Priv: Authentication and privacy.

  The value of the security level cannot be modified if an 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 the security level cannot be modified if an entry already exists. That means you 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 a 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.

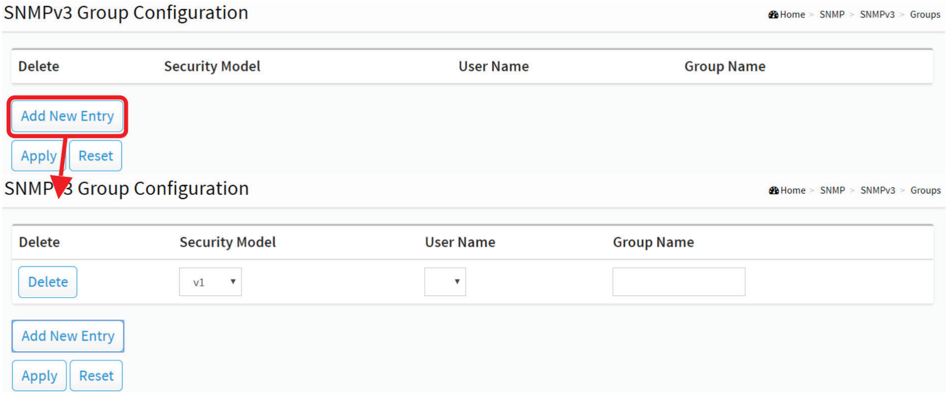
13.2.3 GROUPS

This function is used to configure an SNMPv3 group. The Entry index keys are Security Model and Security Name. To create a new group account, check the <Add new group> button, 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	User Name	Group Name

SNMPv3 Group Configuration

Delete	Security Model	User Name	Group Name
Delete	v1		

FIGURE 13-4. 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 a 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

This function is used to configure an SNMPv3 view. The Entry index keys are OID Subtree and View Name. To create a new view account, check the <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:

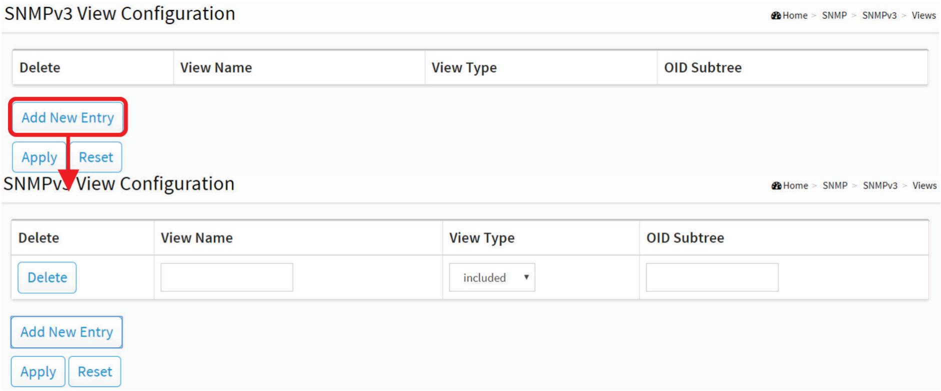
1. Click SNMP, SNMPv3 and Views.

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

Delete	View Name	View Type	OID Subtree

SNMPv3 View Configuration

Delete	View Name	View Type	OID Subtree
Delete		included	

FIGURE 13-5. 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 a 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

This function is used to configure SNMPv3 accesses. The Entry index keys are Group Name, Security Model and Security level. To create a new access account, check the <Add new access> button, enter the access information, then check <Apply>. Max Group Number : 12.

WEB INTERFACE

To display the configure SNMP Access in the web interface:

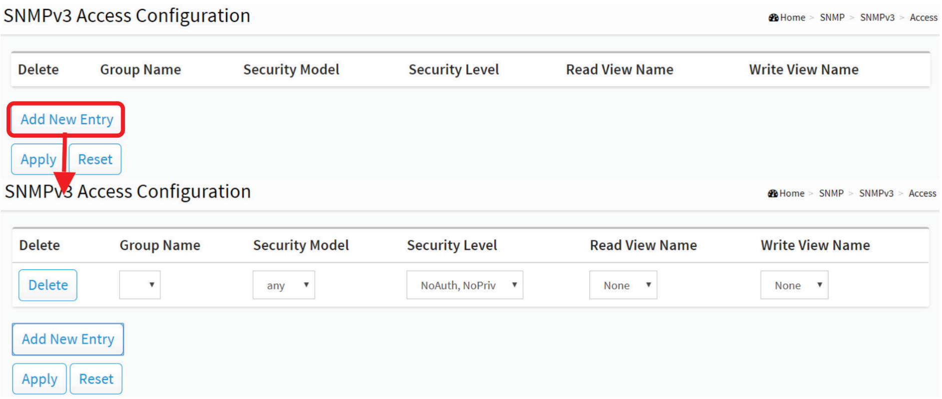
1. Click SNMP, SNMPv3 and Accesses.

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

Home > SNMP > SNMPv3 > Access

Delete	Group Name	Security Model	Security Level	Read View Name	Write View Name

SNMPv3 Access Configuration

Home > SNMP > SNMPv3 > Access

Delete	Group Name	Security Model	Security Level	Read View Name	Write View Name
Delete		any	NoAuth, NoPriv	None	None

FIGURE 13-6. 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 a 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 RMON CONFIGURATION

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

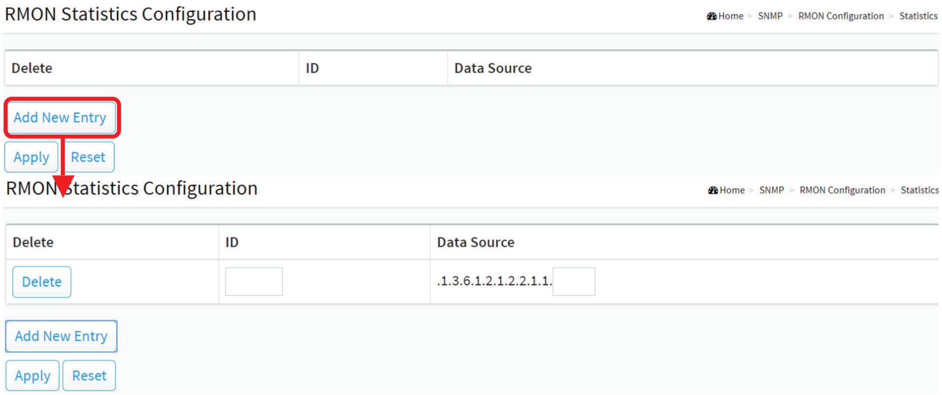
13.3.1 STATISTICS

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



RMON Statistics Configuration

Home > SNMP > RMON Configuration > Statistics

Delete	ID	Data Source

RMON Statistics Configuration

Home > SNMP > RMON Configuration > Statistics

Delete	ID	Data Source
Delete		.1.3.6.1.2.1.2.2.1.1.

FIGURE 13-7. 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 to monitor. If in a stacking switch, the value must add 1000*(switch ID-1), for example, if the port is switch 3 port 5, the value is 2005.

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.

