SISPM1242-582-LRT

Managed Hardened Multi-Gigabit Ethernet POE++ Switch, (4) 10/100/1000Base-T + (4) 100M/1G/2.5G PoE++ Ports, (2) 1G/10G SFP+ Slots

Web User Guide

Part Number 33885
Revision A January 2026

Intellectual Property

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

Warranty

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

Contacts

Lantronix Corporate Headquarters

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 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.	Description
January 2026	A	Initial release

Safety Cautions and Warnings

Cautions indicate that there is the possibility of poor equipment performance or potential damage to the equipment. **Warnings** indicate that there is the possibility of injury to person.

Cautions and Warnings appear here and may appear throughout this manual where appropriate. Failure to read and understand the information identified by this symbol could result in poor equipment performance, damage to the equipment, or injury to persons.

⚠ **Caution**: While installing or servicing the power supply module, wear a grounding device and observe all electrostatic discharge precautions. Failure to observe this caution could result in damage to, or failure of the power module.

⚠ **Warning**: Do not connect the power module to an external power source before installing it into the chassis. Failure to observe this warning could result in an electrical shock, even death.

Warning: Equipment grounding is vital to ensure safe operation. The installer must ensure that the power module is properly grounded during and after installation. Failure to observe this warning could result in an electric shock, even death.

Warning: A readily accessible, suitable National Electrical Code (NEC) or local electrical code approved disconnect device and branch-circuit protector must be part of the building's installed wiring to accommodate permanently connected equipment. Failure to observe this warning could result in an electric shock, even death.

Warning: Turn any external power source OFF and ensure that the power module is disconnected from the external power source before performing any maintenance. Failure to observe this warning could result in an electrical shock, even death.

Warning: Ensure that the disconnect device for the external power source is OPEN *(turned OFF)* before disconnecting or connecting the power leads to the power module. Failure to observe this warning could result in an electric shock, even death.

See the *SISPM1242-582-LRT Install Guide* for electrical safety warnings translated into multiple languages.

Contents

1. Introduction

The SISPM1242-582-LRT is a managed PoE++ switch suitable for connecting and powering devices in hardened environments. It has (4) 10/100/1000 and (4) 100M/1G/2.5G PoE++ ports with (2) 1G/10G dual speed SFP+ slots. The switch can supply up to 90 Watts per port on (4) ports or 45 Watts per port on (8) ports simultaneously.

The switch includes DMS, accessible by local web manager, which provides advanced configuration and management of all IP addressable devices in the network, including a graphical network topology, floor map creator, device map view, traffic monitoring, and network diagnostics for troubleshooting.

Lantronix's hardened switches are certified to operate reliably in harsh environments such as those found on factory floors, outdoor enclosures or other challenging environments.

About This Manual

This manual describes how to configure and manage the SISPM1242-582-LRT switch using the web UI. It is intended for use by network administrators who are responsible for operating and maintaining network equipment.

Related Manuals

- SISPM1242-582-LRT Quick Start Guide, 33883
- SISPM1242-582-LRT Install Guide, 33884
- SISPM1242-582-LRT CLI Reference, 33886
- Release Notes (version specific)

For Lantronix Documentation, Firmware, App Notes, etc. go to https://www.lantronix.com/technical-support/. Note that this manual provides links to third party web sites for which Lantronix is not responsible.

2. Web Management

Default Configuration Settings

The 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

To prevent unauthorized access, change the default password on first use and periodically thereafter.

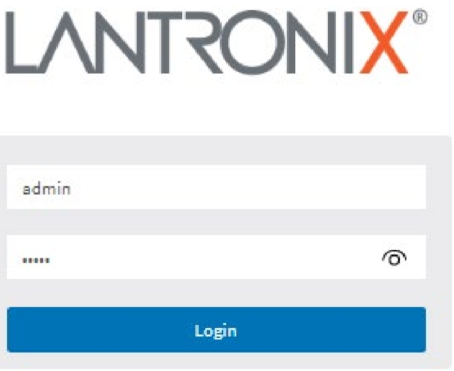
Initial Switch Setup via Web Browser

After powering up the switch for the first time, you can perform the initial switch configuration using a web browser. If you want to do the initial configuration using a console connection, see the Install Guide.

To begin the initial configuration via web browser, you need to reconfigure your PC's IP address and subnet mask to make sure the PC can communicate with the switch. After changing PC's IP address (for example, 192.168.1.250), then you can access the Web interface of the switch using the switch's default IP address and subnet mask.

To connect and login using the Web browser:

1. Power up the PC that you will use for the initial configuration. Make sure the PC has the Ethernet RJ45 connector to be connected to the switch via standard Ethernet LAN cable.
2. Reconfigure the PC's IP address and Subnet Mask so that it can communicate with the switch.
3. Power up the switch for its initial configuration and wait until it has finished its start-up processes.
4. Connect the PC to any port on the switch using a standard Ethernet cable and check the port LED on the switch to make sure the link status is OK.
5. Run your Web browser on the PC and enter the factory default IP address to access the switch's Web interface. If your PC is configured correctly, the Login page of the switch displays.



admin

•••••

Web UI login page

If you do not see the above Login page, perform these steps:

- Refresh the web page.

- Check if there is an IP conflict issue.
- Clear browser cookies and temporary Internet files.
- Check your PC settings again and repeat step 2.

6. Enter the factory default *Username* (**admin**) and *Password* (**admin**) on the Login page (case-sensitive).
7. Click **Login** to log into the switch. The First Time Wizard displays.

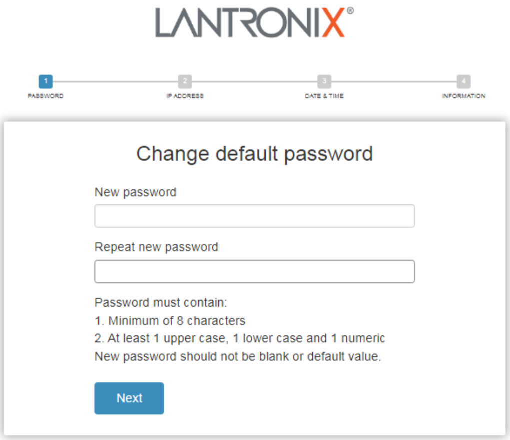
First Time Wizard

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 only displays on the switch web UI. If you have previously logged in via SSH or console connection to the CLI and have saved changes to the running-config file, the First Time Wizard will not be displayed in the web UI.

The First Time Wizard will also display after a factory reset initiated by pressing the Mode/Reset button on the switch. For more information, see Hardware Factory Reset.

Step 1: Change default password

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



Change default password

New password

Repeat new password

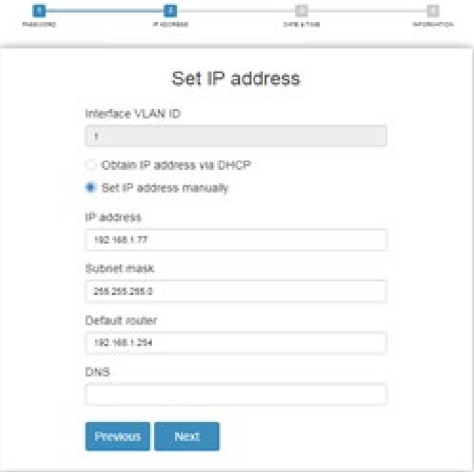
Password must contain:
1. Minimum of 8 characters
2. At least 1 upper case, 1 lower case and 1 numeric
New password should not be blank or default value.

Step 2: Set IP address

Select **Obtain IP address via DHCP** or **Set IP address manually** to set the mode to acquire the IP address.

- If setting the IP address manually, enter IP address, Subnet mask, and Default router. If DNS name resolution will be used, enter a DNS server IP address. The value of 'DNS' must be a valid IP address in dotted decimal notation ('x.y.z.w'). Additional DNS servers can be configured later.
- If obtaining the IP address via DHCP, a DNS server may be used or left blank.

Click the **Next** button.



Set IP address

Interface VLAN ID
1

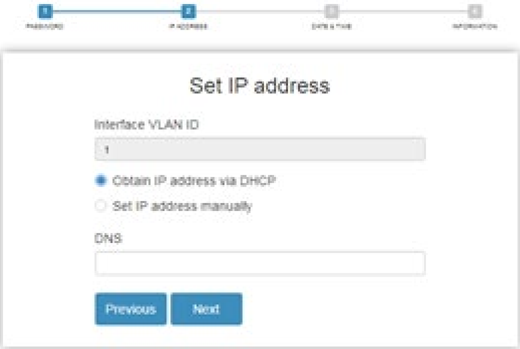
○ Obtain IP address via DHCP
● Set IP address manually

IP address
192.168.1.77

Subnet mask
255.255.255.0

Default router
192.168.1.254

DNS



Set IP address

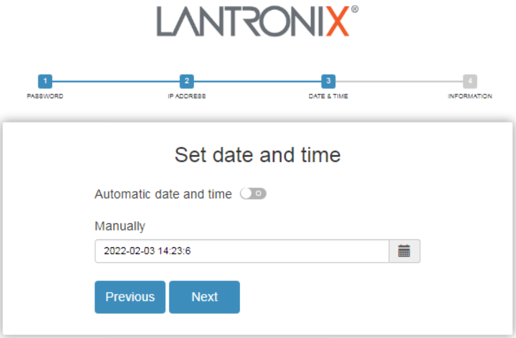
Interface VLAN ID
1

● Obtain IP address via DHCP
○ Set IP address manually

DNS

Step 3: Set date and time

Enable **Automatic date and time** to synchronize the time using an NTP server or select **Manually** to locally set the desired date and time. If you selected the NTP option, enter the NTP server address and select a time zone. Additional NTP servers can be configured later. Click the **Next** button when done.



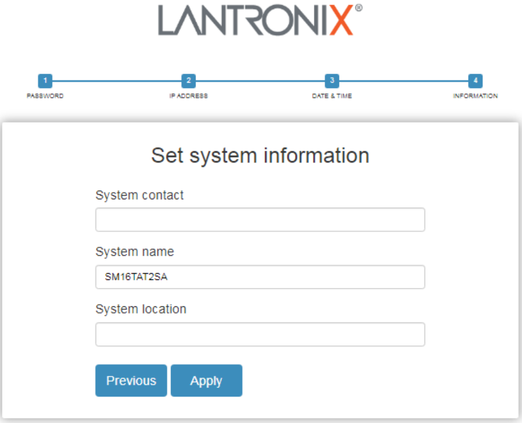
Set date and time

Automatic date and time ○

Manually
2022-02-03 14:23:6

Step 4: Set system information

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



Set system information

System contact

System name
SM16TAT2SA

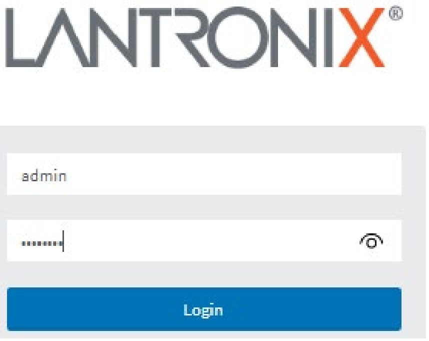
System location

Login to Web UI

Follow this procedure to log into the switch's Web UI after initial configuration.

Your host computer must be able to reach the switch's IP address on the network.

1. Run the web browser and point it to IP address of the switch. The Login page displays.



admin

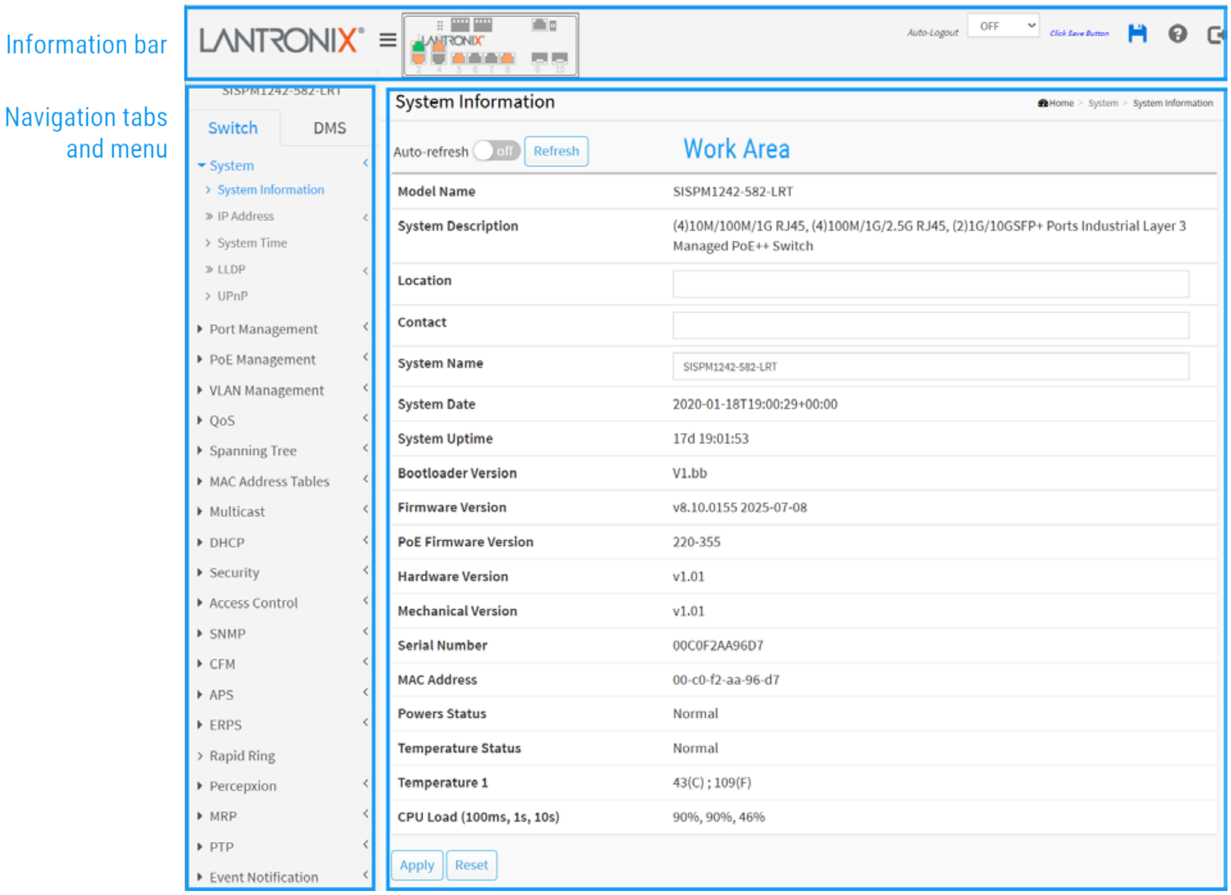
••••••••

2. Enter the username and password.
3. Click **Login**.
4. On successful login, the System Information page displays.

Webpage Navigation

The switch's web interface is composed of the following areas:

- **Information bar** shown at the top of the screen
- **Navigation tabs and contextual menu** which display Switch or DMS menu items
- **Work area** showing information or fields for input entry



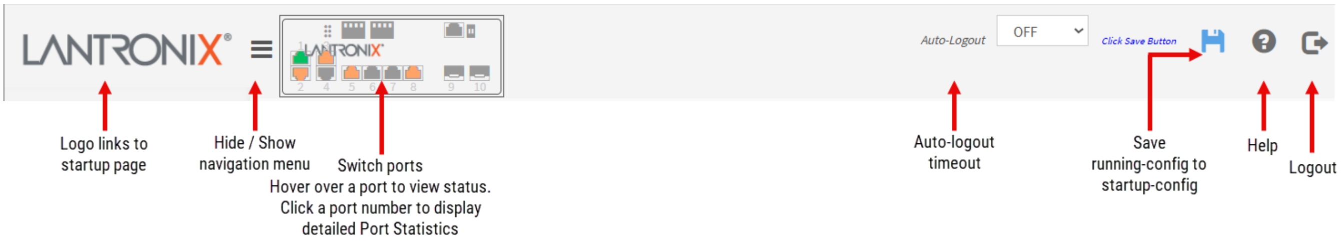
System Information

Model Name	SISPM1242-582-LRT
System Description	(4)10M/100M/1G RJ45, (4)100M/1G/2.5G RJ45, (2)1G/10GSFP+ Ports Industrial Layer 3 Managed PoE++ Switch
Location	
Contact	
System Name	SISPM1242-582-LRT
System Date	2020-01-18T19:00:29+00:00
System Uptime	17d 19:01:53
Bootloader Version	V1.bb
Firmware Version	v8.10.0155 2025-07-08
PoE Firmware Version	220-355
Hardware Version	v1.01
Mechanical Version	v1.01
Serial Number	00C0F2AA96D7
MAC Address	00-c0-f2-aa-96-d7
Powers Status	Normal
Temperature Status	Normal
Temperature 1	43(C) ; 109(F)
CPU Load (100ms, 1s, 10s)	90%, 90%, 46%

Switch web interface

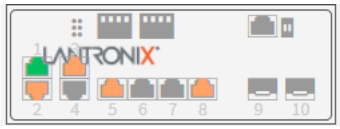
Each of these page areas are described in detail below.

Information Bar


LANTRONIX
Auto-Logout
OFF
Click Save Button
Logo links to startup page
Hide / Show navigation menu
Switch ports
Hover over a port to view status.
Click a port number to display detailed Port Statistics
Auto-logout timeout
Save running-config to startup-config
Help
Logout

The information bar displays a graphic of the switch ports as well as links to display the startup page, hide or show the navigation menu, set auto-logout timeout, save the running-config to startup-config, display page-level help, and log out of the switch.

Switch Ports Graphic

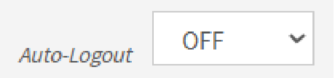


This graphic represents the ports on the switch and provides quick access to view port status and port statistics for a selected port. Ports in use are highlighted to indicate their link state: green for link up (1Gbps), amber for link up (10Mbps or 100Mbps), red for link down, and gray for not connected.

On this graphic you can do the following:

- Hover over a port to view its description.
- Click on the port to display the Port Statistics page for that port.

Auto-Logout



Auto-Logout OFF

The Auto-logout setting defines the amount of idle time before an automatic log out occurs. The selection ranges between 1 and 60 minutes, or OFF. The default is 10 minutes. When set to OFF, no auto-logout occurs.

When the Auto-Logout timeout setting is changed, it directly writes to running-config. After switch reboot (power cycle) or logout and login, the switch gets the timeout setting from the startup-configuration. It is important to save the running-config to the startup-config file after changing the auto-logout if you want to retain the timeout configuration after reboots and logouts.

Note that after reloading factory defaults the switch gets the timeout setting from the default-config.

You can examine the auto-logout setting for the active configuration using the CLI command **show running-config**. The ouput is shown as **exec-timeout autologout 0** where 0 = OFF or a number between 1-5, or 10, 20, 30, 40, 50, 60 represents the idle timeout limit in minutes. If set to the default (10 minutes), the auto-logout configuration is not displayed in the running-config.

Save button

The **Save** button (icon) on the Information bar saves the running-config to startup-config. It behaves as follows:

(blue): The running-config has been modified. Changes in the running-config are volatile and will be lost if the switch is rebooted or loses power. Click to save the running-config to startup-config. **Important: Do not reset or power off the switch while the save to startup-config is in progress.**

(black): The running-config has not been modified.

Help button

Click the **Help** button to display detailed help information for the features, terms glossary, parameters, and buttons on the page. The online help pages provide front-line support for configuring the switch using the Web interface.

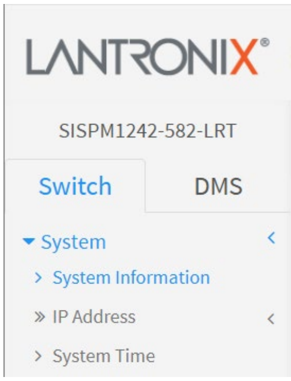
Logout button

Click to end the user session. After logging out, the Web UI login page will be displayed.

Navigation Tabs and Menu

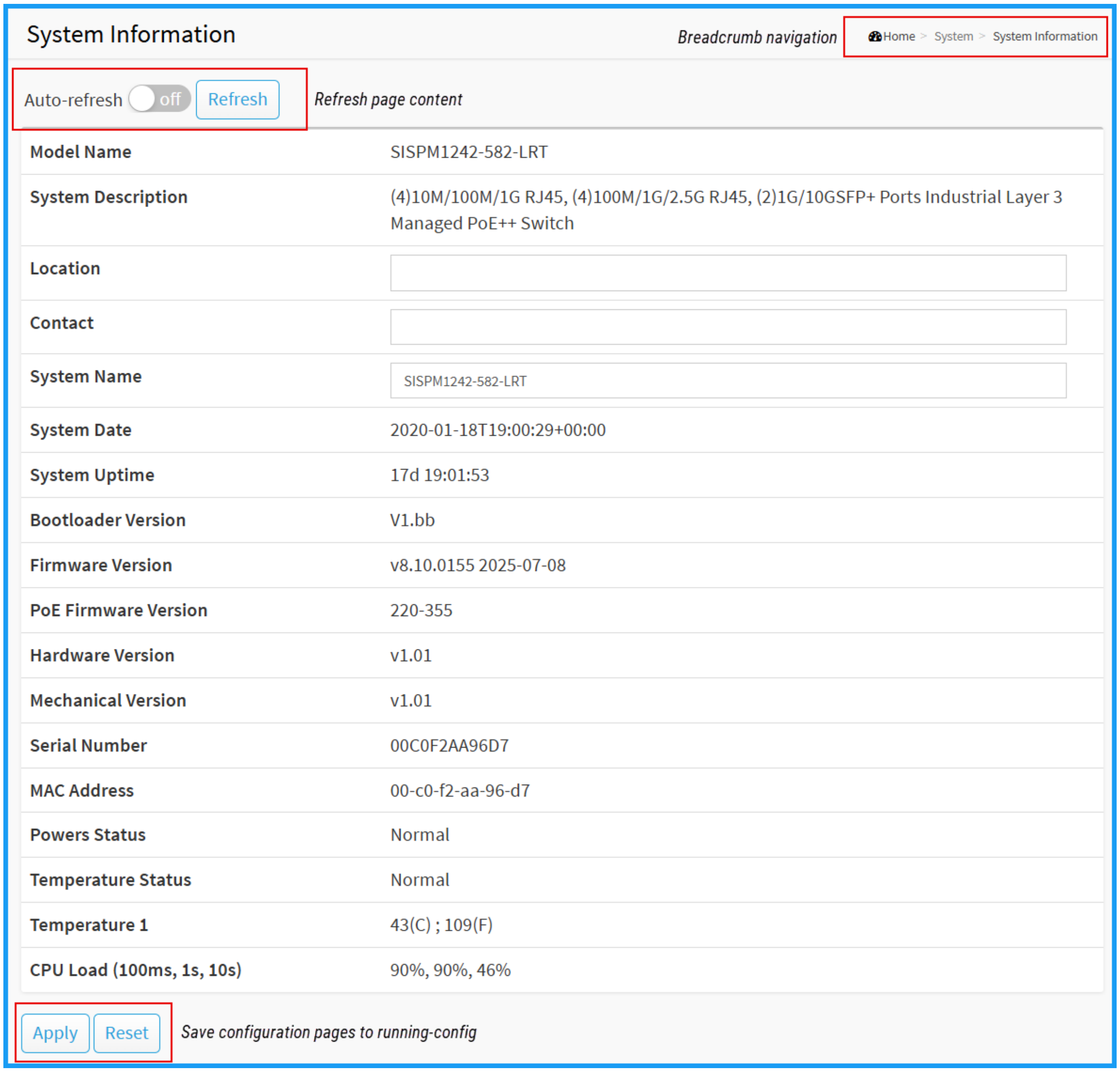
The navigation area provides access to the switch's configuration and status pages and management interface. The navigation pane and menu can be expanded or collapsed. The switch provides the following navigation paths.

- **Switch** – Displays switch configuration and status pages.
- **DMS** – Provides access to the Lantronix Device Management System (DMS), an intelligent management tool embedded in the switch to intuitively help IT/TS in reducing time, cost, and effort.



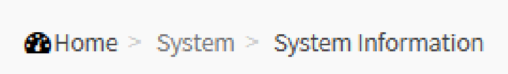
Work Area

The work area displays information and provides input fields to update or reconfigure the switch.



Model Name	SISPM1242-582-LRT
System Description	(4)10M/100M/1G RJ45, (4)100M/1G/2.5G RJ45, (2)1G/10GSFP+ Ports Industrial Layer 3 Managed PoE++ Switch
Location	
Contact	
System Name	SISPM1242-582-LRT
System Date	2020-01-18T19:00:29+00:00
System Uptime	17d 19:01:53
Bootloader Version	V1.bb
Firmware Version	v8.10.0155 2025-07-08
PoE Firmware Version	220-355
Hardware Version	v1.01
Mechanical Version	v1.01
Serial Number	00C0F2AA96D7
MAC Address	00-c0-f2-aa-96-d7
Powers Status	Normal
Temperature Status	Normal
Temperature 1	43(C) ; 109(F)
CPU Load (100ms, 1s, 10s)	90%, 90%, 46%

Breadcrumb-style Navigation

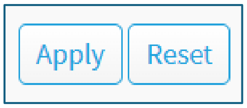


Breadcrumb-style navigation is provided at the top right side of the work area to identify the path to access the displayed page.

Buttons

The pages in the UI contain consistent and familiar buttons to provide ease-of-use in using the switch. The

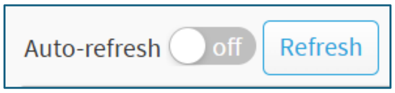
Save or reset configuration changes



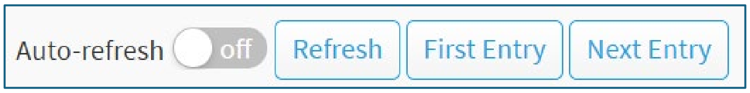
Configuration pages provide the following buttons to save or undo changes on the active page:

- **Apply button**: Click to save changes on the active page to the running-config. If you leave the page without clicking **Apply**, the local changes will not be saved.
  Note: Changes in the running-config are volatile and will be lost if the switch is rebooted or loses power. To save changes in the running-config to the startup-config, click the **Save** button on the Information bar.
- **Reset button**: Click to undo any changes made locally and revert to previously saved values.

Refresh page content and navigate through large data sets



or



Status pages may provide the following buttons to refresh the page's content:

- **Auto-refresh button:** If enabled, the page will refresh automatically every 3 seconds.
- **Refresh button:** Click to refresh the page immediately.
- **Clear:** Click to clear all statistics.
- **First Entry** : Updates the table starting from the first entry in the table.
- **Next Entry** : Updates the table, starting with the entry after the last entry currently displayed.

Certain pages may display additional buttons to help in navigating the information on the page.

3. System

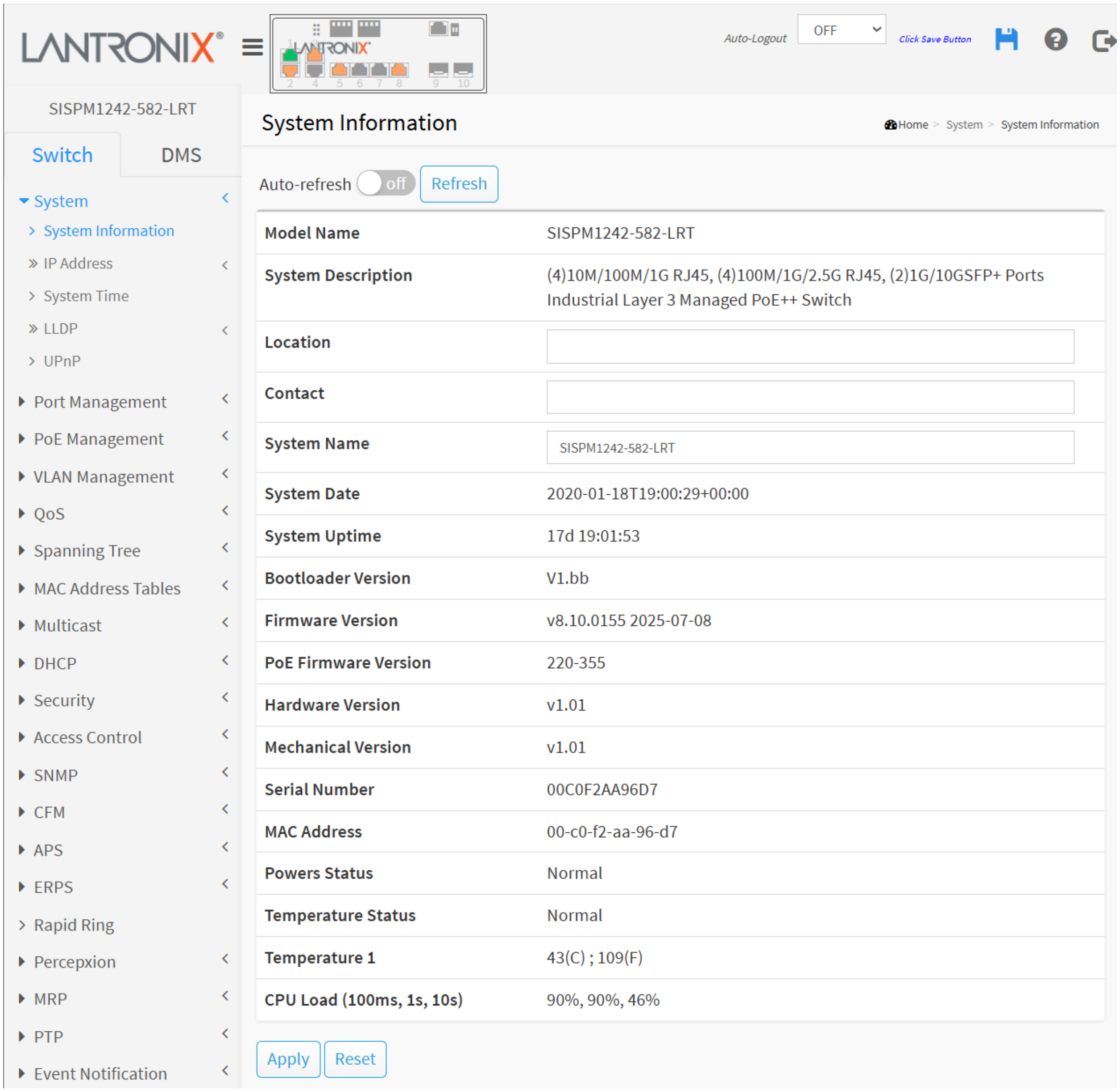
This chapter explains how to set the basic configuration settings for the switch found under the System group menu.

System Information

View system information and configure system name, location, and contact information here.

To view and set System Information in the web UI:

1. Go to System > System Information. The System Information page is displayed.
2. Optional: Enter or edit the available fields.
3. Click the **Apply** button to save the configuration.



System Information

Model Name	SISPM1242-582-LRT
System Description	(4)10M/100M/1G RJ45, (4)100M/1G/2.5G RJ45, (2)1G/10GSFP+ Ports Industrial Layer 3 Managed PoE++ Switch
Location	
Contact	
System Name	SISPM1242-582-LRT
System Date	2020-01-18T19:00:29+00:00
System Uptime	17d 19:01:53
Bootloader Version	V1.bb
Firmware Version	v8.10.0155 2025-07-08
PoE Firmware Version	220-355
Hardware Version	v1.01
Mechanical Version	v1.01
Serial Number	00C0F2AA96D7
MAC Address	00-c0-f2-aa-96-d7
Powers Status	Normal
Temperature Status	Normal
Temperature 1	43(C) ; 109(F)
CPU Load (100ms, 1s, 10s)	90%, 90%, 46%

Parameter descriptions:

Parameter	Description
Model Name	Displays the specific switch model number.
System Description	Displays the given system description.
Location	Edit the field to enter a system location. Default is blank.
Contact	Edit the field to enter a system contact. Default is blank.
System Name	Edit the field to enter a system name. Default is blank.
System Date	Displays the current date and time.
System Uptime	Displays the time the switch has been running since the last power cycle.
Bootloader Version	Displays the current bootloader version number.
Firmware Version	Displays the current firmware version and date.
PoE Firmware Version	Displays the current PoE MCU FW version.
Hardware Version	Displays the hardware version of the device.
Mechanical Version	Displays the mechanical version.
Serial Number	Displays the unique serial number assigned to the switch.
MAC Address	Displays the MAC address of the switch.
Powers Status	Displays the status of power input.
Temperature Status	Displays the status of the operating temperature.
Temperature 1	Displays the temperature at sensor 1.
CPU Load (100ms, 1s, 10s)	Displays the CPU loading of the system.

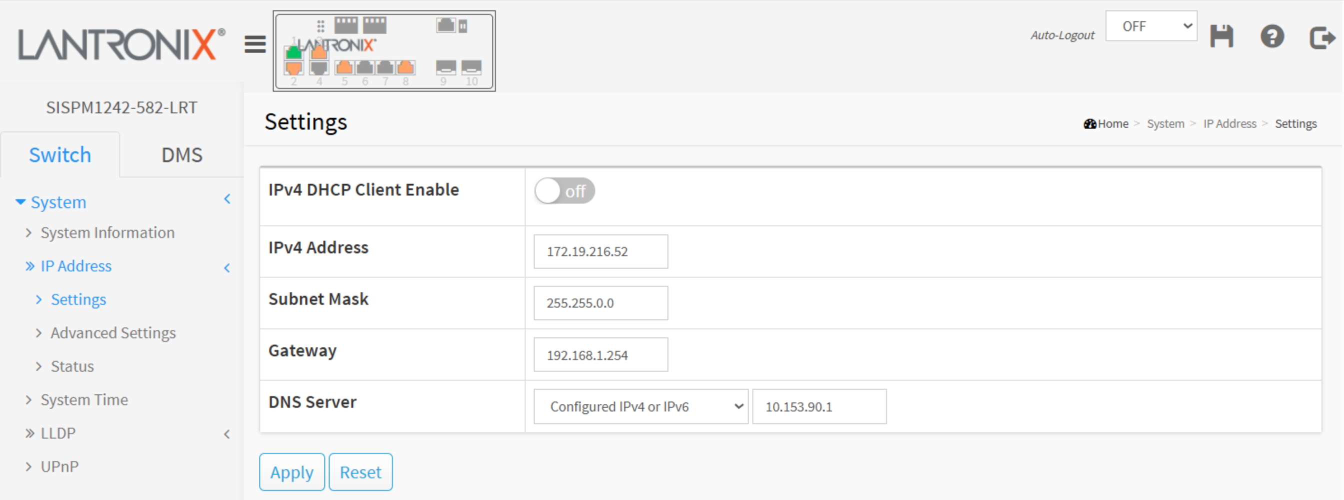
IP Address

IP Settings

The IP settings for VLAN1 can be acquired via DHCP server or configured manually.

To configure IP settings in the web UI:

1. Go to System > IP Address > Settings.
2. Do one of the following:
   - To acquire the IP address via DHCP server, select the **IPv4 DHCP Client Enable** box.
   - To manually configure an IP address, enter an IPv4 address and subnet mask that is 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 domain name resolution, enter the DNS server settings. Multiple DNS servers are configured on the Advanced Settings page.
3. Click **Apply** to save the configuration.



Settings

IPv4 DHCP Client Enable	off
IPv4 Address	172.19.216.52
Subnet Mask	255.255.0.0
Gateway	192.168.1.254
DNS Server	Configured IPv4 or IPv6 10.153.90.1

Parameter descriptions:

Parameter	Description
IPv4 DHCP Client Enable	Check the box to enable DHCP Client support globally. 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. The default is Enabled.
IPv4 Address	The IPv4 address of the interface in dotted decimal notation (e.g., 192.168.1.77). If DHCP is enabled, this field is not user-edited. The field may also be left blank if IPv4 operation on the interface is not desired.
Subnet Mask	The IPv4 network mask. If DHCP is enabled, this field configures the fallback address network mask. The field may be left blank if IPv4 operation on the interface is not desired - or no DHCP fallback address is desired. User IP subnet mask of the entry (e.g., 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. The following modes are supported:

Parameter	Description
	• ***No DNS server***: No DNS server will be used. • ***Configured IPv4 or IPv6***: Explicitly provide the IP address of the DNS Server in dotted decimal notation. • ***From any DHCP interfaces***: The first DNS server offered from a DHCP lease to a DHCP-enabled interface will be used. • ***From this DHCP interface***: Specify from which DHCP-enabled interface a provided DNS server should be preferred. Configured on the Advanced Settings page.

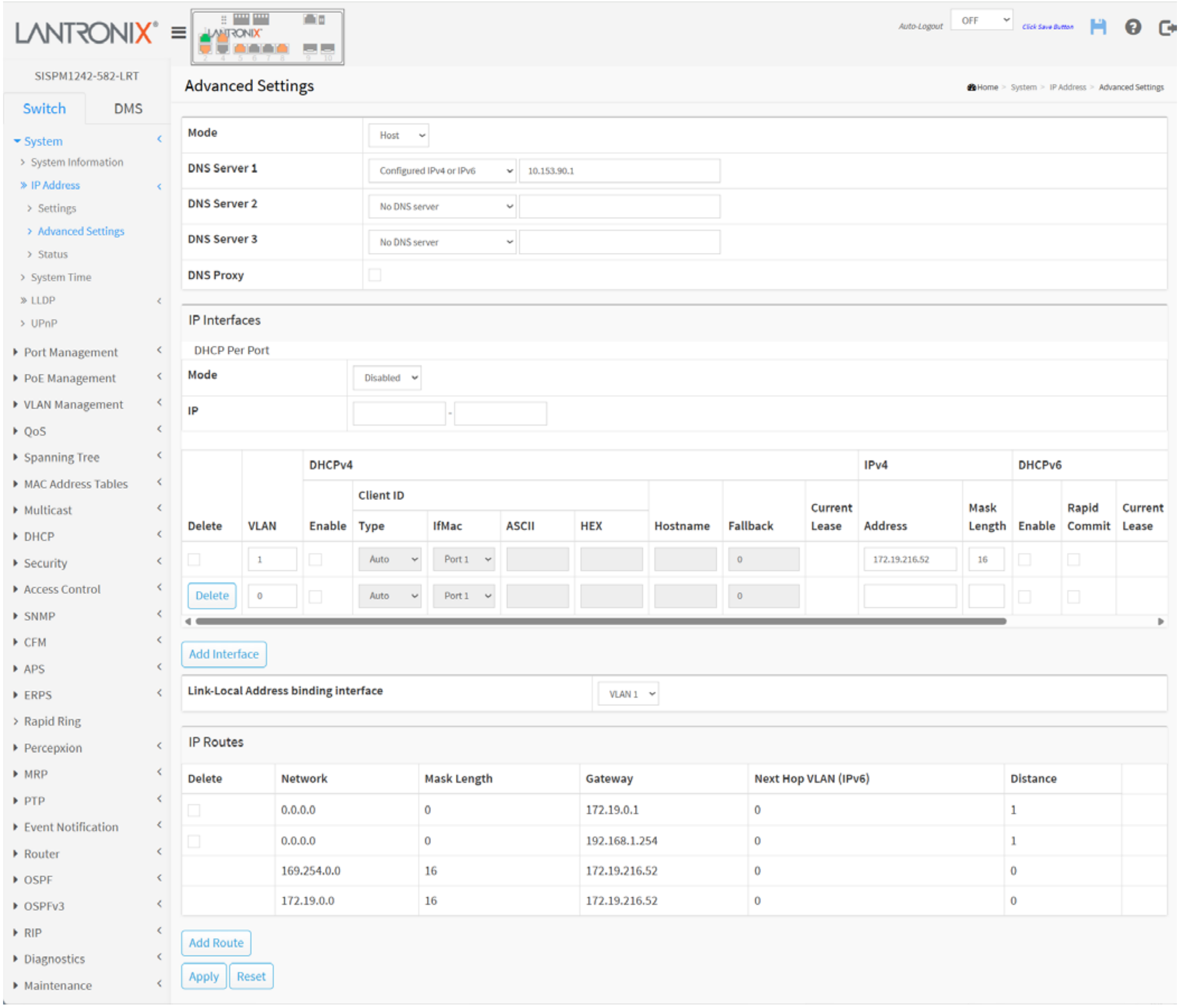
Advanced Settings

Configure managed IP information, IP interfaces, and IP routes. You can configure up to 32 interfaces and 32 routes.

For more information about DHCP per Port, see DHCP per Port and DHCP per VLAN.

To configure advanced IP settings in the web UI:

1. Go to System > IP Address > Advanced Settings.
2. Configure the desired settings. Refer to the Parameter Descriptions below or check the online help page.
3. Click **Apply**.



Advanced Settings

Mode	Host	
DNS Server 1	Configured IPv4 or IPv6	10.153.90.1
DNS Server 2	No DNS server	
DNS Server 3	No DNS server	
DNS Proxy	□	

IP Interfaces

DHCP Per Port

Mode	Disabled
IP	-

		DHCPv4								IPv4		DHCPv6		
			Client ID											
Delete	VLAN	Enable	Type	IfMac	ASCII	HEX	Hostname	Fallback	Current Lease	Address	Mask Length	Enable	Rapid Commit	Current Lease
□	1	□	Auto	Port 1				0		172.19.216.52	16	□	□	
Delete	0	□	Auto	Port 1				0				□	□	

Add Interface

Link-Local Address binding interface	VLAN 1

IP Routes

Delete	Network	Mask Length	Gateway	Next Hop VLAN (IPv6)	Distance
□	0.0.0.0	0	172.19.0.1	0	1
□	0.0.0.0	0	192.168.1.254	0	1
	169.254.0.0	16	172.19.216.52	0	0
	172.19.0.0	16	172.19.216.52	0	0

Add Route

Apply Reset

Parameter descriptions:

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

DNS Server (1-3): Controls the DNS name resolution done by the switch. The index of the server presents the preference (lower number has higher priority) in doing DNS name resolution. The following modes are supported:

- ***No DNS server***: No DNS server will be used.
- ***Configured IPv4 or IPv6***: Explicitly provide the IPv4 or IPv6 address of the DNS Server. Make sure the configured DNS server is reachable for activating DNS service.
- ***From any DHCP interfaces***: The first DNS server offered from a DHCP lease to a DHCP-enabled interface will be used.
- ***From this DHCP interface***: Specify from which DHCP-enabled interface a provided DNS server should be preferred.

DNS Proxy: When DNS proxy is selected, the 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

Add Interface button: Click to add a new IP interface. A maximum of 32 interfaces is supported.

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

DHCP Per Port

For more information about DHCP per Port, see DHCP per Port and DHCP per VLAN.

Mode: Select Enable or Disable DHCP per Port operation. The default is Disabled.

IP: Define the IP range for DHCP Per Port. The range must be equal to the number of switch RJ45/TP ports.

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. This 'DHCP IP per Port' function lets you assign a static IP address from a DHCP pool to a switch port such that 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 typical binding method used on this and most other switches.

DHCPv4 Enabled: Enable the IPv4 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 Client Identifier Type: This specifies which of the three type below, i.e. IfMac, ASCII or HEX, shall be used for the Client Identifier. See RFC-2132 section 9.14.

- **IPv4 Client Identifier IfMac:** The interface name of DHCP client identifier. When DHCPv4 client is enabled and the client identifier type is 'ifmac', the configured interface's hardware MAC address will be used in the DHCP option 61 field.
- **IPv4 Client Identifier ASCII:** The ASCII string of DHCP client identifier. When DHCPv4 client is enabled and the client identifier type is 'ascii', the ASCII string will be used in the DHCP option 61 field.
- **IPv4 Client Identifier HEX:** The hexadecimal string of DHCP client identifier. When DHCPv4 client is enabled and the client identifier type 'hex', the hexadecimal value will be used in the DHCP option 61 field.

IPv4 DHCP Hostname: The hostname of DHCP client. If DHCPv4 client is enabled, the configured hostname will be used in the DHCP option 12 field. When this value is empty string, the field use the configured system name plus the latest three bytes of system MAC addresses as the hostname.

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

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

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

IPv4 Mask: The IPv4 network mask, in number of bits (prefix length). Valid values are 0 - 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 valid IPv4 address. For example, ::192.1.2.34. The field may be left blank if IPv6 operation on the interface is not desired.

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

Resolving IPv6 DAD: The link-local address is formed from an interface identifier based on the hardware address which is supposed to be uniquely assigned. Once the DAD (Duplicate Address Detection) detects the address duplication, the operation on the interface SHOULD be disabled.

At this moment, manual intervention is required to resolve the address duplication. For example, check whether the loop occurs in the VLAN or there is indeed other device occupying the same hardware address as the device in the VLAN.

After making sure the specific link-local address is unique on the IPv6 link in use, delete and then add the specific IPv6 interface to restart the IPv6 operations on this interface.

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

A link-local address is a network address that is valid only for communication within the network segment or the broadcast domain that the host is connected to. Link-local addresses are not guaranteed to be unique beyond their network segment. IPv4 link-local addresses are assigned from address block 169.254.0.0/16 (169.254.0.0 - 169.254.255.255). In IPv6, they are assigned from the block fe80::/10.

IP Routes

Add Route button: Click to add a new IP route. A maximum of 32 routes is supported.

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

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

Note: You must provide this parameter if you will be configuring L3 Routing.

Mask Length: The destination IP network or host mask, in number of bits (prefix length). It defines how much of a network address that must match, to qualify for this route. Valid values are 0 - 32 bits for IPv4 routes and128 bits for IPv6 routes. Only a default route will have a mask length of 0 (as it will match anything).

Note: You must provide this parameter if you will be configuring L3 Routing.

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

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

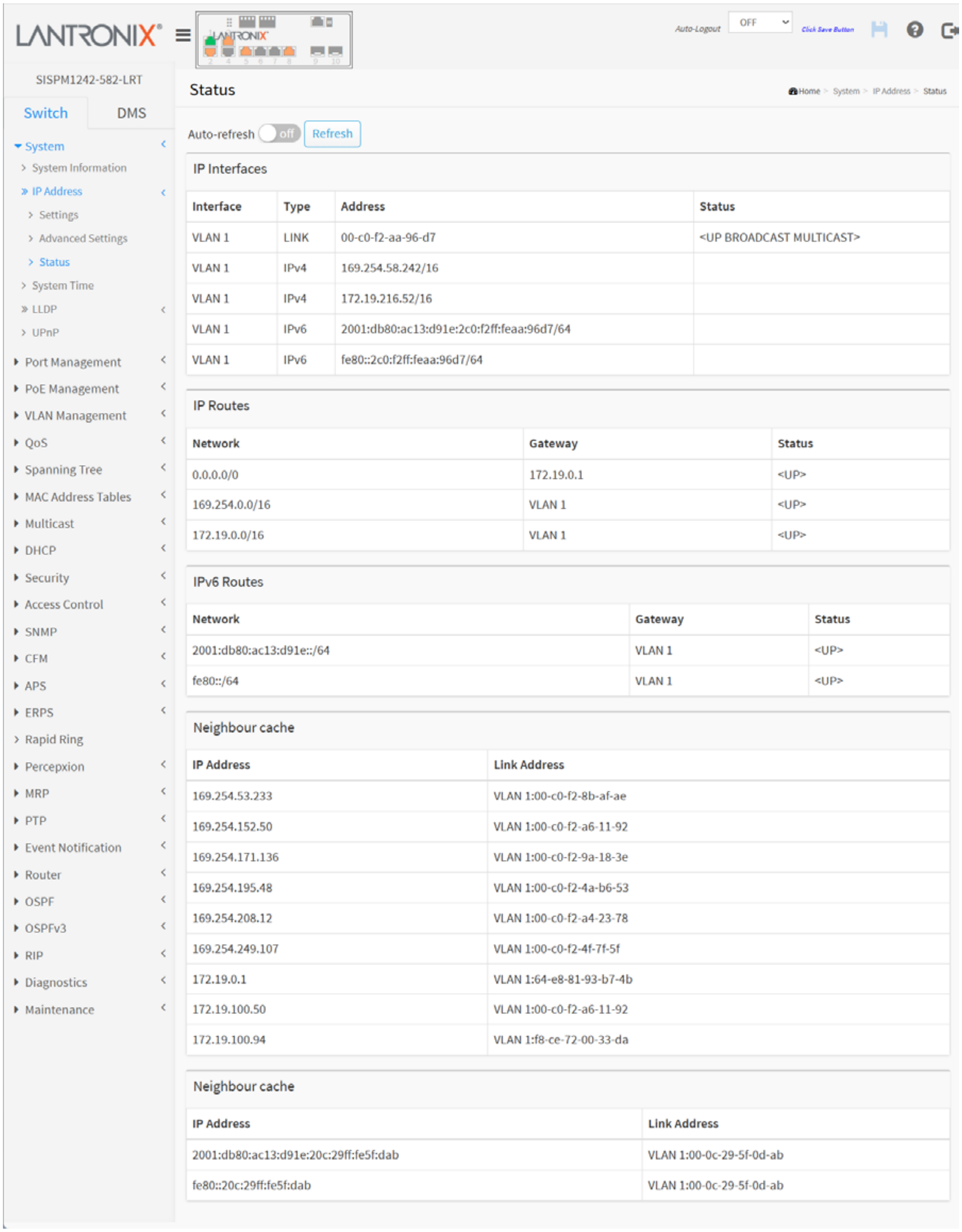
Distance: The distance value of the route entry is used to provide the priority information of the routing protocols to routers. When two or more different routing protocols are involved and have the same destination, the distance value can be used to select the best path.

Status

This page displays the status of the IP protocol layer. This includes the IP interfaces, the IPv4 and IPv6 routes, and the neighbor cache (ARP cache) status.

To view the IP protocol layer status:

1. Go to System > IP Address > Status.
2. **Auto-refresh** will refresh the page every 3 seconds. **Refresh** will refresh the page immediately.



Status

Auto-refresh off Refresh

IP Interfaces

Interface	Type	Address	Status
VLAN 1	LINK	00-c0-f2-aa-96-d7	<UP BROADCAST MULTICAST>
VLAN 1	IPv4	169.254.58.242/16	
VLAN 1	IPv4	172.19.216.52/16	
VLAN 1	IPv6	2001:db80:ac13:d91e:2c0:f2ff:feaa:96d7/64	
VLAN 1	IPv6	fe80::2c0:f2ff:feaa:96d7/64	

IP Routes

Network	Gateway	Status
0.0.0.0/0	172.19.0.1	<UP>
169.254.0.0/16	VLAN 1	<UP>
172.19.0.0/16	VLAN 1	<UP>

IPv6 Routes

Network	Gateway	Status
2001:db80:ac13:d91e::/64	VLAN 1	<UP>
fe80::/64	VLAN 1	<UP>

Neighbour cache

IP Address	Link Address
169.254.53.233	VLAN 1:00-c0-f2-8b-af-ae
169.254.152.50	VLAN 1:00-c0-f2-a6-11-92
169.254.171.136	VLAN 1:00-c0-f2-9a-18-3e
169.254.195.48	VLAN 1:00-c0-f2-4a-b6-53
169.254.208.12	VLAN 1:00-c0-f2-a4-23-78
169.254.249.107	VLAN 1:00-c0-f2-4f-7f-5f
172.19.0.1	VLAN 1:64-e8-81-93-b7-4b
172.19.100.50	VLAN 1:00-c0-f2-a6-11-92
172.19.100.94	VLAN 1:f8-ce-72-00-33-da

Neighbour cache

IP Address	Link Address
2001:db80:ac13:d91e:20c:29ff:fe5f:dab	VLAN 1:00-0c-29-5f-0d-ab
fe80::20c:29ff:fe5f:dab	VLAN 1:00-0c-29-5f-0d-ab

IP Interfaces

Interface : Shows the name of the interface.

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

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

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

IPv4/IPv6 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 IPv4/IPv6 address of the entry.

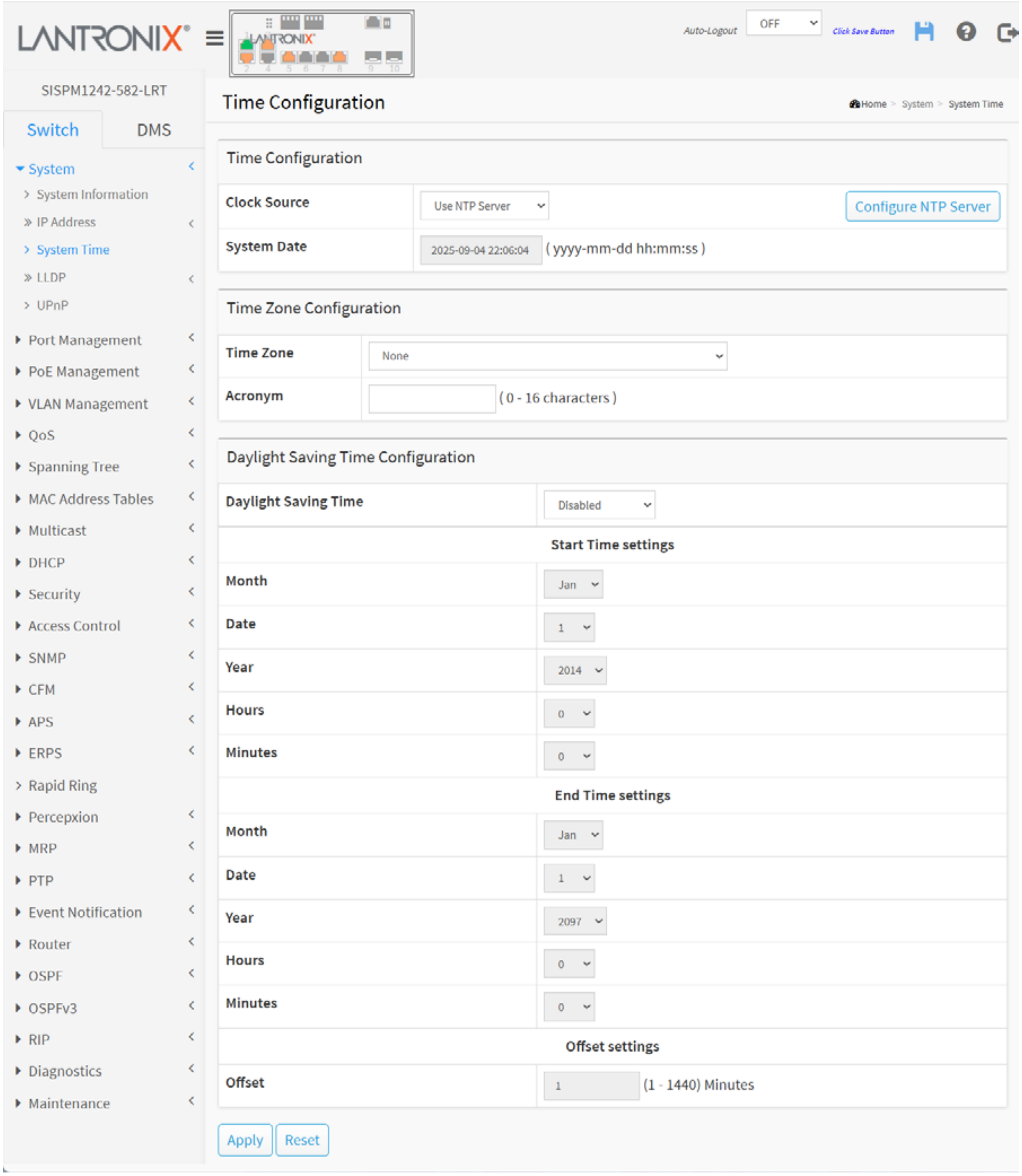
Link Address : Shows the Link (MAC) address for which a binding to the IP address given exists.

System Time

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

To configure the system time:

1. Go to System > System Time.
2. Select the Clock Source. The options are *Use Local Settings* or *Use NTP Server*.
3. Configure the appropriate settings for the clock source selection. If you selected *Use NTP Server*, click *Configure NTP Server* and configure up to 5 NTP servers.
4. Click **Apply**.



Time Configuration

Time Configuration

Clock Source	Use NTP Server (Configure NTP Server)
System Date	2025-09-04 22:06:04 (yyyy-mm-dd hh:mm:ss)

Time Zone Configuration

Time Zone	None
Acronym	(0 - 16 characters)

Daylight Saving Time Configuration

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

Apply Reset

Parameter Descriptions

Time Configuration

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

- ***Use Local Settings*** : Clock Source from Local Time (default).
- ***NTP Server*** : Clock Source from NTP Server.

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

Time Zone Configuration

Time Zone : Lists various Time Zones worldwide. Select appropriate Time Zone from the drop down. The default is None.

Acronym : Set the acronym of the time zone. This is a user-configurable acronym to identify the time zone. Range: Up to 16 characters.

Daylight Saving Time Configuration

Daylight Saving Time : This is used to set the clock forward or backward according to the configurations set below for a defined Daylight Saving Time duration.

- Select '***Disable***' to disable the Daylight Saving Time configuration. The default is Disabled.
- Select '***Recurring***' and configure the Daylight Saving Time duration to repeat the configuration every year.
- Select '***Non-Recurring'*** and configure the Daylight Saving Time duration for a one-time configuration.

Start time settings:

- ***Week*** - Select the starting day, date, and time.
- ***Day*** - Select the starting day.
- ***Month*** - Select the starting month.
- ***Hours*** - Select the starting hour.
- ***Minutes*** - Select the starting minute.

End time settings :

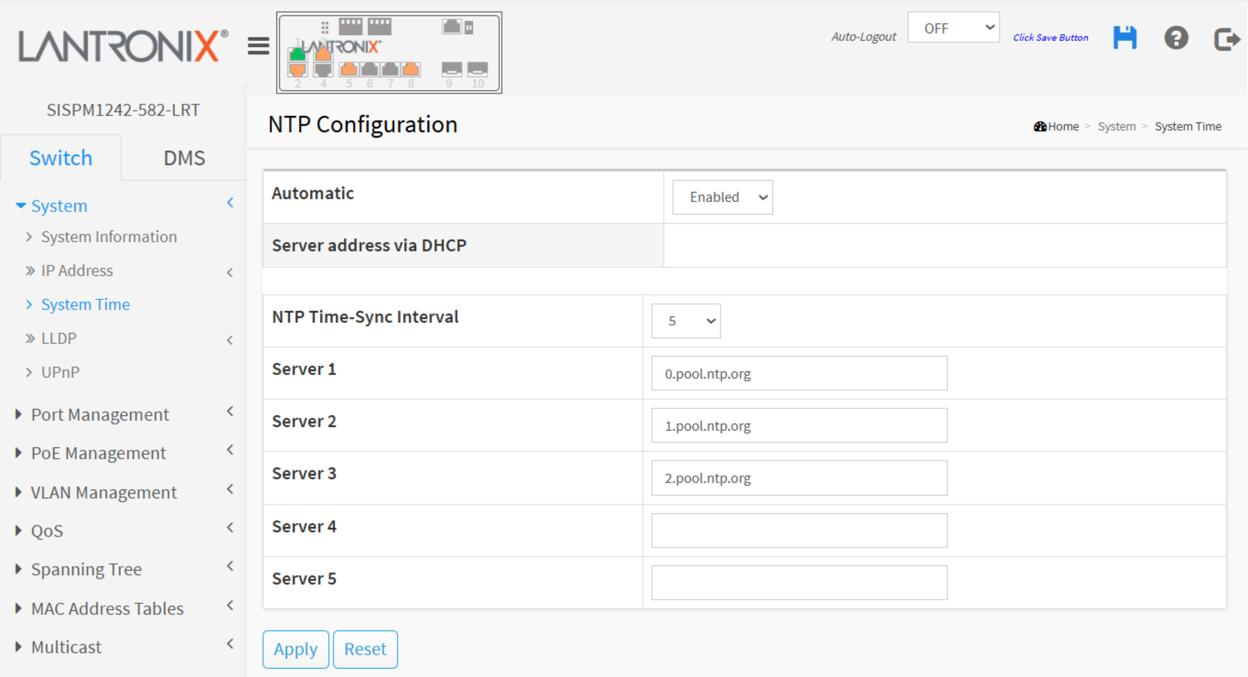
- ***Week*** - Select the ending day, date, and time.
- ***Day*** - Select the ending day.
- ***Month*** - Select the ending month.
- ***Hours*** - Select the ending hour.
- ***Minutes*** - Select the starting minute.

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

Configure NTP Server

NTP (Network Time Protocol) is used to synchronize timekeeping among devices in a network based on Coordinated Universal Time (UTC). It may take a few minutes for the switch to synchronize with the NTP server. The Time Zone setting should be selected before syncing via NTP to display the local time.

Though NTP synchronizes the time automatically, you must refresh the UI page to update the displayed system time.



NTP Configuration

Automatic	Enabled
Server address via DHCP	

NTP Time-Sync Interval	5
Server 1	0.pool.ntp.org
Server 2	1.pool.ntp.org
Server 3	2.pool.ntp.org
Server 4	
Server 5	

Parameter descriptions:

Automatic: Select to enable or disable automatic NTP configuration. The default is Disabled.

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

Server # (1 to 5): Enter the IPv4 or IPv6 address of the NTP server, up to 5 servers.

LLDP

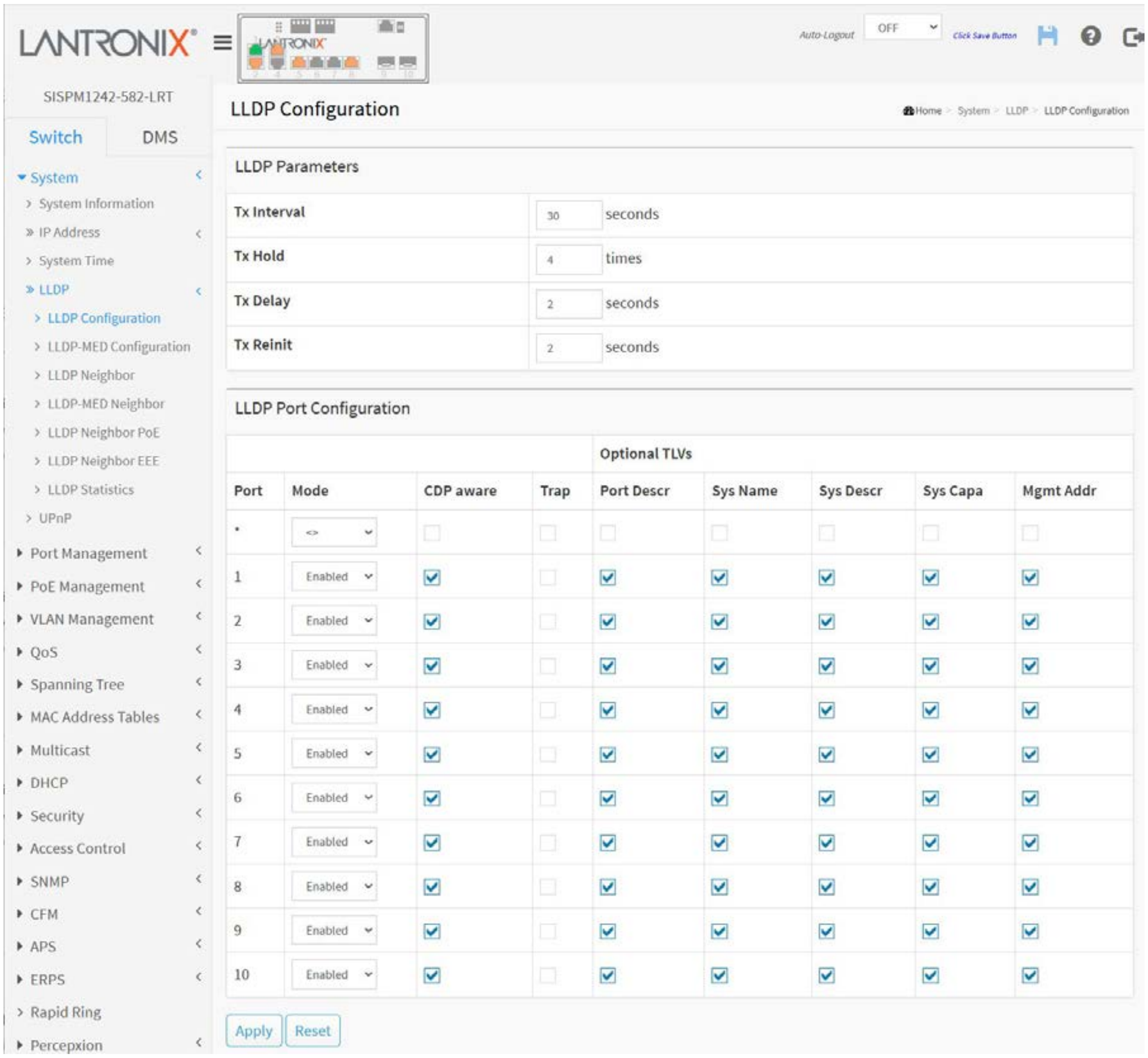
Link Layer Discovery Protocol (LLDP) provides a standards-based method for enabling switches to advertise themselves to adjacent devices and to learn about adjacent LLDP devices. LLDP is a vendor-neutral Link Layer protocol in the Internet Protocol Suite used by network devices for advertising their identity, capabilities, and neighbors on 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.

LLDP Configuration

View and configure the LLDP settings. You can configure LLDP and detailed per-port parameters; the settings will take effect immediately.

To configure LLDP:

1. Go to System > LLDP > LLDP Configuration.
2. Configure the LLDP timing parameters and LLDP port configuration per your requirement.
3. Click **Apply**.



LLDP Configuration

LLDP Parameters

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

LLDP Port Configuration

				Optional TLVs				
Port	Mode	CDP aware	Trap	Port Descr	Sys Name	Sys Descr	Sys Capa	Mgmt Addr
*	<>	□	□	□	□	□	□	□
1	Enabled	☑	□	☑	☑	☑	☑	☑
2	Enabled	☑	□	☑	☑	☑	☑	☑
3	Enabled	☑	□	☑	☑	☑	☑	☑
4	Enabled	☑	□	☑	☑	☑	☑	☑
5	Enabled	☑	□	☑	☑	☑	☑	☑
6	Enabled	☑	□	☑	☑	☑	☑	☑
7	Enabled	☑	□	☑	☑	☑	☑	☑
8	Enabled	☑	□	☑	☑	☑	☑	☑
9	Enabled	☑	□	☑	☑	☑	☑	☑
10	Enabled	☑	□	☑	☑	☑	☑	☑

Parameter descriptions:

LLDP Parameters

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

Tx Hold : Each LLDP frame contains information about how long the information in the LLDP frame will be considered valid. The LLDP information valid period is set to Tx Hold multiplied by Tx Interval seconds. Valid values are 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 time between the shutdown frame and a new LLDP initialization. Valid values are 1 - 10 seconds.

LLDP Port Configuration :

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

Mode : Select an LLDP mode:

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

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

CDP Aware : Select Cisco Discovery Protocol (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 neighbor devices and link malfunctions.

<u>Optional TLVs</u>

- **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.

LLDP-MED Configuration

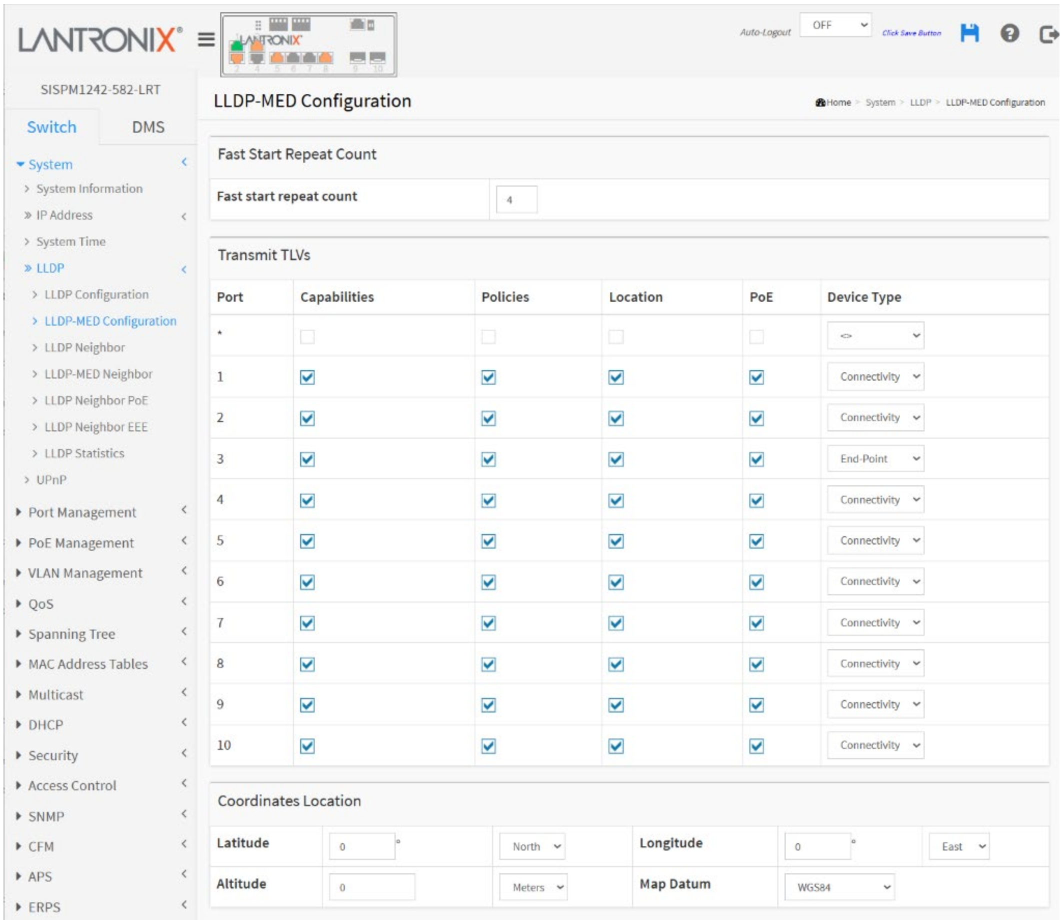
Media Endpoint Discovery (MED) is an enhancement of LLDP, known as LLDP-MED that provides these facilities:

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

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

To configure LLDP-MED:

1. Go to System > LLDP > LLDP-MED Configuration.
2. Configure the settings per your requirement.
3. Click **Apply**.



LLDP-MED Configuration

Fast Start Repeat Count

Fast start repeat count: 4

Transmit TLVs

Port	Capabilities	Policies	Location	PoE	Device Type
*	□	□	□	□	<>
1	☑	☑	☑	☑	Connectivity
2	☑	☑	☑	☑	Connectivity
3	☑	☑	☑	☑	End-Point
4	☑	☑	☑	☑	Connectivity
5	☑	☑	☑	☑	Connectivity
6	☑	☑	☑	☑	Connectivity
7	☑	☑	☑	☑	Connectivity
8	☑	☑	☑	☑	Connectivity
9	☑	☑	☑	☑	Connectivity
10	☑	☑	☑	☑	Connectivity

Coordinates Location

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

Figure 3-1 LLDP-MED Configuration (1/2)

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

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

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

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

Transmit TLVs

Port : The interface name to which the configuration applies.

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

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

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

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

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

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

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

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

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

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

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.

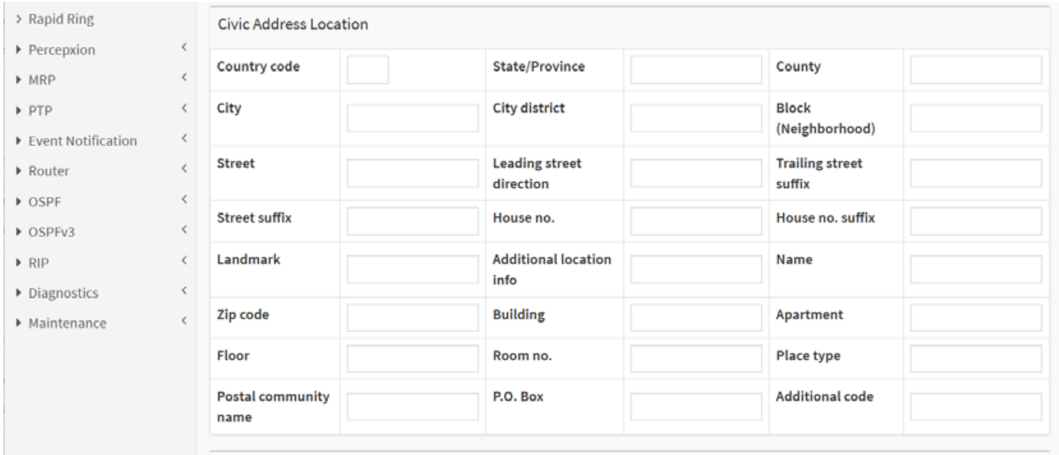
Longitude : Longitude should be normalized to within 0-180 degrees with a maximum of 5 digits. It is possible to specify the direction to either East of the prime meridian or West of the prime meridian.

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

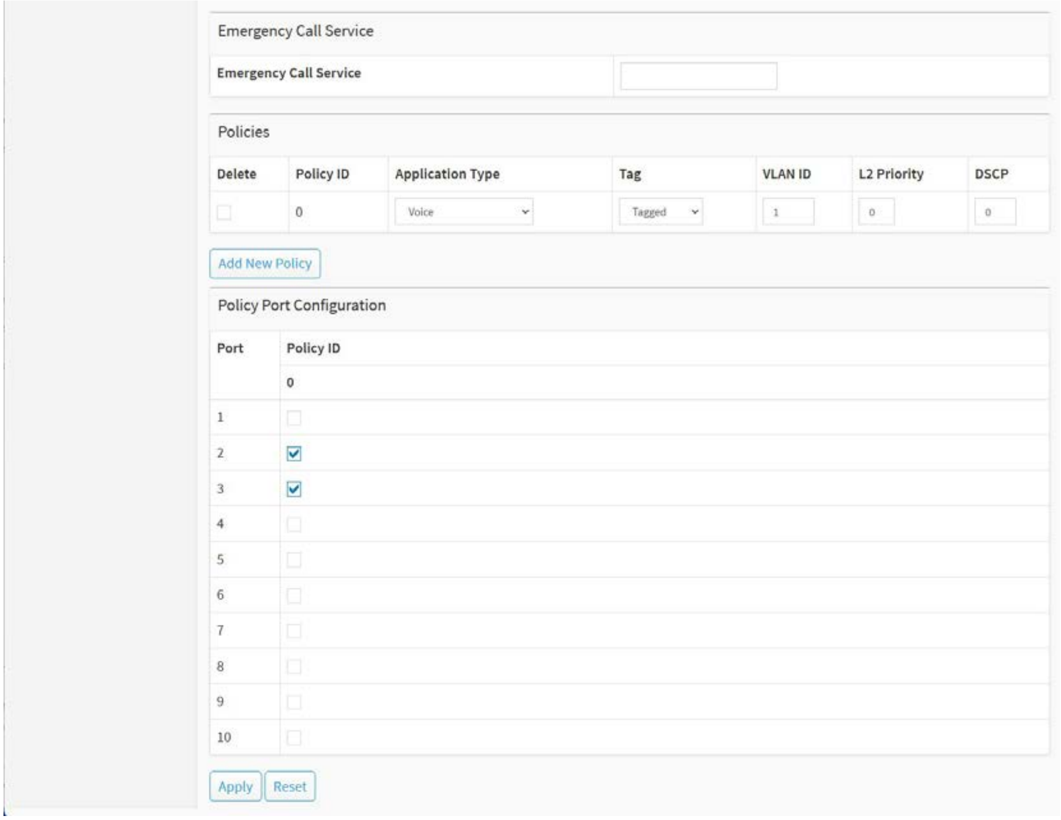
Country code		State/Province		County	
City		City district		Block (Neighborhood)	
Street		Leading street direction		Trailing street suffix	
Street suffix		House no.		House no. suffix	
Landmark		Additional location info		Name	
Zip code		Building		Apartment	
Floor		Room no.		Place type	
Postal community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

Figure 3-2 LLDP-MED Configuration (2/3)

Civic Address Location

This section contains fields to describe where the switch is located. Enter information relevant per your requirements. Click the **Help** button on the UI to view detailed field descriptions.

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



Emergency Call Service

Emergency Call Service	

Policies

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

Policy Port Configuration

Port	Policy ID
	0
1	□
2	☑
3	☑
4	□
5	□
6	□
7	□
8	□
9	□
10	□

Emergency Call Service

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

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

Policies:

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

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

The network policy attributes advertised are:

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

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

1. Voice
2. Guest Voice
3. Softphone Voice

4. Video Conferencing
5. Streaming Video
6. Control / Signaling (conditionally support a separate network policy for the media types above)

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

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

Policy settings:

Add New Policy : Click to add a new policy. Click **Apply** to save changes to running-config.

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

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

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

- ***Voice*** - for use by dedicated IP Telephony handsets and other similar appliances supporting interactive voice services. These devices are typically deployed on a separate VLAN for ease of deployment and enhanced security by isolation from data applications.
- ***Voice Signalling (conditional)*** - for use in network topologies that require a different policy for the voice signaling than for the voice media. This application type should not be advertised if all the same network policies apply as those advertised in the Voice application policy.
- ***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 signaling than for the guest voice media. This application type should not be advertised if all the same network policies apply as those advertised in the Guest Voice application policy.
- ***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 signaling than for the video media. This application type should not be advertised if all the same network policies apply as those advertised in the Video Conferencing application policy.

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

- ***Untagged*** indicates that the device is using an untagged frame format and as such does not include a tag header as defined by IEEE 802.1Q-2003. In this case, both the VLAN ID and the Layer 2 priority fields are ignored and only the DSCP value has relevance.
- ***Tagged*** indicates that the device is using the IEEE 802.1Q tagged frame format, and that both the VLAN ID and the Layer 2 priority values are being used, as well as the DSCP value. The tagged format includes an additional field known as the tag header. The tagged frame format also includes priority tagged frames as defined by IEEE 802.1Q-2003.

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

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

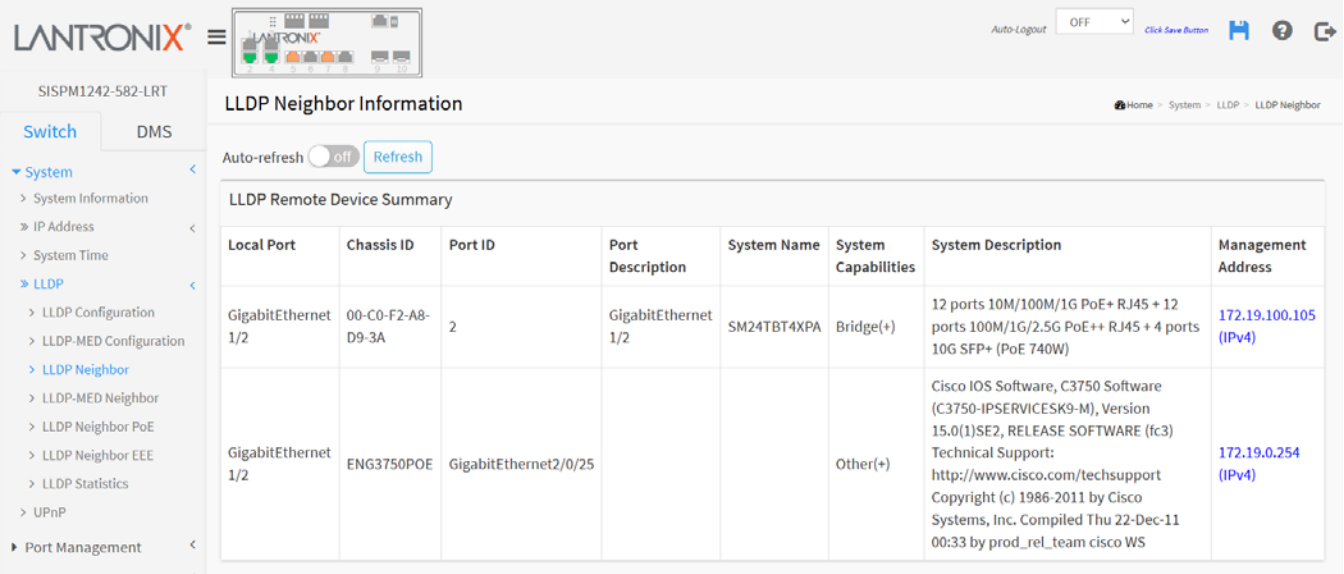
DSCP : The DSCP value to be used to provide Diffserv node behavior for the specified application type as defined in IETF RFC 2474. DSCP may contain one of 64 code point values (0 - 63). A value of 0 represents use of the default DSCP value as defined in IETF RFC 2475.

LLDP Neighbor Information

This page provides a status overview for all LLDP neighbors.

To show LLDP neighbors:

1. Go to System > LLDP > LLDP Neighbor.



LLDP Neighbor Information

Auto-refresh off

LLDP Remote Device Summary

Local Port	Chassis ID	Port ID	Port Description	System Name	System Capabilities	System Description	Management Address
GigabitEthernet 1/2	00-C0-F2-A8-D9-3A	2	GigabitEthernet 1/2	SM24TBT4XPA	Bridge(+)	12 ports 10M/100M/1G PoE+ RJ45 + 12 ports 100M/1G/2.5G PoE++ RJ45 + 4 ports 10G SFP+ (PoE 740W)	172.19.100.105 (IPv4)
GigabitEthernet 1/2	ENG3750POE	GigabitEthernet2/0/25			Other(+)	Cisco IOS Software, C3750 Software (C3750-IPSERVICESK9-M), Version 15.0(1)SE2, RELEASE SOFTWARE (fc3) Technical Support: http://www.cisco.com/techsupport Copyright (c) 1986-2011 by Cisco Systems, Inc. Compiled Thu 22-Dec-11 00:33 by prod_rel_team cisco WS	172.19.0.254 (IPv4)

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

Parameter descriptions:

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

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

Port ID : The Remote Port ID is the identification of the neighbor port.

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

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

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

- Other
- Repeater
- Bridge
- WLAN Access Point
- Router
- Telephone
- DOCSIS cable device
- Station only
- Reserved

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

System Description : Displays the system description.

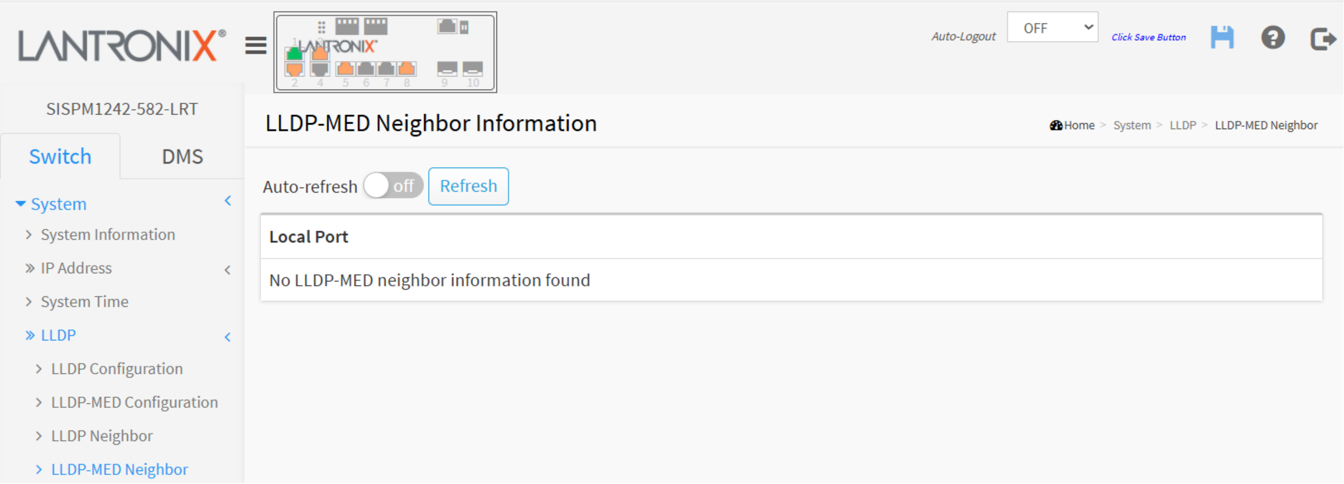
Management Address : The neighbor unit's address that is used for higher layer entities to assist discovery by the network management. This could for instance hold the neighbor's IP address. You can click the linked text to navigate to the device's webpage.

LLDP-MED Neighbor Information

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

To show LLDP-MED neighbor information:

1. Go to System > LLDP > LLDP-MED Neighbor.



LLDP-MED Neighbor Information

Local Port
No LLDP-MED neighbor information found

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

Parameter descriptions:

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

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

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

1. LAN Switch/Router

2. IEEE 802.1 Bridge

3. IEEE 802.3 Repeater (included for historical reasons)

4. IEEE 802.11 Wireless Access Point

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

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

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

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

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

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

1. LLDP-MED capabilities

2. Network Policy

3. Location Identification

4. Extended Power via MDI - PSE

5. Extended Power via MDI - PD

6. Inventory

7. Reserved

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

- ***Voice*** - for use by dedicated IP Telephony handsets and other similar appliances supporting interactive voice services. These devices are typically deployed on a separate VLAN for ease of deployment and enhanced security by isolation from data applications.
- ***Voice Signalling*** - for use in network topologies that require a different policy for the voice signalling than for the voice media.
- ***Guest Voice*** - to support a separate limited feature-set voice service for guest users and visitors with their own IP Telephony handsets and other similar appliances supporting interactive voice services.
- ***Guest Voice Signalling*** - for use in network topologies that require a different policy for the guest voice signalling than for the guest voice media.
- ***Softphone Voice*** - for use by softphone applications on typical data centric devices, such as PCs or laptops.
- ***Video Conferencing*** - for use by dedicated Video Conferencing equipment and other similar appliances supporting real-time interactive video/audio services.
- ***Streaming Video*** - for use by broadcast or multicast based video content distribution and other similar applications supporting streaming video services that require specific network policy treatment. Video applications relying on TCP with buffering would not be an intended use of this application type.
- ***Video Signalling*** - for use in network topologies that require a separate policy for the video signalling than for the video media.

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

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

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

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

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

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

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

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

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

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

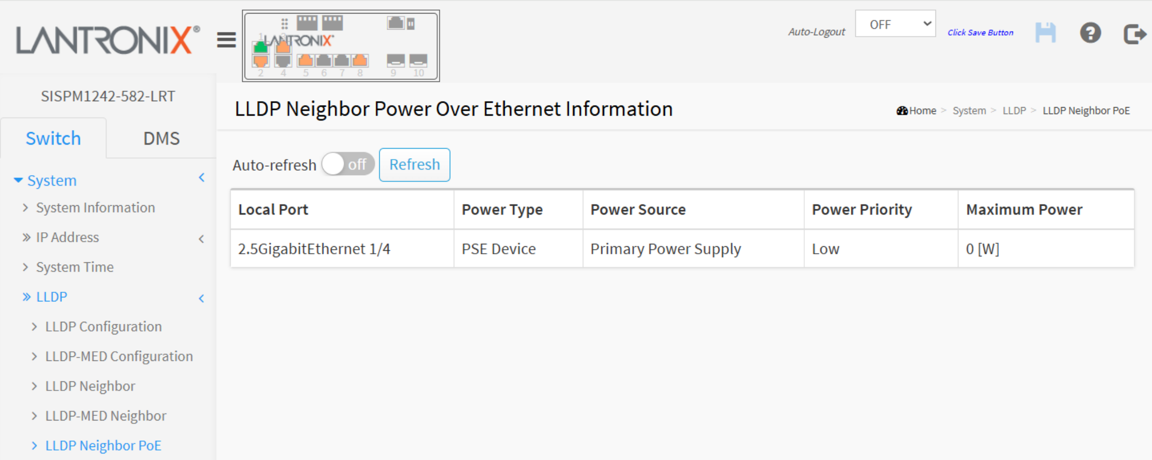
Inventory : A list of interface items.

LLDP Neighbor PoE Information

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 Information:

1. Go to System > LLDP > LLDP Neighbor PoE Information.



LLDP Neighbor Power Over Ethernet Information

Local Port	Power Type	Power Source	Power Priority	Maximum Power
2.5GigabitEthernet 1/4	PSE Device	Primary Power Supply	Low	0 [W]

Parameter Descriptions

Parameter	Description
Local Port	The interface for this switch on which the LLDP frame was received.
Power Type	The Power Type represents whether the device is a Power Sourcing Entity (PSE) or Power Device (PD). If the Power Type is unknown it is represented as "Reserved".
Power Source	The Power Source represents the power source being utilized by a PSE or PD device. If the device is a PSE device it can either run on its Primary Power Source or its Backup Power Source. If it is unknown whether the PSE device is using its Primary Power Source or its Backup Power Source it is indicated as "Unknown" If the device is a PD device it can either run on its local power supply or it can use the PSE as power source. It can also use both its local power supply and the PSE. If it is unknown what power supply the PD device is using it is indicated as "Unknown"
Power Priority	Power 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.

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

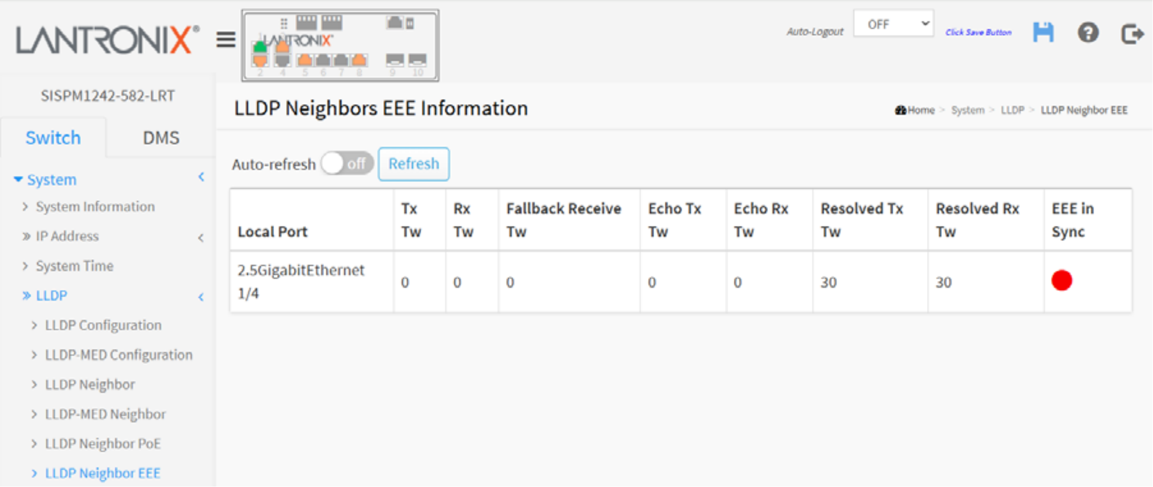
LLDP Neighbor EEE Information

By using EEE (Energy Efficient Ethernet) power savings can be achieved at the expense of traffic latency. This latency occurs because the circuits that EEE turns 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” to agree on the minimum wakeup time they need.

This page displays EEE-related information if it is supported and enabled on the switch and connected devices.

To show LLDP Neighbor EEE information in the web UI:

1. Go to System > LLDP > LLDP Neighbor EEE.



LLDP Neighbors EEE Information

Local Port	Tx Tw	Rx Tw	Fallback Receive Tw	Echo Tx Tw	Echo Rx Tw	Resolved Tx Tw	Resolved Rx Tw	EEE in Sync
2.5GigabitEthernet 1/4	0	0	0	0	0	30	30	●

Parameter descriptions:

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

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

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

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

Echo Tx Tw : The link partner's Echo Tx Tw value. The respective echo values will be defined as the local link partners reflection (echo) of the remote link partners respective values. When a local link partner receives its echoed values from the remote link partner it can determine whether 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.

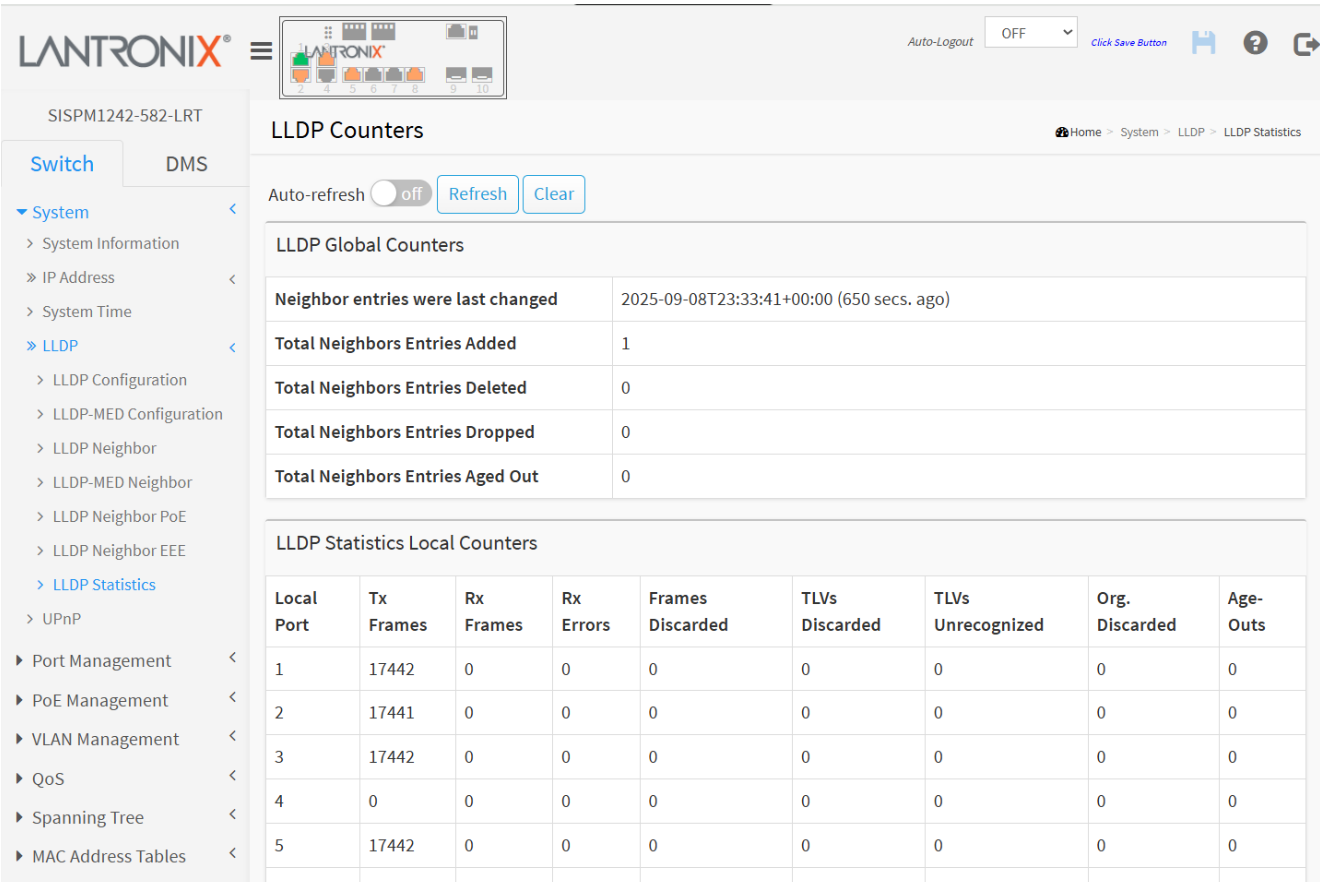
LLDP Statistics

This page provides an overview of all LLDP traffic.

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

To show LLDP Statistics:

1. Go to System > LLDP > LLDP Statistics.
2. **Auto-refresh** will refresh the page every 3 seconds. **Refresh** will refresh the page immediately. **Clear** will clear all statistics.



LLDP Counters

LLDP Global Counters

Neighbor entries were last changed	2025-09-08T23:33:41+00:00 (650 secs. ago)
Total Neighbors Entries Added	1
Total Neighbors Entries Deleted	0
Total Neighbors Entries Dropped	0
Total Neighbors Entries Aged Out	0

LLDP Statistics Local Counters

Local Port	Tx Frames	Rx Frames	Rx Errors	Frames Discarded	TLVs Discarded	TLVs Unrecognized	Org. Discarded	Age-Outs
1	17442	0	0	0	0	0	0	0
2	17441	0	0	0	0	0	0	0
3	17442	0	0	0	0	0	0	0
4	0	0	0	0	0	0	0	0
5	17442	0	0	0	0	0	0	0

Parameter descriptions:

<u>LLDP Global Counters</u>

Neighbor entries were last changed : Shows the time when the last entry was last deleted or added. It also shows the time elapsed since the last change was detected.

Total Neighbors Entries Added : Shows the number of new entries added since switch reboot.

Total Neighbors Entries Deleted : Shows the number of new entries deleted since switch reboot.

Total Neighbors Entries Dropped : Shows the number of LLDP frames dropped due to the entry table being full.

Total Neighbors Entries Aged Out : Shows the number of entries deleted due to Time-To-Live expiring.

<u>LLDP Statistics Local Counters</u> :

Local Port : The port on which LLDP frames are received or transmitted.

Tx Frames : The number of LLDP frames transmitted on the port.

Rx Frames : The number of LLDP frames received on the port.

Rx Errors : The number of received LLDP frames containing some kind of error.

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

TLVs Discarded : Each LLDP frame can contain multiple pieces of information, known as TLVs (Type Length Values). If a TLV is malformed, it is counted and discarded.

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

Org. Discarded : The number of organizationally received TLVs.

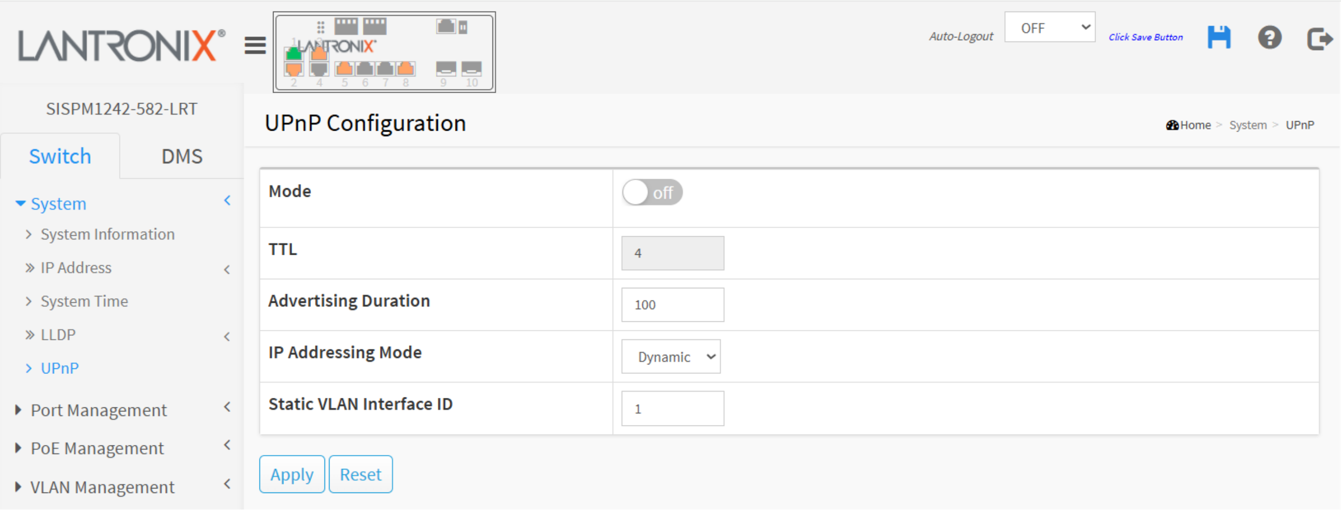
Age-Outs : Each LLDP frame contains information about how long time the LLDP information is valid (age-out time). If no new LLDP frame is received within the age out time, the LLDP information is removed, and the Age-Out counter is incremented.

UPnP

UPnP (Universal Plug and Play) is intended to enable simple robust connectivity to allow devices to discover each other and communicate seamlessly on a network. UPnP has been managed by the Open Connectivity Foundation (OCF) since 2016.

To configure UPnP in the web UI:

1. Go to System > UPnP.
2. Configure the settings.
3. Click **Apply**.



UPnP Configuration

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

Parameter descriptions:

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

- ***on***: Enable UPnP mode operation. When the mode is enabled, two Access Control Entries (ACEs) are added automatically to trap UPnP related packets to CPU.
- ***off***: Disable UPnP mode operation. The ACEs are automatically removed when the mode is disabled.

TTL : Time To Live value used by UPnP to send SSDP advertisement messages. Valid values are 1 - 255.

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

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

- ***Dynamic***: The UPnP module helps users choose the IP address of the switch device. It finds the first available system IP address. This is the default setting for UPnP.
- ***Static***: User specifies the IP interface VLAN for choosing the IP address of the switch device.

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

4. Port Management

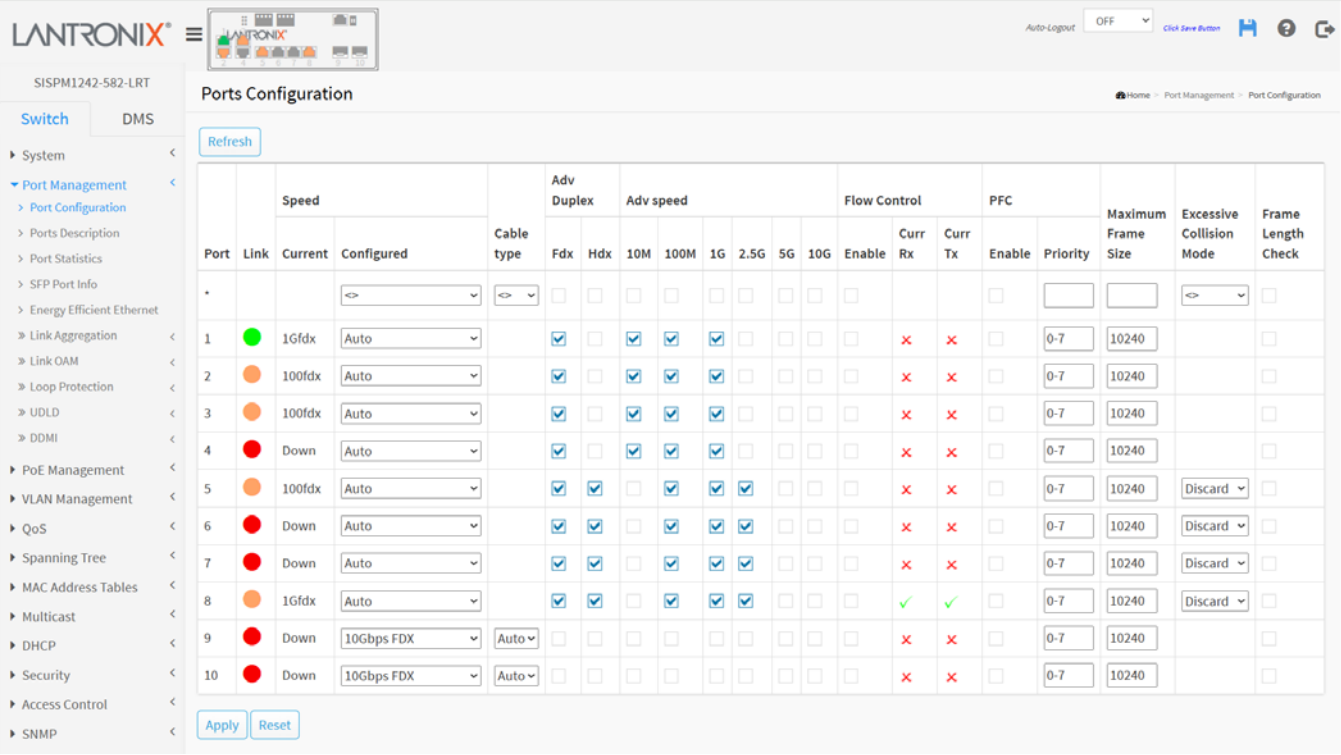
This section lets you view and set Port parameters of the switch. You can use Port management to enable or disable switch ports and monitor ports' content or status.

Port Configuration

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

To configure ports:

1. Go to Port Management > Port Configuration.
2. Configure the desired port settings.
3. Click **Apply**.



Ports Configuration

		Speed			Adv Duplex		Adv speed						Flow Control			PFC				
Port	Link	Current	Configured	Cable type	Fdx	Hdx	10M	100M	1G	2.5G	5G	10G	Enable	Curr Rx	Curr Tx	Enable	Priority	Maximum Frame Size	Excessive Collision Mode	Frame Length Check
*			<>	<>	☐	☐	☐	☐	☐	☐	☐	☐	☐			☐			<>	☐
1	🟢	1Gfdx	Auto		☑	☐	☑	☑	☑	☐	☐	☐	☐	✗	✗	☐	0-7	10240		☐
2	🟠	100fdx	Auto		☑	☐	☑	☑	☑	☐	☐	☐	☐	✗	✗	☐	0-7	10240		☐
3	🟠	100fdx	Auto		☑	☐	☑	☑	☑	☐	☐	☐	☐	✗	✗	☐	0-7	10240		☐
4	🔴	Down	Auto		☑	☐	☑	☑	☑	☐	☐	☐	☐	✗	✗	☐	0-7	10240		☐
5	🟠	100fdx	Auto		☑	☑	☐	☑	☑	☑	☐	☐	☐	✗	✗	☐	0-7	10240	Discard	☐
6	🔴	Down	Auto		☑	☑	☐	☑	☑	☑	☐	☐	☐	✗	✗	☐	0-7	10240	Discard	☐
7	🔴	Down	Auto		☑	☑	☐	☑	☑	☑	☐	☐	☐	✗	✗	☐	0-7	10240	Discard	☐
8	🟠	1Gfdx	Auto		☑	☑	☐	☑	☑	☑	☐	☐	☐	✓	✓	☐	0-7	10240	Discard	☐
9	🔴	Down	10Gbps FDX	Auto	☐	☐	☐	☐	☐	☐	☐	☐	☐	✗	✗	☐	0-7	10240		☐
10	🔴	Down	10Gbps FDX	Auto	☐	☐	☐	☐	☐	☐	☐	☐	☐	✗	✗	☐	0-7	10240		☐

Parameter descriptions:

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

Link : The current link state is displayed graphically. Green indicates the 1Gbps link is up and red that it is down. Amber represents a 10Mbps or 100 Mbps link is up.

Current Link Speed: Provides the current link speed of the port.

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

- ***Disabled*** - Disables the switch port operation.
- ***Auto*** - Port auto negotiates speed with the link partner and selects the highest speed that is compatible with the link partner.

- ***10Mbps FDX*** - Forces the port in 10Mbps full duplex mode.
- ***100Mbps FDX*** - Forces the port in 100Mbps full duplex mode.
- ***1Gbps FDX*** – (SFP+ ports only). Forces the port in 1Gbps full duplex
- ***10Gbps FDX*** - (SFP+ ports only).Forces the port in 10Gbps full duplex mode.

Cable type : (SFP+ ports 9, 10 only) At the dropdown select the 10G cable type setting. The default is Auto.

- ***Auto***: SFP interface in "auto" mode. Automatic SerDes tuning for optical and DAC-3m cables (default).
- ***DAC-1m***: SFP interface in "DAC-1m" mode. Manual SerDes tuning specifically for DAC-1m cables.
- ***DAC-2m***: SFP interface in "DAC-2m" mode. Manual SerDes tuning specifically for DAC-2m cables.
- ***DAC-3m***: SFP interface in "DAC-3m" mode. Manual SerDes tuning specifically for DAC-3m cables.
- ***DAC-5m***: SFP interface in "DAC-5m" mode. Manual SerDes tuning specifically for DAC-5m cables.

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

Advertise Speed: When Speed is set as Auto (auto negotiation), the port will only advertise the specified speeds (10M, 100M, 1G, 2.5G) to the link partner. By default, ports will advertise all the supported speeds if speed is set as Auto.

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

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

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

Excessive Collision Check:

Configure port transmit collision behavior.

- **Discard**: Discard frame after 16 collisions (default).
- **Restart**: Restart backoff algorithm after 16 collisions.

Frame Length Check : Configures if frames with incorrect frame length in the EtherType/Length field will be dropped. An Ethernet frame contains a field EtherType which can be used to indicate the frame payload size (in bytes) for values of 1535 and below. If the EtherType/Length field is above 1535, it indicates that the field is used as an EtherType (indicating which protocol is encapsulated in the payload of the frame). If Frame Length Check is enabled, frames with payload size less than 1536 bytes are dropped, if the EtherType/Length field doesn't match the actual payload length.

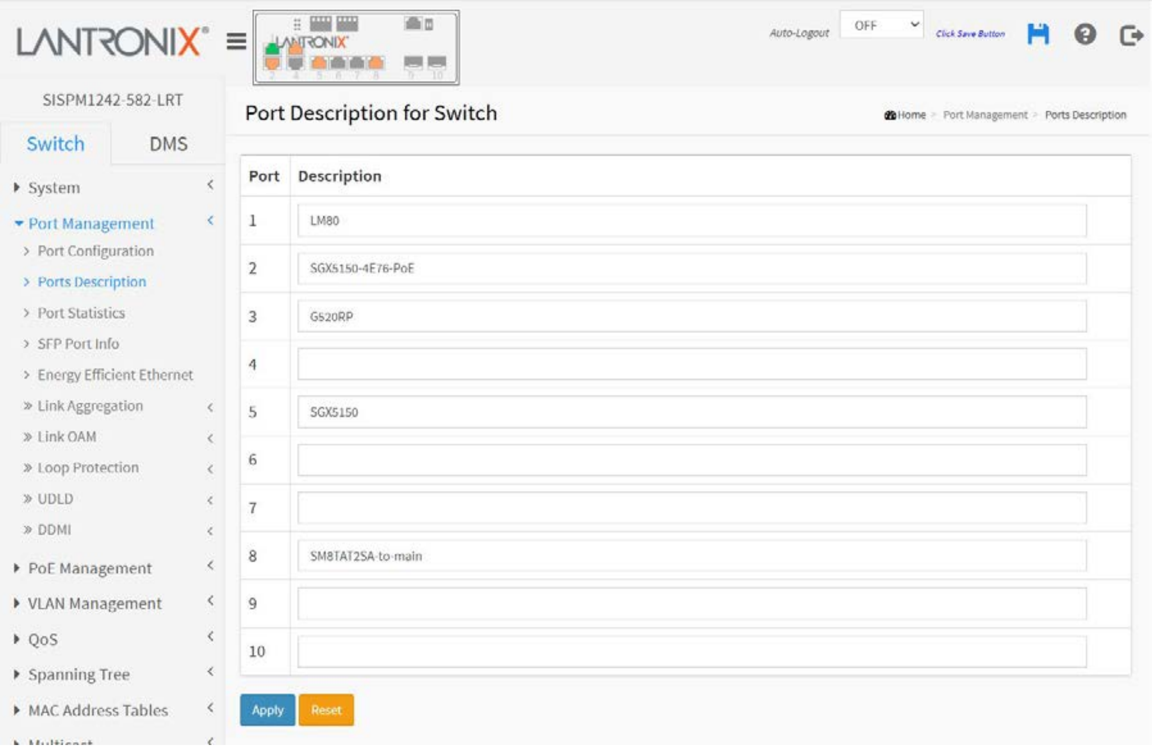
If Frame Length Check is disabled, frames are not dropped due to frame length mismatch. **Note**: No drop counters count frames are dropped due to frame length mismatch.

Port Description

This page lets you view and configure port descriptions.

To configure the port descriptions:

1. Go to Port Management > Port Description.
2. Enter the description for the selected port.
3. Click **Apply**.



Auto-Logout OFF

Port Description for Switch

Port	Description
1	LM80
2	SGX5150-4E76-PoE
3	G520RP
4	
5	SGX5150
6	
7	
8	SM8TAT2SA-to-main
9	
10	

Port: The logical port number for the row.

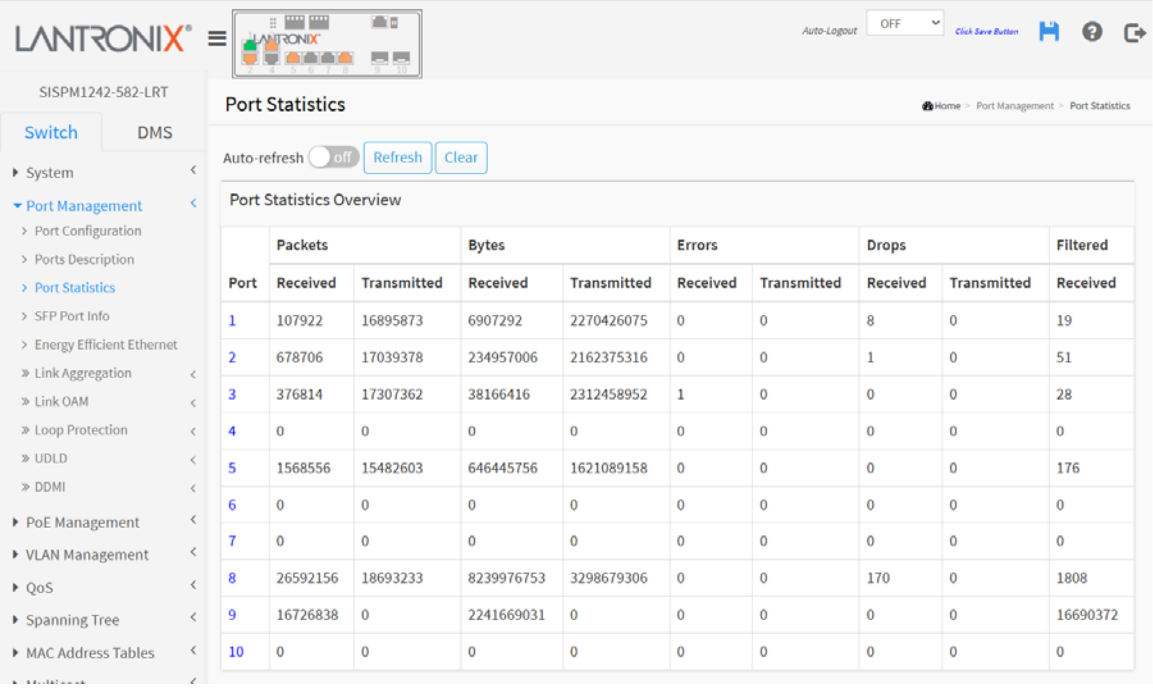
Description: Descriptive name that identifies this port. Enter up to 128 characters.

Port Statistics

Port statistics provides information and general traffic statistics for all switch ports. The displayed counters are the total packets and bytes for receive and transmit, the size counters for receive and transmit, and the error counters for receive and transmit.

To display Port Statistics:

1. Go to Port Management > Port Statistics.
2. To view detailed port statistics, click the port number under the Port column.
3. **Auto-refresh** will refresh the page every 3 seconds. **Refresh** will refresh the page immediately. **Clear** will clear all statistics.



Port Statistics

Port Statistics Overview

	Packets		Bytes		Errors		Drops		Filtered
Port	Received	Transmitted	Received	Transmitted	Received	Transmitted	Received	Transmitted	Received
1	107922	16895873	6907292	2270426075	0	0	8	0	19
2	678706	17039378	234957006	2162375316	0	0	1	0	51
3	376814	17307362	38166416	2312458952	1	0	0	0	28
4	0	0	0	0	0	0	0	0	0
5	1568556	15482603	646445756	1621089158	0	0	0	0	176
6	0	0	0	0	0	0	0	0	0
7	0	0	0	0	0	0	0	0	0
8	26592156	18693233	8239976753	3298679306	0	0	170	0	1808
9	16726838	0	2241669031	0	0	0	0	0	16690372
10	0	0	0	0	0	0	0	0	0

Parameter descriptions:

Port : The logical port for the settings contained in the same row. Click the linked Port number to display details of that port's statistics.

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.

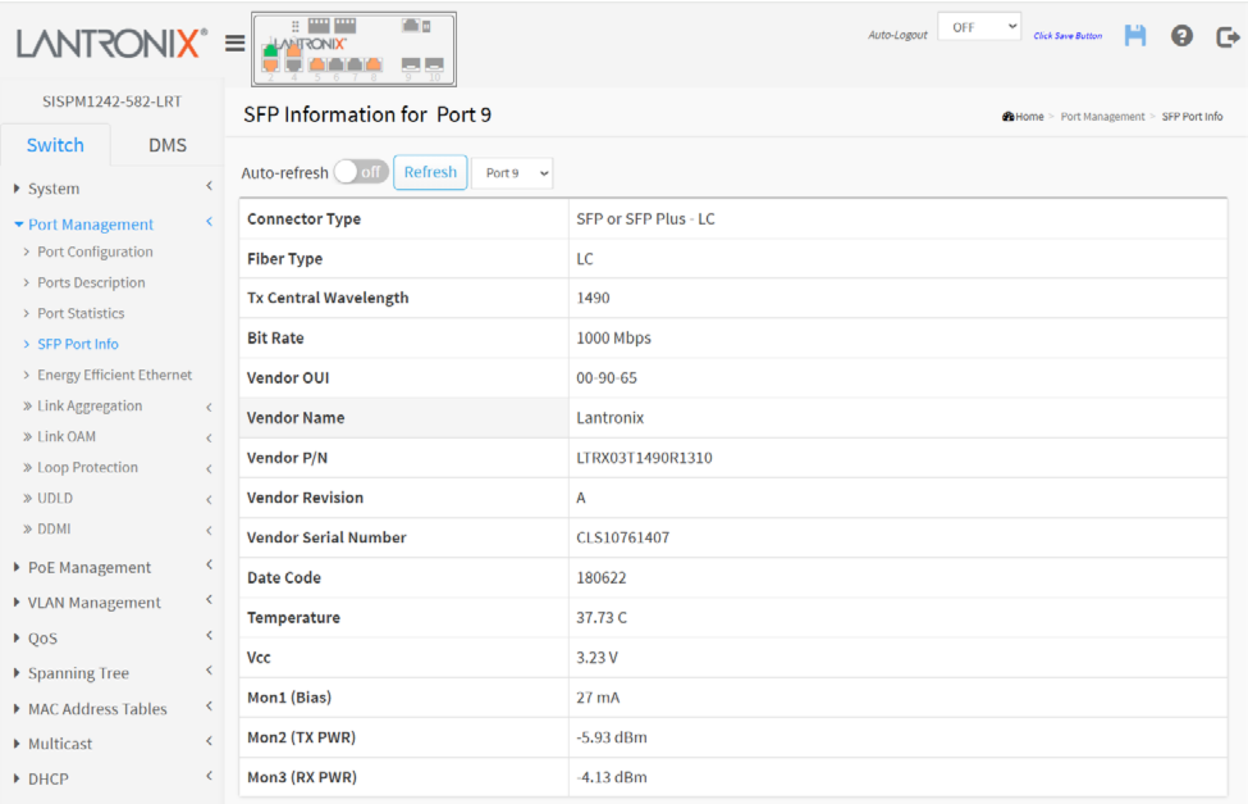
Filtered: The number of received frames filtered by the forwarding process.

SFP Port Info

This page displays SFP module detail information for SFP modules connected to the switch.

To view SFP information in the web UI:

1. Go to Port Management > SFP Port Info.
2. Select the Port number from the Port selector.
3. **Auto-refresh** will refresh the page every 3 seconds. **Refresh** will refresh the page immediately.



SFP Information for Port 9

Connector Type	SFP or SFP Plus - LC
Fiber Type	LC
Tx Central Wavelength	1490
Bit Rate	1000 Mbps
Vendor OUI	00-90-65
Vendor Name	Lantronix
Vendor P/N	LTRX03T1490R1310
Vendor Revision	A
Vendor Serial Number	CLS10761407
Date Code	180622
Temperature	37.73 C
Vcc	3.23 V
Mon1 (Bias)	27 mA
Mon2 (TX PWR)	-5.93 dBm
Mon3 (RX PWR)	-4.13 dBm

Parameter descriptions:

Port selector: Select the port number from the list.

Connector Type: Displays the external optical or electrical cable connector provided as the media interface.

Fiber Type: Displays the fiber transmission media.

Tx Central Wavelength: Displays the nominal transmitter output wavelength in nm (e.g., 850nm, 1310nm).

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

Vendor OUI: Displays the vendor's IEEE-assigned company ID.

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

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

Vendor Revision : Displays the module revision.

Vendor Serial Number : Shows the serial number assigned by the manufacturer.

Date Code : Shows the date this SFP module was made.

Temperature : Shows the current temperature of SFP module.

Vcc : Show the working DC voltage of SFP module.

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

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

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

Energy Efficient Ethernet (EEE)

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

EEE works by powering down circuits when there is no traffic. When a port gets data to be transmitted all circuits are powered up. The time it takes to power up the circuits is the wakeup time. The default wakeup time is 17 us for 1Gbit links and 30 us for other link speeds. EEE devices must agree upon the value of the wakeup time 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.

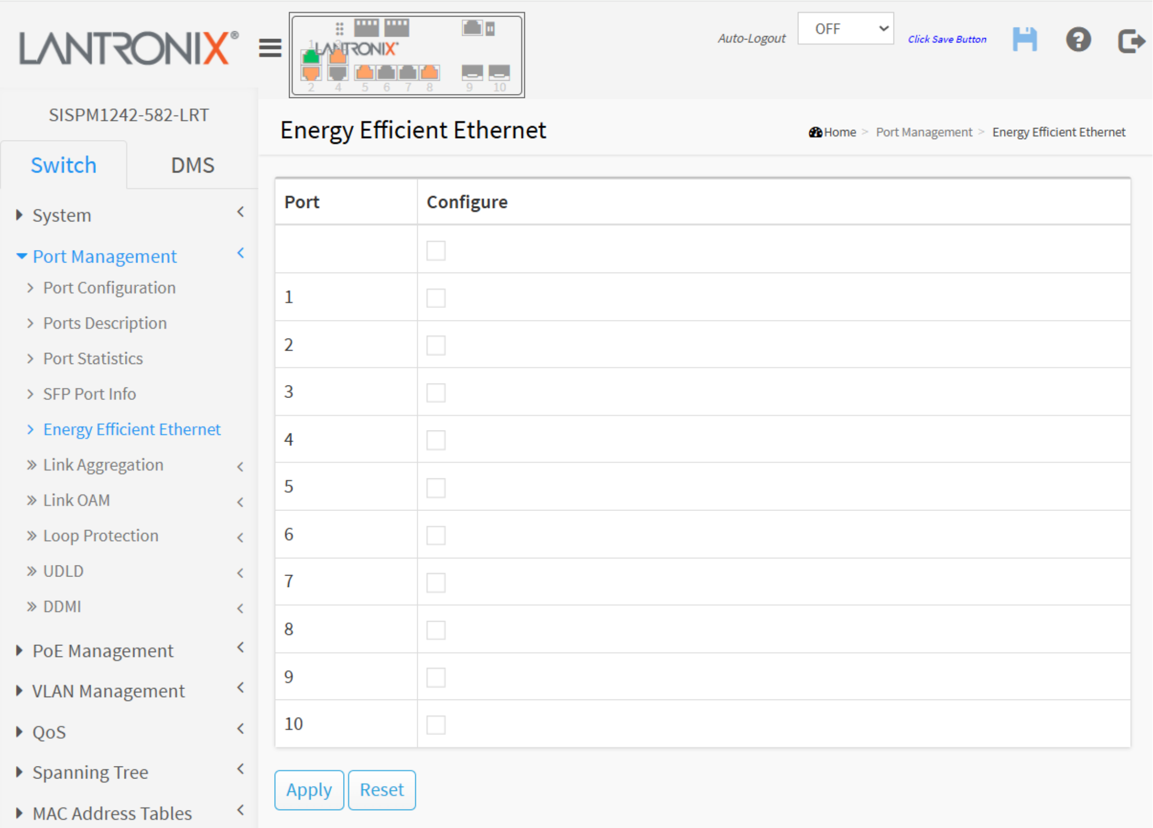
EEE works for ports in auto-negotiation mode, where the port is negotiated to either 1Gbps or 100 Mbit full duplex mode.

For ports that are not EEE-capable the corresponding EEE checkboxes are grayed out and thus impossible to enable EEE for.

When a port is powered down for saving power, outgoing traffic is stored in a buffer until the port is powered up again. Because there are some overhead in turning the port down and up, more power can be saved if the traffic can be buffered up until a large burst of traffic can be transmitted. Buffering traffic will give some latency in the traffic.

To configure Energy Efficient Ethernet in the web UI:

1. Go to Port Management > Energy Efficient Ethernet.
2. Select enable or disable Energy Efficient Ethernet per port.
3. Click **Apply**.



Energy Efficient Ethernet

Port	Configure
	□
1	□
2	□
3	□
4	□
5	□
6	□
7	□
8	□
9	□
10	□

Parameter descriptions:

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

Configure : Controls whether EEE is enabled for this switch port. Check the box to enable EEE per port. The default is disabled (checkbox unchecked).

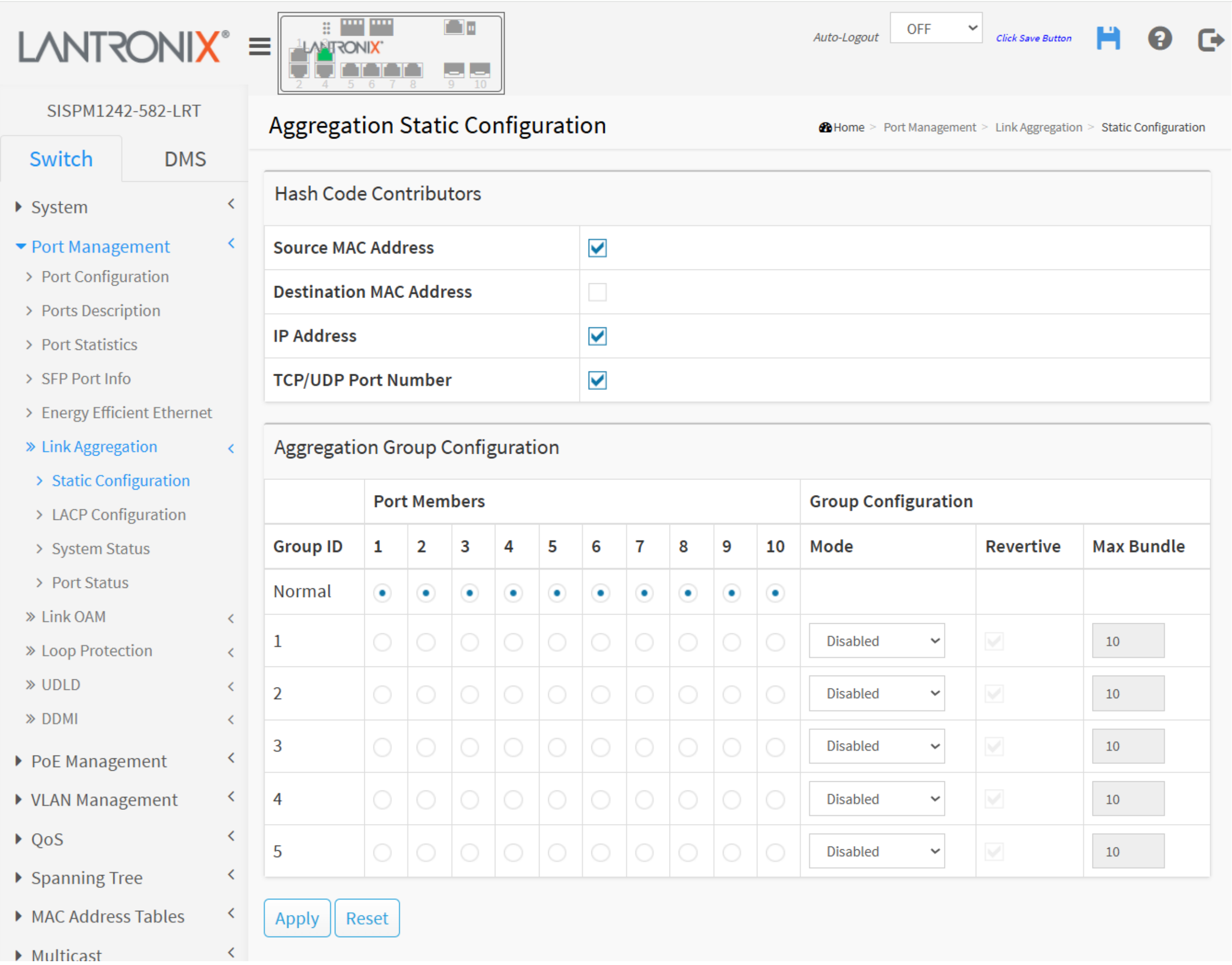
Link Aggregation

Static Configuration

Aggregation refers to the practice of using multiple ports in parallel to increase the link speed and increase the redundancy for higher availability. This page lets you configure the Aggregation hash mode and aggregation groups.

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

1. Go to Port Management > Link Aggregation > Static Configuration.
2. Set the Hash Code Contributors parameters.
3. Set the Aggregation Group configuration parameters.
4. Click **Apply** to save the settings.



Aggregation Static Configuration

Hash Code Contributors

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

Aggregation Group Configuration

	Port Members										Group Configuration		
Group ID	1	2	3	4	5	6	7	8	9	10	Mode	Revertive	Max Bundle
Normal	●	●	●	●	●	●	●	●	●	●			
1	○	○	○	○	○	○	○	○	○	○	Disabled	☑	10
2	○	○	○	○	○	○	○	○	○	○	Disabled	☑	10
3	○	○	○	○	○	○	○	○	○	○	Disabled	☑	10
4	○	○	○	○	○	○	○	○	○	○	Disabled	☑	10
5	○	○	○	○	○	○	○	○	○	○	Disabled	☑	10

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 at the same speed in each group.

Group Configuration

Mode: At the dropdown select the mode for the aggregation group. The default is Disabled. The selections are:

- ***Disabled***: The group is disabled (default).
- ***Static***: The group operates in static aggregation mode.
- ***LACP (Active)***: The group operates in LACP active aggregation mode. See IEEE 801.AX-2014, section 6.4.1 for details.
- ***LACP (Passive)***: The group operates in LACP passive aggregation mode. See IEEE 801.AX-2014, section 6.4.1 for details.

Revertive: For each Group, check the checkbox to enable revertive operation. The default is unchecked (non-revertive).

Max Bundle: This parameter only applies to LACP-enabled groups. It determines the maximum number of active bundled LACP ports allowed in an aggregation.

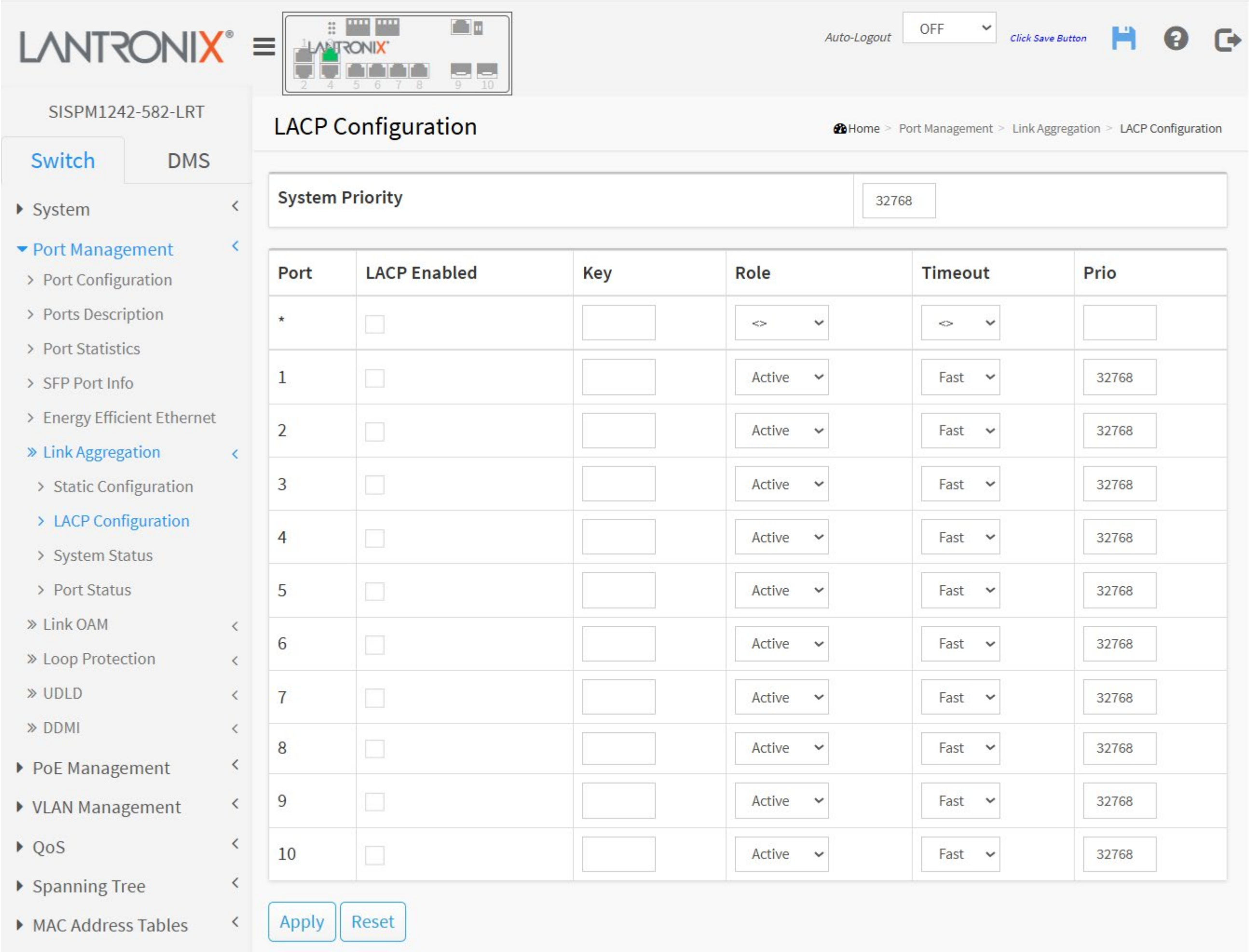
LACP Configuration

LACP is part of the IEEE 802.3ad specification, which allows using multiple ports in parallel to form a single logical channel.

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

To configure LACP Port parameters in the web UI:

1. Go to Port Management > Link Aggregation > LACP Configuration.
2. Enable or disable the LACP on the port of the switch.
3. Select the Key parameter of Auto or Specific. The default is Auto.
4. Select the Role of Active or Passive. The default is Active.
5. Click **Apply** to save the settings.



LACP Configuration

System Priority	32768

Port	LACP Enabled	Key	Role	Timeout	Prio
*	□		<>	<>	
1	□		Active	Fast	32768
2	□		Active	Fast	32768
3	□		Active	Fast	32768
4	□		Active	Fast	32768
5	□		Active	Fast	32768
6	□		Active	Fast	32768
7	□		Active	Fast	32768
8	□		Active	Fast	32768
9	□		Active	Fast	32768
10	□		Active	Fast	32768

Parameter descriptions:

System Priority: A LACP system priority is configured on each device running LACP. The system priority can be configured through the user interface. For priority setting, the range is 1 to 65535. The default is 32768. The lower the value, the higher the system priority.

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. Up to 10 aggregations are supported (if stackable).

Key : The Key value incurred by the port, range 1-5.

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

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

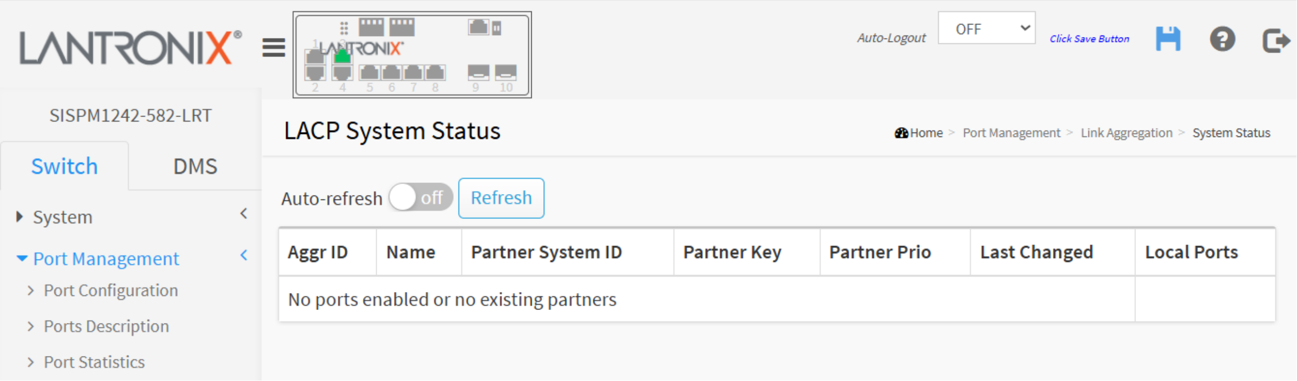
Prio : Controls the priority of the port, range 1-65537. If the LACP partner wants to form a larger group than is supported by this device, then this parameter will control which ports will be active and which ports will be in a backup role. Lower Prio number means higher priority. The default priority is 32768.

LACP System Status

This page provides system status for all LACP instances.

To display the LACP System status in the web UI:

1. Go to Port Management > Link Aggregation > System Status.
2. **Auto-refresh** will refresh the page every 3 seconds. **Refresh** will refresh the page immediately.



LACP System Status

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

Parameter descriptions:

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

Name : Displays the name of the Aggregation group 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.

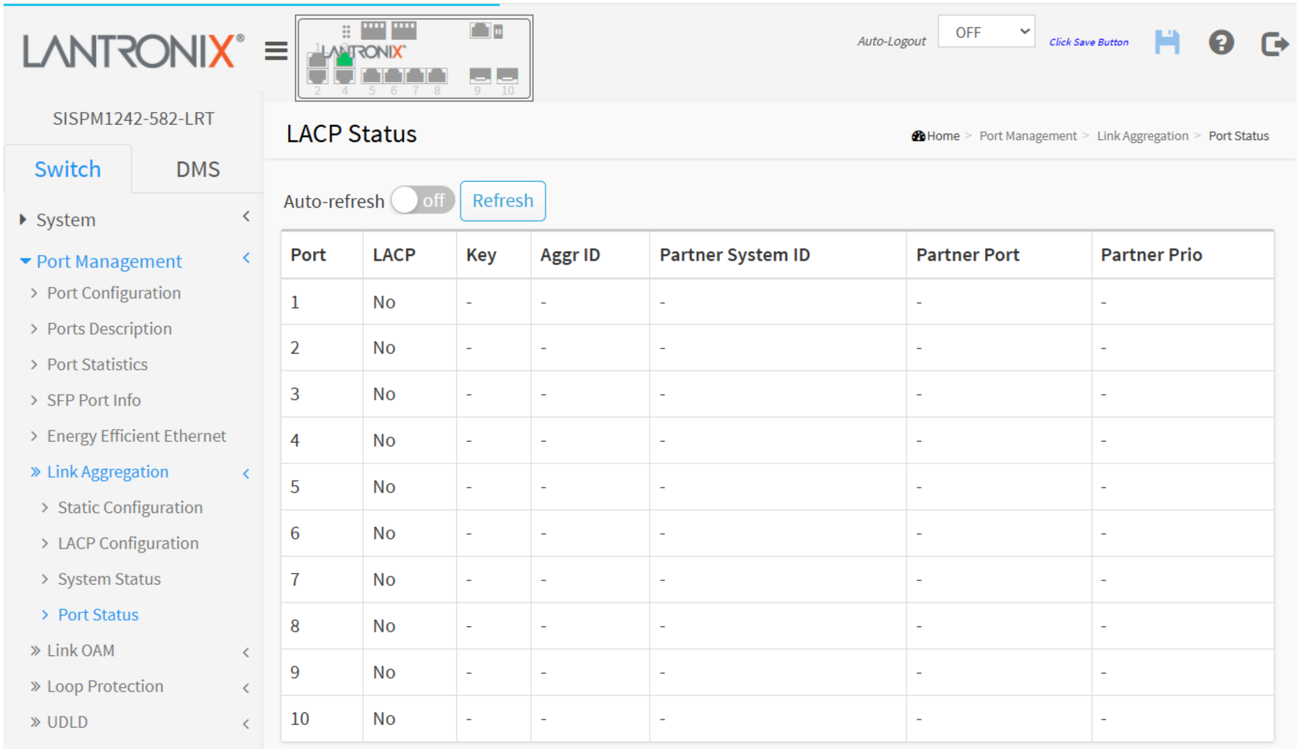
Local Ports : Shows which ports are a part of this aggregation for this switch. The format is "Switch ID:Port".

LACP Port Status

This page provides a status overview for LACP status for all ports.

To display the LACP Port status in the web UI:

1. Go to Port Management > Link Aggregation > Port Status.
2. **Auto-refresh** will refresh the page every 3 seconds. **Refresh** will refresh the page immediately.



LACP Status

Port	LACP	Key	Aggr ID	Partner System ID	Partner Port	Partner Prio
1	No	-	-	-	-	-
2	No	-	-	-	-	-
3	No	-	-	-	-	-
4	No	-	-	-	-	-
5	No	-	-	-	-	-
6	No	-	-	-	-	-
7	No	-	-	-	-	-
8	No	-	-	-	-	-
9	No	-	-	-	-	-
10	No	-	-	-	-	-

Parameter descriptions:

Port : The switch port number.

LACP :

- ***Yes***: LACP is enabled, and the port link is up.
- ***No***: LACP is not enabled or that the port link is down.
- ***Backup***: 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.

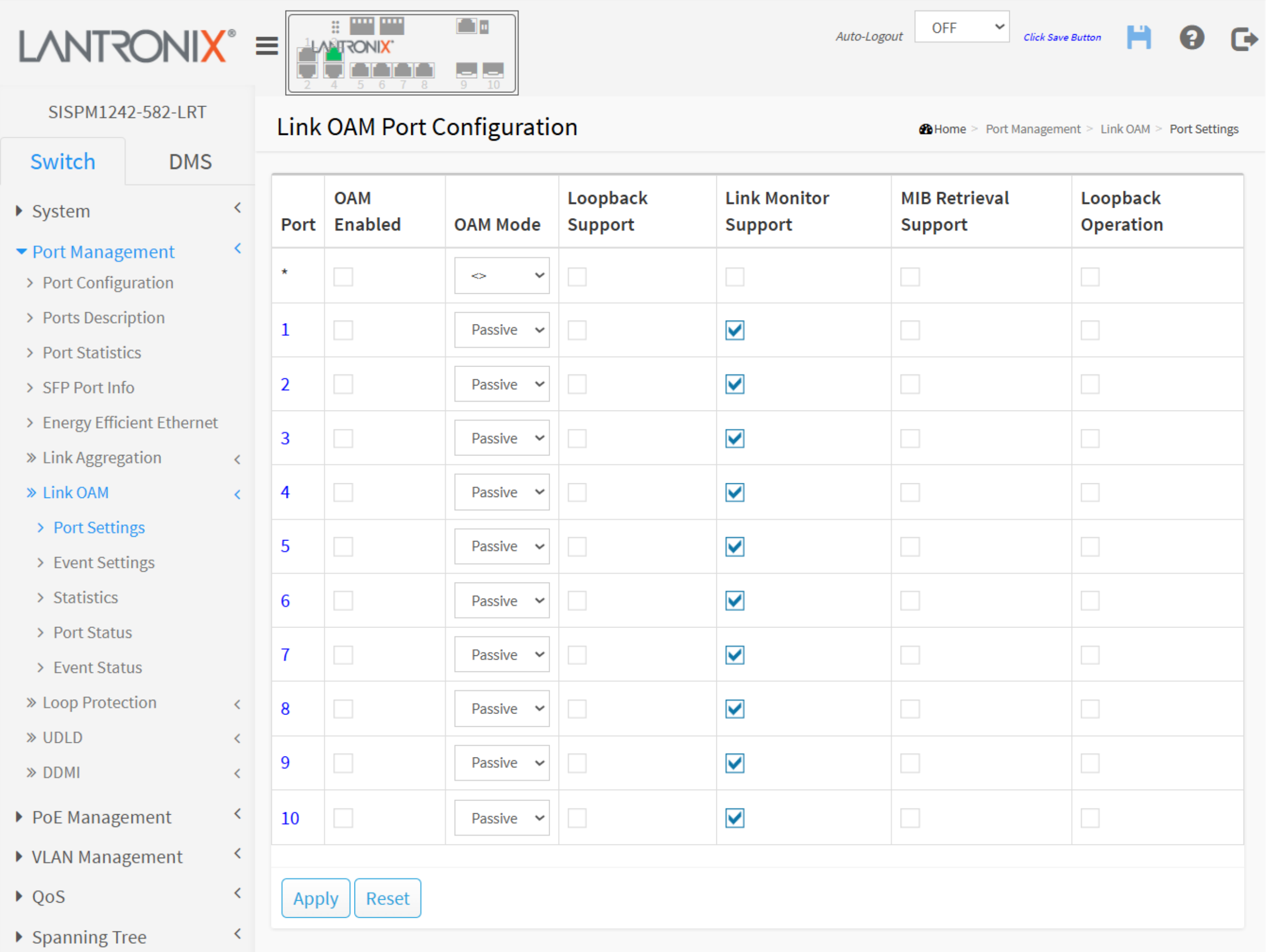
Link OAM

Link OAM is concerned with features for monitoring and troubleshooting the physical link between two devices.

Port Settings

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

Go to Port Management > Link OAM > Port Settings.



Link OAM Port Configuration

Port	OAM Enabled	OAM Mode	Loopback Support	Link Monitor Support	MIB Retrieval Support	Loopback Operation
*	□	<>	□	□	□	□
1	□	Passive	□	☑	□	□
2	□	Passive	□	☑	□	□
3	□	Passive	□	☑	□	□
4	□	Passive	□	☑	□	□
5	□	Passive	□	☑	□	□
6	□	Passive	□	☑	□	□
7	□	Passive	□	☑	□	□
8	□	Passive	□	☑	□	□
9	□	Passive	□	☑	□	□
10	□	Passive	□	☑	□	□

Apply Reset

Parameter descriptions:

Port: The switch port number. Clicking the port number displays a page with detailed status for that port.

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

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

- ***Active***: DTEs configured in Active mode initiate the exchange of Information OAMPDUs as defined by the Discovery process. Once the Discovery process completes, Active DTE's are permitted to send any OAMPDU while connected to a remote OAM peer entity in Active mode. Active DTE's operate in a limited respect if the remote OAM entity is operating in Passive mode. Active devices should not respond to OAM remote loopback commands and variable requests from a Passive peer.

- ***Passive*** : DTEs configured in Passive mode do not initiate the Discovery process. Passive DTEs react to the initiation of the Discovery process by the remote DTE. This eliminates the possibility of passive to passive links. Passive DTEs will not send Variable Request or Loopback Control OAMPDUs.

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

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

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

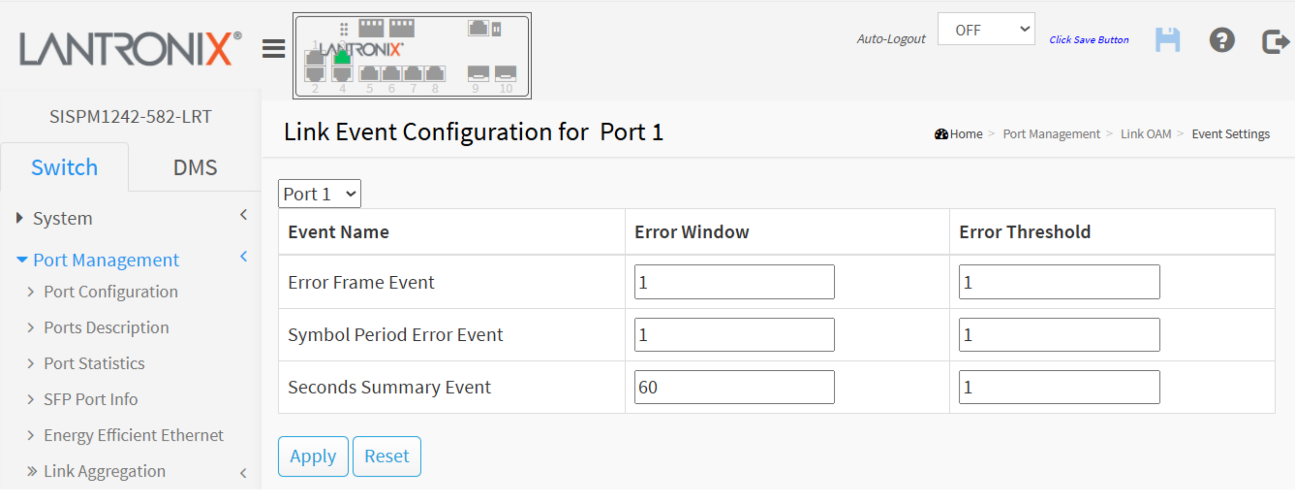
Loopback Operation : If the Loopback support is enabled, enabling this field will start a loopback operation for the port.

Event Settings

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

To do so:

1. Go to Port Management > Link OAM > Event Settings.
2. At the port select dropdown select the desired switch port.
3. For each Event Name, enter an Error Window value and an Error Threshold value.
4. Click the **Apply** button.



Link Event Configuration for Port 1

Port 1

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

Parameter Descriptions

Port : The switch port number.

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

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

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

Events

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

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

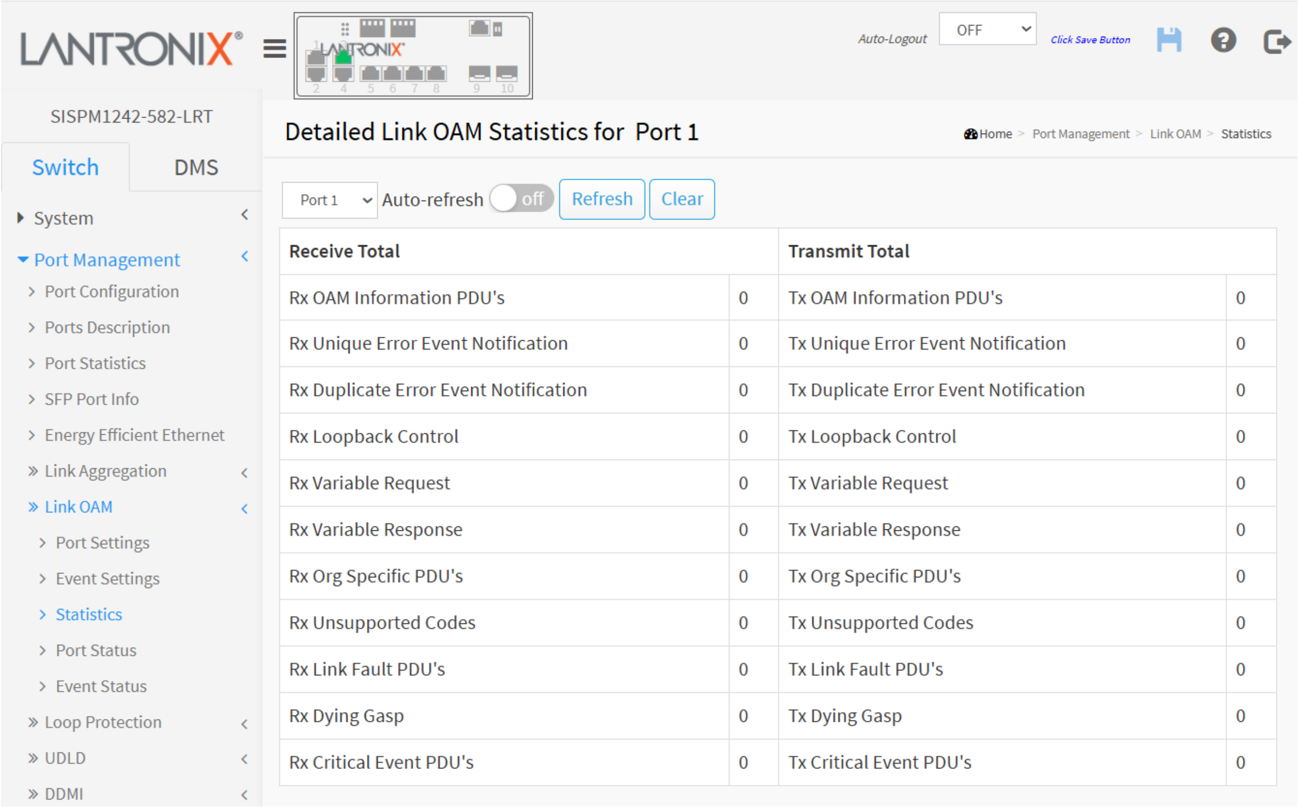
Seconds Summary Event : The Errored Frame Seconds Summary Event TLV counts the number of errored frame seconds that occurred during the specified period. The period is specified by a time interval. This event is generated if the number of errored frame seconds is equal to or greater than the specified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

Statistics

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

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

1. Go to Port Management > Link OAM > Statistics.
2. **Auto-refresh** will refresh the page every 3 seconds. **Refresh** will refresh the page immediately. **Clear** will clear all statistics.



Detailed Link OAM Statistics for Port 1

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

Parameter descriptions :

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

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

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

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

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

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

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

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

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

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

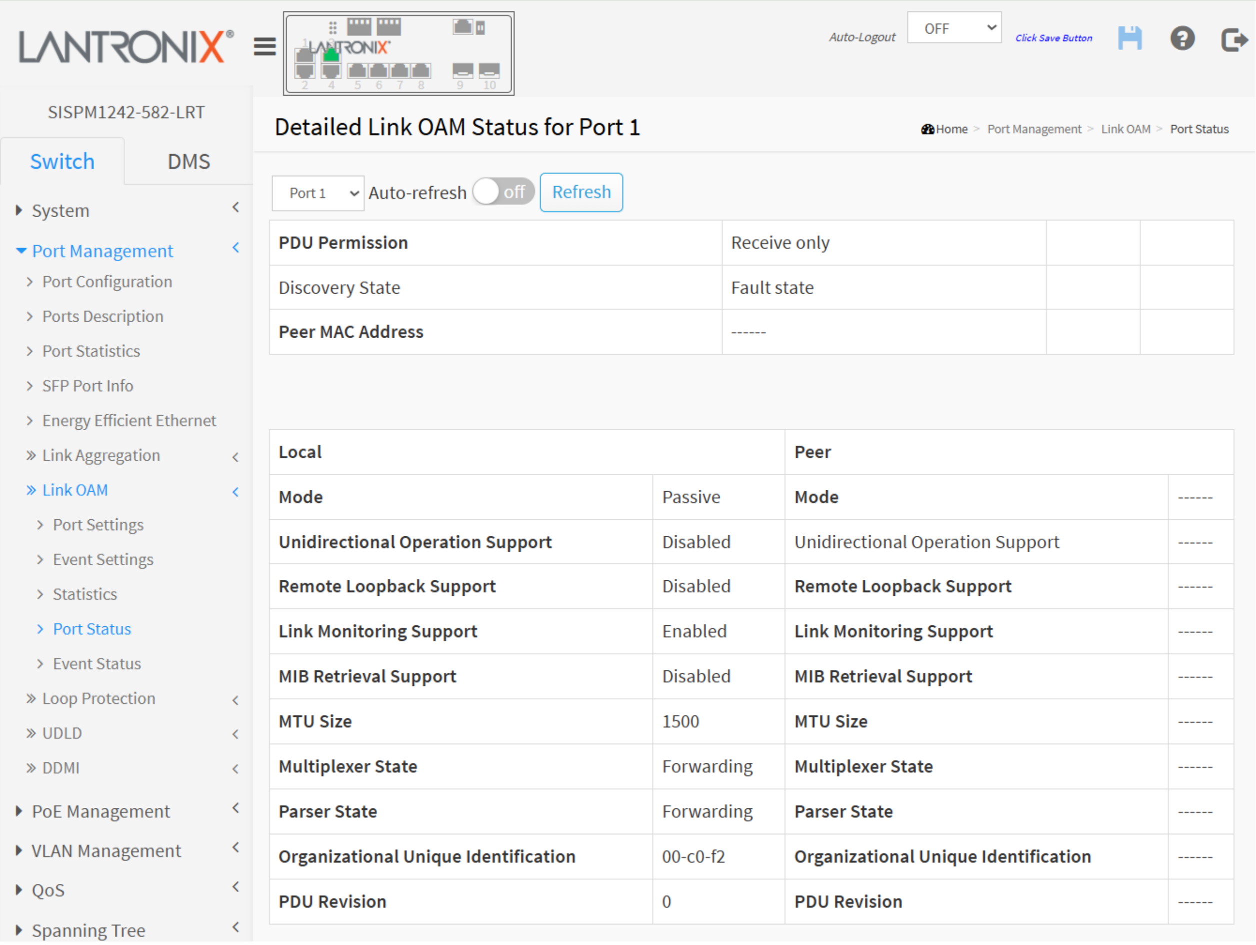
Rx and Tx Critical Event PDUs : A count of the number of Critical event PDUs received and transmitted on this interface.

Port Status

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

To view Link OAM port status:

1. Go to Port Management > Link OAM > Port Status.
2. Select the port number.
3. **Auto-refresh** will refresh the page every 3 seconds. **Refresh** will refresh the page immediately.



Detailed Link OAM Status for Port 1

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

Local		**Peer**	
Mode	Passive	**Mode**	------
Unidirectional Operation Support	Disabled	Unidirectional Operation Support	------
Remote Loopback Support	Disabled	**Remote Loopback Support**	------
Link Monitoring Support	Enabled	**Link Monitoring Support**	------
MIB Retrieval Support	Disabled	**MIB Retrieval Support**	------
MTU Size	1500	**MTU Size**	------
Multiplexer State	Forwarding	**Multiplexer State**	------
Parser State	Forwarding	**Parser State**	------
Organizational Unique Identification	00-c0-f2	**Organizational Unique Identification**	------
PDU Revision	0	**PDU Revision**	------

Parameter descriptions :

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

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

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

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

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

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

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

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

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

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

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

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

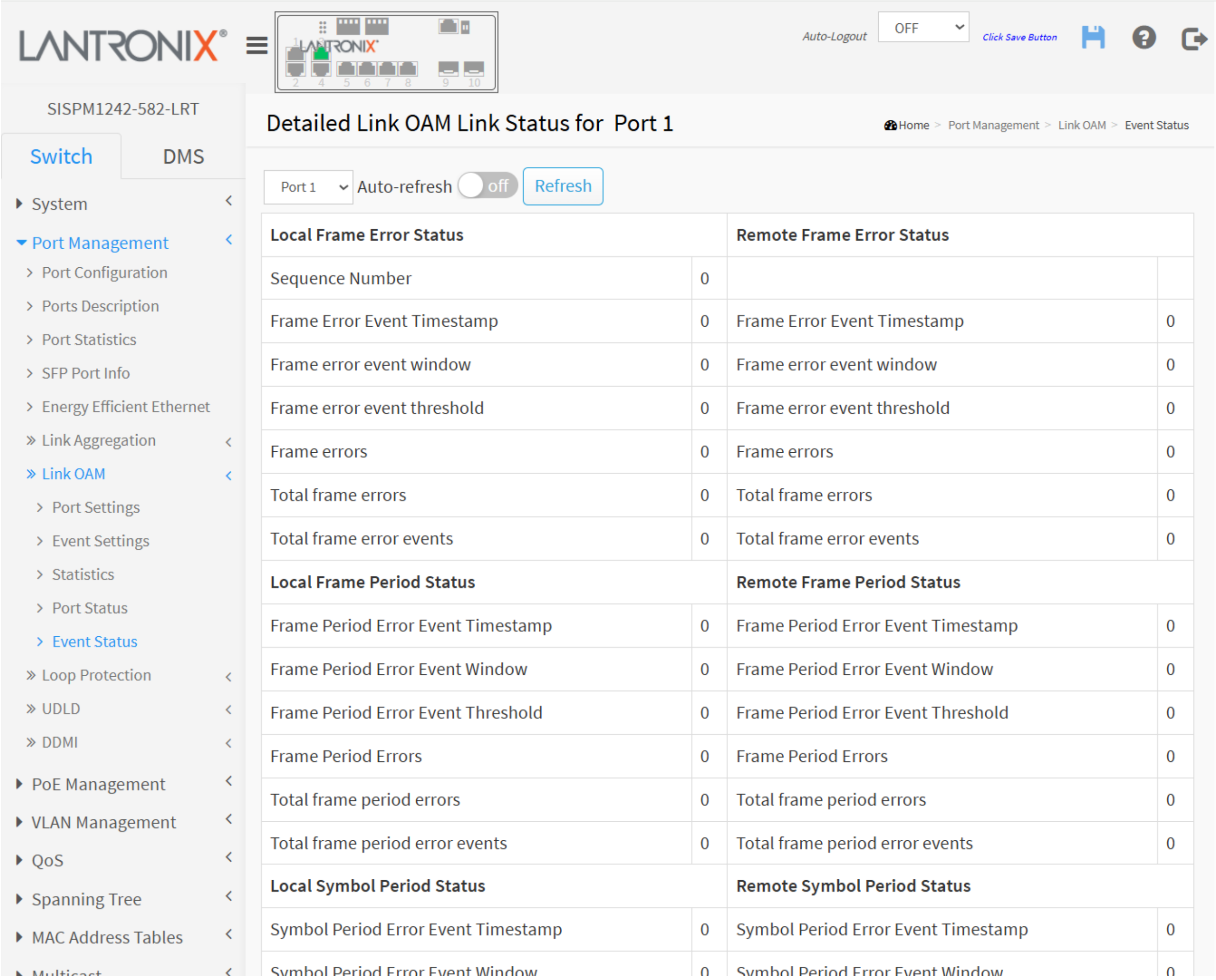
PDU Revision : It indicates the current revision of the Information TLV. The value of this field will start at zero and be incremented each time something in the Information TLV changes. Upon reception of an Information TLV from a peer, an OAM client may use this field to decide if it needs to be processed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

Event Status

This page lets you view the Link OAM Link Event configurations. The left pane displays the Event status for the Local OAM unit while the right pane displays the status for the Peer for the respective port.

