SISPM1040-3xxx-L

Managed Hardened Gigabit Ethernet PoE+ Rack Mountable Switches

SISPM1040-3166-L Managed Hardened Gigabit Ethernet PoE+ Switch, (16) 10/100/1000Base-T PoE+ ports + (4) 100/1000Base-X SFP/RJ-45 Combo + (2) 1G/10G SFP+

SISPM1040-3248-L Managed Hardened Gigabit Ethernet PoE+ Switch, (24) 10/100/1000Base-T PoE+ ports + (4) 100/1000Base-X SFP/RJ-45 Combo + (4) 1G/10G SFP+

Web User Guide

Part Number 33763
Revision H August 2024

Intellectual Property

Warranty

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

Contacts

Lantronix Corporate Headquarters
48 Discovery, Suite 250
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.

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.	Comments
3/15/21	F	FW v8.50.0018: Include one step FW version update. Fix API “get fw upgrade status”. Fix API response if changing IP address. Fix Backup Config issue. Fix LLDP PMD Auto-Negotiation Advertised Capability field. Modify "Always On PoE" to be enabled and displayed on Web UI after upgrading to FW v8.50.0018 or above. Fixes: MRP_Ring state "unknown" issue when cable removed. Add "PoE Firmware Version" data in API get_poe_config. Provide "profile selection" when using API get_poe_config to get PoE schedule.
8/20/21	G	FW v8.50.0032: add Memory Usage info on the system information; fix API Save config problem. Fix change PoE mode from Force mode and MIB PoE Config Port PoE Mode issues. Add new API commands and fix existing API commands. Fix traceroute IPv6 in the Web UI.
8/23/24	H	FW v8.50.0149: Add Percepxion and LPM. ♦ Add option to reboot the switch when DI input goes High. ♦ Change the content of Syslog app name to the switch serial number. ♦ Add DHCP per Port VLAN. ♦ Initial Lantronix rebrand. ♦ Add First Time Wizard. ♦ Change SNMP mode default and Auth Method default. ♦ Update SSH. ♦ Change self-signed certificates and update TLSv1.2 ciphers. ♦ Allow special characters in Web PoE profile name. ♦ Allow - (dash) character for status update interval and content check interval and switch disconnect from server. ♦ Fix PoE Firmware version and PoE power issues. ♦ Allow to delete VLAN1 on web GUI. See the Release Notes for details.

Contents

Chapter 1 - Introduction

The SISPM1040-3xxx-L switches are next-generation rack mount industrial grade Ethernet switches offering powerful L2 and basic L3 features with advanced functionality and usability. In addition to the extensive management features, the SISPM1040-3xxx-L also provide Carrier Ethernet features such as OAM, CFM, ERPS, EPS, and PTPv2 which makes it suitable for industrial and Carrier Ethernet applications.

The **SISPM1040-3248-L** delivers 24 (10M/100M/1G) RJ45/PoE+ (support 802.3at/af, and total up to 250W/370W) ports, 4 GbE SFP ports, 2/4 GbE/10G SFP+ ports and one RJ45 Console port.

The **SISPM1040-3166-L** provides (16) 10/100/1000Base-T PoE+ ports, (4) 100/1000Base-X SFP/RJ-45 Combo and (2) 1G/10G SFP+ ports.

1-1 Key Features

- DMS (Device Management System) built in
- Carrier Ethernet features for easier manageability, security, and QoS
- IEEE 1588v2 PTP
- IEEE 802.3ah OAM
- IEEE 802.1ag CFM (ITU-T Y.1731 Performance Monitoring)
- ITU-T Y.1564 (RFC2544) Ethernet Service Activation Test
- ITU-T G.8031 Ethernet Linear Protection Switching (EPS)
- ITU-T G.8032 Ethernet Ring Protection Switching (ERPS)
- DHCP Server, Relay, and Snooping configuration and statistics
- IPv4/IPv6 L3 Static route
- PoE features (compliant with IEEE 802.3at PoE+ and af PoE); PoE Config, Scheduling, Power Delay, Auto Power Reset, Traffic Monitoring, Always on PoE)
- Rapid Ring configuration
- MRP (Media Redundancy Protocol)
- Percepxion and LPM (Lantronix Provisioning Manager) support

1-2 About This Manual

This manual gives specific information on how to operate and use the management functions of the SISPM1040-3xxx-L via HTTP/HTTPs web browser. This manual documents two similar models; differences are noted where they exist. This manual is intended for use by network administrators who are responsible for operating and maintaining network equipment; it assumes a working knowledge of general switch functions, the Internet Protocol (IP), and Hypertext Transfer Protocol (HTTP). Note that this manual provides links to third party websites for which Lantronix is not responsible.

1-3 Related Manuals

A printed Quick Start Guide is shipped with each device. For Lantronix Firmware, Manuals, Application Notes, etc. go to the Product Support webpage (logon required). Other related manuals are listed below.

- SISPM1040-3xxx-L Quick Start Guide, 33761
- SISPM1040-3xxx-L Install Guide, 33762
- SISPM1040-3xxx-L CLI Reference, 33764
- SISPM1040-3248-L and 3166-L API User Guide, 33831
- Release Notes (version specific)

Chapter 2 - Web User Interface

2-1 Initial Login

This chapter describes how to configure and manage the SISPM1040-3xxx-L via the web user interface (UI). The web UI lets you configure and monitor switch operating parameters via any switch port. The factory 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 SISPM1040-3xxx-L interface configuration is finished, you can browse it. For instance, type **192.168.1.77** in the address row in a browser and hit Enter. The Login screen displays for you to enter the Username and Password in order to access the web UI.

The default username is **admin** and password is **admin**. For first time use, enter the default Username and Password, and then click the **Login** button. The login process now is complete. In this login menu, you must enter the complete Username and Password respectively; the SISPM1040-3xxx-L will not give you a shortcut to the Username / Password automatically. This looks inconvenient but is safer.

The SISPM1040-3xxx-L allows two or more users with administrator rights to manage the switch. Whichever administrator did the last setting will be the one whose configuration affects the switch. When you log in to the SISPM1040-3xxx-L web UI, you can use either IPv4 or IPv6 to login to manage. To optimize the display effect, we recommend Microsoft IE 6.0 above, Netscape V7.1 above or Firefox V1.00 above and have the resolution 1024x768. The switch supports neutral web browser interface.

Note: The SISPM1040-3xxx-L has the DHCP server function disabled by default; if you do not have a DHCP server providing IP addresses to the switch, the switch defaults to IP address 192.168.1.77.

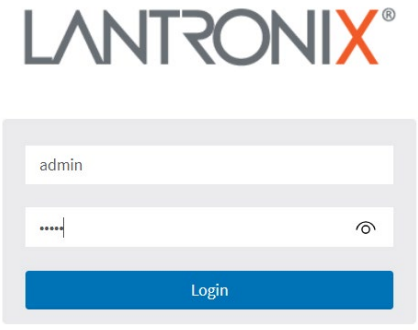


Figure 1: Login page


: Click to show the Login text as you enter it.


: Click to hide the Login text as you enter it (default).

2-2 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. The First Time Wizard was added at FW v8.50.0070. 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.

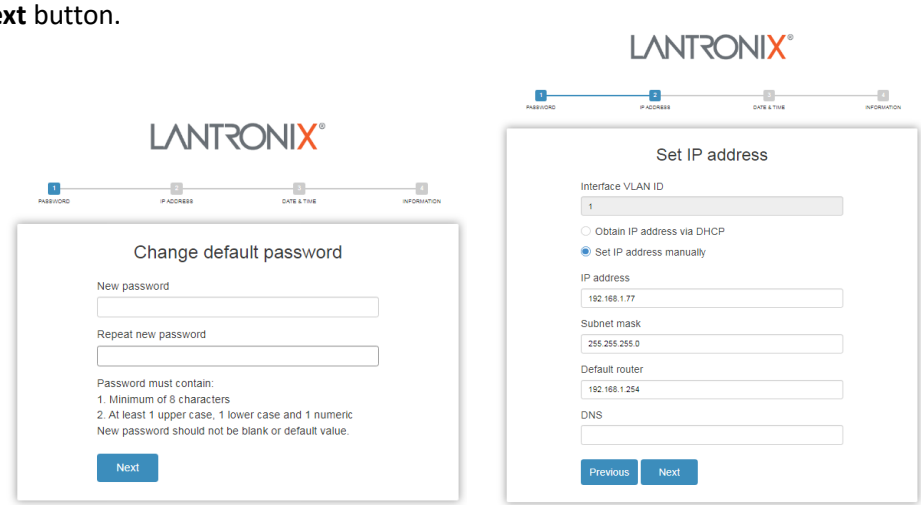


Figure 2-1: Change default password

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.

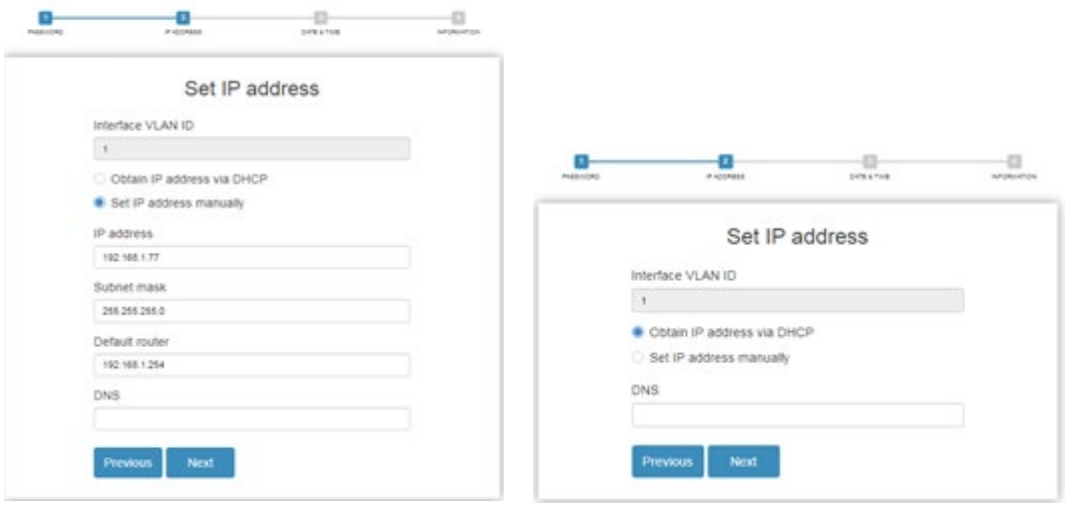


Figure 2-2a: Set IP address

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.

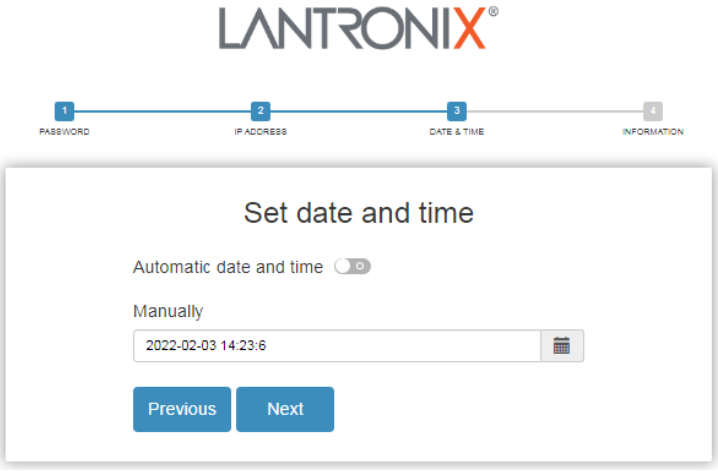


Figure 2-3: Set date and time

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.

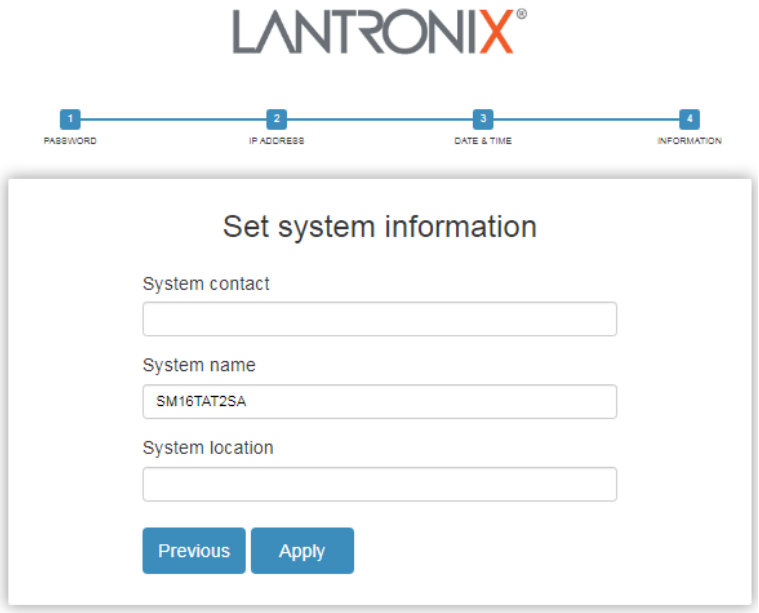


Figure 2-4: Set system information

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.

Notes:

The First Time Wizard only displays on the switch web GUI. If you have logged in via CLI or Console and have saved changes to the running-config file, the First Time Wizard will not display in the web UI.

The First Time Wizard displays when you use the hardware Reset button to reset the switch. Press the Reset button for over 10 seconds; when the front panel LEDs light then release the Reset button; the First Time Wizard then displays.

2-3 Webpage Controls

The Web UI navigation controls are shown and described below.

: Logo; click to return to startup page (Monitor > System > Information) from any webpage.

: Icon to show / hide left hand menu items.

: Device icon with links to Detailed Port Statistics pages.

Click Save Button : **Click Save Button** icon; displays when a page parameter has changed but has not yet been saved.

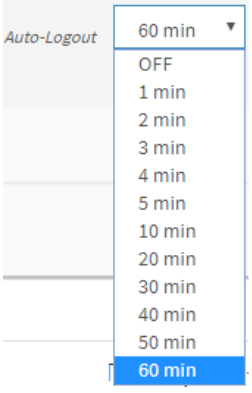
: **Save** changes to startup-config file. At the confirmation prompt "*Are you sure you want to save running-config to startup-config?*" click the OK button. During save configuration, Do not reset or power off the switch!

: **Help**; Click to display online help for the current webpage.

: **Log out** : click to log out of the Web UI. The Login page displays again.

Home > System > System Information : **Menu path** for the currently-displayed webpage.

Auto-Logout 60 min : **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 (default), 20, 30, 40, and 60 minutes. When you select an auto-logout you must click the Save button for it take effect. Save changes is retained after reboot/restart; however, if you reset the switch to factory defaults, then Auto-Logout goes back to its default of 10 min. (added at FW v8.40.1778).



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, run the CLI command "showing running-config".
To save the timeout change into startup-config, you must do a save to startup-config and then reboot the switch.

Auto-Logout 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 disc icon), the changed timeout setting will be applied to running-config and start-up config immediately.	When the 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.

Webpage Messages

Message: *Wrong username or password!*
Recovery: Re-try the login with the correct username and password credentials.

Message: *There are too many users in the system.*
Recovery: Try to log in later.

Chapter 3 - System Configuration

This chapter describes the Web UI sub-menus and their parameters.

3-1 System Information

This page displays device information and lets you identify the system with a system name, location and contact.

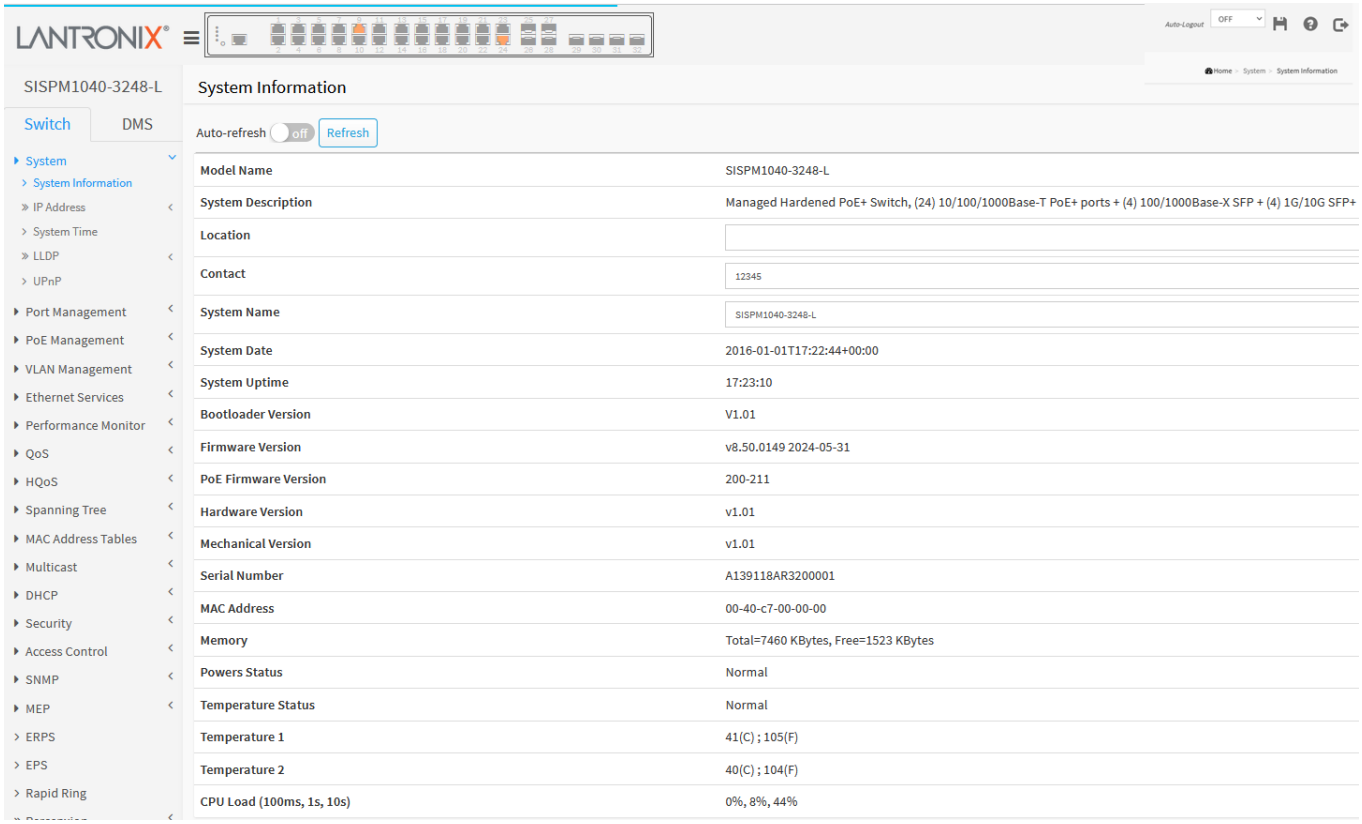


Figure 2-1: System Information

Parameter descriptions:

Model Name: Displays the factory defined model name for identification purposes (e.g., *SISPM1040-3248-L* or *SISPM1040-3166-L*).

System Description: Displays the system description (e.g., *Managed Hardened PoE+ Switch, (24). 10/100/1000Base-T PoE+ ports + (4) 100/1000Base-X SFP/RJ-45 Combo + (4) 1G/10G SFP+*).

Location: Enter a system location for this switch.

Contact: Enter a system contact for this switch.

System Name: Displays the system name (e.g., *SISPM1040-3166-L*).

System Date: The current (GMT) system time and date. The system time is obtained via the Timing server running on the switch, if any. The format is *2021-02-04T14:31:51+00:00*.

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

Bootloader Version: Displays the current boot loader version number (e.g., *V1.01*).

Firmware Version: The software version and date of the firmware on this switch (e.g., *v8.50.0149 2024-05-31*).

PoE Firmware Version: The version of the PoE chip (e.g., *200-211*).

Hardware Version: Displays the hardware version of the device (e.g., *v1.01*).

Mechanical Version: Displays the mechanical version of the device (e.g., *v1.01*).

Serial Number: The serial number of this switch (e.g., *A142118AR3600001* or *A139119BR2500001*).

MAC Address: The MAC Address of this switch (in the format 11-22-33-44-55-66).

Memory: Displays the amount of total and free memory in Kbytes.

Powers Status: Displays the powers status of the system(e.g., *Normal*).

Temperature Status: Displays the temperature status of the system. (e.g., *Normal*).

Temperature 1: The temperature at sensor 1. For example: 40(C) ; 104(F).

Temperature 2: The temperature at sensor 2. For example:39(C) ; 102(F)

CPU Load (100ms, 1s, 10s): Displays the cpu loading (100ms, 1s, 10s) of the system (e.g., *0%, 7%, 5%*).

Buttons

Refresh : Click to manually refresh the page immediately.

Auto-refresh : Click to refresh the page automatically every 3 seconds.

Apply : Click to save changes.

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

3-2 IP Address

3-2.1 Settings

This page lets you set basic IP parameters. 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.

To configure IP Settings in the web UI:

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

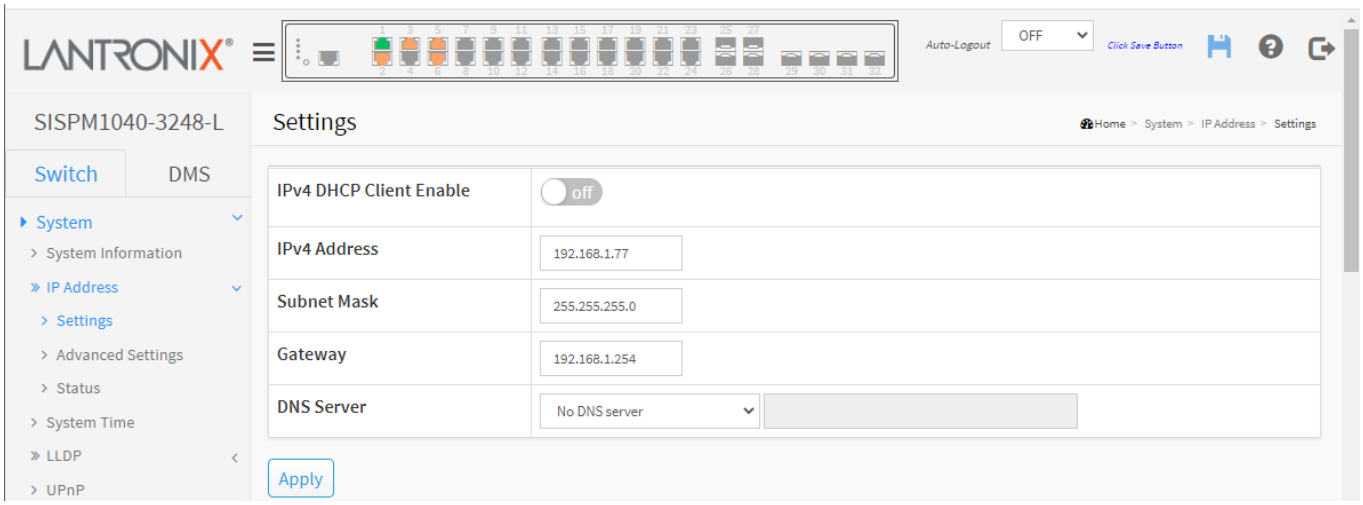


Figure 3-2.1: IP Settings

Parameter descriptions:

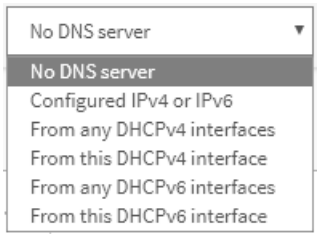
IPv4 DHCP Client Enable : Enable the DHCP client by checking this box. If this option is enabled, the system will configure the IPv4 address and mask of the interface using the DHCP protocol. The DHCP client will announce the configured System Name as hostname to provide DNS lookup.

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

Subnet Mask : The IPv4 network mask, in number of bits (prefix length). Valid values are 0 - 30 bits for an 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 if no DHCP fallback address is desired. The default is 255.255.255.0.

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

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



No DNS server : No DNS server will be used (default).

Configured IPv4 : Explicitly provide the valid IPv4 unicast address of the DNS Server in dotted decimal notation. Make sure the configured DNS server is 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.

3-2.2 Advanced Settings

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

To configure Advanced 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.

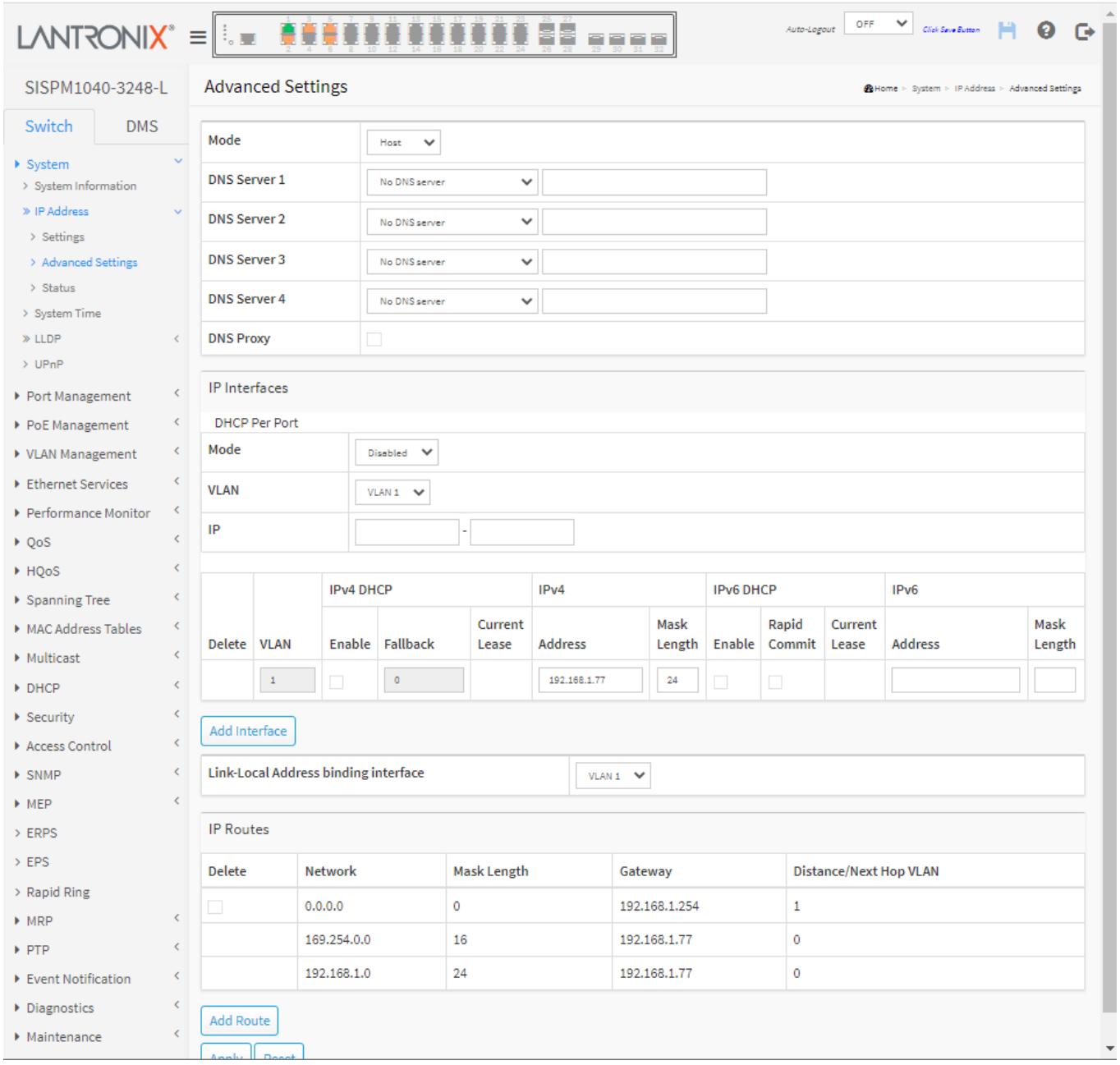


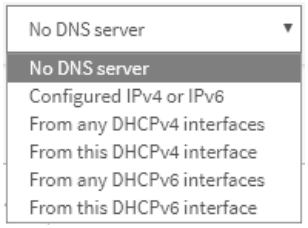
Figure 3-2.2: Advanced IP Settings

Parameter descriptions:

Advanced Settings

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

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

DHCP Per Port Mode : Enable or Disable DHCP per port. The default is Disabled. See Appendix A – DHCP Per Port Configuration on page 481 for more information.

DHCP Per Port VLAN : Set DHCP per port 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.

DHCP Per Port IP : Define the IP address range for DHCP per port. The DHCP Per Port IP range must be equal to switch twisted-pair port number (24). See Appendix A – DHCP Per Port Configuration on page 481 for more information.

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

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

IPv4 DHCP Current Lease: For DHCP interfaces with an active lease, this column shows the current interface address, as provided by the DHCP server.

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

IPv4 Mask Length: The IPv4 network mask, in number of bits (prefix length). Valid values are between 0 and 30 bits for an 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. An IPv6 address is in 128-bit records represented as eight fields of up to four hexadecimal digits with a colon separating each field (:). For example, fe80::215:c5ff:fe03:4dc7. The symbol :: is a special syntax that can be used as a shorthand way of representing multiple 16-bit groups of contiguous zeros; but it can appear only once. It can also represent a legally valid IPv4 address. For example, ::192.1.2.34. This 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 an IPv6 address. The field may be left blank if IPv6 operation on the interface is not desired.

Link-Local Address binding interface: Configure Link-Local IP address to different VLAN interface. The first IP interface entry is for default value.

IP Routes

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

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

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

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

Distance/Next Hop VLAN :

Distance (Only for IPv4) : The distance value of route entry is used to provide the priority information of the routing protocols to routers. When there are two or more different routing protocols are involved and have the same destination, the distance value can be used to select the best path.

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 4095 and will be effective only when the corresponding IPv6 interface is valid.
If the IPv6 gateway address is link-local, it must specify the next hop VLAN for the gateway.
If the IPv6 gateway address is not link-local, the system ignores the next hop VLAN for the gateway.

Buttons

Add Interface : Click to add a new IP interface. A maximum of 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. The message "*Update success!*" displays when successful.

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

Messages

Message: *DHCP Per Port IP range (192.168.1.78 - 192.168.1.98) is not equal to switch TP port number (24)*
Recovery : Click OK to clear the message and re-enter the DHCP Per Port IP parameter as described above.

Message: *DHCP Per Port IP range (192.168.1.70 - 192.168.1.98) includes interface IP address (192.168.1.77)*
Recovery : Click OK to clear the message and re-enter the DHCP Per Port IP parameter as described above.

Message: *Update Success!*
Meaning: Click OK to clear the message and continue operation.

3-2.3 Status

3-2.3.1 IP Status

This page displays the status of the IP protocol layer. The status displayed includes the IP interfaces, IP routes and neighbor cache (ARP cache) status. To display IP status in the web UI:

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

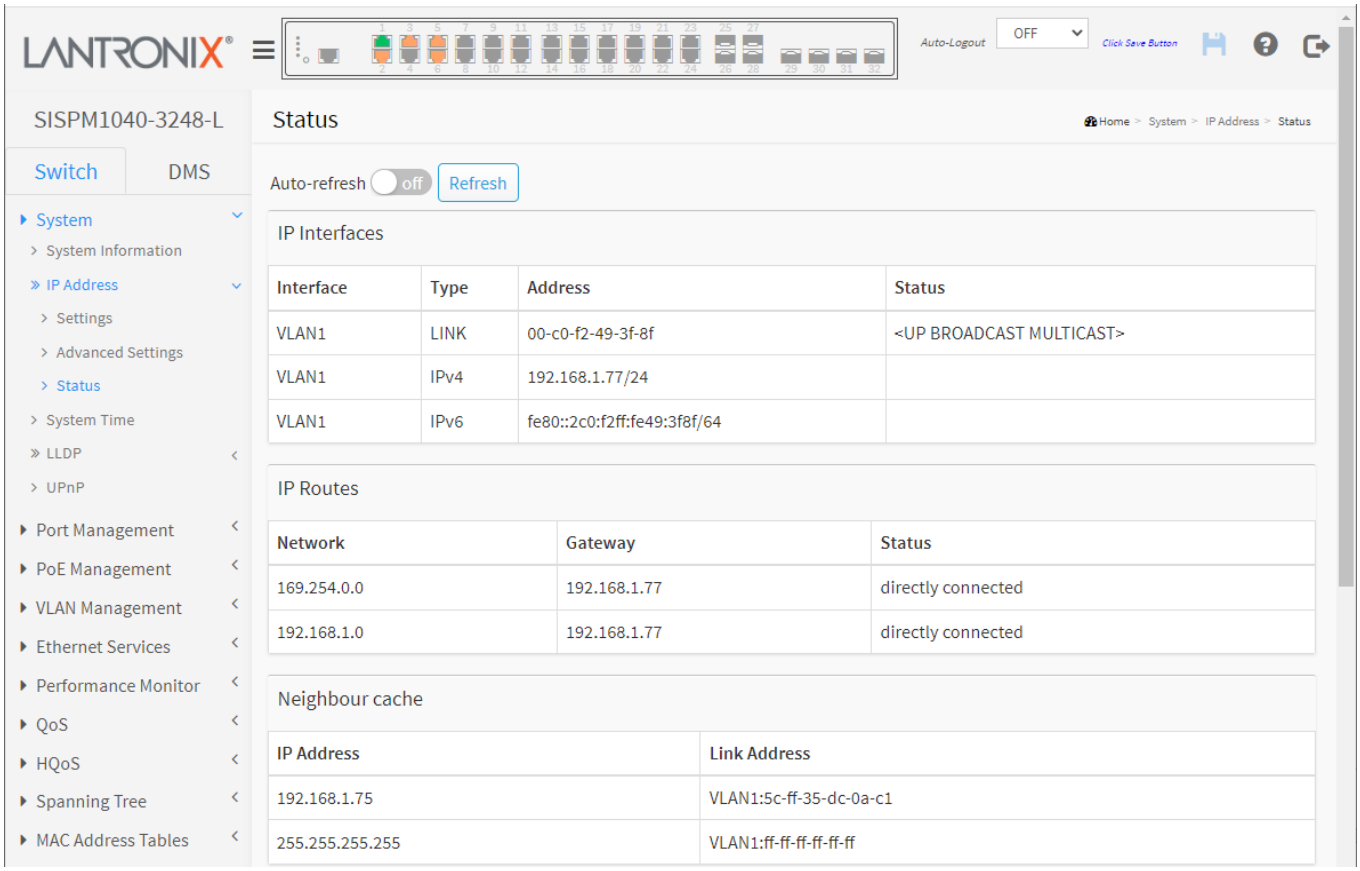


Figure 3-2.3.1: IP Status

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 (e.g., directly connected) 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 exist.

Buttons

Auto-refresh : Click to refresh the page automatically every 3 seconds.

Refresh : Click to manually refresh the page immediately.

3-3 System Time

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

To configure Time in the web UI:

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

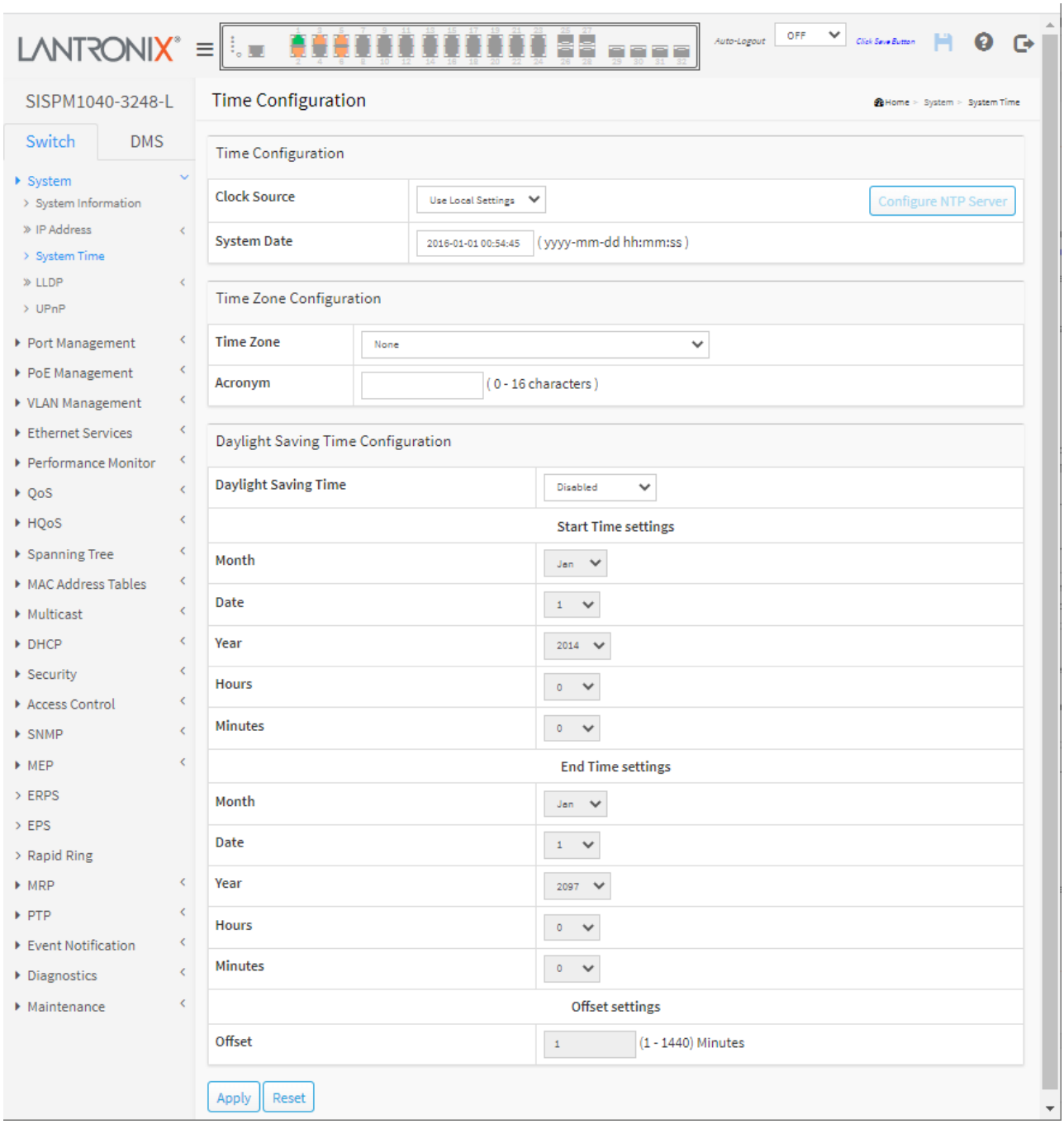


Figure 2-3: Time Configuration

Parameter descriptions:

Time Configuration

Clock Source : There are two modes for configuring Clock Source. Select "Use Local Settings" to use Clock Source from Local Time. Select “Use NTP Server" to use Clock Source from an NTP Server; this enables the “Configure NTP Server” button. See the “Configure NTP Server” section below.

System Date : Show the current date and time of the system in the format *yyyy-mm-dd hh:mm:ss*.

Time Zone Configuration

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

Acronym : Lets you set the acronym of the time zone. This is a user-configurable acronym to identify the time zone. (Range: Up to 16 characters.)

Daylight Saving Time Configuration

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

Start time settings : Week - Select the starting week number.

Day - Select the starting day.
Month - Select the starting month.
Hours - Select the starting hour.
Minutes - Select the starting minute.

End time settings :

Week - Select the ending week number.
Day - Select the ending day.
Month - Select the ending month.
Hours - Select the ending hour.
Minutes - Select the starting minute.

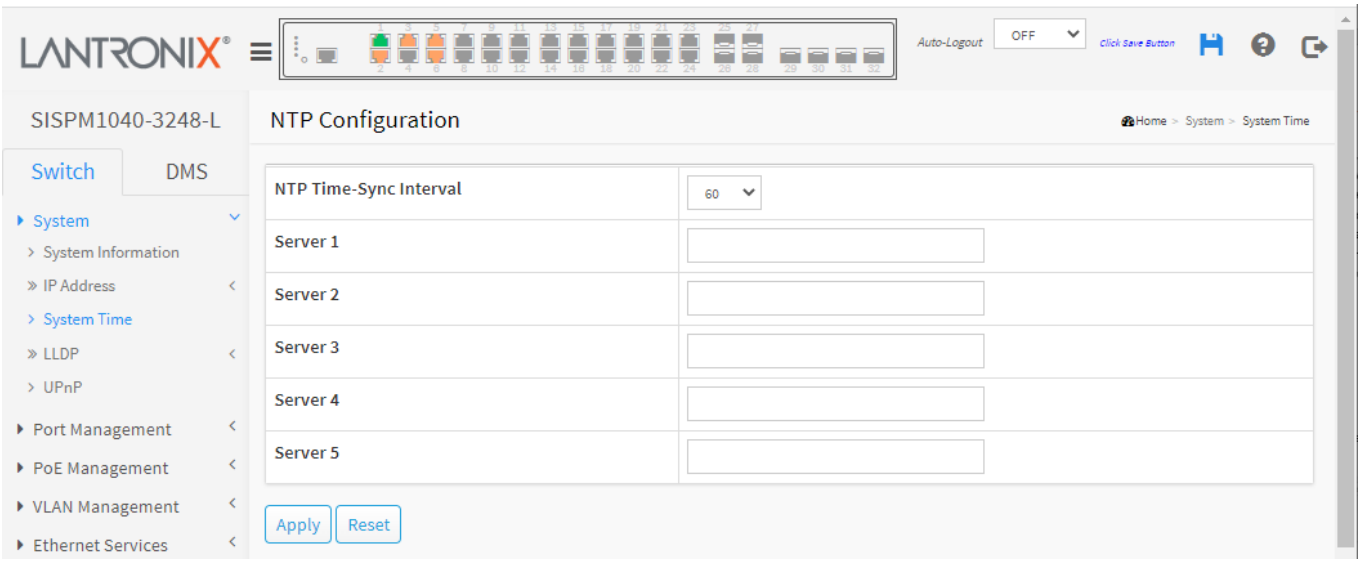
Offset settings : Offset - Enter the number of minutes to add during Daylight Saving Time. (Range: 1 - 1440)
Note: The “Start Time Settings” and “End Time Settings” displays what you set in the “Start Time Settings” and “End Time Settings” fields.

Buttons

Apply : Click to save changes.

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

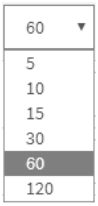
Configure NTP Server: Click this button to configure NTP server, when 'Use NTP Server' is selected at Clock Source select dropdown (see above).



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 after clicking the Apply button. Though it synchronizes the time automatically, NTP does not update the time periodically without user's processing.

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

Parameter descriptions:



NTP Time-Sync Interval: The switch is periodically transmitting NTP frames to its servers for having the network time information up-to-date. The interval between each NTP frame is determined by the NTP Time-Sync Interval value. Valid values are 5, 10, 15, 30, 60, and 120 minutes.

Server 1 to 5: Provide the NTP IPv4 or IPv6 address of this switch. IPv6 address is in 128-bit records represented as eight fields of up to four hexadecimal digits with a colon separating each field (:). For example, 'fe80::215:c5ff:fe03:4dc7'. The symbol '::' is a special syntax that can be used as a shorthand way of representing multiple 16-bit groups of contiguous zeros; but it can only appear once. It can also represent a valid IPv4 address. For example, '::192.1.2.34'.

Buttons:

Apply :Click to save changes.

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

3-4 LLDP

The switch supports the LLDP. The Link Layer Discovery Protocol (LLDP) provides a standards-based method for enabling switches to advertise themselves to adjacent devices and to learn about adjacent LLDP devices. 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 an IEEE 802 local area network, principally wired Ethernet. The protocol is formally referred to by the IEEE as “Station and Media Access Control Connectivity Discovery” specified in standards document IEEE 802.1AB.

3-4.1 LLDP Configuration

You can configure LLDP per port and detail parameters here; the settings will take effect immediately.

To configure LLDP:

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

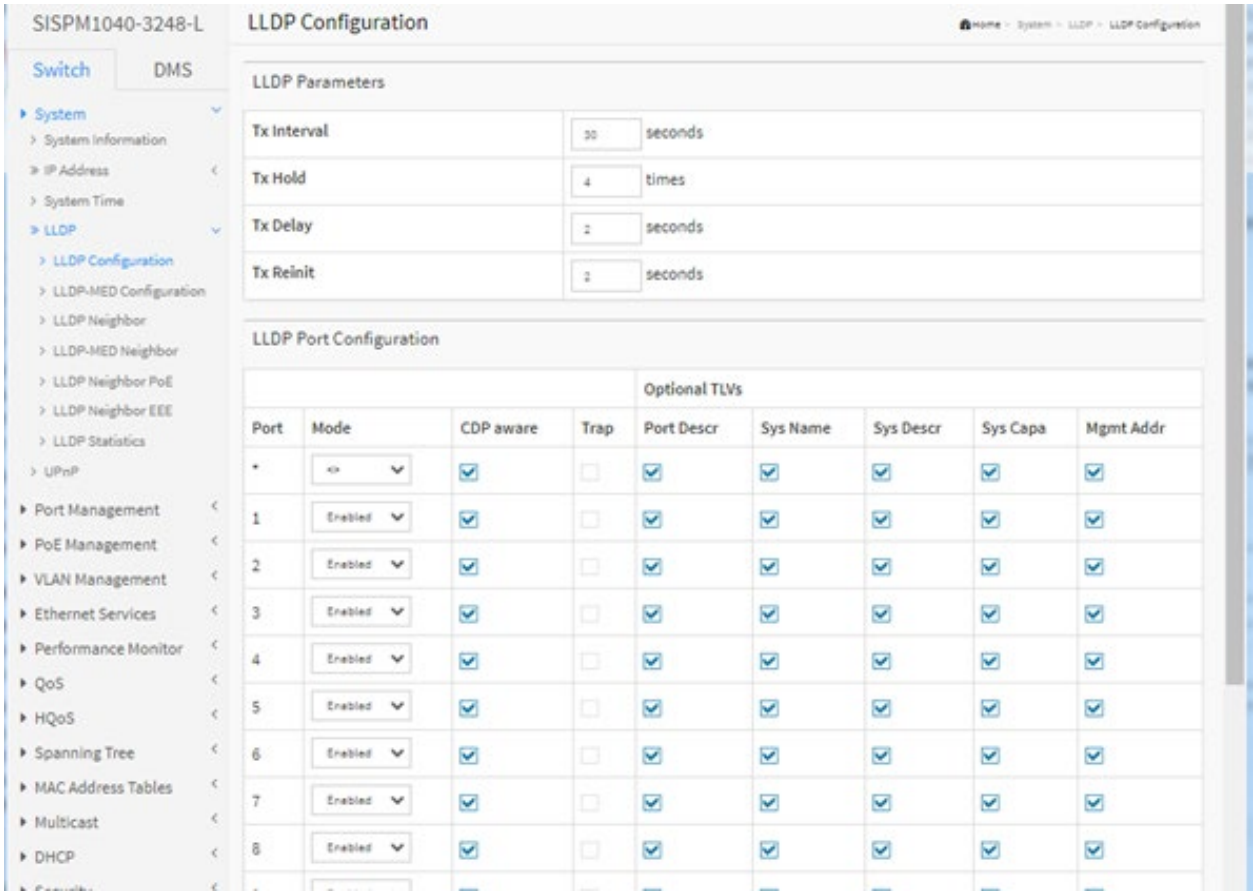


Figure 3-4.1: LLDP Configuration

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 shall be considered valid. The LLDP information valid period is set to Tx Hold multiplied by Tx Interval seconds. Valid values are restricted to 2 - 10 times.

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

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

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

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

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

CDP Aware : Select CDP awareness. 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 neighboring 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.

3-4.2 LLDP-MED Configuration

This page lets you configure the LLDP-MED. This function applies to devices which support LLDP-MED.
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.
- Extended and automated power management of Power over Ethernet (PoE) end points.
- Inventory management, allowing network administrators to track their network devices, and determine their characteristics (manufacturer, software and hardware versions, and serial or asset number).

Web Interface

To configure LLDP-MED:

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

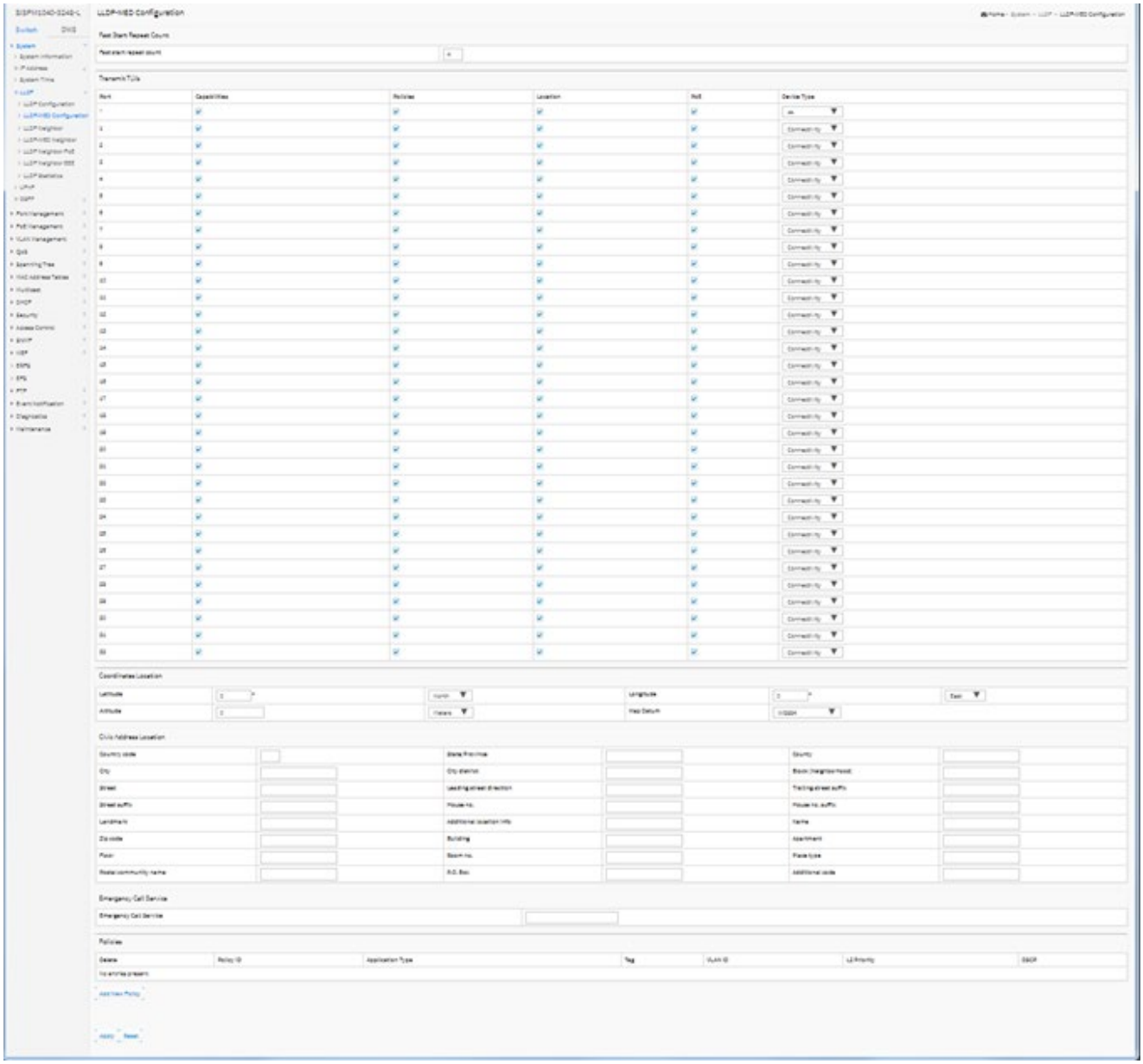


Figure 3-4.2: LLDP-MED Configuration

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

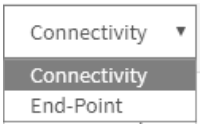
Port : The interface name to which the configuration applies.

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.

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



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

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

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

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

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

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

Even though a switch 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, block.

Street : Street - Example: Poppelvej.

Leading street direction : Leading street direction - Example: N.

Trailing street suffix : Trailing street suffix - Example: SW.

Street suffix : **Street suffix** - Example: Ave, Platz.

House no. : House number - Example: 21.

House no. suffix : House number suffix - Example: A, 1/2.

Landmark : Landmark or vanity address - Example: Columbia University.

Additional location info : Additional location info - Example: South Wing.

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

Zip code : Postal/zip code - Example: 2791.

Building : Building (structure) - Example: Low Library.

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

Floor : Floor - Example: 4.

Room no. : Room number - Example: 450F.

Place type : Place type - Example: Office.

Postal community name : Postal community name - Example: Leonia.

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

Additional code : Additional code - Example: 1320300003.

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

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

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

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

The network policy attributes advertised are:

1. Layer 2 VLAN ID (IEEE 802.1Q-2003)
2. Layer 2 priority value (IEEE 802.1D-2004)
3. Layer 3 Diffserv code point (DSCP) value (IETF RFC 2474): This network policy is potentially advertised and associated with multiple sets of application types supported on a given port. The application types specifically addressed are: 1. Voice, 2. Guest Voice, 3. Softphone Voice, 4. Video Conferencing, 5. Streaming Video, and 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.

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

Delete : Check to delete the policy. It will be deleted immediately.

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

Application Type : Intended use of the application types:

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

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

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

Buttons

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" to save the settings or click “Reset” to clear the settings.

3-4.3 LLDP Neighbor

This page provides a status overview for all LLDP neighbors. The displayed table contains a row for each port on which an LLDP neighbor is detected. If there is no device that supports LLDP in your network then the table will show "*No LLDP neighbor information found*".

To show LLDP neighbors:

1. Click System, LLDP and LLDP Neighbor.
2. Click Refresh to immediately update the page.
3. Click Auto-refresh to automatically update the page every 3 seconds.

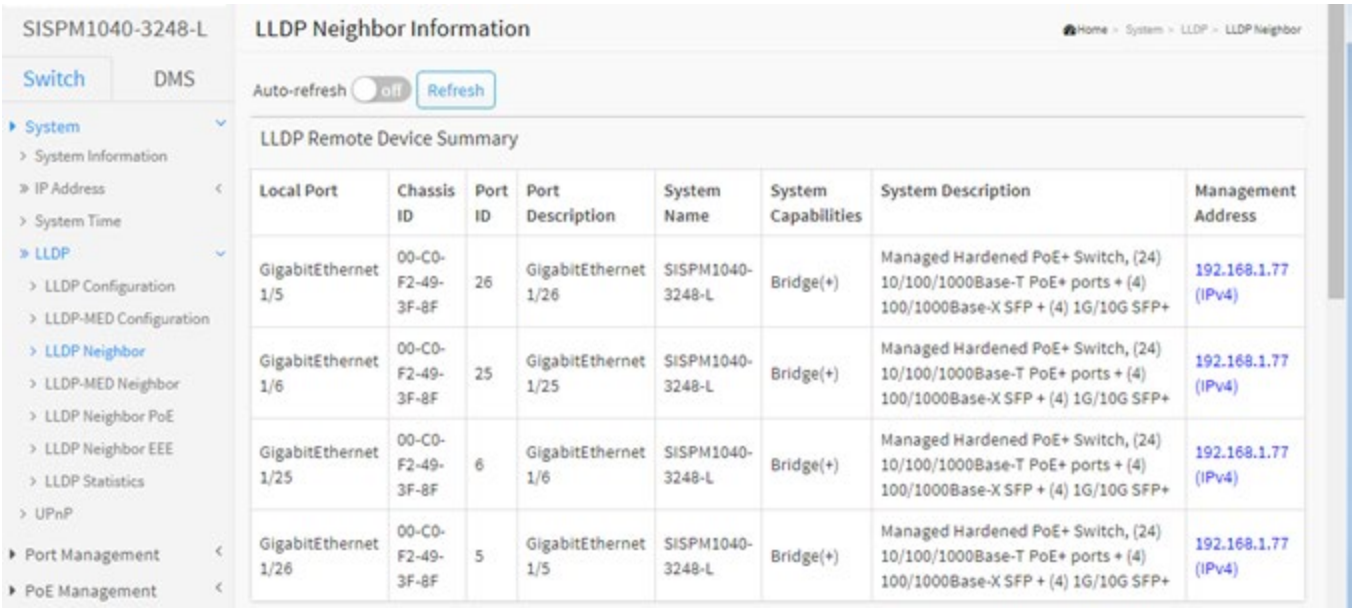


Figure 3-4.3: LLDP Neighbor information

Parameter descriptions:

Local Port : The port on which the LLDP frame was received.

Chassis ID : The identification of the neighbor's LLDP frames.

Port ID : The identification of the neighbor port.

Port Description : The port description advertised by the neighbor unit.

System Name : System Name is the name advertised by the neighbor unit.

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

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

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

System Description: The system description advertised by the neighbor unit (e.g., a camera make, model, and version or *Managed Hardened PoE+ Switch, (24) 10/100/1000Base-T PoE+ ports + (4) 100/1000Base-X SFP + (4) 1G/10G SFP+*).

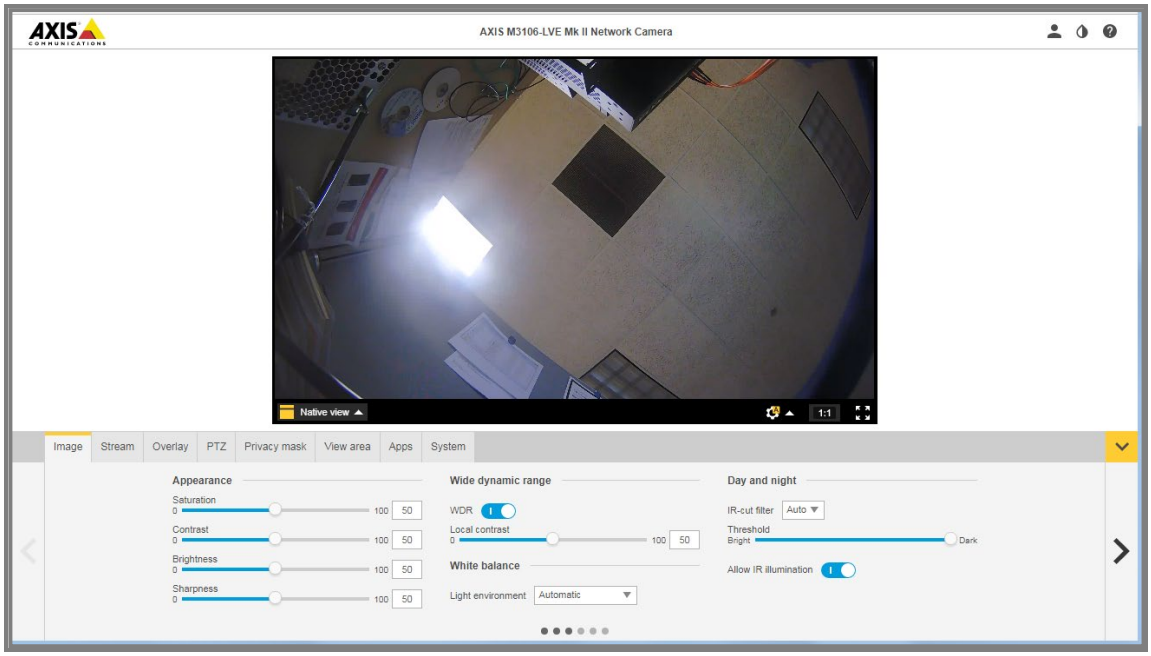
Management Address : Management Address is the neighbor unit's address that is used for higher layer entities to assist discovery by the network management. This could for instance hold the neighbor's IP address. You can click a linked IP address to display the attached device's startup page (see example below).

Buttons

Auto-refresh : Click to refresh the page automatically every 3 seconds.

Refresh : Click to manually refresh the page immediately.

Example: click a linked IP address to display the attached device's startup page:



3-4.4 LLDP-MED Neighbor

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

If no LLDP-MED device is found in your network, the table displays "*No LLDP-MED neighbor information found*".

To show LLDP-MED neighbor information:

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

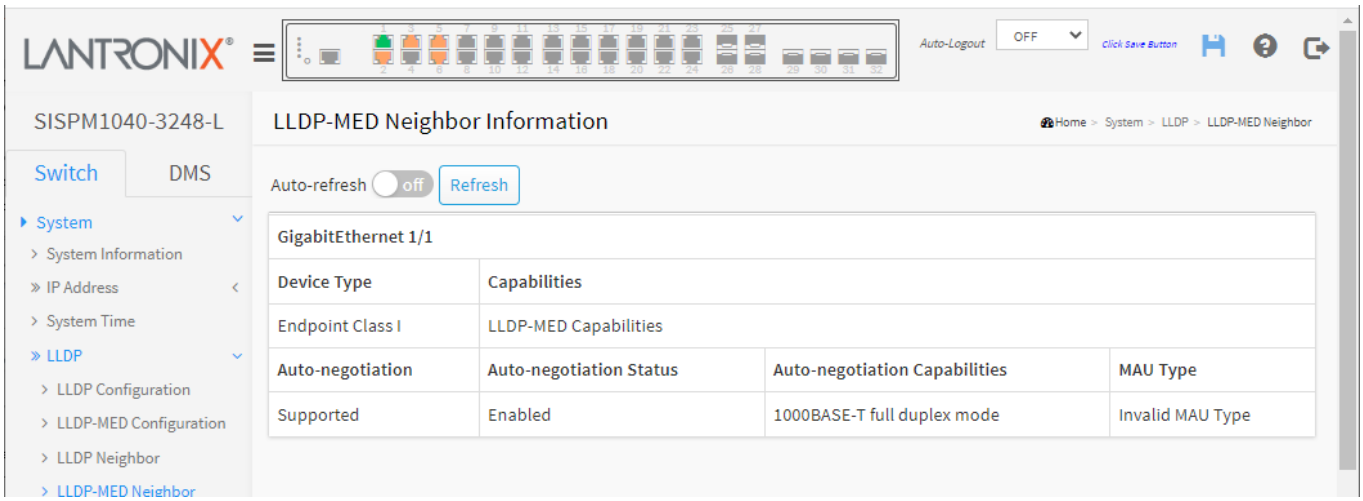


Figure 3-4.4: LLDP-MED Neighbor information

Parameter descriptions:

Port : The interface on which the LLDP frame was received.

Device Type : LLDP-MED Devices are comprised of two primary Device Types: Network Connectivity Devices and Endpoint Devices.

LLDP-MED Network Connectivity Device Definition: LLDP-MED Network Connectivity Devices, as defined in TIA-1057, provide access to the IEEE 802 based LAN infrastructure for LLDP-MED Endpoint Devices. An LLDP-MED Network Connectivity Device is a LAN access device based on any of 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 defined by TIA-1057 and can relay IEEE 802 frames via any method.

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

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

Each LLDP-MED Endpoint Device Class is defined to build upon the capabilities defined for the previous Endpoint

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Defined: The network policy is defined (known).

TAG: indicates whether the specified application type is using a tagged or an untagged VLAN:

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 interface as defined in IEEE 802.1Q-2003. A value of 1 - 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 interface is used instead.

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

DSCP: 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 - 63).

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

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: shows the link partners MAC/PHY capabilities.

Inventory: A list of interface items.

MAU Type: Displays the type of Medium Attachment Unit or "*Invalid MAU Type*".

Buttons

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

Refresh: : Click to manually refresh the page immediately.

3-4.5 LLDP Neighbor PoE

This page provides a status overview for all LLDP PoE neighbors. The displayed table contains a row for each interface on which an LLDP PoE neighbor is detected.

To show LLDP neighbor PoE:

1. Click System, LLDP, and LLDP Neighbor PoE.
2. Click Refresh to immediately update the page.

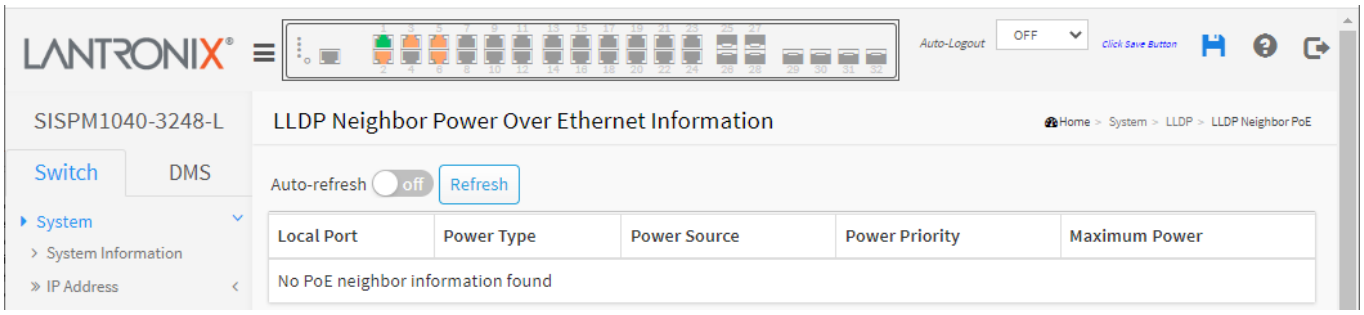


Figure 3-4.5: LLDP Neighbor PoE information

Parameter descriptions:

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

Power Type : Represents whether the device is a Power Sourcing Entity (PSE) or Power Device (PD). If the Power Type is unknown it is represented as "Reserved".

Power Source : Represents the power source being utilized by a PSE or PD device. If the device is a PSE device it can either run on its Primary Power Source or its Backup Power Source. If it is unknown whether the PSE device is using its Primary Power Source or its Backup Power Source it is indicated as "Unknown".

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

Power Priority : Represents the priority of the PD device, or the power priority associated with the PSE type device's interface that is sourcing the power. There are three levels of power priority: Critical, High and Low. If the power priority is unknown it is indicated as "Unknown".

Maximum Power : The Maximum Power Value contains a numerical value that indicates the maximum power in watts required by a PD device from a PSE device, or the minimum power a PSE device is capable of sourcing over a maximum length cable based on its current configuration. The maximum allowed value is 102.3 W. If the device indicates a value higher than 102.3 W, it is represented as "reserved".

Buttons

Auto-refresh : Click to refresh the page automatically every 3 seconds.

Refresh : Click to manually refresh the page immediately.

3-4.6 LLDP Neighbor EEE

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

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

To show LLDP neighbor EEE:

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

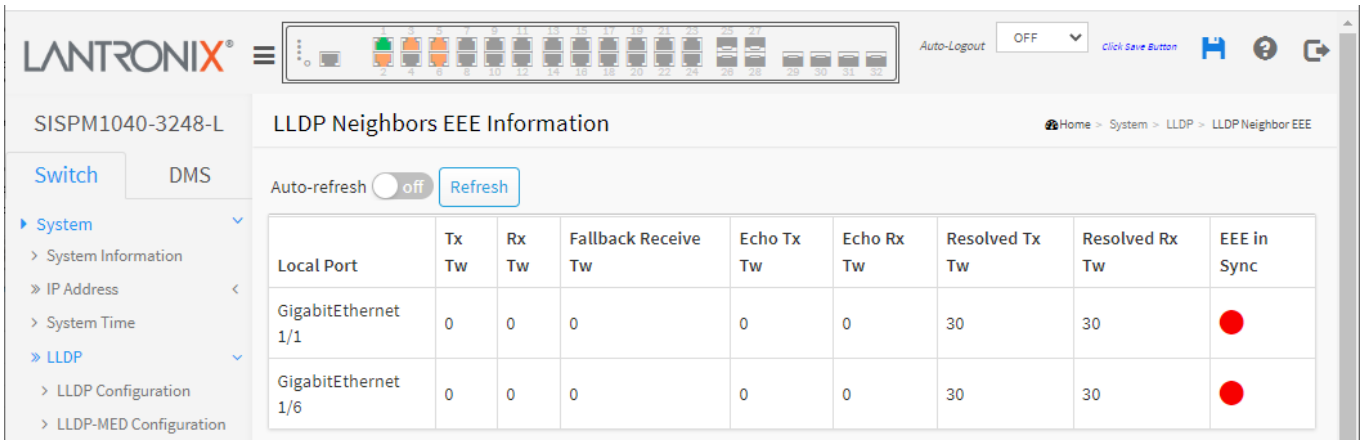


Figure 3-4.6: LLDP Neighbors EEE information

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 (Low Power Idle).

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 is defined as the local link partner's 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 : Click to refresh the page automatically every 3 seconds.

Refresh : Click to manually refresh the page immediately.

3-4.7 LLDP Statistics

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

To show LLDP Statistics:

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

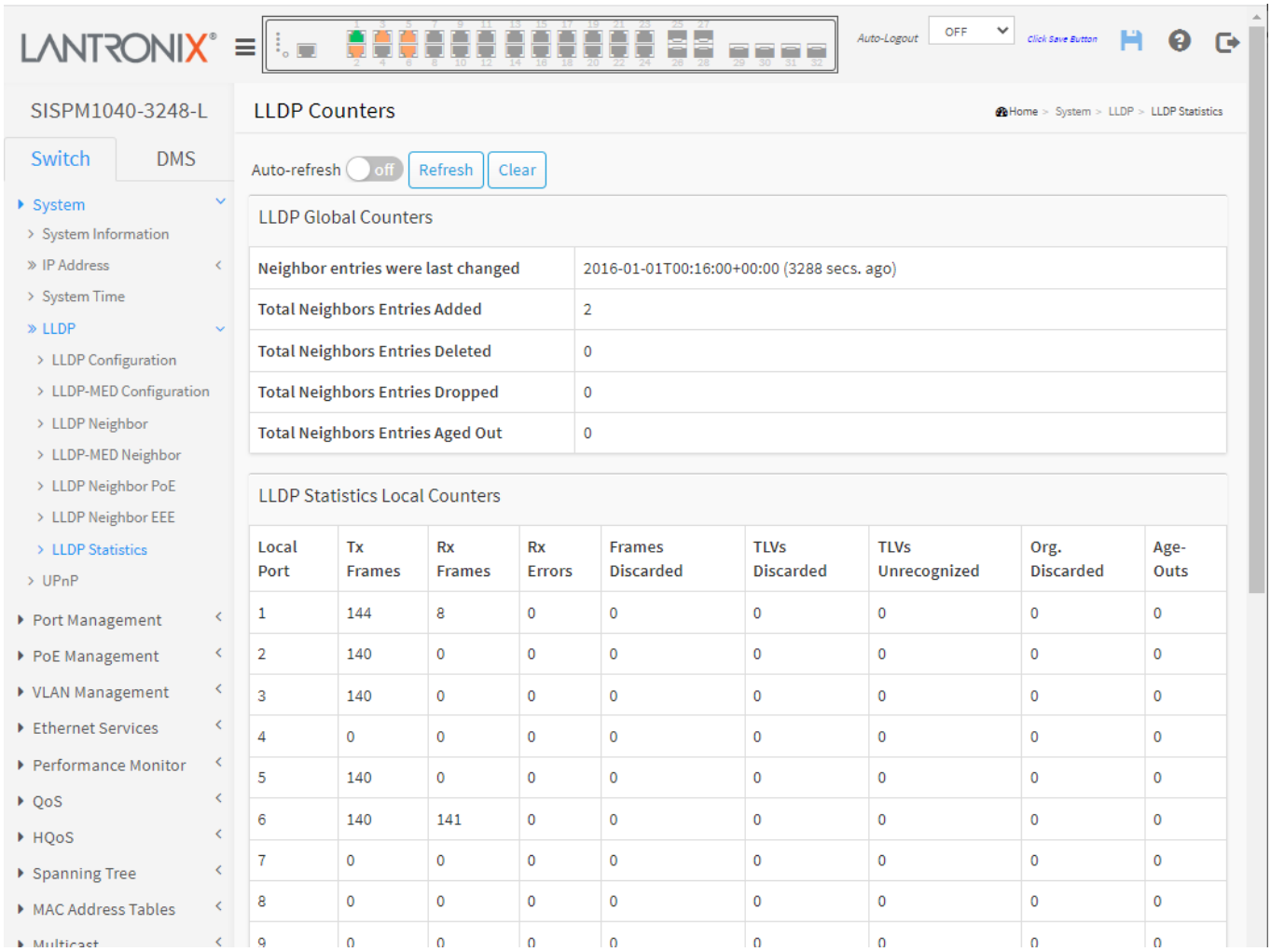


Figure 3-4.7: LLDP Counters and Statistics

Parameter descriptions:

LLDP Global Counters

Neighbor entries were last changed at : 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.

LLDP Statistics Local Counters

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 Value). If a TLV is malformed, it is counted and discarded.

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

Org. Discarded : The number of organizationally received TLVs.

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

Buttons

Auto-refresh : Click to refresh the page automatically every 3 seconds.

Refresh : Click to refresh the page.

Clear : Clears the counters for the selected port.

3-5 UPnP

UPnP (Universal Plug and Play) allows devices to connect seamlessly and simplifies the implementation of networks in the home and in corporate environments. The Universal Plug and Play Forum was formed to standardize discovery and control of networked devices. UPnP has been managed by the Open Connectivity Foundation (OCF) since 2016.

To configure UPnP via the web UI:

1. Click System and UPnP.
2. Select the mode (**on**).
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.

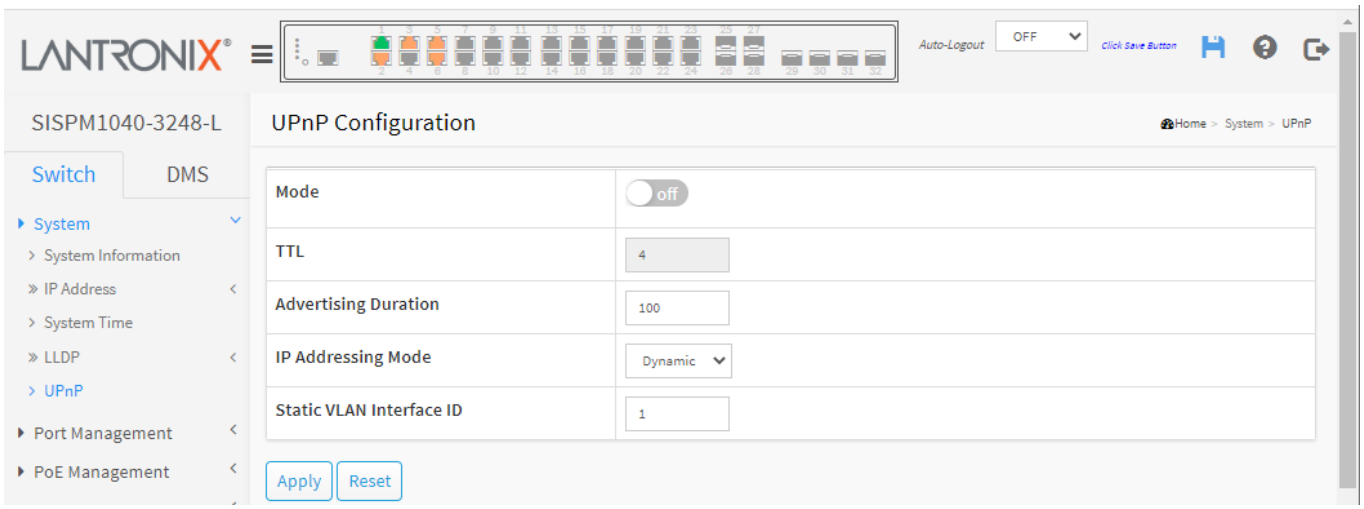


Figure 3-5: UPnP Configuration

Parameter descriptions :

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

on: Enable UPnP mode operation.

off: Disable UPnP mode operation.

When the mode is ***on***, two ACEs are added automatically to trap UPNP related packets to CPU. The ACEs are automatically removed when the mode is ***off***.

TTL : The Time To Live value is used by UPnP to send SSDP advertisement messages. Currently a Read only field.

Advertising Duration : The duration, carried in SSDP packets, is used to inform a control point or control points how often it or they should receive an SSDP advertisement message from this switch. If a control point does not receive any message within the duration, it will think that the switch no longer exists. Due to the unreliable nature of UDP, in the standard it is recommended that such refreshing of advertisements to be done at less than one-half of the advertising duration. In the implementation, the switch sends SSDP messages periodically at the interval one-half of the advertising duration minus 30 seconds. Valid values are 66 to 86400 seconds. The default is 100 seconds.

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

Dynamic: Default selection for UPnP. UPnP module helps users choosing the IP address of the switch device. It finds the first available system IP address.

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

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

Buttons

Apply : Click to save changes.

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

Chapter 4 – Port Management

This section lets you configure the Port parameter details. Here you can enable or disable switch ports, set speed, mode, Flow control, and max frame size for each port, and monitor ports settings and status.

4-1 Port Configuration

This page lets you view and set current port parameters. To configure current Port Configuration parameters in the web UI:

1. Click Port Management and Port Configuration.
2. Specify the Port descriptions as desired.
3. Specify the Speed Mode, Flow Control Mode, and Maximum Frame Size parameters.
4. Click Apply.

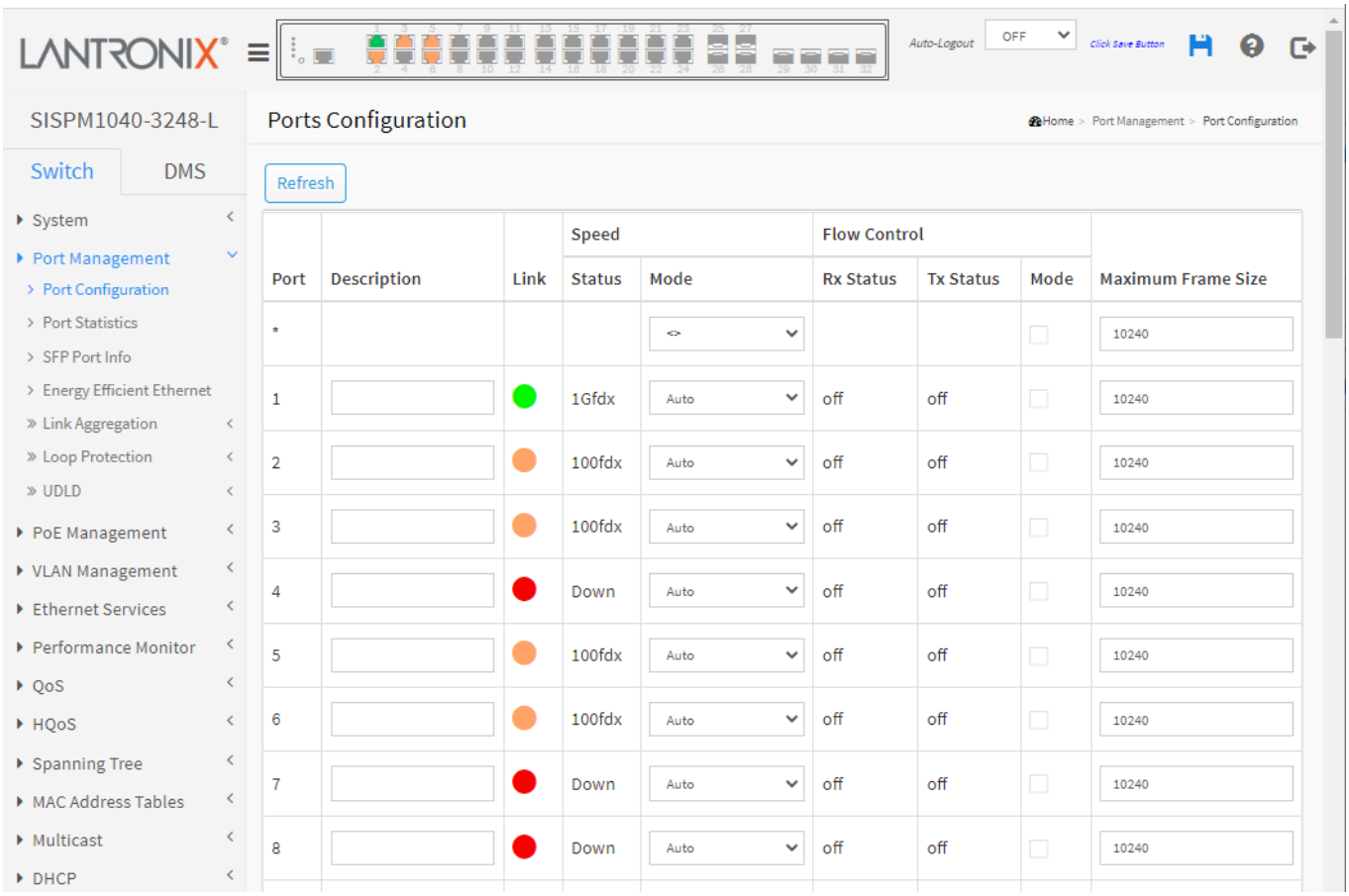


Figure 4-1: Ports Configuration

Parameter descriptions:

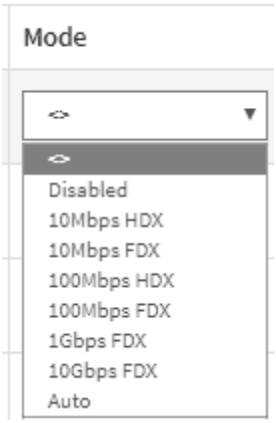
Port : This is the logical port number for this row.

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

Link : The current link state is displayed graphically. Green means the link is up and red means the link is down. Amber indicates the link is up at 10 / 100 Mbps. Green indicates the link is up at 1 Gbps. Blue indicates the link is up at 10 Gbps. Red indicates the link is down.

Current Link Speed Status: Provides the current link speed (e.g., *1Gfdx*, *100fdx*) or status (e.g., *Down (ACL)*) of the port.

Current Link Speed Mode: Selects any available link speed for the given switch port. Only speeds supported by the specific port are shown. Possible speeds are:



Disabled - Disables the switch port operation.

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

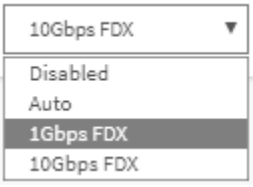
10Mbps HDX - Forces the copper port in 10Mbps half duplex mode.

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

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

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

1Gbps FDX - Forces the port in 1Gbps full duplex Flow Control : When Auto Speed is selected on a port, this section indicates the flow control capability that is advertised to the link partner. When a fixed-speed setting is selected, that is what is used. The Current Rx column indicates whether pause frames on the port are obeyed, and the Current Tx column indicates whether pause frames on the port are transmitted. The Rx and Tx settings are determined by the result of the last Auto-Negotiation. Check the configured column to use flow control. This setting is related to the setting for Configured Link Speed.



Flow Control: When Auto Speed is selected on a port, this section indicates the flow control capability that is advertised to the link partner.
When a fixed-speed setting is selected, that is what is used. The Current Rx column indicates whether pause frames on the port are obeyed, and the Current Tx column indicates whether pause frames on the port are transmitted. The Rx and Tx settings are determined by the result of the last Auto Negotiation.
Check the configured column to use flow control. This setting is related to the setting for Configured Link Speed.
NOTE: The 100FX standard doesn't support Auto Negotiation, so when in 100FX mode the flow control capabilities will always be shown as "disabled".

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

Buttons

Refresh : Click to manually refresh the page immediately.

Apply : Click to save changes.

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

4-2 Port Statistics

This page displays the Port statistics information and an overview of general traffic statistics for all switch ports.

To display the Port Statistics in the web UI:

1. Click Port Management and Port Statistics.
2. To automatically refresh the page every 3 seconds click the Auto-refresh button.
3. Click Refresh to refresh the port statistics immediately or clear all information when you click Clear.
4. To see the detail of port statistic click that port in the Port column.

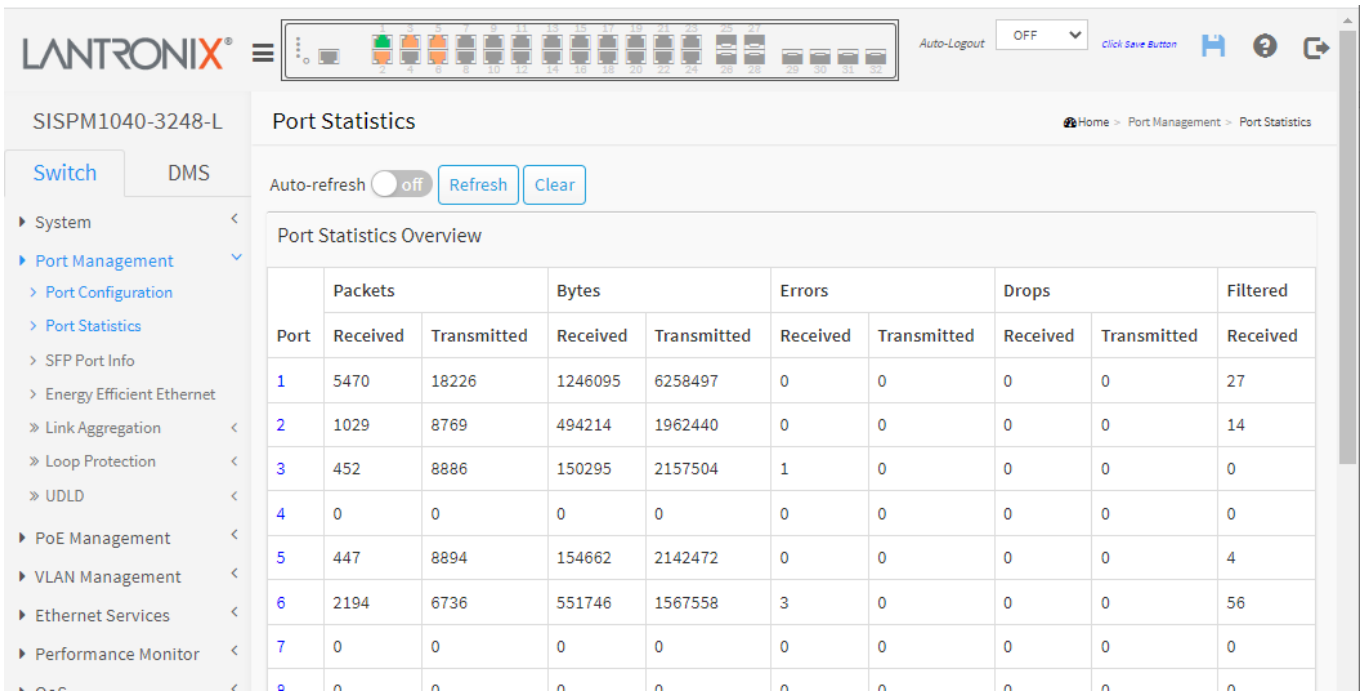


Figure 4-2: Port Statistics Overview

Parameter descriptions:

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

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

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

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

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

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

Buttons

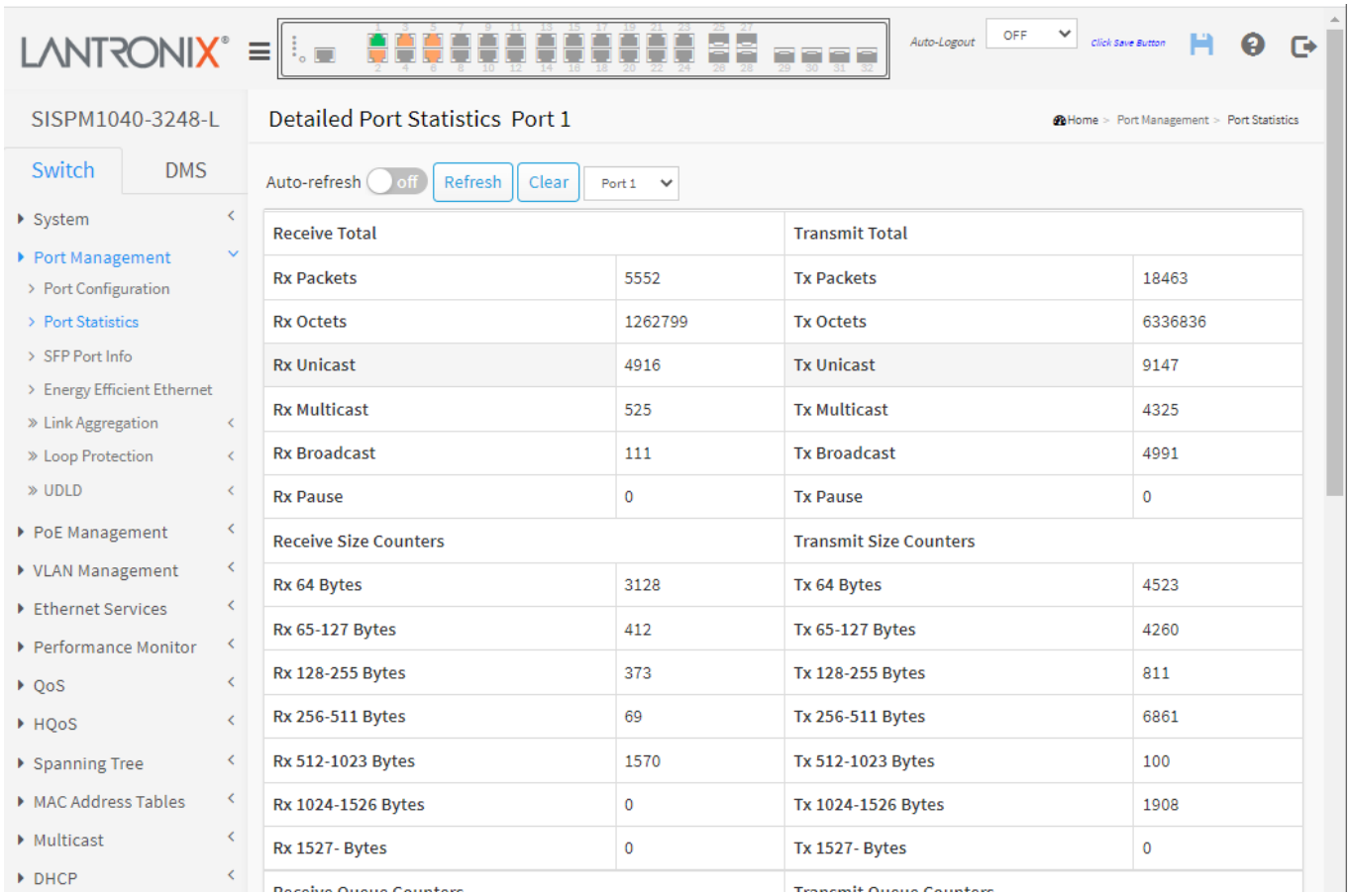
Auto-refresh : Click to refresh the page automatically every 3 seconds.

Refresh : Click to manually refresh the page immediately.

Clear : Clears the counters for all ports.

4-3 Detailed Port Statistics

To view the detail of port statistics, click a linked port number. The displayed counters are the totals for receive and transmit, the size counters for receive and transmit, and the error counters for receive and transmit.



Receive Total		Transmit Total	
Rx Packets	5552	Tx Packets	18463
Rx Octets	1262799	Tx Octets	6336836
Rx Unicast	4916	Tx Unicast	9147
Rx Multicast	525	Tx Multicast	4325
Rx Broadcast	111	Tx Broadcast	4991
Rx Pause	0	Tx Pause	0
Receive Size Counters		Transmit Size Counters	
Rx 64 Bytes	3128	Tx 64 Bytes	4523
Rx 65-127 Bytes	412	Tx 65-127 Bytes	4260
Rx 128-255 Bytes	373	Tx 128-255 Bytes	811
Rx 256-511 Bytes	69	Tx 256-511 Bytes	6861
Rx 512-1023 Bytes	1570	Tx 512-1023 Bytes	100
Rx 1024-1526 Bytes	0	Tx 1024-1526 Bytes	1908
Rx 1527- Bytes	0	Tx 1527- Bytes	0

Figure 4-2: Detailed Port Statistics

Parameter descriptions :

Port select box: At the dropdown, select the port to display the port statistics (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.

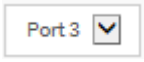
Tx Oversize : The number of frames dropped due to frame oversize.

Buttons

Auto-refresh : Click to refresh the page automatically every 3 seconds.

Refresh : Click to refresh the page.

Clear : Clears the counters for the selected port.



: The port select box lets you select which port's statistics to display.

4-3 SFP Port Info

This page displays detailed SFP module information. The information includes Connector type, Fiber type, wavelength, bit rate, Vendor OUI, etc. To display SFP information in the web UI:

1. Click Port Management and SFP Port Info.
2. Select the desired port at the port select box.
3. View the displayed SFP Information.

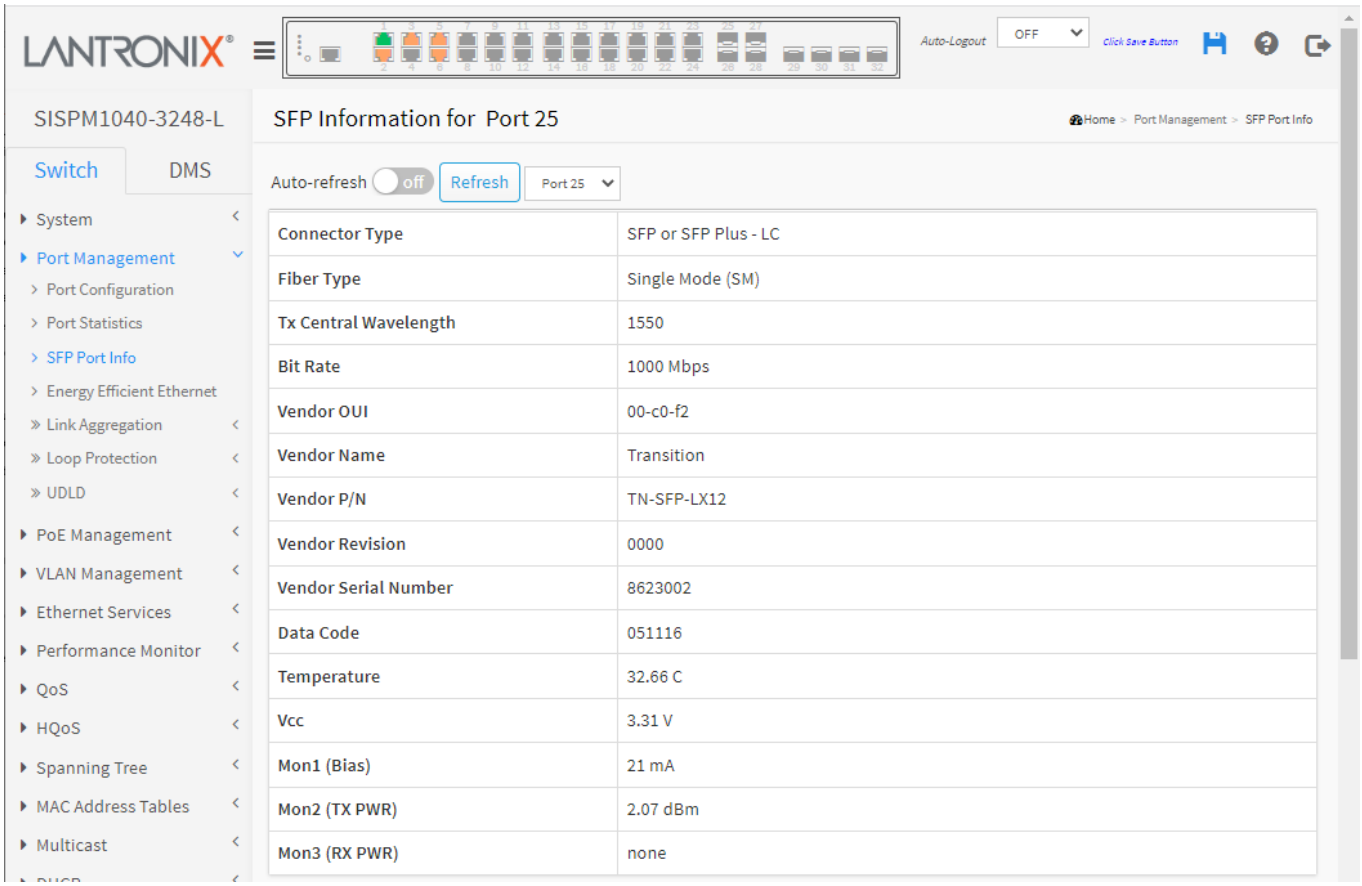


Figure 4-3: SFP Port Information

Parameter descriptions:

Connector Type: Displays the connector type (e.g., UTP, SC, ST, LC, Reserved – LC, SFP or SFP Plus – LC, etc.).

Fiber Type: Displays the fiber mode, for instance, Multi-Mode, Single-Mode.

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

Bit Rate: Displays the nominal bit rate of the transceiver (e.g., 1000 Mbps or none).

Vendor OUI: Displays the Manufacturer's OUI (Organizationally Unique Identifier) code assigned by IEEE.

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

Vendor P/N: Displays the product name of the naming by module manufacturer.

Vendor Revision : Displays the module revision (e.g., 2.0).

Vendor Serial Number : Shows the serial number assigned by the manufacturer (e.g., TWDW34Z001).

Date Code: Shows the date this SFP module was made (e.g., 160730).

Temperature: Shows the current temperature of the SFP module.

Vcc: Shows the working DC voltage of SFP module.

Mon1(Bias) mA: Shows the Bias current of SFP module (e.g., 82 mA).

Mon2(TX PWR): Shows the transmit power of SFP module (e.g., 1.86 dBm).

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

Buttons

Auto-refresh : Click to refresh the page automatically every 3 seconds.

Refresh : Click to refresh the page.

: The port select box lets you select which port's information to display.

4-4 Energy Efficient Ethernet

This page lets you view and configure the current EEE port settings. EEE is a power saving option that reduces the power usage when there is very low traffic utilization (or no traffic).

EEE (Energy Efficient Ethernet) is defined in IEEE 802.3az. 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 µs 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.

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 by the 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.

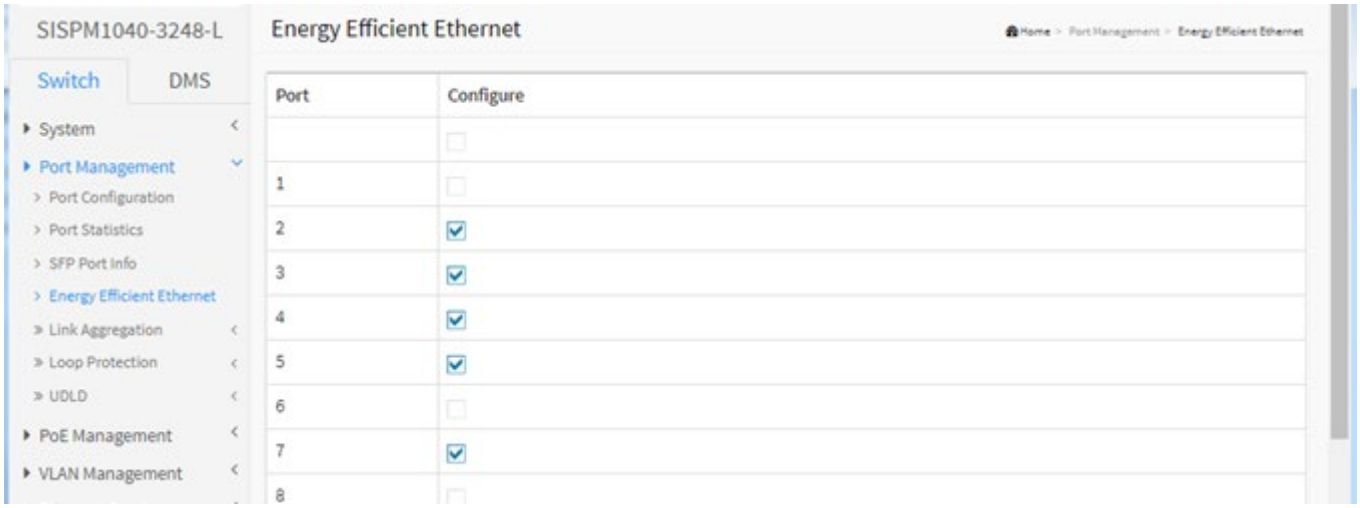


Figure 4-4: Energy Efficient Ethernet Configuration

Parameter descriptions:

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

Configure : Controls whether EEE is enabled for this switch port. The default is unchecked (disabled).

Buttons

Apply : Click to save changes.

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

» Link Aggregation
› Static Configuration
› Aggregation Status
› LACP Configuration
› System Status
› Internal Status
› Neighbor Status
› Port Status

4-5 Link Aggregation

This section lets you view and configure various link aggregation parameters. Aggregation involves using multiple ports in parallel to increase the link speed beyond the limits of a port and to increase the redundancy for higher availability. (AKA Port Aggregation.)

4-5.1 Static Configuration

This page lets you configure Aggregation hash mode and the Aggregation group. **Note** that LACP and Static aggregation cannot both be enabled on the same ports at the same time.

Web Interface

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

1. Click Port Management, Link Aggregation and Static Configuration.
2. Enable or disable the Hash Code Contributors.
3. Select the Port Members in one or more Aggregation Group IDs.
4. Click Apply to save the settings.
5. To cancel the settings click the Reset button to revert to previously saved values.

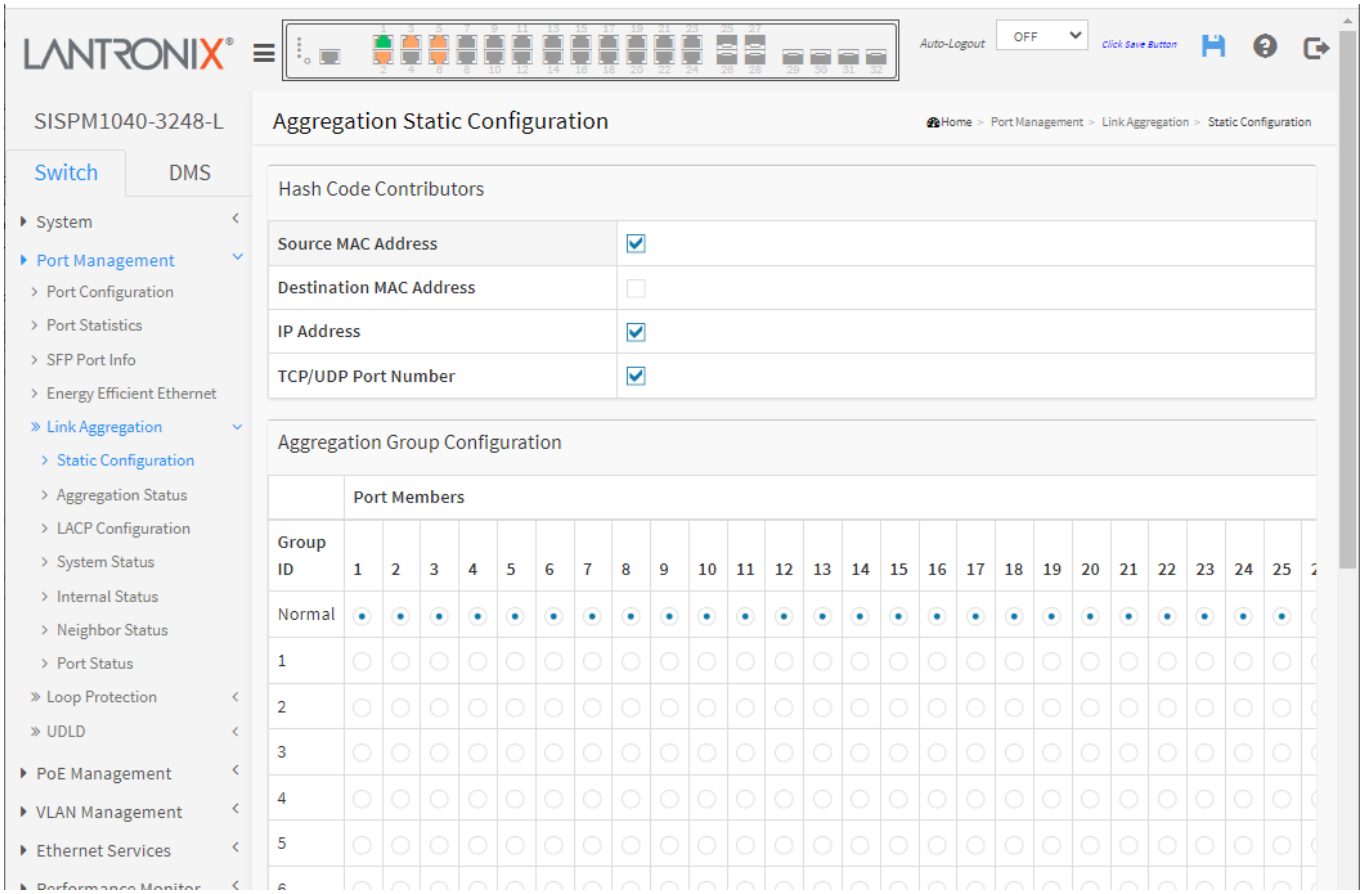


Figure 4-5.1: Aggregation Static Configuration

Parameter descriptions :

Hash Code Contributors

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

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

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

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

Aggregation Group Configuration

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

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

Buttons

Apply : Click to save changes.

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

Message : *LACP and Static aggregation can not both be enabled on the same ports*

4-5.2 Aggregation Status

This page displays the status of ports in Aggregation groups. To view Aggregation status in the web UI:

1. Click Port Management > Link Aggregation > Aggregation Status.
2. View the status parameters.
3. Use the Auto-refresh and refresh buttons as needed.

Figure 4-5.2: Aggregation Status

Parameter descriptions:

Aggregation Group Status

Aggr ID: The Aggregation ID associated with this aggregation instance.

Name: Name of the Aggregation group ID (e.g., LLAG1).

Type: Type of the Aggregation group (STATIC or LACP).

Speed: Speed of the Aggregation group (e.g., 100M or 1G bps or Undefined).

Configured ports: Configured member ports of the Aggregation group (e.g., GigabitEthernet 1/1-2).

Aggregated ports: Aggregated member ports of the Aggregation group (e.g., GigabitEthernet 1/5).

Aggregated Bandwidth: Aggregated Bandwidth of the Aggregation group (e.g., 2G, none, or 200M) in Bps.

Buttons

Auto-refresh: Automatic refresh occurs every 3 seconds.

Refresh: Click to refresh the page immediately.

4-5.3 LACP Configuration

This page lets you view and configure the current LACP port parameters. Note that LACP and Static aggregation cannot both be enabled on the same ports at the same time.

To configure LACP Port parameters in the web UI:

1. Click Port Management, Link Aggregation and LACP Configuration.
2. Enable or disable LACP on the desired switch ports.
3. Select the Key parameter (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. It will revert to previously saved values.

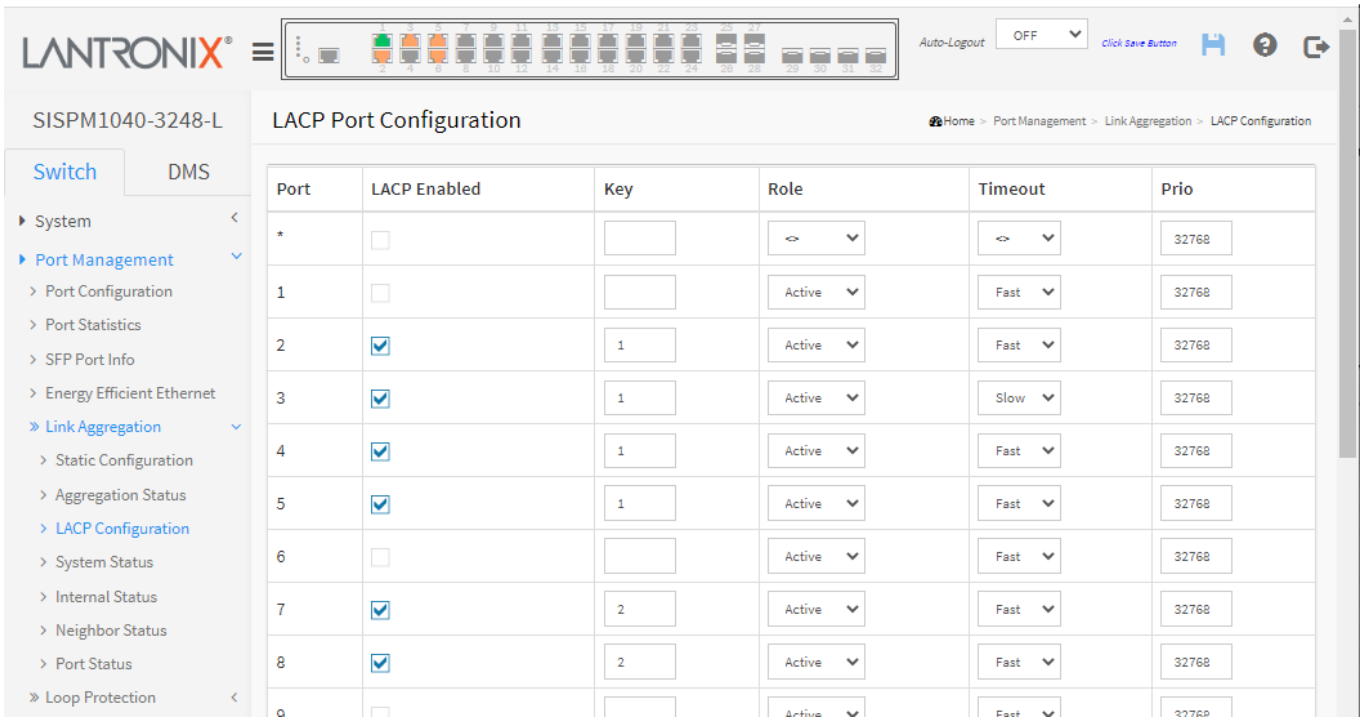


Figure 4-5.2: LACP Port Configuration

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

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

Prio : The 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 number means greater priority. The default is 32768.

Buttons

Apply : Click to save changes.

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

Message :

LACP and Static aggregation can not both be enabled on the same ports
LACP Error Invalid group id

4-5.4 System Status

This page ~~lets you set LACP function and~~ provides a status overview of all LACP instances

To display the LACP System status in the web UI:

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

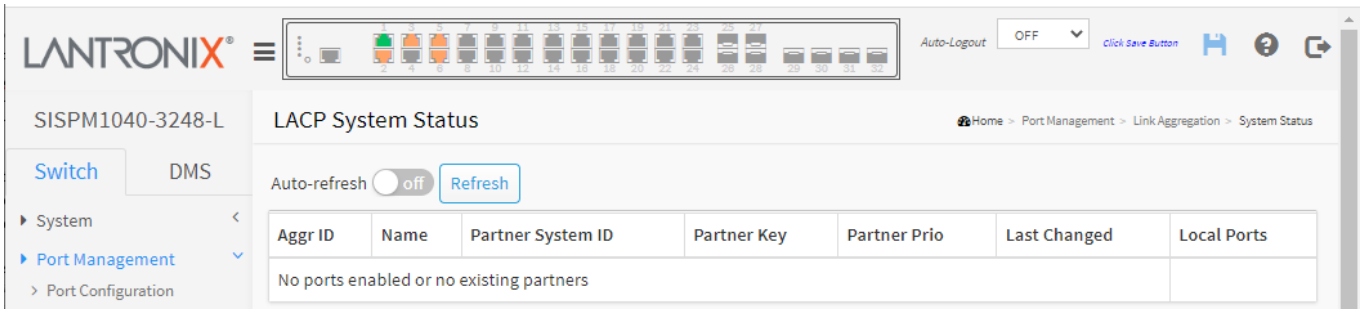


Figure 4-5.3: LACP System Status

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 : Click to automatically refresh the page every 3 seconds.

Refresh : Click to manually refresh the page immediately.

4-5.5 Internal Status

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

To display the LACP Internal Port status in the web UI:

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

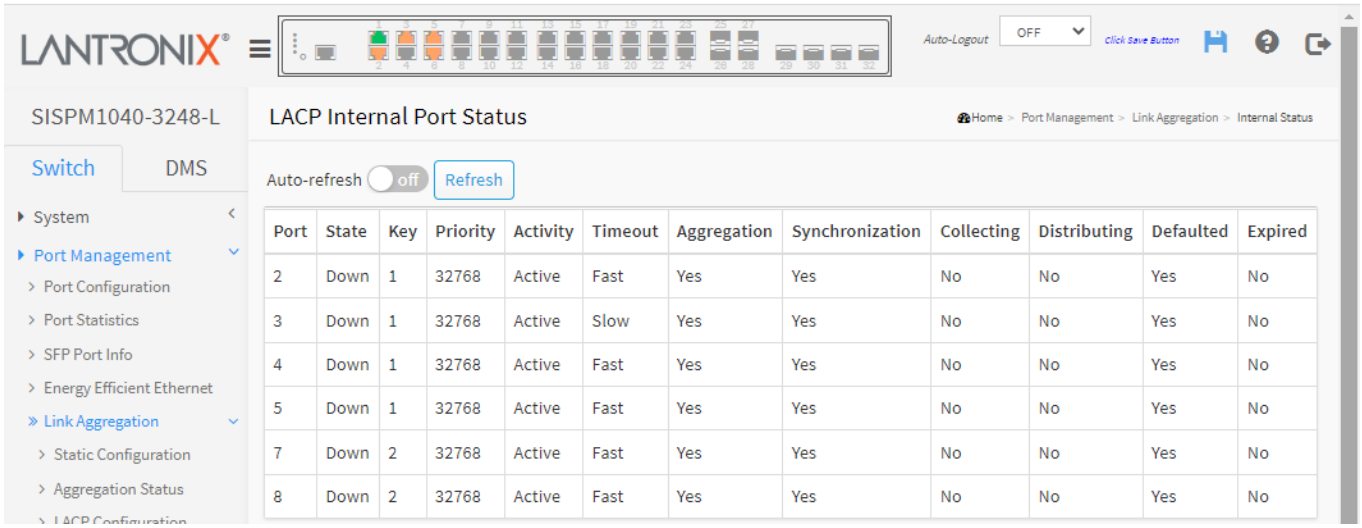


Figure 4-5.4: LACP Internal Port Status

Parameter descriptions:

Port : The switch port number.

State : The current port state:

Down: The port is not active.

Active: The port is in active state.

Standby: The port is in standby state.

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

Priority : The priority assigned to this aggregation group.

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

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

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

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

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

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

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

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

Buttons

Auto-refresh : Click to refresh the page automatically every 3 seconds.

Refresh : Click to refresh the page.

4-5.6 Neighbor Status

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

To display LACP Neighbor Port status in the web UI:

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

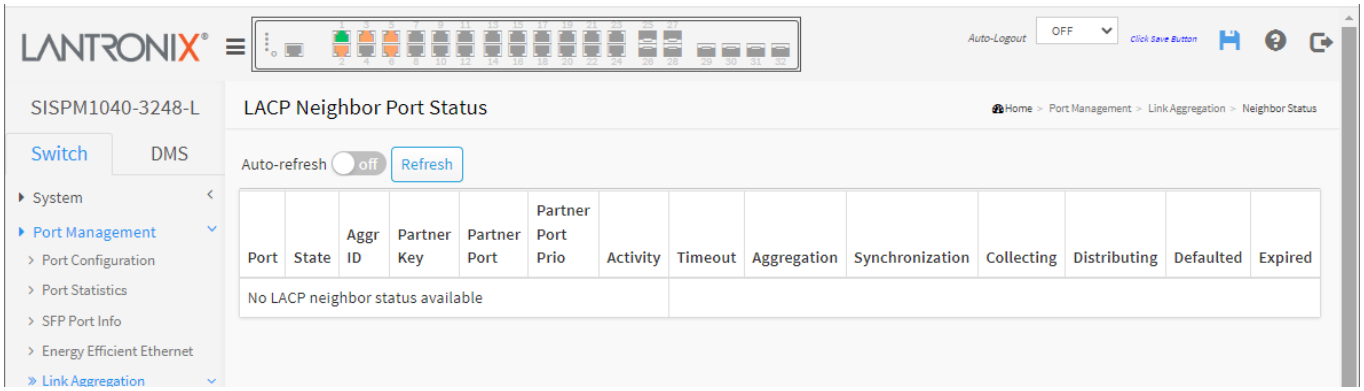


Figure 4-5.5: LACP Neighbor Port Status

Parameter descriptions:

Aggr ID : The aggregation group ID which the port is assigned to.

Port : The switch port number.

State : The current port state:

Down: The port is not active.

Active: The port is in active state.

Standby: The port is in standby state.

Partner Key : The key assigned to this port by the partner.

Partner Port : The partner port number associated with this link.

Partner Port Priority : The priority assigned to this partner port .

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

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

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

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

Collecting : Shows if collection of incoming frames on this link is enabled.

Distributing : Shows if distribution of outgoing frames on this link is enabled.

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

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

Buttons

Auto-refresh : Click to refresh the page automatically every 3 seconds.

Refresh : Click to refresh the page.

4-5.7 Port Status

This page lets you set LACP functions on the switch and provides a Port Status overview of all LACP instances.

To display the LACP Port status in the web UI:

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

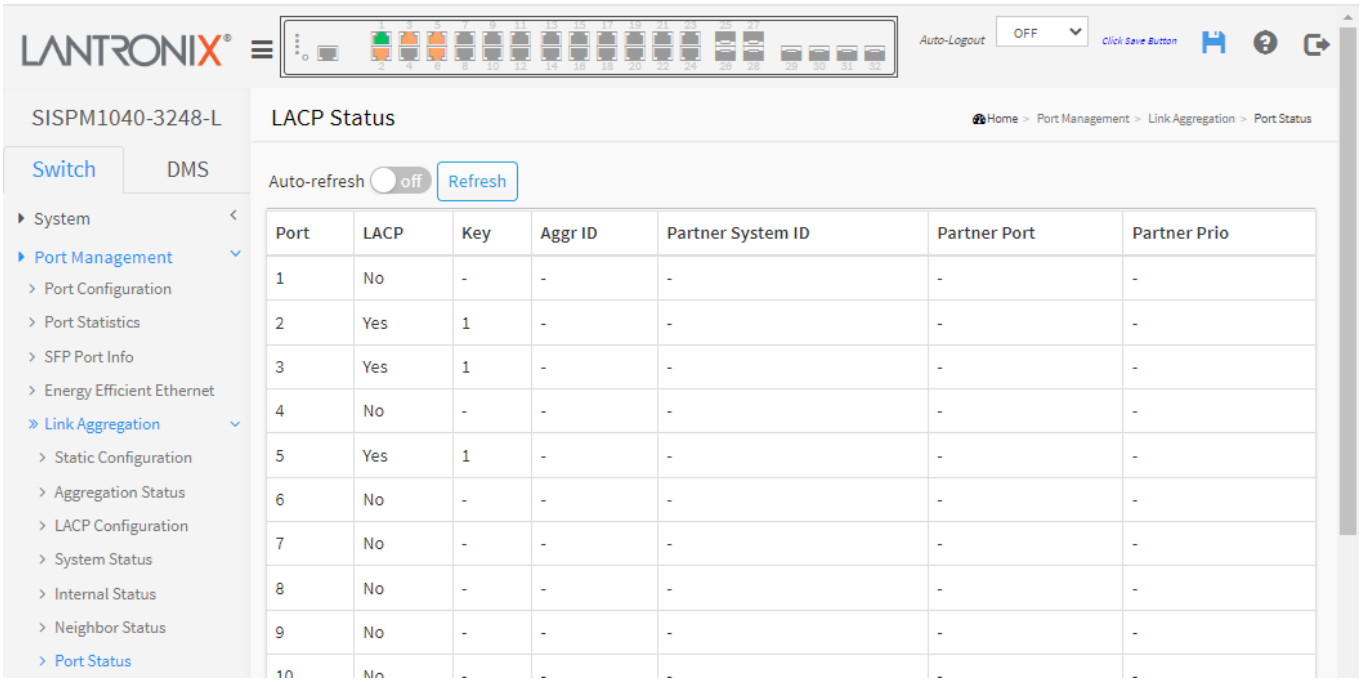


Figure 4-5.6: LACP Status

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 its 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 : Click to refresh the page automatically every 3 seconds.

Refresh : Click to manually refresh the page immediately.

4-6 Loop Protection

4-6.1 Configuration

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

To configure Loop Protection parameters in the web UI:

1. Click Port Management, Loop Protection, and Configuration.
2. Enable or disable port loop Protection for each port.
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.

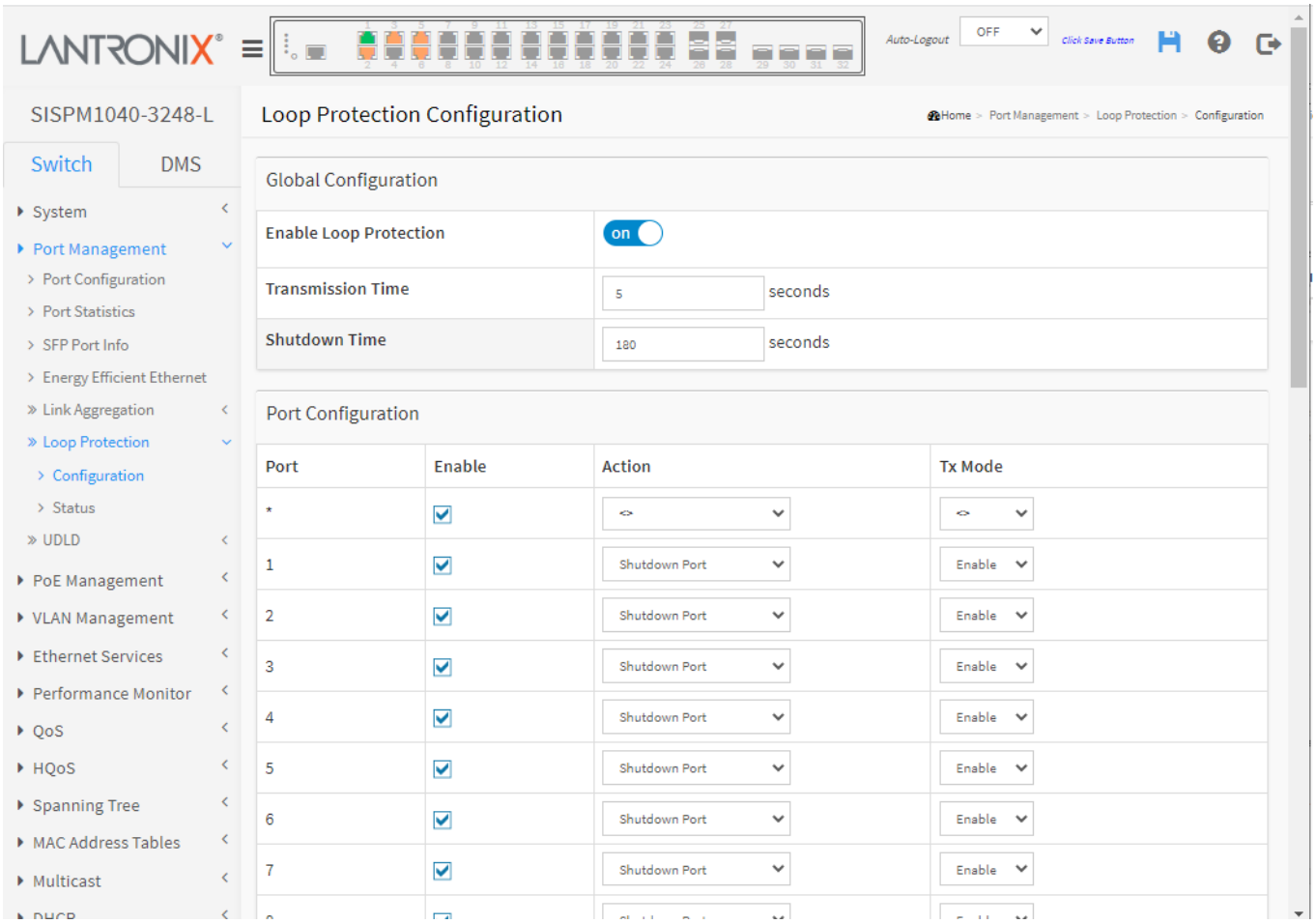


Figure 4-6.1: Loop Protection Configuration

Parameter descriptions:

Global Configuration

Enable Loop Protection : Controls whether loop protections is enabled (as a whole).

Transmission Time : The interval between each loop protection PDU sent on each port. Valid values are 1 - 10 seconds.

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

Port Configuration

Port : The switch port number of the port.

Enable : Controls whether loop protection is enabled on this switch port

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

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

Buttons

Apply : Click to save changes.

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

4-6.2 Status

This page displays loop protection port status for all switch ports. To display Loop Protection status in the web UI:

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

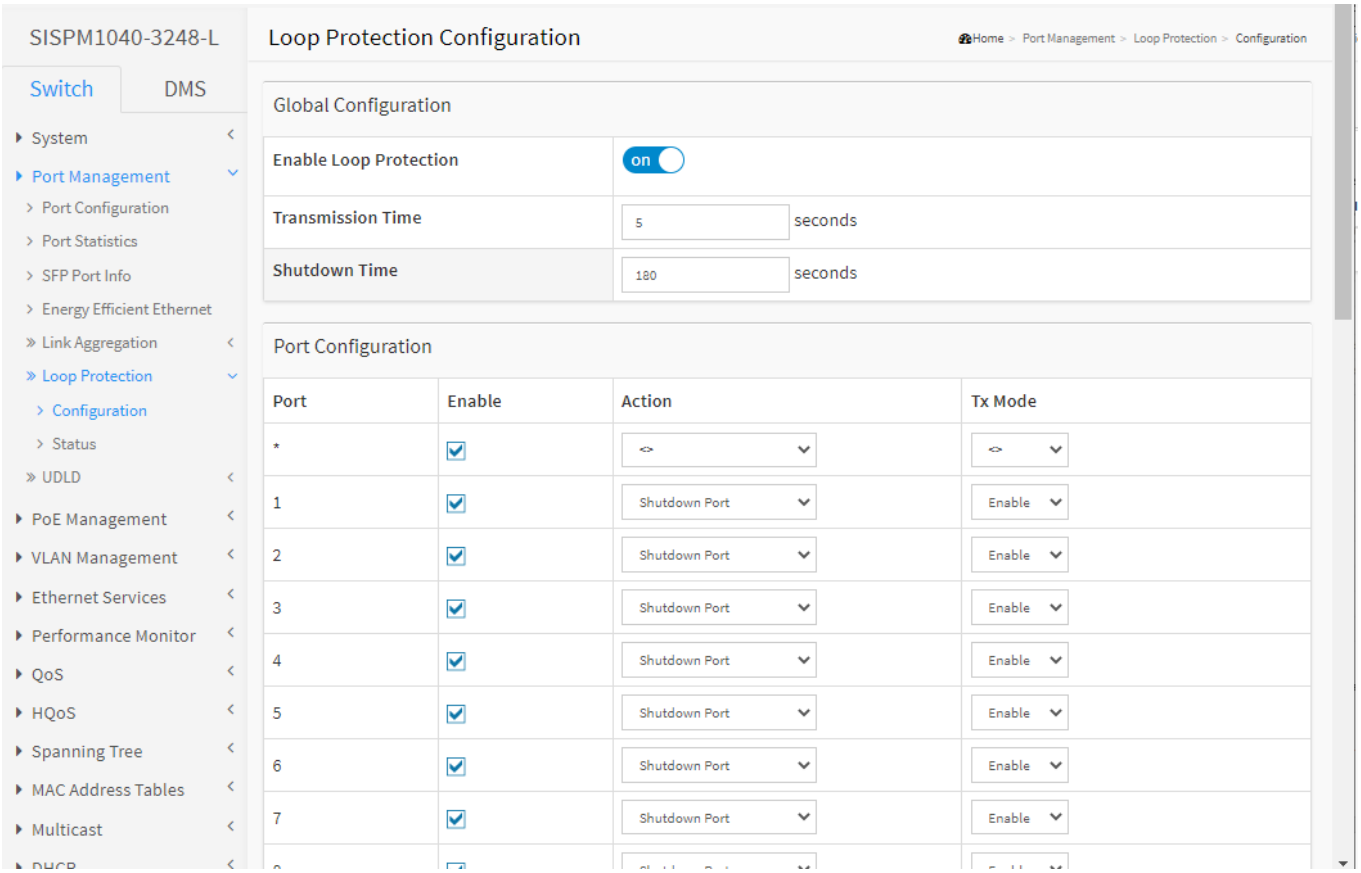


Figure 4-6.2: Loop Protection Status

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 that the last loop event was detected.

Buttons

Auto-refresh : Click to refresh the page automatically every 3 seconds.

Refresh : Click to manually refresh the page immediately.

4-7 UDLD

4-7.1 UDLD Configuration

This page lets you view and configure the current UDLD parameters. The UDLD (Uni Directional Link Detection) protocol monitors the physical configuration of the links between devices and ports that support UDLD. It detects the existence of unidirectional links. Its function is to provide mechanisms useful for detecting one-way connections before they create a loop or other protocol malfunction. IETF RFC 5171 specifies a way at the data link layer to detect Uni directional link.

To configure UDLD parameters in the web UI:

1. Click Port Management, UDLD and UDLD Configuration.
2. Enable or disable the port UDLD.
3. Specify the Message Interval.
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.

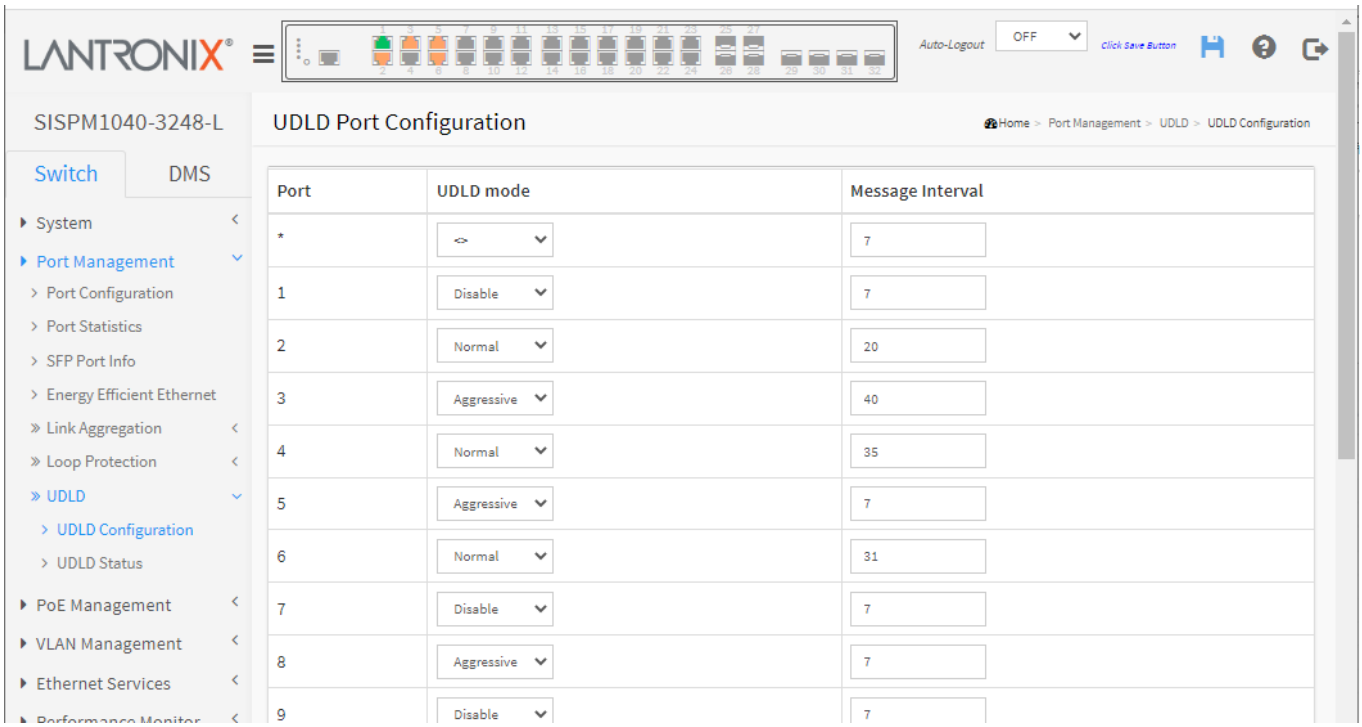


Figure 4-7.1: UDLD Port Configuration

Parameter descriptions :

Port : Port number of the switch.

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

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

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

Aggressive: In aggressive mode, unidirectional detected ports will get shutdown. To bring back the ports up, need to disable 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 this default message interval is the only value supported, due to lack of detailed information in RFC 5171).

Buttons

Apply : Click to save changes.

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

4-7.2 UDLD Status

This page displays Unidirectional Link Detection status of the ports. To display UDLD status in the web UI:

1. Click Port Management, UDLD, and UDLD Status.
2. Select port that you want to display the UDLD Status.
3. To automatically refresh the page every 3 seconds check “Auto refresh”.
4. Click “Refresh” to refresh the Loop Protection Status.

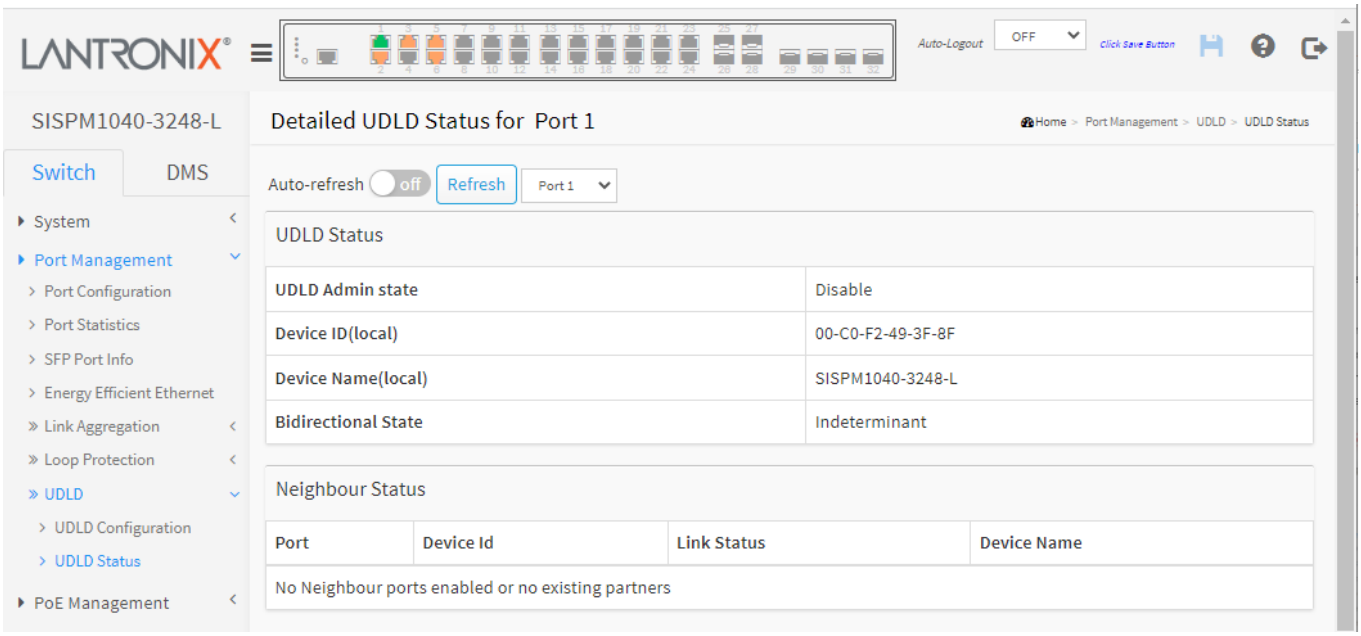


Figure 4-7.2: UDLD Status

Parameter descriptions :

UDLD Status

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

Device ID(local): The ID of Device.

Device Name(local): The 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 : Name of the Neighbor Device.

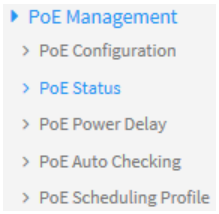
Buttons

Auto-refresh : Click to refresh the page automatically every 3 seconds.

Refresh : Click to manually refresh the page immediately.

Port select box : Select port that you want to display the UDLD Detailed Statistics.

Chapter 5 - PoE Management



PoE (Power over Ethernet) is used to transmit electrical power to remote devices over standard Ethernet cable. It can be used for powering IP cameras, IP phones, wireless LAN access points, media converters, and other equipment, where it would be difficult or expensive to connect the equipment to main power supply.

5-1 PoE Configuration

This page lets you view and configure the current PoE port settings. To configure PoE in the web UI:

1. Click PoE Management and PoE Configuration.
2. Specify the 'Reserved Power determined by' and the 'Power Management Mode' parameters.
3. Specify the PoE Power Supply Configuration parameters and the PoE Port Configuration parameters.
4. Click Apply to save the configuration.

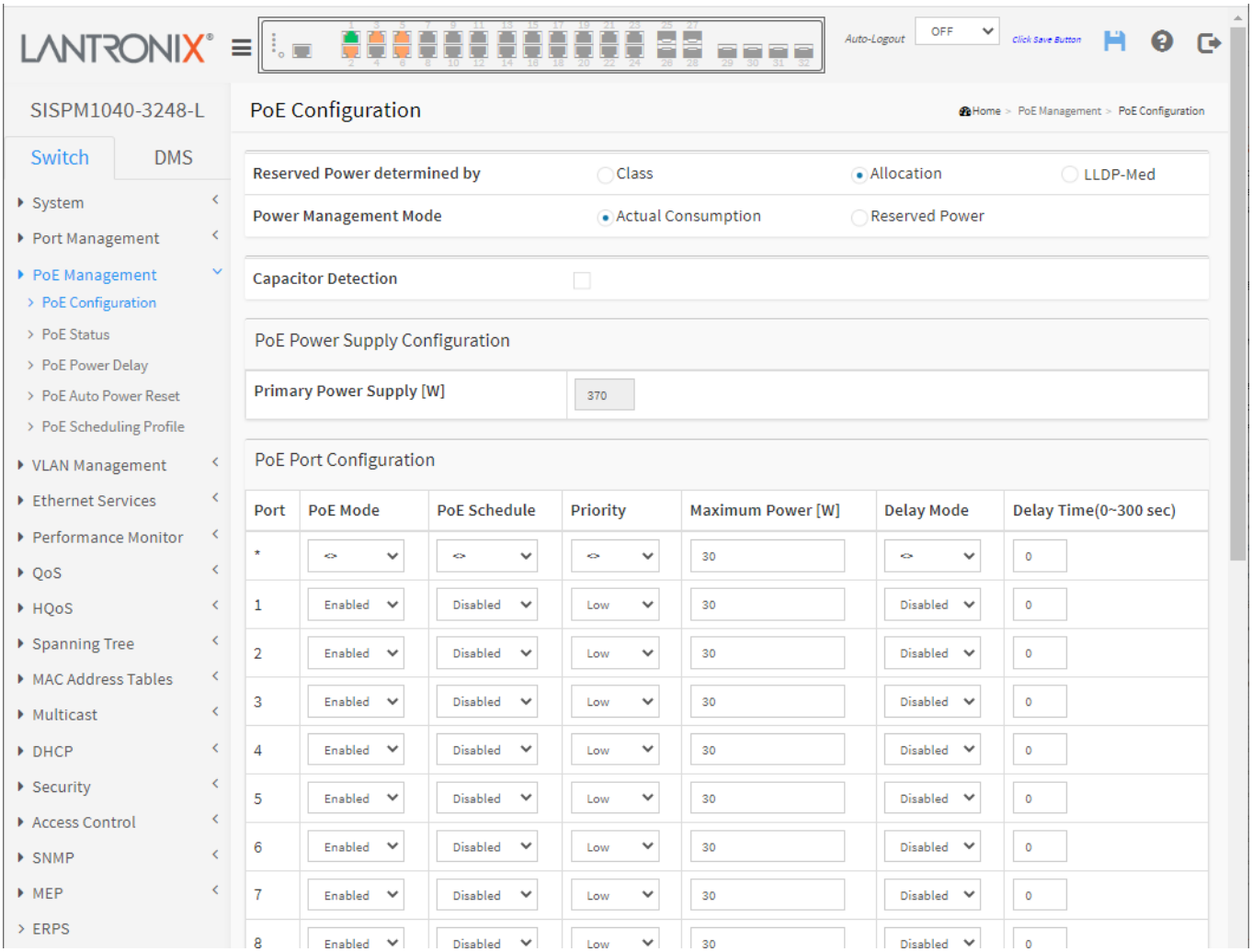


Figure 5-1: PoE Configuration

Parameter Descriptions:

Reserved Power determined by : There are three modes for configuring how the ports/PDs may reserve power.

Class: In this mode each port automatically determines how much power to reserve according to the class the connected PD belongs to and reserves the power accordingly. Four different port classes exist and one for 4, 7, 15.4 or 30 Watts. In this mode the Maximum Power fields have no effect.

Allocation: In this mode you can allocate the amount of power that each port may reserve (default mode). The allocated/reserved power for each port/PD is specified in the Maximum Power fields.

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

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

Power Management Mode : There are two modes for configuring when to shut down the ports:

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

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

Capacitor Detection : Check the box to enable Capacitor Detection mode for legacy PoE device support.

PoE Power Supply Configuration

Primary Power Supply [W]: For being able to determine the amount of power the PD may use, it must be defined what amount of power a power source can deliver. Valid values are 1 to 370 Watts.

PoE Port Configuration

Port : This is the logical port number for this row. Ports that are not PoE-capable are grayed out and thus impossible to configure PoE for.

PoE Mode: Select the PoE operating mode for the port.

Disabled: PoE disabled for the port.

Enabled : Enables PoE IEEE 802.3at (Class 4 PDs limited to 30W).

PoE Schedule : Scheduled by selecting PoE Scheduling Profile. Select Disabled or Profile 1 -16.

Priority : The Priority represents the ports priority. The three levels of power priority are **Low**, **High**, and **Critical**. The priority is used when the remote devices require more power than the power supply can deliver. In this case the port with the lowest priority will be turned off starting from the port with the highest port number.

Maximum Power : The Maximum Power value contains a numerical value that indicates the maximum power in watts that can be delivered to a remote device. The maximum allowed value is 30 W.

Delay Mode : Turn on / off the power delay function.

Enabled: Enable POE Power Delay.

Disabled: Disable POE Power Delay.

