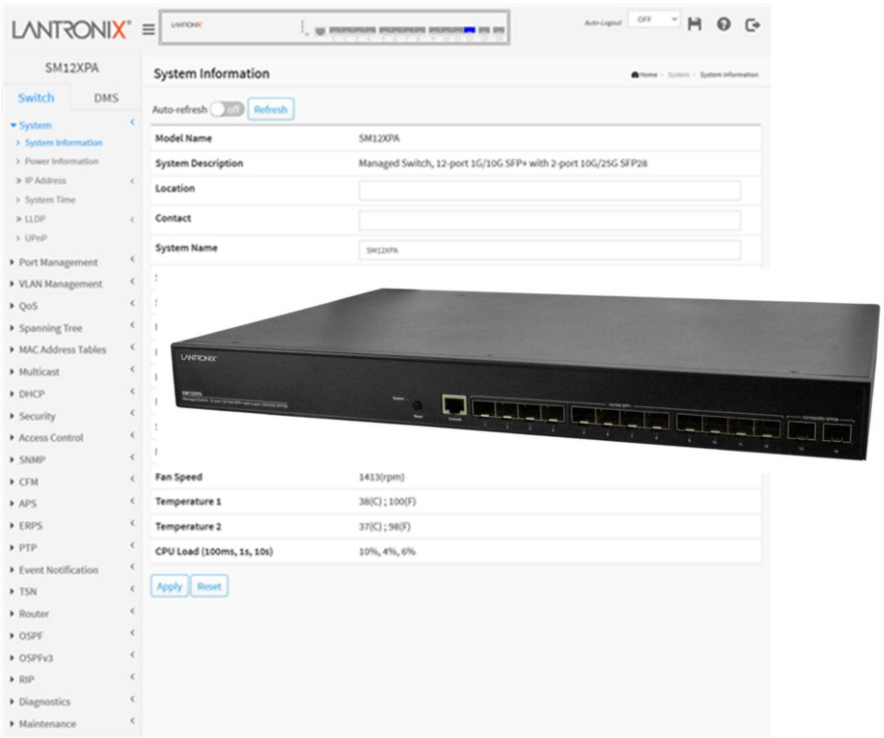
LANTRONIX®



System Information

Model Name	SM12XPA
System Description	Managed Switch, 12-port 1G/10G SFP+ with 2-port 10G/25G SFP28
Location	
Contact	
System Name	SM12XPA
Fan Speed	1413(rpm)
Temperature 1	38(C) ; 100(F)
Temperature 2	37(C) ; 98(F)
CPU Load (100ms, 1s, 10s)	10%, 4%, 6%

SM12XPA

12-port Multi-Gig SFP+ with (2) 10G/25G SFP28 slots
Managed Layer 3 Fiber Switch

Web User Guide

Part Number 33848
Revision A May 2022

Intellectual Property

Patented: https://www.lantronix.com/legal/patents/; additional patents pending.

Warranty

For details on the Lantronix warranty policy, go to http://www.lantronix.com/support/warranty.

Contacts

Lantronix Corporate Headquarters
7535 Irvine Center Drive
Suite100
Irvine, CA 92618, USA
Toll Free: 800-526-8766
Phone: 949-453-3990
Fax: 949-453-3995

Technical Support
Phone: +1.952.358.3601 or 1.800.260.1312
Email: https://www.lantronix.com/technical-support/

Sales Offices
For a current list of our domestic and international sales offices, go to www.lantronix.com/about/contact.

Disclaimer

All information contained herein is provided "AS IS." Lantronix undertakes no obligation to update the information in this publication. Lantronix does not make, and specifically disclaims, all warranties of any kind (express, implied or otherwise) regarding title, non-infringement, fitness, quality, accuracy, completeness, usefulness, suitability or performance of the information provided herein. Lantronix shall have no liability whatsoever to any user for any damages, losses and causes of action (whether in contract or in tort or otherwise) in connection with the user's access or usage of any of the information or content contained herein. The information and specifications contained in this document are subject to change without notice.

Revision History

Date	Rev.	Notes
5/26/22	A	Initial Lantronix release at FW v8.90.884 and HW v1.01.

Contents

1. Introduction

Product Description

The SM12XPA Fiber Aggregation Switch is a managed Layer 3 (L3) Multi-Gigabit Ethernet fiber switch offering powerful Layer 2 and basic Layer 3 features for improved functionality. It also supports enhanced security features such as IP source guard and Access Control Lists to guard networks against unauthorized access.

The SM12XPA switch provides 340 Gbps switching capacity with (12) 1G/10G SFP+ and (2) 1G/10G/25G SFP28 slots and (1) RJ-45 console port. It offers high performance and reliability for high bandwidth aggregation and access network applications. The embedded Device Managed System (DMS) software is easy to use and simplifies configuration, installation, and troubleshooting of devices in applications with high fiber density. The SM12XPA offers an improved user experience, and lowers operating and maintenance costs.

About This Manual

This manual gives specific information on how to operate and use the management functions of the SM12XPA via HTTP/HTTPs web browser.

This manual is intended for use by network administrators who are responsible for operating and maintaining network equipment; consequently, it assumes a good working knowledge of L2 and L3 Ethernet switch functions, the Internet Protocol (IP), and Hypertext Transfer Protocol (HTTP).

Related Documentation

These manuals give specific information on how to install and operate switch functions:

- SM12DPXA Quick Start Guide, 33846
- SM12DPXA Install Guide, 33847
- SM12DPXA Web User Guide, 33848 (this manual)
- SM12DPXA CLI Reference, 33849
- Release Notes (version specific)

2. Operation

Initial Configuration

This chapter describes how to configure and manage the SM12XPA via the web user UI. With this facility, you can easily access and monitor from any switch port and view all switch status, including each port's activity, Spanning Tree status, Port aggregation status, Multicast traffic, VLAN and priority status, etc.

The SM12XPA default values are listed below:

IP Address	192.168.1.77
Subnet Mask	255.255.255.0
Default Gateway	192.168.1.254
Username	admin
Password	admin

After the SM12XPA has been finished configuration it interface, you can browse it. For instance, type http://192.168.1.1 in the address row in a browser, it will show the Login page asking you to enter a username and password to login and access authentication.

The default username and password are "admin". For the first time to use, enter the default username and password, and then click the <Login> button. The login process now is completed. In this Login menu, you must input the complete username and password respectively, the SM12XPA will not give you a shortcut to the username automatically. This looks inconvenient but is safer.

The SM12XPA allows two or more admin users to manage this switch at the same time; whichever admin user made the last settings will present the configuration that the system will use.

When you login to the SM12XPA Web UI management, you can use both ipv4 ipv6 login to manage the switch.

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

Note: The SM12XPA has the DHCP function disabled by default, so If you do not have DHCP server to provide an IP address to the switch, use the default switch IP address of 192.168.1.77. The Login page is shown below:

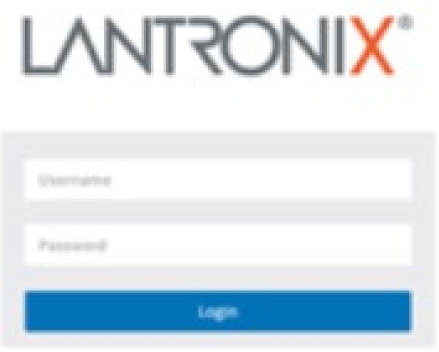
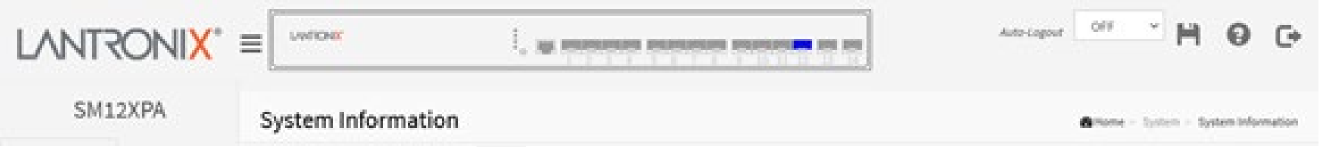


Figure 1: The Login page

Web UI Controls

You can click the logo in the Web UI top left corner to come back to this page from anywhere in the menu system.



The Web UI top left corner displays an icon (☰) that alternately hides and displays the left hand menus.

The Web UI top left also displays a switch icon that lets you hover the cursor over a front panel component to display the status / description for that component (shown below). You can also click on a port to display that port's Detailed Port Statistics.

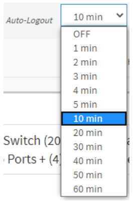
The Web UI top right corner displays a set of three icons (💾 ? ⇥) that let you Save Configuration, display online Help, and Logout. You can hover the cursor over any icon to display its function (Save Configuration Help Logout).

The Web UI top right corner also displays the currently displayed page's menu path (e.g., Home > Monitor > System > Information) as shown below:

Home > Monitor > System > Information

Auto-logout: Auto-Logout OFF The Auto-logout dropdown lets you set the amount of time after a successful login before an automatic log out occurs. The selections are OFF, 1, 2, 3, 4, 5, 10, 20, 30, 40, and 60 minutes (added at FW vB6.54.3494). The default is 10 minutes. When set to OFF, no Auto-logout occurs.

Auto-Logout Timeout: After you change the Auto-Logout timeout and then log out and log back in, the Auto-Logout timeout setting will be the setting saved to the start-up config file.



When the Auto-Logout timeout setting is changed, it directly writes to running-config.

To save the timeout change to start-up config, you must execute a save to startup-config.

To examine the running-config, you can run the CLI command "showing running-config" or in the Web UI just log out and log back in again.
To save the timeout change into startup-config, you must do a save to startup-config and then reboot the switch.

In summary:

- When you power on the switch, it will get the settings from startup-config.
- When you logout and login (without switch reboot), the switch will get the timeout settings from startup-config.
- When you reload defaults, the switch will get the timeout settings default-config.

For the "Save to start-up config" behavior, if you don't save the config, when you change the timeout setting but logout, at the next login the timeout setting remains unchanged as the setting in start-up config.

If you save timeout setting to start-up config:	If you don’t save timeout setting to start-up config:
When you change the timeout setting and save to startup-config (click the diskette icon), the changed timeout setting will be applied to running-config and start-up config immediately.	When you change the timeout setting (without save to startup-config), the timeout change will be applied to running-config immediately.
After Logout and login, the timeout setting will be the setting saved in start-up config.	After Logout and login, the timeout setting will be the setting saved in start-up configure.
After a switch reboot, the timeout setting will be the setting saved in start-up config.	After you reboot the switch, the timeout setting will be the setting saved in start-up config.

Click Save Button

: displays in the top right corner when a change has been made and can be saved by clicking the Save button to save the changes to the startup-config file.

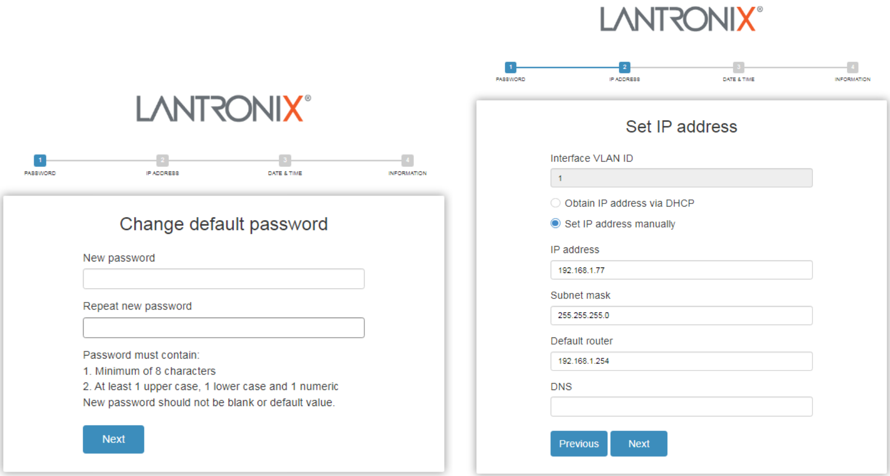
The SM12XPA Web UI management modules are described in the following chapters.

First Time Wizard

The first time you use this device you must configure some basic settings such as password, IP address, date and time, and system information. Use the following procedure:

Step 1: Change default password

Enter a new password and then enter it again. The Password must contain at least 8 characters, at least 1 upper case letter, 1 lower case letter and one numeric character. The new password cannot be blank or the default value. Click the **Next** button.



Change default password

New password

Repeat new password

Password must contain:
1. Minimum of 8 characters
2. At least 1 upper case, 1 lower case and 1 numeric
New password should not be blank or default value.

Next

Set IP address

Interface VLAN ID: 1

○ Obtain IP address via DHCP
● Set IP address manually

IP address: 192.168.1.77

Subnet mask: 255.255.255.0

Default router: 192.168.1.254

DNS

Previous Next

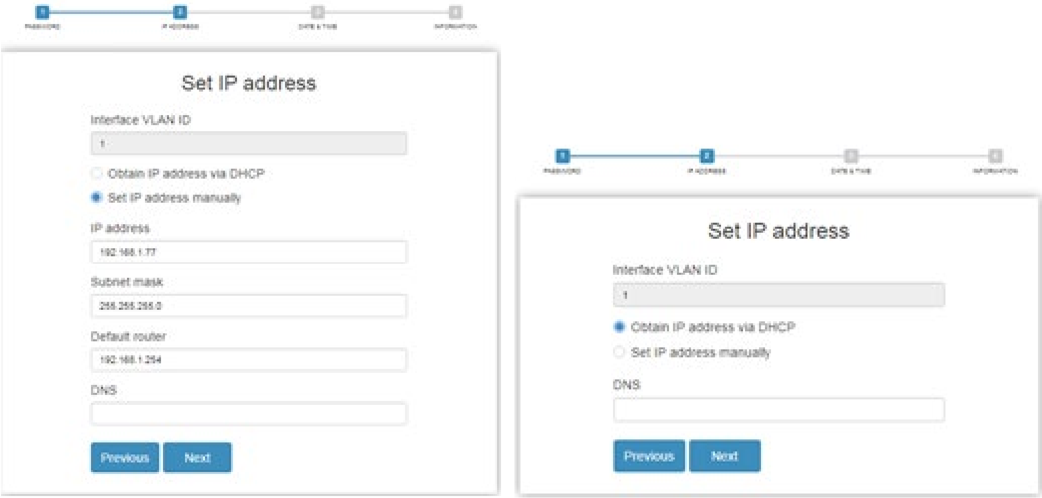
Figure 2-1: Change default password

Step 2: Set IP address

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

- □ If setting manually, enter IP address, Subnet mask, and Default router.
- □ If obtaining via DNS, enter a DNS server IP address. See “Messages” below.
- □ If obtaining via DHCP, enter a DHCP server IP address.

Click the **Next** button.



Set IP address

Interface VLAN ID: 1

○ Obtain IP address via DHCP
● Set IP address manually

IP address: 192.168.1.77

Subnet mask: 255.255.255.0

Default router: 192.168.1.254

DNS

Previous Next

Set IP address

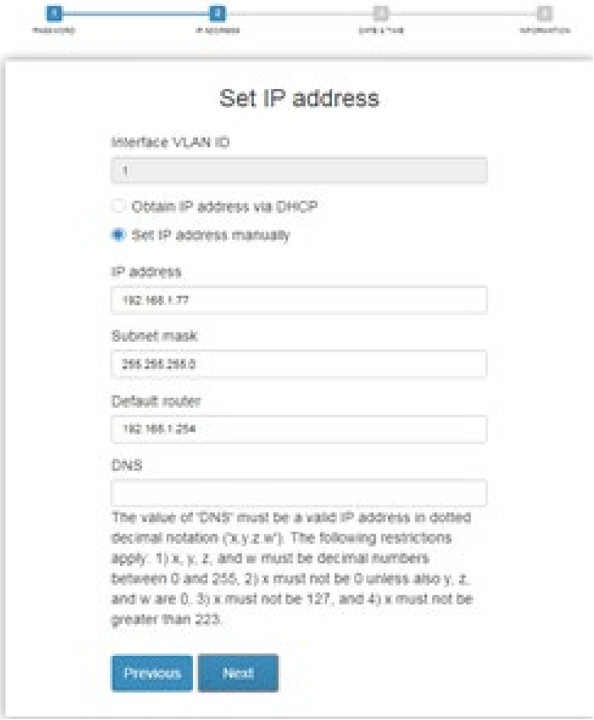
Interface VLAN ID: 1

● Obtain IP address via DHCP
○ Set IP address manually

DNS

Previous Next

Figure 2-2a: Set IP address



Set IP address

Interface VLAN ID: 1

○ Obtain IP address via DHCP

● Set IP address manually

IP address: 192.168.1.77

Subnet mask: 255.255.255.0

Default router: 192.168.1.254

DNS:

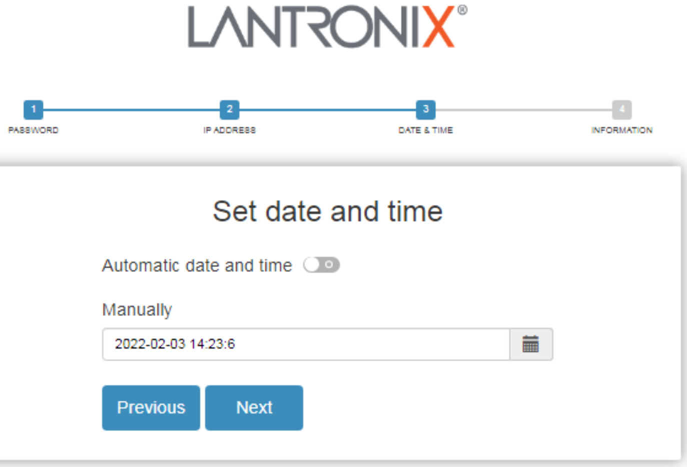
The value of 'DNS' must be a valid IP address in dotted decimal notation ('x.y.z.w'). The following restrictions apply: 1) x, y, z, and w must be decimal numbers between 0 and 255, 2) x must not be 0 unless also y, z, and w are 0, 3) x must not be 127, and 4) x must not be greater than 223.

Figure 2-2b: Set IP address

The value of 'DNS' must be a valid IP address in dotted decimal notation ('x.y.z.w'). The following restrictions apply: 1) x, y, z, and w must be decimal numbers between 0 and 255, 2) x must not be 0 unless also y, z, and w are 0, 3) x must not be 127, and 4) x must not be greater than 223.

Step 3: Set date and time

Enable “Automatic data and time” or select “Manually” to set or select the desired date and time.
If you enable “Automatic data and time” then you must enter a “Server Address” and select a “Time zone”. Click the **Next** button when done.



Set date and time

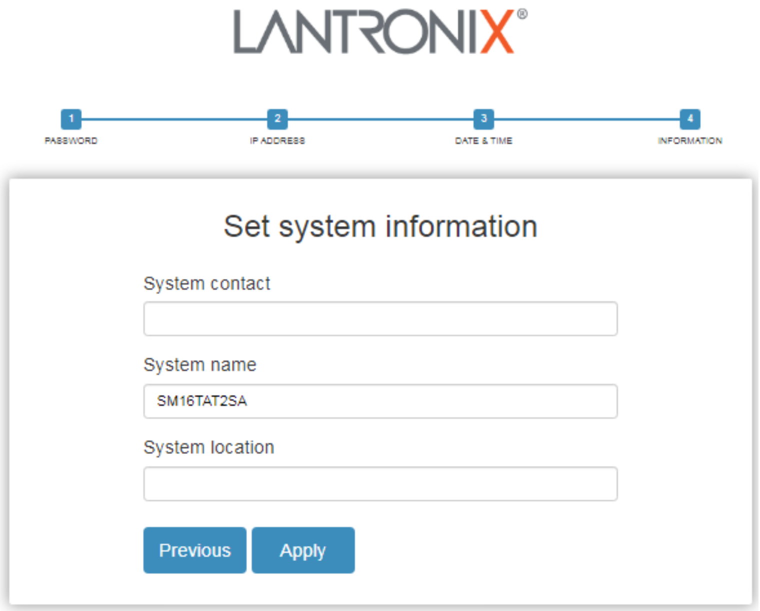
Automatic date and time: off

Manually: 2022-02-03 14:23:6

Figure 2-3: Set date and time

Step 4: Set system information

You can set some system information to this device, such as “System contact”, “System name”, and “System location”. Click the **Apply** button when done.



Set system information

System contact

System name

SM16TAT2SA

System location

Figure 2-4: Set system information

Message: Password format error.

Message: *The value of 'DNS' must be a valid IP address in dotted decimal notation ('x.y.z.w'). The following restrictions apply: 1) x, y, z, and w must be decimal numbers between 0 and 255, 2) x must not be 0 unless also y, z, and w are 0, 3) x must not be 127, and 4) x must not be greater than 223.*

3. System

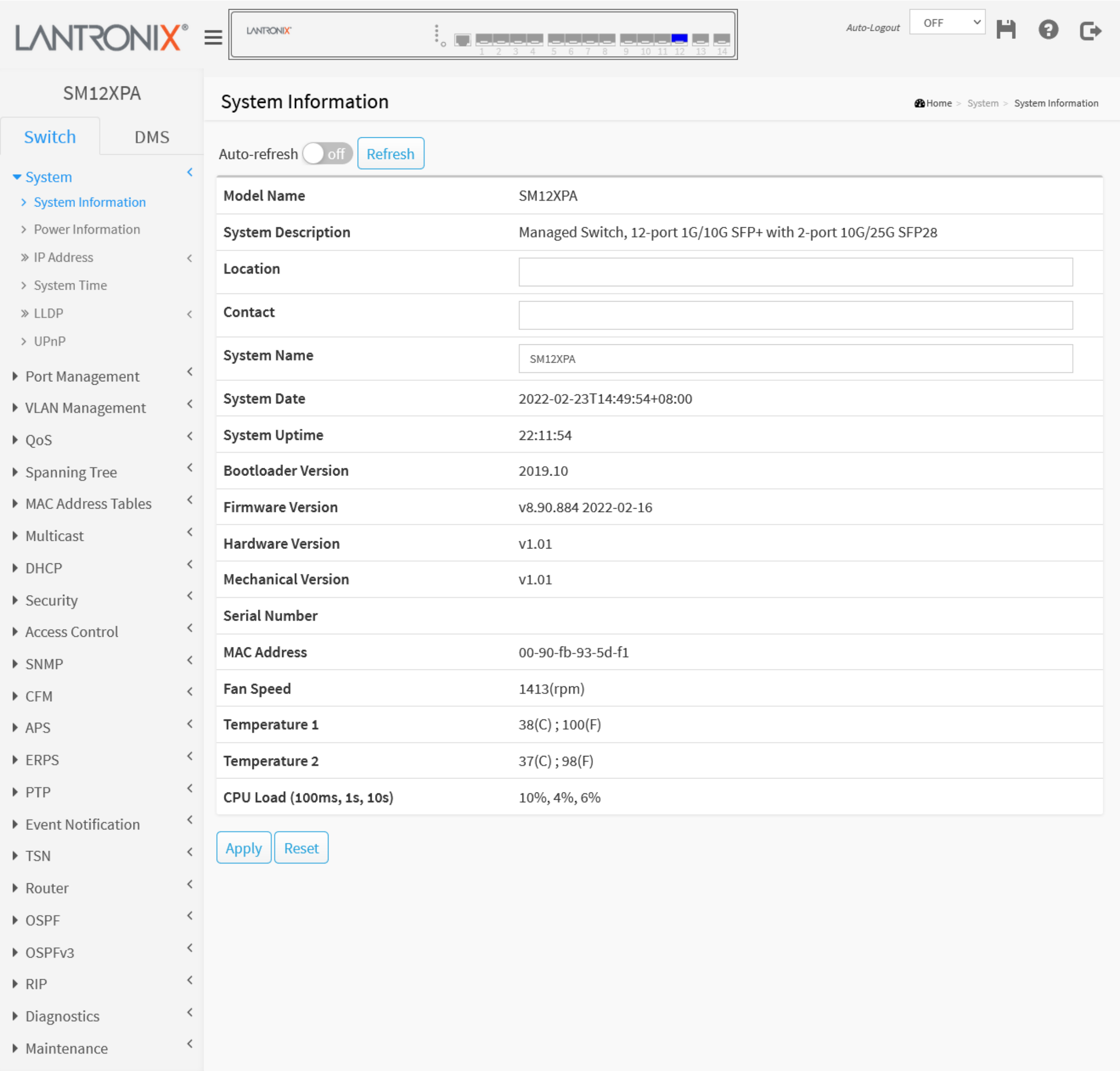
The System menu provides sub-menus for System Information, IP Address, IP Settings, Advanced IP Settings, IP Status, System Time, LLDP, LDP-MED, LLDP Neighbor, LLDP-MED Neighbor, LLDP Neighbor EEE, LLDP Statistics, and UPnP.

System Information

This is the startup page. Here you can set the switch system name, location and contact of the switch, and view related switch information.

To view and set System Information in the web UI:

1. Click System and System Information.
2. Enter System Name, Location, and Contact information as desired.
3. Click the Apply button to save the changes to the running-config file.



System Information

Model Name	SM12XPA
System Description	Managed Switch, 12-port 1G/10G SFP+ with 2-port 10G/25G SFP28
Location	
Contact	
System Name	SM12XPA
System Date	2022-02-23T14:49:54+08:00
System Uptime	22:11:54
Bootloader Version	2019.10
Firmware Version	v8.90.884 2022-02-16
Hardware Version	v1.01
Mechanical Version	v1.01
Serial Number	
MAC Address	00-90-fb-93-5d-f1
Fan Speed	1413(rpm)
Temperature 1	38(C) ; 100(F)
Temperature 2	37(C) ; 98(F)
CPU Load (100ms, 1s, 10s)	10%, 4%, 6%

Figure 2-1: System Information

Parameter descriptions:

Model Name : Displays the factory defined model name for identification purposes (*SM12XPA*).

System Description : Displays the system description (*Managed Switch, 12-port 1G/10G SFP+ with 2-port 10G/25G SFP 28*).

Location : Enter the desired system location text.

Contact : Enter the system contact information as required.

System Name : Displays the name for the switch (*SM12XPA*) which you can edit.

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

System Uptime : The period of time the device has been operational.

Bootloader Version : Displays the current boot loader version number.

Firmware Version : The software version of this switch (e.g., v8.90.884 2022-02-16)

Hardware Version : Displays the hardware version of the device.

Mechanical Version : Displays the mechanical version of the device.

Serial Number : Displays the unique serial number that is assigned to this device.

MAC Address : The MAC Address of this switch.

Temperature 1 : Displays the temperature of sensor 1.

Temperature 2 : Displays the temperature of sensor 2.

CPU Load (100ms, 1s, 10s) : Displays the system cpu loading percentage at 100ms, 1s, and 10s.

Buttons

Apply : Click to save changes.

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

IP Address

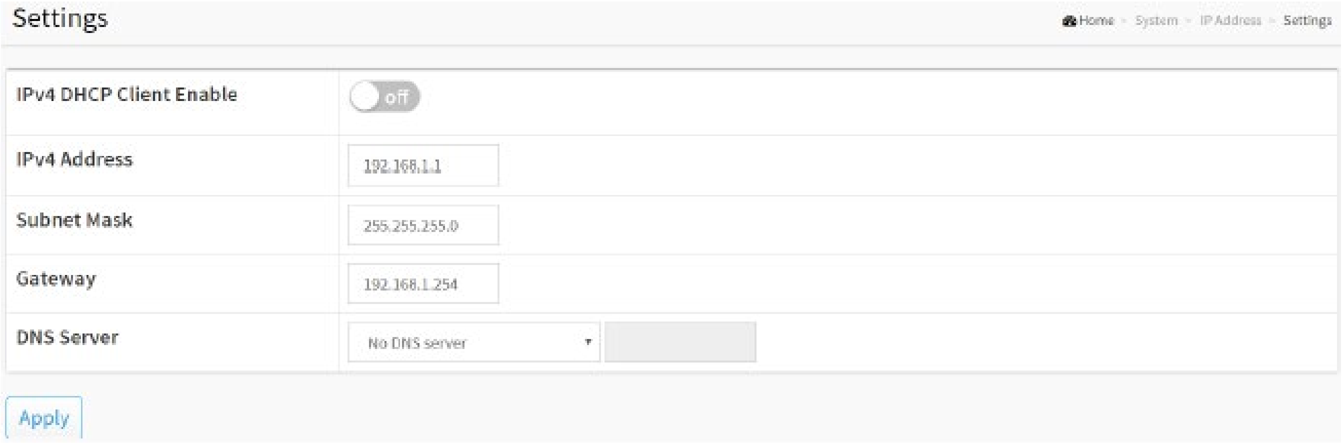
Settings

The IPv4 address for the switch can be obtained via DHCP Server for VLAN 1. To manually configure an address, you must 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.

This page lets you configure basic IP settings, gateway, and DNS server parameters.

To configure IP Settings in the web UI:

1. Click System, IP Address, and Settings.
2. Enable (*on*) or disable the IPv4 DHCP Client. The default is disabled (*off*).
3. Specify the IPv4 Address, Subnet Mask, and Gateway.
4. Select a DNS Server.
5. Click Apply.



Settings

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

Figure 2-2.1: IP Settings

Parameter descriptions:

IPv4 DHCP Client Enable : Enable the DHCP client by clicking here. If this option is enabled (on), 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. The default is off.

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

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

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

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

No DNS server: No DNS server will be used.

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

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

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

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

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

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

Buttons

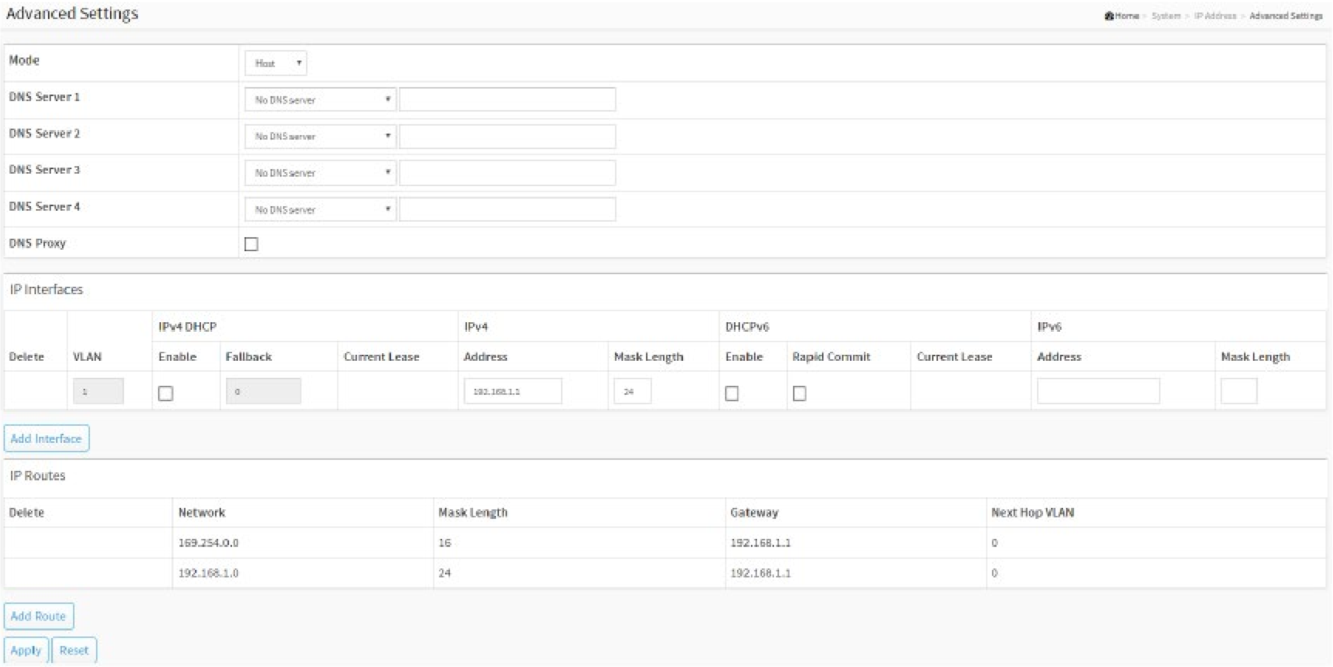
Apply : Click to save changes.

Advanced Settings

Configure switch-managed IP information on this page, including IP basic settings, IP interfaces and IP routes. The maximum number of interfaces supported is 128 and the maximum number of routes is 128.

To configure Advanced IP settings in the web UI:

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



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

IP Interfaces

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

IP Routes

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

Figure 2-2.2: Advanced IP Settings

Parameter descriptions:

Mode : Configure whether the IP stack should act as a ***Host*** or a ***Router***. In Host mode, IP traffic between interfaces will not be routed. In Router mode traffic is routed between all interfaces. This must be set to ***Router*** mode for routing protocol operation (see chapter 20).

DNS Server 1-4: This setting controls the DNS name resolution done by the switch. There are four servers available for configuration, and the index of the server presents the preference (less index has higher priority) in doing DNS name resolution. These modes are supported:

> ***No DNS server***: No DNS server will be used.
>
> ***Configured IPv4*** : Explicitly provide the valid IPv4 unicast address of the DNS Server in dotted decimal notation. Make sure the configured DNS server could be reachable (e.g., via PING) for activating DNS service.
>
> ***Configured IPv6*** : Explicitly provide the valid IPv6 unicast (except linklocal) address of the DNS Server. Make sure the configured DNS server could be reachable (e.g., via PING6) for activating DNS service.
>
> ***From any DHCPv4 interfaces*** : The first DNS server offered from a DHCPv4 lease to a DHCPv4-enabled interface will be used.

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

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

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

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

IP Interfaces

Delete : Select this option to delete an existing IP interface.

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

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 bank if IPv4 operation on the interface is not desired.

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

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

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

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

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

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

IP Routes

Delete : Select this option to delete an existing IP route.

Network : The destination IP network or host address of this route. Valid format is dotted decimal notation or a valid IPv6 notation. A default route can use the value 0.0.0.0 or IPv6 :: notation. Note: You must provide this parameter if you will be configuring L3 Routing as described in Chapter 20.

Mask Length : The destination IP network or host mask, in number of bits (prefix length). It defines how much of a network address that must match, in order to qualify for this route. Valid values are 0 and 32 bits for IPv4 or 128 bits for IPv6 routes. Only a default route will have a mask length of 0 (as it will match anything). Note: You must provide this parameter if you will be configuring L3 Routing as described in Chapter 20.

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

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

Buttons

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

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

Apply : Click to save changes.

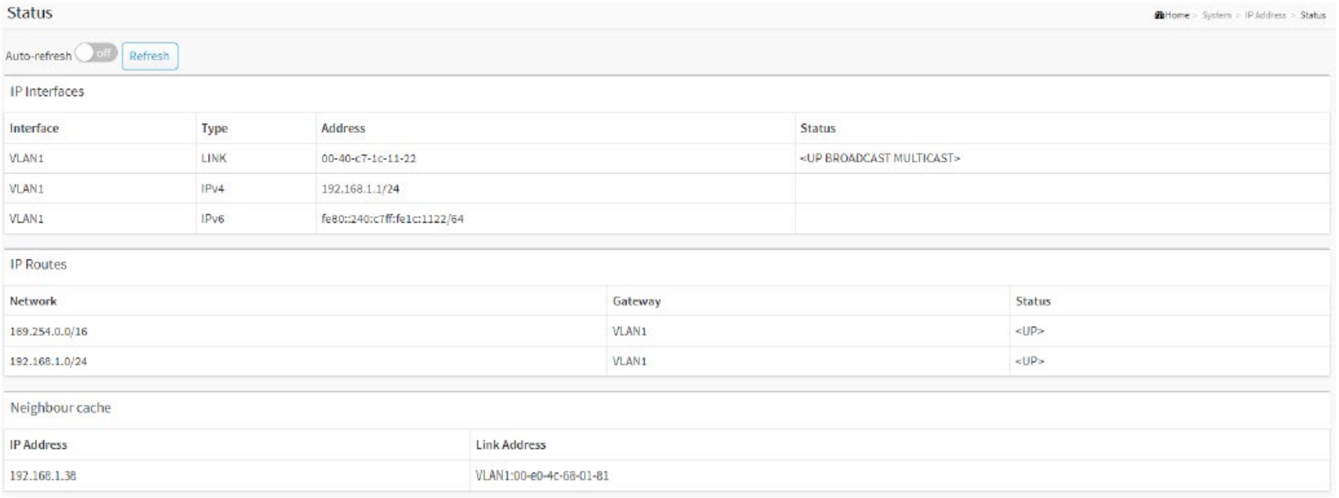
Reset : Click to undo any changes made locally and revert to previously saved values.

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.

To display IP Status in the web UI:

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



IP Interfaces

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

IP Routes

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

Neighbour cache

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

Figure 2-2.3: IP Status

Parameter descriptions:

IP Interfaces

Interface : Shows the name of the interface.

Type : Shows the address type of the entry. This may be LINK or IPv4.

Address : Shows the current address of the interface (of the given type).

Status : Shows the status flags of the interface (and/or address).

IP Routes

Network : Shows the destination IP network or host address of this route.

Gateway : Shows the gateway address of this route.

Status : Shows the status flags of the route.

Neighbor cache

IP Address : Shows the IP address of the entry.

Link Address : Shows the Link (MAC) address for which a binding to the IP address given exists.

Buttons

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

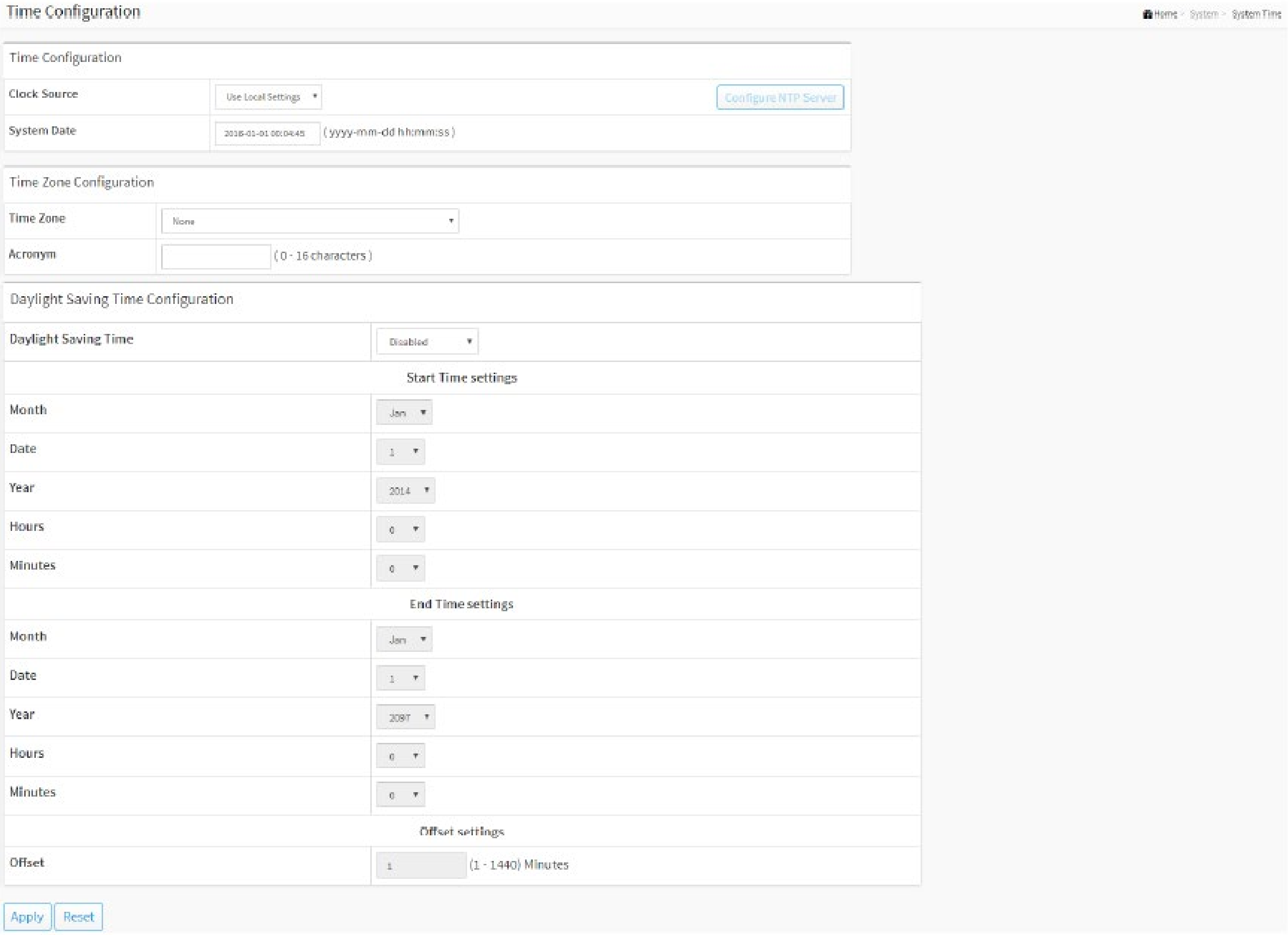
Refresh : Click to refresh the page immediately.

System Time

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

To configure Time parameters in the web UI:

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



Time Configuration

Time Configuration	
Clock Source	Use Local Settings ▾ Configure NTP Server
System Date	2018-01-01 00:04:45 (yyyy-mm-dd hh:mm:ss)

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

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

Figure 2-3: Time Configuration

Parameter descriptions:

Time Configuration

Clock Source : Select one of two modes for configuring where the system clock comes from:

Use Local Settings : Clock Source from Local Time.

NTP Server : Clock Source from NTP Server.

System Date : Shows the current time of the system. The year of system date can be 2011 - 2037.

Time Zone Configuration

Time Zone : Lists various Time Zones worldwide. Select appropriate Time Zone from the drop down and click Apply to set. The default is None.

Acronym : 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. The default is Disabled.

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 a one-time configuration.

Start time settings : Week - Select the starting day, date, and time.

Day - Select the starting day.

Month - Select the starting month.

Hours - Select the starting hour.

Minutes - Select the starting minute.

End time settings : Week - Select the ending day, date, and time.

Day - Select the ending day.

Month - Select the ending month.

Hours - Select the ending hour.

Minutes - Select the starting minute.

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

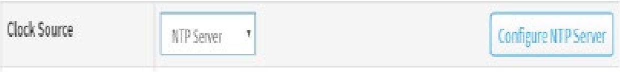
Note: The “Start Time Settings” and “End Time Settings” display what you set on the “Start Time Settings” and “End Time Settings” field information.

Buttons

Apply : Click to save changes.

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

Configure NTP Server button: Click to configure NTP server(s) when Clock Source is “NTP Server”.



Clock Source: NTP Server

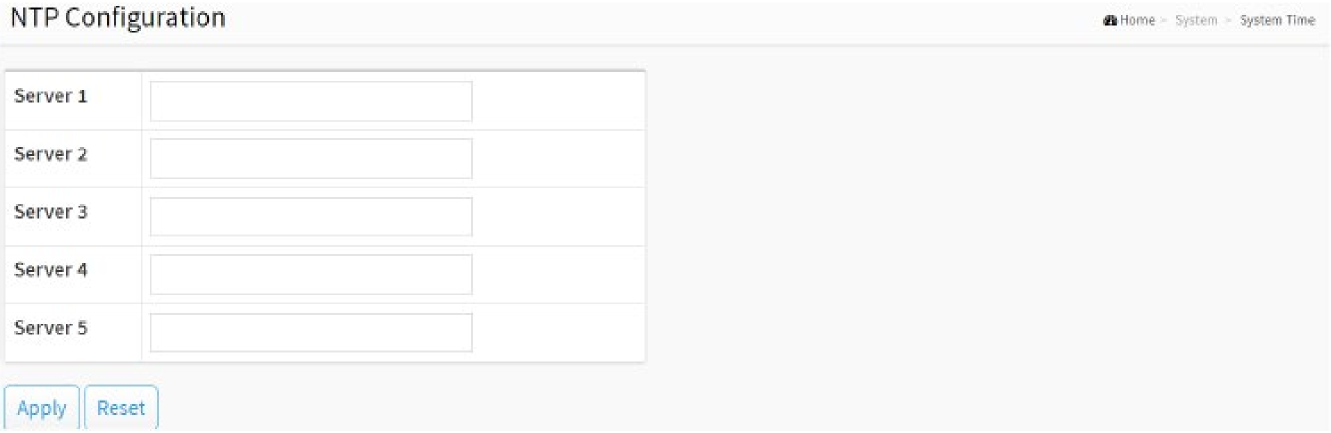


Figure 2-3: NTP Configuration

NTP (Network Time Protocol) is used to sync the network time based Greenwich Mean Time (GMT). If you use 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 in a short while after clicking the Apply button. Though it synchronizes the time automatically, NTP does not update the time periodically without user action.

Time Zone is an offset time of GMT. You must select the time zone first and then perform a time sync via NTP because the switch will combine this time zone offset and updated NTP time to come up with the local time. Otherwise, you will not be able to get the correct time. The switch supports a configurable time zone from –12 to +13 in 1 hour steps. The default Time zone is +8 Hrs.

Parameter descriptions :

Server 1 to 5 : Provide the NTP IPv4 or IPv6 address of this switch. IPv6 address is in 128-bit records represented as eight fields of up to four hexadecimal digits with a colon separating each field (:). For example, with the entry '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. It can only appear once., and it can also represent a valid IPv4 address (e.g., '::192.1.2.34').

Buttons

Apply : Click to save changes.

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

LLDP

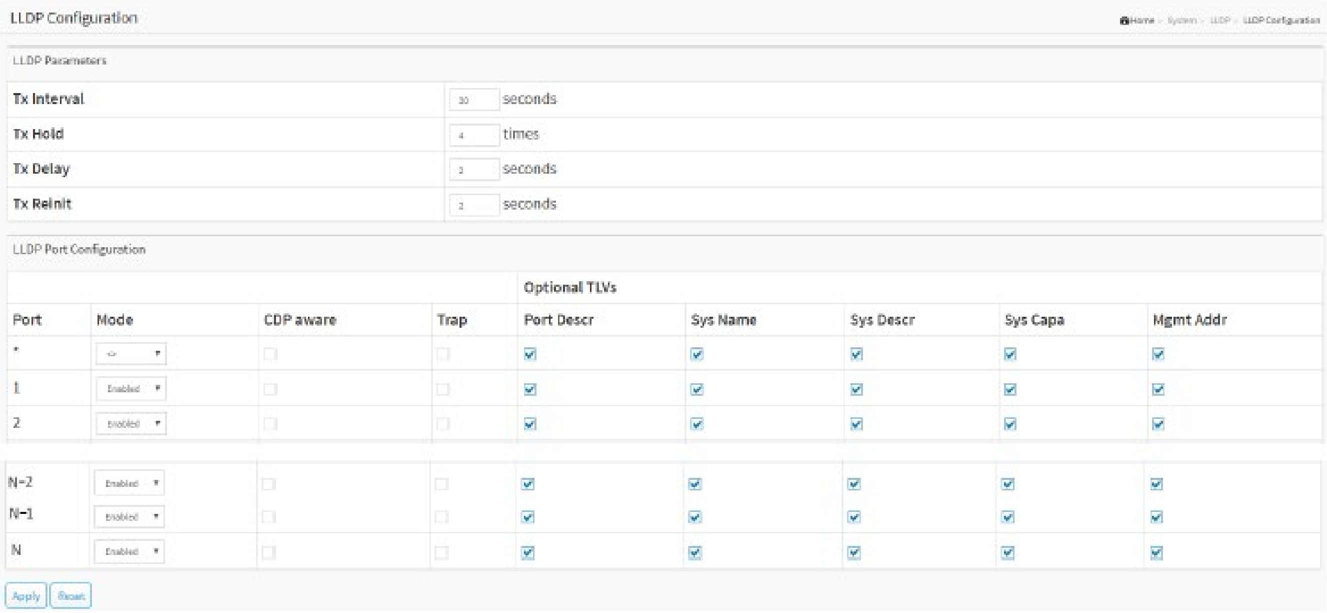
The switch supports LLDP (Link Layer Discovery Protocol). LLDP provides a standards-based method for enabling switches to advertise themselves to adjacent devices and to learn about adjacent LLDP devices. LLDP is a vendor-neutral Link Layer protocol in the Internet Protocol Suite used by network devices 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.

LLDP Configuration

This page lets you view and configure the current LLDP settings. You can configure LLDP and detailed per-port parameters; the settings will take effect immediately.

To configure LLDP:

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



LLDP Configuration

LLDP Parameters

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

LLDP Port Configuration

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

Figure 2-4.1: LLDP Configuration

Parameter descriptions:

LLDP Parameters

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

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

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

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

LLDP Port Configuration :

Port : The switch port number of the logical LLDP port.

Mode : Select an LLDP mode:

> ***Rx only*** : The switch will not send out LLDP information, but LLDP information from neighbor units is analyzed.
>
> ***Tx only*** : The switch will drop LLDP information received from neighbors but will send out LLDP information.
>
> ***Disabled*** : The switch will not send out LLDP information and will drop LLDP information received from neighbors.
>
> ***Enabled*** : the switch will send out LLDP information and will analyze LLDP information received from neighbors.

CDP Aware : Select Cisco Discovery Protocol awareness.

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

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

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

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

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

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

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

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

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

Trap : LLDP trapping notifies events such as newly-detected neighbor devices and link malfunctions.

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

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

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

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

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

Buttons

Apply : Click to save changes.

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

LDP-MED Configuration

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

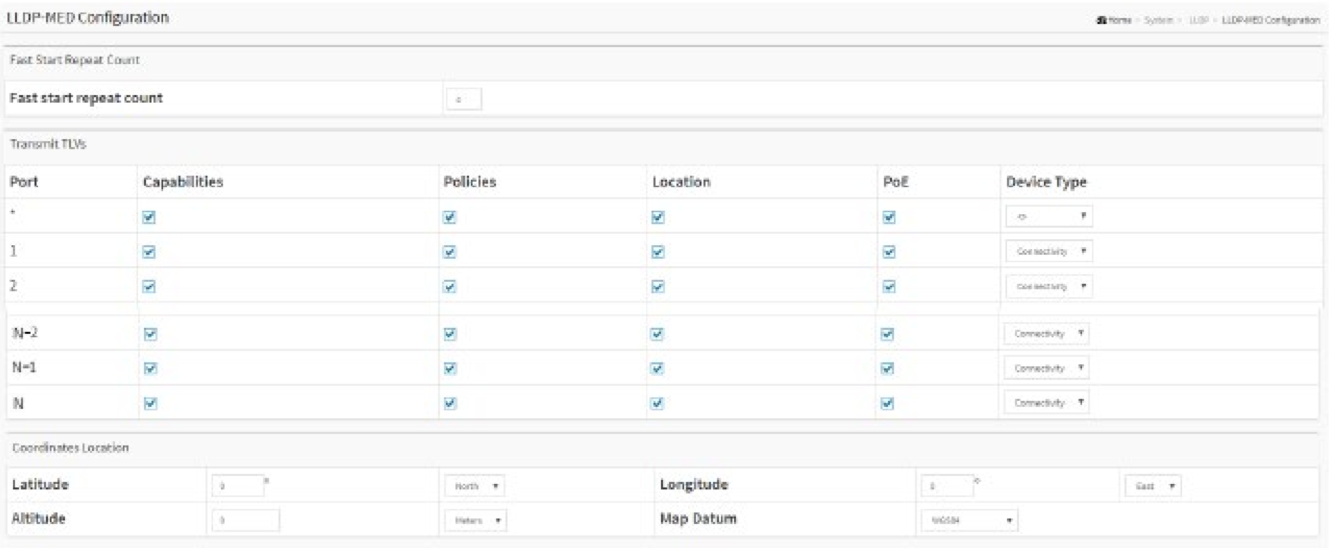
- Auto-discovery of LAN policies (such as VLAN, Layer 2 Priority and Differentiated Services (Diffserv) settings) enabling plug and play networking.
- Device location discovery to allow creation of location databases and, in the case of Voice over Internet Protocol (VoIP), Enhanced 911 services.
- Inventory 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 lets you configure LLDP-MED. This function applies to VoIP devices which support LLDP-MED.

Web Interface

To configure LLDP-MED:

1. Click System, LLDP and LLDP-MED Configuration.
2. Modify Fast start repeat count parameter; the default is 4.
3. Modify Transmit TLVs parameters.
4. Modify Coordinates Location parameters.
5. Fill Civic Address Location parameters.
6. Fill Emergency Call Service parameters.
7. Click Add New Policy.
8. Enter Policy Port configuration and click Apply.
9. Select a Policy ID for each port.
10. Click Apply.



LLDP-MED Configuration

Fast Start Repeat Count

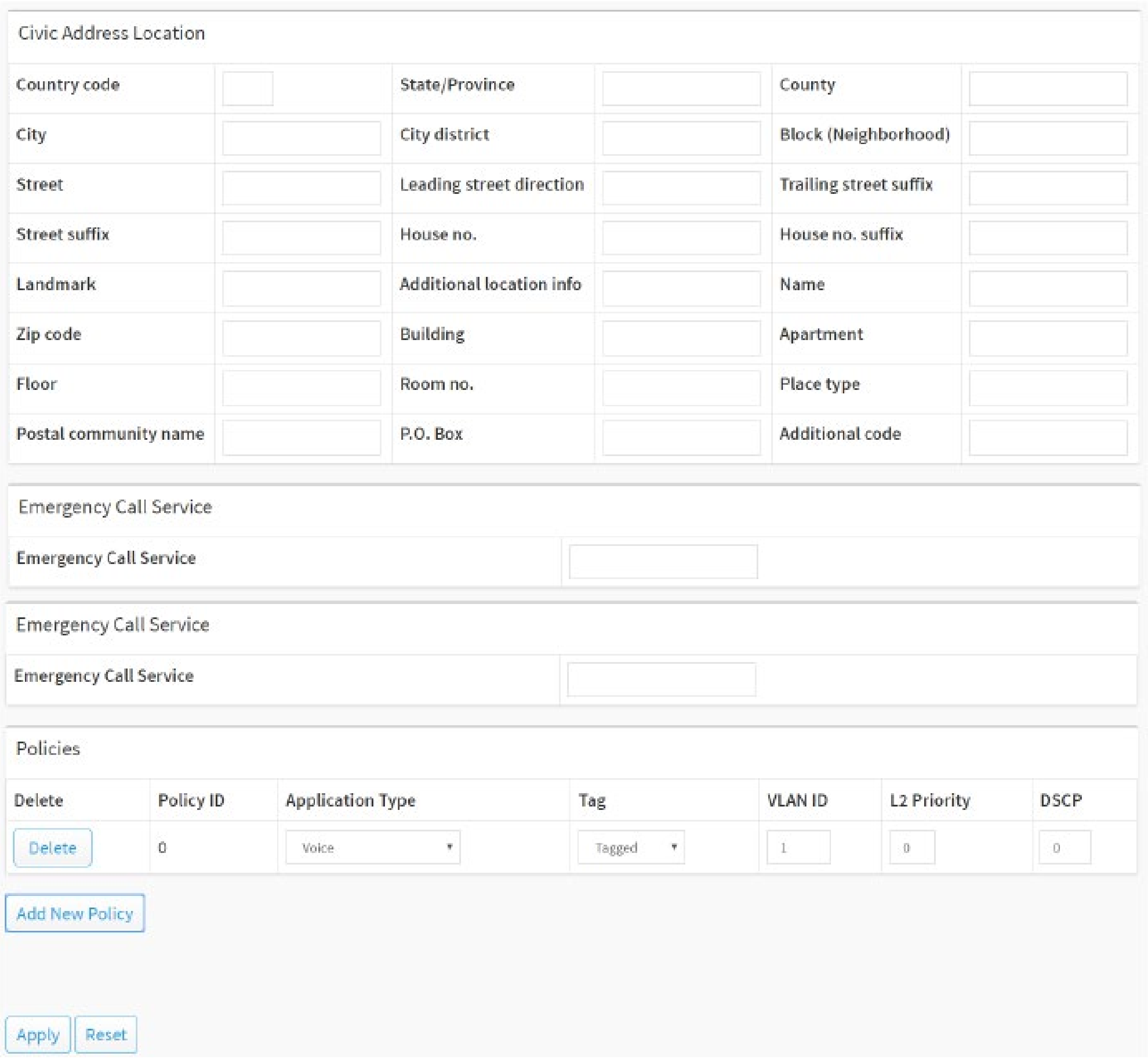
Fast start repeat count	4

Transmit TLVs

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

Coordinates Location

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



Civic Address Location

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

Emergency Call Service

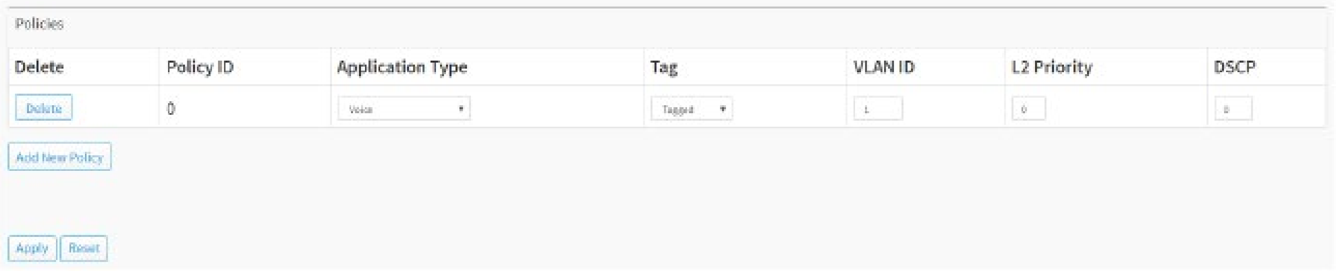
Emergency Call Service	

Emergency Call Service

Emergency Call Service	

Policies

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



Policies

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

Figure 2-4.2: LLDP-MED Configuration

Parameter descriptions :

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

With this in mind LLDP-MED defines an LLDP-MED Fast Start interaction between the protocol and the application layers on top of the protocol, in order to achieve these related properties. Initially, a Network Connectivity Device will only transmit LLDP TLVs in an LLDPDU. Only after an LLDP-MED Endpoint Device is detected, will an LLDP-MED capable Network Connectivity Device start to advertise LLDP-MED TLVs in outgoing LLDPDUs on the associated port. The LLDP-MED application will temporarily speed up the transmission of the LLDPDU to start within a second, when a new LLDP-MED neighbor has been detected in order 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, it is recommended to repeat the fast start transmission multiple times to increase the possibility of the neighbors receiving the LLDP frame. With Fast start repeat count it is possible to specify the number of times the fast start transmission would be repeated. The recommended value is 4 times, given that 4 LLDP frames with a 1 second interval will be transmitted, when an LLDP frame with new information is received.

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

Transmit TLVs

Port : The interface name to which the configuration applies.

Capabilities : When checked the switch's capabilities is included in LLDP-MED information transmitted.

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

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

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

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

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

1. LAN Switch/Router
2. IEEE 802.1 Bridge
3. IEEE 802.3 Repeater (included for historical reasons)
4. IEEE 802.11 Wireless Access Point
5. Any device that supports the IEEE 802.1AB and MED extensions that can relay IEEE 802 frames via any method.

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

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

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

Coordinates Location

Latitude : Latitude should be normalized to within 0-90 degrees with a maximum of 4 digits. It is possible to specify the direction to either North of the equator or South of the equator.

Longitude : Longitude should be normalized to within 0-180 degrees with a maximum of 5 digits. It is possible to specify the direction to either East of the prime meridian or West of the prime meridian.

Altitude : Altitude should be normalized to within -32767 to 32767 with a maximum of 4 digits. It is possible to select between two altitude types (floors or meters).

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

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

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

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

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

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

Civic Address Location

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

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

State/Province : National subdivisions (state, canton, region, province, prefecture).

County : County, parish, gun (Japan), district.

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

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

Block (Neighborhood) : Neighborhood, bock.

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 (Public Safety Answering Point). This format consists of a numerical digit string, corresponding to the ELIN to be used for emergency calling.

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

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

The network policy attributes advertised are:

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

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

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

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

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

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

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

Application Type : Select the intended use of the application types:

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.

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

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.

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

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

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

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.

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

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

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

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

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

L2 Priority : The Layer 2 priority to be used for the specified application type. L2 Priority may specify one of eight priority levels (0 - 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 : The DSCP value to be used to provide Diffserv node behavior for the specified application type as defined in IETF RFC 2474. DSCP may contain one of 64 code point values (0 - 63). A value of 0 represents use of the default DSCP value as defined in RFC 2475.

Buttons

Add 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.

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.

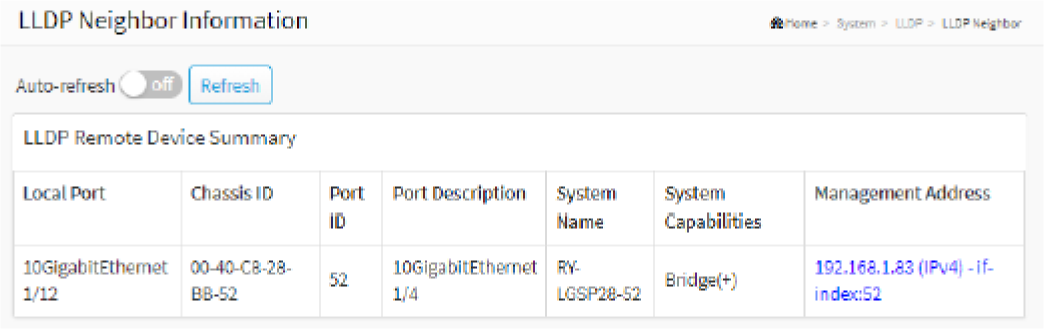
Web Interface

To show LLDP neighbors:

1. Click System, LLDP and LLDP Neighbor.

2. Click Refresh to manually update the web page.

3. Click Auto-refresh to automatically update the webpage.



LLDP Neighbor Information

LLDP Remote Device Summary

Local Port	Chassis ID	Port ID	Port Description	System Name	System Capabilities	Management Address
10GigabitEthernet 1/12	00-40-C8-28-BB-52	52	10GigabitEthernet 1/4	RY-LGSP28-52	Bridge(+)	192.168.1.83 (IPv4) - if-index:52

Figure 2-4.3: LLDP Neighbor Information

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

Parameter descriptions:

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. 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 : 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. You can click the linked text to navigate to the device’s webpage.

Buttons

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

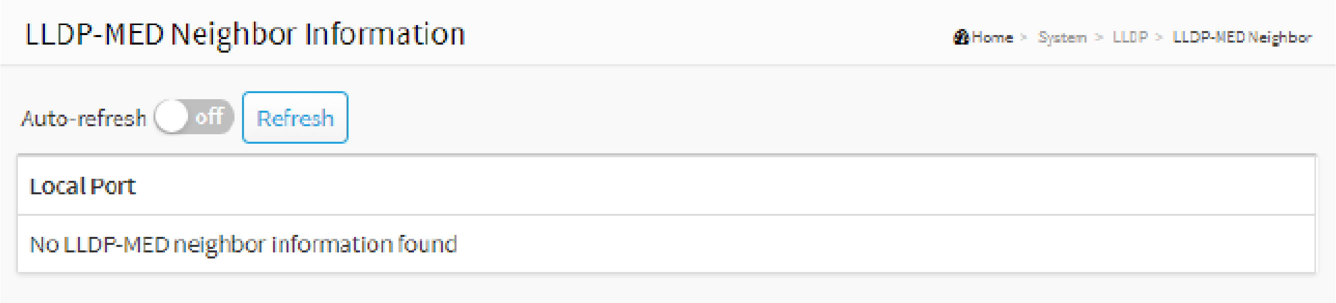
Refresh : Click to refresh the page immediately.

LLDP-MED Neighbor

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

To show LLDP-MED neighbor information in the web UI:

1. Click System, LLDP and LLDP-MED Neighbor.
2. Click Refresh to manually update the web page.
3. Click Auto-refresh to automatically update the web page.



LLDP-MED Neighbor Information

Local Port
No LLDP-MED neighbor information found

Figure 2-4.4: 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 descriptions:

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

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

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

- LLDP-MED Generic Endpoint (Class I) : The LLDP-MED Generic Endpoint (Class I) definition is applicable to all endpoint products that require the base LLDP discovery services defined in TIA-1057, however do not support IP media or act as an end-user communication appliance. Such devices may include (but are not limited to) IP Communication Controllers, other communication related servers, or any device requiring basic services as defined in TIA-1057. Discovery services defined in this class include LAN configuration, device location, network policy, power management, and inventory management.
- LLDP-MED Media Endpoint (Class II) : The LLDP-MED Media Endpoint (Class II) definition is applicable to all endpoint products that have IP media capabilities however may or may not be associated with a particular end user. Capabilities include all of the capabilities defined for the previous Generic Endpoint Class (Class I) and are extended to include aspects related to media streaming. Example product categories expected to adhere to this class include (but are not limited to) Voice / Media Gateways, Conference Bridges, Media Servers, and similar. Discovery services defined in this class include media-type-specific network layer policy discovery.
- LLDP-MED Communication Endpoint (Class III) : The LLDP-MED Communication Endpoint (Class III) definition is applicable to all endpoint products that act as end user communication appliances supporting IP media. Capabilities include all of the capabilities defined for the previous Generic Endpoint (Class I) and Media Endpoint (Class II) classes and are extended to include aspects related to end user devices. Example product categories expected to adhere to this class include (but are not limited to) end user communication appliances, such as IP Phones, PC-based softphones, or other communication appliances that directly support the end user. Discovery services defined in this class include provision of location identifier (including ECS / E911 information), embedded L2 switch support, inventory management.

LLDP-MED Capabilities : Describes the neighborhood unit's LLDP-MED capabilities. Possible capabilities are:

1. LLDP-MED capabilities
2. Network Policy
3. Location Identification
4. Extended Power via MDI - PSE
5. Extended Power via MDI - PD
6. Inventory
7. Reserved

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

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.

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

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.

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

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

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

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.

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

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

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

Defined: The network policy is defined.

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

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

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

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

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

DSCP : DSCP is the DSCP value to be used to provide Diffserv node behavior for the specified application type as defined in IETF RFC 2474. 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.

Inventory : A list of interface items.

Buttons

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

Refresh : Click to refresh the page immediately.

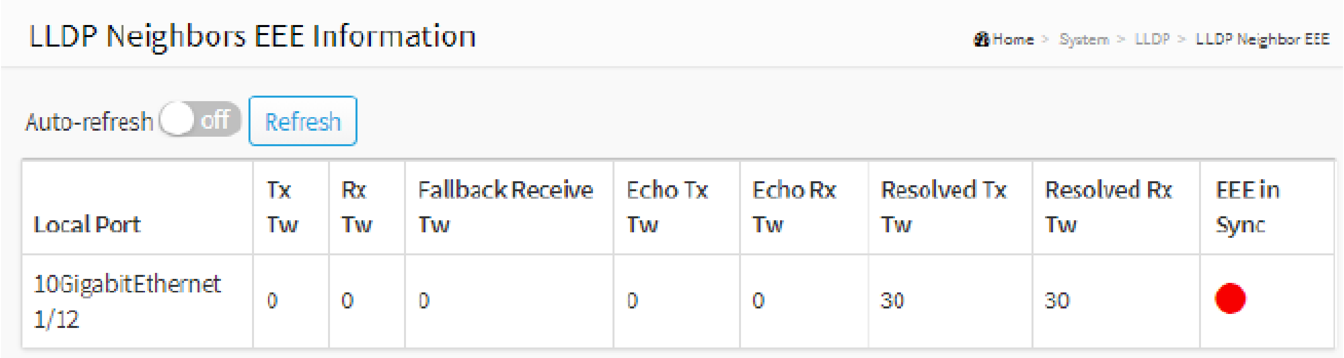
LLDP Neighbor EEE

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

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

To show LLDP Neighbor EEE information in the web UI:

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


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

Local Port	Tx Tw	Rx Tw	Fallback Receive Tw	Echo Tx Tw	Echo Rx Tw	Resolved Tx Tw	Resolved Rx Tw	EEE in Sync
10GigabitEthernet 1/12	0	0	0	0	0	30	30	●

Figure 2-4.5: LLDP Neighbor EEE Information

Parameter descriptions:

Local Port : The interface at which LLDP frames are received or transmitted.

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

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

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

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

Echo Rx Tw : The link partner's Echo Rx Tw value.

Resolved Tx Tw : The resolved Tx Tw for this link. Note : NOT the link partner. The resolved value that is the actual "tx wakeup time " used for this link (based on EEE information exchanged via LLDP).

Resolved Rx Tw : The resolved Rx Tw for this link. Note : NOT the link partner. The resolved value that is the actual "tx wakeup time " used for this link (based on EEE information exchanged via LLDP).

EEE in Sync : Shows whether the switch and the link partner have agreed on wake times.

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

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

Buttons

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

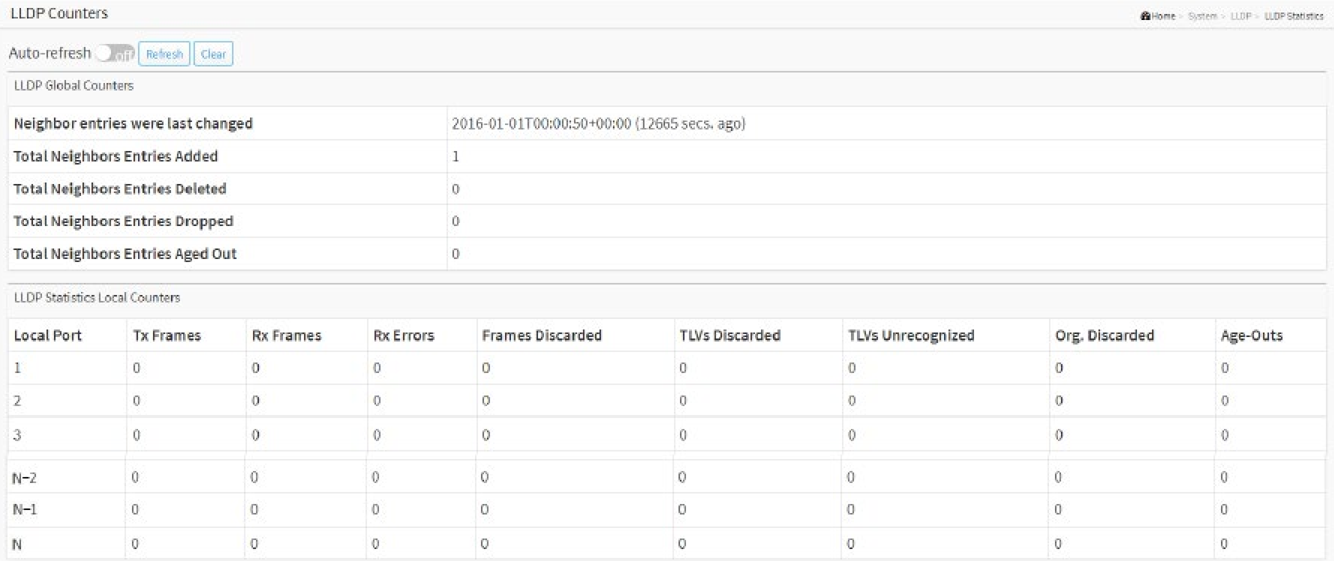
Refresh : Click to refresh the page immediately.

LLDP Statistics

Two types of counters are shown. Global counters are counters that refer to the whole switch; Local counters refer to per-port counters for the switch.

To show LLDP Statistics:

1. Click System, LLDP and LLDP Statistics.
2. Click Refresh to manually update the web page.
3. Click Auto-refresh to automatically update the web page.
4. Click Clear to clear all counters.



LLDP Global Counters

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

LLDP Statistics Local Counters

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

Figure 2-4.6: LLDP Statistics information

Parameter descriptions:

Global Counters

Neighbor entries were last changed : 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.

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 (Type Length Values). If a TLV is malformed, it is counted and discarded.

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

Org. Discarded : The number of organizationally received TLVs.

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

Buttons

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

Refresh : Click to manually refresh the page immediately.

Clear : Clears the counters for the selected port.

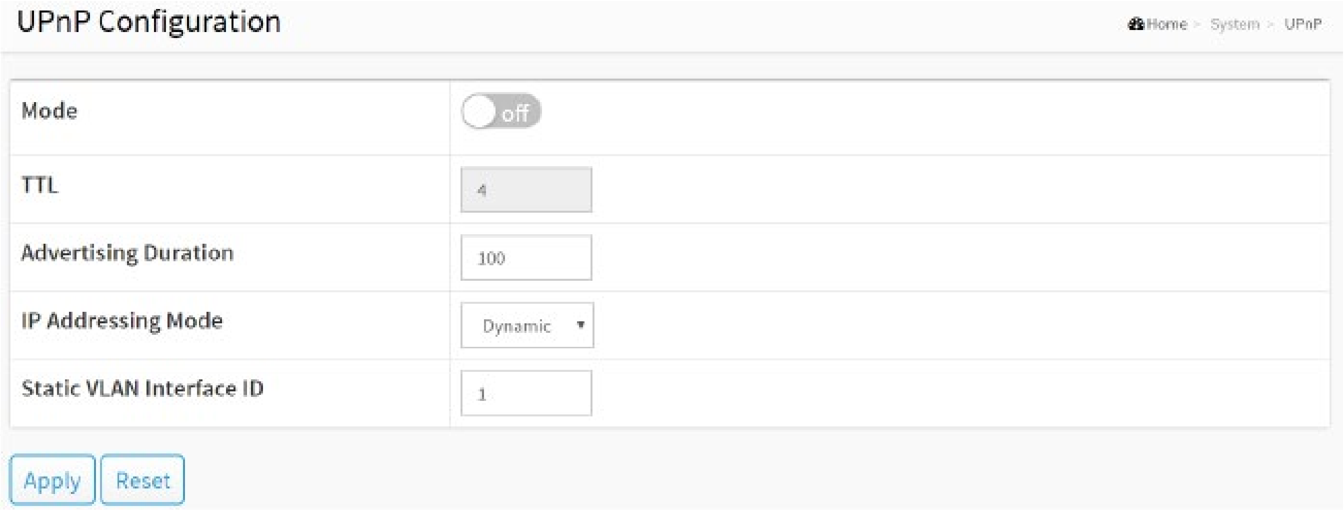
UPnP

UPnP (Universal Plug and Play) was promoted by the UPnP Forum to enable simple robust connectivity to stand-alone devices and PCs from over 800 vendors of consumer electronics, network computing, etc. UPnP has been managed by the Open Connectivity Foundation (OCF) since 2016.

Web Interface

To configure UPnP in the web UI:

1. Click System and UPnP.
2. Select the mode to **on** (enable) or **off** (disable).
3. Specify the parameters in each blank field.
4. Click the Apply button to save the settings.
5. To cancel the settings, click the Reset button to revert to previously saved values.



UPnP Configuration

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

Figure 2-5: UPnP Configuration

Parameter descriptions:

Mode : Indicates the UPnP operation mode. Possible modes are:

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

TTL : Time To Live value used by UPnP to send SSDP advertisement messages. Valid values are 1 - 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, the standard recommends 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 100 - 86400.

IP Addressing Mode : IP addressing mode provides two ways to determine IP address assignment:

__Dynamic__: The UPnP module helps users choose the IP address of the switch device. It finds the first available system IP address. This is the default setting for UPnP.

__Static__: User specifies the IP interface VLAN for choosing the IP address of the switch device.

Static VLAN Interface ID : The index of the specific IP VLAN interface. It will only be applied when IP Addressing Mode is “Static”. Valid values are 1 - 4095. The default value is 1.

Buttons

Apply : Click to save changes.

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

4. Port Management

This section lets you view and set Port parameters of the switch. You can use Port management to enable or disable switch ports and monitor ports' content or status.

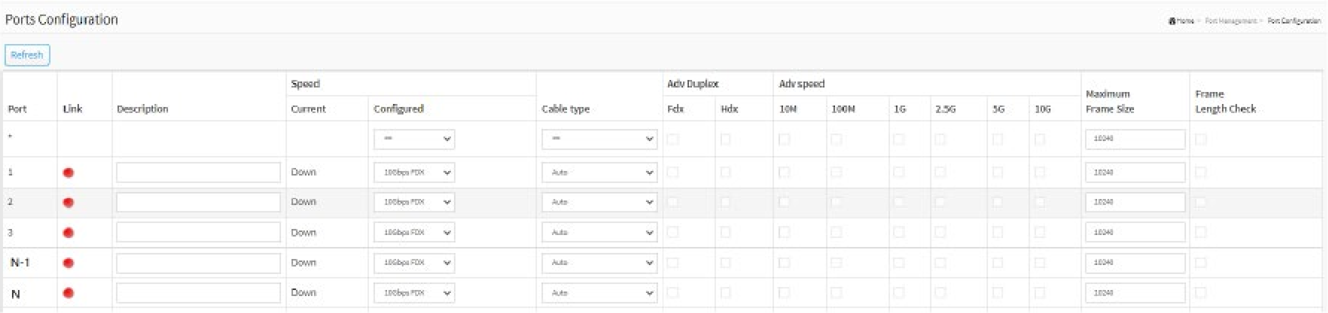
Port Configuration

This page lets you view and set port parameters.

Web Interface

To configure Port Configuration parameters in the web UI:

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



Ports Configuration

			Speed			Adv Duplex		Adv speed						Maximum	Frame
Port	Link	Description	Current	Configured	Cable type	Fdx	Hdx	10M	100M	1G	2.5G	5G	10G	Frame Size	Length Check
*				<>	<>	□	□	□	□	□	□	□	□	10240	□
1	●		Down	10Gbps FDX	Auto	□	□	□	□	□	□	□	□	10240	□
2	●		Down	10Gbps FDX	Auto	□	□	□	□	□	□	□	□	10240	□
3	●		Down	10Gbps FDX	Auto	□	□	□	□	□	□	□	□	10240	□
N-1	●		Down	10Gbps FDX	Auto	□	□	□	□	□	□	□	□	10240	□
N	●		Down	10Gbps FDX	Auto	□	□	□	□	□	□	□	□	10240	□

Figure 3-1: Ports Configuration

Parameter descriptions:

Port : This is the logical port number for this row.

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

Description : Enter up to 63 characters as a descriptive name that identifies this port.

Current Link Speed Status: Provides the current link speed of the port (Down or Up).

Configured Link Speed : Selects any available link speed for the given switch port. Only the speed supported by the specific port is 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 cu port in 10Mbps half duplex mode.

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

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

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

10Gbps FDX - Forces the port in 10Gbps full duplex Flow Control.

1Gbps FDX - Forces the port in 1Gbps full duplex Flow Control :

When Auto Speed is selected on a port, this page 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.

Cable type : At the dropdown select the 10G cable type setting. The default is ***Auto***.

Auto: SFP interface in "auto" mode. Automatic SerDes tuning for optical and DAC-3m cables (default).

DAC-1m: SFP interface in "DAC-1m" mode. Manual SerDes tuning specifically for DAC-1m cables.

DAC-2m: SFP interface in "DAC-2m" mode. Manual SerDes tuning specifically for DAC-2m cables.

DAC-3m: SFP interface in "DAC-3m" mode. Manual SerDes tuning specifically for DAC-3m cables.

DAC-5m: SFP interface in "DAC-5m" mode. Manual SerDes tuning specifically for DAC-5m cables.

Adv Duplex: When duplex is set as Auto (auto negotiation), the port will only advertise the specified duplex as either Fdx or Hdx to the link partner. By default, port will advertise all the supported duplexes if the Duplex is Auto.

Adv Speed: When Speed is set as Auto (auto negotiation), the port will only advertise the specified speeds (10M 100M 1G 2.5G 5G 10G) to the link partner. By default, ports will advertise all the supported speeds if speed is set as Auto. **Note**: The 100FX standard doesn't support Auto Negotiation, so when in 100FX mode the flow control capabilities will always be shown as "disabled".

PFC: When PFC (Priority Flow Control per 802.1Qbb) is enabled on a port then flow control on a priority level is enabled. Through the Priority field, one or more ranges of priorities can be configured (e.g., '0-3,7' which equals '0,1,2,3,7'). PFC is not supported through auto negotiation. PFC and Flow Control cannot both be enabled on the same port.

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

Frame Length Check : Configures if frames with incorrect frame length in the EtherType/Length field will be dropped. An Ethernet frame contains a field EtherType which can be used to indicate the frame payload size (in bytes) for values of 1535 and below.

If the EtherType/Length field is above 1535, it indicates that the field is used as an EtherType (indicating which protocol is encapsulated in the payload of the frame).

If "Frame Length Check" is enabled, frames with payload size less than 1536 bytes are dropped, if the EtherType/Length field doesn't match the actual payload length.

If "Frame Length Check" is disabled, frames are not dropped due to frame length mismatch.

Note: No drop counters count frames are dropped due to frame length mismatch.

Buttons

Refresh : Click to refresh the Port link Status page manually.

Apply : Click to save changes.

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

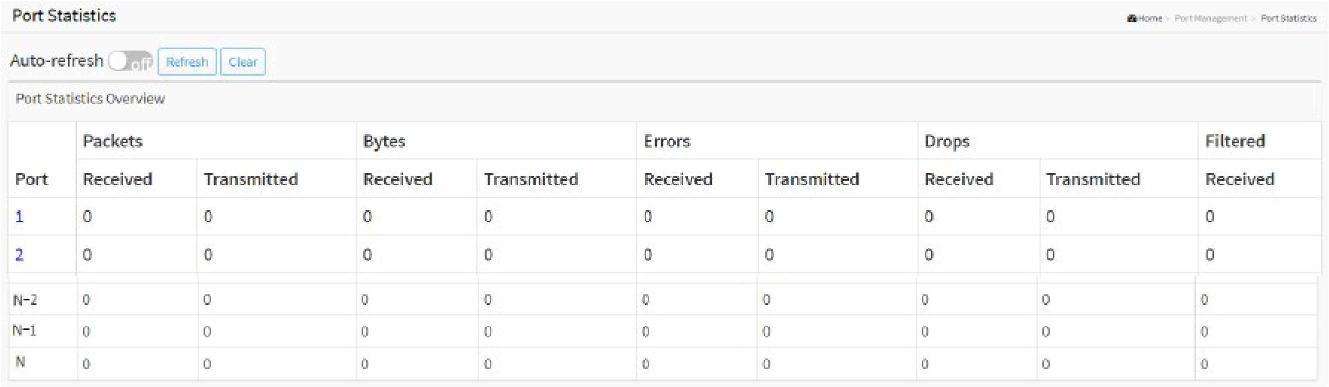
Port Statistics

This page displays Port statistics information and provides general traffic statistics for all switch ports.

Web Interface

To display Port Statistics overview in the web UI:

1. Click Port Management and Port Statistics.
2. To auto-refresh click the “Auto-refresh” button.
3. Click “ Refresh“ to refresh the port statistics or clear all information when you click “ Clear”.
4. To see the details of a port’s statistics, click that port.



Port Statistics Overview

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

Figure 3-2: Port Statistics Overview

Parameter descriptions:

Port : The logical port for the settings contained in the same row. Click the linked Port number to display details of that port’s statistics (see below).

Packets : The number of received and transmitted packets per port.

Bytes : The number of received and transmitted bytes per port.

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

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

Filtered: The number of received frames filtered by the forwarding process.

Buttons

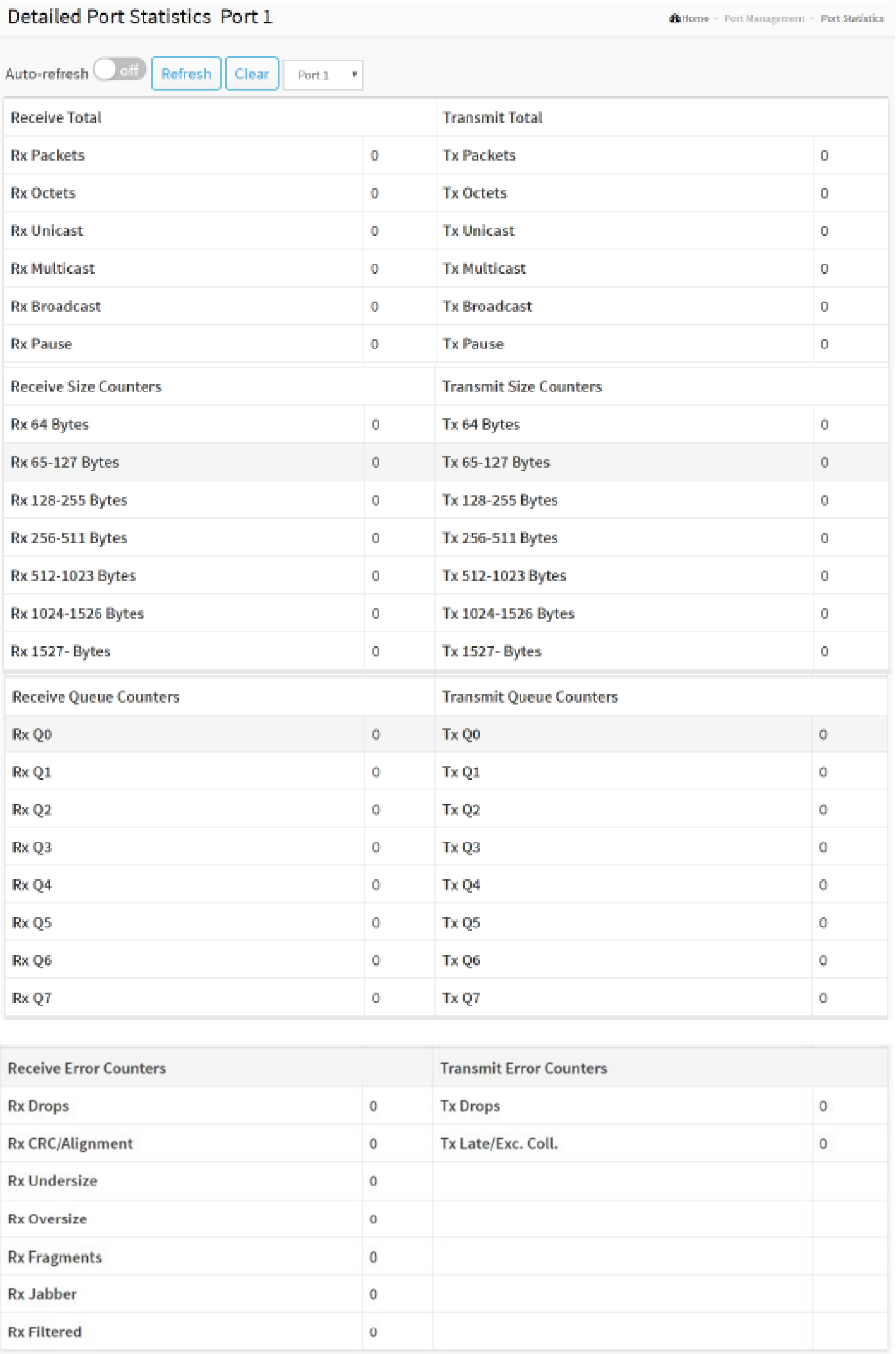
Auto-refresh : Check this box to refresh the page automatically every 3 seconds.

Refresh : Click to manually refresh the page immediately.

Clear : Clears the counters for all ports.

Detailed Port Statistics

To view the details of a port's statistics, click that port. The displayed counters are the totals for receive and transmit, the size counters for receive and transmit, and the error counters for receive and transmit.



Detailed Port Statistics Port 1

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

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

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

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

Figure 3-2: Detailed Port Statistics

Parameter descriptions:

Port select box: Scroll which port to display the Port statistics with “Port-1”, “Port-2”, etc.

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 every 3 seconds.

Refresh : Click to manually refresh the page immediately.

Clear : Clears the counters for the selected port.

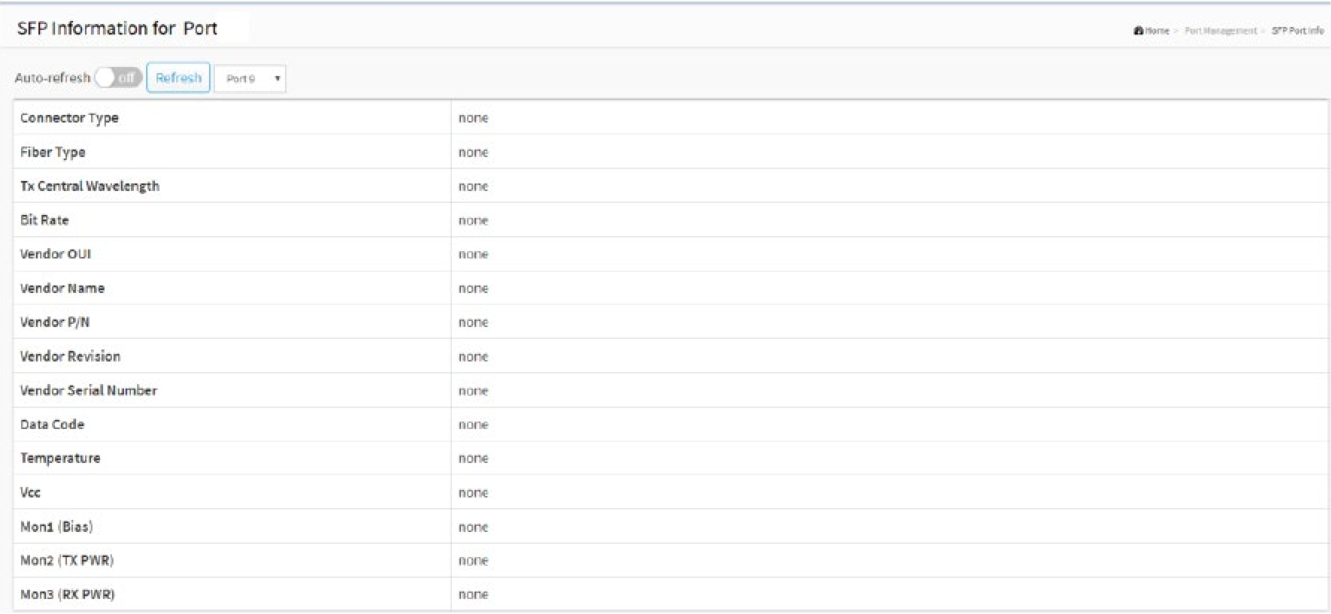
SFP Port Info

This page displays SFP module detail information for SFP modules connected to the switch. The information includes Connector type, Fiber type, wavelength, bit rate, Vendor OUI, etc.

Web Interface

To view SFP information in the web UI:

1. Click Port Management and SFP Port Info.
2. At the Port select dropdown select the desired port.
3. View the SFP Information for the selected port.



SFP Information for Port

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

Figure 3-3: SFP Port Information

Parameter descriptions:

Port select: At the dropdown select which port to display the Port statistics.

Connector Type: Displays the connector type, for instance, UTP, SC, ST, L, etc.

Fiber Type: Displays the fiber mode (e.g., Multi-Mode, Single-Mode).

Tx Central Wavelength: Displays the fiber optical transmitting central wavelength (e.g., 850nm, 1310nm, 1550n, etc.).

Bit Rate: Displays the nominal bit rate of the transceiver (e.g., 1000 Mbps).

Vendor OUI: Displays the Manufacturer's Organizationally Unique Identifier code which is assigned by the IEEE (e.g., 00-c0-f2).

Vendor Name: Displays the company name of the module manufacturer.

Vendor P/N: Displays the manufacturer's product name or part number (e.g., TN-SFP-SXD).

Vendor Revision : Displays the module revision.

Vendor 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 SFP module.

Vcc : Show the working DC voltage of SFP module.

Mon1(Bias) mA : Shows the Bias current of SFP module.

Mon2(TX PWR) : Shows the transmit power of SFP module.

Mon3(RX PWR) : Shows the receiver power of SFP module.

Buttons

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

Refresh : Click to manually refresh the page immediately.

Energy Efficient Ethernet

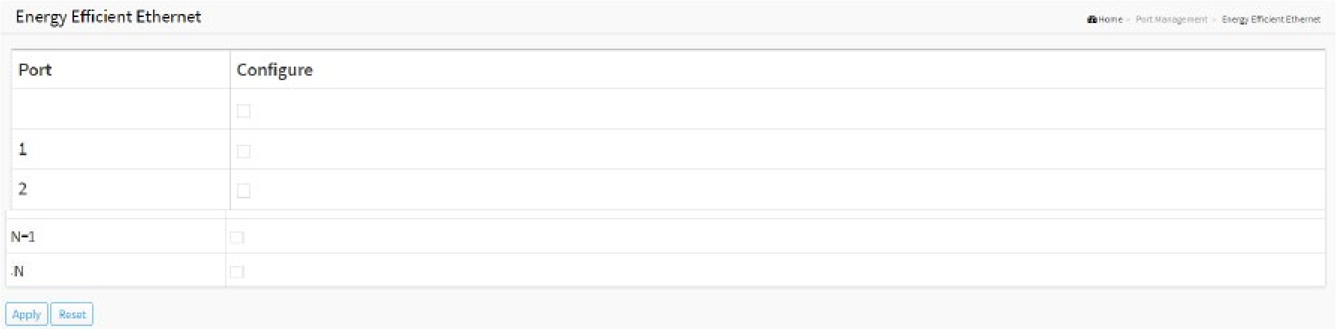
This page lets you view and configure the current EEE port settings. EEE (Energy Efficient Ethernet) is defined in IEEE 802.3az. EEE is a power saving option that reduces the power usage when there is very low traffic utilization (or no traffic).

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

Web Interface

To configure Energy Efficient Ethernet in the web UI:

1. Click Port Management and Energy Efficient Ethernet.
2. Select enable or disable Energy Efficient Ethernet per port.
3. Click the Apply button to save the settings.
4. To cancel the settings, click the Reset button to revert to previously saved values.



Energy Efficient Ethernet

Port	Configure
	□
1	□
2	□
N-1	□
.N	□

Figure 4-4: Energy Efficient Ethernet Configuration

Parameter descriptions:

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.

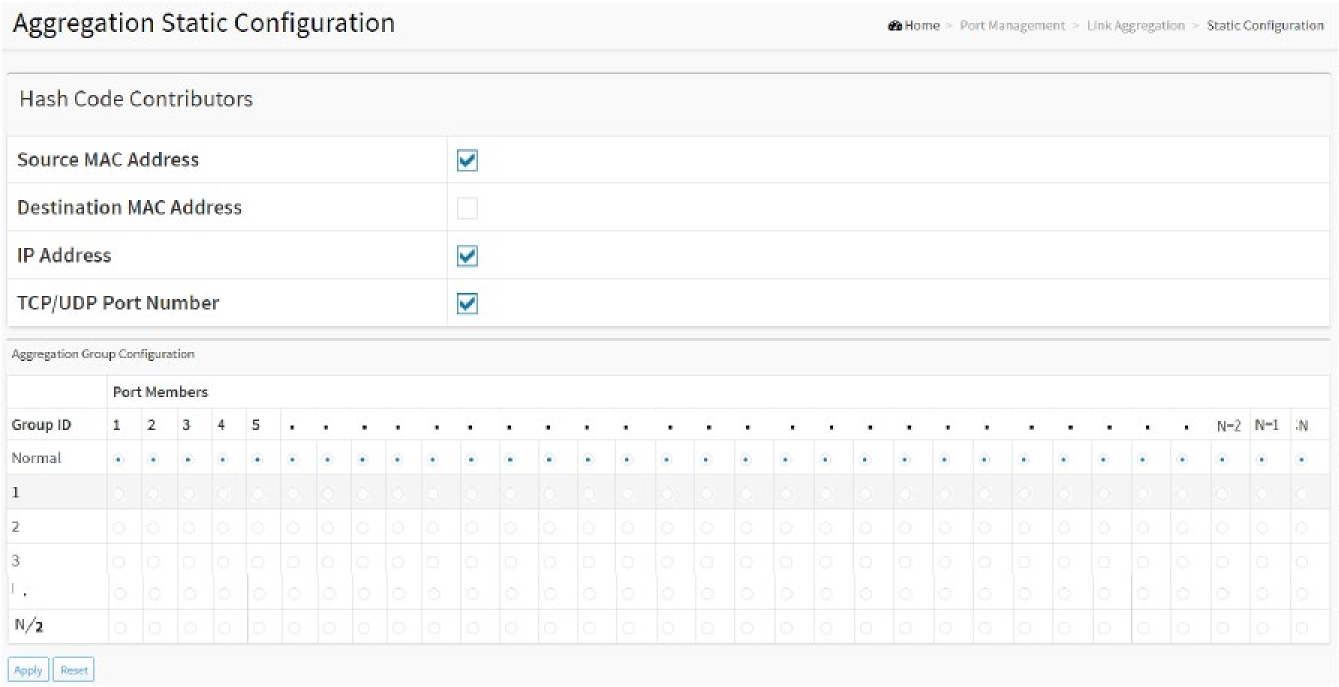
Link Aggregation

Static Configuration

This page lets you configure the Aggregation hash mode and aggregation groups.

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

1. Click Port Management, Link Aggregation and Static Configuration.
2. Evoke to enable or disable the aggregation mode function.
3. Evoke Aggregation Group ID and Port members.
4. Click Apply to save the settings.
5. To cancel the settings, click the Reset button to revert to previously saved values.



Aggregation Static Configuration

Home > Port Management > Link Aggregation > Static Configuration

Hash Code Contributors

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

Aggregation Group Configuration

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

Figure 3-5.1: Aggregation Static Configuration

Parameter descriptions :

<u>Hash Code Contributors</u>

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

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

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

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

Aggregation Group Configuration

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

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

Buttons

Apply : Click to save changes.

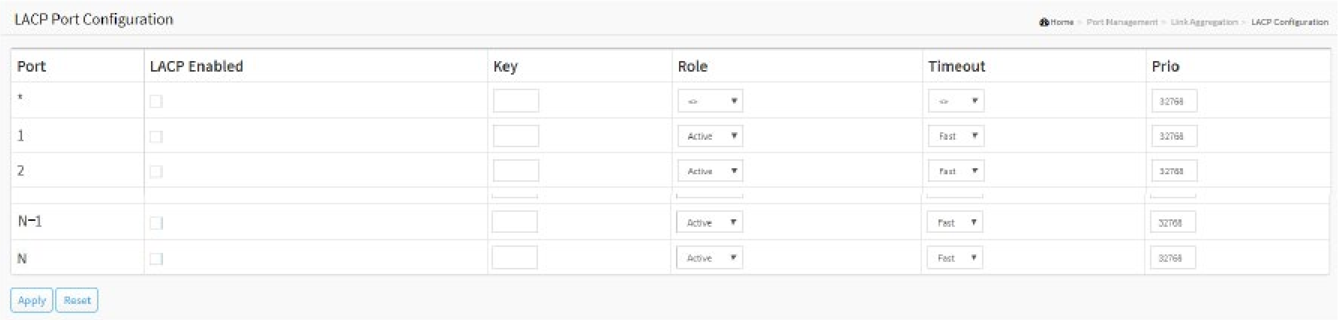
Reset : Click to undo any changes made locally and revert to previously saved values.

LACP Configuration

This page lets you set and view current Link Aggregation Control Protocol port parameters.

To configure LACP Port parameters in the web UI:

1. Click Port Management, Link Aggregation, and LACP Configuration.
2. Enable or disable the LACP on the port of the switch.
3. Select the Key parameter of Auto or Specific. The default is Auto.
4. Select the Role of Active or Passive. The default is Active.
5. Click Apply to save the settings.
6. To cancel the settings, click the reset button to revert to previously saved values.



LACP Port Configuration

Home > Port Management > Link Aggregation > LACP Configuration

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

Figure 3-5.2: LACP Port Configuration

Parameter descriptions:

Port : The switch port number.

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

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

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

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

Prio : Controls the priority of the port. If the LACP partner wants to form a larger group than is supported by this device, then this parameter will control which ports will be active and which ports will be in a backup role.
A lower Prio number means higher priority.

Buttons

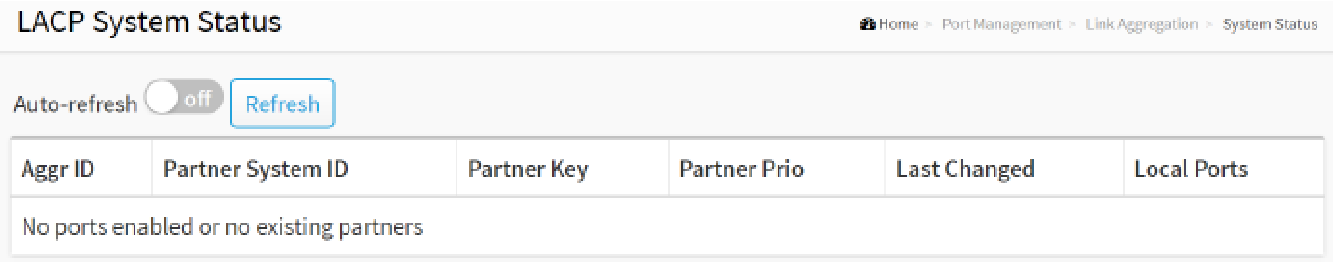
Apply : Click to save changes.

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

System Status

This page provides system status for all LACP instances. To display the LACP System status in the web UI:

1. Click Port Management, Link Aggregation and System Status.
2. Check “Auto-refresh”.
3. Click “Refresh” to refresh the port detailed statistics.


LACP System Status

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

Figure 3-5.3: LACP System Status

Parameter descriptions:

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

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

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

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

Last changed : The time since this aggregation changed.

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

Buttons

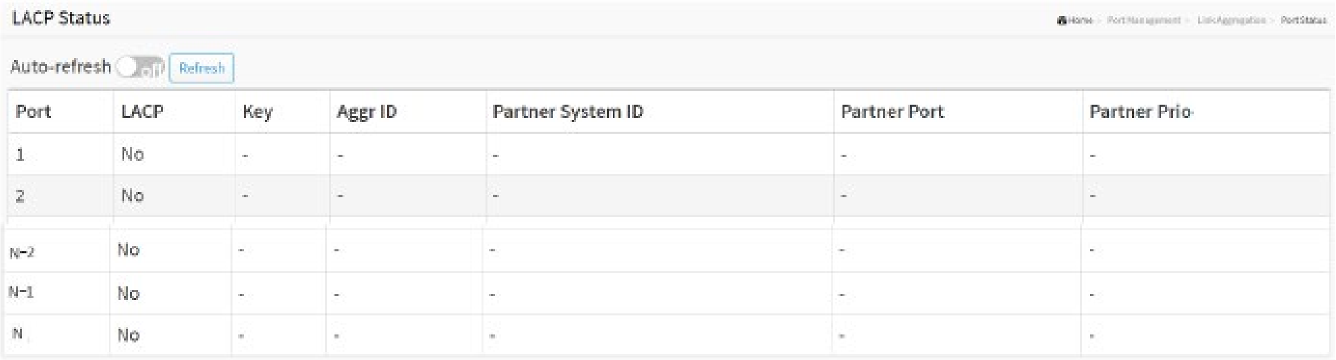
Auto-refresh : Check this box to refresh the page automatically every 3 seconds.

Refresh : Click to manually refresh the page immediately.

Port Status

This page provides a Port Status overview for all LACP instances. To display the LACP Port status in the web UI:

1. Click Port Management, Link Aggregation and Port Status.
2. To automatically refresh the information, click “Auto-refresh”.
3. Click “Refresh” to refresh the LACP Port Status.



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

Figure 3-5.6: LACP Status

Parameter descriptions:

Port : The switch port number.

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

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

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

Partner System ID : The partner's System ID (MAC address).

Partner Port : The partner's port number connected to this port.

Partner Prio : The partner's port priority.

Buttons

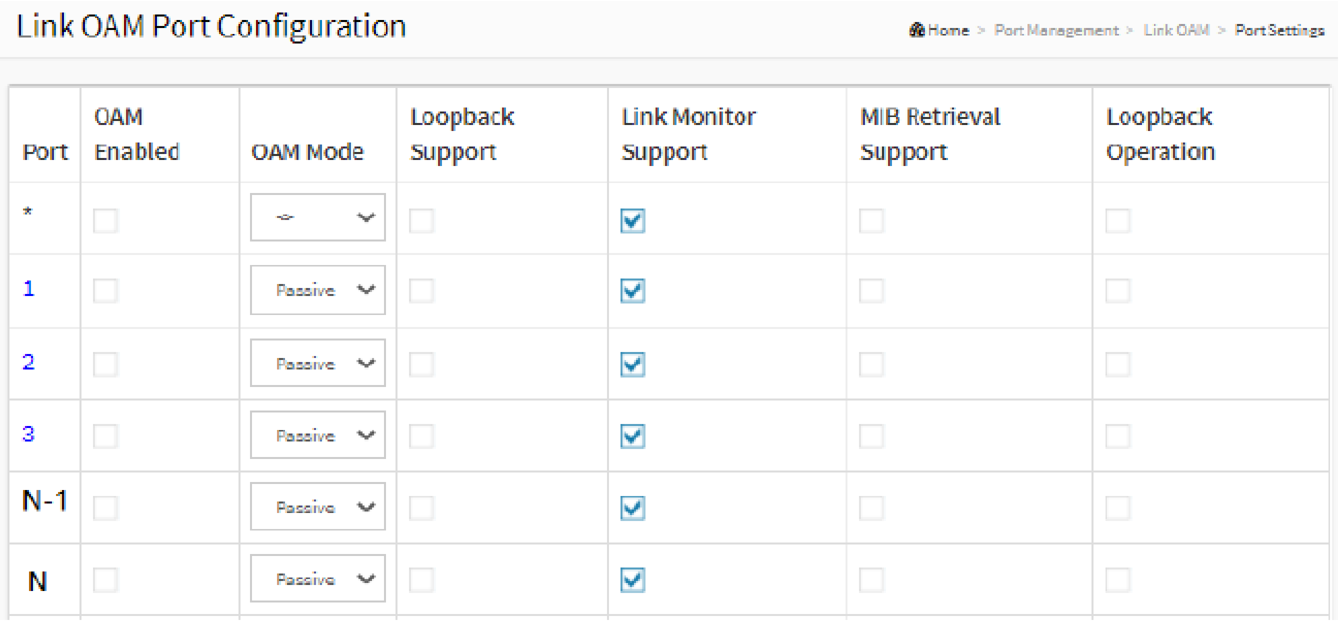
Auto-refresh : Check this box to refresh the page automatically every 3 seconds.

Refresh : Click to manually refresh the page immediately.

Link OAM

Port Settings

This page lets you set and view current Link OAM port parameters.



Link OAM Port Configuration

Port	OAM Enabled	OAM Mode	Loopback Support	Link Monitor Support	MIB Retrieval Support	Loopback Operation
*	□	<>	□	☑	□	□
1	□	Passive	□	☑	□	□
2	□	Passive	□	☑	□	□
3	□	Passive	□	☑	□	□
N-1	□	Passive	□	☑	□	□
N	□	Passive	□	☑	□	□

Figure 3-6.1: Link OAM Port Configuration

Parameter descriptions :

Port: The switch port number.

OAM Enabled : Controls whether Link OAM is enabled on this switch port. Enabling Link OAM provides the network operators the ability to monitor the health of the network and quickly determine the location of failing links or fault conditions.

OAM Mode : Configures the OAM Mode as Active or Passive. The default mode is Passive.

> ***Active*** : DTEs configured in Active mode initiate the exchange of Information OAMPDUs as defined by the Discovery process. Once the Discovery process completes, Active DTE's are permitted to send any OAMPDU while connected to a remote OAM peer entity in Active mode. Active DTE's operate in a limited respect if the remote OAM entity is operating in Passive mode. Active devices should not respond to OAM remote loopback commands and variable requests from a Passive peer.
>
> ***Passive*** : DTEs configured in Passive mode do not initiate the Discovery process. Passive DTE's react to the initiation of the Discovery process by the remote DTE. This eliminates the possibility of passive to passive links. Passive DTE's shall not send Variable Request or Loopback Control OAMPDUs.

Loopback Support : Controls whether loopback support is enabled for the switch port. Link OAM remote loopback can be used for fault localization and link performance testing. Enabling loopback support allows the DTE to execute the remote loopback command that helps in fault detection.

Link Monitor Support : Controls whether Link Monitor support is enabled for the switch port. On enabling Link Monitor support, the DTE supports event notification that permits the inclusion of diagnostic information.

MIB Retrieval Support : Controls whether the MIB Retrieval Support is enabled for the switch port. On enabling the MIB retrieval support, the DTE supports polling of various Link OAM based MIB variables' contents.

Loopback Operation : If the Loopback support is enabled, enabling this field will start a loopback operation for the port.

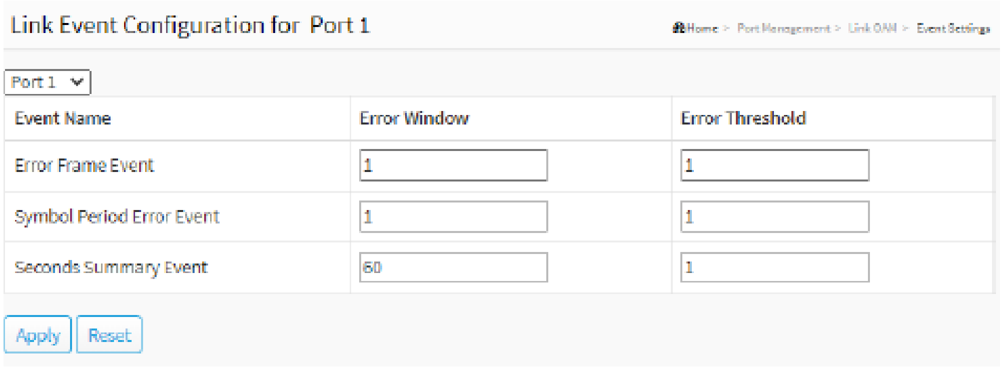
Buttons

Apply : Click to save changes.

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

Event Settings

This page lets you set and view current Link OAM Link Event parameters.



Link Event Configuration for Port 1

Event Name	Error Window	Error Threshold
Error Frame Event	1	1
Symbol Period Error Event	1	1
Seconds Summary Event	60	1

Figure 3-6.2: Link Event Configuration for Port 1

Port : The switch port number.

Event Name : Name of the Link Event which is being configured.

Error Window : Represents the window period in the order of 1 second for observation of various link events.

Error Threshold : Represents the threshold value for the window period for the appropriate Link event so as to notify the peer of this error.

Error Frame Event : Counts the number of errored frames detected during the specified period. The period is specified by a time interval (Window in order of 1 sec). This event is generated if the errored frame count is equal to or greater than the specified threshold for that period (Period Threshold). Errored frames are frames that had transmission errors as detected at the Media Access Control sublayer. Error Window for 'Error Frame Event' must be an integer value between 1-60 and its default value is '1'. Whereas Error Threshold must be between 0-4294967295 and its default value is '1'.

Symbol Period Error Event : Counts the number of symbol errors that occurred during the specified period. The period is specified by the number of symbols that can be received in a time interval on the underlying physical layer. This event is generated if the symbol error count is equal to or greater than the specified threshold for that period. Error Window for 'Symbol Period Error Event' must be an integer value between 1-60 and its default value is '1'. Whereas Error Threshold must be between 0-4294967295 and its default value is '1'.

Seconds Summary Event : The Errored Frame Seconds Summary Event TLV counts the number of errored frame seconds that occurred during the specified period. The period is specified by a time interval. This event is generated if the number of errored frame seconds is equal to or greater than the specified threshold for that period. An errored frame second is a one second interval wherein at least one frame error was detected. Errored frames are frames that had transmission errors as detected at the Media Access Control sublayer. Error Window for 'Seconds Summary Event' must be an integer value between 10-900 and its default value is '60'. Whereas Error Threshold must be 0-65535 and its default value is '1'.

Buttons

Port select box : determines which port is affected by clicking the buttons.

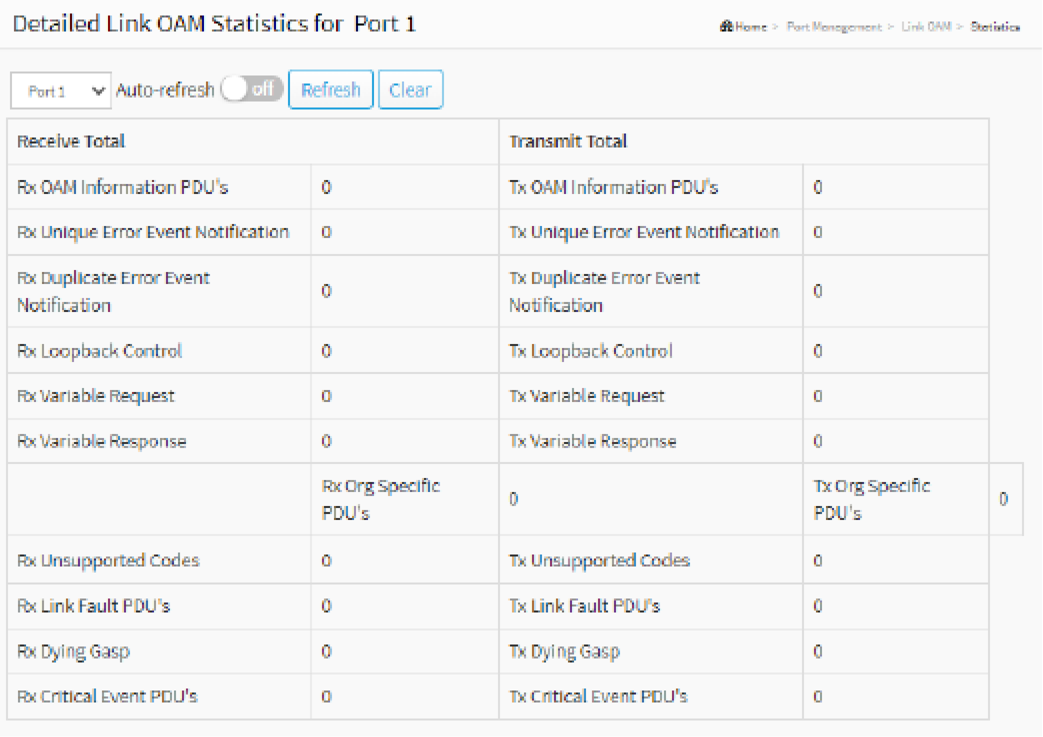
Save: Click to save changes.

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

Statistics

This page provides detailed OAM traffic statistics for a specific switch port. Use the port select box to select which switch port details to display.

The displayed counters represent the total number of OAM frames received and transmitted for the selected port. Discontinuities of these counter can occur at re-initialization of the management system.



Detailed Link OAM Statistics for Port 1

Home > Port Management > Link OAM > Statistics

Port 1 Auto-refresh off Refresh Clear

Receive Total		Transmit Total		
Rx OAM Information PDU's	0	Tx OAM Information PDU's	0	
Rx Unique Error Event Notification	0	Tx Unique Error Event Notification	0	
Rx Duplicate Error Event Notification	0	Tx Duplicate Error Event Notification	0	
Rx Loopback Control	0	Tx Loopback Control	0	
Rx Variable Request	0	Tx Variable Request	0	
Rx Variable Response	0	Tx Variable Response	0	
	Rx Org Specific PDU's	0	Tx Org Specific PDU's	0
Rx Unsupported Codes	0	Tx Unsupported Codes	0	
Rx Link Fault PDU's	0	Tx Link Fault PDU's	0	
Rx Dying Gasp	0	Tx Dying Gasp	0	
Rx Critical Event PDU's	0	Tx Critical Event PDU's	0	

Figure 3-6.3: Detailed Link OAM Statistics for Port 1

Parameter descriptions :

Rx and Tx OAM Information PDUs : The number of received and transmitted OAM Information PDUs. Discontinuities of this counter can occur at re-initialization of the management system.

Rx and Tx Unique Error Event Notification : A count of the number of unique Event OAMPDUs received and transmitted on this interface. Event Notifications may be sent in duplicate to increase the probability of successfully being received, given the possibility that a frame may be lost in transit. Duplicate Event Notification transmissions are counted by Duplicate Event Notification counters for Tx and Rx respectively. A unique Event Notification OAMPDU is indicated as an Event Notification OAMPDU with a Sequence Number field that is distinct from the previously transmitted Event Notification OAMPDU Sequence Number.

Rx and Tx Duplicate Error Event Notification : A count of the number of duplicate Event OAMPDUs received and transmitted on this interface. Event Notification OAMPDUs may be sent in duplicate to increase the probability of successfully being received, given the possibility that a frame may be lost in transit. A duplicate Event Notification OAMPDU is indicated as an Event Notification OAMPDU with a Sequence Number field that is identical to the previously transmitted Event Notification OAMPDU Sequence Number.

Rx and Tx Loopback Control : A count of the number of Loopback Control OAMPDUs received and transmitted on this interface.

Rx and Tx Variable Request : A count of the number of Variable Request OAMPDUs received and transmitted on this interface.

Rx and Tx Variable Response : A count of the number of Variable Response OAMPDUs received and transmitted on this interface

Rx and Tx Org Specific PDUs : A count of the number of Organization Specific OAMPDUs transmitted on this interface.

Rx and Tx Unsupported Codes : A count of the number of OAMPDUs transmitted on this interface with an unsupported op-code.

Rx and Tx Link fault PDUs : A count of the number of Link fault PDUs received and transmitted on this interface.

Rx and Tx Dying Gasp : A count of the number of Dying Gasp events received and transmitted on this interface.

Rx and Tx Critical Event PDUs : A count of the number of Critical event PDUs received and transmitted on this interface.

Buttons

Port select box: determines which port is affected by clicking the buttons.

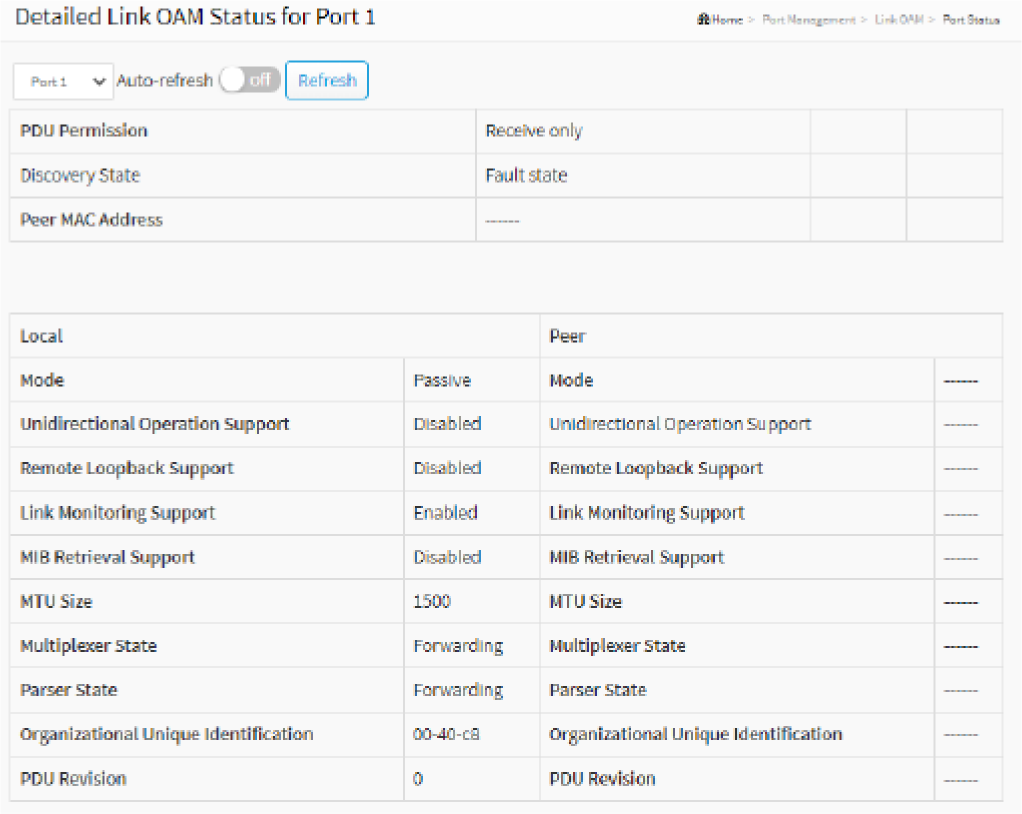
Auto-refresh: Check this box to enable an automatic refresh every 3 seconds.

Refresh: Click to refresh the page immediately.

Clear: Clears the counters for the selected port.

Port Status

This page provides Link OAM configuration operational status. The displayed fields show the active configuration status for the selected port.



Detailed Link OAM Status for Port 1

PDU Permission	Receive only		
Discovery State	Fault state		
Peer MAC Address	------		

Local		Peer	
Mode	Passive	Mode	-------
Unidirectional Operation Support	Disabled	Unidirectional Operation Support	-------
Remote Loopback Support	Disabled	Remote Loopback Support	-------
Link Monitoring Support	Enabled	Link Monitoring Support	-------
MIB Retrieval Support	Disabled	MIB Retrieval Support	-------
MTU Size	1500	MTU Size	-------
Multiplexer State	Forwarding	Multiplexer State	-------
Parser State	Forwarding	Parser State	-------
Organizational Unique Identification	00-40-c8	Organizational Unique Identification	-------
PDU Revision	0	PDU Revision	-------

Figure 3-6.4: Detailed Link OAM Status for Port 1

Parameter descriptions :

PDU Permission : This field is available only for the Local DTE. It displays the current permission rules set for the local DTE. Possible values are "Link fault", "Receive only", "Information exchange only" and "ANY".

Discovery State : Displays the current state of the discovery process. Possible states are Fault state, Active state, Passive state, SEND_LOCAL_REMOTE_STATE, SEND_LOCAL_REMOTE_OK_STATE, SEND_ANY_STATE.

Peer MAC Address : The MAC address of the peer device.

Mode : The Mode in which Link OAM is operating, Active or Passive.

Unidirectional Operation Support : This feature is not available to be configured by the user. The status of this parameter is retrieved from the PHY.

Remote Loopback Support : If status is enabled, the DTE is capable of OAM remote loopback mode.

Link Monitoring Support : If status is enabled, the DTE supports interpreting Link Events.

MIB Retrieval Support : If status is enabled, the DTE supports sending Variable Response OAMPDUs.

MTU Size : It represents the largest OAMPDU, in octets, supported by the DTE. This value is compared to the remotes Maximum PDU Size and the smaller of the two is used.

Multiplexer State : When in forwarding state, the Device is forwarding non-OAMPDUs to the lower sublayer. In case of discarding, the device discards all the non-OAMPDUs.

Parser State : When in forwarding state, Device is forwarding non-OAMPDUs to higher sublayer. When in loopback, Device is looping back non-OAMPDUs to the lower sublayer. When in discarding state, Device is discarding non-OAMPDUs.

Organizational Unique Identification : Displays the 24-bit Organizationally Unique Identifier of the vendor.

PDU Revision : It indicates the current revision of the Information TLV. The value of this field shall start at zero and be incremented each time something in the Information TLV changes. Upon reception of an Information TLV from a peer, an OAM client may use this field to decide if it needs to be processed (an Information TLV that is identical to the previous Information TLV doesn't need to be parsed as nothing in it has changed).

Buttons

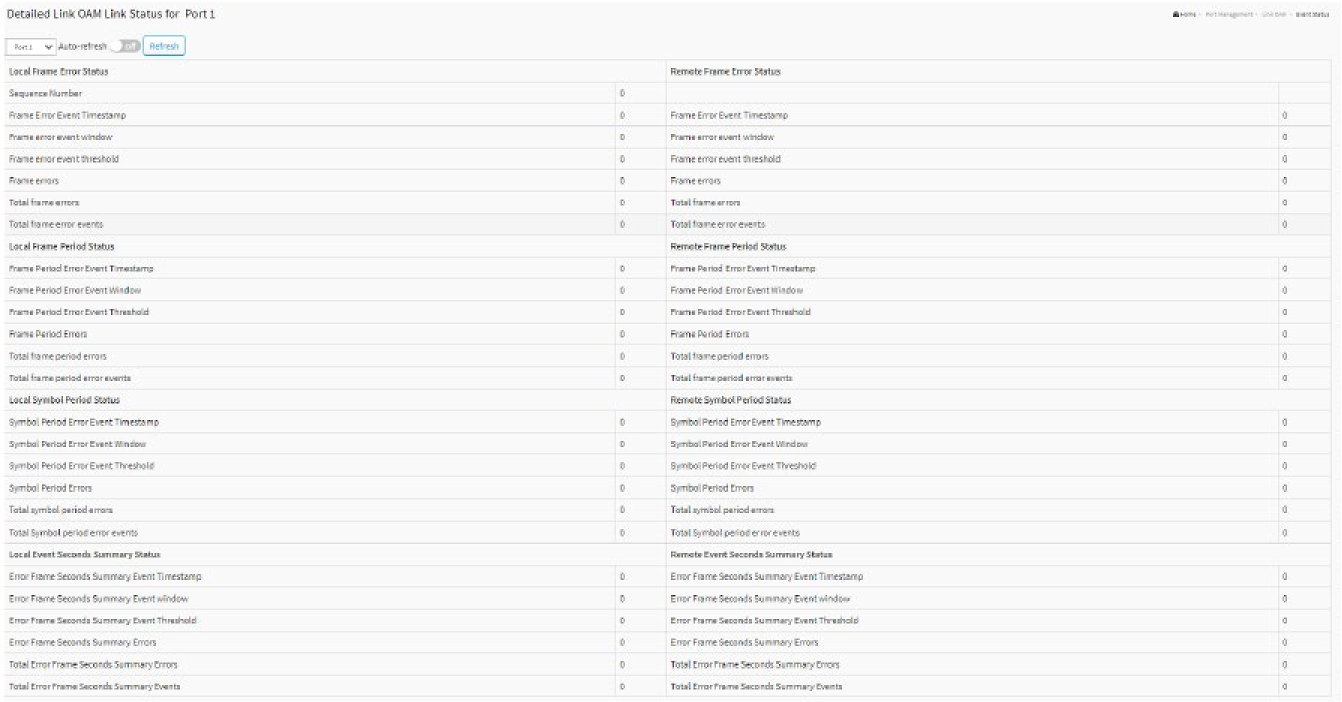
Port select box : At the dropdown select which port’s information is to be displayed.

Refresh : Click to refresh the page immediately.

Auto-refresh : Check this box to enable an automatic refresh every 3 seconds.

Event Status

The left pane displays the Event status for the Local OAM unit while the right pane displays the status for the Peer for the respective port.



Detailed Link OAM Link Status for Port 1

Local Frame Error Status		Remote Frame Error Status	
Sequence Number	0		
Frame Error Event Timestamp	0	Frame Error Event Timestamp	0
Frame error event window	0	Frame error event window	0
Frame error event threshold	0	Frame error event threshold	0
Frame errors	0	Frame errors	0
Total frame errors	0	Total frame errors	0
Total frame error events	0	Total frame error events	0
Local Frame Period Status		**Remote Frame Period Status**	
Frame Period Error Event Timestamp	0	Frame Period Error Event Timestamp	0
Frame Period Error Event Window	0	Frame Period Error Event Window	0
Frame Period Error Event Threshold	0	Frame Period Error Event Threshold	0
Frame Period Errors	0	Frame Period Errors	0
Total frame period errors	0	Total frame period errors	0
Total frame period error events	0	Total frame period error events	0
Local Symbol Period Status		**Remote Symbol Period Status**	
Symbol Period Error Event Timestamp	0	Symbol Period Error Event Timestamp	0
Symbol Period Error Event Window	0	Symbol Period Error Event Window	0
Symbol Period Error Event Threshold	0	Symbol Period Error Event Threshold	0
Symbol Period Errors	0	Symbol Period Errors	0
Total symbol period errors	0	Total symbol period errors	0
Total Symbol period error events	0	Total Symbol period error events	0
Local Event Seconds Summary Status		**Remote Event Seconds Summary Status**	
Error Frame Seconds Summary Event Timestamp	0	Error Frame Seconds Summary Event Timestamp	0
Error Frame Seconds Summary Event window	0	Error Frame Seconds Summary Event window	0
Error Frame Seconds Summary Event Threshold	0	Error Frame Seconds Summary Event Threshold	0
Error Frame Seconds Summary Errors	0	Error Frame Seconds Summary Errors	0
Total Error Frame Seconds Summary Errors	0	Total Error Frame Seconds Summary Errors	0
Total Error Frame Seconds Summary Events	0	Total Error Frame Seconds Summary Events	0

Figure 3-6.5: Detailed Link OAM Link Status for Port 1

Parameter descriptions :

Port : The switch port number.

Sequence Number : This two-octet field indicates the total number of events occurred at the remote end.

Frame Error Event Timestamp : This two-octet field indicates the time reference when the event was generated, in terms of 100 ms intervals.

Frame error event window : This two-octet field indicates the duration of the period in 100 ms intervals.
The default value is one second. The lower bound is one second and the upper bound is one minute.

Frame error event threshold : This four-octet field indicates the number of detected errored frames in the period is required to be equal to or greater than for the event to be generated. The default value is one frame error. The lower bound is zero frame errors, and the upper bound is unspecified.

Frame errors : This four-octet field indicates the number of detected errored frames in the period.

Total frame errors : This eight-octet field indicates the sum of errored frames that have been detected since the OAM sublayer was reset.

Total frame error events : This four-octet field indicates the number of Errored Frame Event TLVs that have been generated since the OAM sublayer was reset.

Frame Period Error Event Timestamp : This two-octet field indicates the time reference when the event was generated, in terms of 100 ms intervals.

Frame Period Error Event Window : This four-octet field indicates the duration of period in terms of frames.

Frame Period Error Event Threshold : This four-octet field indicates the number of errored frames in the period is required to be equal to or greater than in order for the event to be generated.

Frame Period Errors : This four-octet field indicates the number of frame errors in the period.

Total frame period errors : This eight-octet field indicates the sum of frame errors that have been detected since the OAM sublayer was reset.

Total frame period error events : This four-octet field indicates the number of Errored Frame Period Event TLVs that have been generated since the OAM sublayer was reset.

Symbol Period Error Event Timestamp : This two-octet field indicates the time reference when the event was generated, in terms of 100 ms intervals.

Symbol Period Error Event Window : This eight-octet field indicates the number of symbols in the period.

Symbol Period Error Event Threshold : This eight-octet field indicates the number of errored symbols in the period is required to be equal to or greater than for the event to be generated.

Symbol Period Errors : This eight-octet field indicates the number of symbol errors in the period.

Total symbol period errors : This eight-octet field indicates the sum of symbol errors since the OAM sublayer was reset.

Total Symbol period error events : This four-octet field indicates the number of Errored Symbol Period Event TLVs that have been generated since the OAM sublayer was reset.

Error Frame Seconds Summary Event Timestamp : This two-octet field indicates the time reference when the event was generated, in terms of 100 ms intervals, encoded as a 16-bit unsigned integer.

Error Frame Seconds Summary Event window : This two-octet field indicates the duration of the period in terms of 100 ms intervals, encoded as a 16-bit unsigned integer.

Error Frame Seconds Summary Event Threshold : This two-octet field indicates the number of errored frame seconds in the period is required to be equal to or greater than for the event to be generated, encoded as a 16-bit unsigned integer.

Error Frame Seconds Summary Errors : This two-octet field indicates the number of errored frame seconds in the period, encoded as a 16-bit unsigned integer.

Total Error Frame Seconds Summary Errors : This four-octet field indicates the sum of errored frame seconds that have been detected since the OAM sublayer was reset.

Total Error Frame Seconds Summary Events : This four-octet field indicates the number of Errored Frame Seconds Summary Event TLVs that have been generated since the OAM sublayer was reset, encoded as a 32bit unsigned integer.

Buttons

Port select box : Select which port is to be displayed.

Refresh : Click to manually refresh the page immediately.

Auto-refresh : Check this box to enable an automatic refresh every 3 seconds.

Loop Protection

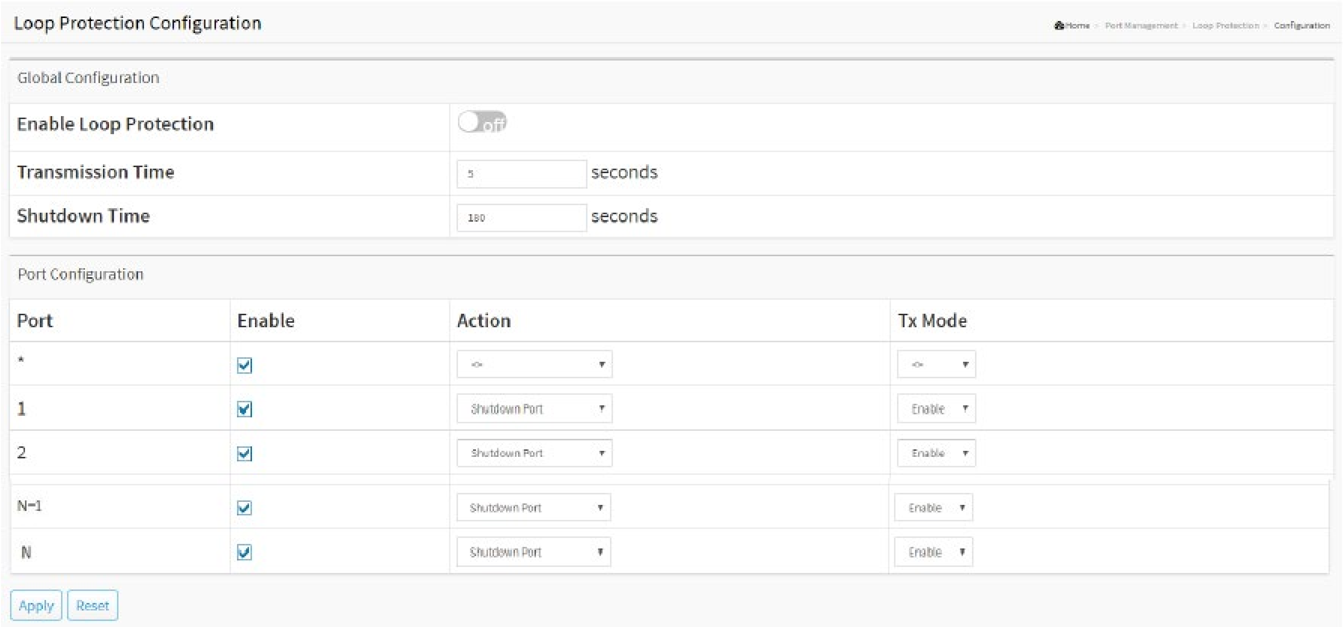
Configuration

Loop Protection is used to detect the presence of traffic. When the switch receives a packet's looping detection frame MAC address that is the same as its own from a port, Loop Protection occurs. The port will be locked when it receives the looping Protection frames. To resume the locked port, determine the looping path, remove the looping path, select the locked port, and click "Resume" to turn the locked port on.