To view port link OAM status:

1. Go to Port Management > Link OAM > Event Status.
2. In the port selector list, select the desired port number.
3. **Auto-refresh** will refresh the page every 3 seconds. **Refresh** will refresh the page immediately.



Detailed Link OAM Link Status for Port 1

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

Parameter descriptions :

Port selection box: At the dropdown select the desired switch port number.

Frame Error Status

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

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

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

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

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

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

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

Frame Period Status

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

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

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

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

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

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

Symbol Period Status

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

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

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

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

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

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

Event Seconds Summary Status

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

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

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

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

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

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

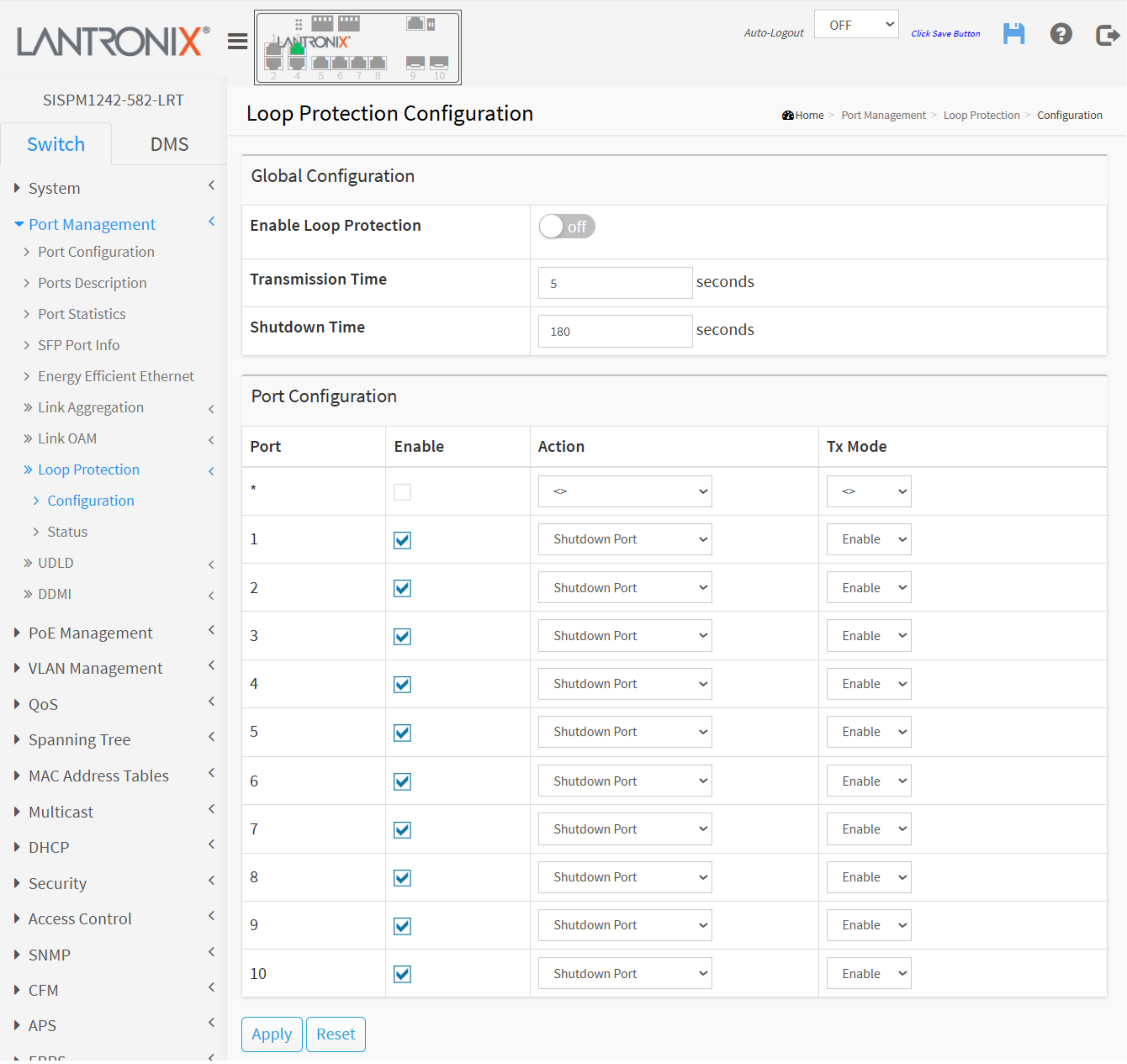
Loop Protection

Configuration

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

To configure Loop Protection parameters in the web UI:

1. Go to Port Management > Loop Protection > Configuration.
2. Select to enable or disable Loop Protection globally.
3. Set the Global and Port Configuration parameters.
4. Click the **Apply** button to save the settings.



Loop Protection Configuration

Global Configuration

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

Port Configuration

Port	Enable	Action	Tx Mode
*	□	<>	<>
1	☑	Shutdown Port	Enable
2	☑	Shutdown Port	Enable
3	☑	Shutdown Port	Enable
4	☑	Shutdown Port	Enable
5	☑	Shutdown Port	Enable
6	☑	Shutdown Port	Enable
7	☑	Shutdown Port	Enable
8	☑	Shutdown Port	Enable
9	☑	Shutdown Port	Enable
10	☑	Shutdown Port	Enable

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. The default is 5 seconds.

Shutdown Time : The period (in seconds) for which a port will be kept disabled in the event a loop is detected (and the port action shuts down the port). Valid values are 10 to 604800 seconds (7 days). A value of zero (0) will keep a port disabled until the next device restart. The default is 180 seconds.

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*.

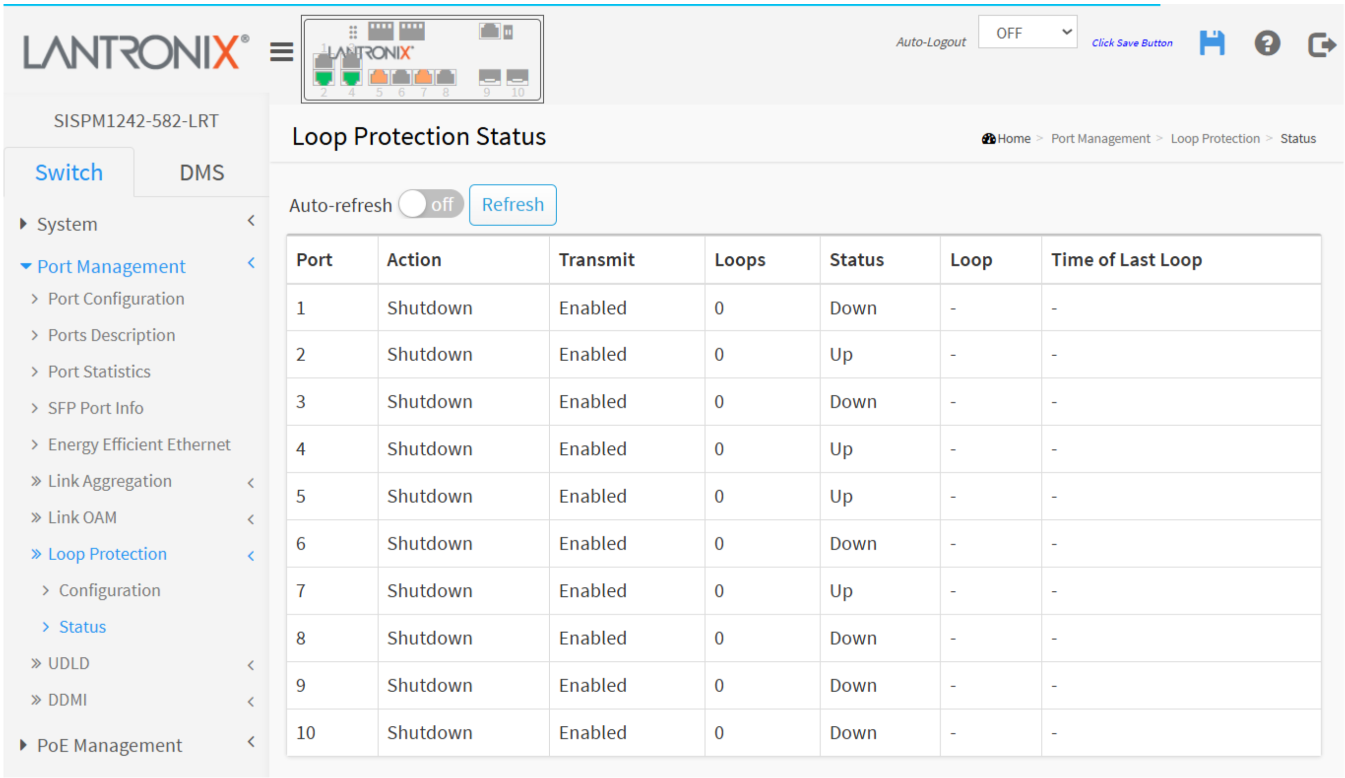
Tx Mode : Controls whether the port is actively generating loop protection PDUs, or whether it is just passively looking for looped PDUs.

Status

This page displays loop protection port status of switch ports.

To display Loop Protection status in the web UI:

1. Go to Port Management > Loop Protection > Status.
2. **Auto-refresh** will refresh the page every 3 seconds. **Refresh** will refresh the page immediately.



Loop Protection Status

Port	Action	Transmit	Loops	Status	Loop	Time of Last Loop
1	Shutdown	Enabled	0	Down	-	-
2	Shutdown	Enabled	0	Up	-	-
3	Shutdown	Enabled	0	Down	-	-
4	Shutdown	Enabled	0	Up	-	-
5	Shutdown	Enabled	0	Up	-	-
6	Shutdown	Enabled	0	Down	-	-
7	Shutdown	Enabled	0	Up	-	-
8	Shutdown	Enabled	0	Down	-	-
9	Shutdown	Enabled	0	Down	-	-
10	Shutdown	Enabled	0	Down	-	-

Parameter descriptions :

Port : The switch port number of the logical port.

Action : The currently configured port action.

Transmit : The currently configured port transmit mode.

Loops : The number of loops detected on this port.

Status : The current loop protection status of the port.

Loop : Whether a loop is currently detected on the port.

Time of Last Loop : The time of the last loop event detected.

UDLD

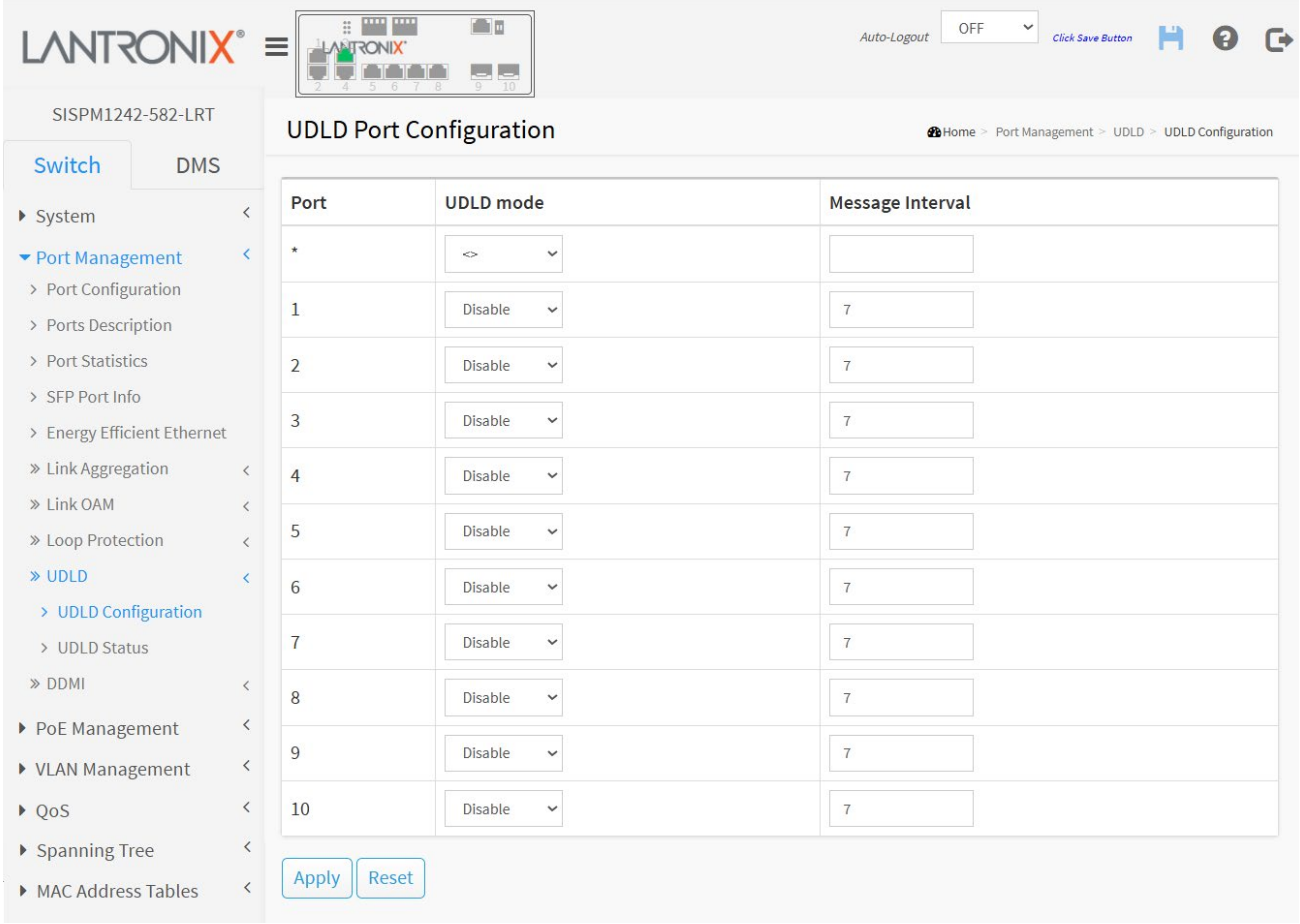
UDLD Configuration

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

Unidirectional Link Detection (UDLD) protocol monitors the physical configuration of the links between devices and ports that support UDLD. It detects the existence of unidirectional links. Its functionality is to provide mechanisms useful for detecting one way connections before they create a loop or other protocol malfunction. RFC 5171 specifies a way at the data link layer to detect unidirectional link.

To configure UDLD parameters in the web UI:

1. Go to Port Management > UDLD > UDLD Configuration.
2. Select the UDLD mode for the required ports.
3. Specify the Message Interval.
4. Click **Apply** to save the settings.



UDLD Port Configuration

Port	UDLD mode	Message Interval
*	<>	
1	Disable	7
2	Disable	7
3	Disable	7
4	Disable	7
5	Disable	7
6	Disable	7
7	Disable	7
8	Disable	7
9	Disable	7
10	Disable	7

Parameter description :

Port : Port number of the switch.

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

- ***Disable***: In disabled mode, UDLD functionality doesn't exist on port.
- ***Normal***: In normal mode, if the link state of the port was determined to be unidirectional, it will not affect the port state.

- ***Aggressive***: In aggressive mode, unidirectional detected ports will get shutdown. To bring back the ports up, you need to disable UDLD on that port.

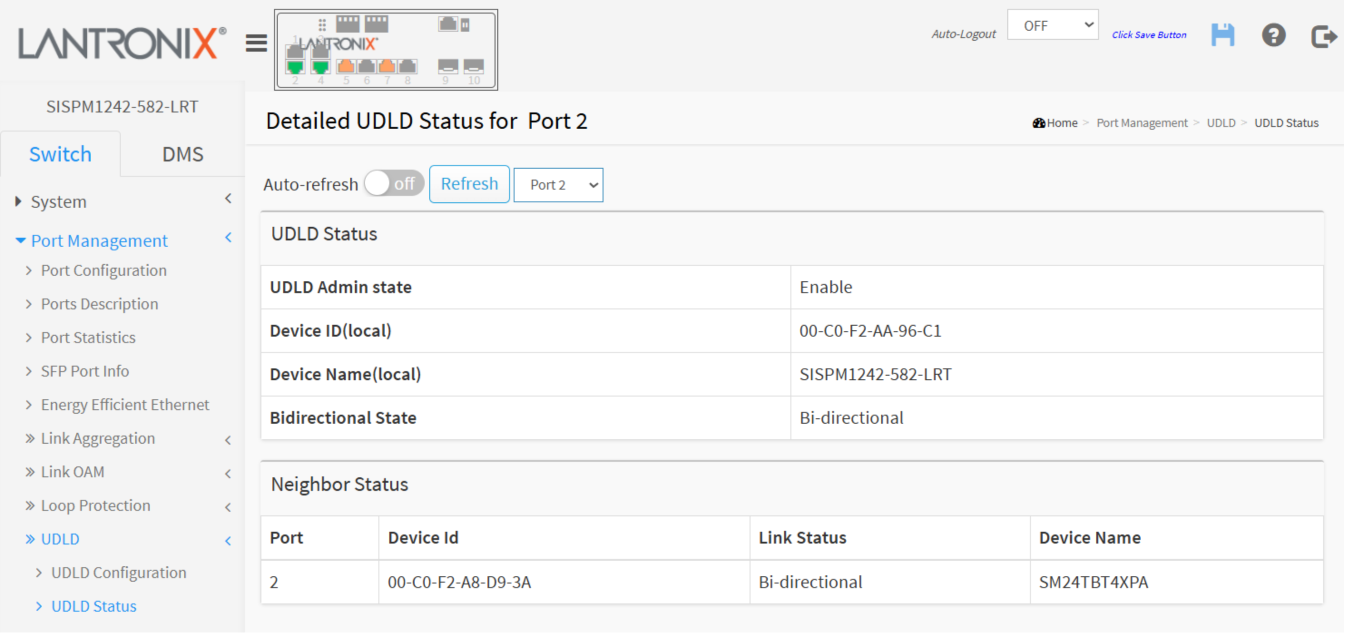
Message Interval : Configures the period between UDLD probe messages on ports that are in the advertisement phase and are determined to be bidirectional. The valid range is 7 - 90 seconds. The default is 7 seconds. Currently only the default time interval is supported due to lack of detailed information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

UDLD Status

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

To display UDLD status:

1. Go to Port Management > UDLD > UDLD Status.
2. At the dropdown select the port on which you want to display UDLD Status.
3. **Auto-refresh** will refresh the page every 3 seconds. **Refresh** will refresh the page immediately.



Detailed UDLD Status for Port 2

UDLD Status

UDLD Admin state	Enable
Device ID(local)	00-C0-F2-AA-96-C1
Device Name(local)	SISPM1242-582-LRT
Bidirectional State	Bi-directional

Neighbor Status

Port	Device Id	Link Status	Device Name
2	00-C0-F2-A8-D9-3A	Bi-directional	SM24TBT4XPA

Parameters

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

Device ID(local) : The ID of Device.

Device Name(local) : Name of the Device.

Bidirectional State : The current state of the port.

Neighbor Status

Port : The current port of neighbor device.

Device Id : The current ID of neighbor device.

Link Status : The current link status of neighbor port.

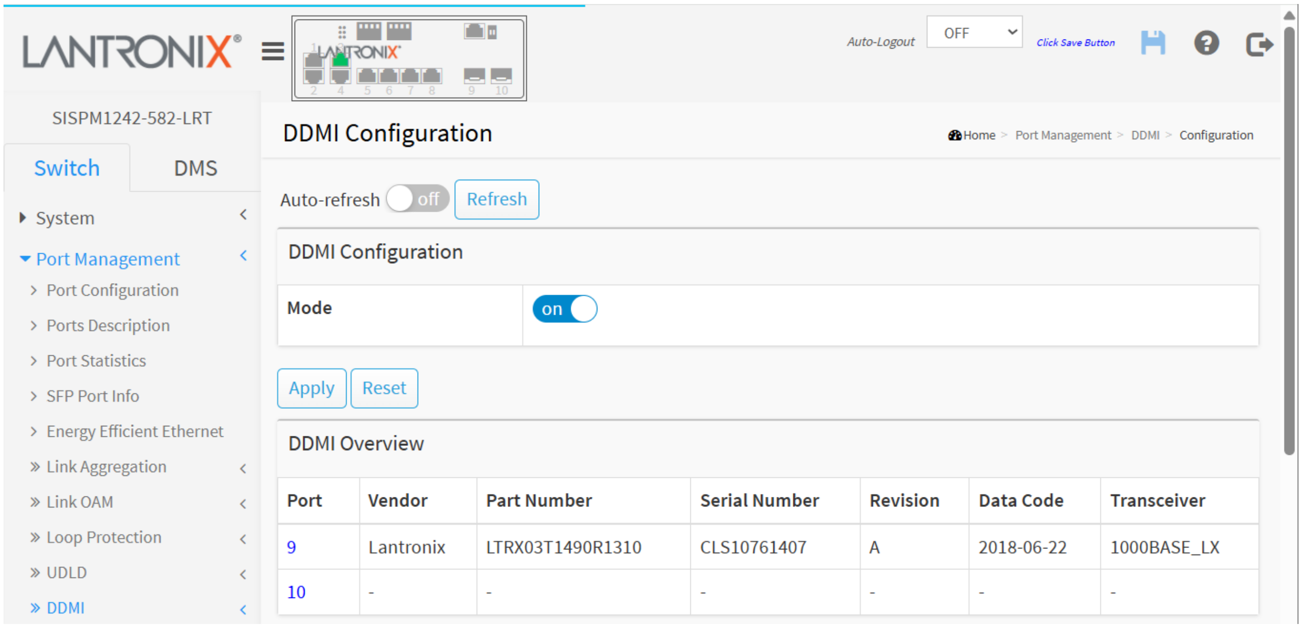
Device Name : The name of the Neighbor Device.

DDMI

Configuration

This page lets you set and view Digital Diagnostics Monitoring Interface (DDMI). DDMI provides an enhanced digital diagnostics monitoring interface for optical transceivers (SFPs) which allows real time access to device operating parameters.

Go to Port Management > DDMI > Configuration.



DDMI Configuration

DDMI Configuration

Mode: on

DDMI Overview

Port	Vendor	Part Number	Serial Number	Revision	Data Code	Transceiver
9	Lantronix	LTRX03T1490R1310	CLS10761407	A	2018-06-22	1000BASE_LX
10	-	-	-	-	-	-

Parameter descriptions :

<u>DDMI Configuration:</u>

Mode : Select the DDMI mode of operation. Possible modes are *On* (enabled) or *Off* (disabled):

<u>DDMI Overview:</u>

Port : The switch port number.

Vendor : Indicates the SFP vendor’s name.

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

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

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

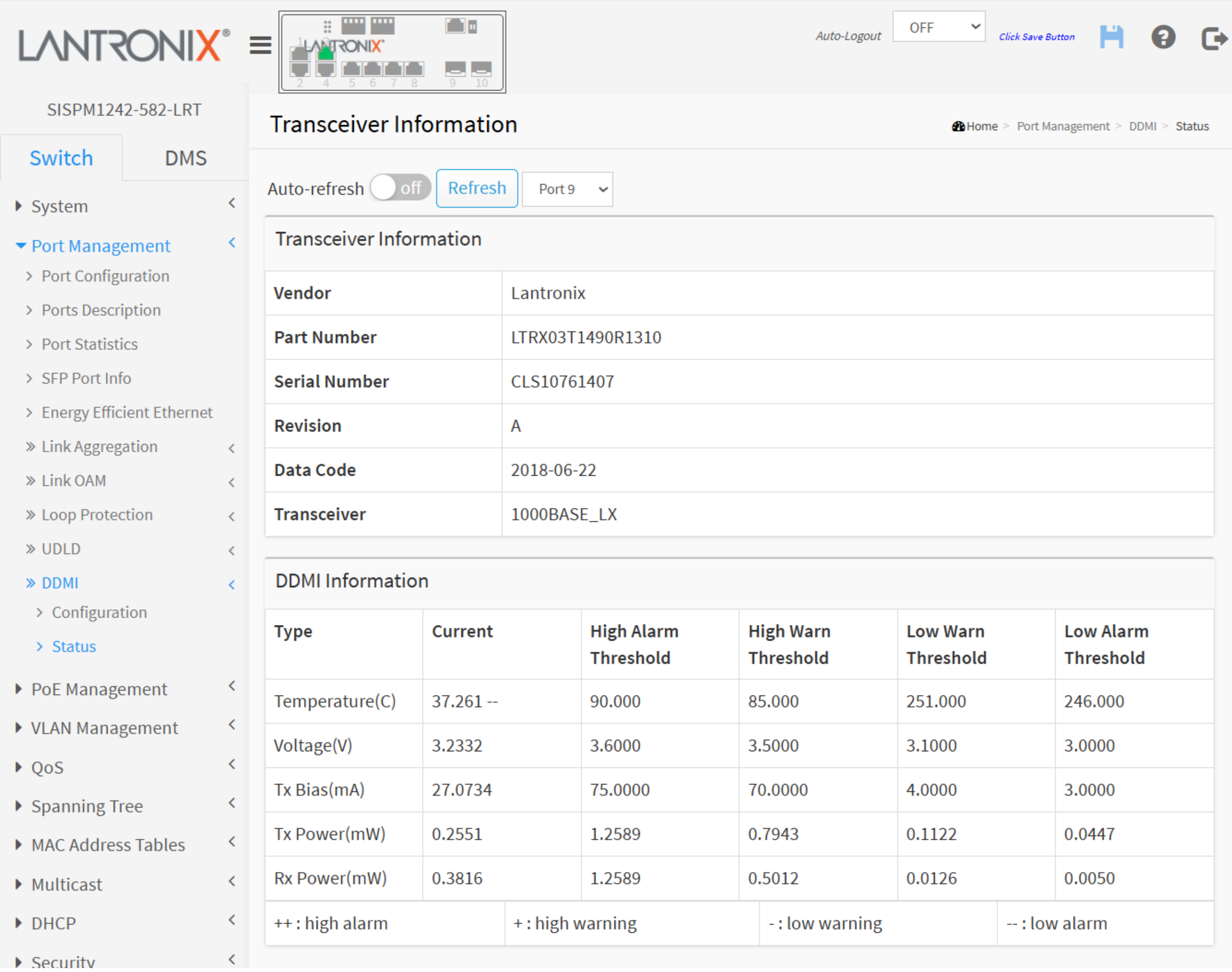
Data Code : Indicates the vendor's manufacturing date code.

Transceiver : Indicates Transceiver compatibility.

Status

This page displays detailed Digital Diagnostics Monitoring Interface (DDMI) information.

1. Go to Port Management > DDMI > Status.
2. At the Port select box select the desired port.
3. **Auto-refresh** will refresh the page every 3 seconds. **Refresh** will refresh the page immediately.



Transceiver Information

Auto-refresh off   Port 9

Transceiver Information

Vendor	Lantronix
Part Number	LTRX03T1490R1310
Serial Number	CLS10761407
Revision	A
Data Code	2018-06-22
Transceiver	1000BASE_LX

DDMI Information

Type	Current	High Alarm Threshold	High Warn Threshold	Low Warn Threshold	Low Alarm Threshold
Temperature(C)	37.261 --	90.000	85.000	251.000	246.000
Voltage(V)	3.2332	3.6000	3.5000	3.1000	3.0000
Tx Bias(mA)	27.0734	75.0000	70.0000	4.0000	3.0000
Tx Power(mW)	0.2551	1.2589	0.7943	0.1122	0.0447
Rx Power(mW)	0.3816	1.2589	0.5012	0.0126	0.0050

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

Parameter descriptions :

Transceiver Information : This section displays transceiver information as described in the previous section.

DDMI Information : This section displays DDMI information.

Type: Temperature, Voltage, Tx bias(mA), Tx Power(mW), Rx Power(mW)

Current : The current value of the associated type.

High Alarm Threshold : The high alarm threshold value of the associated type. (++: high alarm, +: high warning, -: low warning, --: low alarm).

High Warn Threshold : The high warn threshold value of the associated type.

Low Warn Threshold : The low warn threshold value of the associated type.

Low Alarm Threshold : The low alarm threshold value of the associated type.

5. PoE Management

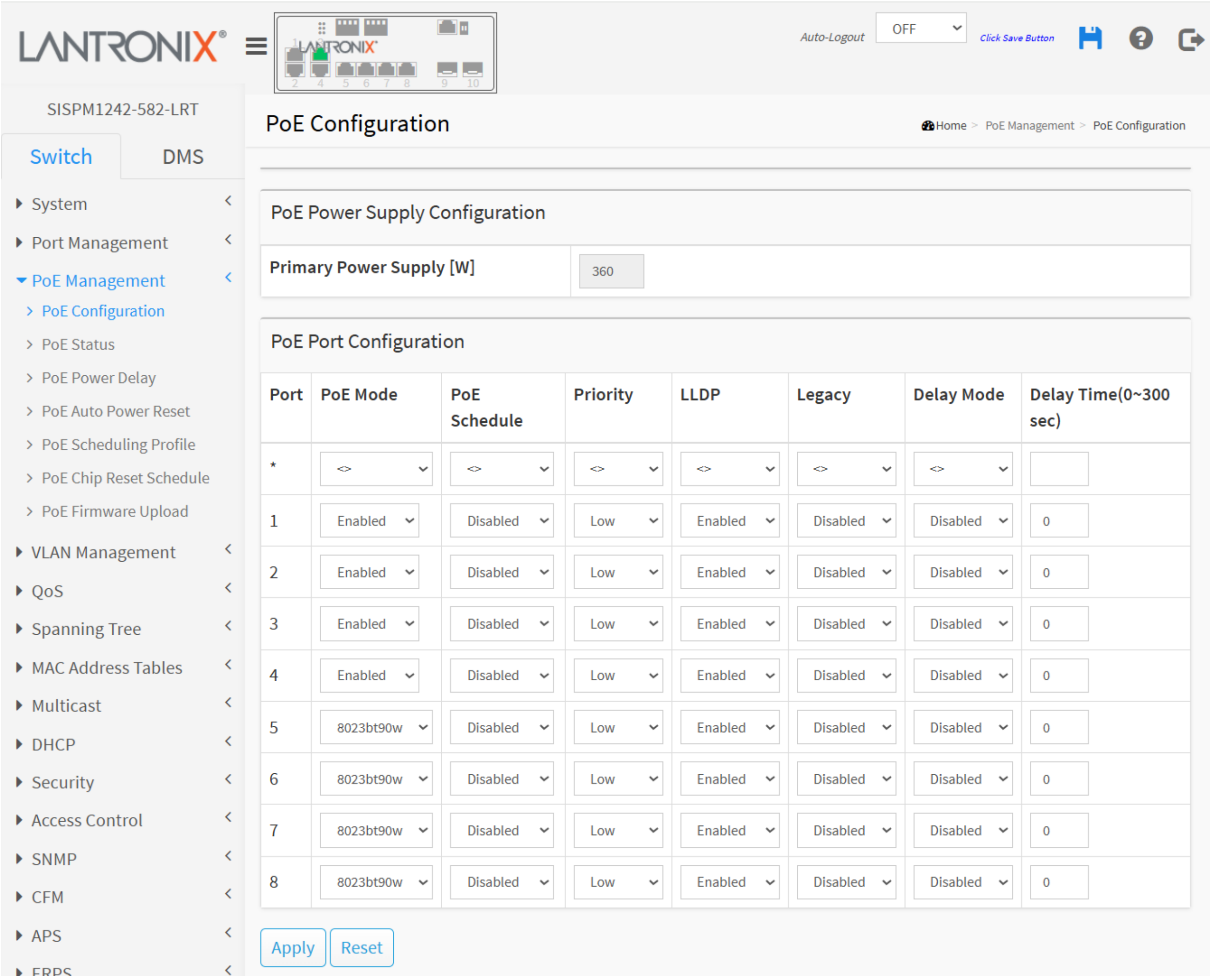
PoE (Power over Ethernet) is used to transmit electrical power to remote devices over standard Ethernet cable. PoE can be used for powering IP phones, wireless LAN access points and other equipment, where it would be difficult or expensive to connect the equipment to main power supply.

PoE Configuration

This page lets you view and configure the PoE port settings.

To configure the Power over Ethernet ports in the web UI:

1. Go to PoE Management > PoE Configuration.
2. Note the *Primary Power Supply* value, which is the total amount of power that the power source can deliver to the powered devices (PDs).
3. Configure the PoE settings for the required ports. Refer to the parameter descriptions for details.
4. Click **Apply**.



PoE Configuration

PoE Power Supply Configuration

Primary Power Supply [W]	360

PoE Port Configuration

Port	PoE Mode	PoE Schedule	Priority	LLDP	Legacy	Delay Mode	Delay Time(0~300 sec)
*	<>	<>	<>	<>	<>	<>	
1	Enabled	Disabled	Low	Enabled	Disabled	Disabled	0
2	Enabled	Disabled	Low	Enabled	Disabled	Disabled	0
3	Enabled	Disabled	Low	Enabled	Disabled	Disabled	0
4	Enabled	Disabled	Low	Enabled	Disabled	Disabled	0
5	8023bt90w	Disabled	Low	Enabled	Disabled	Disabled	0
6	8023bt90w	Disabled	Low	Enabled	Disabled	Disabled	0
7	8023bt90w	Disabled	Low	Enabled	Disabled	Disabled	0
8	8023bt90w	Disabled	Low	Enabled	Disabled	Disabled	0

Parameter descriptions:

PoE Power Supply Configuration

Primary Power Supply: For being able to determine the amount of power the powered device (PD) may use, it must be defined what amount of power a power source can deliver. The power requirements of the PDs must total less than this amount. Valid values are in the range 0 to 360 Watts.

PoE Port Configuration:

Note: Maximum Power [W] Field Settings Limitation: 4 groups consisting of (Port 1+2) , (Port 3+4), (Port 5+ 6), (Port 7+ 8), maximum per group: 120W, maximum per port: 90W.

Port: The logical port number for this row. Ports that are not PoE-capable are grayed out and not available to configure PoE for.

PoE Mode: The PoE Mode represents the PoE operating mode for the port.

Disabled : PoE disabled for the port.

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

Force: The switch port will power up the linked PD without any detect/negotiate mechanism (PD limited to 30 W).

The following selections are available only for the PoE++ ports.

Disabled: PoE disabled for the port.

4pair60w : The switch port will power up the linked PD using 4-pair mode (PDs limited to 60W). This mode is based on PoE 802.3at detection and classification mechanism to support high power 4-Pair 60W. The max power is 60W but can still power 15W or 30W PDs.

4pair90w : The switch port will power up the linked PD using 4-pair mode (PDs limited to 90W). This mode is based on PoE 802.3at detection and classification mechanism to support high power 4-Pair 90W. Max power is 90W, can still power 15W, 30W, or 60W PDs.

8023bt90w : Enables PoE IEEE 802.3bt (Class 8 PDs limited to 90W). Class negotiation up to 90W and supports 802.3 af/at/bt. Max power is 90W.

8023bt60w : Enables PoE IEEE 802.3bt (Class 8 PDs limited to 60W) (default setting). Class negotiation up to 60W and support s802.3 af/at/bt. Max power is 60W.

8023bt30w : Enables PoE IEEE 802.3bt (Class 8 PDs limited to 30W). Max power is 30W.

force90w : Enables PoE force power (PDs limited to 90W). The power output depends on the PD (e.g., if the PD requires 10W, then the output will be 10W and the maximum output will be 90W).

force60w : Enables PoE force power (PDs limited to 60W). The power output depends on the PD (e.g., if the PD requires 10W, then the output will be 10W and the maximum output will be 60W).

Caution: using PoE ‘Force’ mode to force the switch to send PoE to non-PoE devices can physically damage those devices.

Caution: If utilizing the PoE Force mode feature, only connect PDs which support power input in the 48~56V range to prevent damage to PDs. When the port is changed to Force mode, the port's PoE LED lights immediately.

Caution: PoE device components may fail due to transient voltage spikes on the PoE line. It is strongly suggested that a surge suppressor be used on each PoE port, especially in areas with frequent lightning and other types of interference.

PoE Schedule: The PoE Schedule is defined by the Scheduling Profile. Select as ***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 in the case where the remote device requires 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. The default setting is ***Low*** priority.

LLDP: ***Enabled*** means after HW detection and classification to do PoE powering, then the PoE switch can adjust PoE powering behaviors based on LLDP-MED packets from PoE PD devices.

Legacy: ***Enabled*** means support for capacitor detection to detect legacy (pre-standard) PoE PDs (powered devices).

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 runs out of delay time. The default is 0; the valid range is 0-300 seconds.

Recommended Settings

Recommended PoE++ configuration settings for different cameras or other higher powered PDs on the switch.

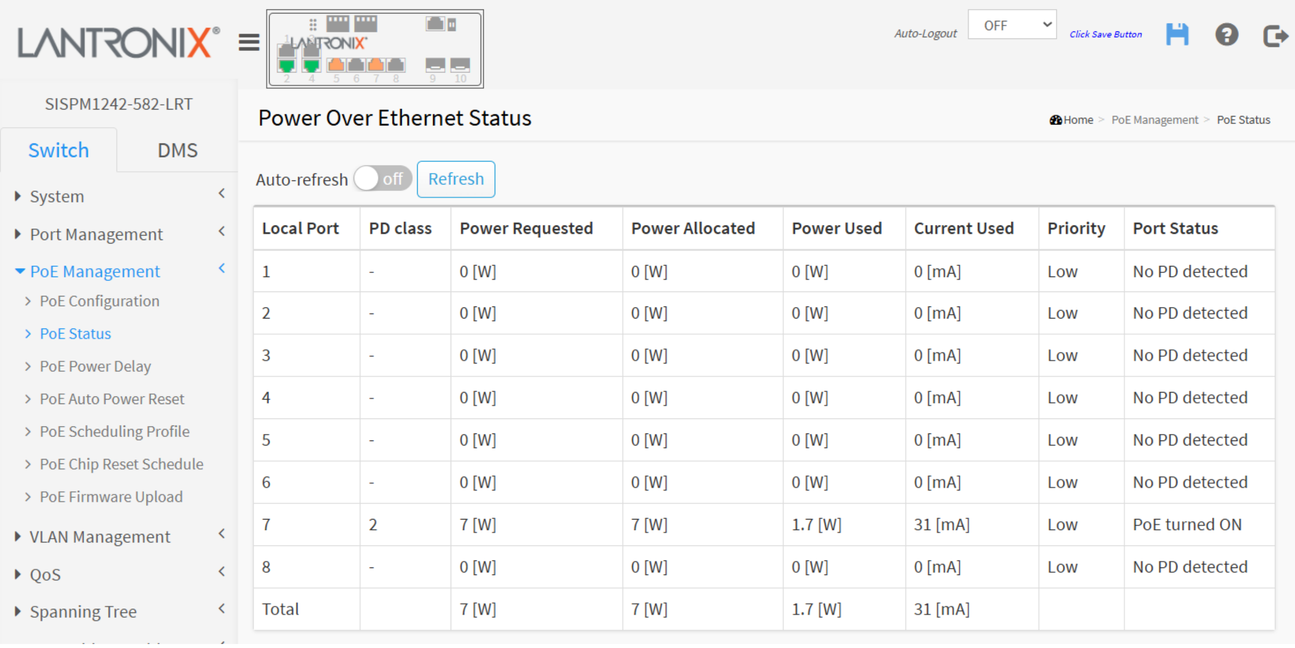
Application	Recommended Setting
Camera is 802.3af/at.	Use 802.3bt30W mode.
Camera is not 802.3bt but requires more than 30W.	Use 802.3bt60W mode.
Camera specifies it is HPOE.	Use 4pair90W mode.

PoE Status

This page displays the status for all PoE ports.

To display PoE port status in the web UI:

1. Go to PoE Management > PoE Status.
2. **Auto-refresh** will refresh the page every 3 seconds. **Refresh** will refresh the page immediately.



Local Port	PD class	Power Requested	Power Allocated	Power Used	Current Used	Priority	Port Status
1	-	0 [W]	0 [W]	0 [W]	0 [mA]	Low	No PD detected
2	-	0 [W]	0 [W]	0 [W]	0 [mA]	Low	No PD detected
3	-	0 [W]	0 [W]	0 [W]	0 [mA]	Low	No PD detected
4	-	0 [W]	0 [W]	0 [W]	0 [mA]	Low	No PD detected
5	-	0 [W]	0 [W]	0 [W]	0 [mA]	Low	No PD detected
6	-	0 [W]	0 [W]	0 [W]	0 [mA]	Low	No PD detected
7	2	7 [W]	7 [W]	1.7 [W]	31 [mA]	Low	PoE turned ON
8	-	0 [W]	0 [W]	0 [W]	0 [mA]	Low	No PD detected
Total		7 [W]	7 [W]	1.7 [W]	31 [mA]		

Parameter descriptions:

Local Port : Logical port number for this row.

PD class : Each PD is classified according to a class that defines the maximum power the PD will use. The PD class column shows each PD's class. These PD Classes are defined:

Class 1: Max. power 4.0 W	**Class 5**: Max/ power 45 W
Class 2: Max. power 7.0 W	**Class 6**: Max/ power 60 W
Class 3: Max. power 15.4 W	**Class 7**: Max/ power 75 W
Class 4: Max. power 30.0 W	**Class 8**: Max/ power 90 W

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

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 in Watts.

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

Priority : Shows the port's priority configured by the user.

Port Status : Shows the port's status. The status can be one of these values:

- ***PoE turned ON*** : The PD is powered on.
- ***PoE not available*** : No PoE chip found - PoE not supported for the port.
- ***PoE turned OFF - PoE disabled*** : PoE is disabled by user.

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

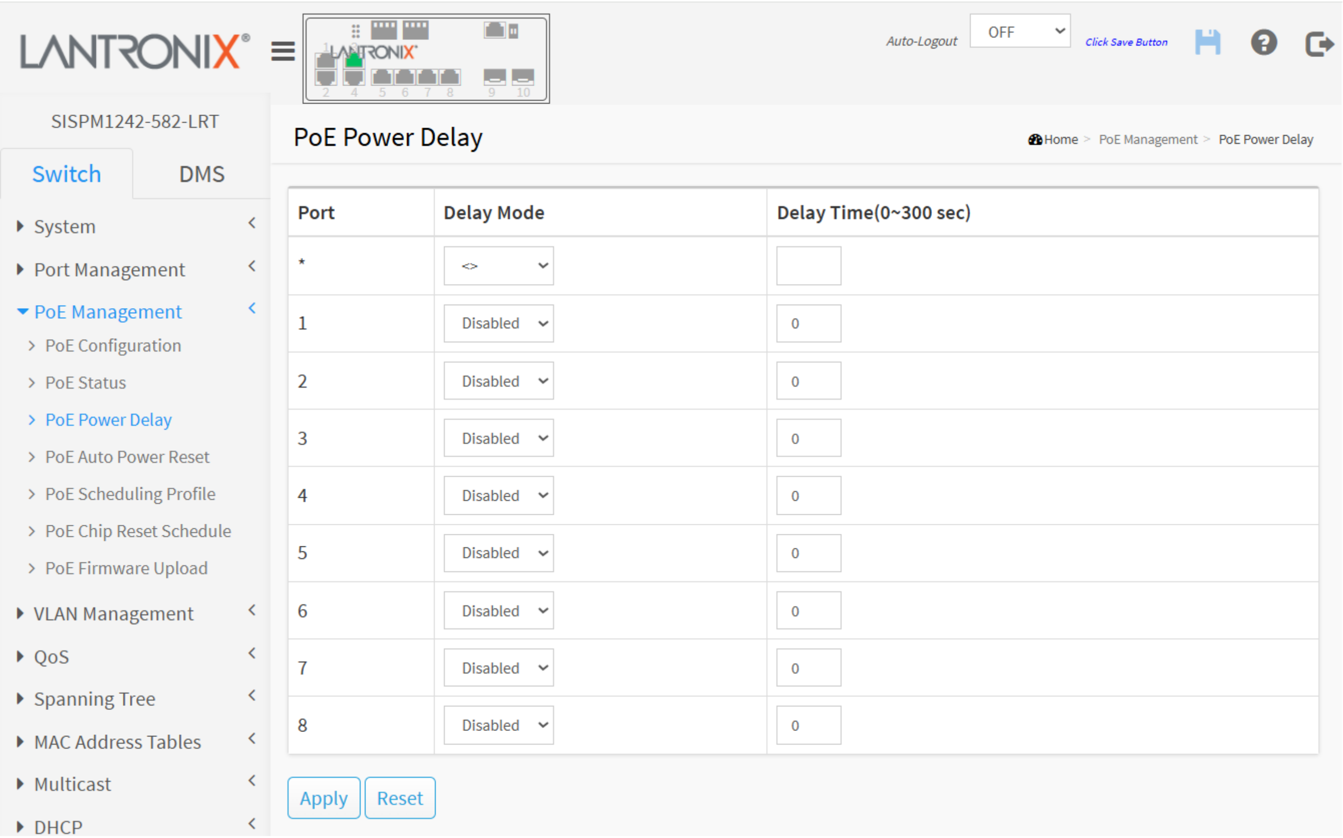
Total: For each port a sum of the Power Requested, Power Allocated, Power Used, and Current Used is provided.

PoE Power Delay

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

To configure PoE Power Delay in the web UI:

1. Go to PoE Management > PoE Power Delay.
2. For each port set the Delay Mode and set the Delay Time.
3. Click **Apply** to save the changes.



PoE Power Delay

Port	Delay Mode	Delay Time(0~300 sec)
*	<>	
1	Disabled	0
2	Disabled	0
3	Disabled	0
4	Disabled	0
5	Disabled	0
6	Disabled	0
7	Disabled	0
8	Disabled	0

Parameter descriptions:

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

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

Enabled: Enable POE Power Delay.

Disabled: Disable POE Power Delay.

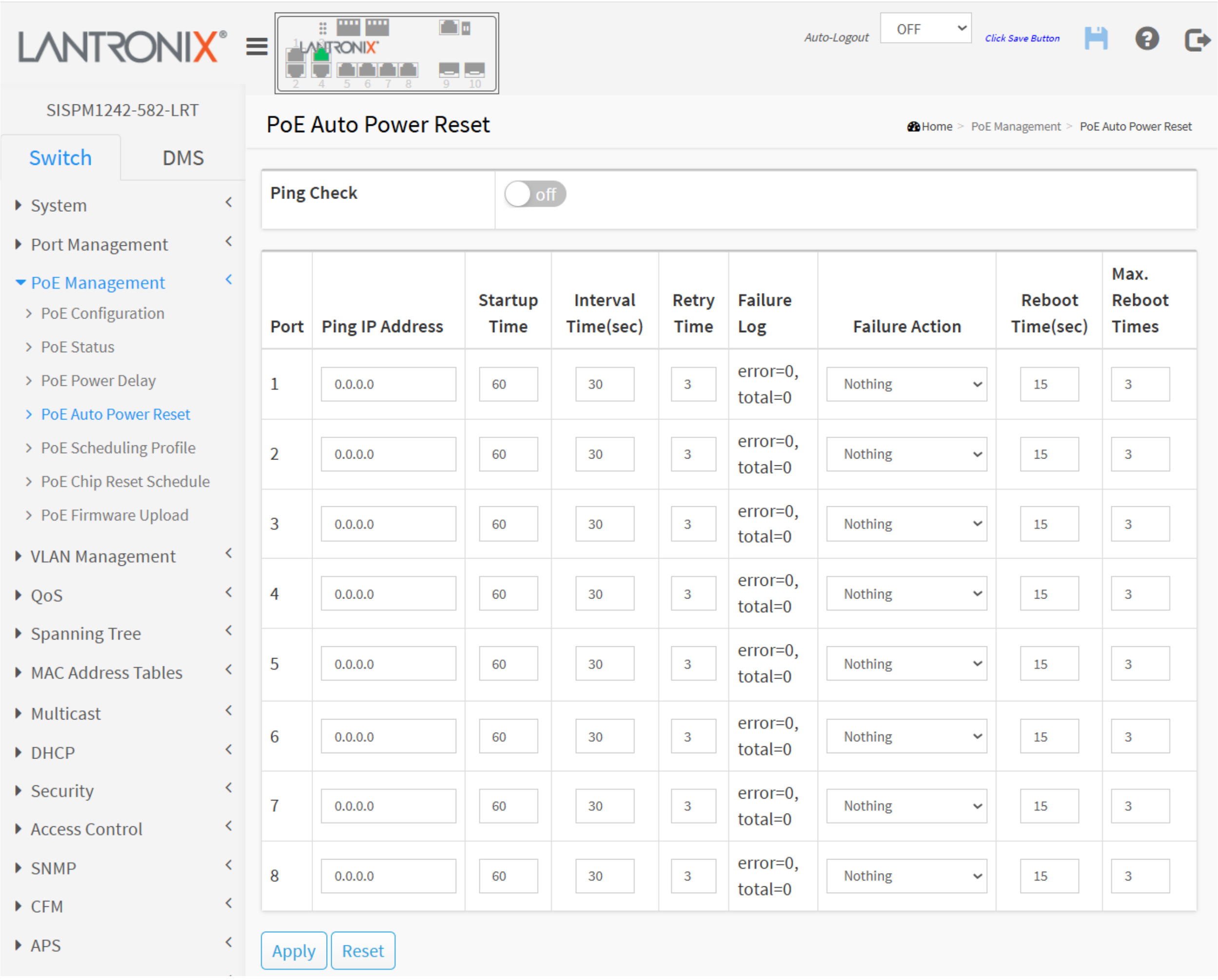
Delay Time(0~300sec) : When rebooting, the PoE port will start to provide power to the PD when it runs out of delay time. The default is 0; the valid range is 0-300 seconds.

PoE Auto Power Reset

This page lets you specify the auto detection parameters to check the link status between switch PoE ports and PDs. When it detects a failed connection, the switch will reboot the remote PD automatically.

To configure PoE Auto Power Reset in the web UI:

1. Go to PoE Management > PoE Auto Power Reset.
2. Enable the Ping Check function.
3. Specify the PDs Ping IP address, startup time, checking interval, retry times, failure action, reboot time, and max. reboot times.
4. Click **Apply** to save the changes.



PoE Auto Power Reset

Ping Check: off

Port	Ping IP Address	Startup Time	Interval Time(sec)	Retry Time	Failure Log	Failure Action	Reboot Time(sec)	Max. Reboot Times
1	0.0.0.0	60	30	3	error=0, total=0	Nothing	15	3
2	0.0.0.0	60	30	3	error=0, total=0	Nothing	15	3
3	0.0.0.0	60	30	3	error=0, total=0	Nothing	15	3
4	0.0.0.0	60	30	3	error=0, total=0	Nothing	15	3
5	0.0.0.0	60	30	3	error=0, total=0	Nothing	15	3
6	0.0.0.0	60	30	3	error=0, total=0	Nothing	15	3
7	0.0.0.0	60	30	3	error=0, total=0	Nothing	15	3
8	0.0.0.0	60	30	3	error=0, total=0	Nothing	15	3

Parameter descriptions:

Ping Check : Enable Ping Check function to detect the connection between PoE port and PD. Disable will turn off the detection.

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

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

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

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

Retry Time : When the PoE port can't ping the PD, it will try to send detection again. After the third unsuccessful try, it will trigger the configured failure action. The default is 3; the valid range is 1-5 retry attempts.

Failure Log : Failure loggings counter (e.g., error=0, total=28).

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 rebooted.

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

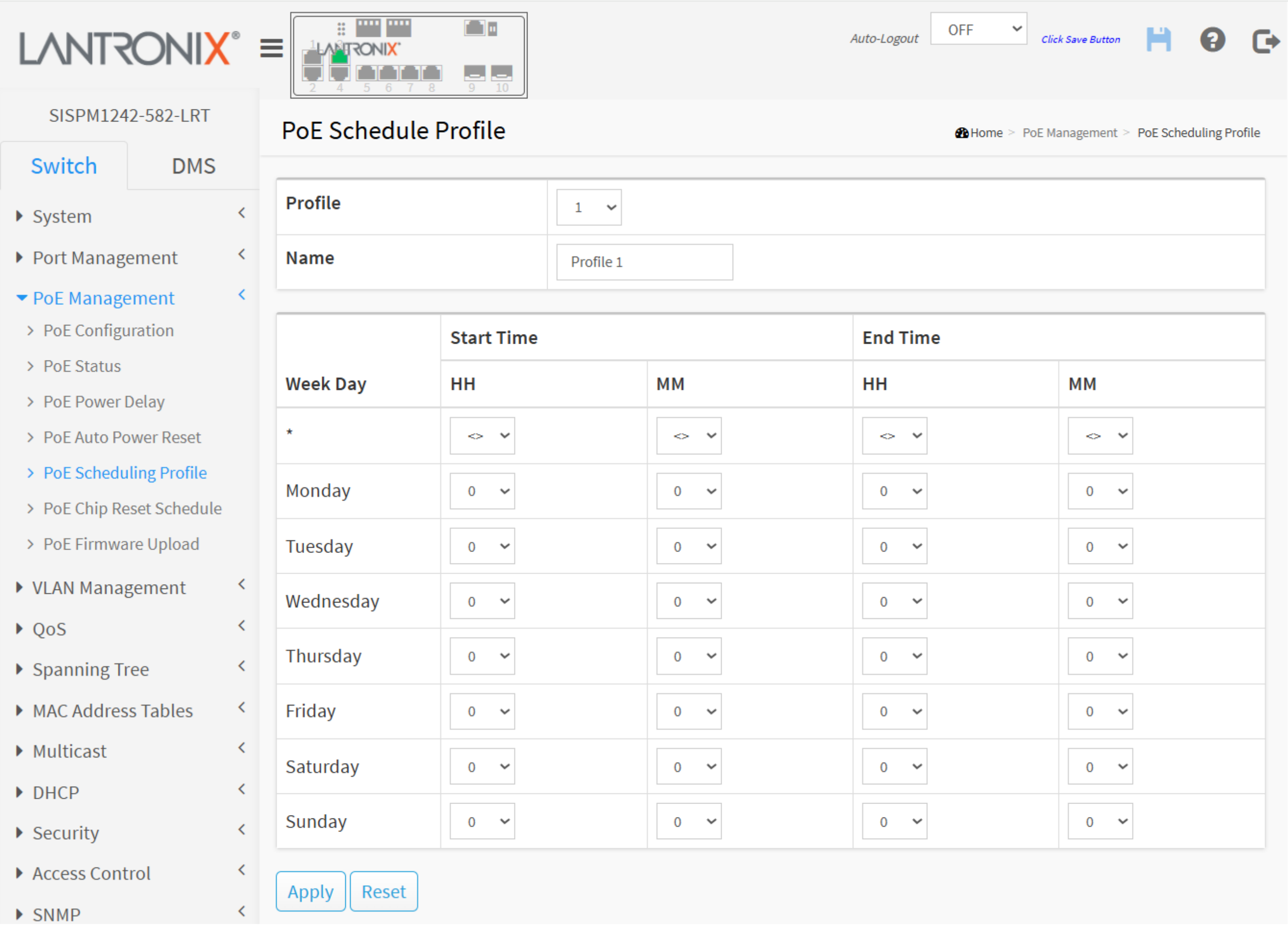
Max. Reboot Times: When Failure Action is set to Reboot Remote PD, it limits the number of times the PD will be rebooted. The default is 3 times; the valid range is 0-10 times. Entering 0 means unlimited reboots.

PoE Scheduling Profile

This page lets you schedule PoE power supply. PoE Scheduling simplifies PoE management and saves energy.

To configure PoE Scheduling in the web UI:

1. Go to PoE Management > PoE Schedule Profile.
2. Select a Profile and Profile Name.
3. Select time and day to supply power.
4. Click **Apply** to apply the changes.



PoE Schedule Profile

Profile	1
Name	Profile 1

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

Parameter descriptions:

Profile : This is the logical port number for this row. You can create and name up to 16 profiles.

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

Week Day : The day to schedule PoE.

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

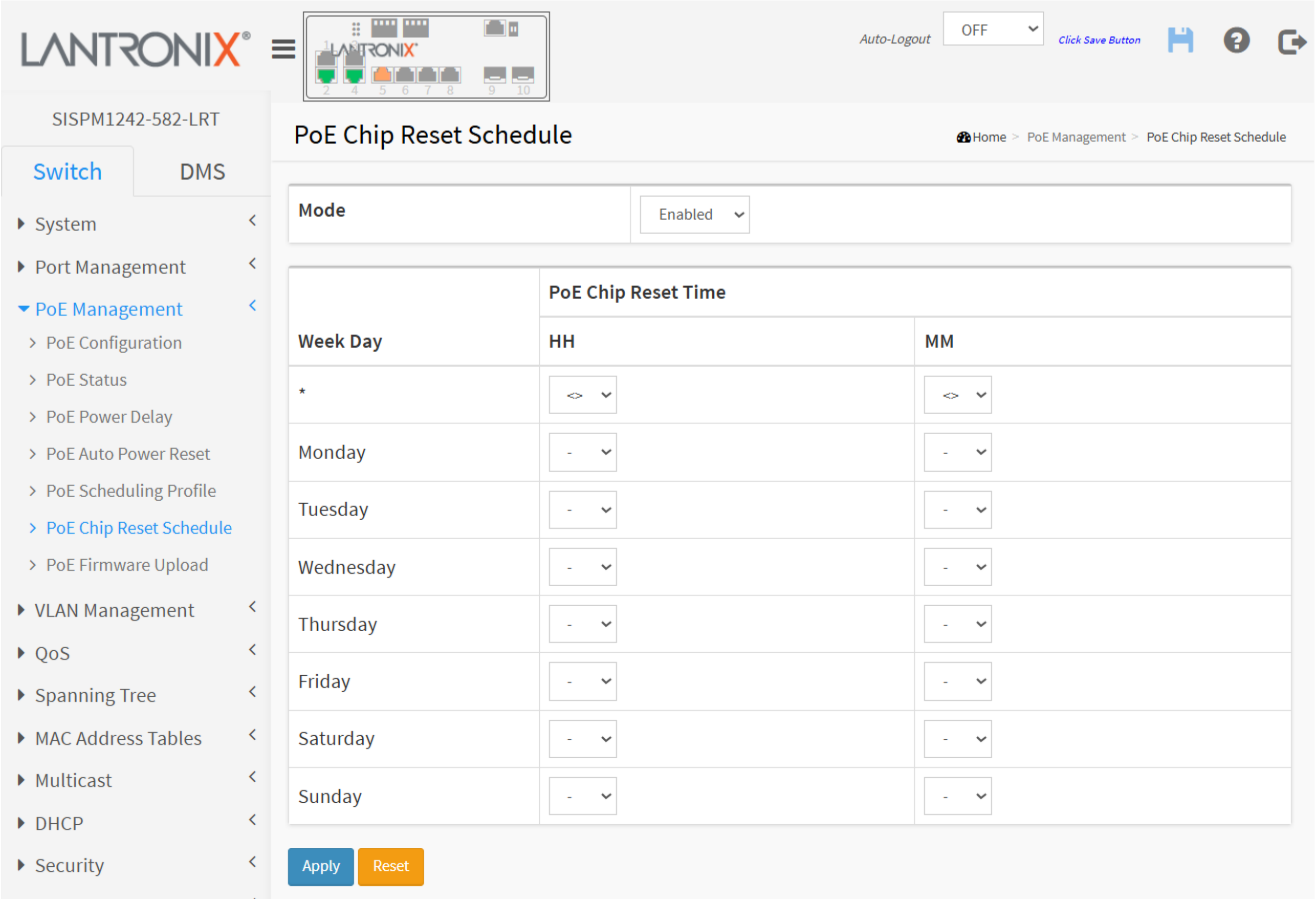
End Time : The time to stop PoE in hours and days. The time 00:00 means the last second of this day.

PoE Chip Reset Schedule

This page lets you schedule when to reset the PoE chip.

To schedule PoE Chip Reset in the web UI:

1. Go to PoE Management > PoE Chip Reset Schedule.
2. At the Mode dropdown, select Enabled. The configurable parameters are displayed.
3. Select the day(s) and time(s) for the PoE chip reset to occur.
4. Click **Apply** to apply the changes.



PoE Chip Reset Schedule

Mode	Enabled

	PoE Chip Reset Time	
Week Day	**HH**	**MM**
*	<>	<>
Monday	-	-
Tuesday	-	-
Wednesday	-	-
Thursday	-	-
Friday	-	-
Saturday	-	-
Sunday	-	-

Parameter descriptions:

Mode : Indicates the chip reset scheduling mode operation. Possible modes are:

> ***Enabled***: Enable PoE chip reset.
>
> ***Disabled***: Disable PoE chip reset.

Week Day : The day to reset PoE chip.

PoE Chip Reset Time : The time to reset PoE chip in hours and minutes.

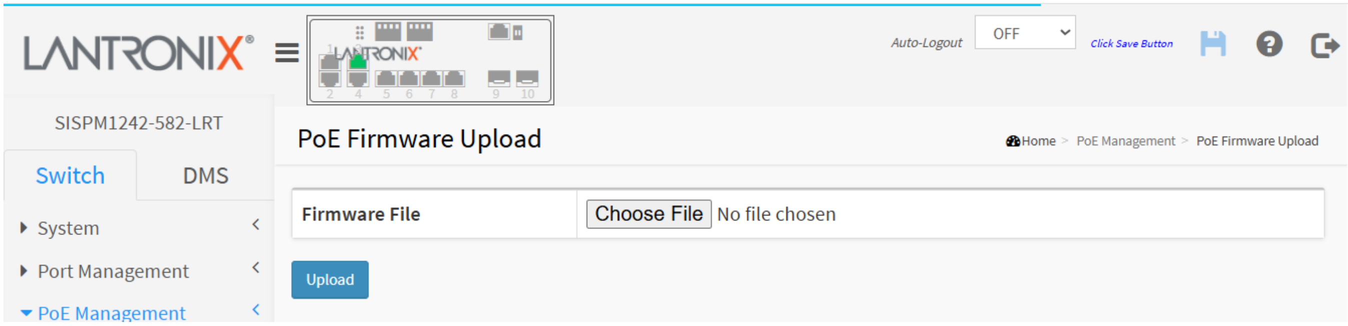
PoE Firmware Upload

Upgrade the PoE firmware controlling the switch.

Important: While the PoE firmware is being upgraded, Web access appears to be defunct. Do not restart or power off the switch at this time or the switch may fail to function afterwards.

To upgrade the PoE firmware:

1. Go to PoE > PoE Firmware Upload.
2. Click **Choose File** to find the location of the PoE firmware file.
3. Select the file and click **Upload**.
4. After the PoE firmware is uploaded, the firmware update will be initiated. Wait about a minute for the firmware to update and the switch to restart.



PoE Firmware Upload

Firmware File	Choose File No file chosen

6. VLAN Management

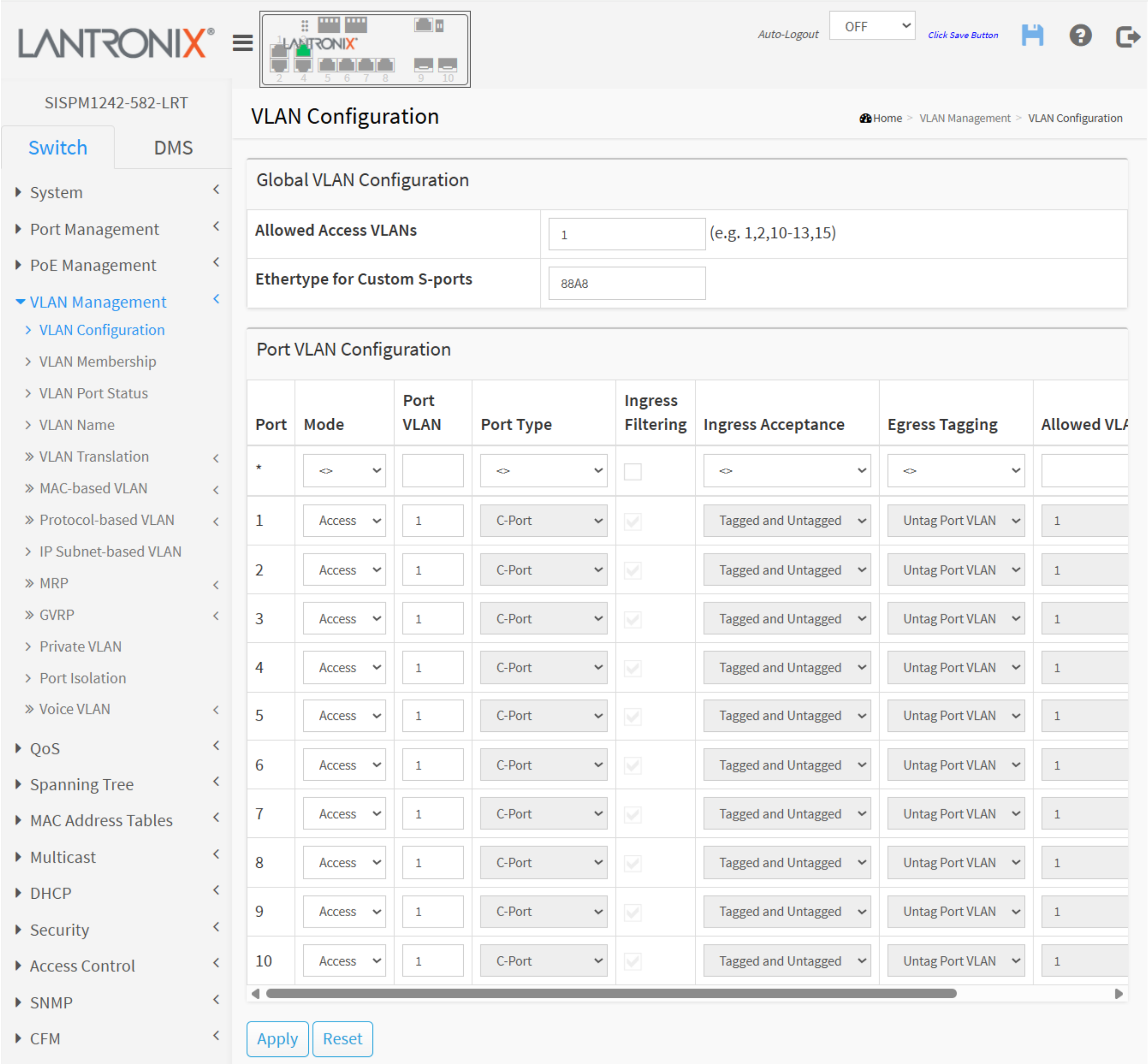
VLAN Configuration

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

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

To configure VLANs globally and per-port in the web UI:

1. Go to VLAN Management > VLAN Configuration.
2. Modify Global VLAN Configuration parameters.
3. Select the Port VLAN Configuration parameters.
4. Click **Apply** to save the settings.



VLAN Configuration

Global VLAN Configuration

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

Port VLAN Configuration

Port	Mode	Port VLAN	Port Type	Ingress Filtering	Ingress Acceptance	Egress Tagging	Allowed VLA
*	<>		<>	☐	<>	<>	
1	Access	1	C-Port	☑	Tagged and Untagged	Untag Port VLAN	1
2	Access	1	C-Port	☑	Tagged and Untagged	Untag Port VLAN	1
3	Access	1	C-Port	☑	Tagged and Untagged	Untag Port VLAN	1
4	Access	1	C-Port	☑	Tagged and Untagged	Untag Port VLAN	1
5	Access	1	C-Port	☑	Tagged and Untagged	Untag Port VLAN	1
6	Access	1	C-Port	☑	Tagged and Untagged	Untag Port VLAN	1
7	Access	1	C-Port	☑	Tagged and Untagged	Untag Port VLAN	1
8	Access	1	C-Port	☑	Tagged and Untagged	Untag Port VLAN	1
9	Access	1	C-Port	☑	Tagged and Untagged	Untag Port VLAN	1
10	Access	1	C-Port	☑	Tagged and Untagged	Untag Port VLAN	1

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, and 200: 1,10-13,200. Spaces are allowed between the delimiters.

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

Port VLAN Configuration

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

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

Access: Access ports are normally used to connect to end stations. Dynamic features like Voice VLAN may add the port to more VLANs behind the scenes. Access ports have these characteristics:

- member of exactly one VLAN, the Port VLAN (a.k.a. Access VLAN), which by default is 1,
- accepts untagged frames and C-tagged frames,
- discards all frames that are not classified to the Access VLAN,
- on egress all frames are transmitted untagged.

Trunk: Trunk ports can carry traffic on multiple VLANs simultaneously and are normally used to connect to other switches. Trunk ports have these characteristics:

- by default, a trunk port is member of all existing VLANs. This may be limited 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 1.

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

On egress, frames classified to the Port VLAN do not get tagged if Egress Tagging configuration is set to untag Port VLAN. The Port VLAN is called an "Access VLAN" for ports in Access mode and “Native VLAN” for ports in Trunk or Hybrid mode.

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

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

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

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

- ***Tagged and untagged***: both tagged and untagged frames are accepted.
- ***Tagged Only*** : Only tagged frames are accepted on ingress. Untagged frames are discarded.
- ***Untagged Only*** : Only untagged frames are accepted on ingress. Tagged frames are discarded.

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

- ***Untag Port VLAN*** : Frames classified to the Port VLAN are transmitted untagged. Other frames are transmitted with the relevant tag.
- ***Tag All*** : All frames, whether classified to the Port VLAN or not, are transmitted with a tag.
- ***Untag All*** : All frames, whether classified to the Port VLAN or not, are transmitted without a tag. This option is only available for ports in Hybrid mode.

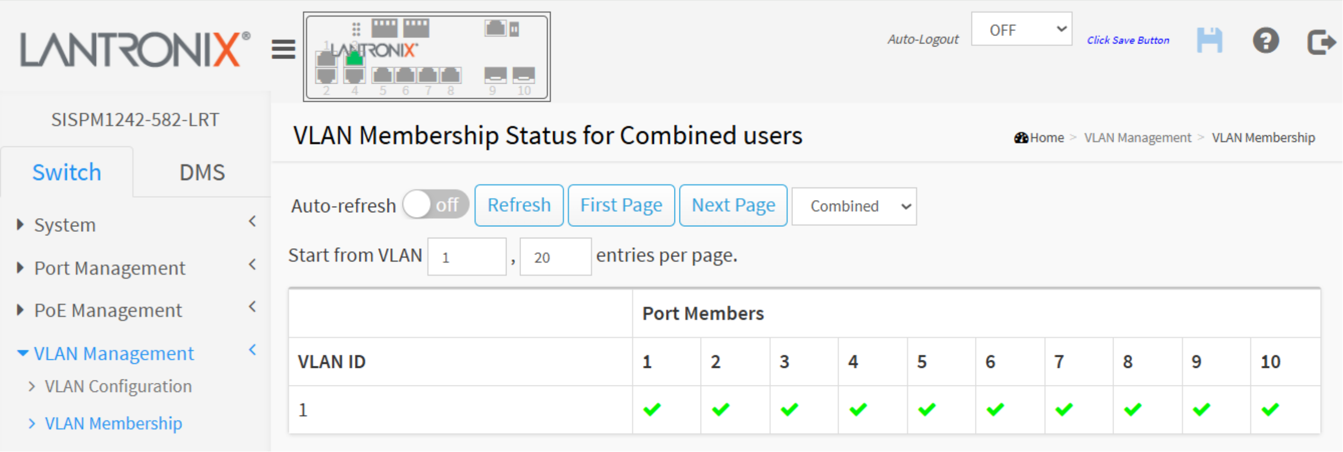
Allowed VLANs : Ports in Trunk and Hybrid mode may control which VLANs they are allowed to become members of. Access ports can only be member of one VLAN, the Access VLAN. The field's syntax is identical to the syntax used in the Existing VLANs field. By default, a port may become member of all possible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

VLAN Membership

This page lets you set membership status of VLAN users. To configure VLAN membership in the web UI:

1. Go to VLAN Management > VLAN Membership.
2. At the User select dropdown choose which VLAN users are to be displayed.
3. **Auto-refresh** will refresh the page every 3 seconds. **Refresh** will refresh the page immediately.
4. Use the page controls and “Start from” entry fields to help you navigate through the list.



VLAN Membership Status for Combined users

Auto-refresh off

Combined

Start from VLAN 1 , 20 entries per page.

	Port Members									
VLAN ID	1	2	3	4	5	6	7	8	9	10
1	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓

Parameter descriptions:

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

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

- ***Combined*** : shows a combination of the administrator and internal software modules configuration, and basically reflects what is configured in hardware.
- ***Admin*** : shows the administrator members status.
- ***NAS*** : provides port-based authentication, which involves communications between a Supplicant, Authenticator, and an Authentication Server.
- ***MVRP*** : MVRP 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.
- ***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.
- ***RMirror***: shows the RMirror members status.
- ***DMS*** : Shows Device Management System VLAN membership status.
- ***MRP***: Shows Multiple Registration Protocol members status.

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.

- ✓ - This icon is displayed if a port is included in a VLAN.
- ✗ - This icon is displayed if a port is in the forbidden port list, the following image will be displayed:.
- ⊘ - This icon is displayed if a port is in the forbidden port list and at the same time attempted included in the VLAN. The port will not be a member of the VLAN in this case.
- Frames classified to the Port VLAN are transmitted tagged (T) or untagged (U).

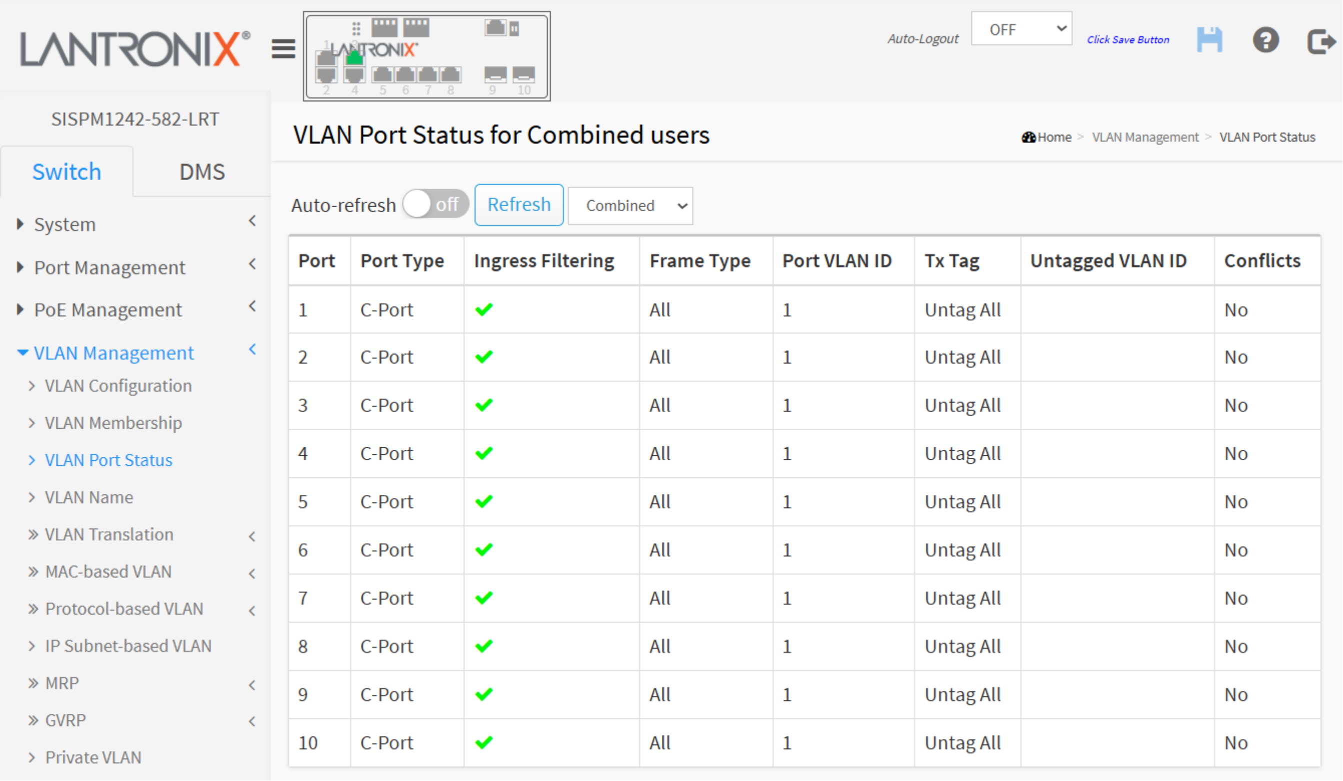
Show Number of entries per page : Choose how many items you want to be displayed. The VLAN Membership Status page shows the current VLAN port members for all VLANs configured by a selected VLAN User (selection allowed by a Combo box). When “Combined” users are selected, it shows this information for all the VLAN Users, and this is by default. VLAN membership allows the frames classified to the VLAN ID to be forwarded on the respective VLAN member ports.

VLAN Port Status

This page displays all VLAN port status.

To display VLAN Port Status in the web UI:

1. Go to VLAN Management > VLAN Port Status.
2. At the dropdown select the VLAN User to be displayed.
3. **Auto-refresh** will refresh the page every 3 seconds. **Refresh** will refresh the page immediately.



VLAN Port Status for Combined users

Port	Port Type	Ingress Filtering	Frame Type	Port VLAN ID	Tx Tag	Untagged VLAN ID	Conflicts
1	C-Port	✓	All	1	Untag All		No
2	C-Port	✓	All	1	Untag All		No
3	C-Port	✓	All	1	Untag All		No
4	C-Port	✓	All	1	Untag All		No
5	C-Port	✓	All	1	Untag All		No
6	C-Port	✓	All	1	Untag All		No
7	C-Port	✓	All	1	Untag All		No
8	C-Port	✓	All	1	Untag All		No
9	C-Port	✓	All	1	Untag All		No
10	C-Port	✓	All	1	Untag All		No

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 configured in hardware. If a given software module hasn't overridden any of the port settings, the text "No data exists for the selected user" is shown in the table.

- ***Combined*** : Shows a combination of the administrator and internal software modules configuration, and basically reflects what is configured in hardware.
- ***Admin*** : Shows VLAN memberships as configured by an Admin, and not by one of these internal software modules.
- ***NAS*** : NAS provides port-based authentication, which involves communications between a Supplicant, Authenticator, and an Authentication Server.
- ***GVRP*** : Adjacent VLAN-aware devices can exchange VLAN information with each other by using Generic VLAN Registration Protocol (GVRP). GVRP is based on the Generic Attribute Registration Protocol (GARP) and propagates VLAN information throughout a bridged network.

- ***MVR*** : MVR is used to eliminate the need to duplicate multicast traffic for subscribers in each VLAN. Multicast traffic for all channels is sent only on a single (multicast) VLAN.
- ***Voice VLAN*** : Voice VLAN is a VLAN configured specially for voice traffic typically originating from IP phones.
- ***MSTP*** : The 802.1s Multiple Spanning Tree protocol (MSTP) uses VLANs to create multiple spanning trees in a network, which significantly improves network resource utilization while maintaining a loop-free environment.
- ***ERPS*** : Shows Ethernet Ring Protection Switching membership status.
- ***DMS*** : Shows DMS VLAN membership status.
- ***VCL*** : VLAN Control List; shows MAC-based VLAN entries configured by various MAC-based VLAN users.
- ***RMirror*** : show VLAN membership entries configured by the Mirroring internal software module.
- ***DMS*** : Shows Device Management System VLAN membership status.
- ***MRP***: Shows Multiple Registration Protocol members status.

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

Port Type : Shows the port type (Unaware, C-Port, S-Port, S-Custom-Port.) that a given user wants to configure on the port. The field is empty if not overridden by the selected user.

Ingress Filtering : Shows whether a given user wants ingress filtering enabled or not. The field is empty if not overridden by the selected user.

Frame Type : Shows the acceptable frame types (All, Taged, Untagged) that a given user wants to configure on the port. The field is empty if not overridden by the selected user.

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 creates a “conflict”, which is solved in a prioritized way. The Administrator has the lowest priority. Other software modules are prioritized according to their position in the drop-down list: the higher in the list, the higher priority. If Conflicts exist, it displays as "Yes" for the "Combined" users and the offending software module. The "Combined" user reflects what is configured in hardware.

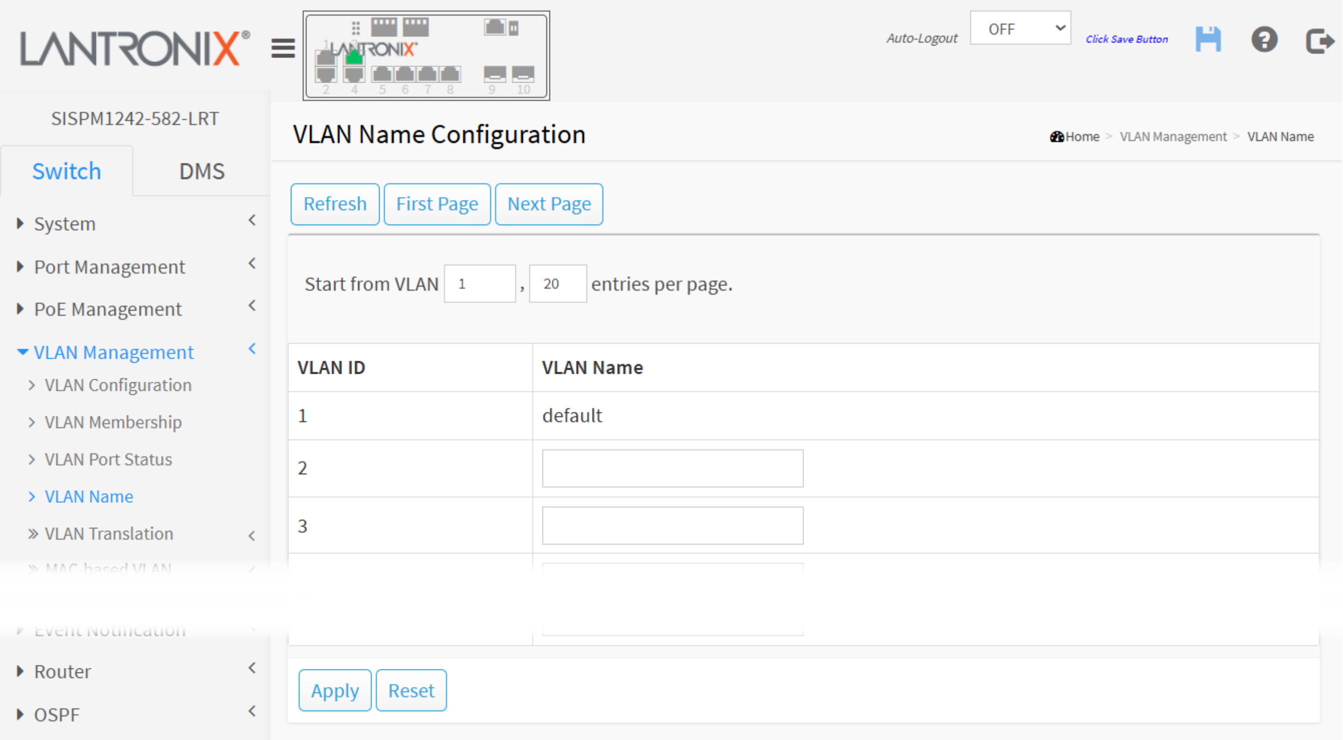
VLAN Name

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

Navigating the VLAN Name configuration table

Each page shows up to 99 entries from the VLAN Name Configuration Table, the 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 Name Configuration Table.

The "*Start from VLAN*" input field lets you select the starting point in the VLAN Name Configuration table. Clicking the **Refresh** button will update the displayed table starting from that or the closest next VLAN Name Configuration Table match. 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.



VLAN Name Configuration

Start from VLAN 1 , 20 entries per page.

VLAN ID	VLAN Name
1	default
2	
3	

Parameter descriptions:

VLAN ID : Displays a VID for each line in the table.

VLAN Name : Enter a Name for each VLAN ID.

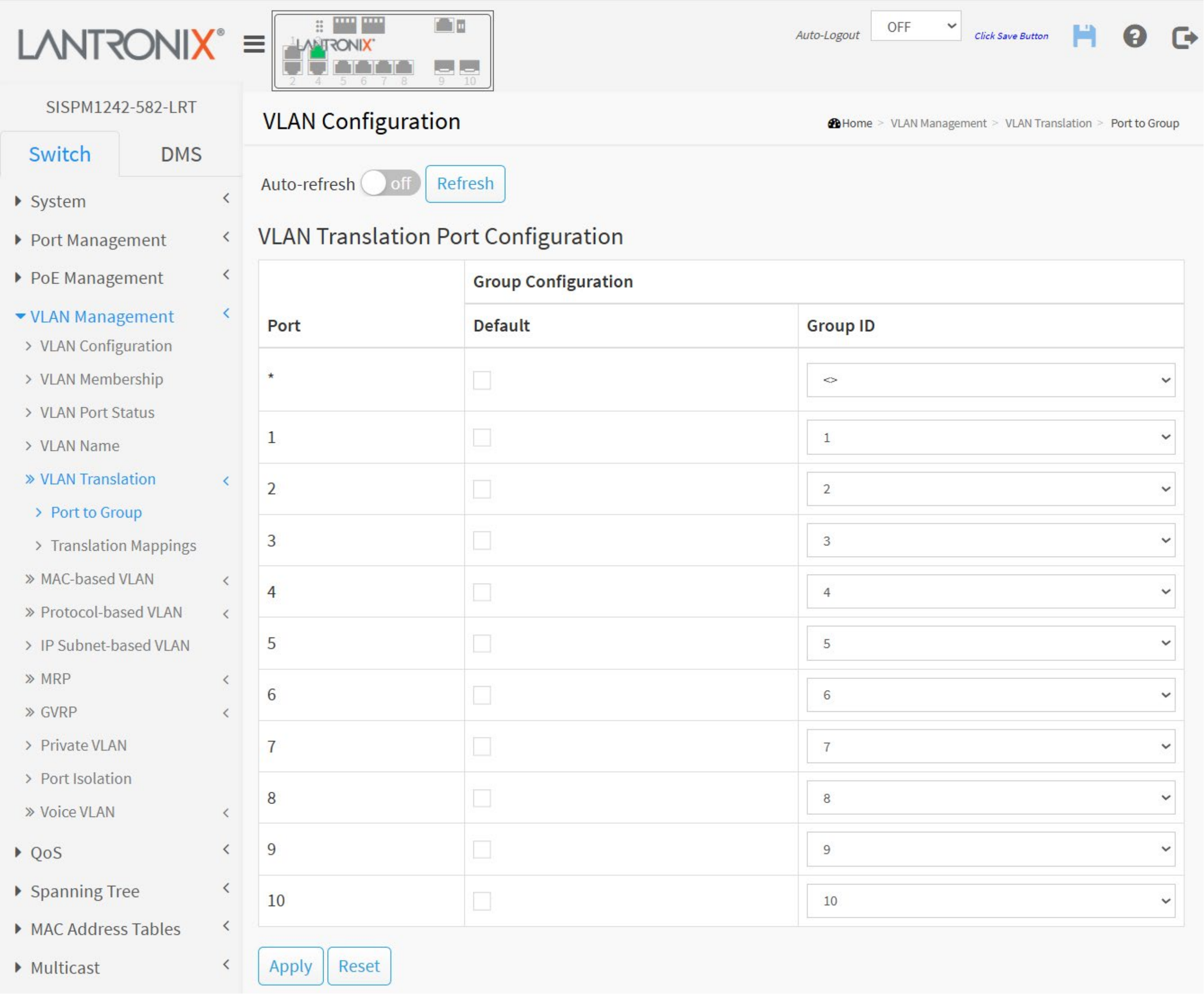
VLAN Translation

Port to Group

This page lets you configure switch Ports to use a given VLAN Translation Mapping Group. This will enable all VLAN Translation mappings of that group (if any) on the selected switch port.

To configure VLAN Translation Port to Group:

1. Go to VLAN Management > VLAN Translation > Port to Group.
2. Configure the settings for your requirement.
3. Click **Apply** to save the changes.



VLAN Translation Port Configuration

Port	Group Configuration	
	Default	Group ID
*	□	<>
1	□	1
2	□	2
3	□	3
4	□	4
5	□	5
6	□	6
7	□	7
8	□	8
9	□	9
10	□	10

Parameter descriptions:

Port : The Port column shows the list of ports for which you can configure the VLAN Translation Mapping Group.

Default : To set the switch port to use the default VLAN Translation Group click the checkbox and press Save.

Group ID : The VLAN Translation mappings are organized into Groups, identified by the Group ID. This way a port is configured to use several VLAN Translation mappings easily by simply configuring it to use a given group. Then number of possible groups in a switch is equal to the number of ports present in this switch. A port can be configured to use any of the groups, but only one at any given time. Multiple ports can be configured to use the same group. A valid Group ID is an integer value from 1 to 14.

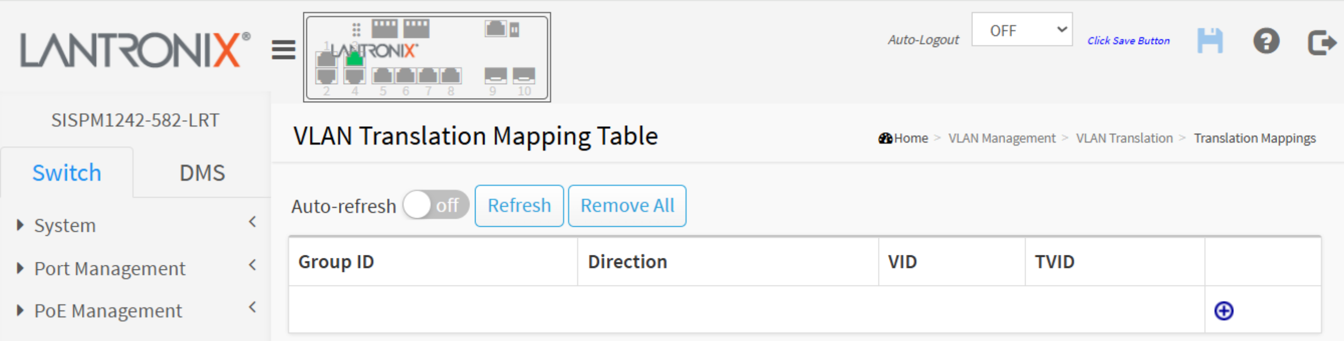
Note: By default, each port is set to use the group with Group ID equal to the port number. For example, port #1 is by default set to use group with GID = 1.

Translation Mappings

This page allows you to create mappings of VLANs > Translated VLANs and organize these mappings into global Groups.

To configure VLAN Translation mappings:

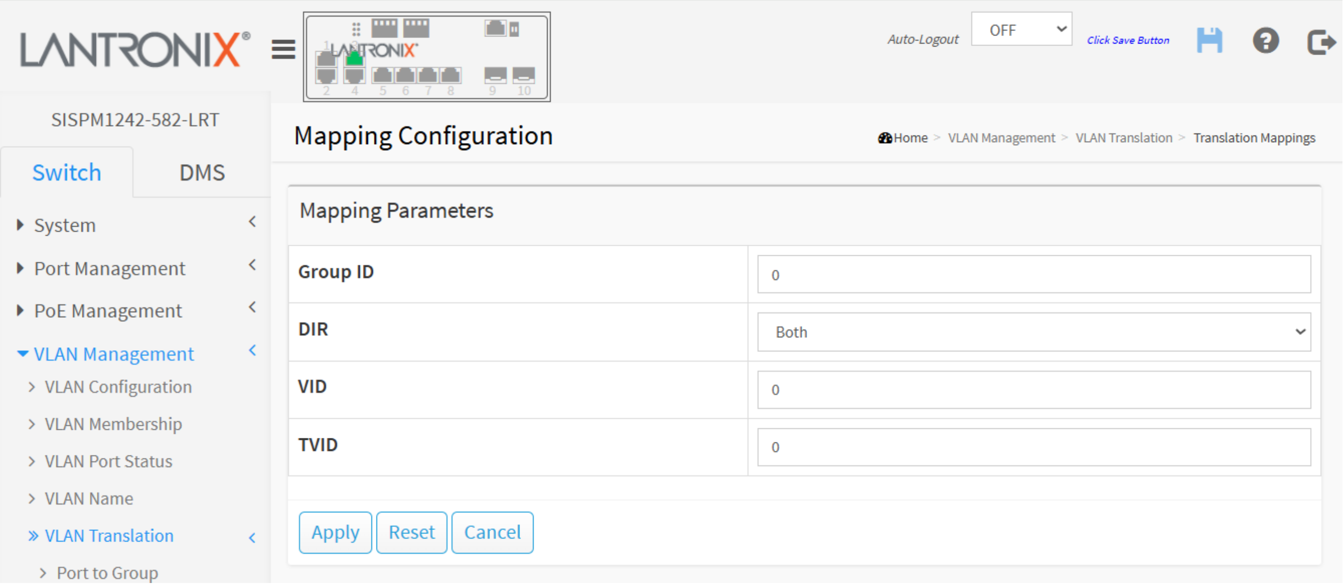
1. Go to VLAN Management > VLAN Translation > Translation Mappings.
2. Click the ⊕ icon to display the mapping parameters.
3. Configure the settings for your requirement.
4. Click **Apply** to save the changes.



VLAN Translation Mapping Table

Group ID	Direction	VID	TVID	
				⊕

↓↓↓↓↓



Mapping Configuration

Mapping Parameters

Group ID	0
DIR	Both
VID	0
TVID	0

Parameter descriptions:

Group ID : The VLAN Translation mappings are organized into Groups, identified by the Group ID. This way a port is configured to use several VLAN Translation mappings easily by simply configuring it to use a given group. Then number of possible groups in a switch is equal to the number of ports present in this switch. A port can be configured to use any of the groups, but only one at any given time. Multiple ports can be configured to use the same group. A valid Group ID is an integer value from 1 to 10.

Note: By default, each port is set to use the group with Group ID equal to the port number. For example, port #1 is by default set to use group with GID = 1.

DIR (Direction) : Indicates the direction of the VLAN Translation and it refers to the switch. The direction can be '***Ingress***', where the translation takes place on the VLAN ID of frames entering the switch port, '***Egress***', where the translation takes place on the VLAN ID of frames exiting the switch port, or '***Both***', where the translation takes place on both the above directions.

VID : Indicates the VLAN ID of the mapping (i.e. 'source' VLAN). A valid VLAN ID ranges from 1 to 4095.

TVID : Indicates the translated VLAN ID to which a VLAN ID of a frame will be translated to. A valid translated VLAN ID ranges from 1 to 4095.

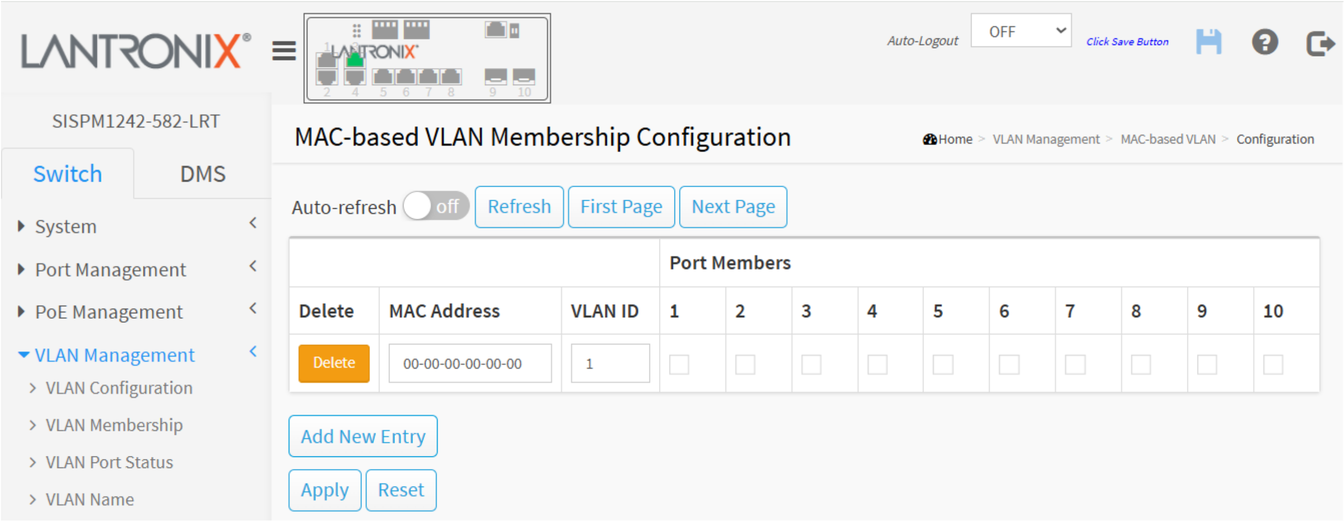
MAC-Based VLAN

Configuration

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

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

1. Go to VLAN Management > MAC-based VLAN > Configuration.
2. Click **Add New Entry**.
3. Specify the MAC address and VLAN ID.
4. Click the desired Port Members checkboxes.
5. Click **Apply**.



MAC-based VLAN Membership Configuration

			Port Members									
Delete	MAC Address	VLAN ID	1	2	3	4	5	6	7	8	9	10
Delete	00-00-00-00-00-00	1	□	□	□	□	□	□	□	□	□	□

Parameter descriptions:

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: Used to delete a MAC to VLAN ID mapping entry. Check this box and click **Apply**.

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.

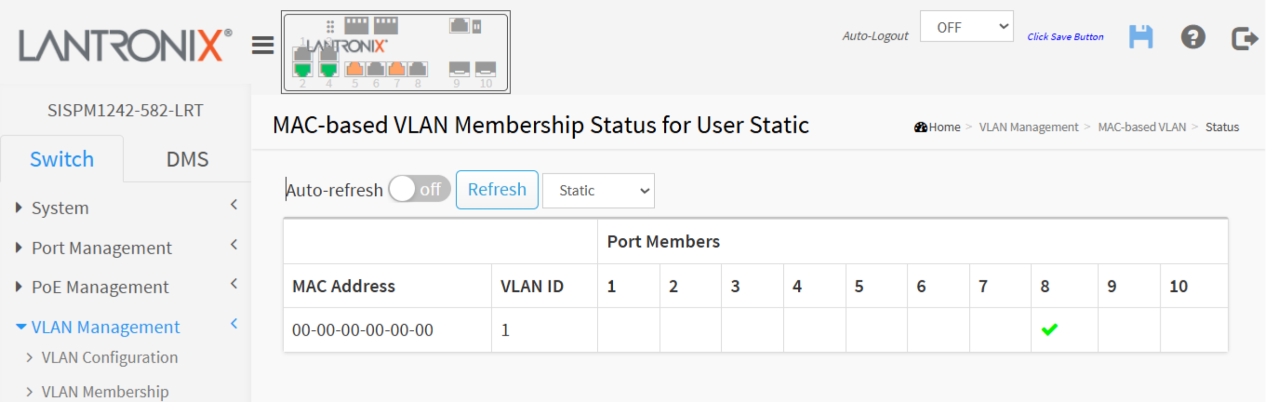
Status

This page shows the MAC-based VLAN membership status.

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

1. Go to VLAN Management > MAC-based VLAN > Status.
2. At the dropdown select the desired User.

3. **Auto-refresh** will refresh the page every 3 seconds. **Refresh** will refresh the page immediately.



MAC-based VLAN Membership Status for User Static

		Port Members									
MAC Address	VLAN ID	1	2	3	4	5	6	7	8	9	10
00-00-00-00-00-00	1								✓		

Parameter descriptions:

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

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

MAC Address : Indicates the MAC address.

VLAN ID : Indicates the VLAN ID.

Port Members : Port members of the MAC-based VLAN entry are indicated by a green checkmark.

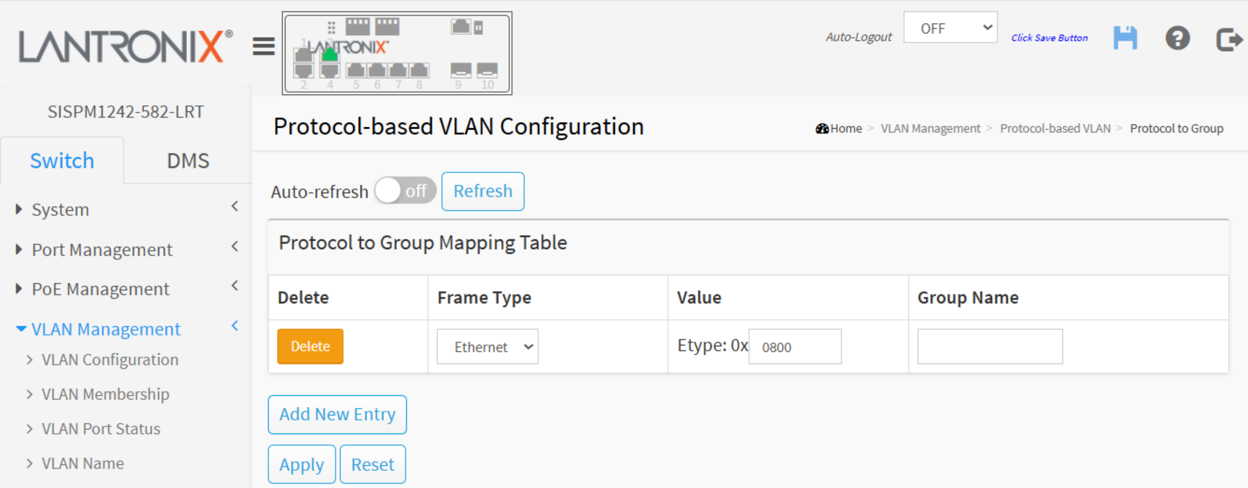
Protocol-Based VLAN

Protocol to Group

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

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

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



Protocol-based VLAN Configuration

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

Protocol to Group Mapping Table

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

Parameter descriptions :

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

Frame Type : At the dropdown select 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. The criteria for three different Frame Types:

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

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

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

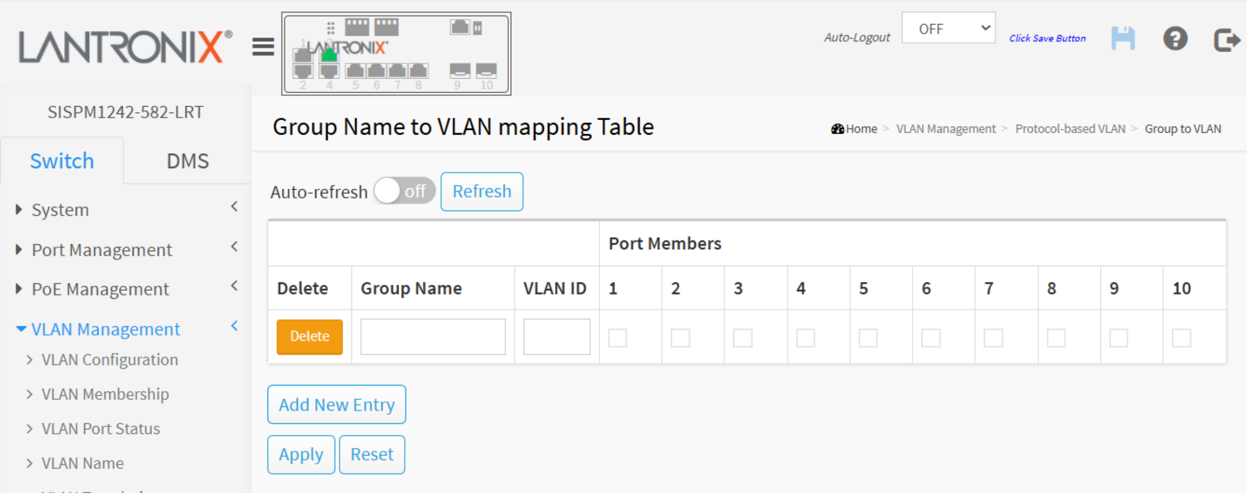
Group Name : A valid Group Name is a unique 16-character string.

Group to VLAN

This page lets you map an already configured Group Name to a VLAN for the switch.

To configure Group Name to VLAN mapping in the web UI:

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



Group Name to VLAN mapping Table

			Port Members									
Delete	Group Name	VLAN ID	1	2	3	4	5	6	7	8	9	10
Delete			□	□	□	□	□	□	□	□	□	□

Parameter descriptions:

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.

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

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

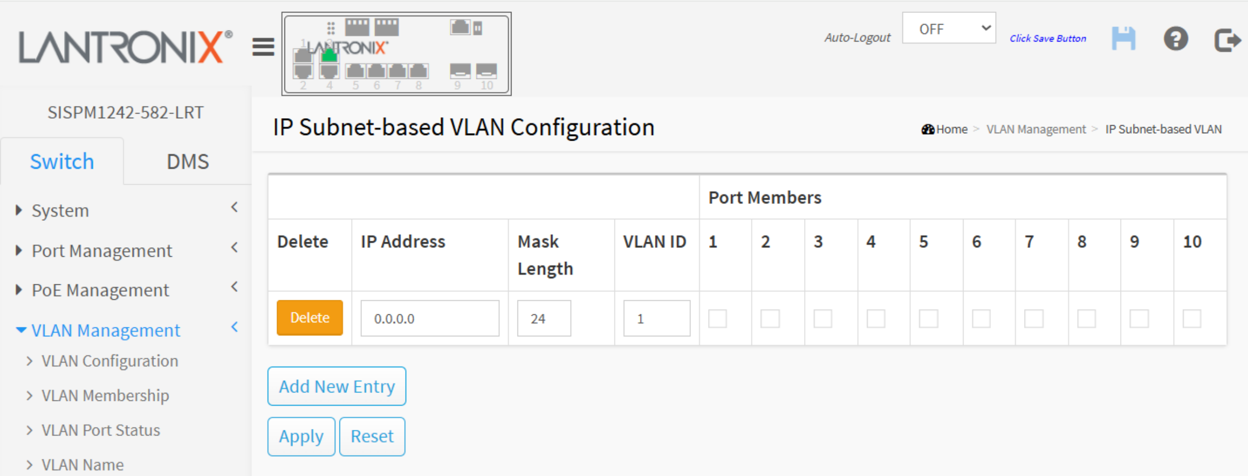
Port Members : A row of check boxes for each port is displayed for each Group Name to VLAN ID mapping.
To include a port in a mapping, check the box. To remove or exclude the port from the mapping, make sure the box is unchecked. By default, no ports are members, and all boxes are unchecked.

IP Subnet-Based VLAN

This page lets you add, update and delete IP subnet-based VLAN entries.

To configure IP subnet-based VLAN Membership in the web UI:

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



IP Subnet-based VLAN Configuration

				Port Members									
Delete	IP Address	Mask Length	VLAN ID	1	2	3	4	5	6	7	8	9	10
Delete	0.0.0.0	24	1	□	□	□	□	□	□	□	□	□	□

Parameter descriptions:

Add New Entry : Click to add a new IP subnet-based VLAN entry. An empty row is added to the table, and the IP subnet-based VLAN entry can be configured as needed. Any IP address/mask can be configured for the IP subnet-based VLAN entry. Legal values for a VLAN ID are 1 - 4095. The "Delete" button can be used to undo the addition of new IP subnet-based VLANs. The maximum possible IP subnet-based VLAN entries is limited to 128.

IP Address : Enter the IP address.

Mask Length : Enter the network mask length.

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

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

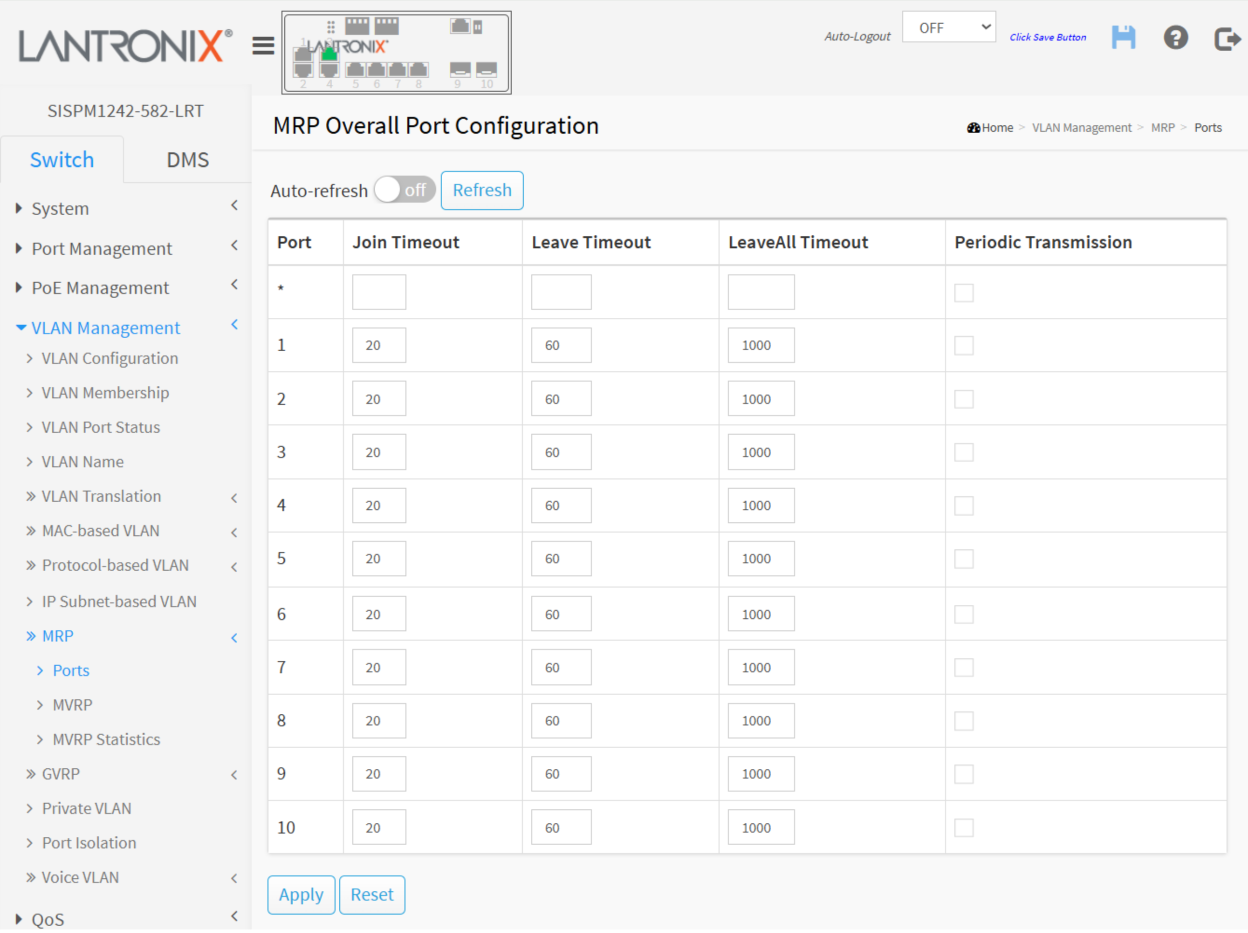
MRP

Multiple Registration Protocol is a generic registration framework that defines the dynamic registration and de-registration of attributes across a Bridged Local Area Network. Such attributes could be for example VLAN identifiers or multicast group MAC addresses. The standard was originally defined by IEEE 802.1ak, and its latest incorporation is in IEEE 802.1Q-2014.

Ports

To configure MRP:

1. Go to VLAN Management > MRP > Ports to display the MRP Overall Port Configuration page.
2. Configure MRP overall settings.



MRP Overall Port Configuration

Port	Join Timeout	Leave Timeout	LeaveAll Timeout	Periodic Transmission
*				□
1	20	60	1000	□
2	20	60	1000	□
3	20	60	1000	□
4	20	60	1000	□
5	20	60	1000	□
6	20	60	1000	□
7	20	60	1000	□
8	20	60	1000	□
9	20	60	1000	□
10	20	60	1000	□

Parameter descriptions:

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

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

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

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

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

About MRP Timers

MRP uses the following timers to control message transmission:

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

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

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

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

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

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

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

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

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

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

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

MMRP Attribute Types

MMRP Defines two attribute types:

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

Two types of service requirements are supported:

- All Groups must be encoded as the value 0. Forward all Multicast is used to support legacy devices that do not support MMRP/GMRP.

- All Unregistered Groups must be encoded as the value 1. Flood unregistered multicast traffic and other traffic is pruned by MMRP.
- The remaining possible values (2 - 255) are reserved.

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

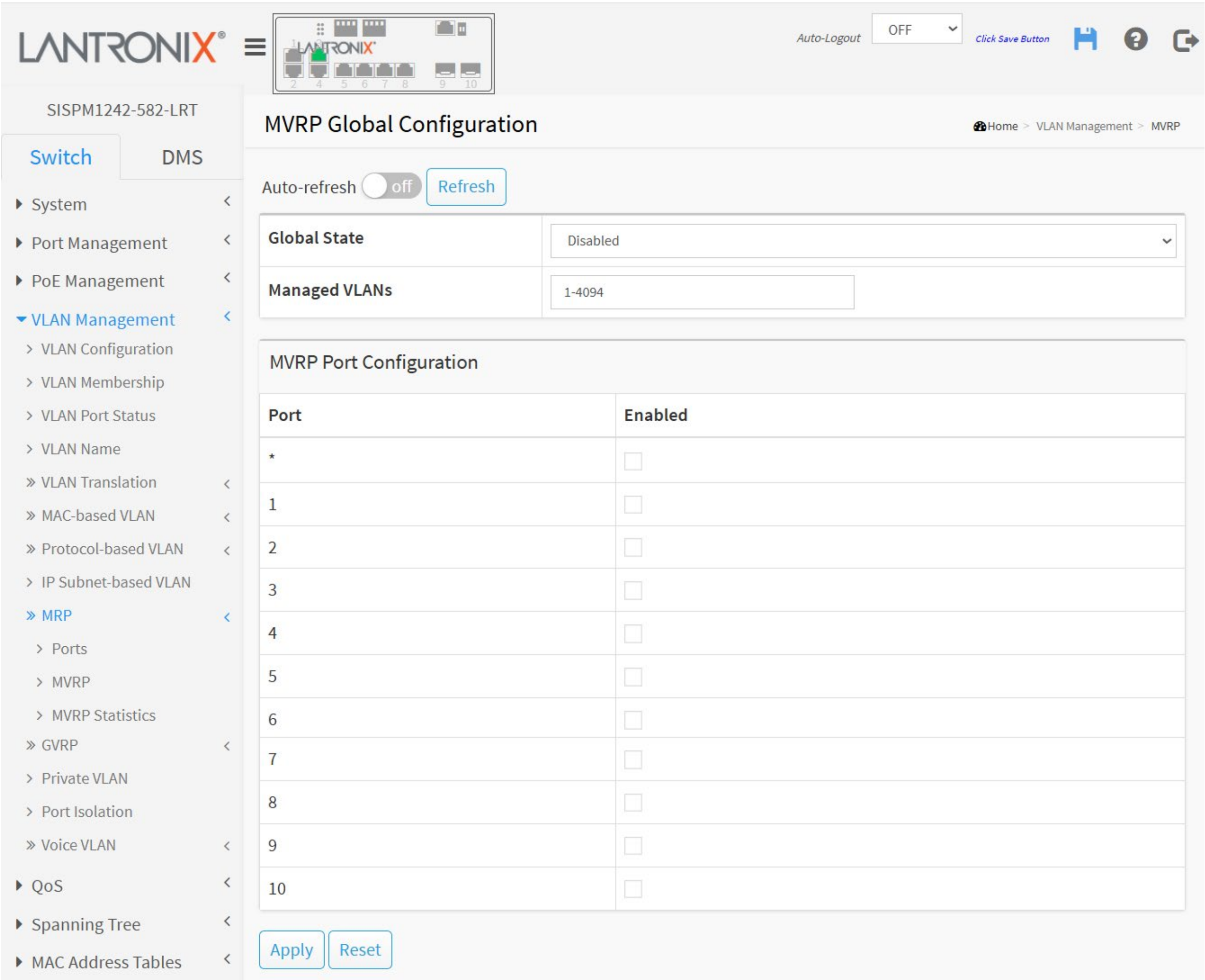
MVRP Configuration

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

This page allows you to configure the MVRP global and per port settings.

To configure MVRP settings:

1. Go to VLAN Management > MRP > MVRP.
2. Configure the settings.
3. Click **Apply** to save the changes.



MVRP Global Configuration

Global State	Disabled
Managed VLANs	1-4094

MVRP Port Configuration

Port	Enabled
*	□
1	□
2	□
3	□
4	□
5	□
6	□
7	□
8	□
9	□
10	□

Parameter Descriptions

MVRP Global Configuration

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

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

MVRP Port Configuration

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

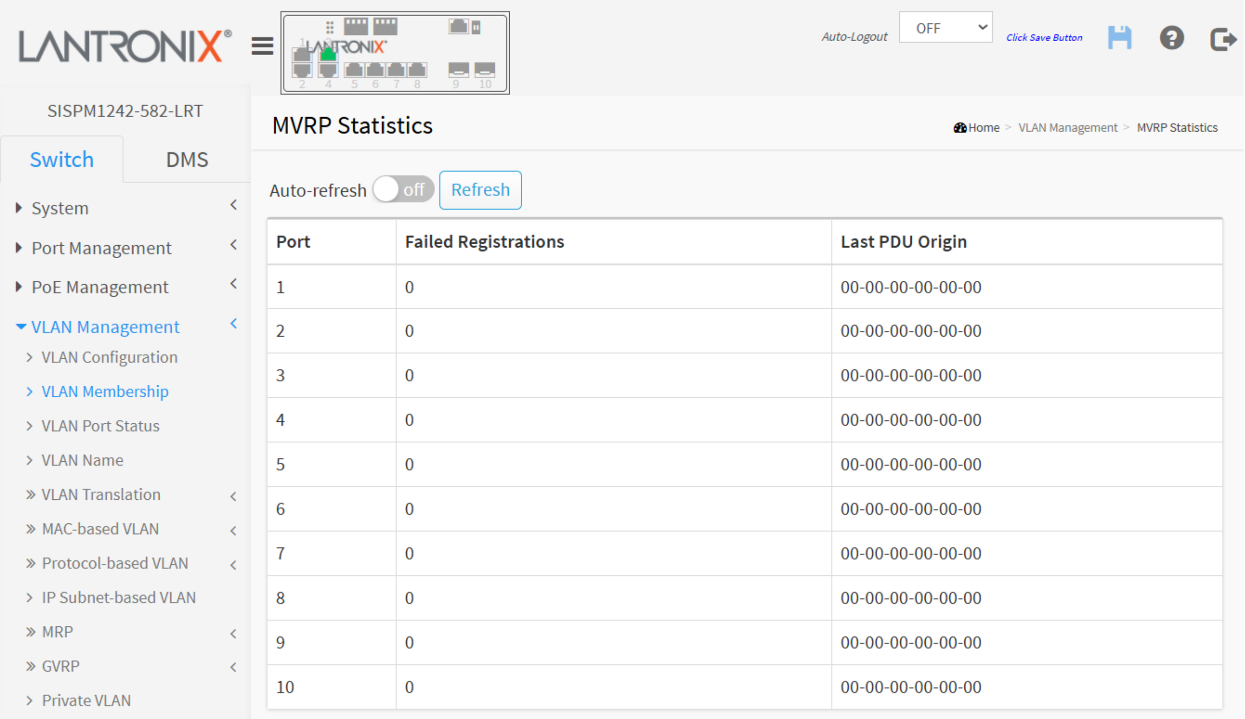
Enabled: Enable or disable the MVRP protocol on this switch port. This will enable or disable the protocol on the switch port given that MVRP is also globally enabled.

MVRP Statistics

This page provides statistics for the MVRP protocol for all switch ports.

To view MVRP statistics:

1. Go to VLAN Management > MRP > MVRP Statistics.
2. **Auto-refresh** will refresh the page every 3 seconds. **Refresh** will refresh the page immediately.



MVRP Statistics

Port	Failed Registrations	Last PDU Origin
1	0	00-00-00-00-00-00
2	0	00-00-00-00-00-00
3	0	00-00-00-00-00-00
4	0	00-00-00-00-00-00
5	0	00-00-00-00-00-00
6	0	00-00-00-00-00-00
7	0	00-00-00-00-00-00
8	0	00-00-00-00-00-00
9	0	00-00-00-00-00-00
10	0	00-00-00-00-00-00

Parameter Descriptions

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

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

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

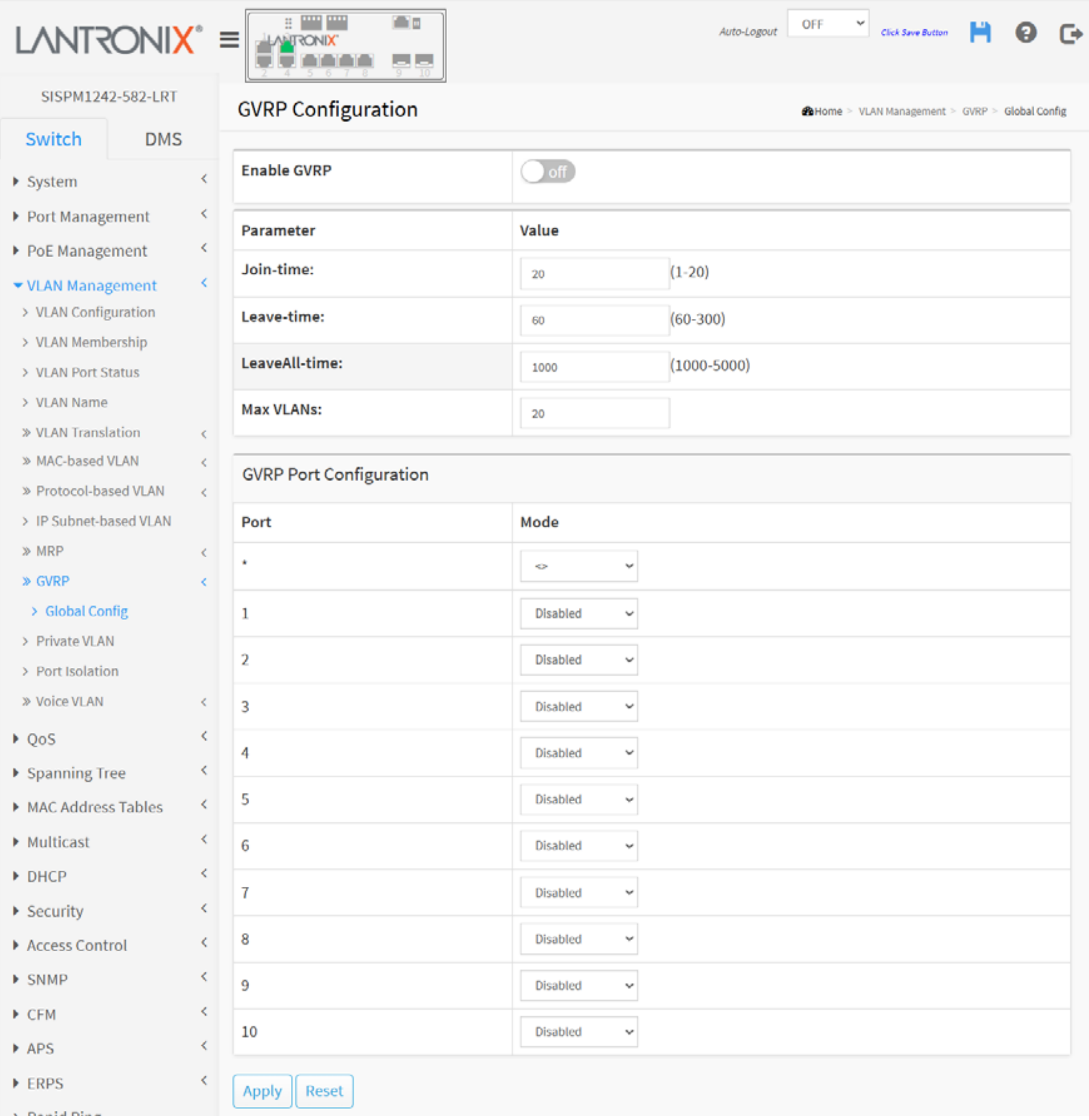
GVRP

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

Global Config

To configure GVRP in the web UI:

1. Go to VLAN Management > GVRP.
2. Enable GVRP.
3. Specify GVRP protocol timers and Max VLANs.
4. Enable or disable the Mode for each port as desired.
5. Click **Apply** to save the changes.



GVRP Configuration

Enable GVRP	off

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

GVRP Port Configuration

Port	Mode
*	<>
1	Disabled
2	Disabled
3	Disabled
4	Disabled
5	Disabled
6	Disabled
7	Disabled
8	Disabled
9	Disabled
10	Disabled

Apply Reset

Parameter descriptions :

Enable GVRP: The GVRP feature is enabled globally by setting Enable GVRP to on.

GVRP Protocol timers

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

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

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

Max VLANs : When GVRP is enabled a maximum number of VLANs supported by GVRP is specified. The default is 20. This number can only be changed when GVRP is Disabled.

<u>GVRP Port Configuration</u>

This configuration can be performed either before or after GVRP is configured globally - the protocol operation will be the same.

Port : The Port column shows the list of ports.

Mode : Enable/disable GVRP Mode on port locally:

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

Enabled: Select to Enable GVRP mode on this port.

Private VLAN

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

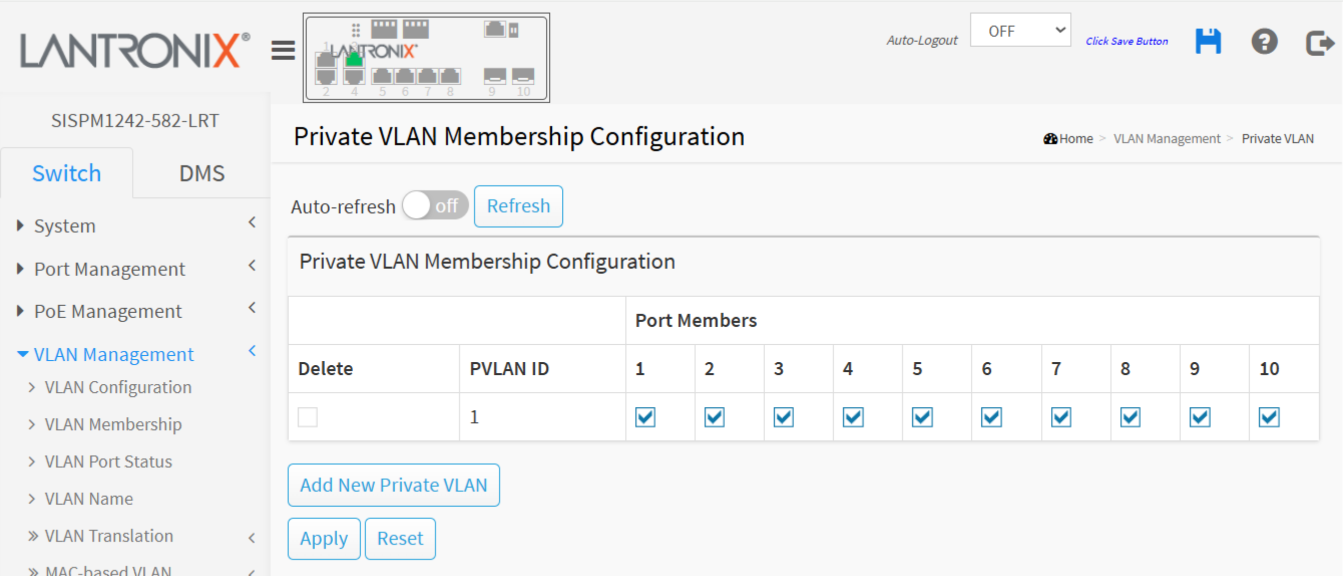
Private VLANs are based on the source port mask, and there are no connections to VLANs. This means that VLAN IDs (VIDs) and Private VLAN IDs (PVIDs) can be identical.

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

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

To configure Private VLAN Membership in the web UI:

1. Go to VLAN Management > Private VLAN.
2. Click the Add New Private VLAN button to add a new private VLAN ID to the table.
3. Select the ports to be included in the private VLAN.
4. Click **Apply**.



Auto-Logout: OFF

Private VLAN Membership Configuration

Auto-refresh: off

Private VLAN Membership Configuration

		Port Members									
Delete	PVLAN ID	1	2	3	4	5	6	7	8	9	10
□	1	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑

Parameter descriptions :

Add New Private VLAN : Click to add a new private VLAN ID. An empty row is added to the table, and the private VLAN can be configured as needed. The valid range for a private VLAN ID is the same as the switch port number range. Any values outside this range are not accepted, and a warning message appears. Click "OK" to discard the incorrect entry or click "Cancel" to return to the editing and make a correction. The Private VLAN is enabled when you click **Apply**. The Reset button can be used to undo the addition of new Private VLANs.

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

PVLAN ID : Indicates the ID of this private VLAN.

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

Port Isolation

This page is used to enable or disable port isolation on ports in a Private VLAN. A port member of a VLAN can be isolated to other isolated ports on the same VLAN and Private VLAN.

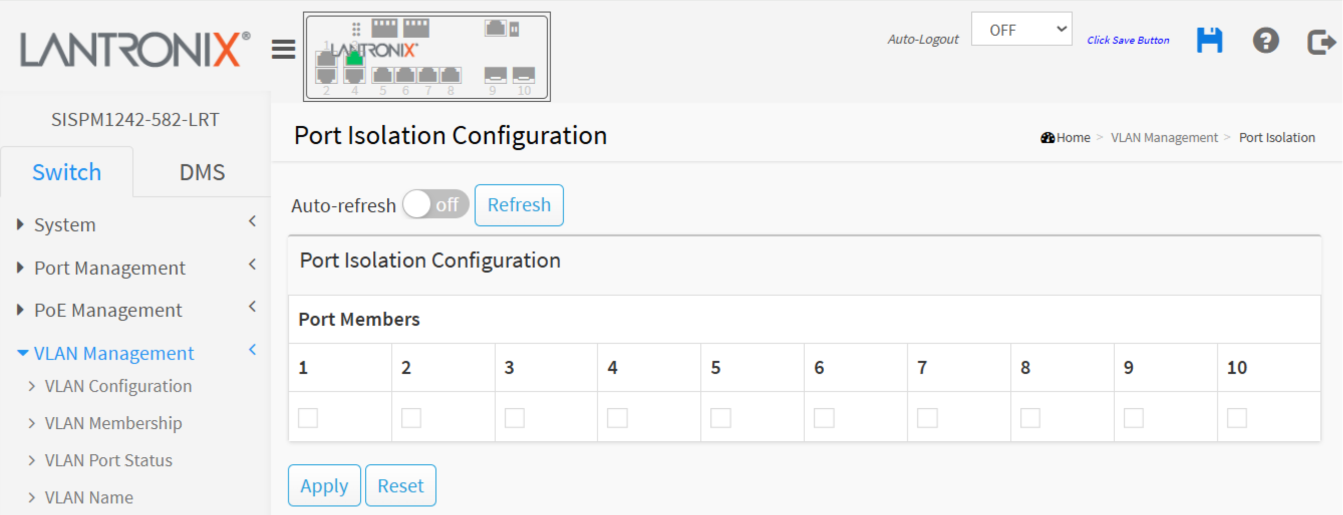
Port Isolation provides an apparatus and a method to isolate ports on layer 2 switches on the same VLAN to restrict traffic flow. The apparatus comprises a switch having said plurality of ports, each port configured as a protected port or a non-protected port. An address table memory stores an address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

To configure Port Isolation in the web UI:

1. Go to VLAN Management > Port Isolation.

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

3. Click **Apply**.



Auto-Logout: OFF

Port Isolation Configuration

Auto-refresh: off

Port Isolation Configuration

Port Members									
1	2	3	4	5	6	7	8	9	10
□	□	□	□	□	□	□	□	□	□

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.

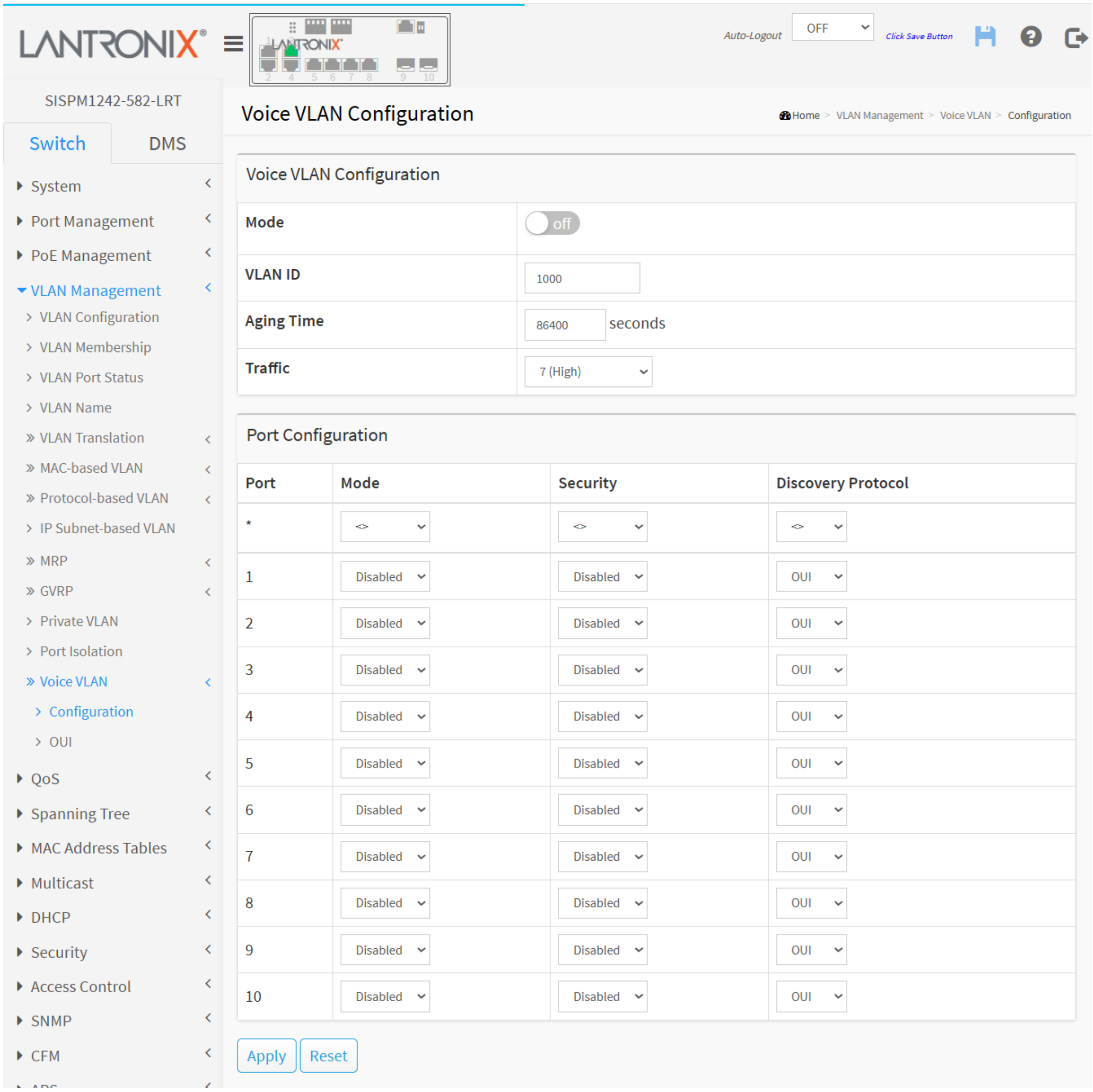
Voice VLAN

Configuration

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

To configure Voice VLAN in the web UI:

1. Go to VLAN Management > Voice VLAN > Configuration.
2. Set Mode to “on” in the Voice VLAN Configuration section.
3. Configure the other Voice VLAN Configuration settings.
4. Configure Port Members in the Port Configuration section.
5. Click the **Apply** button to save the settings.



Voice VLAN Configuration

Voice VLAN Configuration

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

Port Configuration

Port	Mode	Security	Discovery Protocol
*	<>	<>	<>
1	Disabled	Disabled	OUI
2	Disabled	Disabled	OUI
3	Disabled	Disabled	OUI
4	Disabled	Disabled	OUI
5	Disabled	Disabled	OUI
6	Disabled	Disabled	OUI
7	Disabled	Disabled	OUI
8	Disabled	Disabled	OUI
9	Disabled	Disabled	OUI
10	Disabled	Disabled	OUI

Parameter descriptions :

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

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

VLAN ID : Enter the Voice VLAN ID. It should be a unique VLAN ID in the system and cannot equal each port PVID. It is a conflict in configuration if the value equals management VID, MVR VID, PVID, etc. The valid range is 1 to 4095.

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

Traffic : Select the Voice VLAN traffic class. All traffic on the Voice VLAN will apply this class. At the dropdown select a value of 7 (High priority) to 0 (Low priority).

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

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

- ***Disabled*** : Disjoin from Voice VLAN (default).
- ***Auto*** : Enable auto detect mode. It detects whether there is VoIP phone attached to the specific port and configures the Voice VLAN members automatically.
- ***Forced*** : Force join to Voice VLAN.
  This field will be read only if the STP feature is enabled. The STP Port mode will be read only if this field be set to a mode other than Disabled.

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

- ***Enabled***: Enable Voice VLAN security mode operation.
- ***Disabled***: Disable Voice VLAN security mode operation (default).

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

- ***OUI***: Detect telephony device by OUI address.
- ***LLDP***: Detect telephony device by LLDP.
- ***Both***: Detect telephony device by both OUI and LLDP.

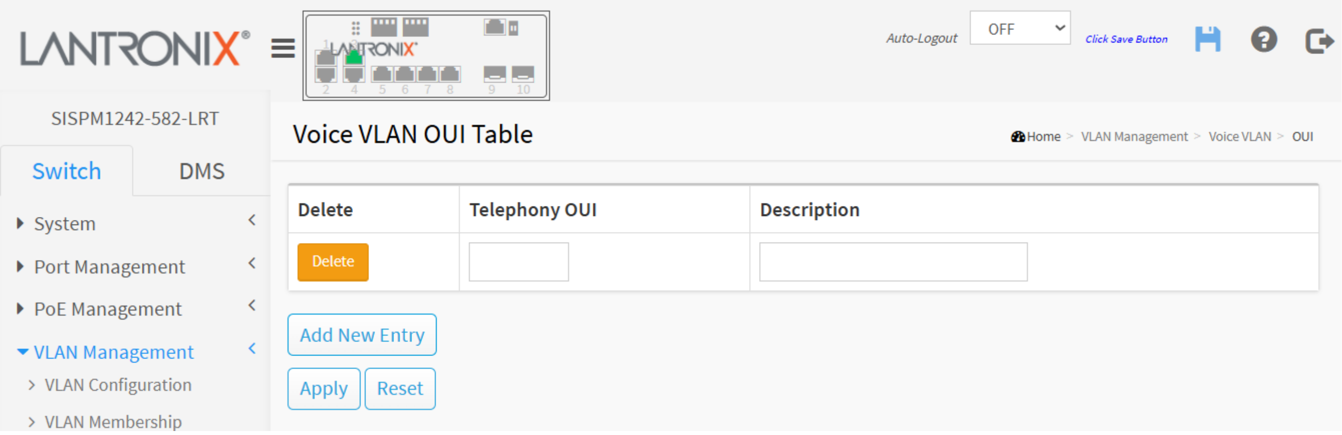
OUI

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

To configure Voice VLAN OUI in the web UI:

1. Go to VLAN Management > Voice VLAN > OUI.
2. Click the **Add New Entry** button.

3. Specify Telephony OUI and Description.
4. Click **Apply**.



Voice VLAN OUI Table

Delete	Telephony OUI	Description
Delete		

Parameter descriptions :

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

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

Telephony OUI : A telephony OUI address is a global organizationally unique identifier assigned to a vendor by the IEEE. It must be 6 characters long and the input format is "xx-xx-xx" (where x is a hexadecimal digit).
For example, 00-01-e3 = Siemens AG Phone, 00-09-6e = Avaya.

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.

7. QoS

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

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

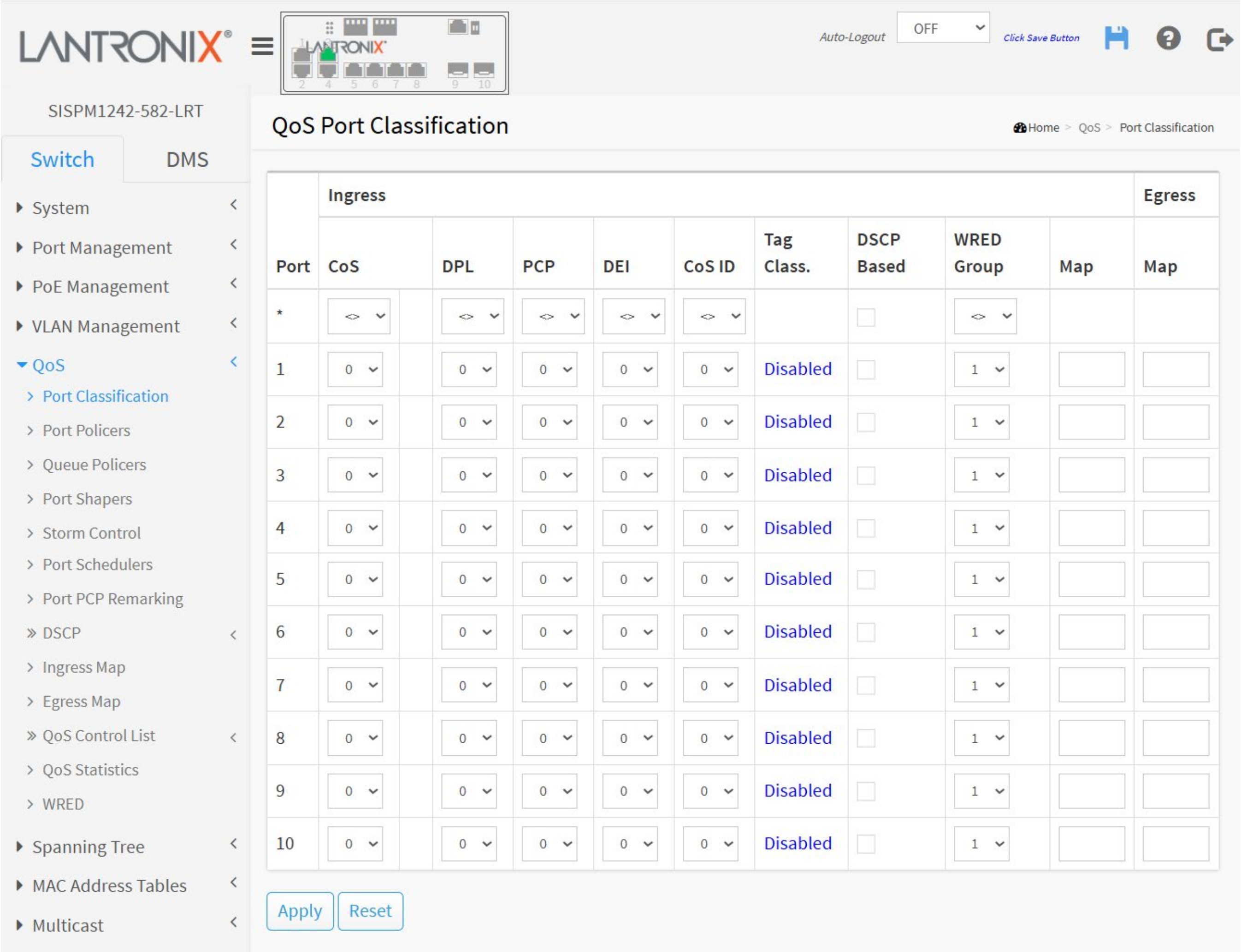
The switch supports advanced memory control mechanisms providing excellent performance of all QoS classes under any traffic scenario, including jumbo frames. The switch provides superior priority queueing with dedicated memory and strict highest-priority arbitration. The ingress super priority queue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

Port Classification

This page lets you configure basic QoS ingress port classification settings for all switch ports.

To configure QoS port classification in the web UI:

1. Go to Quality of Service > Port Classification.
2. Scroll to select QoS Ingress Port parameters.
3. Click **Apply** to save the settings.
4. Click the link under Tag Class. to go to the port tag classification mapping.



QoS Port Classification

	Ingress									Egress
Port	CoS	DPL	PCP	DEI	CoS ID	Tag Class.	DSCP Based	WRED Group	Map	Map
*	<>	<>	<>	<>	<>		□	<>		
1	0	0	0	0	0	Disabled	□	1		
2	0	0	0	0	0	Disabled	□	1		
3	0	0	0	0	0	Disabled	□	1		
4	0	0	0	0	0	Disabled	□	1		
5	0	0	0	0	0	Disabled	□	1		
6	0	0	0	0	0	Disabled	□	1		
7	0	0	0	0	0	Disabled	□	1		
8	0	0	0	0	0	Disabled	□	1		
9	0	0	0	0	0	Disabled	□	1		
10	0	0	0	0	0	Disabled	□	1		

Parameter descriptions :

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

CoS : Select the default Class of Service (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 Classification is enabled, then the frame is classified to a CoS that is mapped from the PCP and DEI value in the tag. Otherwise, the frame is classified to the default CoS.

The classified CoS can be overruled by a QCL entry. The valid range is 0 (default) to 7 (highest priority).

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

DPL : Controls the default Drop Precedence Level (DPL). All frames are classified to a drop precedence level. If the port is VLAN aware, the frame is tagged and Tag Classification is enabled, then the frame is classified to a DPL that is mapped from the PCP and DEI value in the tag. Otherwise, the frame is classified to the default DPL.

The classified DPL can be overruled by a QCL entry.

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

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

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

Ingress Map: Controls the Ingress Map selection through the Map ID. The Ingress Map ID ranges from 0 to 127. An empty field indicates no map selection.

Egress Map: Controls the Egress Map selection through the Map ID. The Egress Map ID ranges from 0 to 255. An empty field indicates no map selection.

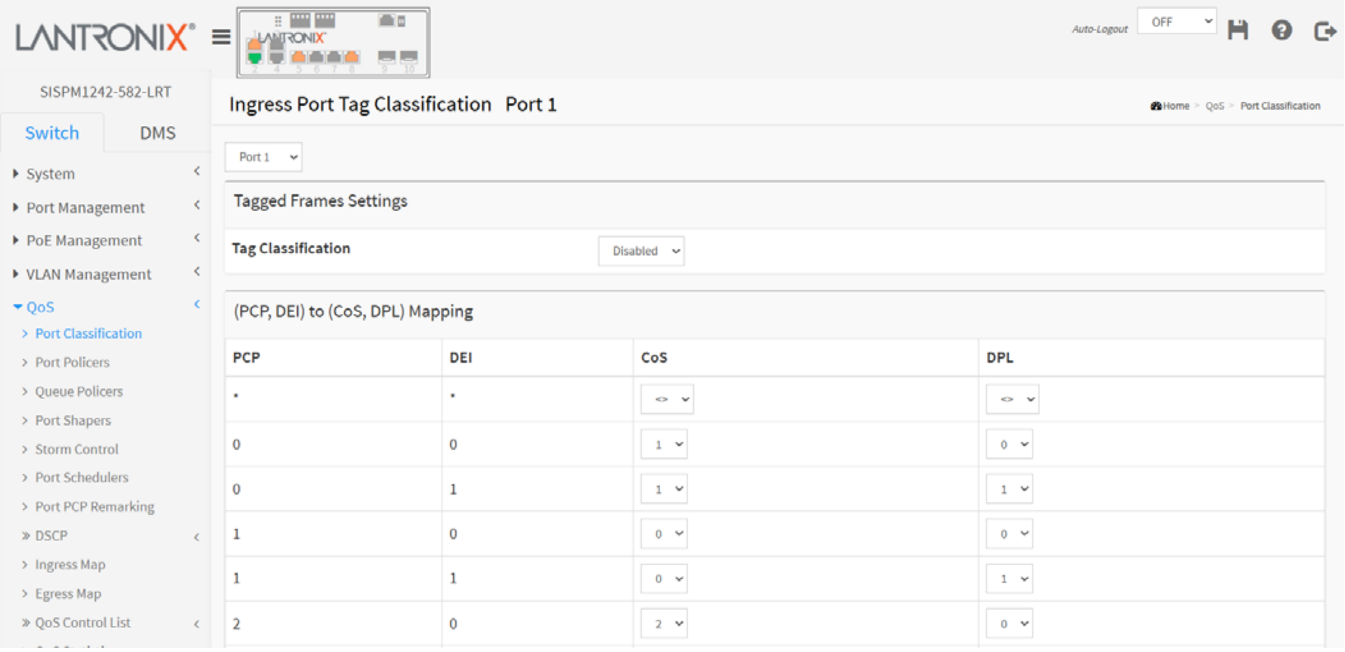
QoS Ingress Port Tag Classification Configuration

Click on the linked text under Tag Class. to configure the port tag classification 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.

Parameter Descriptions

Tag 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.



Ingress Port Tag Classification Port 1

Port 1

Tagged Frames Settings

Tag Classification: Disabled

(PCP, DEI) to (CoS, DPL) Mapping

PCP	DEI	CoS	DPL
*	*	<>	<>
0	0	1	0
0	1	1	1
1	0	0	0
1	1	0	1
2	0	2	0

Parameter descriptions :

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

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

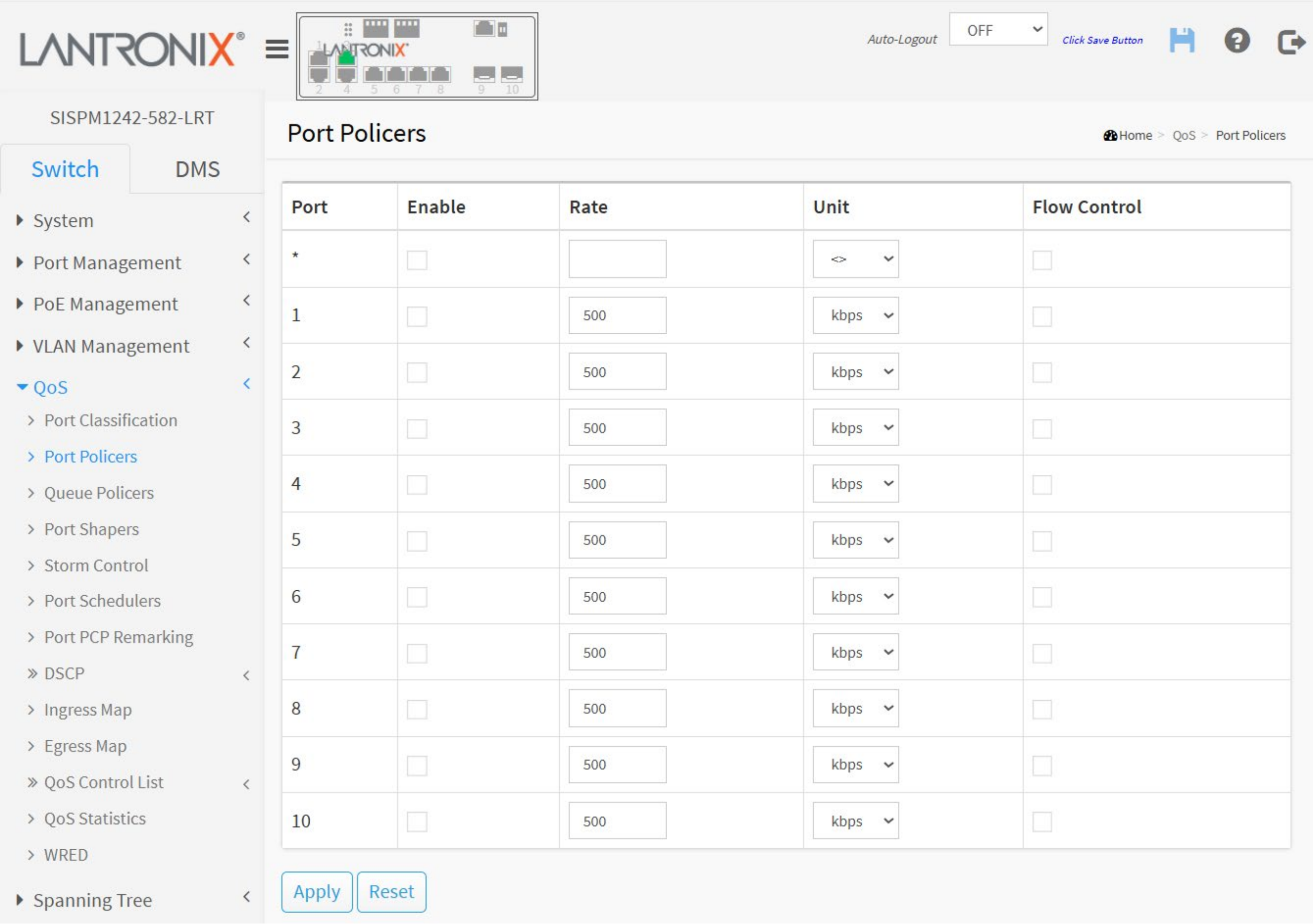
(PCP, DEI) to (Queue Priority, DPL level) Mapping : Controls the mapping of the classified (PCP, DEI) to (Queue Priority, DPL level) values when Tag Classification is set to Enabled.

Port Policers

This page lets you configure the policer settings for all switch ports. Port Policing is useful in constraining traffic flows and marking frames above specific rates. Policing is mainly used for data flows and voice or video flows because voice and video usually maintain a steady rate of traffic.

To configure QoS Port Policers in the web UI:

1. Go to Quality of Service > Port Policers.
2. Click on the port(s) on which you want to enable the QoS Ingress Port Policers.
3. Configure the Rate limit condition.
4. Select parameters for Rate, Unit, and Flow Control.
5. Click **Apply** to save the configuration.



Auto-Logout: OFF

Port Policers

Port	Enable	Rate	Unit	Flow Control
*	□		<>	□
1	□	500	kbps	□
2	□	500	kbps	□
3	□	500	kbps	□
4	□	500	kbps	□
5	□	500	kbps	□
6	□	500	kbps	□
7	□	500	kbps	□
8	□	500	kbps	□
9	□	500	kbps	□
10	□	500	kbps	□

Parameter descriptions:

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

Enable : Check the Port(s) you need to enable the QoS Ingress Port Policers function.

Rate : Set the Rate limit value for this port. The default is 1000000.

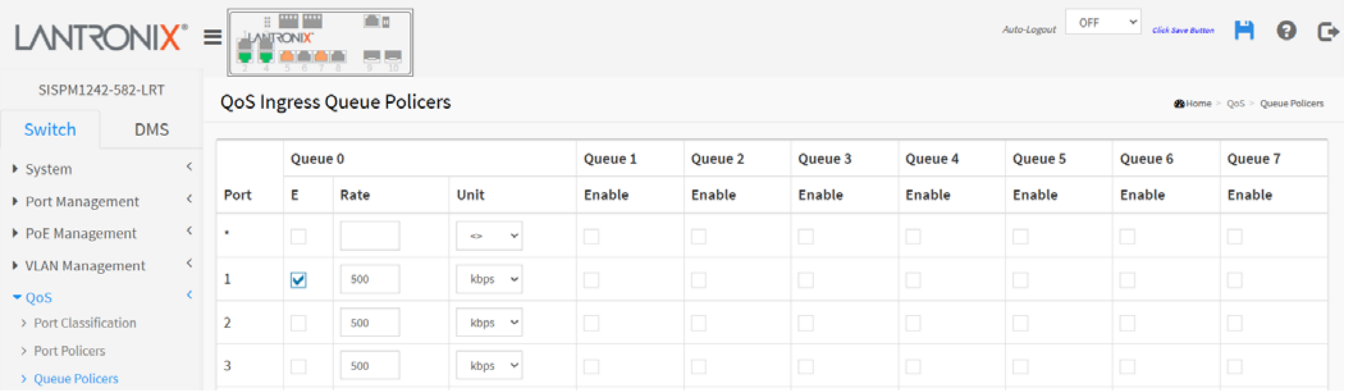
Unit : Controls the unit of measure for the port policer rate as kbps, Mbps, fps (frames per second), or kfps.

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

Queue Policers

To configure queue policers in the Web UI:

1. Go to QoS > Queue Policers to display the QoS Ingress Queue Policers page.
2. Check a box in the **Enable** column of a Queue to display its Rate and Unit of measure parameters.
3. Configure the Queue settings per your requirement.
4. Click **Apply** to save the configuration.



QoS Ingress Queue Policers

	Queue 0			Queue 1	Queue 2	Queue 3	Queue 4	Queue 5	Queue 6	Queue 7
Port	E	Rate	Unit	Enable	Enable	Enable	Enable	Enable	Enable	Enable
*	□		<>	□	□	□	□	□	□	□
1	☑	500	kbps	□	□	□	□	□	□	□
2	□	500	kbps	□	□	□	□	□	□	□
3	□	500	kbps	□	□	□	□	□	□	□

Parameter descriptions:

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

Queue 1 - Queue 7: Check the checkboxes for the queue(s) that you want enabled.

Enable: Enable or disable the queue policer for this switch port.

Rate: Controls the rate for the queue policer. This value is restricted to 25-13128147 when "Unit" is kbps, and 1-13128 when "Unit" is Mbps. The rate is internally rounded up to the nearest value supported by the queue policer. This field is only shown if at least one of the queue policers are enabled.

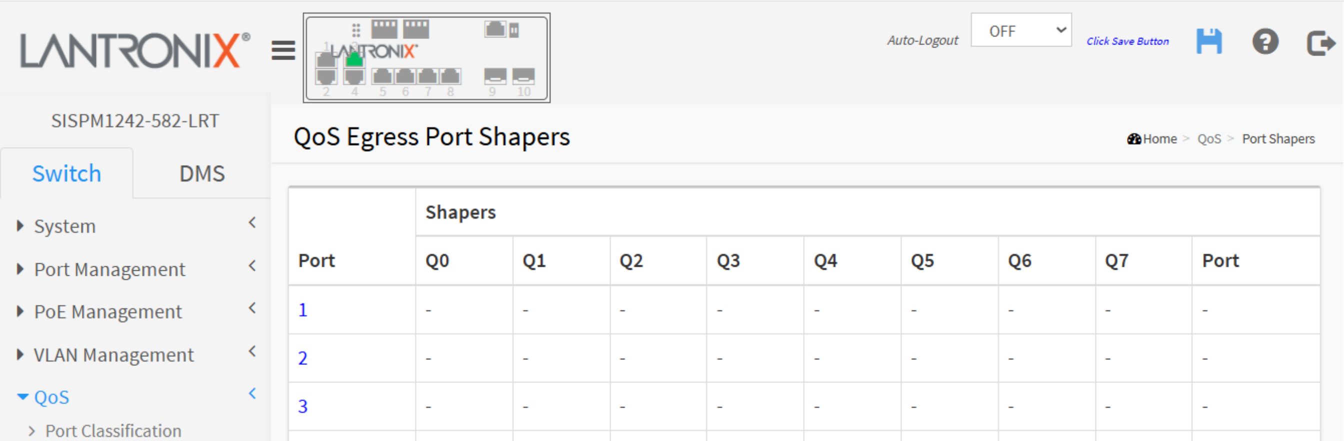
Unit: Controls the unit of measure for the queue policer rate as kbps or Mbps. This field displays only if at least one of the queue policers are enabled.