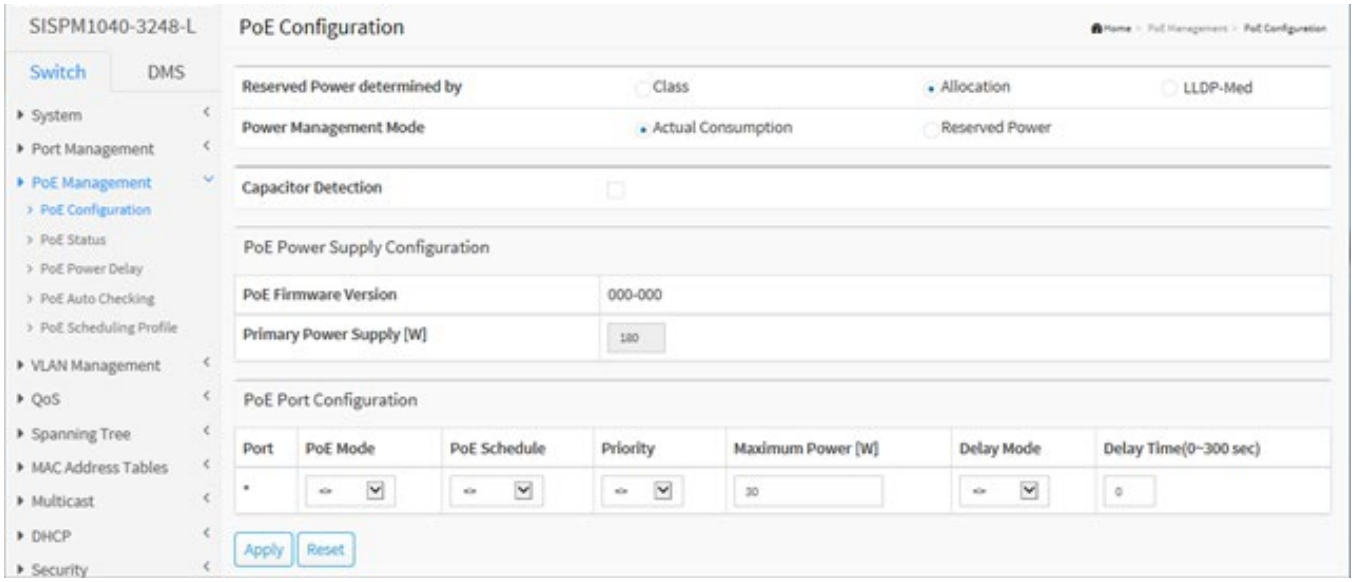
Delay Time(0~300sec) : When rebooting, the PoE port will start to provide power to the PD when it out of delay time. The default is 0 seconds; the valid range is 0-300 seconds.

Buttons

Apply : Click to save changes.

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

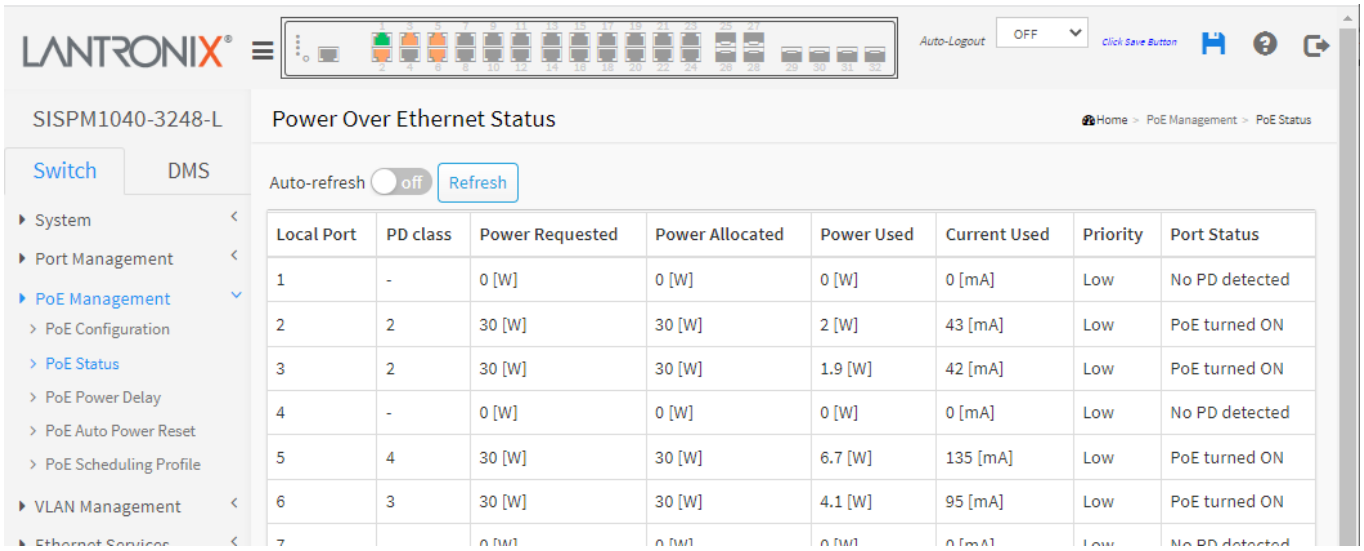
Note: if the power supply is insufficient for PoE operation, then the PoE Port Configuration section will not show any ports:



See the Install Guide for power supply requirements, options, and related PoE information.

5-2 PoE Management > PoE Status

This page displays the current status of all PoE ports.



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

PD Class : Each PD is classified according to a class that defines the maximum power the PD will use. Five PD Classes are defined:

Class 0: Max. power 15.4 W
Class 1: Max. power 4.0 W
Class 2: Max. power 7.0 W
Class 3: Max. power 15.4 W
Class 4: Max. power 30.0 W

Power Requested : Shows the requested amount of power the PD wants to be reserved.

Power Allocated : Shows the amount of power the switch has allocated for the PD.

Power Used : Shows how much power the PD currently is using.

Current Used : Shows how much current the PD currently is using.

Priority : Shows the port's priority configured by the user (Low, High, or Critical).

Port Status : Shows the port's status. Generally, the status can be *PoE not available*, *No PoE chip found*, or *PoE not supported* for the port. The specific status that can be reported includes:

PoE turned ON : A PD was detected for the port.
PoE turned OFF - PoE disabled : PoE is disabled by user.
PoE turned OFF - Power budget exceeded : The total requested or used power by the PDs exceeds the maximum power the Power Supply can deliver, and port(s) with the lowest priority is/are powered down.
No PD detected : No PD detected for the port.
PoE turned OFF - PD overload : The PD has requested or used more power than the port can deliver and is powered down.
PoE turned OFF : PD is off.
Invalid PD : PD detected but is not working correctly.

The bottom of the table shows totals for Power Requested, Power Allocated, Power Used, and Current Used.

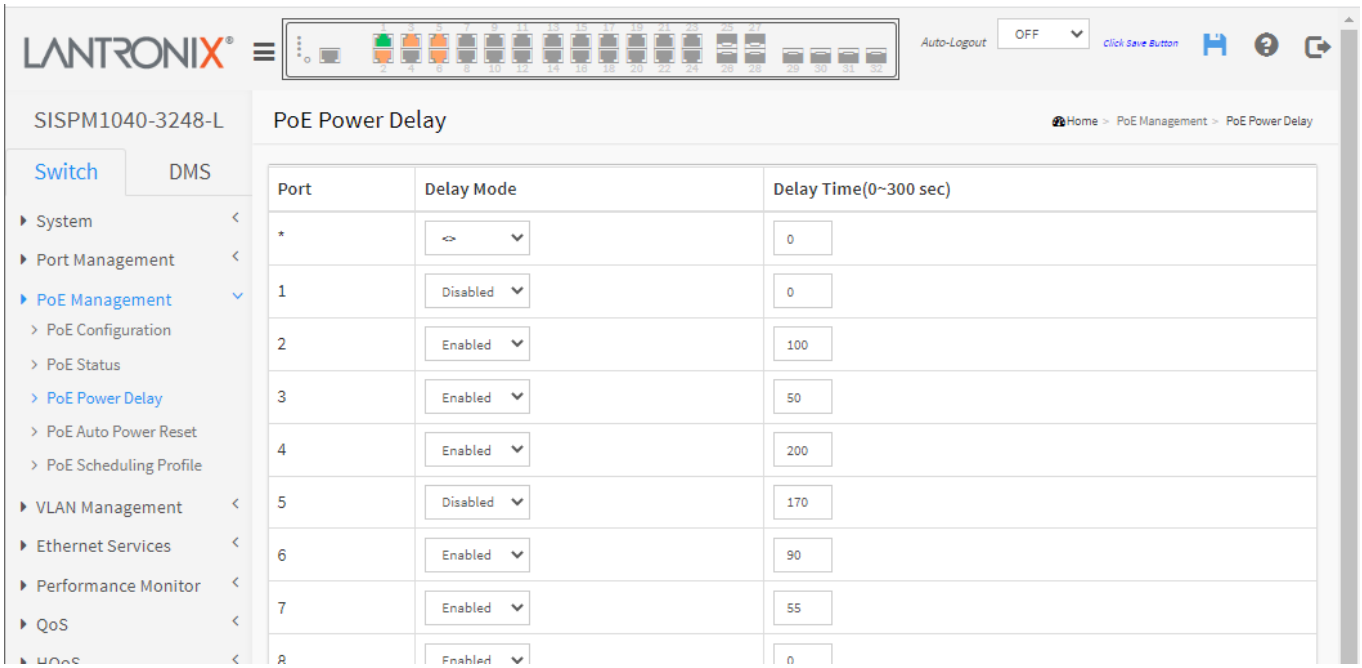
Buttons

Auto-refresh: Click to refresh the page automatically every 3 seconds.

Refresh : Click to manually refresh the page immediately.

5-3 PoE Management > PoE Power Delay

This page lets you set the delay time of power provided after the device is rebooted.



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

Delay Mode : Turn on / off the power delay function.

Enabled: Enable POE Power Delay.

Disabled: Disable POE Power Delay (default).

Delay Time(0~300sec) : When rebooting, the PoE port will start to provide power to the PD when it runs out of delay time. The default is 0 seconds; the valid range is 0-300 seconds.

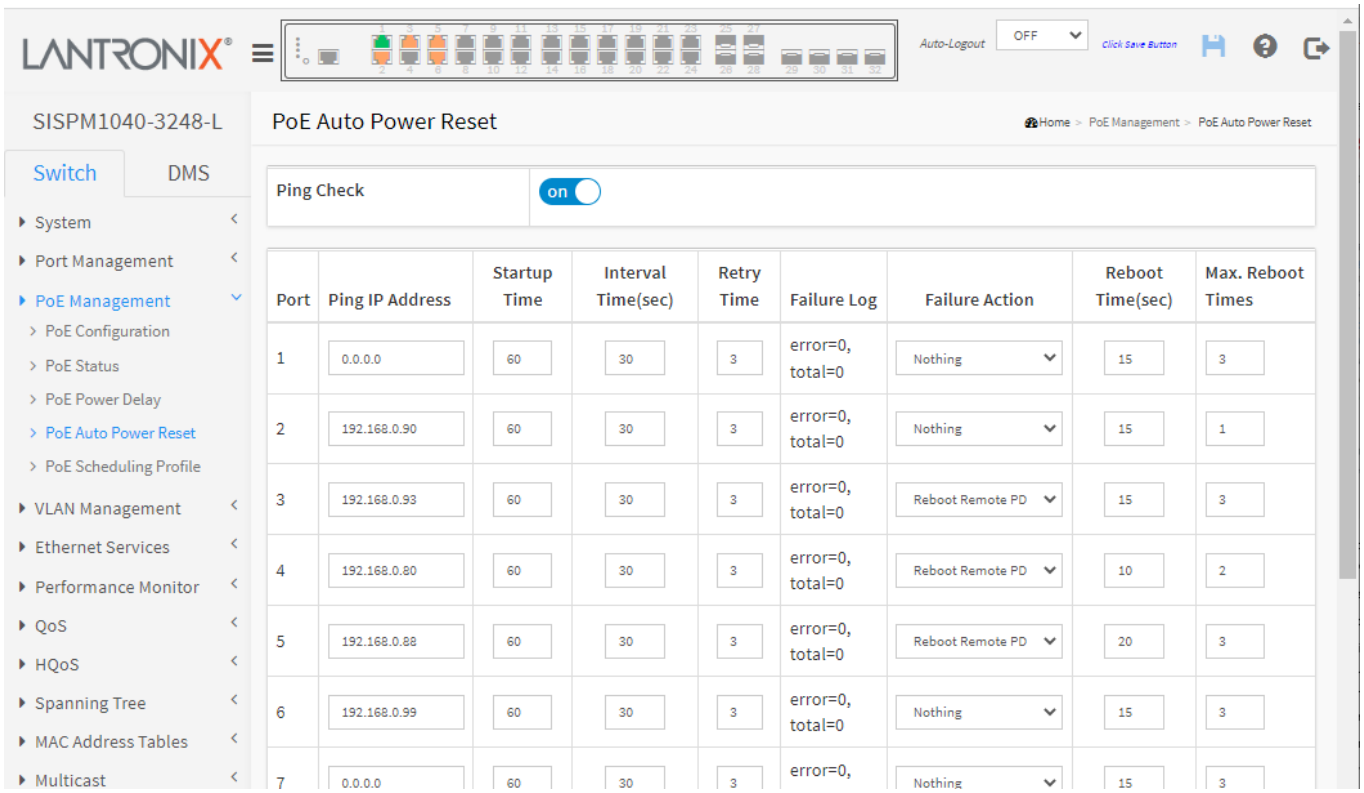
Buttons

Apply : Click to apply changes.

Reset : Click to undo the changes made if not applied.

5-4 PoE Management > PoE Auto Power Reset

This page lets you specify the Auto Power Reset parameters to check the link status between PoE ports and PDs. When a failed connection is detected, the switch will reboot remote the PD automatically.



Ping Check : When ***on***, the Ping Check function detects the connection between PoE port and power device. Setting to ***off*** will turn off the Ping Check function.

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

Ping IP Address : The PD's IP Address the system should ping.

Startup Time(sec) : When PD has been started up, the Switch will wait Start up time to do PoE Auto Power Reset. The default is 60 seconds; the valid range is 30-600 seconds.

Interval Time(sec) : The switch will send checking message to PD each interval time. The default is 30 seconds; the valid range is 10-120 seconds.

Retry Time : When a PoE port cannot ping the PD, it will try to send detection again. After the set number of retry attempts, a configurable failure action is triggered. The default is 3 retries; the valid range is 1-5 retry attempts.

Failure Log : Failure loggings counter.

Failure Action : The action when the third fail detection:

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

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

Reboot Time(sec) : When a PD has been rebooted, the PoE port restored power after the specified time. The default is 15 seconds; the valid range is 3-120 seconds.

Max. Reboot Times: When Failure Action is Reboot Remote PD, it limits the number of times to Reboot. The default is 3 reboots; the range is 0-10. Entering 0 means no reboot limits.

Buttons

Apply : Click to apply changes.

Reset : Click to undo the changes made if not applied.

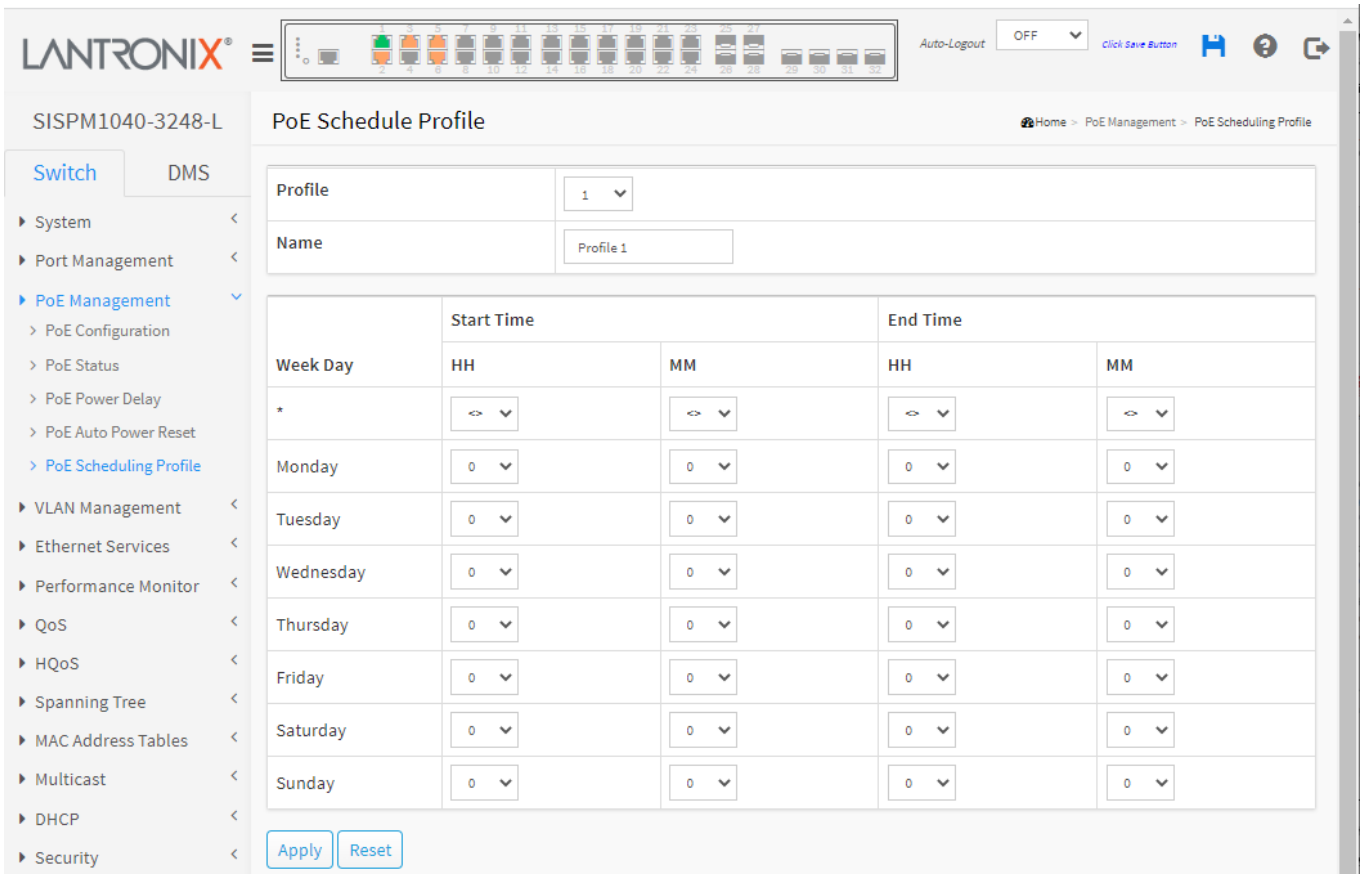
PoE Auto Power Reset "AutoFill" Feature

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 Power Reset" parameter at Switch > PoE Management > PoE Auto Power Reset. The default value of the "Failure Action" parameter is "Reboot Remote PD". Note that "PoE Auto Power Reset" is called "PoE Auto Power Reset" in earlier firmware versions.
2. Configure PoE parameters at DMS > Graphical Monitoring > Topology View.

5-5 PoE Management > PoE Scheduling Profile

This page lets you define 1-16 profiles for PoE scheduling.



Profile : The index of profile. You can configure up to 16 schedule profiles.

Name : The name of profile. The default name is "Profile 1". You can define the name for identifying the profile.

Week Day : The day to schedule PoE.

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

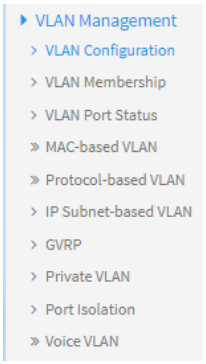
End Time : The time to stop PoE. The time 00:00 means the last second of this day.

Buttons

Apply : Click to save changes.

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

Chapter 6 – VLAN Management



6-1 VLAN Configuration

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

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

To configure VLAN parameters in the web UI:

1. Click VLAN Management and VLAN Configuration.
2. Modify the Global VLAN Configuration parameters.
3. Select the Port VLAN 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.

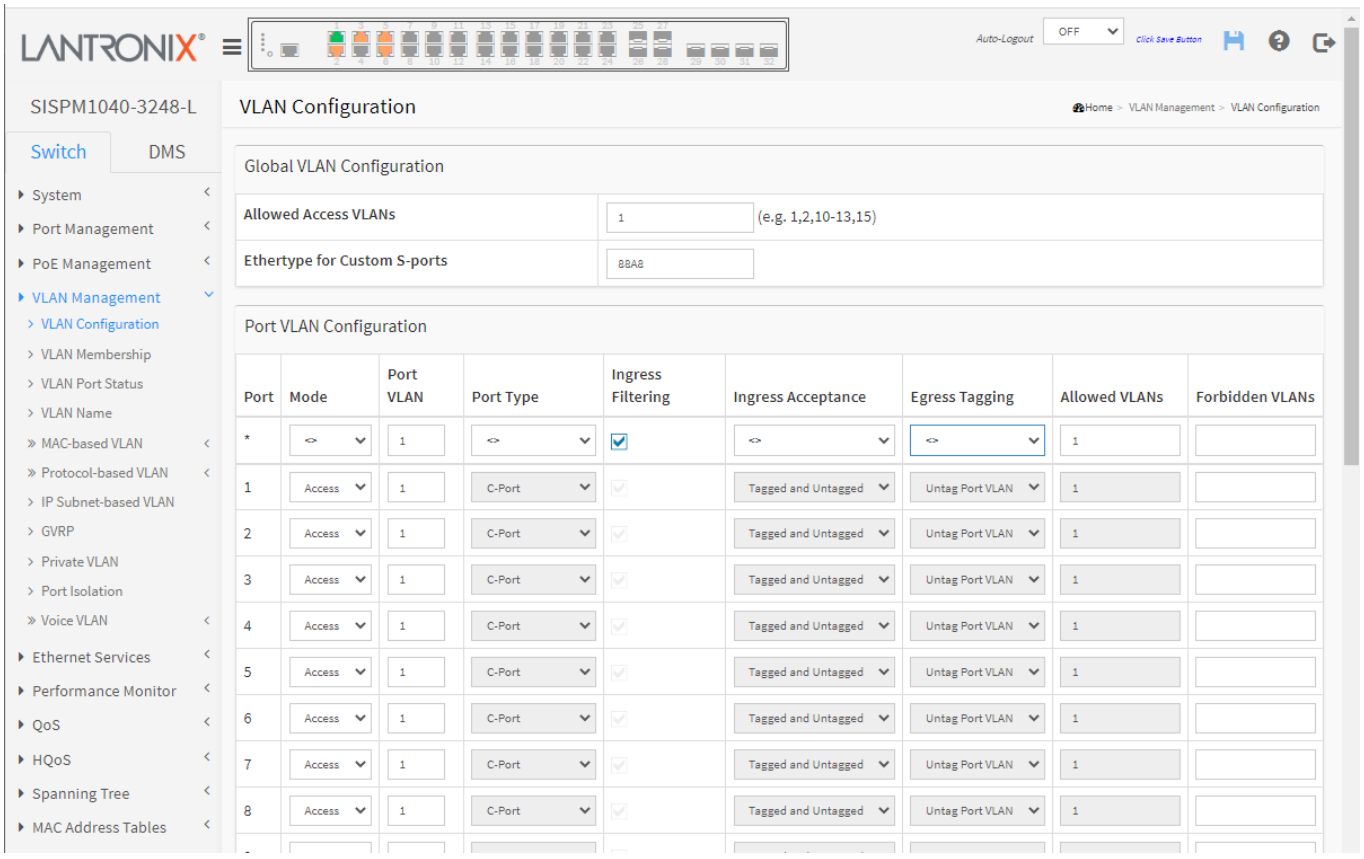


Figure 6-1: VLAN Configuration

Parameter descriptions:

Global VLAN Configuration

Allowed Access VLANs : This field shows the VLANs that are created on the switch. By default, only VLAN 1 exists. More VLANs may be created by using a list syntax where the individual elements are separated by commas. Ranges are specified with a dash separating the lower and upper bound. The following example will create VLANs 1, 10, 11, 12, 13, 200, and 300: 1,10-13,200,300. Spaces are allowed in between the delimiters.

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

Port VLAN Configuration

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

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

Access: Access ports (default) 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 using 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.

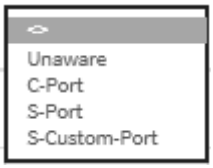
Port VLAN : Determines the port's VLAN ID (a.k.a. PVID). Allowed VLANs are 1 - 4095, the default is VLAN 1.

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. This is the default setting.

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

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

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

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

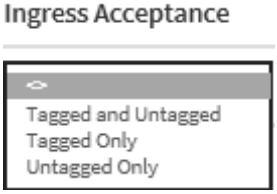
If ingress filtering is ***disabled***, frames classified to a VLAN that the port is not a member of are accepted and forwarded to the switch engine. However, the port will never transmit frames classified to VLANs that it is not a member of.

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

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

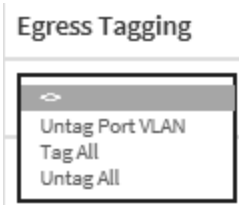
Tagged Only : Only tagged frames are accepted on ingress. Untagged frames are discarded.

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



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

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.

6-2 VLAN Membership

This page lets you view and set 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 box choose which VLAN users to be displayed.
3. Click Refresh to update the page.

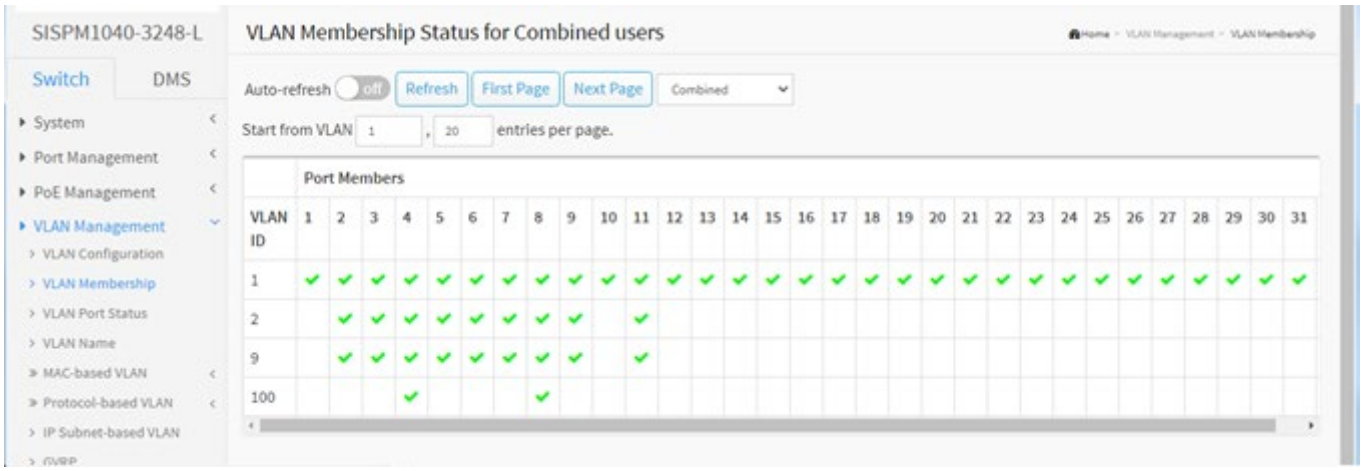


Figure 6-2: VLAN Membership

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 allows for selecting between showing VLAN memberships as configured by an administrator (Admin) or as configured by one of these internal software modules.

The "***Combined***" entry will show a combination of the administrator and internal software modules configuration, and basically reflects what is actually configured in hardware.

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

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

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

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

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

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

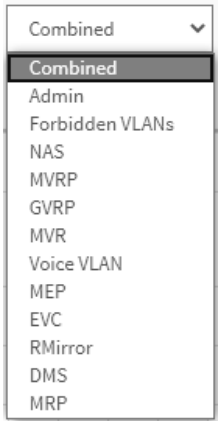
DMS: Shows DMS VLAN membership status.

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

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

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

VLAN Membership : The VLAN Membership Status Page shows the current VLAN port members for all VLANs configured by a selected VLAN User (selection shall be allowed by a Combo Box). When ***Combined*** users are selected, it 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.



Show entries : You can choose how many items you want to be displayed.

User select box : Lets you choose the VLAN User (e.g., Combined, Admin, NAS,MRP, etc.).

Buttons

Auto-refresh : Click to refresh the page automatically every 3 seconds.

Refresh : Click to refresh the page.

First Page : Updates the system log entries, turn to the first page.

Next Page : Updates the system log entries, turn to the next page.

6-3 VLAN Port Status

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

To display VLAN Port Status in the web UI:

1. Click VLAN Management and VLAN Port Status.
2. Specify the user to be displayed at the User select box.
3. View the displayed Port Status information.

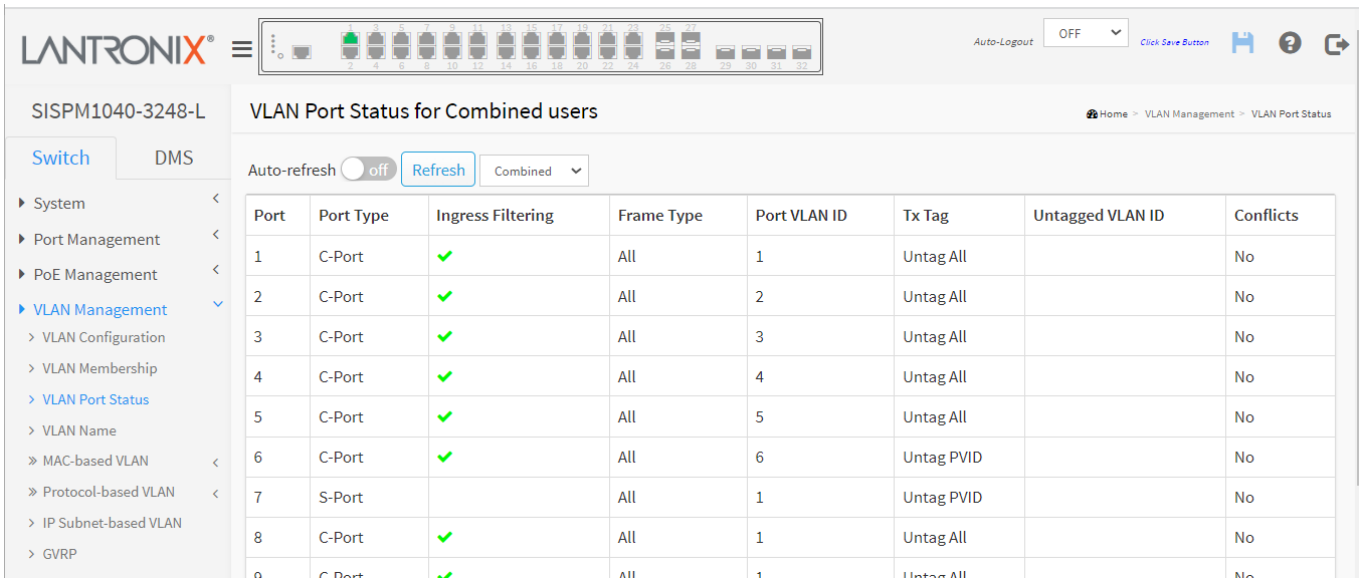


Figure 6-3: VLAN Port Status

Parameter descriptions:

VLAN USER : Various internal software modules may use VLAN services to configure VLAN port configuration on the fly. The drop-down list on the right allows for selecting between showing VLAN memberships as configured by an administrator (Admin) or as configured by one of these internal software modules. The "Combined" entry will show a combination of the administrator and internal software modules configuration, and basically reflects what is actually configured in hardware. If a given software modules hasn't overridden any of the port settings, the text "*No data exists for the selected user*" displays in the table. These VLAN User types are currently supported:

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

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

DMS: Shows DMS VLAN membership status.

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

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

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

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

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

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

Tx Tag : Shows the Tx Tag requirements (Tag All, Tag PVID, Tag UVID, Untag All, Untag PVID, Untag UVID) that a given user has on a port. The field is empty if not overridden by the selected user.

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

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

: **User select box** : Lets you choose the VLAN User. The "Combined" user reflects what is actually configured in hardware.

Buttons

Auto-refresh : Click to refresh the page automatically every 3 seconds.

Refresh : Click to manually refresh the page immediately.

6-4 VLAN Name Configuration

This page displays entries in the VLAN Name Configuration table. The VLAN Name Configuration table can contain up to 4095 entries, and is sorted first by VLAN ID.

To set and display VLAN Names via the web UI:

1. Click VLAN Management, VLAN Name.
2. Enter VLAN Name(s) as desired.
3. Click the Apply button when done.

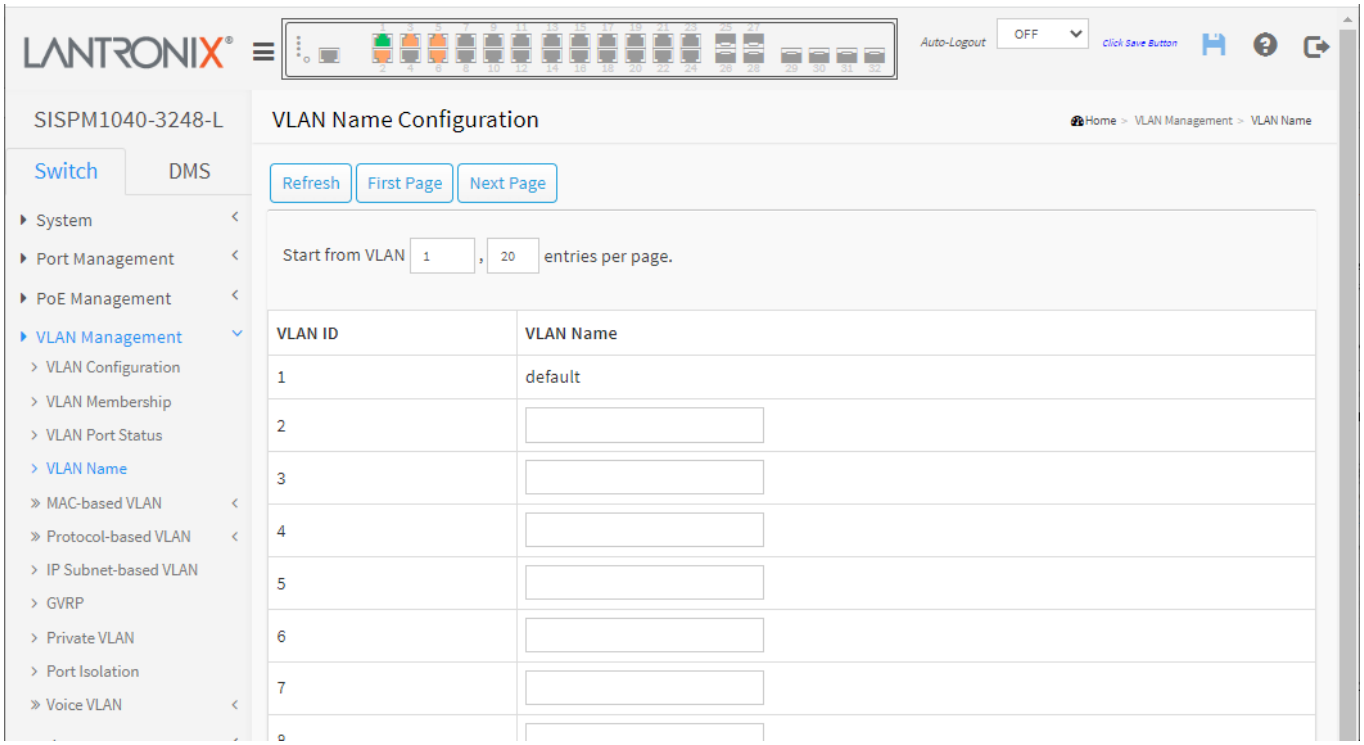


Figure 6-4: VLAN Name Configuration

Parameter descriptions:

VLAN ID: Displays the set of VLAN IDs.

VLAN Name: Lets you enter a name for each VLAN. VLAN ID 1 is assigned the Name 'default'. Some special characters are not accepted.

Buttons

Refresh: Refreshes the displayed table starting from the input fields.

Apply: Click to save changes.

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

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.

6-4 MAC-based VLAN

6-4.1 Configuration

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

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

1. Click VLAN Management, MAC-based VLAN, and Configuration.
2. Click the Add New Entry button.
3. Specify the MAC address and VLAN ID.
4. Check the desired Port Members check box(es).
5. Click Apply.

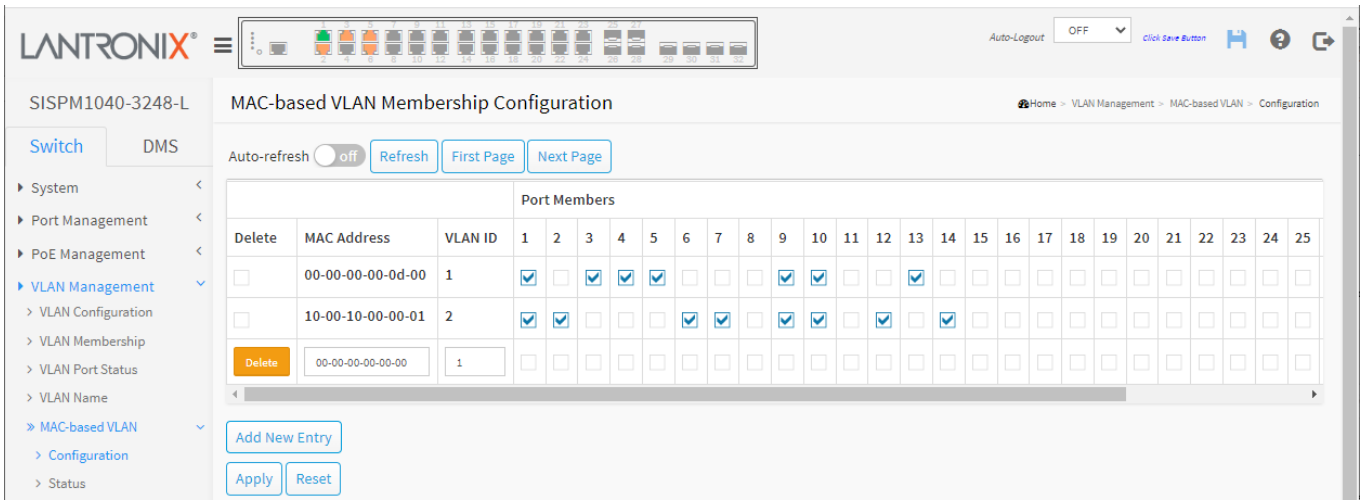


Figure 6-4.1: MAC-based VLAN Membership Configuration

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.

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

Apply : Click to save changes. At least one port must be selected to add an entry.

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

Auto-refresh : Click to refresh the page automatically every 3 seconds.

Refresh : Click to refresh the page.

First Page : Updates the system log entries, turn to the first page.

Next Page : Updates the system log entries, turn to the next page.

Messages:

At least one port must be selected to add an entry

MAC address to VLAN ID mapping already exists and it has to be deleted if new mapping for MAC address to VID is required

6-4.2 Status

Shows the MAC-based VLAN status. This page shows MAC-based VLAN entries configured by various MAC-based VLAN users. These VLAN User types are currently supported:

Static: CLI/Web/SNMP; these are referred to as 'static'.

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

DMS : Displays Device Management System users.

Combined : Displays all of the above users.

To display MAC-based address VLAN Membership in the web UI:

1. Click VLAN Management, MAC-based VLAN, and Status.
2. Select the VLAN User type(s) to be displayed.
3. To automatically refresh the page every 3 seconds click "Auto-refresh" to **on**.
4. Click "Refresh" to immediately refresh the page information.

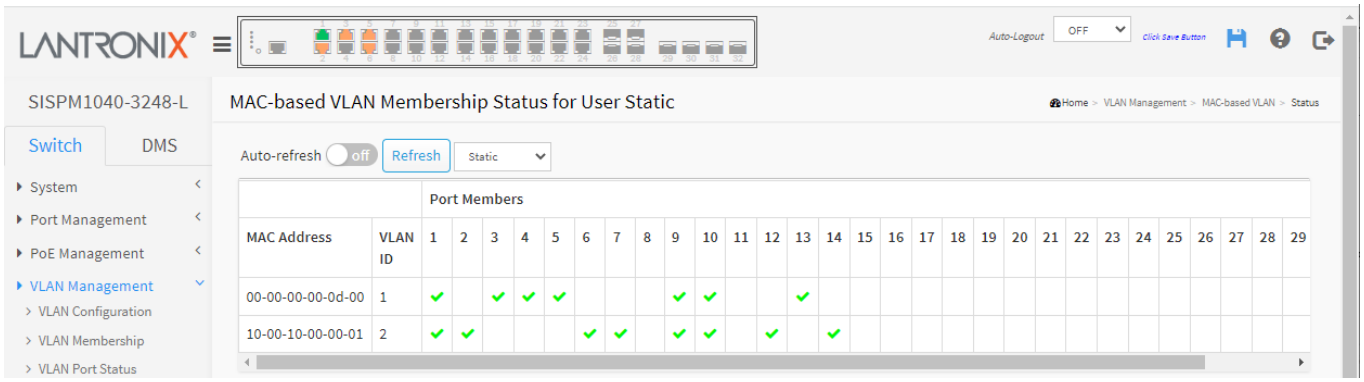


Figure 6-4.2: MAC-based VLAN Membership Status

Parameter descriptions:

MAC Address : Indicates the MAC address.

VLAN ID : Indicates the VLAN ID.

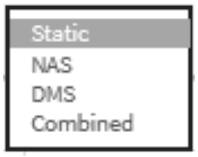
Port Members : A green checkmark indicates Port members of the MAC-based VLAN entry.

Buttons

Auto-refresh : Click to refresh the page automatically every 3 seconds.

Refresh : Click to manually refresh the page immediately.

User select box : Lets you choose the User.



6-5 Protocol-based VLAN

This page lets you configure Protocol -based VLANs; 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, Decnet, 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.

6-5.1 Protocol to Group

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

Web Interface

To configure Protocol -based VLAN configuration 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.

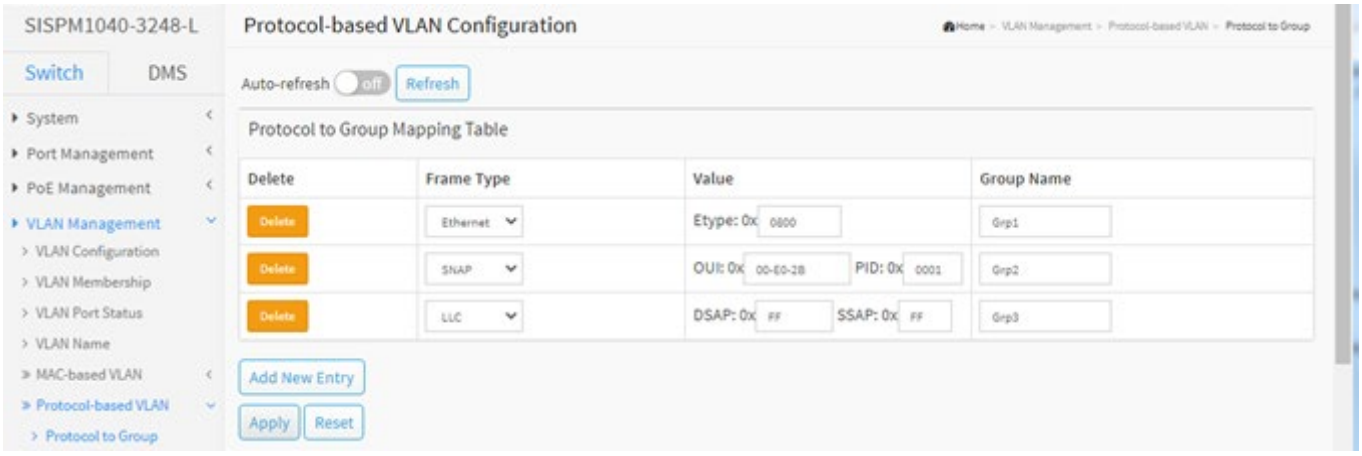
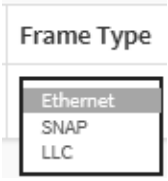


Figure 6-5.1: Protocol-based VLAN Configuration

Parameter descriptions:



Frame Type : Frame Type can have one of these values: Ethernet, LLC, or 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. Below are the criteria for the 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 ranges from 0x0600-0xffff
>
> ***SNAP***: Valid value in this case also is comprised of two different sub-values.
> a. OUI: OUI (Organizationally Unique Identifier) is value in format of xx-xx-xx where each pair (xx) in string is a hexadecimal value 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.
>
> ***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)

Group Name : A valid Group Name is a unique 16-character long string (no special characters allowed).

Buttons

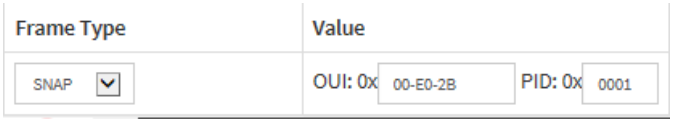
Delete : To delete a Protocol to Group Name map entry, check this box. The entry will be deleted on the switch during the next Save.

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

Apply : Click to save changes.

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

Frame Type Values:



Messages: *Invalid characters found. Please check help page for correct Group name format*.

6-5.2 Group to VLAN

This page lets you map an already configured Group Name to a VLAN for the switch. You can configure up to 256 Group to VLAN mappings.

To configure Group Name to VLAN mapping table configured 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. Click Apply.

Figure 6-5.2: Group Name to VLAN Mapping Table

Parameter descriptions:

Group Name : A valid Group Name is a string of at most 16 characters. A valid Group Name is a string, at the most 16 characters long, which consists of a combination of alphabets (a-z or A-Z) and integers (0-9) with no special characters allowed. You may either use a Group that already includes one or more protocols (see Protocol to Group mappings) or create a Group to VLAN ID mapping that will become active the moment you add one or more protocols inside that Group. Furthermore, the Group to VLAN ID mapping is not unique, as long as the port lists of these mappings are mutually exclusive (e.g. Group1 can be mapped to VID 1 on port#1 and to VID 2 on port#2).

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

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

Buttons

Delete : To delete a Group Name to VLAN map entry, check this box. The entry will be deleted during the next save.

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.

Auto-refresh : Click to refresh the page automatically every 3 seconds.

Refresh : Click to manually refresh the page immediately.

6-6 VCL IP Subnet-based VLAN Configuration

IP subnet-based VLAN entries can be configured here. This page allows adding, updating and deleting IP subnet-based VLAN entries and assigning them to different ports. The maximum number of entries is 128.

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, VLAN ID, and Port Members.
4. Click Apply.

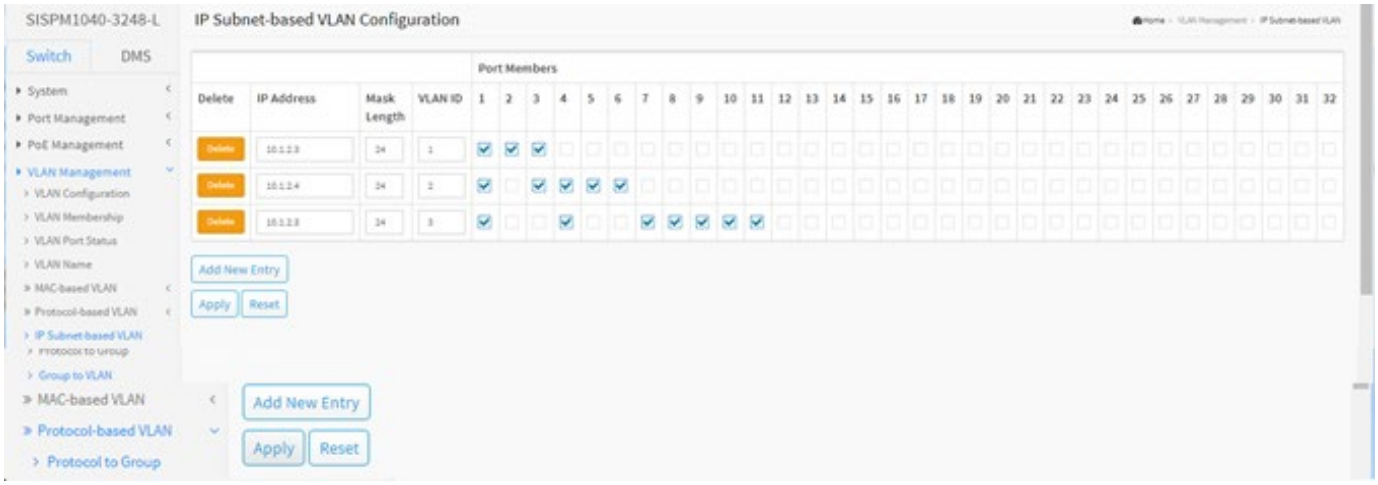


Figure 6-6: IP Subnet-based VLAN Configuration

Parameter descriptions:

IP Address : Indicates the IP address.

Mask Length : Indicates the network mask length.

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

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

Buttons

Delete : To delete an IP subnet-based VLAN entry, check this box and click Apply. The entry will be deleted from the switch.
Add New Entry : Click the button 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. 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.

Messages: *IP Subnet to VLAN ID mapping already exists and it has to be deleted if new mapping is required*

6-7 GVRP

This page lets you configure global GVRP settings that are commonly applied to all GVRP enabled ports.

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

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

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 GVRP Mode for each port.
5. Click Apply to save the settings.

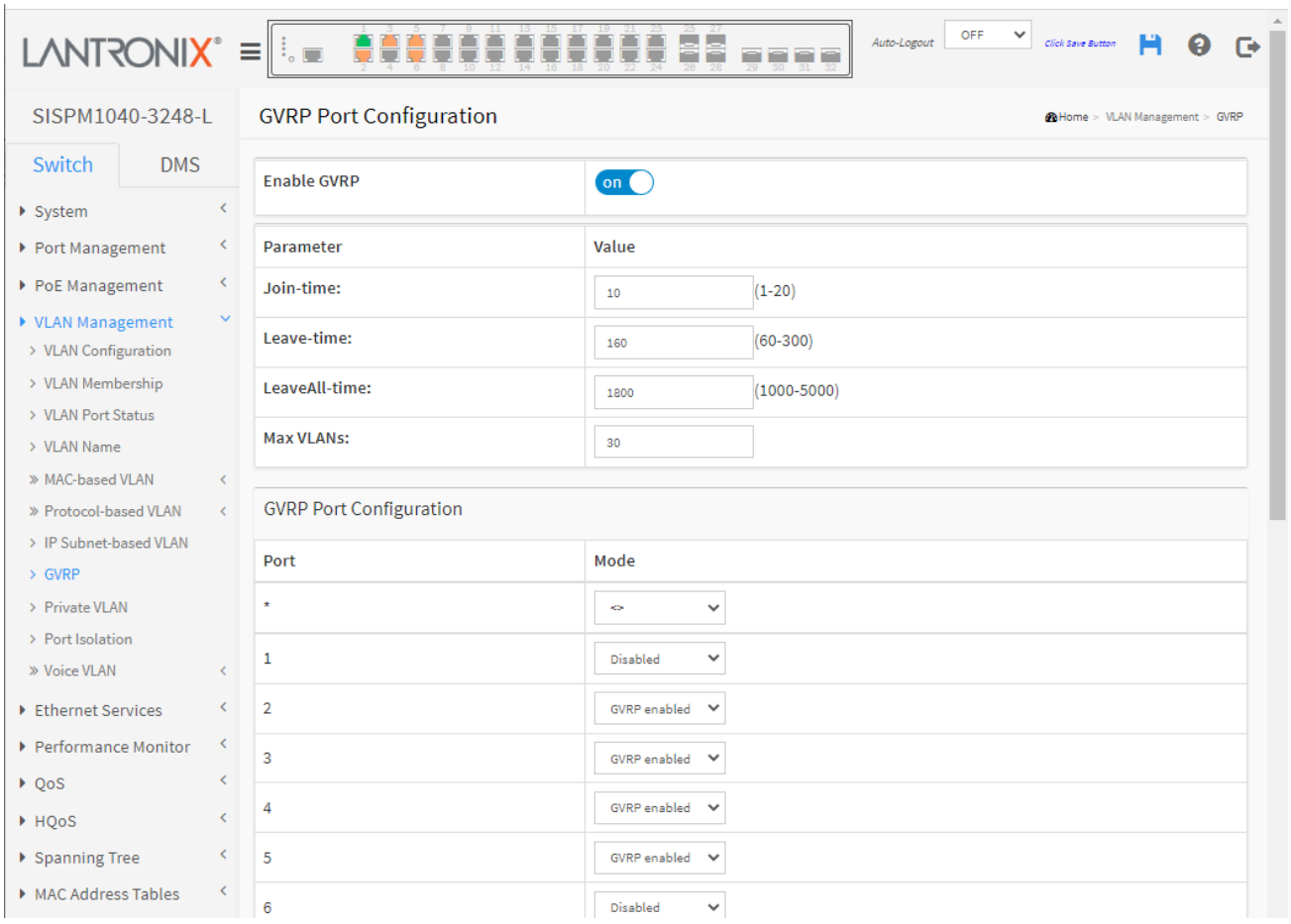


Figure 6-7: GVRP Port Configuration

Parameter descriptions:

Enable GVRP globally : The GVRP feature is enabled by checking the checkbox ‘ Enable GVRP’.

GVRP protocol timers :

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

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

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

Port : The Port column shows the list of ports.

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

Disable: Select to Disable GVRP mode on this port.

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

Buttons

Apply : Click to save changes.

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

6-8 Private VLAN

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

Private VLANs are based on the source port mask, and there are no connections to VLANs. This means that VLAN IDs and Private VLAN IDs can be identical. A port must be a member of both a VLAN and a Private VLAN to be able to forward packets. By default, all ports are VLAN unaware and members of VLAN 1 and Private VLAN 1.

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

To configure Private VLAN Membership in the web UI:

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

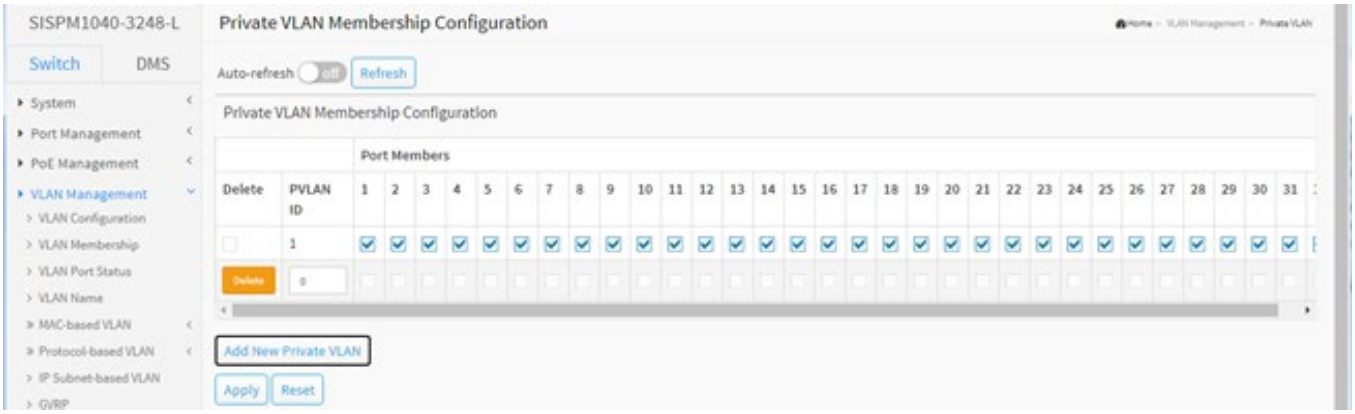


Figure 6-8: Private VLAN Membership Configuration

Parameter descriptions:

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

Private VLAN ID : Indicates the ID of this particular private VLAN.

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

Add New Private VLAN : Click to add a new private VLAN ID. An empty row is added to the table, and the private VLAN can be configured as needed. The allowed range for a private VLAN ID is the switch port number range. Any values outside this range are not accepted, and a warning message displays. The Private VLAN is enabled when you click "Apply". The Reset button can be used to undo the addition of new Private VLANs.

Buttons

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

6-9 Port Isolation

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

This page is used for enabling or disabling port isolation on ports in a Private VLAN. A port member of a VLAN can be isolated from other isolated ports on the same VLAN and Private VLAN.

To configure Port Isolation parameters in the web UI:

1. Click VLAN Management and Port Isolation.
2. Check the port(s) on which you want to enable Port Isolation.
3. Click Apply.

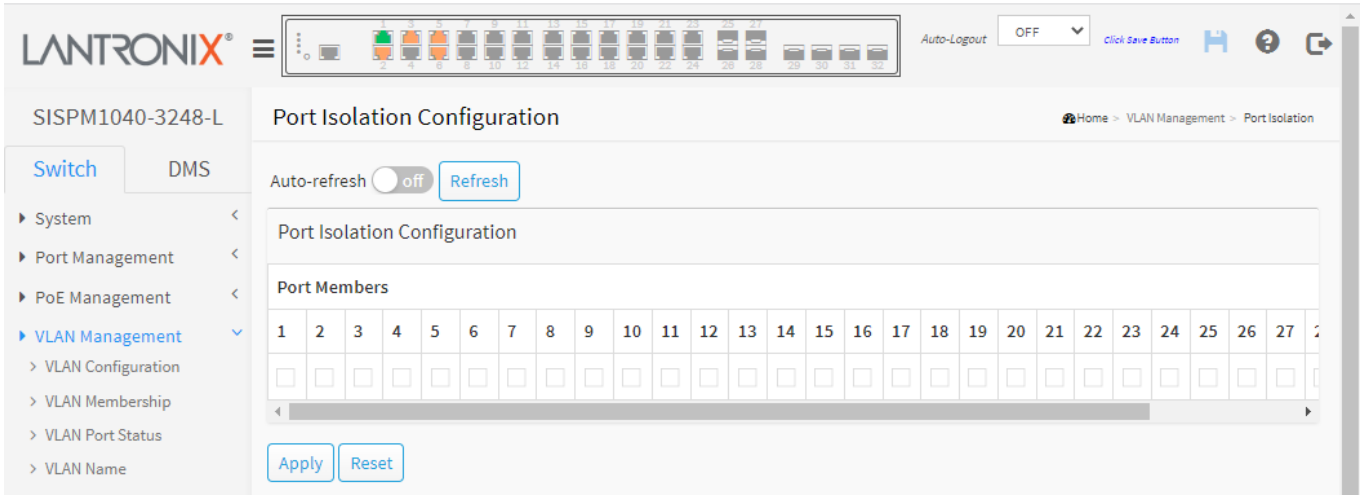


Figure 6-9: Port Isolation Configuration

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.

6-10 Voice VLAN

A Voice VLAN is a VLAN configured specially for voice traffic. By adding ports with voice devices attached to voice VLAN, you can configure QoS-related parameters for voice data, ensuring the transmission priority of voice traffic and voice quality.

6-10.1 Configuration

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

To configure Voice VLAN in the web UI:

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

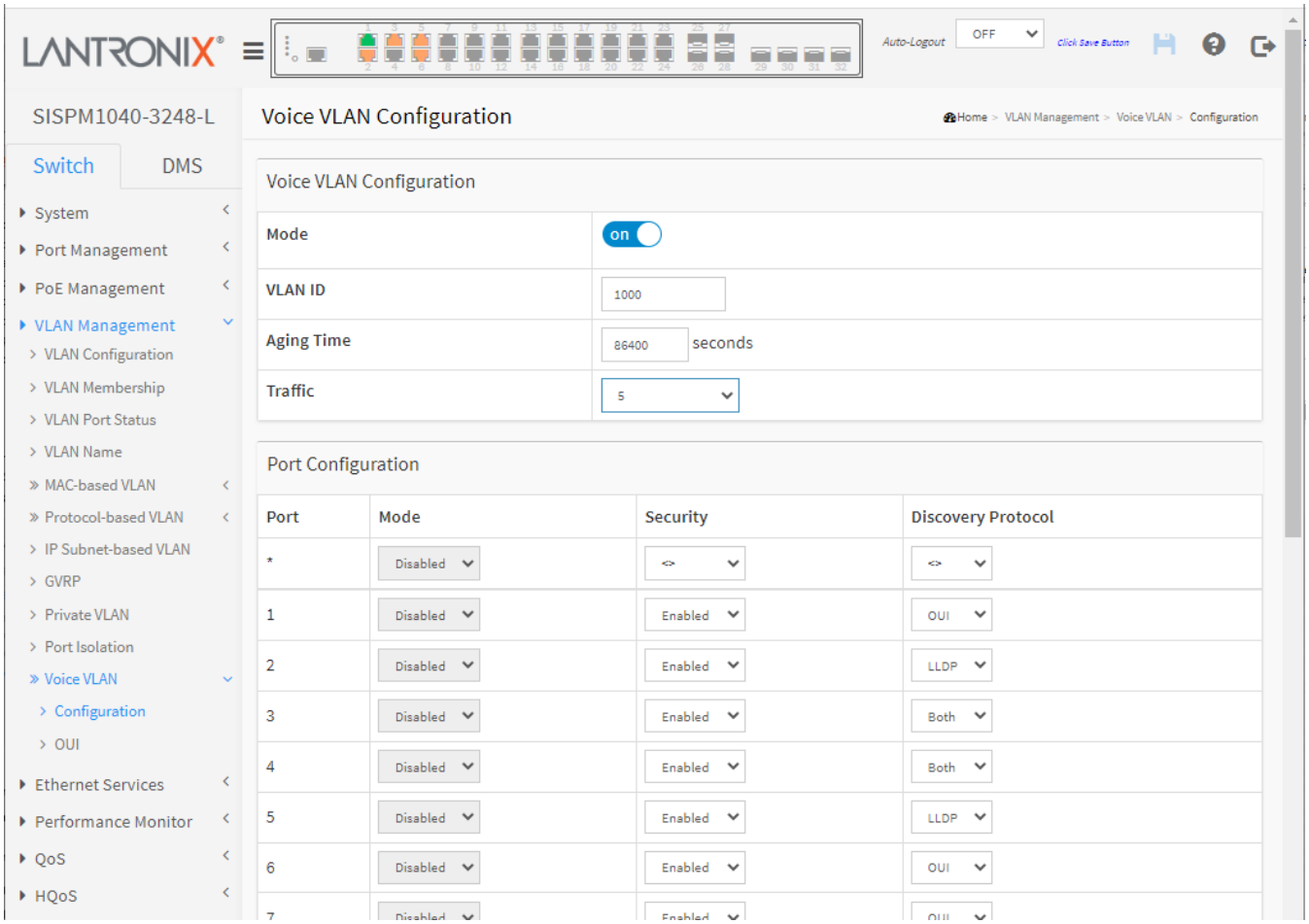


Figure 6-10.1: Voice VLAN Configuration

Parameter descriptions:

Mode : Indicates the Voice VLAN mode operation. You must disable the MSTP feature at Spanning Tree > MSTI Configuration before you enable the Voice VLAN Mode to avoid conflict with ingress filtering. Possible modes are:

on: Enable Voice VLAN mode operation.

off: Disable Voice VLAN mode operation.

VLAN ID : Enter a 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 - 4095.

Aging Time : Indicates the Voice VLAN secure learning aging time. The allowed range is 10 to 10000000 seconds. It is used when security mode or auto detect mode is enabled. In other cases, it will be based on hardware aging time. The actual aging time will be situated between the [age_time; 2 * age_time] interval.

Traffic : Select a Voice VLAN traffic class (***0 (Low)*** to ***7 (High)***. All traffic on the Voice VLAN will apply this class.

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

Mode : Indicates the Voice VLAN port mode. Possible port modes are:

Disabled: Disjoin from Voice VLAN.

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

Forced: Force join to Voice VLAN.

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.

Security : Indicates the Voice VLAN port security mode. When the function is enabled, all non-telephonic MAC addresses in the Voice VLAN will be blocked for 10 seconds. Possible port modes are:

Enabled: Enable Voice VLAN security mode operation.

Disabled: Disable Voice VLAN security mode operation.

Discovery Protocol : Indicates the Voice VLAN port discovery protocol. It will only work when Auto detect mode is enabled. You must enable the LLDP feature at LLDP > LLDP Configuration before setting the 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 Organizationally Unique Identifier address.

LLDP: Detect telephony device by LLDP.

Both: Use both OUI and LLDP to detect telephony device.

Buttons

Apply : Click to save changes.

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

6-10.2 OUI

This page lets you configure the Voice VLAN OUI table. An OUI (Organizationally Unique Identifier (OUI address) is a globally unique identifier assigned to a vendor by IEEE. You can determine which vendor a device belongs to according to the OUI address which forms the first 24 bits of a MAC address. The maximum number of entries is 16. Modifying the OUI table will restart auto detection of the OUI process.

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 in the Voice VLAN OUI Table and click Apply.

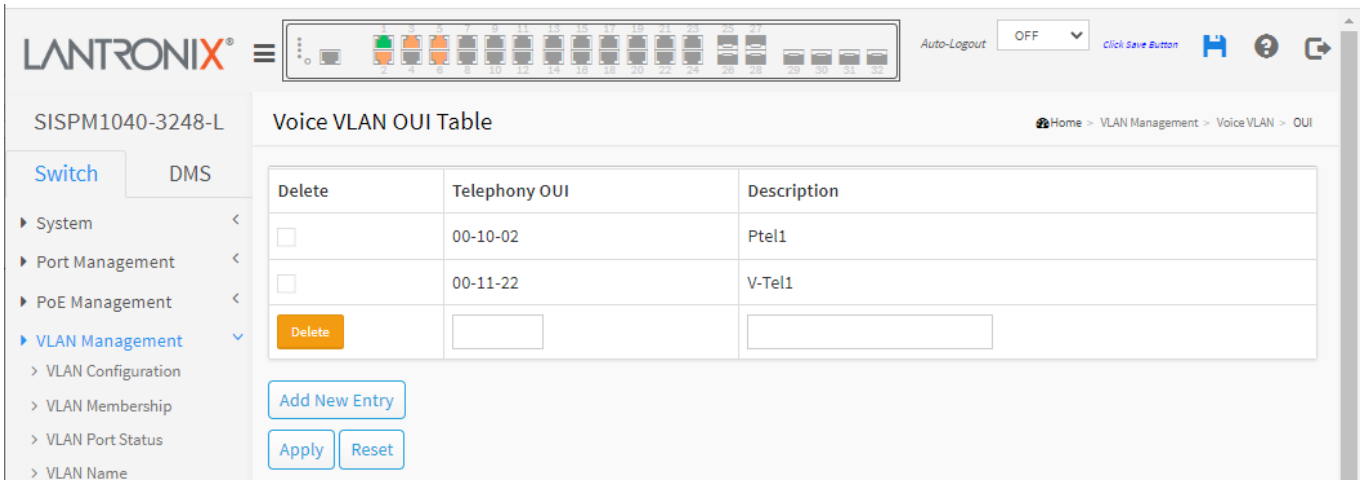


Figure 6-10.2: Voice VLAN OUI Table

Parameter descriptions:

Delete : Check to delete the entry. It will be deleted immediately.

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

00-01-E3	Siemens AG phones
00-03-6B	Cisco phones
00-0F-E2	H3C phones
00-60-B9	Philips and NEC AG phones
00-D0-1E	Pingtel phones
00-E0-75	Polycom phones
00-E0-BB	3Com phones

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 to configure the Telephony OUI and Description parameters.

Apply : Click to save changes.

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

Chapter 7 – Ethernet Services

The switch supports Ethernet Services. This section lets you view and/or configure EVC ports, Encapsulations, L2CP, CoS ID Policers, EVCs, ECEs, and EVC statistics.

EVC (Ethernet Virtual Connection) is a MEF standard that describes services provided to customers at User Network Interfaces (UNIs). Inside provider networks, nodes are connected using Internal Network-to-Network Interfaces (I-NNIs). Connections between service providers are done using External Network-to-Network Interfaces (E-NNIs). An Ethernet Virtual Connection is an association of two or more UNIs.

7-1 Ports

This page lets you view and configure current EVC port parameters from Switch > Ethernet Services > Ports.

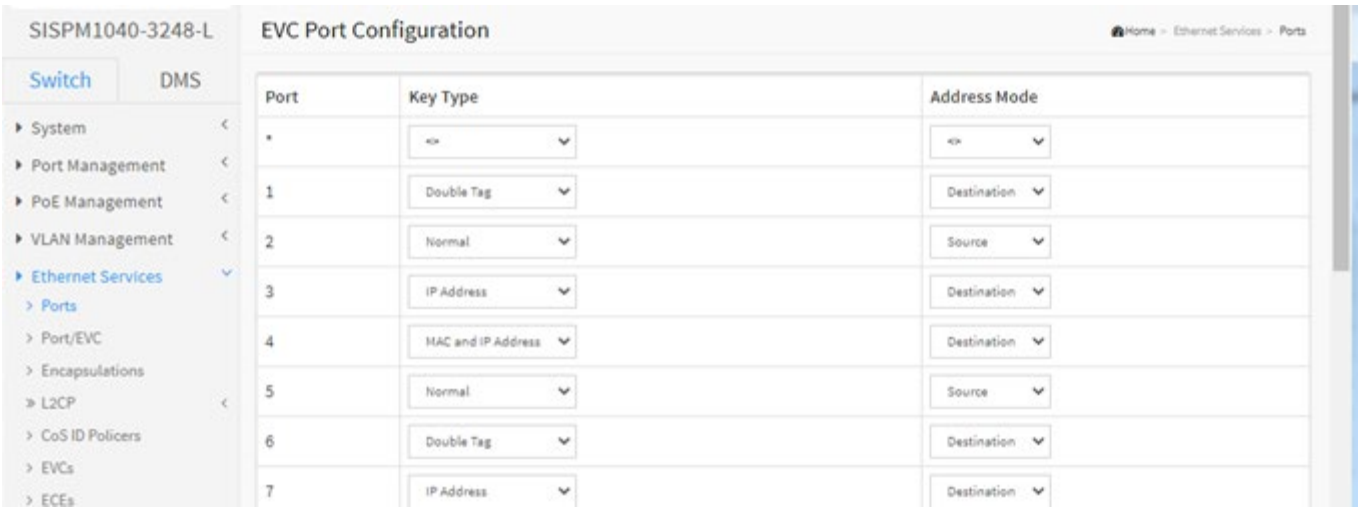
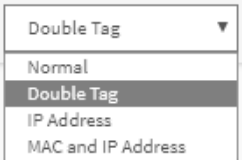


Figure 7-1: EVC Ports Configuration

Parameter descriptions:

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

Key Type : The key type specifying the key generated for frames received on the port. The allowed values are:



Normal: Medium key, match inner and outer tag, SIP/DIP, and SMAC/DMAC.

Double Tag: Small key, match inner and outer tag.

IP Address: Medium key, match inner and outer tag, SIP and DIP.

MAC and IP Address: Large key, match inner and outer tag, SMAC, DMAC, SIP and DIP.

Filtering on DMAC type (unicast/multicast/broadcast) is supported for any key type.

Address Mode : The IP/MAC address mode specifying whether the EVC classification must be based on source (SMAC/SIP) or destination (DMAC/DIP) addresses. This parameter is only used when the key type is Normal. The allowed values are:

Source: Enable SMAC/SIP matching.

Destination: Enable DMAC/DIP matching.

Buttons

Apply : Click to save changes.

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

7-2 EVC Port Configuration

This page lets you view and configure current EVC port parameters from the Switch > Ethernet Services > Port/EVC menu path.

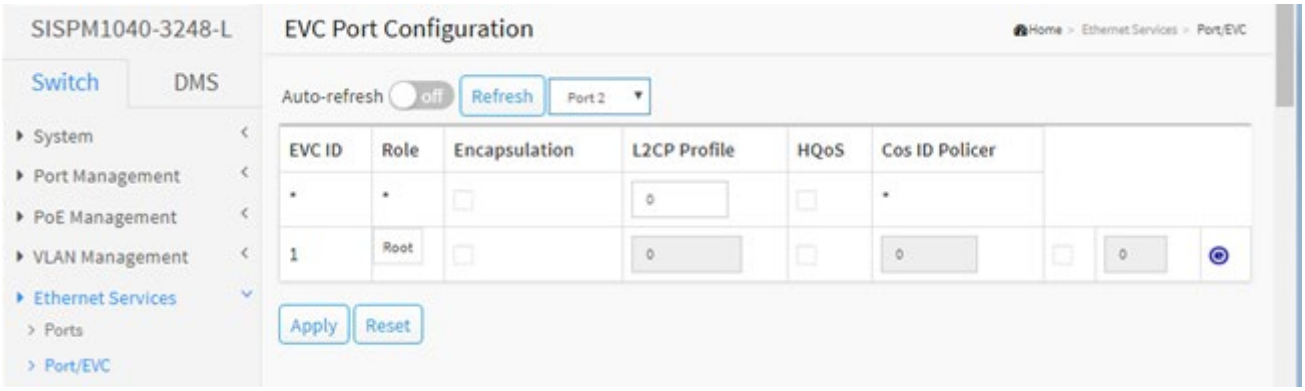


Figure 7-2: EVC Port Configuration

Parameter descriptions:

EVC ID : The EVC ID.

Role : The port role on the specific EVC. Valid values are:

> ***Disabled***: Not UNI or NNI. A ***UNI*** (user–network interface) is a demarcation point between the responsibility of the service provider and the responsibility of the subscriber. An ***NNI*** (network-to-network interface) defines a similar interface between provider networks.
>
> ***NNI***: NNI role.
>
> ***Root***: Root UNI role.
>
> ***Leaf***: Leaf UNI role.

Encapsulation : The encapsulation ID mapping on the specific EVC. The allowed range is 0 - 907.

L2CP Profile : The L2CP Profile ID mapping on the specific EVC. The allowed range is 0 - 62.

HQoS : The Hierarchical QoS ID mapping. The allowed range is 1 - 256.

Cos ID Policer : The Cos ID Policer mapping on the specific EVC. For UNI ports, 8 policers are allocated (COSID 0-7). For NNI ports, one policer is allocated (COSID 0).

Buttons

Auto-refresh: Click to manually refresh the page immediately.

Refresh: Click to manually refresh the page immediately.

Port Select box : At the dropdown select which port's parameters to display.

: Click to go to the EVC CoS ID Policer Configuration table at Switch > Ethernet Services > CoS ID Policers.

Apply : Click to save changes.

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

7-3 EVC Encapsulation Configuration

This page lets you view and configure current EVC encapsulation parameters from the Switch > Ethernet Services Encapsulations menu path.

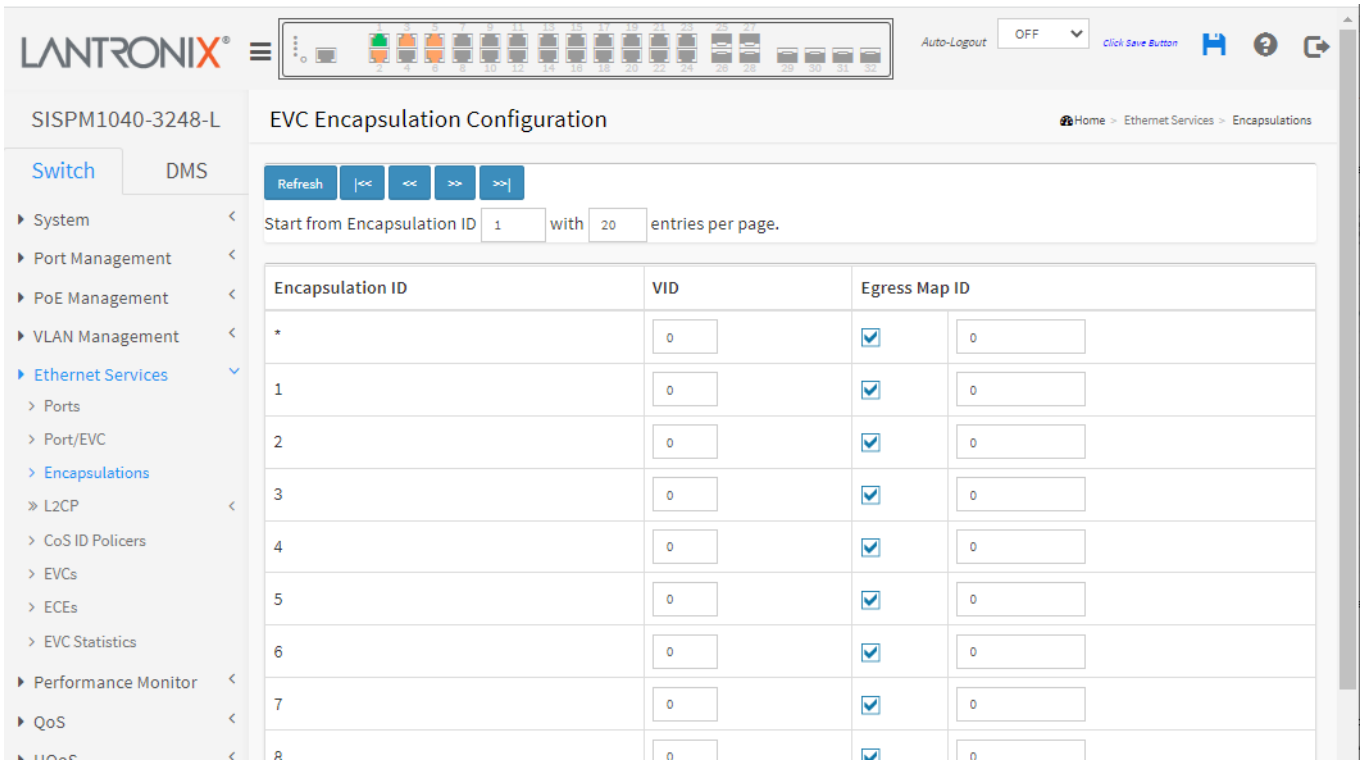


Figure 7-3: EVC Encapsulation Configuration

Parameter descriptions:

Start from Encapsulation ID : The start Encapsulation ID for displaying the table entries. The valid range is 0 – 908 encapsulations.

entries per page : The number of entries to display on each page. The allowed range is 2 - 99. The default is 10.

Encapsulation ID : The encapsulation ID for the encapsulation configuration (1-10).

VID : The VLAN ID for the encapsulation configuration. The valid range is 0 - 4095. The default is 0.

Egress Map ID : The QoS egress mapping ID for the encapsulation configuration. The valid range is 0 - 255.

Buttons

Refresh : Refreshes the displayed table starting from the input fields.

|<< : : Updates the table, starting with the first entry in the table.

<< : Updates the table, ending at the entry before the first entry currently displayed.

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

>>| : : Updates the table, ending at the last entry in the table.

Apply : Click to save changes.

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

7-4 EVC L2CP Profile Configuration

This page lets you view and configure current EVC L2CP (Layer 2 Control Protocol) Profile parameters from the Switch > Ethernet Services > L2CP > L2CP Profiles menu path.

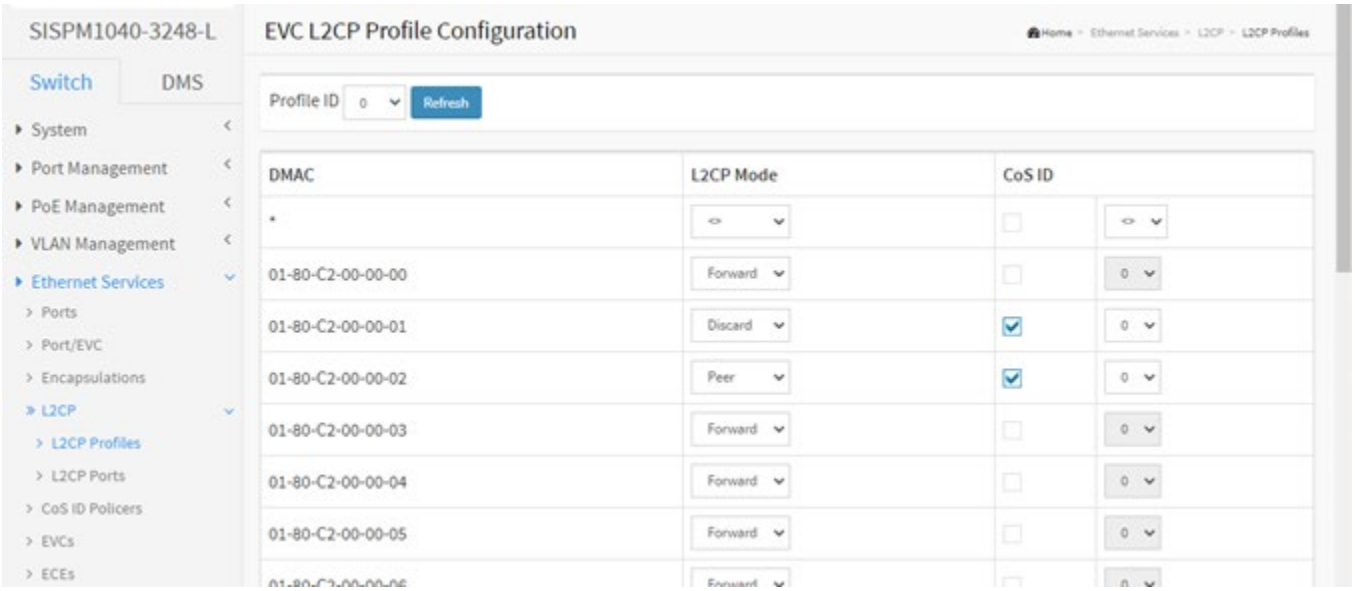


Figure 7-4: EVC L2CP Profile Configuration

Parameter descriptions:

DMAC : The destination BPDU MAC addresses (01-80-C2-00-00-0X) and GARP (01-80-C2-00-00-2X) MAC addresses for the settings contained in the same row.

L2CP Mode : The L2CP mode for the specific profile. Valid values are:

Peer: Allow to peer L2CP frames.

Forward: Allow to forward L2CP frames.

Discard: Drop L2CP frames.

CoS ID : The CoS ID mapping for the specific profile.

: The **Profile ID** select box defines which profile ID is configured on the page.

Buttons

Refresh : Refreshes the displayed table starting from the input fields.

Apply : Click to save changes.

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

7-5 EVC L2CP Port Configuration

This page lets you view and configure current EVC L2CP Port Configuration parameters from the Switch > Ethernet Services > L2CP > L2CP Ports menu path.

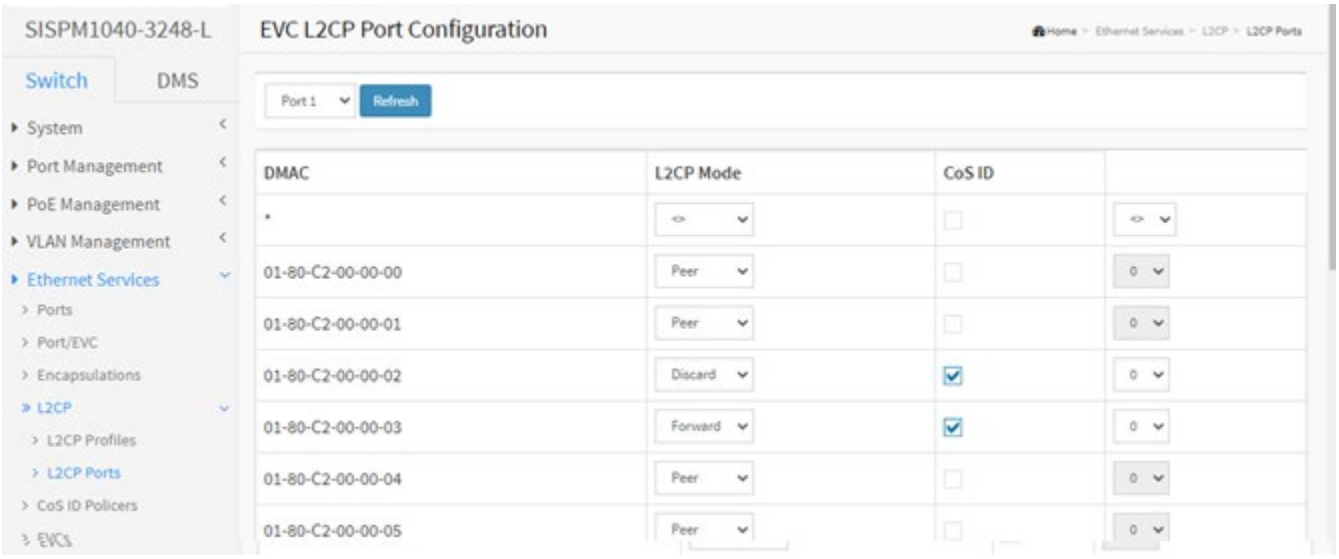


Figure 7-5: EVC L2CP Port Configuration

Parameter descriptions:

: The Port select box determines which profile ID is configured on the page.

DMAC : The destination BPDU MAC addresses (01-80-C2-00-00-0X) and GARP (01-80-C2-00-00-2X) MAC addresses for the settings contained in the same row.

L2CP Mode : The L2CP mode for the specific port. Valid values are:

Peer: Allow to peer L2CP frames (default setting).

Forward: Allow to forward L2CP frames.

Discard: Drop L2CP frames.

CoS ID : The CoS ID mapping for the specific port. If checked (enabled) select a level in the dropdown.

Buttons

Refresh : Refreshes the displayed table starting from the input fields.

Apply : Click to save changes.

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

7-6 EVC CoS ID Policer Configuration

This page lets you view and configure current EVC CoS ID Policer Configuration parameters from the Switch > Ethernet Services > CoS ID Policers menu path. These policers may be used to limit the traffic received on NNI/UNI ports. A policer can limit the bandwidth of received frames. It is located in front of the ingress queue.

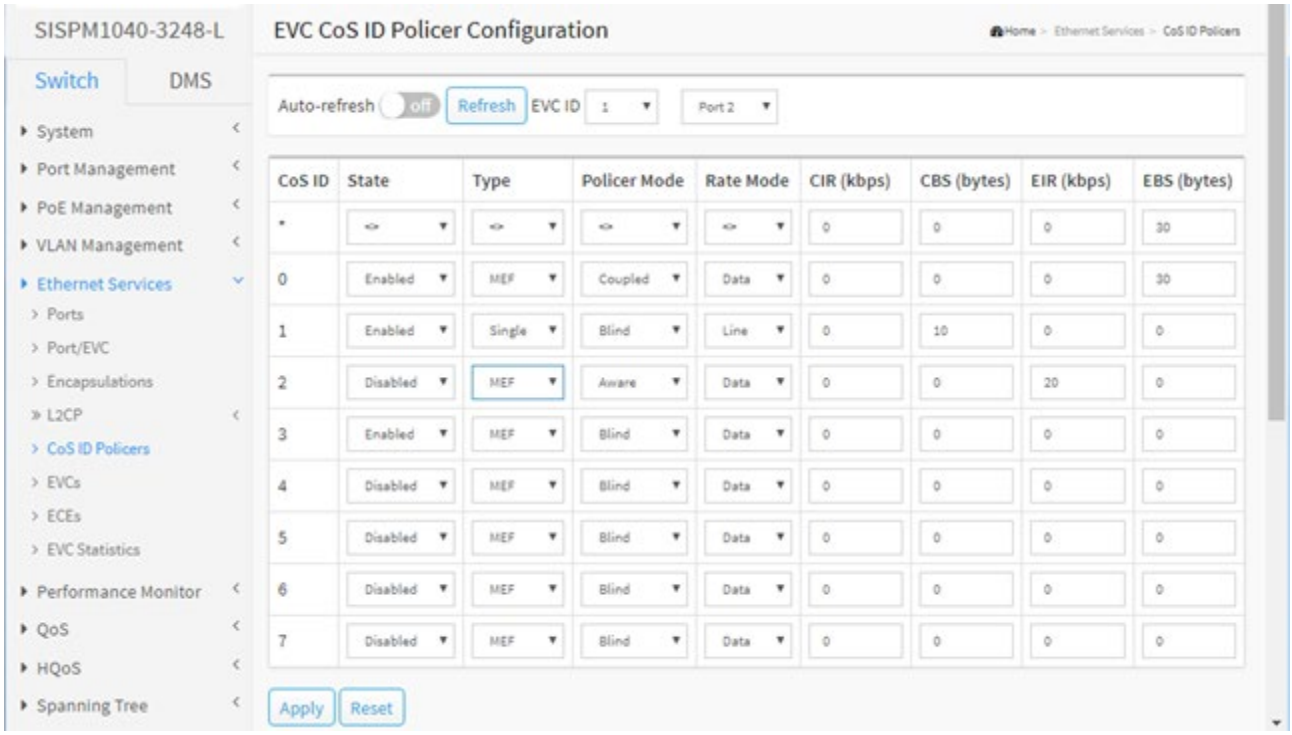


Figure 7-6: EVC CoS ID Policer Configuration

Parameter descriptions:

CoS ID : The Class of Service Identifier.

For ***UNI*** ports, 8 policers are allocated (COSID 0-7).

For ***NNI*** ports one policer is allocated (COSID 0).

State : The administrative state of the policer. Valid values are:

Enabled: The policer enabled.

Disabled: The policer is disabled.

Type : The type of the policer. The allowed values are:

MEF: Metro Ethernet Forum ingress policer.

Single: Single bucket policer.

Policer Mode : The colour mode of the policer. The allowed values are:

Coupled: Colour-aware mode with coupling enabled.

Aware: Colour-aware mode with coupling disabled.

Blind: Colour-blind mode.

Rate Mode : The rate mode of the policer. The allowed values are:

Data: Specify that this policer operates on data rate.

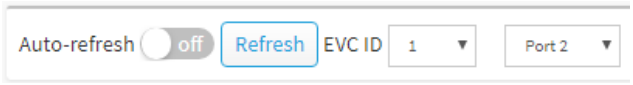
Line: Specify that this policer operates on line rate.

CIR (kbps): The Committed Information Rate of the policer. The valid range is 0 - 1000000 kilobits per second (Kbps).

CBS (bytes): The Committed Burst Size of the policer. The valid range is 0 - 100000 bytes. Burst size can be set to any number of bytes, but the HW accuracy is platform dependent. Ask your platform provider for further details.

EIR (kbps): The Excess Information Rate for MEF type policer. The allowed range is 0 - 1000000 kilobit per second.

EBS (bytes): The Excess Burst Size for MEF type policer. The valid range is 0 - 100000 bytes. Burst size can be set to any number of bytes, but the HW accuracy is platform dependent. Ask your platform provider for further details.



Buttons

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

Refresh : Click to manually refresh the page immediately.

: The EVC ID select box determines which EVC ID is affected by clicking the buttons.

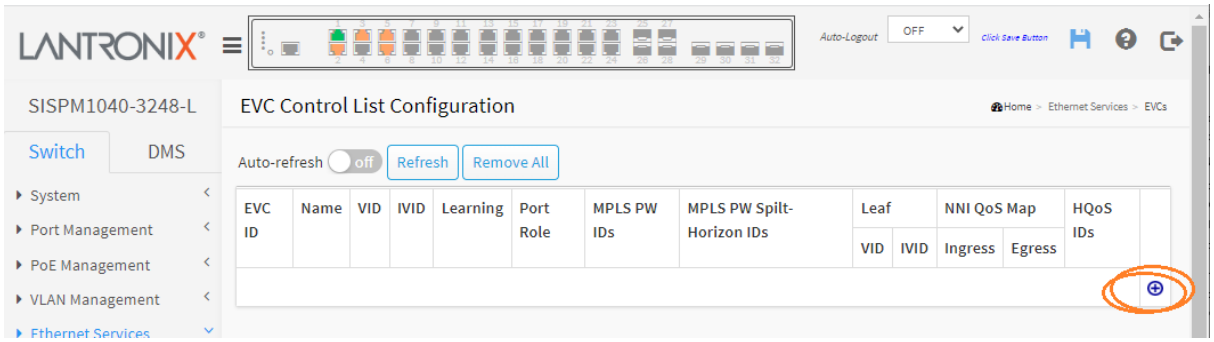
: The port select box determines which port is affected by clicking the buttons.

Apply : Click to save changes.

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

7-7 EVC Configuration

This page lets you view and configure EVC parameters from the Switch > Ethernet Services > EVCs menu path. These policers may be used to limit the traffic received on NNI/UNI ports. A policer can limit the bandwidth of received frames. It is located in front of the ingress queue. Note: only Provider Bridge EVCs are supported.



From the default EVC Control List Configuration page, click the Add EVC (⊕) icon to display the EVC Configuration page and add new EVCs as shown and described below.

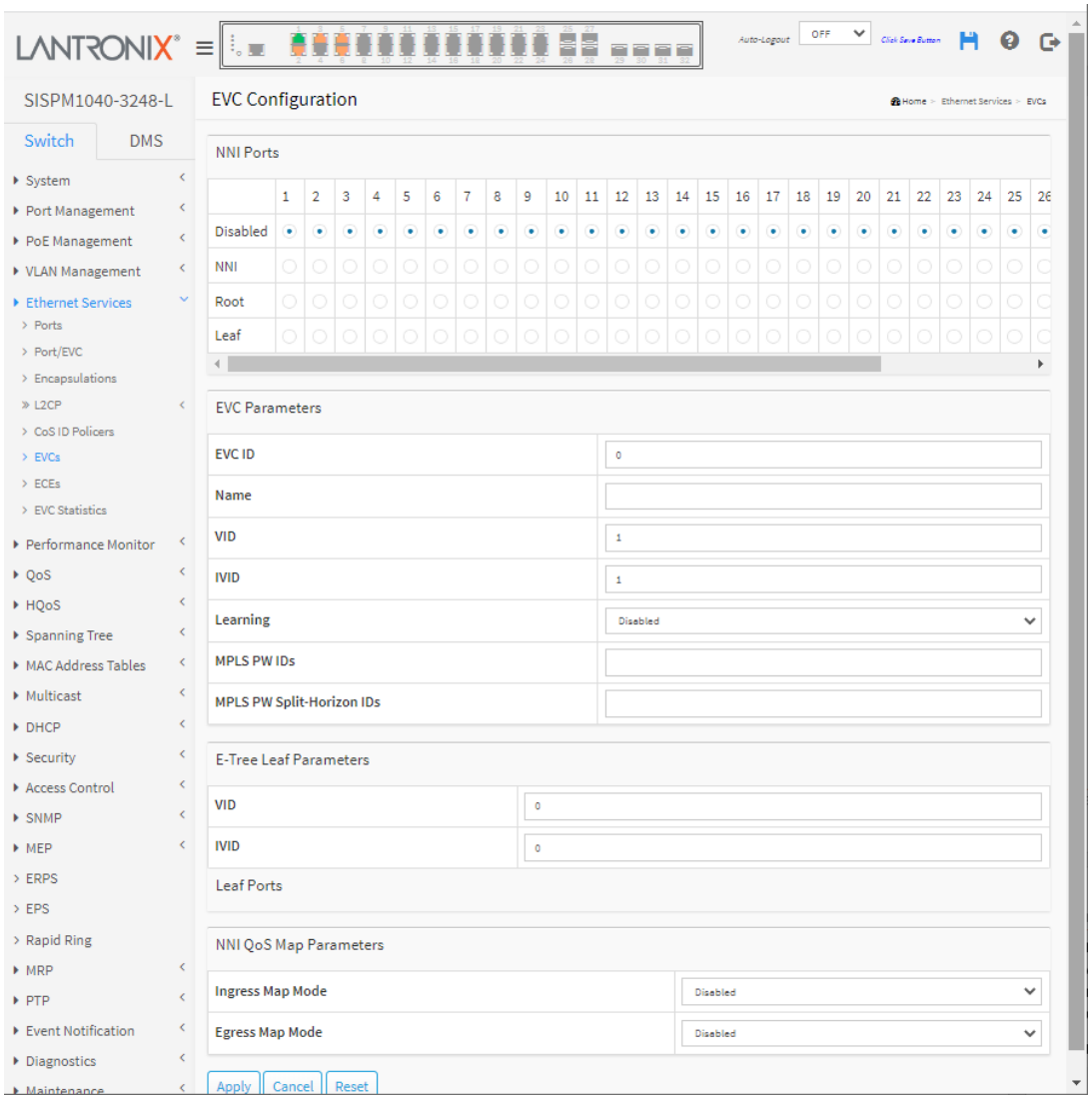


Figure 7-7: EVC Configuration

Parameter descriptions:

NNI Ports : For each port select Disabled, NNI, Root, or Leaf. The default is Disabled.

EVC Parameters :

EVC ID : The EVC ID identifies the EVC. The valid range is 1 - 454. The default is 0.

Name : The name for the EVC.

VID : The VLAN ID in the PB network. It may be inserted in a C-tag, S-tag or S-custom tag depending on the NNI port VLAN configuration. The valid range is 0 - 4095.

IVID : The Internal/classified VLAN ID in the PB network. The valid range is 1 - 4095.

Learning : The learning mode for the EVC controls whether source MAC addresses are learned for frames matching the EVC. Learning may be disabled if the EVC only includes two UNI/NNI ports. Valid values are:

Enabled: Learning is enabled (MAC addresses are learned).

Disabled: Learning is disabled (MAC addresses are not learned).

MPLS PW IDs : Attach EVC to MPLS Pseudo-Wires.

MPLS PW Split-Horizon IDs : Attach EVC to MPLS split-horizon Pseudo-Wires. Split-horizon is just an attribute saying that traffic received on another non-split-horizon PW cannot be forwarded to this split-horizon PW.

E-Tree Leaf Parameters

Leaf VID : The leaf VLAN ID used in the outer tag for the EVC.

Leaf IVID : The leaf internal classified VLAN ID for the EVC.

Leaf Ports : The list of leaf ports for the EVC.

NNI QoS Map Parameters

HQoS IDs : The list of HQoS entries mapped to the EVC ports and a link to configure the mappings. HQoS (Hierarchical Quality of Service) is a method of QoS that can be configured at a service level.

Ingress Map Mode : The NNI QoS ingress map mode or specific map ID for the EVC.

Disabled: The QoS ingress map mode is disabled for the EVC.

Specific: Specify a specific map ID for the EVC.

Ingress Map ID : Specify a specific map ID for the EVC. The valid range is 0 - 255. The default is 0.

Egress Map Mode : The NNI QoS egress map mode or specific map ID for the EVC.

Disabled: The QoS egress map mode is disabled for the EVC.

Specific: Specify a specific map ID for the EVC.

Egress Map ID : Specify a specific map ID for the EVC. The valid range is 0 - 511. The default is 0.

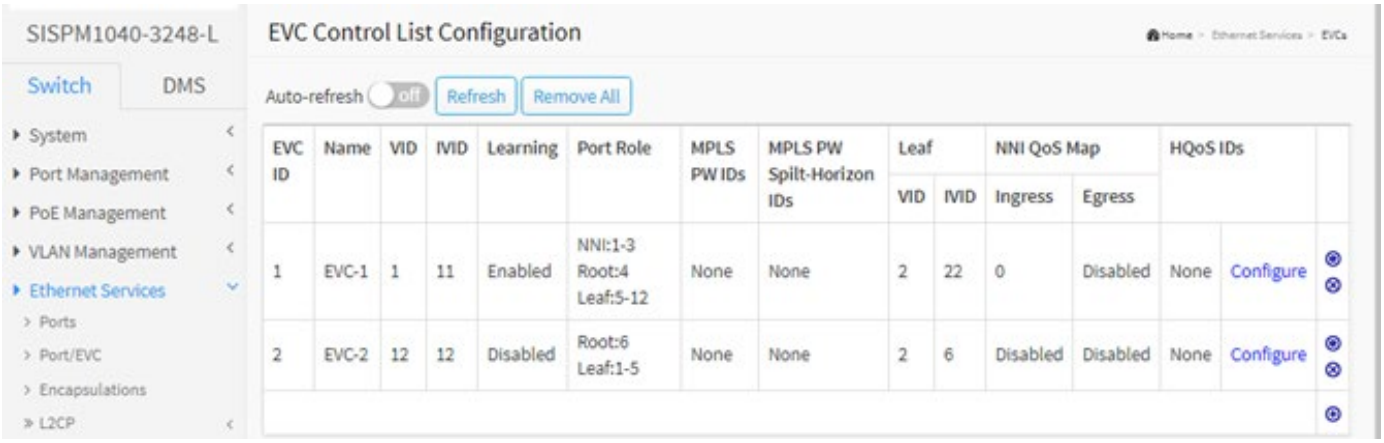
Buttons

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; any changes made locally will be undone.

Example



EVC ID : The EVC ID identifies the EVC. The valid range is 1 - 454.

Name : The name for the EVC.

VID : The VLAN ID in the PB network. It may be inserted in a C-tag, S-tag or S-custom tag depending on the NNI port VLAN configuration. The valid range is 0 - 4095.

IVID : The Internal/classified VLAN ID in the PB network. The valid range is 1 - 4095.

Learning : The learning mode for the EVC controls whether source MAC addresses are learned for frames matching the EVC. Learning may be disabled if the EVC only includes two UNI/NNI ports. The possible values are:

Enabled: Learning is enabled (MAC addresses are learned).

Disabled: Learning is disabled (MAC addresses are not learned).

Port Role : The port role for the EVC (e.g., NNI:3-7 Root:2 Leaf:8-13).

MPLS PW IDs : Attach EVC to MPLS Pseudo-Wires.

MPLS PW Split-Horizon IDs : Attach EVC to MPLS split-horizon Pseudo-Wires. Split-horizon is just an attribute saying that traffic received on another non-split-horizon PW cannot be forwarded to this split-horizon PW.

Leaf VID : The leaf VLAN ID used in the outer tag for the EVC.

Leaf IVID : The leaf internal classified VLAN ID for the EVC.

NNI QoS Ingress Map : The NNI QoS ingress map mode or specific map ID for the EVC.

Disabled: The QoS ingress map mode is disabled for the EVC.

Specific: The range is 0 - 255.

NNI QoS Egress Map : The NNI QoS egress map mode or specific map ID for the EVC.

Disabled: The QoS egress map mode is disabled for the EVC.

Specific: The valid range is 0 - 511.

Leaf Ports : The list of leaf ports for the EVC.

HQoS IDs : The list of HQoS entries mapped to the EVC ports and a link to configure the mappings.

Configure : Click the linked Configure text in the 'HQoS IDs' column to display the HQoS Configuration for EVC page as shown and described below. This page lets you view and configure current EVC HQoS mappings for the port.
HQoS (Hierarchical Quality of Service) is a method of QoS that can be configured at a service level.

Modification Buttons

You can modify EVCs in the table using these buttons:

 : Edit the EVC row.

 : Delete the EVC.

 : Add a new EVC.

Buttons

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

Refresh : : Click to manually refresh the page immediately.

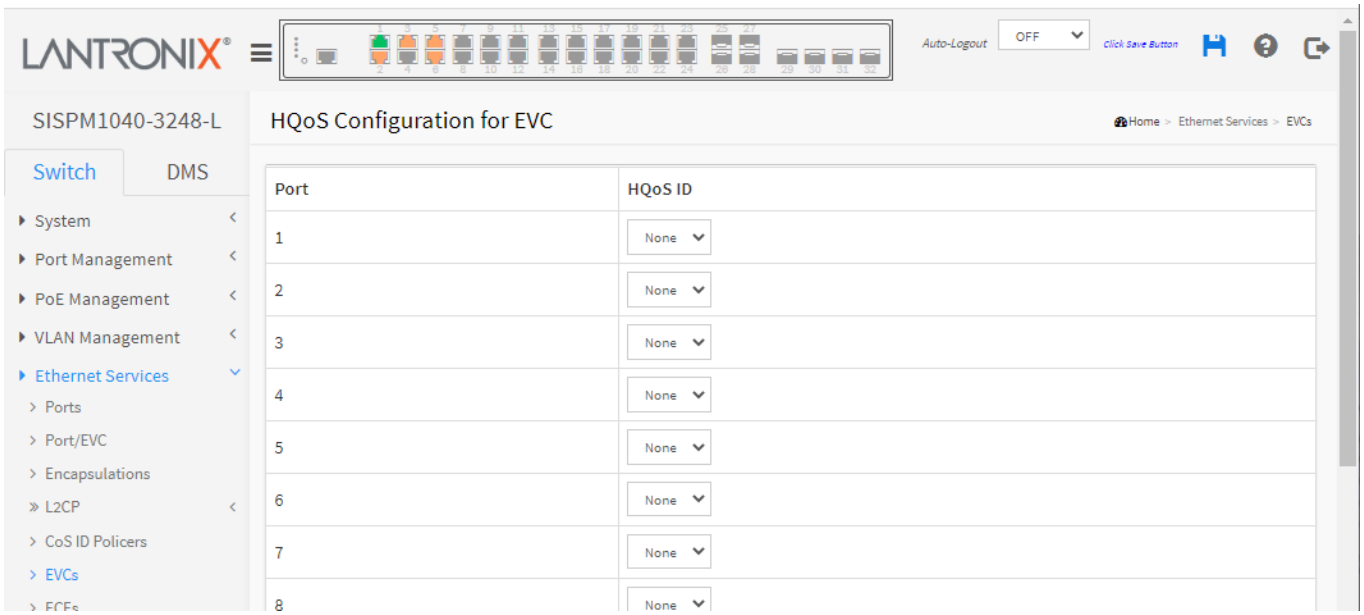
Remove All : Click to remove all EVCs.

HQoS Configuration for EVC

Click the linked Configure text in the 'HQoS IDs' column to display the HQoS Configuration for EVC page as shown and described below. This page lets you view and configure current EVC HQoS mappings for the port.

HQoS (Hierarchical Quality of Service) is a method of QoS that can be configured at a service level. HQoS IDs list the HQoS entries mapped to the EVC ports and a link to configure the mappings.

This page displays lets you view and configure current EVC HQoS mappings for the port.



Parameter descriptions:

Port : The EVC port.

HQoS ID : The mapped HQoS ID or None if the EVC port is mapped to Non-service.

Buttons

Apply : Click to save changes.

Cancel : Return to the previous page; any changes made locally will be undone.

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

7-8 ECE Configuration

This page lets you view and configure current EVC Control Entries (ECEs) from the Switch > Ethernet Services > ECEs menu path. An EVC Control Entry provides rules that are ordered in a list to control the preferred classification.

From the default ECE Control List Configuration page, click the add ECE icon (⊕) to display the EVC Configuration page and add new EVCs as shown and described below.

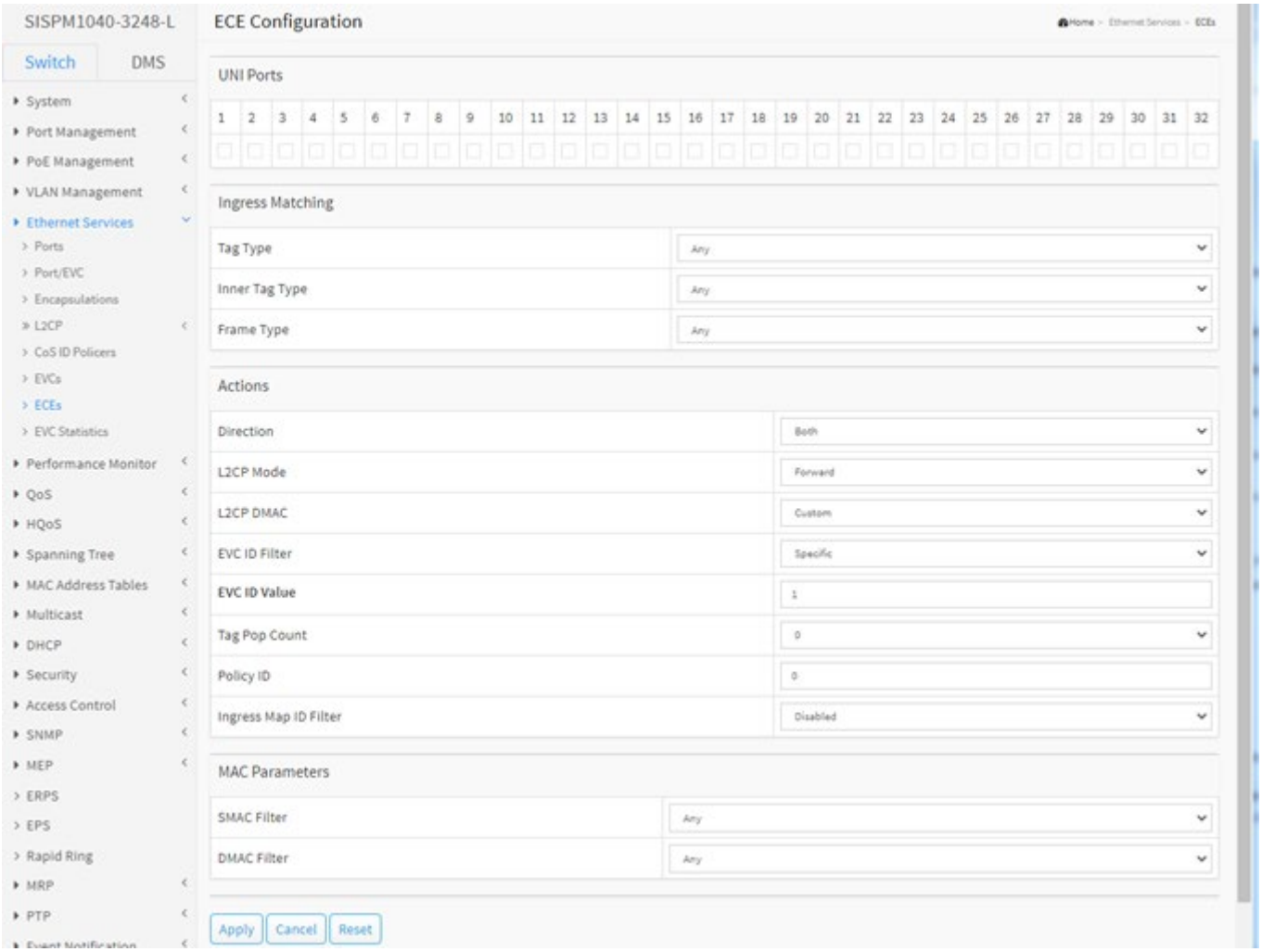


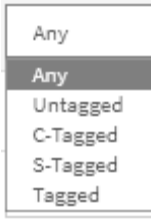
Figure 7-8: ECE Configuration

Parameter descriptions:

UNI Ports : The list of User Network Interfaces for the ECE.

Ingress Matching

Tag Type : The tag type for matching the ECE. Valid values are:



Any: The ECE will match both tagged and untagged frames.

Untagged: The ECE will match untagged frames only.

C-Tagged: The ECE will match custom tagged frames only.

S-Tagged: The ECE will match service tagged frames only.

Tagged: The ECE will match tagged frames only.

VLAN ID Filter : The VLAN ID filter for matching the ECE. It only significant if tag type 'Tagged' is selected. Valid values are:

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 value with this ECE, choose this value. A field for entering a specific value displays.

Range: If you want to filter a specific VLAN ID range filter with this ECE, choose this value. A field for entering a range displays.

VLAN ID Value : When "Specific" is selected for the VLAN ID filter, you can enter a specific value. Valid values are 0 - 4095.

VLAN ID Range : When "Range" is selected for the VLAN ID filter, you can enter a specific range. The valid range is 0 - 4095.

PCP : The PCP value for matching the ECE. It only significant if tag type 'Tagged' is selected. Valid values are:

Any: The ECE will match any PCP value.

Specific: The ECE will match a specific PCP in the range 0 through 7.

Range: The ECE will match PCP values in the selected range 0-1, 2-3, 4-5, 6-7, 0-3 or 4-7.

DEI : The DEI value for matching the ECE. It only significant if tag type 'Tagged' is selected. Valid values are 0, 1 or Any.

Inner Tag Type : The inner tag type for matching the ECE. Valid values are:

Any: The ECE will match both tagged and untagged frames.

Tagged: The ECE will match tagged frames only.

C-Tagged: The ECE will match custom tagged frames only.

S-Tagged: The ECE will match service tagged frames only.

Untagged: The ECE will match untagged frames only.

Inner VLAN ID Filter : The inner VLAN ID filter for matching the ECE. It only significant if tag type 'Tagged' is selected. Valid values are:

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

Specific: If you want to filter a specific inner VLAN ID value with this ECE, choose this value. A field for entering a specific value displays.

Range: If you want to filter a specific inner VLAN ID range filter with this ECE, choose this value. A field for entering a range appears.

Inner VLAN ID Value : When "Specific" is selected for the VLAN ID filter, you can enter a specific value. Valid values are 0 - 4095.

Inner VLAN ID Range : When "Range" is selected for the VLAN ID filter, you can enter a specific range. The valid range is 0 - 4095.

Inner Tag PCP : The inner PCP value for matching the ECE. It only significant if inner tag type 'Tagged' is selected. Valid values are:

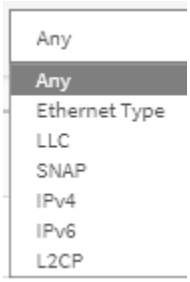
Any: The ECE will match any PCP value.

Range: The ECE will match PCP values in the selected range 0-1, 2-3, 4-5, 6-7, 0-3 or 4-7.

Specific: The ECE will match a specific PCP in the range 0 through 7.

Inner Tag DEI : The inner DEI value for matching the ECE. It only significant if inner tag type 'Tagged' is selected. The allowed value is: 0, 1 or Any.

Frame Type : The frame type for the ECE. Changing this parameter will change the set of parameters displayed on the page. Valid values are:



Any: The ECE will match any frame type.

***Ethernet Type*:** The ECE will match Ethernet Type frames only.

LLC: The ECE will match LLC frames only.

SNAP: The ECE will match SNAP frames only.

IPv4: The ECE will match IPv4 frames only.

IPv6: The ECE will match IPv6 frames only.

L2CP: The ECE will match Layer 2 Control Protocol frames only.

MAC Parameters

SMAC Filter : The source MAC address for matching the ECE. Valid values are:

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

Specific: If you want to filter a specific SMAC value with this ECE, choose this value. A field for entering a specific value displays.

SMAC Value : When "Specific" is selected for the SMAC filter, you can enter a specific value. The legal format is "xx-xx-xx-xx-xx-xx" or "xx.xx.xx.xx.xx.xx" or "xxxxxxxxxxxx" (x is a hexadecimal digit).

DMAC Type : The destination MAC address type for matching the ECE. Valid values are:

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

Unicast: Frame must be unicast.

Multicast: Frame must be multicast.

Broadcast: Frame must be broadcast.

DMAC Filter : The destination MAC address for matching the ECE. Valid values are:

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

Unicast: Frame must be unicast.

Multicast: Frame must be multicast.

Broadcast: Frame must be broadcast.

Specific: If you want to filter a specific DMAC value with this ECE, choose this value. A field for entering a specific value displays.

DMAC Value : When "Specific" is selected for the DMAC filter, you can enter a specific value. The legal format is "xx-xx-xx-xx-xx-xx" or "xx.xx.xx.xx.xx.xx" or "xxxxxxxxxxxx" (where x is a hexadecimal digit).

Ethernet Type Parameters

Ethernet Type Value Filter : The Ethernet type value for matching the ECE. Valid values are:

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

Specific: If you want to filter a specific Ethernet type value with this ECE, choose this value. A field for entering a specific value displays.

Ethernet Type Value : When "Specific" is selected for the Ethernet type filter, you can enter a specific value. Valid values are 0x600 - 0xFFFF but exclude 0x0800 (IPv4), 0x806 (ARP) and 0x86DD (IPv6).

Ethernet Type Data Filter : The Ethernet type data for matching the ECE. Valid values are:

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

Specific: If you want to filter a specific Ethernet type value with this ECE, choose this value. Two fields for entering a specific Ethernet type data and data mask display.

Ethernet Type Data : When "Specific" is selected for the Ethernet type data filter, you can enter a specific value. It a pair of the Ethernet type data and its mask. Valid values are 0x0 - 0xFFFF.

Ethernet Type Data Mask : When "Specific" is selected for the Ethernet type data filter, you can enter a specific mask. Valid values are 0x0 to 0xFFFF.

LLC Parameters

LLC DSAP Filter : The LLC DSAP for matching the ECE. Valid values are:

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

Specific: If you want to filter a specific LLC DSAP value with this ECE, choose this value. A field for entering a specific value displays.

LLC DSAP Value : When "Specific" is selected for the LLC DSAP filter, you can enter a specific value. Valid values are 0x0 through 0xFF.

LLC SSAP Filter : The LLC SSAP for matching the ECE. Valid values are:

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

Specific: If you want to filter a specific LLC SSAP value with this ECE, choose this value. A field for entering a specific value displays.

LLC SSAP Value : When "Specific" is selected for the LLC SSAP filter, you can enter a specific value. Valid values are 0x0 - 0xFF.

LLC Control Filter : The LLC control for matching the ECE. Valid values are:

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

Specific: If you want to filter a specific LLC control value with this ECE, choose this value. A field for entering a specific value displays.

LLC Control Value : When "Specific" is selected for the LLC control filter, you can enter a specific value. Valid values are 0x0 - 0xFF.

LLC Data Filter : The LLC data for matching the ECE. Valid values are:

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

Specific: If you want to filter a specific LLC value with this ECE, choose this value. Two fields for entering a specific Ethernet type data and data mask appears.

LLC Data : When "Specific" is selected for the LLC data filter, you can enter a specific value. It a pairing of the LLC data and its mask. Valid values are 0x0 to 0xFFFF.

LLC Data Mask : When "Specific" is selected for the LLC data filter, you can enter a specific mask. Valid values are 0x0 - 0xFFFF.

SNAP Parameters

SNAP OUI Filter : The SNAP OUI for matching the ECE. Valid values are:

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

Specific: If you want to filter a specific SNAP OUI value with this ECE, choose this value. A field for entering a specific value displays.

SNAP OUI Value : When "Specific" is selected for the SNAP OUI filter, you can enter a specific value. Valid values are 00-00-00 to FF-FF-FF.

SNAP PID Filter : The SNAP PID for matching the ECE. Valid values are:

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

Specific: If you want to filter a specific SNAP PID value with this ECE, choose this value. A field for entering a specific value displays.

SNAP PID Value : When "Specific" is selected for the SNAP PID filter, you can enter a specific value. Valid values are 0x0 - 0xFFFF.

IP Parameters

Protocol Filter : The IP protocol for matching the ECE. Valid values are:

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

UDP: Specify the UDP for matching the ECE.

TCP: Specify the TCP for matching the ECE.

Specific: If you want to filter a specific protocol value with this ECE, choose this value. A field for entering a specific value displays.

Protocol Value : When "Specific" is selected for the protocol filter, you can enter a specific value. Valid values are 0 - 255.

SIP Filter : The source IP address for matching the ECE. Valid values are:

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

Host: When "IPv4" is selected for the Frame Type, if you want to filter a specific host address with this ECE, choose this value. A field for entering a host address displays.

Network: When "IPv4" is selected for the Frame Type, if you want to filter a specific network address with this ECE, choose this value. Two fields for entering a specific network address and network mask appears.

Specific: When "IPv6" is selected for the Frame Type, if you want to filter a specific network address with this ECE, choose this value. Two fields for entering a specific network address and network mask display.

SIP Address : When "Host" or "Network" is selected for the SIP filter, you can enter a specific host or network address. When "IPv6" is selected for the Frame Type, the field only supported 32 bits for IPv6 address.

SIP Mask : When "Host" or "Network" is selected for the SIP filter, you can enter a specific network mask. When "IPv6" is selected for the Frame Type, the field only supported 32 bits for IPv6 address mask.

DIP Filter : The destination IP address for matching the ECE. Valid values are:

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

Host: When "IPv4" is selected for the Frame Type, if you want to filter a specific host address with this ECE, choose this value. A field for entering a host address appears.

Network: When "IPv4" is selected for the Frame Type, if you want to filter a specific network address with this ECE, choose this value. Two fields for entering a specific network address and network mask appears.

Specific: When "IPv6" is selected for the Frame Type, if you want to filter a specific network address with this ECE, choose this value. Two fields for entering a specific network address and network mask appears.

DIP Address : When "IPv4" is selected for the Frame Type and "Host" or "Network" is selected for the DIP filter, you can enter a specific host or network address. When "IPv6" is selected for the Frame Type, the field only supported 32 bits for IPv6 address.

DIP Mask : When "IPv4" is selected for the Frame Type and "Host" or "Network" is selected for the DIP filter, you can enter a specific network mask. When "IPv6" is selected for the Frame Type, the field only supported 32 bits for IPv6 address mask.

DSCP Filter : The DSCP filter for matching the ECE. Valid values are:

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

Specific: If you want to filter a specific DSCP value with this ECE, choose this value. A field for entering a specific value displays.

Range: If you want to filter a specific DSCP range filter with this ECE, choose this value. A field for entering a range displays.

DSCP Value : When "Specific" is selected for the DSCP filter, you can enter a specific value. Valid values are 0 - 63.

DSCP Range : When "Range" is selected for the DSCP filter, you can enter a specific range. Valid values are 0 - 63.

Fragment : The IPv4 Fragment for matching the ECE. This involves the settings for the More Fragments (MF) bit and the Fragment Offset (FRAG OFFSET) field for an IPv4 frame. Valid values are:

Any: The ECE will match any MF bit.

Non-Fragment: 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.

Fragment: IPv4 frames where the MF bit is set or the FRAG OFFSET field is greater than zero must be able to match this entry.

L2CP Parameters

L2CP Type : The L2CP type for the ECE. Valid values are:

STP/RSTP/MSTP: Match STP/RSTP/MSTP frames (default). The destination MAC address is 01-80-C2-00-00-00, LLC value 0x42/0x42 and protocol ID 0x0000.

Pause: Match Pause frames. The destination MAC address is 01-80-C2-00-00-01, Ethernet type value 0x8808.

LACP: Match LACP frames. The destination MAC address is 01-80-C2-00-00-02, Ethernet type 0x8809 and protocol ID 0x01.

LAMP: Match LAMP frames. The destination MAC address is 01-80-C2-00-00-02, Ethernet type 0x8809 and protocol ID 0x02.

Link OAM(802.1ah): Match Link OAM(802.1ah) frames. The destination MAC address is 01-80-C2-00-00-02, Ethernet type 0x8809 and protocol ID 0x03.

Port Authentication(802.1x): Match Port Authentication(802.1x) frames. The destination MAC address is 01-80-C2-00-00-03, Ethernet type 0x888E.

E-LMI: Match PB Group Address frames. The destination MAC address is 01-80-C2-00-00-07, Ethernet type 0x88EE.

PB Group Address: Match PB Group Address frames. The destination MAC address is 01-80-C2-00-00-08, LLC value 0x42/0x42 and protocol ID 0x0000.

***PB GVRP*:** Match PB GVRP frames. The destination MAC address is 01-80-C2-00-00-0D, LLC value 0x42/0x42 and protocol ID 0x0001.

LLDP: Match LLDP frames. The destination MAC address is 01-80-C2-00-00-0E, Ethernet type value 0x88CC.

GMRP: Match GMRP frames. The destination MAC address is 01-80-C2-00-00-20, LLC value 0x42/0x42 and protocol ID 0x0001.

GVRP: Match GVRP frames. The destination MAC address is 01-80-C2-00-00-21, LLC value 0x42/0x42 and protocol ID 0x0001.

ULD: Match ULD frames. The destination MAC address is 01-00-0C-CC-CC-CC, SNAP value 0x00000C and protocol ID 0x0111.

PAgP: Match PAgP frames. The destination MAC address is 01-00-0C-CC-CC-CC, SNAP value 0x00000C and protocol ID 0x0104.

PVST/PVST+: Match PVST/PVST+ frames. The destination MAC address is 01-00-0C-CC-CC-CD, SNAP value 0x00000C and protocol ID 0x010B.

***Cisco BPDU*:** Match Cisco BPDU frames. The destination MAC address is 01-00-0C-CC-CC-CE, SNAP value 0x00000C and protocol ID 0x010C.

CDP: Match CDP frames. The destination MAC address is 01-00-0C-CC-CC-CC, SNAP value 0x00000C and protocol ID 0x2000.

VTP: Match VTP frames. The destination MAC address is 01-00-0C-CC-CC-CC, SNAP value 0x00000C and protocol ID 0x2003.

DTP: Match DTP frames. The destination MAC address is 01-00-0C-CC-CC-CC, SNAP value 0x00000C and protocol ID 0x2004.

STP Uplink Fast: Match STP Uplink Fast frames. The destination MAC address is 01-00-0C-CD-CD-CD, SNAP value 0x00000C and protocol ID 0x200A.

Cisco CFM: Match Cisco CFM frames. The destination MAC address is 01-00-0C-CC-CC-C3, SNAP value 0x00000C and protocol ID 0x0126.

Actions

Direction : The EVCs and ECEs are used to setup flows in one or both directions as determined by the ECE Direction parameter. If the ECE is bidirectional, the ingress rules of the NNI ports will be setup to match the traffic being forwarded to NNI ports. Valid values are:

Both: Bidirectional.

UNI-to-NNI: Unidirectional from UNI to NNI.

NNI-to-UNI: Unidirectional from NNI to UNI.

L2CP Mode : The L2CP mode for the ECE. Valid values are:

Forward: Forward with unchanged DMAC.

Tunnel: Forward EType/LLC/SNAP frame and replace DMAC.

Discard: Drop frame.

Peer: Process frame by local protocol entity.

L2CP DMAC : The L2CP destination MAC for the ECE. Valid values are:

Custom: The L2CP destination MAC address is based on IEEE L2CP MAC addresses (01-01-C1-00-00-XX).

Cisco: The L2CP destination MAC address is based on Cisco L2CP MAC address (01-00-0C-CD-CD-D0).

EVC ID Filter : The EVC ID for the ECE. The ECE is only active when mapping to an existing EVC. Valid values are:

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

Specific: If you want to filter a specific EVC ID with this ECE, choose this value. A field for entering a specific value displays.

EVC ID Value : When "Specific" is selected for the VLAN ID filter, you can enter a specific value. Valid values are 1 - 454.

Tag Pop Count : The ingress tag pop count for the ECE. The valid range is 0 - 2.

Policy ID : The ACL Policy ID for the ECE for matching ACL rules. The valid range is 0 - 127.

Ingress Map ID Filter : The QoS ingress map ID for the ECE. Valid values are:

Disabled: The QoS ingress map mode is disabled for the ECE.

Specific: If you want to filter a specific ingress map ID with this ECE, choose this value. A field for entering a specific value displays.

Ingress Map ID Value : When "Specific" is selected for the Ingress Map ID filter, you can enter a specific value. The valid range is 0 - 255.

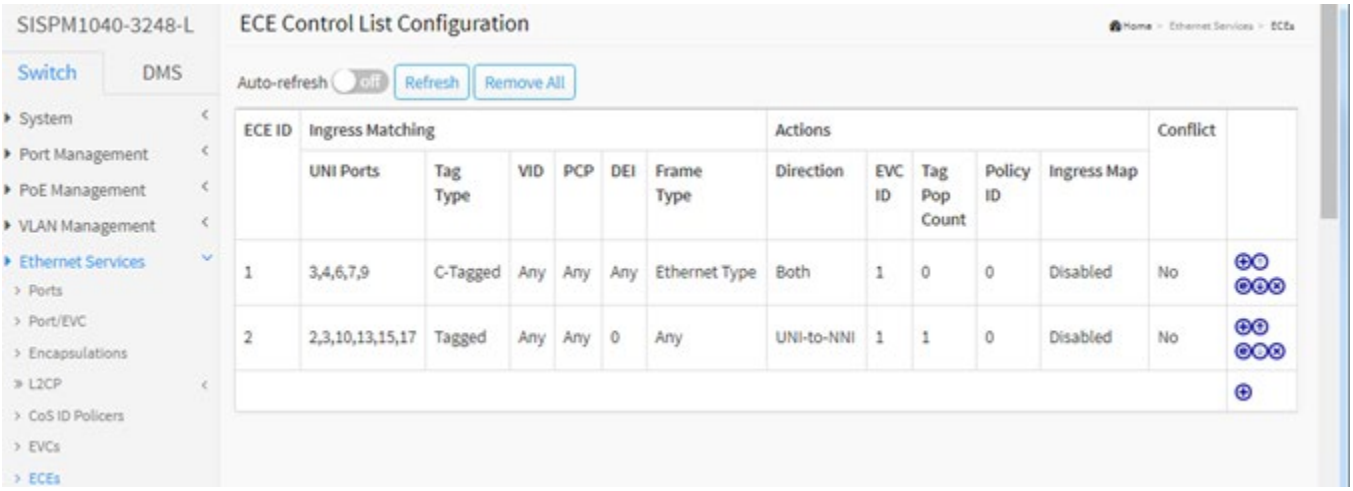
Buttons

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; any changes made locally will be undone.

Example



Modification Buttons

You can modify each ECE (EVC Control Entry) in the table using the following buttons:

: Inserts a new ECE before the current row.

: Edits the ECE row.

: Moves the ECE up the list.

: Moves the ECE down the list.

: Deletes the ECE.

: The lowest plus sign adds a new entry at the bottom of the ECE listings.

7-9 EVC Statistics

This page displays NNI port traffic statistics for the selected EVC. It also displays counters for UNI ports of ECEs mapping to the EVC.

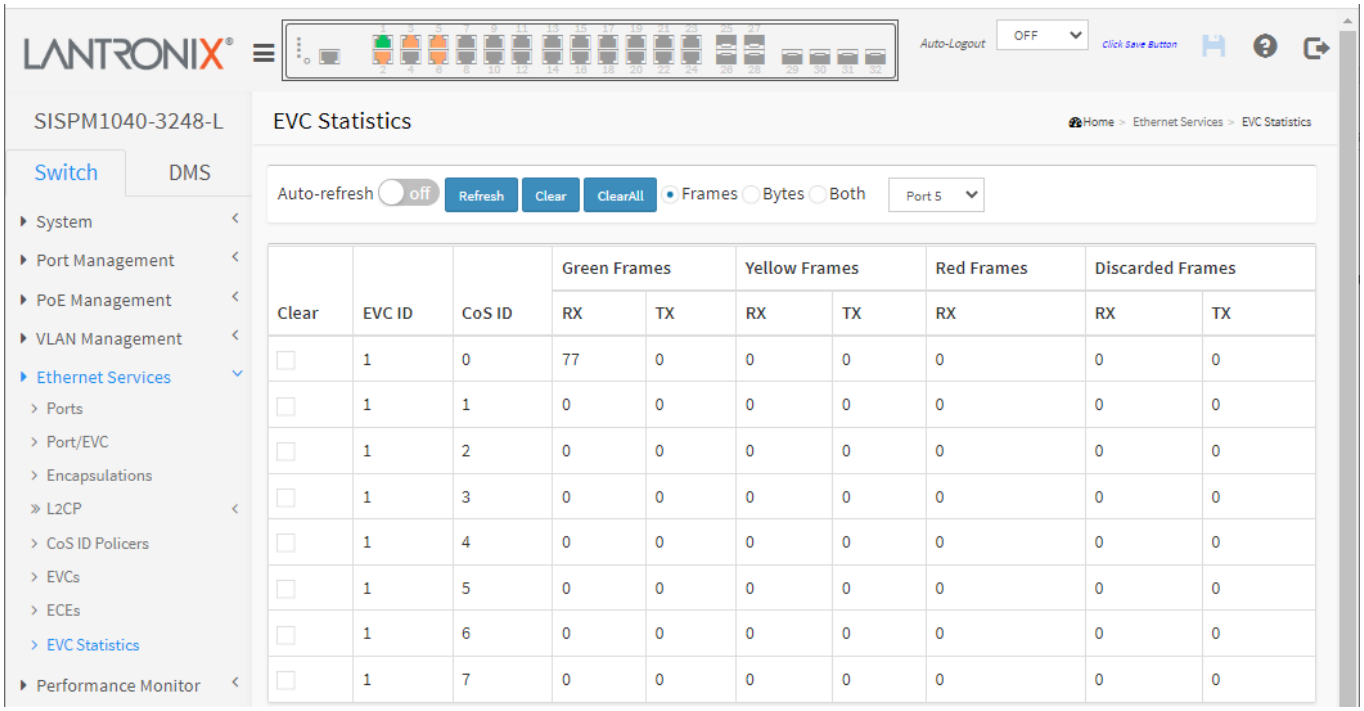


Figure 7-9: EVC Statistics

Parameter descriptions:

Clear : This box is used to mark a entry for clearance in next Clear operation.

EVC ID : The EVC ID.

CoS ID : The CoS (Class of Service) ID for the EVC.

Rx Green : The number of green frames received.

Tx Green : The number of green frames transmitted.

Rx Yellow : The number of yellow frames received.

Tx Yellow : The number of yellow frames transmitted.

Rx Red : The number of red frames received.

Rx Discarded : The number of discarded frames in the ingress queue system.

Tx Discarded : The number of frames discarded in the egress queue system.

Buttons

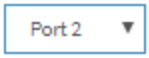
Auto-refresh: Check this box to refresh the page automatically every 3 seconds.

Refresh : Click to manually refresh the page immediately.

Clear : Clears the counters for selected ports.

Clear All : Clears the counters for all ports.

- **Frames**: Show frames statistics only.
- **Bytes**: Show bytes statistics only.
- **Both**: Show both frames and bytes statistics.



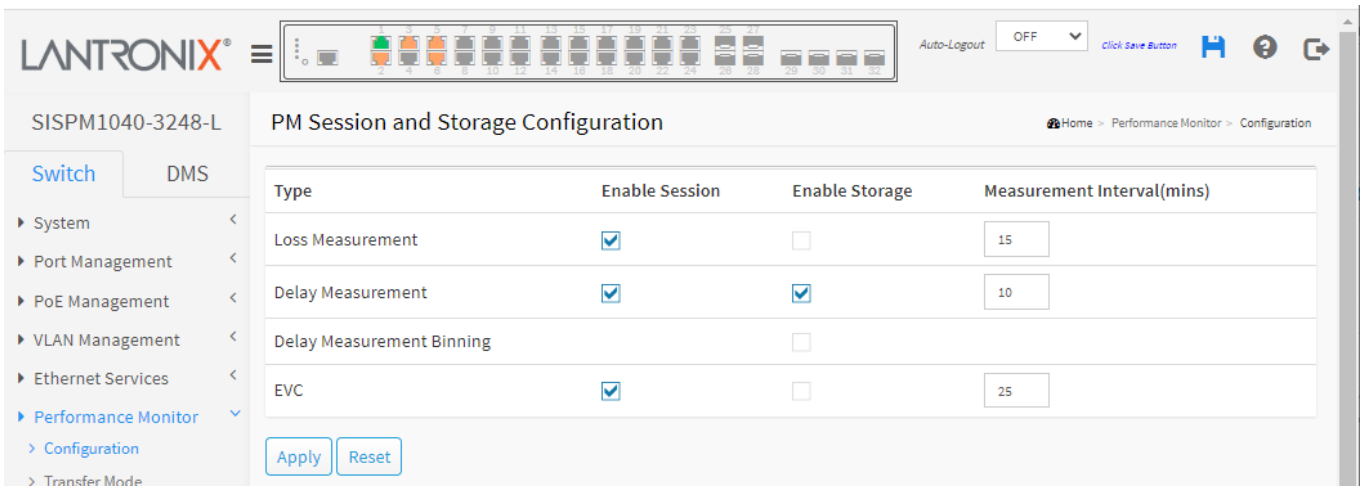
: The port select box lets you select which port to display on the page.

Chapter 8 – Performance Monitor

The switch supports the OAM (Operation Administration and Maintenance) protocol described in ITU-T Y.1731 used to implement carrier Ethernet functionality. MEP functionality like CC and RDI is based on this.

8-1 PM Session and Storage Configuration

This page lets you view and configure current Performance Monitor parameters.



PM Session and Storage Configuration

Parameter descriptions:

Type : The data type of performance monitor (Loss Measurement, Delay Measurement, Delay Measurement Binning, and EVC).

Enable Session : Enable or disable the performance monitor session.

Enable Storage : Enable or disable performance monitor storage.

Measurement Interval(mins) : The measurement interval for the performance monitor (1 – 60 seconds). The default is 15 minutes.

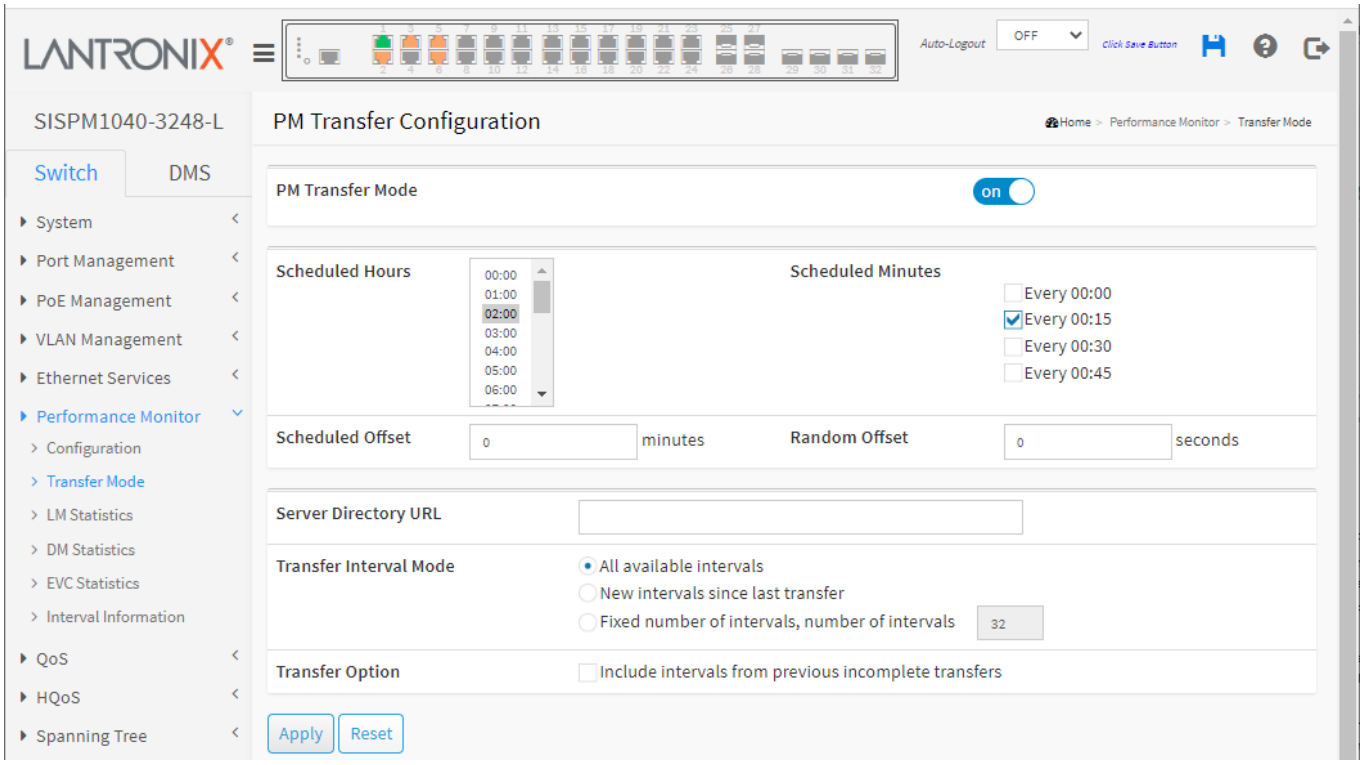
Buttons

Apply : Click to save changes.

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

8-2 PM Transfer Configuration

This page lets you view and configure current PM Transfer parameters.



PM Transfer Configuration

Parameter descriptions:

PM Transfer Mode : click to turn the Performance Monitor Transfer function on or off globally. The default is off.

Scheduled Hours : Select one or more of the 24 hours in a day, when PM data transfer will happen.
The selections are in one hour increments from 00:00 to 23:00. The default is none selected.

Scheduled Minutes : Select one or more of the four 15 minutes in an hour, when PM data transfer will happen.
The selections are 00:00, 00:15, 00:30, or 00:45. The default is none selected.

Scheduled Offset : Enter a fixed offset that is added to the scheduled transfer time. The range is 0-15 minutes. The default is 0 minutes. **Note**: The sum of Scheduled Fixed Offset and Scheduled Random Offset must not exceed 15 minutes.

Random Offset : It is possible to configure a random offset that is added to the scheduled transfer time.
The offset added to the scheduled transfer time must be a random value in the range 0-Scheduled Offset.
The range is 0-900 seconds. The default is 0 seconds. **Note**: The sum of Scheduled Offset and Random Offset must not exceed 15 min.

Server Directory URL : It is possible to configure the full URL of the server and the corresponding directory (if any) for uploading. The supported protocols are HTTP and TFTP.

To enable ***HTTP*** enter http:// followed by the domain name or IP address.

To enable ***TFTP*** enter tftp:// followed by the domain name or IP address.

Transfer Interval Mode: There are three supported interval modes.

All available intervals: To enable transfer of all completed Measurement Intervals.

New intervals since last transfer: To enable transfer of only completed Measurement Intervals since last transfer.

Fixed number of intervals: To enable transfer of all completed Measurement Intervals up to the configured number.

Number of intervals: When Fixed number of interval selected, this value is used to determine the number of intervals to send. The range is 1 to 96 Intervals.

Transfer Option: When this checkbox (*Include intervals from previous incomplete transfers*) is checked, PM data transfer will include the suspended (incomplete) transmission.

Buttons

Apply : Click to save changes.

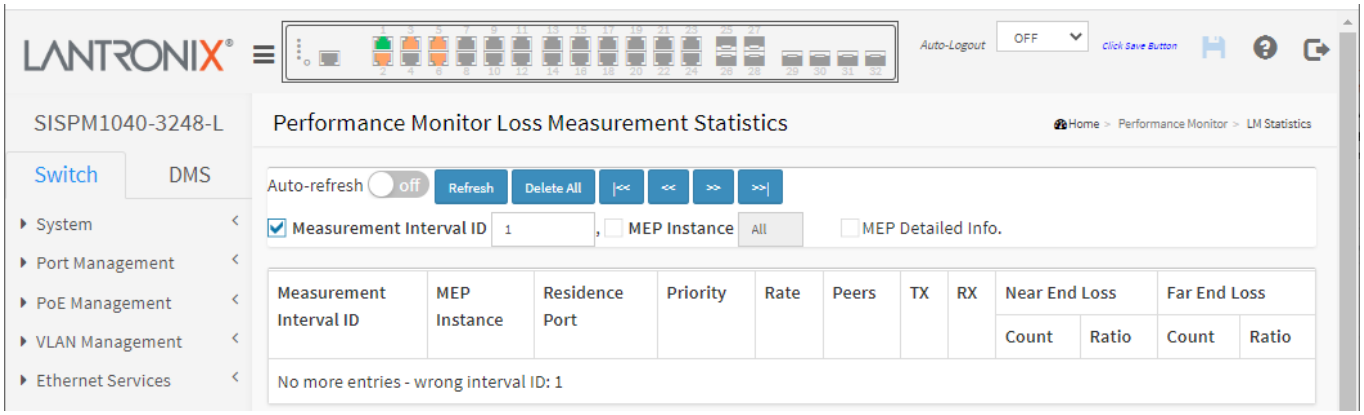
Reset : Click to undo any changes made locally and revert to previously saved values.

Messages

The 'URL' is restricted to protocol 'http' or 'tftp'

8-3 Performance Monitor Loss Measurement Statistics

This page lets you view current Performance Monitor Loss Measurement Statistics from the Switch > Performance Monitor > LM Statistics menu path. This page provides the performance monitor loss measurement traffic statistics for the selected measurement interval ID and Loss Measurement instance.