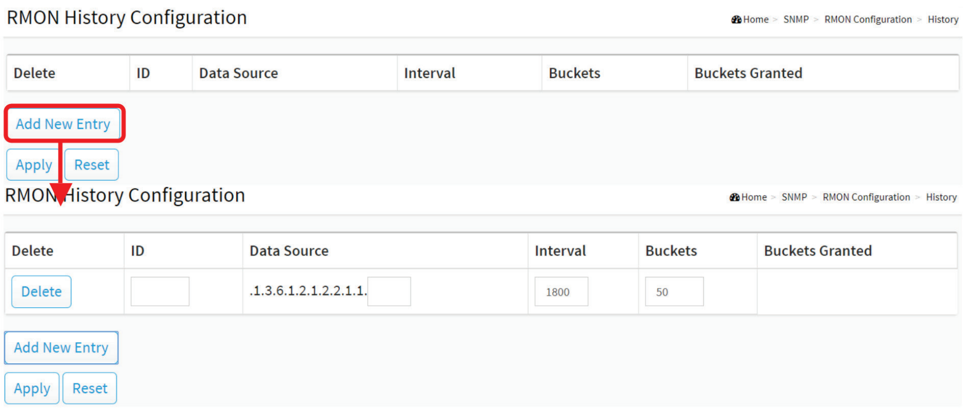
13.3.2 HISTORY

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


Home > SNMP > RMON Configuration > History
Add New Entry
Apply
Reset
Home > SNMP > RMON Configuration > History
Delete
Add New Entry
Apply
Reset

RMON History Configuration

Delete	ID	Data Source	Interval	Buckets	Buckets Granted

RMON History Configuration

Delete	ID	Data Source	Interval	Buckets	Buckets Granted
Delete		.1.3.6.1.2.1.2.2.1.1.	1800	50	

FIGURE 13-8. RMON HISTORY CONFIGURATION

PARAMETER DESCRIPTION

- User 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 to monitor. If in a stacking switch, the value must add 1000*(switch ID-1), for example, if the port is switch 3 port 5, the value is 2005
- Interval: Indicates the interval in seconds for sampling the history statistics data. The range is from 1 to 3600, default value is 1800 seconds.

- Buckets: Indicates the maximum data entries associated with this History control entry stored in RMON. The range is from 1 to 3600, default value is 50.
- Buckets Granted: The number of data that will 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.

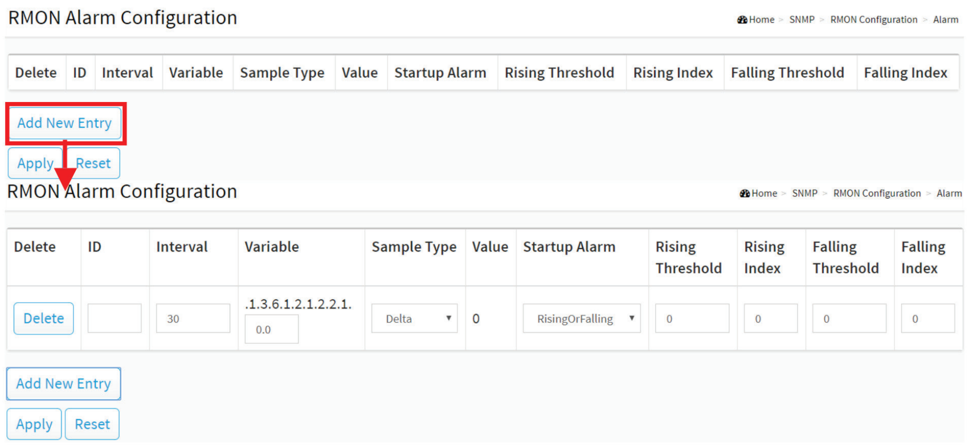
13.3.3 ALARM

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


Home > SNMP > RMON Configuration > Alarm
Add New Entry
Apply
Reset
Home > SNMP > RMON Configuration > Alarm
Add New Entry
Apply
Reset

RMON Alarm Configuration

Delete	ID	Interval	Variable	Sample Type	Value	Startup Alarm	Rising Threshold	Rising Index	Falling Threshold	Falling Index

RMON 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

FIGURE 13-9. 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 unicast packets delivered to a higher-layer protocol.

  - InNUcastPkts: The number of broadcast and multicast packets delivered to a higher-layer protocol.

- InDiscards: The number of inbound packets that are discarded even if 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 an unknown or unsupported protocol.

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

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

- OutNUcastPkts: The number of broadcast and multicast packets that request to transmit.

- OutDiscards: The number of outbound packets that are discarded even if the packets are normal.

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

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

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

- Absolute: Get the sample directly.

- Delta: Calculate the difference between samples (default).

- ◆ Value: The value of the statistic during the last sampling period.
- ◆ Startup Alarm: The method of sampling the selected variable and calculating the value to be compared against the thresholds; possible sample types are:

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

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

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

- ◆ Rising Threshold: Rising threshold value (-2147483648-2147483647).
- ◆ Rising Index: Rising event index (1-65535).
- ◆ Falling Threshold: Falling threshold value (-2147483648-2147483647)
- ◆ Falling Index: Falling event index (1-65535).

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.

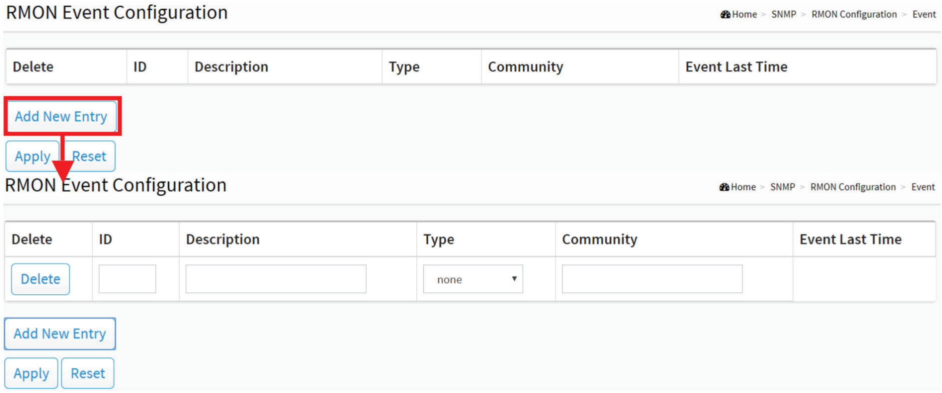
13.3.4 EVENT

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



RMON Event Configuration

Home > SNMP > RMON Configuration > Event

Delete	ID	Description	Type	Community	Event Last Time

Add New Entry
Apply
Reset

RMON Event Configuration

Home > SNMP > RMON Configuration > Event

Delete	ID	Description	Type	Community	Event Last Time
Delete			none		

Add New Entry
Apply
Reset

FIGURE 13-10. 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.
- Description: Indicates this event, the string length is from 0 to 127; default is a null string.
- Type: Indicates the notification of the event; the possible types are:
- None: No SNMP log is created, no SNMP trap is sent.
- Log: Create SNMP log entry when the event is triggered.
- Snmp trap: Send SNMP trap when the event is triggered.
- Log and trap: Create SNMP log entry and sent SNMP trap when the event is triggered.
- Community: Specify the community when trap is sent, the string length is from 0 to 127, default is “public”.
- Event Last Time: Indicates the value of sysUpTime at the time this event entry last generated an event.

Buttons

- Delete: Check to delete the entry. It will be deleted during the next save.
- Add New Entry: Click to add a new entry.
- Apply: Click to save changes.
- Reset: Click to undo any changes made locally and revert to previously saved values.