Port Shapers

This page lets you view and set the scheduler and shapers for all switch ports.

To configure QoS Port Shapers in the web UI:

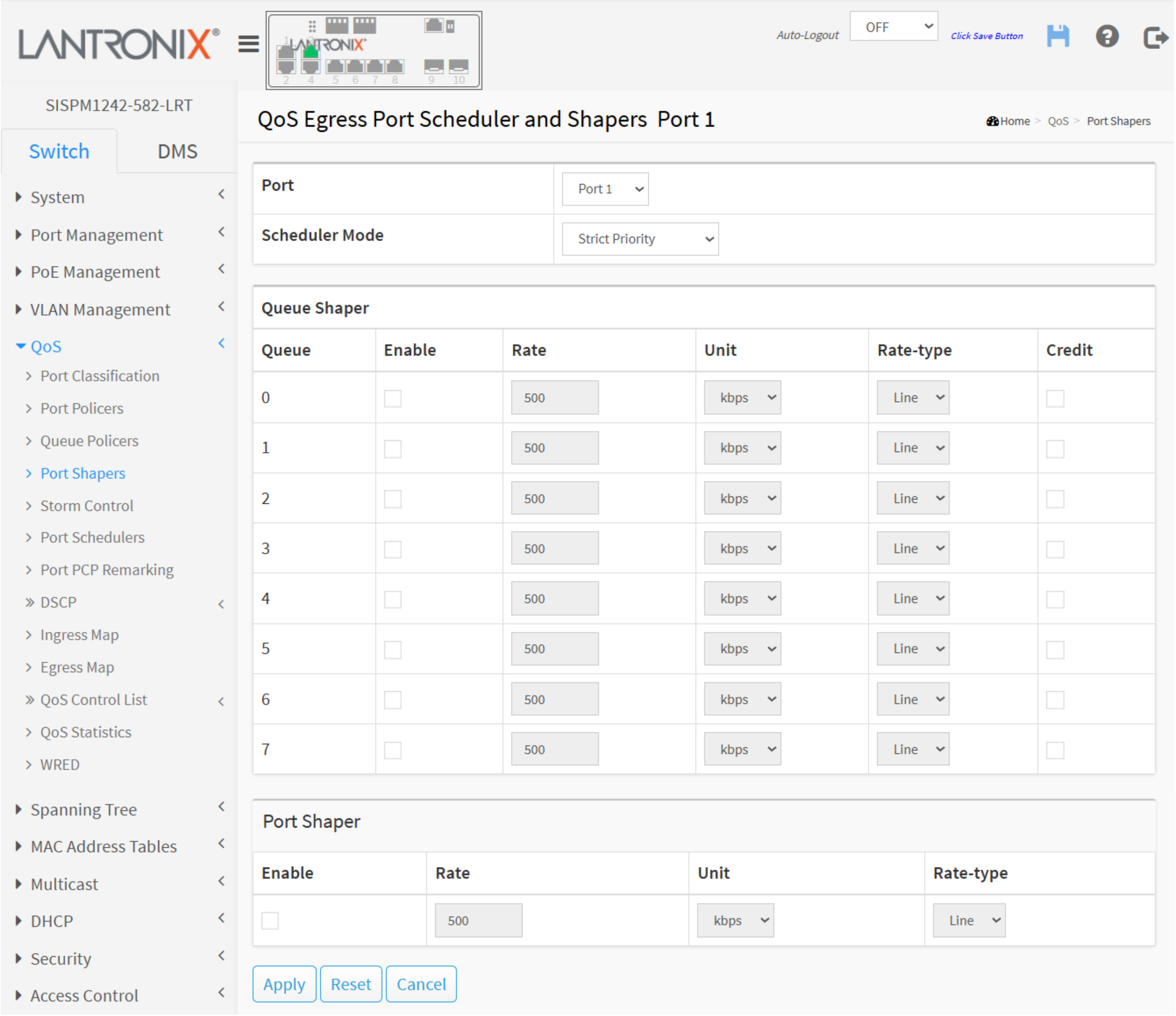
1. Go to QoS > Port Shapers to display the default QoS Egress Port Shapers page.



QoS Egress Port Shapers

Port	Shapers								
	Q0	Q1	Q2	Q3	Q4	Q5	Q6	Q7	Port
1	-	-	-	-	-	-	-	-	-
2	-	-	-	-	-	-	-	-	-
3	-	-	-	-	-	-	-	-	-

2. Click the linked text next to the desired Port to display the QoS Egress Port Scheduler and Shapers page.



QoS Egress Port Scheduler and Shapers Port 1

Port	Port 1
Scheduler Mode	Strict Priority

Queue Shaper

Queue	Enable	Rate	Unit	Rate-type	Credit
0	□	500	kbps	Line	□
1	□	500	kbps	Line	□
2	□	500	kbps	Line	□
3	□	500	kbps	Line	□
4	□	500	kbps	Line	□
5	□	500	kbps	Line	□
6	□	500	kbps	Line	□
7	□	500	kbps	Line	□

Port Shaper

Enable	Rate	Unit	Rate-type
□	500	kbps	Line

3. Select the port and scheduler mode. The Queue Shaper settings will display according to your selection.
4. Configure the queue shaper and port shaper parameters.
5. Click the **Apply** button to save the configuration.

Parameter descriptions :

<u>QoS Egress Port Scheduler and Shapers</u>

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

Scheduler Mode : Controls how many of the queues are scheduled as Strict and how many are scheduled as weighted on this switch port. Select Strict Priority or 2 Queues Weighted - 8 Queues Weighted. The default is Strict Priority.

<u>Queue Shaper</u>

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

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

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

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

- ***Line***: Specify that this shaper operates on the line rate.
- ***Data***: Specify that this shaper operates on the data rate.

Queue Scheduler

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

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.

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

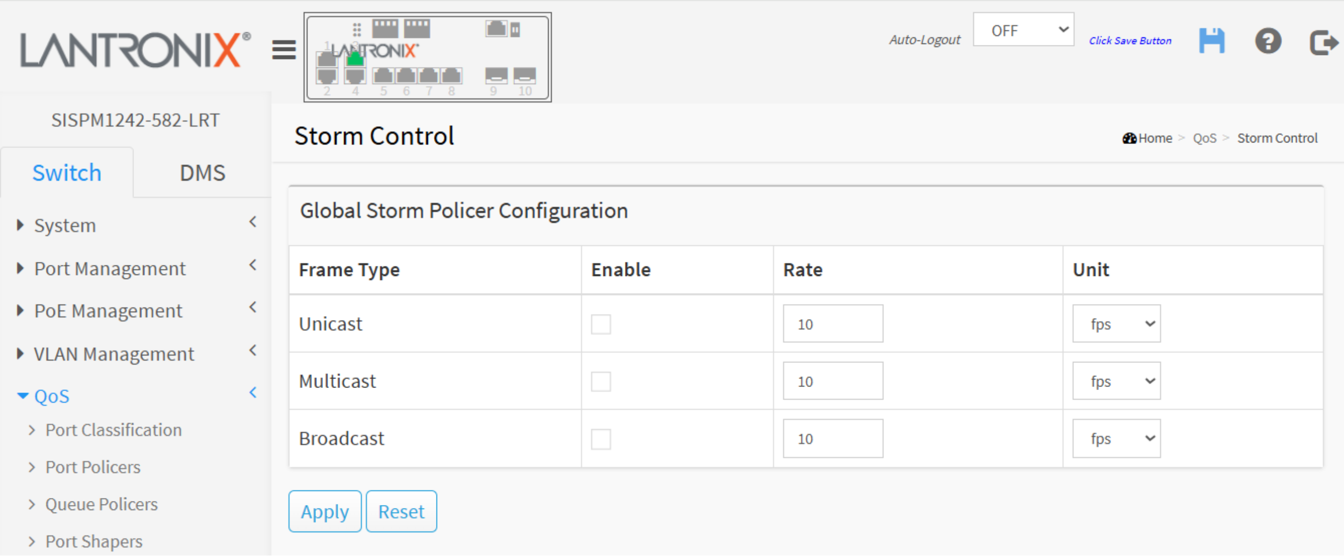
Unit : Controls the unit of measure for the port shaper rate as kbps or Mbps.

Storm Control

This page lets you configure global Storm control parameters. 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.

To configure Storm Control parameters in the web UI:

1. Go to QoS > Storm Control.
2. Select the frame type(s) to enable storm control.
3. Set the Rate and Unit parameters.
4. Click the **Apply** button to save the settings.



Storm Control

Global Storm Policer Configuration

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

Parameter descriptions :

Global Storm Policer Configuration

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

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

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

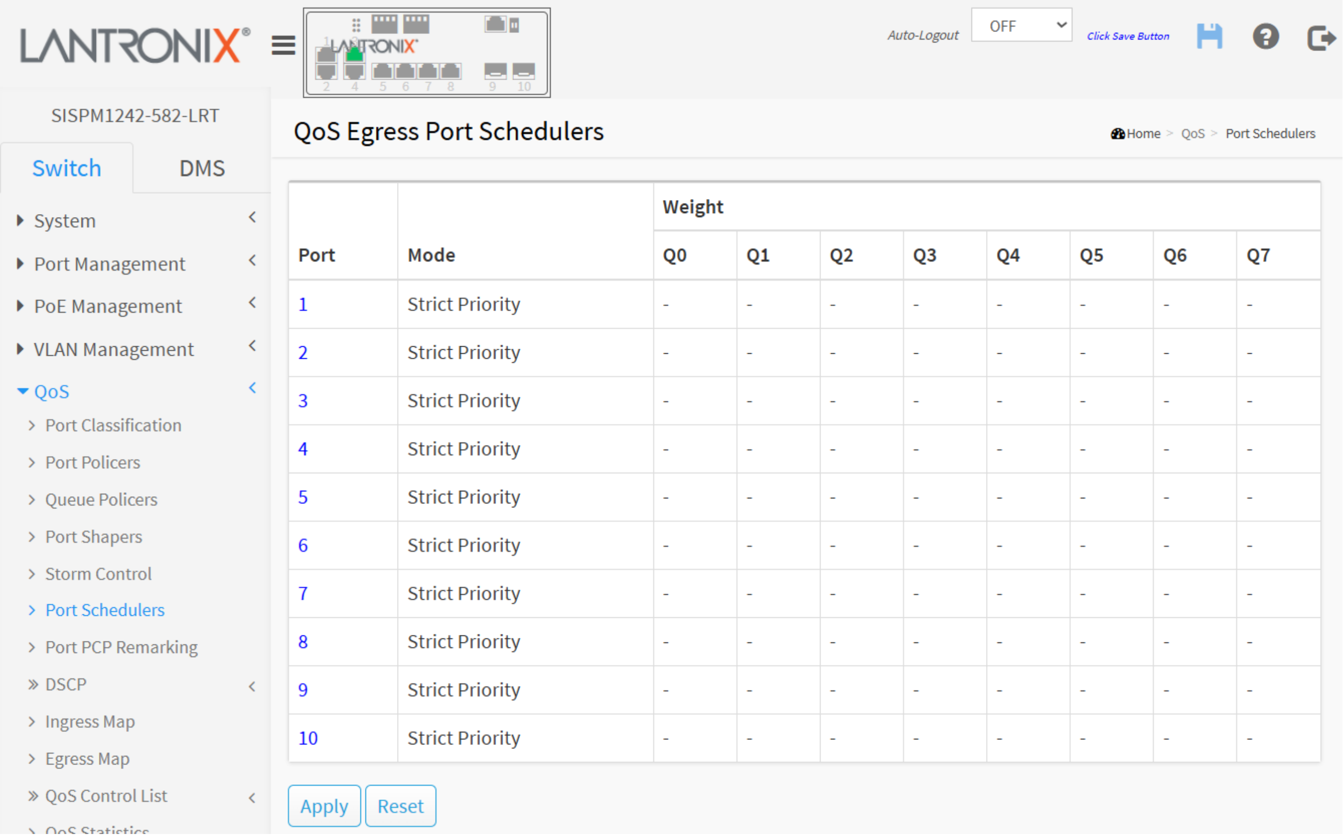
Unit : Select the unit of measure for the global storm policer rate as fps, kfps, kbps or Mbps. The default is ‘fps’.

Port Schedulers

This page provides an overview of QoS Egress Port Schedulers for all switch ports.

To configure QoS Egress Port Schedulers in the web UI:

1. Go to QoS > Port Scheduler.
2. Click the Port and display the QoS Egress Port Schedulers.
3. The configuration is done as described in the section Port Shapers.



QoS Egress Port Schedulers

Port	Mode	Weight							
		Q0	Q1	Q2	Q3	Q4	Q5	Q6	Q7
1	Strict Priority	-	-	-	-	-	-	-	-
2	Strict Priority	-	-	-	-	-	-	-	-
3	Strict Priority	-	-	-	-	-	-	-	-
4	Strict Priority	-	-	-	-	-	-	-	-
5	Strict Priority	-	-	-	-	-	-	-	-
6	Strict Priority	-	-	-	-	-	-	-	-
7	Strict Priority	-	-	-	-	-	-	-	-
8	Strict Priority	-	-	-	-	-	-	-	-
9	Strict Priority	-	-	-	-	-	-	-	-
10	Strict Priority	-	-	-	-	-	-	-	-

Parameter descriptions :

Port : The logical port for the settings contained in the same row. Click a linked Port number to display that port's QoS Egress Port Scheduler and Shapers webpage.

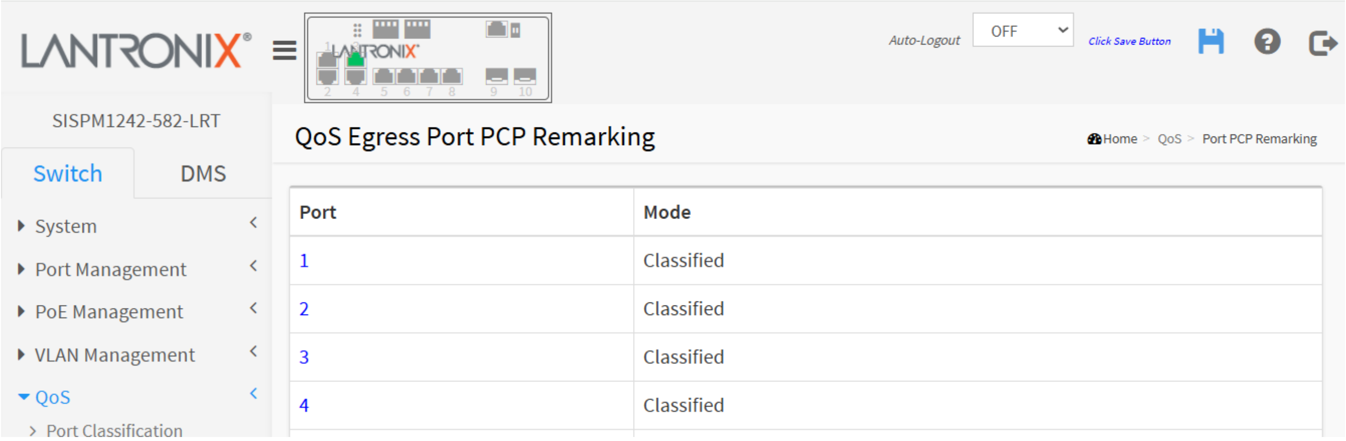
Mode : Select the scheduling mode for this port (e.g., Strict Priority, WRR).

Qn : Shows the weight for this queue and port.

Port PCP Remarking

This page lets you set QoS Egress Port PCP Remarking for each switch port. To configure QoS Port PCP Remarking in the web UI:

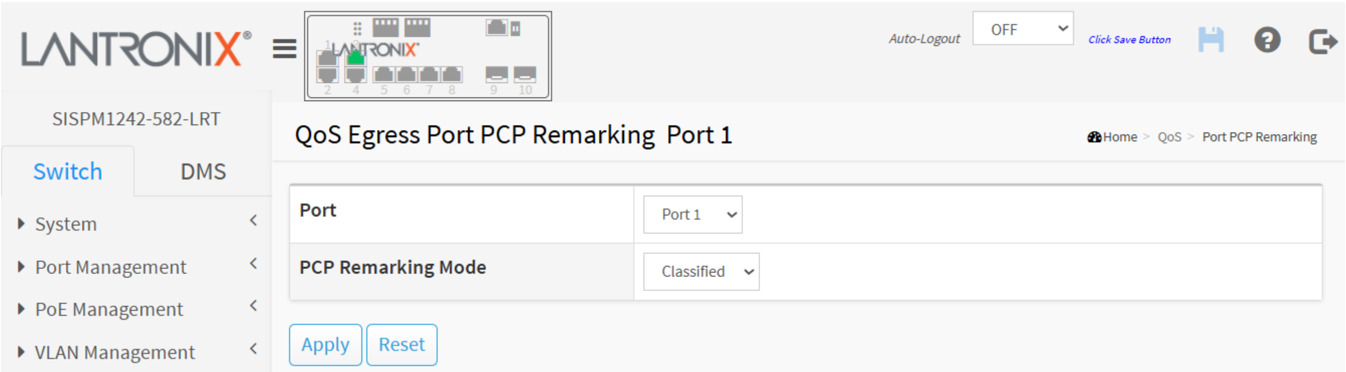
1. Go to Quality of Service > Port PCP Remarking.
2. Select the Port and display the QoS Port PCP Remarking for that port.
3. Select the PCP Remarking Mode and specify the Queue Shaper parameter.
4. Click the **Apply** button to save the settings.



QoS Egress Port PCP Remarking

Port	Mode
1	Classified
2	Classified
3	Classified
4	Classified

↓↓↓↓



QoS Egress Port PCP Remarking Port 1

Port	Port 1
PCP Remarking Mode	Classified

Parameter descriptions:

Port : The logical port for the settings contained in the same row. At the dropdown select the port number to configure PCP remarking.

Mode : Shows the PCP remarking mode for this port.

- ***Classified***: 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**.

CoS, DPL to PCP, DEI Mapping: Controls the mapping of the classified (CoS, DPL) to (PCP, DEI) values when the mode is set to **Mapped**.

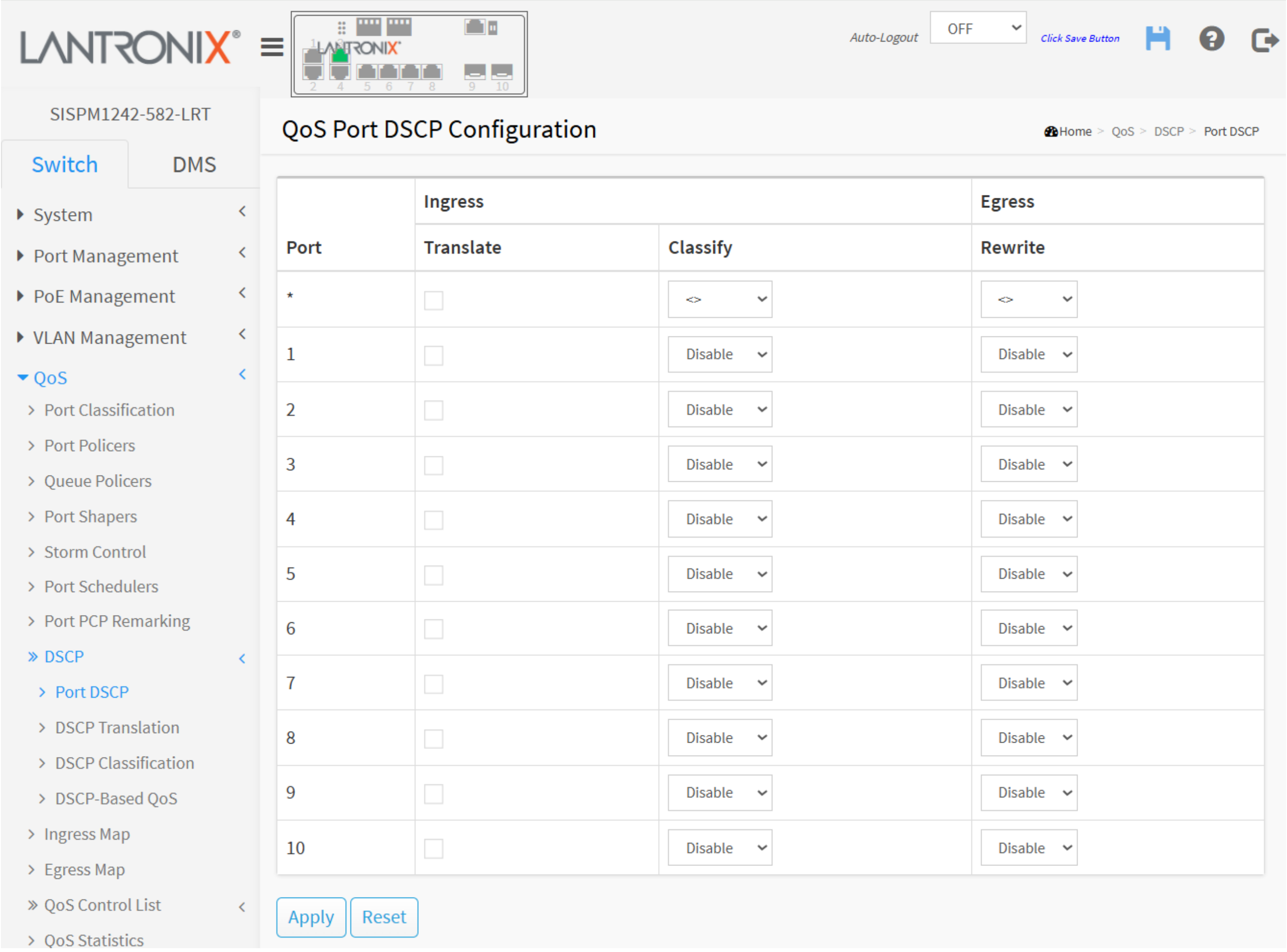
DSCP

Port DSCP

This page lets you set QoS Port DSCP parameters for all switch ports.

To configure QoS Port DSCP parameters in the web UI:

1. Go to Quality of Service > DSCP > Port DSCP.
2. Enable or disable the Ingress Translate and select the Classify parameters.
3. Select the Egress Rewrite parameter.
4. Click **Apply** to save the settings.



QoS Port DSCP Configuration

Port	Ingress		Egress
	Translate	Classify	Rewrite
*	□	<>	<>
1	□	Disable	Disable
2	□	Disable	Disable
3	□	Disable	Disable
4	□	Disable	Disable
5	□	Disable	Disable
6	□	Disable	Disable
7	□	Disable	Disable
8	□	Disable	Disable
9	□	Disable	Disable
10	□	Disable	Disable

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.

Translate : To Enable Ingress Translation check the checkbox.

Classify : Classification for a port have 4 different values:

- ***Disable***: No Ingress DSCP Classification.
- ***DSCP=0***: Classify if incoming (or translated if enabled) DSCP is 0.

- ***Selected***: Classify only selected DSCP for which classification is enabled as specified in DSCP Translation window for the specific DSCP.
- ***All***: Classify all DSCP.

Egress

Rewrite : Port Egress Rewriting can be one of these parameters:

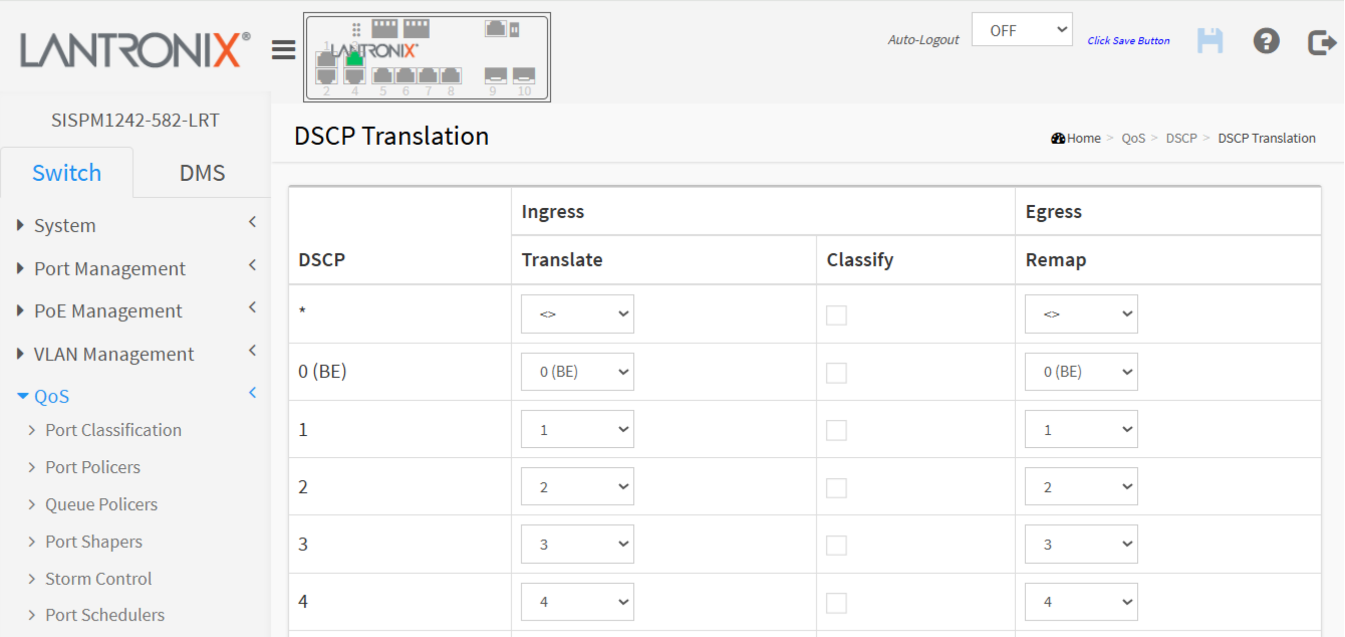
- ***Disable*** : No Egress rewrite (default).
- ***Enable***: Rewrite enable without remapped.
- ***Remap*** : DSCP from analyzer is remapped and frame is remarked with remapped DSCP value.

DSCP Translation

This page lets you configure basic QoS DSCP Translation settings for the switch. DSCP translation can be done in Ingress or Egress.

To configure DSCP Translation parameters in the web UI:

1. Go to QoS > DSCP > DSCP Translation.
2. Set the Ingress Translate and Egress Remap Parameters.
3. Enable or disable Classify.
4. Click **Apply** to save the settings.



DSCP Translation

DSCP	Ingress		Egress
	Translate	Classify	Remap
*	<>	□	<>
0 (BE)	0 (BE)	□	0 (BE)
1	1	□	1
2	2	□	2
3	3	□	3
4	4	□	4

Parameter descriptions:

DSCP : Maximum number of supported DSCP values are 64 and valid DSCP values are 0 - 63.

Ingress : Ingress side DSCP can be first translated to new DSCP before using the DSCP for QoS class and DPL map.

There are two configuration parameters for DSCP Translation:

Translate: DSCP at Ingress side can be translated to any of (0-63) DSCP values.

Classify: Click to enable Classification at Ingress side.

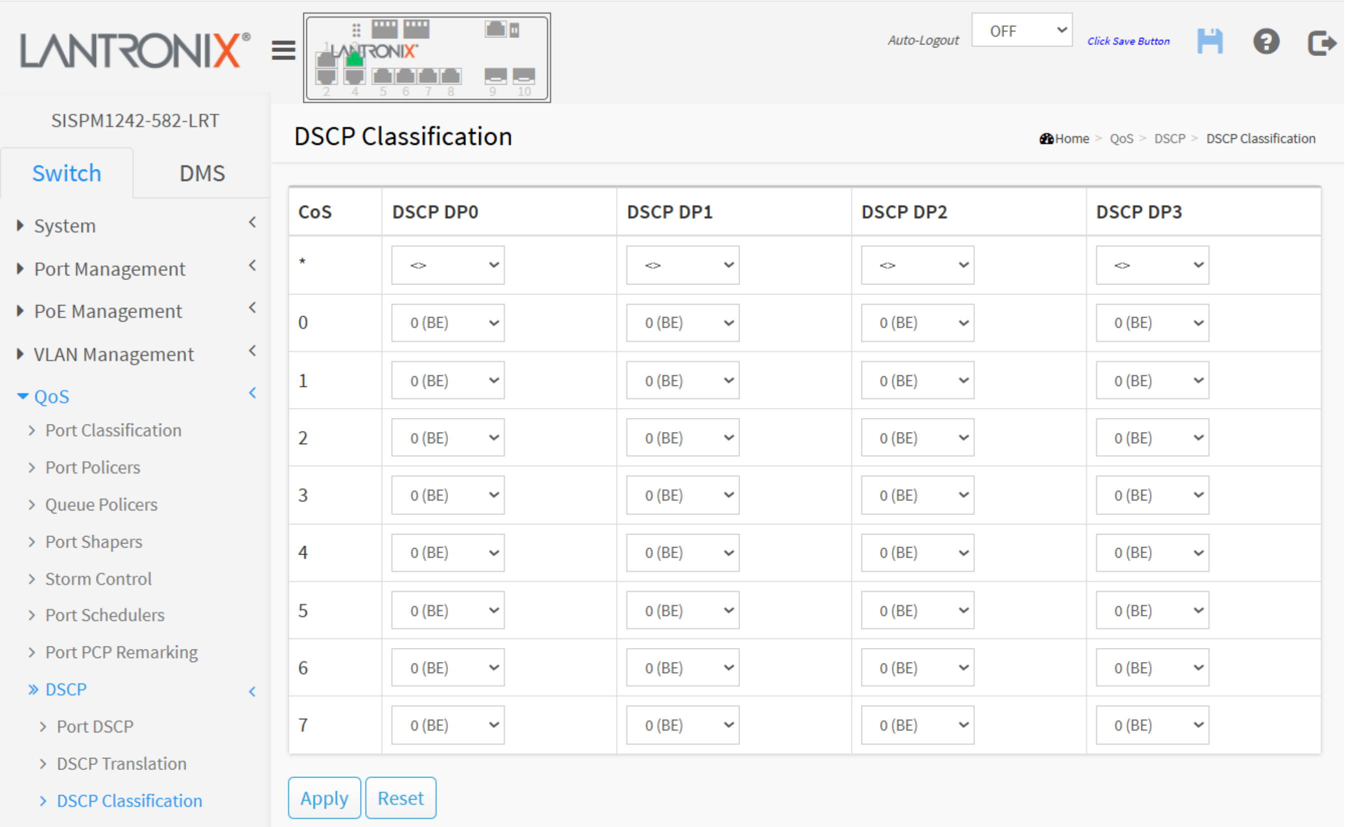
Egress Remap : At the dropdown select the DSCP value to which you want to remap. The DSCP value can be 0 - 63.

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. Go to QoS > DSCP > DSCP Translation
2. Set the DSCP Parameters.
3. Click the **Apply** button to save the settings.



DSCP Classification

CoS	DSCP DP0	DSCP DP1	DSCP DP2	DSCP DP3
*	<>	<>	<>	<>
0	0 (BE)	0 (BE)	0 (BE)	0 (BE)
1	0 (BE)	0 (BE)	0 (BE)	0 (BE)
2	0 (BE)	0 (BE)	0 (BE)	0 (BE)
3	0 (BE)	0 (BE)	0 (BE)	0 (BE)
4	0 (BE)	0 (BE)	0 (BE)	0 (BE)
5	0 (BE)	0 (BE)	0 (BE)	0 (BE)
6	0 (BE)	0 (BE)	0 (BE)	0 (BE)
7	0 (BE)	0 (BE)	0 (BE)	0 (BE)

Parameter descriptions:

Queue Priority : Actual Class of Service (0-7).

DSCP DP0 : Select the classified DSCP value (0-63) for Drop Precedence Level 0.

DSCP DP1 : Select the classified DSCP value (0-63) for Drop Precedence Level 1.

DSCP DP2 : Select the classified DSCP value (0-63) for Drop Precedence Level 2.

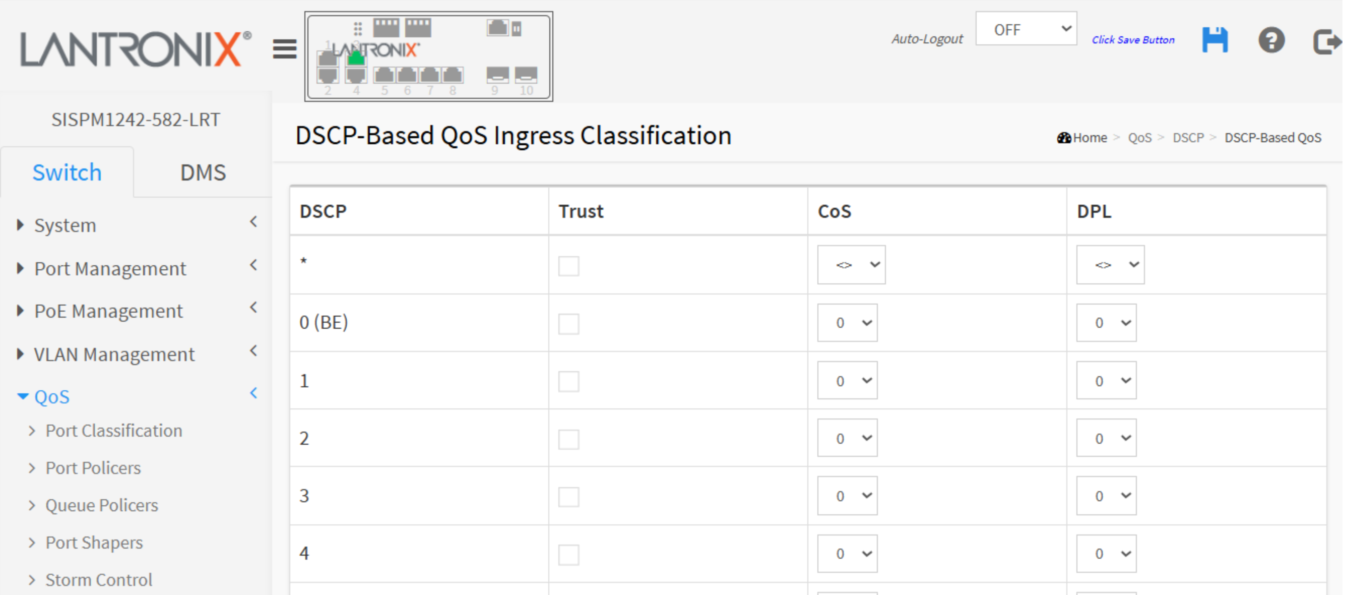
DSCP DP3 : Select the classified DSCP value (0-63) for Drop Precedence Level 3.

DSCP-Based QoS

This page lets you configure basic QoS DSCP based QoS Ingress Classification settings. DSCP is a field in the header of IP packets for packet classification purposes.

To configure DSCP-Based QoS Ingress Classification in the web UI:

1. Go to QoS > DSCP > DSCP-Based QoS.
2. Enable or disable Trust for DSCP.
3. Select Queue Priority and DPL parameters.
4. Click the **Apply** button to save the settings.



DSCP-Based QoS Ingress Classification

DSCP	Trust	CoS	DPL
*	□	<>	<>
0 (BE)	□	0	0
1	□	0	0
2	□	0	0
3	□	0	0
4	□	0	0

Parameter descriptions:

DSCP : Maximum number of supported DSCP values is 64.

Trust : Check the box if the DSCP value is to be trusted.

CoS : Queue Priority value can be 0 – 7, where 7 is the highest priority.

DPL : Drop Precedence Level (0-3).

Ingress Map

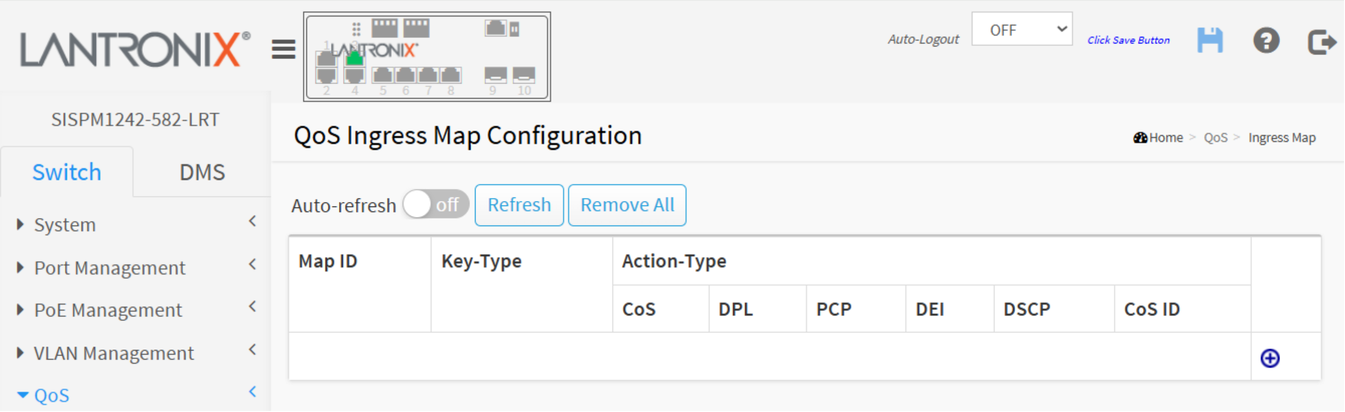
This page shows a table of QoS Ingress Maps which is made up of individual map entries. Each entry has a key and an action. The key indicates which fields of the frame will be mapped to the fields specified by and according to the action. Each Map can hold several map rules, or mappings between possible keys and actions. Which of those rules will be applied depends on the selection of (Key-Type, Action-Type).

Each row describes a user-defined map. The maximum number of Ingress Maps is **128**. Each Ingress Map uses several key-entries in an internal key mapping table which have **1004** key-entries available for configuration. The consumption of key-entries by Key Type are listed as table width in the Key-Type table below. A new Ingress Map can only be defined when there are sufficient free key-entries.

This page is an overview of the configured maps. Use the Modification buttons to add/edit/delete maps.

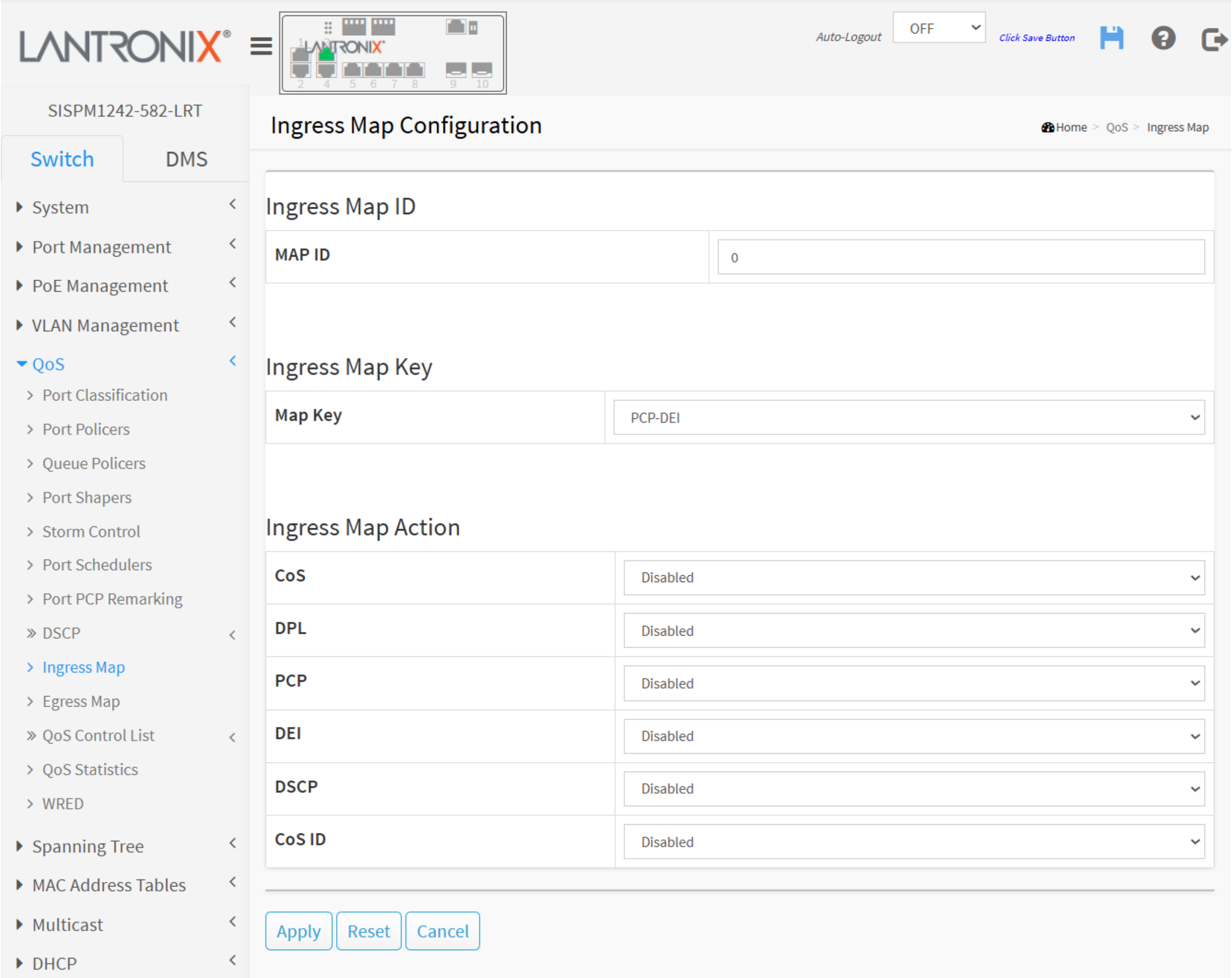
To configure Ingress Map parameters in the web UI:

1. Go to QoS > Ingress Map.
2. On the default page, click the Add ⊕ button to display the Ingress Map Configuration page.
3. Configure the settings.
4. Click the **Apply** button to save the configuration.



QoS Ingress Map Configuration

Map ID	Key-Type	Action-Type						
		CoS	DPL	PCP	DEI	DSCP	CoS ID	
								⊕



Ingress Map Configuration

Ingress Map ID

MAP ID	0

Ingress Map Key

Map Key	PCP-DEI

Ingress Map Action

CoS	Disabled
DPL	Disabled
PCP	Disabled
DEI	Disabled
DSCP	Disabled
CoS ID	Disabled

Parameter descriptions:

Ingress Map ID

Map ID: Indicates the Map (unique) ID. The valid range is 0 - 255. When in edit mode, this is non-configurable. However, it is possible to overwrite an existing mapping through the create mode.

Ingress Map Key

Map Key: Indicates the Key type that will be used to filter the map rules when applying the map. As mentioned above, map rules can have various keys and this is to make a select set of them. Possible Key types are:

- ***PCP - DEI***: Use PCP/DEI as key for tagged frames and none for the rest.
- ***DSCP***: Use DSCP as key for IP frames and none for the rest.
- ***DSCP - PCP - DEI***: Use DSCP as key for IP frames, PCP/DEI for tagged frames and none for the rest.

Ingress Map Action

Indicates the Action type that will be used to filter the map rules when applying the map.
As mentioned above, map rules can have various actions available and this is to make a select set of them.
Possible Map Action types are:

CoS: Class of Service.

DPL: Drop Precedence Level.

PCP: Priority Code Point.

DEI: Drop Eligible Indicator.

DSCP: Differentiated Services Code Point.

CoS ID: CoS ID.

Modification Buttons

⊕ Add New Map (can also be used to overwrite an existing map, so use care on the Map ID).

ⓔ Edit map

⊗ Delete map

Egress Map

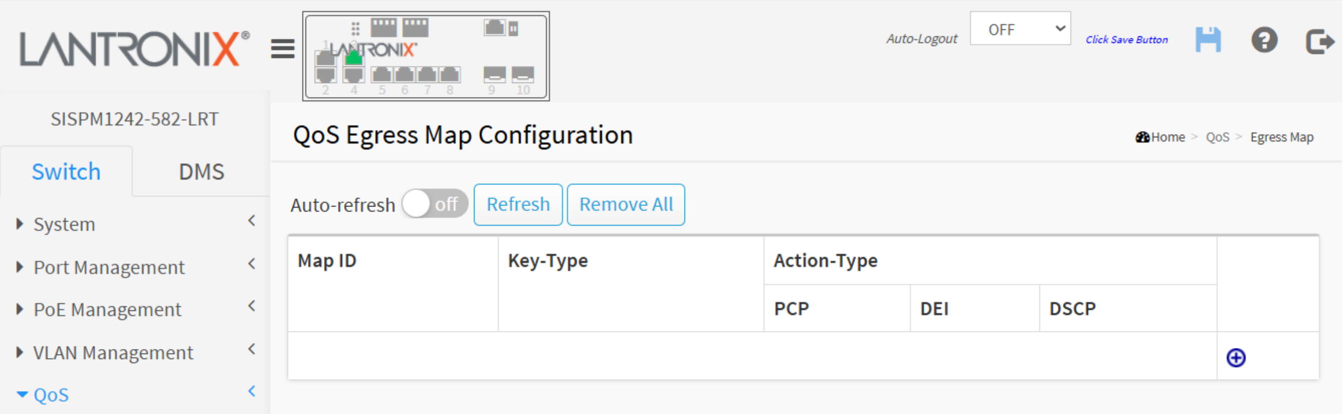
This page lets you create, edit or delete a single QoS Egress Map entry at a time. Each entry has a key and an action. The key indicates which fields of the frame will be mapped to the fields specified by and according to the action. Each Map can hold several map rules, or mappings between possible keys and actions. Which of those rules will be applied depends on the selection of (Key-Type, Action-Type). Here it is possible to configure these 'filters'.

This page shows a table of QoS Egress Maps which is made up of individual map entries. Each entry has a key and an action. The key indicates which fields of the frame will be mapped to the fields specified by and according to the action. Each Map can hold several map rules, or mappings between possible keys and actions. Which of those rules will be applied depends on the selection of (Key-Type, Action-Type). Each row describes a user-defined map. The maximum number of Egress Maps is **256**. Each Egress Map uses a number of key-entries in a internal key mapping table which have **960** key-entries available. The consumption of key-entries by Key Type are listed as table width in the Key-Type table below. A new Egress Map can only be defined when there are sufficient free key-entries.

This page is an overview of the configured maps. Use the Modification buttons to add/edit/delete maps.

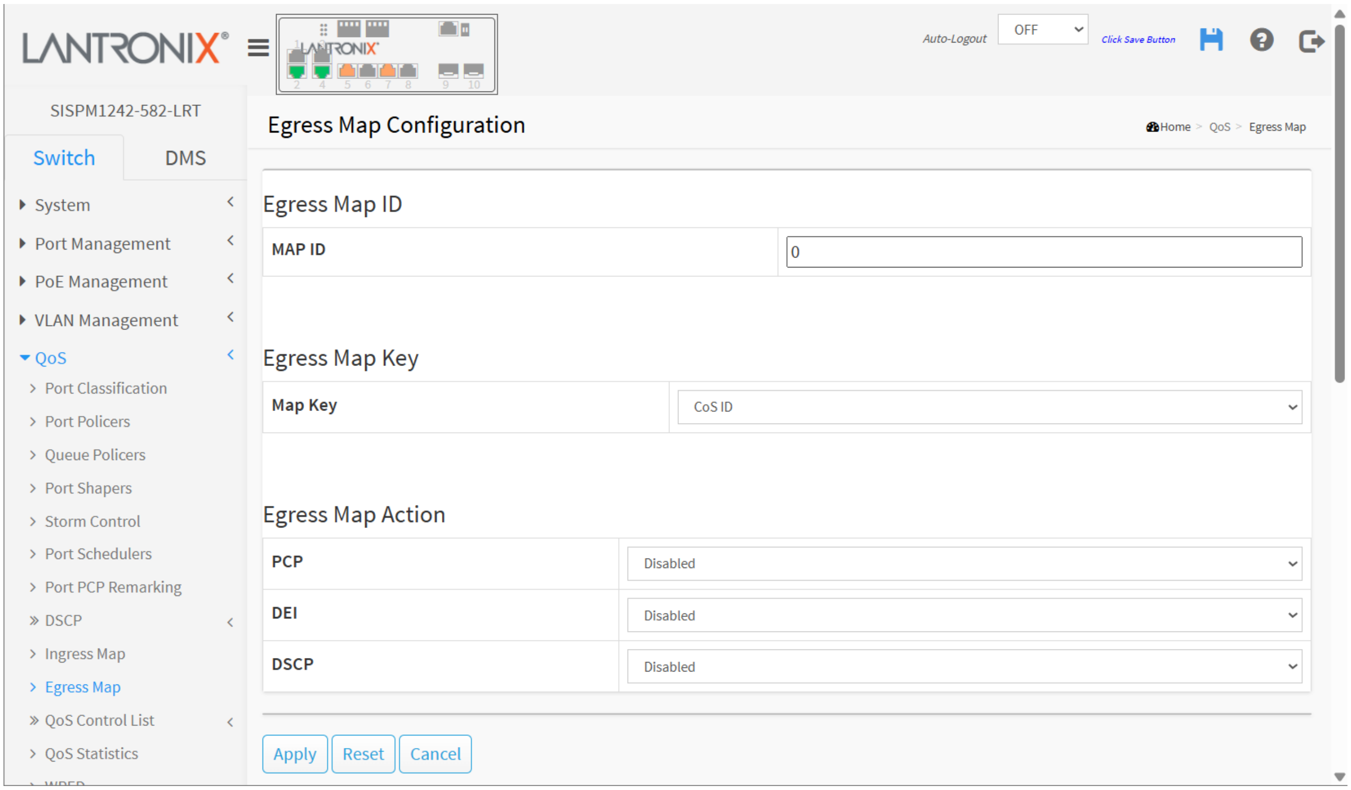
To configure Egress Map parameters in the web UI:

1. Go to QoS > Egress Map.
2. On the default page, click the ⊕ button to display the Egress Map Configuration page.
3. Set the Egress Map ID, Key, and Actions.
4. Click the **Apply** button to save the settings.



QoS Egress Map Configuration

Map ID	Key-Type	Action-Type			
		PCP	DEI	DSCP	
					⊕



Egress Map Configuration

Egress Map ID

MAP ID	0

Egress Map Key

Map Key	CoS ID

Egress Map Action

PCP	Disabled
DEI	Disabled
DSCP	Disabled

Parameter descriptions:

Map ID : Indicates the Map (unique) ID. The valid range is 0 - 511. When in edit mode, this is non-configurable. However, it is possible to overwrite an existing mapping through the create mode.

Map Key : Indicates the Key type that will be used to filter the map rules when applying the map. As mentioned above, map rules can have various keys and this is to make a select set of them. Possible Key types are:

- ***CoS ID*** : Use classified COS ID as key.
- ***CoS ID - DPL*** :Use classified COS ID and DPL as key.
- ***DSCP*** : Use classified DSCP as key.
- ***DSCP - DPL*** : Use classified DSCP and DPL as key.

Map Action: Indicates the Action type that will be used to filter the map rules when applying the map. As mentioned above, map rules can have various actions available and this is to make a select set of them. Possible Map Action types are:

PCP: Priority Code Point.

DEI: Drop Eligible Indicator.

DSCP: Differentiated Services Code Point.

Modification Buttons

⊕ Add New Map (can also be used to overwrite an existing map, so use care on the Map ID).

ⓔ Edit map

⊗ Delete map

QoS Control List

Configuration

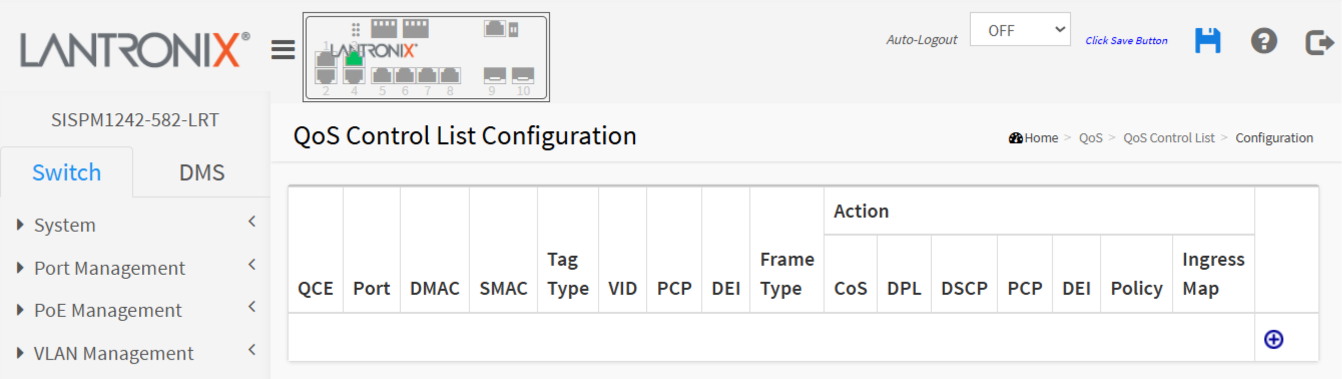
This page lets you add or edit one QoS Control Entry (QCE) at a time. A QCE consists of several parameters. These parameters vary according to the Frame Type that you select.

A QCE (QoS Control Entry) describes a QoS class associated with a particular QCE ID. There are six QCE frame types: Ethernet Type, VLAN, UDP/TCP Port, DSCP, TOS, and Tag Priority. Frames can be classified by one of four different QoS classes: "Low", "Normal", "Medium", and "High" for an individual application.

Each row in the table describes a QCE that is defined. The maximum number of QCEs is 256 per switch. Click on the lowest plus sign to add a new QCE to the list.

To configure QoS Control List parameters in the web UI:

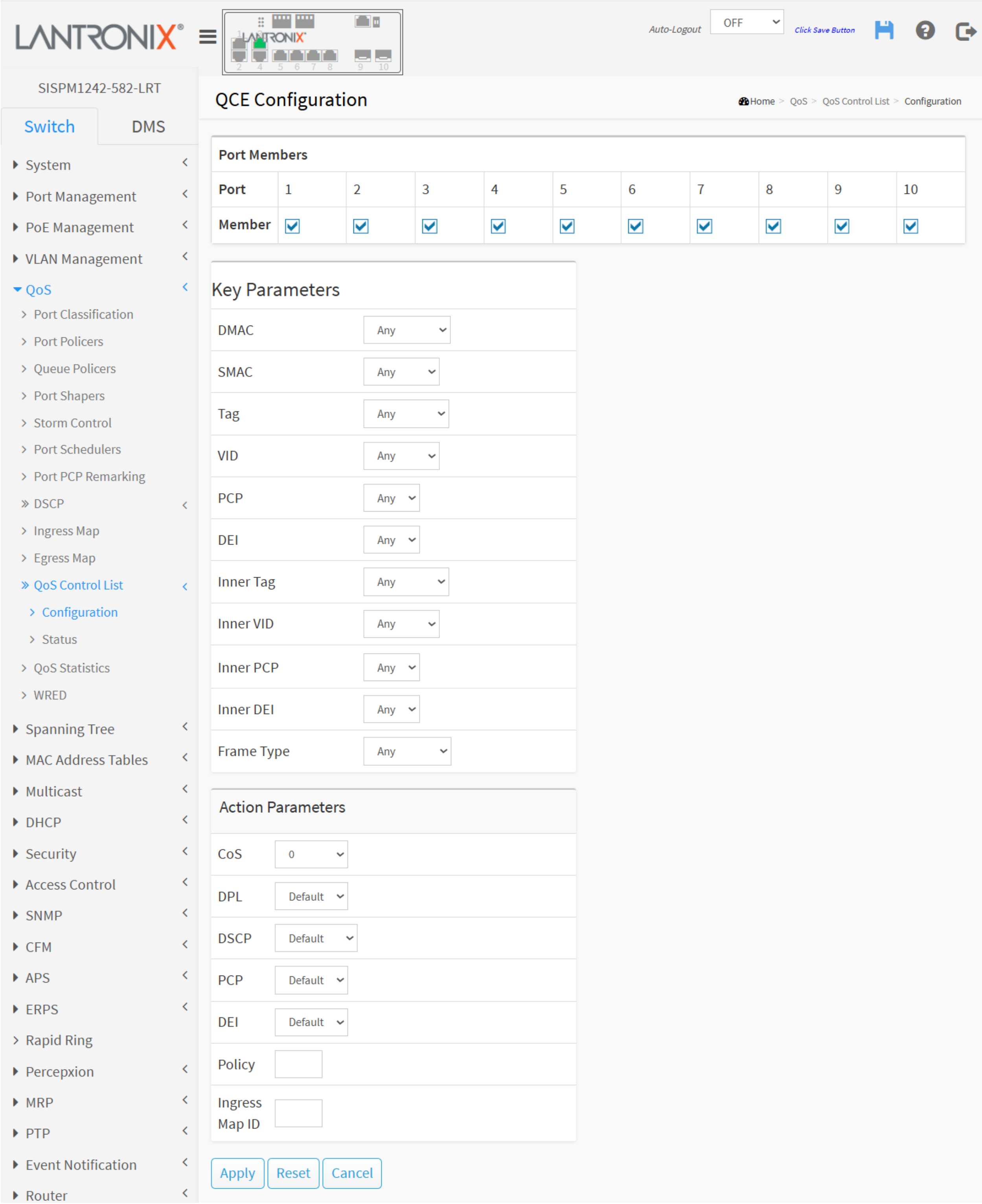
1. Go to QoS > QoS Control List > Configuration.
2. Click the ⊕ button to add a new QoS Control List.



QoS Control List Configuration

									Action							
QCE	Port	DMAC	SMAC	Tag Type	VID	PCP	DEI	Frame Type	CoS	DPL	DSCP	PCP	DEI	Policy	Ingress Map	
																⊕

3. Set all parameters and enable Port Members to join the QCE rules.
4. Click the **Apply** button to save the settings.



QCE Configuration

Port Members

Port	1	2	3	4	5	6	7	8	9	10
Member	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑

Key Parameters

DMAC	Any
SMAC	Any
Tag	Any
VID	Any
PCP	Any
DEI	Any
Inner Tag	Any
Inner VID	Any
Inner PCP	Any
Inner DEI	Any
Frame Type	Any

Action Parameters

CoS	0
DPL	Default
DSCP	Default
PCP	Default
DEI	Default
Policy	
Ingress Map ID	

Parameter descriptions:

Port Members

For each port check the box to enable or disable the port as a member.

Key Parameters

DMAC : Indicates the destination MAC address. Possible values are:

- ***Any***: Match any DMAC. The default value is 'Any'.
- ***Unicast***: Match unicast DMAC.
- ***Multicast***: Match multicast DMAC.
- ***Broadcast***: Match broadcast DMAC.
- ***<MAC>*** : Match specific DMAC.

SMAC : Match specific source MAC address or 'Any'. If a port is configured to match on DMAC/DIP, this field indicates the DMAC.

Tag: Indicates tag type. Possible values are:

- ***Any***: Match tagged and untagged frames. The default value is 'Any'.
- ***Untagged***: Match untagged frames.
- ***Tagged***: Match tagged frames.
- ***C-Tagged***: Match C-tagged frames.
- ***S-Tagged***: Match S-tagged frames.

VID : Indicates (VLAN ID), either a specific VID or range of VIDs. VID can be in the range 1-4095 or 'Any'

PCP : Priority Code Point: Valid values of PCP are specific (0, 1, 2, 3, 4, 5, 6, 7) or range(0-1, 2-3, 4-5, 6-7, 0-3, 4-7) or 'Any'.

DEI : Drop Eligible Indicator: Valid value of DEI are 0, 1 or 'Any'.

Inner Tag : Value of can be 'Untagged', 'Tagged', 'C-Tagged', 'S-Tagged' or 'Any'.

Inner VID : Valid value can be any value in the range 1-4095 or 'Any'; user can enter either a specific value or a range of VIDs.

Inner PCP : Valid value is specific (0, 1, 2, 3, 4, 5, 6, 7) or range (0-1, 2-3, 4-5, 6-7, 0-3, 4-7) or 'Any'.

Inner DEI : Valid value can be '0', '1' or 'Any'.

Frame Type : Indicates the type of frame to look for incoming frames. Possible frame types are:

- ***Any***: The QCE will match all frame type.
- ***Ethertype***: 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.

Frame types are explained below.

<u>Action Parameters</u> : Indicates the classification action taken on ingress frame if parameters configured are matched with the frame's content. Possible actions are:

CoS : Classify Class of Service.

DPL: Classify Drop Precedence Level.

DSCP : Classify DSCP value.

PCP : Classify PCP value.

DEI : Classify DEI value.

Policy : Classify ACL Policy number.

Ingress Map ID : Classify Ingress Map ID.

Buttons : You can modify each QCE (QoS Control Entry) in the table using these buttons:

⊕: Inserts a new QCE before the current row.

ⓔ: Edits the QCE.

↑ : Moves the QCE up the list.

↓ : Moves the QCE down the list.

⊗ : Deletes the QCE.

⊕: The lowest plus sign adds a new entry at the bottom of the QCE listings.

Port Members : Check the checkbox button to include the port in the QCL entry. By default all ports are included.

Key Parameters : Key configuration is described below:

DMAC Destination MAC address: Possible values are 'Unicast', 'Multicast', 'Broadcast', 'Specific' (xx-xx-xx-xx-xx-xx) or 'Any'.

SMAC Source MAC address: xx-xx-xx-xx-xx-xx or 'Any'.

Tag Value of Tag field can be 'Untagged', 'Tagged', 'C-Tagged', 'S-Tagged' or 'Any'.

VID Valid value of VLAN ID can be any value in the range 1-4095 or 'Any'; user can enter either a specific value or a range of VIDs.

PCP : Valid value PCP are specific (0, 1, 2, 3, 4, 5, 6, 7) or range (0-1, 2-3, 4-5, 6-7, 0-3, 4-7) or 'Any'.

DEI : Valid value of DEI can be '0', '1' or 'Any'.

Inner Tag : Value of can be 'Untagged', 'Tagged', 'C-Tagged', 'S-Tagged' or 'Any'.

Inner VID : Valid value can be any value in the range 1-4095 or 'Any'; user can enter either a specific value or a range of VIDs.

Inner PCP : Valid value is specific (0, 1, 2, 3, 4, 5, 6, 7) or range (0-1, 2-3, 4-5, 6-7, 0-3, 4-7) or 'Any'.

Inner DEI : Valid value can be '0', '1' or 'Any'.

Frame Type : Valid values are Any, EtherType, LLC, SNAP, IPv4, or IPv6.

Note: These frame types are described below:

Any : Allow all types of frames.

FrameTypes Explained

EtherType : Valid Ether Type can be 0x600-0xFFFF excluding 0x800(IPv4) and 0x86DD(IPv6) or 'Any'.

LLC : Valid selections are:

- ***DSAP Address***: Valid DSAP(Destination Service Access Point) can vary from 0x00 to 0xFF or 'Any'.
- ***SSAP Address*** : Valid SSAP(Source Service Access Point) can vary from 0x00 to 0xFF or 'Any'.
- ***Control*** : Valid Control field can vary from 0x00 to 0xFF or 'Any'.

SNAP : PID Valid PID (a.k.a., Ether Type) can be 0x0000-0xFFFF or 'Any'.

IPv4 : Valid selections are:

- ***Protocol*** : IP protocol number: (0-255, 'TCP' or 'UDP') or 'Any'.
- ***Source IP*** : Specific Source IP address in value/mask format or 'Any'. IP and Mask are in the format x.y.z.w where x, y, z, and w are decimal numbers between 0 and 255. When Mask is converted to a 32-bit binary string and read from left to right, all bits following the first zero must also be zero.
- ***Destination IP*** : Specific Destination IP address in value/mask format or 'Any'.
- ***IP Fragment*** : IPv4 frame fragmented option: 'Yes', 'No' or 'Any'.
- ***DSCP*** : Diffserv Code Point value (DSCP): It can be a specific value, range of values or 'Any'. DSCP values are in the range 0-63 including BE, CS1-CS7, EF or AF11-AF43.
- ***Sport*** : Source TCP/UDP port:(0-65535) or 'Any', specific or port range applicable for IP protocol UDP/TCP.
- ***Dport*** : Destination TCP/UDP port:(0-65535) or 'Any', specific or port range applicable for IP protocol UDP/TCP.

IPv6: Valid selections are:

- ***Protocol***: IP protocol number: (0-255, 'TCP' or 'UDP') or 'Any'.
- ***Source IP***: 32 LS bits of IPv6 source address in value/mask format or 'Any'.
- ***Destination IP***: Specific Destination IP address in value/mask format or 'Any'.
- ***DSCP***: Diffserv Code Point value (DSCP): It can be a specific value, range of values or 'Any'. DSCP values are in the range 0-63 including BE, CS1-CS7, EF or AF11-AF43.
- ***Sport***: Source TCP/UDP port:(0-65535) or 'Any', specific or port range applicable for IP protocol UDP/TCP.
- ***Dport***: Destination TCP/UDP port:(0-65535) or 'Any', specific or port range applicable for IP protocol UDP/TCP.

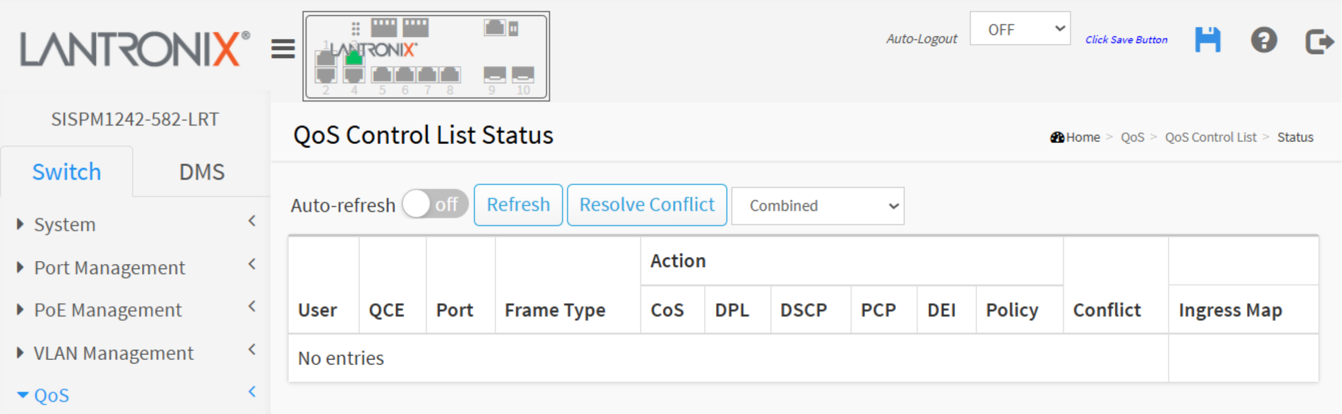
Status

This page lets you view and configure QCL status by different QCL users. Each row describes a defined QCE.

It is a conflict if a specific QCE is not applied to the hardware due to hardware limitations. The maximum number of QCEs is 256 per switch.

To display QoS Control List Status in the web UI:

1. Go to QoS > QoS Control List > Status.
2. Choose the QCL Status selection from the list.
3. **Auto-refresh** will refresh the page every 3 seconds. **Refresh** will refresh the page immediately.



QoS Control List Status

				Action							
User	QCE	Port	Frame Type	CoS	DPL	DSCP	PCP	DEI	Policy	Conflict	Ingress Map
No entries											

Parameter descriptions :

Resolve Conflict : Click this button to release the resources required to add QCL entry if the Conflict status for any QCL entry is 'yes'.

QCL status selection list: At the dropdown select QCL status (Combined, Static, Voice VLAN, DHCP Snooping, Ipv6 Source Guard, undefined, or Conflict). The default is ‘Combined’.

User : Indicates the QCL user.

QCE : Indicates the index of QCE.

Port : Indicates the list of ports configured with the QCE.

Frame Type : Indicates the type of frame. Possible values are:

- ***Any***: Match any frame type.
- ***Ethernet***: Match EtherType frames.
- ***LLC***: Match (LLC) frames.
- ***SNAP***: Match (SNAP) frames.
- ***IPv4***: Match IPv4 frames.
- ***IPv6***: Match IPv6 frames.

Action : Indicates the classification action taken on ingress frame if parameters configured are matched with the frame's content. Possible actions are:

- ***CoS***: Classify Class of Service.
- ***DPL***: Classify Drop Precedence Level.
- ***DSCP***: Classify DSCP value.
- ***PCP***: Classify PCP value.
- ***DEI***: Classify DEI value.
- ***Policy***: Classify ACL Policy number.
- ***Ingress Map***: Classify Ingress Map ID.

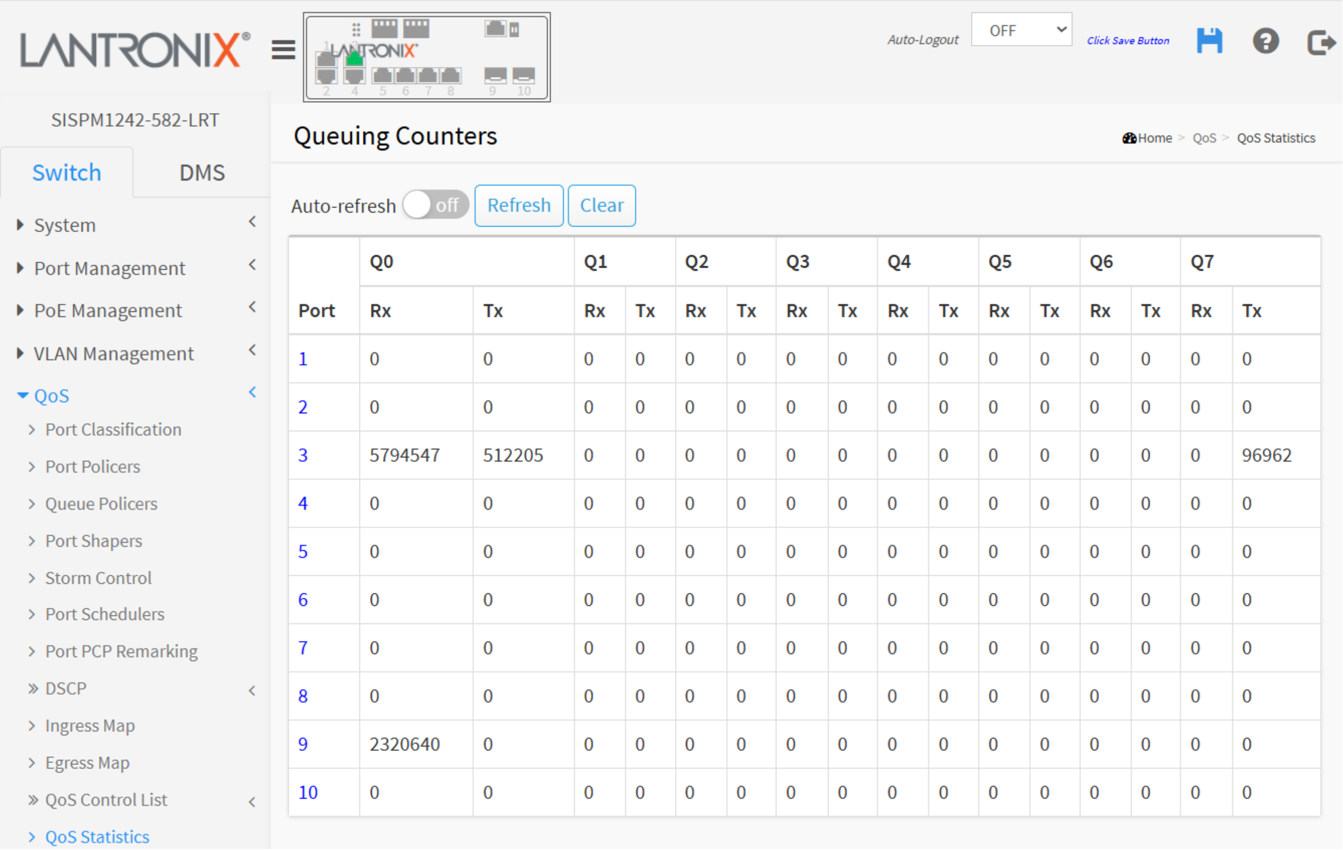
Conflict : Displays Conflict status of QCL entries. It may happen that resources required to add a QCE may not available; in that case it shows Conflict status as 'Yes', otherwise it is always 'No’. **Note** that conflict can be resolved by releasing the Hardware resources required to add QCL entry on clicking the 'Resolve Conflict' button.

QoS Statistics

This page displays statistics for available queues for all switch ports.

To view Queuing Counters in the web UI:

1. Go to QoS > QoS Statistics.
2. **Auto-refresh** will refresh the page every 3 seconds. **Refresh** will refresh the page immediately. **Clear** will clear all statistics.



Queuing Counters

	Q0		Q1		Q2		Q3		Q4		Q5		Q6		Q7	
Port	Rx	Tx	Rx	Tx	Rx	Tx	Rx	Tx	Rx	Tx	Rx	Tx	Rx	Tx	Rx	Tx
1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
2	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
3	5794547	512205	0	0	0	0	0	0	0	0	0	0	0	0	0	96962
4	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
5	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
6	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
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
9	2320640	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
10	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0

Parameter descriptions:

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

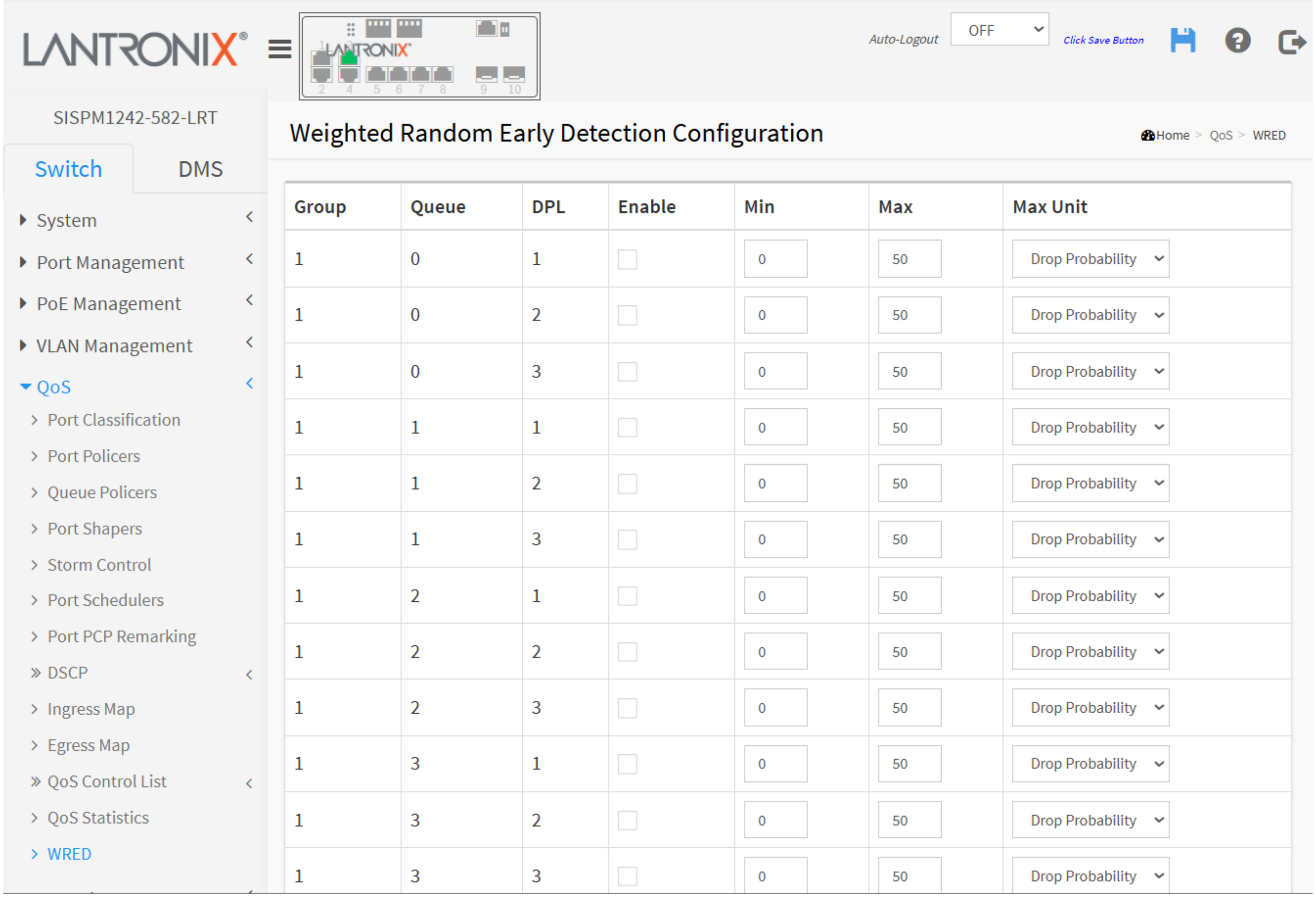
Qn : Qn is the Queue number; there are eight QoS queues per port. Q0 is the lowest priority queue.

Rx/Tx : The number of received and transmitted packets per queue.

WRED

This page allows you to configure the Random Early Detection (RED) settings. Through different RED configuration for the queues, it is possible to obtain Weighted Random Early Detection (WRED) operation between queues. The settings are global for all switch ports.

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.



Weighted Random Early Detection Configuration

Group	Queue	DPL	Enable	Min	Max	Max Unit
1	0	1	☐	0	50	Drop Probability
1	0	2	☐	0	50	Drop Probability
1	0	3	☐	0	50	Drop Probability
1	1	1	☐	0	50	Drop Probability
1	1	2	☐	0	50	Drop Probability
1	1	3	☐	0	50	Drop Probability
1	2	1	☐	0	50	Drop Probability
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
1	3	3	☐	0	50	Drop Probability

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: Check the box for the RED to be enabled for this entry.

Min: Controls the lower RED fill level threshold. If the queue filling level is below this threshold, the drop probability is zero. This value is restricted to 0-100%.

Max: Controls the upper RED drop probability or fill level threshold for frames marked with Drop Precedence Level > 0 (yellow frames). This value is restricted to 1-100%.

Max Unit: Selects the unit for Max. Possible values are:

- ***Drop Probability***: Max controls the drop probability just below 100% fill level (default).
- ***Fill Level***: Max controls the fill level where drop probability reaches 100%.

8. Spanning Tree

The Spanning Tree Protocol (STP) can be used to detect and disable network loops, and to provide backup links between switches, bridges or routers. This allows the switch to interact with other bridging devices (that is, an STP-compliant switch, bridge or router) in your network to ensure that only one route exists between any two stations on the network and provide backup links which automatically take over when a primary link goes down.

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

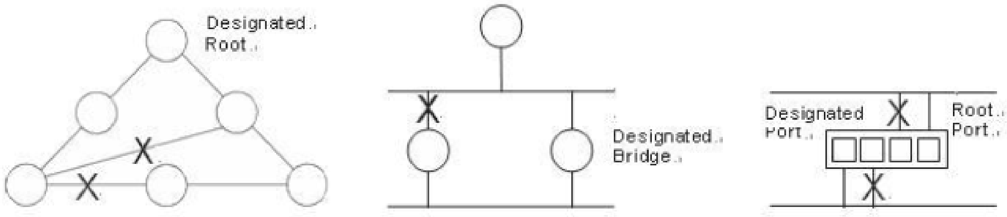


Figure 8-1 The Spanning Tree Protocol

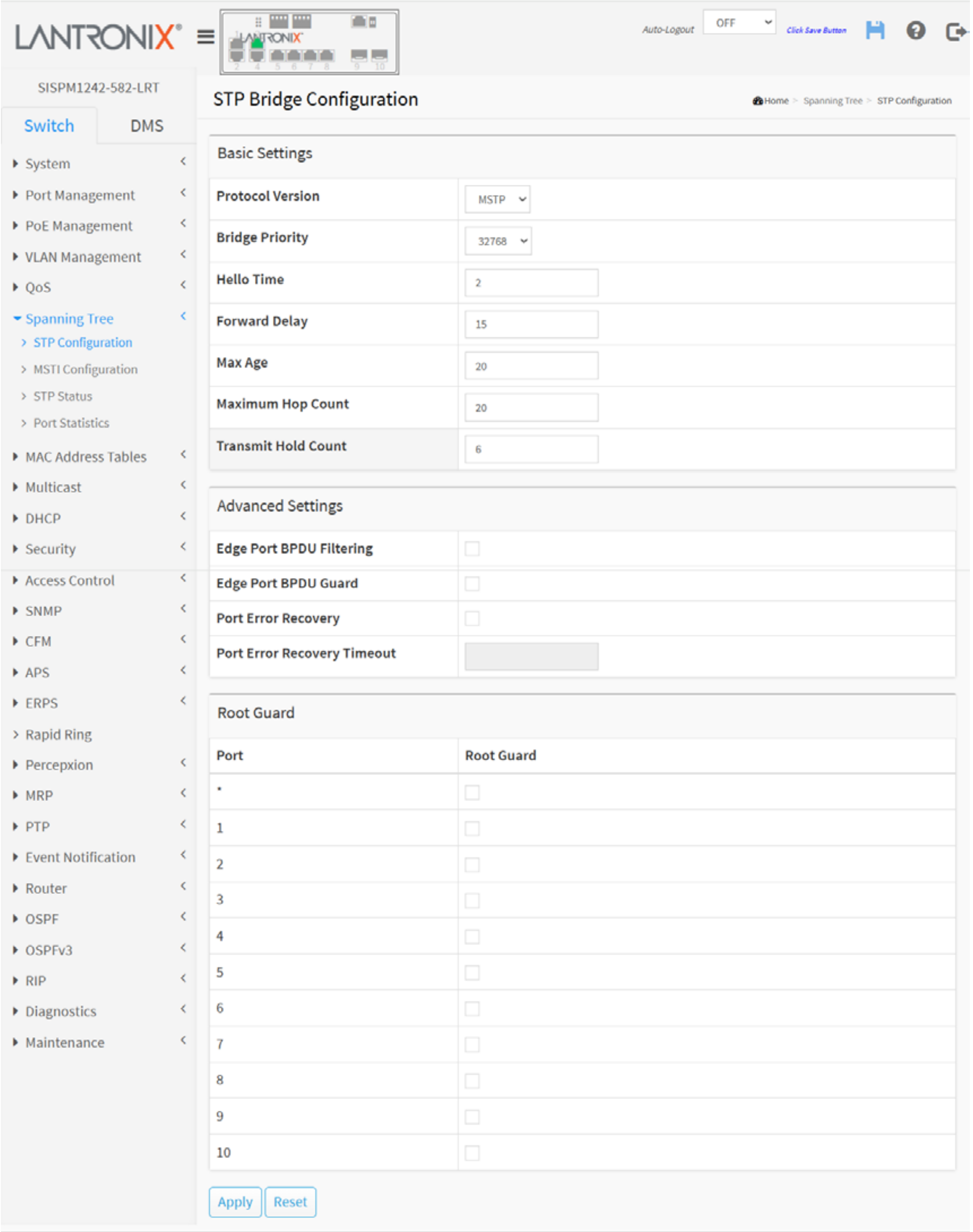
Once a stable network topology has been established, all bridges listen for Hello BPDUs (Bridge Protocol Data Units) transmitted from the Root Bridge. If a bridge does not get a Hello BPDU after a predefined interval (Maximum Age), the bridge assumes that the link to the Root Bridge is down. This bridge will then initiate negotiations with other bridges to reconfigure the network to reestablish a valid network topology.

STP Configuration

This page lets you enable or disable spanning tree protocol and select which protocol version you want.

To configure Spanning Tree Protocol settings in the web UI:

1. Go to Spanning Tree > STP Configuration.
2. Select parameters and enter parameters in blank field in Basic Settings.
3. Enable or disable the parameters and enter parameters in blank fields in Advanced settings.
4. Click the **Apply** button to save the settings.



STP Bridge Configuration

Basic Settings

Protocol Version	MSTP
Bridge Priority	32768
Hello Time	2
Forward Delay	15
Max Age	20
Maximum Hop Count	20
Transmit Hold Count	6

Advanced Settings

Edge Port BPDU Filtering	□
Edge Port BPDU Guard	□
Port Error Recovery	□
Port Error Recovery Timeout	

Root Guard

Port	Root Guard
*	□
1	□
2	□
3	□
4	□
5	□
6	□
7	□
8	□
9	□
10	□

Parameter descriptions:

Basic Settings

Protocol Version : The MSTP / RSTP / STP protocol version setting. Valid values are STP, RSTP and MSTP.

Bridge Priority : Controls the bridge priority. Lower numeric values have better priority. The bridge priority plus the MSTI instance number, concatenated with the 6-byte MAC address of the switch forms a Bridge Identifier. For MSTP operation, this is the priority of the CIST. Otherwise, this is the priority of the STP/RSTP Bridge.

Hello Time : The interval between sending STP BPDUs. Valid values are 1 - 10 seconds; 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 in the range 4 to 30 seconds.

Max Age : The maximum age of the information transmitted by the Bridge when it is the Root Bridge. Valid values are in the range 6 to 40 seconds, and MaxAge must be <= (FwdDelay-1)*2.

Maximum Hop Count : This defines the initial value of remaining Hops for MSTI information generated at the boundary of an MSTI region. It defines how many bridges a root bridge can distribute its BPDU information to. Valid values are 6 - 40 hops.

Transmit Hold Count : The number of BPDUs a bridge port can send per second. When exceeded, transmission of the next BPDU will be delayed. Valid values are 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

For each port, check or uncheck the Root Guard checkbox. The default is unchecked. Root guard is an STP feature that is enabled on a port-by-port basis. It prevents a configured port from becoming a root port. Root guard prevents a downstream switch (often misconfigured or rogue) from becoming a root bridge in a topology. Enable root guard on all ports on which the root bridge should not appear.

MSTI Configuration

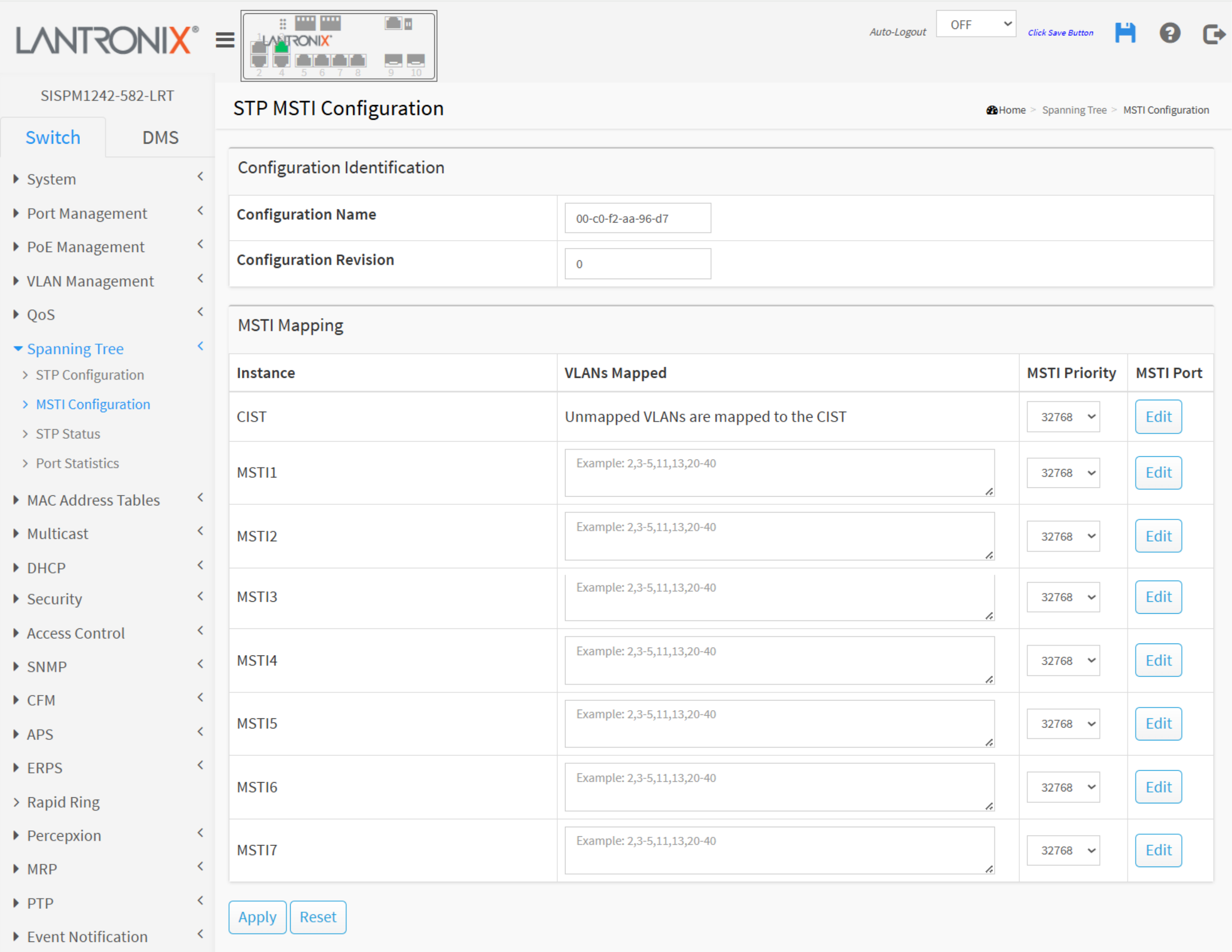
This page lets you set and view current STP MSTI bridge instance priority parameters.

When you implement a Spanning Tree protocol on the switch that is the bridge instance, the CIST is not available for explicit mapping, as it will receive the VLANs not explicitly mapped. Due to the reason that you need to set the list of VLANs mapped to the MSTI. The VLANs must be separated with comma and/or space.

A VLAN can only be mapped to one MSTI. An unused MSTI should just be left empty (i.e., not have any VLANs mapped to it).

To configure Spanning Tree MSTI in the web UI:

1. Go to Spanning Tree > MSTI Configuration.
2. Specify the configuration identification parameters in the field. Specify the VLANs Mapped blank field.
3. Click the **Apply** button to save the settings.
4. Click **Edit** to set STP CIST Port Configuration parameters.



STP MSTI Configuration

Configuration Identification

Configuration Name	00-c0-f2-aa-96-d7
Configuration Revision	0

MSTI Mapping

Instance	VLANs Mapped	MSTI Priority	MSTI Port
CIST	Unmapped VLANs are mapped to the CIST	32768	Edit
MSTI1	Example: 2,3-5,11,13,20-40	32768	Edit
MSTI2	Example: 2,3-5,11,13,20-40	32768	Edit
MSTI3	Example: 2,3-5,11,13,20-40	32768	Edit
MSTI4	Example: 2,3-5,11,13,20-40	32768	Edit
MSTI5	Example: 2,3-5,11,13,20-40	32768	Edit
MSTI6	Example: 2,3-5,11,13,20-40	32768	Edit
MSTI7	Example: 2,3-5,11,13,20-40	32768	Edit

Parameter descriptions:

Configuration Identification

Configuration Name : The name identifying the VLAN to MSTI mapping. Bridges must share the configuration name and configuration revision, as well as the VLAN-to-MSTI mapping configuration to share spanning trees for MSTI's (Intra-region). The name is at most 32 characters.

Configuration Revision : The revision of the MSTI configuration named above. This must be an integer between 0 and 65535.

MSTI Mapping

Instance : The bridge instance. The CIST is not available for explicit mapping, as it will receive the VLANs not explicitly mapped.

VLANs Mapped : The list of VLANs mapped to the MSTI. The VLANs can be given as a single (xx, xx being between 1 and 4094) VLAN, or a range (xx-yy), each of which must be separated with comma and/or space.
A VLAN can only be mapped to one MSTI. An unused MSTI should just be left empty (i.e., not having any VLANs mapped to it). Example: 2,5,20-40.

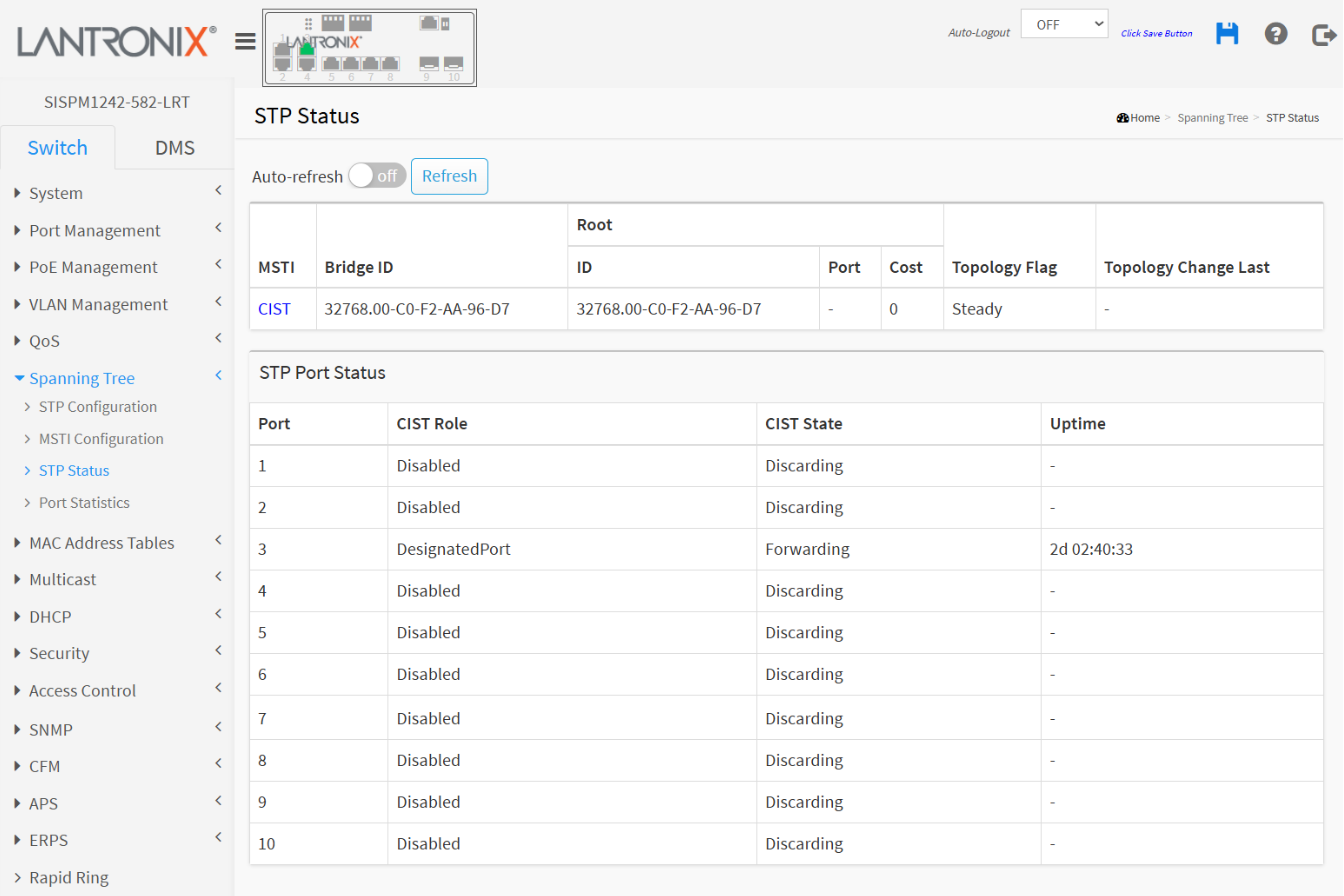
MSTI Priority : Controls the bridge priority. Lower numeric values have better priority. The bridge priority plus the MSTI instance number, concatenated with the 6-byte MAC address of the switch forms a Bridge Identifier.

MSTI Port : Click **Edit** to inspect and edit the current STP MSTI port configuration.

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 STP Bridges status in the web UI:

1. Go to Spanning Tree > STP Status.
2. **Auto-refresh** will refresh the page every 3 seconds. **Refresh** will refresh the page immediately.
3. Click the linked text **CIST** to go to the next page STP Detailed Bridge Status.



STP Status

MSTI	Bridge ID	Root			Topology Flag	Topology Change Last
		ID	Port	Cost		
CIST	32768.00-C0-F2-AA-96-D7	32768.00-C0-F2-AA-96-D7	-	0	Steady	-

STP Port Status

Port	CIST Role	CIST State	Uptime
1	Disabled	Discarding	-
2	Disabled	Discarding	-
3	DesignatedPort	Forwarding	2d 02:40:33
4	Disabled	Discarding	-
5	Disabled	Discarding	-
6	Disabled	Discarding	-
7	Disabled	Discarding	-
8	Disabled	Discarding	-
9	Disabled	Discarding	-
10	Disabled	Discarding	-

Parameter descriptions:

MSTI : The Bridge Instance. This is also a link to the STP Detailed Bridge Status page.

Bridge ID : The Bridge ID of this Bridge instance.

Root ID : The Bridge ID of the currently elected root bridge.

Root Port : The switch port currently assigned the root port role.

Root Cost : Root Path Cost. For the Root Bridge it is zero. For all other Bridges, it is the sum of the Port Path Costs on the least cost path to the Root Bridge.

Topology Flag : The current state of the Topology Change Flag of this Bridge instance.

Topology Change Last : The time since last Topology Change occurred.

STP Port Status

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

CIST Role : The current STP port role of the CIST port. The port role can be one of these values: AlternatePort, Backup Port, RootPort, DesignatedPort, or Disabled.

CIST State : The current STP port state of the CIST port. The port state can be one of these values: Blocking, Learning, or Forwarding.

Uptime : The time since the bridge port was last initialized.

CIST : Click the linked text to display the next page "STP Detailed Bridge Status".

STP Bridge Status

Bridge Instance : The Bridge instance (e.g., CIST, MST1, etc.).

Bridge ID : The Bridge ID of this Bridge instance.

Root ID : The Bridge ID of the currently elected root bridge.

Root Port : The switch port currently assigned the root port role.

Root Cost : Root Path Cost. For the Root Bridge this is zero. For all other Bridges, it is the sum of the Port Path Costs on the least cost path to the Root Bridge.

Regional Root : The Bridge ID of the currently elected regional root bridge, inside the MSTP region of this bridge. (*For the CIST instance only*).

Internal Root Cost : The Regional Root Path Cost. For the Regional Root Bridge this is zero. For all other CIST instances in the same MSTP region, it is the sum of the Internal Port Path Costs on the least cost path to the Internal Root Bridge. (For the CIST instance only.)

Topology Flag : The current state of the Topology Change Flag of this Bridge instance.

Topology Change Count : The number of times where the topology change flag has been set (during a one-second interval).

Topology Change Last : The time passed since the Topology Flag was last set.

CIST Ports & Aggregations State

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

Port ID : The port id as used by the STP protocol. This is the priority part and the logical port index of the bridge port.

Role : The current STP port role. The port role can be one of these values: AlternatePort, BackupPort, RootPort, or DesignatedPort.

State : The current STP port state. The port state can be one of these values: Discarding, Learning , or Forwarding.

Path Cost : The current STP port path cost. This will either be a value computed from the Auto setting, or any explicitly configured value.

Edge : The current STP port (operational) Edge Flag. An Edge Port is a switch port to which no Bridges are attached. The flag may be automatically computed or explicitly configured. Each Edge Port transits directly to the Forwarding Port State, since there is no possibility of it participating in a loop.

Point-to-Point : The current STP port point-to-point flag. A point-to-point port connects to a non-shared LAN media. The flag may be automatically computed or explicitly configured. The point-to-point properties of a port affect how fast it can transit to STP state.

Uptime : The time since the bridge port was last initialized.

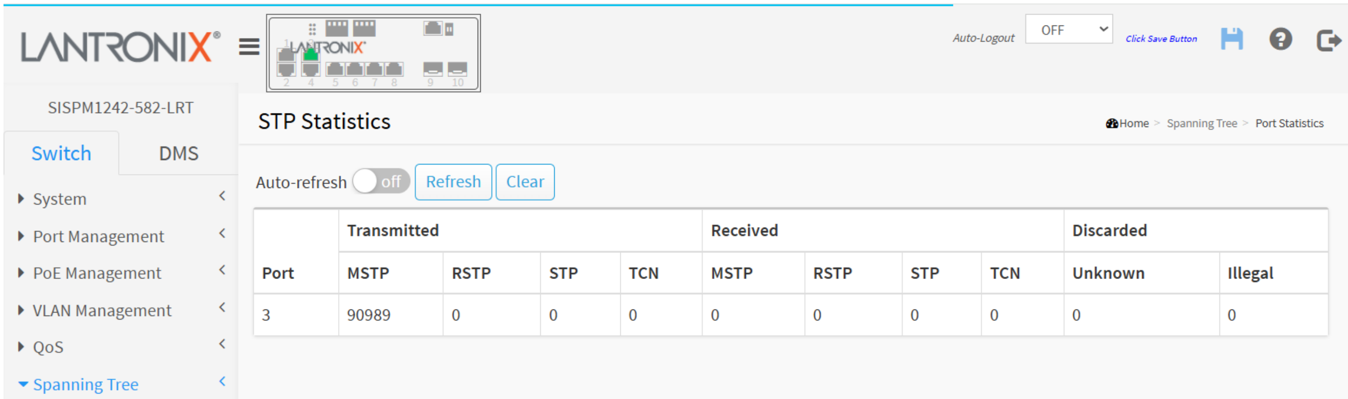
Port Statistics

This page displays the STP port statistics counters of bridge ports in the switch.

To display STP Port Statistics in the web UI:

1. Go to Spanning Tree > Port Statistics.

2. **Auto-refresh** will refresh the page every 3 seconds. **Refresh** will refresh the page immediately. **Clear** will clear all statistics.



STP Statistics

	Transmitted				Received				Discarded	
Port	MSTP	RSTP	STP	TCN	MSTP	RSTP	STP	TCN	Unknown	Illegal
3	90989	0	0	0	0	0	0	0	0	0

Parameter descriptions:

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

MSTP : The number of MSTP Configuration BPDUs received/transmitted on the port.

RSTP : The number of RSTP Configuration BPDUs received/transmitted on the port.

STP : The number of legacy STP Configuration BPDUs received/transmitted on the port.

TCN : The number of (legacy) Topology Change Notification BPDUs received/transmitted on the port.

Discarded Unknown : The number of unknown Spanning Tree BPDUs received (and discarded) on the port.

Discarded Illegal : The number of illegal Spanning Tree BPDUs received (and discarded) on the port.

9. MAC Address Tables

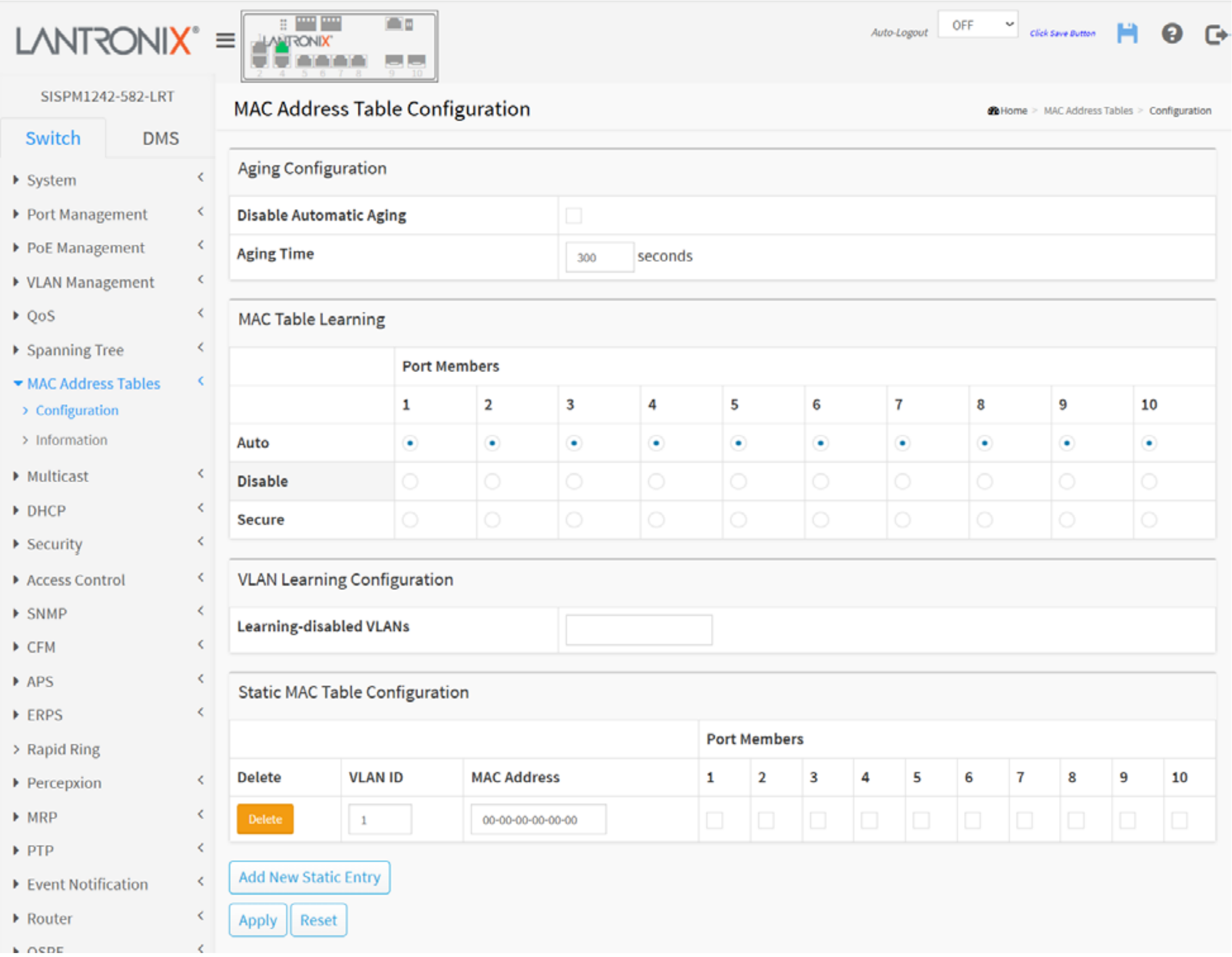
Configuration

Switching of frames is based on the destination MAC address (DMAC) contained in the frame. The switch builds a table that maps MAC addresses to switch ports for knowing which ports the frames should go to (based on the DMAC address in the frame). This table contains both static and dynamic entries. The static entries are configured by the network administrator if the administrator wants to do a fixed mapping between the DMAC address and switch ports.

The frames also contain a source MAC address (SMAC), which shows the MAC address of the equipment sending the frame. The SMAC address is used by the switch to automatically update the MAC table with these dynamic MAC addresses. Dynamic entries are removed from the MAC table if no frame with the corresponding SMAC address have been seen after a configurable age time.

To configure MAC Address Table parameters in the web UI:

1. Go to MAC Address Tables > Configuration.
2. Configure the MAC Address Table settings per your requirement.
3. Configure one or more static entries in the Static MAC Table.
4. Click **Apply**.



MAC Address Table Configuration

Aging Configuration

Disable Automatic Aging	□
Aging Time	300 seconds

MAC Table Learning

	Port Members									
	1	2	3	4	5	6	7	8	9	10
Auto	●	●	●	●	●	●	●	●	●	●
Disable	○	○	○	○	○	○	○	○	○	○
Secure	○	○	○	○	○	○	○	○	○	○

VLAN Learning Configuration

Learning-disabled VLANs	

Static MAC Table Configuration

			Port Members									
Delete	VLAN ID	MAC Address	1	2	3	4	5	6	7	8	9	10
Delete	1	00-00-00-00-00-00	□	□	□	□	□	□	□	□	□	□

Parameter descriptions:

Aging Configuration

By default, dynamic entries are removed from the MAC table after 300 seconds. This removal is also called aging.

Configure aging time by entering a value here in seconds. The valid range is 10 to 1000000 seconds.

Disable the automatic aging of dynamic entries by checking the **Disable Automatic Aging** box.

MAC Table Learning

If the learning mode for a given port is grayed out, another module is in control of the mode, so that it cannot be changed by the user. An example of such a module is the MAC-Based Authentication under 802.1X. Each port can do learning based on the following settings:

Auto : Learning is done automatically as soon as a frame with unknown SMAC is received.

Disable : No learning is done.

Secure : Only static MAC entries are learned; all other frames are dropped.

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

VLAN Learning Configuration

Learning-disabled VLANS : This field shows the Learning-disabled VLANs. When a NEW MAC arrives into a learning disabled VLAN, the MAC won't be learned. By the default, the field is empty. More VLANs may be created by using a list syntax where the individual elements are separated by commas. Ranges are specified with a dash separating the lower and upper bound. The following example will create VLANs 1, 10, 11, 12, 13, 200, and 300: 1,10-13,200,300. Spaces are allowed in between the delimiters.

Static MAC Table Configuration : The static entries in the MAC table are shown in this table. The static MAC table can contain up to 64 entries.

Delete button: Select to delete the entry on the next save.

Add New Static Entry button: Add a new entry to the static MAC table. Specify the VLAN ID, MAC address, and port members for the new entry. Click **Apply** to save the configuration.

VLAN ID : The VLAN ID of the entry.

MAC Address : The MAC address of the entry.

Port Members : Check or uncheck as needed to indicate which ports are members of the entry.

Information

This page displays entries in the MAC Address Table. The MAC Address Table contains up to 8192 entries, and is sorted first by VLAN ID, then by MAC address.

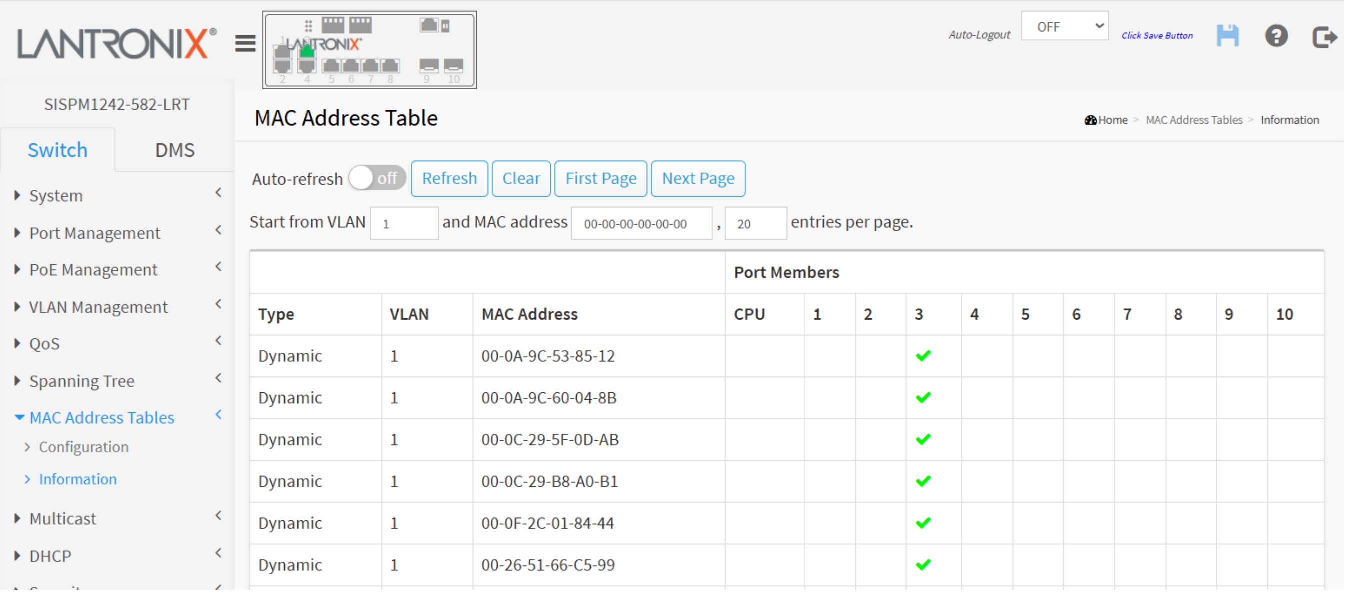
Navigating the MAC Address Table

Each page shows up to 999 entries from the MAC table, selected via the "*entries per page*" input field. When first visited, the web page will show the first 20 entries from the beginning of the MAC Table. The first entry displayed will be the one with the lowest VLAN ID and the lowest MAC address found in the MAC Table.

The "*Start from MAC address*" and "*VLAN*" input fields allow you to select the starting point in the MAC Address Table. Clicking the **Refresh** button will update the displayed table starting from that or the closest next MAC Table match. 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.

To display the MAC Address Table in the web UI:

1. Go to MAC Address Table > Information.
2. **Auto-refresh** will refresh the page every 3 seconds. **Refresh** will refresh the page immediately. **Clear** will flush the dynamic entries.



MAC Address Table

Auto-refresh off

Start from VLAN 1 and MAC address 00-00-00-00-00-00 , 20 entries per page.

			Port Members										
Type	VLAN	MAC Address	CPU	1	2	3	4	5	6	7	8	9	10
Dynamic	1	00-0A-9C-53-85-12				✓							
Dynamic	1	00-0A-9C-60-04-8B				✓							
Dynamic	1	00-0C-29-5F-0D-AB				✓							
Dynamic	1	00-0C-29-B8-A0-B1				✓							
Dynamic	1	00-0F-2C-01-84-44				✓							
Dynamic	1	00-26-51-66-C5-99				✓							

Parameter descriptions:

Type : Indicates whether the entry is a static entry or a dynamic entry.

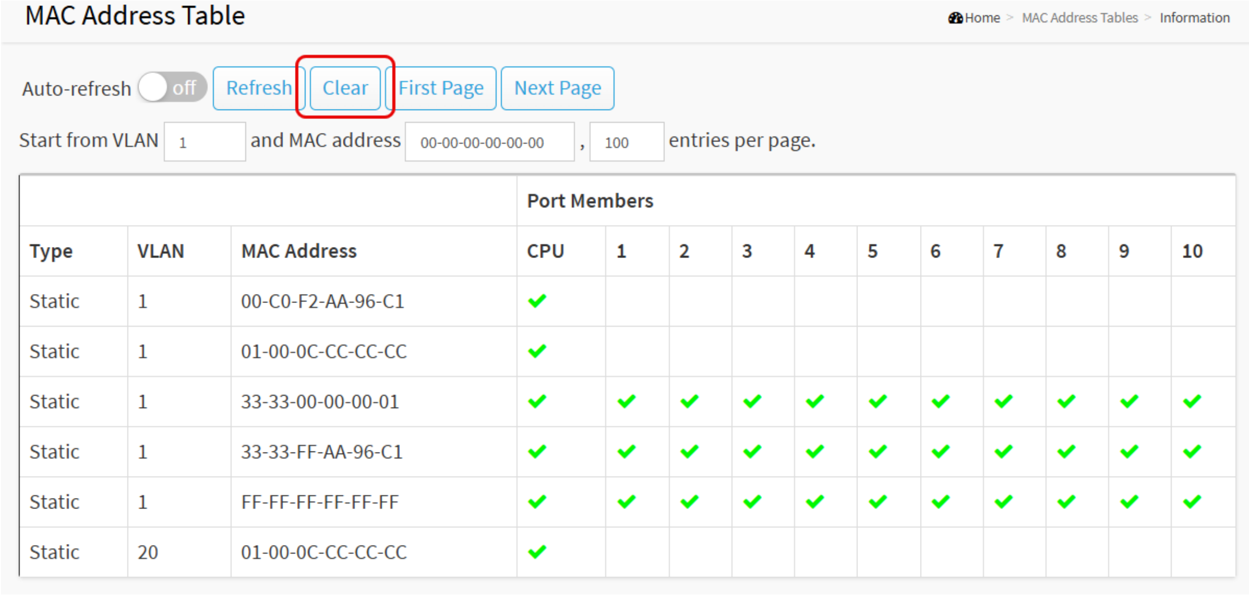
VLAN : The VLAN ID of the entry.

MAC Address : The MAC address of the entry.

Port Members : The ports that are members of the entry.

Example - To view Static Entries:

Click **Clear** to flush all dynamic entries. The static entries will be retained in the list.



MAC Address Table

Start from VLAN 1 and MAC address 00-00-00-00-00-00 , 100 entries per page.

			Port Members										
Type	**VLAN**	**MAC Address**	**CPU**	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**
Static	1	00-C0-F2-AA-96-C1	✓										
Static	1	01-00-0C-CC-CC-CC	✓										
Static	1	33-33-00-00-00-01	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Static	1	33-33-FF-AA-96-C1	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Static	1	FF-FF-FF-FF-FF-FF	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Static	20	01-00-0C-CC-CC-CC	✓										

00-C0-F2-AA-96-C1: own switch MAC address, in this example

01-00-0C-CC-CC-CC: Cisco multicast address for certain device discovery protocols (UDLD, CDP)

33-33-00-00-00-01 : Destination MAC (for IPv6 Router Advertisement)

33-33-FF-73-01-29 : Destination MAC (for IPv6 Neighbor Solicitation)

33-33-FF-AA-96-C1: your switch MAC address (for IPv6 global IP)

FF-FF-FF-FF-FF-FF: for Broadcast.

10. Multicast

IGMP Snooping

This function is used to establish the multicast groups to forward the multicast packet to the member ports, and, in nature, avoids wasting the bandwidth while IP multicast packets are running over the network. This is because a switch that does not support IGMP or IGMP Snooping cannot tell the multicast packet from the broadcast packet, so it can only treat them all as the broadcast packet. Without IGMP Snooping, the multicast packet forwarding function is plain and nothing is different from broadcast packet.

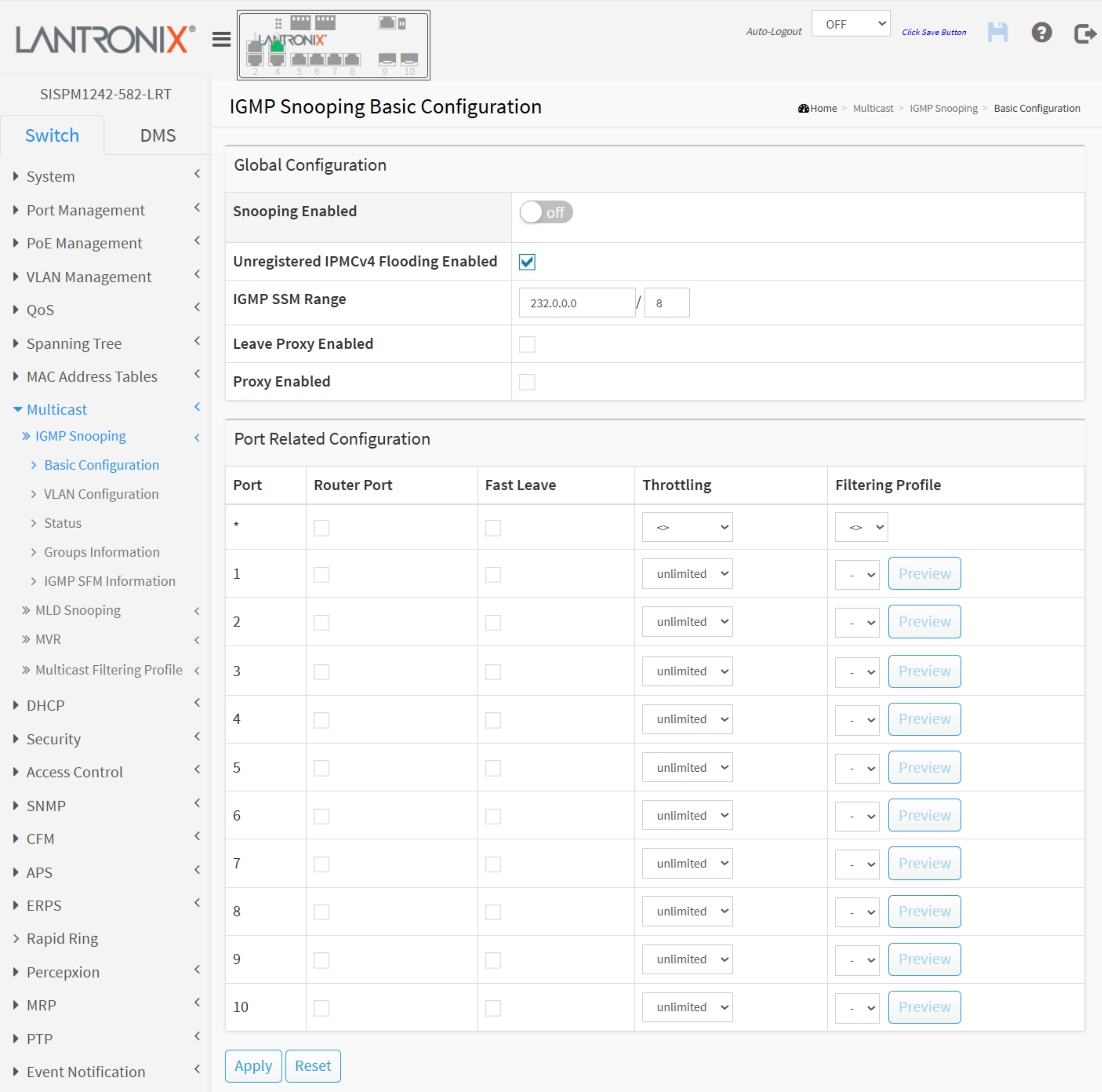
A switch supporting IGMP Snooping with the functions of query, report and leave, a type of packet exchanged between IP Multicast Router/Switch and IP Multicast Host, can update the information of the Multicast table when a member (port) joins or leaves an IP Multicast Destination Address. With this function, once a switch receives an IP multicast packet, it will forward the packet to the members who joined in a specified IP multicast group before. The packets will be discarded by the IGMP Snooping if the user transmits multicast packets to the multicast group that had not been built up in advance. IGMP mode enables the switch to issue IGMP function that you enable IGMP proxy or snooping on the switch, which connects to a router closer to the root of the tree.

Basic Configuration

This page lets you set basic IGMP snooping on the switch, which connects to a router closer to the root of the tree. This interface is the upstream interface. The router on the upstream interface must be running IGMP.

To configure IGMP Snooping parameters in the web UI:

1. Go to Multicast > IGMP Snooping > Basic Configuration.
2. Set the IGMP Snooping Global Configuration parameters.
3. Set the Port Related Configuration parameters.
4. Click **Apply** to save the configuration.



IGMP Snooping Basic Configuration

Global Configuration

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

Port Related Configuration

Port	Router Port	Fast Leave	Throttling	Filtering Profile
*	□	□	<>	<>
1	□	□	unlimited	- Preview
2	□	□	unlimited	- Preview
3	□	□	unlimited	- Preview
4	□	□	unlimited	- Preview
5	□	□	unlimited	- Preview
6	□	□	unlimited	- Preview
7	□	□	unlimited	- Preview
8	□	□	unlimited	- Preview
9	□	□	unlimited	- Preview
10	□	□	unlimited	- Preview

Apply Reset

Parameter descriptions:

Global Configuration

Snooping Enabled : Enable the Global IGMP Snooping.

Unregistered IPMCv4 Flooding Enabled : Enable unregistered IPMCv4 traffic flooding. Unregistered IPMCv4 traffic is so-called unknown multicast. After selected, the unregistered multicast stream will be forwarded like normal packets. Once you un-selected it, such stream will be discarded

IGMP SSM Range : The SSM (Source-Specific Multicast) Range allows the SSM-aware hosts and routers run the SSM service model for the groups in the address range. Format: (IP address/ sub mask)

Leave Proxy Enabled : Enable IGMP Leave Proxy. This feature can be used to avoid forwarding unnecessary leave messages to the router side.

Proxy Enabled : Enable IGMP Proxy. This feature can be used to avoid forwarding unnecessary join and leave messages to the router side.

Port Related Configuration

Port : Shows the physical Port index of switch.

Router Port : Specify which ports act as router ports. A router port is a port on the Ethernet switch that leads towards the Layer 3 multicast device or IGMP querier. If an aggregation member port is selected as a router port, the whole aggregation will act as a router port.

Fast Leave : Enable the fast leave on the port. 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 host is connected to the specific port.

Throttling : Enable to limit the number of multicast groups to which a switch port can belong.

Filtering Profile : Select the profile for this port. Click to preview the page which list the rules associated with the selected profile.

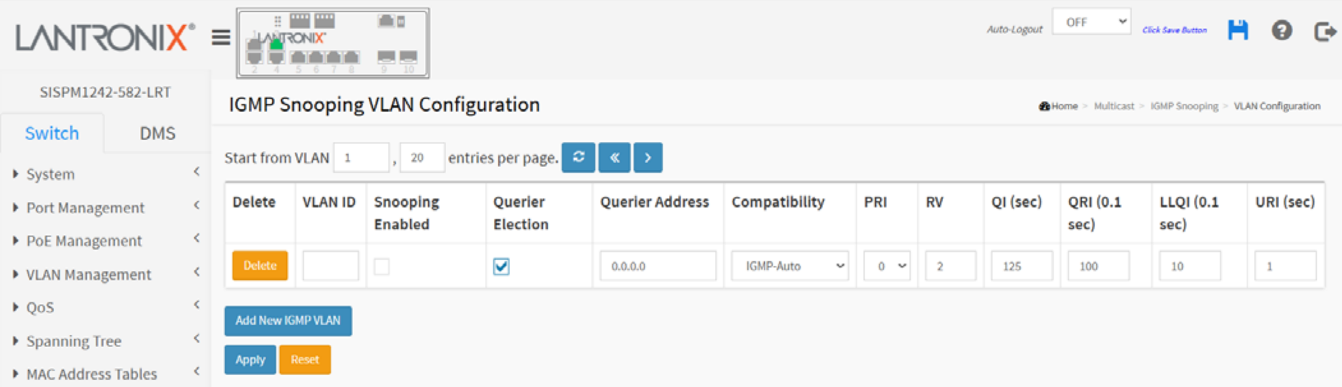
VLAN Configuration

This page lets you enable and configure up to 64 VLANs for per-VLAN IGMP Snooping.

Each page shows 20 entries from the VLAN table. When first visited, the web page will show the first 20 entries from the beginning of the VLAN Table. Clicking the Refresh button will update the displayed table starting from that or the next closest VLAN Table match. The Next Page will use the last entry of the currently displayed entry as a basis for the next lookup. When the end is reached the text "No more entries" is shown in the displayed table. Use the First Page button to start over.

To configure IGMP Snooping VLAN in the web UI:

1. Go to Multicast > IGMP Snooping > VLAN Configuration.
2. Configure the parameters.
3. Click the Apply button.



IGMP Snooping VLAN Configuration

Start from VLAN 1 , 20 entries per page.

Delete	VLAN ID	Snooping Enabled	Querier Election	Querier Address	Compatibility	PRI	RV	QI (sec)	QRI (0.1 sec)	LLQI (0.1 sec)	URI (sec)
Delete		□	☑	0.0.0.0	IGMP-Auto	0	2	125	100	10	1

Add New IGMP VLAN

Apply Reset

Parameter descriptions:

Add New IGMP VLAN button: Click to add new IGMP VLAN. Specify the VID and configure the new entry. Click **Apply**. The specific IGMP VLAN starts working after the corresponding static VLAN is also created.

VLAN ID : The VLAN ID of the entry

IGMP Snooping Enabled : Enable the per-VLAN IGMP Snooping. Up to 64 VLANs can be selected for IGMP Snooping.

Querier Election : Enable to join IGMP Querier election in the VLAN. Disable to act as an IGMP Non-Querier.

Querier Address : Define the IPv4 address as source address used in IP header for IGMP Querier election.

When the Querier address is not set, system uses IPv4 management address of the IP interface associated with this VLAN. When the IPv4 management address is not set, system uses the first available IPv4 management address. Otherwise, the switch uses a pre-defined value. By default, this value will be 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, and Forced IGMPv3. The default compatibility value is IGMP-Auto.

Priority of Interface: It 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), default interface priority value is 0.

Rv : Robustness Variable. The RV allows tuning for the expected packet loss on a network. The valid range is 1 to 255; the default RV value is 2.

QI (sec) : Query Interval. The QI is the interval between General Queries sent by the Querier. The valid range is 1 to 31744 seconds; the default QI is 125 seconds.

QRI (0.1 sec) : Query Response Interval. The Max Response Time used to calculate the Max Resp Code inserted into the periodic General Queries. The valid range is 0 to 31744 in tenths of seconds; the default QRI interval is 100 in tenths of seconds (10 seconds).

LLQI (0.1 sec) : Last Member Query Interval. The LLQI is the time value represented by the Last Member Query Interval, multiplied by the Last Member Query Count. The valid range is 0 to 31744 in tenths of seconds; the default LLQI is 10 in tenths of seconds (1 second).

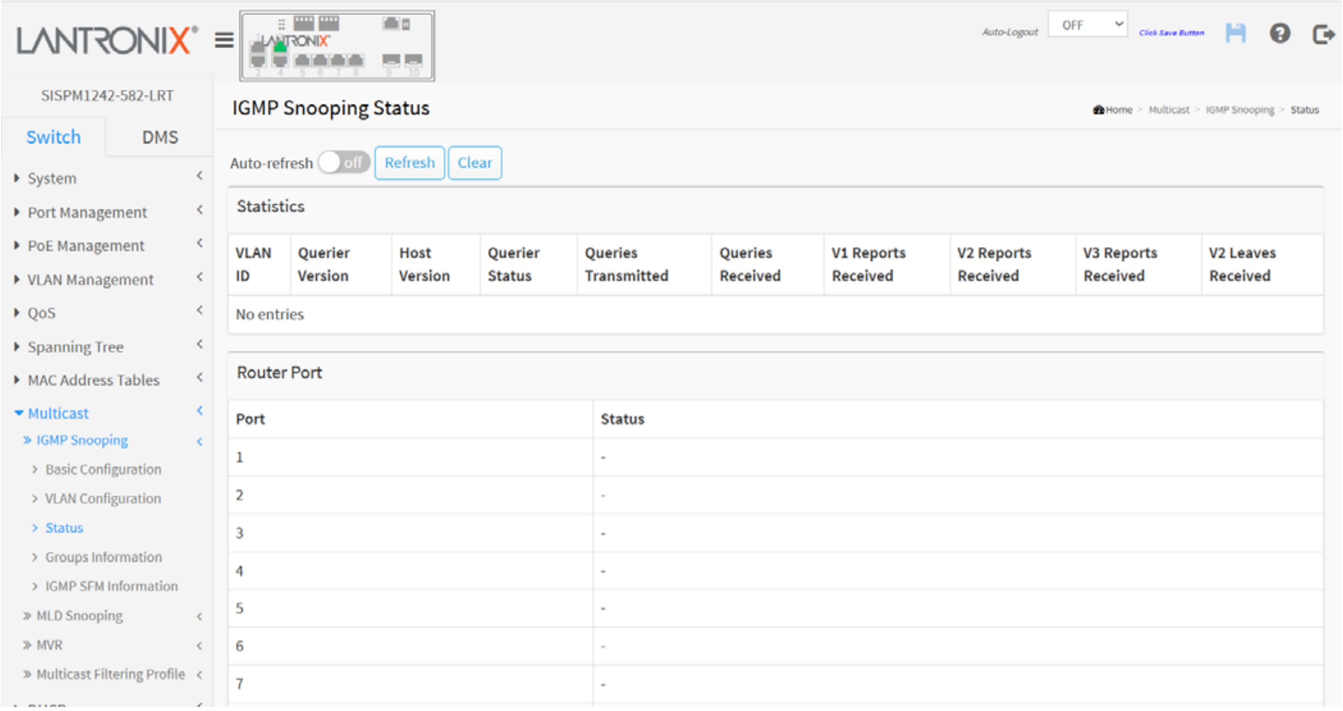
URI (sec) : Unsolicited Report Interval. The URI is the time between repetitions of a host's initial report of membership in a group. The valid range is 0 to 31744 seconds; the default URI is 1 second.

Snooping Status

This page displays IGMP Snooping Status.

To display IGMP Snooping status in the web UI:

1. Go to Multicast > IGMP Snooping > Status.
2. **Auto-refresh** will refresh the page every 3 seconds. **Refresh** will refresh the page immediately. **Clear** will clear the statistic counters.



IGMP Snooping Status

Statistics

VLAN ID	Querier Version	Host Version	Querier Status	Queries Transmitted	Queries Received	V1 Reports Received	V2 Reports Received	V3 Reports Received	V2 Leaves Received
No entries									

Router Port

Port	Status
1	-
2	-
3	-
4	-
5	-
6	-
7	-

Parameter descriptions:

<u>Statistics</u>

VLAN ID : The VLAN ID of the entry.

Querier Version : Working Querier Version currently.

Host Version : Working Host Version currently.

Querier Status : Shows the Querier status as "ACTIVE" or "IDLE". "DISABLE" denotes the specific interface is administratively disabled.

Queries Transmitted : The number of Transmitted Queries.

Queries Received : The number of Received Queries.

V1 Reports Received : The number of Received V1 Reports.

V2 Reports Received : The number of Received V2 Reports.

V3 Reports Received : The number of Received V3 Reports.

V2 Leaves Received : The number of Received V2 Leaves.

<u>Router Port</u>

Displays which ports act as router ports. A router port is a port on the Ethernet switch that leads towards the Layer 3 multicast device or IGMP querier.

- ***Static*** denotes the specific port is configured to be a router port.
- ***Dynamic*** denotes the specific port is learnt to be a router port.
- ***Both*** denote the specific port is configured or learnt to be a router port.

Port : The switch port number.

Status : Indicate whether a specific port is a router port or not.

Snooping Group Information

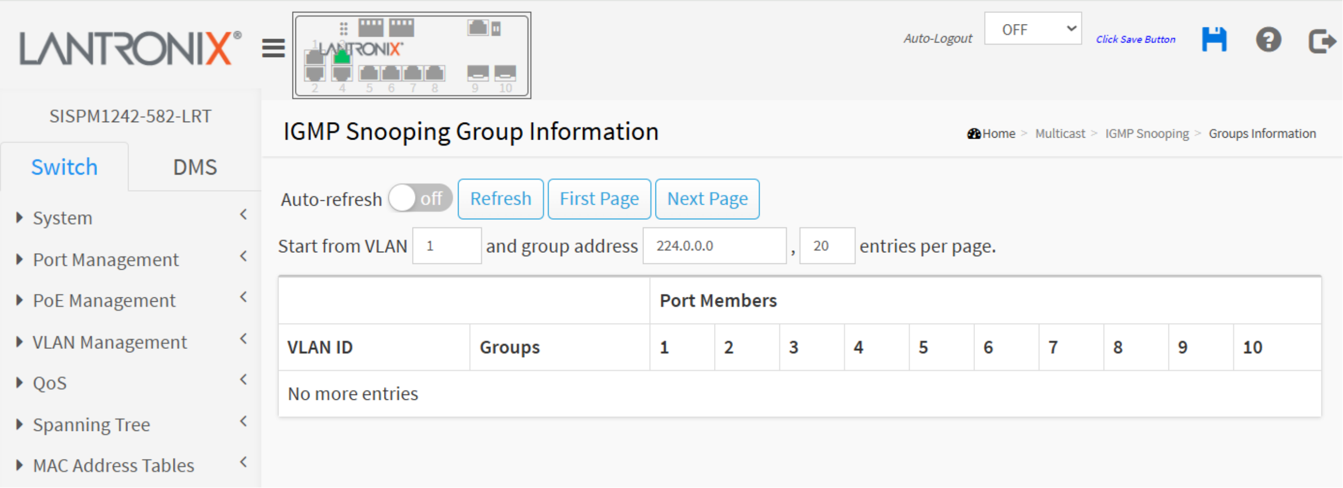
This page displays IGMP Snooping Group Information. Entries in the IGMP Group Table are shown on this page. The IGMP Group Table is sorted first by VLAN ID, and then by group. This will use the last entry of the currently displayed table as a basis for the next lookup. When the end is reached the text "No more entries" is shown in the displayed table.

Each page shows up to 99 entries from the IGMP Group table, selected through the "entries per page" input field. When first visited, the web page will show the first 20 entries from the beginning of the IGMP Group Table.

The "Start from VLAN", and "group" input fields allow the user to select the starting point in the IGMP Group Table. Clicking the **Refresh** button will update the displayed table starting from that or the closest next IGMP Group Table match. In addition, the two input fields will - upon a **Refresh** button click - assume the value of the first displayed entry, allowing for continuous refresh with the same start address.

To display the IGMP Snooping Group Information in the web UI:

1. Go to Multicast > IGMP Snooping > Group Information.
2. **Auto-refresh** will refresh the page every 3 seconds. **Refresh** will refresh the page immediately.
3. Use the page controls and “Start from” entry fields to help you navigate through the list.



IGMP Snooping Group Information

Start from VLAN 1 and group address 224.0.0.0 , 20 entries per page.

		Port Members									
VLAN ID	Groups	1	2	3	4	5	6	7	8	9	10
No more entries											

Parameter descriptions:

VLAN ID : VLAN ID of the group.

Groups : Group address of the group displayed.

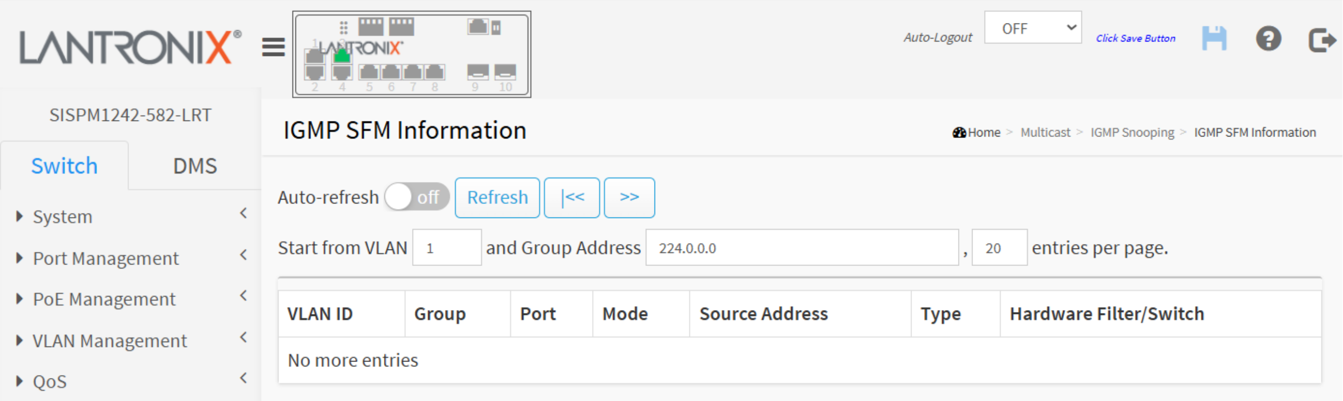
Port Members : Ports under this group.

SFM Information

Entries in the IGMP SFM Information table are shown on this page. The IGMP SFM (Source-Filtered Multicast) Information Table also contains the SSM (Source-Specific Multicast) information. This table is sorted first by VLAN ID, then by group, and then by Port. Different source addresses belonging to the same group are treated as a single entry.

To display IGMP SFM Information in the web UI:

1. Go to Multicast > IGMP Snooping > IGMP SFM Information
2. **Auto-refresh** will refresh the page every 3 seconds. **Refresh** will refresh the page immediately.
3. Use the page controls and “Start from” entry fields to help you navigate through the list.



IGMP SFM Information

Start from VLAN 1 and Group Address 224.0.0.0 , 20 entries per page.

VLAN ID	Group	Port	Mode	Source Address	Type	Hardware Filter/Switch
No more entries						

Parameter descriptions:

VLAN ID : The VLAN ID of the group.

Group : The Group address of the group displayed.

Port : The switch port number.

Mode : Indicates the filtering mode maintained per (VLAN ID, port number, Group Address) basis. It can be either *Include* or *Exclude*.

Source Address : IP Address of the source. The system currently supports 128 IP source addresses for filtering.

Type : Indicates the Type; either *Allow* or *Deny*.

Hardware Filter/Switch : Indicates whether data plane destined to the specific group address from the source IPv4 address can be handled by chip.

MLD Snooping

Multicast Listener Discovery (MLD) is a component of the Internet Protocol Version 6 (IPv6) suite. MLD is used by IPv6 routers for discovering multicast listeners on a directly attached link, much like Internet Group Management Protocol (IGMP) is used in IPv4. The protocol is embedded in ICMPv6 instead of using a separate protocol. MLDv1 is like IGMPv2 and MLDv2 is like IGMPv3. The protocol is described in IETF RFC 3810 which has been updated by RFC 4604.

A network node that acts as a source of IPv6 multicast traffic is only an indirect participant in MLD snooping; it just provides multicast traffic, and MLD doesn't interact with it. (Note, however, that in an application like desktop conferencing a network node may act as both a source and an MLD host; but MLD interacts with that node only in its role as an MLD host.)

A source node creates multicast traffic by sending packets to a multicast address. In IPv6, addresses with the first eight bits set (that is, "FF" as the first two characters of the address) are multicast addresses, and any node that listens to such an address will receive the traffic sent to that address. Application software running on the source and destination systems cooperates to determine what multicast address to use. (Note that this is a function of the application software, not of MLD.)

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

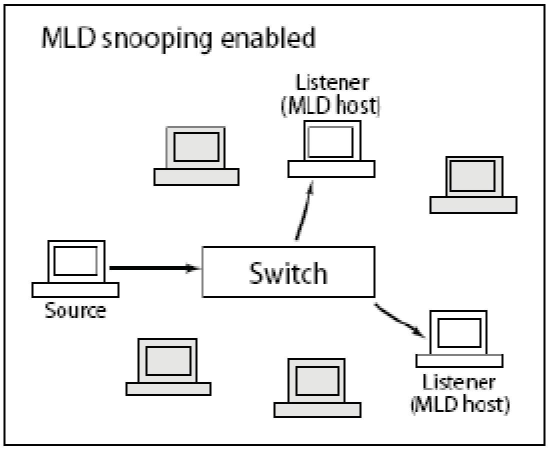
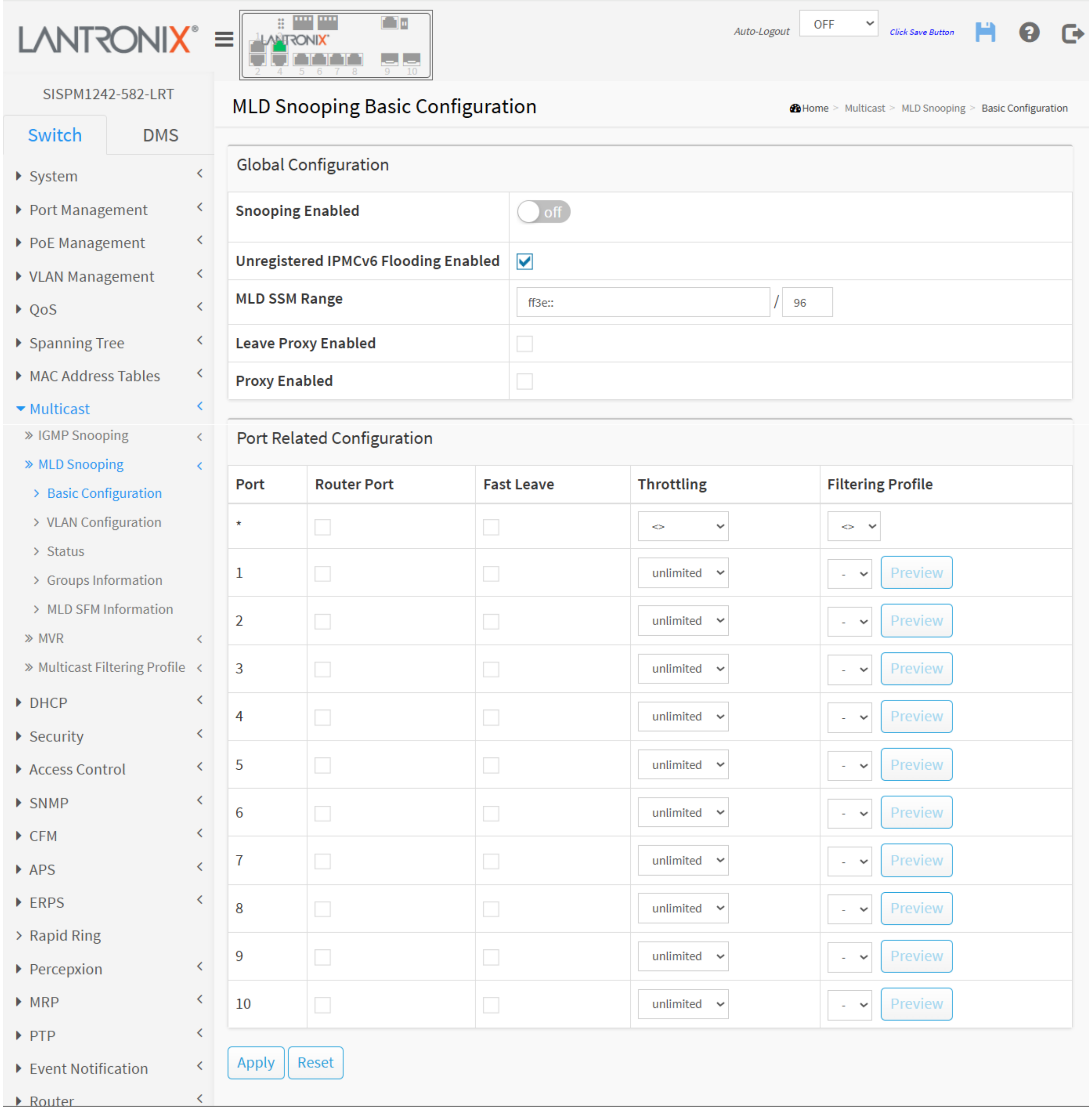


Figure 10-1 MLD snooping enabled

Basic Configuration

To configure MLD Snooping in the web UI:

1. Go to Multicast > MLD Snooping> Basic Configuration.
2. Set the Global Configuration parameters.
3. Set the Port Related Configuration parameters.
4. Click the **Apply** button to save the settings.



MLD Snooping Basic Configuration

Global Configuration

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

Port Related Configuration

Port	Router Port	Fast Leave	Throttling	Filtering Profile
*	□	□	<>	<>
1	□	□	unlimited	- Preview
2	□	□	unlimited	- Preview
3	□	□	unlimited	- Preview
4	□	□	unlimited	- Preview
5	□	□	unlimited	- Preview
6	□	□	unlimited	- Preview
7	□	□	unlimited	- Preview
8	□	□	unlimited	- Preview
9	□	□	unlimited	- Preview
10	□	□	unlimited	- Preview

Apply Reset

Parameter descriptions :

Global Configuration

Snooping Enabled : Set to 'on' to enable MLD Snooping globally.

Unregistered IPMCv6 Flooding Enabled : Enable unregistered IPMCv6 traffic flooding. The flooding control takes effect only when MLD Snooping is enabled. When MLD Snooping is disabled, unregistered IPMCv6 traffic flooding is always active despite this setting.

MLD SSM Range : The SSM (Source-Specific Multicast) Range allows the SSM-aware hosts and routers run the SSM service model for the groups in the address (using IPv6 Address) range.

Leave Proxy Enabled : Check the box to enable MLD Leave Proxy. This feature can be used to avoid forwarding unnecessary leave messages to the router side.

Proxy Enabled : Check the box to enable MLD Proxy. This feature can be used to avoid forwarding unnecessary join and leave messages to the router side.

Port Related Configuration

Router Port : Specify which ports act as router ports. A router port is a port on the Ethernet switch that leads towards the Layer 3 multicast device or MLD querier. If an aggregation member port is selected as a router port, the whole aggregation will act as a router port.

Fast Leave : Check to enable fast leave on the port.

Throttling : Enable to limit the number of multicast groups to which a switch port can belong.

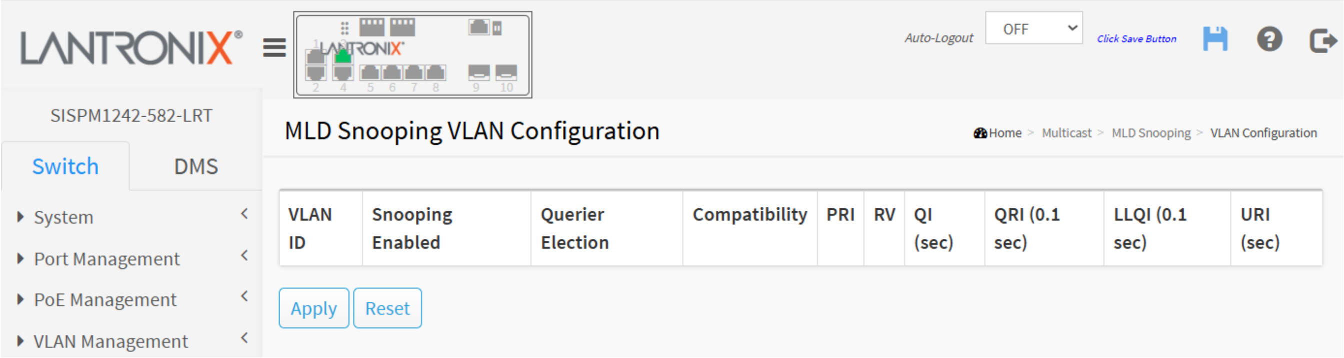
Filtering Profile : You can select profile when you edit in Multicast Filtering Profile.

VLAN Configuration

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

To set MLD Snooping VLAN parameters in the web UI:

1. Go to Multicast > MLD Snooping > VLAN Configuration.
2. Check or uncheck the Snooping Enabled checkbox and the Querier Election checkbox as required.
3. Select the Compatibility mode and set the PRI, RV, QI, QRI, LLQI and URI parameters.
4. Click the **Apply** button when done.



MLD Snooping VLAN Configuration

VLAN ID	Snooping Enabled	Querier Election	Compatibility	PRI	RV	QI (sec)	QRI (0.1 sec)	LLQI (0.1 sec)	URI (sec)

Parameter descriptions:

VLAN ID : The VLAN ID of the entry.

Snooping Enabled : Check to enable per-VLAN MLD Snooping. Up to 64 VLANs can be selected for MLD Snooping.

Querier Election : Enable to join MLD Querier election in the VLAN. Disable to act as a MLD Non-Querier.

Compatibility : Compatibility is maintained by hosts and routers taking appropriate actions depending on the versions of IGMP operating on hosts and routers within a network. The allowed selections are MLD-Auto, Forced IGMPv1, or Forced IGMPv2. The default compatibility value is MLD-Auto.

RV : Robustness Variable. The RV allows tuning for the expected packet loss on a network. The valid range is 1 to 255; the default RV value is 2.

QI (sec) : Query Interval. The QI is the interval between General Queries sent by the Querier. The valid range is 1 to 31744 seconds; the default QI is 125 seconds.

QRI (0.1sec) : Query Response Interval. The Max Response Time used to calculate the Max Resp Code inserted into the periodic General Queries. The valid range is 0 to 31744 in tenths of seconds; the default QRI is 100 in tenths of a second (10 seconds).

LLQI (LMQI for IGMP) : Last Member Query Interval. The Last Member Query Time is the time value represented by the Last Member Query Interval, multiplied by the Last Member Query Count. The valid range is 0 to 31744 in tenths of a second; the default LLQI is 10 in tenths of seconds (1 second).

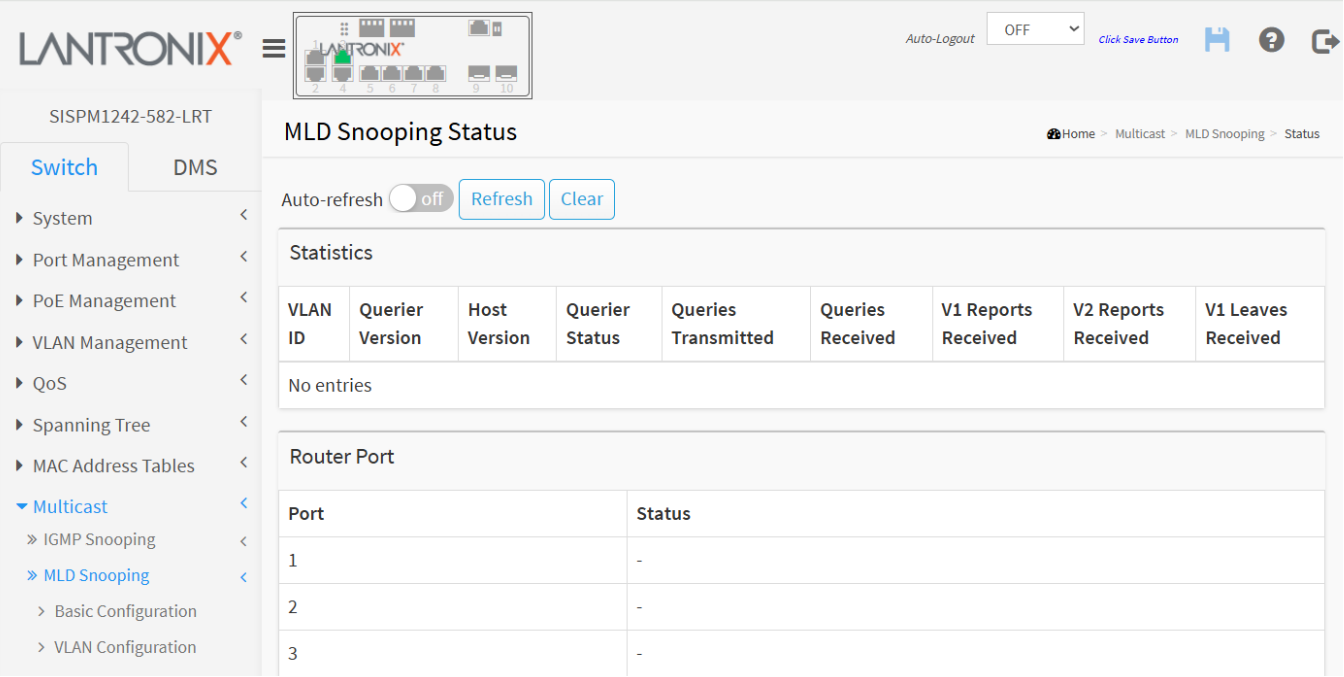
URI (sec) : Unsolicited Report Interval. The URI is the time between repetitions of a host's initial report of membership in a group. The valid URI range is 0 to 31744 seconds; the default is 1 second.

Status

This page provides MLD Snooping status.

This page lets you view MLD Snooping Status and detail information. To display MLD Snooping Status in the web UI:

1. Go to Multicast > MLD Snooping > Status.
2. **Auto-refresh** will refresh the page every 3 seconds. **Refresh** will refresh the page immediately. **Clear** will reset all the statistics.



MLD Snooping Status

Statistics

VLAN ID	Querier Version	Host Version	Querier Status	Queries Transmitted	Queries Received	V1 Reports Received	V2 Reports Received	V1 Leaves Received
No entries								

Router Port

Port	Status
1	-
2	-
3	-

Parameter descriptions:

<u>Statistics</u>

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". The status "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.

- ***Static*** denotes the specific port is configured to be a router port.
- ***Dynamic*** denotes the specific port is learnt to be a router port.
- ***Both*** denote the specific port is configured or learnt to be a router port.

Port: The switch port number.

Status: Indicate whether specific port is a router port or not.

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.

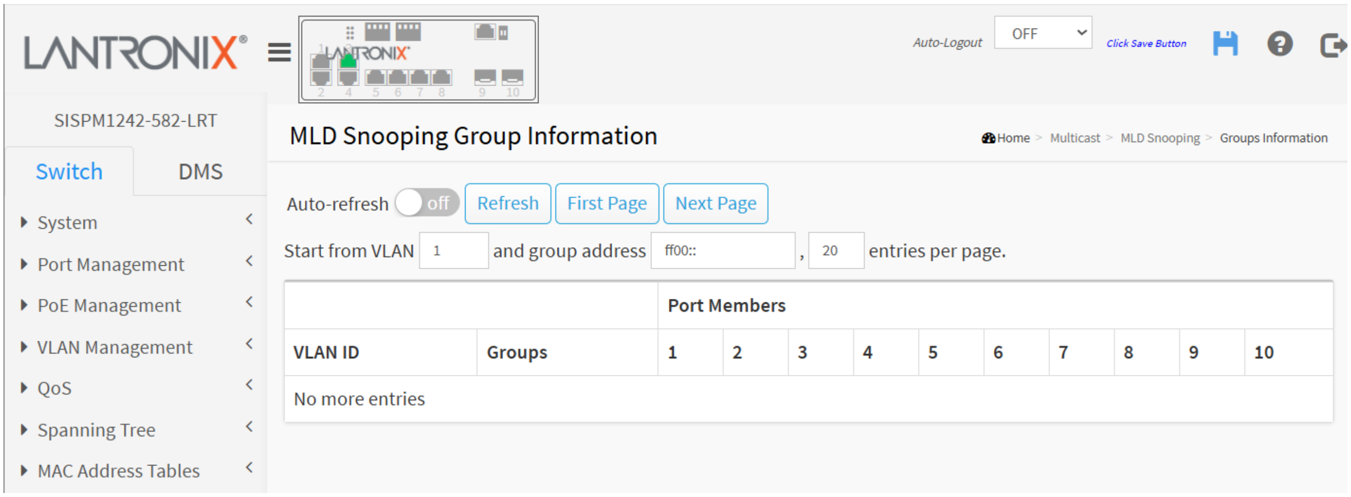
Each page shows up to 99 entries from the MLD Group table, default being 20, selected through the "entries per page" input field. When first visited, the web page will show the first 20 entries from the beginning of the MLD Group Table.

The "Start from VLAN", and "group" input fields allow the user to select the starting point in the MLD Group Table. Clicking the **Refresh** button will update the displayed table starting from that or the closest next MLD Group Table match. In addition, the two input fields will - upon a **Refresh** button click - assume the value of the first displayed entry, allowing for continuous refresh with the same start address.

The Next Page will use the last entry of the currently displayed table as a basis for the next lookup. When the end is reached the text.

To display MLD Snooping Group information in the web UI:

1. Go to Multicast > MLD Snooping > Group Information.
2. **Auto-refresh** will refresh the page every 3 seconds. **Refresh** will refresh the page immediately.
3. Use the page controls and “Start from” entry fields to help you navigate through the list.



MLD Snooping Group Information

Start from VLAN 1 and group address ff00:: , 20 entries per page.

		Port Members									
VLAN ID	Groups	1	2	3	4	5	6	7	8	9	10
No more entries											

Parameter descriptions:

VLAN ID : The VLAN ID of the group.

Groups : Group address of the group displayed.

Port Members : Ports under this group.

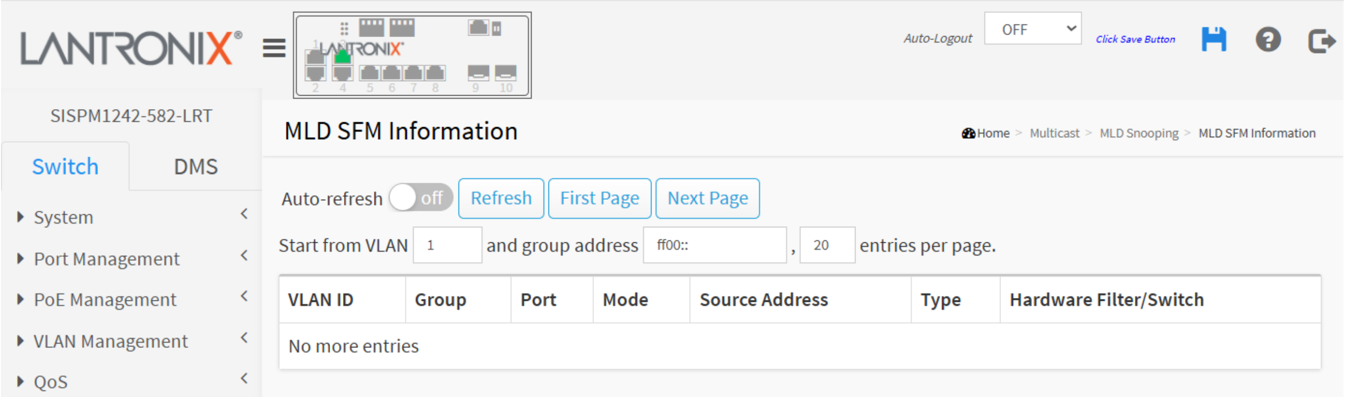
Show entries: Select the number of items to display per page.