Web Interface

To configure Loop Protection parameters in the web UI:

1. Click Port Management, Loop Protection and Configuration.
2. Evoke to select enable or disable the port loop Protection.
3. Click the Apply button to save the settings.
4. To cancel the settings, click the Reset button to revert to previously saved values.



Loop Protection Configuration

Global Configuration

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

Port Configuration

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

Figure 3-7.1: Loop Protection Configuration

Parameter descriptions :

<u>Global Configuration</u>

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 - 10 seconds. The default is 5 seconds.

Shutdown Time : The period (in seconds) for which a port will be kept disabled in the event of a loop is detected (and the port action shuts down the port). Valid values are 10 to 604800 seconds (7 days). The default is 100 seconds.

<u>Port Configuration</u>

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 PDUs, or whether it is just passively looking for looped PDUs.

Buttons

Apply : Click to save changes.

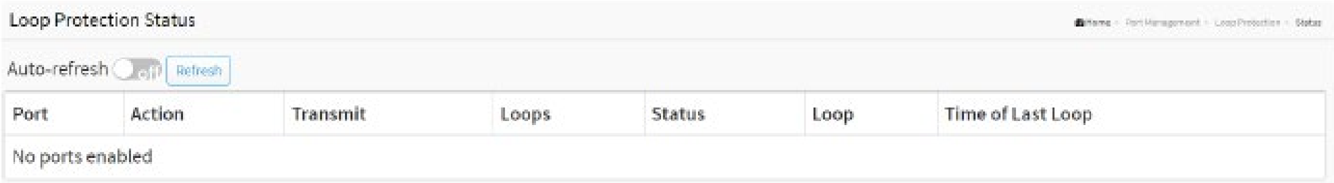
Reset : Click to undo any changes made locally and revert to previously saved values.

Status

This page displays loop protection port status of switch ports.

To display Loop Protection status in the web UI:

1. Click Port Management, Loop Protection and Status.
2. To automatically refresh the information click “Auto refresh”.
3. Click “Refresh” to manually refresh the Loop Protection Status immediately.



Loop Protection Status

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

Figure 3-7.2: Loop Protection Status

Parameter descriptions :

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 every 3 seconds.

Refresh : Click to refresh the page immediately.

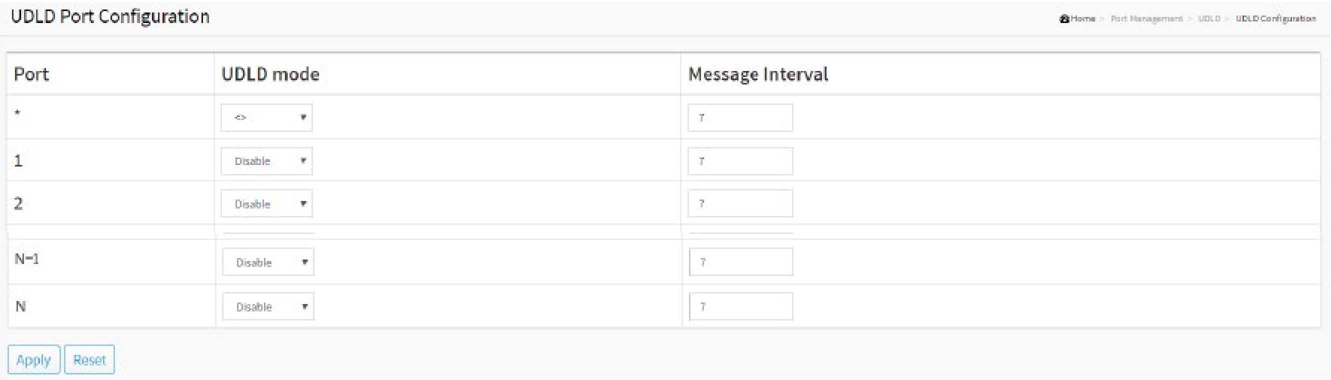
UDLD

UDLD Configuration

This page lets you set and view the current Unidirectional Link Detection parameters.

To configure UDLD parameters in the web UI:

1. Click Port Management, UDLD, and UDLD Configuration.
2. Select enable or disable UDLD mode for each port.
3. Specify the Message Interval.
4. Click Apply to save the settings.
5. To cancel the settings click the Reset button to revert to previously saved values.



UDLD Port Configuration

Home > Port Management > UDLD > UDLD Configuration

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

Figure 3-7.1: UDLD Port Configuration

Parameter description :

Port : Port number of the switch.

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

> ***Disable***: In disabled mode, UDLD functionality doesn't exist on port.
>
> ***Normal***: In normal mode, if the link state of the port was determined to be unidirectional, it will not affect the port state.
>
> ***Aggressive***: In aggressive mode, unidirectional detected ports will get shutdown. To bring back the ports up, need to disable UDLD on that port.

Message Interval : Configures the period of time between UDLD probe messages on ports that are in the advertisement phase and are determined to be bidirectional. The valid range is 7 - 90 seconds.
The default is 7 seconds. Currently only the default time interval is supported due to lack of detailed information in IETF RFC 5171.

Buttons

Apply : Click to save changes.

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

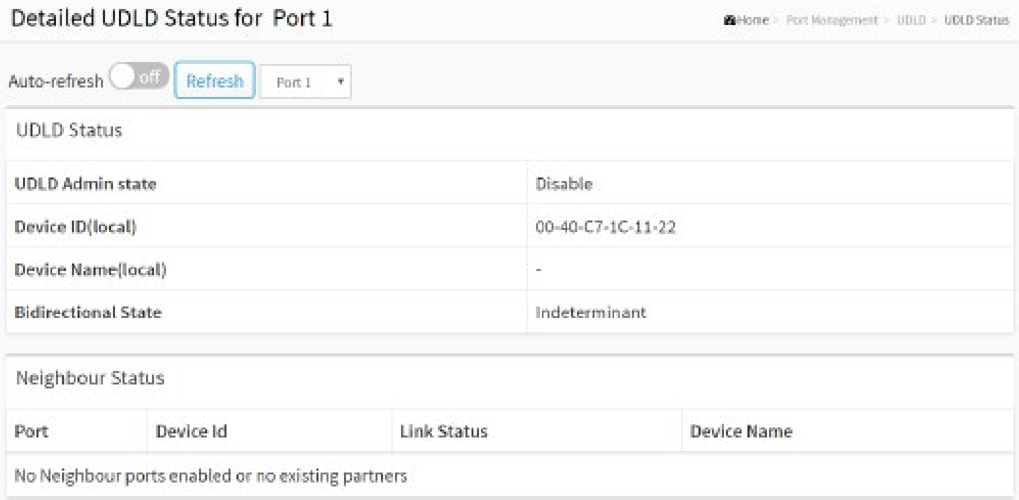
UDLD Status

This page displays the UDLD (Uni Directional Link Detection) status of the ports.

Web Interface

To display ~~Loop Protection~~ UDLD status in the web UI:

1. Click Port Management, UDLD and UDLD Status.
2. At the dropdown select the port on which you want to display UDLD Status.
3. To automatically refresh the page check “Auto refresh”.
4. Click “Refresh” to refresh the Loop Protection Status.



Detailed UDLD Status for Port 1

UDLD Status

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

Neighbour Status

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

Figure 3-7.2: UDLD Status

Parameter descriptions :

UDLD Status

UDLD Admin State : The current port state of the logical port; Enabled if the state (Normal, Aggressive) is Enabled.

Device ID(local) : The ID of Device.

Device Name(local) : Name of the Device.

Bidirectional State : The current state of the port.

Neighbor Status

Port : The current port of neighbor device.

Device ID : The current ID of neighbor device.

Link Status : The current link status of neighbor port.

Device Name : The name of the Neighbor Device.

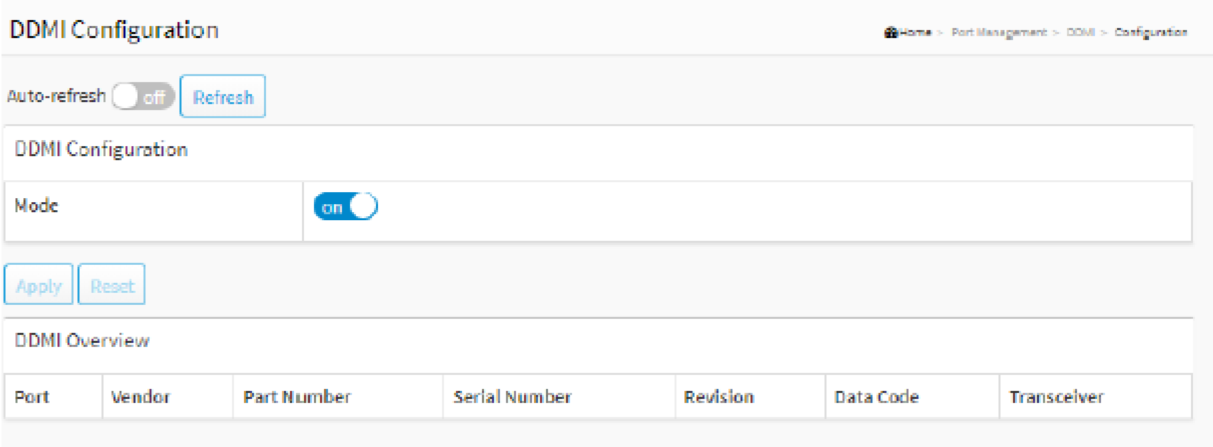
Buttons

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

Refresh : Click to manually refresh the page immediately.

DDMI

Configure Digital Diagnostics Monitoring Interface on this page.



DDMI Configuration

Mode	on

DDMI Overview

Port	Vendor	Part Number	Serial Number	Revision	Data Code	Transceiver

Figure 3-9.1: DDMI Configuration

Parameter descriptions :

DDMI Configuration:

Mode : Select the DDMI mode of operation. Possible modes are:

On: Enable DDMI mode of operation.

Off: Disable DDMI mode of operation.

DDMI Overview:

Port : DDMI port.

Vendor : Indicates the SFP vendor's name.

Part Number : Indicates the Part number provided by the SFP vendor.

Serial Number : Indicates Serial number provided by the SFP vendor.

Revision : Indicates the Revision level provided by the SFP vendor.

Data Code : Indicates the vendor's manufacturing date code.

Transceiver : Indicates Transceiver compatibility.

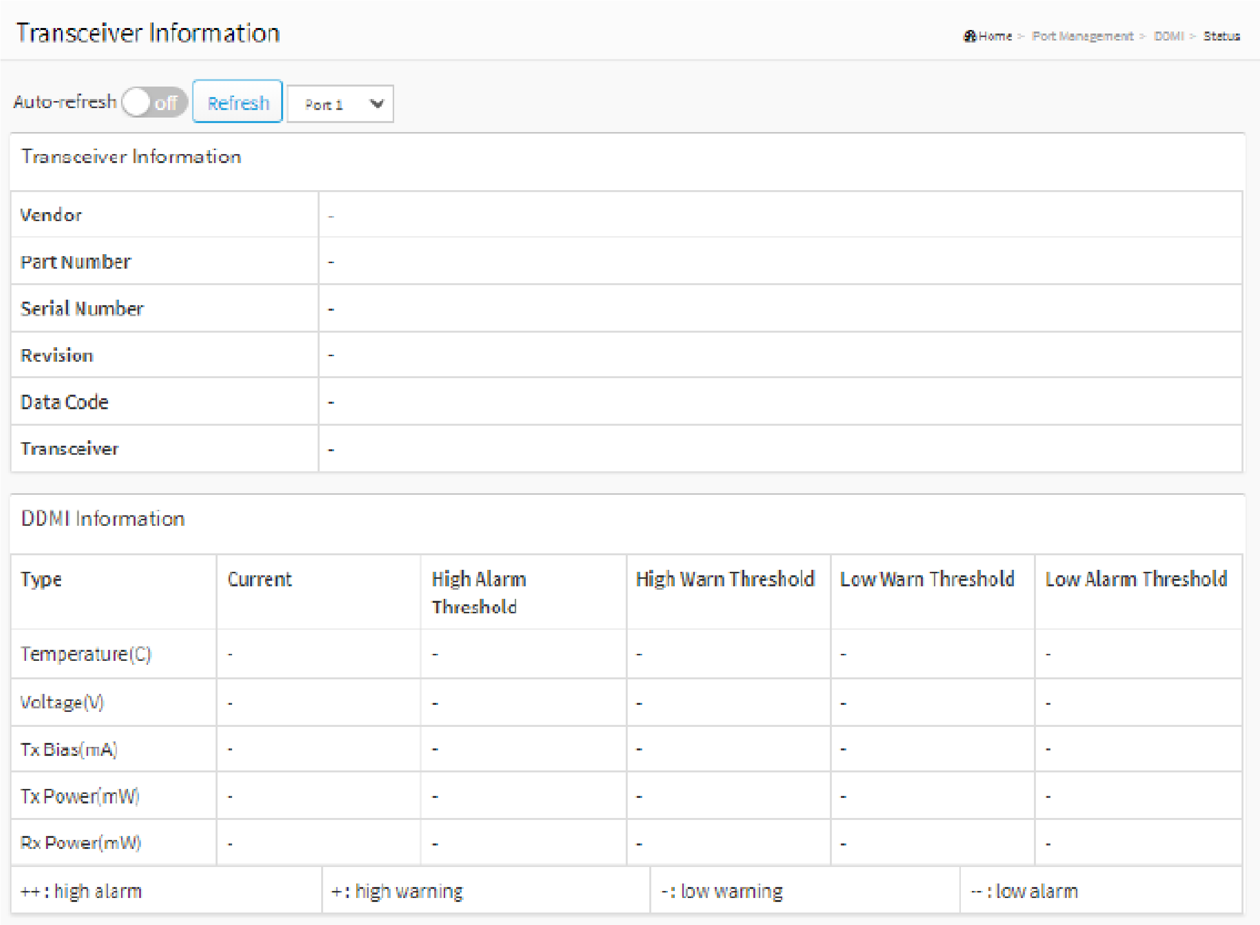
Buttons

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

Refresh: Click to refresh the page immediately.

Status

This page displays detailed Digital Diagnostics Monitoring Interface information.



Transceiver Information

Vendor	-
Part Number	-
Serial Number	-
Revision	-
Data Code	-
Transceiver	-

DDMI Information

Type	Current	High Alarm Threshold	High Warn Threshold	Low Warn Threshold	Low Alarm Threshold
Temperature(C)	-	-	-	-	-
Voltage(V)	-	-	-	-	-
Tx Bias(mA)	-	-	-	-	-
Tx Power(mW)	-	-	-	-	-
Rx Power(mW)	-	-	-	-	-

++ : high alarm | + : high warning | - : low warning | -- : low alarm

Figure 3-9.2: Transceiver Information

Parameter descriptions :

Transceiver Information : This webpage section displays transceiver information.

Vendor : Indicates the SFP vendor's name.

Part Number : Indicates the part number provided by the SFP vendor.

Serial Number : Indicates the serial number provided by the vendor.

Revision : Indicates the Revision level provided by the vendor.

Data Code : Indicates the vendor's manufacturing date code.

Transceiver : Indicates Transceiver compatibility.

DDMI Information : This webpage section displays DDMI information.

Current : The current value of temperature, voltage, TX bias, TX power, and RX power.

High Alarm Threshold : The high alarm threshold value of temperature, voltage, TX bias, TX power, and RX power (++: high alarm, +: high warning, -: low warning, --: low alarm).

High Warn Threshold : The high warn threshold value of temperature, voltage, TX bias, TX power, and RX power.

Low Warn Threshold : The low warn threshold value of temperature, voltage, TX bias, TX power, and RX power.

Low Alarm Threshold : The low alarm threshold value of temperature, voltage, TX bias, TX power, and RX power.

Buttons

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

Refresh: Click to refresh the page immediately.

Port select box : At the dropdown select the desired port.

5. VLAN Management

VLAN Configuration

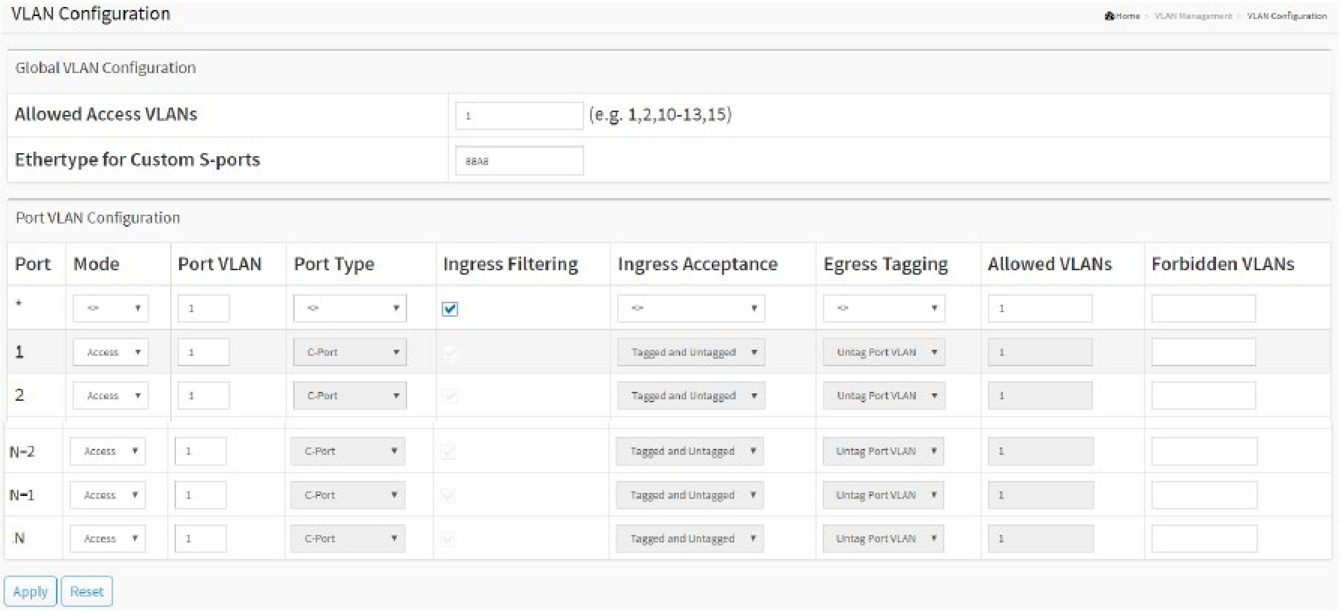
This page lets you assign a specific VLAN for management purposes. The management VLAN is used to establish an IP connection to the switch from a workstation connected to a port in the VLAN. This connection supports an SNMP and Telnet session. By default, the active management VLAN is VLAN 1, but you can set any VLAN as the management VLAN using the Management VLAN window at System > IP Address > Advanced Settings. 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 UI:

1. Click VLAN Management and VLAN Configuration.
2. Modify Global VLAN Configuration parameters.
3. Select the Port VLAN Configuration parameters.
4. Click Apply to save the settings.
5. To cancel the settings, click the Reset button to revert to previously saved values.



Global VLAN Configuration

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

Port VLAN Configuration

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

Figure 5-1: VLAN Configuration

Parameter descriptions:

<u>**Global VLAN Configuration**</u>

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 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 these 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 these characteristics:

- By default, a trunk port is member of all existing VLANs. This may be limited by the use of Allowed VLANs,
- unless VLAN Trunking is enabled on the port, frames classified to a VLAN that the port is not a member of will be discarded,
- by default, all frames but frames classified to the Port VLAN (a.k.a. Native VLAN) get tagged on egress. Frames classified to the Port VLAN do not get C-tagged on egress,
- egress tagging can be changed to tag all frames, in which case only tagged frames are accepted on ingress,
- VLAN trunking may be enabled.

Hybrid: Hybrid ports resemble trunk ports in many ways but adds additional port configuration features. In addition to the characteristics described for trunk ports, Hybrid ports have these abilities:

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

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

Port Type : Ports in hybrid mode allow for changing the port type, that is, whether a frame's VLAN tag is used to classify the frame on ingress to a particular VLAN, and if so, which TPID it reacts on. Likewise, on egress, the Port Type determines the TPID of the tag, if a tag is required. Unaware: On ingress, all frames, whether carrying a VLAN tag or not, get classified to the Port VLAN, and possible tags are not removed on egress.

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

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

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

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

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

Tagged and untagged: both tagged and untagged frames are accepted.

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

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

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

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

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

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

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

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

Buttons

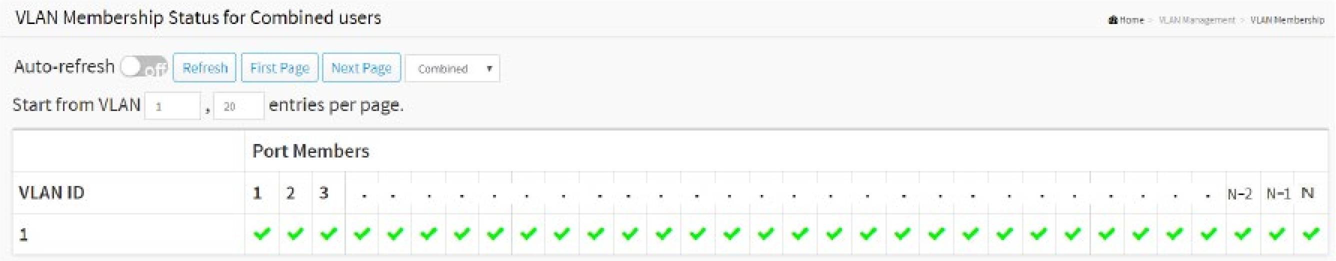
Apply : Click to save changes.

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

Membership

This page provides an overview of membership status of VLAN users. To configure VLAN membership in the web UI:

1. Click VLAN Management and VLAN Membership.
2. At the User select dropdown choose which VLAN users are to be displayed.
3. Use the webpage buttons as required.



VLAN Membership Status for Combined users

Start from VLAN 1 , 20 entries per page.

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

Figure 5-2: VLAN Membership Status

Parameter descriptions:

VLAN User : Various internal software modules may use VLAN services to configure VLAN memberships on the fly. The drop-down list on the right lets you select between showing VLAN memberships as configured by an administrator (Admin) or as configured by one of these internal software modules.

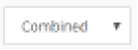
The VLAN User module uses services of the VLAN management functionality to configure VLAN memberships and VLAN port configurations such as PVID and UVID. These VLAN user types are currently supported:

> ***Combined*** : shows a combination of the administrator and internal software modules configuration, and basically reflects what is actually configured in hardware.
>
> ***NAS*** : provides port-based authentication, which involves communications between a Supplicant, Authenticator, and an Authentication Server.
>
> ***GVRP*** : Adjacent VLAN-aware devices can exchange VLAN information with each other by using Generic VLAN Registration Protocol (GVRP). GVRP is based on the Generic Attribute Registration Protocol (GARP) and propagates VLAN information throughout a bridged network.
>
> ***MVR*** : MVR is used to eliminate the need to duplicate multicast traffic for subscribers in each VLAN. Multicast traffic for all channels is sent only on a single (multicast) VLAN.
>
> ***Voice VLAN*** : Voice VLAN is a VLAN configured specially for voice traffic typically originating from IP phones.
>
> ***MSTP*** : The 802.1s Multiple Spanning Tree protocol (MSTP) uses VLANs to create multiple spanning trees in a network, which significantly improves network resource utilization while maintaining a loop-free environment.
>
> ***DMS*** : Shows DMS VLAN membership status.
>
> ***VCL*** : Shows MAC-based VLAN entries configured by various MAC-based VLAN users.

VLAN ID : VLAN ID for which the Port members are displayed.

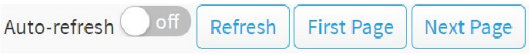
Port Members : A row of check boxes for each port is displayed for each VLAN ID. If a port is included in a VLAN, an image U and T will be displayed. Shows egress filtering frame status whether tagged or untagged. Frames classified to the Port VLAN are transmitted tagged (T) or untagged (U).

Show entries : You can choose how many items you want to be displayed. The VLAN Membership Status page shows the current VLAN port members for all VLANs configured by a selected VLAN User (selection allowed by a Combo box). When “Combined” users are selected, it shows 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.



User select dropdown : At the dropdown choose the VLAN User to be displayed.

Buttons



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

Refresh : Click to manually refresh the page immediately.

First Page : Use the button to start over.

Next Page : Use the last entry of the currently displayed VLAN entry as a basis for the next lookup.

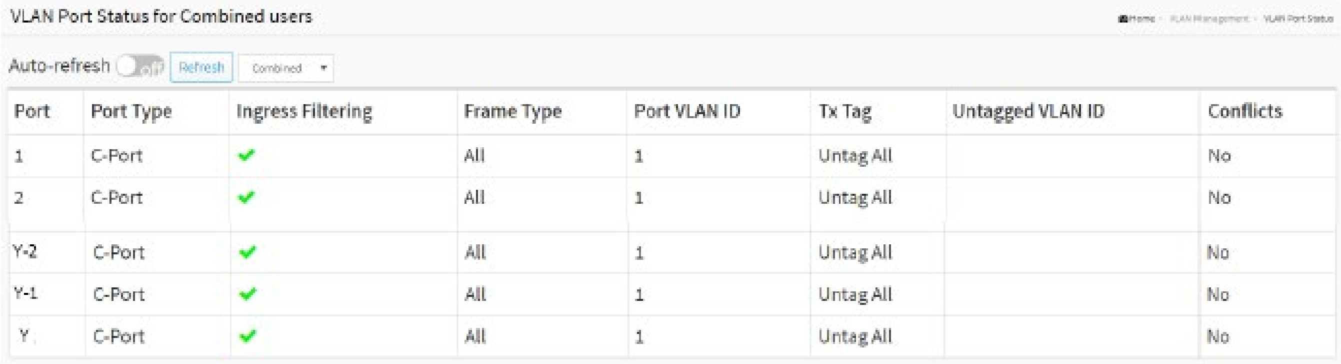
VLAN Port Status

This page displays all VLAN status and reports it in the order of Combined, Admin, NAS, GVRP, MVR, Voice VLAN, MSTP, DMS, VCL.

Web Interface

To display VLAN Port Status in the web UI:

1. Click VLAN Management and VLAN Port Status.
2. At the dropdown select the VLAN User to be displayed.
3. View the displayed Port Status information.


VLAN Port Status for Combined users
Home › VLAN Management › VLAN Port Status
Auto-refresh
off
Refresh
Combined ▾

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

Figure 5-3: VLAN Port Status

Parameter descriptions :

Combined ▾ At the dropdown select the desired VLAN User (Combined, Admin, NAS, GVRP, MVR, Voice VLAN, MSTP, DMS, VCL, RMirror). The VLAN User module uses services of the VLAN management functionality to configure VLAN memberships and VLAN port configuration such as PVID, UVID. These VLAN User types are currently supported:

Combined : Shows a combination of the administrator and internal software modules configuration, and basically reflects what is actually configured in hardware.

Admin : Shows VLAN memberships as configured by an Admin, and not by one of these internal software modules.

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

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

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

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

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

DMS : Shows DMS VLAN membership status.

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

RMirror : show VLAN membership entries configured by the Mirroring internal software module.

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

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

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

Port VLAN ID : Shows the Port VLAN ID (PVID) that a given user wants the port to have. The field is empty if not overridden by the selected user.

Tx Tag : Shows egress filtering frame status whether tagged or untagged.

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

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

Buttons

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

Refresh : Click to manually refresh the page immediately.

User select dropdown : At the dropdown choose the VLAN User to be displayed.

MAC-based VLAN

Configuration

The MAC address to VLAN ID mappings can be configured here. This page lets you add and delete MAC-based VLAN Classification List entries and assign the entries to different ports.

Web Interface

To configure MAC address-based VLAN parameters in the web UI:

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

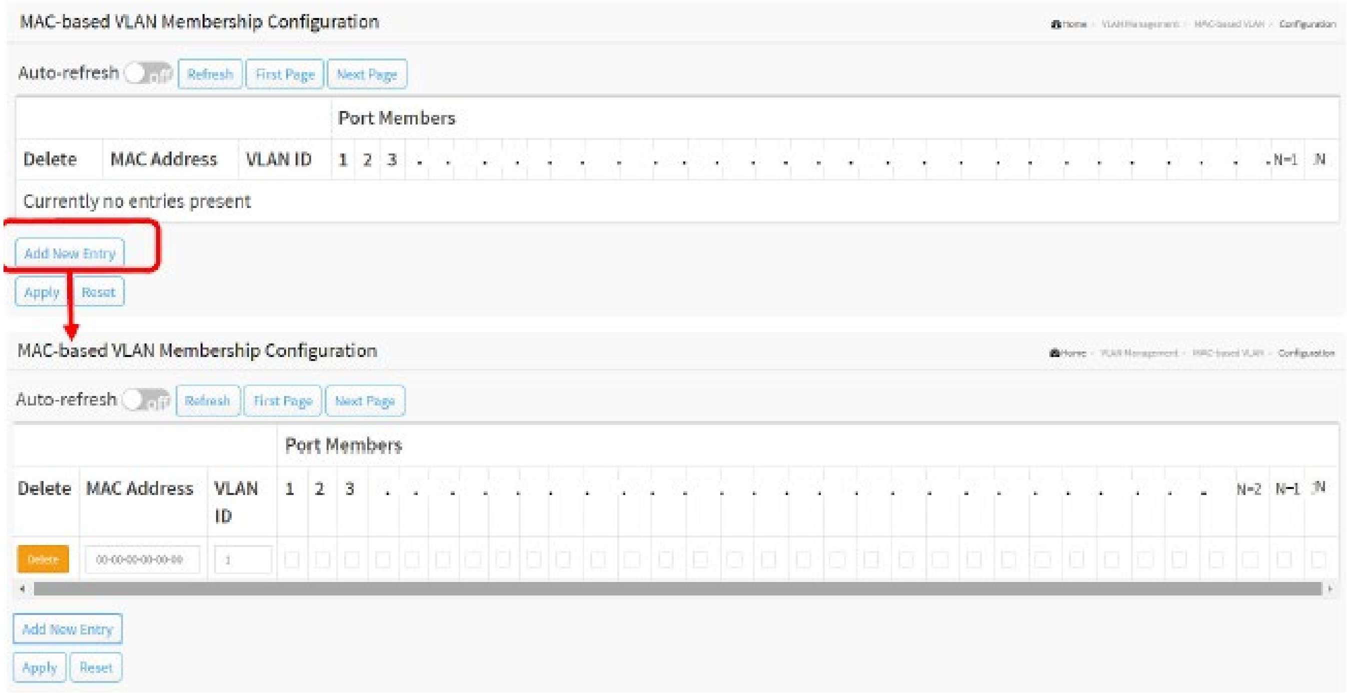


Figure 5-4.1: MAC-based VLAN Membership Configuration

Parameter descriptions:

MAC Address : Indicates the MAC address.

VLAN ID : Indicates the VLAN ID.

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

Buttons

Add 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. Valid VLAN ID values are 1 - 4095.

Apply : Click to save changes.

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

First Page : Click to display the initial page of entries.

Next Page : Click to display the next page of entries.

Delete : To delete a MAC-based VLAN entry, check this box and press Apply.

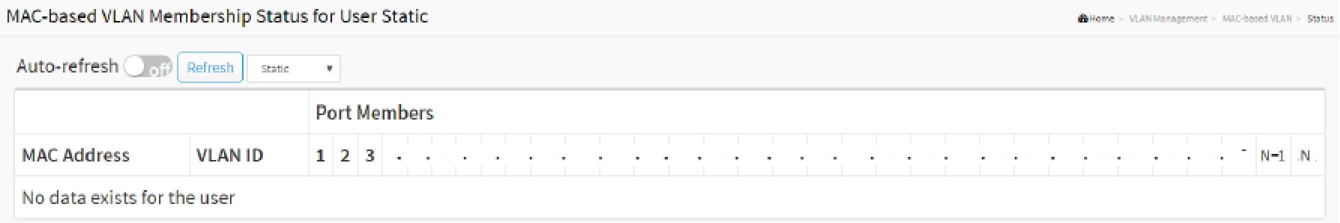
Auto-refresh : Check this box to refresh the page automatically every 3 seconds.

Refresh : Click to manually refresh the page immediately.

Status

This page shows the MAC-based VLAN membership status. To display MAC-based address VLAN configuration in the web UI:

1. Click VLAN Management, MAC-based VLAN and Status.
2. At the dropdown select the desired User (Static, NAS, DMS, or Combined).
3. To automatically refresh the information every 3 seconds, click “Auto-refresh”.
4. Click “Refresh” to manually refresh the webpage immediately.



MAC-based VLAN Membership Status for User Static

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

Figure 5-4.2: MAC-based VLAN Membership Status

Parameter descriptions:

MAC Address : Indicates the MAC address.

VLAN ID : Indicates the VLAN ID.

Port Members : Port members of the MAC-based VLAN entry.

Buttons

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

Refresh : Click to manually refresh the page immediately.

User select dropdown : At the dropdown select the desired User:

> ***Static*** : Refers to CLI/Web/SNMP as static.
>
> ***NAS***: Provides port-based authentication, involving communication between a Supplicant, Authenticator, and an Authentication Server.
>
> ***DMS*** : Shows the set of current Device Management System user’s data.
>
> ***Combined*** : show a combination of all of the User types.

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.

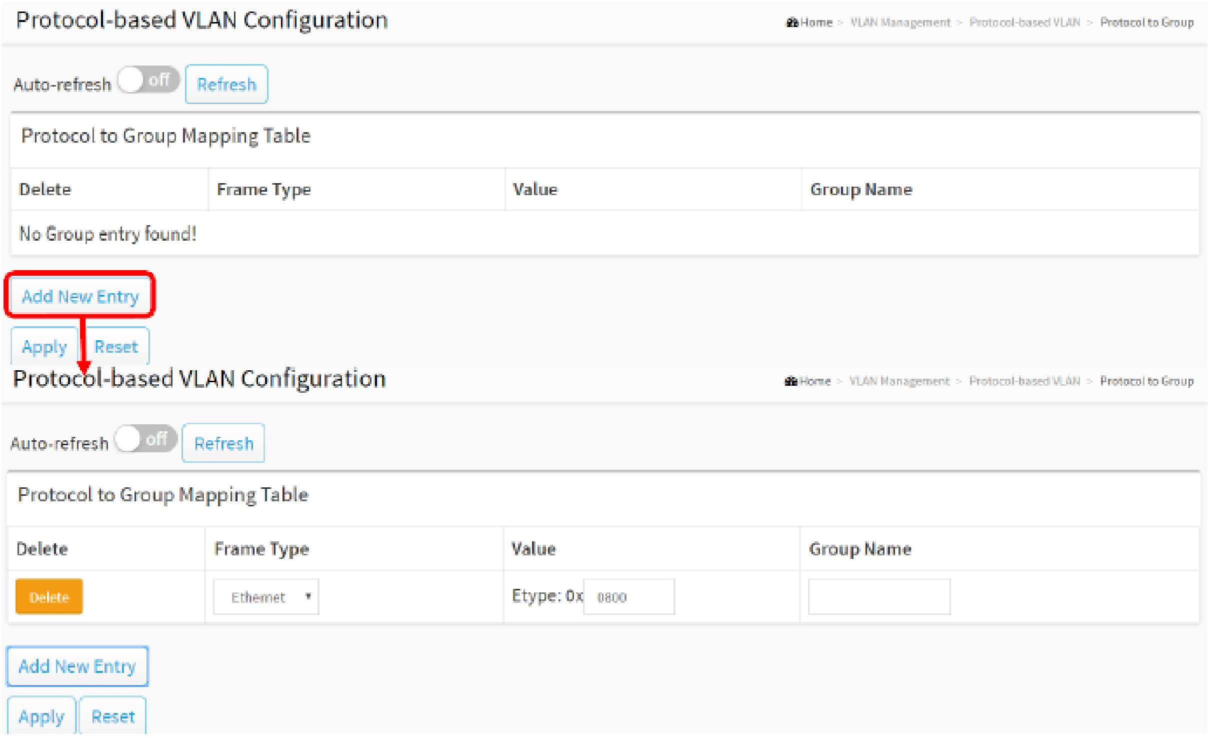
Protocol to Group

This page lets you add new protocols to a Group Name (unique for each Group) mapping entries and lets you view and delete already mapped entries for the switch.

Web Interface

To configure Protocol -based VLAN parameters in the web UI:

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



Protocol-based VLAN Configuration

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

Auto-refresh off Refresh

Protocol to Group Mapping Table

Delete	Frame Type	Value	Group Name
No Group entry found!			

Add New Entry

Apply Reset

Protocol-based VLAN Configuration

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

Auto-refresh off Refresh

Protocol to Group Mapping Table

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

Add New Entry

Apply Reset

Figure 5-5.1: Protocol to Group Mapping Table

Parameter descriptions :

Frame Type : At the dropdown select one of these values:

1. Ethernet
2. LLC
3. SNAP

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

Value : Valid value that can be entered in this text field depends on the option selected from the preceding Frame Type selection menu. The criteria for three different Frame Types:

> ***Ethernet***: Values in the text field when Ethernet is selected as a Frame Type is called etype. Valid values for etype range from 0x0600 - 0xffff.
>
> ***LLC***: Valid value in this case is comprised of two different sub-values. a. DSAP: 1-byte long string (0x00-0xff) b. SSAP: 1-byte long string (0x00 - 0xff).
>
> ***SNAP***: Valid value is also comprised of two different sub-values. ***a.*** OUI: OUI (Organizationally Unique Identifier) is value in format of xx-xx-xx where each pair (xx) in string is a hexadecimal value ranges from 0x00-0xff. ***b.*** PID: If the OUI is hexadecimal 000000, the protocol ID is the Ethernet type (EtherType) field value for the protocol running on top of SNAP; if the OUI is an OUI for a particular organization, the protocol ID is a value assigned by that organization to the protocol running on top of SNAP.

Group Name : A valid Group Name is a unique 16-character 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 operation.

Add New Entry : Click to add a new entry in mapping table. An empty row is added to the table; Frame Type, Value and the Group Name can be configured as needed. The Reset button can be used to undo the addition of new entry.

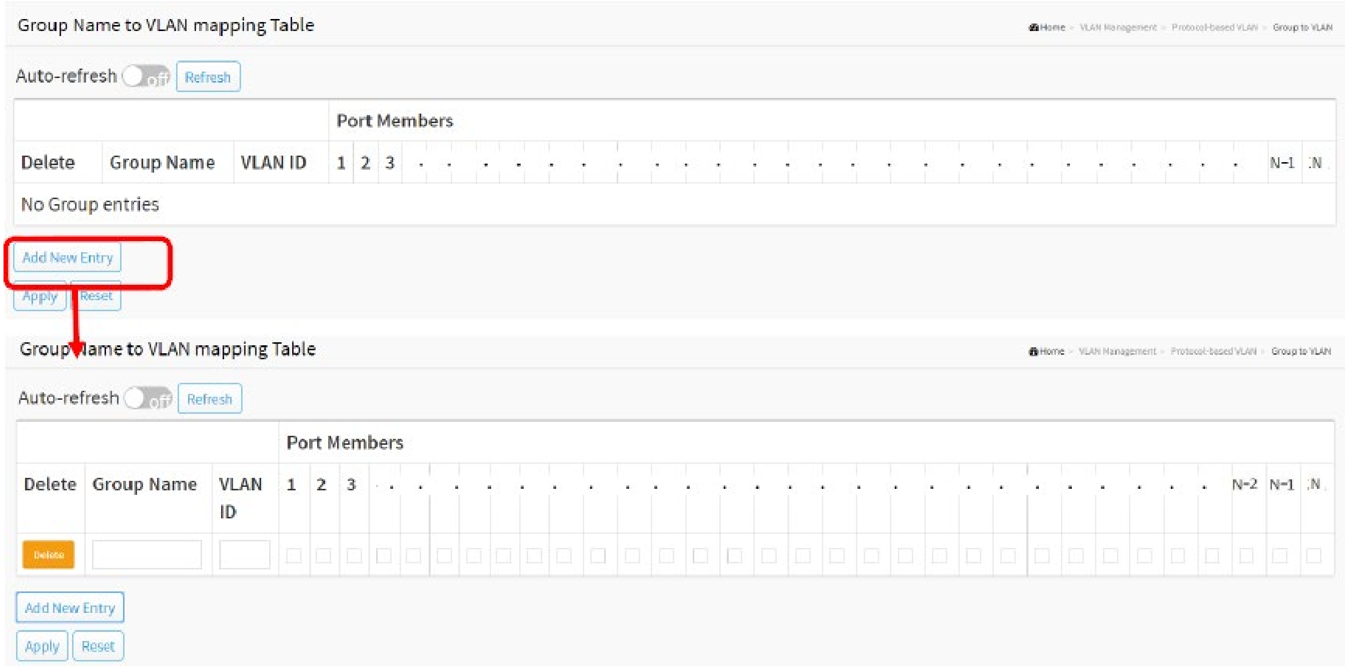
Apply : Click to save changes.

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

Group to VLAN

This page lets you map an already configured Group Name to a VLAN for the switch. To configure Group Name to VLAN mapping in the web UI:

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



Group Name to VLAN mapping Table

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

Auto-refresh off Refresh

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

Add New Entry

Apply Reset

Group Name to VLAN mapping Table

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

Auto-refresh off Refresh

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

Add New Entry

Apply Reset

Figure 5-5.2: Group Name to VLAN mapping Table

Parameter descriptions:

Group Name : A valid Group Name is a string of up to 16 characters.

VLAN ID : Indicates the VID to which Group Name will be mapped. A valid VLAN ID is 1-4095.

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

Buttons

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

Refresh : Click to manually refresh the page immediately.

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

Apply : Click to save changes.

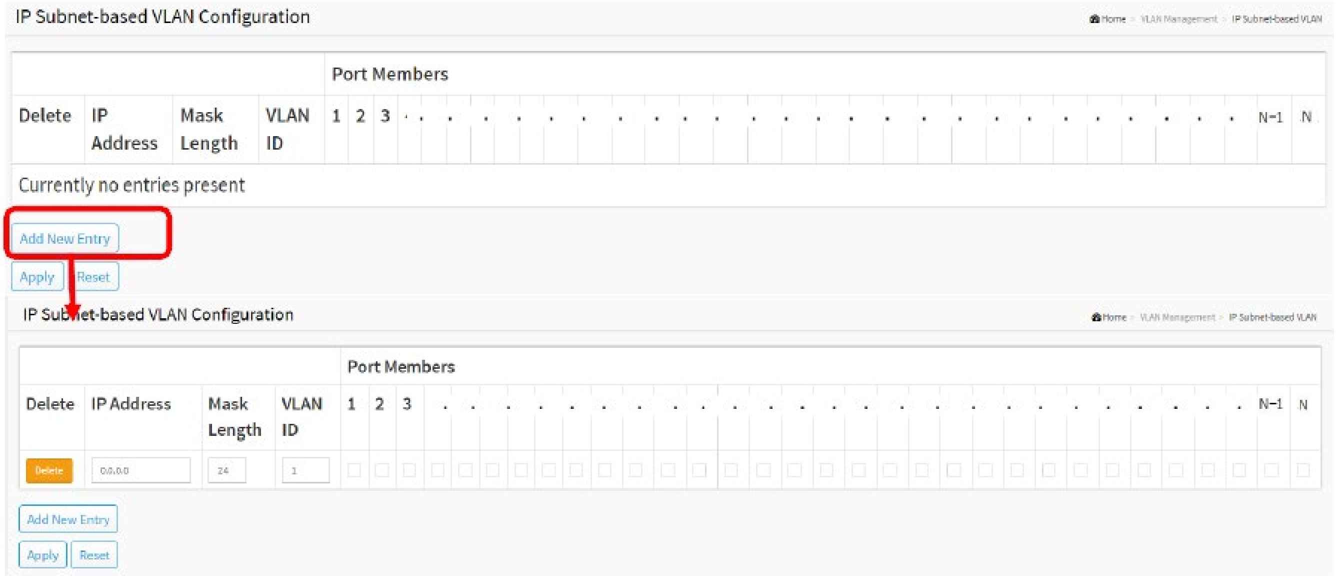
Reset : Click to undo any changes made locally and revert to previously saved values.

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.

IP Subnet-based VLAN

This page lets you add, update and delete IP subnet-based VLAN entries. To configure IP subnet-based VLAN Membership in the web UI:

1. Click VLAN Management and IP Subnet-based VLAN.
2. Click “Add New Entry”.
3. Specify IP Address, Mask Length, and VLAN ID.
4. Check the desired Port Members checkboxes.
5. Click Apply.



IP Subnet-based VLAN Configuration

Home > VLAN Management > IP Subnet-based VLAN

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

Add New Entry
Apply
Reset

IP Subnet-based VLAN Configuration

Home > VLAN Management > IP Subnet-based VLAN

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

Add New Entry
Apply
Reset

Figure 5-6: IP Subnet-based VLAN Configuration

Parameter descriptions:

IP Address : Enter the IP address.

Mask Length : Enter the network mask length.

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

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

Buttons

Delete : To delete a IP subnet-based VLAN entry, check this box and click Apply.

Add New Entry : Click 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 - 4095. The “Delete” button can be used to undo the addition of new IP subnet-based VLANs. The maximum possible IP subnet-based VLAN entries is limited to 128.

Apply : Click to save changes.

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

Stream

This page lets you configure 1-10 Stream instances. A Stream is described as the path through the network from “Talker” to “Listener.”

Navigate to the VLAN Management > Stream > Stream menu path. Click the Add New Stream (⊕) button and enter the desired parameters. Click Apply when done.

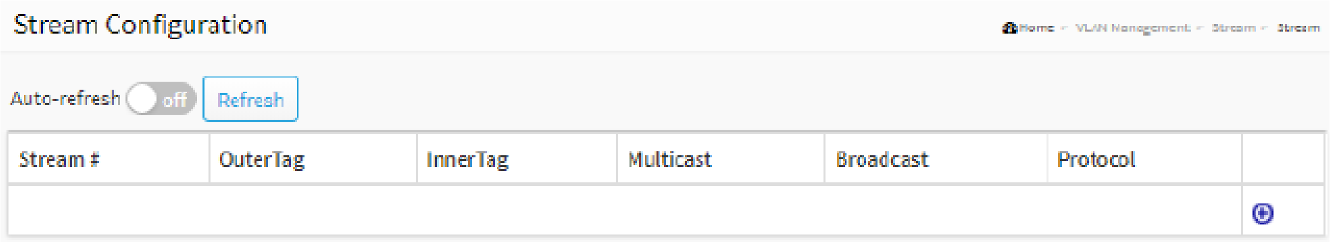
Stream Reservation Protocol (SRP) is an enhancement to Ethernet that implements admission control. In September 2010 SRP was standardized as IEEE 802.1Qat which has subsequently been incorporated into IEEE 802.1Q-2011. SRP defines the concept of streams at layer 2 of the OSI model. Also provided is a mechanism for end-to-end management of the streams' resources, to guarantee quality of service (QoS). SRP is part of the IEEE Audio Video Bridging (AVB) and Time-Sensitive Networking (TSN) standards.

SRP registers a stream and reserves the resources required through the entire path taken by the stream, based on the bandwidth requirement and the latency which are defined by a stream reservation traffic class. Listener (stream destination) and Talker (stream source) primitives are utilized. Listeners indicate what streams are to be received; Talkers announce the streams that can be supplied by a bridged entity. Network resources are allocated and configured in both end nodes of the data stream and the transit nodes along the data streams' path. An end-to-end signaling mechanism to detect the success/failure of the effort is also provided.

An SRP "talker advertise" message includes QoS requirements (e.g., VLAN ID and Priority Code Point (PCP)) to define traffic class, rank (emergency or nonemergency), traffic specification (maximum frame size and maximum number of frames in a traffic class), measurement interval, and accumulated worst case latency). Talker advertise and listener ready messages can be de-registered, which terminates the stream. Periodic polling of advertise and ready messages is used to detect unresponsive devices.

SRP works using the Multiple MAC Registration Protocol (MMRP), the Multiple VLAN Registration Protocol (MVRP), and the Multiple Stream Registration Protocol (MSRP). MMRP controls propagation of group registration, and MVRP controls VLAN membership (MAC address information). MSRP works in a distributed network of bridges and end stations; it registers and advertises data streams and reserves bridge resources to provide the QoS guarantees.

A station (talker) sends a reservation request with the general MRP application. All participants in the stream have an MSRP application and the MRP Attribute Declaration (MAD) specification for describing the stream characteristics. Then each bridge within the same SRP domain can map, allocate, and forward the stream with the necessary resources by using the MRP attribute propagation.



Stream Configuration

Stream #	OuterTag	InnerTag	Multicast	Broadcast	Protocol	
						⊕

Figure 4-7.1: Stream Configuration

Parameter descriptions :

Stream # : The ID of the Stream. Valid values are 1 - 10.

OuterTag : The outer tag in the SRP streaming data frames to be propagated from Talker to Listener.

InnerTag : The Inner tag in the SRP streaming data frames to be propagated from Talker to Listener.

Multicast : The Talker destination address (a multicast or locally administered address).

Broadcast : The configured stream broadcast address.

Protocol : The configured stream protocol used (MMRP, MVRP, or MSRP).

Configuration Buttons

You can modify each Stream in the table using these buttons:

ⓔ : Edit the Stream row in the table.

⊗ : Delete the Stream from the table.

⊕ : Add a new Stream row to the table.

Buttons

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

Refresh: Click to manually refresh the page immediately.

Notes:

1. MRP EtherType values: MMRP EtherType = 88-F6, MVRP EtherType = 88-F5, MSRP EtherType = 22-EA (required for interoperability between MRP Participants).

2. SRP supports emergency and non-emergency traffic. Emergency traffic will interrupt non-emergency traffic if there is insufficient bandwidth or resources available for the emergency traffic. Emergency traffic (Rank 0) includes North America 911 emergency services telephone calls, fire safety announcements, etc.

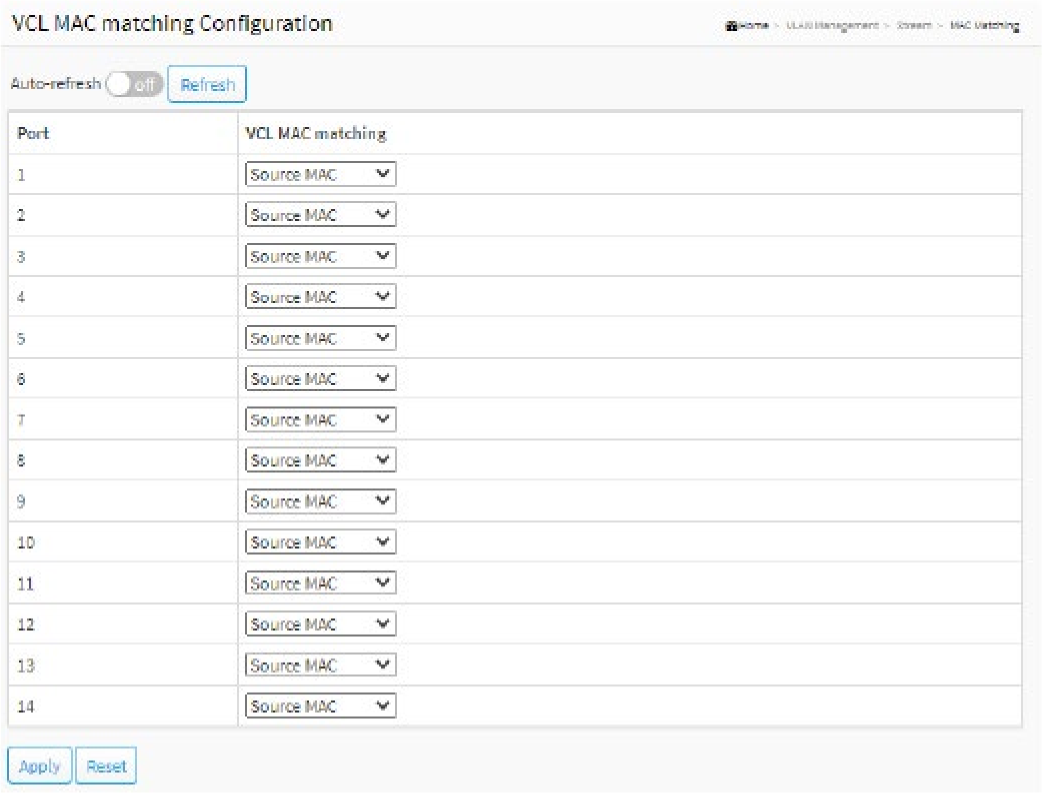
See also:

https://mentor.ieee.org/802.11/dcn/10/11-10-0511-00-00aa-802-1qat-draft-6-0.pdf

https://1.ieee802.org/tsn/802-1qcc/

VCL MAC Matching

This page lets you set VCL (VLAN Control List) MAC matching parameters. You can configure MAC/IP matching for each port. Each port can be configured to use either (source MAC/source IP address) or (destination MAC/destination IP address). A stream can be defined as all traffic that matches a certain key which may contain either destination MAC, source MAC, destination IP address, or source IP address. The matching will not use all fields in the key.



VCL MAC matching Configuration

Home > VLAN Management > Stream > MAC Matching

Auto-refresh ○ off

Refresh

Port	VCL MAC matching
1	Source MAC
2	Source MAC
3	Source MAC
4	Source MAC
5	Source MAC
6	Source MAC
7	Source MAC
8	Source MAC
9	Source MAC
10	Source MAC
11	Source MAC
12	Source MAC
13	Source MAC
14	Source MAC

Apply Reset

Figure 4-7.2: VCL MAC matching Configuration

Parameter descriptions :

Port : Port number of the switch.

VCL MAC Matching : Select the VCL (VLAN Control List) MAC matching. Possible values are:

Source MAC: Use source MAC/source IP address for matching (the default setting).

Destination MAC : Use Destination MAC/Destination IP address for matching.

Buttons

Apply : Click to save changes.

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

MRP

MRP (IEEE Std. 802.1ak-2007 Multiple Registration Protocol) is a robust, efficient protocol for declaring attributes to be registered in a database in each port of each bridge (optionally, station) in a bridged network. MRP replaces GARP (Generic Attribute Registration Protocol (GARP).

Currently, four applications are based on MRP: MVRP, MMRP, MSRP and MIRP.

MVRP (Clause 11): Attribute is a VLAN ID. MVRP replaces GVRP

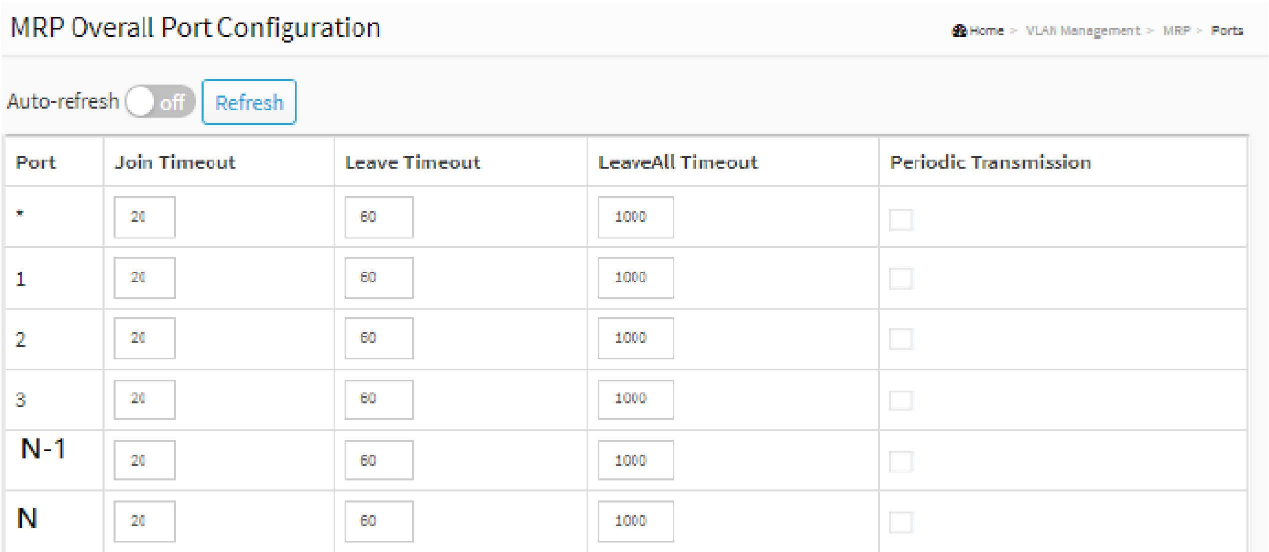
- Stations or configured Bridge Ports make (withdraw) declarations if they do (not) need to receive frames for a given VLAN ID.
- If a VLAN ID is registered on a Bridge Port by MVRP, the Bridge knows that that frames for that VLAN ID should be transmitted on that Bridge Port.

MMRP (Clause 10.9): Attribute is a MAC address, often a multicast address. Replaces GMRP.

- Stations or configured Bridge Ports make (withdraw) declarations if they do (not) need to receive frames for a given address. If an address is registered on a Bridge Port by MMRP, the Bridge knows that that frames for that address should be transmitted on that Bridge Port.

Ports

The MRP Overall Port Configuration page lets you configure MRP overall settings for all switch ports.


MRP Overall Port Configuration
Home > VLAN Management > MRP > Ports
Auto-refresh off
Refresh

Port	Join Timeout	Leave Timeout	LeaveAll Timeout	Periodic Transmission
*	20	60	1000	□
1	20	60	1000	□
2	20	60	1000	□
3	20	60	1000	□
N-1	20	60	1000	□
N	20	60	1000	□

Figure 4-8.1: MRP Overall Port Configuration

Parameter descriptions:

Port : The port number for which the following configuration applies.

Join Timeout : Controls the timeout of the Join Timer for all MRP applications on this switch port. Valid values are 1-20 centiseconds.

Leave Timeout : Controls the timeout of the Leave Timer for all MRP applications on this switch port. Valid values are 60-300 centiseconds.

LeaveAll Timeout : Controls the timeout of the Leave All Timer for all MRP applications on this switch port. Valid values are 1000- 5000 centiseconds.

Periodic Transmission : Enable or disable the Periodic Transmission feature for all MRP applications on this switch port.

Buttons

Apply: Click to save changes.

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

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

Refresh: Click to manually refresh the page immediately.

MRP Timers

MRP uses the following timers to control message transmission:

Join timer : The Join timer controls the transmission of Join messages. An MRP participant starts the Join timer after sending a Join message to the peer participant. Before the Join timer expires, the participant does not resend the Join message when these conditions exist:

- The participant receives a JoinIn message from the peer participant.
- The received JoinIn message has the same attributes as the sent Join message.

When both the Join timer and the Periodic timer expire, the participant resends the Join message.

Leave timer : The Leave timer controls the deregistration of attributes. An MRP participant starts the Leave timer in one of these conditions:

- The participant receives a Leave message from its peer participant.
- The participant receives or sends a LeaveAll message.

The MRP participant does not deregister the attributes in the Leave or LeaveAll message if the following conditions exist:

- The participant receives a Join message before the Leave timer expires.
- The Join message includes the attributes that have been encapsulated in the Leave or LeaveAll message.

If the participant does not receive a Join message for these attributes before the Leave timer expires, MRP deregisters the attributes.

LeaveAll timer : After startup, an MRP participant starts its own LeaveAll timer. When the LeaveAll timer expires, the MRP participant sends out a LeaveAll message and restarts the LeaveAll timer. Upon receiving the LeaveAll message, other participants restart their LeaveAll timer. The value of the LeaveAll timer is randomly selected between the LeaveAll timer and 1.5 times the LeaveAll timer. This mechanism provides these benefits:

- Effectively reduces the number of LeaveAll messages in the network.
- Prevents the LeaveAll timer of a particular participant from always expiring first.

Periodic timer : The Periodic timer controls the transmission of MRP messages. An MRP participant starts its own Periodic timer upon startup, and stores MRP messages to be sent before the Periodic timer expires. When the Periodic timer expires, MRP sends stored MRP messages in as few MRP frames as possible and restarts the Periodic timer. This mechanism reduces the number of MRP frames sent. You can enable or disable the Periodic timer. When the Periodic timer is disabled, MRP does not periodically send MRP messages. Instead, an MRP participant sends MRP messages when the LeaveAll timer expires, or the participant receives a LeaveAll message from the peer participant.

MMRP Attribute Types

MMRP Defines two attribute types:

- Service Requirement Vector Attribute Type (1)
- The MAC Vector Attribute Type (2)

Two types of service requirements are supported:

- All Groups must be encoded as the value 0. Forward all Multicast is used to support legacy devices that do not support MMRP/GMRP.
- All Unregistered Groups must be encoded as the value 1. Flood unregistered multicast traffic and other traffic is pruned by MMRP.
- The remaining possible values (2 - 255) are reserved.

Bridge group filtering behavior for Forward All Groups and Forward Unregistered groups is specified in Clause 8.8.6 of the IEEE 802.1Q-Rev.

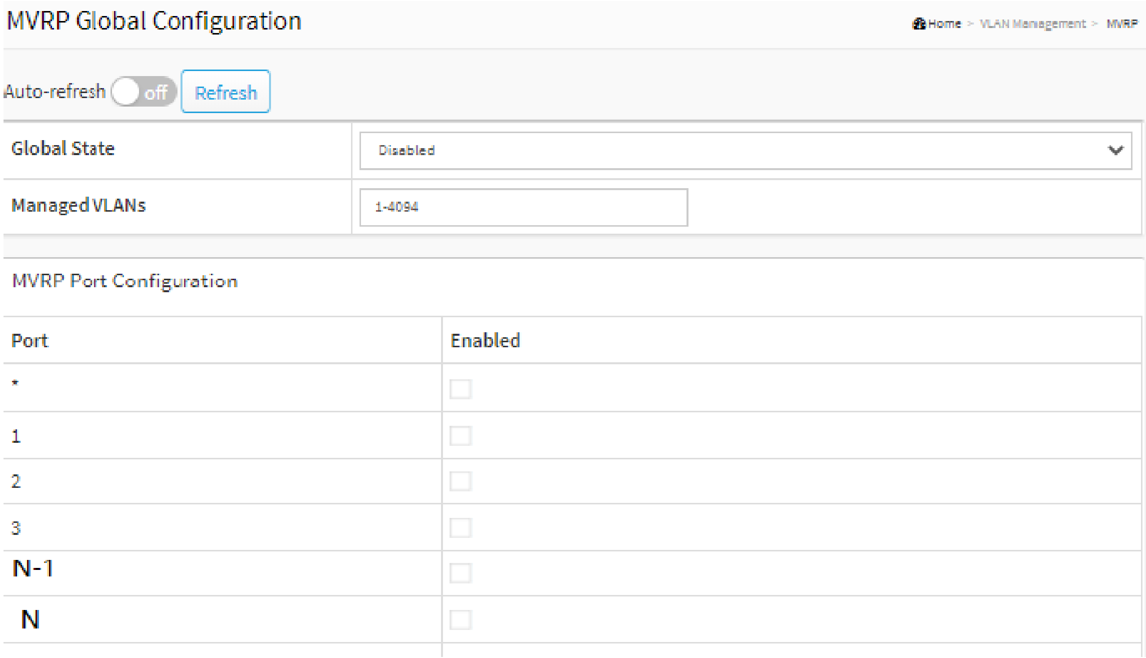
MVRP

This page lets you configure all MVRP global and per-port settings. This page includes a global section and a per-port configuration section.

Multiple VLAN Registration Protocol defines the dynamic registration and de-registration of VLAN identifiers across a Bridged Local Area Network. It uses the MRP framework to define its operation and therefore it is also called an MRP application. The standard was originally defined by IEEE 802.1ak, and its latest incorporation is in IEEE 802.1Q-2014. An MVRP-enabled port is called an MVRP participant.

Multiple VLAN Registration Protocol (MVRP) is a Multiple Registration Protocol (MRP) application that helps create VLANs dynamically (VLAN registration) and automate administrating VLAN membership (distribution and deregistration) within the network without manual intervention.

MVRP provides IEEE 802.1ak-compliant dynamic VLAN creation and VLAN pruning on switch ports connecting core and access switches. An MVRP-aware switch can exchange VLAN configuration information with other MVRP-aware switches, prune unnecessary broadcast and unknown unicast traffic, and dynamically create and manage VLANs on switches. MVRP supports propagating VLAN information from one device to another.



MVRP Global Configuration

Global State	Disabled
Managed VLANs	1-4094

MVRP Port Configuration

Port	Enabled
*	□
1	□
2	□
3	□
N-1	□
N	□

Figure 4-8.1: MVRP Global Configuration

Parameter descriptions :

MVRP Global Configuration

Global State : Enable or disable the MVRP protocol globally. This will enable or disable the protocol globally and at the same time on switch ports that are MVRP enabled.

Managed VLANs : This field shows the managed VLANs (i.e., the VLANs that MVRP will operate on). By default, only VLANs 1- 4094 are managed (i.e., the entire range as defined in IEEE802.1Q-2014 for MVRP). However, this range can be limited by using a list syntax where the individual elements are separated by commas.

A Range is specified with a dash separating the lower and upper bound. The following example will enable VLANs 1, 10, 11, 12, 13, 200, and 300: 1,10-13,200,300. Spaces are allowed in between the delimiters.

MVRP Port Configuration

Port : The port number for which the following configuration applies.

Enabled : Enable or disable the MVRP protocol on this switch port. This will enable or disable the protocol on the switch port given that MVRP is also globally enabled.

Buttons

Apply: Click to save changes.

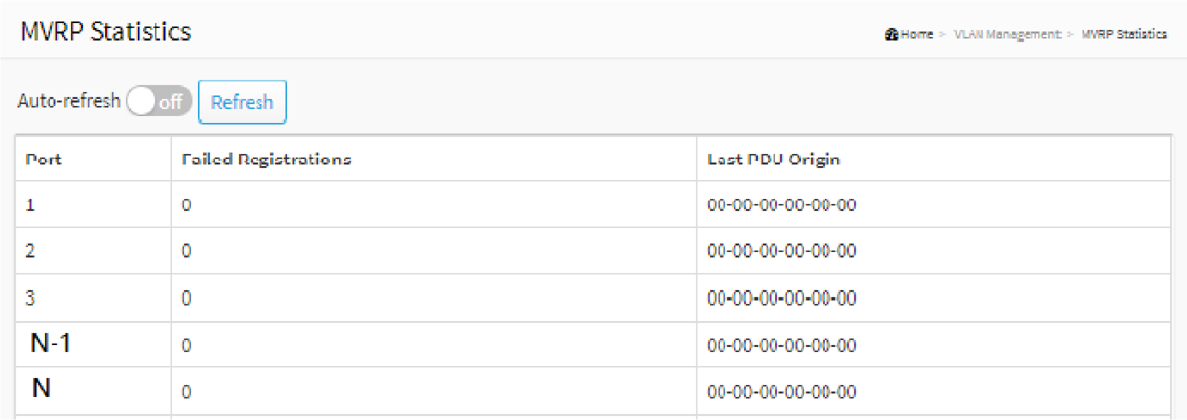
Reset: Click to undo any changes made locally and revert to previously saved values.

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

Refresh: Click to refresh the page.

MVRP Statistics

This page displays MVRP protocol statistics for all switch ports.



Port	Failed Registrations	Last PDU Origin
1	0	00-00-00-00-00-00
2	0	00-00-00-00-00-00
3	0	00-00-00-00-00-00
N-1	0	00-00-00-00-00-00
N	0	00-00-00-00-00-00

Figure 4-8.3: MVRP Statistics

Parameter descriptions :

Port : The logical port for the statistics contained in the same row.

Failed Registrations : The number of failed VLAN registrations on this switch port. Each port implementing the MVRP protocol maintains a count of the number of times it has received a VLAN registration request but has failed to register the VLAN due to lack of space in the Filtering Database.

Last PDU Origin : The MAC address of the most recent MVRP PDU received on this switch port.
The MAC is 00-00-00-00-00-00 if the protocol is not enabled on that switch port, or if the port has not received any MVRP PDUs yet.

Buttons

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

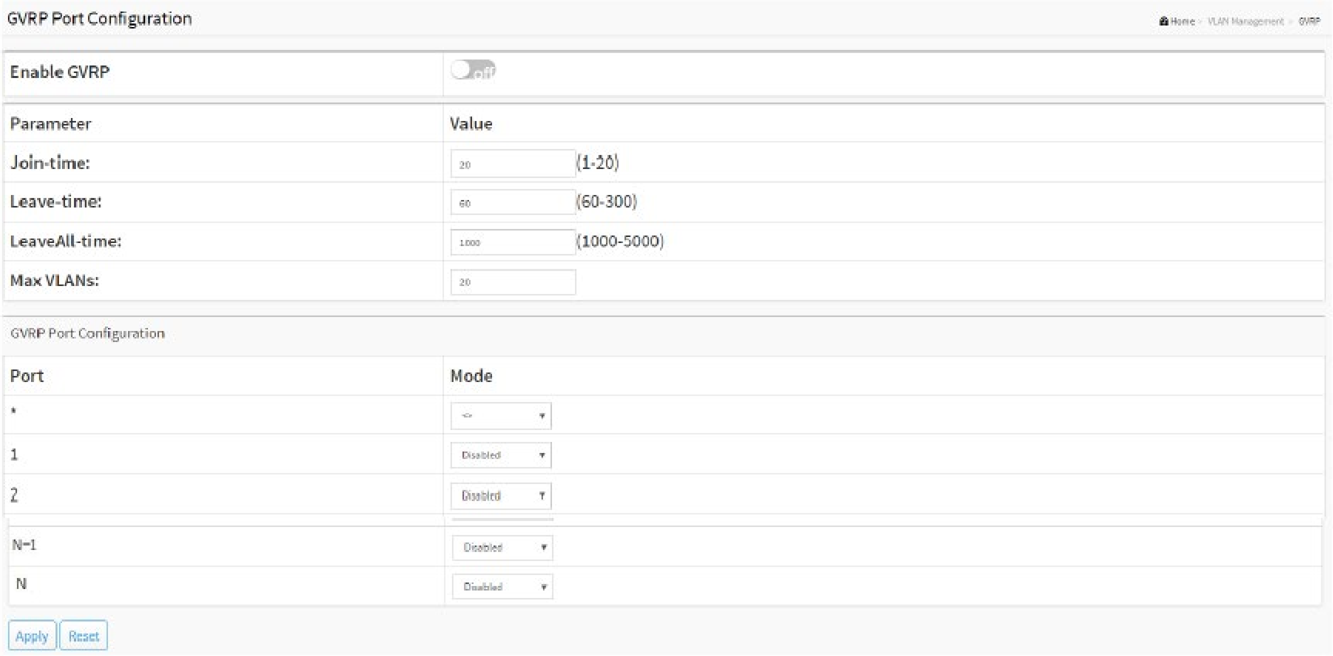
Refresh: Click to refresh the page.

GVRP

GVRP (GARP VLAN Registration Protocol or Generic VLAN Registration Protocol) is a standards-based protocol that facilitates control of virtual local area networks (VLANs) within a larger network. GVRP conforms to the IEEE 802.1Q specification, which defines a method of tagging frames with VLAN configuration data over network trunk interconnects. This enables network devices to dynamically exchange VLAN configuration information with other devices.

To configure GVRP in the web UI:

1. Click VLAN Management and GVRP.
2. Enable or disable GVRP.
3. Specify Join-time, Leave-time, Leave All-time, and Max VLANs.
4. Enable or disable the Mode for each port as desired.
5. Click Apply to save the settings.
6. To cancel the settings, click the Reset button to revert to previously saved values.



GVRP Port Configuration

Home > VLAN Management > GVRP

Enable GVRP	off

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

GVRP Port Configuration

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

Figure 4-9: GVRP Port Configuration

Parameter descriptions :

Enable GVRP: The GVRP feature is enabled globally by checking the Enable GVRP checkbox to on.

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

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

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

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

GVRP Port Configuration:

Port : The Port column shows the list of ports.

Mode : Enable/disable GVRP Mode on particular port locally:

Disabled: Select to Disable GVRP mode on this port (default).

Enabled: Select to Enable GVRP mode on this port.

Buttons

Apply : Click to save changes.

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

Private VLAN

This page lets you add or delete Private VLANs, view and set Private VLAN membership parameters, and add or delete Port members of each Private VLAN.

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

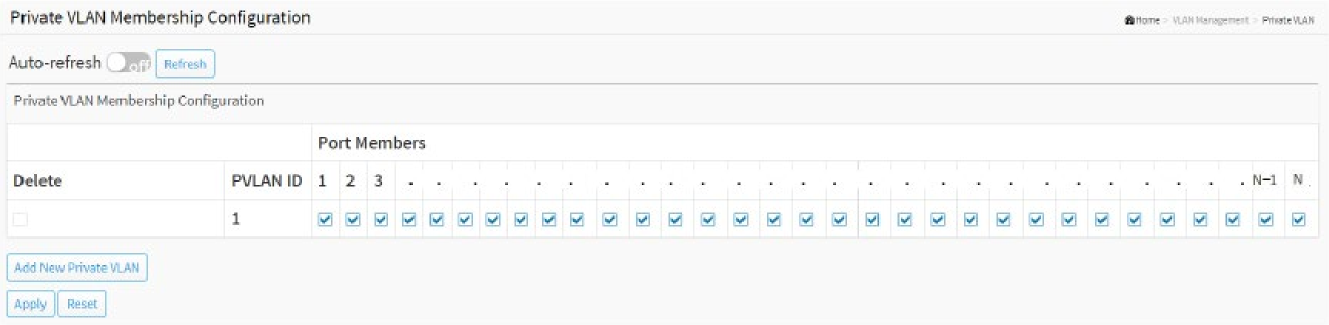
A port must be a member of both a VLAN and a Private VLAN to be able to forward packets. By default, all ports are VLAN unaware and members of VLAN 1 and Private VLAN 1.

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

Web Interface

To configure Private VLAN Membership in the web UI:

1. Click VLAN Management and Private VLAN.
2. Click the Add New Private VLAN button to add a new private VLAN ID to the table.
3. Configure the Private VLAN membership settings.
4. Click Apply.



Private VLAN Membership Configuration

Private VLAN Membership Configuration

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

Figure4-10: Private VLAN Membership Configuration

Parameter descriptions :

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

PVLAN 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.

Buttons

Add New Private VLAN : Click to add a new private VLAN ID. An empty row is added to the table, and the private VLAN can be configured as needed. The valid 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 Reset button can be used to undo the addition of new Private VLANs.

Apply : Click to save changes.

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

Port Isolation

This page is used to enable or disable 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.

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

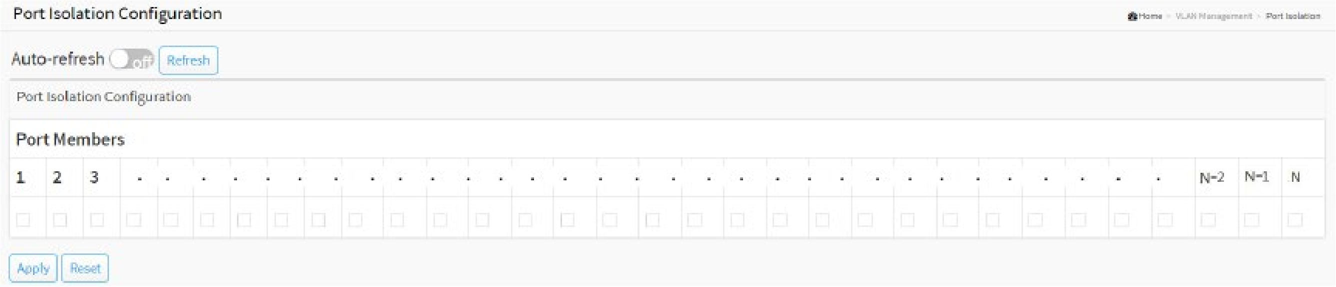
Web Interface

To configure Port Isolation in the web UI:

1. Click VLAN Management and Port Isolation.

2. Evoke which port(s) on which you want Port Isolation.

3. Click Apply.



Port Isolation Configuration

Port Isolation Configuration

Port Members

1 2 3 . . . N-2 N-1 N

□ □

Figure 4-11: Port Isolation Configuration

Parameter descriptions :

Port Members : A check box is provided for each port of a private VLAN. When checked, port isolation is enabled on that port. When unchecked, port isolation is disabled on that port. By default, port isolation is disabled on all ports.

Buttons

Apply : Click to save changes.

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

Voice VLAN

A 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.

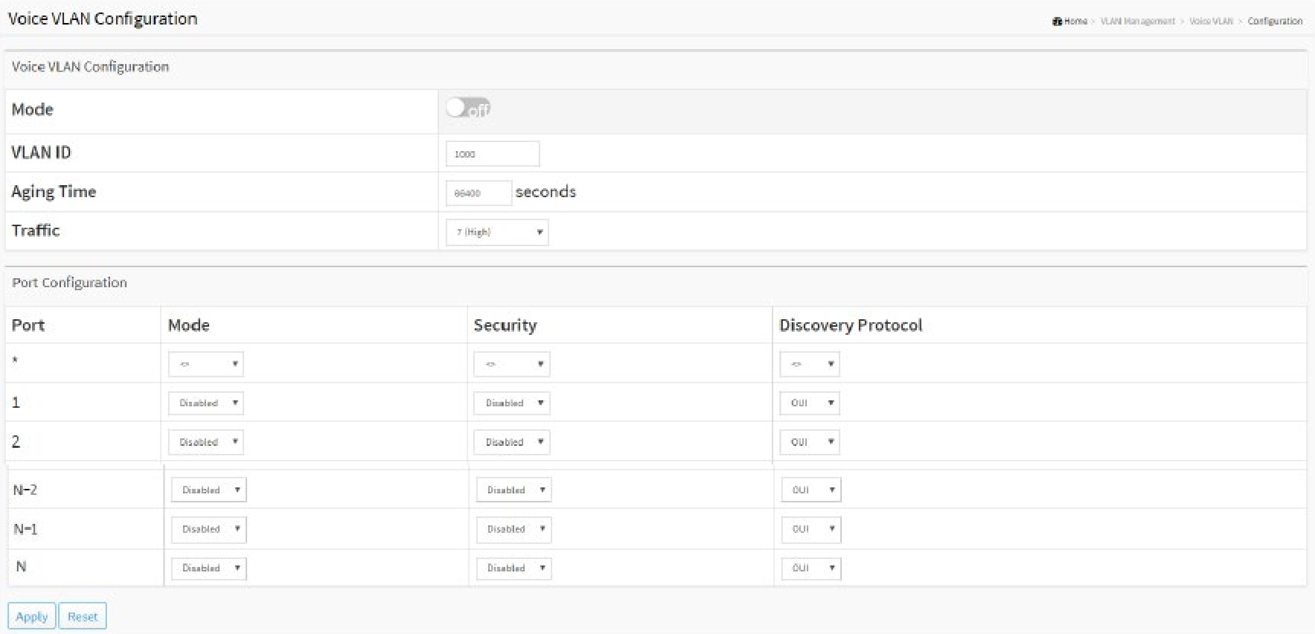
Configuration

The Voice VLAN feature enables voice traffic forwarding on the Voice VLAN, then the switch can classify and schedule network traffic. It is recommended that there be two VLANs on a port - one for voice, one for data. Before connecting the IP device to the switch, the IP phone should configure the voice VLAN ID correctly. It should be configured through its own GUI.

Web Interface

To configure Voice VLAN in the web UI:

1. Click VLAN Management, Voice VLAN, and Configuration.
2. Set Mode to "on" in the Voice VLAN Configuration section.
3. Specify VLAN ID, Aging Time and Traffic Class.
4. Select Port Members in the Voice VLAN Configuration section.
5. Specify (Mode, Security, Discovery Protocol) in the Port Configuration section.
6. Click the Apply button to save the settings.
7. To cancel the settings, click the Reset button to revert to previously saved values.



Voice VLAN Configuration

Voice VLAN Configuration

Mode	off
VLAN ID	1000
Aging Time	86400 seconds
Traffic	7 (High)

Port Configuration

Port	Mode	Security	Discovery Protocol
*	<>	<>	<>
1	Disabled	Disabled	OUI
2	Disabled	Disabled	OUI
N-2	Disabled	Disabled	OUI
N-1	Disabled	Disabled	OUI
N	Disabled	Disabled	OUI

Figure 5-10.1: Voice VLAN Configuration

Parameter descriptions :

Mode : Indicates the Voice VLAN mode operation. You must disable the MSTP feature before you can enable Voice VLAN in order to avoid the conflict of ingress filtering. Possible modes are:

> ***on*** : Enable Voice VLAN mode operation.
>
> ***off*** : Disable Voice VLAN mode operation (default).

VLAN ID : Enter 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 valid range is 1 to 4095.

Aging Time : Select the Voice VLAN secure learning aging time. The valid 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 : Select the Voice VLAN traffic class. All traffic on the Voice VLAN will apply this class. At the dropdown select a value of 7 (High priority) to 0 (Low priority).

Port : The switch port number of the Voice VLAN port.

Port Mode : Select the Voice VLAN port mode. Possible port modes are:

Disabled : Disjoin from Voice VLAN (default).

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

Forced : Force join to Voice VLAN.

This field will be read only if the STP feature is enabled. The STP Port mode will be read only if this field be set to a mode other than Disabled.

Port Security : Select 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 (default).

~~Port~~ Discovery Protocol : Select the Voice VLAN port discovery protocol. It will only work when Auto detect mode is enabled. **Note**: you must enable the LLDP feature before configuring discovery protocol to "LLDP" or "Both". Changing the discovery protocol to "OUI" or "LLDP" will restart the Auto detect process. Possible discovery protocols are:

OUI: Detect telephony device by OUI address.

LLDP: Detect telephony device by LLDP.

Both: Detect telephony device by both OUI and LLDP.

Buttons

Apply : Click to save changes.

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

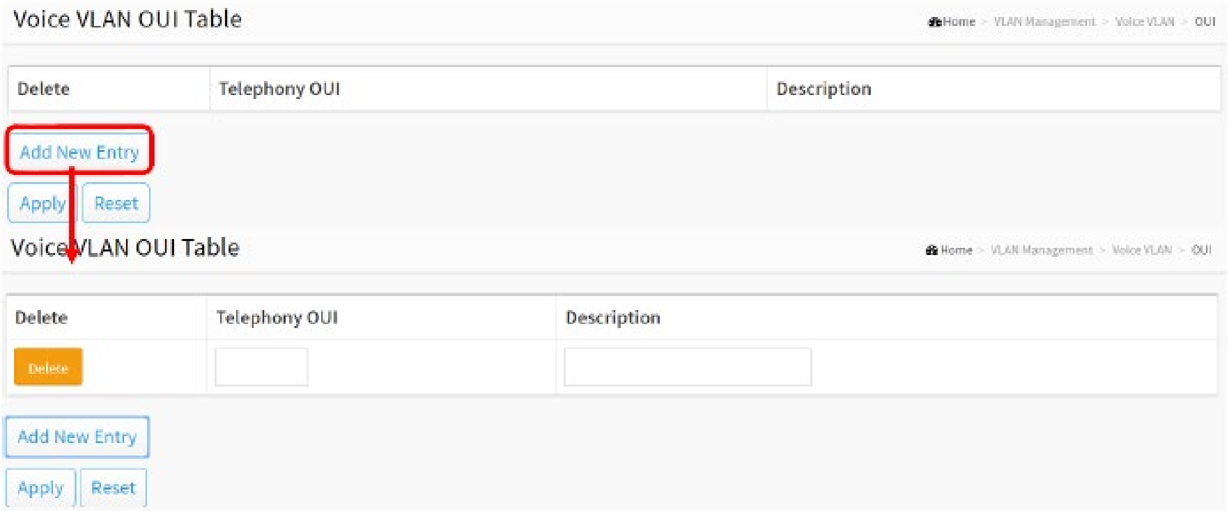
Voice VLAN OUI

Here you can configure Voice VLAN Organization Unique Indicator (OUI) parameters. The maximum number of entries is 16. Modifying the OUI table will restart the Auto detection of OUI process.

Web Interface

To configure Voice VLAN OUI in the web UI:

1. Click VLAN Management, Voice VLAN, and OUI.
2. Click the Add New Entry button.
3. Specify Telephony OUI and Description.
4. Click Apply.



Voice VLAN OUI Table

Home > VLAN Management > Voice VLAN > OUI

Delete	Telephony OUI	Description

Voice VLAN OUI Table

Home > VLAN Management > Voice VLAN > OUI

Delete	Telephony OUI	Description
Delete		

Figure 5-10.2: Voice VLAN OUI Table

Parameter descriptions :

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

Telephony OUI : A telephony OUI address is a global organizationally unique identifier assigned to a vendor by the IEEE. It must be 6 characters long and the input format is "xx-xx-xx" (where 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 characters.

Buttons

Add New Entry : Click to add a new entry in Voice VLAN OUI table. An empty row is added to the table, with the Telephony OUI and Description parameter fields.

Apply : Click to save changes.

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

6. Quality of Service

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

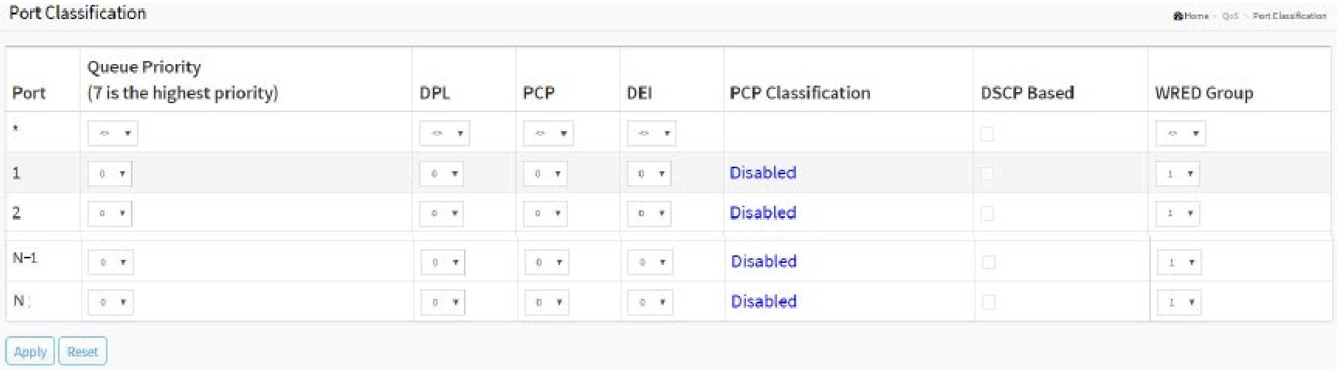
It provides high flexibility in the classification of incoming frames to a QoS class. The QoS classification looks for information up to Layer 4, including IPv4 and IPv6 DSCP, IPv4 TCP/UDP port numbers, and user priority of tagged frames. This QoS classification mechanism is implemented in a QoS control list (QCL). The QoS Class assigned to a frame is used throughout the device for providing queuing, scheduling, and congestion control guarantees to the frame according to what was configured for that specific QoS class.

The switch supports advanced memory control mechanisms providing excellent performance of all QoS classes under any traffic scenario, including jumbo frames. The switch provides superior priority queueing with dedicated memory and strict highest-priority arbitration. The ingress super priority queue allows traffic recognized as CPU traffic to be received and queued for transmission to the CPU even when all the QoS class queues are congested.

Port Classification

This page lets you configure basic QoS Ingress Classification settings for all switch ports. To configure QoS Ingress Port Classification in the web UI:

1. Click Quality of Service and Port Classification.
2. Scroll to select QoS Ingress Port parameters.
3. Click Apply to save the settings.
4. To cancel the settings click the Reset button. It will revert to previously saved values.
5. Click “PCP Classification“ to go to the next page “Port PCP Classification”.


Port Classification

Port	Queue Priority (7 is the highest priority)	DPL	PCP	DEI	PCP Classification	DSCP Based	WRED Group
*	<>	<>	<>	<>		□	<>
1	0	0	0	0	Disabled	□	1
2	0	0	0	0	Disabled	□	1
N-1	0	0	0	0	Disabled	□	1
N	0	0	0	0	Disabled	□	1

Figure 6-1: QoS Ingress Port Classification

Parameter descriptions :

Port : The port number for which the configuration below applies.

Queue Priority : Select the default CoS value. All frames are classified to a CoS. There is a one to one mapping between CoS, queue and priority. A CoS of 0 (zero) has the lowest priority. If the port is VLAN aware, the frame is tagged and Tag Class. is enabled, then the frame is classified to a CoS that is mapped from the PCP and DEI value in the tag. Otherwise the frame is classified to the default CoS.
The classified CoS can be overruled by a QCL entry. The valid range is 0 (default) to 7 (highest priority).

Note: If the default CoS has been dynamically changed, then the actual default CoS is shown in parentheses after the configured default CoS.

DPL : Controls the default Drop Precedence Level. All frames are classified to a drop precedence level. If the port is VLAN aware, the frame is tagged and Tag Class. is enabled, then the frame is classified to a DPL that is mapped from the PCP and DEI value in the tag. Otherwise the frame is classified to the default DPL. The classified DPL can be overruled by a QCL entry.

PCP : Priority Code Point controls the default PCP value. All frames are classified to a PCP value. If the port is VLAN aware and the frame is tagged, then the frame is classified to the PCP value in the tag. Otherwise the frame is classified to the default PCP value.

DEI : Controls the default DEI value. All frames are classified to a DEI value. If the port is VLAN aware and the frame is tagged, then the frame is classified to the DEI value in the tag. Otherwise the frame is classified to the default DEI value.

DSCP Based : Click to Enable DSCP Based QoS Ingress Port Classification.

WRED Group : At the dropdown select the WRED group membership (instance).

Buttons

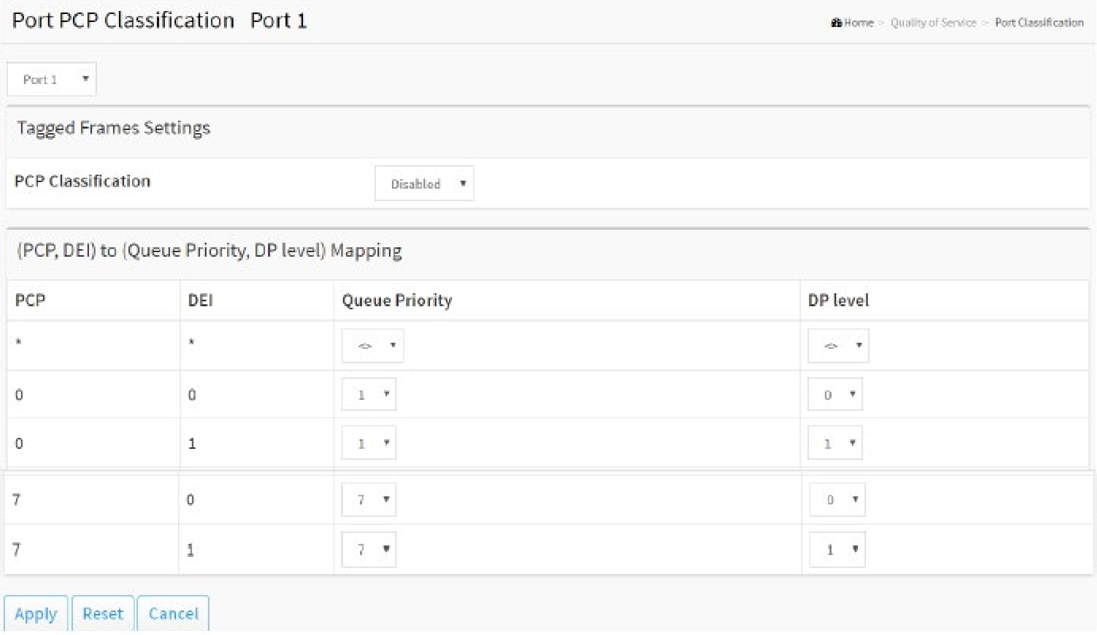
Apply : Click to save changes.

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

PCP Classification : Shows the classification mode for tagged frames on this port.

Disabled: Use default CoS and DPL for tagged frames.
Enabled: Use mapped versions of PCP and DEI for tagged frames.

Click on the linked text to configure the mode and/or mapping for the port. **Note**: This setting has no effect if the port is VLAN unaware. Tagged frames received on VLAN unaware ports are always classified to the default CoS and DPL.



Port PCP Classification Port 1

Port 1 ▾

Tagged Frames Settings

PCP Classification: Disabled ▾

(PCP, DEI) to (Queue Priority, DP level) Mapping

PCP	DEI	Queue Priority	DP level
*	*	<> ▾	<> ▾
0	0	1 ▾	0 ▾
0	1	1 ▾	1 ▾
7	0	7 ▾	0 ▾
7	1	7 ▾	1 ▾

Figure 6-1: Port PCP Classification

Parameter descriptions :

PCP Classification : Priority Code Point controls the classification mode for tagged frames on this port.

Disabled: Use default CoS and DPL for tagged frames.

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

(PCP, DEI) to (Queue Priority, DPL level) Mapping : Controls the mapping of the classified (PCP, DEI) to (Queue Priority, DPL level) values when Tag Classification is set to Enabled.

Buttons

Apply : Click to save changes.

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

Cancel : Click to undo any changes made locally and return to the previous page.

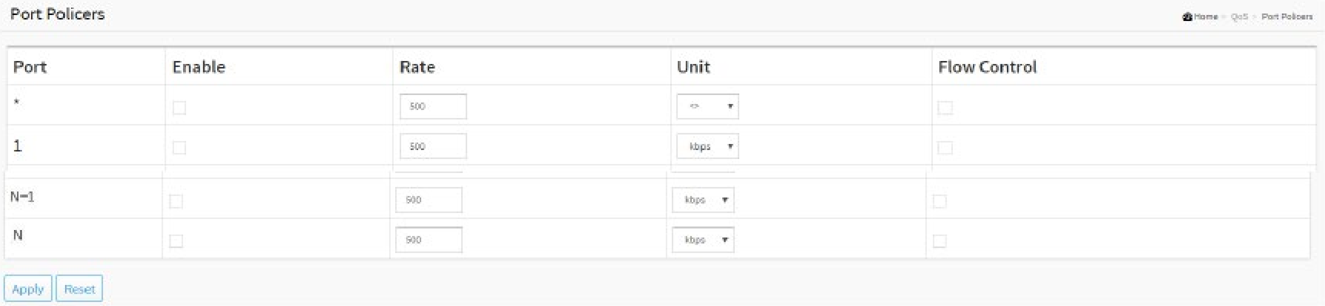
Port Policers

This page 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 mainly used for data flows and voice or video flows because voice and video usually maintain a steady rate of traffic.

Web Interface

To configure QoS Port Policers in the web UI:

1. Click Quality of Service and Port Policers.
2. Click on the port on which you want to enable the QoS Ingress Port Policers.
3. Configure the Rate limit condition.
4. Select parameters in the column Rate and Unit of measure.
5. Click Apply to save the configuration.
6. To cancel the settings, click the Reset button. It will revert to previously saved values.



Port Policers

Port	Enable	Rate	Unit	Flow Control
*	□	500	<> ▾	□
1	□	500	kbps ▾	□
N-1	□	500	kbps ▾	□
N	□	500	kbps ▾	□

Figure 6-2: QoS Ingress Port Policers Configuration

Parameter descriptions:

Port : The logical port for the settings contained in the same row. Click on the port number in order to configure the schedulers.

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

Rate : To set the Rate limit value for this port, the default is 1000000.

Unit : Controls the unit of measure for the port policer rate as kbps, Mbps, fps (frames per second), or kfps.

Flow Control : If flow control is enabled and the port is in flow control mode, then pause frames are sent instead of discarding frames.

Buttons

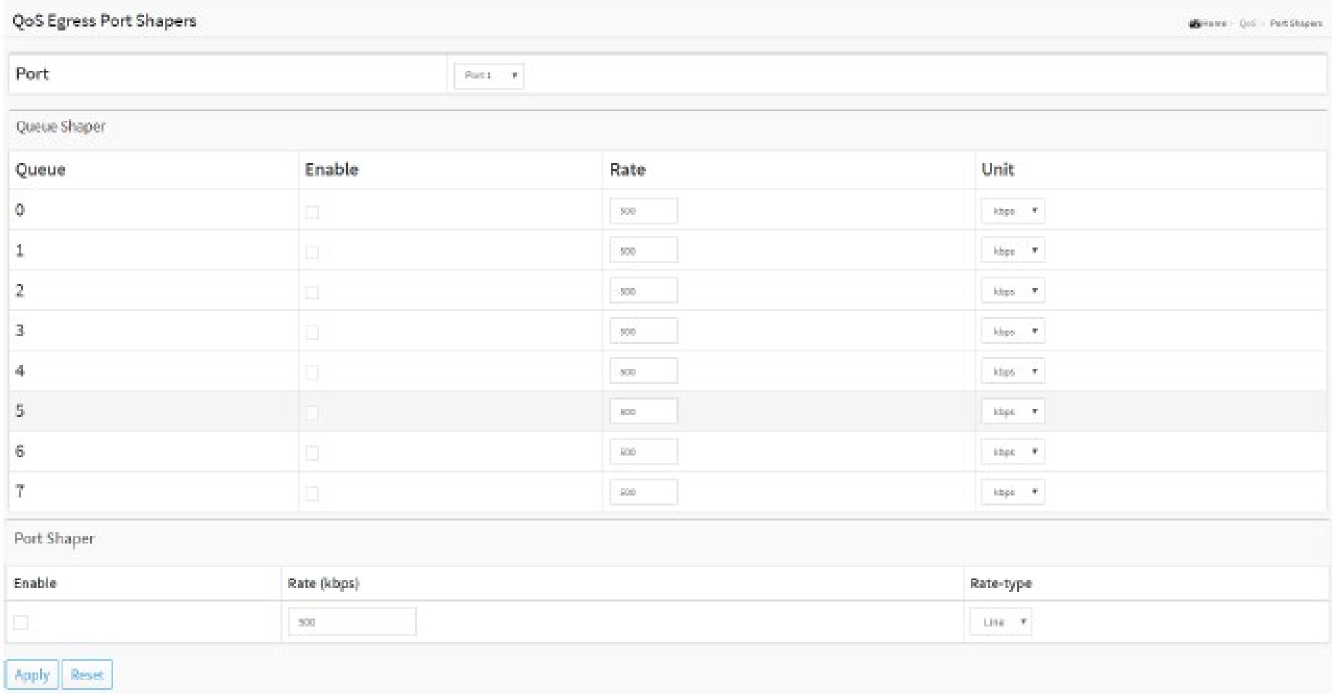
Apply : Click to save changes.

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

Port Shapers

This page provides an overview of QoS Egress Port Shapers for all switch ports. To configure QoS Port Shapers in the web UI:

1. Click Quality of Service and Port Shapers.
2. Select the desired Port to display its QoS Egress Port Shapers.
3. Specify the Queue Shaper parameters.
4. Click the Apply button to save the settings.
5. To cancel the settings, click the Rise button. It will revert to previously saved values.



QoS Egress Port Shapers

Port	Port 1 ▾

Queue Shaper

Queue	Enable	Rate	Unit
0	□	500	kbps ▾
1	□	500	kbps ▾
2	□	500	kbps ▾
3	□	500	kbps ▾
4	□	500	kbps ▾
5	□	500	kbps ▾
6	□	500	kbps ▾
7	□	500	kbps ▾

Port Shaper

Enable	Rate (kbps)	Rate-type
□	500	Line ▾

Figure 6-3: QoS Egress Port Shapers

Parameter descriptions :

Port : At the dropdown select the port number in order to configure its shapers.

Queue Shaper Enable : Check the checkbox to enable the queue shaper for this queue on this switch port.

Queue Shaper Rate : Select the rate for the queue shaper. This value can be 100-13107100 when "Unit" is kbps, and 1-13107 when "Unit" is Mbps. The rate is internally rounded up to the nearest value supported by the queue shaper.

Queue Shaper Unit : Controls the unit of measure for the queue shaper rate as kbps or Mbps.

Queue Shaper Rate-type : The rate type of the queue shaper. The allowed values are:

__Line__: Specify that this shaper operates on the line rate.

__Data__: Specify that this shaper operates on the data rate.

Queue Scheduler Weight : Controls the weight for this queue. This value is restricted to 1-100. This parameter is only shown if "Scheduler Mode" is set to "Weighted".

Queue Scheduler Percent : Shows the weight in percent for this queue. This parameter is only shown if "Scheduler Mode" is set to "Weighted".

Port Shaper Enable : Controls whether the port shaper is enabled for this switch port.

Port Shaper Rate : Controls the rate for the port shaper. This value is restricted to 100-13107100 when "Unit" is kbps, and 1-13107 when "Unit" is Mbps. The rate is internally rounded up to the nearest value supported by the port shaper.

Port Shaper Unit : Controls the unit of measure for the port shaper rate as kbps or Mbps.

Buttons

Apply : Click to save changes.

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

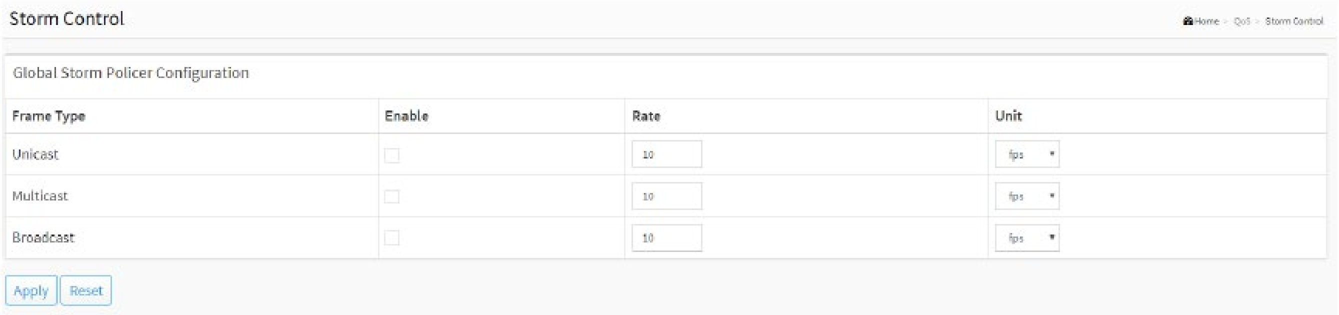
Storm Control

This page lets you configure switch Storm control parameters. 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 in the MAC Address table. The configuration indicates the permitted packet rate for unicast, multicast, or broadcast traffic across the switch

Web Interface

To configure Storm Control parameters in the web UI:

1. Click Quality of Service and Storm Control.
2. Select the frame type(s) to enable storm control.
3. Set the Rate and Unit parameters.
4. Click which port you want to enable and configure the Rate limit condition.
5. Click the Apply button to save the settings.
6. To cancel the settings, click the Reset button. It will revert to previously saved values.



Storm Control

Home > QoS > Storm Control

Global Storm Policer Configuration

Frame Type	Enable	Rate	Unit
Unicast	□	10	fps
Multicast	□	10	fps
Broadcast	□	10	fps

Figure 6-4: Storm Control Configuration

Parameter descriptions :

Global Storm Policer Configuration : Global storm policers for the switch are configured on this page. There is a unicast storm policer, multicast storm policer, and a broadcast storm policer. These only affect flooded frames, i.e., frames with a (VLAN ID, DMAC) pair not present in the MAC Address table.

Frame Type : The frame type (Unicast, Multicast, Broadcast) for which the configuration below applies.

Enable : Enable or disable the global storm policer for the given frame type.

Rate : Set the rate for the global storm policer. This value is restricted to 10-13128147 when "Unit" is fps or kbps, and 1-13128 when "Unit" is kfps or Mbps. The rate is internally rounded up to the nearest value supported by the global storm policer. Supported rates are divisible by 10 fps or 25 kbps.

Unit : Select the unit of measure for the global storm policer rate as fps, kfps, kbps or Mbps. The default is ‘fps’.

Buttons

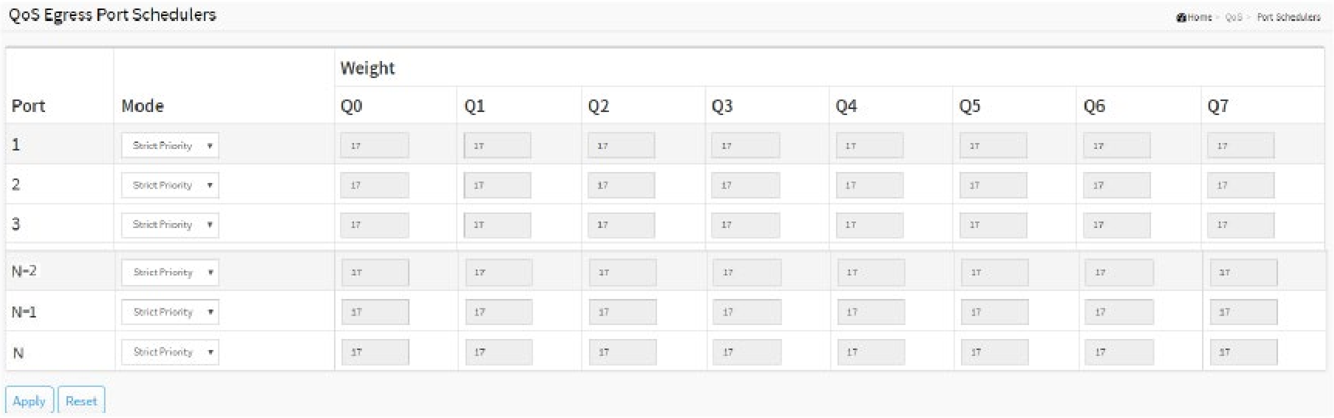
Apply : Click to save changes.

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

Port Scheduler

This page provides an overview of QoS Egress Port Scheduler for all switch ports. To configure QoS Egress Port Schedulers in the web UI:

1. Click Quality of Service and Port Scheduler.
2. Click the Port and display the QoS Egress Port Schedulers.
3. Select Port and Scheduler Mode and specify the Queue Shaper parameter.
4. Click the Apply button to save the settings.
5. To cancel the settings, click the Reset button. It will revert to previously saved values.



QoS Egress Port Schedulers

		Weight							
Port	Mode	Q0	Q1	Q2	Q3	Q4	Q5	Q6	Q7
1	Strict Priority ▾	17	17	17	17	17	17	17	17
2	Strict Priority ▾	17	17	17	17	17	17	17	17
3	Strict Priority ▾	17	17	17	17	17	17	17	17
N-2	Strict Priority ▾	17	17	17	17	17	17	17	17
N-1	Strict Priority ▾	17	17	17	17	17	17	17	17
N	Strict Priority ▾	17	17	17	17	17	17	17	17

Figure 6-5: QoS Egress Port Schedulers

Parameter descriptions :

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

Mode : Select the scheduling mode for this port (e.g., Strict Priority, WRR).

Q0 – Q7 : Shows the weight for this queue and port.

Scheduler Mode : Controls how many of the queues are scheduled as Strict and how many are scheduled as Weighted on this switch port.

Queue Shaper Enable : Controls whether the queue shaper is enabled for this queue on this switch port.

Queue Shaper Rate : Controls the rate for the queue shaper. This value is restricted to 100-13107100 when "Unit" is kbps, and 1-13107 when "Unit" is Mbps. The rate is internally rounded up to the nearest value supported by the queue shaper.

Queue Shaper Unit : Controls the unit of measure for the queue shaper rate as ***kbps*** or ***Mbps***.

Queue Shaper Rate-type : The rate type of the queue shaper. The allowed values are: ***Line***: Specify that this shaper operates on line rate. ***Data***: Specify that this shaper operates on data rate.

Queue Scheduler Weight : Controls the weight for this queue. This value is restricted to 1-100. This parameter is only shown if "Scheduler Mode" is set to "Weighted".

Queue Scheduler Percent : Shows the weight in percent for this queue. This parameter is only shown if "Scheduler Mode" is set to "Weighted".

Port Shaper Enable : Controls whether the port shaper is enabled for this switch port.

Port Shaper Rate : Controls the rate for the port shaper. This value is restricted to 100-13107100 when "Unit" is kbps, and 1-13107 when "Unit" is Mbps. The rate is internally rounded up to the nearest value supported by the port shaper.

Port Shaper Unit : Controls the unit of measure for the port shaper rate as ***kbps*** or ***Mbps***.

Port Shaper Rate-type : The rate type of the port shaper. The allowed values are: ***Line***: Specify that this shaper operates on line rate. ***Data***: Specify that this shaper operates on data rate.

Buttons

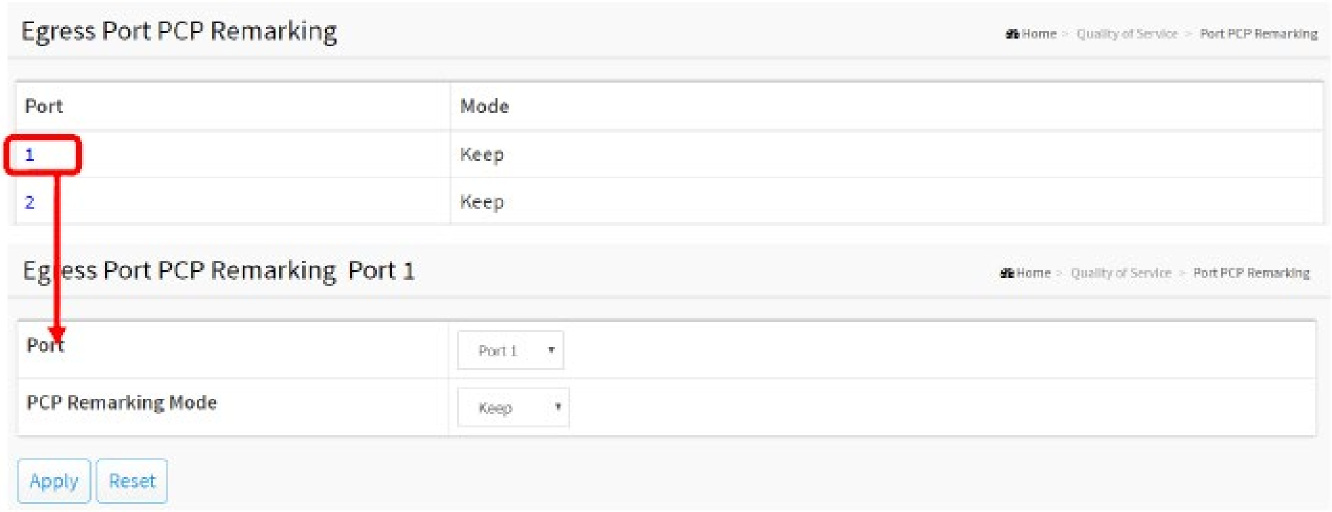
Apply : Click to save changes.

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

Egress Port PCP Remarking

This page lets you set QoS Egress Port PCP Remarking for each switch port. To configure QoS Port PCP Remarking in the web UI:

1. Click Quality of Service and Port PCP Remarking.
2. Select the Port and display the QoS Port PCP Remarking.
3. Select the PCP Remarking Mode and specify the Queue Shaper parameter.
4. Click the Apply button to save the settings.
5. To cancel the settings, click the Reset button. It will revert to previously saved values.



Egress Port PCP Remarking

Home > Quality of Service > Port PCP Remarking

Port	Mode
1	Keep
2	Keep

Egress Port PCP Remarking Port 1

Home > Quality of Service > Port PCP Remarking

Port	Port 1
PCP Remarking Mode	Keep

Figure 6-6: Egress Port PCP Remarking

Parameter descriptions:

Port : The logical port for the settings contained in the same row. At the dropdown select the port number to configure PCP remarking.

Mode : Shows the PCP remarking mode for this port.

Keep: Use classified PCP/DEI values (default).

Specific: Use default PCP/DEI values.

Mapped: Use mapped versions of CoS and DPL.

Buttons

Apply : Click to save changes.

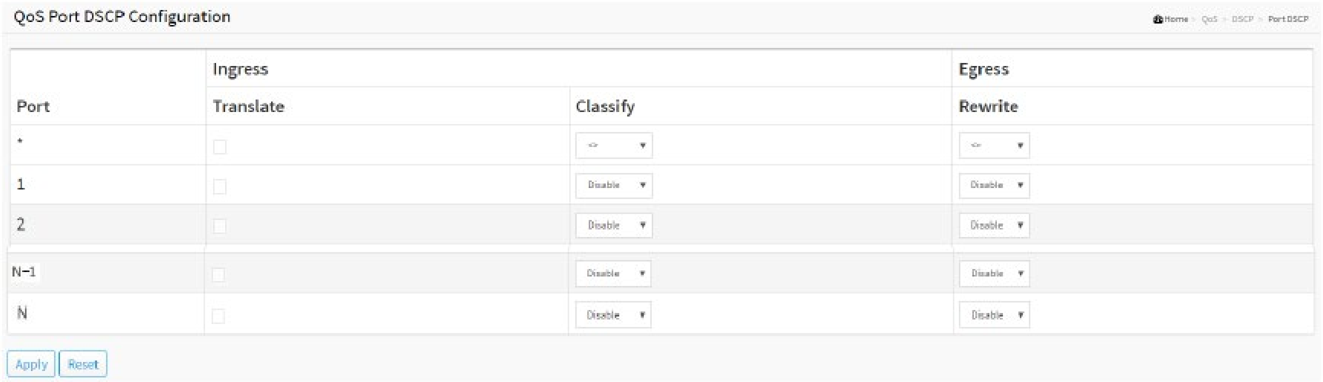
Reset : Click to undo any changes made locally and revert to previously saved values.

DSCP

Port DSCP

This page lets you set QoS Port DSCP parameters for all switch ports. To configure QoS Port DSCP parameters in the web UI:

1. Click Quality of Service, DSCP, and Port DSCP.
2. Enable or disable the Ingress Translate and select the Classify parameters.
3. Select the Egress Rewrite parameter.
4. Click Apply to save the settings.



QoS Port DSCP Configuration

	Ingress		Egress
Port	Translate	Classify	Rewrite
*	□	<> ▾	<> ▾
1	□	Disable ▾	Disable ▾
2	□	Disable ▾	Disable ▾
N-1	□	Disable ▾	Disable ▾
N	□	Disable ▾	Disable ▾

Figure 6-7.1: QoS Port DSCP Configuration

Parameter descriptions:

Port : The Port column shows the list of ports for which you can configure DSCP ingress and egress settings.

Ingress : In Ingress settings you can change ingress translation and classification settings for individual ports. There are two configuration parameters available in Ingress:

Translate : To Enable Ingress Translation check the checkbox.

Classify : Classification for a port have 4 different values:

Disable: No Ingress DSCP Classification.

DSCP=0: Classify if incoming (or translated if enabled) DSCP is 0.

Selected: Classify only selected DSCP for which classification is enabled as specified in DSCP Translation window for the specific DSCP.

All: Classify all DSCP.

Egress Rewrite : Port Egress Rewriting can be one of these parameters:

Disable : No Egress rewrite (default).

Enable: Rewrite enable without remapped.

Remap : DSCP from analyzer is remapped and frame is remarked with remapped DSCP value.

Buttons

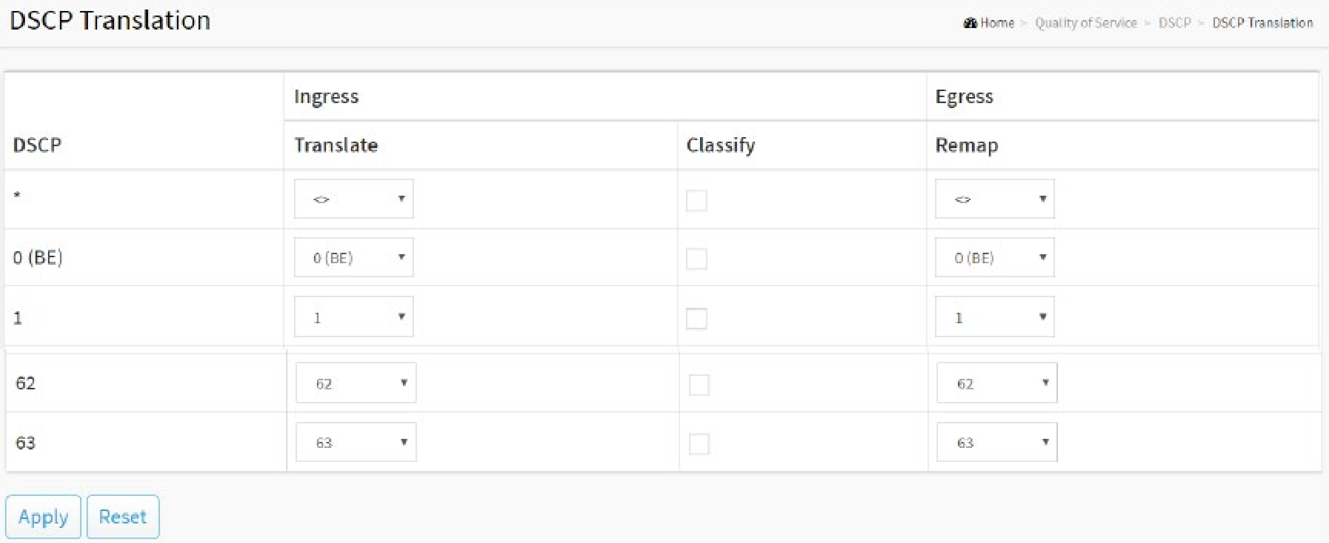
Apply : Click to save changes.

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

DSCP Translation

This page lets you configure basic QoS DSCP Translation settings for the switch. DSCP translation can be done in Ingress or Egress. To configure DSCP Translation parameters in the web UI:

1. Click Quality of Service, DSCP, and DSCP Translation.
2. Set the Ingress Translate and Egress Remap Parameters.
3. Enable or disable Classify.
4. Click the Apply button to save the settings.
5. To cancel the settings, click the Reset button to revert to previously saved values.



DSCP Translation

	Ingress		Egress
DSCP	Translate	Classify	Remap
*	<>	□	<>
0 (BE)	0 (BE)	□	0 (BE)
1	1	□	1
62	62	□	62
63	63	□	63

Figure 6-7.2: DSCP Translation Configuration

Parameter descriptions:

DSCP : Maximum number of supported DSCP values are 64 and valid DSCP values are 0 - 63.

Ingress : Ingress side DSCP can be first translated to new DSCP before using the DSCP for QoS class and DPL map. There are two configuration parameters for DSCP Translation:

Translate: DSCP at Ingress side can be translated to any of (0-63) DSCP values.

Classify: Click to enable Classification at Ingress side.

Egress Remap : At the dropdown select the DSCP value to which you want to remap. The DSCP value can be 0 - 63.

Buttons

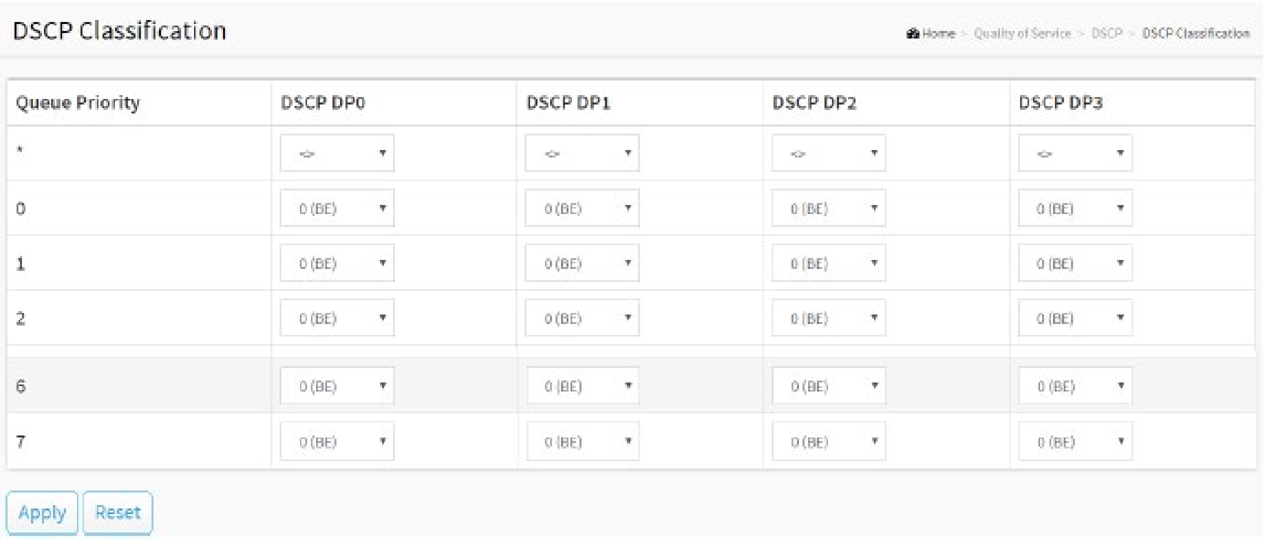
Apply : Click to save changes.

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

DSCP Classification

This page lets you map DSCP value to a QoS Class and DPL value. To configure DSCP Classification parameters in the web UI:

1. Click Quality of Service, DSCP, and DSCP Translation
2. Set the DSCP Parameters.
3. Click the Apply button to save the settings.
4. To cancel the setting click the Reset button. It will revert to previously saved values.



DSCP Classification

Queue Priority	DSCP DP0	DSCP DP1	DSCP DP2	DSCP DP3
*	<>	<>	<>	<>
0	0 (BE)	0 (BE)	0 (BE)	0 (BE)
1	0 (BE)	0 (BE)	0 (BE)	0 (BE)
2	0 (BE)	0 (BE)	0 (BE)	0 (BE)
6	0 (BE)	0 (BE)	0 (BE)	0 (BE)
7	0 (BE)	0 (BE)	0 (BE)	0 (BE)

Figure 6-7.3: DSCP Classification Configuration

Parameter descriptions:

Queue Priority : Actual Class of Service (0-7).

DSCP DP0 : Select the classified DSCP value (0-63) for Drop Precedence Level 0.

DSCP DP1 : Select the classified DSCP value (0-63) for Drop Precedence Level 1.

DSCP DP2 : Select the classified DSCP value (0-63) for Drop Precedence Level 2.

DSCP DP3 : Select the classified DSCP value (0-63) for Drop Precedence Level 3.

Buttons

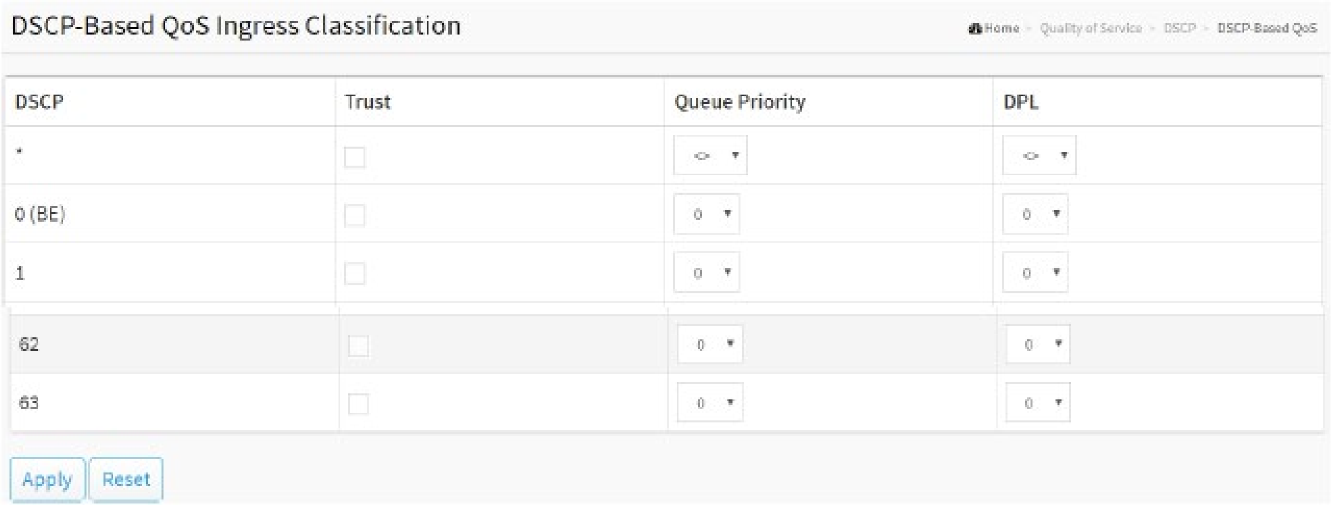
Apply : Click to save changes.

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

DSCP-Based QoS

This page lets you configure basic QoS DSCP based QoS Ingress Classification settings. To configure DSCP-Based QoS Ingress Classification in the web UI:

1. Click Quality of Service, DSCP, and DSCP-Based QoS.
2. Enable or disable Trust for DSCP.
3. Select Queue Priority and DPL parameters.
4. Click the Apply button to save the settings.
5. To cancel the settings, click the Reset button. It will revert to previously saved values.



DSCP-Based QoS Ingress Classification

DSCP	Trust	Queue Priority	DPL
*	□	<> ▾	<> ▾
0 (BE)	□	0 ▾	0 ▾
1	□	0 ▾	0 ▾
62	□	0 ▾	0 ▾
63	□	0 ▾	0 ▾

Figure 6-7.4: DSCP-Based QoS Ingress Classification

Parameter descriptions:

DSCP : Maximum number of supported DSCP values is 64.

Trust : Check the box if the DSCP value is to be trusted.

Queue Priority : Queue Priority value can be 0 – 7, where 7 is the highest priority.

DPL : Drop Precedence Level (0-3).

Buttons

Apply : Click to save changes.

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

QoS Control List

Configuration

This page shows the QoS Control List (QCL), which is made up of the QCEs.

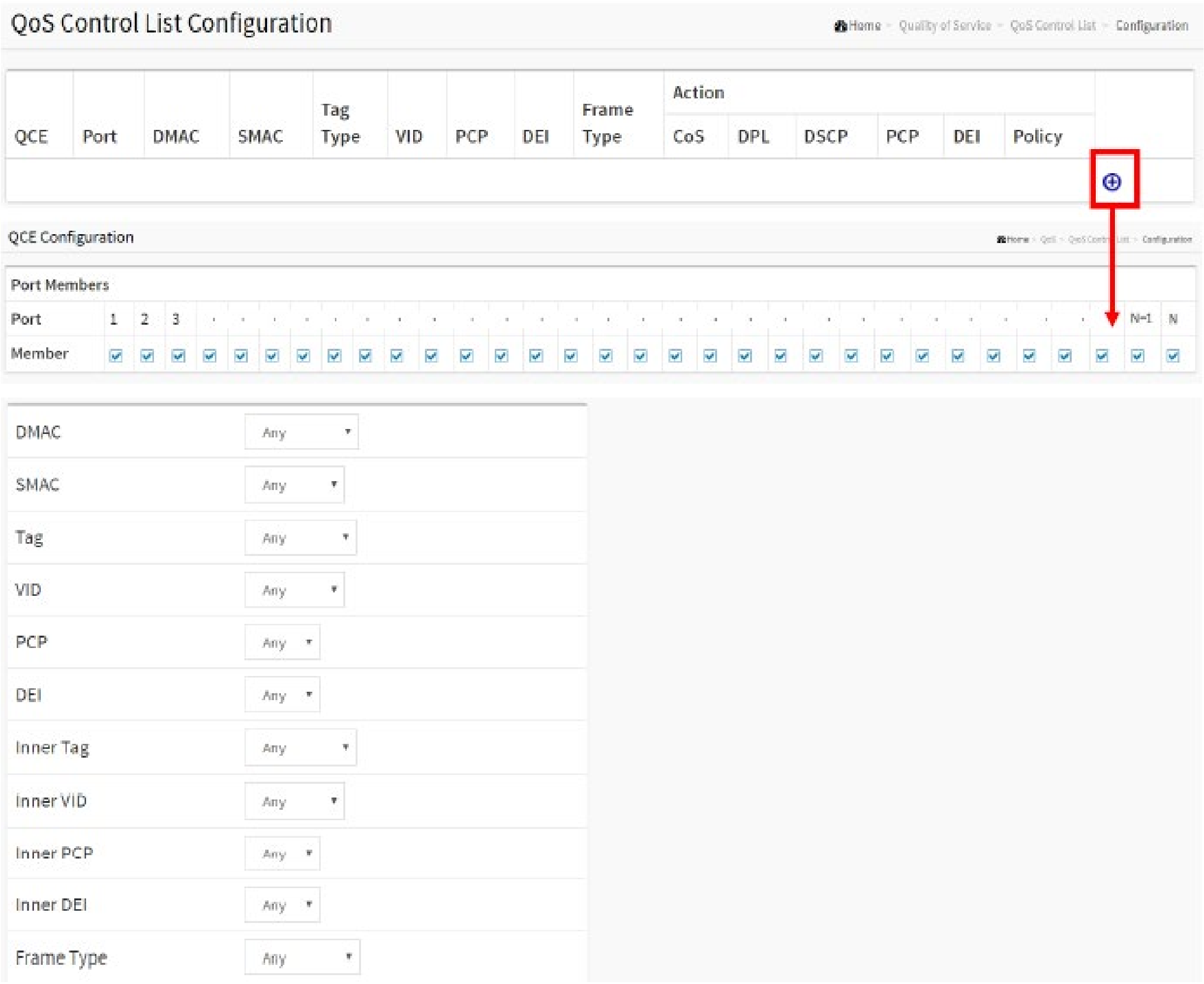
A QCE (QoS Control Entry) describes a QoS class associated with a particular QCE ID. There are six QCE frame types: Ethernet Type, VLAN, UDP/TCP Port, DSCP, TOS, and Tag Priority. Frames can be classified by one of four different QoS classes: "Low", "Normal", "Medium", and "High" for an individual application.

Each row in the table describes a QCE that is defined. The maximum number of QCEs is 256 per switch. Click on the lowest plus sign to add a new QCE to the list.

Web Interface

To configure QoS Control List parameters in the web UI:

1. Click Quality of Service, QoS Control List, and Configuration.
2. Click the plus sign ⊕ to add a new QoS Control List.
3. Set all parameters and enable Port Members to join the QCE rules.
4. Click the Apply button to save the settings.
5. To cancel the settings click the Reset button to revert to previously saved values.



QoS Control List Configuration

Home › Quality of Service › QoS Control List › Configuration

QCE	Port	DMAC	SMAC	Tag Type	VID	PCP	DEI	Frame Type	Action						
									CoS	DPL	DSCP	PCP	DEI	Policy	
															⊕

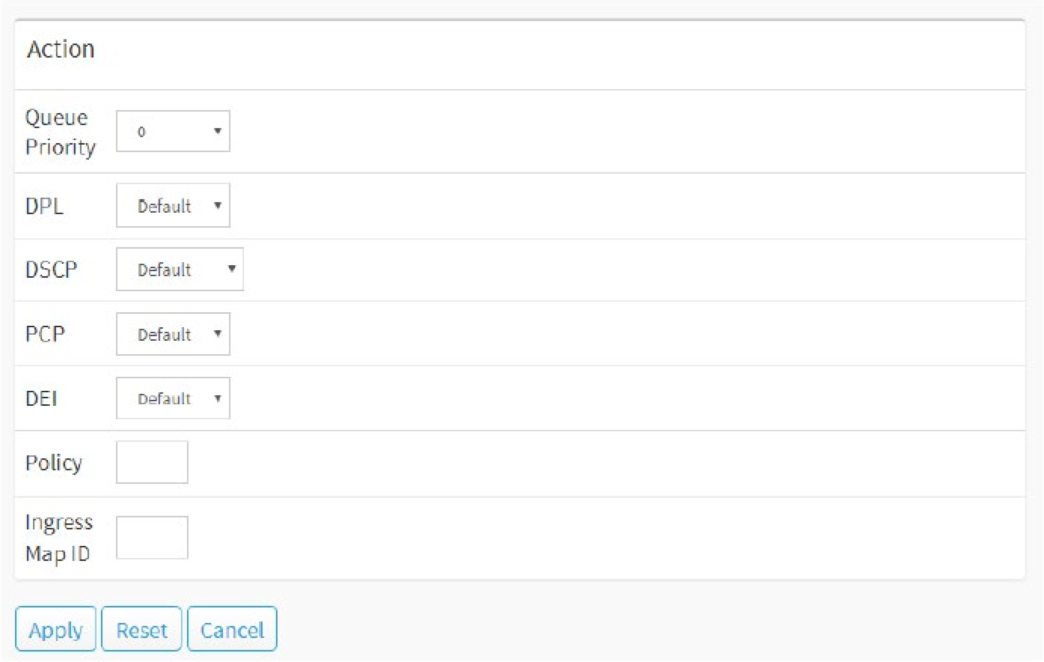
QCE Configuration

Home › QoS › QoS Control List › Configuration

Port Members

Port	1	2	3	·	·	·	·	·	·	·	·	·	·	·	·	·	·	·	·	·	·	·	·	·	·	·	·	·	·	·	N-1	N
Member	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑

DMAC	Any
SMAC	Any
Tag	Any
VID	Any
PCP	Any
DEI	Any
Inner Tag	Any
Inner VID	Any
Inner PCP	Any
Inner DEI	Any
Frame Type	Any



Action

Queue Priority	0
DPL	Default
DSCP	Default
PCP	Default
DEI	Default
Policy	
Ingress Map ID	

Figure 6-8.1: QoS Control List Configuration

Parameter descriptions:

QCE : Indicates the index of QCE.

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

DMAC : Indicates the destination MAC address. Possible values are:

Any: Match any DMAC. The default value is 'Any'.

Unicast: Match unicast DMAC.

Multicast: Match multicast DMAC.

Broadcast: Match broadcast DMAC.

<MAC> : Match specific DMAC.

SMAC : Match specific source MAC address or 'Any'. If a port is configured to match on DMAC/DIP, this field indicates the DMAC.

Tag Type : Indicates tag type. Possible values are:

Any: Match tagged and untagged frames. The default value is 'Any'.

Untagged: Match untagged frames.

Tagged: Match tagged frames.

C-Tagged: Match C-tagged frames.

S-Tagged: Match S-tagged frames.

VID : Indicates (VLAN ID), either a specific VID or range of VIDs. VID can be in the range 1-4095 or 'Any'

PCP : Priority Code Point: Valid values of PCP are specific (0, 1, 2, 3, 4, 5, 6, 7) or range(0-1, 2-3, 4-5, 6-7, 0-3, 4-7) or 'Any'.