Performance Monitor Loss Measurement Statistics (without MEP Detailed Info.)

Parameter descriptions:

Measurement Interval ID : The measurement interval for the performance monitor data sets. The 'Measurement Interval ID' must be an integer value between 1 and 4294967295.

MEP Instance : The MEP instance for the performance monitor data sets.

Residence Port : The residence port for the MEP.

Priority : The priority to be inserted as PCP bits in TAG (if any).

Rate : Selected the frame rate of CCM/LMM PDU. This is the inverse of transmission period as described in Y.1731.

TX : The number of frame transmitted.

RX : The number of frame received.

Near End Loss Count : The near end loss count.

Near End Loss Ratio : The near end loss ratio.

Far End Loss Count : The far end loss count.

Far End Loss Ratio : The far end loss ratio.

Domain : Port: This is a MEP in the Port Domain. 'Flow Instance' is a Port.

Evc: This is a MEP in the EVC Domain. 'Flow Instance' is a EVC.

VLAN: This is a MEP in the VLAN Domain. 'Flow Instance' is a VLAN.

Direction : The MEP direction (Up MEP or Down MEP):

Up: This is a Down MEP - monitoring ingress OAM and traffic on 'Residence Port'.

Down: This is a Up MEP - monitoring egress OAM and traffic on 'Residence Port'.

Level : The MEG level of this MEP.

Flow Instance : The MEP is related to this flow - See 'Domain'.

Tagged VID : Port MEP: An outer C/S-tag (depending on VLAN Port Type) is added with this VID. Entering '0' means no TAG added.

EVC MIP: On Serval, this is the Subscriber VID that identifies the subscriber flow in this EVC where the MIP is active.

MEP ID : This value will become the transmitted two byte CCM MEP ID.

MAC Address : The MAC of this MEP - can be used by other MEP when unicast is selected (Info only).

Peer MEP ID : This value will become an expected MEP ID in a received CCM - see 'cMEP'.

Peer MAC Address : This MAC will be used when unicast is selected with this peer MEP. Also, this MAC is used to create HW checking of receiving CCM PDU (LOC detection) from this MEP.

Buttons

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

Refresh : Click to manually refresh the page immediately.

Delete All : Delete all table entries.

|<< : Updates the table entries, starting from the first available entry.

<< : Updates the table entries, ending at the last entry currently displayed.

>> : Updates the table entries, starting from the last entry currently displayed.

>>| : Updates the table entries, ending at the last available entry.

Measurement Interval ID: Check this box to select a specific interval ID, otherwise to select all the intervals.

MEP Instance: Check this box to select a specific MEP instance, otherwise to select all the MEP instances.

MEP Detailed Info. : Check the box to display additional MEP details in the table.

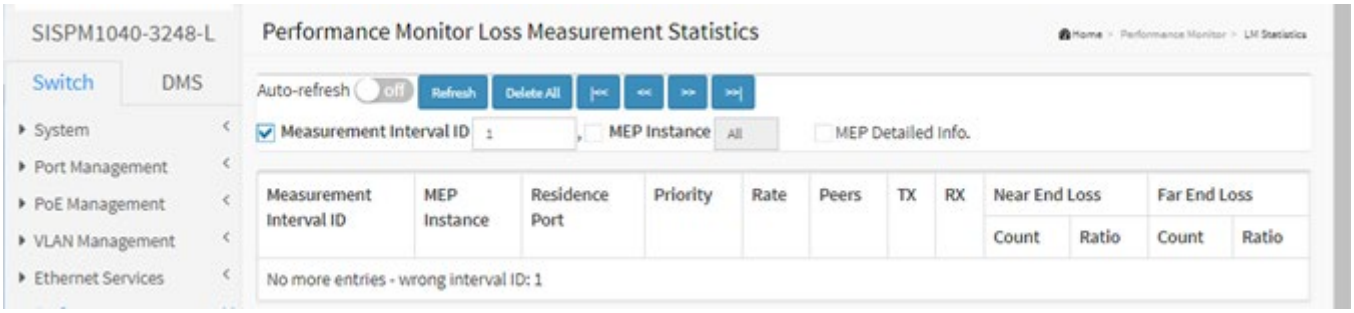
Messages

Message: *No more entries - wrong interval ID: 1*

Meaning: The entry has not been created yet.

8-4 Performance Monitor Delay Measurement Statistics

This page lets you view current PM delay measurement statistics from the Switch > Performance Monitor > LM Statistics menu path. This page provides the performance monitor delay measurement traffic statistics for the selected measurement interval ID and Delay Measurement instance.



Performance Monitor Delay Measurement Statistics (without MEP Detailed Info)

Parameter descriptions:

Measurement Interval ID : The measurement interval for the performance monitor data sets.

MEP Instance : The MEP instance for the performance monitor data sets.

Residence Port : The residence port for the MEP.

Priority : The priority to be inserted as PCP bits in TAG (if any).

Rate : The gap between transmitting 1DM/DMM PDU in 10ms. The range is 10 to 65535.

Unit : The time resolution.

TX : The number of frame transmitted.

RX : The number of frame received.

One-way Far to Near Average Delay : The one-way far to near average delay.

One-way Far to Near Average Delay Variation : The one-way far to near average delay variation.

One-way Far to Near Min. Delay : The minimum one-way near to far delay.

One-way Far to Near Max. Delay : The maximum one-way near to far delay.

One-way Near to Far Average Delay : The number of red received.

One-way Near to Far Average Delay Variation : The one-way near to far average delay variation.

One-way Near to Far Min. Delay. : The minimum one-way near to far delay.

One-way Near to Far Max. Delay. : The maximum one-way near to far delay.

Two-way Delay Average Delay : The two-way average delay.

Two-way Average Delay Variation : The two-way average delay variation.

Two-way Min. Delay : The minimum two-way delay.

Two-way Max. Delay : The maximum two-way delay.

Domain : The MEP domain, either:

Port: This is a MEP in the Port Domain. 'Flow Instance' is a Port.
Evc: This is a MEP in the EVC Domain. 'Flow Instance' is a EVC.
VLAN: This is a MEP in the VLAN Domain. 'Flow Instance' is a VLAN.

Direction : The MEP direction, either:

Up: This is an Up MEP - monitoring ingress OAM and traffic on 'Residence Port'.
Down: This is a Down MEP - monitoring egress OAM and traffic on 'Residence Port'.

Level : The MEG level of this MEP.

Flow Instance : The MEP is related to this flow.

Port: This is a MEP in the Port Domain. 'Flow Instance' is a Port.
Evc: This is a MEP in the EVC Domain. 'Flow Instance' is a EVC.
VLAN: This is a MEP in the VLAN Domain. 'Flow Instance' is a VLAN.

Tagged VID : displays either 'Port MEP' or 'EVC MIP':

Port MEP: An outer C/S-tag (depending on VLAN Port Type) is added with this VID. A '0' means no TAG added.
EVC MIP: On Serval, this is the Subscriber VID that identifies the subscriber flow in this EVC where the MIP is active.

MEP ID : This value will become the transmitted two-byte CCM MEP ID.

MAC Address : The MAC of this MEP; can be used by other MEP when unicast is selected (Info only).

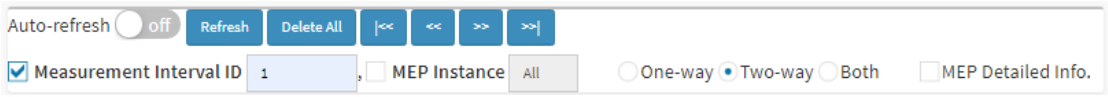
Peer MEP ID : This value will become an expected MEP ID in a received CCM - see 'cMEP'.

Peer MAC Address : This MAC will be used when unicast is selected with this peer MEP. Also this MAC is used to create HW checking of receiving CCM PDU (LOCdetection) from this MEP.

Bin : A Measurement Bin is a counter that stores the number of delay measurements falling within a specified range, during a Measurement Interval. In the example below, the measurement threshold is 5000 usec. and the total number of Measurement Bins is four.

Bin	Threshold	Range
bin0	0 us	0 us <= measurement < 5,000 us
bin1	5,000 us	5,000 us <= measurement < 10,000 us
bin2	10,000 us	10,000 us <= measurement < 15,000 us
bin3	15,000 us	15,000 us <= measurement < infinite us

Buttons



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

Refresh : Click to manually refresh the page immediately.

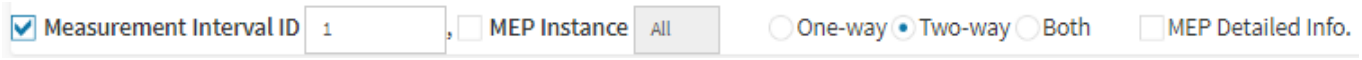
Delete All : Delete all table entries.

|<< : Updates the table entries, starting from the first available entry.

<< : Updates the table entries, ending at the last entry currently displayed.

>> : Updates the table entries, starting from the last entry currently displayed.

>>| : Updates the table entries, ending at the last available entry.

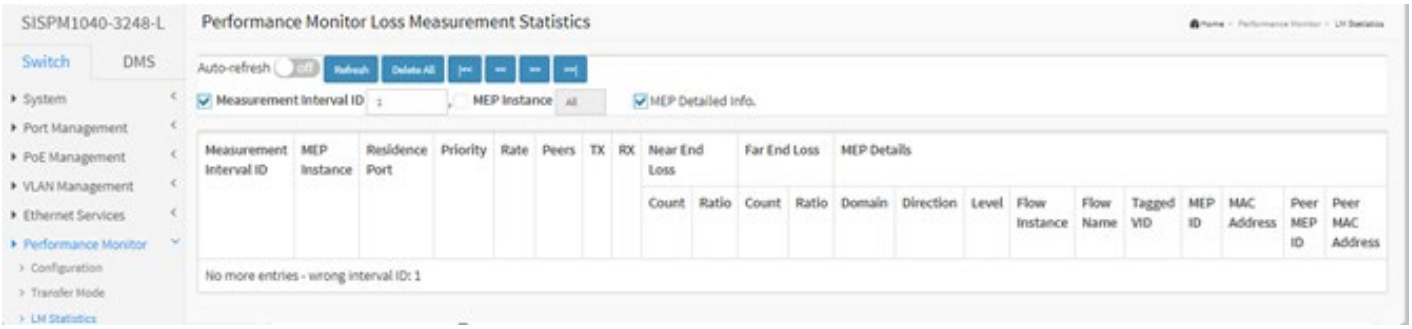


Measurement Interval ID : Check this box to select a specific interval ID, otherwise to select all the intervals.

MEP Instance : Check this box to select a specific MEP instance, otherwise to select all the MEP instances.

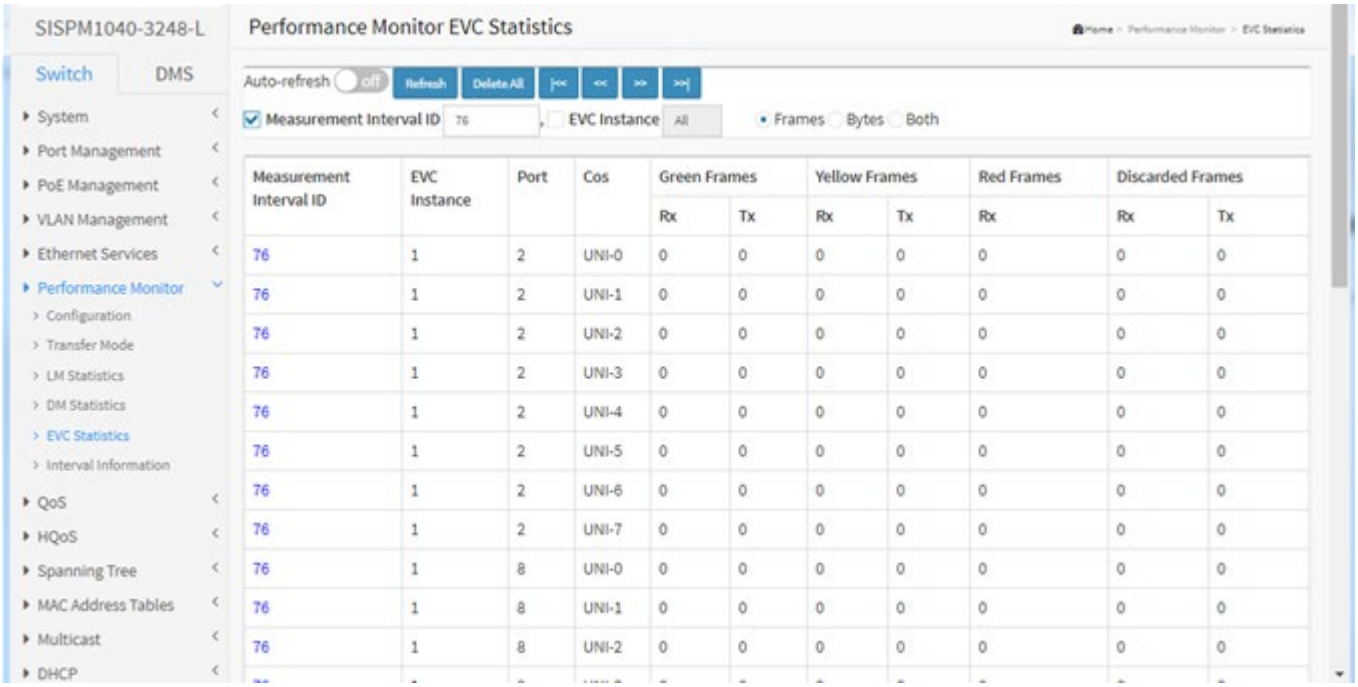
- One-way: Show one-way statistics only.
- Two-way: Show two-way statistics only.
- Both: Show both frames and bytes statistics.

MEP Detailed Info. : Check the MEP Detailed Info checkbox to display additional MEP details in the table:



8-5 Performance Monitor EVC Statistics

This page provides the performance monitor EVC traffic statistics for the selected measurement interval ID and EVC instance from the Switch > Performance Monitor > EVC Statistics menu path.



Performance Monitor EVC Statistics

Parameter descriptions:

Measurement Interval ID : The measurement interval for the performance monitor data sets. Click a linked ID to display its detail page.

EVC Instance : The EVC instance for the performance monitor data sets. 'EVC Instance' must be an integer value between 1 and 454.

MEP Instance : The MEP instance for the performance monitor data sets.

Port : The residence port for the EVC.

Cos : Class of Service, either:

NNI na : this is the NNI port and counters are not per Cos on this port.

UNI 0-7 : this is the UNI port and counters are per Cos on this port.

Rx Green Frames : The number of green frames received.

Tx Green Frames : The number of green frames transmitted.

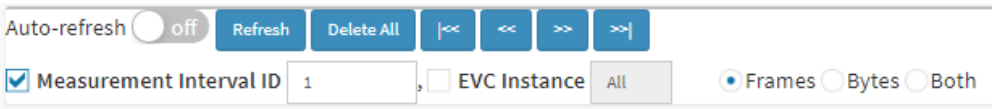
Rx Yellow Frames : The number of yellow frames received.

Tx Yellow Frames : The number of yellow frames transmitted.

Rx Red Frames : The number of red frames received.

Rx Discarded Frames : The number of discarded frames in the ingress queue system.

Tx Discarded Frames : The number of discarded frames in the egress queue system.



Buttons

Measurement Interval ID : Check this box to select a specific interval ID, otherwise to select all the intervals.

EVC Instance : Check this box to select a specific EVC instance, otherwise to select all the EVC instances.

Frames : Show frames statistics only.

Bytes : Show bytes statistics only.

Both : Show both frames and bytes statistics.

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

Refresh : Click to manually refresh the page immediately.

Delete All : Delete all table entries.

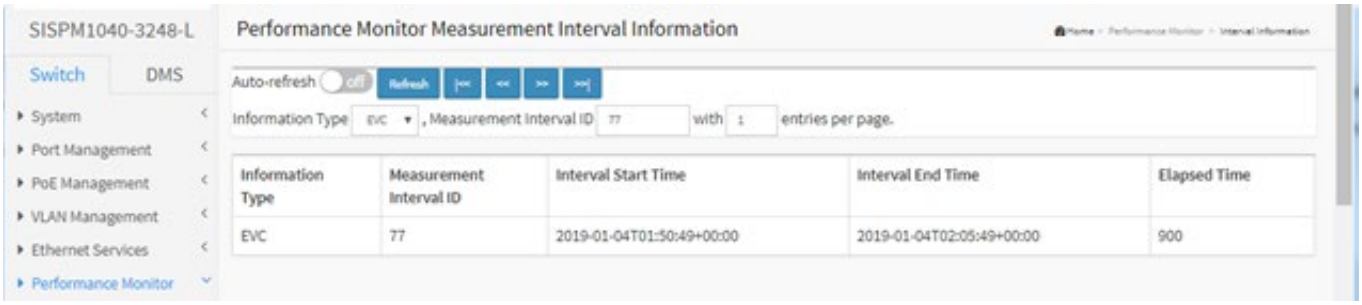
<<| : Updates the table entries, starting from the first available entry.

<< : Updates the table entries, ending at the last entry currently displayed.

>> : Updates the table entries, starting from the last entry currently displayed.

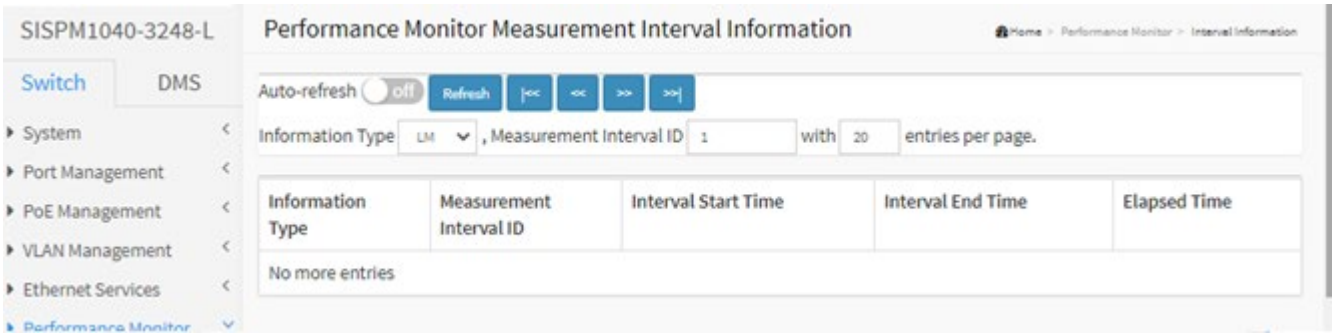
>>| : Updates the table entries, ending at the last available entry.

When you click a linked ID in the **Measurement Interval ID** column, the 'Performance Monitor Measurement Interval Information' page displays as described in the following section.



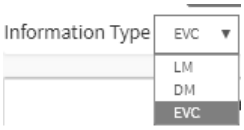
8-6 Performance Monitor Measurement Interval Information

This page provides the performance monitor EVC traffic statistics for the selected measurement interval ID and EVC instance from the Switch > Performance Monitor > Interval Information menu path. You can also click a linked ID in the **Measurement Interval ID** column to display this page.



Performance Monitor Measurement Interval Information

Parameter descriptions:



Information Type : The type for the performance monitor data sets.
At the dropdown select ***LM***, ***DM***, or ***EVC***. The default is ***LM***.

Measurement Interval ID : The measurement interval for the performance monitor data sets.

Interval Start Time : The interval start date and time in the format *2019-01-03T06:41:49+00:00*.

Interval End Time : The interval end date and time in the format *2019-01-03T06:41:49+00:00*.

Elapsed Time : The elapsed time (e.g., *900* seconds).

Buttons

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

Refresh : Click to manually refresh the page immediately.

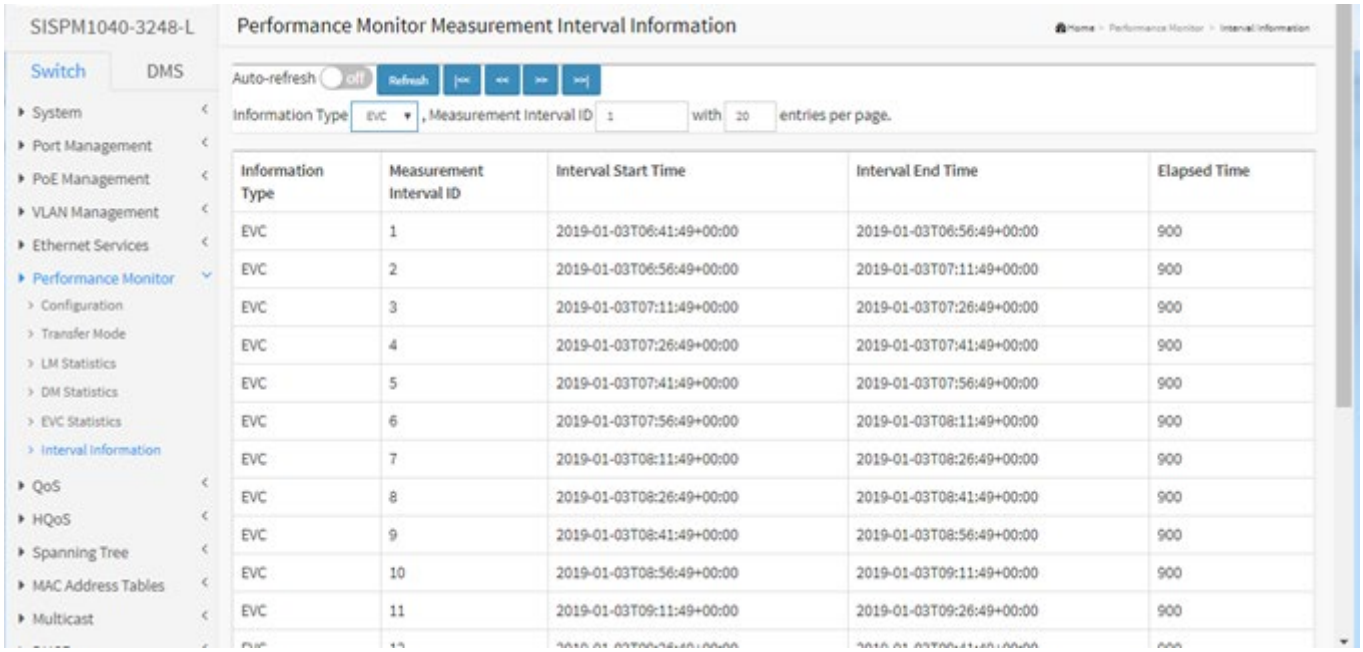
|<< : Updates the table entries, starting from the first available entry.

<< : Updates the table entries, ending at the last entry currently displayed.

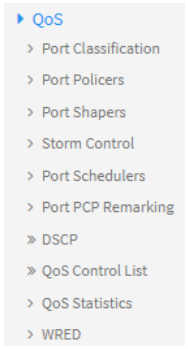
>> : Updates the table entries, starting from the last entry currently displayed.

>>| : Updates the table entries, ending at the last available entry.

Example: Information Type = EVC:



Chapter 9 - Quality of Service (QoS)



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

QoS 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 with excellent performance of all QoS classes under any traffic scenario, including jumbo frame. A super priority queue with dedicated memory and strict highest priority in the arbitration. The ingress super priority queue allows traffic recognized as CPU traffic to be received and queued for transmission to the CPU even when all the QoS class queues are congested.

9-1 Port Classification

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

1. Click QoS and Port Classification.
2. Select QoS Ingress Port parameters.
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 “PCP Classification“ to go to the next page “Port PCP Classification”.

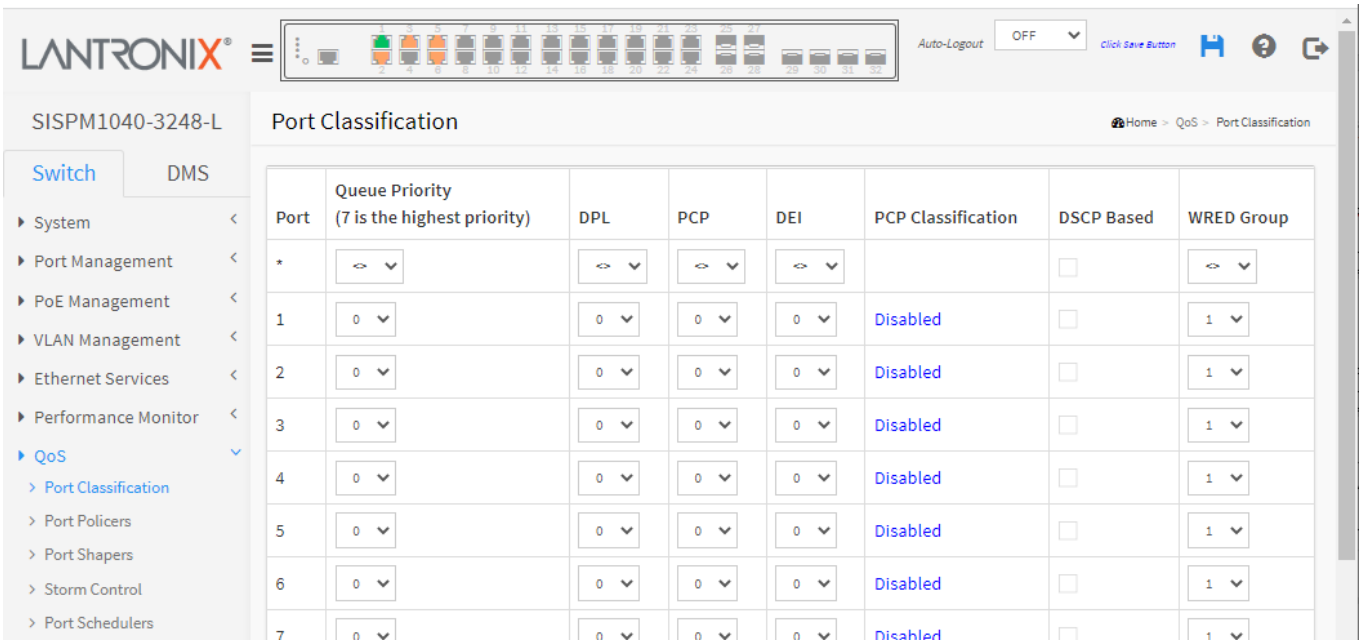


Figure 9-1: QoS Ingress Port Classification

Parameter descriptions:

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

Queue Priority : Controls the default CoS value. All frames are classified to a CoS. There is a one to one mapping between CoS, queue and priority. A CoS of 0 (zero) has the lowest priority.

If the port is VLAN aware, the frame is tagged and Tag Class. is enabled, then the frame is classified to a CoS that is mapped from the PCP and DEI value in the tag. Otherwise the frame is classified to the default CoS.

The classified CoS can be overruled by a QCL entry.

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

DPL : Controls the default drop precedence level. All frames are classified to a drop precedence level.

If the port is VLAN aware, the frame is tagged and Tag Class. is enabled, then the frame is classified to a DPL that is mapped from the PCP and DEI value in the tag. Otherwise the frame is classified to the default DPL.

The classified DPL can be overruled by a QCL entry.

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

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

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

Disabled: Use default CoS and DPL for tagged frames.

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

Click on the mode in order to configure the mode and/or mapping. **Note**: This setting has no effect if the port is VLAN unaware. Tagged frames received on VLAN unaware ports are always classified to the default CoS and DPL. The Ingress Port PCP Classification for the selected Port displays as shown and described below.

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

WRED Group : Controls the WRED group membership.

Buttons

Apply : Click to save changes.

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

Ingress Port PCP Classification

Click “PCP Classification“ to go to the next page “Port PCP Classification”.

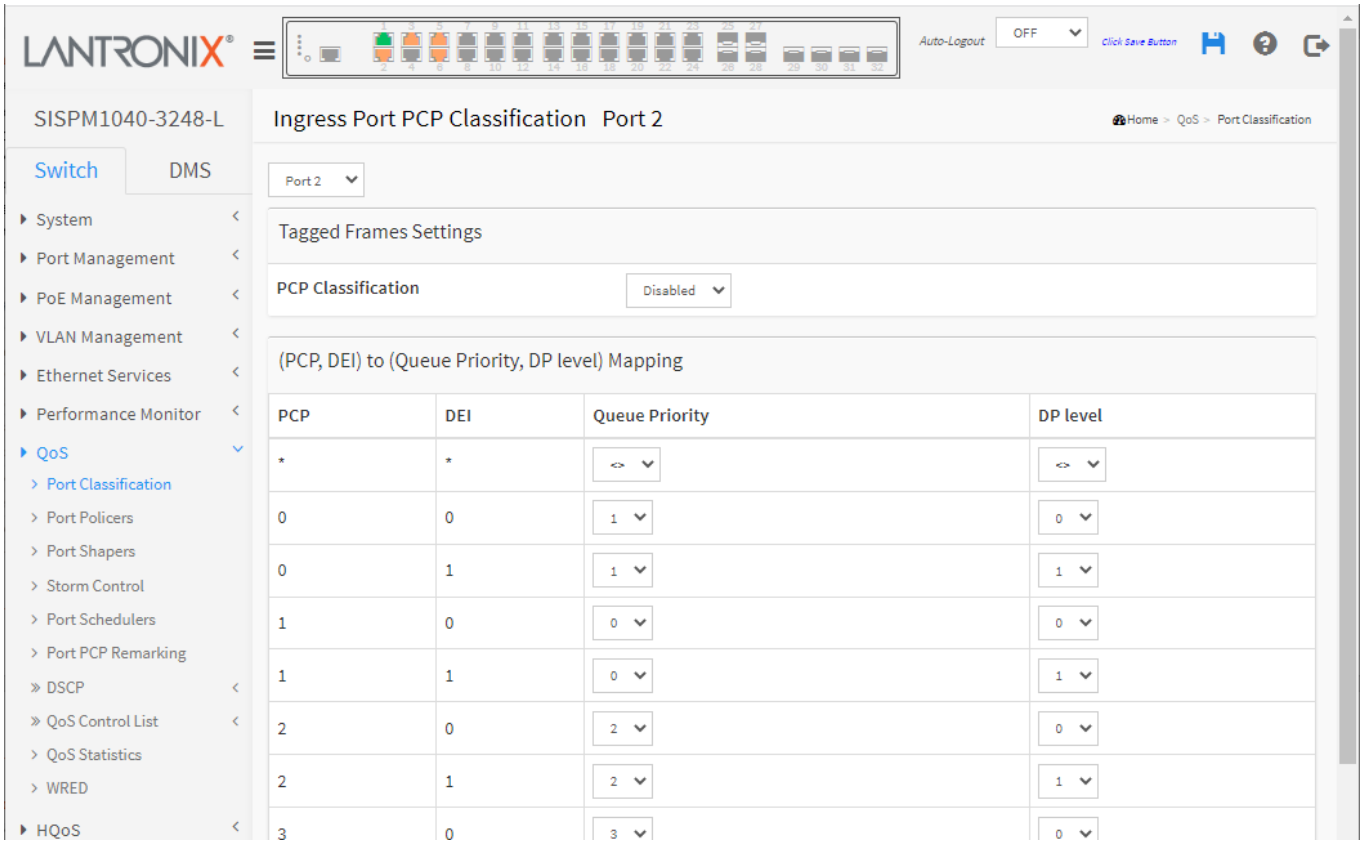


Figure 9-1: Ingress Port PCP Classification

Parameter descriptions:

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

Disabled: Use default CoS and DPL for tagged frames.

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

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

Buttons

Apply : Click to save changes.

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

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

9-2 Port Policers

This page provides an overview of QoS Ingress Port Policers for all switch ports The Port Policing is useful in constraining traffic flows and marking frames above specific rates. Policing is primarily useful for data flows and voice or video flows because voice and video usually demand a steady traffic rate.

To configure QoS Port Policers in the web UI:

1. Click Quality of Service and Port Policers.
2. Click which port(s) on which you want QoS Ingress Port Policers enabled.
3. Set the Rate, Unit, and Flow Control parameters.
4. Click Apply to save the settings.
5. To cancel the settings click the Reset button. It will revert to previously saved values.

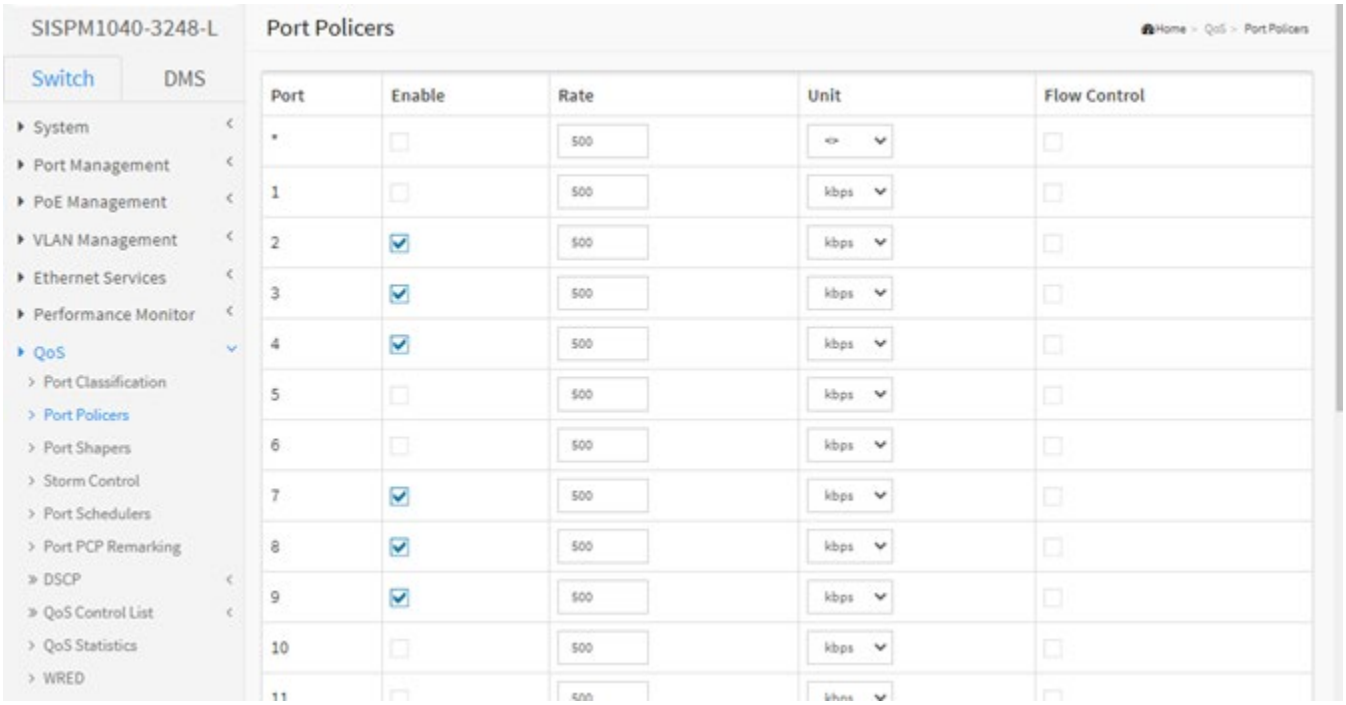


Figure 9-2: QoS Ingress Port Policers Configuration

Parameter descriptions:

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

Enabled : Check the box for the Port(s) on which you want to enable the QoS Ingress Port Policers function.

Rate : To set the Rate limit value for this port, the default is 50000.

Unit : Controls the unit of measure for the port policer rate as kbps, Mbps, fps or kfps. The default is kbps.

Flow Control : If flow control is enabled and the port is in flow control mode, then pause frames are sent instead of discarding frames. The default is disabled (unchecked)

9-3 Port Shapers

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

1. Click Quality of Service and Port Shapers.
2. Click the Port and display the 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 Reset button to revert to previously saved values.

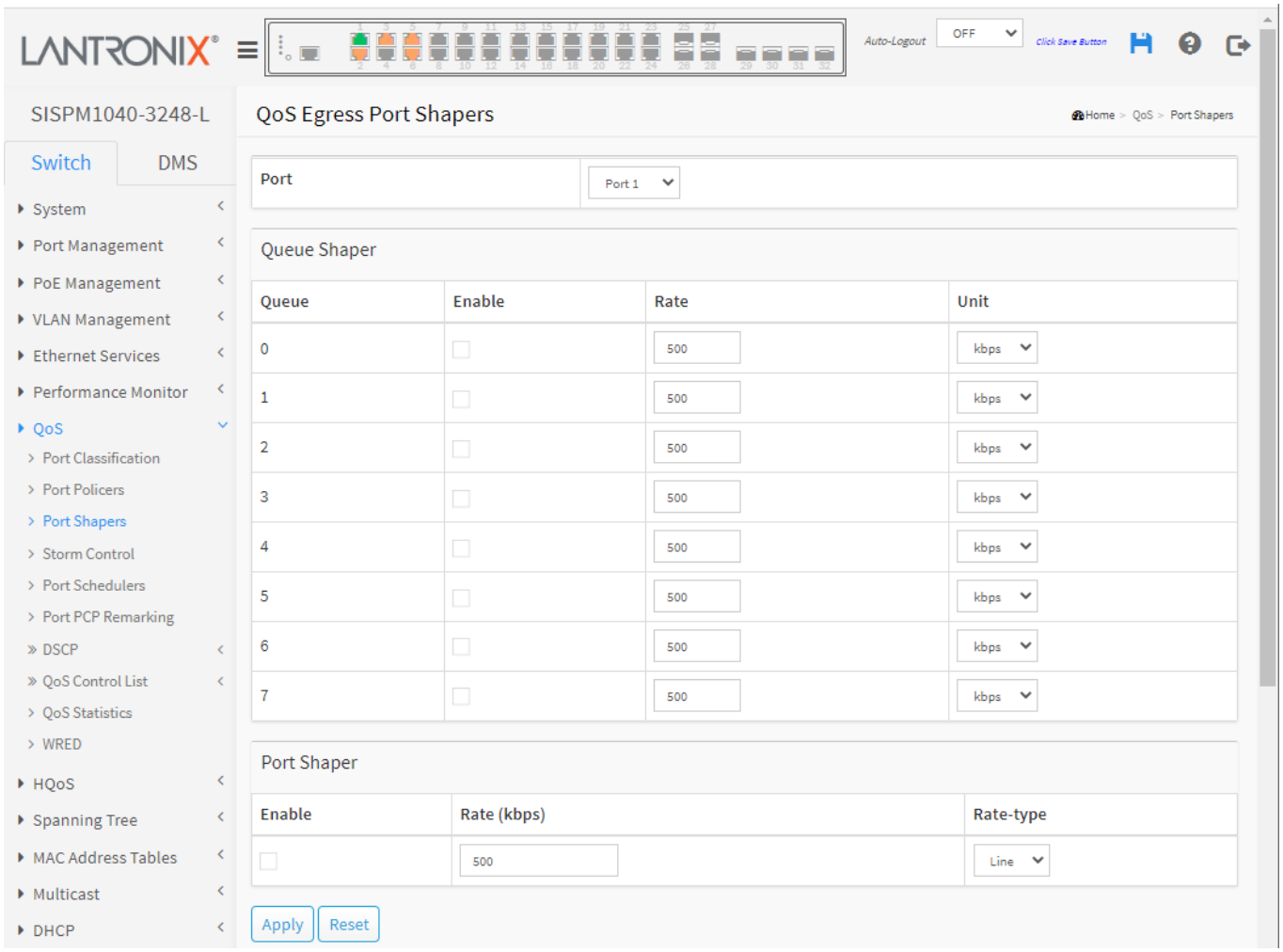


Figure 9-3: QoS Egress Port Shapers

Parameter descriptions:

Port : At the dropdown select a port number.

Queue Shaper

Queue : The queue number for the queue shaper.

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

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.

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

Port Shaper

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

Rate : Controls the rate for the port shaper. This value is restricted to 100-13107100 kbps. The rate is internally rounded up to the nearest value supported by the port shaper.

Rate-type: The rate type of the port shaper. Valid 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.

9-4 Storm Control

This page lets you configure the Storm control for the switch. There is a destination lookup failure storm rate control, multicast storm rate control, and a broadcast storm rate control. These only affect flooded frames, i.e. frames with a (VLAN ID, DMAC) pair not present on the MAC Address table. The configuration indicates the permitted packet rate for unicast, multicast or broadcast traffic across the switch

To configure Storm Control parameters in the web UI:

1. Click Quality of Service and Storm Control.
2. Select the frame type to enable storm control.
3. Set the Rate Parameters and Unit.
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 to revert to previously saved values.

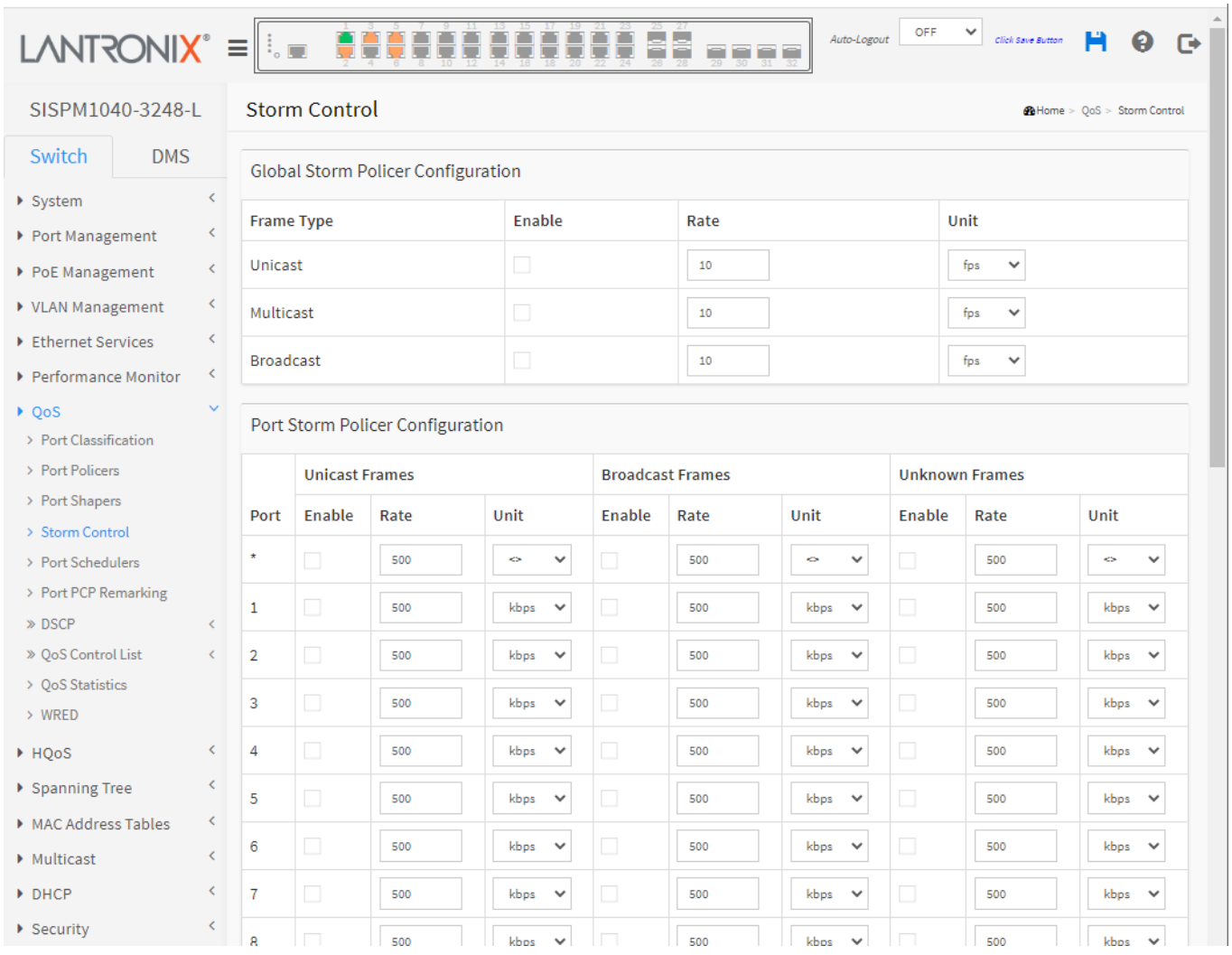


Figure 9-4: Storm Control Configuration

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 for which the configuration below applies.

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

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

Unit : Controls the unit of measure for the global storm policer rate as fps, kfps, kbps or Mbps.

Port Storm Policer Configuration

Port storm policers for all switch ports are configured on this page. There is a storm policer for known and unknown unicast frames, known and unknown broadcast frames and unknown (flooded) unicast, multicast and broadcast frames.

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

Enable : Enable or disable the storm policer for this switch port.

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

Unit : Controls the unit of measure for the port storm policer rate as fps, kfps, kbps or Mbps.

Buttons

Apply : Click to save changes.

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

9-5 Port Schedulers

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

1. Click QoS and Port Schedulers.
2. Click the Port and display the QoS Egress Port Schedulers
3. Scroll Port and Scheduler Mode, specify the Queue Shaper parameter.
4. Click the Apply button to save the settings.
5. To cancel the settings click the Reset button. It will revert to previously saved values.

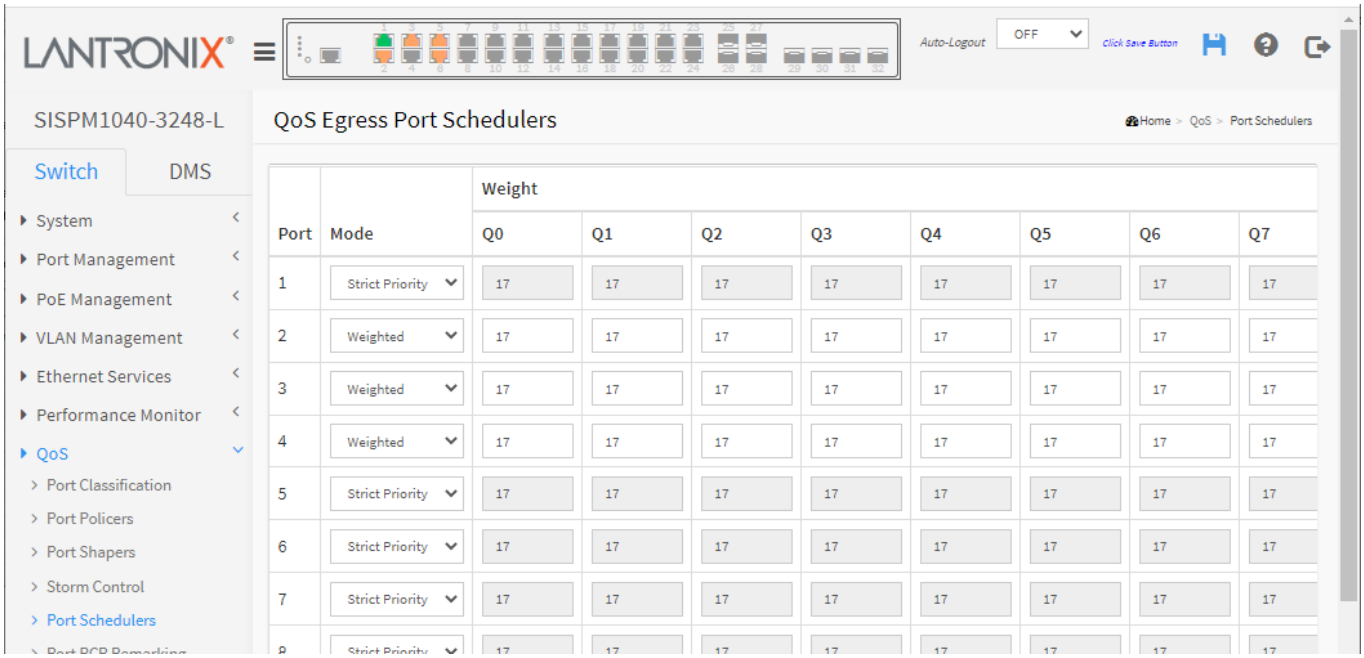


Figure 9-5: QoS Egress Port Schedulers

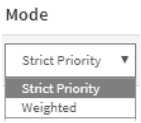
Parameter descriptions:

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

Mode : Shows the scheduling mode for this port. Select scheduling in a Strict Priority or Weighted Mode.

Strict Priority: Scheduling priority is strict; each of Q0 - Q7 weighted at 17%.

Weighted: Scheduling priority is weighted; each of Q0 - Q7 weight is configurable.



Weight Q0-Q7 : Shows the weight for this queue and port. The weight must be an integer value between 1 and 100.

Buttons

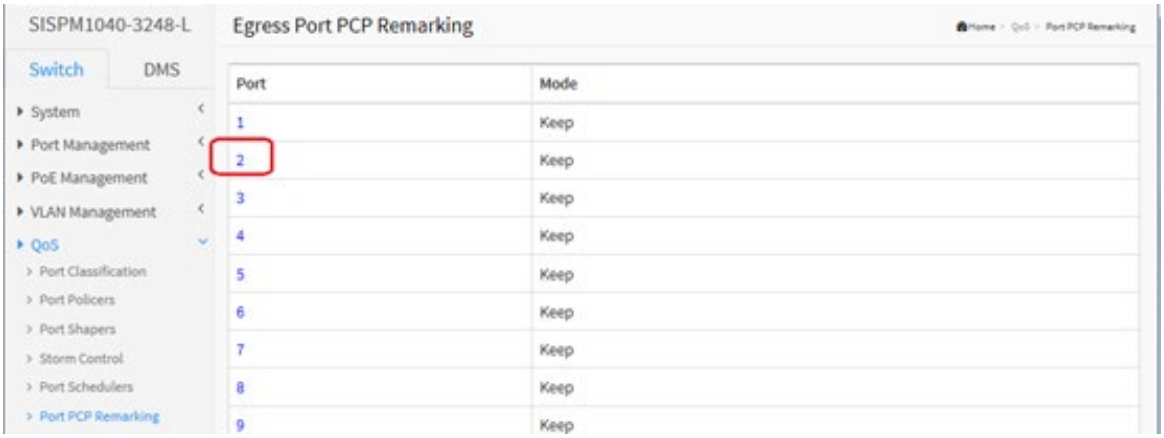
Apply : Click to save changes.

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

9-6 Port PCP Remarking

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

1. Click Quality of Service and Port PCP Remarking.
2. Click a linked Port number (e.g., Port 2 below) to display the Egress Port PCP Remarking page.



3. At the Egress Port PCP Remarking page set the Port and PCP Remarking Mode and specify the Queue Shaper parameter.

4. Click the Apply button to save the setting.
5. To cancel the settings click the Reset button to revert to previously saved values.

Parameter descriptions:

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

Mode : Shows the PCP remarking mode for this port.

Keep: Use classified PCP/DEI values (default).

Specific: Use default PCP/DEI values.

Mapped: Use mapped versions of CoS and DPL.

PCP/DEI Configuration : Controls the default PCP and DEI values used when the mode is set to Default.

Specific PCP: At the dropdown select a specific PCP (0-7).

Specific DEI: At the dropdown select a specific DEI (0 or 1).

(QoS class, DP level) to (PCP, DEI) Mapping : Controls the mapping of the classified (QoS class, DP level) to (PCP, DEI) values when the mode is set to Mapped.

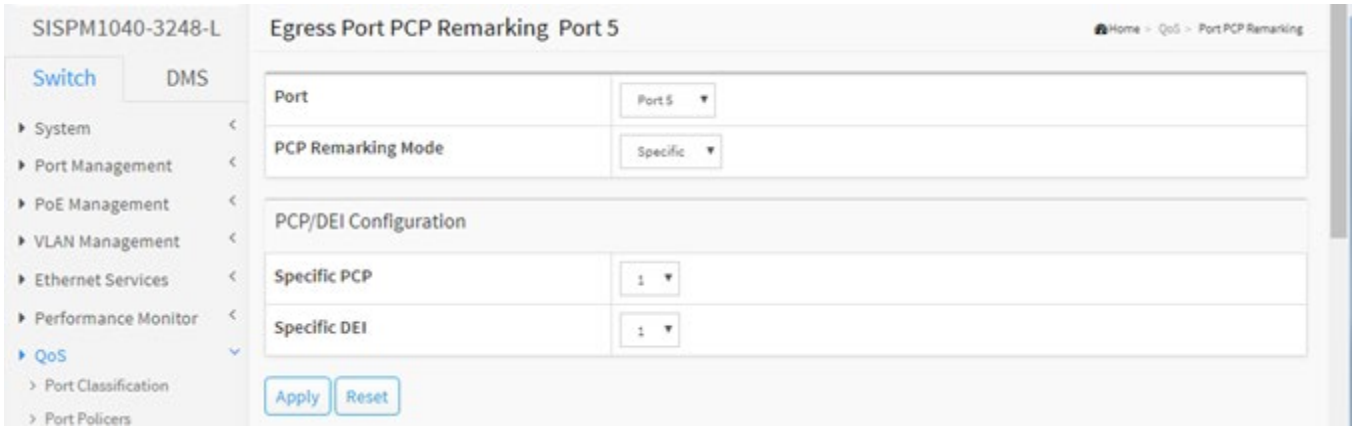
(Queue Priority, DP level) to (PCP, DEI) Mapping: For each Queue Priority / DP level, select a PCP (0-7) and DEI (0 or 1) at the dropdowns.

Buttons

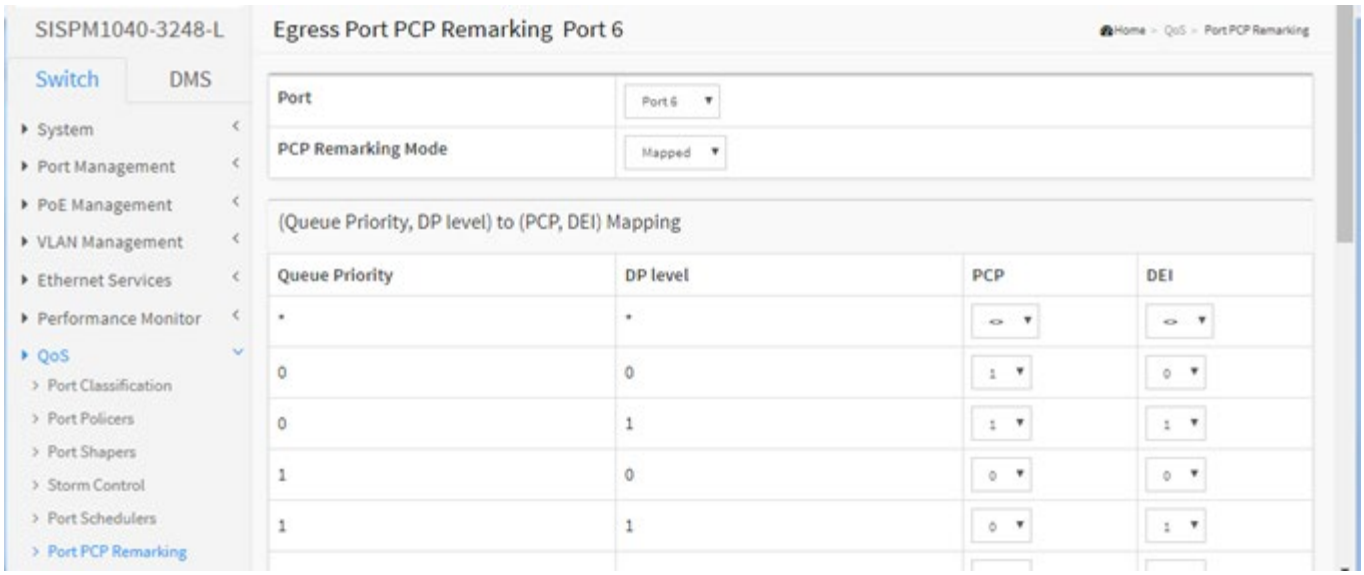
Apply : Click to save changes.

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

Example: PCP Remarking Mode = Specific



Example: PCP Remarking Mode = Mapped



9-7 DSCP

9-7.1 Port DSCP

This page lets you set the QoS Port DSCP configuration for all switch ports. To configure QoS Port DSCP parameters in the web UI:

1. Click QoS, DSCP, and Port DSCP.
2. Enable or disable Ingress Translate and select a Classify parameter.
3. Select Egress Rewrite parameters.
4. Click the Apply button to save the setting.
5. To cancel the settings click the Reset button. It will revert to previously saved values.

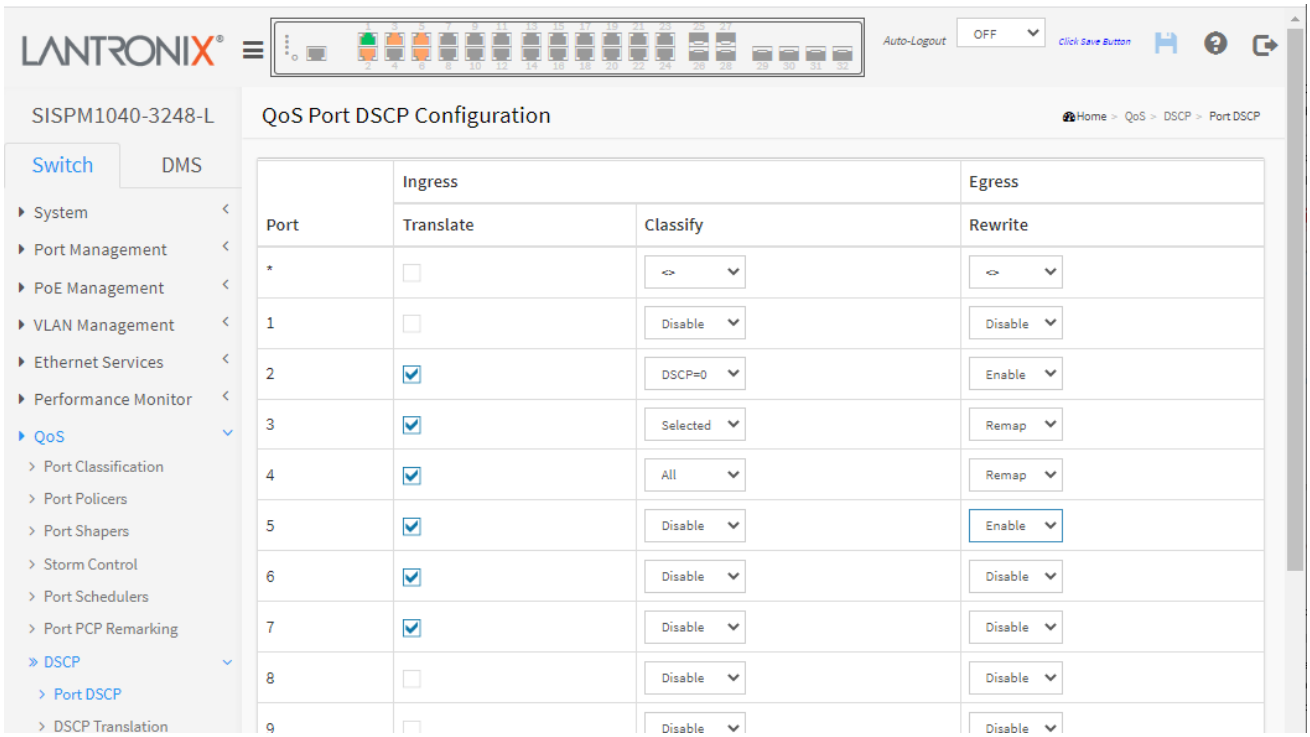


Figure 9-7.1: QoS Port DSCP Configuration

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 the Ingress Translation check the checkbox.

Classify: Classification for a port have one of 4 different values:

Disable: No Ingress DSCP Classification.

***DSCP=0*:** Classify if incoming (or translated if enabled) DSCP is 0.

Selected: Classify only selected DSCP for which classification is enabled as specified in DSCP Translation window for the specific DSCP.

All: Classify all DSCP.

Egress : Port Egress Rewriting can be one of these parameters:

Disable: No Egress rewrite.

Enable: Rewrite enable without remapped.

Remap: DSCP from analyzer is remapped and frame is remarked with remapped DSCP value.

Buttons

Apply : Click to save changes.

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

9-7.2 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 the 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 setting.
5. To cancel the settings click the Reset button. It will revert to previously saved values.

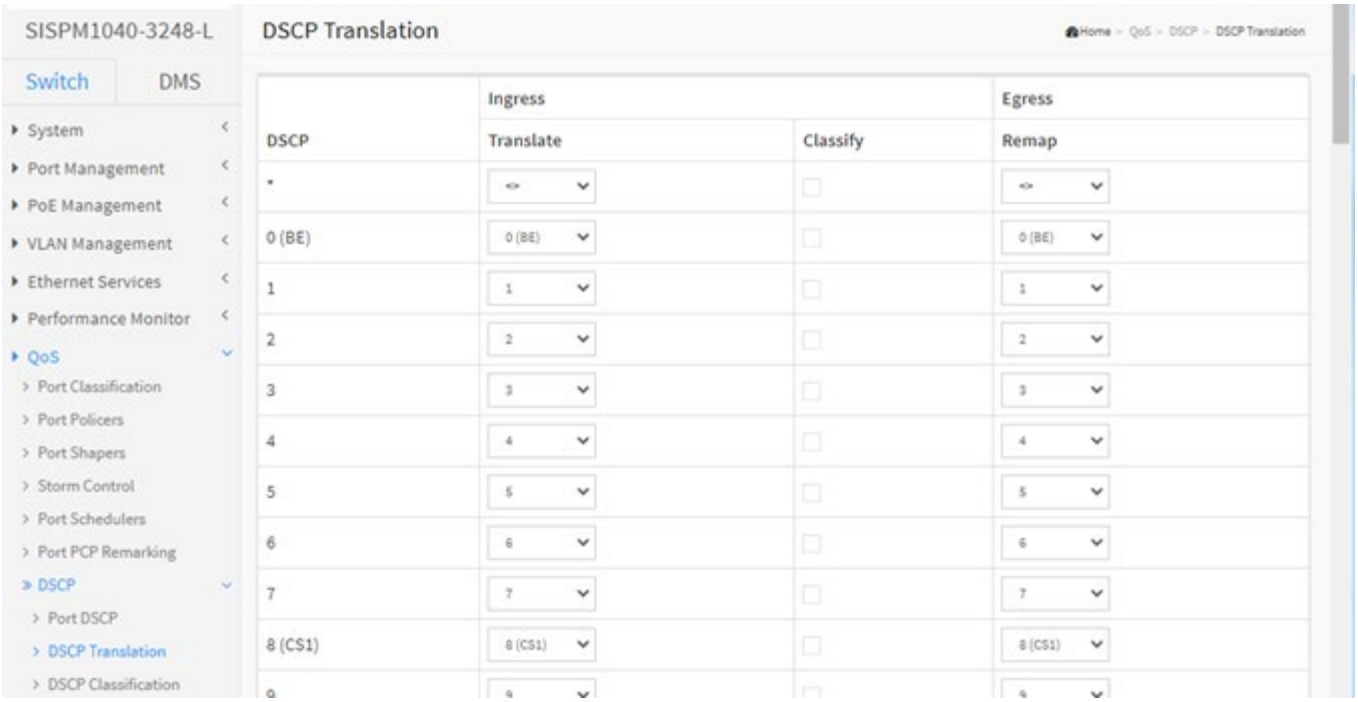


Figure 9-7.2: DSCP Translation

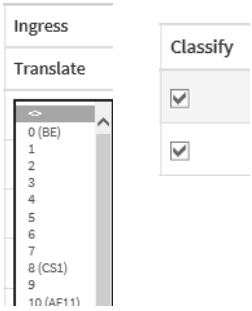
Parameter descriptions:

DSCP : Maximum number of supported DSCP values is 64 and valid DSCP value 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 : Select the DSCP value from select menu to which you want to remap. DSCP value ranges from 0 to 63.

9-7.3 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 settings click the Reset button. It will revert to previously saved values

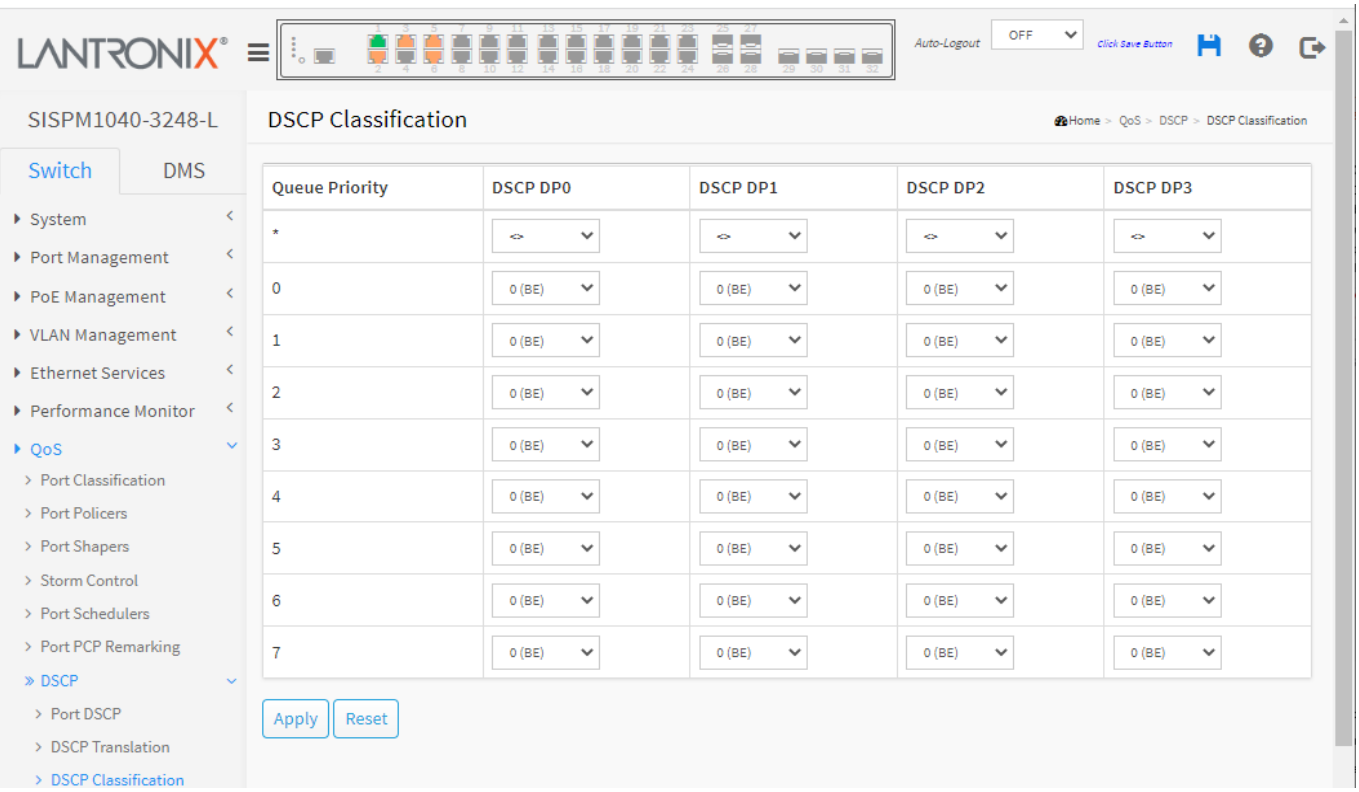


Figure 9-7.3: DSCP Classification Configuration

Parameter descriptions:

Queue Priority : Actual Class of Service.

DSCP DP0 : Select the classified DSCP value (0-63) for Drop Precedence Level 0.

DSCP DP1 : Select the classified DSCP value (0-63) for Drop Precedence Level 1.

DSCP DP2 : Select the classified DSCP value (0-63) for Drop Precedence Level 2.

DSCP DP3 : Select the classified DSCP value (0-63) for Drop Precedence Level 3.

Buttons

Apply : Click to save changes.

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

9-7.4 DSCP-Based QoS

This page lets you configure the basic QoS DSCP based QoS Ingress Classification settings for the switch.

To configure DSCP-Based QoS Ingress Classification parameters in the web UI:

1. Click QoS, DSCP, and DSCP-Based QoS.
2. Enable or disable the DSCP for Trust.
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.

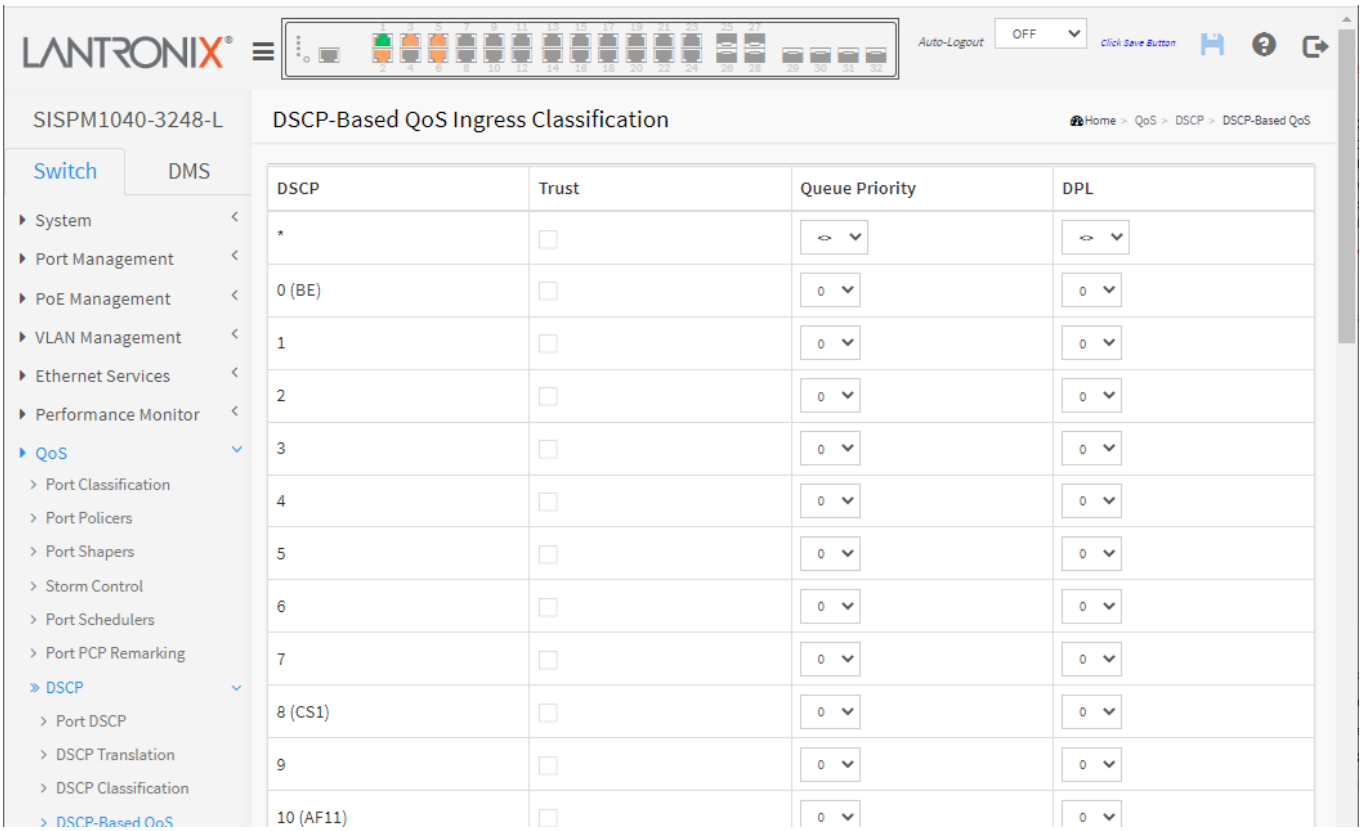


Figure 9-7.4: DSCP-Based QoS Ingress Classification

Parameter descriptions:

DSCP : Maximum number of supported DSCP values are 64.

Trust : Click to check if the DSCP value is trusted.

Queue Priority : Queue Priority value can be 0 - 7. Priority 7 is the highest.

DPL : Drop Precedence Level (0-3).

Buttons

Apply : Click to save changes.

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

9-8 QoS Control List

9-8.1 Configuration

This page shows the QoS Control List (QCL), which is made up of the QCEs. Each row describes a QCE that is defined. The switch supports up to 256 QCEs. Click on the lowest plus sign to add a new QCE to the list.

To configure QoS Control List parameters in the web UI:

1. Click QoS, QoS Control List, and Configuration to display the default QoS Control List Configuration table.
2. Click the Add QCE ( ) icon to add a new QoS Control List on the QCE Configuration page.
3. At the QCE Configuration page, set all parameters and check 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.

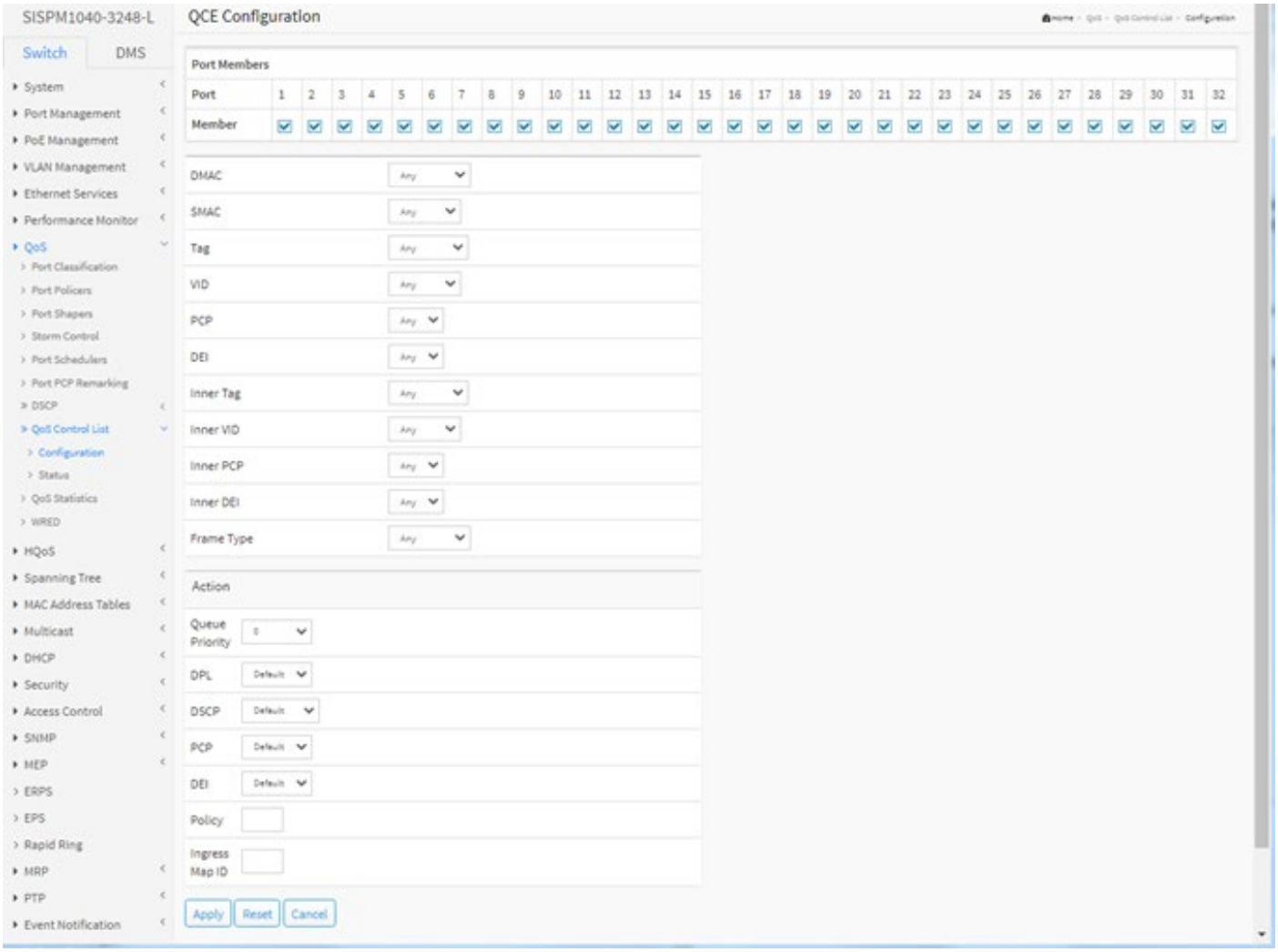


Figure 9-8.1: QCE Configuration

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.

***Specific*:** 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'.

Frame Type : Indicates the type of frame to look for incoming frames. Possible frame types are:

***Any*:** The QCE will match all frame type.

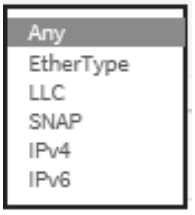
***Ethernet*:** Only Ethernet frames (with Ether Type 0x600-0xFFFF) are allowed.

***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 : At the dropdown select Default or 0-7. 'Default' means that the default classified value is not modified by this QCE.

***DPL*:** Classify Drop Precedence Level.

***DSCP*:** Classify DSCP value.

***PCP*:** Classify PCP value.

***DEI*:** Classify DEI value.

***Policy*:** Classify ACL Policy number.

Modification Buttons : You can modify each QCE (QoS Control Entry) in the table using the following buttons:

 : Inserts a new QCE before the current row.

 : Edits the QCE.

 : Moves the QCE up the list.

 : Moves the QCE down the list.

 : Deletes the QCE.

 : The lowest plus sign adds a new entry at the bottom of the QCE listings.

Port Members : Check the checkbox button to include the port in the QCL entry. By default all ports are included.

Key Parameters : Key configuration as 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 Inner Tag field can be 'Untagged', 'Tagged', 'C-Tagged', 'S-Tagged' or 'Any'.

Inner VID Valid value of Inner VLAN ID can be any value in the range 1-4095 or 'Any'; user can enter either a specific value or a range of VIDs.

Inner PCP Valid value of Inner PCP are specific (0, 1, 2, 3, 4, 5, 6, 7) or range (0-1, 2-3, 4-5, 6-7, 0-3, 4-7) or 'Any'.

Inner DEI Valid value of Inner DEI can be '0', '1' or 'Any'.

Frame Type Frame Type can have any of these values: Any, EtherType, LLC, SNAP, IPv4, or IPv6 as 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 :

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 : For Frame Type IPv4 select:

Protocol IP protocol number: (0-255, 'TCP' or 'UDP') or 'Any'.

SIP 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.

DIP 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 : For Frame Type IPv6 select:

Protocol IP protocol number: (0-255, 'TCP' or 'UDP') or 'Any'.

SIP (32 LSB) 32 LS bits of IPv6 source address in value/mask format or 'Any'.

DIP (32 LSB) 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.

Value: e.g., 0 for Other protocol selection only.

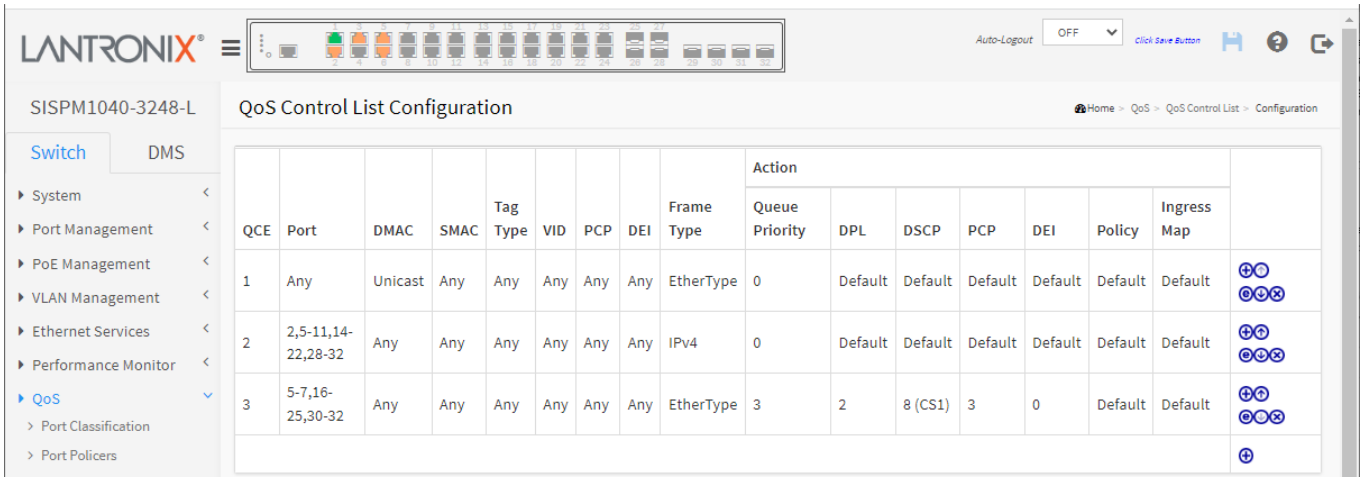
Buttons

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.

Example:



Messages: *PCP and DEI cannot be set individually!*

9-8.2 Status

This page lets you ~~configure and~~ view 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.

To display QoS Control List Status in the web UI:

1. Click QoS, QoS Control List, and Status.
2. To auto-refresh the page automatically every 3 seconds click “Auto-refresh”.
3. At the User select box select the user from the drop down list.
4. Click “Refresh” to refresh an entry of the MVR Statistics Information.

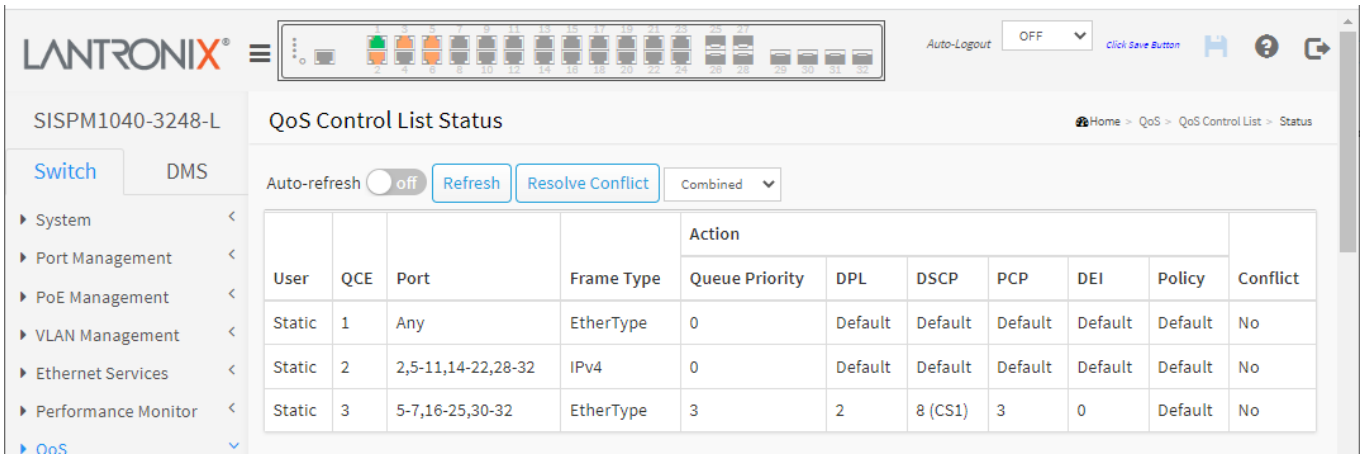


Figure 7-8.2: QoS Control List Status

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:

Queue Priority: (0-7).

CoS: Classify Class of Service.

DPL: Classify Drop Precedence Level.

DSCP: Classify DSCP value.

PCP: Classify PCP value.

DEI: Classify DEI value.

Policy: Classify ACL Policy number.

Ingress Map: Classify Ingress Map ID.

Conflict : Displays Conflict status of QCL entries. It may happen that resources required to add a QCE may not available, in that case it shows conflict status as ***'Yes'***, otherwise it is always ***'No'***. Please note that conflict can be resolved by releasing the H/W resources required to add QCL entry on pressing 'Resolve Conflict' button.

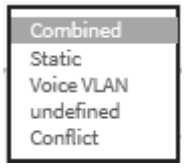
Buttons

Auto-refresh : Click to refresh the page automatically every 3 seconds.

Refresh : Click to manually refresh the page immediately.

Resolve Conflict : Click to release the resources required to add QCL entry in case the conflict status for any QCL entry is 'yes'.

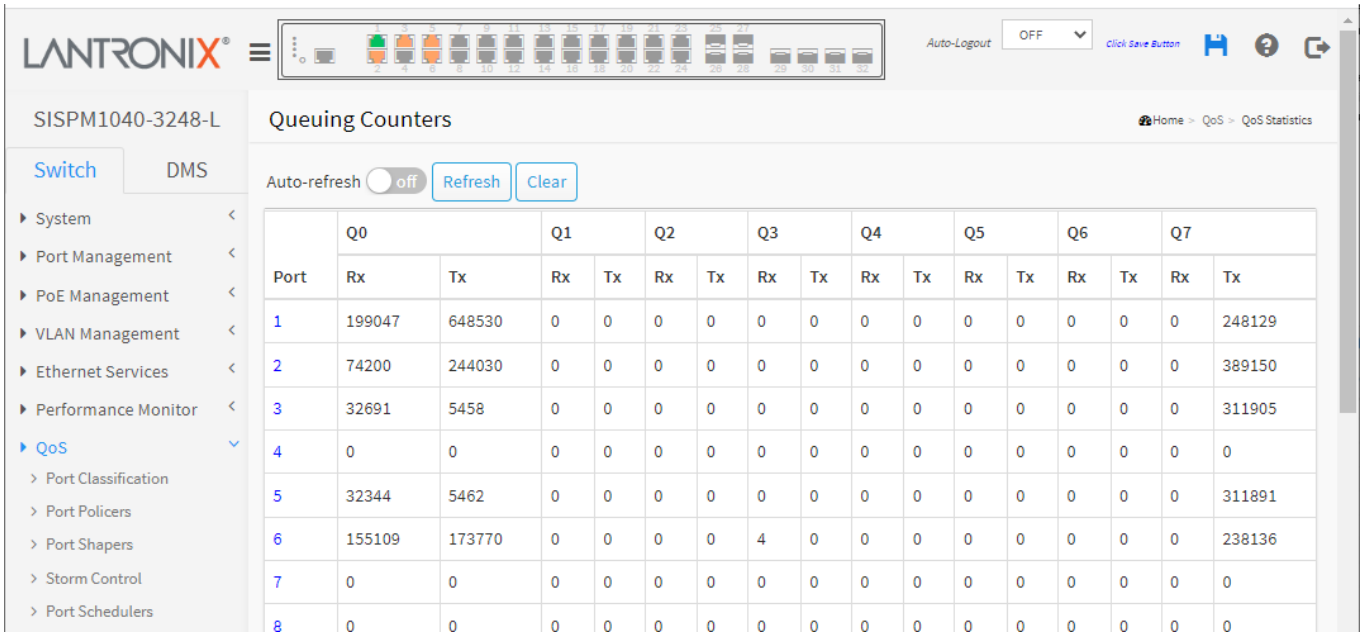
User select box : Select the QCL status from this drop down list.



9-9 QoS Statistics

This page provides statistics for the different queues for all switch ports. To display the Queuing Counters in the web UI:

1. Click QoS and QoS Statistics.
2. To auto-refresh the page click “Auto-refresh”.
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	199047	648530	0	0	0	0	0	0	0	0	0	0	0	0	0	248129
2	74200	244030	0	0	0	0	0	0	0	0	0	0	0	0	0	389150
3	32691	5458	0	0	0	0	0	0	0	0	0	0	0	0	0	311905
4	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
5	32344	5462	0	0	0	0	0	0	0	0	0	0	0	0	0	311891
6	155109	173770	0	0	0	0	4	0	0	0	0	0	0	0	0	238136
7	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
8	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0

Figure 7-9: Queuing Counters

Parameter descriptions:

Port : The logical port for the settings contained in the same row. Click a linked Port number to display its Detailed Port Statistics page. See Port Management > Port Statistics.

Qn : The Queue number, There are 8 QoS queues per port. Q0 is the lowest priority queue.

Rx : The number of received packets per queue.

Tx : The number of transmitted packets per queue.

Buttons

Auto-refresh : Click to refresh the page automatically every 3 seconds.

Refresh : Click to manually refresh the page immediately.

Clear : Click to clear the page.

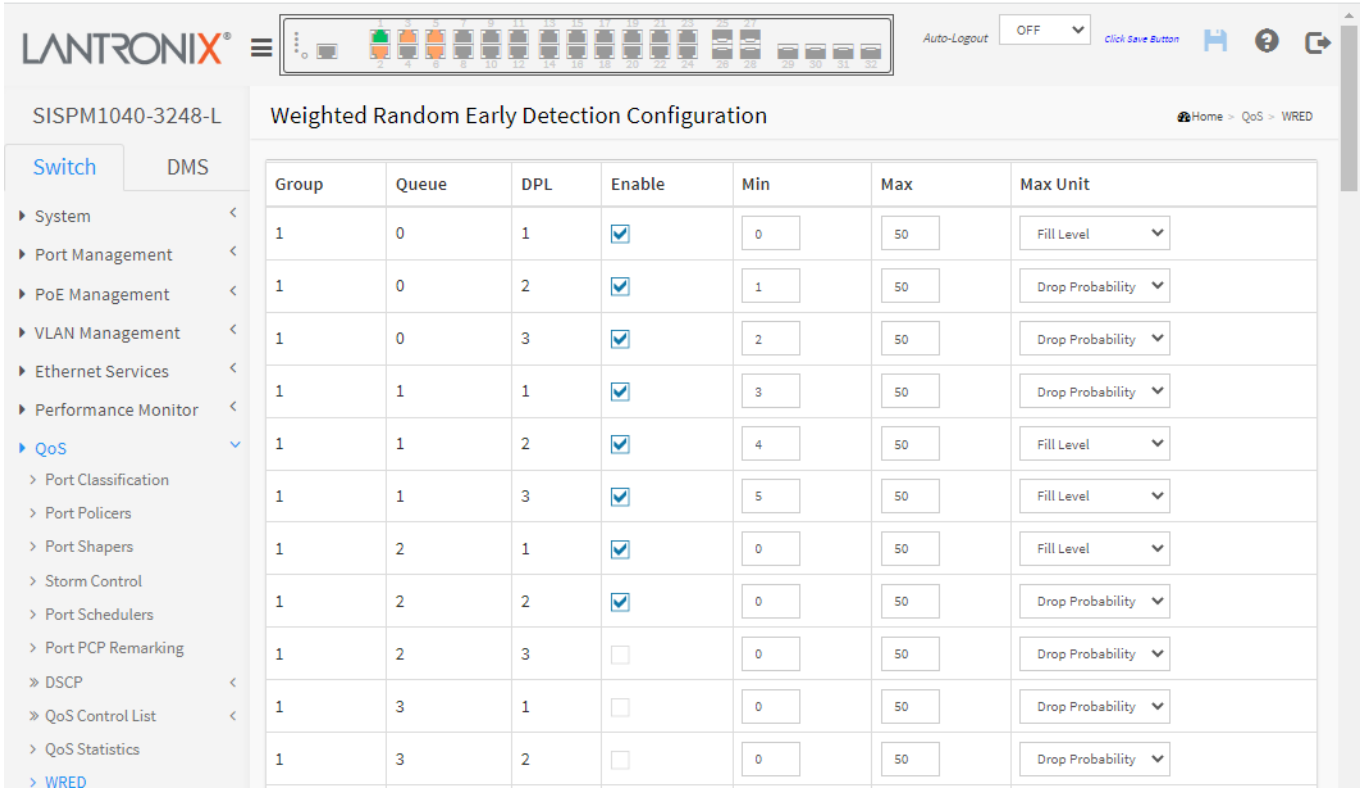
9-10 WRED

This page lets you configure the Random Early Detection (RED) settings. Through different RED configuration for the queues it is possible to obtain Weighted Random Early Detection (WRED) operation between queues. The settings are global for all ports in the switch.

WRED (Weighted Random Early Detection) is an active queue management mechanism that provides preferential treatment of higher priority frames when traffic builds up within a queue. A frame's DPL is used as input to WRED. A higher DPL assigned to a frame results in a higher probability that the frame is dropped during times of congestion.

To configure and display Random Early Detection in the web UI:

1. Click QoS and WRED.
2. Set Enable, Min, and Max parameters.
3. In the Max Unit column select Fill Level or Drop Probability. The default is Fill Level.
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.



Group	Queue	DPL	Enable	Min	Max	Max Unit
1	0	1	☑	0	50	Fill Level
1	0	2	☑	1	50	Drop Probability
1	0	3	☑	2	50	Drop Probability
1	1	1	☑	3	50	Drop Probability
1	1	2	☑	4	50	Fill Level
1	1	3	☑	5	50	Fill Level
1	2	1	☑	0	50	Fill Level
1	2	2	☑	0	50	Drop Probability
1	2	3	☐	0	50	Drop Probability
1	3	1	☐	0	50	Drop Probability
1	3	2	☐	0	50	Drop Probability

Figure 7-10: 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%.

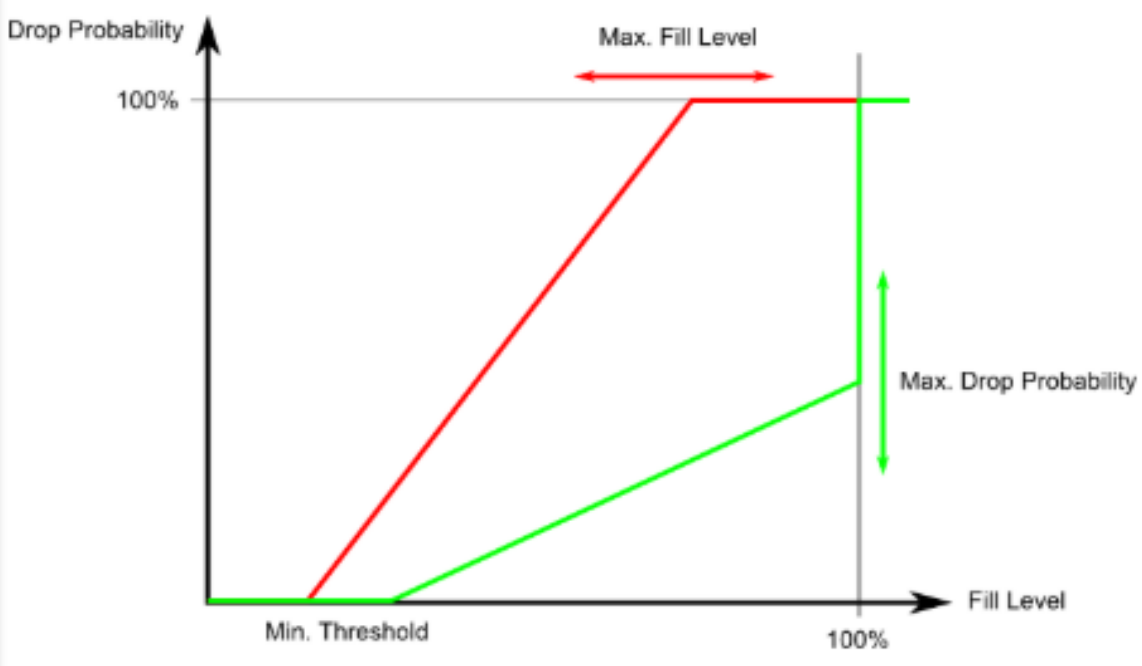
Max Unit : Selects the unit for Max. Possible values are:

Drop Probability: Max controls the drop probability just below the 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 start dropping frames marked with Drop Precedence Level > 0 (yellow frames).

If **Max Unit** is 'Drop Probability' (the green line), Max controls the drop probability when the fill level is just below 100%.

If **Max Unit** is 'Fill Level' (the red line), Max controls the fill level where drop probability reaches 100%. This configuration makes it possible to reserve a portion of the queue exclusively for frames marked with Drop Precedence Level 0 (green frames). The reserved portion is calculated as (100 – Max) %.

Frames marked with Drop Precedence Level 0 (green frames) are never dropped.

The drop probability for frames increases linearly from zero (at Min average queue filling level) to Max Drop Probability or Fill Level.

Buttons

Apply : Click to save changes.

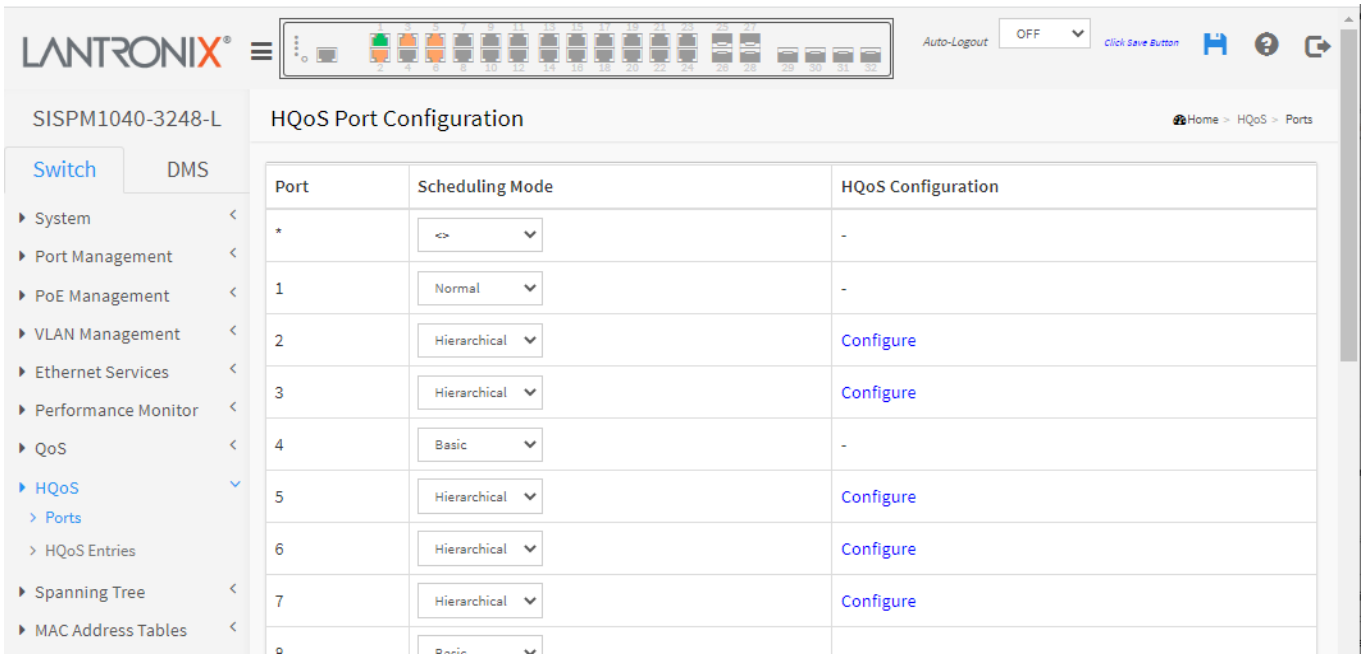
Refresh : Click to refresh the page.

Chapter 10 - HQoS (Hierarchical Quality of Service)

The switch supports HQoS (Hierarchical Quality of Service). HQoS is a method of QoS that can be configured on a service level.

10-1 HQoS Port Configuration

This page lets you configure HQoS Port parameters.

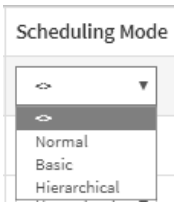


HQoS Port Configuration

Parameter descriptions:

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

Scheduling Mode : The scheduling mode for the port affects which egress QoS options are available. The values are:



Normal: Normal QoS configuration available for non-service traffic only.

Basic: Basic QoS configuration available for non-service traffic only.

Hierarchical: Basic QoS configuration available per HQoS entry.

HQoS Configuration : Link to Hierarchical Quality of Service configuration for ports in Hierarchical Scheduling Mode. See Add New HQoS Entry below.

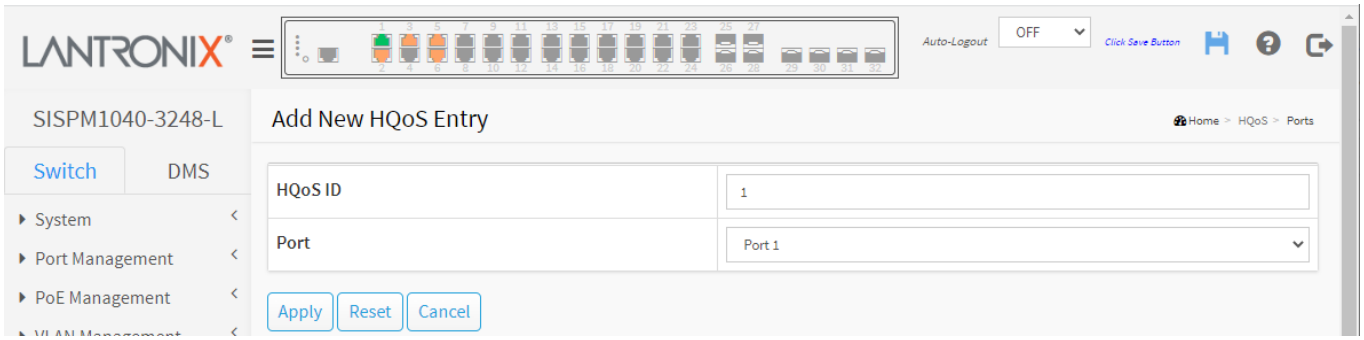
Buttons

Apply : Click to save changes.

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

10-2 Add New HQoS Entry

This page lets you configure HQoS entry parameters from the Switch > HQoS > HQoS Entries menu path. From the default page, click the Add New HQoS Entry icon ( ) to display the Add New HQoS Entry page:



Add New HQoS Entry page

Parameter descriptions:

HQoS ID : The HQoS ID identifies the HQoS entry. The range is 1 – 256. The default is 1.

Port : The destination port for the traffic mapped to the HQoS entry. The default is Port 1.

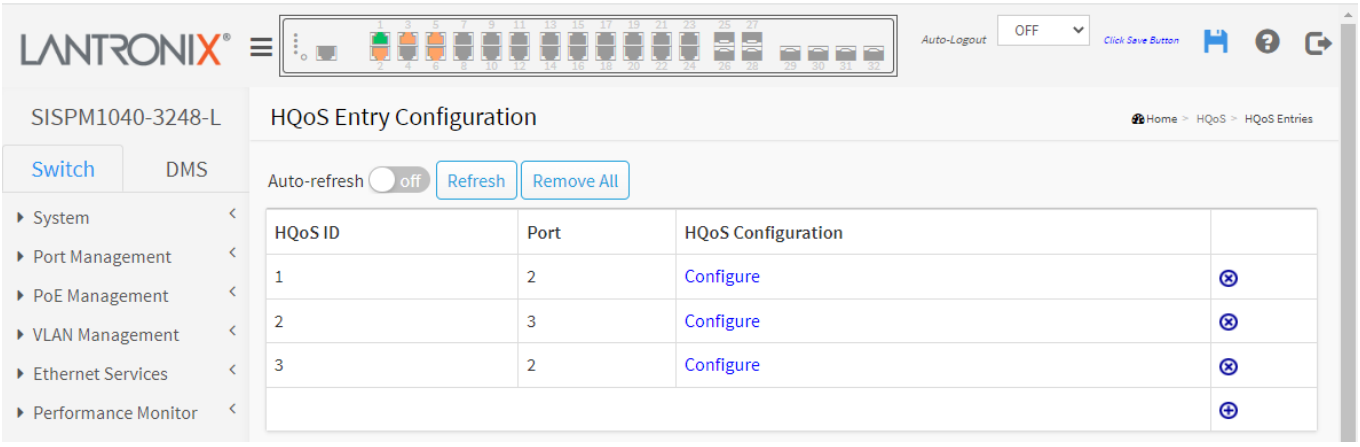
Buttons

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; any changes made locally will be undone.

After you enter the parameters for the new instance and click the Apply button, the HQoS Entry Configuration page displays the currently configured HQoS entries:



Parameter descriptions:

HQoS ID : The HQoS ID identifies the HQoS entry. The valid range is 1 – 256.

Port : The destination port for the traffic mapped to the HQoS entry.

HQoS Configuration : A link to the QoS parameter configuration (see below).

Modification Buttons

You can add or delete HQoS entries in the table using these buttons:

Delete: Click to delete the HQoS entry.

Add: Click to add a new HQoS entry.

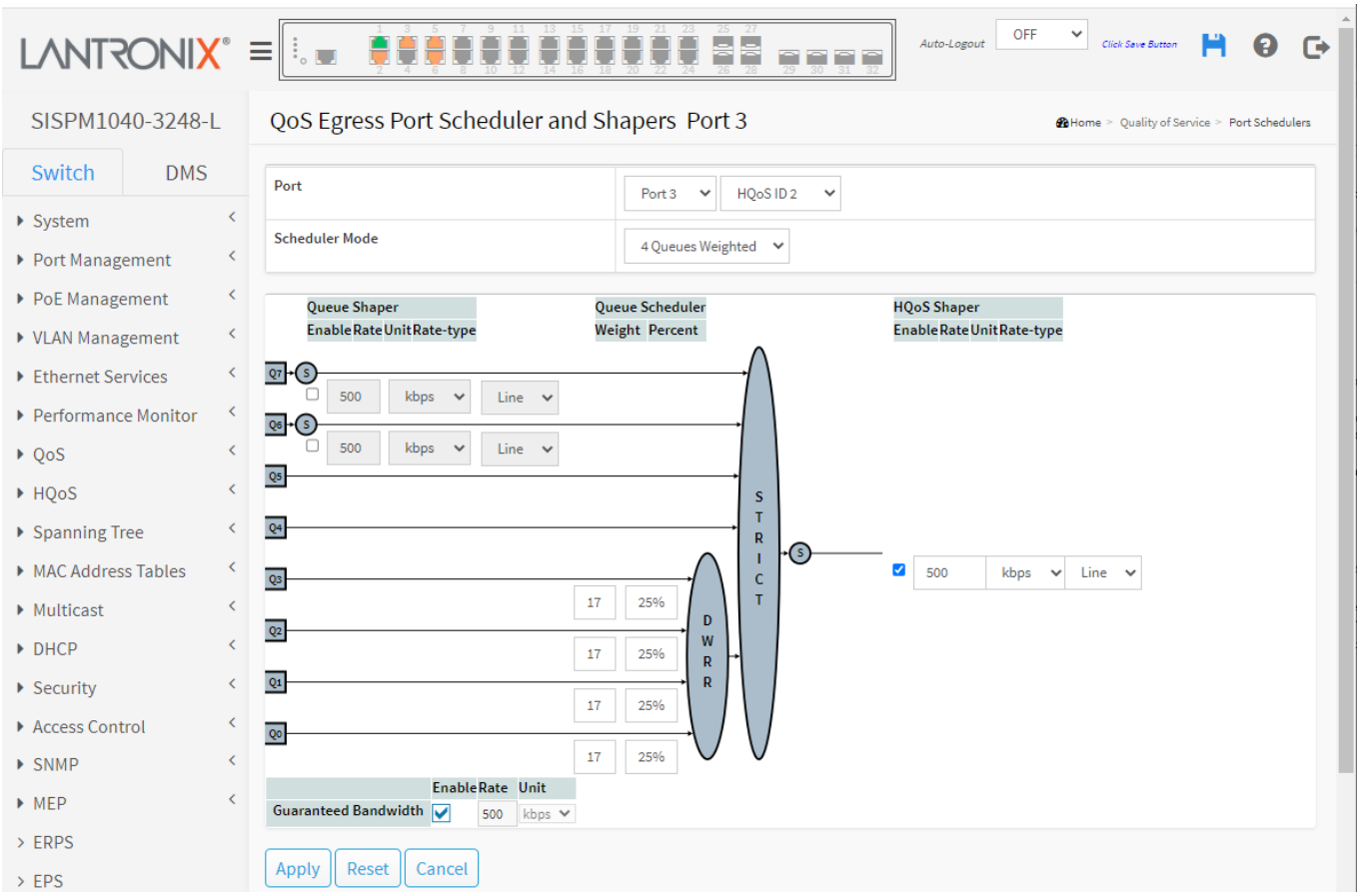
Buttons

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

Refresh : Click to manually refresh the page immediately.

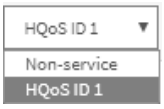
Remove All : Click to remove all HQoS entries.

Click the linked text **Configure** in the HQoS Configuration column to display the QoS Egress Port Scheduler and Shapers page.



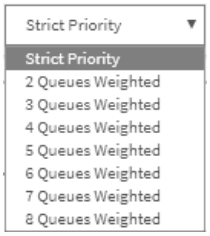
Parameter descriptions:

Port : Dropdown to select the port to configure.



HQoS ID : Dropdown to select 'Non-service' or 'HQoS ID x'. The default is 'Non-service'.

Scheduler Mode : Controls how many of the queues are scheduled as strict and how many are scheduled as weighted on this switch port. At the dropdown select 'Strict Priority' or '2-8 Queues Weighted'. The default is 'Strict Priority'.



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 can be 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. Only shown for Non-service configuration.

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. Only shown for Non-service configuration. 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. Only shown for Non-service configuration.

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.

HQoS Shaper Enable : Controls whether the HQoS shaper is enabled for this HQoS ID. Only shown when configuring HQoS entries.

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

HQoS Shaper Unit : Controls the unit of measure for the HQoS shaper rate as kbps or Mbps. Only shown when configuring HQoS entries.

HQoS Shaper Rate-type : The rate type of the HQoS shaper. Valid values are:

Line: Specify that this shaper operates on line rate.

Data: Specify that this shaper operates on data rate.

Guaranteed Bandwidth Enable : Controls whether the HQoS guaranteed bandwidth is enabled for this HQoS ID. Only shown when configuring HQoS entries.

Guaranteed Bandwidth Rate : Controls the rate for the guaranteed bandwidth. This value is restricted to 0-13107100 when "Unit" is kbps, and 0-13107 when "Unit" is Mbps. Only shown when configuring HQoS entries.

Guaranteed Bandwidth Unit : Controls the unit of measure for the guaranteed bandwidth as kbps or Mbps. Only shown when configuring HQoS entries.

Buttons

Apply : Click to save changes.

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

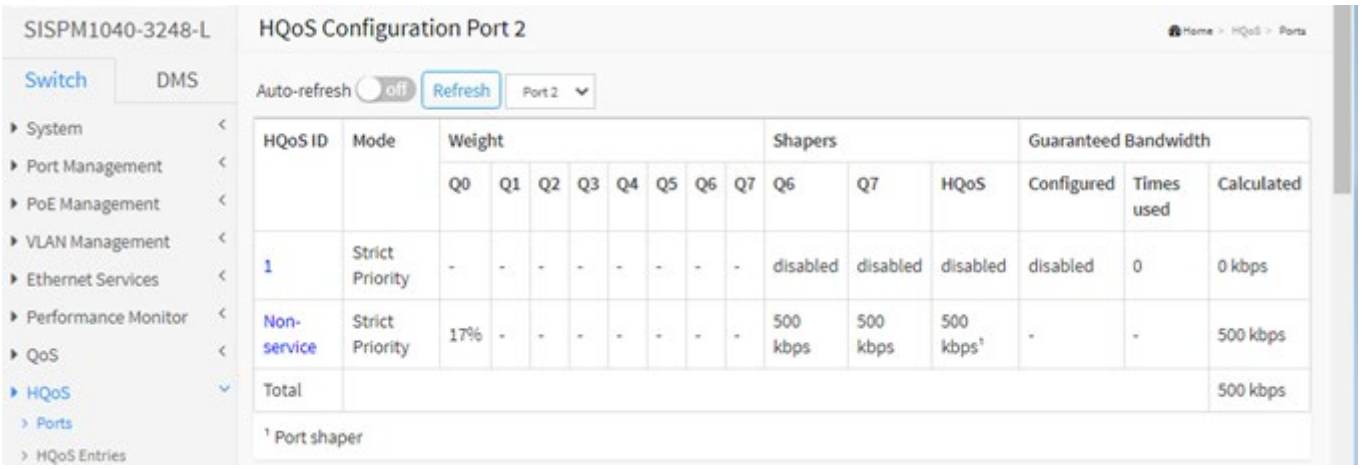
Cancel : Click to undo any changes made locally and return to the previous page.

Messages

Message*: HQoS configuration for this entry will be removed. Do you want to proceed anyway?*

Meaning: Displays when deleting an HQoS entry.

Action: Click the OK button only if you are sure you want to delete the existing entry.



If you click an HQoS ID the HQoS ID column, the QoS Egress Port Scheduler and Shapers page displays for the Port.

If you click the linked text Non-service in the HQoS ID column, the QoS Egress Port Shapers page displays for the Port.

Parameter descriptions:

HQoS ID : The HQoS ID identifies the HQoS entry. Click on the linked HQoS ID in order to configure the scheduler and shapers.

Mode : Shows the scheduling mode for this HQoS entry.

Weight/Qn : Shows the weight for this queue and HQoS entry.

Shapers/Qn : Shows “disabled” or actual queue shaper rate (e.g., “800 Mbps”).

Shapers/HQoS : Shows “disabled” or actual HQoS entry shaper rate – e.g. “800 Mbps”. For Non-service, this is the port shaper rate.

Guaranteed Bandwidth Configured : Shows “disabled” or actual configured HQoS entry guaranteed bandwidth (e.g., “800 Mbps”).

Guaranteed Bandwidth Times Used : Number of services using an HQoS Profile.

Guaranteed Bandwidth Calculated : Shows actual calculated HQoS entry guaranteed bandwidth (e.g., “800 Mbps”). If no traffic is mapped to an HQoS entry, the guaranteed bandwidth is 0 Kbps.

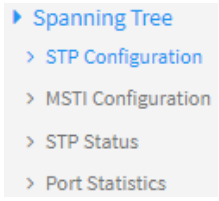
Buttons

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.

Chapter 11 - 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 (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.

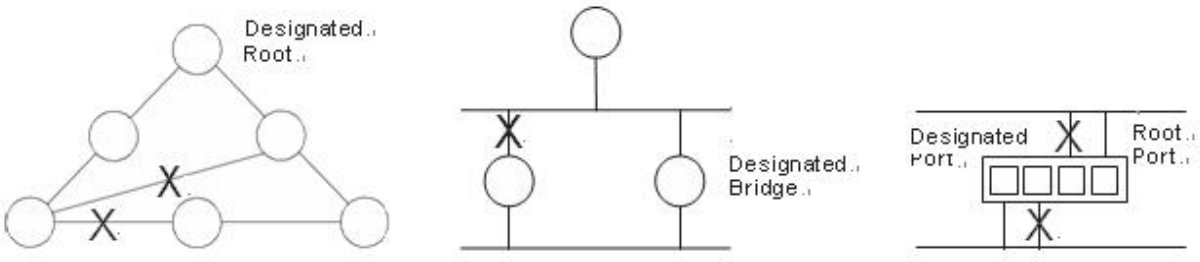


Figure 11-1: The Spanning Tree Protocol

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.

11-1 STP Configuration

This page lets you select and configure a selected protocol version. To configure the Spanning Tree Protocol in the web UI:

1. Click Spanning Tree and STP Configuration.
2. Select the parameters and enter the blank fields in Basic Settings.
3. Enable or disable the parameters and enter parameter values 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.

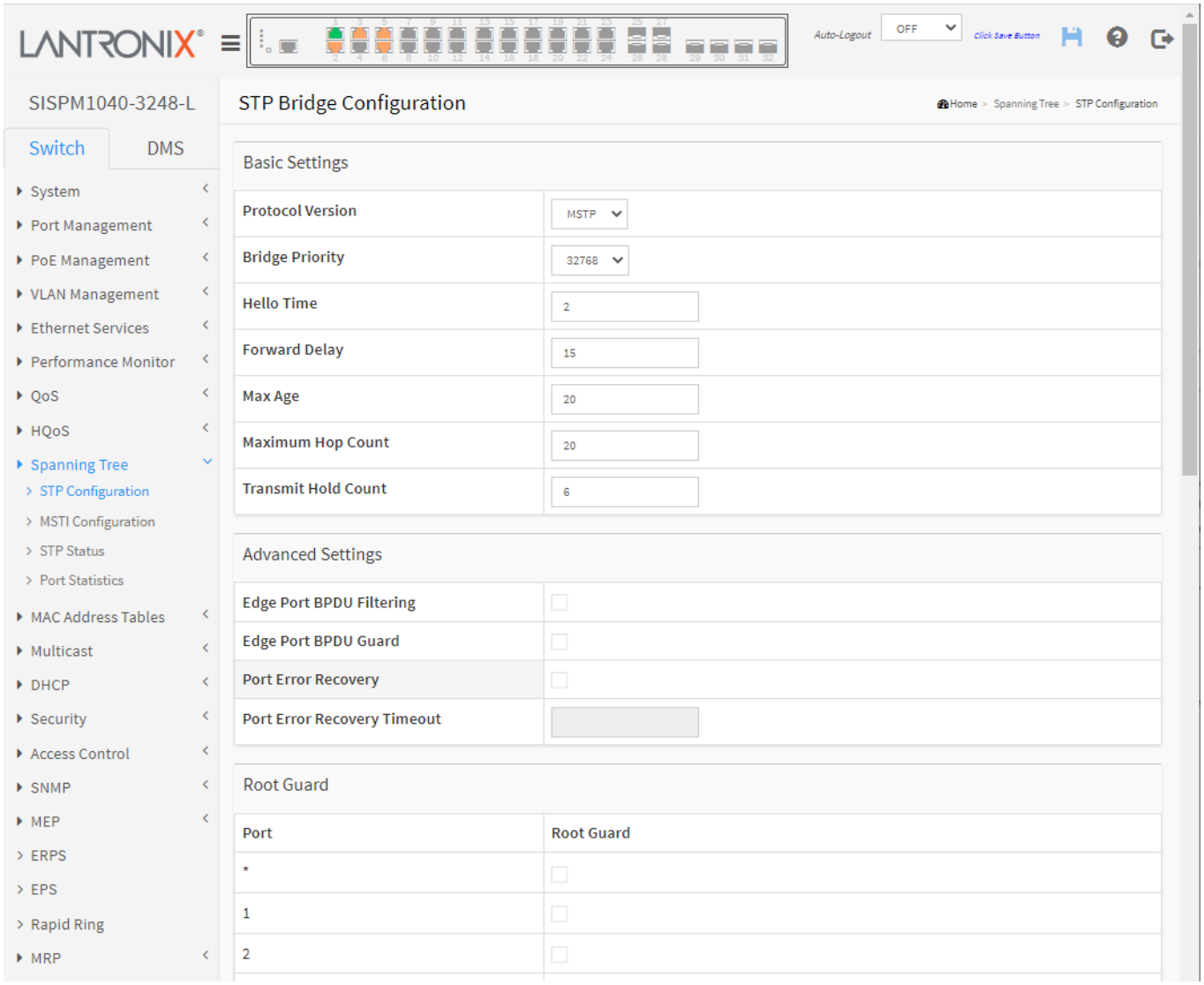


Figure 11-2: STP Configuration

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 BPDU's. Valid values are 1 – 10 seconds; the 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 4 – 30 seconds.

Max Age : The maximum age of the information transmitted by the Bridge when it is the Root Bridge. Valid values are 6 – 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 6 – 40 hops.

Transmit Hold Count : The number of BPDU's a bridge port can send per second. When exceeded, transmission of the next BPDU will be delayed. Valid values are 1 – 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:

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

Root Guard : Root guard allows the device to participate in STP as long as the device does not try to become the root. If root guard blocks the port, subsequent recovery is automatic. Recovery occurs as soon as the offending device ceases to send superior BPDUs.

Buttons

Apply : Click to save changes.

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

11-2 MSTI Configuration

When you implement a Spanning Tree protocol on the switch that the bridge instance. The CIST is not available for explicit mapping, as it will receive the VLANs not explicitly mapped. This is due to the fact 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 have any VLANs mapped to it).

This page lets you view and configure the current STP MSTI bridge instance priority parameters. To configure the Spanning Tree MSTI in the web UI:

1. Click Spanning Tree and MSTI Configuration.
2. Specify the configuration identification parameters in the field.
3. Specify the VLANs Mapped blank field.
4. Click the Apply button to save the setting.
5. To cancel the settings click the Reset button to revert to previously saved values.
6. Click the Edit button to configure the STP CIST Port Configuration.

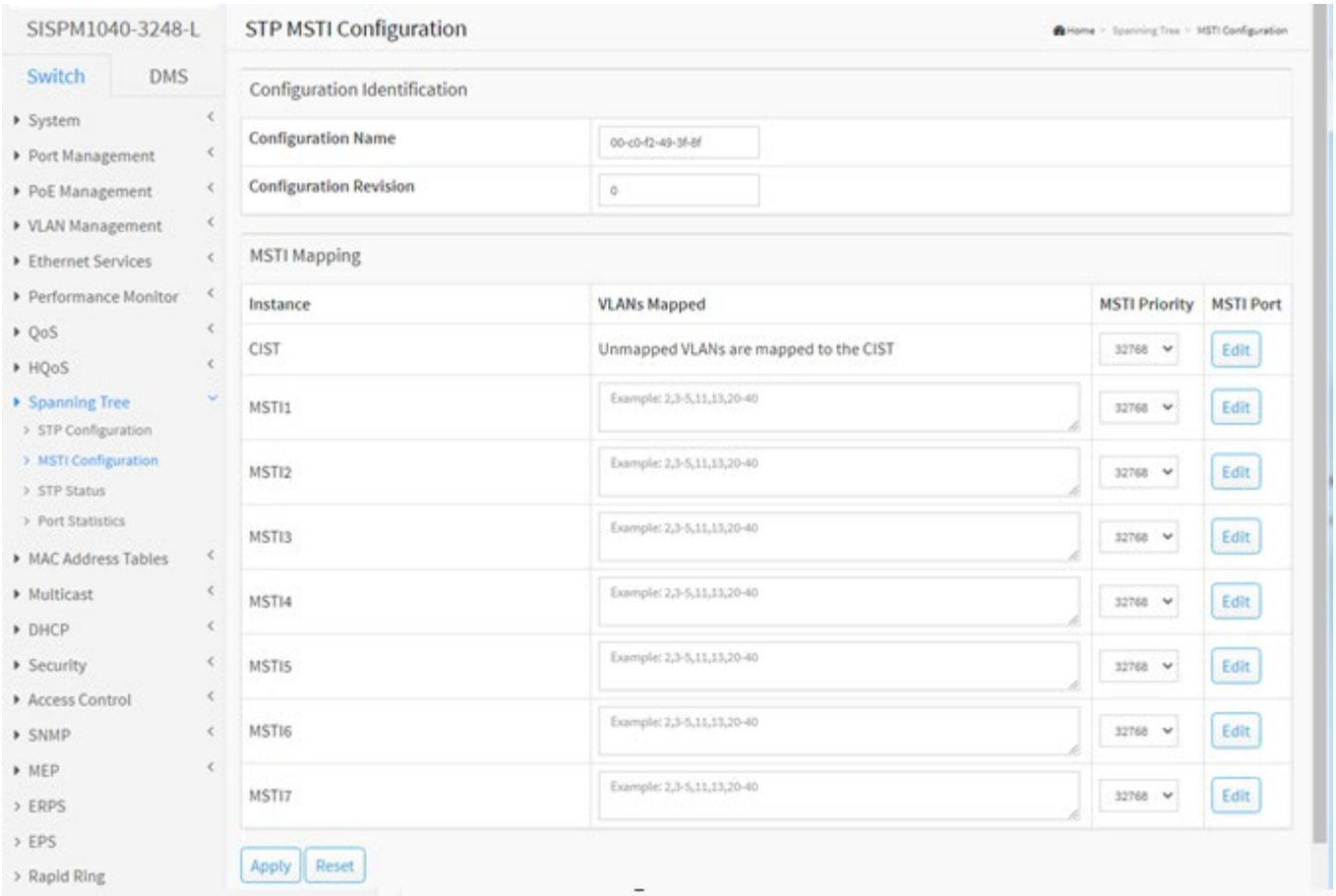


Figure 11-3: STP MSTI Configuration

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). For 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: Click the **Edit** button to configure the STP CIST (or MSTI) Port Configuration as shown and described below.

Buttons

Apply: Click to save changes.

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

Edit: Click the **Edit** button in the **MSTI Port** column to configure the STP CIST (or MSTI) Port Configuration as shown and described below.

STP MSTI Port Configuration

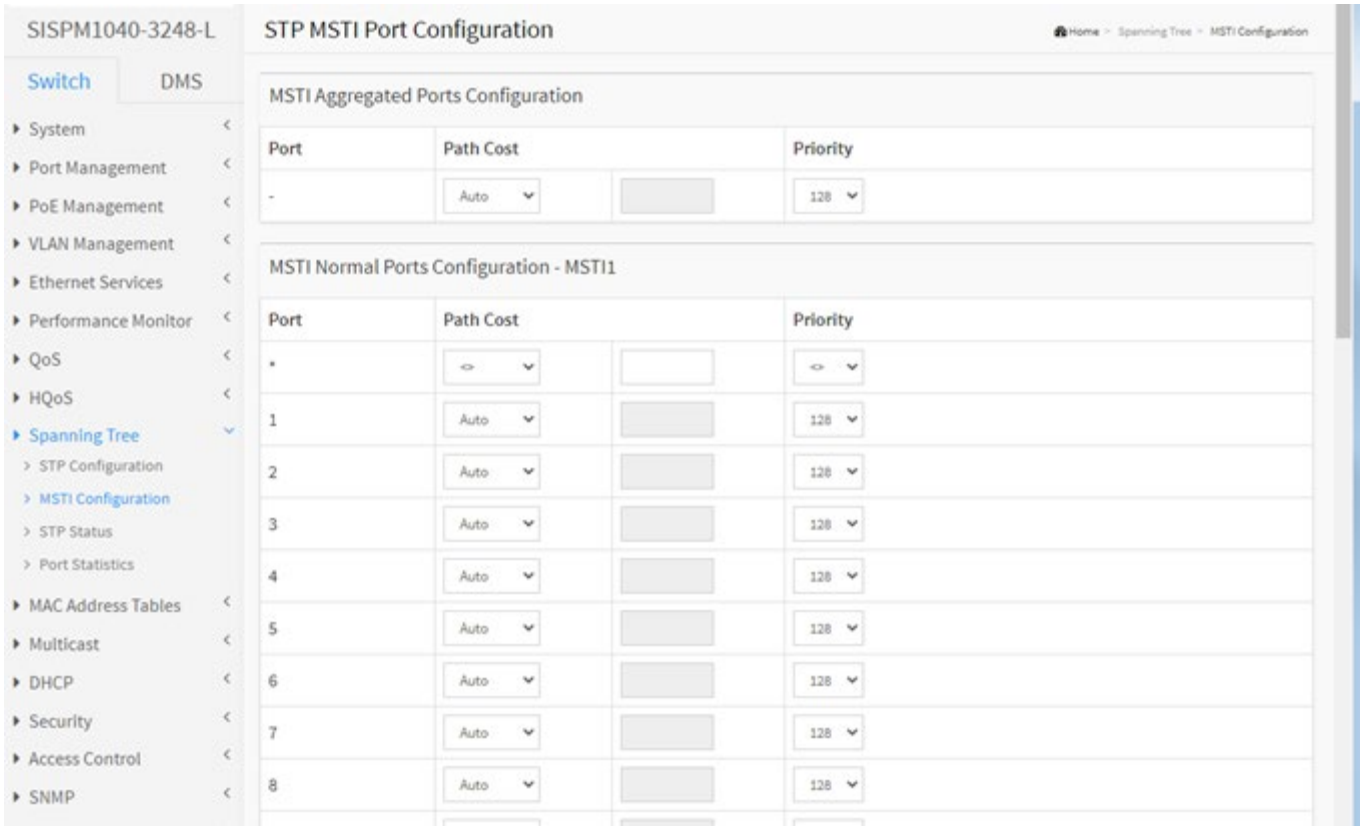


Figure 11-4: STP MSTI Port Configuration

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 : This can be used to control priority of ports having identical port cost. (See above).

AdminEdge : Controls whether the operEdge flag should start as set or cleared. (The initial operEdge state when a port is initialized.)

AutoEdge : Controls whether the bridge should enable automatic edge detection on the bridge port. This allows operEdge to be derived from whether BPDU's are received on the port or not.

Restricted Role : If enabled, causes the port not to be selected as Root Port for the CIST or any MSTI, even if it has the best spanning tree priority vector. Such a port will be selected as an Alternate Port after the Root Port has been selected. If set, it can cause lack of spanning tree connectivity. It can be set by a network administrator to prevent bridges external to a core region of the network influence the spanning tree active topology, possibly

because those bridges are not under the full control of the administrator. This feature is also known as Root Guard.

Restricted TCN : If enabled, causes the port not to propagate received topology change notifications and topology changes to other ports. If set it can cause temporary loss of connectivity after changes in a spanning tree's active topology as a result of persistently incorrect learned station location information. It is set by a network administrator to prevent bridges external to a core region of the network, causing address flushing in that region, possibly because those bridges are not under the full control of the administrator or the physical link state of the attached LANs transits frequently.

BPDU Guard : If enabled, causes the port to disable itself upon receiving valid BPDU's. Contrary to the similar bridge setting, the port Edge status does not affect this setting. A port entering error-disabled state due to this setting is subject to the bridge Port Error Recovery setting as well.

Point to Point : Controls whether the port connects to a point-to-point LAN rather than to a shared medium. This can be automatically determined, or forced either true or false. Transition to the forwarding state is faster for point-to-point LANs than for shared media.

Buttons

Apply : Click to save changes.

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

STP MSTI Port Configuration

This page lets you view and configure the current STP CIST port parameters. This page contains settings for physical and aggregated ports.

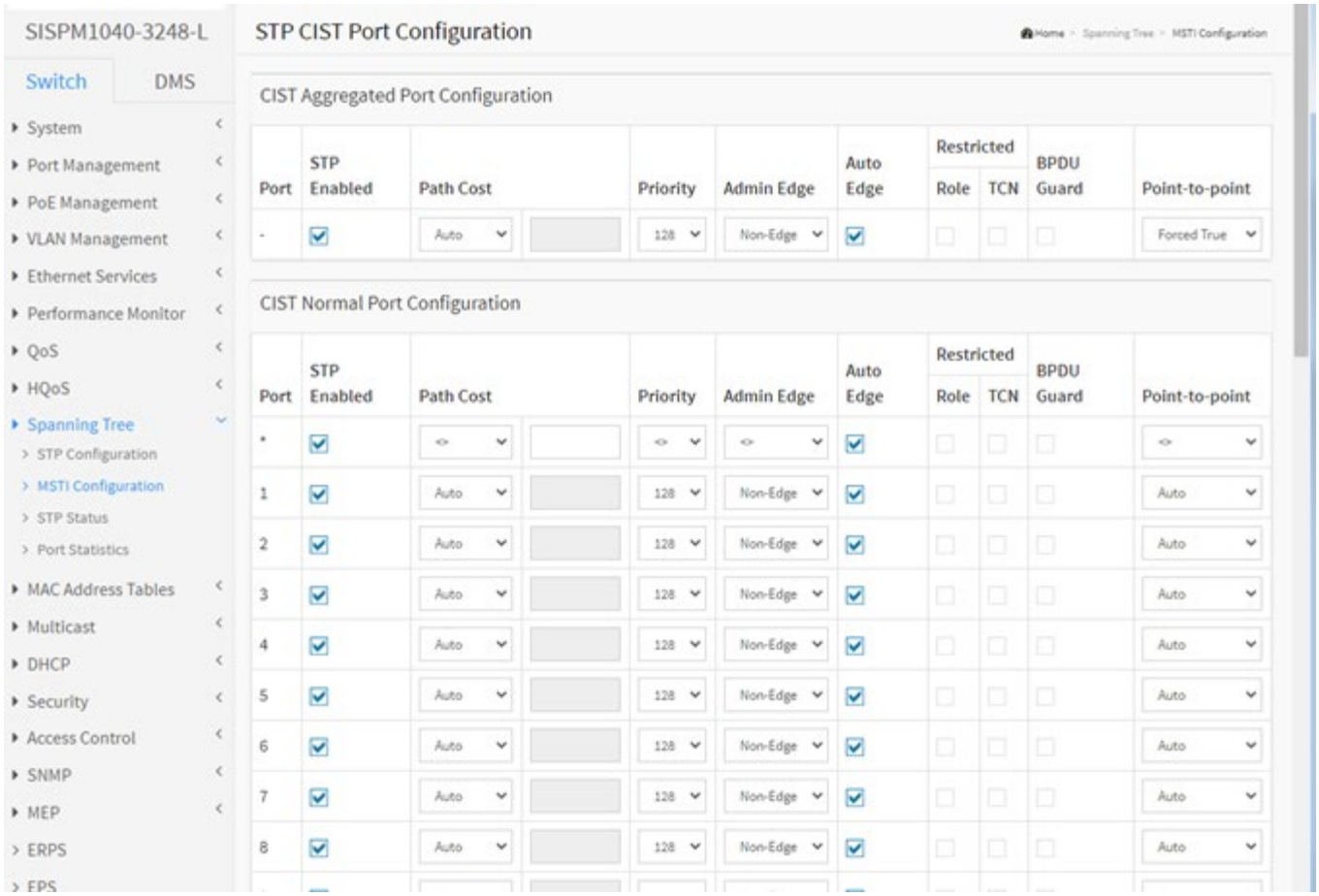


Figure 11-5: STP CIST Port Configuration

Parameter descriptions :

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

STP Enabled : Controls whether STP is enabled on this switch port.

Path Cost : Controls the path cost incurred by the port. The Auto setting will set the path cost as appropriate by the physical link speed, using the 802.1D recommended values. Using the Specific setting, a user-defined value can be entered. The path cost is used when establishing the active topology of the network. Lower path cost ports are chosen as forwarding ports in favor of higher path cost ports. Valid values are in the range 1 to 200000000. Priority : Controls the port priority. This can be used to control priority of ports having identical port cost. (See above). Lower priority is better.

Admin Edge : Controls whether the operEdge flag should start as set or cleared (the initial operEdge state when a port is initialized).

Auto Edge : Controls whether the bridge should enable automatic edge detection on the bridge port. This allows operEdge to be derived from whether BPDU's are received on the port or not.

Restricted Role : If enabled, causes the port not to be selected as Root Port for the CIST or any MSTI, even if it has the best spanning tree priority vector. Such a port will be selected as an Alternate Port after the Root Port has been selected. If set, it can cause lack of spanning tree connectivity. It can be set by a network administrator to prevent bridges external to a core region of the network influence the spanning tree active topology, possibly because those bridges are not under the full control of the administrator. This feature is also known as Root Guard.

Restricted TCN : If enabled, causes the port not to propagate received topology change notifications and topology changes to other ports. If set it can cause temporary loss of connectivity after changes in a spanning tree's active topology as a result of persistently incorrect learned station location information. It is set by a network administrator to prevent bridges external to a core region of the network, causing address flushing in that region, possibly because those bridges are not under the full control of the administrator or the physical link state of the attached LANs transits frequently.

BPDU Guard : If enabled, causes the port to disable itself upon receiving valid BPDU's. Contrary to the similar bridge setting, the port Edge status does not affect this setting. A port entering error-disabled state due to this setting is subject to the bridge Port Error Recovery setting as well.

Point-to-Point : Select whether the port connects to a point-to-point LAN rather than to a shared medium. This can be automatically determined or Forced True or Forced 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.

11-3 STP Status

This page provides a status overview of all STP bridge instances. The displayed table contains a row for each STP bridge instance. To display the STP Bridges status in the web UI:

1. Click Spanning Tree and STP Status.
2. To auto-refresh the information check the “Auto-refresh” box.
3. Click “Refresh” to refresh the STP Bridges.
4. Click “CIST “to go to the “STP Detailed Bridge Status” page.

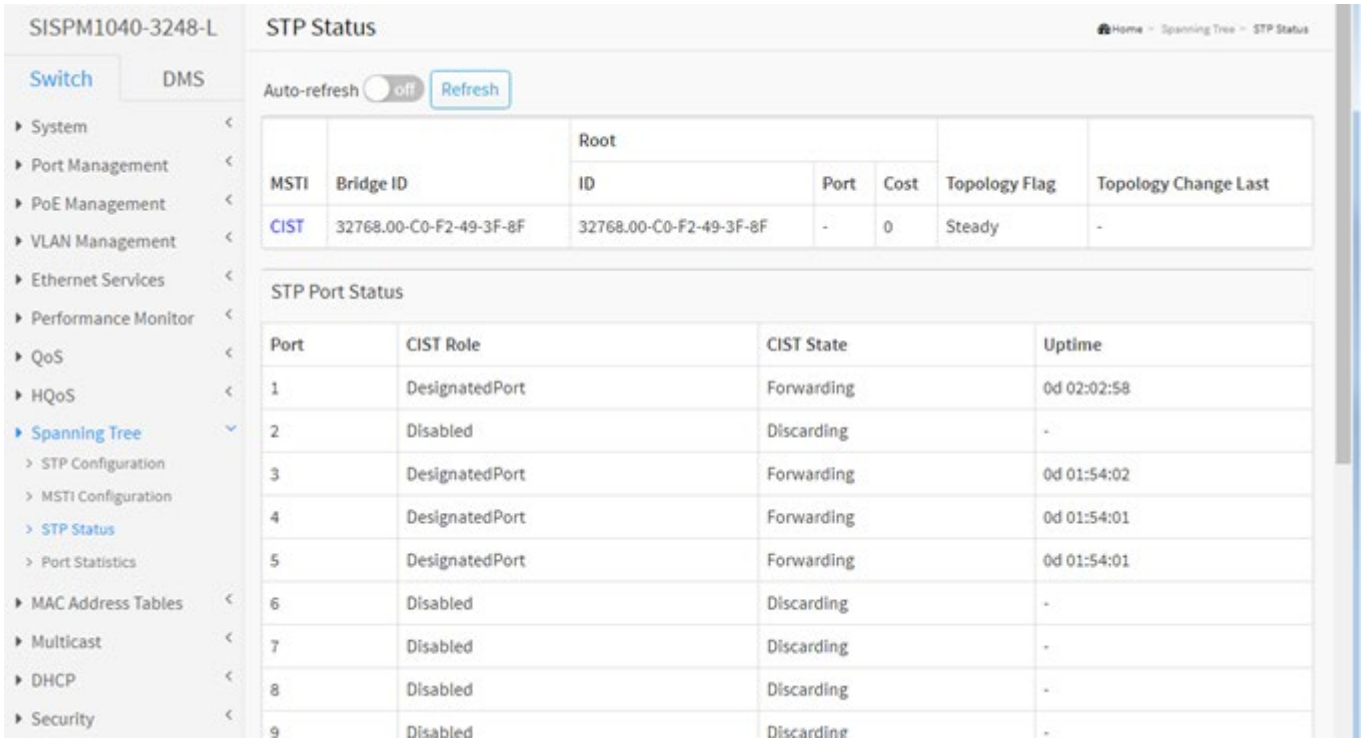


Figure 11-6: STP Status

Parameter descriptions:

MSTI : The Bridge Instance. This is also a link to the STP Detailed Bridge Status.

Bridge ID : The Bridge ID of this Bridge instance.

Root ID : The Bridge ID of the currently elected root bridge.

Root Port : The switch port currently assigned the root port role.

Root Cost : Root Path Cost. For the Root Bridge it is zero. For all other Bridges, it is the sum of the Port Path Costs on the least cost path to the Root Bridge.

Topology Flag : The current state of the Topology Change Flag of this Bridge instance.

Topology Change Last : The time since last Topology Change occurred.

STP Port Status

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

CIST Role : The current STP port role of the CIST port. The port role can be one of the following values: AlternatePort, Backup Port, RootPort, DesignatedPort, or Disabled.

CIST State : The current STP port state of the CIST port. The port state can be one of the following 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 – CIST, MST1, ...

Bridge ID : The Bridge ID of this Bridge instance.

Root ID : The Bridge ID of the currently elected root bridge.

Root Port : The switch port currently assigned the root port role.

Root Cost : Root Path Cost. For the Root Bridge this is zero. For all other Bridges, it is the sum of the Port Path Costs on the least cost path to the Root Bridge.

Regional Root : The Bridge ID of the currently elected regional root bridge, inside the MSTP region of this bridge. (For the CIST instance only.)

Internal Root Cost : The Regional Root Path Cost. For the Regional Root Bridge this is zero. For all other CIST instances in the same MSTP region, it is the sum of the Internal Port Path Costs on the least cost path to the Internal Root Bridge. (For the CIST instance only.)

Topology Flag : The current state of the Topology Change Flag of this Bridge instance.

Topology Change Count : The number of times where the topology change flag has been set (during a one-second interval).

Topology Change Last : The time passed since the Topology Flag was last set.

CIST Ports & Aggregations State

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

Port ID : The port id as used by the STP protocol; the priority part and the logical port index of the bridge port.

Role : The current STP port role. The port role can be one of the following values: AlternatePort, BackupPort, RootPort, or DesignatedPort.

State : The current STP port state. The port state can be one of the following 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.

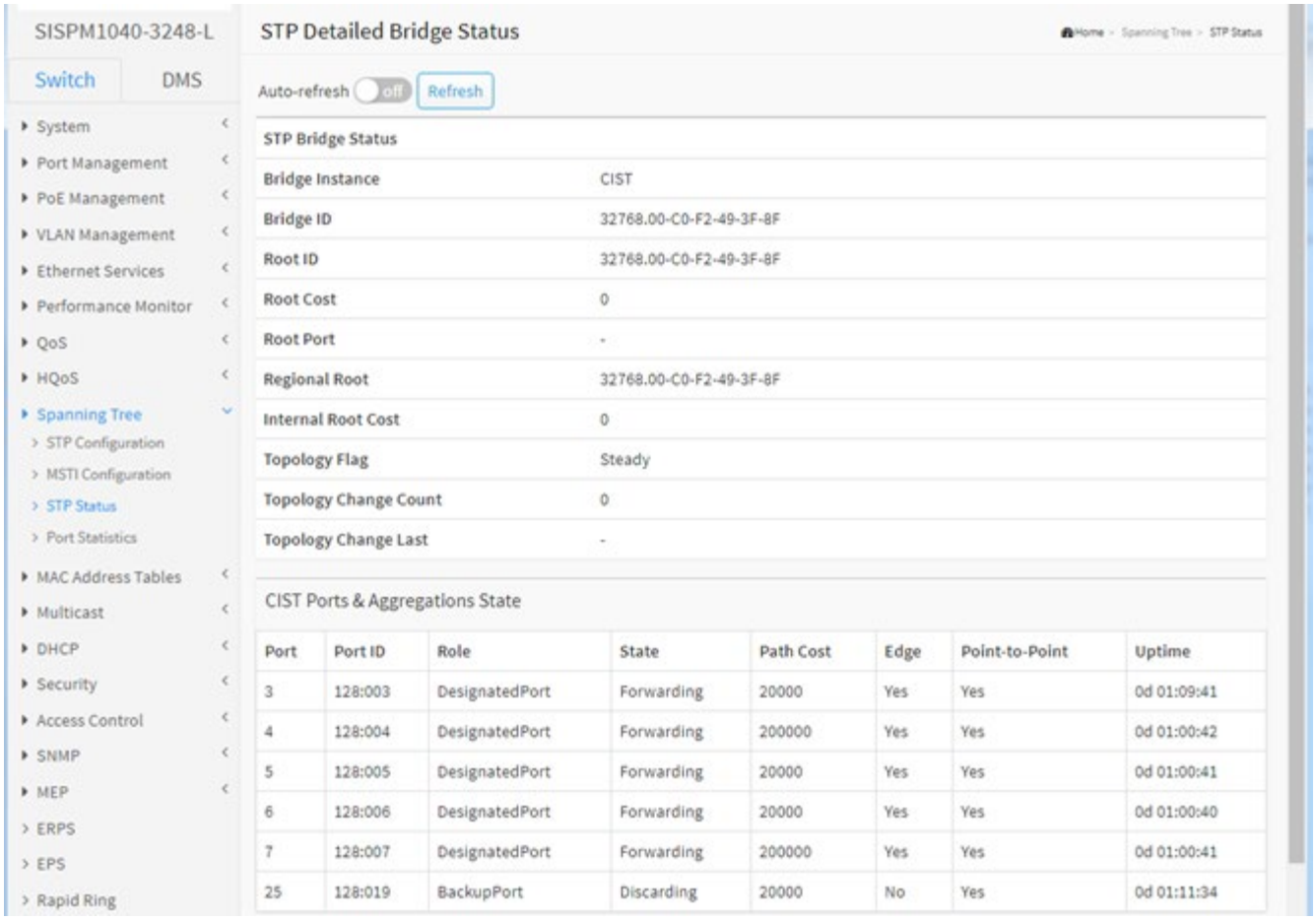
Uptime : The time since the bridge port was last initialized.