MLD SFM Information

Entries in the MLD SFM Information Table are shown on this page. The MLD SFM (Source-Filtered Multicast) Information Table also contains the SSM (Source-Specific Multicast) information. This table is sorted first by VLAN ID, then by group, and then by Port. Different source addresses belong to the same group are treated as single entry.

To display MLD SFM Information in the web UI:

1. Go to Multicast > MLD Snooping > MLD SFM Information.
2. **Auto-refresh** will refresh the page every 3 seconds. **Refresh** will refresh the page immediately.
3. Use the page controls and “Start from” entry fields to help you navigate through the list.



MLD SFM Information

Start from VLAN 1 and group address ff00:: , 20 entries per page.

VLAN ID	Group	Port	Mode	Source Address	Type	Hardware Filter/Switch
No more entries						

Parameter descriptions:

VLAN ID : The VLAN ID of the group.

Group : The IP Multicast Group address.

Port : The Switch port number.

Mode : Indicates the filtering mode maintained per (VLAN ID, port number, Group Address) basis. It can be either Include or Exclude.

Source Address : The IP Address of the source. Currently, system limits the total number of IP source addresses for filtering to be 128.

Type : Indicates the Type. It can be either Allow or Deny.

Hardware Filter/Switch: Indicates whether data plane destined to the specific group address from the source IPv6 address could be handled by chip or not.

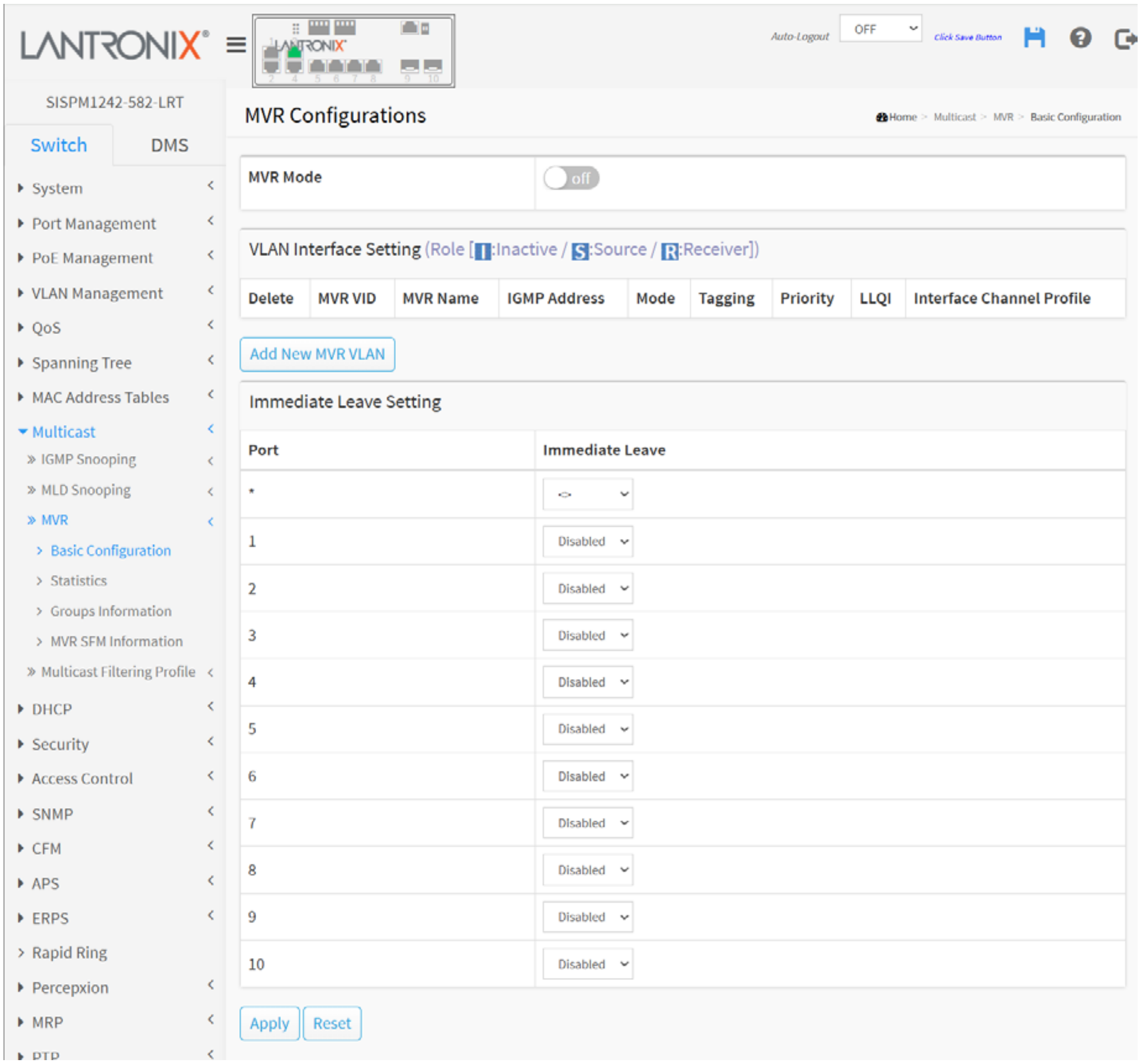
MVR

The MVR feature enables multicast traffic forwarding on the Multicast VLAN. In a multicast television application, a PC or a television with a set-top box can receive the multicast stream. Multiple set-top boxes or PCs can be connected to one subscriber port, which is a switch port configured as an MVR receiver port. When a subscriber selects a channel, the set-top box or PC sends an IGMP join message to Switch A to join the appropriate multicast. Uplink ports that send and receive multicast data to and from the multicast VLAN are called MVR source ports.

Basic Configuration

To set MVR Configuration in the web UI:

1. Go to Multicast > MVR > Basic Configuration.
2. Click **Add New MVR VLAN**.
3. Enable the MVR mode; the default is off (disabled).
4. Specify the MVR VLAN settings.
5. Select which port to enable Immediate Leave. The default is Disabled for all ports.
6. Click **Apply** to save the settings.



MVR Configurations

MVR Mode	off

VLAN Interface Setting (Role [I:Inactive / S:Source / R:Receiver])

Delete	MVR VID	MVR Name	IGMP Address	Mode	Tagging	Priority	LLQI	Interface Channel Profile

Add New MVR VLAN

Immediate Leave Setting

Port	Immediate Leave
*	<>
1	Disabled
2	Disabled
3	Disabled
4	Disabled
5	Disabled
6	Disabled
7	Disabled
8	Disabled
9	Disabled
10	Disabled

Apply Reset

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.

VLAN Interface Setting

Add New MVR VLAN : Click to add a new MVR VLAN. Specify MVR VID, MVR Name, IGMP Address, Mode, Tagging, Priority, LLQI, Interface Channel Profile. Click **Apply**.

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

MVR VID : Specify the Multicast VLAN ID.

Caution: MVR source ports are not recommended to be overlapped with management VLAN ports.

MVR Name : An optional attribute to indicate the name of the specific MVR VLAN. Maximum length of the MVR VLAN Name string is 32. MVR VLAN Name can only contain alphabets or numbers. MVR VLAN name can be edited for the existing MVR VLAN entries, or it can be added to the new entries.

IGMP Address : Define the IPv4 address as source address used in IP header for IGMP control frames.
The default IGMP address is not set (0.0.0.0). When the IGMP address is not set, system uses IPv4 management address of the IP interface associated with this VLAN. When the IPv4 management address is not set, system uses the first available IPv4 management address. Otherwise, system uses a pre-defined value. By default, this value will be 192.0.2.1.

Mode : Specify the MVR mode of operation. In ***Dynamic*** mode, MVR allows dynamic MVR membership reports on source ports. In ***Compatible*** mode, MVR membership reports are forbidden on source ports. The default is Dynamic mode.

Tagging : Specify whether the traversed IGMP/MLD control frames will be sent as ***Untagged*** or ***Tagged*** with MVR VID. The default is tagged.

Priority : Specify how the traversed IGMP/MLD control frames will be sent in prioritized manner. The default Priority is 0.

LLQI : Define the maximum time to wait for IGMP/MLD report memberships on a receiver port before removing the port from multicast group membership. The value is in units of tenths of a second. The range is 0 to 31744. The default LLQI is 5 tenths or one-half second.

Interface Channel Profile : When the MVR VLAN is created, select the profile to expand the corresponding multicast channel settings for the specific MVR VLAN. The file established on Filtering Profile Table.

Port : The logical port for the settings.

Port Role : Configure an MVR port of the designated MVR VLAN as one of these roles:

- ***Inactive***: The designated port does not participate MVR operations.
- ***Source***: Configure uplink ports that receive and send multicast data as source ports. Subscribers cannot be directly connected to source ports.
- ***Receiver***: Configure a port as a receiver port if it is a subscriber port and should only receive multicast data. It does not receive data unless it becomes a member of the multicast group by issuing IGMP/MLD messages.

Caution: MVR source ports are not recommended to be overlapped with management VLAN ports. Select the port role by clicking the Role symbol to switch the setting:

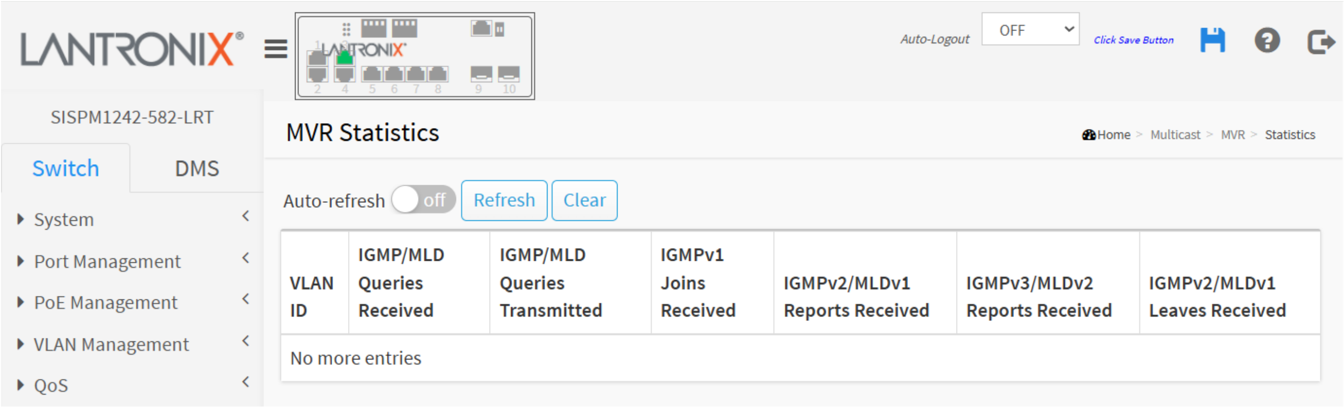
I indicates Inactive; **S** indicates Source; **R** indicates Receiver. The default Role is **I**nactive.

Immediate Leave : Enable the fast leave on the port.

Statistics

This page displays detailed MVR Statistics. To display MVR Statistics Information in the web UI:

1. Go to Multicast > MVR > Statistics.
2. **Auto-refresh** will refresh the page every 3 seconds. **Refresh** will refresh the page immediately. **Clear** will clear all statistics.



MVR Statistics

Auto-Logout: OFF

Auto-refresh: off

VLAN ID	IGMP/MLD Queries Received	IGMP/MLD Queries Transmitted	IGMPv1 Joins Received	IGMPv2/MLDv1 Reports Received	IGMPv3/MLDv2 Reports Received	IGMPv2/MLDv1 Leaves Received
No more entries						

Parameter descriptions:

VLAN ID : The Multicast VLAN ID.

IGMP/MLD Queries Received : The number of Received Queries for IGMP and MLD, respectively.

IGMP/MLD Queries Transmitted : The number of Transmitted Queries for IGMP and MLD, respectively.

IGMPv1 Joins Received : The number of Received IGMPv1 Joins.

IGMPv2/MLDv1 Reports Received : The number of Received IGMPv2 Joins and MLDv1 Reports, respectively.

IGMPv3/MLDv2 Reports Received : The number of Received IGMPv3 Joins and MLDv2 Reports, respectively.

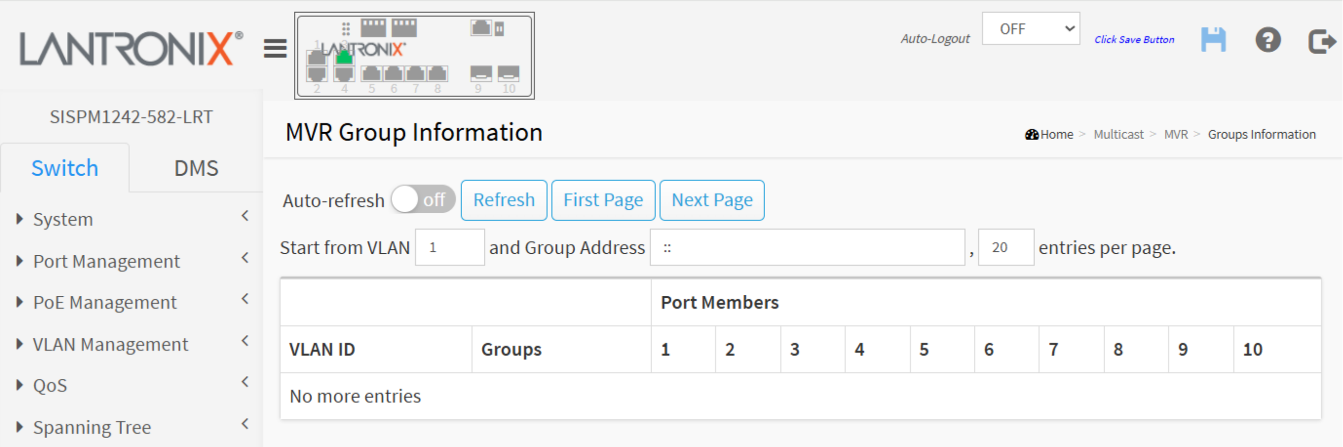
IGMPv2/MLDv1 Leave's Received : The number of Received IGMPv2 Leaves and MLDv1 Dones, respectively.

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. Go to Multicast > MVR > Groups Information.
2. **Auto-refresh** will refresh the page every 3 seconds. **Refresh** will refresh the page immediately.
3. Use the page controls and “Start from” entry fields to help you navigate through the list.



MVR Group Information

Start from VLAN 1 and Group Address :: , 20 entries per page.

		Port Members									
VLAN ID	Groups	1	2	3	4	5	6	7	8	9	10
No more entries											

Parameter descriptions:

VLAN ID : VLAN ID of the group.

Groups : Group ID of the group displayed.

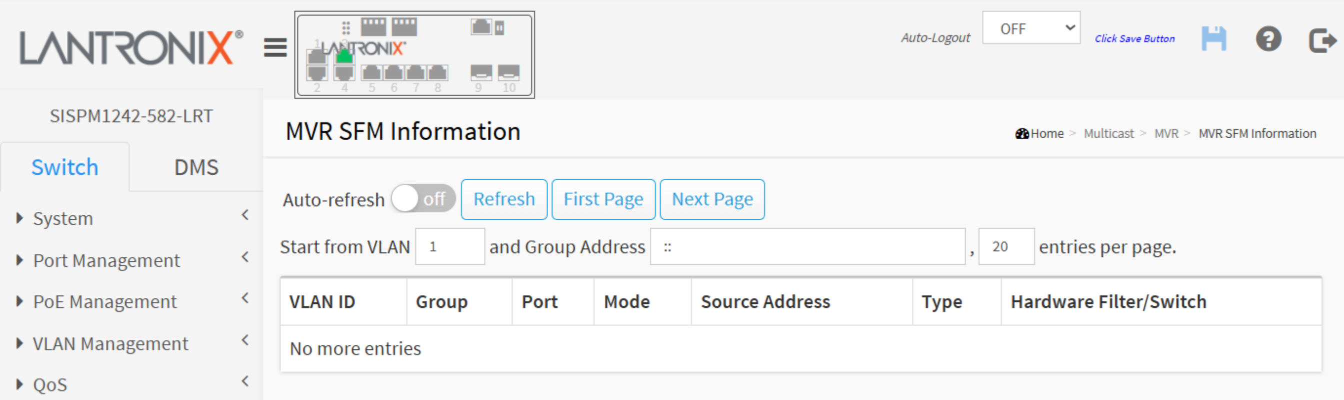
Port Members : Ports under this group.

MVR SFM Information

The MVR SFM (Source-Filtered Multicast) Information Table also contains the SSM (Source-Specific Multicast) information. This table is sorted first by VLAN ID, then by group, and then by Port. Different source addresses belong to the same group are treated as a single entry.

To display MVR SFM Information in the web UI:

1. Go to Multicast > MVR > MVR SFM Information.
2. **Auto-refresh** will refresh the page every 3 seconds. **Refresh** will refresh the page immediately.
3. Use the First Page / Next Page controls and "Start from" entry fields to help you navigate through the list.



MVR SFM Information

Auto-refresh off

Start from VLAN 1 and Group Address :: , 20 entries per page.

VLAN ID	Group	Port	Mode	Source Address	Type	Hardware Filter/Switch
No more entries						

Parameter descriptions:

VLAN ID : VLAN ID of the group.

Group : IP Multicast Group address.

Port : Switch port number.

Mode : Indicates the filtering mode maintained per (VLAN ID, port number, Group Address) basis. It can be either Include or Exclude.

Source Address : IP Address of the source. Currently, system limits the total number of IP source addresses for filtering to be 128. When there is not any source filtering address, the text "None" is shown in the Source Address field.

Type : Indicates the Type. It can be either Allow or Deny.

Hardware Filter/Switch : Indicates whether data plane destined to the specific group address from the source IPv4/IPv6 address could be handled by the chip.

Multicast Filtering Profile

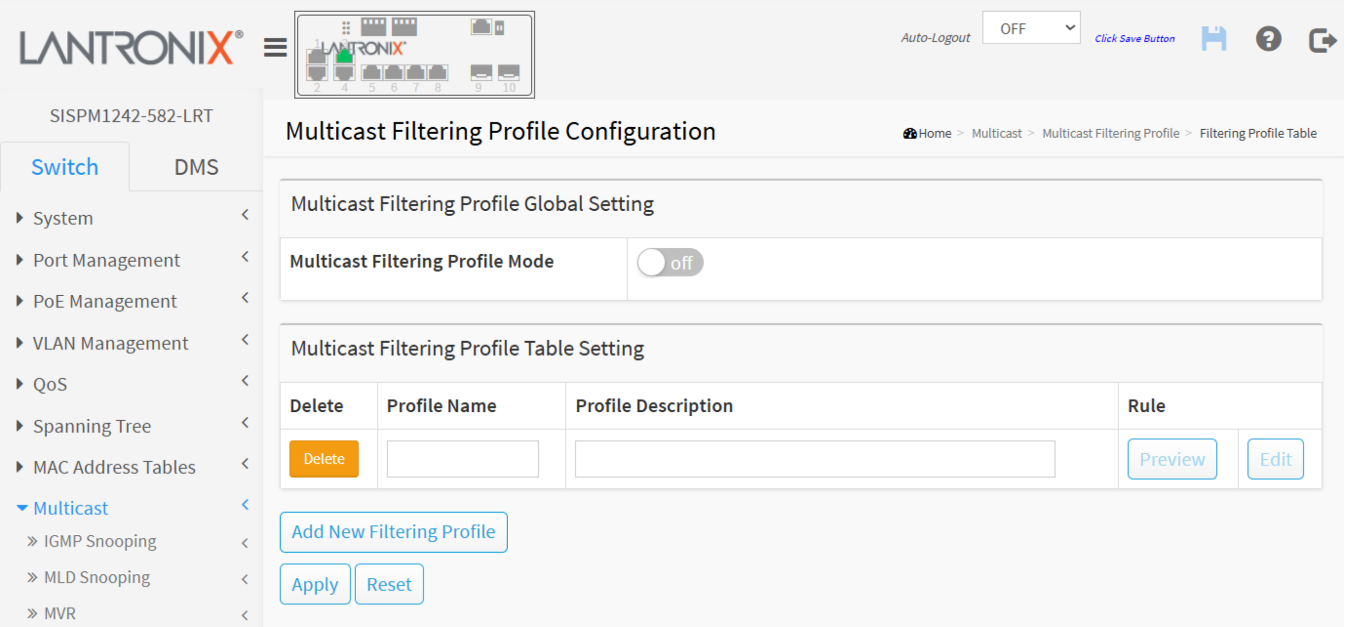
This page provides Multicast Filtering Profile related configurations.

Filtering Profile Table

The IPMC profile is used to deploy access control on IP multicast streams. You can create a maximum 64 Profiles with at maximum 128 corresponding Rules for each Profile.

To configure IPMC Profile parameters in the web UI:

1. Go to Multicast > Multicast Filtering Profile > and Filtering Profile Table.
2. Enable or disable the Multicast Filtering Profile mode.
3. Click **Add New Filtering Profile** to create a filtering profile.



Multicast Filtering Profile Configuration

Multicast Filtering Profile Global Setting

Multicast Filtering Profile Mode	off

Multicast Filtering Profile Table Setting

Delete	Profile Name	Profile Description	Rule	
Delete			Preview	Edit

Add New Filtering Profile

Apply Reset

4. Next, click **Edit** to edit the Rule settings. See Multicast Filtering Profile Rule Settings below.
5. Click **Apply** to save the configuration.

Parameter descriptions:

Multicast Filtering Profile Mode : Enable/Disable the Multicast Filtering Profile. System starts to do filtering based on profile settings only when the global profile mode is enabled.

Multicast Filtering Profile Table Setting

Add New Filtering Profile : Click to add new IPMC profile. Specify the name, configure the new entry, and click **Apply**.

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

Profile Name : The name used for indexing the profile table. Each entry has the unique name which is composed of at maximum 16 alphabetic and numeric characters.

Profile Description : Additional description, composed of at maximum 64 alphabetic and numeric characters, about the profile. No blank or space characters are permitted as part of description. Use "_" or "-" to separate the description sentence.

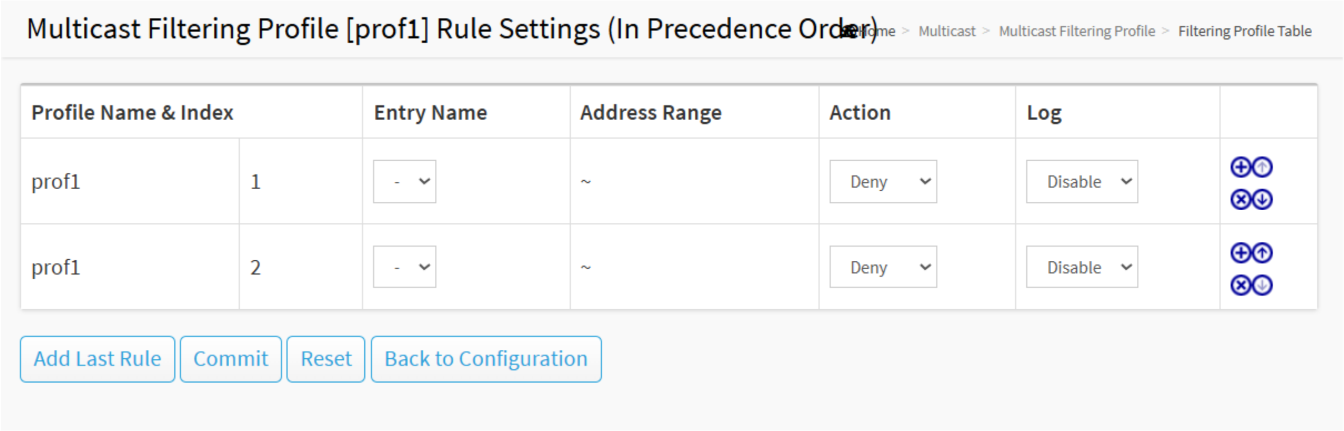
Rule : When the profile is created, click the edit button to enter the rule setting page of the designated profile. Summary about the designated profile will be shown by clicking the View button. You can manage or inspect the rules of the designated profile by using these buttons:

- ***Preview***: Preview the rules associated with the designated profile.
- ***Edit***: Adjust the rules associated with the designated profile.

Multicast Filtering Profile Rule Settings

This page provides the filtering rule settings for a specific IPMC profile. It displays the configured rule entries in precedence order. First rule entry has highest priority in lookup, while the last rule entry has lowest priority in lookup. Notice that the profile performs deny action for all groups if there is not any permit entry is included in the profile.

1. From the Multicast Filtering Profile configuration page, under the Rule column click **Edit**.
2. Click **Add Last Rule** to start adding a rule setting to the profile.



Multicast Filtering Profile [prof1] Rule Settings (In Precedence Order)

Profile Name & Index		Entry Name	Address Range	Action	Log	
prof1	1	-	~	Deny	Disable	⊕⊕ ⊗⊕
prof1	2	-	~	Deny	Disable	⊕⊕ ⊗⊕

Home > Multicast > Multicast Filtering Profile > Filtering Profile Table
Add Last Rule
Commit
Reset
Back to Configuration

Parameter descriptions:

Add Last Rule button: 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 **Commit**.

Commit button: Click to commit the rule changes for the designated profile.

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

Back to Configuration button: Go back to previous configuration page.

Profile Name & Index : The name of the designated profile to be associated and its instance number. This field is not editable.

Entry Name : The name used in specifying the address range used for this rule. Only the existing profile address entries will be chosen in the selected box. This field is not allowed to be selected as none ("-") while the Rule Settings Table is committed.

Address Range : The corresponding address range of the selected profile entry. This field is not editable and will be adjusted automatically according to the selected profile entry.

Action : Indicates the learning action upon receiving the Join/Report frame that has the group address matches the address range of the rule.

- ***Permit***: Group address matches the range specified in the rule will be learned.
- ***Deny***: Group address matches the range specified in the rule will be dropped.

Log : Indicates the logging preference upon receiving the Join/Report frame that has the group address matches the address range of the rule.

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

Rule Management Buttons : You can manage rules and the corresponding precedence order by using the following buttons:

⊕ : Insert a new rule before the current entry of rule.

⊗ : Delete the current entry of rule.

↑ : Move the current entry of rule up in the list.

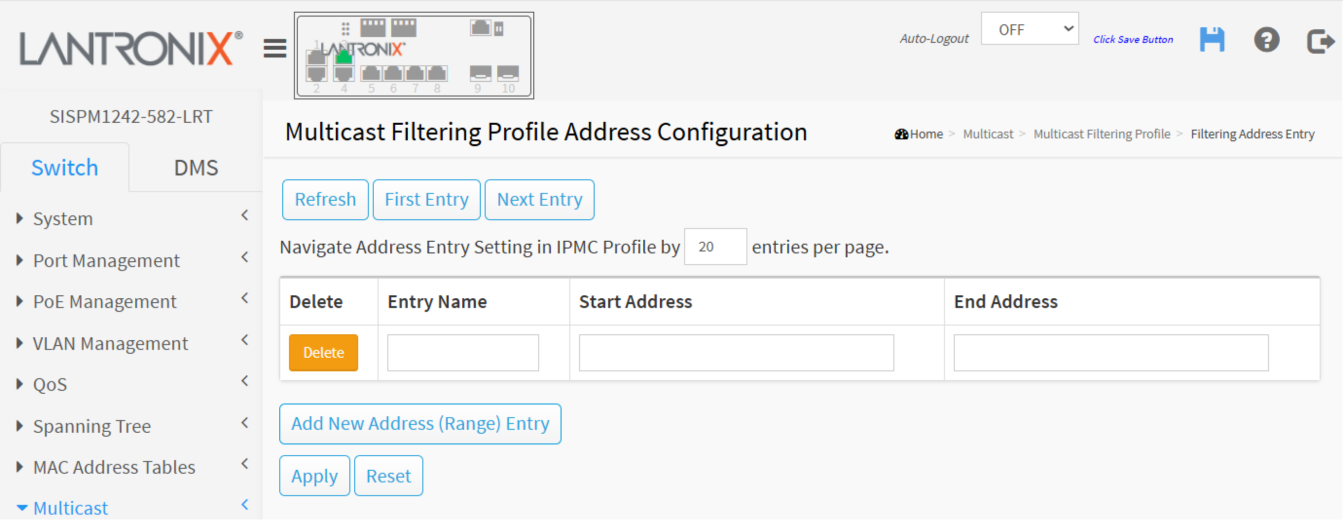
↓ : Move the current entry of rule down in the list.

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. Go to Multicast > Multicast Filtering Profile > Filtering Address Entry.
2. Click **Add New Address (Range) Entry**.
3. Specify Entry Name, Start Address and End Address.
4. Click the **Apply** button.



Multicast Filtering Profile Address Configuration

Navigate Address Entry Setting in IPMC Profile by 20 entries per page.

Delete	Entry Name	Start Address	End Address
Delete			

Buttons

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.

Add New Address (Range) Entry: Click to add new address range. Specify the name and configure the addresses. Click **Apply**.

Apply: Click to save changes.

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

Parameter descriptions:

Entry Name: The name used for indexing the address entry table .Each entry has the unique name which is composed of at maximum16 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.

11. DHCP

This section lets you set and view DHCP snooping, DHCP relay, and DHCP server parameters.

A DHCP server can provide optional configuration parameters to the client. RFC 2132 describes the available DHCP options defined by the Internet Assigned Numbers Authority (IANA) - DHCP and BOOTP Parameters.

A DHCP client can select, manipulate and overwrite parameters provided by a DHCP server.

Snooping

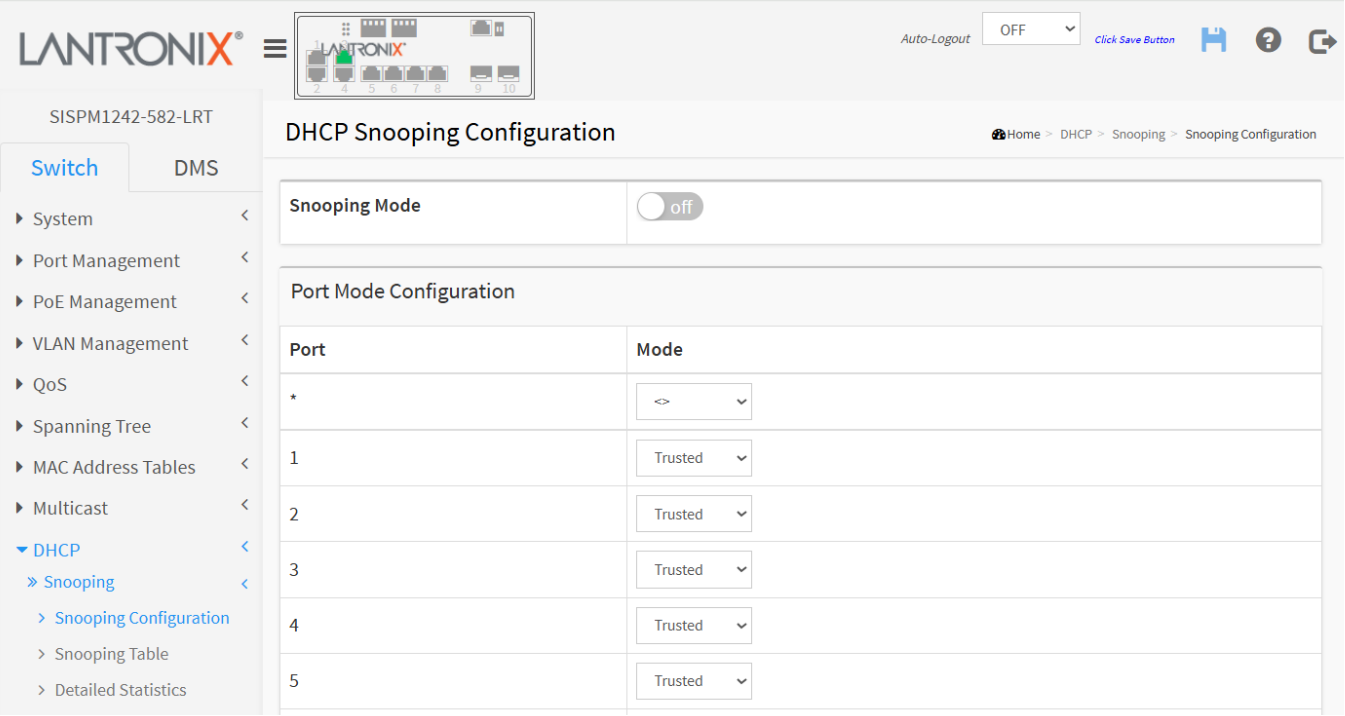
Snooping Configuration

DHCP Snooping is used to block an intruder on the untrusted ports of the switch device when it tries to intervene by injecting a bogus DHCP reply packet to a legitimate conversation between the DHCP client and server. DHCP Snooping can prevent attackers from adding their own DHCP servers to the network.

This page lets you configure DHCP Snooping parameters of the switch.

To configure DHCP snooping in the web UI:

1. Go to DHCP > Snooping > Configuration.
2. Enable Snooping Mode.
3. Select Trusted for the Mode.
4. Click **Apply**.



DHCP Snooping Configuration

Snooping Mode	off

Port Mode Configuration

Port	Mode
*	<>
1	Trusted
2	Trusted
3	Trusted
4	Trusted
5	Trusted

Parameter descriptions:

Snooping Mode : Indicates the DHCP snooping mode operation. Possible modes are:

- ***on*** : Enable DHCP snooping mode operation. When DHCP snooping mode operation is enabled, the DHCP request messages will be forwarded to trusted ports and only allow reply packets from trusted ports.
- ***off*** : Disable DHCP snooping mode operation (default).

Port Mode Configuration : Indicates the DHCP snooping port mode. Possible port modes are:

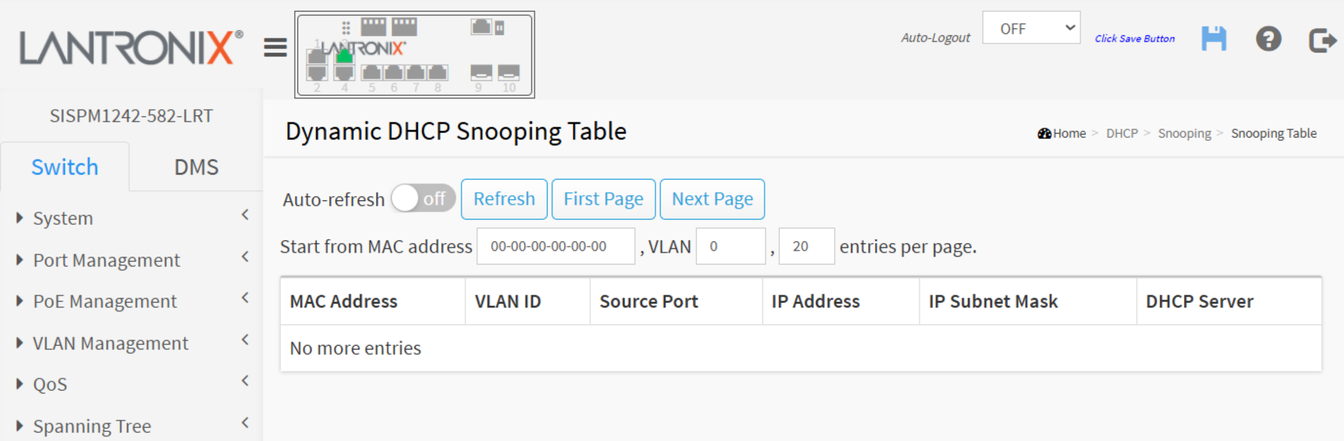
- ***Trusted***: Configures the port as trusted source of the DHCP messages. Trusted port can forward DHCP packets normally.
- ***Untrusted***: Configures the port as untrusted source of the DHCP messages. Untrusted port will discard the packets when it receives DHCP packets.

Snooping Table

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

To monitor DHCP Snooping in the web UI:

1. Go to DHCP > Snooping > Snooping Table.
2. **Auto-refresh** will refresh the page every 3 seconds. **Refresh** will refresh the page immediately.
3. Use the First Page / Next Page controls and "Start from" entry fields to help you navigate through the list.



Dynamic DHCP Snooping Table

Auto-refresh off

Start from MAC address 00-00-00-00-00-00 , VLAN 0 , 20 entries per page.

MAC Address	VLAN ID	Source Port	IP Address	IP Subnet Mask	DHCP Server
No more entries					

Parameter descriptions:

MAC Address : The User MAC address of the entry.

VLAN ID : The VLAN ID in which the DHCP traffic is permitted.

Source Port: The Switch Port Number for which the entries are displayed.

IP Address : User IP address of the entry.

IP Subnet Mask : User IP subnet mask of the entry.

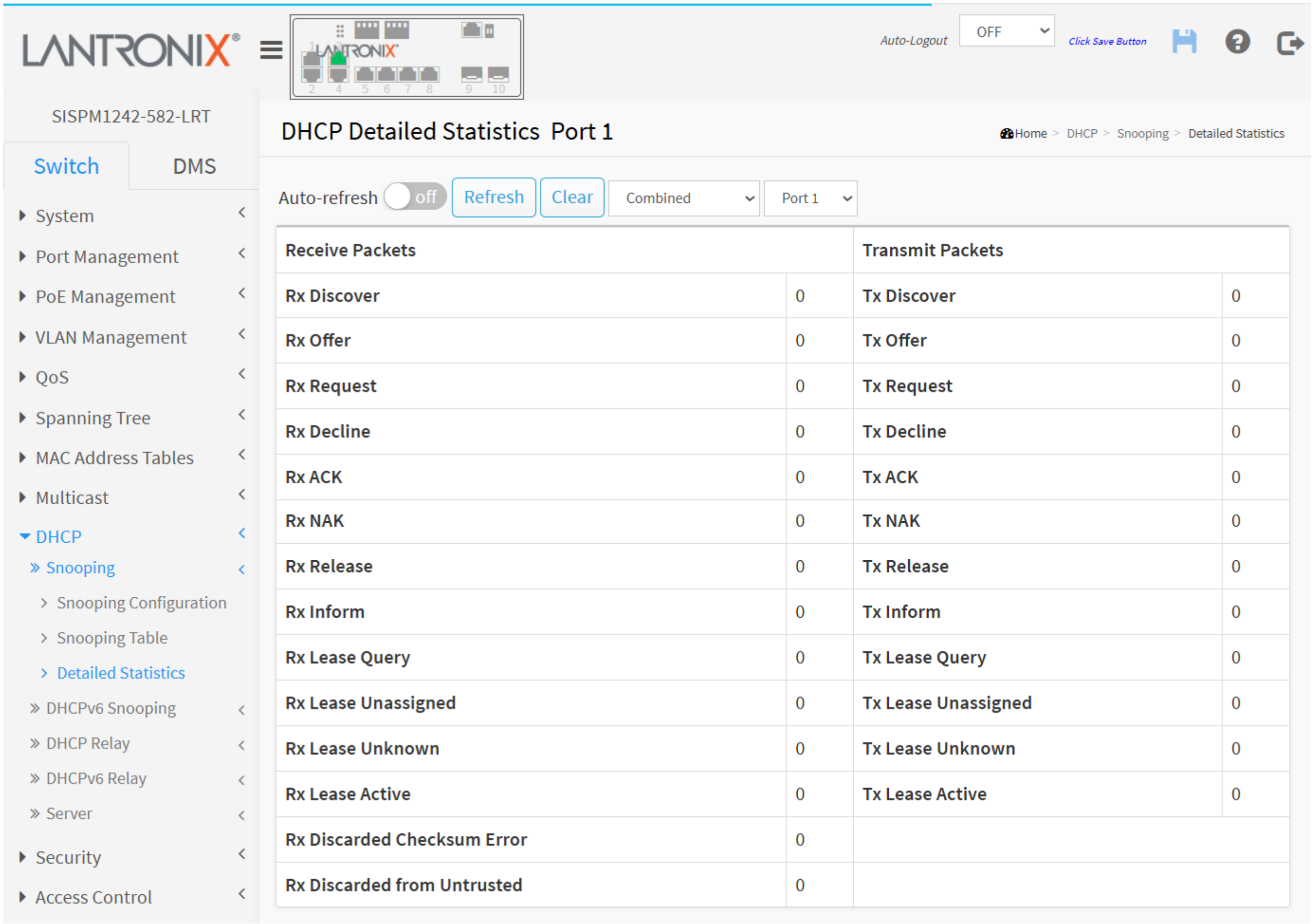
DHCP Server : The DHCP Server address of the entry.

Detailed Statistics

This page provides statistics for DHCP snooping. Note that the normal forward per-port TX statistics are not increased if the incoming DHCP packet is done by L3 forwarding mechanism. Also note that clearing the statistics on a specific port may not take effect on global statistics since it gathers the different layer overview.

To display DHCP detailed statistics in the web UI:

1. Go to DHCP > Snooping > Detailed Statistics.
2. Select the user set and port from selection boxes.
3. **Auto-refresh** will refresh the page every 3 seconds. **Refresh** will refresh the page immediately. **Clear** will clear all statistics.



Auto-Logout: OFF

DHCP Detailed Statistics Port 1

Auto-refresh: off | Combined | Port 1

Receive Packets		Transmit Packets	
Rx Discover	0	Tx Discover	0
Rx Offer	0	Tx Offer	0
Rx Request	0	Tx Request	0
Rx Decline	0	Tx Decline	0
Rx ACK	0	Tx ACK	0
Rx NAK	0	Tx NAK	0
Rx Release	0	Tx Release	0
Rx Inform	0	Tx Inform	0
Rx Lease Query	0	Tx Lease Query	0
Rx Lease Unassigned	0	Tx Lease Unassigned	0
Rx Lease Unknown	0	Tx Lease Unknown	0
Rx Lease Active	0	Tx Lease Active	0
Rx Discarded Checksum Error	0		
Rx Discarded from Untrusted	0		

Parameter descriptions:

Server Statistics

Rx and Tx Discover : The number of discover (option 53 with value 1) packets received and transmitted.

Rx and Tx Offer : The number of offer (option 53 with value 2) packets received and transmitted.

Rx and Tx Request : The number of request (option 53 with value 3) packets received and transmitted.

Rx and Tx Decline : The number of decline (option 53 with value 4) packets received and transmitted.

Rx and Tx ACK : The number of ACK (option 53 with value 5) packets received and transmitted.

Rx and Tx NAK : The number of NAK (option 53 with value 6) packets received and transmitted.

Rx and Tx Release : The number of release (option 53 with value 7) packets received and transmitted.

Rx and Tx Inform : The number of inform (option 53 with value 8) packets received and transmitted.

Rx and Tx Lease Query : The number of lease query (option 53 with value 10) packets received and transmitted.

Rx and Tx Lease Unassigned : The number of lease unassigned (option 53 with value 11) packets received and transmitted.

Rx and Tx Lease Unknown : The number of lease unknown (option 53 with value 12) packets received and transmitted. Rx and Tx Lease Active

Rx and Tx Lease Active : The number of lease active (option 53 with value 13) packets received and transmitted.

Rx Discarded checksum error : The number of discard packet that IP/UDP checksum is error.

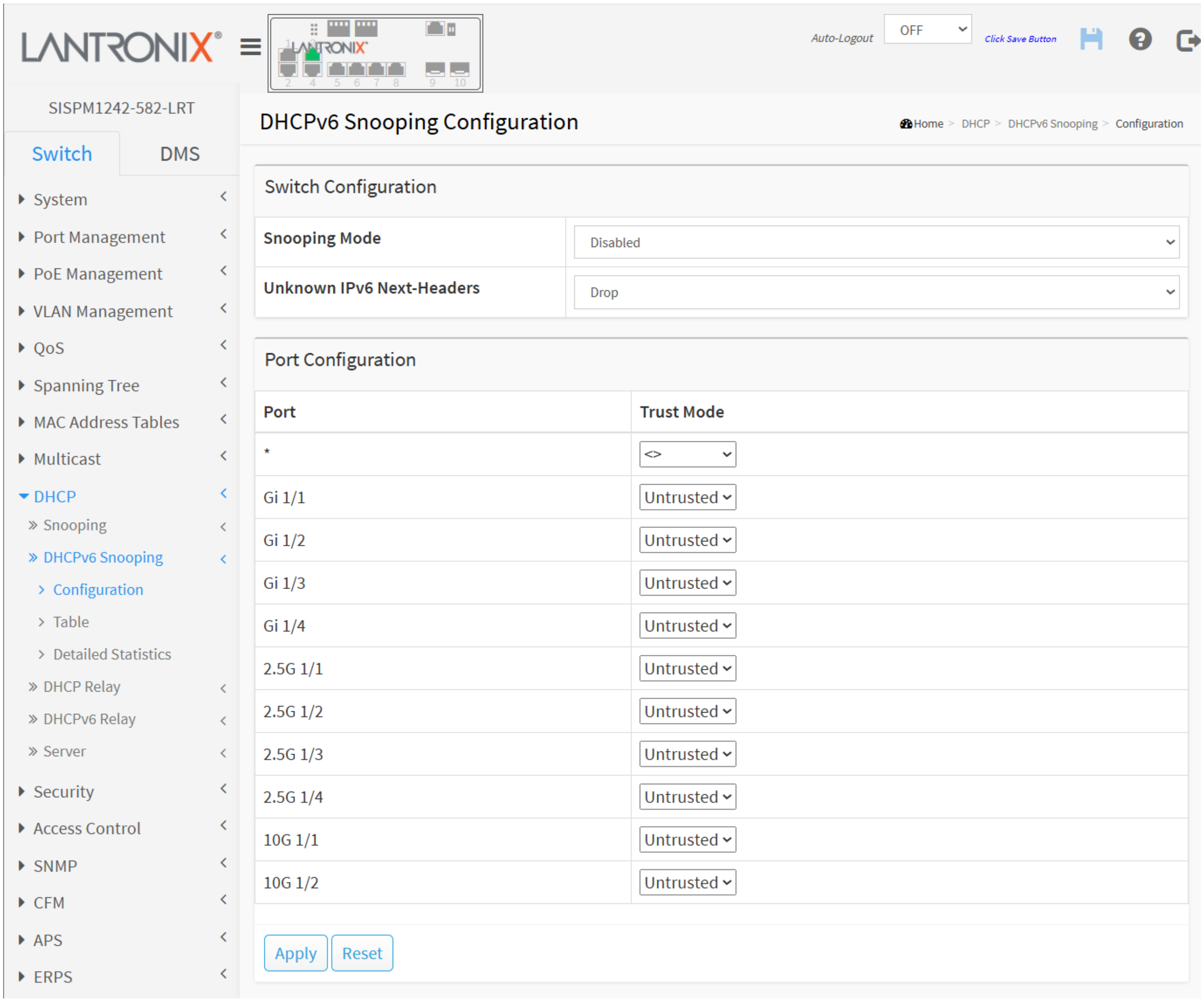
Rx Discarded from Untrusted : The number of discarded packets that are coming from untrusted port.

DHCPv6 Snooping

This page lets you configure DHCP snooping for IPv6. DHCPv6 is standardized in IETF RFC-8415.

Snooping Configuration

Configure DHCPv6 (DHCP over IPv6) Snooping on this page.



DHCPv6 Snooping Configuration

Switch Configuration

Snooping Mode	Disabled
Unknown IPv6 Next-Headers	Drop

Port Configuration

Port	Trust Mode
*	<>
Gi 1/1	Untrusted
Gi 1/2	Untrusted
Gi 1/3	Untrusted
Gi 1/4	Untrusted
2.5G 1/1	Untrusted
2.5G 1/2	Untrusted
2.5G 1/3	Untrusted
2.5G 1/4	Untrusted
10G 1/1	Untrusted
10G 1/2	Untrusted

Snooping Mode : Indicates the DHCPv6 snooping mode operation. Possible modes are:

- ***Enabled***: Enable DHCPv6 snooping mode operation. When DHCPv6 snooping mode operation is enabled, the DHCPv6 client request messages will be forwarded to trusted ports and only allow reply packets from trusted ports.
- ***Disabled***: Disable DHCP snooping mode operation (default).

Unknown IPv6 Next-Headers : Indicates how Unknown IPv6 Next-Header values should be treated. The switch needs to parse all IPv6 packets to a DHCPv6 client to determine if it is in fact a DHCPv6 message. If an unknown IPv6 extension header is encountered the parsing cannot continue. See RFC 7610, section 5, item 3 for details. Possible options are:

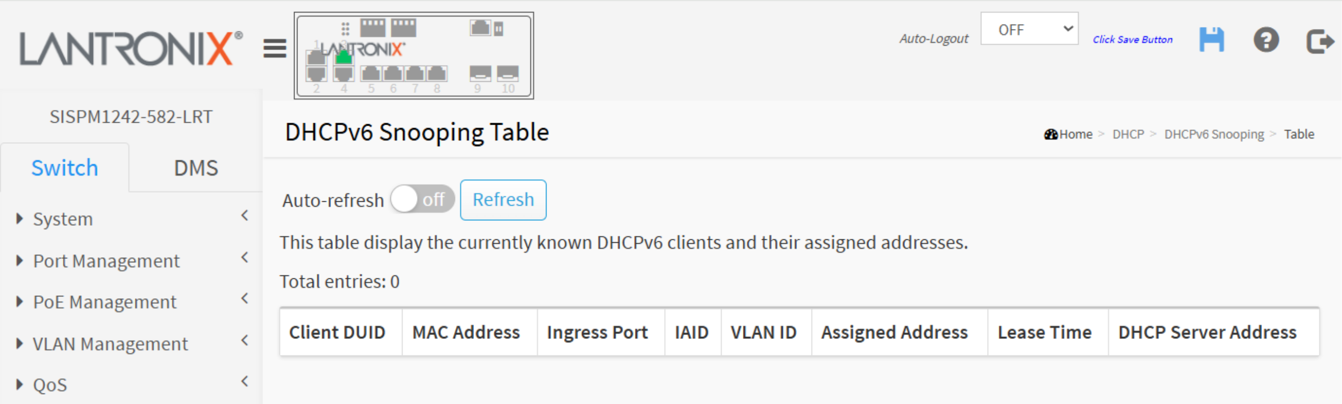
- ***Drop***: Drop packets with unknown IPv6 extension headers. This is the most secure option but may result in traffic disruptions (default).
- ***Allow***: Allow packets with unknown IPv6 extension headers. This is a less secure option but prevents traffic disruptions.

Trust Mode : Indicates the DHCPv6 snooping port mode. Possible port modes are:

- ***Trusted***: Configures the port as trusted source of the DHCPv6 messages.
- ***Untrusted***: Configures the port as untrusted source of the DHCPv6 messages (default).

Snooping Table

This page displays the currently known DHCPv6 clients and their assigned addresses in the DHCPv6 Snooping Table.



DHCPv6 Snooping Table

This table display the currently known DHCPv6 clients and their assigned addresses.

Total entries: 0

Client DUID	MAC Address	Ingress Port	IAID	VLAN ID	Assigned Address	Lease Time	DHCP Server Address

Client DUID : The DHCP Unique Identifier (DUID) for the client. DHCPv6 uses this value to uniquely identify a client host instead of just using the MAC address of one of its interface ports (as DHCPv4 does).

MAC Address : The MAC address for the client interface port that sent the DHCPv6 message.

Ingress Port : The local port on the snooping switch where client messages are received.

IAID : Each client may contain multiple interfaces and may request addresses for each of these in the same DHCPv6 message. The Identity Association ID (IAID) value uniquely identifies the interface in the scope of the client.

VLAN ID : The VLAN ID which is used by the client messages.

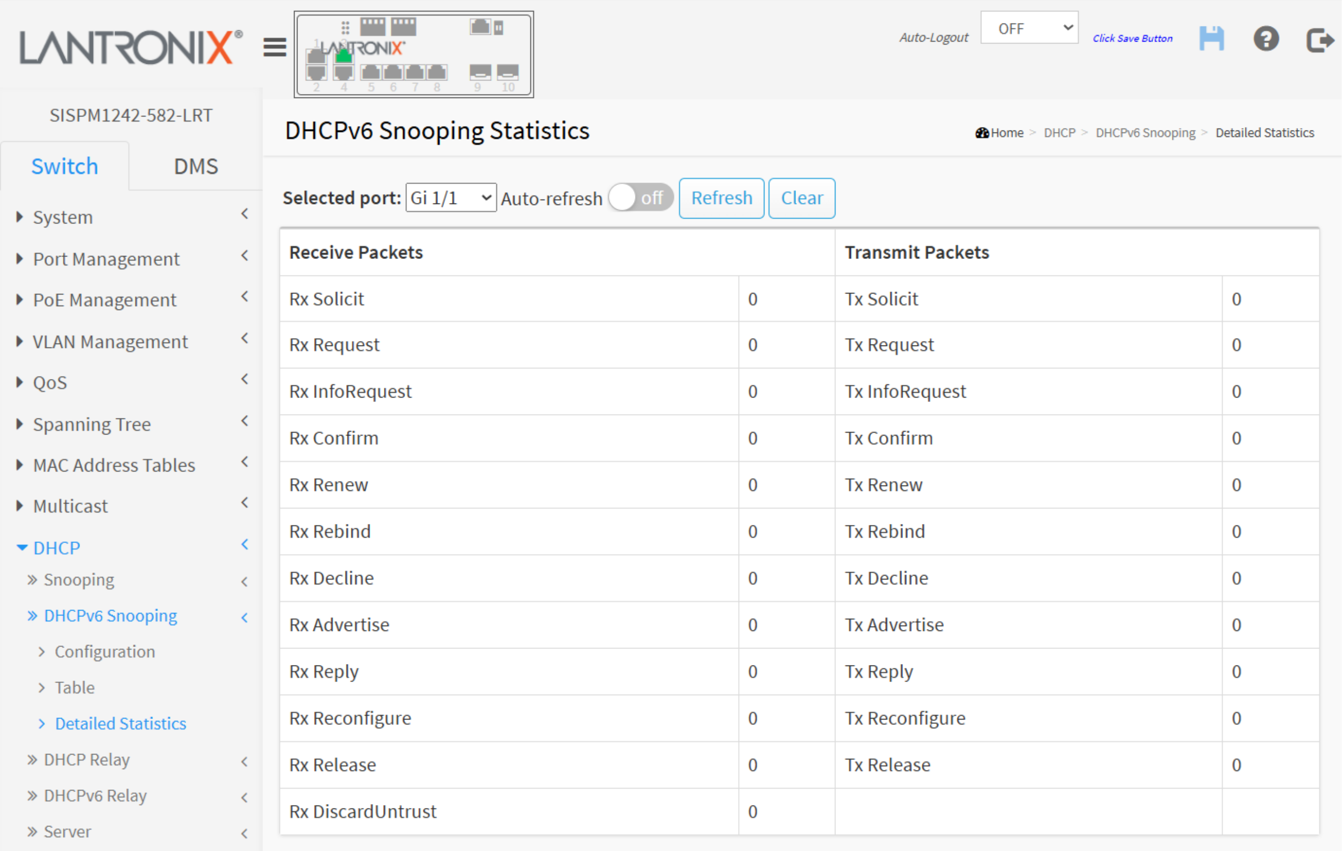
Assigned Address : The address assigned to the interface identified by the IAID value.

Lease Time : The lease time associated with the assigned address in seconds.

DHCP Server Address : The IPv6 address of the DHCP server which assigned the address to the client.

Detailed Statistics

This page displays statistics for DHCPv6 snooping.



DHCPv6 Snooping Statistics

Selected port: Gi 1/1 Auto-refresh off

Receive Packets		Transmit Packets	
Rx Solicit	0	Tx Solicit	0
Rx Request	0	Tx Request	0
Rx InfoRequest	0	Tx InfoRequest	0
Rx Confirm	0	Tx Confirm	0
Rx Renew	0	Tx Renew	0
Rx Rebind	0	Tx Rebind	0
Rx Decline	0	Tx Decline	0
Rx Advertise	0	Tx Advertise	0
Rx Reply	0	Tx Reply	0
Rx Reconfigure	0	Tx Reconfigure	0
Rx Release	0	Tx Release	0
Rx DiscardUntrust	0		

Selected port: The port selection box selects the port for which you want to view and control statistics.

General Receive and Transmit Packets

The page contains both RX and TX counters for all known DHCPv6 message types. Refer to IETF RFC 3315 for details on the various DHCPv6 message types.

Untrusted Discards

The “RX DiscardUntrust” counter indicates the number of received DHCP server packets that have been discarded due to the port being untrusted.

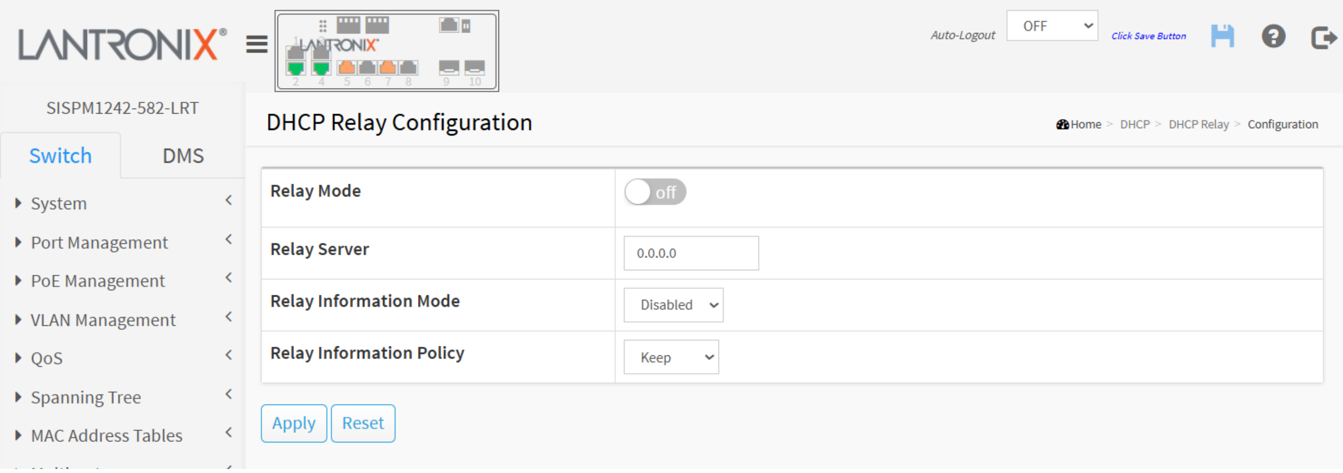
DHCP Relay

Configuration

A DHCP relay agent is used to forward and to transfer DHCP messages between the clients and the server when they are not in the same subnet domain. It stores the incoming interface IP address in the GIADDR field of the DHCP packet. The DHCP server can use the value of GIADDR field to determine the assigned subnet. For such a condition, make sure the switch configuration of VLAN interface IP address and PVID (Port VLAN ID) is correct.

To configure DHCP Relay in the web UI:

1. Go to DHCP > Relay > Configuration.
2. Specify the Relay configuration settings.
3. Click **Apply**.



DHCP Relay Configuration

Relay Mode	off
Relay Server	0.0.0.0
Relay Information Mode	Disabled
Relay Information Policy	Keep

Parameter descriptions:

Relay Mode : Indicates the DHCP relay mode operation. Possible modes are:

- ***on***: Enable DHCP relay mode operation. When DHCP relay mode operation is enabled, the agent forwards and transfers DHCP messages between the clients and the server when they are not in the same subnet domain. And the DHCP broadcast message won't be flooded for security considerations.
- ***off*** : Disable DHCP relay mode operation.

Relay Server : Indicates the DHCP relay server IP address.

Relay Information Mode : Indicates the DHCP relay information mode option operation. The option 82 circuit ID format as "[vlan_id][module_id][port_no]". The first four characters represent the VLAN ID, the fifth and sixth characters are the module ID (in standalone device it always equals 0), and the last two characters are the port number. For example, "00030108" means the DHCP message received from VLAN ID 3, switch ID 1, port No 8 and the option 82 remote ID value equals the switch MAC address.

Possible modes are:

- ***Enabled***: Enable DHCP relay information mode operation. When DHCP relay information mode operation is enabled, the agent inserts specific information (option 82) into a DHCP message when forwarding to DHCP server and removes it from a DHCP message when transferring to DHCP client. It only works when DHCP relay operation mode is enabled.
- ***Disabled***: Disable DHCP relay information mode operation.

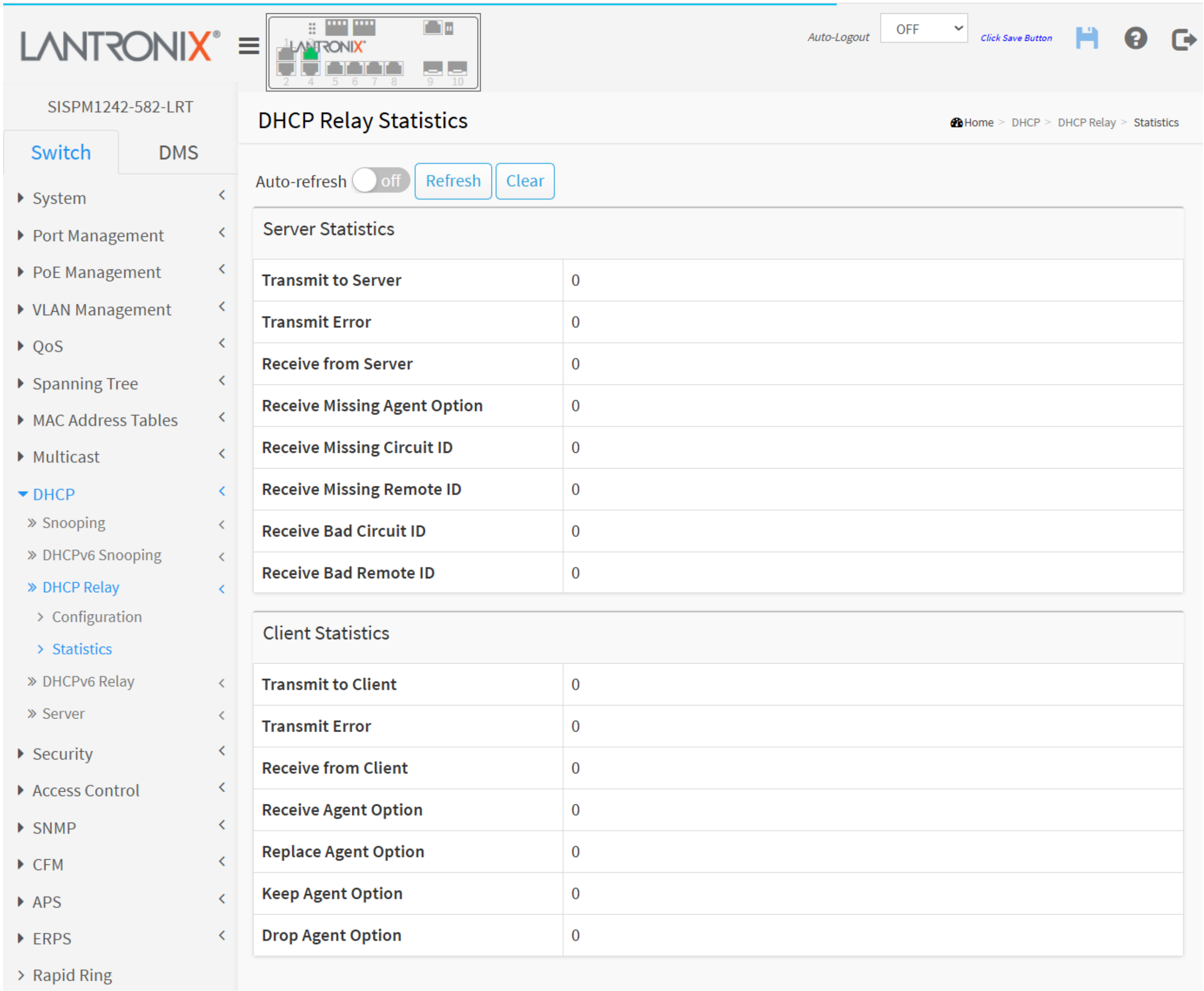
Relay Information Policy : Indicates the DHCP relay information option policy. When DHCP relay information mode operation is enabled, if the agent receives a DHCP message that already contains relay agent information it will enforce the policy. The 'Replace' policy is invalid when relay information mode is disabled. Possible policies are:

- ***Replace***: Replace the original relay information when a DHCP message that already contains it is received.
- ***Keep***: Keep the original relay information when a DHCP message that already contains it is received.
- ***Drop***: Drop the package when a DHCP message that already contains relay information is received.

Statistics

To view DHCP Relay statistics in the web UI:

1. Go to DHCP > Relay > Statistics to display DHCP relay statistics.
2. **Auto-refresh** will refresh the page every 3 seconds. **Refresh** will refresh the page immediately. **Clear** will clear all statistics.



DHCP Relay Statistics

Server Statistics

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

Client Statistics

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

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.

DHCPv6 Relay

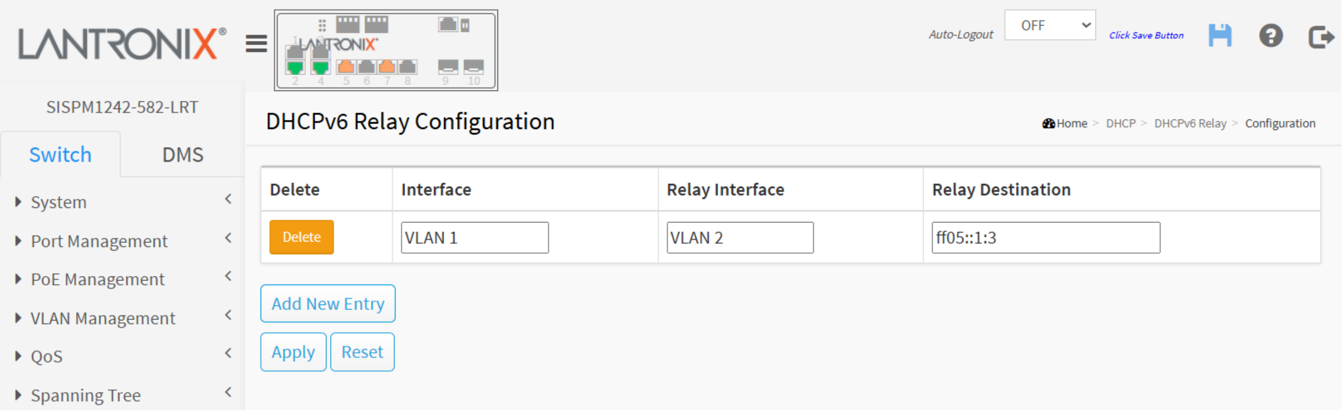
The Dynamic Host Configuration Protocol for IPv6 (DHCPv6) is an extensible mechanism for configuring nodes with network configuration parameters, IP addresses, and prefixes. See IETF RFC-8415 for details.

Configuration

This page shows a table to configure Dhcp6_Relay for a specific VLAN.

To configure DHCPv6 Relay in the web UI:

1. Go to DHCP > DHCPv6 Relay > Configuration.
2. Click the **Add New Entry** button.
3. Specify the relay parameters.
4. Click **Apply**.



DHCPv6 Relay Configuration

Delete	Interface	Relay Interface	Relay Destination
Delete	VLAN 1	VLAN 2	ff05::1:3

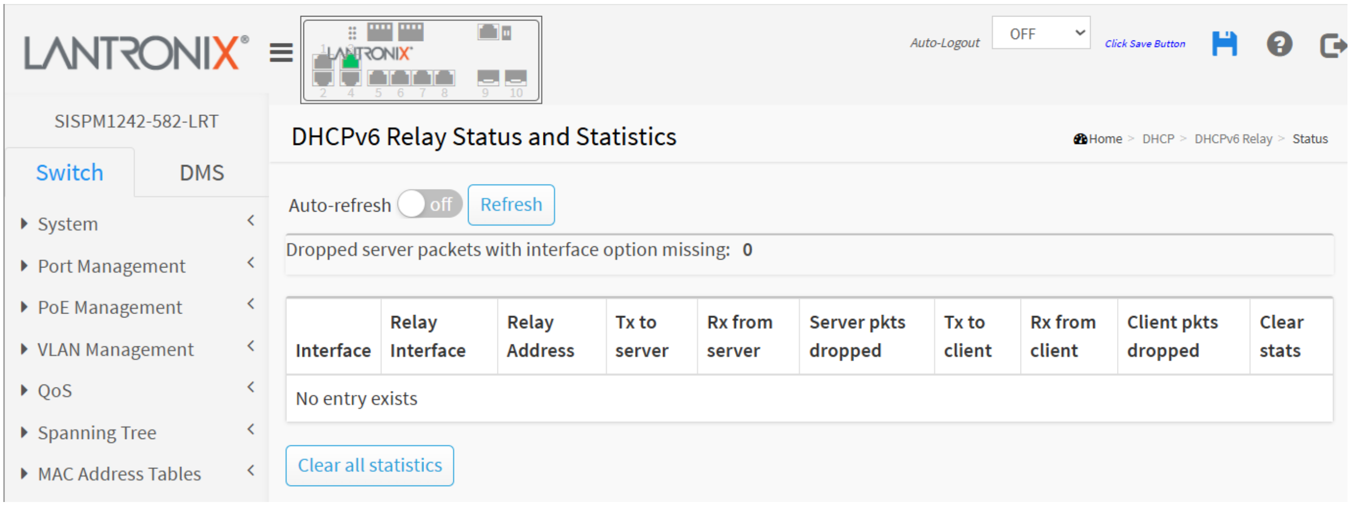
Interface : Interface identification.

Relay Interface : Interface identification. The id of the interface used for relaying.

Relay Destination : An Ipv6 address represented as human readable test as specified in IETF RFC 5952. The IPv6 address of the DHCPv6 server that requests will be relayed to. The default value 'ff05::1:3' mans 'any DHCP server'.

Status

This page displays currently configured relay agents and their statistics.



DHCPv6 Relay Status and Statistics

Dropped server packets with interface option missing: 0

Interface	Relay Interface	Relay Address	Tx to server	Rx from server	Server pkts dropped	Tx to client	Rx from client	Client pkts dropped	Clear stats
No entry exists									

Dropped server packets with interface option missing: Displays the number of server packets that were dropped with the interface option missing.

Interface : Interface identification. The id of the interface that receives client requests.

Relay Interface : Interface identification. The id of the interface used for relaying.

Relay Address : An Ipv6 address represented as human readable test as specified in RFC5952. The IPv6 address that requests will be relayed to. The default value 'ff05::1:3' means 'any DHCPv6 server'.

Tx to server : Integer number. Number of packets relayed to server.

Rx from server : Integer number. Number of packets received from server.

Server pkts dropped : Integer number. Number of packets from server that relay agent drops.

Tx to client : Integer number. Number of packets sent to client.

Rx from client : Integer number. Number of packets received from client.

Client pkts dropped : Integer number. Number of packets from client that relay agent drops.

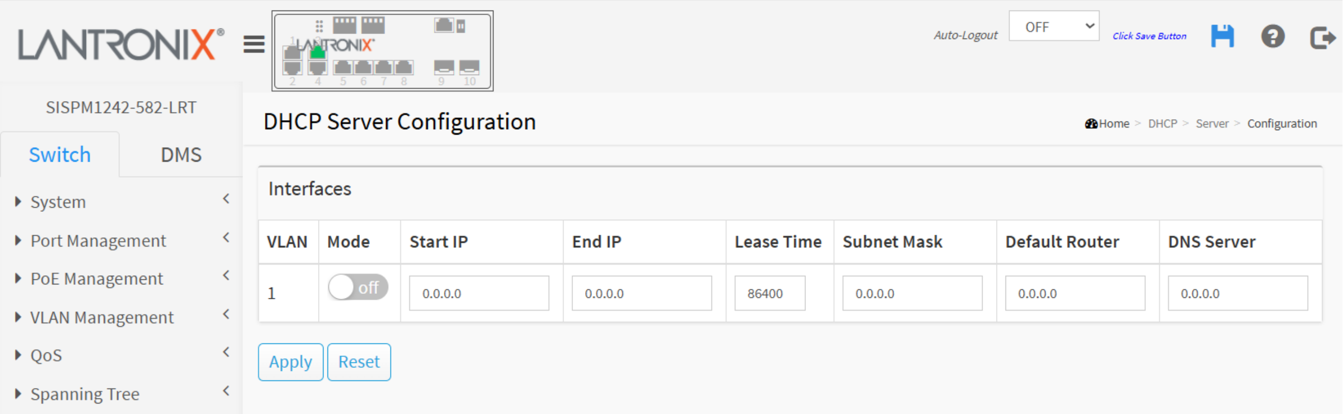
Clear all statistics : Resets all statistics counters of relevant entry to zero.

Server

Configuration

This page lets you enable/disable DHCP server mode per system and per VLAN and configure Start IP and End IP addresses. A DHCP server will allocate these IP addresses to the DHCP client and deliver configuration parameters to the DHCP client. To configure DHCP Server parameters in the web UI:

1. Go to DHCP > Server > Configuration.
2. Click **Add Interface**.
3. Specify VLAN, Mode, Start IP, End IP, Lease time, Subnet mask, Default router, and DNS server.
4. Click **Apply**.



DHCP Server Configuration

Interfaces

VLAN	Mode	Start IP	End IP	Lease Time	Subnet Mask	Default Router	DNS Server
1	off	0.0.0.0	0.0.0.0	86400	0.0.0.0	0.0.0.0	0.0.0.0

Parameter descriptions:

Add Interface : Click to add a new DHCP server.

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

VLAN: Configure the VLAN in which the DHCP server is enabled or disabled. Allowed VLANs are 1 – 4095.

Mode : Indicate the operation mode per VLAN. Possible modes are:

- ***Enable*** : Enable DHCP server per VLAN.
- ***Disable*** : Disable DHCP server pre VLAN.

Start IP and **End IP** : Define the IP address range. The Start IP must be smaller than or equal to the End IP address.

Lease Time : Displays lease time of the pool in minutes. The default is 86400 minutes.

Subnet Mask : Configure subnet mask of the DHCP address.

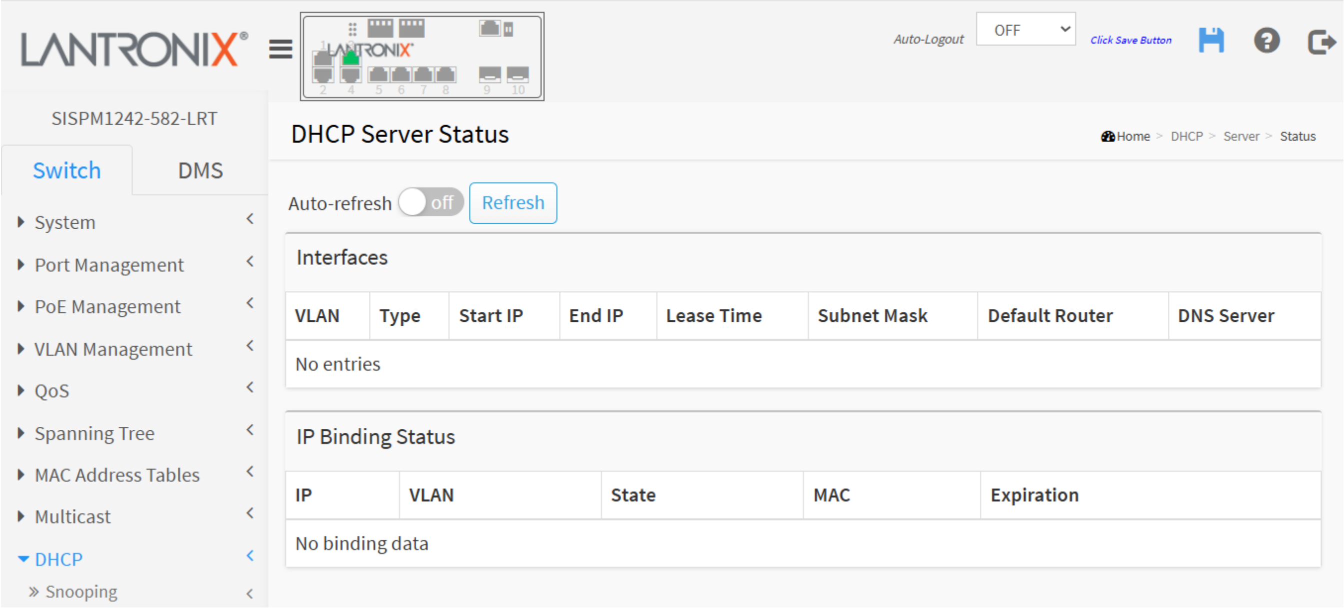
Default Router : Configure the destination IP network or host address of this route.

DNS Server : Specify the DNS server IP address.

Status

This page displays DHCP server status. To display DHCP server status in the web UI:

1. Go to DHCP > Server > and Status.
2. **Auto-refresh** will refresh the page every 3 seconds. **Refresh** will refresh the page immediately.



DHCP Server Status

Interfaces

VLAN	Type	Start IP	End IP	Lease Time	Subnet Mask	Default Router	DNS Server
No entries							

IP Binding Status

IP	VLAN	State	MAC	Expiration
No binding data				

Parameter descriptions:

<u>Interfaces:</u>

VLAN: The VLAN ID of the entry.

Type : Indicate the operation type per VLAN. Possible types are: ***Static*** and ***DMS***.

Start IP and **End IP** : Displays the Start IP address and the End IP address.

Lease Time : Displays lease time of the pool in minutes.

Subnet Mask : Displays subnet mask of the DHCP address.

Default Router : Displays the destination IP network or host address of this route.

DNS Server : Displays DNS server IP address.

<u>IP Binding Status:</u>

IP : Displays the IP address of the binding.

VLAN : Displays the VLAN ID.

State : Displays the binding state.

MAC : Displays the MAC address.

Expiration : Displays the lease expiration date and time.

12. Security

This section lets you add, edit and delete users, and configure various switch Security settings.

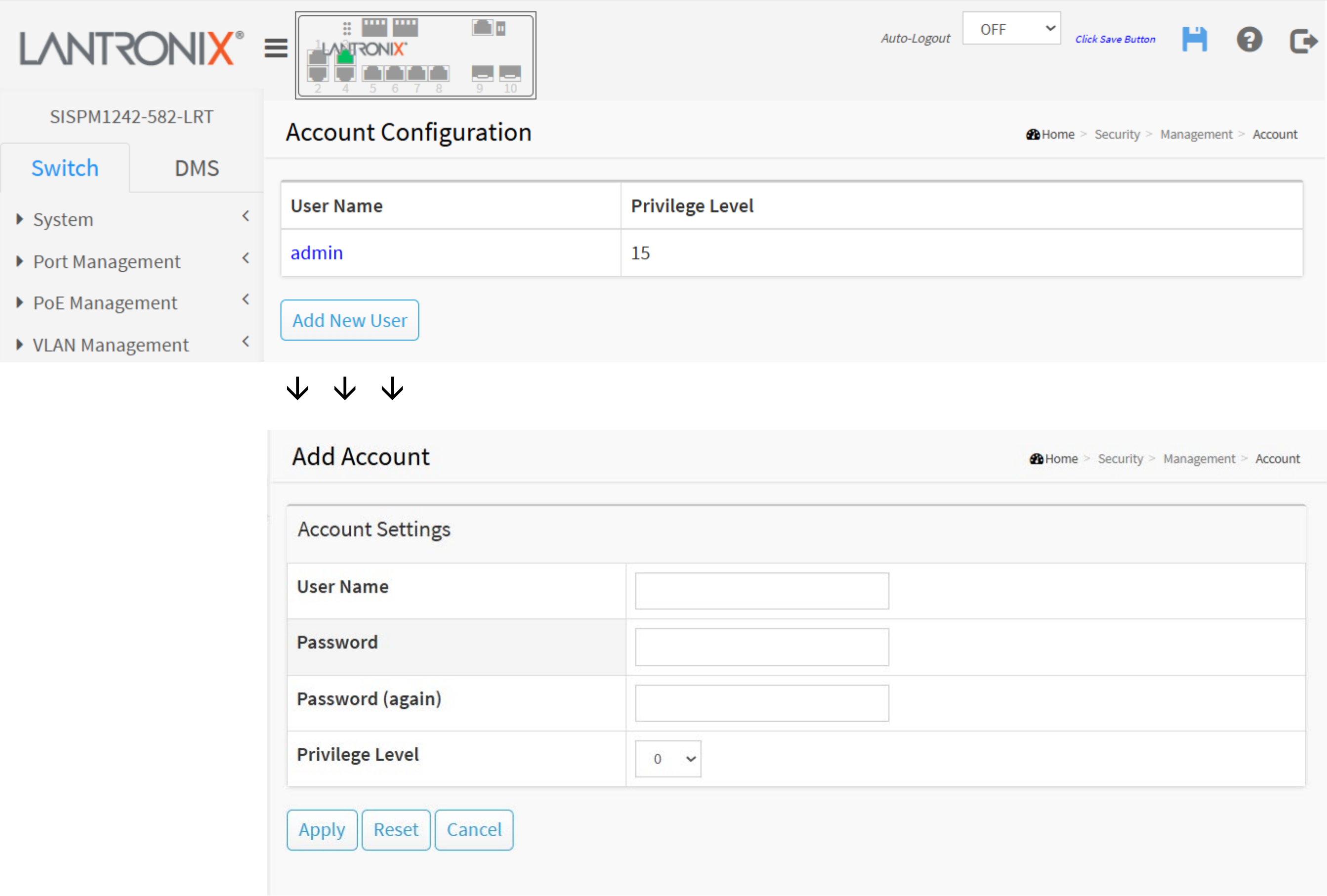
Management

Account

This page provides an overview of the current users and lets you add and configure account users. Currently the only way to login as another user on the web server is to close and reopen the browser.

To add a User in the web UI:

1. Go to Security > Management > Account.
2. Click **Add New User**.
3. Specify the User Name, Password, and Privilege Level parameters.
4. Click **Apply**.



Account Configuration

User Name	Privilege Level
admin	15

Add Account

Account Settings

User Name	
Password	
Password (again)	
Privilege Level	0

Parameter descriptions:

User Name : The name identifying the user. Enter up to 31 characters. This is also a link to Add or Edit a User.

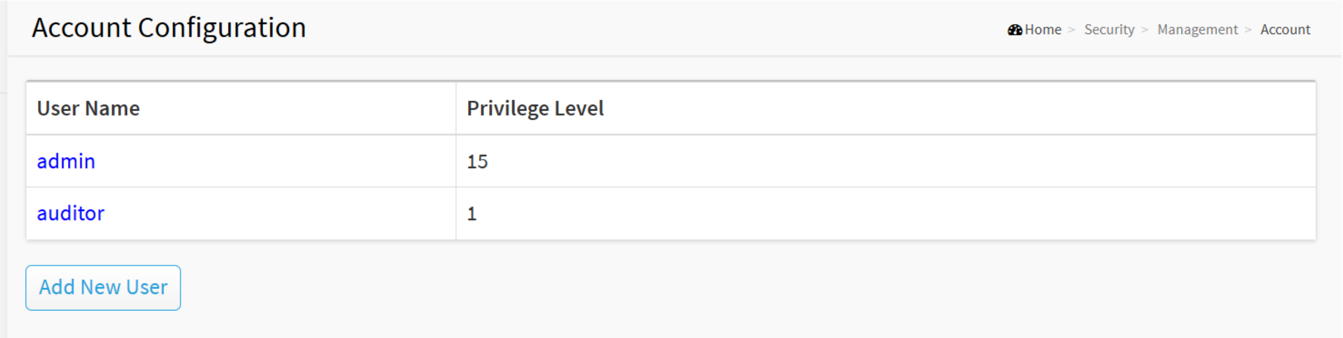
Password : Type the password. The field can be input 31 characters, and the allowed content is ASCII characters 32 - 126.

Password (again) : Type the password again. You must type the exact same password again in this field.

Privilege Level : The privilege level of the user. The valid range is 0 to 15. If the privilege level value is 15, it can access all groups, i.e., that is granted the fully control of the device. But other values must refer to each group privilege level. User's privilege should be same or greater than the group privilege level to have the access of that group. By default setting, most groups privilege level 5 has the read-only access and privilege level 10 has the read-write access. System maintenance functions (software upload, factory defaults etc.) need user privilege level 15. Generally, privilege level 15 is used for an administrator account, privilege level 10 for a standard user account and privilege level 5 for a guest account.

To edit or delete a User in the web UI:

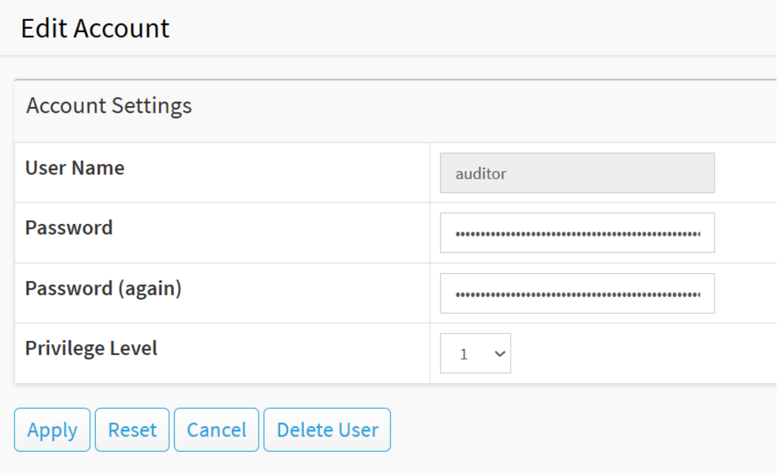
1. Go to Security > Management > Account.



Account Configuration

User Name	Privilege Level
admin	15
auditor	1

2. Click the linked User Name.



Edit Account

Account Settings

User Name	auditor
Password	••
Password (again)	••
Privilege Level	1

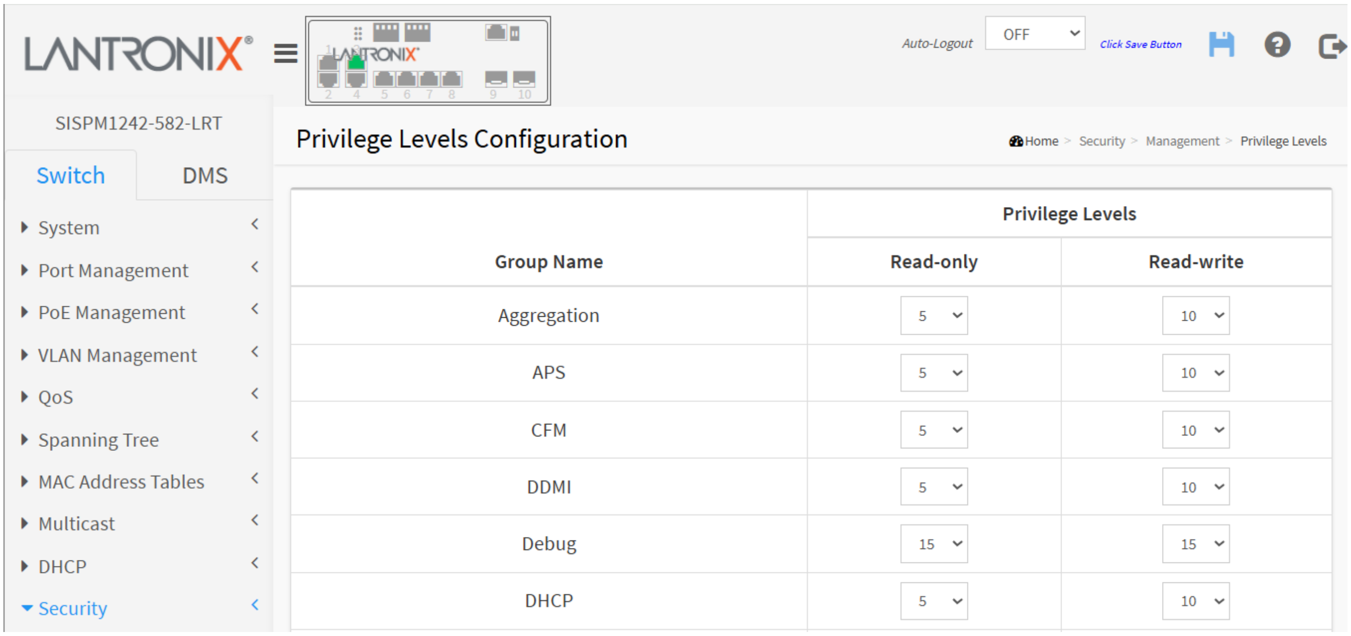
3. Modify the available parameters or click the **Delete User** button.
4. Click **Apply**.

Privilege Levels

This page provides an overview of the privilege levels. Each group can have a Privilege Level setting of 1 to 15.

To configure Privilege Levels in the web UI:

1. Go to Security > Management > Privilege Levels.
2. Specify the Privilege parameters (Read only and Read-write) for the one or more Group Name(s).
3. Click **Apply** to save configuration changes. Click Reset to undo any changes made locally and revert to previously saved values.



Privilege Levels Configuration

Group Name	Privilege Levels	
	Read-only	Read-write
Aggregation	5	10
APS	5	10
CFM	5	10
DDMI	5	10
Debug	15	15
DHCP	5	10

Parameter descriptions:

Group Name : The name identifying the privilege group. In most cases, a privilege level group consists of a single module (e.g., LACP, RSTP or QoS), but a few of them contain more than one. The following defines these privilege level groups in detail:

- ***System***: Contact, Name, Location, Timezone, Daylight Saving Time, Log.
- ***Security***: Authentication, System Access Management, Port (contains Dot1x port, MAC based and the MAC Address Limit), ACL, HTTPS, SSH, ARP Inspection, IP source guard.
- ***IP***: Everything except 'ping'.
- ***Port***: Everything.
- ***Diagnostics***: 'ping'.
- ***Maintenance***: CLI- System Reboot, System Restore Default, System Password, Configuration Save, Configuration Load and Firmware Load. Web- Users, Privilege Levels and everything in Maintenance.
- ***Debug***: Only present in CLI.

Privilege Levels : The Privilege Levels can be configured to 0 - 15 (where 0 is lowest level and 15 is highest level). Every group has an authorization Privilege level for the following sub groups: read-only, read-write. User Privilege should be same or greater than the authorization Privilege level to have the access to that function.

Message: Insufficient Privilege Level

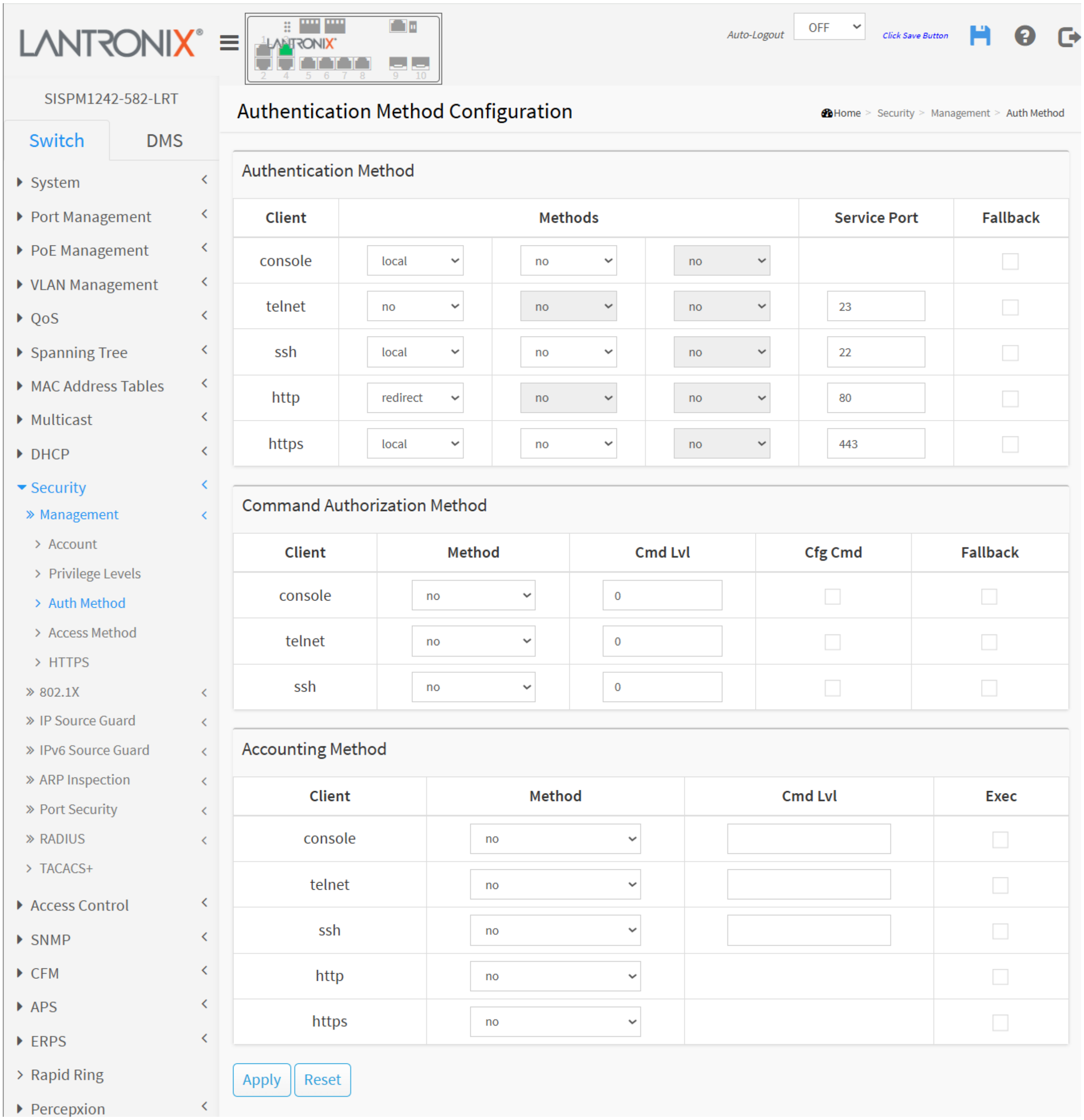
"The web page is non-accessible. Please use the valid privilege level."

Auth Method

Here you can configure a user with one or more Authentication, Authorization, and/or Accounting methods to be used when they log into the switch via one of the management client interfaces.

To configure Auth Method in the web UI:

1. Go to Security > Management > Auth Method.
2. Specify the Client (console, telnet, ssh, http, https) which you want to monitor.
3. Specify the Methods (none, local, radius, tacacs), Service port, Cmd Lvl, Cfg Cmd, Fallback, Exec.
4. Click **Apply**.



Authentication Method Configuration

Authentication Method

Client	Methods			Service Port	Fallback
console	local	no	no		□
telnet	no	no	no	23	□
ssh	local	no	no	22	□
http	redirect	no	no	80	□
https	local	no	no	443	□

Command Authorization Method

Client	Method	Cmd Lvl	Cfg Cmd	Fallback
console	no	0	□	□
telnet	no	0	□	□
ssh	no	0	□	□

Accounting Method

Client	Method	Cmd Lvl	Exec
console	no		□
telnet	no		□
ssh	no		□
http	no		□
https	no		□

Parameter descriptions:

Authentication Method Configuration

Client : The management client for which the configuration below applies.

Method : Authentication Method can be set to one of these values:

- ***none*** : authentication is disabled and login is not possible.
- ***local*** : use the local user database on the switch for authentication.
- ***radius*** : use a remote RADIUS server for authentication.
- ***tacacs*** : use a remote TACACS server for authentication.
- ***http redirect*** : Enable HTTP to HTTPs Automatic Redirect.

Methods that involve remote servers are timed out if the remote servers are offline. In this case the next method is tried. Each method is tried from left to right and continues until a method either approves or rejects a user. If a remote server is used for primary authentication it is recommended to configure secondary authentication as 'local'. This lets the management client login via the local user database if none of the configured authentication servers are alive.

Service Port : The TCP port number for each client service. Valid port numbers are 1 ~ 65534.

Fallback:

Command Authorization Method Configuration

Client : The management client for which the configuration below applies.

Method : Authorization Method can be set to one of these values:

- ***none*** : authorization is disabled, and login is not possible.
- ***tacacs*** : use a remote TACACS+ server for authorization.

Cmd Lvl : Runs authorization for all commands at the specified privilege level. Specific command level that should be authorized. Valid entries are 0 - 15.

Cfg Cmd : Also authorize configuration commands.

Accounting Method Configuration : The accounting section allows you to configure command and exec (login) accounting. The table has one row for each client type and several columns:

Client : The management client for which the configuration below applies.

Method : Method can be set to one of these values:

- ***no*** : Accounting is disabled.
- ***tacacs*** : Use remote TACACS+ server(s) for accounting.

Cmd Lvl : Enable accounting of all commands with a privilege level higher than or equal to this level. Valid values are in the range 0 to 15. Leave the field empty to disable command accounting.

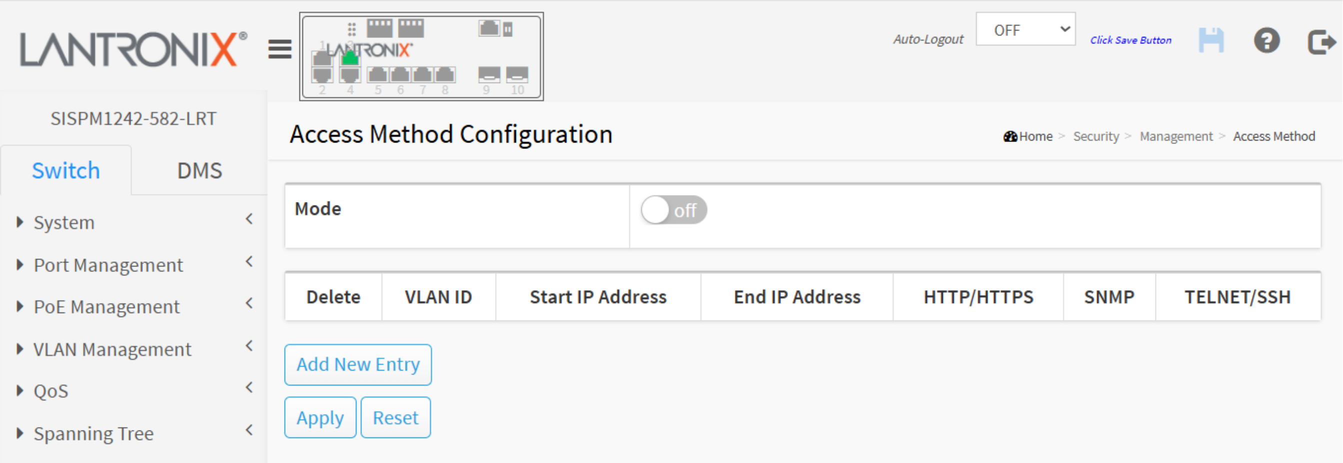
Exec : Enable exec (login) accounting.

Access Method

This page lets you configure access management parameters including HTTP/HTTPS, SNMP, and TELNET/SSH. You can manage the switch over an Ethernet LAN, or over the Internet.

To configure Access Method parameters in the web UI:

1. Go to Security > Management > Access Method.
2. Select “on” in the Mode of Access Management Configuration.
3. Click **Add New Entry**.
4. Specify the VLAN ID, Start IP Address, End IP Address.
5. Check an Access Management method (HTTP/HTTPS, SNMP, and TELNET/SSH) in the entry.
6. Click **Apply**.



Access Method Configuration

Mode	off

Delete	VLAN ID	Start IP Address	End IP Address	HTTP/HTTPS	SNMP	TELNET/SSH

Parameter descriptions:

Mode : Indicates the access management mode operation. Possible modes are:

- ***On*** : Enable access management mode operation.
- ***Off*** : Disable access management mode operation.

VLAN ID : Indicates the VLAN ID for the access management entry.

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

Start IP address : Indicates the start IP unicast address for the access management entry.

End IP address : Indicates the end IP unicast address for the access management entry.

HTTP/HTTPS : Indicates that the host can access the switch from HTTP/HTTPS interface if the host IP address matches the IP address range provided in the entry.

SNMP : Indicates that the host can access the switch from SNMP interface if the host IP address matches the IP address range provided in the entry.

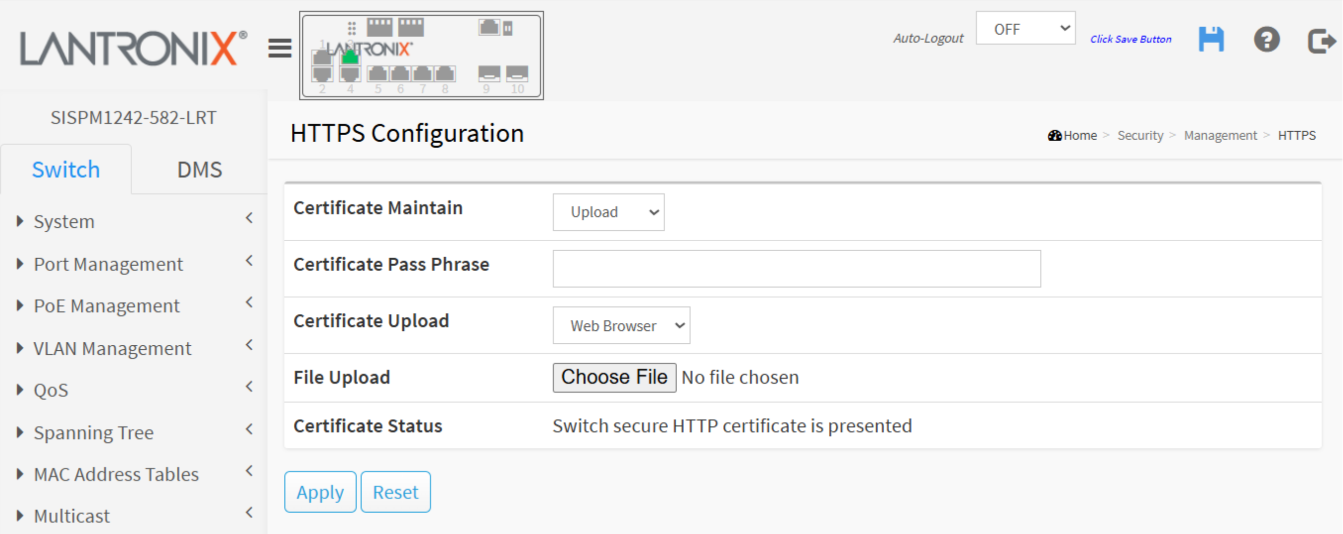
TELNET/SSH : Indicates that the host can access the switch from TELNET/SSH interface if the host IP address matches the IP address range provided in the entry.

HTTPS

This page lets you configure HTTPS settings and maintain a current certificate on the switch.

To configure HTTPS settings in the web UI:

1. Click Configuration > Security > Management > HTTPS.
2. Specify the Certificate Maintain, Certificate Pass Phrase, Certificate Upload.
3. Select the file to upload.
4. Click **Apply**.



HTTPS Configuration

Certificate Maintain	Upload
Certificate Pass Phrase	
Certificate Upload	Web Browser
File Upload	Choose File No file chosen
Certificate Status	Switch secure HTTP certificate is presented

Parameter descriptions:

Certificate Maintain : The operation of certificate maintenance. Possible operations are:

- ***Upload***: Upload a certificate PEM file. Possible Upload methods are ***Web Browser*** or ***URL***. See *Upload Notes* below.
- ***Generate***: Generate a new self-signed RSA certificate.

Certificate Pass Phrase : Enter the pass phrase in this field if your uploading certificate is protected by a specific passphrase.

Certificate Upload : Upload a certificate PEM file into the switch. The file should contain the certificate and private key together. If you have two separated files for saving certificate and private key. Use the Linux cat command to combine them into a single PEM file. For example, cat my.cert my.key > my.pem Notice that the RSA certificate is recommended since most of the new version of browsers has removed support for DSA in certificate, e.g. Firefox v37 and Chrome v39. Possible Certificate Upload methods are:

- ***Web Browser***: Upload a certificate via Web browser.
- ***URL***: Upload a certificate via URL, the supported protocols are HTTP, HTTPS, TFTP and FTP. The URL format is <protocol>://[<username>[:<password>]@]< host>[:<port>][/<path>]/<file_name**>**. For example, *tftp://10.10.10.10/new_image_path/new_image.dat* or *http://username:password@10.10.10.10:80/new_image_path/new_image.dat*.

A valid file name is a text string drawn from alphabet (A-Za-z), digits (0-9), dot (.), hyphen (-), and under score (_). The maximum length is 63 characters, and hyphen must not be first character. A filename that only contains '.' is not allowed.

Certificate Status : Display the 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 ....*

Upload Notes:

1. Ensure that after uploading, you configure any additional required settings such as specifying secure ports or enabling HTTPS exclusively if needed.

2. Remember that using self-signed certificates may trigger security warnings in web browsers because they aren't signed by recognized authorities.

802.1x

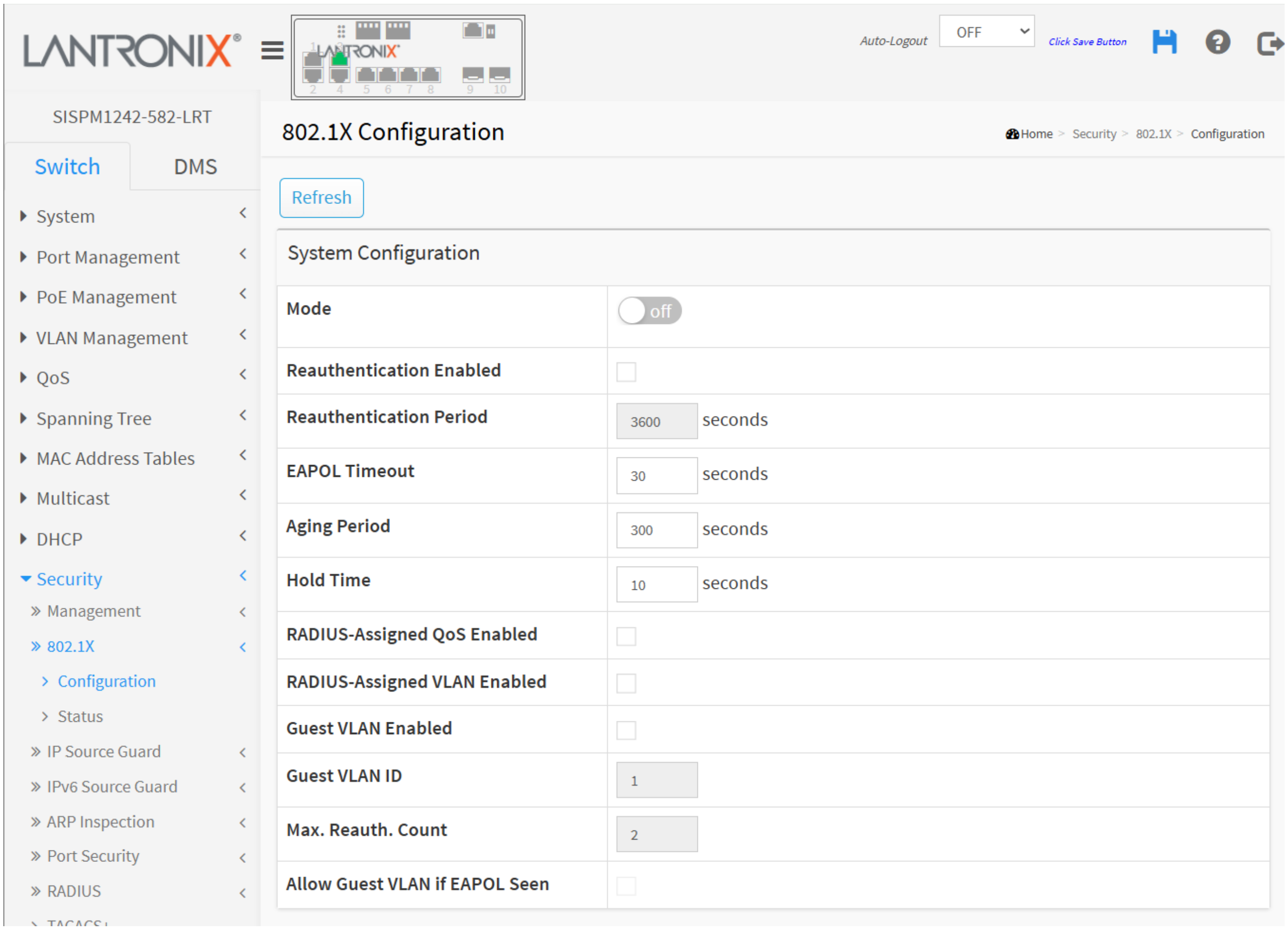
Configuration

Here you can configure the 802.1X parameters of the switch. IEEE 802.1X can be employed to connect users to a variety of resources including Internet access, conference calls, or printing documents on shared printers.

IEEE 802.1X is an IEEE Standard for port-based Network Access Control. It is part of the IEEE 802.1 group of networking protocols. It provides an authentication mechanism to devices wishing to attach to a LAN or WLAN.

To configure IEEE 802.1X in the web UI:

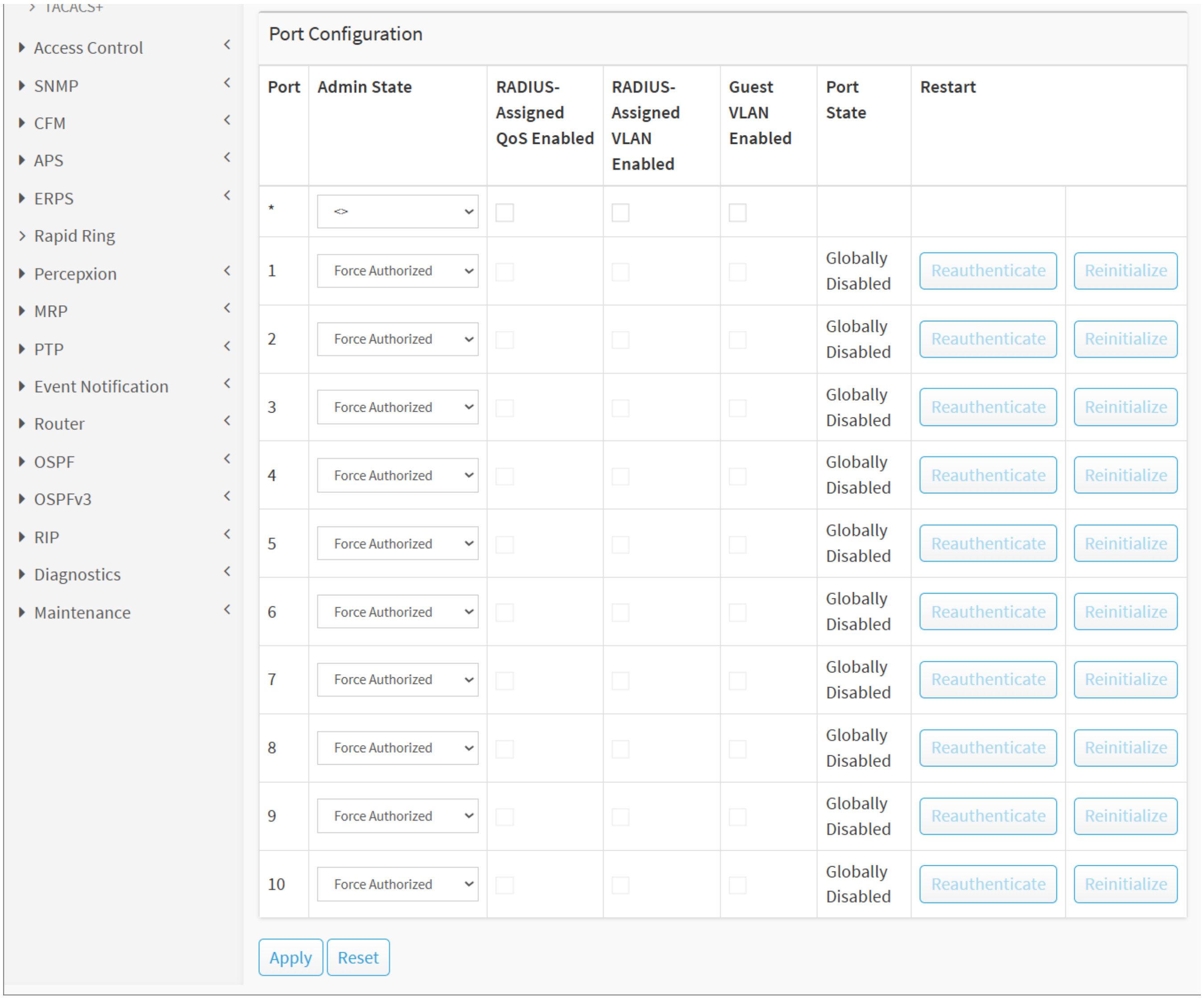
1. Go to Security > 802.1X > Configuration.
2. Set the System Configuration section parameters.
3. Set the Port Configuration section parameters.
4. Click **Apply** to save the settings.



802.1X Configuration

System Configuration

Mode	off
Reauthentication Enabled	□
Reauthentication Period	3600 seconds
EAPOL Timeout	30 seconds
Aging Period	300 seconds
Hold Time	10 seconds
RADIUS-Assigned QoS Enabled	□
RADIUS-Assigned VLAN Enabled	□
Guest VLAN Enabled	□
Guest VLAN ID	1
Max. Reauth. Count	2
Allow Guest VLAN if EAPOL Seen	□



Port Configuration

Port	Admin State	RADIUS-Assigned QoS Enabled	RADIUS-Assigned VLAN Enabled	Guest VLAN Enabled	Port State	Restart	
*	<>	☐	☐	☐			
1	Force Authorized	☐	☐	☐	Globally Disabled	Reauthenticate	Reinitialize
2	Force Authorized	☐	☐	☐	Globally Disabled	Reauthenticate	Reinitialize
3	Force Authorized	☐	☐	☐	Globally Disabled	Reauthenticate	Reinitialize
4	Force Authorized	☐	☐	☐	Globally Disabled	Reauthenticate	Reinitialize
5	Force Authorized	☐	☐	☐	Globally Disabled	Reauthenticate	Reinitialize
6	Force Authorized	☐	☐	☐	Globally Disabled	Reauthenticate	Reinitialize
7	Force Authorized	☐	☐	☐	Globally Disabled	Reauthenticate	Reinitialize
8	Force Authorized	☐	☐	☐	Globally Disabled	Reauthenticate	Reinitialize
9	Force Authorized	☐	☐	☐	Globally Disabled	Reauthenticate	Reinitialize
10	Force Authorized	☐	☐	☐	Globally Disabled	Reauthenticate	Reinitialize

Parameter descriptions:

System Configuration

Mode : on or off. Indicates if IEEE 802.1X is globally enabled or disabled on the switch. If globally disabled, all ports are allowed forwarding of frames.

Reauthentication Enabled : If checked, successfully authenticated supplicants/clients are reauthenticated after the interval specified by the Reauthentication Period. Reauthentication for 802.1X-enabled ports can be used to detect if a new device is plugged into a switch port or if a supplicant is no longer attached.

For MAC-based ports, reauthentication is only useful if the RADIUS server configuration has changed. It does not involve communication between the switch and the client, and therefore doesn't imply that a client is still present on a port (see *Aging Period* below).

Reauthentication Period : Determines the period, in seconds, after which a connected client must be reauthenticated. This is only active if the Reauthentication Enabled checkbox is checked. Valid values are in the range 1 to 3600 seconds.

EAPOL Timeout : Determines the time for retransmission of Request Identity EAPOL frames. IEEE 802.1X defines the encapsulation of the Extensible Authentication Protocol (EAP) over IEEE 802.11, known as "EAP over LAN" or

EAPOL. EAPOL was originally designed for IEEE 802.3 Ethernet in 802.1X-2001.Valid values are 1 - 65535 seconds. This has no effect on MAC-based ports.

Aging Period : This setting applies to the following modes (i.e., modes using the Port Security functionality to secure MAC addresses):

- Single 802.1X
- Multi 802.1X
- MAC-Based Auth

When the NAS module uses the Port Security module to secure MAC addresses, the Port Security module needs to check for activity on the MAC address in question at regular intervals and free resources if no activity is seen within a given period. This parameter controls exactly this period and can be set to a number between 10 and 1000000 seconds. If reauthentication is enabled and the port is in an 802.1X-based mode, this is not so critical, since supplicants that are no longer attached to the port will get removed upon the next reauthentication, which will fail. But if reauthentication is not enabled, the only way to free resources is by aging the entries. For ports in MAC-based Auth. mode, reauthentication doesn't cause direct communication between the switch and the client, so this will not detect whether the client is still attached or not, and the only way to free any resources is to age the entry.

Hold Time : This setting applies to the following modes (i.e., modes using the Port Security function to secure MAC addresses):

- Single 802.1X
- Multi 802.1X
- MAC-Based Auth.

If a client is denied access - either because the RADIUS server denies the client access or because the RADIUS server request times out (according to the timeout specified on the "Configuration > Security > AAA" page) - the client is put on hold in the Unauthorized state. The hold timer does not count during an on-going authentication. In MAC-based Auth. mode, the switch will ignore new frames coming from the client during the hold time. The Hold Time can be set to a number between 10 and 1000000 seconds.

RADIUS-Assigned QoS Enabled : RADIUS-assigned QoS provides a means to centrally control the traffic class to which traffic coming from a successfully authenticated supplicant is assigned on the switch. The RADIUS server must be configured to transmit special RADIUS attributes to take advantage of this feature (see RADIUS-Assigned QoS Enabled below for a detailed description). The "RADIUS-Assigned QoS Enabled" checkbox provides a quick way to globally enable/disable RADIUS-server assigned QoS Class functionality. When checked, the individual ports' ditto setting determines whether RADIUS-assigned QoS Class is enabled on that port. When unchecked, RADIUS-server assigned QoS Class is disabled on all ports.

RADIUS-Assigned VLAN Enabled : RADIUS-assigned VLAN provides a means to centrally control the VLAN on which a successfully authenticated supplicant is placed on the switch. Incoming traffic will be classified to and switched on the RADIUS-assigned VLAN. The RADIUS server must be configured to transmit special RADIUS attributes to take advantage of this feature (see RADIUS-Assigned VLAN Enabled below for a detailed description). The "RADIUS-Assigned VLAN Enabled" checkbox provides a quick way to globally enable/disable RADIUS-server assigned VLAN functionality. When checked, the individual ports' ditto setting determines whether RADIUS-assigned VLAN is enabled on that port. When unchecked, RADIUS-server assigned VLAN is disabled on all ports.

Guest VLAN Enabled : A Guest VLAN is a special VLAN - typically with limited network access - on which 802.1X-unaware clients are placed after a network administrator-defined timeout. The switch follows a set of rules for entering and leaving the Guest VLAN as listed below. The "Guest VLAN Enabled" checkbox provides a quick way to globally enable/disable Guest VLAN functionality. When checked, the individual ports' ditto setting determines whether the port can be moved into Guest VLAN. When unchecked, the ability to move to the Guest VLAN is disabled on all ports.

Guest VLAN ID : This is the value that a port's Port VLAN ID is set to if a port is moved into the Guest VLAN. It can only be changed if the Guest VLAN option is globally enabled. Valid values are in the range [1; 4094].

Max. Reauth. Count : The number of times the switch transmits an EAPOL Request Identity frame without response before considering entering the Guest VLAN is adjusted with this setting. The value can only be changed if the Guest VLAN option is globally enabled. Valid values are in the range [1; 255].

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

Port Configuration

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

Admin State : If 802.1X is globally enabled, this selection sets the port's authentication mode. These modes are available:

- ***Force Authorized*** : In this mode, the switch will send one EAPOL Success frame when the port link comes up, and any client on the port will be allowed network access without authentication.
- ***Force Unauthorized*** : In this mode, the switch will send one EAPOL Failure frame when the port link comes up, and any client on the port will be disallowed network access.
- ***Port-based 802.1X*** : In the 802.1X-world, the user is called the supplicant, the switch is the authenticator, and the RADIUS server is the authentication server. The authenticator acts as the man-in-the-middle, forwarding requests and responses between the supplicant and the authentication server. Frames sent between the supplicant and the switch are special 802.1X frames, known as EAPOL (EAP Over LANs) frames. EAPOL frames encapsulate EAP PDUs (RFC3748). Frames sent between the switch and the RADIUS server are RADIUS packets. RADIUS packets also encapsulate EAP PDUs together with other attributes like the switch's IP address, name, and the supplicant's port number on the switch. EAP is very flexible, in that it allows for different authentication methods, like MD5-Challenge, PEAP, and TLS. The important thing is that the authenticator (the switch) doesn't need to know which authentication method the supplicant and the authentication server are using, or how many information exchange frames are needed for a particular method. The switch simply encapsulates the EAP part of the frame into the relevant type (EAPOL or RADIUS) and forwards it.

  When authentication is complete, the RADIUS server sends a special packet containing a success or failure indication. Besides forwarding this decision to the supplicant, the switch uses it to open 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 not really an IEEE standard, but features many of the same characteristics as does port-based 802.1X. Multi 802.1X is - like Single 802.1X - not an IEEE standard, but a variant that features many of the same characteristics. In Multi 802.1X, one or more supplicants can get authenticated on the same port at the same time. Each supplicant is authenticated individually and secured in the MAC table using the Port Security module.

  In Multi 802.1X it is not possible to use the multicast BPDU MAC address as destination MAC address for EAPOL frames sent from the switch towards the supplicant, since that would cause all supplicants attached to the port to reply to requests sent from the switch. Instead, the switch uses the supplicant's MAC address, which is obtained from the first EAPOL Start or EAPOL Response Identity frame sent by the supplicant. An exception to this is when no supplicants are attached. In this case, the switch sends EAPOL Request Identity frames using the BPDU multicast MAC address as destination - to wake up any supplicants that might be on the port.

  The maximum number of supplicants that can be attached to a port can be limited using the Port Security Limit Control functionality.
- ***MAC-based Auth.:*** Unlike port-based 802.1X, MAC-based authentication is not a standard, but merely a best-practices method adopted by the industry. In MAC-based authentication, users are called clients, and the switch acts as the supplicant on behalf of clients. The initial frame (any kind of frame) sent by a client is snooped by the switch, which in turn uses the client's MAC address as both username and password in the subsequent EAP exchange with the RADIUS server. The 6-byte MAC address is converted to a string on the following form "xx-xx-xx-xx-xx-xx", that is, a dash (-) is used as separator between the lower-cased hexadecimal digits. The switch only supports the MD5-Challenge authentication method, so the RADIUS server must be configured accordingly.

  When authentication is complete, the RADIUS server sends a success or failure indication, which in turn

causes the switch to open up or block traffic for that particular client, using the Port Security module. Only then will frames from the client be forwarded on the switch. There are no EAPOL frames involved in this authentication, and therefore, MAC-based Authentication has nothing to do with the 802.1X standard.
The advantage of MAC-based authentication over port-based 802.1X is that several clients can be connected to the same port (e.g., through a 3rd party switch or a hub) and still require individual authentication, and that the clients don't need special supplicant software to authenticate.
The advantage of MAC-based authentication over 802.1X-based authentication is that the clients don't need special supplicant software to authenticate. The disadvantage is that MAC addresses can be spoofed by malicious users - equipment whose MAC address is a valid RADIUS user can be used by anyone. Also, only the MD5-Challenge method is supported. The maximum number of clients that can be attached to a port can be limited using the Port Security Limit Control functionality.

RADIUS-Assigned QoS Enabled : When RADIUS-Assigned QoS is both globally enabled and enabled (checked) on a given port, the switch reacts to QoS Class information carried in the RADIUS Access-Accept packet transmitted by the RADIUS server when a supplicant is successfully authenticated. If present and valid, traffic received on the supplicant's port will be classified to the given QoS Class. If (re-)authentication fails or the RADIUS Access-Accept packet no longer carries a QoS Class or it's invalid, or the supplicant is otherwise no longer present on the port, the port's QoS Class is immediately reverted to the original QoS Class (which may be changed by the administrator in the meanwhile without affecting the RADIUS-assigned). This option is only available for single-client modes, i.e.:

- Port-based 802.1X
- Single 802.1X RADIUS attributes used in identifying a QoS Class: The User-Priority-Table attribute defined in RFC4675 forms the basis for identifying the QoS Class in an Access-Accept packet. Only the first occurrence of the attribute in the packet will be considered, and to be valid, it must follow this rule:
- All 8 octets in the attribute's value must be identical and consist of ASCII characters in the range '0' - '7', which translates into the desired QoS Class in the range [0; 7].

RADIUS-Assigned VLAN Enabled : When RADIUS-Assigned VLAN is both globally enabled and enabled (checked) for a given port, the switch reacts to VLAN ID information carried in the RADIUS Access-Accept packet transmitted by the RADIUS server when a supplicant is successfully authenticated. If present and valid, the port's Port VLAN ID will be changed to this VLAN ID, the port will be set to be a member of that VLAN ID, and the port will be forced into VLAN unaware mode. Once assigned, all traffic arriving on the port will be classified and switched on the RADIUS-assigned VLAN ID. If (re-)authentication fails or the RADIUS Access-Accept packet no longer carries a VLAN ID or it's invalid, or the supplicant is otherwise no longer present on the port, the port's VLAN ID is immediately reverted to the original VLAN ID (which may be changed by the administrator in the meanwhile without affecting the RADIUS-assigned). This option is only available for single-client modes, such as:

- Port-based 802.1X
- Single 802.1X

For troubleshooting VLAN assignments, use the "Monitor > VLANs > VLAN Membership and VLAN Port" pages. These pages show which modules have (temporarily) overridden the current Port VLAN configuration. RADIUS attributes used in identifying a VLAN ID: RFC2868 and RFC3580 form the basis for the attributes used in identifying a VLAN ID in an Access-Accept packet. The following criteria are used:

- The Tunnel-Medium-Type, Tunnel-Type, and Tunnel-Private-Group-ID attributes must all be present at least once in the Access-Accept packet.

- The switch looks for the first set of these attributes that have the same Tag value and fulfil the following requirements (if Tag == 0 is used, the Tunnel-Private-Group-ID does not need to include a Tag):
  - Value of Tunnel-Medium-Type must be set to "IEEE-802" (ordinal 6).
  - Value of Tunnel-Type must be set to "VLAN" (ordinal 13).
  - Value of Tunnel-Private-Group-ID must be a string of ASCII chars in the range '0' - '9', which is interpreted as a decimal string representing the VLAN ID. Leading '0's are discarded. The final value must be in the range [1; 4095].

Guest VLAN Enabled : When Guest VLAN is both globally enabled and enabled (checked) for a given port, the switch considers moving the port into the Guest VLAN according to the rules outlined below. This option is only available for EAPOL-based modes, i.e.:

- Port-based 802.1X
- Single 802.1X
- Multi 802.1X

For troubleshooting VLAN assignments, use the Monitor > VLANs > VLAN Membership and VLAN Port pages. These pages show which modules have (temporarily) overridden the current Port VLAN configuration. Guest VLAN Operation: When a Guest VLAN enabled port's link comes up, the switch starts transmitting EAPOL Request Identity frames. If the number of transmissions of such frames exceeds Max. Reauth. Count and no EAPOL frames have been received in the meanwhile, the switch considers entering the Guest VLAN. The interval between transmission of EAPOL Request Identity frames is configured with EAPOL Timeout. If Allow Guest VLAN if EAPOL Seen is enabled, the port will now be placed in the Guest VLAN. If disabled, the switch will first check its history to see if an EAPOL frame has previously been received on the port (this history is cleared if the port link goes down or the port's Admin State is changed), and if not, the port will be placed in the Guest VLAN. Otherwise it will not move to the Guest VLAN, but continue transmitting EAPOL Request Identity frames at the rate given by EAPOL Timeout. Once in the Guest VLAN, the port is considered authenticated, and all attached clients on the port are allowed access on this VLAN. The switch will not transmit an EAPOL Success frame when entering the Guest VLAN. While in the Guest VLAN, the switch monitors the link for EAPOL frames, and if one such frame is received, the switch immediately takes the port out of the Guest VLAN and starts authenticating the supplicant according to the port mode. If an EAPOL frame is received, the port will never be able to go back into the Guest VLAN if the "Allow Guest VLAN if EAPOL Seen" is disabled.

Port State : The current state of the port. It can undertake one of the following values:

- ***Globally Disabled***: IEEE 802.1X is globally disabled.
- ***Link Down***: IEEE 802.1X is globally enabled, but there is no link on the port.
- ***Authorized***: The port is in Force Authorized or a single-supplicant mode and the supplicant is authorized.
- ***Unauthorized***: The port is in Force Unauthorized or a single-supplicant mode and the supplicant is not successfully authorized by the RADIUS server.
- ***X Auth/Y Unauth***: The port is in a multi-supplicant mode. Currently X clients are authorized, and Y are unauthorized.

Restart : Two buttons are available for each row. The buttons are only enabled when authentication is globally enabled and the port's Admin State is in an EAPOL-based or MAC-based mode. Clicking these buttons will not cause settings changed on the page to take effect:

- ***Re-authenticate***: Schedules a re-authentication whenever the quiet-period of the port runs out (EAPOL-based authentication). For MAC-based authentication, re-authentication will be attempted immediately.

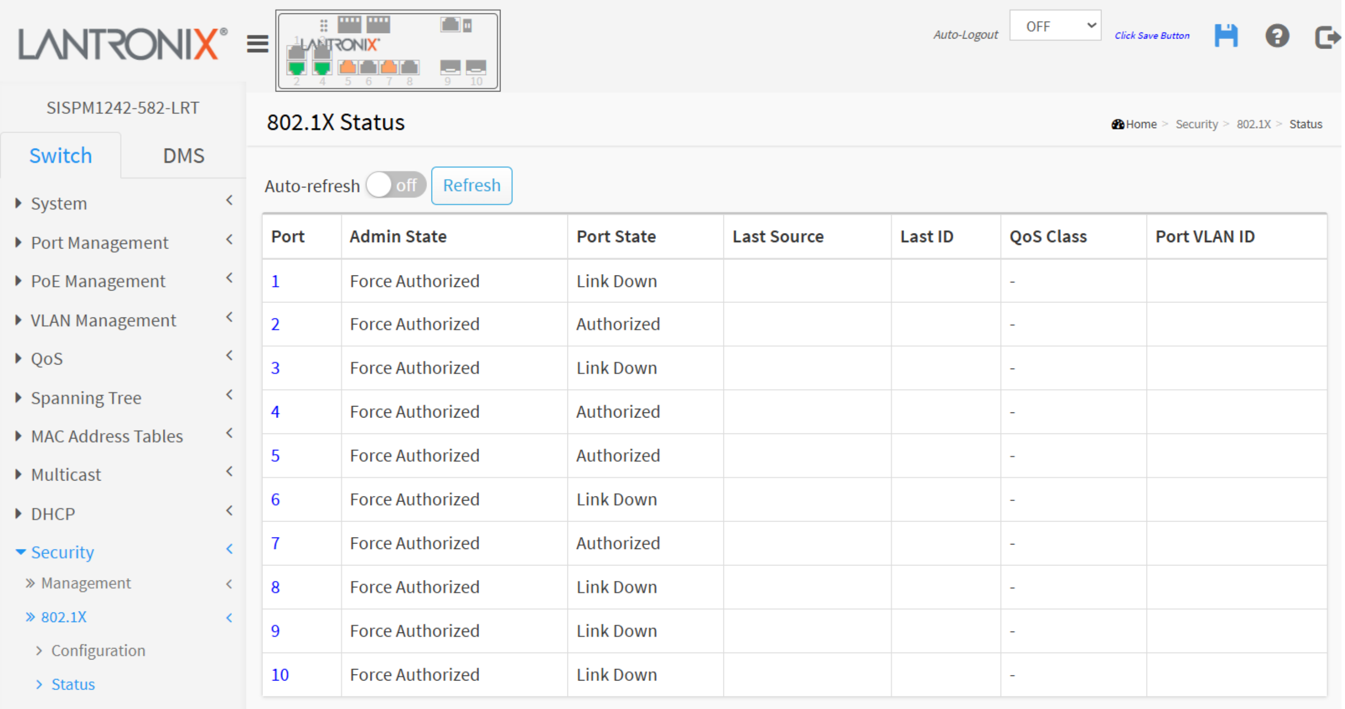
The button only has effect for successfully authenticated clients on the port and will not cause the clients to get temporarily unauthorized.

- ***Reinitialize***: Forces a re-initialization of the clients on the port and thereby a re-authentication immediately. The clients will transfer to the unauthorized state while the re-authentication is in progress.

802.1X Status

This page provides an overview of the current 802.1X port states.

1. Go to Security > 802.1X > Status.
2. **Auto-refresh** will refresh the page every 3 seconds. **Refresh** will refresh the page immediately.



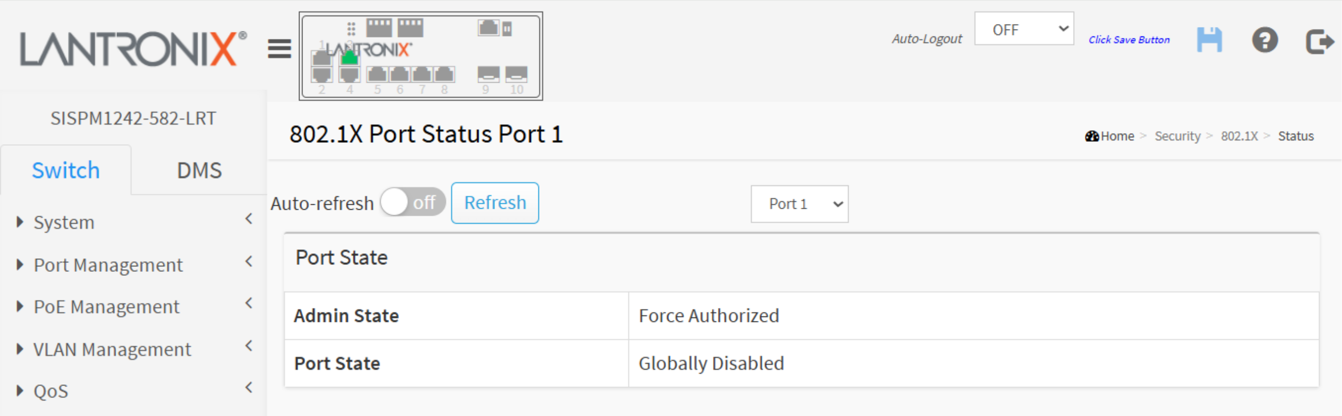
802.1X Status

Port	Admin State	Port State	Last Source	Last ID	QoS Class	Port VLAN ID
1	Force Authorized	Link Down			-	
2	Force Authorized	Authorized			-	
3	Force Authorized	Link Down			-	
4	Force Authorized	Authorized			-	
5	Force Authorized	Authorized			-	
6	Force Authorized	Link Down			-	
7	Force Authorized	Authorized			-	
8	Force Authorized	Link Down			-	
9	Force Authorized	Link Down			-	
10	Force Authorized	Link Down			-	

802.1x Port Status

From the 802.1x Status page, click the linked text port number.

The 802.1X port status page for the designated port is displayed.



802.1X Port Status Port 1

Port State

Admin State	Force Authorized
Port State	Globally Disabled

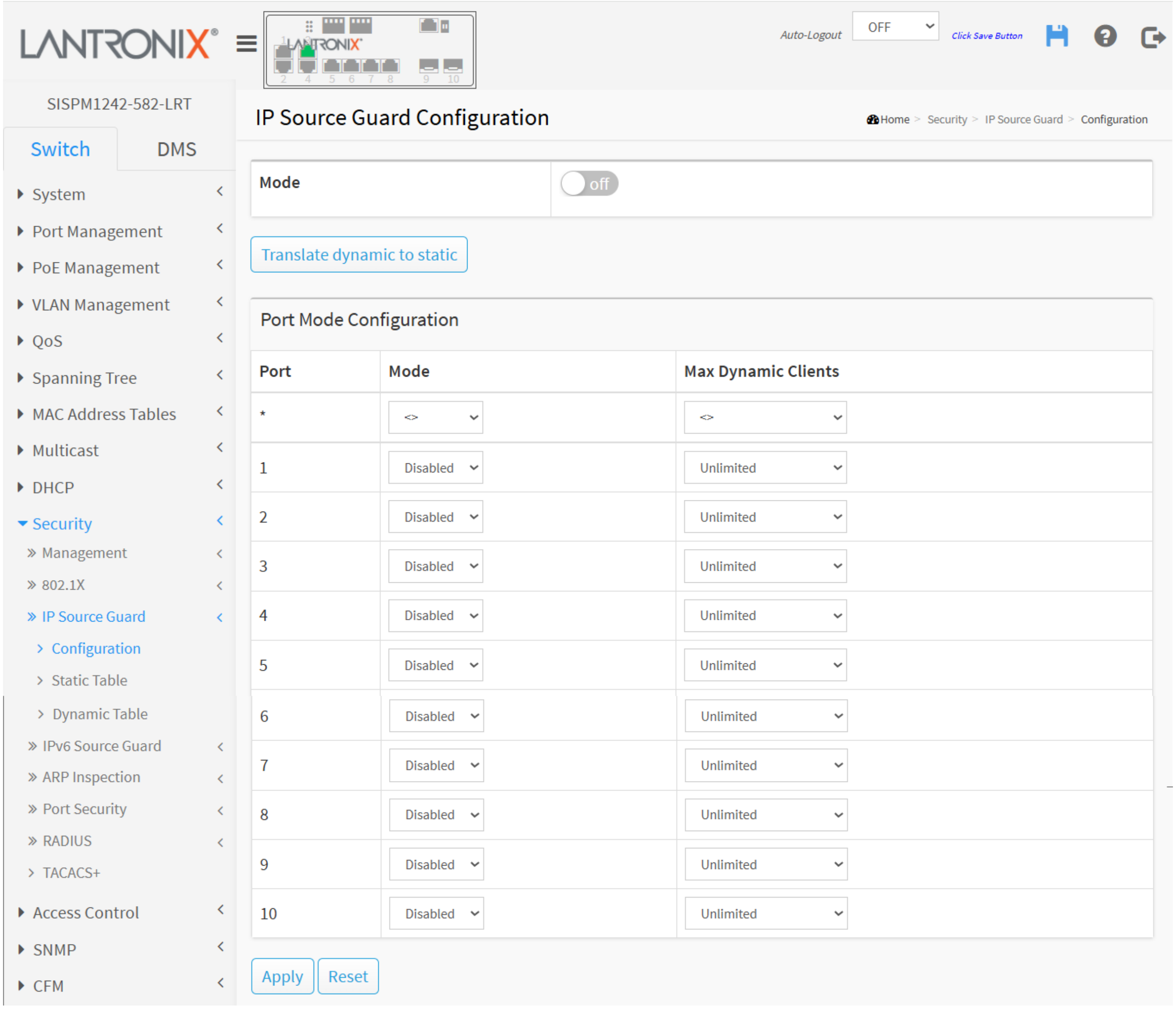
IP Source Guard

This page lets you configure IP Source Guard detail parameters of the switch. You can configure global or port-specific IP Source Guard parameters.

Configuration

To configure IP Source Guard in the web UI:

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



IP Source Guard Configuration

Mode	off

Translate dynamic to static

Port Mode Configuration

Port	Mode	Max Dynamic Clients
*	<>	<>
1	Disabled	Unlimited
2	Disabled	Unlimited
3	Disabled	Unlimited
4	Disabled	Unlimited
5	Disabled	Unlimited
6	Disabled	Unlimited
7	Disabled	Unlimited
8	Disabled	Unlimited
9	Disabled	Unlimited
10	Disabled	Unlimited

Apply Reset

Parameter descriptions :

Mode of IP Source Guard Configuration : Select ***on*** to enable the Global IP Source Guard or select ***off*** to disable the Global IP Source Guard. All configured ACEs will be lost when the mode is on (enabled).

Translate dynamic to static : Click to translate all dynamic entries to static entries.

Port Mode Configuration : Set IP Source Guard to Enabled or Disabled on each port. Only when both Global Mode and Port Mode on a given port are enabled, IP Source Guard is enabled on this given port.

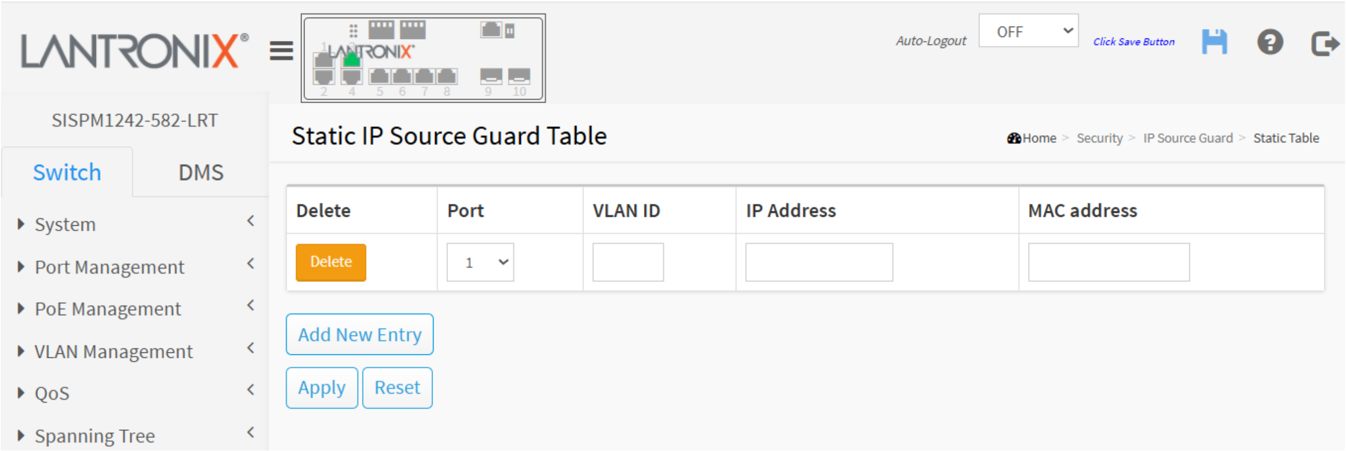
Max Dynamic Clients : Specify the maximum number of dynamic clients that can be learned on given port. This value can be 0, 1, 2 or unlimited. If the Port Mode is enabled and the value of Max Dynamic Clients is 0, it means only allow the IP packets forwarding that are matched in static entries on the specific port.

Static Table

This page lets you configure up to 112 Static IP Source Guard Table rules.

To configure Static IP Source Guard in the web UI:

1. Go to Security > IP Source Guard > Static Table.
2. Click **Add New Entry**.
3. Specify the parameters.
4. Click **Apply**.



Static IP Source Guard Table

Delete	Port	VLAN ID	IP Address	MAC address
Delete	1			

Parameter descriptions :

Add New Entry : Click to add a new entry to the Static IP Source Guard table. Specify the Port, IP address, and MAC address for the new entry. Click **Apply**.

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

Port : At the dropdown select the logical port for the settings.

VLAN ID : The VID for the settings.

IP Address : Allowed Source IP address.

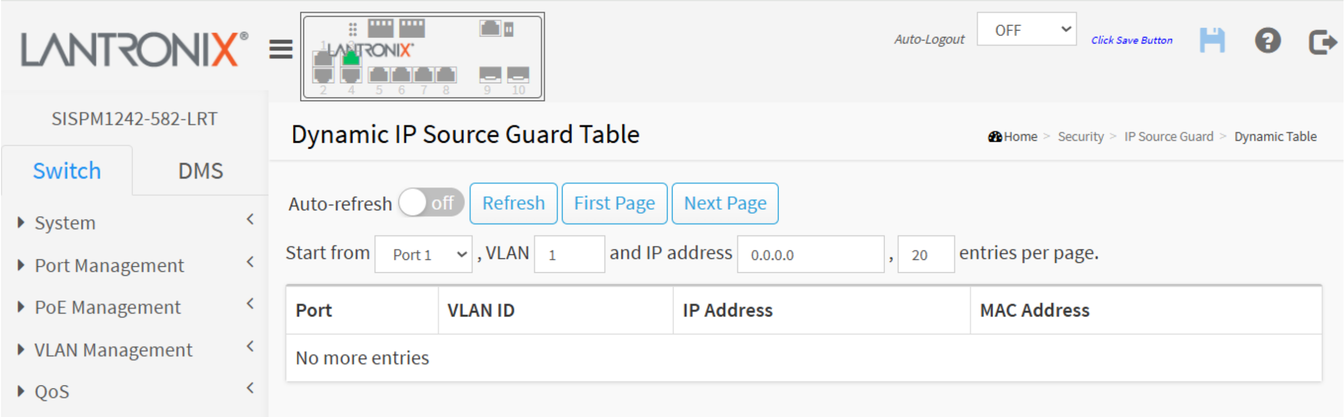
MAC address : Allowed Source MAC address.

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 view Dynamic IP Source Guard Table parameters in the web UI:

1. Go to Security > IP Source Guard > Dynamic Table.



Dynamic IP Source Guard Table

Start from Port 1 , VLAN 1 and IP address 0.0.0.0 , 20 entries per page.

Port	VLAN ID	IP Address	MAC Address
No more entries			

Parameter descriptions :

Port : The switch Port number for which the entries are displayed.

VLAN ID : The VLAN ID in which the IP traffic is permitted.

IP Address : The User IP address of the entry.

MAC Address : The Source MAC address.

IPv6 Source Guard

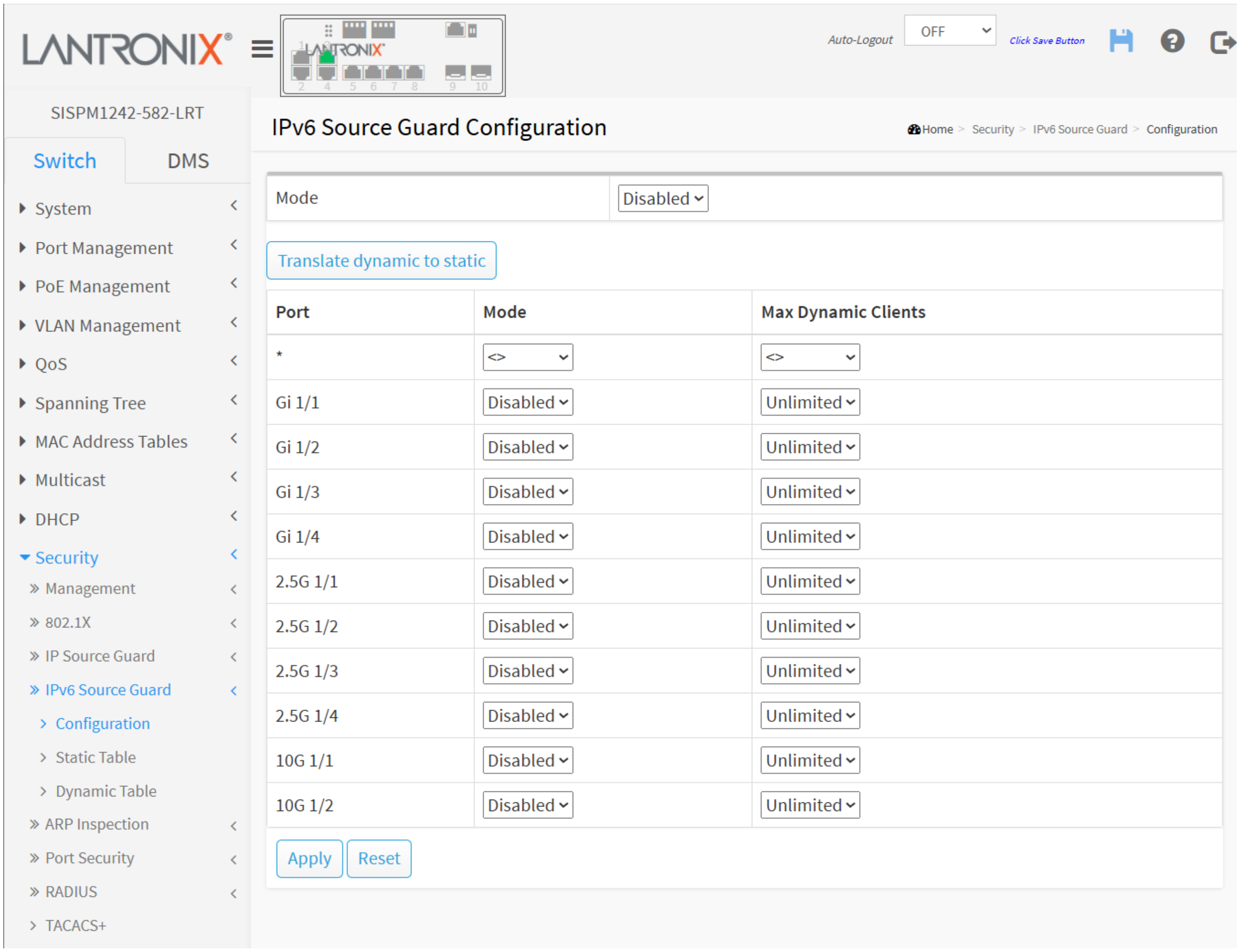
This section provides IPv6 Source Guard related configuration.

IPv6 Source Guard is a security feature used to restrict IPv6 traffic on DHCP snooping untrusted ports by filtering traffic based on the DHCPv6 Snooping Table or manually configured IPv6 Source Bindings. It helps prevent IP spoofing attacks when a host tries to spoof and use the IPv6 address of another host.

Configuration

To configure IPv6 Source Guard in the web UI:

1. Go to Security > IPv6 Source Guard > Configuration.
2. Select “Enabled” at the Mode dropdown.
3. Select “Enabled” of the specific port(s) in the Mode column.
4. Select Maximum Dynamic Clients (0, 1, 2, Unlimited) of the specific port in the Mode of Port Mode Configuration.
5. Click **Apply**.



IPv6 Source Guard Configuration

Mode	Disabled

Port	Mode	Max Dynamic Clients
*	<>	<>
Gi 1/1	Disabled	Unlimited
Gi 1/2	Disabled	Unlimited
Gi 1/3	Disabled	Unlimited
Gi 1/4	Disabled	Unlimited
2.5G 1/1	Disabled	Unlimited
2.5G 1/2	Disabled	Unlimited
2.5G 1/3	Disabled	Unlimited
2.5G 1/4	Disabled	Unlimited
10G 1/1	Disabled	Unlimited
10G 1/2	Disabled	Unlimited

Parameter Descriptions

Mode : Enable or disable the IPv6 Source Guard globally. The global Mode default setting is Disabled.

Translate dynamic to static : Click to translate all dynamic entries to static entries.

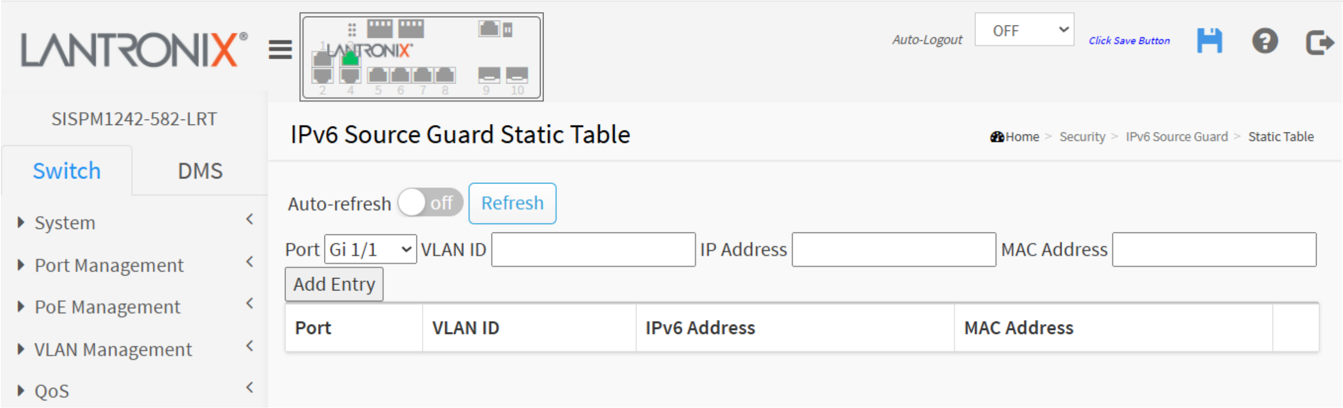
Port Mode Configuration: The table shows all ports on the device. There IPv6 Source Guard can be enabled/disabled on individual ports. Only when both Global Mode and Port Mode on a given port are enabled, IPv6 Source Guard is enabled on this given port. The Mode default setting is Disabled.

Max Dynamic Clients : This value can be 0, 1, 2 or Unlimited. If the port mode is enabled and the value of Max Dynamic Clients is set to 0, only IPv6 packets that are matched in static entries on the specific port are forwarded. The default is Unlimited.

Static Table

This page shows the static IPv6 Source Guard entries. The maximum number of entries is 112 on the switch.

1. Go to Security > IPv6 Source Guard > Static Table.
2. Click **Add Entry** to add a new entry to the static table. Configure the settings.
3. Click **Apply** to save the configuration.



Auto-Logout OFF

IPv6 Source Guard Static Table

Auto-refresh off

Port Gi 1/1 VLAN ID IP Address MAC Address

Port	VLAN ID	IPv6 Address	MAC Address

Parameter descriptions

Add Entry : Click to add a new entry to the Static IPv6 Source Guard table. **Note**: IP address and MAC address must be entered.

Delete : Click entry Delete button to delete the entry.

Port : The logical port the entry is bound to.

VLAN ID : The VLAN id for the settings. If no VLAN ID is associated with the entry, this field shows 0.

IPv6 Address : Allowed Source IPv6 address.

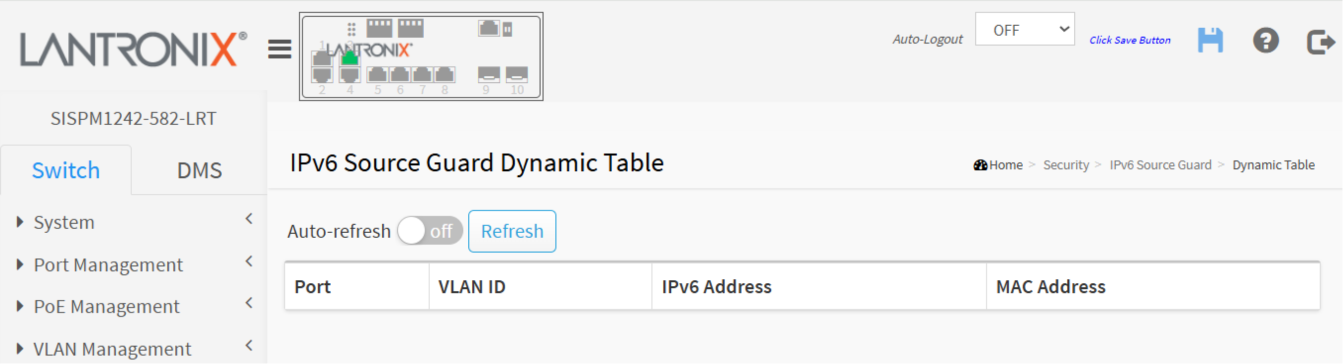
Prefix Size : Prefix size of the IPv6 address.

MAC address : Allowed Source MAC address.

Dynamic Table

Entries in the Dynamic IPv6 Source Guard Table are shown on this page.

1. Go to Security > IPv6 Source Guard.



IPv6 Source Guard Dynamic Table

Port	VLAN ID	IPv6 Address	MAC Address

Port : Switch Port Number for which the entries are displayed.

VLAN ID : VLAN ID in which the IP traffic is permitted. If no VLAN-ID is associated with the entry, this field shows 0.

IP Address : User IPv6 address of the entry.

MAC Address : Source MAC address.

ARP Inspection

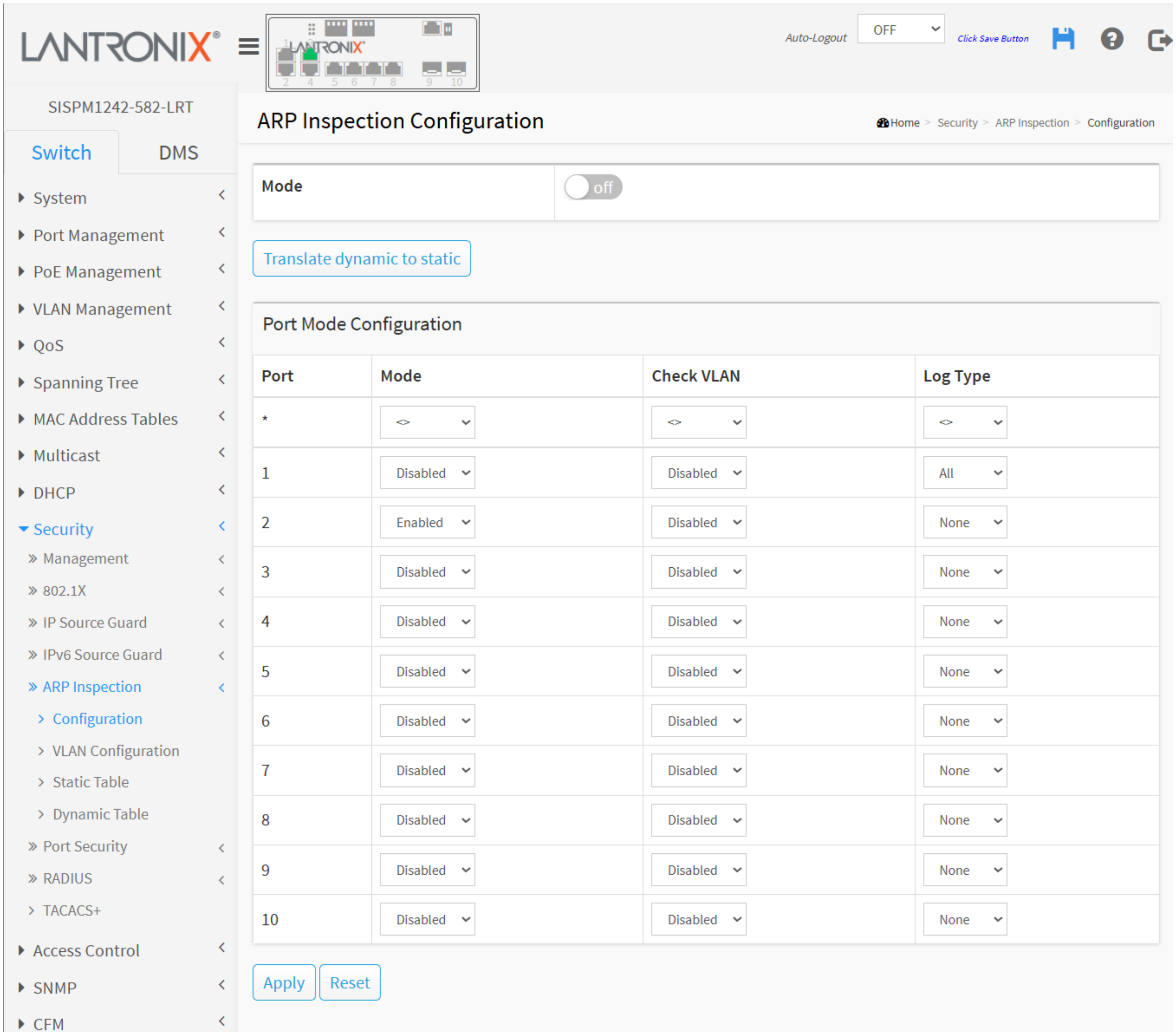
This section lets you configure ARP Inspection parameters. You can use ARP Inspection to manage the ARP table.