DEI : Drop Eligible Indicator: Valid value of DEI are 0, 1 or 'Any'.

Inner Tag : Value of can be 'Untagged', 'Tagged', 'C-Tagged', 'S-Tagged' or 'Any'.

Inner VID : Valid value can be any value in the range 1-4095 or 'Any'; user can enter either a specific value or a range of VIDs.

Inner PCP : Valid value is specific (0, 1, 2, 3, 4, 5, 6, 7) or range (0-1, 2-3, 4-5, 6-7, 0-3, 4-7) or 'Any'.

Inner DEI : Valid value can be '0', '1' or 'Any'.

Frame Type : Indicates the type of frame to look for incoming frames. Possible frame types are:

Any: The QCE will match all frame type.

Ethernet: Only Ethernet frames (with Ether Type 0x600-0xFFFF) are allowed.

LLC: Only (LLC) frames are allowed.

SNAP: Only (SNAP) frames are allowed

IPv4: The QCE will match only IPV4 frames.

IPv6: The QCE will match only IPV6 frames.

Action : Indicates the classification action taken on ingress frame if parameters configured are matched with the frame's content. Possible actions are:

Queue Priority : Classify Class of Service.

DPL: Classify Drop Precedence Level.

DSCP : Classify DSCP value.

PCP : Classify PCP value.

DEI : Classify DEI value.

Policy : Classify ACL Policy number.

Ingress Map ID : Classify Ingress Map ID.

Buttons : You can modify each QCE (QoS Control Entry) in the table using these buttons:

⊕: Inserts a new QCE before the current row.

ⓔ: Edits the QCE.

↑ : Moves the QCE up the list.

↓ : Moves the QCE down the list.

⊗ : Deletes the QCE.

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

Port Members : Check the checkbox button to include the port in the QCL entry. By default all ports are included.

Key Parameters : Key configuration is described below:

> ***DMAC*** Destination MAC address: Possible values are 'Unicast', 'Multicast', 'Broadcast', 'Specific' (xx-xx-xx-xx-xx-xx) or 'Any'.
>
> ***SMAC*** Source MAC address: xx-xx-xx-xx-xx-xx or 'Any'.
>
> Tag Value of Tag field can be 'Untagged', 'Tagged', 'C-Tagged', 'S-Tagged' or 'Any'.
>
> ***VID*** Valid value of VLAN ID can be any value in the range 1-4095 or 'Any'; user can enter either a specific value or a range of VIDs.
>
> ***PCP*** : Valid value PCP are specific (0, 1, 2, 3, 4, 5, 6, 7) or range (0-1, 2-3, 4-5, 6-7, 0-3, 4-7) or 'Any'.
>
> ***DEI*** : Valid value of DEI can be '0', '1' or 'Any'.
>
> ***Inner Tag*** : Value of can be 'Untagged', 'Tagged', 'C-Tagged', 'S-Tagged' or 'Any'.
>
> ***Inner VID*** : Valid value can be any value in the range 1-4095 or 'Any'; user can enter either a specific value or a range of VIDs.
>
> ***Inner PCP*** : Valid value is specific (0, 1, 2, 3, 4, 5, 6, 7) or range (0-1, 2-3, 4-5, 6-7, 0-3, 4-7) or 'Any'.
>
> ***Inner DEI*** : Valid value can be '0', '1' or 'Any'.
>
> ***Frame Type*** : Valid values are Any, EtherType, LLC, SNAP, IPv4, or IPv6.

Note: These frame types are described below:

Any : Allow all types of frames.

EtherType : Valid Ether Type can be 0x600-0xFFFF excluding 0x800(IPv4) and 0x86DD(IPv6) or 'Any'.

LLC : Valid selections are:

> ***DSAP Address***: Valid DSAP(Destination Service Access Point) can vary from 0x00 to 0xFF or 'Any'.
>
> ***SSAP Address*** : Valid SSAP(Source Service Access Point) can vary from 0x00 to 0xFF or 'Any'.
>
> ***Control*** : Valid Control field can vary from 0x00 to 0xFF or 'Any'.

SNAP : PID Valid PID (a.k.a., Ether Type) can be 0x0000-0xFFFF or 'Any'.

IPv4 : Valid selections are:

> ***Protocol*** : IP protocol number: (0-255, 'TCP' or 'UDP') or 'Any'.
>
> ***Source IP*** : Specific Source IP address in value/mask format or 'Any'. IP and Mask are in the format x.y.z.w where x, y, z, and w are decimal numbers between 0 and 255. When Mask is converted to a 32-bit binary string and read from left to right, all bits following the first zero must also be zero.
>
> ***Destination IP*** : Specific Destination IP address in value/mask format or 'Any'.
>
> ***IP Fragment*** : IPv4 frame fragmented option: 'Yes', 'No' or 'Any'.
>
> ***DSCP*** : Diffserv Code Point value (DSCP): It can be a specific value, range of values or 'Any'. DSCP values are in the range 0-63 including BE, CS1-CS7, EF or AF11-AF43.
>
> ***Sport*** : Source TCP/UDP port:(0-65535) or 'Any', specific or port range applicable for IP protocol UDP/TCP.
>
> ***Dport*** : Destination TCP/UDP port:(0-65535) or 'Any', specific or port range applicable for IP protocol UDP/TCP.

IPv6 :

Protocol : IP protocol number: (0-255, 'TCP' or 'UDP') or 'Any'.

Source IP : 32 LS bits of IPv6 source address in value/mask format or 'Any'.

Destination IP : Specific Destination IP address in value/mask format or 'Any'.

DSCP : Diffserv Code Point value (DSCP): It can be a specific value, range of values or 'Any'. DSCP values are in the range 0-63 including BE, CS1-CS7, EF or AF11-AF43.

Sport : Source TCP/UDP port:(0-65535) or 'Any', specific or port range applicable for IP protocol UDP/TCP.

Dport : Destination TCP/UDP port:(0-65535) or 'Any', specific or port range applicable for IP protocol UDP/TCP.

Action Parameters :

Queue : Priority Class of Service: (0-7) or 'Default'.

DPL : Drop Precedence Level: (0-3) or 'Default'.

DSCP: (0-63, BE, CS1-CS7, EF or AF11-AF43) or 'Default'.

PCP: (0-7) or 'Default'. Note: PCP and DEI cannot be set individually.

DEI: Drop Eligibility Indicator (0-1) or 'Default'.

Policy : ACL Policy number: (0-127) or 'Default' (empty field).

Ingress Map Classify Ingress Map ID : (0-127) or 'Default' (empty field).

'*Default*' means that the default classified value is not modified by this QCE.

Buttons

Apply : Click to save changes.

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

Cancel : Return to the previous page without saving the configuration change.

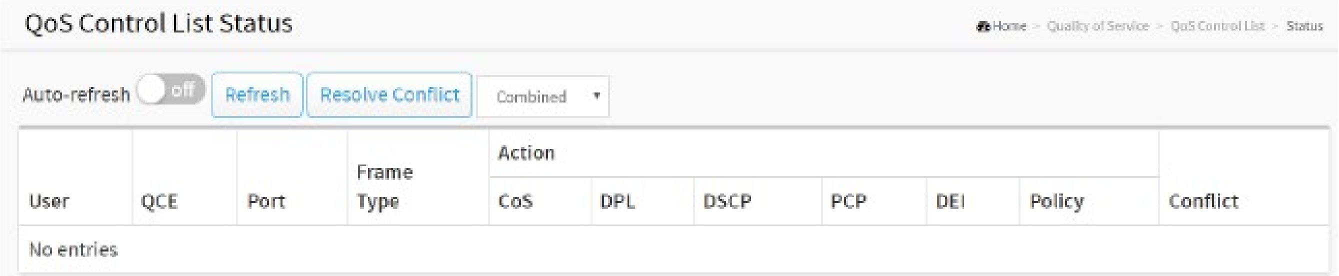
Status

This page lets you view and configure QCL status by different QCL users. Each row describes a defined QCE. It is a conflict if a specific QCE is not applied to the hardware due to hardware limitations. The maximum number of QCEs is 256 per switch.

Web Interface

To display QoS Control List Status in the web UI:

1. Click Quality of Service, QoS Control List, and Status.
2. At the dropdown select Combined, Static, Voice VLAN, or Conflict.
3. To automatically refresh the information, click the “Auto-refresh” button.
4. Click “Refresh” to refresh an entry of the Information.



Auto-refresh off

Combined

User	QCE	Port	Frame Type	Action						Conflict
				CoS	DPL	DSCP	PCP	DEI	Policy	
No entries										

Figure 6-8.2: QoS Control List Status

Parameter descriptions :

User : Indicates the QCL user.

QCE : Indicates the index of QCE.

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

Frame Type : Indicates the type of frame. Possible values are:

Any: Match any frame type.

Ethernet: Match EtherType frames.

LLC: Match (LLC) frames.

SNAP: Match (SNAP) frames.

IPv4: Match IPv4 frames.

IPv6: Match IPv6 frames.

Action : Indicates the classification action taken on ingress frame if parameters configured are matched with the frame's content. Possible actions are:

CoS: Classify Class of Service.

DPL: Classify Drop Precedence Level.

DSCP: Classify DSCP value.

PCP: Classify PCP value.

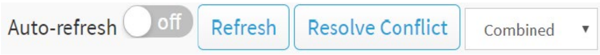
DEI: Classify DEI value.

Policy: Classify ACL Policy number.

Ingress Map: Classify Ingress Map ID.

Conflict : Displays Conflict status of QCL entries. It may happen that resources required to add a QCE may not available; in that case it shows Conflict status as 'Yes', otherwise it is always 'No'. **Note** that conflict can be resolved by releasing the Hardware resources required to add QCL entry on clicking the 'Resolve Conflict' button.

Buttons



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

Refresh : Click to refresh the page immediately.

User select dropdown : Select the QCL status from this drop down list. The default is ‘Combined’.

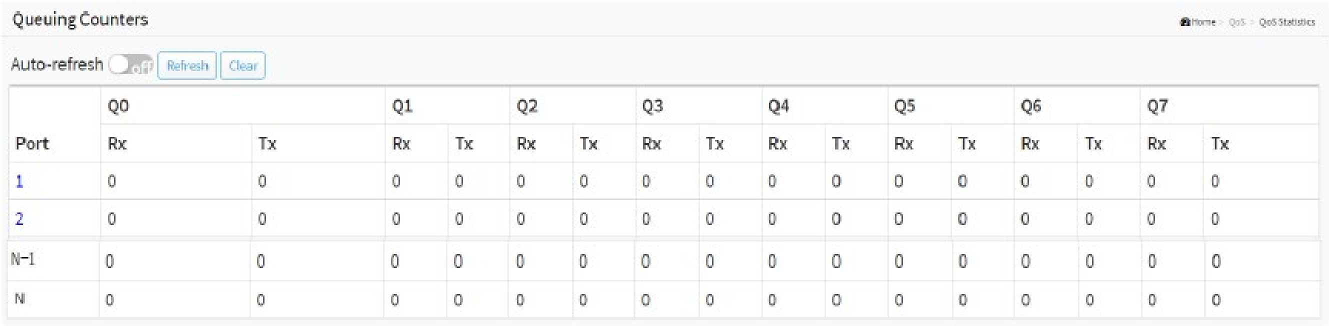
Resolve Conflict : Click to release the resources required to add QCL entry if the Conflict status for any QCL entry is 'yes'.

User select box: At the dropdown select Combined, Static, Voice VLAN, or Conflict.

QoS Statistics

This page displays statistics for the different queues for all switch ports. To display Queuing Counters in the web UI:

1. Click Quality of Service and QoS Statistics.
2. To automatically refresh the information, click the “Auto-refresh” button.
3. Click “Refresh” to refresh the Queuing Counters or clear all information when you click “Clear”.



	Q0		Q1		Q2		Q3		Q4		Q5		Q6		Q7	
Port	Rx	Tx	Rx	Tx	Rx	Tx	Rx	Tx	Rx	Tx	Rx	Tx	Rx	Tx	Rx	Tx
1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
2	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
N-1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
N	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0

Figure 6-9: Queuing Counters

Parameter descriptions:

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

Qn : Qn is the Queue number; there are eight QoS queues per port. Q0 is the lowest priority queue.

Rx/Tx : The number of received and transmitted packets per queue.

Buttons

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

Refresh : Click to manually refresh the page immediately.

Clear : Click to clear the page.

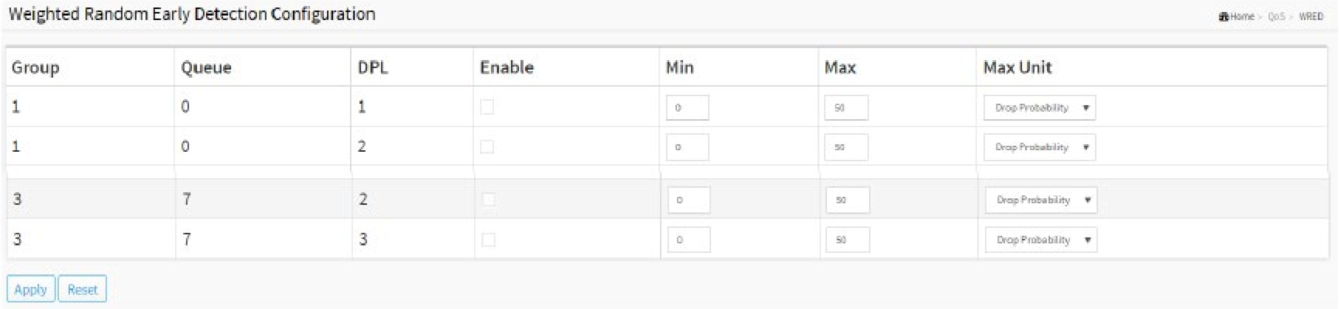
WRED

This page lets you configure the Random Early Detection (RED) settings. Using different RED queue configurations, you can obtain Weighted Random Early Detection (WRED) operation between queues. The settings are global for all ports in the switch.

Web Interface

To view and configure Random Early Detection in the web UI:

1. Click Quality of Service and WRED.
2. Select all parameters and enable the Weighted Random Early Detection Configuration.
3. Click the Apply button to save the settings.
4. To cancel the settings, click the Reset button. It will revert to previously saved values.



Weighted Random Early Detection Configuration

Group	Queue	DPL	Enable	Min	Max	Max Unit
1	0	1	☐	0	50	Drop Probability ▾
1	0	2	☐	0	50	Drop Probability ▾
3	7	2	☐	0	50	Drop Probability ▾
3	7	3	☐	0	50	Drop Probability ▾

Figure 6-10: Weighted Random Early Detection Configuration

Parameter descriptions:

Group: The WRED group number for which the configuration below applies.

Queue : The queue number (CoS) for which the configuration below applies.

DPL : The Drop Precedence Level for which the configuration below applies.

Enable : Controls whether RED is enabled for this entry.

Min : Controls the lower RED fill level threshold. If the queue filling level is below this threshold, the drop probability is zero. This value is restricted to 0-100%.

Max : Controls the upper RED drop probability or fill level threshold for frames marked with Drop Precedence Level > 0 (yellow frames). This value is restricted to 1-100%.

Max Unit : Selects the unit for Max. Possible values are: Drop Probability: Max controls the drop probability just below 100% fill level. Fill Level: Max controls the fill level where drop probability reaches 100%.

RED Drop Probability Function

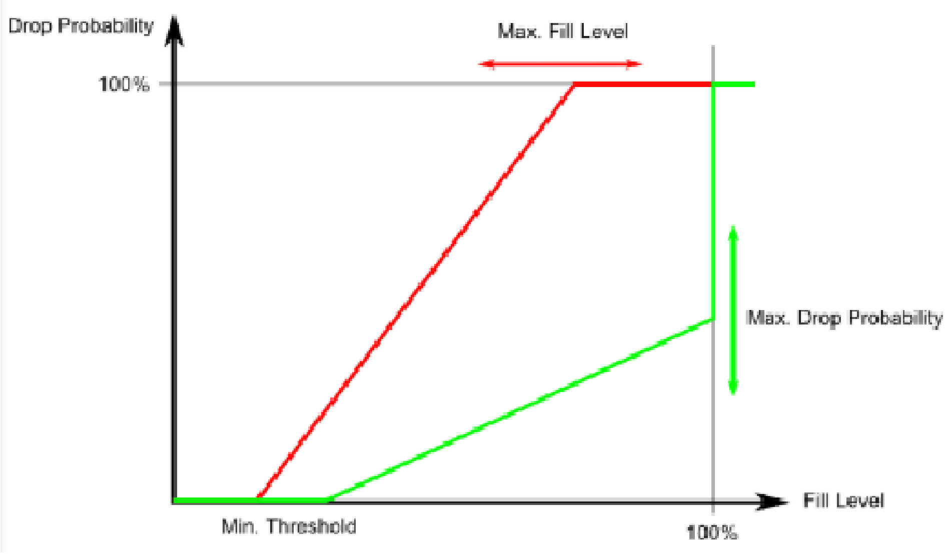
The figure below shows the drop probability versus fill level function with associated parameters.

Min. is the fill level where the queue randomly starts dropping frames marked with Drop Precedence Level > 0 (yellow frames).

If Max Unit is 'Drop Probability' (the green line), Max controls the drop probability when the fill level is just below 100%.

If Max Unit is 'Fill Level' (the red line), Max controls the fill level where drop probability reaches 100%. This configuration makes it possible to reserve a portion of the queue exclusively for frames marked with Drop Precedence Level 0 (green frames). The reserved portion is calculated as (100 - Max) %.

Frames marked with Drop Precedence Level 0 (green frames) are never dropped. The drop probability for frames increases linearly from zero (at Min average queue filling level) to Max Drop Probability or Fill Level.



Buttons

Apply : Click to save changes.

Refresh : Click to manually refresh the page immediately.

7. Spanning Tree

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

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

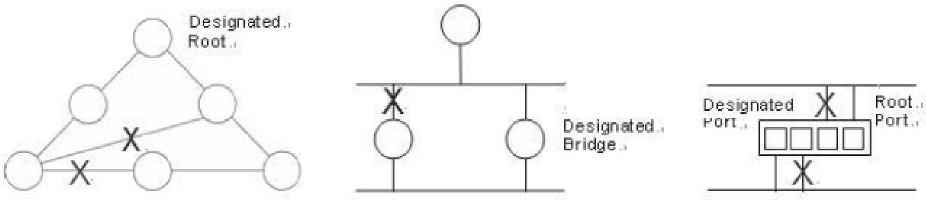


Figure 7: The Spanning Tree Protocol

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

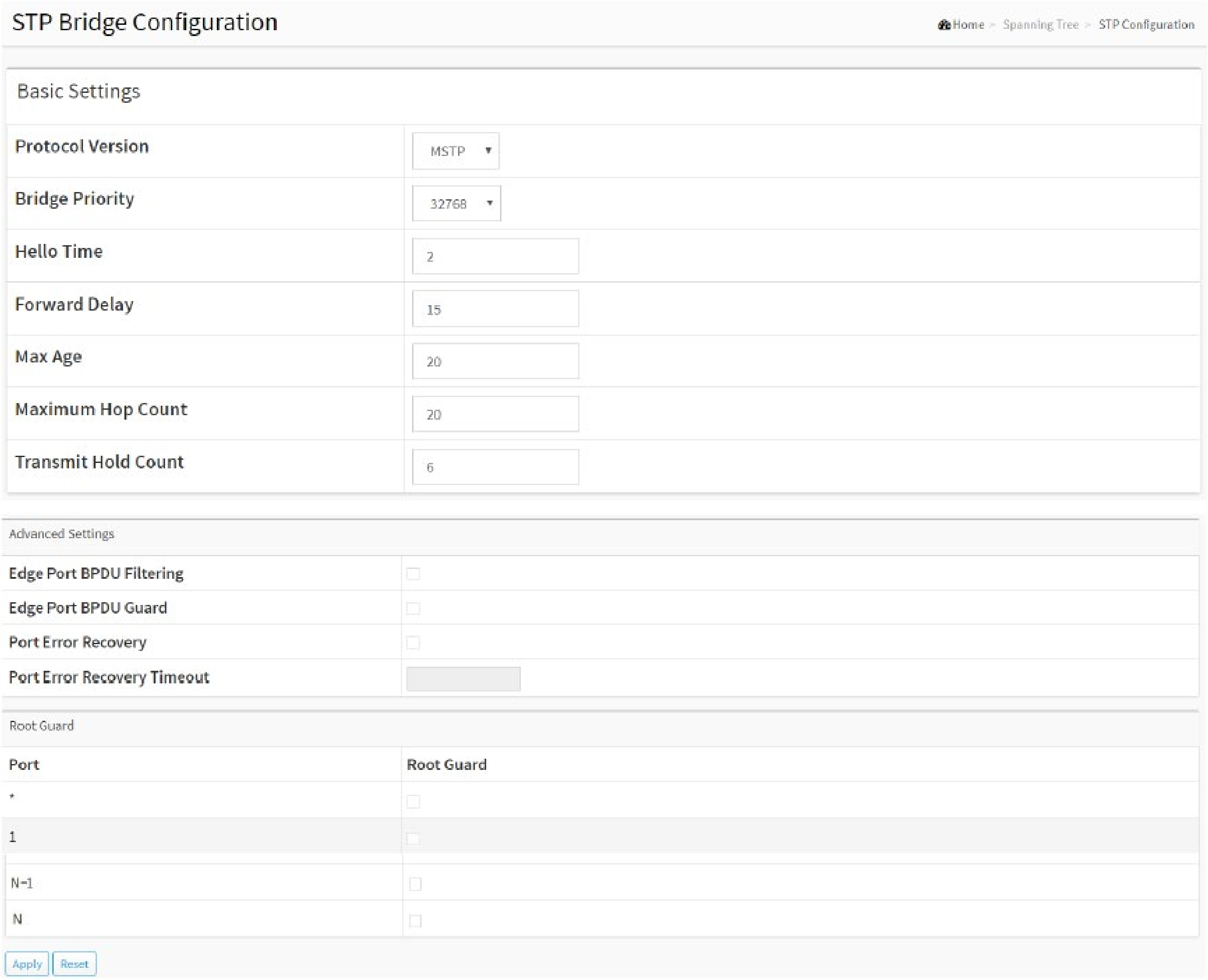
STP Configuration

This page lets you enable or disable spanning tree protocol and select which protocol version you want.

Web Interface

To configure Spanning Tree Protocol settings in the web UI:

1. Click Spanning Tree and STP Configuration.
2. Select parameters and enter parameters in blank field in Basic Settings.
3. Enable or disable the parameters and enter parameters in blank fields in Advanced settings.
4. Click the Apply button to save the settings.
5. To cancel the settings, click the Reset button. It will revert to previously saved values.



STP Bridge Configuration

Basic Settings

Protocol Version	MSTP ▾
Bridge Priority	32768 ▾
Hello Time	2
Forward Delay	15
Max Age	20
Maximum Hop Count	20
Transmit Hold Count	6

Advanced Settings

Edge Port BPDU Filtering	□
Edge Port BPDU Guard	□
Port Error Recovery	□
Port Error Recovery Timeout	

Root Guard

Port	Root Guard
*	□
1	□
N-1	□
N	□

7-1: STP Bridge Configuration

Parameter descriptions:

Basic Settings

Protocol Version : The MSTP / RSTP / STP protocol version setting. Valid values are STP, RSTP and MSTP.

Bridge Priority : Controls the bridge priority. Lower numeric values have better priority. The bridge priority plus the MSTI instance number, concatenated with the 6-byte MAC address of the switch forms a Bridge Identifier. For MSTP operation, this is the priority of the CIST. Otherwise, this is the priority of the STP/RSTP Bridge.

Hello Time : The interval between sending STP BPDUs. Valid values are 1 - 10 seconds, default is 2 seconds. **Note**: Changing this parameter from the default value is not recommended and may have adverse effects on your network.

Forward Delay : The delay used by STP Bridges to transit Root and Designated Ports to Forwarding (used in STP compatible mode). Valid values are in the range 4 to 30 seconds.

Max Age : The maximum age of the information transmitted by the Bridge when it is the Root Bridge. Valid values are in the range 6 to 40 seconds, and MaxAge must be <= (FwdDelay-1)*2.

Maximum Hop Count : This defines the initial value of remaining Hops for MSTI information generated at the boundary of an MSTI region. It defines how many bridges a root bridge can distribute its BPDU information to. Valid values are in the range 6 to 40 hops.

Transmit Hold Count : The number of BPDUs a bridge port can send per second. When exceeded, transmission of the next BPDU will be delayed. Valid values are in the range 1 to 10 BPDUs per second.

Advanced Settings

Edge Port BPDU Filtering : Control whether a port explicitly configured as Edge will transmit and receive BPDUs.

Edge Port BPDU Guard : Control whether a port explicitly configured as Edge will disable itself upon reception of a BPDU. The port will enter the error-disabled state and will be removed from the active topology.

Port Error Recovery : Control whether a port in the error-disabled state automatically will be enabled after a certain time. If recovery is not enabled, ports have to be disabled and re-enabled for normal STP operation. The condition is also cleared by a system reboot.

Port Error Recovery Timeout : The time to pass before a port in the error-disabled state can be enabled. Valid values are 30 - 86400 seconds (24 hours).

Root Guard : For each port, check or uncheck the Root Guard checkbox. The default is unchecked. Root guard is an STP feature that is enabled on a port-by-port basis. It prevents a configured port from becoming a root port. Root guard prevents a downstream switch (often misconfigured or rogue) from becoming a root bridge in a topology. Enable root guard on all ports on which the root bridge should not appear.

Buttons

Apply : Click to save changes.

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

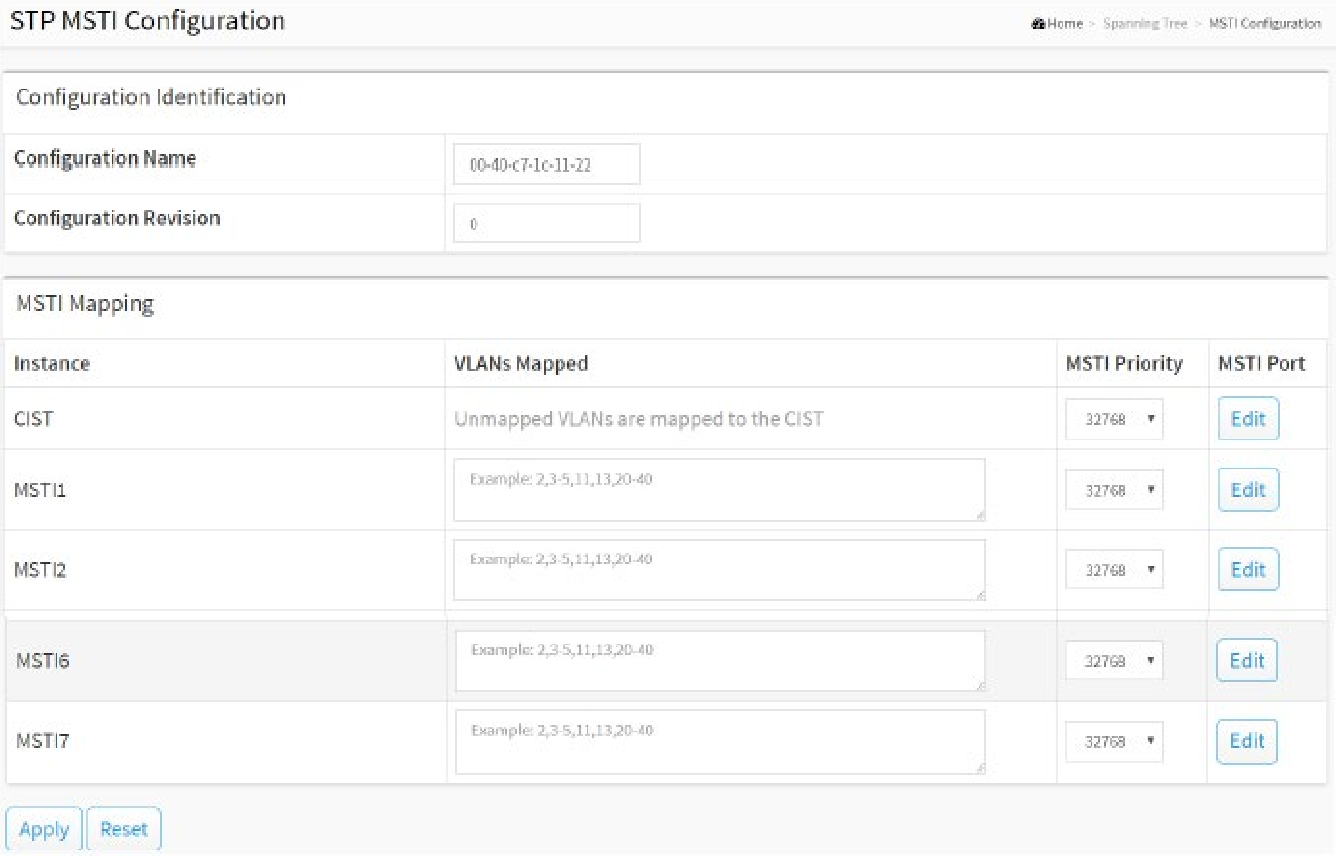
MSTI Configuration

This page lets you set and view current STP MSTI bridge instance priority parameters.

When you implement a Spanning Tree protocol on the switch that is the bridge instance. The CIST is not available for explicit mapping, as it will receive the VLANs not explicitly mapped. Due to the reason that you need to set the list of VLANs mapped to the MSTI. The VLANs must be separated with comma and/or space. A VLAN can only be mapped to one MSTI. An unused MSTI should just be left empty (i.e., not having any VLANs mapped to it).

To configure Spanning Tree MSTI in the web UI:

1. Click Spanning Tree and MSTI Configuration.
2. Specify the configuration identification parameters in the field. Specify the VLANs Mapped blank field.
3. Click the Apply button to save the settings.
4. To cancel the settings, click the Reset button. It will revert to previously saved values.
5. Click Edit to set STP CIST Port Configuration parameters.



STP MSTI Configuration

Configuration Identification

Configuration Name	00-40-c7-1c-11-22
Configuration Revision	0

MSTI Mapping

Instance	VLANs Mapped	MSTI Priority	MSTI Port
CIST	Unmapped VLANs are mapped to the CIST	32768 ▾	Edit
MSTI1	Example: 2,3-5,11,13,20-40	32768 ▾	Edit
MSTI2	Example: 2,3-5,11,13,20-40	32768 ▾	Edit
MSTI6	Example: 2,3-5,11,13,20-40	32768 ▾	Edit
MSTI7	Example: 2,3-5,11,13,20-40	32768 ▾	Edit

Figure 7-2: The MSTI Configuration

Parameter descriptions:

Configuration Identification

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

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

MSTI Mapping

Instance : The bridge instance. The CIST is not available for explicit mapping, as it will receive the VLANs not explicitly mapped.

VLANs Mapped : The list of VLANs mapped to the MSTI. The VLANs can be given as a single (xx, xx being between 1 and 4094) VLAN, or a range (xx-yy), each of which must be separated with comma and/or space. A VLAN can only be mapped to one MSTI. An unused MSTI should just be left empty. (I.e. not having any VLANs mapped to it.) Example: 2,5,20-40.

MSTI Priority : Controls the bridge priority. Lower numeric values have better priority. The bridge priority plus the MSTI instance number, concatenated with the 6-byte MAC address of the switch forms a Bridge Identifier.

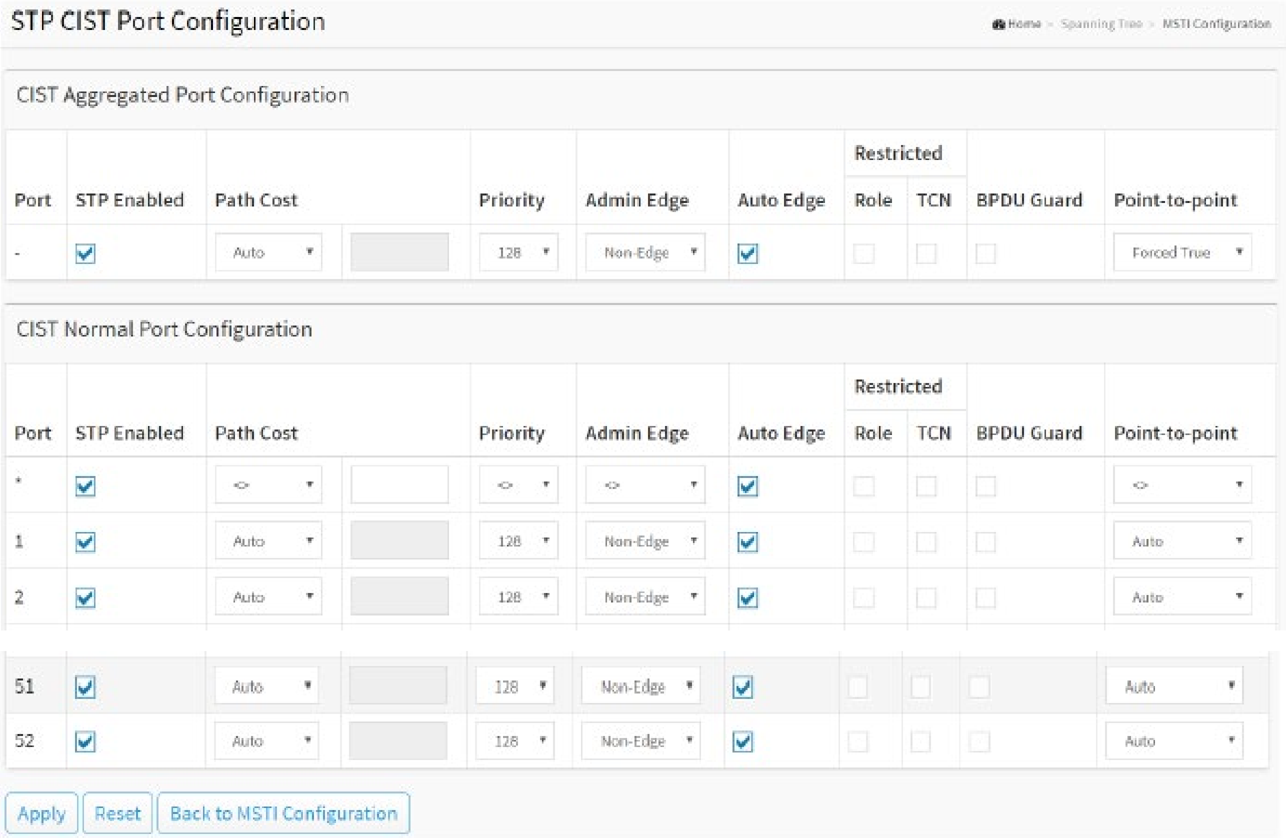
MSTI Port : This column displays the Edit button (see below).

Buttons

Apply : Click to save changes.

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

Edit : In the MSTI Port column, click the Edit button to display the STP CIST Port Configuration as shown and described below.



STP CIST Port Configuration

CIST Aggregated Port Configuration

							Restricted			
Port	STP Enabled	Path Cost		Priority	Admin Edge	Auto Edge	Role	TCN	BPDU Guard	Point-to-point
-	☑	Auto ▾		128 ▾	Non-Edge ▾	☑	□	□	□	Forced True ▾

CIST Normal Port Configuration

							Restricted			
Port	STP Enabled	Path Cost		Priority	Admin Edge	Auto Edge	Role	TCN	BPDU Guard	Point-to-point
*	☑	<> ▾		<> ▾	<> ▾	☑	□	□	□	<> ▾
1	☑	Auto ▾		128 ▾	Non-Edge ▾	☑	□	□	□	Auto ▾
2	☑	Auto ▾		128 ▾	Non-Edge ▾	☑	□	□	□	Auto ▾
51	☑	Auto ▾		128 ▾	Non-Edge ▾	☑	□	□	□	Auto ▾
52	☑	Auto ▾		128 ▾	Non-Edge ▾	☑	□	□	□	Auto ▾

Figure 7-2: STP CIST Port Configuration

Parameter descriptions:

Port : The switch port number of the logical STP port.

STP Enabled : Controls whether STP is enabled on this switch port. This field will be read only if Voice VLAN feature is enabled. The Voice VLAN port mode will be read only if this field be Enabled.

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

Priority : Controls the port priority. This can be used to control priority of ports having identical port cost. (See above).

AdminEdge : Controls whether the operEdge flag should start as set or cleared. (The initial operEdge state when a port is initialized.)

AutoEdge : Controls whether the bridge should enable automatic edge detection on the bridge port. This allows operEdge to be derived from whether BPDUs are received on the port or not.

Restricted Role : If enabled, causes the port not to be selected as Root Port for the CIST or any MSTI, even if it has the best spanning tree priority vector. Such a port will be selected as an Alternate Port after the Root Port has been selected. If set, it can cause lack of spanning tree connectivity. It can be set by a network administrator to prevent bridges external to a core region of the network influence the spanning tree active topology, possibly because those bridges are not under the full control of the administrator. This feature is also called Root Guard.

Restricted TCN : If enabled, causes the port not to propagate received topology change notifications and topology changes to other ports. If set it can cause temporary loss of connectivity after changes in a spanning tree's active topology as a result of persistently incorrect learned station location information. It is set by a network administrator to prevent bridges external to a core region of the network, causing address flushing in that region, possibly because those bridges are not under the full control of the administrator or the physical link state of the attached LANs transits frequently.

BPDU Guard : If enabled, causes the port to disable itself upon receiving valid BPDUs. Contrary to the similar bridge setting, the port Edge status does not affect this setting. A port entering error-disabled state due to this setting is subject to the bridge Port Error Recovery setting as well.

Point to Point : Controls whether the port connects to a point-to-point LAN rather than to a shared medium. This can be automatically determined or forced either true or false. Transition to the forwarding state is faster for point-to-point LANs than for shared media.

Buttons

Apply : Click to save changes.

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

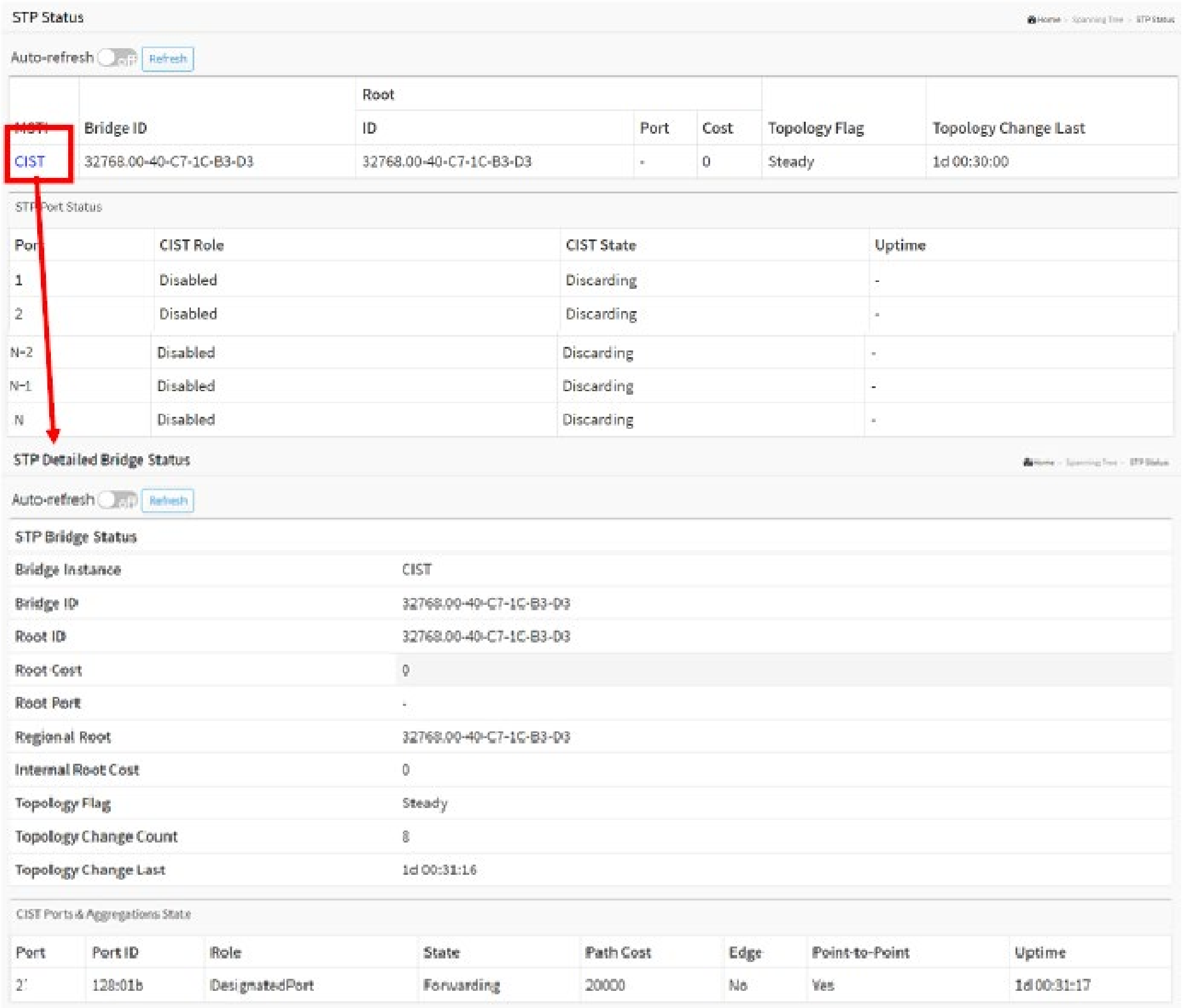
STP Status

This page provides a status overview of all STP bridge instances. The displayed table contains a row for each STP bridge instance.

Web Interface

To display STP Bridges status in the web UI:

1. Click Spanning Tree and STP Status.
2. To automatically refresh the page, click “Auto-refresh” or Click “Refresh” to manually refresh the page immediately.
3. Click “CIST“ to go to the next page “STP Detailed Bridge Status”.


Home > Spanning Tree > STP Status
Auto-refresh
off
Refresh

STP Status

MSTI	Bridge ID	Root			Topology Flag	Topology Change Last
		ID	Port	Cost		
CIST	32768.00-40-C7-1C-B3-D3	32768.00-40-C7-1C-B3-D3	-	0	Steady	1d 00:30:00

STP Port Status

Port	CIST Role	CIST State	Uptime
1	Disabled	Discarding	-
2	Disabled	Discarding	-
N-2	Disabled	Discarding	-
N-1	Disabled	Discarding	-
N	Disabled	Discarding	-

STP Detailed Bridge Status

Home > Spanning Tree > STP Status
Auto-refresh
off
Refresh

STP Bridge Status	
Bridge Instance	CIST
Bridge ID	32768.00-40-C7-1C-B3-D3
Root ID	32768.00-40-C7-1C-B3-D3
Root Cost	0
Root Port	-
Regional Root	32768.00-40-C7-1C-B3-D3
Internal Root Cost	0
Topology Flag	Steady
Topology Change Count	8
Topology Change Last	1d 00:31:16

CIST Ports & Aggregations State

Port	Port ID	Role	State	Path Cost	Edge	Point-to-Point	Uptime
2	128:01b	DesignatedPort	Forwarding	20000	No	Yes	1d 00:31:17

Figure 7-3: STP Status

Parameter descriptions:

MSTI : The Bridge Instance. This is also a link to the STP Detailed Bridge Status webpage.

Bridge ID : The Bridge ID of this Bridge instance.

Root ID : The Bridge ID of the currently elected root bridge.

Root Port : The switch port currently assigned the root port role.

Root Cost : Root Path Cost. For the Root Bridge it is zero. For all other Bridges, it is the sum of the Port Path Costs on the least cost path to the Root Bridge.

Topology Flag : The current state of the Topology Change Flag of this Bridge instance.

Topology Change Last : The time since last Topology Change occurred.

STP Port Status

Port : The switch port number of the logical STP port.

CIST Role : The current STP port role of the CIST port. The port role can be one of these values: AlternatePort, Backup Port, RootPort, DesignatedPort, or Disabled.

CIST State : The current STP port state of the CIST port. The port state can be one of these values: Blocking, Learning, or Forwarding.

Uptime : The time since the bridge port was last initialized.

CIST : Click to next page "STP Detailed Bridge Status".

STP Bridge Status

Bridge Instance : The Bridge instance (e.g., CIST, MST1, etc.).

Bridge ID : The Bridge ID of this Bridge instance.

Root ID : The Bridge ID of the currently elected root bridge.

Root Port : The switch port currently assigned the root port role.

Root Cost : Root Path Cost. For the Root Bridge this is zero. For all other Bridges, it is the sum of the Port Path Costs on the least cost path to the Root Bridge.

Regional Root : The Bridge ID of the currently elected regional root bridge, inside the MSTP region of this bridge. (*For the CIST instance only*).

Internal Root Cost : The Regional Root Path Cost. For the Regional Root Bridge this is zero. For all other CIST instances in the same MSTP region, it is the sum of the Internal Port Path Costs on the least cost path to the Internal Root Bridge. (For the CIST instance only.)

Topology Flag : The current state of the Topology Change Flag of this Bridge instance.

Topology Change Count : The number of times where the topology change flag has been set (during a one-second interval).

Topology Change Last : The time passed since the Topology Flag was last set.

CIST Ports & Aggregations State

Port : The switch port number of the logical STP port.

Port ID : The port id as used by the STP protocol. This is the priority part and the logical port index of the bridge port.

Role : The current STP port role. The port role can be one of these values: AlternatePort, BackupPort, RootPort, or DesignatedPort.

State : The current STP port state. The port state can be one of these values: Discarding, Learning , or Forwarding.

Path Cost : The current STP port path cost. This will either be a value computed from the Auto setting, or any explicitly configured value.

Edge : The current STP port (operational) Edge Flag. An Edge Port is a switch port to which no Bridges are attached. The flag may be automatically computed or explicitly configured. Each Edge Port transits directly to the Forwarding Port State, since there is no possibility of it participating in a loop.

Point-to-Point : The current STP port point-to-point flag. A point-to-point port connects to a non-shared LAN media. The flag may be automatically computed or explicitly configured. The point-to-point properties of a port affect how fast it can transit to STP state.

Uptime : The time since the bridge port was last initialized.

Buttons

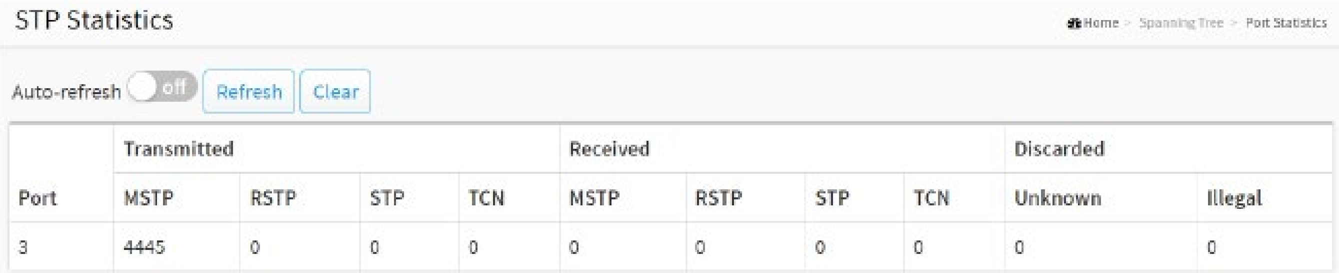
Auto-refresh : Check this box to refresh the page automatically every 3 seconds.

Refresh : Click to manually refresh the page immediately.

Port Statistics

This page displays the STP port statistics counters of bridge ports in the switch. To display STP Port Statistics in the web UI:

1. Click Spanning Tree and Port Statistics.
2. To automatically refresh the page check "Auto-refresh".
3. Click "Refresh" to refresh the STP Bridges.



Port	Transmitted				Received				Discarded	
	MSTP	RSTP	STP	TCN	MSTP	RSTP	STP	TCN	Unknown	Illegal
3	4445	0	0	0	0	0	0	0	0	0

Figure 7-4: STP Port Statistics

Parameter descriptions:

Port : The switch port number of the logical STP port.

MSTP : The number of MSTP Configuration BPDUs received/transmitted on the port.

RSTP : The number of RSTP Configuration BPDUs received/transmitted on the port.

STP : The number of legacy STP Configuration BPDUs received/transmitted on the port.

TCN : The number of (legacy) Topology Change Notification BPDUs received/transmitted on the port.

Discarded Unknown : The number of unknown Spanning Tree BPDUs received (and discarded) on the port.

Discarded Illegal : The number of illegal Spanning Tree BPDUs received (and discarded) on the port.

Buttons

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

Refresh : Click to manually refresh the page immediately.

8. MAC Address Tables

Configuration

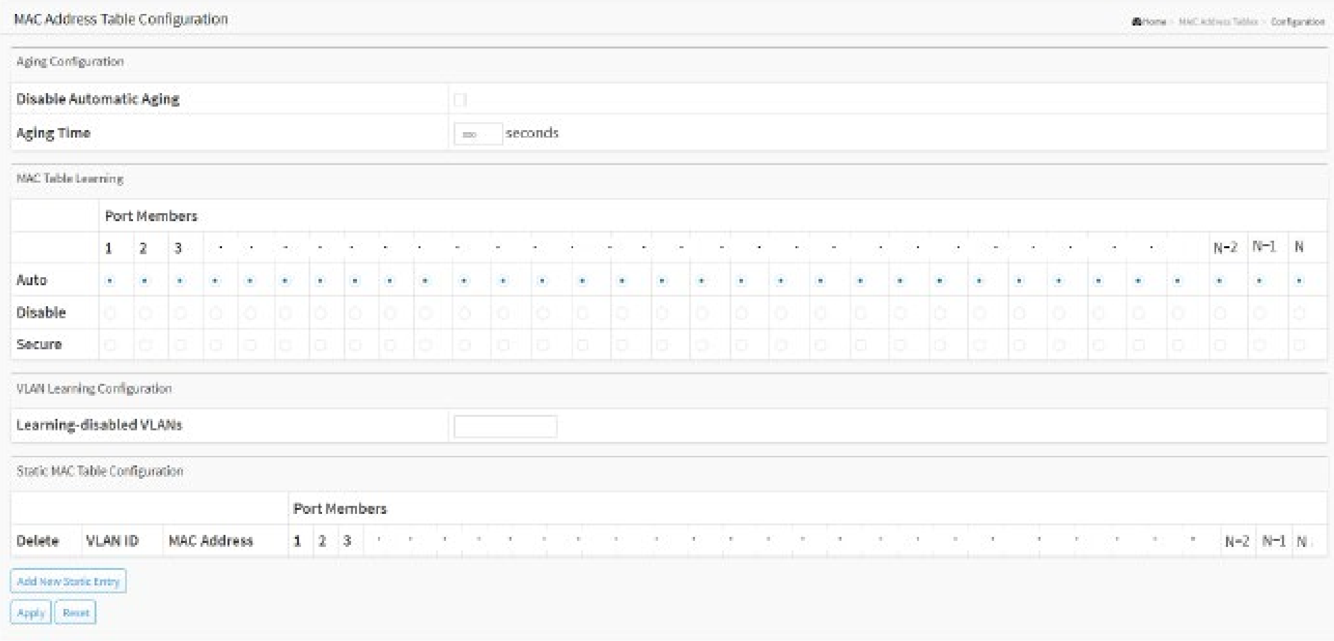
Switching of frames is based on the DMAC address contained in the frame. The switch builds up a table that maps MAC addresses to switch ports for knowing which ports the frames should go to (based on the DMAC address in the frame). This table contains both static and dynamic entries. The static entries are configured by the network administrator if the administrator wants to do a fixed mapping between the DMAC address and switch ports.

The frames also contain a MAC address (SMAC address), which shows the MAC address of the equipment sending the frame. The SMAC address is used by the switch to automatically update the MAC table with these dynamic MAC addresses. Dynamic entries are removed from the MAC table if no frame with the corresponding SMAC address have been seen after a configurable age time.

Web Interface

To configure MAC Address Table parameters in the web UI:

1. Click MAC Address Tables and Configuration.
2. Specify the Disable Automatic Aging and Aging Time.
3. Specify the Port Members (Auto, Disable, Secure).
4. Specify the Learning-disabled VLANs.
5. Click the Add New Static Entry button and specify the VLAN ID, Mac Address, and Port Members.
6. Click Apply.



MAC Address Table Configuration

Aging Configuration

Disable Automatic Aging	□
Aging Time	300 seconds

MAC Table Learning

	Port Members						
	1	2	3	·	N-2	N-1	N
Auto	●	●	●	●	●	●	●
Disable	○	○	○	○	○	○	○
Secure	□	□	□	□	□	□	□

VLAN Learning Configuration

Learning-disabled VLANs	

Static MAC Table Configuration

			Port Members						
Delete	VLAN ID	MAC Address	1	2	3	·	N-2	N-1	N

Figure 8-1: MAC Address Table Configuration

Parameter descriptions:

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. The valid range is 10 to 1000000 seconds. Disable the automatic aging of dynamic entries by checking the “Disable Automatic Aging” box.

MAC Table Learning : If the learning mode for a given port is greyed out, another module is in control of the mode, so that it cannot be changed by the user. An example of such a module is the MAC-Based Authentication under 802.1X. Each port can do learning based on the following settings:

Auto : Learning is done automatically as soon as a frame with unknown SMAC is received.

Disable : No learning is done.

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

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

VLAN Learning Configuration

Learning-disabled VLANS : This field shows the Learning-disabled VLANs. When a NEW MAC arrives into a learning disabled VLAN, the MAC won't be learned. By the default, the field is empty. More VLANs may be created by using a list syntax where the individual elements are separated by commas. Ranges are specified with a dash separating the lower and upper bound. The following example will create VLANs 1, 10, 11, 12, 13, 200, and 300: 1,10-13,200,300. Spaces are allowed in between the delimiters.

Static MAC Table Configuration : The static entries in the MAC table are shown in this table. The static MAC table can contain up to128 entries.

VLAN ID : The VLAN ID of the entry.

MAC Address : The MAC address of the entry.

Port Members : Checkmarks indicate which ports are members of the entry. Check or uncheck as needed to modify the entry.

Buttons

Add New Static Entry : Click to add a new entry to the static MAC table. Specify the VLAN ID, MAC address, and port members for the new entry. Click "Apply".

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

Apply : Click to save changes.

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

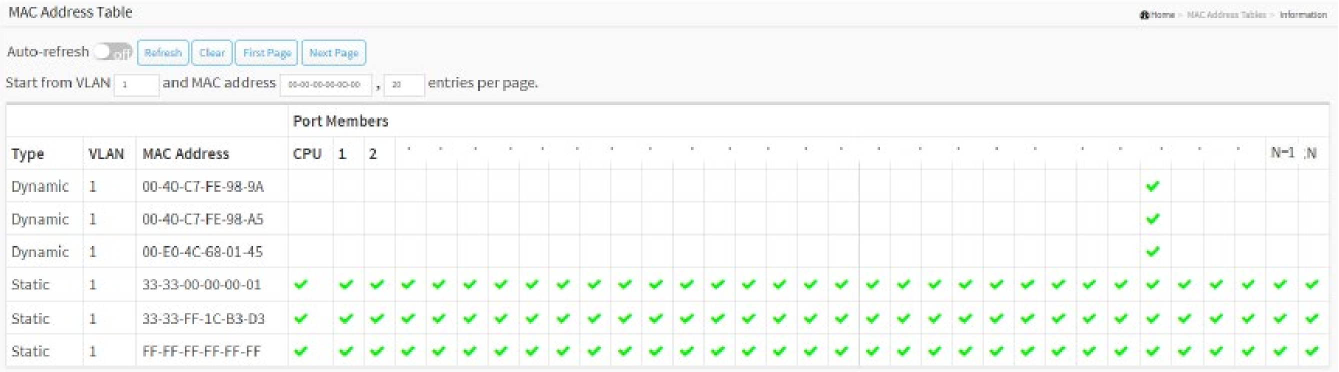
Information

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. Each page shows up to 999 entries from the MAC table, selected via 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.

To display the MAC Address Table in the web UI:

1. Click MAC Address Table and Information.

2. To auto-refresh click “Auto-refresh” or click “Refresh” to refresh the MAC Address Table immediately.



MAC Address Table

Start from VLAN 1 and MAC address 00-00-00-00-00-00 , 20 entries per page.

			Port Members																																
Type	VLAN	MAC Address	CPU	1	2	.	.	.	.	.	.		.	.	.	.		.	.	.	.		.	.	.	.		.	.	.	.	.		N-1	N
Dynamic	1	00-40-C7-FE-98-9A																											✓						
Dynamic	1	00-40-C7-FE-98-A5																											✓						
Dynamic	1	00-E0-4C-68-01-45																											✓						
Static	1	33-33-00-00-00-01	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Static	1	33-33-FF-1C-B3-D3	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Static	1	FF-FF-FF-FF-FF-FF	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓

Figure 8-2: MAC Address Table

Parameter descriptions:

Type : Indicates whether the entry is a static entry, dynamic entry, 802.1x, or DMS entry.

VLAN : The VLAN ID of the entry.

MAC Address : The MAC address of the entry.

Port Members : The ports that are members of the entry.

Buttons

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

Refresh : Click to manually refresh the page immediately.

Clear : Click to clear the page.

First Page : Updates the table starting from the first entry in the MAC Table, i.e. the entry with the lowest VLAN ID and MAC address.

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

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.

9. Multicast

IGMP Snooping

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

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

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

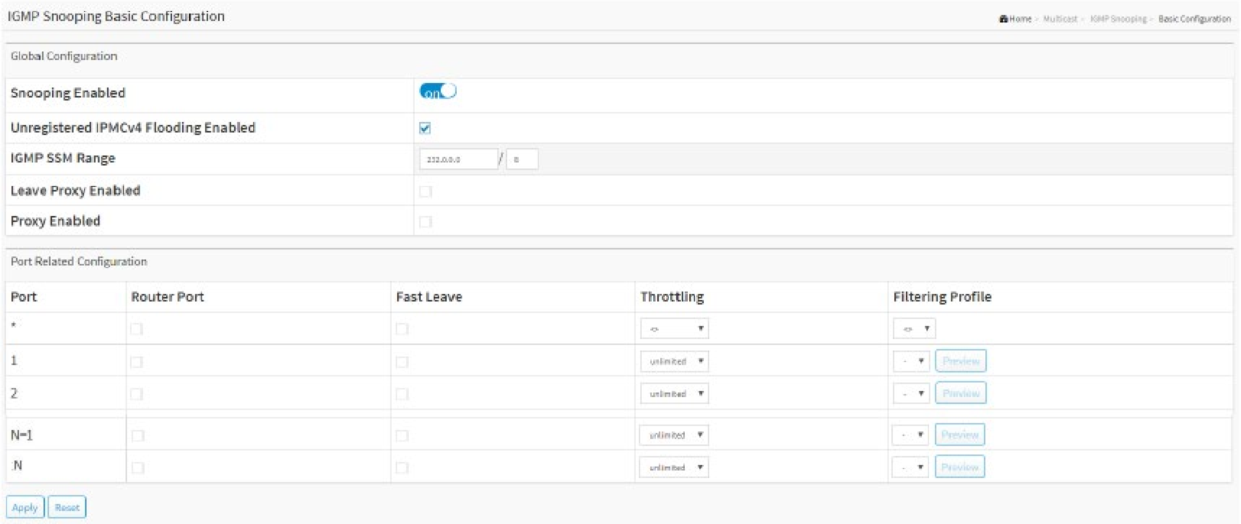
Basic Configuration

This page lets you set basic IGMP snooping on the switch, which connects to a router closer to the root of the tree. This interface is the upstream interface. The router on the upstream interface must be running IGMP

Web Interface

To configure IGMP Snooping parameters in the web UI:

1. Click Multicast, IGMP Snooping, and Basic Configuration.
2. Set the IGMP Snooping Global Configuration parameters.
3. Set the Port Related Configuration parameters.
4. Click the Apply button to save the settings or to cancel the settings click the Reset button.



IGMP Snooping Basic Configuration

Global Configuration

Snooping Enabled	on
Unregistered IPMCv4 Flooding Enabled	☑
IGMP SSM Range	232.0.0.0 / 8
Leave Proxy Enabled	□
Proxy Enabled	□

Port Related Configuration

Port	Router Port	Fast Leave	Throttling	Filtering Profile
*	□	□	<>	<>
1	□	□	unlimited	- Preview
2	□	□	unlimited	- Preview
N-1	□	□	unlimited	- Preview
N	□	□	unlimited	- Preview

Figure 9-1.1: IGMP Snooping Basic Configuration

Parameter descriptions:

Global Configuration

Snooping Enabled : Enable the Global IGMP Snooping.

Unregistered IPMCv4 Flooding Enabled : Enable unregistered IPMCv4 traffic flooding. Unregistered IPMCv4 traffic is so-called unknown multicast. After selected, the unregistered multicast stream will be forwarded like normal packets. Once you un-selected it, such stream will be discarded

IGMP SSM Range : The SSM (Source-Specific Multicast) Range allows the SSM-aware hosts and routers run the SSM service model for the groups in the address range. Format: (IP address/ sub mask)

Leave Proxy Enabled : Enable IGMP Leave Proxy. This feature can be used to avoid forwarding unnecessary leave messages to the router side.

Proxy Enabled : Enable IGMP Proxy. This feature can be used to avoid forwarding unnecessary join and leave messages to the router side.

Port Related Configuration

Port : Shows the physical Port index of switch.

Router Port : Specify which ports act as router ports. A router port is a port on the Ethernet switch that leads towards the Layer 3 multicast device or IGMP querier. If an aggregation member port is selected as a router port, the whole aggregation will act as a router port.

Fast Leave : Enable the fast leave on the port.

Throttling : Enable to limit the number of multicast groups to which a switch port can belong.

Profile : Select the profile for this port. Click to preview the page which list the rules associated with the selected profile.

Buttons

Apply : Click to save changes.

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

VLAN Configuration

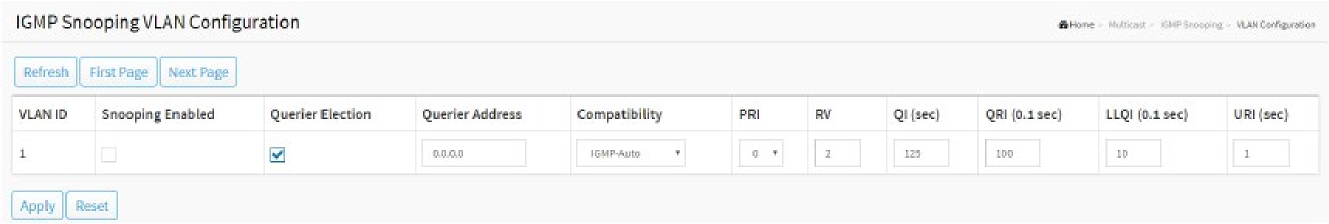
This page lets you enable and configure up to 64 VLANs for per-VLAN IGMP Snooping.

Each page shows 20 entries from the VLAN table. When first visited, the web page will show the first 20 entries from the beginning of the VLAN Table. Clicking the Refresh button will update the displayed table starting from that or the next closest VLAN Table match. The Next Page will use the last entry of the currently displayed entry as a basis for the next lookup. When the end is reached the text "No more entries" is shown in the displayed table. Use the First Page button to start over.

Web Interface

To configure IGMP Snooping VLAN in the web UI:

1. Click Multicast, IGMP Snooping, and VLAN Configuration.
2. Configure the parameters and click the Apply button to save the settings
3. To cancel the settings, click the Reset button. It will revert to previously saved values.
4. To add a VLAN, click System > IP Address > Advanced Settings and click the Add Interface button.



IGMP Snooping VLAN Configuration

VLAN ID	Snooping Enabled	Querier Election	Querier Address	Compatibility	PRI	RV	QI (sec)	QRI (0.1 sec)	LLQI (0.1 sec)	URI (sec)
1	□	☑	0.0.0.0	IGMP-Auto	0	2	125	100	10	1

Figure 9-1.2: IGMP Snooping VLAN Configuration

Parameter descriptions:

VLAN ID : The VLAN ID of the entry

IGMP Snooping Enabled : Enable the per-VLAN IGMP Snooping. Up to 64 VLANs can be selected for IGMP Snooping.

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

Querier Address : Define the IPv4 address as source address used in IP header for IGMP Querier election. When the Querier 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 switch uses a pre-defined value. By default, this value will be 0.0.0.0.

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 selections are IGMP-Auto, Forced IGMPv1, Forced IGMPv2, and Forced IGMPv3. The default compatibility value is IGMP-Auto.

Rv : Robustness Variable. The RV allows tuning for the expected packet loss on a network. The valid range is 1 to 255; the default RV value is 2.

QI (sec) : Query Interval. The QI is the interval between General Queries sent by the Querier. The valid range is 1 to 31744 seconds; the default QI 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 valid range is 0 to 31744 in tenths of seconds; the default QRI interval is 100 in tenths of seconds (10 seconds).

LLQI (0.1 sec) : Last Member Query Interval. The LLQI is the time value represented by the Last Member Query Interval, multiplied by the Last Member Query Count. The valid range is 0 to 31744 in tenths of seconds; the default LLQI is 10 in tenths of seconds (1 second).

URI (sec) : Unsolicited Report Interval. The URI is the time between repetitions of a host's initial report of membership in a group. The valid range is 0 to 31744 seconds; the default URI is 1 second.

Buttons

Apply : Click to save changes.

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

Refresh : Refreshes the displayed table starting from the "VLAN" input fields.

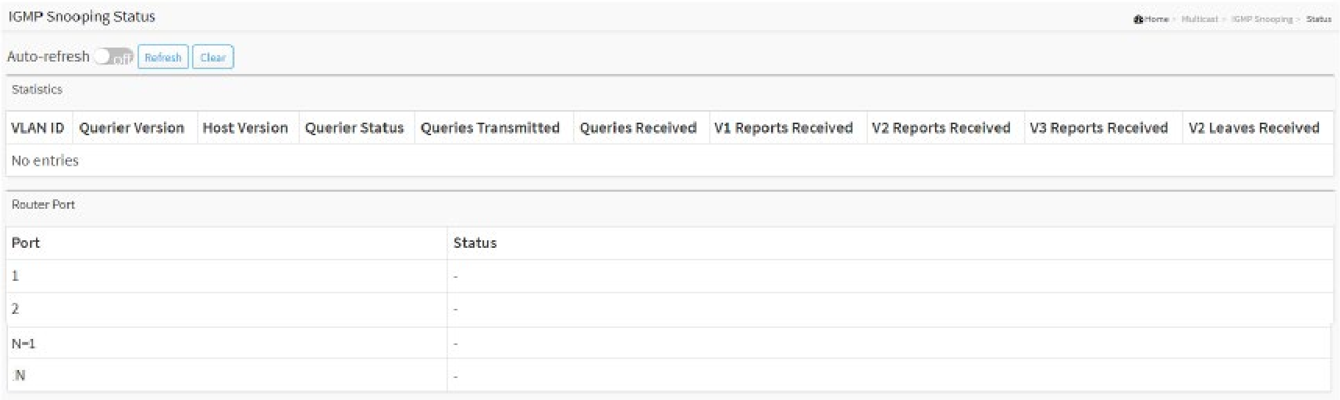
First Page : Updates the table starting from the first entry in the VLAN Table, i.e. the entry with the lowest VLAN ID.

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

Status

This page displays IGMP Snooping Status parameters. To display IGMP Snooping status in the web UI:

1. Click Multicast, IGMP Snooping, and Status.
2. To auto-refresh the information click "Auto-refresh".
3. Click "Refresh" to refresh the IGMP Snooping Status.



Statistics

VLAN ID	Querier Version	Host Version	Querier Status	Queries Transmitted	Queries Received	V1 Reports Received	V2 Reports Received	V3 Reports Received	V2 Leaves Received
No entries									

Router Port

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

Figure 9-1.3: IGMP Snooping Status

Parameter descriptions:

Statistics

VLAN ID : The VLAN ID of the entry.

Querier Version : Working Querier Version currently.

Host Version : Working Host Version currently.

Querier Status : Shows the Querier status as "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 : Displays which ports act as router ports. A router port is a port on the Ethernet switch that leads towards the Layer 3 multicast device or IGMP querier. ***Static*** denotes the specific port is configured to be a router port. ***Dynamic*** denotes the specific port is learnt to be a router port. ***Both*** denote the specific port is configured or learnt to be a router port.

Port : The 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 every 3 seconds.

Refresh : Click to refresh the page immediately.

Clear : Click to clear the page.

Group Information

This page displays 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.

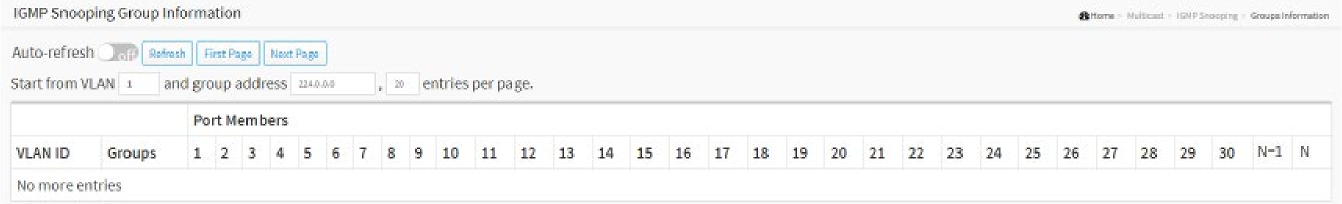
Each page shows up to 99 entries from the IGMP Group table, selected through the "entries per page" input field. When first visited, the web page will show the first 20 entries from the beginning of the IGMP Group Table.

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

Web Interface

To display the IGMP Snooping Group Information in the web UI:

1. Click Multicast, IGMP Snooping and Group Information.
2. Specify how many entries to show in one page.
3. To automatically refresh the information, click “Auto-refresh”.
4. Click “Refresh” to refresh an entry.
5. Click First Page/Next Page to change pages.



IGMP Snooping Group Information

Start from VLAN 1 and group address 224.0.0.0 , 20 entries per page.

		Port Members																															
VLAN ID	Groups	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	N-1	N
No more entries																																	

Figure 9-1.4: The IGMP Snooping Groups Information

Parameter descriptions:

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 every 3 seconds.

Refresh : Click to refresh the page immediately.

First Page : Updates the table, starting with the first entry in the IGMP Group Table.

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

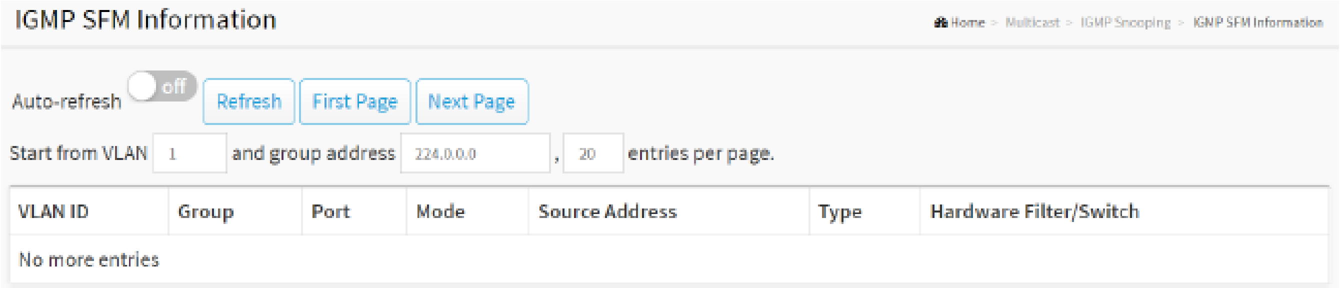
IGMP SFM Information

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 belonging to the same group are treated as a single entry.

Web Interface

To display IGMP SFM Information in the web UI:

1. Click Multicast, IGMP Snooping and IGMP SFM Information
2. To automatically refresh the information check "Auto-refresh" to "on".
3. Click "Refresh" to refresh an entry of the IGMP Snooping Groups Information.
4. Click First/Next Page to change page.



IGMP SFM Information

Home > Multicast > IGMP Snooping > IGNP SFM Information

Auto-refresh off | Refresh | First Page | Next Page

Start from VLAN 1 and group address 224.0.0.0 , 20 entries per page.

VLAN ID	Group	Port	Mode	Source Address	Type	Hardware Filter/Switch
No more entries						

Figure 9-1.5: IGMP SFM Information

Parameter descriptions:

VLAN ID : The VLAN ID of the group.

Group : The Group address of the group displayed.

Port : The 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. The system currently supports 128 IP source addresses for filtering.

Type : Indicates the Type; either ***Allow*** or ***Deny***.

Hardware Filter/Switch : Indicates whether data plane destined to the specific group address from the source IPv4 address can be handled by chip.

Buttons

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

Refresh : Click to refresh the page immediately.

First Page : Updates the table starting from the first entry in the IGMP SFM Information Table.

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

MLD Snooping

Multicast Listener Discovery (MLD) is a component of the Internet Protocol Version 6 (IPv6) suite. MLD is used by IPv6 routers for discovering multicast listeners on a directly attached link, much like Internet Group Management Protocol (IGMP) is used in IPv4. The protocol is embedded in ICMPv6 instead of using a separate protocol. MLDv1 is similar to IGMPv2 and MLDv2 is similar to IGMPv3. The protocol is described in IETF RFC 3810 which has been updated by RFC 4604.

A network node that acts as a source of IPv6 multicast traffic is only an indirect participant in MLD snooping; it just provides multicast traffic, and MLD doesn't interact with it. (Note, however, that in an application like desktop conferencing a network node may act as both a source and an MLD host; but MLD interacts with that node only in its role as an MLD host.)

A source node creates multicast traffic by sending packets to a multicast address. In IPv6, addresses with the first eight bits set (that is, "FF" as the first two characters of the address) are multicast addresses, and any node that listens to such an address will receive the traffic sent to that address. Application software running on the source and destination systems cooperates to determine what multicast address to use. (Note that this is a function of the application software, not of MLD.)

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

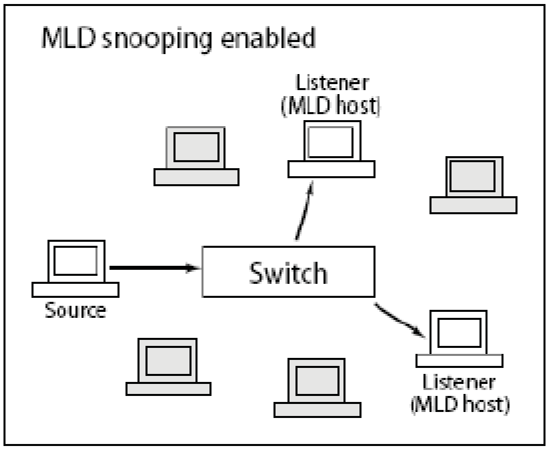
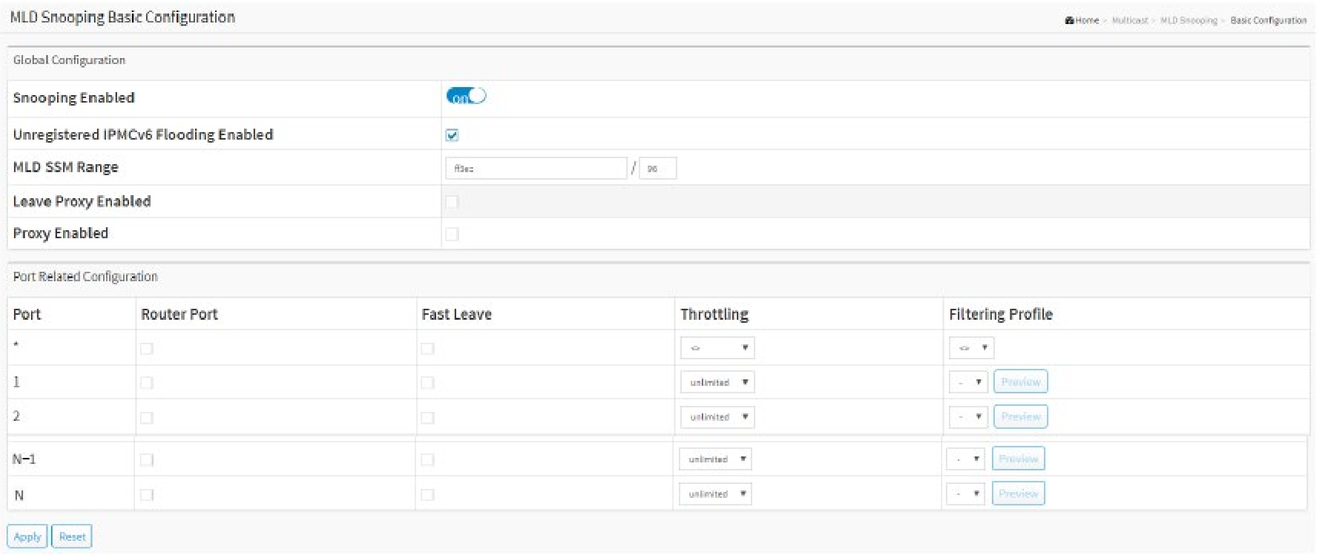


Figure 9-2: MLD snooping enabled

Web Interface

To configure MLD Snooping in the web UI:

1. Click Multicast, MLD Snooping, and Basic Configuration.
2. Set the Global Configuration parameters.
3. Set the Port Related Configuration parameters.
4. Click the Apply button to save the settings.
5. To cancel the settings, click the Reset button. It will revert to previously saved values.



MLD Snooping Basic Configuration

Global Configuration

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

Port Related Configuration

Port	Router Port	Fast Leave	Throttling	Filtering Profile
*	□	□	<>	<>
1	□	□	unlimited	- Preview
2	□	□	unlimited	- Preview
N−1	□	□	unlimited	- Preview
N	□	□	unlimited	- Preview

Figure 9-2.1: MLD Snooping Basic Configuration

Parameter descriptions :

Global Configuration

Snooping Enabled : Set to ‘on’ to enable MLD Snooping globally.

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 : The SSM (Source-Specific Multicast) Range allows the SSM-aware hosts and routers run the SSM service model for the groups in the address (using IPv6 Address) range.

Leave Proxy Enabled : Check the box to enable MLD Leave Proxy. This feature can be used to avoid forwarding unnecessary leave messages to the router side.

Proxy Enabled : Check the box to 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 : Check to enable fast leave on the port.

Throttling : Enable to limit the number of multicast groups to which a switch port can belong.

Filtering Profile : You can select profile when you edit in Multicast Filtering Profile.

Buttons

Apply : Click to save changes.

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

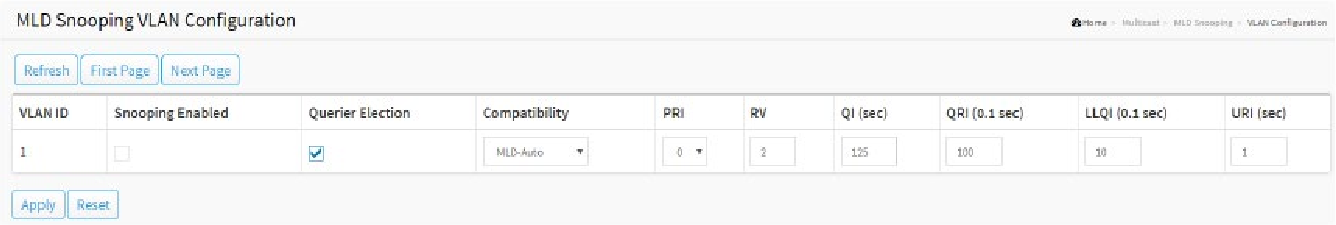
VLAN Configuration

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. The switch drops traffic for ports on the VLAN that have no MLD hosts.

Web Interface

To set MLD Snooping VLAN parameters in the web UI:

1. Click Multicast, MLD Snooping and VLAN Configuration.
2. Check or uncheck the Snooping Enabled checkbox and the Querier Election checkbox as required.
3. Select the Compatibility mode and set the PRI, RV, QI, QRI, LLQI and URI parameters.
4. Click the Apply button when done.


MLD Snooping VLAN Configuration

VLAN ID	Snooping Enabled	Querier Election	Compatibility	PRI	RV	QI (sec)	QRI (0.1 sec)	LLQI (0.1 sec)	URI (sec)
1	□	☑	MLD-Auto	0	2	125	100	10	1

Figure 9-2.2: MLD Snooping VLAN Configuration

Parameter descriptions:

VLAN ID : The VLAN ID of the entry.

Snooping Enabled : Check to enable per-VLAN MLD Snooping. Up to 64 VLANs can be selected for MLD Snooping.

Querier Election : Enable to join MLD Querier election in the VLAN. Disable to act as a MLD 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 selections are MLD-Auto, Forced IGMPv1, or Forced IGMPv2. The default compatibility value is MLD-Auto.

RV : Robustness Variable. The RV allows tuning for the expected packet loss on a network. The valid range is 1 to 255; the default RV value is 2.

QI (sec) : Query Interval. The QI is the interval between General Queries sent by the Querier. The valid range is 1 to 31744 seconds; the default QI 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 valid range is 0 to 31744 in tenths of seconds; the default QRI is 100 in tenths of a second (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 valid range is 0 to 31744 in tenths of a second; the default LLQI 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 valid URI range is 0 to 31744 seconds; the default is 1 second.

Buttons

Refresh : Refreshes the displayed table starting from the "VLAN" input fields.

First Page : Updates the table starting from the first entry in the VLAN Table (i.e., the entry with the lowest VLAN ID).

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

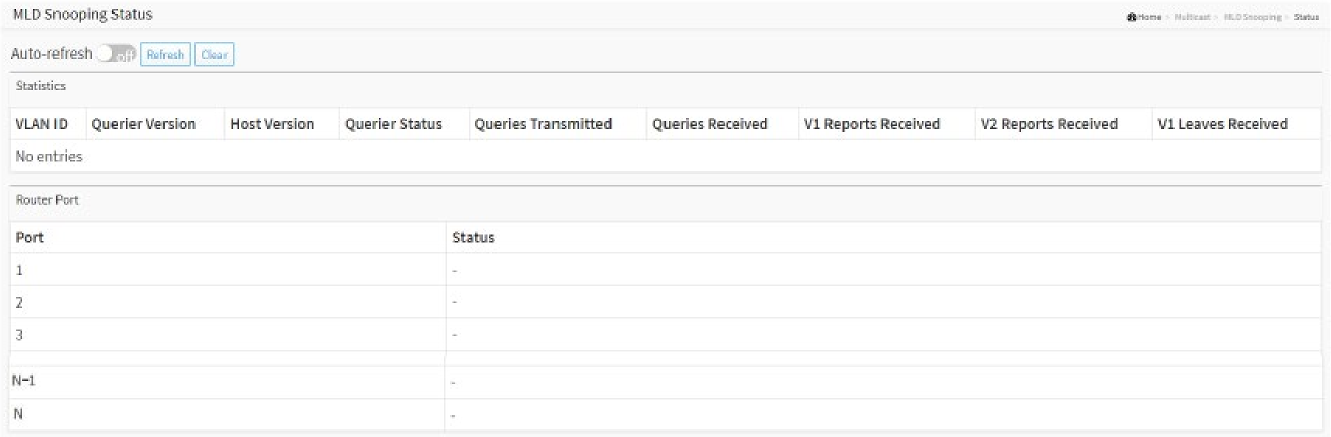
Apply : Click to save changes.

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

Status

This page displays MLD Snooping Status and Router Port details. To display MLD Snooping Status in the web UI:

1. Click Multicast, MLD Snooping, and Status.
2. To automatically refresh the information click “Auto-refresh”.
3. Click “Refresh” to refresh the page or click Clear to clear the counters.



MLD Snooping Status

Statistics

VLAN ID	Querier Version	Host Version	Querier Status	Queries Transmitted	Queries Received	V1 Reports Received	V2 Reports Received	V1 Leaves Received
No entries								

Router Port

Port	Status
1	-
2	-
3	-
N-1	-
N	-

Figure 9-2.3: MLD Snooping Status

Parameter descriptions:

Statistics

VLAN ID : Displays the VLAN ID of the entry.

Querier Version : Displays the current Working Querier Version.

Host Version : Displays the current Working Host Version.

Querier Status : Shows the Querier status as "ACTIVE" or "IDLE". The status "DISABLE" denotes the specific interface is administratively disabled.

Queries Transmitted : Displays the number of Transmitted Queries.

Queries Received : Displays the number of Received Queries.

V1 Reports Received : Displays the number of Received V1 Reports.

V2 Reports Received : Displays the number of Received V2 Reports.

V1 Leaves Received : Displays the number of Received V1 Leaves.

Router Port : Displays which ports are set as router ports. A router port is a port on the Ethernet switch that leads towards the Layer 3 multicast device or MLD querier. Static denotes the specific port is configured to be a router port. Dynamic denotes the specific port is learnt to be a router port. Both denote the specific port is configured or learnt to be a router port.

Port : Switch port number.

Status : Indicate whether specific port is a router port or not.

Buttons

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

Refresh : Click to refresh the page immediately.

Clear : Clears the counters for the selected port.

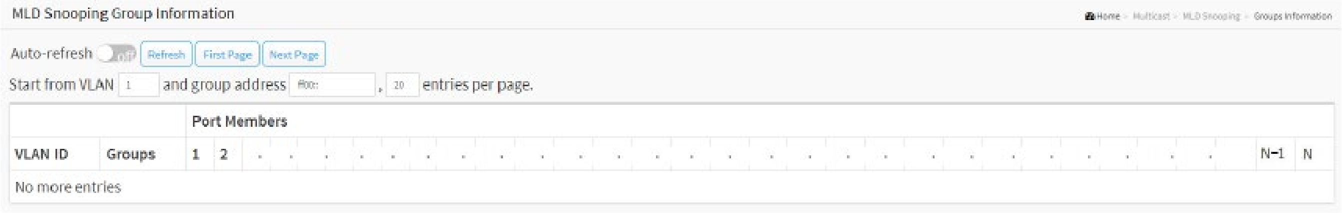
Groups Information

Entries in the MLD Snooping Group Information table are shown on this page. The MLD Group Table is sorted first by VLAN ID, and then by group.

Web Interface

To display MLD Snooping Group information in the web UI:

1. Click Multicast, MLD Snooping, and Group Information.
2. Enter a Start from VLAN, group address, and entries per page.
3. Click “Refresh” to refresh the page immediately or click “Auto-refresh” to automatically refresh the page.
4. Click First/Next Page to change page.



MLD Snooping Group Information

Start from VLAN 1 and group address ff00:: , 20 entries per page.

		Port Members																													
VLAN ID	Groups	1	2	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	N-1	N
No more entries																															

Figure 9-2.4: MLD Snooping Group Information

Parameter descriptions:

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 occurs every 3 seconds.

Refresh : Click to refresh the page immediately.

First Page : Updates the table, starting with the first entry in the MLD Group Table.

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

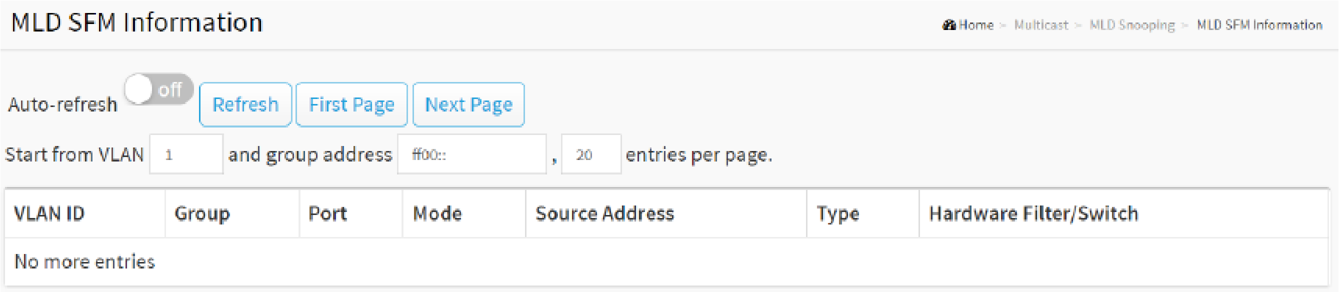
MLD SFM Information

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

Web Interface

To display the MLD SFM Information in the web UI:

1. Click Multicast, MLD Snooping, and MLD SFM Information.
2. Enter a Start from VLAN, group address, and entries per page.
3. Click "Refresh" to refresh the page immediately or click "Auto-refresh" to automatically refresh the page.
4. Click First/Next Page to change pages.



MLD SFM Information

Start from VLAN 1 and group address ff00:: , 20 entries per page.

VLAN ID	Group	Port	Mode	Source Address	Type	Hardware Filter/Switch
No more entries						

Figure 9-2.5: MLD SFM Information

Parameter descriptions:

VLAN ID : Displays the VLAN ID of the group.

Group : Displays the IP Multicast Group address.

Port : Displays the switch port number.

Mode : Displays the filtering mode maintained per (VLAN ID, port number, Group Address) basis. It can be either Include or Exclude.

Source Address : Displays the IP Address of the source. Currently, the system limits the total number of IP source addresses for filtering to be 128.

Type : Displays the Type. It can be either Allow or Deny.

Hardware Filter/Switch : Indicates whether the data plane destined to the specific group address from the source IPv6 address can be handled by the chip.

Buttons

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

Refresh : Click to refresh the page immediately.

First Page : Updates the table starting from the first entry in the MLD SFM Information Table.

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

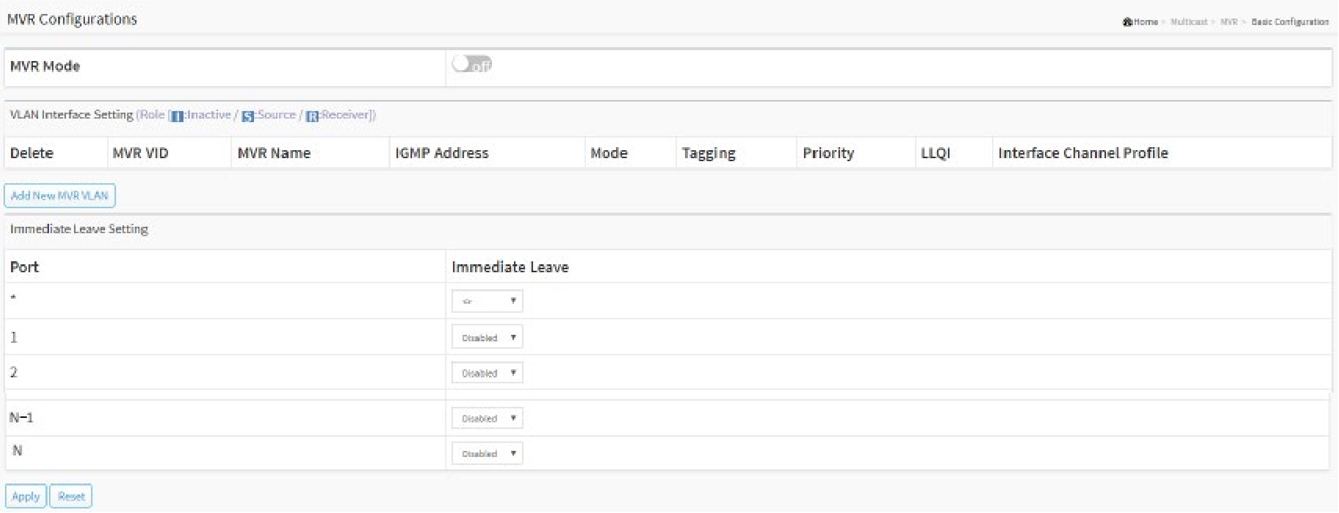
MVR

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.

Basic Configuration

To set MVR Configuration in the web UI:

1. Click Multicast, MVR, and Basic Configuration.
2. Click "Add New MVR VLAN".
3. Enable the MVR mode; the default is off (disabled).
4. Specify MVR VID, MVR Name, IGMP Address, Mode, Tagging, Priority, LLQI, Interface Channel Profile.
5. Select which port to enable Immediate Leave. The default is Disabled for all ports.
6. Click Apply to save the settings.
7. To cancel the settings click the Reset button. It will revert to previously saved values



MVR Configurations

MVR Mode	off

VLAN Interface Setting (Role [I:Inactive / S:Source / R:Receiver])

Delete	MVR VID	MVR Name	IGMP Address	Mode	Tagging	Priority	LLQI	Interface Channel Profile

Immediate Leave Setting

Port	Immediate Leave
*	<>
1	Disabled
2	Disabled
N-1	Disabled
N	Disabled

Figure 9-3.1: MVR Configuration

Parameter descriptions:

MVR Mode : Enable/Disable the Global MVR. The Unregistered Flooding control depends on the current configuration in IGMP/MLD Snooping. It is suggested to enable Unregistered Flooding control when the MVR group table is full.

MVR VID : Specify the Multicast VLAN ID.

Caution: MVR source ports are not recommended to be overlapped with management VLAN ports.

MVR Name : An optional attribute to indicate the name of the specific MVR VLAN. Maximum length of the MVR VLAN Name string is 32. MVR VLAN Name can only contain alphabets or numbers. MVR VLAN name can be edited for the existing MVR VLAN entries or it can be added to the new entries.

IGMP Address : Define the IPv4 address as source address used in IP header for IGMP control frames. The default IGMP address is not set (0.0.0.0). When the IGMP address is not set, system uses IPv4 management address of the IP interface associated with this VLAN. When the IPv4 management address is not set, system uses the first available IPv4 management address. Otherwise, system uses a pre-defined value. By default, this value will be 192.0.2.1.

Mode : Specify the MVR mode of operation. In Dynamic mode, MVR allows dynamic MVR membership reports on source ports. In Compatible mode, MVR membership reports are forbidden on source ports. The default is Dynamic mode.

Tagging : Specify whether the traversed IGMP/MLD control frames will be sent as Untagged or Tagged with MVR VID. The default is tagged.

Priority : Specify how the traversed IGMP/MLD control frames will be sent in prioritized manner. The default Priority is 0.

LLQI : Define the maximum time to wait for IGMP/MLD report memberships on a receiver port before removing the port from multicast group membership. The value is in units of tenths of a second. The range is 0 to 31744. The default LLQI is 5 tenths or one-half second.

Interface Channel Profile : When the MVR VLAN is created, select the profile to expand the corresponding multicast channel settings for the specific MVR VLAN. The file established on Filtering Profile Table.

Port : The logical port for the settings.

Port Role : Configure an MVR port of the designated MVR VLAN as one of these roles:

> ***Inactive***: The designated port does not participate MVR operations.
>
> ***Source***: Configure uplink ports that receive and send multicast data as source ports. Subscribers cannot be directly connected to source ports.
>
> ***Receiver***: Configure a port as a receiver port if it is a subscriber port and should only receive multicast data. It does not receive data unless it becomes a member of the multicast group by issuing IGMP/MLD messages.

Caution: MVR source ports are not recommended to be overlapped with management VLAN ports. Select the port role by clicking the Role symbol to switch the setting:

I indicates Inactive; **S** indicates Source; **R** indicates Receiver. The default Role is **I**nactive.

Immediate Leave : Enable the fast leave on the port.

Buttons

Add New MVR VLAN : Click to add a 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.

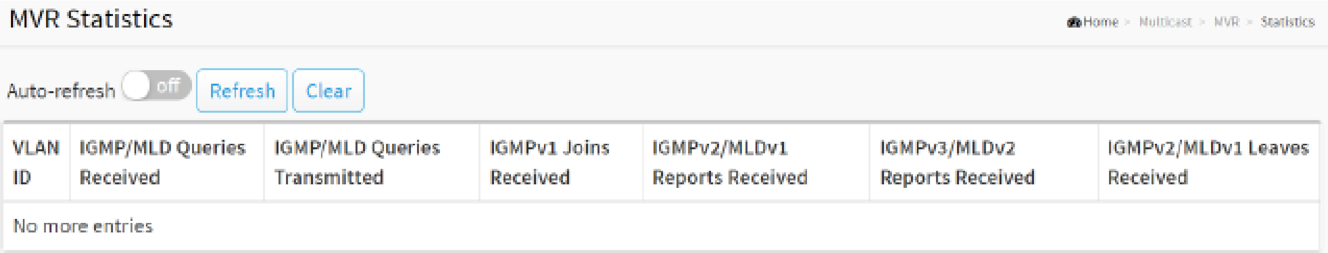
Apply : Click to save changes.

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

Statistics

This page displays detailed MVR Statistics. To display MVR Statistics Information in the web UI:

1. Click Multicast, MVR, and Statistics.
2. To automatically refresh the information click “Auto-refresh”.
3. Click “Refresh” to refresh an entry.



MVR 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
No more entries						

Figure 9-3.2: MVR Statistics

Parameter descriptions:

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 Joins.

IGMPv2/MLDv1 Reports Received : The number of Received IGMPv2 Joins and MLDv1 Reports, respectively.

IGMPv3/MLDv2 Reports Received : The number of Received IGMPv3 Joins and MLDv2 Reports, respectively.

IGMPv2/MLDv1 Leave's Received : The number of Received IGMPv2 Leaves and MLDv1 Dones, respectively.

Buttons

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

Refresh : Click to refresh the page immediately.

Clear : Clears all Statistics counters.

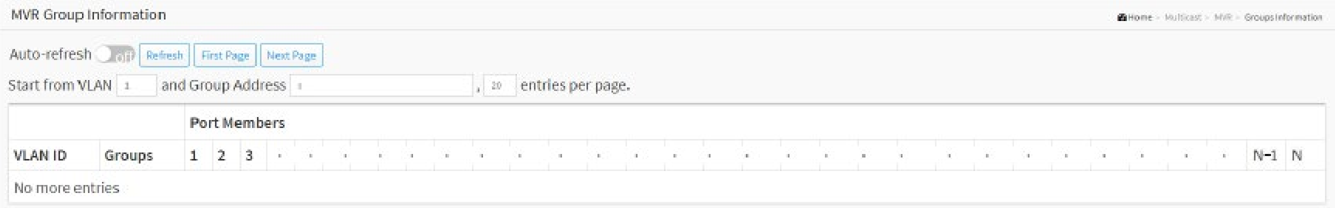
Groups Information

This page displays 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 MVR Groups Information in the web UI:

1. Click Multicast, MVR, and Groups Information.
2. Select ‘Start from VLAN’, ‘’ Group Address’, and ’entries per page’ parameters.
3. To automatically refresh the information click “Auto-refresh”.
4. Click “Refresh” to refresh an entry of the MVR Groups Information.
5. Click First/Next Page to change pages.



MVR Group Information

Start from VLAN 1 and Group Address 0 , 20 entries per page.

		Port Members																													
VLAN ID	Groups	1	2	3	·	·	·	·	·	·	·	·	·	·	·	·	·	·	·	·	·	·	·	·	·	·	·	·	·	N-1	N
No more entries																															

Figure 9-3.3: MVR Groups Information

Parameter descriptions:

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 every 3 seconds.

Refresh : Click to refresh the page immediately.

First Page : Updates the table starting from the first entry in the MVR Channels (Groups) Information Table.

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

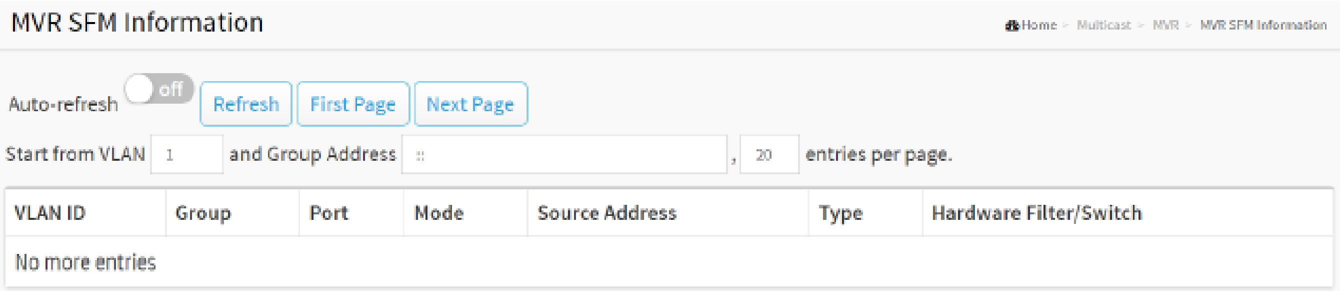
MVR SFM Information

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 belong to the same group are treated as a single entry.

Web Interface

To display MVR SFM Information in the web UI:

1. Click Multicast, MVR, and MVR SFM Information.
2. Select 'Start from VLAN', '' Group Address', and 'entries per page' parameters.
3. Use the "Auto-refresh" or the "Refresh" buttons as needed.
4. Click First/Next Page to change pages.



MVR SFM Information

Start from VLAN 1 and Group Address :: , 20 entries per page.

VLAN ID	Group	Port	Mode	Source Address	Type	Hardware Filter/Switch
No more entries						

Figure 9-3.4: MVR SFM Information

Parameter descriptions:

VLAN ID : VLAN ID of the group.

Group : IP Multicast Group address.

Port : Switch port number.

Mode : Indicates the filtering mode maintained per (VLAN ID, port number, Group Address) basis. It can be either Include or Exclude.

Source Address : IP Address of the source. Currently, system limits the total number of IP source addresses for filtering to be 128. When there is not any source filtering address, the text "None" is shown in the Source Address field.

Type : Indicates the Type. It can be either Allow or Deny.

Hardware Filter/Switch : Indicates whether data plane destined to the specific group address from the source IPv4/IPv6 address could be handled by the chip.

Buttons

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

Refresh : Click to refresh the page immediately.

First Page : Updates the table starting from the first entry in the MVR SFM Information Table.

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

Multicast Filtering Profile

This page provides Multicast Filtering Profile related configurations.

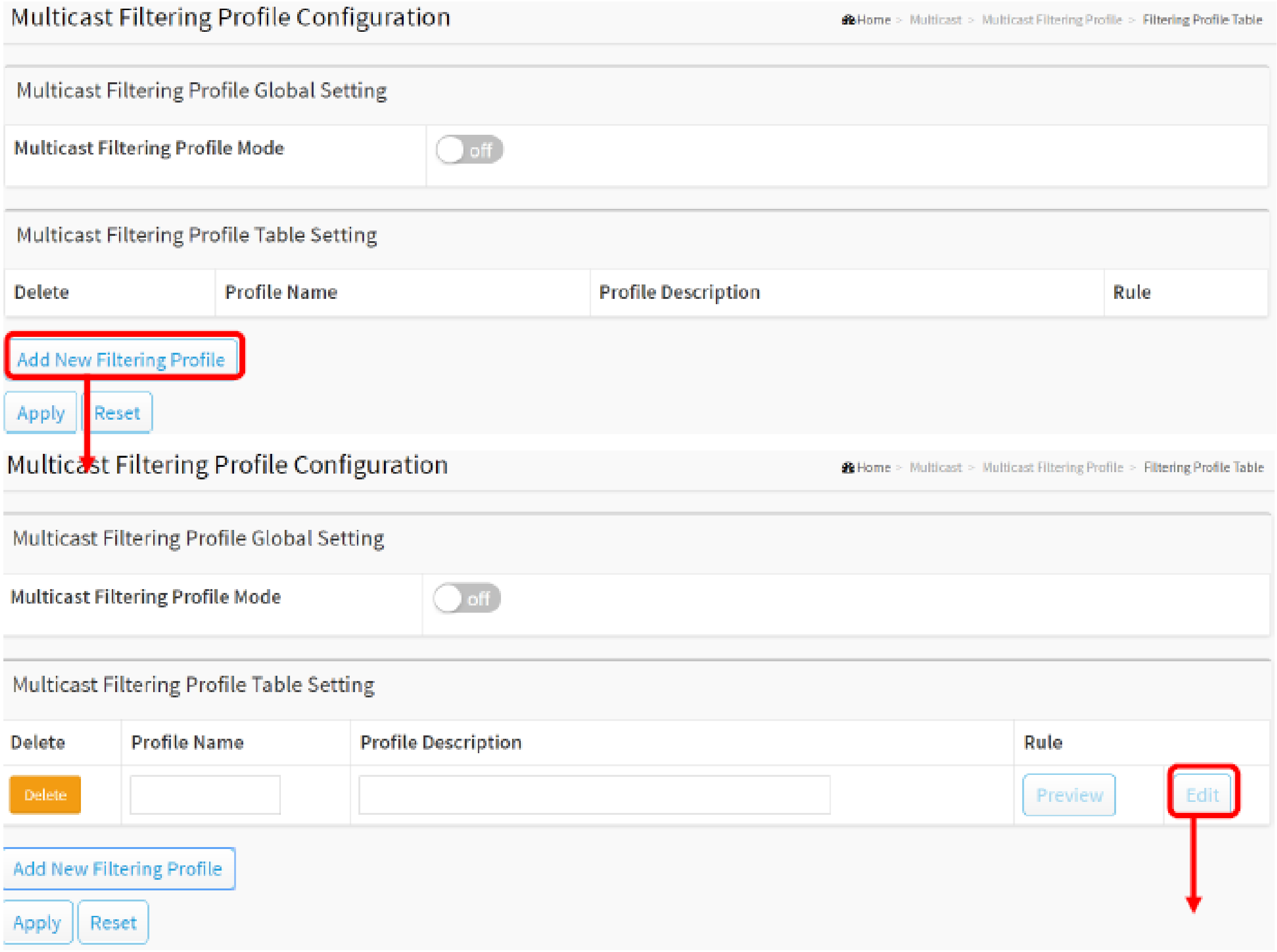
Filtering Profile Table

The IPMC profile is used to deploy access control on IP multicast streams. You can create a maximum 64 Profiles with at maximum 128 corresponding Rules for each Profile.

Web Interface

To configure IPMC Profile parameters in the web UI:

1. Click Multicast, Multicast Filtering Profile, and Filtering Profile Table.
2. Enable or disable the Multicast Filtering Profile mode.
3. Click "Add New Filtering Profile".
4. Specify Profile Name, Profile Description, and Rule.
5. Click Apply to save the settings or click the Reset button to cancel the settings.



Multicast Filtering Profile Configuration

Home > Multicast > Multicast Filtering Profile > Filtering Profile Table

Multicast Filtering Profile Global Setting

Multicast Filtering Profile Mode	off

Multicast Filtering Profile Table Setting

Delete	Profile Name	Profile Description	Rule

Add New Filtering Profile
Apply
Reset

Multicast Filtering Profile Configuration

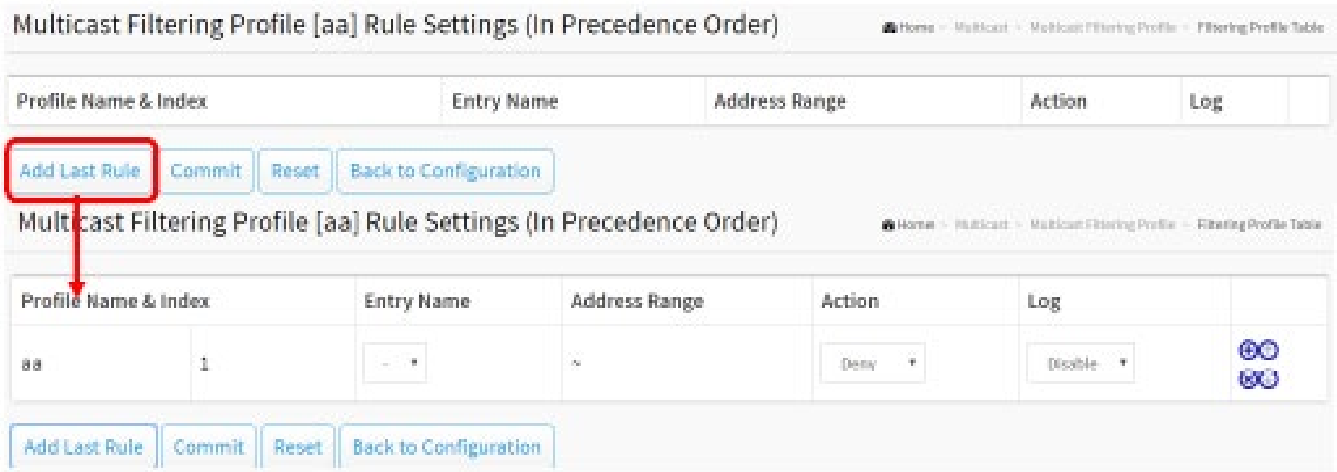
Home > Multicast > Multicast Filtering Profile > Filtering Profile Table

Multicast Filtering Profile Global Setting

Multicast Filtering Profile Mode	off

Multicast Filtering Profile Table Setting

Delete	Profile Name	Profile Description	Rule	
Delete			Preview	Edit



Multicast Filtering Profile [aa] Rule Settings (In Precedence Order)

Profile Name & Index	Entry Name	Address Range	Action	Log

Home » Multicast » Multicast Filtering Profile » Filtering Profile Table
Add Last Rule
Commit
Reset
Back to Configuration

Multicast Filtering Profile [aa] Rule Settings (In Precedence Order)

Profile Name & Index		Entry Name	Address Range	Action	Log	
aa	1	-	~	Deny	Disable	

Home » Multicast » Multicast Filtering Profile » Filtering Profile Table
Add Last Rule
Commit
Reset
Back to Configuration

Figure 9-4.1: IPMC Profile Configuration

Parameter descriptions:

Multicast Filtering Profile Mode : Enable/Disable the Multicast Filtering Profile. System starts to do filtering based on profile settings only when the global profile mode is enabled.

Profile Name : The name used for indexing the profile table. Each entry has the unique name which is composed of at maximum 16 alphabetic and numeric characters.

Profile Description : Additional description, 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. 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 these buttons:

> ***Preview***: Preview the rules associated with the designated profile.
>
> ***Edit***: Adjust the rules associated with the designated profile.

Profile Name & Index : The name of the designated profile to be associated. This field is not editable.

Entry Name : The name used in specifying the address range used for this rule. Only the existing profile address entries will be chosen in the selected box. This field is not allowed to be selected as none ("-") while the Rule Settings Table is committed.

Address Range : The corresponding address range of the selected profile entry. This field is not editable and will be adjusted automatically according to the selected profile entry.

Action : Indicates the learning action upon receiving the Join/Report frame that has the group address matches the address range of the rule.

> ***Permit***: Group address matches the range specified in the rule will be learned.
>
> ***Deny***: Group address matches the range specified in the rule will be dropped.

Log : Indicates the logging preference upon receiving the Join/Report frame that has the group address matches the address range of the rule.

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

Rule Management Buttons : You can manage rules and the corresponding precedence order by using the following buttons:

⊕ : Insert a new rule before the current entry of rule.

⊗ : Delete the current entry of rule.

↑ : Move the current entry of rule up in the list.

↓ : Move the current entry of rule down in the list.

Buttons

Add New Filtering Profile : Click to add new IPMC profile. Specify the name, configure the new entry, and 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.

Add Last Rule : Click to add a new rule to the end of the specific profile's rule list. Specify the address entry and configure the new entry. Click "Apply".

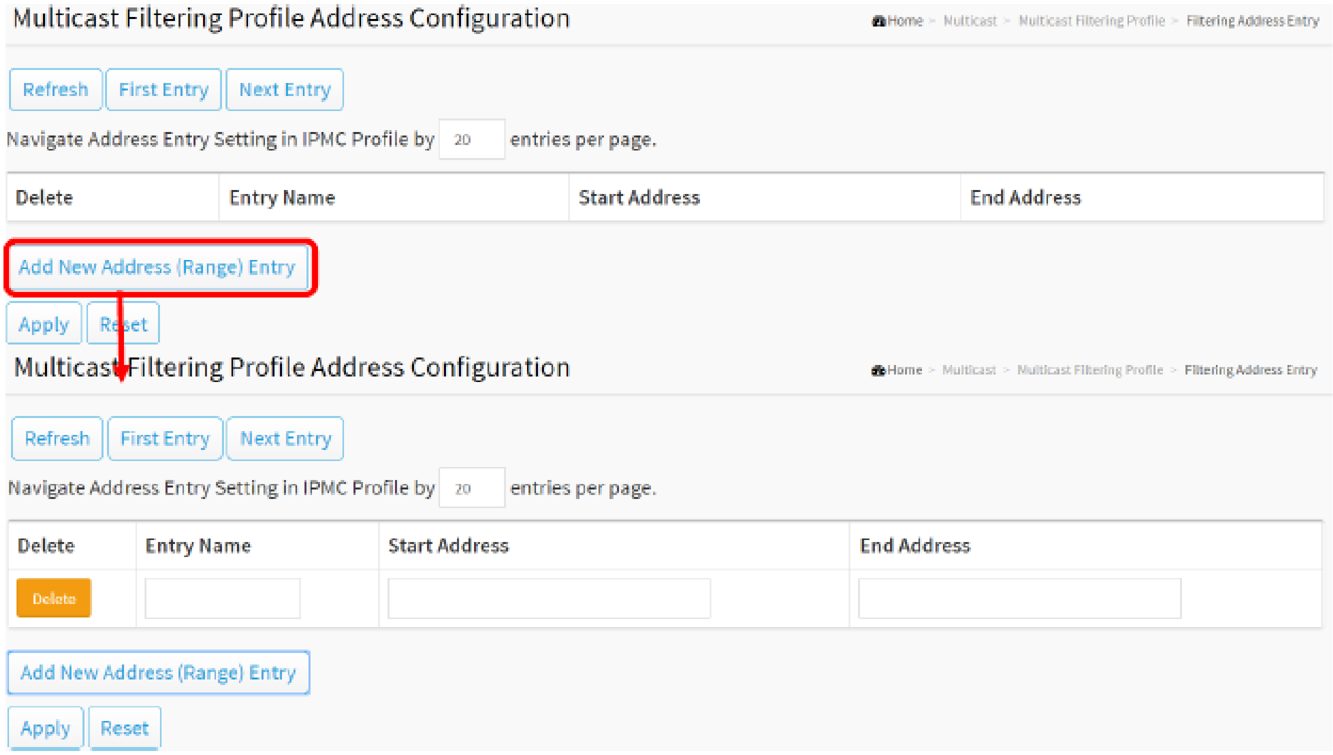
Filtering Address Entry

This page provides address range settings used in an IPMC profile. The address entry is used to specify the address range that will be associated with IPMC Profile. You can create a maximum of 128 address entries in the system.

Web Interface

To configure IPMC Profile Address parameters in the web UI:

1. Click Multicast, Multicast Filtering Profile, and Filtering Address Entry.
2. Click “Add New Address (Range) Entry”.
3. Specify Entry Name, Start Address, and End Address.
4. Click Apply to save the settings.
5. To cancel the settings, click the Reset button. It will revert to previously saved values.
6. Click “Refresh” to refresh an entry.
7. Click First Entry/Next Entry to change Entry.



Multicast Filtering Profile Address Configuration

Navigate Address Entry Setting in IPMC Profile by 20 entries per page.

Delete	Entry Name	Start Address	End Address

Multicast Filtering Profile Address Configuration

Navigate Address Entry Setting in IPMC Profile by 20 entries per page.

Delete	Entry Name	Start Address	End Address
Delete			

Home > Multicast > Multicast Filtering Profile > Filtering Address Entry
Refresh
First Entry
Next Entry
Add New Address (Range) Entry
Apply
Reset

Figure 9-4.2: IPMC Profile Address Configuration

Parameter descriptions:

Entry Name : The name used for indexing the address entry table. Each entry has the unique name which is composed of at maximum 16 alphabetic and numeric characters.

Start Address : The starting IPv4/IPv6 Multicast Group Address that will be used as an address range.

End Address : The ending IPv4/IPv6 Multicast Group Address that will be used as an address range.

Buttons

Add New Address (Range) Entry : Click to add new address range. Specify the name, configure the addresses then click "Apply".

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

Apply : Click to save changes.

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

First Entry : Updates the table starting from the first entry in the table.

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

10. DHCP

This section lets you set and view DHCP snooping, SNMP relay, and SNMP server parameters.

Snooping

Configuration

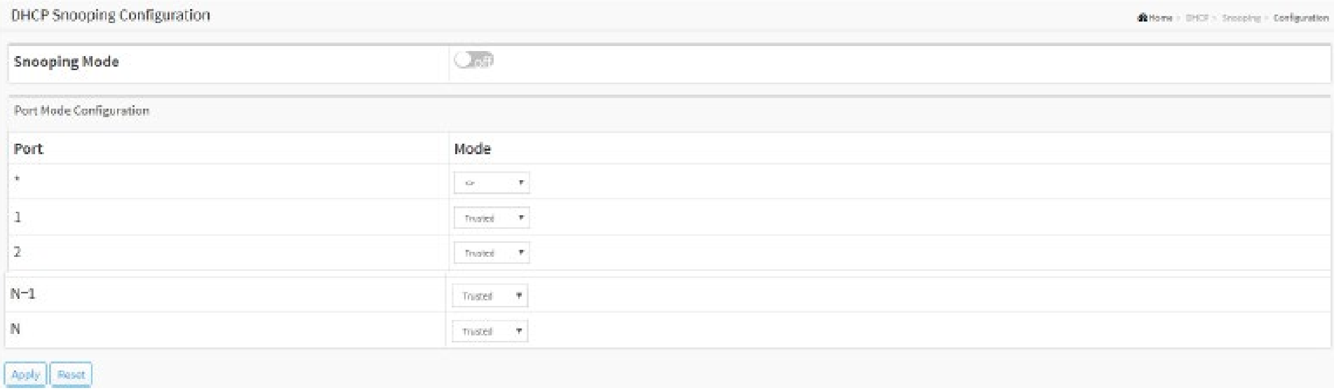
DHCP Snooping is used to block an intruder on the untrusted ports of the switch device when it tries to intervene by injecting a bogus DHCP reply packet to a legitimate conversation between the DHCP client and server.

This page lets you configure 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 UI:

1. Click DHCP, Snooping, and Configuration.
2. At Snooping Mode select "on" to enable snooping globally.
3. At the Mode dropdown Select "Trusted" for the desired ports.
4. Click Apply.



DHCP Snooping Configuration

Home > DHCP > Snooping > Configuration

Snooping Mode: off

Port Mode Configuration

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

Figure 10-1.1: DHCP Snooping Configuration

Parameter descriptions:

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 (default).

Port Mode Configuration : Indicates the DHCP snooping port mode. Possible port modes are:

> ***Trusted***: Configures the port as trusted source of the DHCP messages. Trusted port can forward DHCP packets normally.
>
> ***Untrusted***: Configures the port as untrusted source of the DHCP messages. Untrusted port will discard the packets when it receives DHCP packets.

Buttons

Apply : Click to save changes.

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

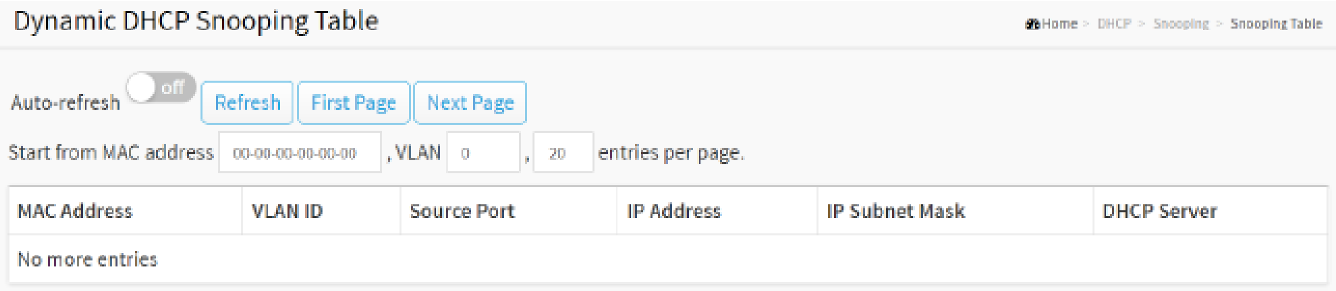
Snooping Table

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

Web Interface

To monitor DHCP Snooping in the web UI:

1. Click DHCP, Snooping, and Snooping Table.
2. To automatically refresh the information click “Auto-refresh”.
3. Click “Refresh” to refresh an entry.
4. Click First/Next Page to change page.



Dynamic DHCP Snooping Table

Start from MAC address 00-00-00-00-00-00 , VLAN 0 , 20 entries per page.

MAC Address	VLAN ID	Source Port	IP Address	IP Subnet Mask	DHCP Server
No more entries					

Figure 10-1.2: DHCP Snooping Table

Parameter descriptions:

Start from MAC address : Choose the starting MAC address.

VLAN : Choose the starting VLAN ID.

entries per page: Choose how many items you want to be displayed per page.

MAC Address : The User MAC address of the entry.

VLAN ID : The VLAN-ID in which the DHCP traffic is permitted.

Source Port: The 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 : The DHCP Server address of the entry.

Buttons

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

Refresh : Click to refresh the page immediately.

First Page : Updates the table starting from the first entry in the Dynamic DHCP snooping Table.

Next Page : Updates the group information entries, turn to the next page.

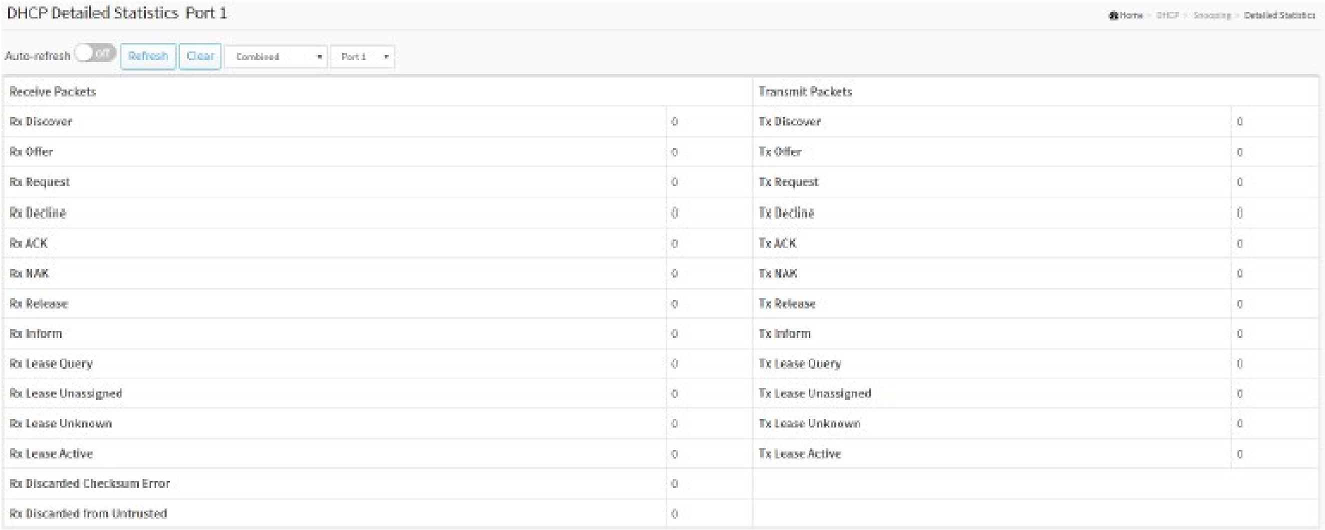
Detailed Statistics

This page provides statistics for DHCP snooping. Note that the normal forward per-port TX statistics isn't increased if the incoming DHCP packet is done by L3 forwarding mechanism. Also note that clearing the statistics on a specific port may not take effect on global statistics since it gathers the different layer overview.

Web Interface

To display DHCP detailed statistics in the web UI:

1. Click DHCP, Snooping and Detailed Statistics.
2. Select port that you want to display the DHCP Detailed Statistics.
3. To automatically refresh the information check the “Auto-refresh” button.
4. To click the “Refresh” to refresh an entry of the DHCP Detailed Statistics.



DHCP Detailed Statistics Port 1

Receive Packets		Transmit Packets	
Rx Discover	0	Tx Discover	0
Rx Offer	0	Tx Offer	0
Rx Request	0	Tx Request	0
Rx Decline	0	Tx Decline	0
Rx ACK	0	Tx ACK	0
Rx NAK	0	Tx NAK	0
Rx Release	0	Tx Release	0
Rx Inform	0	Tx Inform	0
Rx Lease Query	0	Tx Lease Query	0
Rx Lease Unassigned	0	Tx Lease Unassigned	0
Rx Lease Unknown	0	Tx Lease Unknown	0
Rx Lease Active	0	Tx Lease Active	0
Rx Discarded Checksum Error	0		
Rx Discarded from Untrusted	0		

Figure 10-1.3: DHCP Detailed Statistics

Parameter descriptions:

<u>**Server Statistics**</u>

Rx and Tx Discover : The number of discover (option 53 with value 1) packets received and transmitted.

Rx and Tx Offer : The number of offer (option 53 with value 2) packets received and transmitted.

Rx and Tx Request : The number of request (option 53 with value 3) packets received and transmitted.

Rx and Tx Decline : The number of decline (option 53 with value 4) packets received and transmitted.

Rx and Tx ACK : The number of ACK (option 53 with value 5) packets received and transmitted.

Rx and Tx NAK : The number of NAK (option 53 with value 6) packets received and transmitted.

Rx and Tx Release : The number of release (option 53 with value 7) packets received and transmitted.

Rx and Tx Inform : The number of inform (option 53 with value 8) packets received and transmitted.

Rx and Tx Lease Query : The number of lease query (option 53 with value 10) packets received and transmitted.

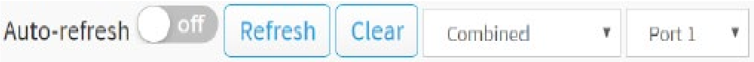
Rx and Tx Lease Unassigned : The number of lease unassigned (option 53 with value 11) packets received and transmitted.

Rx and Tx Lease Unknown : The number of lease unknown (option 53 with value 12) packets received and transmitted. Rx and Tx Lease Active

Rx and Tx Lease Active : The number of lease active (option 53 with value 13) packets received and transmitted.

Rx Discarded checksum error : The number of discard packet that IP/UDP checksum is error.

Rx Discarded from Untrusted : The number of discarded packets that are coming from untrusted port.



Buttons

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

Refresh : Click to refresh the page immediately.

Clear : Click to clear the webpage statistics.

User select box : At the dropdown select the set of users to be displayed.

Port select box : At the dropdown select the port to be displayed.

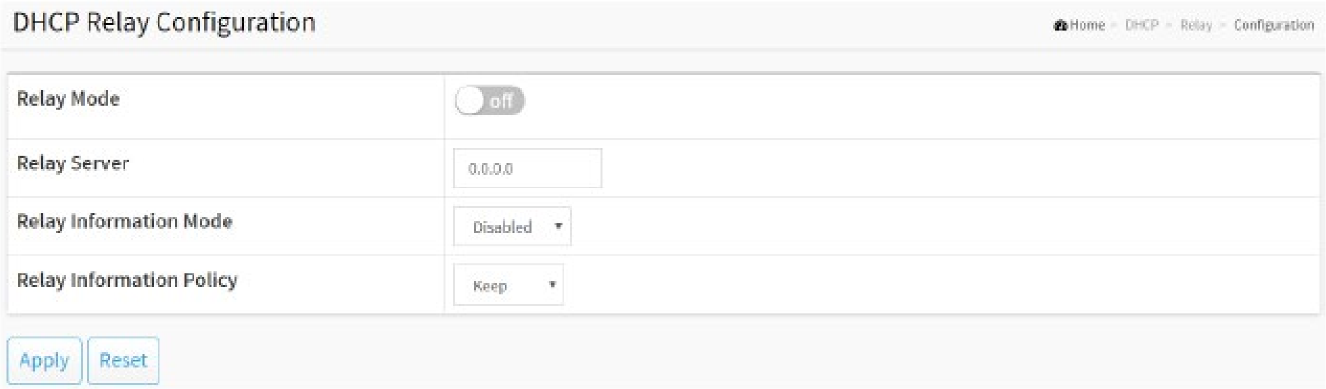
Relay

Configuration

A DHCP relay agent is used to forward and to transfer DHCP messages between the clients and the server when they are not in the same subnet domain. It stores the incoming interface IP address in the GIADDR field of the DHCP packet. The DHCP server can use the value of GIADDR field to determine the assigned subnet. For such a condition, make sure the switch configuration of VLAN interface IP address and PVID (Port VLAN ID) is correct.

To configure DHCP Relay in the web UI:

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



DHCP Relay Configuration

Relay Mode	off
Relay Server	0.0.0.0
Relay Information Mode	Disabled
Relay Information Policy	Keep

Figure 10-2.1: DHCP Relay Configuration

Parameter descriptions:

Relay Mode : Indicates the DHCP relay mode operation. Possible modes are:

> ***on***: Enable DHCP relay mode operation. When DHCP relay mode operation is enabled, the agent forwards and transfers DHCP messages between the clients and the server when they are not in the same subnet domain. And the DHCP broadcast message won't be flooded for security considerations.
>
> ***off*** : Disable DHCP relay mode operation.

Relay Server : Indicates the DHCP relay server IP address.

Relay Information Mode : Indicates the DHCP relay information mode option operation. The option 82 circuit ID format as "[vlan_id][module_id][port_no]". The first four characters represent the VLAN ID, the fifth and sixth characters are the module ID (in standalone device it always equals 0), and the last two characters are the port number. For example, "00030108" means the DHCP message received from VLAN ID 3, switch ID 1, port No 8 and the option 82 remote ID value equals the switch MAC address.

Possible modes are:

> ***Enabled***: Enable DHCP relay information mode operation. When DHCP relay information mode operation is enabled, the agent inserts specific information (option 82) into a DHCP message when forwarding to DHCP server and removes it from a DHCP message when transferring to DHCP client. It only works when DHCP relay operation mode is enabled.
>
> ***Disabled***: Disable DHCP relay information mode operation.

Relay Information Policy : Indicates the DHCP relay information option policy. When DHCP relay information mode operation is enabled, if the agent receives a DHCP message that already contains relay agent information it will enforce the policy. The 'Replace' policy is invalid when relay information mode is disabled. Possible policies are:

Replace: Replace the original relay information when a DHCP message that already contains it is received.

Keep: Keep the original relay information when a DHCP message that already contains it is received.

Drop: Drop the package when a DHCP message that already contains relay information is received.

Buttons

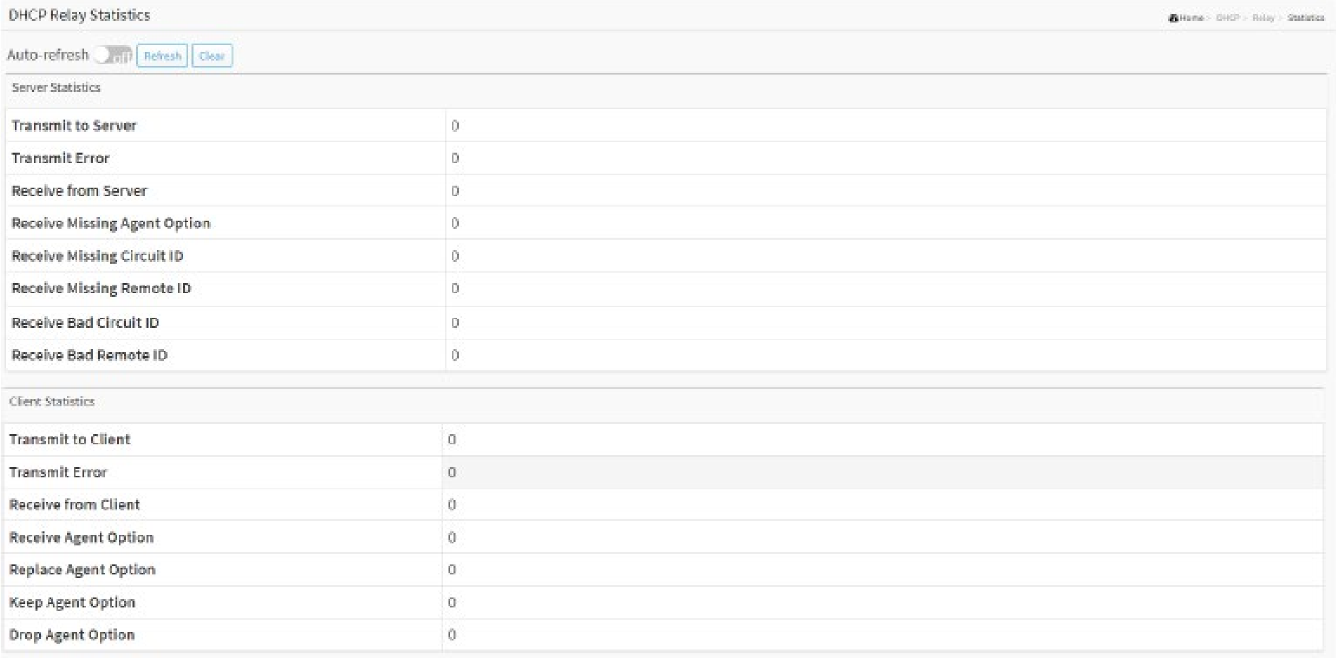
Apply : Click to save changes.

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

Statistics

This page provides statistics for DHCP relay. To view DHCP Relay statistics in the web UI:

1. Click DHCP, Relay and Statistics to display DHCP relay statistics.
2. To automatically refresh the information click “Auto-refresh”.
3. Click the “Refresh” to refresh an entry of the DHCP Detailed Statistics.



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

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

Figure 10-2.2: DHCP Relay Statistics

Parameter descriptions:

Server Statistics

Transmit to Server : The number of packets that are relayed from client to server.

Transmit Error : The number of packets that resulted in errors while being sent to clients.

Receive from Server : The number of packets received from server.

Receive Missing Agent Option : The number of packets received without agent information options.

Receive Missing Circuit ID : The number of packets received with the Circuit ID option missing.

Receive Missing Remote ID : The number of packets received with the Remote ID option missing.

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

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

Client Statistics

Transmit to Client : The number of relayed packets from server to client.

Transmit Error : The number of packets that resulted in error while being sent to servers.

Receive from Client : The number of received packets from server.

Receive Agent Option : The number of received packets with relay agent information option.

Replace Agent Option : The number of packets which were replaced with relay agent information option.

Keep Agent Option : The number of packets whose relay agent information was retained.

Drop Agent Option : The number of packets that were dropped which were received with relay agent information.

Buttons

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

Refresh : Click to refresh the page immediately.

Clear : Clear all statistics.