13.4 RMON STATUS

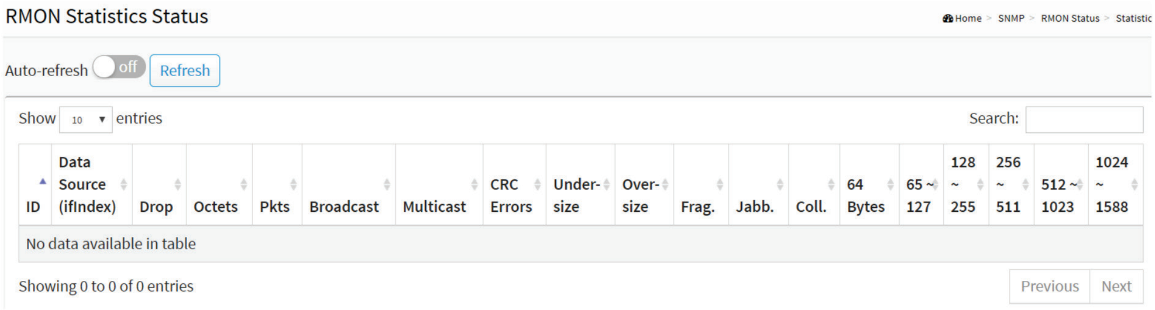
13.4.1 STATISTICS

This section provides an overview of RMON Statistics entries. Each page shows many entries from the Statistics table, default is 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 Statistics table. The first displayed will be the one with the lowest ID found in the Statistics table.

WEB INTERFACE

To display a RMON Statistics Status in the web interface:

1. Click SNMP, RMON Status and Statistics.
2. Specify the Port to check.
3. Check "Auto-refresh".
4. Click "Refresh" to refresh the port detailed statistics.



RMON Statistics Status

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 data available in table																		

Showing 0 to 0 of 0 entries

FIGURE 13-11. RMON STATISTICS STATUS

PARAMETER DESCRIPTION

- ID: Indicates the index of Statistics entry.
- Data Source (if Index): The port ID to monitor.
- Drop: The total number of events in which packets were dropped by the probe due to lack of resources.
- Octets: The total number of octets of data (including those in bad packets) received on the network.
- Pkts: The total number of packets (including bad packets, broadcast packets, and multicast packets) received.
- Broadcast: The total number of good packets received that were directed to the broadcast address.
- Multicast: The total number of good packets received that were directed to a multicast address.
- CRC Errors: The total number of packets received that had a length (excluding framing bits, but including FCS octets) of between 64 and 1518 octets, inclusive, but had either a bad Frame Check Sequence (FCS) with an integral number of octets (FCS Error) or a bad FCS with a non-integral number of octets (Alignment Error).
- Under-size: The total number of packets received that were less than 64 octets.
- Over-size: The total number of packets received that were longer than 1518 octets.
- Frag.: The number of frames with size less than 64 octets received with invalid CRC.
- Jabb : The number of frames with size 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

- 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.

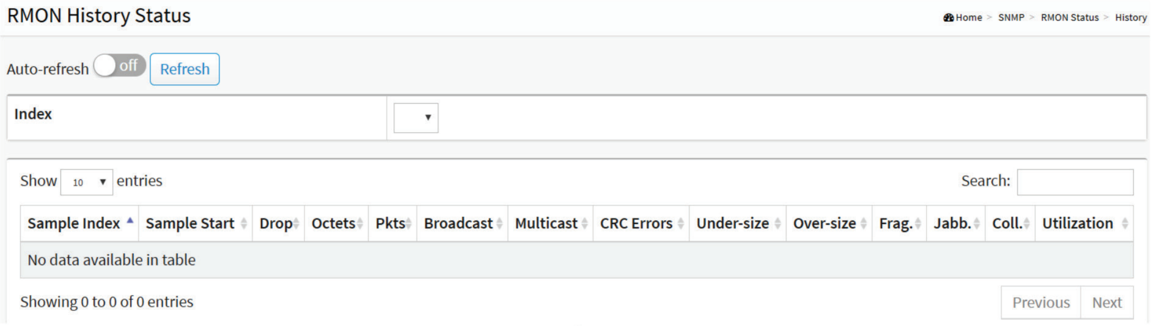
13.4.2 HISTORY

This section provides an overview of RMON History entries. Each page shows many entries from the History table, default is 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 History table. The first displayed will be the one with the lowest History Index and Sample Index found in the History table.

WEB INTERFACE

To display a RMON History Status in the web interface:

1. Click SNMP, RMON Status and History.
2. Check “Auto-refresh”.
3. Click “Refresh” to refresh the port detailed statistics.



RMON History Status

Index ▾

Show 10 ▾ entries

Search:

Sample Index	Sample Start	Drop	Octets	Pkts	Broadcast	Multicast	CRC Errors	Under-size	Over-size	Frag.	Jabb.	Coll.	Utilization
No data available in table													

Showing 0 to 0 of 0 entries

FIGURE 13-12. RMON HISTORY STATUS

PARAMETER DESCRIPTION

- 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 with size less than 64 octets received with invalid CRC.
- Jabb.: The number of frames with size 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.
- 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

- 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.

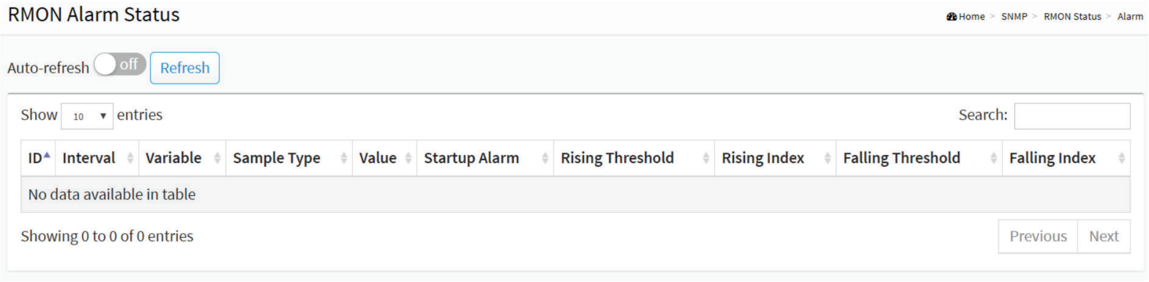
13.4.3 ALARM

This page provides an overview of RMON Alarm entries. Each page shows many entries from the Alarm table, default is 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 Alarm table. The first displayed will be the one with the lowest ID found in the Alarm table.

WEB INTERFACE

To display a RMON Alarm Status in the web interface:

1. Click SNMP, RMON Status and Alarm.
2. Check “Auto-refresh”.
3. Click “Refresh” to refresh the port detailed statistics



RMON Alarm Status

Home > SNMP > RMON Status > Alarm

Auto-refresh ○ off | Refresh

Show 10 ▾ entries | Search:

ID	Interval	Variable	Sample Type	Value	Startup Alarm	Rising Threshold	Rising Index	Falling Threshold	Falling Index
No data available in table									

Showing 0 to 0 of 0 entries | Previous | Next

FIGURE 13-13. 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.
- 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

- 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.

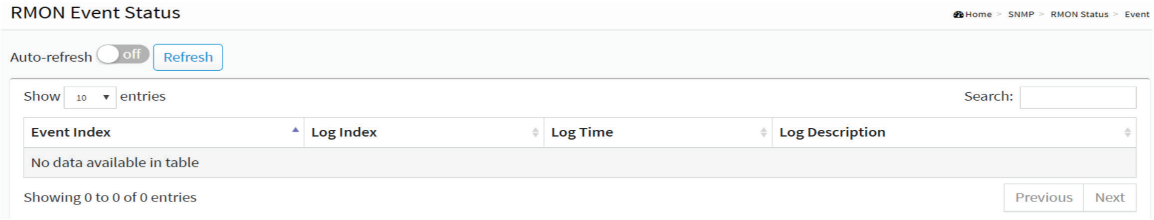
13.4.4 EVENT

This page provides an overview of RMON Event table entries. Each page shows many entries from the Event table, default is 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 Event table. The first displayed will be the one with the lowest Event Index and Log Index found in the Event table.

WEB INTERFACE

To display a RMON Event Status in the web interface:

1. Click SNMP, RMON Status and Event.
2. Check "Auto-refresh".
3. Click " Refresh" to refresh the port detailed statistics
4. Specify the Port to check.