ARP Inspection is a security feature. Several types of attacks can be launched against a host or devices connected to Layer 2 networks by "poisoning" the ARP caches. This feature is used to block such attacks. Only valid ARP requests and responses can go through the switch.

Configuration

To configure ARP Inspection in the web UI:

1. Go to Security > ARP Inspection > Configuration.
2. Enable the Mode in the ARP Inspection Configuration section.
3. Select “Enabled” for the specific port(s) at the Mode dropdown in the Port Mode Configuration section.
4. Set the Port Mode Configuration parameters.
5. Click the **Translate dynamic to static** button to translate all dynamic entries to static entries.
6. Click **Apply**.



ARP Inspection Configuration

Mode	off

Port Mode Configuration

Port	Mode	Check VLAN	Log Type
*	<>	<>	<>
1	Disabled	Disabled	All
2	Enabled	Disabled	None
3	Disabled	Disabled	None
4	Disabled	Disabled	None
5	Disabled	Disabled	None
6	Disabled	Disabled	None
7	Disabled	Disabled	None
8	Disabled	Disabled	None
9	Disabled	Disabled	None
10	Disabled	Disabled	None

Parameter descriptions :

ARP Inspection Configuration section :

Mode : Select ***on*** to enable ARP Inspection globally or select ***off*** to disable ARP Inspection globally. The default is disabled (off).

Translate dynamic to static button : Click to translate all dynamic entries to static entries.

Port Mode Configuration section :

Mode: Set ARP Inspection to Enabled or Disabled on each port. ARP Inspection is enabled on a given port only when both Global Mode and Port Mode on a given port are enabled. Possible modes are:

- ***Enabled***: Enable ARP Inspection operation.
- ***Disabled***: Disable ARP Inspection operation.

Check VLAN : If you want to inspect the VLAN configuration, you must 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. The possible settings are:

- ***Disabled*** : the log type of ARP Inspection will refer to the port setting. Disable check VLAN operation. Only the Global Mode and Port Mode on a given port are enabled, and the setting of "Check VLAN" is disabled, the log type of ARP Inspection will refer to the port setting.
- ***Enabled*** : Enable check VLAN operation; the log type of ARP Inspection will refer to the VLAN setting.

Log Type : 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 possible log types are:

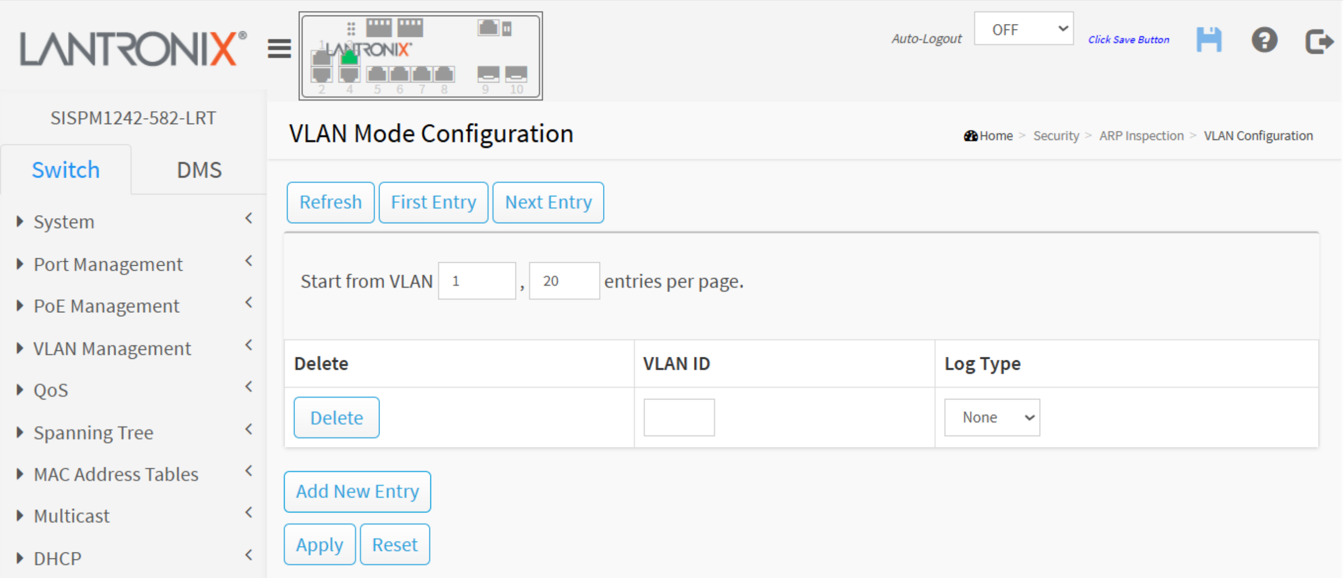
- ***None***: Log nothing.
- ***Deny***: Log only denied entries.
- ***Permit***: Log only permitted entries.
- ***ALL***: Log all entries.

VLAN Configuration

Specify the VLANs on which ARP Inspection is enabled.

To configure VLAN Mode in the web UI:

1. Go to Security > ARP Inspection > VLAN Configuration.
2. Click **Add New Entry**.
3. Specify the VLAN ID and Log Type.
4. Click **Apply**.



VLAN Mode Configuration

Start from VLAN 1 , 20 entries per page.

Delete	VLAN ID	Log Type
Delete		None

Parameter descriptions:

- **Add New Entry :** Click to add a new VLAN to the ARP Inspection VLAN table.
- **Delete :** Check to delete the entry. It will be deleted during the next save.

VLAN ID: 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, you can specify which VLAN will be inspected on VLAN mode configuration web page.

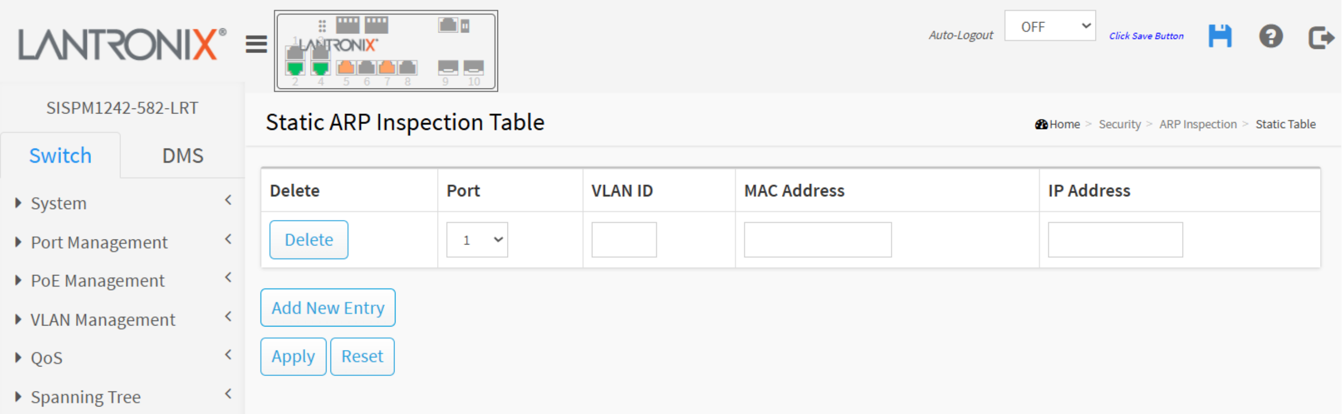
Log Type: The log type also can be configured on per VLAN setting. Possible types are:

- ***None***: Log nothing.
- ***Deny***: Log denied entries.
- ***Permit***: Log permitted entries.
- ***ALL***: Log all entries.

Static Table

This page lets you configure Static ARP Inspection parameters. To configure Static ARP Inspection in the web UI:

1. Go to Security > ARP Inspection > Static Table.
2. Click **Add New Entry**.
3. Specify the Port, VLAN ID, IP Address, MAC address, and IP Address in the entry.
4. Click **Apply**.



Static ARP Inspection Table

Delete	Port	VLAN ID	MAC Address	IP Address
Delete	1			

Parameter descriptions:

Add New Entry : Click to add a new entry to the Static ARP Inspection table.

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.

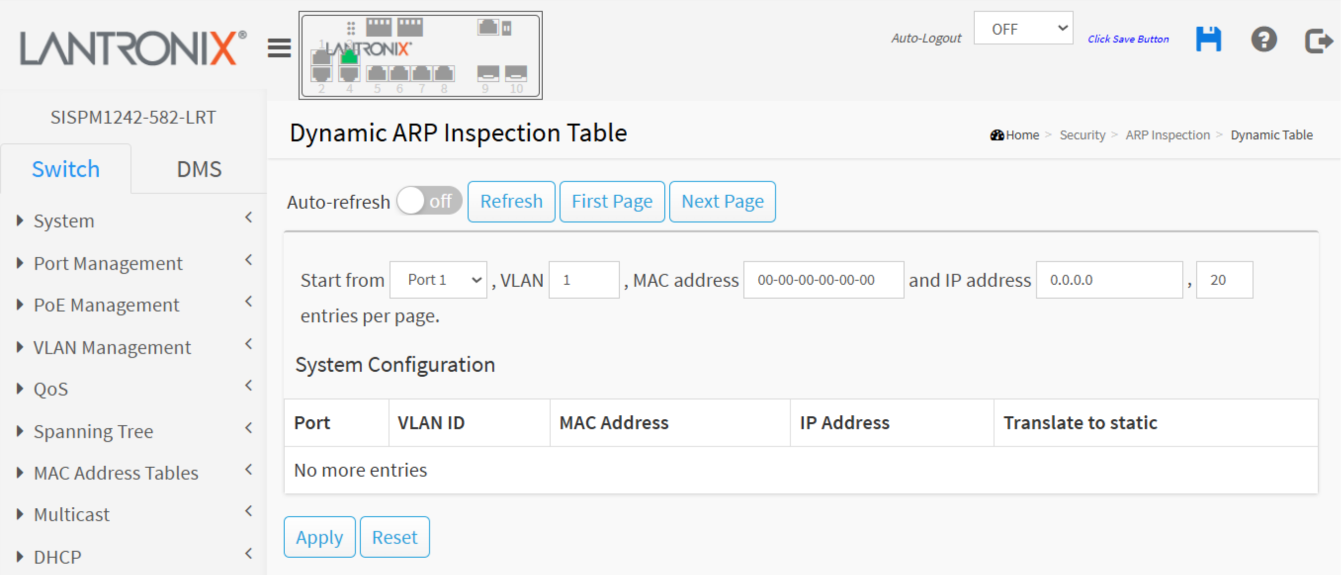
IP Address : Allowed Source IP address in ARP request packets.

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 learned from DHCP Snooping.

To configure Dynamic ARP Inspection in the web UI:

1. Go to Security > ARP Inspection > and Dynamic Table.



Dynamic ARP Inspection Table

Start from Port 1, VLAN 1, MAC address 00-00-00-00-00-00 and IP address 0.0.0.0, 20 entries per page.

System Configuration

Port	VLAN ID	MAC Address	IP Address	Translate to static
No more entries				

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 display.

Port Security

Configuration

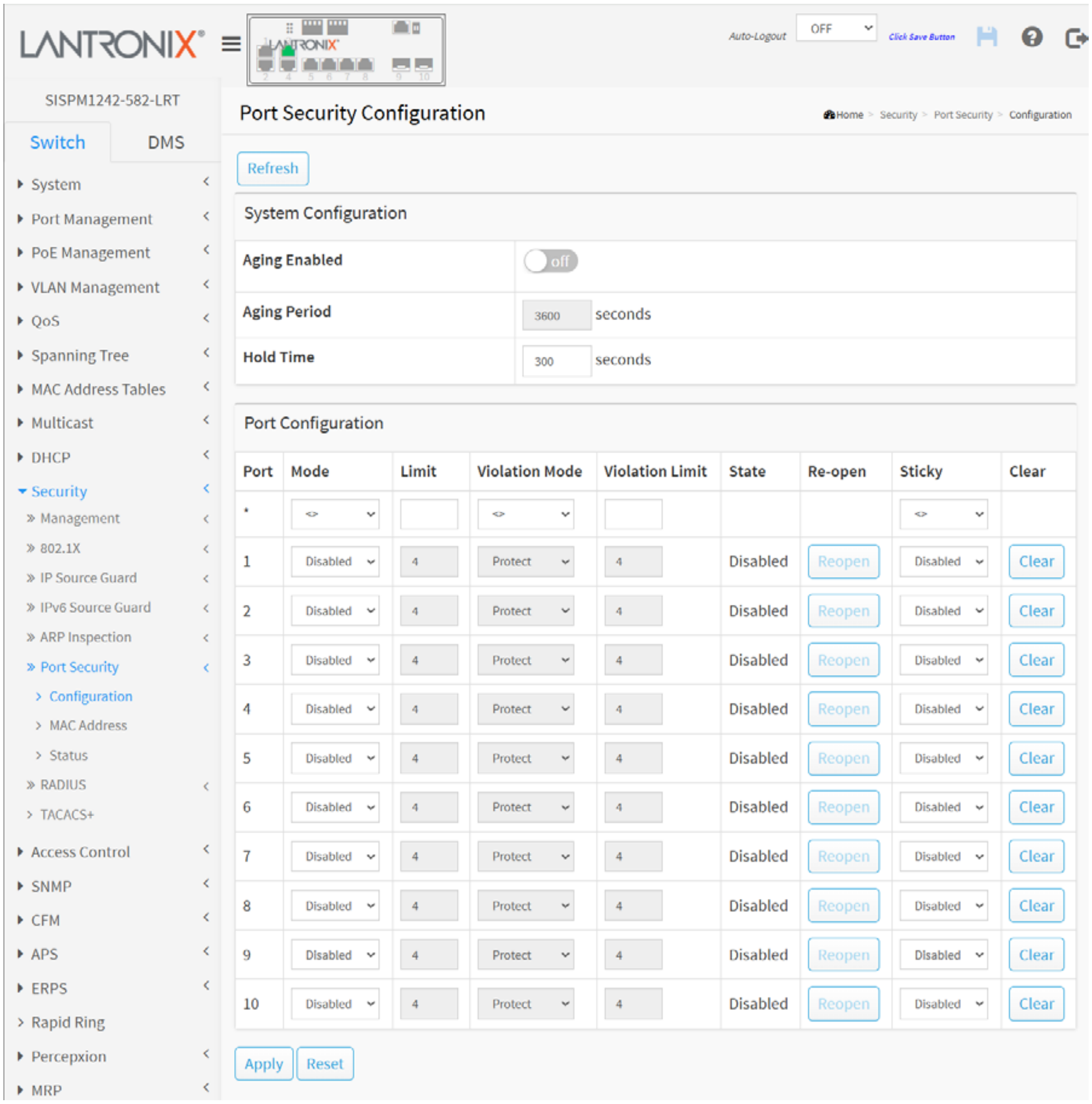
This page lets you configure Port Security settings. You can use the Port Security feature to restrict input to an interface by limiting and identifying MAC addresses.

This page allows you to configure the 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.

The Port Security configuration consists of global and per-port configuration.

To configure Port Security in the web UI:

1. Go to Security > Port Security > Configuration.
2. Set the global and port configuration parameters.
3. Click the **Apply** button to save the configuration.



Port Security Configuration

System Configuration

Aging Enabled	off
Aging Period	3600 seconds
Hold Time	300 seconds

Port Configuration

Port	Mode	Limit	Violation Mode	Violation Limit	State	Re-open	Sticky	Clear
*	<>		<>				<>	
1	Disabled	4	Protect	4	Disabled	Reopen	Disabled	Clear
2	Disabled	4	Protect	4	Disabled	Reopen	Disabled	Clear
3	Disabled	4	Protect	4	Disabled	Reopen	Disabled	Clear
4	Disabled	4	Protect	4	Disabled	Reopen	Disabled	Clear
5	Disabled	4	Protect	4	Disabled	Reopen	Disabled	Clear
6	Disabled	4	Protect	4	Disabled	Reopen	Disabled	Clear
7	Disabled	4	Protect	4	Disabled	Reopen	Disabled	Clear
8	Disabled	4	Protect	4	Disabled	Reopen	Disabled	Clear
9	Disabled	4	Protect	4	Disabled	Reopen	Disabled	Clear
10	Disabled	4	Protect	4	Disabled	Reopen	Disabled	Clear

Parameter descriptions:

System Configuration

Aging Enabled : If checked (on), secured MAC addresses are subject to aging as discussed under Aging Period.

Aging Period : If Aging Enabled is checked (on), then the aging period is controlled with this input. If other modules are using the underlying functionality for securing MAC addresses, they may have other requirements to the aging period. The underlying functionality will use the shorter requested aging period of all modules that have aging enabled.

The Aging Period can be set to a number between 10 and 10000000 seconds with a default of 3600 seconds.

To understand why aging may be desired, consider the following scenario: Suppose an end-host is connected to a 3rd party switch or hub, which in turn is connected to a port on this switch on which Port Security is enabled. The end-host will be allowed to forward if the limit is not exceeded. Now suppose that the end-host logs off or powers down. If it wasn't for aging, the end-host would still take up resources on this switch and will be allowed to forward. To overcome this situation, enable aging. With aging enabled, a timer is started once the end-host gets secured. When the timer expires, the switch starts looking for frames from the end-host, and if such frames are not seen within the next Aging Period, the end-host is assumed to be disconnected, and the corresponding resources are freed on the switch.

Hold Time : The hold time - measured in seconds - is used to determine how long a MAC address is held in the MAC table if it has been found to violate the limit. The valid range is 10 - 10000000 seconds with a default of 300 seconds. The reason for holding a violating MAC address in the MAC table is primarily to ensure that the same MAC address doesn't give rise to continuous notifications (if notifications on violation count is enabled).

Port Configuration :

The table has one row for each port on the switch and several columns:

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

Mode : Controls whether Limit Control is enabled on this port. Both this and the Global Mode must be set to Enabled for Limit Control to be in effect. Note that other modules may still use the underlying port security features without enabling Limit Control on a given port.

Limit : The maximum number of MAC addresses that can be secured on this port. This number cannot exceed 1024. If the limit is exceeded, the corresponding action is taken. The switch is "born" with a total number of MAC addresses from which all ports draw whenever a new MAC address is seen on a Port Security-enabled port. Since all ports draw from the same pool, it may happen that a configured maximum cannot be granted, if the remaining ports have already used all available MAC addresses.

Violation Mode : If Limit is reached, the switch can take one of the following actions:

- ***Protect***: Do not allow more than Limit MAC addresses on the port, but take no further action.
- ***Restrict***: If Limit is reached, subsequent MAC addresses on the port will be counted and marked as violating. Such MAC addresses are removed from the MAC table when the hold time expires. At most Violation Limit MAC addresses can be marked as violating at any given time.
- ***Shutdown***: If Limit is reached, one additional MAC address will cause the port to be shut down. This implies that all secured MAC addresses be removed from the port, and no new addresses be learned. There are three ways to re-open the port: 1) In the "Configuration > Ports" page's "Configured" column, first disable the port, then restore the original mode. 2) Make a Port Security configuration change on the port. 3) Boot the switch.

Violation Limit : The maximum number of MAC addresses that can be marked as violating on this port. This number cannot exceed 1023. The default is 4. It is only used when Violation Mode is ‘Restrict’.

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

- ***Disabled***: Limit Control is either globally disabled or disabled on the port.
- ***Ready***: The limit is not yet reached. This can be shown for all actions.
- ***Limit Reached***: Indicates that the limit is reached on this port. This state only displays if Action is set to none or Trap.
- ***Shutdown***: Indicates that the port is shut down by the Limit Control module. This state can only be displayed if Action is set to Shutdown or Trap & Shutdown.

Re-open : Click to re-open the port.

Sticky : Enables sticky learning of MAC addresses on this port. When the port is in sticky mode, all MAC addresses that would otherwise have been learned as dynamic are learned as sticky.

Sticky MAC addresses are part of the running-config and can therefore be saved to startup-config. Sticky MAC addresses survive link changes (in contrast to Dynamic, which will have to be learned again). They also survive reboots if running-config is saved to startup-config.

A port can be Sticky-enabled whether or not Port Security is enabled on that interface. In that way, it is possible to add sticky MAC addresses management-wise before enabling Port Security. To do that, use the page at "Configuration > Security > Port Security > MAC Addresses".

Clear : Click to clear the violation on the port.

MAC Address

This page lets you add and delete static and sticky MAC addresses managed by Port Security.

Port security defines three types of MAC addresses, of which static and sticky can be added and removed on this page:

Dynamic: A MAC address learned through learn frames coming to the Port Security module while the interface in question is not in sticky mode. Dynamic entries disappear if it ages out or if the interface link goes down.

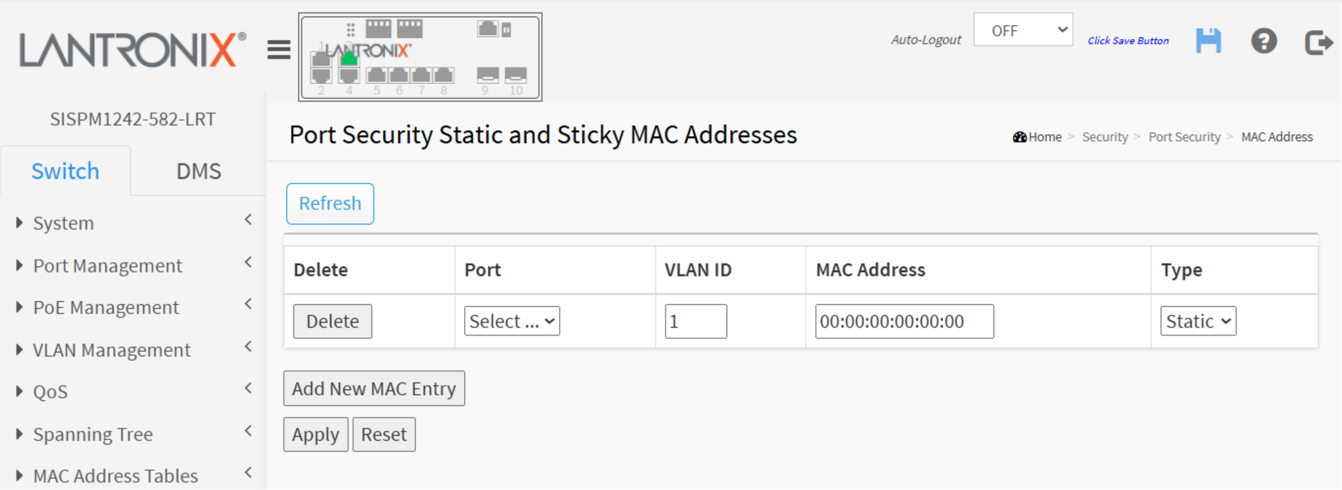
Static: A MAC address added by end-user through management. Static MAC addresses are not subject to aging and will be added to the MAC address table once Port Security gets enabled on the interface. Static entries are part of the running-config and will survive interface link state changes and reboots if saved to startup-config. Static entries can be added to the running-config at any time whether or not Port Security is enabled.

Sticky: When the interface is in Sticky mode, all entries that would otherwise have been learned as dynamic are learned as sticky. Like static entries, sticky entries are part of the running-config and will survive interface link state changes and reboots if saved to the startup-config. Though not the intention with Sticky entries, they can be added by management to the running-config at any time whether or not Port Security is enabled on the interface, as long as the interface is in Sticky mode. Sticky entries will disappear if the interface is taken out of Sticky mode.

To configure static and sticky MAC addresses in the Web UI:

1. Go to Security > Port Security > MAC Address.
2. Click the Add New MAC Entry button.
3. At the dropdown select a Port.

4. Select the desired Port and enter the MAC address.
5. Select the type of entry; either Static or Sticky.
6. Click the **Apply** button.



Port Security Static and Sticky MAC Addresses

Delete	Port	VLAN ID	MAC Address	Type
Delete	Select ...	1	00:00:00:00:00:00	Static

The table contains one row per static or sticky MAC address.

Buttons:

Add New MAC Entry : Clicking this button will add a new row to the table. This new row allows for adding a static or sticky MAC address to a particular interface. Once satisfied, click the **Apply** button to save the changes to running-config. **Note** that Sticky entries are normally added automatically through learning on the interface.

Delete : Press this button to remove the entry from the MAC address table (if present) and the running-config.

Notice that dynamic entries may be removed all-together on an interface at "Monitor > Security > Port Security > Switch" and one-by-one through "Monitor > Security > Port Security > Port".

Parameter descriptions:

Port Select: At the dropdown select the port number to which this MAC address is to be bound (1-14).

VLAN ID : Enter the desired VLAN ID (VID).

MAC Address : Enter the desired MAC address.

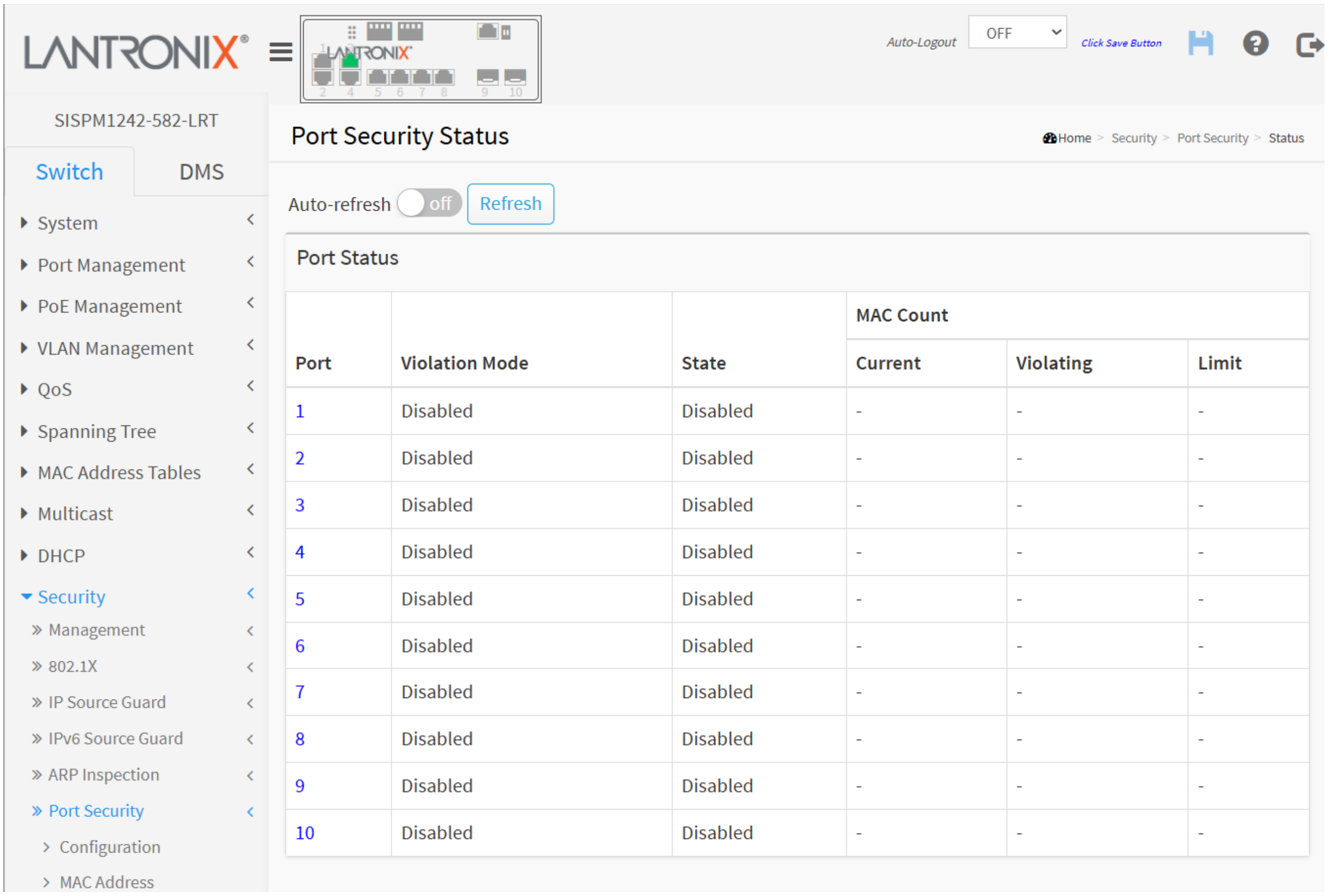
Type : At the dropdown select the type of entry; may be either Static or Sticky (see description above).

Status

This page shows the Port Security status. Port Security is a module with no direct configuration. Configuration comes indirectly from other modules - the user modules. When a user module has enabled port security on a port, the port is set-up for software-based learning. In this mode, frames from unknown MAC addresses are passed on to the port security module, which in turn asks all user modules whether to allow this new MAC address to forward or block it. For a MAC address to be set in the forwarding state, all enabled user modules must unanimously agree on allowing the MAC address to forward. If only one user chooses to block it, it will be blocked until that user module decides otherwise.

To display Port Security Status in the web UI:

1. Go to Security > Port Security > Status.
2. Click the port number to view the status for that port.
3. **Auto-refresh** will refresh the page every 3 seconds. **Refresh** will refresh the page immediately.



Port Security Status

Auto-refresh off Refresh

Port Status

Port	Violation Mode	State	MAC Count		
			Current	Violating	Limit
1	Disabled	Disabled	-	-	-
2	Disabled	Disabled	-	-	-
3	Disabled	Disabled	-	-	-
4	Disabled	Disabled	-	-	-
5	Disabled	Disabled	-	-	-
6	Disabled	Disabled	-	-	-
7	Disabled	Disabled	-	-	-
8	Disabled	Disabled	-	-	-
9	Disabled	Disabled	-	-	-
10	Disabled	Disabled	-	-	-

Parameter descriptions:

Port : The port number for which the status applies. Click the linked port number to view the status for this port.

Violation Mode : Shows the configured Violation Mode of the port. It displays one of four values:

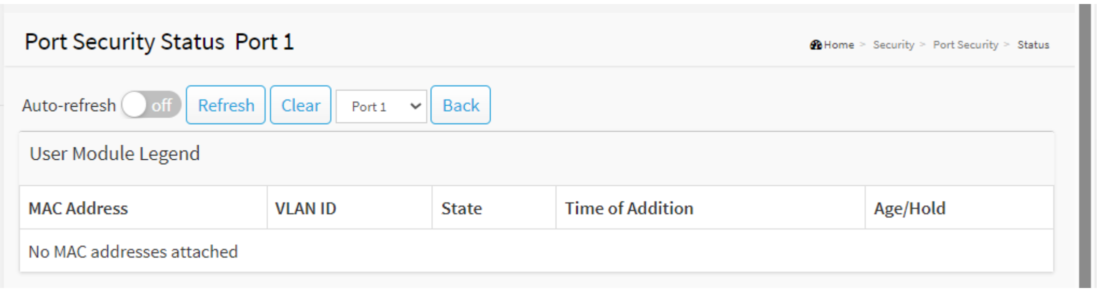
- ***Disabled***: Port Security is not administratively enabled on this port.
- ***Protect***: Port Security is administratively enabled in Protect mode.
- ***Restrict***: Port Security is administratively enabled in Restrict mode.
- ***Shutdown***: Port Security is administratively enabled in Shutdown mode.
- **State** : Shows the current state of the port. It can display one of four values:

- ***Disabled***: No user modules are currently using the Port Security service.
- ***Ready***: The Port Security service is in use by at least one user module, and is awaiting frames from unknown MAC addresses to arrive.
- ***Limit Reached***: The Port Security service is enabled by at least the Limit Control user module, and that module has indicated that the limit is reached and no more MAC addresses should be taken in.
- ***Shutdown***: The Port Security service is enabled by at least the Limit Control user module, and that module has indicated that the limit is exceeded. No MAC addresses can be learned on the port until it is administratively re-opened on the Limit Control configuration Webpage.

MAC Count (Current, Violating, Limit) : The three columns indicate the number of currently learned MAC addresses (forwarding as well as blocked), the number of violating MAC address (only counting in Restrict mode) and the maximum number of MAC addresses that can be learned on the port, respectively. If no user modules are enabled on the port, the Current column will show a dash (**-**). If Port Security is not administratively enabled on the port, the Violating and Limit columns will show a dash (**-**).

Port Security Status Port N

Click the port number to view the status for this port:



Port Security Status Port 1

User Module Legend

MAC Address	VLAN ID	State	Time of Addition	Age/Hold
No MAC addresses attached				

Parameter descriptions:

Port select box: At the dropdown select the port that you want to display the Port Security Status.

Back : Click to go back Port Security Status.

MAC Address & **VLAN ID** : The MAC address and VLAN ID that is seen on this port. If no MAC addresses are learned, a single row stating "No MAC addresses attached" is displayed.

State : Indicates whether the corresponding MAC address is blocked or forwarding. In the Blocked state, it will not be allowed to transmit or receive traffic.

Time of Addition : Shows the date and time when this MAC address was first seen on the port.

Age/Hold : If at least one user module has decided to block this MAC address, it will stay in the Blocked state until the hold time (measured in seconds) expires. If all user modules have decided to allow this MAC address to forward, and aging is enabled, the Port Security module will periodically check that this MAC address still forwards traffic. If the age period (measured in seconds) expires and no frames have been seen, the MAC address will be removed from the MAC table. Otherwise a new age period will begin.

If aging is disabled or a user module has decided to hold the MAC address indefinitely, a dash (-) will be shown.

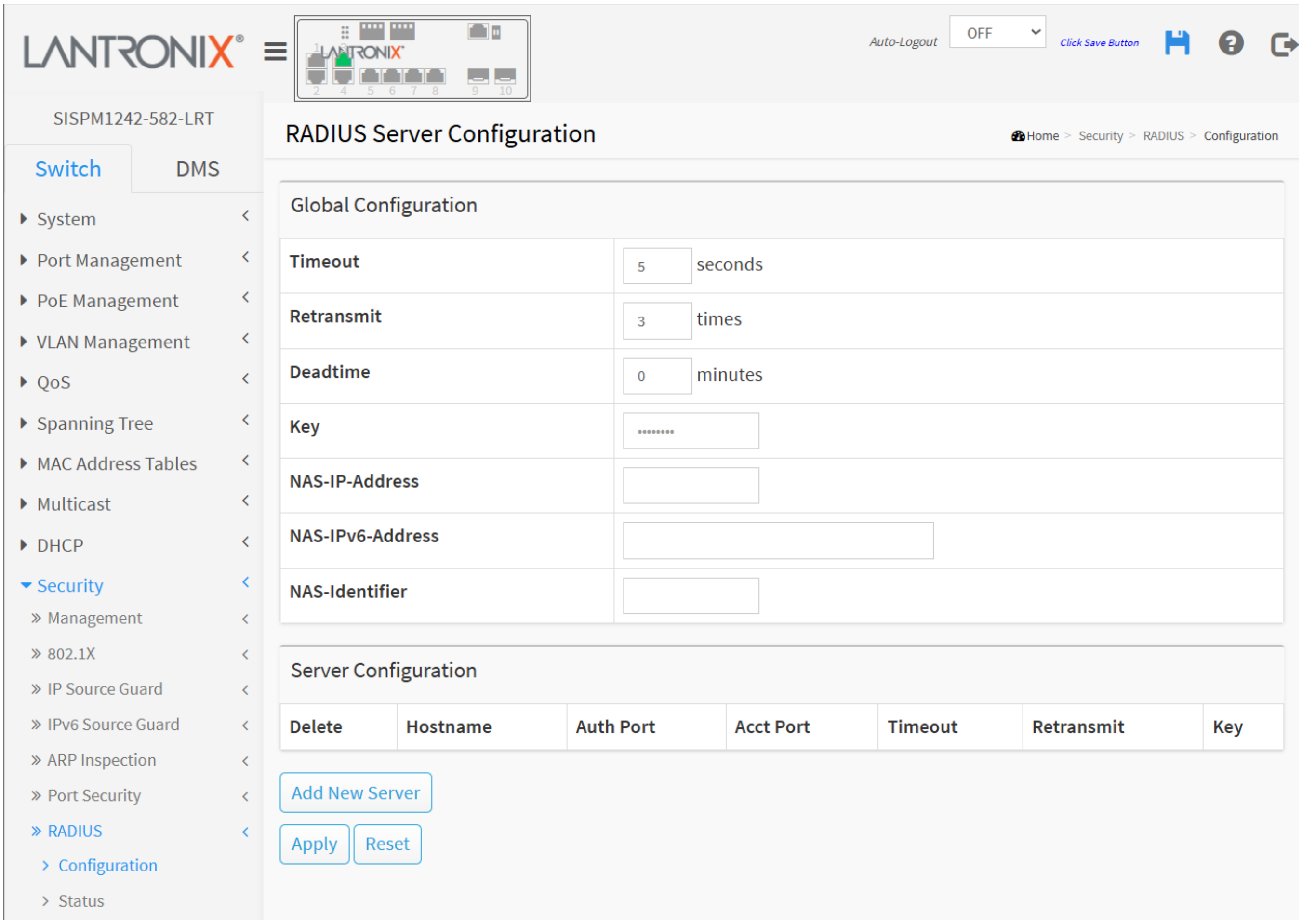
RADIUS

Configuration

This page lets you configure up to five RADIUS servers. RADIUS is a networking protocol that provides centralized access, authorization and accounting management for people or computers to connect and use a network service.

To configure a RADIUS server in the web UI:

1. Go to Security > RADIUS > Configuration.
2. Configure the global configuration settings.
3. Click **Add New Server**.
4. Configure the server settings.
5. Click the **Apply** button to save the settings.



RADIUS Server Configuration

Global Configuration

Timeout	5 seconds
Retransmit	3 times
Deadtime	0 minutes
Key	••••••••
NAS-IP-Address	
NAS-IPv6-Address	
NAS-Identifier	

Server Configuration

Delete	Hostname	Auth Port	Acct Port	Timeout	Retransmit	Key

Parameter descriptions:

Global Configuration : These setting are common for all of the RADIUS servers.

Timeout : The number of seconds, in the range 1 to 1000, to wait for a reply from a RADIUS server before retransmitting the request.

Retransmit : The number of times, in the range 1 to 1000, a RADIUS request is retransmitted to a server that is not responding. If the server has not responded after the last retransmit it is considered to be dead.

Deadtime : Deadtime, which can be set to 0 to 1440 minutes, is the period during which the switch will not send new requests to a server that has failed to respond to a previous request. This will stop the switch from continually trying to contact a server that it has already determined as dead. Setting the Deadtime to a value greater than 0 (zero) will enable this feature, but only if more than one server has been configured.

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

NAS-IP-Address : The IPv4 address to be used as Attribute 4 in RADIUS Access-Request packets. If this field is left blank, the IP address of the outgoing interface is used.

NAS-IPv6-Address : The IPv6 address to be used as Attribute 95 in RADIUS Access-Request packets. If this field is left blank, the IP address of the outgoing interface is used.

NAS-Identifier : The identifier - up to 255 characters long - to be used as Attribute 32 in RADIUS Access-Request packets. If this field is left blank, the NAS-Identifier is not included in the packet.

Server Configuration

Hostname : The IP address or hostname of the RADIUS server.

Auth Port : The UDP port to use on the RADIUS server for authentication.

Acct Port : The UDP port to use on the RADIUS server for accounting.

Timeout : This optional setting overrides the global timeout value. Leaving it blank will use the global timeout value.

Retransmit : This optional setting overrides the global retransmit value. Leaving it blank will use the global retransmit value.

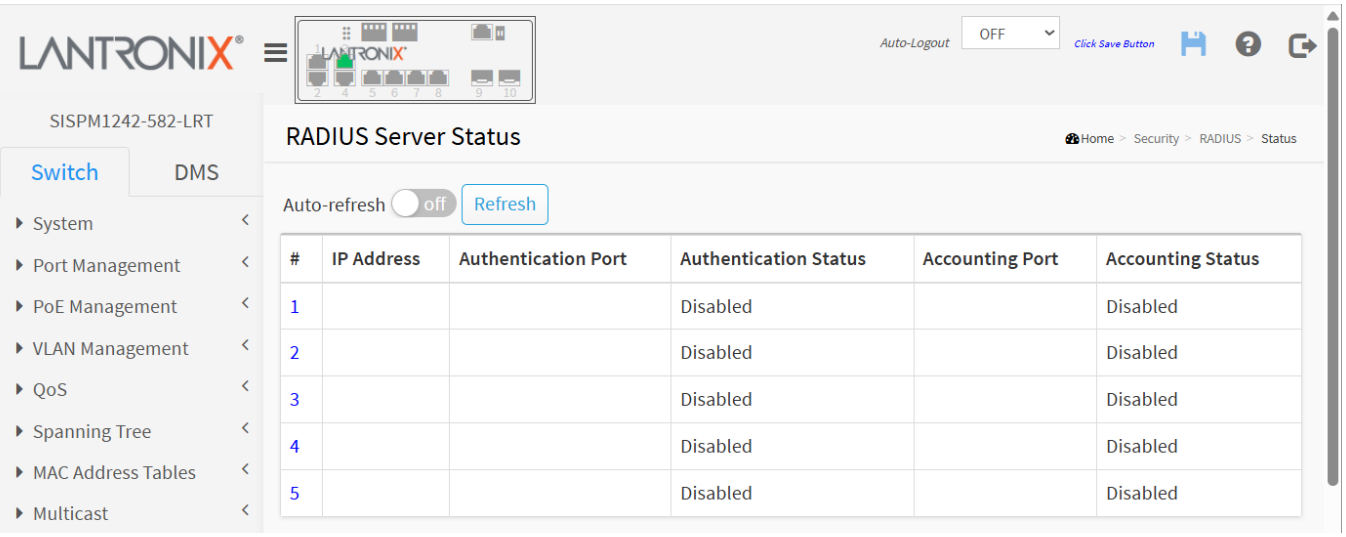
Key : This optional setting overrides the global key. Leaving it blank will use the global key.

Status

This page displays details of the RADIUS Authentication and Accounting servers’ status.

To display RADIUS Server Status in the web UI:

1. Go to Security > RADIUS > Status.
2. Select a server to display its RADIUS detailed statistics.
3. **Auto-refresh** will refresh the page every 3 seconds. **Refresh** will refresh the page immediately.



RADIUS Server Status

#	IP Address	Authentication Port	Authentication Status	Accounting Port	Accounting Status
1			Disabled		Disabled
2			Disabled		Disabled
3			Disabled		Disabled
4			Disabled		Disabled
5			Disabled		Disabled

Parameter descriptions:

: The RADIUS server number. Click to navigate to detailed statistics for this server.

IP Address : The IP address of this server.

Authentication Port : The UDP port number for authentication.

Authentication Status : The 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.

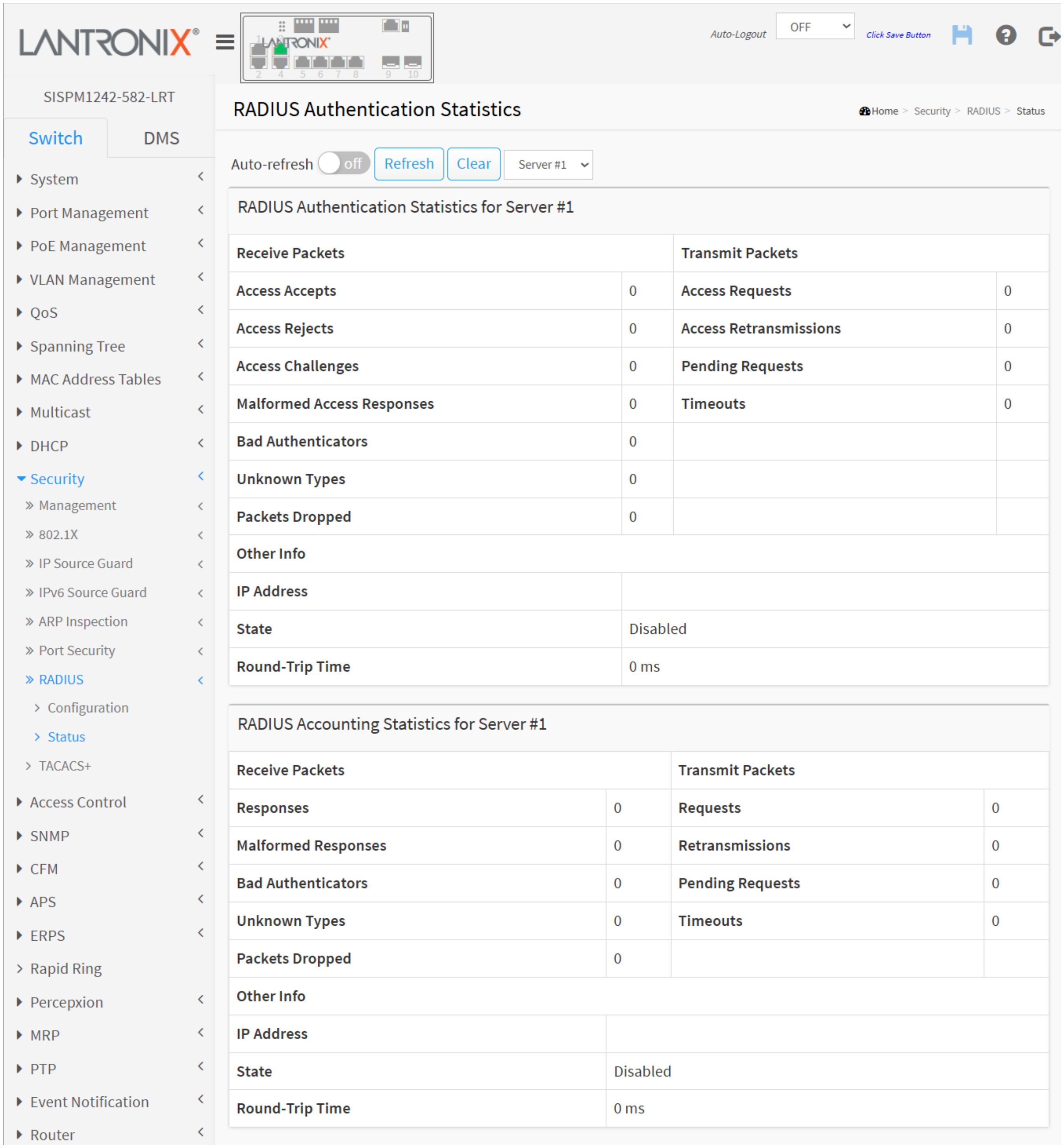
Accounting Port : The UDP port number for accounting.

Accounting Status : The status of the server. This field takes one of these values:

- ***Disabled***: The server is disabled.
- ***Not Ready***: The server is enabled, but IP communication is not yet up and running.
- ***Ready***: The server is enabled, IP communication is up and running, and the RADIUS module is ready to accept access attempts.
- ***Dead (X seconds left***): Access attempts were made to this server, but it did not reply within the configured timeout. The server has temporarily been disabled, but will get re-enabled when the dead-time expires. The number of seconds left before this occurs is displayed in parentheses. This state is only reachable when more than one server is enabled.

Radius Server Authentication Statistics for Server N

If you select Server#1 to display RADIUS Statistics:



RADIUS Authentication Statistics

RADIUS Authentication Statistics for Server #1

Receive Packets		Transmit Packets	
Access Accepts	0	Access Requests	0
Access Rejects	0	Access Retransmissions	0
Access Challenges	0	Pending Requests	0
Malformed Access Responses	0	Timeouts	0
Bad Authenticators	0		
Unknown Types	0		
Packets Dropped	0		
Other Info			
IP Address			
State	Disabled		
Round-Trip Time	0 ms		

RADIUS Accounting Statistics for Server #1

Receive Packets		Transmit Packets	
Responses	0	Requests	0
Malformed Responses	0	Retransmissions	0
Bad Authenticators	0	Pending Requests	0
Unknown Types	0	Timeouts	0
Packets Dropped	0		
Other Info			
IP Address			
State	Disabled		
Round-Trip Time	0 ms		

Parameter descriptions:

Server select box: Select which server that you want to display RADIUS. Use the server select box to switch between the backend servers to show details for.

RADIUS Authentication Statistics : The statistics map closely to those specified in RFC4668 - RADIUS Authentication Client MIB.

Access Accepts : The number of RADIUS Access-Accept packets (valid or invalid) received from the server.

Access Rejects : The number of RADIUS Access-Reject packets (valid or invalid) received from the server.

Access Challenges : The number of RADIUS Access-Challenge packets (valid or invalid) received from the server.

Malformed Access Responses : The number of malformed RADIUS Access-Response packets received from the server. Malformed packets include packets with an invalid length. Bad authenticators or Message Authenticator attributes or unknown types are not included as malformed access responses.

Bad Authenticators : The number of RADIUS Access-Response packets containing invalid authenticators or Message Authenticator attributes received from the server.

Unknown Types : The number of RADIUS packets that were received with unknown types from the server on the authentication port and dropped.

Packets Dropped : The number of RADIUS packets that were received from the server on the authentication port and dropped for some other reason.

Access Requests : The number of RADIUS Access-Request packets sent to the server. This does not include retransmissions.

Access Retransmissions : The number of RADIUS Access-Request packets retransmitted to the RADIUS authentication server.

Pending Requests : The number of RADIUS Access-Request packets destined for the server that have not yet timed out or received a response. This variable is incremented when an Access-Request is sent and decremented due to receipt of an Access-Accept, Access-Reject, Access-Challenge, timeout, or retransmission.

Timeouts : The number of authentication timeouts to the server. After a timeout, the client may retry to the same server, send to a different server, or give up. A retry to the same server is counted as a retransmit as well as a timeout. A send to a different server is counted as a Request as well as a timeout.

IP Address : IP address and UDP port for the authentication server in question.

State : Shows the state of the server. It takes one of these values:

- ***Disabled*** : The selected server is disabled.
- ***Not Ready*** : The server is enabled, but IP communication is not yet up and running.
- ***Ready*** : The server is enabled, IP communication is up and running, and the RADIUS module is ready to accept access attempts.
- ***Dead (X seconds left)*** : Access attempts were made to this server, but it did not reply within the configured timeout. The server has temporarily been disabled but will get re-enabled when the dead-time expires. The number of seconds left before this occurs is displayed in parentheses. This state is only reachable when more than one server is enabled.

Round-Trip Time : The time interval (measured in milliseconds) between the most recent Access-Reply/Access-Challenge and the Access-Request that matched it from the RADIUS authentication server. The granularity of this measurement is 100 ms. A value of 0 ms indicates that there hasn't been round-trip communication with the server yet.

RADIUS Accounting Statistics : The statistics map closely to those specified in RFC4670 - RADIUS Accounting Client MIB. Use the server select box to switch between the backend servers to show details for.

Responses : The number of RADIUS packets (valid or invalid) received from the server.

Malformed Responses : The number of malformed RADIUS packets received from the server. Malformed packets include packets with an invalid length. Bad authenticators or unknown types are not included as malformed access responses.

Bad Authenticators : The number of RADIUS packets containing invalid authenticators received from the server.

Unknown Types : The number of RADIUS packets of unknown types that were received from the server on the accounting port.

Packets Dropped : The number of RADIUS packets that were received from the server on the accounting port and dropped for some other reason.

Requests : The number of RADIUS packets sent to the server. This does not include retransmissions

Retransmissions : The number of RADIUS packets retransmitted to the RADIUS accounting server.

Pending Requests : The number of RADIUS packets destined for the server that have not yet timed out or received a response. This variable is incremented when a Request is sent and decremented due to receipt of a Response, timeout, or retransmission.

Timeouts : The number of accounting timeouts to the server. After a timeout, the client may retry to the same server, send to a different server, or give up. A retry to the same server is counted as a retransmit as well as a timeout. A send to a different server is counted as a Request as well as a Timeout.

IP Address : IP address and UDP port for the accounting server in question.

State : Shows the state of the server. It takes one of the following values:

- ***Disabled*** : The selected server is disabled.
- ***Not Ready*** : The server is enabled, but IP communication is not yet up and running.
- ***Ready*** : The server is enabled, IP communication is up and running, and the RADIUS module is ready to accept accounting attempts.
- ***Dead (X seconds left)*** : Accounting attempts were made to this server, but it did not reply within the configured timeout. The server has temporarily been disabled but will get re-enabled when the dead-time expires. The number of seconds left before this occurs is displayed in parentheses. This state is only reachable when more than one server is enabled.

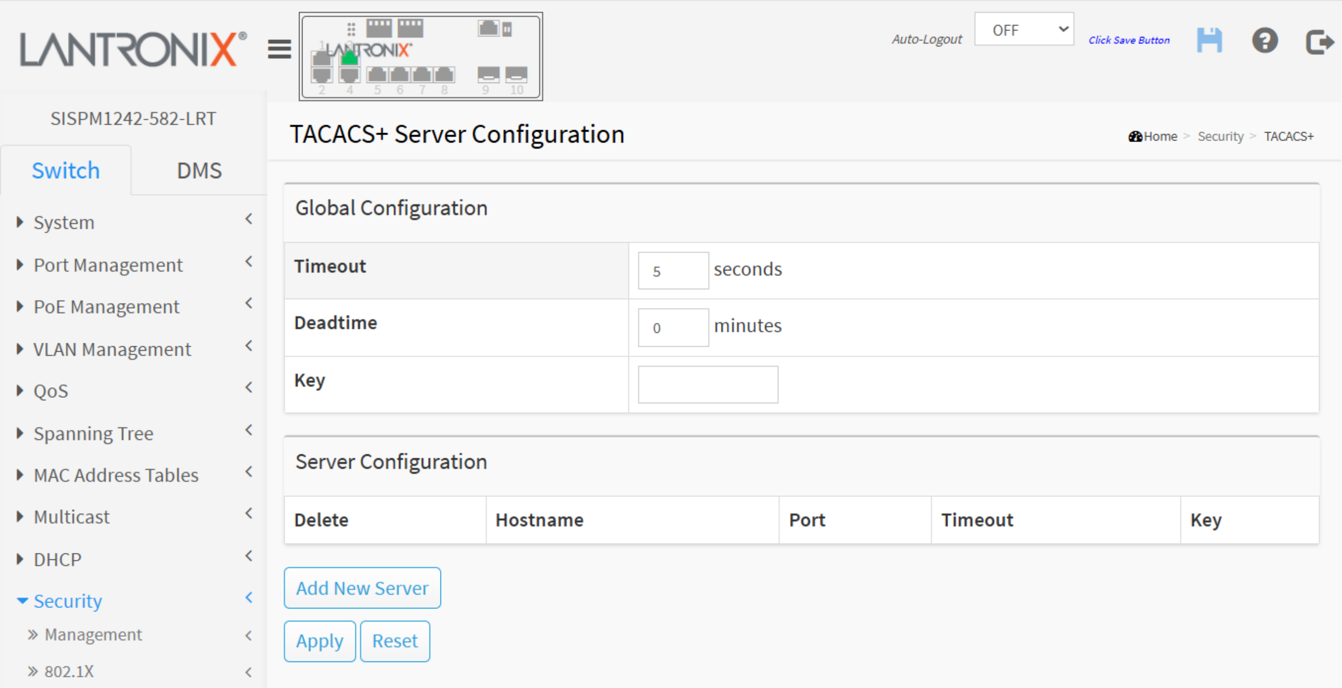
Round-Trip Time : The time interval (measured in milliseconds) between the most recent Response and the Request that matched it from the RADIUS accounting server. The granularity of this measurement is 100 ms. A value of 0 ms indicates that there hasn't been round-trip communication with the server yet.

TACACS+

This page lets you configure up to five TACACS+ servers. The TACACS+ protocol handles authentication, authorization, and accounting (AAA) services.

To configure TACACS+ servers in the web UI:

1. Go to Security > TACACS+.
2. Specify the global configuration settings.
3. Click **Add New Server**.
4. Specify the server settings.
5. Click **Apply**.



TACACS+ Server Configuration

Global Configuration

Timeout	5 seconds
Deadtime	0 minutes
Key	

Server Configuration

Delete	Hostname	Port	Timeout	Key

Parameter descriptions:

<u>**Global Configuration**</u> : These setting are common for all 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.

<u>**Server Configuration**</u>

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.

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.

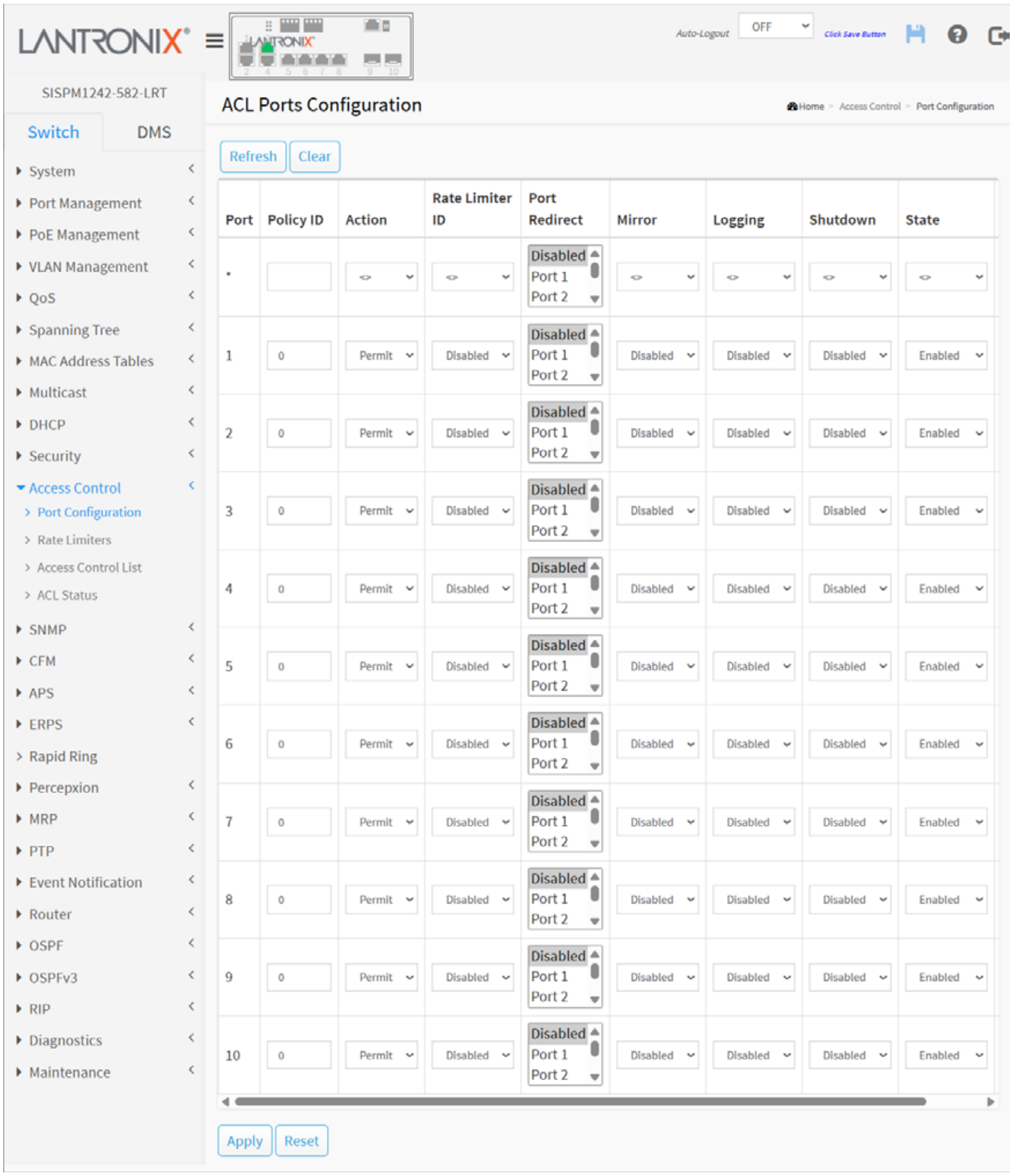
13. Access Control

Ports Configuration

Configure the ACL parameters (ACE) of each switch port. These parameters will affect frames received on a port unless the frame matches a specific ACE.

To configure ACL Ports in the web UI:

1. Go to Access Control > Port Configuration.
2. Specify port ACL settings.
3. Click **Apply** to save the settings.



ACL Ports Configuration

Port	Policy ID	Action	Rate Limiter ID	Port Redirect	Mirror	Logging	Shutdown	State
*		<>	<>	Disabled Port 1 Port 2	<>	<>	<>	<>
1	0	Permit	Disabled	Disabled Port 1 Port 2	Disabled	Disabled	Disabled	Enabled
2	0	Permit	Disabled	Disabled Port 1 Port 2	Disabled	Disabled	Disabled	Enabled
3	0	Permit	Disabled	Disabled Port 1 Port 2	Disabled	Disabled	Disabled	Enabled
4	0	Permit	Disabled	Disabled Port 1 Port 2	Disabled	Disabled	Disabled	Enabled
5	0	Permit	Disabled	Disabled Port 1 Port 2	Disabled	Disabled	Disabled	Enabled
6	0	Permit	Disabled	Disabled Port 1 Port 2	Disabled	Disabled	Disabled	Enabled
7	0	Permit	Disabled	Disabled Port 1 Port 2	Disabled	Disabled	Disabled	Enabled
8	0	Permit	Disabled	Disabled Port 1 Port 2	Disabled	Disabled	Disabled	Enabled
9	0	Permit	Disabled	Disabled Port 1 Port 2	Disabled	Disabled	Disabled	Enabled
10	0	Permit	Disabled	Disabled Port 1 Port 2	Disabled	Disabled	Disabled	Enabled

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 **0** through **127**. The default value is 0.

Action : Select whether forwarding is permitted ("Permit") or denied ("Deny"). The default value is "Permit".

Rate Limiter ID : Select which rate limiter to apply on this port. The allowed values are Disabled or the values 1 - 16. The default value is "Disabled".

Port Redirect : Select which port frames are redirected on. The allowed values are Disabled or a specific port number and it can't be set when action is permitted. The default value is "Disabled".

Mirror : Specify the mirror operation of this port. The allowed values are: Enabled: Frames received on the port are mirrored. Disabled: Frames received on the port are not mirrored. The default value is "Disabled".

Logging : Specify the logging operation of this port. 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. The default value is "Disabled".

Note that the System Log memory size and logging rate is limited.

Shutdown : Specify the port shut down operation of this port. The allowed values are:

- ***Enabled***: If a frame is received on the port, the port will be disabled.
- ***Disabled***: Port shut down is disabled. The default value is "Disabled".

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

State : Specify the port state of this port. The allowed values are:

- ***Enabled***: To reopen ports by changing the volatile port configuration of the ACL user module. The default value is "Enabled".
- ***Disabled***: To close ports by changing the volatile port configuration of the ACL user module.

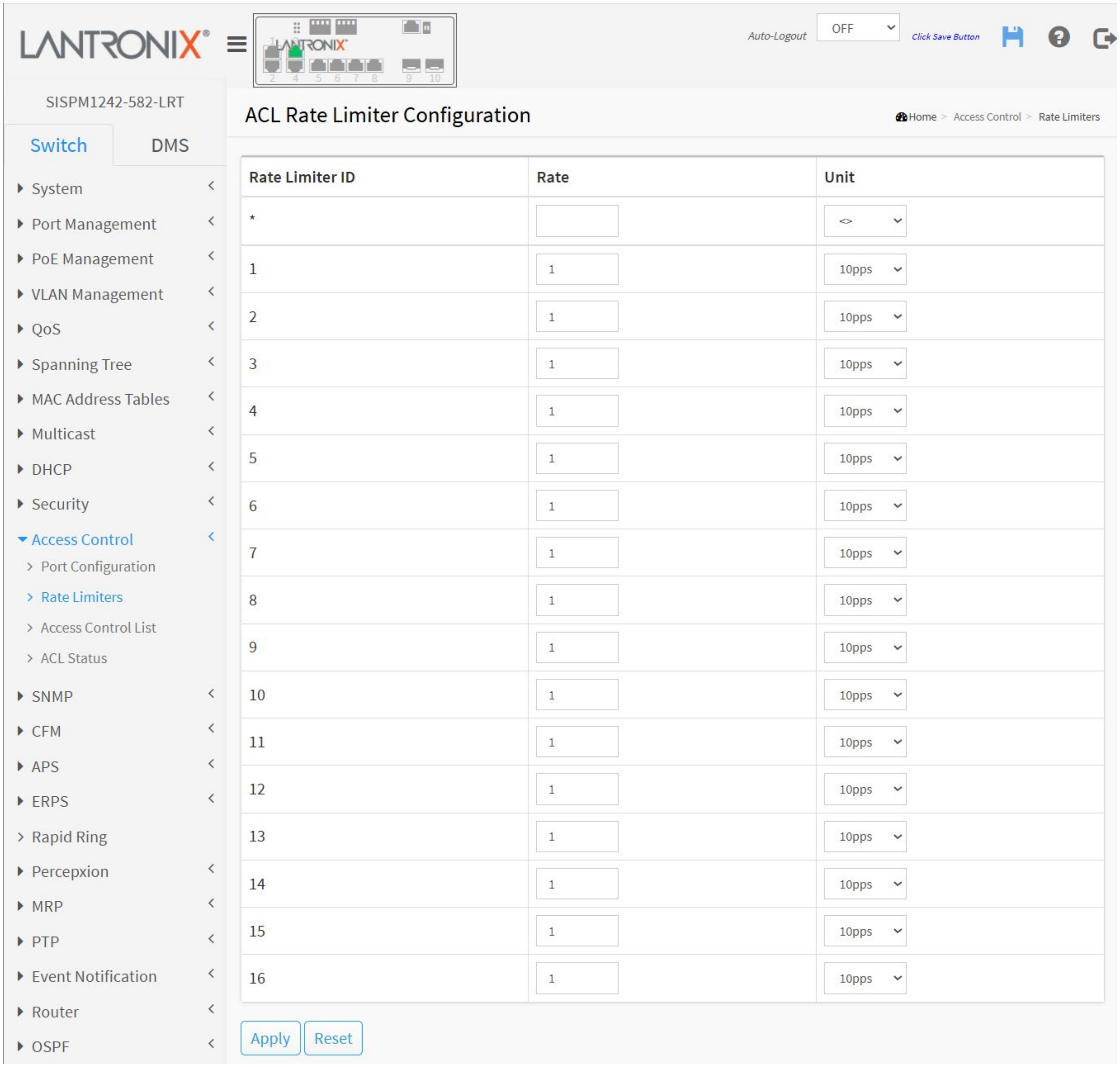
Counter : Counts the number of frames that match this ACE.

Rate Limiters

This page lets you configure the switch's ACL Rate Limiter parameters.

To configure ACL Rate Limiters in the web UI:

1. Go to Access Control > Rate Limiters.
2. Specific the Rate and Unit.
3. Click **Apply** to save the settings.



ACL Rate Limiter Configuration

Rate Limiter ID	Rate	Unit
*		<>
1	1	10pps
2	1	10pps
3	1	10pps
4	1	10pps
5	1	10pps
6	1	10pps
7	1	10pps
8	1	10pps
9	1	10pps
10	1	10pps
11	1	10pps
12	1	10pps
13	1	10pps
14	1	10pps
15	1	10pps
16	1	10pps

Parameter descriptions:

Rate Limiter ID : The rate limiter ID for the settings contained in the same row; its range is 1 to 16.

Rate : The valid rate is 0, 10, 20, 30, ..., 5000000 in pps or 0, 25, 50, 75, ..., 10000000 in kbps.

Unit : Specify the rate unit of measure. Valid values are 10pps: packets per second or 25kbps: Kbits per second.

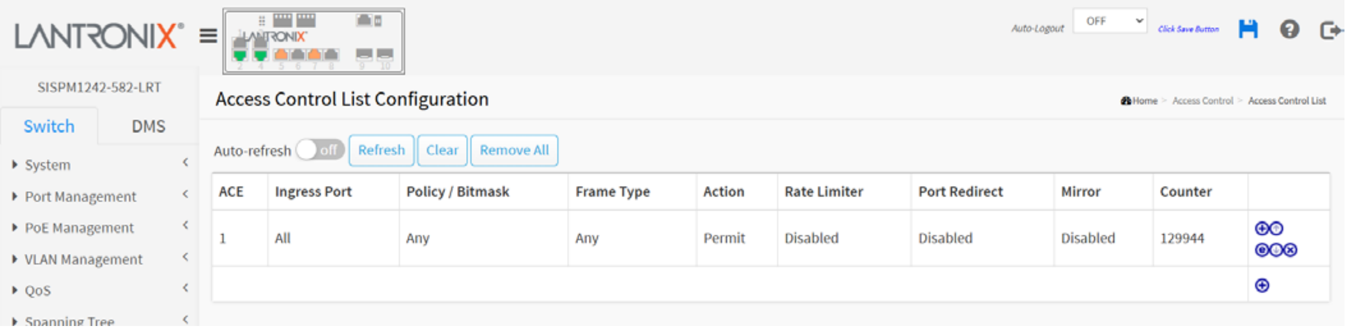
Access Control List

This page shows the Access Control List (ACL), which is made up of the ACEs defined on this switch. Each row describes an ACE that is defined. The maximum number of ACEs is 512 on each switch.

Click on the lowest plus sign to add a new ACE to the list. Reserved ACEs are used for internal protocol and cannot be edited or deleted; the order sequence cannot be changed, and the priority is highest.

To configure Access Control List in the web UI:

1. Go to Access Control > Access Control List.



Access Control List Configuration

ACE	Ingress Port	Policy / Bitmask	Frame Type	Action	Rate Limiter	Port Redirect	Mirror	Counter	
1	All	Any	Any	Permit	Disabled	Disabled	Disabled	129944	⊕ⓘ ⊕⊕⊗
									⊕

2. Click the ⊕ button to add a new ACL. The ACE Configuration page is displayed.
3. Configure the ACE Configuration parameters.
   Note: When editing an entry on the ACE Configuration page, the items displayed vary according to the frame type and IP protocol type selected.
4. Click the **Apply** button to save the settings

Page controls:

Refresh: Click to refresh the page

Clear : Click to clear the data manually.

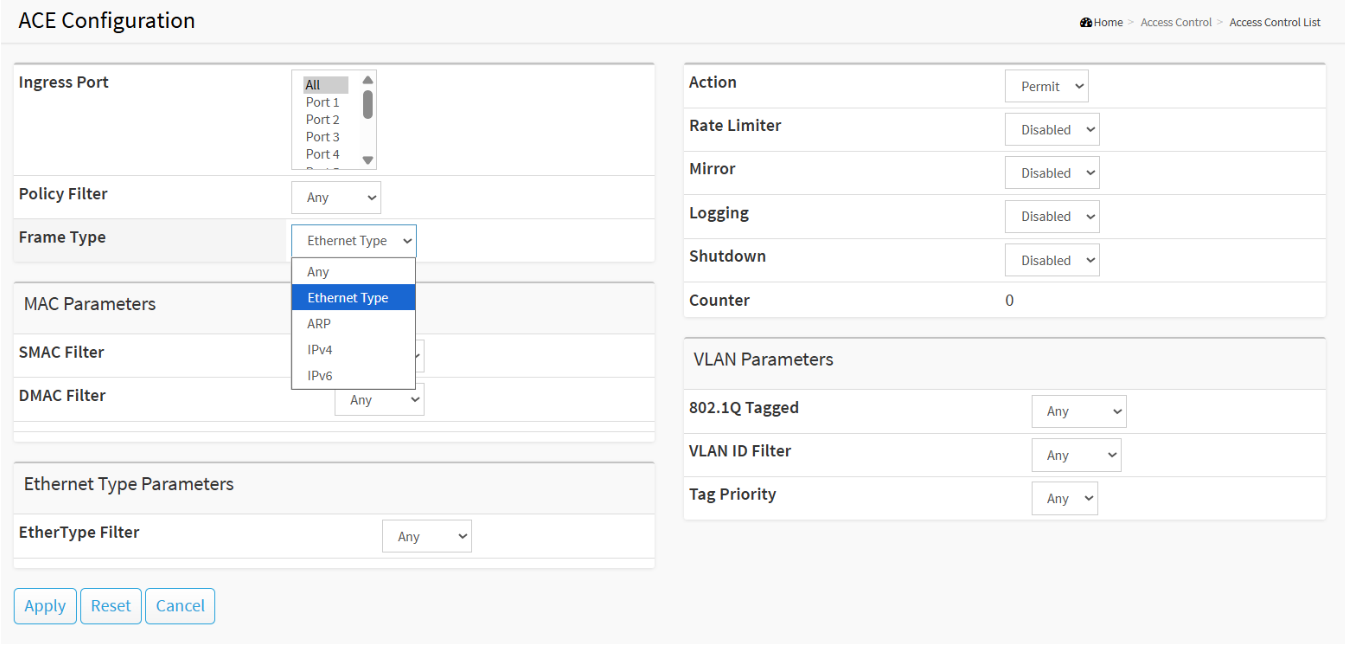
Remove All : Click to remove all ACL instances from the table.

ACE Configuration Page

This page contains ACE configuration settings.

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.



ACE Configuration

Ingress Port	All
Policy Filter	Any
Frame Type	Ethernet Type

MAC Parameters

SMAC Filter	
DMAC Filter	Any

Ethernet Type Parameters

EtherType Filter	Any

Action	Permit
Rate Limiter	Disabled
Mirror	Disabled
Logging	Disabled
Shutdown	Disabled
Counter	0

VLAN Parameters

802.1Q Tagged	Any
VLAN ID Filter	Any
Tag Priority	Any

Parameter descriptions:

Ingress Port : Indicates the ingress port of the ACE. Possible values are:

- ***All***: The ACE applies to all ports.
- ***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 **127**.

Policy Bitmask: When "Specific" is selected for the policy filter, you can enter a specific policy bitmask. The allowed range is 0x0 to 0x7f. 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 : Indicates the frame type of the ACE. Possible values are:

- ***Any***: The ACE will match any frame type.
- ***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) and the value should not be equal to 0x800(IPv4), 0x806(ARP) or 0x86DD(IPv6).
- ***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 : 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.

Filter Port: This field displays when **Filter** is selected as the **Action** type. Select the filter port for action.

- ***All*****:** The action applies to all port.
- ***Port n*****:** The action applies to this port number, where *n* is the number of the switch port.

Rate Limiter : Indicates the rate limiter number of the ACE. The valid range is 1 to 16. When Disabled is displayed, the rate limiter operation is disabled.

Port Redirect : Indicates the port redirect operation of the ACE. Frames matching the ACE are redirected to the port number. The allowed values are Disabled or a specific port number. When Disabled is displayed, the port redirect operation is disabled.

Mirror : Specify the mirror operation of this port. Frames matching the ACE are mirrored to the destination mirror port. The allowed values are:

- ***Enabled***: Frames received on the port are mirrored.
- ***Disabled***: Frames received on the port are not mirrored. The default value is "Disabled".

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 appears.

SMAC Value : When "Specific" is selected for the SMAC filter, you can enter a specific source MAC address.
The legal format is "xx-xx-xx-xx-xx-xx" or "xx.xx.xx.xx.xx.xx" or "xxxxxxxxxxxx" (x is a hexadecimal digit).
A frame that hits this ACE matches this SMAC value.

DMAC Filter : Specify the destination MAC filter for this ACE.

- ***Any***: No DMAC filter is specified. (DMAC filter status is "don't-care".)
- ***MC***: Frame must be multicast.
- ***BC***: Frame must be broadcast.
- ***UC***: Frame must be unicast.
- ***Specific***: If you want to filter a specific destination MAC address with this ACE, choose this value. A field for entering a DMAC value appears.

DMAC Value : When "Specific" is selected for the DMAC filter, you can enter a specific destination MAC address. The legal format is "xx-xx-xx-xx-xx-xx" or "xx.xx.xx.xx.xx.xx" or "xxxxxxxxxxxx" (x is a hexadecimal digit). A frame that hits this ACE matches this DMAC value.

VLAN Parameters

802.1Q Tagged : Specify whether frames can hit the action according to the 802.1Q tagged. Valid values are:

- ***Any***: Any value is allowed ("don't-care"). The default value is "Any".
- ***Enabled***: Tagged frame only.
- ***Disabled***: Untagged frame only.

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

- **Any***:* No VLAN ID filter is specified. (VLAN ID filter status is "don't-care".)
- ***Specific***: If you want to filter a specific VLAN ID with this ACE, choose this value. A field for entering a VLAN ID number appears.

VLAN ID : When "Specific" is selected for the VLAN ID filter, you can enter a specific VLAN ID number. The valid range is 1 to 4095. A frame that hits this ACE matches this VLAN ID value.

Tag Priority : Specify the tag priority for this ACE. A frame that hits this ACE matches this tag priority. The allowed number range is 0 to 7 or range 0-1, 2-3, 4-5, 6-7, 0-3 and 4-7. The value 'Any' means that no tag priority is specified (tag priority is "don't-care".)

ARP Parameters :

The ARP parameters can be configured when Frame Type "ARP" is selected.

ARP/RARP : Specify the available ARP/RARP opcode (OP) flag for this ACE:

- ***Any***: No ARP/RARP OP flag is specified. (OP is "don't-care".)
- ***ARP***: Frame must have ARP opcode set to ARP.
- ***RARP***: Frame must have RARP opcode set to RARP.
- ***Other***: Frame has unknown ARP/RARP Opcode flag.

Request/Reply : Specify the available Request/Reply opcode (OP) flag for this ACE.

- ***Any***: No Request/Reply OP flag is specified. (OP is "don't-care".)
- ***Request***: Frame must have ARP Request or RARP Request OP flag set.
- ***Reply***: Frame must have ARP Reply or RARP Reply OP flag.

Sender IP Filter : Specify the sender IP filter for this ACE.

- ***Any***: No sender IP filter is specified. (Sender IP filter is "don't-care".)
- ***Host***: Sender IP filter is set to Host. Specify the sender IP address in the SIP Address field that appears.

- ***Network***: Sender IP filter is set to Network. Specify the sender IP address and sender IP mask in the SIP Address and SIP Mask fields that appear.

Sender IP Address : When "Host" or "Network" is selected for the sender IP filter, you can enter a specific sender IP address in dotted decimal notation.

Sender IP Mask : When "Network" is selected for the sender IP filter, you can enter a specific sender IP mask in dotted decimal notation.

Target IP Filter : Specify the target IP filter for this specific ACE.

- ***Any***: No target IP filter is specified. (Target IP filter is "don't-care".)
- ***Host***: Target IP filter is set to Host. Specify the target IP address in the Target IP Address field that appears.
- ***Network***: Target IP filter is set to Network. Specify the target IP address and target IP mask in the Target IP Address and Target IP Mask fields that appear.

Target IP Address : When "Host" or "Network" is selected for the target IP filter, you can enter a specific target IP address in dotted decimal notation.

Target IP Mask : When "Network" is selected for the target IP filter, you can enter a specific target IP mask in dotted decimal notation.

ARP Sender MAC Match : Specify whether frames can hit the action according to their sender hardware address field (SHA) settings.

- ***0***: ARP frames where SHA is not equal to the SMAC address.
- ***1***: ARP frames where SHA is equal to the SMAC address.
- ***Any***: Any value is allowed ("don't-care").

RARP Target MAC Match : Specify whether frames can hit the action according to their target hardware address field (THA) settings.

- ***0***: RARP frames where THA is not equal to the target MAC address.
- ***1***: RARP frames where THA is equal to the target MAC address.
- ***Any***: Any value is allowed ("don't-care").

IP/Ethernet Length : Specify whether frames can hit the action according to their ARP/RARP hardware address length (HLN) and protocol address length (PLN) settings.

- ***0***: ARP/RARP frames where the HLN is not equal to Ethernet (0x06) or the (PLN) is not equal to IPv4 (0x04).
- ***1***: ARP/RARP frames where the HLN is equal to Ethernet (0x06) and the (PLN) is equal to IPv4 (0x04).
- ***Any***: Any value is allowed ("don't-care").

Ethernet : Specify whether frames can hit the action according to their ARP/RARP hardware address space (HRD) settings.

- ***0***: ARP/RARP frames where the HLD is not equal to Ethernet (1).
- ***1***: ARP/RARP frames where the HLD is equal to Ethernet (1).
- ***Any***: Any value is allowed ("don't-care").

IP : Specify whether frames can hit the action according to their ARP/RARP protocol address space (PRO) settings.

- ***0***: ARP/RARP frames where the PRO is not equal to IP (0x800).
- ***1***: ARP/RARP frames where the PRO is equal to IP (0x800).
- ***Any***: Any value is allowed ("don't-care").

IP Parameters :

The IP parameters can be configured when Frame Type "IPv4" is selected.

IP Protocol Filter : Specify the IP protocol filter for this ACE.

- ***Any***: No IP protocol filter is specified ("don't-care").
- ***Specific***: If you want to filter a specific IP protocol filter with this ACE, choose this value. A field for entering an IP protocol filter appears.

ICMP: Select ICMP to filter IPv4 ICMP protocol frames. Extra fields for defining ICMP parameters will appear. These fields are explained later in this manual.

UDP: Select UDP to filter IPv4 UDP protocol frames. Extra fields for defining UDP parameters will appear. These fields are explained later in this manual.

TCP: Select TCP to filter IPv4 TCP protocol frames. Extra fields for defining TCP parameters will appear. These fields are explained later in this manual.

IP Protocol Value : When "Specific" is selected for the IP protocol value, you can enter a specific value. The valid range is 0 to 255. A frame that hits this ACE matches this IP protocol value.

IP TTL : Specify the Time-to-Live settings for this ACE.

- ***zero***: IPv4 frames with a Time-to-Live field greater than zero must not be able to match this entry.
- ***non-zero***: IPv4 frames with a Time-to-Live field greater than zero must be able to match this entry.
- ***Any***: Any value is allowed ("don't-care").

IP Fragment : Specify the fragment offset settings for this ACE. This involves the settings for the More Fragments (MF) bit and the Fragment Offset (FRAG OFFSET) field for an IPv4 frame.

- ***No***: IPv4 frames where the MF bit is set or the FRAG OFFSET field is greater than zero must not be able to match this entry.
- ***Yes***: IPv4 frames where the MF bit is set or the FRAG OFFSET field is greater than zero must be able to match this entry.
- ***Any***: Any value is allowed ("don't-care").

IP Option : Specify the options flag setting for this ACE.

- ***No***: IPv4 frames where the options flag is set must not be able to match this entry.
- ***Yes***: IPv4 frames where the options flag is set must be able to match this entry.
- ***Any***: Any value is allowed ("don't-care").

SIP Filter : Specify the source IP filter for this ACE.

- ***Any***: No source IP filter is specified. (Source IP filter is "don't-care".)
- ***Host***: Source IP filter is set to Host. Specify the source IP address in the SIP Address field that appears.
- ***Network***: Source IP filter is set to Network. Specify the source IP address and source IP mask in the SIP Address and SIP Mask fields that appear.

SIP Address : When "Host" or "Network" is selected for the source IP filter, you can enter a specific SIP address in dotted decimal notation.

SIP Mask : When "Network" is selected for the source IP filter, you can enter a specific SIP mask in dotted decimal notation.

DIP Filter : Specify the destination IP filter for this ACE.

- ***Any***: No destination IP filter is specified. (Destination IP filter is "don't-care".)
- ***Host***: Destination IP filter is set to Host. Specify the destination IP address in the DIP Address field that appears.
- ***Network***: Destination IP filter is set to Network. Specify the destination IP address and destination IP mask in the DIP Address and DIP Mask fields that appear.

DIP Address : When "Host" or "Network" is selected for the destination IP filter, you can enter a specific DIP address in dotted decimal notation.

DIP Mask : When "Network" is selected for the destination IP filter, you can enter a specific DIP mask in dotted decimal notation.

IPv6 Parameters :

The IPv6 parameters can be configured when Frame Type "IPv6" is selected.

Next Header Filter : Specify the IPv6 next header filter for this ACE.

- ***Any***: No IPv6 next header filter is specified ("don't-care").
- ***Specific***: If you want to filter a specific IPv6 next header filter with this ACE, choose this value. A field for entering an IPv6 next header filter appears.
- ***ICMP***: Select ICMP to filter IPv6 ICMP protocol frames. Extra fields for defining ICMP parameters will appear. These fields are explained later in this manual.
- ***UDP***: Select UDP to filter IPv6 UDP protocol frames. Extra fields for defining UDP parameters will appear. These fields are explained later in this manual.
- ***TCP***: Select TCP to filter IPv6 TCP protocol frames. Extra fields for defining TCP parameters will appear. These fields are explained later in this document

Next Header Value : When "Specific" is selected for the IPv6 next header value, you can enter a specific value. The valid range is 0 to 255. A frame that hits this ACE matches this IPv6 protocol value.

SIP Filter : Specify the source IPv6 filter for this ACE.

- ***Any***: No source IPv6 filter is specified. (Source IPv6 filter is "don't-care".)
- ***Specific***: Source IPv6 filter is set to Network. Specify the source IPv6 address and source IPv6 mask in the SIP Address fields that appear.

SIP Address : When "Specific" is selected for the source IPv6 filter, you can enter a specific SIPv6 address. The field only supported last 32 bits for IPv6 address.

SIP BitMask : When "Specific" is selected for the source IPv6 filter, you can enter a specific SIPv6 mask. The field only supported last 32 bits for IPv6 address. Notice the usage of bitmask, if the binary bit value is "0", it means this bit is "don't-care". The real matched pattern is [sipv6_address & sipv6_bitmask] (last 32 bits). For example, if the SIPv6 address is 2001::3 and the SIPv6 bitmask is 0xFFFFFFFE(bit 0 is "don't-care" bit), then SIPv6 address 2001::2 and 2001::3 are applied to this rule.

Hop Limit : Specify the hop limit settings for this ACE.

- ***zero***: IPv6 frames with a hop limit field greater than zero must not be able to match this entry.
- ***non-zero***: IPv6 frames with a hop limit field greater than zero must be able to match this entry.
- ***Any***: Any value is allowed ("don't-care").

ICMP Parameters

ICMP Type Filter : Specify the ICMP filter for this ACE.

- ***Any***: No ICMP filter is specified (ICMP filter status is "don't-care").
- ***Specific***: If you want to filter a specific ICMP filter with this ACE, you can enter a specific ICMP value. A field for entering an ICMP value appears.

ICMP Type Value : When "Specific" is selected for the ICMP filter, you can enter a specific ICMP value. The valid range is 0 to 255. A frame that hits this ACE matches this ICMP value.

ICMP Code Filter : Specify the ICMP code filter for this ACE.

- ***Any***: No ICMP code filter is specified (ICMP code filter status is "don't-care").
- ***Specific***: If you want to filter a specific ICMP code filter with this ACE, you can enter a specific ICMP code value. A field for entering an ICMP code value appears.

ICMP Code Value : When "Specific" is selected for the ICMP code filter, you can enter a specific ICMP code value. The valid range is 0 to 255. A frame that hits this ACE matches this ICMP code value.

TCP/UDP Parameters

TCP/UDP Source Filter : Specify the TCP/UDP source filter for this ACE.

- ***Any***: No TCP/UDP source filter is specified (TCP/UDP source filter status is "don't-care").
- ***Specific***: If you want to filter a specific TCP/UDP source filter with this ACE, you can enter a specific TCP/UDP source value. A field for entering a TCP/UDP source value appears.
- ***Range***: If you want to filter a specific TCP/UDP source range filter with this ACE, you can enter a specific TCP/UDP source range value. A field for entering a TCP/UDP source value appears.

TCP/UDP Source No. : When "Specific" is selected for the TCP/UDP source filter, you can enter a specific TCP/UDP source value. The valid range is 0 to 65535. A frame that hits this ACE matches this TCP/UDP source value.

TCP/UDP Source Range : When "Range" is selected for the TCP/UDP source filter, you can enter a specific TCP/UDP source range value. The valid range is 0 to 65535. A frame that hits this ACE matches this TCP/UDP source value.

TCP/UDP Destination Filter : Specify the TCP/UDP destination filter for this ACE.

- ***Any***: No TCP/UDP destination filter is specified (TCP/UDP destination filter status is "don't-care").
- ***Specific***: If you want to filter a specific TCP/UDP destination filter with this ACE, you can enter a specific TCP/UDP destination value. A field for entering a TCP/UDP destination value appears.
- ***Range***: If you want to filter a specific range TCP/UDP destination filter with this ACE, you can enter a specific TCP/UDP destination range value. A field for entering a TCP/UDP destination value appears.

TCP/UDP Destination Number : When "Specific" is selected for the TCP/UDP destination filter, you can enter a specific TCP/UDP destination value. The valid range is 0 to 65535. A frame that hits this ACE matches this TCP/UDP destination value.

TCP/UDP Destination Range : When "Range" is selected for the TCP/UDP destination filter, you can enter a specific TCP/UDP destination range value. The valid range is 0 to 65535. A frame that hits this ACE matches this TCP/UDP destination value.

TCP FIN : Specify the TCP "No more data from sender" (FIN) value for this ACE.

- ***0***: TCP frames where the FIN field is set must not be able to match this entry.
- ***1***: TCP frames where the FIN field is set must be able to match this entry.
- ***Any***: Any value is allowed ("don't-care").

TCP SYN : Specify the TCP "Synchronize sequence numbers" (SYN) value for this ACE.

- ***0***: TCP frames where the SYN field is set must not be able to match this entry.
- ***1***: TCP frames where the SYN field is set must be able to match this entry.
- ***Any***: Any value is allowed ("don't-care").

TCP RST : Specify the TCP "Reset the connection" (RST) value for this ACE.

- ***0***: TCP frames where the RST field is set must not be able to match this entry.
- ***1***: TCP frames where the RST field is set must be able to match this entry.
- ***Any***: Any value is allowed ("don't-care").

TCP PSH : Specify the TCP "Push Function" (PSH) value for this ACE.

- ***0***: TCP frames where the PSH field is set must not be able to match this entry.
- ***1***: TCP frames where the PSH field is set must be able to match this entry.
- ***Any***: Any value is allowed ("don't-care").

TCP ACK : Specify the TCP "Acknowledgment field significant" (ACK) value for this ACE.

- ***0***: TCP frames where the ACK field is set must not be able to match this entry.
- ***1***: TCP frames where the ACK field is set must be able to match this entry.
- ***Any***: Any value is allowed ("don't-care").

TCP URG : Specify the TCP "Urgent Pointer field significant" (URG) value for this ACE.

- ***0***: TCP frames where the URG field is set must not be able to match this entry.
- ***1***: TCP frames where the URG field is set must be able to match this entry.
- ***Any***: Any value is allowed ("don't-care").

Ethernet Type Parameters :

The Ethernet Type parameters can be configured when Frame Type "Ethernet Type" is selected.

EtherType Filter : Specify the Ethernet type filter for this ACE.

- ***Any***: No EtherType filter is specified (EtherType filter status is "don't-care").
- ***Specific***: If you want to filter a specific EtherType filter with this ACE, you can enter a specific EtherType value. A field for entering a EtherType value appears.

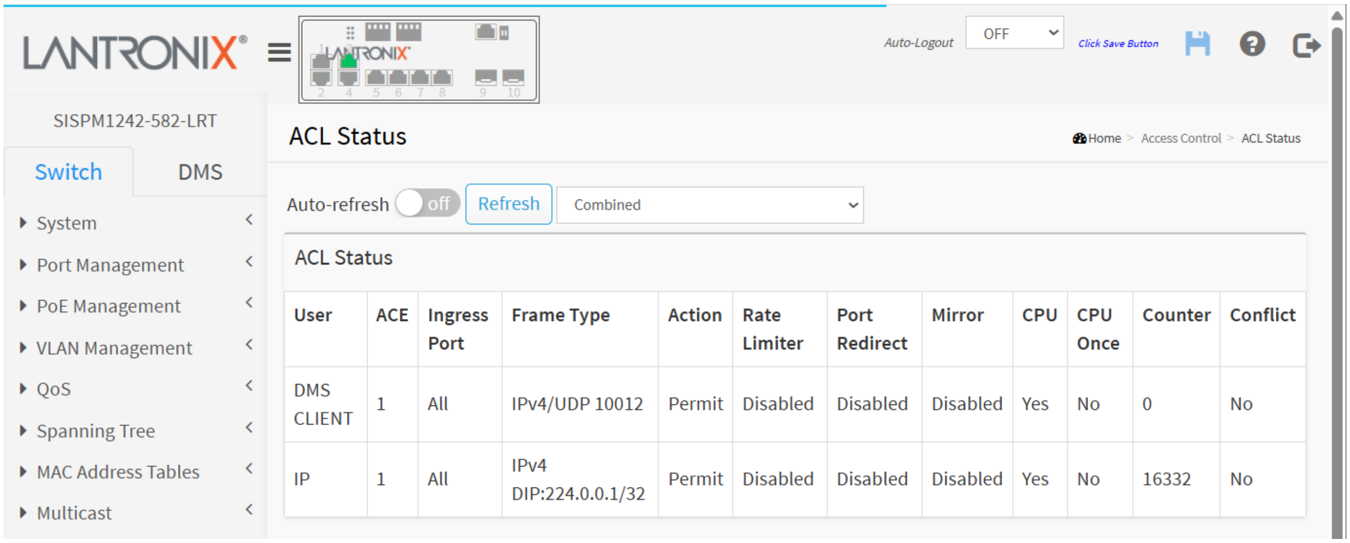
Ethernet Type Value : When "Specific" is selected for the EtherType filter, you can enter a specific EtherType value. The valid range is 0x600 to 0xFFFF but excluding 0x800(IPv4), 0x806(ARP) and 0x86DD(IPv6). A frame that hits this ACE matches this EtherType value.

ACL Status

This page shows ACL status by different ACL users. Each row describes the ACE that is defined. It is a ‘Conflict’ if a specific ACE is not applied to the hardware due to hardware limitations. The maximum number of ACEs is 512 on each switch.

To display ACL status in the web UI:

1. Go to Access Control > ACL Status.
2. At the User select dropdown select the set of user’s information to be displayed. The default is “Combined”.
3. **Auto-refresh** will refresh the page every 3 seconds. **Refresh** will refresh the page immediately.



ACL Status

ACL Status

User	ACE	Ingress Port	Frame Type	Action	Rate Limiter	Port Redirect	Mirror	CPU	CPU Once	Counter	Conflict
DMS CLIENT	1	All	IPv4/UDP 10012	Permit	Disabled	Disabled	Disabled	Yes	No	0	No
IP	1	All	IPv4 DIP:224.0.0.1/32	Permit	Disabled	Disabled	Disabled	Yes	No	16332	No

Parameter descriptions:

User select box : At the dropdown select the set of user’s information to be displayed. The default is the set of “Combined” users.

User : Indicates the ACL user (e.g., IP, DMS CLIENT, Combined, static, etc.).

ACE : Indicates the ACE ID on the local switch.

Ingress Port : Indicates the ingress port of the ACE. Possible values are:

- ***All***: The ACE will match all ingress port.
- ***Port***: The ACE will match a specific ingress port.

Frame Type : Indicates the frame type of the ACE. Possible values are:

- ***Any***: The ACE will match any frame type.
- ***EType***: The ACE will match Ethernet Type frames. Note that an Ethernet Type based ACE will not get matched by IP and ARP frames.
- ***ARP***: The ACE will match ARP/RARP frames.
- ***IPv4***: The ACE will match all IPv4 frames.
- ***IPv4***: The ACE will match all IPv4 frames.
- ***IPv4/ICMP***: The ACE will match IPv4 frames with ICMP protocol.
- ***IPv4/UDP***: The ACE will match IPv4 frames with UDP protocol.
- ***IPv4/TCP***: The ACE will match IPv4 frames with TCP protocol.

- ***IPv4 DIP*** : The ACE will match IPv4 frames with Data Interface Pairs.
- ***IPv4/Other***: The ACE will match IPv4 frames which are not ICMP / UDP / TCP.
- ***IPv6***: The ACE will match all IPv6 standard frames.

Action : Indicates the forwarding action of the ACE.

- ***Permit***: Frames matching the ACE may be forwarded and learned.
- ***Deny***: Frames matching the ACE are dropped.
- ***Filter***: Frames matching the ACE are filtered.

Rate Limiter : Indicates the rate limiter number of the ACE. The valid range is 1 to 16. When Disabled is displayed, the rate limiter operation is disabled.

Port Redirect : Indicates the port redirect operation of the ACE. Frames matching the ACE are redirected to the port number. The allowed values are Disabled or a specific port number. When Disabled is displayed, the port redirect operation is disabled.

Mirror : Specify the mirror operation of this port. The allowed values are:

- ***Enabled***: Frames received on the port are mirrored.
- ***Disabled***: Frames received on the port are not mirrored. The default value is "Disabled".

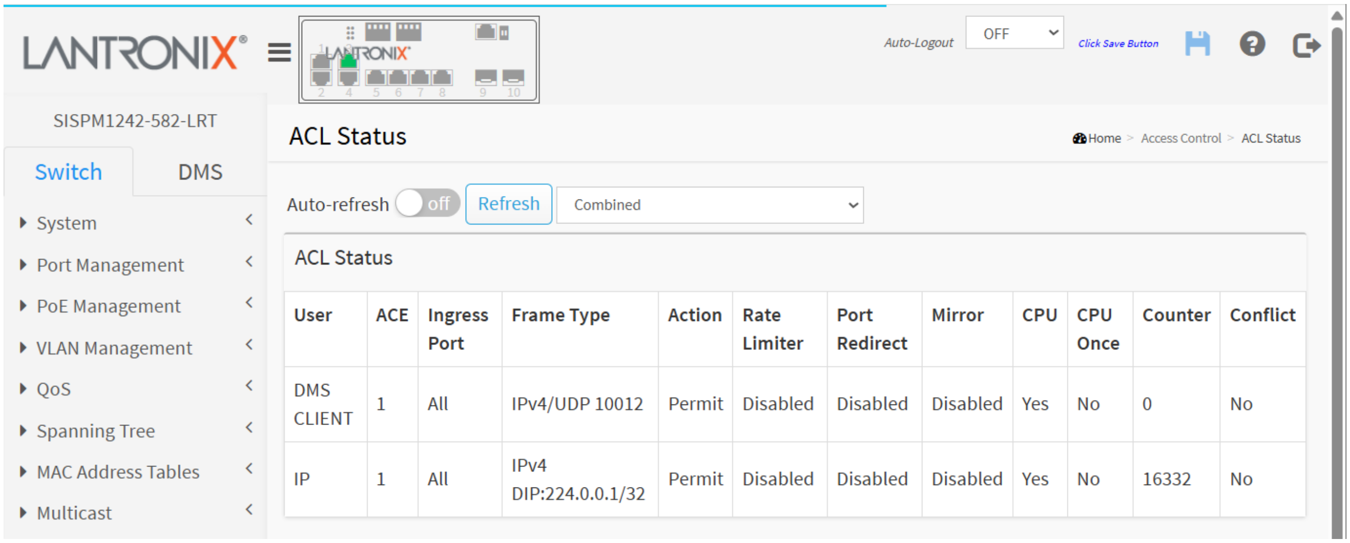
CPU : Forward packets that matched the specific ACE to CPU.

CPU Once : Forward first packet that matched the specific ACE to CPU.

Counter : Indicates the number of times the ACE was hit by a frame.

Conflict : Indicates the hardware status of the specific ACE. The specific ACE is not applied to the hardware due to hardware limitations.

Example:



ACL Status

ACL Status

User	ACE	Ingress Port	Frame Type	Action	Rate Limiter	Port Redirect	Mirror	CPU	CPU Once	Counter	Conflict
DMS CLIENT	1	All	IPv4/UDP 10012	Permit	Disabled	Disabled	Disabled	Yes	No	0	No
IP	1	All	IPv4 DIP:224.0.0.1/32	Permit	Disabled	Disabled	Disabled	Yes	No	16332	No

14. SNMP

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

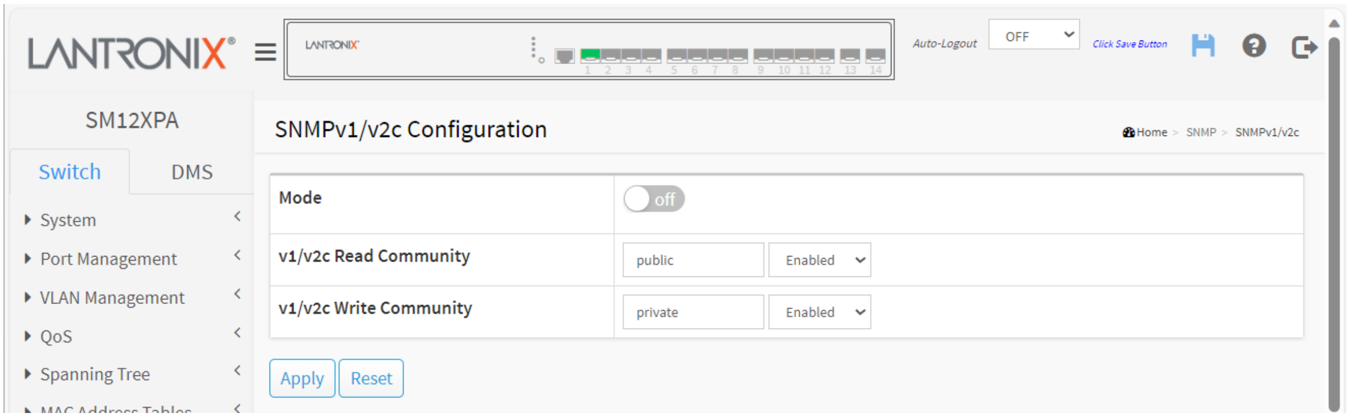
Basically, it is passive except issuing the trap information. The switch can turn the SNMP agent on or off. If you set the SNMPv1/v2c to "***on***", the SNMP agent will start up. All supported MIB OIDs, including the RMON MIB, can be accessed via the SNMP manager. If the SNMP Mode is set to "***off***", the SNMP agent will be de-activated, and the related Community Name, Trap Host IP Address, Trap, and all MIB counters are ignored.

SNMPv1/v2c

This page lets you set SNMP v1 and v2 parameters. This function is used to configure SNMP settings, community name, trap host and public traps. An SNMP manager must pass the authentication by identifying both community names, then it can access the MIB information of the target device. So, both parties must have the same community name.

To configure SNMPv1/v2c in the web UI:

1. Go to SNMP > SNMPv1/v2c Configuration.
2. Enable (on) or disable (off) the SNMP Mode for the SNMPv1/v2c function.
3. Specify the Read Community and Write Community.
4. Click **Apply** to save the configuration.



SNMPv1/v2c Configuration

Mode	off
v1/v2c Read Community	public Enabled
v1/v2c Write Community	private Enabled

Parameter descriptions:

Mode : Sets the SNMP mode of operation. Possible modes are:

- ***on*** : Enable SNMP operation mode.
- ***off*** : Disable SNMP operation mode (default).

Read/Write Community : The ID that allows access/change to the device's data.

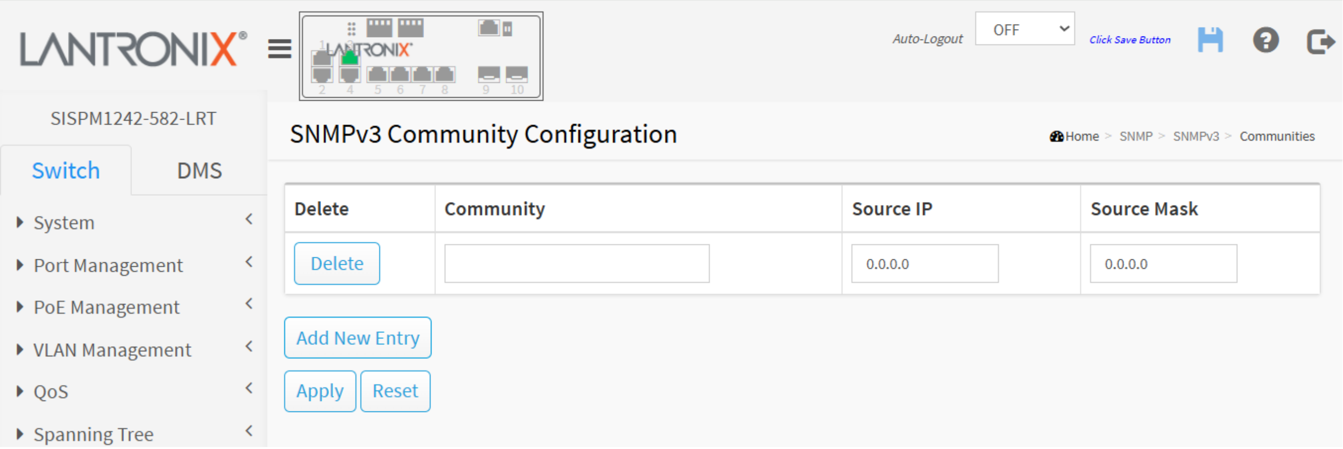
SNMPv3

Communities

Configure SNMPv3 community configuration table on this page. The entry index key is Community.

To configure SNMPv3 Communities in the web UI:

1. Go to SNMP > SNMPv3 > Communities.
2. Click **Add New Entry**.
3. Specify the SNMP community parameters.
4. Click **Apply** to save the configuration.



SNMPv3 Community Configuration

Delete	Community	Source IP	Source Mask
Delete		0.0.0.0	0.0.0.0

Parameter descriptions:

Add New Entry : Click to add a new entry to the table. Specify the name, configure the new entry and click **Apply**.

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

Community : Enter the security name to map the community to the SNMP Groups configuration.
The allowed string length is 1 to 32 characters, and the allowed content is ASCII characters 33 - 126.

Source IP : Enter the SNMP access source address. A particular range of source addresses can be used to restrict source subnet when combined with a Source Mask.

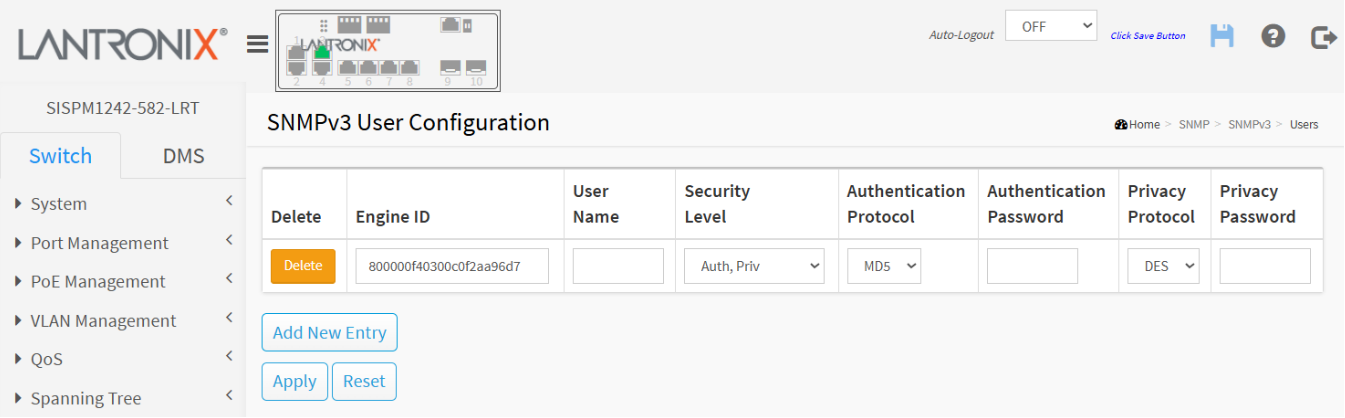
Source Mask : Enter the IP source mask.

Users

This page lets you set SNMPv3 users' parameters. The Entry index key is UserName. The maximum number of Groups is 6.

To configure SNMP Users in the web UI:

1. Go to SNMP > SNMPv3 > Users.
2. Click **Add New Entry**.
3. Specify the SNMPv3 Users parameters.
4. Click **Apply**.



SNMPv3 User Configuration

Delete	Engine ID	User Name	Security Level	Authentication Protocol	Authentication Password	Privacy Protocol	Privacy Password
Delete	800000f40300c0f2aa96d7		Auth, Priv	MD5		DES	

Add New Entry

Apply Reset

Parameter descriptions:

Add New Entry : Click to add a new entry to the table. Specify the name, configure the new entry, and click **Apply**.

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

Engine ID : An octet string identifying the engine ID that this entry should belong to. The string must contain an even number(in hexadecimal format) with number of digits between 10 and 64, but all-zeros and all-'F's are not allowed. The SNMPv3 architecture uses the User-based Security Model (USM) for message security and the View-based Access Control Model (VACM) for access control. For the USM entry, the usmUserEngineID and usmUserName are the entry's keys. In a simple agent, usmUserEngineID is always that agent's own snmpEngineID value. The value can also take the value of the snmpEngineID of a remote SNMP engine with which this user can communicate. In other words, if user engine ID equals system engine ID then it is local user; otherwise, it's remote user.

User Name : A string identifying the user name that this entry should belong to. The allowed string length is 1-31 characters, and the allowed content is ASCII characters 33 - 126.

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

- ***NoAuth, NoPriv*** : No authentication and no privacy.
- ***Auth, NoPriv*** : Authentication and no privacy.
- ***Auth, Priv*** : Authentication and privacy.

The value of security level cannot be modified if entry already exists. That means it must first be ensured that the value is set correctly.

Authentication Protocol : Indicates the authentication protocol that this entry should belong to. Possible authentication protocols are:

- ***MD5***: An optional flag to indicate that this user uses MD5 authentication protocol.
- ***SHA***: An optional flag to indicate that this user uses SHA authentication protocol.

The value of security level cannot be modified if entry already exists. That means you must first ensure that the value is set correctly.

Authentication Password : A string identifying the authentication password phrase. For MD5 authentication protocol, the allowed string length is 8 to 39 characters. For SHA authentication protocol, the allowed string length is 8 to 39 characters. The allowed content is ASCII characters 33 - 126.

Privacy Protocol : Indicates the privacy protocol that this entry should belong to. Possible privacy protocols are:

- ***DES***: An optional flag to indicate that this user uses DES authentication protocol.
- ***AES***: An optional flag to indicate that this user uses AES authentication protocol.

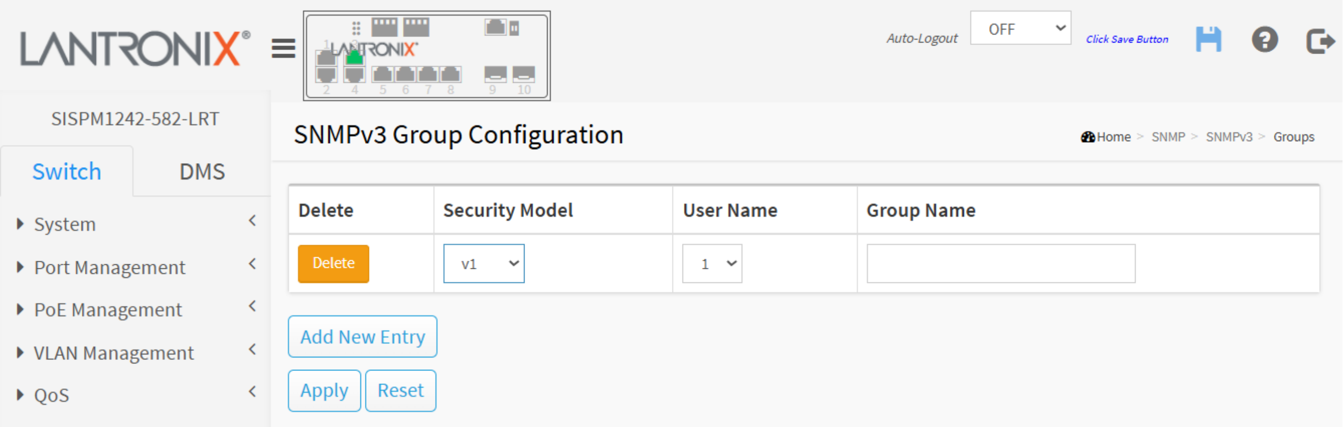
Privacy Password : A string identifying the privacy password phrase. The allowed string length is 8 - 31 characters, and the allowed content is ASCII characters 33 - 126.

Groups

This page lets you configure SNMPv3 groups. The Entry index keys are Security Model and Security Name. The maximum number of Groups supported is 12.

To configure SNMP Groups in the web UI:

1. Go to SNMP > SNMPv3 > Groups.
2. Click **Add New Entry**.
3. Specify the SNMP group parameters.
4. Click **Apply**.



SNMPv3 Group Configuration

Delete	Security Model	User Name	Group Name
Delete	v1	1	

Parameter descriptions:

Add New Entry : Click to add a new entry to the table. Specify the name, configure the new entry, then click **Apply**.

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

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

- ***v1***: Reserved for SNMPv1 (default).

- ***v2c***: Reserved for SNMPv2c.
- ***usm***: User-based Security Model (USM).

User Name : A string identifying the security name that this entry should belong to. The allowed string length is 1 - 31 characters, and the allowed content is ASCII characters 33 - 126.

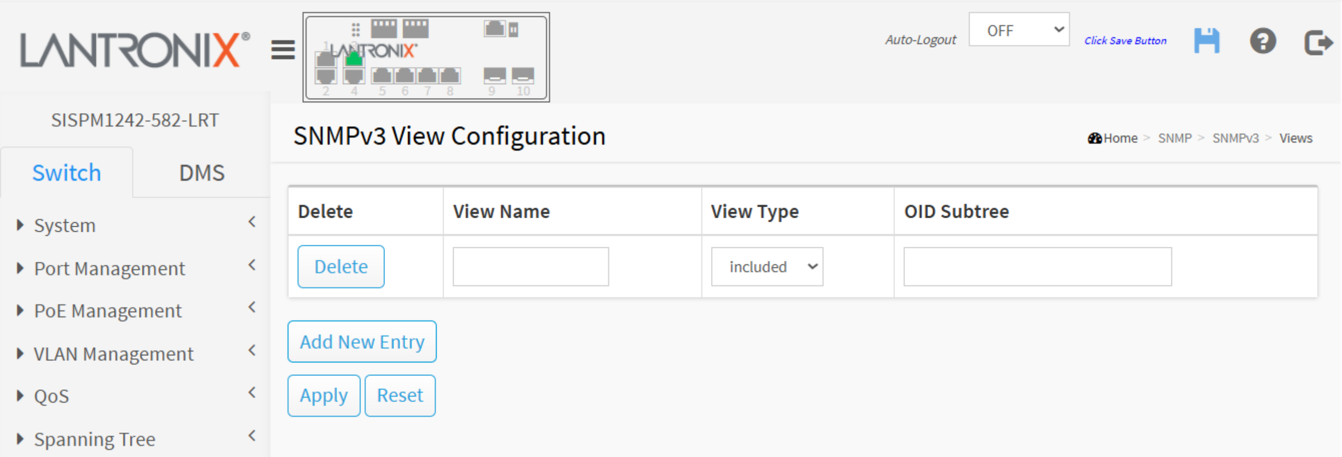
Group Name : A string identifying the group name that this entry should belong to. The allowed string length is 1 - 32 characters, and the allowed content is ASCII characters 33 - 126.

Views

Configure SNMPv3 View on this page. The Entry index keys are OID Subtree and View Name. The maximum number of Views supported is 12.

To configure SNMP Views in the web UI:

1. Go to SNMP > SNMPv3 > Views.
2. Click **Add New Entry.**
3. Specify the SNMP View parameters.
4. Click **Apply**. To modify or clear the settings click Reset.



SNMPv3 View Configuration

Delete	View Name	View Type	OID Subtree
Delete		included	

Parameter descriptions:

Add New Entry : Click to add a new entry to the table. Specify the name, configure the new entry, and click **Apply**.

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

View Name : A string identifying the view name that this entry should belong to. The allowed string length is 1 - 31 characters, and the allowed content is ASCII characters 33 - 126.

View Type : Indicates the view type that this entry should belong to. Possible view types are:

- ***Included***: An optional flag to indicate that this view subtree should be included.
- ***Excluded***: An optional flag to indicate that this view subtree should be excluded. In general, if a view entry's view type is 'Excluded', there should be another view entry existing with view type as 'Included' and it's OID subtree should overstep the 'Excluded' view entry.

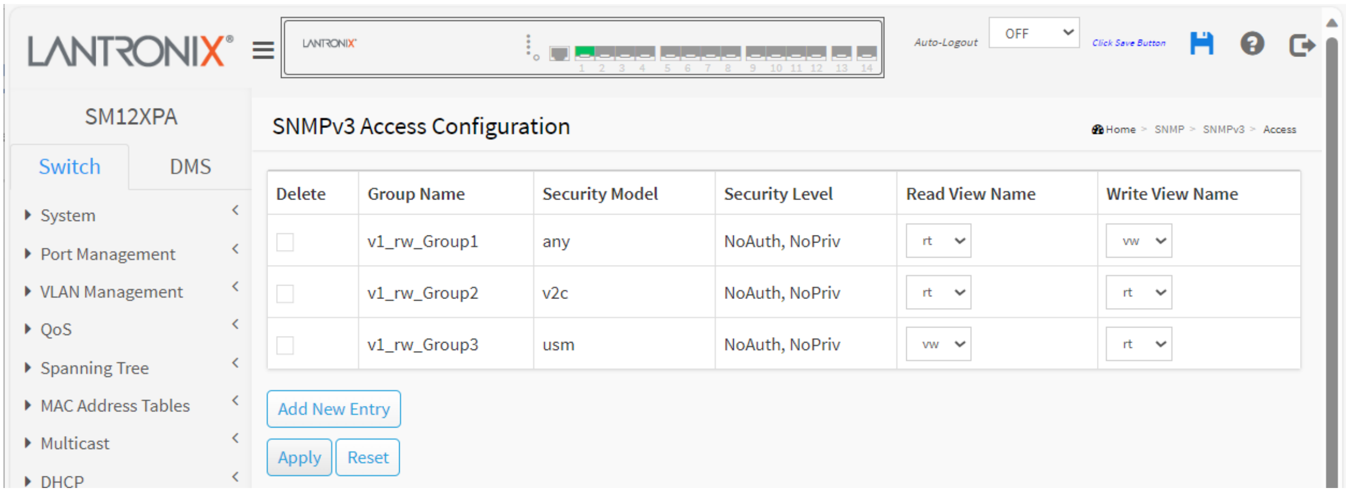
OID Subtree : The OID defining the root of the subtree to add to the named view. The allowed OID length is 1 - 128. The allowed string content is a digital number or an asterisk (*). Object Identifiers (OIDs) uniquely identify or name MIB variables in the tree.

Access

This page lets you configure SNMPv3 accesses. The Entry index keys are Group Name, Security Model and Security Level. The maximum number of Accesses supported is 12.

To configure SNMP Access in the web UI:

1. Go to SNMP > SNMPv3 > Access.
2. Click **Add New Entry.**
3. Specify the SNMP Access parameters.
4. Click **Apply**.



SNMPv3 Access Configuration

Delete	Group Name	Security Model	Security Level	Read View Name	Write View Name
□	v1_rw_Group1	any	NoAuth, NoPriv	rt	vw
□	v1_rw_Group2	v2c	NoAuth, NoPriv	rt	rt
□	v1_rw_Group3	usm	NoAuth, NoPriv	vw	rt

Add New Entry

Apply Reset

Parameter descriptions:

Add New Entry : Click to add a new entry. Specify the name, configure the new entry, and click **Apply**.

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

Group Name : A string identifying the group name that this entry should belong to. The allowed string length is 1 - 31 characters, and the allowed content is ASCII characters 33 - 126.

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

- ***Any***: Any security model accepted (v1|v2c|usm).
- ***v1***: Reserved for SNMPv1.
- ***v2c***: Reserved for SNMPv2c.
- ***usm***: User-based Security Model (USM).

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

- ***NoAuth, NoPriv*** : No authentication and no privacy.
- ***Auth, NoPriv*** : Authentication and no privacy.
- ***Auth, Priv*** : Authentication and privacy.

Read View Name : The name of the MIB view defining the MIB objects for which this request may request the current values. The allowed string length is 1 - 31 characters, and the allowed content is ASCII characters 33 - 126.

Write View Name : The name of the MIB view defining the MIB objects for which this request may potentially set new values. The allowed string length is 1 - 31 characters, and the allowed content is ASCII characters 33 - 126.

Statics

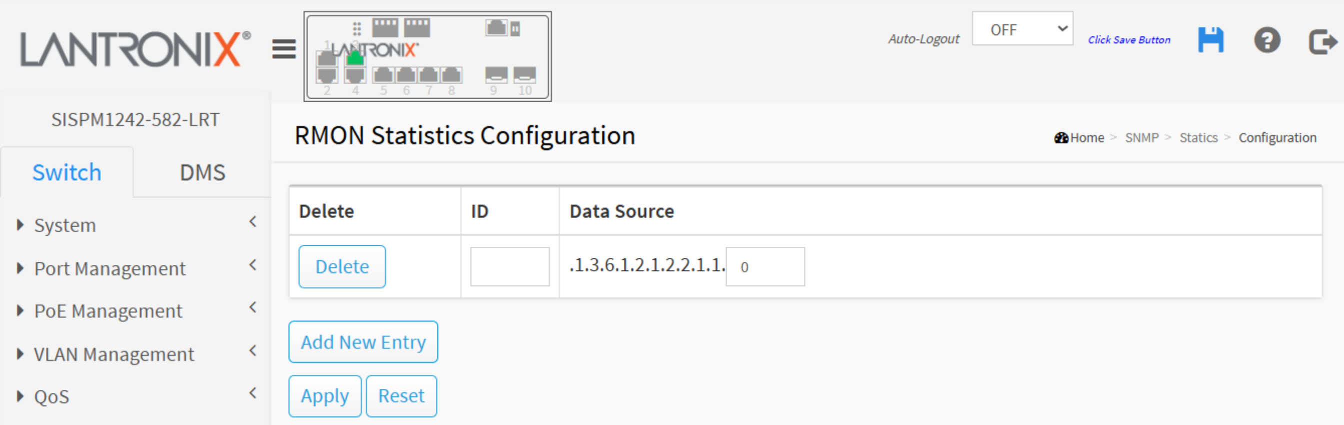
Configuration

Remote Network Monitoring (RMON) is a process for monitoring network traffic on a remote Ethernet segment to detect network issues such as dropped packets, network collisions, and traffic congestion.

Configure RMON Statistics table on this page. The entry index key is ID.

To configure RMON Statistics in the web UI:

1. Go to SNMP > Statics > Configuration.
2. Click **Add New Entry**.
3. Specify the ID and Data Source parameters.
4. Click **Apply**.



RMON Statistics Configuration

Delete	ID	Data Source
Delete		.1.3.6.1.2.1.2.2.1.1. 0

Parameter descriptions:

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

Add New Entry : Click to add a new entry to the table.

ID : Indicates the index of the entry. The valid range is 1 - 65535.

Data Source : Enter the port ID which you want to be monitored.

Statistics

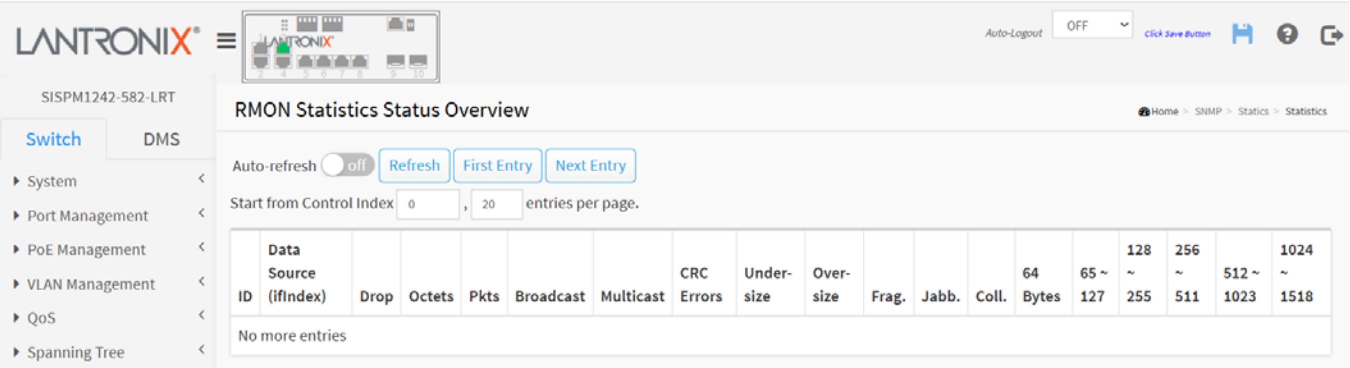
This page displays RMON Statistics entries. Each page shows up to 99 entries from the Statistics table, default being 20, selected through the "entries per page" input field. When first visited, the web page will show the first 20 entries from the beginning of the Statistics table. The first entry displayed will be the one with the lowest ID found in the Statistics table.

The "Start from Control Index" lets you select the starting point in the Statistics table. Clicking the **Refresh** button will update the displayed table starting from that or the next closest Statistics table match.

The **Next Entry** will use the last entry of the currently displayed entry as a basis for the next lookup. When the end is reached the text "No more entries" is shown in the displayed table. Use the **First Entry** button to start over.

To view RMON Statistics Status in the web UI:

1. Go to SNMP > Statics > Statistics.
2. **Auto-refresh** will refresh the page every 3 seconds. **Refresh** will refresh the page immediately.
3. Use the First Entry / Next Entry controls and “Start from” entry fields to help you navigate through the list.



RMON Statistics Status Overview

Start from Control Index 0 , 20 entries per page.

ID	Data Source (ifIndex)	Drop	Octets	Pkts	Broadcast	Multicast	CRC Errors	Under-size	Over-size	Frag.	Jabb.	Coll.	64 Bytes	65 ~ 127	128 ~ 255	256 ~ 511	512 ~ 1023	1024 ~ 1518
No more entries																		

Parameter descriptions:

ID : Indicates the index of Statistics entry.

Data Source(if Index) : The port ID which wants to be monitored.

Drop : The total number of events in which packets were dropped by the probe due to lack of resources.

Octets : The total number of octets of data (including those in bad packets) received on the network.

Pkts : The total number of packets (including bad packets, broadcast packets, and multicast packets) received.

Broadcast : The total number of good packets received that were directed to the broadcast address.

Multicast : The total number of good packets received that were directed to a multicast address.

CRC Errors : The total number of packets received that had a length (excluding framing bits, but including FCS octets) of between 64 and 1518 octets, inclusive, but had either a bad Frame Check Sequence (FCS) with an integral number of octets (FCS Error) or a bad FCS with a non-integral number of octets (Alignment Error).

Under-size : The total number of packets received that were less than 64 octets.

Over-size : The total number of packets received that were longer than 1518 octets.

Frag. : The number of frames which size is less than 64 octets received with invalid CRC.

Jabb. : The number of frames which size is larger than 64 octets received with invalid CRC.

Coll. : The best estimate of the total number of collisions on this Ethernet segment.

64 Bytes : The total number of packets (including bad packets) received that were 64 octets in length.

65~127 : The total number of packets (including bad packets) received that were between 65 to 127 octets in length.

128~255 : The total number of packets (including bad packets) received that were between 128 to 255 octets in length.

256~511 : The total number of packets (including bad packets) received that were between 256 to 511 octets in length.

512~1023 : The total number of packets (including bad packets) received that were between 512 to 1023 octets in length.

1024~1588 : The total number of packets (including bad packets) received that were between 1024 to 1588 octets in length.

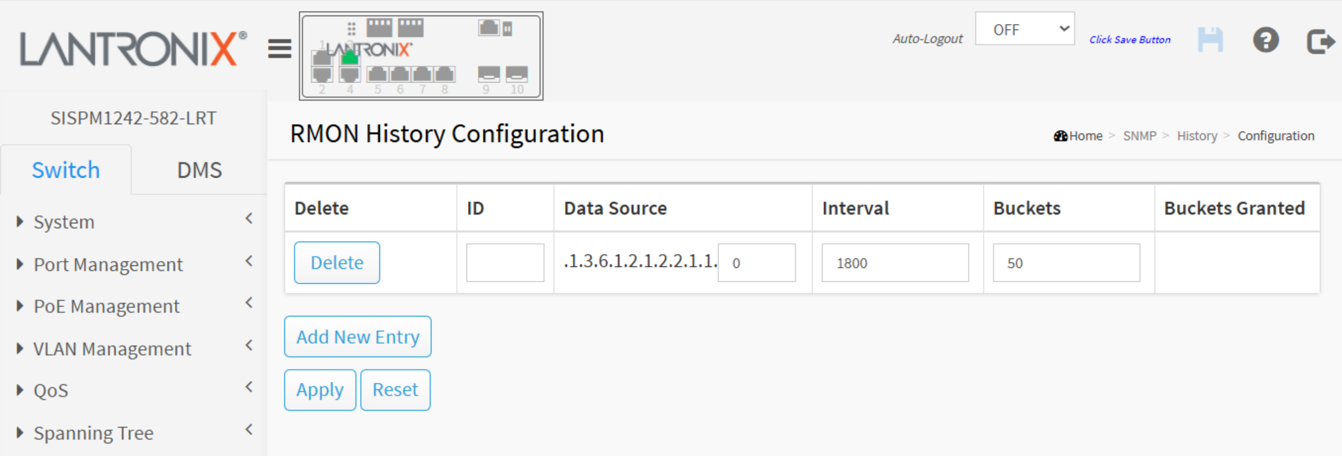
History

Configuration

Configure the RMON History table on this page. The entry index key is ID.

To configure RMON History in the web UI:

1. Go to SNMP, History, and Configuration.
2. Click **Add New Entry.**
3. Specify the ID and parameters.
4. Click **Apply**.



Auto-Logout: OFF

RMON History Configuration

Delete	ID	Data Source	Interval	Buckets	Buckets Granted
Delete		.1.3.6.1.2.1.2.2.1.1. 0	1800	50	

Add New Entry

Apply Reset

Parameter descriptions:

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

Add New Entry : Click to add a new entry to the table.

ID : Indicates the index of the entry. The range is 1 - 65535.

Data Source : Enter the port ID which you want to be monitored.

Interval : Sets the interval in seconds for sampling history statistics data. The valid range is 1 - 3600; the default value is 1800 seconds.

Buckets : Sets the maximum data entries associated with this History control entry stored in RMON. The valid range is 1 - 3600; the default value is 50.

Buckets Granted : The number of data to be saved in the RMON.

Status

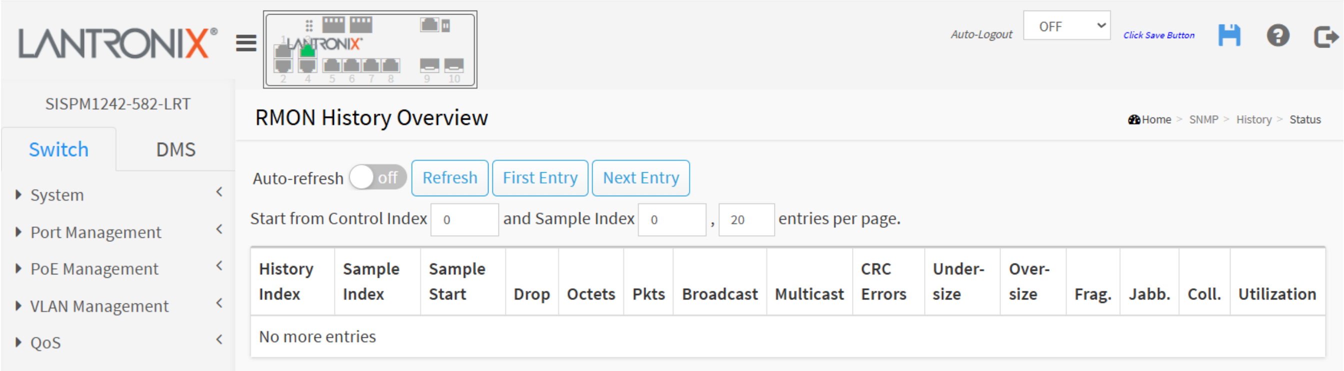
This page provides an overview of RMON History entries. Each page shows up to 99 entries from the History table, default being 20, selected through the "entries per page" input field. When first visited, the web page will show the first 20 entries from the beginning of the History table. The first displayed 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. Go to SNMP > History > Status.
2. **Auto-refresh** will refresh the page every 3 seconds. **Refresh** will refresh the page immediately.
3. Use the First Entry / Next Entry controls and "Start from" entry fields to help you navigate through the list.



RMON History Overview

Start from Control Index 0 and Sample Index 0 , 20 entries per page.

History Index	Sample Index	Sample Start	Drop	Octets	Pkts	Broadcast	Multicast	CRC Errors	Under-size	Over-size	Frag.	Jabb.	Coll.	Utilization
No more entries														

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.

Alarm

Configuration

Configure RMON Alarm table parameters on this page. The entry index key is ID.

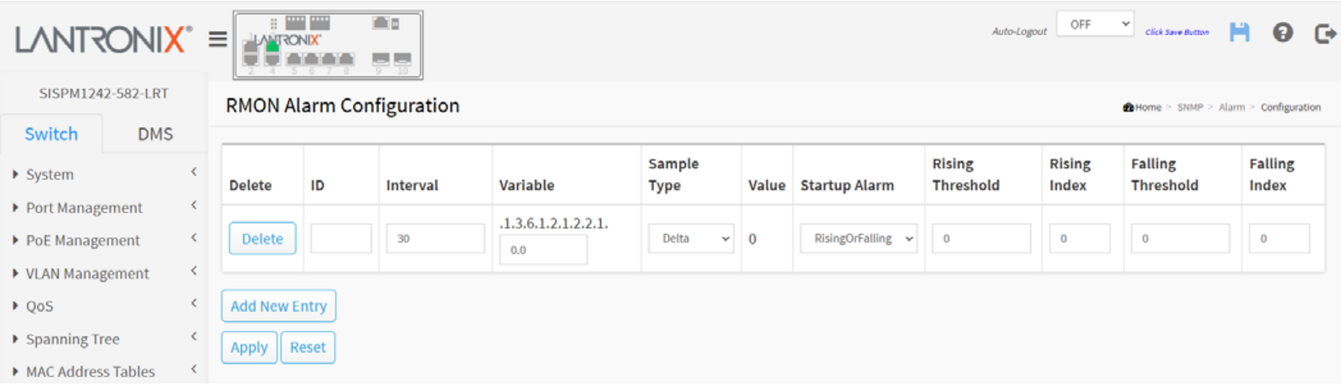
To configure RMON Alarm Configuration parameters in the web UI:

1. Go to SNMP > Alarm > Configuration.

2. Click **Add New Entry**.

3. Specify the alarm parameters.

4. Click **Apply**.



RMON Alarm Configuration

Delete	ID	Interval	Variable	Sample Type	Value	Startup Alarm	Rising Threshold	Rising Index	Falling Threshold	Falling Index
Delete		30	.1.3.6.1.2.1.2.2.1. 0.0	Delta	0	RisingOrFalling	0	0	0	0

Add New Entry

Apply Reset

Parameter descriptions:

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

Add New Entry : Click to add a new entry.

ID : Sets the index of the entry. The range is 1 to 65535.

Interval : Sets the interval in seconds for sampling and comparing the rising and falling threshold. The range is from 1 to 2^31-1.

Variable : Indicates the variable to be sampled. The possible variables are:

- ***InOctets***: The total number of octets received on the interface, including framing characters.
- ***InUcastPkts*** : The number of unicast packets delivered to a higher-layer protocol.
- ***InNUcastPkts*** : The number of broad-cast and multi-cast packets delivered to a higher-layer protocol.
- ***InDiscards*** : The number of inbound packets that are discarded even the packets are normal.
- ***InErrors*** : The number of inbound packets that contained errors preventing them from being deliverable to a higher-layer protocol.
- ***InUnknownProtos***: the number of the inbound packets that were discarded because of the unknown or un-support protocol.
- ***OutOctets*** : The number of octets transmitted out of the interface , including framing characters.
- ***OutUcastPkts*** : The number of unicast packets that request to transmit.
- ***OutNUcastPkts*** : The number of broad-cast and multi-cast packets that request to transmit.
- ***OutDiscards*** : The number of outbound packets that are discarded event the packets is normal.
- ***OutErrors*** : The number of outbound packets that could not be transmitted because of errors.
- ***OutQLen*** **:** The length of the output packet queue (in packets).

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

- ***Absolute***: Get the sample directly.
- ***Delta***: Calculate the difference between samples (default).

Value : The value of the statistic during the last sampling period.

Startup Alarm : The method of sampling the selected variable and calculating the value to be compared against the thresholds, possible sample types are:

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

Rising Threshold : Rising threshold value (-2147483648-2147483647). 'Rising threshold' must be larger than 'Falling threshold'

Rising Index : Rising event index (1-65535).

Falling Threshold : Falling threshold value (-2147483648-2147483647)

Falling Index : Falling event index (1-65535).

Status

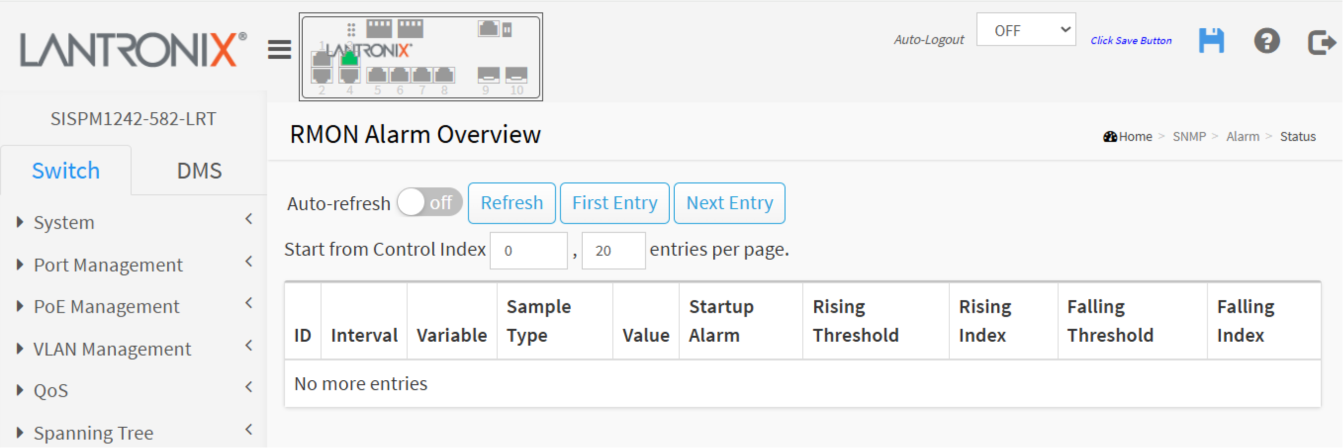
This page provides an overview of RMON Alarm entries. Each page shows up to 99 entries from the Alarm table, default being 20, selected through the "entries per page" input field. When first visited, the web page shows the first 20 entries from the beginning of the Alarm table. The first displayed will be the one with the lowest ID found in the Alarm table.

The "Start from Control Index" lets you select the starting point in the Alarm table. Clicking the Refresh button will update the displayed table starting from that or the next closest Alarm table match.

The Next Entry will use the last entry of the currently displayed entry as a basis for the next lookup. When the end is reached the text "*No more entries*" displays in the table. Use the First Entry button to start over.

To display RMON Alarm Status in the web UI:

1. Go to SNMP > Alarm > Status.
2. **Auto-refresh** will refresh the page every 3 seconds. **Refresh** will refresh the page immediately.
3. Use the First Entry / Next Entry controls and “Start from” entry fields to help you navigate through the list.



RMON Alarm Overview

Start from Control Index 0 , 20 entries per page.

ID	Interval	Variable	Sample Type	Value	Startup Alarm	Rising Threshold	Rising Index	Falling Threshold	Falling Index
No more entries									

Parameter descriptions:

ID : Indicates the index of Alarm control entry.

Interval : Indicates the interval in seconds for sampling and comparing the rising and falling threshold.

Variable : Indicates the variable to be sampled.

Sample Type : The method of sampling the selected variable and calculating the value to be compared against the thresholds.

Value : The value of the statistic during the last sampling period.

Startup Alarm : The alarm that may be sent when this entry is first set to valid.

Rising Threshold : Rising threshold value.

Rising Index : Rising event index.

Falling Threshold : Falling threshold value.

Falling Index : Falling event index.

Start from Control Index : Lets you select the starting point in the table.

entries per page : You can choose how many items you want to show per page.

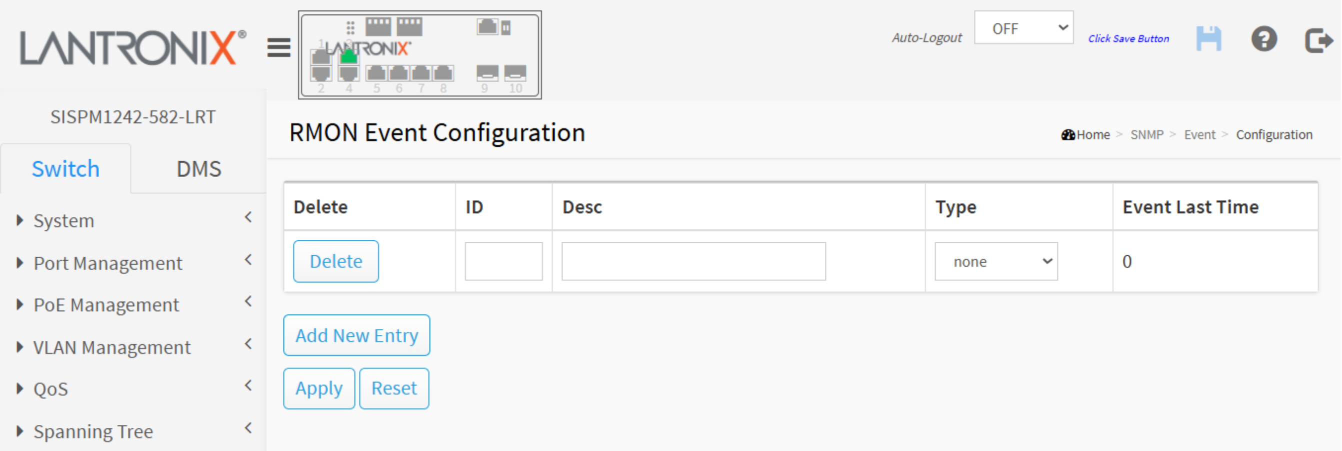
Event

Configuration

Configure RMON Event parameters on this page. The entry index key is ID.

To configure RMON Event parameters in the web UI:

1. Go to SNMP > Event > Configuration.
2. Click **Add New Entry**.
3. Specify the RMON event parameters.
4. Click **Apply**.



RMON Event Configuration

Delete	ID	Desc	Type	Event Last Time
Delete			none	0

Parameter descriptions:

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

Add New Entry : Click to add a new entry to the table.

ID : Enter the index of the entry. The range is 1 to 65535.

Desc : Enter this event, the string length is 0 to 127, default is a null string.

Type : Enter the notification of the event; the possible types are:

- ***None***: No SNMP log is created, and no SNMP trap is sent.
- ***Log***: Create an SNMP log entry when the event is triggered.
- ***Snmp trap***: Send an SNMP trap when the event is triggered.
- ***Log and trap***: Create an SNMP log entry and send an SNMP trap when the event is triggered.

Event Last Time : Shows the value of *sysUpTime* at the time this event entry last generated an event.

Status

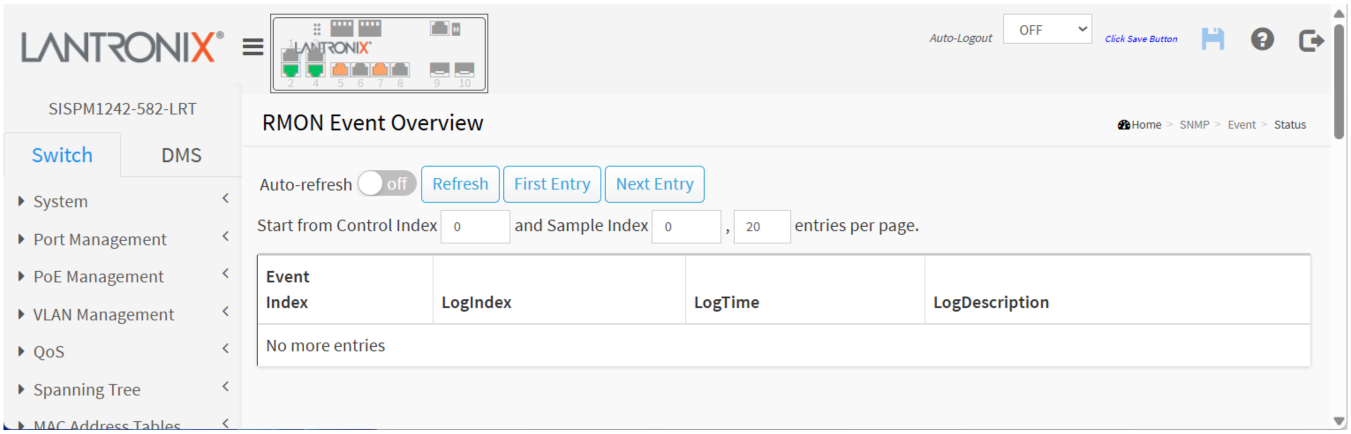
This page displays RMON Event table entries. Each page shows up to 99 entries from the Event table, default being 20, selected through the "entries per page" input field. When first visited, the web page will show the first 20 entries from the beginning of the Event table. The first displayed will be the one with the lowest Event Index and Log Index found in the Event table.

The "Start from Event Index and Log Index" lets you select the starting point in the Event table. Clicking the Refresh button will update the displayed table starting from that or the next closest Event table match.

The Next Entry button uses the last entry of the currently displayed entry as a basis for the next lookup. When the end is reached the text "*No more entries*" is displayed in the table. Use the First Entry button to start over.

To display RMON Event Status in the web UI:

1. Go to SNMP > Event > and Status.
2. **Auto-refresh** will refresh the page every 3 seconds. **Refresh** will refresh the page immediately.
3. Use the First Entry / Next Entry controls and “Start from” entry fields to help you navigate through the list.



RMON Event Overview

Start from Control Index 0 and Sample Index 0 , 20 entries per page.

Event Index	LogIndex	LogTime	LogDescription
No more entries			

Parameter descriptions:

Event Index : Indicates the index of the event entry.

LogIndex : Indicates the index of the log entry.

LogTIme : Indicates Event log time

LogDescription : Indicates the Event description.

15. CFM

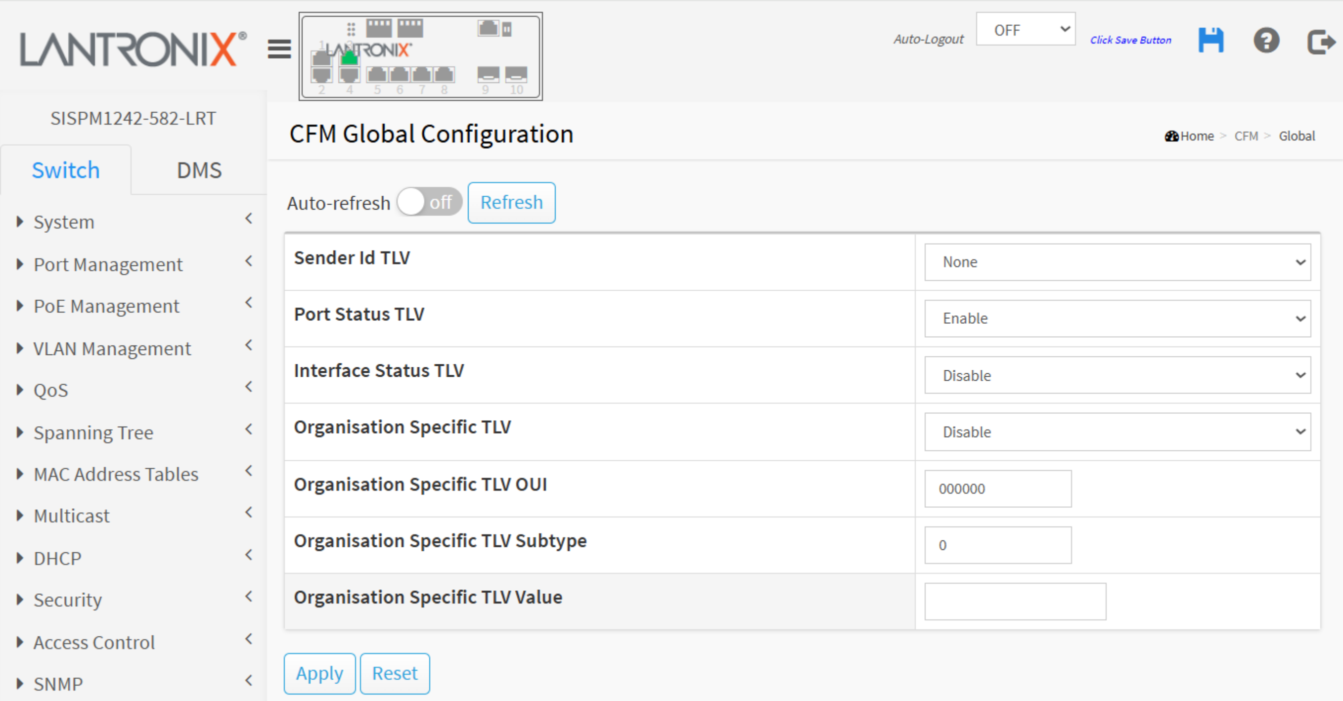
This section lets you set CFM (Connectivity Fault Management) Global, Domain, and Service parameters.

CFM is a standard defined by IEEE 802.1ag. It defines protocols and practices for OAM and is largely identical with ITU-T Recommendation Y.1731.

The standard **1**) defines maintenance domains, their constituent maintenance points, and the managed objects required to create and administer them. **2**) defines the relationship between maintenance domains and the services offered by VLAN-aware bridges and provider bridges. **3**) describes the protocols and procedures used by maintenance points to maintain and diagnose connectivity faults within a maintenance domain. **4**) provides means for future expansion of the capabilities of maintenance points and their protocols.

Global

Configure global CFM parameters on this page.



CFM Global Configuration

Sender Id TLV	None
Port Status TLV	Enable
Interface Status TLV	Disable
Organisation Specific TLV	Disable
Organisation Specific TLV OUI	000000
Organisation Specific TLV Subtype	0
Organisation Specific TLV Value	

Parameter descriptions:

Sender Id TLV : Choose whether and what to use as Sender ID TLVs in CCMs generated by this switch. This parameter can be overridden by Domain and Service level configuration.

- ***None*** : Do not include Sender ID TLVs.
- ***Chassis*** : Enable Sender ID TLV and send Chassis ID (MAC Address).
- ***Manage*** : Enable Sender ID TLV and send Management address (IPv4 Address).
- ***ChassisManage*** : Enable Sender ID TLV and send both Chassis ID (MAC Address) and Management Address (IPv4 Address).
- ***Defer***: Let the Domain configuration decide if Sender ID TLVs will be included.

Port Status TLV : Choose whether to send Port Status TLVs in CCMs generated by this switch. Can be overridden by Domain and Service level configuration.

- ***Enable*** : Send Port Status TLVs in CCMs generated by this switch.
- ***Disable*** : Do not send Port Status TLVs in CCMs generated by this switch.

Interface Status TLV : Choose whether to send Interface Status TLVs in CCMs generated by this switch. Can be overridden by Domain and Service level configuration.

- ***Enable*** : Send Interface Status TLVs in CCMs generated by this switch.
- ***Disable*** : Do not Send Interface Status TLVs in CCMs generated by this switch.

Organisation Specific TLV : Choose whether to send Organisation Specific TLVs in CCMs generated by this switch. Can be overridden by Domain and Service level configuration.

- ***Enable*** : Send Organization Specific TLVs in CCMs generated by this switch.
- ***Disable*** : Do not send Organisation Specific TLVs in CCMs generated by this switch.

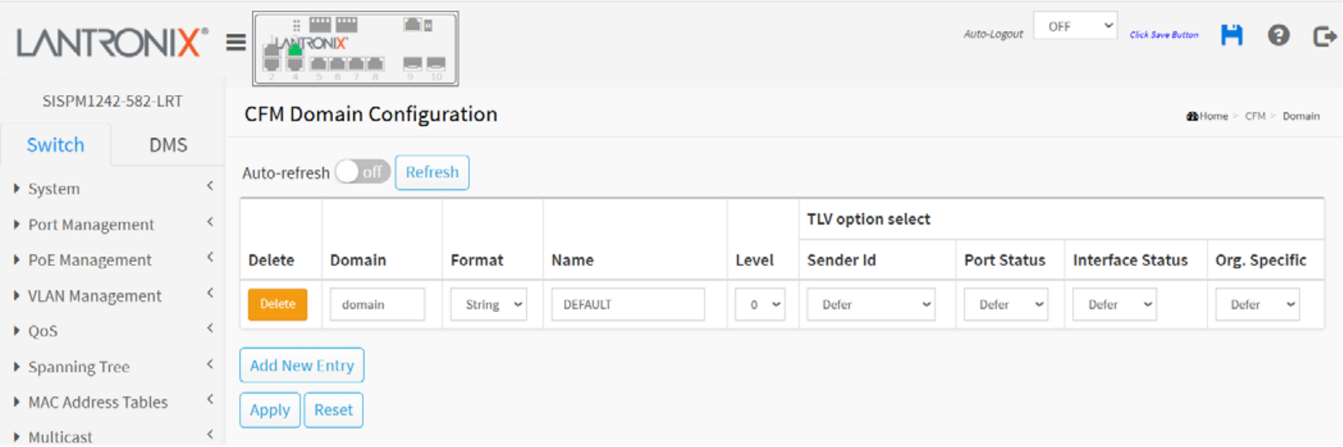
Organisation Specific TLV OUI : This is the three-bytes OUI transmitted with the Organization-Specific TLVs. Enter as six characters 0-9, a-f.

Organisation Specific TLV Subtype : This is the subtype transmitted with the Organization-Specific TLV. Can be any value in the range [0; 255].

Organisation Specific TLV Value : This is the value transmitted in the Organization-Specific TLVs. Can be a printable character string of length 0-63.

Domain

Configure CFM Domain parameters on this page. Ethernet Connectivity Fault Management (CFM per IEEE 802.1ag) is an end-to-end Ethernet OAM that can cross multiple domains to monitor the health of the entire service instance.



CFM Domain Configuration

					TLV option select			
Delete	Domain	Format	Name	Level	Sender Id	Port Status	Interface Status	Org. Specific
Delete	domain	String	DEFAULT	0	Defer	Defer	Defer	Defer

Parameter descriptions:

Add New Entry : Click to add a new Domain entry.

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

Domain : Name of the Domain. The value is a single word which begins with an alphabetic letter A-Z or a-z with a length of 1-15 letters.

Format : Select the MD name format.

- ***None*** : Select to mimic ITU-T Y.1731 MEG IDs (contains only the MEG ID).
- ***String*** : Select to mimic 802.1ag format (contains both MD and MA names).

Name : The contents of this parameter depend on the value of the format member. If format is None then Name is not used but will be set to all-zeros behind the scenes. This format is typically used by Y.1731 kind of PDUs. If format is String, then the Name must contain a string 1 - 43 characters long.

Level : MD/MEG level of this domain. Valid values are 0 - 7.

About leak prevention *: Leak prevention is about discarding OAM PDUs with MEG levels lower than the MEP they hit when the OAM PDUs are ingressing the port on which the MEP resides, and to discard OAM PDUs with MEG levels at or lower than the MEP's when the OAM PDUs are ingressing other ports.*

There are two categories of architectures, when it comes to leak-prevention: those that use Shared MEG level and those that use Independent MEG level:

Shared MEG level *: On Shared MEG level architectures, Port Down MEPs always perform level filtering no matter which VLAN ID (VID) OAM PDUs get classified to, unless the same port has a VLAN MEP on the VID in question. So if you have a Port MEP in VID X and a VLAN MEP in VID Y, an OAM frame arriving on the port and gets classified to VID X or VID Z will be handled/level-filtered by the Port MEP, whereas an OAM frame ingressing the port in VID Y will be handled by the VLAN MEP. Likewise, if the switch has a Port MEP on VID X on Port X and an OAM frame ingresses on VID Y on Port Y, it is subject to level filtering before egressing Port X, unless Port X also has a VLAN MEP on VID Y, in which case the VLAN MEP will take care of level-filtering the OAM PDU.*

On Shared MEG level architectures, all Port MEPs must have the same MEG level and any VLAN MEP must have a MEG level higher than the Port MEPs' MEG level.

***Independent MEG level** : On Independent MEG level architectures, Port Down MEPs never perform level filtering on frames not classified to the MEP's VID. So if you have a Port MEP on VID X and a VLAN MEP on VID Y and an OAM frame ingresses any port on VID Z, it is not subject to handling/level-filtering by any of the two MEPs.*

This switch exhibits Independent MEG level.

TLV option select

Sender Id: Default Sender ID TLV format to be used in CCMs generated by this Domain (may be overridden in service).

- ***None*** : Do not include Sender ID TLVs.
- ***Chassis*** : Enable Sender ID TLV and send Chassis ID (MAC Address).
- ***Manage*** : Enable Sender ID TLV and send Management address (IPv4 Address).
- ***ChassisManage*** : Enable Sender ID TLV and send both Chassis ID (MAC Address) and Management Address (IPv4 Address).
- ***Defer*** : Let the global configuration decide if Sender ID TLVs will be included (may be overridden

in service).

Port Status: Include or exclude Port Status TLV in CCMs generated by this Domain or let higher level determine (may be overridden in Service).

- ***Disable*** : Do not include Port Status TLVs.
- ***Enable*** : Include Port Status TLVs.
- ***Defer*** : Let the global configuration decide if Port Status TLVs will be included (may be overridden in Service).

Interface Status: Include or exclude Interface Status TLV in CCMs generated by this Domain or let higher level determine (may be overridden in Service).

- ***Disable*** : Do not include Interface Status TLVs.
- ***Enable*** : Include Interface Status TLVs.
- ***Defer*** : Let the global configuration decide if Interface Status TLVs will be included (may be overridden in Service).

Org. Specific: Exclude Organization-Specific TLV in CCMs generated by this Domain or let higher level determine (may be overridden in Service).

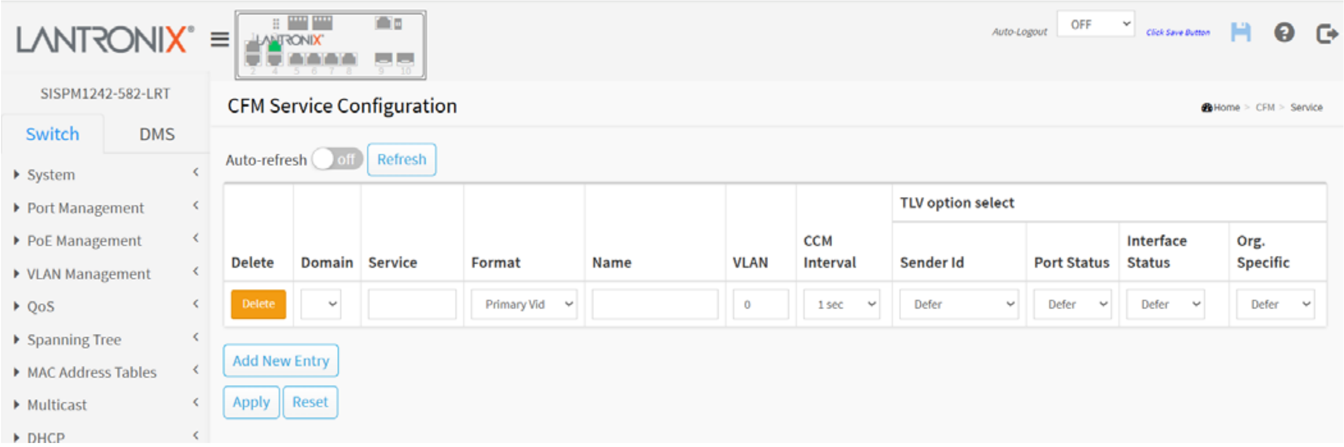
- ***Disable*** : Do not include Organization-Specific TLVs.
- ***Defer*** : Let the global configuration decide if Organization-Specific TLVs will be included (may be overridden in Service).

Service

Configure CFM Service parameters on this page.