Buttons

Auto-refresh : Click to refresh the page automatically every 3 seconds.

Refresh : Click to refresh the page.

Example: STP Detailed Bridge Status for Bridge Instance “CIST”:



11-4 Port Statistics

This page displays the STP port statistics counters of bridge ports in the switch. To display the STP Port Statistic in the web UI:

1. Click Spanning Tree and Port Statistics.
2. To auto-refresh the information check the “Auto-refresh” box.
3. Click “Refresh” to refresh the page.

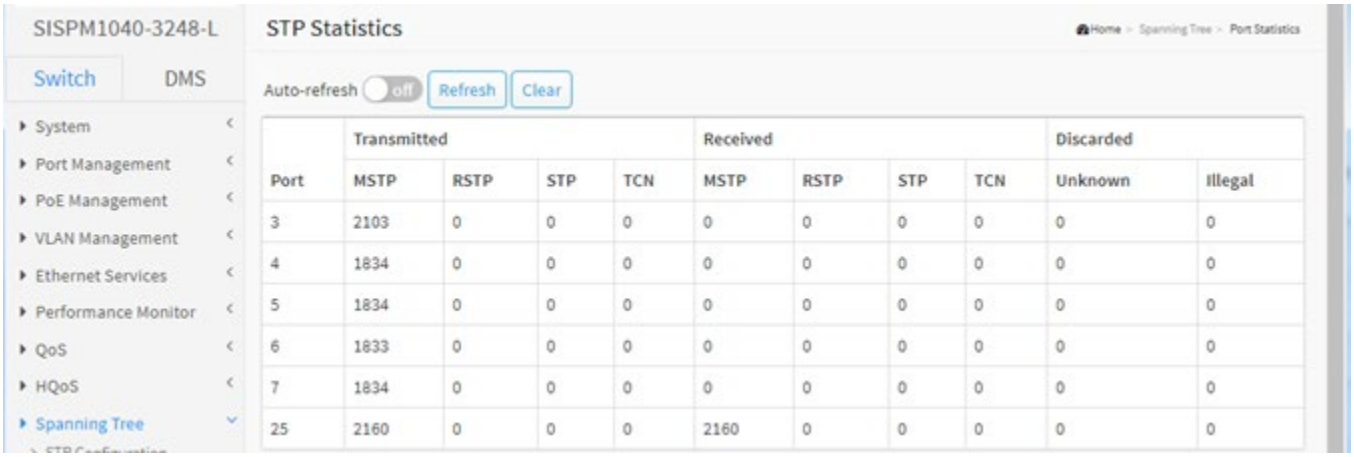


Figure 11-7: STP Port Statistics

Parameter descriptions:

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

MSTP : The number of MSTP Configuration BPDU’s received/transmitted on the port.

RSTP : The number of RSTP Configuration BPDU’s received/transmitted on the port.

STP : The number of legacy STP Configuration BPDU’s received/transmitted on the port.

TCN : The number of (legacy) Topology Change Notification BPDU’s received/transmitted on the port.

Discarded Unknown : The number of unknown Spanning Tree BPDU’s received (and discarded) on the port.

Discarded Illegal : The number of illegal Spanning Tree BPDU’s received (and discarded) on the port.

Buttons

Auto-refresh : Click to refresh the page automatically every 3 seconds.

Refresh : Click to manually refresh the page immediately.

Chapter 12 - MAC Address Tables

12-1 Configuration

Switching of frames is based upon the DMAC address contained in the frame. The switch builds up a table that maps MAC addresses to switch ports for knowing which ports the frames should go to (based upon the DMAC address in the frame). This table contains both static and dynamic entries. Static entries are configured by the network administrator if they want 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 has been seen after a configurable age time

To configure MAC Address Table parameters in the web UI:

1. Click MAC Address Tables and Configuration.
2. Specify 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 IP, Mac address, and Port Members.
6. Click Apply.

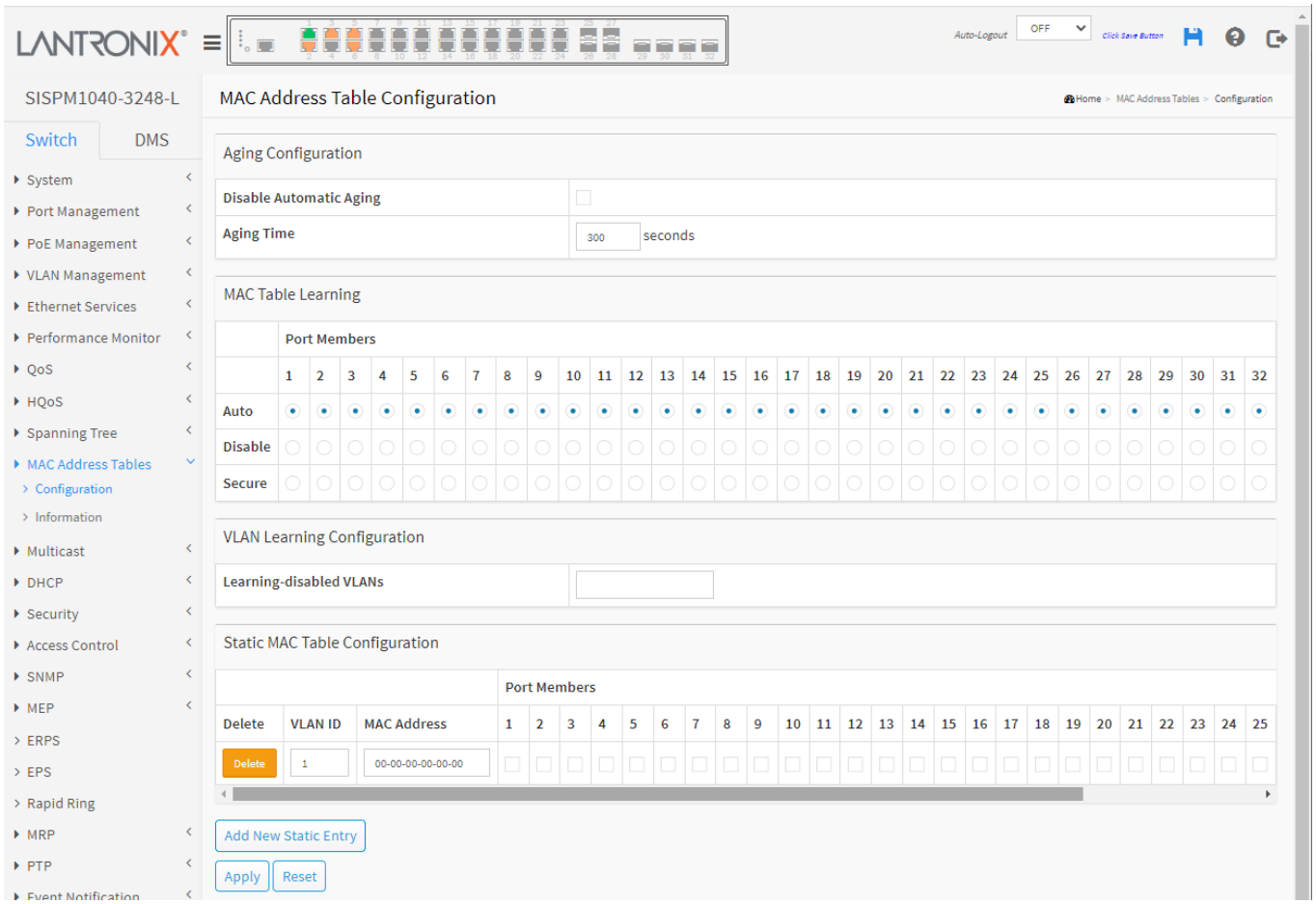


Figure 12-1: MAC Address Table Configuration

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; for example, Age time seconds. The allowed range is 10 to 1000000 seconds. Disable the automatic aging of dynamic entries by checking ☑ Disable automatic aging.

MAC Table Learning: If the learning mode for a given port is greyed out, another module is in control of the mode, so that it cannot be changed by the user. An example of such a module is the MAC-Based Authentication under 802.1X. Each port can do learning based upon the following settings:

Auto : Learning is done automatically as soon as a frame with unknown SMAC is received.

Disable : No learning is done.

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

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

VLAN Learning Configuration

Learning-disabled VLANS : This field shows the Learning-disabled VLANs. When a NEW MAC arrives into a learning-disabled VLAN, the MAC won't be learnt. By the default, the field is empty. More VLANs may be created by using a list syntax where the individual elements are separated by commas. Ranges are specified with a dash separating the lower and upper bound. The following example will create VLANs 1, 10, 11, 12, 13, 200, and 300: 1,10-13,200,300. Spaces are allowed in between the delimiters.

Static MAC Table Configuration: Up to 128 static entries in the MAC table are shown in this table..

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 immediately.

Apply : Click to save changes.

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

Message: *Error: mac address:00-00-00-00-00-00 is not multicast mac address, support only one port.*
Message*: No port members selected for VLAN ID: 11 and MAC address: 11-00-00-00-00-00. This will block the MAC address for all ports. Is this correct?*

12-2 Information

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

1. Click MAC Address Tables > Information.
2. Select Start from VLAN, MAC address, and entries per page.
3. To automatically refresh the information every 3 seconds click “Auto-refresh”.
4. Click “Refresh” to manually refresh the page immediately.

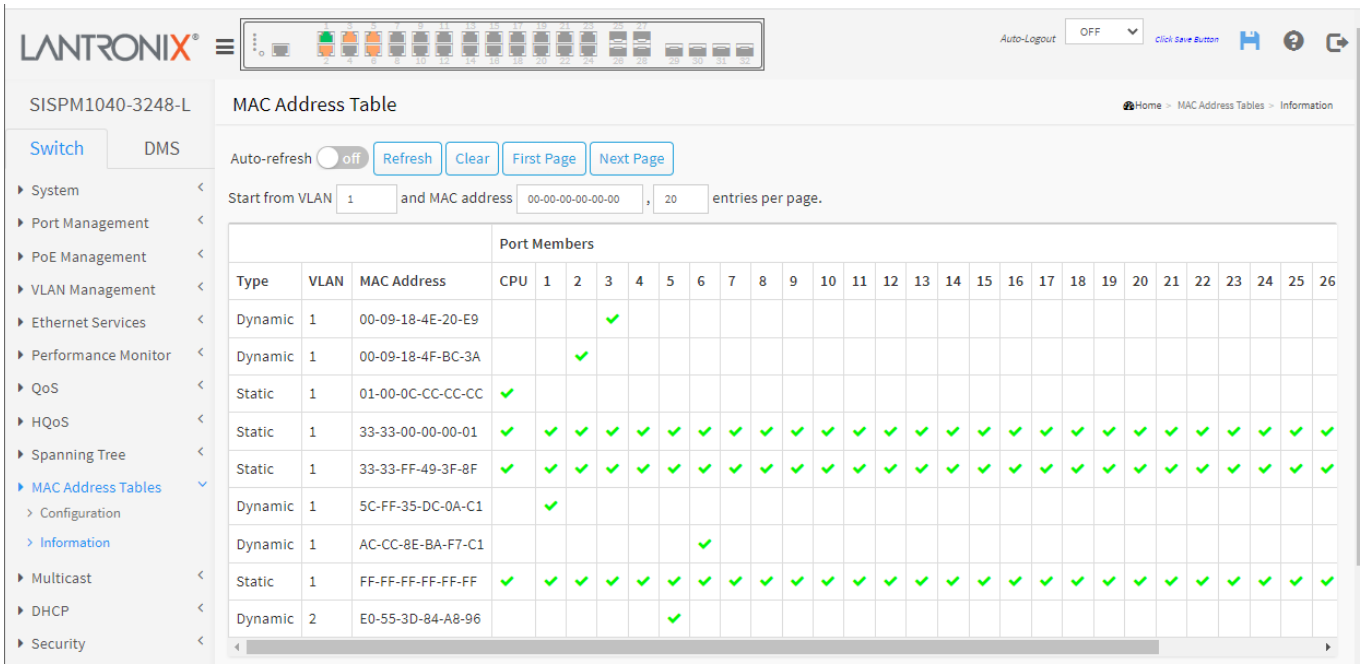


Figure 12-2: MAC Address Table Information

Each page shows up to 999 entries from the MAC table, default being 10, selected through the "entries per page" input field. When first visited, the web page will show the first 10 entries from the beginning of the MAC Table. The first displayed will be the one with the lowest VLAN ID and the lowest MAC address found in the MAC Table.

Parameter descriptions:

Type : Indicates whether the entry is a static or a dynamic entry, 802.1x, DMS.

VLAN : The VLAN ID of the entry.

MAC address : The MAC address of the entry.

Port Members : The ports that are members of the entry.

Buttons

Auto-refresh : Click to refresh the page automatically every 3 seconds.

Refresh : Click to refresh the page.

Clear : Click to clear the page.

First Page : Updates the system log entries, turn to the first page.

Next Page : Updates the system log entries, turn to the next page.

NOTE:

00-40-C7-73-01-29 : your switch MAC address (for IPv4)

33-33-00-00-00-01 : Destination MAC (for IPv6 Router Advertisement) (reference IPv6 RA.JPG)

33-33-00-00-00-02 : Destination MAC (for IPv6 Router Solicitation) (reference IPv6 RS.JPG)

33-33-FF-73-01-29 : Destination MAC (for IPv6 Neighbor Solicitation) (reference IPv6 DAD.JPG)

33-33-FF-A8-01-01: your switch MAC address (for IPv6 global IP)

FF-FF-FF-FF-FF-FF: for Broadcast.

Chapter 13 - Multicast

13-1 IGMP Snooping

IGMP Snooping 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 broadcast packets. Without IGMP Snooping, the multicast packet forwarding function is plain and nothing is different from broadcast packets.

A switch supporting IGMP Snooping with query, report and leave (a type of packet exchanged between IP Multicast Router/Switch and IP Multicast Host) functions 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 a multicast group that had not been built up in advance. IGMP mode lets the switch issue IGMP function that you enable IGMP proxy or snooping on the switch, which connects to a router closer to the root of the tree. This interface is the upstream interface. The router on the upstream interface should be running IGMP.

13-1.1 Basic Configuration

This page lets you set the basic IGMP snooping on the switch, which connects to a router closer to the root of the tree. This interface is the upstream interface. The router on the upstream interface must be running IGMP.
To configure IGMP Snooping parameters in the web UI:

1. Click Multicast, IGMP Snooping and Basic Configuration.
2. Enable or disable Global configuration parameters.
3. Select the port want to become a Router Port or enable/ disable the Fast Leave function.
4. Set Throttling and Profile, then click the Apply button to save the settings.

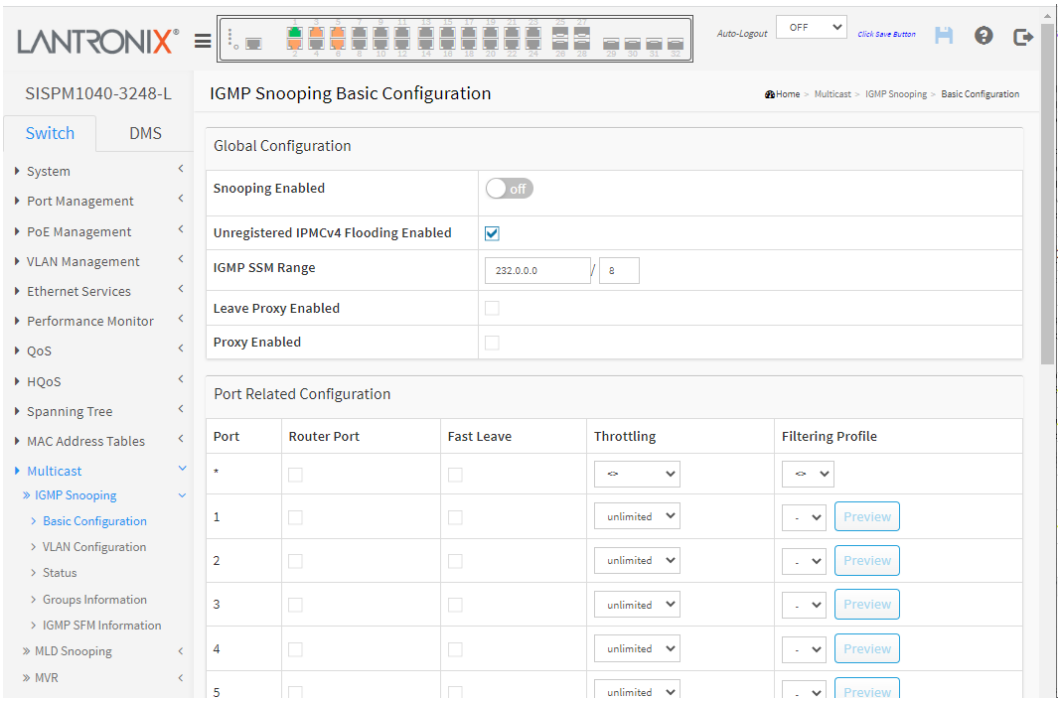


Figure 13-1.1: IGMP Snooping Basic Configuration

Parameter descriptions:

Global Configuration

Snooping Enabled : Enable Global IGMP Snooping.

Unregistered IPMCv4 Flooding enabled : Enable unregistered IPMCv4 traffic flooding. Unregistered IPMCv4 traffic is so-called unknown multicast. After selected, the unregistered multicast stream will be forwarded like normal packets. Once you un-selected it, such stream will be discarded

IGMP SSM Range : SSM (Source-Specific Multicast) Range allows the SSM-aware hosts and routers run the SSM service model for the groups in the address range. Format: (IP address/ sub mask).

Leave Proxy Enabled : Enable IGMP Leave Proxy. This feature can be used to avoid forwarding unnecessary leave messages to the router side.

Proxy Enabled : Enable IGMP Proxy. This feature can be used to avoid forwarding unnecessary join and leave messages to the router side.

Port Related Configuration

Port : 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 lists 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.

13-1.2 VLAN Configuration

This page lets you configure the VLAN settings for the process integrated with the IGMP Snooping function.
To configure the IGMP Snooping VLAN Configuration in the web UI:

1. Click Multicast, IGMP Snooping and VLAN Configuration.
2. Click the Add New IGMP VLAN button.
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

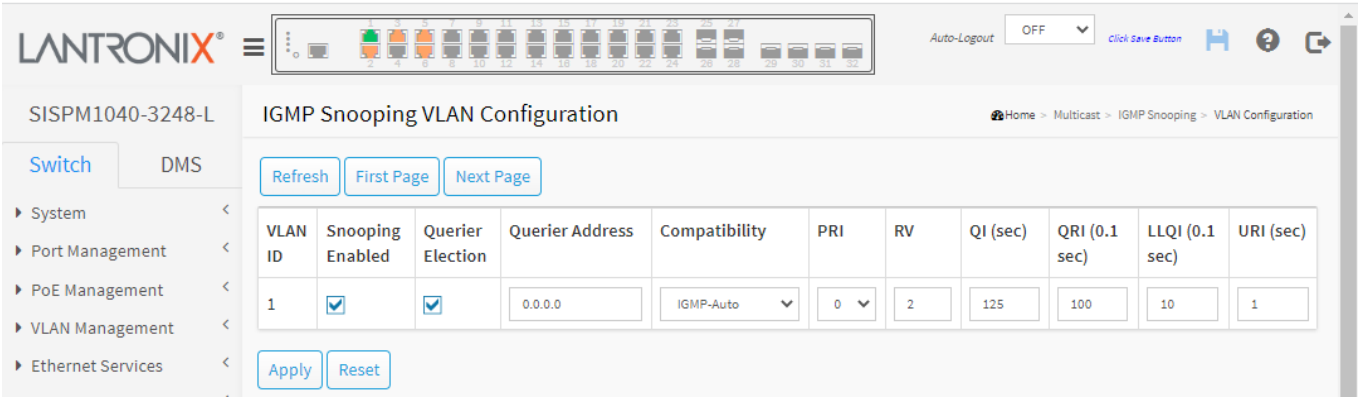


Figure 13-1.2: IGMP Snooping VLAN Configuration

Parameter descriptions:

VLAN ID : Displays the VLAN ID of the entry.

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, system uses a pre-defined value. By default, this value will be 192.0.2.1.

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, or Forced IGMPv3. The default compatibility value is IGMP-Auto.

PRI : Priority of Interface indicates the IGMP control frame priority level generated by the system. These values can be used to prioritize different classes of traffic. The allowed range is 0 (best effort) to 7 (highest). The default PRI value is 0.

Rv : Robustness Variable. The Robustness Variable allows tuning for the expected packet loss on a network. The allowed range is 1 to 255; the default RV value is 2.

QI(sec) : Query Interval. The QI is the interval between General Queries sent by the Querier. The allowed 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 allowed range is 0 to 31744 in tenths of seconds; the default QRI is 100 in tenths of seconds (10 seconds).

LLQI (0.1 sec) : The Last Member Query Time is the time value represented by the Last Member Query Interval, multiplied by the Last Member Query Count. The allowed range is 0 to 31744 in tenths of seconds; the default 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 allowed 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.

13-1.3 Status

This page displays IGMP Snooping detail status. To display IGMP Snooping status in the web UI:

1. Click Multicast, IGMP Snooping and Status.
2. To automatically refresh the page every 3 seconds click “Auto-refresh”.
3. Click “Refresh” to refresh the IGMP Snooping Status.

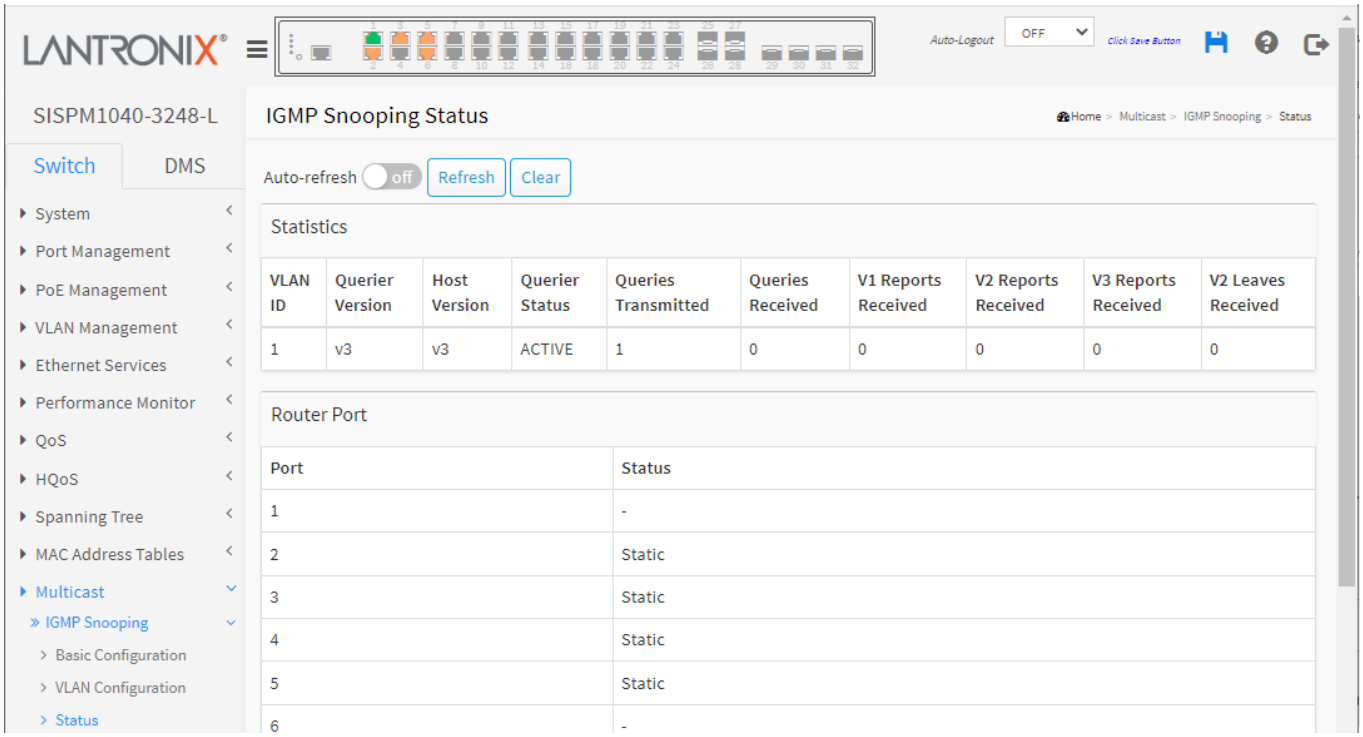


Figure 13-1.3: IGMP Snooping Status

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 is "ACTIVE" or "IDLE". "DISABLE" denotes the specific interface is administratively disabled.

Queries Transmitted : The number of Transmitted Queries.

Queries Received : The number of Received Queries.

V1 Reports Received : The number of Received V1 Reports.

V2 Reports Received : The number of Received V2 Reports.

V3 Reports Received : The number of Received V3 Reports.

V2 Leaves Received : The number of Received V2 Leaves.

Router Port: 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 : Switch port number.

Status : Indicate whether specific port is a router port.

Buttons

Auto-refresh : Click to refresh the page automatically every 3 seconds.

Refresh : Click to manually refresh the page immediately.

Clear : Click to clear the page.

13-1.4 Groups Information

After you configure IGMP Snooping the switch can display 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*" displays in the table.

To display the IGMP Snooping Group Information in the web UI:

1. Click Multicast, IGMP Snooping and Groups Information.
2. Specify how many entries to show in one page.
3. To auto-refresh the information check the “Auto-refresh” box.
4. Click “Refresh” to refresh the page.
5. Click the First/Next Page to change pages.

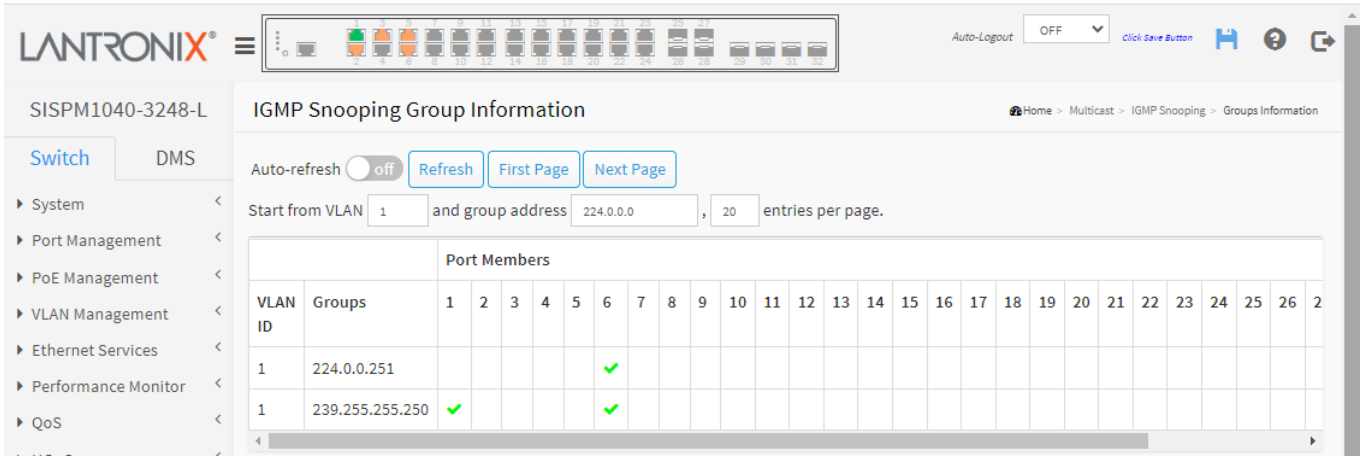


Figure 13-1.4: IGMP Snooping Groups Information

Parameter descriptions :

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.

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

Entries per page: Choose how many items you want displayed; the default is 20.

VLAN ID : VLAN ID of the group.

Groups : Group address of the group displayed.

Port Members : Ports under this group.

Buttons

Auto-refresh : Click to refresh the page automatically every 3 seconds.

Refresh : Click to manually refresh the page immediately.

First Page : Updates the system log entries, turn to the first page.

Next Page : Updates the group information entries, turn to the next page.

13-1.5 IGMP SFM Information

Entries in the IGMP SFM Information Table are shown on this page. The IGMP SFM (Source-Filtered Multicast) Information Table also contains the SSM (Source-Specific Multicast) information. This table is sorted first by VLAN ID, then by group, and then by Port. Different source addresses that belong to the same group are treated as a single entry.

To display IGMP SFM Information in the web UI:

1. Click Multicast, IGMP Snooping and IGMP SFM Information
2. To auto-refresh the information check the “Auto-refresh” box.
3. Click “Refresh” to refresh an entry of the IGMP Snooping Groups Information.
4. Click First/Next Page to change page.

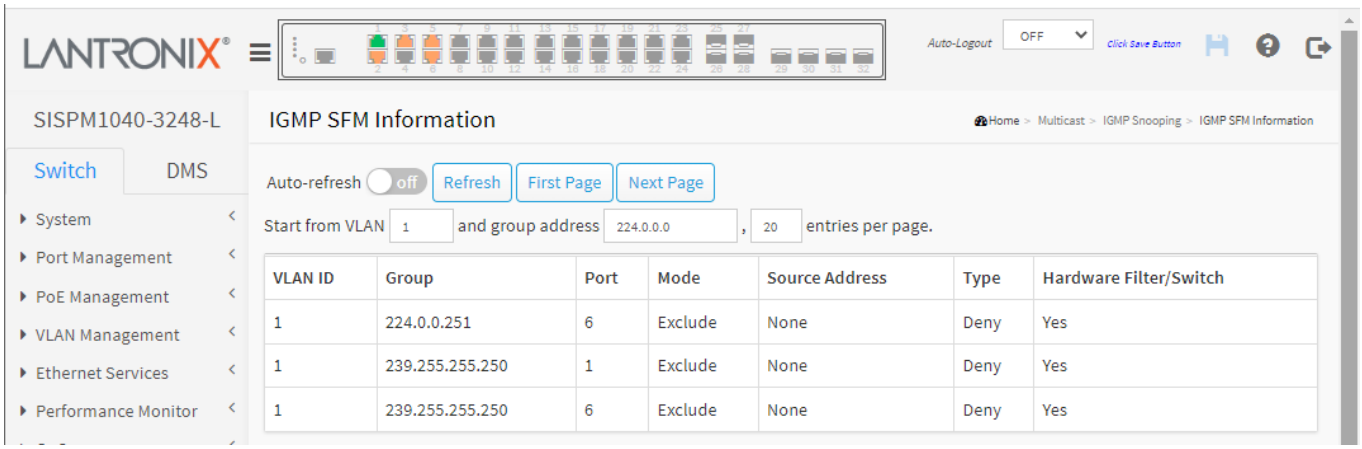


Figure 13-1.5: IGMP SFM Information

Parameter descriptions:

Each page shows up to 99 entries from the IGMP SFM Information table, default being 20, selected through the "entries per page" input field. When first visited, the web page will show the first 20 entries from the beginning of the IGMP SFM Information Table.

The "Start from VLAN", and "group" input fields allow the user to select the starting point in the IGMP SFM Information Table. Clicking the Refresh button will update the displayed table starting from that or the closest next IGMP SFM Information Table match. In addition, the two input fields will - upon a Refresh button click - assume the value of the first displayed entry, allowing for continuous refresh with the same start address.

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

entries per page : Lets you choose how many items you want to be displayed per page.

VLAN ID : VLAN ID of the group.

Group : Group address of the group displayed.

Port : Switch port number.

Mode : Indicates the filtering mode maintained per (VLAN ID, port number, Group Address) basis. It can be either ***Include*** or ***Exclude***.

Source Address : IP Address of the source. Currently, system limits the total number of IP source addresses for filtering to 128.

Type : Indicates the Type. It can be either ***Allow*** or ***Deny***.

Hardware Filter/Switch : Indicates whether data plane destined to the specific group address from the source IPv4 address could be handled by chip.

Buttons

Auto-refresh : Click to refresh the page automatically every 3 seconds.

Refresh : Click to manually refresh the page immediately.

First Page : Updates the system log entries, turn to the first page.

Next Page : Updates the group information entries, turn to the next page.

13-2 MLD Snooping

Curiously enough, a network node that acts as a source of IPv6 multicast traffic is only an indirect participant in MLD snooping—it just provides multicast traffic, and MLD doesn't interact with it. (Note, however, that in an application like desktop conferencing a network node may act as both a source and an MLD host; but MLD interacts with that node only in its role as an MLD host.)

A source node creates multicast traffic by sending packets to a multicast address. In IPv6, addresses with the first eight bits set (that is, "FF" as the first two characters of the address) are multicast addresses, and any node that listens to such an address will receive the traffic sent to that address. Application software running on the source and destination systems cooperates to determine what multicast address to use. (Note that this is a function of the application software, not of MLD.)

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

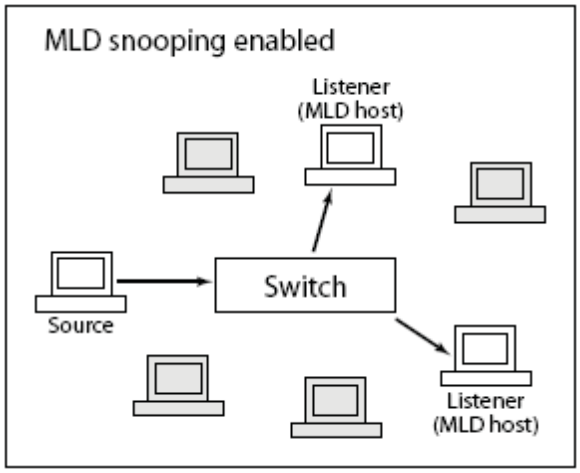


Figure 3-2: MLD snooping enable

13-2.1 Basic Configuration

This page lets you configure MLD Snooping basic parameters. 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.

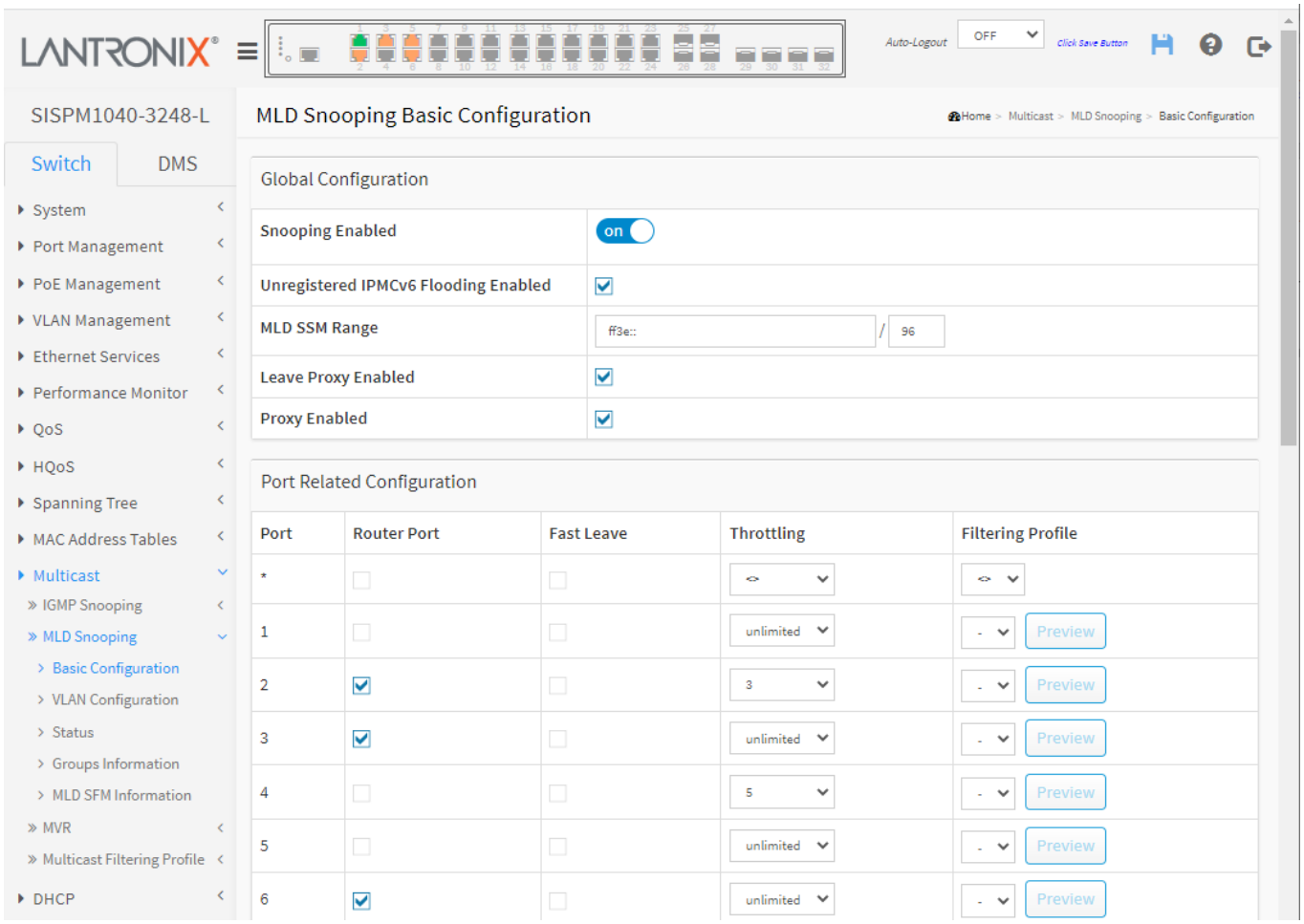


Figure 13-2.1: MLD Snooping Basic Configuration

Parameter descriptions :

Global Configuration

Snooping Enabled : Enable the Global MLD Snooping.

Unregistered IPMCv6 Flooding enabled : Enable unregistered IPMCv6 traffic flooding. The flooding control takes effect only when MLD Snooping is enabled. When MLD Snooping is disabled, unregistered IPMCv6 traffic flooding is always active in spite of this setting.

MLD SSM Range : SSM (Source-Specific Multicast) Range allows the SSM-aware hosts and routers run the SSM service model for the groups in the address (Using IPv6 Address) range.

Leave Proxy Enabled : Enable MLD Leave Proxy. This feature can be used to avoid forwarding unnecessary leave messages to the router side.

Proxy Enabled :Enable MLD Proxy. This feature can be used to avoid forwarding unnecessary join and leave messages to the router side.

Port Related Configuration

Router Port : Specify which ports act as router ports. A router port is a port on the Ethernet switch that leads towards the Layer 3 multicast device or MLD querier. If an aggregation member port is selected as a router port, the whole aggregation will act as a router port.

Fast Leave : To enable the fast leave on the port.

Throttling : Enable to limit the number of multicast groups to which a switch port can belong.

Filtering Profile : You can select a profile when you edit in Multicast Filtering Profile.

Preview: Click the button to display a preview of the instance.

13-2.2 VLAN Configuration

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

To configure MLD Snooping VLAN parameters in the web UI:

1. Click Multicast, MLD Snooping, and VLAN Configuration.
2. Click Add New MLD VLAN.
3. Specify the MLD Snooping VLAN parameters.

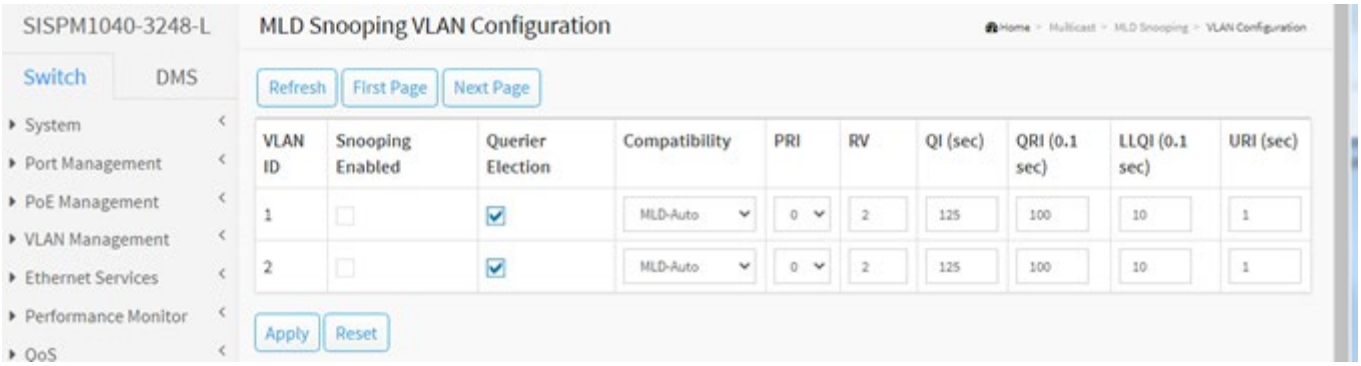


Figure 13-2.2: MLD Snooping VLAN Configuration

Parameter descriptions :

VLAN ID : Displays the VLAN ID of the entry.

Snooping Enabled : Enable the per-VLAN IGMP Snooping. Up to 32 VLANs can be enabled.

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 IGMP-Auto, Forced IGMPv1, and Forced IGMPv2. The default Compatibility value is IGMP-Auto.

PRI : Priority of Interface indicates the MLD control frame priority level generated by the system. These values can be used to prioritize different classes of traffic. The allowed range is 0 (best effort) to 7 (highest); the default interface PRI value is 0.

RV : Robustness Variable. The RV allows tuning for the expected packet loss on a network. The allowed 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 allowed 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 allowed range is 0 to 31744 in tenths of seconds; the default QRI is 100 in tenths of seconds (10 seconds).

LLQI (LMQI for IGMP) : Last Member Query Interval. The Last Member Query Time is the time value represented by the Last Member Query Interval, multiplied by the Last Member Query Count. The allowed range is 0 to 31744 in tenths of seconds; 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 allowed range is 0 to 31744 seconds; the default URI 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.

13-2.3 Status

This page displays MLD Snooping Status and detail information. To display MLD Snooping Status in the web UI:

1. Click Multicast, MLD Snooping and Status.
2. To auto-refresh the information check “Auto-refresh”
3. Click “Refresh” to refresh an entry of the MLD Snooping Status Information.

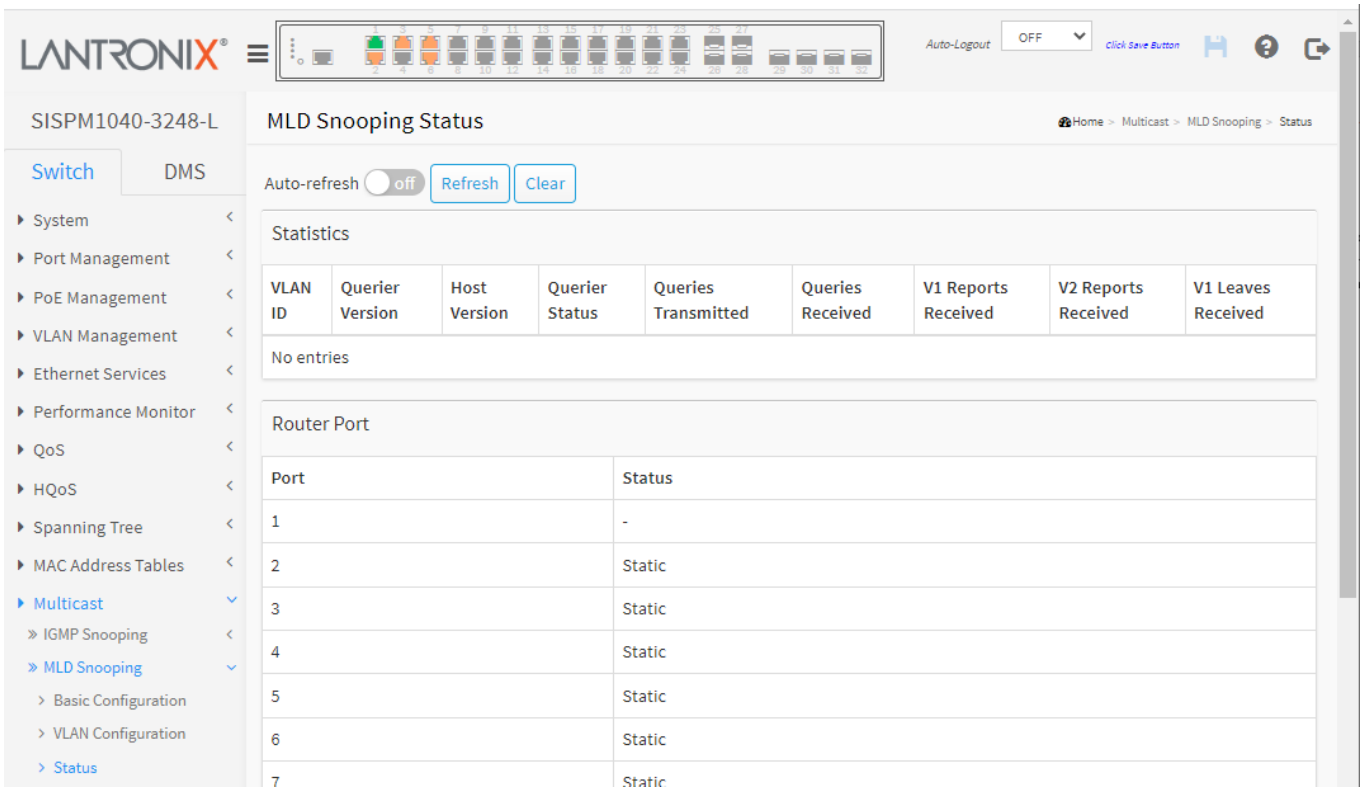


Figure 13-2.3: MLD Snooping Status

Statistics:

VLAN ID : The VLAN ID of the entry.

Querier Version : Working Querier Version currently.

Host Version : Working Host Version currently.

Querier Status : Show the Querier status is "ACTIVE" or "IDLE". "DISABLE" denotes the specific interface is administratively disabled.

Queries Transmitted : The number of Transmitted Queries.

Queries Received : The number of Received Queries.

V1 Reports Received : The number of Received V1 Reports.

V2 Reports Received : The number of Received V2 Reports.

V1 Leaves Received : The number of Received V1 Leaves.

Router Port: 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 MLD querier.

Port : Switch port number.

Status : Indicates whether specific port is a router port.

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 denotes the specific port is configured or learnt to be a router port.

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.

13-2.4 Groups Information

Entries in the MLD Group Table are shown on this page. The MLD Group Table is sorted first by VLAN ID, and then by group. To display MLD Snooping Group information in the web UI:

1. Click Multicast, MLD Snooping, and Group Information.
2. To automatically refresh the page every 3 seconds click “Auto-refresh”
3. Click “Refresh” to refresh an entry of the MLD Snooping Group Information.

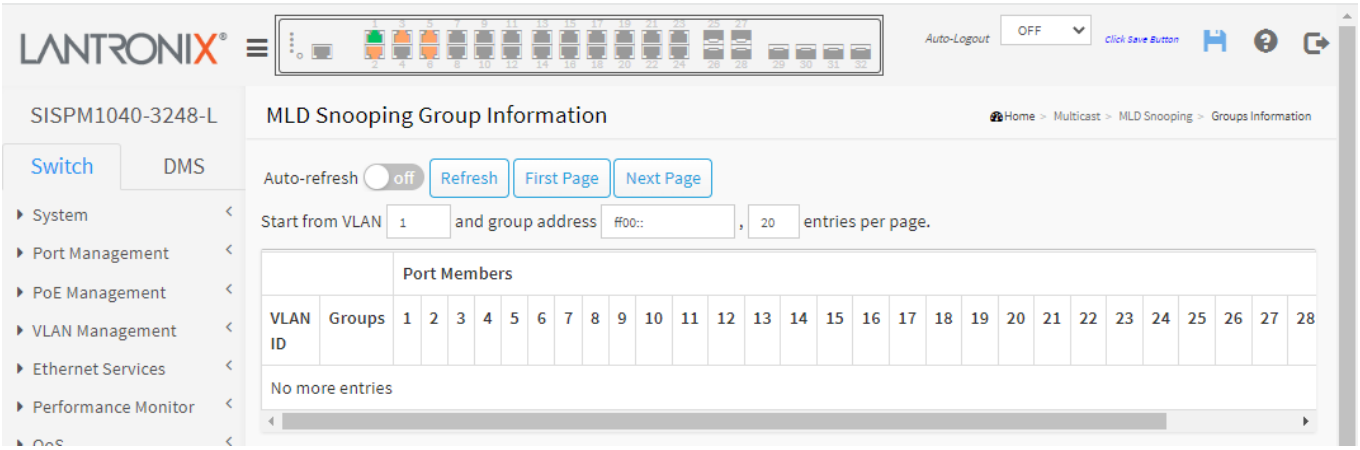


Figure 13-2.4: MLD Snooping Group Information

Parameter descriptions:

Each page shows up to 99 entries from the MLD Group table, default being 20, selected via the "entries per page" input field. When first visited, the web page will show the first 20 entries from the start of the MLD Group Table.

The "Start from VLAN", and "group" input fields allow the user to select the starting point in the MLD Group Table. Clicking the Refresh button will update the displayed table starting from that or the closest next MLD Group Table match. In addition, the two input fields will - upon a Refresh button click - assume the value of the first displayed entry, allowing for continuous refresh with the same start address.

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

VLAN ID : VLAN ID of the group.

Groups : Group address of the group displayed.

Port Members : Ports under this group.

entries per page: Choose how many items you want to be displayed.

Buttons

Auto-refresh : Click to refresh the page automatically every 3 seconds.

Refresh : Click to manually refresh the page immediately.

First Page : Updates the system log entries, turn to the first page.

Next Page : Updates the group information entries, turn to the next page.

13-2.5 MLD SFM Information

Entries in the MLD SFM Information table are shown on this page. The MLD SFM (Source-Filtered Multicast) Information table also contains the SSM (Source-Specific Multicast) information. This table is sorted first by VLAN ID, then by group, and then by Port. Different source addresses belonging to the same group are treated as a single entry.

To display MLD SFM Information in the web UI:

1. Click Multicast, MLD Snooping, and MLD SFM Information.
2. To auto-refresh the information check “Auto-refresh”.
3. Click “Refresh” to refresh an entry of the page Information.
4. Click First/Next Page to change page.

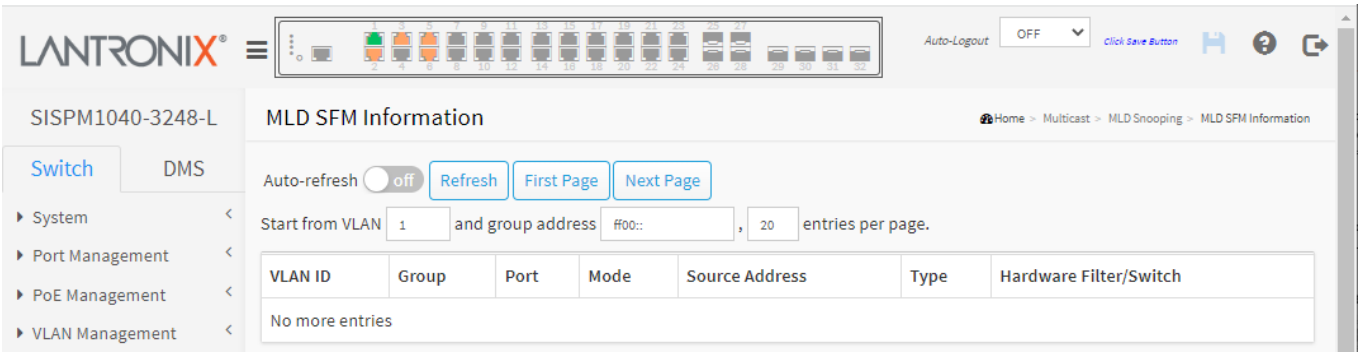


Figure 13-2.5: MLD SFM Information

Parameter descriptions:

Each page shows up to 99 entries from the MLD SFM Information table, default being 20, selected through the "entries per page" input field. When first visited, the web page will show the first 20 entries from the beginning of the MLD SFM Information Table.

The "Start from VLAN", and "group" input fields allow the user to select the starting point in the MLD SFM Information Table. Clicking the Refresh button will update the displayed table starting from that or the closest next MLD SFM Information Table match. In addition, the two input fields will - upon a Refresh button click - assume the value of the first displayed entry, allowing for continuous refresh with the same start address.

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

VLAN ID : VLAN ID of the group.

Group : IP Multicast Group address.

Port : Switch port number.

Mode : Indicates the filtering mode maintained per (VLAN ID, port number, Group Address) basis. It can be either Include or Exclude.

Type : Indicates the Type. It can be either Allow or Deny.

Source Address : The IP Address of the source. The current maximum number of IPv6 source address for filtering (per group) is 8. When there is no source filtering address, the text "None" displays in the Source Address field.

Hardware Filter/Switch : Indicates whether data plane destined to the specific group address from the source IPv6 address could be handled by chip.

Buttons

Auto-refresh : Click to refresh the page automatically every 3 seconds.

Refresh : Click to manually refresh the page immediately.

First Page : Updates the system log entries, turn to the first page.

Next Page : Updates the group information entries, turn to the next page.

13-3 MVR

The MVR feature enables multicast traffic forwarding on the Multicast VLAN. In a multicast television application, a PC or a television with a set-top box can receive the multicast stream. Multiple set-top boxes or PCs can be connected to one subscriber port, which is a switch port configured as an MVR receiver port. When a subscriber selects a channel, the set-top box or PC sends an IGMP join message to Switch A to join the appropriate multicast. Uplink ports that send and receive multicast data to and from the multicast VLAN are called MVR source ports.

Multicast VLAN Registration (MVR) is a protocol for Layer 2 (IP) networks that enables multicast-traffic from a source VLAN to be shared with subscriber-VLANs. The main reason for using MVR is to save bandwidth by preventing duplicate multicast streams from being sent in the core network, instead the stream(s) are received on the MVR-VLAN and forwarded to the VLANs where hosts have requested it/them (Wikipedia).

10-3.1 Basic Configuration

To configure MVR in the web UI:

1. Click Multicast, MVR and Basic Configuration.
2. Set MVR mode on or off and set all parameters.
3. Click “Add New MVR VLAN”.
4. Specify all of the VLAN Interface Settings.
5. Select which port(s) you want to have Immediate Leave.
6. Click the Apply button to save the settings.

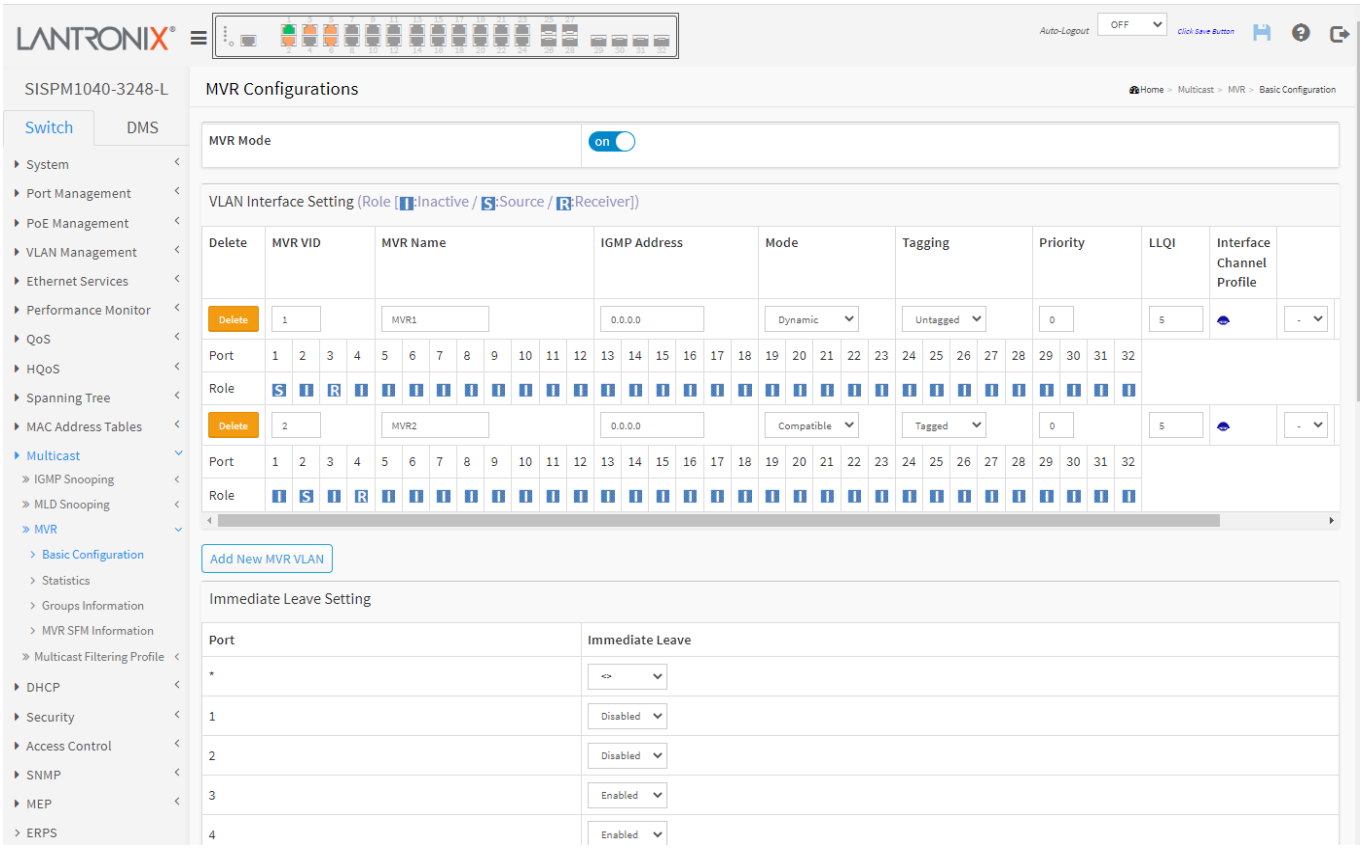


Figure 13-3.1: MVR Configuration

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 : MVR Name is an optional attribute to indicate the name of the specific MVR VLAN. Maximum length of the MVR VLAN Name string is 32. MVR VLAN Name can only contain alphabets or numbers. MVR VLAN name can be edited for the existing MVR VLAN entries or it can be added to the new entries.

IGMP Address : Define the IPv4 address as source address used in IP header for IGMP control frames. The default IGMP address is not set (0.0.0.0). When the IGMP address is not set, system uses IPv4 management address of the IP interface associated with this VLAN. When the IPv4 management address is not set, system uses the first available IPv4 management address. Otherwise, system uses a pre-defined value. By default, this value will be 192.0.2.1.

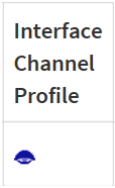
Mode : Specify the MVR mode of operation. In ***Dynamic*** mode, MVR allows dynamic MVR membership reports on source ports. In ***Compatible*** mode, MVR membership reports are forbidden on source ports. The default is ***Dynamic*** mode.

Tagging : Specify whether the traversed IGMP/MLD control frames will be sent as ***Untagged*** or ***Tagged*** with MVR VID. The default is ***tagged***.

Priority : Specify how the traversed IGMP/MLD control frames will be sent in prioritized manner. The default Priority is 0.

LLQI : Define the maximum time to wait for IGMP/MLD report memberships on a receiver port before removing the port from multicast group membership. The value is in units of tenths of a second. The range is 0 - 31744. The default LLQI is 5 tenths or one-half second.

Interface Channel Profile : When the MVR VLAN is created, select the profile () to expand the corresponding multicast channel settings for the specific MVR VLAN. The file established on Filtering Profile Table.



Port : The logical port for the settings.

Port Role : Configure an MVR port of the designated MVR VLAN as one of the following roles.

Inactive: The designated port does not participate in MVR operations.

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

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

S indicates Source;

R indicates Receiver.

Immediate Leave : Enable or disable fast leave on the port. System will remove group record and stop forwarding data upon receiving the leave message without sending last member query messages. It is recommended to enable this feature only when a single IGMPv2/MLDv1 host is connected to the specific 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" when done.

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.

13-3.2 Statistics

This page displays the MVR detail Statistics after you have configured MVR on the switch. To display MVR Statistics in the web UI:

1. Click Multicast, MVR, and Statistics.
2. To auto-refresh the information check “Auto-refresh”.
3. Click the “Refresh” to refresh an entry of the MVR Statistics information.

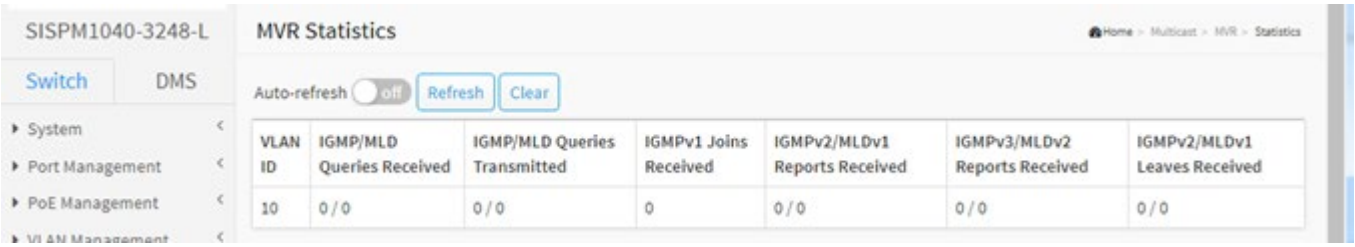


Figure 13-3.2: MVR Statistics Information

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 Join's.

IGMPv2/MLDv1 Report's Received : The number of Received IGMPv2 Join's and MLDv1 Report's, respectively.

IGMPv3/MLDv2 Report's Received : The number of Received IGMPv3 Join's and MLDv2 Report's, respectively.

IGMPv2/MLDv1 Leave's Received : The number of Received IGMPv2 Leave's and MLDv1 Done's, respectively.

Buttons

Auto-refresh : Click to refresh the page automatically every 3 seconds.

Refresh : Click to manually refresh the page immediately.

Clear : Clears all Statistics counters.

13-3.3 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.

To display MVR Groups Information in the web UI:

1. Click Multicast, MVR, and Groups Information.
2. To auto-refresh the information check “Auto-refresh”.
3. Click the “Refresh” to refresh an entry of the MVR Groups Information.
4. Click First/Next Page to change page.

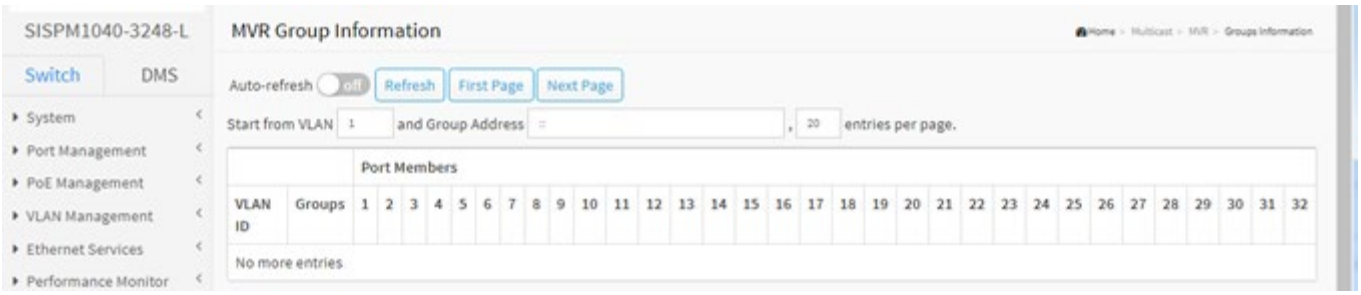


Figure 13-3.3: MVR Groups Information

Each page shows up to 99 entries from the MVR Group table, default being 20, selected through the "entries per page" input field. When first visited, the web page will show the first 20 entries from the beginning of the MVR Channels (Groups) Information Table.

The "Start from VLAN", and "Group Address" input fields allow the user to select the starting point in the MVR Channels (Groups) Information Table. Clicking the Refresh button will update the displayed table starting from that or the closest next MVR Channels (Groups) Information Table match. In addition, the two input fields will - upon a Refresh button click - assume the value of the first displayed entry, allowing for continuous refresh with the same start address.

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

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 : Click to refresh the page automatically every 3 seconds.

Refresh : Click to manually refresh the page immediately.

First Page : Updates the system log entries, turn to the first page.

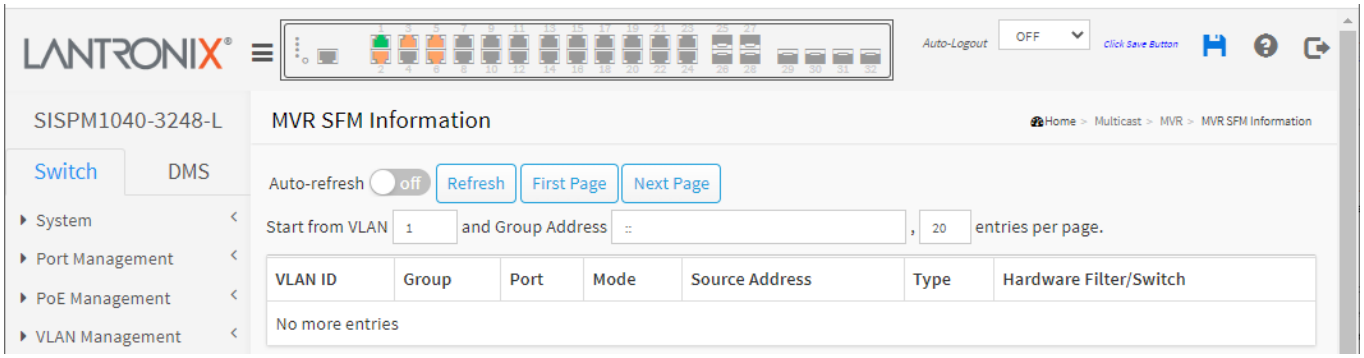
Next Page : Updates the group information entries, turn to the next page.

13-3.4 SFM Information

The MVR SFM (Source-Filtered Multicast) Information Table also contains the SSM (Source-Specific Multicast) information. This table is sorted first by VLAN ID, then by group, and then by Port. Different source addresses belonging to the same group are treated as single entry.

To display the MVR SFM Information in the web UI:

1. Click Multicast, MVR, and MVR SFM Information.
2. To auto-refresh the information check “Auto-refresh”.
3. Click “Refresh” to refresh an entry of the MVR Groups Information.
4. Click First/Next Page to change page.



Each page shows up to 99 entries from the MVR SFM Information Table, default being 20, selected through the "entries per page" input field. When first visited, the web page will show the first 20 entries from the beginning of the MVR SFM Information Table.

The "Start from VLAN", and "Group Address" input fields allow the user to select the starting point in the MVR SFM Information Table. Clicking the Refresh button will update the displayed table starting from that or the closest next MVR SFM Information Table match. In addition, the two input fields will - upon a Refresh button click - assume the value of the first displayed entry, allowing for continuous refresh with the same start address.

The Next Page will use the last entry of the currently displayed table as a basis for the next lookup. When the end is reached the text "No more entries" is shown in the displayed table. Use the First Page button to start over.
In the entries per page field, choose how many items you want to be displayed.

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 the data plane destined to the specific group address from the source IPv4/IPv6 address could be handled by the chip.

Buttons

Auto-refresh : Click to refresh the page automatically every 3 seconds.

Refresh : Click to manually refresh the page immediately.

First Page : Updates the system log entries, turn to the first page.

Next Page : Updates the group information entries, turn to the next page.

13-4 Multicast Filtering Profile

This page provides Multicast Filtering Profile related configurations.

13-4.1 Filtering Profile Table

The IPMC profile is used to deploy access control on IP multicast streams. You can create up to 64 Profiles and up to 128 corresponding rules for each Profile.

To configure the IPMC Profile Configuration in the web UI:

1. Click Multicast, Multicast Filtering Profile and Filtering Profile Table.
2. Turn Multicast Filtering Profile Mode on.
3. Click “Add New Filtering Profile” and specify Profile Name, Profile Description and Rule.
4. Click Apply to save the settings.

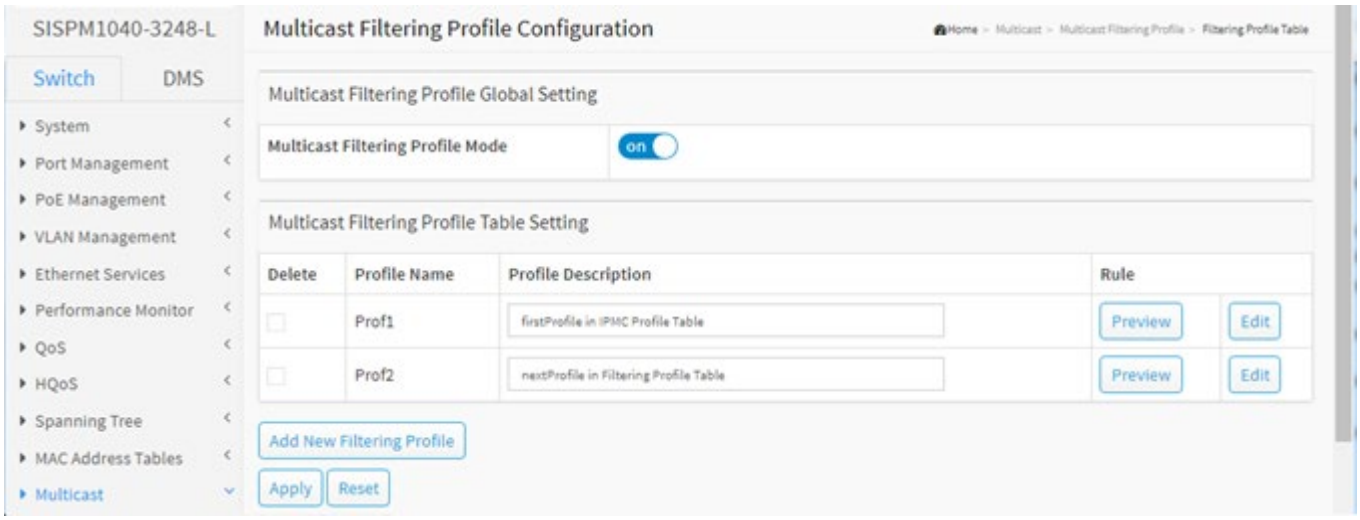


Figure 13-4.1: IPMC Profile Configuration

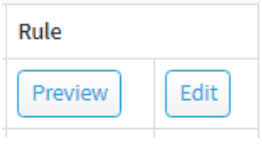
Parameter descriptions:

Multicast Filtering Profile Mode : Enable/Disable the Multicast Filtering Profile. The system starts to do filtering based on profile settings only when the global profile mode is enabled.

Profile Name : The name used for indexing the profile table. Each entry has the unique name which is composed of at maximum 16 alphabetic and numeric characters.

Profile Description : Additional description, which is composed of at maximum 64 alphabetic and numeric characters, about the profile. No blank or space characters are permitted as part of description. Use "_" or "-" to separate the description sentence.

Rule : When the profile is created, click the edit button to enter the rule setting page of the designated profile. 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 : Manage rules and the corresponding precedence order by using these buttons:

: Insert a new rule before the current entry of rule.

: Delete the current entry of rule.

: Moves the current entry of rule up in the list.

: Moves the current entry of rule down in the list.

Buttons

Add New Filtering Profile : Click to add new IPMC profile. Specify the name and configure the new entry. Click "Apply".

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

Apply : Click to save changes.

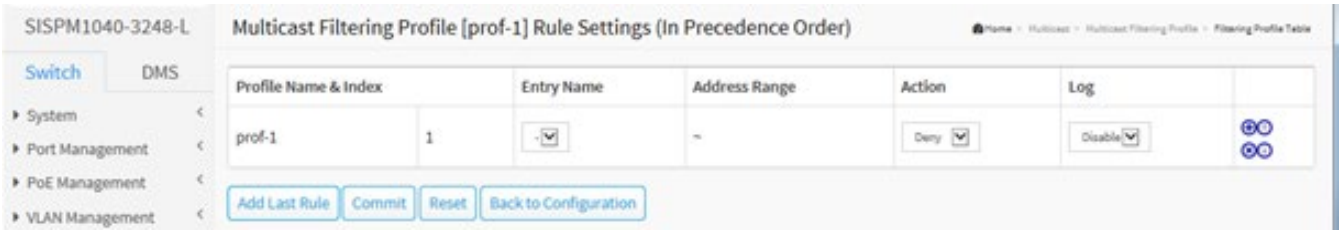
Reset : Click to undo any changes made locally and revert to previously saved values.

Add Last Rule : Click to add a new rule in the end of the specific profile's rule list. Specify the address entry and configure the new entry. Click "Apply" when done.

Back to Configuration : Go back to previous configuration page.

Commit : Click to commit rule changes for the designated profile.

Multicast Filtering Profile [prof-1] Rule Settings (In Precedence Order)



Multicast Filtering Profile Configuration table

13-4.2 Filtering Address Entry

This page provides address range settings used in IPMC profile. The address entry is used to specify the address range that will be associated with IPMC Profile. You can create up to 128 address entries in the system.

To configure IPMC Profile Address parameters in the web UI:

1. Click Multicast, Multicast Filtering Profile and Filtering Address Entry.
2. Click the “Add New Address (Range) Entry” button.
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 to revert to previously saved values.
6. Click “Refresh” to refresh an entry of the MLD Snooping Group Information.
7. Click First Entry/Next Entry to change entries.

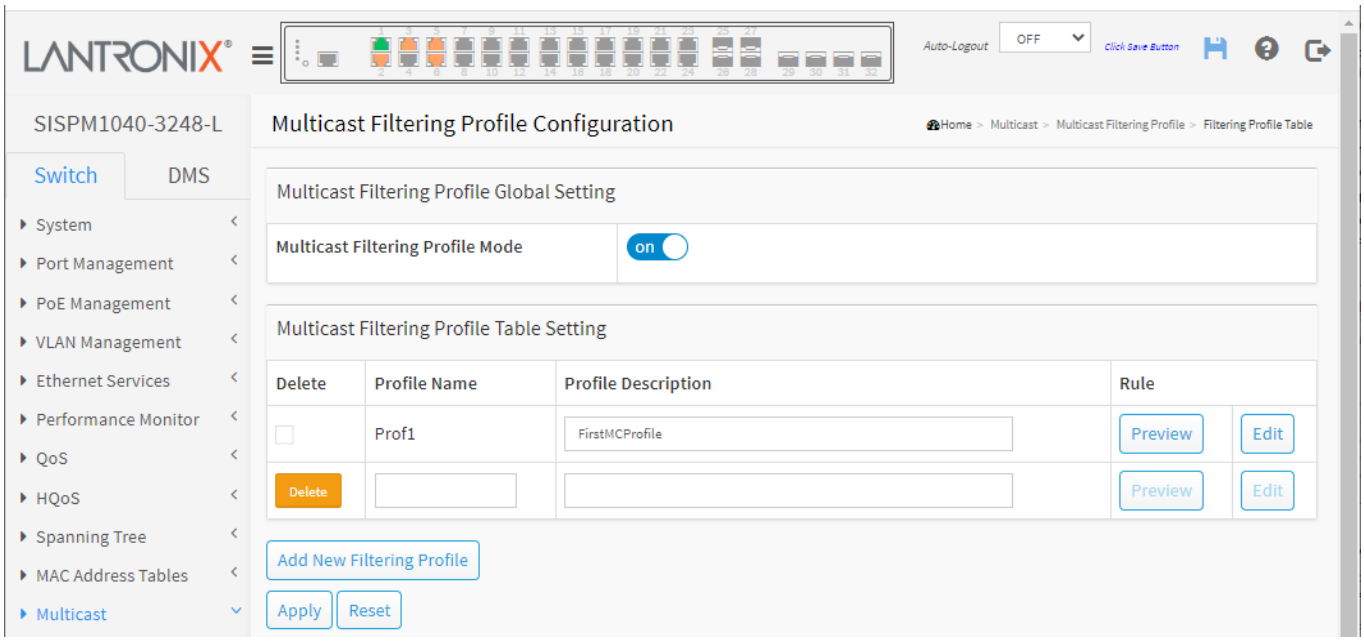


Figure 13-4.2: IPMC Profile Address Configuration

Parameter descriptions:

Entry Name : The name used for indexing the address entry table. Each entry must have a unique name composed of 1-16 alphabetic and numeric characters.

Start Address : The starting IPv4/IPv6 Multicast Group Address that will be used as an address range.

End Address : The ending IPv4/IPv6 Multicast Group Address that will be used as an address range.

Buttons

Add New Address (Range) Entry : Click to add new address range. Specify the name and configure the addresses. Click "Apply"

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

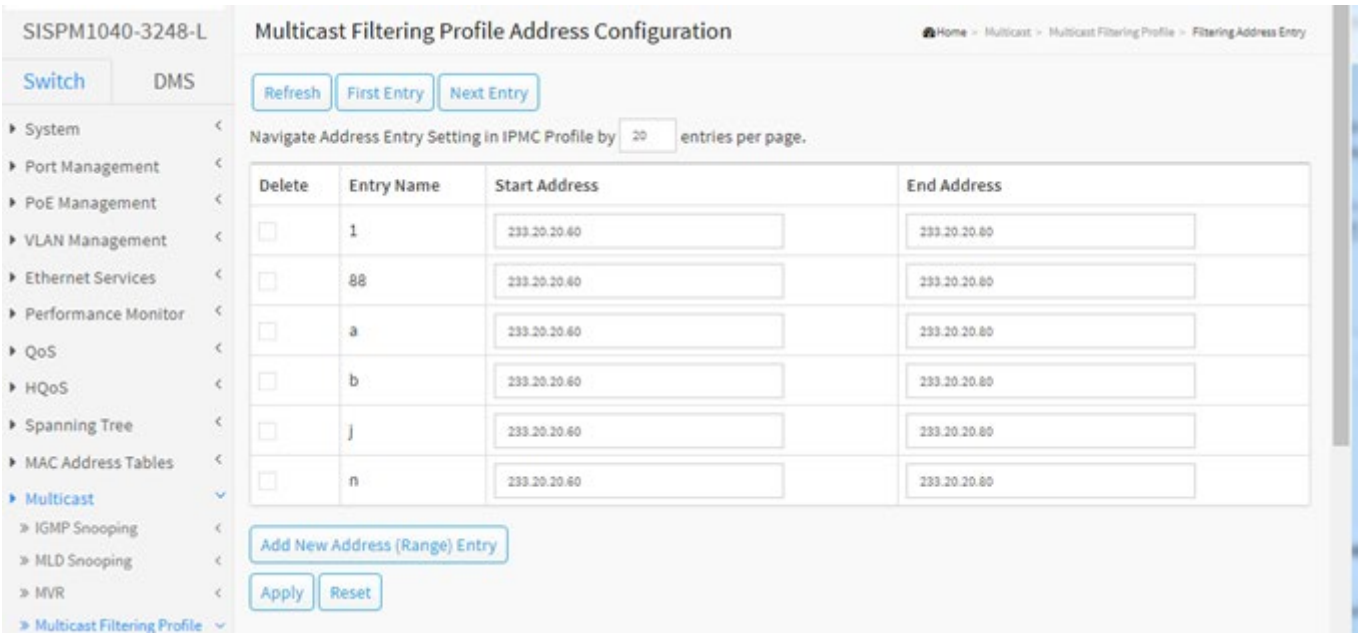
Apply : Click to save changes.

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

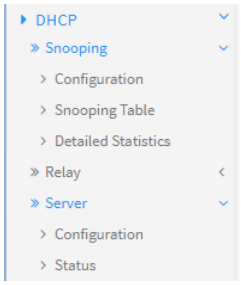
First Entry : Updates the table starting from the first entry in the IPMC Profile Address Configuration.

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

Example:



Chapter 14 - DHCP



This section lets you configure and view switch DHCP Snooping, Relay, and Server parameters. DHCP (Dynamic Host Configuration Protocol) automatically assigns a unique IP address to each device that connects to a network. With DHCP, there is no need to manually assign IP addresses to new devices.

14-1 Snooping

DHCP Snooping is used to block intruders 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.

14-1.1 Configuration

This page lets you configure DHCP Snooping parameters. The DHCP Snooping can prevent attackers from adding their own DHCP servers to the network. To configure DHCP snooping in the web UI:

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

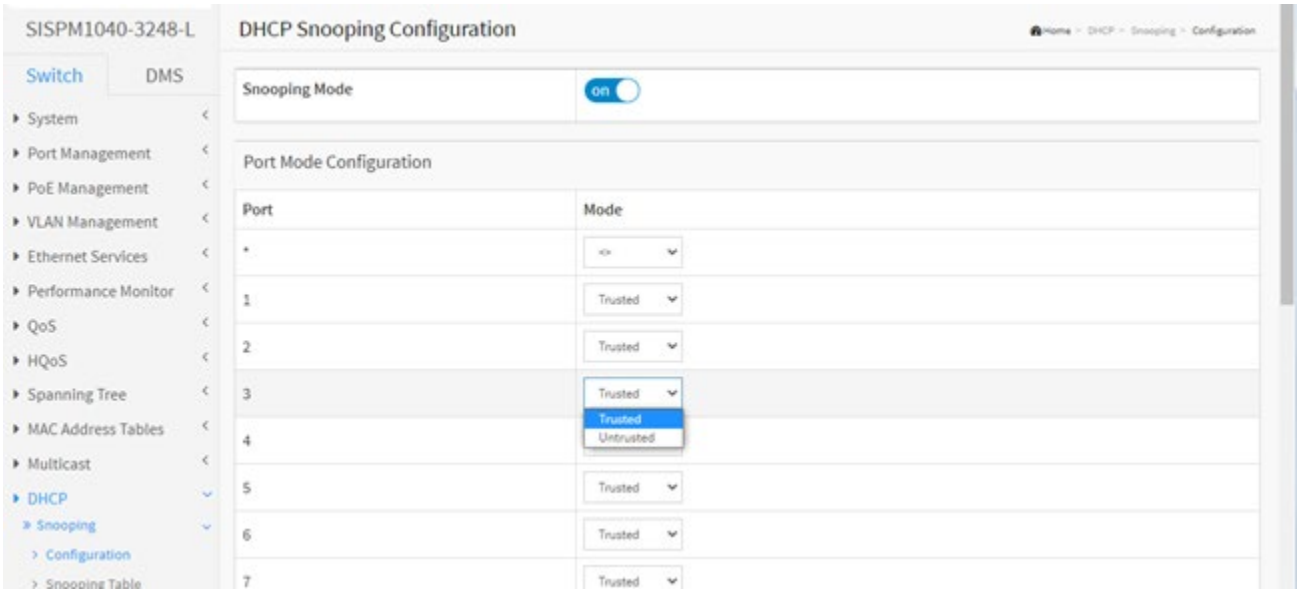


Figure 14-1.1: DHCP Snooping Configuration

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.

Port Mode Configuration : Indicates the DHCP snooping port mode. Possible port modes are:

Trusted: Configures the port as trusted source of the DHCP messages. A Trusted port can forward DHCP packets normally.

Untrusted: Configures the port as untrusted source of the DHCP messages. An Untrusted port will discard the packets when it receives DHCP packets.

Buttons

Apply : Click to save changes.

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

14-1.2 Snooping Table

Entries in the Dynamic DHCP snooping Table are shown on this page. This page displays 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.

To monitor Dynamic DHCP Snooping in the web UI:

1. Click DHCP, Snooping, and Snooping table.
2. Select Start from MAC address, VLAN, and entries per page.
3. To auto-refresh the information check “Auto-refresh”.
4. Click “Refresh” to refresh an entry of the MVR Groups Information.
5. Click First/Next Page to change page.

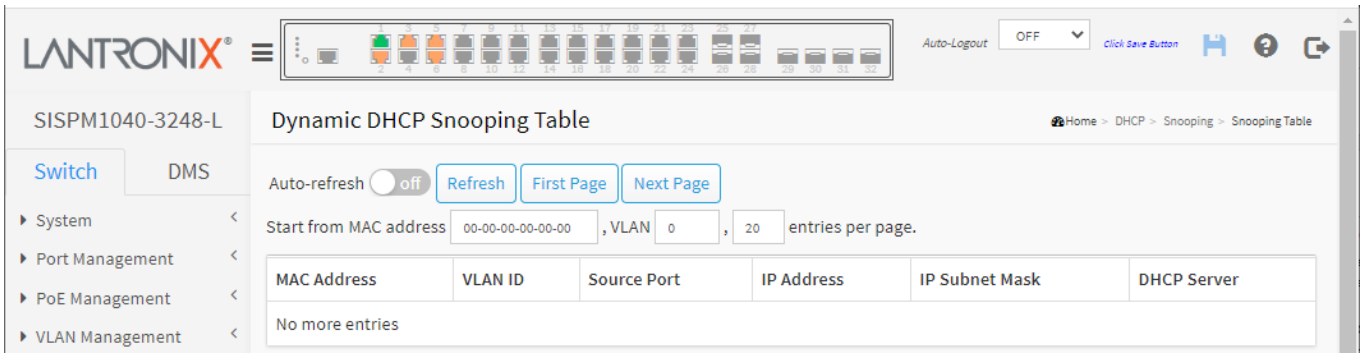


Figure 14-1.2: Dynamic DHCP Snooping Table

Parameter descriptions:

Show entries : Choose how many items you want to be displayed.

MAC Address : User MAC address of the entry.

VLAN ID : VLAN-ID in which the DHCP traffic is permitted.

Source Port: Switch Port Number for which the entries are displayed.

IP Address : User IP address of the entry.

IP Subnet Mask : User IP subnet mask of the entry.

DHCP Server : DHCP Server address of the entry.

Buttons

Auto-refresh : Click to refresh the page automatically every 3 seconds.

Refresh : Click to manually refresh the page immediately.

First Page : Updates the system log entries, turn to the first page.

Next Page : Updates the group information entries, turn to the next page.

14-1.3 Detailed Statistics

This page displays statistics for DHCP snooping. Note that the normal forward per-port TX statistics aren't increased if the incoming DHCP packet is done by L3 forwarding mechanism. Also, clearing the statistics on a specific port may not take effect on global statistics since it gathers from different layers overview.

To display DHCP detailed statistics in the web UI:

1. Click DHCP, Snooping, and Detailed Statistics.
2. Select the port that you want to display the DHCP Detailed Statistics.
3. To auto-refresh the information check “Auto-refresh”.
4. Click “Refresh” to refresh an entry of the DHCP Detailed Statistics.

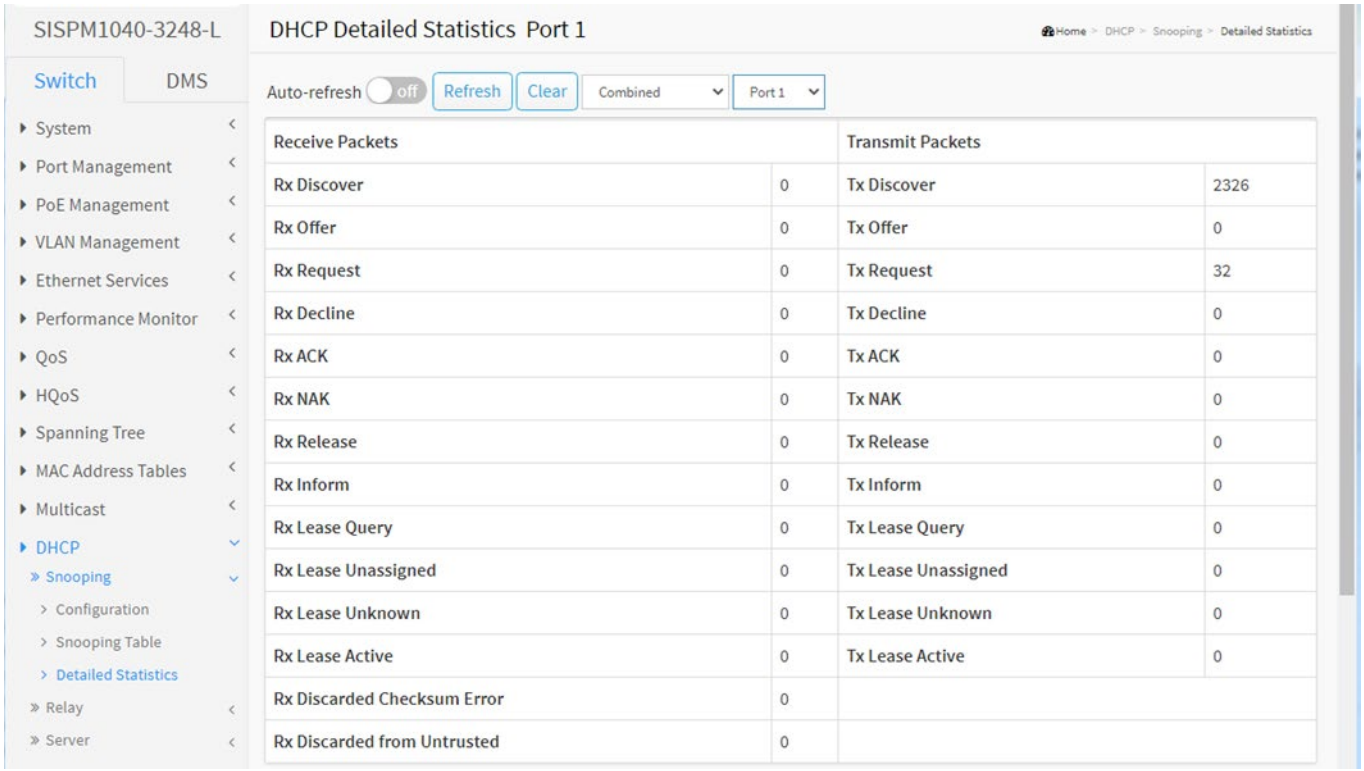


Figure 14-1.3: DHCP Detailed Statistics

Parameter descriptions:

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.

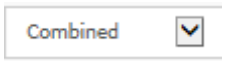
Rx Discarded from Untrusted : The number of discarded packets that are coming from untrusted port.

Buttons

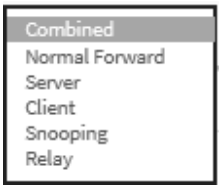
Auto-refresh : Click to refresh the page automatically every 3 seconds.

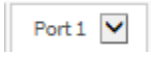
Refresh : Click to manually refresh the page immediately.

Clear : Clears all Statistics counters.



: The DHCP user select box determines which user is affected by clicking the buttons.





: Select the port that you want to display the DHCP Detailed Statistics. The port select box determines which port is affected by clicking the buttons.

14-2 Relay

14-2.1 Configuration

A DHCP relay agent is used to forward and 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) correctly.

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.

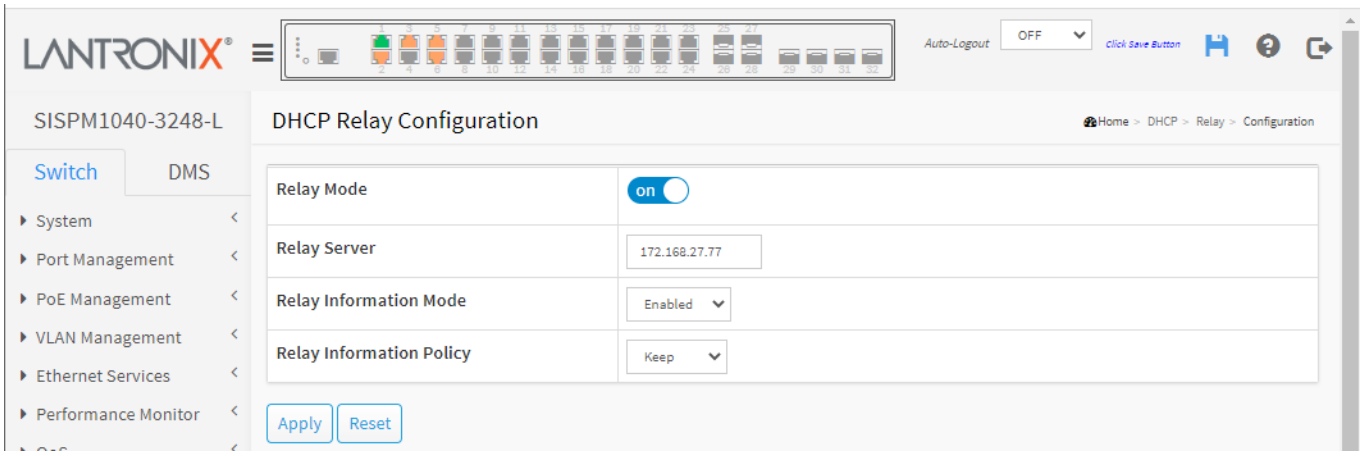


Figure 14-2.1: DHCP Relay Configuration

Parameter descriptions:

Relay Mode : Select the DHCP relay mode of 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 : Enter the DHCP relay server IP address.

Relay Information Mode : Select the DHCP relay information mode of 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, in stackable device it means switch ID), and the last two characters are the port number. For example, "00030108" means the DHCP message receive form VLAN ID 3, switch ID 1, port No 8. And the option 82 remote ID value is equal the switch MAC address.

Possible Relay Information 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. Possible policies are:

Replace: Replace the original relay information when a DHCP message that already contains it is received. The 'Replace' policy is invalid when relay information mode is disabled.

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.

Messages: *Please make sure the DHCP server connected on trust port?*

14-2.2 Statistics

This page displays DHCP relay statistics. To view DHCP Relay statistics in the web UI:

1. Click DHCP, Relay and Statistics.
2. To automatically refresh the page every 3 seconds click “Auto-refresh”.
3. Click the “Refresh” button to refresh the webpage.
4. Click the Clear button to reset the statistics.

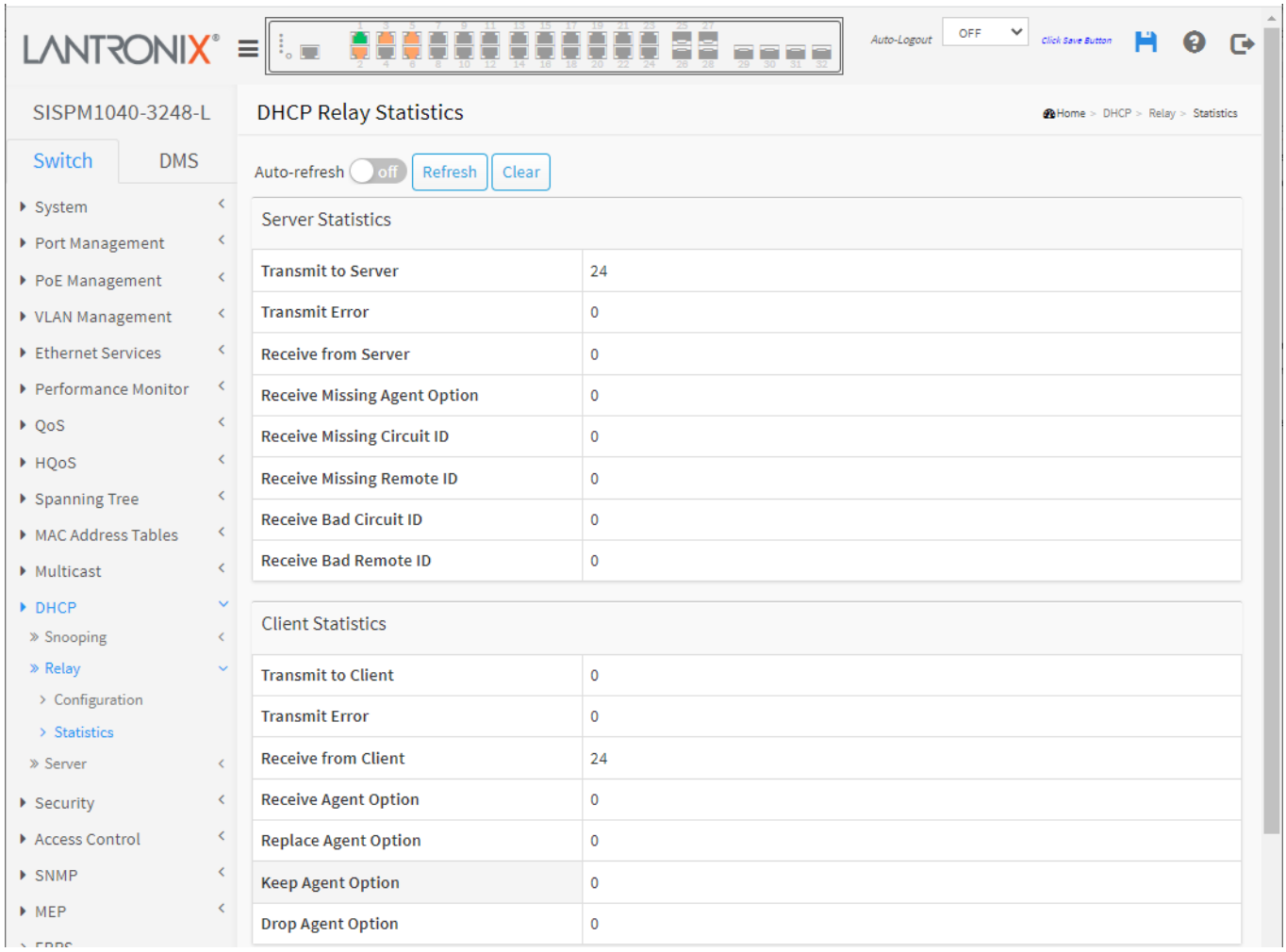


Figure 14-2.2: DHCP Relay Statistics

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 : Click to refresh the page automatically every 3 seconds.

Refresh : Click to manually refresh the page immediately.

Clear : Clear all statistics.

14-3 Server

14-3.1 Configuration

This page lets you configure DHCP server mode per system and per VLAN. You can also configure Start IP and End IP addresses and Lease Time here. A DHCP server allocates these IP addresses to DHCP clients and delivers configuration parameters to the DHCP client.

To configure DHCP Server parameters in the web UI:

1. Click DHCP, Server, and Configuration.
2. Specify VLAN, Mode, Start IP, End IP, Lease time, Subnet mask, Default router, and DNS server.
3. Click Apply.

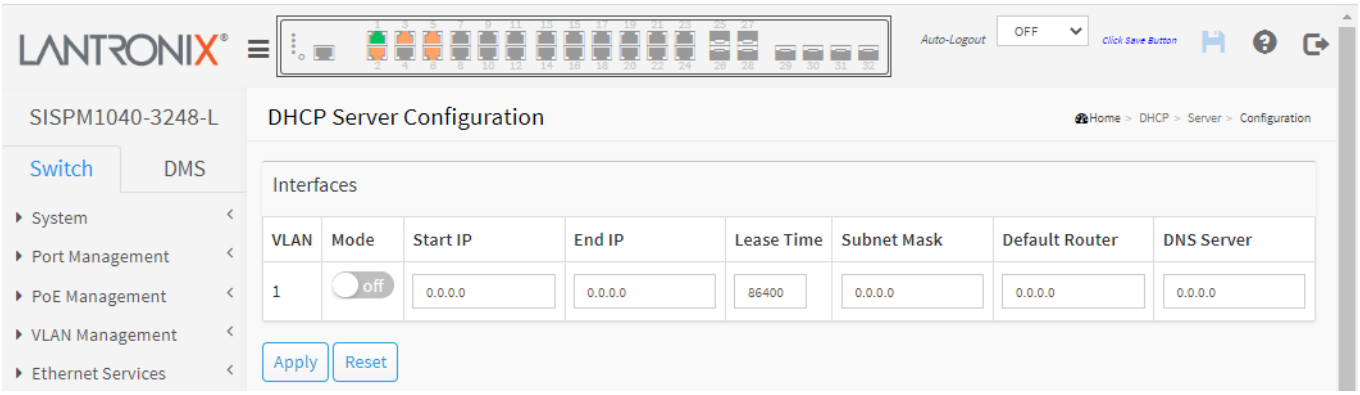


Figure 14-3.1: DHCP Server Configuration

Parameter descriptions:

VLAN: Configure the VLAN in which DHCP server is enabled or disabled. Allowed VLAN are 1 - 4095

Mode : Indicate the operation mode per VLAN. Possible modes are:

on: Enable DHCP server per VLAN.

off: Disable DHCP server per VLAN (default).

Start IP and **End IP** : Define the IP range. The Start IP must be smaller than or equal to the End IP.

Lease Time : Set the lease time of the pool in seconds. The default value is 86400 seconds (one day).

Subnet Mask : Enter the subnet mask of the DHCP address.

Default Router : Enter the the destination IP network or host address of this route.

DNS Server : Specify a DNS server IP address.

Buttons

Apply : Click to save changes.

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

14-3.2 Status

This page displays DHCP server status. To display DHCP server status in the web UI:

1. Click DHCP, Server, and Status.
2. To auto-refresh the information check “Auto-refresh”.
3. Click “Refresh” to refresh an entry of the DHCP server status.

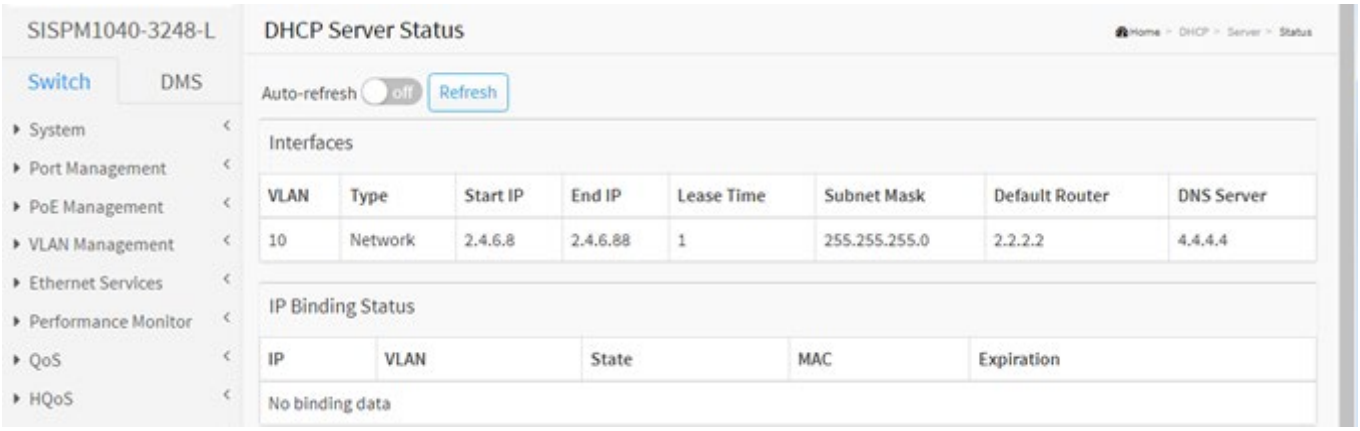


Figure 14-3.2: DHCP Server Status

Interfaces:

VLAN: The VLAN ID of the entry.

Type : Displays the operation type per VLAN.

Network: to service more than one DHCP client.

Host: for a specific DHCP client identified by client identifier or hardware address.

Start IP and **End IP** : Displays the Start IP address and the End IP address.

Lease Time : Displays lease time of the pool.

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’s IP address.

IP Binding Status

IP: The leased IP address.

VLAN: The VLAN ID of the entry.

State: The current state of the IP address (e.g., allocated or committed).

MAC: The hardware address of the device.

Expiration: The left lease time be expired in the format 21 hours 42 minutes 40 seconds.

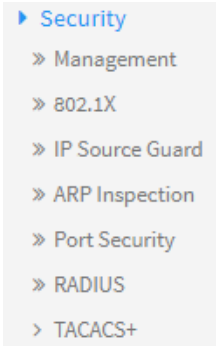
Buttons

Auto-refresh : Click to refresh the page automatically every 3 seconds.

Refresh : Click to manually refresh the page immediately.

Messages: *No entries* *No binding data*

Chapter 15 - Security



This section lets you configure switch Security settings.

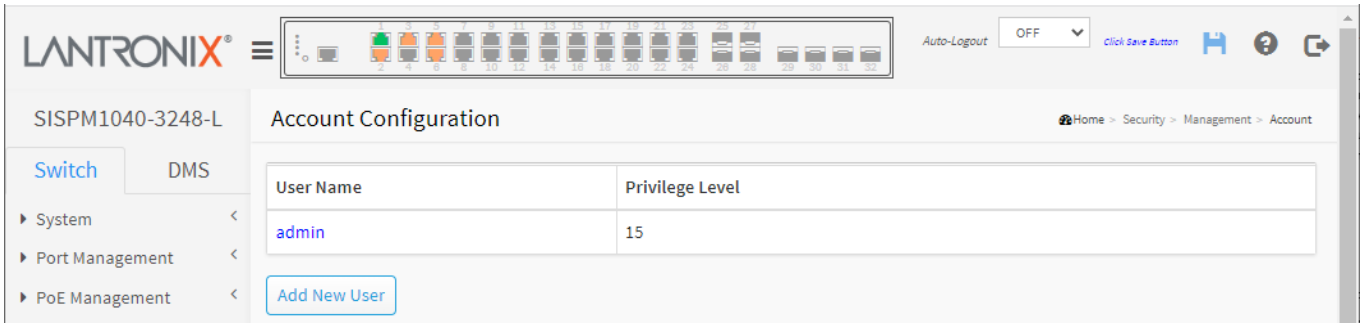
15-1 Management

15-1.1 Account

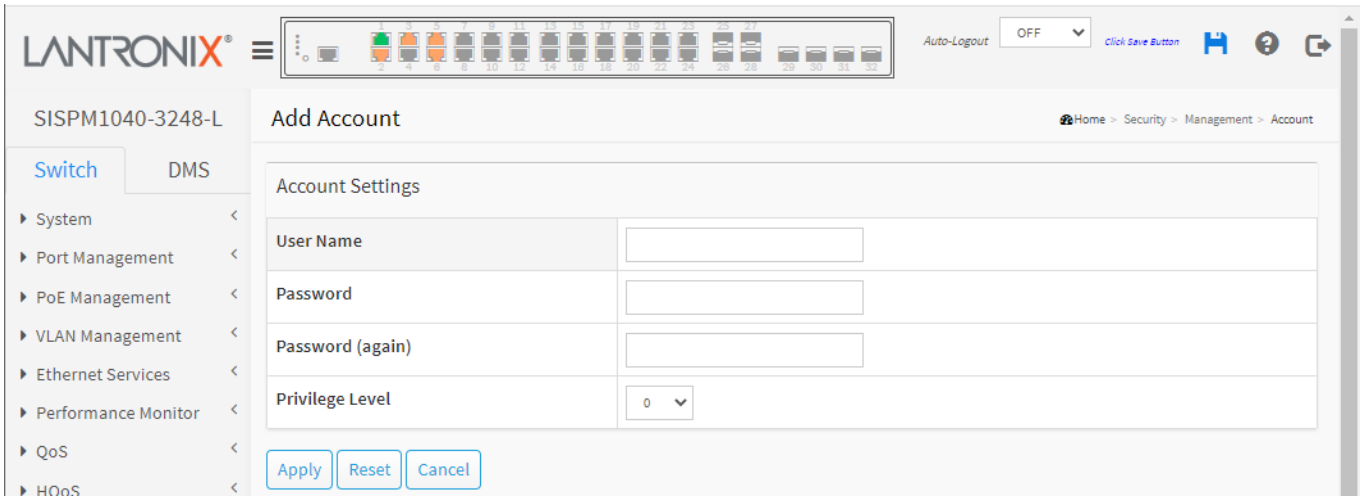
This page shows the current users, and lets you add, configure, and remove users. Currently the only way to login as another user on the web server is to close and reopen the browser.

To add a new user via the web UI:

1. Click Security, Management, and Account to display the default Account Configuration page.



2. Click the Add New User button to display the Add Account page.



3. Specify the User Name parameters.
4. Click Apply.

Parameter descriptions:

User Name : The name identifying the user. Enter up to 31 characters. This is also a link to Add/Edit/Delete users.

Password : Type the password. The field can be input 31 characters, and the allowed content is ASCII characters 32 - 126.

Password (again) : To type the password again. You must type the same password again in the field.

Privilege Level : The privilege level of the user. The allowed range is 0 - 15. If the privilege level value is 15, it can access all groups, i.e. that is granted full control of the device. A user's privilege should be same or greater than the group privilege level to have the access of that group. By default, most group's privilege level of 5 gives read-only access, and privilege level 10 gives read-write access. System maintenance (software upload, factory defaults and etc.) needs user privilege level 15. Generally, privilege level 15 can be used for an administrator account, privilege level 10 for a standard user account and privilege level 5 for a guest account.

Buttons

Apply : Click to save changes.

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

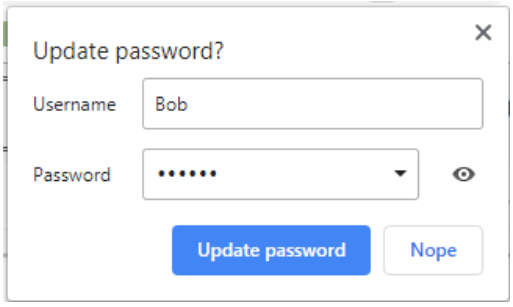
Cancel : Click to undo any changes made locally and return to the Users.

Delete User : Delete the current user. This button is not available for new configurations (Add New User).

Messages:

Can't change the privilege level since no other highest privilege account exist if change it.

Browser-specific *Update password?* messages; for example:



To edit an existing user via the web interface:

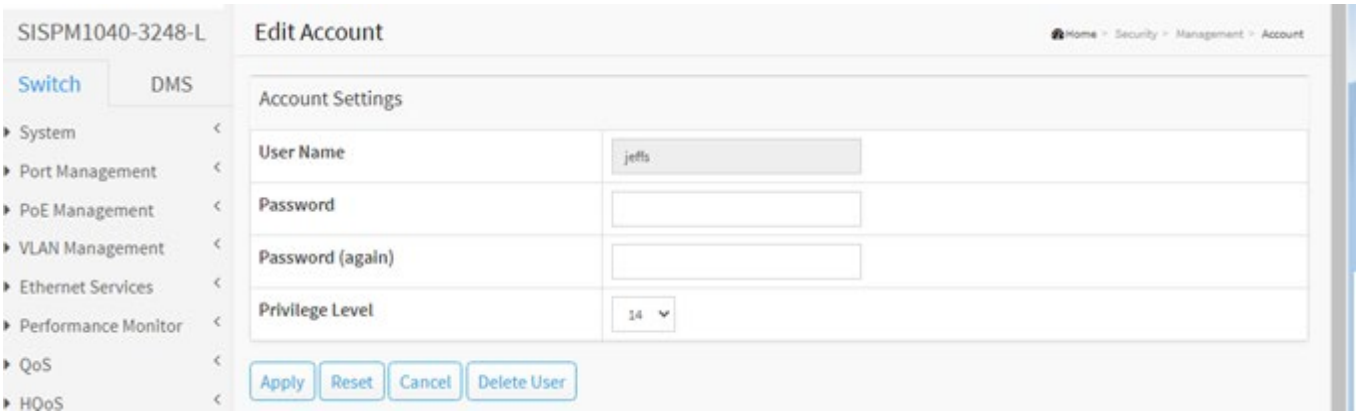
1. Click Security, Management, and Account.
2. Click the linked users name.
3. Specify the User Name parameter.
4. Click Apply.

Edit Account

To Edit an existing Account via the web UI:

1. On the “Account Configuration” page click a linked User Name.

2. On the Edit Account page Enter the Password twice and select a Privilege Level for the user.



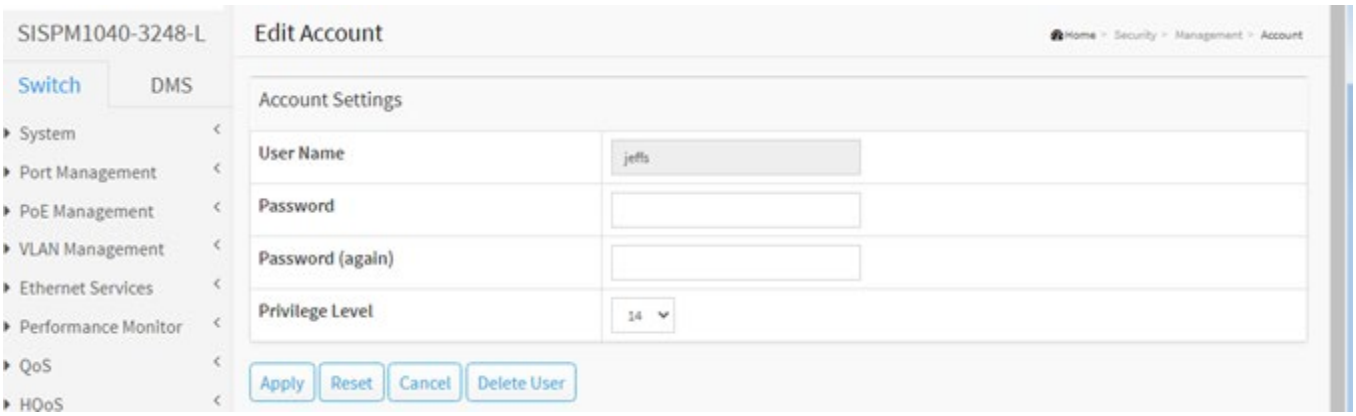
3. Click the Apply button.

Delete User

To Delete an existing User account via the web UI:

1. On the “Account Configuration” page click a linked User Name.

2. On the “Account Configuration” page click a linked User Name.



3. On the Edit Account page click the Delete User button.
4. At the “Delete User?” prompt click the OK button to delete the user. The Account Configuration page displays with the user deleted.

15-1.2 Privilege Levels

This page provides an overview of the privilege levels. The switch lets you set privilege levels for various Groups. Privilege Levels can be set from 0 to 15.

To configure Privilege Levels in the web UI:

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

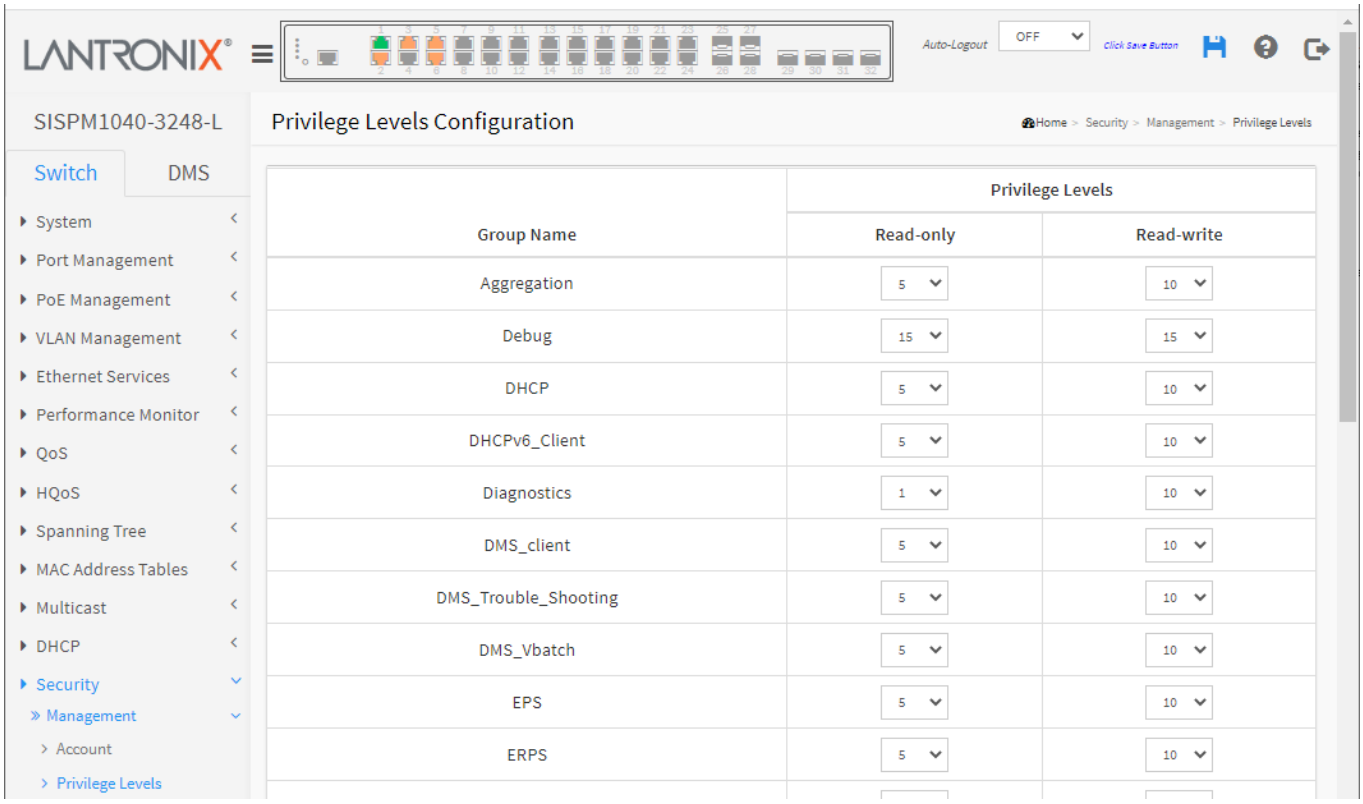


Figure15-1.2: Privilege Levels Configuration

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, STP or QoS), but a few of them contains more than one. The following description 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 : Privilege Levels can be set to 0 - 15 (where 0 is lowest level and 15 is highest level). Every group has an authorization Privilege level for read-only and read-write sub groups. 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.

Configurable Group Names:

Aggregation	LACP	Security(network)
Debug	LLDP	sFlow
DHCP	Loop_Protect	SMTP
DHCPv6_Client	MAC_Table	Spanning_Tree
Diagnostics	MEP	System
DMS_client	Miscellaneous	Trap_Event
DMS_Trouble_Shooting	MPLS_TP	TT_LOOP
DMS_Vbatch	MRP	UDLD
EPS	MVR	uFDMA_AIL
ERPS	NTP	uFDMA_CIL
ETH_LINK_OAM	Performance_Monitor	UPnP
EVC	POE	VCL
Firmware	Ports	VLAN_Translation
FRR	Private_VLANs	VLANs
Green_Ethernet	PTP	Voice_VLAN
HQoS	QoS	Watchdog
Install_Wizard	RFC2544	XXRP
IP	RMirror	Y.1564(SAM)
IPMC_Snooping	Security(access)	

15-1.3 Auth Method

This page lets you configure users with authentication method, command authorization method, and accounting method for the various client types.

To set Auth Method Configuration 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.

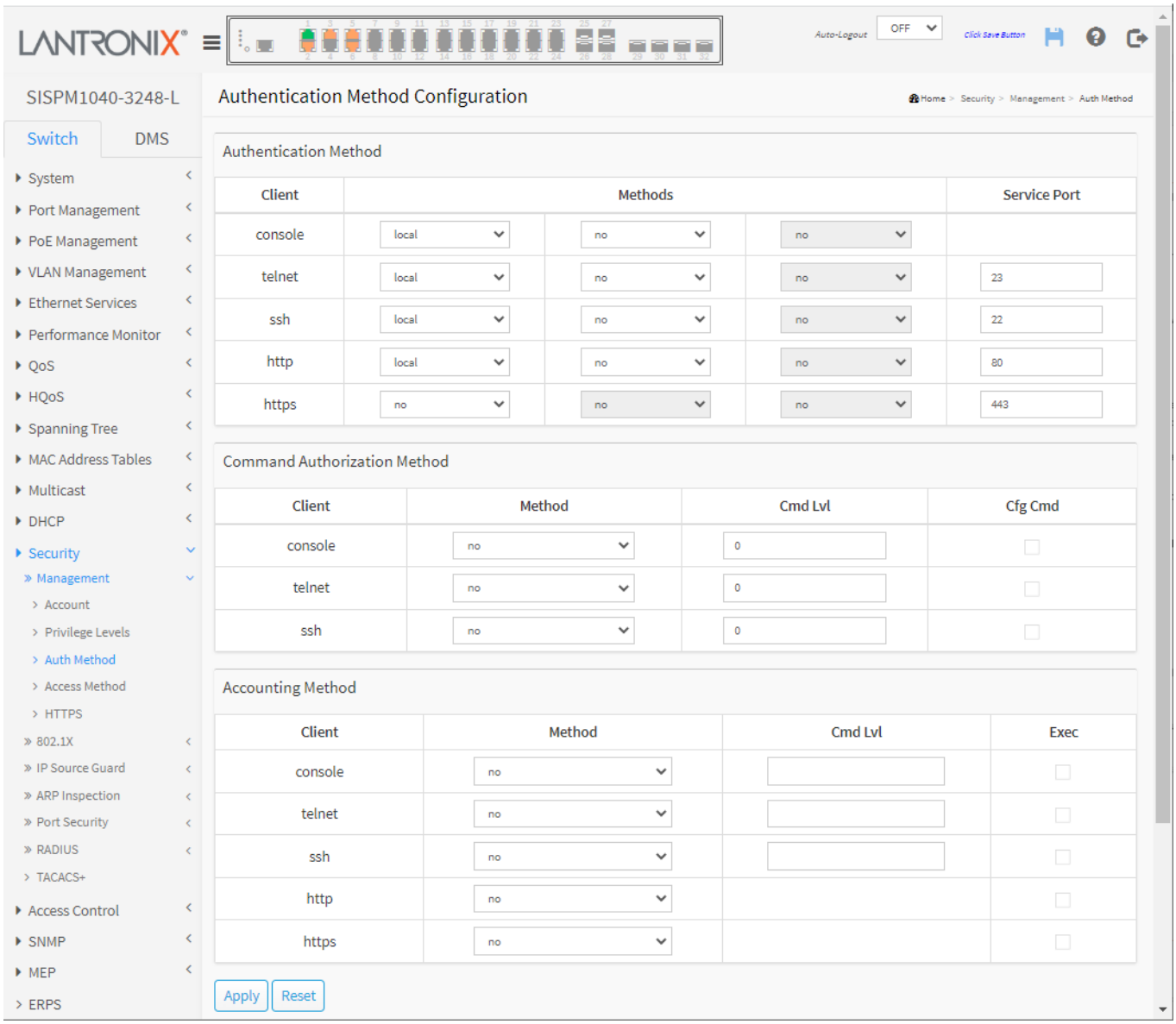


Figure 15-1.3: Authentication Method Configuration

Parameter descriptions:

Authentication Method : this section lets you configure how a user is authenticated when they log into the switch via one of the management client interfaces. The table has one row for each client type and a number of columns:

Client : The management client for which the configuration below applies (console, telnet, ssh, http, https).

Methods : Authentication Method can be set to one of these values:

no : authentication is disabled and login is not possible.

redirect: When HTTPS is enabled, enable HTTPS automatic redirect on the switch.

local : use the local user database on the switch for authentication.

radius : use a remote RADIUS server for authentication.

tacacs : use a remote TACACS server for authentication.

Methods that involves remote servers are timed out if the remote servers are offline. In this case the next method is tried. Each method is tried from left to right and continues until a method either approves or rejects a user. **Note**: If a remote server is used for primary authentication it is recommended to configure secondary authentication as 'local'. This will enable the management client to login via the local user database if none of the configured authentication servers are alive.

Service Port : The TCP port for each client service. The network port number to which this client is bound to provide service. A valid port number is 1 ~ 65534.

Command Authorization Method: this section lets you limit the CLI commands available to a user (console, telnet, ssh). The table has one row for each client type and a number of columns:

Client : The management client for which the configuration below applies.

Method : Authorization Method can be set to one of these values:

no: authorization is disabled and login is not possible.

tacacs : use a remote TACACS+ server for authorization.

Cmd Lvl : Authorize all commands with a privilege level higher than or equal to this level. Valid entries are 0 - 15.

Cfg Cmd : Checkbox to Enable or disable configuration commands.

Accounting Method: this section lets you configure command and exec (login) accounting. The table has one row for each client type and a number of columns:

Client : The management client (console, telnet, ssh, http, https) for which the configuration below applies.

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

none : accounting is disabled and login is not possible.

tacacs : use a remote TACACS+ server for accounting.

Cmd Lvl : 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 : Check the box to Enable exec (login) accounting. Runs accounting to determine if the user is allowed to run an EXEC shell. This facility might return user profile information such as auto command information.

Buttons

Apply : Click to save changes.

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

15-1.4 Access Method

This page lets you configure switch access method parameters, including HTTP/HTTPS, SNMP, and TELNET/SSH. You can manage the switch over an Ethernet LAN, or over the Internet. The maximum number of entries is 16. If the application's type matches any one of the access management entries, it will allow access to the switch.

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 Access Management method (HTTP/HTTPS, SNMP, and TELNET/SSH) in the entry.
6. Click Apply.

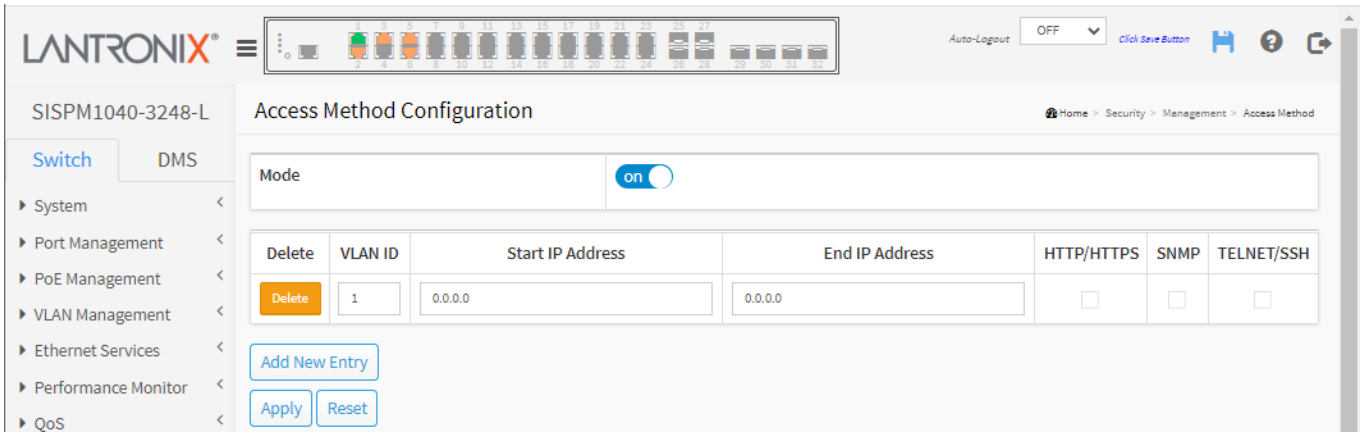


Figure 15-1.4: Access Method Configuration

Parameter descriptions:

Mode : Indicates the access management mode operation. Possible modes are:

on : Enable access management mode operation.

off : Disable access management mode operation.

Delete : Click to delete the entry. It will be deleted immediately.

VLAN ID : Indicates the VLAN ID for the access management entry.

Start IP address : Indicates the start IP unicast address for the access management entry.

End IP address : Indicates the end IP unicast address for the access management entry.

HTTP/HTTPS : Indicates that the host can access the switch from HTTP/HTTPS interface if the host IP address matches the IP address range provided in the entry.

SNMP : Indicates that the host can access the switch from SNMP interface if the host IP address matches the IP address range provided in the entry.

TELNET/SSH : Indicates that the host can access the switch from TELNET/SSH interface if the host IP address matches the IP address range provided in the entry.

Buttons

Add New Entry : Click to add a new access management entry.

Apply : Click to save changes.

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

15-1.5 HTTPS

This page lets you upload or generate a certificate on the switch. To configure HTTPS in the web UI:

1. Click Security, Management and HTTPS.
2. Specify the Certificate Maintain, Certificate Pass Phrase, and Certificate Upload.
3. Click Choose File to browse to and select the file to upload.
4. Click Apply.

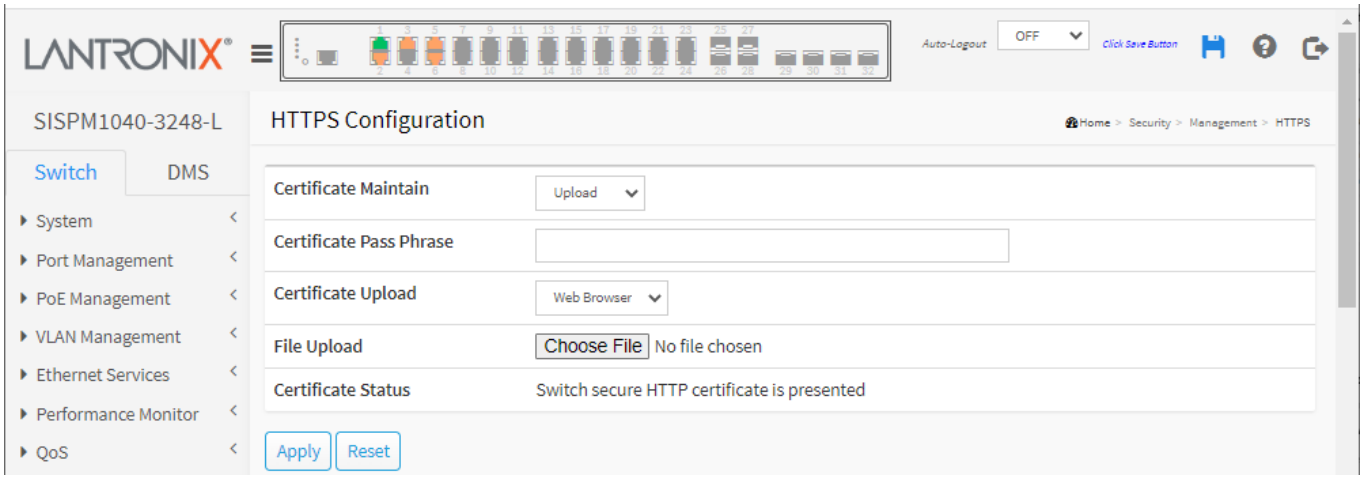


Figure 15-1.5: HTTPS Configuration

Parameter descriptions:

Certificate Maintain : The operation of certificate maintenance. Possible operations are:

Upload: Upload a certificate PEM file. Possible methods are: Web Browser or URL.

Generate: Generate a new self-signed RSA certificate.

Certificate Pass Phrase : Enter the pass phrase in this field if your uploading certificate is protected by a specific passphrase.

Certificate Upload : Upload a certificate PEM file into the switch. The file should contain the certificate and private key together. If you have two separated files for saving certificate and private key. Use the Linux cat command to combine them into a single PEM file. For example, cat my.cert my.key > my.pem.

Note that the RSA certificate is recommended since most new browsers versions have removed support for DSA in certificates (e.g. Firefox v37 and Chrome v39). Possible methods are:

Web Browser: Upload a certificate via Web browser.

URL: Upload a certificate via URL; the supported protocols are HTTP, HTTPS, TFTP and FTP.
The URL format is <protocol>://[<username>[:<password>]@]< host>[:<port>][/<path>]/<file_name>.
For example:

tftp://10.10.10.10/new_image_path/new_image.dat,
http://username:password@10.10.10.10:80/new_image_path/new_image.dat.

A valid file name is a text string drawn from alphabet (A-Za-z), digits (0-9), dot (.), hyphen (-), under score (_). The maximum length is 63 and hyphen must not be first character. A file name that only contains '.' is not allowed.

File Upload: Displays “No file chosen” by default. Click the Choose File button and navigate to and open the certificate file that you want to upload.

Certificate Status : Displays the current status of certificate on the switch. Possible statuses are:

Switch secure HTTP certificate is presented.

Switch secure HTTP certificate is not presented.

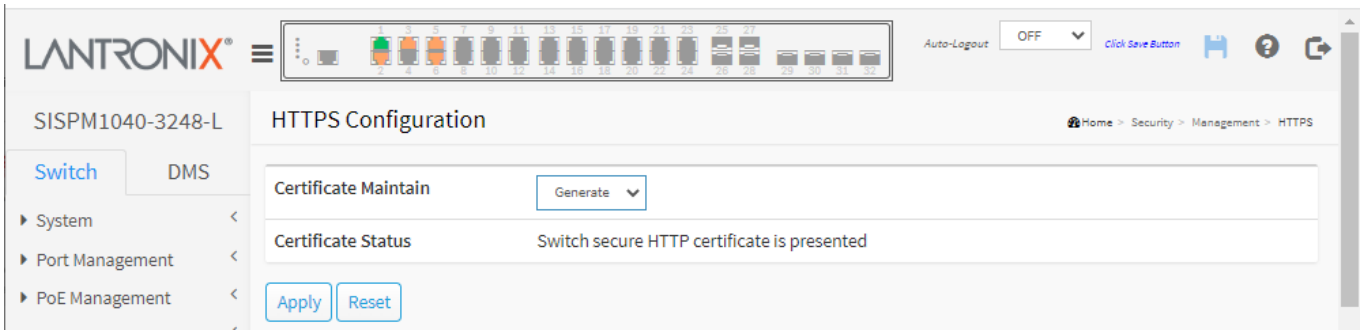
Switch secure HTTP certificate is generating ....

Buttons

Apply : Click to save changes to the running-config file.

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

Example:



Messages:

HTTPS invalid URL parameter

Upload certificate failure

Certificate PEM file size too big

15-2 802.1X

15-2.1 Configuration

This page lets you configure the IEEE 802.1X and MAC-based authentication system and port settings.

The IEEE 802.1X standard defines a port-based access control procedure that prevents unauthorized access to a network by requiring users to first submit credentials for authentication. One or more central servers, the backend servers, determine whether the user is allowed access to the network. These backend (RADIUS) servers are configured on the "Security > RADIUS > Configuration" page. The IEEE802.1X standard defines port-based operation, but non-standard variants overcome security limitations as described below.

MAC-based authentication allows for authentication of more than one user on the same port, and doesn't require the user to have special 802.1X supplicant software installed on his system. The switch uses the user's MAC address to authenticate against the backend server. Intruders can create counterfeit MAC addresses, which makes MAC-based authentication less secure than 802.1X authentication.

To configure IEEE 802.1X in the web UI:

1. Click Security, 802.1X and Configuration.
2. Select “on” in the Mode of IEEE 802.1X Configuration.
3. Set the System Configuration section parameters.
4. Set the Port Configuration section parameters.
5. Click Apply to save the settings to running-config.

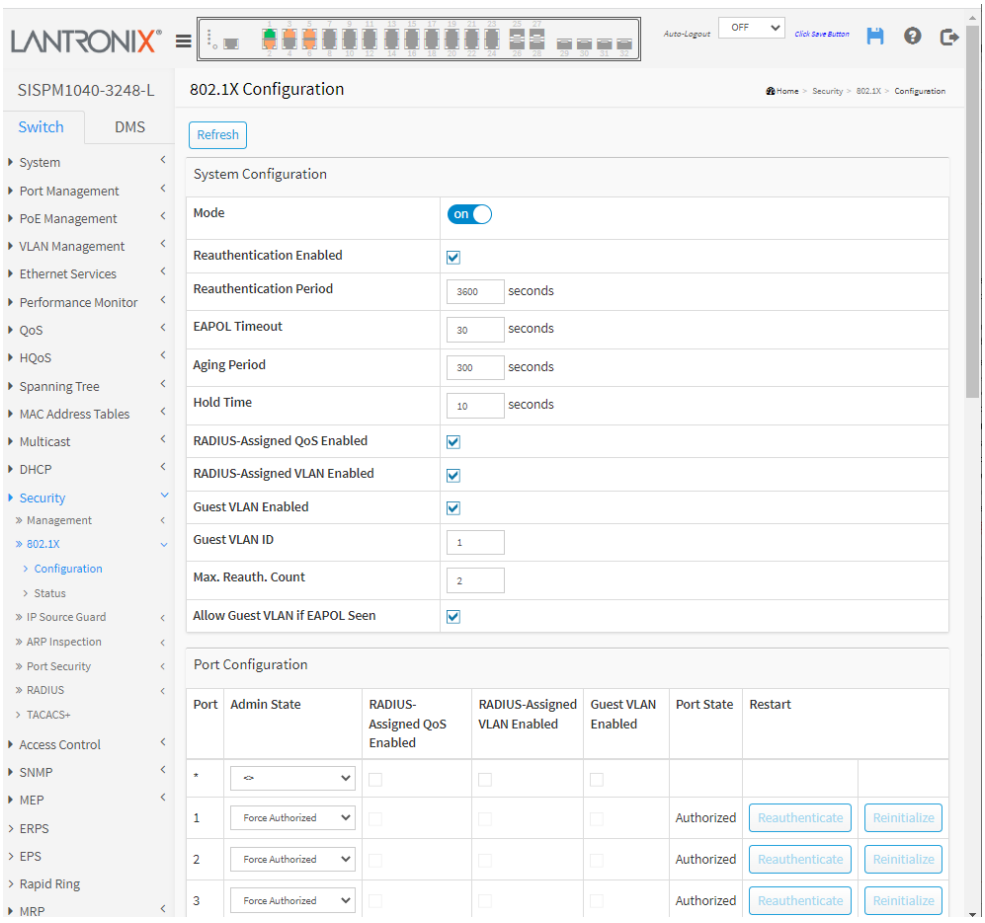


Figure 15-2.1: IEEE 802.1X Configuration

Parameter descriptions:

System Configuration section parameters

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 1 - 3600 seconds.

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

Aging Period : This setting applies to the following modes, i.e. modes using the Port Security functionality to secure MAC addresses:

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

When the NAS module uses the Port Security module to secure MAC addresses, the Port Security module needs to check for activity on the MAC address in question at regular intervals and free resources if no activity is seen within a given period of time. This parameter controls exactly this period and can be set to a number between 10 and 1000000 seconds.

If reauthentication is enabled and the port is in an 802.1X-based mode, this is not so critical, since supplicants that are no longer attached to the port will get removed upon the next reauthentication, which will fail. But if reauthentication is not enabled, the only way to free resources is by aging the entries.

For ports in MAC-based Auth. mode, reauthentication doesn't cause direct communication between the switch and the client, so this will not detect whether the client is still attached or not, and the only way to free any resources is to age the entry.

Hold Time : This setting applies to the following modes, i.e. modes using the Port Security 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 > AA" 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.

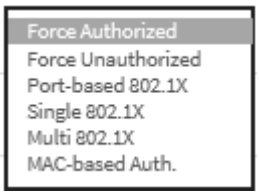
The "Guest VLAN Enabled" checkbox provides a quick way to globally enable/disable Guest VLAN functionality. When checked, the individual ports' ditto setting determines whether the port can be moved into Guest VLAN. When unchecked, the ability to move to the Guest VLAN is disabled on all ports.

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 is only changeable if the Guest VLAN option is globally enabled. Valid values are 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 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 section parameters



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

Admin State : If 802.1X is globally enabled, this selection controls the port's authentication mode. 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. The 802.1X Admin State must be set to Force Authorized for ports that are enabled for Spanning Tree.

Force Unauthorized : In this mode, the switch will send one EAPOL Failure frame when the port link comes up, and any client on the port will be disallowed network access.

Port-based 802.1X : In the 802.1X-world, the user is called the supplicant, the switch is the authenticator, and the RADIUS server is the authentication server. The authenticator acts as the man-in-the-middle, forwarding requests and responses between the supplicant and the authentication server. Frames sent between the supplicant and the switch are special 802.1X frames, known as EAPOL (EAP Over LANs) frames. EAPOL frames encapsulate EAP PDUs (RFC3748). Frames sent between the switch and the RADIUS server are RADIUS packets. RADIUS packets also encapsulate EAP PDUs together with other attributes like the switch's IP address, name, and the supplicant's port number on the switch. EAP is very flexible, in that it allows for different authentication methods, like MD5-Challenge, PEAP, and TLS. The important thing is that the authenticator (the switch) doesn't need to know which authentication method the supplicant and the authentication server are using, or how many information exchange frames are needed for a particular method. The switch simply encapsulates the EAP part of the frame into the relevant type (EAPOL or RADIUS) and forwards it.

When authentication is complete, the RADIUS server sends a special packet containing a success or failure indication. Besides forwarding this decision to the supplicant, the switch uses it to open up or block traffic on the switch port connected to the supplicant

Note: Suppose two backend servers are enabled and that the server timeout is configured to X seconds (using the AAA configuration page), and suppose that the first server in the list is currently down (but not considered dead).
Now, if the supplicant retransmits EAPOL Start frames at a rate faster than X seconds, then it will never get authenticated, because the switch will cancel on-going backend authentication server requests whenever it receives a new EAPOL Start frame from the supplicant.
And since the server hasn't yet failed (because the X seconds haven't expired), the same server will be contacted upon the next backend authentication server request from the switch. This scenario will loop forever. Therefore, the server timeout should be smaller than the supplicant's EAPOL Start frame retransmission rate.

Single 802.1X : In port-based 802.1X authentication, once a supplicant is successfully authenticated on a port, the whole port is opened for network traffic. This allows other clients connected to the port (for instance through a hub) to piggy-back on the successfully authenticated client and get network access even though they really aren't authenticated. To overcome this security breach, use the Single 802.1X variant. Single 802.1X is really not an IEEE standard, but features many of the same characteristics as

does port-based 802.1X. In Single 802.1X, at most one supplicant can get authenticated on the port at a time. Normal EAPOL frames are used in the communication between the supplicant and the switch. If more than one supplicant is connected to a port, the one that comes first when the port's link comes up will be the first one considered. If that supplicant doesn't provide valid credentials within a certain amount of time, another supplicant will get a chance. Once a supplicant is successfully authenticated, only that supplicant will be allowed access. This is the most secure of all the supported modes. In this mode, the Port Security module is used to secure a supplicant's MAC address once successfully authenticated.