Event Index	Log Index	Log Time	Log Description
No data available in table			

Showing 0 to 0 of 0 entries

FIGURE 13-14. 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.
- 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

- 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.

CHAPTER 14: EVENT NOTIFICATION

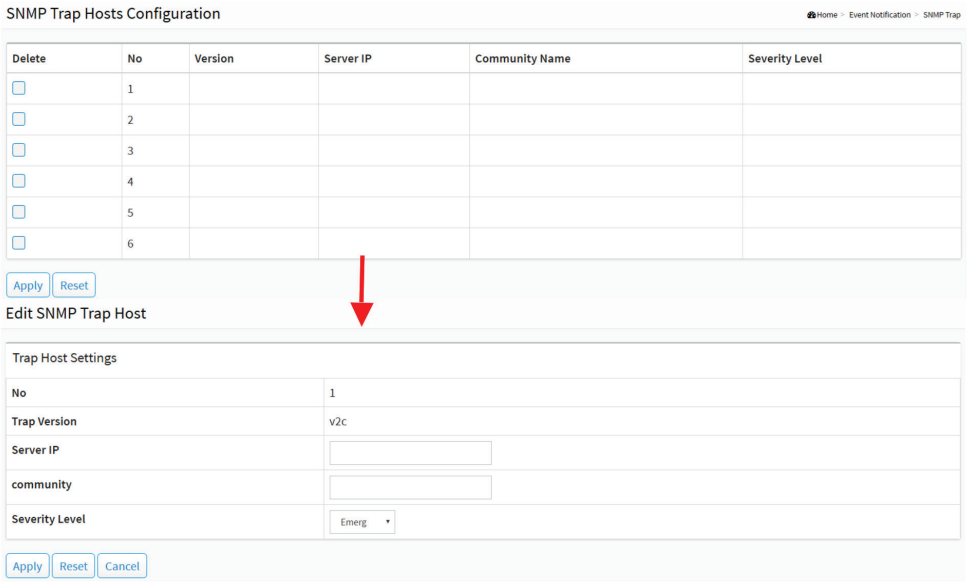
14.1 SNMP TRAP

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 any entry, then you can create a new SNMP Trap on the switch.
3. Specify Server IP Community, Severity Level.
4. Click Apply.



SNMP Trap Hosts Configuration

Delete	No	Version	Server IP	Community Name	Severity Level
□	1				
□	2				
□	3				
□	4				
□	5				
□	6				

Edit SNMP Trap Host

Trap Host Settings

No	1
Trap Version	v2c
Server IP	
community	
Severity Level	Emerg

FIGURE 14-1. SNMP TRAP CONFIGURATION

PARAMETER DESCRIPTION

- No: The index of the trap host entry.
- Version: Indicates the SNMP trap supported version. Possible versions are: SNMP v2c: Set SNMP trap supported version 2c.
- Server IP: This is the IP of the trap host.
- Community Name: Indicates the community access string when sending an SNMP trap packet. The allowed string length is 0 to 255, and the allowed content is ASCII characters from 33 to 126.
- Severity Level: Indicates what kind of message will send to the trap server. Possible modes are:

  - Emerg: System is unusable.

  - Alert: Action must be taken immediately.

  - Crit: Critical conditions.

  - Error: Error conditions.

  - Warning: Warning conditions.

  - Notice: Normal but significant conditions.

  - Info: Information messages.

- Debug: Debug-level messages.

Buttons

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

14.2 SYSLOG

14.2.1 SYSLOG CONFIGURATION

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

WEB INTERFACE

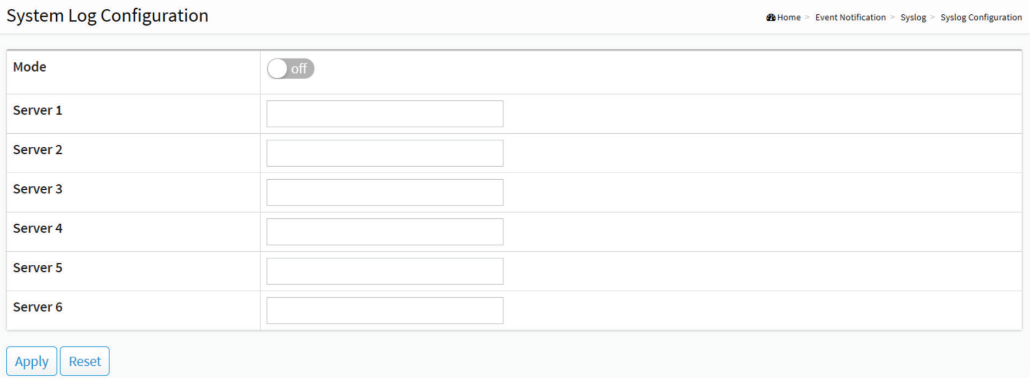
To configure Syslog Configuration in the web interface:

1. Click Event Notification, Syslog and Syslog Configuration.

2. Specify the syslog parameters, including the IP Address of the Syslog server and the Port number.

3. Enable the Syslog.

4. Click Apply.



Mode	off
Server 1	
Server 2	
Server 3	
Server 4	
Server 5	
Server 6	

FIGURE 14-2. SYSTEM LOG CONFIGURATION

PARAMETER DESCRIPTION

- Mode: Indicates the server mode operation. When the mode operation is enabled, the syslog message will send out to the 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 to the 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:

  - On: Enable server mode operation.
  - Off: Disable server mode operation.

- Server 1 to 6: Indicates the IPv4 hosts address of the syslog server. If the switch provides a DNS feature, it also can be a host name.

Buttons

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

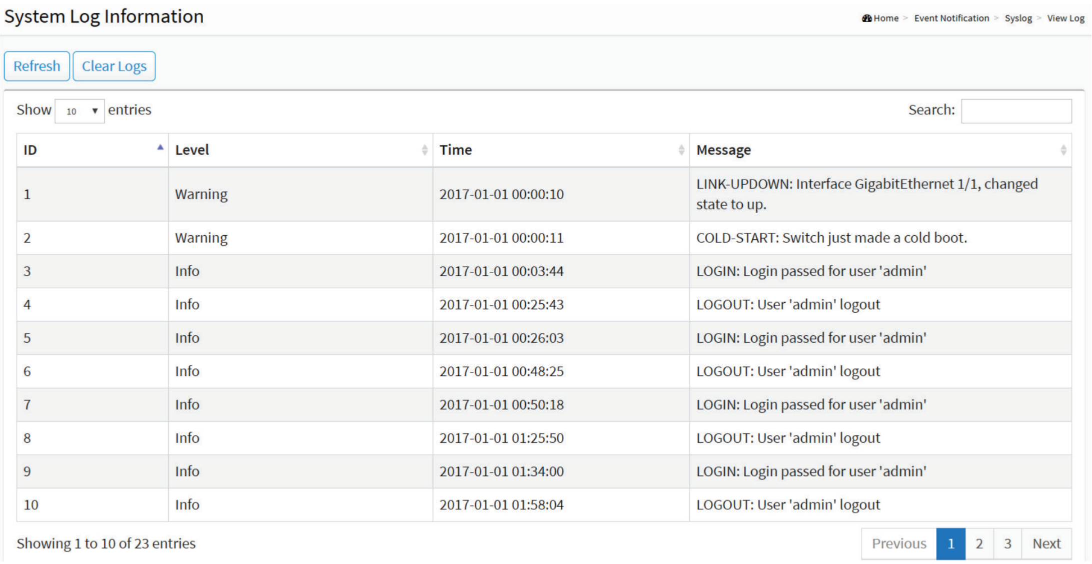
14.2.2 VIEW LOG

This section describes how to display the system log information of the switch.