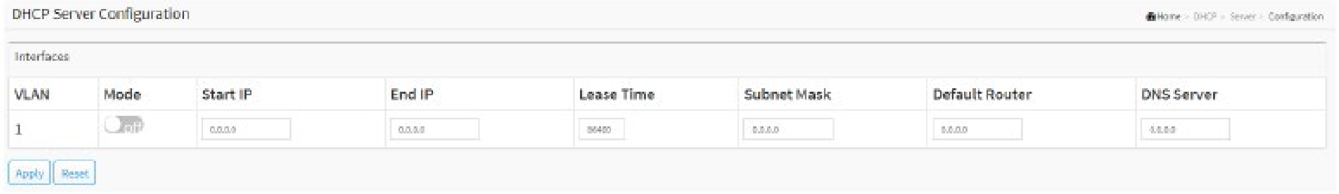
Server

Configuration

This page lets you enable/disable DHCP server per system and per VLAN and set Start IP and End IP addresses. A DHCP server will allocate these IP addresses to the DHCP client and deliver configuration parameters to the DHCP client.

To configure DHCP Server parameters in the web UI:

1. Click DHCP, Server, and Configuration.
2. Click “Add Interface”.
3. Specify VLAN, Mode, Start IP, End IP, Lease time, Subnet mask, Default router, and DNS server.
4. Click Apply.



DHCP Server Configuration

Interfaces

VLAN	Mode	Start IP	End IP	Lease Time	Subnet Mask	Default Router	DNS Server
1	off	0.0.0.0	0.0.0.0	86400	0.0.0.0	0.0.0.0	0.0.0.0

Figure 10-3.1: DHCP Server Configuration

Parameter descriptions:

VLAN: Configure the VLAN in which the DHCP server is enabled or disabled. Allowed VLANs are 1 – 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 address range. The Start IP must be smaller than or equal to the End IP address.

Lease Time : Displays lease time of the pool in minutes.

Subnet Mask : Configure subnet mask of the DHCP address.

Default Router : Configure the destination IP network or host address of this route.

DNS Server : Specify the 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.

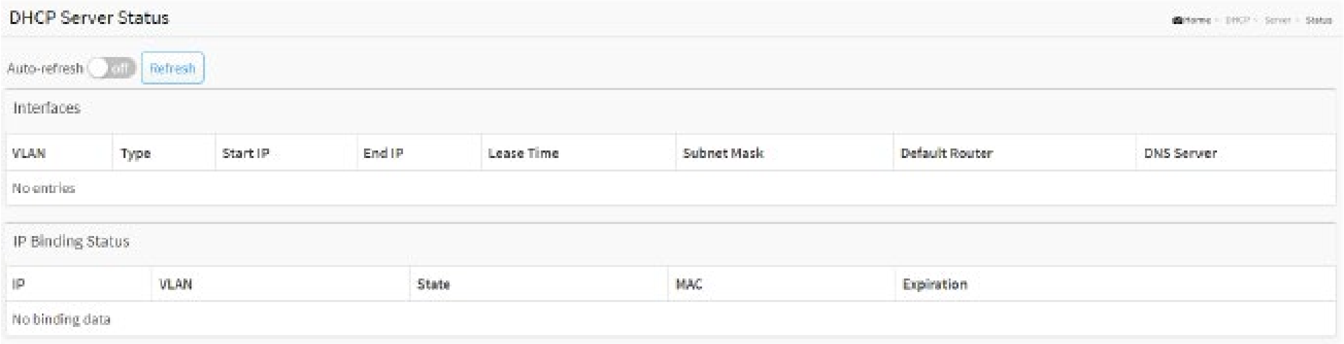
Apply : Click to save changes.

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

Status

This page displays DHCP server status. To display DHCP server status in the web UI:

1. Click DHCP, Server, and Status.
2. To automatically refresh the information, click “Auto-refresh”.
3. Click “Refresh” to refresh the DHCP server status page.



Interfaces

VLAN	Type	Start IP	End IP	Lease Time	Subnet Mask	Default Router	DNS Server
No entries							

IP Binding Status

IP	VLAN	State	MAC	Expiration
No binding data				

Figure 10-3.2: DHCP Server Status

Parameter descriptions:

<u>Interfaces</u>:

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** : Displays the Start IP address and the End IP address.

Lease Time : Displays lease time of the pool in minutes.

Subnet Mask : Displays subnet mask of the DHCP address.

Default Router : Displays the destination IP network or host address of this route.

DNS Server : Displays DNS server IP address.

<u>IP Binding Status</u>:

IP : Displays the IP address of the binding.

VLAN : Displays the VLAN ID.

State : Displays the binding state.

MAC : Displays the MAC address.

Expiration : Displays the lease expiration date and time.

Buttons

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

Refresh : Click to refresh the page immediately.

11. Security

This section lets you configure switch Security settings. You can use the Security features to configure a wide array of security functions.

Management

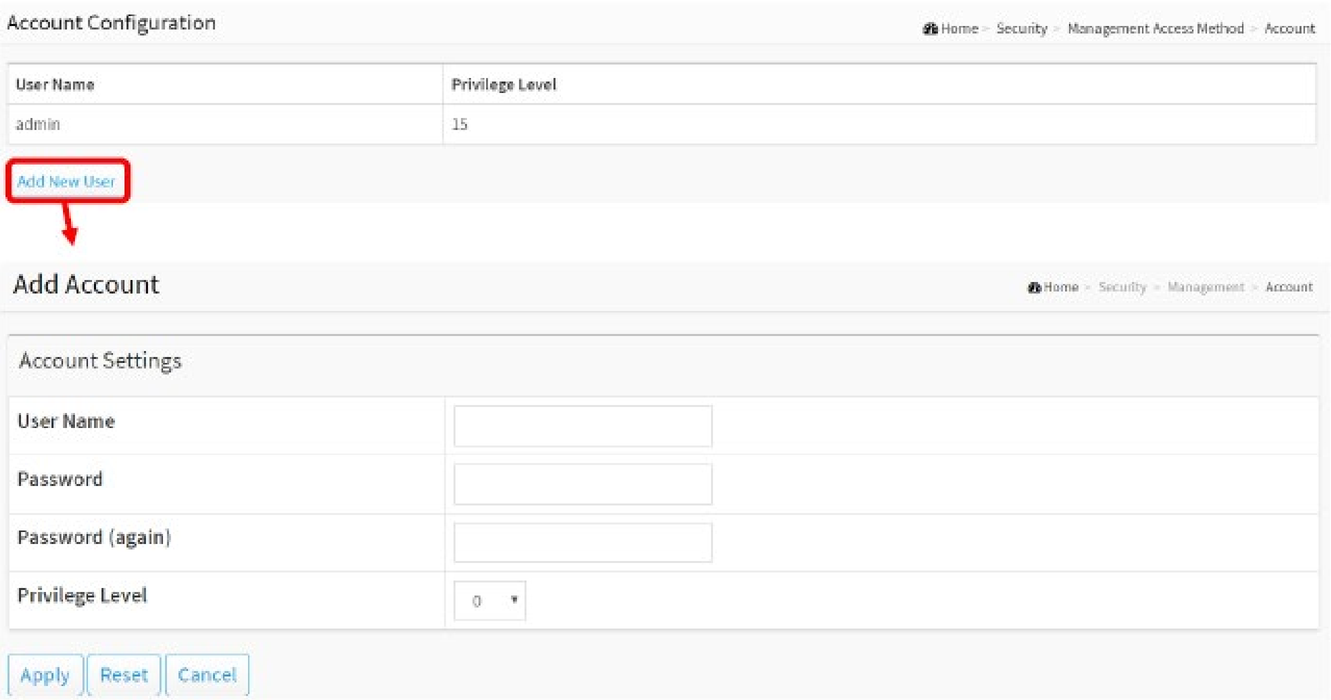
Account

This page provides an overview of the current users and lets you add and configure account users. Currently the only way to login as another user on the web server is to close and reopen the browser.

Web Interface

To add a User in the web UI:

1. Click Security, Management, and Account.
2. Click Add New User.
3. Specify the User Name, Password, and Privilege Level parameters.
4. Click Apply.



Home > Security > Management Access Method > Account
Add New User
Home > Security > Management > Account
Apply
Reset
Cancel

Account Configuration

User Name	Privilege Level
admin	15

Add Account

Account Settings

User Name	
Password	
Password (again)	
Privilege Level	0

Figure 11-1.1: Account Configuration

Parameter descriptions:

User Name : The name identifying the user. Enter up to 31 characters. This is also a link to Add or Edit a User.

Password : Type the password. The field can be input 31 characters, and the allowed content is ASCII characters 32 - 126.

Password (again) : Type the password again. You must type the exact same password again in this field.

Privilege Level : The privilege level of the user. The valid range is 0 to 15. If the privilege level value is 15, it can access all groups, i.e., that is granted the fully control of the device. But other values must refer to each group privilege level. User's privilege should be same or greater than the group privilege level to have the access of that group. By default setting, most groups privilege level 5 has the read-only access and privilege level 10 has the read-write access. System maintenance functions (software upload, factory defaults etc.) need user privilege level 15. Generally, privilege level 15 is 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).

To edit a User in the web UI:

1. Click Security, Management, and Account.
2. Click the linked User Name.
3. Specify new User Name, Password, and Privilege Level parameters.
4. Click Apply.

To delete a User in the web UI:

1. Click Security, Management, and Account.
2. Click
3. Click Apply.

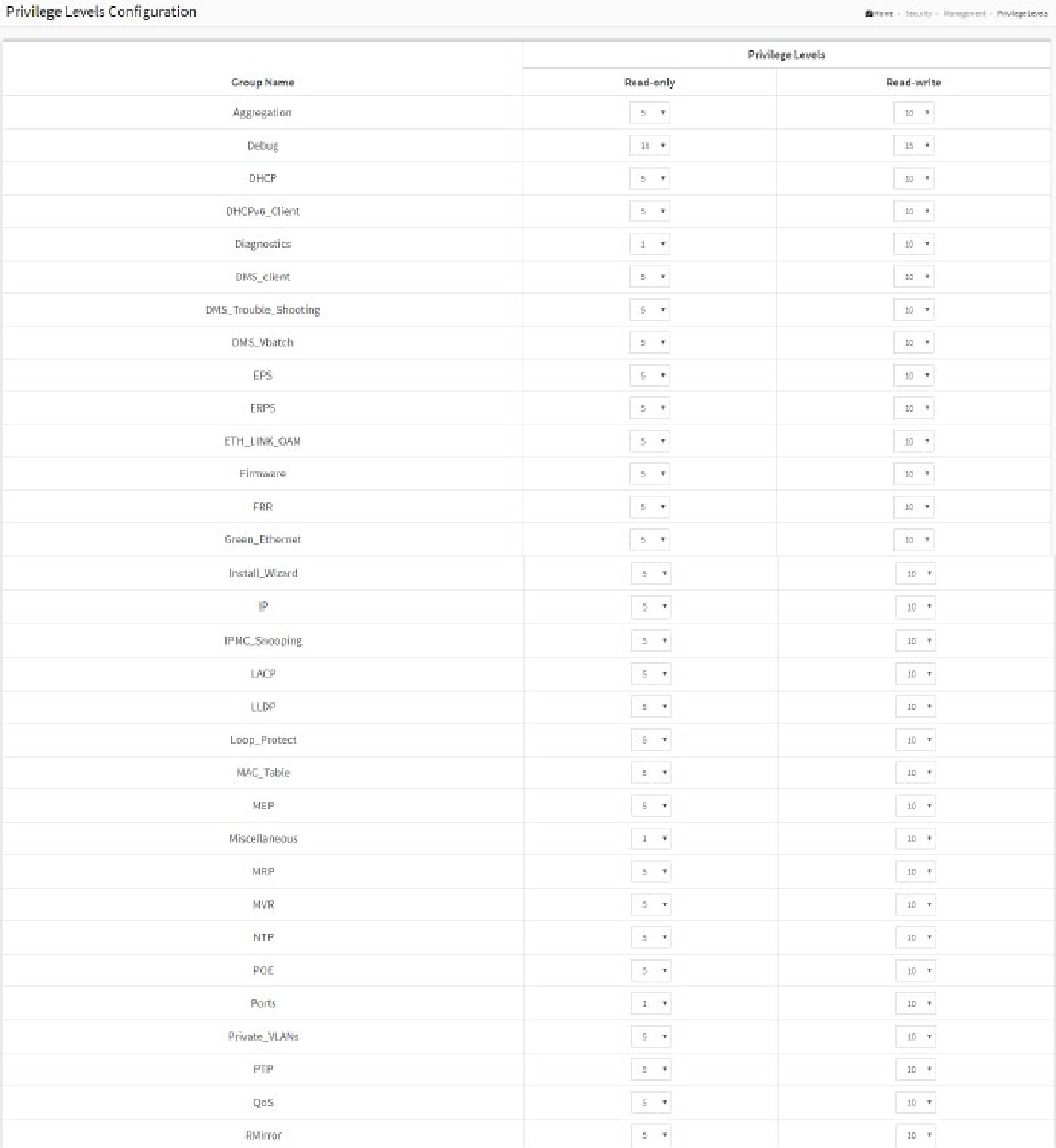
Privilege Levels

This page provides an overview of the privilege levels. The switch provides user privilege level settings for these groups: Aggregation, Debug, DHCP, DHCPv6_Client, Diagnostics, DMS_client, DMS_Trouble_shooting, DMS_vBatch, EPS, ERPS, ETH_LINK_OAM, Firmware, FRR, Green_Ethernet, Install_Wizard, IP, IPMC_Snooping, LACP, LLDP, Loop_Protect, MAC_Table, MEP, Miscellaneous, MRP, MVR, NTP, PoE, Ports, Private_VLANs, PTP, QoS, RMirror, Security_Access, Security_network, SFlow, SMTP, Spanning Tree, System, Trap_Event, UDLD, uFDMA_AIL, uFDMA_CIL, uPMP, VCL, VLAN_Translation, VLANs, Voice_VLAN, Watchdog, XXRP.

Each group can have a Privilege Level setting of 1 to 15.

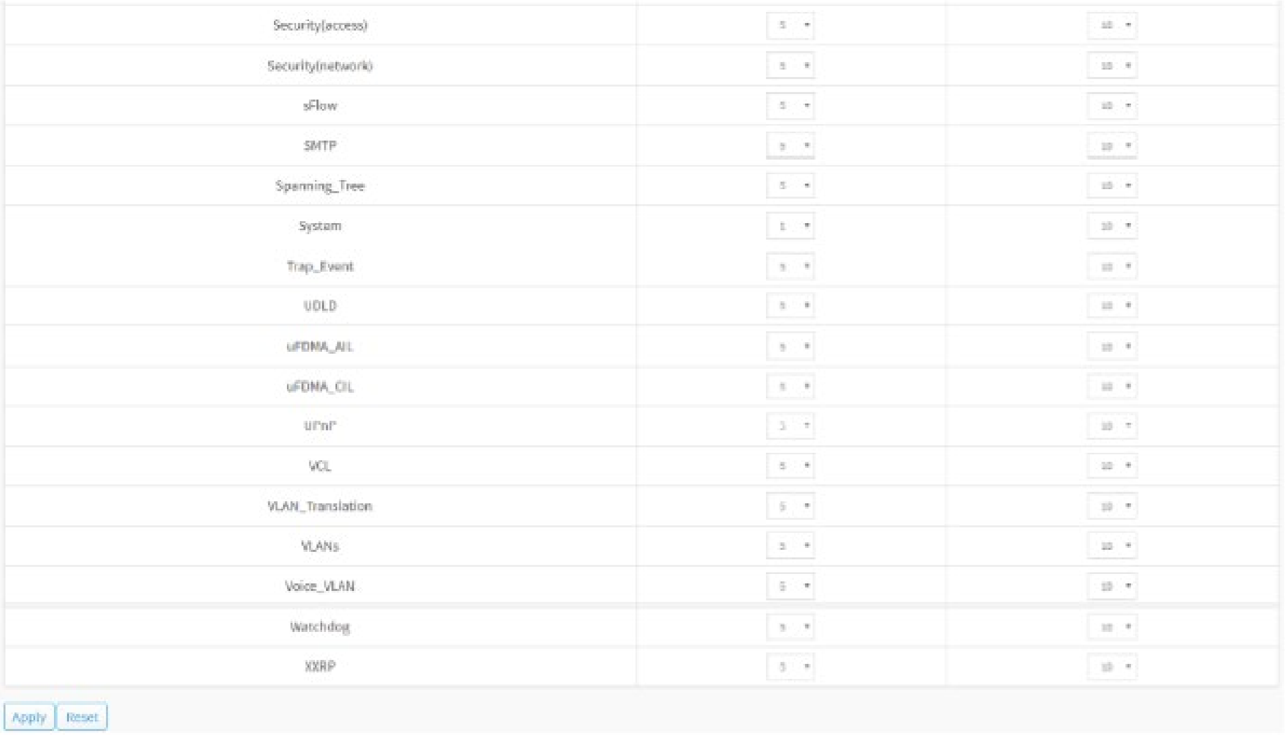
To configure Privilege Levels in the web UI:

1. Click Security, Management, and Privilege Levels.
2. Specify the Privilege parameters (Read only and Read-write) for the one or more Group Name(s).
3. Click Apply.



Privilege Levels Configuration

Group Name	Privilege Levels	
	Read-only	Read-write
Aggregation	5	10
Debug	15	15
DHCP	5	10
DHCPv6_Client	5	10
Diagnostics	1	10
DMS_client	5	10
DMS_Trouble_Shooting	5	10
DMS_Vbatch	5	10
EPS	5	10
ERPS	5	10
ETH_LINK_OAM	5	10
Firmware	5	10
FRR	5	10
Green_Ethernet	5	10
Install_Wizard	5	10
IP	5	10
IPMC_Snooping	5	10
LACP	5	10
LLDP	5	10
Loop_Protect	5	10
MAC_Table	5	10
MEP	5	10
Miscellaneous	1	10
MRP	5	10
MVR	5	10
NTP	5	10
POE	5	10
Ports	1	10
Private_VLANs	5	10
PTP	5	10
QoS	5	10
RMirror	5	10



Security(access)	5 ▾	10 ▾
Security(network)	5 ▾	10 ▾
sFlow	5 ▾	10 ▾
SMTP	5 ▾	10 ▾
Spanning_Tree	5 ▾	10 ▾
System	1 ▾	10 ▾
Trap_Event	5 ▾	10 ▾
UDLD	5 ▾	10 ▾
uFDMA_AIL	5 ▾	10 ▾
uFDMA_CIL	5 ▾	10 ▾
UPnP	5 ▾	10 ▾
VCL	5 ▾	10 ▾
VLAN_Translation	5 ▾	10 ▾
VLANs	5 ▾	10 ▾
Voice_VLAN	5 ▾	10 ▾
Watchdog	5 ▾	10 ▾
XXRP	5 ▾	10 ▾

Figure11-1.2: Privilege Level Configuration

Parameter descriptions:

Group Name : The name identifying the privilege group. In most cases, a privilege level group consists of a single module (e.g., LACP, RSTP or QoS), but a few of them contains more than one. The following defines these privilege level groups in detail:

System: Contact, Name, Location, Timezone, Daylight Saving Time, Log.

Security: Authentication, System Access Management, Port (contains Dot1x port, MAC based and the MAC Address Limit), ACL, HTTPS, SSH, ARP Inspection, IP source guard.

IP: Everything except 'ping'.

Port: Everything except 'Cable Diagnostics'.

Diagnostics: 'ping' and 'Cable Diagnostics'.

Maintenance: CLI- System Reboot, System Restore Default, System Password, Configuration Save, Configuration Load and Firmware Load. Web- Users, Privilege Levels and everything in Maintenance.

Debug: Only present in CLI.

Privilege Levels : The Privilege Levels can be configured to 0 - 15 (where 0 is lowest level and 15 is highest level). Every group has an authorization Privilege level for the following sub groups: read-only, read-write. User Privilege should be same or greater than the authorization Privilege level to have the access to that function.

Buttons

Apply : Click to save changes.

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

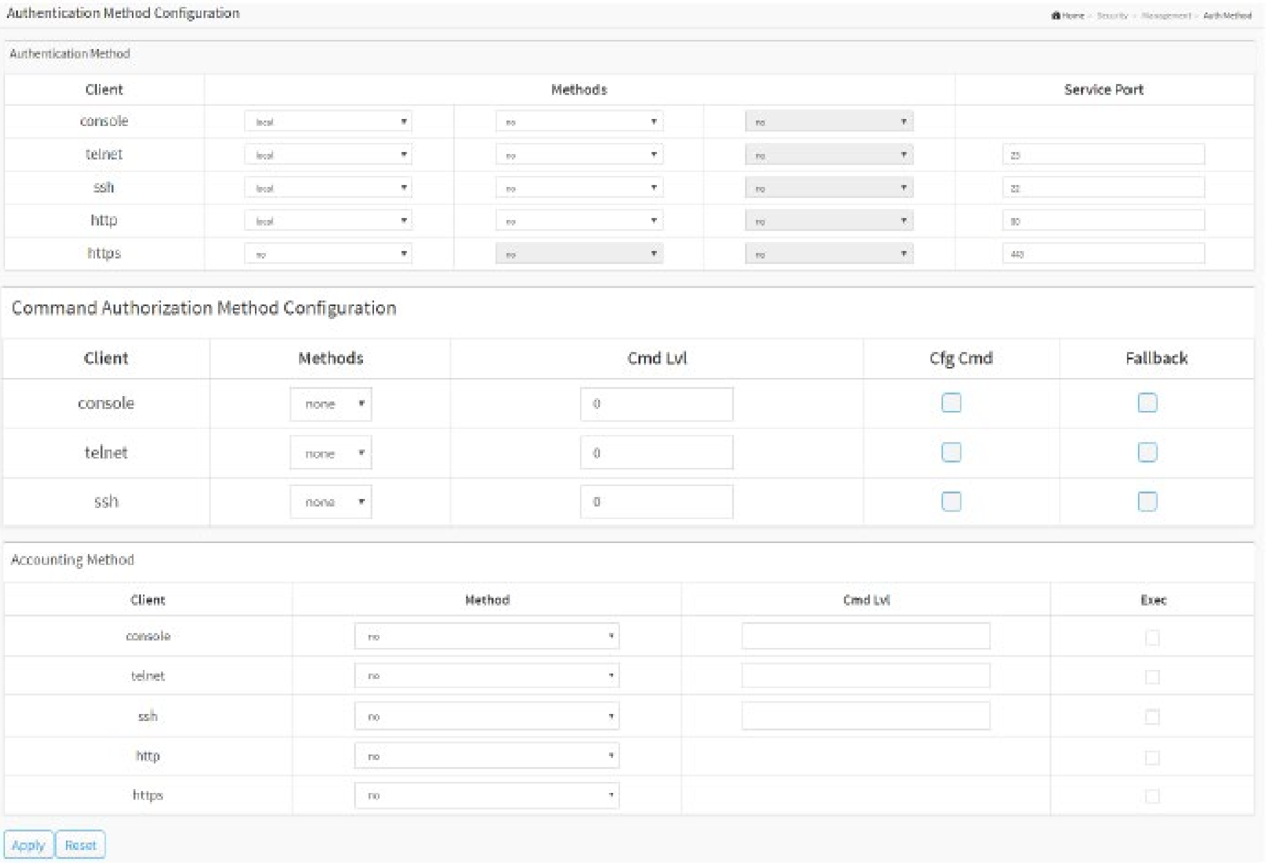
Auth Method

Here you can configure a user with one or more Authentication, Authorization, and/or Accounting methods to be used when they log into the switch via one of the management client interfaces.

Web Interface

To configure Auth Method in the web UI:

1. Click Security, Management and Auth Method.
2. Specify the Client (console, telnet, ssh, web) which you want to monitor.
3. Specify the Methods (none, local, radius, tacacs), Service port, Cmd Lvl, Cfg Cmd, Fallback, Exec.
4. Click Apply.



Authentication Method Configuration

Authentication Method

Client	Methods			Service Port
console	local	no	no	
telnet	local	no	no	23
ssh	local	no	no	22
http	local	no	no	80
https	no	no	no	443

Command Authorization Method Configuration

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

Accounting Method

Client	Method	Cmd Lvl	Exec
console	no		□
telnet	no		□
ssh	no		□
http	no		□
https	no		□

Figure 11-1.3: Authentication Method Configuration

Parameter descriptions:

Authentication Method Configuration

Client : The management client for which the configuration below applies.

Method : Authentication Method can be set to one of these 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 it is recommended to configure secondary authentication as 'local'. This lets the management client login via the local user database if none of the configured authentication servers are alive.

Service Port : The TCP port number for each client service. Valid port numbers are 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 these values:

none : authorization is disabled, and login is not possible.

tacacs : use a remote TACACS+ server for authorization.

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

Cfg Cmd : Also authorize configuration commands.

Accounting Method Configuration : The accounting section allows you to configure command and exec (login) accounting. The table has one row for each client type and several columns:

Client : The management client for which the configuration below applies.

Method : Method can be set to one of these values:

no : Accounting is disabled.

tacacs : Use remote TACACS+ server(s) for accounting.

Cmd Lvl : Enable accounting of all commands with a privilege level higher than or equal to this level. Valid values are in the range 0 to 15. Leave the field empty to disable command accounting.

Exec : Enable exec (login) accounting.

Buttons

Apply : Click to save changes.

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

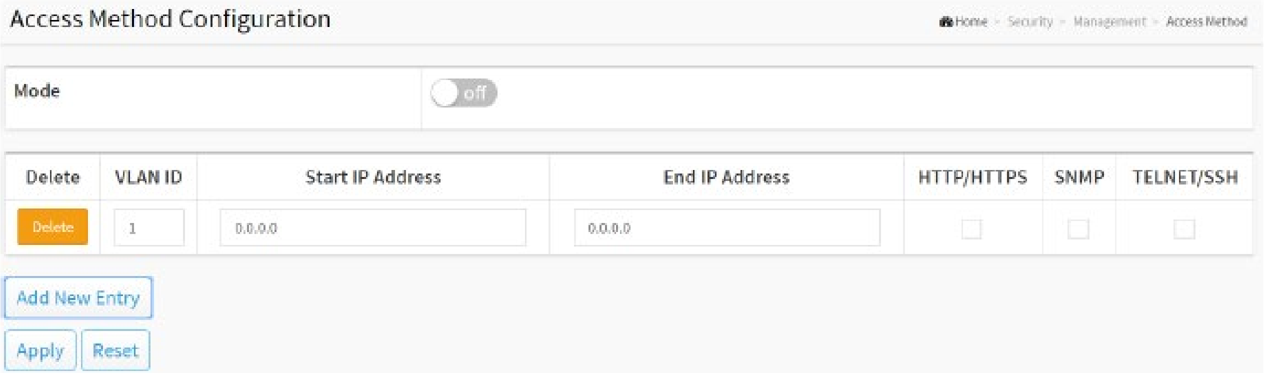
Access Method

This page lets you configure access management parameters including HTTP/HTTPS, SNMP, and TELNET/SSH. You can manage the switch over an Ethernet LAN, or over the Internet. Note: at SM12XPA FW v8.90.884 the default changed to HTTPS, and HTTP will get redirected to HTTPS. Also, SSH stays enabled, Telnet stays disabled, and you are given the option to enable Telnet.

Web Interface

To configure Access Method parameters in the web UI:

1. Click Security, Management and Access Method.
2. Select “on” in the Mode of Access Management Configuration.
3. Click “Add New Entry”.
4. Specify the VLAN ID, Start IP Address, End IP Address.
5. Check an Access Management method (HTTP/HTTPS, SNMP, and TELNET/SSH) in the entry.
6. Click Apply.



Access Method Configuration

Home › Security › Management › Access Method

Mode	off

Delete	VLAN ID	Start IP Address	End IP Address	HTTP/HTTPS	SNMP	TELNET/SSH
Delete	1	0.0.0.0	0.0.0.0	□	□	□

Figure 11-1.4: Access Method Configuration

Parameter descriptions:

Mode : Indicates the access management mode operation. Possible modes are:

> ***On*** : Enable access management mode operation.
>
> ***Off*** : Disable access management mode operation.

VLAN ID : Indicates the VLAN ID for the access management entry.

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

Start IP address : Indicates the start IP unicast address for the access management entry.

End IP address : Indicates the end IP unicast address for the access management entry.

HTTP/HTTPS : Indicates that the host can access the switch from HTTP/HTTPS interface if the host IP address matches the IP address range provided in the entry.

SNMP : Indicates that the host can access the switch from SNMP interface if the host IP address matches the IP address range provided in the entry.

TELNET/SSH : Indicates that the host can access the switch from TELNET/SSH interface if the host IP address matches the IP address range provided in the entry.

Buttons

Add New Entry : Click to add a new access management entry to the table.

Apply : Click to save changes.

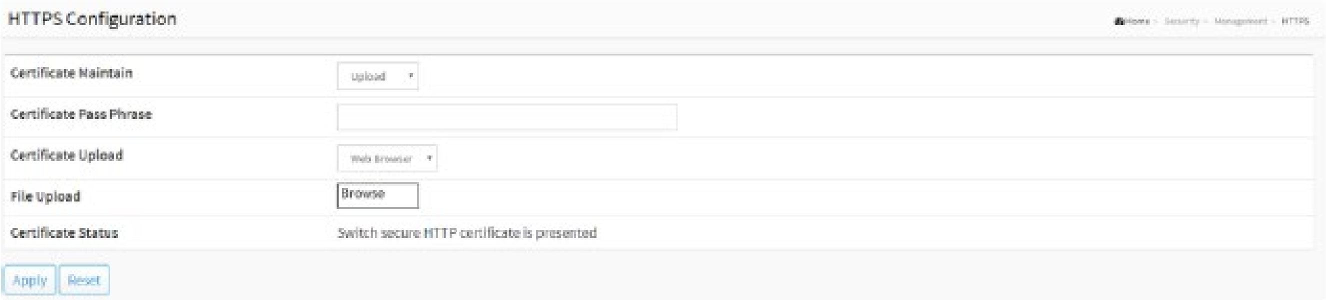
Reset : Click to undo any changes made locally and revert to previously saved values.

HTTPS

This page lets you configure HTTPS settings and maintain the current certificate on the switch.

To configure HTTPS settings in the web UI:

1. Click Configuration, Security, Management and HTTPS.
2. Specify the Certificate Maintain, Certificate Pass Phrase, Certificate Upload.
3. Click the Browse button to select the file to upload.
4. Click Apply.



HTTPS Configuration

Certificate Maintain	Upload ▾
Certificate Pass Phrase	
Certificate Upload	Web Browser ▾
File Upload	Browse
Certificate Status	Switch secure HTTP certificate is presented

Figure 11-1.5: HTTPS Configuration

Parameter descriptions:

Certificate Maintain : The operation of certificate maintenance. Possible operations are:

> ***Upload***: Upload a certificate PEM file. Possible Upload methods are ***Web Browser*** or ***URL***.
>
> ***Generate***: Generate a new self-signed RSA certificate.

Certificate Pass Phrase : Enter the pass phrase in this field if your uploading certificate is protected by a specific passphrase.

Certificate Upload : Upload a certificate PEM file into the switch. The file should contain the certificate and private key together. If you have two separated files for saving certificate and private key. Use the Linux cat command to combine them into a single PEM file. For example, cat my.cert my.key > my.pem Notice that the RSA certificate is recommended since most of the new version of browsers has removed support for DSA in certificate, e.g. Firefox v37 and Chrome v39. Possible Certificate Upload methods are:

> ***Web Browser***: Upload a certificate via Web browser.
>
> ***URL***: Upload a certificate via URL, the supported protocols are HTTP, HTTPS, TFTP and FTP. The URL format is <protocol>://[<username>[:<password>]@]< host>[:<port>][/<path>]/<file_name**>**. For example, *tftp://10.10.10.10/new_image_path/new_image.dat* or *http://username:password@10.10.10.10:80/new_image_path/new_image.dat*.
>
> A valid file name is a text string drawn from alphabet (A-Za-z), digits (0-9), dot (.), hyphen (-), and under score (_).
> The maximum length is 63 and hyphen must not be first character. A filename content that only contains '.'
> is not allowed.

Certificate Status : Display the current status of certificate on the switch. Possible statuses are:

Switch secure HTTP certificate is presented.

Switch secure HTTP certificate is not presented.

Switch secure HTTP certificate is generating ....

Buttons

Apply : Click to save changes.

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

802.1X

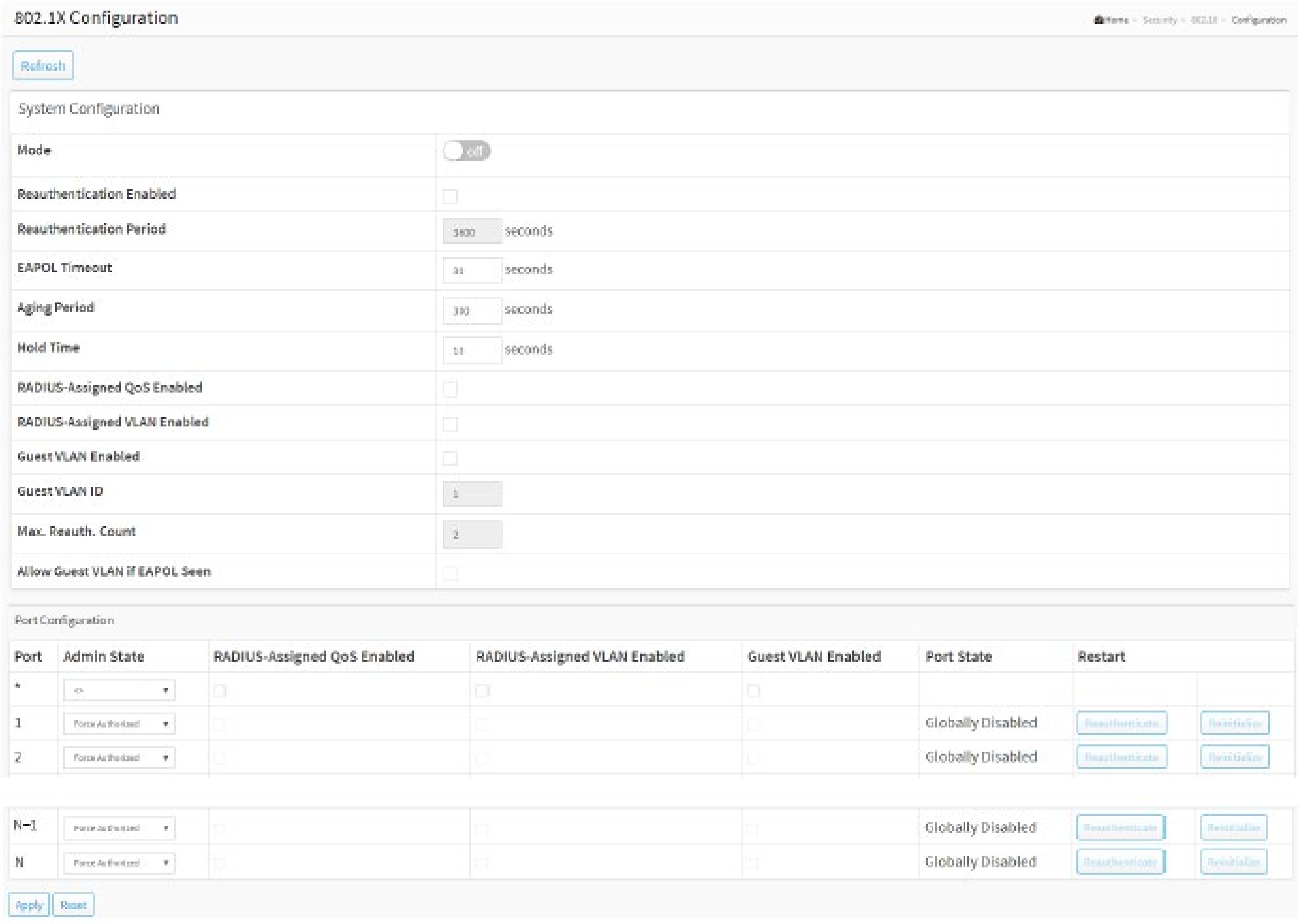
Configuration

Here you can configure the 802.1X parameters of the switch. IEEE 802.1X can be employed to connect users to a variety of resources including Internet access, conference calls, or printing documents on shared printers.

IEEE 802.1X is an IEEE Standard for port-based Network Access Control. It is part of the IEEE 802.1 group of networking protocols. It provides an authentication mechanism to devices wishing to attach to a LAN or WLAN.

To configure IEEE 802.1X in the web UI:

1. Click Security, 802.1X and Configuration.
2. Set the System Configuration section parameters.
3. Set the Port Configuration section parameters.
4. Click the Apply button to save the settings.
5. To cancel the settings, click the Reset button. It will revert to previously saved values.



802.1X Configuration

System Configuration

Mode	off
Reauthentication Enabled	□
Reauthentication Period	3600 seconds
EAPOL Timeout	30 seconds
Aging Period	300 seconds
Hold Time	10 seconds
RADIUS-Assigned QoS Enabled	□
RADIUS-Assigned VLAN Enabled	□
Guest VLAN Enabled	□
Guest VLAN ID	1
Max. Reauth. Count	2
Allow Guest VLAN if EAPOL Seen	□

Port Configuration

Port	Admin State	RADIUS-Assigned QoS Enabled	RADIUS-Assigned VLAN Enabled	Guest VLAN Enabled	Port State	Restart	
*	<>	□	□	□			
1	Force Authorized	□	□	□	Globally Disabled	Reauthenticate	Reinitialize
2	Force Authorized	□	□	□	Globally Disabled	Reauthenticate	Reinitialize
N-1	Force Authorized	□	□	□	Globally Disabled	Reauthenticate	Reinitialize
N	Force Authorized	□	□	□	Globally Disabled	Reauthenticate	Reinitialize

Figure 11-2.1: IEEE 802.1X Configuration

Parameter descriptions:

System Configuration

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

Reauthentication Enabled : If checked, successfully authenticated supplicants/clients are reauthenticated after the interval specified by the Reauthentication Period. Reauthentication for 802.1X-enabled ports can be used to detect if a new device is plugged into a switch port or if a supplicant is no longer attached.

For MAC-based ports, reauthentication is only useful if the RADIUS server configuration has changed. It does not involve communication between the switch and the client, and therefore doesn't imply that a client is still present on a port (see Aging Period below).

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

EAPOL Timeout : Determines the time for retransmission of Request Identity EAPOL frames. IEEE 802.1X defines the encapsulation of the Extensible Authentication Protocol (EAP) over IEEE 802.11, known as "EAP over LAN" or EAPOL. EAPOL was originally designed for IEEE 802.3 Ethernet in 802.1X-2001.Valid values are 1 - 65535 seconds. This has no effect on MAC-based ports.

Aging Period : This setting applies to the following modes (i.e., modes using the Port Security functionality to secure MAC addresses):

Single 802.1X

Multi 802.1X

MAC-Based Auth.

When the NAS module uses the Port Security module to secure MAC addresses, the Port Security module needs to check for activity on the MAC address in question at regular intervals and free resources if no activity is seen within a given period of time. This parameter controls exactly this period and can be set to a number between 10 and 1000000 seconds. If reauthentication is enabled and the port is in an 802.1X-based mode, this is not so critical, since supplicants that are no longer attached to the port will get removed upon the next reauthentication, which will fail. But if reauthentication is not enabled, the only way to free resources is by aging the entries. For ports in MAC-based Auth. mode, reauthentication doesn't cause direct communication between the switch and the client, so this will not detect whether the client is still attached or not, and the only way to free any resources is to age the entry.

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

Single 802.1X

Multi 802.1X

MAC-Based Auth.

If a client is denied access - either because the RADIUS server denies the client access or because the RADIUS server request times out (according to the timeout specified on the "Configuration > Security > AAA" page) - the client is put on hold in the Unauthorized state. The hold timer does not count during an on-going authentication. In MAC-based Auth. mode, the switch will ignore new frames coming from the client during the hold time. The Hold Time can be set to a number between 10 and 1000000 seconds.

RADIUS-Assigned QoS Enabled : RADIUS-assigned QoS provides a means to centrally control the traffic class to which traffic coming from a successfully authenticated supplicant is assigned on the switch. The RADIUS server must be configured to transmit special RADIUS attributes to take advantage of this feature (see RADIUS-Assigned QoS Enabled below for a detailed description). The "RADIUS-Assigned QoS Enabled" checkbox provides a quick way to globally enable/disable RADIUS-server assigned QoS Class functionality. When checked, the individual ports' ditto setting determines whether RADIUS-assigned QoS Class is enabled on that port. When unchecked, RADIUS-server assigned QoS Class is disabled on all ports.

RADIUS-Assigned VLAN Enabled : RADIUS-assigned VLAN provides a means to centrally control the VLAN on which a successfully authenticated supplicant is placed on the switch. Incoming traffic will be classified to and switched on the RADIUS-assigned VLAN. The RADIUS server must be configured to transmit special RADIUS attributes to take advantage of this feature (see RADIUS-Assigned VLAN Enabled below for a detailed description). The "RADIUS-Assigned VLAN Enabled" checkbox provides a quick way to globally enable/disable RADIUS-server assigned VLAN functionality. When checked, the individual ports' ditto setting determines whether RADIUS-assigned VLAN is enabled on that port. When unchecked, RADIUS-server assigned VLAN is disabled on all ports.

Guest VLAN Enabled : A Guest VLAN is a special VLAN - typically with limited network access - on which 802.1X-unaware clients are placed after a network administrator-defined timeout. The switch follows a set of rules for entering and leaving the Guest VLAN as listed below. The "Guest VLAN Enabled" checkbox provides a quick way to globally enable/disable Guest VLAN functionality. When checked, the individual 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 can only be changed if the Guest VLAN option is globally enabled. Valid values are in the range [1; 4094].

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

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

Port Configuration

Port : The port number for which the configuration below applies.

Admin State : If 802.1X is globally enabled, this selection sets the port's authentication mode. These modes are available:

> ***Force Authorized*** : In this mode, the switch will send one EAPOL Success frame when the port link comes up, and any client on the port will be allowed network access without authentication.
>
> ***Force Unauthorized*** : In this mode, the switch will send one EAPOL Failure frame when the port link comes up, and any client on the port will be disallowed network access.
>
> ***Port-based 802.1X*** : In the 802.1X-world, the user is called the supplicant, the switch is the authenticator, and the RADIUS server is the authentication server. The authenticator acts as the man-in-the-middle, forwarding requests and responses between the supplicant and the authentication server.

Frames sent between the supplicant and the switch are special 802.1X frames, known as EAPOL (EAP Over LANs) frames. EAPOL frames encapsulate EAP PDUs (RFC3748). Frames sent between the switch and the RADIUS server are RADIUS packets. RADIUS packets also encapsulate EAP PDUs together with other attributes like the switch's IP address, name, and the supplicant's port number on the switch. EAP is very flexible, in that it allows for different authentication methods, like MD5-Challenge, PEAP, and TLS. The important thing is that the authenticator (the switch) doesn't need to know which authentication method the supplicant and the authentication server are using, or how many information exchange frames are needed for a particular method. The switch simply encapsulates the EAP part of the frame into the relevant type (EAPOL or RADIUS) and forwards it.

When authentication is complete, the RADIUS server sends a special packet containing a success or failure indication. Besides forwarding this decision to the supplicant, the switch uses it to open up or block traffic on the switch port connected to the supplicant.

Note: Suppose two backend servers are enabled and that the server timeout is configured to X seconds (using the AAA configuration page) and suppose that the first server in the list is currently down (but not considered dead). Now, if the supplicant retransmits EAPOL Start frames at a rate faster than X seconds, then it will never get authenticated, because the switch will cancel on-going backend authentication server requests whenever it receives a new EAPOL Start frame from the supplicant. And since the server hasn't yet failed (because the X seconds haven't expired), the same server will be contacted upon the next backend authentication server request from the switch. This scenario will loop forever. Therefore, the server timeout should be smaller than the supplicant's EAPOL Start frame retransmission rate.

Single 802.1X : In port-based 802.1X authentication, once a supplicant is successfully authenticated on a port, the whole port is opened for network traffic. This allows other clients connected to the port (for instance through a hub) to piggy-back on the successfully authenticated client and get network access even though they really aren't authenticated. To overcome this security breach, use the Single 802.1X variant. Single 802.1X is really not an IEEE standard, but features many of the same characteristics as does port-based 802.1X. In Single 802.1X, at most one supplicant can get authenticated on the port at a time. Normal EAPOL frames are used in the communication between the supplicant and the switch. If more than one supplicant is connected to a port, the one that comes first when the port's link comes up will be the first one considered. If that supplicant doesn't provide valid credentials within a certain amount of time, another supplicant will get a chance. Once a supplicant is successfully authenticated, only that supplicant will be allowed access. This is the most secure of all the supported modes. In this mode, the Port Security module is used to secure a supplicant's MAC address once successfully authenticated.

Multi 802.1X : In port-based 802.1X authentication, once a supplicant is successfully authenticated on a port, the whole port is opened for network traffic. This allows other clients connected to the port (for instance through a hub) to piggy-back on the successfully authenticated client and get network access even though they really aren't authenticated. To overcome this security breach, use the Multi 802.1X variant.

Multi 802.1X is really not an IEEE standard, but features many of the same characteristics as does port-based 802.1X. Multi 802.1X is - like Single 802.1X - not an IEEE standard, but a variant that features many of the same characteristics. In Multi 802.1X, one or more supplicants can get authenticated on the same port at the same time. Each supplicant is authenticated individually and secured in the MAC table using the Port Security module.

In Multi 802.1X it is not possible to use the multicast BPDU MAC address as destination MAC address for EAPOL frames sent from the switch towards the supplicant, since that would cause all supplicants attached to the port to reply to requests sent from the switch. Instead, the switch uses the supplicant's

MAC address, which is obtained from the first EAPOL Start or EAPOL Response Identity frame sent by the supplicant. An exception to this is when no supplicants are attached. In this case, the switch sends EAPOL Request Identity frames using the BPDU multicast MAC address as destination - to wake up any supplicants that might be on the port.

The maximum number of supplicants that can be attached to a port can be limited using the Port Security Limit Control functionality.

MAC-based Auth.: Unlike port-based 802.1X, MAC-based authentication is not a standard, but merely a best-practices method adopted by the industry. In MAC-based authentication, users are called clients, and the switch acts as the supplicant on behalf of clients. The initial frame (any kind of frame) sent by a client is snooped by the switch, which in turn uses the client's MAC address as both username and password in the subsequent EAP exchange with the RADIUS server. The 6-byte MAC address is converted to a string on the following form "xx-xx-xx-xx-xx-xx", that is, a dash (-) is used as separator between the lower-cased hexadecimal digits. The switch only supports the MD5-Challenge authentication method, so the RADIUS server must be configured accordingly.

When authentication is complete, the RADIUS server sends a success or failure indication, which in turn causes the switch to open up or block traffic for that particular client, using the Port Security module. Only then will frames from the client be forwarded on the switch. There are no EAPOL frames involved in this authentication, and therefore, MAC-based Authentication has nothing to do with the 802.1X standard.

The advantage of MAC-based authentication over port-based 802.1X is that several clients can be connected to the same port (e.g., through a 3rd party switch or a hub) and still require individual authentication, and that the clients don't need special supplicant software to authenticate.
The advantage of MAC-based authentication over 802.1X-based authentication is that the clients don't need special supplicant software to authenticate. The disadvantage is that MAC addresses can be spoofed by malicious users - equipment whose MAC address is a valid RADIUS user can be used by anyone. Also, only the MD5-Challenge method is supported. The maximum number of clients that can be attached to a port can be limited using the Port Security Limit Control functionality.

RADIUS-Assigned QoS Enabled : When RADIUS-Assigned QoS is both globally enabled and enabled (checked) on a given port, the switch reacts to QoS Class information carried in the RADIUS Access-Accept packet transmitted by the RADIUS server when a supplicant is successfully authenticated. If present and valid, traffic received on the supplicant's port will be classified to the given QoS Class. If (re-)authentication fails or the RADIUS Access-Accept packet no longer carries a QoS Class or it's invalid, or the supplicant is otherwise no longer present on the port, the port's QoS Class is immediately reverted to the original QoS Class (which may be changed by the administrator in the meanwhile without affecting the RADIUS-assigned). This option is only available for single-client modes, i.e.:

- Port-based 802.1X
- Single 802.1X RADIUS attributes used in identifying a QoS Class: The User-Priority-Table attribute defined in RFC4675 forms the basis for identifying the QoS Class in an Access-Accept packet. Only the first occurrence of the attribute in the packet will be considered, and to be valid, it must follow this rule:
- All 8 octets in the attribute's value must be identical and consist of ASCII characters in the range '0' - '7', which translates into the desired QoS Class in the range [0; 7].

RADIUS-Assigned VLAN Enabled : When RADIUS-Assigned VLAN is both globally enabled and enabled (checked) for a given port, the switch reacts to VLAN ID information carried in the RADIUS Access-Accept packet transmitted by the RADIUS server when a supplicant is successfully authenticated. If present and valid, the port's Port VLAN ID will be changed to this VLAN ID, the port will be set to be a member of that VLAN ID, and the port will be forced into VLAN unaware mode. Once assigned, all traffic arriving on the port will be classified and switched on the RADIUS-assigned VLAN ID. If (re-)authentication fails or the RADIUS Access-Accept packet no longer carries a VLAN ID or it's invalid, or the supplicant is otherwise no longer present on the port, the port's VLAN ID is immediately reverted to the original VLAN ID (which may be changed by the administrator in the meanwhile without affecting the RADIUS-assigned). This option is only available for single-client modes, such as:

- Port-based 802.1X
- Single 802.1X

For troubleshooting VLAN assignments, use the "Monitor > VLANs > VLAN Membership and VLAN Port" pages. These pages show which modules have (temporarily) overridden the current Port VLAN configuration. RADIUS attributes used in identifying a VLAN ID: RFC2868 and RFC3580 form the basis for the attributes used in identifying a VLAN ID in an Access-Accept packet. The following criteria are used:

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

Guest VLAN Enabled : When Guest VLAN is both globally enabled and enabled (checked) for a given port, the switch considers moving the port into the Guest VLAN according to the rules outlined below. This option is only available for EAPOL-based modes, i.e.:

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

For troubleshooting VLAN assignments, use the Monitor > VLANs > VLAN Membership and VLAN Port pages. These pages show which modules have (temporarily) overridden the current Port VLAN configuration. Guest VLAN Operation: When a Guest VLAN enabled port's link comes up, the switch starts transmitting EAPOL Request Identity frames. If the number of transmissions of such frames exceeds Max. Reauth. Count and no EAPOL frames have been received in the meanwhile, the switch considers entering the Guest VLAN. The interval between transmission of EAPOL Request Identity frames is configured with EAPOL Timeout. If Allow Guest VLAN if EAPOL Seen is enabled, the port will now be placed in the Guest VLAN. If disabled, the switch will first check its history to see if an EAPOL frame has previously been received on the port (this history is cleared if the port link goes down or the port's Admin State is changed), and if not, the port will be placed in the Guest VLAN. Otherwise it will not move to the Guest VLAN, but continue transmitting EAPOL Request Identity frames at the rate given by EAPOL Timeout. Once in the Guest VLAN, the port is considered authenticated, and all attached clients on the port are allowed access on this VLAN. The switch will not transmit an EAPOL Success frame when entering the Guest VLAN. While in the Guest VLAN, the switch monitors the link for EAPOL frames, and if one such frame is received, the switch immediately takes the port out of the Guest VLAN and starts authenticating the supplicant according to the port mode. If an EAPOL frame is received, the port will never be able to go back into the Guest VLAN if the "Allow Guest VLAN if EAPOL Seen" is disabled.

Port State : The current state of the port. It can undertake one of the following values:

Globally Disabled: IEEE 802.1X is globally disabled.

Link Down: IEEE 802.1X is globally enabled, but there is no link on the port.

Authorized: The port is in Force Authorized or a single-supplicant mode and the supplicant is authorized.

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

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

Restart : Two buttons are available for each row. The buttons are only enabled when authentication is globally enabled and the port's Admin State is in an EAPOL-based or MAC-based mode. Clicking these buttons will not cause settings changed on the page to take effect:

Re-authenticate: Schedules a re-authentication whenever the quiet-period of the port runs out (EAPOL-based authentication). For MAC-based authentication, re-authentication will be attempted immediately. The button only has effect for successfully authenticated clients on the port and will not cause the clients to get temporarily unauthorized.

Reinitialize: Forces a re-initialization of the clients on the port and thereby a re-authentication immediately. The clients will transfer to the unauthorized state while the re-authentication is in progress.

Buttons

Apply : Click to save changes.

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

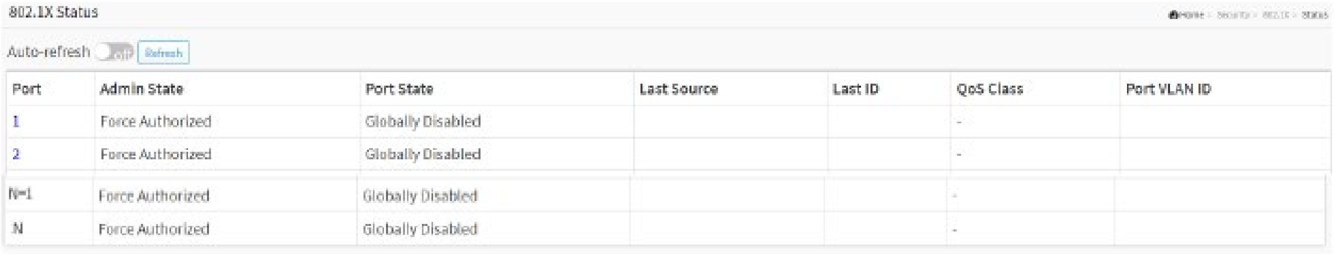
Status

This page displays port 802.1X status information of the switch. The status includes Admin State, Port State, Last Source, Last ID, QoS Class, and Port VLAN ID.

Web Interface

To display 802.1X Status in the web UI:

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



Port	Admin State	Port State	Last Source	Last ID	QoS Class	Port VLAN ID
1	Force Authorized	Globally Disabled			-	
2	Force Authorized	Globally Disabled			-	
N-1	Force Authorized	Globally Disabled			-	
N	Force Authorized	Globally Disabled			-	

Figure 11-2.2: IEEE 802.1X Status

Parameter descriptions:

<u>802.1X Status</u>

Port : The switch port number. Click to navigate to the 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.

QoS Class : The QoS Class assigned to the port by the RADIUS server if enabled.

Port VLAN ID : The VLAN ID that 802.1X has put the port in. The field is blank if the Port VLAN ID is not overridden by 802.1X.

If the VLAN ID is assigned by the RADIUS server, "(RADIUS-assigned)" is appended to the VLAN ID. Read more about RADIUS-assigned VLANs on page 194.

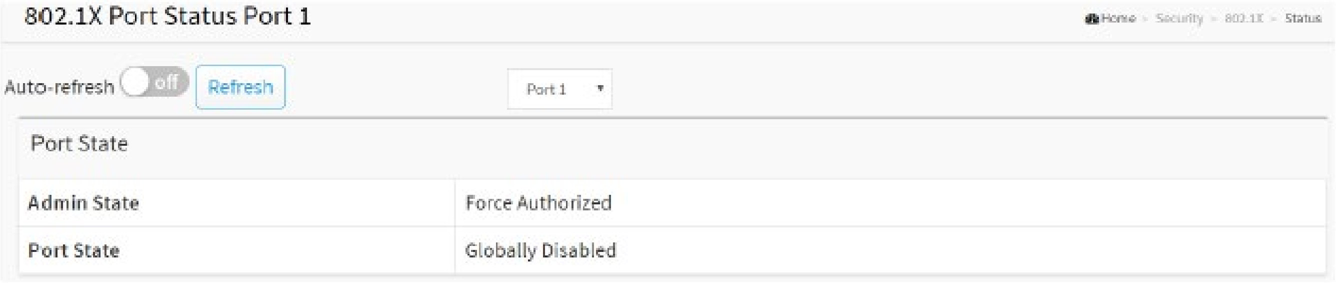
If the port is moved to the Guest VLAN, "(Guest)" is appended to the VLAN ID. Read more about Guest VLANs on page 194.

Buttons

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

Refresh : Click to refresh the page immediately.

If you select port1 to display 802.1X Statistics:



802.1X Port Status Port 1

Port State

Admin State	Force Authorized
Port State	Globally Disabled

Parameter descriptions:

Port select box: At the dropdown select which port that you want display 802.1X Statistics.

Admin State : The port's current administrative state. Refer to 802.1X Admin State for a description of possible values.

Port State : The current state of the port. Refer to 802.1X Port State for a description of the individual states.

Buttons

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

Refresh : Click to manually refresh the page immediately.

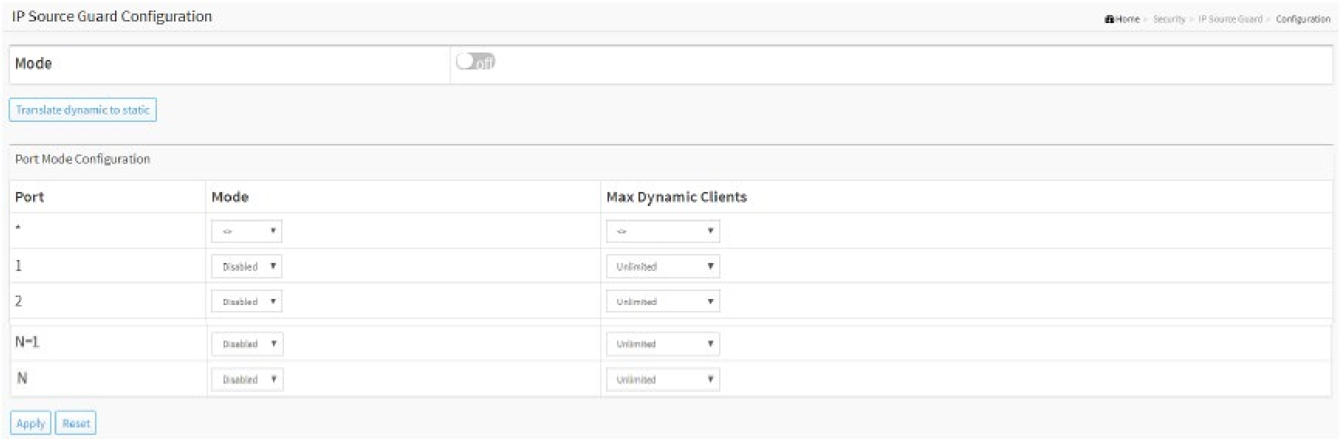
IP Source Guard

This page lets you configure IP Source Guard detail parameters of the switch. You can configure IP Source Guard parameters to enable or disable switch ports.

Configuration

To configure IP Source Guard in the web UI:

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

Home > Security > IP Source Guard > Configuration

Mode	off

Translate dynamic to static

Port Mode Configuration

Port	Mode	Max Dynamic Clients
*	<>	<>
1	Disabled	Unlimited
2	Disabled	Unlimited
N-1	Disabled	Unlimited
N	Disabled	Unlimited

Figure 11-3.1: IP Source Guard Configuration

Parameter descriptions :

Mode of IP Source Guard Configuration : Select ***on*** to enable the Global IP Source Guard or select ***off*** to disable the Global IP Source Guard. All configured ACEs will be lost when the mode is on (enabled.

Port Mode Configuration : Specify IP Source Guard is enabled on which ports. Only when both Global Mode and Port Mode on a given port are enabled, IP Source Guard is enabled on this given port.

Max Dynamic Clients : Specify the maximum number of dynamic clients that can be learned on given port. This value can be 0, 1, 2 or unlimited. If the Port Mode is enabled and the value of Max Dynamic Clients is 0, it means only allow the IP packets forwarding that are matched in static entries on the specific port.

Buttons

Apply : Click to save changes.

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

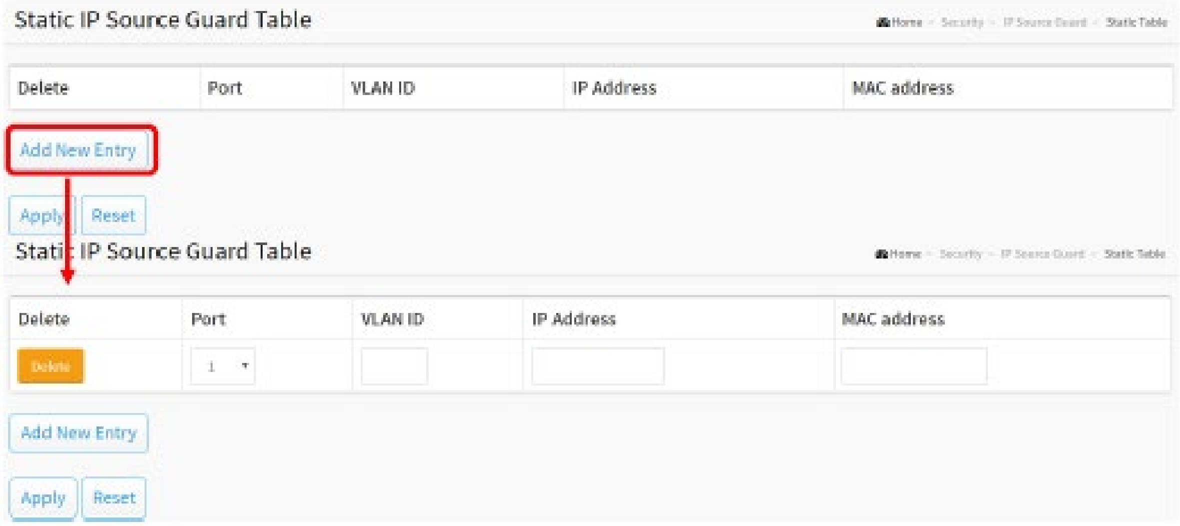
Translate dynamic to static : Click to translate all dynamic entries to static entries.

Static Table

This page lets you configure Static IP Source Guard Table parameters. You can use the Static IP Source Guard Table configure to manage the entries.

To configure Static IP Source Guard in the web UI:

1. Click Security, IP Source Guard 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 IP Source Guard Table

Home » Security » IP Source Guard » Static Table

Delete	Port	VLAN ID	IP Address	MAC address

Add New Entry

Apply Reset

Static IP Source Guard Table

Home » Security » IP Source Guard » Static Table

Delete	Port	VLAN ID	IP Address	MAC address
Delete	1 ▾			

Add New Entry

Apply Reset

Figure 11-3.2: Static IP Source Guard Table

Parameter descriptions :

Port : At the dropdown select the logical port for the settings.

VLAN ID : The VID 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.

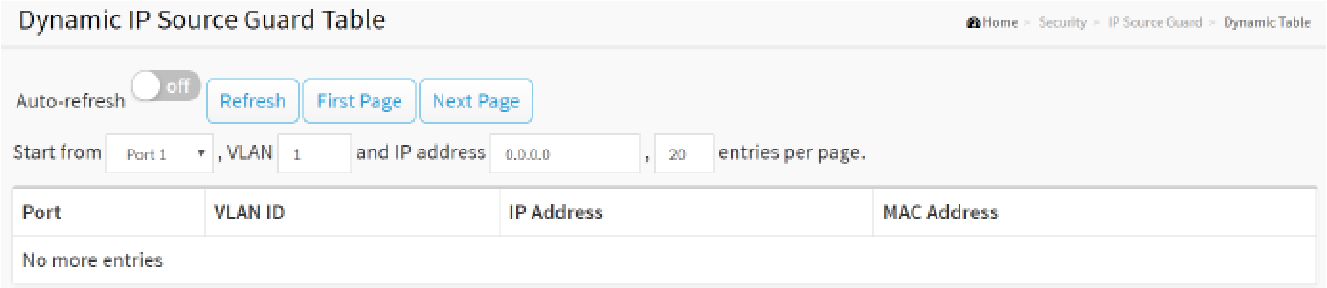
Reset : Click to undo any changes made locally and revert to previously saved values.

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.

To configure Dynamic IP Source Guard Table parameters in the web UI:

1. Click Security, IP Source Guard and Dynamic Table.
2. Check “Auto-refresh”.
3. Click “Refresh” to refresh the port detailed statistics.
4. Click First Page/Next Page to change page.
5. Specify the Start from port, VLAN, IP Address, and entries per page.


Dynamic IP Source Guard Table
Home > Security > IP Source Guard > Dynamic Table
Auto-refresh
off
Refresh
First Page
Next Page

Start from Port 1, VLAN 1 and IP address 0.0.0.0, 20 entries per page.

Port	VLAN ID	IP Address	MAC Address
No more entries			

Figure 11-3.3: Dynamic IP Source Guard Table

Parameter descriptions :

Port : The switch Port number for which the entries are displayed.

VLAN ID : The VLAN ID in which the IP traffic is permitted.

IP Address : The User IP address of the entry.

MAC Address : The Source MAC address.

Buttons

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

Refresh : Click to refresh the page immediately.

First Page : Updates the table starting from the first entry in the Dynamic IP Source Guard Table.

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

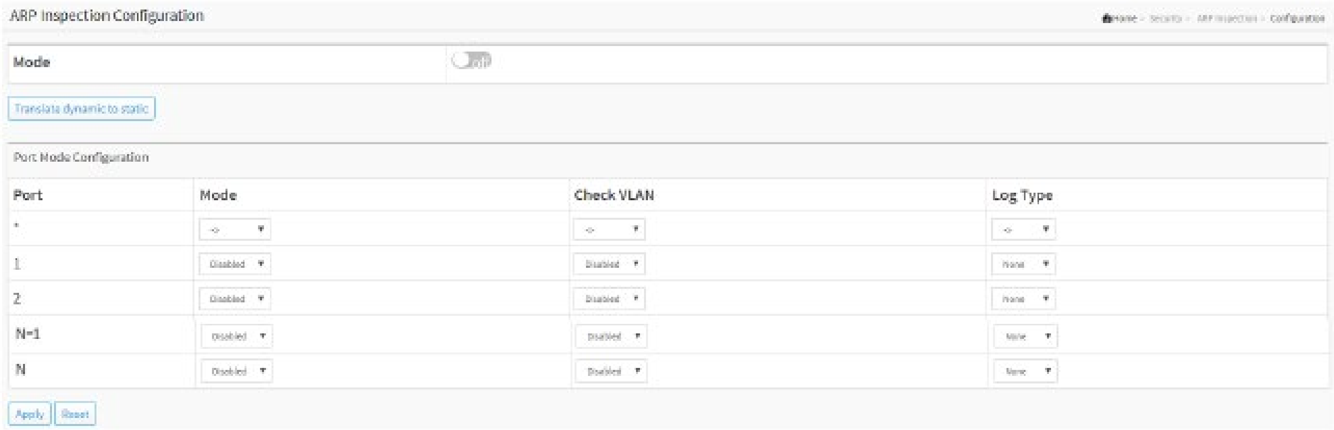
ARP Inspection

This page lets you configure ARP Inspection parameters. You can use ARP Inspection to manage the ARP table.

Configuration

To configure ARP Inspection in the web UI:

1. Click Security, ARP Inspection and Configuration.
2. Select “on” as the Mode in the ARP Inspection Configuration section.
3. Select “Enabled” for the specific port(s) at the Mode dropdown in the Port Mode Configuration section.
4. Set the Port Mode Configuration section parameters.
5. Click the “Translate dynamic to static” button to translate all dynamic entries to static entries.
6. Click Apply.



ARP Inspection Configuration

Home > Security > ARP Inspection > Configuration

Mode: off

Translate dynamic to static

Port Mode Configuration

Port	Mode	Check VLAN	Log Type
*	<>	<>	<>
1	Disabled	Disabled	None
2	Disabled	Disabled	None
N-1	Disabled	Disabled	None
N	Disabled	Disabled	None

Figure 11-4.1: ARP Inspection Configuration

Parameter descriptions :

ARP Inspection Configuration section :

Mode : Select ***on*** to enable ARP Inspection globally or select ***off*** to disable ARP Inspection globally. The default is disabled (off).

Port Mode Configuration section :

Mode: Set ARP Inspection to Enabled or Disabled on each port. ARP Inspection is enabled on a given port only when both Global Mode and Port Mode on a given port are enabled. Possible modes are:

Enabled: Enable ARP Inspection operation.

Disabled: Disable ARP Inspection operation.

Check VLAN : To inspect the VLAN configuration, the "Check VLAN" parameter must be enabled. The default setting of "Check VLAN" is disabled. The possible settings are:

Disabled : the log type of ARP Inspection will refer to the port setting. Disable check VLAN operation. Only the Global Mode and Port Mode on a given port are enabled, and the setting of "Check VLAN" is disabled, the log type of ARP Inspection will refer to the port setting.

Enabled : Enable check VLAN operation; the log type of ARP Inspection will refer to the VLAN setting.

Log Type : The four possible log types are:

None: Log nothing.

Deny: Log only denied entries.

Permit: Log only permitted entries.

ALL: Log all entries.

Buttons

Translate dynamic to static : Click to translate all dynamic entries to static entries.

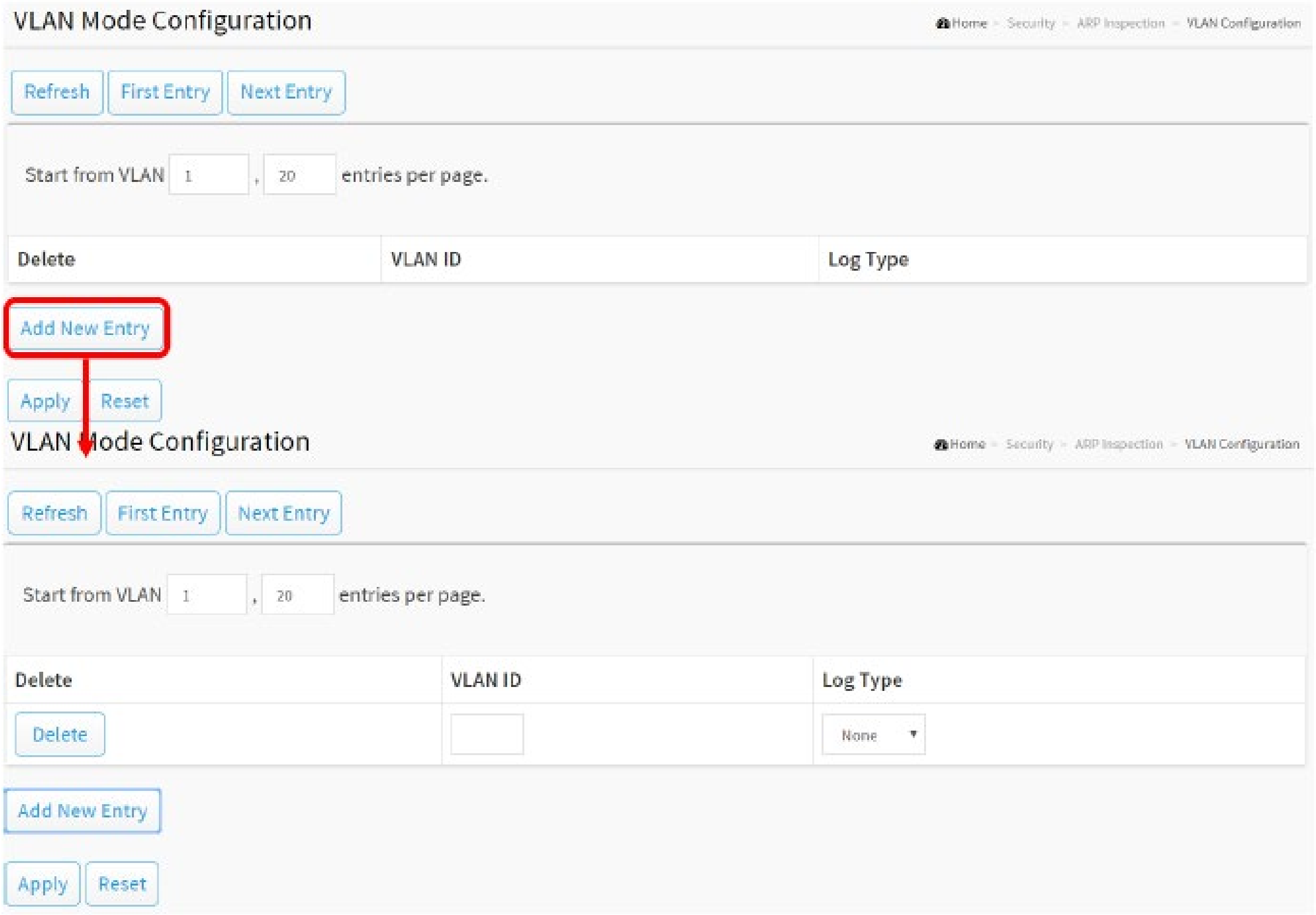
Apply : Click to save changes.

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

VLAN Configuration

Specify on which VLANs ARP Inspection is enabled and the type of logging to be used:

1. Click Security, ARP Inspection, and VLAN Configuration.
2. Click “Add New Entry”.
3. Specify the VLAN ID, Log Type.
4. Click Apply.
5. Click First Entry/Next Entry to change Entry.



Start from VLAN 1 , 20 entries per page.

Delete	VLAN ID	Log Type

Start from VLAN 1 , 20 entries per page.

Delete	VLAN ID	Log Type
Delete		None ▾

Figure 11-4.2: VLAN Mode Configuration

Parameter descriptions:

VLAN Mode Configuration : Specify ARP Inspection is enabled on which VLANs. First, you must enable the port setting on the 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, specify which VLAN will be inspected on the VLAN Mode Configuration web page. The log type also can be configured on a per VLAN basis.

Possible Log types are: ***None***: Log nothing. ***Deny***: Log only denied entries. ***Permit***: Log only permitted entries. ***ALL***: Log all entries.

Buttons

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

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

Apply : Click to save changes.

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

First Entry : Updates the table starting from the first entry in the VLAN Mode Configuration table.

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

Refresh : Click to refresh the page immediately.

Static Table

This page lets you view and set Static ARP Inspection parameters of the switch. You can use the Static ARP Inspection Table to manage ARP entries.

To configure Static ARP Inspection parameters in the web UI:

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

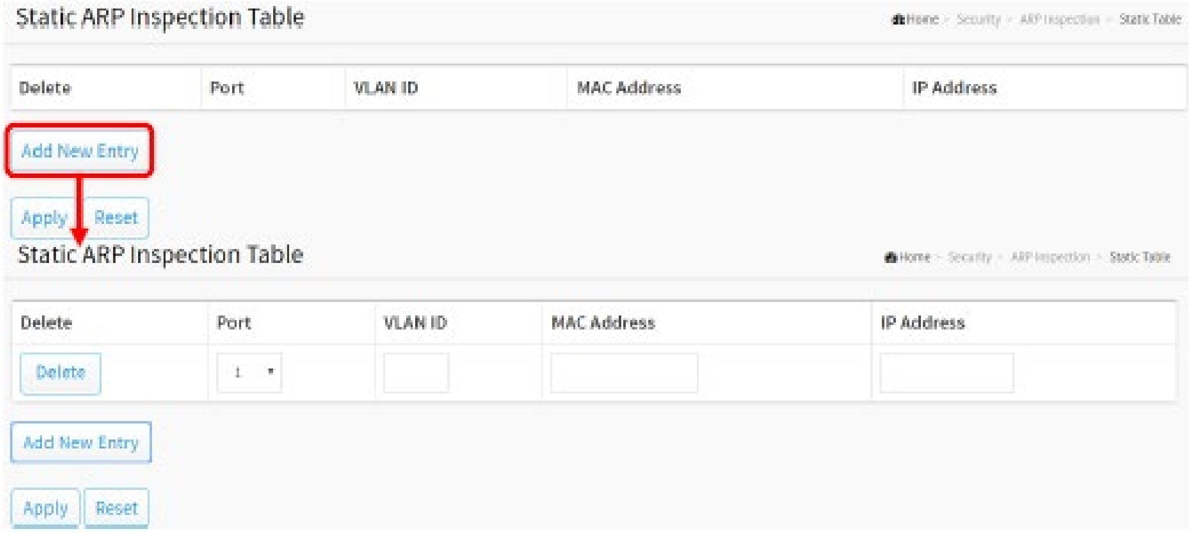

Static ARP Inspection Table
Home > Security > ARP Inspection > Static Table
Delete
Port
VLAN ID
MAC Address
IP Address
Add New Entry
Apply
Reset
Static ARP Inspection Table
Home > Security > ARP Inspection > Static Table
Delete
Port
VLAN ID
MAC Address
IP Address
Delete
1
Add New Entry
Apply
Reset

Figure11-4.3: Static ARP Inspection Table

Parameter descriptions:

Port : At the dropdown select the logical port for the settings.

VLAN ID : The VLAN ID (VID) for the settings.

MAC Address : Allowed Source MAC address in ARP request packets.

IP Address : Allowed Source IP address in ARP request packets.

Buttons

Add New Entry : Click to add a new entry to the Static ARP Inspection table.

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

Apply : Click to save changes.

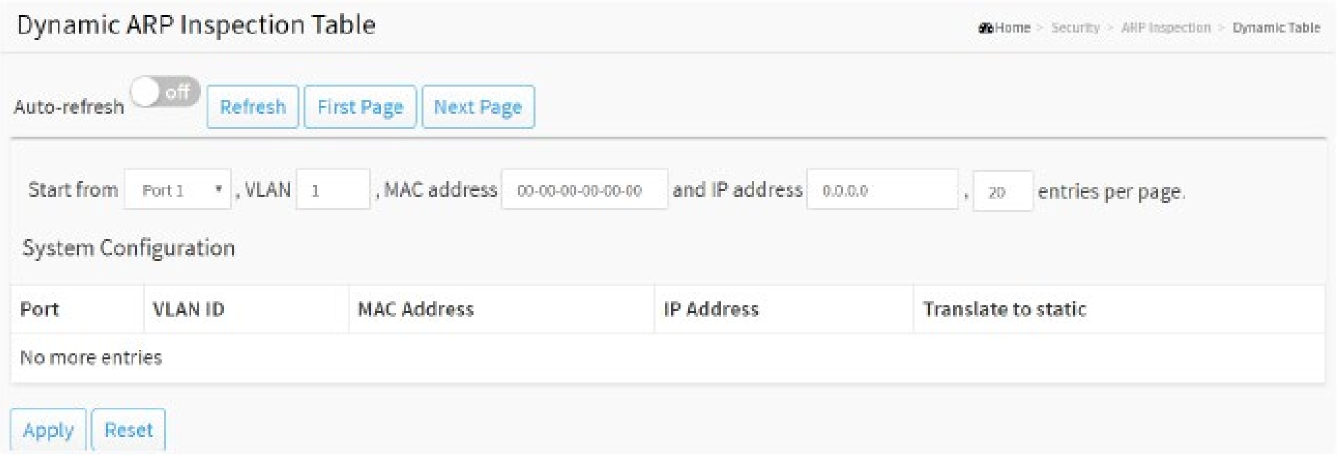
Reset : Click to undo any changes made locally and revert to previously saved values.

Dynamic Table

Entries in the Dynamic ARP Inspection Table are shown on this page. The Dynamic ARP Inspection Table can contain up to 256 entries, and is sorted first by port, then by VLAN ID, then by MAC address, and then by IP address. All dynamic entries are learned from DHCP Snooping.

To configure Dynamic ARP Inspection in the web UI:

1. Click Security, ARP Inspection, and Dynamic Table.
2. Specify the Start from port, VLAN, MAC Address, IP Address, and entries per page.
3. Check “Auto-refresh” or click “Refresh” to refresh the port detailed statistics.
4. Click First/Next Page to change page.



Dynamic ARP Inspection Table

Start from Port 1, VLAN 1, MAC address 00-00-00-00-00-00 and IP address 0.0.0.0, 20 entries per page.

System Configuration

Port	VLAN ID	MAC Address	IP Address	Translate to static
No more entries				

Figure 11-4.4: Dynamic ARP Inspection Table

Parameter descriptions:

Port : The switch Port number for which the entries are displayed.

VLAN ID : The VLAN ID in which the ARP traffic is permitted.

MAC Address : The user MAC address of the entry.

IP Address : The user IP address of the entry.

Buttons

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

Refresh : Click to refresh the page immediately.

First Page : Updates the table starting from the first entry in the Dynamic ARP Inspection Table.

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

Apply : Click to save changes.

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

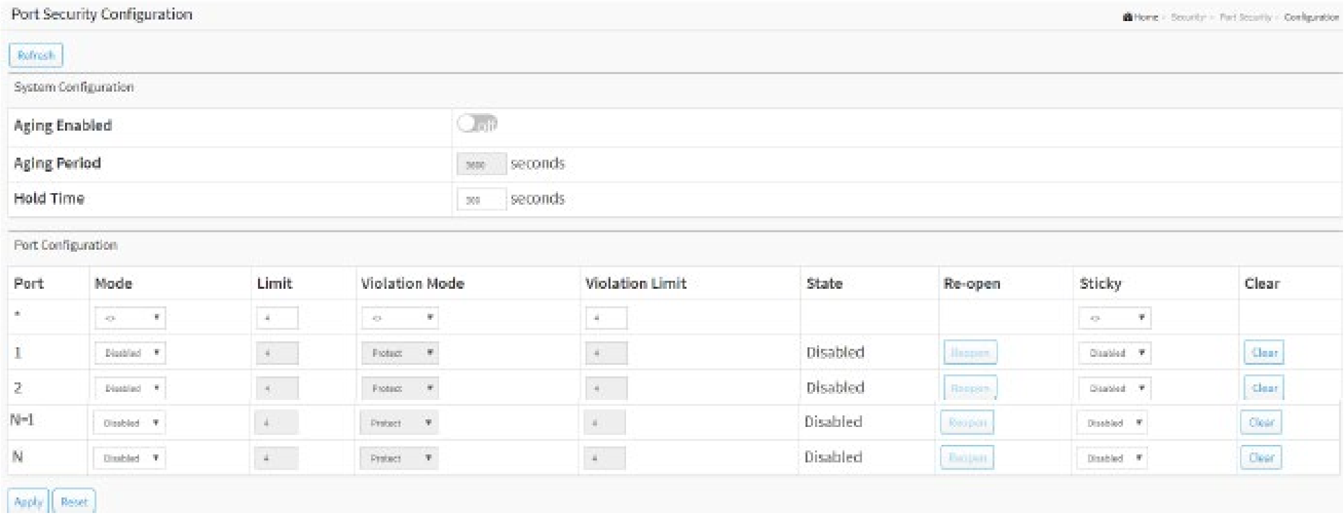
Port Security

Configuration

This page lets you configure Port Security settings. You can use the Port Security feature to restrict input to an interface by limiting and identifying MAC addresses.

To configure Port Security in the web UI:

1. Click Security, Port Security, and Configuration.
2. Set the System Configuration section parameters.
3. Set the Port Configuration section parameters.
4. Click the Apply button to save the settings.
5. To cancel the settings click the Reset button. It will revert to previously saved values.



Port Security Configuration

System Configuration

Aging Enabled	off
Aging Period	3600 seconds
Hold Time	300 seconds

Port Configuration

Port	Mode	Limit	Violation Mode	Violation Limit	State	Re-open	Sticky	Clear
*	<>	4	<>	4			<>	
1	Disabled	4	Protect	4	Disabled	Reopen	Disabled	Clear
2	Disabled	4	Protect	4	Disabled	Reopen	Disabled	Clear
N-1	Disabled	4	Protect	4	Disabled	Reopen	Disabled	Clear
N	Disabled	4	Protect	4	Disabled	Reopen	Disabled	Clear

Figure 11-5.1: Port Security Configuration

Parameter descriptions:

System Configuration

Aging Enabled : If checked (on), secured MAC addresses are subject to aging as discussed under Aging Period .

Aging Period : If Aging Enabled is checked (on), then the aging period is controlled with this input. If other modules are using the underlying functionality for securing MAC addresses, they may have other requirements to the aging period. The underlying functionality will use the shorter requested aging period of all modules that have aging enabled.

The Aging Period can be set to a number between 10 and 10000000 seconds with a default of 3600 seconds.

To understand why aging may be desired, consider the following scenario: Suppose an end-host is connected to a 3rd party switch or hub, which in turn is connected to a port on this switch on which Port Security is enabled. The end-host will be allowed to forward if the limit is not exceeded. Now suppose that the end-host logs off or powers down. If it wasn't for aging, the end-host would still take up resources on this switch and will be allowed to forward. To overcome this situation, enable aging. With aging enabled, a timer is started once the end-host gets secured. When the timer expires, the switch starts looking for frames from the end-host, and if such frames are not seen within the next Aging Period, the end-host is assumed to be disconnected, and the corresponding resources are freed on the switch.

Hold Time : The hold time - measured in seconds - is used to determine how long a MAC address is held in the MAC table if it has been found to violate the limit. The valid range is 10 - 10000000 seconds with a default of 300 seconds. The reason for holding a violating MAC address in the MAC table is primarily to ensure that the same MAC address doesn't give rise to continuous notifications (if notifications on violation count is enabled).

Port Configuration : The table has one row for each port on the selected switch and several columns:

Port : The port number to which the configuration below applies.

Mode : Controls whether Limit Control is enabled on this port. Both this and the Global Mode must be set to Enabled for Limit Control to be in effect. Notice that other modules may still use the underlying port security features without enabling Limit Control on a given port.

Limit : The maximum number of MAC addresses that can be secured on this port. This number cannot exceed 1024. If the limit is exceeded, the corresponding action is taken. The switch is "born" with a total number of MAC addresses from which all ports draw whenever a new MAC address is seen on a Port Security-enabled port. Since all ports draw from the same pool, it may happen that a configured maximum cannot be granted, if the remaining ports have already used all available MAC addresses.

Violation Mode : If Limit is reached, the switch can take one of the following actions:

> ***Protect***: Do not allow more than Limit MAC addresses on the port, but take no further action.
>
> ***Restrict***: If Limit is reached, subsequent MAC addresses on the port will be counted and marked as violating. Such MAC addresses are removed from the MAC table when the hold time expires. At most Violation Limit MAC addresses can be marked as violating at any given time.
>
> ***Shutdown***: If Limit is reached, one additional MAC address will cause the port to be shut down. This implies that all secured MAC addresses be removed from the port, and no new addresses be learned. There are three ways to re-open the port: 1) In the "Configuration > Ports" page's "Configured" column, first disable the port, then restore the original mode. 2) Make a Port Security configuration change on the port. 3) Boot the switch.

Violation Limit : The maximum number of MAC addresses that can be marked as violating on this port.
This number cannot exceed 1023. The default is 4. It is only used when Violation Mode is ‘Restrict’.

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

> ***Disabled***: Limit Control is either globally disabled or disabled on the port.
>
> ***Ready***: The limit is not yet reached. This can be shown for all actions.
>
> ***Limit Reached***: Indicates that the limit is reached on this port. This state only displays 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 displayed if Action is set to Shutdown or Trap & Shutdown.

Buttons

Apply : Click to save changes.

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

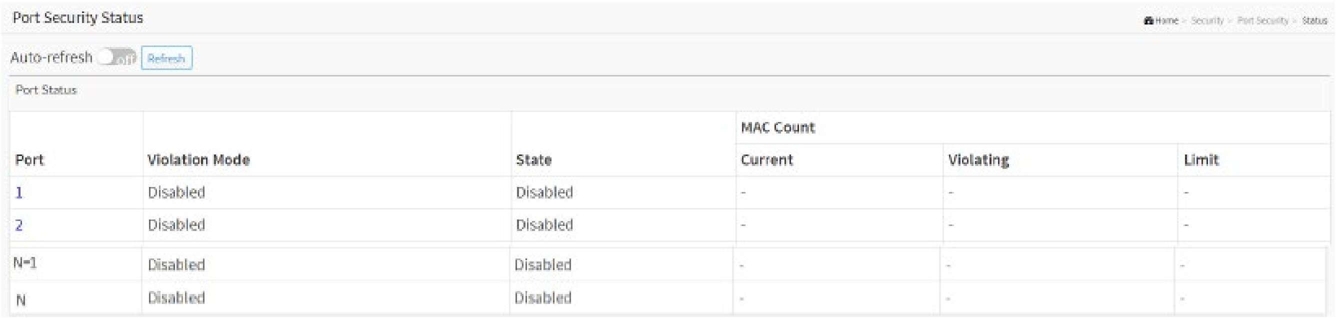
Status

This page 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 user chooses to block it, it will be blocked until that user module decides otherwise.

Web Interface

To display Port Security Status in the web UI:

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 that particular port.



Port Security Status

Port Status

			MAC Count		
Port	Violation Mode	State	Current	Violating	Limit
1	Disabled	Disabled	-	-	-
2	Disabled	Disabled	-	-	-
N-1	Disabled	Disabled	-	-	-
N	Disabled	Disabled	-	-	-

Figure 11-5.2: Port Security Status

Parameter descriptions:

Port : The port number for which the status applies. Click the linked port number to see the status for this particular port.

Violation Mode : Shows the configured Violation Mode of the port. It displays one of four values:

> ***Disabled***: Port Security is not administratively enabled on this port.
>
> ***Protect***: Port Security is administratively enabled in Protect mode.
>
> ***Restrict***: Port Security is administratively enabled in Restrict mode.
>
> ***Shutdown***: Port Security is administratively enabled in Shutdown mode.

State : Shows the current state of the port. It can display 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 Webpage.

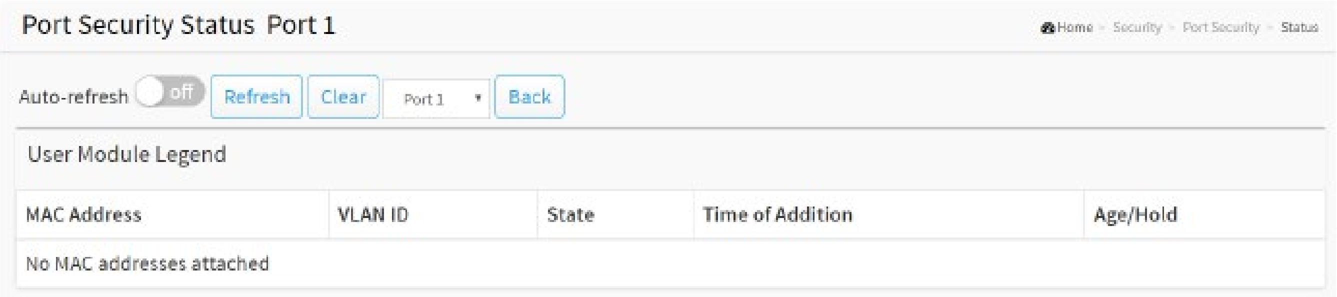
MAC Count (Current, Violating, Limit) : The three columns indicate the number of currently learned MAC addresses (forwarding as well as blocked), the number of violating MAC address (only counting in Restrict mode) and the maximum number of MAC addresses that can be learned on the port, respectively. If no user modules are enabled on the port, the Current column will show a dash (**-**). If Port Security is not administratively enabled on the port, the Violating and Limit columns will show a dash (**-**).

Buttons

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

Refresh : Click to refresh the page immediately.

Click the port number to see the status for this particular port:


Port Security Status Port 1
Home » Security » Port Security » Status
Auto-refresh
off
Refresh
Clear
Port 1
Back

User Module Legend

MAC Address	VLAN ID	State	Time of Addition	Age/Hold
No MAC addresses attached				

Figure 11-5.2: Port Security Status

Parameter descriptions:

MAC Address & **VLAN ID** : The MAC address and VLAN ID that is seen on this port. If no MAC addresses are learned, a single row stating "No MAC addresses attached" is displayed.

State : Indicates whether the corresponding MAC address is blocked or forwarding. In the Blocked state, it will not be allowed to transmit or receive traffic.

Time of Addition : Shows the date and time when this MAC address was first seen on the port.

Age/Hold : If at least one user module has decided to block this MAC address, it will stay in the Blocked state until the hold time (measured in seconds) expires. If all user modules have decided to allow this MAC address to forward, and aging is enabled, the Port Security module will periodically check that this MAC address still forwards traffic. If the age period (measured in seconds) expires and no frames have been seen, the MAC address will be removed from the MAC table. Otherwise a new age period will begin.
If aging is disabled or a user module has decided to hold the MAC address indefinitely, a dash (-) will be shown.

Buttons

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

Refresh : Click to refresh the page immediately.

Clear : Click to remove this particular MAC addresses from MAC table.

Port select box: At the dropdown select the port that you want to display the Port Security Status.

Back : Click to go back Port Security Status.

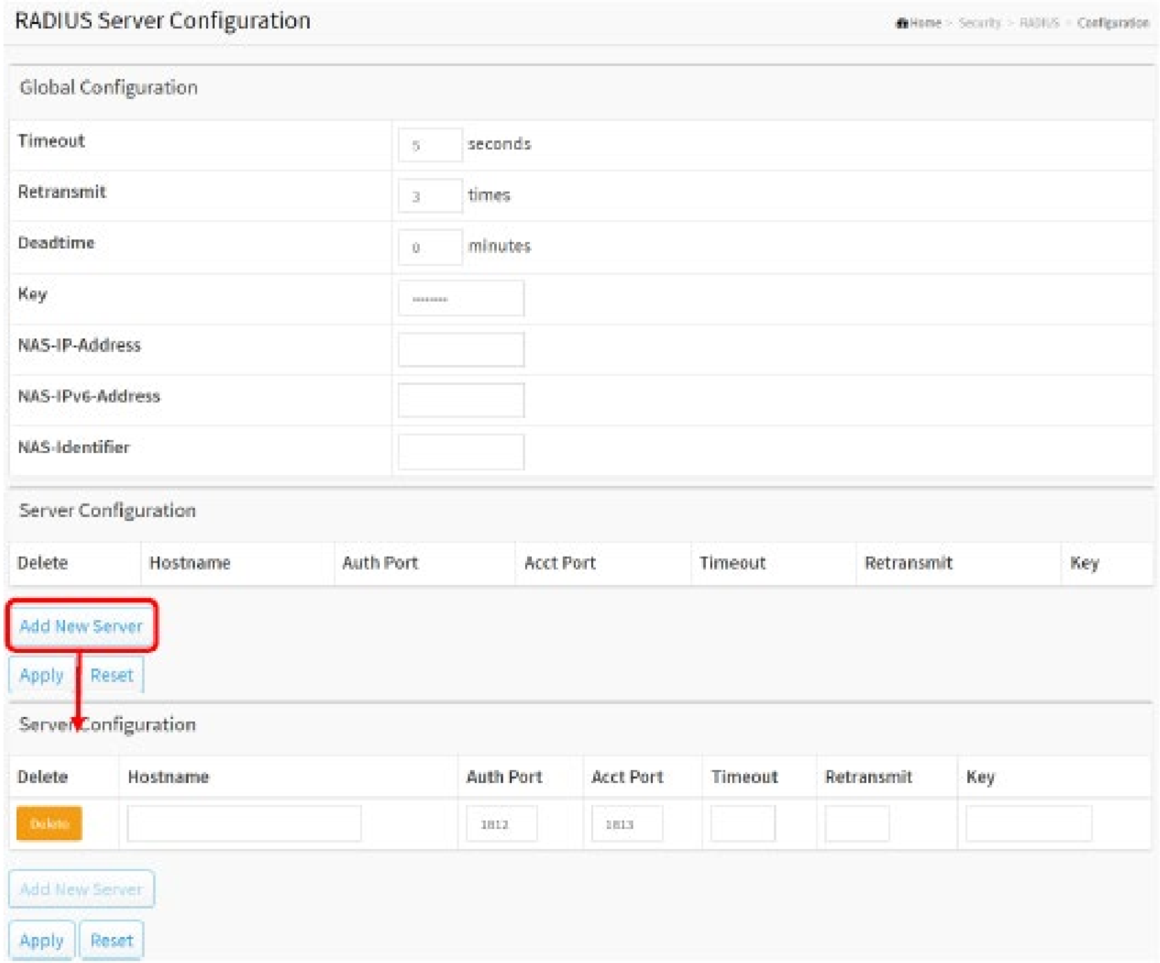
RADIUS

Configuration

This page lets you configure up to five RADIUS servers. Remote Authentication Dial In User Service is a networking protocol that provides centralized access, authorization and accounting management for people or computers to connect and use a network service.

To configure a RADIUS server in the web UI:

1. Click Security, RADIUS and Configuration.
2. Set Timeout, Retransmit, Deadtime, Key, NAS-IP-Address, NAS IPv6-Address, NAS-Identifier.
3. Click "Add New Entry".
4. Set Hostname, Auth Port, Acct Port, Timeout, Retransmit, Key.
5. Click the Apply button to save the settings.
6. To cancel the settings click the Reset button. It will revert to previously saved values.



RADIUS Server Configuration

Home > Security > RADIUS > Configuration

Global Configuration

Timeout	5 seconds
Retransmit	3 times
Deadtime	0 minutes
Key	••••••••
NAS-IP-Address	
NAS-IPv6-Address	
NAS-Identifier	

Server Configuration

Delete	Hostname	Auth Port	Acct Port	Timeout	Retransmit	Key

Server Configuration

Delete	Hostname	Auth Port	Acct Port	Timeout	Retransmit	Key
Delete		1812	1813			

Figure 11-6.1: RADIUS Configuration

Parameter descriptions:

Global Configuration : These setting are common for all of the RADIUS servers.

Timeout : The number of seconds, in the range 1 to 1000, to wait for a reply from a RADIUS server before retransmitting the request.

Retransmit : 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 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 several columns, which are:

Hostname : The IP address or hostname of the RADIUS server.

Auth Port : The UDP port to use on the RADIUS server for authentication.

Acct Port : The UDP port to use on the RADIUS server for accounting.

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

Retransmit : This optional setting overrides the global retransmit value. Leaving it blank will use the global retransmit value.

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

Buttons

Delete : To delete a RADIUS server entry, check this box. The entry will be deleted during the next Save.

Add New Entry : Click to add a new RADIUS server. An empty row is added to the table, and the RADIUS server can be configured as needed. Up to 5 servers are supported. The Reset button can be used to undo the addition of the new server.

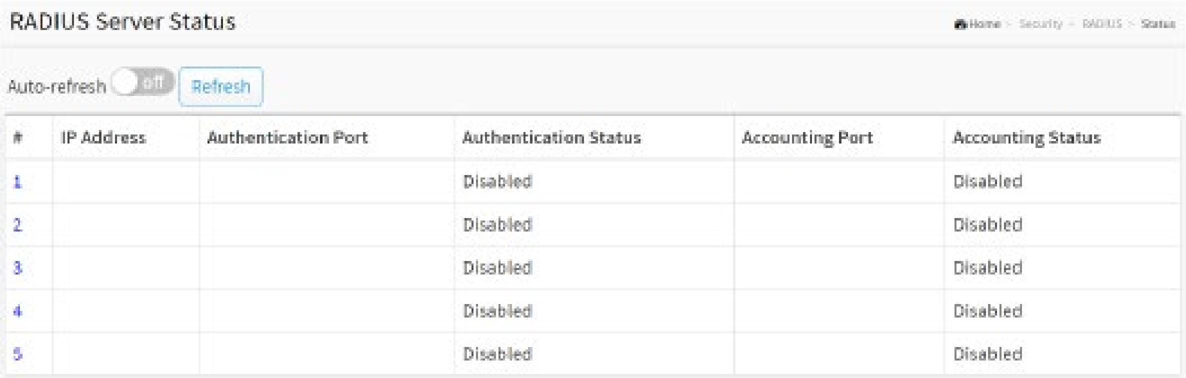
Apply : Click to save changes.

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

Status

This page displays details of the RADIUS Authentication and Accounting servers' status. To display RADIUS Server Status in the web UI:

1. Click Security, RADIUS and Status.
2. Select a server to display its particular RADIUS detailed statistics.



RADIUS Server Status

#	IP Address	Authentication Port	Authentication Status	Accounting Port	Accounting Status
1			Disabled		Disabled
2			Disabled		Disabled
3			Disabled		Disabled
4			Disabled		Disabled
5			Disabled		Disabled

Figure 11-6.2: RADIUS Server Status Overview

Parameter descriptions:

: The RADIUS server number. Click to navigate to detailed statistics for this server.

IP Address : The IP address and UDP port number (in <IP Address>:<UDP Port> notation) of this server.

Authentication Port : UDP port number for authentication.

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

Accounting Port : UDP port number for accounting.

Accounting Status : The current status of the server. This field takes one of these values:

Disabled: The server is disabled.

Not Ready: The server is enabled, but IP communication is not yet up and running.

Ready: The server is enabled, IP communication is up and running, and the RADIUS module is ready to accept access attempts.

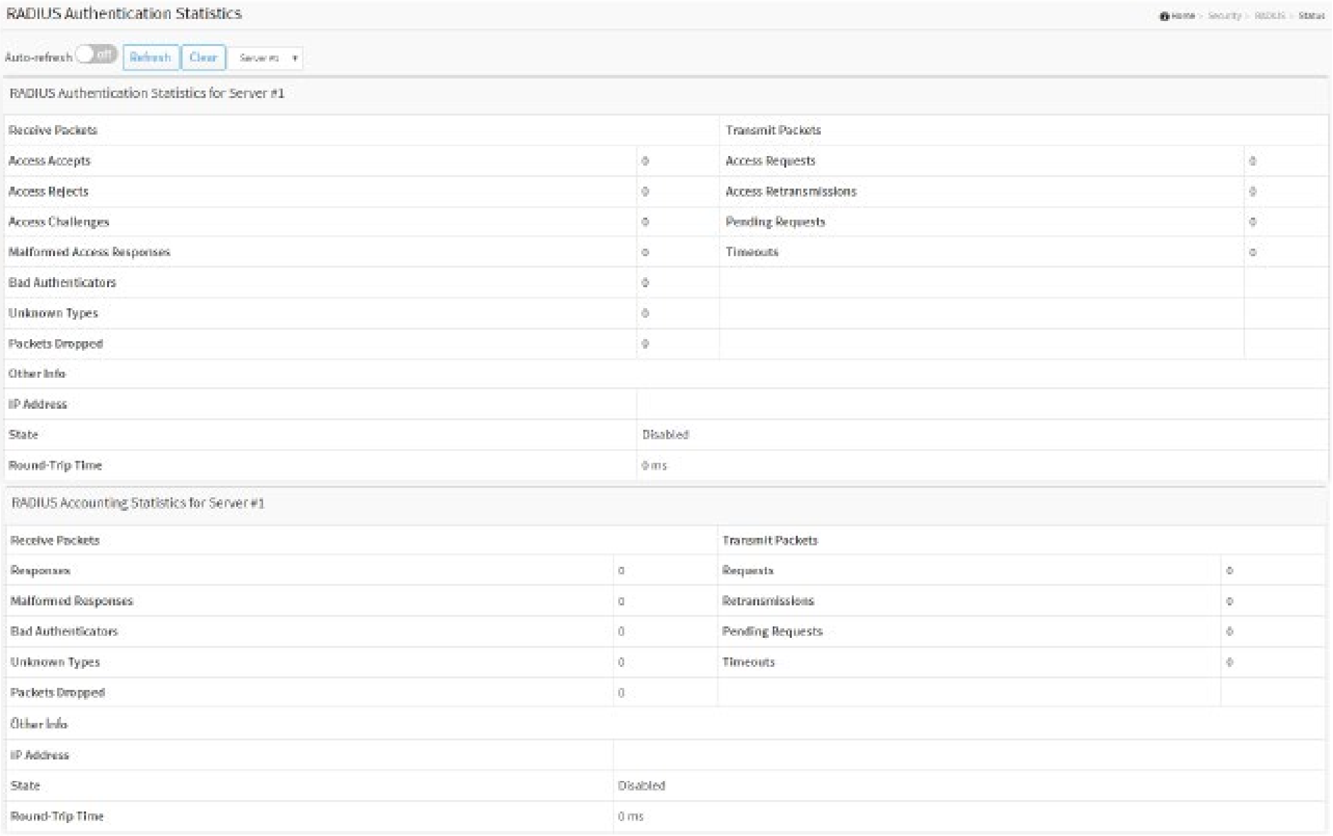
Dead (X seconds left): Access attempts were made to this server, but it did not reply within the configured timeout. The server has temporarily been disabled, but will get re-enabled when the dead-time expires. The number of seconds left before this occurs is displayed in parentheses. This state is only reachable when more than one server is enabled.

Buttons

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

Refresh : Click to refresh the page immediately.

If you select Server#1 to display RADIUS Statistics:



RADIUS Authentication Statistics

RADIUS Authentication Statistics for Server #1

Receive Packets		Transmit Packets	
Access Accepts	0	Access Requests	0
Access Rejects	0	Access Retransmissions	0
Access Challenges	0	Pending Requests	0
Malformed Access Responses	0	Timeouts	0
Bad Authenticators	0		
Unknown Types	0		
Packets Dropped	0		

Other Info	
IP Address	
State	Disabled
Round-Trip Time	0 ms

RADIUS Accounting Statistics for Server #1

Receive Packets		Transmit Packets	
Responses	0	Requests	0
Malformed Responses	0	Retransmissions	0
Bad Authenticators	0	Pending Requests	0
Unknown Types	0	Timeouts	0
Packets Dropped	0		

Other Info	
IP Address	
State	Disabled
Round-Trip Time	0 ms

Figure 11-6.2: RADIUS Statistics for Server

Parameter descriptions:

Server select box: Select which server that you want to display RADIUS. Use the server select box to switch between the backend servers to show details for.

RADIUS Authentication Statistics : The statistics map closely to those specified in RFC4668 - RADIUS Authentication Client MIB.

Access Accepts : The number of RADIUS Access-Accept packets (valid or invalid) received from the server.

Access Rejects : The number of RADIUS Access-Reject packets (valid or invalid) received from the server.

Access Challenges : The number of RADIUS Access-Challenge packets (valid or invalid) received from the server.

Malformed Access Responses : The number of malformed RADIUS Access-Response packets received from the server. Malformed packets include packets with an invalid length. Bad authenticators or Message Authenticator attributes or unknown types are not included as malformed access responses.

Bad Authenticators : The number of RADIUS Access-Response packets containing invalid authenticators or Message Authenticator attributes received from the server.

Unknown Types : The number of RADIUS packets that were received with unknown types from the server on the authentication port and dropped.

Packets Dropped : The number of RADIUS packets that were received from the server on the authentication port and dropped for some other reason.

Access Requests : The number of RADIUS Access-Request packets sent to the server. This does not include retransmissions.

Access Retransmissions : The number of RADIUS Access-Request packets retransmitted to the RADIUS authentication server.

Pending Requests : The number of RADIUS Access-Request packets destined for the server that have not yet timed out or received a response. This variable is incremented when an Access-Request is sent and decremented due to receipt of an Access-Accept, Access-Reject, Access-Challenge, timeout, or retransmission.

Timeouts : The number of authentication timeouts to the server. After a timeout, the client may retry to the same server, send to a different server, or give up. A retry to the same server is counted as a retransmit as well as a timeout. A send to a different server is counted as a Request as well as a timeout.

IP Address : IP address and UDP port for the authentication server in question.

State : Shows the state of the server. It takes one of these 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 : The statistics map closely to those specified in RFC4670 - RADIUS Accounting Client MIB. Use the server select box to switch between the backend servers to show details for.

Responses : The number of RADIUS packets (valid or invalid) received from the server.

Malformed Responses : The number of malformed RADIUS packets received from the server. Malformed packets include packets with an invalid length. Bad authenticators or unknown types are not included as malformed access responses.

Bad Authenticators : The number of RADIUS packets containing invalid authenticators received from the server.

Unknown Types : The number of RADIUS packets of unknown types that were received from the server on the accounting port.

Packets Dropped : The number of RADIUS packets that were received from the server on the accounting port and dropped for some other reason.

Requests : The number of RADIUS packets sent to the server. This does not include retransmissions

Retransmissions : The number of RADIUS packets retransmitted to the RADIUS accounting server.

Pending Requests : The number of RADIUS packets destined for the server that have not yet timed out or received a response. This variable is incremented when a Request is sent and decremented due to receipt of a Response, timeout, or retransmission.

Timeouts : The number of accounting timeouts to the server. After a timeout, the client may retry to the same server, send to a different server, or give up. A retry to the same server is counted as a retransmit as well as a timeout. A send to a different server is counted as a Request as well as a timeout.

IP Address : IP address and UDP port for the accounting server in question.

State : Shows the state of the server. It takes one of the following values:

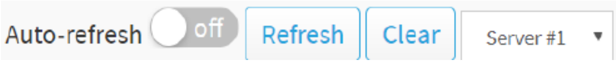
Disabled : The selected server is disabled.

Not Ready : The server is enabled, but IP communication is not yet up and running.

Ready : The server is enabled, IP communication is up and running, and the RADIUS module is ready to accept accounting attempts.

Dead (X seconds left) : Accounting attempts were made to this server, but it did not reply within the configured timeout. The server has temporarily been disabled but will get re-enabled when the dead-time expires. The number of seconds left before this occurs is displayed in parentheses. This state is only reachable when more than one server is enabled.

Round-Trip Time : The time interval (measured in milliseconds) between the most recent Response and the Request that matched it from the RADIUS accounting server. The granularity of this measurement is 100 ms. A value of 0 ms indicates that there hasn't been round-trip communication with the server yet.



Buttons

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

Refresh : Click to refresh the page immediately.

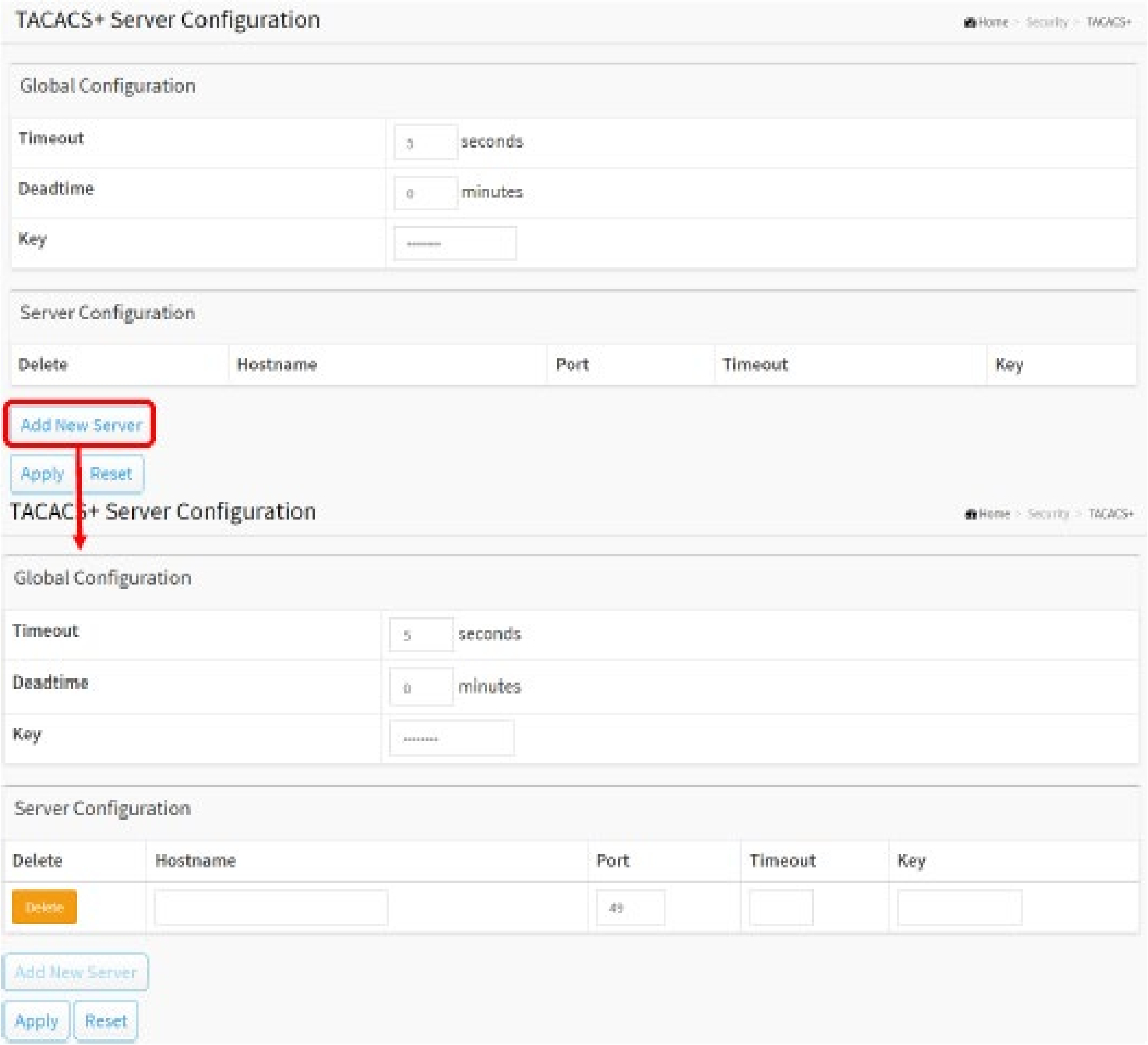
Clear : Clears the counters for the selected server. The "Pending Requests" counter will not be cleared by this operation.

Server select box: Select which server for which you want to display RADIUS. Use the server select box to switch between the backend servers to show details for.

TACACS+

This page lets you configure up to five TACACS+ servers. To configure TACACS+ servers in the web UI:

1. Click Security and TACACS+.
2. Click “Add New Entry”.
3. Specify the Timeout, Deadtime, and Key.
4. Specify the Hostname, Port, Timeout and Key in the server.
5. Click Apply.



TACACS+ Server Configuration

Global Configuration

Timeout	5 seconds
Deadtime	0 minutes
Key	••••••••

Server Configuration

Delete	Hostname	Port	Timeout	Key

TACACS+ Server Configuration

Global Configuration

Timeout	5 seconds
Deadtime	0 minutes
Key	••••••••

Server Configuration

Delete	Hostname	Port	Timeout	Key
Delete		49		

Figure 11-7: TACACS+ Server Configuration

Parameter descriptions:

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 several 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.

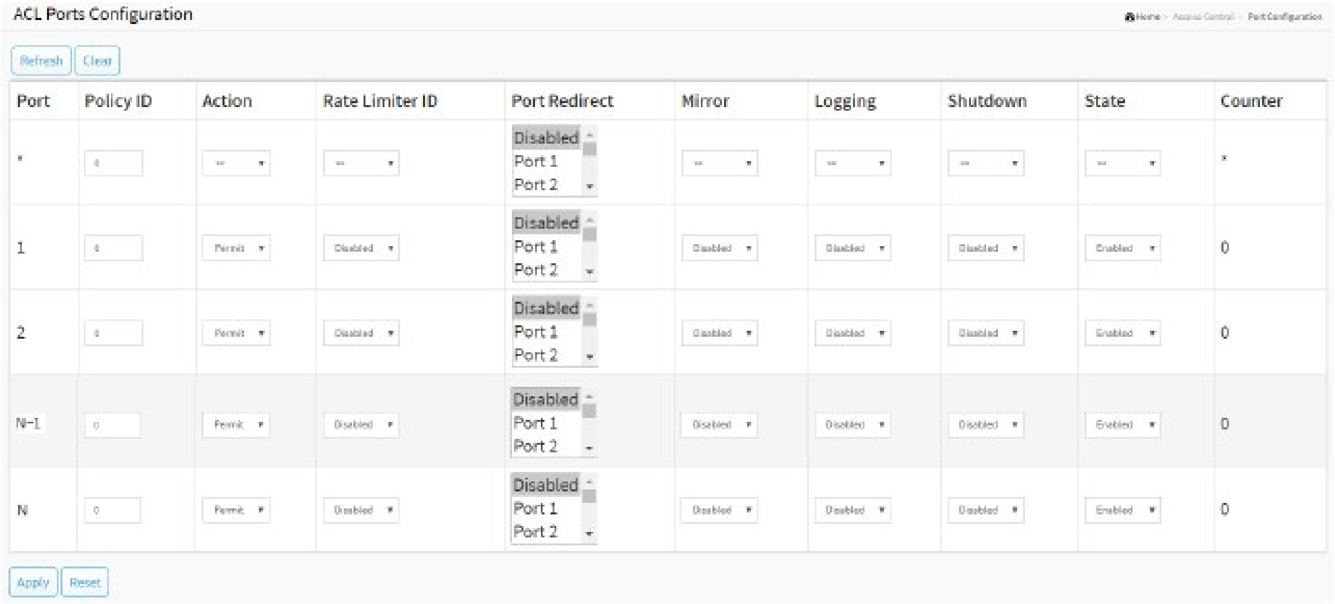
12. Access Control

Ports Configuration

Configure the ACL parameters (ACE) of each switch port. These parameters will affect frames received on a port unless the frame matches a specific ACE.

To configure ACL Ports in the web UI:

1. Click Access Control and Port Configuration.
2. Specify parameter values for port ACL setting.
3. Click Apply to save the settings.
4. To cancel the settings, click the reset button. It will revert to previously saved values.



ACL Ports Configuration

Port	Policy ID	Action	Rate Limiter ID	Port Redirect	Mirror	Logging	Shutdown	State	Counter
*	0	<>	<>	Disabled Port 1 Port 2	<>	<>	<>	<>	*
1	0	Permit	Disabled	Disabled Port 1 Port 2	Disabled	Disabled	Disabled	Enabled	0
2	0	Permit	Disabled	Disabled Port 1 Port 2	Disabled	Disabled	Disabled	Enabled	0
N-1	0	Permit	Disabled	Disabled Port 1 Port 2	Disabled	Disabled	Disabled	Enabled	0
N	0	Permit	Disabled	Disabled Port 1 Port 2	Disabled	Disabled	Disabled	Enabled	0

Figure 12-1: ACL Ports Configuration

Parameter descriptions:

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

Policy ID : Select the policy to apply to this port. Valid values are 1 - 8. The default value is 1.

Action : Select whether forwarding is permitted ("Permit") or denied ("Deny"). The default value is "Permit".

Rate Limiter ID : Select which rate limiter to apply on this port. The allowed values are Disabled or the values 1 - 16. The default value is "Disabled".

Port Redirect : Select which port frames are redirected on. The allowed values are Disabled or a specific port number and it can't be set when action is permitted. The default value is "Disabled".

Mirror : Specify the mirror operation of this port. The allowed values are: Enabled: Frames received on the port are mirrored. Disabled: Frames received on the port are not mirrored. The default value is "Disabled".

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

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

__Disabled__: Frames received on the port are not logged. The default value is "Disabled".

Note that the System Log memory size and logging rate is limited.

Shutdown : Specify the port shut down operation of this port. The allowed values are:

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

__Disabled__: Port shut down is disabled. The default value is "Disabled".

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

__Enabled__: To reopen ports by changing the volatile port configuration of the ACL user module. The default value is "Enabled".

__Disabled__: To close ports by changing the volatile port configuration of the ACL user module.

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

Buttons

Refresh : Click to refresh the ACL Port Configuration.

Clear : Click to clear the ACL Port Configuration manually.

Apply : Click to save changes.

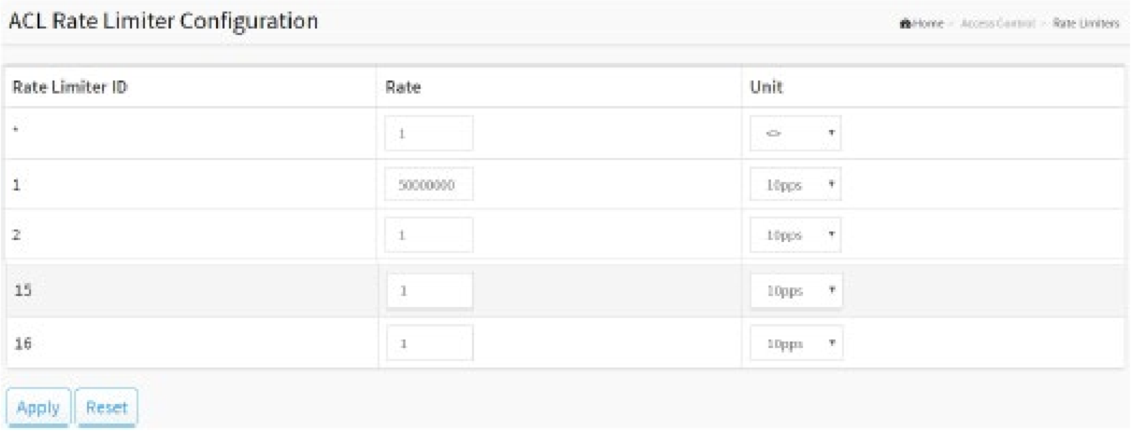
Reset : Click to undo any changes made locally and revert to previously saved values.

Rate Limiters

This page lets you configure the switch’s ACL Rate Limiter parameters.

To configure ACL Rate Limiters in the web UI:

1. Click Access Control and Rate Limiters.
2. Specific the Rate and Unit.
3. Click Apply to save the settings.
4. To cancel the settings click the Reset button. It will revert to previously saved values.



ACL Rate Limiter Configuration

Rate Limiter ID	Rate	Unit
*	1	<>
1	50000000	10pps
2	1	10pps
15	1	10pps
16	1	10pps

Figure 12-2: ACL Rate Limiter Configuration

Parameter descriptions:

Rate Limiter ID : The rate limiter ID for the settings contained in the same row; its range is 1 to 16.

Rate : The valid rate is 0, 10, 20, 30, ..., 5000000 in pps or 0, 25, 50, 75, ..., 10000000 in kbps.

Unit : Specify the rate unit of measure. Valid values are 10pps: packets per second or 25kbps: Kbits per second.

Buttons

Apply : Click to save changes.

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

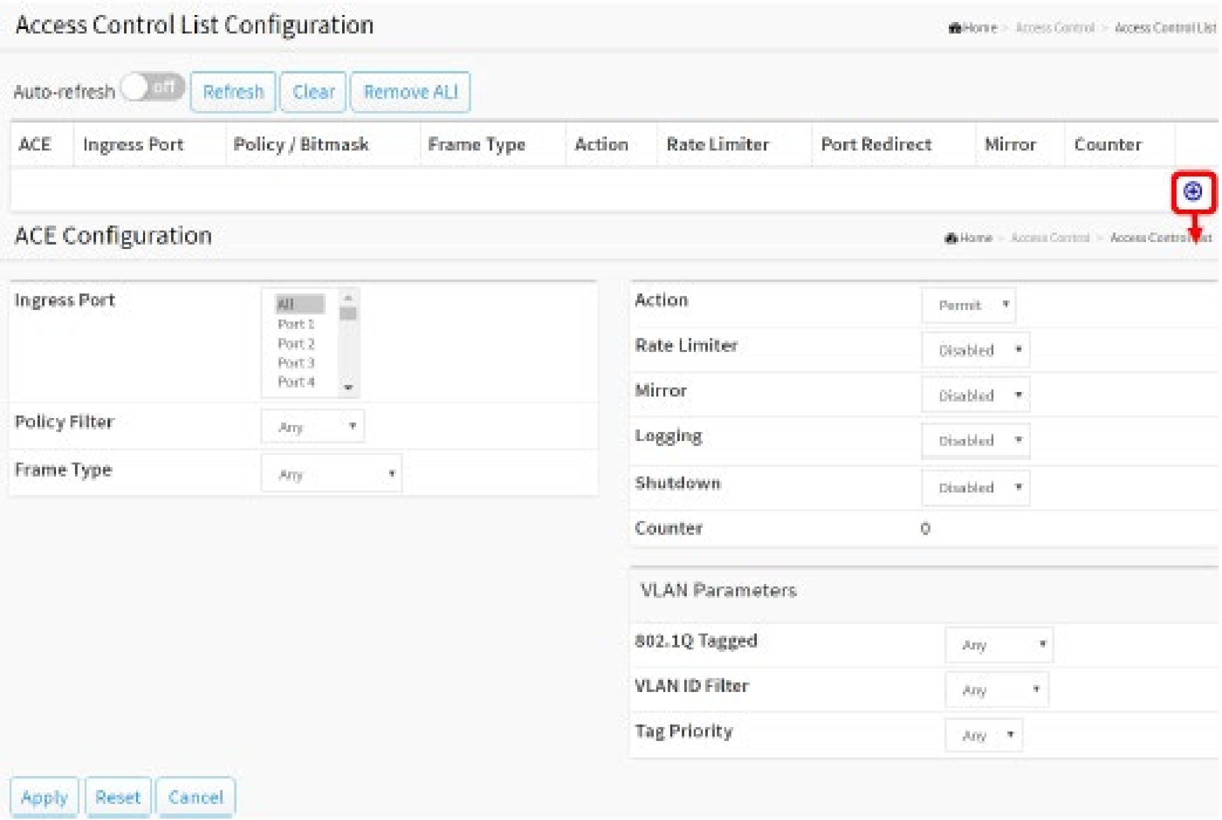
Access Control List

This page shows the Access Control List (ACL), which is made up of the ACEs defined on this switch. Each row describes an ACE that is defined. The maximum number of ACEs is 512 on each switch.

Click on the lowest plus sign to add a new ACE to the list. Reserved ACEs are used for internal protocol and cannot be edited or deleted; the order sequence cannot be changed, and the priority is highest.

To configure Access Control List in the web UI:

1. Click Access Control and Access Control List.
2. Click the ⊕ button to add a new ACL, or use the other ACL modification buttons to specify the editing action (i.e., edit, delete, or moving the relative position of entry in the list)
3. Specify the ACE parameters.
4. Click the Apply button to save the settings
5. To cancel the settings 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 (e.g., Rate Limiter, Port Copy, Logging, and Shutdown).


Home > Access Control > Access Control List
Auto-refresh off
Refresh
Clear
Remove All
⊕
Home > Access Control > Access Control List
Apply
Reset
Cancel

Access Control List Configuration

ACE	Ingress Port	Policy / Bitmask	Frame Type	Action	Rate Limiter	Port Redirect	Mirror	Counter

ACE Configuration

Ingress Port	All Port 1 Port 2 Port 3 Port 4
Policy Filter	Any
Frame Type	Any

Action	Permit
Rate Limiter	Disabled
Mirror	Disabled
Logging	Disabled
Shutdown	Disabled
Counter	0

VLAN Parameters

802.1Q Tagged	Any
VLAN ID Filter	Any
Tag Priority	Any

Figure 12-3: Access Control List Configuration

Parameter descriptions:

ACE : Indicates the ACE ID.

Ingress Port : Indicates the ingress port of the ACE. Possible values are:

Any: The ACE will match any ingress port.

Policy: The ACE will match ingress ports with a specific policy.

Port: The ACE will match a specific ingress port.

Policy / Bitmask : Indicates the policy number and bitmask of the ACE.

Frame Type : Indicates the frame type of the ACE. Possible values are:

Any: The ACE will match any frame type.

EType: The ACE will match Ethernet Type frames. Note that an Ethernet Type based ACE will not get matched by IP and ARP frames.

ARP: The ACE will match ARP/RARP frames.

IPv4: The ACE will match all IPv4 frames.

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

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

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

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

IPv6: The ACE will match all IPv6 standard frames.

Action : Indicates the forwarding action of the ACE.

Permit: Frames matching the ACE may be forwarded and learned.

Deny: Frames matching the ACE are dropped.

Filter: Frames matching the ACE are filtered.

Rate Limiter : Indicates the rate limiter number of the ACE. The valid range is 1 to 16. When Disabled is displayed, the rate limiter operation is disabled.

Port Redirect : Indicates the port redirect operation of the ACE. Frames matching the ACE are redirected to the port number. The allowed values are Disabled or a specific port number. When Disabled is displayed, the port redirect operation is disabled.

Mirror : Specify the mirror operation of this port. Frames matching the ACE are mirrored to the destination mirror port. The allowed values are:

Enabled: Frames received on the port are mirrored.

Disabled: Frames received on the port are not mirrored. The default value is "Disabled".

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

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

⊕ : Inserts a new ACE before the current row.

ⓔ : Edits the ACE row.

⇧ : Moves the ACE up the list.

⇩ : Moves the ACE down the list.

⊗ : Deletes the ACE.

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

ACE Configuration : An ACE consists of several parameters. These parameters vary according to the frame type that you select. First select the ingress port for the ACE, and then select the frame type. Different parameter options are displayed depending on the frame type selected. A frame that hits this ACE matches the configuration that is defined here.

Ingress Port : Select the ingress port for which this ACE applies.

All: The ACE applies to all port.

Port n: The ACE applies to this port number, where n is the number of the switch port.

Policy Filter : Specify the policy number filter for this ACE.

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

Specific: If you want to filter a specific policy with this ACE, choose this value. Two fields for entering a policy value and a bitmask appear.

Policy Value : When "Specific" is selected for the policy filter, you can enter a specific policy value. The valid range is 0 to 255.

Policy Bitmask : When "Specific" is selected for the policy filter, you can enter a specific policy bitmask. The valid range is 0x0 to 0xff. Notice the usage of bitmask, if the binary bit value is "0", it means this bit is "don't-care". The real matched pattern is [policy_value & policy_bitmask]. For example, if the policy value is 3 and the policy bitmask is 0x10(bit 0 is "don't-care" bit), then policy 2 and 3 are applied to this rule.

Frame Type : Select the frame type for this ACE. These frame types are mutually exclusive.

Any: Any frame can match this ACE.

Ethernet Type: Only Ethernet Type frames can match this ACE. The IEEE 802.3 describes the value of Length/Type Field specifications to be greater than or equal to 1536 decimal (equal to 0600 hexadecimal).

ARP: Only ARP frames can match this ACE. Notice the ARP frames won't match the ACE with ethernet type.

IPv4: Only IPv4 frames can match this ACE. Notice the IPv4 frames won't match the ACE with ethernet type.

IPv6: Only IPv6 frames can match this ACE. Notice the IPv6 frames won't match the ACE with Ethernet type.

Action : Specify the action to take with a frame that hits this ACE.

Permit: The frame that hits this ACE is granted permission for the ACE operation.

Deny: The frame that hits this ACE is dropped.

Filter: Frames matching the ACE are filtered.

Rate Limiter : Specify the rate limiter in number of base units. The valid range is 1 to 16. Disabled indicates that the rate limiter operation is disabled.

Port Redirect : Frames that hit the ACE are redirected to the port number specified here. The rate limiter will affect these ports. The valid range is the same as the switch port number range. Disabled indicates that the port redirect operation is disabled and the specific port number of 'Port Redirect' can't be set when action is permitted.

Mirror : Specify the mirror operation of this port. Frames matching the ACE are mirrored to the destination mirror port. The rate limiter will not affect frames on the mirror port. Valid values are:

Enabled: Frames received on the port are mirrored.

Disabled: Frames received on the port are not mirrored. The default value is "Disabled".

Logging : Specify the logging operation of the ACE. Note that the logging message doesn't include the 4 bytes of CRC information. Valid values are:

Enabled: Frames matching the ACE are stored in the System Log.

Disabled: Frames matching the ACE are not logged.

Note: The logging feature only works when the packet length is less than 1518 (without VLAN tags) and the System Log memory size and logging rate is limited.

Shutdown : Specify the port shut down operation of the ACE. The allowed values are:

Enabled: If a frame matches the ACE, the ingress port will be disabled.

Disabled: Port shut down is disabled for the ACE.

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

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

MAC Parameter

SMAC Filter : (Only displayed when the frame type is Ethernet Type or ARP.) Specify the source MAC filter for this ACE:

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

Specific: If you want to filter a specific source MAC address with this ACE, choose this value. A field for entering an SMAC value appears.

SMAC Value : When "Specific" is selected for the SMAC filter, you can enter a specific source MAC address.
The legal format is "xx-xx-xx-xx-xx-xx" or "xx.xx.xx.xx.xx.xx" or "xxxxxxxxxxxx" (x is a hexadecimal digit).
A frame that hits this ACE matches this SMAC value.

DMAC Filter : Specify the destination MAC filter for this ACE.

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

MC: Frame must be multicast.

BC: Frame must be broadcast.

UC: Frame must be unicast.

Specific: If you want to filter a specific destination MAC address with this ACE, choose this value. A field for entering a DMAC value appears.

DMAC Value : When "Specific" is selected for the DMAC filter, you can enter a specific destination MAC address. The legal format is "xx-xx-xx-xx-xx-xx" or "xx.xx.xx.xx.xx.xx" or "xxxxxxxxxxxx" (x is a hexadecimal digit). A frame that hits this ACE matches this DMAC value.

VLAN Parameters

802.1Q Tagged : Specify whether frames can hit the action according to the 802.1Q tagged. Valid values are:

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

Enabled: Tagged frame only.

Disabled: Untagged frame only.

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

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

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

VLAN ID : When "Specific" is selected for the VLAN ID filter, you can enter a specific VLAN ID number. The valid range is 1 to 4095. A frame that hits this ACE matches this VLAN ID value.

Tag Priority : Specify the tag priority for this ACE. A frame that hits this ACE matches this tag priority. The allowed number range is 0 to 7 or range 0-1, 2-3, 4-5, 6-7, 0-3 and 4-7. The value 'Any' means that no tag priority is specified (tag priority is "don't-care".)

ARP Parameters : The ARP parameters can be configured when Frame Type "ARP" is selected.

ARP/RARP : Specify the available ARP/RARP opcode (OP) flag for this ACE:

Any: No ARP/RARP OP flag is specified. (OP is "don't-care".)

ARP: Frame must have ARP opcode set to ARP.

RARP: Frame must have RARP opcode set to RARP.

Other: Frame has unknown ARP/RARP Opcode flag.

Request/Reply : Specify the available Request/Reply opcode (OP) flag for this ACE.

Any: No Request/Reply OP flag is specified. (OP is "don't-care".)

Request: Frame must have ARP Request or RARP Request OP flag set.

Reply: Frame must have ARP Reply or RARP Reply OP flag.

Sender IP Filter : Specify the sender IP filter for this ACE.

Any: No sender IP filter is specified. (Sender IP filter is "don't-care".)

Host: Sender IP filter is set to Host. Specify the sender IP address in the SIP Address field that appears.

Network: Sender IP filter is set to Network. Specify the sender IP address and sender IP mask in the SIP Address and SIP Mask fields that appear.

Sender IP Address : When "Host" or "Network" is selected for the sender IP filter, you can enter a specific sender IP address in dotted decimal notation.

Sender IP Mask : When "Network" is selected for the sender IP filter, you can enter a specific sender IP mask in dotted decimal notation.

Target IP Filter : Specify the target IP filter for this specific ACE.

__Any__: No target IP filter is specified. (Target IP filter is "don't-care".)

__Host__: Target IP filter is set to Host. Specify the target IP address in the Target IP Address field that appears.

__Network__: Target IP filter is set to Network. Specify the target IP address and target IP mask in the Target IP Address and Target IP Mask fields that appear.

Target IP Address : When "Host" or "Network" is selected for the target IP filter, you can enter a specific target IP address in dotted decimal notation.

Target IP Mask : When "Network" is selected for the target IP filter, you can enter a specific target IP mask in dotted decimal notation.