Multi 802.1X : In port-based 802.1X authentication, once a supplicant is successfully authenticated on a port, the whole port is opened for network traffic. This allows other clients connected to the port (for instance through a hub) to piggy-back on the successfully authenticated client and get network access even though they really aren't authenticated. To overcome this security breach, use the Multi 802.1X variant.

Multi 802.1X is really not an IEEE standard, but features many of the same characteristics as does port-based 802.1X. Multi 802.1X is - like Single 802.1X - not an IEEE standard, but a variant that features many of the same characteristics. In Multi 802.1X, one or more supplicants can get authenticated on the same port at the same time. Each supplicant is authenticated individually and secured in the MAC table using the Port Security module.

In Multi 802.1X it is not possible to use the multicast BPDU MAC address as destination MAC address for EAPOL frames sent from the switch towards the supplicant, since that would cause all supplicants attached to the port to reply to requests sent from the switch. Instead, the switch uses the supplicant's MAC address, which is obtained from the first EAPOL Start or EAPOL Response Identity frame sent by the supplicant. An exception to this is when no supplicants are attached. In this case, the switch sends EAPOL Request Identity frames using the BPDU multicast MAC address as destination - to wake up any supplicants that might be on the port.

The maximum number of supplicants that can be attached to a port can be limited using the Port Security Limit Control functionality.

MAC-based Auth.: Unlike port-based 802.1X, MAC-based authentication is not a standard, but merely a best-practices method adopted by the industry. In MAC-based authentication, users are called clients, and the switch acts as the supplicant on behalf of clients. The initial frame (any kind of frame) sent by a client is snooped by the switch, which in turn uses the client's MAC address as both username and password in the subsequent EAP exchange with the RADIUS server. The 6-byte MAC address is converted to a string on the following form "xx-xx-xx-xx-xx-xx", that is, a dash (-) is used as separator between the lower-cased hexadecimal digits. The switch only supports the MD5-Challenge authentication method, so the RADIUS server must be configured accordingly.

When authentication is complete, the RADIUS server sends a success or failure indication, which in turn causes the switch to open up or block traffic for that particular client, using the Port Security module. Only then will frames from the client be forwarded on the switch. There are no EAPOL frames involved in this authentication, and therefore, MAC-based Authentication has nothing to do with the 802.1X standard.

The advantage of MAC-based authentication over port-based 802.1X is that several clients can be connected to the same port (e.g. through a 3rd party switch or a hub) and still require individual authentication, and that the clients don't need special supplicant software to authenticate. The advantage of MAC-based authentication over 802.1X-based authentication is that the clients don't need special supplicant software to authenticate. The disadvantage is that MAC addresses can be spoofed by malicious users - equipment whose MAC address is a valid RADIUS user can be used by anyone. Also, only the MD5-Challenge method is supported. The maximum number of clients that can be attached to a port can be limited using the Port Security Limit Control functionality.

RADIUS-Assigned QoS Enabled : When RADIUS-Assigned QoS is both globally enabled and enabled (checked) on a given port, the switch reacts to QoS Class information carried in the RADIUS Access-Accept packet transmitted by the RADIUS server when a supplicant is successfully authenticated. If present and valid, traffic received on the supplicant's port will be classified to the given QoS Class. If (re-)authentication fails or the RADIUS Access-Accept packet no longer carries a QoS Class or it's invalid, or the supplicant is otherwise no longer present on the port, the port's QoS Class is immediately reverted to the original QoS Class (which may be changed by the administrator in the meanwhile without affecting the RADIUS-assigned).

This option is only available for single-client modes, i.e.:

- Port-based 802.1X
- Single 802.1X

RADIUS attributes used in identifying a QoS Class: The User-Priority-Table attribute defined in RFC4675 forms the basis for identifying the QoS Class in an Access-Accept packet.

Only the first occurrence of the attribute in the packet will be considered, and to be valid, it must follow this rule:

- All 8 octets in the attribute's value must be identical and consist of ASCII characters in the range '0' - '7', which translates into the desired QoS Class in the range [0; 7].

RADIUS-Assigned VLAN Enabled : When RADIUS-Assigned VLAN is both globally enabled and enabled (checked) for a given port, the switch reacts to VLAN ID information carried in the RADIUS Access-Accept packet transmitted by the RADIUS server when a supplicant is successfully authenticated. If present and valid, the port's Port VLAN ID will be changed to this VLAN ID, the port will be set to be a member of that VLAN ID, and the port will be forced into VLAN unaware mode. Once assigned, all traffic arriving on the port will be classified and switched on the RADIUS-assigned VLAN ID.

If (re-)authentication fails or the RADIUS Access-Accept packet no longer carries a VLAN ID or it's invalid, or the supplicant is otherwise no longer present on the port, the port's VLAN ID is immediately reverted to the original VLAN ID (which may be changed by the administrator in the meanwhile without affecting the RADIUS-assigned).

This option is only available for single-client modes, i.e.

- Port-based 802.1X
- Single 802.1X

For trouble-shooting VLAN assignments, use the "Monitor > VLANs > VLAN Membership and VLAN Port" pages. These pages show which modules have (temporarily) overridden the current Port VLAN configuration.

RADIUS attributes used in identifying a VLAN ID: RFC2868 and RFC3580 form the basis for the attributes used in identifying a VLAN ID in an Access-Accept packet. The following criteria are used:

• The Tunnel-Medium-Type, Tunnel-Type, and Tunnel-Private-Group-ID attributes must all be present at least once in the Access-Accept packet.

• The switch looks for the first set of these attributes that have the same Tag value and fulfil the following requirements (if Tag == 0 is used, the Tunnel-Private-Group-ID does not need to include a Tag):

- Value of Tunnel-Medium-Type must be set to "IEEE-802" (ordinal 6).

- Value of Tunnel-Type must be set to "VLAN" (ordinal 13).

- Value of Tunnel-Private-Group-ID must be a string of ASCII chars in the range '0' - '9', which is interpreted as a decimal string representing the VLAN ID. Leading '0's are discarded. The final value must be in the range [1; 4095].

Guest VLAN Enabled : When Guest VLAN is both globally enabled and enabled (checked) for a given port, the switch considers moving the port into the Guest VLAN according to the rules outlined below. This option is only available for EAPOL-based modes, i.e.:

• Port-based 802.1X

• Single 802.1X

• Multi 802.1X

For trouble-shooting VLAN assignments, use the "Monitor > VLANs > VLAN Membership and VLAN Port" pages. These pages show which modules have (temporarily) overridden the current Port VLAN configuration.

Guest VLAN Operation:

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

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

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

Port State : The current state of the port. It can undertake one of the following values:

Globally Disabled: IEEE 802.1X is globally disabled.

Link Down: IEEE 802.1X is globally enabled, but there is no link on the port.

Authorized: The port is in Force Authorized or a single-supplicant mode and the supplicant is authorized.

Unauthorized: The port is in Force Unauthorized or a single-supplicant mode and the supplicant is not successfully authorized by the RADIUS server.

X Auth/Y Unauth: The port is in a multi-supplicant mode. Currently X clients are authorized and Y are unauthorized.

Restart : Two buttons are available for each row. The buttons are only enabled when authentication is globally enabled and the port's Admin State is in an EAPOL-based or MAC-based mode. Clicking these buttons will not cause settings changed on the page to take effect.

Re-authenticate: Schedules a re-authentication whenever the quiet-period of the port runs out (EAPOL-based authentication). For MAC-based authentication, re-authentication will be attempted immediately. The button only has effect for successfully authenticated clients on the port and will not cause the clients to get temporarily unauthorized.

Reinitialize: Forces a re-initialization of the clients on the port and thereby a re-authentication immediately. The clients will transfer to the unauthorized state while the re-authentication is in progress.

Buttons

Apply : Click to save changes.

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

Message: *NAS Error*
The 802.1X Admin State must be set to Authorized for ports that are enabled for Spanning Tree

15-2.2 Status

This page shows port 802.1X status information. The status includes Admin State, Port State, Last Source, Last ID, QoS Class and Port VLAN ID. To display 802.1X Status in the web UI:

1. Click Security, IEEE 802.1X ,and Status.
2. Click the Auto-refresh button.
3. Click “Refresh” to refresh the port detailed statistics.
4. You can click a port to display the 802.1X Statistics for that individual port.

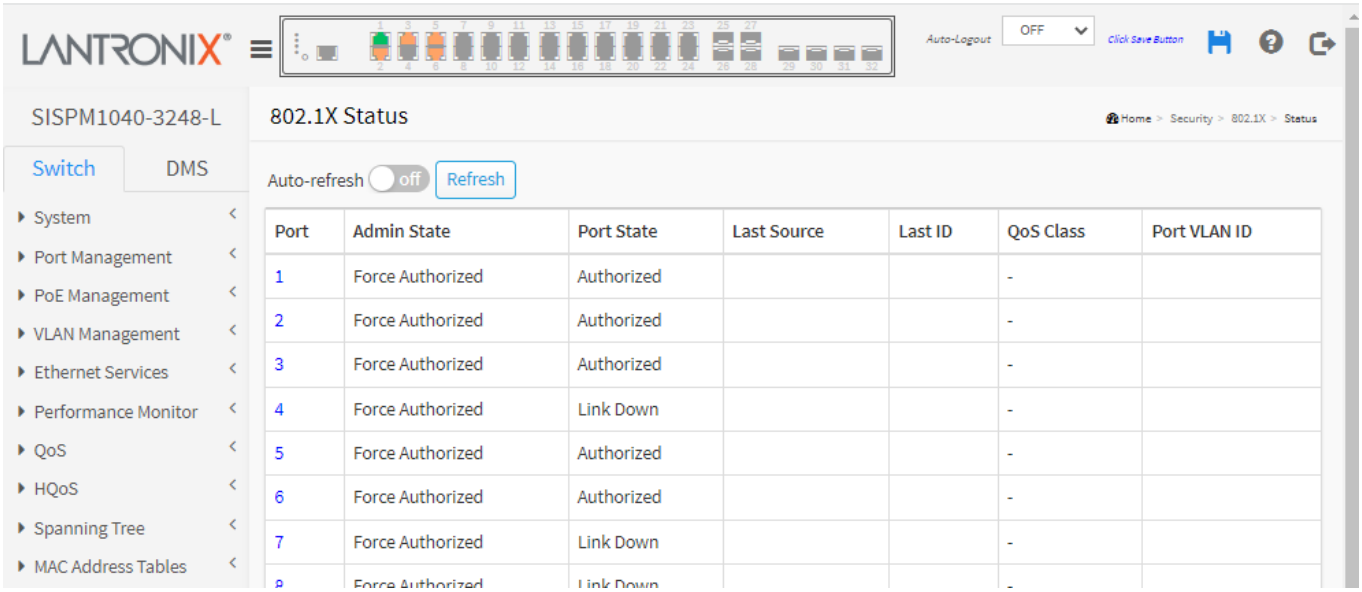


Figure 15-2.2: IEEE 802.1X Status

Parameter descriptions:

Port : The switch port number. Click to navigate to detail 802.1X statistics for this port.

Admin State : The port's current administrative state. Refer to 802.1X Admin State for a description of possible values.

Port State : The current state of the port. Refer to 802.1X Port State for a description of the individual states.

Last Source : The source MAC address carried in the most recently received EAPOL frame for EAPOL-based authentication, and the most recently received frame from a new client for MAC-based authentication.

Last ID : The user name (supplicant identity) carried in the most recently received Response Identity EAPOL frame for EAPOL-based authentication, and the source MAC address from the most recently received frame from a new client for MAC-based authentication.

QoS Class : QoS Class assigned to the port by the RADIUS server if enabled.

Port VLAN ID : The VLAN ID that 802.1X has put the port in. The field is blank if the Port VLAN ID is not overridden by 802.1X.
If the VLAN ID is assigned by the RADIUS server, "(RADIUS-assigned)" is appended to the VLAN ID. Read more about RADIUS-assigned VLANs here.

If the port is moved to the Guest VLAN, "(Guest)" is appended to the VLAN ID. Read more about Guest VLANs here.

Buttons

Auto-refresh : Click to refresh the page automatically every 3 seconds.

Refresh : Click to manually refresh the page immediately.

Individual Port Statistics: If you select port1 to display its 802.1X Port Status:

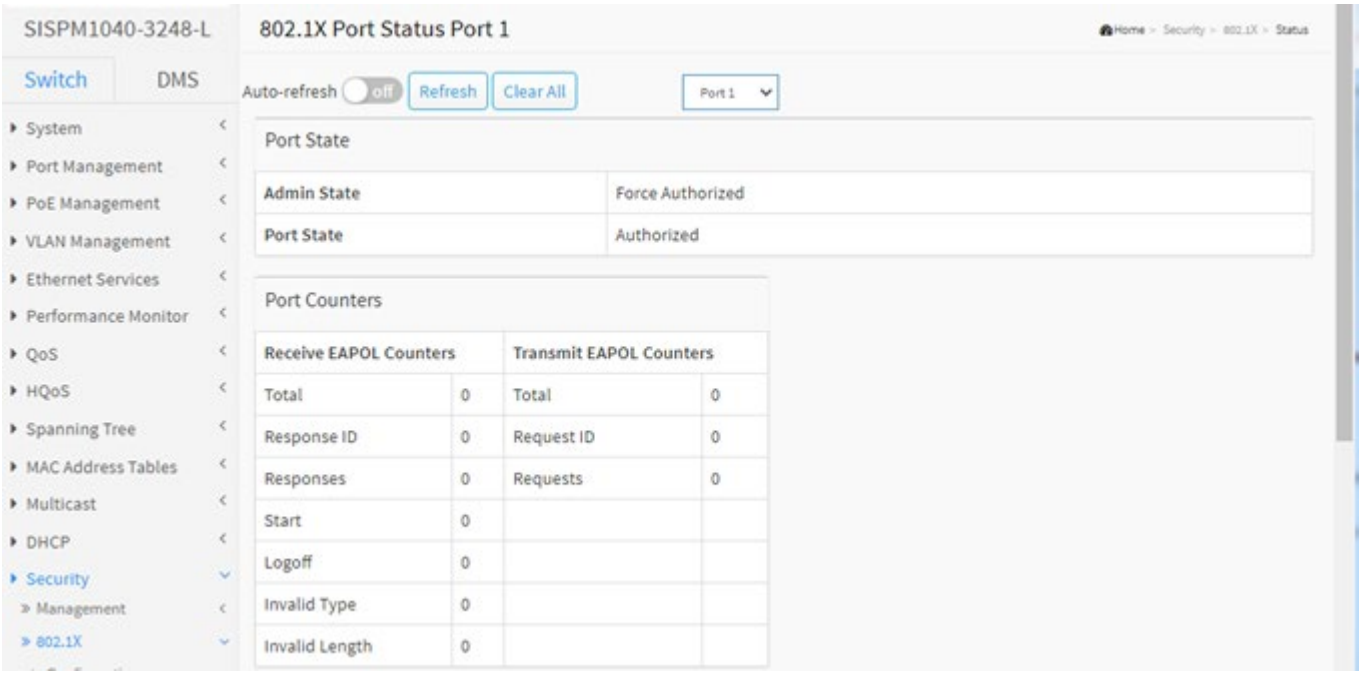


Figure 15-2.2: 802.1X Statistics Port 1

Parameter descriptions:

Port State :

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.

QoS Class: The QoS class assigned by the RADIUS server. The field is blank if no QoS class is assigned.

Port VLAN ID: The VLAN ID that 802.1X has put the port in. The field is blank if the Port VLAN ID is not overridden by 802.1X.
If the VLAN ID is assigned by the RADIUS server, "(RADIUS-assigned)" is appended to the VLAN ID.
If the port is moved to the Guest VLAN, "(Guest)" is appended to the VLAN ID.

Port Counters

EAPOL Counters : These supplicant frame counters are available for these administrative states:

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

EAPOL Counters:

Direction	Name	IEEE Name	Description
RX	Total	dot1xAuthEapolFramesRx	The number of valid EAPOL frames of any type that have been received by the switch.
RX	Response ID	dot1xAuthEapolRespIdFramesRx	The number of valid EAPOL Response Identity frames that have been received by the switch.
RX	Responses	dot1xAuthEapolRespFramesRx	The number of valid EAPOL response frames (other than Response Identity frames) that have been received by the switch.
RX	Start	dot1xAuthEapolStartFramesRx	The number of EAPOL Start frames that have been received by the switch.
RX	Logoff	dot1xAuthEapolLogoffFramesRx	The number of valid EAPOL Logoff frames that have been received by the switch.
RX	Invalid Type	dot1xAuthInvalidEapolFramesRx	The number of EAPOL frames that have been received by the switch in which the frame type is not recognized.
RX	Invalid Length	dot1xAuthEapLengthErrorFramesRx	The number of EAPOL frames that have been received by the switch in which the Packet Body Length field is invalid.
TX	Total	dot1xAuthEapolFramesTx	The number of EAPOL frames of any type that have been transmitted by the switch.
TX	Request ID	dot1xAuthEapolReqIdFramesTx	The number of EAPOL Request Identity frames that have been transmitted by the switch.
TX	Requests	dot1xAuthEapolReqFramesTx	The number of valid EAPOL Request frames (other than Request Identity frames) that have been transmitted by the switch.

Backend Server Counters : These backend (RADIUS) frame counters are available for these administrative states:

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

Backend Counters:

Direction	Name	IEEE Name	Description
RX	Access Challenges	dot1xAuthBackendAccessChallenges	802.1X-based: Counts the number of times that the switch receives the first request from the backend server following the first response from the supplicant. Indicates that the backend server has communication with the switch. MAC-based: Counts all Access Challenges received from the backend server for this port (left-most table) or client (right-most table).
RX	Other Requests	dot1xAuthBackendOtherRequestsToSupplicant	802.1X-based: Counts the number of times that the switch sends an EAP Request packet following the first to the supplicant. Indicates that the backend server chose an EAP-method. MAC-based: Not applicable. 802.1X- and MAC-based: Counts the number of times that the switch receives a success indication. Indicates that the supplicant/client has successfully authenticated to the backend server.
RX	Auth. Successes	dot1xAuthBackendAuthSuccesses	802.1X- and MAC-based: Counts the number of times that the switch receives a failure message. This indicates that the supplicant/client has not authenticated to the backend server.
RX	Auth. Failures	dot1xAuthBackendAuthFails	802.1X-based: Counts the number of times that the switch attempts to send a supplicant's first response packet to the backend server. Indicates the switch attempted communication with the backend server. Possible retransmissions are not counted.
TX	Responses	dot1xAuthBackendResponses	MAC-based: Counts all the backend server packets sent from the switch towards the backend server for a given port (left-most table) or client (right-most table). Possible retransmissions are not counted.

Last Supplicant/Client Info : Information about the last supplicant/client that attempted to authenticate. This information is available for these administrative states:

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

Last Supplicant/Client Info :

Name	IEEE Name	Description
MAC Address	dot1xAuthLastEapolFrameSource	The MAC address of the last supplicant/client.
VLAN ID -		The VLAN ID on which the last frame from the last supplicant/client was received.
Version	dot1xAuthLastEapolFrameVersion	802.1X-based: The protocol version number carried in the most recently received EAPOL frame. MAC-based: Not applicable.
Identity -		802.1X-based: The user name (supplicant identity) carried in the most recently received Response Identity EAPOL frame. MAC-based: Not applicable.

Selected Counters

Selected Counters : The Selected Counters table is visible when the port is in one of these administrative states:

- Multi 802.1X
- MAC-based Auth.

The table is identical to and is placed next to the Port Counters table, and will be empty if no MAC address is currently selected. To populate the table, select one of the attached MAC Addresses from the table below.

Attached MAC Addresses

Identity : Shows the identity of the supplicant, as received in the Response Identity EAPOL frame.

Clicking the link causes the supplicant's EAPOL and Backend Server counters to be shown in the Selected Counters table. If no supplicants are attached, it shows No supplicants attached.

This column is not available for MAC-based Auth.

MAC Address : For Multi 802.1X, this column holds the MAC address of the attached supplicant. For MAC-based Auth., this column holds the MAC address of the attached client.

Clicking the link causes the client's Backend Server counters to be shown in the Selected Counters table. If no clients are attached, it shows No clients attached.

VLAN ID : This column holds the VLAN ID that the corresponding client is currently secured through the Port Security module.

State : The client can either be authenticated or unauthenticated. In the authenticated state, it is allowed to forward frames on the port, and in the unauthenticated state, it is blocked. As long as the backend server hasn't successfully authenticated the client, it is unauthenticated. If an authentication fails for one or the other reason, the client will remain in the unauthenticated state for Hold Time seconds.

Last Authentication : Shows the date and time of the last authentication of the client (successful as well as unsuccessful).

Buttons

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

Refresh: Click to refresh the page immediately.

Clear: This button is available in the following modes:

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

Clear All: Click to clear the counters for the selected port. This button is available in these modes:

- Multi 802.1X
- MAC-based Auth.X

Clear This: Click to clear both the port counters and all of the attached client's counters. The "Last Client" will not be cleared, however. This button is available in these modes:

- Multi 802.1X
- MAC-based Auth.X

Click to clear only the currently selected client's counters.

15-3 IP Source Guard

This section lets you configure IP Source Guard detail parameters of the switch. IP Source Guard is a security feature used to restrict IP traffic on DHCP snooping untrusted ports by filtering traffic based on the DHCP Snooping Table or manually configured IP Source Bindings. It helps prevent IP spoofing attacks when a host tries to spoof and use the IP address of another host.

15-3.1 Configuration

This page describes how to configure IP Source Guard setting including Mode (Enabled or Disabled) and Maximum Dynamic Clients (0, 1, 2, Unlimited). To configure an IP Source Guard Configuration 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 of the specific port in the Mode of Port Mode Configuration.
5. Click Apply.

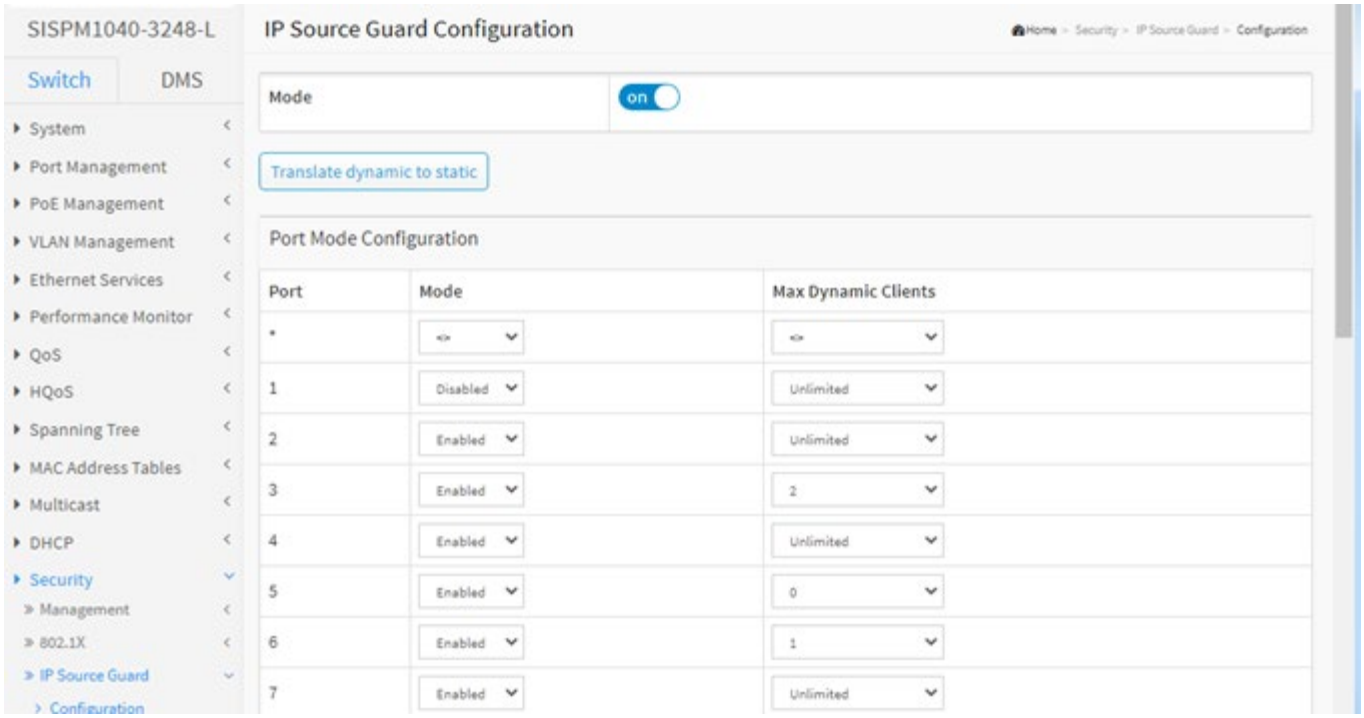


Figure 15-3.1: IP Source Guard Configuration

Parameter descriptions :

Mode of IP Source Guard Configuration : Enable the Global IP Source Guard or disable the IP Source Guard globally. All configured ACEs will be lost when the mode is enabled.

Port Mode Configuration : Specify IP Source Guard is enabled on which ports. Only when both Global Mode and Port Mode on a given port are enabled, IP Source Guard is enabled on this given port.

Max Dynamic Clients : Specify the maximum number of dynamic clients that can be learned on given port. This value can be 0, 1, 2 or unlimited. If the port mode is enabled and the value of max dynamic client is equal to 0, it means only allow the IP packets forwarding that are matched in static entries on the specific port.

Buttons

Apply : Click to save changes.

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

Translate dynamic to static : Click to translate all dynamic entries to static entries.

Message: *The new setting of max dynamic clients on some port maybe lost some dynamic entries. Do you want to proceed anyway?*

Meaning: You set Max Dynamic Clients to “Unlimited” for all ports.

Recovery:

1. Click the OK button to clear the message.
2. Either change Max Dynamic Clients to 1 or 2, or change Mode to Disabled for some ports.

15-3.2 Static Table

This page lets you configure the Static IP Source Guard Table parameters of the switch. To configure Static IP Source Guard parameters 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 for the entry.
4. Click Apply.

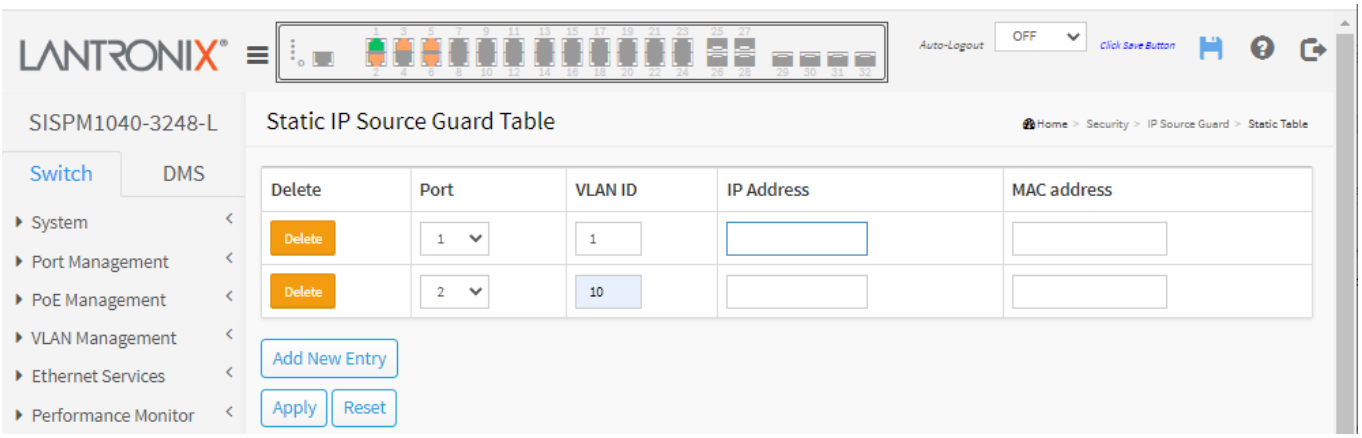


Figure 15-3.2: Static IP Source Guard Table

Parameter descriptions:

Port : The logical port for the settings.

VLAN ID : The VLAN ID for the settings.

IP Address : Allowed Source IP address.

MAC address : Allowed Source MAC address.

Buttons

Add New Entry : Click to add a new entry to the Static IP Source Guard table. Specify the Port, IP address, and MAC address for the new entry. Click "Apply".

Delete :Check to delete the entry. It will be deleted immediately.

Apply : Click to save changes.

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

15-3.3 Dynamic Table

Entries in the Dynamic IP Source Guard Table are shown on this page. The Dynamic IP Source Guard Table is sorted first by port, then by IP address, and then by MAC address.

To configure a Dynamic IP Source Guard Table Configuration 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/Next Page to change page.
5. Specify the Start from port, VLAN, IP Address, and entries per page.

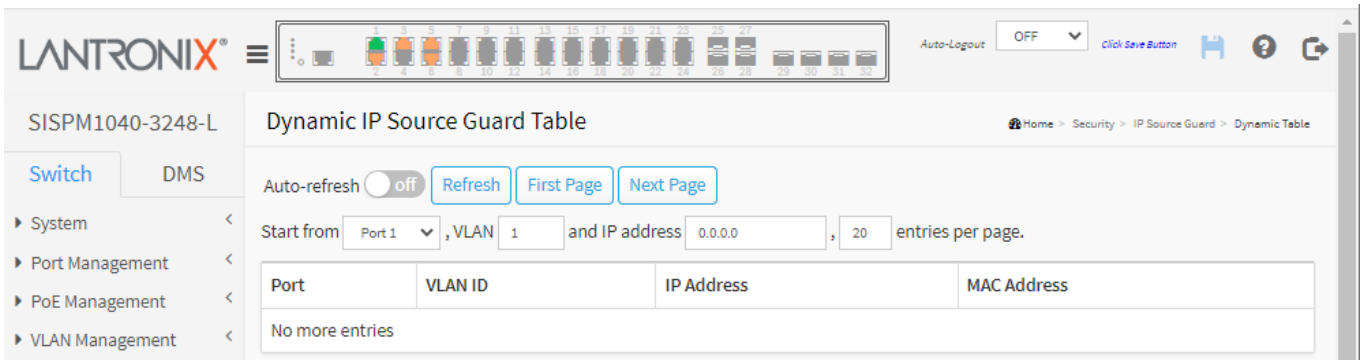


Figure 15-3.3: Dynamic IP Source Guard Table

Parameter descriptions:

Each page shows up to 99 entries from the Dynamic IP Source Guard table, default being 20, selected through the "entries per page" input field. When first visited, the web page will show the first 20 entries from the beginning of the Dynamic IP Source Guard Table.

The "Start from port address", "VLAN" and "IP address" input fields allow the user to select the starting point in the Dynamic IP Source Guard Table. Clicking “Refresh” the button will update the displayed table starting from that or the closest next Dynamic IP Source Guard Table match. In addition, the two input fields will - upon a “Refresh” button click - assume the value of the first displayed entry, allowing for continuous refresh with the same start address.

The Next Page button will use the last entry of the currently displayed table as a basis for the next lookup. When the end is reached the text "*No more entries*" is shown in the displayed table. Use the First Page button to start over.

Port : Switch Port Number for which the entries are displayed.

VLAN ID : VLAN-ID in which the IP traffic is permitted.

IP Address : User IP address of the entry.

MAC Address : Source MAC address.

Show entries : You can choose how many items you want to show.

Buttons

Auto-refresh : Click to refresh the page automatically every 3 seconds.

Refresh : Click to manually refresh the page immediately.

First Page : Updates the system log entries, turn to the first page.

Next Page : Updates the group information entries, turn to the next page.

15-4 ARP Inspection

This section lets you configure the ARP Inspection parameters of the switch. ARP (Address Resolution Protocol) is a protocol used to convert an IP address into a physical address, such as an Ethernet address. ARP allows a host to communicate with other hosts when only the Internet address of its neighbors is known. Before using IP, the host sends a broadcast ARP request containing the Internet address of the desired destination system.

15-4.1 Configuration

This page lets you configure ARP Inspection parameters. To configure ARP Inspection in the web UI:

1. Click Security, ARP Inspection, and Configuration.
2. Select “on” in the Mode of ARP Inspection Configuration.
3. Select Port Mode Configuration parameters.
4. Click Apply.

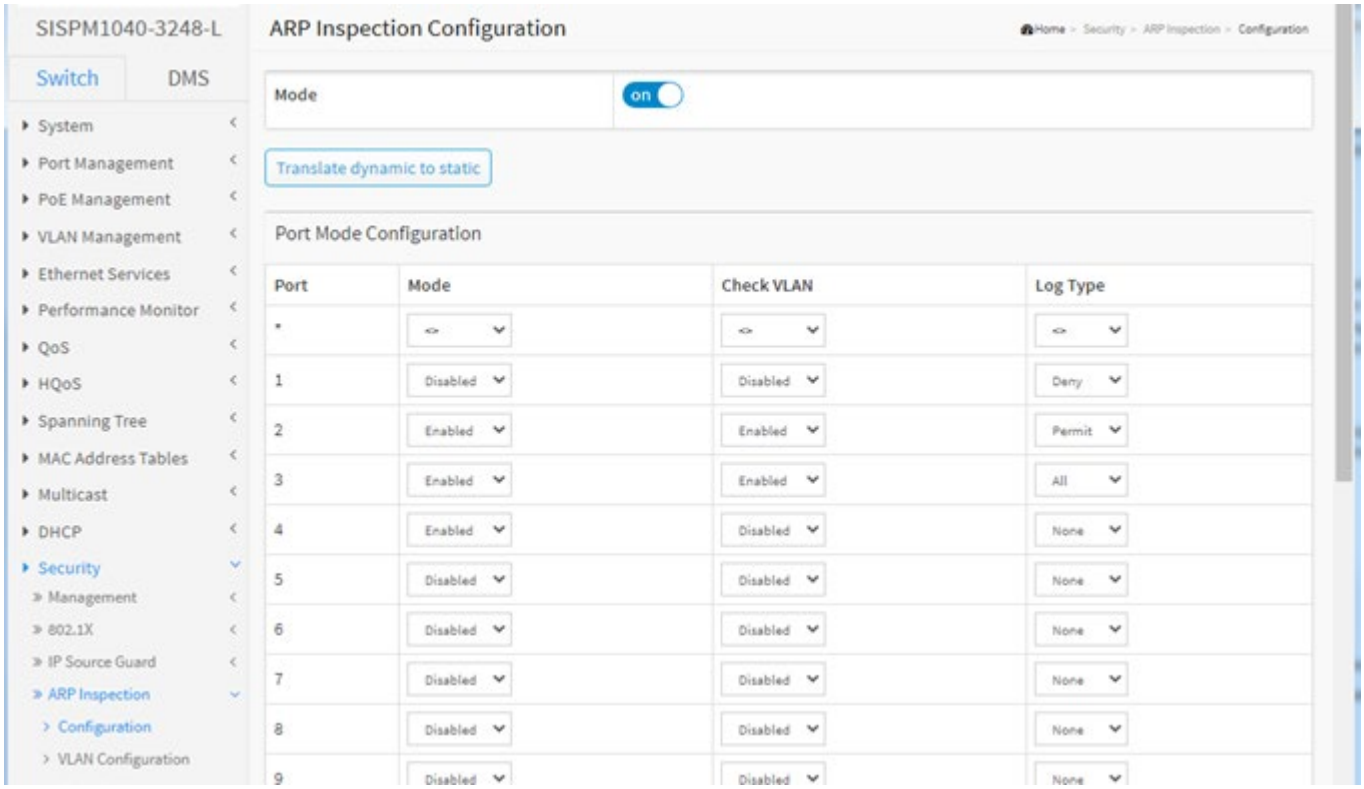


Figure 15-4.1: ARP Inspection Configuration

Parameter descriptions:

Mode : Select ***on*** to enable ARP Inspection globally, select ***off*** or disable global ARP Inspection.

Port Mode Configuration : Specify ARP Inspection is enabled on which ports. Only when both Global Mode and Port Mode on a given port are enabled, ARP Inspection is enabled on this given port. Possible modes are:

Enabled: Enable ARP Inspection operation.

Disabled: Disable ARP Inspection operation.

To inspect the VLAN configuration, enable the setting of "Check VLAN". The default setting of "Check VLAN" is disabled. When the setting of "Check VLAN" is disabled, the log type of ARP Inspection will refer to the port setting. After setting "Check VLAN" to enabled, the log type of ARP Inspection will refer to the VLAN setting. Possible setting of "Check VLAN" are:

Enabled: Enable check VLAN operation.

Disabled: Disable check VLAN operation.

Only when both Global Mode and Port Mode on a given port are enabled, and the setting of "Check VLAN" is disabled, the log type of ARP Inspection will refer to the port setting. There are four log types:

None: Log nothing.

Deny: Log denied entries.

Permit: Log permitted entries.

ALL: Log all entries.

Check VLAN : If you want to inspect the VLAN configuration, you have to enable the setting of "Check VLAN". The default setting of "Check VLAN" is disabled. When the setting of "Check VLAN" is disabled, the log type of ARP Inspection will refer to the port setting. And the setting of "Check VLAN" is enabled, the log type of ARP Inspection will refer to the VLAN setting. Possible setting of "Check VLAN" are:

Enabled: Enable check VLAN operation.

Disabled: Disable check VLAN operation.

Log Type : Only the Global Mode and Port Mode on a given port are enabled, and the setting of "Check VLAN" is disabled, the log type of ARP Inspection will refer to the port setting. The four possible log types are:

None: Log nothing.

Deny: Log denied entries.

Permit: Log permitted entries.

ALL: Log all entries.

Buttons

Apply : Click to save changes.

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

Translate dynamic to static : Click to translate all dynamic entries to static entries.

15-4.2 VLAN Configuration

Specify on which VLANs ARP Inspection is enabled. To configure VLAN Mode in the web UI:

1. Click Security, ARP Inspection, and VLAN Configuration.
2. Click “Add New Entry”.
3. Specify the VLAN ID and Log Type.
4. Click Apply.
5. Click First Entry/Next Entry to change Entry.

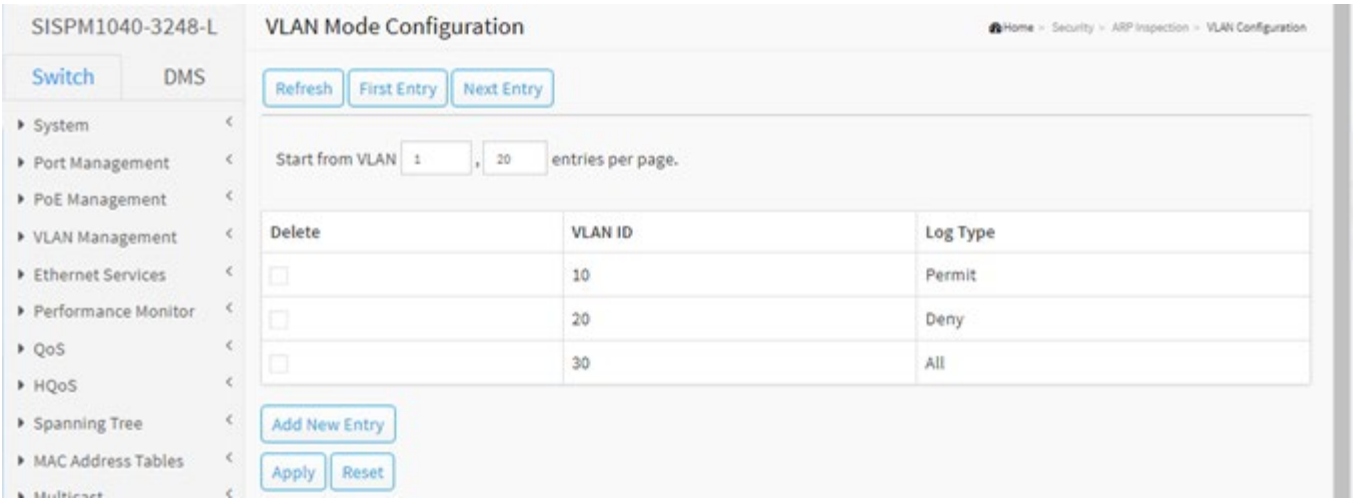


Figure 15-4.2: VLAN Mode Configuration

Parameter descriptions:

Each page shows up to 9999 entries from the VLAN table, default being 20, selected through the "entries per page" input field. When first visited, the web page will show the first 20 entries from the beginning of the VLAN Table. The first displayed will be the one with the lowest VLAN ID found in the VLAN Table.

The "VLAN" input fields allow the user to select the starting point in the VLAN Table. Clicking the “Refresh” button will update the displayed table starting from that or the closest next VLAN Table match. The “Next Entry” will use the next entry of the currently displayed VLAN entry as a basis for the next lookup. When the end is reached the warning message is shown in the displayed table. Use the First Entry button to start over.

VLAN Mode Configuration : Specify ARP Inspection is enabled on which VLANs. First, you must enable the port setting on Port mode configuration web page. Only when both Global Mode and Port Mode on a given port are enabled, ARP Inspection is enabled on this given port. Second, specify which VLAN will be inspected on VLAN mode configuration web page. The log type also can be configured on per VLAN setting.

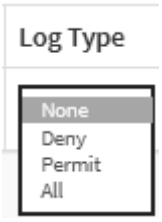
Possible log types are:

None: Log nothing.

Deny: Log denied entries.

Permit: Log permitted entries.

ALL: Log all entries.



Buttons

Add New Entry : Click to add a new VLAN to the ARP Inspection VLAN table.

Delete : Check to delete the entry. It will be deleted immediately.

Apply : Click to save changes.

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

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

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

Refresh : Click to manually refresh the page immediately.

15-4.3 Static Table

This page lets you set Static ARP Inspection Table parameters. To configure Static ARP Inspection 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.

Figure 15-4.3: Static ARP Inspection Table

Parameter descriptions:

Port : 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 immediately.

Apply : Click to save changes.

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

12-4.4 Dynamic Table

Entries in the Dynamic ARP Inspection Table are shown on this page. The Dynamic ARP Inspection Table contains up to 256 entries, and is sorted first by port, then by VLAN ID, then by MAC address, and then by IP address. All dynamic entries are learning from DHCP Snooping.

Each page shows up to 99 entries from the Dynamic ARP Inspection table, default being 20, selected through the "entries per page" input field. When first visited, the web page will show the first 20 entries from the beginning of the Dynamic ARP Inspection Table.

The "Start from port address", "VLAN", "MAC address" and "IP address" input fields allow the user to select the starting point in the Dynamic ARP Inspection Table. Clicking the “Refresh” button will update the displayed table starting from that or the closest next Dynamic ARP Inspection Table match. In addition, the two input fields will - upon a “Refresh” button click - assume the value of the first displayed entry, allowing for continuous refresh with the same start address.

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

To configure Dynamic ARP Inspection in the web UI:

1. Click Security, ARP Inspection, and Dynamic Table.
2. Click the Auto-refresh button.
3. Click “Refresh” to refresh the port detailed statistics.
4. Click First/Next Page to change pages.
5. Specify the Start from port, VLAN, MAC Address, IP Address, and entries per page.

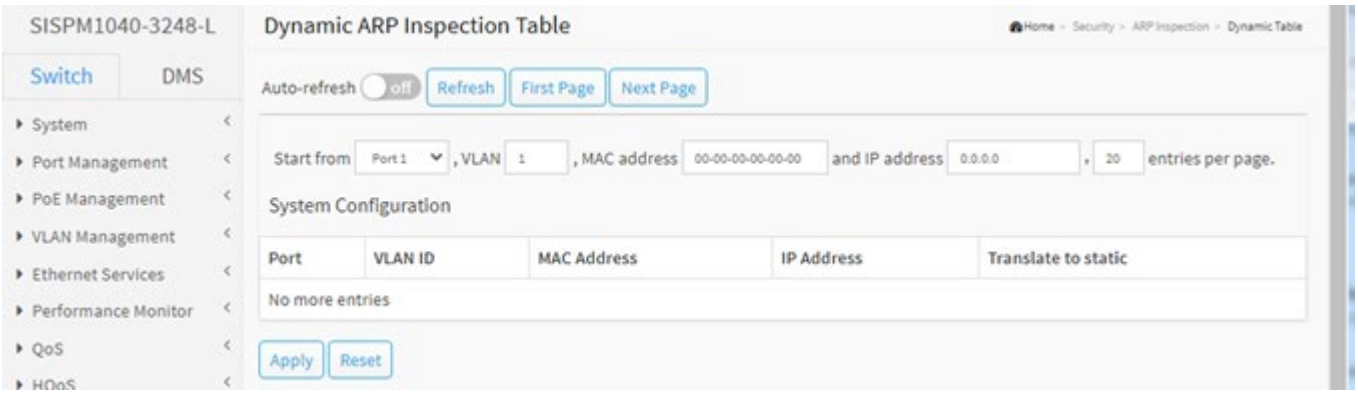


Figure 15-4.4: Dynamic ARP Inspection Table

Parameter descriptions:

Port : Switch Port Number for which the entries are displayed.

VLAN ID :VLAN ID in which the ARP traffic is permitted.

MAC Address :User MAC address of the entry.

IP Address : User IP address of the entry.

Show entries : Choose how many items you want to be displayed.

Buttons

Auto-refresh : Click to refresh the page automatically every 3 seconds.

Refresh :Click to manually refresh the page immediately.

First Page : Updates the system log entries, turn to the first page.

Next Page : Updates the group information entries, turn to the next page.

15-5 Port Security

12-5.1 Configuration

This page lets you configure Port Security global and per-port settings.

Port Security allows for limiting the number of users on a given port. A user is identified by a MAC address and VLAN ID. If Port Security is enabled on a port, the limit specifies the maximum number of users on the port. If this number is exceeded, an action is taken depending on violation mode as described below.

The Port Security configuration consists of two sections, a system section and a per-port section.

To configure Port Security in the web UI:

1. Click Security, Port Security and Configuration.
2. Click to Enable the Aging and specify Aging Period and Hold Time.
3. Set the Port Configuration parameters for each port.
4. Click the Apply button to save the settings

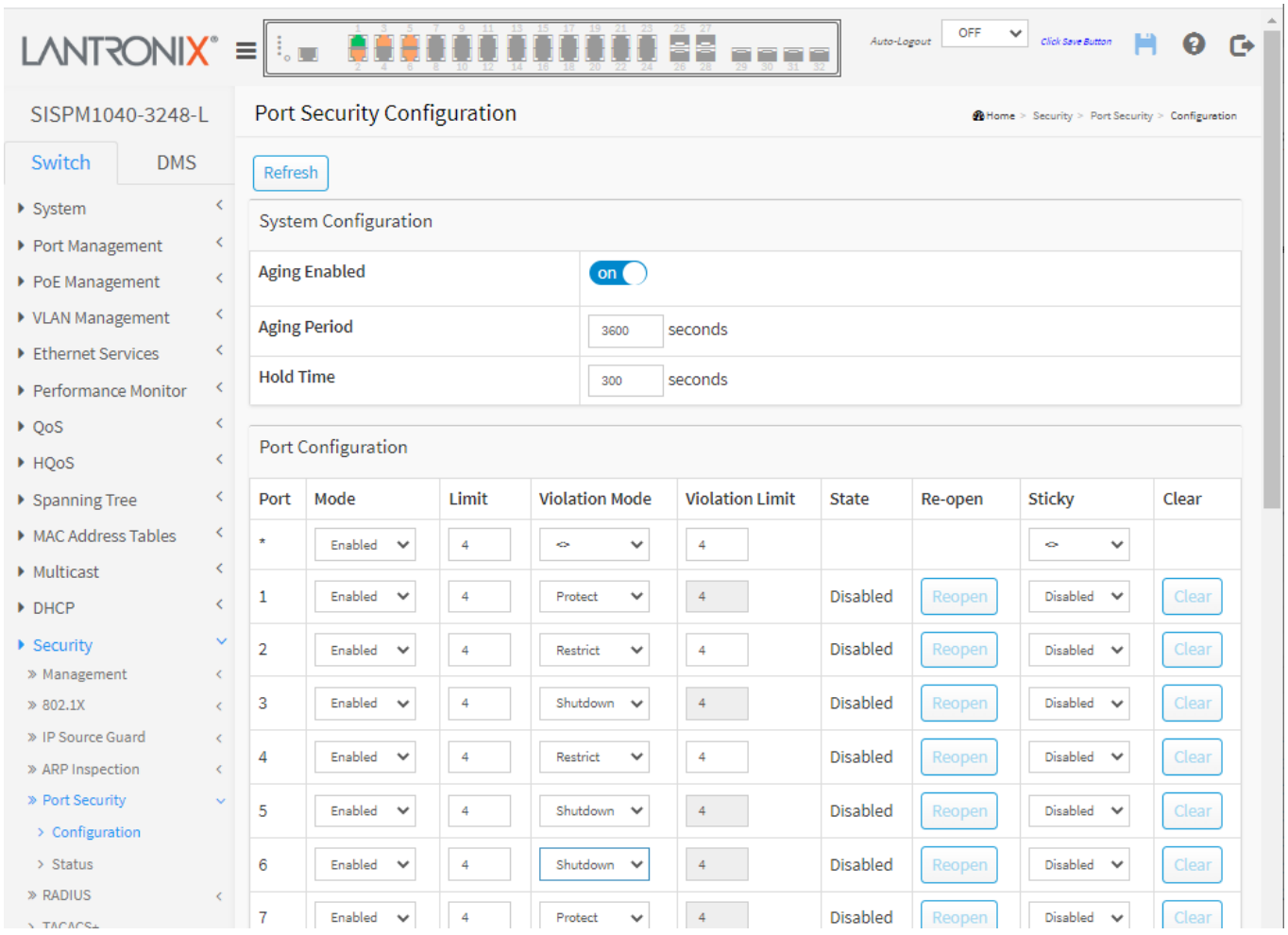


Figure 15-5.1: Port Security Configuration

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, 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 10 - 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. 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

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 these 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) At the Configuration > Ports page in the "Configured" column, first disable the port, then restore the original mode.

2) Make a Port Security configuration change on the port.

3) Boot the switch.

Violation Limit : The maximum number of MAC addresses that can be marked as violating on this port. This number cannot exceed 1023. Default is 4. It is only used when Violation Mode is Restrict.

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

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

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

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

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

Re-open button : If a port is shut down by this module, you may reopen it by clicking this button, which will only be enabled if this is the case. For other methods, refer to Shutdown in the Violation Mode section. Note that clicking the Reopen button causes the page to be refreshed, so non-committed changes will be lost.

Sticky : If running config has sticky MAC addresses, then these MAC addresses are automatically to be static MAC addresses on the MAC table.

Clear : To clear the static MAC addresses added by the sticky function.

Buttons

Apply : Click to save changes.

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

15-5.2 Status

This page shows the Port Security status.

Port Security may be configured both administratively and indirectly through other software modules - the so-called user modules. When a user module has enabled port security on a port, the port is set-up for software-based learning. In this mode, frames from unknown MAC addresses are passed on to the port security module, which in turn asks all user modules whether to allow this new MAC address to forward or block it. For a MAC address to be set in the forwarding state, all enabled user modules must unanimously agree on allowing the MAC address to forward. If only one chooses to block it, it will be blocked until that user module decides otherwise.

To display Port Security Status in the web UI:

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

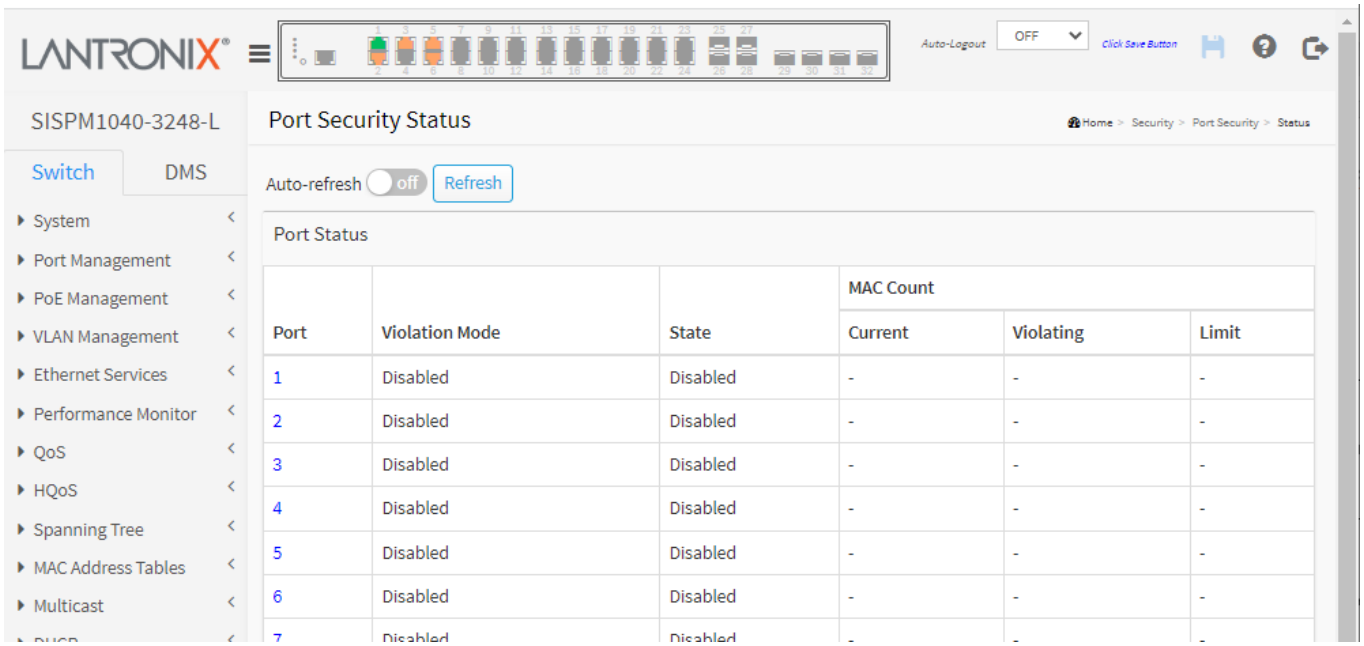


Figure 15-5.2: Port Security Status

Parameter descriptions:

Port : The port number for which the status applies. Click the port number to see the status for this particular port.

Violation Mode : Shows the configured Violation Mode of the port. It can take one of four values:

Disabled: Port Security is not administratively enabled on this port.

Protect: Port Security is administratively enabled in Protect mode.

Restrict: Port Security is administratively enabled in Restrict mode.

Shutdown: Port Security is administratively enabled in Shutdown mode.

State : Shows the current state of the port. It can take one of four values:

Disabled: No user modules are currently using the Port Security service.

Ready: The Port Security service is in use by at least one user module, and is awaiting frames from unknown MAC addresses to arrive.

Limit Reached: The Port Security service is enabled by at least the Limit Control user module, and that module has indicated that the limit is reached and no more MAC addresses should be taken in.

Shutdown: The Port Security service is enabled by at least the Limit Control user module, and that module has indicated that the limit is exceeded. No MAC addresses can be learned on the port until it is administratively re-opened on the Limit Control configuration Web-page.

MAC Count (Current, Violating, Limit) : The three columns indicate the number of currently learned MAC addresses (forwarding as well as blocked), the number of violating MAC address (only counting in Restrict mode) and the maximum number of MAC addresses that can be learned on the port, respectively.

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

If Port Security is not administratively enabled on the port, the Violating and Limit columns will show a dash (-).

Buttons

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

Refresh : Click to manually refresh the page immediately.

Individual Port Security Status : Click a linked port number to see the status for a particular port.

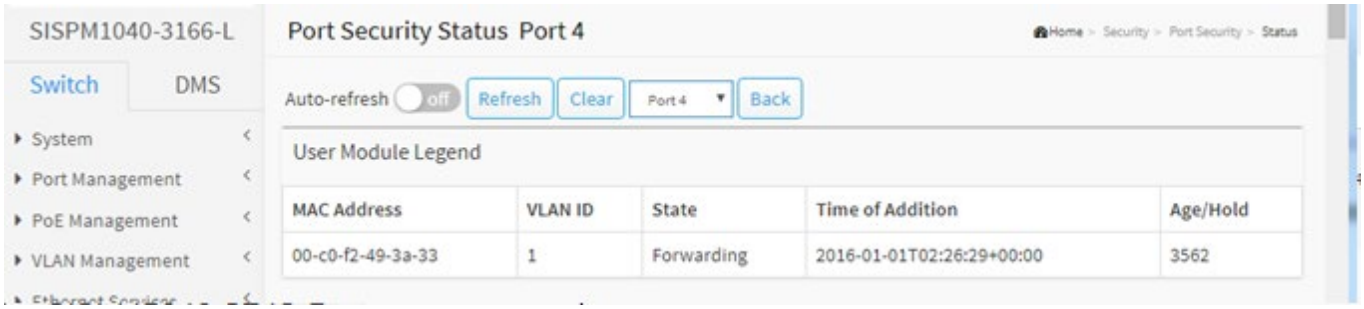


Figure 12-5.2: Port Security Status

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 (-) is displayed.

Buttons

Auto-refresh : Click to refresh the page automatically every 3 seconds.

Refresh : Click to manually refresh the page immediately.

Clear : Click to remove this particular MAC addresses from MAC table.

Port x : Select port that you want to display the Port Security Status.

Back : Click to go back Port Security Status.

15-6 RADIUS

15-6.1 Configuration

This page lets you configure up to five RADIUS servers. To configure RADIUS servers in the web UI:

1. Click Security, RADIUS, and Configuration.
2. Set the Global Configuration parameters.
3. Click “Add New Entry”.
4. Set the Server Configuration parameters.
5. Click Apply to save the settings.
6. To cancel the settings click the Reset button to revert to previously saved values.

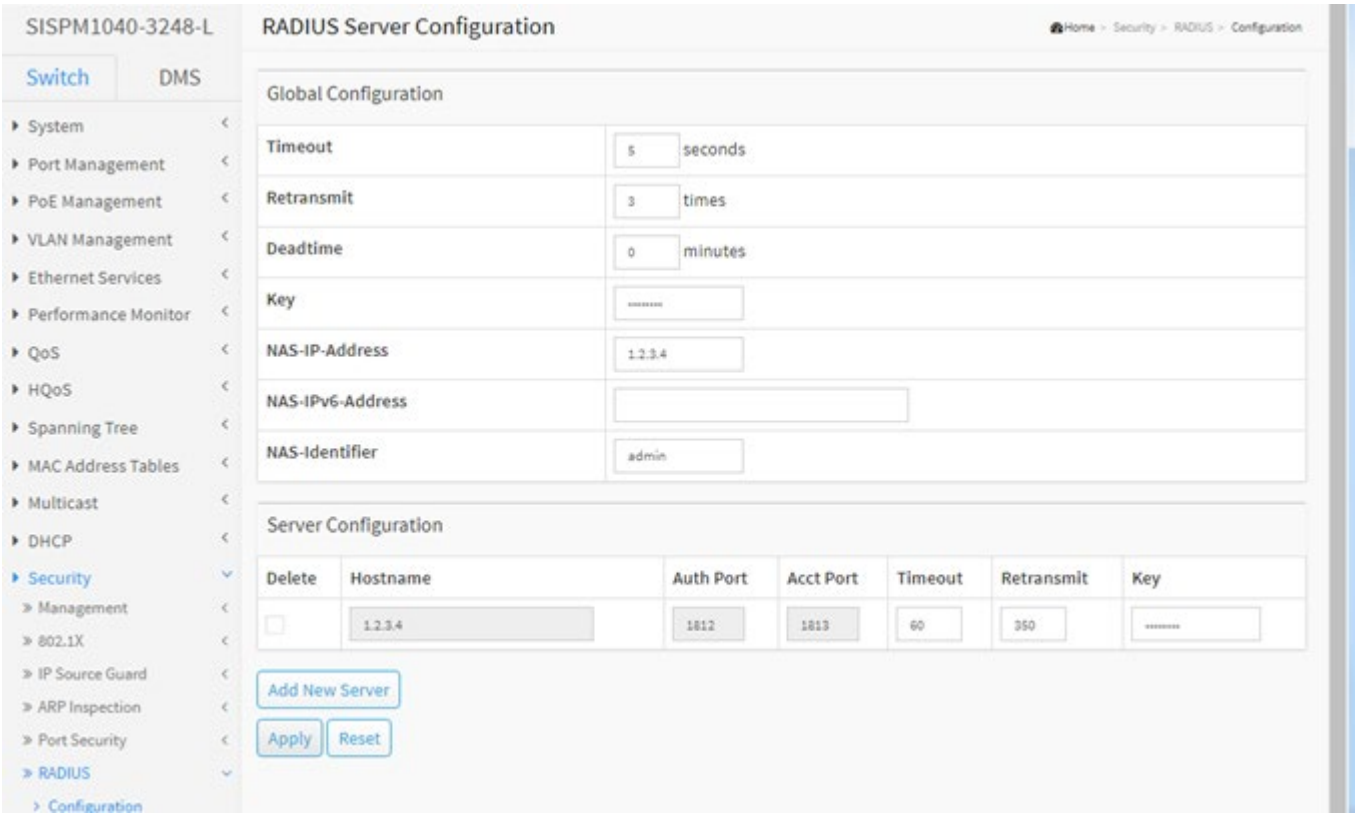


Figure 15-6.1: RADIUS Configuration

Parameter descriptions:

Global Configuration : These setting are common for all of the RADIUS servers.

Timeout : Timeout is the number of seconds, in the range 1 - 1000, to wait for a reply from a RADIUS server before retransmitting the request.

Retransmit : Retransmit is the number of times, in the range 1 - 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 (Attribute 4) : 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 (Attribute 95): 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 (Attribute 32) : The identifier - up to 255 characters long - to be used as attribute 32 in RADIUS Access-Request packets. If this field is left blank, the NAS-Identifier is not included in the packet.

Server Configuration : The table has one row for each RADIUS server and a number of columns:

Hostname : The IP address or hostname of the RADIUS server.

Auth Port : The UDP port to use on the RADIUS server for authentication. Set to 0 to disable authentication. The officially assigned port number for RADIUS Accounting is 1812. **Note**: by default, many access servers use port 1645 for authentication requests.

> **Note**: For Windows Server information on how to configure ports that Network Policy Server (NPS) uses for Remote Authentication Dial-In User Service (RADIUS) authentication and accounting traffic see https://docs.microsoft.com/en-us/windows-server/networking/technologies/nps/nps-udp-ports-configure#:~:text=The%20port%20values%20of%201812,and%201646%20for%20accounting%20requests

Acct Port : The UDP port to use on the RADIUS server for accounting. Set to 0 to disable accounting. The officially assigned port number for RADIUS Accounting is 1813. **Note**: by default, many access servers use port 1646 for accounting requests.

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 won't change the current key.

Buttons

Delete : To delete a RADIUS server entry, check this box. The entry will be deleted during the next Save.

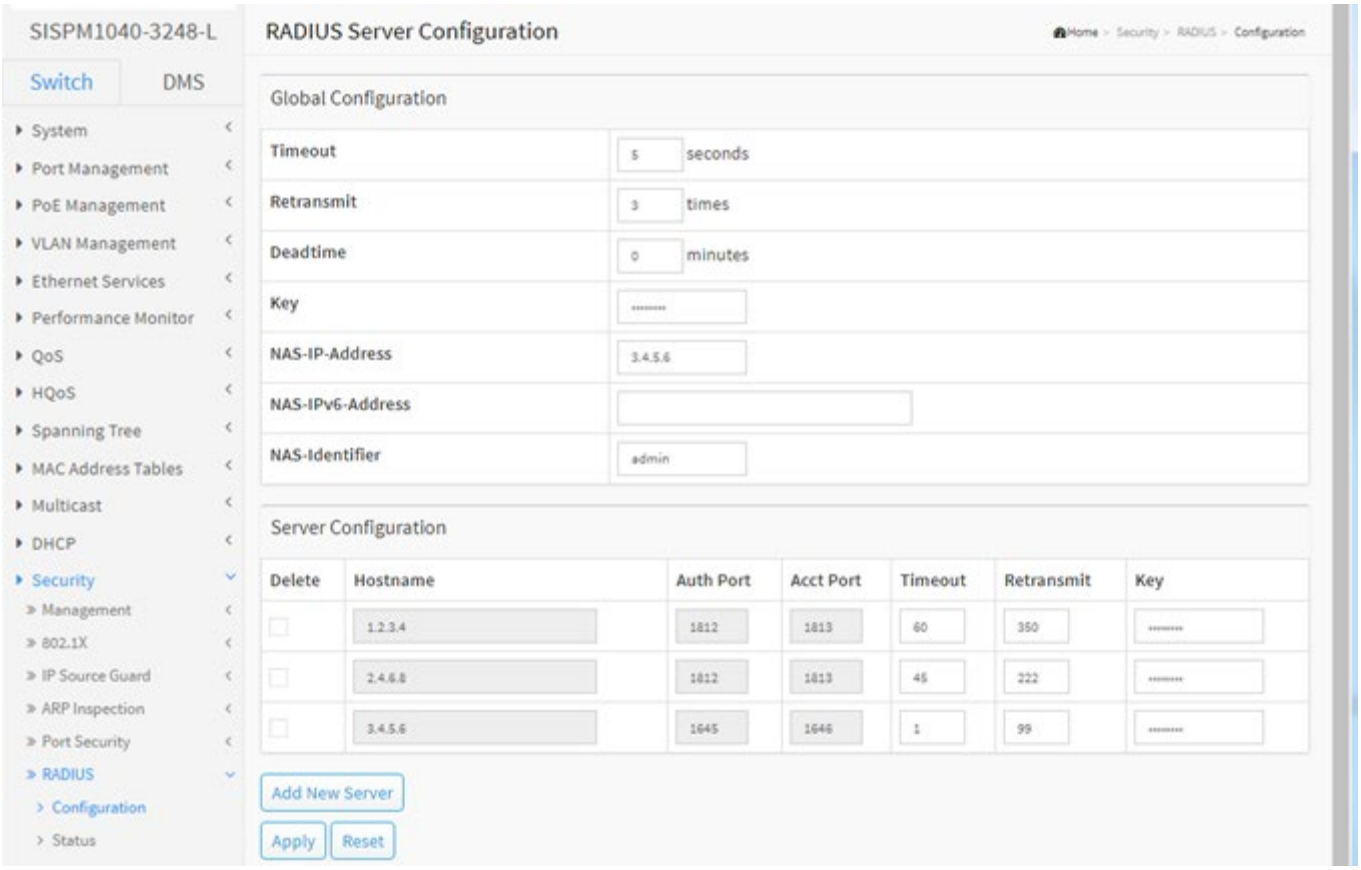
Add New Server : Click to add a new RADIUS server. An empty row is added to the table, and the RADIUS server can be configured as needed. Up to 5 servers are supported. The Reset button can be used to undo the addition of the new server.

Apply : Click to save changes.

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

Messages: Authentication Error Invalid secret key configuration parameter

Example:


SISPM1040-3248-L
Switch
DMS
System
Port Management
PoE Management
VLAN Management
Ethernet Services
Performance Monitor
QoS
HQoS
Spanning Tree
MAC Address Tables
Multicast
DHCP
Security
Management
802.1X
IP Source Guard
ARP Inspection
Port Security
RADIUS
Configuration
Status
RADIUS Server Configuration
Home > Security > RADIUS > Configuration
Global Configuration
Timeout
5
seconds
Retransmit
3
times
Deadtime
0
minutes
Key
NAS-IP-Address
3.4.5.6
NAS-IPv6-Address
NAS-Identifier
admin
Server Configuration
Delete
Hostname
Auth Port
Acct Port
Timeout
Retransmit
Key
1.2.3.4
1812
1813
60
350
2.4.6.8
1812
1813
45
222
3.4.5.6
1645
1646
1
99
Add New Server
Apply
Reset

15-6.2 Status

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

To display RADIUS Status in the web UI:

1. Click Security, RADIUS and Status.
2. Select server to display the detail statistics for a particular RADIUS

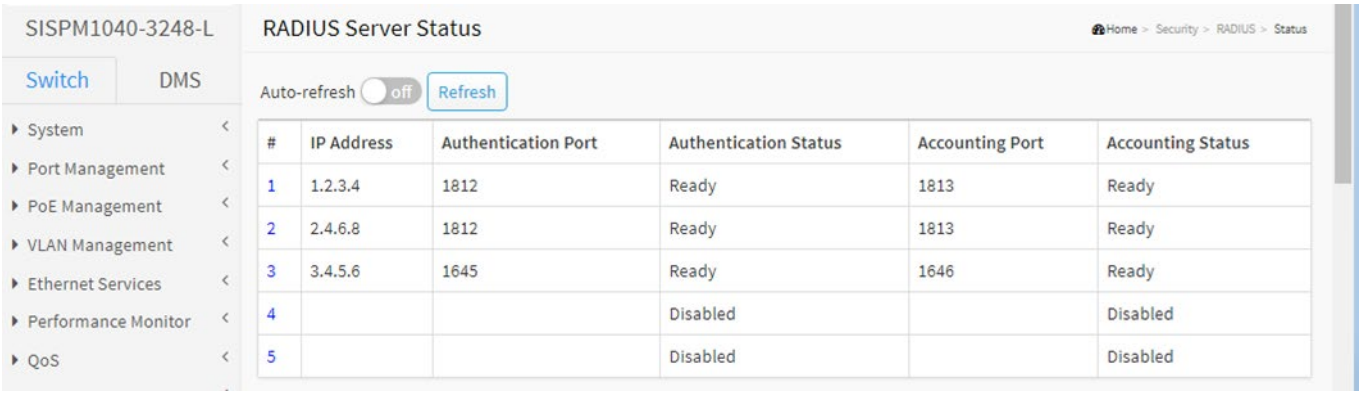


Figure 15-6.2: RADIUS Server Status

Parameter descriptions:

: The RADIUS server number. Click to navigate to detailed statistics for this server (see example below).

IP Address : The IP address and UDP port number (in <IP Address>:<UDP Port> notation) of this server.

Authentication Port : UDP port number for authentication.

Authentication Status : The current status of the server. This field takes one of the following values:

Disabled: The server is disabled.

Not Ready: The server is enabled, but IP communication is not yet up and running.

Ready: The server is enabled, IP communication is up and running, and the RADIUS module is ready to accept access attempts.

Dead (X seconds left): Access attempts were made to this server, but it did not reply within the configured timeout. The server has temporarily been disabled, but will get re-enabled when the dead-time expires. The number of seconds left before this occurs is displayed in parentheses. This state is only reachable when more than one server is enabled.

Accounting Port : UDP port number for accounting.

Accounting Status : The current status of the server. This field takes one of the following values:

Disabled: The server is disabled.

Not Ready: The server is enabled, but IP communication is not yet up and running.

Ready: The server is enabled, IP communication is up and running, and the RADIUS module is ready to accept access attempts.

Dead (X seconds left): Access attempts were made to this server, but it did not reply within the configured timeout. The server has temporarily been disabled, but will get re-enabled when the dead-time expires. The number of seconds left before this occurs is displayed in parentheses. This state is only reachable when more than one server is enabled.

Buttons

Auto-refresh : Click to refresh the page automatically every 3 seconds.

Refresh : Click to manually refresh the page immediately.

Example: If you select Server#1 to display RADIUS Statistics:

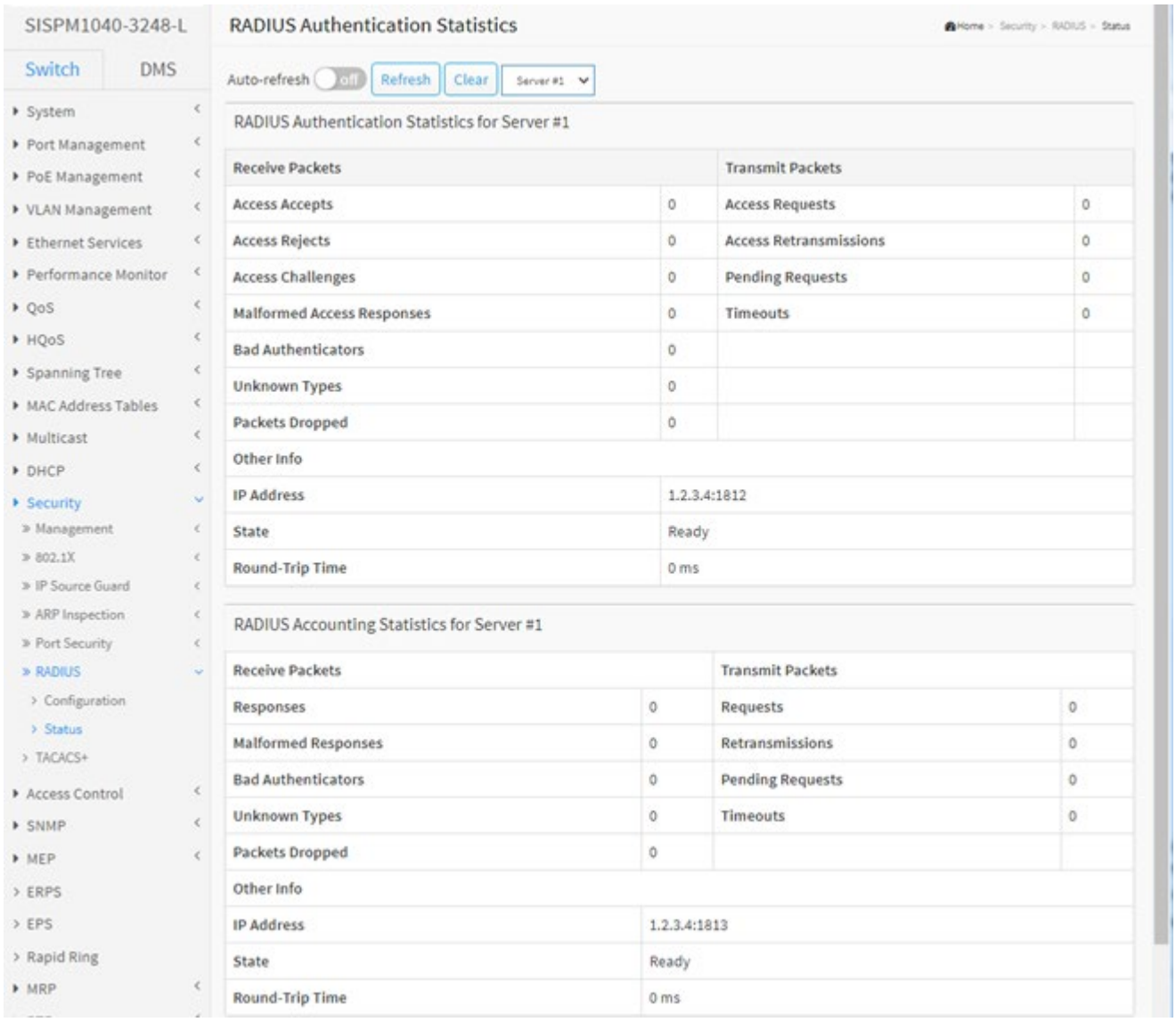


Figure 15-6.2: RADIUS Authentication Statistics for Server # 1

Parameter descriptions:

Server : At the server select dropdown select which server that you want to display RADIUS statistics for.

RADIUS Authentication Statistics: The Receive Packets and Transmit Packets statistics map closely to those specified in RFC4668 - RADIUS Authentication Client MIB. Use the server select box to switch between the backend servers to show details for.

Access Accepts : The number of RADIUS Access-Accept packets (valid or invalid) received from the server.

Access Rejects : The number of RADIUS Access-Reject packets (valid or invalid) received from the server.

Access Challenges : The number of RADIUS Access-Challenge packets (valid or invalid) received from the server.

Malformed Access Responses : The number of malformed RADIUS Access-Response packets received from the server. Malformed packets include packets with an invalid length. Bad authenticators or Message Authenticator attributes or unknown types are not included as malformed access responses.

Bad Authenticators : The number of RADIUS Access-Response packets containing invalid authenticators or Message Authenticator attributes received from the server.

Unknown Types : The number of RADIUS packets that were received with unknown types from the server on the authentication port and dropped.

Packets Dropped : The number of RADIUS packets that were received from the server on the authentication port and dropped for some other reason.

Access Requests : The number of RADIUS Access-Request packets sent to the server. This does not include retransmissions.

Access Retransmissions : The number of RADIUS Access-Request packets retransmitted to the RADIUS authentication server.

Pending Requests : The number of RADIUS Access-Request packets destined for the server that have not yet timed out or received a response. This variable is incremented when an Access-Request is sent and decremented due to receipt of an Access-Accept, Access-Reject, Access-Challenge, timeout, or retransmission.

Timeouts : The number of authentication timeouts to the server. After a timeout, the client may retry to the same server, send to a different server, or give up. A retry to the same server is counted as a retransmit as well as a timeout. A send to a different server is counted as a Request as well as a timeout.

IP Address : IP address and UDP port for the authentication server in question.

State : Shows the state of the server. It takes one of the following values:

Disabled : The selected server is disabled.

Not Ready : The server is enabled, but IP communication is not yet up and running.

Ready : The server is enabled, IP communication is up and running, and the RADIUS module is ready to accept access attempts.

Dead (X seconds left) : Access attempts were made to this server, but it did not reply within the configured timeout. The server has temporarily been disabled, but will get re-enabled when the dead-

time expires. The number of seconds left before this occurs is displayed in parentheses. This state is only reachable when more than one server is enabled.

Round-Trip Time : The time interval (measured in milliseconds) between the most recent Access-Reply / Access-Challenge and the Access-Request that matched it from the RADIUS authentication server. The granularity of this measurement is 100 ms. A value of 0 ms indicates that there hasn't been round-trip communication with the server yet.

RADIUS Accounting Statistics: The Receive Packets and Transmit Packets 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 : Click to refresh the page automatically every 3 seconds.

Refresh : Click to manually refresh the page immediately.

Clear : Clears the counters for the selected server. The "Pending Requests" counter will not be cleared by this operation.

15-7 TACACS+

This page lets you configure up to 5 TACACS+ servers. To configure TACACS+ servers in the web UI:

1. Click Security and TACACS+. Please set the Global Configuration key first.
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.

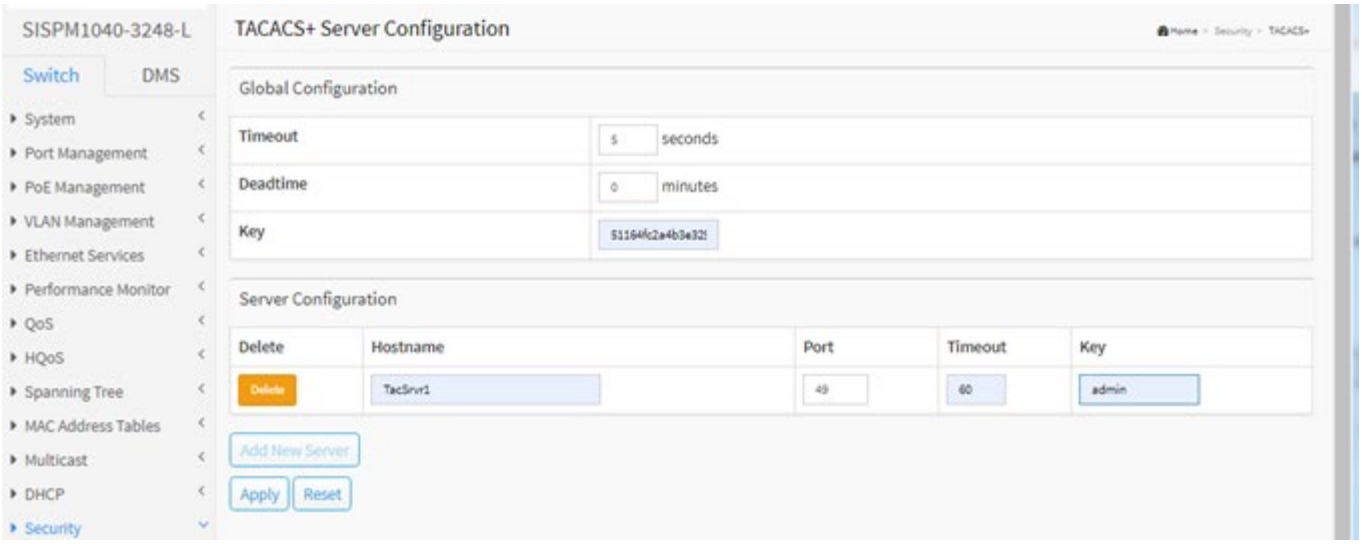


Figure 15-7: TACACS+ Server Configuration

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.
Note: You must set the global configuration key before you can set the Server Configuration parameters.

Server Configuration : The table has one row for each TACACS+ server and a number of columns, which are:

Delete : To delete a TACACS+ server entry, check this box. The entry will be deleted during the next Save.

Hostname : The IP address or hostname of the TACACS+ server.

Port : The TCP port to use on the TACACS+ server for authentication.

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

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

Buttons

Delete : This button can be used to undo the addition of the new server.

Add New Server : Click to add a new TACACS+ server. An empty row is added to the table, and the TACACS+ server can be configured as needed. Up to 5 servers are supported.

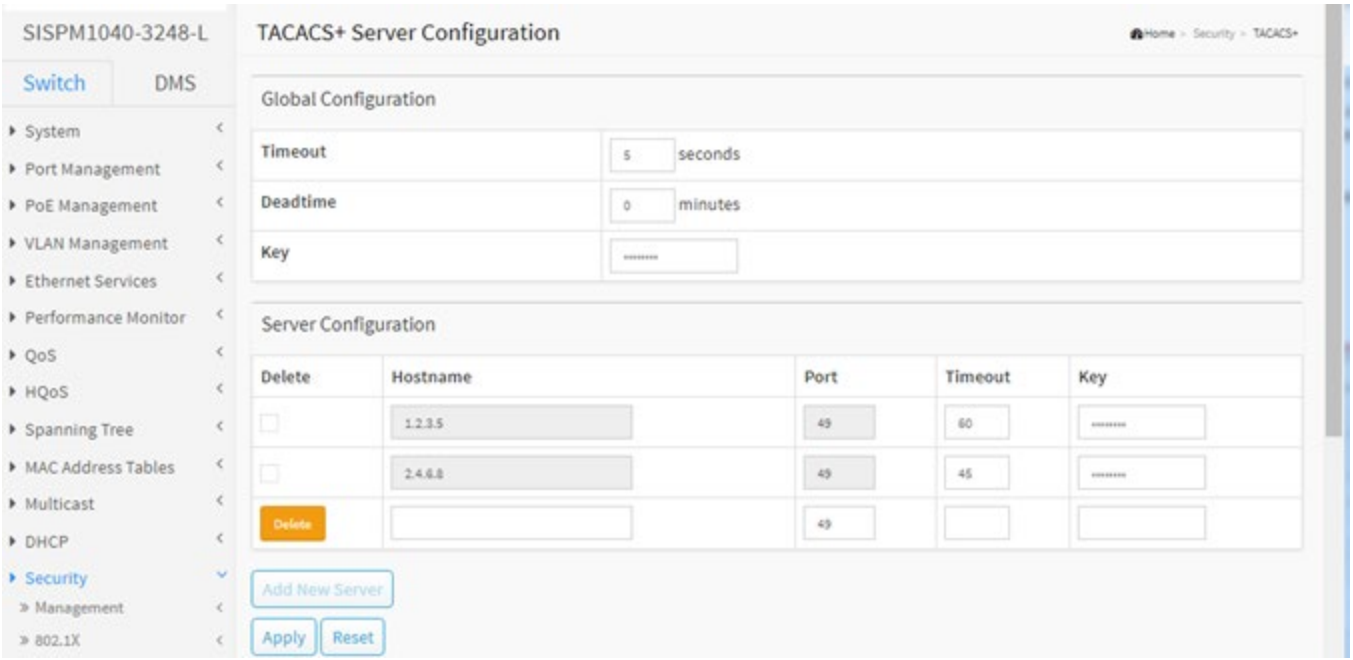
Apply : Click to save changes.

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

Messages:

Please set the global configuration key first.
invalid host address

Example:



Chapter 16 - Access Control

16-1 Ports Configuration

Configure the ACL parameters (ACE) of each switch port. These parameters will affect frames received on a port unless the frame matches a specific ACE.

To configure ACL Ports in the web UI:

1. Click Access Control and Port Configuration.
2. Select the desired values for port ACL settings.
3. Click Apply to save the settings.
4. To cancel the settings click the Reset button. It will revert to previously saved values.
5. When configured completely you can view the ACL Ports Configuration. You can click Refresh to update the counter or click Clear to clear the information.

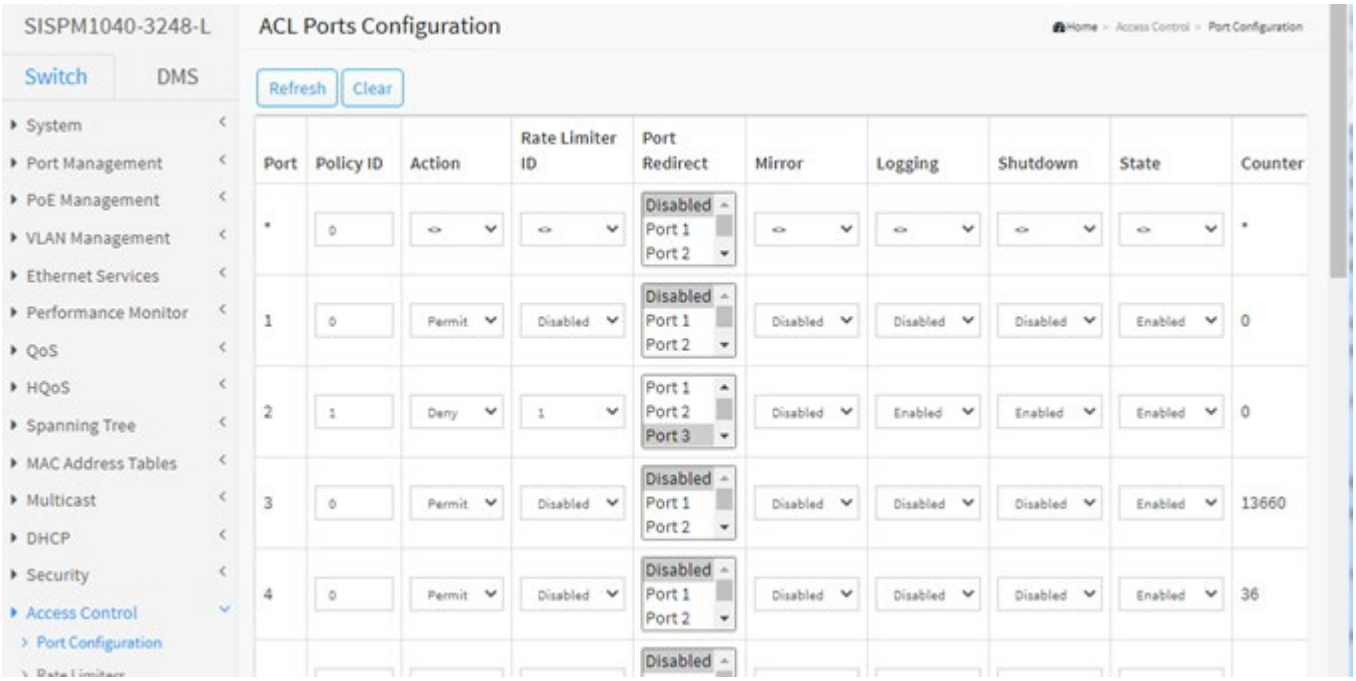


Figure 16-1: ACL Ports Configuration

Parameter descriptions:

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

Policy ID : Select the policy to apply to this port. The allowed values are 1 - 8. The default is 1.

Action : Select whether forwarding is permitted ("Permit") or denied ("Deny"). The default is "Permit".

Rate Limiter ID : Select which rate limiter to apply on this port. The allowed values are Disabled or 1 - 16. The default 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 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 System Log memory size and logging rate is limited.

Shutdown : Specify the port shut down operation of this port. The allowed values are:

Enabled: If a frame is received on the port, the port will be disabled.

Disabled: Port shut down is disabled. The default value is "Disabled".

State : Specify the port state of this port. The allowed values are:

Enabled: To reopen ports by changing the volatile port configuration of the ACL user module.

Disabled: To close ports by changing the volatile port configuration of the ACL user module. The default value is "Enabled"

Counter : Counts the number of frames that match this ACE.

Buttons

Refresh : Click to manually refresh the page immediately.

Clear : Click to clear the page data manually.

Apply : Click to save changes.

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

Messages: *The parameter of 'Port Redirect' can't be set when action is permitted*

16-2 Rate Limiters

This page lets you set switch ACL Rate Limiter parameters. The Rate Limiter Level (1 to 16) lets you set rate limiter value and unit of measure.

An ACL (Access Control List) is a table of ACEs, containing Access Control Entries that specify individual users or groups permitted or denied to specific traffic objects, such as a process or a program. Each accessible traffic object contains an identifier to its ACL. The privileges determine whether there are specific traffic object access rights.

To configure ACL Rate Limiter in the web UI:

1. Click Access Control and Rate Limiters.
2. Specify the Rate and Unit of measure.
3. Click Apply to save the settings. To cancel the settings click the Reset button to revert to previously saved values.

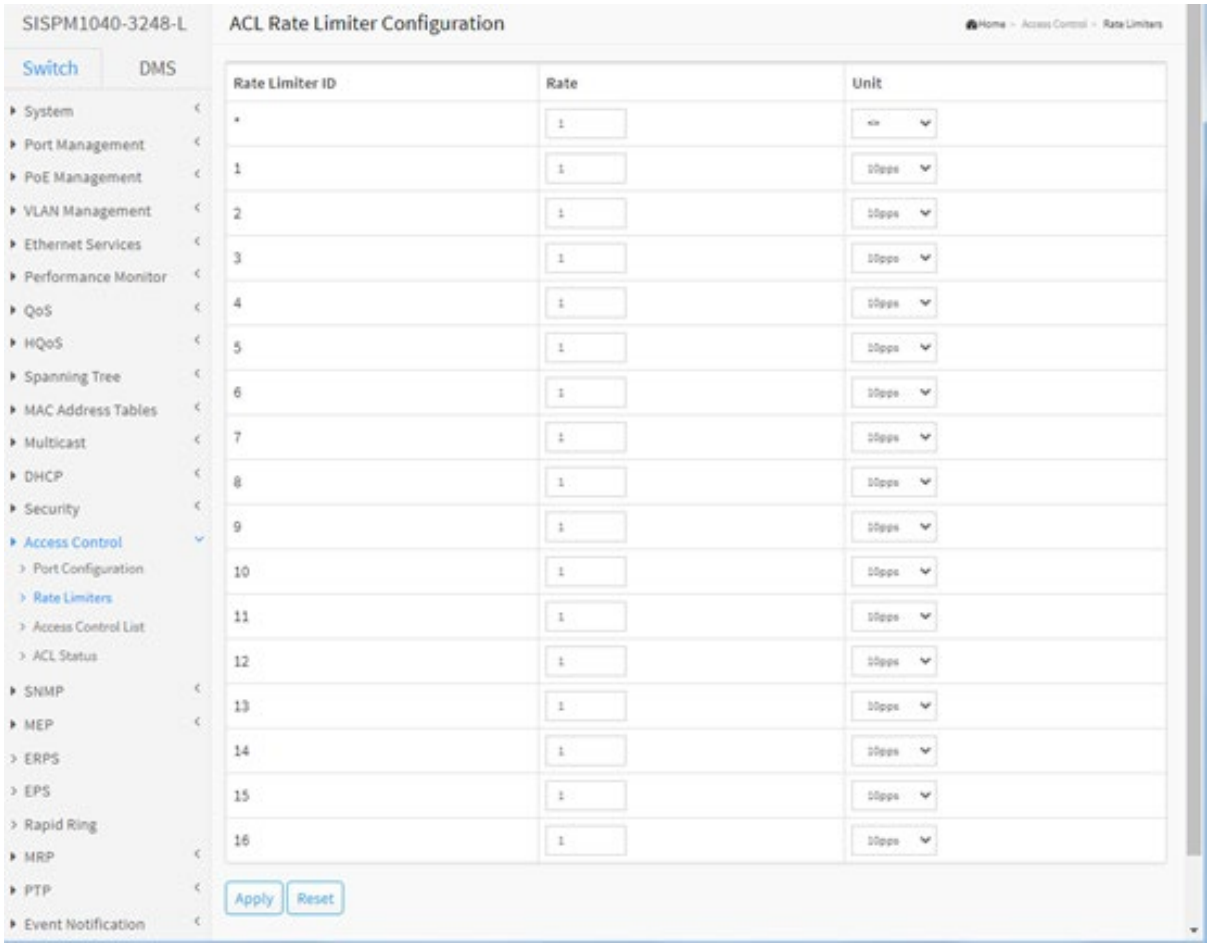


Figure 16-2: ACL Rate Limiter Configuration

Parameter descriptions:

Rate Limiter ID : The rate limiter ID for the settings contained in the same row and its range is 1 to 16.

Rate : The valid rate is 0, 10, 20, 30, ..., 5000000 in pps or 0, 25, 50, 75, ..., 10000000 in kbps.

Unit : Specify the rate unit of measure. The allowed values are:

10pps: Ten packets per second.

25kbps: Twenty-five Kbits per second.

Buttons

Apply: Click to save changes.

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

16-3 Access Control List

This page shows the Access Control List (ACL), which is made up of the ACEs defined on this switch. Each row describes the ACE that is defined. The maximum number of ACEs is 512 on each switch.

Click on the lowest plus sign to add a new ACE to the list. The reserved ACEs used for internal protocol, cannot be edited or deleted, the order sequence cannot be changed and the priority is highest.

To configure Access Control List in the web UI:

1. Click Access Control and Access Control List.
2. Click the Add ACE ( ) icon to add a new ACL, or use the other ACL modification buttons to specify the editing action (i.e., edit, delete, or move the relative position of entry in the list).
3. Specify the ACE parameters.
4. Click the Apply button to save the settings. To cancel the settings click the Reset button to revert to previously saved values.
5. When editing an entry on the ACE Configuration page, note that the parameters displayed depend on various selections, such as Frame Type and IP Protocol Type. Specify the relevant parameters to be matched for this rule, and set the actions to take when a rule is matched (such as Rate Limiter, Port Copy, Logging, and Shutdown).

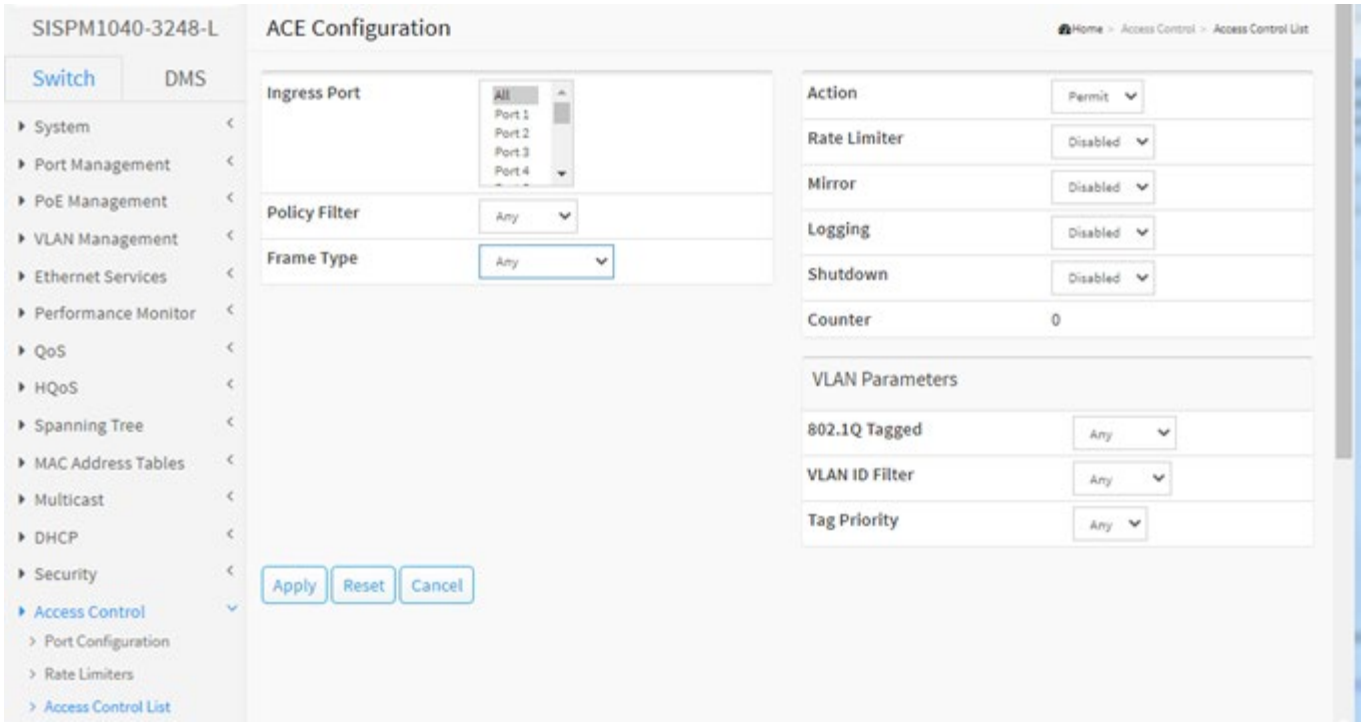


Figure 16-3: Access Control List Configuration

Parameter descriptions :

ACE : Indicates the ACE ID. An ACE (Access Control Entry) describes access permission associated with a particular ACE ID. There are three ACE frame types (Ethernet Type, ARP, and IPv4) and two ACE actions (permit and deny). The ACE also contains many detailed, different parameter options that are available for individual application.

Policy / Bitmask: Indicates the policy number and bitmask of the ACE.

Ingress Port: Select 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.

Policy Filter : Select ***Any*** or ***Specific***.

Frame Type : Select the frame type for this ACE. These frame types are mutually exclusive:

Any: The ACE will match any frame type.

Ethernet Type: The ACE will match Ethernet Type frames. Note that an Ethernet Type based ACE will not get matched by IP and ARP frames.

ARP: The ACE will match ARP/RARP frames.

IPv4: The ACE will match all IPv4 frames.

IPv6: The ACE will match all IPv6 standard frames.

Action : Indicates the forwarding action of the ACE.

Permit: Frames matching the ACE may be forwarded and learned.

Deny: Frames matching the ACE are dropped.

Filter: Frames matching the ACE are filtered.

Rate Limiter : Indicates the rate limiter number of the ACE. The allowed range is 1 to 16. When Disabled is displayed, the rate limiter operation is disabled.

Port Redirect : Indicates the port redirect operation of the ACE. Frames matching the ACE are redirected to the port number. The allowed values are Disabled or a specific port number. When Disabled is displayed, the port redirect operation is disabled.

Mirror : Specify the mirror operation of this port. Frames matching the ACE are mirrored to the destination mirror port. The allowed values are:

Enabled: Frames received on the port are mirrored.

Disabled: Frames received on the port are not mirrored. The default value is "Disabled".

Logging: Specify the logging operation of this port. Notice that the logging message doesn't include the 4 bytes CRC. 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 (default).

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.

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

Modification Buttons : You can modify each ACE (Access Control Entry) in the table using the following buttons:

: Inserts a new ACE before the current row.

: Edits the ACE row.

: Moves the ACE up the list.

: Moves the ACE down the list.

: Deletes the ACE.

: The lowest plus sign adds a new entry at the bottom of the ACE listings.

ACE Configuration : An ACE consists of several parameters. These parameters vary according to the frame type that you select. First select the ingress port for the ACE, and then select the frame type. Different parameter options are displayed depending on the frame type selected. A frame that hits this ACE matches the configuration that is defined here.

Ingress Port : Select the ingress port for which this ACE applies.

All: The ACE applies to all port.

Port n: The ACE applies to this port number, where n is the number of the switch port.

Policy Filter : Specify the policy number filter for this ACE.

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

***Specific*:** If you want to filter a specific policy with this ACE, choose this value. Two field for entering an policy value and bitmask appears.

Policy Value : When "Specific" is selected for the policy filter, you can enter a specific policy value. The allowed range is 0 to 255.

Policy Bitmask : When "Specific" is selected for the policy filter, you can enter a specific policy bitmask. The allowed range is 0x0 to 0xff. Notice the usage of bitmask, if the binary bit value is "0", it means this bit is "don't-care". The real matched pattern is [policy_value & policy_bitmask]. For example, if the policy value is 3 and the policy bitmask is 0x10(bit 0 is "don't-care" bit), then policy 2 and 3 are applied to this rule.

Frame Type : Select the frame type for this ACE. These frame types are mutually exclusive.

Any: Any frame can match this ACE.

Ethernet Type: Only Ethernet Type frames can match this ACE. The IEEE 802.3 describes the value of Length/Type Field specifications to be greater than or equal to 1536 decimal (equal to 0600 hexadecimal).

ARP: Only ARP frames can match this ACE. Notice the ARP frames won't match the ACE with ethernet type.

IPv4: Only IPv4 frames can match this ACE. Notice the IPv4 frames won't match the ACE with ethernet type.

IPv6: Only IPv6 frames can match this ACE. Notice the IPv6 frames won't match the ACE with Ethernet type.

Action : Specify the action to take with a frame that hits this ACE.

Permit: The frame that hits this ACE is granted permission for the ACE operation.

Deny: The frame that hits this ACE is dropped.

Filter: Frames matching the ACE are filtered.

Rate Limiter : Specify the rate limiter in number of base units. The allowed range is 1 to 16. Disabled indicates that the rate limiter operation is disabled.

Port Redirect : Frames that hit the ACE are redirected to the port number specified here. The rate limiter will affect these ports. The allowed range is the same as the switch port number range. Disabled indicates that the port redirect operation is disabled and the specific port number of 'Port Redirect' can't be set when action is permitted.

Mirror : Specify the mirror operation of this port. Frames matching the ACE are mirrored to the destination mirror port. The rate limiter will not affect frames on the mirror port. The allowed values are:

Enabled: Frames received on the port are mirrored.

Disabled: Frames received on the port are not mirrored. The default value is "Disabled".

Logging : Specify the logging operation of the ACE. Notice that the logging message doesn't include the 4 bytes CRC information. The allowed values are:

Enabled: Frames matching the ACE are stored in the System Log.

Disabled: Frames matching the ACE are not logged.

Note: The logging feature only works when the packet length is less than 1518 (without VLAN tags) and the System Log memory size and logging rate is limited.

Shutdown : Specify the port shut down operation of the ACE. The allowed values are:

Enabled: If a frame matches the ACE, the ingress port will be disabled.

Disabled: Port shut down is disabled for the ACE.

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

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

MAC Parameters

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 displays.

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 displays.

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. Allowed 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 allowed range is 1 to 4095. A frame that hits this ACE matches this VLAN ID value.

Tag Priority : Specify the tag priority for this ACE. A frame that hits this ACE matches this tag priority. The allowed number range is 0 to 7 or range 0-1, 2-3, 4-5, 6-7, 0-3 and 4-7. The value Any means that no tag priority is specified (tag priority is "don't-care".)

ARP Parameters : The ARP parameters can be configured when Frame Type "ARP" is selected.

ARP/RARP : Specify the available ARP/RARP opcode (OP) flag for this ACE.

Any: No ARP/RARP OP flag is specified. (OP is "don't-care".)

ARP: Frame must have ARP opcode set to ARP.

RARP: Frame must have RARP opcode set to RARP.

Other: Frame has unknown ARP/RARP Opcode flag.

Request/Reply : Specify the available Request/Reply opcode (OP) flag for this ACE.

Any: No Request/Reply OP flag is specified. (OP is "don't-care".)

Request: Frame must have ARP Request or RARP Request OP flag set.

Reply: Frame must have ARP Reply or RARP Reply OP flag.

Sender IP Filter : Specify the sender IP filter for this ACE.

Any: No sender IP filter is specified. (Sender IP filter is "don't-care".)

Host: Sender IP filter is set to Host. Specify the sender IP address in the SIP Address field that appears.

Network: Sender IP filter is set to Network. Specify the sender IP address and sender IP mask in the SIP Address and SIP Mask fields that appear.

Sender IP Address : When "Host" or "Network" is selected for the sender IP filter, you can enter a specific sender IP address in dotted decimal notation.

Sender IP Mask : When "Network" is selected for the sender IP filter, you can enter a specific sender IP mask in dotted decimal notation.

Target IP Filter : Specify the target IP filter for this specific ACE.

Any: No target IP filter is specified. (Target IP filter is "don't-care".)

Host: Target IP filter is set to Host. Specify the target IP address in the Target IP Address field that appears.

Network: Target IP filter is set to Network. Specify the target IP address and target IP mask in the Target IP Address and Target IP Mask fields that appear.

Target IP Address : When "Host" or "Network" is selected for the target IP filter, you can enter a specific target IP address in dotted decimal notation.

Target IP Mask : When "Network" is selected for the target IP filter, you can enter a specific target IP mask in dotted decimal notation.

ARP Sender MAC Match : Specify whether frames can hit the action according to their sender hardware address field (SHA) settings.

0: ARP frames where SHA is not equal to the SMAC address.

1: ARP frames where SHA is equal to the SMAC address.

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

RARP Target MAC Match : Specify whether frames can hit the action according to their target hardware address field (THA) settings.

0: RARP frames where THA is not equal to the target MAC address.

1: RARP frames where THA is equal to the target MAC address.

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

IP/Ethernet Length : Specify whether frames can hit the action according to their ARP/RARP hardware address length (HLN) and protocol address length (PLN) settings.

0: ARP/RARP frames where the HLN is not equal to Ethernet (0x06) or the (PLN) is not equal to IPv4 (0x04).

1: ARP/RARP frames where the HLN is equal to Ethernet (0x06) and the (PLN) is equal to IPv4 (0x04).

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

Ethernet : Specify whether frames can hit the action according to their ARP/RARP hardware address space (HRD) settings.

0: ARP/RARP frames where the HLD is not equal to Ethernet (1).

1: ARP/RARP frames where the HLD is equal to Ethernet (1).

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

IP : Specify whether frames can hit the action according to their ARP/RARP protocol address space (PRO) settings.

0: ARP/RARP frames where the PRO is not equal to IP (0x800).

1: ARP/RARP frames where the PRO is equal to IP (0x800).

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

IP Parameters : The IP parameters can be configured when Frame Type "IPv4" is selected.

IP Protocol Filter : Specify the IP protocol filter for this ACE.

Any: No IP protocol filter is specified ("don't-care").

Specific: If you want to filter a specific IP protocol filter with this ACE, choose this value. A field for entering an IP protocol filter appears.

ICMP: Select ICMP to filter IPv4 ICMP protocol frames. Extra fields for defining ICMP parameters will appear. These fields are explained later in this section.

UDP: Select UDP to filter IPv4 UDP protocol frames. Extra fields for defining UDP parameters will appear. These fields are explained later in this section.

TCP: Select TCP to filter IPv4 TCP protocol frames. Extra fields for defining TCP parameters will appear. These fields are explained later in this section.

IP Protocol Value : When "Specific" is selected for the IP protocol value, you can enter a specific value. The allowed range is 0 to 255. A frame that hits this ACE matches this IP protocol value.

IP TTL : Specify the Time-to-Live settings for this ACE.

zero: IPv4 frames with a Time-to-Live field greater than zero must not be able to match this entry.

non-zero: IPv4 frames with a Time-to-Live field greater than zero must be able to match this entry.

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

IP Fragment : Specify the fragment offset settings for this ACE. This involves the settings for the More Fragments (MF) bit and the Fragment Offset (FRAG OFFSET) field for an IPv4 frame.

No: IPv4 frames where the MF bit is set or the FRAG OFFSET field is greater than zero must not be able to match this entry.

Yes: IPv4 frames where the MF bit is set or the FRAG OFFSET field is greater than zero must be able to match this entry.

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

IP Option : Specify the options flag setting for this ACE.

No: IPv4 frames where the options flag is set must not be able to match this entry.

Yes: IPv4 frames where the options flag is set must be able to match this entry.

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

SIP Filter : Specify the source IP filter for this ACE.

Any: No source IP filter is specified. (Source IP filter is "don't-care".)

Host: Source IP filter is set to Host. Specify the source IP address in the SIP Address field that appears.

Network: Source IP filter is set to Network. Specify the source IP address and source IP mask in the SIP Address and SIP Mask fields that appear.

SIP Address : When "Host" or "Network" is selected for the source IP filter, you can enter a specific SIP address in dotted decimal notation.

SIP Mask : When "Network" is selected for the source IP filter, you can enter a specific SIP mask in dotted decimal notation.

DIP Filter : Specify the destination IP filter for this ACE.

Any: No destination IP filter is specified. (Destination IP filter is "don't-care".)

Host: Destination IP filter is set to Host. Specify the destination IP address in the DIP Address field that appears.

Network: Destination IP filter is set to Network. Specify the destination IP address and destination IP mask in the DIP Address and DIP Mask fields that appear.

DIP Address : When "Host" or "Network" is selected for the destination IP filter, you can enter a specific DIP address in dotted decimal notation.

DIP Mask : When "Network" is selected for the destination IP filter, you can enter a specific DIP mask in dotted decimal notation.

IPv6 Parameters : The IPv6 parameters can be configured when Frame Type "IPv6" is selected.

Next Header Filter : Specify the IPv6 next header filter for this ACE.

Any: No IPv6 next header filter is specified ("don't-care").

Specific: If you want to filter a specific IPv6 next header filter with this ACE, choose this value. A field for entering an IPv6 next header filter appears.

ICMP: Select ICMP to filter IPv6 ICMP protocol frames. Extra fields for defining ICMP parameters will appear. These fields are explained later in this section.

UDP: Select UDP to filter IPv6 UDP protocol frames. Extra fields for defining UDP parameters will appear. These fields are explained later in this section.

TCP: Select TCP to filter IPv6 TCP protocol frames. Extra fields for defining TCP parameters will appear. These fields are explained later in this section.

Next Header Value : When "Specific" is selected for the IPv6 next header value, you can enter a specific value. The allowed range is 0 to 255. A frame that hits this ACE matches this IPv6 protocol value.

SIP Filter : Specify the source IPv6 filter for this ACE.

Any: No source IPv6 filter is specified. (Source IPv6 filter is "don't-care".)

Specific: Source IPv6 filter is set to Network. Specify the source IPv6 address and source IPv6 mask in the SIP Address fields that appear.

SIP Address : When "Specific" is selected for the source IPv6 filter, you can enter a specific SIPv6 address. The field only supported last 32 bits for IPv6 address.

SIP BitMask : When "Specific" is selected for the source IPv6 filter, you can enter a specific SIPv6 mask. The field only supported last 32 bits for IPv6 address. Notice the usage of bitmask, if the binary bit value is "0", it means this bit is "don't-care". The real matched pattern is [sipv6_address & sipv6_bitmask] (last 32 bits). For example, if the SIPv6 address is 2001::3 and the SIPv6 bitmask is 0xFFFFFFFE(bit 0 is "don't-care" bit), then SIPv6 address 2001::2 and 2001::3 are applied to this rule.

Hop Limit : Specify the hop limit settings for this ACE.

zero: IPv6 frames with a hop limit field greater than zero must not be able to match this entry.

non-zero: IPv6 frames with a hop limit field greater than zero must be able to match this entry.

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

ICMP Parameters

ICMP Type Filter : Specify the ICMP filter for this ACE.

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

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

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

ICMP Code Filter : Specify the ICMP code filter for this ACE.

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

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

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

TCP/UDP Parameters

TCP/UDP Source Filter : Specify the TCP/UDP source filter for this ACE.

Any: No TCP/UDP source filter is specified (TCP/UDP source filter status is "don't-care").

Specific: If you want to filter a specific TCP/UDP source filter with this ACE, you can enter a specific TCP/UDP source value. A field for entering a TCP/UDP source value displays.

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 displays.

TCP/UDP Source No. : When "Specific" is selected for the TCP/UDP source filter, you can enter a specific TCP/UDP source value. The allowed range is 0 to 65535. A frame that hits this ACE matches this TCP/UDP source value.

TCP/UDP Source Range : When "Range" is selected for the TCP/UDP source filter, you can enter a specific TCP/UDP source range value. The allowed range is 0 to 65535. A frame that hits this ACE matches this TCP/UDP source value.

TCP/UDP Destination Filter : Specify the TCP/UDP destination filter for this ACE.

Any: No TCP/UDP destination filter is specified (TCP/UDP destination filter status is "don't-care").

Specific: If you want to filter a specific TCP/UDP destination filter with this ACE, you can enter a specific TCP/UDP destination value. A field for entering a TCP/UDP destination value displays.

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 displays.

TCP/UDP Destination Number : When "Specific" is selected for the TCP/UDP destination filter, you can enter a specific TCP/UDP destination value. The allowed range is 0 to 65535. A frame that hits this ACE matches this TCP/UDP destination value.

TCP/UDP Destination Range : When "Range" is selected for the TCP/UDP destination filter, you can enter a specific TCP/UDP destination range value. The allowed range is 0 to 65535. A frame that hits this ACE matches this TCP/UDP destination value.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Ethernet Type Parameters : The Ethernet Type parameters can be configured when Frame Type "Ethernet Type" is selected.

EtherType Filter : Specify the Ethernet type filter for this ACE.

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

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

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

Buttons

Apply : Click to save changes.

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

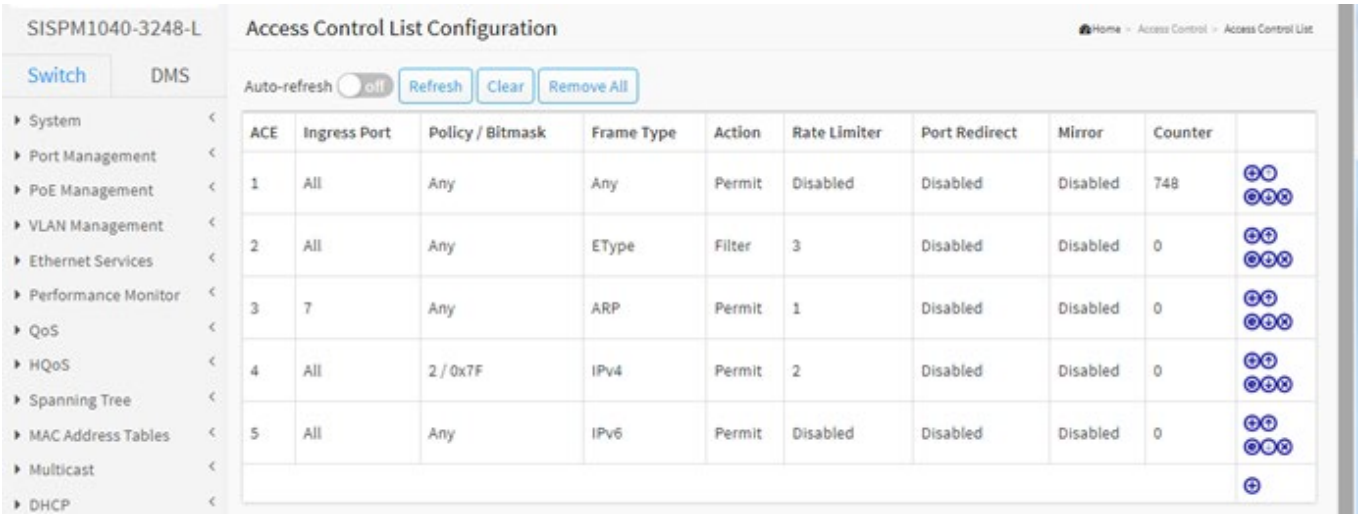
Refresh: Click to refresh the page; any changes made locally will be undone.

Clear: Click to clear the counters.

Messages:

The parameter of 'VLAN ID' and 'Tag Priority' can't be set when 802.1Q Tagged is disabled

Example:

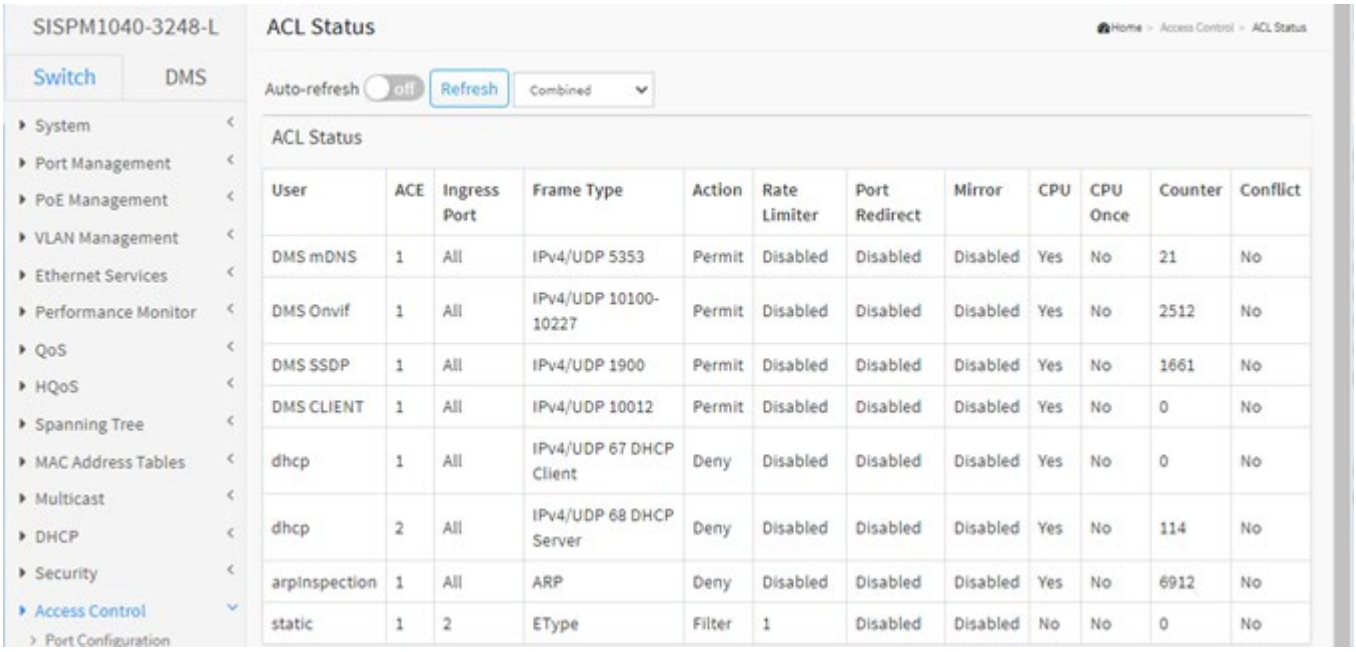


16-4 ACL Status

This webpage displays the ACL status by different ACL users. Each row describes the ACE that is defined. It is a conflict if a specific ACE is not applied to the hardware due to hardware limitations. The maximum number of ACEs is 512 per switch.

To display ACL status in the web UI:

1. Click Access Control and ACL status.
2. Use the User select box to select the ACL user to be displayed.
3. To automatically refresh the page every 3 seconds click “Auto-refresh”.
4. Click “Refresh” to immediately refresh the ACL Status.



User	ACE	Ingress Port	Frame Type	Action	Rate Limiter	Port Redirect	Mirror	CPU	CPU Once	Counter	Conflict
DMS mDNS	1	All	IPv4/UDP 5353	Permit	Disabled	Disabled	Disabled	Yes	No	21	No
DMS Onvif	1	All	IPv4/UDP 10100-10227	Permit	Disabled	Disabled	Disabled	Yes	No	2512	No
DMS SSDP	1	All	IPv4/UDP 1900	Permit	Disabled	Disabled	Disabled	Yes	No	1661	No
DMS CLIENT	1	All	IPv4/UDP 10012	Permit	Disabled	Disabled	Disabled	Yes	No	0	No
dhcp	1	All	IPv4/UDP 67 DHCP Client	Deny	Disabled	Disabled	Disabled	Yes	No	0	No
dhcp	2	All	IPv4/UDP 68 DHCP Server	Deny	Disabled	Disabled	Disabled	Yes	No	114	No
arpInspection	1	All	ARP	Deny	Disabled	Disabled	Disabled	Yes	No	6912	No
static	1	2	EType	Filter	1	Disabled	Disabled	No	No	0	No

Figure 16-4: ACL Status

Parameter descriptions:

User : Indicates the ACL user for the row (e.g., dhcp).

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 ports.

Port: The ACE will match a specific ingress port.

Frame Type : Indicates the frame type of the ACE. Possible values are:

Any: The ACE will match any frame type.

EType: The ACE will match Ethernet Type frames. Note that an Ethernet Type based ACE will not get matched by IP and ARP frames.

ARP: The ACE will match ARP/RARP frames.

IPv4: The ACE will match all IPv4 frames.

IPv4: The ACE will match all IPv4 frames.

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

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

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

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

IPv6: The ACE will match all IPv6 standard frames.

Action : Indicates the forwarding action of the ACE.

Permit: Frames matching the ACE may be forwarded and learned.

Deny: Frames matching the ACE are dropped.

Filter: Frames matching the ACE are filtered.

Rate Limiter : Indicates the rate limiter number of the ACE. The allowed range is 1 to 16. When Disabled is displayed, the rate limiter operation is disabled.

Port Redirect : Indicates the port redirect operation of the ACE. Frames matching the ACE are redirected to the port number. The allowed values are Disabled or a specific port number. When Disabled is displayed, the port redirect operation is disabled.

Mirror : Specify the mirror operation of this port. The allowed values are:

Enabled: Frames received on the port are mirrored.

Disabled: Frames received on the port are not mirrored. The default value is "Disabled".

CPU : Forward packet that matches the specific ACE to CPU.

CPU Once : Forward first packet that matches the specific ACE to CPU.

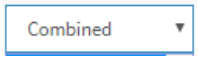
Counter : The counter indicates the number of times the ACE was hit by a frame.

Conflict : Indicates the hardware status of the specific ACE. The specific ACE is not applied to the hardware due to hardware limitations.

Buttons

Auto-refresh : Click to refresh the page automatically every 3 seconds.

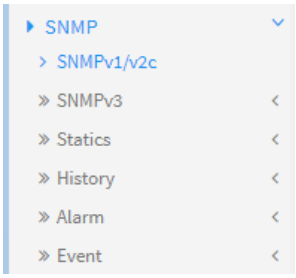
Refresh : Click to manually refresh the page immediately.



: **User select box** : The select box lets you select which ACL user is displayed.

User selections include: Combined, static, ipSourceGuard, IP, ipmc, ttLoopLp, evc, mep, arpinspection, upnp, ptp, dhcp, loopProtect, y1564, linkOam, DMS CLIENT, DMS Server, DMS SSDP, DMS Onvif, DMSmDNS, ttLoopHp, Rapid Ring, MRP, and conflict.

Chapter 17 - SNMP



Any Network Management System (NMS) running the Simple Network Management Protocol (SNMP) can manage the managed devices equipped with SNMP agent, provided that the Management Information Base (MIB) is installed correctly on the managed devices. The SNMP is a protocol that is used to govern the transfer of information between SNMP manager and agent and traverses the Object Identifier (OID) of the management Information Base (MIB), described in the form of SMI syntax.
The 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 field SNMP “Enable”, SNMP agent will be started up. All supported MIB OIDs, including RMON MIB, can be accessed via SNMP manager. If the field SNMP is set “Disable”, SNMP agent will be de-activated, the related Community Name, Trap Host IP Address, Trap and all MIB counters will be ignored.

17-1 SNMPv1/v2c Configuration

This page lets you configure SNMP V1 and V2 parameters. To configure SNMP v1/v2c parameters in the web UI:

1. Click SNMP and SNMPv1/v2c.
2. Enable or disable the SNMP Mode.
3. Specify the Read Community and Write Community.
4. Click Apply.

Figure 17-1: SNMP v1/v2c Configuration

Parameter descriptions:

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

on: Enable SNMP mode operation.

off: Disable SNMP mode operation.

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

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

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

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

Buttons

Apply : Click to save changes.

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

17-2 SNMPv3

17-2.1 Communities

Configure SNMPv3 community parameters on this page. The entry index key is Community. To configure the 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.

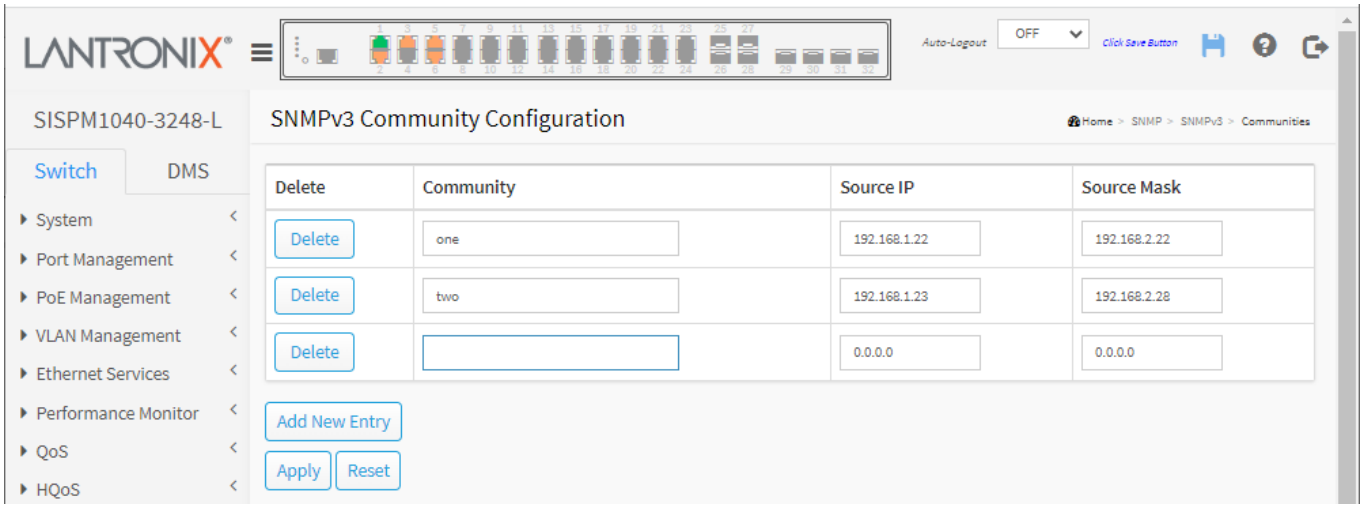


Figure 17-2.1: SNMPv3 Communities Configuration

Parameter descriptions:

Community : Enter the security name to map the community to the SNMP Groups configuration. The allowed string length is 1 – 32 characters, and the allowed content is ASCII characters 33 - 126.

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

Source Mask : Enter the SNMP access source address network mask.

Buttons

Add New Entry : Click to add new entry. Specify the name and configure the new entry.

Delete : Check to delete the entry. It will be deleted immediately.

Apply : Click to save changes.

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

17-2.2 Users

This function is used to configure SNMPv3 user. The Entry index key is UserName. The max number of SNMPv3 Users 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 parameter.
4. Click Apply.

Figure 17-2.2: SNMPv3 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 equal system engine ID then it is local user; otherwise it's remote user.

User Name : A string identifying the user name that this entry should belong to. 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 – 32 characters. For SHA authentication protocol, the allowed string length is 8 - 32 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 - 32 characters, and the allowed content is ASCII characters 33 - 126.

Buttons

Add New Entry : Click to add new entry. Specify the name and configure the new entry. Click "Apply".

Delete : Check to delete the entry. It will be deleted immediately.

Apply : Click to save changes.

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

Messages

The length of 'MD5 Authentication Password' is restricted to 8 – 32

17-2.3 Groups

This page lets you configure SNMPv3 group. The Entry index key are Security Model and Security Name.
To create a new group account, click the Add New Group button, enter the group information, and then click Apply. The max number of Groups 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.

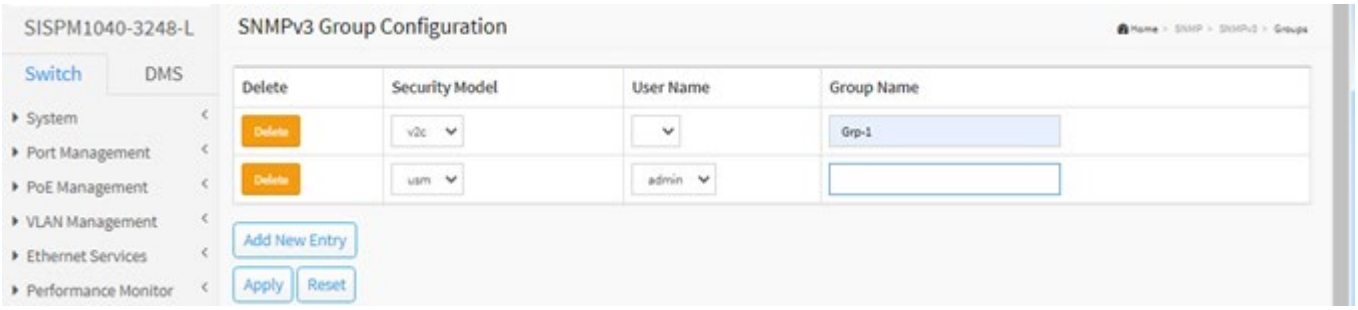


Figure 17-2.3: SNMPv3 Groups Configuration

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).

User Name : At the dropdown select an existing Group Name.

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 new entry. Specify the name and configure the new entry.

Delete : Check to delete the entry. It will be deleted immediately.

Apply : Click to save changes.

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

Messages:

No available User Name, please add community or user first.

SNMPv3 has invalid IP address or prefix length

17-2.4 Views

This function is used to configure SNMPv3 view. The Entry index keys are OID Subtree and View Name.
To create a new View account, click the Add New Entry button, enter the view information, and then click Apply. The maximum number of Groups is 12. The entry index keys are View Name and OID Subtree.

To configure SNMPv3 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.

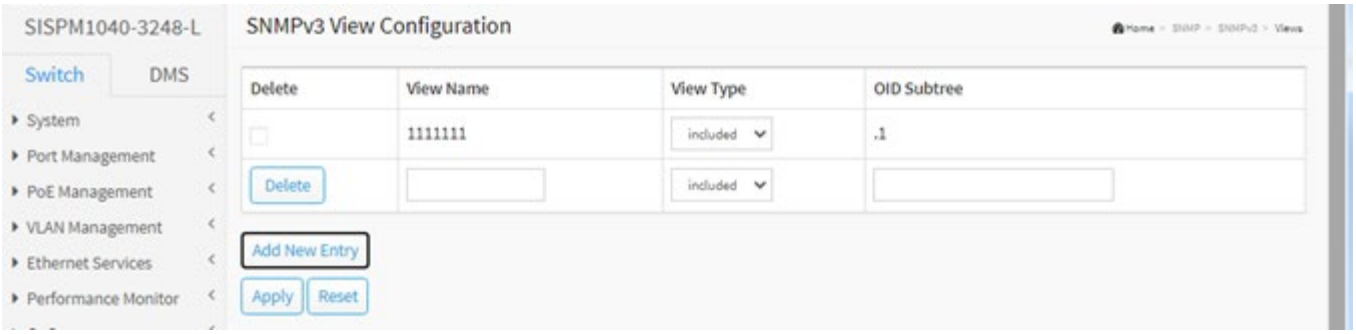


Figure 17-2.4: SNMPv3 View Configuration

Parameter descriptions:

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

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

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

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

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

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

Buttons

Add New Entry: Click to add new entry. Specify the name and configure the new entry.

Delete: Check to delete the entry. It will be deleted immediately.

Apply: Click to save changes.

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

17-2.5 Access

This page lets you configure SNMPv3 access. The Entry index key are Group Name, Security Model and Security level. To create a new access account, click the Add New Entry button, enter the access information and then click Apply. You can configure up to 12 Groups. To configure SNMPv3 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.

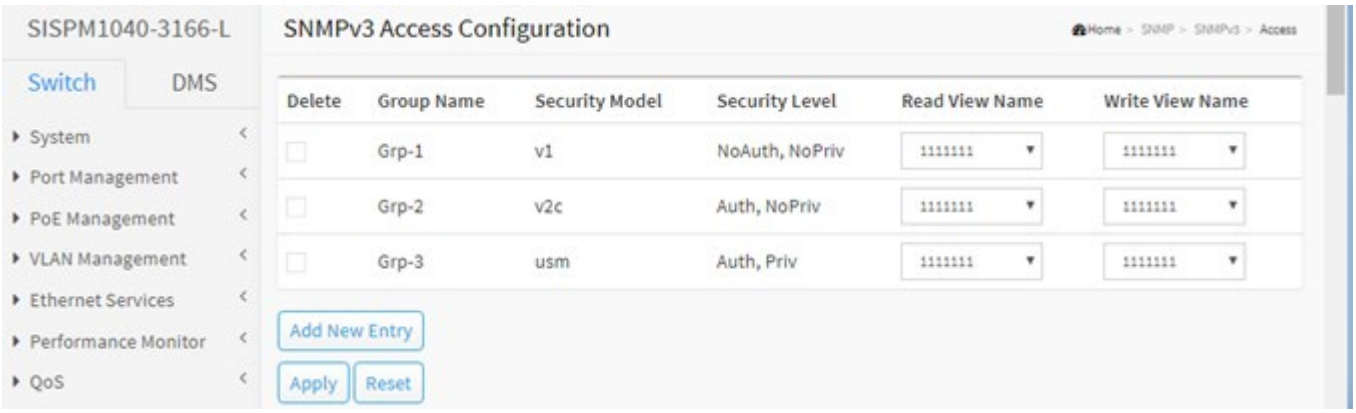


Figure 17-2.5: SNMPv3 Accesses Configuration

Parameter descriptions:

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

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

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

v1: Reserved for SNMPv1.

v2c: Reserved for SNMPv2c.

usm: User-based Security Model (USM).

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

NoAuth, NoPriv: No authentication and no privacy.

Auth, NoPriv: Authentication and no privacy.

Auth, Priv: Authentication and privacy.

Read View Name : The name of the MIB view defining the MIB objects for which this request may request the current values. The allowed string length is 1 – 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 new entry. Specify the name and configure the new entry. Click "Apply".

Delete : Check to delete the entry. It will be deleted immediately.

Apply : Click to save changes.

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

Message: *No available group name, please add group first.*

17-3 RMON Statistics

17-3.1 Configuration

Configure RMON Statistics on this page. The entry index key is ID. To configure RMON Statistics in the web UI:

1. Click SNMP > Statics > Configuration.
2. Click Add New Entry.
3. Specify the ID and Data Source parameters.
4. Click Apply.

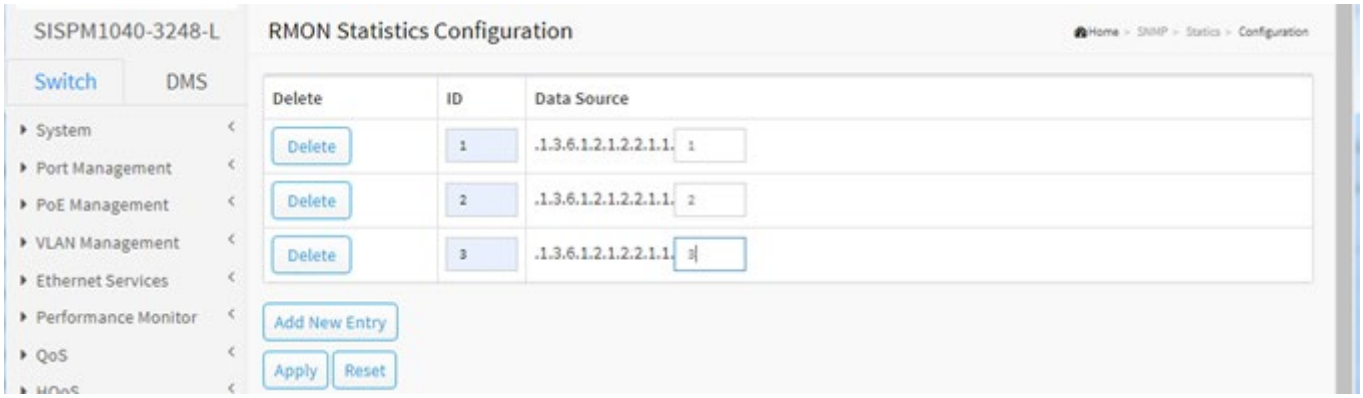


Figure 17-3.1: RMON Statistics Configuration

Parameter descriptions:

ID : Indicates the index of the entry. The range is 1 - 65535.

Data Source : Indicates the port ID which wants to be monitored.

Buttons

Delete : Check to delete the entry. It will be deleted immediately.

Add New Entry : Click to add a new entry.

Apply : Click to save changes.

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

17-3.2 Status

This page provides a summary of RMON Statistics entries. Each page shows up to 99 entries from the Statistics table, default being 20, selected through the "entries per page" input field. When first visited, the web page will show the first 20 entries from the beginning of the Statistics table. The first displayed will be the one with the lowest ID found in the Statistics table.

The "Start from Control Index" allows the user to select the starting point in the Statistics table. Clicking the Refresh button will update the displayed table starting from that or the next closest Statistics table match.

The Next Entry will use the last entry of the currently displayed entry as a basis for the next lookup. When the end is reached the text "*No more entries*" is shown in the displayed table. Use the First Entry button to start over.

To display the RMON Statistics Status Overview webpage:

1. Click Security, RMON, Statistics and Status.
2. Specify Start from Control Index and entries per page.
3. Check “Auto-refresh”.
4. Click “Refresh” to refresh the port detailed statistics.

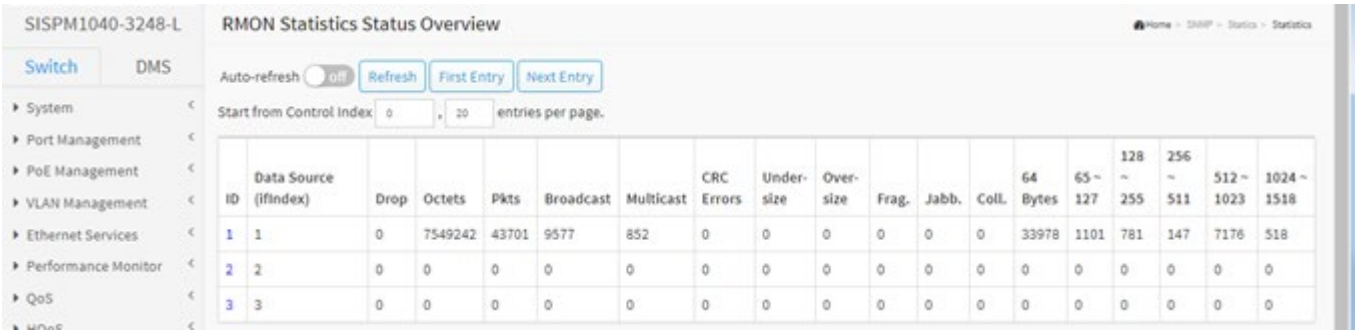


Figure 17-3.2: RMON Statistics Status Overview

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 65 to 127 octets in length.

128~255 : The total number of packets (including bad packets) received that were 128 to 255 octets in length.

256~511 : The total number of packets (including bad packets) received that were 256 to 511 octets in length.

512~1023 : The total number of packets (including bad packets) received that were 512 to 1023 octets in length.

1024~1588 : The total number of packets (including bad packets) received that were 1024 to 1588 octets in length.

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

Show entries : You can choose how many items you want displayed.

Buttons

Auto-refresh : Click to refresh the page automatically every 3 seconds.

Refresh : Click to manually refresh the page immediately.

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

Previous : Updates the system log entries, turn to the previous page.

17-4 RMON History

17-4.1 Configuration

Configure RMON History table on this page. The entry index key is ID. To configure the RMON History parameters in the web UI:

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

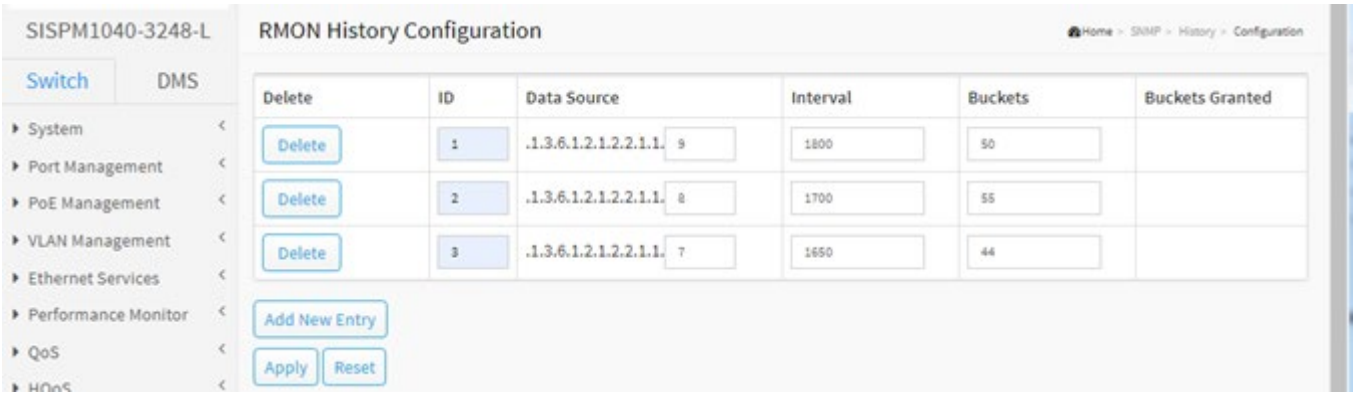


Figure 17-4.1: RMON History Configuration

Parameter descriptions:

ID : Indicates the index of the entry. The range is 1 - 65535.

Data Source : Indicates the port ID which wants to be monitored.

Interval : Indicates the interval in seconds for sampling the history statistics data. The range is 1 – 3600; the default is 1800 seconds.

Buckets : Indicates the maximum data entries associated this History control entry stored in RMON. The range is 1 – 3600; the default is 50 buckets.

Buckets Granted : The number of data to be saved in the RMON.

Buttons

Delete : Check to delete the entry. It will be deleted immediately.

Add New Entry : Click to add a new entry.

Apply : Click to save changes.

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

17-4.2 Status

This page provides an overview of RMON History entries. Each page shows up to 99 entries from the History table, default being 20, selected through the "entries per page" input field. When first visited, the web page will show the first 20 entries from the beginning of the History table. The first displayed will be the one with the lowest History Index and Sample Index found in the History table.

The "Start from History Index and Sample Index" 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.

To display RMON History Status in the web UI:

1. Click SNMP, History, and Status.
2. Click the Auto-refresh button.
3. Click “Refresh” to refresh the port detailed statistics.
4. Click First Entry/Next Entry to change the Entries listed.