WEB INTERFACE

To display the log Information in the web interface:

1. Click Event Notification, Syslog and View Log.
2. Display the log information.



ID	Level	Time	Message
1	Warning	2017-01-01 00:00:10	LINK-UPDOWN: Interface GigabitEthernet 1/1, changed state to up.
2	Warning	2017-01-01 00:00:11	COLD-START: Switch just made a cold boot.
3	Info	2017-01-01 00:03:44	LOGIN: Login passed for user 'admin'
4	Info	2017-01-01 00:25:43	LOGOUT: User 'admin' logout
5	Info	2017-01-01 00:26:03	LOGIN: Login passed for user 'admin'
6	Info	2017-01-01 00:48:25	LOGOUT: User 'admin' logout
7	Info	2017-01-01 00:50:18	LOGIN: Login passed for user 'admin'
8	Info	2017-01-01 01:25:50	LOGOUT: User 'admin' logout
9	Info	2017-01-01 01:34:00	LOGIN: Login passed for user 'admin'
10	Info	2017-01-01 01:58:04	LOGOUT: User 'admin' logout

Showing 1 to 10 of 23 entries

FIGURE 14-3. 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

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

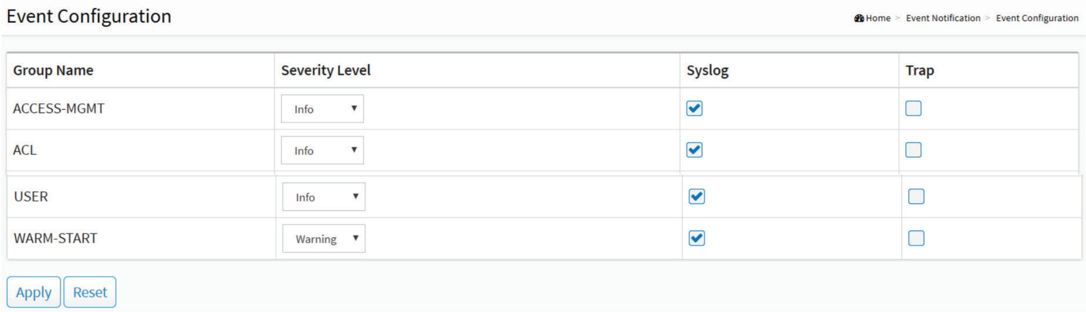
14.3 EVENT CONFIGURATION

This page displays the current trap event severity configuration. 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 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.



Event Configuration

Group Name	Severity Level	Syslog	Trap
ACCESS-MGMT	Info	☑	□
ACL	Info	☑	□
USER	Info	☑	□
WARM-START	Warning	☑	□

FIGURE 14-4. EVENT CONFIGURATION

PARAMETER DESCRIPTION

- Group Name: The name identifying the severity group.
- Severity Level: Every group has a severity level. The following level types are supported:

<0> 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.

Buttons

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

CHAPTER 15: DIAGNOSTICS

This chapter provides a set of basic system diagnosis. These includes Ping, Traceroute, Cable Diagnostics and port mirror.

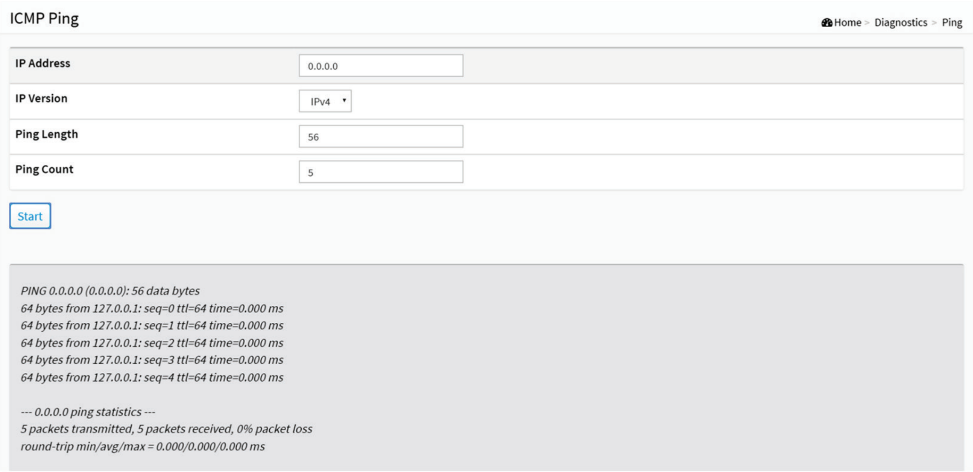
15.1 PING

This section allows you to issue ICMP PING packets to troubleshoot IPv6 connectivity issues.

WEB INTERFACE

To configure a PING in the web interface:

1. Click Diagnostics and Ping.
2. Specify IP Address, IP Version, Ping Length and Ping Count.
3. Click Start.



IP Address	0.0.0.0
IP Version	IPv4 ▾
Ping Length	56
Ping Count	5

```
PING 0.0.0.0 (0.0.0.0): 56 data bytes
64 bytes from 127.0.0.1: seq=0 ttl=64 time=0.000 ms
64 bytes from 127.0.0.1: seq=1 ttl=64 time=0.000 ms
64 bytes from 127.0.0.1: seq=2 ttl=64 time=0.000 ms
64 bytes from 127.0.0.1: seq=3 ttl=64 time=0.000 ms
64 bytes from 127.0.0.1: seq=4 ttl=64 time=0.000 ms

--- 0.0.0.0 ping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max = 0.000/0.000/0.000 ms
```

FIGURE 15-1. ICMP PING SCREEN

PARAMETER DESCRIPTION

- IP Address: Specify the target IP Address of the Ping.
- IP Version: Select the IP Version.
- Ping Length: The payload size of the ICMP packet. Values range from 1 byte to 1452 bytes.
- Ping Count: The count of the ICMP packet. Values range from 1 time to 60 times.
- Start: Click the “Start” button to start to ping the target IP Address.

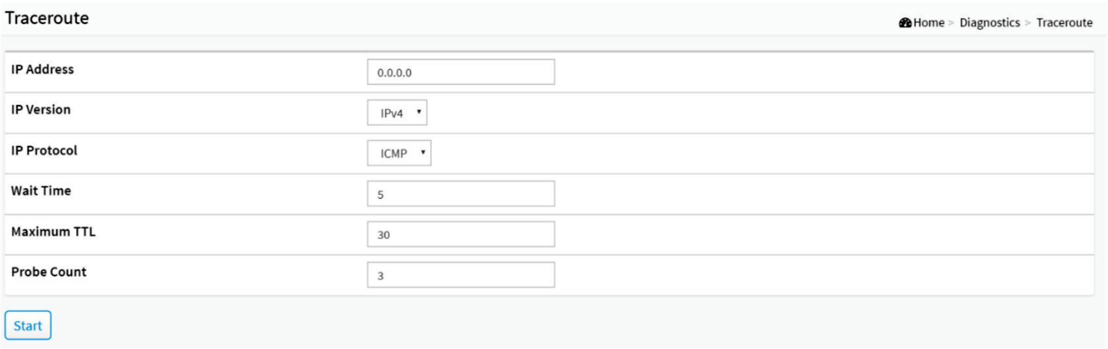
15.2 TRACEROUTE

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:

1. Click Diagnostics and Traceroute.
2. Specify IP Address, IP Version, IP Protocol, traceroute Size.
3. Click Start.



Traceroute

IP Address	0.0.0.0
IP Version	IPv4
IP Protocol	ICMP
Wait Time	5
Maximum TTL	30
Probe Count	3

FIGURE 15-2. TRACEROUTE SCREEN

PARAMETER DESCRIPTION

- IP Address: The destination IP Address.
- IP Version: Set the IP Version that you want.
- Protocol: The protocol (ICMP, UDP, TCP) packets to send.
- 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.
- Maximum 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.