To configure CFP service parameters in the Web UI:

1. Go to CFM > Service.
2. Click **Add New Entry.**
3. Enter the configuration.
4. Click **Apply** to save the changes.



CFM Service Configuration

							TLV option select			
Delete	Domain	Service	Format	Name	VLAN	CCM Interval	Sender Id	Port Status	Interface Status	Org. Specific
Delete			Primary Vid		0	1 sec	Defer	Defer	Defer	Defer

Parameter descriptions:

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

Add New Entry : Click to add a new Domain entry to the table.

Domain : Name of Domain under which this Service resides.

Service : Name of Service; a single word which begins with an alphabetic letter A-Z or a-z with length 1-15.

Format : Select the short Service name format. This decides how the value of the Name parameter will be interpreted. To mimic Y.1731 MEG IDs, create an MD instance with an empty name and use Y1731 ICC or Y1731 ICC CC. Possible values are:

- String
- Two Octets
- Y1731 ICC
- Y1731 ICC CC

Name : The contents of this parameter depend on the value of the format member. Besides the limitations explained for each of them, the following applies in general:

- If the Domain Format is ***None***, the size of this cannot exceed 45 bytes.
- If the Domain Format is ***not None***, the size of this cannot exceed 44 bytes.
- If Format is ***String***, the following applies:
  - Length must be in range [1; 44]
  - Contents must be in range [32; 126]

- If Format is ***Two Octets***, the following applies: Name[0] and Name[1] will both be interpreted as unsigned 8-bit integers (allowing a range of [0; 255]). Name[0] will be placed in the PDU before Name[1]. The remaining available bytes in name will not be used.
- If Format is ***Y1731 ICC***, the following applies:
    - Length must be 13.
    - Contents must be in range [a-z,A-Z,0-9]
    - Y.1731 specifies that it is a concatenation of ICC (ITU Carrier Code) and UMC (Unique MEG ID Code):
    - ICC: 1-6 bytes
    - UMC: 7-12 bytes
    - In principle, UMC can be any value in range [1; 127], but this API does not allow for specifying length of ICC, so the underlying code doesn't know where ICC ends and UMC starts. The Domain Format must be None.
- If Format is ***Y1731 ICC CC***, the following applies:
    - Length must be 15.
    - First 2 chars (CC): Must be among [A-Z]
    - Next 1-6 chars (ICC): Must be among [a-z,A-Z,0-9]
    - Next 7-12 chars (UMC): Must be among [a-z,A-Z,0-9]
    - There may be ONE (slash) present in name[3-7].
    - The Domain format must be None.

VLAN : The MA's primary VID. A primary VID of 0 means that all MEPs created within this MA will be created as port MEPs (interface MEPs). There can only be one port MEP per interface. A given port MEP may still be created with tags if that MEP's VLAN is non-zero.

A non-zero primary VID means that all MEPs created within this MA will be created as VLAN MEPs. A given MEP may be configured with another VLAN than the MA's primary VID, but it is impossible to have untagged VLAN MEPs.

CCM Interval : The CCM rate of all MEPs bound to this Service.

TLV option select:

Sender Id: Default Sender ID TLV format to be used in CCMs generated by this Service.

- ***None*** : Do not include Sender ID TLVs.
- ***Chassis*** : Enable Sender ID TLV and send Chassis ID (MAC Address).
- ***Manage*** : Enable Sender ID TLV and send Management address (IPv4 Address).
- ***ChassisManage*** : Enable Sender ID TLV and send both Chassis ID (MAC Address) and Management Address (IPv4 Address).
- ***Defer***: Let the Domain configuration decide if Sender ID TLVs will be included.

Port Status: Include or exclude Port Status TLV in CCMs generated by this Service or let higher level determine.

- ***Disable*** : Do not include Port Status TLVs.
- ***Enable*** : Include Port Status TLVs.
- ***Defer*** : Let the Domain configuration decide if Port Status TLVs will be included.

Interface Status: Include or exclude Interface Status TLV in CCMs generated by this Service or let higher level determine.

- ***Disable*** : Do not include Interface Status TLVs.

- ***Enable*** : Include Interface Status TLVs.
- ***Defer*** : Let the Domain configuration decide if Interface Status TLVs will be included.

Org. Specific : Exclude Organization-Specific TLV in CCMs generated by this Service or let higher level determine.

- ***Disable*** : Do not include Organization-Specific TLVs.
- ***Defer*** : Let the Domain configuration decide if Organization-Specific TLVs will be included.

MEP

Configure CFM MEP (Maintenance Entity Point) parameters on this page. This switch supports two types of MEPs: Port Down-MEPs and VLAN Down-MEPs:

Port Down-MEPs : In 802.1Q terminology, Port MEPs are located below the EISS entity (i.e., closest to the physical port). Port MEPs are used by, for example, APS for protection purposes. Port MEPs are created when the encompassing service has type "Port". Port MEPs may send OAM PDUs tagged or untagged. An OAM PDU will be sent untagged only if the MEP's VLAN is set to "Inherit" (0). Any other value will cause it to be sent tagged with the port's TPID, whether the VLAN matches the port's PVID and that PVID is meant to be sent untagged.

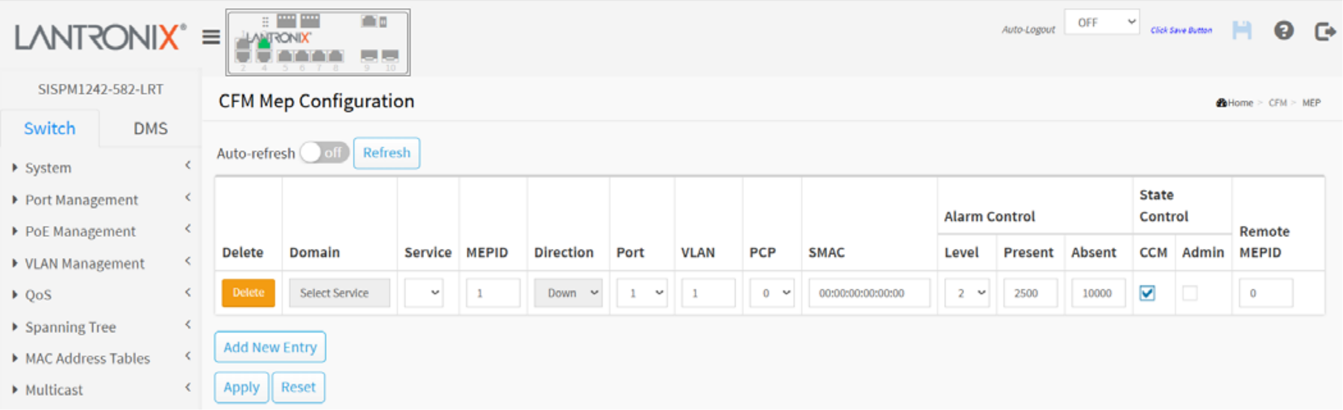
VLAN Down-MEPs : In 802.1Q terminology, VLAN MEPs are located above the EISS (Enhanced Internal Sub-layer Service) entity. This means that tagging of OAM PDUs will follow the port's VLAN configuration. Thus, if a VLAN MEP is created on the Port's PVID and PVID is configured to be untagged, OAM PDUs will be transmitted untagged. VLAN MEPs are created when the encompassing service has type "VLAN".

Down-MEP creation rules:

There are a few rules for creating Down-MEPs:

1. There can only be one Port MEP on the same port.
2. There can only be one VLAN MEP on the same port and VLAN.
3. A VLAN MEP must have a higher MD/MEG level than a Port MEP on the same port and VLAN.

These checks are performed automatically on administratively enabled MEPs when you change a particular MEP, change the Service Type from Port to VLAN or vice versa, or change the domain's MD/MEG level.



CFM Mep Configuration

Auto-refresh off Refresh

									Alarm Control			State Control		Remote
Delete	Domain	Service	MEPID	Direction	Port	VLAN	PCP	SMAC	Level	Present	Absent	CCM	Admin	MEPID
Delete	Select Service		1	Down	1	1	0	00:00:00:00:00:00	2	2500	10000	☑	□	0

Add New Entry

Apply Reset

Parameter descriptions:

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

Add New Entry : Click to add a new MEP entry.

Domain : The name of Domain under which this MEP resides.

Service : The name of Service under which this MEP resides.

MEPID : The identification of this MEP. Must be an integer [1..8091]

Direction : Set whether this MEP is an Up-MEP or a Down-MEP.

Port : Port on which this MEP resides.

VLAN : VLAN ID. Use the value 0 to indicate untagged traffic (implies a port MEP).

PCP : Choose PCP value in PDUs' VLAN tag. Not used if untagged.

SMAC : Set a Source MAC address to be used in CCM PDUs originating at this MEP. Must be a unicast address. Format is XX:XX:XX:XX:XX:XX. If all-zeros, the switch port's MAC address will be used instead.

Alarm Control :

Level: If a defect is detected with a priority higher than this level, a fault alarm notification will be generated. The valid range is [1; 6] with 1 indicating that any defect will cause a fault alarm and 6 indicating that no defect can cause a fault alarm. See 802.1Q-2018, clause 20.9.5, *LowestAlarmPri*.
The possible defects and their priorities are:

Short name	Description	Priority
DefRDICCM	Remote Defect Indication	1
DefMACstatus	MAC Status	2
DefRemoteCCM	Remote CCM	3
DefErrorCCM	Error CCM Received	4
DefXconCCM	Cross Connect CCM Received	5

Present: The time in milliseconds that defects must be present before a fault alarm notification is issued. Default is 2500 ms.

Absent: The time in milliseconds that defects must be absent before a fault alarm notification is reset. Default is 10000 ms.

State Control :

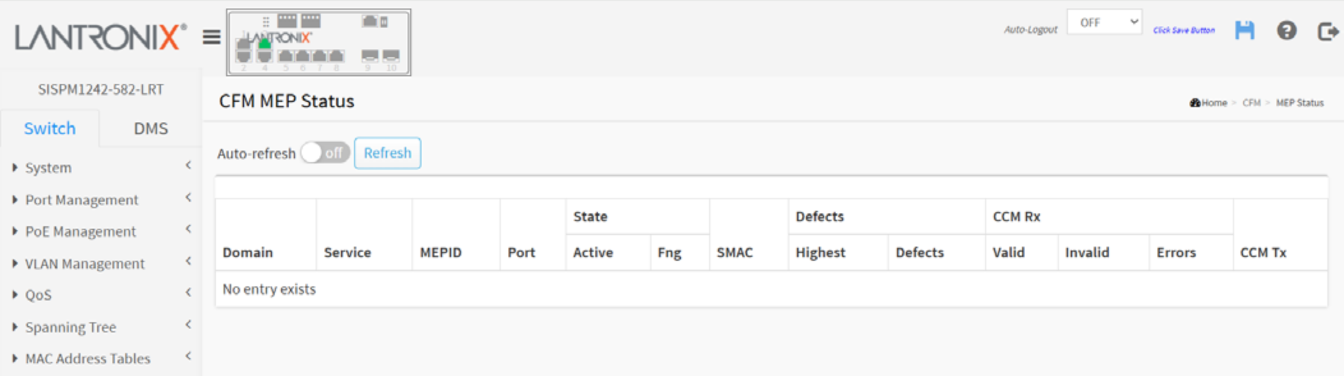
CCM: Enable or disable generation of continuity-check messages (CCMs)

Admin: Enable or disable this MEP. When this MEP is enabled, it will check received/missing CCMs and can raise defects.

Remote MEPID : Specify the Remote MEP that this MEP is expected to receive CCM PDUs from. Must be an integer [0..8091] where 0 means undefined. The value of Remote MEPID must be different from the value of MEPID.

MEP Status

This page displays CFM MEP (Maintenance association End Point) Status.



CFM MEP Status

				State			Defects		CCM Rx			
Domain	Service	MEPID	Port	Active	Fng	SMAC	Highest	Defects	Valid	Invalid	Errors	CCM Tx
No entry exists												

Parameter descriptions:

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

Domain : Name of Domain under which this MEP resides.

Service : Name of Service under which this MEP resides.

MEPID : The identification of this MEP.

Port : Port on which this MEP resides.

State Active : Operational state of the MEP.

- ***off*** : OFF indicates that the MEP Admin State is disabled.
- ***down*** : DOWN indicates the MEP Admin State is enabled, but an error state exists.
- ***up*** : UP indicates the MEP Admin State is enabled, and no errors and defects exist.

State Fng : The current state of the Fault Notification Generator state machine. Values will be one of these:

- ***reset*** No defect has been present since reset timer expired or State Machine was last reset.
- ***defect*** A defect is present, but not for a long enough time to be reported.
- ***reportDefect*** A transient state during which the defect is reported.
- ***defectReported*** A defect is present, and some defect has been reported.
- ***defectClearing*** No defect is present, but the ResetTime timer has not yet expired.

SMAC : This MEP's MAC address.

Defects Highest : The highest priority defect that has been present since the MEP's Fault Notification Generator state machine was last in the reset state.

Defects : A MEP can detect and report several defects, and multiple defects can be present at the same time. This is indicated the following letter code.

Code	Defect	Description
-	Defect not present	Defect not present.
R	someRDIdefect	RDI received from at least one remote MEP.
M	someMACstatusDefect	Received Port Status TLV != psUp or Interface Status TLV != isUp.
C	someRMEPCCMdefect	Valid CCM is not received within 3.5 times CCM interval from at least one remote MEP.
E	errorCCMdefect	Received CCM from an unknown remote MEP-ID or CCM interval mismatch.
X	xconCCMdefect	Received CCM with an MD/MEG level smaller than configured or wrong. MAID/MEGID (cross-connect).

CCM Rx : CCM PDUs received by this MEP.

Valid: Total number of CCMs that hit this MEP and passed the validation test.

Invalid: Total number of CCMs that hit this MEP and didn't pass the validation test.

Errors: Total number of out-of-sequence errors seen from RMEPs.

CCM Tx : Total number of CCM PDUs transmitted by this MEP.

16. APS

The APS (Automatic Protection Switching) module implements the protocol and linear protection switching mechanisms for point-to-point VLAN-based ETH SNC in Ethernet transport networks. APS is defined by the ITU-T G.8031 standard.

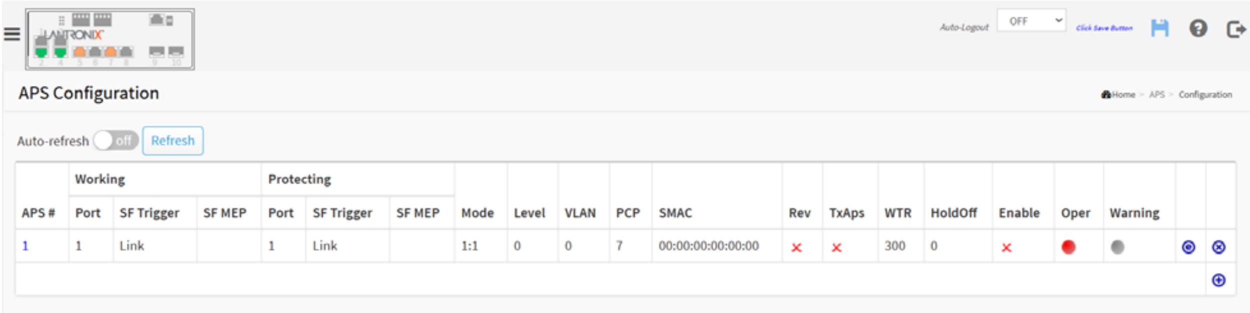
Point-to-point VLAN-based ETH SNCs (SubNetwork Connections) provide connectivity between two ETH flow points in an ETH flow domain. VLAN identifiers (VIDs) can be used to identify point-to-point VLAN-based ETH SNC(s) within ETH links. Additional details on ETH and related atomic functions can be obtained from ITU-T G.8021 and ITU-T G.8010. Other entities to be protected are for further study.

In the linear protection architecture defined in this version of the Recommendation, protection switching occurs at the two distinct endpoints of a point-to-point VLAN-based ETH SNC. Between these endpoints, there will be both "working" and "protection" transport entities.

Configuration

This page lets you create and configure up to 14 APS Instances.

1. Go to APS > Configuration. The APS Configuration page is displayed.

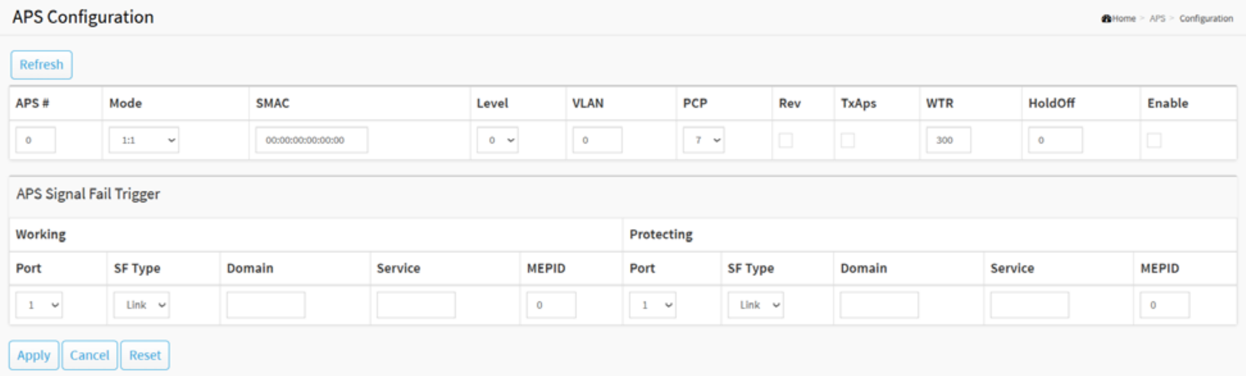


APS Configuration

Auto-refresh off

	Working			Protecting																
APS #	Port	SF Trigger	SF MEP	Port	SF Trigger	SF MEP	Mode	Level	VLAN	PCP	SMAC	Rev	TxAps	WTR	HoldOff	Enable	Oper	Warning		
1	1	Link		1	Link		1:1	0	0	7	00:00:00:00:00:00	✗	✗	300	0	✗	●	●	⊙	⊗
																				⊕

2. Click the plus symbol ⊕ to add an APS instance.



APS Configuration

APS #	Mode	SMAC	Level	VLAN	PCP	Rev	TxAps	WTR	HoldOff	Enable
0	1:1	00:00:00:00:00:00	0	0	7	□	□	300	0	□

APS Signal Fail Trigger

Working					Protecting				
Port	SF Type	Domain	Service	MEPID	Port	SF Type	Domain	Service	MEPID
1	Link			0	1	Link			0

3. Configure the APS settings.
4. Click **Apply**.

Parameter descriptions:

APS # : The ID of the APS. You can create a maximum of 14 APS instances. Click on the linked text to display the APS Instance page (see below), where you can reset counters and issue commands.

Port : The Port this flow is attached to.

SF Trigger : Selects whether Signal Fail (SF) comes from the link state of a given Port, or from a Down-MEP.

SF MEP : The *Domain::Service::MEPID* refers to a MEP instance which will represent the Working flow. Only used when SF Trigger is MEP. The selected MEP instance does not need to exist when this APS is configured.

Mode : The APS mode of operation:

- ***1:1*** : This will create a 1:1 APS. In the linear 1:1 protection switching architecture, the protection transport entity is dedicated to the working transport entity. However, normal traffic is transported either on the working transport entity or on the protection transport entity using a selector bridge at the source of the protected domain. The selector at the sink of the protected domain selects the entity which carries the normal traffic.
- ***1+1 Uni*** : This will create a 1+1 Unidirectional APS.
- ***1+1 Bi*** : This will create a 1+1 Bidirectional APS. In the linear 1+1 protection switching architecture, a protection transport entity is dedicated to each working transport entity. The normal traffic is copied and fed to both working and protection transport entities with a permanent bridge at the source of the protected domain. The traffic on working and protection transport entities is transmitted simultaneously to the sink of the protected domain, where a selection between the working and protection transport entities is made based on some predetermined criteria, such as server defect indication.

Level : The MD/MEG Level (0-7).

VLAN : The VLAN ID used in the L-APS PDUs. 0 means untagged.

PCP : PCP (priority) (default 7). The PCP value used in the VLAN tag unless the L-APS PDU is untagged. Must be a value in range 0 - 7.

SMAC : Source MAC address used in L-APS PDUs. Must be a unicast address. If all-zeros, the switch port's MAC address will be used.

Rev : When checked, the port recovery mode is ***revertive***, that is, traffic switches back to the working port after the condition(s) causing a switch has cleared. In the case of clearing a command (e.g. forced switch), this happens immediately. In the case of clearing of a defect, this generally happens after the expiry of the WTR (Wait-To-Restore) timer.

When unchecked, the port recovery mode is ***non-revertive*** and traffic is allowed to remain on the protect port after a switch reason has cleared.

TxAps : Choose whether this end transmits APS PDUs. Only used for 1+1, unidirectional.

WTR : When Rev is checked, WTR (Wait-To-Restore) sets how many seconds to wait before restoring to the working port after a fault condition has cleared. The valid range 1 – 720 seconds.

HoldOff : When a new (or more severe) defect occurs, the hold-off timer will be started, and the event will be reported after the timer expires. HoldOff time is measured in milliseconds, and valid values are 0 – 10000 ms. The default is 0, which means immediate reporting of the defect.

Enable : The administrative state of this APS instance. Check to make it function normally and uncheck to make it cease functioning.

Oper : This field cannot be configured but shows the operational state. You can click on the link in the APS # field to get more details on the status (see below).

🟢 APS instance is functional.

🔴 APS instance is not functional.

Warning : If the operational state is Active, the APS instance is indeed active, but it may be that it doesn't run as the administrator thinks, because of configuration errors, which are reflected in the warnings below.

● No warnings

🟡 Warning. Use the tooltip to get detailed warning information.

APS Signal Fail Trigger

Working: The Working port configuration.

Working Port: Assign an interface to the working port.

Working SF Type: Choose whether the working port's interface link state or a MEP installed on working's interface is used as signal-fail trigger.

- ***link***: Working interface link state is used as signal-fail trigger.
- ***mep***: A MEP installed on working interface is used as signal-fail trigger.

Working Domain: The MEP's domain name.

Working Service: The MEP's service name within the domain.

Working MEPID: The MEP's MEP-ID.

Protecting: The Protect port configuration.

Protecting Port: Assign an interface to the Protect port.

Protecting SF Type: Choose whether the protect port's interface link state or a MEP installed on protect's interface is used as signal-fail trigger.

- ***link***: protect interface link state is used as signal-fail trigger.
- ***mep***: A MEP installed on protect interface is used as signal-fail trigger.

Protecting Domain: The MEP's domain name.

Protecting Service: The MEP's service name within the domain.

Protecting MEPID: The MEP's MEP-ID.

Configuration Buttons : You can modify each APS in the table using these buttons:

ⓔ **Edit**: Edit the APS instance.

⊗ **Delete**: Delete the APS instance.

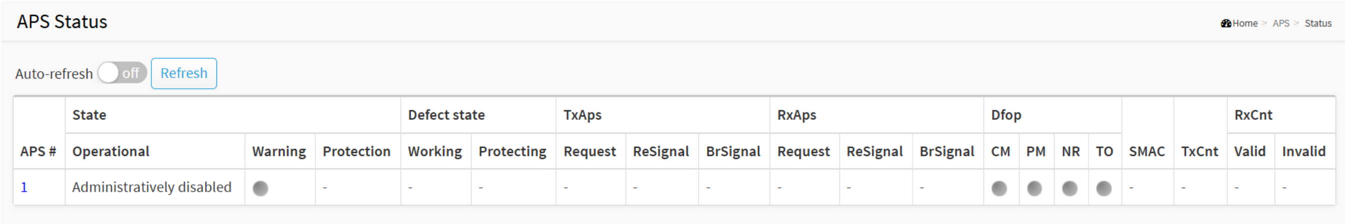
⊕ **Add**: Add new APS instance.

APS Instance Status page

When you click on the linked text in the APS # column the APS Instance Status page displays, where you can reset counters and issue commands. See APS Instance Status.

Status

Go to APS > Status to view the APS Status page:



APS Status

	State			Defect state		TxAps			RxAps			Dfop						RxCnt	
APS #	Operational	Warning	Protection	Working	Protecting	Request	ReSignal	BrSignal	Request	ReSignal	BrSignal	CM	PM	NR	TO	SMAC	TxCnt	Valid	Invalid
1	Administratively disabled	●	-	-	-	-	-	-	-	-	-	●	●	●	●	-	-	-	-

Parameter descriptions:

APS # : The ID of the APS. Click on the linked text to view the APS Instance (APS status) page where you can reset counters and issue commands.

State, Operational : The operational state of the APS instance. There are many ways to not have the instance active. Each of them has its own value. Only when the state is Active, will the APS instance be active and up and running. If the Operational state is not "Active", the remaining fields are invalid. The possible values of this field are shown below:

- ***Administratively disabled***: Instance is inactive because it is administratively disabled.
- ***Active***: The instance is active and up and running.
- ***Internal Error***: Instance is inactive because an internal error has occurred.
- ***Working MEP not Found***: Instance is inactive, because the Working MEP is not found.
- ***Protecting MEP not Found***: Instance is inactive, because the Protecting MEP is not found.
- ***Working MEP is not administrative active***: Instance is inactive, because the Working MEP is not admin enabled.
- ***Protecting MEP is not administrative active***: Instance is inactive, because the Protecting MEP is not admin enabled.
- ***Working MEP is not a Down MEP***: Instance is inactive, because the Working MEP is not a Down-MEP.
- ***Protecting MEP is not a Down MEP***: Instance is inactive, because the Protecting MEP is not a Down-MEP.
- ***Working and Protecting MEP use the same interface***: Instance is inactive, because both Working and Protecting MEPs use the same I/F.
- ***Another instance uses the same Working port***: Instance is inactive, because another instance uses the same Working port.

State, Warning : If the operational state is Active, the APS instance is indeed active, but it may be that it doesn't run as the administrator thinks, because of configuration errors, which are reflected in the warnings below.

The Warning information is indicated by down: no warning, down: warning. Use the tooltip to get the detailed warning information.

State, Protection : The possible protection group states. The letters refer to the state noted in G.8031 Annex:

- No request Working: **A**.
- No request Protecting: **B**.
- Lockout: **C**.
- Forced Switch: **D**.
- Signal fail Working: **E**.
- Signal fail Protecting: **F**.
- Manual switch to Protecting: **G**.

- Manual switch to Working: **H**.
- Wait to restore: **I**.
- Do not revert: **J**.
- Exercise Working: **K**.
- Exercise Protecting: **L**.
- Reverse request Working: **M**.
- Reverse request Protecting: **N**.
- Signal degrade Working: **P**.
- Signal degrade Protecting: **Q**.

Defect state, Working, Protection : The possible values of this field are shown below:

- ***ok***: The port defect state is OK
- ***sd***: The port defect state is Signal Degrade
- ***sf***: The port defect state is Signal Fail

TxAps, RxAps – Request : The possible transmitted or received APS request according to G.8031.

- ***nr***: No Request.
- ***dnr***: Do Not Revert.
- ***rr***: Reverse Request.
- ***exer***: Exercise.
- ***wtr***: Wait-To-Restore.
- ***ms***: Manual Switch.
- ***sd***: Signal Degrade.
- ***sfW***: Signal Fail for Working.
- ***fs***: Forced Switch.
- ***sfP***: Signal Fail for Protect.
- ***lo***: Lockout.

TxAps, ReSignal : Transmitted requested signal according to G.8031.

TxAps, BrSignal : Transmitted bridged signal according to G.8031.

RxAps, ReSignal : Received requested signal according to G.8031.

RxAps, BrSignal : Received bridged signal according to G.8031.

Dfop : The "Failure of Protocol defect" and presence of a defect is indicated by up: no defect, down: defect.

- ***CM***: Configuration Mismatch (received APS PDU on working interface within last 17.5 seconds).
- ***PM*** : Provisioning Mismatch (far and near ends are not using the same mode; bidir only).
- ***NR*** : No Response (far end hasn't agreed on 'Requested Signal' within 50 ms; bidir only).
- ***TO*** : Time Out (near end hasn't received a valid APS PDU within last 17.5 seconds; bidir only).

SMAC : Source MAC address of last received APS PDU or all-zeros if no PDU has been received.

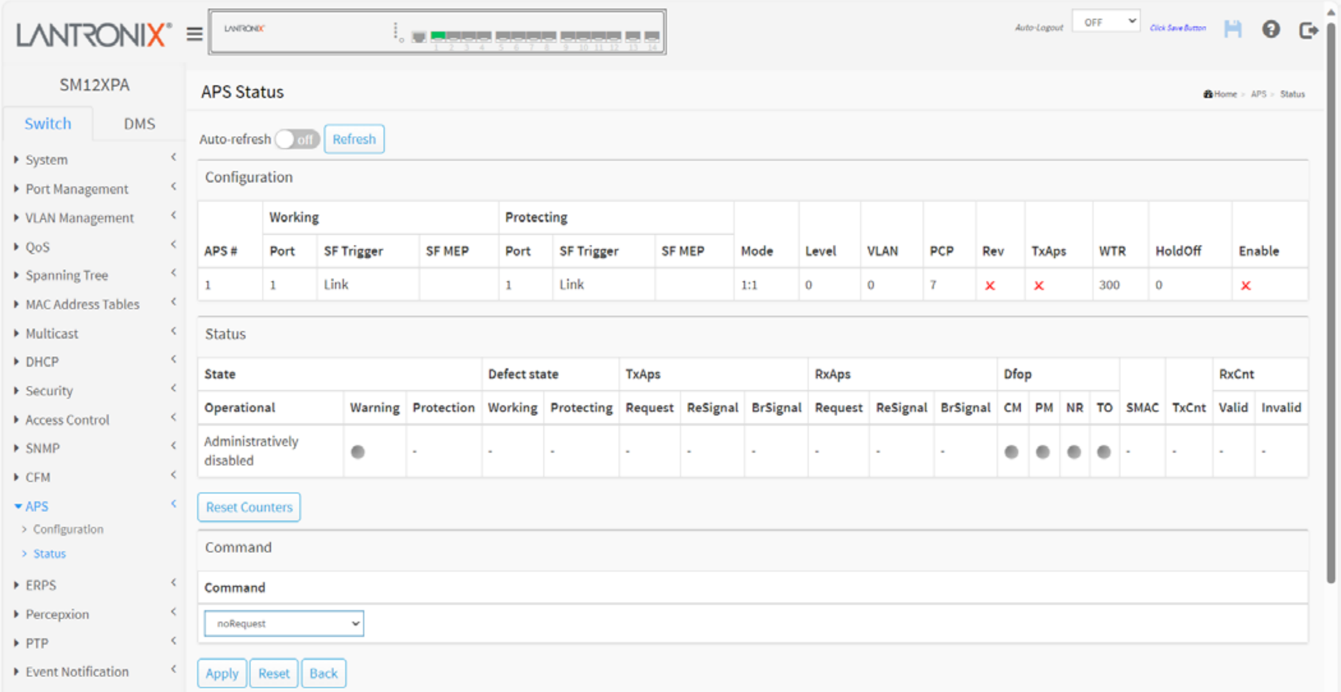
TxCnt : Number of APS PDU frames transmitted.

RxCnt, Valid : Number of valid APS PDU frames received on the protect port.

RxCnt, Invalid : Number of invalid APS PDU frames received on the protect port.

APS Instance Status

At APS > Status, click on the linked text of the APS instance to get to APS status page where you can reset counters and issue commands.



APS Status

Auto-refresh off Refresh

Configuration

	Working			Protecting											
APS #	Port	SF Trigger	SF MEP	Port	SF Trigger	SF MEP	Mode	Level	VLAN	PCP	Rev	TxAps	WTR	HoldOff	Enable
1	1	Link		1	Link		1:1	0	0	7	✗	✗	300	0	✗

Status

State			Defect state		TxAps			RxAps			Dfop						RxCnt	
Operational	Warning	Protection	Working	Protecting	Request	ReSignal	BrSignal	Request	ReSignal	BrSignal	CM	PM	NR	TO	SMAC	TxCnt	Valid	Invalid
Administratively disabled	●	-	-	-	-	-	-	-	-	-	●	●	●	●	-	-	-	-

Reset Counters

Command

Command
noRequest

Apply Reset Back

Parameter descriptions (not previously described in the APS configuration section)

Reset Counters button: Click to reset counters for this APS instance.

Commands:

- **noRequest**: There is no active local command on this instance. Issuing this command has no effect.
- **clear**: Clear a switchover, exercise request and a WTR condition.
- **forceswitch**: Causes a switchover to protect if no lockout is in effect.
- **manualSwitchToProtecting**: Causes a manual signal switchover from the working path to the protection path whether the working path signal is active or not.
- **manualSwitchToWorking**: Causes a manual signal switchover from the protection path to the working path if the protection path signal has not failed.
- **exercise**: Exercise the APS instance. Use clear command to clear the request.
- **freeze**: Freezes the state of the APS instance. While in this mode, additional near-end commands, condition changes, and received APS information are ignored. Use command "freezeClear" to get out of this mode.
- **freezeClear**: Use this command to get out of the freeze mode.
- **lockout**: Lockout APS instance of protection. Use command "clear" to clear the request.

17. ERPS

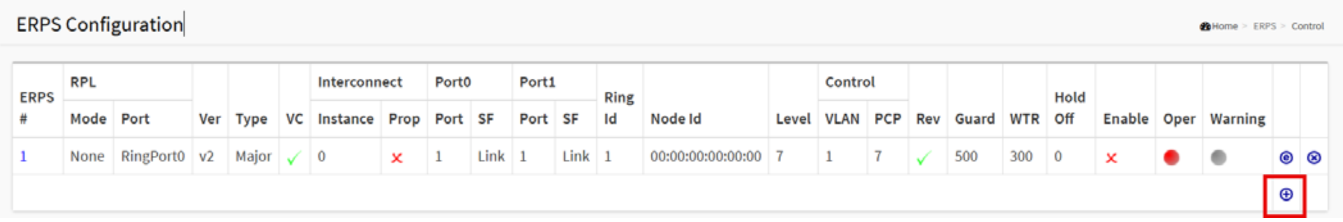
This page lets you view and configure Ethernet Ring Protection Switching (ERPS) instances.

The switch supports ERPS, defined in ITU/T G.8032. It provides fast protection and recovery switching for Ethernet traffic in a ring topology while also ensuring that the Ethernet layer remains loop-free.

Control

To configure an ERPS instance in the Web UI:

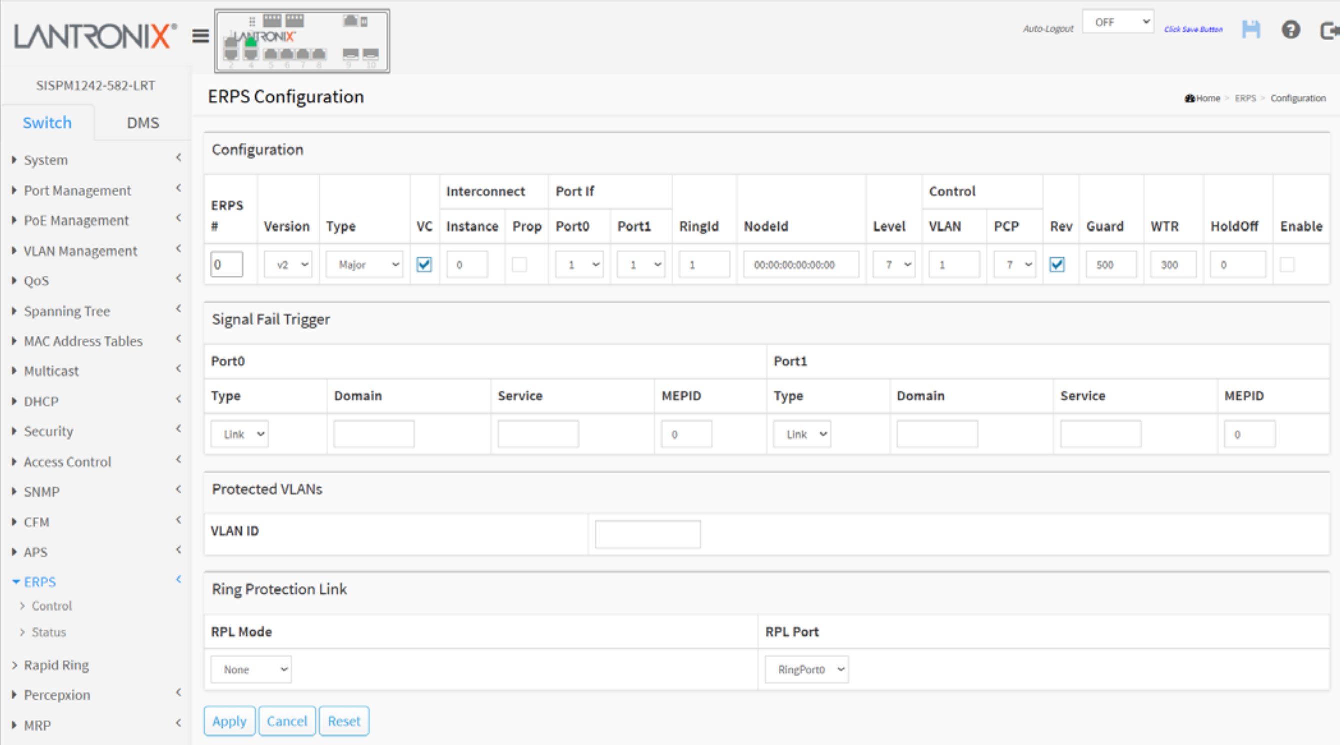
1. Go to ERPS > Control.



ERPS Configuration

ERPS	RPL					Interconnect		Port0		Port1		Ring			Control					Hold					
#	Mode	Port	Ver	Type	VC	Instance	Prop	Port	SF	Port	SF	Id	Node Id	Level	VLAN	PCP	Rev	Guard	WTR	Off	Enable	Oper	Warning		
1	None	RingPort0	v2	Major	✓	0	✗	1	Link	1	Link	1	00:00:00:00:00:00	7	1	7	✓	500	300	0	✗	●	●	⊙	⊗
																								⊕	

2. Click the plus sign (⊕) to add an ERPS instance.



ERPS Configuration

Configuration

ERPS				Interconnect		Port If					Control						
#	Version	Type	VC	Instance	Prop	Port0	Port1	RingId	NodeId	Level	VLAN	PCP	Rev	Guard	WTR	HoldOff	Enable
0	v2	Major	☑	0	□	1	1	1	00:00:00:00:00:00	7	1	7	☑	500	300	0	□

Signal Fail Trigger

Port0				Port1			
Type	Domain	Service	MEPID	Type	Domain	Service	MEPID
Link			0	Link			0

Protected VLANs

VLAN ID	

Ring Protection Link

RPL Mode	RPL Port
None	RingPort0

Apply Cancel Reset

3. Configure the settings. Refer to the parameter descriptions below.
4. Click **Apply** to save the configuration.

Parameter descriptions:

Configuration

ERPS # : The ID of ERPS. Valid range 1 - 64. Click on the linked text to display the APS Instance page (see below), where you can reset counters and issue commands.

Version : ERPS protocol version. v1 and v2 are supported.

Type : Type of ring. Possible values:

- ***Major*** : ERPS major ring (G.8001-2016, clause 3.2.39).
- ***Sub*** : ERPS sub-ring (G.8001-2016, clause 3.2.66).
- ***InterSub*** : ERPS sub-ring on an interconnection node (G.8001-2016, clause 3.2.66).

VC : Controls whether to use a Virtual Channel with a sub-ring.

Interconnect Instance : For a sub-ring on an interconnection node, this must reference the instance ID of the ring to which this sub-ring is connected.

Interconnect Prop : Controls whether the ring referenced by Interconnect Instance will propagate R-APS flush PDUs whenever this sub-ring's topology changes.

Ring Id : The Ring ID is used, along with the control VLAN, to identify R-APS PDUs as belonging to a particular ring.

Node Id : The Node ID is used inside the R-APS specific PDU to uniquely identify this node (switch) on the ring.

Level : MD/MEG Level of R-APS PDUs we transmit.

Control VLAN : The VLAN on which R-APS PDUs are transmitted and received on the ring ports.

Control PCP : The PCP value used in the VLAN tag of the R-APS PDUs.

Rev : Revertive (true) or Non-revertive (false) mode.

Guard : Guard time in ms. Valid range is 10 - 2000 ms.

WTR : Wait-to-Restore time in seconds. Valid range 1 - 720 sec.

Hold Off : Hold off time in ms. Value is rounded down to 100ms precision. The valid range is 0 - 10000 ms.

Enable : The administrative state of this APS ERPS. Check to make it function normally and uncheck to make it cease functioning.

Signal Fail Trigger

Type: Selects whether Signal Fail (SF) comes from the link state of a given interface, or from a Down-MEP.

Domain, Service, MEPID: Identification of the MEP instance to provide Signal Fail, if Type is MEP.

Protected VLANs

VLANs which are protected by this ring instance. At least one VLAN must be protected. Specify as a comma separated list of vlan numbers or vlan ranges. Ex.: 1,4,7,30-70

Ring Protection Link

RPL Mode : The Ring Protection Link mode. Possible values are:

- ***None*** : There is no link.
- ***Owner*** : The Ring Protection Link mode is “Owner”.
- ***Neighbor*** : The Ring Protection Link mode is “Neighbor”.

RPL Port : Indicates whether it is port0 or port1 that is the Ring Protection Link. Not used if RPL Mode is None.

Port0/Port1 SF : Select whether Signal Fail (SF) comes from the link state of a given interface, or from a Down-MEP. Possible values:

- ***MEP***: Down-MEP

- ***Link***: Link

After an instance has been created, the following additional fields are displayed on the ERPS Control page.

Oper : The operational state of the ERPS instance.

🟢 Active

🔴 Disabled or Internal error.

Warning : Operational warnings for the ERPS instance. If the operational state is Active, the instance is indeed active, but it may be that it doesn't run as the administrator thinks, because of configuration errors, which are reflected in the warnings below.

● No warnings

🟡 Warning. Use the tooltip to get detailed warning information.

Configuration Buttons :

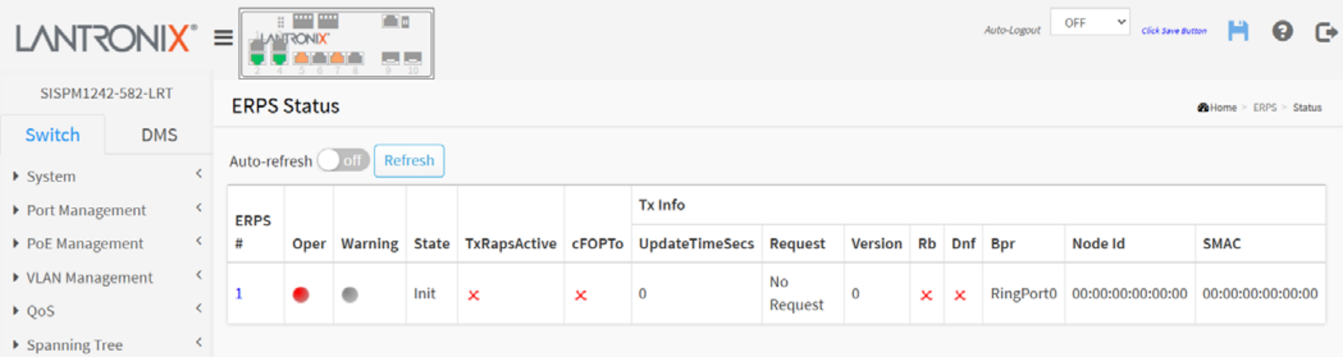
ⓔ **Edit**: Edits the ERPS row.

⊗ **Delete**: Deletes the ERPS.

⊕ **Add**: Adds new ERPS.

Status

1. Go to ERPS > Status to view the ERPS Status page.
2. **Auto-refresh** will refresh the page every 3 seconds. **Refresh** will refresh the page immediately.



ERPS Status

Auto-refresh off Refresh

ERPS #	Oper	Warning	State	TxRapsActive	cFOPTo	Tx Info							
						UpdateTimeSecs	Request	Version	Rb	Dnf	Bpr	Node Id	SMAC
1	●	●	Init	✗	✗	0	No Request	0	✗	✗	RingPort0	00:00:00:00:00:00	00:00:00:00:00:00

Parameter descriptions:

ERPS # : The ID of the ERPS. Click on the linked text to display the ERPS detailed instance page, where you can reset counters and issue commands (see below).

Oper : The operational state of ERPS instance.

● • Active

● • Disabled or Internal error.

Warning : Operational warnings of ERPS instance.

● • No warnings

● • Warning. Use the tooltip to get detailed warning information.

State : Specifies protection/node state of ERPS.

TxRapsActive : Specifies whether the switch is to be transmitting R-APS PDUs on its ring ports.

cFOPTo : Failure of Protocol - R-APS Rx Time Out.

UpdateTimeSecs : Time in seconds since boot that this structure was last updated.

Request : Request/state

Version : Version of received/used R-APS Protocol. 0 means v1, 1 means v2, etc.

Rb : RB (RPL blocked) bit of R-APS info.

Dnf : DNF (Do Not Flush) bit of R-APS info.

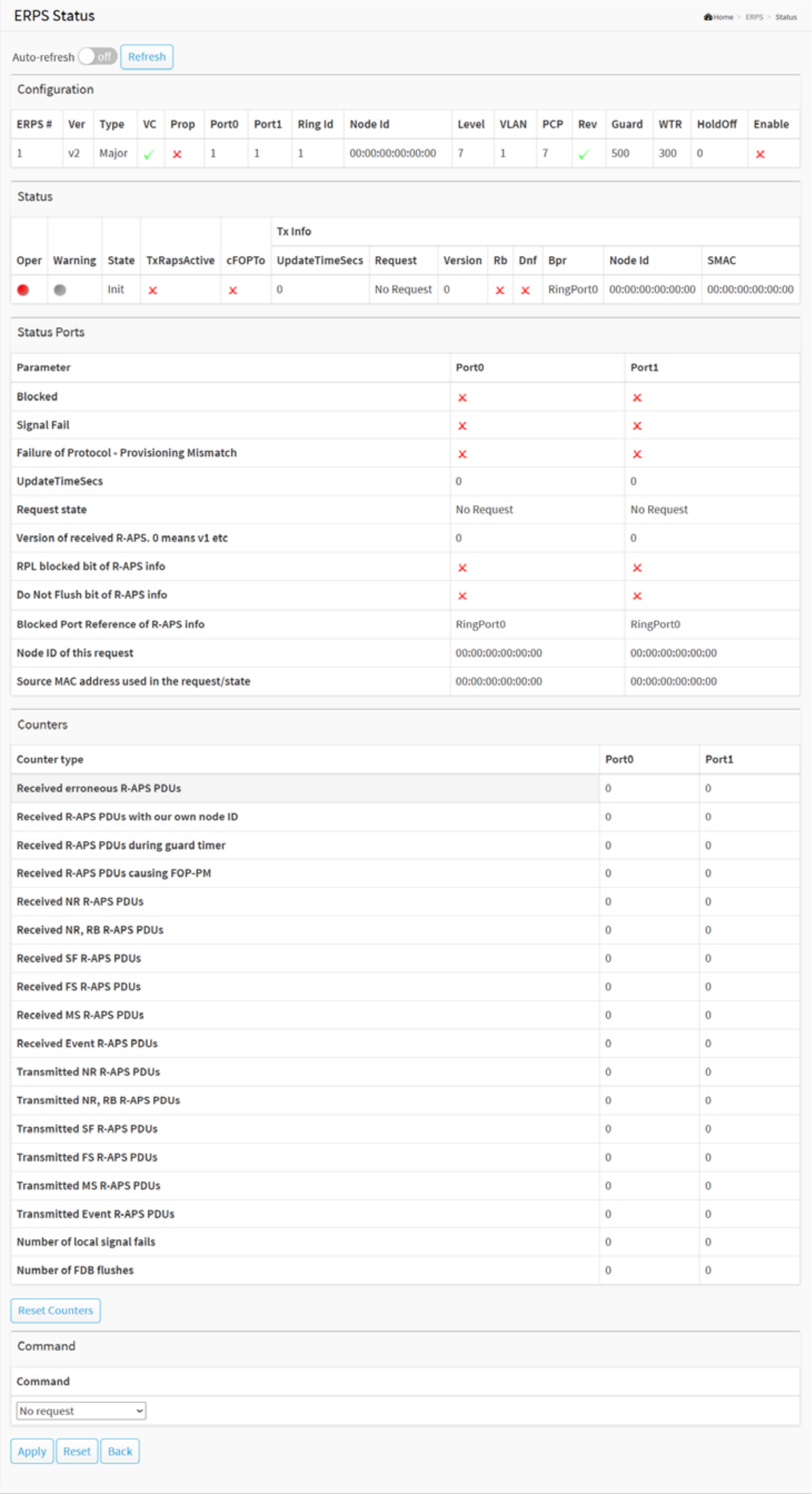
Bpr : BPR (Blocked Port Reference) of R-APS info.

Node Id : The Node ID of this request.

SMAC : The Source MAC address used in the request/state.

ERPS Instance Status

At the ERPS Status page, click on the linked text of the ERPS instance to get to ERPS status page where you can reset counters and issue commands (shown below).



ERPS Status

Configuration

ERPS #	Ver	Type	VC	Prop	Port0	Port1	Ring Id	Node Id	Level	VLAN	PCP	Rev	Guard	WTR	HoldOff	Enable
1	v2	Major	✓	✗	1	1	1	00:00:00:00:00:00	7	1	7	✓	500	300	0	✗

Status

					Tx Info							
Oper	Warning	State	TxRapsActive	cFOPTo	UpdateTimeSecs	Request	Version	Rb	Dnf	Bpr	Node Id	SMAC
●	●	Init	✗	✗	0	No Request	0	✗	✗	RingPort0	00:00:00:00:00:00	00:00:00:00:00:00

Status Ports

Parameter	Port0	Port1
Blocked	✗	✗
Signal Fail	✗	✗
Failure of Protocol - Provisioning Mismatch	✗	✗
UpdateTimeSecs	0	0
Request state	No Request	No Request
Version of received R-APS. 0 means v1 etc	0	0
RPL blocked bit of R-APS info	✗	✗
Do Not Flush bit of R-APS info	✗	✗
Blocked Port Reference of R-APS info	RingPort0	RingPort0
Node ID of this request	00:00:00:00:00:00	00:00:00:00:00:00
Source MAC address used in the request/state	00:00:00:00:00:00	00:00:00:00:00:00

Counters

Counter type	Port0	Port1
Received erroneous R-APS PDUs	0	0
Received R-APS PDUs with our own node ID	0	0
Received R-APS PDUs during guard timer	0	0
Received R-APS PDUs causing FOP-PM	0	0
Received NR R-APS PDUs	0	0
Received NR, RB R-APS PDUs	0	0
Received SF R-APS PDUs	0	0
Received FS R-APS PDUs	0	0
Received MS R-APS PDUs	0	0
Received Event R-APS PDUs	0	0
Transmitted NR R-APS PDUs	0	0
Transmitted NR, RB R-APS PDUs	0	0
Transmitted SF R-APS PDUs	0	0
Transmitted FS R-APS PDUs	0	0
Transmitted MS R-APS PDUs	0	0
Transmitted Event R-APS PDUs	0	0
Number of local signal fails	0	0
Number of FDB flushes	0	0

Command

Command
No request

Parameter descriptions

Configuration

This table shows the current configuration for this ERPS instance. Go to the ERPS Configuration help page for further explanation.

Status

This shows the status of the ERPS instance. Go to the ERPS Status help page for further explanation.

Status Ports

This shows the status of the ERPS instance. Go to the ERPS Status help page for further explanation.

Counters

This section shows several counters useful for debug purpose. The Counter type column indicate the counted frame attribute.

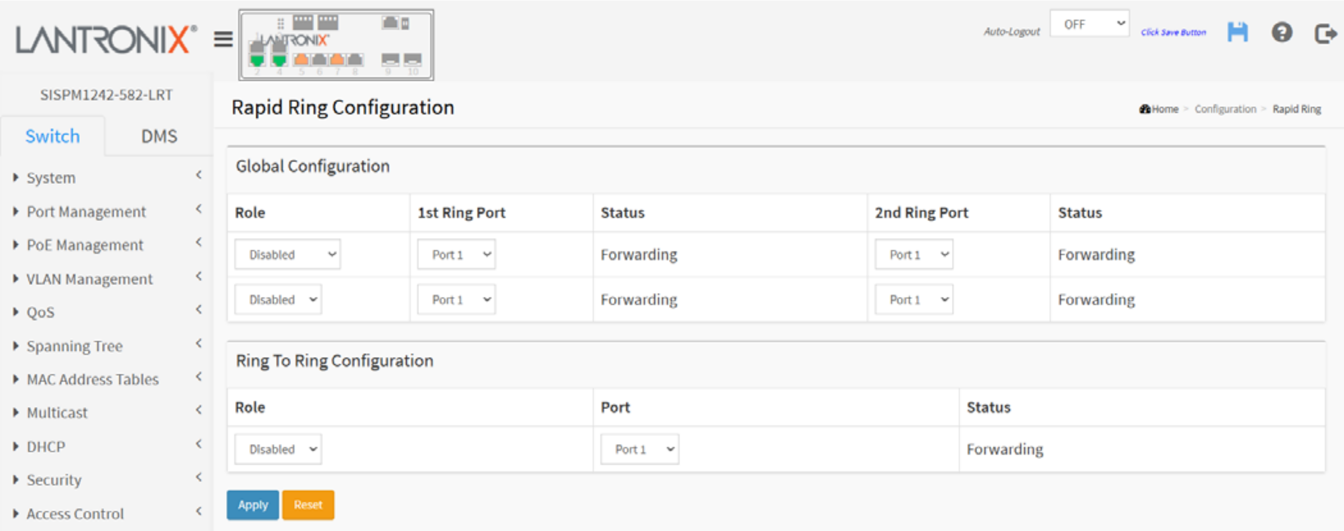
Reset Counters button: Click to reset counters for this APS instance.

ERPS Commands:

- **No request:** There is no active local command on this instance. Issuing this command has no effect.
- **Clear:** Clear a switchover (FS or MS) request and a WTB/WTR condition and force reversion even if not revertive.
- **Force switch to Port0:** Causes a forced switchover. Blocks port1 and unblocks port0.
- **Force switch to Port1:** Causes a forced switchover. Blocks port0 and unblocks port1.
- **Manual switch to Port0:** Causes a switchover if the signal is good and no forced switch is in effect. Blocks port1 and unblocks port0.
- **Manual switch to Port1:** Causes a switchover if the signal is good and no forced switch is in effect. Blocks port0 and unblocks port1.

18. Rapid Ring

This page lets you view and set current Rapid Ring parameters. **Note** that other Ring technologies (e.g., STP, MRP) must be disabled. 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. Rapid Ring recovery time can be less than 20ms on up to 250 switches (much lower recovery time than other redundancy protocols).



Rapid Ring Configuration

Global Configuration

Role	1st Ring Port	Status	2nd Ring Port	Status
Disabled	Port 1	Forwarding	Port 1	Forwarding
Disabled	Port 1	Forwarding	Port 1	Forwarding

Ring To Ring Configuration

Role	Port	Status
Disabled	Port 1	Forwarding

Global Configuration

Index: Displays the Rapid Ring Instance number (1-4).

Role: Set the Rapid Ring role value (Disabled, Master, or Member).

Port: The switch port number of the port (e.g., 1-4).

Status: The current Rapid Ring status of the port (e.g., Forwarding, Discarding).

Message:

Rapid Ring Configuration Error   Error in port 25, STP is enabled

19. MRP

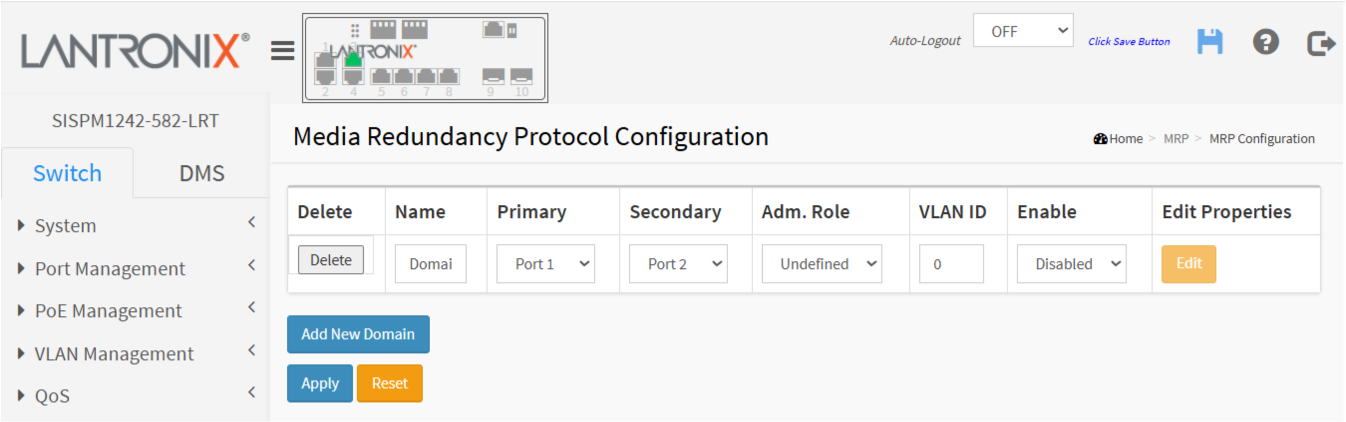
Media Redundancy Protocol (MRP) is a data networking protocol that provides fast fault recovery in a ring topology, commonly used in industrial automation networks. MRP is standardized as IEC 62439-2.

For more information about MRP configuration and application examples, see MRP Pre-Requisites and Application Examples.

MRP Configuration

To configure an MRP domain:

1. Go to MRP > Configuration.
2. Click **Add New Domain**.
3. Configure the settings.
4. Click **Apply** to save the configuration.



Media Redundancy Protocol Configuration

Delete	Name	Primary	Secondary	Adm. Role	VLAN ID	Enable	Edit Properties
Delete	Domai	Port 1	Port 2	Undefined	0	Disabled	Edit

Parameter Descriptions

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

Add New Domain: Click to add a new domain row.

Name: A logical name for the MRP domain to ease 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).

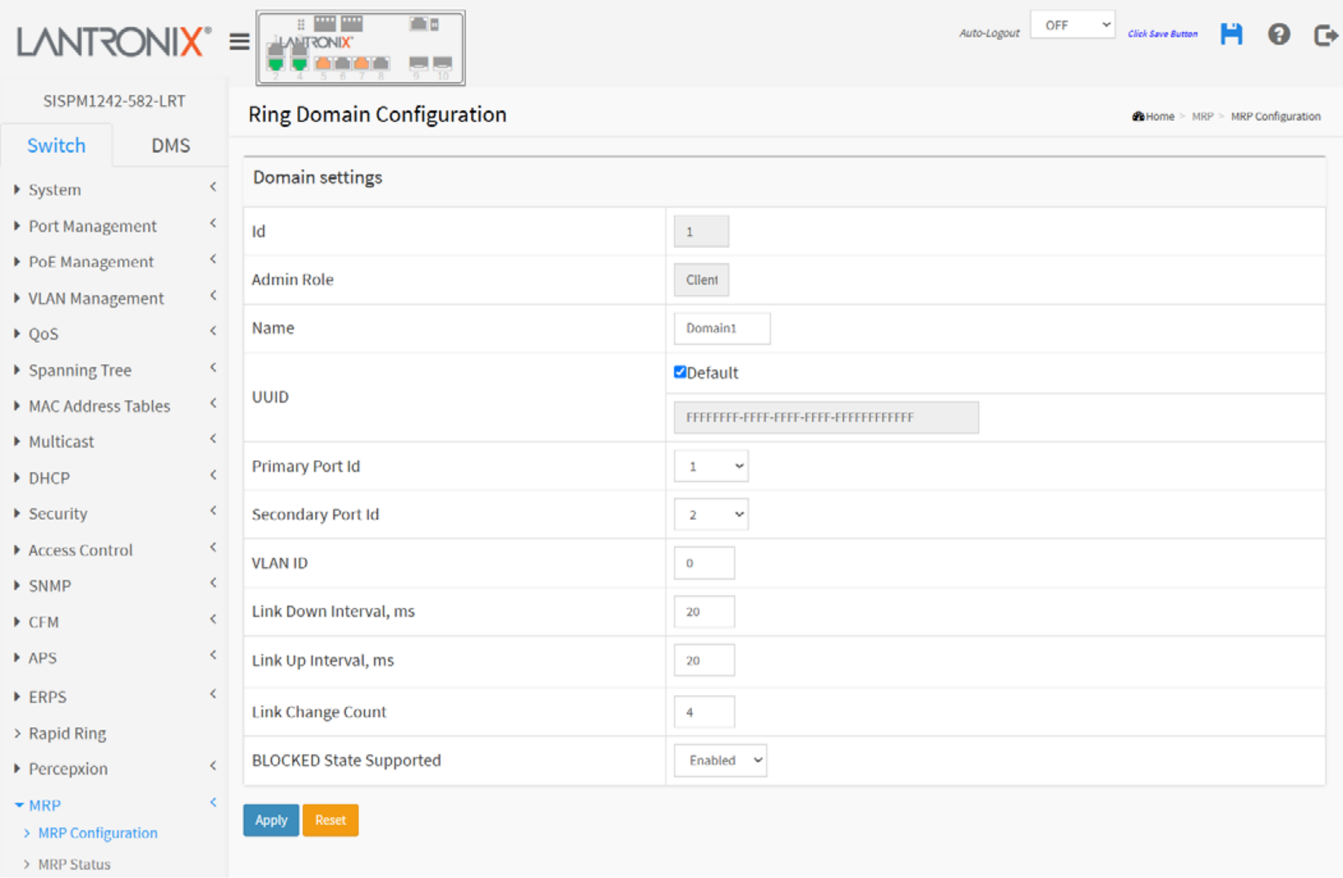
VLAN ID: The VLAN ID assigned to the MRP protocol. The allowed range is **0** to **4094**.

Enable: Enable/Disable MRP protocol.

Edit properties: Click to edit domain properties.

Edit MRP domain properties:

On the MRP configuration page, click **Edit** to edit the domain configuration.



Ring Domain Configuration

Domain settings

Id	1
Admin Role	Client
Name	Domain1
UUID	☑Default FFFFFFFF-FFFF-FFFF-FFFF-FFFFFFFFFFFF
Primary Port Id	1
Secondary Port Id	2
VLAN ID	0
Link Down Interval, ms	20
Link Up Interval, ms	20
Link Change Count	4
BLOCKED State Supported	Enabled

Parameter Descriptions:

ID: the index of the entry

Admin 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).

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: This parameter selects whether monitoring of MRM state is enabled or disabled.

Only MRM.

Topology Change Interval, ms: This parameter 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.

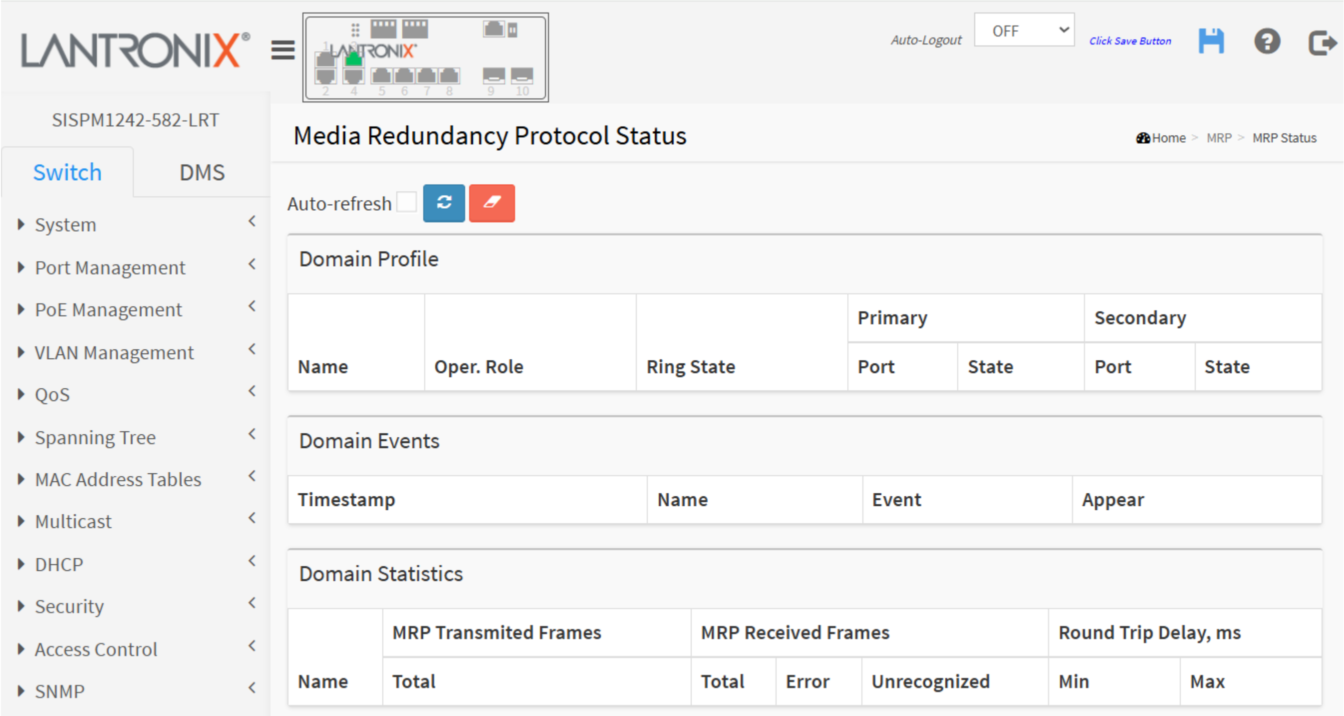
BLOCKED State Supported: This parameter specifies whether the MRC supports BLOCKED state at its ring ports or not.

Only MRC.

MRP Status

To view MRP status:

1. Go to MRP > MRP Status.



Auto-Logout: OFF

Media Redundancy Protocol Status

Auto-refresh □

Domain Profile

			Primary		Secondary	
Name	Oper. Role	Ring State	Port	State	Port	State

Domain Events

Timestamp	Name	Event	Appear

Domain Statistics

	MRP Transmited Frames	MRP Received Frames			Round Trip Delay, ms	
Name	Total	Total	Error	Unrecognized	Min	Max

Parameter Descriptions

Domain Profile

Name: A logical name for the MRP domain to easy the management of MRP domains.

Oper. Role: The operational role of an MRP entity per domain.

Ring State: Ring status of the MRP entity.

Primary: The ifIndex of the layer 2 interface which is used as ring port 1.

Secondary: The ifIndex of the layer 2 interface which is used as ring port 2.

Domain Events

Timestamp: The value of sysUpTime at the time of the logged event.

Name: A logical name for the MRP domain.

Event: Event type.

Appear: Event appear or disappear.

Domain Statistics

Name: logical name for the domain

MRP Transmitted Frames: The total transmitted frames.

MRP Received Frames: The total received frames.

Round Trip Delay (ms): Round-Trip-Delay (in milliseconds) which was measured since startup. Minimum and maximum values.

20. PTP

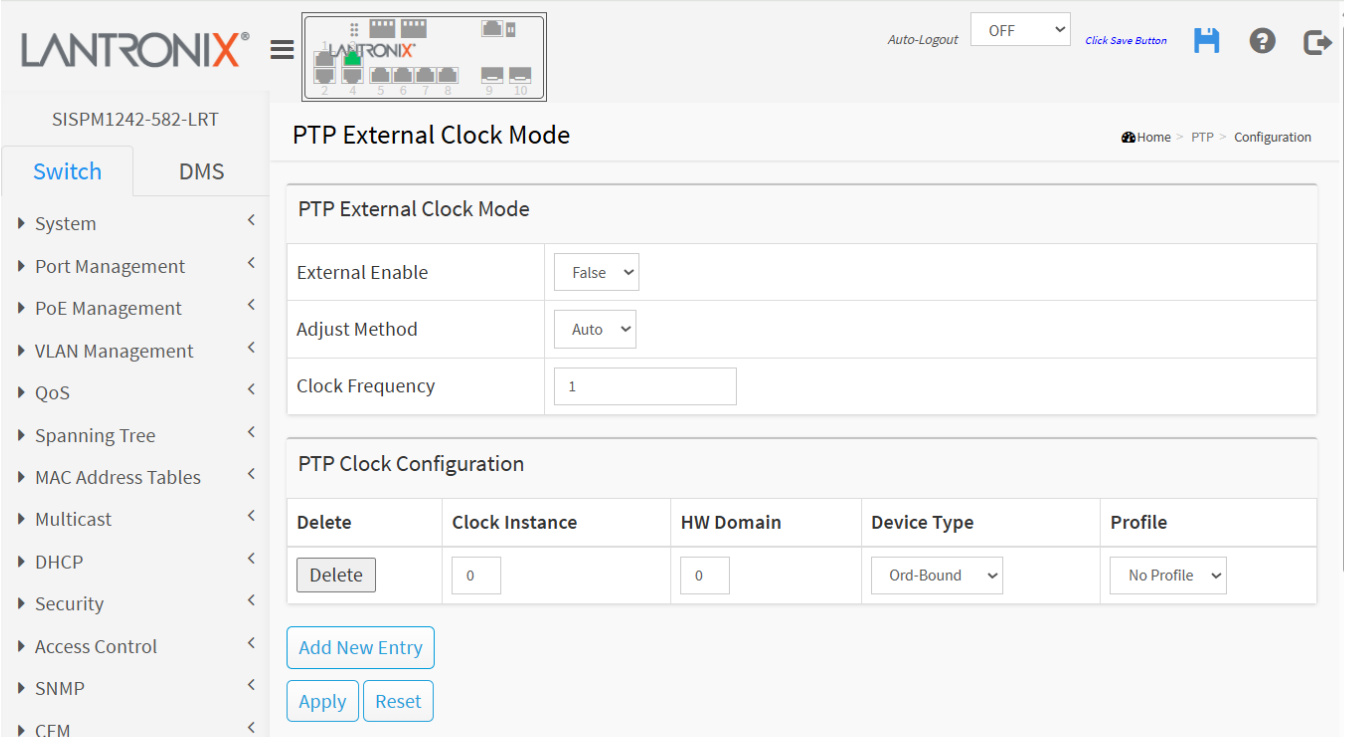
The Precision Time Protocol (PTP) is a protocol used to synchronize clocks throughout a computer network. On a local area network, it achieves clock accuracy in the sub-microsecond range, making it suitable for measurement and control systems.

Configuration

This page lets you set and view current PTP parameters. The switch lets you configure up to four PTP instances.

To configure a PTP instance in the web UI:

1. Go to PTP > Configuration. The PTP External Clock Mode page is displayed.
2. Set the PTP External Clock Mode parameters.
3. Click the **Add New Entry** button to create a new clock instance.
4. Configure the PTP clock settings.
5. Click the **Apply** button to save the settings.



PTP External Clock Mode

PTP External Clock Mode

External Enable	False
Adjust Method	Auto
Clock Frequency	1

PTP Clock Configuration

Delete	Clock Instance	HW Domain	Device Type	Profile
Delete	0	0	Ord-Bound	No Profile

Parameter descriptions:

PTP External Clock Mode

External Enable : This selection box lets you configure External Clock output.

- ***True*** : Enable the external clock output.
- ***False*** : Disable the external clock output (default).

Adjust Method : This selection box lets you configure the Frequency adjustment configuration as follows:

- ***LTC*** : Select Local Time Counter (LTC) frequency control.
- ***Independent*** : Select an oscillator independent of SyncE for frequency control, if supported by the HW
- ***Auto*** : Automatically select a clock control, based on PTP profile and available HW resources (default).

Clock Frequency : This lets you set the Clock Frequency in the range 1 – 25000000 Hz (1 - 25MHz).

PTP Clock Configuration

Add New Entry : Click to add a new clock instance.

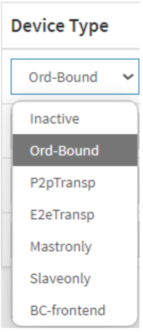
Delete : Check this box and click on **Apply** to delete the clock instance.

Clock Instance : Indicates the instance number of a particular Clock Instance [0..3]. Click on the Clock Instance number to inspect and edit the Clock details.

HW Domain : Indicates the HW clock domain used by the clock.

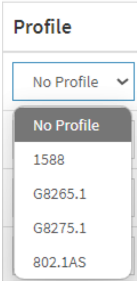
Device Type : Indicates the Type of the Clock Instance. There are five Device Type selections:

- ***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.
- ***BC-frontend*** - clock's Device Type is Boundary Clock front end.

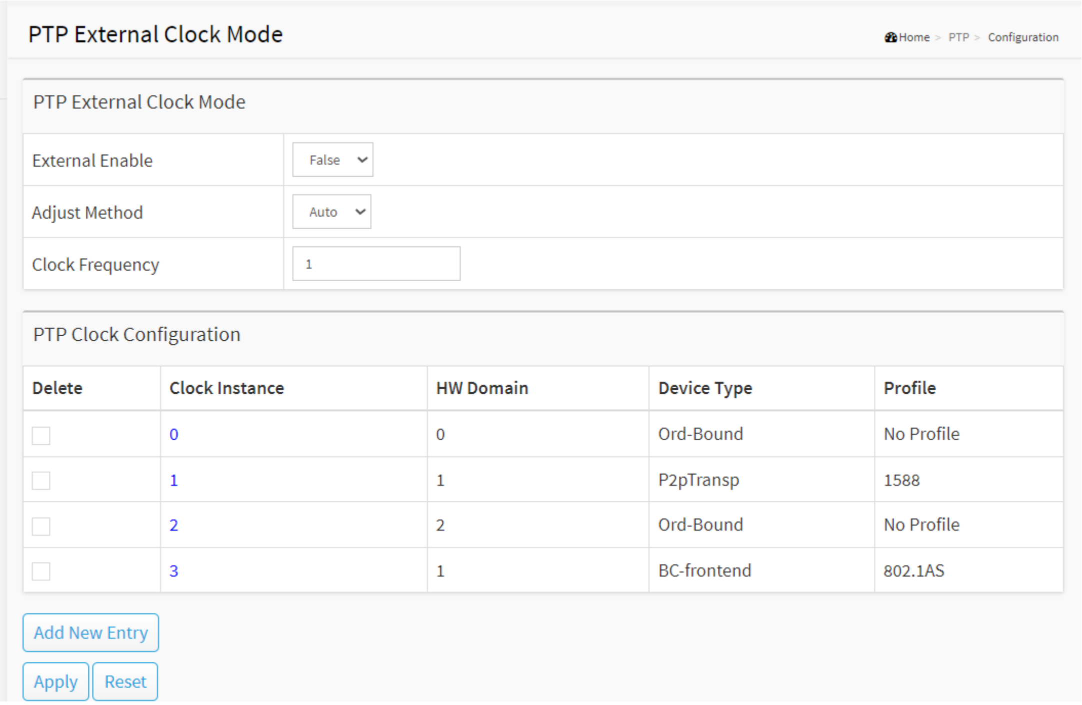


Profile : Indicates the profile used by the clock. The Profile selections are:

- ***No Profile*** : No PTP clock profile.
- ***1588*** : Use the IEEE Std 1588 profile. The protocol enables heterogeneous systems that include clocks of various inherent precision, resolution, and stability to synchronize to a grandmaster clock. The protocol supports synchronization in the sub-microsecond range with minimal network bandwidth and local clock computing resources. The protocol enhances support for synchronization to better than 1 nanosecond.
- ***G.8265.1*** : Use the ITU G.8265.1 Precision time protocol telecom profile for frequency synchronization.
- ***G.8275.1*** : Use the ITU G.8275.1 profile for Precision time protocol telecom profile for phase/time synchronization with full timing support from the network.
- ***802.1AS*** : Use the 802.1AS IEEE Standard for Local and Metropolitan Area Networks–Timing and Synchronization for Time-Sensitive Applications. It provides Protocols, procedures, and managed objects for the transport of timing over local area networks are defined in this standard. It includes the transport of synchronized time, the selection of the timing source (i.e., best master), and the indication of the occurrence and magnitude of timing impairments (i.e., phase and frequency discontinuities).



Example: Four PTP Clock Instances (0-3) configured



PTP External Clock Mode

PTP External Clock Mode

External Enable	False
Adjust Method	Auto
Clock Frequency	1

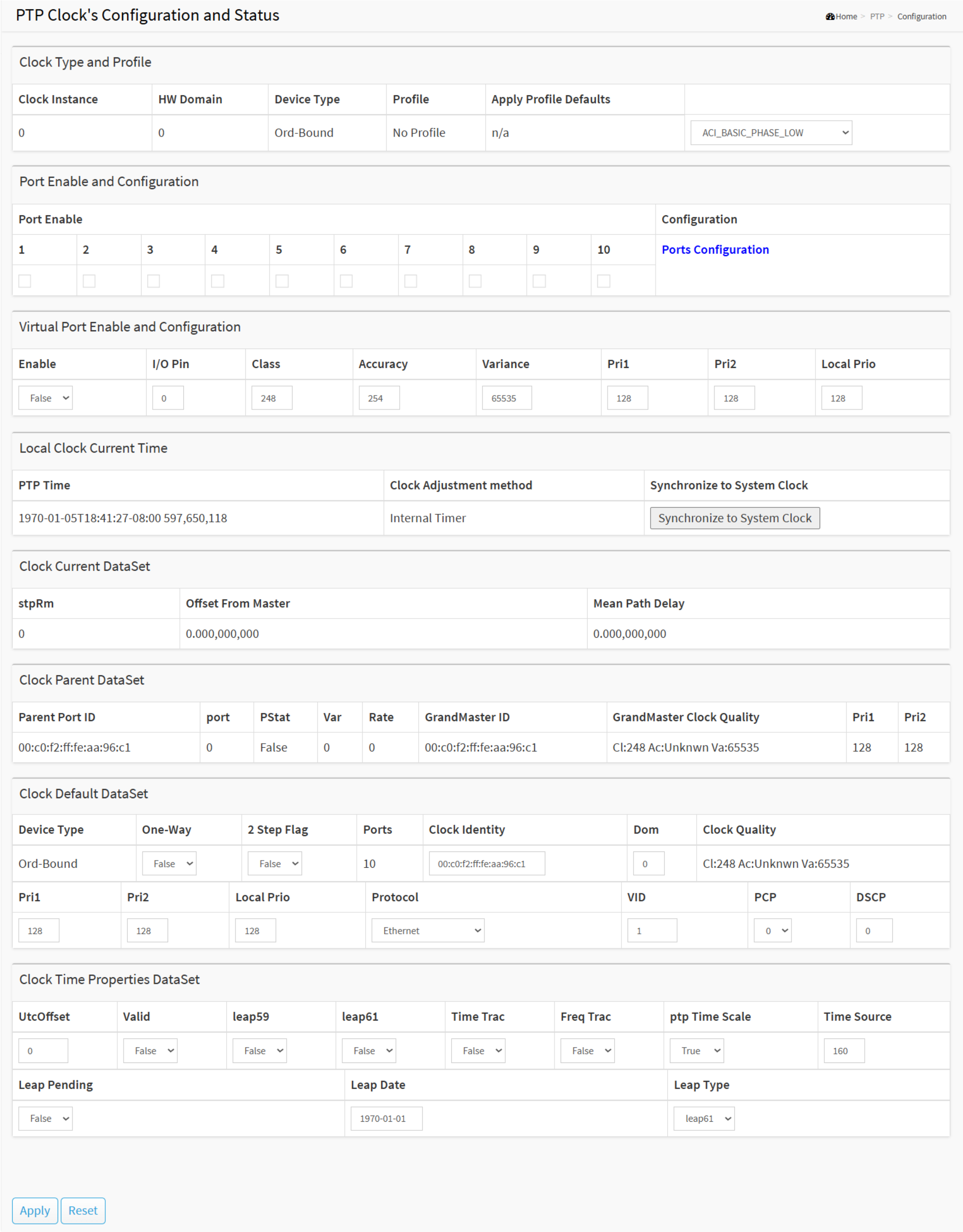
PTP Clock Configuration

Delete	Clock Instance	HW Domain	Device Type	Profile
□	0	0	Ord-Bound	No Profile
□	1	1	P2pTransp	1588
□	2	2	Ord-Bound	No Profile
□	3	1	BC-frontend	802.1AS

PTP Clock's Configuration and Status

Click on a linked Clock Instance number on the PTP External Clock Mode page to inspect and configure current PTP clock setting. See the figure above.

The PTP Clock’s Configuration and Status page is displayed.



PTP Clock's Configuration and Status

Clock Type and Profile

Clock Instance	HW Domain	Device Type	Profile	Apply Profile Defaults	
0	0	Ord-Bound	No Profile	n/a	ACI_BASIC_PHASE_LOW

Port Enable and Configuration

Port Enable										Configuration
1	2	3	4	5	6	7	8	9	10	Ports Configuration
□	□	□	□	□	□	□	□	□	□	

Virtual Port Enable and Configuration

Enable	I/O Pin	Class	Accuracy	Variance	Pri1	Pri2	Local Prio
False	0	248	254	65535	128	128	128

Local Clock Current Time

PTP Time	Clock Adjustment method	Synchronize to System Clock
1970-01-05T18:41:27-08:00 597,650,118	Internal Timer	Synchronize to System Clock

Clock Current DataSet

stpRm	Offset From Master	Mean Path Delay
0	0.000,000,000	0.000,000,000

Clock Parent DataSet

Parent Port ID	port	PStat	Var	Rate	GrandMaster ID	GrandMaster Clock Quality	Pri1	Pri2
00:c0:f2:ff:fe:aa:96:c1	0	False	0	0	00:c0:f2:ff:fe:aa:96:c1	Cl:248 Ac:Unknwn Va:65535	128	128

Clock Default DataSet

Device Type	One-Way	2 Step Flag	Ports	Clock Identity	Dom	Clock Quality
Ord-Bound	False	False	10	00:c0:f2:ff:fe:aa:96:c1	0	Cl:248 Ac:Unknwn Va:65535

Pri1	Pri2	Local Prio	Protocol	VID	PCP	DSCP
128	128	128	Ethernet	1	0	0

Clock Time Properties DataSet

UtcOffset	Valid	leap59	leap61	Time Trac	Freq Trac	ptp Time Scale	Time Source
0	False	False	False	False	False	True	160

Leap Pending	Leap Date	Leap Type
False	1970-01-01	leap61

Parameter descriptions:

The PTP clock's configuration sections are described below. For descriptions of individual parameters, refer to the online help page.

Clock Type and Profile: Show/update the clock type and profile details.

Port Enable and Configuration: Enable specific ports for this clock instance and configure the PTP Clock's Port Data Set Configuration. Port data set is defined in the IEEE 1588 standard.

Virtual Port Enable and Configuration: Enable and configure virtual ports for this clock instance.

Local Clock Current time: Show/update local clock data.

Clock Current Data Set: The clock current data set is defined in the IEEE 1588 Standard. The current data set is dynamic.

Clock Parent Data Set: The clock parent data set is defined in the IEEE 1588 standard. The parent data set is dynamic.

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.

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

Servo Parameters: The Basic clock servo uses a PID (Proportional Integral Derivative) regulator to calculate the current clock rate. i.e.:

clockAdjustment =

OffsetFromMaster/ P constant +

Integral(OffsetFromMaster)/ I constant +

Differential OffsetFromMaster)/ D constant

Filter Parameters: The default delay filter is a low pass filter, with a time constant of 2**DelayFilter*DelayRequestRate.

If the DelayFilter parameter is set to 0 or the Dist parameter is 0, the delay filter uses the same algorithm as the offset filter.

The default offset filter uses a minimum offset or a mean filter method i.e. The minimum measured offset during Period samples is used in the calculation.

The distance between two calculations is Dist periods.

Note: In configurations with Timestamp enabled PHYs, the period is automatically increased, if (period*dist < SyncPackets pr sec/4), i.e. max 4 adjustments are made per second.

If Dist is 0 the offset is low pass filtered, the filter BW is 0.1 Hz, the filter automatically adapts to the packet rate,

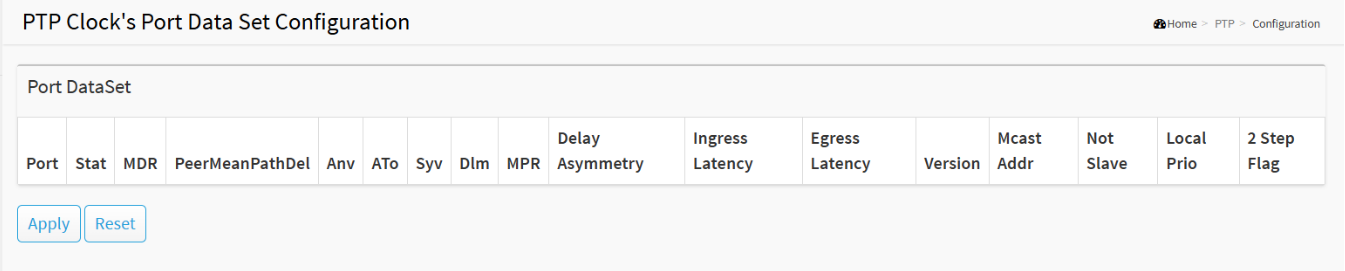
If Dist is 1 the offset is averaged over the Period,

If Dist is >1 the offset is calculated using 'min' offset.

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 request Sync messages from the selected master.

PTP Clock's Port Data Set Configuration

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.



PTP Clock's Port Data Set Configuration

Port DataSet

Port	Stat	MDR	PeerMeanPathDel	Anv	ATo	Syv	Dlm	MPR	Delay Asymmetry	Ingress Latency	Egress Latency	Version	Mcast Addr	Not Slave	Local Prio	2 Step Flag

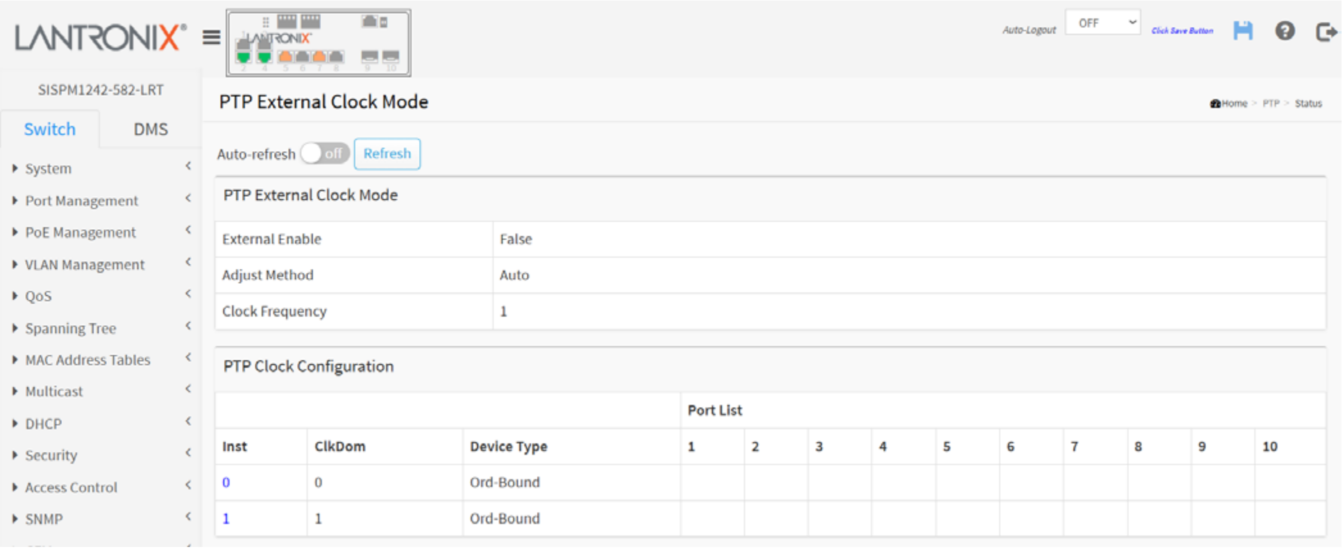
Refer to the online help page for parameter descriptions.

Status

This page lets you view current PTP clock settings. If none are configured, it displays the message "*No Clock Instances Present*".

To display PTP status in the web UI:

1. Go to PTP > Status.
2. View the PTP overall status.
3. If desired, click on the linked Clock Instance number to view the PTP Clock's configuration for that instance.



PTP External Clock Mode

PTP External Clock Mode	
External Enable	False
Adjust Method	Auto
Clock Frequency	1

PTP Clock Configuration

			Port List									
Inst	ClkDom	Device Type	1	2	3	4	5	6	7	8	9	10
0	0	Ord-Bound										
1	1	Ord-Bound										

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.
- ***Single*** : Use SyncE DPLL frequency control, if allowed by SyncE.
- ***Independent*** : Use an oscillator independent of SyncE for frequency control, if supported by the hardware.
- ***Common*** : Use second DPLL for PTP, Both DPLL have the same (SyncE recovered) clock.
- ***Auto*** : Auto Select clock control, based on PTP profile and available hardware resources.

Clock Frequency : Shows the current clock frequency used by the External Clock. Possible values are 1 - 25000000 (1 - 25MHz).

PTP Clock Description

Inst : Indicates the Instance of a particular Clock Instance [0..3]. Click on a linked Clock Instance number to view the clock instance's details. See the description in PTP Clock's Configuration and Status.

ClkDom : Indicates the Clock domain used by a particular Clock Instance [0..3].

Device Type : Indicates the Type of the Clock Instance. There are five Device Types.

- ***Ord-Bound*** - Clock's Device Type is Ordinary-Boundary Clock.
- ***P2p Transp*** - Clock's Device Type is Peer to Peer Transparent Clock.
- ***E2e Transp*** - Clock's Device Type is End to End Transparent Clock.
- ***Master Only*** - Clock's Device Type is Master Only.
- ***Slave Only*** - Clock's Device Type is Slave Only.

Port List : Shows the ports configured for that Clock Instance.

Ports Monitor Page

From the PTP Clock's Configuration page, click the linked text "Ports Monitor" to view the port data set configuration. See the PTP Clock's Port Data Set Configuration page.

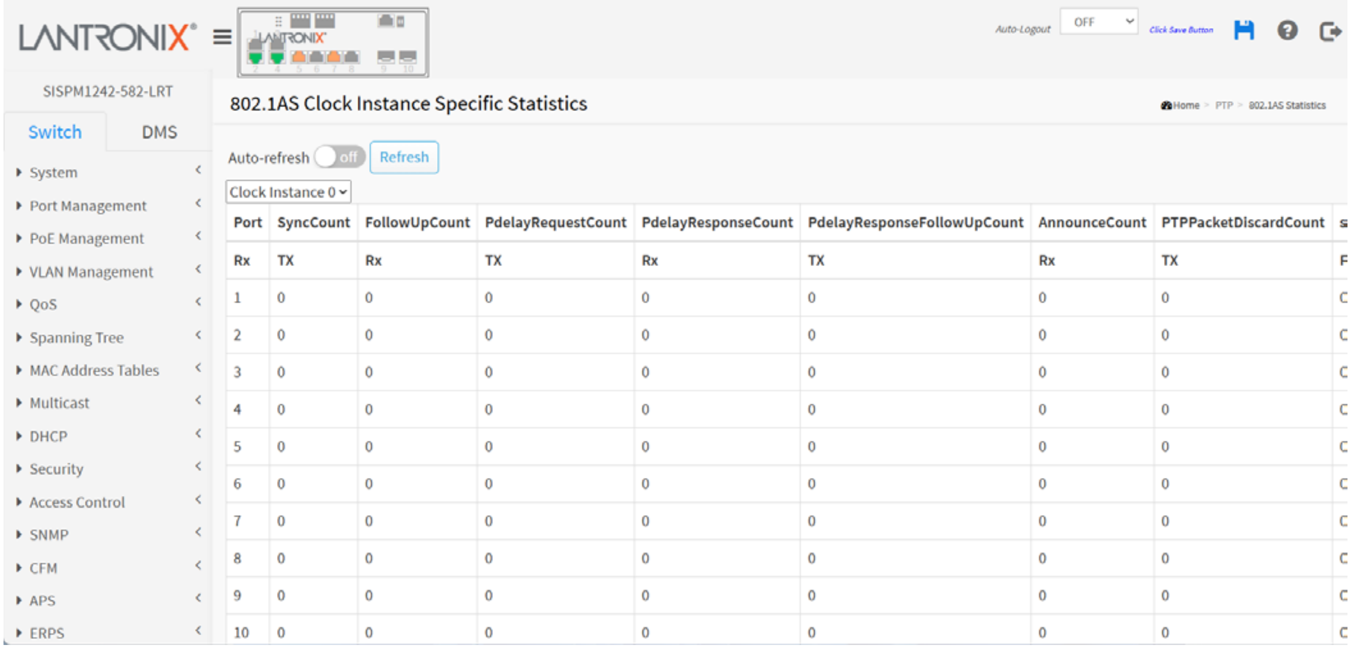
802.1AS Statistics

This page lets you view current 802.1AS Clock Instance-specific statistics. The IEEE 802.1AS standard enables stations attached to bridged LANs to meet the respective jitter, wander, and time synchronization requirements for time-sensitive applications. IEEE 802.1AS-2011 is part of the IEEE Audio Video Bridging (AVB) group of standards, further extended by the IEEE 802.1 Time-Sensitive Networking (TSN) Task Group.

802.1AS defines how IEEE 802.3 (Ethernet), IEEE 802.11 (Wi-Fi), and MoCA (Multimedia over Coax Alliance) can all be parts of the same PTP timing domain.

To display 802.1AS Clock Instance-specific statistics in the web UI:

1. Go to PTP > 802.1AS Statistics.
2. Select the Clock Instance (0 - 3 or CMLDS) at the dropdown.
3. **Auto-refresh** will refresh the page every 3 seconds. **Refresh** will refresh the page immediately.



802.1AS Clock Instance Specific Statistics

Auto-refresh off Refresh

Clock Instance 0

Port	SyncCount	FollowUpCount	PdelayRequestCount	PdelayResponseCount	PdelayResponseFollowUpCount	AnnounceCount	PTPPacketDiscardCount	S
Rx	TX	Rx	TX	Rx	TX	Rx	TX	F
1	0	0	0	0	0	0	0	C
2	0	0	0	0	0	0	0	C
3	0	0	0	0	0	0	0	C
4	0	0	0	0	0	0	0	C
5	0	0	0	0	0	0	0	C
6	0	0	0	0	0	0	0	C
7	0	0	0	0	0	0	0	C
8	0	0	0	0	0	0	0	C
9	0	0	0	0	0	0	0	C
10	0	0	0	0	0	0	0	C

Parameter descriptions:

For descriptions of the individual parameters, see the online help page.

Clock Instance : At the dropdown select a PTP Instance. The selections are Clock Instance 0-3 or CMLDS (Common Mean Link Delay Service).

802.1AS Received counters: this section displays the received counters.

802.1As Transmit Counters: this section displays the transmit counters.

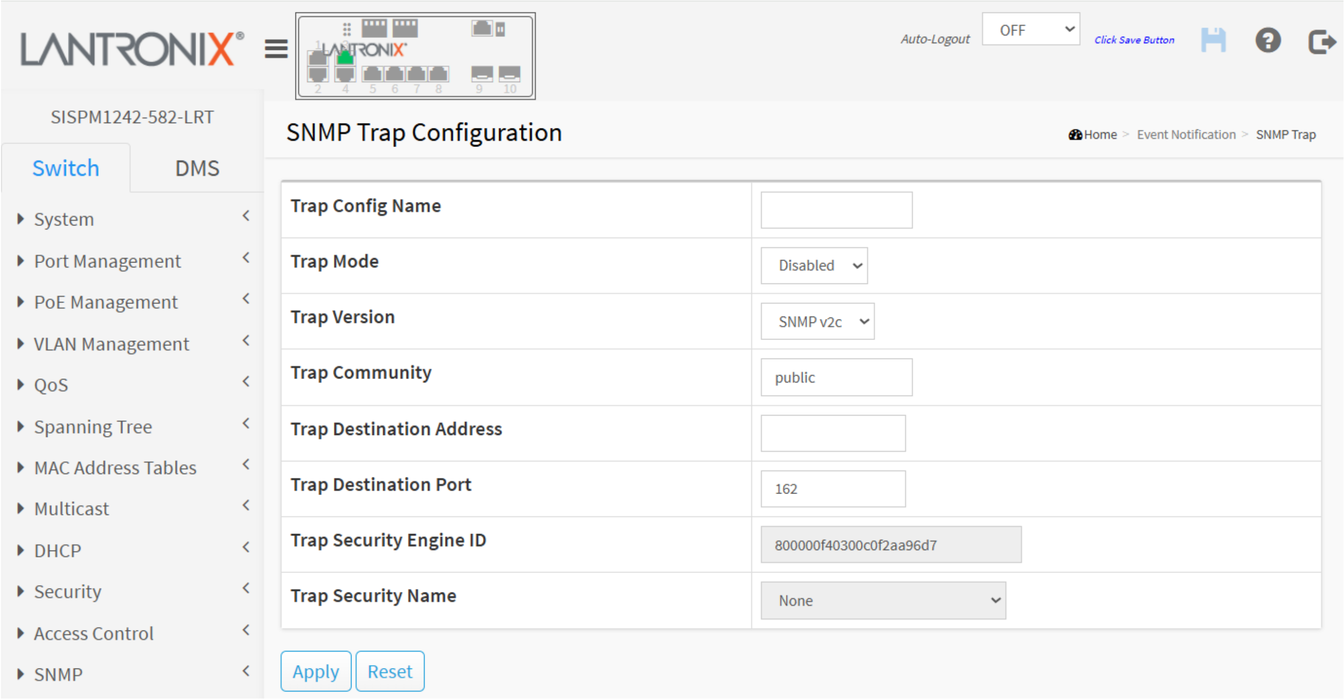
21. Event Notification

SNMP Trap

Configure SNMP Trap destinations on this page.

To configure SNMP traps in the web UI:

1. Go to Event Notification > SNMP Trap.
2. Click the **Add New Entry** button.
3. Configure the SNMP trap destination parameters.
4. Click **Apply** to save the configuration.



SNMP Trap Configuration

Trap Config Name	
Trap Mode	Disabled
Trap Version	SNMP v2c
Trap Community	public
Trap Destination Address	
Trap Destination Port	162
Trap Security Engine ID	800000f40300c0f2aa96d7
Trap Security Name	None

Parameter descriptions:

Trap Detailed Configuration

Trap Config Name : Enter the trap Configuration's name. Indicates the trap destination's 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 : Select the SNMP mode operation. Possible modes are:

- ***TCP***: Enable TCP SNMP mode operation.
- ***UDP***: Enable UDP SNMP mode operation.
- ***Disabled***: Disable SNMP mode operation.

Trap Version : Select the SNMP trap supported version. Possible versions are:

- ***SNMPv1*** : Set SNMP trap supported version 1.
- ***SNMPv2c*** **:** Set SNMP trap supported version 2c.
- ***SNMPv3*** *:* Set SNMP trap supported version 3.

Trap Community : Indicates the community access string when sending SNMP trap packet. The allowed string length is 0 to 63 characters, and the allowed content is ASCII characters 33 - 126.

Trap Destination Address : Indicates the SNMP trap destination address. It allows a valid IP address in dotted decimal notation ('x.y.z.w'). It also allows a valid hostname. A valid hostname is a string drawn from the alphabet (A-Za-z), digits (0-9), dot (.), dash (-). Spaces are not allowed, the first character must be an alpha character, and the first and last characters must not be a dot or a dash.

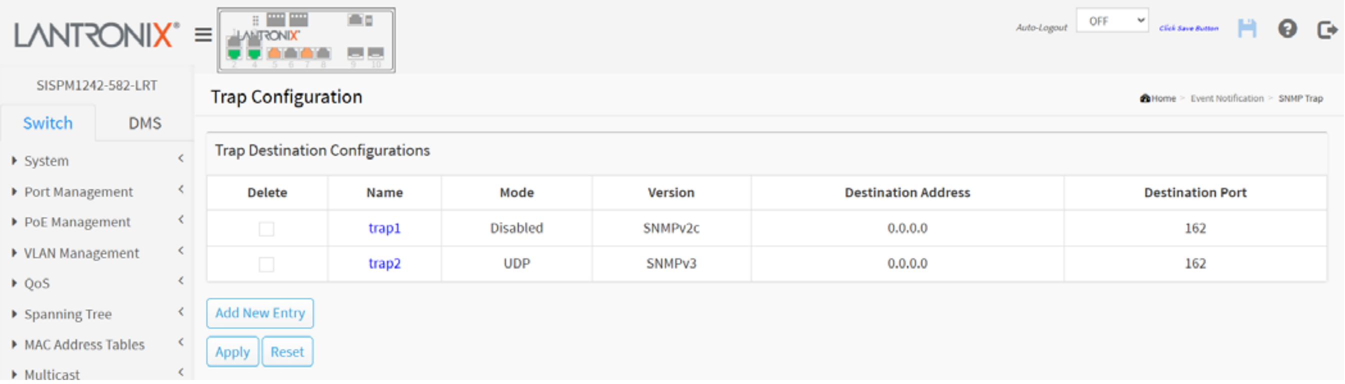
Indicates the SNMP trap destination IPv6 address. IPv6 address is in 128-bit records represented as eight fields of up to four hexadecimal digits with a colon separating each field (:). For example, 'fe80::215:c5ff:fe03:4dc7'. The symbol '::' is a special syntax that can be used as a shorthand way of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

Trap Destination Port : Indicates the SNMP trap destination port. SNMP Agent will send SNMP message via this port; the valid port range is 1~65535.

Trap Security Engine ID : Indicates the SNMP trap security engine ID. SNMPv3 sends traps and informs using USM for authentication and privacy. A unique engine ID for these traps and informs is needed. When "Trap Probe Security Engine ID" is enabled, the ID will be probed automatically. Otherwise, the ID specified in this field is used. The string must contain an even number(in hexadecimal format) with the number of digits between 10 and 64, but all-zeros and all 'F's are not allowed.

Trap Security Name : Indicates the SNMP trap security name. SNMPv3 traps and informs using USM for authentication and privacy. A unique security name is needed when traps and informs are enabled.

Example:



Trap Configuration

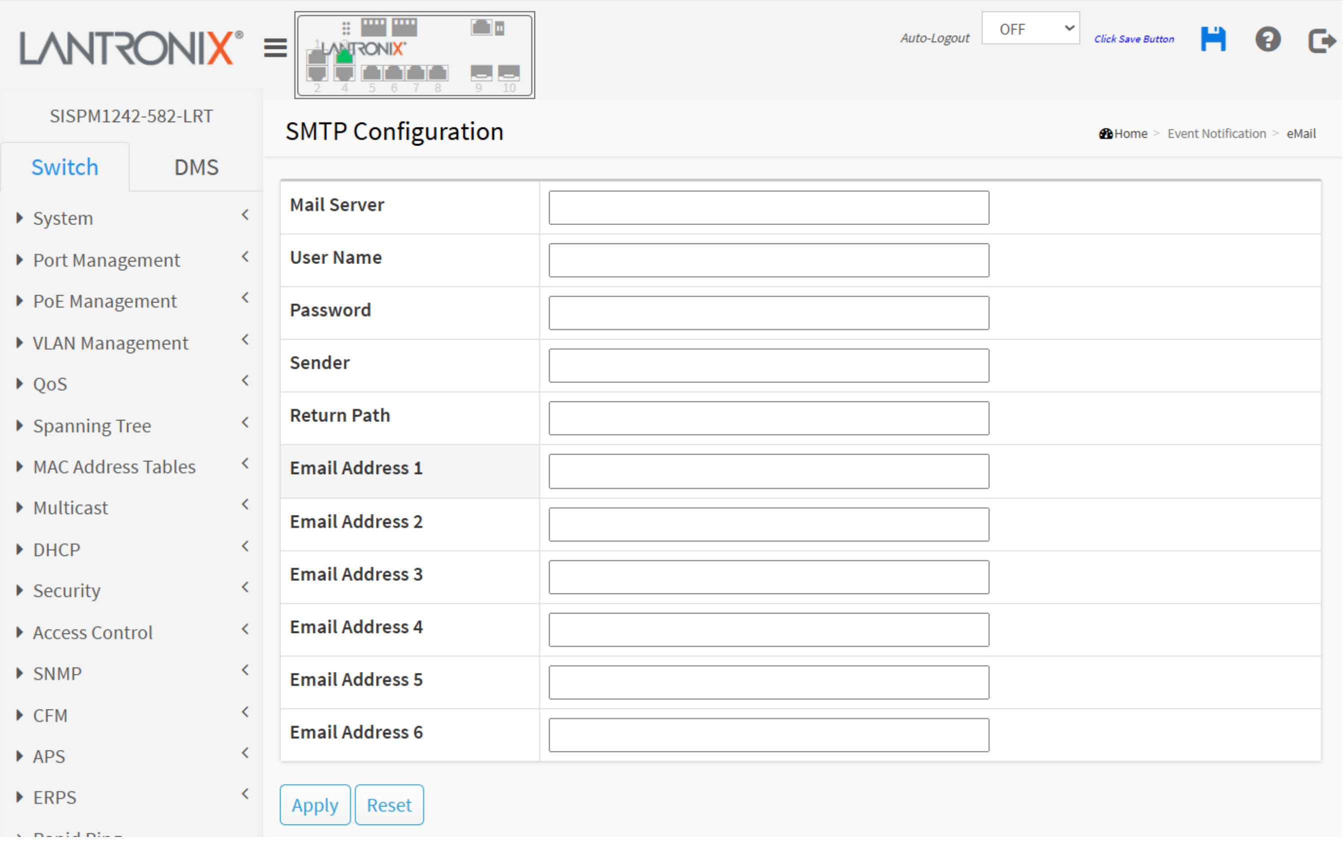
Trap Destination Configurations

Delete	Name	Mode	Version	Destination Address	Destination Port
□	trap1	Disabled	SNMPv2c	0.0.0.0	162
□	trap2	UDP	SNMPv3	0.0.0.0	162

Note: Click the linked Trap Name to view and edit details.

SMTP (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.



SMTP Configuration

Mail Server	
User Name	
Password	
Sender	
Return Path	
Email Address 1	
Email Address 2	
Email Address 3	
Email Address 4	
Email Address 5	
Email Address 6	

Apply Reset

Mail Server: The IP address or hostname of the mail server. IP address is expressed in dotted decimal notation. This will be the device that sends out the mail for you

User Name: Specify the username on the mail server.

Password: Specify the password of the user on the mail server.

Sender: Specify the sender name of the alarm mail.

Return Path: Specify the sender email address of the alarm mail. This address will be the "from" address on the email message.

Email Address #: Specify the email address of 1-6 receivers.

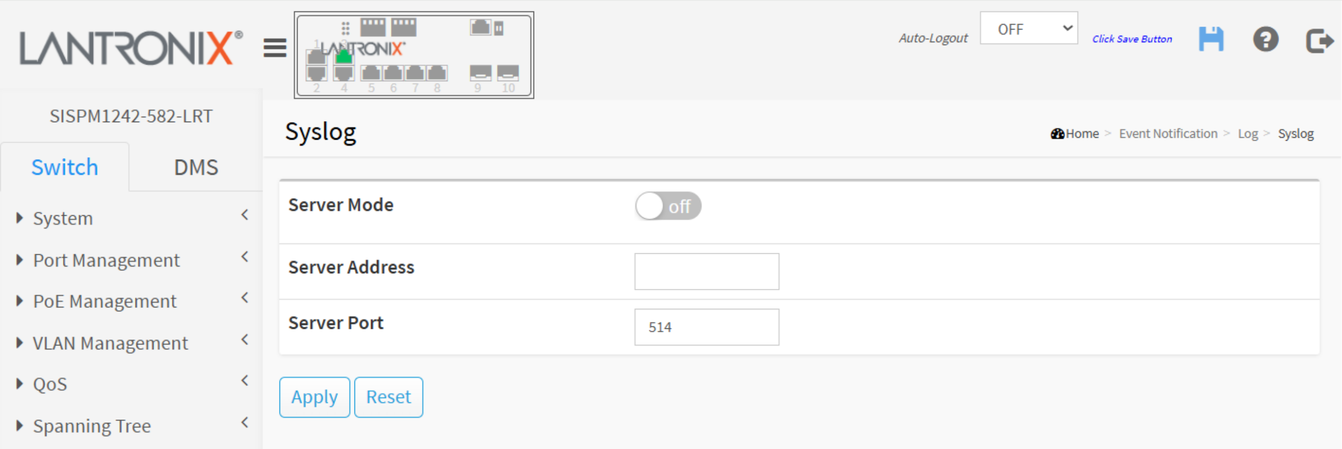
Log

Syslog

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

To configure Syslog in the web UI:

1. Go to Event Notification > Log > Syslog.
2. Enable the Server Mode.
3. Specify the Server Address and Server Port parameters.
4. Click **Apply**.



Syslog

Server Mode	off
Server Address	
Server Port	514

Parameter descriptions:

Server Mode : Set the Syslog server mode of operation. When the mode is enabled (on), a syslog message is sent to the Syslog server. The Syslog protocol is based on UDP communication and received on UDP port 514. The Syslog server will not send acknowledgments back to the sender since UDP is a connectionless protocol and it does not provide acknowledgments. The Syslog packet is always sent even if the Syslog server does not exist. Possible modes are:

- ***on*** : Enable server mode operation (enabled).
- ***off***: Disable server mode operation (disabled). The default is off.

Server Address : Enter the IPv4 host address or domain name (if DNS on the switch is enabled) of the Syslog server.

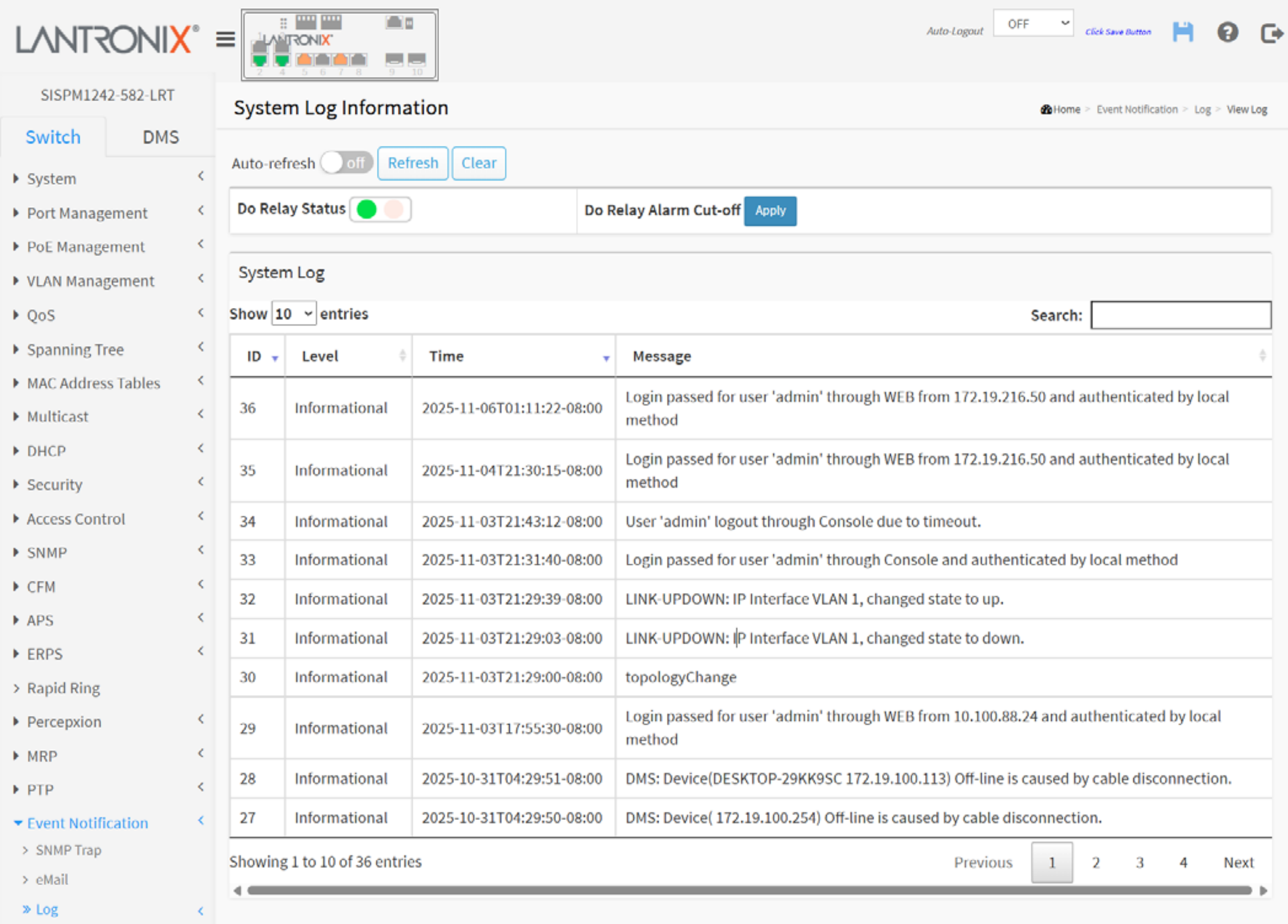
Server Port : Indicates the service port of the Syslog server. The default is port 514.

View Log

This page displays system log information of the switch. Use the Trap Event Severity Configuration page to configure the syslog groups and severity levels.

To display system log Information in the web UI:

1. Go to Event Notification > Log > View Log.
2. View the log information.



System Log Information

Do Relay Status ●

Do Relay Alarm Cut-off

System Log

Show 10 entries

Search:

ID	Level	Time	Message
36	Informational	2025-11-06T01:11:22-08:00	Login passed for user 'admin' through WEB from 172.19.216.50 and authenticated by local method
35	Informational	2025-11-04T21:30:15-08:00	Login passed for user 'admin' through WEB from 172.19.216.50 and authenticated by local method
34	Informational	2025-11-03T21:43:12-08:00	User 'admin' logout through Console due to timeout.
33	Informational	2025-11-03T21:31:40-08:00	Login passed for user 'admin' through Console and authenticated by local method
32	Informational	2025-11-03T21:29:39-08:00	LINK-UPDOWN: IP Interface VLAN 1, changed state to up.
31	Informational	2025-11-03T21:29:03-08:00	LINK-UPDOWN: IP Interface VLAN 1, changed state to down.
30	Informational	2025-11-03T21:29:00-08:00	topologyChange
29	Informational	2025-11-03T17:55:30-08:00	Login passed for user 'admin' through WEB from 10.100.88.24 and authenticated by local method
28	Informational	2025-10-31T04:29:51-08:00	DMS: Device(DESKTOP-29KK9SC 172.19.100.113) Off-line is caused by cable disconnection.
27	Informational	2025-10-31T04:29:50-08:00	DMS: Device(172.19.100.254) Off-line is caused by cable disconnection.

Showing 1 to 10 of 36 entries

Navigating the System Log Information Table

Each page shows table entries, selected through the "Show x entries" per page input field.

Click the **Clear** button to clear the system log entries.

Click the **Refresh** button to update the displayed table.

Do Relay Status shows the status of digital-out relay contact.

Do Relay Alarm Cut-off forcibly cuts off the digital-out relay contact.

Parameter descriptions:

System Log Information

ID : ID (>= 1) of the system log entry.

Level : The level of the system log entry. The following level types are supported:

- ***Debug*** : debug level message.

- ***Info*** : informational message.
- ***Notice*** : normal, but significant, condition.
- ***Warning*** : warning condition.
- ***Error*** : error condition.
- ***Crit*** : critical condition.
- ***Alert*** : action must be taken immediately.
- ***Emerg*** : system is unusable.

Time : Displays the log record by device time. The date and time of the system log entry.

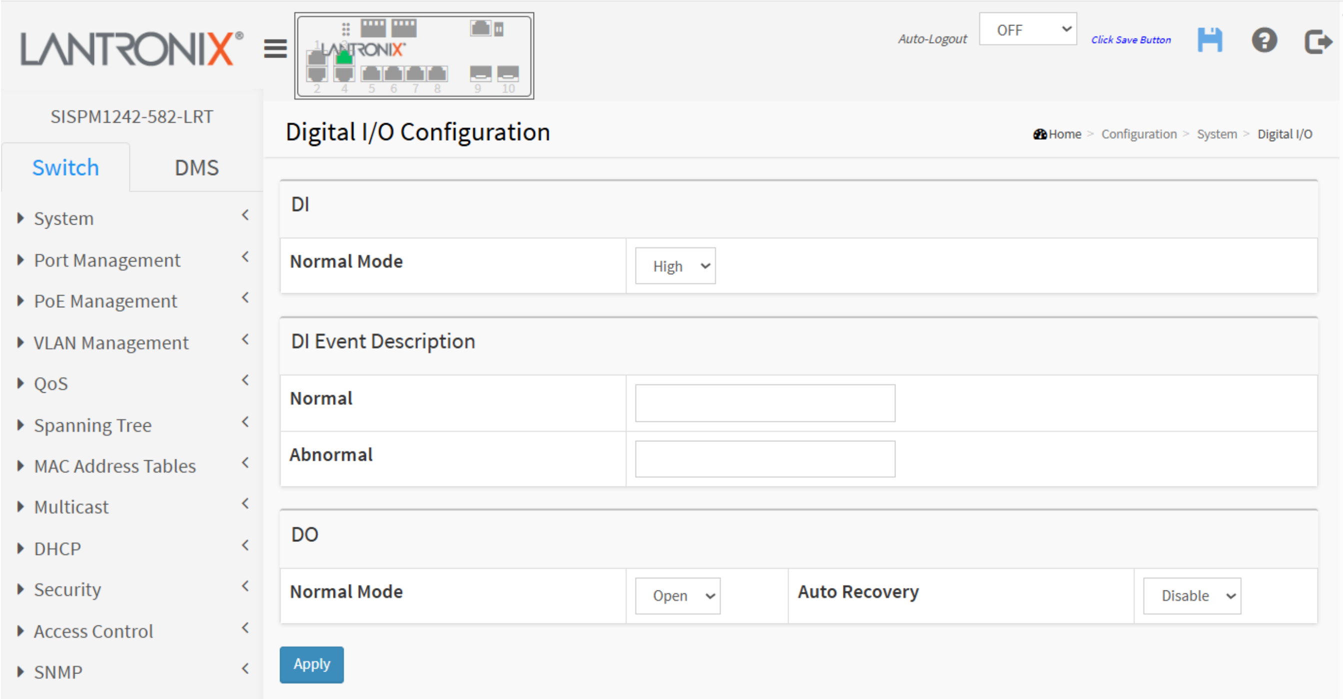
Message : Displays the log detail message.

Digital I/O

This page lets you configure the normal modes of digital input/output (DI/DO).

To configure Digital I/O configuration:

1. Go to Event Notification >Digital I/O.
2. Configure the parameters.
3. Click **Apply** to save the settings.



Digital I/O Configuration

DI	
Normal Mode	High

DI Event Description	
Normal	
Abnormal	

DO			
Normal Mode	Open	Auto Recovery	Disable

Parameter Descriptions:

DI Normal Mode: Set the normal mode of the digital input. The options are High or Low.

DI Event Description Normal: Customize the event message.

DI Event Description Abnormal: Customize the event message.

DO Normal Mode: Set the normal mode of the digital output. The options are Open or Close.

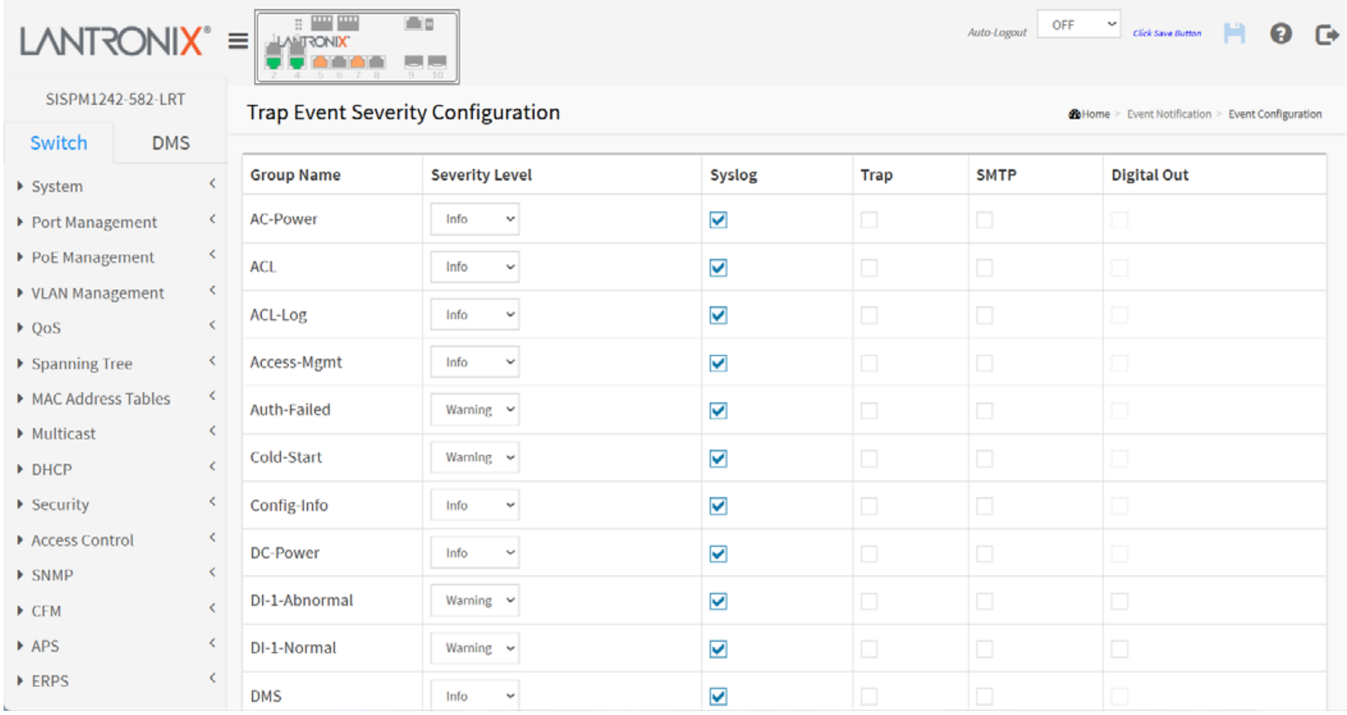
Auto Recovery: Enable the function of Auto Recovery, Digital Output will automatically back to normal mode when Digital Input change back to normal mode.

Event Configuration

This page lets you view and set current trap event severity level parameters.

To configure Trap Event Severity:

1. Go to Event Notification > Event Configuration.
2. Select the Group Name and Severity Level.
3. Check one or more checkboxes to enable different trap events.
4. Click **Apply** to save the settings.



Trap Event Severity Configuration

Group Name	Severity Level	Syslog	Trap	SMTP	Digital Out
AC-Power	Info	☑	☐	☐	☐
ACL	Info	☑	☐	☐	☐
ACL-Log	Info	☑	☐	☐	☐
Access-Mgmt	Info	☑	☐	☐	☐
Auth-Failed	Warning	☑	☐	☐	☐
Cold-Start	Warning	☑	☐	☐	☐
Config-Info	Info	☑	☐	☐	☐
DC-Power	Info	☑	☐	☐	☐
DI-1-Abnormal	Warning	☑	☐	☐	☐
DI-1-Normal	Warning	☑	☐	☐	☐
DMS	Info	☑	☐	☐	☐

Parameter descriptions:

Group Name : The name identifying the severity group.

Severity Level : Each group has a severity level. These eight severity levels are supported:

- ***Emerg***ency : System is unusable.
- ***Alert*** : Action must be taken immediately.
- ***Crit***ical : Critical conditions.
- ***Error*** : Error conditions.
- ***Warn***ing : Warning conditions.
- ***Notice*** : Normal but significant conditions.
- ***Info***rmation : Information messages.
- ***Debug*** : Debug-level messages.

Syslog : Check the box to select this Group Name in Syslog.

Trap : Check the box to select this Group Name in Trap.

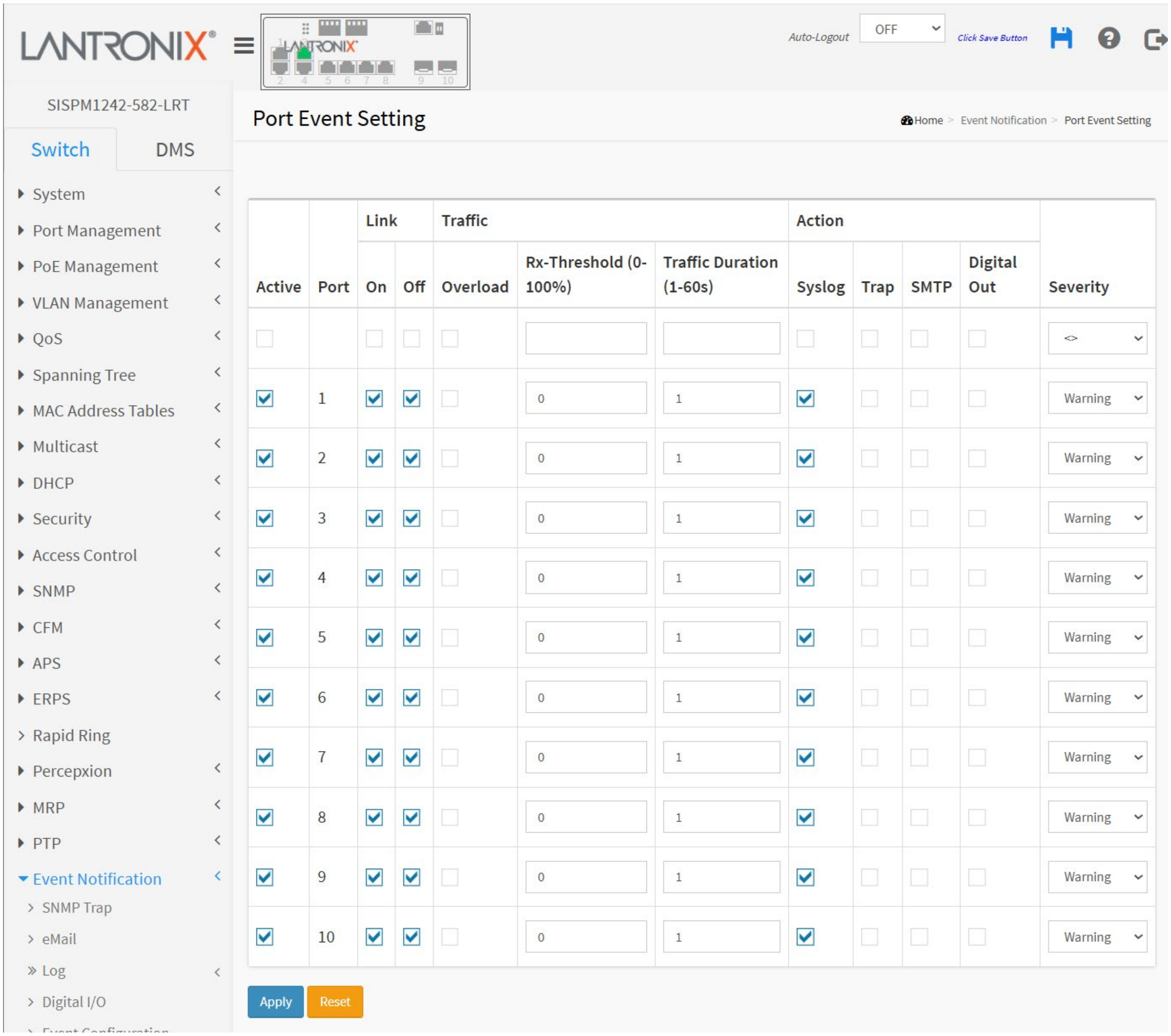
SMTP : Check the box to enable this Group Name in SMTP.

Port Event Setting

This page lets you configure the port events.

To configure port events in the Web UI:

1. Go to Event Notification > Event Configuration.
2. Configure the port event settings.
3. Click **Apply** to save the settings.



Port Event Setting

		Link		Traffic			Action				
Active	Port	On	Off	Overload	Rx-Threshold (0-100%)	Traffic Duration (1-60s)	Syslog	Trap	SMTP	Digital Out	Severity
□		□	□	□			□	□	□	□	<>
☑	1	☑	☑	□	0	1	☑	□	□	□	Warning
☑	2	☑	☑	□	0	1	☑	□	□	□	Warning
☑	3	☑	☑	□	0	1	☑	□	□	□	Warning
☑	4	☑	☑	□	0	1	☑	□	□	□	Warning
☑	5	☑	☑	□	0	1	☑	□	□	□	Warning
☑	6	☑	☑	□	0	1	☑	□	□	□	Warning
☑	7	☑	☑	□	0	1	☑	□	□	□	Warning
☑	8	☑	☑	□	0	1	☑	□	□	□	Warning
☑	9	☑	☑	□	0	1	☑	□	□	□	Warning
☑	10	☑	☑	□	0	1	☑	□	□	□	Warning

Parameter Descriptions

Active: Select to activate the event handler of this port.

Port: The logical port number for this row.

Link On: Event is triggered when link state moves to on.

Link Off: Event is triggered when link is off.

Traffic Overload: Event is triggered when the traffic is overload.

Traffic Rx-Threshold (0-100%): Event is triggered when Rx reach this threshold.

Traffic Duration (1-60 seconds): Event is triggered when the traffic duration reach this value.

Action Syslog: Enable this port for Syslog.

Action Trap: Enable this port for Trap.

Action SMTP: Enable this port for SMTP.

Severity: Every port has a severity level. The following level types are supported:

- **<0> Emergency**: System is unusable.
- **<1> Alert**: Action must be taken immediately.
- **<2> Critical**: Critical conditions.
- **<3> Error**: Error conditions.
- **<4> Warning**: Warning conditions.
- **<5> Notice**: Normal but significant conditions.
- **<6> Information**: Information messages.
- **<7> Debug**: Debug-level messages.

22. Router

The router module lets you configure key-chain and access list parameters.

Note: The IP Address > Advanced Settings page has a Mode dropdown to select Host or Router mode. It must be set to Router to be able to use the Router function.

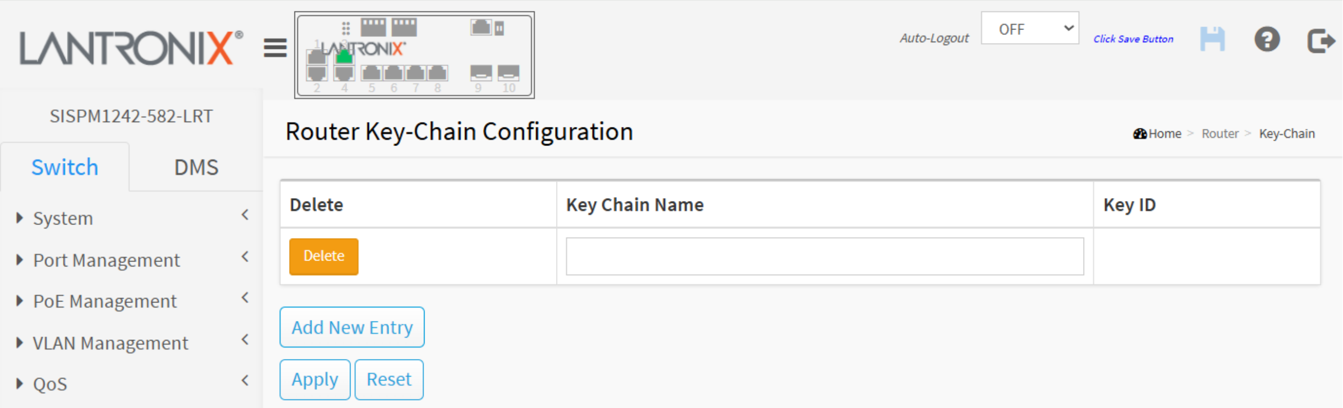
Key-Chain

This page lets you set router key-chain name table parameters.

A key chain is a set of keys used in succession; each has a limited lifetime. Change the keys frequently to reduce the chance of an intruder guessing a key. A key is not used during inactive time (when not activated). If a period occurs when no key is activated, no neighbor authentication can occur, and routing updates will fail.

To configure key-chain in the Web UI:

1. Go to Router > Key-Chain.
2. Click **Add New Entry**.
3. Configure the settings.
4. Click **Apply** to save the configuration.



Router Key-Chain Configuration

Delete	Key Chain Name	Key ID
Delete		

Parameter descriptions:

Delete : Click to delete an existing entry.

Add New Entry: Click to add a new entry (row) to the table.

Key Chain Name : The name of the key-chain entry. A valid name string length is 1 - 31 characters and allows all printable characters excluding the space character.

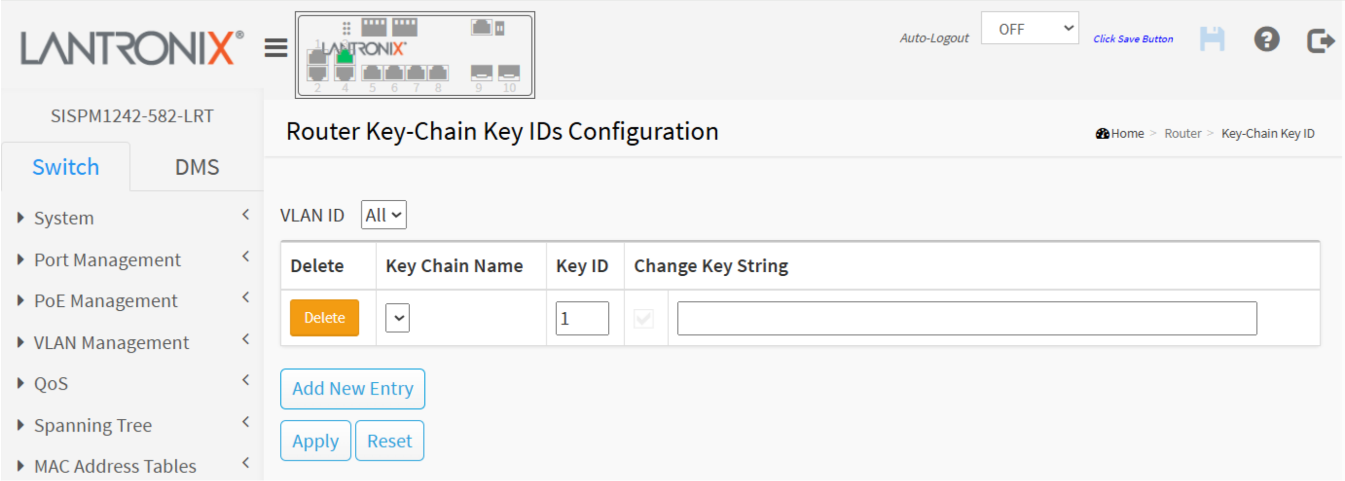
Key ID : Click the icon to edit the key. Key ID must be an integer value of 1 - 255. The minimum length is 1.

Key-Chain Key ID

Each key in a keychain has a key string, authentication algorithm, sending lifetime, and receiving lifetime. When the system time is within the lifetime of a key in a keychain, an application uses the key to authenticate incoming and outgoing packets. The keys in the keychain take effect one by one according to the sequence of the configured lifetimes. This way, the authentication algorithms and keys are dynamically changed to implement dynamic authentication.

To configure the key-chain key ID in the Web UI:

1. Go to Router > Key-Chain.
2. Click **Add New Entry** to add a row.
3. Configure the settings.
4. Click **Apply** to save the configuration.



Router Key-Chain Key IDs Configuration

VLAN ID All

Delete	Key Chain Name	Key ID	Change Key String	
Delete		1	☑	

Parameter descriptions:

VLAN ID : At the dropdown select the set of VIDs to display (All or a specific VLAN ID).

Delete : Click to delete an existing entry. It will be deleted during the next save.

Add New Entry: Click to add a new entry to the table.

Key Chain Name : The given name of the key chain. The valid name string length is 1-31 characters and allows all printable characters excluding the space character.

Key ID : The assigned key chain identifier. Click the icon to edit the key. Key ID must be an integer value of 1 - 255. The minimum length is 1.

Change Key String: Check the box to be able to change the existing Key String. Click the **Apply** button to save the change.

Access-list

This page lets you view and set Router Access-List instances and parameters.

You can filter incoming and outgoing routes for a given IP interface using two Standard Access Lists - one for input and one for output.

The standard Access List is a named, ordered list of pairs of IP prefix (IP address and IP mask length) and action. The action can be ***deny*** or ***permit***.

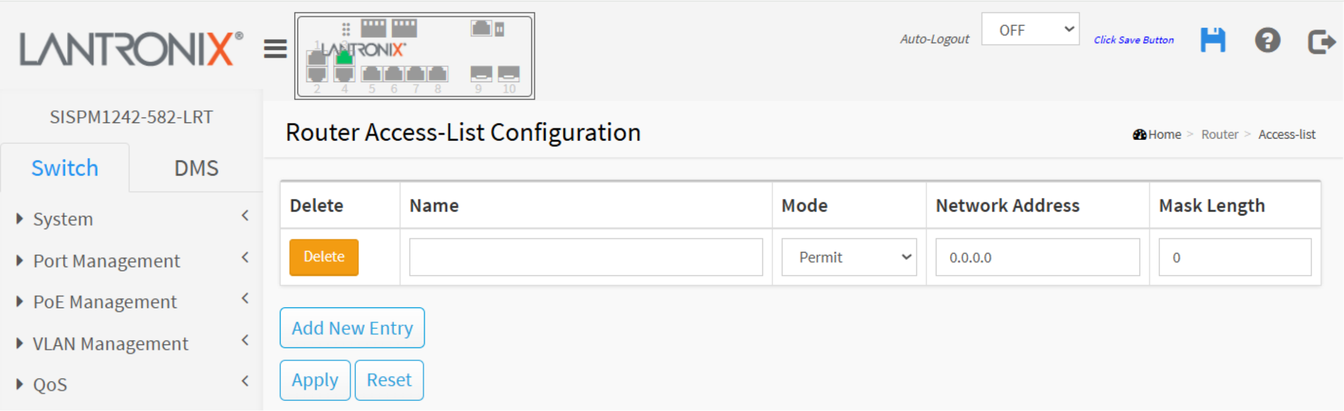
If an access list is defined, each route from the RIP message is checked against the list starting from the first pair:

- if it matches the first pair and the action is ***permit***, the route is passed;
- if the action is ***deny***, the route is not passed. If the route does not match, the following pair is considered.

If there is no pair that the route matches, the ***deny*** action is applied.

To configure the access list in the Web UI:

1. Go to the Router > Access List.
2. Configure the settings.
3. Click **Apply** to save the settings.



Router Access-List Configuration

Delete	Name	Mode	Network Address	Mask Length
Delete		Permit	0.0.0.0	0

Add New Entry

Apply Reset

Parameter descriptions:

Delete : Click to delete an existing entry.

Add New Entry: Click to add a new entry to the table.

Name : The name of the router access list instance. The name of the access-list entry. The valid name string length is from 1 to 31 and allows all printable characters excluding space character.

Mode : The access right mode of the access list entry.

- ***Deny***: Deny the access right.
- ***Permit***: Permit the access right.

Network Address : The IPv4 address of the router access list.

Mask Length : The netmask length of the router access list.

23. OSPF

Open Shortest Path First (OSPF) is a link-state routing protocol designed to be run internal to a single Autonomous System. Each OSPF router maintains an identical database describing the Autonomous System's topology. Using this database, a routing table is calculated by constructing a shortest-path tree.
For more OSPFv2 information see https://datatracker.ietf.org/doc/html/rfc2328.

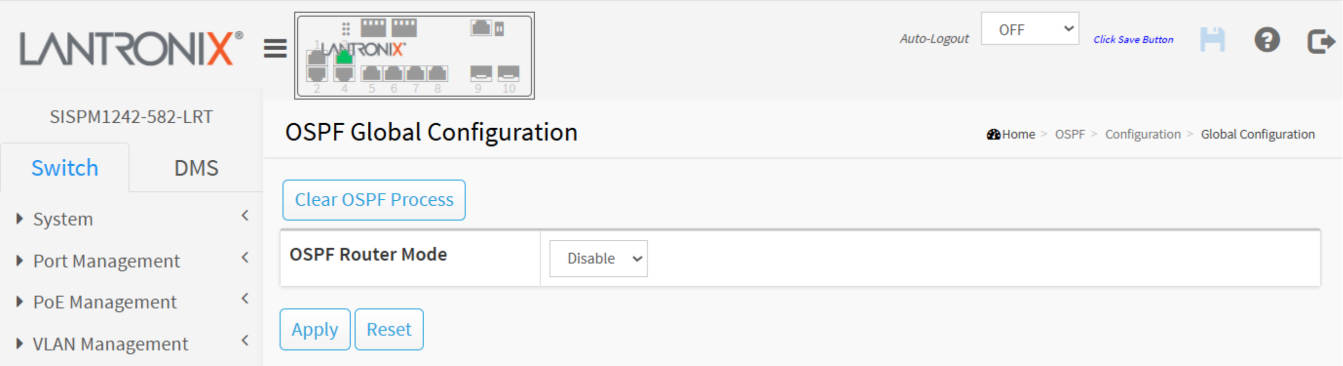
Configuration

Global Configuration

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

To configure OSPF in the Web UI:

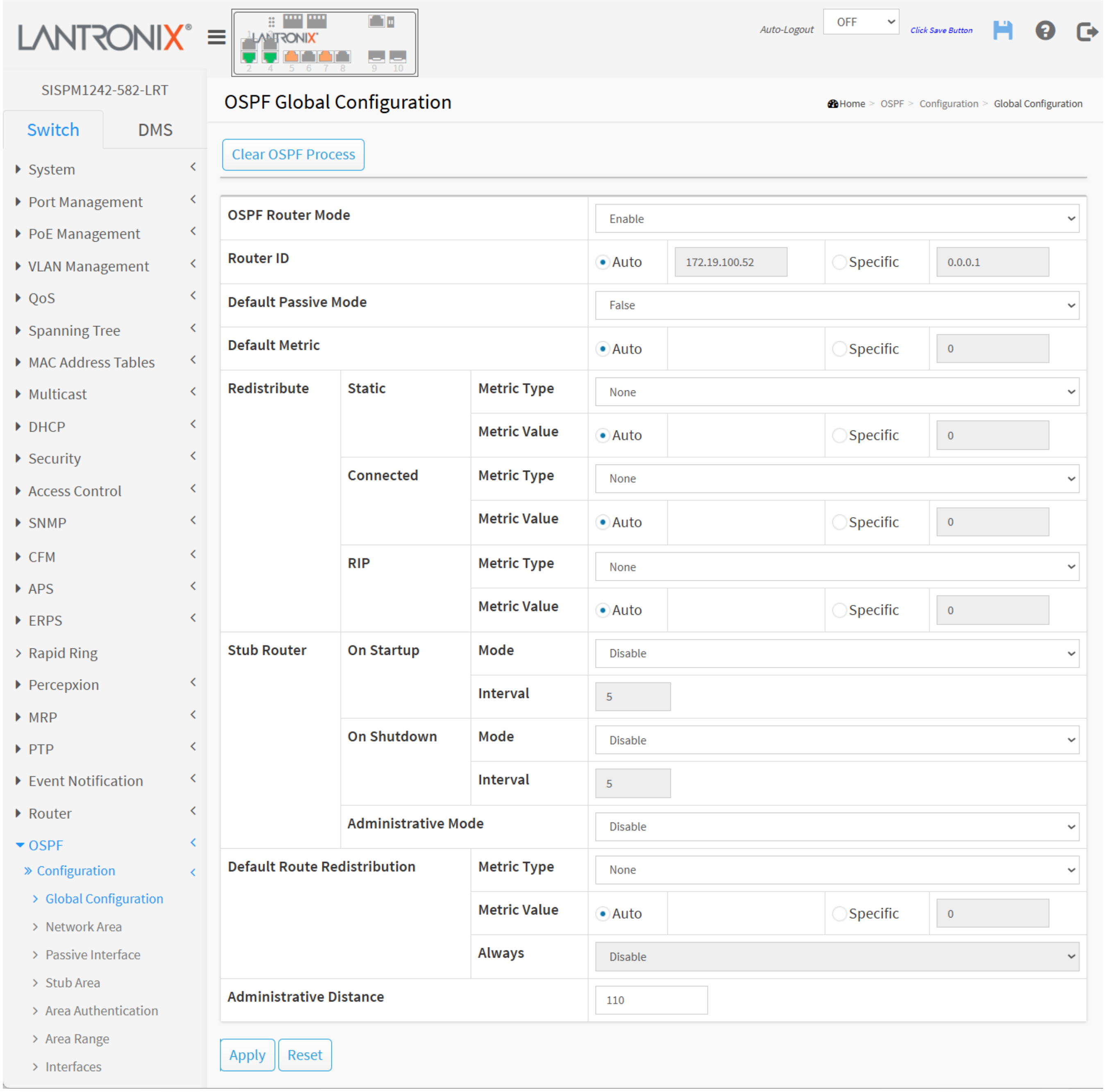
1. Go to OSPF > Configuration > Global Configuration.



OSPF Global Configuration

OSPF Router Mode	Disable

2. You may need to click **Clear OSPF Process** to reset the current process.
3. Enable the OSPF Router Mode.
4. Click **Apply** to save the mode change. The page will expand to show the configurable parameters.



OSPF Global Configuration

Clear OSPF Process

OSPF Router Mode			Enable			
Router ID			● Auto	172.19.100.52	○ Specific	0.0.0.1
Default Passive Mode			False			
Default Metric			● Auto		○ Specific	0
Redistribute	Static	Metric Type	None			
		Metric Value	● Auto		○ Specific	0
	Connected	Metric Type	None			
		Metric Value	● Auto		○ Specific	0
	RIP	Metric Type	None			
		Metric Value	● Auto		○ Specific	0
Stub Router	On Startup	Mode	Disable			
		Interval	5			
	On Shutdown	Mode	Disable			
		Interval	5			
	Administrative Mode		Disable			
Default Route Redistribution		Metric Type	None			
		Metric Value	● Auto		○ Specific	0
		Always	Disable			
Administrative Distance			110			

Apply Reset

5. Enter the settings.
6. Click **Apply** to save the new configuration.

Parameter descriptions:

Clear OSPF Process : Click to reset the current OSPF process. At the confirmation prompt click OK.

OSPF Router Mode : At the dropdown select to Enable or Disable the OSPF router mode. The default is Disabled.

Router ID : The OSPF Router ID in IPv4 address format (A.B.C.D). When the router's OSPF Router ID is changed, if there is one or more fully adjacent neighbors in current OSPF area, the new router ID will take effect after restart

OSPF process. Note that the router ID must be unique in the Autonomous System and value '0.0.0.0' is invalid since it is reserved for the default algorithm.

- ***Auto***: The default algorithm will choose the largest IP address assigned to the router.
- ***Specific***: User specified router ID. The valid range is from 0.0.0.1 to 255.255.255.254.

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

Default Metric : User specified default metric value for the OSPF routing protocol. The field is significant only when the argument 'I*sSpecificDefMetric*' is TRUE.

- ***Auto***: The default metric is calculated automatically based on the routing protocols.
- ***Specific***: User specified default metric. The valid range is 0 to 16777214.

Static Redistribute Metric Type : The OSPF redistributed metric type for the static routes:

- ***None***: The static routes are not redistributed.
- ***External Type 1***: External Type 1 of the static routes.
- ***External Type 2***: External Type 2 of the static routes.

Static Redistribute Metric Value : User specified metric value for the static routes. The field is significant only when the argument '*StaticRedistIsSpecificMetric*' is TRUE. The valid range is 0 to 16777214.

- ***Auto***: The redistributed metric is the same as the original metric value.
- ***Specific***: User specified metric for the static routes.

Connected Redistribute Metric Type : The OSPF redistributed metric type for the connected interfaces.

- ***None***: The connected interfaces are not redistributed.
- ***External Type 1***: External Type 1 of the connected interfaces routes.
- ***External Type 2***: External Type 2 of the connected interfaces routes.

Connected Redistribute Metric Value : User specified metric value for the connected interfaces. The field is significant only when the argument *'ConnectedRedistIsSpecificMetric'* is TRUE. The valid range is 0 to 16777214.

- ***Auto***: The redistributed metric is the same as the original metric value.
- ***Specific***: User specified metric for the connected routes.

RIP Redistribute Metric Type : The OSPF redistributed metric type for the RIP routes. The field is significant only when the RIP protocol is supported on the device.

- ***None***: The RIP routes are not redistributed.
- ***External Type 1***: External Type 1 of the RIP routes.
- ***External Type 2***: External Type 2 of the RIP routes.

RIP Redistribute Metric Value : User specified metric value for the RIP routes. The field is significant only when the RIP protocol is supported on the device and argument *'RipRedistIsSpecificMetric'* is TRUE. The valid range is 0 to 16777214.

- ***Auto***: The redistributed metric is the same as the original metric value.
- ***Specific***: User specified metric for the RIP routes.

Stub router during startup period : Configures OSPF to advertise a maximum metric during startup for a configured period.

Stub router on startup interval time : User specified time interval (seconds) to advertise itself as stub area. The field is significant only when the on-startup mode is enabled. The valid range is 5 to 86400 seconds.

Stub router during shutdown period : Configures OSPF to advertise a maximum metric during shutdown for a configured period. The device advertises a maximum metric when the OSPF router mode is disabled and notice that the mechanism also works when the device reboots but not for the 'reload default' case.

Stub router on shutdown interval time : User specified time interval (seconds) to wait till shutdown completed. The field is significant only when the on-shutdown mode is enabled. The valid range is 5 to 100 seconds.

Stub router administrative mode : Configures OSPF stub router mode administratively applied, for an indefinite period.

Default Route Redistribution Metric Type : The OSPF redistributed metric type for a default route:

- ***None***: The default route are not redistributed.
- ***External Type 1***: External Type 1 of the default route.
- ***External Type 2***: External Type 2 of the default route.

Default Route Redistribution Metric value : User specified metric value for a default route. The field is significant only when the argument *'DefaultRouteRedistIsSpecificMetric'* is TRUE. The valid range is 0 to 16777214.

- ***Auto***: The redistributed metric is the same as the original metric value.
- ***Specific***: User specified metric for the default route.

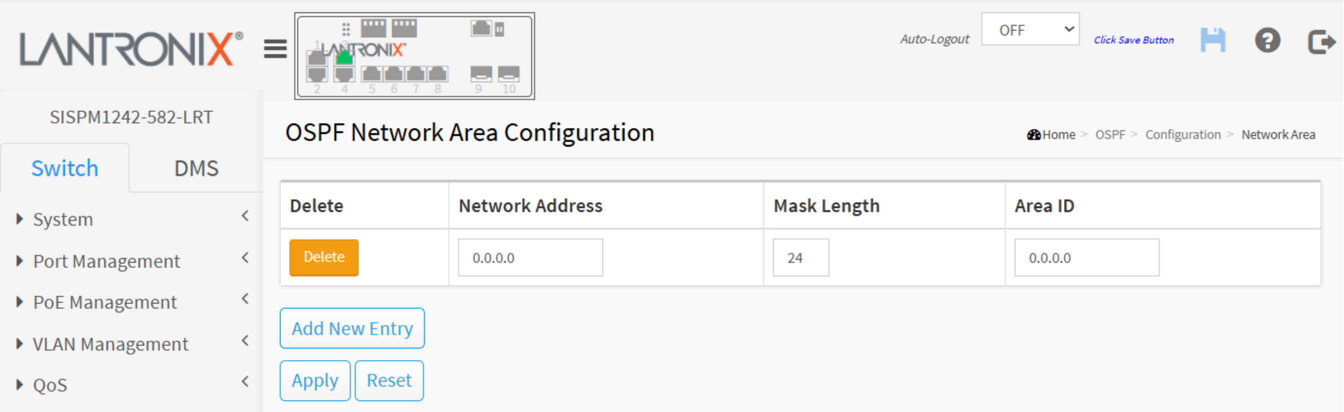
Default Route Redistribution Always : Specifies to always advertise a default route into all external-routing capable areas. Otherwise, the router only to advertise the default route when the advertising router already has a default route.

Administrative Distance : The OSPF administrative distance.

Network Area

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

1. Go to OSPF > Configuration > Network Area.
2. Click **Add New Entry**.
3. Configure the settings.
4. Click **Apply** to save the configuration.



OSPF Network Area Configuration

Delete	Network Address	Mask Length	Area ID
Delete	0.0.0.0	24	0.0.0.0

Parameter descriptions:

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

Add New Entry: Click to add a new entry to the table.

Network Address : Enter a valid IPv4 network address.

Mask Length : Enter a valid IPv4 network mask length.

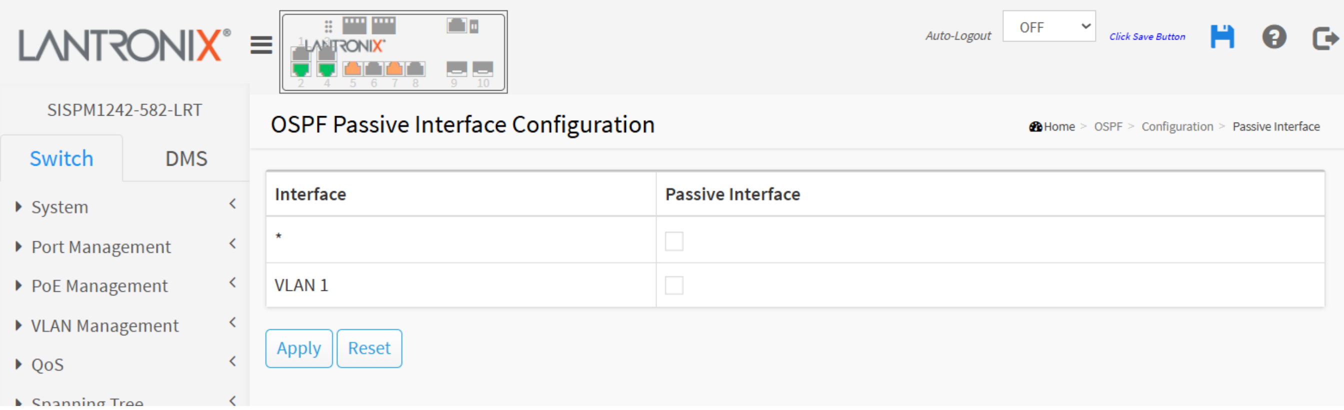
Area ID : Enter the OSPF area ID.

Passive Interface

This page provides the OSPF router passive interface configuration table. When enabled, this tells OSPF not to send hello packets on certain interfaces.

To configure the OSPF router passive interface:

5. Go to OSPF6 > Configuration > Passive Interface.
6. Configure the settings.
7. Click **Apply** to save the configuration.



OSPF Passive Interface Configuration

Interface	Passive Interface
*	□
VLAN 1	□

Parameter descriptions:

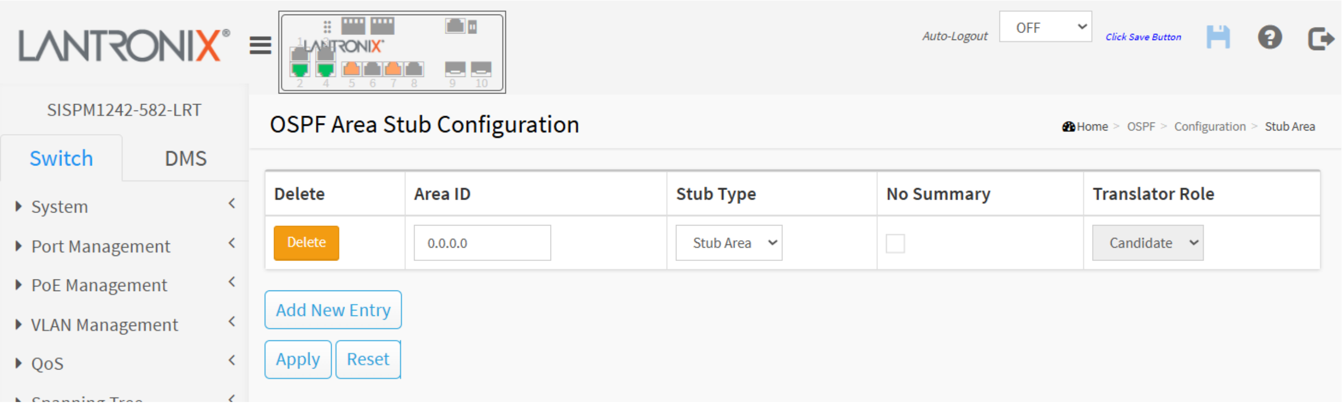
Interface : Interface identification.

Passive Interface : Enable the interface as OSPF passive-interface. When an interface is configured as a passive-interface, sending of OSPF routing updates is suppressed, so the interface does not establish adjacencies (no OSPF Hellos). The subnet of all interfaces (both passive and active) is advertised by the OSPF router.

Stub Area

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

1. Go to OSPF > Configuration > Stub Area.
2. Click **Add New Entry** to add a new entry to the table.
3. Configure the settings.
4. Click **Apply** to save the configuration.



OSPF Area Stub Configuration

Delete	Area ID	Stub Type	No Summary	Translator Role
Delete	0.0.0.0	Stub Area	□	Candidate

Parameter descriptions:

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

Add New Entry : Click to add a new entry to the table.

Area ID : The OSPF area ID.

Stub Type : The OSPF stub configured type.

- ***Stub Area***: Configure the area as stub area.
- ***NSSA***: Configure the area as not-so-stubby area (NSSA).

No Summary : The value is true to configure the inter-area routes do not inject into this stub area.

Translator Role : The OSPF NSSA translator role.

- ***Candidate***: this NSSA-ABR router will participate in the translator election (default).
- ***Never***: this NSSA-ABR router never translates.
- ***Always***: this NSSA-ABR router always translates.

See also:

OSPF v2: https://www.rfc-editor.org/rfc/pdfrfc/rfc2328.txt.pdf

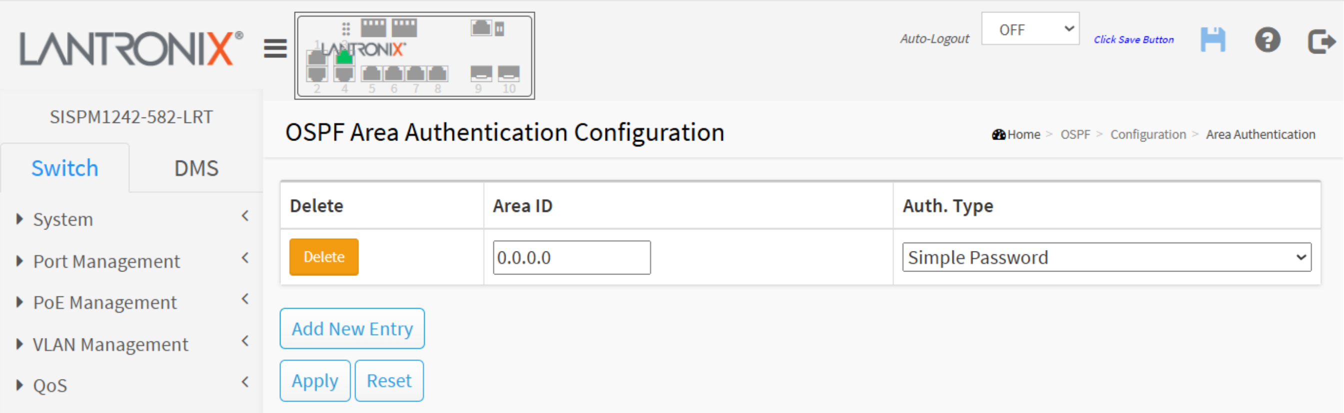
NSSA: https://datatracker.ietf.org/doc/html/rfc3101

Area Authentication

This page displays the OSPF Area Authentication Configuration table. It is used to apply the authentication to all the interfaces belonging to the area.