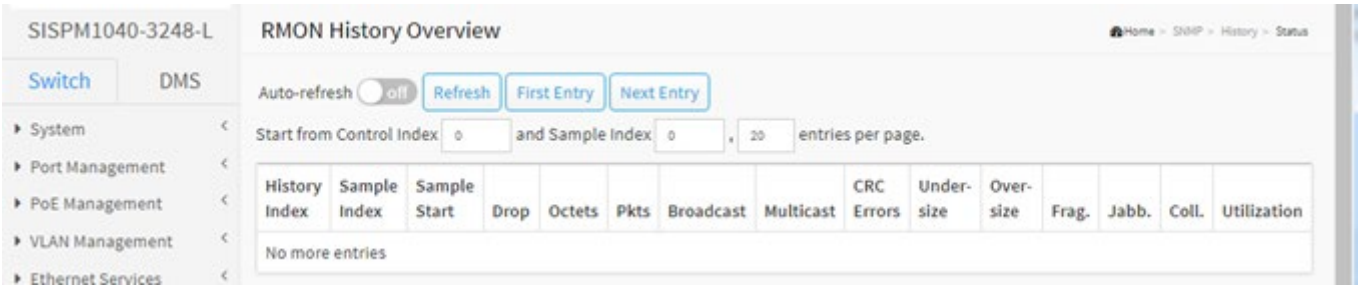


Figure 17-4.2: RMON History Status

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.

S**how entries** : You can choose how many items you want to show.

Buttons

Auto-refresh : Click to refresh the page automatically every 3 seconds.

Refresh : Click to manually refresh the page immediately.

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

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

17-5 RMON Alarm

17-5.1 Configuration

Configure RMON Alarm table on this page. The entry index key is ID.

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

Figure 17-5.1: RMON Alarm Configuration

Parameter descriptions:

ID : Indicates the index of the entry. The valid range is 1 - 65535.

Interval : Indicates the interval in seconds for sampling and comparing the rising and falling threshold. The range is 1 to 2^31-1.

Variable : Indicates the particular variable to be sampled, the possible variables are:

InOctets: The total number of octets received on the interface, including framing characters.

InUcastPkts: The number of uni-cast packets delivered to a higher-layer protocol.

InNUcastPkts: The number of broad-cast and multi-cast packets delivered to a higher-layer protocol.

InDiscards: The number of inbound packets that are discarded even the packets are normal.

InErrors: The number of inbound packets that contained errors preventing them from being deliverable to a higher-layer protocol.

InUnknownProtos: the number of the inbound packets that were discarded because of an unknown or un-support protocol.

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

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

OutNUcastPkts: The number of broad-cast and multi-cast packets that request to transmit.

OutDiscards: The number of outbound packets that are discarded event the packets is normal.

OutErrors: The 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 immediately.

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.

Messages:

invalid 'datasource', invalid llag

Variable value is xxx.yyy, xxx is 10-21, yyy is 1-65535

'Rising threshold' must be larger than 'Falling threshold'

17-5.2 Status

This page provides an overview of RMON Alarm entries. Each page shows up to 99 entries from the Alarm table, default being 20, selected through the "entries per page" input field. When first visited, the web page will show the first 20 entries from the beginning of the Alarm table. The first displayed will be the one with the lowest ID found in the Alarm table.

The "Start from Control Index" allows the user to select the starting point in the Alarm table. Clicking the Refresh button will update the displayed table starting from that or the next closest Alarm table match.

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

To display RMON Alarm Status in the web UI:

1. Click SNMP, Alarm, and Status.
2. Click “Auto-refresh” or click “Refresh” to refresh the port detailed statistics.
3. Click First Entry/Next Entry to change the Entry.

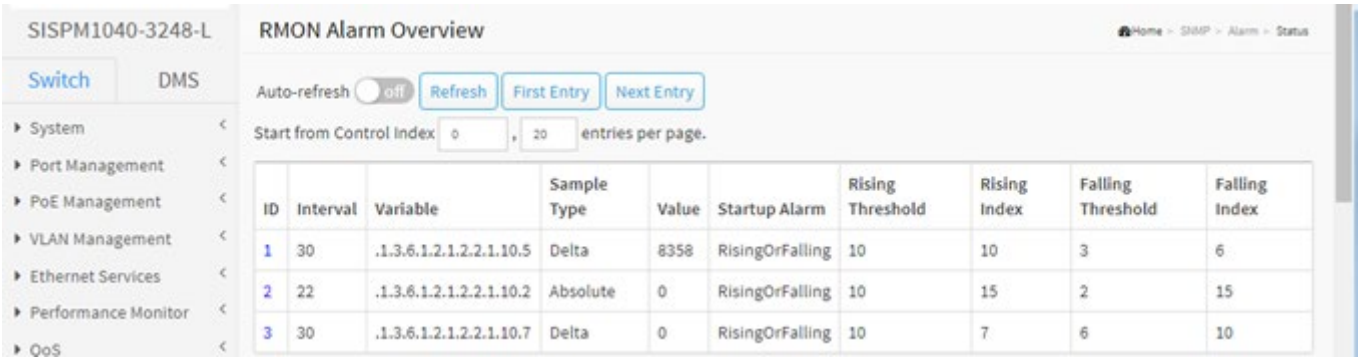


Figure 17-5.2: RMON Alarm Overview

Parameter descriptions:

ID : Indicates the index of Alarm control entry. Click a linked ID to display its specific information.

Interval : Indicates the interval in seconds for sampling and comparing the rising and falling threshold.

Variable : Indicates the particular variable to be sampled.

Sample Type : The method of sampling the selected variable and calculating the value to be compared against the thresholds.

Value : The value of the statistic during the last sampling period.

Startup Alarm : The alarm that may be sent when this entry is first set to valid.

Rising Threshold : Rising threshold value.

Rising Index : Rising event index.

Falling Threshold : Falling threshold value.

Falling Index : Falling event index.

Show entries : Choose how many items you want to be displayed.

Buttons

Auto-refresh : Click to refresh the page automatically every 3 seconds.

Refresh : Click to manually refresh the page immediately.

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

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

17-6 RMON Event

17-6.1 Configuration

Configure RMON Events 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.

Figure 17-6.1: RMON Event Configuration

Parameter descriptions:

ID : Indicates the index of the entry. The range is from 1 to 65535.

Desc : Indicates this event, the allowed string length is 0 - 127; the default is a null string.

Type : Indicates the notification of the event, the possible types are:

None: No SNMP log is created; no SNMP trap is sent.

Log: Create SNMP log entry when the event is triggered.

Snmp trap: Send SNMP trap when the event is triggered.

Log and trap: Create SNMP log entry and sent SNMP trap when the event is triggered.

Event Last Time : Indicates the value of sysUpTime at the time this event entry last generated an event.

Buttons

Delete : Check to delete the entry. It will be deleted immediately.

Add New Entry : Click to add a new entry.

Apply : Click to save changes.

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

17-6.2 Status

This page provides an overview of RMON Event table entries. Each page shows up to 99 entries from the Event table, default being 20, selected through the "entries per page" input field. When first visited, the web page will show the first 20 entries from the beginning of the Event table. The first displayed will be the one with the lowest Event Index and Log Index found in the Event table.

The "Start from Event Index and Log Index" allows the user to select the starting point in the Event table. Clicking the Refresh button will update the displayed table starting from that or the next closest Event table match.

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

To display a RMON Event Status in the web UI:

1. Click SNMP, Event, and Status.
2. Check “Auto-refresh”.
3. Click “ Refresh“ to refresh the port detailed statistics.
4. Click First Entry/Next Entry to change Entry.

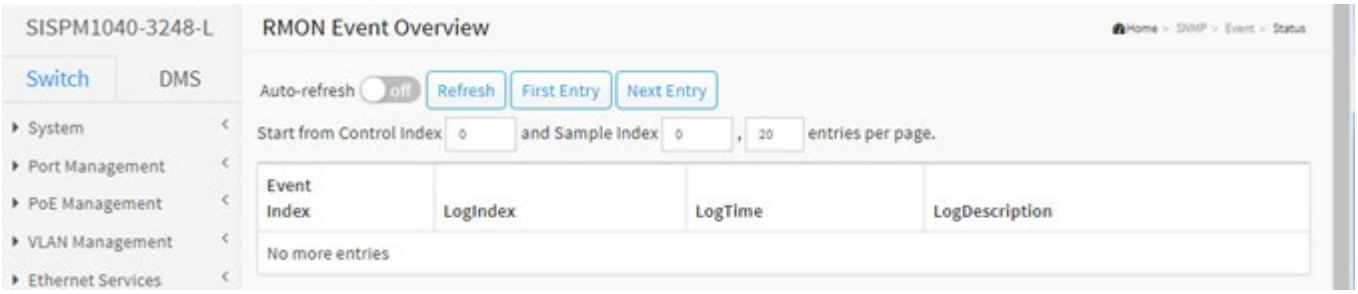


Figure 17-6.2: RMON Event Status

Parameter descriptions:

Event Index : Indicates the index of the event entry.

Log Index : Indicates the index of the log entry.

LogTIme : Indicates Event log time

LogDescription : Indicates the Event description.

Show entries : You can choose how many items you want to show.

Buttons

Auto-refresh : Click to refresh the page automatically every 3 seconds.

Refresh : Click to manually refresh the page immediately.

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

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

Chapter 18 - MEP

18-1 MEP Configuration

Maintenance Entity Point instances are configured here. A MEP (Maintenance Entity Endpoint) is an endpoint in a Maintenance Entity Group (ITU-T Y.1731). To configure the MEP parameters in the web UI:

1. Click MEP > MEP Configuration.
2. Click the “Add New MEP” button. Only one MEP can be added for each apply operation.
3. Specify the Maintenance Entity Point parameters.
4. Click Apply to save the changes.

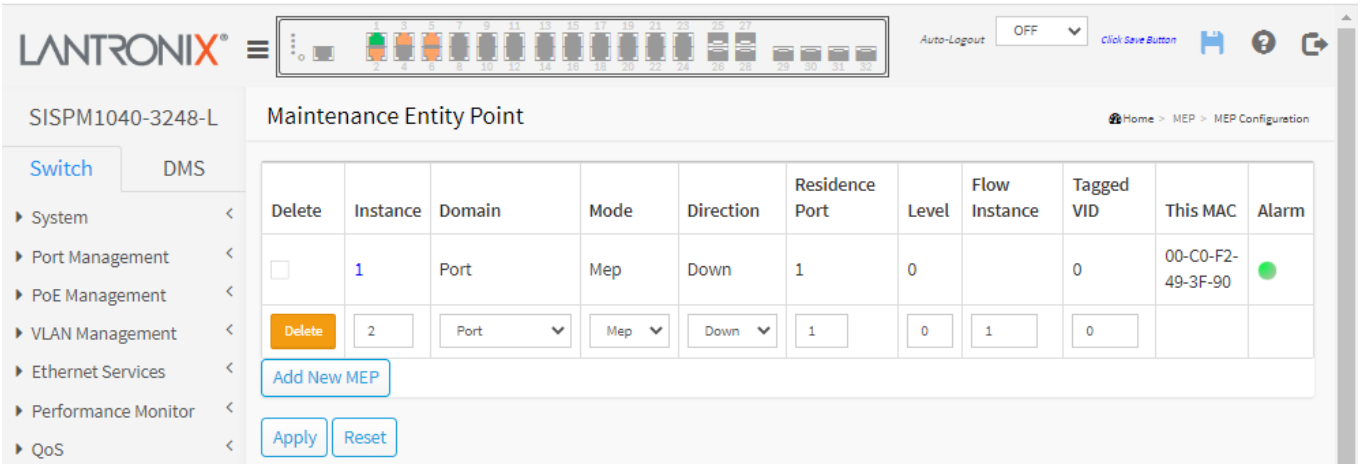


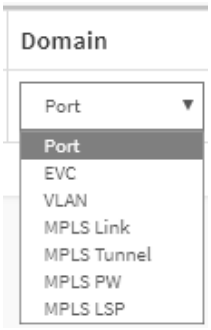
Figure 15-1: Maintenance Entity Point

Parameter descriptions:

Delete : This box is used to delete a MEP immediately.

Instance : The ID of the MEP. Click on the ID of a MEP to enter the configuration page. The range is 1 - 3124.

Domain : Select the domain for this instance:



Port: This is a MEP in the Port Domain.

EVC: This is a MEP in the EVC Domain. 'Flow Instance' is an EVC. The EVC must be created

VLAN: This is a MEP in the VLAN Domain. 'Flow Instance' is a VLAN. In case of Up-MEP the VLAN must be created

MPLS Link: This is a MEP in the MPLS Link Domain.

MPLS Tunnel: This is a MEP in the MPLS Tunnel Domain.

MPLS PW: This is a MEP in the MPLS Pseudo Wires Domain.

MPLS LSP: This is a MEP in the MPLS LSP Domain.

Mode : Select MEP or MIP:

MEP: This is a Maintenance Entity End Point.

MIP: This is a Maintenance Entity Intermediate Point.

Direction : Select Up or Down:

Down: This is a Down MEP - monitoring ingress OAM and traffic on 'Residence Port'.

Up: This is an Up MEP - monitoring egress OAM and traffic on 'Residence Port'.

Residence Port : The port where MEP is monitoring - see 'Direction'. For a EVC MEP the port must be a port in the EVC. For a VLAN MEP the port must be a VLAN member.

Level : The MEG level of this MEP.

Flow Instance : The MEP is related to this flow - See 'Domain'. This is not relevant and not shown in case of Port MEP.

Tagged VID :

Port MEP: An outer C/S-tag (depending on VLAN Port Type) is added with this VID. Entering '0' means no TAG added.

EVC MEP: This is not used.

VLAN MEP: This is not used.

EVC MIP: On Serval, this is the Subscriber VID that identifies the subscriber flow in this EVC where the MIP is active.

This MAC : The MAC of this MEP - can be used by other MEP when unicast is selected (Info only).

Alarm : ● There is an active alarm on the MEP or operational state is not "Up". Otherwise ● displays.

Buttons

Add New MEP : Click to add a new MEP entry. Only one MEP can be added for each apply operation.

Apply : Click to save changes.

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

Messages

Only one MEP can be added for each apply operation

The residence port is not valid in this domain or for this MEP type

MPLS-TP: Invalid MPLS-TP link interface number

MEP direction must be 'Down' while 'MPLS Tunnel' domain

MPLS-TP: Invalid MPLS-TP tunnel endpoint number

MPLS-TP: Invalid MPLS-TP PW number

MEP mode must be 'Mip' while 'MPLS LSP' domain

MPLS-TP: Invalid MPLS-TP LSP cross-connect number

This MIP is not supported

The MEPs operational state is not up

MAX number of Down-MEPs is exceeded in this flow

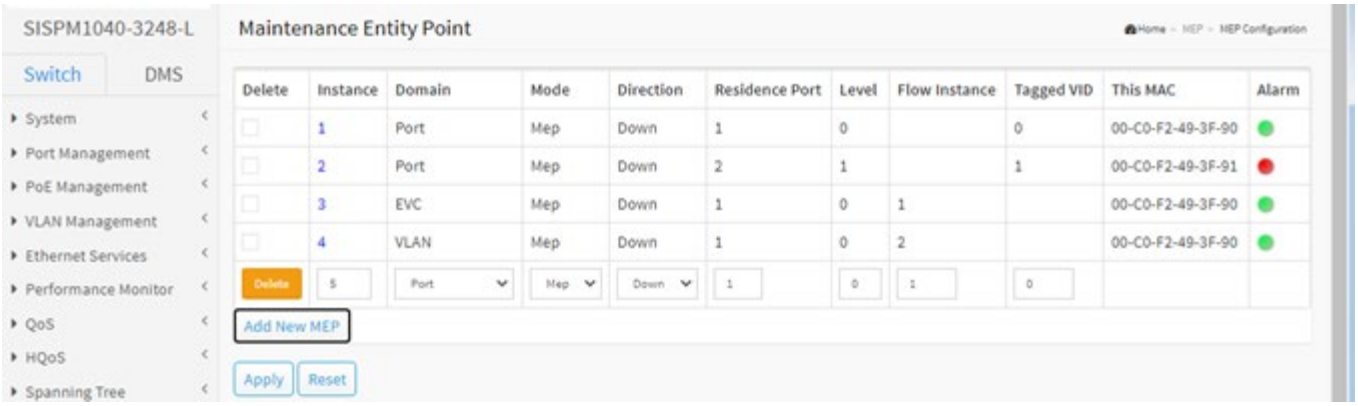
UP MEP/MIP is not supported in this domain

This MIP is not supported

Could not set aps config for instance 4

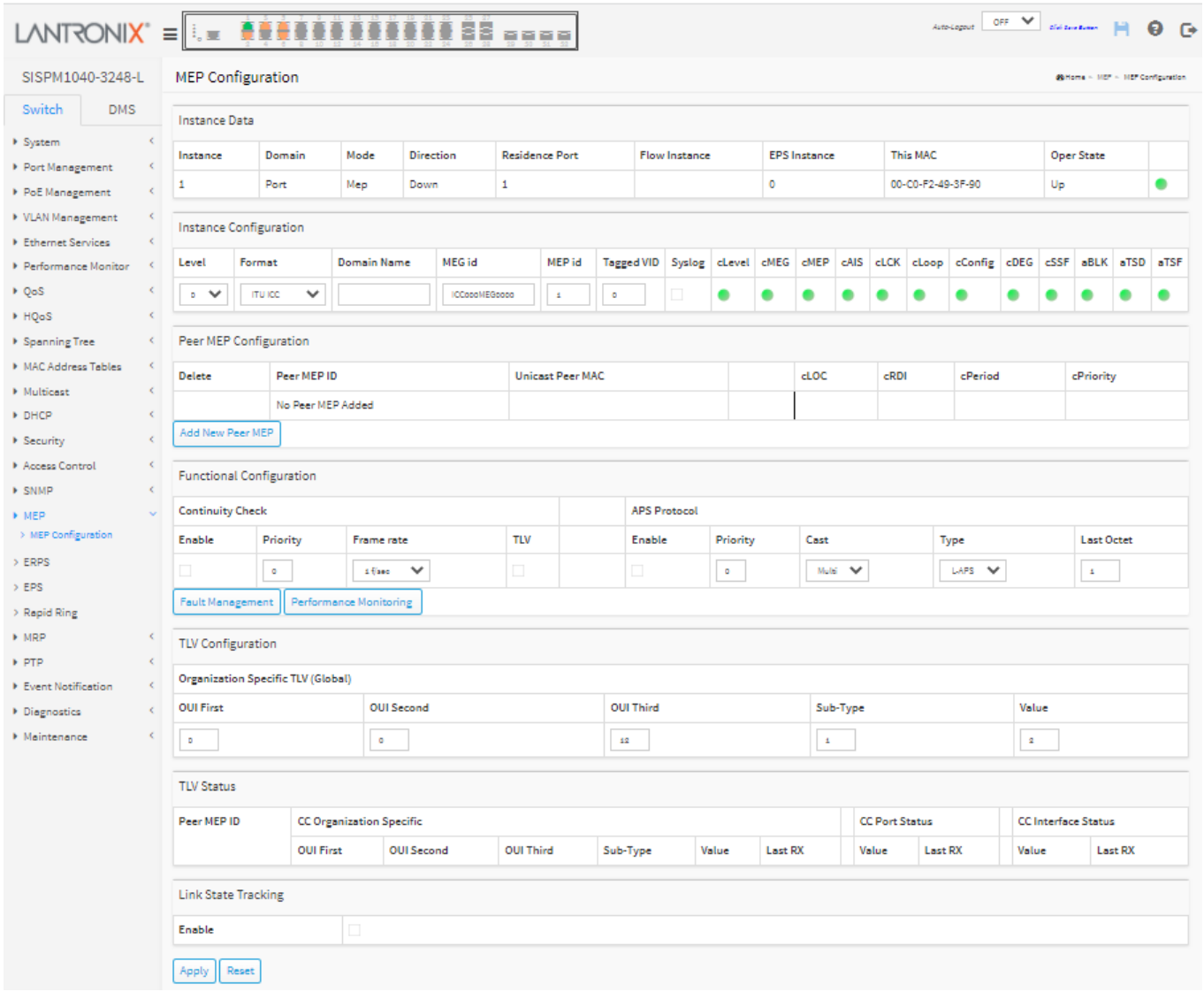
Internal Server Error 500 : Click the browser Back button and continue operation.

Example:



18-2 MEP Configuration Page

Click on the ID of a MEP to display the MEP Configuration page. This page lets you view and configure the current MEP Instance.



Parameter descriptions

Instance Data

Instance : The ID of the MEP. Click on the ID of a MEP to enter the configuration page. The range is 1 - 3124.

Domain : Select ***Port*** or ***VLAN***.

Port: This is a MEP in the Port Domain.

VLAN: This is a MEP in the VLAN Domain. 'Flow Instance' is a VLAN. In case of an Up-MEP, the VLAN must already have been created.

Mode : Select MEP or MIP:

MEP: This is a Maintenance Entity End Point.

MIP: This is a Maintenance Entity Intermediate Point.

Direction : Select Up or Down:

Down: This is a Down MEP - monitoring ingress OAM and traffic on 'Residence Port'.

Up: This is a Up MEP - monitoring egress OAM and traffic on 'Residence Port'.

Residence Port : The port where MEP is monitoring - see 'Direction'. For a EVC MEP the port must be a port in the EVC. For a VLAN MEP the port must be a VLAN member.

Level : The MEG level of this MEP.

Flow Instance : The MEP is related to this flow - See 'Domain' above. This is not relevant and not shown in case of Port MEP.

Tagged VID :

Port MEP: An outer C/S-tag (depending on VLAN Port Type) is added with this VID. Entering '0' means no TAG added.

EVC MEP: This is not used.

VLAN MEP: This is not used.

EVC MIP: On Serval, this is the Subscriber VID that identify the subscriber flow in this EVC where the MIP is active.

This MAC : The MAC of this MEP - can be used by other MEP when unicast is selected (Info only).

Oper State : Operational State that can have one of these values:

Up: The instance is UP meaning it is physically configured and operational.

Down: The instance is DOWN meaning it is NOT physically configured and operational.

Config: The instance is DOWN due to invalid configuration.

HW: The instance is DOWN due to failing OAM supporting HW resources.

MCE: The instance is DOWN due to failing MCE resources.

Instance Configuration

Level : The MEG level of this MEP.

Format : This is the configuration of the two possible Maintenance Association Identifier formats.

ITU ICC: This is defined by ITU (Y1731 Fig. A3). 'Domain Name' is not used. 'MEG id' must be max. 13 char.

IEEE String: This is defined by IEEE (802.1ag Section 21.6.5). 'Domain Name' can be max. 16 char. 'MEG id' (Short MA Name) can be max. 16 char.

ITU CC ICC: This is defined by ITU (Y1731 Fig. A5). 'Domain Name' is not used. 'MEG id' must be max. 15 char.

Domain Name : This is the IEEE Maintenance Domain Name and is only used in case of 'IEEE String' format. This string can be empty giving Maintenance Domain Name Format 1 - Not present. This can be max 16 char.

MEG Id : This is either ITU MEG ID or IEEE Short MA Name - depending on 'Format'. See 'Format'. In case of ITU ICC format this must be 13 char. In case of ITU CC ICC format this must be 15 char. In case of IEEE String format this can be a maximum of 16 character.

MEP Id : This value will become the transmitted two byte CCM MEP ID.

Tagged VID : This value will be the VID of a TAG added to the OAM PDU.

Syslog : If enabled, notifications are logged to Syslog.

cLevel : Fault Cause indicating that a CCM is received with a lower level than the configured for this MEP.

cMEG : Fault Cause indicating that a CCM is received with a MEG ID different from configured for this MEP.

cMEP : Fault Cause indicating that a CCM is received with a MEP ID different from all 'Peer MEP ID' configured for this MEP.

cAIS : Fault Cause indicating that AIS PDU is received.

cLCK : Fault Cause indicating that LCK PDU is received.

cLoop : Fault Cause indicating that a loop is detected, since CCM is received with own MEP ID and SMAC.

cConfig : Fault Cause indicating that a configuration error is detected, since CCM is received with own MEP ID.

cDEG : Fault Cause indicating that server layer is indicating Signal Degraded.

cSSF : Fault Cause indicating that server layer is indicating Signal Fail.

aBLK : The consequent action of blocking service frames in this flow is active.

aTSD : The consequent action of indicating Trail Signal Degrade is calculated.

aTSF : The consequent action of indicating Trail Signal Fail to-wards protection is active.

Peer MEP Configuration

Delete : This box is used to mark a Peer MEP for deletion in next Save operation.

Peer MEP ID : This value will become an expected MEP ID in a received CCM - see 'cMEP'.

Unicast Peer MAC : This MAC will be used when unicast is selected with this peer MEP. Also this MAC is used to create HW checking of receiving CCM PDU (LOC detection) from this MEP.

cLOC : Fault Cause indicating that no CCM has been received (in 3,5 periods) - from this peer MEP.

cRDI : Fault Cause indicating that a CCM is received with Remote Defect Indication - from this peer MEP.

cPeriod : Fault Cause indicating that a CCM is received with a period different what is configured for this MEP - from this peer MEP.

cPriority : Fault Cause indicating that a CCM is received with a priority different what is configured for this MEP - from this peer MEP.

Buttons

Add New Peer MEP : Click to add a new peer MEP.

Functional Configuration

Continuity Check : Enable Continuity Check based on transmitting/receiving CCM PDU can be enabled/disabled. The CCM PDU is always transmitted as Multi-cast Class 1.
Priority : The priority to be inserted as PCP bits in TAG (if any). In case of enable of Continuity Check and Loss Measurement both implemented on SW based CCM, 'Priority' has to be the same.
Frame rate : Selecting the frame rate of CCM PDU. This is the inverse of transmission period as described in Y.1731. This value has these uses:

- The transmission rate of the CCM PDU.
- Fault Cause cLOC is declared if no CCM PDU has been received within 3.5 periods - see 'cLOC'.
- Fault Cause cPeriod is declared if a CCM PDU has been received with different period - see 'cPeriod'.

Selecting 300f/sec or 100f/sec will configure HW based CCM (if possible). Selecting other frame rates will configure SW based CCM. In case of enable of Continuity Check and Loss Measurement both implemented on SW based CCM, 'Frame Rate' has to be the same.

TLV : Enable/disable of TLV insertion in the CCM PDU.

APS Protocol : Enable Automatic Protection Switching protocol information transportation based on transmitting/receiving R-APS/L-APS PDU can be enabled/disabled. Must be enabled to support ERPS/ELPS implementing APS. This is only valid with one Peer MEP configured.

Priority : The priority to be inserted as PCP bits in TAG (if any).

Cast : Selection of APS PDU transmitted unicast or multi-cast. The unicast MAC will be taken from the 'Unicast Peer MAC' configuration. Unicast is only valid for L-APS - see 'Type'. The R-APS PDU is always transmitted with multi-cast MAC described in G.8032.

Type : R-APS: APS PDU is transmitted as R-APS - this is for ERPS.

L-APS: APS PDU is transmitted as L-APS - this is for ELPS.

Last Octet : This is the last octet of the transmitted and expected RAPS multi-cast MAC. In G.8031 (03/2010) a RAPS multi-cast MAC is defined as 01-19-A7-00-00-XX. In current standard the value for this last octet is '01' and the usage of other values is for further study.

TLV Configuration : Configuration of the OAM PDU TLV. Currently only TLV in the CCM is supported.

Organization Specific - OUI First : The transmitted first value in the OS TLV OUI field.

Organization Specific - OUI Second : The transmitted second value in the OS TLV OUI field.

Organization Specific - OUI Third : The transmitted third value in the OS TLV OUI field.

Organization Specific - Sub-Type : The transmitted value in the OS TLV Sub-Type field.

Organization Specific – Value : The transmitted value in the OS TLV Value field.

TLV Status : Display of the last received TLV. Currently only TLV in the CCM is supported.

CC Organization Specific - OUI First : The last received first value in the OUI field.

CC Organization Specific - OUI Second : The last received second value in the OS TLV OUI field.

CC Organization Specific - OUI Third : The last received third value in the OS TLV OUI field.

CC Organization Specific - Sub-Type : The last received value in the OS TLV Sub-Type field.

CC Organization Specific – Value : The last received value in the OS TLV Value field.

CC Organization Specific - Last RX : OS TLV was received in the last received CCM PDU.

CC Port Status – Value : The last received value in the PS TLV Value field.

CC Port Status - Last RX : PS TLV was received in the last received CCM PDU.

CC Interface Status – Value : The last received value in the IS TLV Value field.

CC Interface Status - Last RX : IS TLV was received in the last received CCM PDU.

Link State Tracking

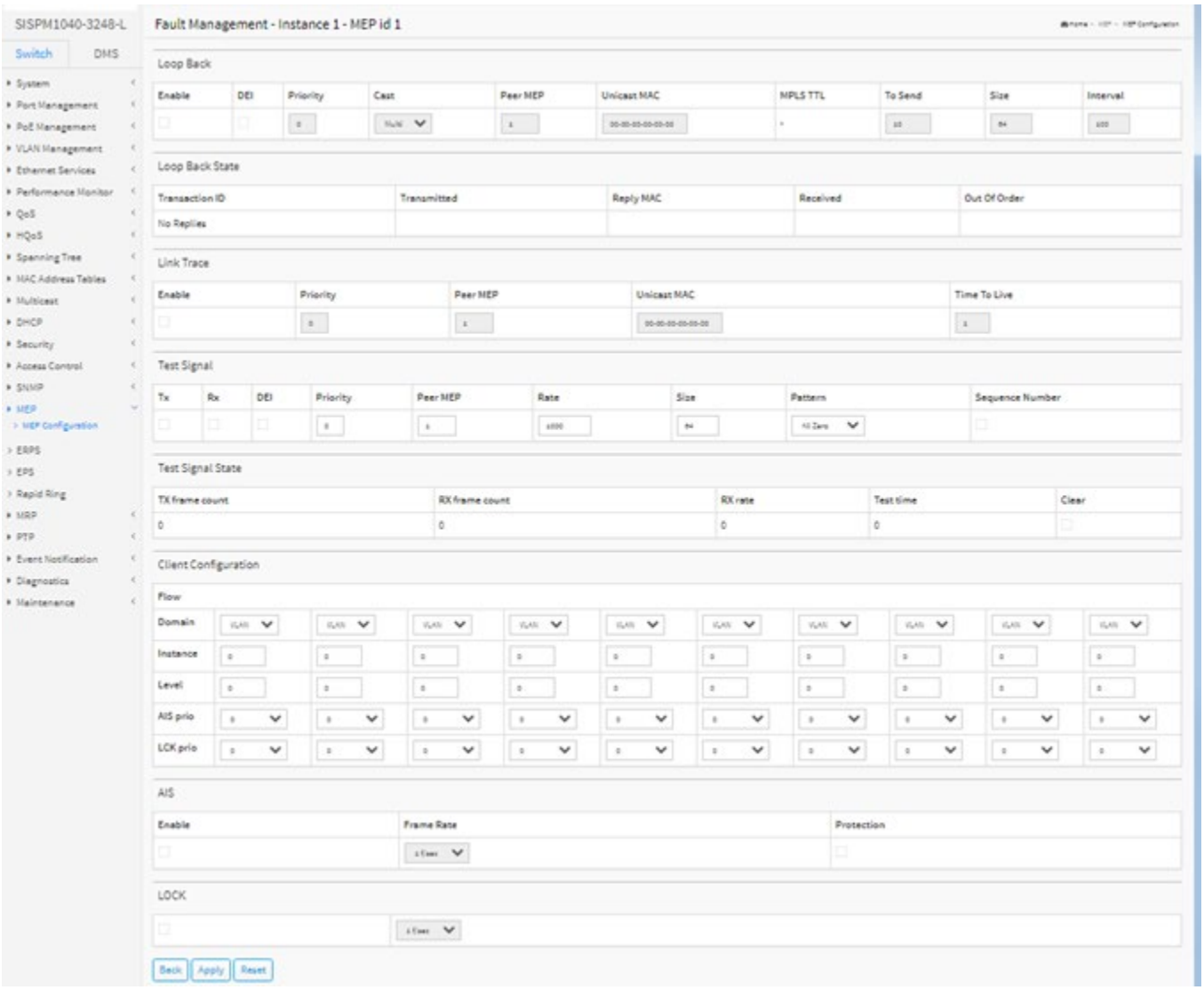
Enable : When LST is enabled in an instance, Local SF or received 'isDown' in CCM Interface Status TLV, will bring down the residence port. Only valid in Up-MEP. The CCM rate must be 1 f/s or faster.

Buttons

Fault Management : Click to go to Fault Management page (see below).
Performance Monitor: Click to go to Performance Monitor page (see below).
Apply : Click to save changes.
Reset: Click to undo any changes made locally and revert to previously saved values.

18-2.1 Fault Management

This page lets you view and configure the Fault Management of the current MEP Instance.



Parameter descriptions:

Loop Back

Enable : Loop Back based on transmitting/receiving LBM/LBR PDU can be enabled/disabled. Loop Back is automatically disabled when all 'To Send' LBM PDU has been transmitted - waiting 5 seconds for all LBR from the end.

DEI : The DEI to be inserted as PCP bits in TAG (if any).

Priority : The priority to be inserted as PCP bits in TAG (if any).

Cast : Selection of LBM PDU transmitted unicast or multi-cast. The unicast MAC will be configured through 'Peer MEP' or 'Unicast Peer MAC'. To-wards MIP only unicast Loop Back is possible.

Peer MEP : This is only used if the 'Unicast MAC' is configured to all zero. The LBM unicast MAC will be taken from the 'Unicast Peer MAC' configuration of this peer.

Unicast MAC : This is only used if NOT configured to all zero. This will be used as the LBM PDU unicast MAC. This is the only way to configure Loop Back to-wards a MIP.

To Send : The number of LBM PDU to send in one loop test. The value 0 indicate infinite transmission (test behavior). This is HW based LBM/LBR and Requires VOE.

Size : The LBM frame size. This is entered as the wanted size (in bytes) of a un-tagged frame containing LBM OAM PDU - including CRC (four bytes). Example when 'Size' = 64=> Un-tagged frame size = DMAC(6) + SMAC(6) + TYPE(2) + LBM PDU LENGTH(46) + CRC(4) = 64 bytes. The transmitted frame will be four bytes longer for each tag added - 8 bytes in case of a tunnel EVC. There are two frame MAX sizes to consider.

Switch RX frame MAX size: The MAX frame size (all inclusive) accepted on the switch port of 10240 Bytes
CPU RX frame MAX size: The MAX frame size (all inclusive) possible to copy to CPU of 10240 Bytes

Consider that the Peer MEP must be able to handle the selected frame size. Consider that In case of SW based MEP, the received LBR PDU must be copied to CPU. A Warning will be given if selected frame size exceeds the CPU RX frame MAX size. Frame MIN Size is 64 Bytes.

Interval : The interval between transmitting LBM PDU. In 10ms. in case 'To Send' != 0 (max 100 - '0' is as fast as possible) In 1µs increments. in case 'To Send' == 0 (max 10.000)",

Loop Back State

Transaction ID : The transaction id of the first LBM transmitted. For each LBM transmitted the transaction id in the PDU is incremented.
Transmitted : The total number of LBM PDU transmitted.
Reply MAC : The MAC of the replying MEP/MIP. In case of multi-cast LBM, replies can be received from all peer MEP in the group. This MAC is not shown in case of 'To Send' == 0.
Received : The total number of LBR PDU received from this 'Reply MAC'.
Out Of Order : The number of LBR PDU received from this 'Reply MAC' with incorrect 'Transaction ID'.

Link Trace

Enable : Link Trace based on transmitting/receiving LTM/LTR PDU can be enabled/disabled. Link Trace is automatically disabled when all 5 transactions are done with 5 sec. interval - waiting 5 sec. for all LTR in the end. The LTM PDU is always transmitted as Multi-cast Class 2.
Priority : The priority to be inserted as PCP bits in TAG (if any).
Peer MEP : This is only used if the 'Unicast MAC' is configured to all zero. The Link Trace Target MAC will be taken from the 'Unicast Peer MAC' configuration of this peer.
Unicast MAC : This is only used if NOT configured to all zero. This will be used as the Link Trace Target MAC. This is the only way to configure a MIP as Target MAC.
Time To Live : This is the LTM PDU TTL value as described in Y.1731. This value is decremented each time forwarded by a MIP. Will not be forwarded reaching zero.

Link Trace State

Transaction ID : The transaction id is incremented for each LTM send. This value is inserted the transmitted LTM PDU and is expected to be received in the LTR PDU. Received LTR with wrong transaction id is ignored. There are five transactions in one Link Trace activated.

Time To Live : This is the TTL value taken from the LTM received by the MIP/MEP sending this LTR - decremented as if forwarded.
Mode : Indicating if was a MEP/MIP sending this LTR.
Direction : Indicating if MEP/MIP sending this LTR is ingress/egress.

Forwarded : Indicating if MEP/MIP sending this LTR has forwarded the LTM.

Relay : The Relay action can be one of the following

MAC: The was a hit on the LT Target MAC
FDB: LTM is forwarded based on hit in the Filtering DB
MFDB: LTM is forwarded based on hit in the MIP CCM DB

Last MAC : The MAC identifying the last sender of the LBM causing this LTR - initiating MEP or previous MIP forwarding.

Next MAC : The MAC identifying the next sender of the LBM causing this LTR - MIP forwarding or terminating MEP.

Test Signal :

Enable : Test Signal based on transmitting TST PDU can be enabled/disabled.

DEI : The DEI to be inserted as PCP bits in TAG (if any).

Priority : The priority to be inserted as PCP bits in TAG (if any).

Peer MEP : The TST frame destination MAC will be taken from the 'Unicast Peer MAC' configuration of this peer.

Rate : The TST frame transmission bit rate - in Kilobits pr. second. Limit in 10 Gbps. This is the bit rate of a standard frame without any encapsulation. If 1 Mbps rate is selected in a EVC MEP, the added tag will give a higher bitrate on the wire.

Size : The TST frame size. This is entered as the wanted size (in bytes) of a un-tagged frame containing TST OAM PDU - including CRC (four bytes). Example when 'Size' = 64=> Un-tagged frame size = DMAC(6) + SMAC(6) + TYPE(2) + TST PDU LENGTH(46) + CRC(4) = 64 bytes. The transmitted frame will be four bytes longer for each tag added - 8 bytes in case of a tunnel EVC. There are two frame MAX sizes to consider.

Switch RX frame MAX size: The MAX frame size (all inclusive) accepted on the switch port of 10240 Bytes
CPU RX frame MAX size: The MAX frame size (all inclusive) possible to copy to CPU of 10240 Bytes

Consider that the Peer MEP must be able to handle the selected frame size. Consider that in order to calculate the 'RX rate' a received TST PDU must be copied to CPU. A Warning is given if selected frame size exceeds the CPU RX frame MAX size. Frame MIN Size is 64 Bytes.

Pattern : The 'empty' TST PDU has the size of 12 bytes. In order to achieve the configured frame size a data TLV will be added with a pattern. Example: when 'Size' = 64=> Un-tagged frame size = DMAC(6) + SMAC(6) + TYPE(2) + TST PDU LENGTH(46) + CRC(4) = 64 bytes. The TST PDU must be 46 bytes so a pattern of 46-12=34 bytes is added.

All Zero: Pattern will be '00000000'
All One: Pattern will be '11111111'
10101010: Pattern will be '10101010'

Sequence Number : When checked, looped Y.1731 TST/LBR frames are tested for out-of-order upon reception.

Test Signal State

TX frame count : The number of transmitted TST frames since last 'Clear'.

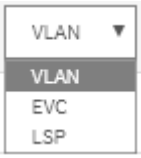
RX frame count : The number of received TST frames since last 'Clear'.

RX rate : The current received TST frame bit rate in Kbps. This is calculated on a 1 s. basis, starting when first TST frame is received after 'Clear'. The frame size used for this calculation is the first received after 'Clear'

Test time : The number of seconds passed since first TST frame received after last 'Clear'.

Clear : This will clear all Test Signal State. Transmission of TST frame will be restarted. Calculation of 'Rx frame count', 'RX rate' and 'Test time' will be started when receiving first TST frame.

Client Configuration : Only a Port MEP is able to be a server MEP with flow configuration. The Priority in the client flow is always the highest priority configured in the EVC.



Domain : The domain of the client layer flow (e.g., VLAN, EVC, LSP).

Instance : Client layer flow instance numbers.

Level : Client layer level - AIS and LCK PDU transmitted in this client layer flow will be on this level.

AIS Prio : The priority to be used when transmitting AIS in each client flow. Priority resulting in highest possible PCP can be selected.

LCK Prio : The priority to be used when transmitting LCK in each client flow. Priority resulting in highest possible PCP can be selected.

AIS

Enable : Insertion of AIS signal (AIS PDU transmission) in client layer flows, can be enable/disabled.

Frame Rate : Selecting the frame rate of AIS PDU. This is the inverse of transmission period as described in Y.1731.

Protection : Selecting this means that the first 3 AIS PDU is transmitted as fast as possible - in case of using this for protection in the end point.

LOCK

Enable : Insertion of LOCK signal (LCK PDU transmission) in client layer flows, can be enable/disabled.

Frame Rate : Displays the frame rate of LCK PDU. This is the inverse of transmission period as described in Y.1731.

Buttons

Back : Click to go back to this MEP instance main page.

Apply : Click to save changes.

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

Messages

The MEPs operational state is not up

Invalid MEP instance ID

Need to disable AIS and LOCK too when client configuration is disabled

Invalid parameter error returned from MEP

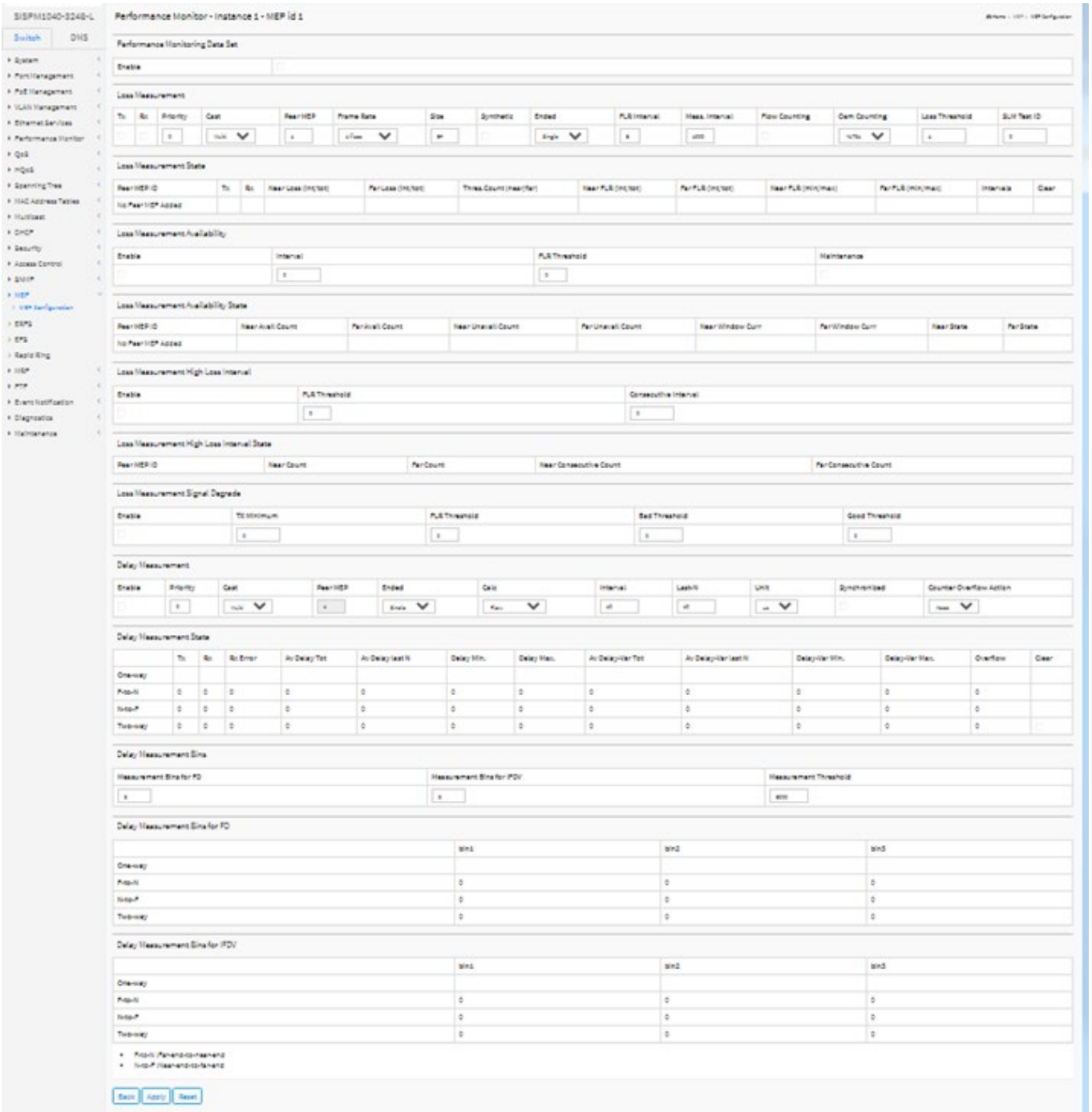
MAX number of Down-MEPs is exceeded in this flow

The VID is invalid or VLAN is not created for this VID or attribut 'VID' is illegal in this domain

Invalid peer MEP ID

18-2.2 Performance Monitoring

This page lets you view and configure the performance monitor of the current MEP Instance.



Parameter descriptions:

Performance Monitoring Data Set

Enable : When enabled this MEP instance will contribute to the 'PM Data Set' gathered by the PM Session.

Loss Measurement

Tx : Loss Measurement initiator is enabled/disabled. Initiator is transmitting/receiving CCM or LMM/LMR or SLM/SLR/1SL PDUs - see 'Synthetic' and 'Ended'. Service frame LM (not 'Synthetic') is only allowed with one Peer MEP configured. Synthetic frame LM is allowed with multiple Peer MEPs configured.

Rx : Enable loss calculation when receiving dual-ended LM PDUs (CCM-LM/1SL). This should be used in conjunction with a dual-ended remote initiator sending either CCM-LM or 1SL PDUs to this MEP instance. This setting is ignored when the LM single-ended initiator is enabled on the same MEP instance, as this initiator is fully capable of calculating both near-to-far and far-to-near loss calculation. This setting should only be used if the initiator is not enabled or for a TX dual-ended initiator (which does not receive anything back).

Priority : The priority to be inserted as PCP bits in TAG (if any). In case of enable of Continuity Check and Loss Measurement both implemented on SW based CCM, 'Priority' has to be the same.

Cast : Selection of LM PDU transmitted unicast or multicast. The unicast MAC will be taken from the 'Unicast Peer MAC' configuration. In case of enable of Continuity Check and dual ended Loss Measurement both implemented on SW based CCM, 'Cast' has to be the same.

Peer MEP : Peer MEP-ID for unicast LM. The MAC is taken from the 'Unicast Peer MAC' database. Only used in case of multiple peers ('Synthetic' LM).

Frame Rate : This parameter selects the frame rate for the LM PDUs. This is the inverse of the transmission period as described in Y.1731. Selecting 6f/min is not valid in case of dual ended 'Service frame' LM (CCM PDU based). In case of enable of Continuity Check and Loss Measurement both implemented on SW based CCM, 'Frame Rate' has to be the same.

Size : The 'Synthetic' SLM/1SL frame size. This is entered as the wanted size (in bytes) of a un-tagged frame containing LM OAM PDU - including CRC (four bytes). Example when 'Size' = 64=> Un-tagged frame size = DMAC(6) + SMAC(6) + TYPE(2) + LBM PDU LENGTH(46) + CRC(4) = 64 bytes. The transmitted frame will be four bytes longer for each tag added - 8 bytes in case of a tunnel EVC. There are two frame MAX sizes to consider.

Switch RX frame MAX size: The MAX frame size (all inclusive) accepted on the switch port of Bytes.

CPU RX frame MAX size: The MAX frame size (all inclusive) possible to copy to CPU of Bytes.

Consider that the Peer MEP must be able to handle the selected frame size. Consider that the received SLR PDU must be copied to CPU. A Warning is given if selected frame size exceeds the CPU RX frame MAX size. Frame MIN Size is 64 Bytes.

Synthetic : Synthetic frame LM is enabled. This is SLM/SLR/1SL PDU based LM.

Ended : Single: Single ended Loss Measurement implemented on LMM/LMR or SLM/SLR.

Dual: Dual ended Loss Measurement implemented on SW based CCM or 1SL.

FLR Interval : This is the interval in number of measurement intervals where the interval Frame Loss Ratio is calculated.

Meas Interval : This is the 'synthetic' LM measurement interval in milliseconds. This must be a whole number of the LM PDU transmission interval (inverse 'Rate'). This is the interval in time where the loss and FLR is calculated based on the counted number of SL OAM PDUs. It is in this interval that the calculated FLR is checked against availability, high loss and degraded FLR threshold. For example: 'Rate' = 10f/sec => 'Meas Interval' = N*100 milliseconds. In case of service frame based LM this attribute is not used and the measurement interval is always the LM PDU transmission interval.

Loss Threshold : Far end loss threshold count is incremented if a loss measurement is above this threshold.

SLM Test ID : The Test ID value to use in SLM PDUs (see G.8013, section 9.22.1). The default value is 0.

Loss Measurement State

Peer MEP : The Peer MEP ID that the following state relates to.

Tx : The accumulated transmitted LM PDUs - since last 'clear'.

Rx : The accumulated received LM PDUs - since last 'clear'.

Near Loss : This field contains both the number of measurement intervals that has contributed to the near end frame loss and the total near end frame loss count - since last 'clear'.

Far Loss : This field contains both the number of measurement intervals that has contributed to the far end frame loss and the total far end frame loss count - since last 'clear'.

Thres.Count (near/far) : The number of times the near end and far end frame loss thresholds has been crossed.

Near FLR (int/tot) : The interval and total near end frame loss ratio calculated based on the near end frame loss count and far end frame transmitted. The result is given in 100 * percent.

Far FLR (int/tot) : The interval and total far end frame loss ratio calculated based on the far end frame loss count and near end frame transmitted. The result is given in 100 * percent.

Near FLR (min/max) : The minimum and maximum non-zero near end frame loss ratio calculated based on the near end frame loss count and far end frame transmitted. The result is given in 100 * percent. A value of zero means that no loss has been encountered since last clear.

Far FLR (min/max) : The minimum and maximum non-zero far end frame loss ratio calculated based on the far end frame loss count and near end frame transmitted. The result is given in 100 * percent. A value of zero means that no loss has been encountered since last clear.

Intervals : The number of FLR expired intervals.

Clear : Set of this check and save will clear the accumulated counters and restart ratio calculation.

Loss Measurement Availability

Enable : Enable/disable of loss measurement availability.

Interval : Availability interval - number of measurements with same availability in order to change availability state. The valid range is 1 to 1000.

FLR Threshold : Availability frame loss ratio threshold in per mille (per thousand).

Maintenance : Enable/disable of loss measurement availability maintenance.

Loss Measurement Availability State

Peer MEP : The Peer MEP ID that the following state relates to.

Near Avail Count : The number of measurements performed while the near end has been in the "Avail" state.

Far Avail Count : The number of measurements performed while the far end has been in the "Avail" state.

Near Unavail Count : The number of measurements performed while the near end has been in the "Unavail" state.

Far Unavail Count : The number of measurements performed while the far end has been in the "Unavail" state.

Near Window Curr : The current near-end availability window size. When Near State is "Avail" this value indicate the current number of consecutive measurements that are above the defined frame loss ratio threshold.
When Near State is "Unavail" this value indicate the current number of consecutive measurements that are equal to or below the defined frame loss ratio threshold. Once this value reaches the defined "Interval" value (aka. the "window size") the availability state will change.

Far Window Curr : The current far-end availability window size. See the description for Near Window Curr for more details.

Near State : The current near end availability state.

Far State : The current far end availability state.

Loss Measurement High Loss Interval

Enable : Enable/disable of loss measurement high loss interval.

FLR Threshold : High Loss Interval frame loss ratio threshold in per mille (per thousand).

Consecutive Interval : High Loss Interval consecutive interval (number of measurements).

Loss Measurement High Loss Interval Status

Near Count : Near end high loss interval count (number of measurements where availability state is available and FLR is above high loss interval FLR threshold.

Far Count : Far end high loss interval count (number of measurements where availability state is available and FLR is above high loss interval FLR threshold.

Near Consecutive Count : Near end high loss interval consecutive count.

Far Consecutive Count : Far end high loss interval consecutive count.

Loss Measurement Signal Degrade

Enable : Enable/disable of loss measurement signal degrade.

TX Minimum : Minimum number of frames that must be transmitted in a measurement before frame loss ratio is tested against loss ratio threshold.

FLR Threshold : Signal Degraded frame loss ratio threshold in per mille (per thousand).

Bad Threshold : Number of consecutive bad interval measurements required to set degrade state.

Good Threshold : Number of consecutive good interval measurements required to clear degrade state.

Delay Measurement

Enable : Delay Measurement based on transmitting 1DM/DMM PDU can be enabled/disabled. Delay Measurement based on receiving and handling 1DM/DMR PDU is always enabled.

Priority : The priority to be inserted as PCP bits in TAG (if any).

Cast : Selection of 1DM/DMM PDU transmitted ***uni***cast or ***multi***cast. The unicast MAC will be configured through 'Peer MEP'.

Peer MEP : This is only used if the 'Cast' is configured to Uni. The 1DM/DMR unicast MAC will be taken from the 'Unicast Peer MAC' configuration of this peer.

Ended

Single: Single ended Delay Measurement implemented on DMM/DMR.

Dual: Dual ended Delay Measurement implemented on 1DM.

Tx Mode

Standardize: Y.1731 standardize way to transmit 1DM/DMR.

Proprietary: Vitesse proprietary way with follow-up packets to transmit 1DM/DMR.

Calc : This is only used if the 'Ended' is configured to single ended.

Round trip: The frame delay calculated by the transmitting and receiving timestamps of initiators.
Frame Delay = RxTimeb-TxTimeStampf

Flow: The frame delay calculated by the transmitting and receiving timestamps of initiators and remotes. Frame Delay = (RxTimeb-TxTimeStampf)-(TxTimeStampb-RxTimeStampf)

Interval : The interval between transmitting 1DM/DMM PDU in 10ms. The range is 10 to 65535.

Last-N : The last N delays measurements used for average last N calculation. Min value is 10. Max value is 100

Unit : The time resolution (***uS*** for microseconds or ***nS*** for nano-seconds).

Synchronized : Enable to use DMM/DMR packet to calculate dual ended DM. If the option is enabled, the following action will be taken. When DMR is received, two-way delay (roundtrip or flow) and both near-end-to-far-end and far-end-to-near-end one-way delay are calculated. When DMM or 1DM is received, only far-end-to-near-end one-way delay is calculated.

Counter Overflow Action : The action to counter when an overflow occurs (***Keep*** or ***Reset***).

Delay Measurement State

Tx : The accumulated transmit count - since last 'clear'.

Rx : The accumulated receive count - since last 'clear'.

Rx Error : The accumulated receive error count - since last 'clear'. This is counting if the frame delay is larger than 1 second or if far end residence time is larger than the round trip time.

Av Delay Tot : The average total delay - since last 'clear'.

Av Delay last N : The average delay of the last n packets - since last 'clear'.

Delay Min. : The minimum delay - since last 'clear'.

Delay Max. : The maximum delay - since last 'clear'.

Av Delay-Var Tot : The average total delay variation - since last 'clear'.

Av Delay-Var last N : The average delay variation of the last n packets - since last 'clear'.

Delay-Var Min. : The minimum delay variation - since last 'clear'.

Delay-Var Max. : The maximum delay variation - since last 'clear'.

Overflow : The number of counter overflow - since last 'clear'.

Clear : Set of this check and save will clear the accumulated counters.

Far-end-to-near-end one-way delay : The one-way delay is from remote devices to the local devices. Here are the conditions to calculate this delay. 1. 1DM received. 2. DMM received with Synchronized enabled. 3. DMR received with Synchronized enabled.

Near-end-to-far-end one-way delay : The one-way delay is from the local devices to remote devices. The only case to calculate this delay is below. DMR received with Synchronized enabled.

Delay Measurement Bins : A Measurement Bin is a counter that stores the number of delay measurements falling within a specified range, during a Measurement Interval.

Measurement Bins for FD **:** Configurable number of Frame Delay Measurement Bins per Measurement Interval.
The minimum number of FD Measurement Bins per Measurement Interval supported is 2.
The maximum number of FD Measurement Bins per Measurement Interval supported is 10.
The default number of FD Measurement Bins per Measurement Interval supported is 3.
Measurement Bins for IFDV : Configurable number of Inter-Frame Delay Variation Measurement Bins per Measurement Interval.
The minimum number of FD Measurement Bins per Measurement Interval supported is 2.
The maximum number of FD Measurement Bins per Measurement Interval supported is 10.
The default number of FD Measurement Bins per Measurement Interval supported is 3.

Measurement Threshold **:** Configurable the Measurement Threshold for each Measurement Bin.
The unit for a measurement threshold is in microseconds (us).
The default configured measurement threshold for a Measurement Bin is an increment of 5000 us.

Delay Measurement Bins for FD

A Measurement Bin is a counter that stores the number of delay measurements falling within a specified range, during a Measurement Interval. If the measurement threshold is 5000 us and the total number of Measurement Bins is four, example are as follows.

Bin	Threshold	Range
bin0	0 us	0 us <= measurement < 5,000 us
bin1	5,000 us	5,000 us <= measurement < 10,000 us
bin2	10,000 us	10,000 us <= measurement < 15,000 us
bin3	15,000 us	15,000 us <= measurement < infinite us

Delay Measurement Bins for IFDV

A Measurement Bin is a counter that stores the number of delay measurements falling within a specified range, during a Measurement Interval. If the measurement threshold is 5000 us and the total number of Measurement Bins is four, example are as follows.

Bin	Threshold	Range
bin0	0 us	0 us <= measurement < 5,000 us
bin1	5,000 us	5,000 us <= measurement < 10,000 us
bin2	10,000 us	10,000 us <= measurement < 15,000 us
bin3	15,000 us	15,000 us <= measurement < infinite us

Buttons

Back : Click to go back to the MEP instance main page.

Apply : Click to save changes.

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

Messages

Invalid number of peer's for this configuration

Chapter 19 - ERPS

The ERPS (Ethernet Ring Protection Switching) instances are configured here. ERPS is defined in ITU/T G.8032. ERPS provides fast protection and recovery switching for Ethernet traffic in a ring topology while also ensuring that the Ethernet layer remains loop-free.

19-1 Ethernet Ring Protection Switching

To configure the Ethernet Ring Protection Switching parameters in the web UI:

1. Click ERPS.
2. Click the Add New Entry button.
3. Specify the Ethernet Ring Protection Switching parameters.
4. Click Apply to save the changes.

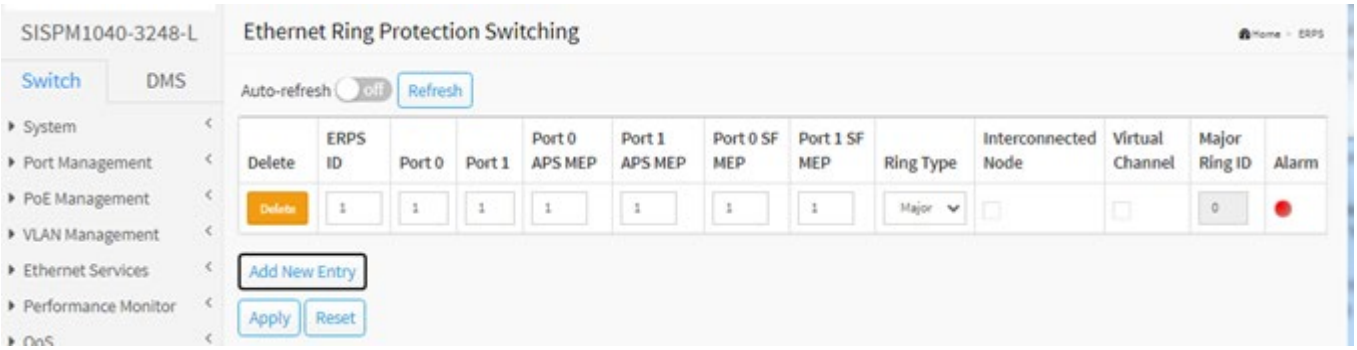


Figure 16: Ethernet Ring Protection Switching

Parameter descriptions:

Delete : This box is used to mark an EPS for deletion in next save operation.

ERPS ID : The ID of the created Protection group; It must be an integer value between 1 and 64. You can create up to 64 ERPS Protection Groups. Click on the ID of a Protection group to enter the configuration page.

Port 0 : This will create a Port 0 of the switch in the ring. 'Port 0' and 'Port 1' cannot be the same.

Port 1 : This will create "Port 1" of the switch in the Ring. As interconnected sub-ring will have only one ring port, "Port 1" is configured as "0" for interconnected sub-ring. A "0" in this field indicates that no "Port 1" is associated with this instance

Port 0 SF MEP : The Port 0 Signal Fail reporting MEP. The 'Port 0 SF MEP' must be an integer 1 - 3124.

Port 1 SF MEP : The Port 1 Signal Fail reporting MEP. As only one SF MEP is associated with interconnected sub-ring without virtual channel, it is configured as "0" for such ring instances. "0" in this field indicates that no Port 1 SF MEP is associated with this instance.

Port 0 APS MEP : The Port 0 APS PDU handling MEP. 'Port 0 APS MEP' and 'Port 1 APS MEP' can not be the same.

Port 1 APS MEP : The Port 1 APS PDU handling MEP. As only one APS MEP is associated with interconnected sub-ring without virtual channel, it is configured as "0" for such ring instances. "0" in this field indicates that no Port 1 APS MEP is associated with this instance. 'Port 1 APS MEP' must be an integer 1 - 3124.

Ring Type : Type of Protecting ring. It can be either major ring or sub-ring.

Interconnected Node : Interconnected Node indicates that the ring instance is interconnected. Click on the checkbox to configure this. "Yes" indicates it is an interconnected node for this instance. "No" indicates that the configured instance is not interconnected.

Virtual Channel : Sub-rings can either have virtual channel or not on the interconnected node. This is configured using "Virtual Channel" checkbox. "Yes" indicates it is a sub-ring with virtual channel. "No" indicates, sub-ring doesn't have virtual channel.

Major Ring ID : Major ring group ID for the interconnected sub-ring. It is used to send topology change updates on major ring. If ring is major, this value is same as the protection group ID of this ring.

Alarm : There is an active alarm on the ERPS. A red dot (●) indicates 'Down'.

Buttons

Auto-refresh : Click to refresh the page automatically every 3 seconds.

Refresh : Click to manually refresh the page immediately.

Add New Entry: Click to add a new Protection group entry. Only one ERPS can be added for each Apply operation.

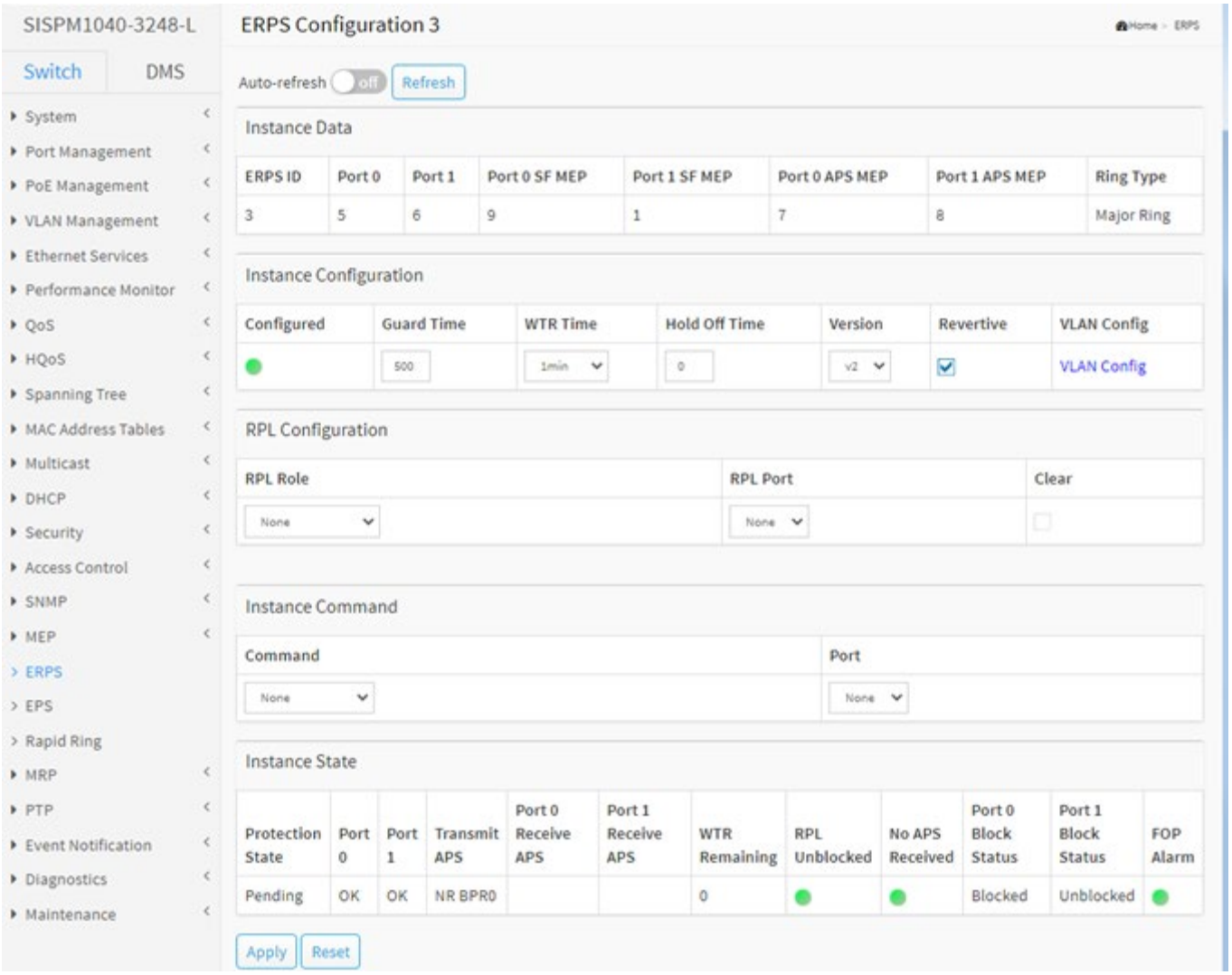
Apply : Click to save changes.

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

Example

Click on the ID of a Protection group to enter the configuration page. ERPS Configuration 3 is shown below.

ERPS Configuration 3



Parameter descriptions:

Instance Data

ERPS ID : The ID of the Protection group.

Port 0 : This will create a Port 0 of the switch in the ring. 'Port 0' and 'Port 1' can not be the same.

Port 1 : This will create "Port 1" of the switch in the Ring. As interconnected sub-ring will have only one ring port, "Port 1" is configured as "0" for interconnected sub-ring. A "0" in this field indicates that no "Port 1" is associated with this instance

Port 0 SF MEP : The Port 0 Signal Fail reporting MEP. 'Port 0 SF MEP' must be an integer 1 - 3124.

Port 1 SF MEP : The Port 1 Signal Fail reporting MEP. As only one SF MEP is associated with interconnected sub-ring without virtual channel, it is configured as "0" for such ring instances. "0" in this field indicates that no Port 1 SF MEP is associated with this instance.

Port 0 APS MEP : The Port 0 APS PDU handling MEP. 'Port 0 APS MEP' and 'Port 1 APS MEP' can not be the same.

Port 1 APS MEP : The Port 1 APS PDU handling MEP. As only one APS MEP is associated with interconnected sub-ring without virtual channel, it is configured as "0" for such ring instances. "0" in this field indicates that no Port 1 APS MEP is associated with this instance. 'Port 1 APS MEP' must be an integer 1 - 3124.

Ring Type : Type of Protecting ring. It can be either ***Major Ring*** or ***Sub Ring***.

19-2 ERPS Instance Configuration

Configured : Displays a red or green dot to indicate whether the ERPS instance is active or not active:

- **Red:** This ERPS is only created and has not yet been configured and is not active.
- **Green:** This ERPS is configured and is active.

Guard Time : Guard timeout value to be used to prevent ring nodes from receiving outdated R-APS messages. The period of the guard timer can be configured in 10 ms steps between 10 ms and 2 seconds, with a default value of 500 ms.

WTR Time : The Wait To Restore timing value to be used in revertive switching. The period of the WTR time can be configured in 1 minute steps of 1 - 12 minutes with a default value of 5 minutes.

Hold Off Time : The timing value to be used to make persistent check on Signal Fail before switching. The range is 0 - 10 seconds in steps of 100 ms.

Version : ERPS Protocol Version - v1 or v2.

Revertive : In ***Revertive*** mode, after the conditions causing a protection switch has cleared, the traffic channel is restored to the working transport entity, i.e., blocked on the RPL.
In ***Non-Revertive*** mode, the traffic channel continues to use the RPL, if it is not failed, after a protection switch condition has cleared.

VLAN config : VLAN configuration of the Protection Group. Click on the "VLAN Config" link to configure VLANs for this protection group. See below.

19-3 RPL Configuration

RPL Role : It can be either RPL owner or RPL Neighbor.

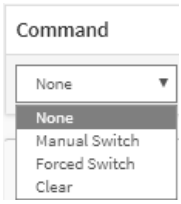
RPL Port : This allows to select the east port or west port as the RPL block.

Clear : If the owner has to be changed, then the clear check box allows to clear the RPL owner for that ERPS ring.

19-4 Sub-Ring Configuration

Topology Change : Clicking this checkbox indicates that the topology changes in the sub-ring are propagated in the major ring.

19-5 Instance Command



Command : Administrative command. A port can be administratively configured to be in either Manual Switch or Forced Switch state:

Forced Switch : Forced Switch command forces a block on the ring port where the command is issued.

Manual Switch : In the absence of a failure or FS, Manual Switch command forces a block on the ring port where the command is issued.

Clear : Clear command used for clearing an active local admin command (e.g., Forced Switch or Manual Switch).

Port : Port selection - Port0 or Port1 of the protection Group on which the command is applied.

Instance State

Instance State

Protection State	Port 0	Port 1	Transmit APS	Port 0 Receive APS	Port 1 Receive APS	WTR Remaining	RPL Unblocked	No APS Received	Port 0 Block Status	Port 1 Block Status	FOP Alarm
Manual	OK	OK	MS DNF BPR0			0			Blocked	Unblocked	

Protection State : ERPS state according to State Transition Tables in G.8032 (e.g., Manual).

Port 0 : **OK:** State of East port is ok. **SF:** State of East port is Signal Fail.

Port 1 : **OK:** State of West port is ok. **SF:** State of West port is Signal Fail

Transmit APS : The transmitted APS from G.8032 State Transition Tables (e.g., *MS DNF BPR1* or *NR RB DNF BPR0*).

Port 0 Receive APS : The received APS on Port 0 according to State Transition Tables in G.8032.

Port 1 Receive APS : The received APS on Port 1 according to State Transition Tables in G.8032.

WTR Remaining : Remaining WTR timeout in milliseconds.

RPL Un-blocked : APS is received on the working flow.

No APS Received : RAPS PDU is not received from the other end.

Port 0 Block Status : Block status for Port 0 (both traffic and R-APS block status). R-APS channel is never blocked on sub-rings without virtual channel.

Port 1 Block Status : Block status for Port 1 (both traffic and R-APS block status). R-APS channel is never blocked on sub-rings without virtual channel.

FOP Alarm : Failure of Protocol Defect (FOP) status. If FOP is detected, red LED displays; else green LED displays.

Buttons

Apply : Click to save changes.

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

Refresh : Click to manually refresh the page immediately.

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

19-6 ERPS VLAN Configuration

In the 'Instance Configuration' section click the VLAN Config link to display ERPS VLAN Configuration 3:

Parameter descriptions:

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

VLAN ID : Indicates the ID of this particular VLAN.

Add New Entry : Click to add a new VLAN ID. Valid values for a VLAN ID are 1 - 4095. The VLAN is enabled when you click Apply. A VLAN without any port members will be deleted when you click Apply. The Delete button can be used to undo the addition of new VLANs.

Buttons

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

Refresh **Refresh** : Click to manually refresh the page immediately. Refreshes the displayed table starting from the "VLAN ID" input fields.

Apply : Click to save changes.

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

Back : Click to go back to the main page.

Messages:

'Port 0' and 'Port 1' can not be same

'Port 0 APS MEP' and 'Port 1 APS MEP' can not be same

Port 0 SF MEP and Port 1 SF MEP can not be same

'Port 1' must be zero

'Port 1 SF MEP' must be zero

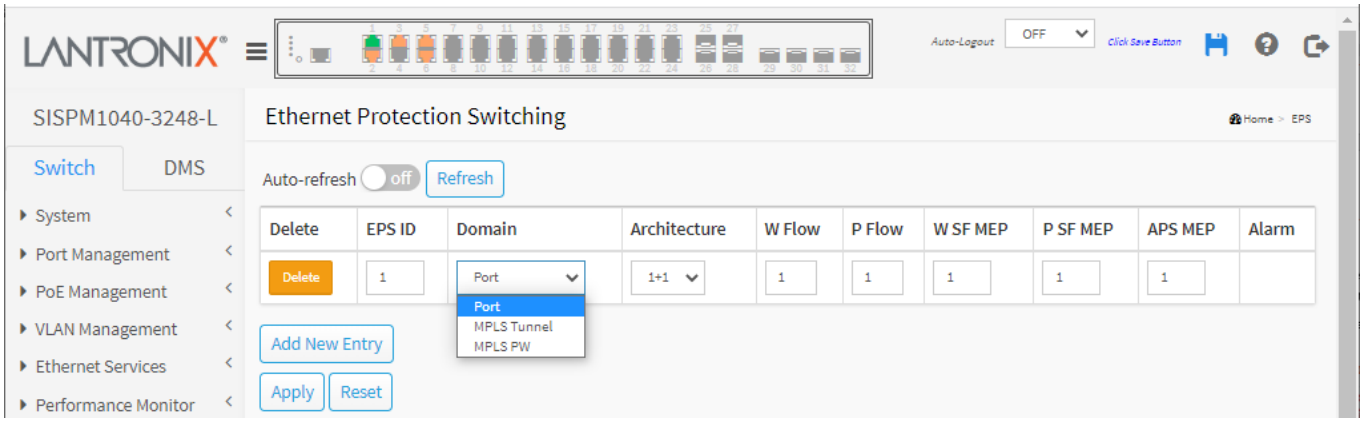
'Port 0 SF MEP' must be an integer value between 1 and 3124

Chapter 20 - EPS

The EPS (Ethernet Protection Switching) instances are configured here. EPS is defined by ITU-T G.8031 Ethernet Linear Protection Switching (EPS).

From the default page, click the Add New Entry button to display the Ethernet Protection Switching page.

20-1 EPS Configuration



Parameter descriptions:

Delete : This box is used to mark an EPS for deletion in next Save operation.

EPS ID : The ID of the EPS. The range is 1-100. Click on the ID of an EPS to enter the configuration page (see the example below).

Domain : Dropdown to select either Port, MPLS Tunnel, or MPLS PW:

Port: This will create a EPS in the Port Domain. 'W/P Flow' is a Port.

MPLS Tunnel: This will create a EPS in the MPLS Tunnel Domain. 'W/P Flow' is a MPLS Tunnel.

MPLS PW: This will create a EPS in the MPLS PW Domain. 'W/P Flow' is a MPLS PW.

Architecture : Dropdown to select:

Port: This will create a 1+1 EPS.

Port: This will create a 1:1 EPS.

W Flow : The working flow for the EPS - See 'Domain' above. The working flow and protection flow cannot be equal. The default is 1.

P Flow : The protecting flow for the EPS - See 'Domain' above. The default is 1. The working flow and protection flow cannot be equal.

W SF MEP : The working Signal Fail reporting MEP. The default is 1. The Working MEP and Protecting SF MEP cannot be the same instance.

P SF MEP : The protecting Signal Fail reporting MEP. The default is 1. The Working MEP and Protecting SF MEP cannot be the same instance.

APS MEP : The APS PDU handling MEP. The default is 1.

Alarm : Displays if there is an active alarm on the EPS. Green (●) means Up, Red (●) means Down.

Buttons

Auto-refresh : Click to refresh the page automatically every 3 seconds.

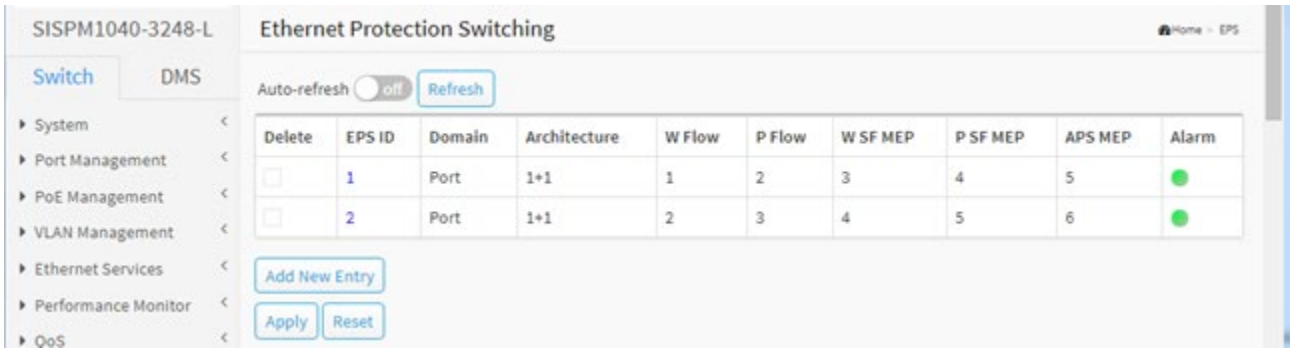
Refresh : Click to manually refresh the page immediately.

Add New Entry: Click to add a new EPS entry. Note: Only one EPS can be added for each Save operation.

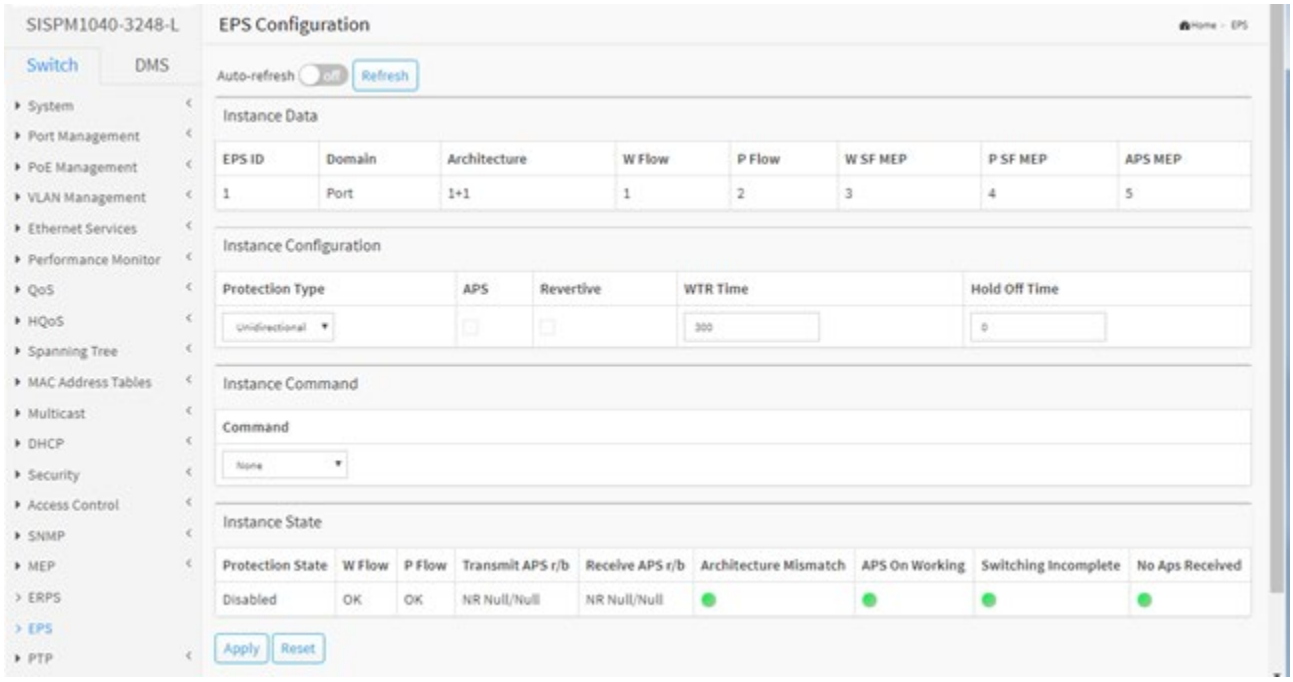
Apply: Click to save changes. **Note:** Only one EPS can be added for each Save operation.

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

Example



Click an EPS ID to display its configuration page:



Parameter descriptions:

Instance Data

EPS ID : The ID of the EPS.

Domain : Dropdown to select either Port, MPLS Tunnel, or MPLS PW:

Port: This will create a EPS in the Port Domain. 'W/P Flow' is a Port.

MPLS Tunnel: This will create a EPS in the MPLS Tunnel Domain. 'W/P Flow' is a MPLS Tunnel.

MPLS PW: This will create a EPS in the MPLS PW Domain. 'W/P Flow' is a MPLS PW.

Architecture : Dropdown to select:

Port: This will create a 1+1 EPS.

Port: This will create a 1:1 EPS.

W Flow : The working flow for the EPS - See 'Domain'. The working flow and protection flow cannot be equal.

P Flow : The protecting flow for the EPS - See 'Domain'. The working flow and protection flow cannot be equal.

W SF MEP : The working Signal Fail reporting MEP. The Working MEP and Protecting SF MEP cannot be the same instance.

P SF MEP : The protecting Signal Fail reporting MEP. The Working MEP and Protecting SF MEP cannot be the same instance.

APS MEP : The APS PDU handling MEP.

Instance Configuration

Configured : Red or green:

Red: This EPS is only created and has not yet been configured - is not active.

Green: This EPS is configured - is active.

Protection Type : Unidirectional or Bidirectional:

Unidirectional: EPS in the two ends can select traffic from different working/protecting flow. This is only possible in case of 1+1.

Bidirectional: EPS in the two ends is selecting traffic from the same working/protecting flow. This requires APS enabled. This is mandatory for 1:1

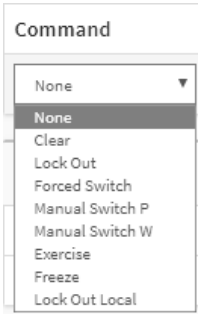
APS : The Automatic Protection Switching protocol can be enabled/disabled. This is mandatory for 1:1.

Revertive : The revertive switching to working flow can be enabled/disabled.

WTR Time : The Wait To Restore timing value to be used in revertive switching. The valid range is 1 to 720 seconds. The default is 200 seconds.

Hold Off Time : The timing value to be used to make persistent check on Signal Fail before switching. This is in 100 ms. and the max value is 100 (10 seconds). The default is 0 seconds.

Instance Command



Command : At the dropdown select one of the following commands:

None: There is no active local command on this instance (default).

Clear: The active local command will be cleared.

Lock Out: This EPS is locked to working (not active). In case of 1:N (more than one EPS with same protecting flow) - when one EPS switch to protecting flow, other EPS is enforced this command

Forced Switch: Forced switch to protecting.

Manual Switch P: Manual switch to protecting.

Manual Switch W: Manual switch to working. This is only allowed in case of 'non-revertive' mode

Exercise: Exercise of the protocol - not traffic effecting. This is only allowed in case of 'Bidirectional' protection type

Freeze: This EPS is locally freezed - ignoring all input.

Lock Out Local: This EPS is locally "locked out" - ignoring local SF detected on working.

Instance State

Protection State : EPS state according to the State Transition Tables in G.8031.

W Flow : Can be OK or SF:

OK: State of working flow is ok

SF: State of working flow is Signal Fail

SD: State of working flow is Signal Degrade (for future use)

P Flow : Can be OK or SF:

OK: State of protecting flow is ok

SF: State of protecting flow is Signal Fail

SD: State of protecting flow is Signal Degrade (for future use)

Transmit APS r/b : The transmitted APS according to State Transition Tables in G.8031.

Receive APS r/b : The received APS according to State Transition Tables in G.8031.

Architecture Mismatch : The architecture indicated in the received APS does not match the locally configured.

APS on working : APS is received on the working flow.

Switching Incomplete : Traffic is not selected from the same flow instance in the two ends.

No APS Received : APS PDU is not received from the other end.

Buttons

Auto-refresh : Click to refresh the page automatically every 3 seconds.

Refresh : Click to manually refresh the page immediately.

Apply : Click to save changes.

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

Messages

Only one EPS can be added for each Save operation

Invalid architecture for this domain

The working and protection flows are equal

The working flow is used by other EPS instance

Working MEP and protecting SF MEP is same instance

MEP instance must not be zero

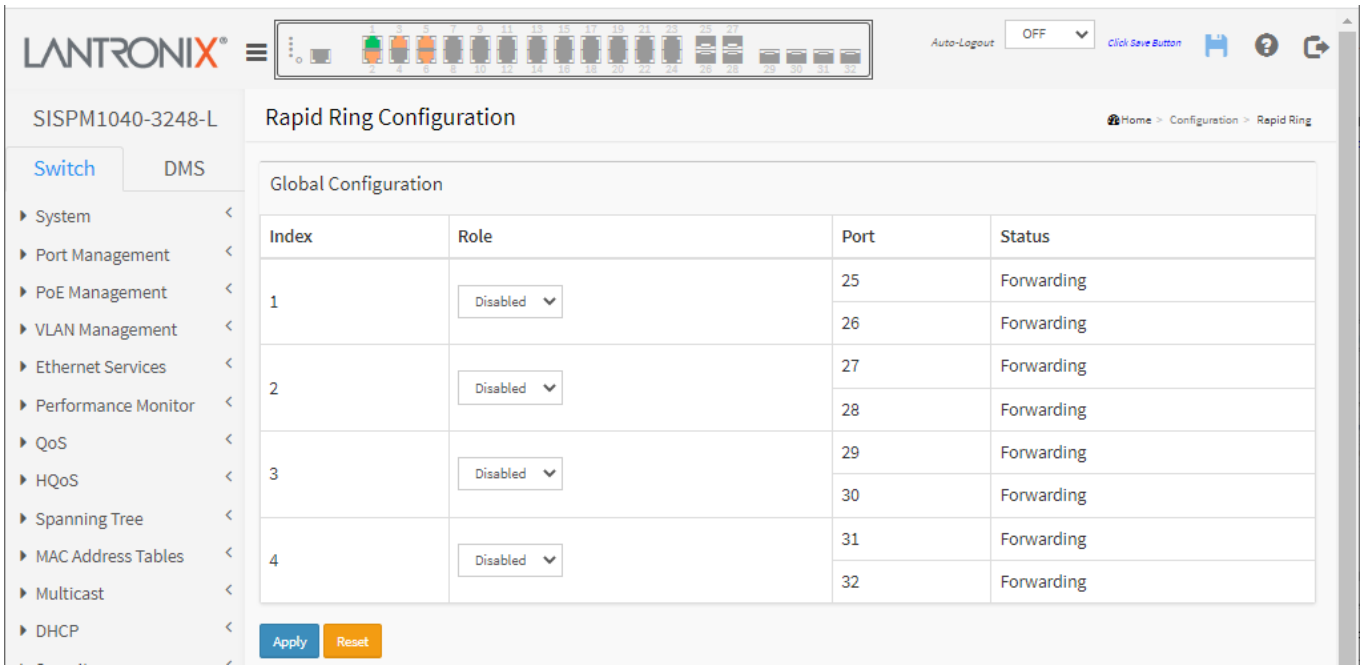
Chapter 21 - Rapid Ring

21-1 Configuration

This page lets you configure and view Rapid Ring Global parameters. Other Ring technologies (e.g. STP, MRP) must be disabled for Rapid Ring to be configured..

Rapid Ring is a redundancy proprietary protocol on your network, it can be used to recover the network system from critical links failure to protect from network loops. Many redundant or network recovery protocols are defined by IEEE, such as spanning tree (STP, RSTP, MSTP) developed to recover the network system for the connection failure, but the recovery time of Rapid Ring can be less than 20ms on up to 250 switches (much less than the other redundancy protocols).

1. Navigate to Configuration > Rapid Ring.
2. Set role values for the desired ports.
3. Click the Apply button.
4. Observe the Status column.



Parameter descriptions:

Role: Set role value. The selections are Disabled, Master, and Member. The default is Disabled.

Port: The switch port number of the port (e.g., 25-32).

Status: The current Rapid Ring status of the port (e.g., *Forwarding*).

Messages:
Rapid Ring Configuration Error
Error in port 25, STP is enable

Chapter 22 –Percepxion and LPM

22-1 Configuration

This page lets you configure Percepxion parameters. This page has four sections: the Status, Configuration, Percepxion Connection 1, and Connection 2 sections as shown and described below.

Percepxion is Lantronix cloud-hosted or on-premise management platform that provides a single pane of glass for centralized management and automated monitoring of deployed Lantronix devices, along with real-time notifications, managed APIs, and data dashboards. See https://www.lantronix.com/percepxion/ for more information.

Lantronix Provisioning Manager (LPM) is a software application that provisions, configures and updates Lantronix Console Managers and IoT Gateways for local site installations and deployments. LPM discovery is enabled by default and is not configurable. For more LPM information see https://www.lantronix.com/products/lantronix-provisioning-manager/.

There are three pieces of information that the Percepxion client needs to complete registration and to publish data and configuration to the Percepxion server: Serial Number, Device ID, and Device Key. The Serial Number is always preprogrammed on the device (typically derived from the MAC address of the first Ethernet port). A new device would also be preprogrammed with the Device ID and Key.

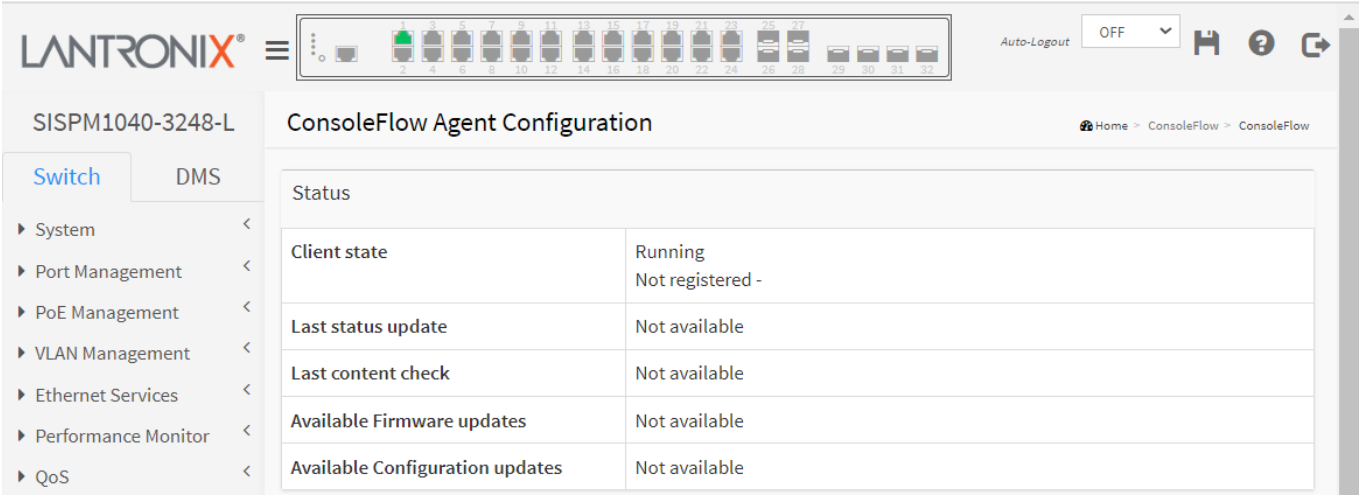
For existing devices where the ID and Key are not pre-programmed, LPM uses Lantronix proprietary search and query protocol to get the device serial number, and then uses the switch REST API interface to set the Device ID and Device Key.

Supported Firmware Versions

Devices must meet firmware requirements in order to work with Percepxion and LPM. SISPM1040-3166-L and SISPM1040--3248-L require firmware v8.50.0149 or above.

Percepxion Agent Configuration

Navigate to Configuration > Percepxion to display the Percepxion Agent Configuration page:



Parameter descriptions:

Status:

Client state: Displays the existing Percepxion client state (e.g., *Exited*, *Active, Inactive, Running,* or *Not Registered*).

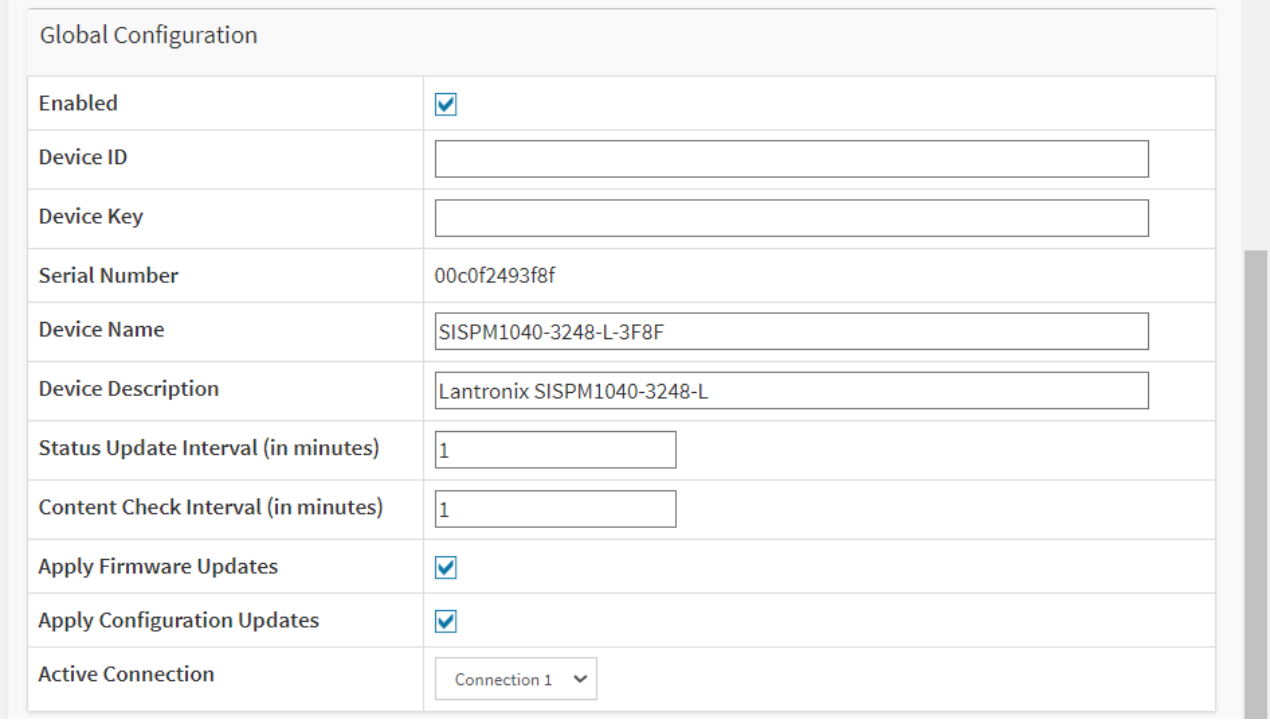
Last status update: Displays the amount of time in minutes between status updates (1-1440 minutes or *<Not Available>.*

Last content check: Displays the amount of time in minutes between content checks; 1 minute to 90 days (in minutes) or *<Not Available>.*

Available Firmware updates: Displays a list of firmware that is available on the server. Select the firmware from this list and click Update now to upgrade or downgrade the firmware. Displays *<Not available>* if no Firmware updates are currently available.

Available Configuration updates: Displays a list of configuration that is available on the server. Select the configuration from this list and click Update now to upgrade or downgrade the firmware. Displays *<Not available>* if no configuration updates are currently available.

Global Configuration:



Enabled : Check the box to enable Percepxion globally. The default is disabled (unchecked).

Device ID: Enter the switch Device ID. The Device ID may be provisioned through Lantronix Provisioning Manager (LPM). **Note**: The Device ID can only be provisioned once. It will persist across resets.

Device Key: Enter the key for the device; 32 alphanumeric characters. **Note**: Device Key may be configured via the Lantronix Provision Manager (LPM). The entry field shows two icons:

 : Click to Show the Device Key text as you enter it.

 : Click to Hide the Device Key text as you enter it (default).

Serial Number : Displays the serial number of the switch in the format *11-22-33-44-55-66*. Read only.

Device Name : Enter a Percepxion Device Name for the switch of up to 32 alphanumeric characters (e.g., *SISPM1040-384-SAAS*). Device Name can have only alphanumeric (a-z, A-Z, 0-9) characters, hyphens (-), and underscores (_). Device Name must begin and end with an alphanumeric character.

Device Description : Enter a Percepxion Device Description for the switch of up to 32 alphanumeric characters (e.g., *SISGM1040-284-LRT*).

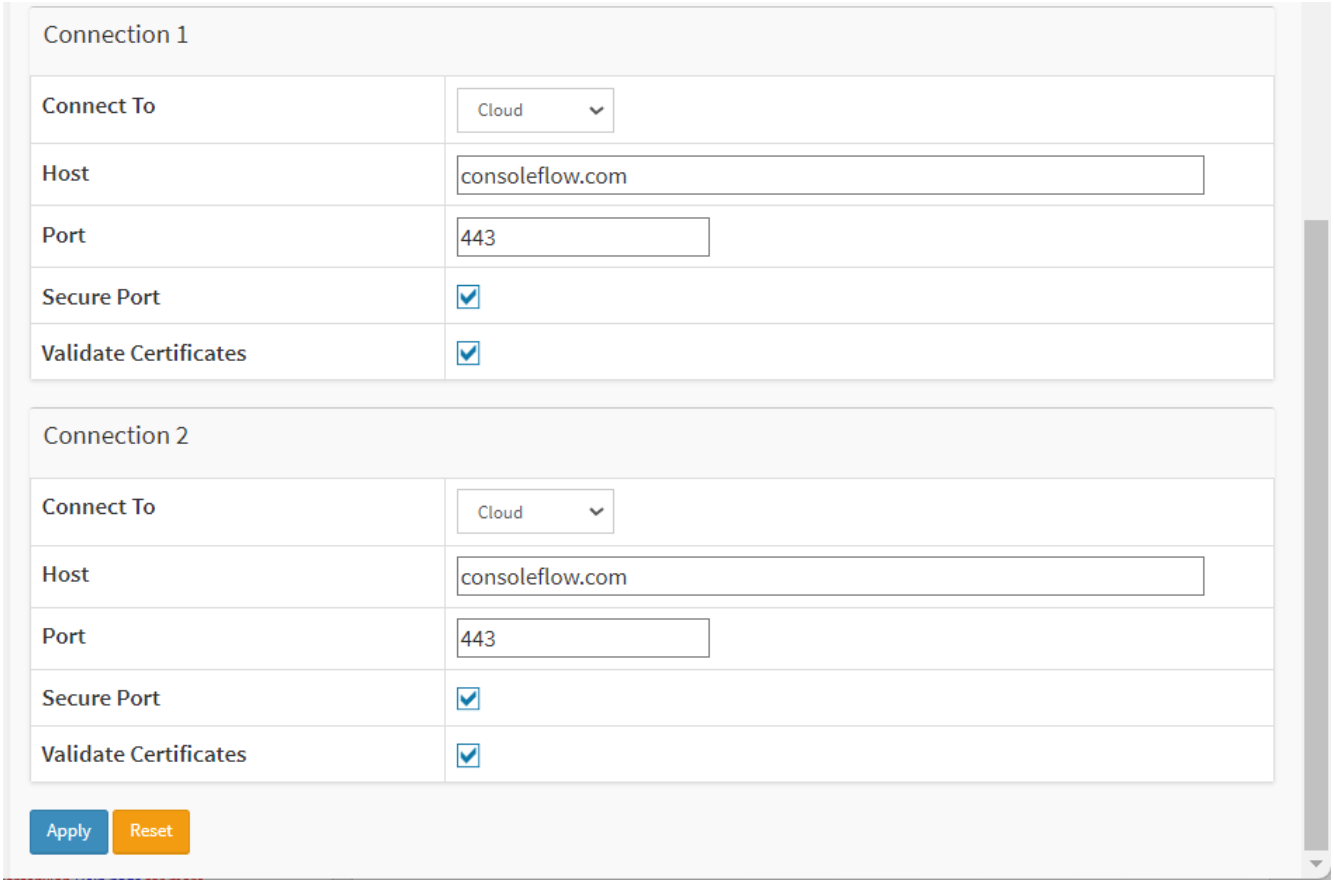
Status Update Interval : Select the amount of time in minutes between updates (1-1440 minutes). The default is 1 minute. This is the frequency that the switch updates the device status to Percepxion.

Content Check Interval : Select the amount of time in minutes between content checks (1-56160 minutes). The default is 1 minute. This is the frequency that the switch checks Percepxion for updates to configuration or firmware. The valid range is 1 hour – 2160 hours (90 days).

Apply Firmware Updates : Check the box to enable automatic switch firmware upgrades via Percepxion. The default is enabled.

Apply Configuration Updates : Check the box to enable automatic switch configuration upgrades via Percepxion. The default is enabled.

Active Connection: At the dropdown select the configuration you want to be active (i.e., *Connection 1* or *Connection 2*. The default is *Connection 1*. This is the connection to use when connecting to Percepxion. The configurable parameters for Connection 1 and Connection 2 are shown and described below.



Parameter descriptions:

Connection 1 :

Connect To : At the dropdown, select Cloud (default) or On Premise as the Percepxion connection type for Connection 1. Percepxion is available in cloud or on-premise installation. Choose cloud or on-premise setup according to the determination of your organization. See the Percepxion Signin page for more information.

Cloud setup connects you directly to the Percepxion server URL, allowing you to access your devices through the Internet.

On-premise setup connects you to Percepxion through your organization's network. This means you need to be physically "on-premises" to access your organization's network via Wi-Fi, or may need to use a VPN connection. You may later view and update on-premise setup.

Host : Enter the IP address or host name of the Percepxion server for Connection 1. This is used by Percepxion to register the switch.

Port : Enter the port number for Connection 1. The default is port 443.

Secure Port : Check the box to make the selected port a secure port for Connection 1. The default is enabled.

Validate Certificates : Check the box to force using certificate validation for Connection 1. The default is enabled. To validate certificates, Secure Port must be enabled.

Connection 2 :

Connect To : At the dropdown, select Cloud (default) or On Premise as the Percepxion connection type for Connection 1. Percepxion is available in cloud or on-premise installation. Choose cloud or on-premise setup according to the determination of your organization. See the Percepxion Signin page for more information.

Cloud setup connects you directly to the Percepxion server URL, allowing you to access your devices through the Internet.

On-premise setup connects you to Percepxion through your organization's network. This means you need to be physically "on-premises" to access your organization's network via Wi-Fi, or may need to use a VPN connection. You may later view and update on-premise setup.

Host : Enter the IP address of the Percepxion Host for Connection 2.

Port : Enter the port number for Connection 2 for Connection 2. The default is port 443.

Secure Port : Check the box to make the selected port a secure port for Connection 2. The default is enabled.

Validate Certificates : Check the box to enable using certificate validation of the Percepxion server certificates. To validate certificates, Secure Port must be enabled. The default is enabled.

Buttons

Apply : Click to apply changes.

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

Messages:

device id : 32 alphanumeric characters

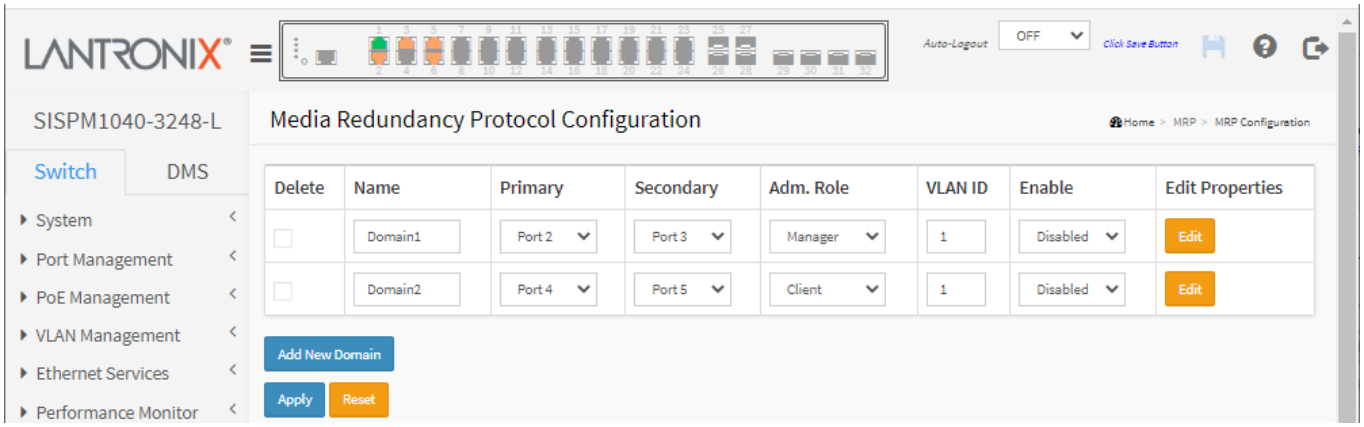
5

Chapter 23 - MRP

23-1 Configuration

This page lets you configure and view Media Redundancy Protocol parameters. Other Ring technologies (e.g. STP, Rapid Ring) must be disabled. See “Appendix B – MRP Configuration” on page 485 for more MRP information.

1. Navigate to Configuration > MRP > MRP Configuration.
2. Click the Add New Domain button.
3. Set the values for the parameters listed below.
4. Click the Apply button.
5. Click the Edit button to edit domain properties.



Parameter descriptions:

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

Name: A logical name for the MRP domain to easy the management of MRP domains.

Primary: The index of the layer 2 interface which is used as ring port 1.

Secondary: The index of the layer 2 interface which is used as ring port 2.

Adm. Role: If the value is set to client the entity shall be set to the role of a Media Redundancy Client (MRC). If the value is set to manager the entity shall be set to the role of a Media Redundancy Manager (MRM).

VLAN ID: The VLAN ID assigned to the MRP protocol. The valid range is 0 - 4094.

Enable: Enable/Disable MRP protocol.

Edit Properties: Contains the Edit Properties button. See the “Ring Domain Configuration” section below.

Buttons

Add New Domain: Click to add a new domain row.

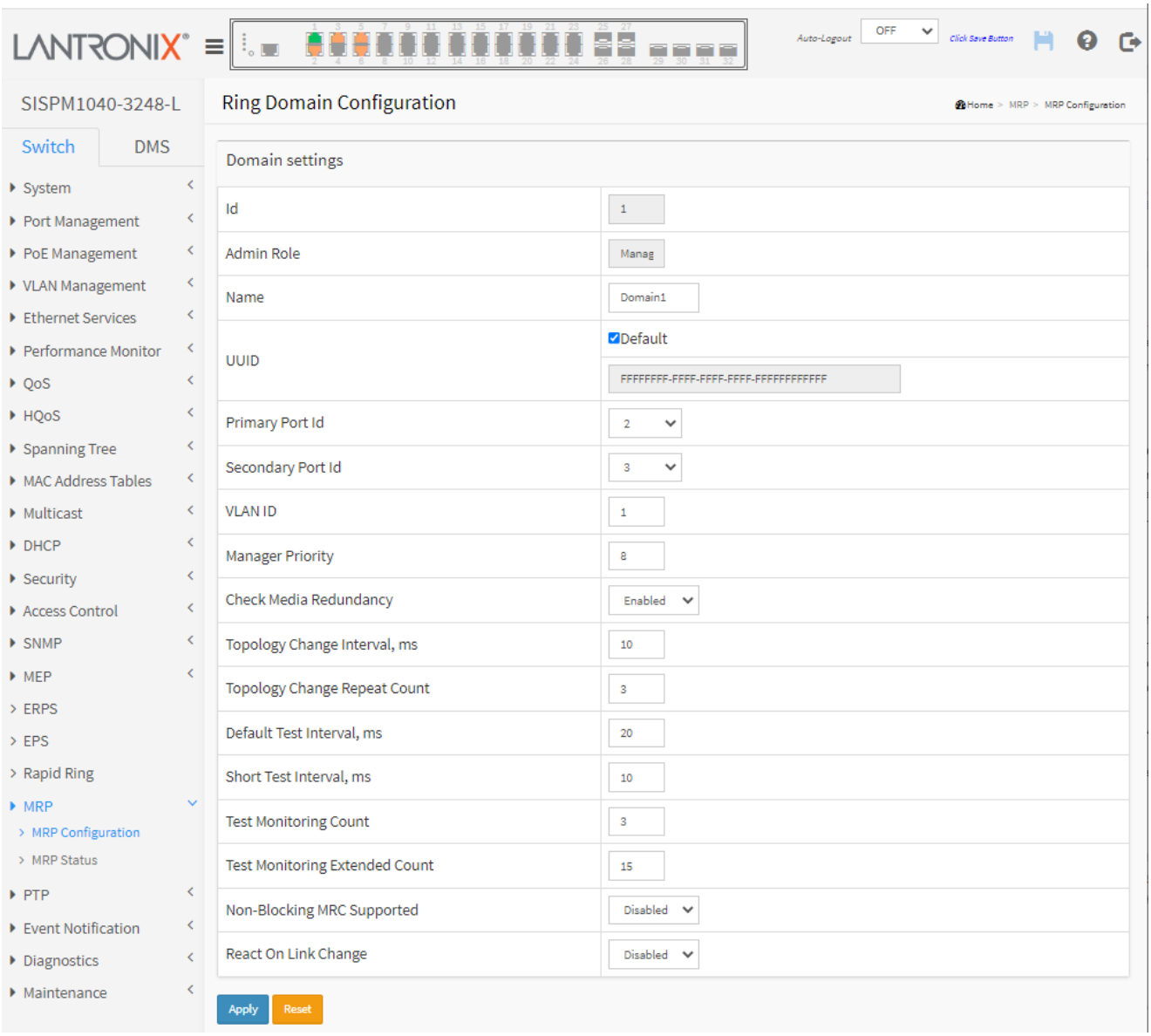
Edit: Click the button in the Edit Properties column to edit domain properties.

Apply: Click to save changes.

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

Ring Domain Configuration

When you click the Edit button the Ring Domain Configuration page displays:



Parameter descriptions:

ID: The index of the entry.

Admin Role: If the value is set to Client the entity will be set to the role of a Media Redundancy Client (MRC). If the value is set to Manager the entity will be set to the role of a Media Redundancy Manager (MRM).

Name: A logical name for the MRP domain to easy the management of MRP domains.

UUID: Universally unique identifier belongs to the MRP domain which represents a ring.

Primary Port ID: The index of the layer 2 interface which is used as ring port 1.

Secondary Port ID: The index of the layer 2 interface which is used as ring port 2.

VLAN ID: The VLAN ID assigned to the MRP protocol. The allowed range is 0 to 4094.

Manager Priority: This parameter contains the value for the manager priority.

Check Media Redundancy: Select whether monitoring of MRM state is enabled or disabled. Only MRM.

Topology Change Interval, ms: Contains the value of the interval for sending MRP_TopologyChange frames. The allowed range is 1 to 20. Only MRM.

Topology Change Repeat Count: This parameter contains the value of the interval count which controls repeated transmissions of MRP_TopologyChange frames. The allowed range is 1 to 5. Only MRM.

Default Test Interval, ms: This parameter contains the value of the default interval for sending MRP_Test frames on ring ports. The allowed range is 1 to 50. Only MRM.

Short Test Interval, ms: This parameter contains the value of the short interval for sending MRP_Test frames on ring ports after link changes in the ring. The allowed range is 1 to 30. Only MRM.

Test Monitoring Count: This parameter contains the value of the interval count for monitoring the reception of MRP_Test frames. The allowed range is 1 to 15. Only MRM.

Test Monitoring Extended Count: This optional parameter contains the value of the extended interval count for monitoring the reception of MRP_Test frames. The allowed range is 1 to 30. Only MRM.

Non-Blocking MRC Supported: This parameter specifies the ability of the MRM to support MRCs without BLOCKED port state support in the ring. Only MRM.

React On Link Change: This optional parameter specifies whether the MRM reacts on MRP_LinkChange frames or not. Only MRM.

Link Down Interval, ms: This parameter contains the value of the interval for sending MRP_LinkDown frames on ring ports. The allowed range is 1 to 50. Only MRC.

Link Up Interval, ms: This parameter contains the value of the interval for sending MRP_LinkUp frames on ring ports. The allowed range is 1 to 50. Only MRC.

Link Change Count: This parameter contains the value of the MRP_LinkChange frame count which controls repeated transmissions of MRP_LinkUp or MRP_LinkDown frames. The allowed range is 1 to 10. Only MRC.

BLOCKED State Supported: Specifies whether the MRC supports BLOCKED state at its ring ports. Only MRC.

Buttons

Apply: Click to save changes.

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

Messages:

Ring port is used

The name is used with other domain

The maximum number of entries is 2

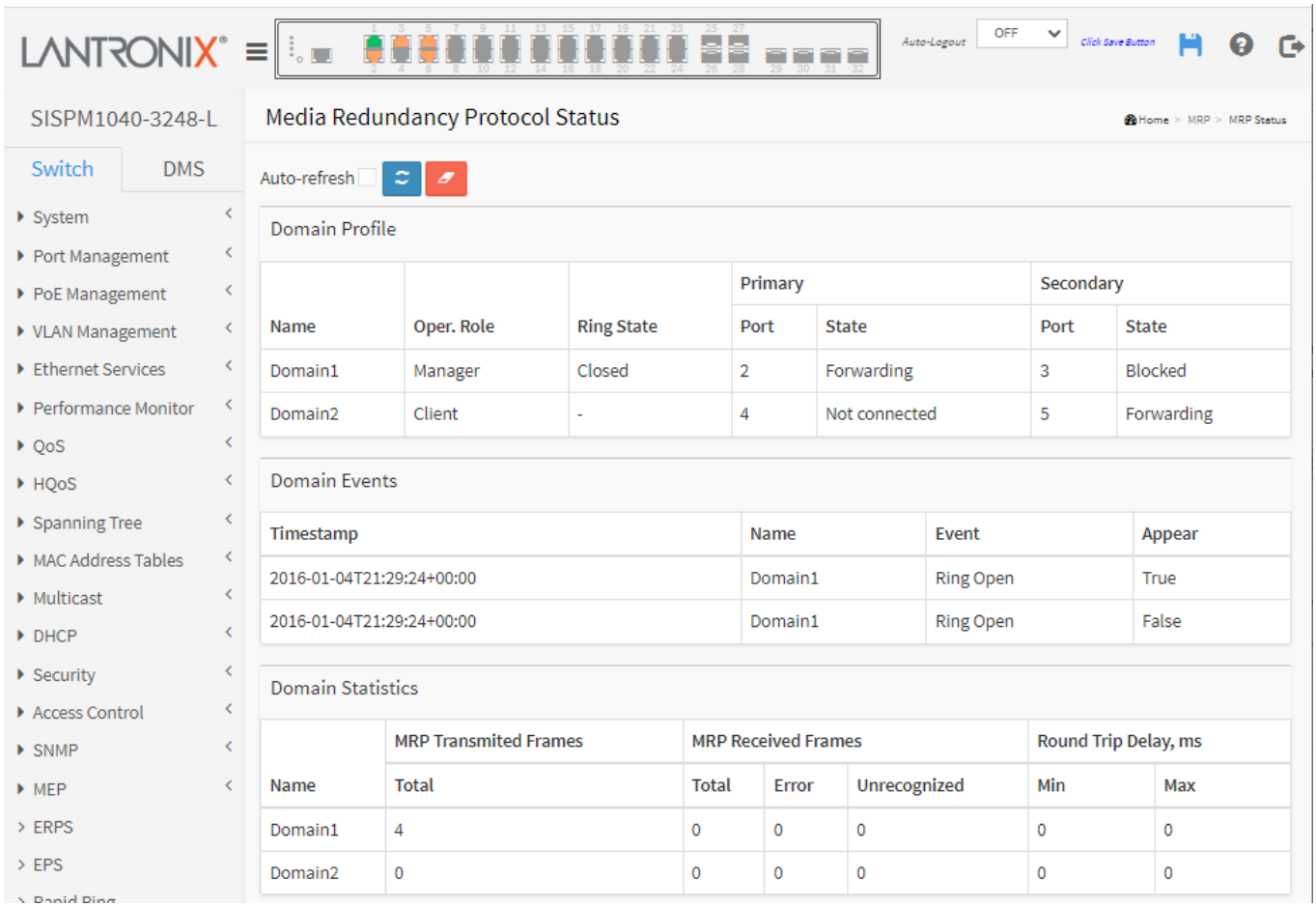
VLAN ID is used in other ring domain

Domain is enabled

23-2 Status

This page lets you view Media Redundancy Protocol parameters:

1. Navigate to Configuration > MRP > MRP Status.
2. Observe the page data.
3. Click the Refresh button to update the page data.
4. Click the Clear button to clear the settings.



Parameter descriptions:

Domain Profile

Name: A logical name for the MRP domain to easy the management of MRP domains (Domain1 or Domain2).

Oper. Role: The operational role of an MRP entity per domain (Manager, Client, or Undefined).

Ring State: Ring status of the MRP entity (e.g., Open, Closed, Undefined).

Primary: The Port number of the layer 2 interface which is used as ring port 1.

Secondary: The Port number of the layer 2 interface which is used as ring port 2.

State: The current state (e.g., Forwarding, Not connected, Unknown).

Domain Events

Timestamp: The amount of system up time at the time of the logged event in the format 2020-05-28T16:41:30+00:00).

Name: A logical name for the MRP domain (e.g., Domain1 or Domain2).

Event: The Event type (e.g., Ring Open).

Appear: Event appear (True) or disappear (False).

Domain Statistics

Name: The domain for this row (Domain1 or Domain2).

MRP Transmitted Frames: The total transmitted frames.

MRP Received Frames: The total received frames.

Round Trip Delay (ms): The Round-Trip-Delay (in milliseconds) which was measured since startup. Minimum and maximum values.

Buttons

Refresh: Click the button to update the page data.

Clear: Click the button to clear the settings.

Chapter 24 - PTP

24-1 Configuration

This page lets you configure and view up to four PTP clock instances.

PTP (Precision Time Protocol) is a network protocol for synchronizing the clocks of computer systems. PTPv2 per IETF RFC 8173 defines a portion of the Management Information Base (MIB) module for use with network management protocols in the Internet community. In particular, it describes managed objects used for managing PTP devices including ordinary clocks, transparent clocks, and boundary clocks. This MIB module is read-only and not intended to provide the ability to configure PTP clocks. Since PTP clocks are often embedded in other network elements such as routers, switches, and gateways, this ability is generally provided via the configuration interface for the network element.

To configure PTP in the web UI:

1. Click PTP and Configuration.
2. Click the Add New Entry button.
3. Set the parameters in the PTP External Clock Mode section.
4. Specify the parameters in the PTP Clock Configuration section.
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

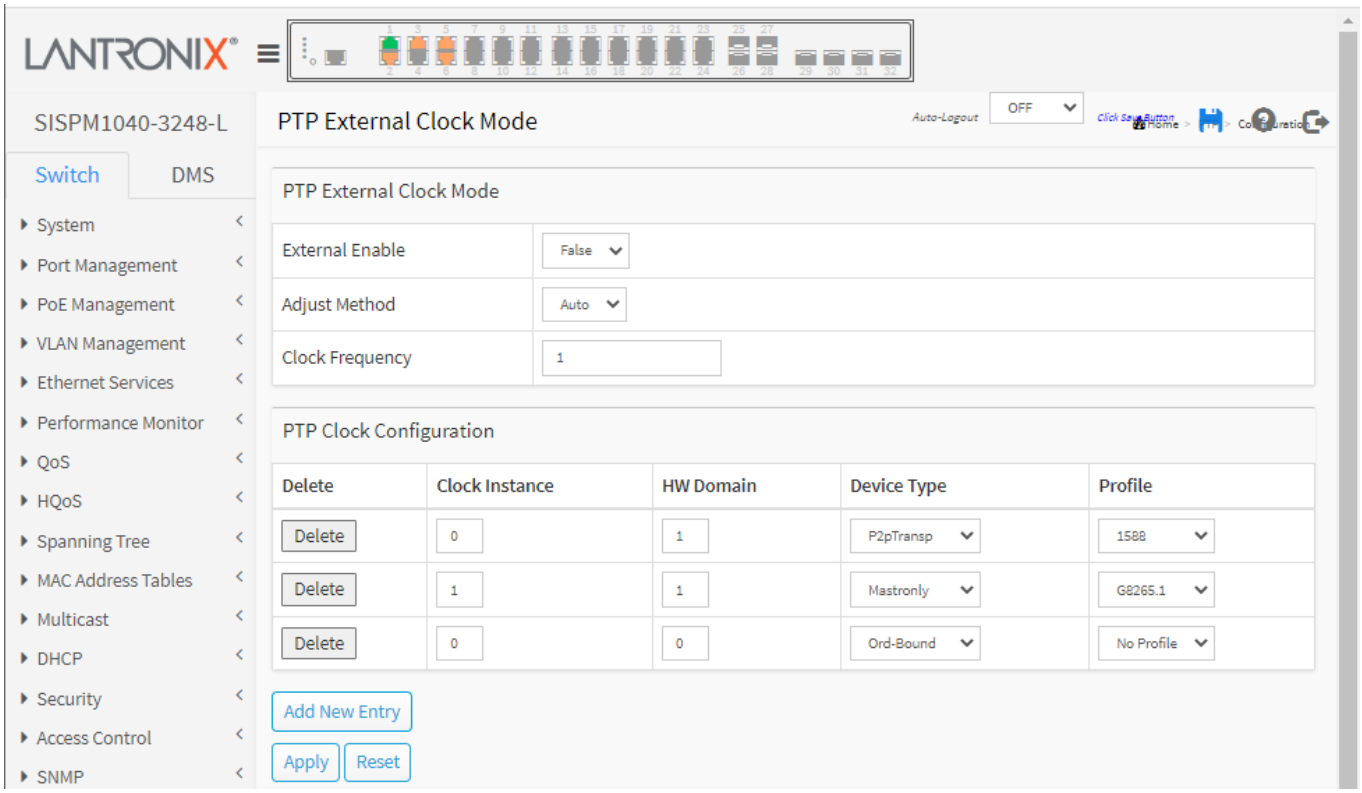


Figure 23-1: PTP Configuration

Parameter descriptions:

PTP External Clock Mode

External Enable : This selection box lets you configure the External Clock output. Possible values are:

True : Enable the external clock output.

False : Disable the external clock output.

Adjust Method : This selection box lets you configure the Frequency adjustment configuration.

LTC : Select Local Time Counter (LTC) frequency control.

Auto : AUTO Select clock control, based on PTP profile and available HW resources.

Clock Frequency : This sets the Clock Frequency. Possible values are 1 - 25000000 (1 - 25MHz).

PTP Clock Configuration

Delete : Check this box and click on 'Save' to delete the clock instance.

Clock Instance : Indicates the instance number of a particular Clock Instance [0..3]. Click on the Clock Instance number to edit the Clock details.

HW Domain : Indicates the HW clock domain used by the clock.

Device Type : Sets the Type of the Clock Instance. The Device Types are:

Inactive : clock's Device Type is Inactive.

Ord-Bound : clock's Device Type is Ordinary-Boundary Clock (default).

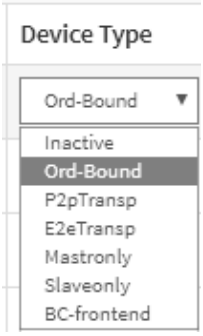
P2pTransp : clock's Device Type is Peer to Peer Transparent Clock.

E2eTransp : clock's Device Type is End to End Transparent Clock.

Mastronly : clock's Device Type is Master Only.

Slaveonly : clock's Device Type is Slave Only.

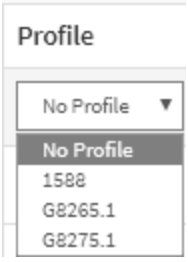
BC-frontend : clock's Device Type is BC Frontend.



Profile : Sets the profile used by the clock. The selections are:

No Profile : A profile is not yet defined. (default)

1588 : Sets the profile to the IEEE 1588 standard. “This standard defines a protocol enabling precise synchronization of clocks in measurement and control systems implemented with technologies such as network communication, local computing and distributed objects.”



G.8265.1 : Sets the profile to the ITU.T G.8265.1 : Precision time protocol telecom profile for frequency synchronization standard.

G.8275.1 : Sets the profile to the ITU.T G.8275.1 : Precision time protocol telecom profile for phase/time.

Buttons

Add New Entry : Click to add a new clock instance.

Apply : Click to save changes.

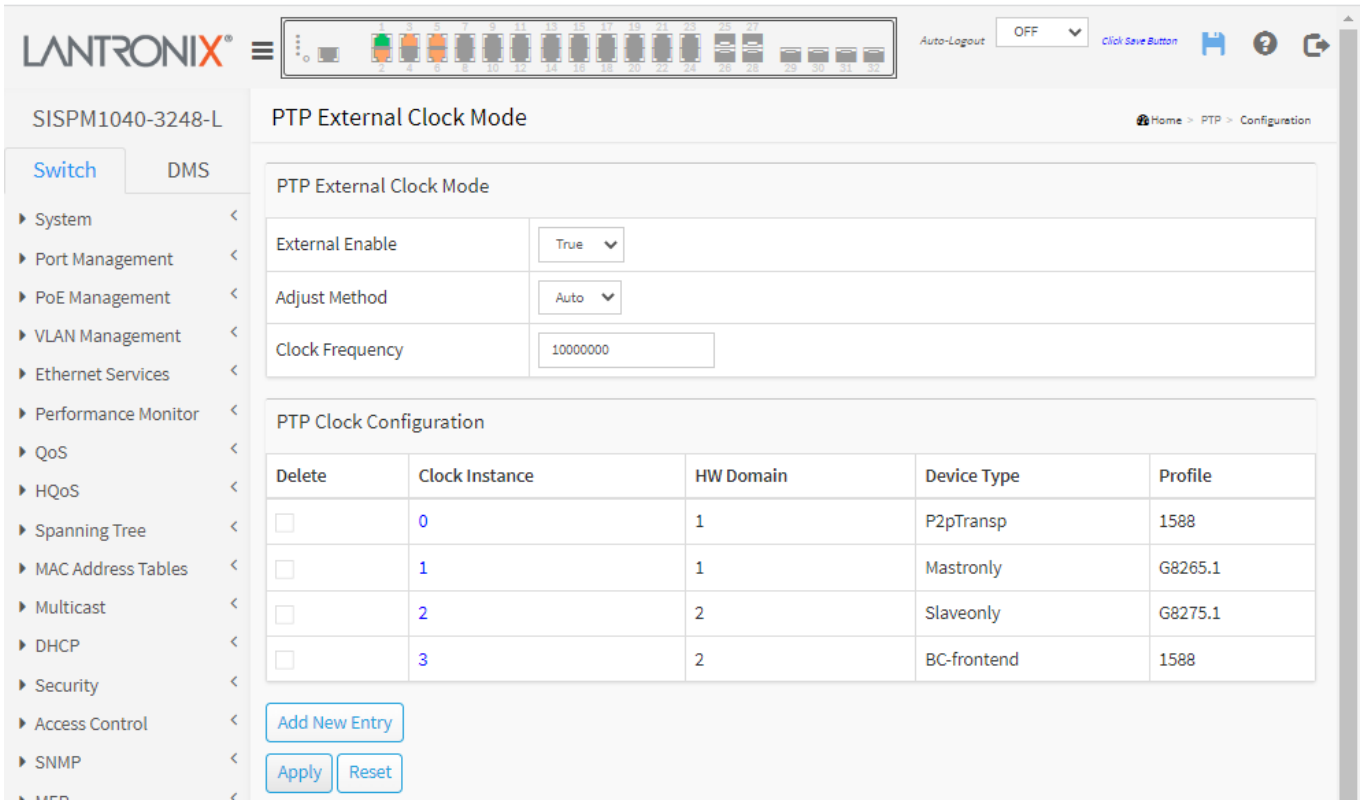
Reset : Click to undo any changes made locally and revert to previously saved values.

Messages:

Maximum of 4 clock instances can be created.

Cannot create more than one new clock with a given instance number

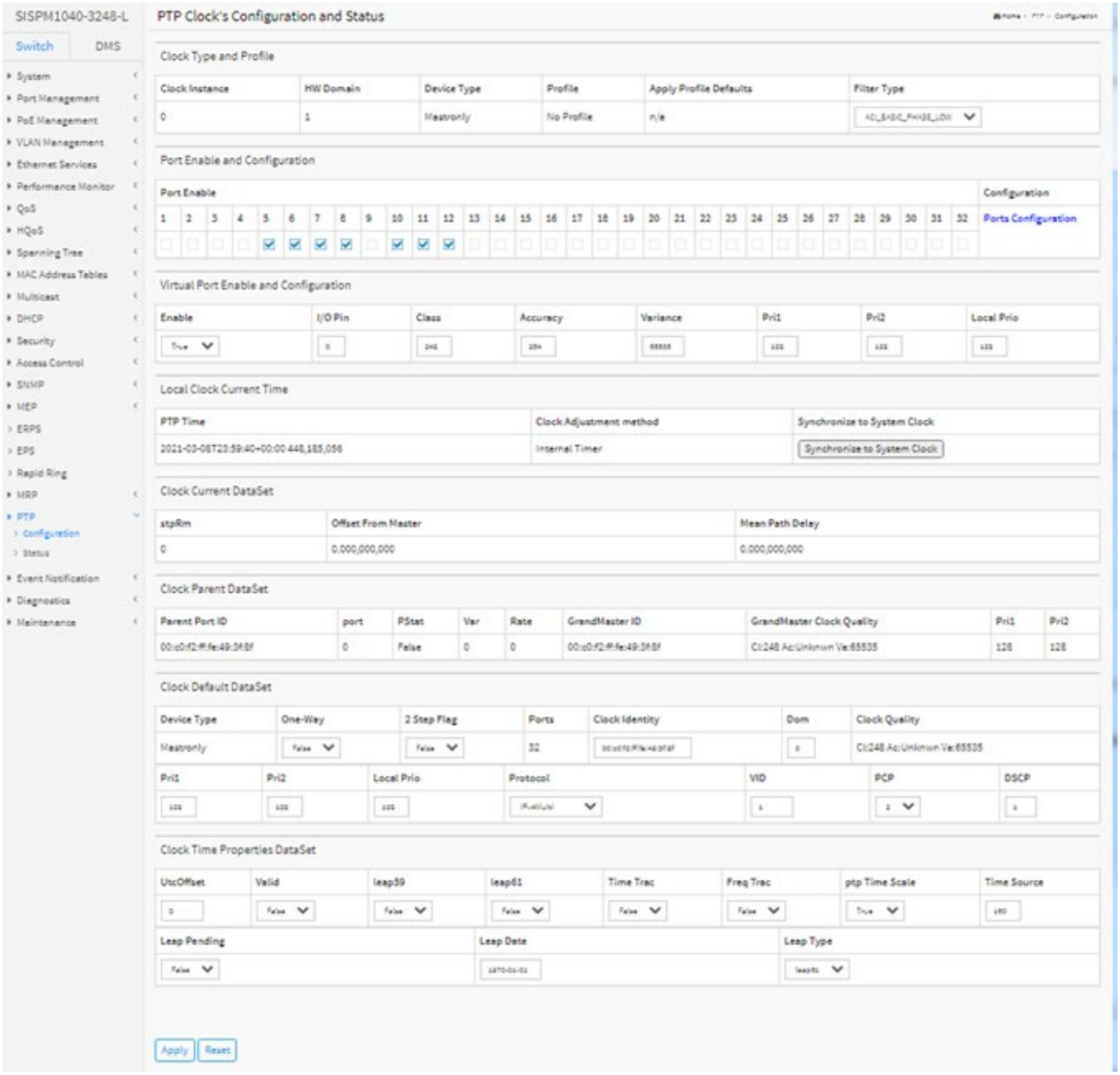
Example:



Click on a linked Clock Instance number to edit the Clock details as shown and described below.

Edit the Clock Details

The PTP Clock's Configuration and Status page displays when you click on a linked Clock Instance number. This page lets you edit the details of the selected Clock instance.



Parameter descriptions:

Clock Type and Profile

Clock Instance : Indicates the instance number of a particular Clock Instance [0..3].

HW Domain : Indicates the HW clock domain used by the clock.

Device Type : Indicates the Type of the Clock Instance. The Device Types include:

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.

Apply Profile Defaults : If the clock has been configured to use a profile, clicking the 'Apply' button will reset configured values to profile defaults.

Filter Type : The PTP filter type determines should match the operating conditions of the network and the PTP profile. Filter Types include:

PTP Profile	SyncE enabled (hybrid)	Filter Type	Description
1588	No	ACI_BASIC_PHASE	Requires PTP Sync and Delay_req frame rate of 16 fps or higher.
1588	Yes	ACI_BASIC_PHASE_SYNCE	Requires PTP Sync and Delay_req frame rate of 16 fps or higher.
1588	No	ACI_BASIC_PHASE_LOW	Use when the PTP Sync and Delay_req frame rate is between 1 fps to 16 fps.
1588	Yes	ACI_BASIC_PHASE_LOW_SYNCE	Use when the PTP Sync and Delay_req frame rate is between 1 fps to 16 fps.
None	No	ACI_BC_FULL_ON_PATH_FREQ	Used for Syntonized TC with basic filter.

Port Enable and Configuration

Port Enable : Set check mark for each port configured for this Clock Instance.

Configuration : Click the linked text 'Ports Configuration' to edit the port data set for the ports assigned to this clock instance.

Virtual Port Enable and Configuration

Enable : Disabled or Enabled.

I/O Pin : Virtual Port I/O Pin. The valid range is 0 to 3.

Class : Clock class value for clock as defined in IEEE Std 1588. The valid range is from 0 - 255.

Accuracy : Clock accuracy value as defined in IEEE Std 1588. The valid range is 0 - 255.

Variance : *offsetScaledLogVariance* for clock as defined in IEEE Std 1588. The valid range is 0 - 65535.

Pri1 : Clock priority 1 [0..255] used by the BMC master select algorithm.

Pri2 : Clock priority 2 [0..255] used by the BMC master select algorithm.

Local Prio : Priority [1..255]used in the 8275.1 BMCA.

Local Clock Current time : Show/update local clock data.

PTP Time : Shows the actual PTP time with nanosecond resolution.

Clock Adjustment Method : Shows the actual clock adjustment method. The method depends on the available hardware.

Synchronize to System Clock : Activate this button to synchronize the System Clock to PTP Time.

Clock Current Data Set : The clock current data set is defined in the IEEE 1588 Standard. The current data set is dynamic.

stpRm : Steps Removed : It is the number of PTP clocks traversed from the grandmaster to the local slave clock.

Offset From Master : Time difference between the master clock and the local slave clock, measured in ns.

Mean Path Delay : The mean propagation time for the link between the master and the local slave.

Clock Parent Data Set : The clock parent data set is defined in the IEEE 1588 standard. The parent data set is dynamic.

Parent Port ID : Clock identity for the parent clock, if the local clock is not a slave, the value is the clocks own id.

Port : Port Id for the parent master port.

PStat : Parents Stats (always false).

Var : It is observed parent offset scaled log variance.

Rate : Observed Parent Clock Phase Change Rate. i.e. the slave clocks rate offset compared to the master. (unit = nanoseconds per second).

Grand Master ID : Clock identity for the grand master clock, if the local clock is not a slave, the value is the clocks own ID.

Grand Master Clock Quality : The clock quality announced by the grand master (See description of Clock Default DataSet:Clock Quality).

Pri1 : Clock priority 1 announced by the grand master.

Pri2 : Clock priority 2 announced by the grand master.

Clock Default Dataset : The clock default data set is defined in the IEEE 1588 Standard. It holds three groups of data: the static members defined at clock creation time, the Dynamic members defined by the system, and the configurable members which can be set here.

Device Type : Indicates the Type of the Clock Instance. The Device Types include:

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.

One-Way : If true, one way measurements are used. This parameter applies only to a slave. In one-way mode no delay measurements are performed, i.e. this is applicable only if frequency synchronization is needed. The master always responds to delay requests.

2 Step Flag : True if two-step Sync events and Pdelay_Resp events are used.

Ports : The total number of physical ports in the node.

Clock Identity : Shows unique clock identifier.

Dom : Clock domain [0..127].

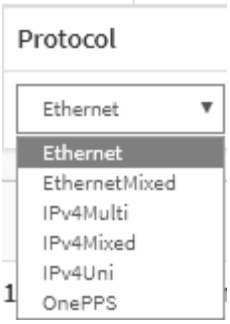
Clock Quality : The clock quality is determined by the system, and holds 3 parts: Clock Class, Clock Accuracy and OffsetScaledLog Variance as defined in IEEE1588. The Clock Accuracy values are defined in IEEE1588 table 6 (Currently the clock Accuracy is set to 'Unknown' as default).

Pri1 : Clock priority 1 [0..255] used by the BMC master select algorithm.

Pri2 : Clock priority 2 [0..255] used by the BMC master select algorithm.

Local Prio : Priority [1..255] used in the 8275.1 BMCA.

Protocol : The Transport protocol used by the PTP protocol engine:



Ethernet : PTP over Ethernet multicast.

EthernetMixed : PTP using a combination of Ethernet multicast and unicast.

IPv4Multi : PTP over IPv4 multicast.

IPv4Mixed : PTP using a combination of IPv4 multicast and unicast.

IPv4Uni : PTP over IPv4 unicast.

OnePPS : Use one pps protocol.

VID : VLAN Identifier used for tagging the VLAN packets.

PCP : Priority Code Point value used for PTP frames.

DSCP : DSCP value used when transmitting IPv4 encapsulated packets.

Clock Time Properties Data Set : The clock time properties data set is defined in the IEEE 1588 Standard. The data set is both configurable and dynamic, i.e. the parameters can be configured for a grandmaster. In a slave clock the parameters are overwritten by the grandmasters timing properties. The parameters are not used in the current PTP implementation. The valid values for the Time Source parameter are:

16 (0x10) ATOMIC_CLOCK

32 (0x20) GPS

48 (0x30) TERRESTRIAL_RADIO

64 (0x40) PTP

80 (0x50) NTP

96 (0x60) HAND_SET

144 (0x90) OTHER

160 (0xA0) INTERNAL_OSCILLATOR

UtcOffset : In systems whose epoch is UTC, it is the offset between TAI and UTC.

Valid : When true, the value of *currentUtcOffset* is valid

leap59 : When true, this field indicates that last minute of the current UTC day has only 59 seconds.

leap61 : When true, this field indicates that last minute of the current UTC day has 61 seconds.

Time Trac : True if the timescale and the value of *currentUtcOffset* are traceable to a primary reference.

Freq Trac : True if the frequency determining the timescale is traceable to a primary reference.

ptp Time Scale : True if the clock timescale of the grandmaster clock and false otherwise.

Time Source : The source of time used by the grandmaster clock.

Leap Pending : When true, there is a leap event pending at the date defined by *leapDate*.

Leap Date : The date for which the leap will occur at the end of its last minute. Date is represented as the number of days after 1970-01-01 (the latter represented as 0).

Leap Type : The type of leap event (i.e., leap59 or leap61).

Unicast Slave Configuration : When operating in IPv4 Unicast mode, the slave is configured up to 5 master IP addresses. The slave then requests Announce messages from all the configured masters. The slave uses the BMC algorithm to select one as master clock, the slave then requests Sync messages from the selected master.

Duration : The number of seconds a master is requested to send Announce/Sync messages. The request is repeated from the slave each Duration/4 seconds.

ip_address : The IPv4 Address of the Master clock .

grant : The granted repetition period for the sync message.

CommState : The state of the communication with the master, possible values are:

IDLE : The entry is not in use.

INIT : Announce is sent to the master (Waiting for a response).

CONN : The master has responded.

SELL : The assigned master is selected as current master.

SYNC : The master is sending Sync messages.

Buttons

Apply : Click to save changes.

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

Ports Configuration

When you click 'Ports Configuration' (on the PTP Clock's Configuration and Status page) the Ports Configuration page displays as shown and described below. Note that an empty table displays if you have not configured any ports yet.

The port data set is defined in the IEEE 1588 Standard. It holds three groups of data: the static members, the dynamic members, and configurable members which can be set here.

Parameter descriptions :

Port DataSet

Port : Static member port Identity : Port number [1..max port no]

Stat : Dynamic member portState: Current state of the port.

MDR : Dynamic member log Min Delay Req Interval: The delay request interval announced by the master.

Peer Mean Path Del : The path delay measured by the port in P2P mode. In E2E mode this value is 0.

Anv : The interval for issuing announce messages in master state. Range is -3 to 4.

ATo : The timeout for receiving announce messages on the port. Range is 1 to 10.

Syv : The interval for issuing sync messages in master. Range is -7 to 4.

Dlm : Configurable member delayMechanism: The delay mechanism used for the port:

e2e : End to end delay measurement

p2p : Peer to peer delay measurement.

DLM can be defined per port in an Ordinary/Boundary clock. In a transparent clock all ports use the same delay mechanism, determined by the clock type.

MPR : The interval for issuing Delay_Req messages for the port in E2E mode. This value is announced from the master to the slave in an announce message. The value is reflected in the MDR field in the Slave. The interval for issuing Pdelay_Req messages for the port in P2P mode. **Note**: The interpretation of this parameter has changed from release 2.40. In earlier versions the value was interpreted relative to the Sync interval, this was a violation of the standard, so now the value is interpreted as an interval (i.e., *MPR=0 => 1 Delay_Req pr sec*) independent of the Sync rate. Range is -7 to 5.

Delay Asymmetry : If the transmission delay for a link in not symmetric, the asymmetry can be configured here, see IEEE 1588 Section 7.4.2 Communication path asymmetry. Range is -100000 to 100000.

Version : The current implementation only supports PTP version 2.

Ingress latency : Ingress latency measured in ns, as defined in IEEE 1588 Section 7.3.4.2. Range is -100000 to 100000.

Egress Latency : Egress latency measured in ns, as defined in IEEE 1588 Section 7.3.4.2. Range is -100000 to 100000.

Version : PTP version used by this port.

Mcast Addr : Configured destination address for multicast packets (PTP ***Default*** or ***LinkLocal***).

Not Slave : TRUE indicates that this interface cannot enter slave mode.

Local Prio : 1-255, priority used in the 8275.1 BMCA.

2 Step Flag : Option to override the 2-step option on port level. The IEEE 802.1AS specific parameters are only available when the 802.1AS profile is selected.

Buttons

Apply : Click to save changes.