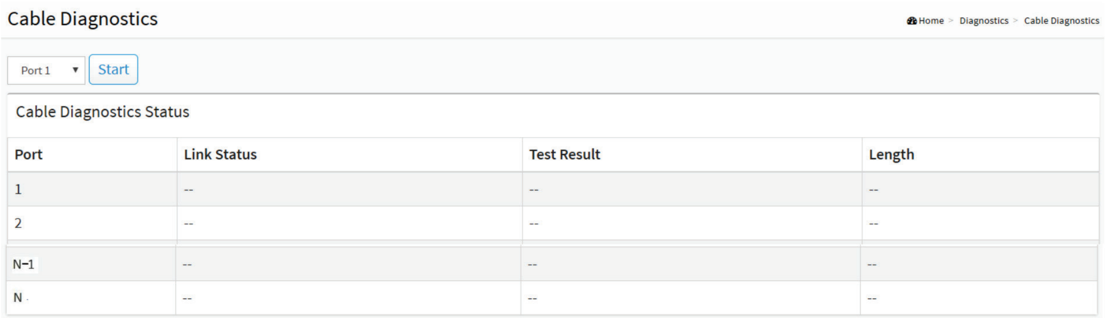
15.3 CABLE DIAGNOSTICS

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 the Port to check.
3. Click Start.



Cable Diagnostics Status

Port	Link Status	Test Result	Length
1	--	--	--
2	--	--	--
N-1	--	--	--
N	--	--	--

FIGURE 15-3. CABLE DIAGNOSTICS

PARAMETER DESCRIPTION

- Port: The port where you are requesting Cable Diagnostics.

Cable Status

- Port: Port number.
- Link Status: Provides the current link speed of the port.
- Test Result: The status of the cable pair.
- Length: The length (in meters) of the cable pair.

Button

- Start: Start the cable diagnostics for the port that you selected.

15.4 MIRROR

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

Mirror Configuration monitors the traffic of the network. For example, we assume that Port A and Port B are a Monitoring Port and a 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:

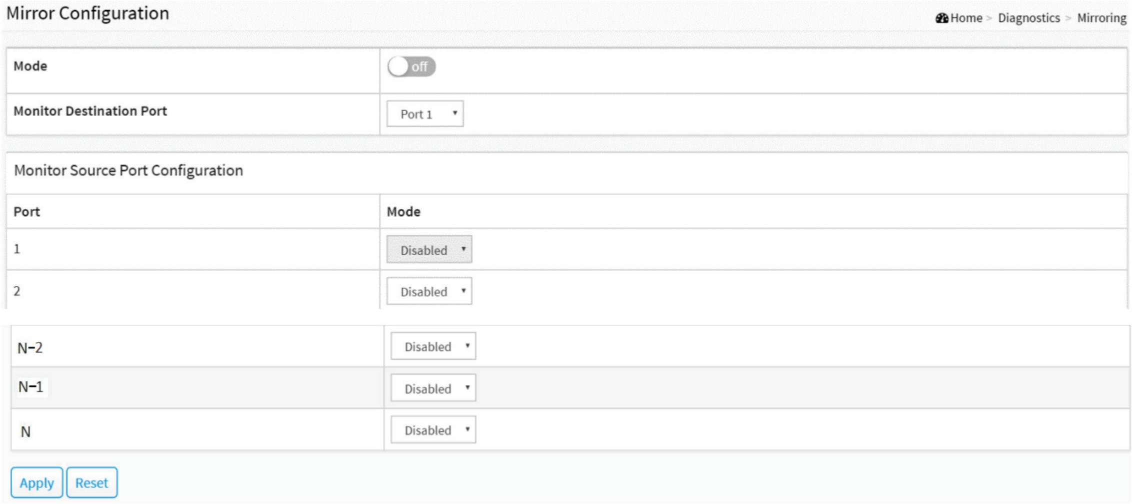
1. Click Diagnostics and Mirroring.

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

Mode	off
Monitor Destination Port	Port 1

Monitor Source Port Configuration

Port	Mode
1	Disabled
2	Disabled
N-2	Disabled
N-1	Disabled
N	Disabled

FIGURE 15-4. MIRROR CONFIGURATION

PARAMETER DESCRIPTION

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

  on: Enable Mirror mode operation.

  off: Disable Mirror mode operation.

- 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.

CHAPTER 16: MAINTENANCE

This chapter describes the entire Maintenance configuration tasks including Save/Backup/Restore/Activate/Delete Restart Device, Factory Defaults, Firmware upgrade.

16.1 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.

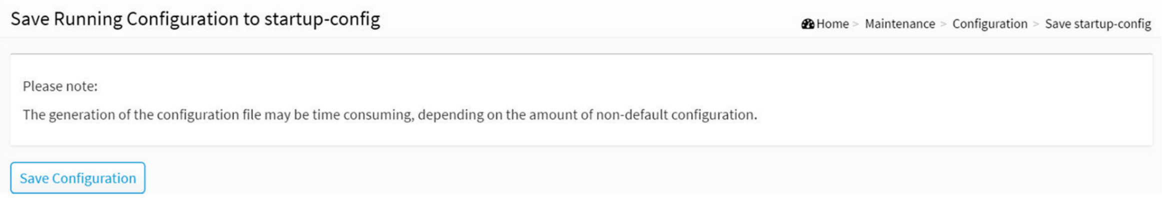
16.1.1 SAVE STARTUP-CONFIG

This copies 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 to startup-config

Please note:

The generation of the configuration file may be time consuming, depending on the amount of non-default configuration.

FIGURE 16-1. 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.

16.1.2 BACKUP

This section describes how to export the Switch Configuration for maintenance needs. Any current configuration files will be exported as text format.

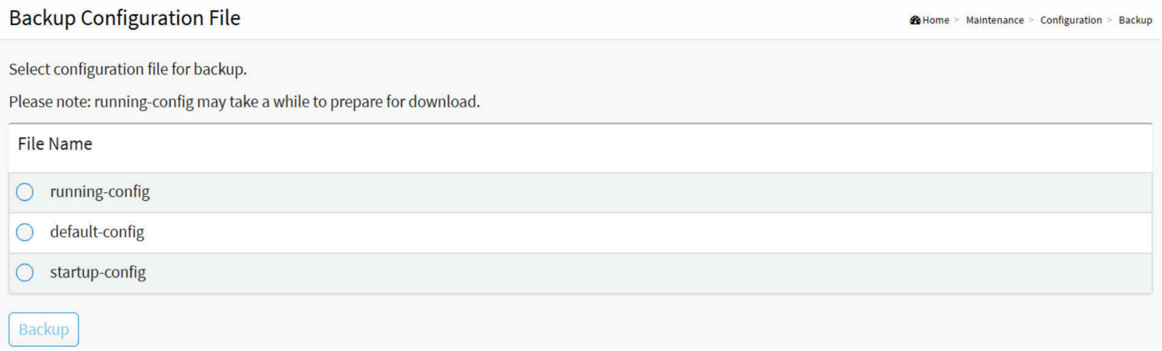
The configuration files on the switch can be backed up and saved on the station running the web browser.

You can transfer any of the files on the switch to the web browser. Selecting 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 File

Select configuration file for backup.

Please note: running-config may take a while to prepare for download.

File Name

○ running-config

○ default-config

○ startup-config

FIGURE 16-2. 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

- Backup: Click the “Backup” button, then the switch will start to transfer the configuration file to your workstation.