To configure Area Authentication:

1. Go to OSPF > Configuration > Area Authentication.
2. Click **Add New Entry** to add a new entry to the table.
3. Configure the settings.
4. Click **Apply** to save the configuration.



OSPF Area Authentication Configuration

Delete	Area ID	Auth. Type
Delete	0.0.0.0	Simple Password

Parameter Descriptions

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

Add New Entry : Click to add a new entry to the table.

Area ID : The OSPF area ID in the format 0.0.0.0.

Auth. Type : The authentication type on an area is applied to all the interfaces belong to that area.
The authentication type on an IP interface or a virtual link overrides the authentication type on an area and is useful if different interfaces in the same area use different authentication types. Specify the authentication type:

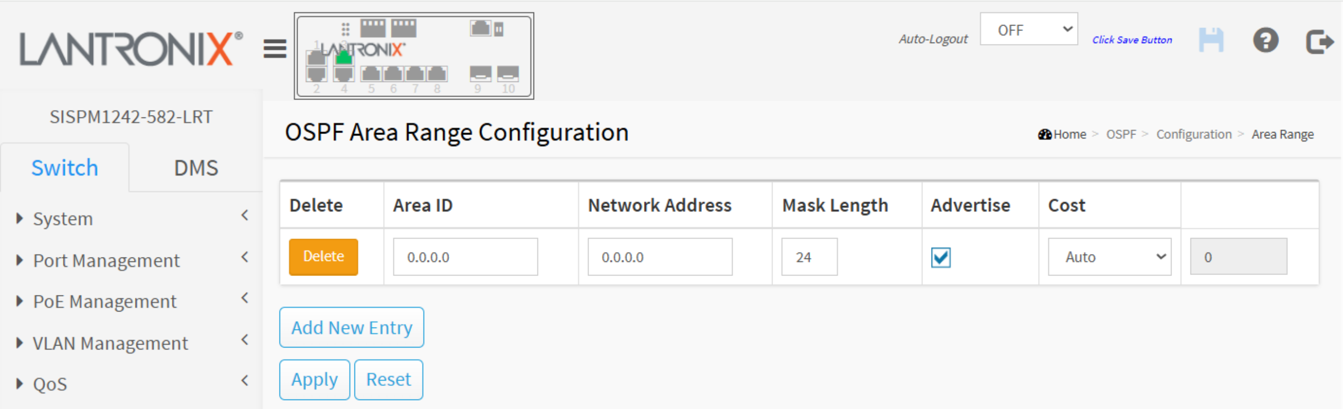
- ***Simple Password***: Simple password authentication (default).
- ***Message Digest***: MD5 digest authentication.

Area Range

This page displays the OSPF Area Range Configuration table. It is used to summarize the intra area paths from a specific address range in one summary-LSA (Type-3) and advertised to other areas or configure the address range status as '*DoNotAdvertise*' which the summary-LSA (Type-3) is suppressed.

The area range configuration is used for Area Border Routers (ABRs) and only router-LSAs (Type-1) and network-LSAs (Type-2) can be summarized. The AS-external-LSAs (Type-5) cannot be summarized because the scope is OSPF autonomous system (AS). The AS-external-LSAs (Type-7) cannot be summarized because the feature is not supported yet.

1. Go to OSPF > Configuration > Area Range.
2. Click **Add New Entry** to add a new entry to the table.
3. Configure the settings.
4. Click **Apply** to save the configuration.



OSPF Area Range Configuration

Delete	Area ID	Network Address	Mask Length	Advertise	Cost	
Delete	0.0.0.0	0.0.0.0	24	☑	Auto	0

Parameter descriptions:

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

Add New Entry : Click to add a new entry to the table.

Area ID : The OSPF area ID.

Network Address : The IPv4 network address.

Mask Length : The IPv4 network mask length.

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

Cost : User-specified cost (metric) for this summary route. The default setting is 'Auto' cost mode.

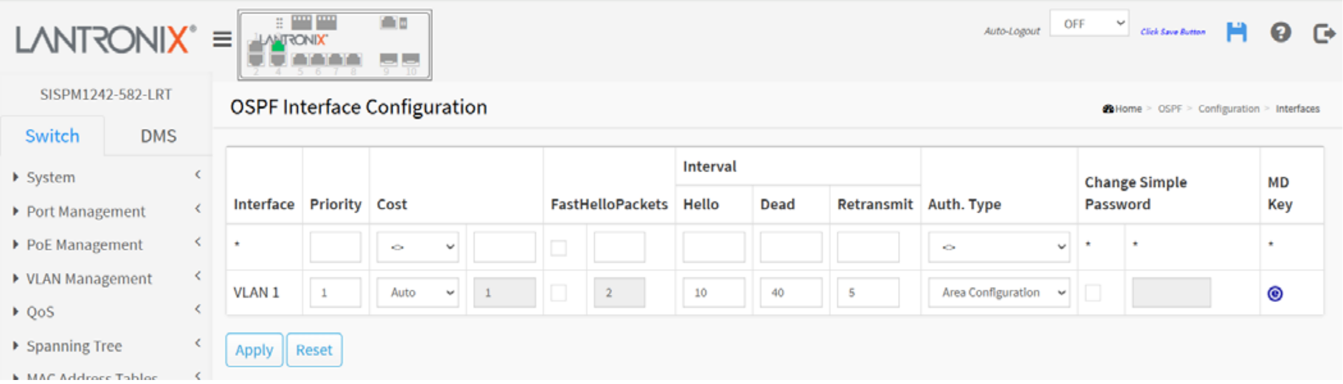
- ***Auto*** : When 'Auto' is selected, the cost value is set to 0 automatically and isn't allowed to be configured.
- ***Specific*** : When 'Specific' is selected the valid range is 0 to 16777215.

Interfaces

This page shows the OSPF Interface Configuration table.

To configure the OSPF Interface table:

5. Go to OSPF > Configuration > Interfaces.
6. Configure the settings.
7. Click **Apply** to save the configuration.



OSPF Interface Configuration

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

Apply Reset

Parameter descriptions:

Interface : Interface identification (e.g., VLAN1).

Priority : Specify a router priority for the interface. The valid range is 0 - 255; the default value is 1.

Cost : User specified cost for this interface (*Auto* or *Specific*); its link state metric for the interface. The field is significant only when '*IsSpecificCost'* is TRUE (when '*Specific'* is selected). The valid range is 1 - 65535 and the default setting is 'Auto' cost mode.

FastHelloPackets : How many Hello packets will be sent per second. The valid range is 1 - 10 and the default setting is disabled.

Hello Interval : How many Hello packets will be sent per second. The valid range is 1 - 65535 seconds and the default value is 10 seconds. OSPF uses Hello packets and two timers to check if a neighbor is still alive:

- ***Hello Interval*** defines how often the hello packet is sent.
- ***Dead Interval*** defines how long to wait for hello packets before declaring the neighbor dead.

The hello and dead interval values can be different based on the OSPF network type.

Dead Interval : The time interval (in seconds) between hello packets. The valid range is 1 - 65535 seconds and the default value is 40 seconds.

Retransmit Interval : The time interval (in seconds) between Link-State Advertisement (LSA) retransmissions for adjacencies. The valid range is 3 - 65535 seconds and the default value is 5 seconds.

Auth. Type : The authentication type:

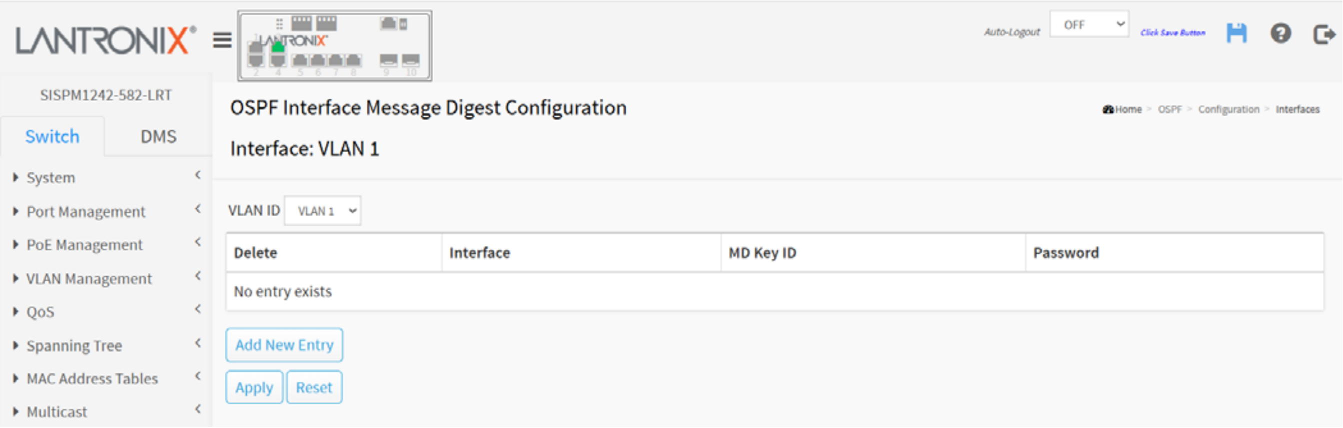
- ***Simple Password***: It's using a plain text authentication. A password must be configured, but a simple password can be read by a packet sniffer.
- ***Message Digest***: Its message-digest algorithm 5 (MD5) authentication. Keying material must also be configured. This is the most secure method.
- ***Null Authentication***: No authentication.
- ***Area Configuration***: See Area Authentication section.

Change Simple Password : Check the box to change the simple password (fill with plain text). The allowed input length is 1 - 8 characters.

MD Key : Click the Edit MD Key (ⓔ) icon to edit the Message Digest key.

Message Digest Configuration

This is the interface authentication message digest key configuration table. The listed entry sequence is ordered by the message digest key precedence.



OSPF Interface Message Digest Configuration

Interface: VLAN 1

VLAN ID: VLAN 1

Delete	Interface	MD Key ID	Password
No entry exists			

Parameter descriptions:

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

Add New Entry: Click to add a new entry.

Interface: Interface identification.

MD Key ID: The key ID for message digest authentication. The allowed range is 1 to 255.

Password: The message digest key. The allowed input length is 1 to 16 characters.

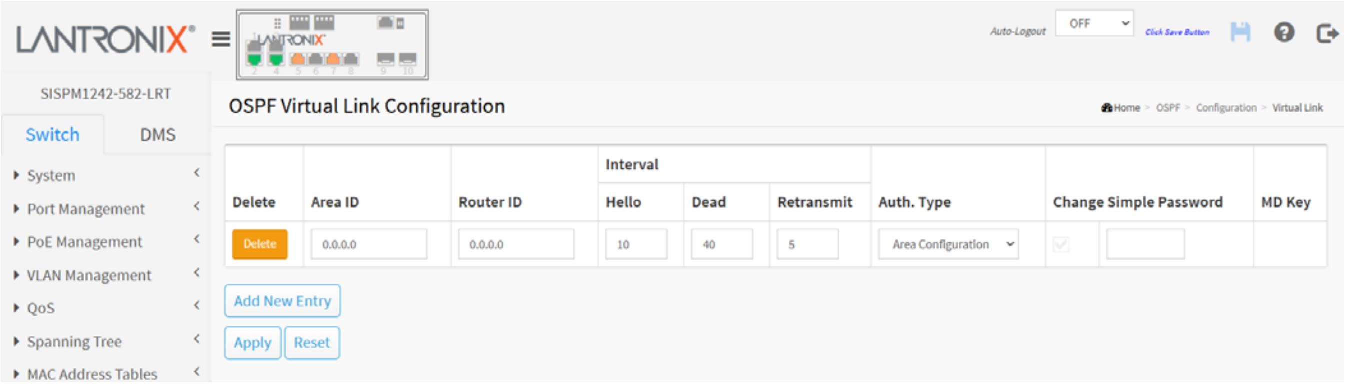
Virtual Link

This page shows the OSPF virtual link configuration table. The virtual link is established between two ABRs to overcome the fact that all the areas must be connected directly to the backbone area. The backbone must be contiguous, but it does not need to be physically contiguous. Backbone connectivity can be established and maintained by the configuration of “virtual links”.

Virtual links can be configured between any two backbone routers that have an interface to a common non-backbone area. Virtual links belong to the backbone. The protocol treats two routers joined by a virtual link as if they were connected by an unnumbered point-to-point backbone network. The routing protocol traffic that flows along the virtual link uses intra-area routing only.

To configure OSPF virtual link in the Web UI:

1. Go to OSPF > Configuration > Area Range.
2. Click **Add New Entry** to add a new entry to the table.
3. Configure the settings.
4. Click **Apply** to save the configuration.



OSPF Virtual Link Configuration

Delete	Area ID	Router ID	Interval			Auth. Type	Change Simple Password		MD Key
			Hello	Dead	Retransmit				
Delete	0.0.0.0	0.0.0.0	10	40	5	Area Configuration	□		

Add New Entry

Apply Reset

Parameter descriptions:

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

Add New Entry : Click to add a new entry to the table.

Area ID : The OSPF Area ID.

Router ID : The OSPF router ID.

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

OSPF uses Hello packets and two timers to check if a neighbor is still alive:

- ***Hello Interval*** defines how often the hello packet is sent.
- ***Dead Interval*** defines how long to wait for hello packets before declaring the neighbor dead.

The Hello and the Dead interval values can be different based on the OSPF network type.

Dead Interval : The number of seconds to wait until the neighbor is declared to be dead. The valid range is 1 to 65535 seconds and the default value is 40 seconds.

Retransmit Interval : The time interval (in seconds) between link-state advertisement (LSA) retransmissions for adjacencies. The valid range is 3 to 65535 and the default value is 5 seconds.

Auth. Type : The authentication type on an area.

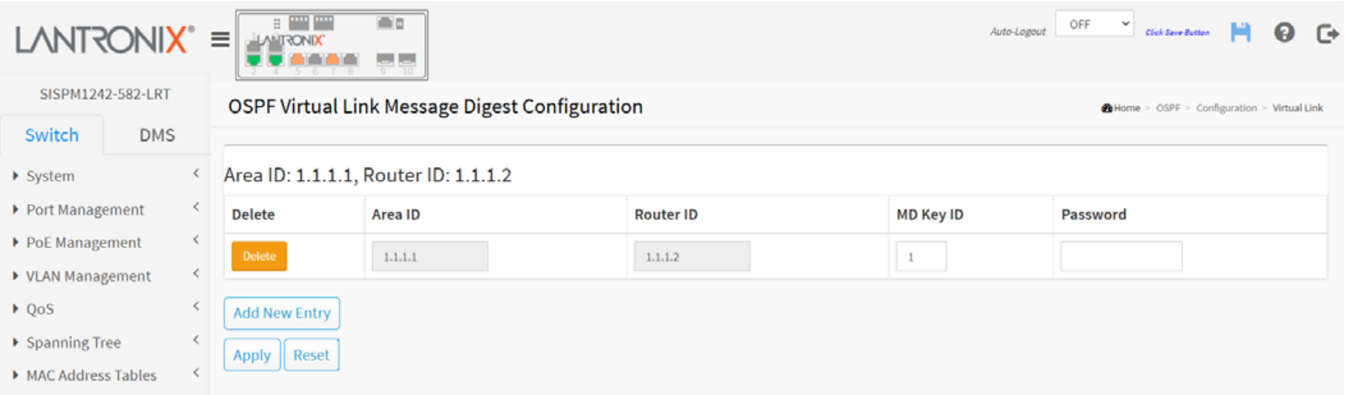
- ***Simple Password*** : It's using a plain text authentication. A password must be configured, but the password can be read by packet sniffers.
- ***Message Digest*** : It's Message-Digest algorithm 5 (MD5) authentication. Keying material must also be configured in the MD Key field. This is the most secure method.
- ***Null Authentication*** : No authentication.
- ***Area Configuration***: See Area Authentication section.

Change Simple Password : It is used to change the simple password (fill with plain text). The allowed input length is 1 to 8 characters. You can hide or show the displayed text.

MD Key : Click the (e) icon to edit the Message Digest key for the entry. This parameter only applies if Message Digest was selected at the Auth. Type dropdown.

Message Digest Key Configuration

This is OSPF virtual link configuration table. The virtual link is established between 2 ABRs to overcome that all the areas must be connected directly to the backbone area. The listed entry sequence is ordered by the message digest key precedence.



OSPF Virtual Link Message Digest Configuration

Area ID: 1.1.1.1, Router ID: 1.1.1.2

Delete	Area ID	Router ID	MD Key ID	Password
Delete	1.1.1.1	1.1.1.2	1	

Add New Entry

Apply Reset

Parameter descriptions:

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

Add New Entry : Click to add a new entry to the table.

Area ID: The OSPF Area ID.

Router ID: The OSPF router ID.

MD Key ID: The key ID for message digest authentication. The allowed range is 1 to 255.

Password: The password of the message digest key, it is the plain text input field for the new entry. The allowed input length is 1 to 16.

Status

The OSPF Status menu provides information for the following status pages:

- **Global status** – OSPF router status information
- **Area status** – OSPF network area status information
- **Neighbor status** – OSPF IPv4 neighbors status information
- **Interface status** – OSPF interface status information
- **Routing** – OSPF routing status information
- **General Database** – OSPF link state database
- **Router** – OSPF router link state database
- **Network** – OSPF LSA link state database
- **Summary** – OSPF summary link state database
- **ASBR Summary** – OSPF ASBR summary link state database
- **External** – OSPF external link state database
- **NSSA External** – OSPF NSSA external link state database

Please refer to the online help pages for parameter descriptions of the OSPF Status pages.

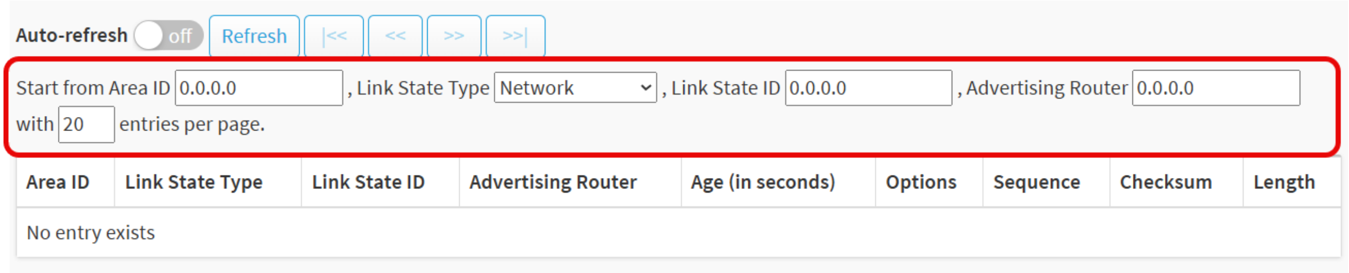
Navigating the Status Tables

Several of the status table pages provide navigational controls to let you change the starting point in the table.

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

The "Start from Area ID" input field allows the user to change the starting point in this table. Clicking the **Refresh** button will update the displayed table starting from that or the closest next entry match. In addition, by clicking the **Refresh** button, these input fields will assume the value of the first displayed entry, allowing for continuous refresh with the same start input field.

Example page:



Start from Area ID 0.0.0.0 , Link State Type Network , Link State ID 0.0.0.0 , Advertising Router 0.0.0.0
with 20 entries per page.

Area ID	Link State Type	Link State ID	Advertising Router	Age (in seconds)	Options	Sequence	Checksum	Length
No entry exists								

Additional Navigational Controls

|<< : Updates the table entries, starting from the first available entry. If the first entry of the table is displayed, the button is disabled

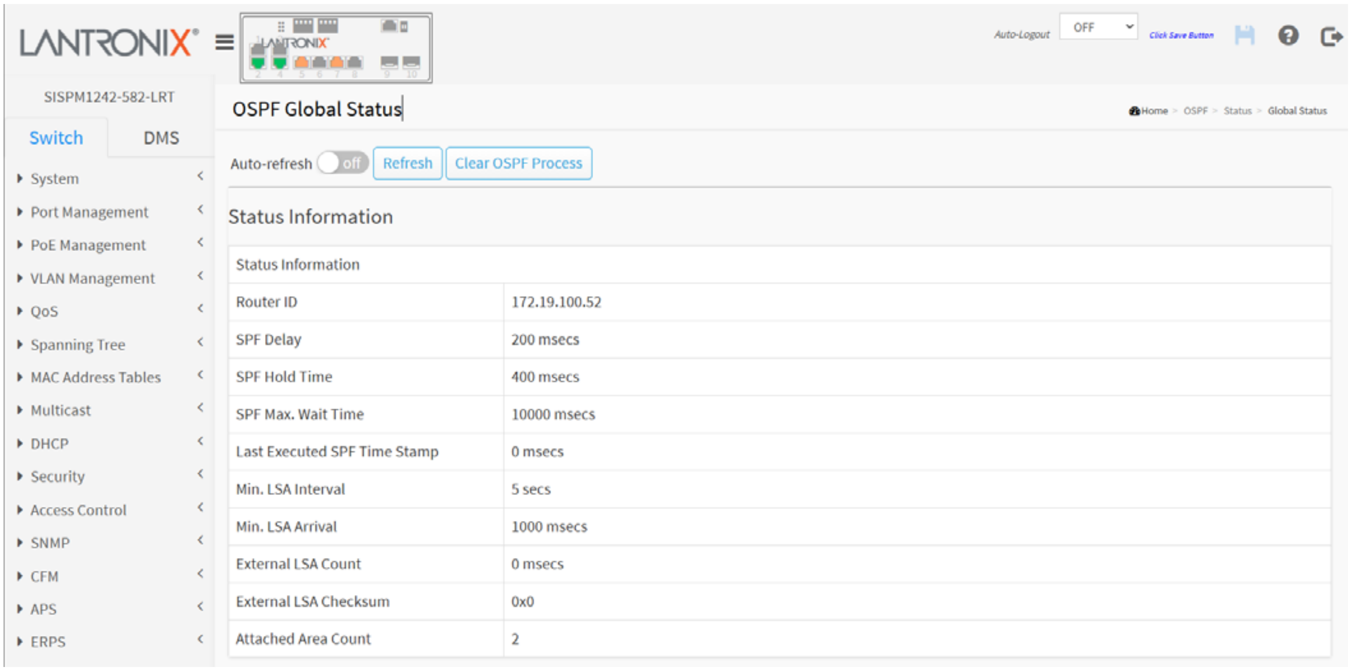
<< : Updates the table entries, ending at the entry prior to the first entry currently displayed. If the first entry of the table is displayed, the button is disabled

>> : Updates the table entries, starting from the entry next to the last entry currently displayed. If the last entry of the table is displayed, the button is disabled.

>>| : Updates the table entries, ending at the last available entry. If the last entry of the table is displayed, the button is disabled.

Global Status

This page shows the OSPF router Global Status. It is used to provide OSPF router status information.



OSPF Global Status

Status Information

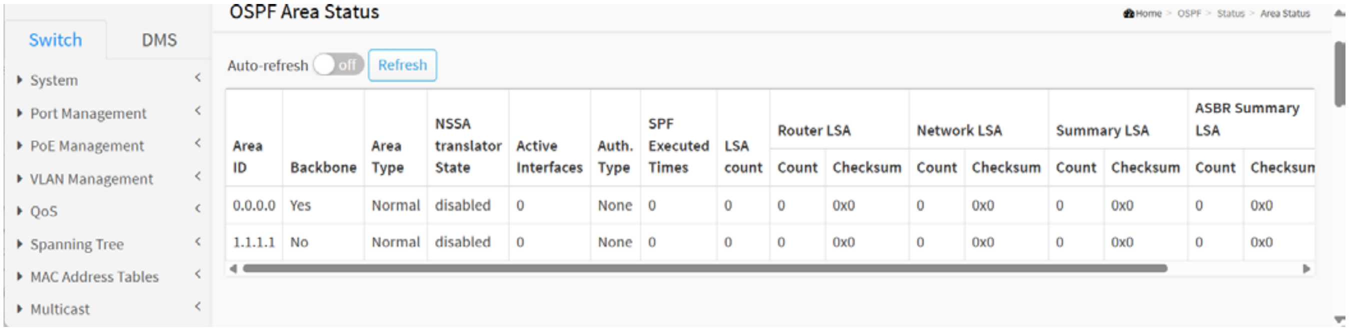
Status Information	
Router ID	172.19.100.52
SPF Delay	200 msecs
SPF Hold Time	400 msecs
SPF Max. Wait Time	10000 msecs
Last Executed SPF Time Stamp	0 msecs
Min. LSA Interval	5 secs
Min. LSA Arrival	1000 msecs
External LSA Count	0 msecs
External LSA Checksum	0x0
Attached Area Count	2

Parameter Descriptions

Please refer to the online help page for parameter descriptions for this page.

Area Status

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



OSPF Area Status

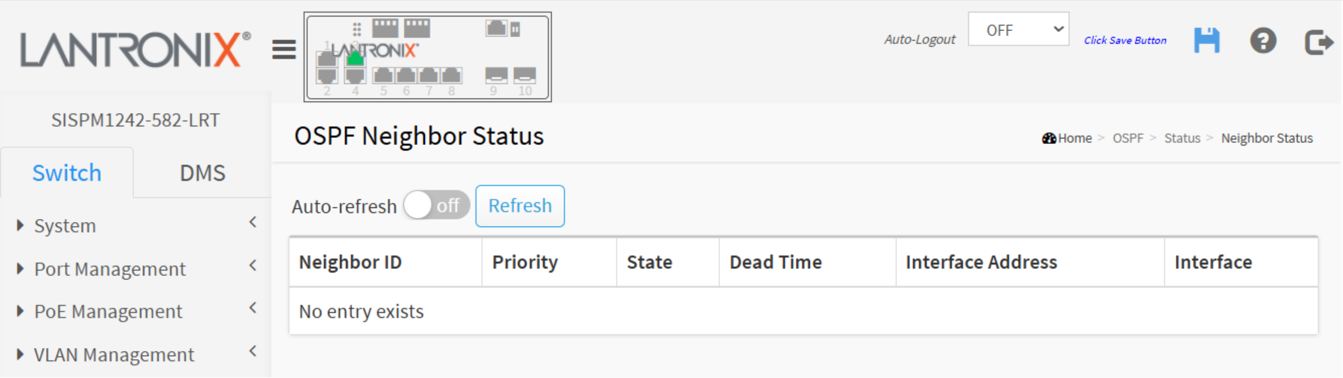
Area ID	Backbone	Area Type	NSSA translator State	Active Interfaces	Auth. Type	SPF Executed Times	LSA count	Router LSA		Network LSA		Summary LSA		ASBR Summary LSA	
								Count	Checksum	Count	Checksum	Count	Checksum	Count	Checksun
0.0.0.0	Yes	Normal	disabled	0	None	0	0	0	0x0	0	0x0	0	0x0	0	0x0
1.1.1.1	No	Normal	disabled	0	None	0	0	0	0x0	0	0x0	0	0x0	0	0x0

Parameter Descriptions

Please refer to the online help page for parameter descriptions for this page.

Neighbor Status

This page displays the OSPF IPv4 Neighbor Status table. It is used to provide the OSPF neighbor status information.



OSPF Neighbor Status

Auto-refresh off Refresh

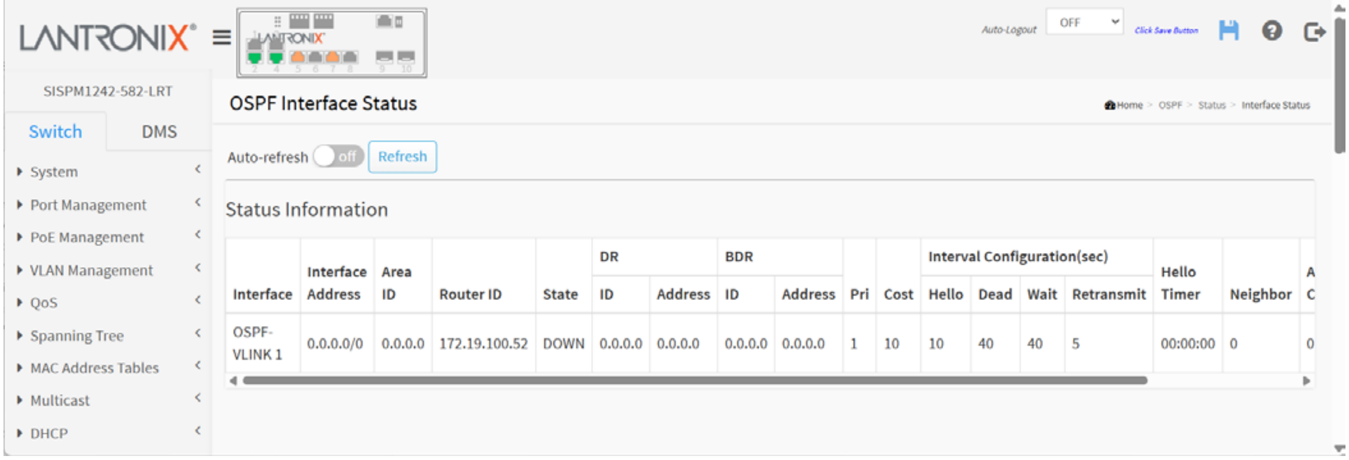
Neighbor ID	Priority	State	Dead Time	Interface Address	Interface
No entry exists					

Parameter Descriptions

Please refer to the online help page for parameter descriptions for this page.

Interface Status

This page displays the OSPF interface status table. It is used to provide the OSPF interface status information.



OSPF Interface Status

Auto-refresh off Refresh

Status Information

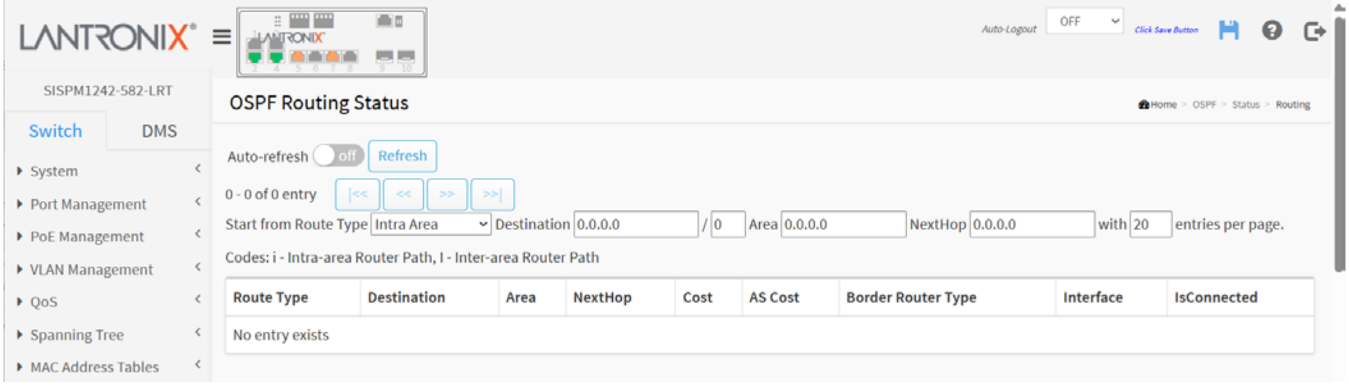
Interface	Interface Address	Area ID	Router ID	State	DR		BDR		Pri	Cost	Interval Configuration(sec)				Hello Timer	Neighbor	A C
					ID	Address	ID	Address			Hello	Dead	Wait	Retransmit			
OSPF-VLINK 1	0.0.0.0/0	0.0.0.0	172.19.100.52	DOWN	0.0.0.0	0.0.0.0	0.0.0.0	0.0.0.0	1	10	10	40	40	5	00:00:00	0	0

Parameter Descriptions

Please refer to the online help page for parameter descriptions for this page.

Routing Status

This page displays the OSPF routing status table. It is used to provide the OSPF routing status information.



OSPF Routing Status

Auto-refresh off

0 - 0 of 0 entry

Start from Route Type Intra Area Destination 0.0.0.0 / 0 Area 0.0.0.0 NextHop 0.0.0.0 with 20 entries per page.

Codes: i - Intra-area Router Path, I - Inter-area Router Path

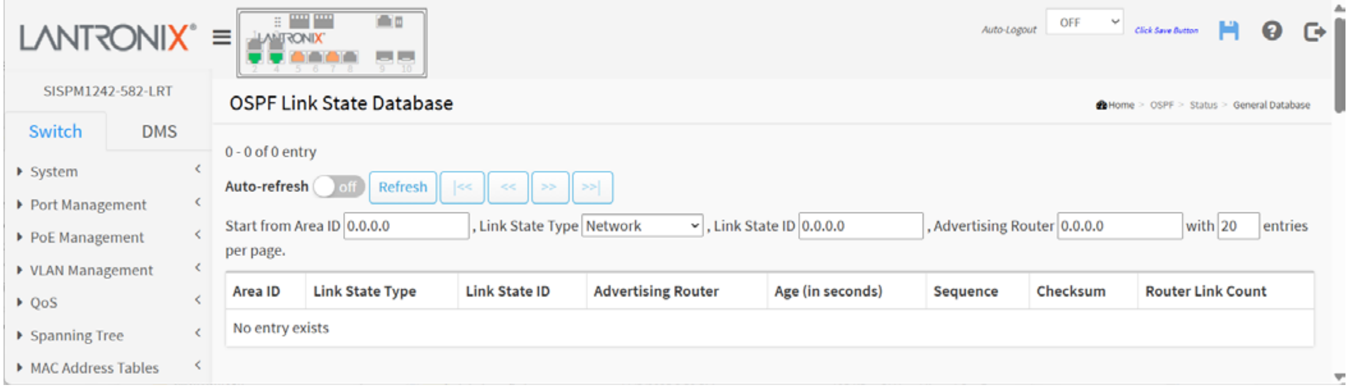
Route Type	Destination	Area	NextHop	Cost	AS Cost	Border Router Type	Interface	IsConnected
No entry exists								

Parameter Descriptions

Please refer to the online help page for parameter descriptions for this page.

General Database

This page displays the OSPF LSA link state database information table.



OSPF Link State Database

0 - 0 of 0 entry

Auto-refresh off

Start from Area ID 0.0.0.0 , Link State Type Network , Link State ID 0.0.0.0 , Advertising Router 0.0.0.0 with 20 entries per page.

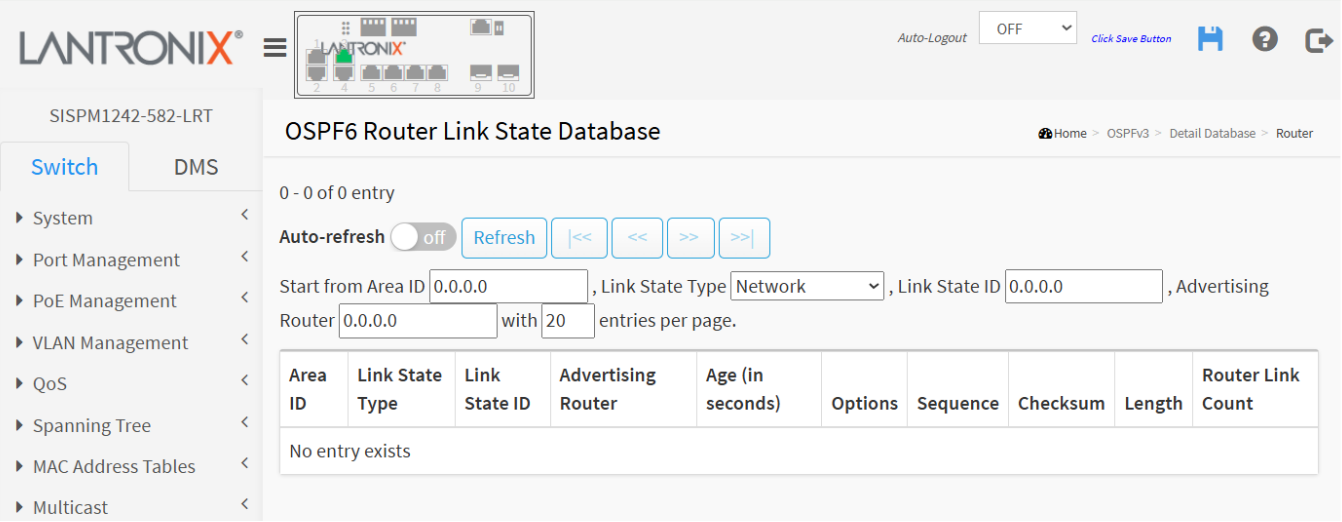
Area ID	Link State Type	Link State ID	Advertising Router	Age (in seconds)	Sequence	Checksum	Router Link Count
No entry exists							

Parameter Descriptions

Please refer to the online help page for parameter descriptions for this page.

Router

This page displays the OSPF LSA Router link state database information table.



OSPF6 Router Link State Database

0 - 0 of 0 entry

Auto-refresh off

Start from Area ID 0.0.0.0 , Link State Type Network , Link State ID 0.0.0.0 , Advertising Router 0.0.0.0 with 20 entries per page.

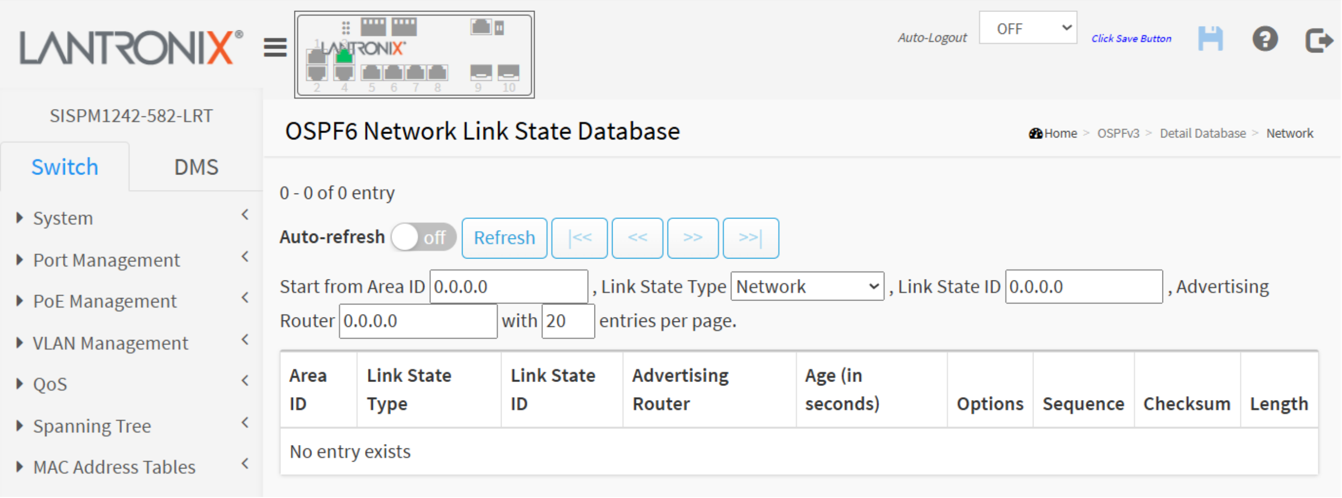
Area ID	Link State Type	Link State ID	Advertising Router	Age (in seconds)	Options	Sequence	Checksum	Length	Router Link Count
No entry exists									

Parameter Descriptions

Please refer to the online help page for parameter descriptions for this page.

Network

This page displays the OSPF LSA Network link state database information table.



OSPF6 Network Link State Database

0 - 0 of 0 entry

Auto-refresh off

Start from Area ID 0.0.0.0 , Link State Type Network , Link State ID 0.0.0.0 , Advertising Router 0.0.0.0 with 20 entries per page.

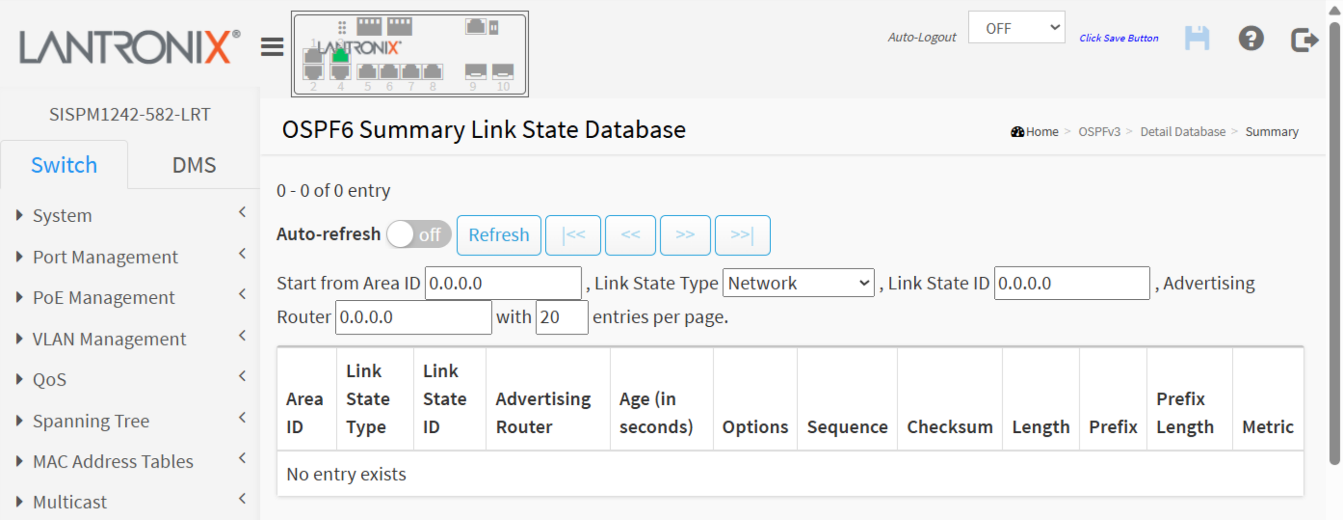
Area ID	Link State Type	Link State ID	Advertising Router	Age (in seconds)	Options	Sequence	Checksum	Length
No entry exists								

Parameter Descriptions

Please refer to the online help page for parameter descriptions for this page.

Summary

This page displays the OSPF LSA Summary link state database information table.



OSPF6 Summary Link State Database

0 - 0 of 0 entry

Auto-refresh off

Start from Area ID 0.0.0.0 , Link State Type Network , Link State ID 0.0.0.0 , Advertising Router 0.0.0.0 with 20 entries per page.

Area ID	Link State Type	Link State ID	Advertising Router	Age (in seconds)	Options	Sequence	Checksum	Length	Prefix	Prefix Length	Metric
No entry exists											

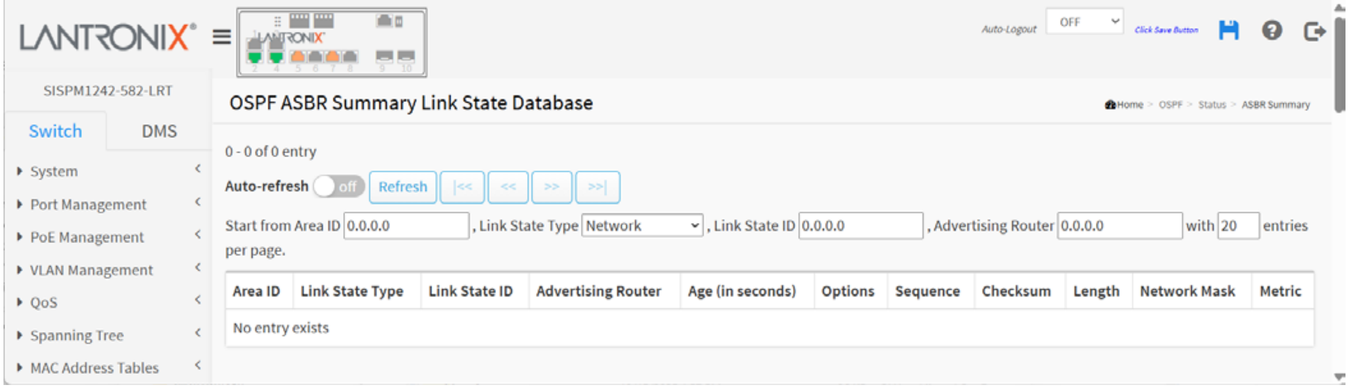
Parameter Descriptions

Please refer to the online help page for parameter descriptions for this page.

ASBR Summary

This page displays the OSPF LSA ASBR Summary link state database information table.

An Autonomous System Boundary Router (ASBR) is a router that is running multiple protocols and serves as a gateway to routers outside the OSPF domain and to those operating with different protocols. The ASBR can import and translate different protocol routes into OSPF through a process known as ‘redistribution’.



OSPF ASBR Summary Link State Database

0 - 0 of 0 entry

Auto-refresh off

Start from Area ID 0.0.0.0 , Link State Type Network , Link State ID 0.0.0.0 , Advertising Router 0.0.0.0 with 20 entries per page.

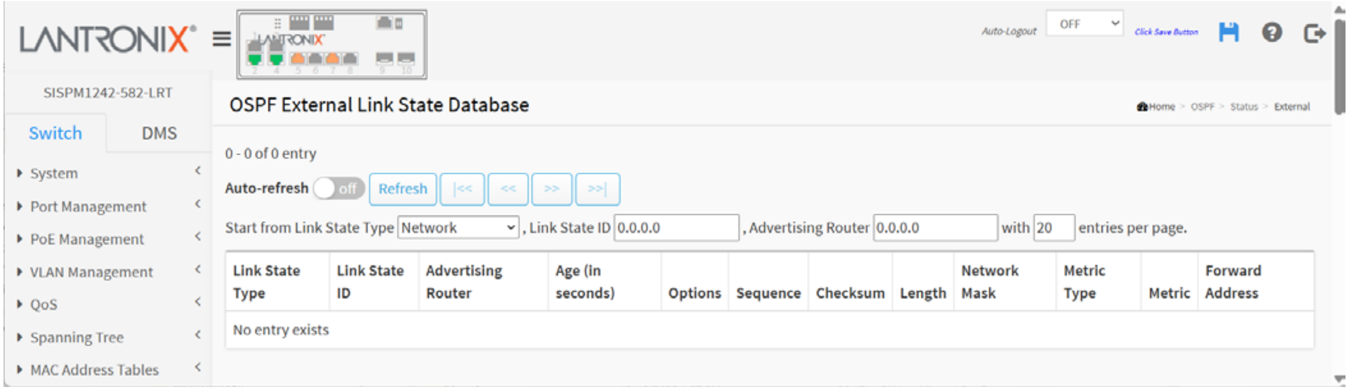
Area ID	Link State Type	Link State ID	Advertising Router	Age (in seconds)	Options	Sequence	Checksum	Length	Network Mask	Metric
No entry exists										

Parameter Descriptions

Please refer to the online help page for parameter descriptions for this page.

External

This page displays the OSPF LSA External link state database information table.



OSPF External Link State Database

0 - 0 of 0 entry

Auto-refresh off

Start from Link State Type Network , Link State ID 0.0.0.0 , Advertising Router 0.0.0.0 with 20 entries per page.

Link State Type	Link State ID	Advertising Router	Age (in seconds)	Options	Sequence	Checksum	Length	Network Mask	Metric Type	Metric	Forward Address
No entry exists											

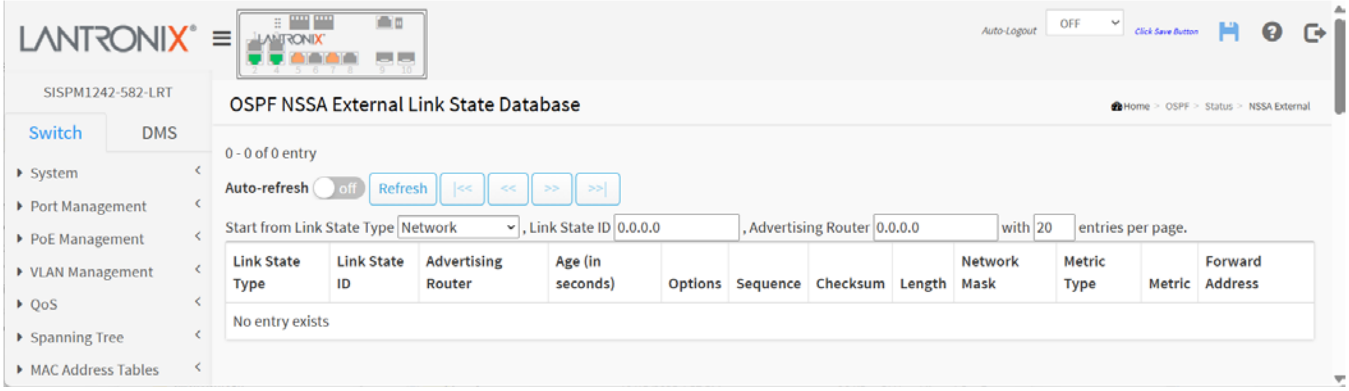
Parameter Descriptions

Please refer to the online help page for parameter descriptions for this page.

NSSA External

This page displays the OSPF LSA NSSA External link state database information table. An NSSA (not-so-stubby area) has the capability of importing external routes in a limited fashion.

Proper operation of the OSPF protocol requires that all OSPF routers maintain an identical copy of the OSPF link state database. But when the LDSB size becomes too large, some routers may not be able to keep the entire database due to resource shortages. This is called "database overflow". When this is anticipated, routers with limited resources can be accommodated by configuring OSPF stub areas and NSSAs. See IETF RFC 3101 for more information.



OSPF NSSA External Link State Database

0 - 0 of 0 entry

Auto-refresh off

Start from Link State Type Network , Link State ID 0.0.0.0 , Advertising Router 0.0.0.0 with 20 entries per page.

Link State Type	Link State ID	Advertising Router	Age (in seconds)	Options	Sequence	Checksum	Length	Network Mask	Metric Type	Metric	Forward Address
No entry exists											

Parameter Descriptions

Please refer to the online help page for parameter descriptions for this page.

Troubleshooting OSPF

1. Verify that Hello and Dead timers match on each end of the link
2. Verify that the link is up. Ping the other end of the link.
3. Make sure that the interfaces at both ends are configured to support OSPF.
4. Check for a mismatch in the OSPF Network Type.
5. Verify that Neighboring interfaces are in the same OSPF Area.
6. If the device is in more than one area, then it must have at least one interface in Area 0.
7. OSPF Area IDs: When using multiple network area statements in the OSPF configuration, the order of the statements is critical. Check that the networks have been assigned the desired area IDs by checking the output of the `show ip ospf interface` command.
8. OSPF Does Not Start: The OSPF process cannot start on a router if a router ID cannot be established. Check the output of `show ip ospf` to see if a router ID has been established. If a router ID has not been established, check to see if the router has an active interface (preferably a loopback interface) with an IP address.
9. Verify Neighbor relationships: Once a router can start OSPF, it establishes an interface data structure for each interface configured to run OSPF. Check the output of `show ip ospf interface` to ensure that OSPF is active on the intended interfaces. If OSPF is active, check for an incorrectly configured interface.
10. Check if there is an entry in the OSPF Database for a particular external route, but it is not showing in the routing table. Check the Forwarding Address associated with the route.

24. OSPFv3

OSPF for IPv6 is described in IETF RFC 2740. The fundamental mechanisms of OSPF (flooding, DR election, area support, SPF calculations, etc.) remain unchanged from OSPF for IPv4. However, some changes have been necessary, either due to changes in protocol semantics between IPv4 and IPv6, or simply to handle the increased address size of IPv6.

All OSPF for IPv4's optional capabilities, including on-demand circuit support, NSSA areas, and the multicast extensions to OSPF are also supported in OSPF for IPv6. OSPF for IPv6 runs per-link instead of the IPv4 behavior of per-IP-subnet.

Configuration

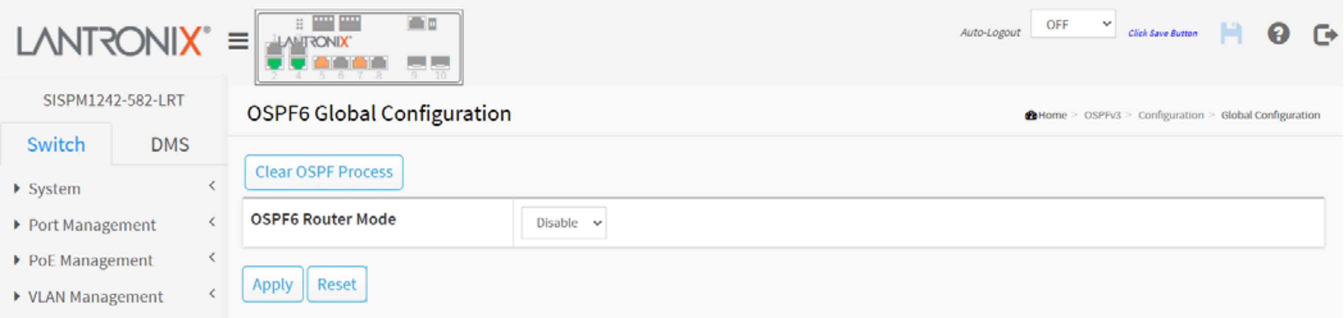
Global Configuration

This page displays the OSPF6 Global Configuration table. It is a general group to configure the OSPF6 common router parameters.

OSPFv3 is the Open Shortest Path First routing protocol for IPv6. It is like OSPFv2 in its concept of a link state database, intra- and inter-area, and AS external routes and virtual links.

To configure the OSPF6 global configuration:

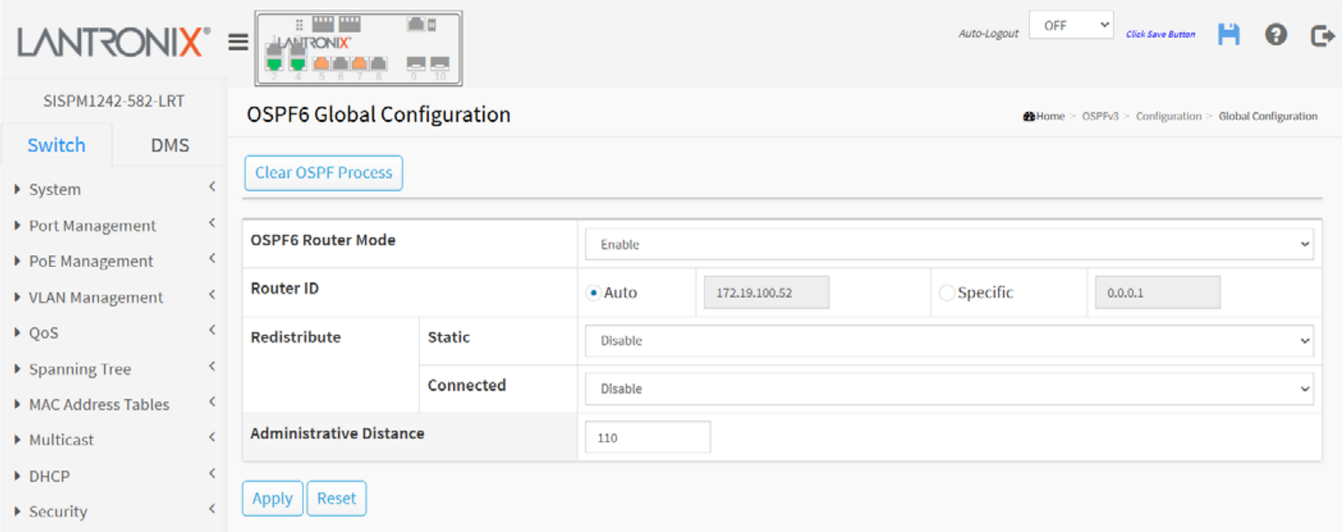
1. Go to OSPFv3 > Configuration > Global Configuration.



OSPF6 Global Configuration

OSPF6 Router Mode	Disable

2. You may need to click **Clear OSPF Process** to reset the current process.
3. Enable the OSPF6 Router Mode.
4. Click **Apply** to save the mode change. The page will expand to show the configurable parameters.



OSPF6 Global Configuration

OSPF6 Router Mode		Enable			
Router ID		● Auto	172.19.100.52	○ Specific	0.0.0.1
Redistribute	Static	Disable			
	Connected	Disable			
Administrative Distance		110			

5. Enter the settings.
6. Click **Apply** to save the new configuration.

Parameter descriptions:

Clear OSPF Process : Click to reset the current OSPF6 process.

OSPF6 Router Mode : Enable or Disable the OSPF6 router mode.

Router ID : The OSPF6 Router ID in IPv4 address format (A.B.C.D). When the router's OSPF6 Router ID is changed, if there is one or more fully adjacent neighbors in the current OSPF6 area, the new router ID will take effect after restart OSPF6 process. **Note** that the router ID should be unique in the Autonomous System and that the value '0.0.0.0' is invalid since it is reserved for the default algorithm.

- ***Auto***: The default algorithm will choose the largest IP address assigned to the router.
- ***Specific***: User specified router ID. The valid range is from 0.0.0.1 to 255.255.255.254.

Static Redistribute : Whether the OSPF redistribute function is enabled for the static routes. Static routes are manually-defined (remote) routes.

- ***Enable***: The static routes are redistributed.
- ***Disable***: The static routes are not redistributed

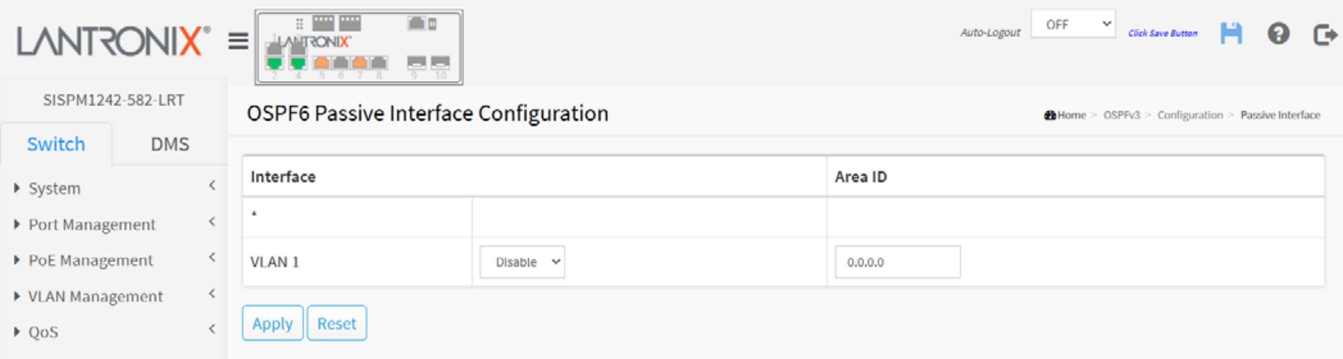
Connected Redistribute : The OSPF redistribute enabled for connected route or not. Connected = RIP routes that correspond to defined IP interfaces on which RIP is not enabled (defined locally). By default, the RIP Routing Table only includes routes that correspond to IP interfaces on which RIP is enabled.

- ***Enable***: The connected interfaces are redistributed.
- ***Disable***: The connected interfaces are not redistributed (the default setting).

Administrative Distance : The OSPF6 administrative distance in hops.

Passive Interface

This page displays the OSPF6 passive interface configuration table. When enabled, this tells OSPF not to send hello packets on certain interfaces.



OSPF6 Passive Interface Configuration

Interface		Area ID
*		
VLAN 1	Disable	0.0.0.0

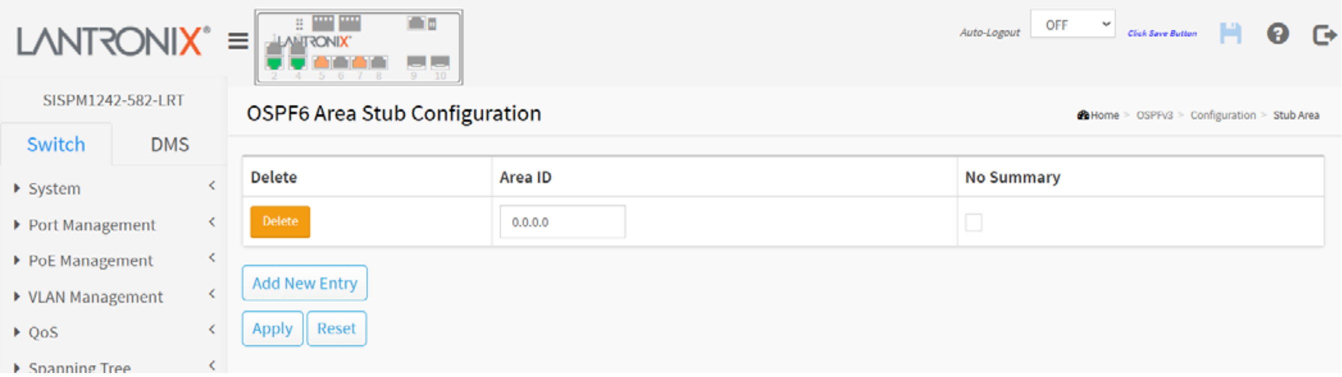
Parameter descriptions:

Interface : Interface identification. For each interface (e.g., VLAN 1) select Enable at the dropdown.

Area ID : The OSPF6 interface Area ID. Only valid if Router ID *'is_specific_id'* is true (Router ID set to “Specific” as described in the “OSPF6 Global Configuration” section above).

Stub Area

This page displays the OSPF6 area stub configuration table. The configuration is used to reduce the link-state database size and therefore reduce memory and CPU requirement by forbidding some LSAs.



OSPF6 Area Stub Configuration

Delete	Area ID	No Summary
Delete	0.0.0.0	□

Parameter descriptions:

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

Add New Entry : Click to add a new entry to the table.

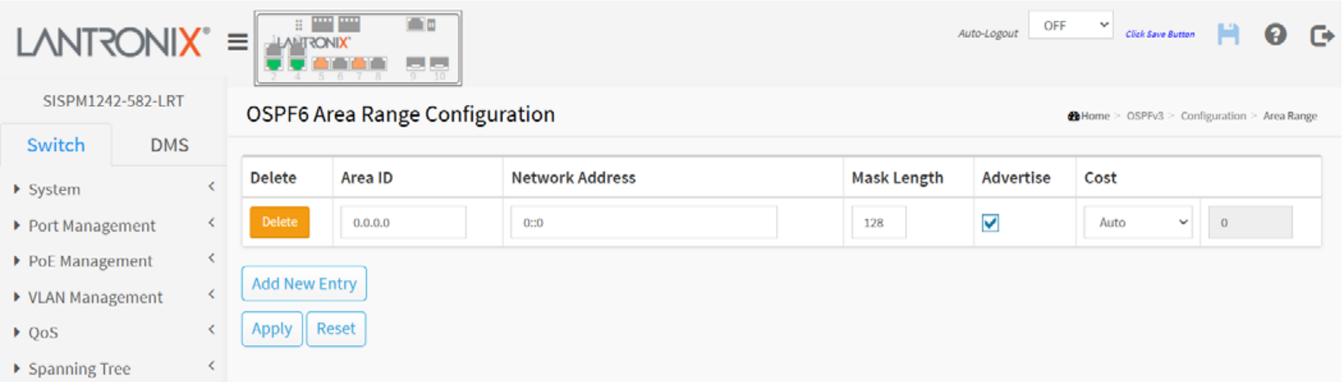
Area ID : The OSPF6 area ID.

No Summary : The value is true (checkbox checked) to configure the inter-area routes to not inject into this stub area.

Area Range

This page displays the OSPF6 area range configuration table. It is used to summarize the intra area paths from a specific address range in one summary-LSA(Type-0x2003) and advertised to other areas or configure the address range status as '*DoNotAdvertise*' which the summary-LSA (Type-0x2003) is suppressed. The area range configuration is used for Area Border Routers (ABRs) and only router-LSAs (Type-0x2001) and network-LSAs (Type-0x2002) can be summarized.

AS-external-LSAs (Type-0x4005) cannot be summarized because the scope is OSPF6 autonomous system (AS). AS-external-LSAs (Type-0x4007) cannot be summarized because the feature is not supported yet.



OSPF6 Area Range Configuration

Delete	Area ID	Network Address	Mask Length	Advertise	Cost	
Delete	0.0.0.0	0::0	128	☑	Auto	0

Parameter descriptions:

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

Add New Entry : Click to add a new entry to the table.

Area ID : The OSPF6 area ID.

Network Address : IPv6 network address.

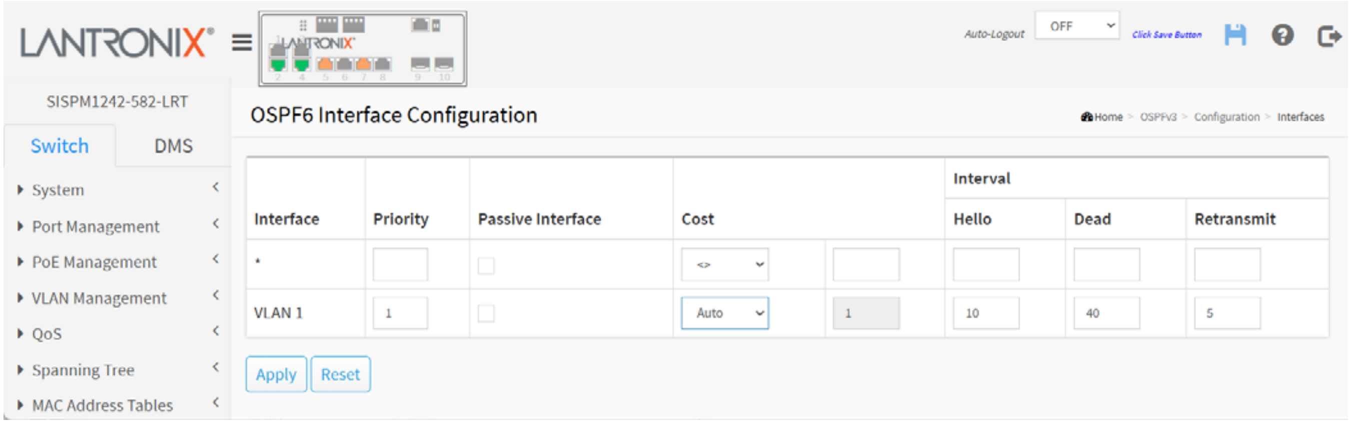
Mask Length : IPv6 network mask length.

Advertise : When the value is true, it summarizes intra-area paths from the address range in one Inter-Area Prefix LSA (Type-0x2003) and advertised to other areas. Otherwise, the intra-area paths from the address range are not advertised to other areas.

Cost : User-specified cost (or metric) for this summary route. It can be configured only when 'Specific' is selected, then the valid range is 0 to 16777215. The default setting is 'Auto’ cost mode. When 'Auto' is selected, the cost value is set to 0 automatically and isn't allowed to be configured.

Interfaces

This page displays the interface configuration table.



OSPF6 Interface Configuration

Interface	Priority	Passive Interface	Cost		Interval		
					Hello	Dead	Retransmit
*		□	<>				
VLAN 1	1	□	Auto	1	10	40	5

Parameter descriptions:

Interface : Interface identification.

Priority : User-specified router priority for the interface. The valid range is 0 - 255 and the default is 1.

Passive Interface : Check the box to indicate that the interface is passive.

Cost : Select Automatic or User-specified cost for this interface. It's the link state metric for the interface. This field is only configurable if Cost is set to Specific, then the valid range is 1 - 65535.
The default setting is 'Auto' cost mode.

Hello Interval : The number of Hello packets to be sent per second. The valid range is 1 - 65535 and the default value is 10 per second.

OSPF uses Hello packets and two timers to check if a neighbor is still alive:

> ***Hello Interval*** defines how often the hello packet is sent.
>
> ***Dead Interval*** defines how long to wait for hello packets before declaring the neighbor dead.

The hello and dead interval values can be different based on the OSPF network type.

Dead Interval : The time interval (in seconds) between hello packets. The valid range is 1 - 65535 seconds and the default value is 40 seconds.

Retransmit Interval : The time interval (in seconds) between link-state advertisement (LSA) retransmissions for adjacencies. The valid range is 3 - 65535 seconds and the default value is 5 seconds.

Status

The OSPFv3 Status menu provides information for the following status pages:

- **Global status** – OSPF6 router status information
- **Area status** – OSPF6 network area status information
- **Neighbor status** – OSPF6 neighbors status information
- **Interface status** – OSPF6 interface status information
- **Routing** – OSPF6 routing status information
- **General Database** – OSPF6 link state database
- **Detail Database / Router** – OSPF6 router link state database
- **Detail Database / Network** – OSPF6 LSA link state database
- **Detail Database / Link** – OSPF6 link state database
- **Detail Database / IntraAreaPrefix –** OSPF6 LSA Inter Area Prefix link state database
- **Detail Database / ASBR Summary** – OSPF6 ASBR summary link state database
- **Detail Database / External** – OSPF6 external link state database

Please refer to the online help pages for parameter descriptions of the OSPF6 Status pages.

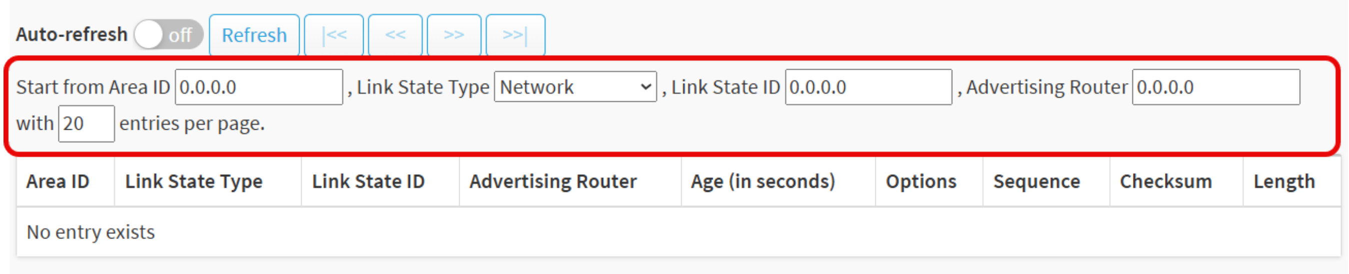
Navigating the Status Tables

Several of the status table pages provide navigational controls to let you change the starting point in the table.

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

The “Start from Area ID” input field allows the user to change the starting point in this table. Clicking the **Refresh** button will update the displayed table starting from that or the closest next entry match. In addition, by clicking the **Refresh** button, these input fields will assume the value of the first displayed entry, allowing for continuous refresh with the same start input field.

Example page:



Start from Area ID 0.0.0.0 , Link State Type Network , Link State ID 0.0.0.0 , Advertising Router 0.0.0.0
with 20 entries per page.

Area ID	Link State Type	Link State ID	Advertising Router	Age (in seconds)	Options	Sequence	Checksum	Length
No entry exists								

Additional Navigational Controls

|<< : Updates the table entries, starting from the first available entry. If the first entry of the table is displayed, the button is disabled

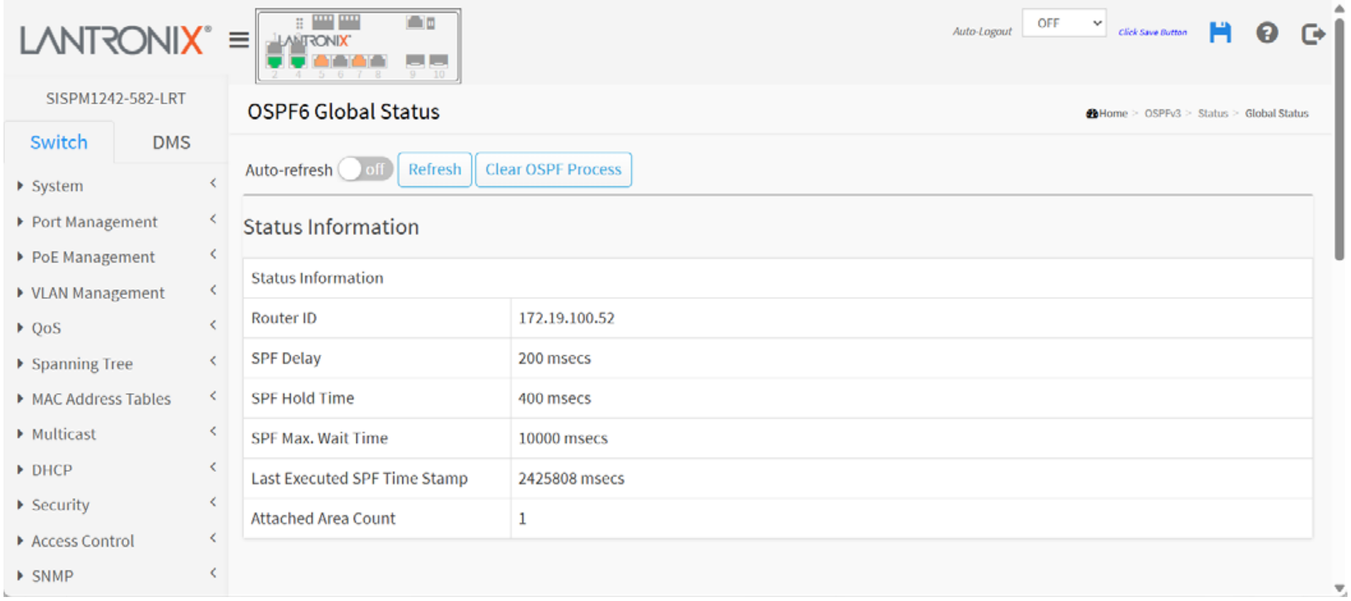
<< : Updates the table entries, ending at the entry prior to the first entry currently displayed. If the first entry of the table is displayed, the button is disabled

>> : Updates the table entries, starting from the entry next to the last entry currently displayed. If the last entry of the table is displayed, the button is disabled.

>>| : Updates the table entries, ending at the last available entry. If the last entry of the table is displayed, the button is disabled.

Global Status

This page displays the OSPF6 router status table. It is used to provide the OSPF6 router status information.



OSPF6 Global Status

Status Information

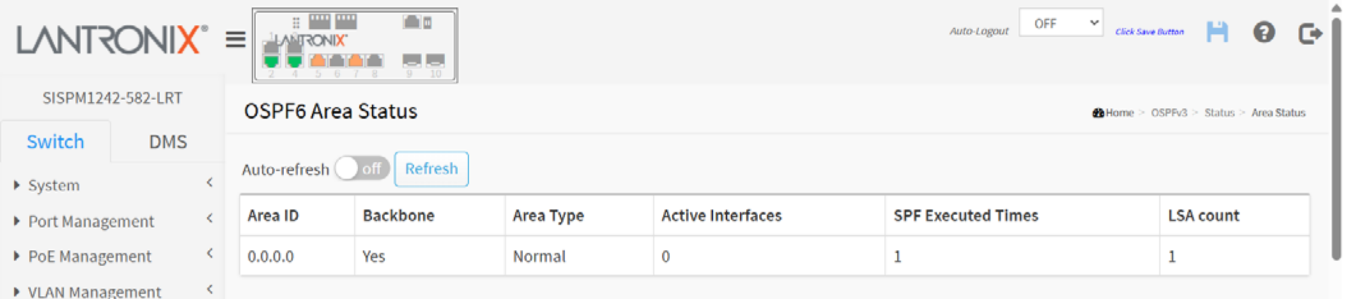
Status Information	
Router ID	172.19.100.52
SPF Delay	200 msecs
SPF Hold Time	400 msecs
SPF Max. Wait Time	10000 msecs
Last Executed SPF Time Stamp	2425808 msecs
Attached Area Count	1

Parameter Descriptions

Please refer to the online help page for parameter descriptions for this page.

Area Status

This page displays the OSPF6 network area status table, which provides OSPF6 network area status information.



OSPF6 Area Status

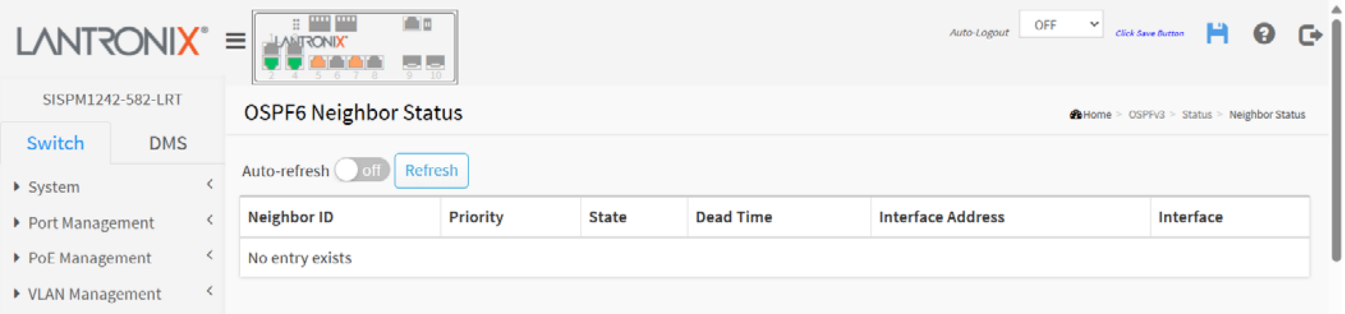
Area ID	Backbone	Area Type	Active Interfaces	SPF Executed Times	LSA count
0.0.0.0	Yes	Normal	0	1	1

Parameter Descriptions

Please refer to the online help page for parameter descriptions for this page.

Neighbor Status

This page displays the OSPF6 IPv6 neighbor status table.



OSPF6 Neighbor Status

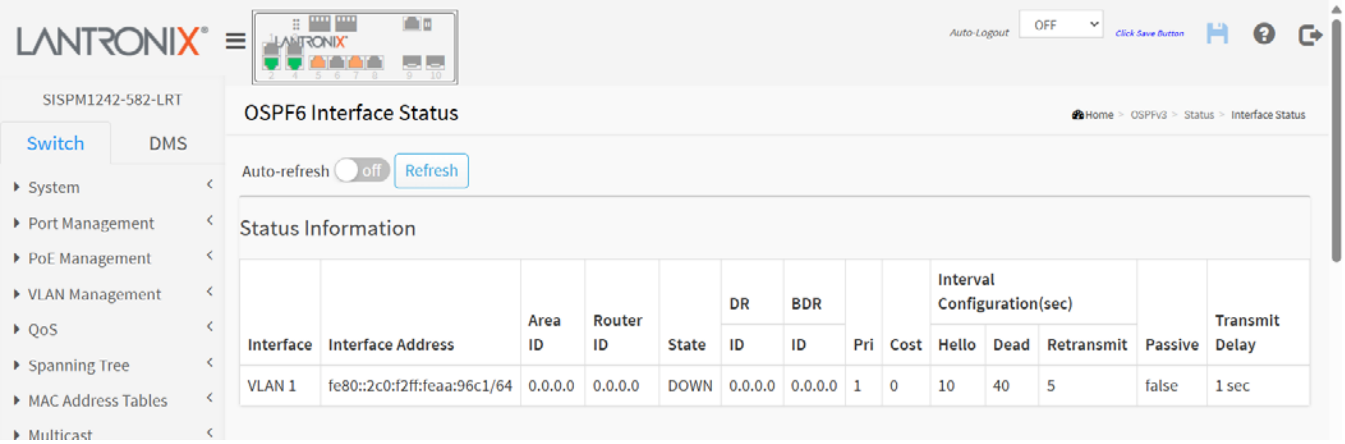
Neighbor ID	Priority	State	Dead Time	Interface Address	Interface
No entry exists					

Parameter Descriptions

Please refer to the online help page for parameter descriptions for this page.

Interface Status

This page displays the OSPF6 interface status table at OSPFv3 > Status > Interface Status.



OSPF6 Interface Status

Status Information

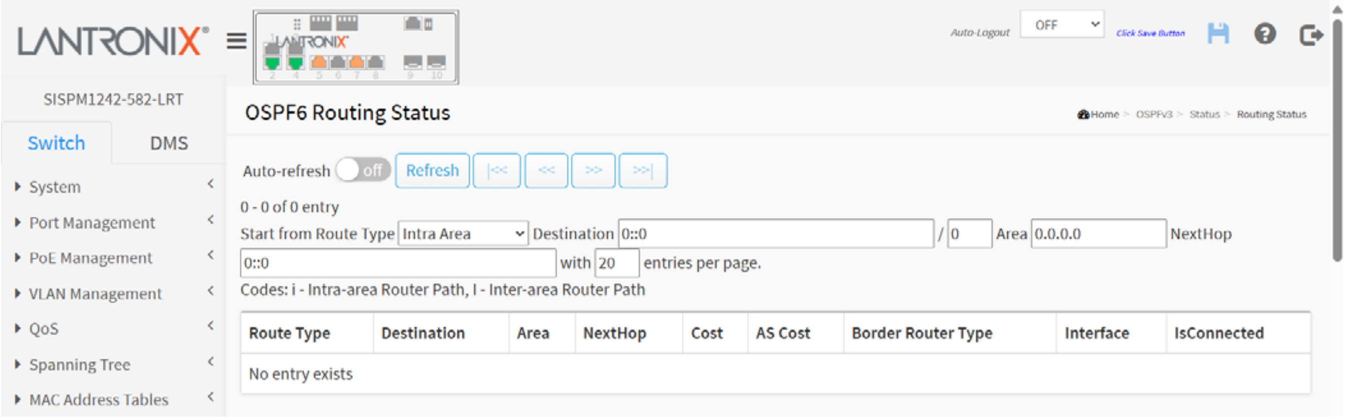
		Area	Router		DR	BDR			Interval Configuration(sec)				Transmit
Interface	Interface Address	ID	ID	State	ID	ID	Pri	Cost	Hello	Dead	Retransmit	Passive	Delay
VLAN 1	fe80::2c0:f2ff:feaa:96c1/64	0.0.0.0	0.0.0.0	DOWN	0.0.0.0	0.0.0.0	1	0	10	40	5	false	1 sec

Parameter Descriptions

Please refer to the online help page for parameter descriptions for this page.

Routing Status

This page displays the OSPF6 routing status table.



OSPF6 Routing Status

Auto-refresh off

0 - 0 of 0 entry

Start from Route Type Intra Area, Destination 0::0 / 0 Area 0.0.0.0 NextHop 0::0 with 20 entries per page.

Codes: i - Intra-area Router Path, I - Inter-area Router Path

Route Type	Destination	Area	NextHop	Cost	AS Cost	Border Router Type	Interface	IsConnected
No entry exists								

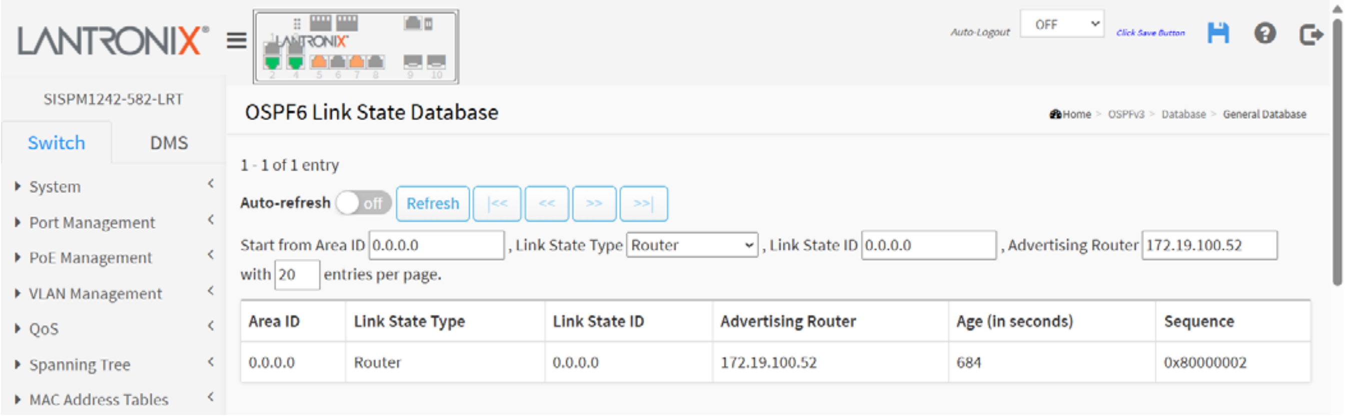
Parameter Descriptions

Please refer to the online help page for parameter descriptions for this page.

Database

General Database

This page displays the OSPF6 LSA link state database information table.



OSPF6 Link State Database

1 - 1 of 1 entry

Auto-refresh off

Start from Area ID 0.0.0.0, Link State Type Router, Link State ID 0.0.0.0, Advertising Router 172.19.100.52 with 20 entries per page.

Area ID	Link State Type	Link State ID	Advertising Router	Age (in seconds)	Sequence
0.0.0.0	Router	0.0.0.0	172.19.100.52	684	0x80000002

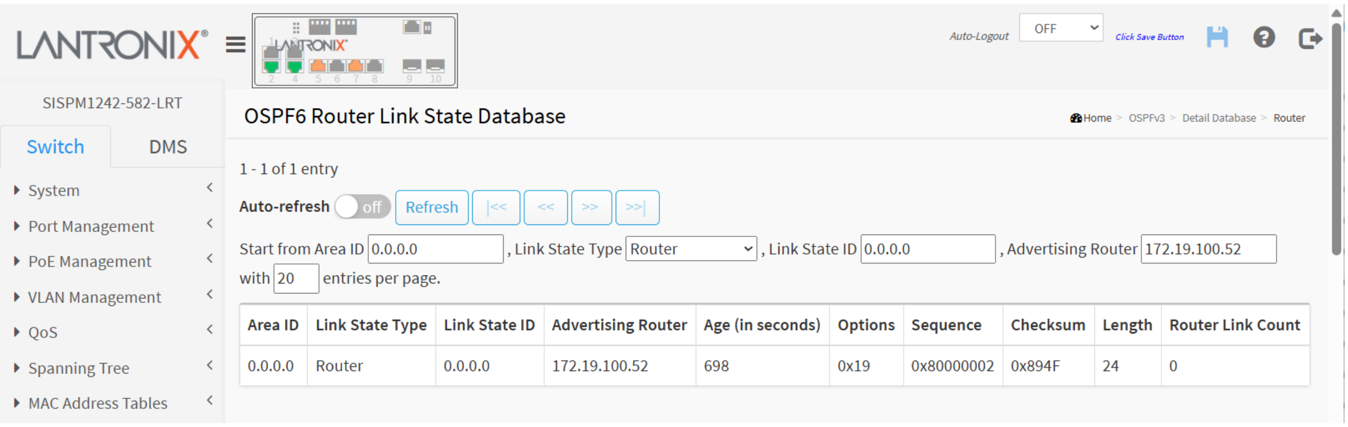
Parameter Descriptions

Please refer to the online help page for parameter descriptions for this page.

Detail Database

Router

This page displays the OSPF6 LSA Router link state database information table.



OSPF6 Router Link State Database

1 - 1 of 1 entry

Auto-refresh off

Start from Area ID 0.0.0.0 , Link State Type Router , Link State ID 0.0.0.0 , Advertising Router 172.19.100.52

with 20 entries per page.

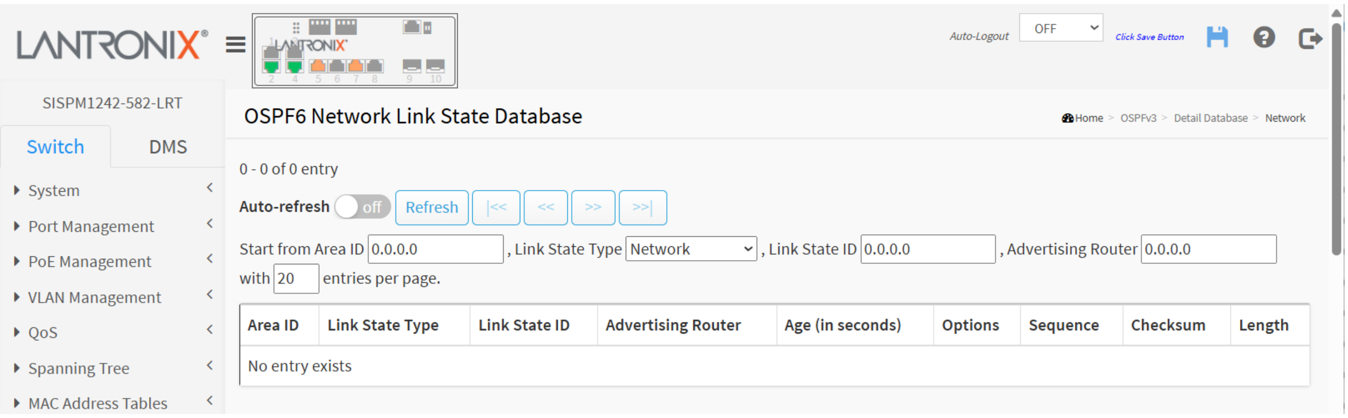
Area ID	Link State Type	Link State ID	Advertising Router	Age (in seconds)	Options	Sequence	Checksum	Length	Router Link Count
0.0.0.0	Router	0.0.0.0	172.19.100.52	698	0x19	0x80000002	0x894F	24	0

Parameter Descriptions

Please refer to the online help page for parameter descriptions for this page.

Network

The OSPF6 LSA Network link state database information table.



OSPF6 Network Link State Database

0 - 0 of 0 entry

Auto-refresh off

Start from Area ID 0.0.0.0 , Link State Type Network , Link State ID 0.0.0.0 , Advertising Router 0.0.0.0

with 20 entries per page.

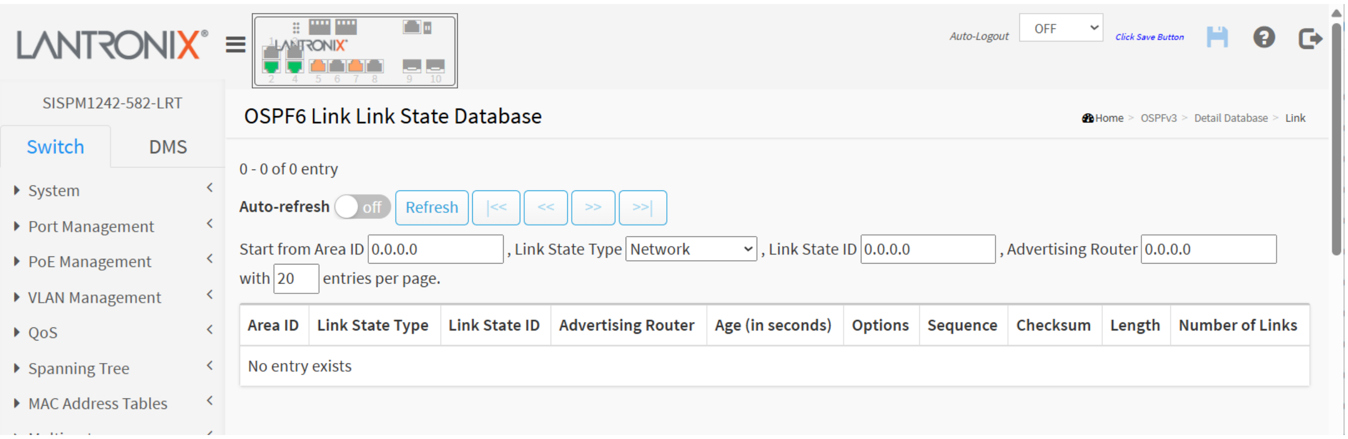
Area ID	Link State Type	Link State ID	Advertising Router	Age (in seconds)	Options	Sequence	Checksum	Length
No entry exists								

Parameter Descriptions

Please refer to the online help page for parameter descriptions for this page.

Link

This page displays the Link Link State database information table.



OSPF6 Link Link State Database

0 - 0 of 0 entry

Auto-refresh off

Start from Area ID 0.0.0.0 , Link State Type Network , Link State ID 0.0.0.0 , Advertising Router 0.0.0.0
with 20 entries per page.

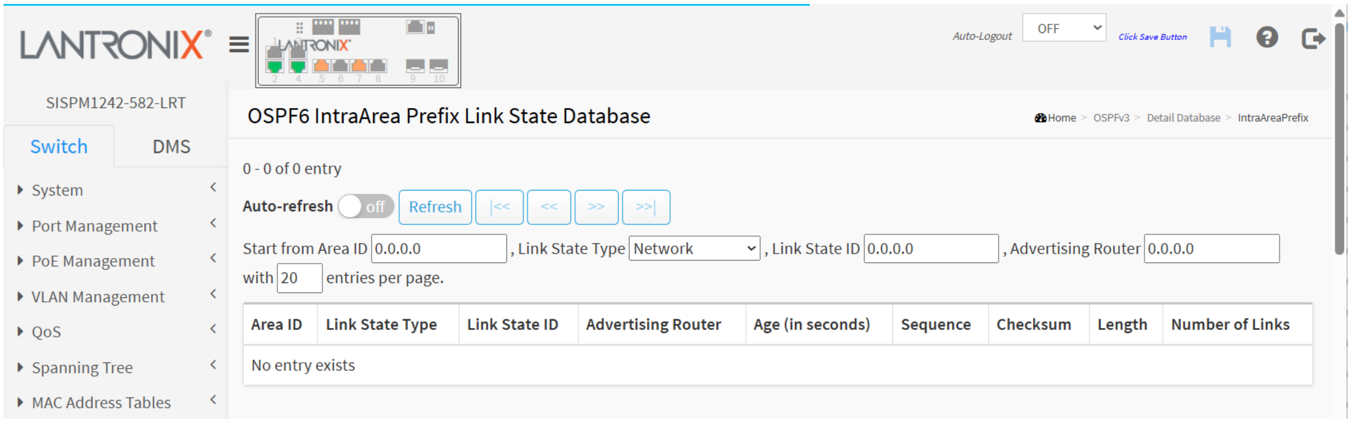
Area ID	Link State Type	Link State ID	Advertising Router	Age (in seconds)	Options	Sequence	Checksum	Length	Number of Links
No entry exists									

Parameter Descriptions

Please refer to the online help page for parameter descriptions for this page.

IntraArea Prefix

The OSPF6 LSA Intra Area Prefix link state database information table.



OSPF6 IntraArea Prefix Link State Database

0 - 0 of 0 entry

Auto-refresh off

Start from Area ID 0.0.0.0 , Link State Type Network , Link State ID 0.0.0.0 , Advertising Router 0.0.0.0
with 20 entries per page.

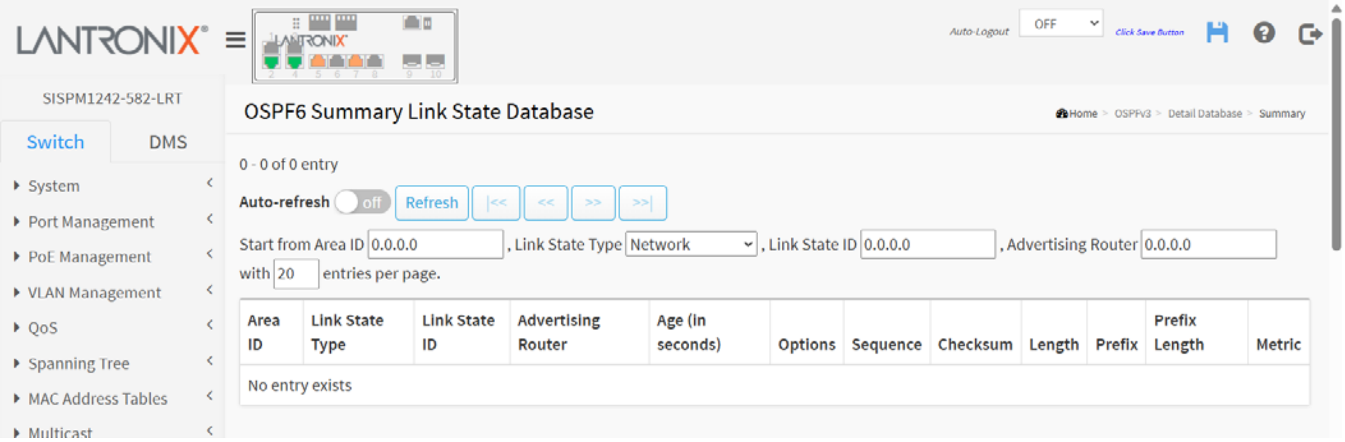
Area ID	Link State Type	Link State ID	Advertising Router	Age (in seconds)	Sequence	Checksum	Length	Number of Links
No entry exists								

Parameter Descriptions

Please refer to the online help page for parameter descriptions for this page.

Summary

This page displays the OSPF6 LSA Summary link state database information table.



OSPF6 Summary Link State Database

0 - 0 of 0 entry

Start from Area ID 0.0.0.0 , Link State Type Network , Link State ID 0.0.0.0 , Advertising Router 0.0.0.0

with 20 entries per page.

Area ID	Link State Type	Link State ID	Advertising Router	Age (in seconds)	Options	Sequence	Checksum	Length	Prefix	Prefix Length	Metric
No entry exists											

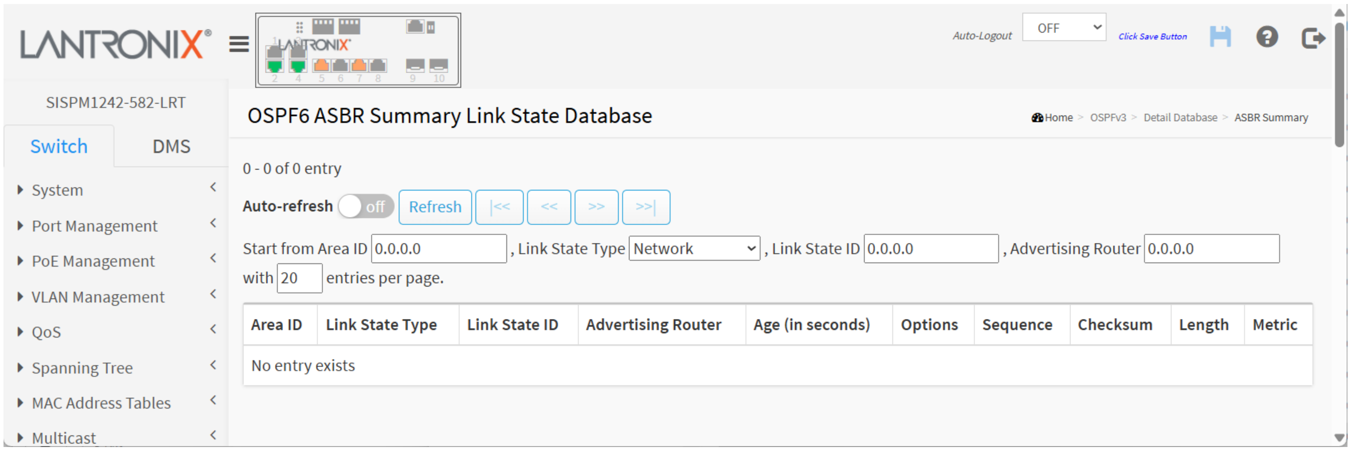
Parameter Descriptions

Please refer to the online help page for parameter descriptions for this page.

ASBR Summary

This page displays the OSPF6 LSA ASBR Summary link state database information table.

An ASBR (Autonomous System Boundary Router) is a router that is running multiple protocols and serves as a gateway to routers outside the OSPF domain and to those operating with different protocols. The ASBR can import and translate different protocol routes into OSPF through a process known as ‘redistribution’.



OSPF6 ASBR Summary Link State Database

0 - 0 of 0 entry

Start from Area ID 0.0.0.0 , Link State Type Network , Link State ID 0.0.0.0 , Advertising Router 0.0.0.0

with 20 entries per page.

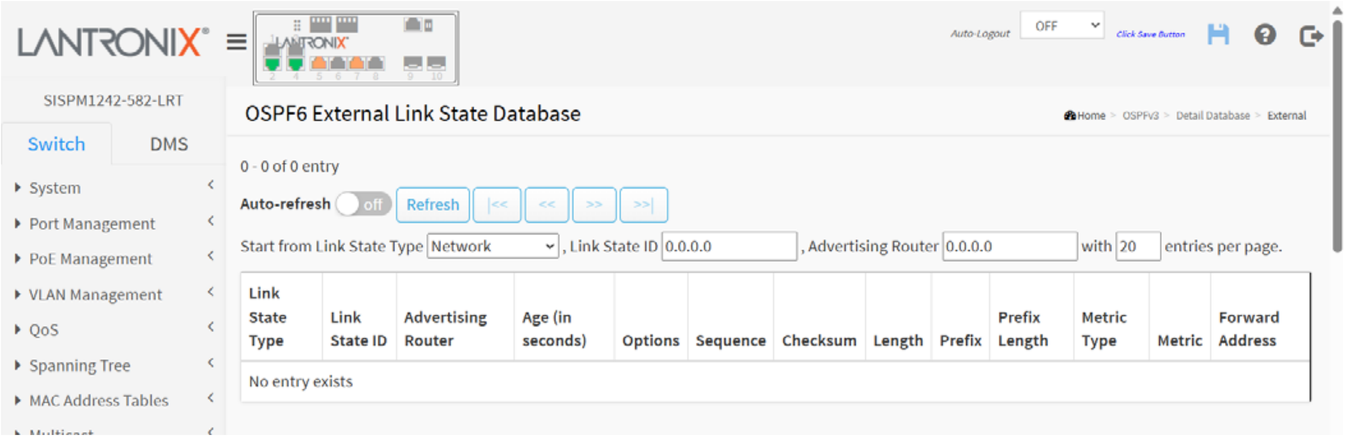
Area ID	Link State Type	Link State ID	Advertising Router	Age (in seconds)	Options	Sequence	Checksum	Length	Metric
No entry exists									

Parameter Descriptions

Please refer to the online help page for parameter descriptions for this page.

External

This page displays the OSPF6 LSA External link state database information table.



OSPF6 External Link State Database

0 - 0 of 0 entry

Start from Link State Type Network , Link State ID 0.0.0.0 , Advertising Router 0.0.0.0 with 20 entries per page.

Link State Type	Link State ID	Advertising Router	Age (in seconds)	Options	Sequence	Checksum	Length	Prefix	Prefix Length	Metric Type	Metric	Forward Address
No entry exists												

Parameter Descriptions

Please refer to the online help page for parameter descriptions for this page.

Troubleshooting OSPF6

Before performing the troubleshooting steps, please note the following:

- OSPFv3 has the same functionality as OSPFv2, but OSPFv3 uses IPv6 addresses to communicate with OSPFv3 peers.
- OSPFv3 uses the same SPF algorithm as OSPFv2.
- OSPFv3 has a different process than OSPFv2.
- OSPFv3 maintains separate neighbor tables, topology tables and routing tables from OSPFv2.

OSPF6 Troubleshooting Steps:

1. Verify there is no mismatch in the hello parameters or in the dead timer.
2. Verify that the link is up. Ping the other end of the link.
3. Make sure that the interfaces at both ends are configured to support OSPF.
4. Check for a mismatch in the OSPF Network Type.
5. Verify that Hello and Dead timers match on each end of the link
6. Verify that Neighboring interfaces are in the same OSPF Area.
7. If the device is in more than one area, then it MUST have at least one interface in Area 0.
8. OSPF Area IDs: When using multiple network area statements in the OSPF configuration, the order of the statements is critical. Check that the networks have been assigned the desired area IDs by checking the output of the `show ip ospf` interface command.
9. OSPF Does Not Start: The OSPF process cannot start on a router if a router ID cannot be established. Check the output of `show ip ospf` to see if a router ID has been established. If a router ID has not been established, check to see if the router has an active interface (preferably a loopback interface) with an IP address.
10. Verify Neighbor relationships: Once a router can start OSPF, it establishes an interface data structure for each interface configured to run OSPF. Check the output of `show ip ospf interface` to ensure that OSPF is active on the intended interfaces. If OSPF is active, check for an incorrectly configured interface.
11. Check if there is an entry in the OSPF Database for a particular external route, but it is not showing in the routing table. Check the Forwarding Address associated with the route.

25. RIP

RIP (Routing Information Protocol) lets routers exchange network topology information. It is considered an interior gateway protocol, typically used in small to medium-sized networks.

RIP is a distance vector routing protocol that shares routing information between its neighbors to help build the network topology table. There are currently two IPv4 RIP versions: Version 1 and Version 2. The main difference between versions is that v2 supports subnet masks and authentication.

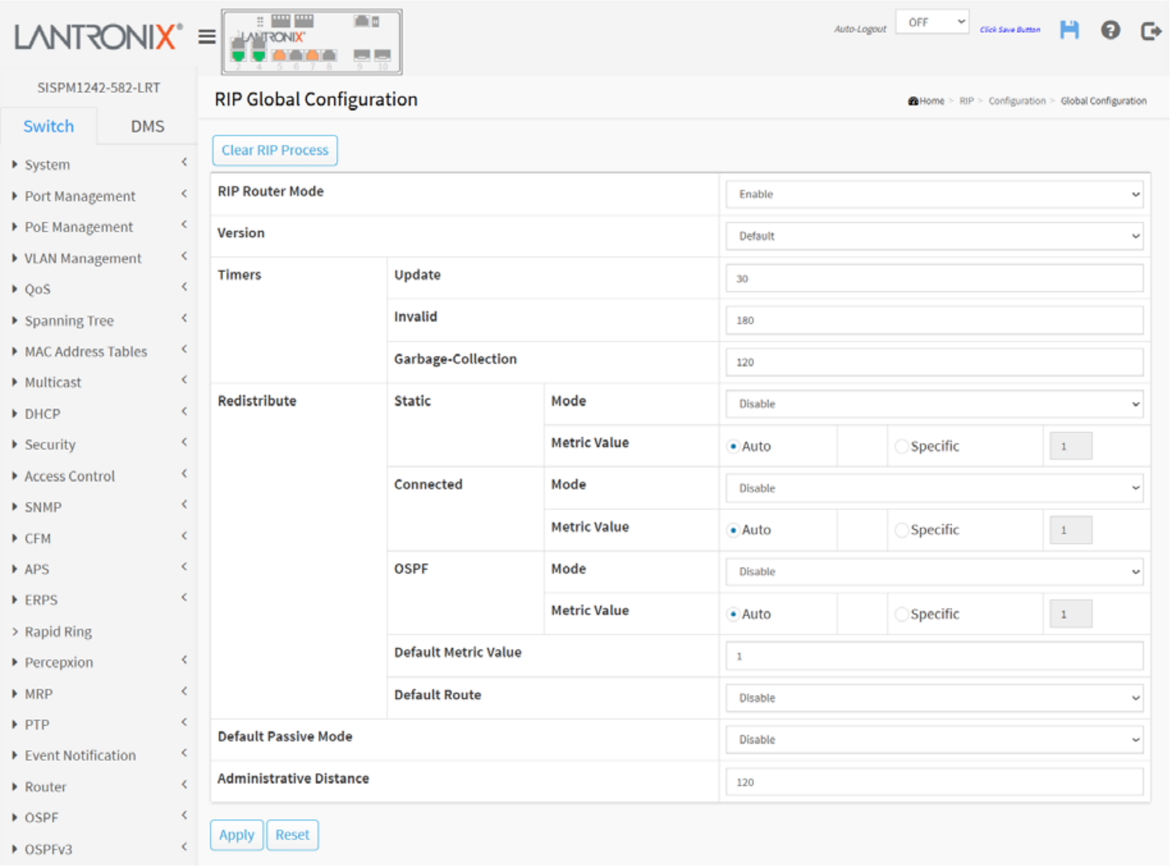
RIP uses a metric called hops to determine the cost of a route. A hop is a router which the traffic must pass through. If there are three routers that the traffic must pass through, there is a route cost of three hops. The maximum number of hops RIP will support is 15. If a route has more than 15 hops, the route will be discarded as invalid. RIP is susceptible to routing loops and uses mechanisms such as split horizon and others to prevent routing loops.

RIP Global Configuration

This page lets you set RIP global parameters at the RIP router configuration table. It is a general group to configure the RIP common router parameters.

To configure RIP global parameters in the Web UI:

1. Go to RIP > Configuration > Global Configuration.
2. You may need to click **Clear OSPF Process** to reset the current process.
3. Enable the OSPF Router Mode.
4. Configure the settings.
5. Click **Apply** to save the configuration.



RIP Global Configuration

Clear RIP Process

RIP Router Mode			Enable		
Version			Default		
Timers	Update		30		
	Invalid		180		
	Garbage-Collection		120		
Redistribute	Static	Mode	Disable		
		Metric Value	● Auto	○ Specific	1
	Connected	Mode	Disable		
		Metric Value	● Auto	○ Specific	1
	OSPF	Mode	Disable		
		Metric Value	● Auto	○ Specific	1
	Default Metric Value		1		
	Default Route		Disable		
Default Passive Mode			Disable		
Administrative Distance			120		

Apply Reset

Parameter descriptions:

Clear RIP Process : Click to reset the current RIP process.

RIP Router Mode: Enable/Disable the RIP router mode.

- ***Enable***: Enable the RIP router mode.
- ***Disable***: Disable the RIP router mode (default).

Version: RIP version support.

- ***Default***: Base on the default version process. The router sends RIPv2 and accepts both RIPv1 and RIPv2. When the router receives either version of REQUESTS or triggered updates packets, it replies with the appropriate version.
- ***Version 1***: Receive/Send RIPv1 only.
- ***Version 2***: Receive/Send RIPv2 only.

Update Timer: The timer interval (in seconds) between the router sends the complete routing table to all neighboring RIP routers. The allowed range is 5 to 2147483 seconds.

Invalid Timer: The invalid timer is the number of seconds after which a route will be marked invalid. The allowed range is 5 to 2147483 seconds.

Garbage Collection Timer: The garbage collection timer is the number of seconds after which a route will be deleted. The allowed range is 5 to 2147483 seconds.

Static Redistribute Mode: Indicate if the router redistribute the static routes into the RIP domain or not.

- ***Enable***: Enable static routes redistribution.
- ***Disable***: Enable static routes redistribution.

Static Redistribute Metric Value: User specified metric value for the static routes. The field is significant only when the argument 'StaticRedistIsSpecificMetric' is TRUE. If the specific metric setting is removed while the static redistributed mode is enabled, the router will update the original static redistributed routes with metric value 16 before updates to the new metric value. The allowed range is 1 to 16 hops.

- ***Auto***: The redistributed metric value is automatically set.
- ***Specific***: User specified metric for the static routes.

Connected Redistribute Mode: Indicate if the router redistributes the directly connected routes with RIP not enabled into the RIP domain or not.

- ***Enable***: Enable connected routes redistribution.
- ***Disable***: Enable connected routes redistribution.

Connected Redistribute Metric Value: User specified metric value for the connected interfaces. The field is significant only when the argument 'ConnectedRedistIsSpecificMetric' is TRUE. If the specific metric setting is removed while the connected redistributed mode is enabled, the router will updates the original connected redistributed routes with metric value 16 before updates to the new metric value. The allowed range is 1 to 16 hops.

- ***Auto***: The redistributed metric value is automatically set.
- ***Specific***: User specified metric for the connected routes.

OSPF Redistribute Mode: Indicate if the router redistribute the OSPF routes into the RIP domain or not. The field is significant only when the OSPF protocol is supported on the device.

- ***Enable***: Enable OSPF routes redistribution.
- ***Disable***: Enable OSPF routes redistribution.

OSPF Redistribute Metric Value: User specified metric value for the RIP routes. The field is significant only when the OSPF protocol is supported on the device and argument 'OspfRedistIsSpecificMetric' is TRUE. If the specific metric setting is removed while the OSPF redistributed mode is enabled, the router will update the original OSPF redistributed routes with metric value 16 before updates to the new metric value. The allowed range is 1 to 16 hops.

- ***Auto***: The redistributed metric value is automatically set.
- ***Specific***: User specified metric for the OSPF routes.

Redistribute Default Metric Value: The RIP default redistributed metric. It is used when the metric value isn't specified for the redistributed protocol type. The allowed range is 1 to 16 hops.

Redistribute Default Route: The RIP default route redistribution.

Default Passive Mode: Set to True to configure all interfaces as passive-interface by default. Otherwise set to False. The default is True.

Administrative Distance: The RIP administrative distance. The allowed range is 1 to 255 hops.

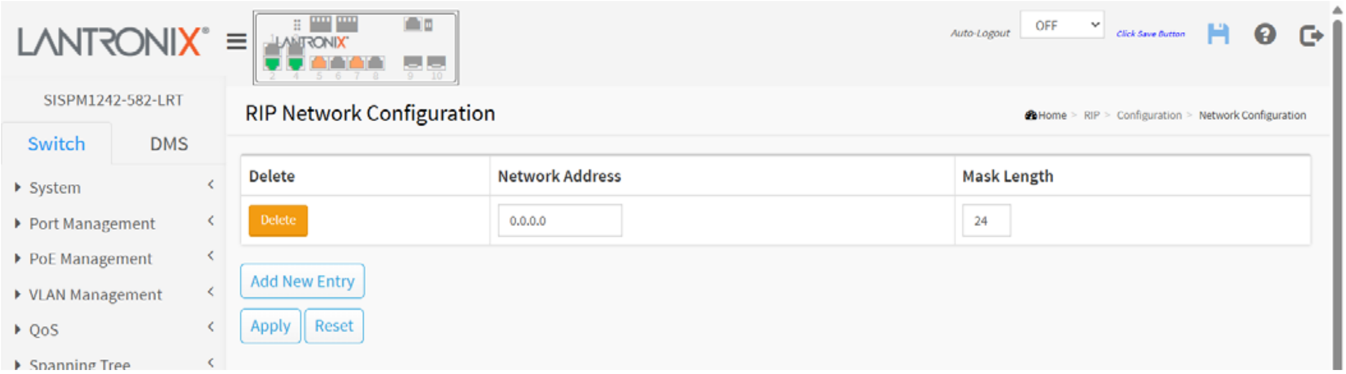
RIP Network Configuration

This page lets you add and configure new RIP entries.

When RIP is enabled on the specific interface(s), the router can provide the network information to the other RIP routers via those interfaces.

To configure RIP network parameters in the Web UI:

1. Go to RIP > Configuration > Network Configuration.
2. Click **Add New Entry** to add a new entry to the table.
3. Configure the settings.
4. Click **Apply** to save the configuration.



Auto-Logout OFF

RIP Network Configuration

Delete	Network Address	Mask Length
Delete	0.0.0.0	24

Parameter descriptions:

Delete : Click to delete the table entry.

Add New Entry : Click to add a new entry to the table.

Network Address : Enter the IPv4 address of the network.

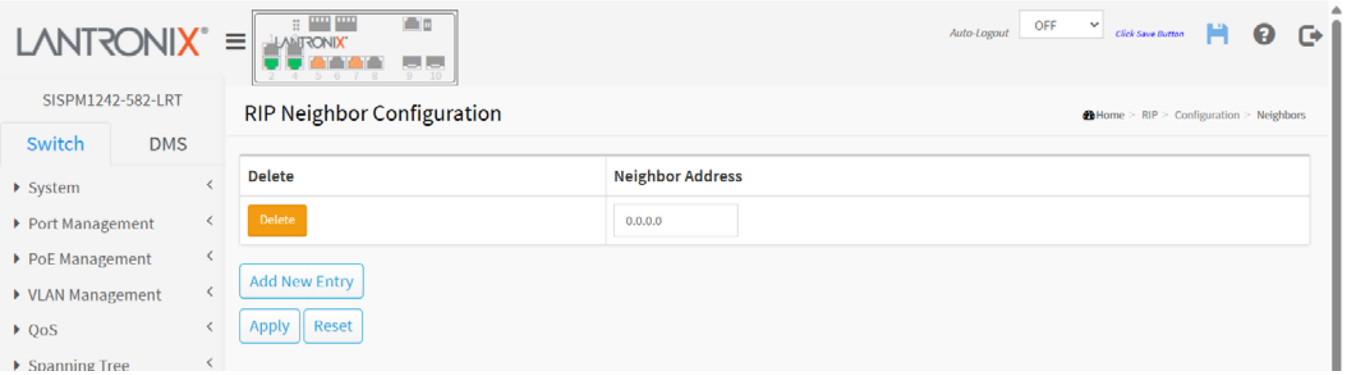
Mask Length : Enter the IPv4 netmask of the network.

RIP Neighbor Configuration

This page lets you add and configure new RIP neighbor entries. It is used to configure the RIP router to send RIP updates to specific neighbors using the unicast, broadcast, or network IP address after update timer expiration.

To configure RIP neighbor parameters in the Web UI:

1. Go to RIP > Configuration > Neighbors.
2. Click **Add New Entry** to add a new entry to the table.
3. Configure the neighbor IPv4 address.
4. Click **Apply** to save the configuration.



RIP Neighbor Configuration

Delete	Neighbor Address
Delete	0.0.0.0

Parameter descriptions:

Delete : Click to delete the table entry.

Add New Entry : Click to add a new entry to the table.

Neighbor Address : Enter the IP address of the neighbor device. This is an IPv4 address encoded as "a.b.c.d", where a-d is a base-10 human readable integer in the range [0-255]. The neighbor address can be a unicast (excluding loopback), broadcast, or network IP address.

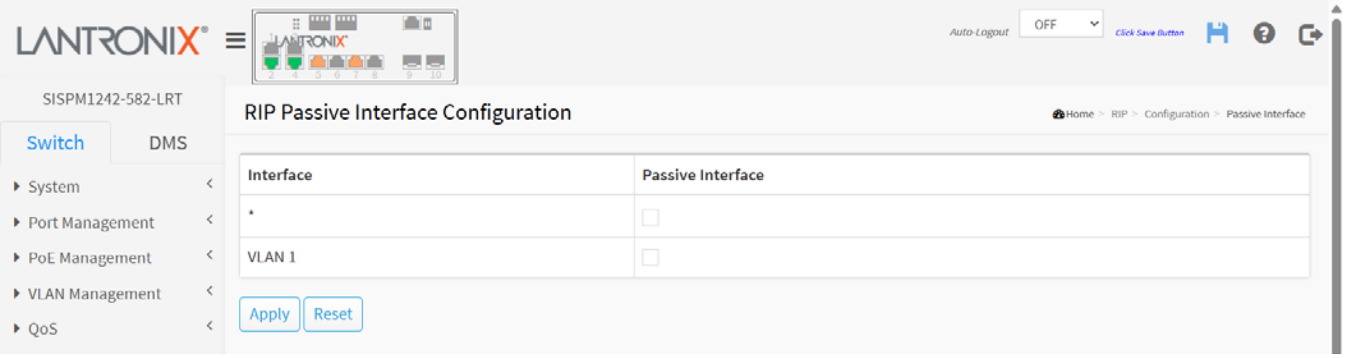
RIP Passive Interface

This page lets you use the RIP passive interface function to prevent RIP updates from being sent on particular interfaces. The passive interface function tells an interface to listen to RIP routes but not to advertise them. When routing announcements on an interface are disabled, the router will “listen but don’t talk.” This feature can reduce the routing load on the CPU by reducing the number of interfaces on which a protocol will communicate.

Note: Use this function only if you are sure the routing protocol doesn’t need to talk to anything on the specified interface.

To configure RIP passive interface in the Web UI:

1. Go to RIP > Configuration > Passive Interface.
2. Select or clear the Passive Interface box for the relevant interface in the table.
3. Click **Apply** to save the configuration.



RIP Passive Interface Configuration

Interface	Passive Interface
*	□
VLAN 1	□

Apply Reset

Parameter descriptions:

Interface : Shows the RIP Interface identification (e.g., VLAN 1)**.**

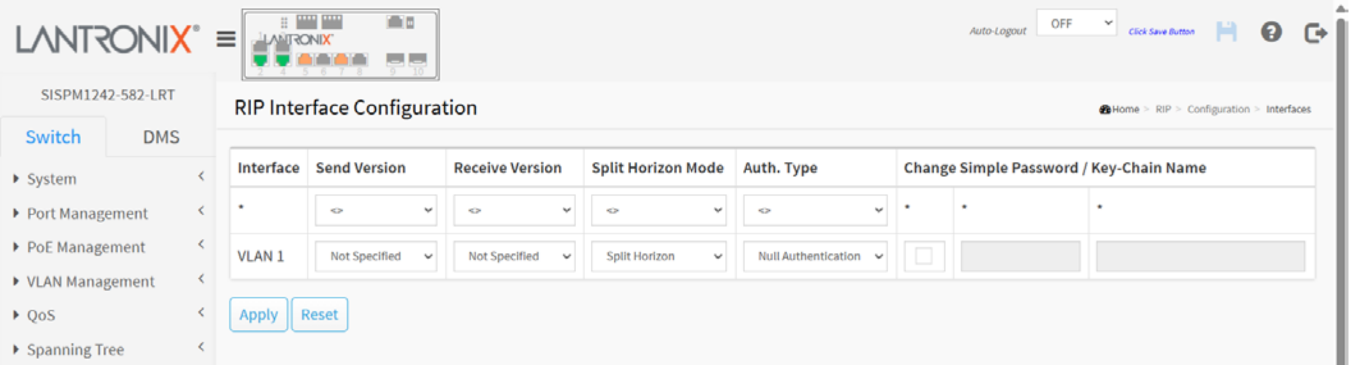
Passive Interface : Check the box to enable the interface as RIP passive-interface.

RIP Interface Configuration

This page lets you configure RIP interface parameters.

To configure the RIP interface in the Web UI:

1. Go to RIP > Configuration > Interfaces.
2. Configure the settings.
3. Click **Apply** to save the configuration.



RIP Interface Configuration

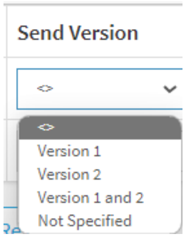
Interface	Send Version	Receive Version	Split Horizon Mode	Auth. Type	Change Simple Password / Key-Chain Name		
*	<>	<>	<>	<>	*	*	*
VLAN 1	Not Specified	Not Specified	Split Horizon	Null Authentication	□		

Parameter descriptions:

Interface: Interface identification (e.g., VLAN 1).

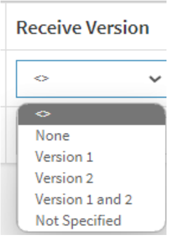
Send Version: The RIP version for the advertisement transmission on the interface.

- ***Version 1***: Use RIP v1 for advertisement transmission on the interface.
- ***Version 2***: Use RIP v2 for advertisement transmission on the interface.
- ***Version 1 and 2***: Use RIP v1 and v2 for advertisement transmission on the interface.
- ***Not Specified***: Do not specify a RIP version (default).



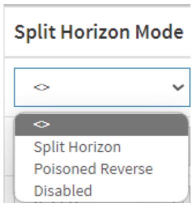
Receive Version: The RIP version for the advertisement reception on the interface.

- ***None***: Do not use RIP for advertisement reception on the interface.
- ***Version 1***: Use RIP v1 for advertisement reception on the interface.
- ***Version 2***: Use RIP v2 for advertisement reception on the interface.
- ***Version 1 and 2***: Use RIP v1 and v2 for advertisement reception on the interface.
- ***Not Specified***: Do not specify a RIP version (default).



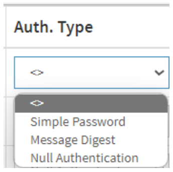
Split Horizon Mode: The split horizon mode.

- ***Split Horizon***: To omit routes learned from one neighbor in updates sent to that neighbor.
- ***Poisoned Reverse***: The neighbor learned routes are included in updates sent to the neighbors but their metrics are set to infinity.
- ***Disabled***: Split horizon is disabled.



Auth. Type: The authentication type.

- ***Simple Password*:** It's using a plain text authentication. A password must be configured, but the password can be read by sniffer the packets.
- ***Message Digest***: It's using message-digest algorithm 5 (MD5) authentication. Keying material must also be configured. This is the most secure method.



- ***Null Authentication***: No authentication.

Change Simple Password: It is used to change the simple password (fill with plain text). The allowed input length is 1 - 15 printable characters excluding space character. The null string means that no simple password is set on the interface. **Note** that you cannot set key chain and simple password at the same time.

Change Key-Chain Name: It is used to change the key chain name used by MD5 authentication. The allowed input length is 1 - 31 printable characters excluding space character. The null string means that no key-chain name is set on the interface. **Note** that you cannot set key chain and simple password at the same time.

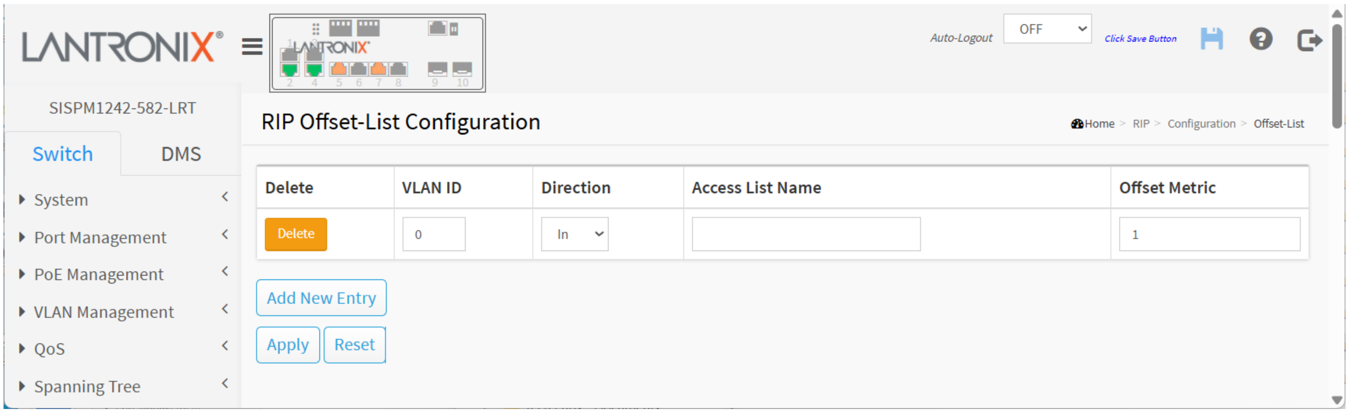
Offset-List

This page lets you create and configure RIP offset list parameters.

A RIP message includes a metric (number of hops) for each route. An ‘offset’ is an additional number that is added to a metric to affect the cost of paths. The offset is set per interface and, for example, can reflect the speed, delay, or some other quality of that specific interface. The relative cost of the interfaces can then be adjusted as desired. You must set the offset for each interface (the default offset is 1).

To configure the offset-list in the Web UI:

1. Go to RIP > Configuration > Offset-List.
2. Click **Add New Entry** to add a new entry to the table.
3. Configure the neighbor IPv4 address.
4. Click **Apply** to save the configuration.



Auto-Logout: OFF

RIP Offset-List Configuration

Delete	VLAN ID	Direction	Access List Name	Offset Metric
Delete	0	In		1

Parameter descriptions:

Delete : Click the button to delete an existing entry from the table and the switch**.**

Add New Entry : Click to add a new entry to the table.

VLAN ID : Enter the VLAN ID for entry. The VLAN interface to which the offset list applies. The range of VLAN ID is 0 - 4095. A 0 entry means that the offset list applies to all interfaces.

Direction : Enter the direction for entry. The direction to add the offset to routing metric update.

- ***In*** : Apply to the inbound direction (default).
- ***Out*** : Apply to the outbound direction.

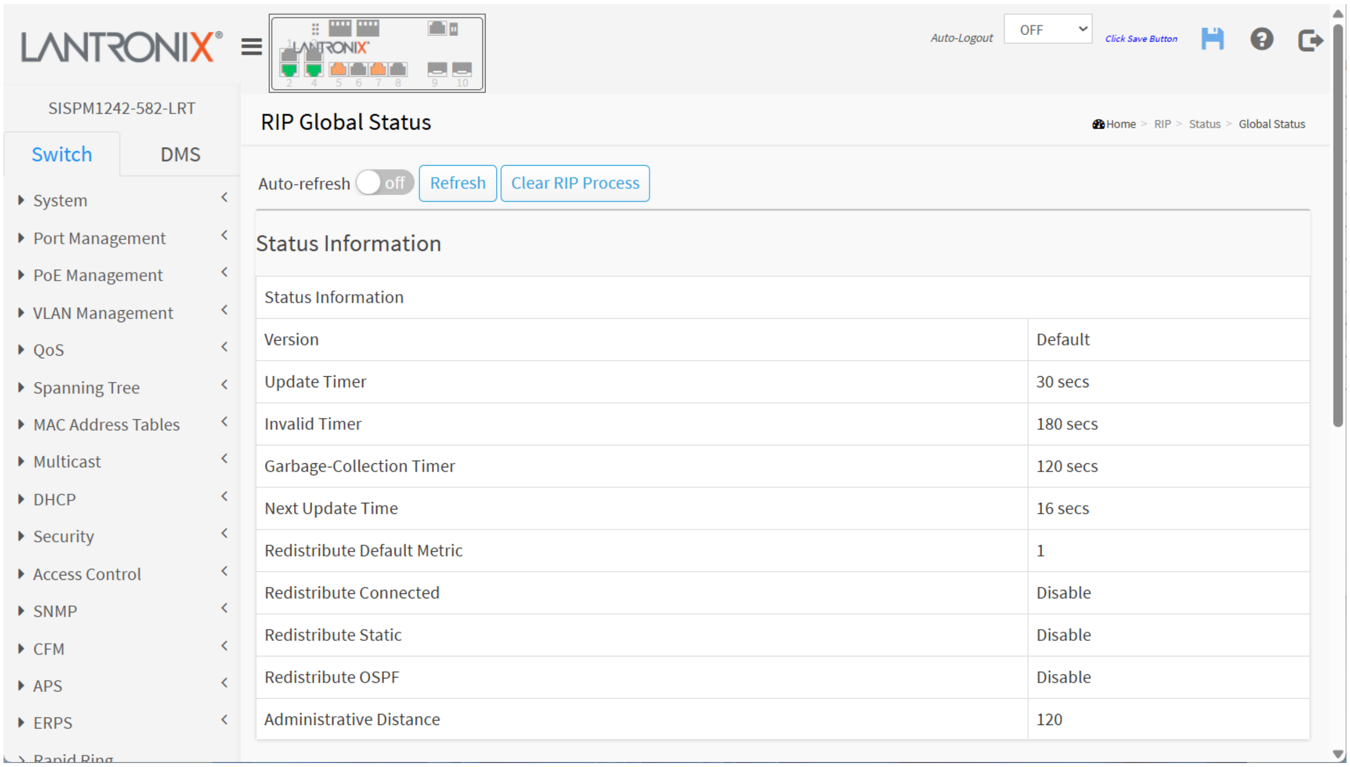
Access List Name : Enter the name of the access list for entry. A valid Name string length is 1 - 31 characters and allows all printable characters excluding the space character. The Access List Name field cannot be empty.

Offset Metric : Set the offset for each interface (the valid range is 0-16; the default offset is 1).

RIP Status

RIP Global Status

This page shows the RIP general status information table.



RIP Global Status

Status Information

Status Information	
Version	Default
Update Timer	30 secs
Invalid Timer	180 secs
Garbage-Collection Timer	120 secs
Next Update Time	16 secs
Redistribute Default Metric	1
Redistribute Connected	Disable
Redistribute Static	Disable
Redistribute OSPF	Disable
Administrative Distance	120

Parameter descriptions:

Clear RIP Process : Click to reset the current RIP process..

Version: This indicates the global rip version. By default, the router sends RIPv2 and accepts both RIPv1 and RIPv2. When the router receives either version of REQUESTS or triggered updates packets, it replies with the appropriate version. Be aware of the RIP network class configuration when RIPv1 is involved in the topology. RIPv1 uses classful routing; the subnet information is not included in the routing updates. This limitation makes it impossible to have different sized subnets inside of the same network class. In other words, all subnets in a network class must have the same size.

Update Timer: The timer interval (in seconds) between the router sends the complete routing table to all neighboring RIP routers

Invalid Timer: The number of seconds after which a route will be marked invalid.

Garbage-Collection Timer: The number of seconds after which a route will be deleted.

Next Update Time: Specifies when the next round of updates will be sent out from this router in seconds.

Redistribute Default Metric: This indicates the default metric value of redistributed routes.

Redistribute Connected: This indicates the connected route is redistributed or not.

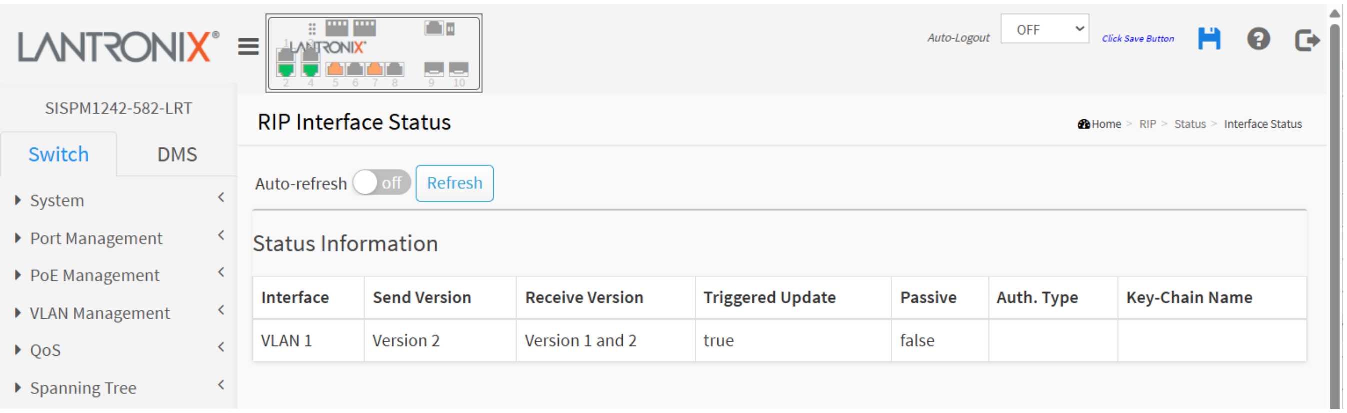
Redistribute Static: This indicates the static route is redistributed or not.

Redistribute OSPF: This indicates the OSPF route is redistributed or not.

Administrative Distance: This indicates administrative distance value.

RIP Interface Status

This page displays current RIP Interface Status.



Status Information

Interface	Send Version	Receive Version	Triggered Update	Passive	Auth. Type	Key-Chain Name
VLAN 1	Version 2	Version 1 and 2	true	false		

Parameter descriptions:

Interface : Displays the current RIP Interface**.**

Send Version: Displays the currently configured send version (v1 or v2).

Receive Version: Displays the currently configured receive version (v1 or v2).

Triggered Update: indicates if the interface enable triggered update or not.

Passive : indicates if the passive-interface is active on the interface or not.

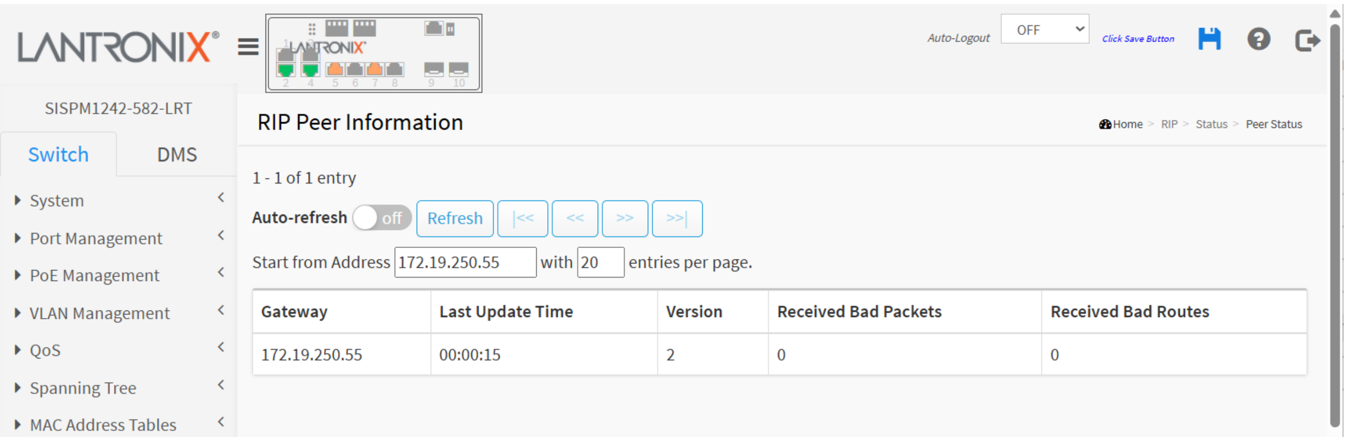
Auth. Type : Displays the type of authentication currently configured (plain text or MD5) **.**

Key-Chain Name : Displays the key chain name for the entry**.**

RIP Peer Information

This is the RIP peer table. It is used to provide the RIP peer information.

Each page shows up to 999 table entries, selected at the "entries per page" input field. When first visited, the web page shows the beginning entries of this table. The "Start from Address " input field lets you change the starting point in this table. Click **Refresh** to update the displayed table from the specified starting address.



RIP Peer Information

1 - 1 of 1 entry

Auto-refresh off Refresh |<< << >> >>|

Start from Address 172.19.250.55 with 20 entries per page.

Gateway	Last Update Time	Version	Received Bad Packets	Received Bad Routes
172.19.250.55	00:00:15	2	0	0

Parameter descriptions:

Gateway : Displays the Peer IPv4 address.

Last Update Time : Displays the time of the last update. The time duration in seconds from the time the last RIP packet was received from the neighbor to now.

Version : Displays the RIP peer version (v1 or v2). The RIP version number in the header of the last RIP packet that was received from the neighbor.

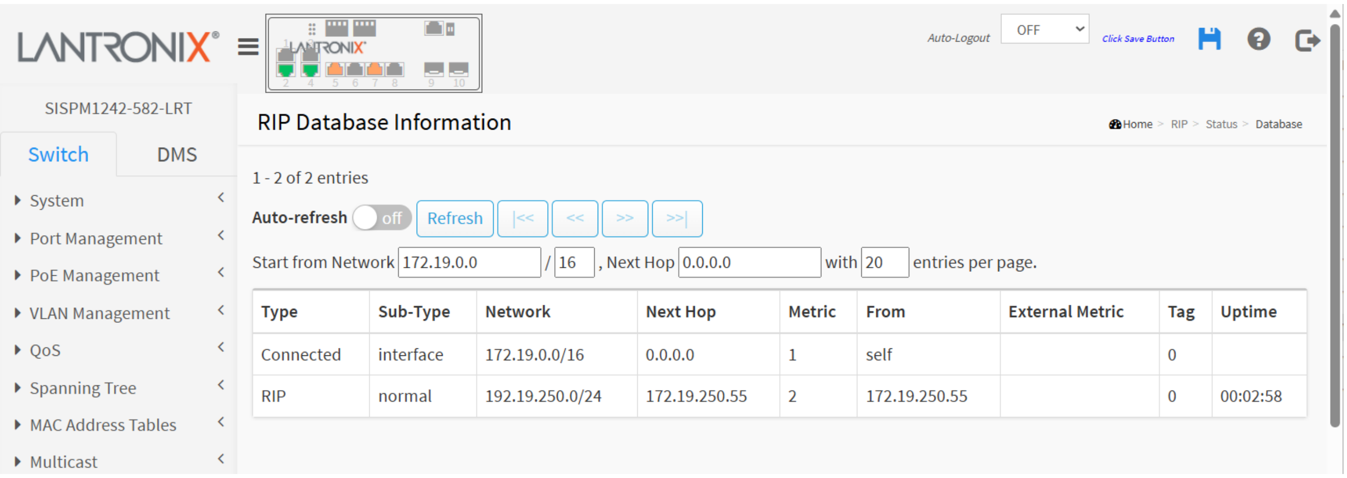
Received Bad Packets : Displays the number of RIP response packets from the neighbor discarded as invalid.

Received Bad Routes : Displays the number of routes from the neighbor that were ignored because they were invalid.

RIP Database Information

This page displays RIP database information. Go to the System > RIP > Status > Global Status menu path.

Each page shows up to 999 table entries, selected through the "entries per page" input field. When first visited, the web page will show the beginning entries of this table. The "Start from Network" input field lets you change the starting point in this table. The Next Hop input field lets you enter the IP address of the next hop.



RIP Database Information

1 - 2 of 2 entries

Auto-refresh off

Start from Network 172.19.0.0 / 16 , Next Hop 0.0.0.0 with 20 entries per page.

Type	Sub-Type	Network	Next Hop	Metric	From	External Metric	Tag	Uptime
Connected	interface	172.19.0.0/16	0.0.0.0	1	self		0	
RIP	normal	192.19.250.0/24	172.19.250.55	2	172.19.250.55		0	00:02:58

Parameter descriptions:

Type : Displays the protocol type of the route (plain text or MD5).

Sub-Type : Displays protocol sub-type of the route.

Network : Displays the destination IP address and mask of the route.

Next Hop : Displays the first gateway along the route to the destination.

Metric : Displays the metric of the route.

From : Indicates the route is learned an IP address or generated from one of the local interfaces.

External Metric : The field is significant only when the route is redistributed from other protocol type, for example, OSPF. This indicates the metric value from the original redistributed source

Tag : The tag of the route. It is used to provide a method of separating 'internal' RIP routes, which may have been imported from an EGP (Exterior Gateway Protocol) or another IGP (Interior Gateway Protocol). For example, routes imported from OSPF can have a route tag value which the other routing protocols can use to prevent advertising the same route back to the original protocol routing domain.

Uptime : The time field is significant only when the route is learned from the neighbors. When the route destination is reachable (its metric value less than 16), the time field means the invalid time of the route. When the route destination is unreachable (its metric value greater than 16), the Uptime field indicates the garbage-collection time of the route.

RIP Troubleshooting

1. Wrong network command(s): the network command is used to tell RIP what networks to advertise, but also where to send RIP routing updates. Wrong or missing network commands will cause issues.
2. Interface shut: A network on an interface that is in Shutdown will not be advertised.
3. Passive interface: An interface that is configured as Passive will not send any RIP updates.
4. Version mismatch: RIP has two versions; both routers must use the same version.
5. Max hop count: When the hop count is 16, the network is considered unreachable. If the network is small, check for offset-lists that increase the metric.
6. Route Filtering: Filters might prevent RIP updates from being sent or received.
7. Authentication: Both RIP routers must have the same authentication parameters.
8. Split horizon: Networks that are learned on an interface are not advertised out of the same interface.

26. Diagnostics

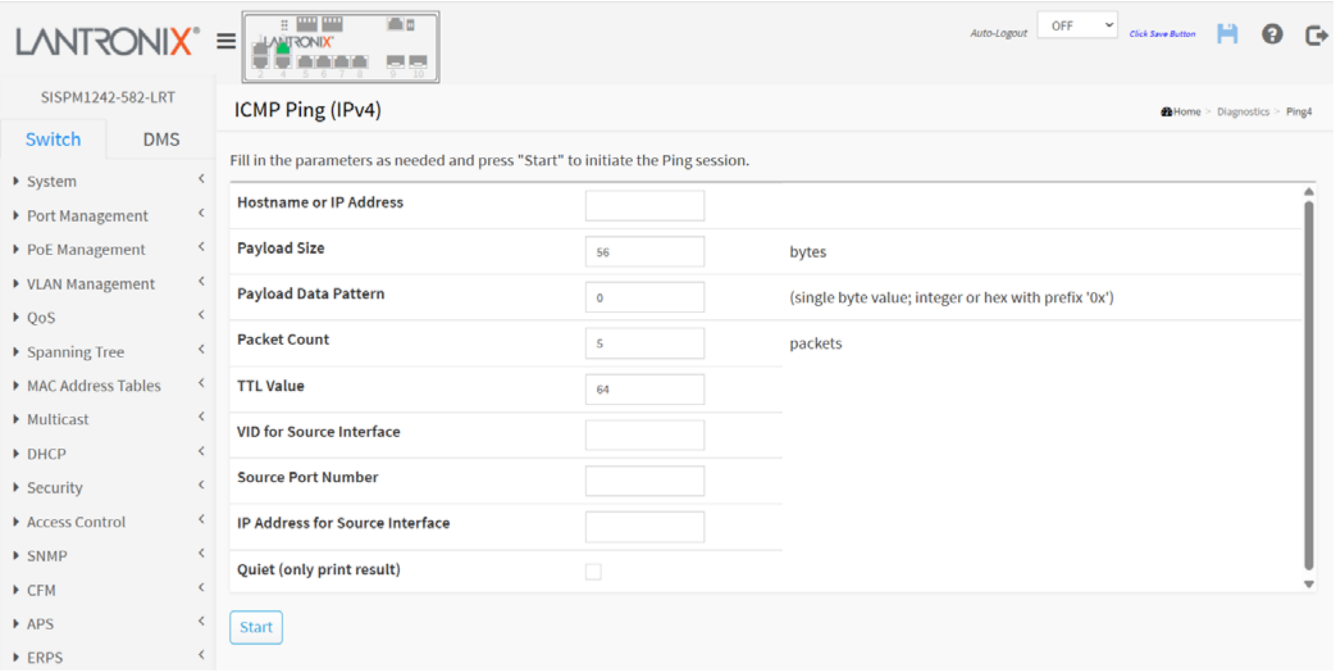
This menu section provides a set of basic system diagnostics including Ping, Traceroute, and Port Mirror.

Ping4

This page lets you issue ICMP (IPv4) PING packets to troubleshoot IP connectivity issues.

To configure a Ping session in the web UI:

1. Go to Diagnostics > Ping.
2. Specify the target IP Address and other parameters if desired.
3. Click **Start**.



ICMP Ping (IPv4)

Fill in the parameters as needed and press "Start" to initiate the Ping session.

Hostname or IP Address		
Payload Size	56	bytes
Payload Data Pattern	0	(single byte value; integer or hex with prefix '0x')
Packet Count	5	packets
TTL Value	64	
VID for Source Interface		
Source Port Number		
IP Address for Source Interface		
Quiet (only print result)	□	

Parameter descriptions:

Hostname or IP Address : The address of the destination host, either as a symbolic hostname or an IP Address.

Payload Size : Specify the size of the ICMP data payload in bytes (excluding the size of Ethernet, IP and ICMP headers). The default value is 56 bytes. The valid range is 2-1452 bytes.

Payload Data Pattern : Specify the pattern used in the ICMP data payload. The default value is 0. The valid range is 0-255.

Packet Count : Specify the number of Ping requests sent. The default value is 5. The valid range is 1-60.

TTL Value : Specify the Time-To-Live/TTL) field value in the IPv4 header. The default value is 64 seconds. The valid range is 1-255 seconds.

VID for Source Interface : This field can be used to force the test to use a specific local VLAN interface as the source interface. Leave this field empty for automatic selection based on routing configuration. **Note**: You may only specify either the VID or the IP Address for the source interface.

Source Port Number : This field can be used to force the test to use a specific local interface with the specified port number as the source interface. The specified port must be configured with a suitable IP address. Leave this field empty for automatic selection based on routing configuration. **Note**: You may only specify either the Source Port Number or the IP Address for the source interface.

Address for Source Interface : This field can be used to force the test to use a specific local interface with the specified IP address as the source interface. The specified IP address must be configured on a local interface. Leave this field empty for automatic selection based on routing configuration. **Note**: You may only specify either the VID or the IP Address for the source interface.

Quiet (only print result) : Checking this option will not print the result of each Ping request but will only show the final result.

Start : Click the button to start to ping the target IP Address.

After you press Start, ICMP packets are transmitted, and the sequence number and round trip time are displayed upon reception of a reply.

The amount of data received inside of an IP packet of type ICMP ECHO_REPLY will always be 8 bytes more than the requested payload data size (the difference is the ICMP header).

The page refreshes automatically until responses to all packets are received, or until a timeout occurs.

Ping output looks like this:

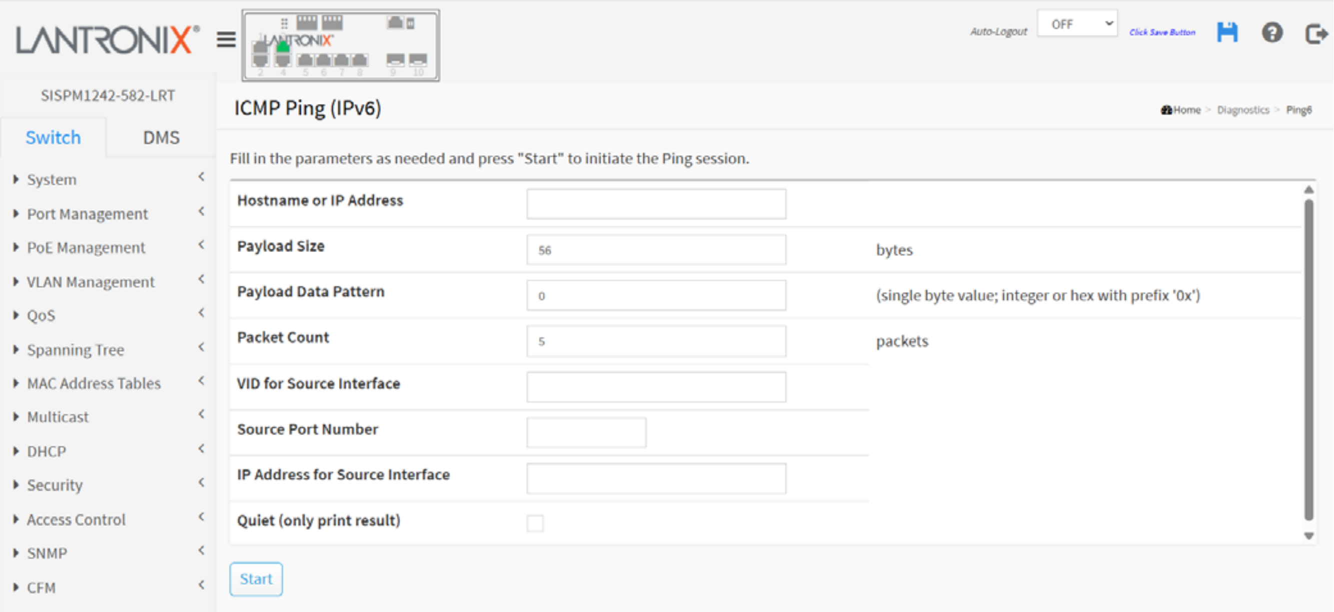
```
PING 172.16.1.1 (172.16.1.1) from 172.16.1.10: 56 data bytes
64 bytes from 172.16.1.1: seq=0 ttl=64 time=2.034 ms
64 bytes from 172.16.1.1: seq=1 ttl=64 time=1.729 ms
64 bytes from 172.16.1.1: seq=2 ttl=64 time=1.954 ms
64 bytes from 172.16.1.1: seq=3 ttl=64 time=1.699 ms
64 bytes from 172.16.1.1: seq=4 ttl=64 time=1.916 ms

--- 172.16.1.1 ping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max = 1.699/1.866/2.034 ms

Ping session completed.
```

Ping6

This page allows you to issue ICMPv6 PING packets to troubleshoot IPv6 connectivity issues.



ICMP Ping (IPv6)

Fill in the parameters as needed and press "Start" to initiate the Ping session.

Hostname or IP Address		
Payload Size	56	bytes
Payload Data Pattern	0	(single byte value; integer or hex with prefix '0x')
Packet Count	5	packets
VID for Source Interface		
Source Port Number		
IP Address for Source Interface		
Quiet (only print result)	□	

Hostname or IP Address : The address of the destination host, either as a symbolic hostname or an IP Address.

Payload Size : Set the size of the ICMP data payload in bytes (excluding the size of Ethernet, IP, and ICMP headers). The default value is 56 bytes. The valid range is 2-1452 bytes.

Payload Data Pattern : Set the pattern used in the ICMP data payload. The default value is 0. The valid range is 0-255.

Packet Count : Select the number of PING requests sent. The default value is 5. The valid range is 1-60.

VID for Source Interface : This field can be used to force the test to use a specific local VLAN interface as the source interface. Leave this field empty for automatic selection based on routing configuration. **Note**: You may only specify either the VID or the IP Address for the source interface.

Source Port Number : This field can be used to force the test to use a specific local interface with the specified port number as the source interface. The specified port must be configured with a suitable IP address. Leave this field empty for automatic selection based on routing configuration. **Note**: You may only specify either the Source Port Number or the IP Address for the source interface.

Address for Source Interface : This field can be used to force the test to use a specific local interface with the specified IP address as the source interface. The specified IP address must be configured on a local interface. Leave this field empty for automatic selection based on routing configuration. **Note**: You may only specify either the VID or the IP Address for the source interface.

Quiet (only print result) : Checking this option will not print the result of each ping request but will only show the result.

Start : Click the “Start” button to start to ping the target IP Address.

New Ping : Click to start a new Ping diagnostics.

After you press the Start button, ICMP packets are transmitted, and the sequence number and round trip time are displayed upon reception of a reply.

The amount of data received inside of an IP packet of type ICMP ECHO_REPLY will always be 8 bytes more than the requested payload data size (the difference is the ICMP header).

The page refreshes automatically until responses to all packets are received, or until a timeout occurs.

Ping6 output looks like the following:

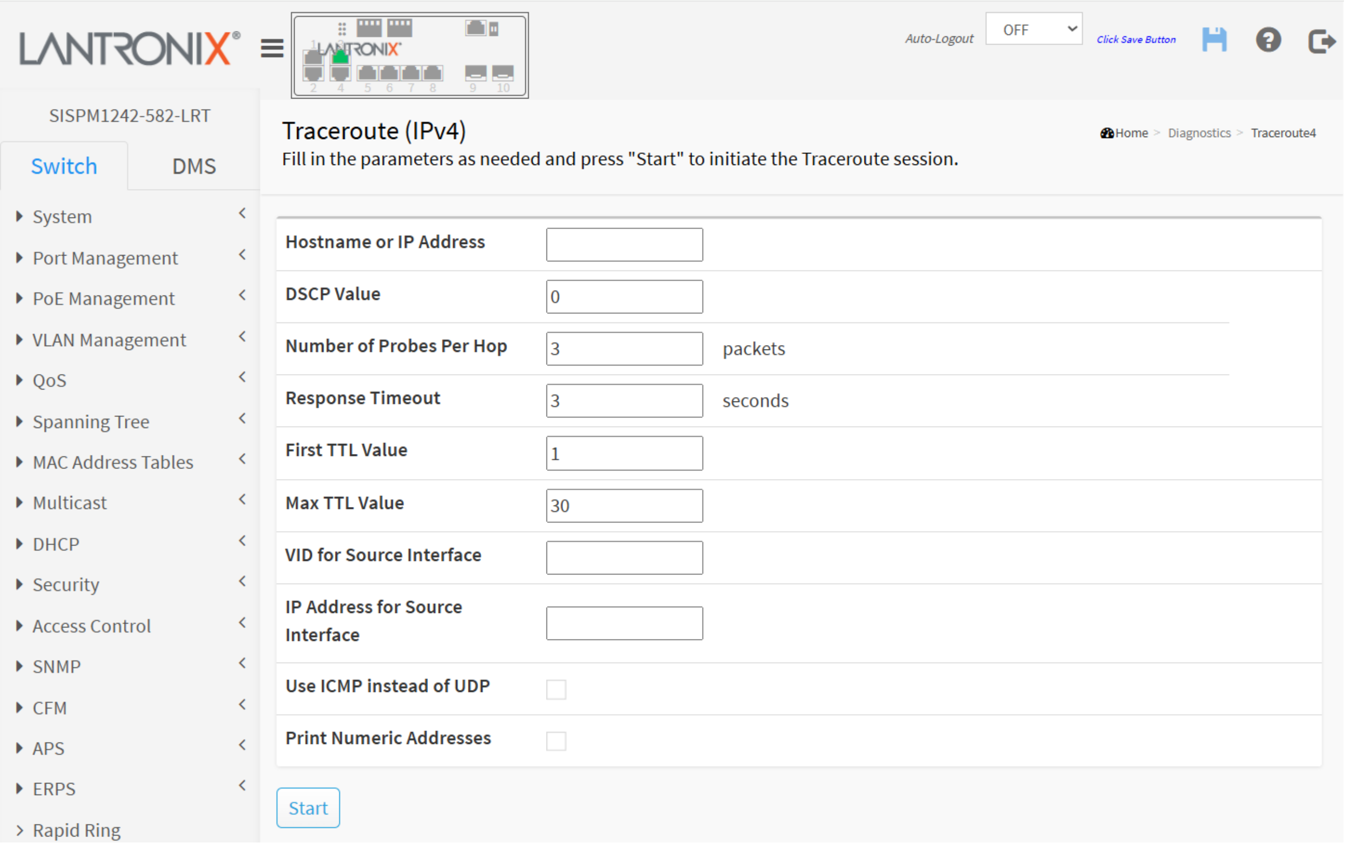
```
PING 2001::01 (2001::1) from 2001::3: 56 data bytes
64 bytes from 2001::1: seq=0 ttl=64 time=2.118 ms
64 bytes from 2001::1: seq=1 ttl=64 time=2.009 ms
64 bytes from 2001::1: seq=2 ttl=64 time=1.852 ms
64 bytes from 2001::1: seq=3 ttl=64 time=2.869 ms
64 bytes from 2001::1: seq=4 ttl=64 time=1.845 ms
--- 2001::01 ping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max = 1.845/2.138/2.869 ms
```

Traceroute (IPv4)

This page lets you perform a traceroute test over IPv4 towards a remote host. Traceroute is a diagnostic tool for displaying the route and measuring transit delays of packets across an IPv4 network.

To start a traceroute in the web UI:

1. Go to Diagnostics > Traceroute4.
2. Fill in the parameters as needed.
3. Click **Start**.



Traceroute (IPv4)

Fill in the parameters as needed and press "Start" to initiate the Traceroute session.

Hostname or IP Address		
DSCP Value	0	
Number of Probes Per Hop	3	packets
Response Timeout	3	seconds
First TTL Value	1	
Max TTL Value	30	
VID for Source Interface		
IP Address for Source Interface		
Use ICMP instead of UDP	□	
Print Numeric Addresses	□	

Start

Parameter descriptions:

Hostname or IP Address : The destination IP Address.

DSCP Value : This value is used for the DSCP value in the IPv4 header. The default value is 0. The valid range is 0-63.

Number of Probes Per Hop : Determines the number of probes (packets) sent for each hop. The default value is 3. The valid range is 1-60.

Response Timeout : Determines the number of seconds to wait for a reply to a sent request. The default number is 3 seconds. The valid range is 1-86400.

First TTL Value : Determines the value of the Time-To-Live (TTL) field in the IPv4 header in the first packet sent. The default number is 1. The valid range is 1-30.

Max TTL Value : Determines the maximum value of the Time-To-Live (TTL) field in the IPv4 header. If this value is reached before the specified remote host is reached the test stops. The default number is 30. The valid range is 1-255.

VID for Source Interface : This field can be used to force the test to use a specific local VLAN interface as the source interface. Leave this field empty for automatic selection based on routing configuration. **Note**: You may only specify either the VID or the IP Address for the source interface.

Address for Source Interface : This field can be used to force the test to use a specific local interface with the specified IP address as the source interface. The specified IP address must be configured on a local interface. Leave this field empty for automatic selection based on routing configuration. **Note**: You may only specify either the VID or the IP Address for the source interface.

Use ICMP instead of UDP : By default, the traceroute command will use UDP datagrams. Selecting this option forces it to use ICMP ECHO packets instead.