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

Messages:

Announce Interval must be an integer value between -3 and 4

Announce Receive Timeout must be an integer value between -1 and 10

Mininum Delay Required Interval must be an integer value between -7 and 5

Sync Interval must be an integer value between -7 and 4

Ingress Latency must be an integer value between -100000 and 100000

24-2 Status

This page lets you view current PTP clock settings. To display current PTP status in the web UI:

1. Click PTP and Status.
2. View the PTP parameters.
3. Click Apply to apply (save) the changes.

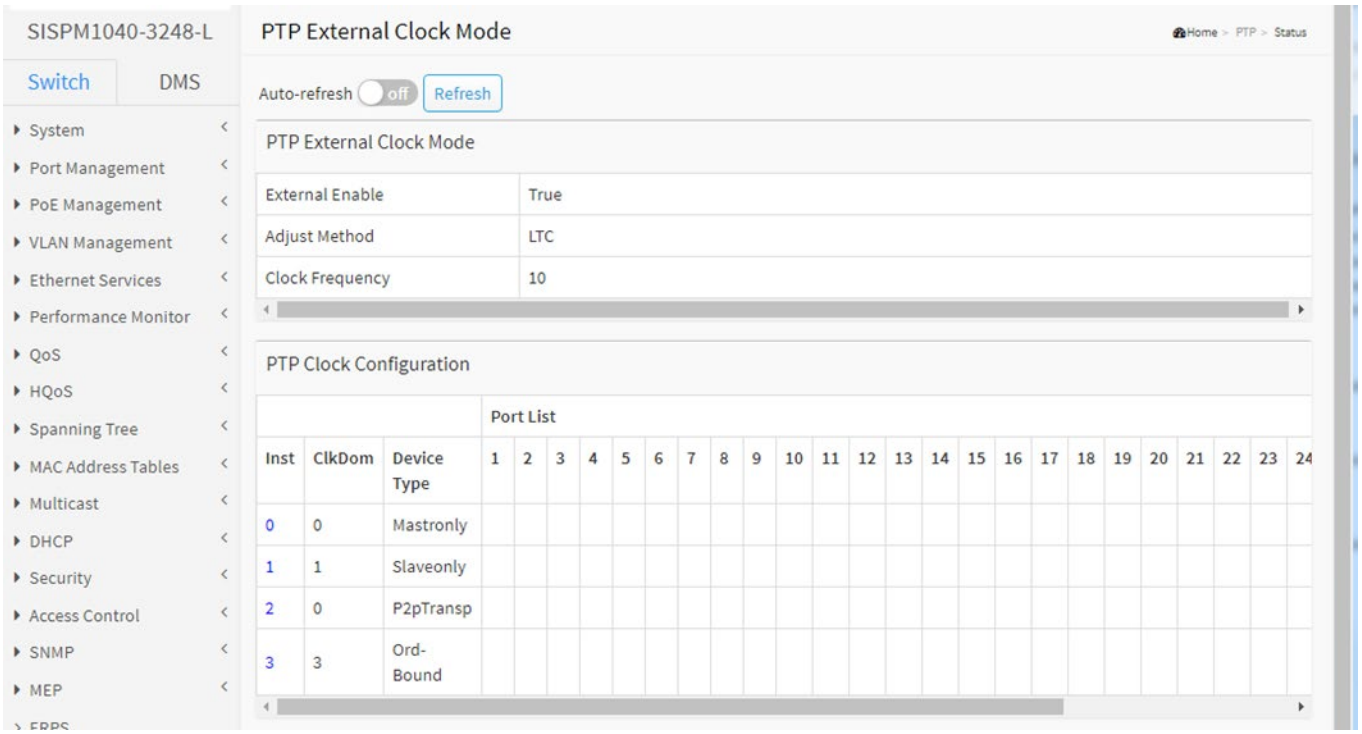


Figure 23-2: PTP Status

Parameter descriptions:

PTP External Clock Mode

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.

Auto : Switch automatically selects clock control, based on PTP profile and available HW resources.

Clock Frequency : Shows the current clock frequency used by the External Clock. Possible values are 1 - 25000000 (1 - 25MHz). The default is 10 MHz.

PTP Clock Configuration

Inst : Indicates the Instance of a particular Clock Instance [0..3]. Click on the Clock Instance number to monitor the Clock details.

ClkDom : Indicates the Clock domain used by the Instance of a particular Clock Instance [0..3].

Device Type : Indicates the Type of the Clock Instance. The Device Types include:

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 each Clock Instance configured.

Buttons

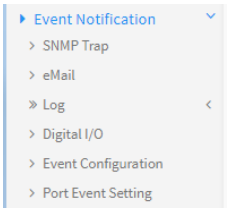
Auto-refresh : Click to refresh the page automatically every 3 seconds.

Refresh : Click to manually refresh the page immediately.

Apply : Click to save changes.

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

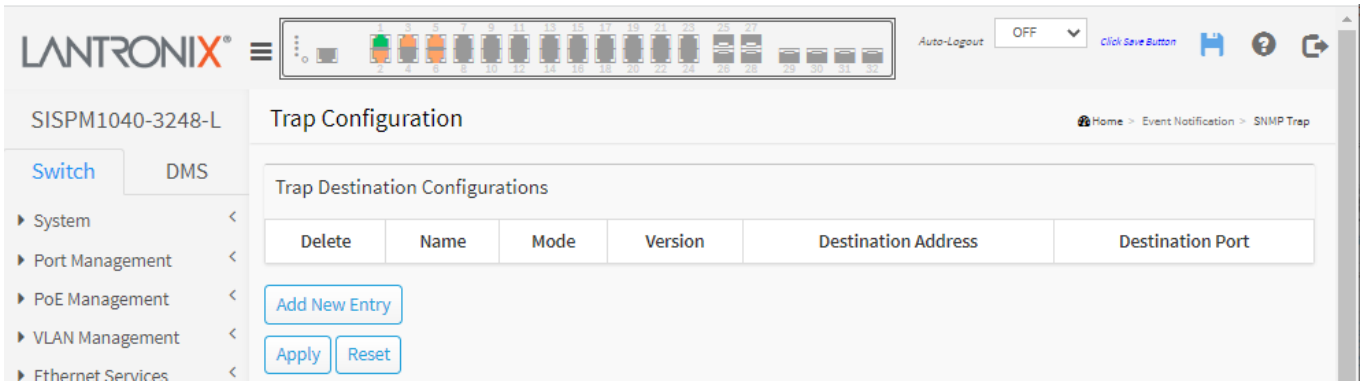
Chapter 25 - Event Notification



25-1 SNMP Trap

Configure SNMP Traps on this page. To configure SNMP Traps 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.

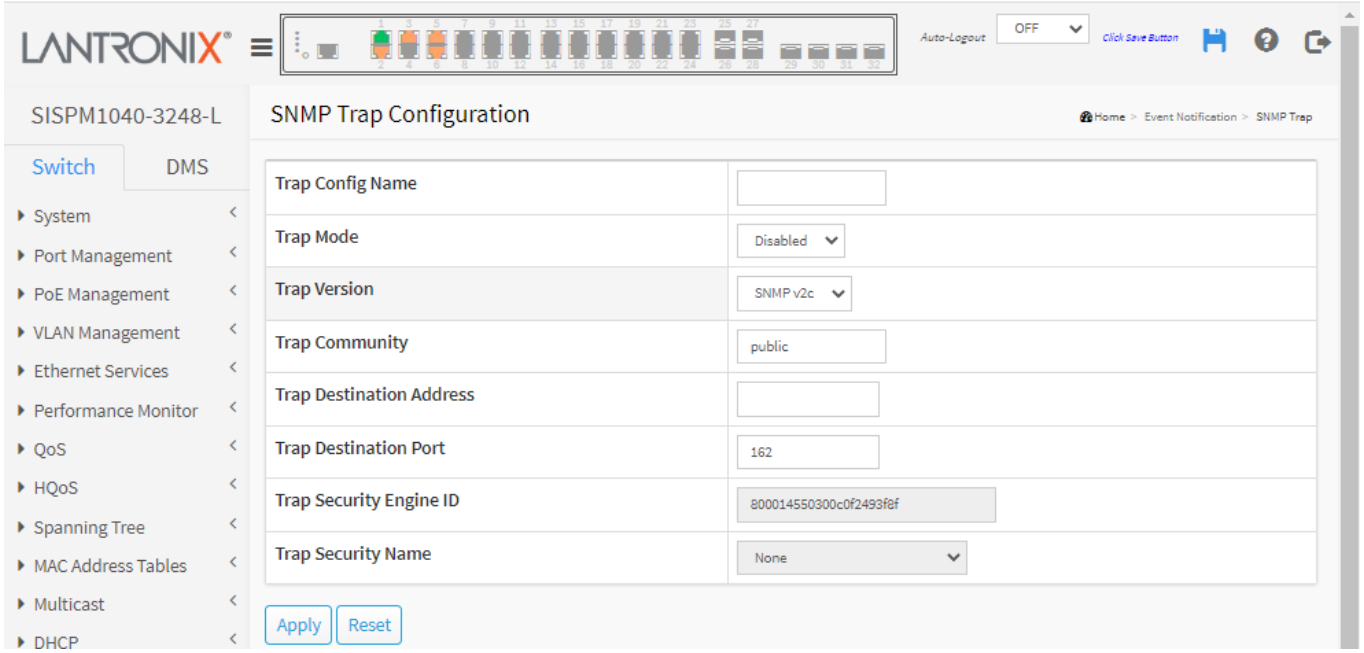
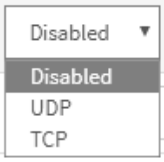


Figure 25-1: SNMP Trap Configuration

Parameter descriptions:

Trap Config Name : Indicates which trap Configuration's name for configuring. The allowed string length is 1 – 32 characters, and the allowed content is ASCII characters 33 - 126.

Trap Mode : Indicates the SNMP mode operation. Possible modes are:

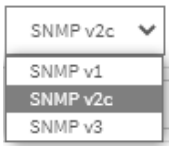


Disabled: Disable SNMP mode operation.

UDP: Use UDP as the SNMP mode operation.

TCP: Use TCP as the SNMP mode operation.

Trap Version : Indicates the SNMP supported version. Possible versions are:



SNMP v1: Set SNMP supported version 1.

SNMP v2c: Set SNMP supported version 2c.

SNMP v3: Set SNMP supported version 3.

Trap Community : Indicates the community access string when sending SNMP trap packet. The allowed string length is 0 to 63 characters, and the allowed content is ASCII characters from 33 to 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. The SNMP Agent will send SNMP messages via this port, the port range is 1~65535.

Trap Security Engine ID : Indicates the SNMP trap security engine ID. SNMPv3 sends traps and informs using USM for authentication and privacy. A unique engine ID for these traps and informs is needed. When "Trap Probe Security Engine ID" is enabled, the ID will be probed automatically. Otherwise, the ID specified in this field is used. The string must contain an even number (in hexadecimal format) with number of digits between 10 and 64, but all-zeros and all-'F's are not allowed.

Trap Security Name : Indicates the SNMP trap security name. SNMPv3 traps and informs using USM for authentication and privacy. A unique security name is needed when traps and informs are enabled.

Buttons

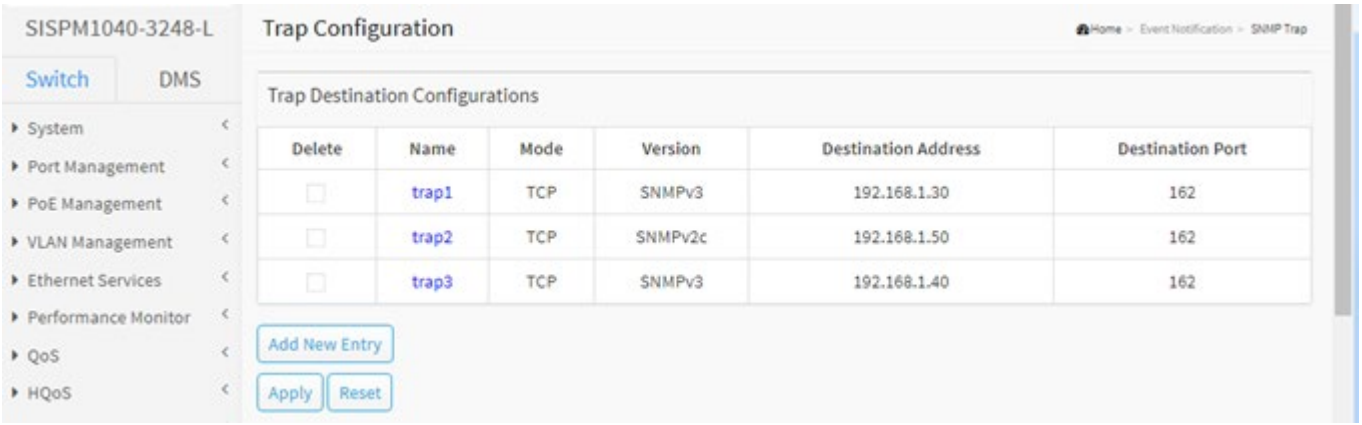
Add New Entry : Click to add a new entry.

Apply : Click to save changes. After saving configuration, remember to select the correct trap security name.

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

After you click Apply to save the changes, the page displays with the Trap Destination Configurations table as shown and described below.

Trap Destination Configurations table



Parameter descriptions:

Name : Indicates the trap Configuration's name.

Mode : Indicates the trap destination mode operation. Possible modes are:

Disabled: SNMP mode is Disabled.

UDP: UDP used as the SNMP mode operation.

TCP: TCP used as the SNMP mode operation.

Version : Indicates the SNMP trap supported version. Possible versions are:

SNMPv1: Set SNMP trap supported version 1.

SNMPv2c: Set SNMP trap supported version 2c.

SNMPv3: Set SNMP trap supported version 3.

Destination Address : Indicates the SNMP trap destination address. It 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.

It 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 valid IPv4 address (e.g., '::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.

Messages:

Message: *The value of 'Trap Destination Address' is 0.0.0.0. Do you want to proceed anyway?*

Message: *After saving configuration, remember select the correct trap security name.*

25-2 eMail

Configure SMTP (Simple Mail Transfer Protocol) on this page. SMTP is the message-exchange standard for the Internet. The switch is to be configured as a client of SMTP while the server is a remote device that will receive messages from the switch that alarm events occurred.

To configure SMTP Configuration in the web UI:

1. Click Event Notification and eMail.
2. Specify the SMTP Configuration parameters.
3. Click Apply.

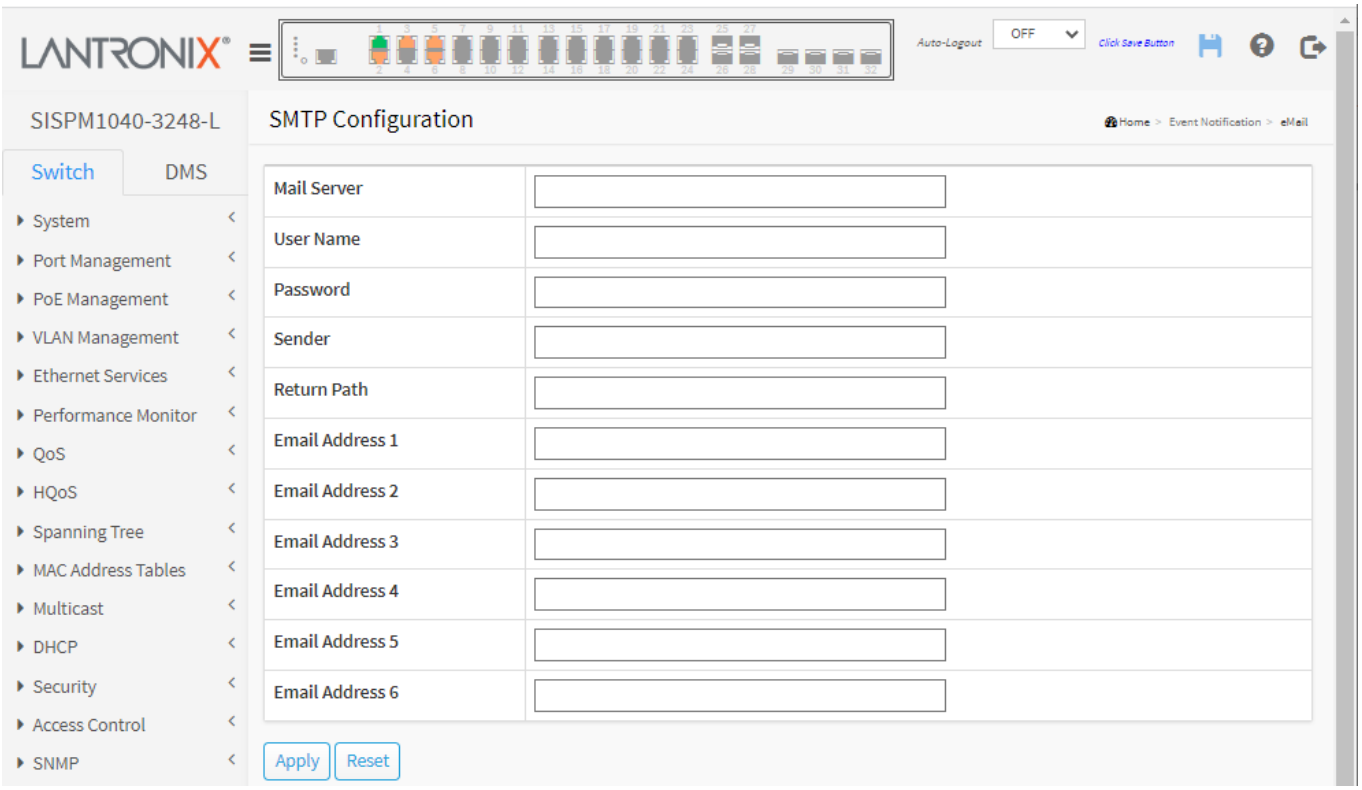


Figure 25-2: SMTP Configuration

Parameter descriptions:

Mail Server : The IP address or hostname of the mail server. IP address is expressed in dotted decimal notation. This will be the device that sends out the mail.

User Name : Specify the username on the mail server.

Password : Specify the password of the user on the mail server.

Sender : Specify the sender name of the alarm mail.

Return Path : Specify the sender email address of the alarm mail. This address will be the "from" address on the email message.

Email Address # : Specify 1-6 email addresses of the receiver(s).

Buttons

Apply : Click to save changes.

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

25-3 Log

25-3.1 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 be used as well a generalized informational, analysis and debugging messages. It is supported by a wide variety of devices and receivers across multiple platforms.

To configure Syslog parameters in the web UI:

1. Click Event Notification, Log, and Syslog.
2. Set Server Mode to **on** to enable it.
3. Specify the syslog parameters Server Address and Server Port.
4. Click Apply.

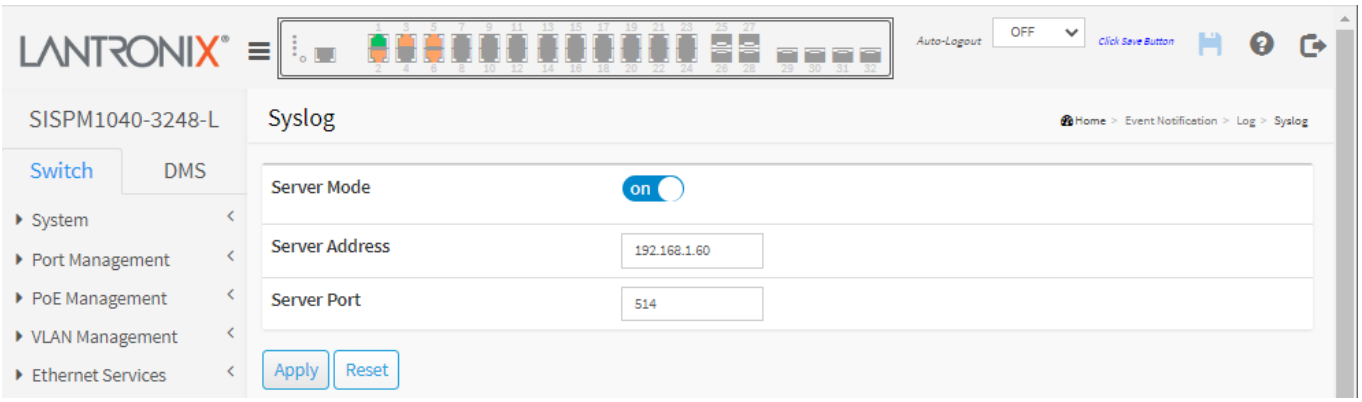


Figure 25-3.1: Syslog configuration

Parameter descriptions:

Server Mode : Indicates the server mode of operation. When the mode operation is *on*, the syslog message will send out to syslog server. The syslog protocol is based on UDP communication and received on UDP port 514 and the syslog server will not send acknowledgments back sender since UDP is a connectionless protocol and it does not provide acknowledgments. The syslog packet is always sent out even if the syslog server does not exist. Possible modes:

on: Enable server mode operation.

off: Disable server mode operation.

Server Address : Indicates the IPv4 host address of the syslog server. If the switch provides a DNS feature, it can also 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.

25-3.2 View Log

This page displays the system log information of the switch. To display log Information in the web UI:

1. Click Event Notification, Log, and View Log.
2. View the log information.
3. View the Do Relay Status, and apply the Do Relay Alarm Cut-off as desired.

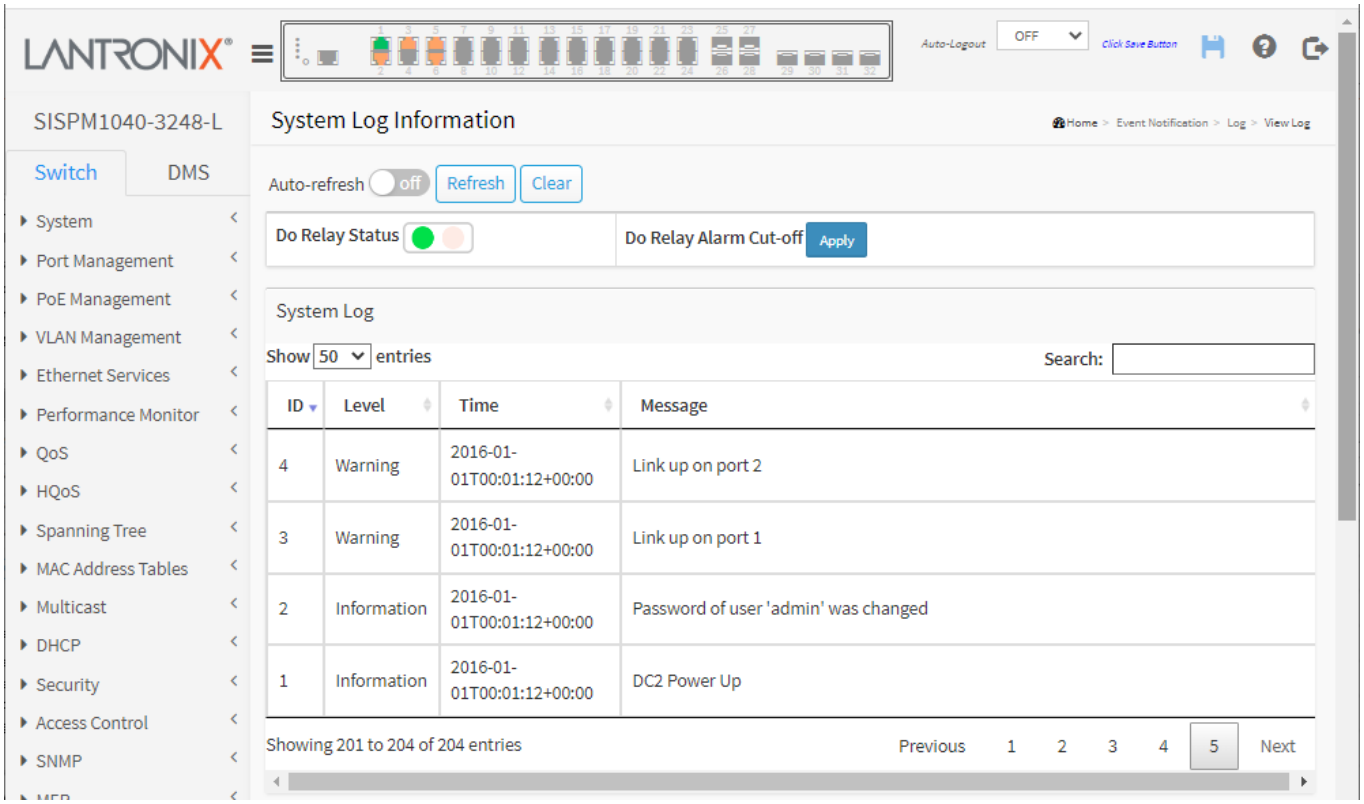


Figure 25-3.2: System Log

Parameter descriptions:

Do Relay Status : Shows the status of digital-out relay contact.

Do Relay Alarm Cut-off : Click Apply to force cut off the digital-out relay contact.

ID : The ID of the system log entry.

Level : level of the system log entry. These level types are supported:

Debug : debug level message.

Information : informational message.

Notice : normal, but significant, condition.

Warning : warning condition.

Error : error condition.

Critical: critical condition.

Alert : action must be taken immediately.

Emergency : 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 of the system log entry.

Buttons

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

Refresh : Updates the table entries, starting from the current entry.

Clear: Flushes the selected entries.

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

Previous : Updates the system log entries, turn to the previous page.

Show entries :Dropdown to select how may entries to show per page (10, 25, 50, or 100).

Search : Search box to enter a keyword and display all message entries containing that keyword.

Syslog Entry Examples

ID	Level	Time	Message
461	Notice	2019-09-17T03:52:46+00:00	LINK-UPDOWN: Interface Vlan 1, changed state to up.
460	Information	2019-09-17T03:52:42+00:00	topologyChange
459	Notice	2019-09-17T03:52:40+00:00	LINK-UPDOWN: Interface Vlan 1, changed state to down.
458	Information	2019-09-17T03:52:38+00:00	topologyChange
457	Warning	2019-09-17T02:57:04+00:00	PoE Auto Power Reset Reboot PD Failure, Port 3, IP: 192.168.1.99
456	Information	2019-09-17T02:43:22+00:00	DMS: Device (169.254.11.169) Off-line caused by network disconnection.
455	Information	2019-09-17T02:42:59+00:00	LACP was enabled on port 13 with key 0
462	Warning	2019-09-17T05:53:33+00:00	DI 1 change to normal

25-4 Digital I/O

Configure the normal modes of digital input/output (DI/DO). See the *Install Guide* for DI/DO hardware information.

To configure the digital input/output:

1. Click Event Notification and Digital I/O.
2. Select DI Normal Mode and DO Normal Mode.
3. Click the Apply button to save the setting.

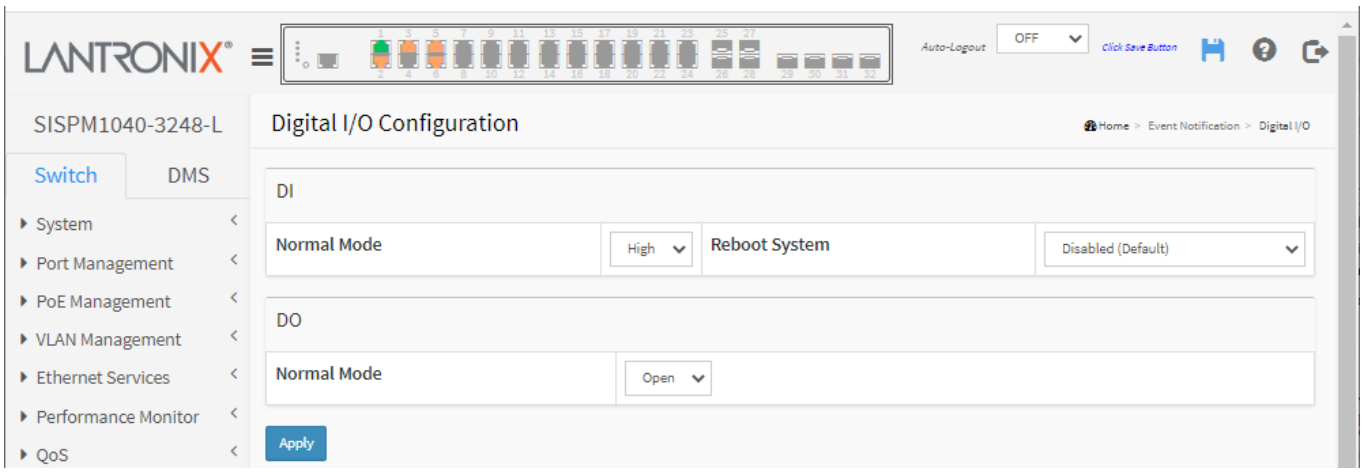


Figure 25-4: Digital I/O Configuration

Parameter descriptions:

DI Normal Mode: Set the normal mode of the digital input (DI). You can set it to ***High*** or ***Low***. The default is ***High***.

Reboot System: Set the reboot system of the digital input(DI). The default setting is Disabled (no reboot system action taken). You can set it to "When DI was changed to abnormal" to reboot the switch when DI input goes High. The default setting is Disabled. Added at FW v 7.50.0111.

DO Normal Mode: Set the normal mode of the digital output (DO). You can set it to ***Open*** or ***Close***. The default is ***Open***.

Buttons

Apply: Click to save changes.

Message: A syslog Warning is issued indicating, for example, "*DI 1 change to normal*".

25-5 Event Configuration

This page lets you view and set current trap event severity parameters.

To configure Trap Event Severity via the web UI:

1. Click Event Notification and Event Configuration.
2. For Group Name(s) select a Severity Level.
3. Check the desired checkbox(es) to enable different trap events.
4. Click the Apply button to save the settings.

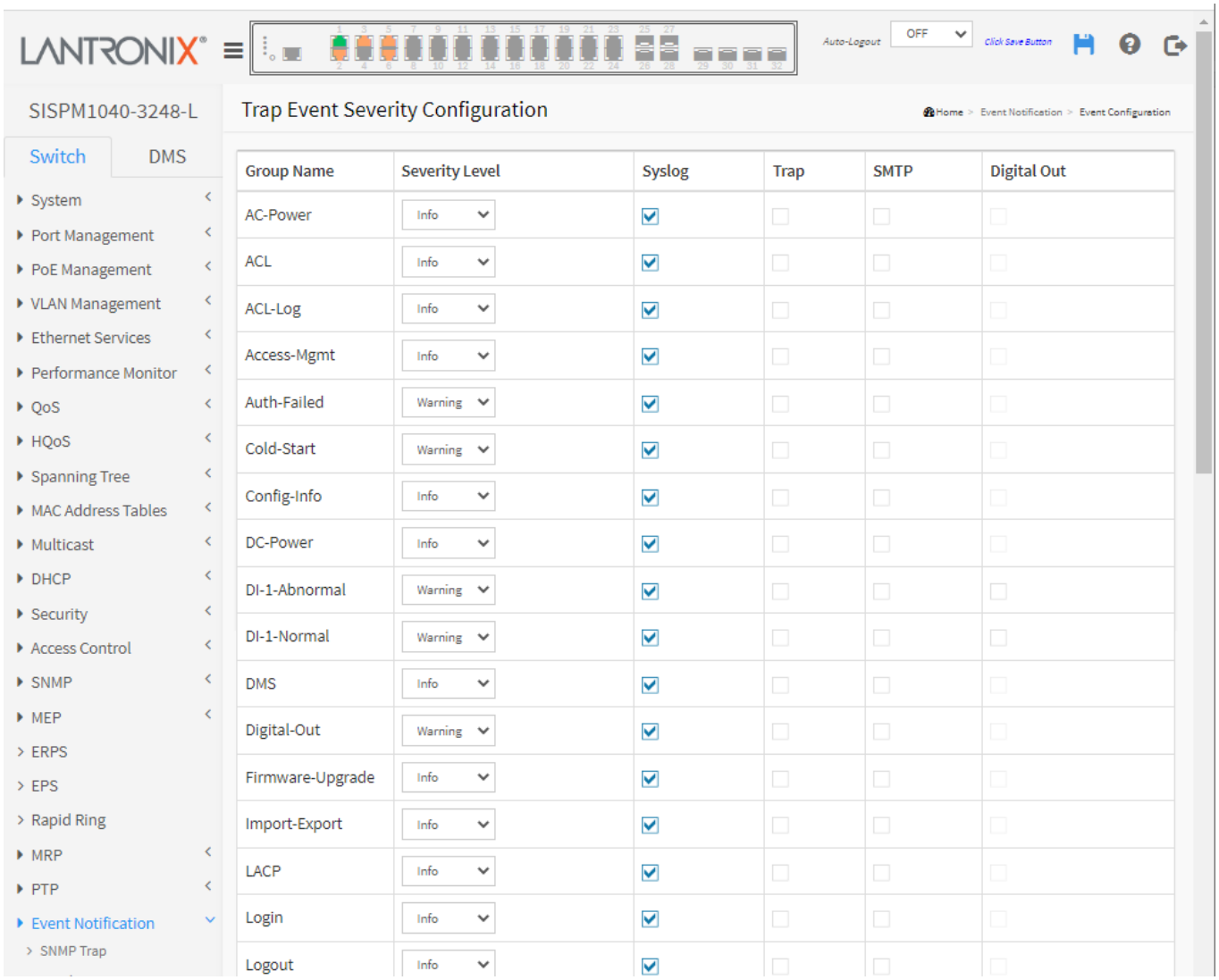


Figure 25-5: Trap Event Severity Configuration

Parameter descriptions:

Group Name : The name identifying the severity group.

Severity Level : Every group has a severity level. The following level types are supported:

Emerg: Emergency; System is unusable.
Alert: Action must be taken immediately.
Crit*:* Critical conditions.
Error: Error conditions.
Warning: Warning conditions.
Notice: Normal but significant conditions.
Info: Information messages.
Debug: Debug-level messages.

Syslog : Check this Group Name in the Syslog column.

Trap : Check this Group Name in the Trap column.

SMTP : Check this Group Name for email event notifications.

Digital Out : Check this Group Name in the Digital Out column.

Buttons

Apply : Click to save changes.

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

25-6 Port Event Setting

This page is for configuring port events. To configure Port Events via the web UI:

1. Click Event Notification and Port Event Setting.
2. Set the Port Event Link, Traffic, and Action section parameters.
3. Click the Apply button to save the settings.

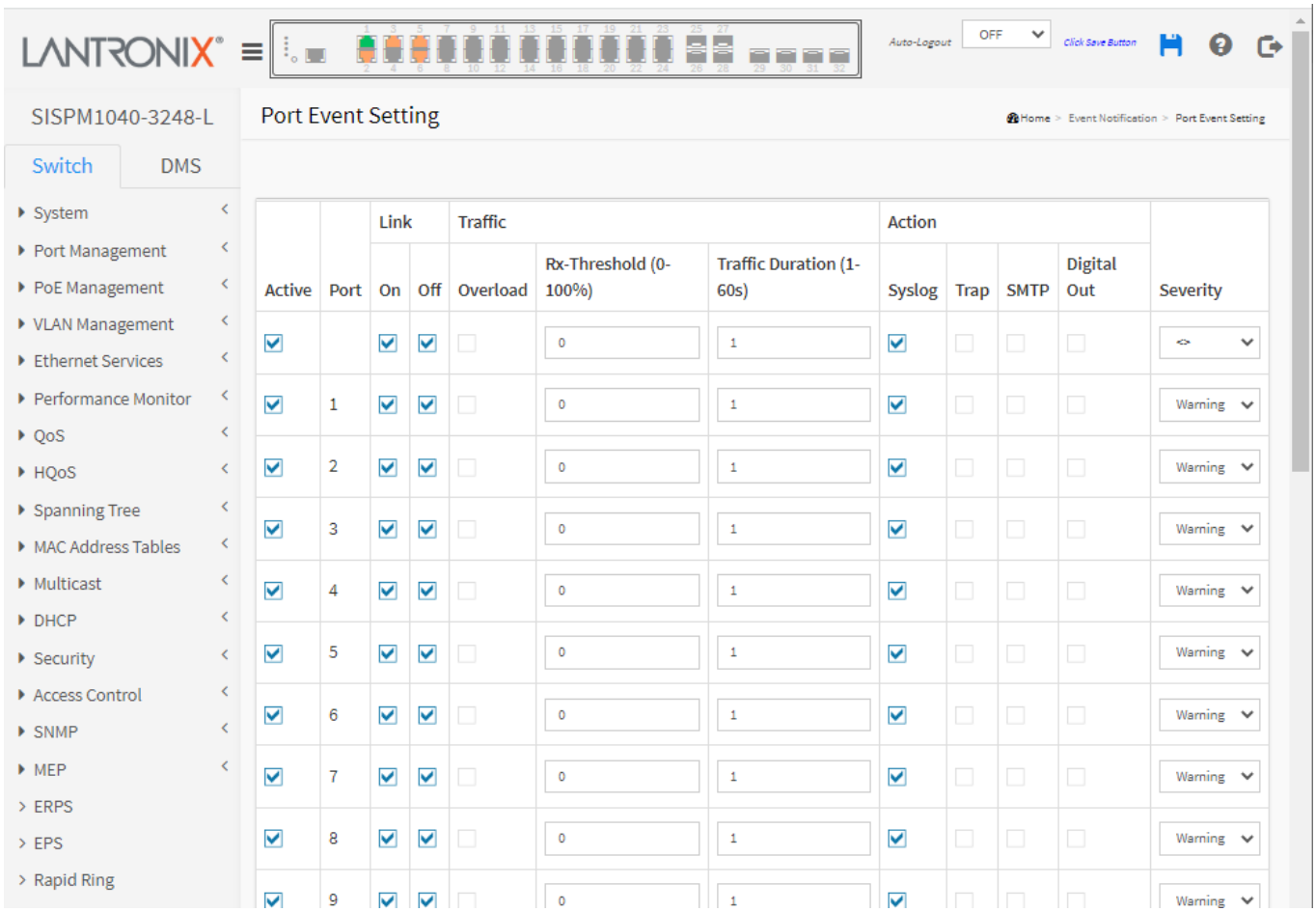


Figure 25-5: Port Event Setting

Parameter descriptions:

Active : Check to active the event handler of this port.

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

Link On : Event is triggered when link on.

Link Off : Event is triggered when link off.

Traffic Overload : Event is triggered when the traffic is overloaded.

Traffic Rx-Threshold (0-100%): Event is triggered when Rx reaches this threshold.

Traffic Duration (1-60s) : Event is triggered when the traffic duration reaches this value.

Action Syslog : Enable this port for Syslog. This is enabled for all ports by default.

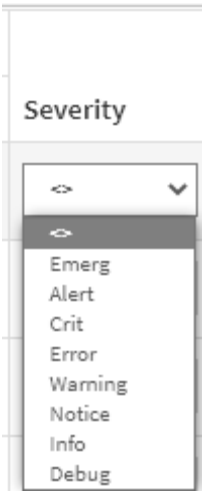
Action Trap : Enable this port for Trap.

Action SMTP : Enable this port for SMTP.

Action Digital Out : Enable this port for Digital Output.

Severity : Every port has a severity level setting. The following level types are supported:

Emerg: Emergency; System is unusable.
Alert: Action must be taken immediately.
Crit: Critical conditions.
Error: Error conditions.
Warning: Warning conditions.
Notice: Normal but significant conditions.
Info: Information messages.
Debug: Debug-level messages.



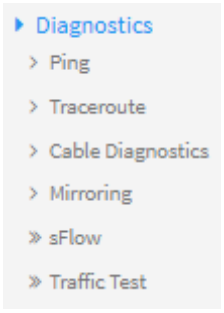
The default level is ***Warning***.

Buttons

Apply : Click to apply changes.

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

Chapter 26 - Diagnostics



This section provides a set of system diagnostics including Ping, Traceroute, Cable Diagnostics, Mirroring, sFlow, and Traffic Test.

26-1 Ping

This page lets you issue ICMP Echo packets to troubleshoot IPv4 or IPv6 connectivity issues.

To configure a Ping via the web UI:

1. Click Diagnostics and Ping.
2. Specify IP Address, Ping Length, Ping Count, Ping Interval, and Egress Interface.

Figure 26-1: ICMP Ping

3. Click 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 data space (the ICMP header). The page refreshes automatically until responses to all packets are received, or until a timeout occurs.

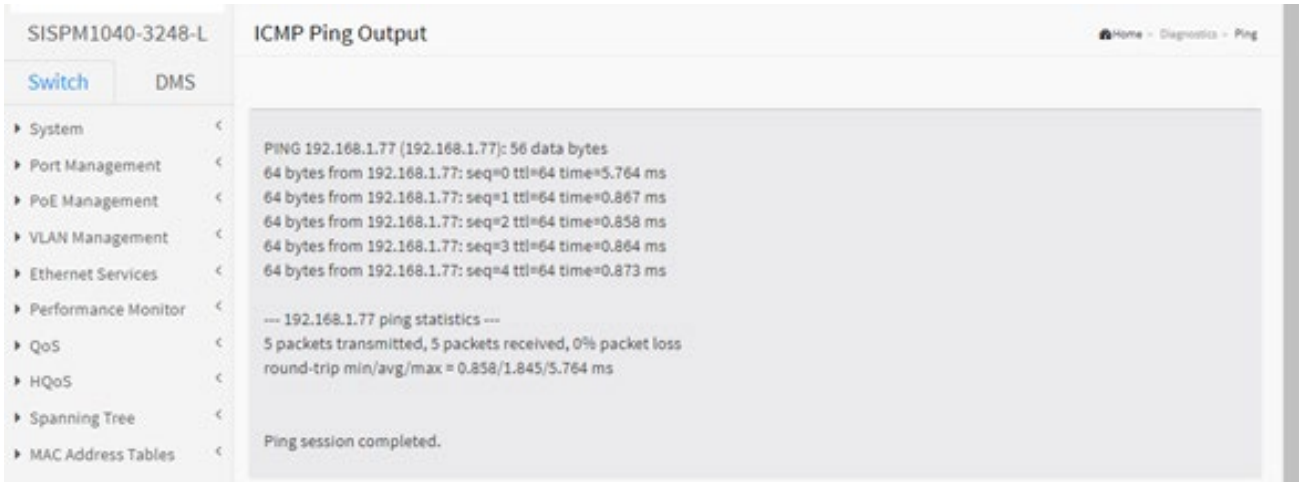


Figure 26-2: ICMP Ping Output

Parameter descriptions:

IP Address : Specify the target IP Address of the Ping.

Ping Length : The payload size of the ICMP packet. Valid values are 2 - 1452 bytes.

Ping Count : The count of the ICMP packet. Valid values are 1 - 60 times.

Ping Interval :The interval of the ICMP packet. Valid values are 0 - 30seconds.

Egress Interface (Only for IPv6) : The VLAN ID (VID) of the specific egress IPv6 interface where the ICMP packet goes. Valid VID ranges from 1 to 4094 and will be effective only when the corresponding IPv6 interface is valid. When the egress interface is not given, PING6 finds the best match interface for destination.
Do not specify egress interface for loopback address.
Do specify egress interface for link-local or multicast addresses.

Buttons

Start :Click the button to start to ping the target IP Address.

New Ping : Back to ICMP Ping page.

Sample Ping Output:

```
ICMP Ping Output

PING 192.168.1.77 (192.168.1.77): 56 data bytes
64 bytes from 192.168.1.77: seq=0 ttl=64 time=5.764 ms
64 bytes from 192.168.1.77: seq=1 ttl=64 time=0.867 ms
64 bytes from 192.168.1.77: seq=2 ttl=64 time=0.858 ms
64 bytes from 192.168.1.77: seq=3 ttl=64 time=0.864 ms
64 bytes from 192.168.1.77: seq=4 ttl=64 time=0.873 ms

--- 192.168.1.77 ping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max = 0.858/1.845/5.764 ms


Ping session completed.
```

26-2 Traceroute

This page lets you issue ICMP packets to diagnose network connectivity issues. To start a Traceroute in the web UI:

1. Click Diagnostics and Traceroute.
2. Specify IP Address, Wait Time, Max TTL, and Probe Count.

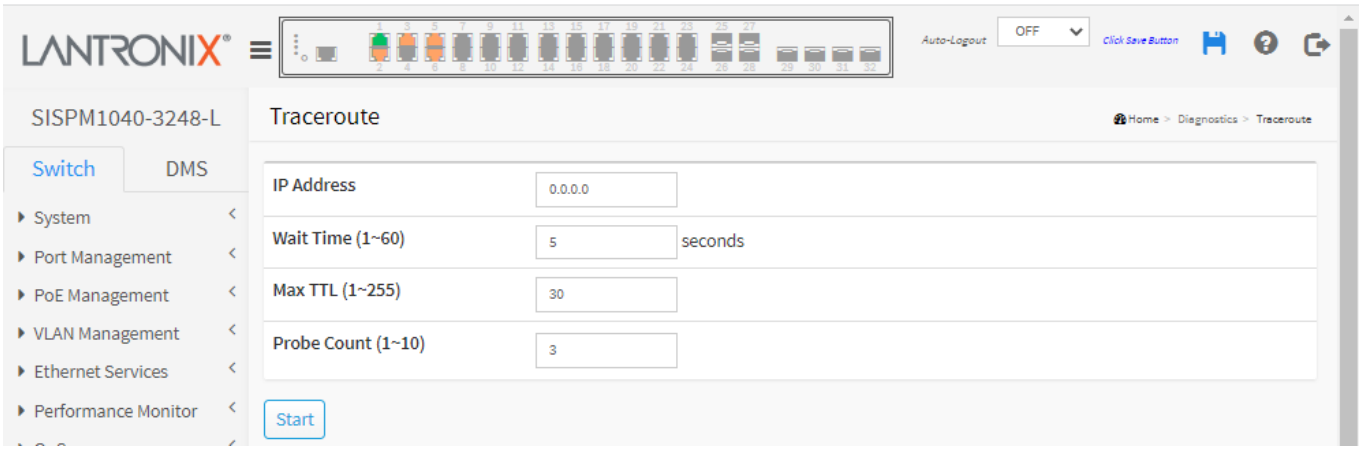


Figure 26-1: Traceroute

3. Click **Start**. Traceroute sends packets with gradually increasing TTL value, starting with TTL value of 1. The first router receives the packet, decrements the TTL value and drops the packet because it then has TTL value zero. The router sends an ICMP Time Exceeded message back to the source. The next set of packets are given a TTL value of 2, so the first router forwards the packets, but the second router drops them and replies with ICMP Time Exceeded. Proceeding in this way, traceroute uses the returned ICMP Time Exceeded messages to build a list of routers that packets traverse, until the destination is reached and returns an ICMP Echo Reply message.

Figure 26-2: Traceroute Output

Parameter descriptions:

IP Address : The destination IP Address.

Wait Time : Set the time (in seconds) to wait for a response to a probe (default 5.0 seconds). Valid values are 1 - 60 seconds.

Max TTL : Specifies the maximum number of hops (max time-to-live value) traceroute will probe. Valid values are 1 – 255 hops. The default is 30 hops.

Probe Count : Sets the number of probe packets per hop. Valid values are 1 - 10. The default is 3.

Buttons

Start : Click the button to start to traceroute the target IP Address.

New Traceroute: Click to go back to the Traceroute page.

Sample Traceroute Output:

```
Traceroute

traceroute to 192.168.1.77 (192.168.1.77), 50 hops max, 38 byte packets
1 192.168.1.77 (192.168.1.77) 0.184 ms 0.141 ms 0.109 ms 0.096 ms 0.096 ms 0.101 ms
```

26-3 Cable Diagnostics

This page lets you run Cable Diagnostics for 10/100 and 1G copper ports. To run Cable Diagnostics via the web UI:

1. Click Diagnostics and Cable Diagnostics.
2. Specify which Port you want to test.
3. Click Start. At the confirmation prompt click OK. This will take approximately 5 seconds. When completed, the page refreshes automatically, and you can view the cable diagnostics results in the cable status table. Note that Cable Diagnostics is only accurate for cables of length 7 - 120 meters with 5-meter accuracy. 10 and 100 Mbps ports will be linked down while running Cable Diagnostics. Therefore, running Cable Diagnostics on a 10 or 100 Mbps management port will cause the switch to stop responding until Cable Diagnostics is complete.

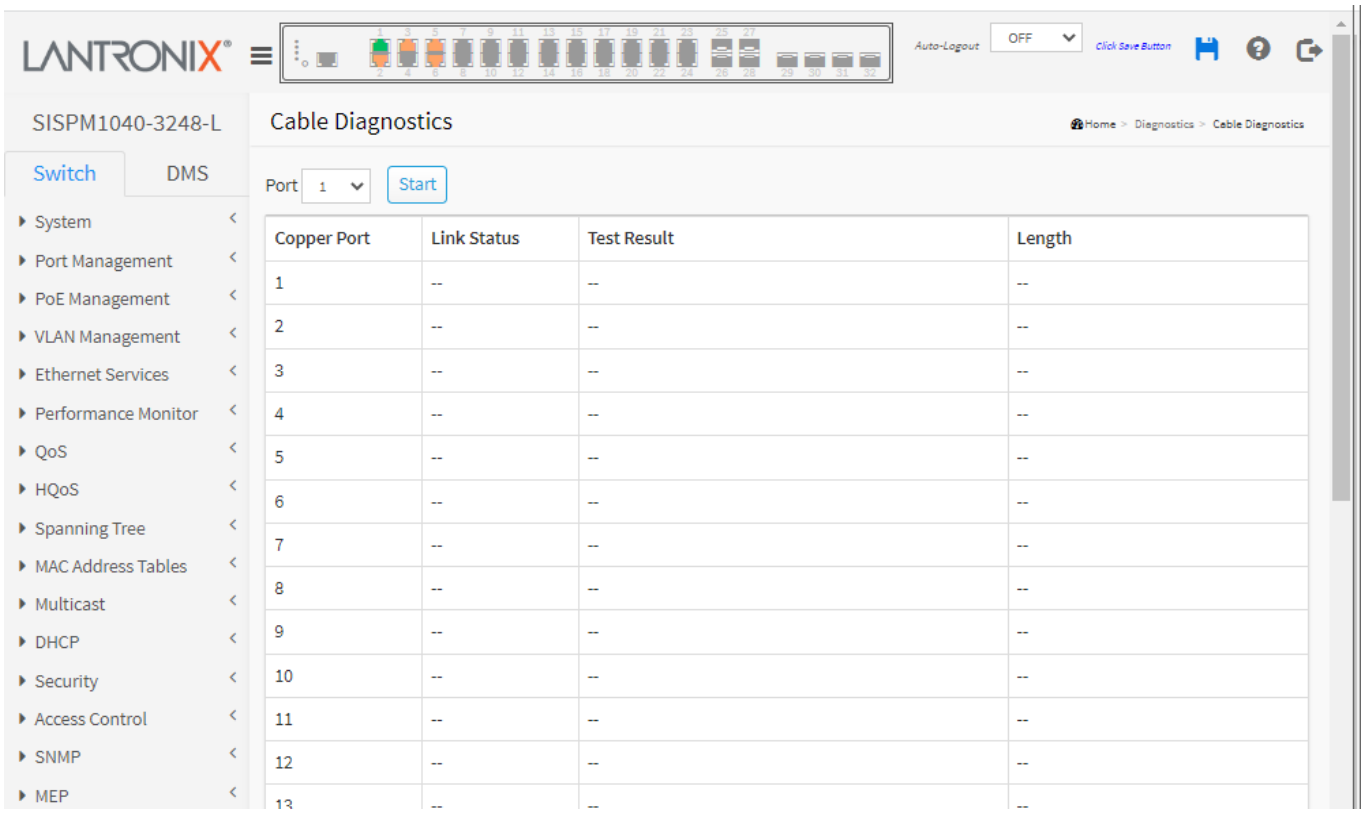


Figure 26-3: Cable Diagnostics

Parameter descriptions:

Port : At the dropdown select the port for which you are requesting Cable Diagnostics.

Copper Port : Copper port number.

Link Status : The status of the cable.

10M: Cable is link up and correct. Speed is 10Mbps

100M: Cable is link up and correct. Speed is 100Mbps

1G: Cable is link up and correct. Speed is 1Gbps

Link Down: Link down or cable is not correct.

Test Result : Test result of the cable.

OK: Correctly terminated pair.

Abnormal: Incorrectly terminated pair or link down.

Length : The length (in meters) of the cable pair. The resolution is 3 meters. When Link Status is shown as 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.

Buttons

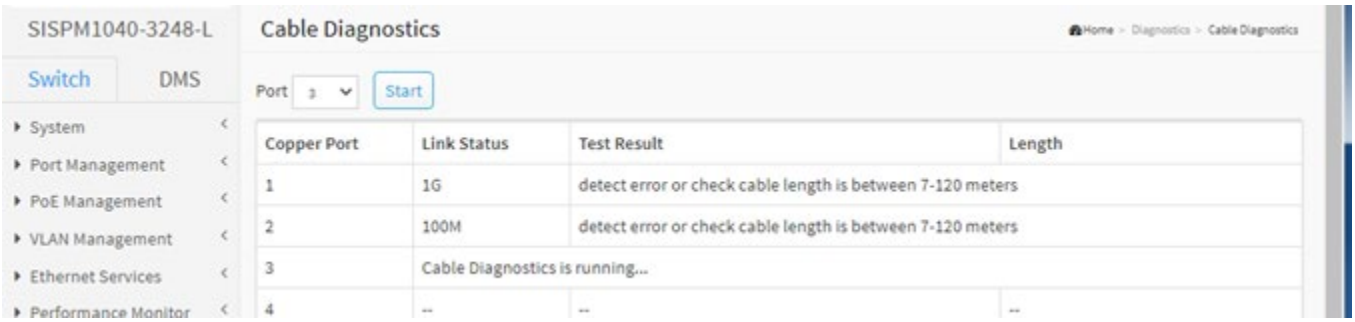
Start : Start to cable diagnostics the port that you selected.

Port select box: At the dropdown select the port on which to run the cable diagnostics.

Messages:

Cable Diagnostics is running...
detect error or check cable length is between 7-120 meters

Example:



26-4 Mirroring

Port mirroring allows you to monitor network traffic with an external network analyzer. The administrator can use Mirroring to debug network problems. The selected traffic can be mirrored or copied on a destination port where a network analyzer can be attached to analyze the network traffic.

For debugging network problems or monitoring network traffic, the switch can be configured to mirror frames from multiple ports to a mirror port. (In this context, mirroring a frame is the same as copying the frame.) Both incoming (source) and outgoing (destination) frames can be mirrored to the mirror port.

To configure the Port Mirror function in the web UI:

1. Click Diagnostics and Mirroring.
2. Select a Monitor Session number (1-5)
3. Select the Monitor Destination Port (Mirror Port).
4. Select a Mode (Disabled, enable, TX Only and RX only) for each monitored port.
5. Click the Apply button to save the settings.
6. To cancel the settings click the Reset button to revert to previously saved values.

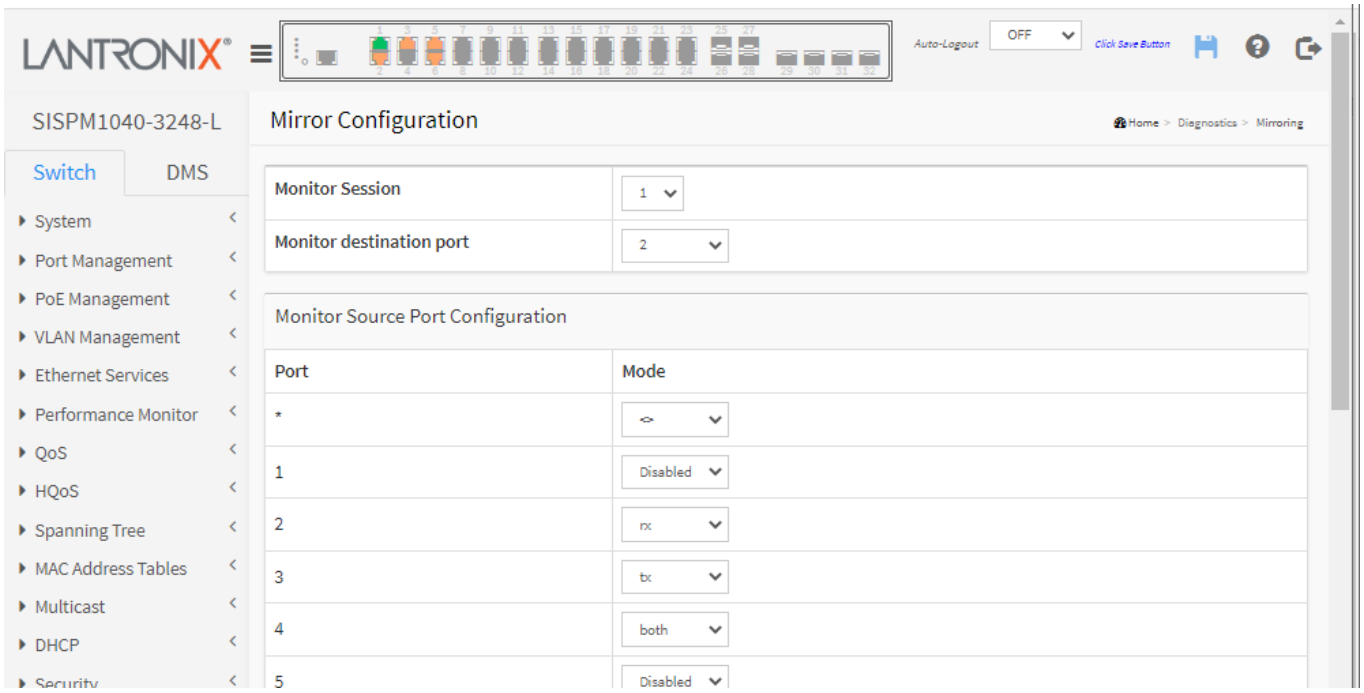


Figure 26-4: Mirror Configuration

Parameter descriptions:

Monitor Session : Dropdown to select a Session ID (1-5) to configure.

Monitor destination port : Port to output the mirrored traffic. Also known as the mirror port. Frames from ports that have either source (rx) or destination (tx) mirroring enabled are mirrored on this port. At the dropdown select Disabled or port 1-32. The default is Disabled.

Mirror Source Port Configuration : The Port and Mode parameters are used for Rx and Tx enabling:

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

Mode : Select mirror mode.

rx: Frames received on this port are mirrored on the mirror port. Frames transmitted are not mirrored.

tx: 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.

both : both Frames received and frames transmitted are mirrored on the Intermediate/Destination port.

Buttons

Apply : Click to save changes.

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

26-5 sFlow

26-5.1 Configuration

The sFlow Collector configuration for the switch can be monitored and modified here. The configuration is divided into two parts: configuration of the sFlow receiver (a.k.a. sFlow collector) and configuration of per-port flow and counter samplers. sFlow configuration is not persisted to non-volatile memory, which means that a reboot or master change will disable sFlow sampling.

sFlow is an industry standard technology for monitoring switched networks through random sampling of packets on switch ports and time-based sampling of port counters. The sampled packets and counters (referred to as flow samples and counter samples, respectively) are sent as sFlow UDP datagrams to a central network traffic monitoring server. This central server is called an sFlow receiver or sFlow collector. More information can be found at http://sflow.org. 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.

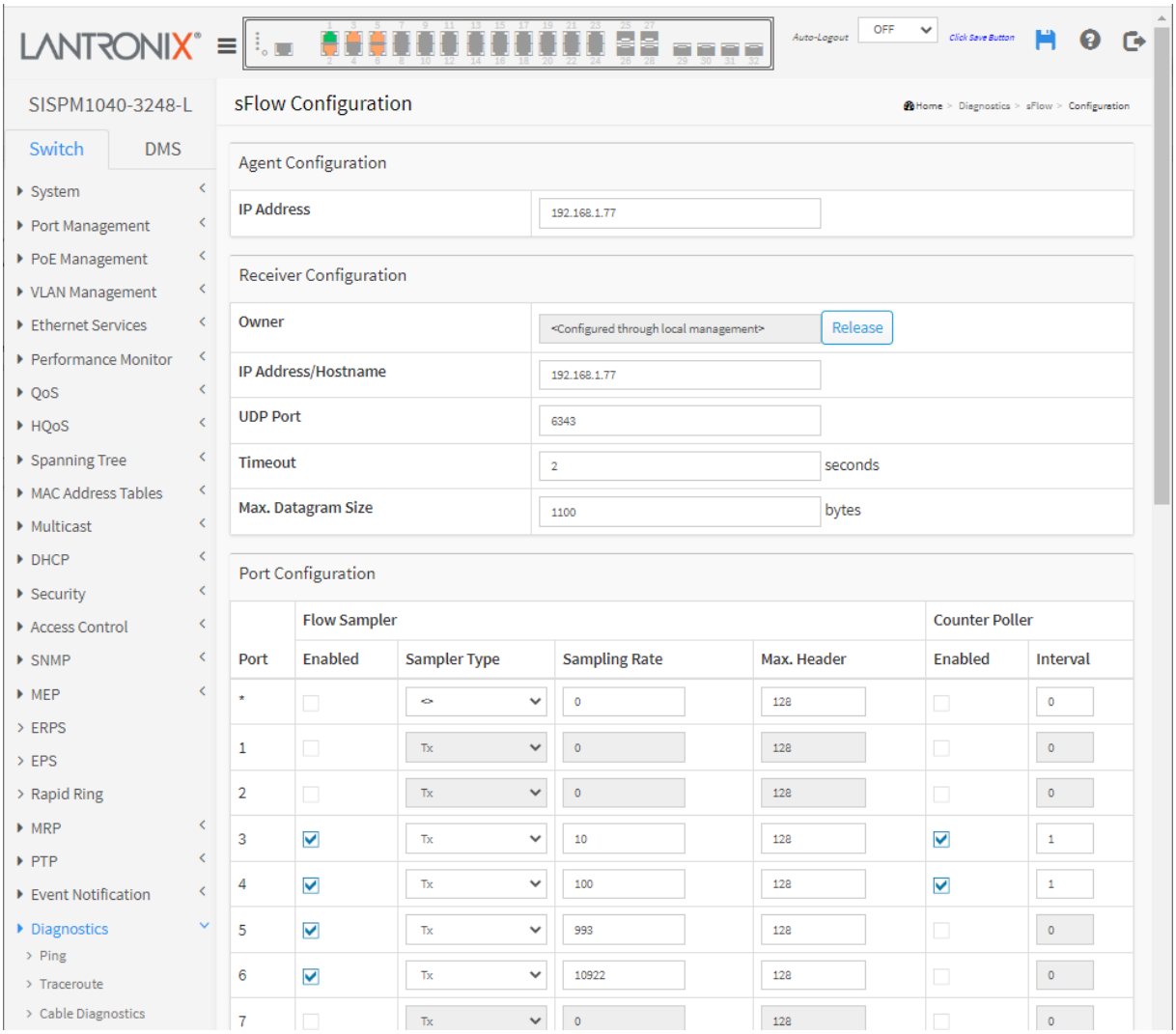


Figure 26-5.1: sFlow Configuration

Parameter descriptions:

Agent Configuration

IP Address : The IP address used as Agent IP address in sFlow datagrams. It serves as a unique key that will identify this agent over extended periods of time. Both IPv4 and IPv6 addresses are supported.

Receiver Configuration

Owner : Basically, sFlow can be configured in two ways: through local management using the Web or CLI interface or through SNMP. This read-only field shows the owner of the current sFlow configuration and assumes values as follows:

- If sFlow is currently unconfigured/unclaimed, Owner contains <*none*>.
- If sFlow is currently configured through Web or CLI, Owner contains <*Configured through local management*>.
- If sFlow is currently configured via SNMP, Owner contains a string identifying the sFlow receiver. If sFlow is configured via SNMP, all controls - except for the Release button - are disabled to avoid inadvertent reconfiguration.

The **Release** button allows for releasing the current owner and disable sFlow sampling. The button is disabled if sFlow is currently unclaimed. If configured through SNMP, the release must be confirmed (a confirmation request will 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. Valid range is 200 to 1468 bytes with default being 1400 bytes.

Port Configuration

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

Flow Sampler Enabled : Enables/disables flow sampling on this port.

Flow Sampler Sampling Rate : The statistical sampling rate for packet sampling. Set to N to sample on average 1/Nth of the packets transmitted/received on the port. Not all sampling rates are achievable. If an unsupported sampling rate is requested, the switch will automatically adjust it to the closest achievable. This will be reported back in this field. Valid range is 1 - 4294967295.

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 - 200 bytes; the default is 128 bytes. If the maximum datagram size does not take into account the maximum header size, samples may be dropped.

Counter Poller Enabled : Enables/disables counter polling on this port.

Counter Poller Interval : With counter polling enabled, this specifies the interval - in seconds - between counter poller samples.

Buttons

Release : Allows for releasing the current owner and disable sFlow sampling. The button is disabled if sFlow is currently unclaimed. If configured through SNMP, the release must be confirmed (a confirmation request will display).

Apply : Click to save changes.

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

Release : See description under 'Owner' above.

Refresh : Click to refresh the page. Note that unsaved changes will be lost.

26-5.2 Statistics

This page shows sFlow receiver and per-port statistics. To display sFlow statistics in the web UI:

1. Click Diagnostics, sFlow, and Statistics.
2. View the displayed sFlow information.

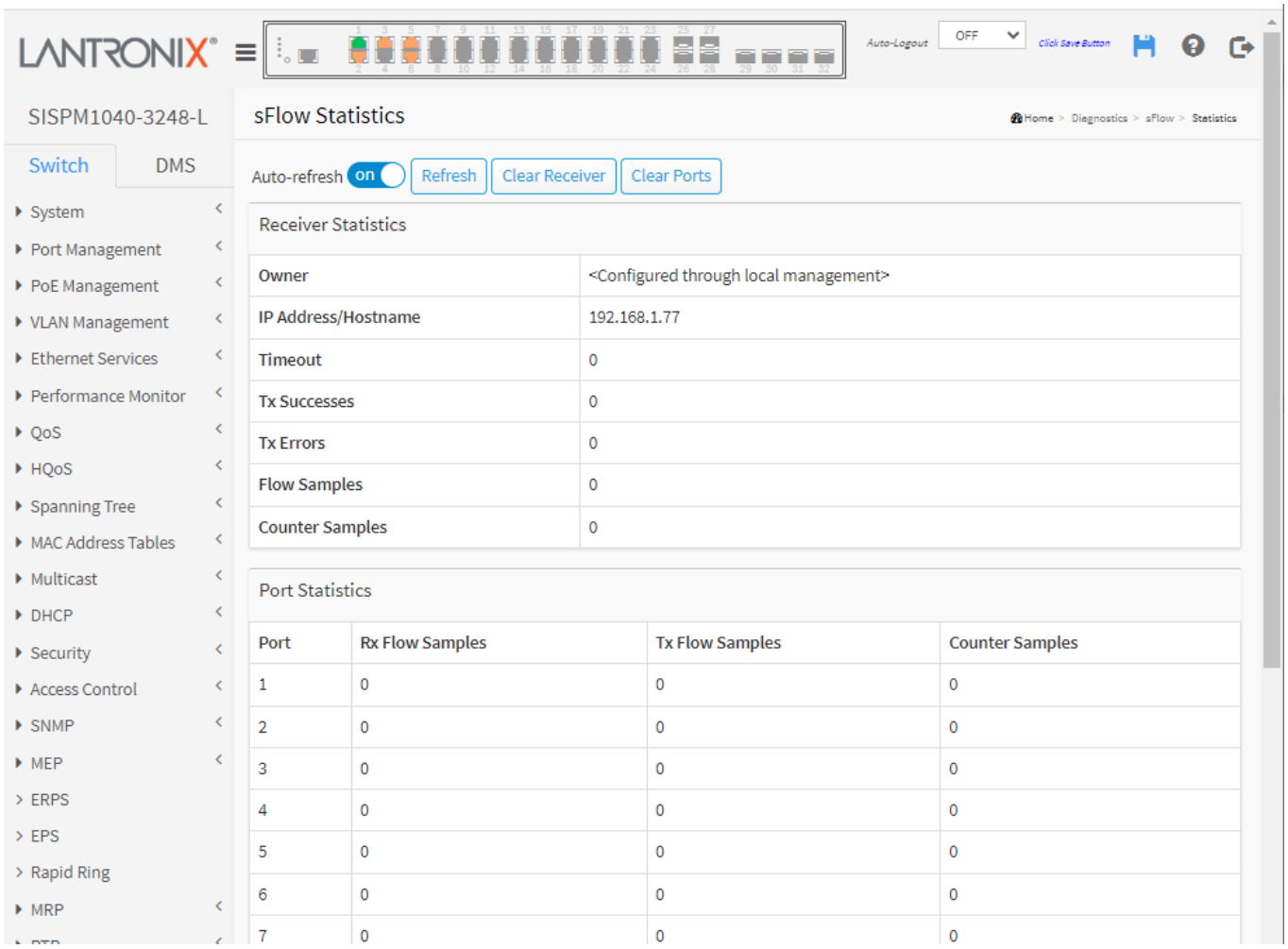


Figure 26-5.2: sFlow Statistics

Parameter descriptions:

Receiver Statistics

Owner : This field shows the current owner of the sFlow configuration. It assumes one of three values as follows:

- If sFlow is currently unconfigured/unclaimed, Owner contains <*none*>.
- If sFlow is currently configured through Web or CLI, Owner contains <*Configured through local management*>.
- If sFlow is currently configured through SNMP, Owner contains a string identifying the sFlow receiver.

IP Address/Hostname : The IP address or hostname of the sFlow receiver.

Timeout : The number of seconds remaining before sampling stops and the current sFlow owner is released.

Tx Successes : The number of UDP datagrams successfully sent to the sFlow receiver.

Tx Errors : The number of UDP datagrams that has failed transmission. The most common source of errors is invalid sFlow receiver IP/hostname configuration. To diagnose, paste the receiver's IP address/hostname into the Ping webpage (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

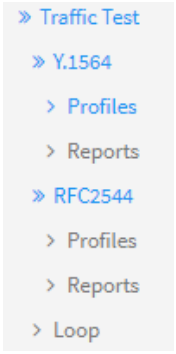
Auto-refresh : Click to refresh the page automatically every 3 seconds.

Refresh : Click to manually refresh the page immediately.

Clear Receiver : Clears the sFlow receiver counters.

Clear Ports : Clears the sFlow per-port counters.

26-6 Traffic Test



This menu section lets you perform Y.1564 and RFC 2544 traffic tests and Traffic Test Loop (TT-LOOP).

26-6.1 Y.1564

Here you can configure Y.1564 Profiles and Reports.

The available y.1564 tests are CIR Configuration Test, EIR Configuration Test, Traffic Policing Test, and Performance Test.

Y.1564 is an Ethernet service activation test methodology whose purpose is to test Ethernet Virtual Connections (EVCs). An EVC is a collection of one or more ordered set of rules, known as ECEs. Each ECE describes matching criteria for traffic arriving at the UNI. The matching criteria configuration is very flexible, and can be made almost arbitrarily complex, but also very simple. For example, an Ethernet Virtual Private Line (EVPL) ECE simply matches a particular VLAN ID.

Besides UNI matching criteria, the ECE defines a set of actions. In relation to Y.1564, the most important action is the policer it maps to. Policers are configured separately, and multiple ECEs may point to the same physical policer, thus sharing the bandwidth set aside by the policer. Policers can also be attached to an EVC, and the ECE can be configured to use the EVC policer rather than its own.

In order to execute a Y.1564 test, a set of Y.1564-specific configuration parameters along with information about which EVC/ECE to test is needed. The Y.1564-specific configuration is independent of the EVC/ECE to test, and is called a 'profile'. The profile can be persisted to flash and used over and over again as input configuration to test EVCs/ECEs as they are created. The result of executing a test is called a 'report'. Up to 16 profiles and 10 reports can be stored on the switch.

Test of an EVC/ECE is initiated from the Diagnostics > Traffic Test > Y.1564 > Reports page. Once executing, the switch takes the EVC under test out of service and generates frames on behalf of the customer at rates defined by the selected Y.1564 subtests and the individual ECEs' policer configurations. The frames will undergo the same mechanisms as had the frames arrived on the UNI, and therefore be subject to policing and switching in the NNI domain.

In the profile, you can choose between having the switch generate Y.1731 OAM frames as test traffic and so-called simulated customer traffic. See Traffic Type for details. In either case, the software expects the frame flows be looped at the remote end (DST; destination) while swapping DMAC and SMAC. If the DST switch is of the same type as this, the loop may be configured by using the Configuration > Traffic Test > Loop page.

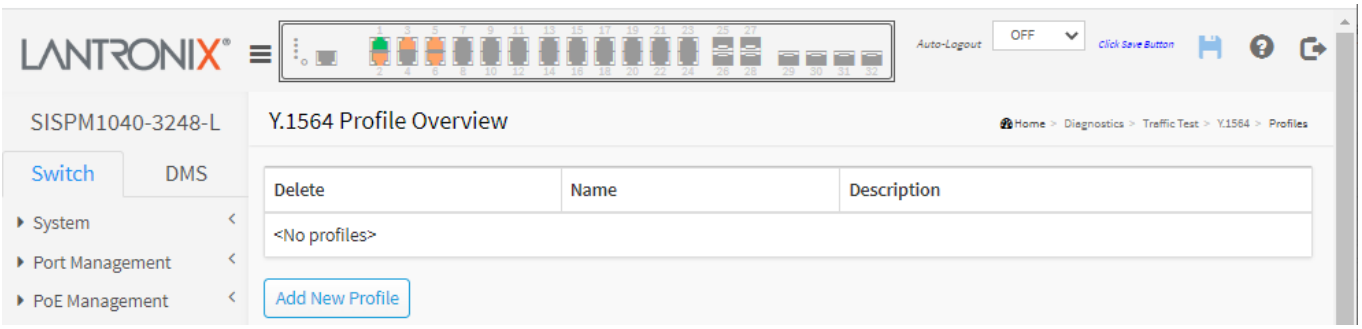
For delay measurements, the switch will transmit Y.1731 DMM if the remote end is OAM aware and Y.1731 1DM frames if not OAM aware.

On subtest completion, the switch will assess the measured performance against the policer configuration (SLA), while observing the Service Acceptance Criteria (SAC) embedded in the profile. The result of a subtest is either SKIP, PASS, or FAIL. If a subtest fails, execution stops and the whole test is considered failing.

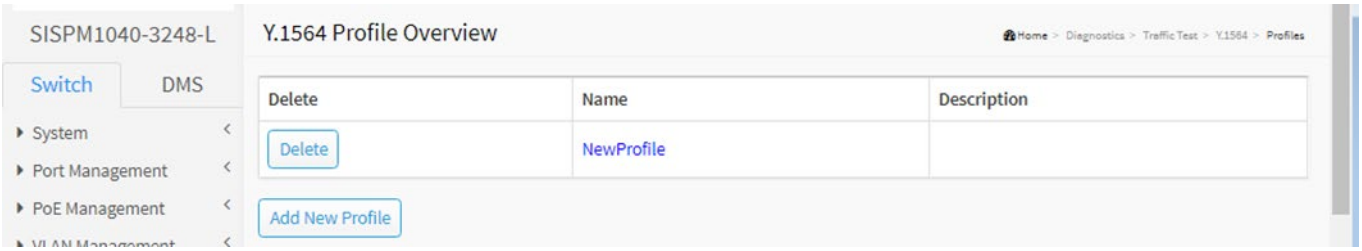
This page provides an overview of the defined profiles along with options for editing and deleting them and creating new.

Y.1564 Profile Overview

Navigate to the Switch > Diagnostics > Traffic Test > Y.1564 > Profiles menu path.



If no profiles are currently defined, the table displays "<No profiles>".



Otherwise there is a table row for each defined profile with these three parameters:

Delete : Click the button to delete the profile in question.

Name : A unique name identifying the profile. Click the name to edit the profile.

Description : The profile's description as entered in the profile editor, which is activated by clicking the name of the profile.

Buttons

Add New Profile : Create a new profile. This button is grayed out if the maximum number of profiles is already defined.

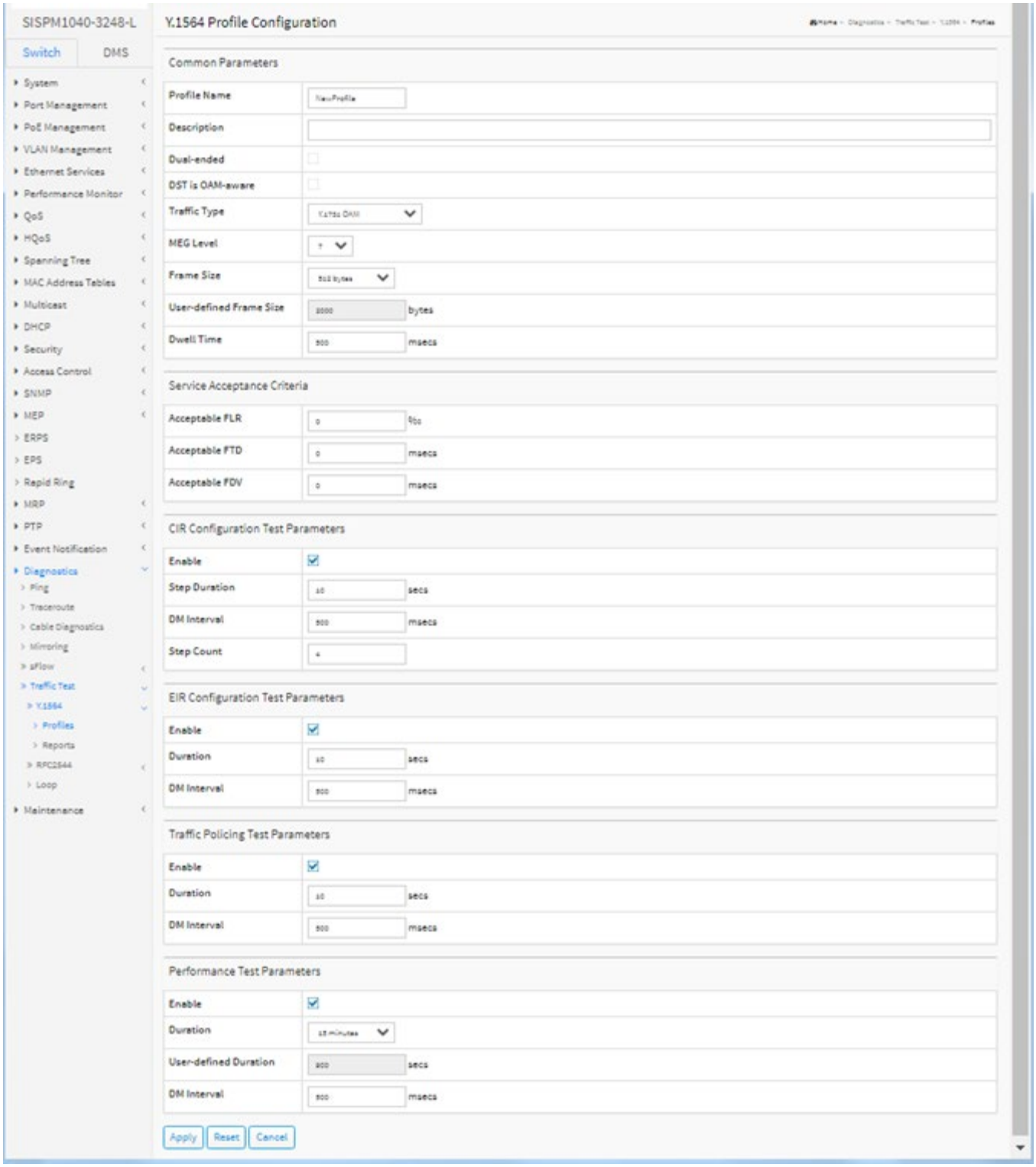
At the default Y.1564 Profile Overview screen, click the Add New Entry button to display the Y.1564 Profile Configuration page.

A profile defines key parameters and subtests to be executed as part of the Y.1564 service activation testing. The profile configuration is divided into a Common section, a Service Acceptance Criteria section, and a section for each of the four subtests that can be selected. At least one subtest must be enabled, and the enabled tests are executed in the order listed here.

Once a profile is created, use it to test one or more ECEs on the Y.1564 Test Start page by clicking the "Start New Test" button on the Diagnostics > Traffic Test > Y.1564 > Reports page.

Y.1564 Profile Configuration

Navigate to the Switch > Diagnostics > Traffic Test > Y.1564 > Profiles menu path and click the Add New Profile button to display the Y.1564 Profile Configuration page.



Parameter descriptions:

Common Parameters

Profile Name : Each profile must have a name that uniquely identifies it, since it is this name that is used in the process of executing a test. The length must be from 1 to 32 characters with each ASCII character being in the range [33; 126] except for /, \", <, >, and \' characters.

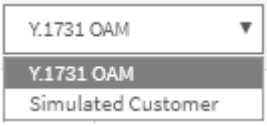
Description : This field allows for providing a textual description of the profile. Up to 128 characters can be entered using ASCII characters 32 - 126.

Dual-ended : For future use. In this revision of the software, this checkbox must be unchecked, meaning that this switch expects all generated traffic to be looped at the remote end (single-ended). Reporting and assessing of PASS/FAIL is therefore done by this switch. Dual-ended measurement is not supported yet.

DST is OAM-aware : When checked, this switch transmits Y.1731 DMM frames for delay measurements and Y.1731 1DM frames when unchecked. When Traffic Type is 'Y.1731 OAM', this switch transmits Y.1731 LBM frames as test traffic when DST is configured as OAM-aware, and Y.1731 TST frames when not configured as OAM-aware.

Traffic Type : At the dropdown select 'Y.1731 OAM' or 'Simulated Customer'.

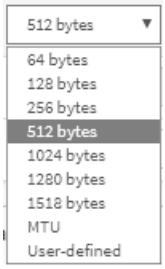
When set to '***Y.1731 OAM***', this switch transmits Y.1731 OAM PDUs as test traffic, and DST is OAM-aware determines the PDU type. Special rules capturing the Y.1731 traffic is installed on the fly, which means that the actual UNI Ingress ECE rules are not used with Y.1731 traffic as test traffic.



When set to '***Simulated Customer***', the software will generate a traffic-pattern that is supposed to hit the ECEs under test. The ECEs' counters are used to determine PASS/FAIL criteria. 'Simulated Customer' has the advantage that the tester can see directly from the report if ECEs are configured incorrectly, since the report will show per-ECE counters and fail if an ECE under test is not hit as expected by the traffic pattern.

MEG Level : The MEG level (0-7) used in generated Y.1731 OAM frames (both LBM/TST and DMM/1DM).

Frame Size : Selects the frame size of the test traffic. The frame size does not include possible C-tag(s) added to match the ECE. Standard frame size selections are 64, 128, 256, 512, 1024, 1280, and 1518 bytes per frame.
Besides these standard frame sizes there are two custom selections (MTU and User-defined).



MTU : The UNI's MTU will be used for the test traffic. Notice that if the EVC is tagged, the NNI port's MTU must be four bytes larger than the UNI port's.

User-defined : When Frame Size is set to 'User-defined', this field will un-grey, allowing for a custom specification of a frame size of the test traffic. Valid range is 64 - 10236 bytes.

Dwell Time : When a trial (a single step of a subtest) is executed, test traffic is transmitted for a certain period of time. When that period has elapsed, the Dwell Time defines how long to wait before reading hardware counters and status. The dwell time must be at least the worst-case roundtrip time, and therefore among others, depends on the physical distance between the near and far ends. The valid range is 100 - 10000 in steps of 100 milliseconds with a default of 500 milliseconds.

Service Acceptance Criteria (SAC)

After each test trial, the trial's measurements are evaluated with respect to a set of Service Acceptance Criteria parameters. If the trial fails, test execution is aborted, and the whole test is considered failing. Otherwise, execution proceeds to the next subtest.

Acceptable FLR : Defines the acceptable Frame Loss Ratio (FLR) measured in per mille. Setting this to 1000 effectively disables this check. The number is used in all enabled subtests. Only delay measurement PDUs and green test traffic undergo an FLR check. If the number of looped green frames differs from the number of transmitted green frames by more than the 'Acceptable FLR', the test is considered failing, otherwise passing. Valid range is 0 - 1000 with a default of 0‰.

Acceptable FTD : Defines the acceptable Frame Transfer Delay, measured in milliseconds. If the highest observed frame transfer delay exceeds this, the test fails. Valid range is 0 - 10000 with a default of 0 milliseconds. A value of 0 disables this check.

Acceptable FDV : Defines the acceptable Frame Delay Variation, measured in milliseconds. If the highest observed frame delay variation exceeds this, the test fails. Valid range is 0 - 10000 with a default of 0 milliseconds. A value of 0 disables this check.

CIR Configuration Test Parameters

In the CIR configuration test, frames are transmitted in steps of the policer's configured CIR. The 'Step Count' parameter determines the number of steps (trials) it takes to reach CIR. If CIR is zero, the test is skipped.

If the policer is color-aware and it's impossible to create a flow that is green when it hits the policer, the test is skipped along with a description of why.

If the sum of all ECEs under test's test traffic exceeds the UNI's link speed, the test is skipped.

If the policer is color-blind and it's possible to create a flow that is green when it hits the policer, use that flow. If the policer is color-blind and it's impossible to create a flow that is green when it hits the policer, use a yellow flow.

Step load is used for the CIR configuration test to gradually reach CIR. When step count is configured to 4 (default), a test flow will transmit at 25%, 50%, 75%, and 100% of CIR. For each step, the received IR, FLR, FTD, and FDV is measured and compared against the SAC, and the test fails if either of these doesn’t meet the SAC. If 100% of CIR has been reached successfully, the CIR test succeeds. Only green flows have their FLR compared to the SAC, since it's not possible to fail on yellow flows.

The general steps of a trial execution are provided below:

Trial Execution: For each trial, transmit a green, a yellow or both a green and yellow test flows per ECE under test for '(Step) Duration' seconds, after which the profile's Dwell Time is observed, before counters are read. The green traffic counters are evaluated against the SAC's Acceptable FLR. During a trial, delay measurements (DM) are performed and evaluated according to the description in DM Interval.

Enable : Check to enable the CIR configuration test.

Step Duration : Each step in the CIR configuration test applies test traffic for this number of seconds. Valid range is 1 - 3600 with a default of 10 seconds.

DM Interval : A Y.1731 1DM or DMM frame (depending on type of test) is transmitted every so many milliseconds, in order to perform delay measurements (DM). Select the number so that at least three DM frames are transmitted during a trial in order to obtain useful delay variation results.

After each trial the measured FTD and FDV is compared against the SAC's Acceptable FLR, FTD, and FDV.

Valid range is from 100 to 10000 in steps of 100 milliseconds with a default of 500 milliseconds. A value of 0 effectively disables transmission of DM frames, which thereby indirectly disables the check against the SAC.

Step Count : The number of steps (trials) used to reach CIR. For example, if Step Count is set to 4, four trials are executed. The first runs at 25% of CIR, the second at 50%, then 75%, and finally 100%.

A step count of 1 corresponds to executing Y.1564's A.1 test (Simple CIR Validation Test). A step count greater than 1 corresponds to executing Y.1564's A.2 test (Step Load CIR Test). Valid range is 1 - 1000 with a default of 4 steps.

EIR Configuration Test Parameters

The purpose of the EIR configuration test is to test the policer's configured EIR.

If EIR is 0 or the policer is of type Single Leaky Bucket, the test is skipped.

If the policer is color-aware, we must be able to hit the policer with both a green and a yellow flow unless CIR is zero, where the green flow is not necessary. If not, the test is skipped along with a description of why. The green flow will have a rate of CIR and the yellow flow will have a rate of EIR.

For the green flow only, measure IR, FLR, FTD, and FDV and compare it to the SAC. If it meets the SAC, the test passes, otherwise it fails. IR and FLR for the yellow flow are computed for reporting purposes, but are not matched against the SAC, and therefore can't make the test fail.

If the policer is color-blind, only one flow will be generated. Since - from a policer perspective - it's equally good to use a green and a yellow flow towards the policer, either colored flow will work. A green flow will be chosen if it's possible to create it. The rate of the flow will be CIR + EIR.

If the ingress flow is green, measure IR and FLR and compare it to the SAC. If the ingress flow is yellow, measure IR and FLR only for reporting purposes, since the test can fail on yellow frames. Also measure FTD and FDV and compare it to the SAC. If the SAC is met, the test passes, otherwise it fails.

The EIR configuration test execution follows the description in Trial Execution above.

Enable : Check this to enable the EIR configuration test.

Duration : The EIR configuration test is executed in one single trial, whose duration is configured with this parameter. Valid range is 1 - 3600 with a default of 10 seconds.

DM Interval : A Y.1731 1DM or DMM frame (depending on type of test) is transmitted every so many milliseconds, in order to perform delay measurements (DM). Select the number so that at least three DM frames are transmitted during a trial in order to obtain useful delay variation results.

Traffic Policing Test Parameters

The purpose of the traffic policing test is to test the service when applying more traffic than the policers allow for. If the policer is color-aware, the following algorithm from the ITU-T Y.1564 Recommendation applies:

```
If EIR < 20% * CIR
 Green  = 100% * CIR
 Yellow =  25% * CIR + 100% * EIR
Else
  Green  = 100% * CIR
  Yellow = 125% * EIR
EndIf
```

If CIR is non-zero, it must be possible to create a flow that hits the policer as green. Otherwise the test is skipped. If the resulting yellow frame rate is non-zero, it must be possible to create a flow that hits the policer as yellow. Otherwise the test is skipped. Note that even though EIR is 0, it must be possible to create a yellow flow for the test not to be skipped.

If the policer is color-blind, only one flow will be generated. The rate of that flow is given by the following algorithm from the ITU-T Y.1564 Recommendation:

```
If EIR < 20% * CIR
  Rate = 125% * CIR + 100% * EIR
Else
  Rate = 100% * CIR + 125% * EIR
EndIf
```

Since - from a policer perspective - it's equally good to use a green and a yellow flow towards the policer, either colored flow will work. A green flow will be chosen if it's possible to create it.

If the ingress flow is green, measure IR and FLR and compare it to the SAC.

If the ingress flow is yellow, measure IR and FLR only for reporting purposes, since the test can fail on yellow frames. Also measure FTD and FDV and compare it to the SAC. If the SAC is met, the test passes, otherwise it fails.

Enable : Check this to enable the traffic policing test.

Duration : The traffic policing test is executed in one single trial, whose duration is configured with this parameter. Valid range is 1 - 3600 with a default of 10 seconds.

DM Interval : A Y.1731 1DM or DMM frame (depending on type of test) is transmitted every so many milliseconds, in order to perform delay measurements (DM). Select the number so that at least three DM frames are transmitted during a trial in order to obtain useful delay variation results.

Performance Test Parameters

In the service performance Test, green frames are transmitted at CIR, usually for a longer period of time (configured with Duration below) to validate the quality of the service. Execution of the test is similar to a one-step CIR configuration test.

Enable : Check this to enable the performance test.

Duration : The service performance test is executed in one single trial, whose duration is configured with this parameter. The drop-down box allows for selecting Y.1564-specified standard durations and a custom duration, selected by setting the drop-down box value to "User-defined" and specifying the duration in the "User-defined Duration" field below the drop-down box.

User-defined Duration : When the "Duration" drop-down box is set to "User-defined", this field provides the desired duration. Valid range is 1 - 86400 with a default of 900 seconds.

DM Interval : A Y.1731 1DM or DMM frame (depending on type of test) is transmitted every so many milliseconds, in order to perform delay measurements (DM). Select the number so that at least three DM frames are transmitted during a trial in order to obtain useful delay variation results.

Configuring DST

Refer to the Y.1564 Configuration Guide for help on configuring the remote end in case it is of the same brand as this switch. The remote end's loop configuration can be found in Diagnostics > Traffic Test > Loop on the DST switch. Contact Lantronix Technical Support for the Y.1564 Software Configuration Guide; see Contact Us below.

Buttons

Apply : If all input parameters are valid, the profile will be part of the running config and the Y.1564 Profile Overview page displays the new profile (see the Example below).

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

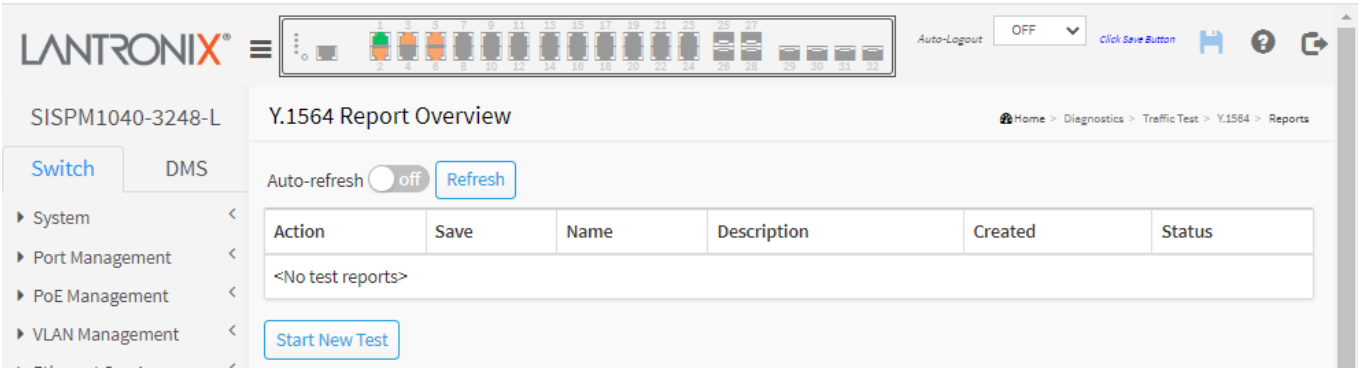
Cancel : Return to the Y.1564 Profile Overview page without creating a new profile.

Example

Y.1564 Report Overview

This page provides an overview of the currently stored reports along with options for deleting, downloading, and viewing them. Initiation of test execution is also handled through this page.

Navigate to the Switch > Diagnostics > Traffic Test > Y.1564 > Reports menu path to display the Y.1564 Report Overview page.



If no reports are currently stored, the table displays <No test reports>. Otherwise there is a table row for each test report, each containing the following elements:

Action : If a test is currently being executed, a Stop button displays. Clicking the Stop button will cause a request to be sent to gracefully cancel the execution. During this cancellation, the button will be disabled. At most one test can execute at a time. Once execution of a test is complete, successfully or not, the resulting report is persisted to non-volatile memory. Up to 10 reports can be persisted. New reports will replace the oldest. Only reports stored in non-volatile memory can be erased. This is done with the Delete button.

Save : Test reports can be downloaded and stored on the local computer with the use of the Start New Test button. The suggested file name will be the report name concatenated with ".txt".

Name : A unique name identifying the report. Click the name to view the report in the browser.

Description : The description assigned to the report as entered on the test execution page, invoked with the Start New Test button.

Created : The date and time at which execution started.

Status : The current status of executing a test:

Inactive: Test just initiated, but not started. This is a transitional state that is unlikely to be noticed.

In progress: Test is currently executing. At most one test can execute at a time.

Under cancellation: Test has just been stopped by the user. This is a transitional state that is unlikely to be noticed.

Cancelled by user: Test was stopped by the user and report is stored in non-volatile memory.

Succeeded: Test passed successfully and report is stored in non-volatile memory.

Failed: Test failed execution and report is stored in non-volatile memory. Details as to why the test failed are embedded in the report.

Buttons

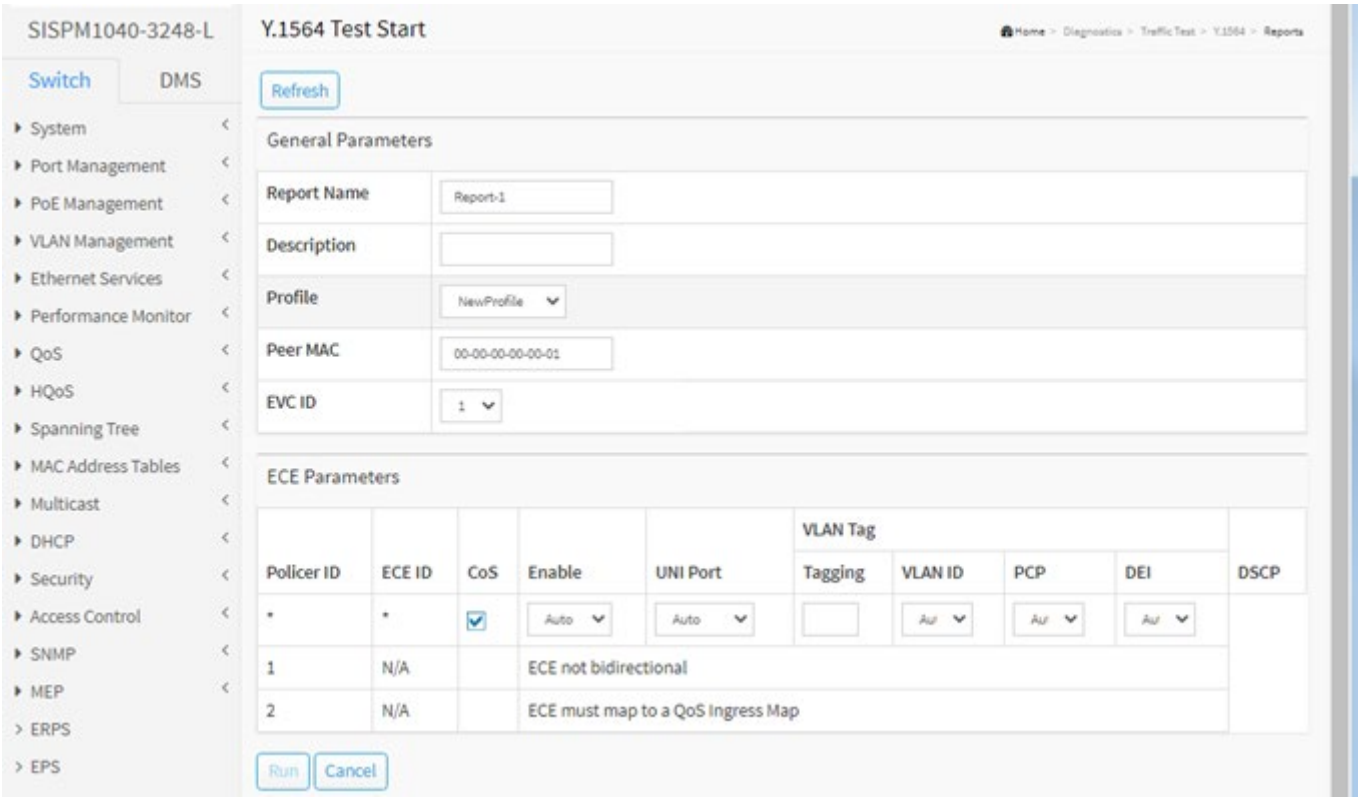
Start New Test : Initiate execution of a Y.1564 test. This button is grayed out if one test is already in progress.

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

Refresh : Click to manually refresh the page immediately.

Y.1564 Test Start

This page allows for initiating execution of a Y.1564 test while naming and describing the resulting report. Once a test is started, a snap-shot of the chosen profile is made, so that subsequent profile changes won't be reflected in the running test.



General Parameters

Report Name : Each test report must have a name that uniquely identifies it, since it is this name that identifies it in the non-volatile file system. The length must be from 1 to 32 characters with each ASCII character being in the range [33; 126] except for /, \", <, >, and \'.

Description : This field allows for providing a textual description of the report. Up to 128 characters can be entered with each ASCII character being in the range [32; 126].

Profile : Select the profile to use. The drop-down box is populated with the names of the currently defined Y.1564 profiles. If no profiles are defined, the text "<No Profiles>" is displayed and a test cannot commence.

Peer MAC : This field determines the destination MAC address used in generation of the test and delay measurement frames. This must be a non-zero unicast MAC address. Using a correct peer MAC address is critical

if the Y.1564 uses Y.1731 LBM/DMM for test traffic and delay measurements (that is, 'DST is OAM-Aware' is checked in the profile), because the remote end is supposed to reply with Y.1731 LBR/DMR.
If the remote end (DST) is configured as a facility loop, this should be the MAC address of the DST's NNI port for the EVC under test.
On the other hand, if DST is configured as a terminal loop, this should be the MAC address of the DST's UNI port for the EVC under test. To quickly get to re-test an EVC, the Peer MAC is preserved from test-start to test-start, but not across boots.

EVC ID : This drop-down box lists the IDs of all currently defined EVCs. If no EVCs are defined, the text "<No EVCs>" is displayed. When selecting an EVC ID, the list of ECEs in the table below is automatically updated to reflect the ECEs carried in the newly selected EVC. Note that when you change EVC ID with this drop-down box, any changes you may have made to the ECE parameters in the ECE table below will be lost.

ECE Parameters : The purpose of the ECE table is to allow for specifying which ECEs to test and optionally select per-ECE parameters used during the testing.
Both an EVC and its ECEs must adhere to a number of rules before they are considered testable.
If an EVC is not testable, one single line in the table displays why. No ECEs are displayed in that case.
If an ECE is not testable, that ECE's input fields are removed and instead a description of why is displayed.
Possible misconfigurations fall into two categories: 1) Those that can be checked prior to starting the test (pre-checks), and those that can only be checked when the profile and ECE parameters are selected (post-checks).
The latter category of misconfigurations is shown in a dialog box after the user hits the "Run" button. In that case, all information entered on the Test Start page will be lost.
As mentioned, all ECEs on the EVC - whether under test or not - are taken out of service during testing. Frames that may arrive on the UNI that match the ECEs taken out of service will therefore be discarded.
When test traffic is simulated customer, the Y.1564 software will clone each of the ECEs and match on EtherType 0x8880 or TPID 0x88A8, depending on the original ECEs' matching criteria. This is reflected in the test report, where the frame applied at UNI ingress is printed.

ECE ID : The ID of the ECE belonging to the selected EVC. The ECEs are listed in the same order as they are applied to hardware.

CoS : Shows the class of service that this ECE maps to. When the profile specifies Y.1731 as test traffic, two ECEs that map to the same CoS cannot be tested at a time.

Enable : This checkbox is only available if the ECE is testable.
When checked, the corresponding ECE is selected for test.
When using Y.1731 OAM as test traffic, up to 8 CoSs (8 ECEs mapping to different CoSs) can be tested at a time.
When using simulated customer traffic, up to 8 ECEs can be tested simultaneously.

UNI Port : In cases where the selected ECE is installed on two or more UNI ports, a particular port on which the test traffic is applied can be chosen with this drop-down box. Default is 'Auto', which causes the lowest port number in the set of ports to be chosen automatically. The drop-down box is populated only with the UNIs that the ECE is installed on.

Tagging : Drop-down box with the tagging options for the ECE in question. The drop-down box always contains the Auto selection, which means that it is up to the Y.1564 software to pick a suitable tag-type and VLAN ID to

put in the frame when testing the ECE. The two other possible values are: Untagged and Specific. If the ECE matches untagged traffic, Untagged will be present. If the ECE matches VLAN tagged traffic Specific is present in the drop-down box.

VLAN ID : This is only available if 'Tagging' is set to Specific. It allows the user to select a particular VLAN ID to be used in the generated packets for that ECE. The test will not start, if the selected VLAN ID is not within the ECE's matching range.

PCP : Selects the PCP value used in the VLAN tag (if present) of the UNI ingress traffic for this ECE. Default is Auto, which means that the Y.1564 software selects a suitable PCP value itself. This value is only used if the selected profile's 'Traffic Type' is set to Simulated Customer. For Y.1731 test traffic, the PCP value will be that of the CoS the ECE maps to.

DEI : Selects the DEI value used in the VLAN tag (if present) of the UNI ingress traffic for this ECE. The DEI value normally controls the color of the ingress traffic through classification of DEI to Drop Precedence (DP), but several things may cause the DP not to follow the DEI. The ECE, for instance, may force all traffic into a particular DP, making the DEI irrelevant, or the UNI's QoS Ingress Port Tag Classification configuration may cause a DEI of 0 to map to a DP of 1. If set to Auto (which is the default), the Y.1564 software analyzes which color a flow with DEI 0 will have when it reaches the policer and which color a flow with DEI 1 will have when it reaches the policer. If both DEI values result in the same color, only one flow will be generated, otherwise two flows will be generated when needed.
The drop-down box has two other values, 0 and 1. Selecting either will cause at most one flow to be generated. The Y.1564 software will analyze the color of that flow when it reaches the policer, so typically, one can restrict the test to green-only flows or yellow-only flows by selecting a value different from Auto.

DSCP : This field is only available when the Frame Type the ECE matches is IPv4 or IPv6. In other cases, the field will show N/A.
Setting it to Auto causes the software to select the lowest DSCP value the ECE matches.
Setting it to any other value will cause the software to use that value in the generated test traffic. The value is only used if using simulated customer traffic as test traffic.

Messages:

ECE not bidirectional

ECE must map to a QoS Ingress Map

Dual-ended measurements not supported yet

Buttons

Run : If all input parameters are valid, the test will attempt to start executing the test. If a post-check fails, an error dialog box will appear and you will stay on the page. Otherwise you will be forwarded to the Y.1564 Report View page to follow the progress of the test.

Cancel : Return to the Y.1564 Report Overview page without initiating a new test.

Refresh : Click to refresh the page immediately.

26-6.2 RFC2544

Here you can configure RFC 2544 Profiles and Reports. The available RFC 2544 tests are Throughput Test, Latency Test, Frame Loss Test, and Back-to-Back Test. IETF RFC2544 is a benchmark testing tool that allows for testing an Ethernet service connection end-to-end with respect to various key parameters.

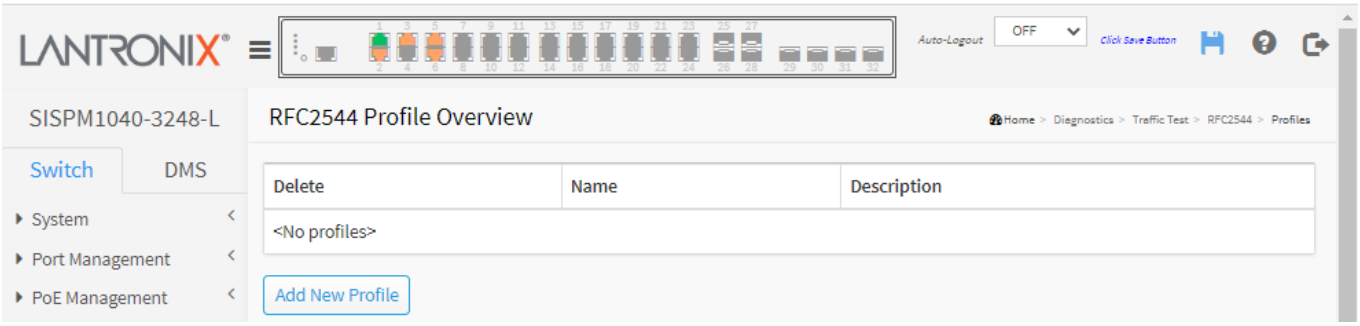
Each test configuration is called a 'profile', and each result of executing the profile is called a 'report'. You can store up to 16 profiles and 10 reports. Execution of a profile is initiated from the Diagnostics > Traffic Test > RFC2544 > Reports page.

Executing a profile causes the switch (near end) to generate and transmit frames at certain rates on the configured egress port. The remote end is supposed to loop these frames while swapping source and destination MAC addresses. The looped frames are then expected to arrive at the same port as they egressed at the near end. The switch that generated the frames can therefore assess whether an Ethernet service connection meets the SLA.

The switch supports the near-end functionality only (generation + check of frames). Remote end functionality (loop + MAC address swap) is not supported.

26-6.2.1 RFC Profile Overview

Navigate to the Switch > Diagnostics > Traffic Test > RFC2544 > Profiles menu path. This page provides an overview of the defined profiles along with options for creating new profiles and editing and deleting existing profiles.



If no profiles are currently defined, the table displays <No profiles>. Click the Add New Profile button to begin creating and configuring a new IETF RFC 2544 profile.

Delete : Click the button to delete the profile in question.

Name : A unique name identifying the profile. Click the name to edit the profile.

Description : The profile's description as entered in the profile editor, which is activated by clicking the name of the profile.

Buttons

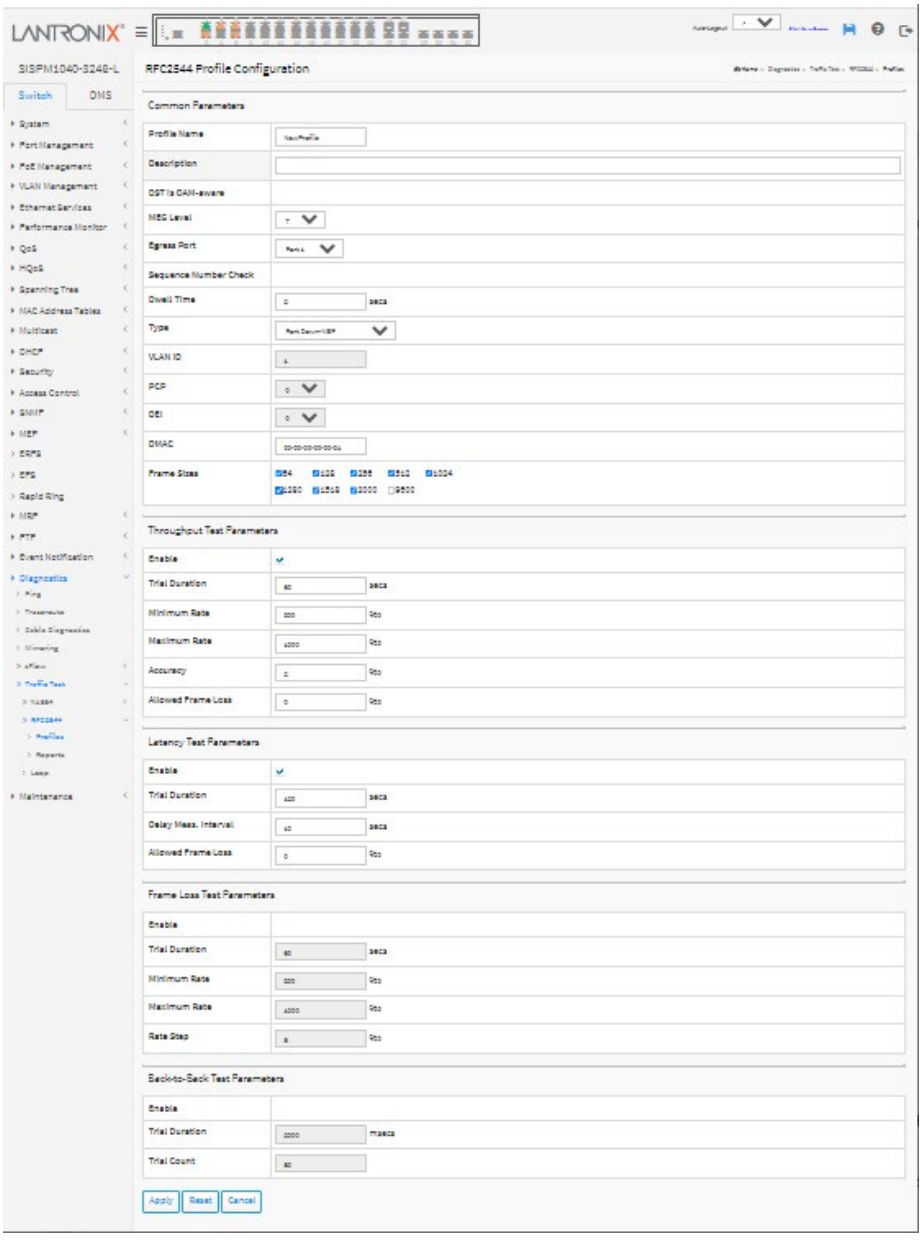
Add New Profile : Click to create a new profile as described below. This button is grayed out if the maximum number of profiles is already defined.

26-6.2.2 RFC2544 Profile Configuration

A profile defines key parameters and sub-tests to be executed as part of the RFC2544 benchmark testing. The profile configuration is divided into a common section, which contains parameters shared by the four tests that can be defined for a profile. At least one of the four tests must be enabled.

All rates configured in a profile are measured in ‰ of the line rate. The reason for not using bits per second or other units is that egress ports may be configured at various speeds, so in order to have a link-speed independent way of configuring rates, a percentage (‰) of the line rate is chosen.

All rates configured in a profile are interpreted as requested rates on the customer-facing side of the switch. The egress port on which the tests are conducted is considered the network-facing side. If the switch adds a VLAN tag to frames (see Type), the rate on the network-facing side will therefore be higher than the requested customer-facing side's rate, except that the rate cannot exceed the line rate.



Common Parameters

Profile Name : Each profile must have a name that uniquely identifies it, since it is this name that is used in the process of executing a profile. The length must be 1 - 32 characters with each ASCII character being in the range 33 - 126 except for /, \", <,>, and \' characters.

Description : This field allows for providing a textual description of the profile. Up to 128 characters can be entered with each ASCII character being in the range 32 - 126.

DST is OAM-aware : The frame types used in the RFC2544 tests are Y.1731 OAM. This field selects between using TST/1DM (when 'DST is OAM-aware' is un-checked) and LBM/DMM (when 'DST is OAM-aware' is checked).

In the first case, it is expected that the frames returned by the remote end are of the same type as the ones transmitted by this end (i.e., TST/1DM), whereas in the latter case, it is expected that the frames returned by the remote end are of type LBR/DMR.

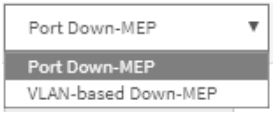
MEG Level : The frame types used in the various tests are Y.1731 OAM frames (See 'DST is OAM-aware' for actual type). These frame types contain a MEG Level (MEL) field, which can be controlled with the value entered in this select box, which ranges from 0 to 7 with 7 being the default.

Egress Port : The port on which the generated frames are transmitted and expected received.

Sequence Number Check : When checked, looped Y.1731 TST/LBR frames are tested for out-of-order upon reception. Out-of-order frames are frames received in a different order than they were transmitted. If an out-of-order sequence is detected, the sub-test or trial is considered failing.

Dwell Time : When a trial is executed, Y.1731 TST or LBM frames are transmitted for a certain period of time. When that period has elapsed, the Dwell Time defines how long to wait before reading hardware counters and status in order to assess the status of the trial. The required dwell time must be at least the worst-case roundtrip time, and therefore depends on the physical distance between the near and far ends. Valid range is 1 - 10 with a default of 2 seconds.

Type : The RFC2544 test suite supports two types of tagging of frames on egress:



Port Down-MEP, where all frames are transmitted untagged.

VLAN-based Down-MEP, where all frames are transmitted with a VLAN tag. In order for this to work, the following manual VLAN configuration of the egress port is required:

- The VLAN Port Mode must be Trunk or Hybrid in order to get frames tagged upon transmission.
- The VLAN Port Type must be either C-, S-, or S-Custom.
- VLAN Egress Tagging must be set to either tag all or untag Port VLAN. In the latter case the chosen VLAN ID for the profile must be different from the configured VLAN Port VLAN ID.
- The port must be member of the chosen VLAN ID.
- Whichever type is selected, frames are generated as close to the egress port as possible (hence the "Down-MEP" term) and therefore are not sent through the queueing system, due to lack of integration with EVCs in this version of the software.

When VLAN-based Down-MEP is selected, the VLAN tag's ID, PCP, and DEI values are selected with the subsequent fields.

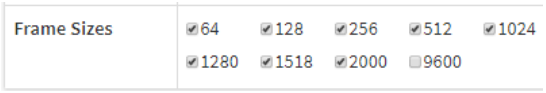
VLAN ID : When Type is set to VLAN-based Down-MEP, this field determines the VLAN ID used in the tag. Valid values are 1 - 4095.

PCP : When Type is set to VLAN-based Down-MEP, this field determines the PCP value used in the VLAN tag.

DEI : When Type is set to VLAN-based Down-MEP, this field determines the DEI value used in the VLAN tag.

DMAC : This field determines the destination MAC address used in generation of the Y.1731 OAM frames. This must be a non-zero unicast MAC address. Notice, that it is possible to override this MAC address during start of a particular test. The source MAC address will automatically become the egress port's native MAC address. Note that it is important that the remote end swaps DMAC and SMAC while looping the frame.

Frame Sizes : Each sub-test is repeated for every selected frame size. At least one frame size must be checked. By default, all but the jumbo frame size are selected.



Throughput Test Parameters

Enable : Check to enable the throughput sub-test. The throughput test searches for the maximum rate at which at most a certain percentage of the frames are lost. The throughput test starts at the maximum configured rate and uses a dichotomist algorithm (binary search) to find the optimum rate. The trials continue until the difference between a failing and succeeding rate is smaller than the configured accuracy.

Trial Duration : The time - in seconds - to transmit Y.1731 TST or LBM frames at one given rate and frame size. This is known as a "trial". Valid range is 1 - 1800 seconds with a default of 60 seconds.

Minimum Rate : The minimum rate - in ‰ of the egress port's line rate - to transmit Y.1731 TST or LBM frames at. If a trial fails at this rate, the test fails. Valid range is 1 - 1000‰ with a default of 800 ‰ of the line rate.

Maximum Rate : The maximum rate - in ‰ of the egress port's line rate - transmit Y.1731 TST or LBM frames at while searching for maximum throughput. This is the rate that the search starts at. Valid range is 1 - 1000 with a default of 1000 ‰ of the line rate.

Accuracy : This specifies the stop criterion for the search for a maximum throughput rate. When the difference between a failing and succeeding rate is smaller than the accuracy, the search stops and the succeeding rate becomes the result. Valid range is 1 - 1000 with a default of 2 ‰ of the line rate.

Allowed Frame Loss : In some cases, it may be acceptable to have loss on a connection. The allowed loss can be specified with this parameter. The loss is measured in ‰ of the number of transmitted frames during a trial, so if allowed loss is set to e.g. 1 ‰ and 1000 frames is transmitted during a trial, the trial will be considered successful if 999 or 1000 frames return to the transmitter. Valid range is from 0 to 100 with a default of 0 ‰ of the number of transmitted frames.

Latency Test Parameters

Note: Latency test depends on the Throughput test. Both must be enabled and configured for the Latency test to work.

Enable : Check to enable the latency sub-test. The latency test measures the round-trip time of frames leaving the near-end until they get back to the near-end.

Y.1731 TST or LBM frames are transmitted at the maximum rate determined by the throughput test less 200 Kbps. Every so many seconds, a Y.1731 1DM or DMM frame is transmitted and the time from this frame leaves the switch until it comes back is measured. If more than two 1DM frames are transmitted during a trial, also the delay variation will be part of the generated report.

Selecting the latency test causes the throughput test to be selected automatically.

Trial Duration : The time - in seconds - to transmit Y.1731 TST or LBM frames at a given rate and frame size. This is known as a "trial". Valid range is 10 - 1800 with a default of 120 seconds.

Delay Measurement Interval : This controls the period - in seconds - at which Y.1731 1DM frames are transmitted. The first 1DM frame is transmitted this number of seconds after the trial has started. The total number of transmitted 1DM frames in one trial therefore depends on the configured trial duration.
Valid range is 1 - 60 with a default of 10 seconds.

Allowed Frame Loss : In some cases, it may be acceptable to have loss on a connection. The allowed loss can be specified with this parameter. A trial is considered failing if more than this percentage of frames are lost. Valid range is 0 - 100 with a default of 0 ‰ of the number of transmitted frames.

Frame Loss Test Parameters

Enable : Check to enable the frame loss sub-test. The frame loss test measures frame loss at configurable transmission rates. It starts at the configured maximum rate and steps down by the configured step size and stops when two consecutive trials succeed (test succeeded in that case) or the minimum rate is reached (test failed in that case). For a trial to succeed, two criteria must be fulfilled:

- Test must have zero frame loss.
- The actual Tx rate must be greater than the applied Tx rate minus the step rate. The rates reported are seen by the customer. Encapsulation possibly added on the network-facing side (e.g. a VLAN tag) may cause the actual Tx rate to be smaller than the applied Tx rate while the frame loss is still measured as zero. Hence this additional criterion. When this situation occurs, software may skip steps that it "knows" will fail in order to quickly get to the rates that are expected passing.

For each trial, the report displays the frame loss ratio.

Trial Duration : The time - in seconds - to transmit Y.1731 TST or LBM frames at a given rate and frame size. This is known as a "trial". Valid range is 1 - 1800 with a default of 60 seconds.

Minimum Rate : The minimum rate - in ‰ of the egress port's line rate - to transmit Y.1731 TST or LBM frames at. Valid range is 1 - 1000 with a default of 800 ‰ of the line rate.

Maximum Rate : The highest (and first) rate - in ‰ of the egress port's line rate - to transmit Y.1731 TST or LBM frames at. Valid range is 1 - 1000 with a default of 1000 ‰ of the line rate.

Rate Step : The rate decrement, in ‰ of the egress port's line rate, per trial. Valid range is 1 - 1000 with a default of 5 ‰ of the line rate.

Back-to-Back Test Parameters

Enable : Click to enable the back-to-back sub-test. The back-to-back test aims to measure the network's ability to absorb bursty traffic. The test runs at line rate less 200 Kbps, and bursts of Y.1731 TST or LBM frames are generated a configurable number of times. The duration of a burst is configured in milliseconds, and the time from one burst ends until the next starts is configured through the Dwell Time.

Trial Duration : The time - in milliseconds - to transmit a burst of Y.1731 TST or LBM frames at line rate and frame size. This is known as a "trial". Valid range is 100 - 10000 with a default of 2000 milliseconds.

Trial Count : The number of times to repeat the burst. Valid range is 1 - 100 with a default of 50 times.

Buttons

Apply : If all input parameters are valid, the profile will be saved to non-volatile memory and you will be returned to the RFC2544 Profile Overview page. See the Example below.

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

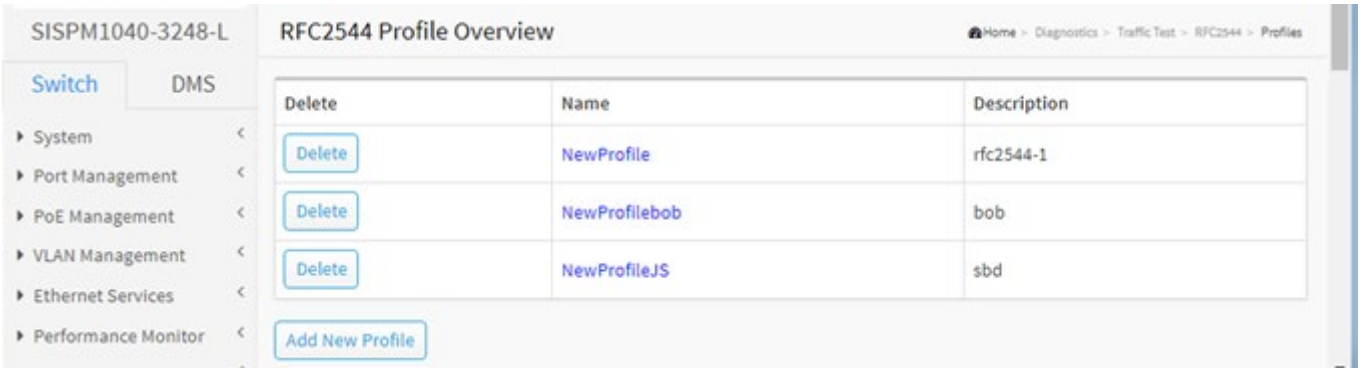
Cancel : Return to the RFC2544 Profile Overview page without creating a new profile.

Messages

Internal Error: Invalid form

A profile with that name already exists

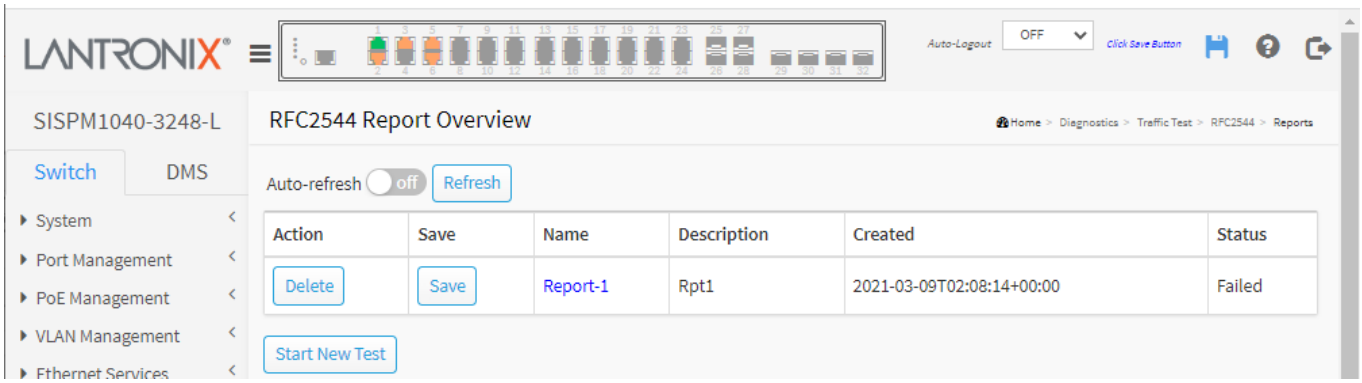
Example



26-6.2.3 RFC2544 Reports

Navigate to the Switch > Diagnostics > Traffic Test > RFC2544 Reports menu path to display the RFC2544 Report Overview page.

This page lets you view currently stored reports and provides options to delete, download, and view them. You can also start execution of a profile on this page.



If no reports are currently stored, the table displays <No test reports>. Otherwise there is a table row for each test report, each containing these elements:

Action : If a test is currently being executed, a Stop button is shown. Clicking the Stop button will cause a request to be sent to gracefully cancel the execution. During this cancellation, the Delete button will be disabled.
At most one test can execute at a time. Once execution of a test is complete, successfully or not, the resulting report is persisted to non-volatile memory. Up to 10 reports can be persisted. New reports will replace the oldest. Only reports stored in non-volatile memory can be erased. This is done with the Delete button.

Save : Test reports can be downloaded and stored on the local computer with the use of the Save button.
The suggested file name will be the report name concatenated with ".txt".

Name : A unique name identifying the report. Click the name to view the report.

Description : The description assigned to the report as entered on the test execution page.

Created : The date and time at which execution started.

Status : The current status of executing a test:

Inactive: Test just initiated, but not started. This is a transitional state that is unlikely to be noticed.

Executing: Test is currently executing. At most one test can execute at a time.

Cancelling: Test has just been stopped by the user. This is a transitional state that is unlikely to be noticed.

Cancelled: Test was stopped by the user and report is stored in non-volatile memory.

Passed: Test passed successfully and the report is stored in non-volatile memory.

Failed: Test failed execution and report is stored in non-volatile memory. Details as to why the test failed are embedded in the report.

Failing: Test failed due to an outside circumstance. This is a transitional state unlikely to be noticed.

Buttons

Start New Test : Initiate execution of a profile. This button is grayed out if a test is already in progress. If no test is currently in progress, click to display the RFC2544 Test Start page as described below.

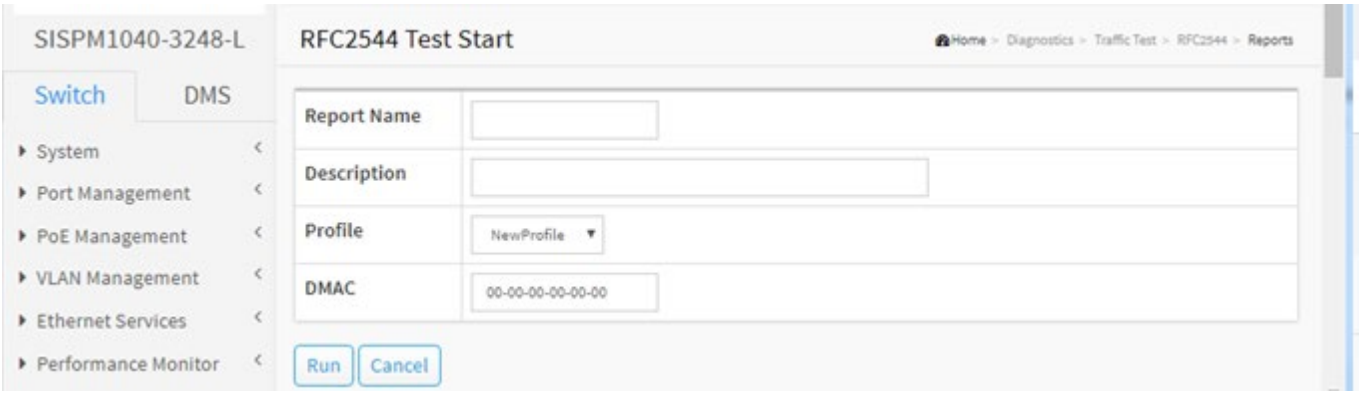
Auto-refresh: Check this box to refresh the page automatically every 3 seconds.

Refresh : Click to manually refresh the page immediately.

26-6.2.4 RFC2544 Test Start

To start an RFC 2544 Test, navigate to the Switch > Diagnostics > Traffic Test > RFC2544 > Reports menu path and press the Start New Test button to display the RFC2544 Test Start page.

This page lets you initiate execution of a profile while naming and describing the resulting report. Once a test is started, a snap-shot of the chosen profile is made, so that subsequent changes in the profile editor won't be reflected in the running test.



Report Name : Each test report must have a name that uniquely identifies it, since it is this name that identifies it in the non-volatile file system. The length must be 1 - 32 characters and each ASCII character must be in the range of 3 - 126 except for /, \", <,>, and \' characters.

Description : This field allows for providing a textual description of the report. Up to 128 characters can be entered with each ASCII character being in the range 32 - 126.

Profile : Select the profile to execute. The drop-down box is populated with the names of the currently defined profiles.

DMAC : This field allows for overriding the destination MAC address specified in the profile.

If left as a zero MAC address, no override will take place, and the DMAC specified in the profile will be used.

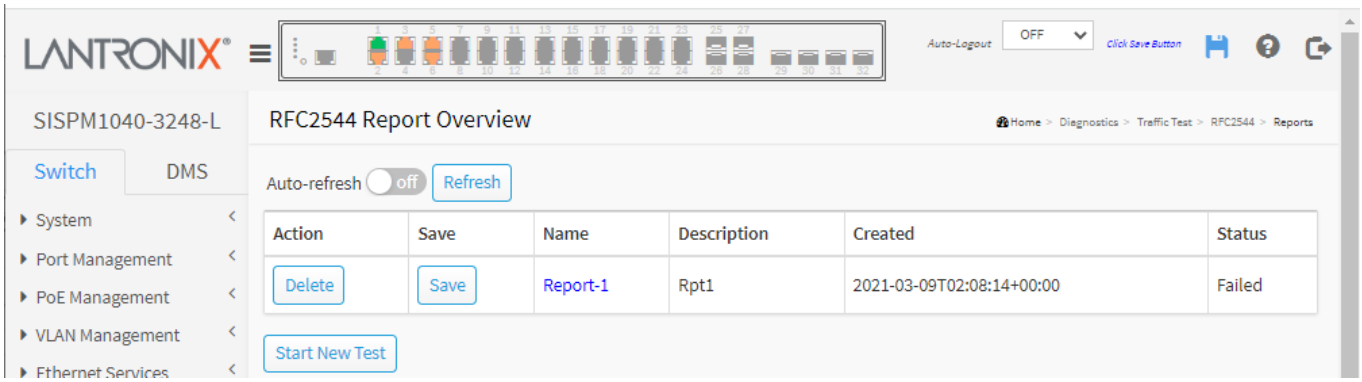
If a non-zero MAC address is entered, it must be a unicast MAC address, and this address will be used in generation of the Y.1731 OAM frames.

Buttons

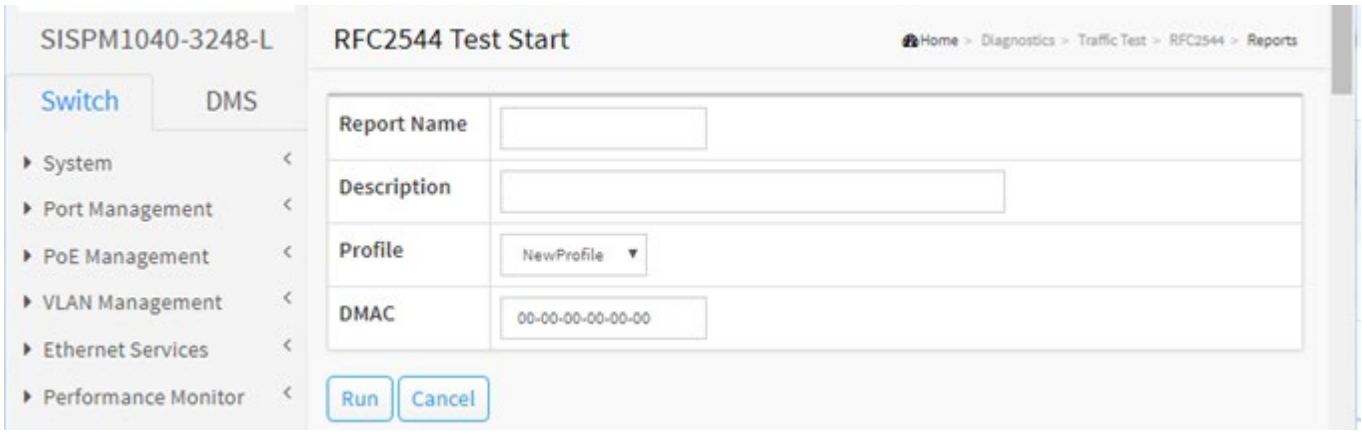
Run : If all input parameters are valid, the test will start executing and you will be returned to the RFC2544 Report Overview page.

Cancel : Return to the RFC2544 Report Overview page without initiating a new test.

RFC2544 Report Overview



Click the Start New Test button to display the RFC2544 Test Start page. This page allows for initiating execution of a profile while naming and describing the resulting report. Once a test is started, a snap-shot of the chosen profile is made, so that subsequent changes in the profile editor won't be reflected in the running test.



Enter the parameters as described below:

Report Name : Each test report must have a name that uniquely identifies it, since it is this name that identifies it in the non-volatile file system. The length must be 1 - 32 characters long with each ASCII character in the range 33 - 126 except for /, \", <,>, and \' characters.

Description : This field lets you enter a text description of the report. Up to 128 characters can be entered with each ASCII character in the range of 32 - 126.

Profile : Select the profile to execute. The drop-down box is populated with the names of the currently defined profiles. If no profiles are defined, the text "<No Profiles>" is displayed.

DMAC : This field allows for overriding the destination MAC address specified in the profile.

If left as a zero MAC address, no override will take place, and the DMAC specified in the profile will be used.

If a non-zero MAC address is entered, it must be a unicast MAC address, and this address will be used in generation of the Y.1731 OAM frames.

Buttons

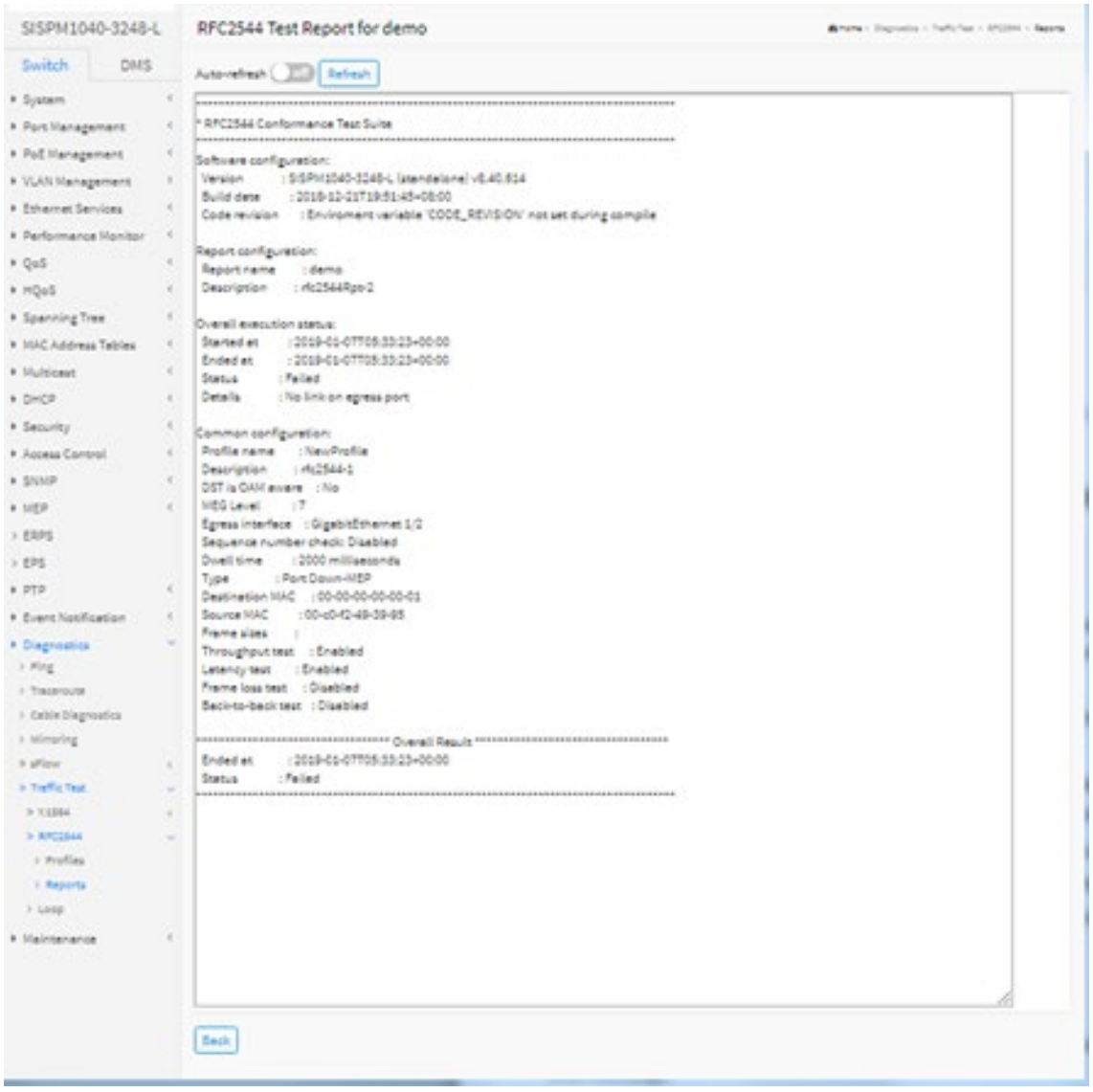
Run : If all input parameters are valid, the test will start executing and you will be returned to the RFC2544 Report Overview page.

Cancel : Return to the RFC2544 Report Overview page without initiating a new test.

Messages

Message : *A report with that name already exists*

Sample RFC2544 Report



Click the **Back** button to return to the previous page.

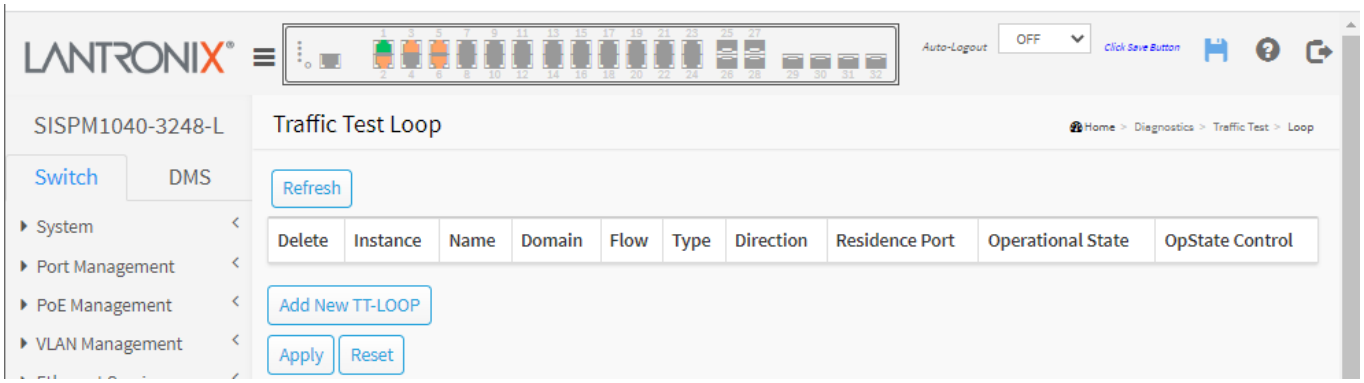
RFC2544 Report Parameters:

```
*******************************************************************************
* RFC2544 Conformance Test Suite
*******************************************************************************
Software configuration:
  Version             : SISPM1040-3166-L (standalone) v8.40.1106
  Build date          : 2019-01-22T15:39:31+08:00
  Code revision       : Enviroment variable 'CODE_REVISION' not set during compile

Report configuration:
  Report name         : demo
  Description         : rfc2544Rpt-1

Overall execution status:
  Started at          : 2016-01-03T20:55:35+00:00
  Ended at            : 2016-01-03T20:57:39+00:00
  Status              : Failed

Common configuration:
  Profile name        : NewProfile
  Description         : rfc2544-1
  DST is OAM aware    : No
  MEG Level           : 7
  Egress interface    : GigabitEthernet 1/1
  Sequence number check: Disabled
  Dwell time          : 2000 milliseconds
  Type                : Port Down-MEP
  Destination MAC     : 00-00-00-00-00-01
  Source MAC          : 00-c0-f2-49-3a-21
  Frame sizes         : 64 128 256 512 1024 1280 1518 2000
  Throughput test     : Enabled
  Latency test        : Disabled
  Frame loss test     : Disabled
  Back-to-back test   : Disabled

******************************** Throughput Test ********************************
Throughput configuration:
  Trial duration      : 60 seconds
  Minimum rate        : 800 permille
  Maximum rate        : 1000 permille
  Accuracy            : 2 permille
  Allowed frame loss  : 0 permille

Throughput status:
  Started at          : 2016-01-03T20:55:35+00:00
  Ended at            : 2016-01-03T20:57:39+00:00
  Status              : Failed
  Details             : Allowed background traffic frame loss exceeded

Note that the "Appl. TxRate" may differ from the "Actual TxRate" depending on the
port configuration. In this case the "Actual TxRate" represents the resulting
throughput rate for a successful test.

Frame   Appl.   Actual  Actual  Actual   Actual   Tx        Rx        Frame Status
Size    TxRate  TxRate  RxRate  TxRate   RxRate   Frames    Frames     Loss
[bytes] [Mbps]  [Mbps]  [Mbps]  [fps]    [fps]                       [%]
------- ------- ------- ------- -------- -------- ---------- ---------- ----- ------
     64   799.9   799.9     0.0  1190472        0   71430746          0 100.0 FAIL

******************************** Overall Result ********************************
  Ended at            : 2016-01-03T20:57:39+00:00
  Status              : Failed
*******************************************************************************
```

26-6.3 Traffic Test Loop

Navigate to the Switch > Diagnostics > Traffic Test > Loop menu path to display the Traffic Test Loop page where you can create Traffic Test Loop (TT-LOOP) instances.