16.1.3 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:

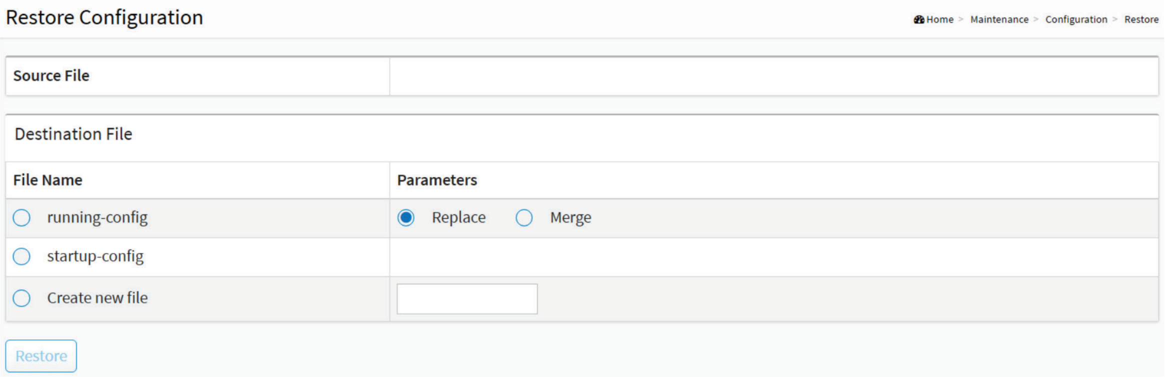
- Replace mode: The current configuration is fully replaced with the configuration specified in the source file.
- Merge mode: The source file configuration is merged into running-config.

WEB INTERFACE

To restore configuration in the web interface:

1. Click Maintenance, Configuration and Restore.

2. Click Restore.



Restore Configuration

Source File

Destination File

File Name	Parameters
○ running-config	● Replace ○ Merge
○ startup-config	
○ Create new file	

FIGURE 16-3. RESTORE CONFIG

PARAMETER DESCRIPTION

There are two system files:

1. running-config: A virtual file that represents the currently active configuration on the switch. This file is volatile.

2. startup-config: The startup configuration for the switch, read at boot time.

Parameter description:

Buttons

- Browse: Click the “Browse” button to search the configuration text file and filename.
- Restore: Click the “Restore” button to start transfer the source file to the destination file.

16.1.4 ACTIVATE CONFIG

You can activate any of the configuration files present on the switch, except for running-config, which represents the currently active configuration.

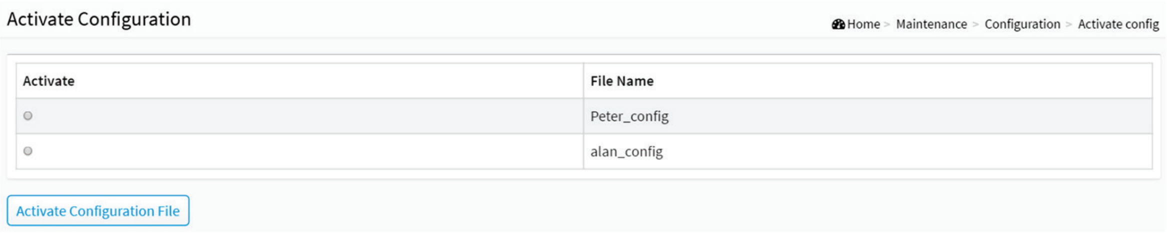
Select the file to activate and click. This will initiate the process of completely replacing the existing configuration with that of the selected file.

WEB INTERFACE

To activate configuration in the web interface:

1. Click Maintenance, Configuration and Activate config..

2. Click Activate Select.


Home > Maintenance > Configuration > Activate config
Activate Configuration File

Activate Configuration

Activate	File Name
○	Peter_config
○	alan_config

FIGURE 16-4. CONFIGURATION ACTIVATION

PARAMETER DESCRIPTION

- System files: startup-config: The startup configuration for the switch, read at boot time.

Parameter description:

- Activate: You can select the file that you want to activate.

Buttons

- Activate Configuration File: Click the “Activate Configuration File” button, then the selected file will be activated to be the switch’s running configuration.

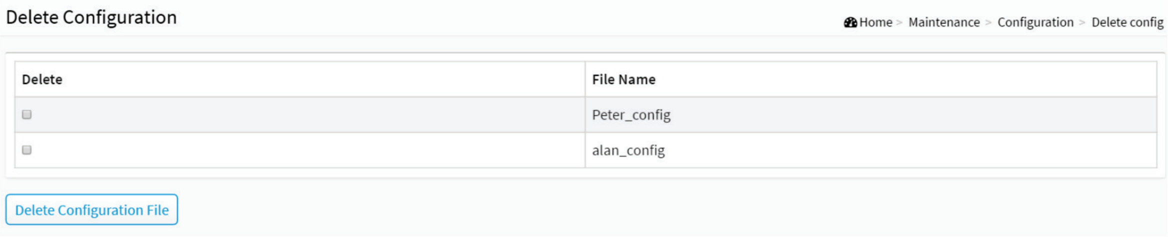
16.1.5 DELETE CONFIG

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 config.
2. Click Delete Select.


Home > Maintenance > Configuration > Delete config
Delete Configuration File

Delete Configuration

Delete	File Name
□	Peter_config
□	alan_config

FIGURE 16-5. DELETE CONFIGURATION

PARAMETER DESCRIPTION

- Delete: You can select the file that you want to delete.

Buttons

- Delete Configuration File: Click the “Delete Configuration File” button, then the selected file will be deleted.

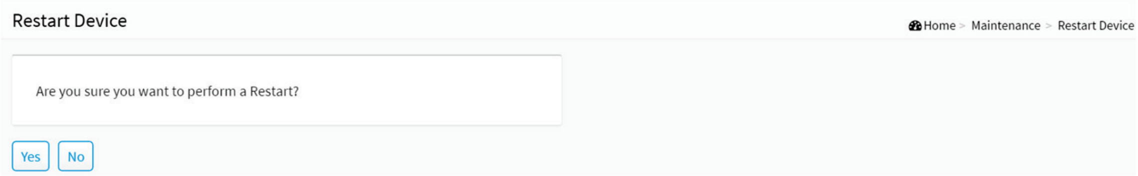
16.2 RESTART DEVICE

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

WEB INTERFACE

To configure a Restart Device Configuration in the web interface:

1. Click Restart Device.
2. Click Yes.



Are you sure you want to perform a Restart?

FIGURE 16-6. RESTART DEVICE SCREEN

PARAMETER DESCRIPTION

Restart Device: You can restart the switch on this page. After restart, the switch will boot normally.

Buttons

- Yes: Click to restart device.
- No: Click to return to the Port State page without restarting.

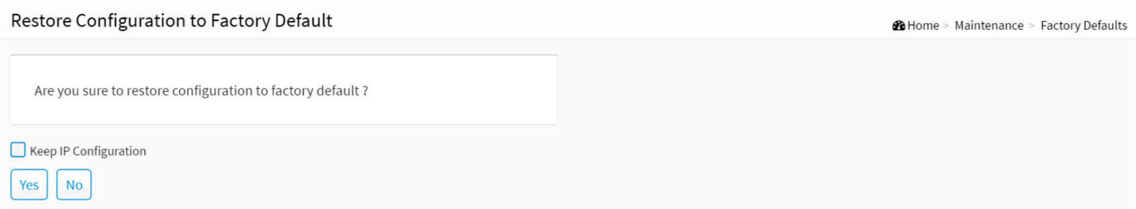
16.3 FACTORY DEFAULTS

This section describes how to restore the Switch configuration to Factory Defaults.

WEB INTERFACE

To restore Factory Defaults in the web interface:

1. Click Maintenance and Factory Defaults.
2. You can choose if you want to keep the ip configuration or not.
3. Click Yes.


Restore Configuration to Factory Default
Home > Maintenance > Factory Defaults

Are you sure to restore configuration to factory default ?