ARP Sender MAC Match : Specify whether frames can hit the action according to their sender hardware address field (SHA) settings.

__0__: ARP frames where SHA is not equal to the SMAC address.

__1__: ARP frames where SHA is equal to the SMAC address.

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

RARP Target MAC Match : Specify whether frames can hit the action according to their target hardware address field (THA) settings.

__0__: RARP frames where THA is not equal to the target MAC address.

__1__: RARP frames where THA is equal to the target MAC address.

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

IP/Ethernet Length : Specify whether frames can hit the action according to their ARP/RARP hardware address length (HLN) and protocol address length (PLN) settings.

__0__: ARP/RARP frames where the HLN is not equal to Ethernet (0x06) or the (PLN) is not equal to IPv4 (0x04).

__1__: ARP/RARP frames where the HLN is equal to Ethernet (0x06) and the (PLN) is equal to IPv4 (0x04).

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

Ethernet : Specify whether frames can hit the action according to their ARP/RARP hardware address space (HRD) settings.

__0__: ARP/RARP frames where the HLD is not equal to Ethernet (1).

__1__: ARP/RARP frames where the HLD is equal to Ethernet (1).

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

IP : Specify whether frames can hit the action according to their ARP/RARP protocol address space (PRO) settings.

__0__: ARP/RARP frames where the PRO is not equal to IP (0x800).

__1__: ARP/RARP frames where the PRO is equal to IP (0x800).

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

IP Parameters : The IP parameters can be configured when Frame Type "IPv4" is selected.

IP Protocol Filter : Specify the IP protocol filter for this ACE.

Any: No IP protocol filter is specified ("don't-care").

Specific: If you want to filter a specific IP protocol filter with this ACE, choose this value. A field for entering an IP protocol filter appears.

ICMP: Select ICMP to filter IPv4 ICMP protocol frames. Extra fields for defining ICMP parameters will appear. These fields are explained later in this manual.

UDP: Select UDP to filter IPv4 UDP protocol frames. Extra fields for defining UDP parameters will appear. These fields are explained later in this manual.

TCP: Select TCP to filter IPv4 TCP protocol frames. Extra fields for defining TCP parameters will appear. These fields are explained later in this manual.

IP Protocol Value : When "Specific" is selected for the IP protocol value, you can enter a specific value. The valid range is 0 to 255. A frame that hits this ACE matches this IP protocol value.

IP TTL : Specify the Time-to-Live settings for this ACE.

zero: IPv4 frames with a Time-to-Live field greater than zero must not be able to match this entry.

non-zero: IPv4 frames with a Time-to-Live field greater than zero must be able to match this entry.

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

IP Fragment : Specify the fragment offset settings for this ACE. This involves the settings for the More Fragments (MF) bit and the Fragment Offset (FRAG OFFSET) field for an IPv4 frame.

No: IPv4 frames where the MF bit is set or the FRAG OFFSET field is greater than zero must not be able to match this entry.

Yes: IPv4 frames where the MF bit is set or the FRAG OFFSET field is greater than zero must be able to match this entry.

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

IP Option : Specify the options flag setting for this ACE.

No: IPv4 frames where the options flag is set must not be able to match this entry.

Yes: IPv4 frames where the options flag is set must be able to match this entry.

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

SIP Filter : Specify the source IP filter for this ACE.

Any: No source IP filter is specified. (Source IP filter is "don't-care".)

Host: Source IP filter is set to Host. Specify the source IP address in the SIP Address field that appears.

Network: Source IP filter is set to Network. Specify the source IP address and source IP mask in the SIP Address and SIP Mask fields that appear.

SIP Address : When "Host" or "Network" is selected for the source IP filter, you can enter a specific SIP address in dotted decimal notation.

SIP Mask : When "Network" is selected for the source IP filter, you can enter a specific SIP mask in dotted decimal notation.

DIP Filter : Specify the destination IP filter for this ACE.

Any: No destination IP filter is specified. (Destination IP filter is "don't-care".)

Host: Destination IP filter is set to Host. Specify the destination IP address in the DIP Address field that appears.

Network: Destination IP filter is set to Network. Specify the destination IP address and destination IP mask in the DIP Address and DIP Mask fields that appear.

DIP Address : When "Host" or "Network" is selected for the destination IP filter, you can enter a specific DIP address in dotted decimal notation.

DIP Mask : When "Network" is selected for the destination IP filter, you can enter a specific DIP mask in dotted decimal notation.

IPv6 Parameters : The IPv6 parameters can be configured when Frame Type "IPv6" is selected.

Next Header Filter : Specify the IPv6 next header filter for this ACE.

Any: No IPv6 next header filter is specified ("don't-care").

Specific: If you want to filter a specific IPv6 next header filter with this ACE, choose this value. A field for entering an IPv6 next header filter appears.

ICMP: Select ICMP to filter IPv6 ICMP protocol frames. Extra fields for defining ICMP parameters will appear. These fields are explained later in this manual.

UDP: Select UDP to filter IPv6 UDP protocol frames. Extra fields for defining UDP parameters will appear. These fields are explained later in this manual.

TCP: Select TCP to filter IPv6 TCP protocol frames. Extra fields for defining TCP parameters will appear. These fields are explained later in this document

Next Header Value : When "Specific" is selected for the IPv6 next header value, you can enter a specific value. The valid range is 0 to 255. A frame that hits this ACE matches this IPv6 protocol value.

SIP Filter : Specify the source IPv6 filter for this ACE.

Any: No source IPv6 filter is specified. (Source IPv6 filter is "don't-care".)

Specific: Source IPv6 filter is set to Network. Specify the source IPv6 address and source IPv6 mask in the SIP Address fields that appear.

SIP Address : When "Specific" is selected for the source IPv6 filter, you can enter a specific SIPv6 address. The field only supported last 32 bits for IPv6 address.

SIP BitMask : When "Specific" is selected for the source IPv6 filter, you can enter a specific SIPv6 mask. The field only supported last 32 bits for IPv6 address. Notice the usage of bitmask, if the binary bit value is "0", it means this bit is "don't-care". The real matched pattern is [sipv6_address & sipv6_bitmask] (last 32 bits). For example, if the SIPv6 address is 2001::3 and the SIPv6 bitmask is 0xFFFFFFFE(bit 0 is "don't-care" bit), then SIPv6 address 2001::2 and 2001::3 are applied to this rule.

Hop Limit : Specify the hop limit settings for this ACE.

zero: IPv6 frames with a hop limit field greater than zero must not be able to match this entry.

non-zero: IPv6 frames with a hop limit field greater than zero must be able to match this entry.

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

ICMP Parameters

ICMP Type Filter : Specify the ICMP filter for this ACE.

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

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

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

ICMP Code Filter : Specify the ICMP code filter for this ACE.

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

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

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

TCP/UDP Parameters

TCP/UDP Source Filter : Specify the TCP/UDP source filter for this ACE.

Any: No TCP/UDP source filter is specified (TCP/UDP source filter status is "don't-care").

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

Range: If you want to filter a specific TCP/UDP source range filter with this ACE, you can enter a specific TCP/UDP source range value. A field for entering a TCP/UDP source value appears.

TCP/UDP Source No. : When "Specific" is selected for the TCP/UDP source filter, you can enter a specific TCP/UDP source value. The valid range is 0 to 65535. A frame that hits this ACE matches this TCP/UDP source value.

TCP/UDP Source Range : When "Range" is selected for the TCP/UDP source filter, you can enter a specific TCP/UDP source range value. The valid range is 0 to 65535. A frame that hits this ACE matches this TCP/UDP source value.

TCP/UDP Destination Filter : Specify the TCP/UDP destination filter for this ACE.

Any: No TCP/UDP destination filter is specified (TCP/UDP destination filter status is "don't-care").

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

Range: If you want to filter a specific range TCP/UDP destination filter with this ACE, you can enter a specific TCP/UDP destination range value. A field for entering a TCP/UDP destination value appears.

TCP/UDP Destination Number : When "Specific" is selected for the TCP/UDP destination filter, you can enter a specific TCP/UDP destination value. The valid range is 0 to 65535. A frame that hits this ACE matches this TCP/UDP destination value.

TCP/UDP Destination Range : When "Range" is selected for the TCP/UDP destination filter, you can enter a specific TCP/UDP destination range value. The valid range is 0 to 65535. A frame that hits this ACE matches this TCP/UDP destination value.

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

__0__: TCP frames where the FIN field is set must not be able to match this entry.

__1__: TCP frames where the FIN field is set must be able to match this entry.

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

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

__0__: TCP frames where the SYN field is set must not be able to match this entry.

__1__: TCP frames where the SYN field is set must be able to match this entry.

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

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

__0__: TCP frames where the RST field is set must not be able to match this entry.

__1__: TCP frames where the RST field is set must be able to match this entry.

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

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

__0__: TCP frames where the PSH field is set must not be able to match this entry.

__1__: TCP frames where the PSH field is set must be able to match this entry.

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

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

__0__: TCP frames where the ACK field is set must not be able to match this entry.

__1__: TCP frames where the ACK field is set must be able to match this entry.

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

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

__0__: TCP frames where the URG field is set must not be able to match this entry.

__1__: TCP frames where the URG field is set must be able to match this entry.

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

Ethernet Type Parameters : The Ethernet Type parameters can be configured when Frame Type "Ethernet Type" is selected.

EtherType Filter : Specify the Ethernet type filter for this ACE.

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

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

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

Buttons

Apply : Click to save changes.

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

Auto-refresh : Click to automatically refresh page information every 3 seconds.

Refresh : Click to manually refresh the page immediately.

Clear : Click to clear the data manually.

Remove All : Click to remove all to clean up all ACL configurations on the table.

Cancel : Return to the previous page.

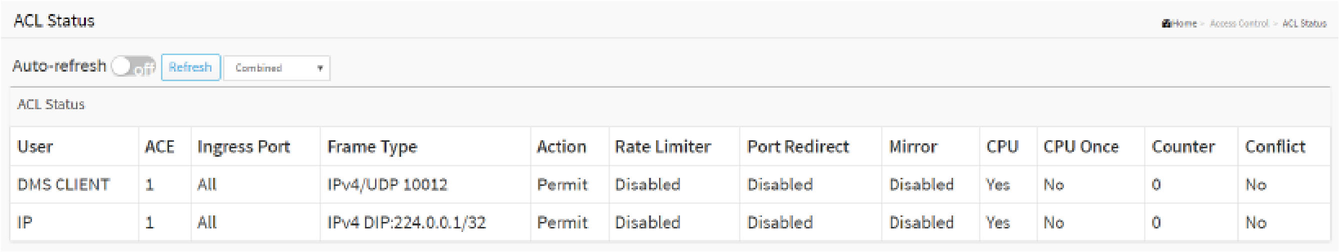
ACL Status

This page shows ACL status by different ACL users. Each row describes the ACE that is defined. It is a 'Conflict' if a specific ACE is not applied to the hardware due to hardware limitations. The maximum number of ACEs is 512 on each switch.

Web Interface

To display ACL status in the web UI:

1. Click Access Control and ACL Status.
2. At the User select dropdown select the set of user's information to be displayed. The default is "Combined".
3. To automatically refresh the information click "Auto-refresh".
4. Click "Refresh" to manually refresh the ACL Status immediately.



User	ACE	Ingress Port	Frame Type	Action	Rate Limiter	Port Redirect	Mirror	CPU	CPU Once	Counter	Conflict
DMS CLIENT	1	All	IPv4/UDP 10012	Permit	Disabled	Disabled	Disabled	Yes	No	0	No
IP	1	All	IPv4 DIP:224.0.0.1/32	Permit	Disabled	Disabled	Disabled	Yes	No	0	No

Figure 12-4: ACL Status

Parameter descriptions:

User : Indicates the ACL user (e.g., IP, DMS CLIENT, Combined, etc.).

ACE : Indicates the ACE ID on local switch.

Ingress Port : Indicates the ingress port of the ACE. Possible values are:

All: The ACE will match all ingress port.

Port: The ACE will match a specific ingress port.

Frame Type : Indicates the frame type of the ACE. Possible values are:

Any: The ACE will match any frame type.

EType: The ACE will match Ethernet Type frames. Note that an Ethernet Type based ACE will not get matched by IP and ARP frames.

ARP: The ACE will match ARP/RARP frames.

IPv4: The ACE will match all IPv4 frames.

IPv4: The ACE will match all IPv4 frames.

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

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

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

IPv4 DIP : The ACE will match IPv4 frames with Data Interface Pairs.

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

IPv6: The ACE will match all IPv6 standard frames.

Action : Indicates the forwarding action of the ACE.

Permit: Frames matching the ACE may be forwarded and learned.

Deny: Frames matching the ACE are dropped.

Filter: Frames matching the ACE are filtered.

Rate Limiter : Indicates the rate limiter number of the ACE. The valid range is 1 to 16. When Disabled is displayed, the rate limiter operation is disabled.

Port Redirect : Indicates the port redirect operation of the ACE. Frames matching the ACE are redirected to the port number. The allowed values are Disabled or a specific port number. When Disabled is displayed, the port redirect operation is disabled.

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

Enabled: Frames received on the port are mirrored.

Disabled: Frames received on the port are not mirrored. The default value is "Disabled".

CPU : Forward packets that matched the specific ACE to CPU.

CPU Once : Forward first packet that matched the specific ACE to CPU.

Counter : Indicates the number of times the ACE was hit by a frame.

Conflict : Indicates the hardware status of the specific ACE. The specific ACE is not applied to the hardware due to hardware limitations.

Buttons

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

Refresh : Click to manually refresh the page immediately.

User select box : At the dropdown select the set of user’s information to be displayed. The default is the set of “Combined” users.

13. SNMP

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

Basically, it is passive except issuing the trap information. The switch can turn the SNMP agent on or off. If you set the SNMPv1/v2c to "***on***", the SNMP agent will start up. All supported MIB OIDs, including the RMON MIB, can be accessed via the SNMP manager. If the SNMP Mode is set to "***off***", the SNMP agent will be de-activated, and the related Community Name, Trap Host IP Address, Trap, and all MIB counters are ignored.

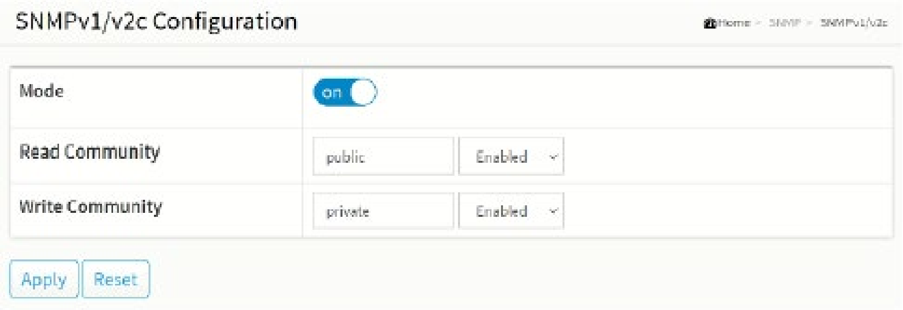
SNMPv1/v2c

This page lets you set SNMP v1 and v2 parameters. This function is used to configure SNMP settings, community name, trap host and public traps. 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.

Web Interface

To configure SNMPv1/v2c in the web UI:

1. Click SNMP and Configuration.
2. Enable (on) or disable (off) the SNMP Mode for the SNMPv1/v2c function.
3. Specify the Read Community and Write Community.
4. Click Apply.



SNMPv1/v2c Configuration

Mode	on	
Read Community	public	Enabled
Write Community	private	Enabled

Figure 12-1: SNMPv1/v2c Configuration

Parameter descriptions:

Mode : Sets the SNMP mode of operation. Possible modes are:

on : Enable SNMP operation mode.

off : Disable SNMP operation mode.

Read/Write Community : The ID that allows access/change to the device's data.

Buttons

Apply : Click to save changes.

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

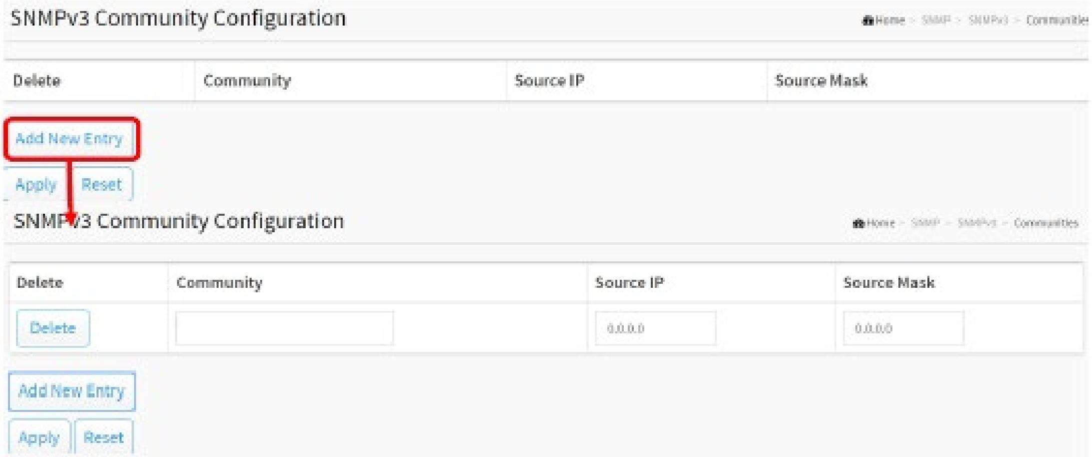
SNMPv3

Communities

Configure SNMPv3 community configuration table on this page. The entry index key is Community.

To configure SNMP Communities in the web UI:

1. Click SNMP, SNMPv3, and Communities.
2. Click Add New Entry.
3. Specify the SNMP community parameters.
4. Click Apply.
5. To modify or clear the settings click Reset.



SNMPv3 Community Configuration

Home > SNMP > SNMPv3 > Communities

Delete	Community	Source IP	Source Mask

SNMPv3 Community Configuration

Home > SNMP > SNMPv3 > Communities

Delete	Community	Source IP	Source Mask
Delete		0.0.0.0	0.0.0.0

Figure 13-2.1: SNMPv3 Communities Configuration

Parameter descriptions:

Community : Enter the security name to map the community to the SNMP Groups configuration.
The allowed string length is 1 to 32 characters, and the allowed content is ASCII characters 33 - 126.

Source IP : Enter the SNMP access source address. A particular range of source addresses can be used to restrict source subnet when combined with a Source Mask.

Source Mask : Enter the IP source mask.

Buttons

Add New Entry : Click to add a new entry to the table. Specify the name, configure the new entry and click "Apply".

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

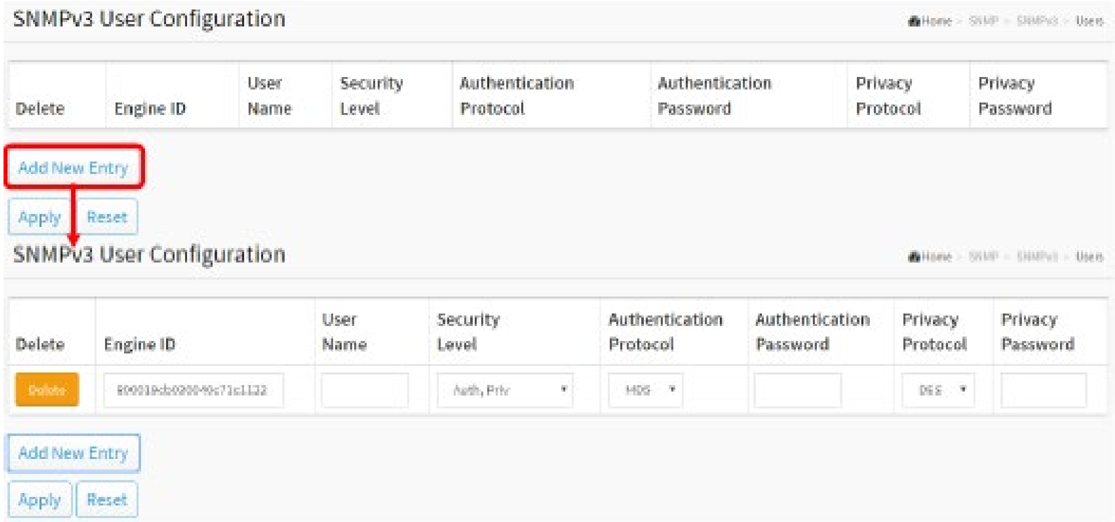
Apply : Click to save changes.

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

Users

This page lets you set SNMPv3 users' parameters. The Entry index key is UserName. The maximum number of Groups is 6. To configure SNMP Users in the web UI:

1. Click SNMP, SNMPv3, and Users.
2. Click Add New Entry.
3. Specify the SNMPv3 Users parameters.
4. Click Apply.



SNMPv3 User Configuration

Home > SNMP > SNMPv3 > Users

Delete	Engine ID	User Name	Security Level	Authentication Protocol	Authentication Password	Privacy Protocol	Privacy Password

SNMPv3 User Configuration

Home > SNMP > SNMPv3 > Users

Delete	Engine ID	User Name	Security Level	Authentication Protocol	Authentication Password	Privacy Protocol	Privacy Password
Delete	800019cb020040c71c1122		Auth, Priv	MD5		DES	

Figure 13-2.2: SNMP Users Configuration

Parameter descriptions:

Engine ID : An octet string identifying the engine ID that this entry should belong to. The string must contain an even number(in hexadecimal format) with number of digits between 10 and 64, but all-zeros and all-'F's are not allowed. The SNMPv3 architecture uses the User-based Security Model (USM) for message security and the View-based Access Control Model (VACM) for access control. For the USM entry, the usmUserEngineID and usmUserName are the entry's keys. In a simple agent, usmUserEngineID is always that agent's own snmpEngineID value. The value can also take the value of the snmpEngineID of a remote SNMP engine with which this user can communicate. In other words, if user engine ID equals system engine ID then it is local user; otherwise it's remote user.

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

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

NoAuth, NoPriv : No authentication and no privacy.

Auth, NoPriv : Authentication and no privacy.

Auth, Priv : Authentication and privacy.

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

Authentication Protocol : Indicates the authentication protocol that this entry should belong to. Possible authentication protocols are:

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

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

The value of security level cannot be modified if entry already exists. That means 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 characters. For SHA authentication protocol, the allowed string length is 8 to 39 characters. The allowed content is ASCII characters 33 - 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 - 31 characters, and the allowed content is ASCII characters 33 - 126.

Buttons

Add New Entry : Click to add a new entry to the table. Specify the name, configure the new entry, and click "Apply".

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

Apply : Click to save changes.

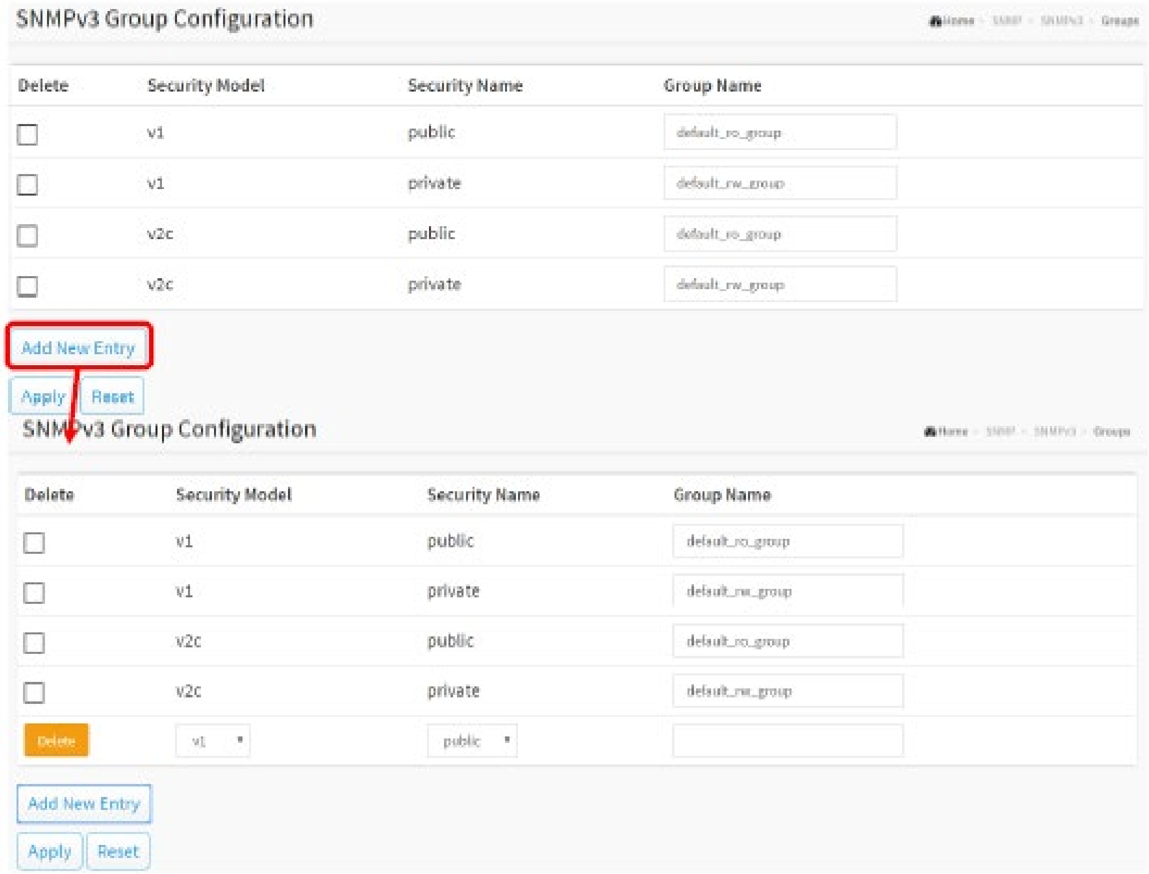
Reset : Click to undo any changes made locally and revert to previously saved values.

Groups

This page lets you configure SNMPv3 groups. The Entry index keys are Security Model and Security Name. The maximum number of Groups supported is 12.

To configure SNMP Groups in the web UI:

1. Click SNMP, SNMPv3, and Groups.
2. Click Add New Entry.
3. Specify the SNMP group parameters.
4. Click Apply.



SNMPv3 Group Configuration

Delete	Security Model	Security Name	Group Name
□	v1	public	default_ro_group
□	v1	private	default_rw_group
□	v2c	public	default_ro_group
□	v2c	private	default_rw_group

SNMPv3 Group Configuration

Delete	Security Model	Security Name	Group Name
□	v1	public	default_ro_group
□	v1	private	default_rw_group
□	v2c	public	default_ro_group
□	v2c	private	default_rw_group
Delete	v1 ▾	public ▾	

Figure 13-2.3: SNMP Groups Configuration

Parameter descriptions:

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

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

Buttons

Add New Entry : Click to add a new entry to the table. Specify the name, configure the new entry, then 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.

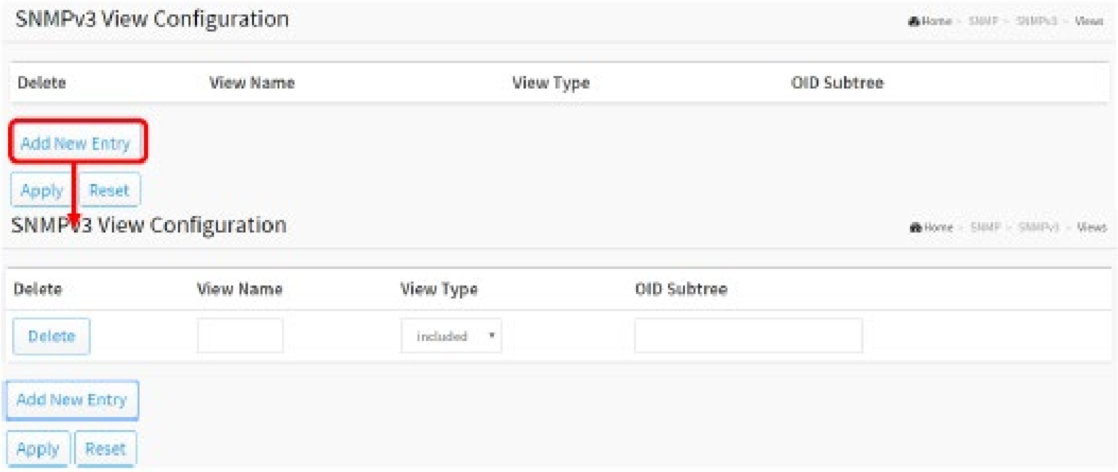
Views

Configure SNMPv3 View on this page. The Entry index keys are OID Subtree and View Name. The maximum number of Views supported is 12.

Web Interface

To configure SNMP Views in the web UI:

1. Click SNMP, SNMPv3, and Views.
2. Click Add New Entry.
3. Specify the SNMP View parameters.
4. Click Apply. To modify or clear the settings 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 13-2.4: SNMP View Configuration

Parameter descriptions:

View Name : A string identifying the view name that this entry should belong to. The allowed string length is 1 - 31 characters, and the allowed content is ASCII characters 33 - 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 - 128. The allowed string content is a digital number or an asterisk (*). Object Identifiers (OIDs) uniquely identify or name MIB variables in the tree.

Buttons

Add New Entry : Click to add a new entry to the table. Specify the name, configure the new entry, and click "Apply".

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

Apply : Click to save changes.

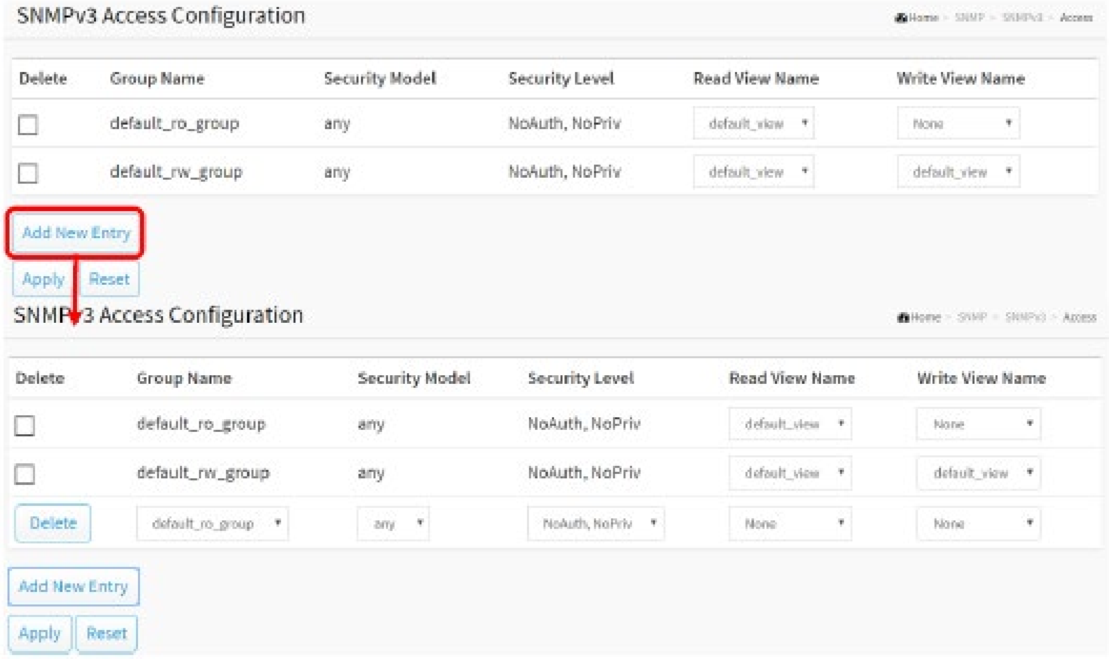
Reset : Click to undo any changes made locally and revert to previously saved values.

Access

This page lets you configure SNMPv3 accesses. The Entry index keys are Group Name, Security Model and Security Level. The maximum number of Accesses supported is 12.

To configure SNMP Access in the web UI:

1. Click SNMP, SNMPv3, and Accesses.
2. Click Add New Entry.
3. Specify the SNMP Access parameters.
4. Click Apply.
5. To modify or clear the settings click Reset.



SNMPv3 Access Configuration

Delete	Group Name	Security Model	Security Level	Read View Name	Write View Name
□	default_ro_group	any	NoAuth, NoPriv	default_view	None
□	default_rw_group	any	NoAuth, NoPriv	default_view	default_view

SNMPv3 Access Configuration

Delete	Group Name	Security Model	Security Level	Read View Name	Write View Name
□	default_ro_group	any	NoAuth, NoPriv	default_view	None
□	default_rw_group	any	NoAuth, NoPriv	default_view	default_view
Delete	default_ro_group	any	NoAuth, NoPriv	None	None

Figure 13-2.5: SNMP Access Configuration

Parameter descriptions:

Group Name : A string identifying the group name that this entry should belong to. The allowed string length is 1 - 31 characters, and the allowed content is ASCII characters 33 - 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 - 31 characters, and the allowed content is ASCII characters 33 - 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 - 31 characters, and the allowed content is ASCII characters 33 - 126.

Buttons

Add New Entry : Click to add a new entry. Specify the name, configure the new entry, and 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.

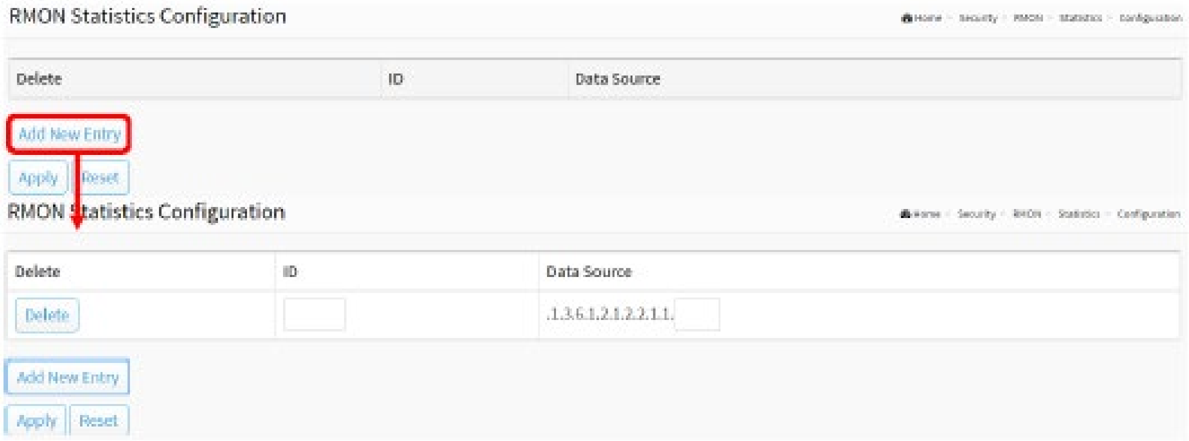
RMON Statistics

Remote Network Monitoring (RMON) is a process for monitoring network traffic on a remote Ethernet segment to detect network issues such as dropped packets, network collisions, and traffic congestion.

Configuration

Configure RMON Statistics table on this page. The entry index key is ID. To configure RMON Statistics in the web UI:

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



RMON Statistics Configuration

Delete	ID	Data Source

RMON Statistics Configuration

Delete	ID	Data Source
Delete		.1.3.6.1.2.1.2.2.1.1.

Figure 13-3.1: RMON Statistics Configuration

Parameter descriptions:

ID : Indicates the index of the entry. The valid range is 1 - 65535.

Data Source : Enter the port ID which you want to be monitored.

Buttons

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

Add New Entry : Click to add a new entry to the table.

Apply : Click to save changes.

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

Statistics Status

This page displays RMON Statistics entries. Each page shows up to 99 entries from the Statistics table, default being 20, selected through the "entries per page" input field. When first visited, the web page will show the first 20 entries from the beginning of the Statistics table. The first entry displayed will be the one with the lowest ID found in the Statistics table.

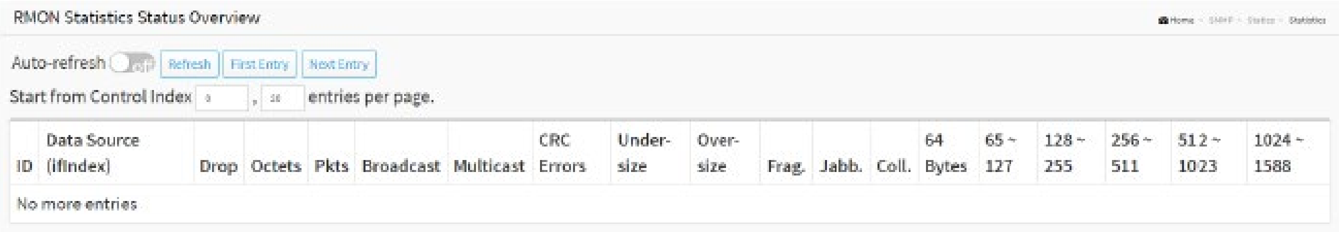
The "Start from Control Index" lets you select the starting point in the Statistics table. Clicking the Refresh button will update the displayed table starting from that or the next closest Statistics table match.

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

Web Interface

To view RMON Statistics Status in the web UI:

1. Click Security, RMON, Statistics, and Status.
2. Select a Start from Control Index and an entries per page.
3. Check “Auto-refresh” to automatically refresh the page every 3 seconds.
4. Click “Refresh” to manually refresh the page immediately.



RMON Statistics Status Overview

Start from Control Index , entries per page.

ID	Data Source (ifIndex)	Drop	Octets	Pkts	Broadcast	Multicast	CRC Errors	Under-size	Over-size	Frag.	Jabb.	Coll.	64 Bytes	65 ~ 127	128 ~ 255	256 ~ 511	512 ~ 1023	1024 ~ 1588
No more entries																		

Figure 13-3.2: RMON Statistics Status Overview

Parameter descriptions:

ID : Indicates the index of Statistics entry.

Data Source(if Index) : The port ID which wants to be monitored.

Drop : The total number of events in which packets were dropped by the probe due to lack of resources.

Octets : The total number of octets of data (including those in bad packets) received on the network.

Pkts : The total number of packets (including bad packets, broadcast packets, and multicast packets) received.

Broadcast : The total number of good packets received that were directed to the broadcast address.

Multicast : The total number of good packets received that were directed to a multicast address.

CRC Errors : The total number of packets received that had a length (excluding framing bits, but including FCS octets) of between 64 and 1518 octets, inclusive, but had either a bad Frame Check Sequence (FCS) with an integral number of octets (FCS Error) or a bad FCS with a non-integral number of octets (Alignment Error).

Under-size : The total number of packets received that were less than 64 octets.

Over-size : The total number of packets received that were longer than 1518 octets.

Frag. : The number of frames which size is less than 64 octets received with invalid CRC.

Jabb. : The number of frames which size is larger than 64 octets received with invalid CRC.

Coll. : The best estimate of the total number of collisions on this Ethernet segment.

64 Bytes : The total number of packets (including bad packets) received that were 64 octets in length.

65~127 : The total number of packets (including bad packets) received that were between 65 to 127 octets in length.

128~255 : The total number of packets (including bad packets) received that were between 128 to 255 octets in length.

256~511 : The total number of packets (including bad packets) received that were between 256 to 511 octets in length.

512~1023 : The total number of packets (including bad packets) received that were between 512 to 1023 octets in length.

1024~1588 : The total number of packets (including bad packets) received that were between 1024 to 1588 octets in length.

Buttons

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

Refresh : Click to refresh the page immediately.

First Entry : Updates the table starting from the first entry in the table.

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

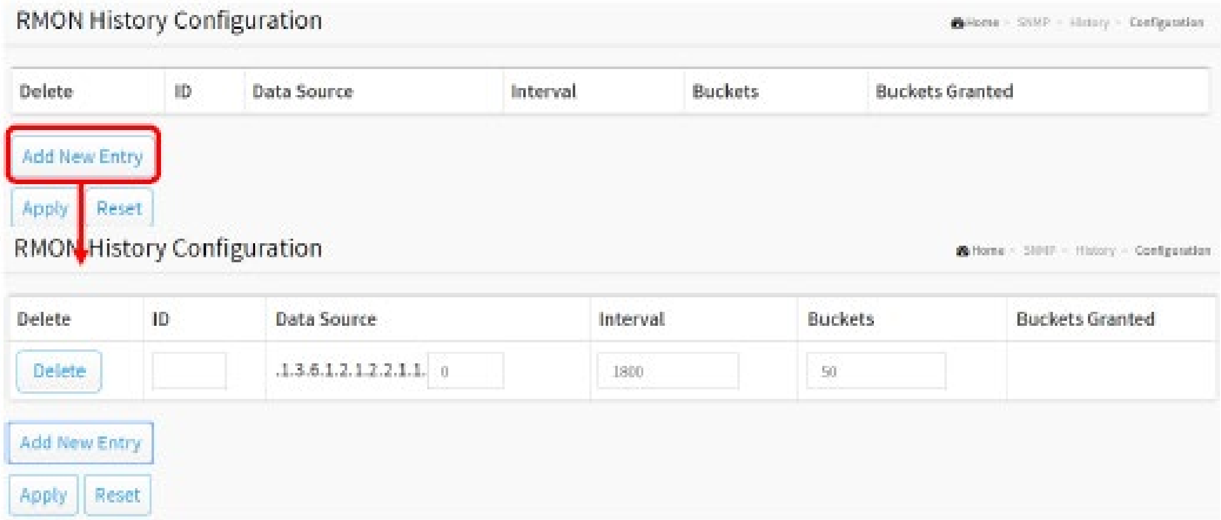
History

Configuration

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

To configure RMON History in the web UI:

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



RMON History Configuration

Home > SNMP > History > Configuration

Delete	ID	Data Source	Interval	Buckets	Buckets Granted

Add New Entry
Apply
Reset

RMON History Configuration

Home > SNMP > History > Configuration

Delete	ID	Data Source	Interval	Buckets	Buckets Granted
Delete		.1.3.6.1.2.1.2.2.1.1. 0	1800	50	

Add New Entry
Apply
Reset

Figure 13-4.1: The RMON History Configuration

Parameter descriptions:

ID : Indicates the index of the entry. The range is 1 - 65535.

Data Source : Enter the port ID which you want to be monitored.

Interval : Sets the interval in seconds for sampling history statistics data. The valid range is 1 - 3600; the default value is 1800 seconds.

Buckets : Sets the maximum data entries associated this History control entry stored in RMON. The valid range is 1 - 3600; the default value is 50.

Buckets Granted : The number of data to 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 to the table.

Apply : Click to save changes.

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

Status

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

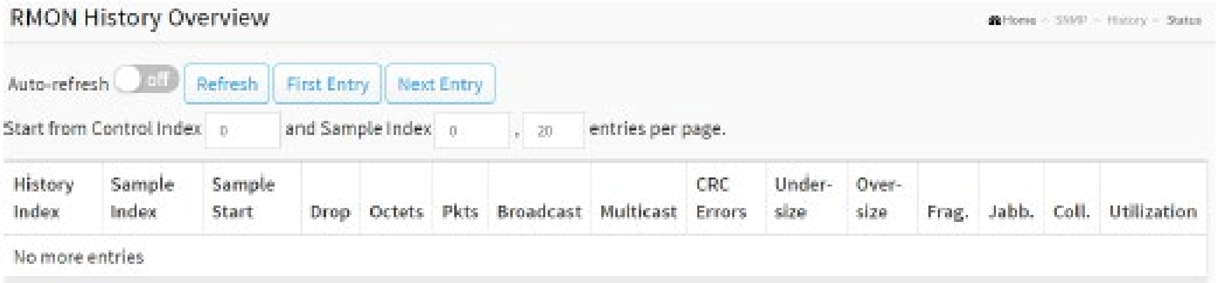
The "Start from History Index and Sample Index" lets you select the starting point in the History table. Clicking the Refresh button will update the displayed table starting from that or the next closest History table match.

The Next Entry will use the last entry of the currently displayed entry as a basis for the next lookup. When the end is reached the text "*No more entries*" is shown in the displayed table. Use the First Entry button to start over.

Web Interface

To display RMON History Status in the web UI:

1. Click SNMP, History, and Status.
2. Check “Auto-refresh” or click “Refresh” to refresh the port detailed statistics.
3. Click First Entry/Next Entry to change Entry.
4. Select “Start from Control Index”, “and Sample Index”, and “entries per page”.



RMON History Overview

Start from Control Index 0 and Sample Index 0 , 20 entries per page.

History Index	Sample Index	Sample Start	Drop	Octets	Pkts	Broadcast	Multicast	CRC Errors	Under-size	Over-size	Frag.	Jabb.	Coll.	Utilization
No more entries														

Figure 13-4.2: RMON History Overview

Parameter descriptions:

History Index : Indicates the index of History control entry.

Sample Index : Indicates the index of the data entry associated with the control entry.

Sample Start : The value of sysUpTime at the start of the interval over which this sample was measured.

Drop : The total number of events in which packets were dropped by the probe due to lack of resources.

Octets : The total number of octets of data (including those in bad packets) received on the network.

Pkts : The total number of packets (including bad packets, broadcast packets, and multicast packets). received.

Broadcast : The total number of good packets received that were directed to the broadcast address.

Multicast : The total number of good packets received that were directed to a multicast address.

CRC Errors : The total number of packets received that had a length (excluding framing bits, but including FCS octets) of between 64 and 1518 octets, inclusive, but had either a bad Frame Check Sequence (FCS) with an integral number of octets (FCS Error) or a bad FCS with a non-integral number of octets (Alignment Error).

Under-size : The total number of packets received that were less than 64 octets.

Over-size : The total number of packets received that were longer than 1518 octets.

Frag. : The number of frames which size is less than 64 octets received with invalid CRC.

Jabb. : The number of frames which size is larger than 64 octets received with invalid CRC.

Coll. : The best estimate of the total number of collisions on this Ethernet segment.

Utilization : The best estimate of the mean physical layer network utilization on this interface during this sampling interval, in hundredths of a percent.

Buttons

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

Refresh : Click to refresh the page immediately.

First Entry : Updates the table starting from the first entry in the table.

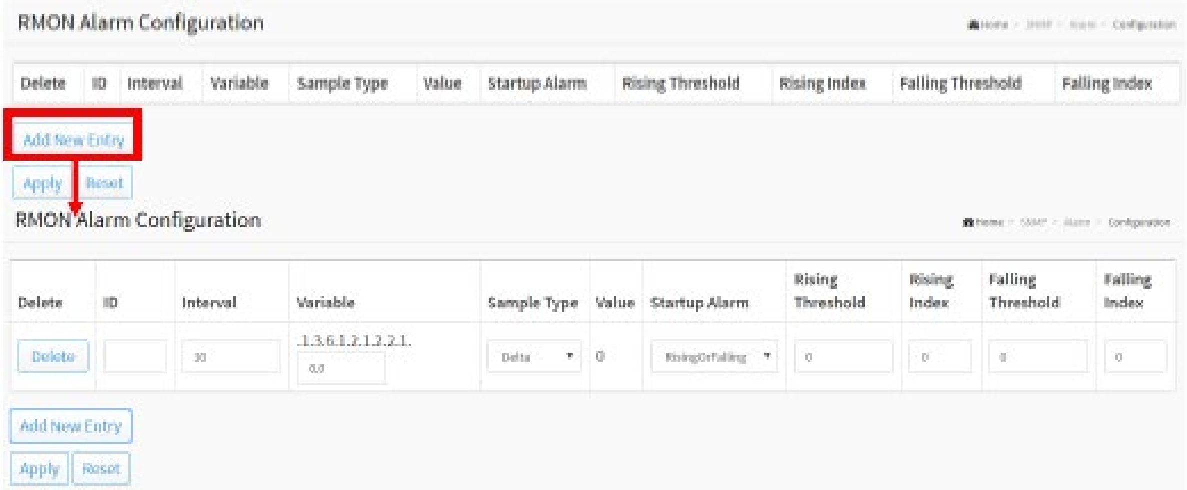
Next Entry : Updates the table, starting with the entry after the last entry currently displayed.

Alarm

Configuration

Configure RMON Alarm table parameters on this page. The entry index key is ID. To configure RMON Alarm Configuration parameters in the web UI:

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



RMON Alarm Configuration

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

Home > SNMP > Alarm > Configuration
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
Delete		30	.1.3.6.1.2.1.2.2.1. 0.0	Delta	0	RisingOrFalling	0	0	0	0

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

Figure 13-5.1: RMON Alarm Configuration

Parameter descriptions:

ID : Sets the index of the entry. The range is 1 to 65535.

Interval : Sets 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 broad-cast and multi-cast packets delivered to a higher-layer protocol.

InDiscards : The number of inbound packets that are discarded even the packets are normal.

InErrors : The number of inbound packets that contained errors preventing them from being deliverable to a higher-layer protocol.

InUnknownProtos: the number of the inbound packets that were discarded because of the unknown or un-support protocol.

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

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

OutNUcastPkts : The number of broad-cast and multi-cast packets that request to transmit.

OutDiscards : The number of outbound packets that are discarded event the packets is normal.

OutErrors : The 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.

Alarm Status

This page provides an overview of RMON Alarm entries. Each page shows up to 99 entries from the Alarm table, default being 20, selected through the "entries per page" input field. When first visited, the web page shows the first 20 entries from the beginning of the Alarm table. The first displayed will be the one with the lowest ID found in the Alarm table.

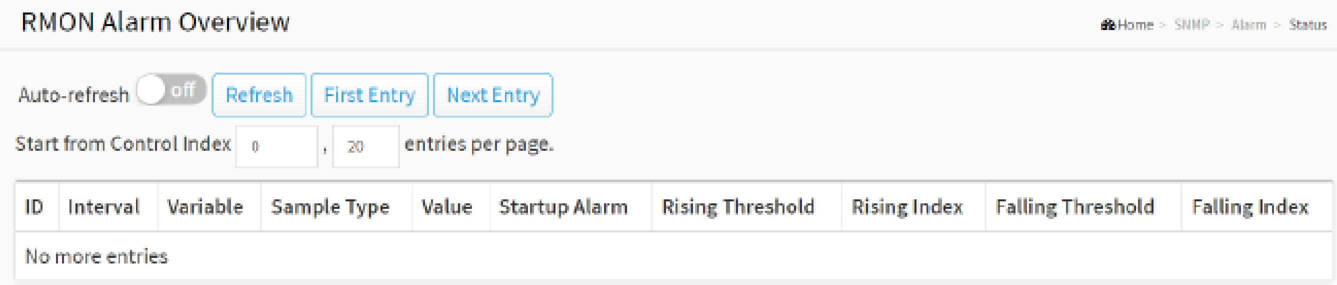
The "Start from Control Index" lets you select the starting point in the Alarm table. Clicking the Refresh button will update the displayed table starting from that or the next closest Alarm table match.

The Next Entry will use the last entry of the currently displayed entry as a basis for the next lookup. When the end is reached the text "*No more entries*" displays in the table. Use the First Entry button to start over.

Web Interface

To display RMON Alarm Status in the web UI:

1. Click SNMP, Alarm, and Status.
2. Check “Auto-refresh”.
3. Click “Refresh” to refresh the port detailed statistics.
4. Click First Entry/Next Entry to change Entry.



Start from Control Index 0 , 20 entries per page.

ID	Interval	Variable	Sample Type	Value	Startup Alarm	Rising Threshold	Rising Index	Falling Threshold	Falling Index
No more entries									

Figure 13-5.2: RMON Alarm Status

Parameter descriptions:

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.

Start from Control Index : Lets you select the starting point in the table.

entries per page : You can choose how many items you want to show per page.

Buttons

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

Refresh : Click to refresh the page immediately.

First Entry : Updates the table starting from the first entry in the table.

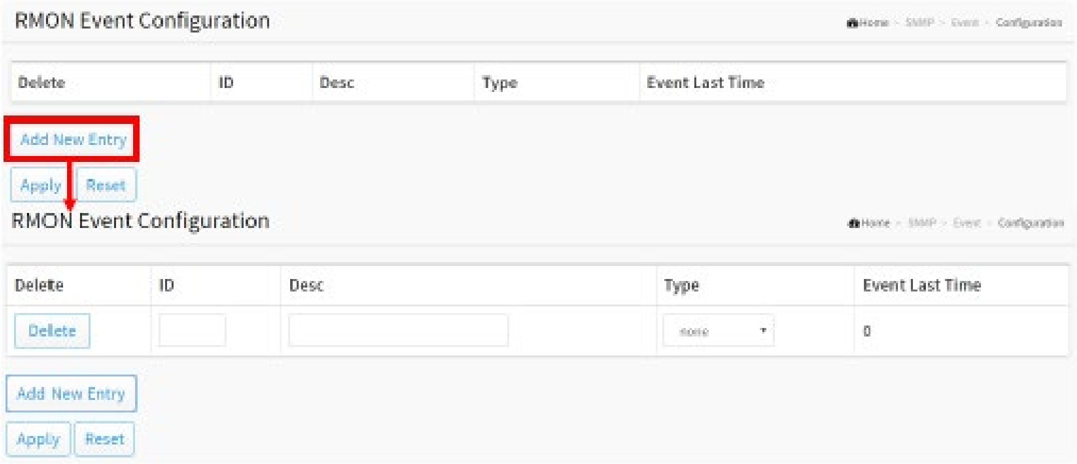
Next Entry : Updates the table, starting with the entry after the last entry currently displayed.

Event

Configuration

Configure RMON Event parameters on this page. The entry index key is ID. To configure RMON Event parameters in the web UI:

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



RMON Event Configuration

Home > SNMP > Event > Configuration

Delete	ID	Desc	Type	Event Last Time

RMON Event Configuration

Home > SNMP > Event > Configuration

Delete	ID	Desc	Type	Event Last Time
Delete			none	0

Figure 13-6.1: RMON Event Configuration

Parameter descriptions:

ID : Enter the index of the entry. The range is 1 to 65535.

Desc : Enter this event, the string length is 0 to 127, default is a null string.

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

> ***None***: No SNMP log is created, and no SNMP trap is sent.
>
> ***Log***: Create an SNMP log entry when the event is triggered.
>
> ***Snmp trap***: Send an SNMP trap when the event is triggered.
>
> ***Log and trap***: Create an SNMP log entry and send an SNMP trap when the event is triggered.

Event Last Time : Shows 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 to the table.

Apply : Click to save changes.

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

Status

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

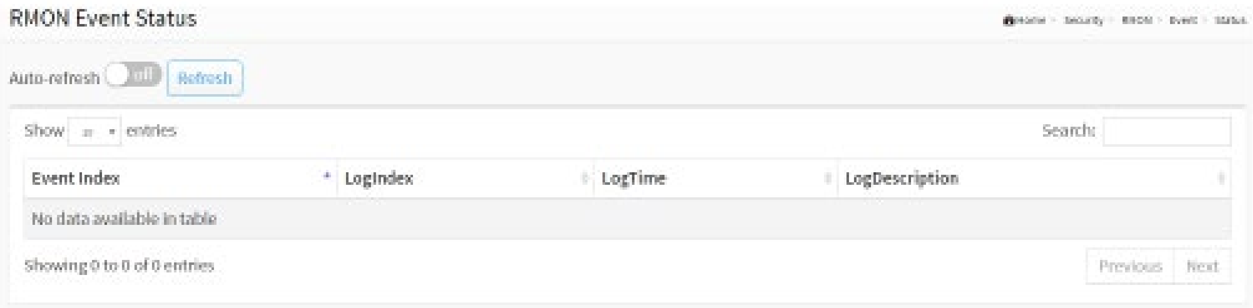
The "Start from Event Index and Log Index" lets you select the starting point in the Event table. Clicking the Refresh button will update the displayed table starting from that or the next closest Event table match.

The Next Entry button uses 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 displayed in the table. Use the First Entry button to start over.

Web Interface

To display RMON Event Status in the web UI:

1. Click SNMP, Event, and Status.
2. At the Show entries dropdown choose how many items you want to be displayed per page.
3. Check "Auto-refresh".
4. Click " Refresh" to refresh the port detailed statistics
5. Click Previous or Next button to change entries.



RMON Event Status

Auto-refresh off Refresh

Show entries Search:

Event Index	LogIndex	LogTime	LogDescription
No data available in table			

Showing 0 to 0 of 0 entries

Figure 13-6.2: RMON Event Status

Parameter descriptions:

Event Index : Indicates the index of the event entry.

LogIndex : Indicates the index of the log entry.

LogTIme : Indicates Event log time

LogDescription : Indicates the Event description.

Buttons

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

Refresh : Click to refresh the page immediately.

Previous : Click to display the previous table entry.

Next : Click to display the next table entry.

14. CFM

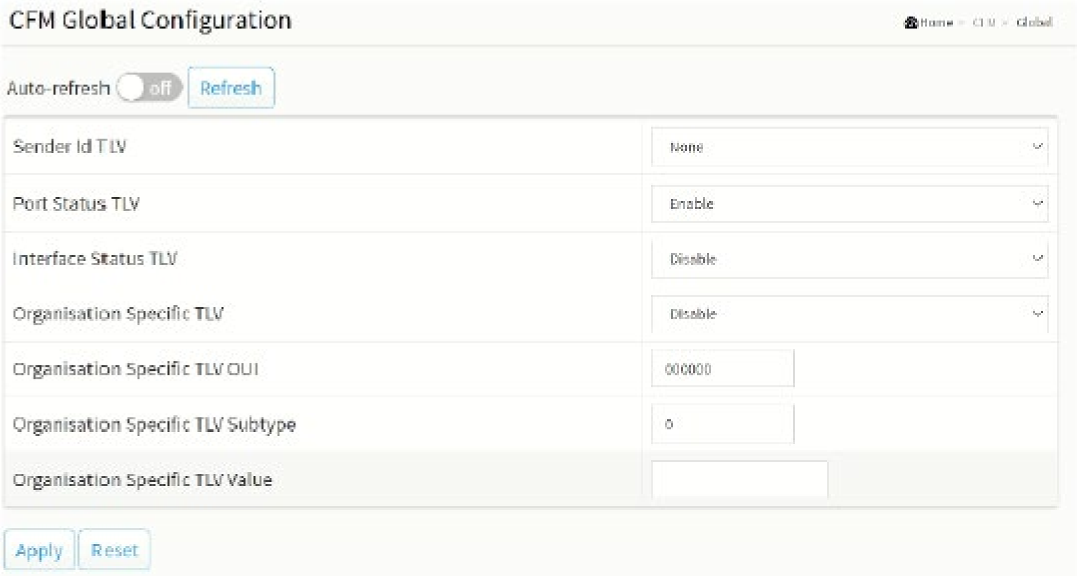
This section lets you set CFM (Connectivity Fault Management) Global, Service, and Domain parameters.

CFM is an IEEE standard that defines protocols and practices for OAM (Operations, Administration, and Maintenance) for paths through 802.1 bridges and LANs. It is an amendment to IEEE 802.1Q-2005 and was approved in 2007. IEEE 802.1ag is copied from the earlier ITU-T Recommendation Y.1731, which additionally addresses performance monitoring.

The standard **1**) defines maintenance domains, their constituent maintenance points, and the managed objects required to create and administer them. **2**) defines the relationship between maintenance domains and the services offered by VLAN-aware bridges and provider bridges. **3**) describes the protocols and procedures used by maintenance points to maintain and diagnose connectivity faults within a maintenance domain. **4**) provides means for future expansion of the capabilities of maintenance points and their protocols.

Global

Configure global CFM parameters on this page.



CFM Global Configuration

Sender Id TLV	None
Port Status TLV	Enable
Interface Status TLV	Disable
Organisation Specific TLV	Disable
Organisation Specific TLV OUI	000000
Organisation Specific TLV Subtype	0
Organisation Specific TLV Value	

Figure 13-1: CFM Global Configuration

Parameter descriptions:

Sender Id TLV : Choose whether and what to use as Sender ID TLVs in CCMs generated by this switch. This parameter can be overridden by Domain and Service level configuration.

None : Do not include Sender ID TLVs.

Chassis : Enable Sender ID TLV and send Chassis ID (MAC Address).

Manage : Enable Sender ID TLV and send Management address (IPv4 Address).

ChassisManage : Enable Sender ID TLV and send both Chassis ID (MAC Address) and Management Address (IPv4 Address).

Defer: Let the Domain configuration decide if Sender ID TLVs will be included.

Port Status TLV : Choose whether to send Port Status TLVs in CCMs generated by this switch. Can be overridden by Domain and Service level configuration.

Enable : Send Port Status TLVs in CCMs generated by this switch.

Disable : Do not send Port Status TLVs in CCMs generated by this switch.

Interface Status TLV : Choose whether to send Interface Status TLVs in CCMs generated by this switch. Can be overridden by Domain and Service level configuration.

Enable : Send Interface Status TLVs in CCMs generated by this switch.

Disable : Do not Send Interface Status TLVs in CCMs generated by this switch.

Organisation Specific TLV : Choose whether to send Organisation Specific TLVs in CCMs generated by this switch. Can be overridden by Domain and Service level configuration.

Enable : Send Organization Specific TLVs in CCMs generated by this switch.

Disable : Do not send Organisation Specific TLVs in CCMs generated by this switch.

Organisation Specific TLV OUI : This is the three-bytes OUI transmitted with the Organization-Specific TLVs. Enter as six characters 0-9, a-f.

Organisation Specific TLV Subtype : This is the subtype transmitted with the Organization-Specific TLV. Can be any value in the range [0; 255].

Organisation Specific TLV Value : This is the value transmitted in the Organization-Specific TLVs. Can be a printable character string of length 0-63.

Buttons

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

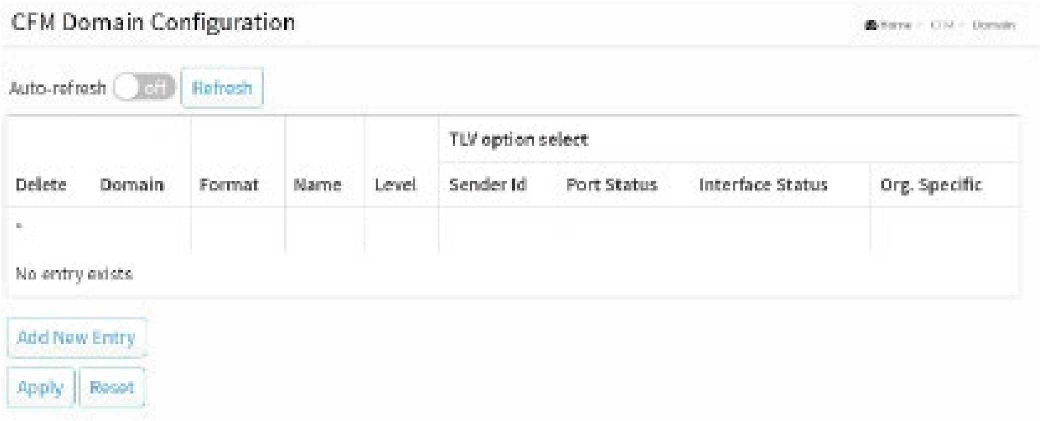
Refresh : Click to refresh the page immediately.

Apply : Click to save changes.

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

Domain

Configure CFM Domain parameters on this page. Ethernet Connectivity Fault Management (CFM per IEEE 802.1ag) is an end-to-end Ethernet OAM that can cross multiple domains to monitor the health of the entire service instance.



CFM Domain Configuration

					TLV option select			
Delete	Domain	Format	Name	Level	Sender Id	Port Status	Interface Status	Org. Specific
No entry exists								

Figure 13-2: CFM Domain Configuration

Parameter descriptions:

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

Domain : Name of the Domain. The value is a single word which begins with an alphabetic letter A-Z or a-z with a length of 1-15 letters.

Format : Select the MD name format.

> ***None*** : Select to mimic ITU-T Y.1731 MEG IDs (contains only the MEG ID).
>
> ***String*** : Select to mimic 802.1ag format (contains both MD and MA names).

Name : The contents of this parameter depend on the value of the format member. If format is None then Name is not used but will be set to all-zeros behind the scenes. This format is typically used by Y.1731 kind of PDUs. If format is String, then the Name must contain a string 1 - 43 characters long.

Level : MD/MEG level of this domain. Valid values are 0 - 7.

About leak prevention : Leak prevention is about discarding OAM PDUs with MEG levels lower than the MEP they hit when the OAM PDUs are ingressing the port on which the MEP resides, and to discard OAM PDUs with MEG levels at or lower than the MEP's when the OAM PDUs are ingressing other ports.

There are two categories of architectures, when it comes to leak-prevention: those that use Shared MEG level and those that use Independent MEG level:

> ***Shared MEG level*** : On Shared MEG level architectures, Port Down MEPs always perform level filtering no matter which VLAN ID (VID) OAM PDUs get classified to, unless the same port has a VLAN MEP on the VID in question. So if you have a Port MEP in VID X and a VLAN MEP in VID Y, an OAM frame arriving on the port and gets classified to VID X or VID Z will be handled/level-filtered by the Port MEP, whereas an OAM frame ingressing the port in VID Y will be handled by the VLAN MEP. Likewise, if the switch has a Port MEP on VID X on Port X and an OAM frame ingresses on VID Y on Port Y, it is subject to level filtering before egressing Port X, unless Port X also has a VLAN MEP on VID Y, in which case the VLAN MEP will take care of level-filtering the OAM PDU.

On Shared MEG level architectures, all Port MEPs must have the same MEG level and any VLAN MEP must have a MEG level higher than the Port MEPs' MEG level.

Independent MEG level : On Independent MEG level architectures, Port Down MEPs never perform level filtering on frames not classified to the MEP's VID. So if you have a Port MEP on VID X and a VLAN MEP on VID Y and an OAM frame ingresses any port on VID Z, it is not subject to handling/level-filtering by any of the two MEPs.

<u>**This switch exhibits Independent MEG level**</u>.

TLV option select : **Sender Id**: Default Sender ID TLV format to be used in CCMs generated by this Domain (may be overridden in service).

None : Do not include Sender ID TLVs.

Chassis : Enable Sender ID TLV and send Chassis ID (MAC Address).

Manage : Enable Sender ID TLV and send Management address (IPv4 Address).

ChassisManage : Enable Sender ID TLV and send both Chassis ID (MAC Address) and Management Address (IPv4 Address).

Defer : Let the global configuration decide if Sender ID TLVs will be included (may be overridden in service).

Port Status: Include or exclude Port Status TLV in CCMs generated by this Domain or let higher level determine (may be overridden in Service).

Disable : Do not include Port Status TLVs.

Enable : Include Port Status TLVs.

Defer : Let the global configuration decide if Port Status TLVs will be included (may be overridden in Service).

Interface Status: Include or exclude Interface Status TLV in CCMs generated by this Domain or let higher level determine (may be overridden in Service).

Disable : Do not include Interface Status TLVs.

Enable : Include Interface Status TLVs.

Defer : Let the global configuration decide if Interface Status TLVs will be included (may be overridden in Service).

Org. Specific: Exclude Organization-Specific TLV in CCMs generated by this Domain or let higher level determine (may be overridden in Service).

Disable : Do not include Organization-Specific TLVs.

Defer : Let the global configuration decide if Organization-Specific TLVs will be included (may be overridden in Service).

Buttons

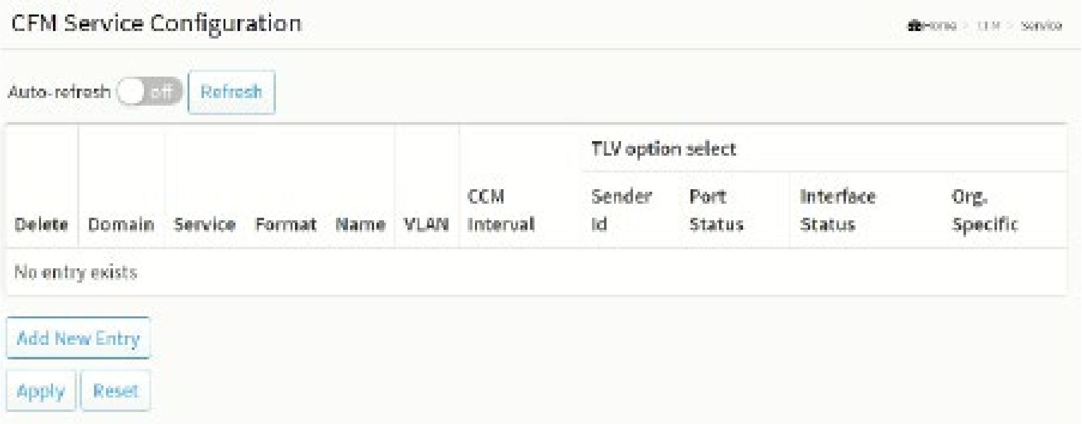
Add New Entry : Click to add a new Domain entry.

Apply : Click to save changes.

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

Service

Configure CFM Service parameters on this page.



							TLV option select			
Delete	Domain	Service	Format	Name	VLAN	CCM Interval	Sender Id	Port Status	Interface Status	Org. Specific
No entry exists										

Figure 13-3: CFM Service Configuration

Parameter descriptions:

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

Domain : Name of Domain under which this Service resides.

Service : Name of Service; a single word which begins with an alphabetic letter A-Z or a-z with length 1-15.

Format : Select the short Service name format. This decides how the value of the Name parameter will be interpreted. To mimic Y.1731 MEG IDs, create an MD instance with an empty name and use Y1731 ICC or Y1731 ICC CC. Possible values are: String, Two Octets, Y1731 ICC, and Y1731 ICC CC as described under the Name parameter below.

Name : The contents of this parameter depend on the value of the format member. Besides the limitations explained for each of them, the following applies in general:

If the Domain Format is ***None***, the size of this cannot exceed 45 bytes.

If the Domain Format is ***not*** ***None***, the size of this cannot exceed 44 bytes.

If Format is ***String***, the following applies:

Length must be in range [1; 44]

Contents must be in range [32; 126]

If Format is ***Two Octets***, the following applies: Name[0] and Name[1] will both be interpreted as unsigned 8-bit integers (allowing a range of [0; 255]). Name[0] will be placed in the PDU before Name[1]. The remaining available bytes in name will not be used.

If Format is ***Y1731 ICC***, the following applies:

Length must be 13.

Contents must be in range [a-z,A-Z,0-9]

Y.1731 specifies that it is a concatenation of ICC (ITU Carrier Code) and UMC (Unique MEG ID Code):

ICC: 1-6 bytes

UMC: 7-12 bytes

In principle, UMC can be any value in range [1; 127], but this API does not allow for specifying length of ICC, so the underlying code doesn't know where ICC ends and UMC starts. The Domain Format must be None.

If Format is ***Y1731 ICC CC***, the following applies:

Length must be 15.

First 2 chars (CC): Must be among [A-Z]

Next 1-6 chars (ICC): Must be among [a-z,A-Z,0-9]

Next 7-12 chars (UMC): Must be among [a-z,A-Z,0-9]

There may be ONE (slash) present in name[3-7]. The Domain format must be None.

VLAN : The MA's primary VID. A primary VID of 0 means that all MEPs created within this MA will be created as port MEPs (interface MEPs). There can only be one port MEP per interface. A given port MEP may still be created with tags, if that MEP's VLAN is non-zero.

A non-zero primary VID means that all MEPs created within this MA will be created as VLAN MEPs. A given MEP may be configured with another VLAN than the MA's primary VID, but it is impossible to have untagged VLAN MEPs.

CCM Interval : The CCM rate of all MEPs bound to this Service.

TLV option select:

Sender Id: Default Sender ID TLV format to be used in CCMs generated by this Service.

None : Do not include Sender ID TLVs.

Chassis : Enable Sender ID TLV and send Chassis ID (MAC Address).

Manage : Enable Sender ID TLV and send Management address (IPv4 Address).

ChassisManage : Enable Sender ID TLV and send both Chassis ID (MAC Address) and Management Address (IPv4 Address).

Defer: Let the Domain configuration decide if Sender ID TLVs will be included.

Port Status: Include or exclude Port Status TLV in CCMs generated by this Service or let higher level determine.

Disable : Do not include Port Status TLVs.

Enable : Include Port Status TLVs.

Defer : Let the Domain configuration decide if Port Status TLVs will be included.

Interface Status: Include or exclude Interface Status TLV in CCMs generated by this Service or let higher level determine.

Disable : Do not include Interface Status TLVs.

Enable : Include Interface Status TLVs.

Defer : Let the Domain configuration decide if Interface Status TLVs will be included.

Org. Specific : Exclude Organization-Specific TLV in CCMs generated by this Service or let higher level determine.

Disable : Do not include Organization-Specific TLVs.

Defer : Let the Domain configuration decide if Organization-Specific TLVs will be included.

Buttons

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

Refresh : Click to manually update webpage values immediately.

Add New Entry : Click to add a new Domain entry to the table.

Apply : Click to save changes.

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

MEP

Configure CFM MEP (Maintenance Entity Point) parameters on this page. This switch supports two types of MEPs: Port Down-MEPs and VLAN Down-MEPs:

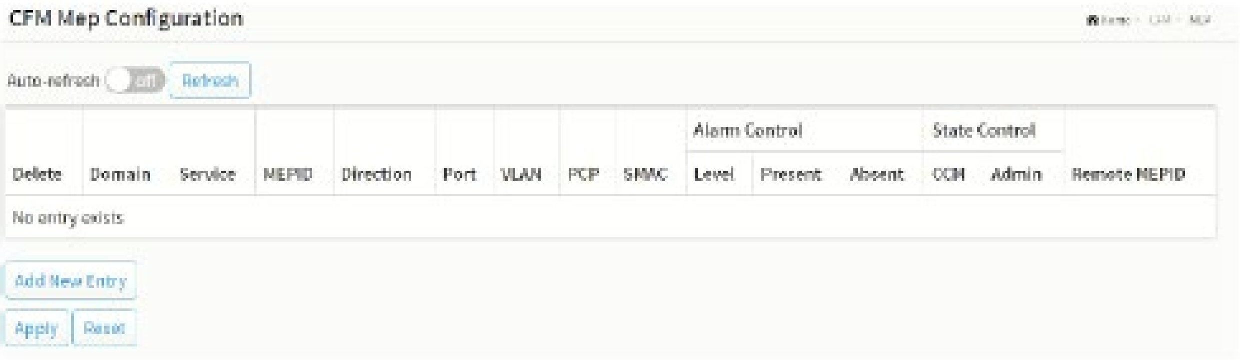
> **Port Down-MEPs** : In 802.1Q terminology, Port MEPs are located below the EISS entity (i.e., closest to the physical port). Port MEPs are used by, for example, APS for protection purposes. Port MEPs are created when the encompassing service has type "Port". Port MEPs may send OAM PDUs tagged or untagged. An OAM PDU will be sent untagged only if the MEP's VLAN is set to "Inherit" (0). Any other value will cause it to be sent tagged with the port's TPID, whether the VLAN matches the port's PVID and that PVID is meant to be sent untagged.
>
> **VLAN Down-MEPs** : In 802.1Q terminology, VLAN MEPs are located above the EISS (Enhanced Internal Sub-layer Service) entity. This means that tagging of OAM PDUs will follow the port's VLAN configuration. Thus, if a VLAN MEP is created on the Port's PVID and PVID is configured to be untagged, OAM PDUs will be transmitted untagged. VLAN MEPs are created when the encompassing service has type "VLAN".

Down-MEP creation rules:

There are a few rules for creating Down-MEPs:

1. There can only be one Port MEP on the same port.
2. There can only be one VLAN MEP on the same port and VLAN.
3. A VLAN MEP must have a higher MD/MEG level than a Port MEP on the same port and VLAN.

These checks are performed automatically on administratively enabled MEPs when you change a particular MEP, change the Service Type from Port to VLAN or vice versa, or change the domain's MD/MEG level.



CFM Mep Configuration

Auto-refresh off Refresh

									Alarm Control			State Control		
Delete	Domain	Service	MEPID	Direction	Port	VLAN	PCP	SMAC	Level	Present	Absent	CCM	Admin	Remote MEPID
No entry exists														

Figure 13-4: CFM Mep Configuration

Parameter descriptions:

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

Domain : The name of Domain under which this MEP resides.

Service : The name of Service under which this MEP resides.

MEPID : The identification of this MEP. Must be an integer [1..8091]

Direction : Set whether this MEP is an Up-MEP or a Down-MEP.

Port : Port on which this MEP resides.

VLAN : VLAN ID. Use the value 0 to indicate untagged traffic (implies a port MEP).

PCP : Choose PCP value in PDUs' VLAN tag. Not used if untagged.

SMAC : Set a Source MAC address to be used in CCM PDUs originating at this MEP. Must be a unicast address. Format is XX:XX:XX:XX:XX:XX. If all-zeros, the switch port's MAC address will be used instead.

Alarm Control :

Level: If a defect is detected with a priority higher than this level, a fault alarm notification will be generated. The valid range is [1; 6] with 1 indicating that any defect will cause a fault alarm and 6 indicating that no defect can cause a fault alarm. See 802.1Q-2018, clause 20.9.5, *LowestAlarmPri*. The possible defects and their priorities are:

Short name	Description	Priority
DefRDICCM	Remote Defect Indication	1
DefMACstatus	MAC Status	2
DefRemoteCCM	Remote CCM	3
DefErrorCCM	Error CCM Received	4
DefXconCCM	Cross Connect CCM Received	5

Present: The time in milliseconds that defects must be present before a fault alarm notification is issued. Default is 2500 ms.

Absent: The time in milliseconds that defects must be absent before a fault alarm notification is reset. Default is 10000 ms.

State Control :

CCM: Enable or disable generation of continuity-check messages (CCMs)

Admin: Enable or disable this MEP. When this MEP is enabled, it will check received/missing CCMs and can raise defects.

Remote MEPID : Specify the Remote MEP that this MEP is expected to receive CCM PDUs from. Must be an integer [0..8091] where 0 means undefined. The value of Remote MEPID must be different from the value of MEPID.

Buttons

Auto-refresh : Check this box to automatically refresh the page immediately.

Refresh : Click to update values.

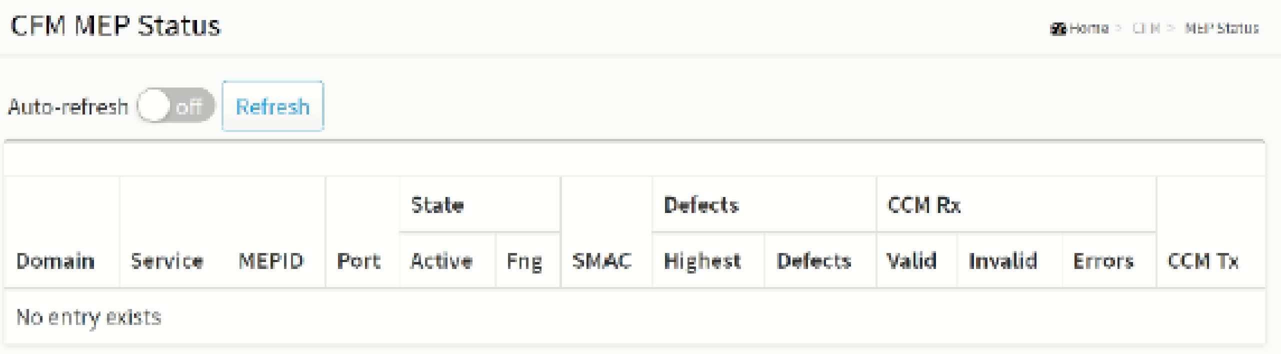
Add New Entry : Click to add a new MEP entry.

Apply : Click to save changes.

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

MEP Status

This page displays CFM MEP (Maintenance association End Point) Status.



CFM MEP Status

Home > CFM > MEP Status

Auto-refresh off Refresh

				State			Defects		CCM Rx			
Domain	Service	MEPID	Port	Active	Fng	SMAC	Highest	Defects	Valid	Invalid	Errors	CCM Tx
No entry exists												

Figure 13-5: CFM MEP Status

Parameter descriptions:

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

Domain : Name of Domain under which this MEP resides.

Service : Name of Service under which this MEP resides.

MEPID : The identification of this MEP.

Port : Port on which this MEP resides.

State Active : Operational state of the MEP.

off : OFF indicates that the MEP Admin State is disabled.

down : DOWN indicates the MEP Admin State is enabled, but an error state exists.

up : UP indicates the MEP Admin State is enabled, and no errors and defects exist.

State Fng : The current state of the Fault Notification Generator state machine. Values will be one of these:

State	Description
reset	No defect has been present since reset timer expired or State Machine was last reset.
defect	A defect is present, but not for a long enough time to be reported.
reportDefect	A transient state during which the defect is reported.
defectReported	A defect is present, and some defect has been reported.
defectClearing	No defect is present, but the ResetTime timer has not yet expired.

SMAC : This MEP's MAC address.

Defects Highest : The highest priority defect that has been present since the MEP's Fault Notification Generator state machine was last in the reset state.

Defects : A MEP can detect and report several defects, and multiple defects can be present at the same time. This is indicated the following letter code.

Code	Defect	Description
-	Defect	not present Defect not present.
R	someRDIdefect	RDI received from at least one remote MEP.
M	someMACstatusDefect	Received Port Status TLV != psUp or Interface Status TLV != isUp.
C	someRMEPCCMdefect	Valid CCM is not received within 3.5 times CCM interval from at least one remote MEP.
E	errorCCMdefect	Received CCM from an unknown remote MEP-ID or CCM interval mismatch.
X	xconCCMdefect	Received CCM with an MD/MEG level smaller than configured or wrong. MAID/MEGID (cross-connect).

CCM Rx : CCM PDUs received by this MEP.

Valid: Total number of CCMs that hit this MEP and passed the validation test.

Invalid: Total number of CCMs that hit this MEP and didn't pass the validation test.

Errors: Total number of out-of-sequence errors seen from RMEPs.

CCM Tx : Total number of CCM PDUs transmitted by this MEP.

Buttons

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

Refresh : Click to manually update webpage values immediately.

15. APS

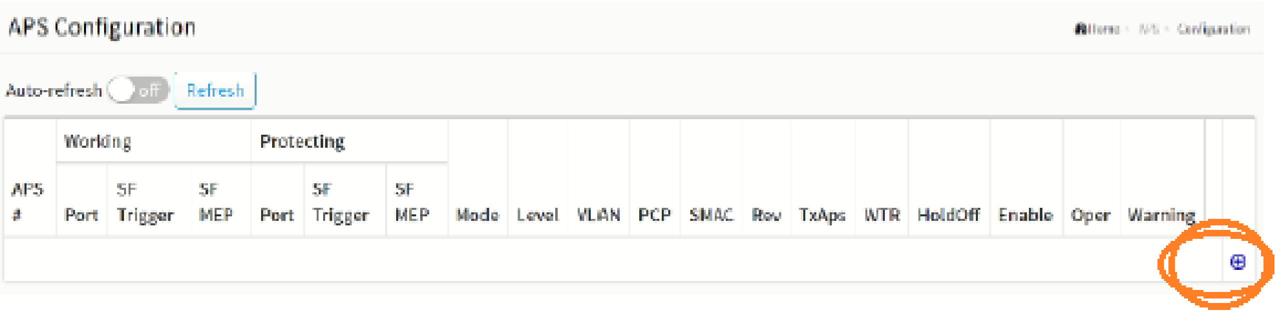
The APS (Automatic Protection Switching) module implements the protocol and linear protection switching mechanisms for point-to-point VLAN-based ETH SNC in Ethernet transport networks. APS is defined by the ITU-T G.8031 standard.

Point-to-point VLAN-based ETH SNCs (SubNetwork Connection) provide connectivity between two ETH flow points in an ETH flow domain. VLAN identifiers (VIDs) can be used to identify point-to-point VLAN-based ETH SNC(s) within ETH links. Additional details on ETH and related atomic functions can be obtained from ITU-T G.8021 and ITU-T G.8010. Other entities to be protected are for further study.

In the linear protection architecture defined in this version of the Recommendation, protection switching occurs at the two distinct endpoints of a point-to-point VLAN-based ETH SNC. Between these endpoints, there will be both "working" and "protection" transport entities.

14-1 Configuration

This page lets you create and configure a maximum of 14 APS Instances. Click the plus sign (⊕) to add a row to the table.



APS Configuration

Home › APS › Configuration

Auto-refresh ○ off Refresh

	Working			Protecting																
APS #	Port	SF Trigger	SF MEP	Port	SF Trigger	SF MEP	Mode	Level	VLAN	PCP	SMAC	Rev	TxAps	WTR	HoldOff	Enable	Oper	Warning		
																				⊕

Figure 14-1: APS Configuration

Parameter descriptions:

CCM Tx : Total number of CCM PDUs transmitted by this MEP.

APS # : The ID of the APS. You can create a maximum of 14 APS instances. Click on the linked text to display the APS Instance page (see below), where you can reset counters and issue commands.

Port : The Port this flow is attached to.

SF Trigger : Selects whether Signal Fail (SF) comes from the link state of a given Port, or from a Down-MEP.

SF MEP : The *Domain::Service::MEPID* refers to a MEP instance which will represent the Working flow. Only used when SF Trigger is MEP. The selected MEP instance does not need to exist when this APS is configured.

Mode : The APS mode of operation:

> ***1:1*** : This will create a 1:1 APS. In the linear 1:1 protection switching architecture, the protection transport entity is dedicated to the working transport entity. However, normal traffic is transported either on the working transport entity or on the protection transport entity using a selector bridge at the source of the protected domain. The selector at the sink of the protected domain selects the entity which carries the normal traffic.
>
> ***1+1 Uni*** : This will create a 1+1 Unidirectional APS.

1+1 Bi : This will create a 1+1 Bidirectional APS. In the linear 1+1 protection switching architecture, a protection transport entity is dedicated to each working transport entity. The normal traffic is copied and fed to both working and protection transport entities with a permanent bridge at the source of the protected domain. The traffic on working and protection transport entities is transmitted simultaneously to the sink of the protected domain, where a selection between the working and protection transport entities is made based on some predetermined criteria, such as server defect indication.

Level : The MD/MEG Level (0-7).

VLAN : The VLAN ID used in the L-APS PDUs. 0 means untagged.

PCP : PCP (priority) (default 7). The PCP value used in the VLAN tag unless the L-APS PDU is untagged. Must be a value in range 0 - 7.

SMAC : Source MAC address used in L-APS PDUs. Must be a unicast address. If all-zeros, the switch port's MAC address will be used.

Rev : When checked, the port recovery mode is ***revertive***, that is, traffic switches back to the working port after the condition(s) causing a switch has cleared. In the case of clearing a command (e.g. forced switch), this happens immediately. In the case of clearing of a defect, this generally happens after the expiry of the WTR (Wait-To-Restore) timer.

When unchecked, the port recovery mode is ***non-revertive*** and traffic is allowed to remain on the protect port after a switch reason has cleared.

TxAps : Choose whether this end transmits APS PDUs. Only used for 1+1, unidirectional.

WTR : When Rev is checked, WTR (Wait-To-Restore) sets how many seconds to wait before restoring to the working port after a fault condition has cleared. The valid range 1 – 720 seconds.

HoldOff : When a new (or more severe) defect occurs, the hold-off timer will be started, and the event will be reported after the timer expires. HoldOff time is measured in milliseconds, and valid values are 0 – 10000 ms. The default is 0, which means immediate reporting of the defect.

Enable : The administrative state of this APS instance. Check to make it function normally and uncheck to make it cease functioning.

Oper : This field cannot be configured but shows the operational state. You can click on the link in the APS # field to get more details on the status (see below).

up : APS instance is functional.

down : APS instance is not functional.

Warning : If the operational state is Active, the APS instance is indeed active, but it may be that it doesn't run as the administrator thinks, because of configuration errors, which are reflected in the warnings below.

The Warning information is indicated by down: no warning, down: warning. Use the tooltip to get detailed warning information.

Configuration Buttons : You can modify each APS in the table using these buttons:

ʘ **Edit**: Edits the APS row.

ʘ **Delete**: Deletes the APS.

⊕ **Add**: Adds new APS.

Buttons

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

Refresh : Click to manually update table values immediately.

APS Instance page

When you click on the linked text in the APS # column (see above) the APS Instance page displays as shown and described below. Here you can reset counters and issue commands.

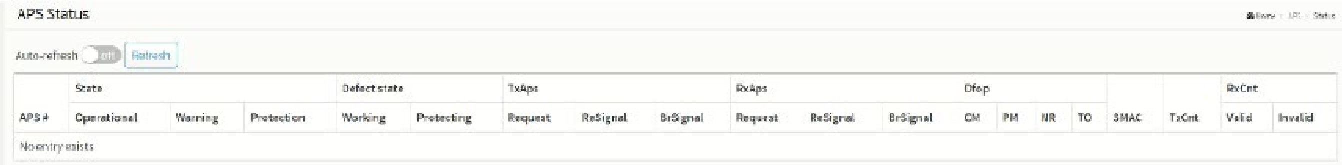
To be supplied

Figure 14-2: APS Instance

Parameter descriptions: To be supplied

Status

This page displays the current status of the Automatic Protection Switching instances.



APS Status

Auto-refresh off Refresh

	State			Defect state		TxAps			RxAps			Dfop						RxCnt	
APS #	Operational	Warning	Protection	Working	Protecting	Request	ReSignal	BrSignal	Request	ReSignal	BrSignal	CM	PM	NR	TO	SMAC	TxCnt	Valid	Invalid
No entry exists																			

Figure 14-1: APS Status

Parameter descriptions:

APS # : The ID of the APS. Click on link to get to APS instance page, you can reset counters and issue commands.

State, Operational : The operational state of the APS instance. There are many ways to not have the instance active. Each of them has its own value. Only when the state is Active, will the APS instance be active and up and running. If the Operational state is not "Active", the remaining fields are invalid. The possible values of this field are shown below:

Administratively disabled: Instance is inactive because it is administratively disabled.

Active: The instance is active and up and running.

Internal Error: Instance is inactive because an internal error has occurred.

Working MEP not Found: Instance is inactive, because the Working MEP is not found.

Protecting MEP not Found: Instance is inactive, because the Protecting MEP is not found.

Working MEP is not administrative active: Instance is inactive, because the Working MEP is not admin enabled.

Protecting MEP is not administrative active: Instance is inactive, because the Protecting MEP is not admin enabled.

Working MEP is not a Down MEP: Instance is inactive, because the Working MEP is not a Down-MEP.

Protecting MEP is not a Down MEP: Instance is inactive, because the Protecting MEP is not a Down-MEP.

Working and Protecting MEP use the same interface: Instance is inactive, because both Working and Protecting MEPs use the same I/F.

Another instance uses the same Working port: Instance is inactive, because another instance uses the same Working port.

State, Warning : If the operational state is Active, the APS instance is indeed active, but it may be that it doesn't run as the administrator thinks, because of configuration errors, which are reflected in the warnings below.

The Warning information is indicated by down: no warning, down: warning. Use the tooltip to get the detailed warning information.

State, Protection : The possible protection group states. The letters refer to the state noted in G.8031 Annex:

No request Working: **A**.

No request Protecting: **B**.

Lockout: **C**.

Forced Switch: **D**.

Signal fail Working: **E**.

Signal fail Protecting: **F**.

Manual switch to Protecting: **G**.

Manual switch to Working: **H**.

Wait to restore: **I**.

Do not revert: **J**.

Exercise Working: **K**.

Exercise Protecting: **L**.

Reverse request Working: **M**.

Reverse request Protecting: **N**.

Signal degrade Working: **P**.

Signal degrade Protecting: **Q**.

Defect state, Working, Protection : The possible values of this field are shown below:

ok: The port defect state is OK

sd: The port defect state is Signal Degrade

sf: The port defect state is Signal Fail

TxAps, RxAps – Request : The possible transmitted or received APS request according to G.8031, Table 11-1.

nr: No Request.

dnr: Do Not Revert.

rr: Reverse Request.

exer: Exercise.

wtr: Wait-To-Restore.

ms: Manual Switch.

sd: Signal Degrade.

sfW: Signal Fail for Working.

fs: Forced Switch.

sfP: Signal Fail for Protect.

lo: Lockout.

TxAps, ReSignal : Transmitted requested signal according to G.8031 figure 11-2.

TxAps, BrSignal : Transmitted bridged signal according to G.8031 figure 11-2.

RxAps, ReSignal : Received requested signal according to G.8031 figure 11-2.

RxAps, BrSignal : Received bridged signal according to G.8031 figure 11-2.

Dfop : The "Failure of Protocol defect" and presence of a defect is indicated by up: no defect, down: defect.

CM: Configuration Mismatch (received APS PDU on working interface within last 17.5 seconds).

PM : Provisioning Mismatch (far and near ends are not using the same mode; bidir only)

NR : No Response (far end hasn't agreed on 'Requested Signal' within 50 ms; bidir only)

TO : Time Out (near end hasn't received a valid APS PDU within last 17.5 seconds; bidir only)

SMAC : Source MAC address of last received APS PDU or all-zeros if no PDU has been received.

TxCnt : Number of APS PDU frames transmitted.

RxCnt, Valid : Number of valid APS PDU frames received on the protect port.

RxCnt, Invalid : Number of invalid APS PDU frames received on the protect port.

Buttons

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

Refresh : Click to manually update values immediately.

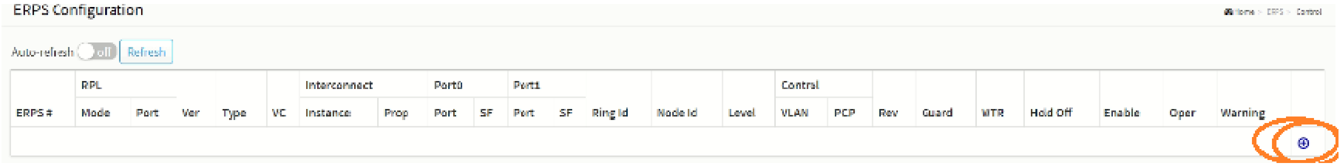
16. ERPS

This page lets you set and view ERPS instances.

The switch supports ITU-T G.8032 Ethernet Ring Protection Switching. Recommendation ITU-T G.8032/Y.1344 defines the automatic protection switching (APS) protocol and protection switching mechanisms for Ethernet layer network (ETH) ring topologies. Included are details on Ethernet ring protection characteristics, architectures and the ring APS (R-APS) protocol.

Control

Click the plus sign (⊕) to add a row to the table.



ERPS Configuration

Home > ERPS > Control

Auto-refresh off Refresh

	RPL					Interconnect		Port0		Port1					Control									
ERPS #	Mode	Port	Ver	Type	VC	Instance	Prop	Port	SF	Port	SF	Ring Id	Node Id	Level	VLAN	PCP	Rev	Guard	WTR	Hold Off	Enable	Oper	Warning	
																								⊕

Figure 15-1: ERPS Configuration

Parameter descriptions:

Delete : This box is used to mark an EPS for deletion in next save operation.

ERPS # : The ID of ERPS. Valid range 1 - 64.

RPL Mode : The Ring Protection Link mode. Possible values are:

None : There is no link.

Owner : The Ring Protection Link mode is “Owner”.

Neighbor : The Ring Protection Link mode is “Neighbor”.

RPL Port : Indicates whether it is port0 or port1 that is the Ring Protection Link. Not used if RPL Mode is None.

Ver : ERPS protocol version. v1 and v2 are supported.

Type : Type of ring. Possible values:

Major : ERPS major ring (G.8001-2016, clause 3.2.39).

Sub : ERPS sub-ring (G.8001-2016, clause 3.2.66).

InterSub : ERPS sub-ring on an interconnection node (G.8001-2016, clause 3.2.66).

VC : Controls whether to use a Virtual Channel with a sub-ring.

Interconnect Instance : For a sub-ring on an interconnection node, this must reference the instance ID of the ring to which this sub-ring is connected.

Interconnect Prop : Controls whether the ring referenced by Interconnect Instance will propagate R-APS flush PDUs whenever this sub-ring's topology changes.

Port0/Port1 Interface : Interface index of ring protection Port0/Port1.

Port0/Port1 SF : Select whether Signal Fail (SF) comes from the link state of a given interface, or from a Down-MEP. Possible values:

MEP: Down-MEP

Link: Link

Ring Id : The Ring ID is used, along with the control VLAN, to identify R-APS PDUs as belonging to a particular ring.

Node Id : The Node ID is used inside the R-APS specific PDU to uniquely identify this node (switch) on the ring.

Level : MD/MEG Level of R-APS PDUs we transmit.

Control VLAN : The VLAN on which R-APS PDUs are transmitted and received on the ring ports.

Control PCP : The PCP value used in the VLAN tag of the R-APS PDUs.

Rev : Revertive (true) or Non-revertive (false) mode.

Guard : Guard time in ms. Valid range is 10 - 2000 ms.

WTR : Wait-to-Restore time in seconds. Valid range 1 - 720 sec.

Hold Off : Hold off time in ms. Value is rounded down to 100ms precision. The valid range is 0 - 10000 ms.

Enable : The administrative state of this APS ERPS. Check to make it function normally and uncheck to make it cease functioning.

Oper : The operational state of ERPS instance.

up: Active

down: Disabled or Internal error.

Warning : Operational warnings of ERPS instance.

up: No warnings

down: There are warnings, use the tooltip to see.

Configuration Buttons : You can modify each APS in the table using these buttons:

Θ **Edit**: Edits the APS row.

Θ **Delete**: Deletes the APS.

⊕ **Add**: Adds new APS.

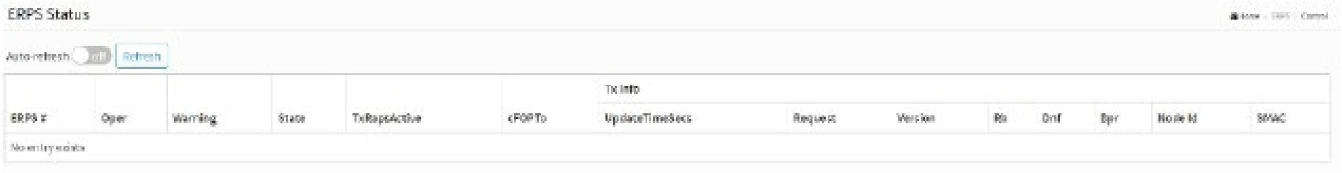
Buttons

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

Refresh : Click to manually refresh the page immediately.

Status

This page shows the current status of the ERPS instances.



ERPS Status

					Tx Info							
ERPS #	Oper	Warning	State	TxRapsActive	cFOPTo	UpdateTimeSecs	Request	Version	Rb	Dnf	Bpr	Node Id	SMAC
No entry exists													

Figure 15-1: ERPS Configuration

Parameter descriptions:

ERPS # : The ID of the ERPS. Click on link to display the ERPS detailed instance page, where you can reset counters and issue commands (see below).

Oper : The operational state of ERPS instance.

up: Active.

down: Disabled or Internal error.

Warning : Operational warnings of ERPS instance.

up: No warnings.

down: There are warnings, use tooltip to see.

State : Specifies protection/node state of ERPS.

TxRapsActive : Specifies whether the switch is to be transmitting R-APS PDUs on its ring ports.

cFOPTo : Failure of Protocol - R-APS Rx Time Out.

UpdateTimeSecs : Time in seconds since boot that this structure was last updated.

Request : Request/state according to G.8032, table 10-3.

Version : Version of received/used R-APS Protocol. 0 means v1, 1 means v2, etc.

Rb : RB (RPL blocked) bit of R-APS info. See Figure 10-3 of G.8032.

Dnf : DNF (Do Not Flush) bit of R-APS info. See Figure 10-3 of G.8032.

Bpr : BPR (Blocked Port Reference) of R-APS info. See Figure 10-3 of G.8032.

Node Id : The Node ID of this request.

SMAC : The Source MAC address used in the request/state.

Buttons

Auto-refresh : Check this box to automatically refresh the page every three seconds.

Refresh : Click to manually refresh the page immediately.

ERPS detailed instance page

Click on the linked ERPS # to display the ERPS detailed instance page as shown and described below. Here you can reset counters and issue commands.

To be supplied

Parameter descriptions: To be supplied.

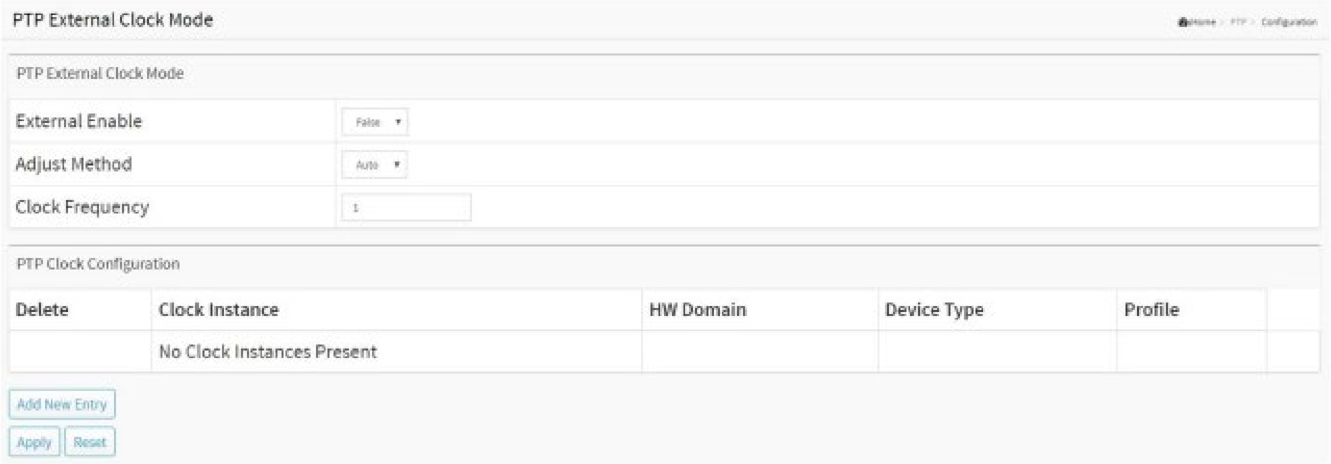
17. PTP

Configuration

This page lets you set and view current Precision Timing Protocol parameters. The switch let you configure up to four PTP instances.

To configure a PTP instance in the web UI:

1. Click PTP and Configuration.
2. Set the PTP External Clock Mode parameters.
3. Click the Add New Entry button.
4. Specify the parameters in each blank field.
5. Click the Apply button to save the settings.
6. To cancel the settings, click the Reset button to revert to previously saved values.



PTP External Clock Mode

PTP External Clock Mode

External Enable	False ▾
Adjust Method	Auto ▾
Clock Frequency	1

PTP Clock Configuration

Delete	Clock Instance	HW Domain	Device Type	Profile	
	No Clock Instances Present				

Figure 16-1a: PTP External Clock Mode Configuration

Parameter descriptions:

PTP External Clock Mode

External Enable : This selection box lets you configure External Clock output. These values are possible:

True : Enable the external clock output.

False : Disable the external clock output (default).

Adjust Method : This selection box lets you configure the Frequency adjustment configuration as follows:

LTC : Select Local Time Counter (LTC) frequency control.

Single : Select SyncE DPLL frequency control, if allowed by SyncE.

Independent : Select an oscillator independent of SyncE for frequency control, if supported by the HW

Common : Select second DPLL for PTP, Both DPLL have the same (SyncE recovered) clock.

Auto : AUTO Select clock control, based on PTP profile and available HW resources (default).

Clock Frequency : This lets you set the Clock Frequency in the range 1 – 25000000 Hz (1 - 25MHz).

PTP Clock Configuration

Delete : Check this box and click on 'Save' to delete the clock instance.

Clock Instance : Indicates the instance number of a particular Clock Instance [0..3]. Click on the Clock Instance number to edit the Clock details.

HW Domain : Indicates the HW clock domain used by the clock.

Device Type : Indicates the Type of the Clock Instance. There are five Device Types:

Ord-Bound - clock's Device Type is Ordinary-Boundary Clock.

P2p Transp - clock's Device Type is Peer to Peer Transparent Clock.

E2e Transp - clock's Device Type is End to End Transparent Clock.

Master Only - clock's Device Type is Master Only.

Slave Only - clock's Device Type is Slave Only.

Profile : Indicates the profile used by the clock.

Buttons

Add New Entry : Click to add a new clock instance.

Apply : Click to save changes.

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

PTP Configuration Example (four PTP Instances)

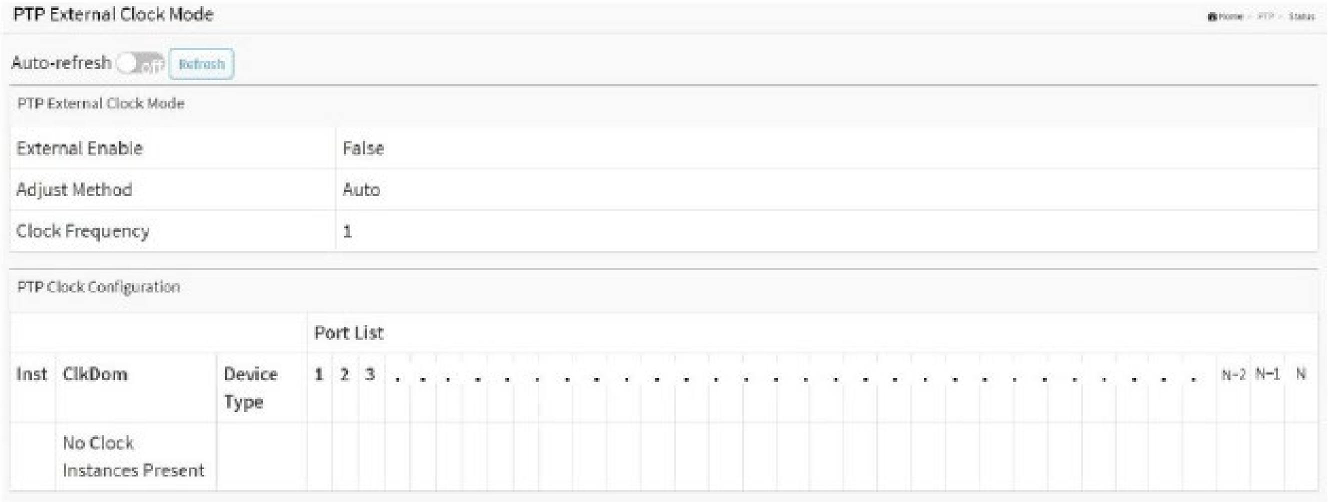
To be supplied

Status

This page lets you view current PTP clock settings. If none are configured, displays the message "*No Clock Instances Present*".

To display PTP status in the web UI:

1. Click PTP and Status.
2. Specify the PTP parameters.
3. Click Apply to apply the changes.



PTP External Clock Mode

PTP External Clock Mode

External Enable	False
Adjust Method	Auto
Clock Frequency	1

PTP Clock Configuration

			Port List																																	
Inst	ClkDom	Device Type	1	2	3	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	N-2	N-1	N
	No Clock Instances Present																																			

Figure 16-2: PTP External Clock Mode page

Parameter descriptions:

<u>PTP External Clock Mode</u>

External Enable : Shows the current External clock output configuration:

True : Enable the external clock output.

False : Disable the external clock output.

Adjust Method : Shows the current Frequency adjustment configuration:

LTC : Use Local Time Counter (LTC) frequency control.

Single : Use SyncE DPLL frequency control, if allowed by SyncE.

Independent : Use an oscillator independent of SyncE for frequency control, if supported by the hardware.

Common : Use second DPLL for PTP, Both DPLL have the same (SyncE recovered) clock.

Auto : Auto Select clock control, based on PTP profile and available hardware resources.

Clock Frequency : Shows the current clock frequency used by the External Clock. Possible values are 1 - 25000000 (1 - 25MHz).

PTP Clock Configuration

Inst : Indicates the Instance of a particular Clock Instance [0..3]. Click on a Clock Instance number to monitor the clock instance’s details.

ClkDom : Indicates the Clock domain used by a particular Clock Instance [0..3].

Device Type : Indicates the Type of the Clock Instance. There are five Device Types.

Ord-Bound - Clock's Device Type is Ordinary-Boundary Clock.

P2p Transp - Clock's Device Type is Peer to Peer Transparent Clock.

E2e Transp - Clock's Device Type is End to End Transparent Clock.

Master Only - Clock's Device Type is Master Only.

Slave Only - Clock's Device Type is Slave Only.

Port List : Shows the ports configured for that Clock Instance.

Buttons

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

Refresh : Click to refresh the page immediately.

Apply : Click to save changes.

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

Clock Details

Click on a Clock Instance number to monitor the Clock details:

To be supplied

Parameter descriptions: To be supplied

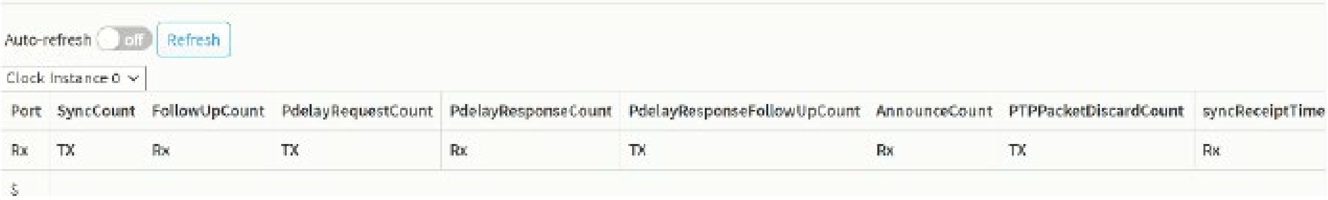
802.1AS Statistics

This page lets you view current 802.1AS Clock Instance-specific statistics. The IEEE 802.1AS standard enables stations attached to bridged LANs to meet the respective jitter, wander, and time synchronization requirements for time-sensitive applications. IEEE 802.1AS-2011 is part of the IEEE Audio Video Bridging (AVB) group of standards, further extended by the IEEE 802.1 Time-Sensitive Networking (TSN) Task Group.
In particular, 802.1AS defines how IEEE 802.3 (Ethernet), IEEE 802.11 (Wi-Fi), and MoCA (Multimedia over Coax Alliance) can all be parts of the same PTP timing domain.

Web Interface

To display 802.1AS Clock Instance-specific statistics in the web UI:

1. Click PTP and Status.
2. Select the Clock Instance (0-3) at the dropdown.
3. Click Apply to display the clock instance statistics.



Clock Instance 0

Port	SyncCount	FollowUpCount	PdelayRequestCount	PdelayResponseCount	PdelayResponseFollowUpCount	AnnounceCount	PTPPacketDiscardCount	syncReceiptTime
Rx	TX	Rx	TX	Rx	TX	Rx	TX	Rx
5								

Figure 16-3: 802.1AS Clock Instance Specific Statistics

Parameter descriptions:

Instance : At the dropdown select a PTP Instance (Clock Instance 0-3 or CMLDS (Common Mean Link Delay Service)).

802.1AS Received counters

SyncCount : A counter that increments every time when synchronization information is received.

FollowUpCount : A counter that increments every time when a Follow Up message is received.

PdelayRequestCount : A counter that increments every time when a Pdelay_Req message is received.

PdelayResponseCount : A counter that increments every time when a Pdelay_Resp message is received.

PdelayResponseFollowUpCount : A counter that increments every time when a Pdelay_Resp_Follow_Up message is received.

AnnounceCount : A counter that increments every time when an Announce message is received.

PTPPacketDiscardCount : A counter that increments every time when a PTP message is discarded.

syncReceiptTimeoutCount : A counter that increments every time when sync receipt timeout occurs.

announceReceiptTimeoutCount : A counter that increments every time when announce receipt timeout occurs.

pdelayAllowedLostResponsesExceededCount : A counter that increments every time the value of the variable lostResponses exceeds the value of the variable allowedLostResponses.

802.1As Transmit Counters

SyncCount : A counter that increments every time synchronization information is transmitted.

FollowUpCount : A counter that increments every time a Follow_Up message is transmitted.

PdelayRequestCount : A counter that increments every time a Pdelay_Req message is transmitted.

PdelayResponseCount : A counter that increments every time a Pdelay_Resp message is transmitted.

PdelayResponseFollowUpCount : A counter that increments every time a Pdelay_Resp_Follow_Up message is transmitted.

AnnounceCount : A counter that increments every time an Announce message is transmitted.

Buttons

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

Refresh : Click to refresh the page immediately.

Display : Click to show the configured values.

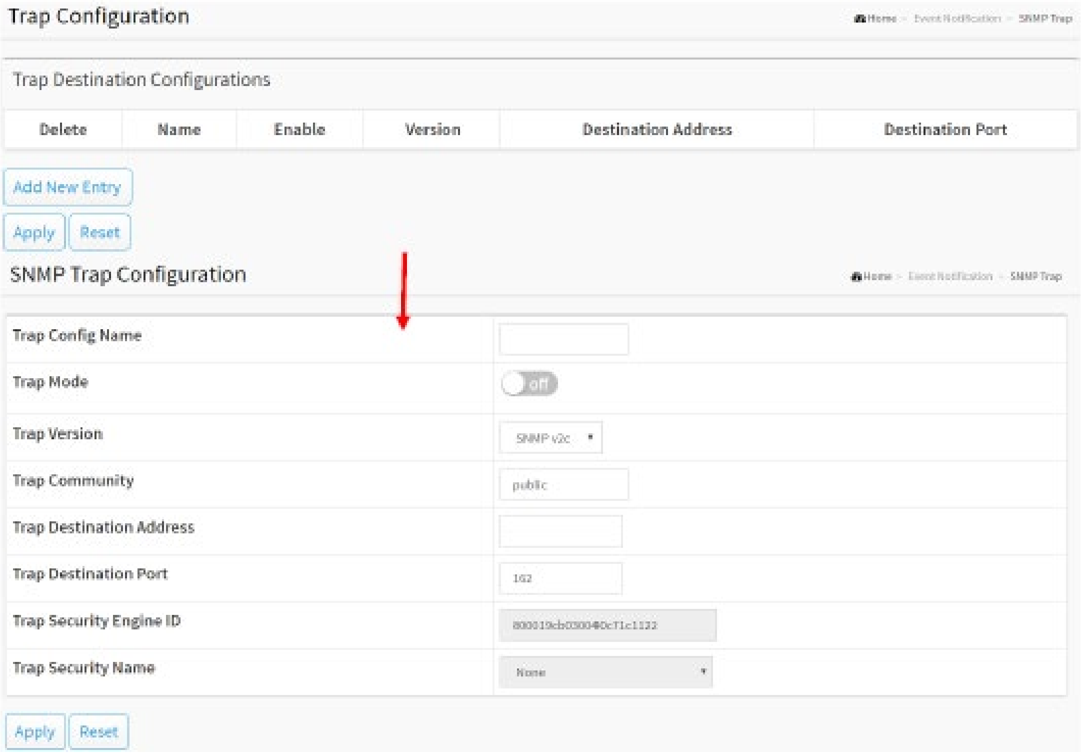
Clear: Clears the statistics.

18. Event Notification

SNMP Trap

Configure SNMP Traps on this page. To configure SNMP Trap parameters in the web UI:

1. Click Event Notification and SNMP Trap.
2. Click the Add New Entry button.
3. Specify the SNMP Trap parameters.
4. Click Apply.


Trap Configuration
Home - Event Notification - SNMP Trap
Add New Entry
Apply
Reset
SNMP Trap Configuration
Home - Event Notification - SNMP Trap
Apply
Reset

Trap Destination Configurations

Delete	Name	Enable	Version	Destination Address	Destination Port

Trap Config Name	
Trap Mode	off
Trap Version	SNMP v2c
Trap Community	public
Trap Destination Address	
Trap Destination Port	162
Trap Security Engine ID	800019cb030040c71c1122
Trap Security Name	None

Figure 17-1: SNMP Trap Configuration

Parameter descriptions:

Trap Destination Configurations

Delete : Check the box to delete the instance at the next save operation.

Name : Enter the trap Configuration's name. Indicates the trap destination's name.

Mode : Select the trap destination mode of operation. Possible modes are:

Enabled : SNMP trap mode of operation is on.

Disabled : SNMP trap mode operation is off.

Version : Select the SNMP trap supported version. Possible versions are:

SNMPv1 : Set SNMP trap supported version 1.

***SNMPv2c* :** Set SNMP trap supported version 2c.

SNMPv3 *:* Set SNMP trap supported version 3.

Destination Address : Indicates the SNMP trap destination address. It allows a valid IP address in dotted decimal notation ('x.y.z.w'). It also allows a valid hostname. A valid hostname is a string drawn from the alphabet (A-Za-z), digits (0-9), dot (.), dash (-). Spaces are not allowed, the first character must be an alpha character, and the first and last characters must not be a dot or a dash.

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

Destination Port : Indicates the SNMP trap destination port. SNMP Agent will send SNMP message via this port, the port range is 1~65535.

SNMP Trap Configuration

Trap Config Name : Indicates which trap Configuration's name for configuring. The allowed string length is 1 to 32 characters, and the allowed content is ASCII characters 33 - 126.

Trap Mode : Indicates the SNMP mode operation. Possible modes are:

on: Enable SNMP mode operation.

off: Disable SNMP mode operation.

Trap Version : Indicates the SNMP supported version. Possible versions are:

SNMPv1 : Set SNMP trap supported version 1.

***SNMPv2c* :** Set SNMP trap supported version 2c.

SNMPv3 *:* Set SNMP trap supported version 3.

Trap Community : Indicates the community access string when sending SNMP trap packet. The allowed string length is 0 to 63 characters, and the allowed content is ASCII characters 33 - 126.

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

It also allows a valid hostname. A valid hostname is a string drawn from the alphabet (A-Za-z), digits (0-9), dot (.), dash (-). Spaces are not allowed, the first character must be an alpha character, and the first and last characters must not be a dot or a dash.

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

Trap Destination Port : Indicates the SNMP trap destination port. SNMP Agent will send SNMP message via this port, the port range is 1~65535.

Trap Security Engine ID : Indicates the SNMP trap security engine ID. SNMPv3 sends traps and informs using USM for authentication and privacy. A unique engine ID for these traps and informs is needed. When "Trap Probe Security Engine ID" is enabled, the ID will be probed automatically. Otherwise, the ID specified in this field is used. The string must contain an even number(in hexadecimal format) with the number of digits between 10 and 64, but all-zeros and all 'F's are not allowed.

Trap Security Name : Indicates the SNMP trap security name. SNMPv3 traps and informs using USM for authentication and privacy. A unique security name is needed when traps and informs are enabled.

Buttons

Add New Entry : Click to add a new entry.

Apply : Click to save changes.

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

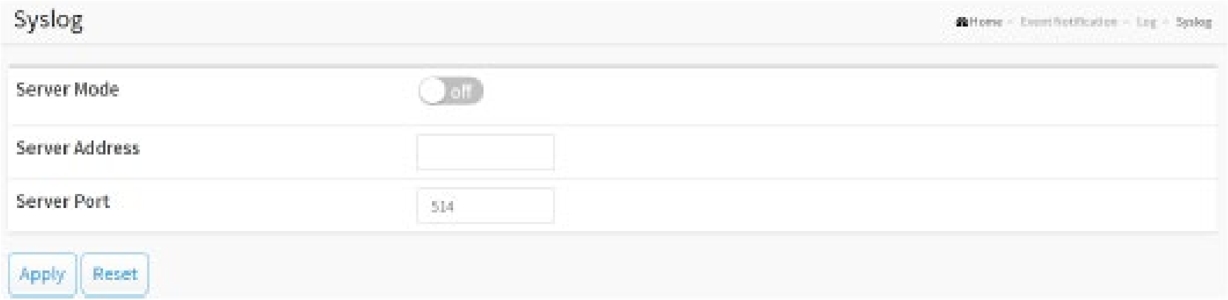
Log

Syslog

Syslog 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 also be used for general informational, analysis and debugging messages. It is supported by a wide variety of devices and receivers across multiple platforms.

To configure Syslog in the web UI:

1. Click Event Notification, Log, and Syslog.
2. Enable the Server Mode.
3. Specify the Server Address and Server Port parameters.
4. Click Apply.



Syslog

Home > Event Notification > Log > Syslog

Server Mode	off
Server Address	
Server Port	514

Figure 17-2.1: System Log Configuration

Parameter descriptions:

Server Mode : Set the Syslog server mode of operation. When the mode is enabled (on), a syslog message is sent to the Syslog server. The Syslog protocol is based on UDP communication and received on UDP port 514. The Syslog server will not send acknowledgments back to the sender since UDP is a connectionless protocol and it does not provide acknowledgments. The Syslog packet is always sent even if the Syslog server does not exist. Possible modes are:

> ***on*** : Enable server mode operation (enabled).
>
> ***off***: Disable server mode operation (disabled). The default is off.

Server Address : Enter the IPv4 host address of the Syslog server. If the switch has the DNS feature enabled and configured, it also can be a domain name.

Server Port : Indicates the service port of the Syslog server. The default is port 514.

Buttons

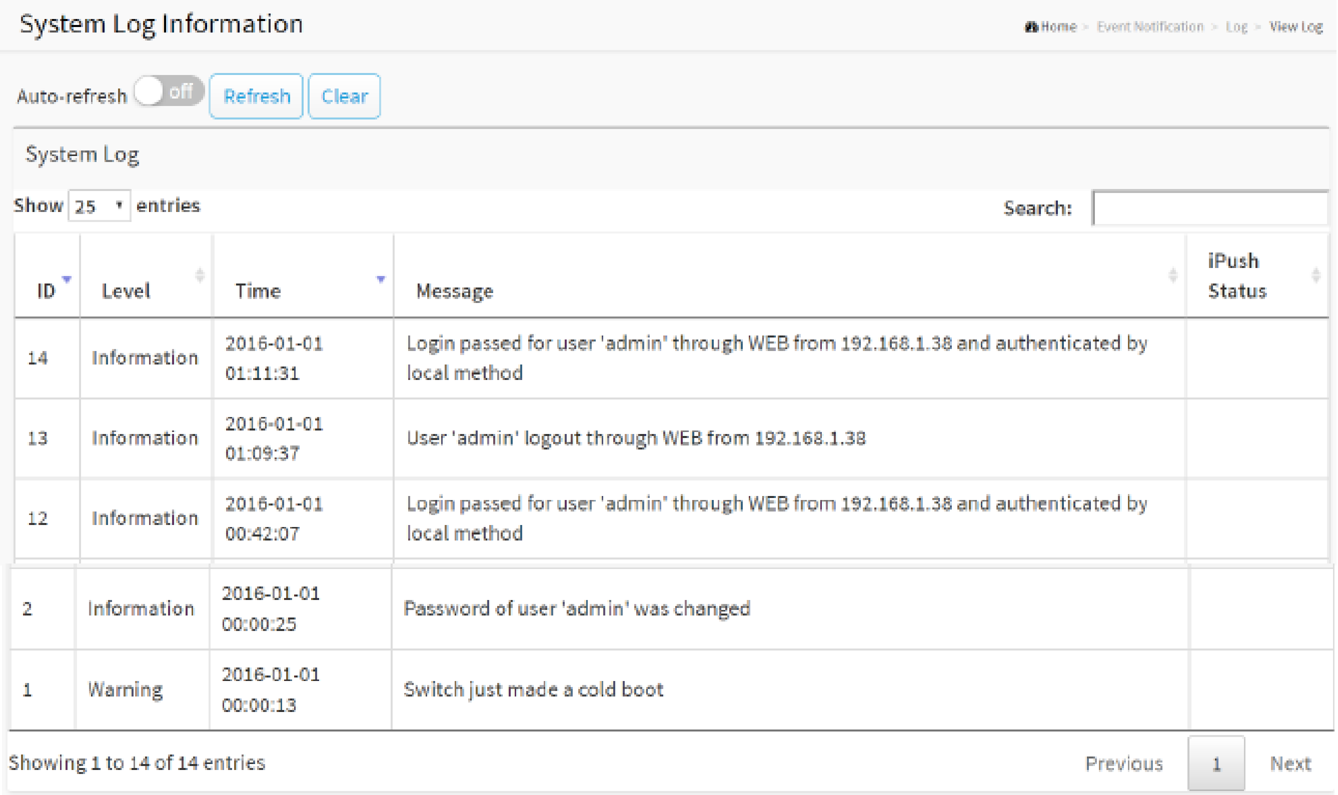
Apply : Click to save changes.

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

View Log

This page displays system log information of the switch. To display system log Information in the web UI:

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



ID	Level	Time	Message	iPush Status
14	Information	2016-01-01 01:11:31	Login passed for user 'admin' through WEB from 192.168.1.38 and authenticated by local method	
13	Information	2016-01-01 01:09:37	User 'admin' logout through WEB from 192.168.1.38	
12	Information	2016-01-01 00:42:07	Login passed for user 'admin' through WEB from 192.168.1.38 and authenticated by local method	
2	Information	2016-01-01 00:00:25	Password of user 'admin' was changed	
1	Warning	2016-01-01 00:00:13	Switch just made a cold boot	

Showing 1 to 14 of 14 entries

Figure 17-3.2: System Log Information

Parameter descriptions:

ID : ID (>= 1) of the system log entry.

Level : The 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 : Displays the log record by device time. The date and time of the system log entry.

Message : Displays the log detail message (e.g., *Switch just made a cold boot*).

iPush Status : Displays the iPush status.

Search : You can search for the information that you want to be displayed.

Show entries : Select the number of items you want to be displayed per page.

Buttons

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

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

Clear : Clear all the system log entries.

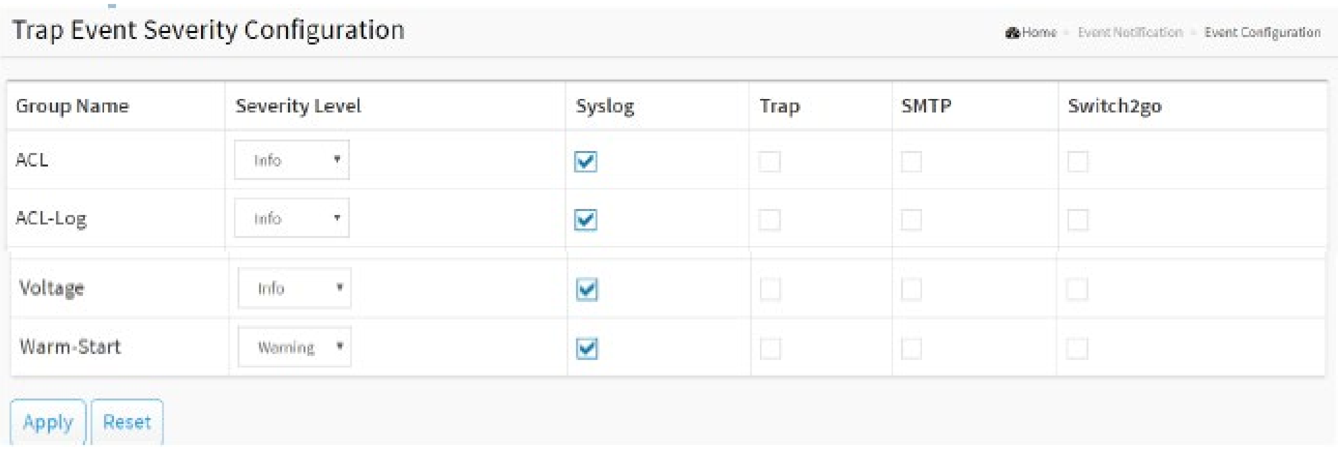
Previous : Updates the system log entries, turn to the previous page.

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

Event Configuration

This page lets you view and set current trap event severity level parameters. To configure Trap Event Severity in the web UI:

1. Click Event Notification and Event Configuration.
2. Select the Group Same and Severity Level.
3. Check one or more checkboxes to enable different trap events.
4. Click Apply to save the settings.



Trap Event Severity Configuration

Group Name	Severity Level	Syslog	Trap	SMTP	Switch2go
ACL	Info	☑	□	□	□
ACL-Log	Info	☑	□	□	□
Voltage	Info	☑	□	□	□
Warm-Start	Warning	☑	□	□	□

Figure 17-3: Event Severity Configuration

Group Name : The name identifying the severity group.

Severity Level : Each group has a severity level. These eight severity levels are supported:

*Emerg*ency : System is unusable.

Alert : Action must be taken immediately.

*Crit*ical : Critical conditions.

Error : Error conditions.

*War*ning : Warning conditions.

Notice : Normal but significant conditions.

*Info*rmation : Information messages.

Debug : Debug-level messages.

Syslog : Check the box to select this Group Name in Syslog.

Trap : Check the box to select this Group Name in Trap.

SMTP : Check the box to enable this Group Name in SMTP.

Switch2go : Check the box to enable Push Notifications for this Group Name.

Buttons

Apply : Click to save changes.

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

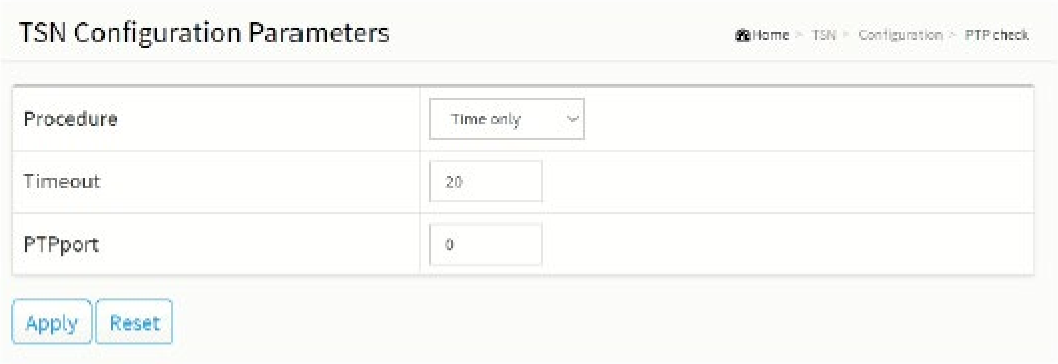
19. TSN

The TSN (Time-Sensitive Networking) Task Group (TG) is a part of the IEEE 802.1 Working Group (WG). The charter of the TSN TG is to provide deterministic services through IEEE 802 networks (i.e., guaranteed packet transport with bounded latency, low packet delay variation, and low packet loss).See Time-Sensitive Networking (TSN) Task Group | (ieee802.org).

Configuration

PTP Check

When using TAS and PSFP between network elements, there must exist a common global time reference provided by PTP. When booting the device, it will take some time for a configured PTP application to get locked to the common time reference. It may cause malfunctioning of TAS and PSFP if *config-change* is issued before PTP time is in a Locked or Locking state. A function which can delay the issue of *config-change* until PTP is Locked/Locking or a configurable time has passed, can be configured here.



TSN Configuration Parameters

Procedure	Time only
Timeout	20
PTPport	0

Figure 1-1.1: TSN Configuration Parameters

Parameter descriptions:

Procedure : At the dropdown select how to ensure the PTP state:

Time only : Use just the time parameter to ensure the PTP state.

Xxxxxx : additional parameter(s) to be supplied.

Timeout : Specify the maximal number of seconds to wait before a config_change is issued. The valid range is x to y seconds. The default is 20 seconds.

PTPport : Specify the PTP port to use for sensing PTP status. The valid range is x to y . The default is PTP Port 0.

Buttons

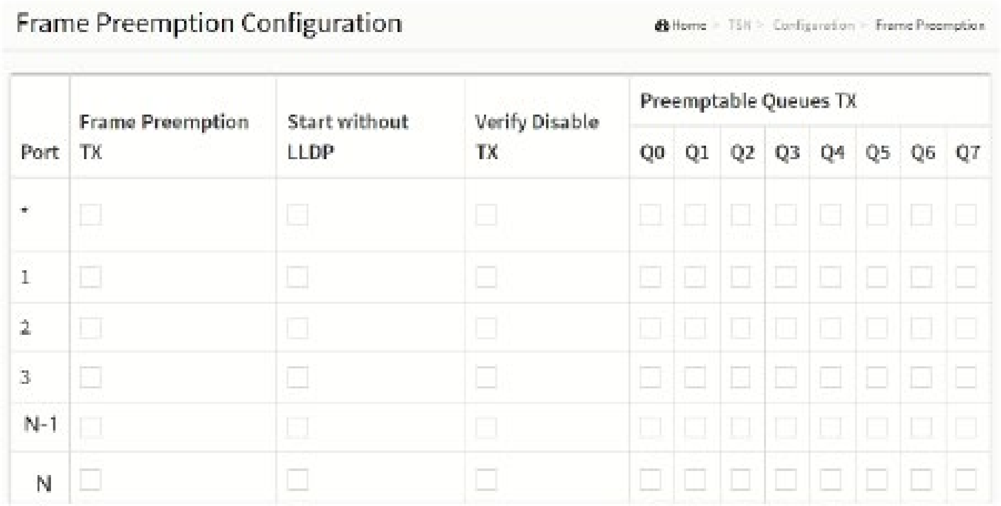
Apply : Click to save changes.

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

Frame Preemption Configuration

This page provides an overview of TSN Egress Port Frame Preemption configuration.

Frame preemption defines two MAC services for an egress port: preemptable MAC (pMAC) and express MAC (eMAC). Express frames can interrupt transmission of preemptable frames. On resume, the MAC merge sublayer re-assembles frame fragments in the next bridge.



Frame Preemption Configuration

Port	Frame Preemption TX	Start without LLDP	Verify Disable TX	Preemptable Queues TX							
				Q0	Q1	Q2	Q3	Q4	Q5	Q6	Q7
*	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐
1	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐
2	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐
3	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐
N-1	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐
N	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐

Figure 18-1.2: Frame Preemption Configuration

Parameter descriptions:

Port : The logical port for the settings contained in the same row. **Note** that Frame Preemption is not supported on ports with maximum speed 25 Gigabit/second and is also not supported on 10G Gigabit/sec Aquantia Copper ports.

Frame Preemption TX : The value of the 802.3br *aMACMergeEnableTx* parameter for the port. This value determines whether frame preemption is enabled (checked) or disabled (unchecked) in the MAC Merge sublayer in the transmit direction. The default is checkbox unchecked.

Start without LLDP : When this field is checked, Frame Preemption will be active when Frame Preemption TX is checked. The default is FALSE (checkbox unchecked).