TT-LOOP (Traffic Test Loop) is a firmware module that provides methods to perform tests that are defined in IETF RFC 2544 (Benchmarking Methodology for Network Interconnect Devices) and ITU-T Y.1564 (remote end).



Click the Add New TT-LOOP button and enter the parameters as shown and described below.

Delete : This box is used to mark a TT-LOOP for deletion in next Save operation.

Instance : The ID of the TT-LOOP. Click on the ID of a TT-LOOP to enter the instance's configuration page.

Name : This is a configurable name of the instance.

Domain : The domain for the TT-LOOP (Port, EVC, or VLAN):

Port: A TT-LOOP in the Port Domain will loop all frames (including OAM frames) on the given port. The 'Flow' parameter identifies the port.

Evc: A TT-LOOP in the EVC Domain will loop all frames classified as belonging to the EVC. Any other frame will not be affected. The 'Flow' parameter identifies the EVC. The EVC must be created.

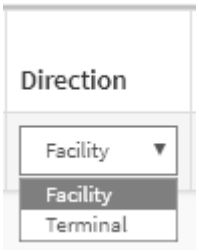
VLAN: A TT-LOOP in the VLAN Domain will loop all frames with a given VLAN tag. The 'Flow' parameter identifies the VLAN. Any other frame will not be affected.

Flow : The flow instance number related to this TT-LOOP instance - depending on the 'Domain'. See 'Domain'.

Type : At the dropdown select either ***Mac-Loop*** or ***Oam-Loop***. Note that the OAM Loop type is currently only supported in an EVC domain.

MAC Loop: This TT-LOOP is the MAC looping type. All frames in the flow are looped with MAC swap.

OAM Loop: This TT-LOOP is the OAM looping type. It is Y.1731 OAM aware and is looping LBM->LBR and DMM->DMR.



Direction : At the dropdown select either ***Facility*** or ***Terminal***. Note that currently ***Terminal*** Loop is only supported in the EVC domain.

Facility: This TT-LOOP is pointing out to the port. Looping is done from ingress to egress.

Terminal: This TT-LOOP is pointing into the forwarding plane. Looping is done from egress to ingress.

Residence Port : The port where TT-LOOP is resident - see 'Direction'. For an EVC TT-LOOP the port must be a port in the EVC. For a VLAN TT-LOOP the port must be a VLAN member.

Operational State : can be operationally Up or Down:

Up: Instance Operational State is UP - all resources are available and allocated

Down: Instance Operational State is DOWN - not all resources are available or administrative state is disabled.

OpState Control : Indicate what mechanism is controlling the operation state of this loop:

Static: The loop is controlled by management commands (i.e., the operational state is fully controlled by the administrative state).

Latch.LB: The loop is controlled by the MEF 46 Latching Loopback (LL) protocol. The administrative state can control whether the loop responds to LL PDUs but the loop will only enter the active state if a valid LLM Activate PDU is received from a remote host.

Buttons

Add New TT-LOOP: Click to add a new TT-LOOP entry.

Refresh : Click to manually refresh the page immediately.

Apply : Click to save changes. Only one TT-LOOP can be added for each Save operation.

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

Usage Notes

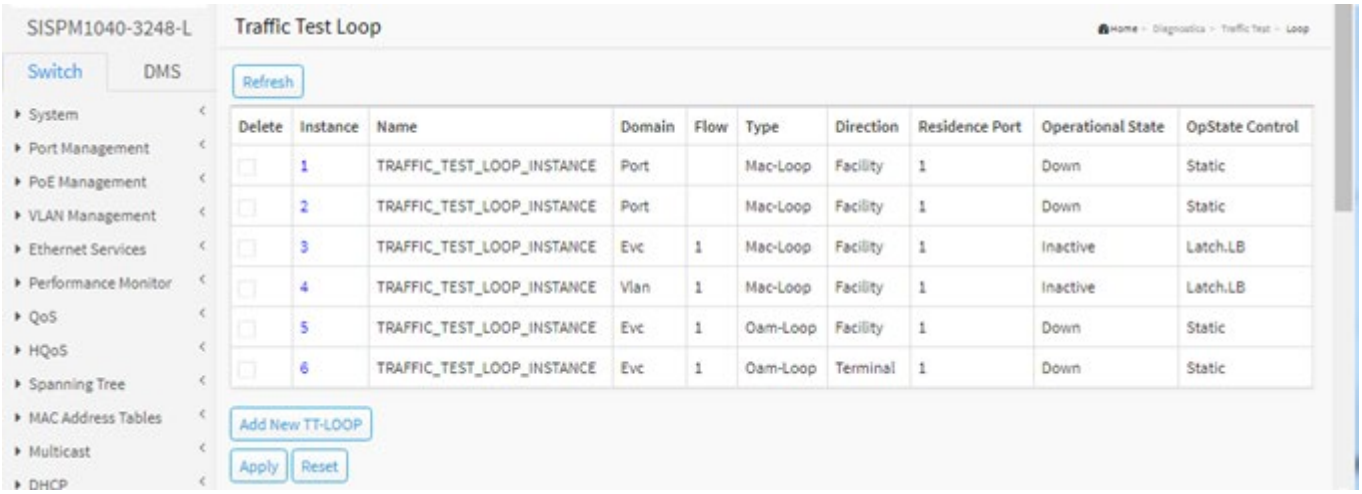
Terminal Loop on UNI With Multiple NNIs : A Terminal loop may be created on a UNI in an EVC with multiple NNIs. A frame received by one of the NNIs will then be looped back to all NNIs. If this behavior is not desired, you can avoid this by creating static MAC table entries that direct the looped frames to the desired port.

Messages

Configuration not supported displays if you entered an unsupported configuration (e.g., if Type = Oam-Loop or Direction = Terminal).

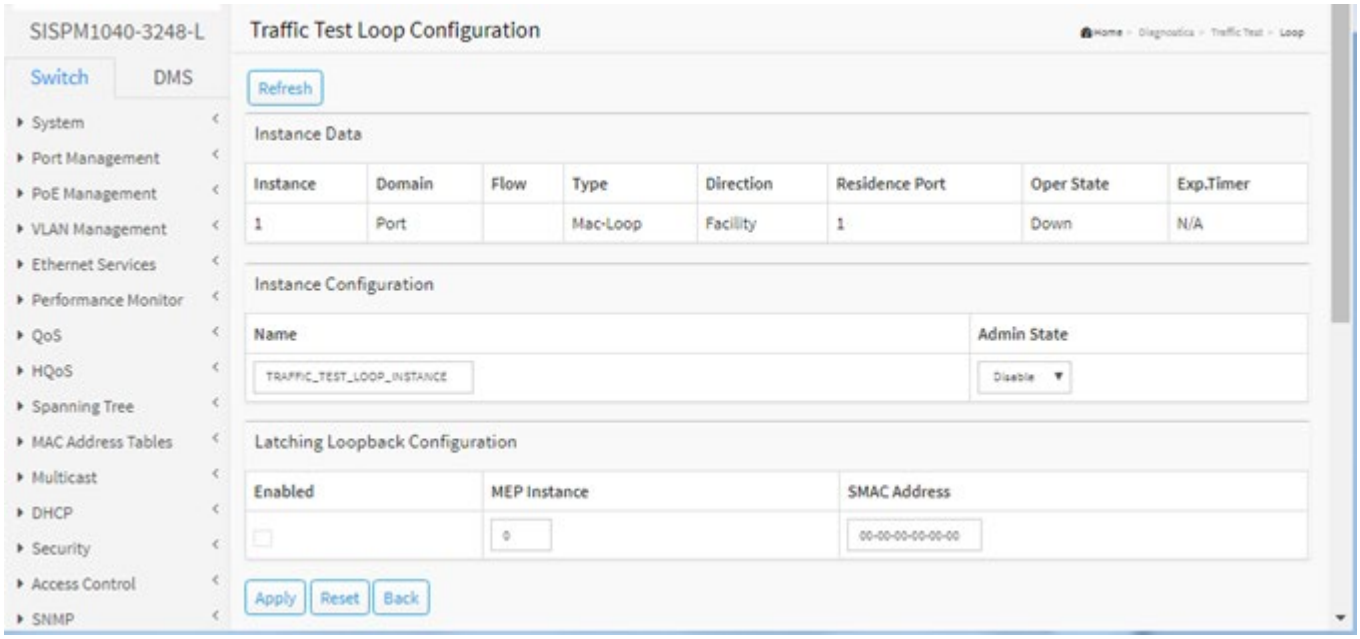
Example

The sample Traffic Test Loop page below shows six Traffic Test Loop instances configured.



Traffic Test Loop Configuration

Click a linked Instance number to display the instance's Traffic Test Loop Configuration page. This page lets you view and configure the selected TT-LOOP Instance parameters as shown and described below.



Instance Data

Instance : The ID of the TT-LOOP.

Domain : Port, EVC, or VLAN (see the description above).

Flow : The flow instance number related to this TT-LOOP instance - depending on the 'Domain'. See 'Domain'.

Type : Either Mac-Loop or Oam-Loop (see the description above).

Direction : Either Facility or Terminal (see the description above).

Residence Port : The port where TT-LOOP is resident - see 'Direction'.

Oper State : Can be operationally Up or Down (see the description above).

Exp.Timer : The current value of the Latching Loop expiry timer in seconds. Only available when the Latching Loop function has been enabled for this loop instance. Otherwise displays 'N/A'.

Instance Configuration

Name : See the description above.

Level : The EVC domain OAM aware loop MEG level. Only available when loop type is "OAM Loop".

Subscriber : Control how the loop behaves in the subscriber sub-domain of the EVC.
Only available when loop domain is "EVC".

None: This EVC loop instance operates purely in the main EVC domain. It can be associated with either a down-MEP or an up-MEP.

All: This EVC loop instance operates in the EVC subscriber sub-domain and handles all frames. It can be associated with either a down-MIP or an up-MIP on an EVC UNI port.

Untagged: EVC loop instance operates in the EVC subscriber sub-domain and handles all untagged frames. It can be associated with either a down-MIP or an up-MIP on an EVC UNI port. VID EVC loop instance operates in the EVC subscriber sub-domain and handles all frames (single-)tagged with the specified VID. It can be associated with either a down-MIP or an up-MIP on an EVC UNI port.

VID : This parameter specifies the VID used when the Subscriber parameter is set to "VID". The value is not used for any other Subscriber settings.

Admin State : This is the configuration of the two possible Administrative States.

Enabled: Administrative State is Enabled - "active" and operational state can change to 'UP' if possible.

Disabled: Administrative State is Disabled - not "active" but still created - all resources are deleted.

Latching Loopback Configuration : This section contains configuration options for the MEF 46 Latching Loopback function. The Latching Loopback function can be enabled on any TT-LOOP instance.

Enabled : Check the box to enable the Latching Loopback (LL) function for the TT-LOOP instance.

MEP Instance : Defines the MEP (or MIP) instance which handles reception and transmission of LL PDUs.
The indicated MEP instance may not exist when the TT-LOOP instance is configured but PDUs destined to the TT-LOOP instance will obviously not be handled until the MEP instance is created. **Note** that MEP ID for Latching Loopback is not valid.

SMAC Address : Defines the source MAC address from which incoming LLM PDUs will be accepted.

Buttons

Refresh : Click to manually refresh the page immediately.

Apply : Click to save changes.

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

Back : Click to go back to the Traffic Test Loop page.

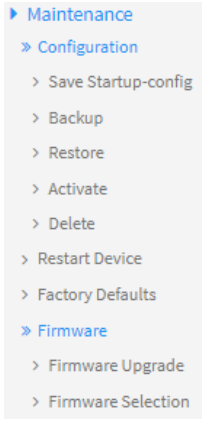
Messages

Configuration not supported

Residence port is not found valid

EVC is not found valid

Chapter 27 - Maintenance



This section provides Maintenance configuration tasks including Save, Backup, Restore, Activate, Delete, Restart, Factory Defaults, and Firmware upgrade and selection.

27-1 Configuration

The switch stores its configuration in a number of files in text format. The files are either virtual (RAM-based) or stored in flash on the switch.

The system files are:

- **running-config**: A virtual file representing the current 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.

27-1.1 Save startup-config

This copies running-config to startup-config; the current active configuration will be used at the next reboot.

To save running configuration in the web UI:

1. Click Maintenance, Configuration, and Save Startup-config.
2. Select a file name to save (startup-config or enter a filename).
3. Click the Save Configuration button.

Figure 27-1.1: Save Startup Configuration

Button

Save Configuration : Click to save configuration; the running configuration will be written to flash memory for system boot up to load this startup configuration file. When successfully completed, the message "*save running config to startup-config successfully*." displays. Click the **OK** button to clear the message.

27-1.2 Backup

This page lets you export the Switch Configuration for maintenance needs. Any current configuration files will be exported as text format.

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

It is possible to transfer any of the files on the switch to the web browser. Download of running-config may take a little while to complete, as the file must be prepared before backup.

To back up a configuration in the web UI:

1. Click Maintenance, Configuration, and Backup.
2. Select a file name to save.
3. Click the Download Configuration button.

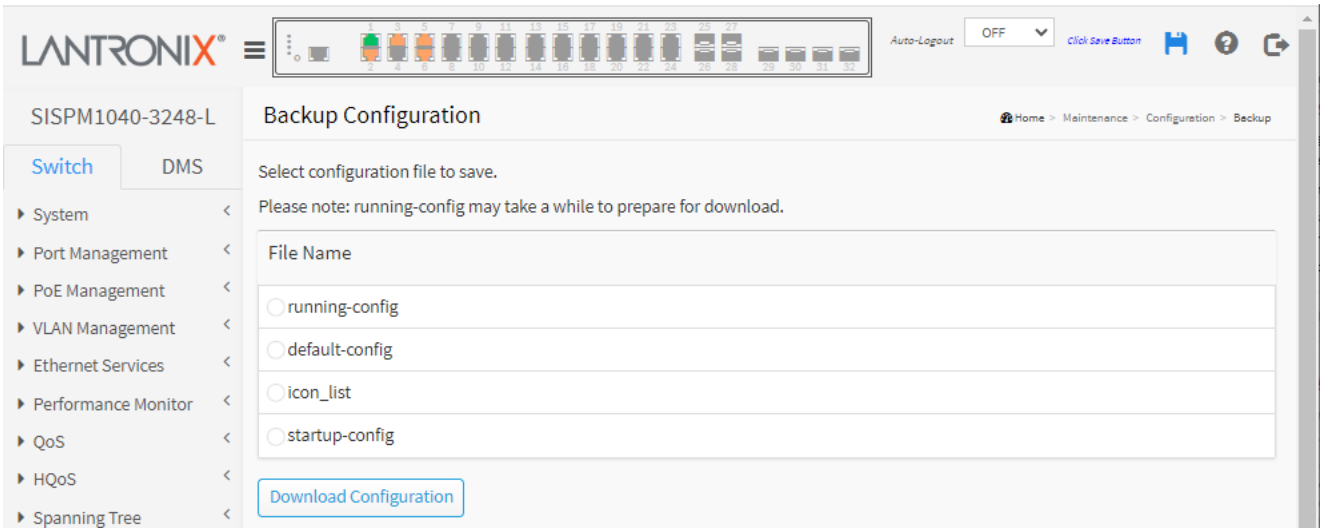


Figure 27-1.2: Backup Configuration

Parameter descriptions :

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

default-config : A read-only file with vendor-specific configuration. This file is read when the system is restored to default settings.

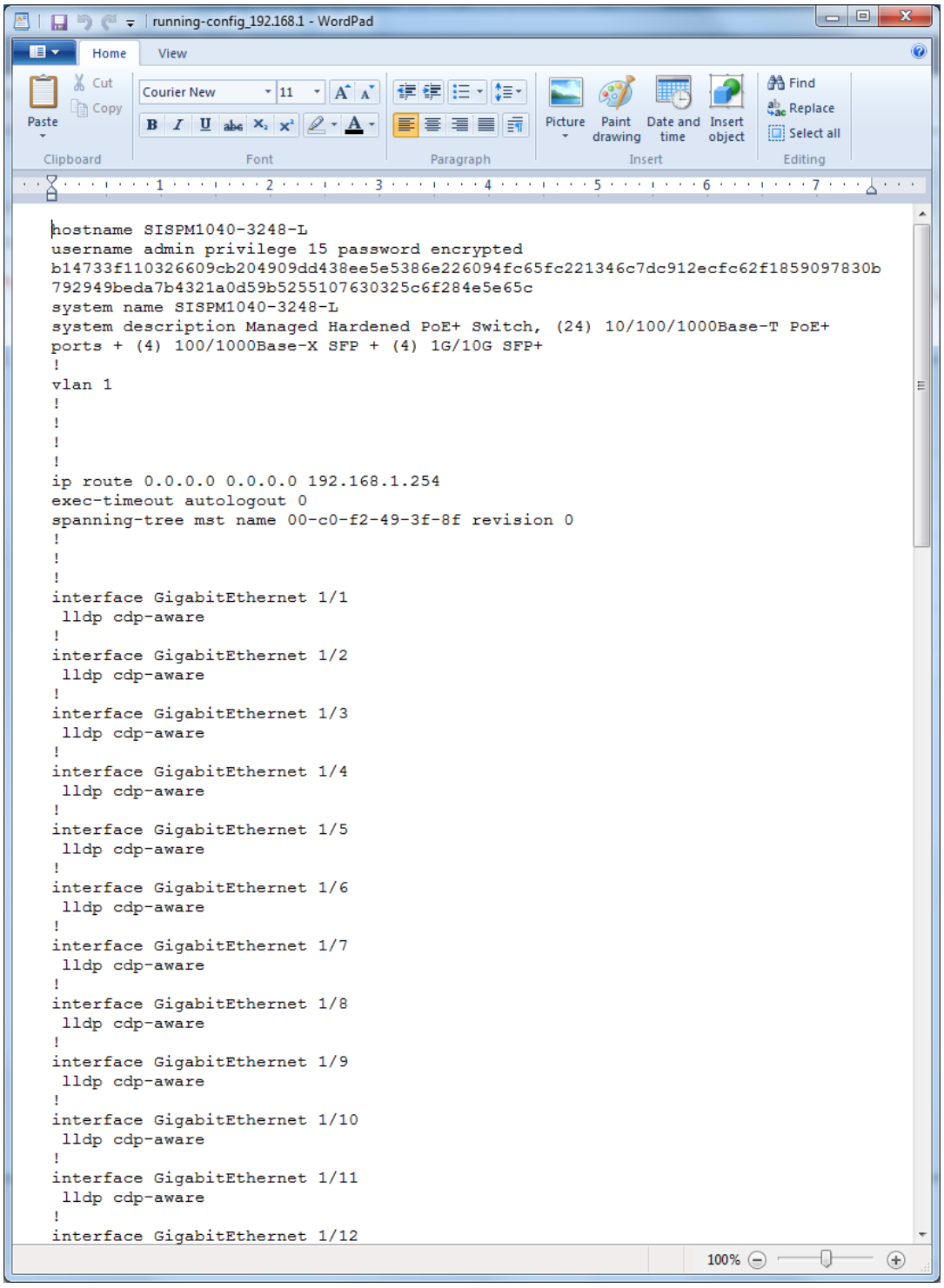
icon_list: a list of image files.

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

Buttons

Download Configuration : Click the button then the switch will start to transfer the configuration file to your workstation.

Example: default-running-config file page



27-1.3 Restore

It is possible to import a file from the web browser to all the files on the switch, except default-config, which is read-only. Select the source file to restore and select the destination file on the target. If the destination is running-config, the file will be applied to the switch configuration. This can be done in two ways:

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

To restore a configuration in the web UI:

1. Click Maintenance, Configuration, and Restore
2. Click the Choose File button.
3. Select a file name to restore.
4. Click the Upload Configuration button.

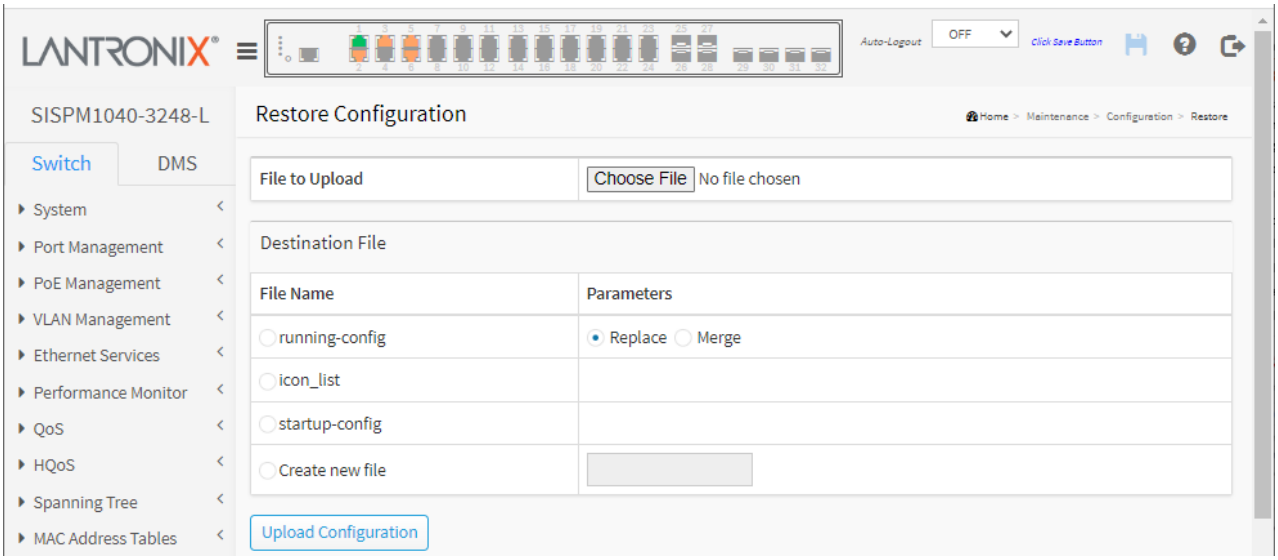


Figure 27-1.3: Restore Configuration

Parameter descriptions:

File to Upload : Click the Choose File button and navigate to and choose a file to restore.

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

Replace: The current configuration is fully replaced with the configuration in the uploaded file.

Merge: The uploaded file is merged into running-config.

icon_list: a list of image files.

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

Create new file : Enter a file name to create a new file.

Buttons

Choose File :Click the button to search the configuration text file and filename.

Upload Configuration : Click the button to start transfer the source file to the destination file.

27-1.4 Activate

It is possible to activate any of the configuration files present on the switch, except for running-config which represents the currently active configuration. Select a configuration file to activate and click the Activate Configuration button. **Note**: the previous configuration will be completely replaced, potentially leading to loss of management connectivity. **Note**: The activated configuration file will NOT be saved to startup-config automatically. Note that if the configuration changes IP settings, management connectivity may be lost.

To activate a configuration file in the web UI:

1. Click Maintenance, Configuration and Activate.
2. Select a file name to activate.
3. Click the Activate Configuration button.

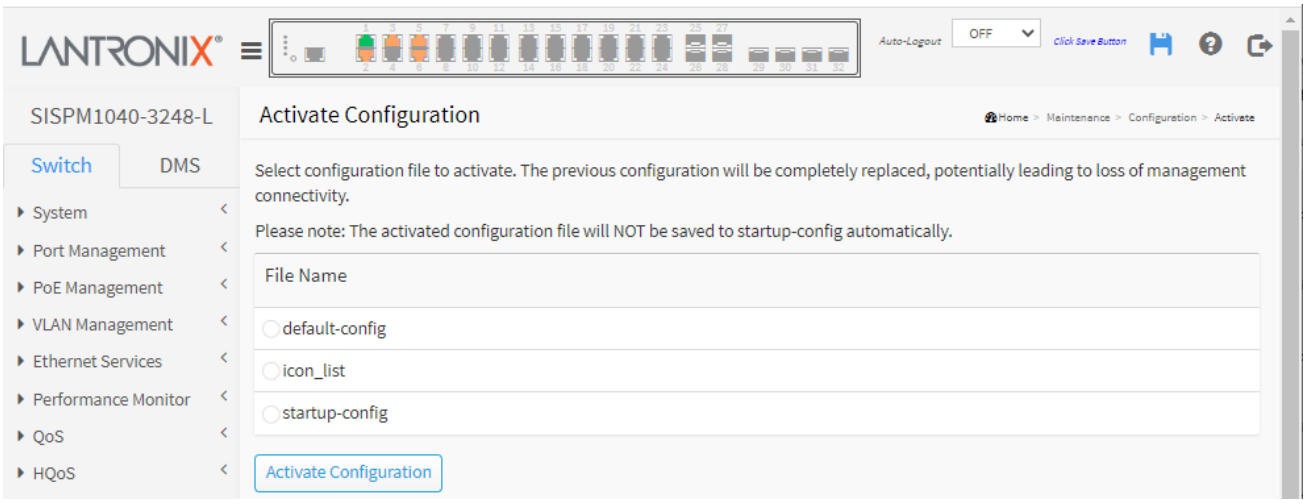


Figure 27-1.4: Activate Configuration

Parameter descriptions:

Filename: Check a radio button to activate:

default-config : A read-only file with vendor-specific configuration. This file is read when the system is restored to its default settings.

icon_list: a list of image files.

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

Buttons

Activate Configuration : Click the button then the selected file will be activated to be the switch's running configuration.

Messages

Status

Warning: Syntax check completed with errors; configuration has not been activated.

```
% Error in file startup-config, line 41:

ip source binding interface GigabitEthernet 1/2 10 192.168.1.77 11-22-33-44-55-
                                                                              ^
66

% Invalid word detected at '^' marker.

% Error in file startup-config, line 42:

ip source binding interface GigabitEthernet 1/3 20 192.168.1.77 11-22-33-44-55-
                                                                              ^
77

% Invalid word detected at '^' marker.

% Error in file startup-config, line 43:

ip source binding interface GigabitEthernet 1/4 30 192.168.1.77 11-22-33-44-55-
                                                                              ^
88

% Invalid word detected at '^' marker.

% Syntax check done, 3 problems found.
```

27-1.5 Delete

It is possible to delete any of the writable files stored in flash, including startup-config. If this is done and the switch is rebooted without a prior save operation, this effectively resets the switch to its default configuration.

To delete a configuration file in the web UI:

1. Click Maintenance, Configuration, and Delete.
2. Select a configuration file name to delete.
3. Click the Delete Configuration File button.

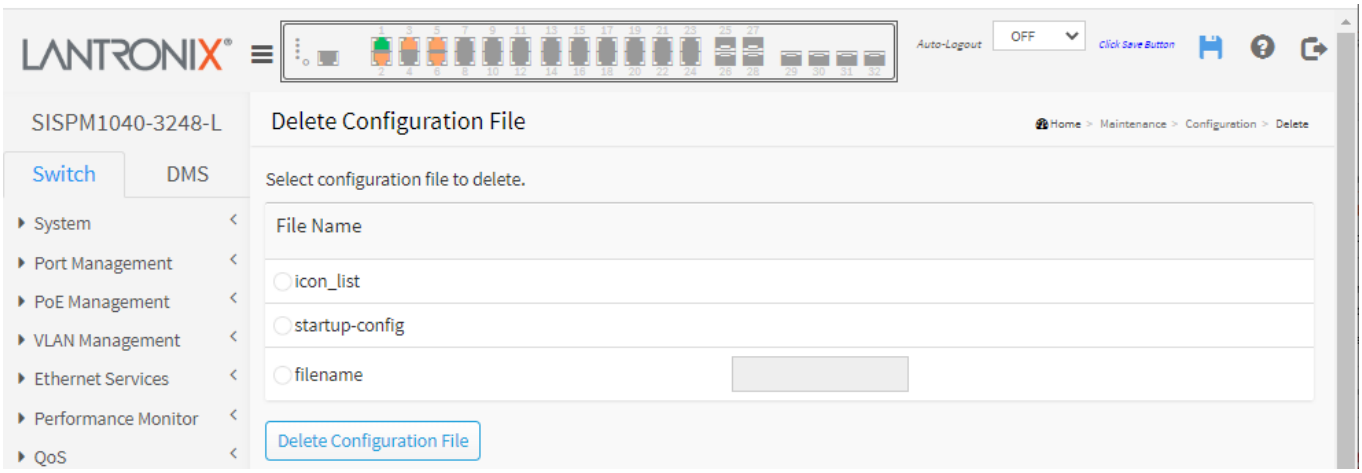


Figure 26-1.5: Delete Configuration File

Parameter descriptions:

File Name: select the desired filename:

icon_list: a list of image files.

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

filename: Lets you enter the name of an existing file to delete.

Buttons

Delete Configuration File: Click the button. At the confirmation prompt "*Are you sure you want to delete icon_list*?" click the OK button, the selected file will then be deleted.

27-2 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.

You can use the Always On PoE function so that when the switch warm restarts, it will continue supplying PoE power to the PDs.

To restart the device in the web UI:

1. Click Maintenance and Restart Device.
2. Check or uncheck the Always On PoE button.
3. Click Yes at the *Are you sure…* prompt.

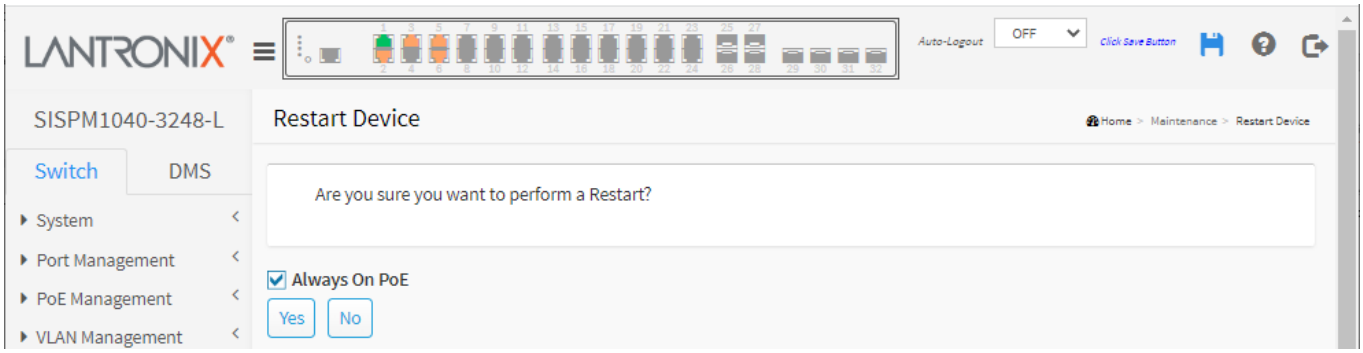


Figure 27-2: Restart Device

Parameter descriptions :

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

Always On PoE : Check this button so when the switch warm restarts, it continues supplying PoE power to PDs.

Buttons

Yes : Click to restart the device.

No : Click to cancel the operation.

27-3 Factory Defaults

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

To restore a Factory Defaults in the web UI:

1. Click Maintenance and Factory Defaults.
2. Check or uncheck Keep IP setup.
3. Click Yes at the *Are you sure…* prompt.

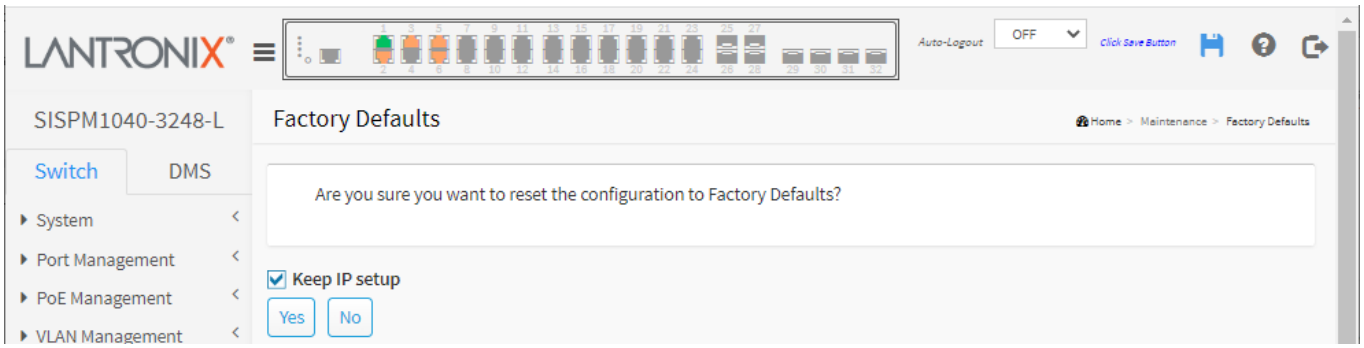


Figure 26-3: Factory Defaults

Buttons

Keep IP Setup : Check the checkbox if you want to keep the IP setup after resetting to factory defaults.

Yes : Click to reset the configuration to Factory Defaults.

No : Click to cancel the operation.

27-4 Firmware

This section describes how to upgrade (update) Firmware and lets you revert to the alternate firmware image.

27-4.1 Firmware Upgrade

This page lets you update the switch firmware. You can use the Always On PoE function so that when the switch warm restarts, it will retain PoE supply to the PDs.

To update firmware of the device in the web interface:

1. Click Maintenance, Firmware and Firmware Upgrade.
2. Click the Choose File button.
3. Navigate to, select, and open a firmware file.
4. Check or uncheck the Always On PoE checkbox.
5. Click the Upload button.

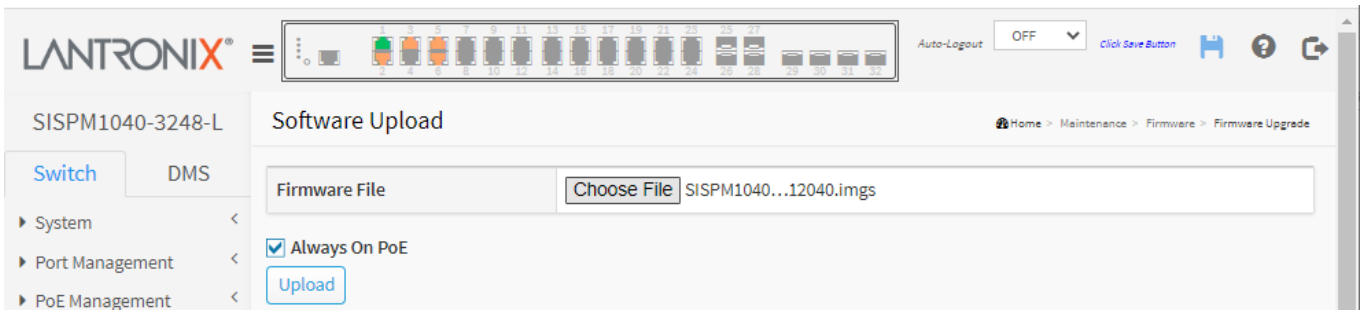


Figure 27-4.1 Firmware Upgrade

Parameter descriptions:

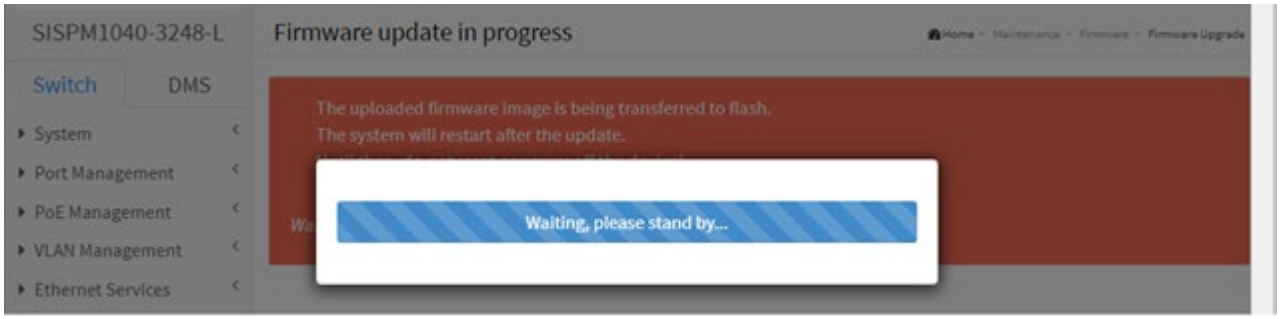
Choose File: Click the button to browse to and select a firmware file to upload. The format *is SISPM1040-3248-L_v8.50.0149_CM_202412040.imgs*.

Always On PoE : Check this button so when the switch warm restarts, it continues supplying PoE power to PDs.

Buttons

Upload: Click to upgrade (update) Firmware.

Messages: Firmware update in progress:



27-4.2 Firmware Selection

This page provides information about the active and alternate (backup) firmware images in the device and allows you to activate the alternate image. The web page displays two tables with information about the active and alternate firmware images.

To show the Firmware information or swap booting firmware in the web UI:

1. Click Maintenance, Firmware, and Firmware Selection to display the Software Image Selection page.
2. Click the Activate Alternate Image button.
3. At the *Are you sure …* confirmation prompt click OK or Cancel.

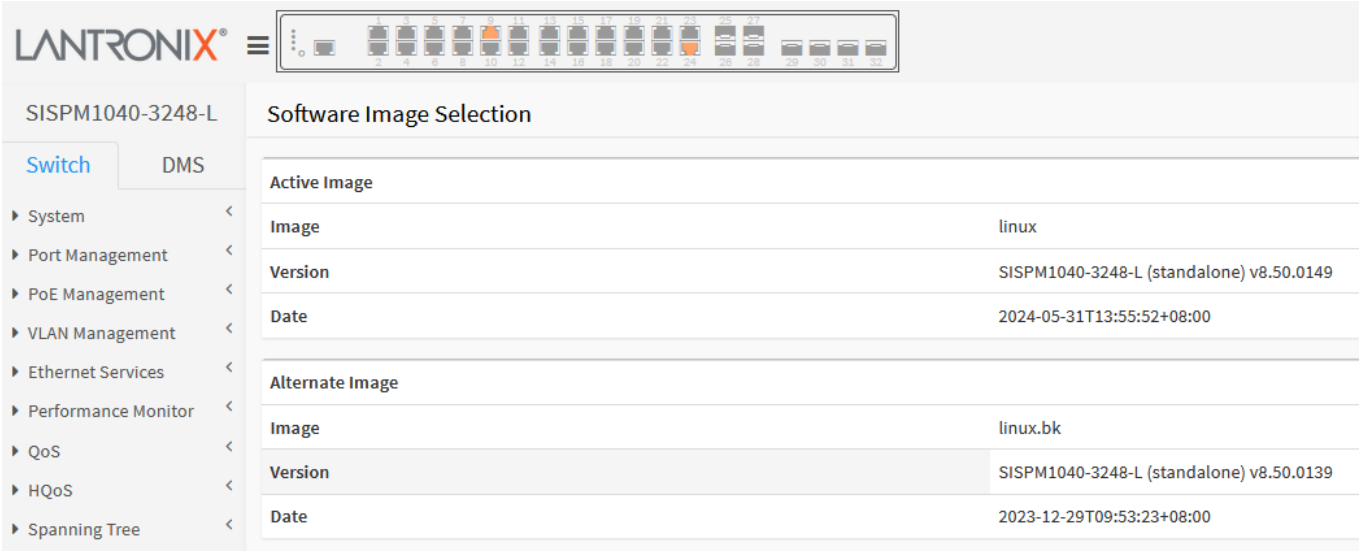


Figure 26-4.2 Software Image Selection

Parameters:

Image : The file name of the firmware image, from when the image was last updated (e.g., *linux* or *linux.bk*).

Version : The version of the firmware image (e.g., *SISPM1040-3248-L (standalone) v8.50.0149*).

Date : The date and time when the firmware was produced (e.g., *2024-05-31T13:55:52+08:00*).

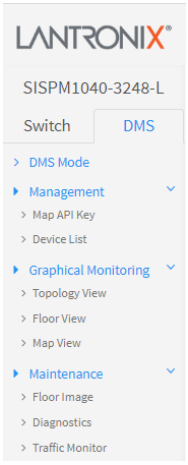
Buttons

Always On PoE : Check this button so when the switch warm restarts, it continues supplying PoE power to PDs.

Activate Alternate Image: Click to use the Alternate Image. This button may be disabled depending on system state.

Cancel: Cancel activating the alternate image. Navigates away from this page.

Chapter 28 - DMS (Device Management System)



28-1 About DMS

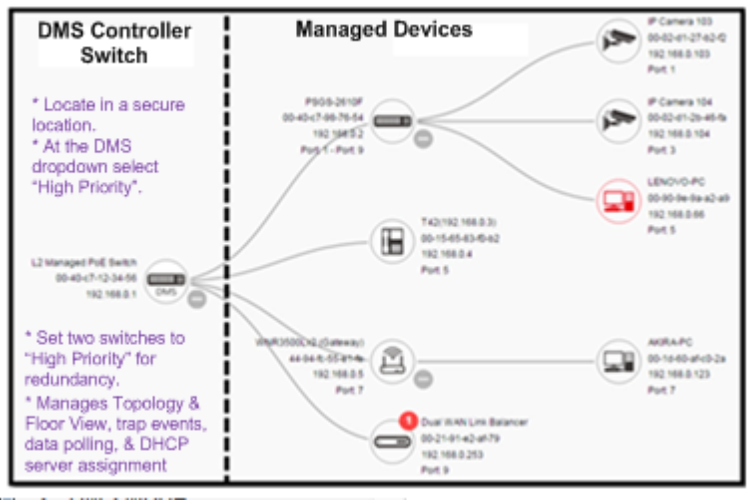
The Lantronix DMS (Device Management System) is an intelligent management tool embedded in the switch to intuitively help IT/TS in reducing support time, cost, and effort. In the SISPM1040-3xxx-L main menu pane on the left, navigate to the DMS tab to display the main DMS features (DMS Mode, Management, Graphical Monitoring, and Maintenance).

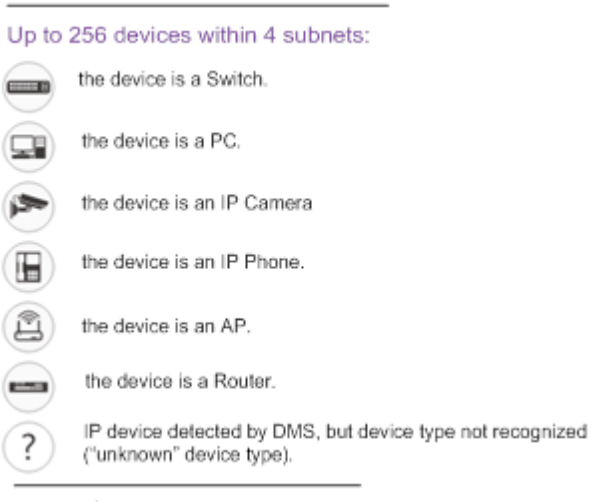
DMS features include:

- DMS automatically discovers and displays all devices connected to the switch using standard networking protocols such as LLDP, UPnP, ONVIF, etc.
- DMS supports up to 256 devices within four subnets.
- DMS operates via an intuitive web GUI to allow you to:
  - Power down the IP cameras, NVRs, or any PoE devices.
  - Remotely identify the exact cable break location.
  - Detect abnormal traffic issues on IP cameras/NVR.
  - Monitor devices' status (e.g., link up, PoE power, traffic, etc.).
  - Configure VLAN/QoS intuitively for better solution quality/reliability.

28-2 DMS Mode - DMS Controller Switch

- 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.





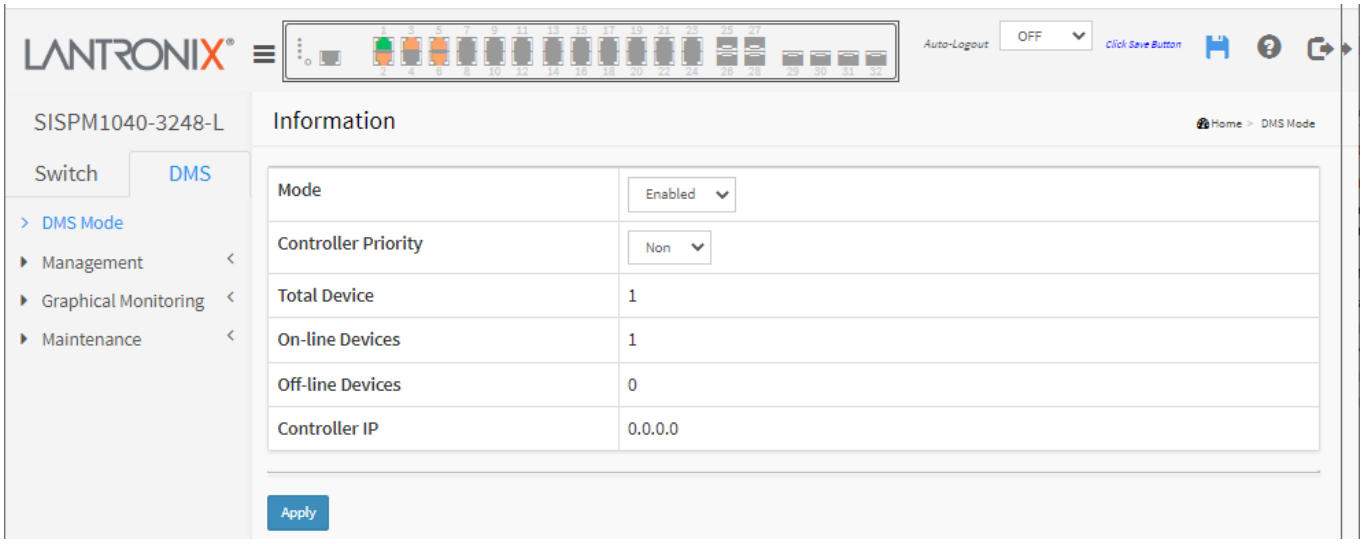
28-3 DMS Controller Switch and Managed Devices

Note:

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.
   b. The DMS Controller Switch will Collect, Poll, and Sync DMS information, and act as the Event Notification control center to manage all device information.

28-4 DMS > DMS Mode

Click on DMS Mode to display the DMS Information page:



Parameter Descriptions:

Mode : Enable or Disable the DMS function globally. The default is Enabled.

Controller Priority: Choose "Controller Priority" when enabling DMS; this sets the priority to change the control level of the switch.

High: Sets level of the switch to the highest level of control (DMS Controller switch).

Mid: Sets the switch to a medium level of control.

Low: Sets the switch to a low level of control.

Non: If you choose "Non", the switch will never become the controller (default).

Total Device : Shows how many IP devices are detected and displayed in Topology View.

On-Line Devices : Shows how many IP devices on-line in the Topology View.

Off-Line Devices : Shows how many IP devices off-line in the Topology View.

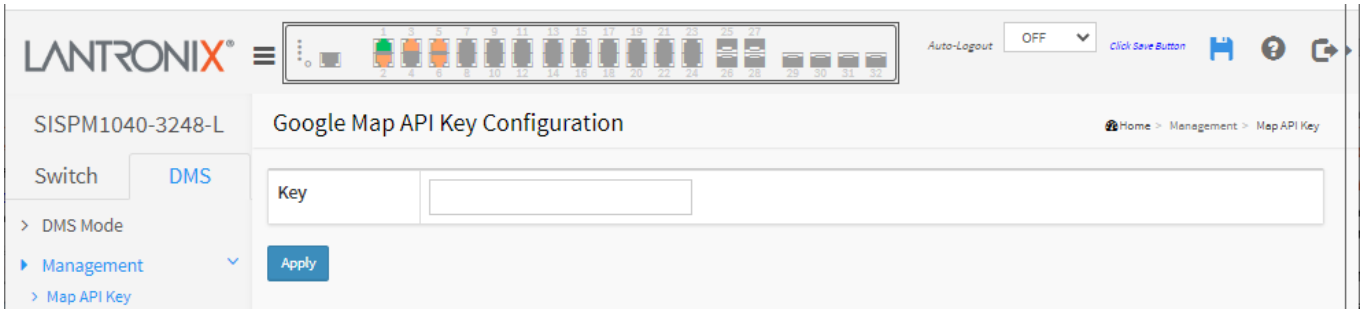
Controller IP : Shows the Master IP address (the IP address of the DMS Controller Switch).

Buttons

Apply : Click to save changes.

28-5 DMS > Management > Map API Key

This page lets you get the Google Map API Key from https://developers.google.com/maps/documentation/directions/get-api-key to use DMS Map View for enterprise applications. Follow the on-screen instructions.



Parameter descriptions:

Key : Specify the Google API Key.

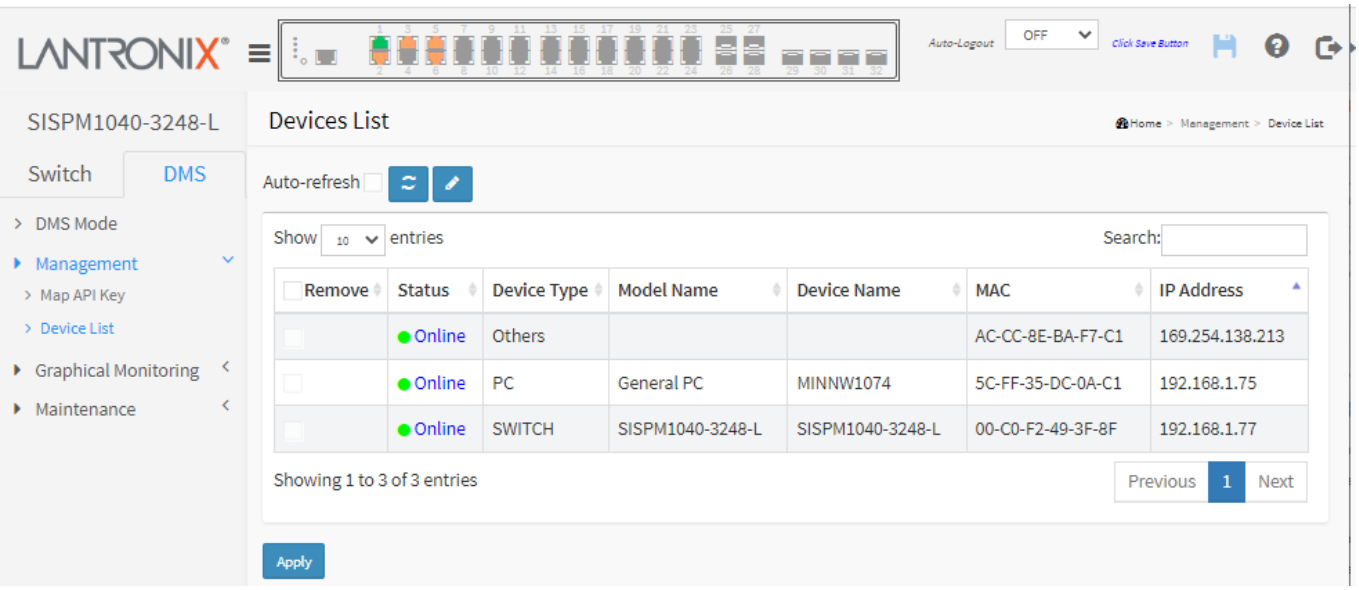
Buttons

Apply : Click to save changes.

Message: *This page can't load Google Maps correctly.*

28-6 DMS > Management > Device List

This page provides an overview of the devices list.



Remove : Check to remove an off-line device from the list.

Status : Device Online or Offline. Click the linked text to run diagnostics at Maintenance > Diagnostics.

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.

Edit Device Name : Lets you edit the Device Name field. This field only displays after you click the 'Edit Device Name' ( ) icon.

MAC : The MAC address of the device.

IP Address : The IP address of the network connectivity devices.

Edit Http Port : Lets you edit the Http Port field. This field only displays after you click the 'Edit Device Name' ( ) icon.

Version : Lets you edit the Version field. This field only displays after you click the 'Edit Device Name' ( ) icon.

Edit User Name : Lets you edit the User Name field. This field only displays after you click the 'Edit Device Name' ( ) icon.

Edit User Password : Lets you edit the User Password field. This field only displays after you click the 'Edit Device Name' ( ) icon.

Buttons

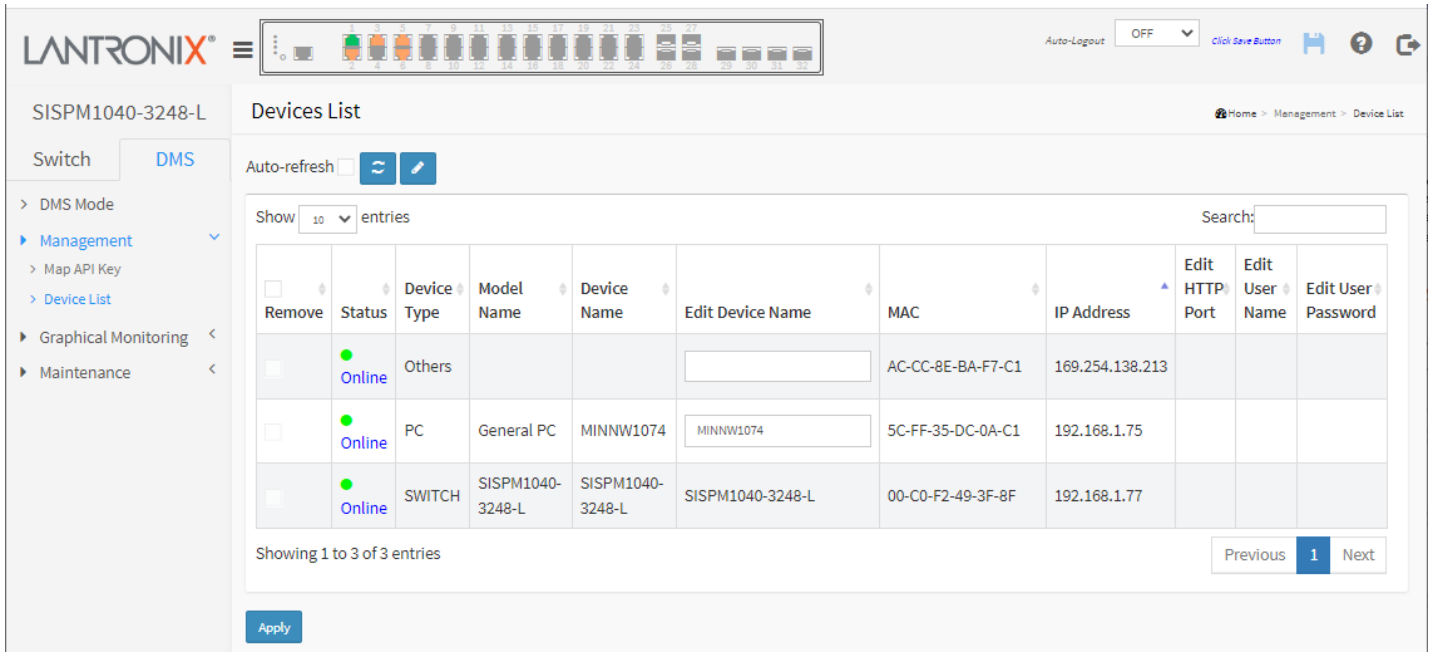
Auto-refresh: Check this box to refresh the page automatically every 3 seconds.

Refresh : Refreshes the displayed table starting from the input fields.

Edit Device Name : Click to add the input fields for editing the device names and the Http ports (see sample screen below).

Apply : Click to save changes.

Added input fields for editing after clicking the **Edit Device Name** icon ( ).

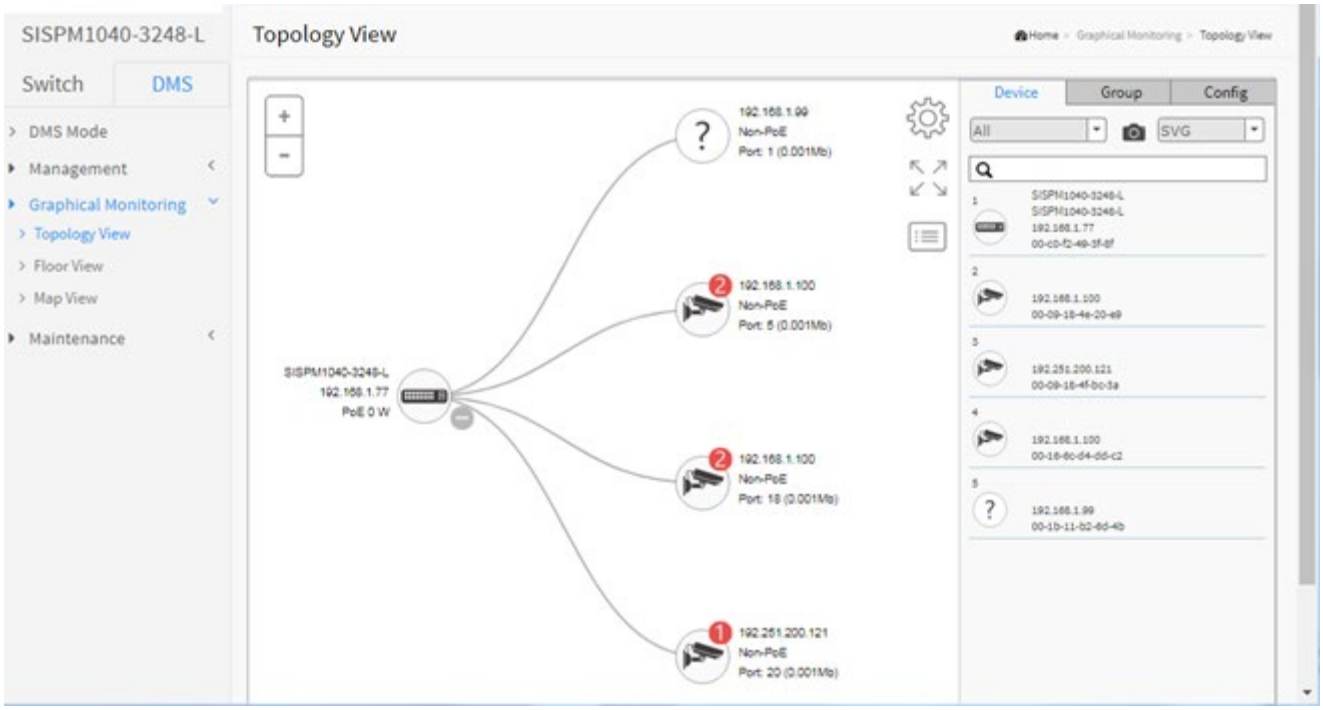


28-7 DMS > Graphical Monitoring

DMS can automatically discover all IP devices and display the devices by graphic networking topology view. User could manage and monitor them by the Topology View, such as to remotely diagnose the cable connection status, auto alarm notifications on critical events, remotely reboot PoE device when it's not alive. Therefore, the user can apply DMS platform to solve the abnormal issues anytime and anywhere by tablet or smart phone, and keep the network running smoothly.

28-7.1 DMS > Graphical Monitoring > Topology View

Click Graphical Monitoring > Topology View to view the network topology.



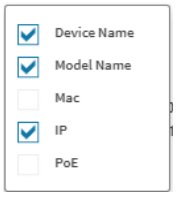
Parameter descriptions :


The upper right corner "Setting icon". When you click the icon, it will pop-up Device, Group, Config, export topology view and advanced search functions for the topology.

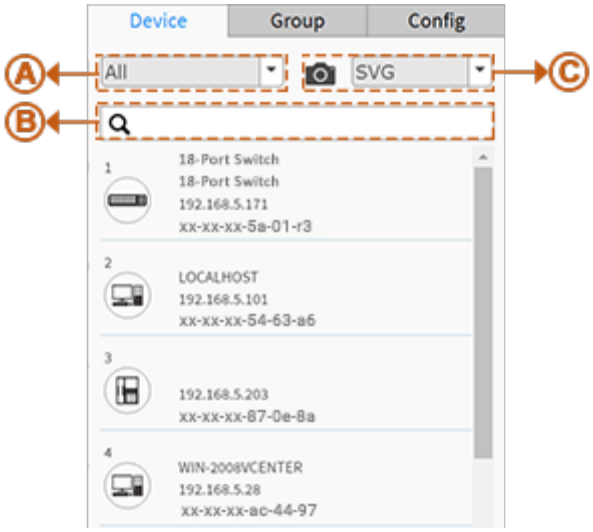

Click to move the devices graphic in the arrow direction (up, down, left, right).


Plus and minus icons: Zoom in and zoom out the topology view; scroll up/down with mouse to achieve the same purpose.


Click to display the set of Topology View parameters to display. Click again to hide the parameters.

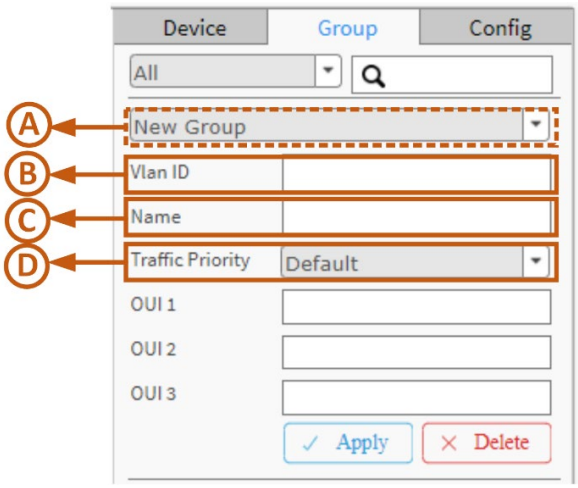


1. Device Search Console



Function
A. Filter devices by Device Type
B. Search devices by key words full text search
C. Save the whole View to SVG, PNG or PDF

Group Setting Console

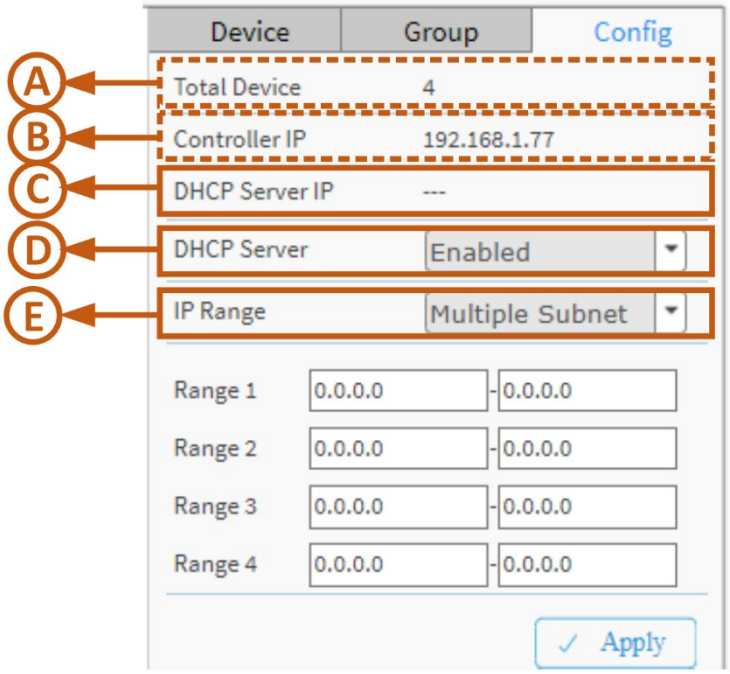


- Using Mac Based VLAN to isolate groups.
- One IP device only can join one VLAN group.

Function

A. Group devices by filtering, searching, clicking device icons, or specifying OUI.
B. Assign a VLAN ID to the Group **or**
C. Assign a Name to the Group.
D. Select a Traffic Priority (0=Low, 7=High)

Config Setting Console



Function

A. Shows how many IP devices are detected and displayed in the Topology view.

B. Shows the Controller (Master) IP.

C. Enter a DHCP Server IP address.

D. Enable or Disable DHCP Server.

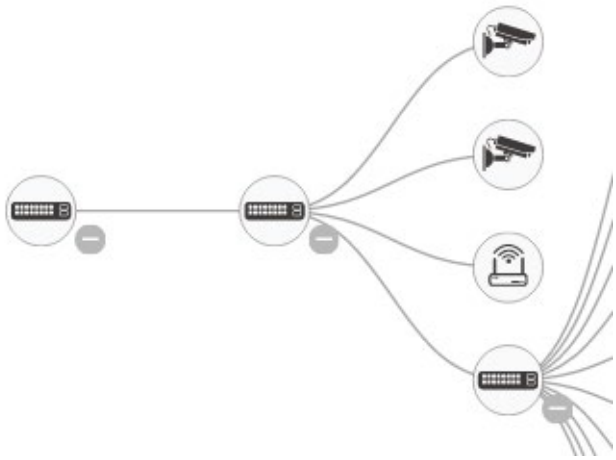
E. IP Range; Select 'Single Subnet' **or** "Multiple Subnet':

- 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.)

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 will be shown on the topology view of each device. Up to 3 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 numbers: It means some event(s) happened (e.g. Device Off-line, IP Duplicate, etc.) on the IP device, user can click on the device icon to check events in Notification.

Device consoles

Left-click any device icon to display the device consoles for further actions:

Dashboard Console: it displays device info and related actions for the device.

Different device type supports different function:

If an IP device is recognized as a DMS switch, it will support "Upgrade" and "Find Switch" function.

If an IP device is recognized as a PoE device, it will support more "Reboot" function in addition to "Upgrade".

If an IP device is recognized as an IP Camera via ONVIF protocol, it will support "Streaming" function.

Device Type: Displayed automatically. If an unknown type is detected, you can still select type from a pre-defined list.

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: Click the Login Action Icon to log in the device via http for further configuration or status monitoring.

Upgrade: Click to upgrade software version.

Find Switch: When this feature is activated, the switch LED all flash for 15 seconds.

Diagnostics: Click to perform the cable diagnostics, to exam 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.

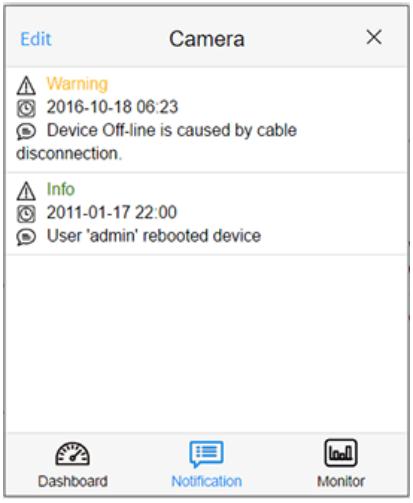
Red icon: Device is not transmitted /receiving data correctly. Which means it might not be pinged successfully.

Reboot: Click Reboot Action Icon to reboot the device remotely so as recover the device back to its normal operation.

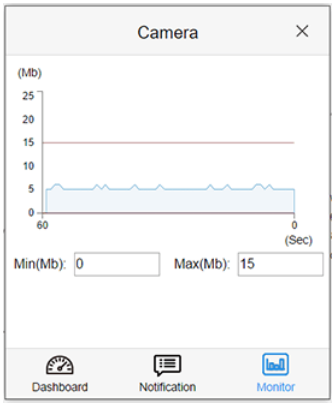
Streaming: Click Streaming Action Icon to display the video images streaming, if the device supports this feature.

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. Use "Parent Node" function to adjust layout in Dashboard.

Notification Console: Displays alarms and logs triggered by events.



Monitor Console: Displays the traffics for device health check purpose.

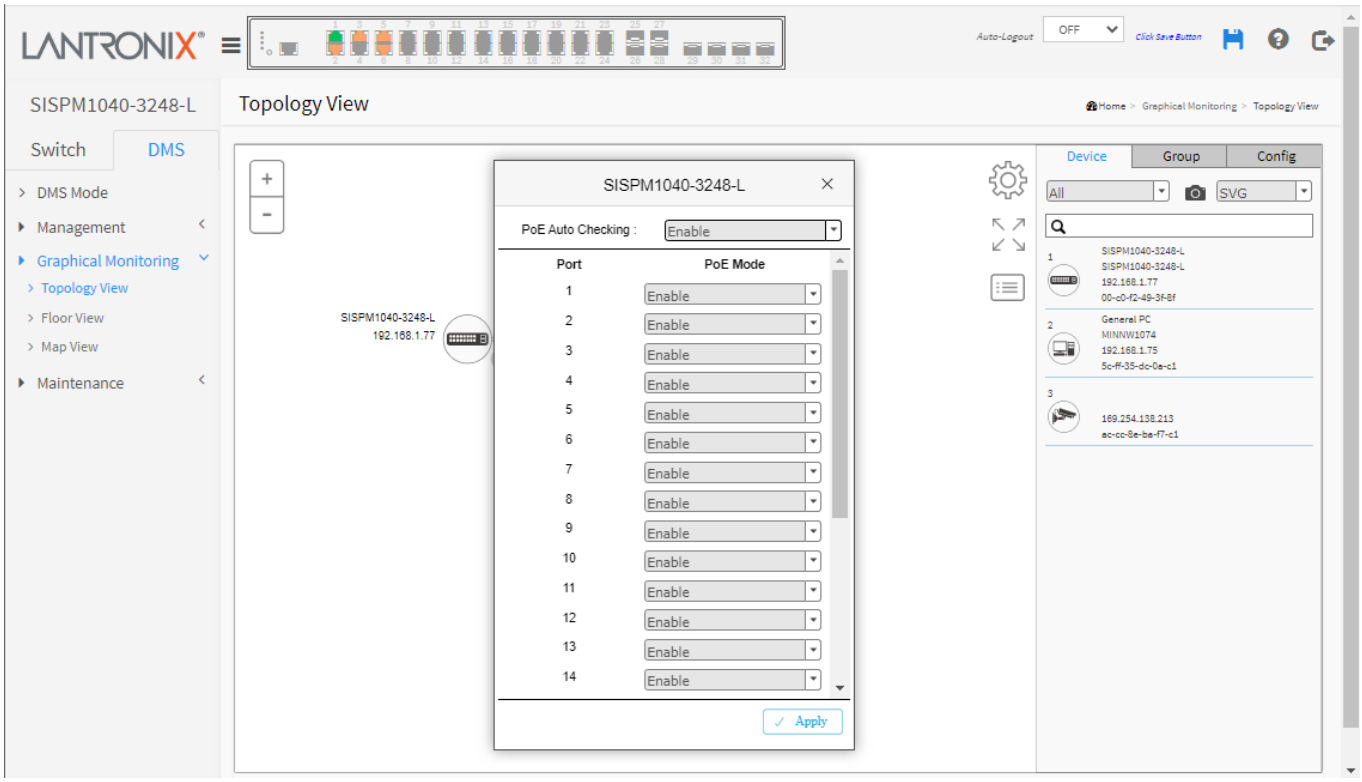


- For each IP device except DMS switches, User can set a threshold of throughput for IP devices, and get notification when throughput is lower or higher than settings.
- If both values are "0", it means the function is disabled.
- Polling interval is 1 second, when the page is closed, the Polling interval will change to around 5 seconds.

PoE Auto Power Reset "AutoFill" Feature

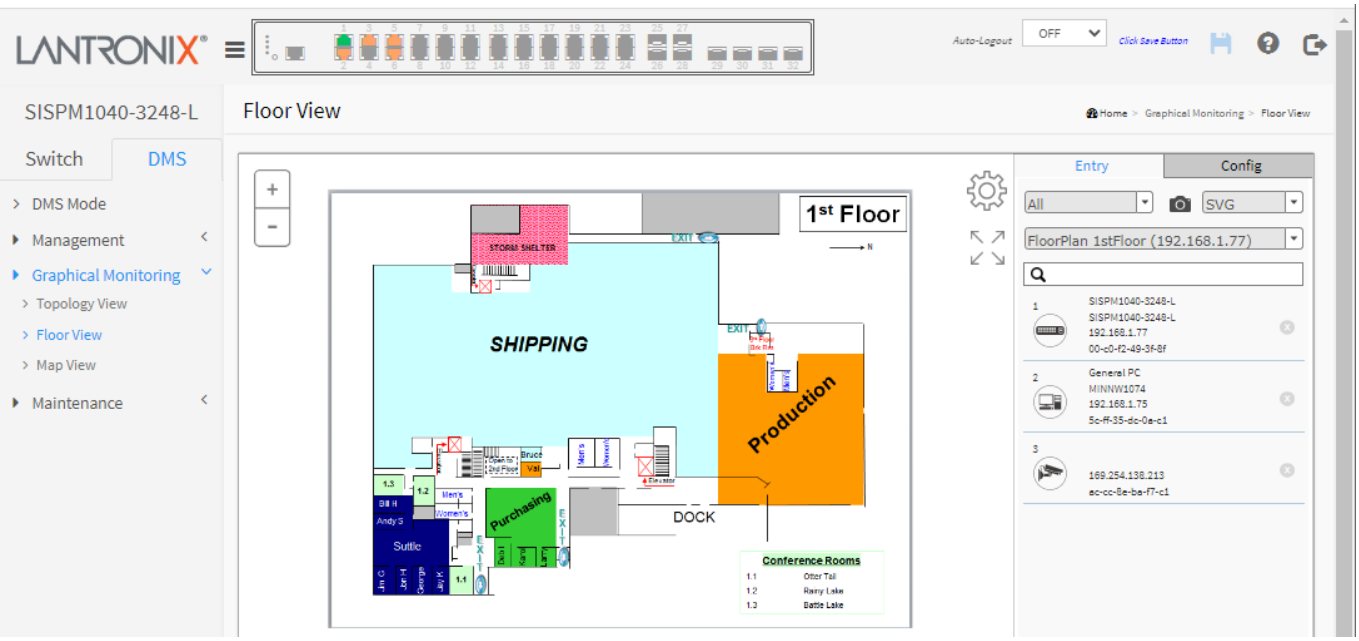
When you enable Auto power reset (PoE auto checking) in DMS, the IP addresses of the connected devices are automatically filled on the Auto Power Reset configuration page.

1. Configure the "PoE Auto Power Reset" parameter at Switch > PoE Management > PoE Auto Power Reset. The default value of the "Failure Action" parameter is "Reboot Remote PD". Note that "PoE Auto Power Reset" 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 Power Reset pane:



27-7.2 DMS > Graphical Monitoring > Floor View

Click **DMS > Graphical Monitoring** > **Floor View** to view the network topology. You can click and hold left mouse button and drag-and-drop the icon to the desired location on the floor view.

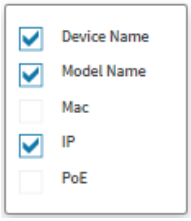


Parameter descriptions:

The upper right corner "Setting icon". When you click the icon, it will pop-up Device, Group, and Config tabs, with export topology view and advanced search functions for the topology. When you click it again the tabs no longer display.

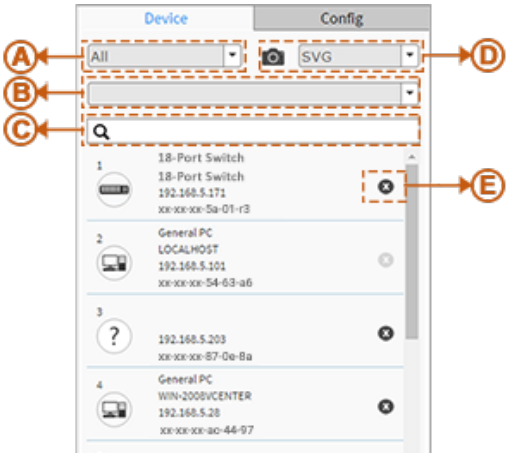
Icons with plus and minus signs: Zoom in and zoom out the floor view; you can scroll up/down with your mouse to achieve the same purpose.

Click to select which three device parameters to display; choose between Device Name, Model Name, Mac address, IP address, and PoE information.



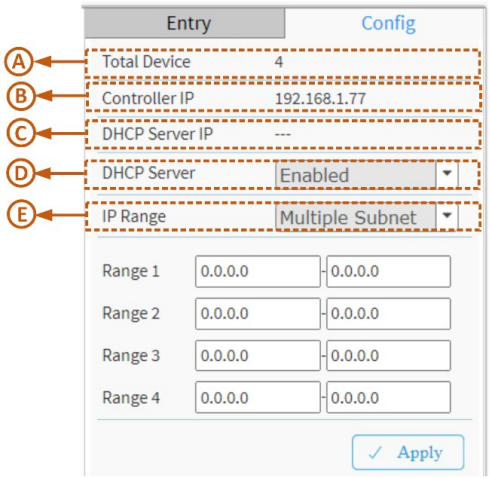
: Click to alternately hide and display the left-hand menu tree.

1. Device Search Console



Function	
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

2. Config Setting Console



Function

A. Shows how many IP devices are detected and displayed in the Topology view.

B. Shows the Controller (Master) IP.

C. Enter a DHCP Server IP address.

D. Enable or Disable DHCP Server.

E. IP Range; Select 'Single Subnet' **or** "Multiple Subnet':

- 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.)

 Icon with screen view type: Click it to change to Full Screen View of Floor or return to the Normal View.

Floor View

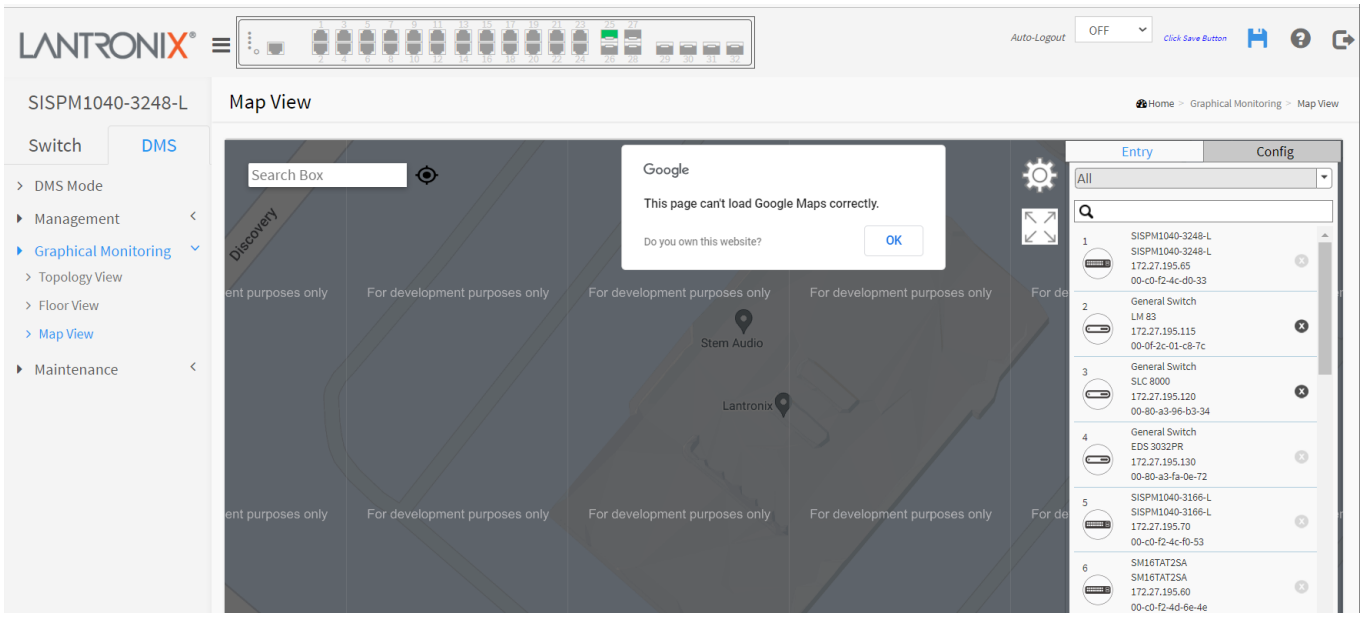
- Anchor Devices onto Floor Maps
- Find Device Location Instantly
- 10 Maps can be Stored in Each Switch
- IP Surveillance/VoIP/WiFi Applications
- Other Feature same as Topology View
- To place and remove a device icon
    i. Select a device and click its icon from the device list.
    ii. The device icon will show on the floor image's default location.
    iii. Click and hold left mouse to drag-and-drop the icon to the correct location on the floor view.
    iv. 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. You can select function and check issues.

 Icon with red mark: Device link down. You can diagnose the link status.

28-7.3 DMS > Graphical Monitoring > Map View

Click DMS > Graphical Monitoring > Map View to display the DMS Map View. Map View can help to find the location of the devices even they are installed in a different building. You can place the device icon on the Map View which is navigated by Google Maps. If the message "*This page can't load Google Maps correctly.*" displays, click the OK button to clear the message and go to "28-5 DMS > Management > Map API Key" on page 454.



Parameter descriptions :

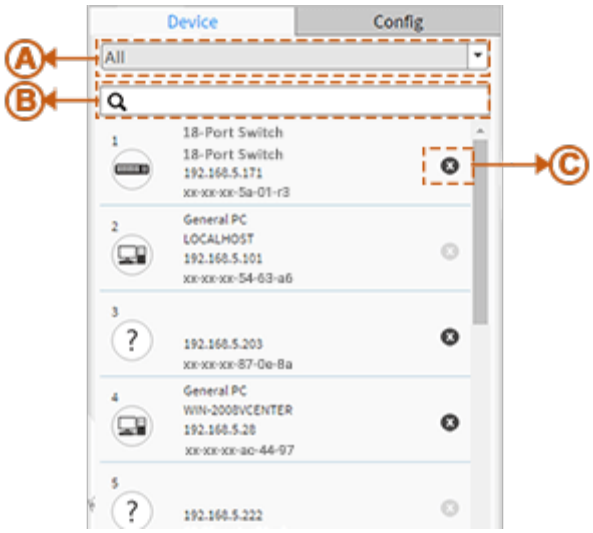
In the upper right corner, there is a "Setting icon". When you click the icon, it will pop-up Entry and Config tabs, and advanced search functions for the device.

Note that you must Sign In to continue to Google Maps.

At the message "*This page can't load Google Maps correctly*." click the OK button to clear the message.

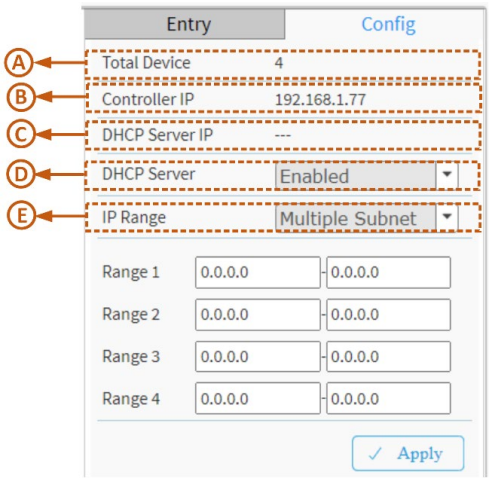
Click the text *Do you own this website?* to go to click the OK button to the Google Maps Platform Error Message page.

1. Device Search (Entry) Console



Function	
A.	Filter devices by Device Type
B.	Search devices by key words full text search
C.	Remove a device from map view

2. Config Setting Console



Function

A. Shows how many IP devices are detected and displayed in the Topology view.

B. Shows the Controller (Master) IP.

C. Enter a DHCP Server IP address.

D. Enable or Disable DHCP Server.

E. IP Range; Select 'Single Subnet' **or** "Multiple Subnet':

- 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.)

 Icon with screen view type: Click it to change to Full Screen View of Map or return to the Normal View.

Map View

- Anchor Devices onto Google Maps.
- Find Devices Instantly from Google Maps.
- On-Line Search Company/Address.
- Outdoor IP Cam/WiFi Applications.
- Other Feature same as Topology View
- To place and remove a device icon:
  i. Select a device and click its icon from the device list.
  ii. The device icon will show on the map's default location.
  iii. Click and hold left mouse to drag-and-drop the icon to the correct location in Map view.
  iv. Click the cross sign on the right side of a device icon to remove a device from Map view.

Device Status

 Icon with black mark: Device link up. You can select function and check issues.

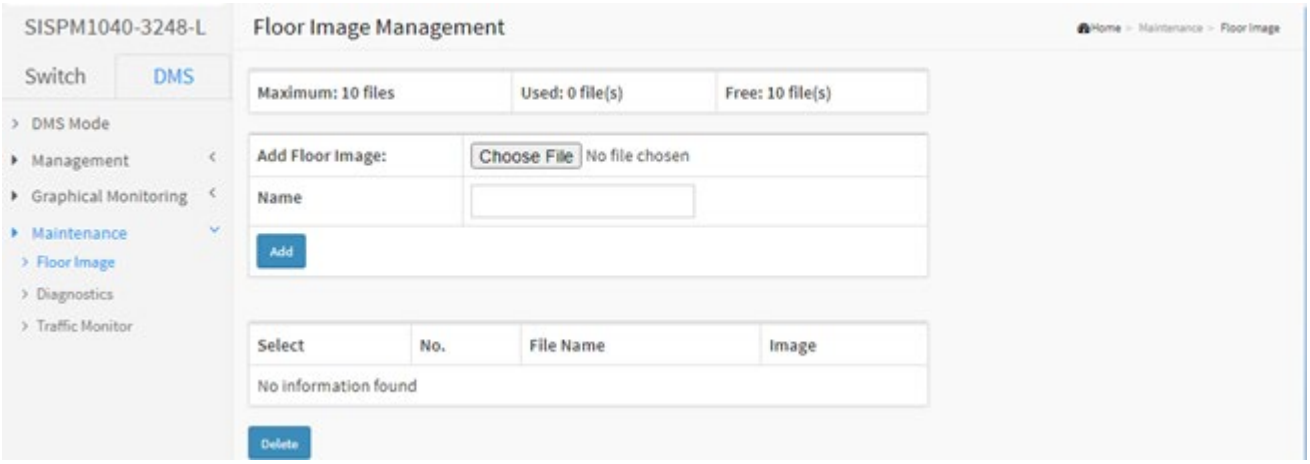
 Icon with red mark: Device link down. You can diagnose the link status.

28-8 DMS > Maintenance

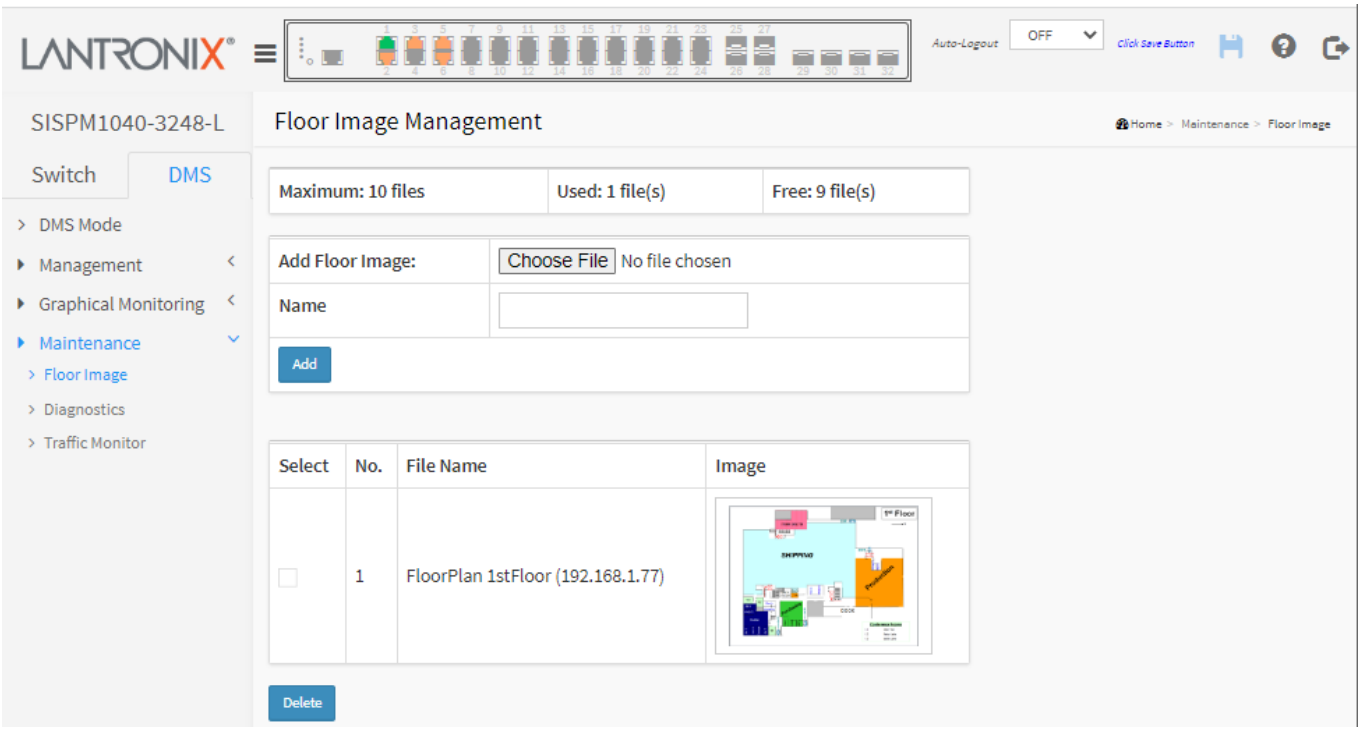
28-8.1 DMS > Maintenance > Floor Image

Click DMS > Maintenance > Floor Image to display the Floor Image Management table. Here you can upload and manage floor map images. Up to 20 JPEG or PNG images, each a maximum of 256KB size, can be uploaded to the switch.

1. Click DMS > Graphical Monitoring > Floor Image to view the default Floor Image Management page.



2. Click the Choose File button.
3. Navigate to and open the desired floor image file (.jpg or .png).
4. Give the image a name.
5. Click the Add button to display the image.



Parameter Descriptions :

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.

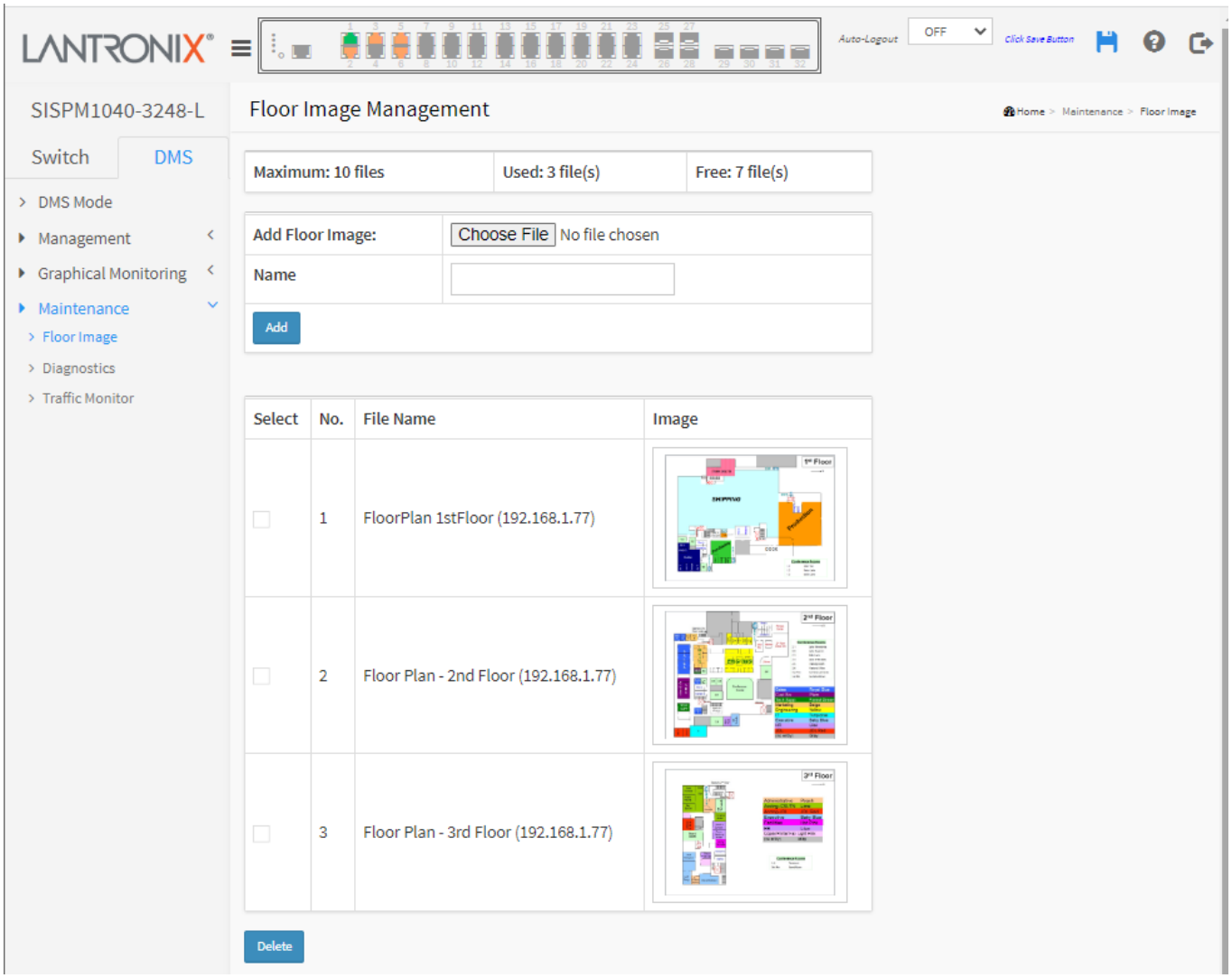
Buttons

Add: Click Add to upload. When done, a snapshot will be available on screen.

Delete: To remove an existing floor map, select its checkbox and click Delete to remove the selected flor map.

Messages: *Only jpg. png 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.

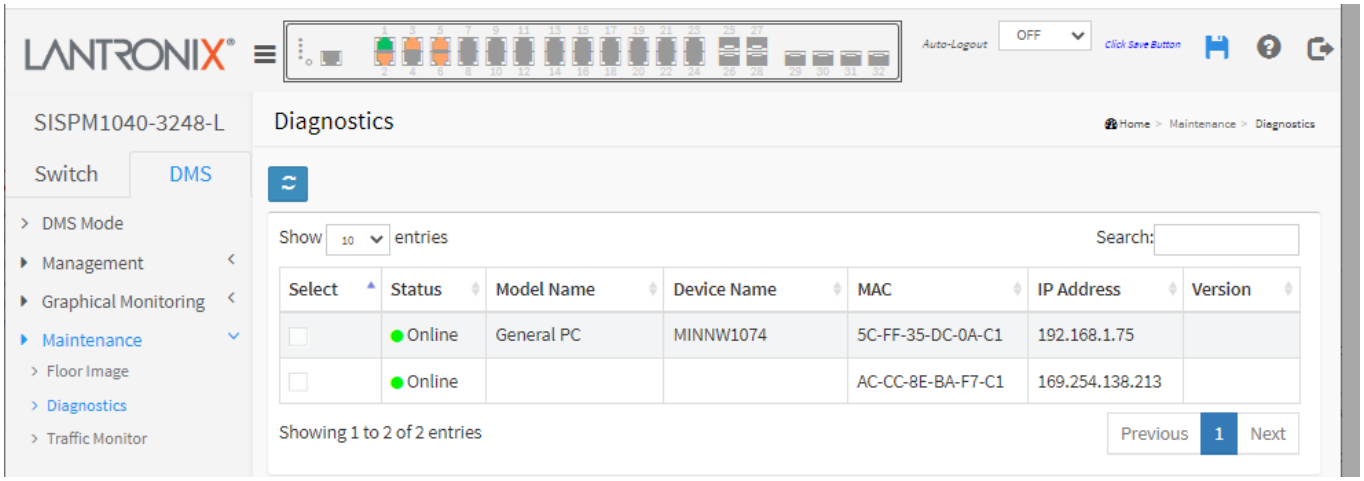
Example: Floor Image Management showing 3 floor images:



28-8.2 DMS > Maintenance > Diagnostics

This page lets you run a test to display Connection and Cable status on a selected device instance.

1. Navigate to DMS > Maintenance > Diagnostics to display the default Diagnostics page.



2. Check the Select checkbox of the desired instance to display the Diagnostics page for the selected instance.

Parameter Descriptions :

Select : Select off-line device from the list.

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.

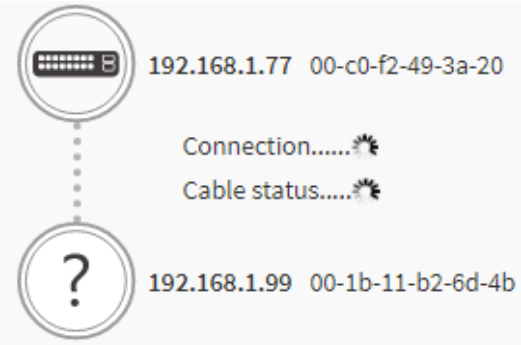
Version : The Version of the network connectivity devices.

Buttons

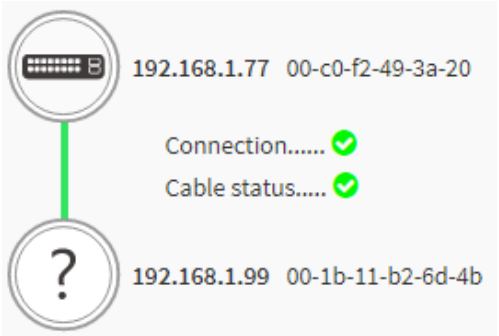
Refresh : Refreshes the displayed table starting from the input fields.

Search : Search for a key word.

Another Try : Click to go back to the default Diagnostics page after viewing the Diagnostic page for the selected instance.

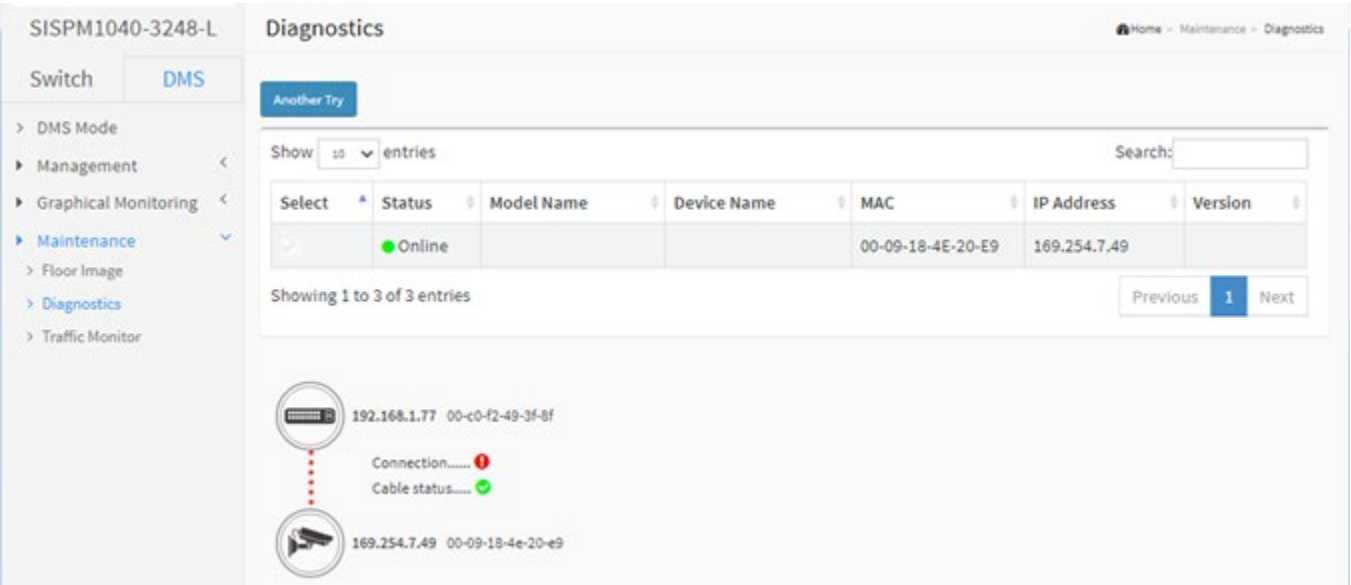


Diagnostic In process



Diagnostic Completed

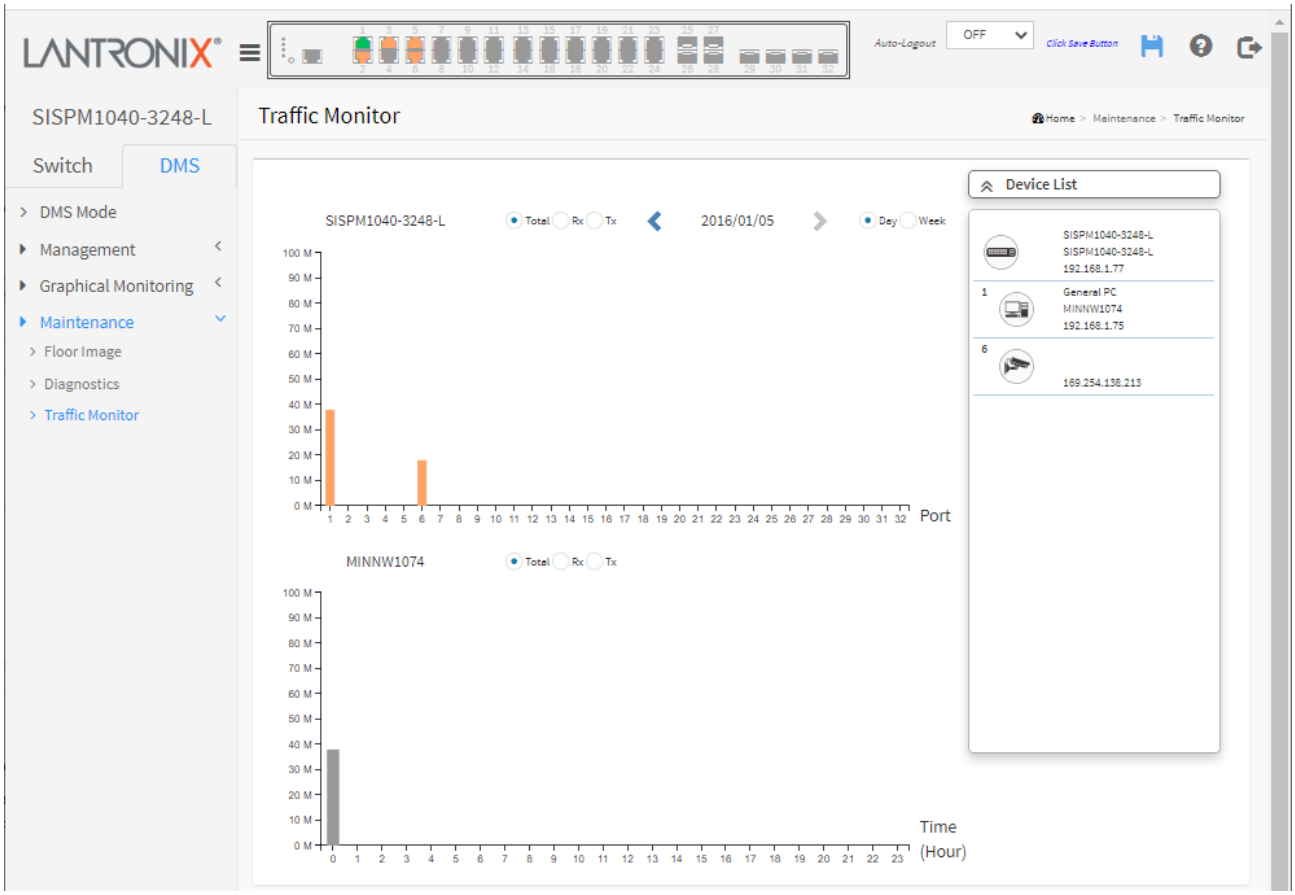
Example



28-8.3 DMS > Maintenance > Traffic Monitor

This page displays charts of network traffic of all the devices managed by the DMS Controller switch. Note that FW v8.40.1252 added Traffic Monitor back to DMS. To configure Traffic Monitoring in the web UI:

1. Click DMS, Maintenance, Traffic Monitor.
2. Select the displayed detail (Total, Rx, or Tx).
3. Select the date of monitored traffic to display.
4. Select the amount of monitored traffic to display (Day or Week).
5. View the monitored traffic displayed.
6. Click a chart column to display a device's second chart.



Parameter descriptions:

Total / Rx / Tx: Select the set of data to be displayed. The default is Total.

< 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).

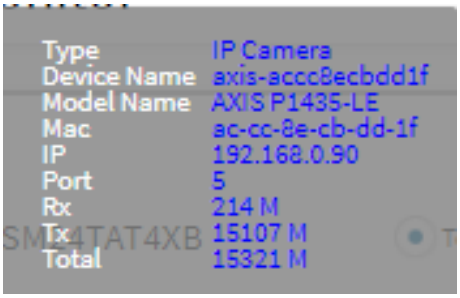
Port: Horizontal axis shows the switch port numbers.

Time (Hour): Horizontal axis shows the time elapsed in hours (0-23).

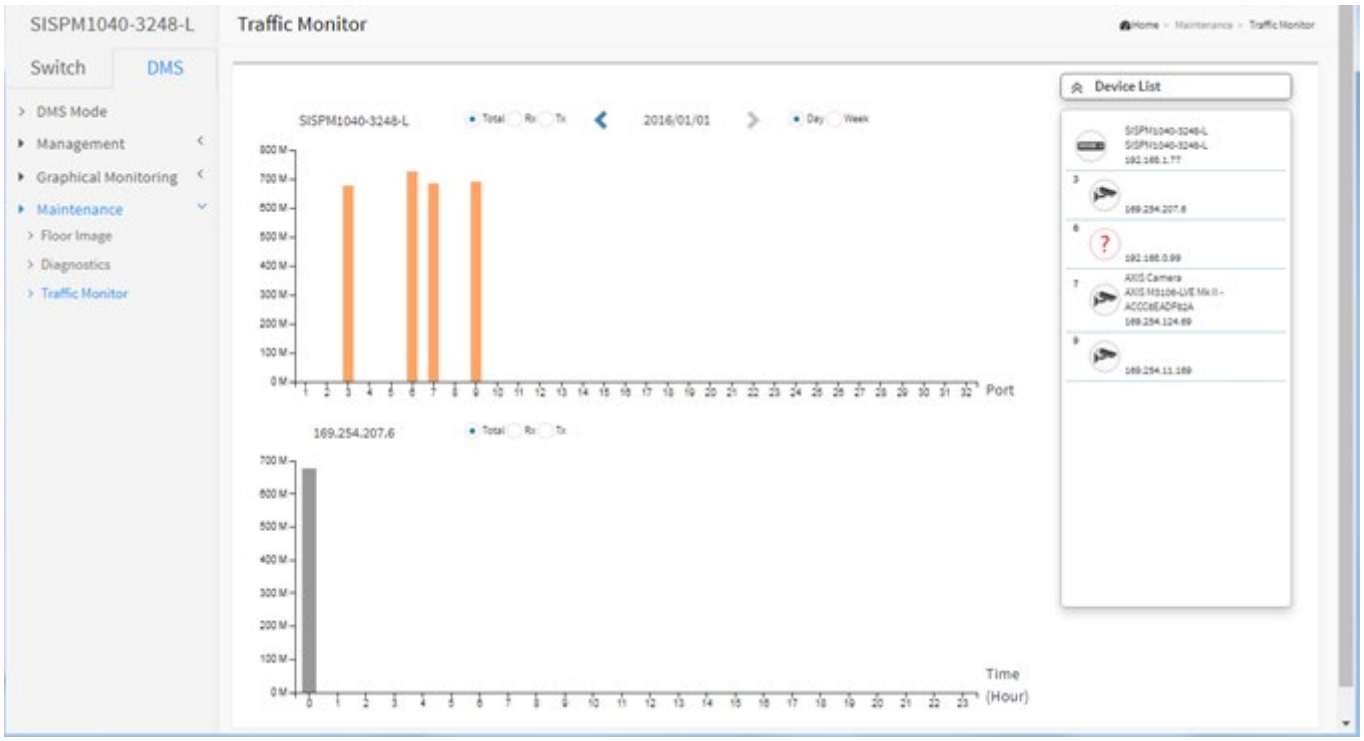
DMS Traffic Monitor Procedure

1. Navigate to DMS > Maintenance > Traffic Monitor.

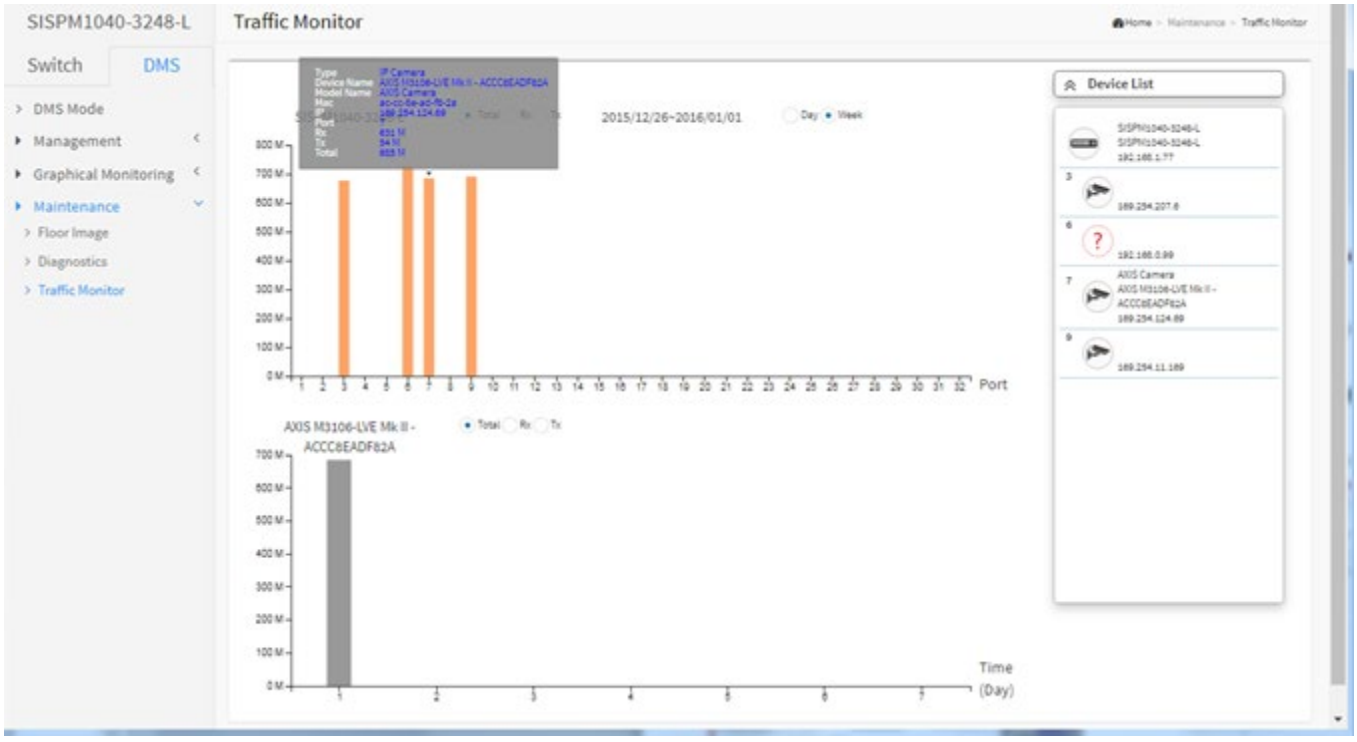
2. Hover the cursor over a column in the graph to view its details.

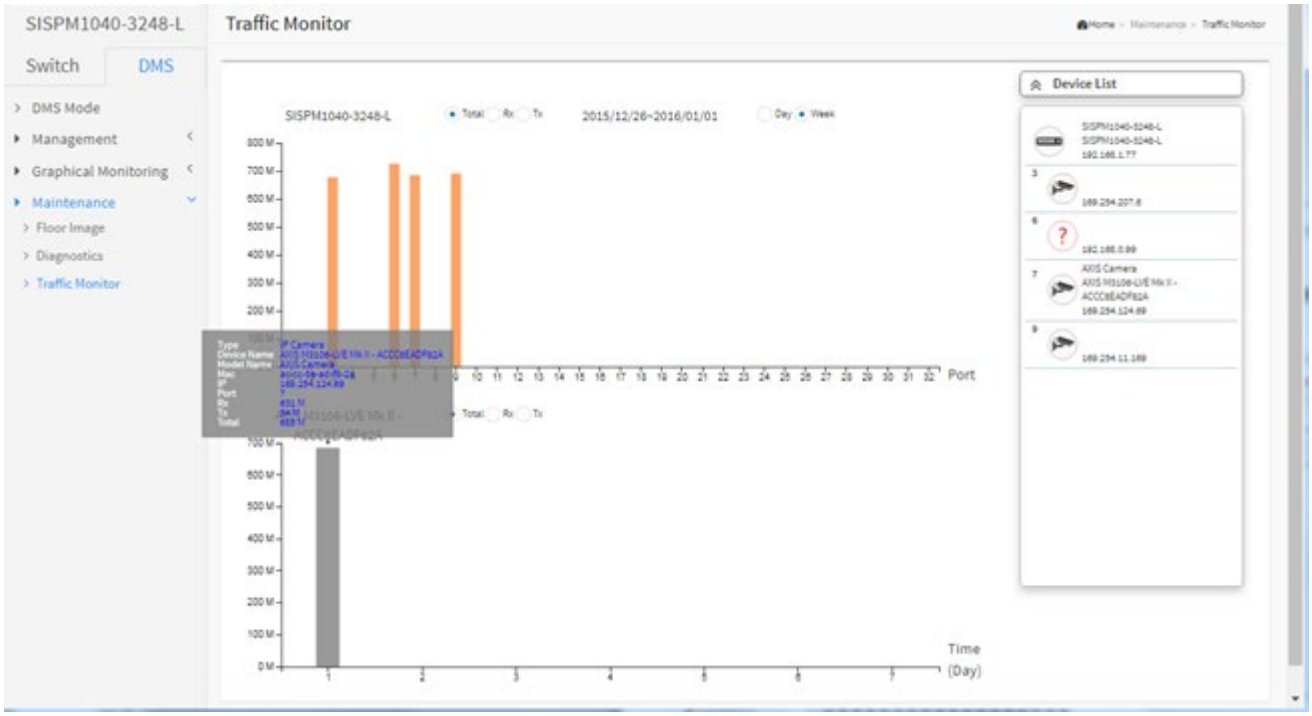


3. Click the graph column to display its axis information in the lower graph table.



Traffic Monitor Examples





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 section 28-8.2 DMS > Maintenance > Traffic Monitor on page 474.

Bandwidth vs Throughput vs Network Throughput

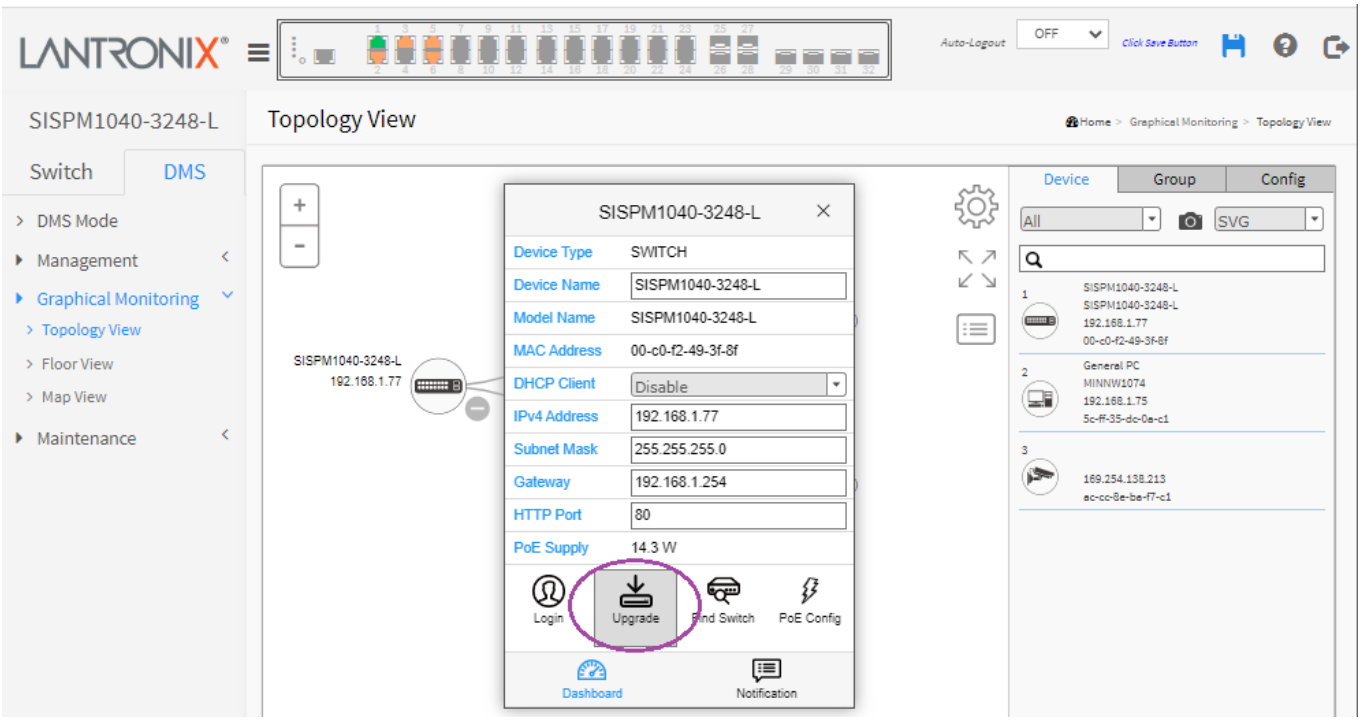
Bandwidth: the maximum amount of data that can go through a given medium.
Throughput: the amount of data that actually goes through that medium.
Network throughput: the amount of data that is transmitted through a given network medium over a given amount of time.

Throughput Units of Measurement

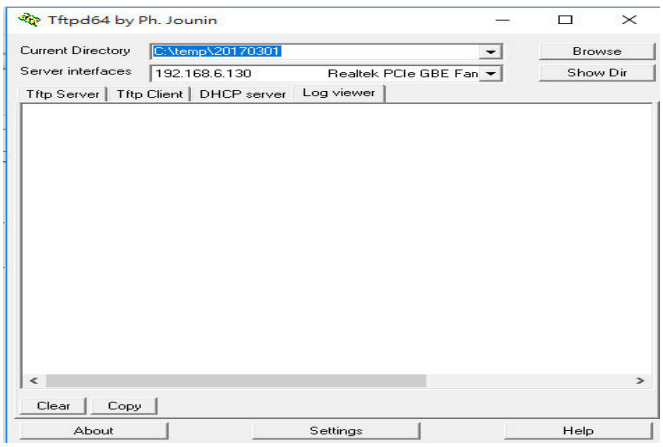
Bit: The smallest size of binary information used by computer devices (the ones and zeros in binary)
Byte: 8 bits
Megabit: 1 million bits
Megabyte: 1 million bytes
Gigabit: 1 billion bits
Gigabyte: 1 billion bytes
Mbps: Megabits per second
MBps: Megabytes per second
Gbps: Gigabits per second
GBps: Gigabytes per second

28-8.4 DMS Firmware Upgrade Procedure

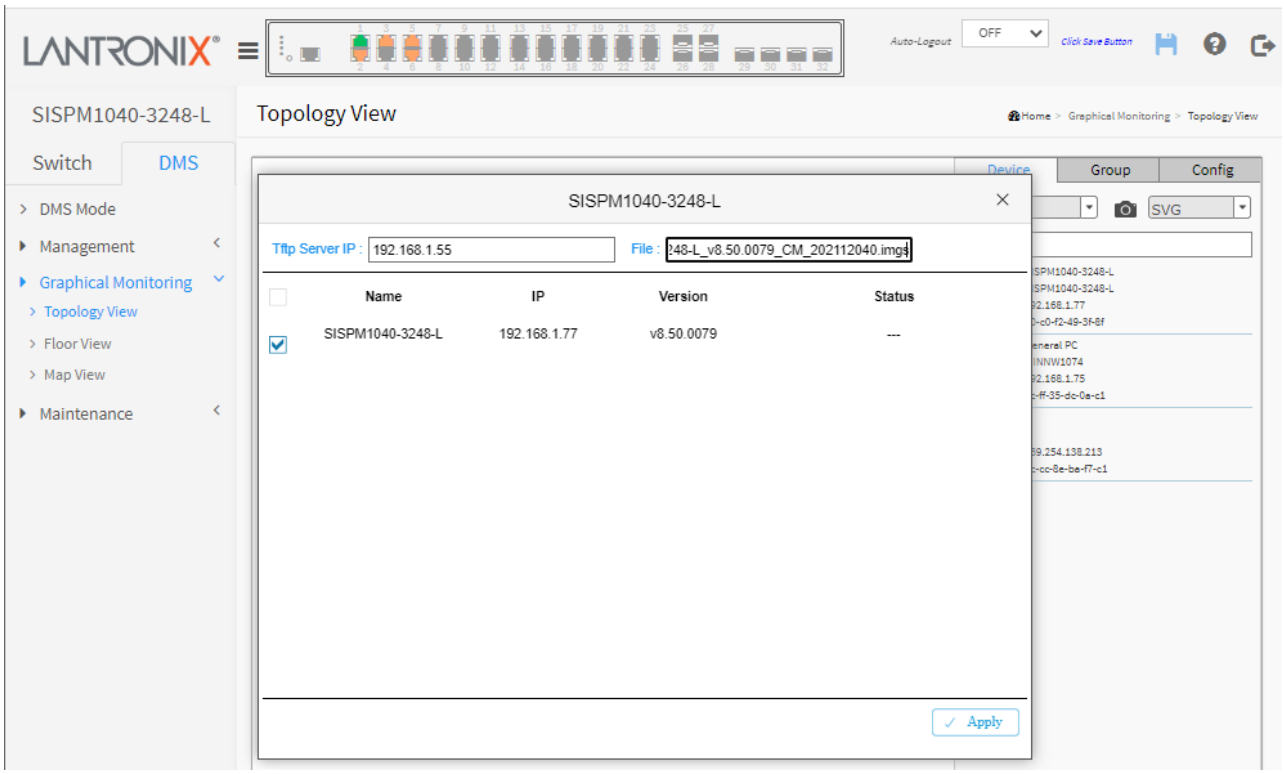
1. Navigate to the DMS > Graphical Monitoring > Topology View menu path.
2. Click the  button to display the right pane menu tabs (Device, Group, and Config).
3. Connect all switches and make sure DMS is working.
   - Set all switches with different IP addresses and in the same IP segment.
   - Make sure gateway IP address is configured.



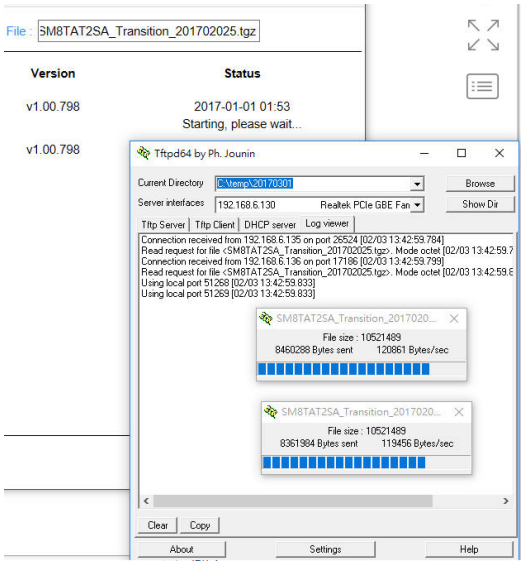
4. Enable the TFTP server and set the correct image path.



5. Click the switch icon, and then click the “Upgrade” button in the Dashboard.
6. Enter the TFTP server IP address and FW file name, and select the switch on which you want to upgrade the FW.



7. Click “Apply” to start the FW upgrade and save to Running-config..
8. Observe the upgrade status until completion.



Messages

Starting, please wait...

Error : Firmware download fail

28-9 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 TN 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 28-5 DMS > Management > Map API Key on page 454.

Appendix A – DHCP Per Port Configuration

You can configure DHCP Per Port via the Web UI as described below.

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.

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.

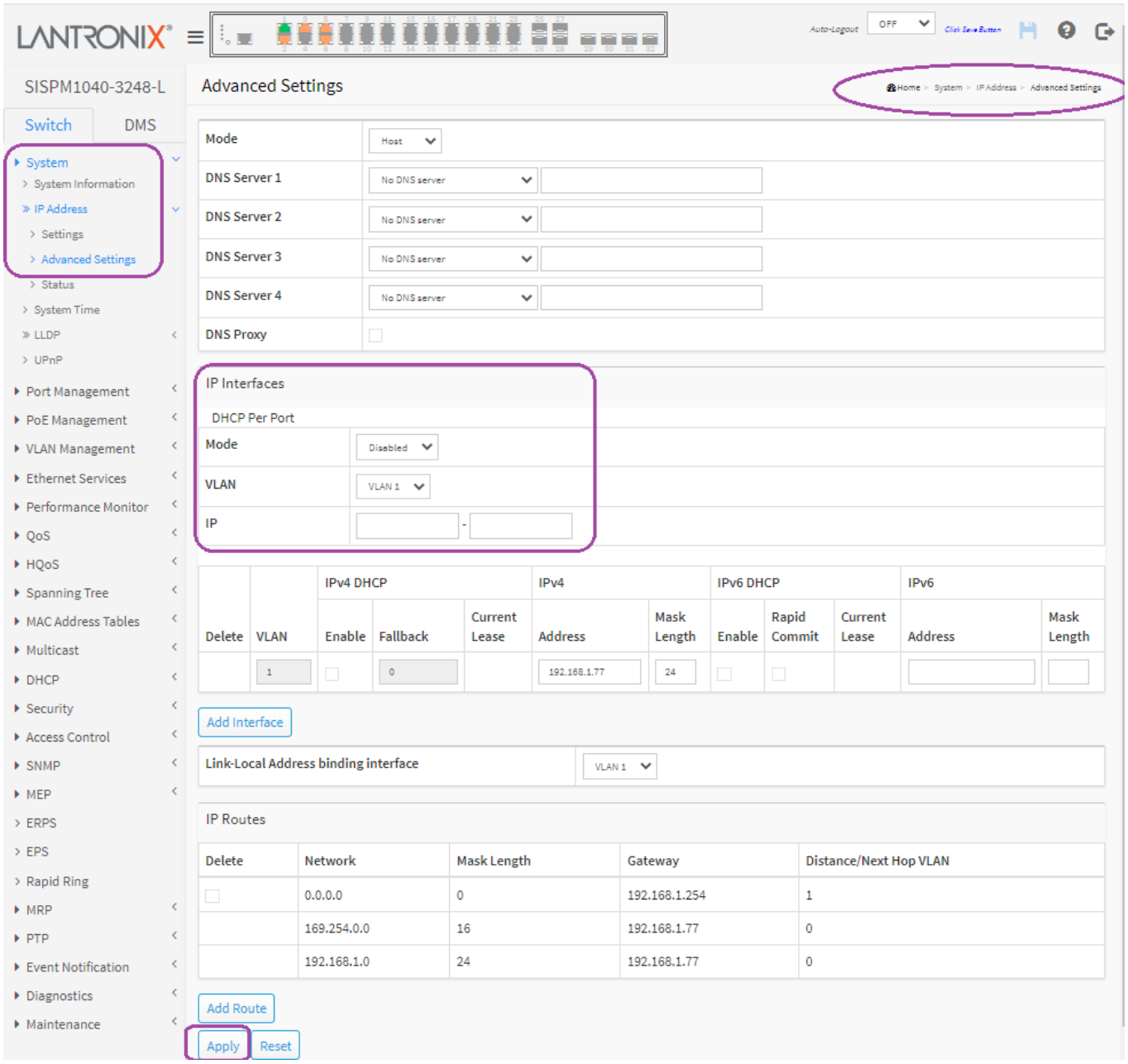
The DHCP Per Port pages and parameters are described below.

DHCP Per Port Mode, VLAN, and IP 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 and monitor DHCP Per Port via the Web UI, navigate to the Switch > System > IP Address > Advanced Settings menu path.



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**.

DHCP Per Port VLAN: at the dropdown select an IP address from a DHCP pool on a switch be statically assigned to a switchport, such that whichever device plugs into the switchport it will always be assigned that specific IP address. The IP address is configured in the interface config settings. Note that this is binding an IP address to an interface, not to a MAC address, which is the classic binding technique found on most switches.

DHCP Per Port IP: enter the IPv4 IP address range to be used when the DHCP Per Port function is enabled (e.g., 192.168.1.78 - 192.168.1.101). 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.

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.

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.

Message: *DHCP Per Port IP range (192.168.1.78 - 192.168.1.100) is not equal to switch TP port number (24)*

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.

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).

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 Configuration

You can configure Media Redundancy Protocol (MRP) parameters via the Web UI at MRP > MRP Configuration and monitored at MRP > MRP Status, and via the CLI. See "Chapter 22 - MRP" on page 365 for MRP parameter descriptions.

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.

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).

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.

MRP Sample Setup

The example below shows SISPM1040-384-LRT-C switches (one MRM and five MRCs).

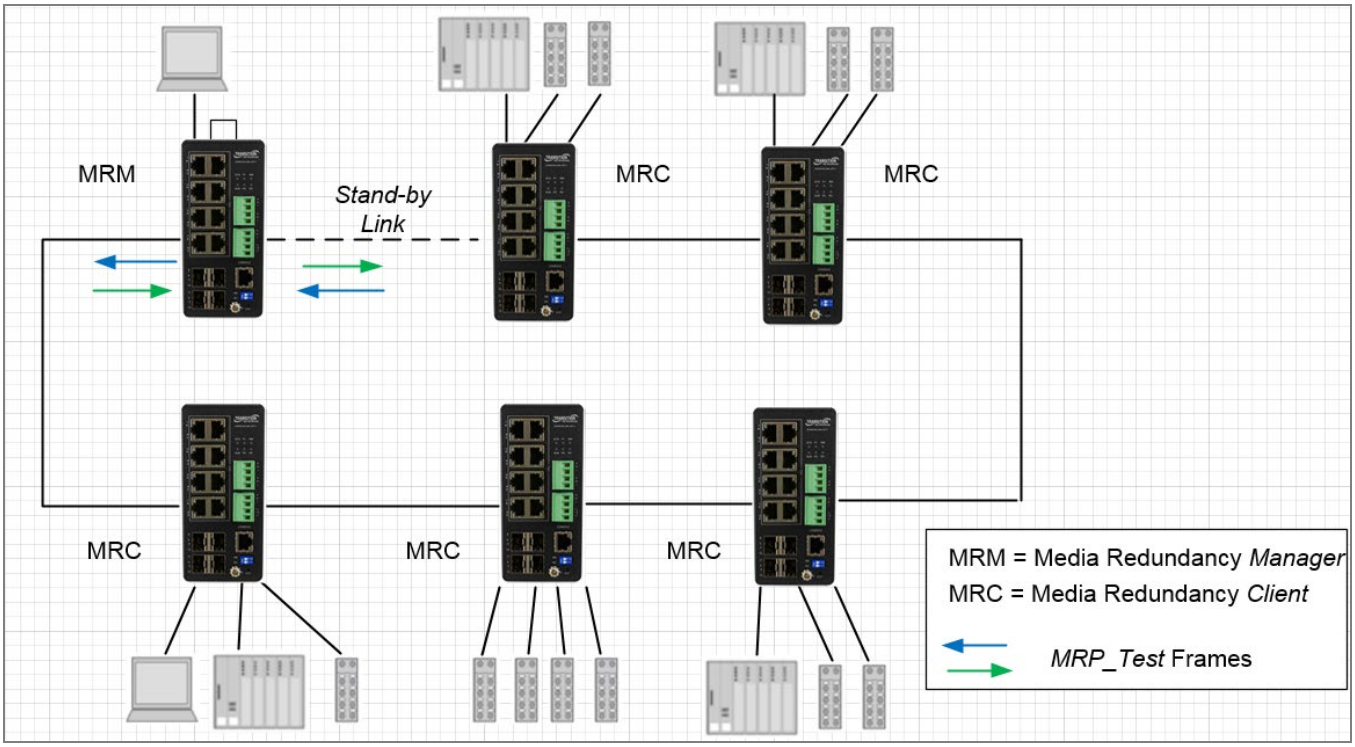


Figure: MRP Sample Setup

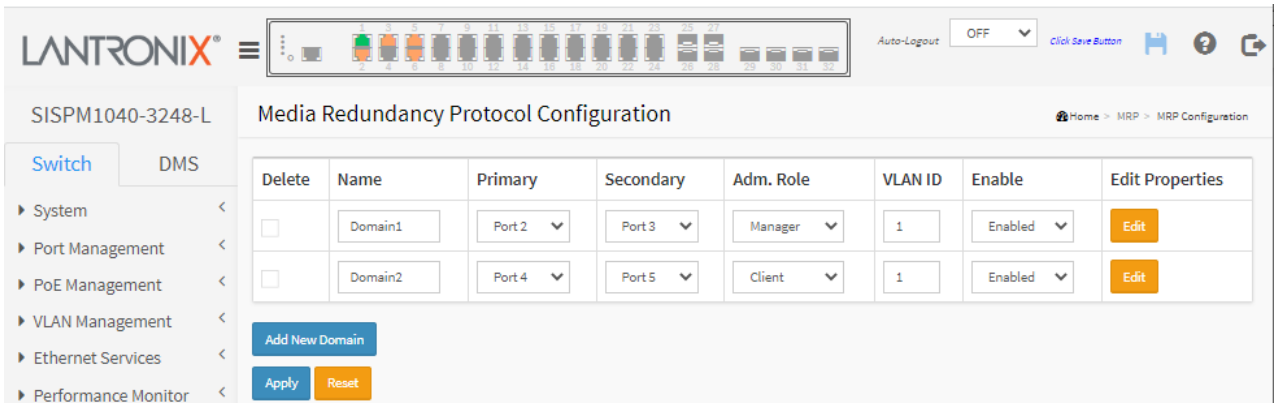
MRP Pre-Requisites (General)

The following are required to perform MRP setups.

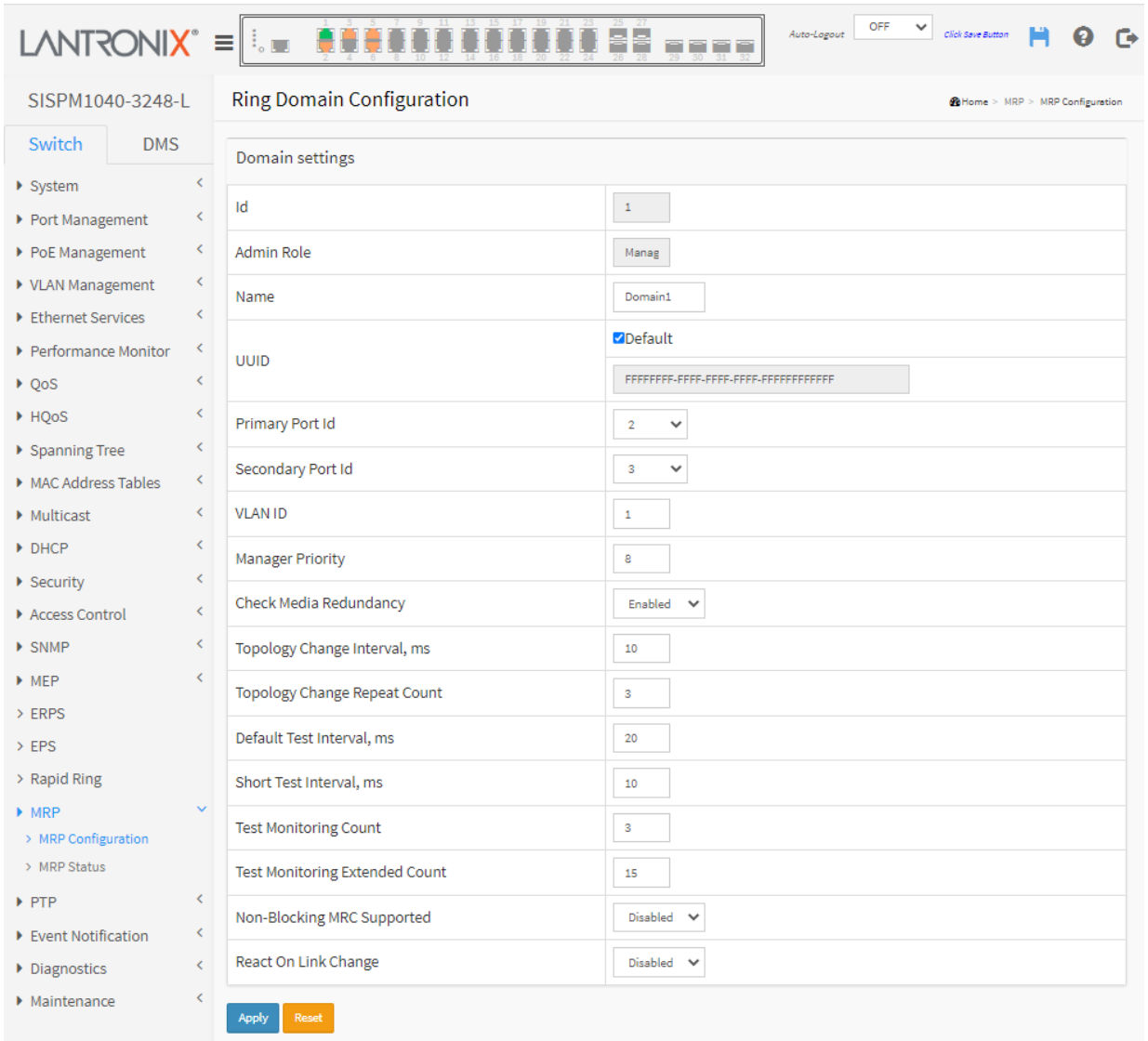
1. Spanning Tree must be disabled at Configuration > Spanning Tree > CIST Port.
2. Other Ring technologies must be disabled (G.8031 EPS, G.8032 ERPS, Rapid-Ring, Ring-To-Ring, etc.).
3. Other pre-requisites may apply to the specific examples below.

MRP Web UI Configuration

1. Navigate to MRP > MRP Configuration and click the Add New Domain button and initially configure two MRP Domains:

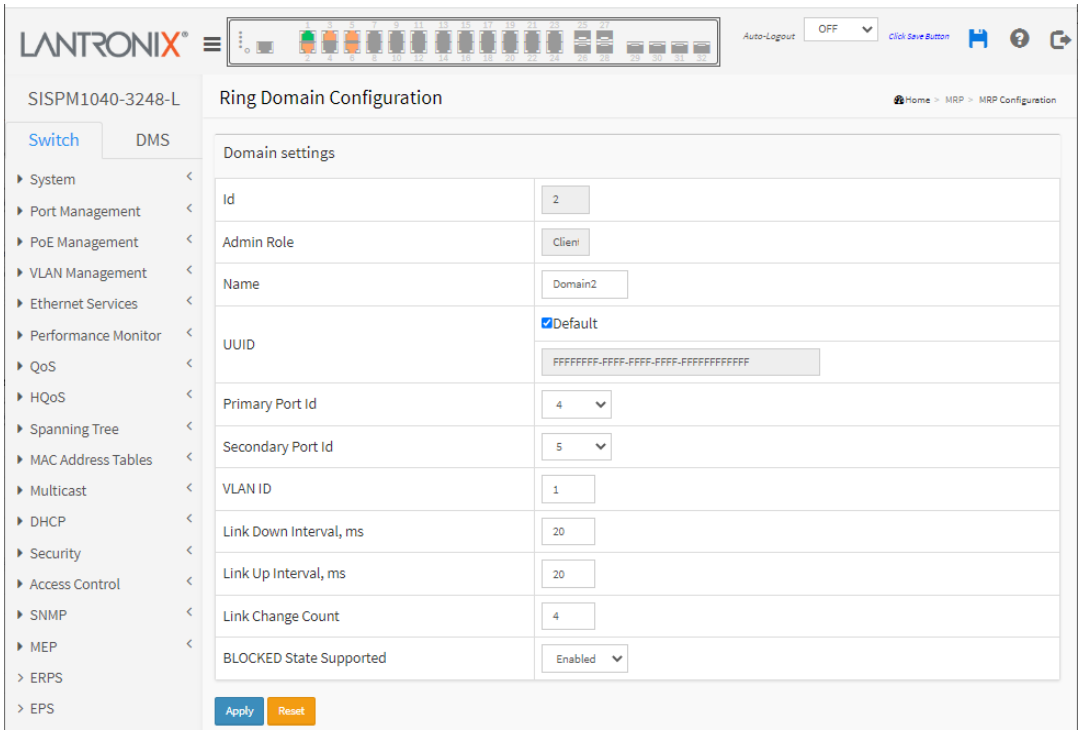


2. Edit the Primary, Secondary, Adm. Role, and VLAN ID columns. Leave the Enabled column at Disabled.
3. Click Apply to save, and then click the Edit button to configure the first MRP Domain (Domian1).



4. 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.

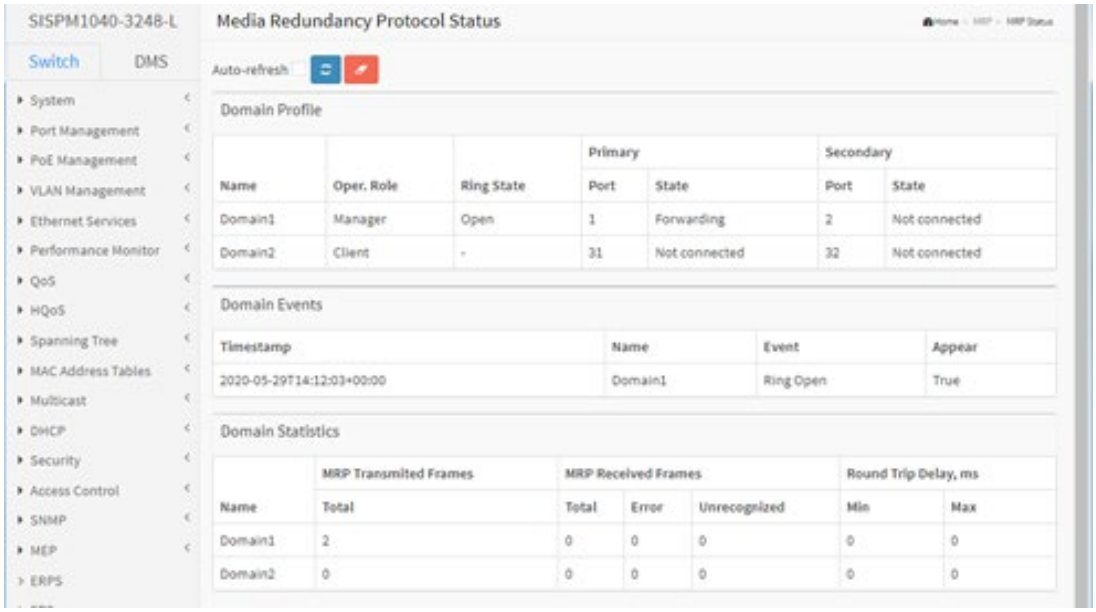
5. Click the Edit button to display the second MRP Domain (Domian2).



6. Edit the Domain Settings as required. Click Apply to save; the message "*Domain is enabled*" displays. Click OK to clear the webpage message.

7. When the "Media Redundancy Protocol Configuration" page displays again, verify the settings.

8. Navigate to MRP > MRP Status and verify the Domain Profile, Events, and Statistics displayed.



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.

Lantronix Corporate Headquarters
48 Discovery, Suite 250
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.