□ Keep IP Configuration

FIGURE 16-7. FACTORY DEFAULTS

PARAMETER DESCRIPTION

Buttons

- Keep IP Configuration: Choose if you want to keep ip configuration or not.
- Yes: Click the "Yes" button to reset the configuration to Factory Defaults.
- No: Click to cancel the operation.

16.4 FIRMWARE

This section describes how to upgrade Firmware.

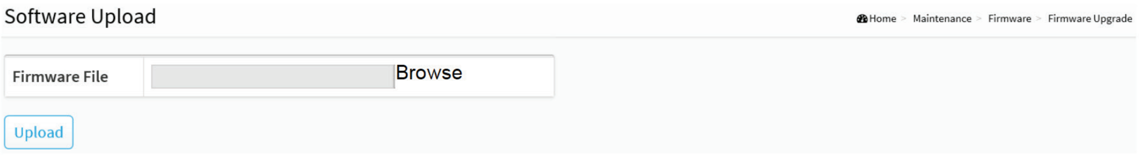
16.4.1 FIRMWARE UPGRADE

This page facilitates an update of the firmware controlling the switch.

WEB INTERFACE

To update the firmware of the device in the web interface:

1. Click Maintenance, Firmware and Firmware Upgrade.
2. Click Upload.



Software Upload

Home > Maintenance > Firmware > Firmware Upgrade

Firmware File | Browse

Upload

FIGURE 16-8. FIRMWARE UPGRADE

PARAMETER DESCRIPTION

Buttons

- Browse: Click the "Browse..." button to search the Firmware URL and filename and click "Upload."

16.4.2 FIRMWARE SELECTION

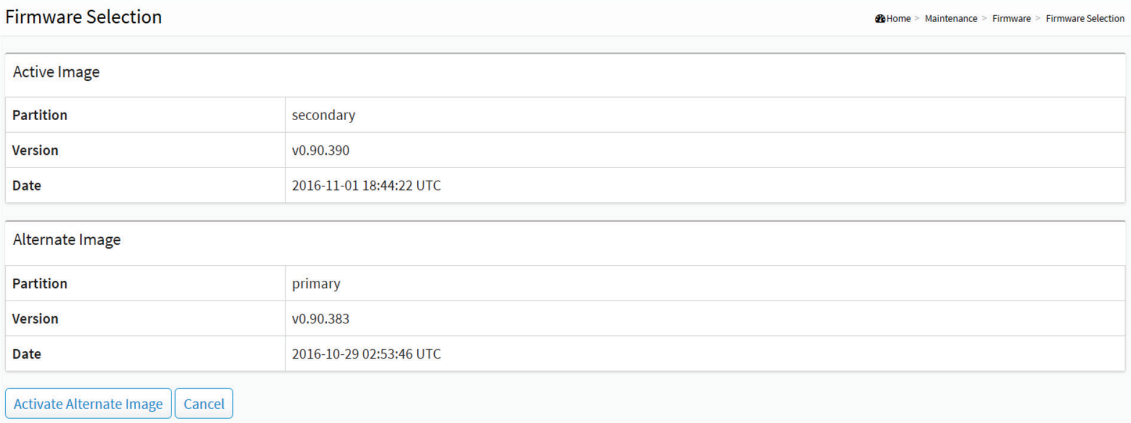
This page provides information about the active and alternate (backup) firmware images in the device, and allows you to revert to the alternate image.

The web page displays two tables with information about the active and alternate firmware images.

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.



Active Image

Partition	secondary
Version	v0.90.390
Date	2016-11-01 18:44:22 UTC

Alternate Image

Partition	primary
Version	v0.90.383
Date	2016-10-29 02:53:46 UTC

FIGURE 16-9. FIRMWARE SELECTION

PARAMETER DESCRIPTION

Image Information

- Partition: Indicates whether primary or secondary partition in the flash is used for storing the firmware image.
- Version: The version of the firmware image.
- Date: The date when 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.

APPENDIX A: REGULATORY INFORMATION

A.1 FCC STATEMENT

This equipment has been found to comply with the limits for a Class A digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference in which case the user will be required to correct the interference at his own expense.

Changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.

Shielded cables must be used with this equipment to maintain compliance with radio frequency energy emission regulations and ensure a suitably high level of immunity to electromagnetic disturbances.

All power supplies are certified to the relevant major international safety standards.

APPENDIX A: REGULATORY INFORMATION

A.2 NOM STATEMENT

1. Todas las instrucciones de seguridad y operación deberán ser leídas antes de que el aparato eléctrico sea operado.
2. Las instrucciones de seguridad y operación deberán ser guardadas para referencia futura.
3. Todas las advertencias en el aparato eléctrico y en sus instrucciones de operación deben ser respetadas.
4. Todas las instrucciones de operación y uso deben ser seguidas.
5. El aparato eléctrico no deberá ser usado cerca del agua—por ejemplo, cerca de la tina de baño, lavabo, sótano mojado o cerca de una alberca, etc.
6. El aparato eléctrico debe ser usado únicamente con carritos o pedestales que sean recomendados por el fabricante.
7. El aparato eléctrico debe ser montado a la pared o al techo sólo como sea recomendado por el fabricante.
8. Servicio—El usuario no debe intentar dar servicio al equipo eléctrico más allá a lo descrito en las instrucciones de operación. Todo otro servicio deberá ser referido a personal de servicio calificado.
9. El aparato eléctrico debe ser situado de tal manera que su posición no interfiera su uso. La colocación del aparato eléctrico sobre una cama, sofá, alfombra o superficie similar puede bloquea la ventilación, no se debe colocar en libreros o gabinetes que impidan el flujo de aire por los orificios de ventilación.
10. El equipo eléctrico deber ser situado fuera del alcance de fuentes de calor como radiadores, registros de calor, estufas u otros aparatos (incluyendo amplificadores) que producen calor.
11. El aparato eléctrico deberá ser connectado a una fuente de poder sólo del tipo descrito en el instructivo de operación, o como se indique en el aparato.
12. Precaución debe ser tomada de tal manera que la tierra fisica y la polarización del equipo no sea eliminada.
13. Los cables de la fuente de poder deben ser guiados de tal manera que no sean pisados ni pellizcados por objetos colocados sobre o contra ellos, poniendo particular atención a los contactos y receptáculos donde salen del aparato.
14. El equipo eléctrico debe ser limpiado únicamente de acuerdo a las recomendaciones del fabricante.
15. En caso de existir, una antena externa deberá ser localizada lejos de las lineas de energia.
16. El cable de corriente deberá ser desconectado del cuando el equipo no sea usado por un largo periodo de tiempo.
17. Cuidado debe ser tomado de tal manera que objectos liquidos no sean derramados sobre la cubierta u orificios de ventilación.
18. Servicio por personal calificado deberá ser provisto cuando:
    A: El cable de poder o el contacto ha sido dañado; u
    B: Objectos han caído o líquido ha sido derramado dentro del aparato; o
    C: El aparato ha sido expuesto a la lluvia; o
    D: El aparato parece no operar normalmente o muestra un cambio en su desempeño; o
    E: El aparato ha sido tirado o su cubierta ha sido dañada.

APPENDIX B: DISCLAIMER/TRADEMARKS

B.1 DISCLAIMER

Black Box Corporation shall not be liable for damages of any kind, including, but not limited to, punitive, consequential or cost of cover damages, resulting from any errors in the product information or specifications set forth in this document and Black Box Corporation may revise this document at any time without notice.

B.2 TRADEMARKS USED IN THIS MANUAL

Black Box and the Black Box logo type and mark are registered trademarks of Black Box Corporation.

Any other trademarks mentioned in this manual are acknowledged to be the property of the trademark owners.

NOTES