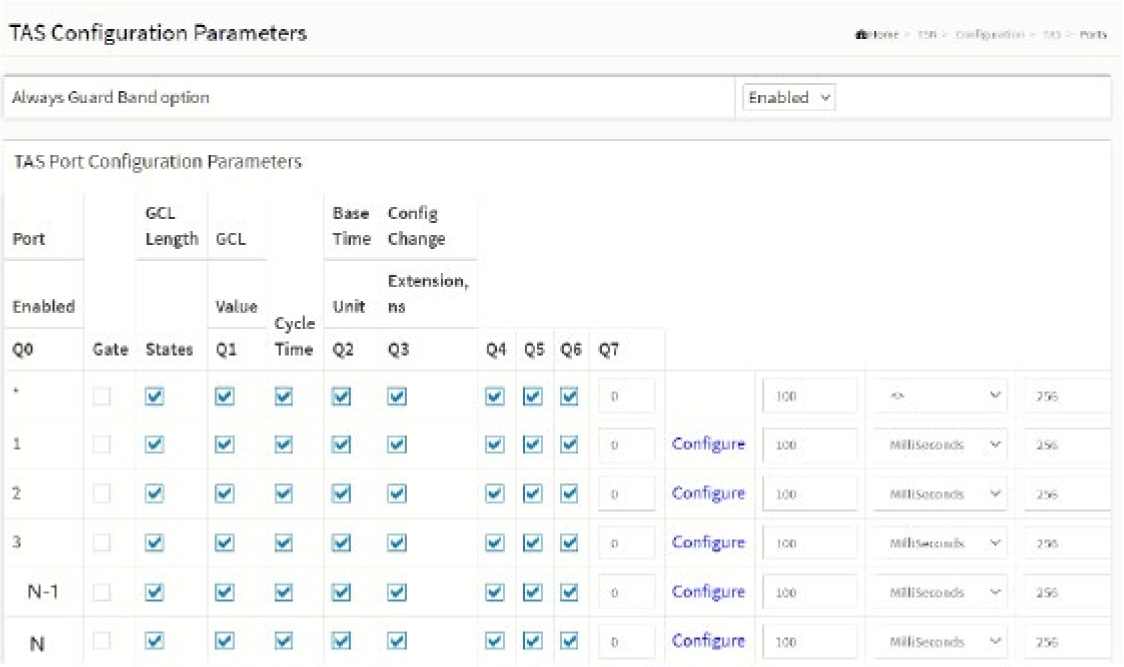
Verify Disable TX : The value of the 802.3br *aMACMergeVerifyDisableTx* parameter for the port. This value determines whether the verify function is enabled (checked) or disabled (unchecked) in the MAC Merge sublayer in the transmit direction. The default is FALSE (checkbox unchecked).

Preemptable Queues TX : This parameter is the administrative value of the preemption status for the priority. If checked, it takes value preemptable if frames queued for the priority are to be transmitted using the preemptable service for the Port. If not checked, it takes value express if frames queued for the priority are to be transmitted using the express service for the Port and preemption is enabled for the Port.

TAS Configuration Parameters

Ports

A time-triggered scheduling mechanism called a Time-Aware Shaper (TAS) is an IEEE802.1 Standard. TAS uses a parameter called a Gate Control List (GCL) to control for each class of stream or traffic. QoS will be degraded if TAS does not use an appropriate value of the GCL. See https://ieeexplore.ieee.org/document/9292023



TAS Configuration Parameters

Home > TSN > Configuration > TAS > Ports

Always Guard Band option: Enabled

TAS Port Configuration Parameters

Port		GCL Length	GCL		Base Time	Config Change								
Enabled			Value		Unit	Extension, ns								
Q0	Gate	States	Q1	Cycle Time	Q2	Q3	Q4	Q5	Q6	Q7				
*	□	☑	☑	☑	☑	☑	☑	☑	☑	0		100	<>	256
1	□	☑	☑	☑	☑	☑	☑	☑	☑	0	Configure	100	MilliSeconds	256
2	□	☑	☑	☑	☑	☑	☑	☑	☑	0	Configure	100	MilliSeconds	256
3	□	☑	☑	☑	☑	☑	☑	☑	☑	0	Configure	100	MilliSeconds	256
N-1	□	☑	☑	☑	☑	☑	☑	☑	☑	0	Configure	100	MilliSeconds	256
N	□	☑	☑	☑	☑	☑	☑	☑	☑	0	Configure	100	MilliSeconds	256

Figure 18-1.3.1: TAS Configuration Parameters

Parameter descriptions:

Always Guard Band option : This option defines how the guard band values are calculated:

> If a Gate Control List does not contain *SetAndHold* and/or *SetAndRelease* operations the Always Guard Band option has no effect.
>
> If a Gate Control List does contain *SetAndHold* and *SetAndRelease* operations, then:
>
> > When Always Guard Band is Enabled, a guard band is implemented on all queues, both Express and Preemptible queues. The default is Enabled.
> >
> > When Always Guard Band is Disabled, a guard band is only implemented on Preemptible queues.

TAS Port Configuration Parameters

Port : Port number of the switch.

Gate Enabled : The Enabled parameter determines whether traffic scheduling is active (true) or inactive (false).

Gate **States** : The initial value of the port open states that is used when no Gate Control List is active on the Port.

GCL Length : The Admin Gate Control List length parameter for the Port. Valid range is 0-256. The integer value indicates the number of entries Gate Control Elements in the Gate Control List. If you change the value, press the Save button before configuring the Gate Control List by pressing the GCL link.

GCL : A link to the Gate Control List parameter configuration.

Cycle Time : The Admin value of the gating cycle for the Port. The Admin Cycle Time variable is a rational number of seconds, defined by value and a unit.

Cycle Time Value : The Admin Cycle Time is defined by this number of units defined in the Unit field. The Admin Cycle Time is a value in the range 1-999999999 and combined with the Cycle Time Unit the value will be in the range 256-999999999 nanoseconds. The default value is 100 milliseconds.

Cycle Time Unit : The Admin Cycle Time unit. May be milliseconds, microseconds or nanoseconds.

Cycle Time Extension : An integer number of nanoseconds in the range 256-999999999, defining the maximum amount of time by which the gating cycle for the Port is permitted to be extended when a new cycle configuration is installed. The default value is 256 nanoseconds.

Base Time : The Admin value of base time, expressed as an IEEE 1588 Precision Time Protocol (PTP) timescale.

Config Change : The Configuration Change parameter signals the start of a configuration change. After a successful configuration change, the configured Admin values will become the Oper values, which are displayed on the Monitor > TSN > TAS webpage

If the value of Base Time is in the future, the configuration change will be executed at Base Time.

If Base Time is in the past, the configuration change will be executed as soon as possible. In practice it will be within approximately 2 seconds, at a time which is an integral number of Cycle Time ahead of the configured value of Base Time. This way, synchronization between schedules in elements across a scheduled network can be maintained.

Buttons

Apply : Click to save changes.

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

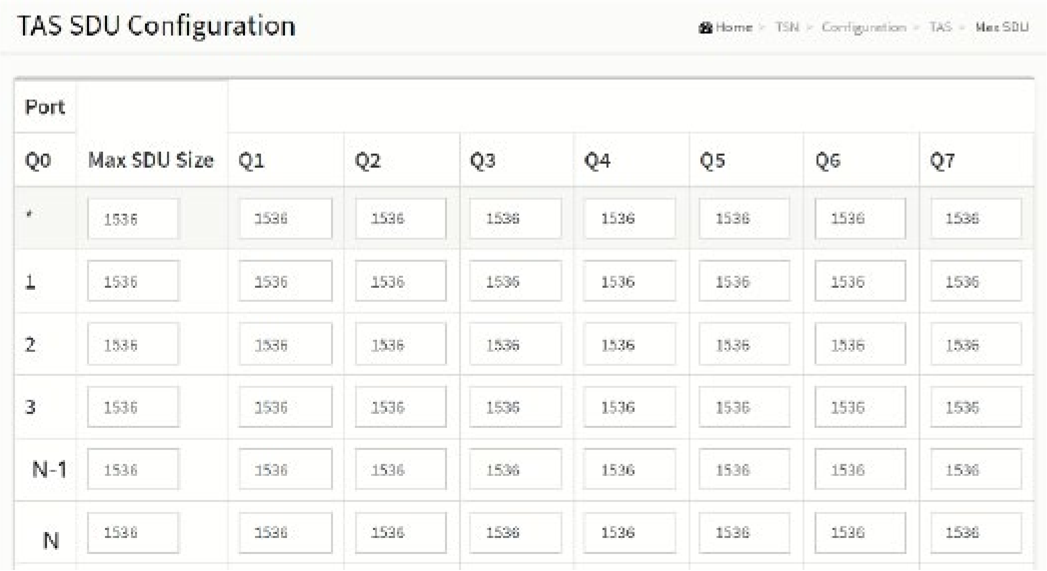
You can click the linked text Configure to display ...

To be supplied.

TAS SDU Configuration

This page lets you view and set current TAS SDU parameters. An SDU (Service Data Unit) is a unit of data that has been passed down from an OSI layer to a lower layer.

A time-triggered scheduling mechanism called Time-Aware Shaper (TAS) is one of IEEE802.1 Standards and has a parameter called Gate Control List (GCL), to control for each class of stream or traffic.



TAS SDU Configuration

Port								
Q0	Max SDU Size	Q1	Q2	Q3	Q4	Q5	Q6	Q7
*	1536	1536	1536	1536	1536	1536	1536	1536
1	1536	1536	1536	1536	1536	1536	1536	1536
2	1536	1536	1536	1536	1536	1536	1536	1536
3	1536	1536	1536	1536	1536	1536	1536	1536
N-1	1536	1536	1536	1536	1536	1536	1536	1536
N	1536	1536	1536	1536	1536	1536	1536	1536

Figure 18-1.3.2: TAS SDU Configuration

Parameter descriptions:

Port : Port number of the switch.

Max SDU Size : The value of the Maximum SDU size parameter for the traffic class supported by the port. This value is represented as an unsigned integer in the range 0-10240. A value of 0 is interpreted as the Maximum SDU size supported by the underlying MAC: 10240. The default value of the Maximum SDU parameter is 1536.

The Max SDU Size parameter is used to calculate the guard band time = Maximum SDU * 8 / LINK_SPEED (sec).

If frame preemption is enabled and a gate operation is *SetAndHold*, the guard band time in preemptable queues is automatically selected as the frame preemption minimum fragment size plus 64 bytes.

A queue is said to be preemptible if frame preemption is enabled and if this queue is not opened in a *SetAndHold* gate operation.

Buttons

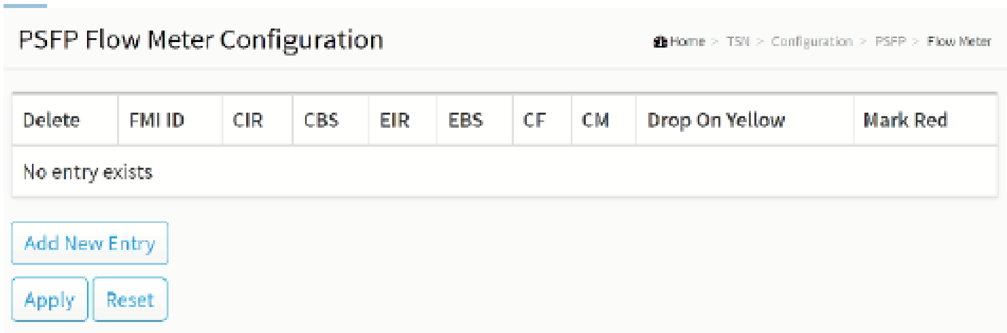
Apply : Click to save changes.

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

PSFP

This page lets you view and set current PSFP flow meter parameters.

Per-Stream Filtering and Policing (PSFP) improves network robustness by filtering individual traffic streams. PSFP prevents traffic overload conditions that may affect bridges and the receiving endpoints due to malfunction or Denial of Service (DoS) attacks. The stream filter uses rule matching to allow frames with specified stream IDs and priority levels and apply policy actions otherwise. All streams are coordinated at their gates, similar to 802.1Qch signaling. Flow metering applies predefined bandwidth profiles for each stream. See IEEE 802.1Qci or the MEF Reference Wiki.



PSFP Flow Meter Configuration

Home > TSN > Configuration > PSFP > Flow Meter

Delete	FMI ID	CIR	CBS	EIR	EBS	CF	CM	Drop On Yellow	Mark Red
No entry exists									

Figure 18-1.4: PSFP Flow Meter Configuration

Parameter descriptions:

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

FMI ID : The *FlowMeterInstance* parameter is an index into the PSPF Flow Meter Configuration table.

CIR : The *FlowMeterCIR* parameter contains an integer value that represents the CIR value for the flow meter, in bits/second. Committed Ingress Rate (CIR) sets the average maximum bandwidth allowed to be sent on the egress interface, measured in bits per second.

CBS : The *FlowMeterCBS* parameter contains an integer value that represents the CBS value for the flow meter, in octets. Committed Burst Shape (CBS) is the burst of data allowed to be sent even though it is above the CIR. This is defined in number of bytes of data.

EIR : Excess Information Rate is the average rate (in bytes per unit of time), in excess of the CIR, up to which the network may transfer frames without any performance objectives.

EBS : (Excess Burst Size) defines a limit on the maximum number of information units (e.g., bytes) available for a burst of frames sent at the interface speed to remain EIR-conformant.

CF : Coupling flag (CF) allows the choice between two modes of operation of the rate enforcement algorithm.

CM : Color mode (CM) indicates whether the "color-aware" or "color-blind" property is employed by the bandwidth profile.

> ***Color Aware***: Algorithm considers the color indication of incoming frames. Incoming frames without a color indication get a default color prior to entering the meter. Frames are never “promoted”; an incoming yellow frame is never changed to green.
>
> ***Color Blind***: Algorithm ignores the color indication (if any) of incoming frames. Effectively all incoming frames are assumed to start out green.

Drop On Yellow : Drop on Yellow (Excess) frames .

Mark RED Enable : The *FlowMeterMarkAllFramesRedEnable* parameter contains a Boolean value that indicates whether the *MarkAllFramesRed* function is enabled (TRUE) or disabled (FALSE).

Mark RED : The *FlowMeterMarkAllFramesRed* parameter contains a Boolean value that indicates whether, if the *MarkAllFramesRed* function is enabled, all frames are to be discarded (TRUE) or not (FALSE).

MEF interpretation of color: MEF Bandwidth Profiles use three color indications:

Green : "Committed" frames. Service Level Objectives such as frame loss rate, delay, delay variation, etc. are applicable to these frames. In theory, with proper policing at the edge of the network and proper allocation of buffer and bandwidth resources within the network, it is possible to guarantee lossless and timely delivery of all committed frames.

Yellow : "Excess" frames. Service Level Objectives are not applicable to these frames. Excess frames are delivered on a "best effort" basis.

Red : "Non-conformant" frames that are always discarded.

See https://www.ieee802.org/1/files/public/docs2013/new-tsn-haddock-flow-metering-in-Q-0113-v01.pdf

Buttons

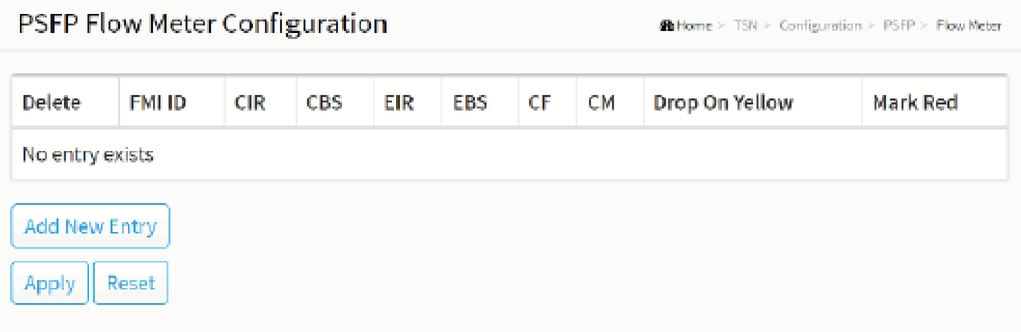
Add New Entry : Click to add a new row to the table.

Apply : Click to save changes.

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

Flow Meter

This page lets you view and set current PSFP (Per-Stream Filtering and Policing) parameters.



PSFP Flow Meter Configuration

Delete	FMI ID	CIR	CBS	EIR	EBS	CF	CM	Drop On Yellow	Mark Red
No entry exists									

Figure 18-1.4.1: PSFP Flow Meter Configuration

Parameter descriptions:

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

FMI ID : The *FlowMeterInstance* parameter is an index into the FlowMeterTable.

CIR : The *FlowMeterCIR* parameter contains an integer value that represents the CIR value for the flow meter, in bit/s.

CBS : The *FlowMeterCBS* parameter contains an integer value that represents the CBS value for the flow meter, in octets.

EIR : Excess Information Rate is the average rate (in bytes per unit of time), in excess of the CIR, up to which the network may transfer frames without any performance objectives.

EBS : (Excess Burst Size) defines a limit on the maximum number of information units (e.g., bytes) available for a burst of frames sent at the interface speed to remain EIR-conformant.

CF : Coupling flag (CF) allows the choice between two modes of operation of the rate enforcement algorithm.

CM : Color mode (CM) indicates whether the "color-aware" or "color-blind" property is employed by the bandwidth profile.

> ***Color Aware***: Algorithm considers the color indication of incoming frames. Incoming frames without a color indication get a default color prior to entering the meter. Frames are never “promoted”; an incoming yellow frame is never changed to green.
>
> ***Color Blind***: Algorithm ignores the color indication (if any) of incoming frames. Effectively all incoming frames are assumed to start out green.

Drop On Yellow : Flow-meter-instance boolean drop-on-yellow = // r-w.

Mark RED Enable : The *FlowMeterMarkAllFramesRedEnable* parameter contains a Boolean value that indicates whether the MarkAllFramesRed function is enabled (TRUE) or disabled (FALSE).

Mark Red : The *FlowMeterMarkAllFramesRed* parameter contains a Boolean value that indicates whether, if the *MarkAllFramesRed* function is enabled, all frames are to be discarded (TRUE) or not (FALSE).

Buttons

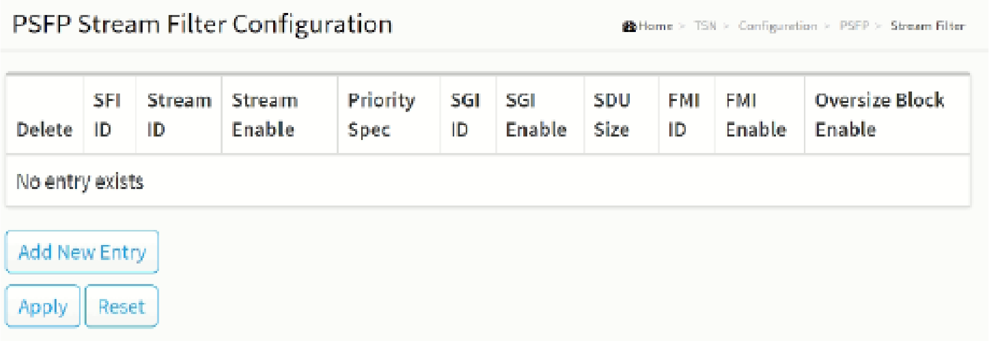
Add New Entry : Click to add a new Flow Meter entry.

Apply : Click to save changes.

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

Stream Filter

This page lets you view and set current PSFP (Per-Stream Filtering and Policing) parameters.



PSFP Stream Filter Configuration

Delete	SFI ID	Stream ID	Stream Enable	Priority Spec	SGI ID	SGI Enable	SDU Size	FMI ID	FMI Enable	Oversize Block Enable
No entry exists										

Figure 18-1.4.2: PSFP Stream Filter Configuration

Parameter descriptions:

SFI ID : The Stream Filter Instance parameter is an index into the *StreamFilterTable*.

Stream ID : The Stream Handle Spec parameter contains a stream identifier specification value. A value of -1 denotes the wild card value; all positive values denote stream identifier values.

Stream Enable : Shows current stream status (Enable or Disable).

Priority Spec : The Priority Spec parameter contains a priority specification value. A value of -1 denotes the wild card value; zero or positive values denote priority values.

Interface Spec : The *InterfaceSpec* parameter contains an interface specification value. A value of VTSS_IFINDEX_NONE denotes the wild card value.

SGI ID : The Stream Gate Instance parameter contains the index of an entry in the Stream Gate Table.

SGI Enable : Shows current stream gate instance status (Enable or Disable).

SDU Size : The *MaximumSDUSize* parameter specifies the maximum allowed frame size for the stream. Any frame exceeding this value will be dropped. A value of 0 denote that the *MaximumSDUSize* filter is disabled for this stream.

FMI ID : The *FlowMeterInstanceID* parameter contains the index of an entry in the Flow Meter Table. A value of -1 denotes that no flow meter is assigned; zero or positive values denote flow meter IDs.

FMI Enable: Shows current Flow Meter Instance status (Enable or Disable).

Oversize Block Enable : The *StreamBlockedDueToOversizeFrameEnable* object contains a Boolean value that indicates whether the *StreamBlockedDueToOversizeFrame* function is enabled (TRUE) or disabled (FALSE).

Block Oversize : The *StreamBlockedDueToOversizeFrame* object contains a Boolean value that indicates whether, if the *StreamBlockedDueToOversizeFrame* function is enabled, all frames are to be discarded (TRUE) or not discarded (FALSE).

Buttons

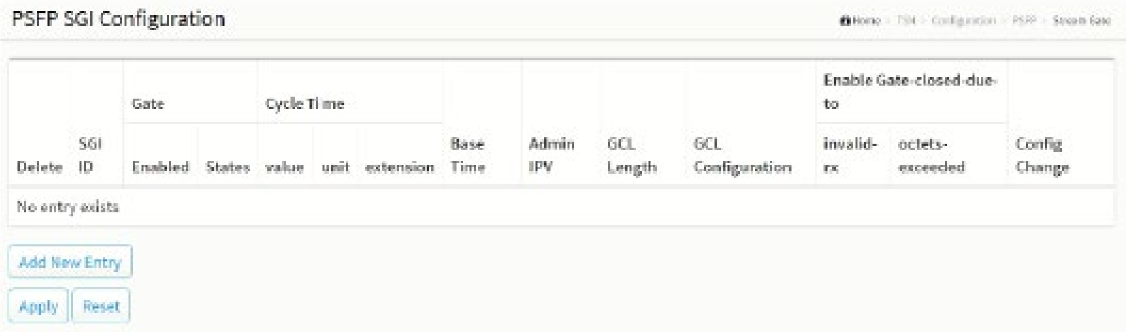
Add New Entry : Click to add Flow Meter entry.

Apply : Click to save changes.

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

Stream Gate

This page lets you view and set current PSFP (Per-Stream Filtering and Policing) SGI (Stream Gate Instance) parameters.



PSFP SGI Configuration

Home > TSN > Configuration > PSFP > Stream Gate

		Gate		Cycle Time							Enable Gate-closed-due-to		
Delete	SGI ID	Enabled	States	value	unit	extension	Base Time	Admin IPV	GCL Length	GCL Configuration	invalid-rx	octets-exceeded	Config Change
No entry exists													

Figure 18-1.4.3: PSFP SGI Configuration

Parameter descriptions:

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

SGI ID : The Stream Gate Instance parameter is an index into the Stream Gate Table.

Gate Enabled : The Gate Enabled parameter determines whether the stream gate is active (true) or inactive (false).

Gate States : The administrative value of the *GateStates* parameter for the stream gate. The *Open* value indicates that the gate is open, the *Closed* value indicates that the gate is closed.

Cycle Time value : The administrative value of the cycle time for the gate. The time may be specified in either milliseconds, microseconds, or nano seconds as defined by the field Cycle Time unit.

Cycle Time unit : The unit used for specifying the administrative cycle time. possible values are ns, us or ms.

Cycle Time extension : The administrative value of the *CycleTimeExtension* parameter for the gate. The value is an unsigned integer number of nanoseconds.

Base Time : The administrative value of the *BaseTime* parameter for the gate. The value is a representation of a *PTPtime* value, consisting of decimal number of seconds since epoch. The time can be given with a resolution of nine decimals.

Admin IPV : The administrative value of the IPV parameter for the gate. A value of -1 denotes the null value. The IPV (Internal Priority Value) is an 'inside the box' value; it is a recent addition to 802.1Q that supports more than eight Traffic Class queues.

GCL Length : The number of entries in the Gate Control List.

GCL Configuration : Configuration of the Gate Control List.

Enable Gate-closed-due-to invalid-rx : A Boolean value that indicates whether to close the gate if invalid data is received.

Enable Gate-closed-due-to octets-exceeded : A Boolean value that indicates whether to close the gate if too many octets are received

Config Change : The *ConfigChange* parameter signals the start of a configuration change for the gate when it is set to TRUE. This should only be done when the various administrative parameters are all set to appropriate values.

Buttons

Add New Entry: Click to add a new PSPF SGI entry.

Apply : Click to save changes.

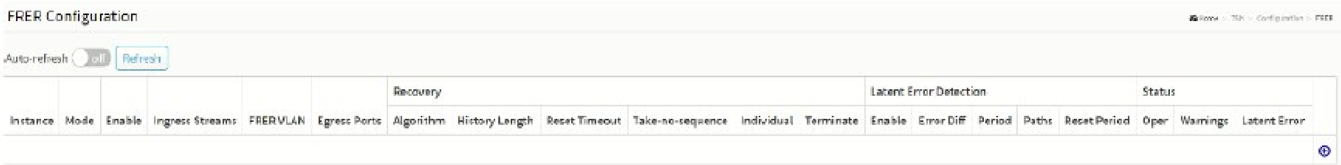
Reset : Click to undo any changes made locally and revert to previously saved values.

FRER

This page lets you view current Frame Replication and Elimination for Reliability (FRER) parameters.

IEEE 802.1Qca integrates control protocols to manage multiple topologies, configure an explicit forwarding path (a predefined path for each stream), reserve bandwidth, provide data protection and redundancy, and distribute flow synchronization and flow control messages.

Click the Add button (FRER) (⊕) to add a new FRER to the table.



FRER Configuration

Home > TSN > Configuration > FRER

Auto-refresh off Refresh

						Recovery						Latent Error Detection					Status		
Instance	Mode	Enable	Ingress Streams	FRER VLAN	Egress Ports	Algorithm	History Length	Reset Timeout	Take-no-sequence	Individual	Terminate	Enable	Error Diff	Period	Paths	Reset Period	Oper	Warnings	Latent Error

⊕

Figure 18-1.5: FRER Configuration

Parameter descriptions:

Instance : The FRER instance number.

Mode : The FRER mode of operation.

Generation : This FRER instance is currently generating.

Recovery : This FRER instance is currently recovering from a failure.

Enable : FRER instance enabled or disabled.

up: Enabled.

down: Disabled

Ingress Streams : List of ingress stream IDs.

FRER VLAN : The VLAN ID that ingress flows get classified to.

Egress Ports : The port numbers that this FRER instance will hit.

Algorithm : The algorithm used by the Recovery function. ***Vector*** or ***match***.

History Length : History length of the vector algorithm.

Reset Timeout : Reset timeout of the Recovery function.

Take-no-sequence : If true, accept all frames whether or not they are R-tagged. FRER introduced the Redundancy tag (RTAG) as an example of sequence number formatting.

Individual : Use individual recovery.

Terminate : Strip R-Tag from a frame before presenting it on egress.

Enable : Enable/disable Latent Error Detection.

Error Diff : Latent error detection error difference.

Period : Latent Error Detection period.

Paths : Latent Error Detection paths.

Reset Period : Latent Error Detection reset period.

Oper : The operational state of the FRER instance.

up: Active.

down: Disabled or Internal error.

Warnings : Operational warnings of the FRER instance.

up: No warnings.

down: There are warnings, use tooltip to see which.

Latent Error :

up: No errors.

down: There are latent errors.

Buttons

Auto-refresh : Check this box to refresh the page automatically.

Refresh : Click to refresh the page immediately.

Configuration Buttons : You can modify each FRER instance in the table using these buttons:

Θ **Edit**: Edits the FRER row.

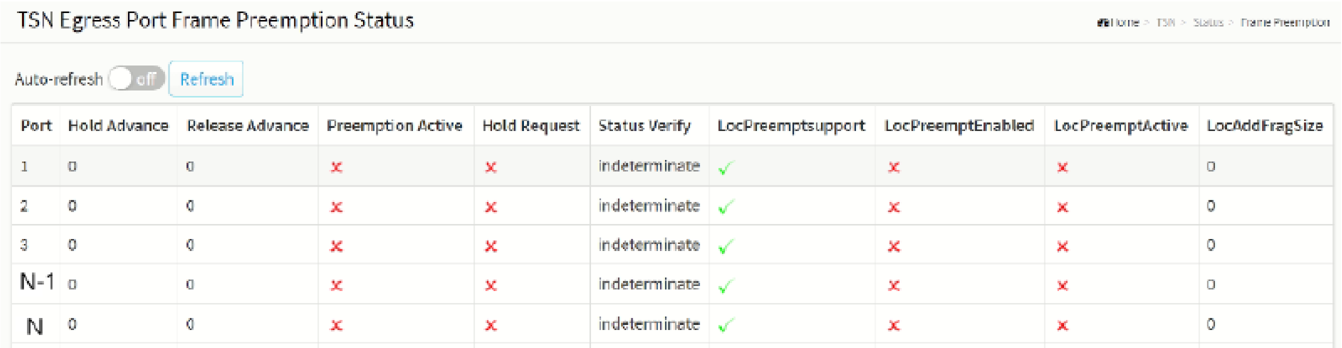
Θ **Delete**: Deletes the FRER from the table.

⊕ **Add**: Adds a new FRER to the table.

Status

Frame Preemption

This page provides an overview of TSN Egress Port Frame Preemption Status for all switch ports.



TSN Egress Port Frame Preemption Status

Port	Hold Advance	Release Advance	Preemption Active	Hold Request	Status Verify	LocPreemptsupport	LocPreemptEnabled	LocPreemptActive	LocAddFragSize
1	0	0	✗	✗	indeterminate	✓	✗	✗	0
2	0	0	✗	✗	indeterminate	✓	✗	✗	0
3	0	0	✗	✗	indeterminate	✓	✗	✗	0
N-1	0	0	✗	✗	indeterminate	✓	✗	✗	0
N	0	0	✗	✗	indeterminate	✓	✗	✗	0

Figure 18-2.1:TSN Egress Port Frame Preemption Status

Parameter descriptions:

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

Hold Advance : The value of the *holdAdvance* parameter for the Port in nanoseconds. There is no default value; the *holdAdvance* is a property of the underlying MAC.

Release Advance : The value of the *releaseAdvance* parameter for the Port in nanoseconds. There is no default value; the *releaseAdvance* is a property of the underlying MAC.

Preemption Active : The value is active (TRUE) when preemption is operationally active for the Port, and idle (FALSE) otherwise.

Hold Request : The value is hold (TRUE) when the sequence of gate operations for the Port has executed a Set-And-Hold-MAC operation, and release (FALSE) when the sequence of gate operations has executed a Set-And-Release-MAC operation. The value of this object is release (FALSE) on system initialization.

Status Verify : The status of the MAC Merge sublayer verification for the given device.

LocPreemptsupport : The value is TRUE when preemption is supported on the port, and FALSE otherwise.

LocPreemptEnabled : The value is TRUE when preemption is enabled on the port, and FALSE otherwise.

LocPreemptActive : The value is TRUE when preemption is operationally active on the port, and FALSE otherwise.

LocAddFragSize : The value of the 802.3br *LocAddFragSize* parameter for the port. The minimum size of non-final fragments supported by the receiver on the local port. This value is expressed in units of 64 octets of additional fragment length. The minimum non-final fragment size is: (LocAddFragSize + 1) * 64 octets.

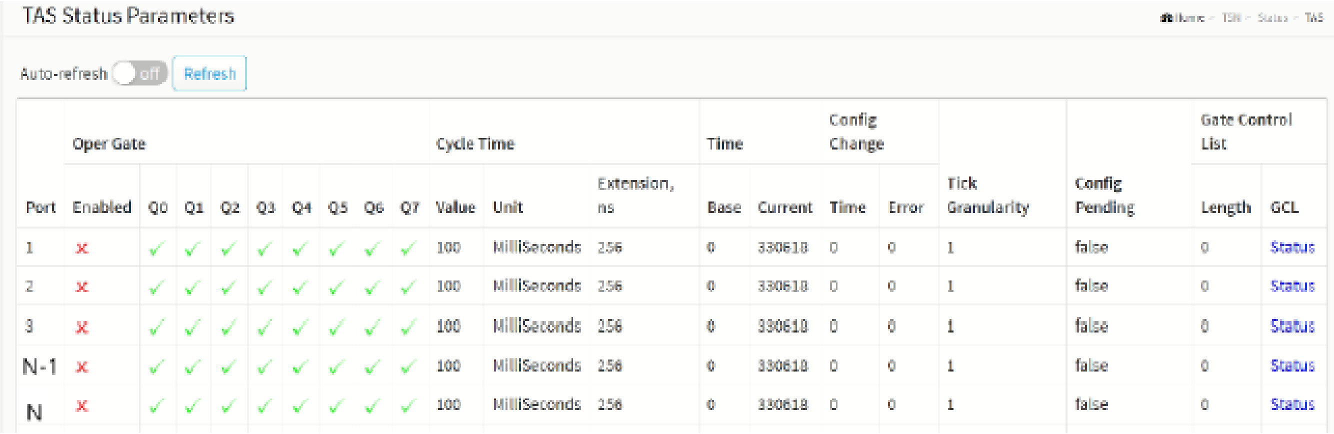
Buttons

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

Refresh : Click to manually refresh the page immediately.

TAS

This page lets you view and set current TAS (Time-Aware Shaper) parameters.



	Oper Gate									Cycle Time			Time		Config Change				Gate Control List	
Port	Enabled	Q0	Q1	Q2	Q3	Q4	Q5	Q6	Q7	Value	Unit	Extension, ns	Base	Current	Time	Error	Tick Granularity	Config Pending	Length	GCL
1	✗	✓	✓	✓	✓	✓	✓	✓	✓	100	MilliSeconds	256	0	330618	0	0	1	false	0	Status
2	✗	✓	✓	✓	✓	✓	✓	✓	✓	100	MilliSeconds	256	0	330618	0	0	1	false	0	Status
3	✗	✓	✓	✓	✓	✓	✓	✓	✓	100	MilliSeconds	256	0	330618	0	0	1	false	0	Status
N-1	✗	✓	✓	✓	✓	✓	✓	✓	✓	100	MilliSeconds	256	0	330618	0	0	1	false	0	Status
N	✗	✓	✓	✓	✓	✓	✓	✓	✓	100	MilliSeconds	256	0	330618	0	0	1	false	0	Status

Figure 18-2.2: TAS Status Parameters

Parameter descriptions:

Port : Port number of the switch.

Oper Gate Enabled : The Enabled parameter shows whether traffic scheduling is active (true) or inactive (false).

Oper Gate States : The current state of the gate associated with each Queue (Q0 – Q7) for the Port.

Cycle Time Value : The operational value of the gating cycle for the Port. The Cycle Time variable is a rational number of seconds, defined by value and a unit.

Cycle Time Unit : The operational Cycle Time unit of measure. May be Milliseconds, Microseconds or Nanoseconds.

Cycle Time Extension : An integer number of nanoseconds, defining the maximum amount of time by which the gating cycle for the Port is permitted to be extended when a new cycle configuration is installed.

Base Time : The operational value of base time, expressed as an IEEE 1588 Precision Time Protocol (PTP) timescale.

Current Time : The current time, in *PTPtime*, as maintained by the local system. The value is a representation of a *PTPtime* value, consisting of a 48-bit integer number of seconds and a 32-bit integer number of nanoseconds. Only the seconds are displayed.

Config Change Time : The *PTPtime* at which the next config change is scheduled to occur. The value is a representation of a PTPtime value, consisting of a 48-bit integer number of seconds and a 32-bit integer number of nanoseconds.

Config Change Error : A counter of the number of times that a re-configuration of the traffic schedule has been requested with the old schedule still running and the requested base time was in the past.

Tick Granularity : The granularity of the cycle time clock, represented as an unsigned number of tenths of nanoseconds.

Config Pending : The value of the *ConfigPending* state machine variable. The value is TRUE if a configuration change is in progress but has not yet completed.

GCL Length : The operational value of the Gate Control List length parameter for the Port. The integer value indicates the number of entries (TLVs) in the operational Gate Control List.

GCL : A link to the Gate Control List Status parameter (see below).

Buttons

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

Refresh : Click to manually refresh the page immediately.

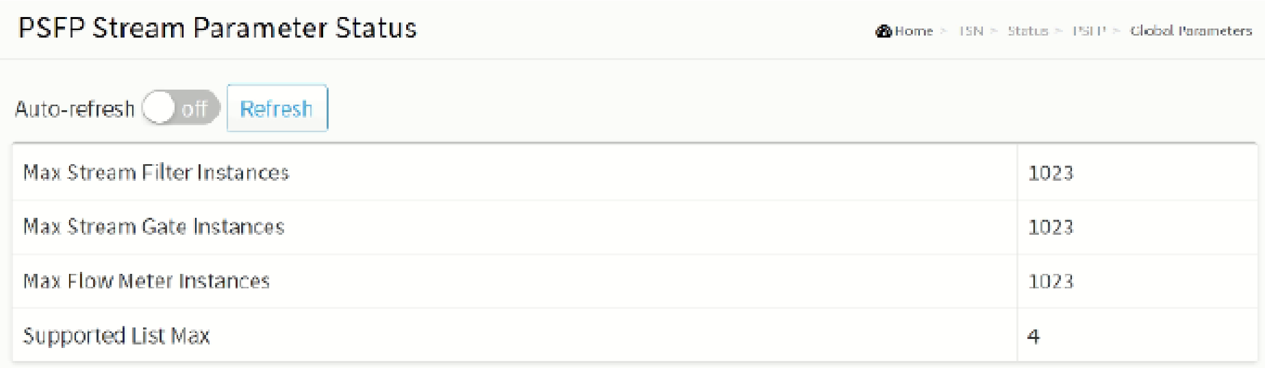
Gate Control List Status

To be supplied.

PSFP

Global Parameters

This page lets you view and set current PSFP (Per-Stream Filtering and Policing) parameters.



PSFP Stream Parameter Status

Max Stream Filter Instances	1023
Max Stream Gate Instances	1023
Max Flow Meter Instances	1023
Supported List Max	4

Figure 18-2.3.1: PSFP Stream Parameter Status

Parameter descriptions:

Max Stream Filter Instances : The *MaxStreamFilterInstances* parameter defines the maximum number of stream filter instances that are supported by this Bridge component.

Max Stream Gate Instances : The *MaxStreamGateInstances* parameter defines the maximum number of stream gate instances that are supported by this Bridge component.

Max Flow Meter Instances : The *MaxFlowMeterInstances* parameter defines the maximum number of flow meter instances that are supported by this Bridge component.

Supported List Max : The *SupportedListMax* parameter defines the maximum value supported by this Bridge component of the *AdminControlListLength* and *OperControlListLength* parameters.

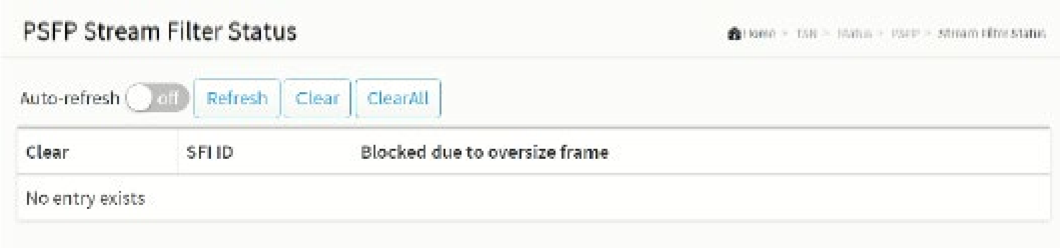
Buttons

Auto-refresh : Check to ***on*** to refresh the page automatically every 3 seconds. The default is ***off***.

Refresh : Click to manually refresh the page immediately.

Stream Filter Status

This page lets you view current PSFP status settings.



PSFP Stream Filter Status

Clear	SFI ID	Blocked due to oversize frame
No entry exists		

Figure 18-2.3.2: PSFP Stream Filter Status

Parameter descriptions:

Clear : This box is used to mark an entry for clearance in next Clear operation.

SFI ID : The id of the stream filter instance.

Blocked due to oversize frame : True if the filter has been blocked due to an oversize frame, otherwise false.

Buttons

Auto-refresh : Check this box to ***on*** to refresh the page automatically every 3 seconds.

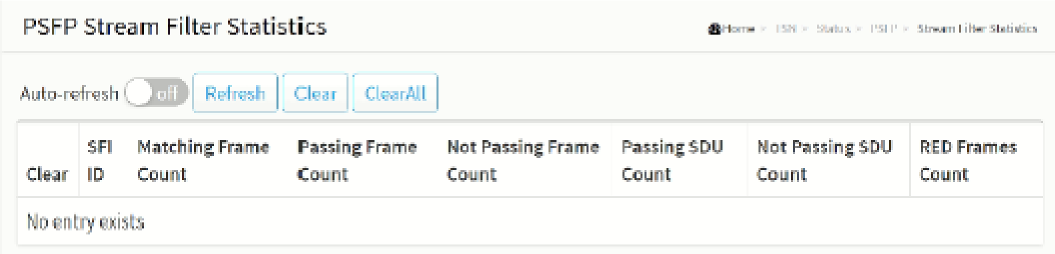
Refresh : Click to refresh the page immediately.

Clear : Clears the blocked flag for selected entries.

ClearAll : Clears the blocked flag for all entries.

Stream Filter Statistics

This page displays current PSFP statistics parameters.



PSFP Stream Filter Statistics

Clear	SFI ID	Matching Frame Count	Passing Frame Count	Not Passing Frame Count	Passing SDU Count	Not Passing SDU Count	RED Frames Count
No entry exists							

Figure 18-2.3.3: PSFP Stream Filter Statistics

Parameter descriptions:

Clear : This box is used to mark an entry for clearance in the next Clear operation.

SFI ID : The *MaxStreamFilterInstances* parameter defines the maximum number of stream filter instances that are supported by this Bridge component.

Matching Frame Count : The *MatchingFramesCount* counter counts received frames that match this stream filter.

Passing Frame Count : The *PassingFramesCount* counter counts received frames that pass the gate associated with this stream filter.

Not Passing Frame Count : The *NotPassingFramesCount* counter counts received frames that do not pass the gate associated with this stream filter.

Passing SDU Count : The *PassingSDUCount* counter counts received frames that pass the SDU size filter specification associated with this stream filter.

Not Passing SDU Count : The *NotPassingSDUCount* counter counts received frames that do not pass the SDU size filter specification associated with this stream filter.

RED Frames Count : The REDFramesCount counter counts received random early detection (RED) frames associated with this stream filter.

Buttons

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

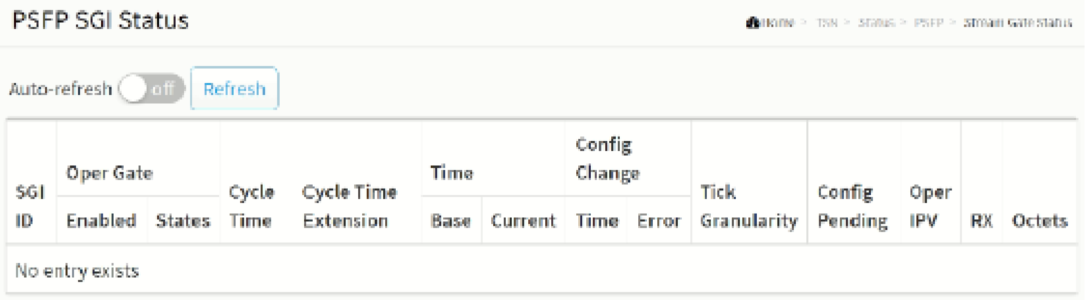
Refresh : Click to refresh the page immediately.

Clear : Clears the blocked flag for selected entries.

Clear All : Clears the blocked flag for all entries.

Stream Gate Status

This page lets you view and set current PSFP SGI (Stream Gate Instance) status.



SGI	Oper Gate		Cycle	Cycle Time	Time		Config Change		Tick	Config	Oper		
ID	Enabled	States	Time	Extension	Base	Current	Time	Error	Granularity	Pending	IPV	RX	Octets
No entry exists													

Figure 18-2.3.4: PSFP SGI Status

Parameter descriptions:

SGI ID : The Stream Gate Instance parameter is an index in the Stream Gate table.

Oper Gate Enabled : The Gate Enabled parameter determines whether the stream gate is active (true) or inactive (false).

Oper Gate States : The operational value of the *GateStates* parameter for the stream gate. The open value indicates that the gate is open, the closed value indicates that the gate is closed.

Cycle Time Numerator : The operational value of the numerator of the *CycleTime* parameter for the gate. The numerator and denominator together represent the cycle time as a rational number of seconds.

Cycle Time Denominator : The operational value of the denominator of the *CycleTime* parameter for the gate. The numerator and denominator together represent the cycle time as a rational number of seconds.

Cycle Time Extension : The operational value of the *CycleTimeExtension* parameter for the gate. The value is an unsigned integer number of nanoseconds.

Base Time : The operational value of the *BaseTime* parameter for the gate. The value is a representation of a PTPtime value, consisting of a 48-bit integer number of seconds and a 32-bit integer number of nanoseconds.

Current Time : The current time, in PTPtime, as maintained by the local system. The value is a representation of a PTPtime value, consisting of a 48-bit integer number of seconds and a 32-bit integer number of nanoseconds. Only the seconds are displayed.

Config Change Time : The PTPtime at which the next config change is scheduled to occur. The value is a representation of a PTPtime value, consisting of a 48-bit integer number of seconds and a 32-bit integer number of nanoseconds.

Config Change Error : A counter of the number of times that a re-configuration of the traffic schedule has been requested with the old schedule still running and the requested base time was in the past.

Tick Granularity : The granularity of the cycle time clock, represented as an unsigned number of tenths of nanoseconds.

Config Pending : The value of the *ConfigPending* state machine variable. The value is TRUE if a configuration change is in progress but has not yet completed.

Oper IPV : The operational value of the IPV parameter for the gate. A value of -1 denotes the null value. The IPV (Internal Priority Value) is an ‘inside the box’ value; it is a recent addition to 802.1Q that supports more than eight Traffic Class queues.

RX Octets : The number of received octets.

GCL Length : The operational value of the *ListMax* parameter for the gate. The integer value indicates the number of entries (TLVs) in the *operControlList*.

GCL Status : A link to the GCL parameter status.

Buttons

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

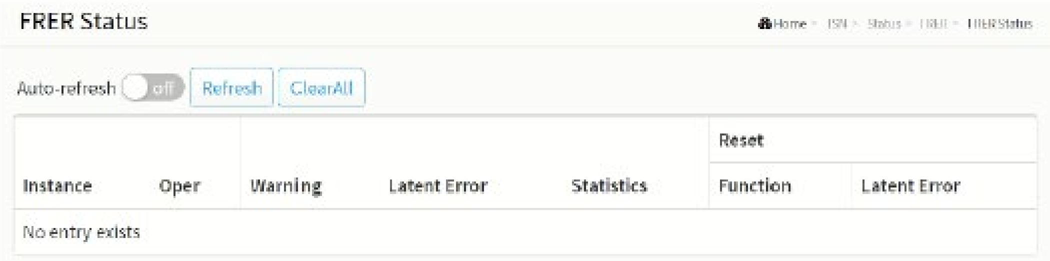
Refresh : Click to refresh the page immediately.

FRER

FRER Status

This page lets you view, reset, and clear current FRER (Frame Replication and Elimination for Reliability) status.

IEEE 802.1Qca integrates control protocols to manage multiple topologies, configure an explicit forwarding path (a predefined path for each stream), reserve bandwidth, provide data protection and redundancy, and distribute flow synchronization and flow control messages.



					Reset	
Instance	Oper	Warning	Latent Error	Statistics	Function	Latent Error
No entry exists						

Figure 18-2.4.1: FRER Status

Parameter descriptions:

Instance : The ID of the FRER instance.

Oper : The operational state of the FRER instance.

up: Active.

down: Disabled or Internal error.

Warning : Operational warnings of the FRER instance.

up: No warnings.

down: There are warnings, use tooltip to see.

Latent Error :

up: No errors.

down: There are latent errors.

Statistics : Check to reset statistics counters.

Reset Function : Click to perform a reset function.

If this FRER instance is in generation mode, this is used to reset the sequence number of the sequence generator.

If this FRER instance is in recovery mode, this is used to reset the recovery function. It resets both possible individual recovery functions and the compound recovery functions.

Reset Latent Error : Click to clear a sticky latent error.

Buttons

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

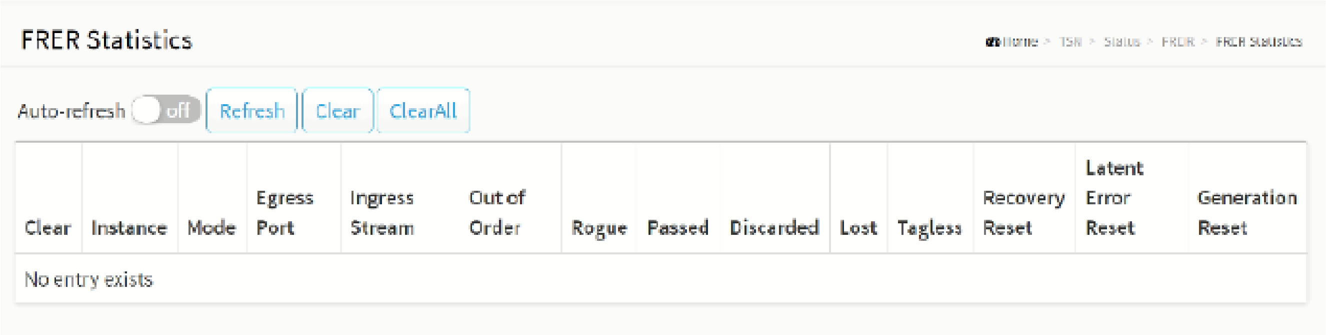
Refresh: Click to refresh the page immediately.

Clear : Clears the blocked flag for selected entries.

Clear all : Clears the blocked flag for all entries.

FRER Statistics

This page lets you view and clear current FRER (Frame Replication and Elimination for Reliability) statistics counters.



FRER Statistics

Home > TSN > Status > FRER > FRER Statistics

Clear	Instance	Mode	Egress Port	Ingress Stream	Out of Order	Rogue	Passed	Discarded	Lost	Tagless	Recovery Reset	Latent Error Reset	Generation Reset
No entry exists													

Figure 18-2.4.2: FRER Statistics

Parameter descriptions:

Clear : Check this box to mark an entry for clearance in the next Clear operation.

Instance : The FRER instance ID.

Mode : The mode of operation, either Generation or Recovery:

Generation : This FRER instance is currently generating.

Recovery : This FRER instance is currently recovering from a failure.

Egress Port : List of egress port numbers.

Ingress Stream : List of Ingress stream Ids.

Out of Order : IEEE 802.1CB-2017: *frerCpsSeqRcvyOutOfOrderPackets*.

Rogue : IEEE 802.1CB-2017: *frerCpsSeqRcvyRoguePackets*.

Passed : IEEE 802.1CB-2017: *frerCpsSeqRcvyPassedPackets*.

Discarded : IEEE 802.1CB-2017: *frerCpsSeqRcvyDiscardedPackets*.

Lost : IEEE 802.1CB-2017: frerCpsSeqRcvyLostPackets.

Tagless : IEEE 802.1CB-2017: frerCpsSeqRcvyTaglessPackets.

Recovery Reset : IEEE 802.1CB-2017: frerCpsSeqRcvyResets.

Latent Error Reset : IEEE 802.1CB-2017: frerCpsSeqRcvyLatentErrorResets.

Generation Reset : IEEE 802.1CB-2017: frerCpsSeqGenResets.

Buttons

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

Refresh : Click to refresh the page immediately.

Clear : Clears the blocked flag for selected entries.

Clear All : Clears the blocked flag for all entries.

TSN Troubleshooting

Note that TSN (time-sensitive networking) is not a single technology. TSN is a set of standards, maintained by the IEEE 802.1 task group, defining mechanisms for time-sensitive transmission of data.

TSN provides these 3 main functions: synchronizing all clocks on the network, scheduling the highest priority traffic, and then "shaping" remaining traffic to set the desired traffic patterns.

> **Time synchronization**: All devices that are participating in real-time communication need to have a common understanding of time.
>
> **Scheduling and traffic shaping**: All devices that are participating in real-time communication adhere to the same rules in processing and forwarding communication packets.
>
> **Selection of communication paths, path reservations, and fault-tolerance**: All devices that are participating in real-time communication adhere to the same rules in selecting communication paths and in reserving bandwidth and time slots, possibly utilizing more than one simultaneous path to achieve fault-tolerance.

The set of Time-Sensitive Networking standards includes IEEE 802.1Qat Stream Reservation Protocol (SRP), 802.1aq Shortest Path Bridging (SPB), 802.1Qcc-2018 Stream Reservation Protocol (SRP) Enhancements and Performance Improvements, 802.1Qci Per-Stream Filtering and Policing, 802.1CB-2017 FRER (Frame Replication and Elimination for Reliability), etc.

Since TSN is an evolving set of standards, it is recommended that you:

1. Review in detail the available status and statistics webpages for obvious problems: Stream Filter Status on page 306, Stream Filter Statistics on page 307, Stream Gate Status on page 308, and FRER Statistics on page 311.

2. Verify that the various TSN parameter settings are valid and consistent with your configuration. See these webpages: PTP Check on page 289, Frame Preemption Configuration on page 290, TAS Configuration Parameters on page 291, Max SDU Size on page 293, PSFP on page 294, Flow Meter on page 296, Stream Filter on page 297, Stream Gate on page 298, FRER on page 300, TAS on page 303, and PSFP on page 305.

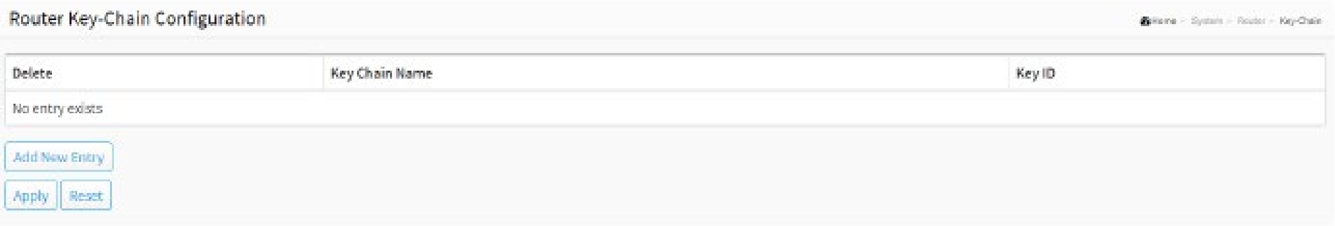
20. Router

A router is a networking device that forwards data packets between computer networks. Routers perform the traffic directing functions on the Internet. Data sent through the Internet, such as a web page or email, in the form of data packets. A packet is typically forwarded from one router to another router through an internetwork (e.g., the Internet) until it reaches its destination node. A router is connected to two or more data lines from different IP networks. When a data packet comes in on one of the lines, the router reads the network address information in the packet header to determine the ultimate destination. Then, using information in its routing table or routing policy, it directs the packet to the next network on its journey.

Note: At the System > IP Settings > Advanced IP Settings page there is a Network Mode parameter where you can set the IP stack to act as a Host or a Router. A Router mode entry is required for L3 Routing operations. On the same page, in the IP Routes section, you must provide this parameter if you will be configuring L3 Routing as described in this chapter.

Key-Chain

A keychain is a sequence of keys that provides dynamic authentication to ensure secure communication by periodically changing the key and authentication algorithm without service interruption.



Router Key-Chain Configuration

Delete	Key Chain Name	Key ID
No entry exists		

Figure 19-1: Router Key-Chain Configuration

Parameter descriptions:

Delete : Click to delete an existing entry.

Key Chain Name : The given name of the key chain.

Key ID : The assigned key chain identifier.

Buttons

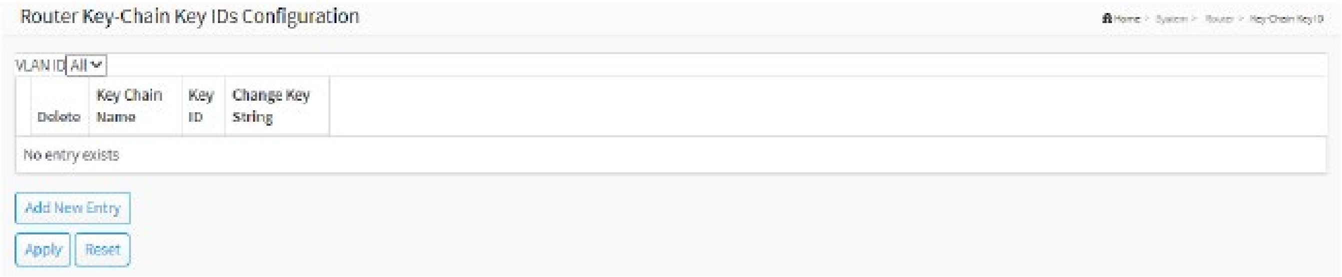
Add New Entry: Click to add a new entry (row) to the table.

Apply : Click to save changes.

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

Key-Chain Key ID

Each key in a keychain has a key string, authentication algorithm, sending lifetime, and receiving lifetime. When the system time is within the lifetime of a key in a keychain, an application uses the key to authenticate incoming and outgoing packets. The keys in the keychain take effect one by one according to the sequence of the configured lifetimes. This way, the authentication algorithms and keys are dynamically changed to implement dynamic authentication.



Router Key-Chain Key IDs Configuration

VLAN ID All

Delete	Key Chain Name	Key ID	Change Key String
No entry exists			

Figure 19-2: Router Key-Chain Key IDs Configuration

Parameter descriptions:

VLAN ID : At the dropdown select the set of VIDs to display (All or a specific VLAN ID).

Delete : Click to delete an existing entry.

Key Chain Name : The given name of the key chain.

Key ID : The assigned key chain identifier

Change Key String :Click to change the current key chain.

Buttons

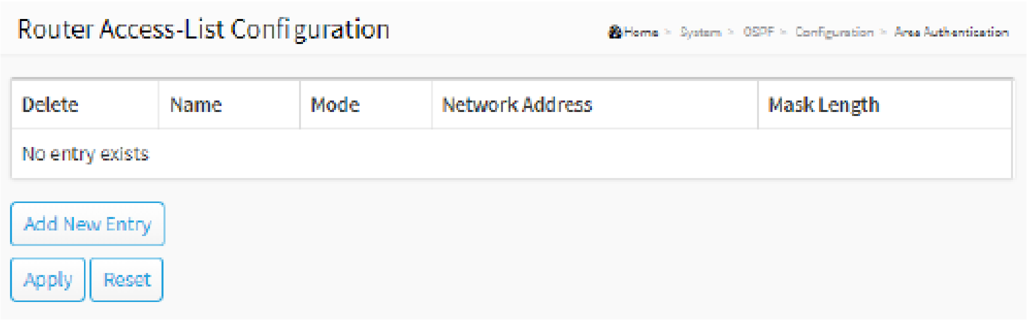
Add New Entry: Click to add a new entry to the table.

Apply : Click to save changes.

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

Access-list

This page lets you view and set Router Access-List instances and parameters. Navigate to the System > OSPF > Configuration > Area Authentication menu path to display the Router Access-List Configuration page:



Router Access-List Configuration

Delete	Name	Mode	Network Address	Mask Length
No entry exists				

Figure 19-3: Router Access-List Configuration

Parameter descriptions:

Delete : Click to delete an existing entry.

Name : The name of the router access list.

Mode : The access list operating mode.

Network Address : The network address of the router access list.

Mask Length : The netmask length of the router access list.

Buttons

Add New Entry: Click to add a new entry to the table.

Apply : Click to save changes.

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

You can filter incoming and outgoing routes for a given IP interface using two Standard Access Lists - one for input and one for output.

The standard Access List is a named, ordered list of pairs of IP prefix (IP address and IP mask length) and action. The action can be ***deny*** or ***permit***.

> If an access list is defined, each route from the RIP message is checked against the list starting from the first pair:
>
> > if it matches the first pair and the action is ***permit***, the route is passed;
> > if the action is ***deny***, the route is not passed. If the route does not match, the following pair is considered.

If there is no pair that the route matches, the ***deny*** action is applied.

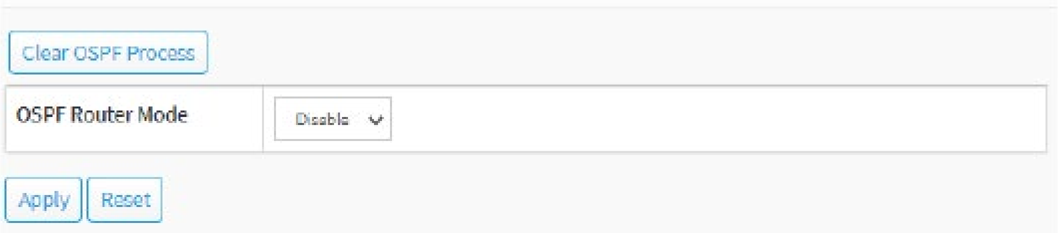
21. OSFP

Configuration

Open Shortest Path First (OSPF) is a link-state routing protocol. It is designed to be run internal to a single Autonomous System. Each OSPF router maintains an identical database describing the Autonomous System's topology. Using this database, a routing table is calculated by constructing a shortest-path tree.
For more OSPFv2 information see https://datatracker.ietf.org/doc/html/rfc2328.

Global Configuration

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



OSPF Router Mode	Disable

Figure 20-1: OSPF Global Configuration

Parameter descriptions:

OSPF Router Mode : At the dropdown select to Enable or Disable the OSPF router mode. The default is Disabled.

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

Auto: The default algorithm will choose the largest IP address assigned to the router.

Specific: User specified router ID. The valid range is from 0.0.0.1 to 255.255.255.254.

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

Default Metric : User specified default metric value for the OSPF routing protocol. The field is significant only when the argument 'I*sSpecificDefMetric*' is TRUE.

Auto: The default metric is calculated automatically based on the routing protocols.

Specific: User specified default metric. The valid range is 0 to 16777214.

Static Redistribute Metric Type : The OSPF redistributed metric type for the static routes:

None: The static routes are not redistributed.

External Type 1: External Type 1 of the static routes.

External Type 2: External Type 2 of the static routes.

Static Redistribute Metric Value : User specified metric value for the static routes. The field is significant only when the argument '*StaticRedistIsSpecificMetric*' is TRUE. The valid range is 0 to 16777214.

Auto: The redistributed metric is the same as the original metric value.

Specific: User specified metric for the static routes.

Connected Redistribute Metric Type : The OSPF redistributed metric type for the connected interfaces.

None: The connected interfaces are not redistributed.

External Type 1: External Type 1 of the connected interfaces routes.

External Type 2: External Type 2 of the connected interfaces routes.

Connected Redistribute Metric Value : User specified metric value for the connected interfaces. The field is significant only when the argument *'ConnectedRedistIsSpecificMetric'* is TRUE. The valid range is 0 to 16777214.

Auto: The redistributed metric is the same as the original metric value.

Specific: User specified metric for the connected routes.

RIP Redistribute Metric Type : The OSPF redistributed metric type for the RIP routes. The field is significant only when the RIP protocol is supported on the device.

None: The RIP routes are not redistributed.

External Type 1: External Type 1 of the RIP routes.

External Type 2: External Type 2 of the RIP routes.

RIP Redistribute Metric Value : User specified metric value for the RIP routes. The field is significant only when the RIP protocol is supported on the device and argument *'RipRedistIsSpecificMetric'* is TRUE. The valid range is 0 to 16777214.

Auto: The redistributed metric is the same as the original metric value.

Specific: User specified metric for the RIP routes.

Stub router during startup period : Configures OSPF to advertise a maximum metric during startup for a configured period of time.

Stub router on startup interval time : User specified time interval (seconds) to advertise itself as stub area. The field is significant only when the on-startup mode is enabled. The valid range is 5 to 86400 seconds.

Stub router during shutdown period : Configures OSPF to advertise a maximum metric during shutdown for a configured period of time. The device advertises a maximum metric when the OSPF router mode is disabled and notice that the mechanism also works when the device reboots but not for the 'reload default' case.

Stub router on shutdown interval time : User specified time interval (seconds) to wait till shutdown completed. The field is significant only when the on-shutdown mode is enabled. The valid range is 5 to 100 seconds.

Stub router administrative mode : Configures OSPF stub router mode administratively applied, for an indefinite period.

Default Route Redistribution Metric Type : The OSPF redistributed metric type for a default route:

None: The default route are not redistributed.

External Type 1: External Type 1 of the default route.

External Type 2: External Type 2 of the default route.

Default Route Redistribution Metric value : User specified metric value for a default route. The field is significant only when the argument *'DefaultRouteRedistIsSpecificMetric'* is TRUE. The valid range is 0 to 16777214. Auto: The redistributed metric is the same as the original metric value. Specific: User specified metric for the default route.

Default Route Redistribution Always : Specifies to always advertise a default route into all external-routing capable areas. Otherwise, the router only to advertise the default route when the advertising router already has a default route.

Administrative Distance : The OSPF administrative distance.

Buttons

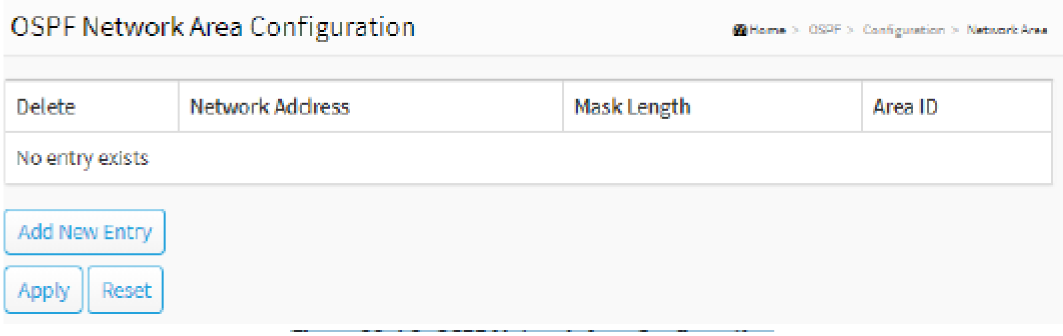
Clear OSPF Process : Click to reset the current OSPF process.

Apply : Click to save changes.

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

Network Area

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



OSPF Network Area Configuration

Home > OSPF > Configuration > Network Area

Delete	Network Address	Mask Length	Area ID
No entry exists			

Figure 20-1.2: OSPF Network Area Configuration

Parameter descriptions:

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

Network Address : IPv4 network address.

Mask Length : IPv4 network mask length.

Area ID : The OSPF area ID.

Buttons

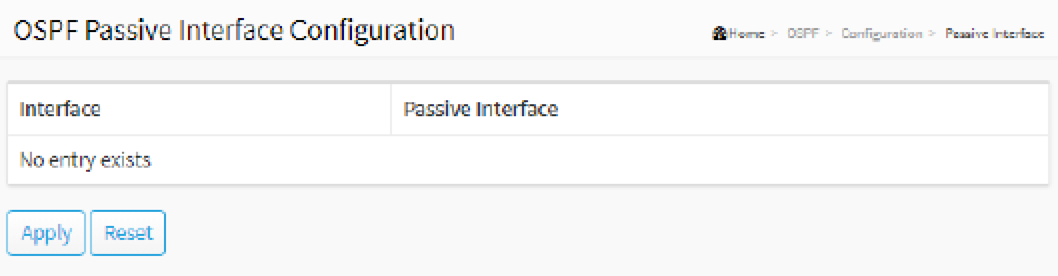
Add New Entry: Click to add a new entry to the table.

Apply : Click to save changes.

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

Passive Interface

This page provides the OSPF router passive interface configuration table.



OSPF Passive Interface Configuration

Interface	Passive Interface
No entry exists	

Figure 20-1.3: OSPF Passive Interface Configuration

Parameter descriptions:

Interface : Interface identification.

Passive Interface : Enable the interface as OSPF passive-interface. When an interface is configured as a passive-interface, sending of OSPF routing updates is suppressed, so the interface does not establish adjacencies (no OSPF Hellos). The subnet of all interfaces (both passive and active) is advertised by the OSPF router.

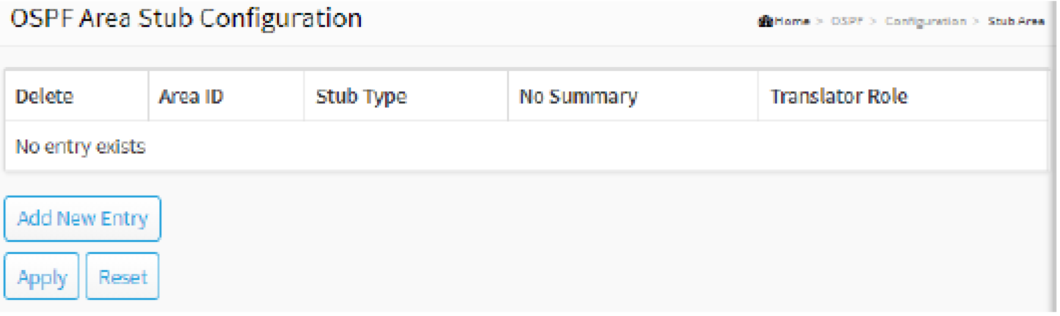
Buttons

Apply : Click to save changes.

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

Stub Area

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



OSPF Area Stub Configuration

Delete	Area ID	Stub Type	No Summary	Translator Role
No entry exists				

OSPF Stub Area Configuration

Parameter descriptions:

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

Area ID : The OSPF area ID.

Stub Type : The OSPF stub configured type.

Stub Area: Configure the area as stub area.

NSSA: Configure the area as not-so-stubby area (NSSA).

No Summary : The value is true to configure the inter-area routes do not inject into this stub area.

Translator Role : The OSPF NSSA translator role.

Candidate: this NSSA-ABR router will participate in the translator election.

Never: this NSSA-ABR router never translates.

Always: this NSSA-ABR router always translates.

Buttons

Add New Entry : Click to add a new entry to the table.

Apply : Click to save changes.

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

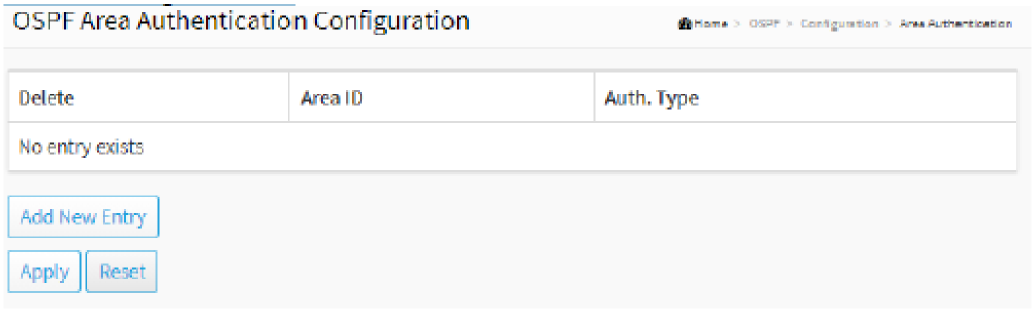
See also:

OSPF v2: https://www.rfc-editor.org/rfc/pdfrfc/rfc2328.txt.pdf

NSSA: https://datatracker.ietf.org/doc/html/rfc3101

Area Authentication

This page displays the OSPF Area Authentication Configuration table. It is used to apply the authentication to all the interfaces belonging to the area.



OSPF Area Authentication Configuration

Delete	Area ID	Auth. Type
No entry exists		

OSPF Area Authentication Configuration

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

Area ID : The OSPF area ID.

Auth. Type : The authentication type on an area is applied to all the interfaces belong to that area.
The authentication type on an IP interface or a virtual link overrides the authentication type on an area and is useful if different interfaces in the same area use different authentication types. Specify the authentication type:

Simple Password: Simple password authentication.

Message Digest: MD5 digest authentication.

Buttons

Add New Entry : Click to add a new entry to the table.

Apply : Click to save changes.

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

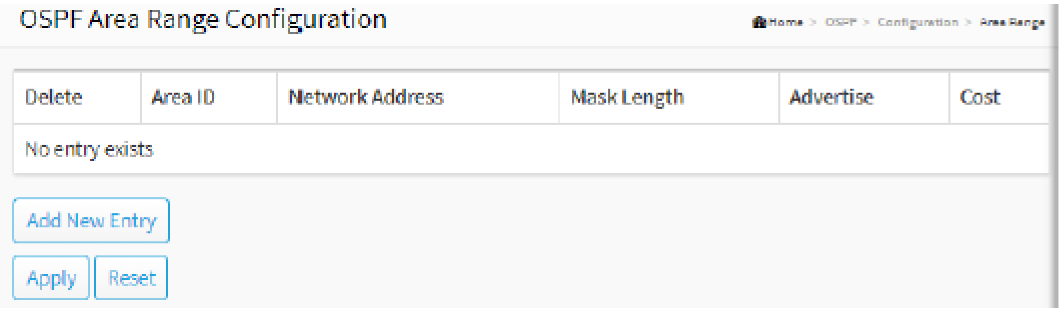
Area Range

This page displays the OSPF Area Range Configuration table. It is used to summarize the intra area paths from a specific address range in one summary-LSA(Type-3) and advertised to other areas or configure the address range status as '*DoNotAdvertise*' which the summary-LSA (Type-3) is suppressed.

The area range configuration is used for Area Border Routers (ABRs) and only router-LSAs (Type-1) and network-LSAs (Type-2) can be summarized.

The AS-external-LSAs (Type-5) cannot be summarized because the scope is OSPF autonomous system (AS).

The AS-external-LSAs (Type-7) cannot be summarized because the feature is not supported yet.



OSPF Area Range Configuration

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

Figure 20-1.6: OSPF Area Range Configuration

Parameter descriptions:

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

Area ID : The OSPF area ID.

Network Address : The IPv4 network address.

Mask Length : The IPv4 network mask length.

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

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

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

Buttons

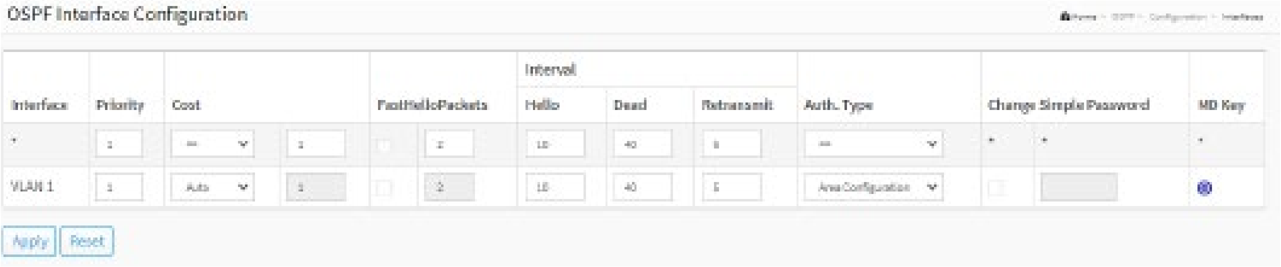
Add New Entry : Click to add a new entry to the table.

Apply : Click to save changes.

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

Interfaces

This page shows the OSPF Interface Configuration table.



OSPF Interface Configuration

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

Figure 20-1.7: OSPF Interface Configuration

Parameter descriptions:

Interface : Interface identification (e.g., VLAN1).

Priority : Specify a router priority for the interface. The valid range is 0 – 255; the default value is 1.

Cost : User specified cost for this interface. It's link state metric for the interface. The field is significant only when *'IsSpecificCost'* is TRUE. The valid range is 1 - 65535 and the default setting is 'Auto' cost mode.

FastHelloPackets : How many Hello packets will be sent per second. The valid range is 1 - 10 and the default setting is disabled.

Hello Interval : How many Hello packets will be sent per second. The valid range is 1 - 65535 seconds and the default value is 10 seconds.

OSPF uses Hello packets and two timers to check if a neighbor is still alive:

Hello Interval defines how often the hello packet is sent.

Dead Interval defines how long to wait for hello packets before declaring the neighbor dead.

The hello and dead interval values can be different based on the OSPF network type.

Dead Interval : The time interval (in seconds) between hello packets. The valid range is 1 - 65535 seconds and the default value is 40 seconds.

Retransmit Interval : The time interval (in seconds) between Link-State Advertisement (LSA) retransmissions for adjacencies. The valid range is 3 - 65535 seconds and the default value is 5 seconds.

Auth. Type : The authentication type:

Simple Password: It's using a plain text authentication. A password must be configured, but a simple password can be read by a packet sniffer.

Message Digest: It's message-digest algorithm 5 (MD5) authentication. Keying material must also be configured. This is the most secure method.

Null Authentication: No authentication.

Area Configuration: Refer to Area Authentication setting on page 317.

Change Simple Password : Check the box to change the simple password (fill with plain text). The allowed input length is 1 - 8 characters.

MD Key : Click the icon to edit the Message Digest key for the entry (see below).

Buttons

Add New Entry : Click to add a new entry to the table.

Apply : Click to save changes.

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

Edit the Message Digest key:

In the MD Key field click the (●) icon to edit the Message Digest key:

To be supplied.

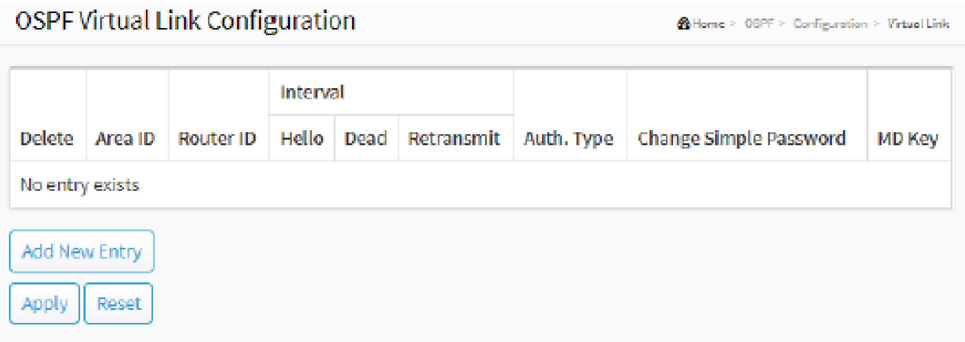
Parameter descriptions: To be supplied.

Virtual Link

This page shows the OSPF virtual link configuration table. The virtual link is established between two ABRs to overcome the fact that all the areas must be connected directly to the backbone area.

The backbone must be contiguous, but it does not need to be physically contiguous. Backbone connectivity can be established and maintained by the configuration of "virtual links".

Virtual links can be configured between any two backbone routers that have an interface to a common non-backbone area. Virtual links belong to the backbone. The protocol treats two routers joined by a virtual link as if they were connected by an unnumbered point-to-point backbone network. The routing protocol traffic that flows along the virtual link uses intra-area routing only.



OSPF Virtual Link Configuration

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

OSPF Virtual Link Configuration

Parameter descriptions:

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

Area ID : The OSPF Area ID.

Router ID : The OSPF router ID.

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

OSPF uses Hello packets and two timers to check if a neighbor is still alive:

Hello Interval defines how often the hello packet is sent.
Dead Interval defines how long to wait for hello packets before declaring the neighbor dead.

The Hello and the Dead interval values can be different based on the OSPF network type.

Dead Interval : The number of seconds to wait until the neighbor is declared to be dead. The valid range is 1 to 65535 seconds and the default value is 40 seconds.

Retransmit Interval : The time interval (in seconds) between link-state advertisement (LSA) retransmissions for adjacencies. The valid range is 3 to 65535 and the default value is 5 seconds.

Auth. Type : The authentication type on an area.

Simple Password : It's using a plain text authentication. A password must be configured, but the password can be read by packet sniffers.

Message Digest : It's message-digest algorithm 5 (MD5) authentication. Keying material must also be configured. This is the most secure method.

Null Authentication : No authentication.

Area Configuration : Refer to Area Authentication setting on page 317.

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

MD Key : Click the (●) icon to edit the Message Digest key for the entry (see below).

Buttons

Add New Entry : Click to add a new entry to the table.

Apply : Click to save changes.

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

Edit the Message Digest key:

In the MD Key field click the (●) icon to edit the Message Digest key:

To be supplied.

Parameter descriptions: To be supplied.

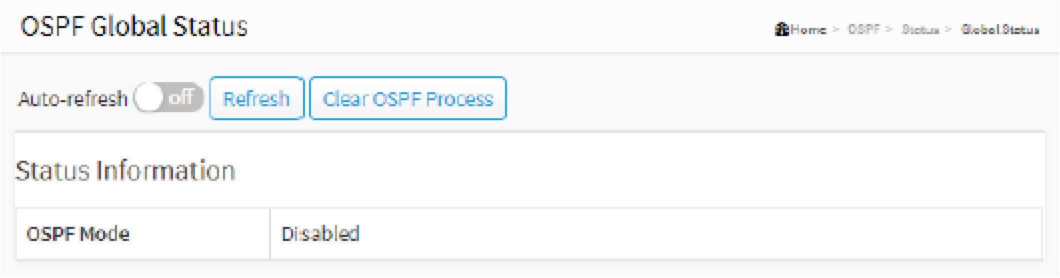
Parameter descriptions:

It doesn't matter which key number you choose but it has to be the same on both ends.

Status

Global Status

This page shows the OSPF router Global status. It is used to provide the OSPF router status information.



OSPF Global Status

Status Information

OSPF Mode	Disabled

Figure 20-2.1: OSPF Global Status

Parameter descriptions:

Status Information

OSPF Mode: Displays the OSPF mode of operation (e.g., Disabled, Enabled).

Router ID : OSPF router ID.

SPF Delay : Delay time (in seconds)of SPF calculations.

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

SPF Max. Wait Time : Maximum wait time (in milliseconds) between consecutive SPF calculations.

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

Min. LSA Interval : Minimum interval (in seconds) between link-state advertisements.

Min. LSA Arrival : Maximum arrival time (in milliseconds) of link-state advertisements.

External LSA Count : Number of external link-state advertisements.

External LSA Checksum : Number of external link-state checksum.

Attached Area Count : Number of areas attached for the router.

Buttons

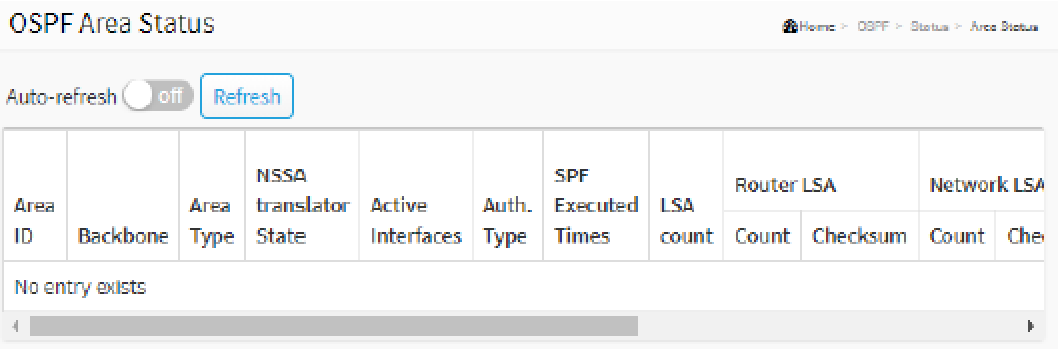
Auto-refresh : Check this box to refresh the page automatically every 3 seconds.

Refresh : Click to manually refresh the page immediately.

Clear OSPF Process : Click to reset the current OSPF process.

Area Status

This page shows the OSPF network area status table.



OSPF Area Status

Area ID	Backbone	Area Type	NSSA translator State	Active Interfaces	Auth. Type	SPF Executed Times	LSA count	Router LSA		Network LSA	
								Count	Checksum	Count	Che
No entry exists											

Figure 20-2.2: OSPF Area Status

Parameter descriptions:

Area ID : The Area ID.

Backbone : Indicate if it is the backbone area or not.

Area Type : The area type.

NSSA translator state : Indicate the current state of the NSSA-ABR translator which the router uses to translate Type-7 LSAs in the NSSA to Type-5 LSAs in backbone area.

Active Interfaces : Number of active interfaces attached in the area.

Auth. Type : The authentication type in the area.

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

LSA Count : Number of the total LSAs for the particular area.

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

Router LSA Checksum : The router-LSAs (Type-1) checksum.

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

Network LSA Checksum : The network-LSAs (Type-2) checksum.

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

Summary LSA Checksum : The summary-LSAs (Type-3) checksum.

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

ASBR Summary LSA Checksum : The ASBR-summary-LSAs (Type-4) checksum.

NSSA LSA Count :   Number of the NSSA LSAs of a given type for the particular area.

NSSA LSA Checksum : The NSSA LSAs checksum.

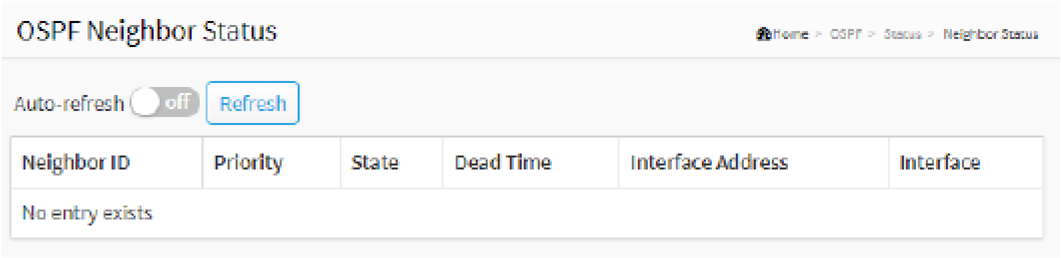
Buttons

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

Refresh : Click to refresh the page immediately.

Neighbor Status

This page displays the OSPF IPv4 neighbor status table.



OSPF Neighbor Status

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

Figure 20-2.3: OSPF Neighbor Status

Parameter descriptions:

Neighbor ID : The Neighbor ID.

Priority : The priority of OSPF neighbor router. This parameter is used when selecting the DR for the network. The router with the highest priority becomes the DR.

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

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

Interface Address : The IP address.

Interface : The network interface.

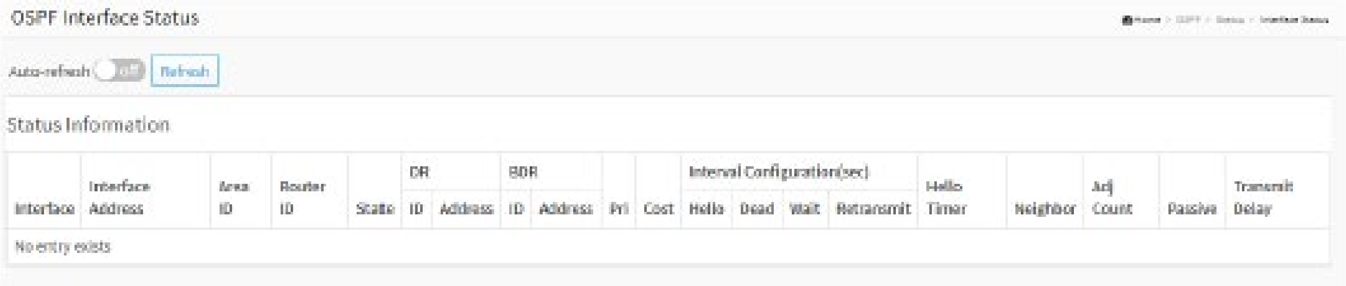
Buttons

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

Refresh : Click to refresh the page immediately.

Interface Status

This page displays the OSPF interface status table. It is used to provide the OSPF interface status information.



OSPF Interface Status

Status Information

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

Figure 20-2.4: OSPF Interface Status

Parameter descriptions:

Interface : Interface identification.

Interface Address : IPv4 network address.

Area ID : The OSPF area ID.

Router ID : The OSPF router ID.

State : The state of the link.

DR ID : The router ID of DR. Each broadcast and NBMA network that has at least two attached routers has a DR. The DR generates an LSA for the network and has other special responsibilities in the running of the protocol. The DR is elected by the Hello Protocol.

DR Address : The IP address of DR.

BDR ID : The router ID of BDR.

BDR Address : The IP address of BDR.

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

Cost : The cost of the interface.

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

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

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

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

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

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

Adj Count : Adjacent neighbor count. This is the number of routers running OSPF that are fully adjacent with this router. When OSPF neighbor adjacency is not in the full state then it is in one of the other states: there's no

OSPF neighbor at all, or the state is 'stuck' in a state of ATTEMPT, INIT, 2-WAY, EXSTART/EXCHANGE, or LOADING.

Passive : Indicate if the interface is a passive interface. When an interface is configured as a passive-interface, sending of OSPF routing updates is suppressed, so the interface does not establish adjacencies (no OSPF Hellos). The subnet of all interfaces (both passive and active) is advertised by the OSPF router.

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

Buttons

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

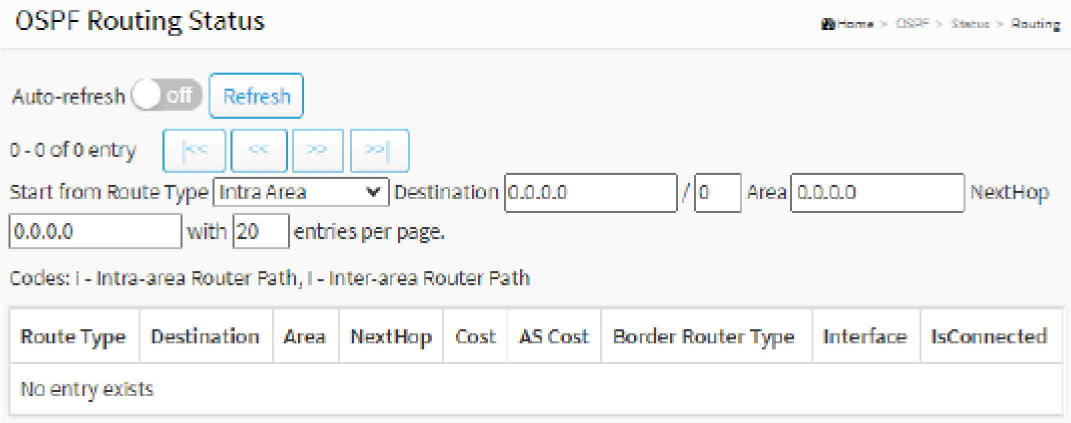
Refresh : Click to refresh the page immediately.

Routing Status

This page displays the OSPF Routing Status table.

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

The "Start from ID" input field allow the user to change the starting point in this table. Clicking the **>>** button will update the displayed table starting from that or the closest next entry match. In addition, these input fields will upon a **|<<** button click - assume the value of the first displayed entry, allowing for continuous refresh with the same start input field.



OSPF Routing Status

Home > OSPF > Status > Routing

Auto-refresh off Refresh

0 - 0 of 0 entry |<< << >> >>|

Start from Route Type Intra Area Destination 0.0.0.0 / 0 Area 0.0.0.0 NextHop 0.0.0.0 with 20 entries per page.

Codes: i - Intra-area Router Path, I - Inter-area Router Path

Route Type	Destination	Area	NextHop	Cost	AS Cost	Border Router Type	Interface	IsConnected
No entry exists								

Figure 20-2.5: OSPF Routing Status

<u>**Entry fields**</u> :

Start from Route Type : At the dropdown select Intra Area, Inter Area, Border Router, External Type-1, or External Type-2. The default is Intra Area.

Destination : Enter the destination IP address. The default is 0.0.0.0/0.

Area : Enter the area IP address The default is 0.0.0.0.

NextHop : Enter the IP address of the next hop. The default is 0.0.0.0.

Codes : i – Intra-area Router Path, I – Inter-area Router Path.

<u>**Table parameters**</u> :

Route Type : The OSPF route type:

Intra Area: The destination is an OSPF route which is located on intra-area.

Inter Area: The destination is an OSPF route which is located on inter-area.

Border Router: The destination is a border router.

External Type-1: The destination is an external Type-1 route.

External Type-2: The destination is an external Type-2 route.

Destination : Network and prefix (e.g., 10.0.0.0/16) of the given route entry.

Area : Indicates which area the route or router can be reached via/to.

NextHop : Ipv4 address encoded as "a.b.c.d", where a-d is a base-10 human readable integer in the range [0-255]

Cost : The cost of the route.

AS Cost : The cost of the route within the OSPF network. It is valid for External Type-2 routes and is always '0' for other route types.

Border Router Type : The border router type of the OSPF route entry:

- ***i-ABR*** : The border router is an ABR.
- ***i-ASBR*** : The border router is an ASBR located on Intra-area.
- ***I-ASBR*** : The border router is an ASBR located on Inter-area.
- ***i-ABR/ASBR:*** The border router is an ASBR attached to at least 2 areas.

Interface : The interface where the IP packet is outgoing.

IsConnected : The destination is connected directly or not.

Buttons

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

Refresh : Click to refresh the page immediately.

|<< : Updates the table entries, starting from the first available entry. If the first entry of the table is displayed, the button is disabled

<< : Updates the table entries, ending at the entry prior to the first entry currently displayed. If the first entry of the table is displayed, the button is disabled

>> : Updates the table entries, starting from the entry next to the last entry currently displayed. If the last entry of the table is displayed, the button is disabled.

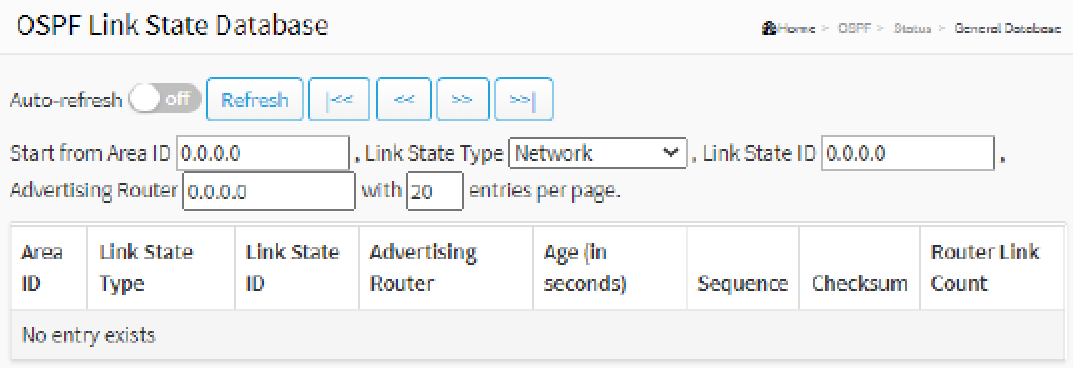
>>| : Updates the table entries, ending at the last available entry. If the last entry of the table is displayed, the button is disabled.

General Database

This page displays the OSPF LSA link state database information table.

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

Clicking the >> button will update the displayed table starting from that or the closest next entry match. In addition, these input fields will upon a |<< button click - assume the value of the first displayed entry, allowing for continuous refresh with the same start input field.



OSPF Link State Database

Start from Area ID 0.0.0.0 , Link State Type Network , Link State ID 0.0.0.0 , Advertising Router 0.0.0.0 with 20 entries per page.

Area ID	Link State Type	Link State ID	Advertising Router	Age (in seconds)	Sequence	Checksum	Router Link Count
No entry exists							

Figure 20-2.6: OSPF Routing Status

<u>**Entry fields**</u> :

Start from Area ID : Input field lets you change the starting point in this table. The default is 0.0.0.0. Enter the OSPF area ID of the link state advertisement. It is not required for external LSA.

Link State Type : At the dropdown select the type of the link state advertisement (e.g., Router, Network, Summary, Summary ASBR).

Network : Use Network type of link state advertisement (default).

Router : Use Router type of link state advertisement.

Summary : Use Summary type of link state advertisement.

Summary ASBR : Use Summary type of link state advertisement.

Link State ID : Enter the OSPF link state IP. It identifies the piece of the routing domain that is being described by the LSA.

Advertising Router : Enter the advertising router ID which originated the LSA. The default is 0.0.0.0.

<u>**Table parameters**</u> :

Area ID : Displays the OSPF area ID of the link state advertisement. It is not required for external LSA.

Age (in seconds) : The time in seconds since the LSA was originated.

Sequence : The LS sequence number of the LSA.

Checksum : The checksum of the LSA contents.

Router Link Count : The link count of the LSA. The field is significant only when the Link State Type is 'Router Link State' (Type 1).

Buttons

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

Refresh : Click to refresh the page immediately.

|<< : Updates the table entries, starting from the first available entry. If the first entry of the table is displayed, the button is disabled

<< : Updates the table entries, ending at the entry prior to the first entry currently displayed. If the first entry of the table is displayed, the button is disabled

>> : Updates the table entries, starting from the entry next to the last entry currently displayed. If the last entry of the table is displayed, the button is disabled.

>>| : Updates the table entries, ending at the last available entry. If the last entry of the table is displayed, the button is disabled.

OSPF LSA Types

OSPF uses a Link State Database (LSDB) and fills it with LSAs (Link State Advertisements). OSPF uses several different types of LSAs:

LSA Type 1: Router LSA

LSA Type 2: Network LSA

LSA Type 3: Summary LSA

LSA Type 4: Summary ASBR LSA

LSA Type 5: Autonomous system external LSA

LSA Type 6: Multicast OSPF LSA

LSA Type 7: Not-so-stubby area LSA

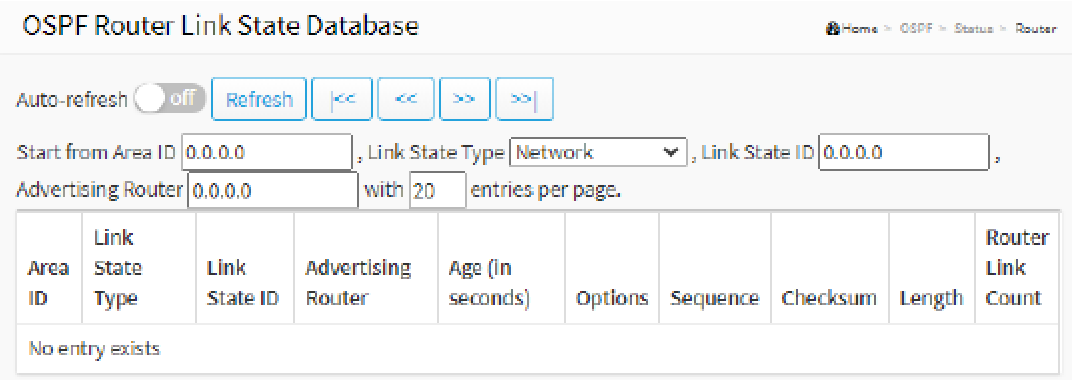
LSA Type 8: External attribute LSA for BGP

Router

This page displays the OSPF LSA Router link state database information table.

Navigating to the OSPF Status > Router menu pat to display the OSPF Router Link State Database page.

Each page shows up to 999 table entries, selected through the "entries per page" input field. When first visited, the web page will show the beginning entries of this table. The "Start from entry keys" input field lets you change the starting point in this table. Clicking the >> button will update the displayed table starting from that or the closest next entry match. In addition, these input fields will upon a |<< button click - assume the value of the first displayed entry, allowing for continuous refresh with the same start input field.



OSPF Router Link State Database

Start from Area ID 0.0.0.0 , Link State Type Network , Link State ID 0.0.0.0 , Advertising Router 0.0.0.0 with 20 entries per page.

Area ID	Link State Type	Link State ID	Advertising Router	Age (in seconds)	Options	Sequence	Checksum	Length	Router Link Count
No entry exists									

Figure 20-2.7: OSPF Router Link State Database

<u>**Entry fields**</u> :

Start from Area ID : Input field lets you change the starting point in this table. The default is 0.0.0.0. Enter the OSPF area ID of the link state advertisement. It is not required for external LSA.

Link State Type : At the dropdown select the type of the link state advertisement (e.g., Router, Network, Summary, Summary ASBR).

Network : Use Network type of link state advertisement (default).

Router : Use Router type of link state advertisement.

Summary : Use Summary type of link state advertisement.

Summary ASBR : Use Summary type of link state advertisement.

Link State ID : Enter the OSPF link state IP. It identifies the piece of the routing domain that is being described by the LSA.

Advertising Router : Enter the advertising router ID which originated the LSA. The default is 0.0.0.0.

<u>**Table parameters**</u> :

Area ID : The OSPF area ID of the link state advertisement

Link State Type : The type of the link state advertisement.

Link State ID : The OSPF link state ID. It identifies the piece of the routing domain that is being described by the LSA.

Advertising Router : The advertising router ID which originated the LSA.

Age : The time in seconds since the LSA was originated.

Options : The OSPF option field, present in OSPF hello packets, enables OSPF routers to support (or not support) optional capabilities, and to communicate their capability level to other OSPF routers.

Sequence : The LS sequence number of the LSA.

Checksum : The checksum of the LSA contents.

Length : The Length in bytes of the LSA.

Router Link Count : The link count of the LSA.

Buttons

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

Refresh : Click to refresh the page immediately.

|<< : Updates the table entries, starting from the first available entry. If the first entry of the table is displayed, the button is disabled

<< : Updates the table entries, ending at the entry prior to the first entry currently displayed. If the first entry of the table is displayed, the button is disabled

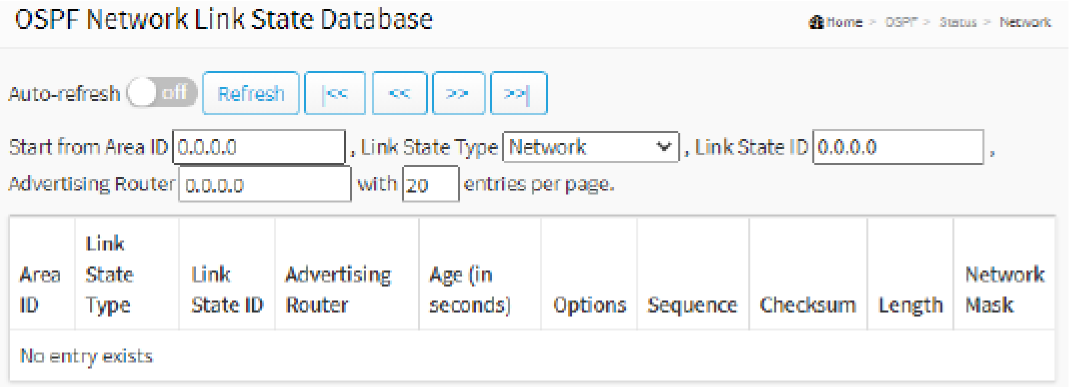
>> : Updates the table entries, starting from the entry next to the last entry currently displayed. If the last entry of the table is displayed, the button is disabled.

>>| : Updates the table entries, ending at the last available entry. If the last entry of the table is displayed, the button is disabled.

Network

This page displays the OSPF LSA Network link state database information table.

Each page shows up to 999 table entries, selected through the "entries per page" input field. When first visited, the web page will show the beginning entries of this table. The "Start from entry keys" input field lets you change the starting point in this table. Clicking the button will update the displayed table starting from that or the closest next entry match. In addition, these input fields will upon a button click - assume the value of the first displayed entry, allowing for continuous refresh with the same start input field.



OSPF Network Link State Database

Start from Area ID 0.0.0.0 , Link State Type Network , Link State ID 0.0.0.0 , Advertising Router 0.0.0.0 with 20 entries per page.

Area ID	Link State Type	Link State ID	Advertising Router	Age (in seconds)	Options	Sequence	Checksum	Length	Network Mask
No entry exists									

Figure 20-2.8: OSPF Network Link State Database

<u>**Entry fields**</u> :

Start from Area ID : Input field lets you change the starting point in this table. The default is 0.0.0.0. Enter the OSPF area ID of the link state advertisement. It is not required for external LSA.

Link State Type : At the dropdown select the type of the link state advertisement (e.g., Router, Network, Summary, Summary ASBR).

Network : Use Network type of link state advertisement (default).

Router : Use Router type of link state advertisement.

Summary : Use Summary type of link state advertisement.

Summary ASBR : Use Summary type of link state advertisement.

Link State ID : Enter the OSPF link state IP. It identifies the piece of the routing domain that is being described by the LSA.

Advertising Router : Enter the advertising router ID which originated the LSA. The default is 0.0.0.0.

<u>**Table parameters**</u> :

Area ID : The OSPF area ID of the link state advertisement

Link State Type : The type of the link state advertisement.

Link State ID : The OSPF link state ID. It identifies the piece of the routing domain that is being described by the LSA.

Advertising Router : The advertising router ID which originated the LSA.

Age : The time in seconds since the LSA was originated.

Options : The OSPF option field, present in OSPF hello packets, which enables OSPF routers to support (or not support) optional capabilities, and to communicate their capability level to other OSPF routers.

Sequence : The LS sequence number of the LSA.

Checksum : The checksum of the LSA contents.

Length : The Length in bytes of the LSA.

Network Mask : Network mask length. The field is significant only when the Link State Type is 'Network Link State' (Type 2).

Buttons

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

Refresh : Click to refresh the page immediately.

|<< : Updates the table entries, starting from the first available entry. If the first entry of the table is displayed, the button is disabled

<< : Updates the table entries, ending at the entry prior to the first entry currently displayed. If the first entry of the table is displayed, the button is disabled

>> : Updates the table entries, starting from the entry next to the last entry currently displayed. If the last entry of the table is displayed, the button is disabled.

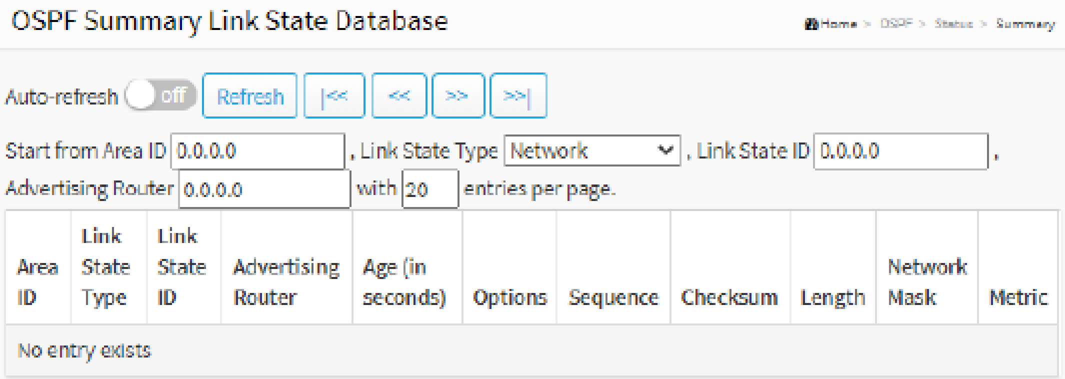
>>| : Updates the table entries, ending at the last available entry. If the last entry of the table is displayed, the button is disabled.

Summary

This page displays the OSPF LSA Summary link state database information table.

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

The "Start from entry keys" input field lets you change the starting point in this table. Clicking the button will update the displayed table starting from that or the closest next entry match. In addition, these input fields will upon a button click - assume the value of the first displayed entry, allowing for continuous refresh with the same start input field.



OSPF Summary Link State Database

Start from Area ID 0.0.0.0 , Link State Type Network , Link State ID 0.0.0.0 , Advertising Router 0.0.0.0 with 20 entries per page.

Area ID	Link State Type	Link State ID	Advertising Router	Age (in seconds)	Options	Sequence	Checksum	Length	Network Mask	Metric
No entry exists										

Figure 20-2.9: OSPF Summary Link State Database

<u>Entry fields</u> :

Start from Area ID : Input field lets you change the starting point in this table. The default is 0.0.0.0. Enter the OSPF area ID of the link state advertisement. It is not required for external LSA.

Link State Type : At the dropdown select the type of the link state advertisement (e.g., Router, Network, Summary, Summary ASBR).

Network : Use Network type of link state advertisement (default).

Router : Use Router type of link state advertisement.

Summary : Use Summary type of link state advertisement.

Summary ASBR : Use Summary type of link state advertisement.

Link State ID : Enter the OSPF link state IP. It identifies the piece of the routing domain that is being described by the LSA.

Advertising Router : Enter the advertising router ID which originated the LSA. The default is 0.0.0.0.

<u>Table parameters</u> :

Area ID : The OSPF area ID of the link state advertisement

Link State Type : The type of the link state advertisement.

Link State ID : The OSPF link state ID. It identifies the piece of the routing domain that is being described by the LSA.

Advertising Router : The advertising router ID which originated the LSA.

Age : The time in seconds since the LSA was originated.

Options : The OSPF option field, present in OSPF hello packets, which enables OSPF routers to support (or not support) optional capabilities, and to communicate their capability level to other OSPF routers.

Sequence : The LS sequence number of the LSA.

Checksum : The checksum of the LSA contents.

Length : The Length in bytes of the LSA.

Network Mask : Network mask length. The field is significant only when the Link State Type is 'Summary/ASBR Summary Link State' (Type 3, 4).

Metric : User specified metric for this summary route. The field is significant when the Link State Type is 'Summary/ASBR Summary Link State' (Type 3, 4).

Buttons

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

Refresh : Click to refresh the page immediately.

|<< : Updates the table entries, starting from the first available entry. If the first entry of the table is displayed, the button is disabled

<< : Updates the table entries, ending at the entry prior to the first entry currently displayed. If the first entry of the table is displayed, the button is disabled

>> : Updates the table entries, starting from the entry next to the last entry currently displayed. If the last entry of the table is displayed, the button is disabled.

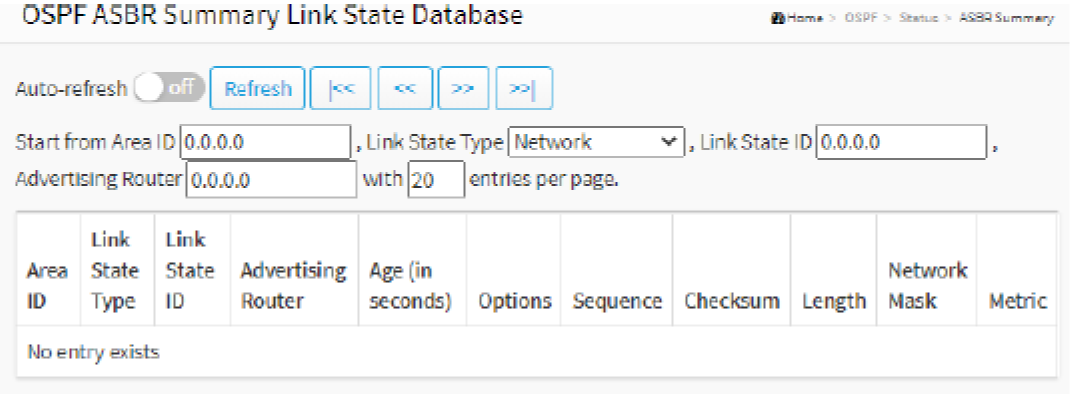
>>| : Updates the table entries, ending at the last available entry. If the last entry of the table is displayed, the button is disabled.

ASBR Summary

This page displays the OSPF LSA ASBR Summary link state database information table.

An Autonomous System Boundary Router (ASBR) is a router that is running multiple protocols and serves as a gateway to routers outside the OSPF domain and to those operating with different protocols. The ASBR can import and translate different protocol routes into OSPF through a process known as ‘redistribution’.

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



OSPF ASBR Summary Link State Database

Start from Area ID 0.0.0.0 , Link State Type Network , Link State ID 0.0.0.0 , Advertising Router 0.0.0.0 with 20 entries per page.

Area ID	Link State Type	Link State ID	Advertising Router	Age (in seconds)	Options	Sequence	Checksum	Length	Network Mask	Metric
No entry exists										

Figure 20-2.10: OSPF Summary Link State Database

Entry fields :

Start from Area ID : Input field lets you change the starting point in this table. The default is 0.0.0.0. Enter the OSPF area ID of the link state advertisement. It is not required for external LSA.

Link State Type : At the dropdown select the type of the link state advertisement (e.g., Router, Network, Summary, Summary ASBR).

Network : Use Network type of link state advertisement (default).

Router : Use Router type of link state advertisement.

Summary : Use Summary type of link state advertisement.

Summary ASBR : Use Summary type of link state advertisement.

Link State ID : Enter the OSPF link state IP. It identifies the piece of the routing domain that is being described by the LSA.

Advertising Router : Enter the advertising router ID which originated the LSA. The default is 0.0.0.0.

Table parameters :

Area ID : The OSPF area ID of the link state advertisement

Link State Type : The type of the link state advertisement.

Link State ID : The OSPF link state ID. It identifies the piece of the routing domain that is being described by the LSA.

Advertising Router : The advertising router ID which originated the LSA.

Age : The time in seconds since the LSA was originated.

Options : The OSPF option field, which is present in OSPF Hello packets, which enables OSPF routers to support (or not support) optional capabilities, and to communicate their capability level to other OSPF routers.

Sequence : The LS sequence number of the LSA.

Checksum : The checksum of the LSA contents.

Length : The Length in bytes of the LSA.

Network Mask : Network mask length. The field is significant only when the Link State Type is 'Summary/ASBR Summary Link State' (Type 3, 4).

Metric : User specified metric for this summary route. The field is significant only when the Link State Type is 'Summary/ASBR Summary Link State' (Type 3, 4).

Buttons

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

Refresh : Click to refresh the page immediately.

|<< : Updates the table entries, starting from the first available entry. If the first entry of the table is displayed, the button is disabled

<< : Updates the table entries, ending at the entry prior to the first entry currently displayed. If the first entry of the table is displayed, the button is disabled

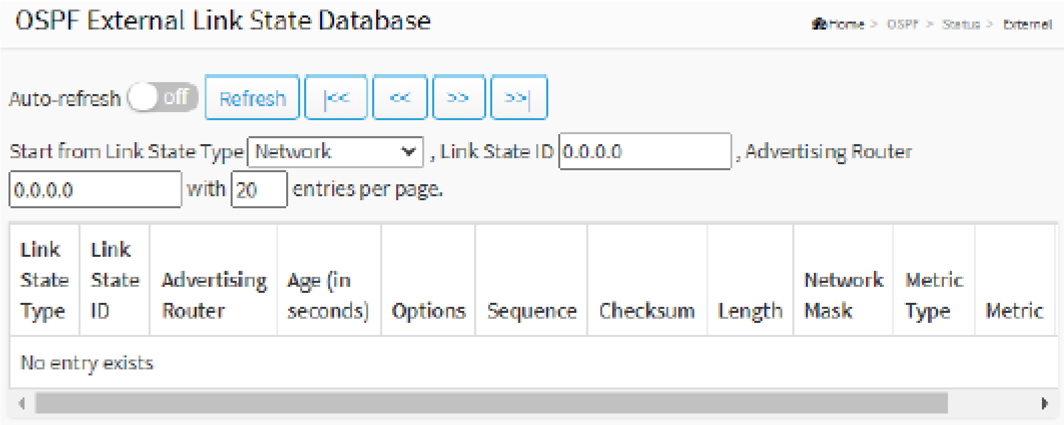
>> : Updates the table entries, starting from the entry next to the last entry currently displayed. If the last entry of the table is displayed, the button is disabled.

>>| : Updates the table entries, ending at the last available entry. If the last entry of the table is displayed, the button is disabled.

External

This page displays the OSPF LSA External link state database information table.

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



OSPF External Link State Database
Home > OSPF > Status > External
Auto-refresh
off
Refresh
|<<
<<
>>
>>|

Start from Link State Type Network, Link State ID 0.0.0.0, Advertising Router 0.0.0.0 with 20 entries per page.

Link State Type	Link State ID	Advertising Router	Age (in seconds)	Options	Sequence	Checksum	Length	Network Mask	Metric Type	Metric
No entry exists										

Figure 20-2.10: OSPF Summary Link State Database

<u>**Entry fields**</u> :

Start from Link State Type : At the dropdown select the type of the link state advertisement (e.g., Router, Network, Summary, Summary ASBR).

> ***Network*** : Use Network type of link state advertisement (default).
>
> ***Router*** : Use Router type of link state advertisement.
>
> ***Summary*** : Use Summary type of link state advertisement.
>
> ***Summary ASBR*** : Use Summary type of link state advertisement.

Link State ID : Enter the OSPF link state ID. It identifies the piece of the routing domain that is being described by the LSA.

Advertising Router : Enter the advertising router IP address which originated the LSA. The default is 0.0.0.0.

<u>**Table Parameters**</u> **:**

Link State Type : The type of the link state advertisement.

Link State ID : The OSPF link state ID. It identifies the piece of the routing domain that is being described by the LSA.

Advertising Router : The advertising router ID which originated the LSA.

Age (in seconds) : The time in seconds since the LSA was originated.

Options : The OSPF option field, which is present in OSPF hello packets, which enables OSPF routers to support (or not support) optional capabilities, and to communicate their capability level to other OSPF routers.

Sequence : The LS sequence number of the LSA.

Checksum : The checksum of the LSA contents.

Length : The Length in bytes of the LSA.

Network Mask : Network mask length. The field is significant only when the Link State Type is 'External/NSSA External Link State' (Type 5, 7).

Metric Type : The External type of the LSA. The field is significant only when the Link State Type is 'External/NSSA External Link State' (Type 5, 7).

Metric : User specified metric for this summary route. The field is significant only when the Link State Type is 'External/NSSA External Link State' (Type 5, 7).

Forward Address : The IP address of forward address. The field is significant only when the Link State Type is 'External/NSSA External Link State' (Type 5, 7).

Buttons

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

Refresh : Click to refresh the page immediately.

|<< : Updates the table entries, starting from the first available entry. If the first entry of the table is displayed, the button is disabled

<< : Updates the table entries, ending at the entry prior to the first entry currently displayed. If the first entry of the table is displayed, the button is disabled

>> : Updates the table entries, starting from the entry next to the last entry currently displayed. If the last entry of the table is displayed, the button is disabled.

>>| : Updates the table entries, ending at the last available entry. If the last entry of the table is displayed, the button is disabled.

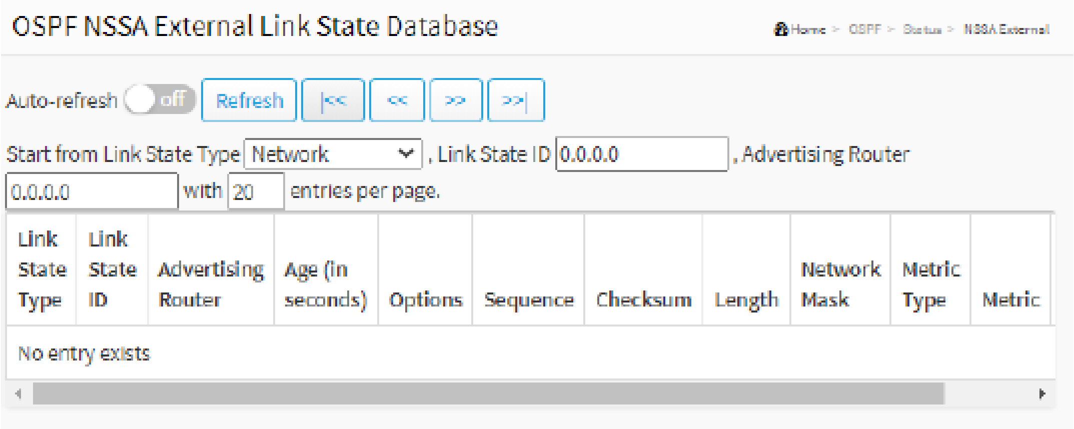
NSSA External

This page displays the OSPF LSA NSSA External link state database information table. An NSSA (not-so-stubby area) has the capability of importing external routes in a limited fashion.

Proper operation of the OSPF protocol requires that all OSPF routers maintain an identical copy of the OSPF link state database. But when the LDSB size becomes too large, some routers may not be able to keep the entire database due to resource shortages. This is called "database overflow". When this is anticipated, routers with limited resources can be accommodated by configuring OSPF stub areas and NSSAs.

See IETF RFC 3101 for more information.

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



OSPF NSSA External Link State Database

Start from Link State Type Network , Link State ID 0.0.0.0 , Advertising Router 0.0.0.0 with 20 entries per page.

Link State Type	Link State ID	Advertising Router	Age (in seconds)	Options	Sequence	Checksum	Length	Network Mask	Metric Type	Metric
No entry exists										

Figure 20-2.12: OSPF NSSA External Link State Database

<u>**Entry fields**</u> :

Start from Link State Type : At the dropdown select the type of the link state advertisement (e.g., Router, Network, Summary, Summary ASBR).

> ***Network*** : Use Network type of link state advertisement (default).
>
> ***Router*** : Use Router type of link state advertisement.
>
> ***Summary*** : Use Summary type of link state advertisement.
>
> ***Summary ASBR*** : Use Summary type of link state advertisement.

Link State ID : Enter the OSPF link state IP address. It identifies the piece of the routing domain that is being described by the LSA. The default is 0.0.0.0.

Advertising Router : Enter the advertising router ID which originated the LSA. The default is 0.0.0.0.

Table parameters :

Link State Type : The type of the link state advertisement.

Link State ID : The OSPF link state ID identifies the piece of the routing domain being described by the LSA.

Advertising Router : The advertising router ID which originated the LSA.

Age (in seconds) : The time in seconds since the LSA was originated.

Options : The OSPF option field, present in OSPF hello packets, enables OSPF routers to support (or not support) optional capabilities, and to communicate their capability level to other OSPF routers.

Sequence : The LS sequence number of the LSA.

Checksum : The checksum of the LSA contents.

Length : The Length in bytes of the LSA.

Network Mask : Network mask length. The field is significant only when the Link State Type is 'External/NSSA External Link State' (Type 5, 7).

Metric Type : The External type of the LSA. The field is significant only when the Link State Type is 'External/NSSA External Link State' (Type 5, 7).

Metric : User specified metric for this summary route. The field is significant only when the Link State Type is 'External/NSSA External Link State' (Type 5, 7).

ForwardAddress : The IP address of forward address. The field is significant only when the Link State Type is 'External/NSSA External Link State' (Type 5, 7).

Buttons

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

Refresh : Click to refresh the page immediately.

|<< : Updates the table entries, starting from the first available entry. If the first entry of the table is displayed, the button is disabled

<< : Updates the table entries, ending at the entry prior to the first entry currently displayed. If the first entry of the table is displayed, the button is disabled

>> : Updates the table entries, starting from the entry next to the last entry currently displayed. If the last entry of the table is displayed, the button is disabled.

>>| : Updates the table entries, ending at the last available entry. If the last entry of the table is displayed, the button is disabled.

Troubleshooting OSPF

1. Verify there is no mismatch in the hello parameters or in the dead timer.
2. Verify that the link is up. Ping the other end of the link.
3. Make sure that the interfaces at both ends are configured to support OSPF.
4. Check for a mismatch in the OSPF Network Type.
5. Verify that Hello and Dead timers match on each end of the link
6. Verify that Neighboring interfaces are in the same OSPF Area.
7. If the device is in more than one area, then it must have at least one interface in Area 0.
8. OSPF Area IDs: When using multiple network area statements in the OSPF configuration, the order of the statements is critical. Check that the networks have been assigned the desired area IDs by checking the output of the `show ip ospf interface` command.
9. OSPF Does Not Start: The OSPF process cannot start on a router if a router ID cannot be established. Check the output of `show ip ospf` to see if a router ID has been established. If a router ID has not been established, check to see if the router has an active interface (preferably a loopback interface) with an IP address.
10. Verify Neighbor relationships: Once a router is able to start OSPF, it establishes an interface data structure for each interface configured to run OSPF. Check the output of `show ip ospf interface` to ensure that OSPF is active on the intended interfaces. If OSPF is active, check for an incorrectly configured interface.
11. Check if there is an entry in the OSPF Database for a particular external route, but it is not showing in the routing table. Check the Forwarding Address associated with the route.

22. OSPF6

OSPF for IPv6 is described in IETF RFC 2740. The fundamental mechanisms of OSPF (flooding, DR election, area support, SPF calculations, etc.) remain unchanged. However, some changes have been necessary, either due to changes in protocol semantics between IPv4 and IPv6, or simply to handle the increased address size of IPv6.

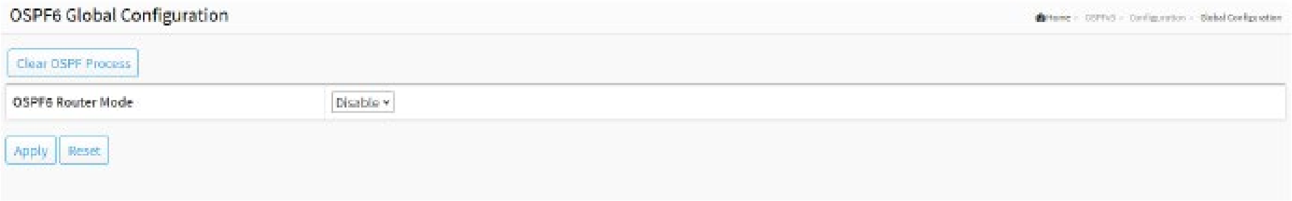
All of OSPF for IPv4's optional capabilities, including on-demand circuit support, NSSA areas, and the multicast extensions to OSPF are also supported in OSPF for IPv6. OSPF for IPv6 runs per-link instead of the IPv4 behavior of per-IP-subnet.

Configuration

Global Configuration

This page displays the OSPF6 Global Configuration table. It is a general group to configure the OSPF6 common router parameters.

OSPFv3 is the Open Shortest Path First routing protocol for IPv6. It is similar to OSPFv2 in its concept of a link state database, intra- and inter-area, and AS external routes and virtual links.



OSPF6 Global Configuration

OSPF6 Router Mode	Disable

Figure 21-1: OSPF6 Global Configuration

Parameter descriptions:

OSPF6 Router Mode : Enable or Disable the OSPF6 router mode.

Router ID : The OSPF6 Router ID in IPv4 address format (A.B.C.D). When the router's OSPF6 Router ID is changed, if there is one or more fully adjacent neighbors in the current OSPF6 area, the new router ID will take effect after restart OSPF6 process. **Note** that the router ID should be unique in the Autonomous System and that the value '0.0.0.0' is invalid since it is reserved for the default algorithm.

Auto: The default algorithm will choose the largest IP address assigned to the router.

Specific: User specified router ID. The valid range is from 0.0.0.1 to 255.255.255.254.

Static Redistribute : Whether the OSPF redistribute function is enabled for the static routes. Static routes are manually-defined (remote) routes.

Enable: The static routes are redistributed.

Disable: The static routes are not redistributed

Connected Redistribute : The OSPF redistribute enabled for connected route or not. Connected = RIP routes that correspond to defined IP interfaces on which RIP is not enabled (defined locally). By default, the RIP Routing Table only includes routes that correspond to IP interfaces on which RIP is enabled.

Enable: The connected interfaces are redistributed.

Disable: The connected interfaces are not redistributed (the default setting).

Administrative Distance : The OSPF6 administrative distance in hops.

Buttons

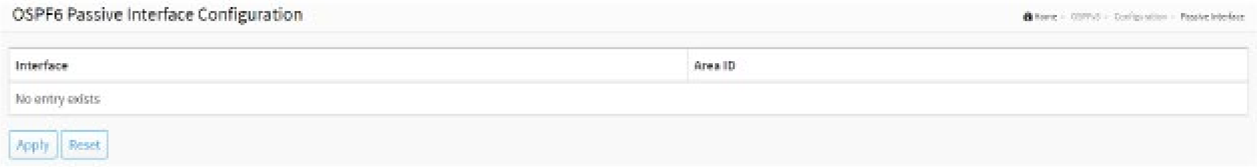
Clear OSPF Process : Click to reset the current OSPF6 process.

Apply : Click to save changes.

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

Passive Interface

This displays the OSPF6 passive interface configuration table. When enabled, this tells OSPF not to send hello packets on certain interfaces.



OSPF6 Passive Interface Configuration

Interface	Area ID
No entry exists	

Figure 21-1.2: OSPF6 Passive Interface Configuration

Parameter descriptions:

Interface : Interface identification.

Area ID : The OSPF6 interface Area ID. Only valid if Router ID *'is_specific_id'* is true.

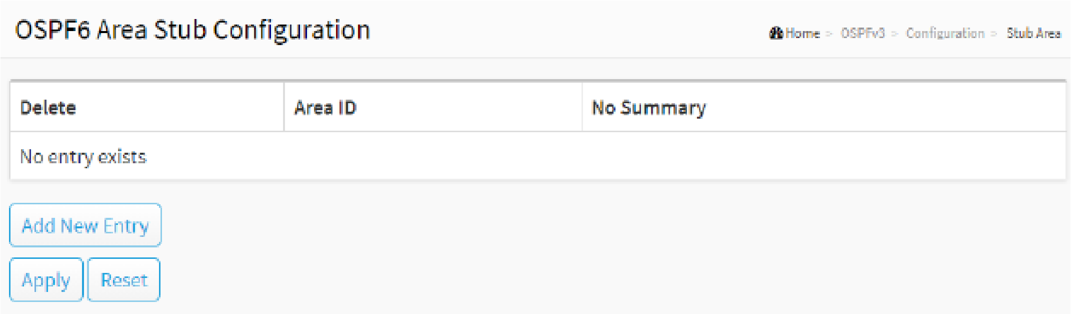
Buttons

Apply : Click to save changes.

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

Stub Area

This page displays the OSPF6 area stub configuration table. The configuration is used to reduce the link-state database size and therefore reduce memory and CPU requirement by forbidding some LSAs.



OSPF6 Area Stub Configuration

Delete	Area ID	No Summary
No entry exists		

Figure 21-1.3: OSPF6 Area Stub Configuration

Parameter descriptions:

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

Area ID : The OSPF6 area ID.

No Summary : The value is true to configure the inter-area routes to not inject into this stub area.

Buttons

Add New Entry : Click to add a new entry to the table.

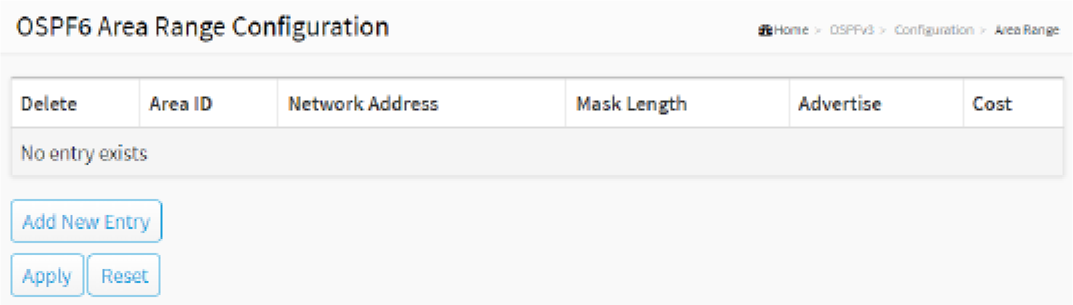
Apply : Click to save changes.

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

Area Range

This page displays the OSPF6 area range configuration table. It is used to summarize the intra area paths from a specific address range in one summary-LSA(Type-0x2003) and advertised to other areas or configure the address range status as '*DoNotAdvertise*' which the summary-LSA (Type-0x2003) is suppressed. The area range configuration is used for Area Border Routers (ABRs) and only router-LSAs (Type-0x2001) and network-LSAs (Type-0x2002) can be summarized.

AS-external-LSAs (Type-0x4005) cannot be summarized because the scope is OSPF6 autonomous system (AS). AS-external-LSAs (Type-0x4007) cannot be summarized because the feature is not supported yet.



OSPF6 Area Range Configuration

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

Figure 21-1.4: OSPF6 Area Range Configuration

Parameter descriptions:

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

Area ID : The OSPF6 area ID.

Network Address : IPv6 network address.

Mask Length : IPv6 network mask length.

Advertise : When the value is true, it summarizes intra-area paths from the address range in one Inter-Area Prefix LSA (Type-0x2003) and advertised to other areas. Otherwise, the intra-area paths from the address range are not advertised to other areas.

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

Cost : User-specified cost (or metric) for this summary route. It can be configured only when 'Specific' is selected. The valid range is 0 to 16777215 and the default setting is 'Auto cost' mode.

Buttons

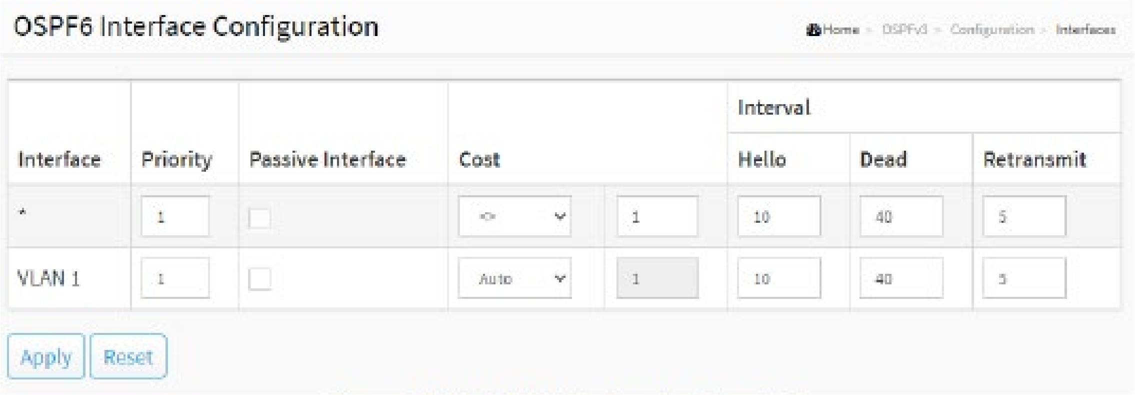
Add New Entry : Click to add a new entry to the table.

Apply : Click to save changes.

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

Interfaces

This page displays the interface configuration parameter table.



OSPF6 Interface Configuration

Interface	Priority	Passive Interface	Cost		Interval		
					Hello	Dead	Retransmit
*	1	□	<>	1	10	40	5
VLAN 1	1	□	Auto	1	10	40	5

Figure 21-1.5: OSPF6 Interface Configuration

Parameter descriptions:

Interface : Interface identification.

Priority : User-specified router priority for the interface. The valid range is 0 - 255 and the default is 1.

Passive Interface : Check the box to indicate that the interface is passive.

Cost : User-specified cost for this interface. It's link state metric for the interface. The field is significant only when '*IsSpecificCos*t' is TRUE. The valid range is 1 - 65535 and the default setting is 'Auto' cost mode.

Hello Interval : The number of Hello packets to be sent per second. The valid range is 1 - 65535 and the default value is 10 per second.

OSPF uses Hello packets and two timers to check if a neighbor is still alive:

Hello Interval defines how often the hello packet is sent.

Dead Interval defines how long to wait for hello packets before declaring the neighbor dead.

The hello and dead interval values can be different based on the OSPF network type.

Dead Interval : The time interval (in seconds) between hello packets. The valid range is 1 - 65535 and the default value is 40 seconds.

Retransmit Interval : The time interval (in seconds) between link-state advertisement (LSA) retransmissions for adjacencies. The valid range is 3 - 65535 seconds and the default value is 5 seconds.

Buttons

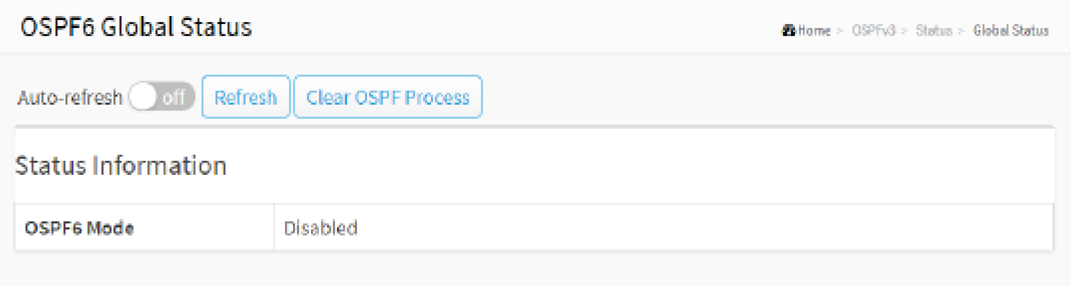
Apply : Click to save changes.

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

Status

Global Status

This page displays the OSPF6 router status table. It is used to provide the OSPF6 router status information. Navigate to the OSPF > Status > Global Status menu path to display the OSPF6 Global Status information.



OSPF6 Global Status

Status Information

OSPF6 Mode	Disabled

OSPF6 Global Status

Parameter descriptions:

Router ID : The OSPF6 router ID.

SPF Delay : The Delay time (in seconds) of SPF calculations.

SPF Hold Time : The Minimum hold time (in milliseconds) between consecutive SPF calculations.

SPF Max. Wait Time : The Maximum wait time (in milliseconds) between consecutive SPF calculations.

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

Attached Area Count : Number of areas attached for the router.

Buttons

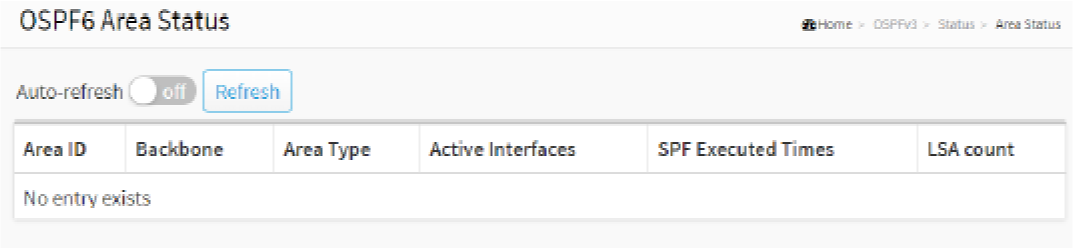
Clear OSPF~~6~~ Process : Click to reset the current OSPF6 process.

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

Refresh : Click to refresh the page immediately.

Area Status

This page displays the OSPF6 network area status table, which provides OSPF6 network area status information. Navigate to the ...



OSPF6 Area Status

Area ID	Backbone	Area Type	Active Interfaces	SPF Executed Times	LSA count
No entry exists					

Figure 21-2.2: OSPF6 Area Status

Area ID : The OSPF6 Area ID.

Backbone : Indicate if this area is a backbone area or not.

Area Type : The OSPF6 area type. There are five types of OSPF areas: Backbone area (area 0), Standard area, Stub area, Totally stubby area, and Not so stubby area (NSSA).

Active Interfaces : Number of active interfaces attached in the area.

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

LSA Count : The total number of LSAs for the particular area.

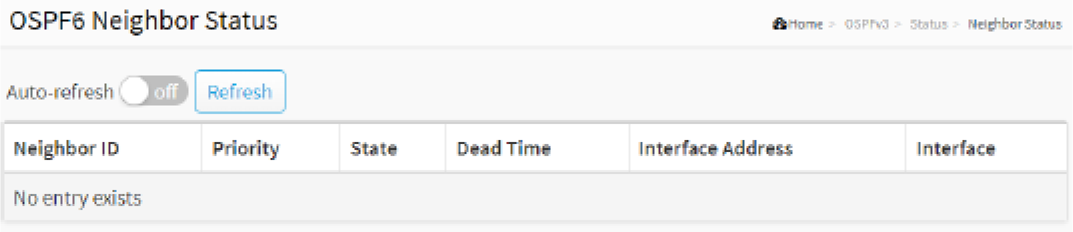
Buttons

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

Refresh : Click to refresh the page immediately.

Neighbor Status

This page displays the OSPF6 IPv6 neighbor status table.



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

Figure 21-2.3: OSPF6 Neighbor Status

Neighbor ID : The Neighbor ID.

Priority : The priority of OSPF6 neighbor. It indicates the priority of the neighbor router. This item is used when selecting the DR for the network. The router with the highest priority becomes the DR.

State : The state of OSPF6 neighbor. It indicates the functional state of the neighbor router.

Dead Time : The Dead timer indicates the amount of time remaining that the router waits to receive an OSPF6 hello packet from the neighbor before declaring the neighbor down.

Interface Address : The IP address.

Interface : The network interface.

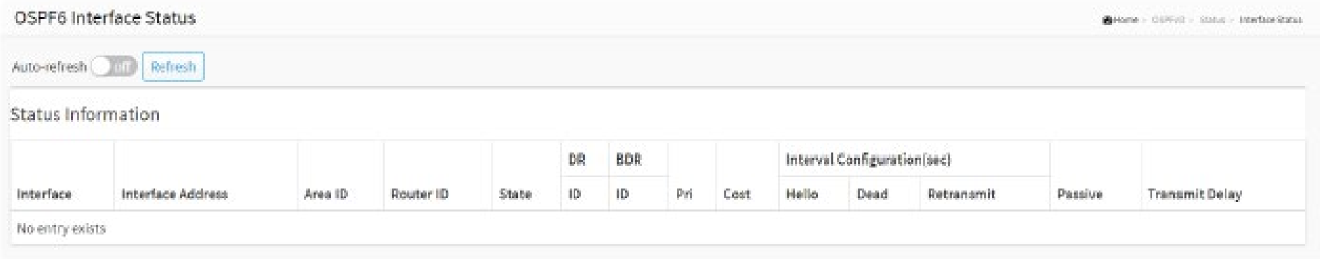
Buttons

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

Refresh : Click to refresh the page immediately.

Interface Status

This page displays the OSPF6 interface status table. It is used to provide the OSPF6 interface status information.



OSPF6 Interface Status

Status Information

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

Figure 21-2.4: OSPF6 Interface Status

Parameter Descriptions:

Interface : The Interface identification.

Interface Address : The IPv6 network address.

Area ID : The OSPF6 area ID.

Router ID : The OSPF6 router ID.

State : The state of the link.

DR ID : The router ID of the DR (Designated Router). Each broadcast and NBMA network that has at least two attached routers has a DR. The DR generates an LSA for the network and has other special responsibilities in the running of the protocol. The DR is elected by the Hello Protocol.

> If two or more routers are connected on a broadcast network and are configured for OSPF, they must select a **DR** (Designated Router) and a **BDR** (Backup Designated Router). All routers in the broadcast network must form an OSPF adjacency with all other routers. The goal of DR and BDR is to reduce the complexity of the multi-access network from a link state database point-of-view. The DR/BDR act as central points of exchanging link-state information instead of having to exchange info with all other routers in the broadcast network (mesh). This reduces greatly the link-state database of routers.
>
> Two factors influence DR/BDR election: **1)** Router ID: The Router ID is the highest IP address of the device or the highest IP address among loopback addresses (if one is configured) on the Cisco router or can be configured manually by “router-id a.b.c.d” command under the OSPF process. **2)** OSPF Priority: This is by default 1 for all routers. The OSPF priority is configured per interface. The router with the Highest OSPF Priority value will become the DR. If the priorities are the same (the default priority is 1 for all routers), then the Router ID is the tie breaker. The router with the highest Router ID becomes the **DR**, and the router with the next highest IP becomes the **BDR**.

BDR ID : The router ID of the BDR (Backup Designated Router) as described above.

Pri : The OSPF6 priority. It helps determine the DR and BDR on the network to which this interface is connected.

Cost : The cost of the interface.

Hello : Hello timer. A time interval that a router sends an OSPF6 hello packet.

Dead : Dead timer. A time interval to wait before declaring a neighbor dead. The unit of measure is seconds.

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

Passive : Indicates if the interface is passive interface.

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

Buttons:

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

Refresh : Click to refresh the page immediately.

Routing Status

This page displays the OSPF6 routing status table. Each page shows up to 999 table entries, selected with the "entries per page" input field. When first visited, the web page shows the beginning entries of this table.

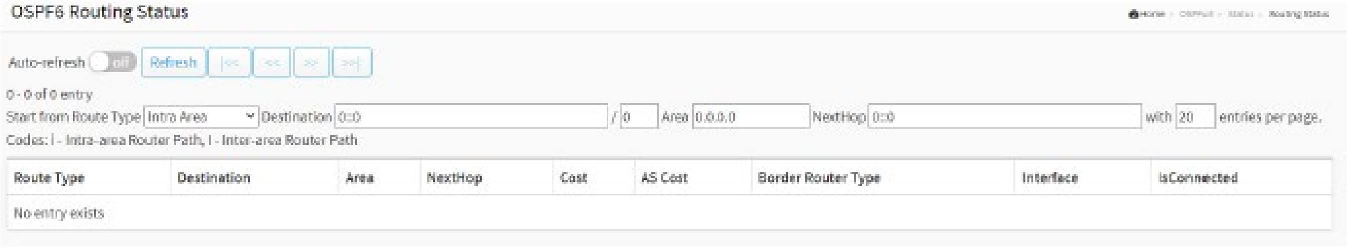
The "Start from Route Type" input field lets you change the starting point in this table.

At the “Destination” input field enter the IPv6 address of the destination.

At the “Area” input field enter the area IP area address.

At the “NextHop” input field enter the IPv6 address of the next hop.

Codes: **i** – Intra-area Router Path, **I** - Inter-area Router Path



OSPF6 Routing Status

0 - 0 of 0 entry

Start from Route Type Intra Area Destination 0::0 / 0 Area 0.0.0.0 NextHop 0::0 with 20 entries per page.

Codes: I - Intra-area Router Path, I - Inter-area Router Path

Route Type	Destination	Area	NextHop	Cost	AS Cost	Border Router Type	Interface	IsConnected
No entry exists								

OSPF6 Routing Status

Parameter descriptions:

Route Type : At the dropdown select the OSPF6 route type:

Intra Area : The destination is an OSPF6 route which is located on intra-area (default).

Inter Area : The destination is an OSPF6 route which is located on inter-area.

Border Router : The destination is a border router.

External Type-1 : The destination is an external Type-1 route.

External Type-2 : The destination is an external Type-2 route.

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

Area : Indicates which area the route or router can be reached via/to.

NextHop : An Ipv6 address represented as human readable test as specified in IETF RFC 5952.

Cost : The cost of the route.

AS Cost : The cost of the route within the OSPF6 network. It is valid for External Type-2 routes and is always '0' for other route types.

Border Router Type : The border router type of the OSPF6 route entry.

i-ABR : The border router is an ABR.

i-ASBR : The border router is an ASBR located on Intra-area.

I-ASBR : The border router is an ASBR located on Inter-area.

i-ABR/ASBR : The border router is an ASBR attached to at least 2 areas.

Interface : The interface where the IP packet is outgoing.

IsConnected : The destination is connected directly or not.

Buttons

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

Refresh : Click to manually refresh the page immediately.

|<< : Updates the table entries, starting from the first available entry. If the first entry of the table is displayed, the button is disabled.

<< : Updates the table entries, ending at the entry prior to the first entry currently displayed. If the first entry of the table is displayed, the button is disabled

>> : Updates the table entries, starting from the entry next to the last entry currently displayed. If the last entry of the table is displayed, the button is disabled.

>>| : Updates the table entries, ending at the last available entry. If the last entry of the table is displayed, the button is disabled.

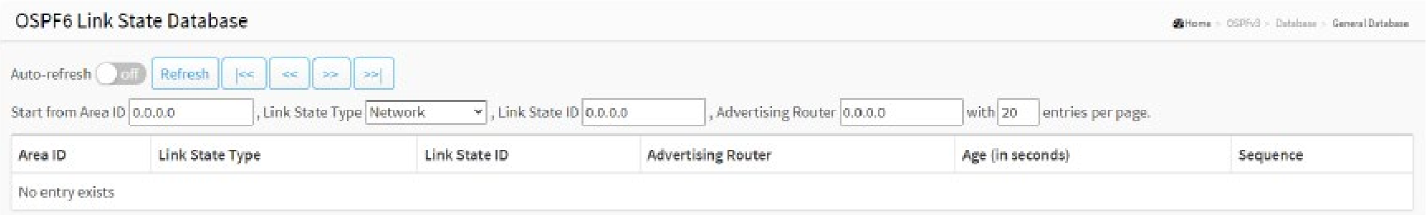
Database

General Database

This page displays the OSPF6 LSA link state database information table. Navigate to the OSPFv3 > Database > General Database menu path to display the OSPF6 Link State Database page. Enter parameters for the Start from Area ID, Link State Type, Link State ID, Advertising Router, and entries per page fields.

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

The "Start from entry keys" input field lets you change the starting point in this table. Clicking the Refresh button will update the displayed table starting from that or the closest next entry match. In addition, these input fields will, upon a Refresh button click, assume the value of the first displayed entry, allowing for continuous refresh with the same start input field.


OSPF6 Link State Database

Start from Area ID 0.0.0.0 , Link State Type Network , Link State ID 0.0.0.0 , Advertising Router 0.0.0.0 with 20 entries per page.

Area ID	Link State Type	Link State ID	Advertising Router	Age (in seconds)	Sequence
No entry exists					

Figure 21-3.1: OSPF6 Link State Database

Area ID : The OSPF6 area ID of the link state advertisement. It is not required for external LSA.

Link State Type : The type of the link state advertisement.

Link State ID : The OSPF6 link state ID. It identifies the piece of the routing domain that is being described by the LSA.

Advertising Router : The advertising router ID which originated the LSA.

Age (in seconds) : The time in seconds since the LSA was originated.

Sequence : The LS sequence number of the LSA.

Buttons

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

Refresh : Click to manually refresh the page immediately.

|<< : Updates the table entries, starting from the first available entry. If the first entry of the table is displayed, the button is disabled.

<< : Updates the table entries, ending at the entry prior to the first entry currently displayed. If the first entry of the table is displayed, the button is disabled

>> : Updates the table entries, starting from the entry next to the last entry currently displayed. If the last entry of the table is displayed, the button is disabled.

>>| : Updates the table entries, ending at the last available entry. If the last entry of the table is displayed, the button is disabled.

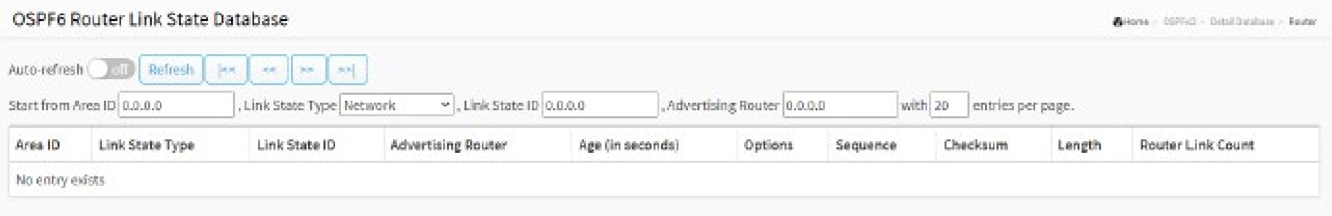
Detail Database

Router

This page displays the OSPF6 LSA Router link state database information table. Navigate to the OSPFv3 > Detail Database > Router menu path to display the OSPF6 Router Link State Database page.

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

Enter parameters for the Start from Area ID, Link State Type, Link State ID, Advertising Router, and entries per page fields.



OSPF6 Router Link State Database

Start from Area ID 0.0.0.0 , Link State Type Network , Link State ID 0.0.0.0 , Advertising Router 0.0.0.0 with 20 entries per page.

Area ID	Link State Type	Link State ID	Advertising Router	Age (in seconds)	Options	Sequence	Checksum	Length	Router Link Count
No entry exists									

Figure 21-4.1: OSPF6 Router Link State Database

Parameter descriptions:

Area ID : The OSPF6 area ID of the link state advertisement

Link State Type : The type of the link state advertisement (Router, Network, Summary, or Summary ASBR).

Link State ID : The OSPF6 link state ID. It identifies the piece of the routing domain that is being described by the LSA.

Advertising Router : The advertising router ID which originated the LSA.

Age (in seconds) : The time in seconds since the LSA was originated.

Options : The OSPF6 options field, present in OSPF6 hello packets, which enables OSPF6 routers to support (or not support) optional capabilities, and to communicate their capability level to other OSPF6 routers.

Sequence : The LS sequence number of the LSA.

Checksum : The checksum of the LSA contents.

Length : The Length in bytes of the LSA.

Router Link Count : The link count of the LSA. The field is significant only when the Link State Type is 'Router Link State' (Type 1).

Buttons

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

Refresh : Click to manually refresh the page immediately.

|<< : Updates the table entries, starting from the first available entry. If the first entry of the table is displayed, the button is disabled.

<< : Updates the table entries, ending at the entry prior to the first entry currently displayed. If the first entry of the table is displayed, the button is disabled

>> : Updates the table entries, starting from the entry next to the last entry currently displayed. If the last entry of the table is displayed, the button is disabled.

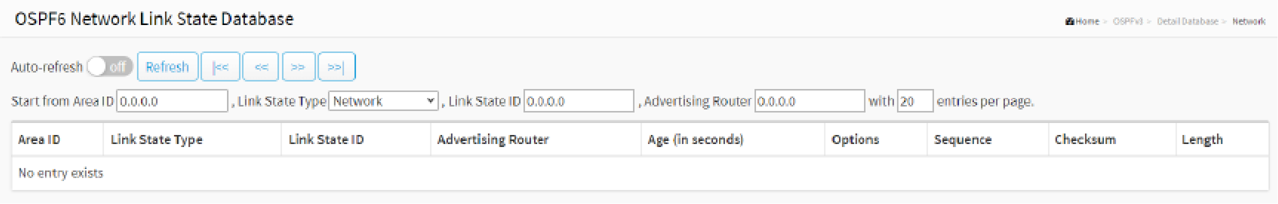
>>| : Updates the table entries, ending at the last available entry. If the last entry of the table is displayed, the button is disabled.

Network

Navigate to the OSPFv3 > Detail Database > Network menu path to display the OSPF6 Network Link State Database page. This page displays the OSPF6 LSA Network link state database information table.

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

Enter parameters for the Start from Area ID, Link State Type, Link State ID, Advertising Router, and entries per page fields.



OSPF6 Network Link State Database

Start from Area ID 0.0.0.0 , Link State Type Network , Link State ID 0.0.0.0 , Advertising Router 0.0.0.0 with 20 entries per page.

Area ID	Link State Type	Link State ID	Advertising Router	Age (in seconds)	Options	Sequence	Checksum	Length
No entry exists								

Figure 21-4.2: OSPF6 Network Link State Database

Area ID : The OSPF6 area ID of the link state advertisement

Link State Type : The type of the link state advertisement.

Link State ID : The OSPF6 link state ID. It identifies the piece of the routing domain being described by the LSA.

Advertising Router : The advertising router ID which originated the LSA.

Age : The time in seconds since the LSA was originated.

Options : The OSPF6 option field, which is present in OSPF6 hello packets, which enables OSPF6 routers to support (or not support) optional capabilities, and to communicate their capability level to other OSPF6 routers.

Sequence : The LS sequence number of the LSA.

Checksum : The checksum of the LSA contents.

Length : The Length in bytes of the LSA.

Buttons

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

Refresh : Click to manually refresh the page immediately.

|<< : Updates the table entries, starting from the first available entry. If the first entry of the table is displayed, the button is disabled.

<< : Updates the table entries, ending at the entry prior to the first entry currently displayed. If the first entry of the table is displayed, the button is disabled

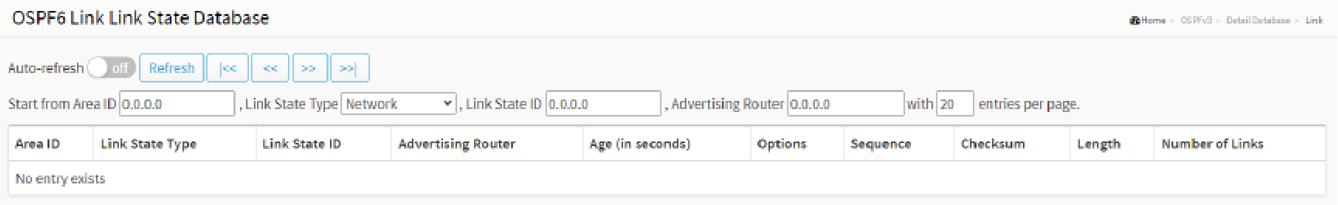
>> : Updates the table entries, starting from the entry next to the last entry currently displayed. If the last entry of the table is displayed, the button is disabled.

>>| : Updates the table entries, ending at the last available entry. If the last entry of the table is displayed, the button is disabled.

Link

This page displays the Link State database information table from OSPFv3 > Detail Database > Link menu path.

Enter parameters for the Start from Area ID, Link State Type, Link State ID, Advertising Router, and entries per page fields.



OSPF6 Link Link State Database

Start from Area ID 0.0.0.0 , Link State Type Network , Link State ID 0.0.0.0 , Advertising Router 0.0.0.0 with 20 entries per page.

Area ID	Link State Type	Link State ID	Advertising Router	Age (in seconds)	Options	Sequence	Checksum	Length	Number of Links
No entry exists									

Figure 21-4.3: OSPF6 Link State Database

Parameter descriptions:

Area ID : The OSPF6 area ID of the link state advertisement

Link State Type : The type of the link state advertisement.

Link State ID : The OSPF6 link state ID. It identifies the piece of the routing domain that is being described by the LSA.

Advertising Router : The advertising router ID which originated the LSA.

Age : The time in seconds since the LSA was originated.

Options : The OSPF6 option field, which is present in OSPF6 hello packets, which enables OSPF6 routers to support (or not support) optional capabilities, and to communicate their capability level to other OSPF6 routers.

Sequence : The LS sequence number of the LSA.

Checksum : The checksum of the LSA contents.

Length : The Length in bytes of the LSA.

Number of Links : The count of the LSA.

Buttons

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

Refresh : Click to refresh the page immediately.

|<< : Updates the table entries, starting from the first available entry. If the first entry of the table is displayed, the button is disabled.

<< : Updates the table entries, ending at the entry prior to the first entry currently displayed. If the first entry of the table is displayed, the button is disabled

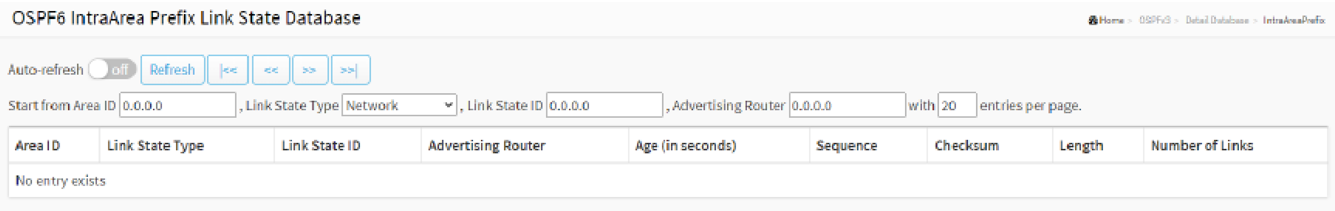
>> : Updates the table entries, starting from the entry next to the last entry currently displayed. If the last entry of the table is displayed, the button is disabled.

>>| : Updates the table entries, ending at the last available entry. If the last entry of the table is displayed, the button is disabled.

IntraArea Prefix

Navigate to the OSPFv3 > Detail Database > IntraAreaPrefix menu path to display the OSPF6 IntraArea Prefix Link State Database table.

Enter parameters for the Start from Area ID, Link State Type, Link State ID, and Advertising Router.



OSPF6 IntraArea Prefix Link State Database

Start from Area ID 0.0.0.0 , Link State Type Network , Link State ID 0.0.0.0 , Advertising Router 0.0.0.0 with 20 entries per page.

Area ID	Link State Type	Link State ID	Advertising Router	Age (in seconds)	Sequence	Checksum	Length	Number of Links
No entry exists								

Figure 21-4.4: OSPF6 IntraArea Prefix Link State Database

Area ID : The OSPF6 area ID of the link state advertisement

Link State Type : The type of the link state advertisement.

Link State ID : The OSPF6 link state ID. It identifies the piece of the routing domain that is being described by the LSA.

Advertising Router : The advertising router ID which originated the LSA.

Age (in seconds) : The time in seconds since the LSA was originated.

Sequence : The LS sequence number of the LSA.

Checksum : The checksum of the LSA contents.

Length : The Length in bytes of the LSA.

Number of Links : The count of the Prefixes.

Buttons

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

Refresh : Click to refresh the page immediately.

|<< : Updates the table entries, starting from the first available entry. If the first entry of the table is displayed, the button is disabled.

<< : Updates the table entries, ending at the entry prior to the first entry currently displayed. If the first entry of the table is displayed, the button is disabled

>> : Updates the table entries, starting from the entry next to the last entry currently displayed. If the last entry of the table is displayed, the button is disabled.

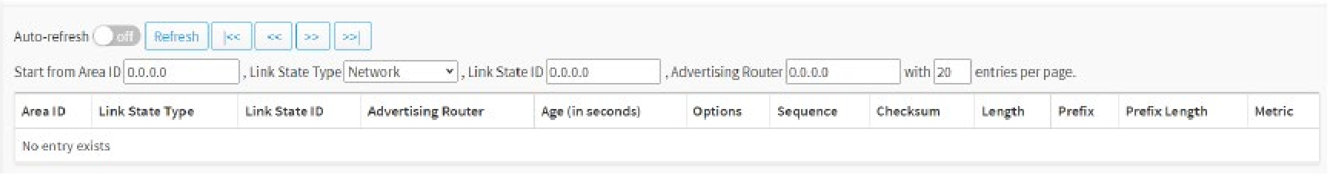
>>| : Updates the table entries, ending at the last available entry. If the last entry of the table is displayed, the button is disabled.

Summary

This page displays the OSPF6 LSA Summary link state database information table. Navigate to the OSPFv3 > Detail Database > OSPF6 Summary Link State Database menu path to display the OSPF6 Summary Link State Database.

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

Enter parameters for the Start from Area ID, Link State Type, Link State ID, and Advertising Router.



Start from Area ID 0.0.0.0 , Link State Type Network , Link State ID 0.0.0.0 , Advertising Router 0.0.0.0 with 20 entries per page.

Area ID	Link State Type	Link State ID	Advertising Router	Age (in seconds)	Options	Sequence	Checksum	Length	Prefix	Prefix Length	Metric
No entry exists											

Figure 21-4.5: OSPF6 Summary Link State Database

Area ID : The OSPF6 area ID of the link state advertisement.

Link State Type : The type of the link state advertisement.

Link State ID : The OSPF6 link state ID. It identifies the piece of the routing domain that is being described by the LSA.

Advertising Router : The advertising router ID which originated the LSA.

Age : The time in seconds since the LSA was originated.

Options : The OSPF6 option field, present in OSPF6 hello packets, enables OSPF6 routers to support (or not support) optional capabilities, and to communicate their capability level to other OSPF6 routers.

Sequence : The LS sequence number of the LSA.

Checksum : The checksum of the LSA contents.

Length : The Length in bytes of the LSA.

Prefix : IPv6 network address.

Prefix Length : IPv6 network mask length.

Metric : User specified metric for this summary route. The field is significant only when the Link State Type is 'Inter_Area Prefix/Router Link State' (Type 3, 4).

Buttons

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

Refresh : Click to refresh the page immediately.

|<< : Updates the table entries, starting from the first available entry. If the first entry of the table is displayed, the button is disabled.

<< : Updates the table entries, ending at the entry prior to the first entry currently displayed. If the first entry of the table is displayed, the button is disabled

>> : Updates the table entries, starting from the entry next to the last entry currently displayed. If the last entry of the table is displayed, the button is disabled.

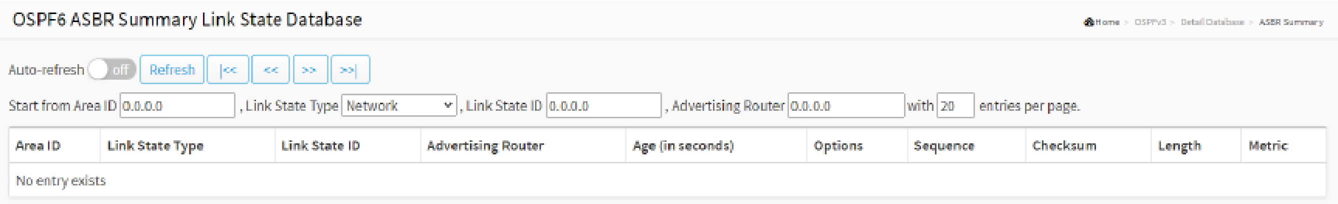
>>| : Updates the table entries, ending at the last available entry. If the last entry of the table is displayed, the button is disabled.

ASBR Summary

This page displays the OSPF6 LSA ASBR Summary link state database information table. Navigate to the OSPFv3 > Detail Database > OSPF6 Summary Link State Database menu path to display the OSPF6 ASBR Summary Link State Database.

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

Enter parameters for the Start from Area ID, Link State Type, Link State ID, and Advertising Router.



OSPF6 ASBR Summary Link State Database

Start from Area ID 0.0.0.0 , Link State Type Network , Link State ID 0.0.0.0 , Advertising Router 0.0.0.0 with 20 entries per page.

Area ID	Link State Type	Link State ID	Advertising Router	Age (in seconds)	Options	Sequence	Checksum	Length	Metric
No entry exists									

Figure 21-4.6: OSPF6 ASBR Summary Link State Database

Parameter descriptions:

Area ID : The OSPF6 area ID of the link state advertisement

Link State Type : The type of the link state advertisement.

Link State ID : The OSPF6 link state ID. It identifies the piece of the routing domain being described by the LSA.

Advertising Router : The advertising router ID which originated the LSA.

Age : The time in seconds since the LSA was originated.

Options : The OSPF6 option field which is present in OSPF6 hello packets, which enables OSPF6 routers to support (or not support) optional capabilities, and to communicate their capability level to other OSPF6 routers.

Sequence : The LS sequence number of the LSA.

Checksum : The checksum of the LSA contents.

Length : The Length in bytes of the LSA.

Metric : User-specified metric for this summary route. The field is significant only when the Link State Type is 'Summary/ASBR Summary Link State' (LSA Type 3, 4).

Buttons

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

Refresh : Click to refresh the page immediately.

|<< : Updates the table entries, starting from the first available entry. If the first entry of the table is displayed, the button is disabled.

<< : Updates the table entries, ending at the entry prior to the first entry currently displayed. If the first entry of the table is displayed, the button is disabled.

>> : Updates the table entries, starting from the entry next to the last entry currently displayed. If the last entry of the table is displayed, the button is disabled.

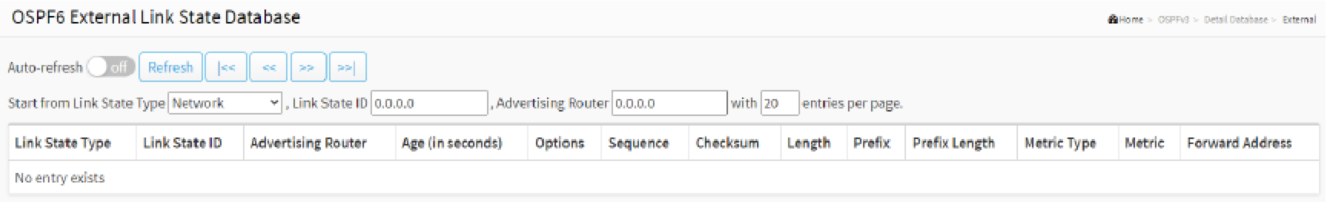
>>| : Updates the table entries, ending at the last available entry. If the last entry of the table is displayed, the button is disabled.

External

This page displays the OSPF6 LSA External link state database information table. Navigate to the OSPFv3 > Detail Database > OSPF6 External Link State Database menu path to display the OSPF6 External Link State Database.

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

Select the Start from Link State Type, Link State ID, and Advertising Router.


OSPF6 External Link State Database
Home > OSPFv3 > Detail Database > External
Auto-refresh
off
Refresh
|<<
<<
>>
>>|

Start from Link State Type Network , Link State ID 0.0.0.0 , Advertising Router 0.0.0.0 with 20 entries per page.

Link State Type	Link State ID	Advertising Router	Age (in seconds)	Options	Sequence	Checksum	Length	Prefix	Prefix Length	Metric Type	Metric	Forward Address
No entry exists												

Figure 21-4.7: OSPF6 External Link State Database

Parameter descriptions:

Link State Type : The type of the link state advertisement.

Link State ID : The OSPF6 link state ID. It identifies the piece of the routing domain that is being described by the LSA.

Advertising Router : The advertising router ID which originated the LSA.

Age : The time in seconds since the LSA was originated.

Options : The OSPF6 option field which is present in OSPF6 hello packets, which enables OSPF6 routers to support (or not support) optional capabilities, and to communicate their capability level to other OSPF6 routers.

Sequence : The LS sequence number of the LSA.

Checksum : The checksum of the LSA contents.

Length : The Length in bytes of the LSA.

Prefix : IPv6 network address.

Prefix Length : IPv6 network mask length.

MetricType : The External type of the LSA. The field is significant only when the Link State Type is 'External/NSSA External Link State' (LSA Type 5, 7).

Metric : User specified metric for this summary route. The field is significant only when the Link State Type is 'External/NSSA External Link State' (LSA Type 5, 7).

ForwardAddress : The IP address of forward address. The field is significant only when the Link State Type is 'External/NSSA External Link State' (LSA Type 5, 7).

Buttons

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

Refresh : Click to refresh the page immediately.

|<< : Updates the table entries, starting from the first available entry. If the first entry of the table is displayed, the button is disabled.

<< : Updates the table entries, ending at the entry prior to the first entry currently displayed. If the first entry of the table is displayed, the button is disabled

>> : Updates the table entries, starting from the entry next to the last entry currently displayed. If the last entry of the table is displayed, the button is disabled.

>>| : Updates the table entries, ending at the last available entry. If the last entry of the table is displayed, the button is disabled.

Troubleshooting OSPF6

Before performing the troubleshooting steps, please note the following:

- OSPFv3 has the same functionality as OSPFv2, but OSPFv3 uses IPv6 addresses to communicate with OSPFv3 peers.
- OSPFv3 uses the same SPF algorithm as OSPFv2.
- OSPFv3 has a different process than OSPFv2.
- OSPFv3 maintains separate neighbor tables, topology tables and routing tables from OSPFv2.

OSPF6 Troubleshooting Steps:

1. Verify there is no mismatch in the hello parameters or in the dead timer.
2. Verify that the link is up. Ping the other end of the link.
3. Make sure that the interfaces at both ends are configured to support OSPF.
4. Check for a mismatch in the OSPF Network Type.
5. Verify that Hello and Dead timers match on each end of the link
6. Verify that Neighboring interfaces are in the same OSPF Area.
7. If the device is in more than one area, then it MUST have at least one interface in Area 0.
8. OSPF Area IDs: When using multiple network area statements in the OSPF configuration, the order of the statements is critical. Check that the networks have been assigned the desired area IDs by checking the output of the `show ip ospf` interface command.
9. OSPF Does Not Start: The OSPF process cannot start on a router if a router ID cannot be established. Check the output of `show ip ospf` to see if a router ID has been established. If a router ID has not been established, check to see if the router has an active interface (preferably a loopback interface) with an IP address.
10. Verify Neighbor relationships: Once a router is able to start OSPF, it establishes an interface data structure for each interface configured to run OSPF. Check the output of `show ip ospf interface` to ensure that OSPF is active on the intended interfaces. If OSPF is active, check for an incorrectly configured interface.
11. Check if there is an entry in the OSPF Database for a particular external route, but it is not showing in the routing table. Check the Forwarding Address associated with the route.

23. RIP

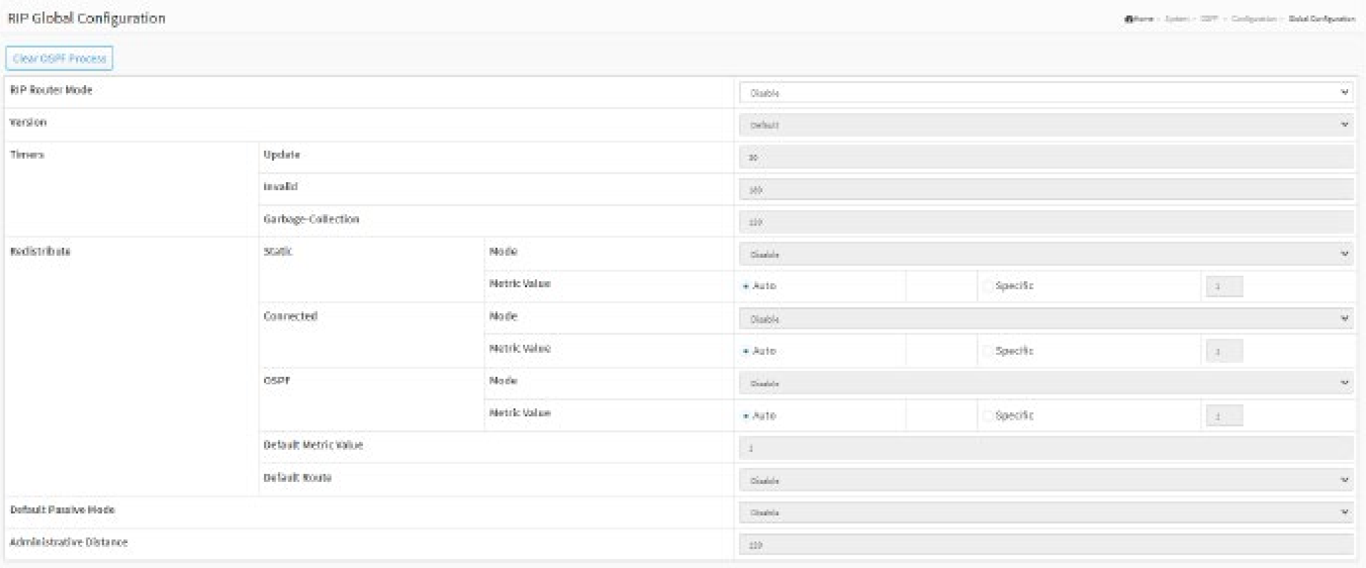
RIP (Routing Information Protocol) lets routers exchange network topology information. It is considered an interior gateway protocol, typically used in small to medium-sized networks.

RIP is a distance vector routing protocol which shares routing information between its neighbors to help build the network topology table. There are currently two IPv4 RIP versions: Version 1 and Version 2. The main difference between versions is that v2 supports subnet masks and authentication.

RIP uses a metric called hops to determine the cost of a route. A hop is a router which the traffic must pass through. If there are three routers that the traffic must pass through, there is a route cost of three hops. The maximum number of hops RIP will support is 15. If a route has more than 15 hops, the route will be discarded as invalid. RIP is susceptible to routing loops and uses mechanisms such as split horizon and others to prevent routing loops.

RIP Global Configuration

This page lets you set RIP global parameters.



RIP Global Configuration

RIP Router Mode			Disable			
Version			Default			
Timers	Update		30			
	Invalid		180			
	Garbage-Collection		120			
Redistribute	Static	Mode	Disable			
		Metric Value	● Auto		○ Specific	1
	Connected	Mode	Disable			
		Metric Value	● Auto		○ Specific	1
	OSPF	Mode	Disable			
		Metric Value	● Auto		○ Specific	1
	Default Metric Value		1			
	Default Route		Disable			
Default Passive Mode			Disable			
Administrative Distance			120			

Figure 22-1.1: RIP Global Configuration

Parameter descriptions:

RIP Router Mode : At the dropdown select Enable or Disable the RIP router operating mode.

version : At the dropdown select Version 1 or Version 2. The main difference between v1 and v2 is that v2 supports subnet masks and authentication.

Timers : These timers are user-configurable on the RIP Global Configuration page:

> ***Update*** : Sets the amount of time between RIP routing updates. Possible values are 3 - 21845. The default is 30 seconds.
>
> ***Invalid*** : specifies how long a routing entry can be in the RIP routing table without being updated. The default value is 180 seconds.
>
> ***Garbage-Collection*** : Sets the amount of time after which a route is removed from the RIP routing table. Possible values are 0 - 65535. The default is 120 seconds.

Redistribute : You can have multiple routing protocols on a network, but you will need a method to exchange routing information between the different protocols. This is done with redistribution. Redistribution is for more than just between routing protocols, it is also useful for between routing protocols (RIP, OSPF), static routes can be redistributed into a routing protocol, directly connected routes can be redistributed into a routing protocol, etc.

The following type of routes exist and can be distributed by RIP:

Static : Manually-defined (remote) routes. This tells RIP to forward static routes in addition to the directly connected routes and the routes that have been learned from other RIP routers, which it forwards by default.

Mode : ____ .
Metric Value : A RIP message includes a metric (number of hops) for each route.

Connected : RIP can redistribute directly connected interfaces. RIP routes that correspond to defined IP interfaces on which RIP is not enabled (defined locally). By default, the RIP Routing Table only includes routes that correspond to IP interfaces on which RIP is enabled.

Mode : ____ .
Metric Value : A RIP message includes a metric (number of hops) for each route.

OSPF : Open Shortest Path First.

Mode : ____ .
Metric Value : A RIP message includes a metric (number of hops) for each route.
Select ***Auto*** (default) or ***Specific***. If ***Specific***, enter a specific metric value. The valid range is 1 to __. The default is 1 .

Default Metric Value : ____ .

Default Route : At the dropdown select the default route to use.

Default Passive Mode : Transmission of routing update messages over a specific IP interface can be disabled. In this case, the router is passive, and only receives updated RIP information on this interface. By default, transmission of routing updates on an IP interface is enabled.

Special address 0.0.0.0 is used to describe a default route. A default route is used to avoid listing every possible network in the routing updates, when one or more closely-connected routers in the system are set to transfer traffic to the networks that are not listed explicitly. These routers create RIP entries for the address 0.0.0.0, just as if it was a network to which they are connected. You can enable the default route advertisement and configure it with a given metric.

Administrative Distance : AD is the "believability" of routing protocols. Routers measure each route source on a scale of 0 to 255, where 0 is the best route and 255 is the worst route. The smaller the administrative distance value, the more reliable the protocol. Typical administrative distances include: Directly connected=0, Static route=1, OSPF=110, RIP=120, Unknown=255, etc.

Buttons

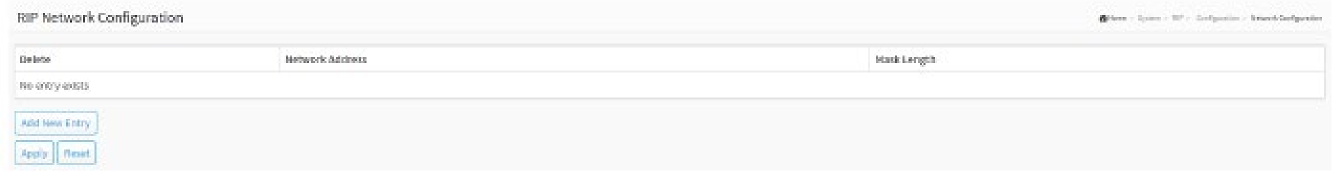
Clear OSPF Process : Click to reset the current OSPF process.

Apply : Click to save changes.

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

RIP Network Configuration

This page lets you add and configure new RIP entries. Navigate to the System > RIP > Configuration > Network Configuration menu path.



RIP Network Configuration

Home > System > RIP > Configuration > Network Configuration

Delete	Network Address	Mask Length
No entry exists		

Figure 22-1.2: RIP Network Configuration

Parameter descriptions:

Delete : Click to delete the table entry.

Network Address : Enter the IP address of the network.

Mask Length : Enter the netmask of the network.

Buttons

Add New Entry : Click to add a new entry to the table.

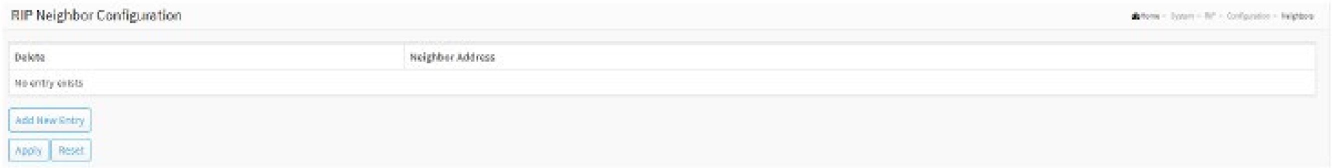
Apply : Click to save changes.

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

RIP Neighbor Configuration

This page lets you add and configure new RIP neighbor entries.

Navigate to the System > RIP > Configuration > Neighbor Configuration menu path.



RIP Neighbor Configuration

Delete	Neighbor Address
No entry exists	

Figure 22-1.3: RIP Neighbor Configuration

Parameter descriptions:

Delete : Click to delete the table entry.

Neighbor Address : Enter the IP address of the neighbor device .

Buttons

Add New Entry : Click to add a new entry to the table.

Apply : Click to save changes.

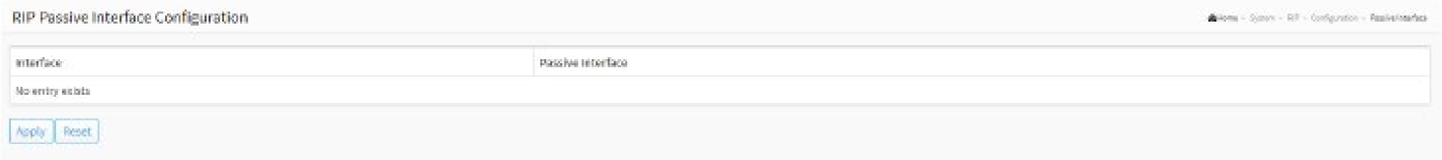
Reset : Click to undo any changes made locally and revert to previously saved values.

RIP Passive Interface

This page lets you use the RIP passive interface function to prevent RIP updates from being sent on particular interfaces.

The passive interface function tells an interface to listen to RIP routes but not to advertise them. When routing announcements on an interface are disabled, the router will "listen but don't talk." This feature can reduce the routing load on the CPU by reducing the number of interfaces on which a protocol will communicate. Use this function only if you are sure the routing protocol doesn't need to talk to anything on the specified interface.

Navigate to the System > RIP > Configuration > Passive Interface menu path.



RIP Passive Interface Configuration

Interface	Passive Interface
No entry exists	

Figure 22-1.4: RIP Passive Interface Configuration

Parameter descriptions:

Interface : Shows the RIP Interface**.**

Passive Interface : Shows the RIP Passive Interface**.**

Buttons

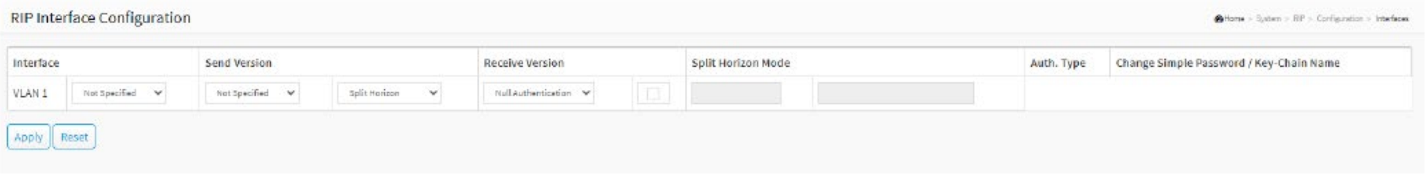
Apply : Click to save changes.

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

RIP Interface Configuration

This page lets you configure RIP interface parameters. Navigate to the System > RIP > Configuration > Interfaces menu path.

Passive Interface



RIP Interface Configuration

Interface		Send Version		Receive Version		Split Horizon Mode		Auth. Type	Change Simple Password / Key-Chain Name
VLAN 1	Not Specified	Not Specified	Split Horizon	Null Authentication	□				

Figure 22-1.5: RIP Interface Configuration

Parameter descriptions:

Interface : At the dropdown select ________, ________ , or _________. The default is ‘Not Specified’.

Send Version : There are two dropdown selections: ______________ and _______________ . The first default is ‘Not Specified’**.** The second default is ‘Split Horizon’**.** ‘Split Horizon’ prevents routing loops in distance-vector routing protocols by prohibiting a router from advertising a route back onto the interface from which it was learned.

Receive Version : At the dropdown select ________, ________ , or _________ . The default is ‘Null Authentication’.

Split Horizon Mode : Enter the _________________ and _______________. RIP is susceptible to routing loops; it uses the split horizon mechanism to prevent routing loops from forming.

Auth Type : Enter the type of authentication to use; plain text or MD5 authentication

Change Simple Password / Key-Chain Name : Enter a new simple password and keychain name.

Buttons

Apply : Click to save changes.

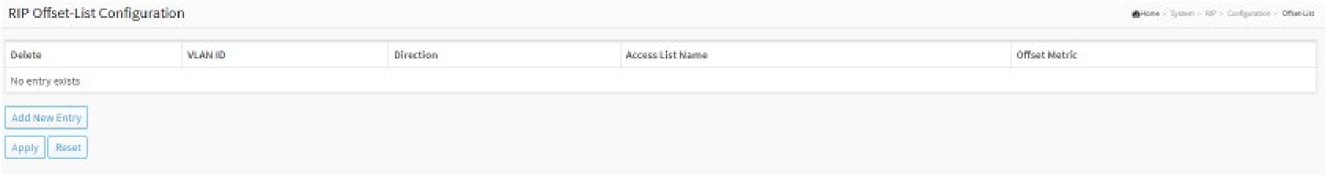
Reset : Click to undo any changes made locally and revert to previously saved values.

Offset-List

This page lets you create and configure RIP offset list parameters.

A RIP message includes a metric (number of hops) for each route. An ‘offset’ is an additional number that is added to a metric to affect the cost of paths. The offset is set per interface and, for example, can reflect the speed, delay, or some other quality of that specific interface. The relative cost of the interfaces can then be adjusted as desired. You must set the offset for each interface (the default offset is 1).

Navigate to the System > RIP > Configuration > Offset-List menu path.


RIP Offset-List Configuration

Delete	VLAN ID	Direction	Access List Name	Offset Metric
No entry exists				

Figure 22-1.6: RIP Offset-List Configuration

Parameter descriptions:

Delete : Click the button to delete an existing entry from the table and the switch**.**

VLAN ID : Enter the VLAN ID for entry**.**

Direction : Enter the direction for entry**.**

Access List Name : Enter the name of the access list for entry**.**

Offset Metric : Set the offset for each interface (the default offset is 1).

Buttons

Add New Entry : Click to add a new entry to the table.

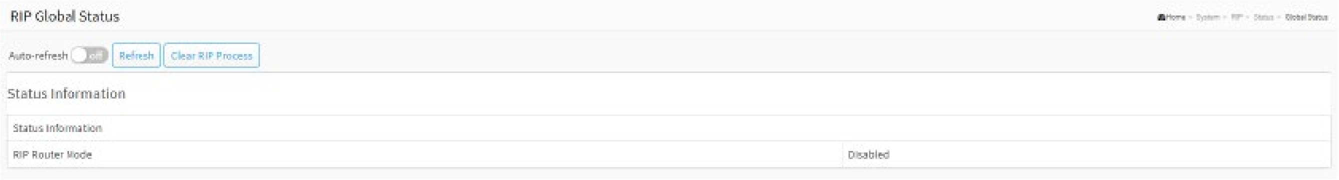
Apply : Click to save changes.

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

RIP Status

RIP Global Status

This page displays RIP overall status. Navigate to the System > RIP > Status > Global Status menu path.



Status Information

Status Information	
RIP Router Mode	Disabled

Figure 22-2.1: RIP Global Status

Parameter descriptions:

Status Information : Displays the current RIP router status information.

RIP Router Mode : Displays the current RIP router mode setting (_______________, or Disabled).

Buttons

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

Refresh : Click to manually refresh the page immediately.

Clear RIP Process : Click to reset the current RIP process.

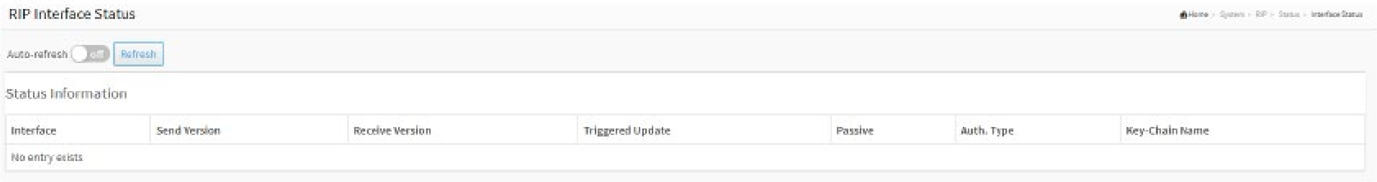
RIP Interface Status

This page displays current RIP Interface Status. Navigate to the System > RIP > Status > Interface Status menu path.

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

The "Start from entry keys" input field lets you change the starting point in this table. Clicking the Refresh button will update the displayed table starting from that or the closest next entry match.

In addition, these input fields will upon a Refresh button click, assume the value of the first displayed entry, allowing for continuous refresh with the same start input field.



Status Information

Interface	Send Version	Receive Version	Triggered Update	Passive	Auth. Type	Key-Chain Name
No entry exists						

Figure 22-2.2: RIP Interface Status

Parameter descriptions:

Interface : Displays the current RIP Interface**.**

Send Version: Displays the currently configured send version (v1 or v2).

Receive Version: Displays the currently configured receive version (v1 or v2).

Triggered Update: Displays the ______________ **.**

Passive : Displays the ___________________________ **.**

Auth. Type : Displays the type of authentication currently configured (plain text or MD5) **.**

Key-Chain Name : Displays the key chain name for the entry**.**

Buttons:

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

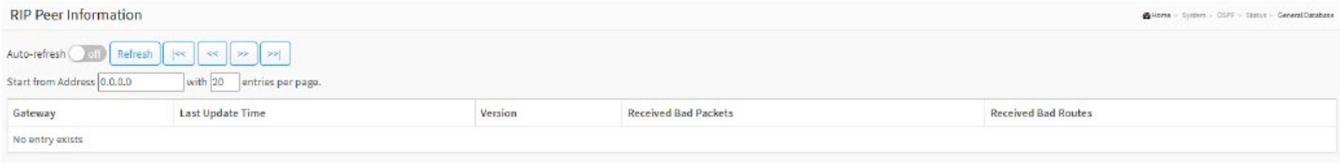
Refresh : Click to refresh the page immediately.

RIP Peer ~~Status~~ Information

This page displays current RIP peer information. Navigate to the System > RIP > Status > General Database menu path.

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

The "Start from Address " input field lets you change the starting point in this table. Clicking the Refresh button will update the displayed table starting from that or the closest next entry match. In addition, these input fields will upon a Refresh button click - assume the value of the first displayed entry, allowing for continuous refresh with the same start input field.



Start from Address 0.0.0.0 with 20 entries per page.

Gateway	Last Update Time	Version	Received Bad Packets	Received Bad Routes
No entry exists				

Figure 22-2.3: RIP Peer Information

Parameter descriptions:

Gateway : Displays the gateway ______________ .

Last Update Time : Displays the time of the last update.

Version : Displays the RIP peer version (v1 or v2). .

Received Bad Packets : Displays the number of bad packets received.

Received Bad Routes : Displays the number of bad routes received.

Buttons

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

Refresh : Click to refresh the page immediately.

|<< : Updates the table entries, starting from the first available entry. If the first entry of the table is displayed, the button is disabled.

<< : Updates the table entries, ending at the entry prior to the first entry currently displayed. If the first entry of the table is displayed, the button is disabled

>> : Updates the table entries, starting from the entry next to the last entry currently displayed. If the last entry of the table is displayed, the button is disabled.

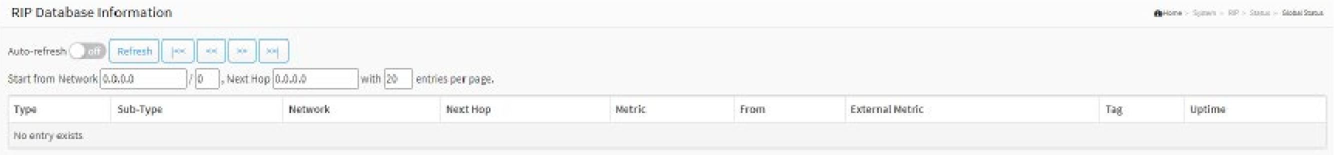
>>| : Updates the table entries, ending at the last available entry. If the last entry of the table is displayed, the button is disabled.

RIP Database Information

This page displays RIP database information. Navigate to the System > RIP > Status > Global Status menu path.

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

The "Start from Network" input field lets you change the starting point in this table. The Next Hop input field lets you enter the IP address of the next hop.



RIP Database Information

Start from Network 0.0.0.0 / 0 , Next Hop 0.0.0.0 with 20 entries per page.

Type	Sub-Type	Network	Next Hop	Metric	From	External Metric	Tag	Uptime
No entry exists								

Figure 22-2.4: RIP Database Information

Parameter descriptions:

Type : Displays the entry’s configured authentication type (plain text or MD5).

Sub-Type : Displays the entry’s configured authentication sub type (___________ or _________).

Network : Displays the entry’s network IP address.

Next Hop : Displays the entry’s next hop IP address.

Metric : Displays the entry’s metric.

From : Displays the entry’s ___________________ .

External Metric : Displays the entry’s external metric.

Tag : Displays the entry’s _______________________ .

Uptime : Displays the amount of time that the entry has been running.

Buttons

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

Refresh : Click to refresh the page immediately.

|<< : Updates the table entries, starting from the first available entry. If the first entry of the table is displayed, the button is disabled.

<< : Updates the table entries, ending at the entry prior to the first entry currently displayed. If the first entry of the table is displayed, the button is disabled

>> : Updates the table entries, starting from the entry next to the last entry currently displayed. If the last entry of the table is displayed, the button is disabled.

>>| : Updates the table entries, ending at the last available entry. If the last entry of the table is displayed, the button is disabled.

RIP Troubleshooting

1. Wrong network command(s): the network command is used to tell RIP what networks to advertise, but also where to send RIP routing updates. Wrong or missing network commands will cause issues.
2. Interface shut: A network on an interface that is in shutdown will not be advertised.
3. Passive interface: An interface that is configured as passive will not send any RIP updates.
4. Version mismatch: RIP has two versions; both routers must use the same version.
5. Max hop count: When the hop count is 16, the network is considered unreachable. If the network is small, check for offset-lists that increase the metric.
6. Route Filtering: Filters might prevent RIP updates from being sent or received.
7. Authentication: Both RIP routers must have the same authentication parameters.
8. Split horizon: Networks that are learned on an interface are not advertised out of the same interface.

24. Diagnostics

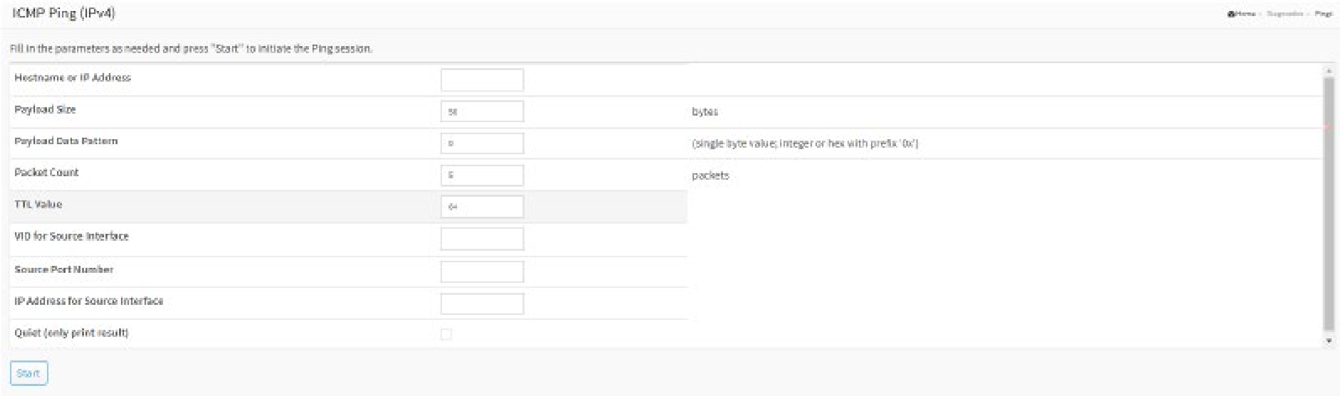
This menu section provides a set of basic system diagnostics including Ping, Traceroute, Cable Diagnostics and Port Mirror.

Ping4

This page lets you issue ICMP (IPv4) PING packets to troubleshoot IP connectivity issues.

To configure a Ping in the web UI:

1. Click Diagnostics and Ping.
2. Specify IP Address, Ping Length, Ping Count, Ping Interval and Egress Interface.
3. Click Start.



ICMP Ping (IPv4)

Fill in the parameters as needed and press "Start" to initiate the Ping session.

Hostname or IP Address		
Payload Size	56	bytes
Payload Data Pattern	0	(single byte value; integer or hex with prefix '0x')
Packet Count	5	packets
TTL Value	64	
VID for Source Interface		
Source Port Number		
IP Address for Source Interface		
Quiet (only print result)	□	

Figure 23-1: ICMP Ping (IPv4)

Parameter descriptions:

Hostname or IP Address : The address of the destination host, either as a symbolic hostname or an IP Address.

Payload Size : Specify the size of the ICMP data payload in bytes (excluding the size of Ethernet, IP and ICMP headers). The default value is 56 bytes. The valid range is 2-1452 bytes.

Payload Data Pattern : Specify the pattern used in the ICMP data payload. The default value is 0. The valid range is 0-255.

Packet Count : Specify the number of Ping requests sent. The default value is 5. The valid range is 1-60.

TTL Value : Specify the Time-To-Live/TTL) field value in the IPv4 header. The default value is 64 seconds. The valid range is 1-255 seconds.

VID for Source Interface : This field can be used to force the test to use a specific local VLAN interface as the source interface. Leave this field empty for automatic selection based on routing configuration. **Note**: You may only specify either the VID or the IP Address for the source interface.

Source Port Number : This field can be used to force the test to use a specific local interface with the specified port number as the source interface. The specified port must be configured with a suitable IP address. Leave this field empty for automatic selection based on routing configuration. **Note**: You may only specify either the Source Port Number or the IP Address for the source interface.

Address for Source Interface : This field can be used to force the test to use a specific local interface with the specified IP address as the source interface. The specified IP address must be configured on a local interface.

Leave this field empty for automatic selection based on routing configuration. **Note**: You may only specify either the VID or the IP Address for the source interface.

Quiet (only print result) : Checking this option will not print the result of each Ping request but will only show the final result.

After you press Start, ICMP packets are transmitted, and the sequence number and round trip time are displayed upon reception of a reply.

The amount of data received inside of an IP packet of type ICMP ECHO_REPLY will always be 8 bytes more than the requested payload data size (the difference is the ICMP header).

The page refreshes automatically until responses to all packets are received, or until a timeout occurs.

Ping output looks like this:

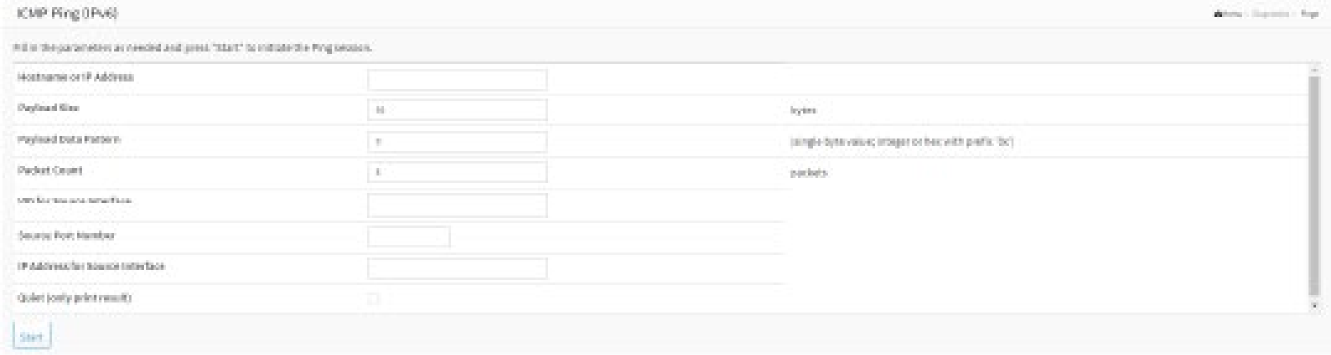
```
PING 172.16.1.1 (172.16.1.1) from 172.16.1.10: 56 data bytes
64 bytes from 172.16.1.1: seq=0 ttl=64 time=2.034 ms
64 bytes from 172.16.1.1: seq=1 ttl=64 time=1.729 ms
64 bytes from 172.16.1.1: seq=2 ttl=64 time=1.954 ms
64 bytes from 172.16.1.1: seq=3 ttl=64 time=1.699 ms
64 bytes from 172.16.1.1: seq=4 ttl=64 time=1.916 ms
--- 172.16.1.1 ping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max = 1.699/1.866/2.034 ms
```

Buttons

Start : Click the button to start to ping the target IP Address.

Ping6

This page allows you to issue ICMPv6 PING packets to troubleshoot IPv6 connectivity issues.



ICMP Ping (IPv6)

Fill in the parameters as needed and press "Start" to initiate the Ping session.

Hostname or IP Address		
Payload Size	56	bytes
Payload Data Pattern	0	(single-byte value; integer or hex with prefix '0x')
Packet Count	5	packets
VID for Source Interface		
Source Port Number		
IP Address for Source Interface		
Quiet (only print result)	□	

Figure 23-2: ICMP Ping (IPv6)

Hostname or IP Address : The address of the destination host, either as a symbolic hostname or an IP Address.

Payload Size : Set the size of the ICMP data payload in bytes (excluding the size of Ethernet, IP, and ICMP headers). The default value is 56 bytes. The valid range is 2-1452 bytes.

Payload Data Pattern : Set the pattern used in the ICMP data payload. The default value is 0. The valid range is 0-255.

Packet Count : Select the number of PING requests sent. The default value is 5. The valid range is 1-60.

VID for Source Interface : This field can be used to force the test to use a specific local VLAN interface as the source interface. Leave this field empty for automatic selection based on routing configuration. **Note**: You may only specify either the VID or the IP Address for the source interface.

Source Port Number : This field can be used to force the test to use a specific local interface with the specified port number as the source interface. The specified port must be configured with a suitable IP address. Leave this field empty for automatic selection based on routing configuration. **Note**: You may only specify either the Source Port Number or the IP Address for the source interface.

Address for Source Interface : This field can be used to force the test to use a specific local interface with the specified IP address as the source interface. The specified IP address must be configured on a local interface. Leave this field empty for automatic selection based on routing configuration. **Note**: You may only specify either the VID or the IP Address for the source interface.

Quiet (only print result) : Checking this option will not print the result of each ping request but will only show the final result.

After you press the Start button, ICMP packets are transmitted, and the sequence number and round trip time are displayed upon reception of a reply.

The amount of data received inside of an IP packet of type ICMP ECHO_REPLY will always be 8 bytes more than the requested payload data size (the difference is the ICMP header).

The page refreshes automatically until responses to all packets are received, or until a timeout occurs.

Ping6 output looks like the following:

```
PING 2001::01 (2001::1) from 2001::3: 56 data bytes
64 bytes from 2001::1: seq=0 ttl=64 time=2.118 ms
64 bytes from 2001::1: seq=1 ttl=64 time=2.009 ms
64 bytes from 2001::1: seq=2 ttl=64 time=1.852 ms
64 bytes from 2001::1: seq=3 ttl=64 time=2.869 ms
64 bytes from 2001::1: seq=4 ttl=64 time=1.845 ms
--- 2001::01 ping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max = 1.845/2.138/2.869 ms
```

Buttons

Start : Click the “Start” button to start to ping the target IP Address.

New Ping : Click to start a new Ping diagnostics.

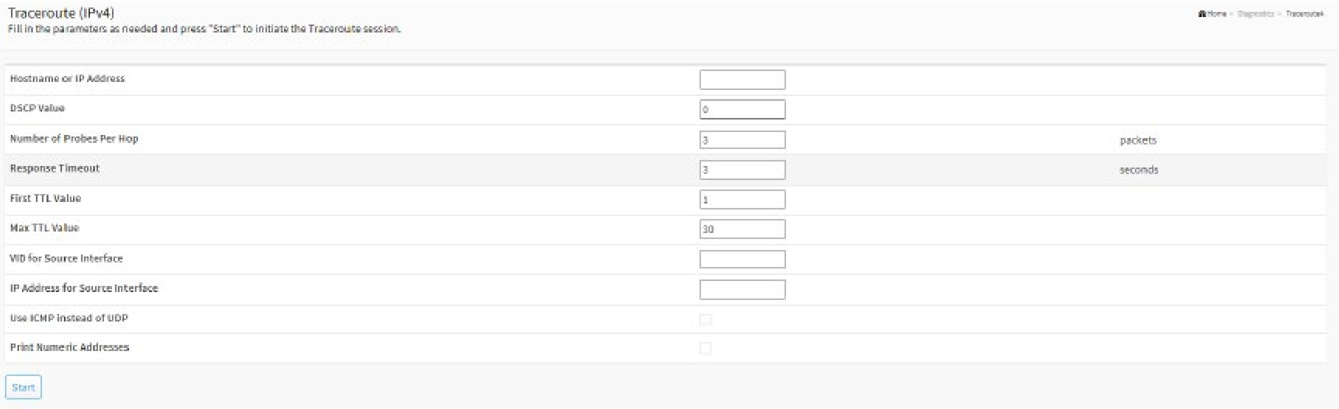
Traceroute (IPv4)

This page lets you perform a traceroute test over IPv4 towards a remote host. Traceroute is a diagnostic tool for displaying the route and measuring transit delays of packets across an IPv4 network.

Web Interface

To start a Traceroute in the web UI:

1. Click Diagnostics and Traceroute.
2. Specify IP Address, Wait Time, Max TTL and Probe Count.
3. Click Start.



Traceroute (IPv4)

Fill in the parameters as needed and press "Start" to initiate the Traceroute session.

Hostname or IP Address		
DSCP Value	0	
Number of Probes Per Hop	3	packets
Response Timeout	3	seconds
First TTL Value	1	
Max TTL Value	30	
VID for Source Interface		
IP Address for Source Interface		
Use ICMP instead of UDP	□	
Print Numeric Addresses	□	

Figure 23-3: Traceroute (IPv4)

Parameter descriptions:

Hostname or IP Address : The destination IP Address.

DSCP Value : This value is used for the DSCP value in the IPv4 header. The default value is 0. The valid range is 0-63.

Number of Probes Per Hop : Determines the number of probes (packets) sent for each hop. The default value is 3. The valid range is 1-60.

Response Timeout : Determines the number of seconds to wait for a reply to a sent request. The default number is 3 seconds. The valid range is 1-86400.

First TTL Value : Determines the value of the Time-To-Live (TTL) field in the IPv4 header in the first packet sent. The default number is 1. The valid range is 1-30.

Max TTL Value : Determines the maximum value of the Time-To-Live (TTL) field in the IPv4 header. If this value is reached before the specified remote host is reached the test stops. The default number is 30. The valid range is 1-255.

VID for Source Interface : This field can be used to force the test to use a specific local VLAN interface as the source interface. Leave this field empty for automatic selection based on routing configuration. **Note**: You may only specify either the VID or the IP Address for the source interface.

Address for Source Interface : This field can be used to force the test to use a specific local interface with the specified IP address as the source interface. The specified IP address must be configured on a local interface. Leave this field empty for automatic selection based on routing configuration. **Note**: You may only specify either the VID or the IP Address for the source interface.

Use ICMP instead of UDP : By default, the traceroute command will use UDP datagrams. Selecting this option forces it to use ICMP ECHO packets instead.

Print Numeric Addresses : By default, the traceroute command will print out hop information using a reverse DNS lookup for the acquired host IP addresses. This may slow down the display if the DNS information is not available. Selecting this option will prevent the reverse DNS lookup and force the traceroute command to print numeric IP addresses instead.

Buttons

Start : Click the "Start" button to start the IPv4 Traceroute.

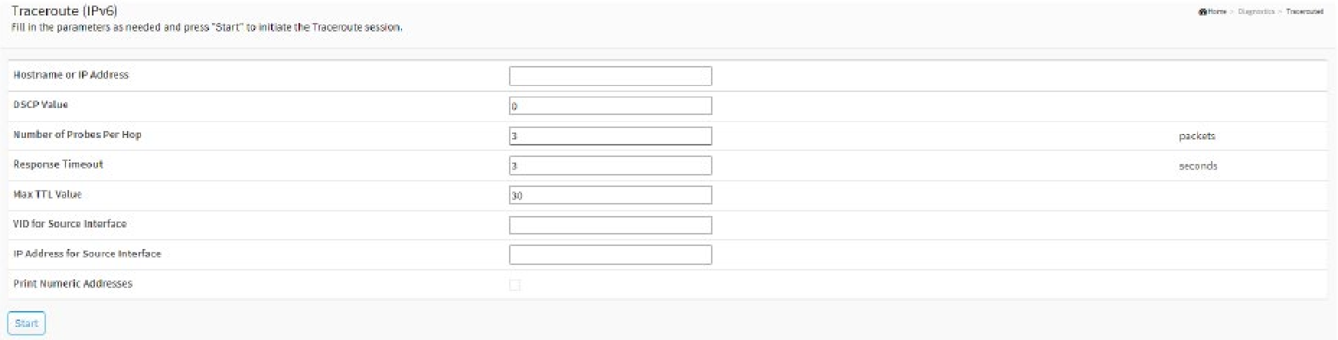
Traceroute (IPv6)

This page lets you perform a traceroute test over IPv6 towards a remote host. Traceroute is a diagnostic tool for displaying the route and measuring transit delays of packets across an IPv6 network.

Web Interface

To start an IPv6 Traceroute in the web UI:

1. Click Diagnostics and Traceroute.
2. Fill in the parameters as needed and press “Start” to initiate the Traceroute session.



Traceroute (IPv6)

Fill in the parameters as needed and press "Start" to initiate the Traceroute session.

Hostname or IP Address		
DSCP Value	0	
Number of Probes Per Hop	3	packets
Response Timeout	3	seconds
Max TTL Value	30	
VID for Source Interface		
IP Address for Source Interface		
Print Numeric Addresses	□	

Figure 23-4: Traceroute (IPv6)

Parameter descriptions:

Hostname or IP Address : The destination IP Address.

DSCP Value : This value is used for the DSCP value in the IPv4 header. The default value is 0. The valid range is 0-255.

Number of Probes Per Hop : Determines the number of probes (packets) sent for each hop. The default value is 3 packets. The valid range is 1-60 packets.

Response Timeout : Determines the number of seconds to wait for a reply to a sent request. The default is 3 seconds. The valid range is 1-86400 seconds.

Max TTL Value : Determines the maximum value of the Time-To-Live (TTL) field in the IPv4 header. If this value is reached before the specified remote host is reached the test stops. The default is 255. The valid range is 1-255.

VID for Source Interface : This field can be used to force the test to use a specific local VLAN interface as the source interface. Leave this field empty for automatic selection based on routing configuration. **Note**: You may only specify either the VID or the IP Address for the source interface.

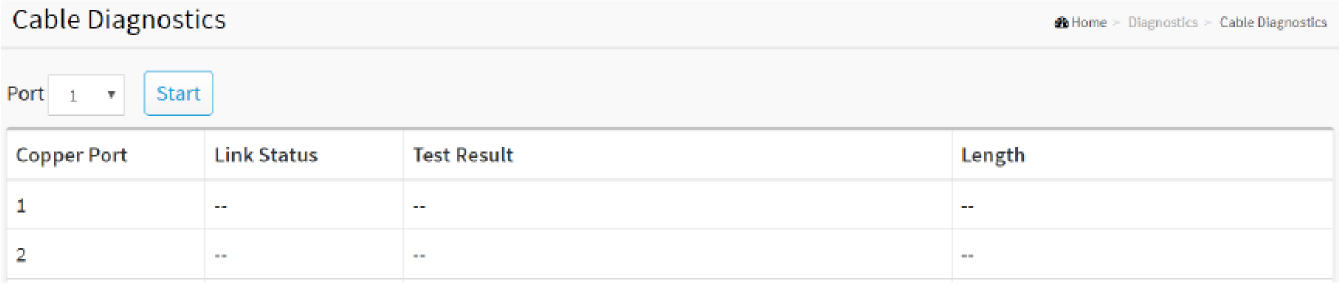
Address for Source Interface : This field can be used to force the test to use a specific local interface with the specified IP address as the source interface. The specified IP address must be configured on a local interface. Leave this field empty for automatic selection based on routing configuration. **Note**: You may only specify either the VID or the IP Address for the source interface.

Print Numeric Addresses : By default, the traceroute command will print out hop information using a reverse DNS lookup for the acquired host IP addresses. This may slow down the display if the DNS information is not available. Selecting this option will prevent the reverse DNS lookup and force the traceroute command to print numeric IP addresses instead.

Cable Diagnostics

This page lets you run Cable Diagnostics on copper ports. To configure Cable Diagnostics in the web UI:

1. Click Diagnostics and Cable Diagnostics.
2. Specify which Port you want to check.
3. Click Start.



Cable Diagnostics

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

Figure 23-5: Cable Diagnostics

Parameter descriptions:

Port : The port on which you are requesting Cable Diagnostics.

Copper Port : The copper port number.

Link Status : The status of the cable:

10M: Cable is link up and correct. Speed is 10Mbps

100M: Cable is link up and correct. Speed is 100Mbps

1G: Cable is link up and correct. Speed is 1Gbps

Link Down: Link down or cable is not correct.

Test Result : Test Result of the cable:

OK: Correctly terminated pair

Abnormal: Incorrectly terminated pair or link down

Length : The length (in meters) of the cable pair. The resolution is 3 meters. When Link Status is shown as follows, the length has different definitions:

1G: The length is the minimum value of 4-pair.

10M/100M: The length is the minimum value of 2-pair.

Link Down: The length is the minimum value of non-zero of 4-pair.

Button

Start : Click to begin the cable diagnostics on the selected port.

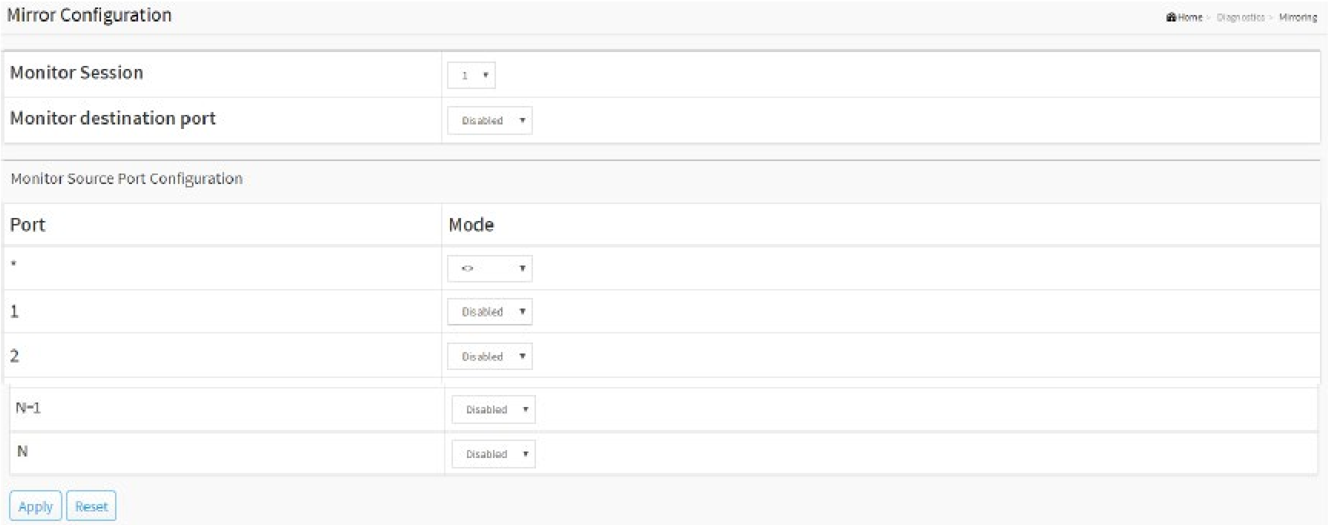
Mirroring

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

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

To configure the Port Mirror function in the web UI:

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 settings.
5. To cancel the settings click the Reset button to revert to previously saved values.



Mirror Configuration

Monitor Session	1
Monitor destination port	Disabled

Monitor Source Port Configuration

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

Figure 23-6: Mirror Configuration

Parameter descriptions:

Monitor Session : At the dropdown select a Session number (instance).

Monitor Destination Port : The 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 enabling Rx and Tx.

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.

sFlow

Configuration

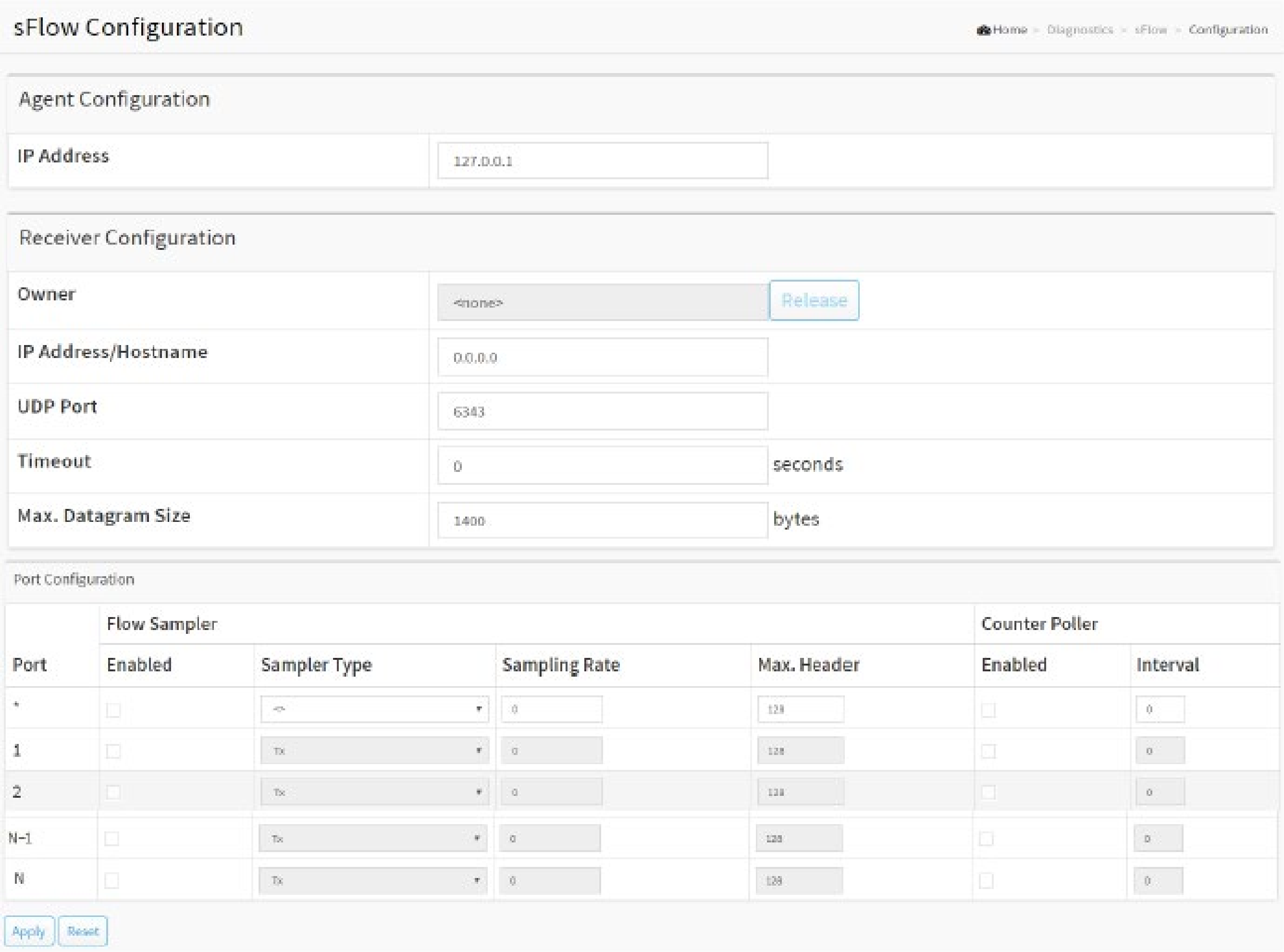
The sFlow Collector configuration for the switch can be monitored and modified here. The configuration is divided into two parts: Configuration of the sFlow receiver (a.k.a. sFlow collector) and configuration of per-port flow and counter samplers.

sFlow configuration is not persisted to non-volatile memory, which means that a reboot or master change will disable sFlow sampling.

Web Interface

To configure sFlow in the web UI:

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



sFlow Configuration

Agent Configuration

IP Address	127.0.0.1

Receiver Configuration

Owner	<none>	Release
IP Address/Hostname	0.0.0.0	
UDP Port	6343	
Timeout	0	seconds
Max. Datagram Size	1400	bytes

Port Configuration

	Flow Sampler				Counter Poller	
Port	Enabled	Sampler Type	Sampling Rate	Max. Header	Enabled	Interval
*	□	<>	0	128	□	0
1	□	Tx	0	128	□	0
2	□	Tx	0	128	□	0
N-1	□	Tx	0	128	□	0
N	□	Tx	0	128	□	0

Figure 23-7.2: sFlow Configuration

Parameter descriptions:

Agent Configuration

IP Address : The IP address used as the Agent IP address in sFlow datagrams. It serves as a unique key that will identify this agent over extended periods of time. Both IPv4 and IPv6 addresses are supported.

Receiver Configuration

Owner : Basically, sFlow can be configured in two ways: 1) via local management using the Web or CLI interface or 2) via SNMP. This read-only field shows the owner of the current sFlow configuration and assumes values as follows:

- If sFlow is currently unconfigured/unclaimed, Owner contains <none>.
- If sFlow is currently configured through Web or CLI, Owner contains <Configured through local management>.
- If sFlow is currently configured through SNMP, the Owner contains a string identifying the sFlow receiver. If sFlow is configured through SNMP, all controls - except for the Release-button - are disabled to avoid inadvertent reconfiguration.

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

IP Address/Hostname : The IP address or hostname of the sFlow receiver. Both IPv4 and IPv6 addresses are supported.

UDP Port : The UDP port on which the sFlow receiver listens to sFlow datagrams. If set to 0 (zero), the default port (6343) is used.

Timeout : The number of seconds remaining before sampling stops and the current sFlow owner is released. While active, the current time left can be updated with a click on the Refresh-button. If locally managed, the timeout can be changed on the fly without affecting any other settings.

Max. Datagram Size : The maximum number of data bytes that can be sent in a single sample datagram. This should be set to a value that avoids fragmentation of the sFlow datagrams. The valid range is 200 to 1468 bytes and the default is 1400 bytes.

Port Configuration

Port : The port number for which the configuration below applies.

Flow Sampler Enabled : Enables/disables flow sampling on this port.

Flow Sampler Sampling Rate : The statistical sampling rate for packet sampling. Set to N to sample on average 1/Nth of the packets transmitted/received on the port. Not all sampling rates are achievable. If an unsupported sampling rate is requested, the switch will automatically adjust it to the closest achievable. This will be reported back in this field.

Flow Sampler Max. Header : The maximum number of bytes that should be copied from a sampled packet to the sFlow datagram. Valid range is 14 to 200 bytes with default being 128 bytes. If the maximum datagram size does not consider the maximum header size, samples may be dropped.

Counter Poller Enabled : Enables/disables counter polling on this port.

Counter Poller Interval : With counter polling enabled, this specifies the interval - in seconds - between counter poller samples.

Buttons

Apply : Click to save changes.

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

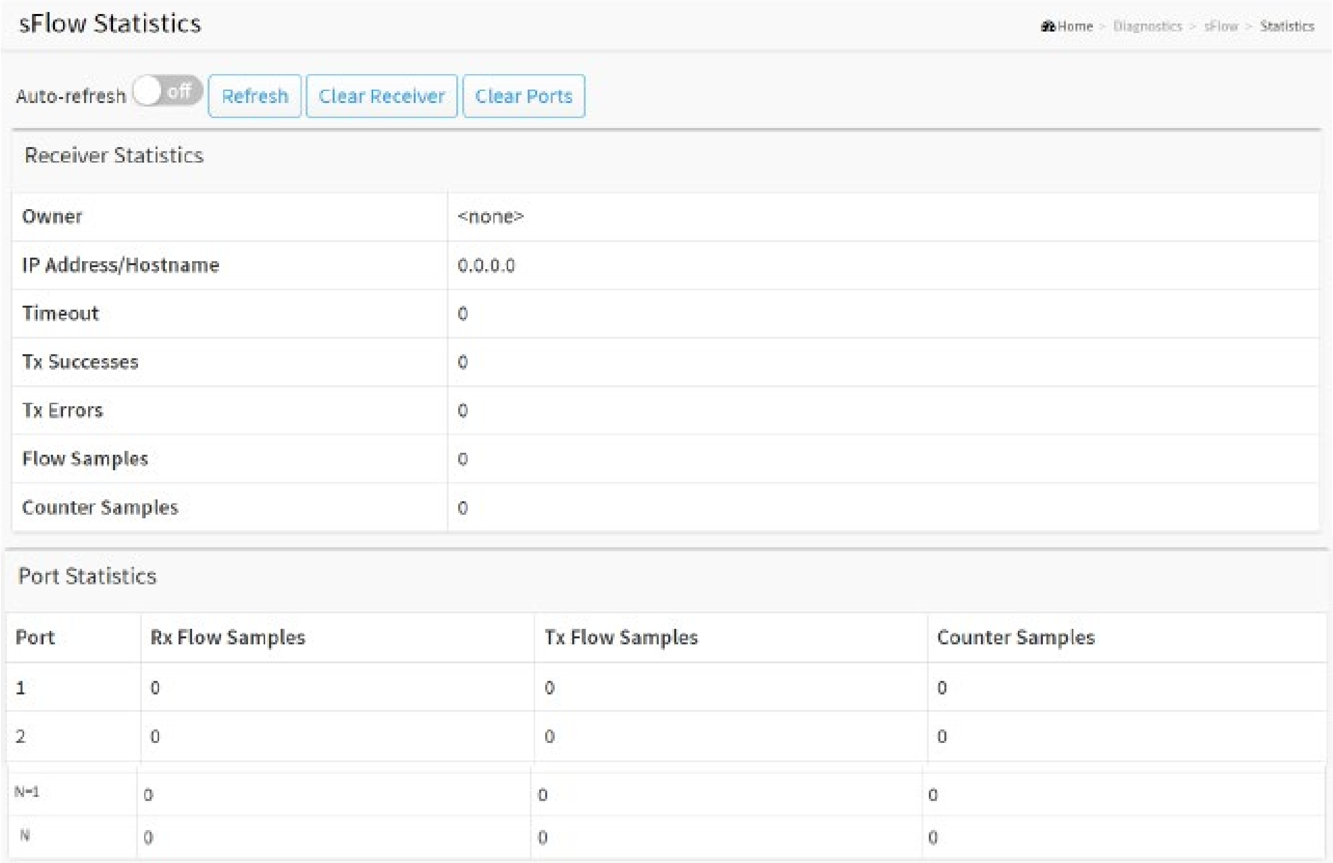
Release : Click to release the current owner and disable sFlow sampling. The Release button is disabled if sFlow is currently unclaimed. If configured via SNMP, the release must be confirmed (a confirmation request will display).

Refresh : Click to manually refresh the page immediately. Note that unsaved changes will be lost.

Statistics

This page shows sFlow receiver and per-port statistics. To display port sFlow statistics in the web UI:

1. Click Diagnostics, sFlow and statistics.
2. View the sFlow information.



sFlow Statistics

Receiver Statistics

Owner	<none>
IP Address/Hostname	0.0.0.0
Timeout	0
Tx Successes	0
Tx Errors	0
Flow Samples	0
Counter Samples	0

Port Statistics

Port	Rx Flow Samples	Tx Flow Samples	Counter Samples
1	0	0	0
2	0	0	0
N-1	0	0	0
N	0	0	0

Figure 23-7.2: sFlow Statistics

Parameter descriptions:

Receiver Statistics

Owner : Shows the current owner of the sFlow configuration. It assumes one of these three values:

- If sFlow is currently unconfigured or unclaimed, the Owner field contains <none>.
- If sFlow is currently configured via Web or CLI, Owner contains <Configured via local management>.
- If sFlow is currently configured via SNMP, Owner contains a string identifying the sFlow receiver.`

IP Address/Hostname : The IP address or hostname of the sFlow receiver.

Timeout : The number of seconds remaining before sampling stops and the current sFlow owner is released.

Tx Successes : The number of UDP datagrams successfully sent to the sFlow receiver.

Tx Errors : The number of UDP datagrams that has failed transmission. The most common source of errors is invalid sFlow receiver IP/hostname configuration. To diagnose, paste the receiver's IP address/hostname into the Ping Web page (Diagnostics > Ping/Ping6).

Flow Samples : The total number of flow samples sent to the sFlow receiver.

Counter Samples : The total number of counter samples sent to the sFlow receiver.

Port Statistics

Port : The port number for which the following statistics applies.

Rx and Tx Flow Samples : The number of flow samples sent to the sFlow receiver originating from this port. Here, flow samples are divided into Rx and Tx flow samples, where Rx flow samples contains the number of packets that were sampled upon reception (ingress) on the port and Tx flow samples contains the number of packets that were sampled upon transmission (egress) on the port.

Counter Samples : The total number of counter samples sent to the sFlow receiver originating from this port.

Buttons

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

Refresh : Click to refresh the page immediately.

Clear Receiver : Clears the sFlow receiver counters.

Clear Ports : Clears the per-port counters.

25. Maintenance

This chapter describes Maintenance tasks Save, Backup, Restore, Activate, Delete, Restart Device, Factory Defaults, Firmware Selection, and Firmware Upgrade.

Configuration

The switch stores its configuration in several 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.

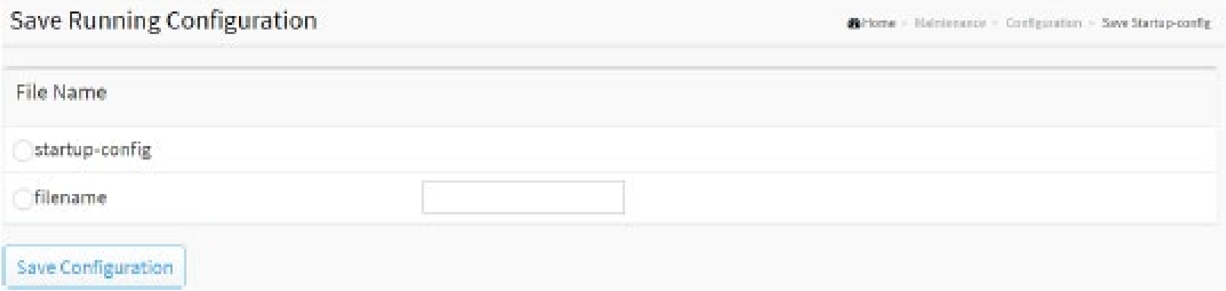
Save running-config to startup-config

This copies the running-config file to startup-config, ensuring that the current active configuration will be used at the next reboot.

Web Interface

To save running configuration in the web UI:

1. Click Maintenance, Configuration and Save Startup-config.
2. Click Save Configuration.



Save Running Configuration

Home > Maintenance > Configuration > Save Startup-config

File Name

○ startup-config

○ filename

Figure 24-1.1: Save Running Config to Startup Config

Buttons

Save Configuration : Click to save the configuration; the running configuration will be written to flash memory for system boot up to load this startup configuration file.

Backup Configuration

This page lets you export the switch configuration for maintenance needs. Any current configuration files will be exported in text format.

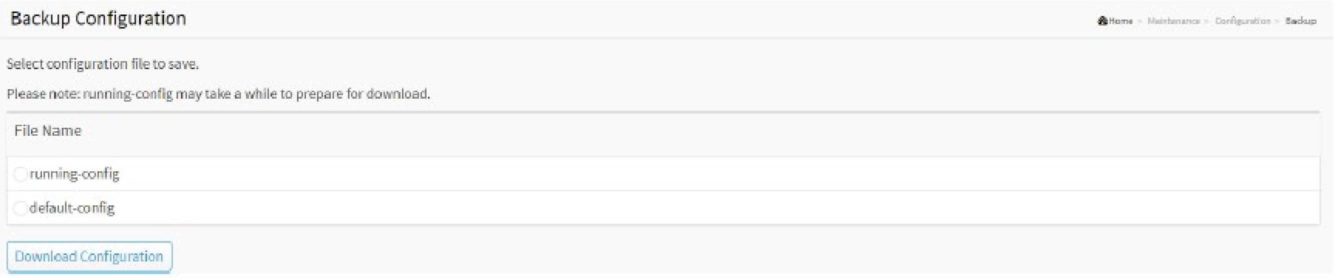
The configuration files on the switch can be backed up and saved on the station running the web browser.

It is possible to transfer any of the files on the switch to the web browser. Selecting the running-config may take a little while to complete, as the file must be prepared before backup.

Web Interface

To perform a configuration backup in the web UI:

1. Click Maintenance, Configuration, and Backup.
2. Select a File Name.
3. Click the Download Configuration button.



Select configuration file to save.

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

File Name
○ running-config
○ default-config

Figure 24-1.2: Backup Configuration

Parameter descriptions:

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

default-config : A read-only file with vendor-specific configuration. This file is read when the system is restored to default settings.

Buttons

Download Configuration : Click the button then the switch will start to transfer the configuration file to your workstation.

Restore Configuration

You can 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.

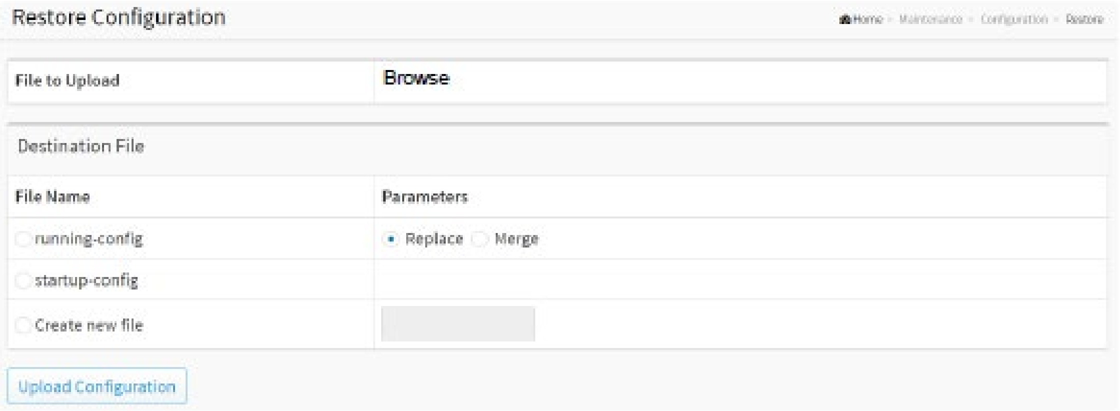
If the destination is running-config, the file will be applied to the switch configuration in one of two ways:

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

Web Interface

To restore configuration in the web UI:

1. Click Maintenance, Configuration and Restore.
2. Click the Browse button and browse to and select a file.
3. Select a File Name. If you select “running-config” select Replace mode or Merge mode.
4. Click Restore.



Restore Configuration

File to Upload	Browse

Destination File

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

Figure 24-1.3: Restore Configuration

Parameter descriptions:

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

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

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

Create new file : Enter a filename to create new file to restore.

Buttons

Browse : Click the button to search for a configuration text file and filename.

Upload Configuration : Click the button to start transfer the source file to the destination file.

Activate

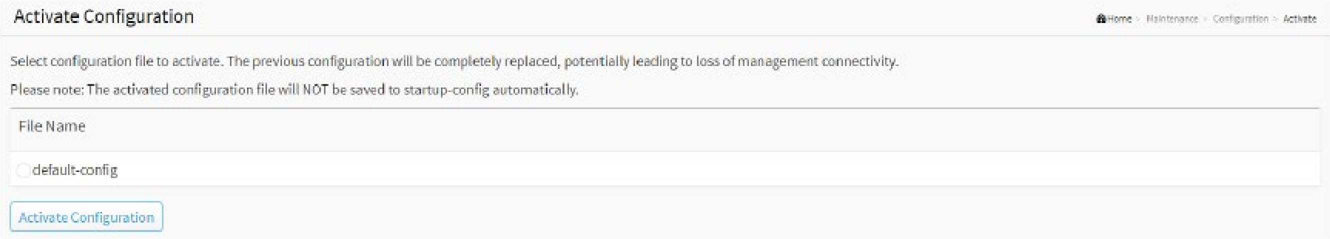
You can activate any of the config files present on the switch, except for running-config which represents the currently active configuration.

Select the file to activate and click the “Activate Configuration” button. This will initiate the process of completely replacing the existing config with that of the selected file.

Web Interface

To activate a configuration in the web UI:

1. Click Maintenance, Configuration and Activate.
2. Select a configuration file to activate. The previous configuration will be completely replaced, potentially leading to loss of management connectivity.
3. **Note**: The activated configuration file will NOT be saved to startup-config automatically.
4. Click the Activate Configuration button.



Activate Configuration

Select configuration file to activate. The previous configuration will be completely replaced, potentially leading to loss of management connectivity.

Please note: The activated configuration file will NOT be saved to startup-config automatically.

File Name
○ default-config

Figure 24-1.4: Activate Configuration

Parameter descriptions:

File Name : Check a radio button for the file to be activated.

Buttons

Activate Configuration : Click the button and the selected file will be activated to be the switch's running configuration.

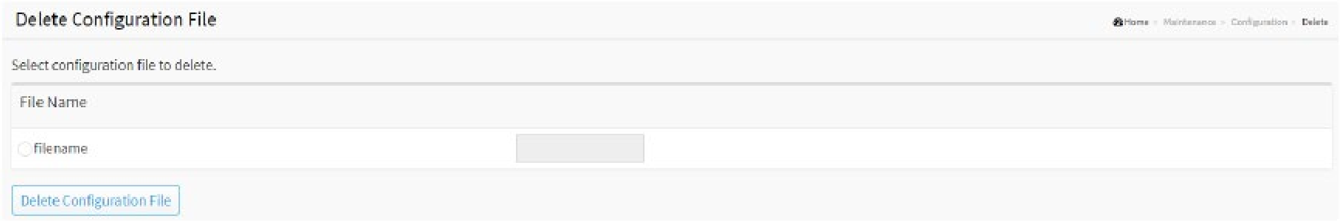
Delete

You can 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 its default configuration.

Web Interface

To delete a configuration file in the web UI:

1. Click Maintenance, Configuration, and Delete.
2. Select a configuration file to delete.
3. Click the Delete Configuration File button.



Delete Configuration File

Home » Maintenance » Configuration » Delete

Select configuration file to delete.

File Name	
○ filename	

Delete Configuration File

Figure 24-1.5: Delete Configuration File

Parameter descriptions:

File Name : Select the filename radio button and enter the desired file name.

Buttons

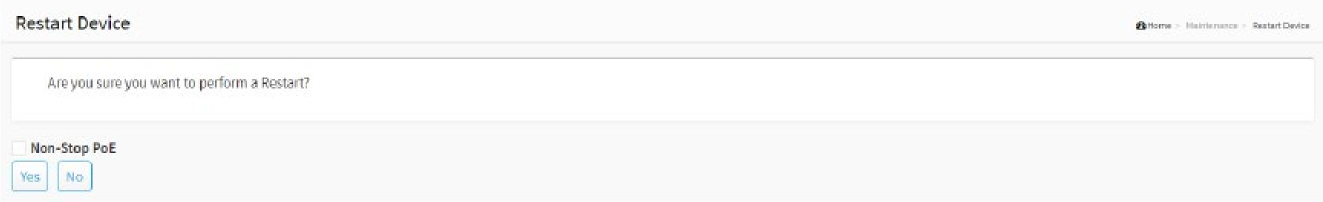
Delete Configuration File: Click the “Delete Configuration File” button then the selected file will be deleted.

Restart Device

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

To restart the switch in the web UI:

1. Click Maintenance and Restart Device.
2. At the "*Are you sure ...*?" prompt click Yes.



Are you sure you want to perform a Restart?

□ Non-Stop PoE

Figure 24-2: Restart Device

Parameter descriptions:

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

Non-Stop PoE : Check the box if you want the switch to keep providing PoE power to the PDs during the restart process.

Buttons

Yes : Click "Yes" then the device will restart.

No : Click to cancel the operation.

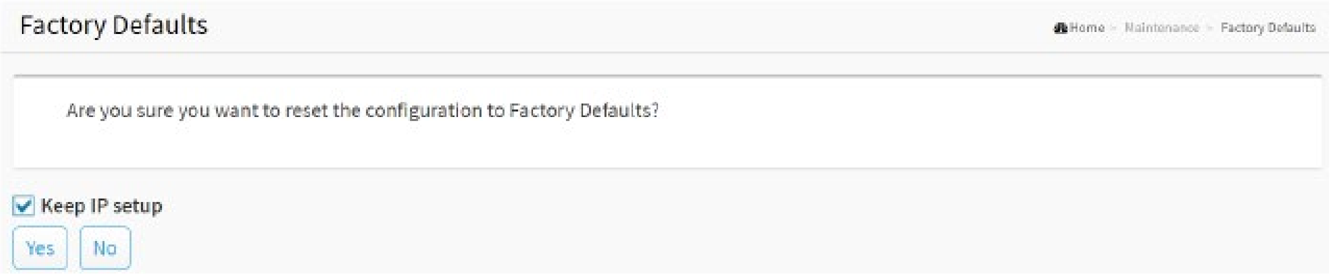
Factory Defaults

This page lets you restore the switch configuration to its Factory Default settings.

Web Interface

To restore the switch to its Factory Defaults in the web UI:

1. Click Maintenance and Factory Defaults.
2. Check the "Keep IP setup" box if you want to keep the existing IP setup.
3. At the "*Are you sure ... ?"* prompt click Yes.



Are you sure you want to reset the configuration to Factory Defaults?

☑ Keep IP setup

Figure 24-3: Factory Defaults

Buttons

Keep IP Configuration : Check the box if you want to keep the current IP configuration.

Yes : Click to "Yes" button to reset the configuration to Factory Defaults.

No : Click to cancel the operation.

Firmware

This section lets you upgrade (update) device firmware and activate the alternate firmware image.

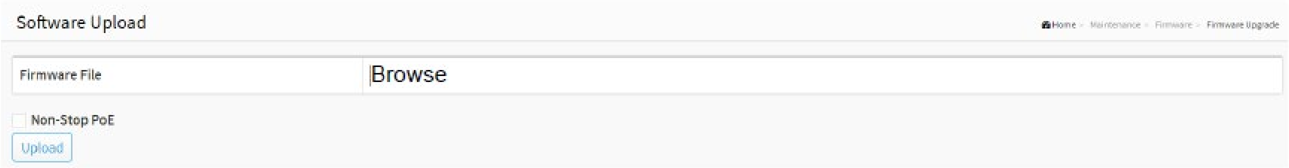
Firmware Upgrade

This page lets you update the switch firmware.

Web Interface

To update switch firmware in the web UI:

1. Click Maintenance, Firmware and Firmware Upgrade.
2. Browse to and select the desired firmware file.
3. Click the Upload button.



Software Upload

Firmware File	Browse

□ Non-Stop PoE

Figure 24-4.1 Firmware Upgrade

Parameter descriptions:

Browse : Click to search for the Firmware URL and filename.

Non-Stop PoE : Check the box if you want the switch to keep providing PoE power to the PDs during the firmware upgrade process.

Upload : Click to upload the selected firmware file.

Firmware Selection

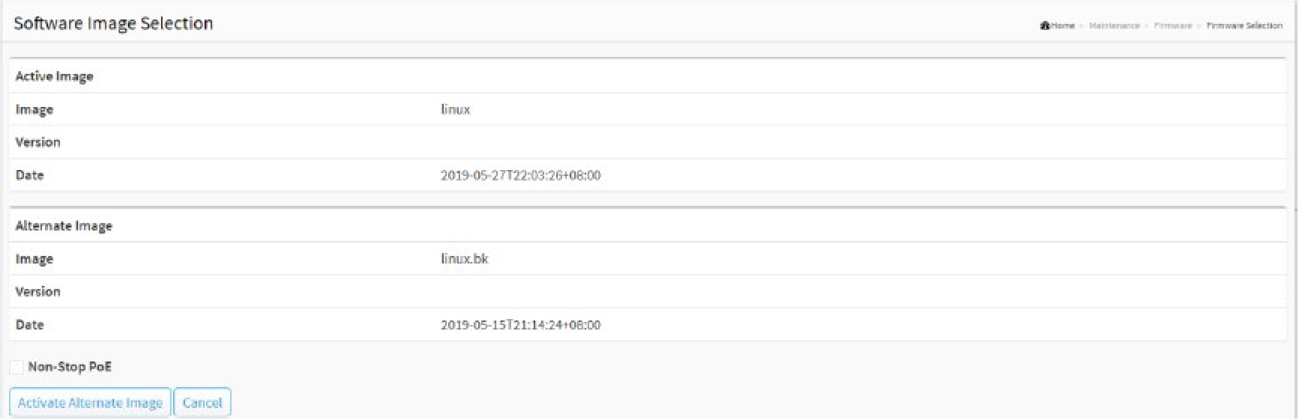
This page displays information about the active and alternate (backup) firmware images in the device, and lets you activate the alternate image.

The web page displays two tables with information about the Active and Alternate firmware images.

To show the firmware information or swap boot firmware in the web UI:

1. Click Maintenance, Firmware, and Firmware Selection to view firmware information.

2. Click the Activate Alternate Image button to swap firmware versions.



Software Image Selection

Active Image	
Image	linux
Version	
Date	2019-05-27T22:03:26+08:00

Alternate Image	
Image	linux.bk
Version	
Date	2019-05-15T21:14:24+08:00

□ Non-Stop PoE

Figure 24-4.2 Firmware Selection

Software Image Selection

Image : The file name of the firmware image, from when the image was last updated.

Version : The version of the firmware image.

Date : The date and time that the firmware was produced.

Buttons

Non-Stop PoE : Check the box if you want the switch to keep providing PoE power to the PDs during the firmware selection process.

Activate Alternate Image : Click to use the “Activate Alternate Image”. This button may be disabled depending on system state.

Cancel : Click to cancel activating the alternate image. Navigates away from this page.

26. Device Management System (DMS)

This chapter describes the integrated Device Management System (DMS) software that provides a unique set of value-added features and capabilities that provide lower overall cost, less downtime, and easier management and maintenance of the entire network.

DMS Features

Advanced Features

- Automatically discover and remotely configure attached IP-addressable powered devices (PDs)
- Establish and document a baseline deployment
- Graphical topology view for device management
- Floor view for device management (import JPEG design drawings)
- Google Maps™ view for device management
- Auto Power Reset (APR) monitors and automatically restarts edge devices
- Troubleshoot cable and IP connection issues
- Monitor and analyze traffic by Day/Week/Port/Device
- Perform health checks with thresholds
- Auto-Alarm on error conditions

Management

- Pop-up window interface
- Device Type, Device Name, MAC Address, IP Address, and PoE Wattage used by the PD
- Remotely log in, configure, monitor, and reboot PDs

Visibility

- Device-Management-System-Visibility
- Click to enlarge image
- Topology View provides end-to-end visibility of attached PDs with remote access into each device
- Floor View allows the designer to import existing JPEGs of the floor and site drawings into the DMS
- Google Maps™ View allows the PDs to be visible by State, City, and Street Address

Diagnostics

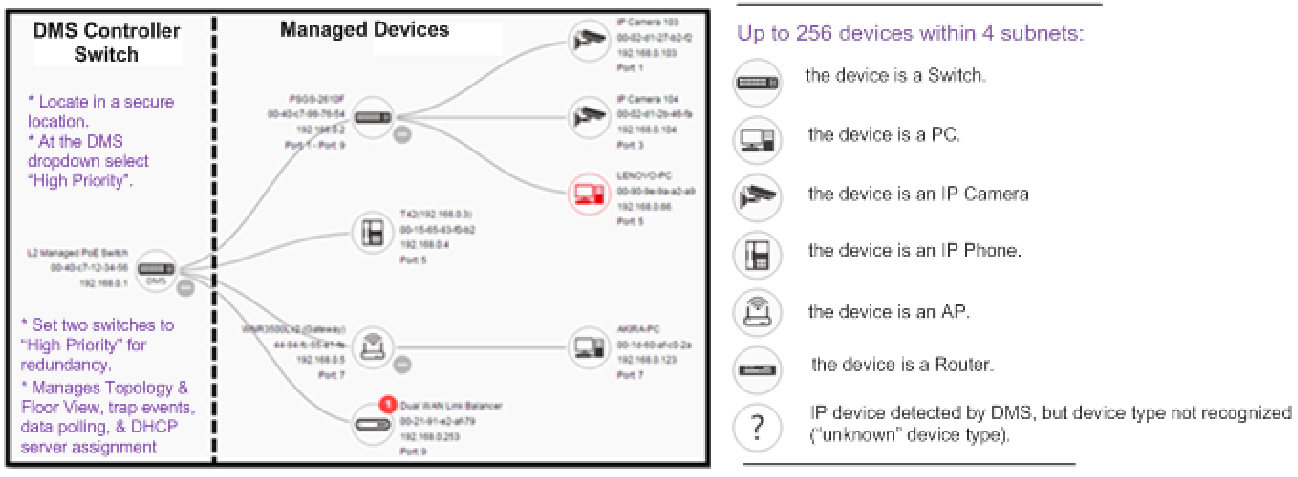
- One-click cable diagnostics
- One-click to check device alive
- Instant identification of faulty cable connections
- Convenient reboot of remote devices to resume operation

Monitoring

- Monitor traffic and packets of devices
- Analyze by day/week/port/device
- Perform health check by threshold
- Auto-alarm notification if an abnormal condition exists

DMS > DMS Mode

- Configure DMS mode and monitor device numbers/ DMS Controller Switch IP.
- DMS is controlled by the DMS Controller switch, as specified by the DMS Mode selection.
- The DMS Controller Switch controls syncing DMS information in order to manage Topology View, Floor View, and trap event / data polling / DHCP server assignment.

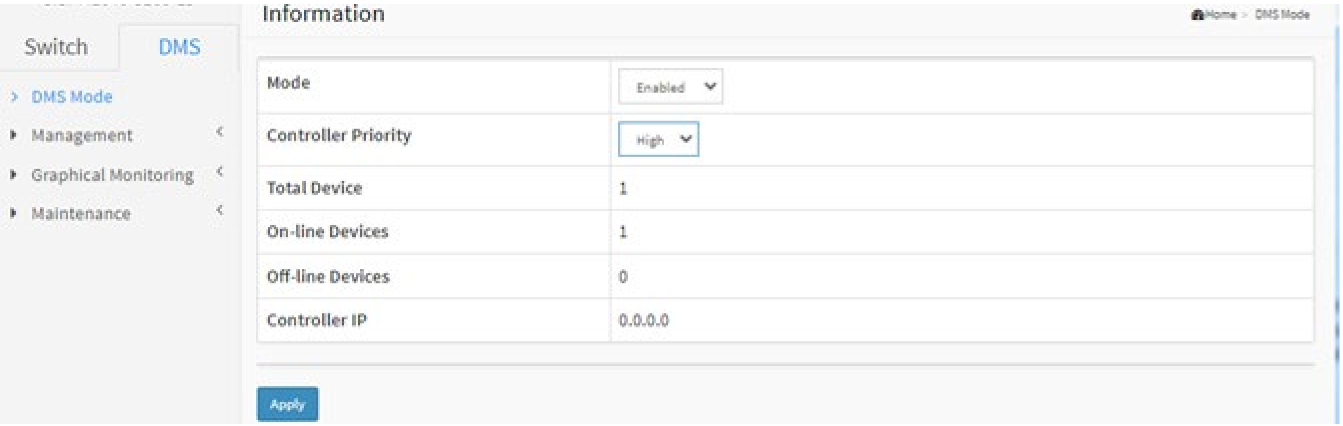

DMS Controller Switch
* Locate in a secure location.
* At the DMS dropdown select "High Priority".
L2 Managed PoE Switch
DMS
* Set two switches to "High Priority" for redundancy.
* Manages Topology & Floor View, trap events, data polling, & DHCP server assignment
Managed Devices
IP Camera 103
IP Camera 104
LENOVO-PC
AKIRA-PC
Dual WAN Link Balancer
Up to 256 devices within 4 subnets:
the device is a Switch.
the device is a PC.
the device is an IP Camera
the device is an IP Phone.
the device is an AP.
the device is a Router.
?
IP device detected by DMS, but device type not recognized ("unknown" device type).

1. If there are more than two switches set as High-priority or no High-priority mode switch, the Switch with the longer system uptime will be selected as the DMS Controller switch. If two switches have same up time, the switch with the smaller MAC address will be assigned as the DMS Controller Switch.
2. You can set two switches to High Priority for Controller Switch redundancy.
3. The DMS Controller Switch should be put in a secure location such as a server room, with access/authority limited to IT staff.
4. The DMS Controller Switch is the center of IP / Event management to operate the DMS:
   a. When enabled DHCP Server mode in DMS network, the DMS Controller switch is responsible for assigning IP address for all devices.

The DMS Controller Switch will Collect, Poll, and Sync DMS information, and act as the Event Notification control center to manage all device information.

DMS Information page

The DMS Information page lets you enable and disable DMS mode and specify DMS Controller Priority. DMS is controlled by the DMS Controller switch, as specified by the DMS Mode selection. The DMS Controller Switch controls syncing DMS information in order to manage Topology View, Floor View, and trap event / data polling / DHCP server assignment.



Information

Mode	Enabled
Controller Priority	High
Total Device	1
On-line Devices	1
Off-line Devices	0
Controller IP	0.0.0.0

Mode: At the dropdown select Enable or Disable the DMS function globally. The default is Enabled.

Controller Priority: At the dropdown select a "Controller Priority" when enabling DMS:

High: High priority; this switch will become the “Controller” (Master) switch.

Mid: Mid-level priority.

Low: Low level priority (default).

Non: the switch will never become the Controller switch (default).

Total Device: Displays the number of IP devices that are detected and displayed in Topology view.

On-Line Devices: Displays the number of IP devices on-line in Topology view.

Off-Line Devices: Displays the number of IP devices off-line in the topology view.

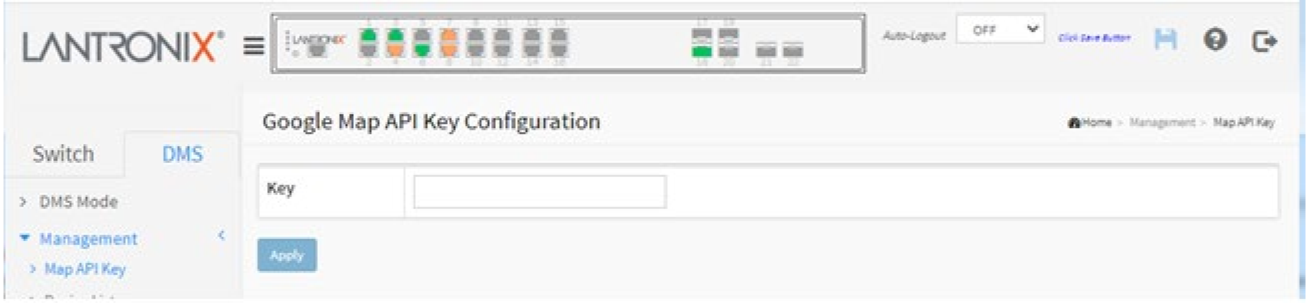
Controller IP: Displays the IP address of the Controller (Master) switch.

Apply: Click to save changes.

DMS > Management > Map API Key

You will need a valid API key and a Google Cloud Platform billing account to access Google core product. If not, DMS Map View will not be able to load Google Maps correctly.

Visit the Google website below and follow the directions to get an API key: https://developers.google.com/maps/documentation/directions/get-api-key.



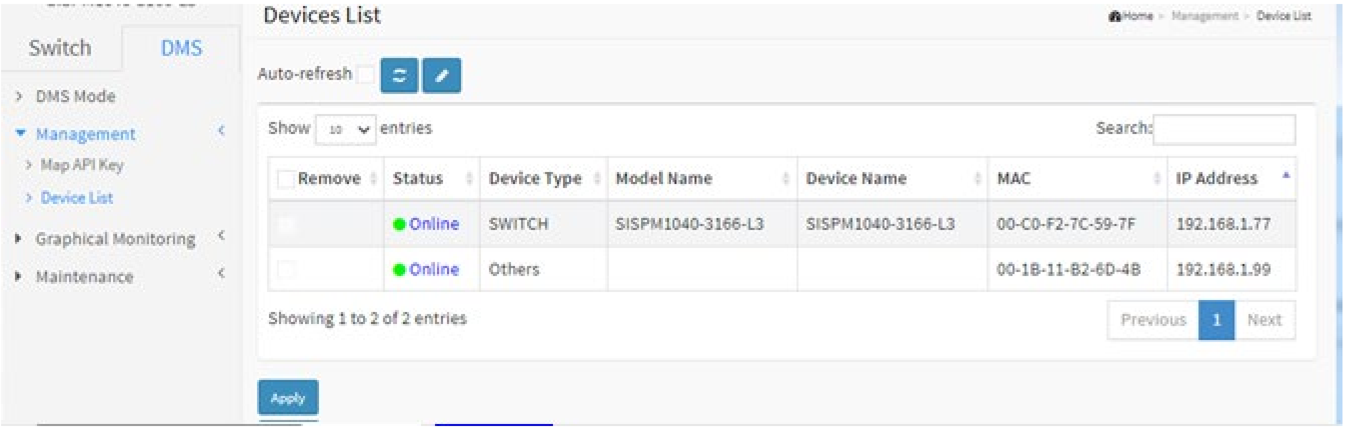
Key: Enter the Google API Key.

Buttons

Apply: Click to save changes.

DMS > Management > Device List

This page provides an overview of the devices list. It initially displays with seven columns:



Remove	Status	Device Type	Model Name	Device Name	MAC	IP Address
□	● Online	SWITCH	SISPM1040-3166-L3	SISPM1040-3166-L3	00-C0-F2-7C-59-7F	192.168.1.77
□	● Online	Others			00-1B-11-B2-6D-4B	192.168.1.99

Showing 1 to 2 of 2 entries

Remove: Remove off-line device from the list.

Status: Device Online or Offline. You can click the linked text to display the Maintenance > Diagnostics page.

Device Type: The type of the network connectivity devices such as PC, SWITCH, AP, IP Cam, IP Phone, or Others.

Model Name: The model name of the network connectivity devices.

Device Name: The device name of the network connectivity devices.

MAC: The mac address of the device.

IP Address: The IP address of the network connectivity devices.

Buttons

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

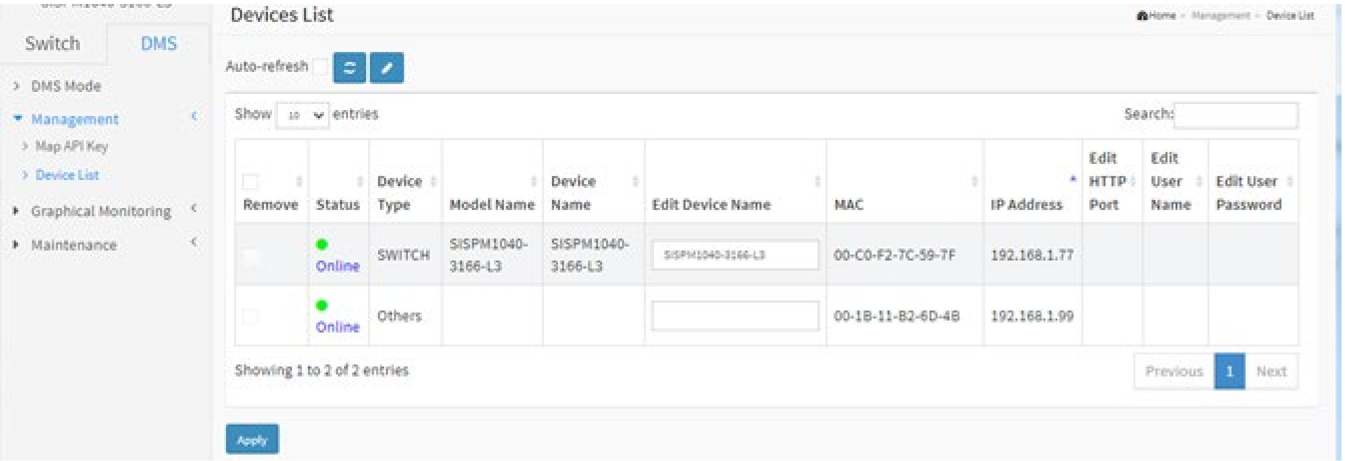
Refresh: Refreshes the displayed table starting from the input fields.

✎ **Edit Device Name**: Add the input fields for editing the device names and the http ports (see below).

Apply: Click to save changes.

Devices List with added input columns:

When you can click the ✎ **Edit Device Name** button, the Devices List page displays with four additional columns:



Devices List

Auto-refresh □

Show 10 entries Search:

Remove	Status	Device Type	Model Name	Device Name	Edit Device Name	MAC	IP Address	Edit HTTP Port	Edit User Name	Edit User Password
□	● Online	SWITCH	SISPM1040-3166-L3	SISPM1040-3166-L3	SISPM1040-3166-L3	00-C0-F2-7C-59-7F	192.168.1.77			
□	● Online	Others				00-1B-11-B2-6D-4B	192.168.1.99			

Showing 1 to 2 of 2 entries

Previous 1 Next

Apply

Edit Device Name: Entry field to edit a device's Name.

Edit HTTP Port: Entry field to edit a device's HTTP port number.

Edit User Name: Entry field to edit a device's user name.

Edit User Password: Entry field to edit a device's user password.

Buttons:

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

Refresh: Refreshes the displayed table starting from the input fields.

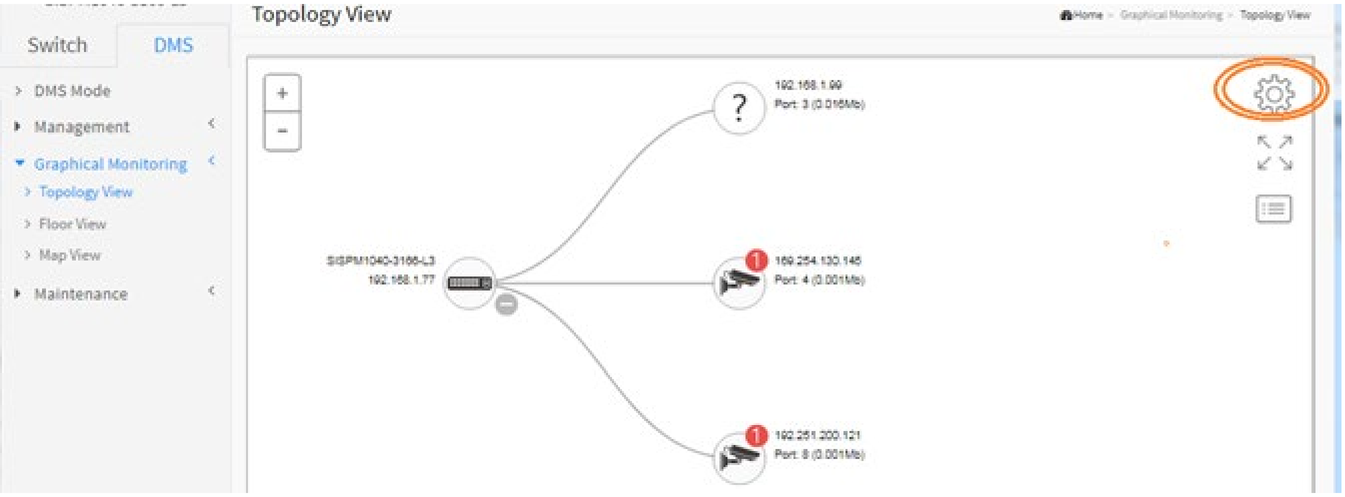
✎ **Edit Device Name**: Add the input fields for editing the device names and the http ports (see below).

Apply: Click to save changes.

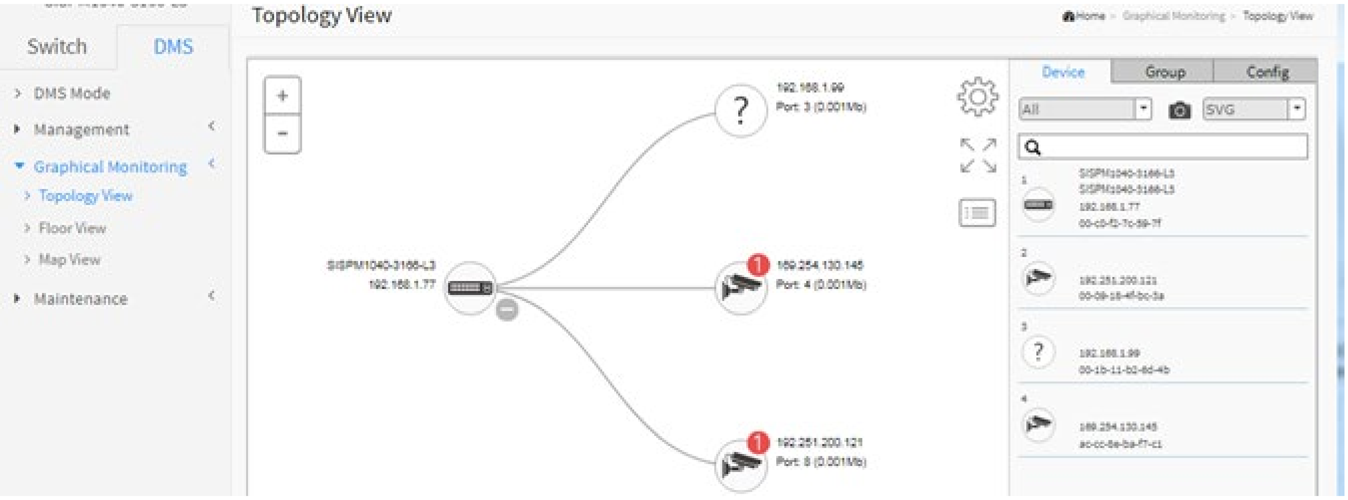
DMS > Graphical Monitoring > Topology View

DMS can automatically discover all IP devices and display the devices by graphic networking topology view. You can manage and monitor them in the Topology View, such as to remotely diagnose the cable connection status, auto alarm notifications on critical events, and remotely reboot a PoE device. You can use the DMS platform to solve the abnormal issues anytime and anywhere by tablet or smart phone, and keep the network works smoothly.

Click Graphical Monitoring > Topology View to see a visual representation of the network topology:



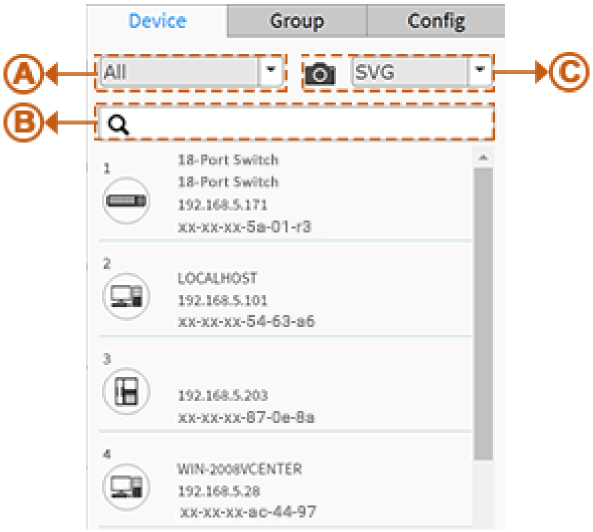
Click the Setting icon (⚙) to display additional right-hand menu items:



+ − : Icon with plus and minus marks to let you zoom in and zoom out the topology view. You can scroll up/down with mouse to achieve the same purpose.

⚙ In the upper right corner, there is a "Setting icon". When you click the icon, it will pop-up Device, Group, Config, export topology view and advanced search functions for the topology.

Device Search Console



1
18-Port Switch
18-Port Switch
192.168.5.171
xx-xx-xx-5a-01-r3

2
LOCALHOST
192.168.5.101
xx-xx-xx-54-63-a6

3
192.168.5.203
xx-xx-xx-87-0e-8a

4
WIN-2008VCENTER
192.168.5.28
xx-xx-xx-ac-44-97

Functions:

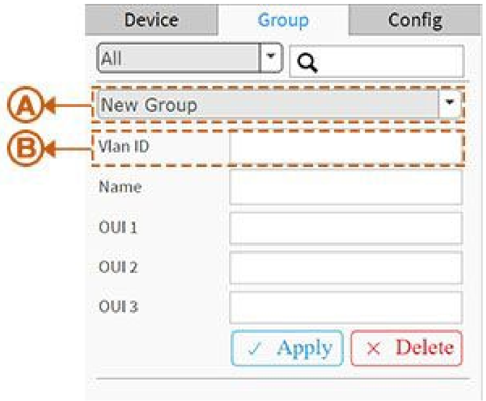
Ⓐ Filter devices by Device Type

Ⓑ Search devices by key words full text search

Ⓒ Save the whole View to SVG, PNG or PDF

Group Setting Console

- Uses MAC-based VLAN to isolate groups.
- One IP device only can join one VLAN group.

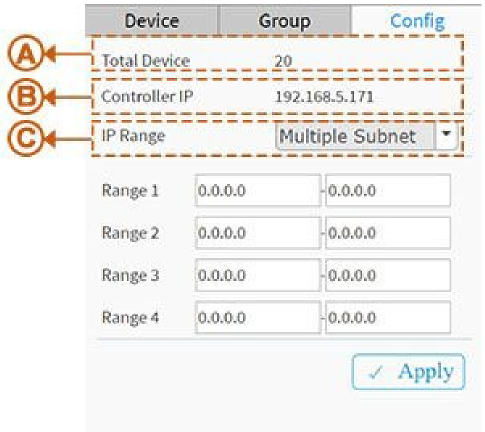


Functions:

Ⓐ Group devices by filtering, searching, clicking device icons, or specifying OUI.

Ⓑ Assign VLAN ID or Name to Group.

System Setting Console



Total Device 20

Controller IP 192.168.5.171

IP Range Multiple Subnet

Range 1	0.0.0.0	0.0.0.0
Range 2	0.0.0.0	0.0.0.0
Range 3	0.0.0.0	0.0.0.0
Range 4	0.0.0.0	0.0.0.0

Functions:

Ⓐ Shows how many IP devices are detected and displayed in Topology view.

Ⓑ Shows the Master IP.

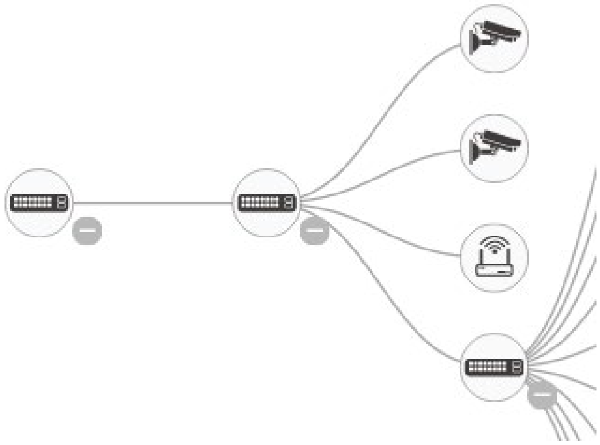
Ⓒ Single Subnet: DMS is based on the Master switch's IP address. Here the subnet means "255.255.255.0"

Multiple Subnet: Provides 4 ranges for inputting manually.(In this case, we suggest you adjust the switch subnet mask to "255.255.0.0" also to avoid IP devices that can't be recognized.)

Icon with screen view type: Click it to change to Full Screen View of Topology or return to the Normal View.

Icon with information list: Select what kind of information should be shown on the topology view of each device. Up to three items can be selected.

Device Tree View



Device Categories

The device is a Switch.

The device is a PC.

The device is an IP Camera.

The device is an IP Phone.

The device is an Access Point.

The device is a Router.

Icon with question mark: The IP device is detected by DMS, but the device type can't be recognized, and will be classified as an “Unknown” device type.

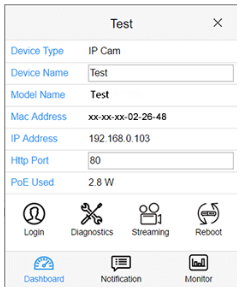
Device Status

Icon with black mark: Device link up. User can select function and check issues.

Icon with red mark: Device link down. User can diagnose the link status.

Icon with number: An event has occurred (e.g., Device Off-line, IP Duplicate, etc.) on the IP device. Click on the device icon to check Events in Notification.

Device Consoles



Test

Device Type	IP Cam
Device Name	Test
Model Name	Test
Mac Address	xx-xx-xx-02-26-48
IP Address	192.168.0.103
Http Port	80
PoE Used	2.8 W

Left-click any device icon to display the device consoles for further actions.

Dashboard Console: displays device info and related actions for the device.

Different device types support different function:

If an IP device is recognized as DMS switch, it will support "Upgrade" and "Find Switch" function.

If an IP device is recognized as PoE device, it will support more "Reboot" function in addition to "Upgrade".

If an IP device is recognized as IP Cam via ONVIF protocol, it will support "Streaming" function.

Device Type: Can be displayed automatically. If an unknown type is detected, you can still select type from a pre-defined list. Device Types include **PC** (General PC), **IP Camera** (General IP Cam), **IP Phone** (General IP Phone, Cisco SPA303), **AP** (General AP), and **Others** (Mobile Device, General Switch, Internet Gateway, IP PBX, NAS, Printer, NVR, VMS, Unknown Device).

Device Name: Create your own Device Name or alias for easy management, such as 1F_Lobby_Cam1.

Model Name, MAC Address, IP Address, Subnet Mask, Gateway, PoE Supply and PoE Used are displayed automatically by DMS.

HTTP Port: Re-assign HTTP port number to the device for better security.

Login

Login: Click the Login Action Icon to log in the device via HTTP for further configuration or status monitoring.

Upgrade

Upgrade: Click it to upgrade software version.

Find Switch

Find Switch: When this feature is activated, the switch LED will all lighten up and flicker for 15 seconds.

Diagnostics

Diagnostics: Click Diagnostic Action Icon to perform the cable diagnostics, to examine where the broken cable is, and check if the device connection is alive or not by ping.

- **Cable Status:**
  - **Green icon:** Cable is connected correctly.
  - **Red icon:** Cable is not connected correctly. User can check the distance info (XX meters) to identify the broken cable location.
- **Connection:**
  - **Green icon:** Device is pinged correctly.
  - **Red icon:** Device is not transmitted /receiving data correctly. Which means it might not be pinged successfully.

Reboot

Reboot: Click Reboot Action Icon to reboot the device remotely so as recover the device back to its normal operation.

Streaming

Streaming: Click Streaming Action Icon to display the video images streaming if the device supports this feature.

Parent Node

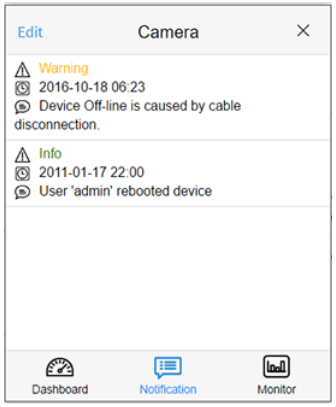
Parent Node: When DMS switch detects more than two IP devices from the same port, switch can't resolve this IP device's layout, instead, it will show a blank node to present this situation. User can use "Parent Node" function to adjust layout in Dashboard.

Notification Console: Displays alarms and logs triggered by events. For example:

Warning: <date> Device Off-line is caused by cable disconnection.

Info <date> User 'admin' rebooted device

No Message

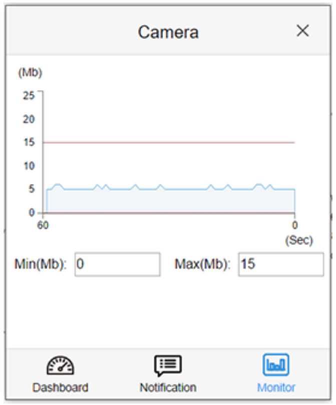


Warning
2016-10-18 06:23
Device Off-line is caused by cable disconnection.

Info
2011-01-17 22:00
User 'admin' rebooted device

Monitor Console: It displays the traffics for device health check purpose.

- For each IP device except DMS switches, you can set a threshold of throughput for IP devices, and get notification when throughput is lower or higher than settings.
- If both values are "0", it means the function is disabled.
- Polling interval is 1 second; when the page is closed, the Polling interval will change to around 5 seconds.

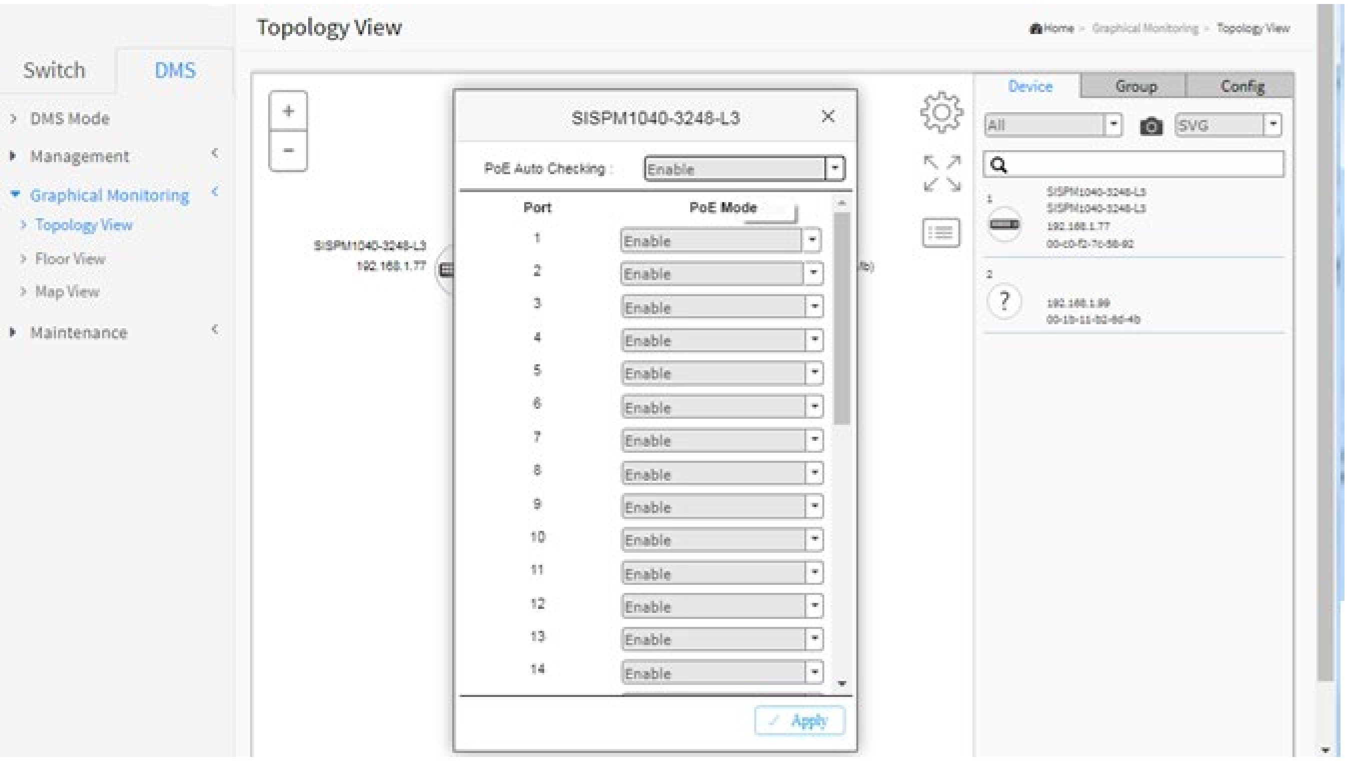


Min(Mb): 0 Max(Mb): 15

PoE Auto Checking "AutoFill" Feature

When you enable Auto power reset (PoE auto checking) in DMS, the IP addresses of the connected devices are automatically filled on the Auto Power Reset configuration page.

1. Configure the "PoE Auto Checking" parameter at Switch > PoE Management > PoE Auto Checking. The default value of the "Failure Action" parameter is "Reboot Remote PD". Note that "PoE Auto Checking" is called "PoE Auto Power Reset" in earlier firmware versions.
2. Configure PoE parameters at DMS > Graphical Monitoring > Topology View. Left click on the switch icon to display its device configuration popup. Click the PoE Config (PoE Config) icon to display the PoE Auto Checking pane:



SISPM1040-3248-L3

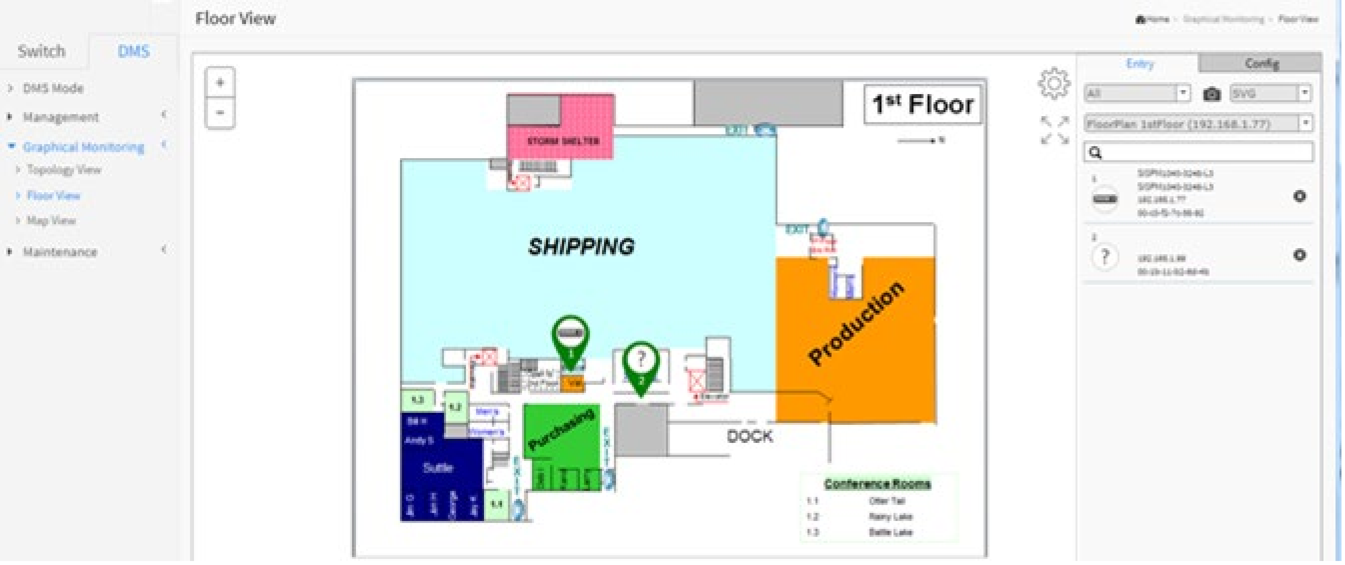
PoE Auto Checking : Enable

Port	PoE Mode
1	Enable
2	Enable
3	Enable
4	Enable
5	Enable
6	Enable
7	Enable
8	Enable
9	Enable
10	Enable
11	Enable
12	Enable
13	Enable
14	Enable

DMS > Graphical Monitoring > Floor View

This page displays the graphical image created at DMS > Maintenance > Floor Image. Initially, no Floor View images are displayed. Go to DMS > Maintenance > Floor Image to upload floor images.

The Floor View lets you easily plan IP devices installation locations by dragging the uploaded floor images into place.



+ −

Icon with plus and minus marks: Zoom in and zoom out the floor view, user can scroll up/down with mouse to achieve the same purpose.

⚙ There is a "Setting icon" in the upper right corner. When you click the icon, it will pop-up Device, Config, export floor view and advanced search functions for the device. You can click it again to hide the functions.

↖ ↗ ↙ ↘ Icon with screen view type: Click it to change to Full Screen view of Floor or return to the Normal View.

Device Search Console

Functions:

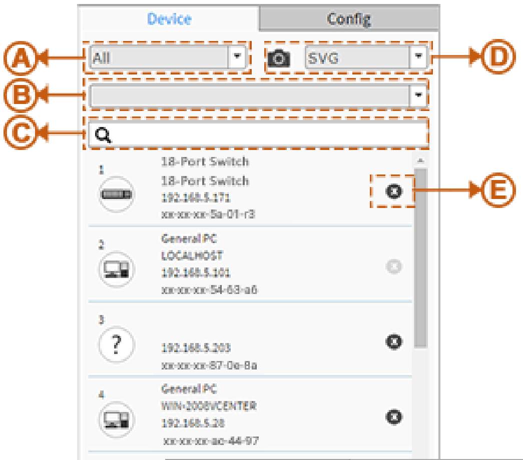
A. Filter devices by Device Type

B. Select floor images

C. Search devices by key words full text search

D. Save the whole View to SVG, PNG or PDF

E. Remove a device from all floor view images



1
18-Port Switch
18-Port Switch
192.168.5.171
xx-xx-xx-5a-01-r3

2
General PC
LOCALHOST
192.168.5.101
xx-xx-xx-54-63-a6

3
192.168.5.203
xx-xx-xx-87-0e-8a

4
General PC
WIN-2008VCENTER
192.168.5.28
xx-xx-xx-ac-44-97

System Setting Console

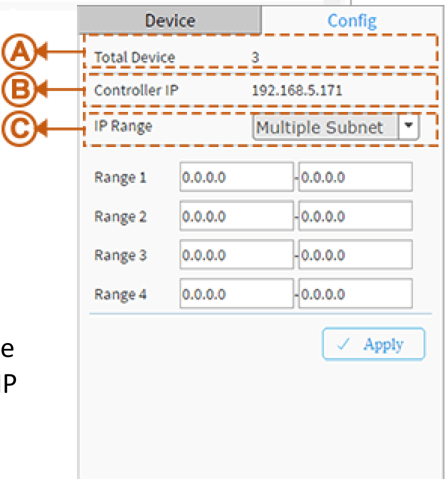
Functions:

A. Shows how many IP devices are detected and displayed in the topology view.

B. Shows the Master switch's IP address.

C. Single Subnet: DMS will base on the master switch's IP address. Here the subnet means "255.255.255.0".

Multiple Subnet: To provide 4 ranges for inputting manually. (In the case, we suggest you adjust the switch's subnet mask to "255.255.0.0" also to avoid IP devices that can't be recognized.)



Total Device 3

Controller IP 192.168.5.171

IP Range Multiple Subnet

Range 1 0.0.0.0 0.0.0.0

Range 2 0.0.0.0 0.0.0.0

Range 3 0.0.0.0 0.0.0.0

Range 4 0.0.0.0 0.0.0.0

Floor View

- Anchor devices onto Floor Maps
- Find device location instantly
- 10 Maps can be stored per Switch
- IP Surveillance/VoIP/WiFi applications
- Other features same as Topology View
- To place and remove a device icon:
  - Select a device and click its icon from the device list.
  - The device icon will show on the floor image's default location.
  - Click and hold left mouse to drag-and-drop the icon to the correct location on the Floor View.
  - Click cross sign on the right side of device icon to remove a device from all Floor View images.

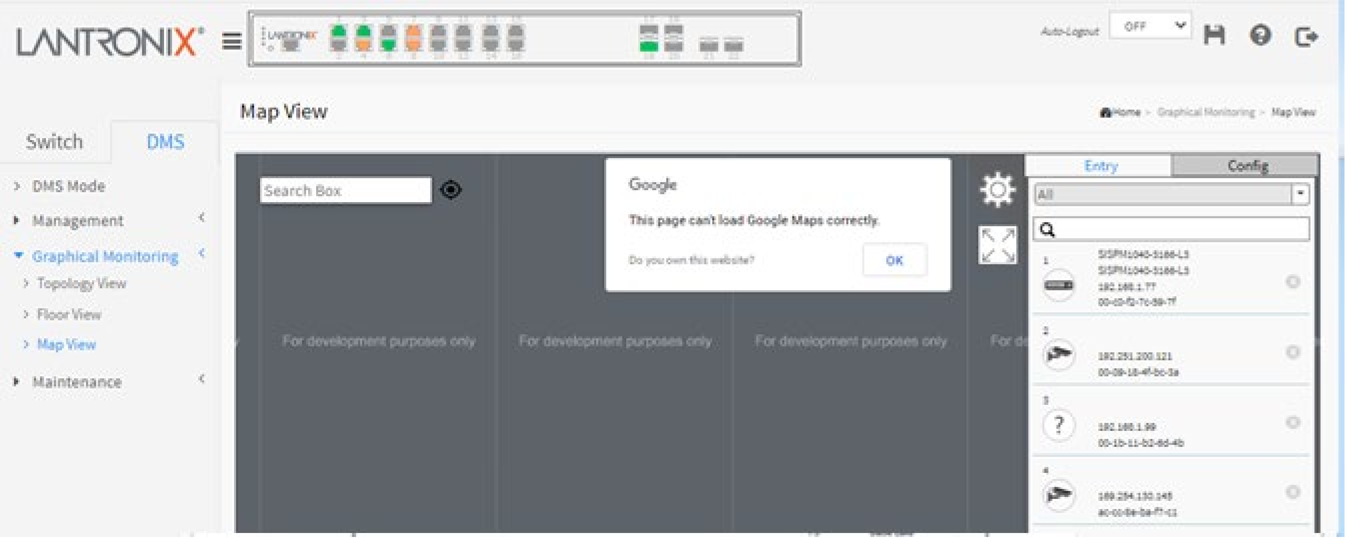
Device Status

Icon with black mark: Device link up. User can select function and check issues.

Icon with red mark: Device link down. User can diagnose the link status.

DMS > Graphical Monitoring > Map View

This page helps you find the location of devices even when they are installed in a different building. You can place a device icon on the Map View and navigate using Google Maps. You need a valid API key and a Google Cloud Platform billing account to access a Google core product. If not, DMS Map View will not be able to load Google Maps correctly. See DMS > Management > Map API Key on page 420.



Google

This page can't load Google Maps correctly.

Do you own this website?

1 SISPM1040-3166-L3 SISPM1040-3166-L3 192.168.1.77 00-c0-f2-7c-59-7f

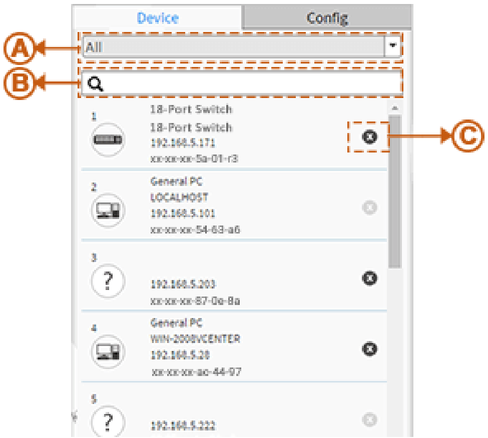
2 192.251.200.121 00-09-18-4f-bc-3a

3 192.168.1.99 00-1b-11-b2-6d-4b

4 169.254.130.145 ac-cd-6e-ba-f7-c1

There is a "Settings icon in the upper right corner. When you click the icon, it will pop-up Device, Config, export floor view and advanced search functions for the device.

1. Device Search Console



1 18-Port Switch 18-Port Switch 192.168.5.171 xx-xx-xx-5a-01-r3

2 General PC LOCALHOST 192.168.5.101 xx-xx-xx-54-63-a6

3 192.168.5.203 xx-xx-xx-87-0e-8a

4 General PC WIN-2008VCENTER 192.168.5.28 xx-xx-xx-ac-44-97

5 192.168.5.222

Function:

A. Filter devices by Device Type

B. Search devices by key words full text search

C. Remove a device from Map view

2. System Setting Console

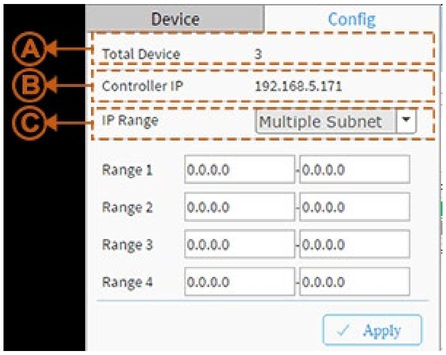
Function:

A. Shows how many IP devices are detected and displayed in the topology view.

B. Shows the Master switch IP address.

C. Single Subnet: DMS will base on the master switch's IP address. Here the subnet means "255.255.255.0".

Multiple Subnet: To provide 4 ranges for inputting manually.(In the case, we will suggest user to adjust switch's subnet mask to "255.255.0.0" also to avoid IP devices can't be recognized.)



Total Device 3

Controller IP 192.168.5.171

IP Range Multiple Subnet

Range 1	0.0.0.0	0.0.0.0
Range 2	0.0.0.0	0.0.0.0
Range 3	0.0.0.0	0.0.0.0
Range 4	0.0.0.0	0.0.0.0

↖ ↗ ↙ ↘ Icon with screen view type: Click it to change to Full Screen View of the Map View page or return to the Normal View.

Map View

- Anchor Devices onto Google Maps.
- Find Devices Instantly from Map View.
- On-Line Search Company/Address.
- Outdoor IP Cam/WiFi Applications.
- Other Features same as Topology View
- To place and remove a device icon
  - Select a device and click its icon from the device list.
  - The device icon will show on the map's default location.
  - Click and hold left mouse to drag-and-drop the icon to the correct location on the Map View.
  - Click the cross sign on the right side of device icon to remove a device from Map View.

Device Status

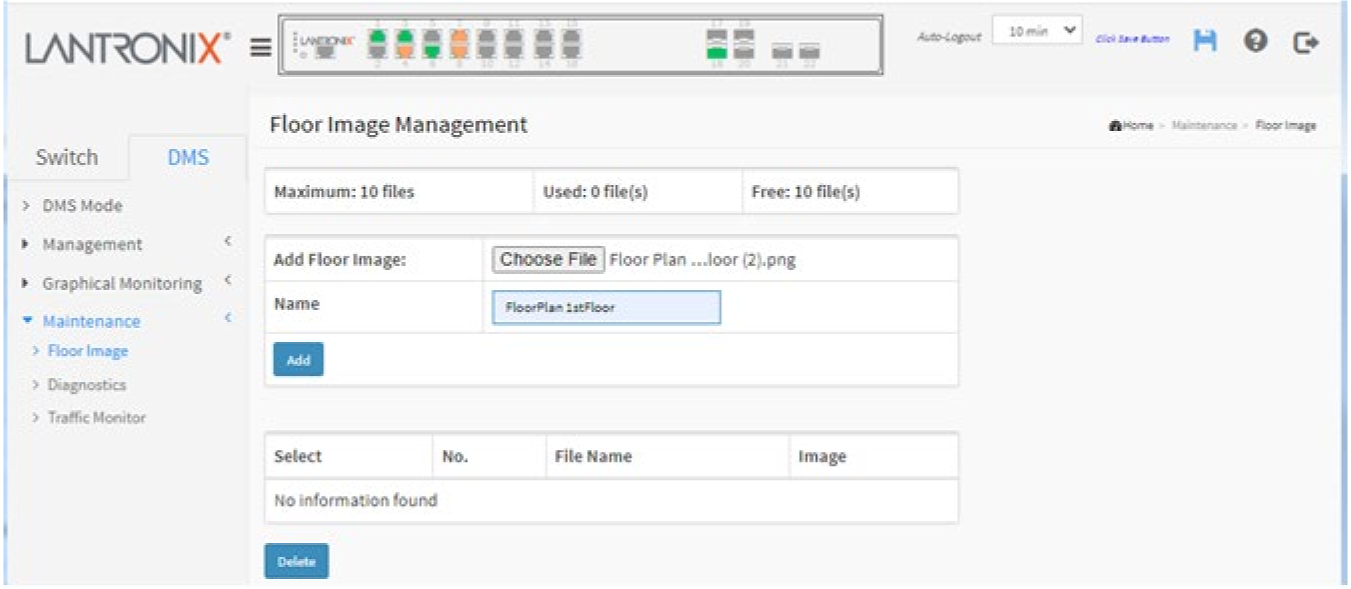
Icon with black mark: Device link up. You can select functions and check issues.

Icon with red mark: Device link down. You can diagnose the link status.

Message: *This page can't load Google Maps correctly.*
Recovery: See DMS > Management > Map API Key on page 420.

DMS > Maintenance > Floor Image

This page lets you upload and manage floor map images. You can upload up to 20 JPEG or PNG images, each a maximum of 256KB in size.



Floor Image Management

Maximum: 10 files	Used: 0 file(s)	Free: 10 file(s)

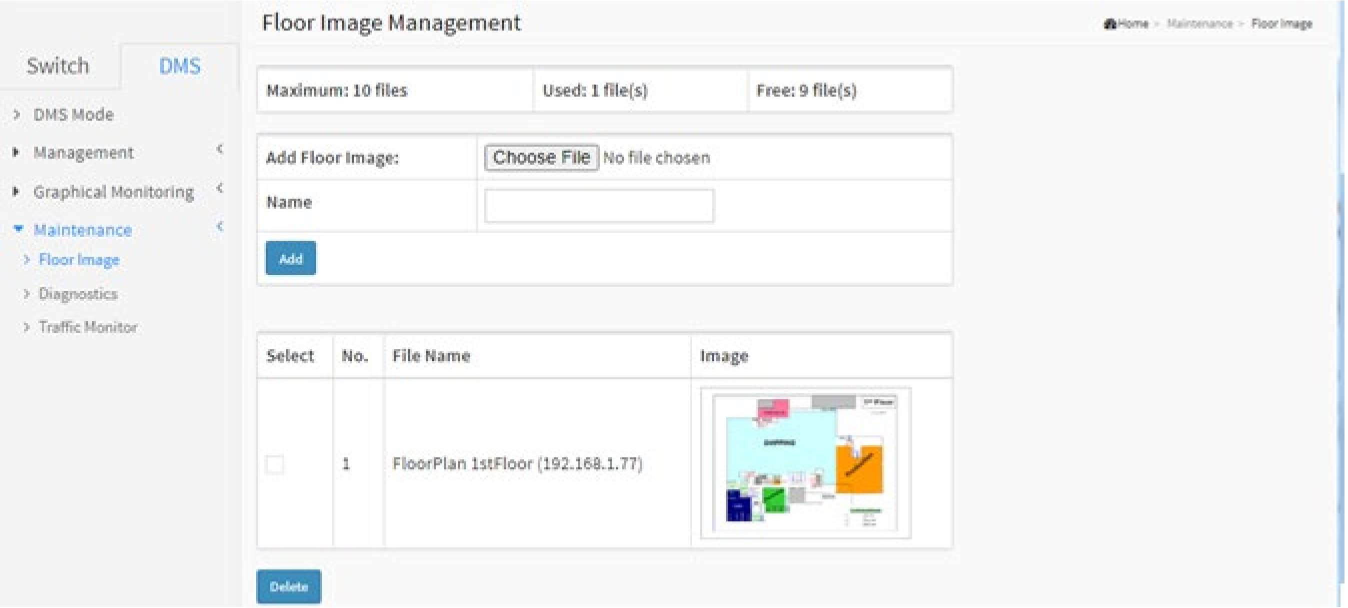
Add Floor Image:	Choose File Floor Plan ...loor (2).png
Name	FloorPlan 1stFloor

Add

Select	No.	File Name	Image
No information found			

Delete

1. At the default Floor Image Management page click the Choose File icon.
2. Navigate to and select a JPEG or PNG image.
3. Enter a Name and click the Add button to display the selected image:



Floor Image Management

Maximum: 10 files	Used: 1 file(s)	Free: 9 file(s)

Add Floor Image:	Choose File No file chosen
Name	

Add

Select	No.	File Name	Image
□	1	FloorPlan 1stFloor (192.168.1.77)	

Delete

Select : Check the checkbox to select an image from the list.

No.: Floor Image instance number (maximum 10 image files).

File Name : Displays the file name information (e.g., *Floor Plan - 1st Floor (192.168.1.77)*).

Image: Displays a thumbnail of the floor image.

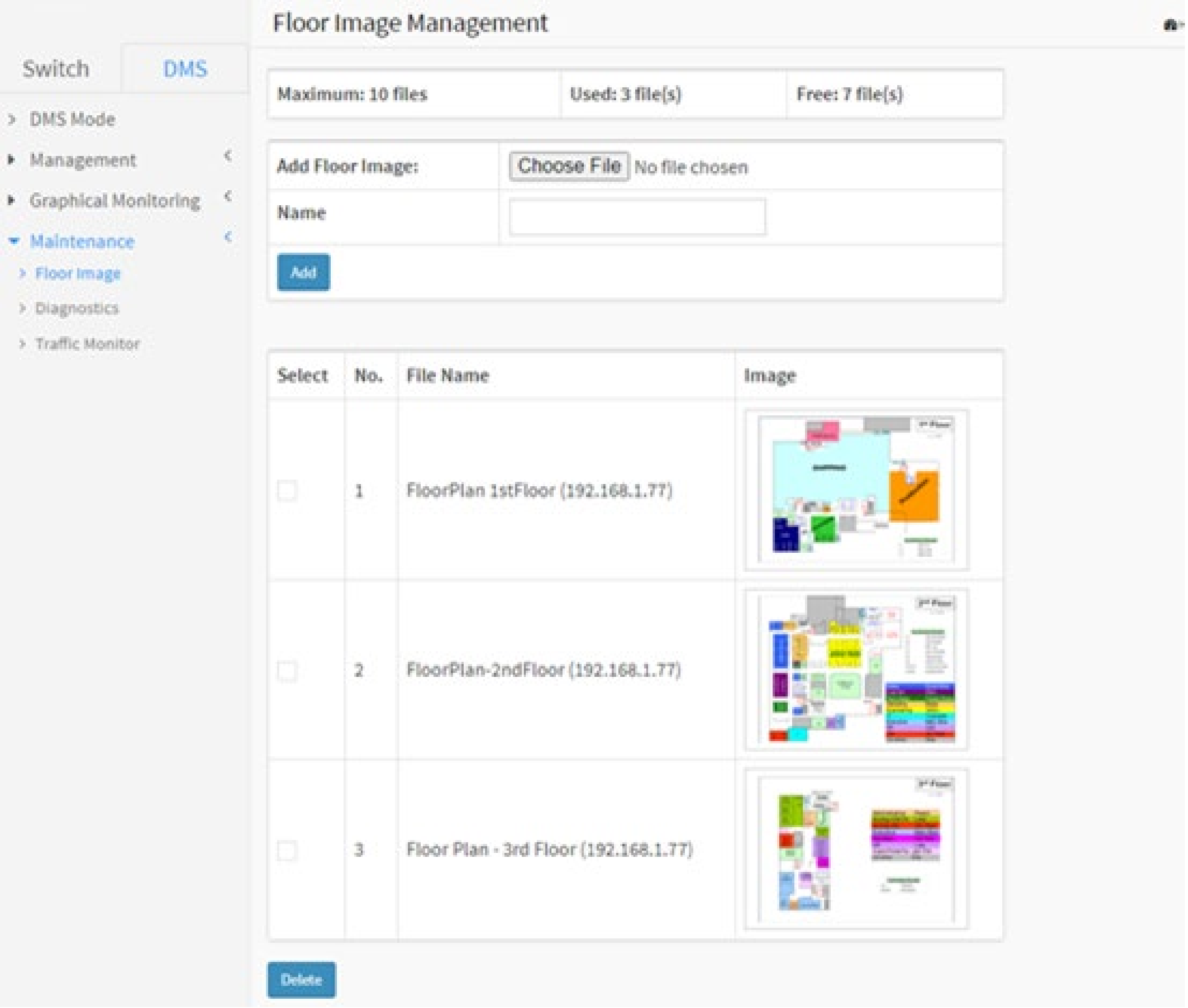
Buttons

Add: Click Add to upload. When done, a snapshot will be available on screen.

Delete: If you need to remove an existing floor map, select its checkbox and click Delete to remove.

Messages: *Only jpg, png are allowed* displays if you selected a file type other than JPG or PNG. Click OK to clear the message and select a PNG or JPG file.

Example:



Floor Image Management

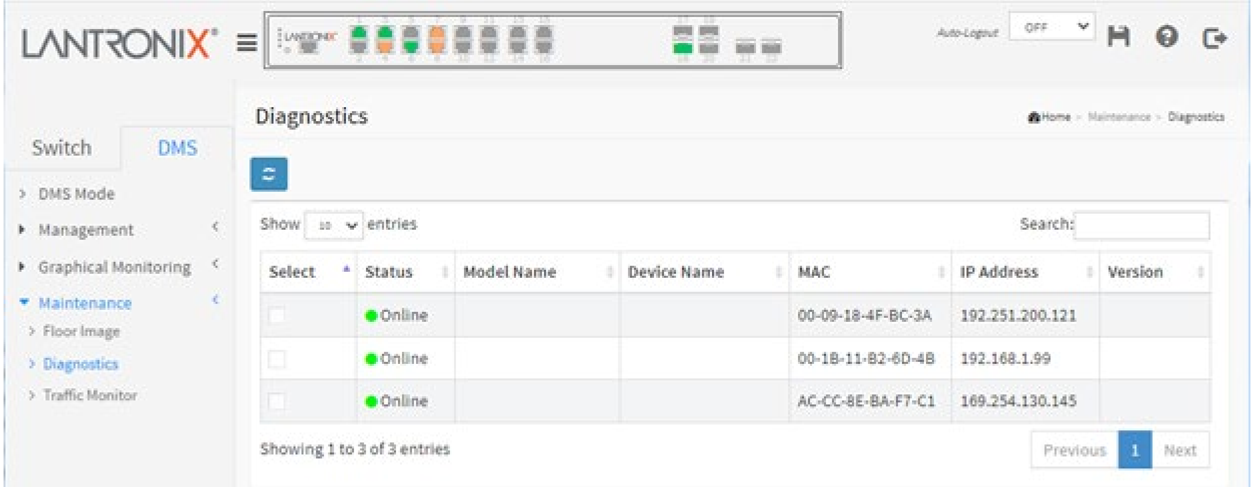
Maximum: 10 files	Used: 3 file(s)	Free: 7 file(s)

Add Floor Image:	Choose File No file chosen
Name	

Select	No.	File Name	Image
□	1	FloorPlan 1stFloor (192.168.1.77)	
□	2	FloorPlan-2ndFloor (192.168.1.77)	
□	3	Floor Plan - 3rd Floor (192.168.1.77)	

DMS > Maintenance > Diagnostics

This page lets you run a diagnostic test on a selected device.



Diagnostics

Show 10 entries Search:

Select	Status	Model Name	Device Name	MAC	IP Address	Version
□	● Online			00-09-18-4F-BC-3A	192.251.200.121	
□	● Online			00-1B-11-B2-6D-4B	192.168.1.99	
□	● Online			AC-CC-8E-BA-F7-C1	169.254.130.145	

Showing 1 to 3 of 3 entries

Previous 1 Next

Select: Select an on-line device from the list. The diagnostic test starts.

Status: Device Online or Offline.

Model Name: The model name of the network connectivity devices.

Device Name: The device name of the network connectivity devices.

MAC: The mac address of the device.

IP Address: The IP address of the network connectivity devices.

Version: The Version of the network connectivity devices.

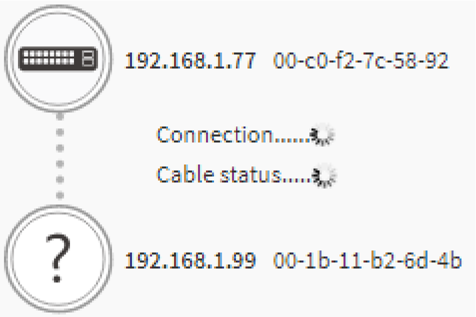
Buttons

Refresh: Refreshes the displayed table starting from the input fields.

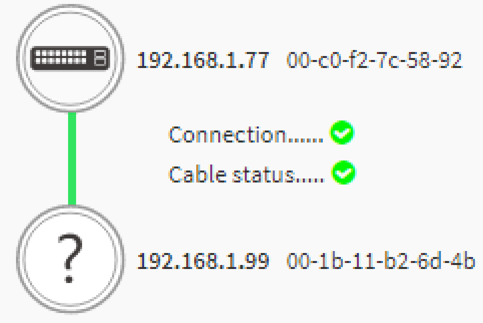
Show x entries: At the dropdown select the number of devices to display per page.

Search: Enter a key word to search for.

Another Try: When a diagnostic test completes, click the button to clear the page and run another diagnostic test.

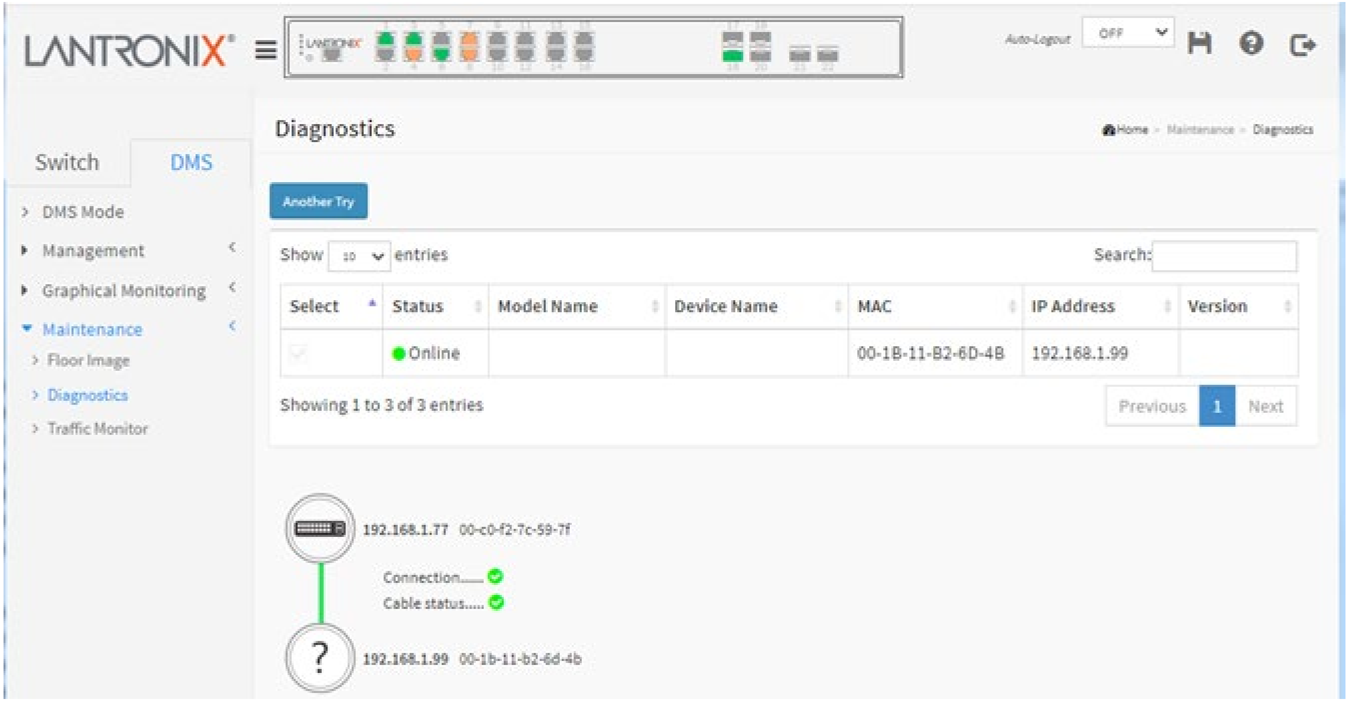

192.168.1.77 00-c0-f2-7c-58-92
Connection......
Cable status.....
?
192.168.1.99 00-1b-11-b2-6d-4b

Diagnostic In process


192.168.1.77 00-c0-f2-7c-58-92
Connection...... ✓
Cable status..... ✓
?
192.168.1.99 00-1b-11-b2-6d-4b

Diagnostic Completed

Example



Diagnostics

Select	Status	Model Name	Device Name	MAC	IP Address	Version
□	● Online			00-1B-11-B2-6D-4B	192.168.1.99	

Showing 1 to 3 of 3 entries

192.168.1.77 00-c0-f2-7c-59-7f

Connection...... ✓

Cable status..... ✓

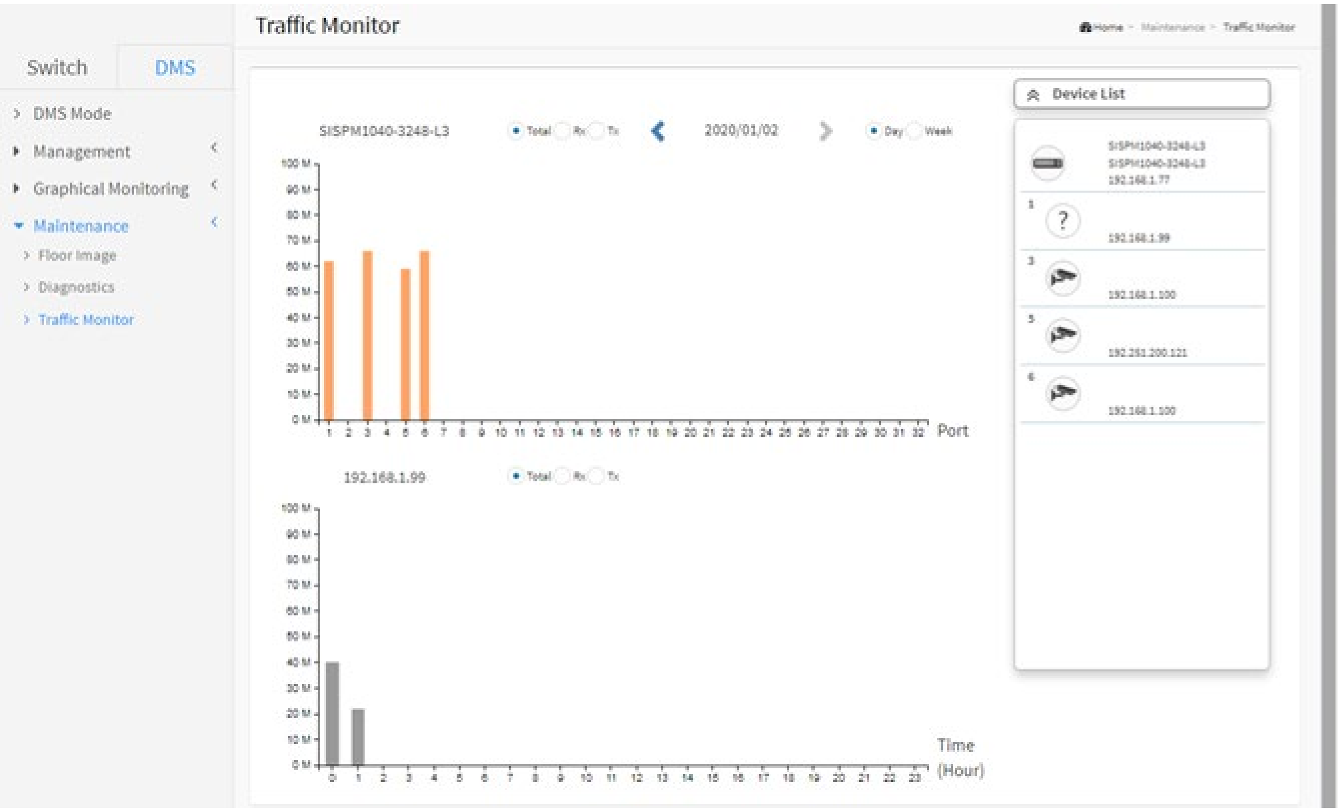
192.168.1.99 00-1b-11-b2-6d-4b

DMS > Maintenance > Traffic Monitor

This page displays a visual chart of network traffic of all the devices. Numbers are shown in Mbit/s.

To view the traffic of all the ports or just a specific port; click on a specific port on the traffic chart to reveal its traffic during the day.

You can select to display a summary of a day's or a week's traffic by selecting the check circle on top. The same applies to the selection of Rx Tx traffic. A single port's traffic is shown at the lower half of the screen.



SISPM1040-3248-L3 ● Total ○ Rx ○ Tx < 2020/01/02 > ● Day ○ Week

192.168.1.99 ● Total ○ Rx ○ Tx

Device List:

SISPM1040-3248-L3
SISPM1040-3248-L3
192.168.1.77

1 ? 192.168.1.99

3 192.168.1.100

5 192.251.200.121

6 192.168.1.100

● Total ○ Rx ○ Tx

Total / Rx / Tx: Select the set of data to be displayed. The default is Total.

< 2011/01/04 > ● Day ○ Week

< yy/mm/dd >: Select the date of data displayed.

Day / Week: Select a day’s worth of data or a week’s worth of data to be displayed.

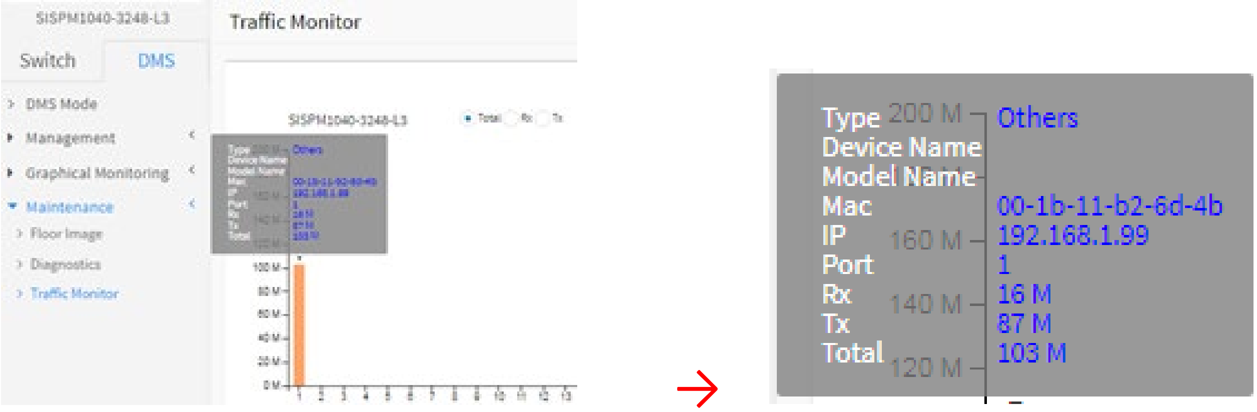
Device List: Displays the set of discovered devices.

Throughput: Vertical axis shows the device throughput (e.g., 0 M-18000 M or 0 M-1200 M).

Port: Horizontal axis shows the switch port numbers.

Time (Hour): Horizontal axis shows the time elapsed in hours (0-23).

Hover the mouse cursor over a column in the table to display its specific parameters:



Type Others
Device Name
Model Name
Mac 00-1b-11-b2-6d-4b
IP 192.168.1.99
Port 1
Rx 16 M
Tx 87 M
Total 103 M

Message: “*Traffic Monitor feature is only available on master switch*” added at FW v8.40.1523.

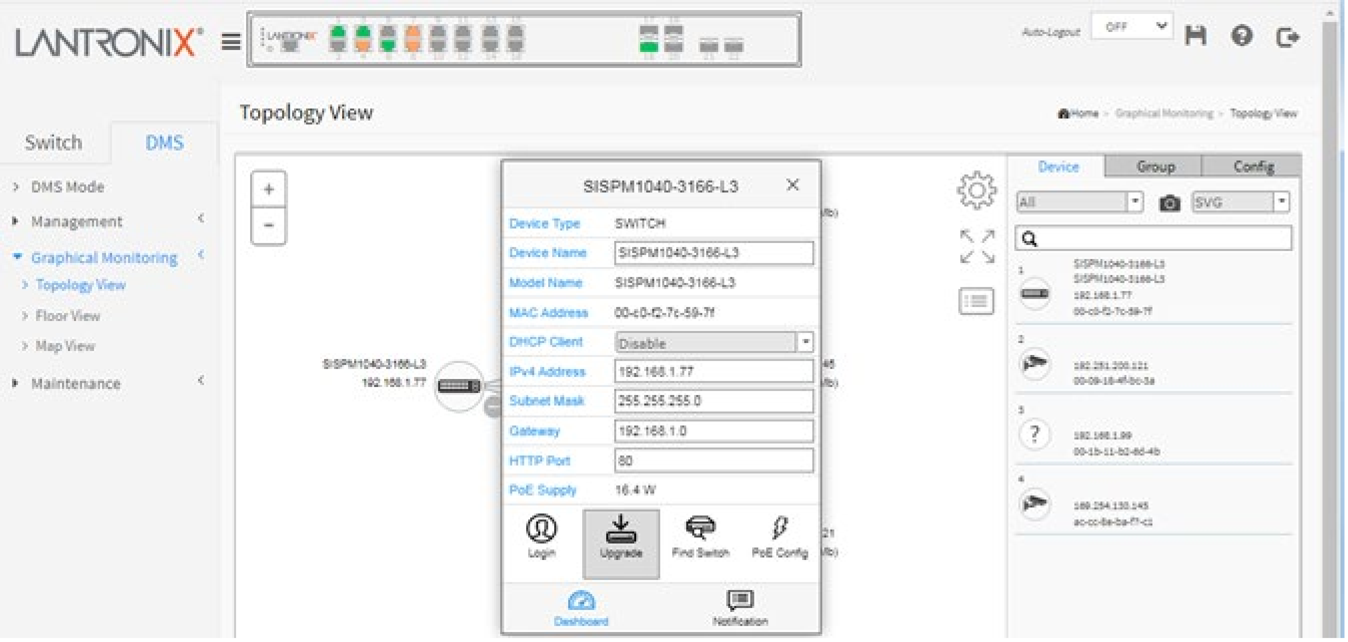
Meaning: You clicked on “Traffic Monitor” at DMS > Traffic Monitor, but this switch is not the DMS Controller (Master) Switch.

Recovery: Either make this switch the DMS Controller (Master) Switch or use the designated DMS Controller (Master) Switch for traffic monitoring. See “DMS Information page” on page 419.

DMS Firmware Upgrade Procedure

To upgrade a device's firmware via DMS:

1. Navigate to the DMS > Graphical Monitoring > Topology View menu path.
2. Click the ⚙ button to display the right pane menu tabs (Device, Group, and Config).
3. Connect all switches and make sure DMS is working.
   - Set all switches with different IP addresses and in the same IP segment.
   - Make sure gateway IP address is configured.
4. Left-click the desired device icon to display the options:



SISPM1040-3166-L3

Device Type	SWITCH
Device Name	SISPM1040-3166-L3
Model Name	SISPM1040-3166-L3
MAC Address	00-c0-f2-7c-59-7f
DHCP Client	Disable
IPv4 Address	192.168.1.77
Subnet Mask	255.255.255.0
Gateway	192.168.1.0
HTTP Port	80
PoE Supply	16.4 W

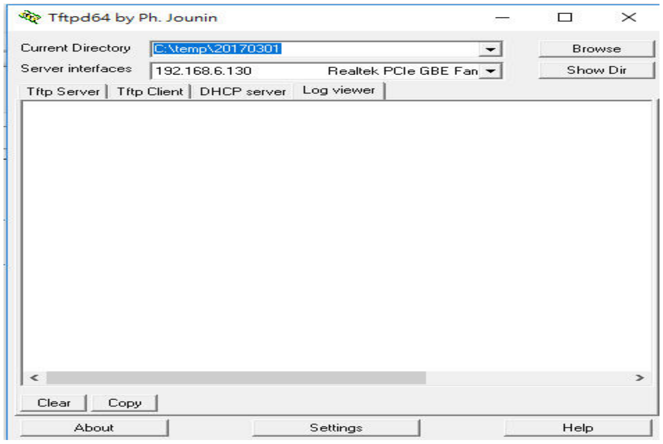
1 SISPM1040-3166-L3 SISPM1040-3166-L3 192.168.1.77 00-c0-f2-7c-59-7f

2 192.251.200.121 00-09-18-4f-bc-3a

3 192.168.1.99 00-1b-11-b2-6d-4b

4 169.254.130.145 ac-cc-8a-ba-f7-c1

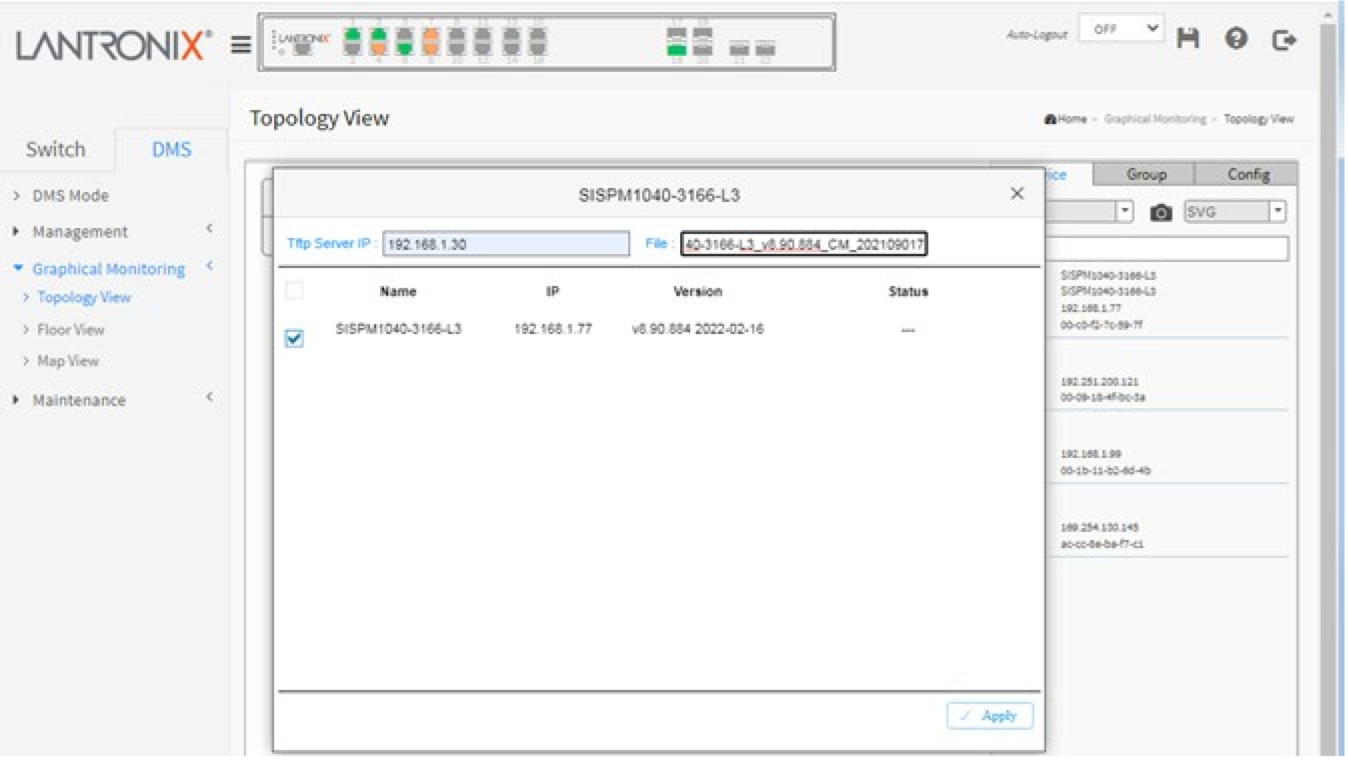
5. Enable the TFTP server and set the correct image path.



Current Directory C:\temp\20170301

Server interfaces 192.168.6.130 Realtek PCIe GBE Fan

6. Click the switch icon, and then click the "Upgrade" button in the Dashboard.
7. Enter the TFTP server IP address and FW file name and select the switch on which you want to upgrade the FW.

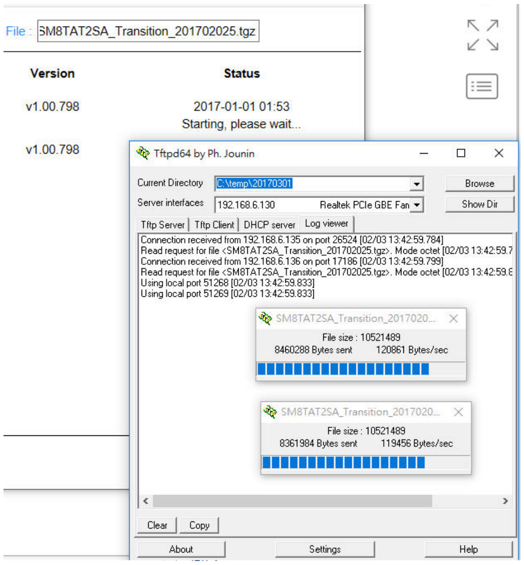


SISPM1040-3166-L3

Tftp Server IP : 192.168.1.30 File : 40-3166-L3_v8.90.884_CM_202109017

□	Name	IP	Version	Status
☑	SISPM1040-3166-L3	192.168.1.77	v8.90.884 2022-02-16	---

8. Click “Apply” to start the FW upgrade and save to Running-config.
9. Observe the upgrade status until completion.



File : SM8TAT2SA_Transition_201702025.tgz

Version	Status
v1.00.798	2017-01-01 01:53 Starting, please wait...
v1.00.798	

Current Directory: C:\temp\20170301

Server interfaces: 192.168.6.130 Realtek PCIe GBE Fan

```
Connection received from 192.168.6.135 on port 26524 [02/03 13:42:59.784]
Read request for file <SM8TAT2SA_Transition_201702025.tgz>. Mode octet [02/03 13:42:59.7
Connection received from 192.168.6.136 on port 17186 [02/03 13:42:59.799]
Read request for file <SM8TAT2SA_Transition_201702025.tgz>. Mode octet [02/03 13:42:59.8
Using local port 51268 [02/03 13:42:59.833]
Using local port 51269 [02/03 13:42:59.833]
```

SM8TAT2SA_Transition_2017020...
File size : 10521489
8460288 Bytes sent 120861 Bytes/sec

SM8TAT2SA_Transition_2017020...
File size : 10521489
8361984 Bytes sent 119456 Bytes/sec

Messages

Starting, please wait…

Error : Firmware download fail

DMS Troubleshooting

Problem: The switch lists itself as the only device in Topology View of DMS.

Problem: In DMS, the Local image shows the IP address of another switch.

Description: The switch is listed as only device in DMS Topology View in DMS; all devices are listed in DMS device list. This is usually because the switch's gateway is not configured appropriately.

Resolution: An IP Route must be configured manually. For example, a switch IP address of 192.168.1.77 should have the following IP route configured: ip route 0.0.0.0 0.0.0.0 192.168.1.x. Without the IP route configured, you may be unable to view all devices on the network in DMS.

1. Go to DMS > Management > DMS Mode to check if the controller IP is correct.
2. Verify that the gateway of this switch is correctly configured.
3. Verify that all connected devices are displayed in DMS Topology View.

Problem: DMS Connectivity diagnostics fails to ICMP reachable device.

Description: DMS displays a device which is reachable via ICMP ping as failing the connection status in diagnostics. Cable status displays as *OK*.

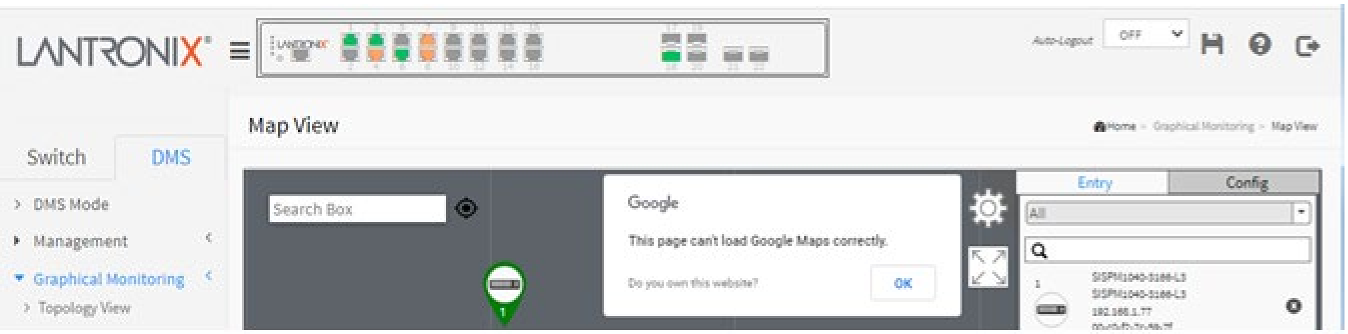
Resolution: Contact Technical Support. See Contact Us below.

Problem: DMS will discover the device type, name and model of some cameras and hosts but others are displayed as *Unknown*.

Description: When a device is detected by DMS, the device's information (such as type, model name…etc.) can be recognized via LLDP (e.g., Switch), UPnP (e.g., AP), ONVIF (e.g. IP cam), NBNS (e.g. PC) packets if the device supports these protocols. So if the device display as *Unknown*, that means this device do not issue above mentioned protocol for DMS to recognize.

Resolution: You can manually assign and configure the device type and name for the unknown devices. See the Topology View > Dashboard or the Topology View section.

Message: *This page can't load Google Maps correctly.* See DMS > Graphical Monitoring > Map View on page 434 above.



Google

This page can't load Google Maps correctly.

Do you own this website? OK

For More DMS Information

See the online DMS Video.

See the online DMS Overview.

Appendix A. DHCP Per Port

You can configure DHCP Per Port via the CLI and Web UI as described below. The DHCP Per Port factory default mode is Disabled. See the *CLI Reference* for CLI mode operation.

A-1. Configure DHCP Per Port via the Web UI

The switch's DHCP server assigns IP addresses. Clients get IP addresses in sequence and the switch assigns IP addresses on a per-port basis starting from the configured IP range. For example, if the IP address range is configured as 192.168.10.20 - 192.168.10.37 with one DHCP device connected to port 1, the client will always get IP address 192.168.10.20, then port 3 is always distributed IP address 192.168.10.22, even if port 2 is an empty port (because port 2 is always distributed IP address 192.168.10.21).

The switch does not allow a DHCP per Port pool to include the switch's address.

IP address assigned range and VLAN 1 should stay in the same subnet mask.

The configurable IP address range is allowed to configure over 18 IP addresses, but the switch always assigns one IP address per port connecting device.

The DHCP Per Port function is only supported on VLAN 1.

When the DHCP Per Port function is enabled, the switch software will automatically create the related DHCP pool named "DHCP_Per _Port".

Once the DHCP Per Port function is enabled on one switch, IPv4 DHCP client at VLAN1 mode (DMS DHCP mode), DHCP server mode are all limited to be enabled at the same time (an error message displays if attempted).

If the DHCP server pool has been configured, once you enable the DHCP Per Port function, then that DHCP server pool configuration will be overwritten.

Only for VLAN 1, clients issued DHCP packets will not be broadcast/forwarded to other ports. DHCP packets in others VLANs will be broadcast/forwarded to other ports.
The DHCP Per Port function allows the switch to connect only one DHCP client device.
DHCP-Per-Port is configured entirely on the **Switch** > **Configuration** > **System** > **IP** page, IP Interfaces window. The feature is enabled here and an IP range (pool) is entered. The "automatic" results of this action can be displayed in:

- **Switch** > **Configuration** > **System** > **DHCP** > **Server** > **Mode** (Global Mode – Enabled, VLAN Mode - VLAN 1 created)
- **Switch** > **Configuration** > **System** > **DHCP** > **Excluded** (Excluded range created based on range entered)
- **Switch** > **Configuration** > **System** > **DHCP** > **Pool** (Pool "DHCP_Per_Port" created based on range entered)

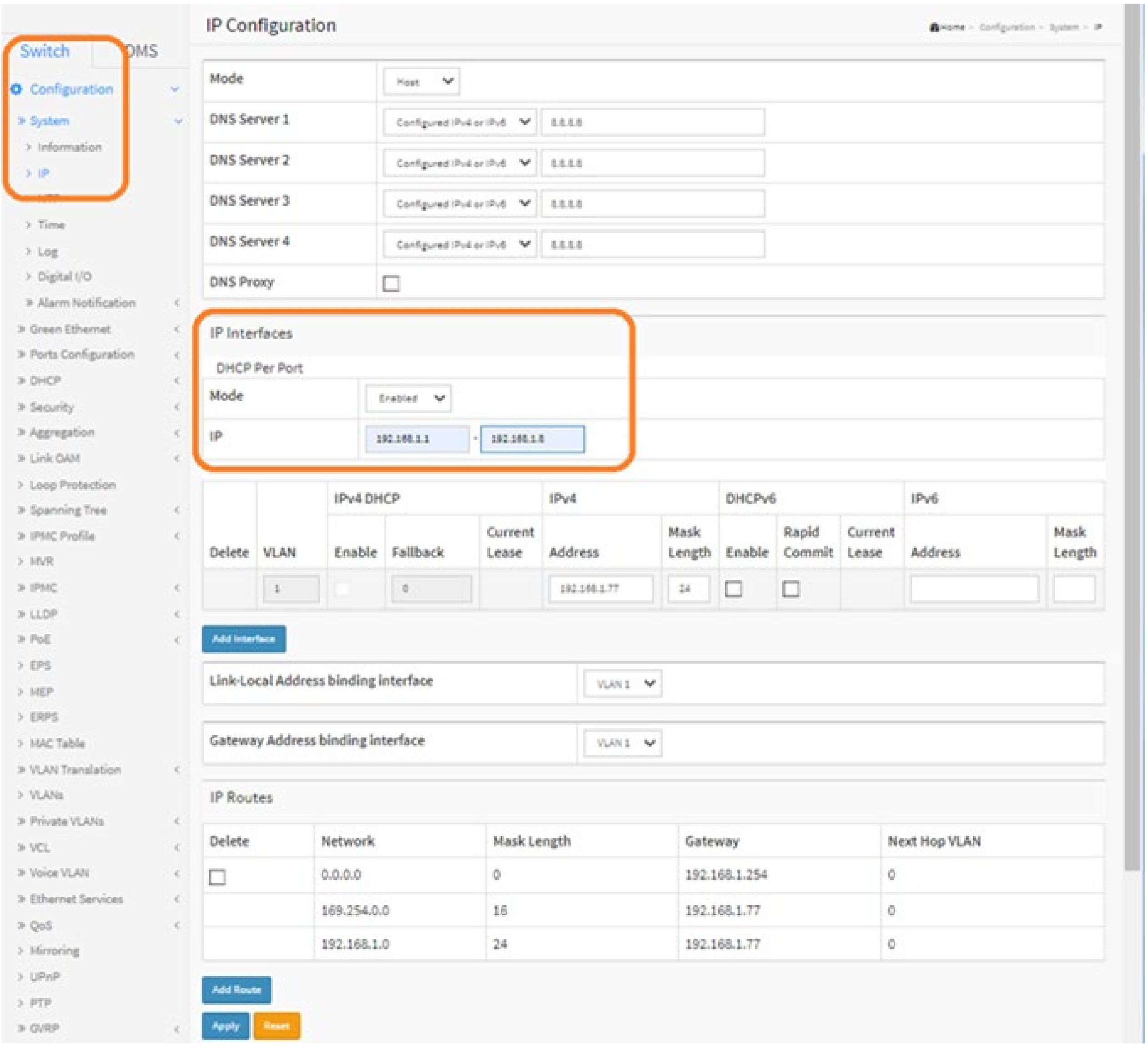
Actual DHCP operation is monitored as normal under **System** > **Monitor** > **DHCP**.

The DHCP Per Port pages and parameters are described below.

A-2. DHCP Per Port Mode Configuration

The DHCP Per Port function lets you assign an IP address based on the switch port the device is connected to. This will speed up installation of IP cameras, as the cameras can be configured after they are on the network. The DHCP Per Port assignment lets you know which IP was assigned to which camera.
Note: to prevent IP conflict, each switch can be allocated a different IP range.

To configure DHCP Per Port via the Web UI, navigate to the **Configuration** > **System** > **IP** menu path.



IP Configuration

Mode	Host	
DNS Server 1	Configured IPv4 or IPv6	8.8.8.8
DNS Server 2	Configured IPv4 or IPv6	8.8.8.8
DNS Server 3	Configured IPv4 or IPv6	8.8.8.8
DNS Server 4	Configured IPv4 or IPv6	8.8.8.8
DNS Proxy	□	

IP Interfaces

DHCP Per Port

Mode	Enabled
IP	192.168.1.1 - 192.168.1.8

		IPv4 DHCP			IPv4		DHCPv6			IPv6	
Delete	VLAN	Enable	Fallback	Current Lease	Address	Mask Length	Enable	Rapid Commit	Current Lease	Address	Mask Length
	1	□	0		192.168.1.77	24	□	□			

Link-Local Address binding interface	VLAN 1
Gateway Address binding interface	VLAN 1

IP Routes

Delete	Network	Mask Length	Gateway	Next Hop VLAN
□	0.0.0.0	0	192.168.1.254	0
	169.254.0.0	16	192.168.1.77	0
	192.168.1.0	24	192.168.1.77	0

Parameter descriptions: The DHCP Per Port parameters and buttons are described below.

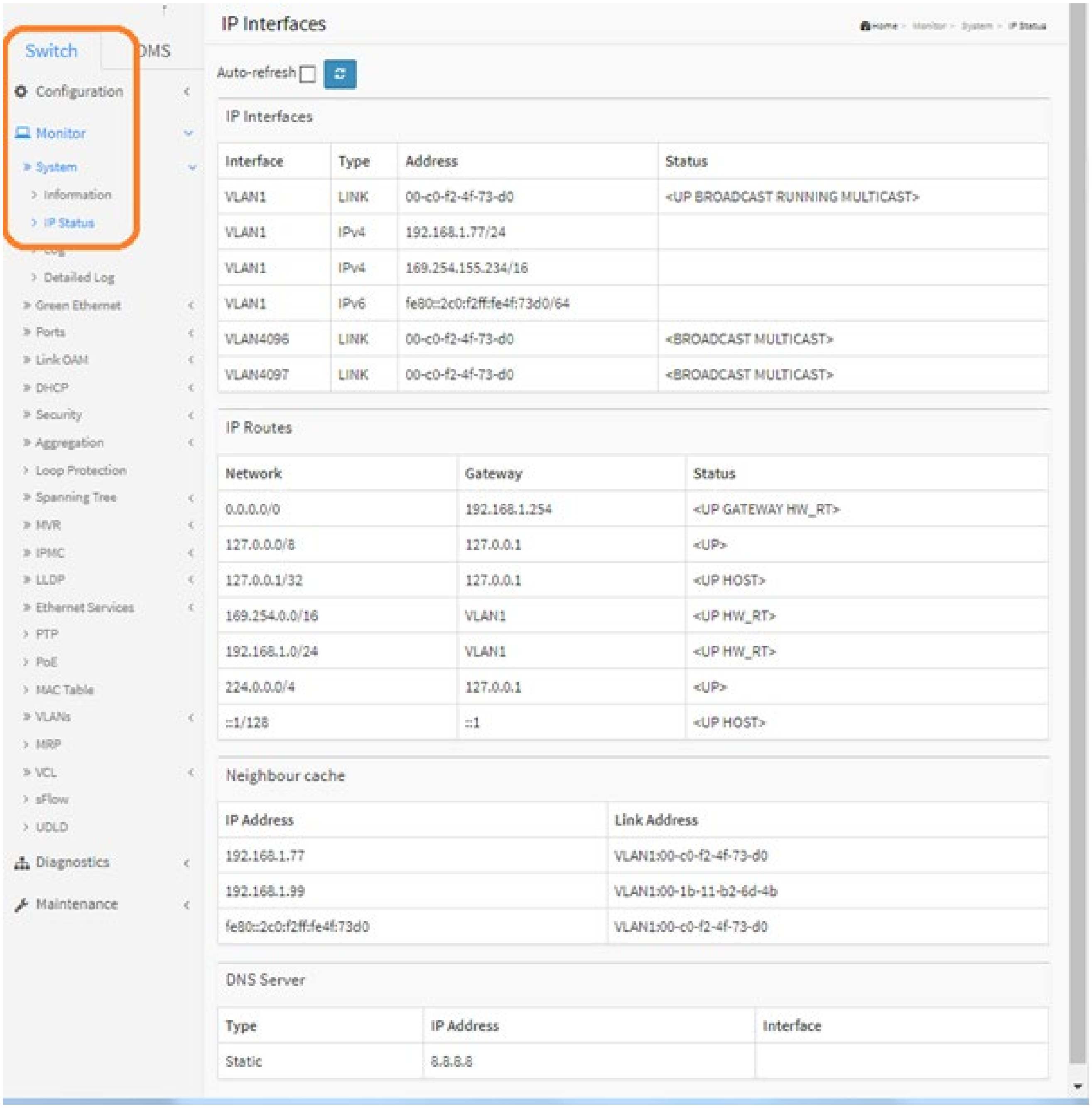
DHCP Per Port Mode: at the dropdown select **Enable** or **Disable** the DHCP Per Port function globally. The default is **Disabled**.

IP: enter the IPv4 IP address range to be used when the DHCP Per Port function is enabled (e.g., 192.168.10.20 - 192.168.10.37). The DHCP Per Port IP range must be within the interface subnet. Note that DHCP Per Port with IPv6 is not supported at this time. The DHCP Per Port IP range must equal the switch port number excluding uplink ports (16).

Apply: Click to save changes to the entries. If the entries are valid, the webpage message "*Update success!*" displays. Click the **OK** button to clear the message. If any entries are invalid, an error message displays. Click the **OK** button to clear the message and enter valid values, then click the **Apply** button again.

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

To monitor DHCP Per Port status, navigate to the **Monitor** > **System** > **IP Status** menu path.



IP Interfaces

Auto-refresh □

IP Interfaces

Interface	Type	Address	Status
VLAN1	LINK	00-c0-f2-4f-73-d0	<UP BROADCAST RUNNING MULTICAST>
VLAN1	IPv4	192.168.1.77/24	
VLAN1	IPv4	169.254.155.234/16	
VLAN1	IPv6	fe80::2c0:f2ff:fe4f:73d0/64	
VLAN4096	LINK	00-c0-f2-4f-73-d0	<BROADCAST MULTICAST>
VLAN4097	LINK	00-c0-f2-4f-73-d0	<BROADCAST MULTICAST>

IP Routes

Network	Gateway	Status
0.0.0.0/0	192.168.1.254	<UP GATEWAY HW_RT>
127.0.0.0/8	127.0.0.1	<UP>
127.0.0.1/32	127.0.0.1	<UP HOST>
169.254.0.0/16	VLAN1	<UP HW_RT>
192.168.1.0/24	VLAN1	<UP HW_RT>
224.0.0.0/4	127.0.0.1	<UP>
::1/128	::1	<UP HOST>

Neighbour cache

IP Address	Link Address
192.168.1.77	VLAN1:00-c0-f2-4f-73-d0
192.168.1.99	VLAN1:00-1b-11-b2-6d-4b
fe80::2c0:f2ff:fe4f:73d0	VLAN1:00-c0-f2-4f-73-d0

DNS Server

Type	IP Address	Interface
Static	8.8.8.8	

Web UI Messages

Message: *Interface xx not using DHCP*

Meaning: The Interface being configured does not have DHCP enabled and configured.

Recovery: **1**. Click the **OK** button to clear the webpage message. **2**. Enable and configure DHCP for the interface being configured. See DHCP Server Mode Configuration on page 180.

Message: *'DHCP Per Port IP range (192-168-1.80 - 192-168-1.99*) is not equal to switch port number excluding uplink ports (10)

Meaning: The IPv4 IP address range entered for the DHCP Per Port function was invalid.

Recovery: **1**. Click the **OK** button to clear the webpage message. **2**. Re-configure DHCP Per Port. See the DHCP Per Port Mode Configuration section above.

Message: *'DHCP Per Port IP range (192-168-1.70 - 192-168-1.85*) *includes interface IP Address (192.168.1.77)*

Meaning: The IPv4 IP address range entered for the DHCP Per Port function was invalid.

Recovery: **1**. Click the **OK** button to clear the webpage message. **2**. Re-configure DHCP Per Port.
See the DHCP Per Port Mode Configuration section above. On the screen below, the range should be something like 192-168-1.80 - 192-168-1.85 to be valid.

Message: *The value of 'DNS Server' must be a valid IP address in dotted decimal notation ('x.y.z.w').*

Meaning: You entered an invalid IP address for the DNS Server being configured.

Recovery: **1**. Click the **OK** button to clear the webpage message. **2**. Enter a valid IP address in the format x.y.z.w per the on-screen restrictions. See DHCP Server Mode Configuration on page 180.

Message: *'DHCP Interface VLAN ID' must be an integer value between 1 and 4095.*

Meaning: You entered an invalid VLAN ID for the DHCP Interface.

Recovery: **1**. Click the **OK** button to clear the webpage message. **2**. Enter a valid VLAN ID for the DHCP Interface (1-4095). See DHCP Server Mode Configuration on page 180.

Message: *DHCP per Port range (192.168.1.50 - 192.168.1.66) is not equal to switch TP port number (8).*

Message: *Update success!*

Appendix B. MRP Pre-Requisites and Application Examples

You can configure Media Redundancy Protocol (MRP) parameters via the Web UI at Configuration > MRP and monitor them at Monitor > MRP, or via the CLI. See the *CLI Reference* for Command Line operation.

According to ANSI, IEC 62439-2 Ed. 1.0 b:2010 is applicable to high-availability automation networks based on ISO/IEC 8802-3 / IEEE 802.3 Ethernet technology. It specifies a recovery protocol based on a ring topology, designed to react deterministically on a single failure of an inter-switch link or switch in the network, under the control of a dedicated Media Redundancy Manager (MRM) node.

Media Redundancy Protocol per IEC 62439-2 is an interoperable ring technology designed to allow a switch to connect onto a universal redundant high speed ring. MRP is self-healing and self-adjusting, requiring no operator interaction. MRP is based on the concept of standby connections for seamless redundancy.

B-1. MRP Description

1. MRP operates at the MAC Layer of the Ethernet Switch.
2. The Ring Manager is called the Media Redundancy Manager (MRM).
3. Ring Clients are called Media Redundancy Clients (MRCs).
4. MRM and MRC ports support three Status Types:
   a. *Disabled* ring ports drop all the received frames.
   b. *Blocked* ring ports drop all the received frames except the MRP control frames.
   c. *Forwarding* ring ports forward all the received frames.
5. Ring Reconfiguration speed is 200 ms for 50 switches on average.
6. The MRM continuously sends Watchdog Packets into the ring network to verify communication between ring points.
7. During normal operation, no packets are transmitted over the redundant link.
8. When the MRM no longer receives the Watchdog Packets it sent out, the redundant path is immediately activated, and it becomes the primary layer 2 packet path.
9. When the failed link is restored:
   a. The MRM switches back to normal operation and the first Path becomes the primary path again.
   b. You can configure a period of time before the MRM switches back to the primary path (to prevent the circuit from flapping if it is not stable).

B-2. MRP Operation

Normal operation: the network works in the *Ring-Closed* status. In this status, one of the MRM ring ports is blocked, while the other is forwarding. Conversely, both ring ports of all MRCs are forwarding. Loops are avoided because the physical ring topology is reduced to a logical stub topology.

Failure mode: the network works in the *Ring-Open* status. For instance, in case of failure of a link connecting two MRCs, both ring ports of the MRM are forwarding. The MRCs adjacent to the failure have a blocked and a forwarding ring port; the other MRCs have both ring ports forwarding. The physical ring topology is also a logical stub topology in the Ring-Open status.

B-3. Related Devices

MRP is implemented at FW v7.10.2368 for SISPM1040-384-LRT-C, SISPM1040-362-LRT, SISPM1040-582-LRT, SISGM1040-284-LRT, SISPM1040-3166-L, and SISPM1040-3248-L.

B-4. MRP Sample Setup

The example below shows SISPM1040-384-LRT-C switches (one MRM and five MRCs).

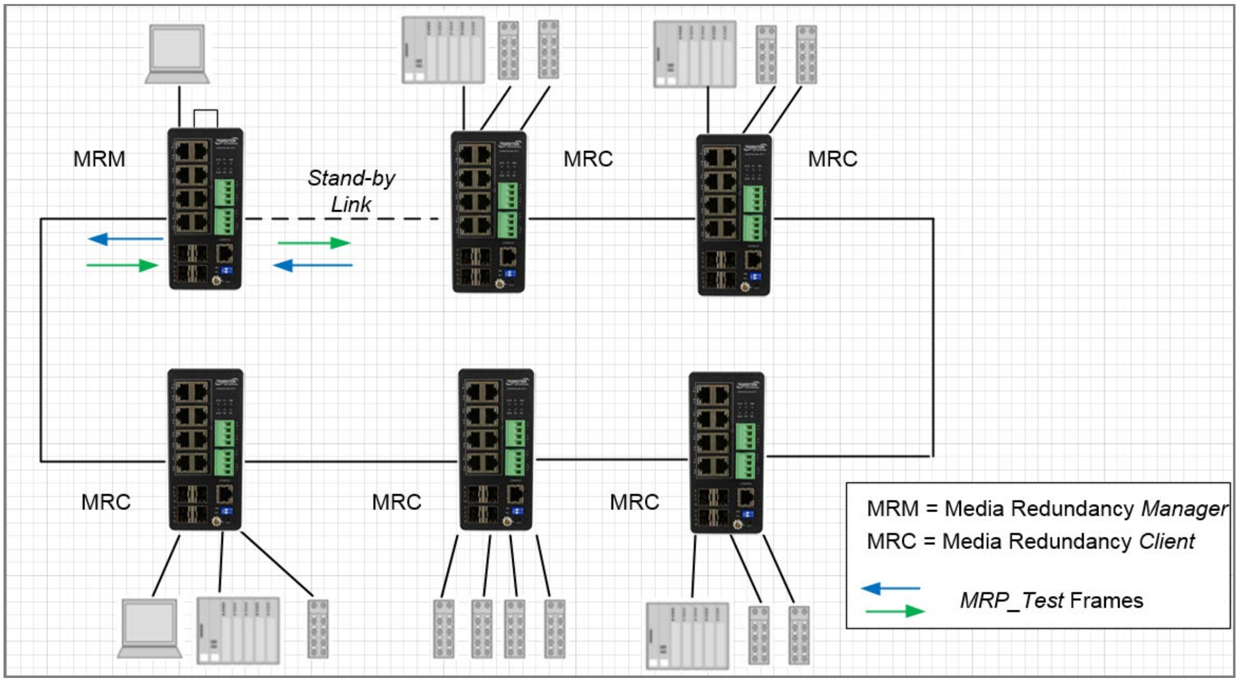

MRM
Stand-by Link
MRC
MRC
MRC
MRC
MRC
MRM = Media Redundancy *Manager*
MRC = Media Redundancy *Client*
MRP_Test Frames

Figure: MRP Sample Setup

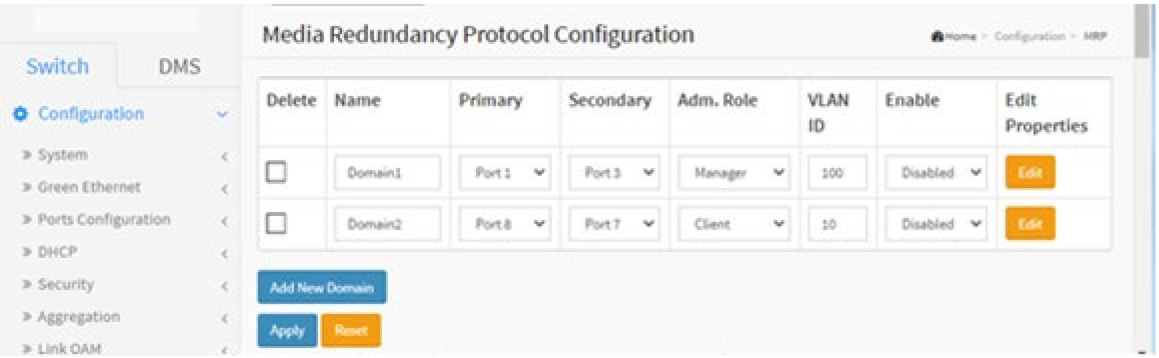
B-5. MRP Pre-Requisites (General)

The following are required to perform MRP setups.

1. Spanning Tree must be disabled at Configuration > Spanning Tree > CIST Port.
2. Other Ring technologies must also be disabled (G.8031 EPS, G.8032 ERPS, Rapid-Ring, Ring-To-Ring, etc.).
3. Only one MRM (Manager) is supported per ring.
4. Other pre-requisites may apply to the specific examples below.
5. One Manager Admin Role is supported.

B-6. MRP Web UI Configuration

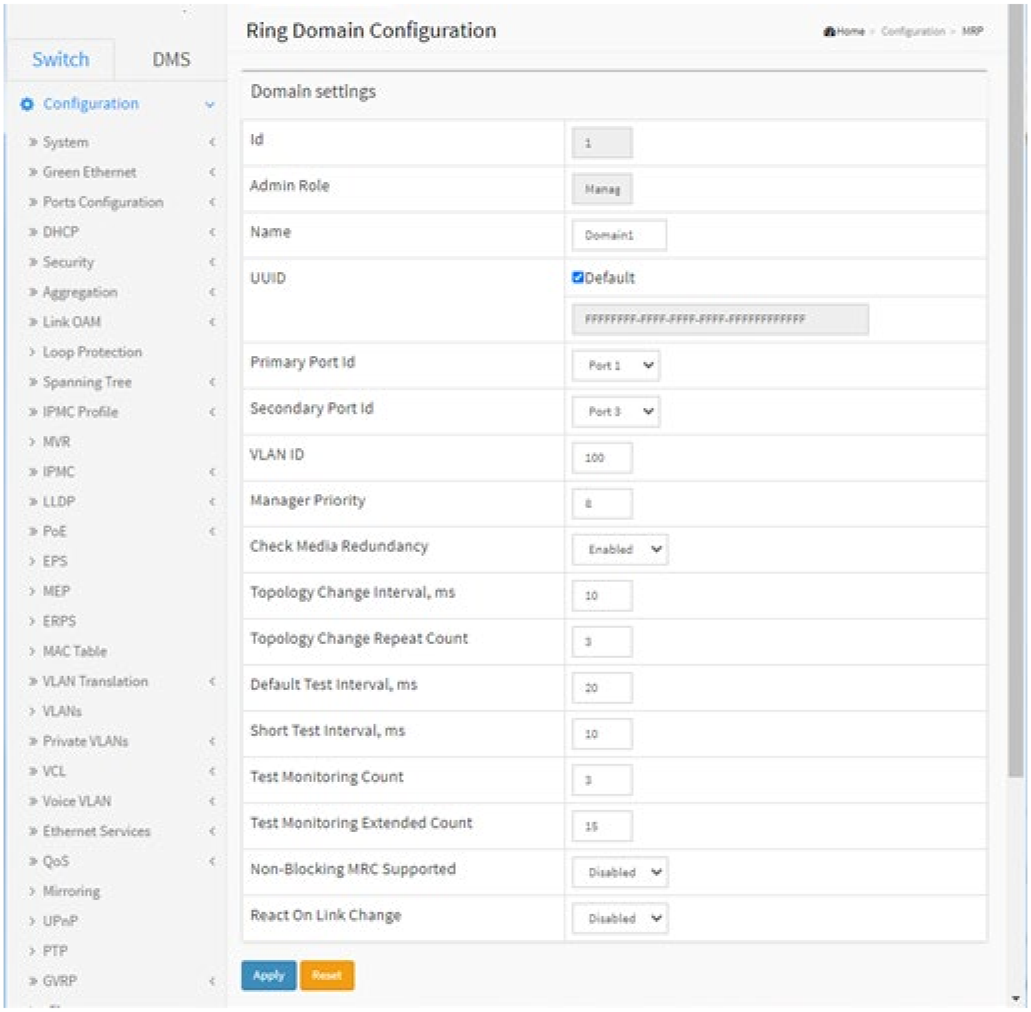
1. Navigate to Switch > Configuration > MRP to initially configure two MRP Domains:



Media Redundancy Protocol Configuration

Delete	Name	Primary	Secondary	Adm. Role	VLAN ID	Enable	Edit Properties
□	Domain1	Port 1	Port 3	Manager	100	Disabled	Edit
□	Domain2	Port 8	Port 7	Client	10	Disabled	Edit

2. Click Apply to save, and then click the Edit button to configure the first MRP Domain (Domian1).



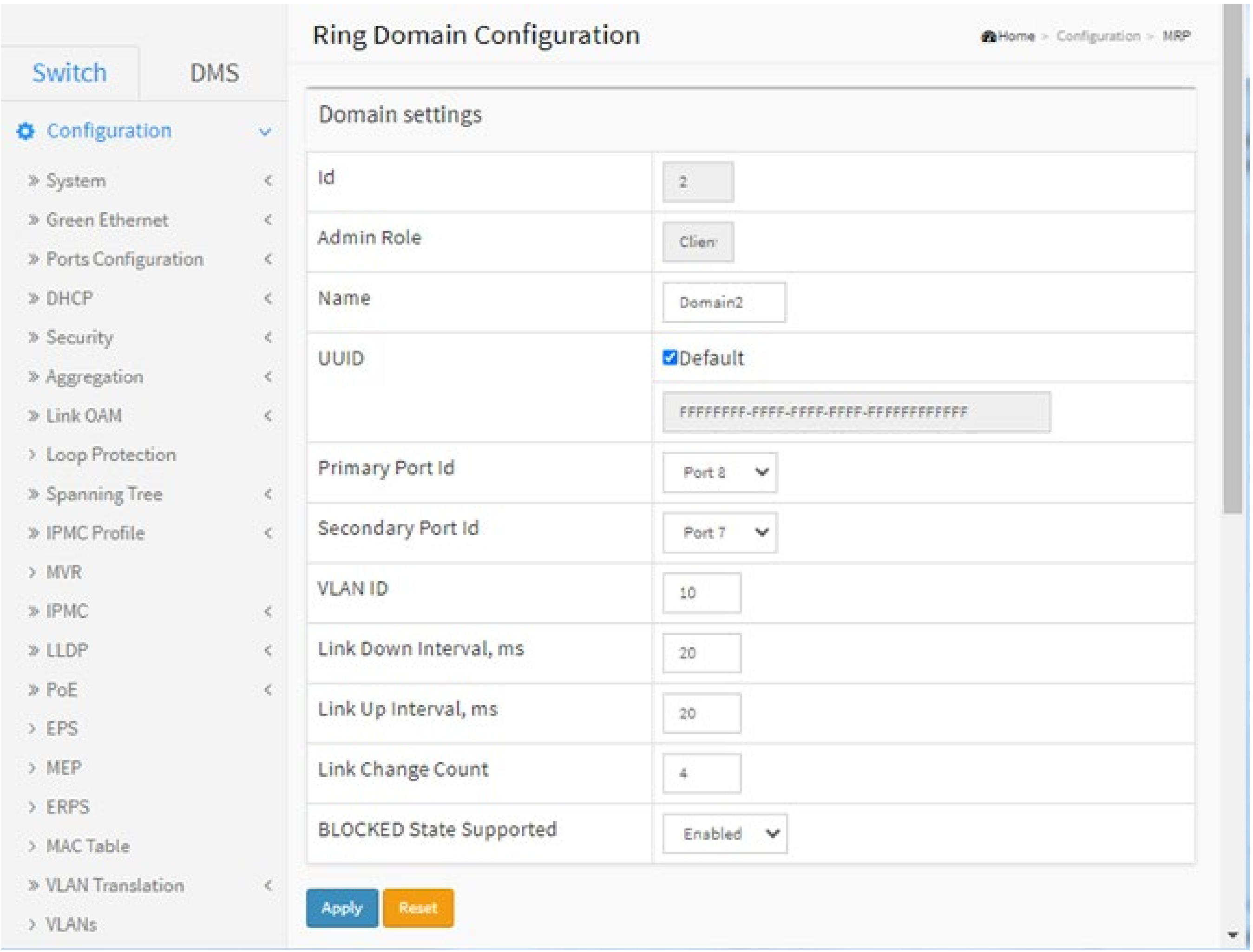
Ring Domain Configuration

Domain settings

Id	1
Admin Role	Manag
Name	Domain1
UUID	☑ Default FFFFFFFF-FFFF-FFFF-FFFF-FFFFFFFFFFFF
Primary Port Id	Port 1
Secondary Port Id	Port 3
VLAN ID	100
Manager Priority	8
Check Media Redundancy	Enabled
Topology Change Interval, ms	10
Topology Change Repeat Count	3
Default Test Interval, ms	20
Short Test Interval, ms	10
Test Monitoring Count	3
Test Monitoring Extended Count	15
Non-Blocking MRC Supported	Disabled
React On Link Change	Disabled

3. Edit the Domain Settings as required. Click Apply to save; the message "*Domain is enabled*" displays. Click OK to clear the webpage message. The "Media Redundancy Protocol Configuration" page displays again.

4. Click the Edit button to display the second MRP Domain (Domian2).



Ring Domain Configuration

Domain settings

Id	2
Admin Role	Clien
Name	Domain2
UUID	☑ Default FFFFFFFF-FFFF-FFFF-FFFF-FFFFFFFFFFFF
Primary Port Id	Port 8
Secondary Port Id	Port 7
VLAN ID	10
Link Down Interval, ms	20
Link Up Interval, ms	20
Link Change Count	4
BLOCKED State Supported	Enabled

5. Edit the Domain Settings as required. Click Apply to save; the message "*Domain is enabled*" displays. Click OK to clear the webpage message.

6. When the "Media Redundancy Protocol Configuration" page displays again, verify the settings.

Example 1: MRP Manager Re-Config (Web UI)

This application example shows the MRP Manager reconfiguring the traffic path based on the client state.

Sample Setup: This setup includes one device with MRP enabled and has an admin role set as Manager and three clients connected in a ring topology. See the MRP Sample Setup diagram below.

Procedure:

1. Disable any other Ring technologies and disable Spanning-tree at Configuration > Spanning Tree > CIST Port.
2. For the device acting as MRM click 'Add New Domain' button to configure the MRP instance in the 'Media Redundancy Protocol Configuration' page.
3. Assign the first ring port under 'Primary' and the second ring port under 'Secondary'.
4. Set the Administrative Role to 'Manager' under 'Adm. Role'. Assign any VLAN ID from 2-4094.
5. Set the instance to 'enable'.
6. Go to the 'Ring Domain Configuration (Manager Role)' page and set a Domain name.
7. Tick the Default box for UUID.
8. Select the Primary and Secondary Port IDs.
9. Enable 'Check Media Redundancy'.
10. Leave other settings as default.
11. For the devices acting as MRCs in the 'Ring Domain Configuration (Client Role)' page assign the first Primary and Secondary Port IDs for the ring ports.
12. Enter the same VLAN ID as in step 4 above.
13. Link Down Interval should be 20ms. Link Up Interval should be 20ms. Link change count should be 4.
14. 'BLOCKED State Supported' must be enabled. By default, one ring port will be disabled for loop-free communication.
15. Configure ring ports to Hybrid mode on the VLAN Configuration page. Assign the VLAN ID as configured in step 4.
16. Send bi-directional traffic tagged with the VLAN ID set in step 4 above.
17. Create a failure on any one of the client ring ports by disconnecting the cable. The MRM should reconfigure the path within 200<500ms. The Redundancy Manager will send test frames marked with a unique MAC with OUI of 00-15-4E and forwarded by the MRCs to the opposite ring ports per the interval specified. The disabled ring port should now be enabled, creating a new loop-free topology.
18. There should be no traffic loss after path reconfiguration.

Example 2: Non-Blocking MRC State Recognized by MRM (Web UI)

This application example shows a Non-blocking MRC state is recognized by the MRM.

Setup: This setup and steps 1-18 in Example 1 above are required.

Procedure:

1. Disable any other Ring technologies and disable Spanning-tree at Configuration > Spanning Tree > CIST Port.
2. Disable 'BLOCKED State Supported'.
3. Configure ring ports to Hybrid mode on the VLAN Configuration page. Assign the VLAN ID as configured in step 4 of Example 1.
4. Send bi-directional traffic tagged with the VLAN ID set in the previous step.
5. Create a failure on any one of the client ring ports by disconnecting the cable. The client ring ports will be in a forwarding state instead of blocking. The MRM should reconfigure the path within 200<500ms. The MRM will send test frames marked with a unique MAC with OUI of 00-15-4E and forwarded by the MRCs to the opposite ring ports per the interval specified.
6. Verify the MRC reacts to the reconfiguration frames as received by the MRM. The link down on the client ring port should be detected by the MRC.
7. There should be no traffic loss after path reconfiguration.

Example 3: MRP Roles Set in Web UI

Setup: This setup shows that the MRP can have both Manager and Undefined roles.

Procedure:

1. Disable any other Ring technologies and disable Spanning-tree at Configuration > Spanning Tree > CIST Port.
2. 'BLOCKED State Supported' should be enabled. By default, one ring port will be disabled for loop-free communication.
3. Configure ring ports to Hybrid mode on the VLAN Configuration page. Assign the VLAN ID as set in step 4 of Example 1.
4. Send bi-directional traffic tagged with the VLAN ID set in the previous step.
5. Create a failure on any one of the client ring ports by disconnecting the cable. The MRM should reconfigure the path within 200<500ms. The Redundancy manager will send test frames marked with a unique MAC with OUI of 00-15-4E and forwarded by the MRCs to the opposite ring ports per the interval specified. The disabled ring port should now be enabled and creates a new loop-free topology.
6. There should be no traffic loss after path reconfiguration.
7. On a second client set the 'BLOCKED State Supported' option to disable. The ring port will now be in a forwarding state. Cause a failure on the ring port of another device that has its blocked state disabled.
8. Verify that frames are forwarded and received by the MRC with blocking enabled. There should be no traffic loss after path reconfiguration.

Appendix C. G.8032 Major and Sub Rings Configuration

Introduction

Ethernet Ring Protection Switching (ERPS) is a protocol defined by the International Telecommunication Union - Telecommunication Standardization Sector (ITU-T) to prevent loops at Layer 2. With the standard number is ITU-T G.8032, and ERPS is also called G.8032. Generally, redundant links are used on a network to provide link backup and enhance network reliability. The use of redundant links, however, may produce loops, causing broadcast storms and rendering the MAC address table unstable. These can affect the network, where the communication quality is not good enough, and communication services might be interrupted.

ERPS provides advantages of traditional ring network technologies such as STP/RSTP/MSTP and optimizes detection mechanism to provide faster convergence. For example, the ERPS-enabled switch provides 50-ms convergence for broadcast packets. See section "16 ERPS" on page 278 for general G.8032 ERPS configuration information.

Basic Concepts

There are some basic concepts that support ERPS Ring:

- **Ring Protection Link (RPL)** – Link designated by mechanism that is blocked during Idle state to prevent loop on Bridged ring.
- **RPL Owner node** – Node connected to RPL that blocks traffic on RPL during Idle state and unblocks during Protection state.
- **RPL Neighbor node** – Node connected to RPL that blocks traffic on RPL during Idle state and unblocks during Protection state (v2).
- **Link Monitoring** – Links of ring are monitored using standard ETH CC OAM messages (CFM) • Signal Fail (SF) – Signal Fail is declared when signal fail condition is detected.
- **No Request (NR)** – No Request is declared when there are no outstanding conditions (e.g., SF, etc.) on the node.
- **Ring APS (R-APS) Messages** – Protocol messages defined in Y.1731 and G.8032.
- **Automatic Protection Switching (APS) Channel** - Ring-wide VLAN used exclusively for transmission of OAM messages including R-APS messages.

IP Addresses

The sample configurations below use these IP addresses:

SISPM1040-582-LRT : 192.168.1.85

SISPM1040-384-LRT-C : 192.168.1.95

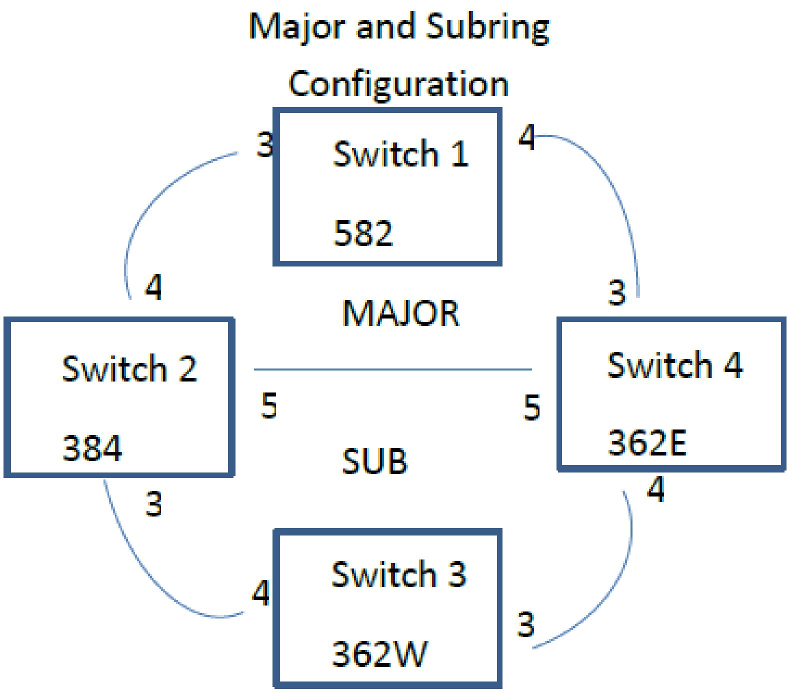
362W : 192.168.1.125

362E : 192.168.1.135

Sample Configuration

Major Ring and Sub Ring : 4 Switches

Major : SW#1, SW#2, SW#4; **Sub** : SW#2, SW#3, SW#4



VLANs	**APS**	**Data**	
		10,20	5

RPL Mode	**Major**	**Sub**	**Major**	**Sub**	**Major**	**Sub**
	Owner Switch #1	Owner Switch #3	Neighbor Switch #2	Neighbor Switch #2	None Switch #4	None Switch #4

Switch 1 Configuration (SISPM1040-582-LRT)

VLANs	Port 3	Trunk	Tag All	5,10
	Port 4	Trunk	Tag All	5,10
STP	Port 3	Disable		
	Port 4	Disable		

MEPs	Instance	Port	VLAN	MAC	MEP ID	Peer MAC	Peer MEP ID
	1	3	10	00-C0-F2-49-39-5F	1	00-40-C7-1C-C7-30	4
	2	4	10	00-C0-F2-49-39-60	5	00-C0-F2-53-EF-FC	5

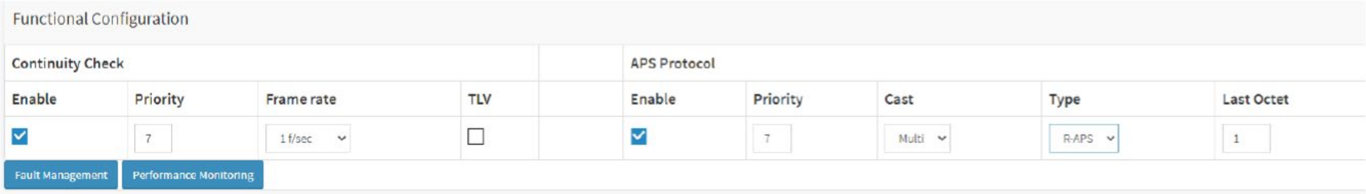
Note: All MEPs are programed the same under the Functional Configuration

Continuity Check

Check Enable – Priority: 7 – Frame rate: 1f/sec

APS Protocol

Check Enable – Priority: 7 – Cast: Multi – Type: R-APS



Functional Configuration

Continuity Check					APS Protocol				
Enable	Priority	Frame rate	TLV		Enable	Priority	Cast	Type	Last Octet
☑	7	1 f/sec	☐		☑	7	Multi	R-APS	1

ERPS

ERPS ID	Port 0	Port 1	Port 0 SF	Port 1 SF	Port 0 APS	Port 1 APS	Ring	RPL	Port	VLAN
1	1	2	1	2	1	2	Major	Owner	0	5

Switch 2 Configuration (SISPM1040-384-LRT-C)

VLANs	Port 3	Trunk	Tag All	5,20
	Port 4	Trunk	Tag All	5,10
	Port 5	Trunk	Tag All	5,10,20

STP	Port 3	Disable
	Port 4	Disable
	Port 5	Disable

MEPs	Instance	Port	VLAN	MAC	MEP ID	Peer MAC	Peer MEP ID
	1	3	20	00-40-C7-1C-C7-2F	3	00-C0-F2-53-F0-BA	8
	2	4	10	00-C0-F2-49-39-60	4	00-C0-F2-49-39-5F	1
	3	5	10	00-40-C7-1C-C7-31	9	00-C0-F2-53-EF-FE	10

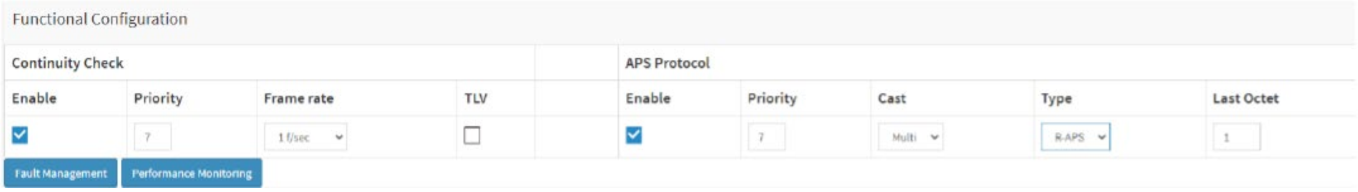
Note: All MEPs are programed the same under the Functional Configuration

Continuity Check

Check Enable – Priority: 7 – Frame rate: 1f/sec

APS Protocol

Check Enable – Priority: 7 – Cast: Multi – Type: R-APS



Functional Configuration

Continuity Check				APS Protocol				
Enable	Priority	Frame rate	TLV	Enable	Priority	Cast	Type	Last Octet
☑	7	1 f/sec	☐	☑	7	Multi	R-APS	1

ERPS

ERPS ID	Port 0	Port 1	Port 0 SF	Port 1 SF	Port 0 APS	Port 1 APS	Ring	RPL	Port	VLAN
1	3	2	3	2	3	2	Major	Neighbor	1	5
2	1	0	1	0	1	0	Sub	Neighbor	0	5

Interconnect Yes, Major 1

Switch 3 Configuration (SISPM1040-362-LRT[W])

VLANs	Port 3	Trunk Tag All 5,20
	Port 4	Trunk Tag All 5,20
STP	Port 3	Disable
	Port 4	Disable

MEPs	Instance	Port	VLAN	MAC	MEP ID	Peer MAC	Peer MEP ID
	1	3	20	00-C0-F2-53-F0-B9	7	00-C0-F2-53-EF-FD	6
	2	4	20	00-C0-F2-53-F0-BA	8	00-40-C7-1C-C7-2F	3

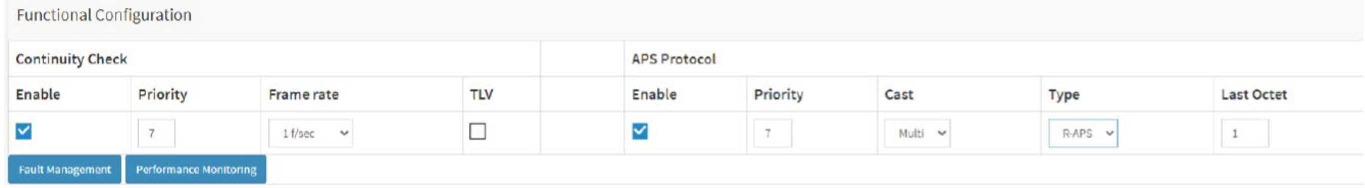
Note: All MEPs are programed the same under the Functional Configuration

Continuity Check

Check Enable – Priority: 7 – Frame rate: 1f/sec

APS Protocol

Check Enable – Priority: 7 – Cast: Multi – Type: R-APS



Functional Configuration

Continuity Check				APS Protocol				
Enable	Priority	Frame rate	TLV	Enable	Priority	Cast	Type	Last Octet
☑	7	1 f/sec	☐	☑	7	Multi	R-APS	1

ERPS

ERPS ID	Port 0	Port 1	Port 0 SF	Port 1 SF	Port 0 APS	Port 1 APS	Ring	RPL	Port	VLAN
1	1	2	1	2	1	2	Sub	Owner	1	5

Switch 4 Configuration (SISPM1040-362-LRT[E])

VLANs	Port 3	Trunk	Tag All	5,10
	Port 4	Trunk	Tag All	5,20
	Port 5	Trunk	Tag All	5,10,20

STP	Port 3	Disable
	Port 4	Disable
	Port 5	Disable

MEPs	Instance	Port	VLAN	MAC	MEP ID	Peer MAC	Peer MEP ID
	1	3	10	00-C0-F2-53-EF-FC	5	00-C0-F2-49-39-60	2
	2	4	20	00-C0-F2-53-EF-FD	6	00-C0-F2-53-F0-B9	7
	3	5	10	00-C0-F2-53-EF-FE	10	00-40-C7-1C-C7-31	9

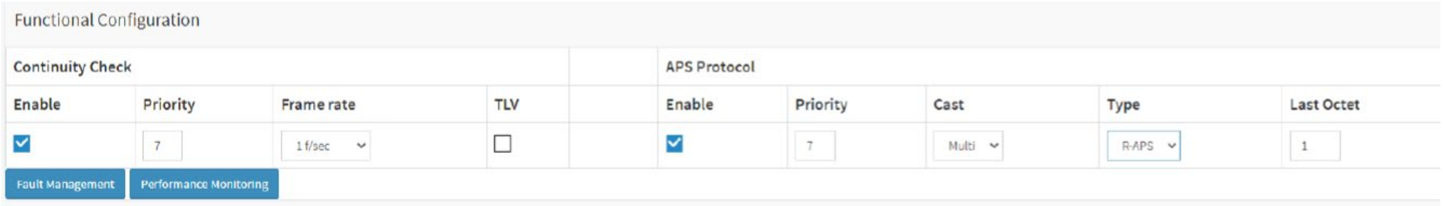
Note: All MEPs are programed the same under the Functional Configuration

Continuity Check

Check Enable – Priority: 7 – Frame rate: 1f/sec

APS Protocol

Check Enable – Priority: 7 – Cast: Multi – Type: R-APS



Functional Configuration

Continuity Check				APS Protocol				
Enable	Priority	Frame rate	TLV	Enable	Priority	Cast	Type	Last Octet
☑	7	1 f/sec	☐	☑	7	Multi	R-APS	1

ERPS

ERPS ID	Port 0	Port 1	Port 0 SF	Port 1 SF	Port 0 APS	Port 1 APS	Ring	RPL	Port VLAN
1	1	3	1	3	1	3	Major	None	5
2	2	0	2	0	2	0	Sub	None	5

Interconnect Yes, Major 1

Testing

Testing Pings from Switch 4 to Switch 1 – Major Ring

Failing Major ring, No lost pings

```
C:\Users\dennist>ping 192.168.1.85 -t
Pinging 192.168.1.85 with 32 bytes of data:
Reply from 192.168.1.85: bytes=32 time<1ms TTL=64
Reply from 192.168.1.85: bytes=32 time<1ms TTL=64
Reply from 192.168.1.85: bytes=32 time<1ms TTL=64
Reply from 192.168.1.85: bytes=32 time<1ms TTL=64
Reply from 192.168.1.85: bytes=32 time<1ms TTL=64
Reply from 192.168.1.85: bytes=32 time<1ms TTL=64
Reply from 192.168.1.85: bytes=32 time<1ms TTL=64
Reply from 192.168.1.85: bytes=32 time<1ms TTL=64
Reply from 192.168.1.85: bytes=32 time<1ms TTL=64
Reply from 192.168.1.85: bytes=32 time<1ms TTL=64
Reply from 192.168.1.85: bytes=32 time<1ms TTL=64
Reply from 192.168.1.85: bytes=32 time<1ms TTL=64
Reply from 192.168.1.85: bytes=32 time<1ms TTL=64
Reply from 192.168.1.85: bytes=32 time<1ms TTL=64
Reply from 192.168.1.85: bytes=32 time<1ms TTL=64
Reply from 192.168.1.85: bytes=32 time<1ms TTL=64
Reply from 192.168.1.85: bytes=32 time<1ms TTL=64
Reply from 192.168.1.85: bytes=32 time<1ms TTL=64
Reply from 192.168.1.85: bytes=32 time=1ms TTL=64
Reply from 192.168.1.85: bytes=32 time<1ms TTL=64
Reply from 192.168.1.85: bytes=32 time<1ms TTL=64
Reply from 192.168.1.85: bytes=32 time<1ms TTL=64
Reply from 192.168.1.85: bytes=32 time<1ms TTL=64
Reply from 192.168.1.85: bytes=32 time<1ms TTL=64
Reply from 192.168.1.85: bytes=32 time<1ms TTL=64
Reply from 192.168.1.85: bytes=32 time<1ms TTL=64
Reply from 192.168.1.85: bytes=32 time<1ms TTL=64
Reply from 192.168.1.85: bytes=32 time<1ms TTL=64
Reply from 192.168.1.85: bytes=32 time<1ms TTL=64
Reply from 192.168.1.85: bytes=32 time=5ms TTL=64  ←---------------------
Reply from 192.168.1.85: bytes=32 time<1ms TTL=64  Cable Disconnect
Reply from 192.168.1.85: bytes=32 time=3ms TTL=64  ←---------------------
Reply from 192.168.1.85: bytes=32 time<1ms TTL=64
Reply from 192.168.1.85: bytes=32 time=1ms TTL=64
Reply from 192.168.1.85: bytes=32 time<1ms TTL=64
Reply from 192.168.1.85: bytes=32 time<1ms TTL=64
Reply from 192.168.1.85: bytes=32 time=1ms TTL=64
Reply from 192.168.1.85: bytes=32 time<1ms TTL=64
Reply from 192.168.1.85: bytes=32 time<1ms TTL=64
Ping statistics for 192.168.1.85:
Packets: Sent = 45, Received = 45, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 0ms, Maximum = 5ms, Average = 0ms
```

Testing Pings from Switch 4 to Switch 3 – Sub Ring

Fail Subring, No lost pings

```
C:\Users\dennist>ping 192.168.1.125 -t

Pinging 192.168.1.125 with 32 bytes of data:
Reply from 192.168.1.125: bytes=32 time=1ms TTL=64
Reply from 192.168.1.125: bytes=32 time<1ms TTL=64
Reply from 192.168.1.125: bytes=32 time<1ms TTL=64
Reply from 192.168.1.125: bytes=32 time<1ms TTL=64
Reply from 192.168.1.125: bytes=32 time<1ms TTL=64
Reply from 192.168.1.125: bytes=32 time<1ms TTL=64
Reply from 192.168.1.125: bytes=32 time<1ms TTL=64
Reply from 192.168.1.125: bytes=32 time<1ms TTL=64
Reply from 192.168.1.125: bytes=32 time<1ms TTL=64
Reply from 192.168.1.125: bytes=32 time<1ms TTL=64
Reply from 192.168.1.125: bytes=32 time<1ms TTL=64
Reply from 192.168.1.125: bytes=32 time<1ms TTL=64
Reply from 192.168.1.125: bytes=32 time<1ms TTL=64
Reply from 192.168.1.125: bytes=32 time=1ms TTL=64
Reply from 192.168.1.125: bytes=32 time<1ms TTL=64
Reply from 192.168.1.125: bytes=32 time<1ms TTL=64
Reply from 192.168.1.125: bytes=32 time<1ms TTL=64
Reply from 192.168.1.125: bytes=32 time<1ms TTL=64
Reply from 192.168.1.125: bytes=32 time<1ms TTL=64
Reply from 192.168.1.125: bytes=32 time<1ms TTL=64
Reply from 192.168.1.125: bytes=32 time<1ms TTL=64
Reply from 192.168.1.125: bytes=32 time=7ms TTL=64   ←--------------------
Reply from 192.168.1.125: bytes=32 time<1ms TTL=64   Cable Disconnect
Reply from 192.168.1.125: bytes=32 time<1ms TTL=64
Reply from 192.168.1.125: bytes=32 time<1ms TTL=64
Reply from 192.168.1.125: bytes=32 time<1ms TTL=64
Reply from 192.168.1.125: bytes=32 time<1ms TTL=64
Reply from 192.168.1.125: bytes=32 time<1ms TTL=64
Reply from 192.168.1.125: bytes=32 time<1ms TTL=64
Reply from 192.168.1.125: bytes=32 time=1ms TTL=64
Reply from 192.168.1.125: bytes=32 time<1ms TTL=64
Reply from 192.168.1.125: bytes=32 time=1ms TTL=64
Reply from 192.168.1.125: bytes=32 time<1ms TTL=64
Reply from 192.168.1.125: bytes=32 time<1ms TTL=64
Reply from 192.168.1.125: bytes=32 time<1ms TTL=64
Reply from 192.168.1.125: bytes=32 time<1ms TTL=64
Reply from 192.168.1.125: bytes=32 time<1ms TTL=64
Reply from 192.168.1.125: bytes=32 time<1ms TTL=64
Reply from 192.168.1.125: bytes=32 time<1ms TTL=64
Ping statistics for 192.168.1.125:
Packets: Sent = 41, Received = 41, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 0ms, Maximum = 7ms, Average = 0ms
```

Config files

running-config_192.168.1

```
hostname SISPM1040-362-LRT-E
username admin privilege 15 password encrypted
feec1d1085ff075fd03b1d2d5ab4c0befbff0917079c8abb3a77338041bf5d6e1771bdbbd1a317ea2f42fc2aacc8c
50a8e667456d7c04099f74f8ef9dcc0fbd4
!
vlan 1
!
!
!
!
ip route 0.0.0.0 0.0.0.0 192.168.1.254
tzidx 0
exec-timeout autologout 0
snmp-server location DT Lab Ring
system name SISPM1040-362-LRT-E
system location DT Lab Ring
system description Managed Hardened PoE+ Switch, (4) 10/100/1000Base-T PoE+ Ports + (2)
10/100/1000Base-T Ports + (2) 100/1000Base-X SFP Ports
!
interface GigabitEthernet 1/1
!
interface GigabitEthernet 1/2
!
interface GigabitEthernet 1/3
 no spanning-tree
 switchport trunk allowed vlan 5,10
 switchport trunk vlan tag native
 switchport mode trunk
 poe mode disable
!
interface GigabitEthernet 1/4
 no spanning-tree
 switchport trunk allowed vlan 5,20
 switchport trunk vlan tag native
 switchport mode trunk
 poe mode disable
!
interface GigabitEthernet 1/5
 no spanning-tree
 switchport trunk allowed vlan 5,10,20
 switchport trunk vlan tag native
 switchport mode trunk
!
interface GigabitEthernet 1/6
!
interface GigabitEthernet 1/7
!
interface GigabitEthernet 1/8
!
interface vlan 1
 ip address 192.168.1.135 255.255.255.0
 ip dhcp server
!
mep 1 down domain port level 4 interface GigabitEthernet 1/3
mep 1 mep-id 5
mep 1 vid 10
mep 1 peer-mep-id 2 mac 00-C0-F2-49-39-60
mep 1 cc 7
mep 1 aps 7 raps
mep 2 down domain port level 4 interface GigabitEthernet 1/4
mep 2 mep-id 6
mep 2 vid 20
mep 2 peer-mep-id 7 mac 00-C0-F2-53-F0-B9
mep 2 cc 7
mep 2 aps 7 raps
mep 3 down domain port level 4 interface GigabitEthernet 1/5
mep 3 mep-id 10
mep 3 vid 10
mep 3 peer-mep-id 9 mac 00-40-C7-1C-C7-31
mep 3 cc 7
mep 3 aps 7 raps
erps 1 major port0 interface GigabitEthernet 1/3 port1 interface GigabitEthernet 1/5
erps 1 mep port0 sf 1 aps 1 port1 sf 3 aps 3
erps 1 vlan 5
erps 2 sub port0 interface GigabitEthernet 1/4 interconnect 1
erps 2 mep port0 sf 2 aps 2
erps 2 vlan 5
!
spanning-tree aggregation
 spanning-tree link-type point-to-point
!
!
line console 0
!
line vty 0
!
line vty 1
!
line vty 2
!
line vty 3
!
line vty 4
!
line vty 5
!
line vty 6
!
line vty 7
!
line vty 8
!
line vty 9
!
line vty 10
!
line vty 11
!
line vty 12
!
line vty 13
!
line vty 14
!
line vty 15
!
!
end
```

running-config_192.168.1

```
hostname SISPM1040-582-LRT
logging on
logging host 192.168.1.253
username admin privilege 15 password encrypted
7073dec86c15b8a9907bb4106ef783adde46bd5b5969cc68fb55b430336bd7c80d5ded65d2fdb39abe81cc9caa5a9
3620f270c21bca86e776cee9c5588bfb8c7
username superuser privilege 15 password encrypted
4643fdc71f39fd4cb955943fcaf89faca81bc650fbaeebe25a796662d5c225bf0d5ded65d2fdb39abe81cc9c51449
7e27799560e488713aabaac4f167e7732ca
!
vlan 1
!
!
!
!
ip route 0.0.0.0 0.0.0.0 192.168.1.254
ntp automatic
ntp server 1 ip-address ntp1.transition.com
ntp server 2 ip-address ntp2.transition.com
clock timezone '' 9
tzidx 0
exec-timeout autologout 0
poe ping-check enable
snmp-server contact DTroxel
snmp-server location DT Office
system contact DTroxel
system name SISPM1040-582-LRT
system location DT Office
system description Managed Hardened PoE++ Switch (8) 10/100/1000Base-T PoE++ Ports + (2)
100/1000Base-X SFP Slot
!
interface GigabitEthernet 1/1
 no spanning-tree
 poe ping-ip-addr 192.168.1.70
 poe failure-action reboot-Remote-PD
!
interface GigabitEthernet 1/2
 no spanning-tree
 switchport forbidden vlan add 3,5
!
interface GigabitEthernet 1/3
 no spanning-tree
 switchport trunk allowed vlan 5,10
 switchport trunk vlan tag native
 switchport mode trunk
 poe mode disable
!
interface GigabitEthernet 1/4
 no spanning-tree
 switchport trunk allowed vlan 5,10
 switchport trunk vlan tag native
 switchport mode trunk
 poe mode disable
 poe ping-ip-addr 192.168.1.200
!
interface GigabitEthernet 1/5
 no spanning-tree
!
interface GigabitEthernet 1/6
 no spanning-tree
!
```

```
interface GigabitEthernet 1/7
!
interface GigabitEthernet 1/8
 poe mode disable
!
interface GigabitEthernet 1/9
 no spanning-tree
!
interface GigabitEthernet 1/10
 no spanning-tree
!
interface vlan 1
 ip address 192.168.1.85 255.255.255.0
 ip dhcp server
!
mep 1 down domain port level 4 interface GigabitEthernet 1/3
mep 1 vid 10
mep 1 peer-mep-id 4 mac 00-40-C7-1C-C7-30
mep 1 cc 7
mep 1 aps 7 raps
mep 2 down domain port level 4 interface GigabitEthernet 1/4
mep 2 mep-id 2
mep 2 vid 10
mep 2 peer-mep-id 5 mac 00-C0-F2-53-EF-FC
mep 2 cc 7
mep 2 aps 7 raps
erps 1 major port0 interface GigabitEthernet 1/3 port1 interface GigabitEthernet 1/4
erps 1 mep port0 sf 1 aps 1 port1 sf 2 aps 2
erps 1 rpl owner port0
erps 1 vlan 5
!
spanning-tree aggregation
 no spanning-tree
 spanning-tree link-type point-to-point
!
!
line console 0
!
line vty 0
!
line vty 1
!
line vty 2
!
line vty 3
!
line vty 4
!
line vty 5
!
line vty 6
!
line vty 7
!
line vty 8
!
line vty 9
!
line vty 10
!
line vty 11
!
line vty 12
```

```
!
line vty 13
!
line vty 14
!
line vty 15
!
map-api-key AIzaSyBItuM0hDtK6nJeZPEk7jnrcoGGi92EpFM
!
end
```

running-config_192.168.1

hostname SISPM1040-384-LRT-C

```
username admin privilege 15 password encrypted
6593186b999f348becd63b8612ac561c114250a1a00bd38f6afb5378acb6d08c1864c59b092b0e2b29ba4f1d55916
6800846cbc52c4558a90e4cdf95d3cfcbf4
username dennis privilege 5 password encrypted
a92a5dbf4fcd2e13d35adb36d2418476e907de19a641fa7baf80b1abb2bacd8ee5dbdd44e246b88be1636df6b8769
af790aa8721622481085e33c32e6e119dbd
!
vlan 1
!
!
!
!
ip route 0.0.0.0 0.0.0.0 192.168.1.254
tzidx 0
exec-timeout autologout 0
poe ping-check enable
access-list ace 2 ingress interface GigabitEthernet 1/2 action deny
access-list ace 1 next 2 ingress interface GigabitEthernet 1/2 frame-type ipv4-tcp dport 443
system name SISPM1040-384-LRT-C
system description Managed Hardened PoE+ Switch, (8) 10/100/1000Base-T PoE+ Ports + (4)
100/1000Base-X SFP
!
interface GigabitEthernet 1/1
 no spanning-tree
 lldp cdp-aware
 poe ping-ip-addr 192.168.1.100
 poe failure-action reboot-Remote-PD
!
interface GigabitEthernet 1/2
 no spanning-tree
 lldp cdp-aware
 speed 1000
 duplex full
!
interface GigabitEthernet 1/3
 no spanning-tree
 switchport trunk allowed vlan 5,20
 switchport trunk vlan tag native
 switchport mode trunk
 lldp cdp-aware
 poe mode disable
!
interface GigabitEthernet 1/4
 no spanning-tree
 switchport trunk allowed vlan 5,10
 switchport trunk vlan tag native
 switchport mode trunk
 lldp cdp-aware
 poe mode disable
!
interface GigabitEthernet 1/5
 no spanning-tree
 switchport trunk allowed vlan 5,10,20
 switchport trunk vlan tag native
 switchport mode trunk
 lldp cdp-aware
 poe mode disable
!
interface GigabitEthernet 1/6
 no spanning-tree
 lldp cdp-aware
!
interface GigabitEthernet 1/7
 lldp cdp-aware
!
interface GigabitEthernet 1/8
 lldp cdp-aware
!
interface GigabitEthernet 1/9
 no spanning-tree
 switchport trunk allowed vlan 1,50,100
 switchport trunk vlan tag native
 lldp cdp-aware
!
interface GigabitEthernet 1/10
 no spanning-tree
 lldp cdp-aware
!
interface GigabitEthernet 1/11
 no spanning-tree
 lldp cdp-aware
!
interface GigabitEthernet 1/12
 no spanning-tree
 lldp cdp-aware
!
interface vlan 1
 ip address 192.168.1.95 255.255.255.0
 ip dhcp server
!
mep 1 down domain port level 4 interface GigabitEthernet 1/3
mep 1 mep-id 3
mep 1 vid 20
mep 1 peer-mep-id 8 mac 00-C0-F2-53-F0-BA
mep 1 cc 7
mep 1 aps 7 raps
mep 2 down domain port level 4 interface GigabitEthernet 1/4
mep 2 mep-id 4
mep 2 vid 10
mep 2 peer-mep-id 1 mac 00-C0-F2-49-39-5F
mep 2 cc 7
mep 2 aps 7 raps
mep 3 down domain port level 4 interface GigabitEthernet 1/5
mep 3 mep-id 9
mep 3 vid 10
mep 3 peer-mep-id 10 mac 00-C0-F2-53-EF-FE
mep 3 cc 7
mep 3 aps 7 raps
erps 1 major port0 interface GigabitEthernet 1/5 port1 interface GigabitEthernet 1/4
erps 1 mep port0 sf 3 aps 3 port1 sf 2 aps 2
erps 1 rpl neighbor port1
erps 1 vlan 5
erps 2 sub port0 interface GigabitEthernet 1/3 interconnect 1
erps 2 mep port0 sf 1 aps 1
erps 2 rpl neighbor port0
erps 2 vlan 5
!
spanning-tree aggregation
 no spanning-tree
 spanning-tree link-type point-to-point
!
!
line console 0
```

```
!
line vty 0
!
line vty 1
!
line vty 2
!
line vty 3
!
line vty 4
!
line vty 5
!
line vty 6
!
line vty 7
!
line vty 8
!
line vty 9
!
line vty 10
!
line vty 11
!
line vty 12
!
line vty 13
!
line vty 14
!
line vty 15
!
map-api-key AIzaSyBItuM0hDtK6nJeZPEk7jnrcoGGi92EpFM
!
end
```

running-config_192.168.1

```
hostname SISPM1040-362-LRT-W
username admin privilege 15 password encrypted
6158ed7daf39d06ded0e7c4828c3b15bb4c40673bd445afcd643295925ae425d9611d1cbe872708237571aacc7b92
37f33b01ae6866e2484009edfe1fa0bf56f
!
vlan 1
!
!
!
!
ip route 0.0.0.0 0.0.0.0 192.168.1.254
tzidx 0
exec-timeout autologout 0
snmp-server location DT Lab Ring
system name SISPM1040-362-LRT-W
system location DT Lab Ring
system description Managed Hardened PoE+ Switch, (4) 10/100/1000Base-T PoE+ Ports + (2)
10/100/1000Base-T Ports + (2) 100/1000Base-X SFP Ports
!
interface GigabitEthernet 1/1
!
interface GigabitEthernet 1/2
!
interface GigabitEthernet 1/3
 no spanning-tree
 switchport trunk allowed vlan 5,20
 switchport trunk vlan tag native
 switchport mode trunk
 poe mode disable
!
interface GigabitEthernet 1/4
 no spanning-tree
 switchport trunk allowed vlan 5,20
 switchport trunk vlan tag native
 switchport mode trunk
 poe mode disable
!
interface GigabitEthernet 1/5
!
interface GigabitEthernet 1/6
!
interface GigabitEthernet 1/7
!
interface GigabitEthernet 1/8
!
interface vlan 1
 ip address 192.168.1.125 255.255.255.0
 ip dhcp server
!
mep 1 down domain port level 4 interface GigabitEthernet 1/3
mep 1 mep-id 7
mep 1 vid 20
mep 1 peer-mep-id 6 mac 00-C0-F2-53-EF-FD
mep 1 cc 7
mep 1 aps 7 raps
mep 2 down domain port level 4 interface GigabitEthernet 1/4
mep 2 mep-id 8
mep 2 vid 20
mep 2 peer-mep-id 3 mac 00-40-C7-1C-C7-2F
mep 2 cc 7
mep 2 aps 7 raps
```

```
erps 1 sub port0 interface GigabitEthernet 1/3 port1 interface GigabitEthernet 1/4
erps 1 mep port0 sf 1 aps 1 port1 sf 2 aps 2
erps 1 rpl owner port1
erps 1 vlan 5
!
spanning-tree aggregation
 spanning-tree link-type point-to-point
!
!
line console 0
!
line vty 0
!
line vty 1
!
line vty 2
!
line vty 3
!
line vty 4
!
line vty 5
!
line vty 6
!
line vty 7
!
line vty 8
!
line vty 9
!
line vty 10
!
line vty 11
!
line vty 12
!
line vty 13
!
line vty 14
!
line vty 15
!
!
end
```

LANTRONIX®

Lantronix Corporate Headquarters

7535 Irvine Center Drive
Suite100
Irvine, CA 92618, USA
Toll Free: 800-526-8766
Phone: 949-453-3990
Fax: 949-453-3995

Technical Support
Online: https://www.lantronix.com/technical-support/

Sales Offices
For a current list of our domestic and international sales offices, go to the Lantronix web site at www.lantronix.com/about/contact.