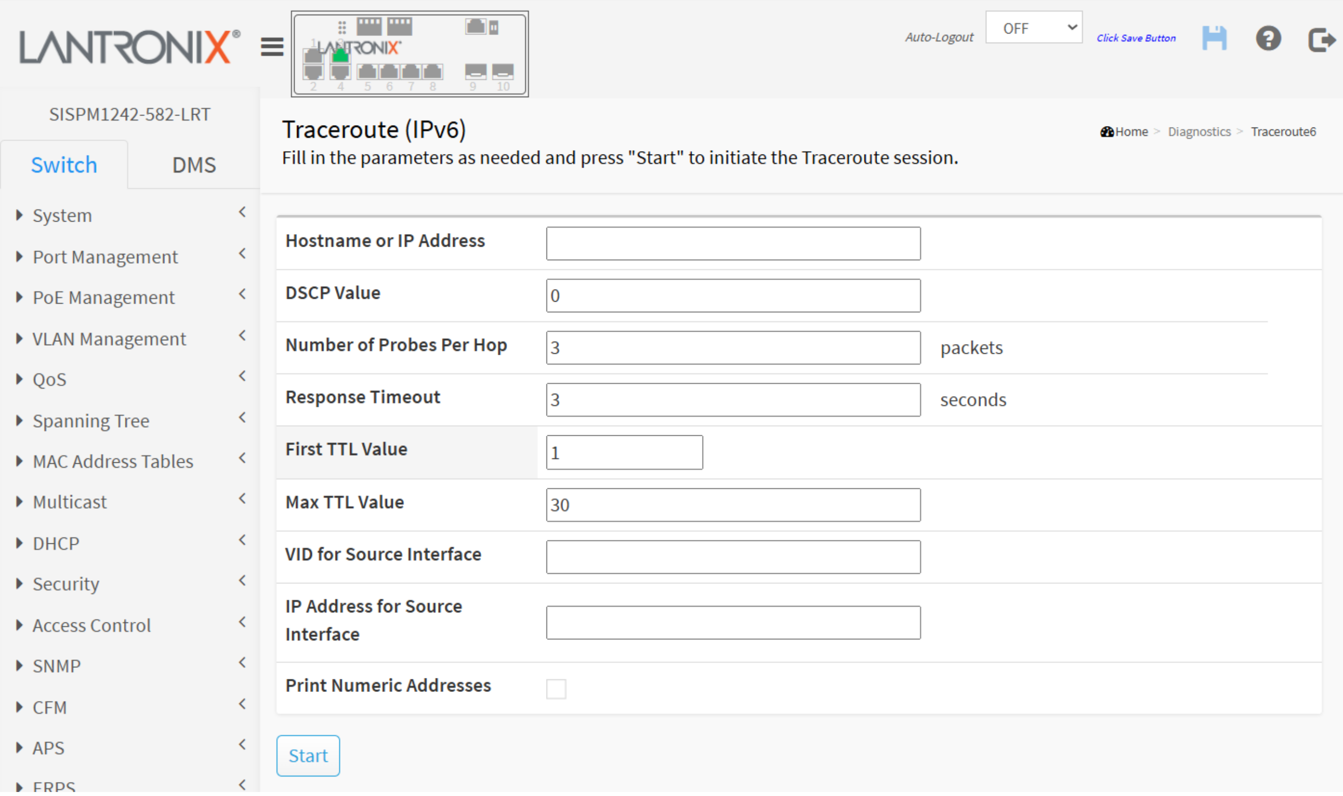
Print Numeric Addresses : By default, the traceroute command will print out hop information using a reverse DNS lookup for the acquired host IP addresses. This may slow down the display if the DNS information is not available. Selecting this option will prevent the reverse DNS lookup and force the traceroute command to print numeric IP addresses instead.

Traceroute (IPv6)

This page lets you perform a traceroute test over IPv6 towards a remote host. Traceroute is a diagnostic tool for displaying the route and measuring transit delays of packets across an IPv6 network.

To start an IPv6 Traceroute in the web UI:

1. Go to Diagnostics > Traceroute6.
2. Fill in the parameters as needed and click **Start** to initiate the Traceroute session.



Traceroute (IPv6)

Fill in the parameters as needed and press "Start" to initiate the Traceroute session.

Hostname or IP Address		
DSCP Value	0	
Number of Probes Per Hop	3	packets
Response Timeout	3	seconds
First TTL Value	1	
Max TTL Value	30	
VID for Source Interface		
IP Address for Source Interface		
Print Numeric Addresses	☐	

Parameter descriptions:

Hostname or IP Address : The destination IP Address.

DSCP Value : This value is used for the DSCP value in the IPv4 header. The default value is 0. The valid range is 0-255.

Number of Probes Per Hop : Determines the number of probes (packets) sent for each hop. The default value is 3 packets. The valid range is 1-60 packets.

Response Timeout : Determines the number of seconds to wait for a reply to a sent request. The default is 3 seconds. The valid range is 1-86400 seconds.

Max TTL Value : Determines the maximum value of the Time-To-Live (TTL) field in the IPv4 header. If this value is reached before the specified remote host is reached the test stops. The default is 255. The valid range is 1-255.

VID for Source Interface : This field can be used to force the test to use a specific local VLAN interface as the source interface. Leave this field empty for automatic selection based on routing configuration. **Note**: You may only specify either the VID or the IP Address for the source interface.

Address for Source Interface : This field can be used to force the test to use a specific local interface with the specified IP address as the source interface. The specified IP address must be configured on a local interface.

Leave this field empty for automatic selection based on routing configuration. **Note**: You may only specify either the VID or the IP Address for the source interface.

Print Numeric Addresses : By default, the traceroute command will print out hop information using a reverse DNS lookup for the acquired host IP addresses. This may slow down the display if the DNS information is not available. Selecting this option will prevent the reverse DNS lookup and force the traceroute command to print numeric IP addresses instead.

Start : Click the "Start" button to start the IPv6 Traceroute.

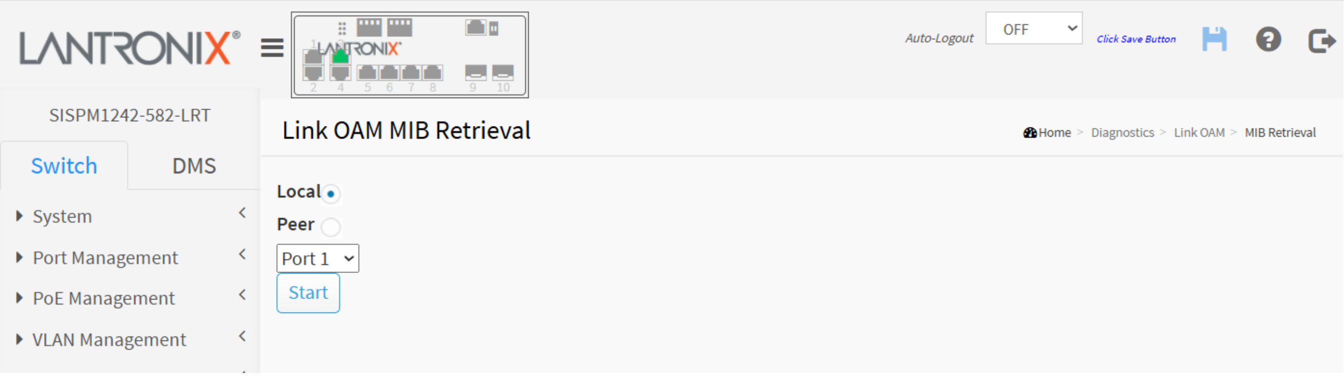
Link OAM MIB Retrieval

This page lets you retrieve the local or remote OAM MIB variable data on a particular port.

Select the appropriate radio button and enter the port number of the switch to retrieve the content of interest.

Click **Start** to retrieve the content.

Click **New Retrieval** to retrieve another content of interest.



Port: At the dropdown select the desired port.

Start: Click the button to begin the MIB retrieval.

Cable Diagnostics

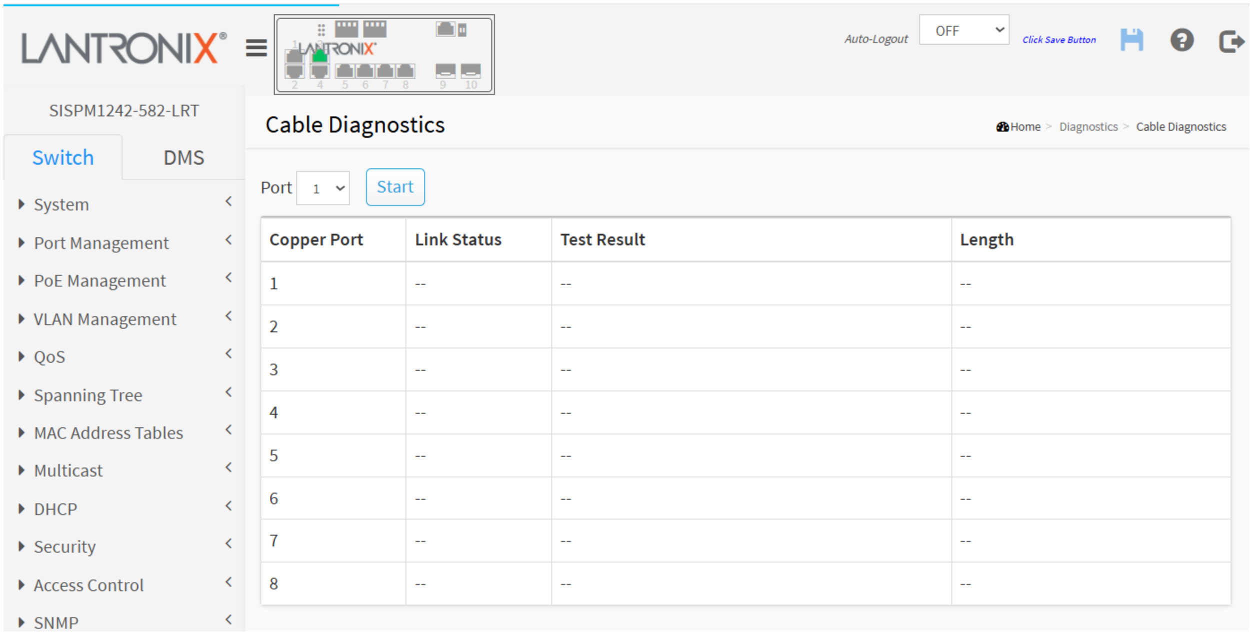
This page is used for running the Cable Diagnostics for 10/100 Mbps and 1G copper ports.

Click **Start** to run the diagnostics. This will take approximately 5 seconds.

While processing, the message "*Cable Diagnostics is running…*" is displayed.

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.

Note that 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.

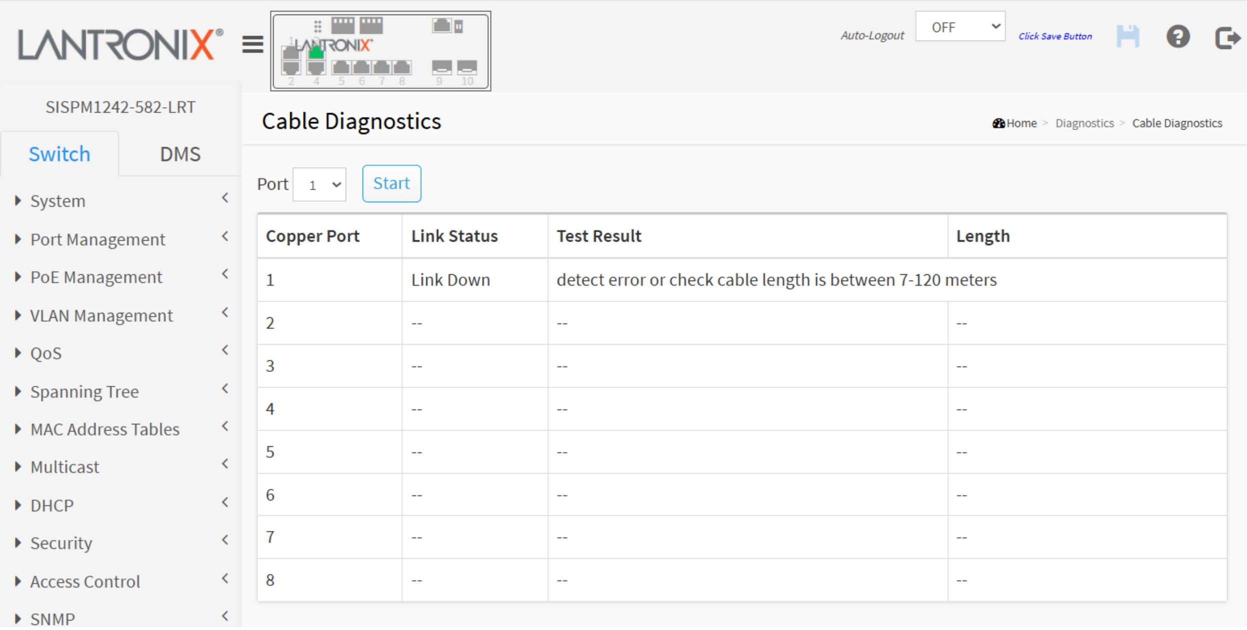


Cable Diagnostics

Port 1

Copper Port	Link Status	Test Result	Length
1	--	--	--
2	--	--	--
3	--	--	--
4	--	--	--
5	--	--	--
6	--	--	--
7	--	--	--
8	--	--	--

Example result



Cable Diagnostics

Port 1

Copper Port	Link Status	Test Result	Length
1	Link Down	detect error or check cable length is between 7-120 meters	
2	--	--	--
3	--	--	--
4	--	--	--
5	--	--	--
6	--	--	--
7	--	--	--
8	--	--	--

Parameter Descriptions:

Port: the port where you are requesting cable diagnostics.

Copper Port: the copper port number

Link Status: the status of the cable

- ***10M***: cable is link up and correct. Speed is 10Mbps
- ***100M***: cable is link up and correct. Speed is 100Mbps
- ***1G***: cable is link up and correct. Speed is 1Gbps
- ***2.5G***: cable is link up and correct. Speed is 2.5Gps
- ***Link Down:*** link down or cable not connected.

Test Result: test result of the cable

- ***OK:*** Correctly terminated pair
- ***Abnormal:*** incorrectly terminate pair or link down.

Length: The length in meters for the cable pair. The resolution is 3 meters. When Link Status is shown as follows the length has different definition.

2.5G:

The length is the minimum value of 4-pair. (Intel chip only detect length when cable is open.)

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.

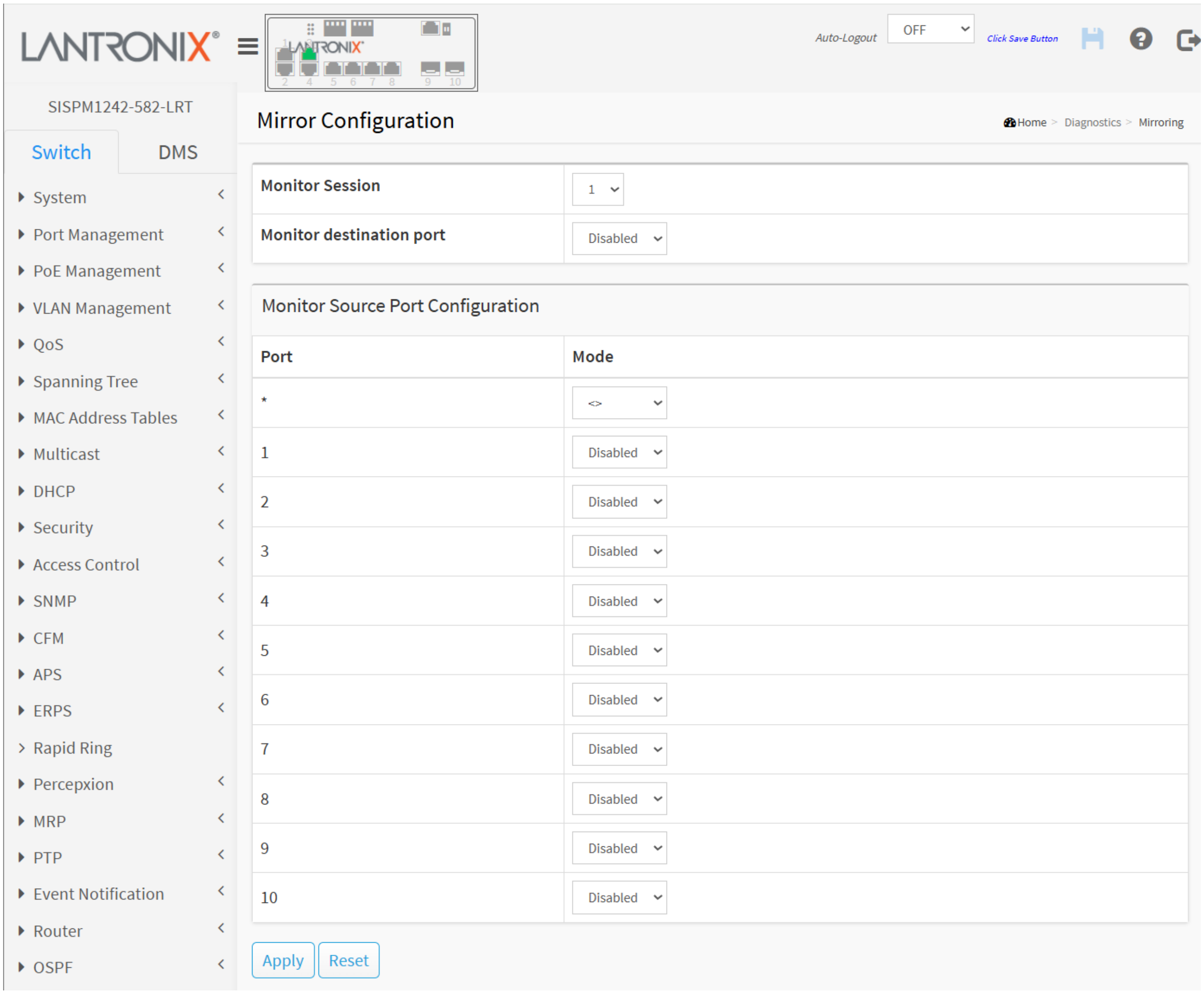
Mirroring

You can mirror traffic from any source port to a destination port for real-time analysis and 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.

Mirror Configuration is used to monitor network traffic. For example, assume that Port A and Port B are Destination Port and Monitored Port respectively, so the traffic received by Port B will be copied to Port A for monitoring.

To configure Port Mirroring in the web UI:

1. Go to Diagnostics > Mirroring.
2. Select the monitor session ID. Only one session may be active at a time.
3. Select the Monitor Destination Port.
4. Select a Mode (Disabled, TX only or RX only) for each monitored port.
5. Click the **Apply** button.



Mirror Configuration

Monitor Session	1
Monitor destination port	Disabled

Monitor Source Port Configuration

Port	Mode
*	<>
1	Disabled
2	Disabled
3	Disabled
4	Disabled
5	Disabled
6	Disabled
7	Disabled
8	Disabled
9	Disabled
10	Disabled

Parameter descriptions:

Monitor Session : At the dropdown select a Session number (instance).

Monitor Destination Port : The Port to output the mirrored traffic (also known as the mirror port). Frames from ports that have either source (RX) or destination (TX) mirroring enabled are mirrored on this port.

Mirror Source Port Configuration : The source node configuration for monitor flow.

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

Mode : Select mirror mode.

- ***Rx only*** : Frames received on this port are mirrored on the mirror port. Frames transmitted are not mirrored.
- ***Tx only*** : Frames transmitted on this port are mirrored on the mirror port. Frames received are not mirrored.
- ***Disabled*** : Neither frames transmitted nor frames received are mirrored.
- ***Enabled*** : Frames received and frames transmitted are mirrored on the mirror port.

sFlow

sFlow allows for monitoring real-time data flow in switched networks.

Configuration

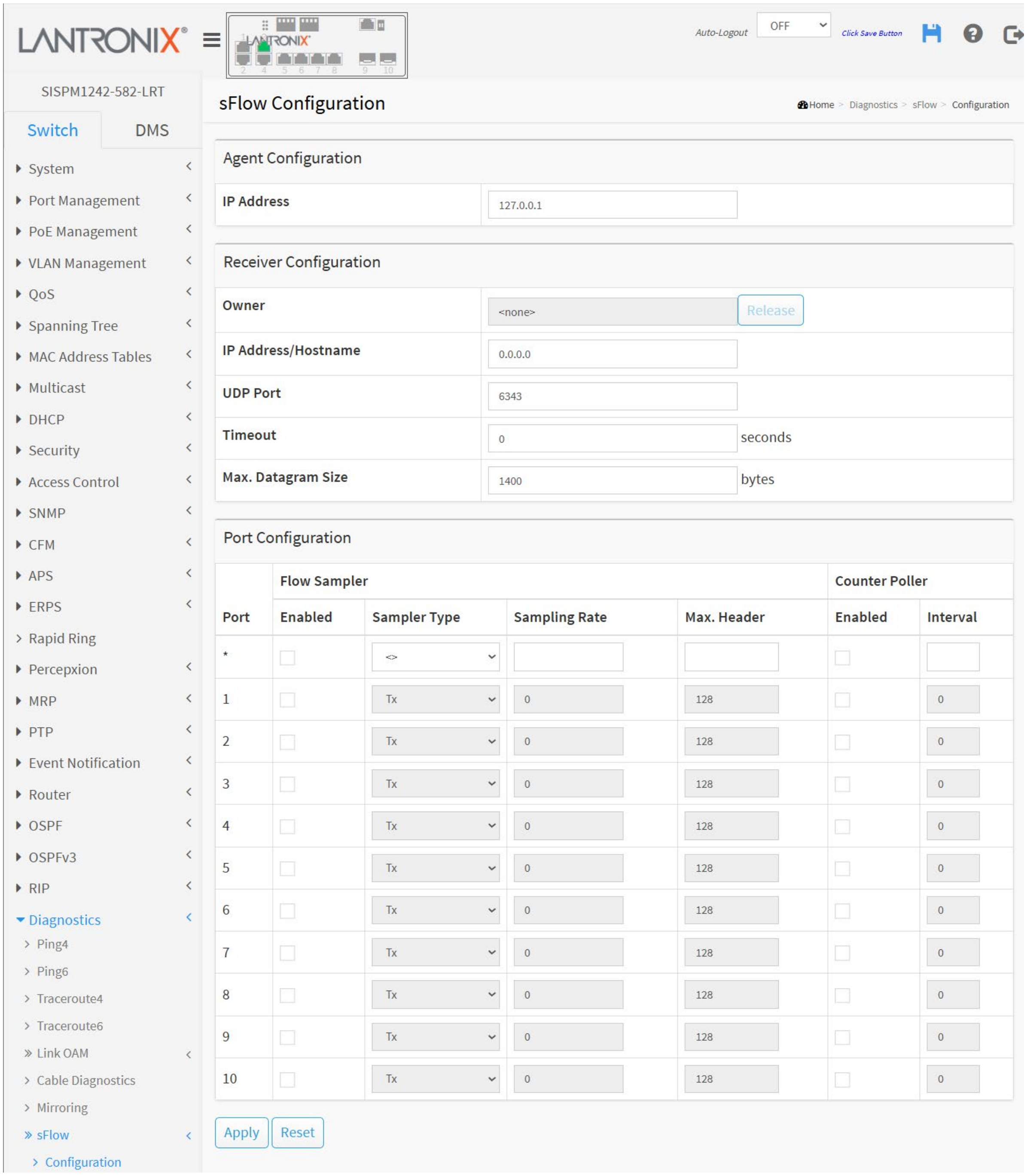
This page allows for configuring sFlow. The configuration is divided into two parts: Configuration of the sFlow receiver (a.k.a. sFlow collector) and configuration of per-port flow and counter samplers.

sFlow configuration does not persist to non-volatile memory, which means that a reboot 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 sFlow information can be found at http://sflow.org.

To configure sFlow in the web UI:

1. Go to Diagnostics > sFlow > Configuration.
2. Set the parameters.
3. Click **Apply**.



sFlow Configuration

Agent Configuration

IP Address	127.0.0.1

Receiver Configuration

Owner	<none>
IP Address/Hostname	0.0.0.0
UDP Port	6343
Timeout	0 seconds
Max. Datagram Size	1400 bytes

Port Configuration

	Flow Sampler				Counter Poller	
Port	Enabled	Sampler Type	Sampling Rate	Max. Header	Enabled	Interval
*	□	<>			□	
1	□	Tx	0	128	□	0
2	□	Tx	0	128	□	0
3	□	Tx	0	128	□	0
4	□	Tx	0	128	□	0
5	□	Tx	0	128	□	0
6	□	Tx	0	128	□	0
7	□	Tx	0	128	□	0
8	□	Tx	0	128	□	0
9	□	Tx	0	128	□	0
10	□	Tx	0	128	□	0

Parameter descriptions:

Agent Configuration

IP Address : The IP address used as the Agent IP address in sFlow datagrams. It serves as a unique key that will identify this agent over extended periods of time. Both IPv4 and IPv6 addresses are supported.

Receiver Configuration

Owner : sFlow can be configured via local management using the Web or CLI interface **or** via SNMP. This read-only field shows the owner of the current sFlow configuration and assumes values as follows:

- If sFlow is currently unconfigured/unclaimed, Owner contains <none>.

- If sFlow is currently configured through Web or CLI, Owner contains <Configured through local management>.
- If sFlow is currently configured through SNMP, the Owner contains a string identifying the sFlow receiver. If sFlow is configured through SNMP, all controls - except for the Release-button - are disabled to avoid inadvertent reconfiguration.

The Release button allows for releasing the current owner and disable sFlow sampling. The Release button is disabled if sFlow is currently unclaimed. If configured through SNMP, the release must be confirmed (a confirmation request will display).

Release button: Click to release the current owner and disable sFlow sampling. The Release button is disabled if sFlow is currently unclaimed. If configured via SNMP, the release must be confirmed (a confirmation request will display).

IP Address/Hostname : The IP address or hostname of the sFlow receiver. Both IPv4 and IPv6 addresses are supported.

UDP Port : The UDP port on which the sFlow receiver listens to sFlow datagrams. If set to 0 (zero), the default port (6343) is used.

Timeout : The number of seconds remaining before sampling stops and the current sFlow owner is released. While active, the current time left can be updated with a click on the Refresh-button. If locally managed, the timeout can be changed on the fly without affecting any other settings.

Max. Datagram Size : The maximum number of data bytes that can be sent in a single sample datagram. This should be set to a value that avoids fragmentation of the sFlow datagrams. The valid range is 200 to 1468 bytes and the default is 1400 bytes.

Port Configuration

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

Flow Sampler Enabled : Enables/disables flow sampling on this port.

Flow Sampler Sampling Rate : The statistical sampling rate for packet sampling. Set to N to sample on average 1/Nth of the packets transmitted/received on the port. Not all sampling rates are achievable. If an unsupported sampling rate is requested, the switch will automatically adjust it to the closest achievable. This will be reported back in this field.

Flow Sampler Max. Header : The maximum number of bytes that should be copied from a sampled packet to the sFlow datagram. The valid range is 14 - 200 bytes and the default is 128 bytes. If the maximum datagram size does not consider the maximum header size, samples may be dropped.

Counter Poller Enabled : Enables/disables counter polling on this port.

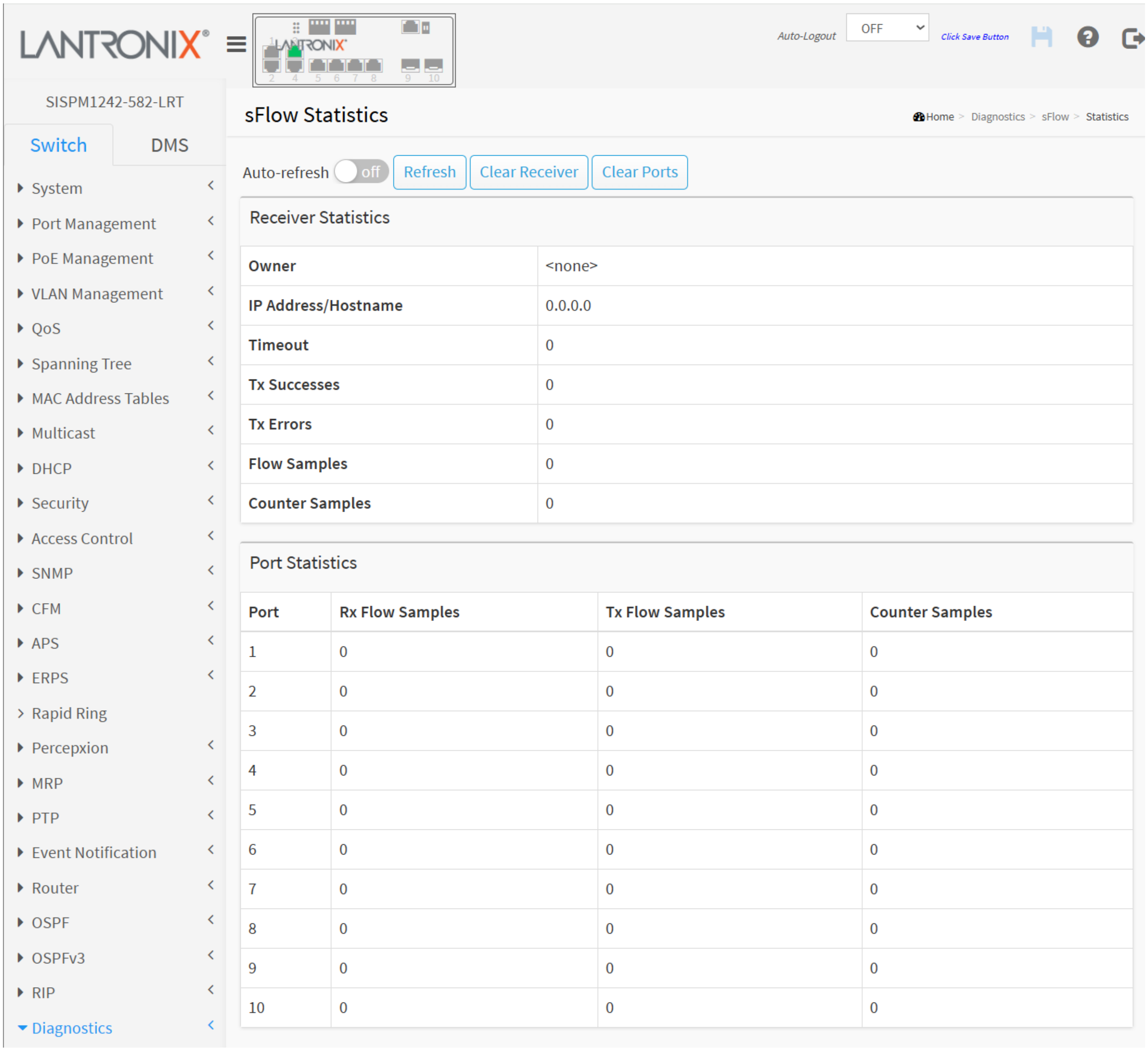
Counter Poller Interval : With counter polling enabled, this specifies the interval - in seconds - between counter poller samples.

Statistics

This page shows sFlow receiver and per-port statistics.

To display sFlow statistics in the web UI:

1. Go to Diagnostics > sFlow > Statistics.
2. **Auto-refresh** will refresh the page every 3 seconds. **Refresh** will refresh the page immediately. Clear the Receiver Statistics or Port Statistics on the page by clicking the appropriate **Clear** button .



sFlow Statistics

Receiver Statistics

Owner	<none>
IP Address/Hostname	0.0.0.0
Timeout	0
Tx Successes	0
Tx Errors	0
Flow Samples	0
Counter Samples	0

Port Statistics

Port	Rx Flow Samples	Tx Flow Samples	Counter Samples
1	0	0	0
2	0	0	0
3	0	0	0
4	0	0	0
5	0	0	0
6	0	0	0
7	0	0	0
8	0	0	0
9	0	0	0
10	0	0	0

Parameter descriptions:

Clear Receiver : Clears the sFlow receiver counters.

Clear Ports : Clears the per-port counters.

Receiver Statistics

Owner : Shows the current owner of the sFlow configuration. It assumes one of these three values:

- If sFlow is currently unconfigured or unclaimed, the Owner field contains <none>.
- If sFlow is currently configured via Web or CLI, Owner contains <Configured via local management>.
- If sFlow is currently configured via SNMP, Owner contains a string identifying the sFlow receiver.`

IP Address/Hostname : The IP address or hostname of the sFlow receiver.

Timeout : The number of seconds remaining before sampling stops and the current sFlow owner is released.

Tx Successes : The number of UDP datagrams successfully sent to the sFlow receiver.

Tx Errors : The number of UDP datagrams that has failed transmission. The most common source of errors is invalid sFlow receiver IP/hostname configuration. To diagnose, paste the receiver's IP address/hostname into the Ping Web page (Diagnostics > Ping/Ping6).

Flow Samples : The total number of flow samples sent to the sFlow receiver.

Counter Samples : The total number of counter samples sent to the sFlow receiver.

Port Statistics

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

Rx and Tx Flow Samples : The number of flow samples sent to the sFlow receiver originating from this port. Here, flow samples are divided into Rx and Tx flow samples, where Rx flow samples contains the number of packets that were sampled upon reception (ingress) on the port and Tx flow samples contains the number of packets that were sampled upon transmission (egress) on the port.

Counter Samples : The total number of counter samples sent to the sFlow receiver originating from this port.

27. Maintenance

This chapter describes configuration and management operations for the switch.

Configuration

The switch stores its configuration in several files in text format. The files are either virtual (RAM-based) or stored in flash on the switch. There are three system files:

- **running-config**: A virtual file that represents the currently active configuration on the switch. This file is volatile.
- **startup-config**: The startup configuration for the switch, read at boot time. If this file doesn't exist at boot time, the switch will start up in default configuration.
- **default-config**: A read-only file with vendor-specific configuration. This file is read when the system is restored to default settings.

Up to 99 other files can be stored in flash, typically for configuration backups or alternative configurations.

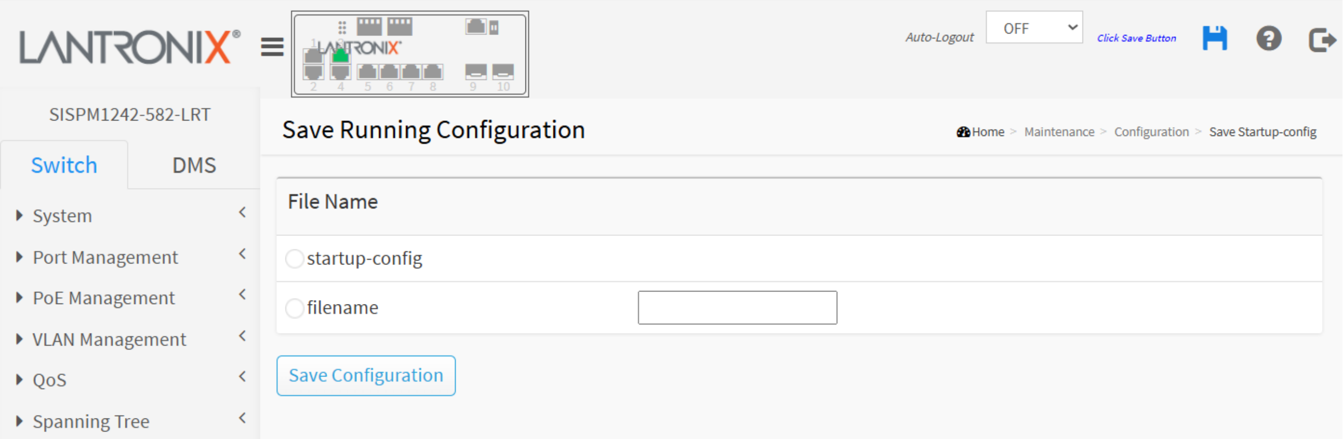
Save running-config to startup-config

This copies the running-config file to startup-config, ensuring that the current active configuration will be used at the next reboot.

Note: Clicking the 💾 icon on the Information bar will also save the running-config to startup-config.

To save the running configuration to startup-config in the web UI:

1. Go to Maintenance > Configuration > Save Startup-config.
2. Select the startup-config button. Alternatively, enter a filename to save the configuration to a file by a different name.
3. Click the **Save Configuration** button.



Save Running Configuration

File Name

○ startup-config

○ filename

Save Configuration

Description:

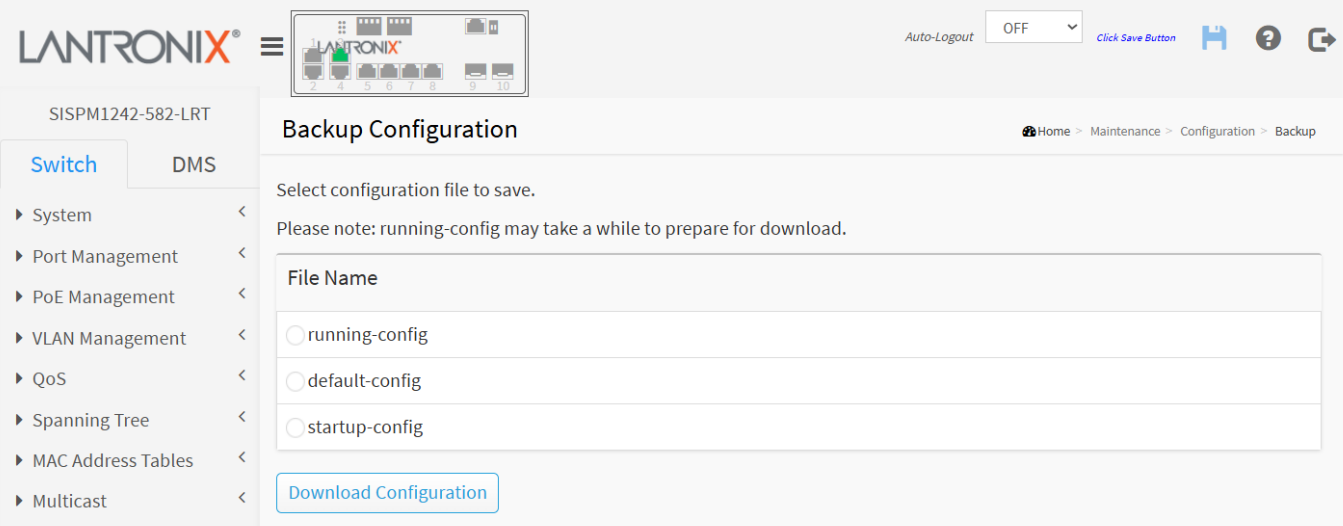
Save Configuration : Click to save the configuration; the running configuration will be written to flash memory for system boot up to load this startup configuration file.

Backup Configuration

This page lets you download the switch configuration for maintenance needs. Configuration files will be exported in text format. It is possible to download any of the files on the switch to the web browser. Downloading the running-config may take a little while to complete, as the file must be prepared before backup.

To download a configuration file from the web UI:

1. Go to Maintenance > Configuration > Backup.
2. Select a File Name.
3. Click the **Download Configuration** button.



Backup Configuration

Select configuration file to save.

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

File Name
○ running-config
○ default-config
○ startup-config

Download Configuration

Parameter descriptions:

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

default-config : A read-only file with vendor-specific configuration. This file is read when the system is restored to default settings.

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

Buttons

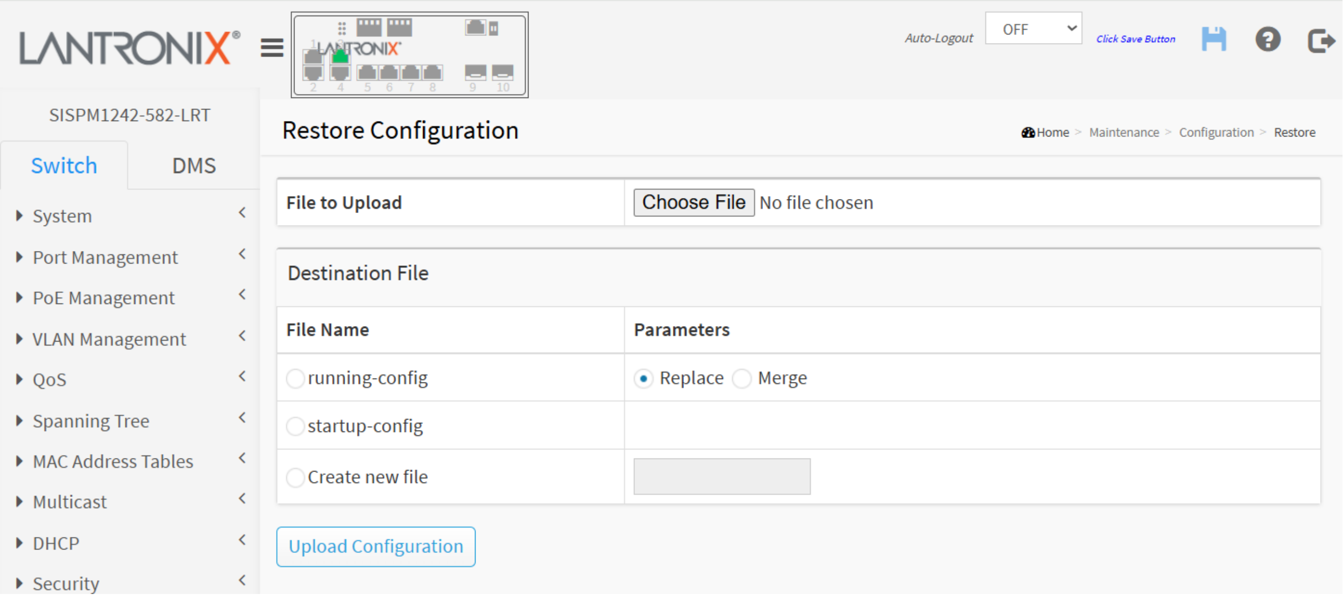
Download Configuration : Click the button then the switch will start to transfer the configuration file to your workstation.

Restore Configuration

You can upload a file from the web browser to all the files on the switch, except *default-config*, which is read-only.

To restore configuration:

1. Go to Maintenance > Configuration > Restore.
2. Select the file to upload.
3. Select the destination file on the target.
4. Click **Upload Configuration**.



Restore Configuration

File to Upload	Choose File No file chosen

Destination File

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

Upload Configuration

If the destination is running-config, the file will be applied to the switch configuration in one of two ways:

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

If the flash file system is full (i.e. it contains *default-config* and 100 other files, usually including *startup-config*), it is not possible to create new files. A file must be overwritten or deleted first.

Parameter descriptions:

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

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

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

Create new file : Enter a filename to restore the configuration as a new file.

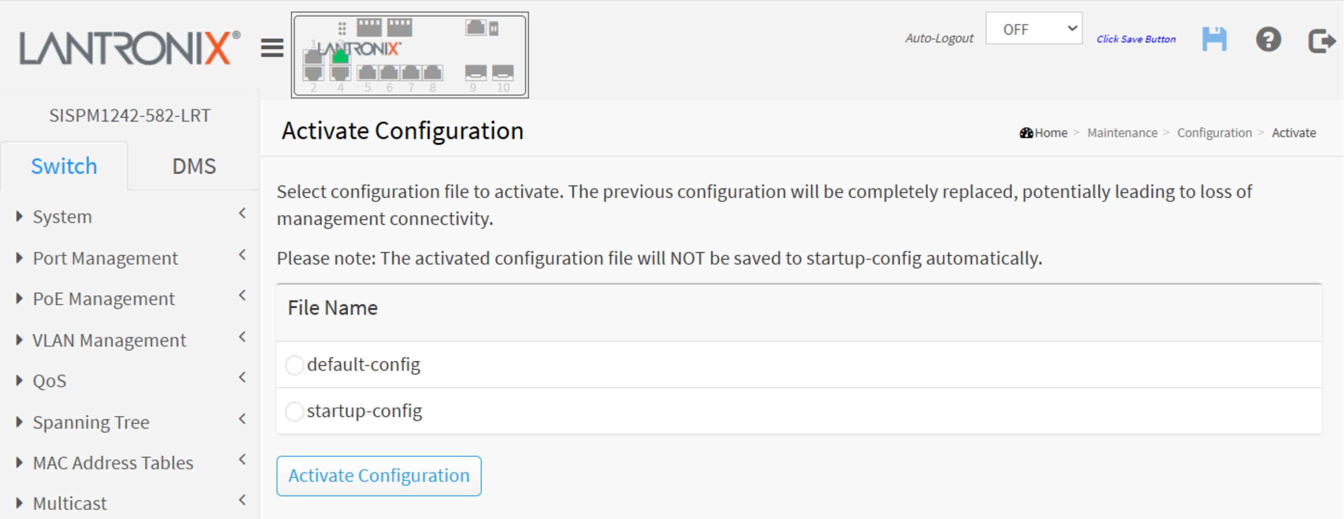
Activate

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

Select the file to activate and click the **Activate Configuration** button. This will initiate the process of completely replacing the existing config with that of the selected file.

To activate a configuration in the web UI:

1. Go to Maintenance > Configuration > Activate. Read the messages displayed on the page.



Activate Configuration

Select configuration file to activate. The previous configuration will be completely replaced, potentially leading to loss of management connectivity.

Please note: The activated configuration file will NOT be saved to startup-config automatically.

File Name
○ default-config
○ startup-config

2. Select a configuration file to activate.
3. Click the **Activate Configuration** button. The selected file will be activated to be the switch's running configuration.

Parameter descriptions:

File Name : Check a radio button for the file to be activated.

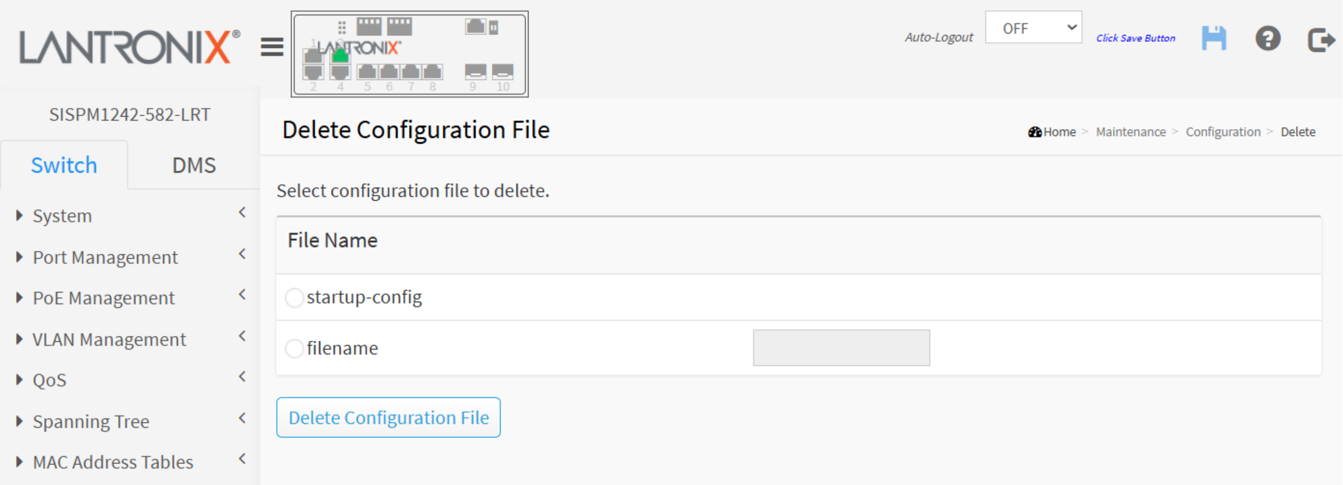
- ***default-config*** : A read-only file with vendor-specific configuration. This file is read when the system is restored to default settings.
- ***startup-config*** : The startup configuration for the switch, read at boot time.

Delete

You can delete any of the writable files stored in flash, including startup-config. If this is done and the switch is rebooted without a prior save operation, this effectively resets the switch to its default configuration.

To delete a configuration file in the web UI:

1. Go to Maintenance > Configuration > Delete.
2. Select a configuration file to delete.
3. Click the **Delete Configuration File** button.



Delete Configuration File

Select configuration file to delete.

File Name
○ startup-config
○ filename

Parameter descriptions:

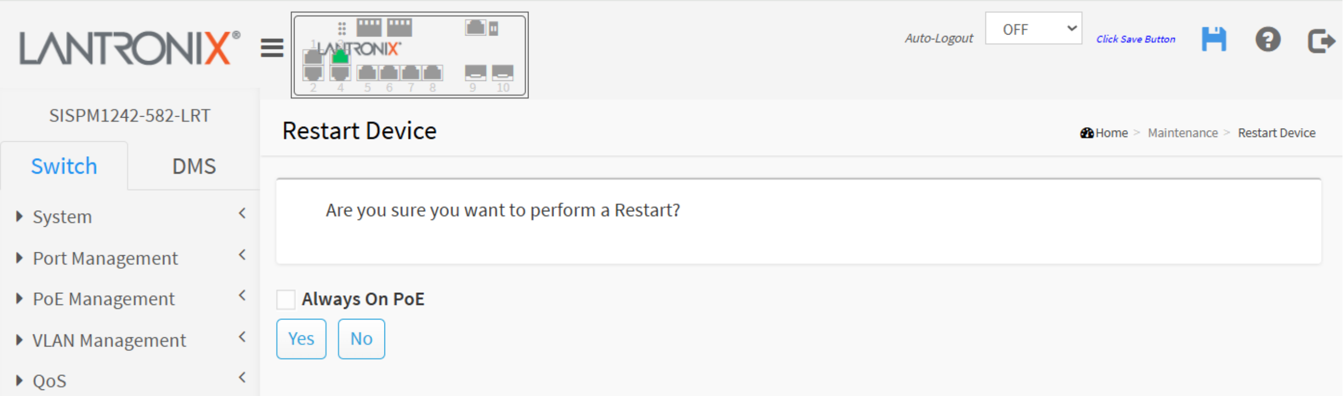
File Name : Select the configuration file to delete.

Restart Device

This command will perform a warm restart on the switch. After restart, the switch will boot normally. Any configuration files or scripts saved in the switch should be available afterwards.

To restart the switch in the Web UI:

1. Go to Maintenance > Restart Device.
2. At the "*Are you sure ...*?" prompt click **Yes**. The device will restart. Otherwise, click No to cancel the restart operation.



Restart Device

Are you sure you want to perform a Restart?

□ Always On PoE

Yes No

Parameter descriptions:

Always on PoE: If selected, during a warm restart the switch's PoE ports will maintain power to connected devices.

Message: *System restart in progress*

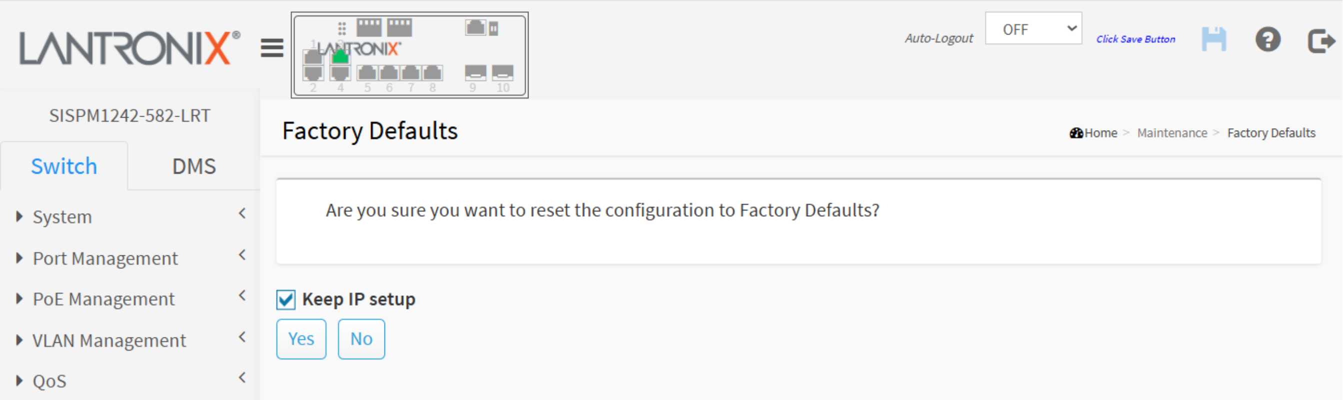
Please wait while the system restarts.

Factory Defaults

This page lets you restore the switch configuration to its factory default settings. Only the IP configuration is retained. The new configuration is available immediately, which means that no restart is necessary.

To restore the switch to its factory defaults in the web UI:

1. Go to Maintenance > Factory Defaults.
2. Check the **Keep IP setup** box if you want to keep the existing IP setup.
3. Click **Yes** to proceed with the reset to factory defaults operation.



Factory Defaults

Are you sure you want to reset the configuration to Factory Defaults?

☑ Keep IP setup

Yes No

Buttons

Keep IP setup : Check the box if you want to keep the current IP configuration.

Yes : Click to **Yes** button to reset the configuration to Factory Defaults.

No : Click to cancel the operation.

Note: Restoring factory default can also be performed by making a physical loopback between port 1 and port 2 within the first minute from switch reboot. In the first minute after boot, 'loopback' packets will be transmitted at port 1. If a 'loopback' packet is received at port 2 the switch will do a restore to default.

Hardware Factory Reset

Factory reset can be initiated by pressing the hardware Mode/Reset button on the front of the switch. The First Time Wizard will display after a hardware factory reset if you are configuring the switch using the Web interface.

Press and hold the Mode/Reset button until all port LEDs light (approximately 7 to 12 seconds), then release the button. This will set the unit back to its factory default IP address; log back in to display the startup wizard.

Firmware

This section lets you upgrade (update) device firmware and activate the alternate firmware image.

Firmware Upgrade

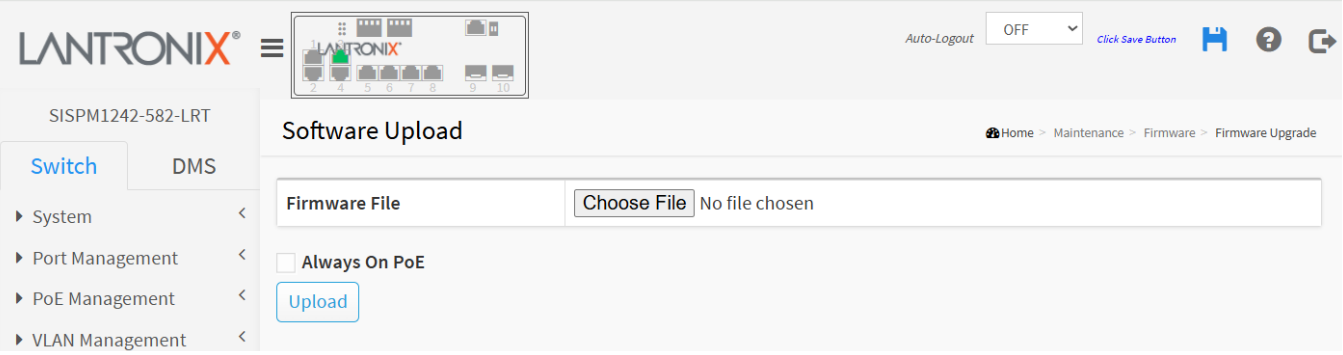
This page lets you update the switch firmware.

To update switch firmware in the web UI:

1. Go to Maintenance > Firmware > Firmware Upgrade.
2. Select the desired firmware file.
3. If persistent PoE is desired, select the **Always on PoE** box.
4. Click the **Upload** button.

After the software image is uploaded, a page announces that the firmware update is initiated. After about a minute, the firmware is updated and the switch restarts.

Warning*: While the firmware is being updated, Web access appears to be defunct. The front LED flashes Green/Off with a frequency of 10 Hz while the firmware update is in progress.* ***Do not restart or power off the device at this time*** *or the switch may fail to function afterwards.*



Software Upload

Firmware File	Choose File No file chosen

□ Always On PoE

Parameter descriptions:

Choose File : Click to search for the Firmware URL and filename.

Always on PoE: If selected, during a warm restart the switch's PoE ports will maintain power to connected devices.

Upload : Click to upload the selected firmware file.

Firmware Selection

This page displays information about the active and alternate (backup) firmware images in the device, and lets you revert to the alternate image.

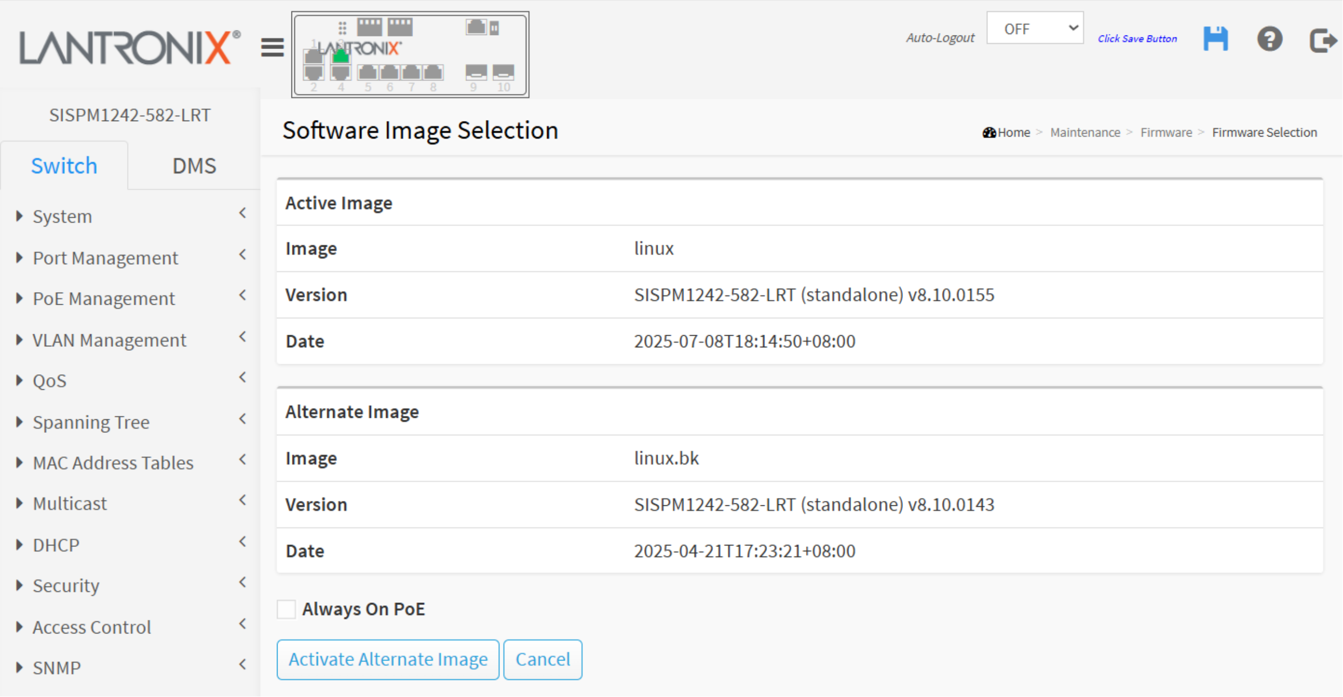
The web page displays two tables with information about the active and alternate firmware images.

Note:

- If the active firmware image is the alternate image, only the "Active Image" table is shown. In this case, the **Activate Alternate Image** button is also disabled.
- If the alternate image is active (due to a corruption of the primary image or by manual intervention), uploading a new firmware image to the device will automatically use the primary image and activate this.
- The firmware version and date information may be empty for older firmware releases. This does not constitute an error.

To show the firmware information or swap boot firmware in the web UI:

1. Go to Maintenance > Firmware > Firmware Selection. The Software Image Selection page is displayed.
2. Click the **Activate Alternate Image** button to swap firmware versions.



Software Image Selection

Active Image	
Image	linux
Version	SISPM1242-582-LRT (standalone) v8.10.0155
Date	2025-07-08T18:14:50+08:00

Alternate Image	
Image	linux.bk
Version	SISPM1242-582-LRT (standalone) v8.10.0143
Date	2025-04-21T17:23:21+08:00

☐ Always On PoE

Software Image Selection

Image : The file name of the firmware image, from when the image was last updated.

Version : The version of the firmware image.

Date : The date that the firmware was produced.

Buttons

Activate Alternate Image : Click to use the “alternate image”. This button may be disabled depending on system state.

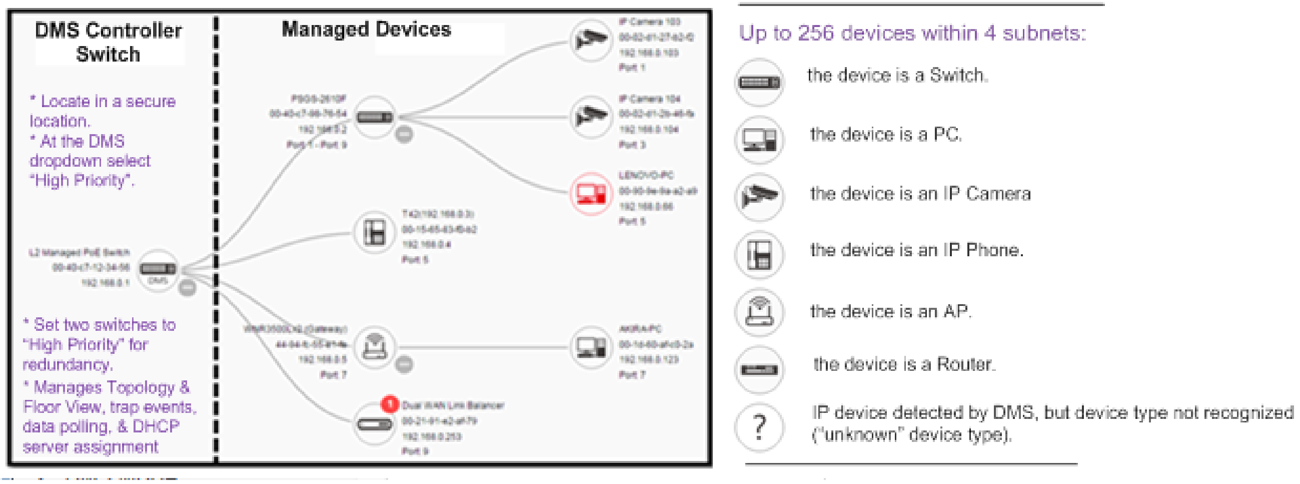
Cancel : Click to cancel activating the alternate image. Navigates away from this page.

28. DMS (Device Management System)

This chapter describes the integrated Device Management System (DMS) software that provides a unique set of value-added features and capabilities that provide lower overall cost, less downtime, and easier management and maintenance of the entire network.

DMS Mode

- Configure DMS mode and monitor device numbers/ DMS Controller Switch IP.
- DMS is controlled by the **DMS Controller switch**, as specified by the DMS Mode selection.
- The DMS Controller Switch controls syncing DMS information to manage Topology View, Floor View, and trap event / data polling / DHCP server assignment.

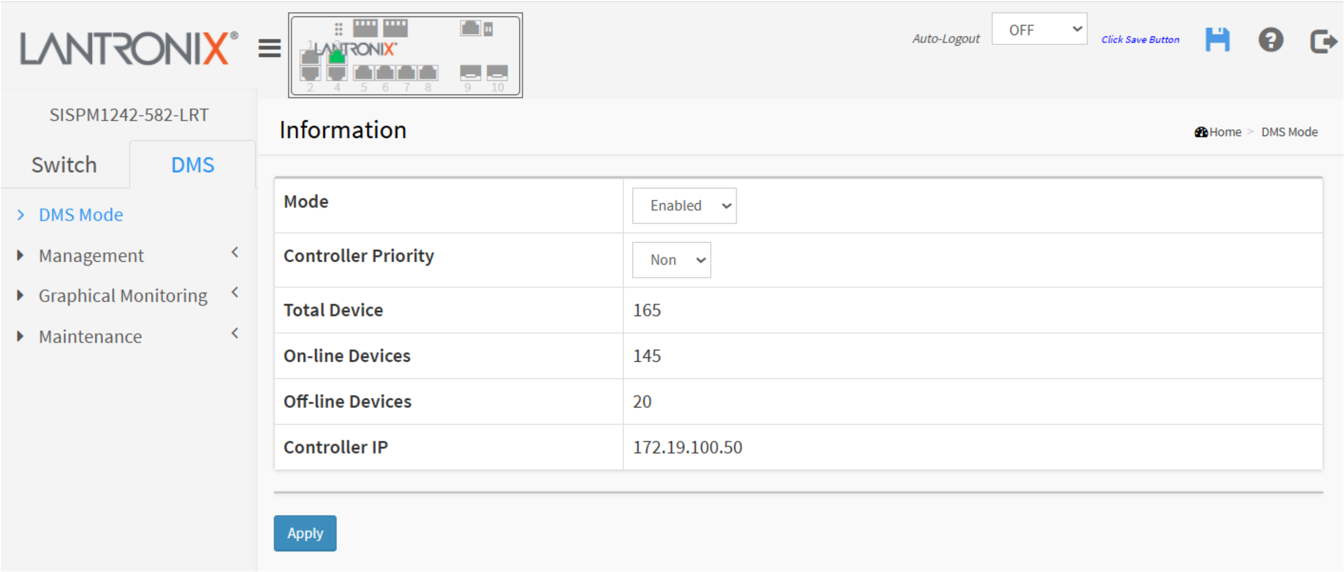

DMS Controller Switch
Managed Devices
* Locate in a secure location.
* At the DMS dropdown select "High Priority".
* Set two switches to "High Priority" for redundancy.
* Manages Topology & Floor View, trap events, data polling, & DHCP server assignment
L2 Managed PoE Switch
DMS
IP Camera 103
IP Camera 104
LENOVO-PC
Dual WAN Link Balancer
Up to 256 devices within 4 subnets:
the device is a Switch.
the device is a PC.
the device is an IP Camera
the device is an IP Phone.
the device is an AP.
the device is a Router.
?
IP device detected by DMS, but device type not recognized ("unknown" device type).

1. If there are more than two switches set as High-priority or no High-priority mode switch, the Switch with the longer system uptime will be selected as the DMS Controller switch. If two switches have same up time, the switch with the smaller MAC address will be assigned as the DMS Controller Switch.
2. You can set two switches to High Priority for Controller Switch redundancy.
3. The DMS Controller Switch should be put in a secure location such as a server room, with access/authority limited to IT staff.
4. The DMS Controller Switch is the center of IP / Event management to operate the DMS:
    a. When enabled DHCP Server mode in DMS network, the DMS Controller switch is responsible for assigning IP address for all devices.

The DMS Controller Switch will Collect, Poll, and Sync DMS information, and act as the Event Notification control center to manage all device information.

DMS Information

The DMS Information page lets you enable and disable DMS mode and specify DMS Controller Priority. DMS is controlled by the DMS Controller switch, as specified by the DMS Mode selection. The DMS Controller Switch controls syncing DMS information to manage Topology View, Floor View, and trap event / data polling / DHCP server assignment.



Mode	Enabled
Controller Priority	Non
Total Device	165
On-line Devices	145
Off-line Devices	20
Controller IP	172.19.100.50

Mode: At the dropdown select Enabled or Disabled for the DMS function globally. The default is Enabled.

Controller Priority: At the dropdown select a "Controller Priority" to be used when enabling DMS:

- ***High***: High priority; this switch will become the “Controller” (Master) switch.
- ***Mid***: Mid-level priority.
- ***Low***: Low level priority.
- ***Non***: the switch will never become the Controller switch (default).

Total Device: Displays the number of IP devices that are detected and displayed in Topology view.

On-Line Devices: Displays the number of IP devices on-line in Topology view.

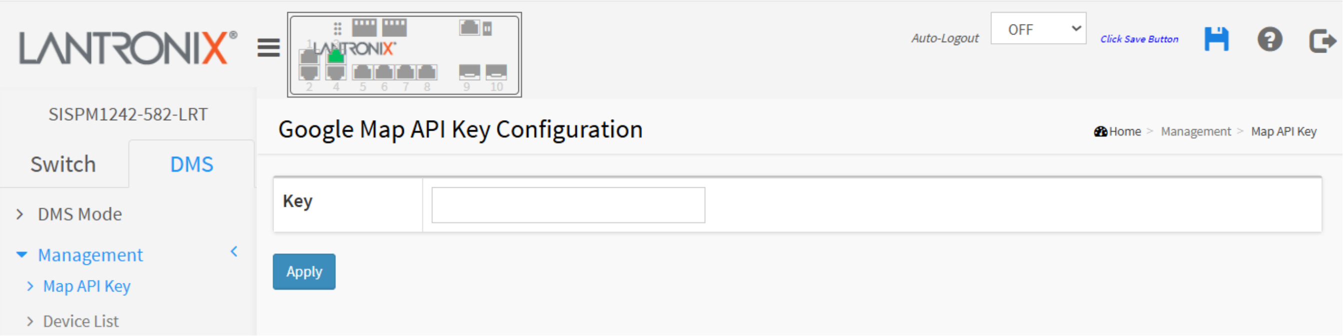
Off-Line Devices: Displays the number of IP devices off-line in the topology view.

Controller IP: Displays the IP address of the Controller (Master) switch.

DMS Management

Map API Key

The Google Map API key allows you to load maps for the DMS Map View feature. Visit the Google website below and follow the directions to get an API key: https://developers.google.com/maps/documentation/directions/get-api-key.



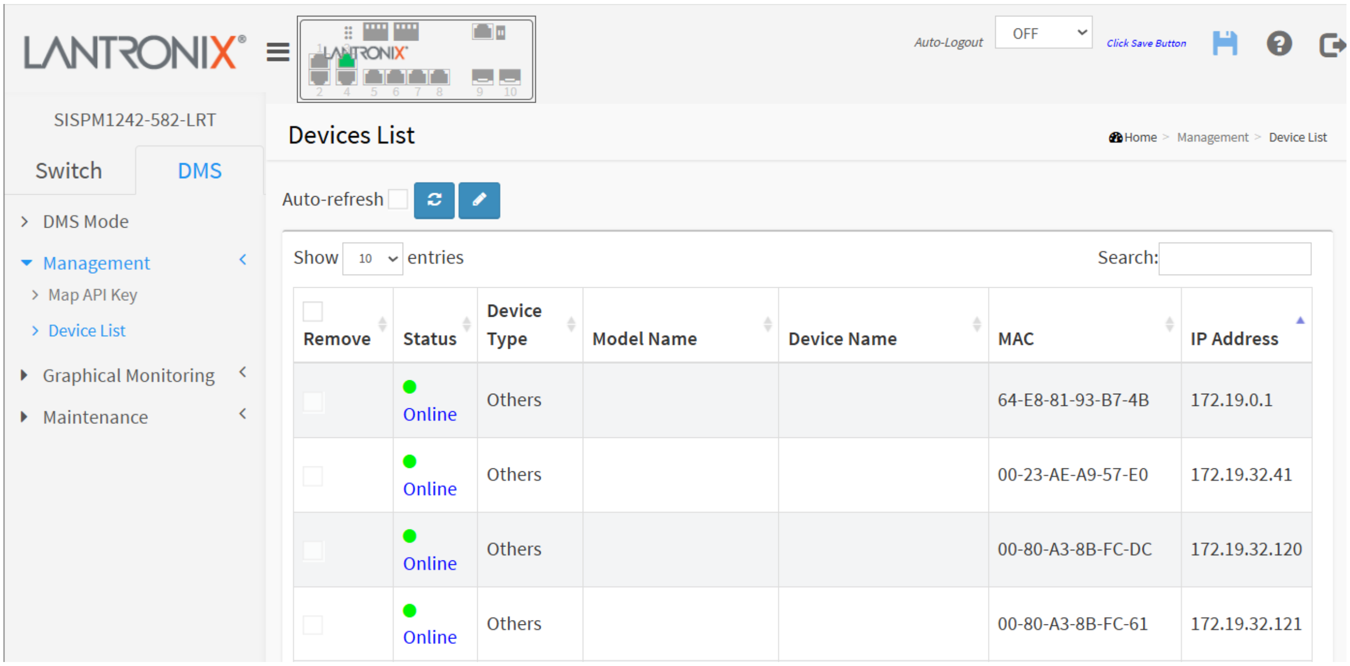
Key: Enter the Google API Key.

Buttons

Apply: Click to save changes.

Device List

This page provides an overview of the devices list. It initially displays with seven columns:



Remove	Status	Device Type	Model Name	Device Name	MAC	IP Address
□	● Online	Others			64-E8-81-93-B7-4B	172.19.0.1
□	● Online	Others			00-23-AE-A9-57-E0	172.19.32.41
□	● Online	Others			00-80-A3-8B-FC-DC	172.19.32.120
□	● Online	Others			00-80-A3-8B-FC-61	172.19.32.121

Parameter Descriptions

Remove: If selected, deletes the off-line device from the list.

Status: Displays whether the device is Online or Offline. Click the linked text to display the Maintenance > Diagnostics page.

Device Type: The type of the network connectivity devices such as PC, SWITCH, AP, IP Cam, IP Phone, or Others.

Model Name: The model name of the network connectivity devices.

Device Name: The device name of the network connectivity devices.

MAC: The mac address of the device.

IP Address: The IP address of the network connectivity device.

Edit mode columns:

Edit: Displays edit mode. The following fields are editable.

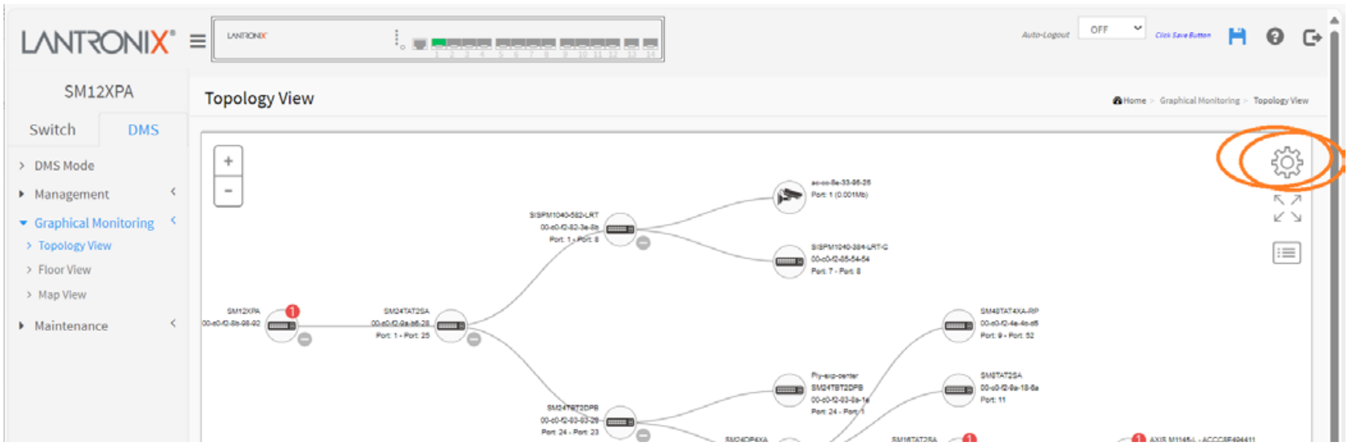
- ***Device Name***: Entry field to edit a device’s Name.
- ***HTTP Port***: Entry field to edit a device’s HTTP port number.
- ***User Name***: Entry field to edit a device’s user name.
- ***User Password***: Entry field to edit a device’s user password.

DMS Graphical Monitoring

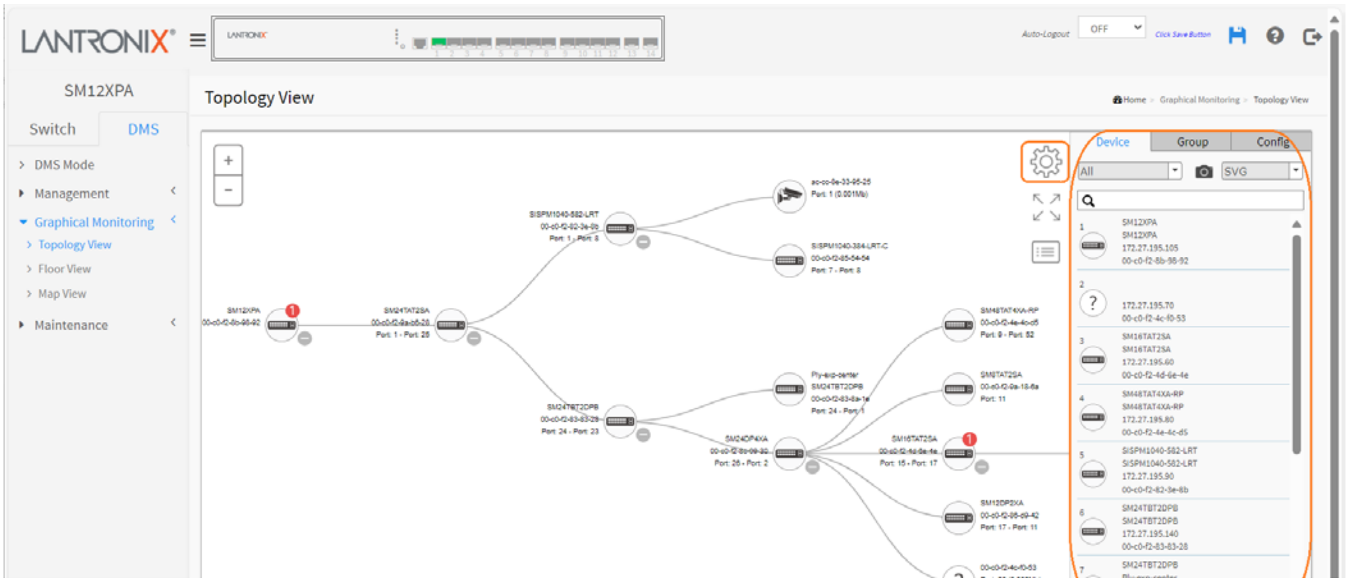
Topology View

DMS can automatically discover all IP devices and display the devices by graphic networking topology view. You can manage and monitor them in the Topology View, such as to remotely diagnose the cable connection status, auto alarm notifications on critical events, and remotely reboot a device. You can use the DMS platform to solve network issues anytime and anywhere by tablet or smart phone and keep the network working smoothly.

On the DMS menu, go to Graphical Monitoring > Topology View to display a visual representation of the network topology:



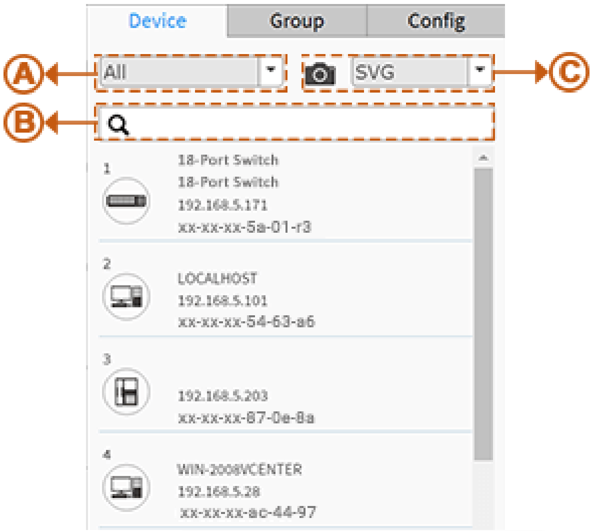
Click the Setting icon (⚙) to display additional right-hand menu items:


LANTRONIX
Auto-Logout
OFF
Click Save Button
SM12XPA
Switch
DMS
DMS Mode
Management
Graphical Monitoring
Topology View
Floor View
Map View
Maintenance
Topology View
Home > Graphical Monitoring > Topology View
+
−
Device
Group
Config
All
SVG
1 SM12XPA SM12XPA 172.27.195.105 00-c0-f2-8b-98-92
2 172.27.195.70 00-c0-f2-4c-f0-53
3 SM16TAT2SA SM16TAT2SA 172.27.195.60 00-c0-f2-4d-6e-4e
4 SM48TAT4XA-RP SM48TAT4XA-RP 172.27.195.80 00-c0-f2-4e-4c-d5
5 SISPM1040-582-LRT SISPM1040-582-LRT 172.27.195.90 00-c0-f2-82-3e-8b
6 SM24TBT2DPB SM24TBT2DPB 172.27.195.140 00-c0-f2-83-83-28
7 SM24TBT2DPB

+ − : Icon with plus and minus marks to let you zoom in and zoom out the topology view. You can scroll up/down with mouse to achieve the same purpose.

In the upper right corner, there is a "Setting icon". When you click the icon, it will pop-up Device, Group, Config, export topology view and advanced search functions for the topology.

Device Search Console



1
18-Port Switch
18-Port Switch
192.168.5.171
xx-xx-xx-5a-01-r3

2
LOCALHOST
192.168.5.101
xx-xx-xx-54-63-a6

3
192.168.5.203
xx-xx-xx-87-0e-8a

4
WIN-2008VCENTER
192.168.5.28
xx-xx-xx-ac-44-97

Functions:

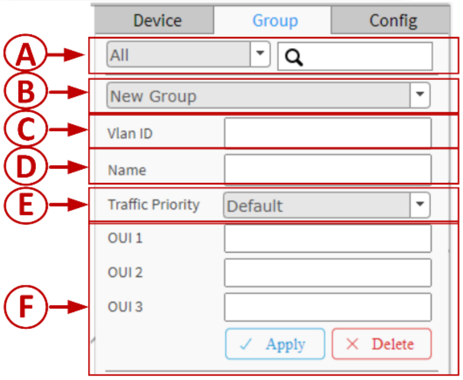
A Filter devices by Device Type

B Search devices by key words full text search

C Save the whole View to an SVG, PNG or PDF file.

Group Setting Console

- Uses MAC-based VLAN to isolate groups.
- One IP device only can join one VLAN group.



Functions:

A At the dropdown select the Group of devices to be displayed (e.g., ALL, SWITCH, PC, IP Camera, etc.)..

B At the dropdown select to create a new Group or select an existing Group name.

C Enter a VLAN ID for this Group.

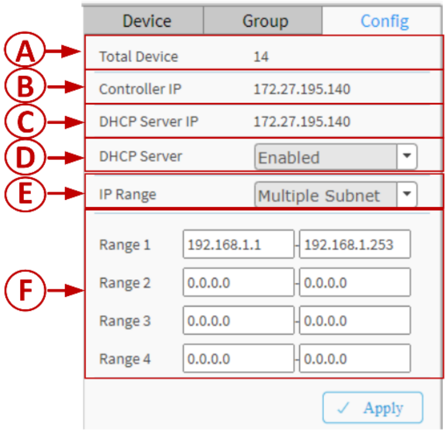
D Enter a Name for this Group.

E Traffic Priority; select 0 (low) -7 (high) or Default.

F OUI 1-3 for Organizationally Unique Identifier(s).

System Setting Console

Config Tab Functions:



Total Device	14
Controller IP	172.27.195.140
DHCP Server IP	172.27.195.140
DHCP Server	Enabled
IP Range	Multiple Subnet

Range 1	192.168.1.1	192.168.1.253
Range 2	0.0.0.0	0.0.0.0
Range 3	0.0.0.0	0.0.0.0
Range 4	0.0.0.0	0.0.0.0

✓ Apply

A Shows how many IP devices are detected and displayed in Topology view.

B Shows the Controller (Master) IP address.

C Shows the DHCP Server IP address.

D DHCP Server Enabled/Disabled.

E Shows IP Range selection; select Single Subnet or Multiple Subnets.

* Single Subnet: DMS is based on the Master switch's IP address. Here subnet means "255.255.255.0"

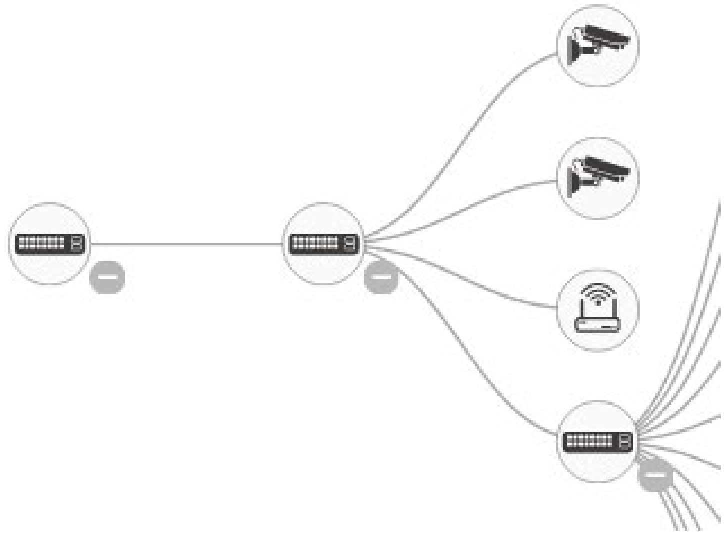
* Multiple Subnet: Provides 4 ranges for inputting manually. In this case, we suggest you adjust the switch subnet mask to "255.255.0.0" also to avoid IP devices that can't be recognized.

F IP Ranges 1-4 for Multiple Subnets selection.

⤢ **Icon with screen view type**: Click it to change to Full Screen View of Topology or return to the Normal View.

☰ **Icon with information list**: Select what kind of information should be shown on the topology view of each device. Up to three items can be selected.

Device Tree View



Device Categories

The device is a Switch.

The device is a PC.

The device is an IP Camera.

The device is an IP Phone.

The device is an Access Point.

The device is a Router.

Icon with question mark: The IP device is detected by DMS, but the device type can't be recognized, and will be classified as an “Unknown” device type.

Device Status

Icon with black mark: Device link up. User can select function and check issues.

Icon with red mark: Device link down. User can diagnose the link status.

Icon with number: An event has occurred (e.g., Device Off-line, IP Duplicate, etc.) on the IP device. Click on the device icon to check Events in Notification.

Device Consoles

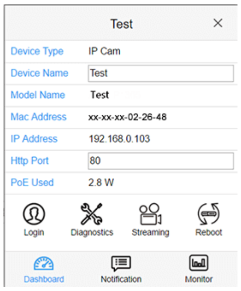
Left-click any device icon to display the device consoles for further actions.

Dashboard Console: displays device info and related actions for the device.

Different device types support different functions:

If an IP device is recognized as DMS switch, it will support "Upgrade" and "Find Switch" function.

If an IP device is recognized as PoE device, it will support more "Reboot" function in addition to "Upgrade".



Test ×

Device Type	IP Cam
Device Name	Test
Model Name	Test
Mac Address	xx-xx-xx-02-26-48
IP Address	192.168.0.103
Http Port	80
PoE Used	2.8 W

If an IP device is recognized as IP Cam via ONVIF protocol, it will support "Streaming" function.

Device Type: Can be displayed automatically. If an unknown type is detected, you can still select type from a pre-defined list. Device Types include **PC** (General PC), **IP Camera** (General IP Cam), **IP Phone** (General IP Phone, Cisco SPA303), **AP** (General AP), and **Others** (Mobile Device, General Switch, Internet Gateway, IP PBX, NAS, Printer, NVR, VMS, or Unknown Device).

Device Name: Create your own Device Name or alias for easy management, such as 1F_Lobby_Cam1.

Model Name, MAC Address, IP Address, Subnet Mask, Gateway, PoE Supply and PoE Used are displayed automatically by DMS.

HTTP Port: Re-assign HTTP port number to the device for better security.

Login **Login:** Click the Login Action Icon to log in the device via HTTP for further configuration or status monitoring.

Upgrade **Upgrade:** Click it to upgrade software version.

Find Switch **Find Switch:** When this feature is activated, the switch LED will all lighten up and flicker for 15 seconds.

Diagnostics **Diagnostics:** Click Diagnostic Action Icon to perform the cable diagnostics, to examine where the broken cable is, and check if the device connection is alive or not by ping.

- Cable Status:
    - **Green icon:** Cable is connected correctly.
    - **Red icon:** Cable is not connected correctly. User can check the distance info (XX meters) to identify the broken cable location.
- Connection:
    - **Green icon:** Device is pinged correctly.
    - **Red icon:** Device is not transmitted /receiving data correctly. Which means it might not be pinged successfully.

Reboot **Reboot:** Click Reboot Action Icon to reboot the device remotely so as recover the device back to its normal operation.

Streaming **Streaming:** Click Streaming Action Icon to display the video images streaming if the device supports this feature.

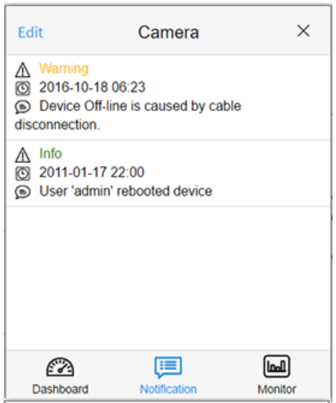
Parent Node **Parent Node:** When DMS switch detects more than two IP devices from the same port, switch can't resolve this IP device's layout, instead, it will show a blank node to present this situation. User can use "Parent Node" function to adjust layout in Dashboard.

Notification Console: Displays alarms and logs triggered by events. For example:

Warning: <date> Device Off-line is caused by cable disconnection.

Info <date> User ‘admin’ rebooted device

No Message



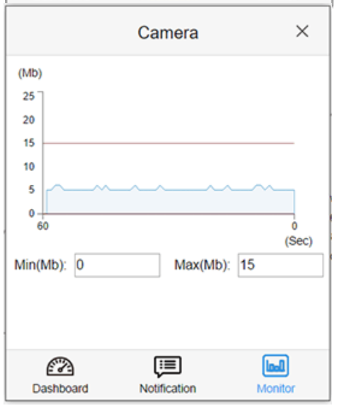
Edit Camera ✕

⚠ Warning
2016-10-18 06:23
Device Off-line is caused by cable disconnection.

⚠ Info
2011-01-17 22:00
User 'admin' rebooted device

Monitor Console: It displays the traffics for device health check purpose.

- For each IP device except DMS switches, you can set a threshold of throughput for IP devices, and get notification when throughput is lower or higher than settings.
- If both values are "0", it means the function is disabled.
- Polling interval is 1 second; when the page is closed, the Polling interval will change to around 5 seconds.

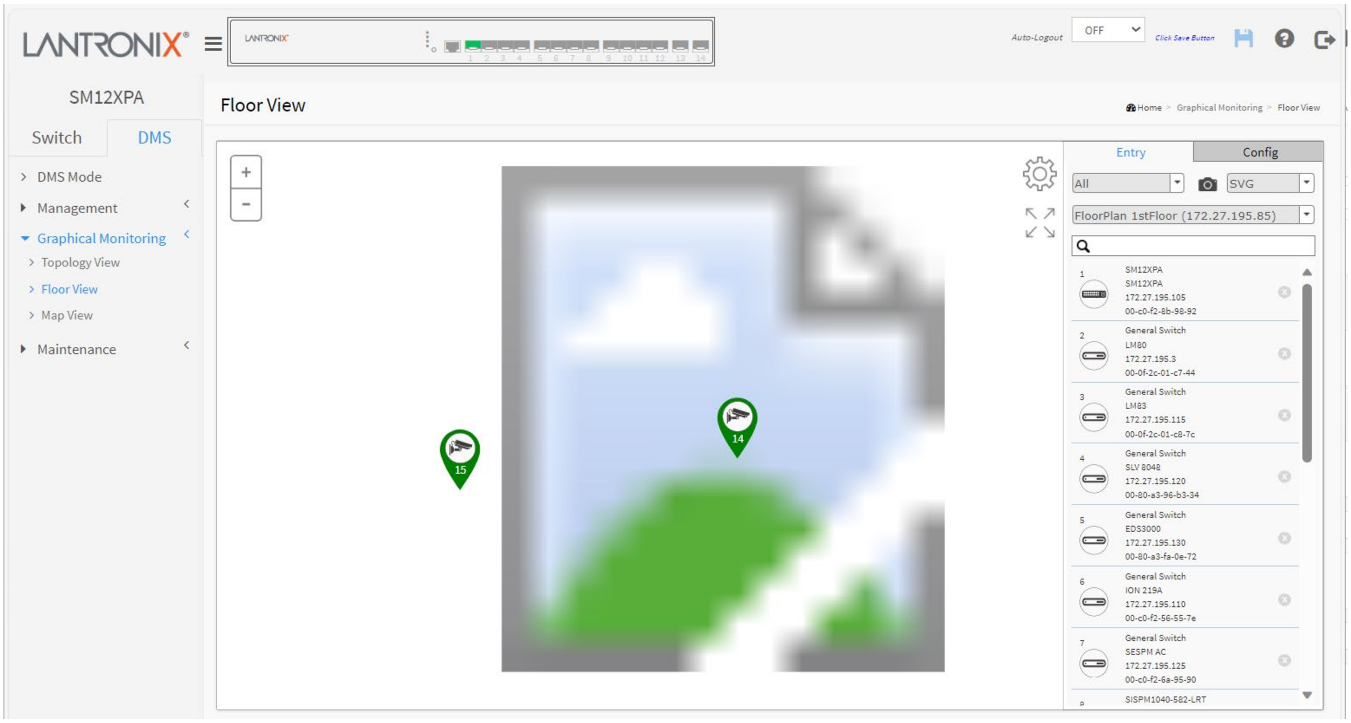


Min(Mb): 0 Max(Mb): 15

Floor View

This page displays the graphical image created at DMS > Maintenance > Floor Image. Initially, no Floor View images are displayed. Go to DMS > Maintenance > Floor Image to upload floor images.

The Floor View lets you easily plan IP devices installation locations by dragging the uploaded floor images into place.



1	SM12XPA	SM12XPA	172.27.195.105	00-c0-f2-8b-98-92
2	General Switch	LM80	172.27.195.3	00-0f-2c-01-c7-44
3	General Switch	LM83	172.27.195.115	00-0f-2c-01-c8-7c
4	General Switch	SLV 8048	172.27.195.120	00-80-a3-96-b3-34
5	General Switch	EDS3000	172.27.195.130	00-80-a3-fa-0e-72
6	General Switch	ION 219A	172.27.195.110	00-c0-f2-56-55-7e
7	General Switch	SESPM AC	172.27.195.125	00-c0-f2-6a-95-90
8	SISPM1040-582-LRT			

+ − Icon with plus and minus marks: Zoom in and zoom out the floor view, user can scroll up/down with mouse to achieve the same purpose.

⚙ There is a "Setting icon" in the upper right corner. When you click the icon, it will pop-up Device, Config, export floor view and advanced search functions for the device. You can click it again to hide the functions.

↖ ↗ ↙ ↘ Icon with screen view type: Click it to change to Full Screen view of Floor or return to the Normal View.

Device Search Console

Functions:

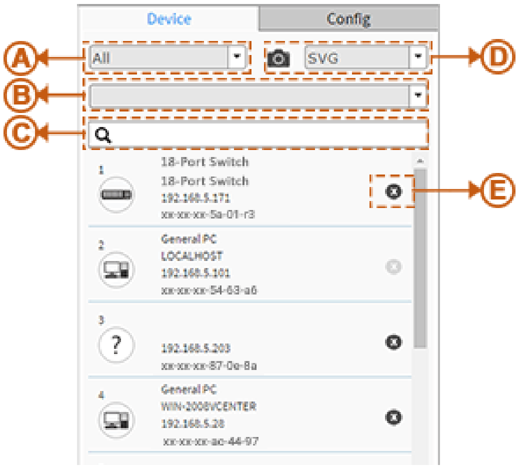
A. Filter devices by Device Type

B Select floor images

C Search devices by key words full text search

D Save the whole View to SVG, PNG or PDF

E Remove a device from all floor view images



1
18-Port Switch
18-Port Switch
192.168.5.171
xx-xx-xx-5a-01-r3

2
General PC
LOCALHOST
192.168.5.101
xx-xx-xx-54-63-a6

3
?
192.168.5.203
xx-xx-xx-87-0e-8a

4
General PC
WIN-2008VCENTER
192.168.5.28
xx-xx-xx-ac-44-97

System Setting Console

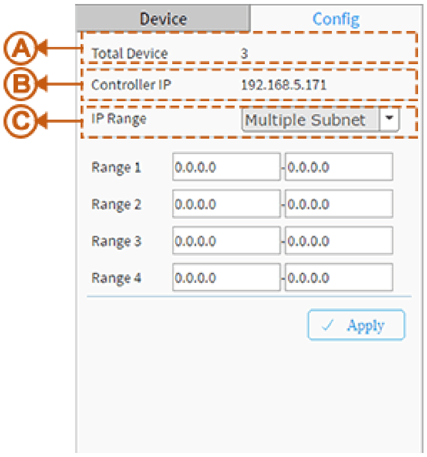
Functions:

A. Shows how many IP devices are detected and displayed in the topology view.

B. Shows the Master switch's IP address.

C. Single Subnet: DMS will base on the master switch's IP address. Here the subnet means "255.255.255.0".

Multiple Subnet: To provide 4 ranges for inputting manually. (In the case, we suggest you adjust the switch's subnet mask to "255.255.0.0" also to avoid IP devices that can't be recognized.)



Total Device 3
Controller IP 192.168.5.171
IP Range Multiple Subnet
Range 1 0.0.0.0 - 0.0.0.0
Range 2 0.0.0.0 - 0.0.0.0
Range 3 0.0.0.0 - 0.0.0.0
Range 4 0.0.0.0 - 0.0.0.0

Floor View

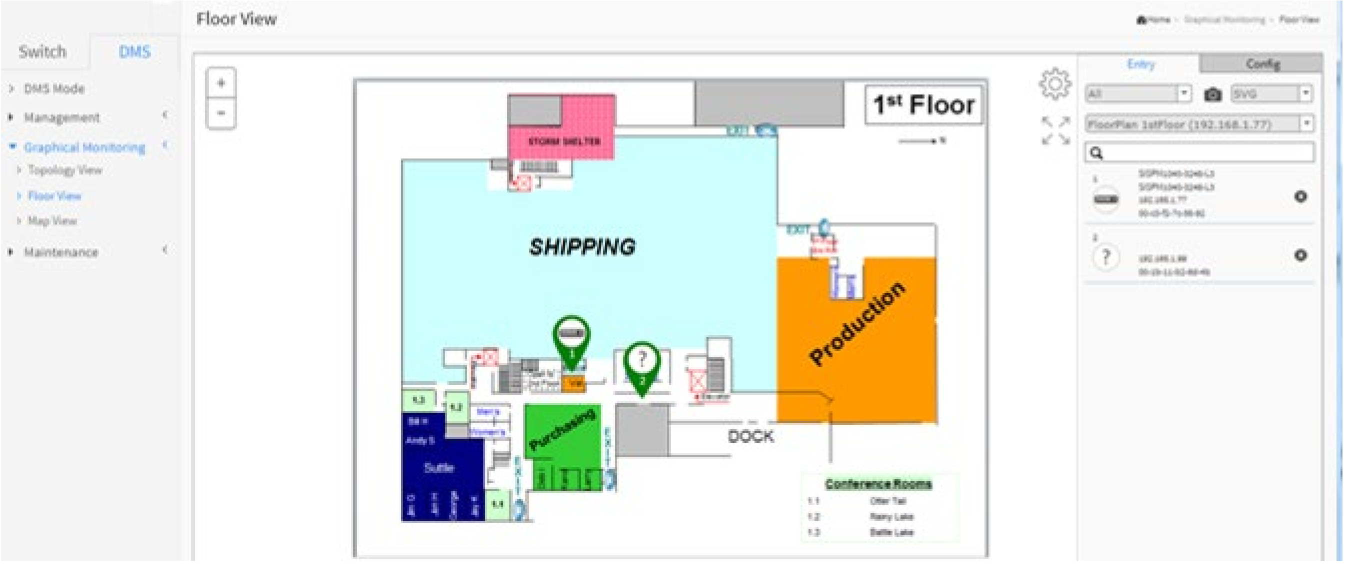
1. Anchor devices onto Floor Maps
2. Find device location instantly
3. 10 Maps can be stored per Switch
4. IP Surveillance/VoIP/WiFi applications
5. Other features same as Topology View
6. To place and remove a device icon:
   - Select a device and click its icon from the device list.
   - The device icon will show on the floor image's default location.
   - Click and hold left mouse to drag-and-drop the icon to the correct location on the Floor View.
   - Click cross sign on the right side of device icon to remove a device from all Floor View images.

Device Status

Icon with black mark: Device link up. User can select function and check issues.

Icon with red mark: Device link down. User can diagnose the link status.

Floor View Example:



All

SVG

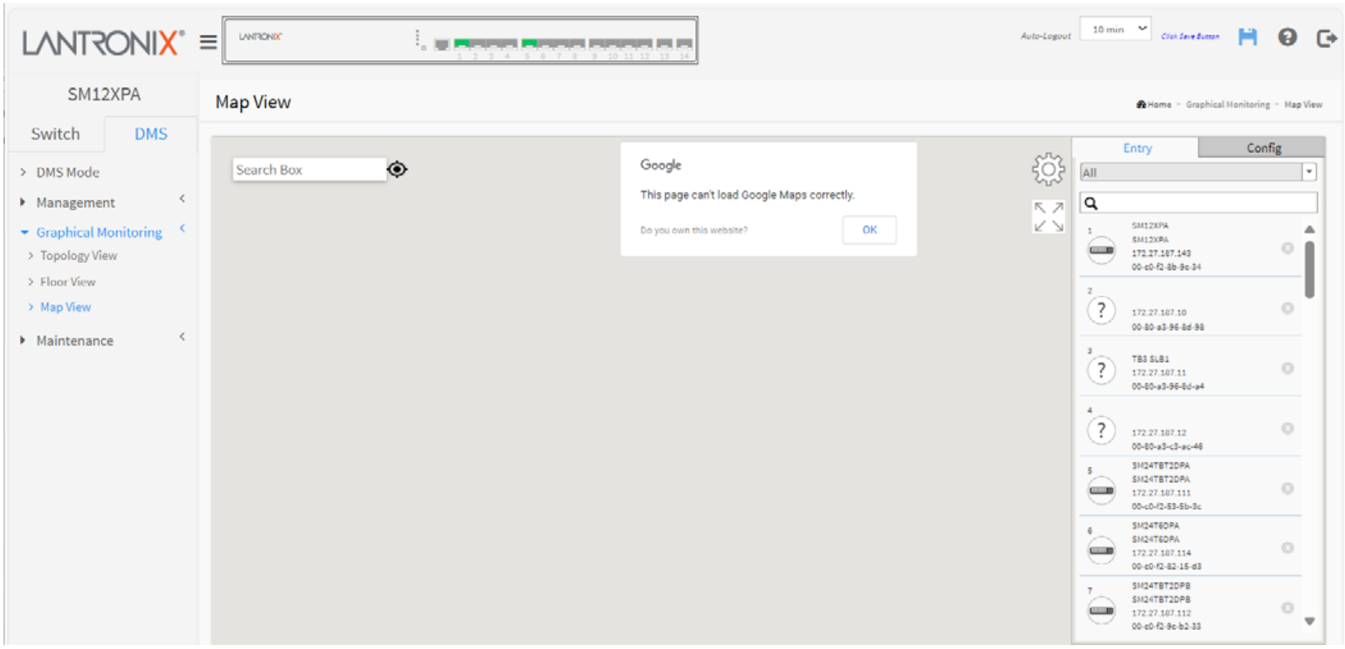
FloorPlan 1stFloor (192.168.1.77)

1
SISPM1040-3248-L3
SISPM1040-3248-L3
192.168.1.77

2
192.168.1.98

Map View

This page helps you find the location of devices even when they are installed in a different building. You can place a device icon on the Map View and navigate using Google Maps. You need a valid API key and a Google Cloud Platform billing account to access a Google core product. If not, DMS Map View will not be able to load Google Maps correctly. See *DMS > Management > Map API Key*.



Google

This page can't load Google Maps correctly.

Do you own this website? OK

1 SM12XPA SM12XPA 172.27.187.143 00-c0-f2-8b-9c-34

2 172.27.187.10 00-80-a3-96-8d-98

3 TB3 SLB1 172.27.187.11 00-80-a3-96-8d-a4

4 172.27.187.12 00-80-a3-c3-ac-46

5 SM24TBT2DPA SM24TBT2DPA 172.27.187.111 00-c0-f2-53-5b-3c

6 SM24T6DPA SM24T6DPA 172.27.187.114 00-c0-f2-82-15-d3

7 SM24TBT2DPB SM24TBT2DPB 172.27.187.112 00-c0-f2-9c-b2-33

⚙ **Settings icon** in the upper right corner. When you click the icon, it will pop-up Device, Config, export floor view and advanced search functions for the device.

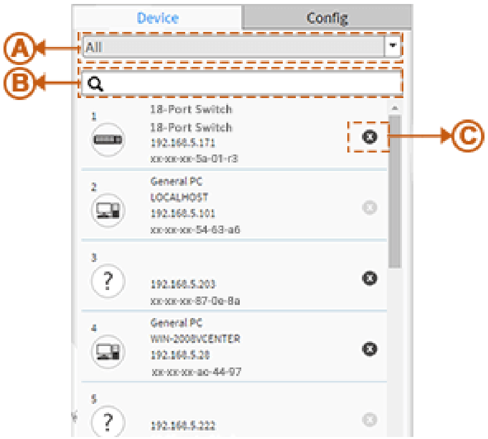
1. Device Search Console

Function:

A. Filter devices by Device Type

B. Search devices by key words full text search

C. Remove a device from Map view



1 18-Port Switch 18-Port Switch 192.168.5.171 xx-xx-xx-5a-01-r3

2 General PC LOCALHOST 192.168.5.101 xx-xx-xx-54-63-a6

3 192.168.5.203 xx-xx-xx-87-0e-8a

4 General PC WIN-2008VCENTER 192.168.5.28 xx-xx-xx-ac-44-97

5 192.168.5.222

2. System Setting Console

Function:

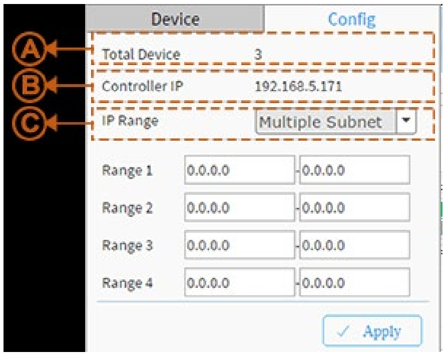
A. Shows how many IP devices are detected and displayed in the topology view.

B. Shows the Master switch IP address.

C. Single Subnet: DMS will base on the master switch's IP address.

Here the subnet means "255.255.255.0".

Multiple Subnet: To provide 4 ranges for inputting manually.(In the case, we will suggest user to adjust switch's subnet mask to "255.255.0.0" also to avoid IP devices can't be recognized.)



Total Device	3	
Controller IP	192.168.5.171	
IP Range	Multiple Subnet	
Range 1	0.0.0.0	0.0.0.0
Range 2	0.0.0.0	0.0.0.0
Range 3	0.0.0.0	0.0.0.0
Range 4	0.0.0.0	0.0.0.0

↖ ↗
↙ ↘ **Screen view type** icon: Click it to change to Full Screen View of the Map View page or return to the Normal View.

Map View

- Anchor Devices onto Google Maps.
- Find Devices Instantly from Map View.
- On-Line Search Company/Address.
- Outdoor IP Cam/WiFi Applications.
- Other Features same as Topology View
- To place and remove a device icon
    - o Select a device and click its icon from the device list.
    - o The device icon will show on the map's default location.
    - o Click and hold left mouse to drag-and-drop the icon to the correct location on the Map View.
    - o Click the cross sign on the right side of device icon to remove a device from Map View.

Device Status

Icon with black mark: **Device link up**. You can select functions and check issues.

Icon with red mark: **Device link down**. You can diagnose the link status.

Message: *“This page can't load Google Maps correctly.”*

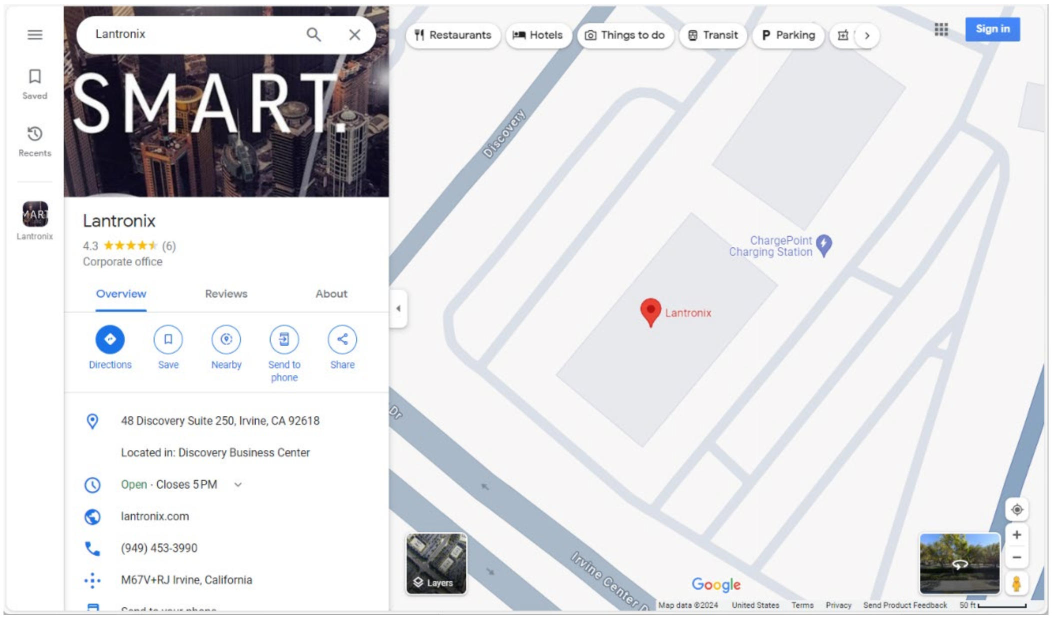
Recovery: See DMS > Management > Map API Key on page 420.

Message: *“Do you own this website?”*

Recovery: 1. Click the linked text to display the Google Maps Troubleshooting webpage.

2. Go to the Google Maps Platform Support and Resources webpage.

Map View Example:



Lantronix

4.3 ★★★★★ (6)

Corporate office

48 Discovery Suite 250, Irvine, CA 92618

Located in: Discovery Business Center

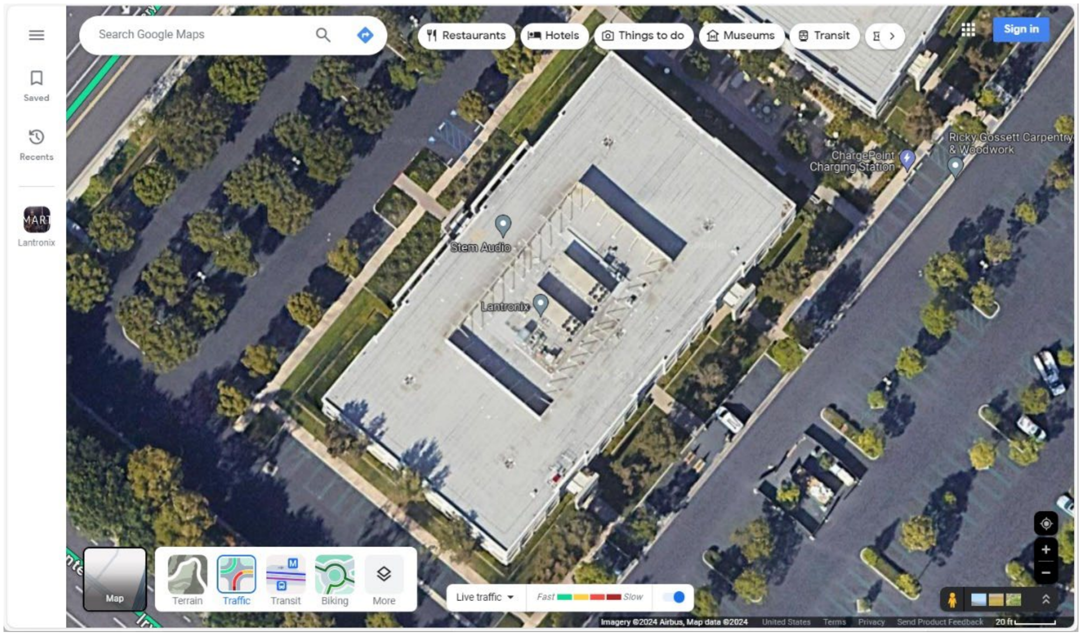
Open · Closes 5 PM

lantronix.com

(949) 453-3990

M67V+RJ Irvine, California

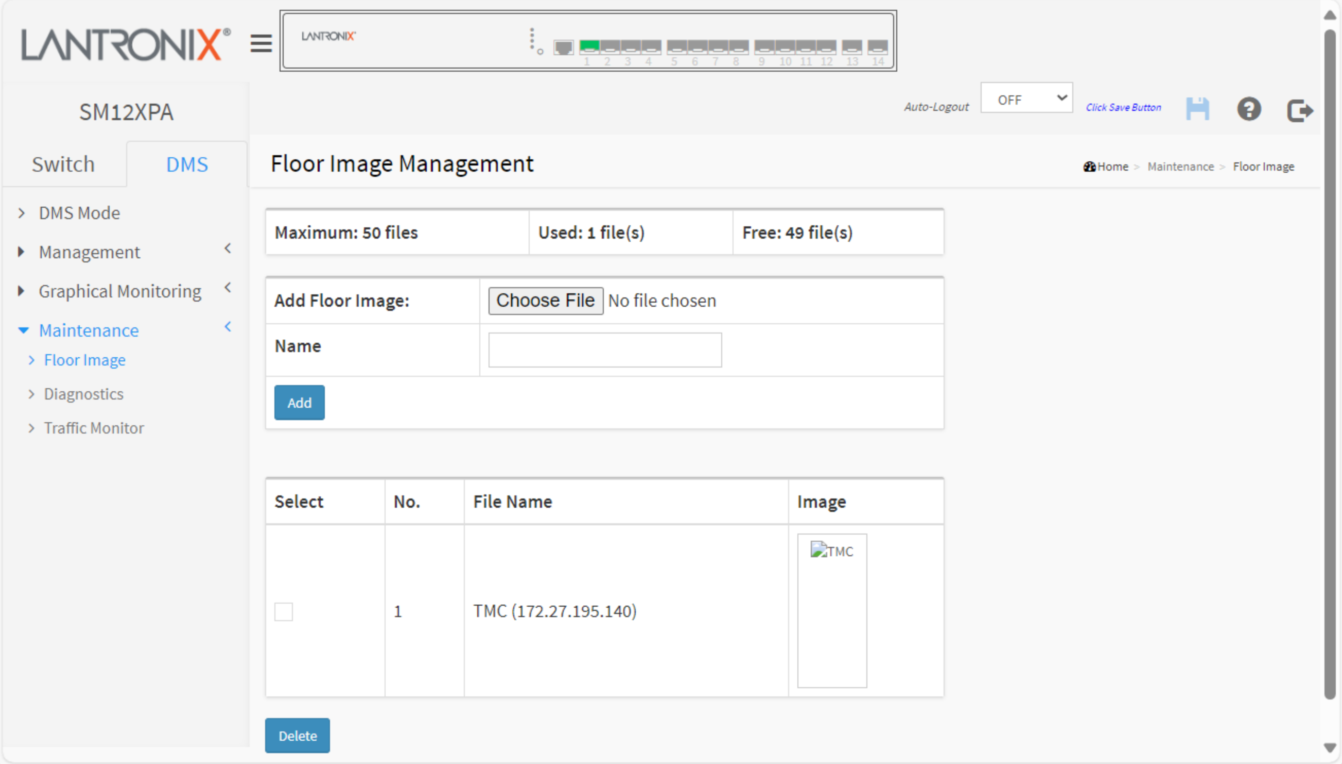
Map View Example - Satellite View:



DMS Maintenance

Floor Image

This page lets you upload and manage floor map images. You can upload up to 20 JPEG or PNG images, each a maximum of 256KB in size.



Floor Image Management

Maximum: 50 files	Used: 1 file(s)	Free: 49 file(s)

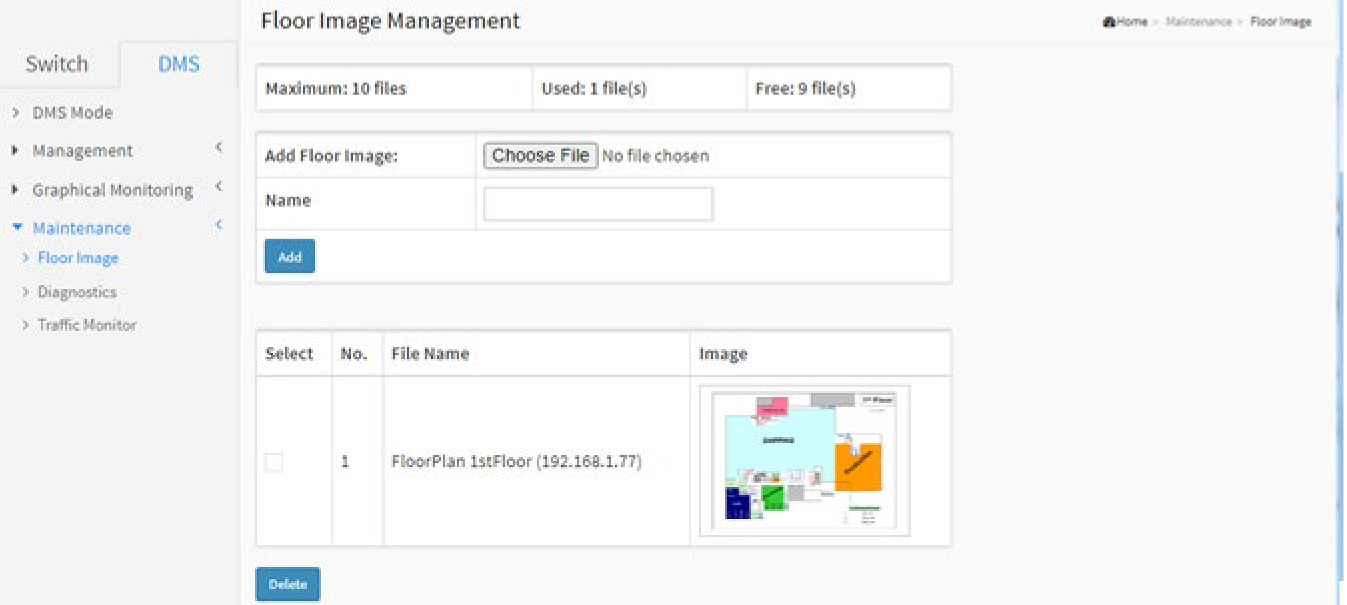
Add Floor Image:	Choose File No file chosen
Name	

Add

Select	No.	File Name	Image
□	1	TMC (172.27.195.140)	TMC

Delete

1. At the default Floor Image Management page click the **Choose File** icon.
2. Select a JPEG or PNG image.
3. Enter a Name and click the **Add** button to display the selected image:



Floor Image Management

Maximum: 10 files	Used: 1 file(s)	Free: 9 file(s)

Add Floor Image:	Choose File No file chosen
Name	

Add

Select	No.	File Name	Image
□	1	FloorPlan 1stFloor (192.168.1.77)	

Delete

Select : Check the checkbox to select an image from the list.

No.: Floor Image instance number (maximum 10 image files).

File Name : Displays the file name information (e.g., *Floor Plan - 1st Floor (192.168.1.77)*).

Image: Displays a thumbnail of the floor image.

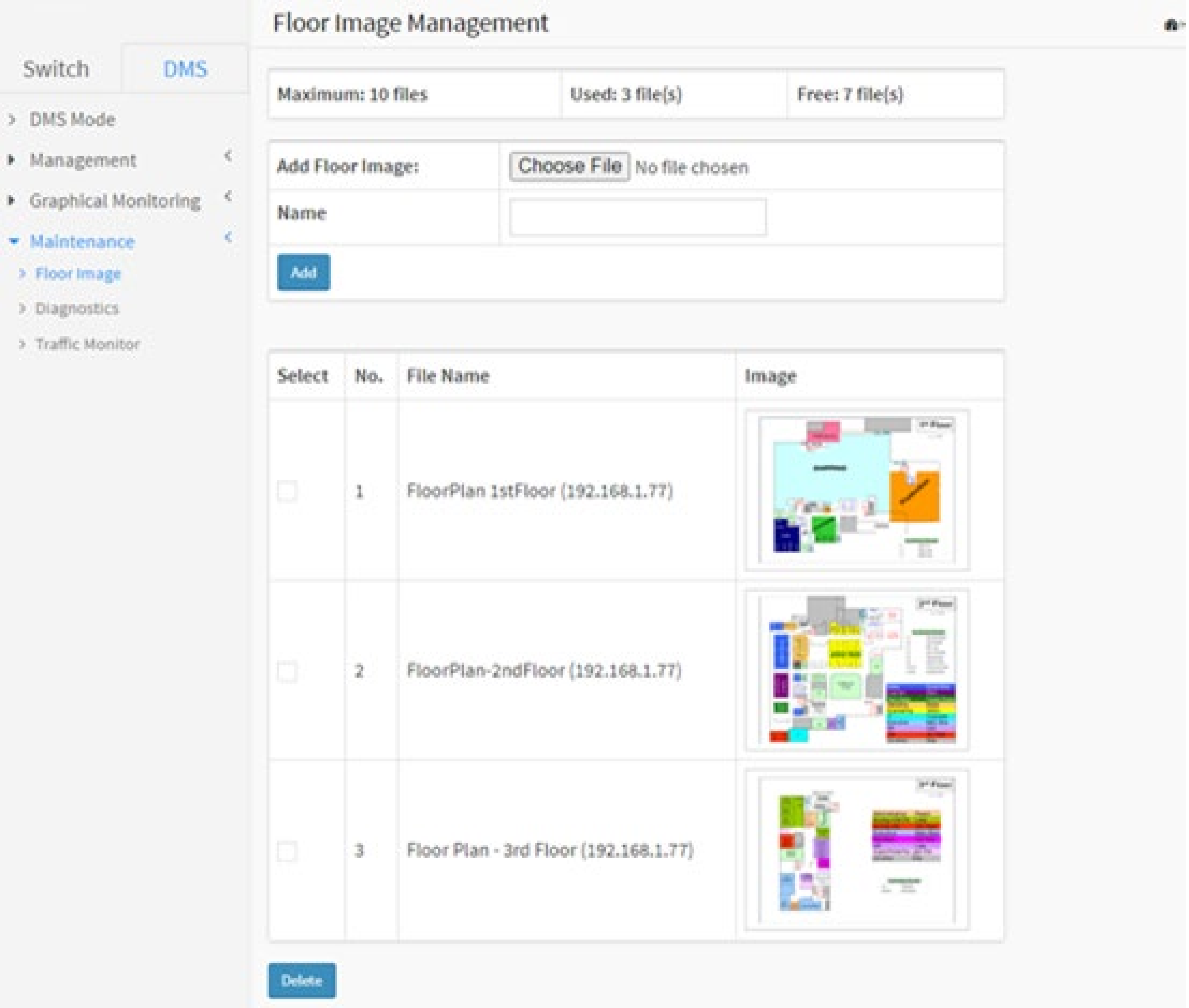
Buttons

Add: Click Add to upload. When done, a snapshot will be available on screen.

Delete: If you need to remove an existing floor map, select its checkbox and click Delete to remove.

Messages: *"Only jpg, png are allowed"* displays if you selected a file type other than JPG or PNG. Click OK to clear the message and select a PNG or JPG file.

Example:



Floor Image Management

Maximum: 10 files	Used: 3 file(s)	Free: 7 file(s)

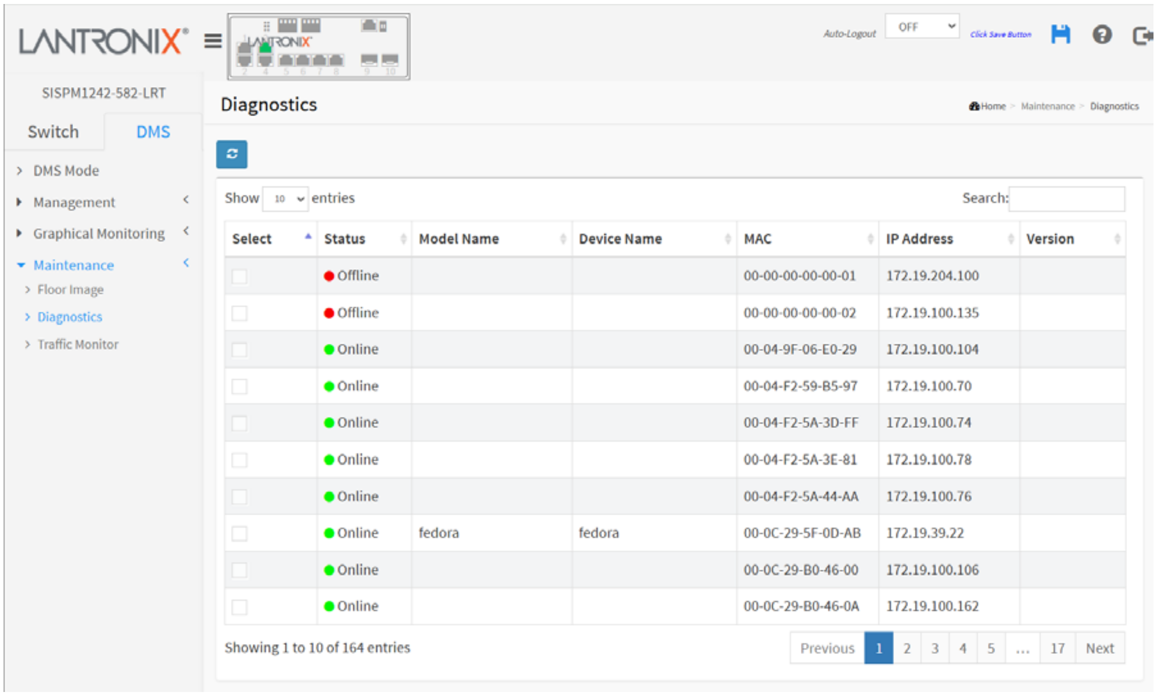
Add Floor Image:	Choose File No file chosen
Name	

Select	No.	File Name	Image
□	1	FloorPlan 1stFloor (192.168.1.77)	
□	2	FloorPlan-2ndFloor (192.168.1.77)	
□	3	Floor Plan - 3rd Floor (192.168.1.77)	

Diagnostics

This page lets you run a diagnostic test on a selected device.

1. Go to DMS > Diagnostics. The Diagnostics page displays.



Diagnostics

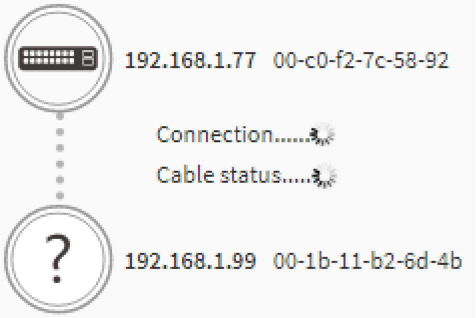
Show 10 entries Search:

Select	Status	Model Name	Device Name	MAC	IP Address	Version
□	● Offline			00-00-00-00-00-01	172.19.204.100	
□	● Offline			00-00-00-00-00-02	172.19.100.135	
□	● Online			00-04-9F-06-E0-29	172.19.100.104	
□	● Online			00-04-F2-59-B5-97	172.19.100.70	
□	● Online			00-04-F2-5A-3D-FF	172.19.100.74	
□	● Online			00-04-F2-5A-3E-81	172.19.100.78	
□	● Online			00-04-F2-5A-44-AA	172.19.100.76	
□	● Online	fedora	fedora	00-0C-29-5F-0D-AB	172.19.39.22	
□	● Online			00-0C-29-B0-46-00	172.19.100.106	
□	● Online			00-0C-29-B0-46-0A	172.19.100.162	

Showing 1 to 10 of 164 entries

Previous 1 2 3 4 5 … 17 Next

2. Select an online or offline device from the list. The diagnostic test starts. The status updates as the diagnostic is run.

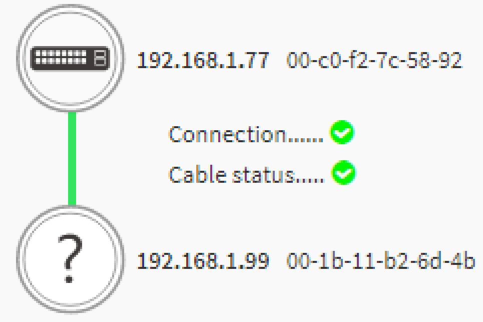


192.168.1.77 00-c0-f2-7c-58-92

Connection......

Cable status.....

192.168.1.99 00-1b-11-b2-6d-4b



192.168.1.77 00-c0-f2-7c-58-92

Connection...... ✓

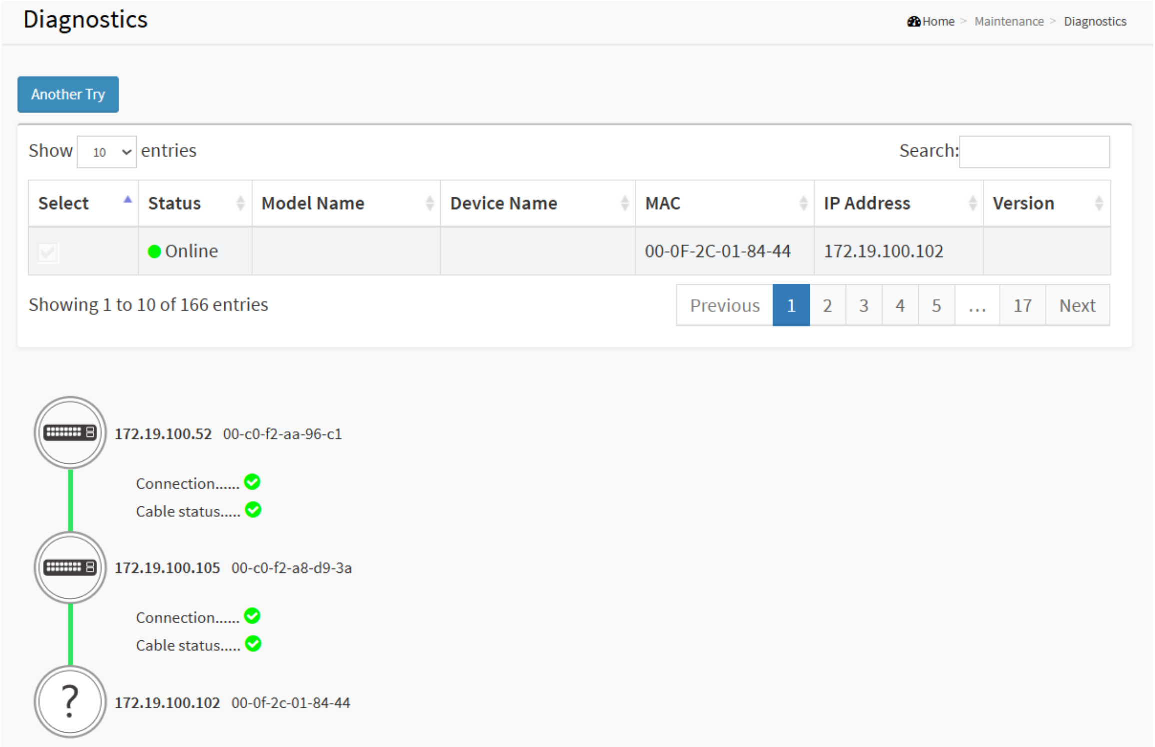
Cable status..... ✓

192.168.1.99 00-1b-11-b2-6d-4b

Diagnostic In process

Diagnostic Completed

3. The completed test may look as follows:



Diagnostics

Home > Maintenance > Diagnostics
Another Try

Show 10 entries Search:

Select	Status	Model Name	Device Name	MAC	IP Address	Version
☑	● Online			00-0F-2C-01-84-44	172.19.100.102	

Showing 1 to 10 of 166 entries

Previous 1 2 3 4 5 … 17 Next

172.19.100.52 00-c0-f2-aa-96-c1

Connection...... ✓
Cable status..... ✓

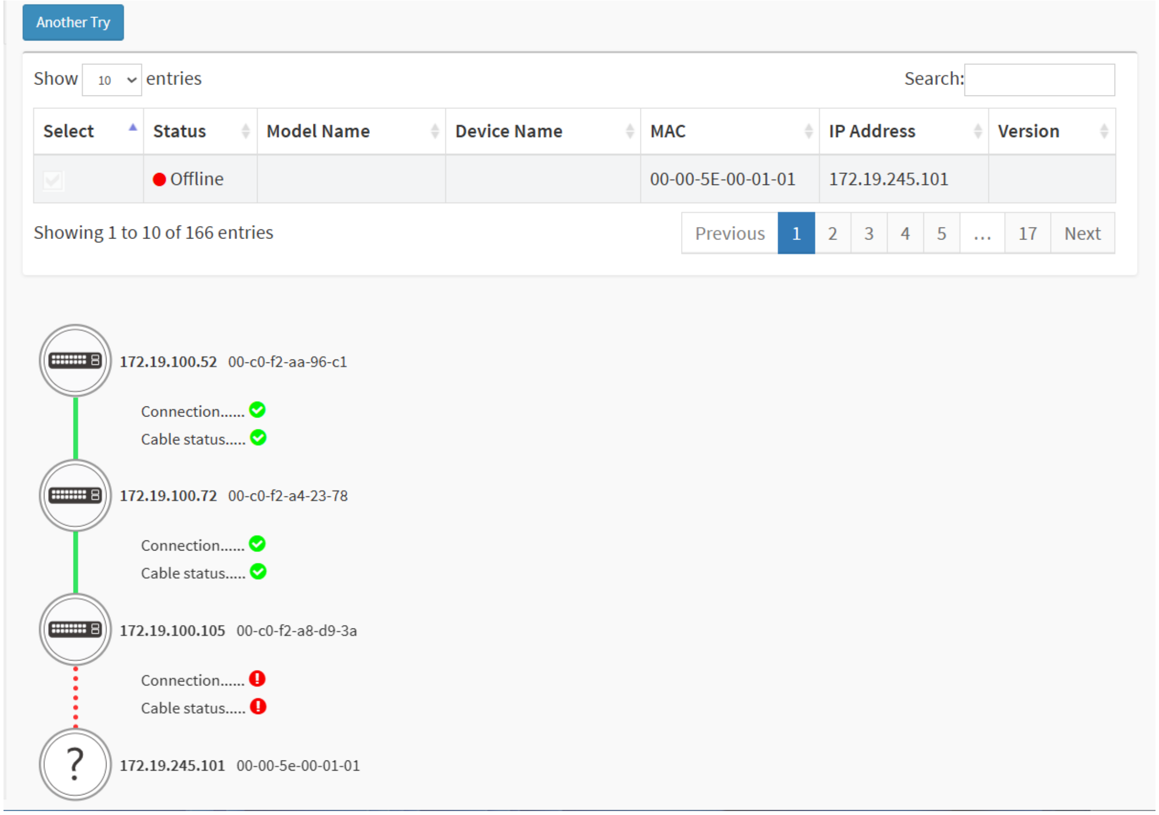
172.19.100.105 00-c0-f2-a8-d9-3a

Connection...... ✓
Cable status..... ✓

? 172.19.100.102 00-0f-2c-01-84-44

4. When a diagnostic test completes, click the **Another Try** button to clear the page and start anew.

Example diagnostics for an offline device:



Show 10 entries Search:

Select	Status	Model Name	Device Name	MAC	IP Address	Version
☑	● Offline			00-00-5E-00-01-01	172.19.245.101	

Showing 1 to 10 of 166 entries

172.19.100.52 00-c0-f2-aa-96-c1

Connection...... ✓
Cable status..... ✓

172.19.100.72 00-c0-f2-a4-23-78

Connection...... ✓
Cable status..... ✓

172.19.100.105 00-c0-f2-a8-d9-3a

Connection...... !
Cable status..... !

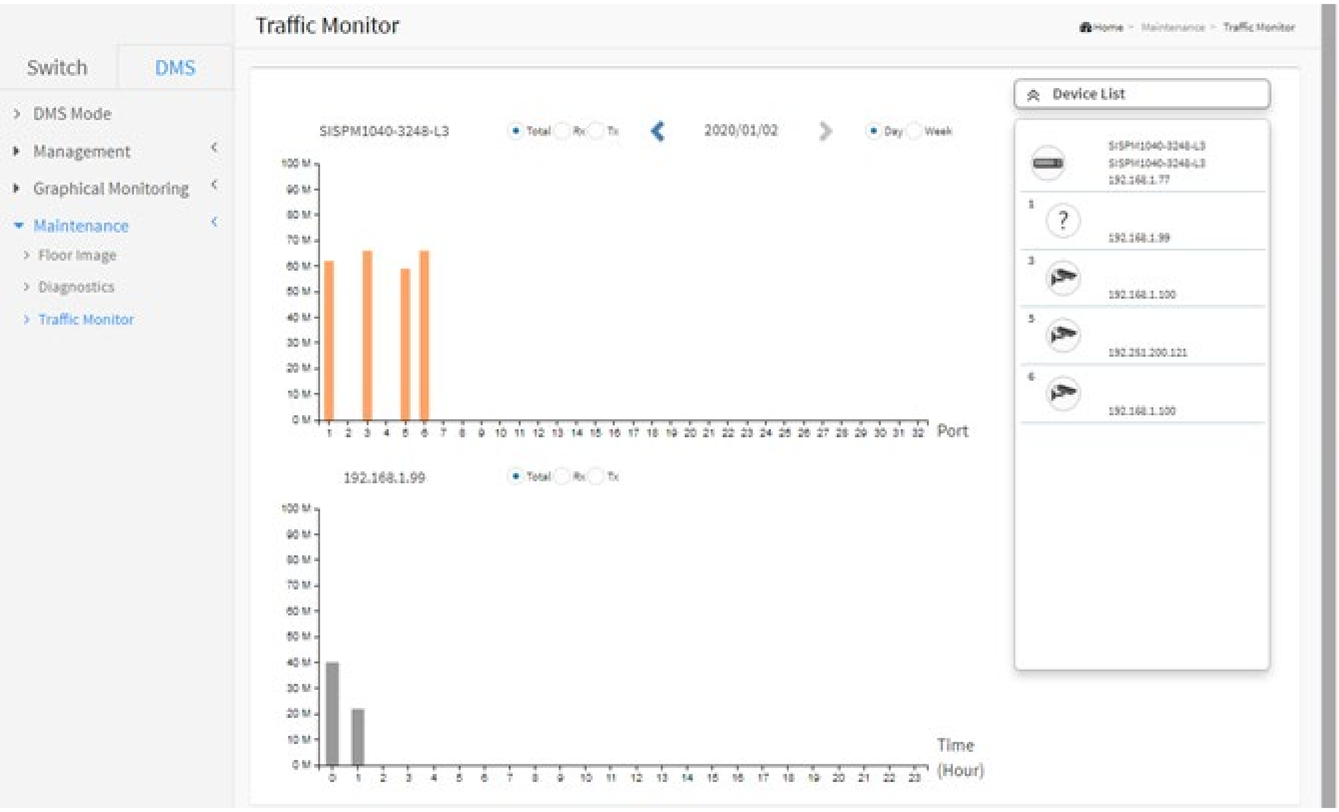
? 172.19.245.101 00-00-5e-00-01-01

Traffic Monitor

This page displays a visual chart of network traffic of all the devices. Numbers are shown in Mbit/s.

To view the traffic of all the ports or just a specific port; click on a specific port on the traffic chart to reveal its traffic during the day.

You can select to display a summary of a day's or a week's traffic by selecting the check circle on top. The same applies to the selection of Rx Tx traffic. A single port's traffic is shown at the lower half of the screen.



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.

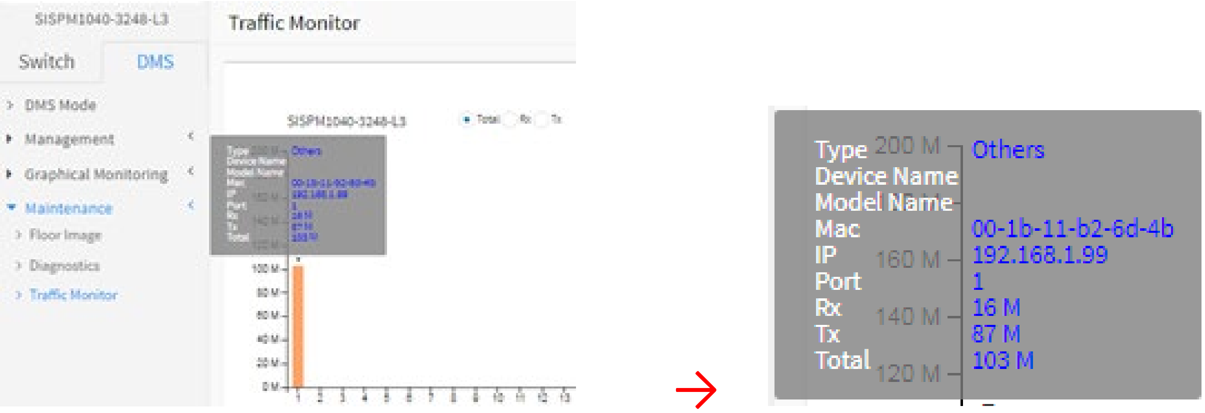
Device List: Displays the set of discovered devices.

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).

Hover the mouse cursor over a column in the table to display its specific parameters:



Type Others
Device Name
Model Name
Mac 00-1b-11-b2-6d-4b
IP 192.168.1.99
Port 1
Rx 16 M
Tx 87 M
Total 103 M

Message: “*Traffic Monitor feature is only available on master switch.*”

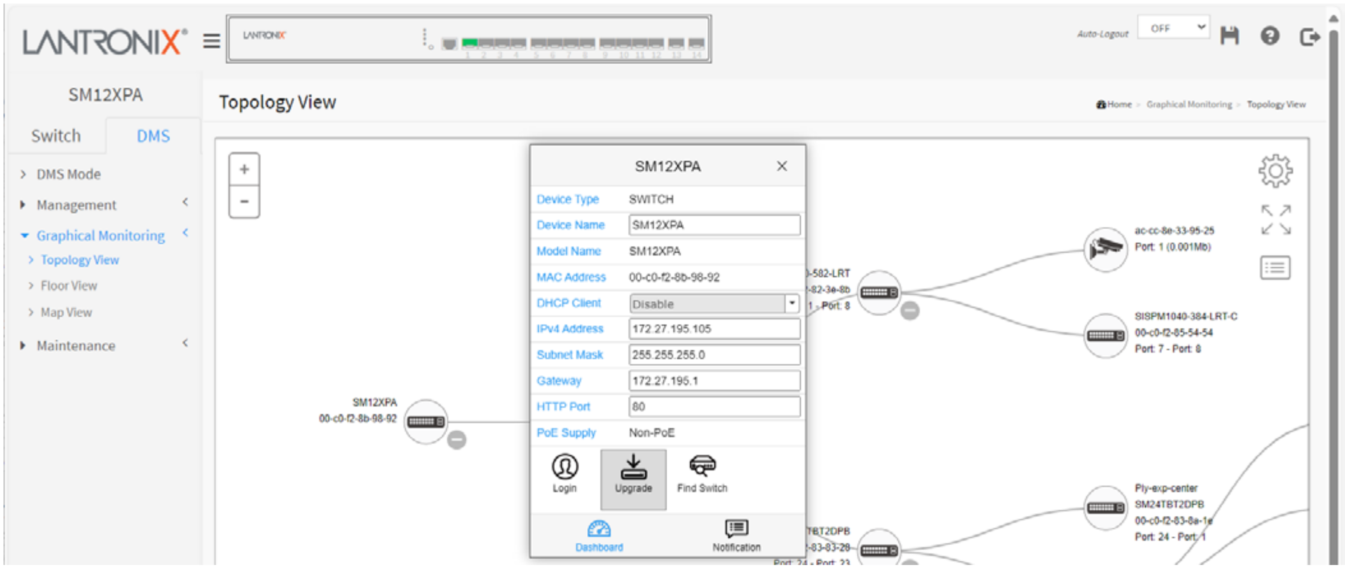
Meaning: You clicked on “Traffic Monitor” at DMS > Traffic Monitor, but this switch is not the DMS Controller (Master) Switch.

Recovery: Either make this switch the DMS Controller (Master) Switch or use the designated DMS Controller (Master) Switch for traffic monitoring.

DMS Firmware Upgrade

To upgrade a device's firmware via DMS:

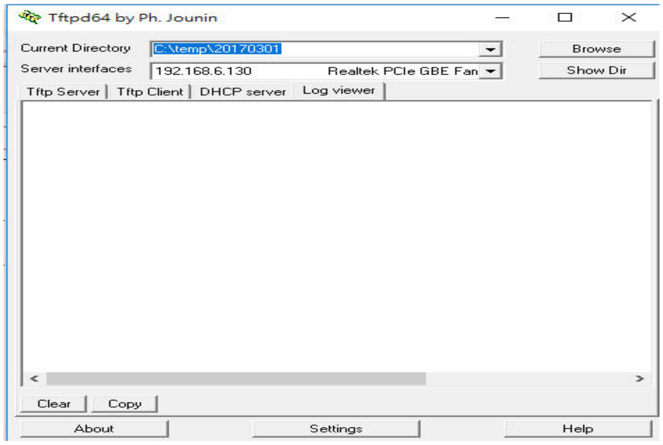
1. Go to the DMS > Graphical Monitoring > Topology View menu path.
2. Click the ⚙ button to display the right pane menu tabs (Device, Group, and Config).
3. Connect all switches and make sure DMS is working.
   - Set all switches with different IP addresses and in the same IP segment.
   - Make sure gateway IP address is configured.
4. Left-click the desired device icon to display the options:



SM12XPA

Device Type	SWITCH
Device Name	SM12XPA
Model Name	SM12XPA
MAC Address	00-c0-f2-8b-98-92
DHCP Client	Disable
IPv4 Address	172.27.195.105
Subnet Mask	255.255.255.0
Gateway	172.27.195.1
HTTP Port	80
PoE Supply	Non-PoE

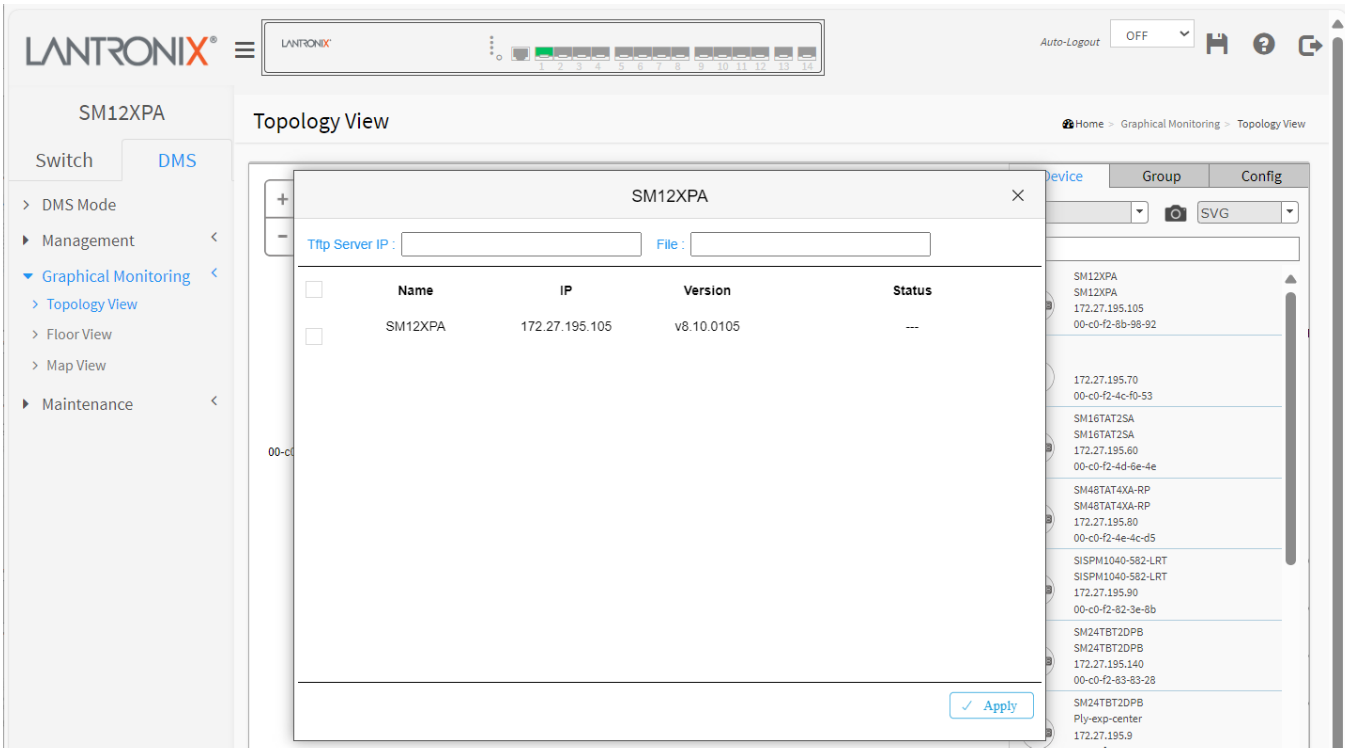
5. Enable the TFTP server and set the correct image path.



Current Directory: C:\temp\20170301

Server interfaces: 192.168.6.130 Realtek PCIe GBE Fan

6. Click the switch icon, and then click the **Upgrade** button in the Dashboard.
7. Enter the TFTP server IP address and FW file name and select the switch on which you want to upgrade the FW.



SM12XPA

Tftp Server IP :

File :

	Name	IP	Version	Status
□	SM12XPA	172.27.195.105	v8.10.0105	---
□				

SM12XPA
SM12XPA
172.27.195.105
00-c0-f2-8b-98-92

172.27.195.70
00-c0-f2-4c-f0-53

SM16TAT2SA
SM16TAT2SA
172.27.195.60
00-c0-f2-4d-6e-4e

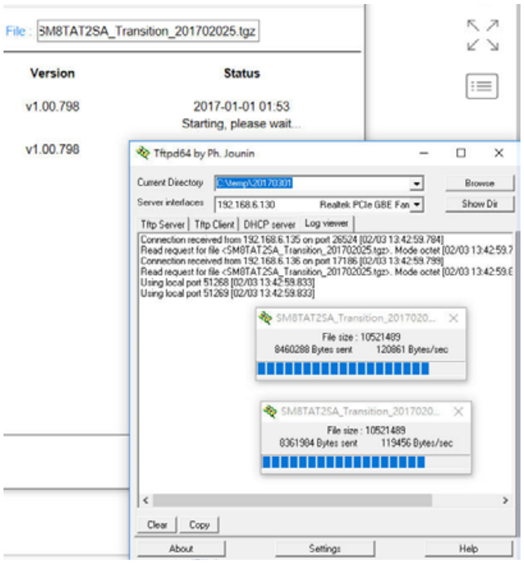
SM48TAT4XA-RP
SM48TAT4XA-RP
172.27.195.80
00-c0-f2-4e-4c-d5

SISPM1040-582-LRT
SISPM1040-582-LRT
172.27.195.90
00-c0-f2-82-3e-8b

SM24TBT2DPB
SM24TBT2DPB
172.27.195.140
00-c0-f2-83-83-28

SM24TBT2DPB
Ply-exp-center
172.27.195.9

8. Click **Apply** to start the FW upgrade and save to Running-config.
9. Observe the upgrade status until completion.



File : SM8TAT2SA_Transition_201702025.tgz

Version	Status
v1.00.798	2017-01-01 01:53 Starting, please wait...
v1.00.798	

Current Directory C:\temp\20170301

Server interfaces 192.168.6.130 Realtek PCIe GBE Fan

```
Connection received from 192.168.6.135 on port 26524 [02/03 13:42:59.784]
Read request for file <SM8TAT2SA_Transition_201702025.tgz>. Mode octet [02/03 13:42:59.7
Connection received from 192.168.6.136 on port 17186 [02/03 13:42:59.799]
Read request for file <SM8TAT2SA_Transition_201702025.tgz>. Mode octet [02/03 13:42:59.8
Using local port 51268 [02/03 13:42:59.833]
Using local port 51269 [02/03 13:42:59.833]
```

SM8TAT2SA_Transition_2017020...
File size : 10521489
8460288 Bytes sent 120861 Bytes/sec

SM8TAT2SA_Transition_2017020...
File size : 10521489
8361984 Bytes sent 119456 Bytes/sec

Messages

Starting, please wait…

Error : *Firmware download fail*

DMS Troubleshooting

Problem: The switch lists itself as the only device in Topology View of DMS.

Problem: In DMS, the Local image shows the IP address of another switch.

Description: The switch is listed as only device in DMS Topology View in DMS; all devices are listed in DMS device list. This is usually because the switch's gateway is not configured appropriately.

Resolution: An IP Route must be configured manually. For example, a switch IP address of 192.168.1.77 should have the following IP route configured: ip route 0.0.0.0 0.0.0.0 192.168.1.x. Without the IP route configured, you may be unable to view all devices on the network in DMS.

1. Go to DMS > Management > DMS Mode to check if the controller IP is correct.

2. Verify that the gateway of this switch is correctly configured.

3. Verify that all connected devices are displayed in DMS Topology View.

Problem: DMS Connectivity diagnostics fails to ICMP reachable device.

Description: DMS displays a device which is reachable via ICMP ping as failing the connection status in diagnostics. Cable status displays as *OK*.

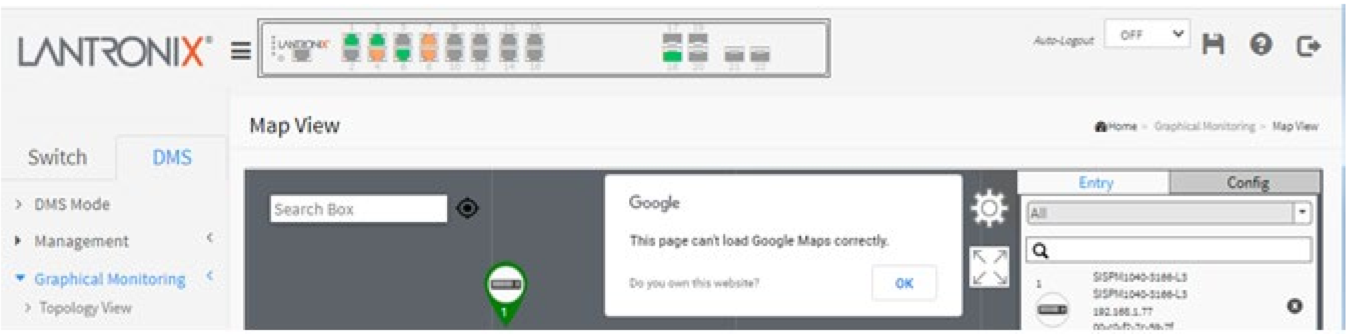
Resolution: Contact Technical Support. See Contact Us below.

Problem: DMS will discover the device type, name and model of some cameras and hosts but others are displayed as *Unknown*.

Description: When a device is detected by DMS, the device’s information (such as type, model name…etc.) can be recognized via LLDP (e.g., Switch), UPnP (e.g., AP), ONVIF (e.g. IP cam), NBNS (e.g. PC) packets if the device supports these protocols. So if the device display as *Unknown*, that means this device do not issue above mentioned protocol for DMS to recognize.

Resolution: You can manually assign and configure the device type and name for the unknown devices. See the Topology View > Dashboard or the Topology View section.

Message: *This page can’t load Google Maps correctly.* See DMS > Graphical Monitoring > Map View.



Google

This page can't load Google Maps correctly.

Do you own this website?

OK

Appendix A. DHCP Per Port and DHCP per VLAN

You can configure DHCP Per Port via the CLI and Web UI as described below. The DHCP Per Port factory default mode is Disabled. See the *CLI Reference* for CLI mode operation.

Configure DHCP Per Port via the Web UI

The switch's DHCP server assigns IP addresses. Clients get IP addresses in sequence and the switch assigns IP addresses on a per-port basis starting from the configured IP range. For example, if the IP address range is configured as 192.168.10.20 - 192.168.10.37 with one DHCP device connected to port 1, the client will always get IP address 192.168.10.20, then port 3 is always distributed IP address 192.168.10.22, even if port 2 is an empty port (because port 2 is always distributed IP address 192.168.10.21).

The switch does not allow a DHCP per Port pool to include the switch's address.

IP address assigned range and VLAN 1 should stay in the same subnet mask.

The configurable IP address range is allowed to configure over 18 IP addresses, but the switch always assigns one IP address per port connecting device.

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**.

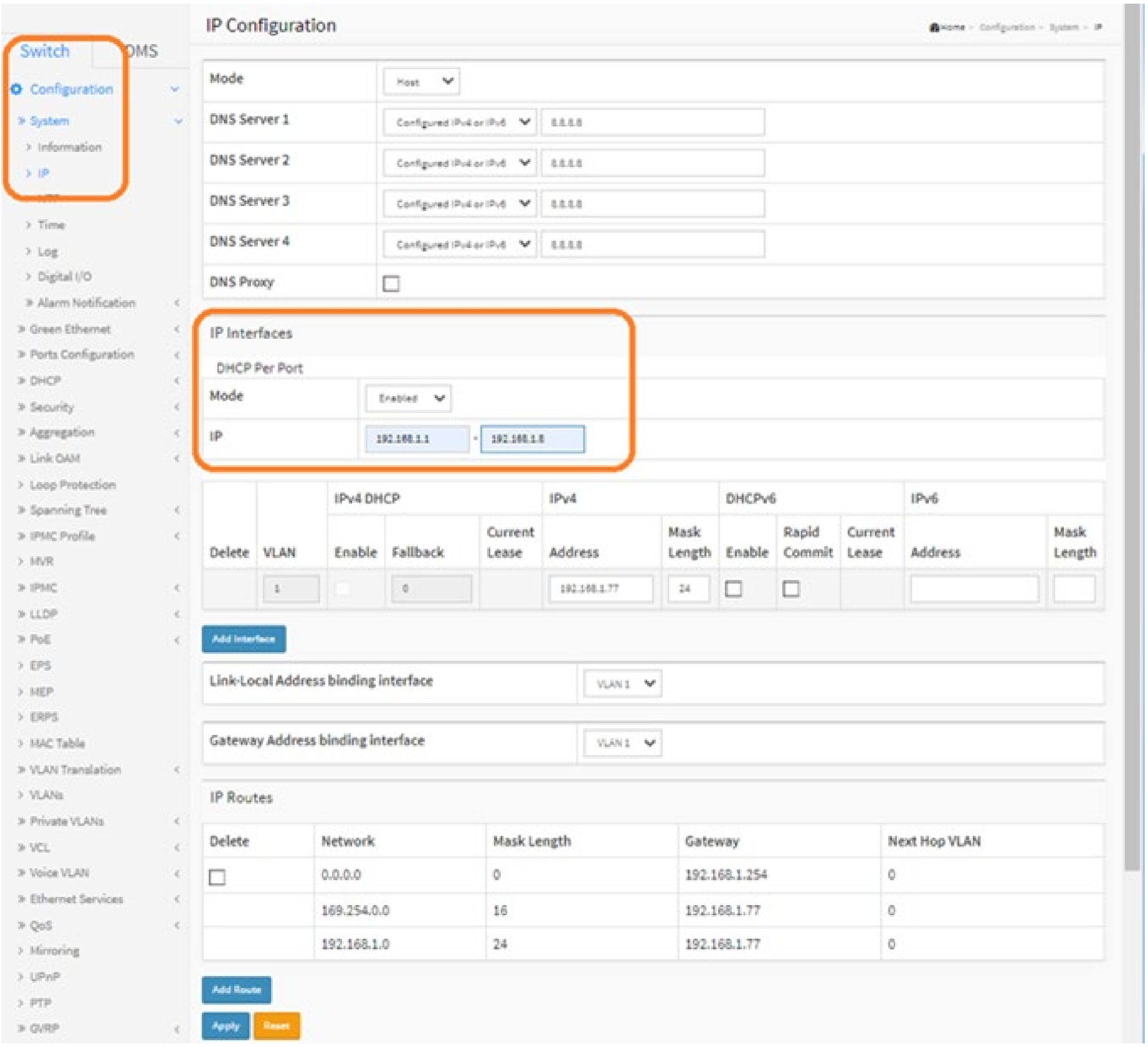
The DHCP Per Port pages and parameters are described below.

DHCP Per Port Mode Configuration

The DHCP Per Port function lets you assign an IP address based on the switch port the device is connected to. This will speed up installation of IP cameras, as the cameras can be configured after they are on the network. The DHCP Per Port assignment lets you know which IP was assigned to which camera.

Note: to prevent IP conflict, each switch can be allocated a different IP range.

To configure DHCP Per Port in the web UI, navigate to the **Configuration** > **System** > **IP** menu path.



IP Configuration

Mode	Host	
DNS Server 1	Configured IPv4 or IPv6	8.8.8.8
DNS Server 2	Configured IPv4 or IPv6	8.8.8.8
DNS Server 3	Configured IPv4 or IPv6	8.8.8.8
DNS Server 4	Configured IPv4 or IPv6	8.8.8.8
DNS Proxy	□	

IP Interfaces

DHCP Per Port

Mode	Enabled
IP	192.168.1.1 - 192.168.1.8

		IPv4 DHCP			IPv4		DHCPv6			IPv6	
Delete	VLAN	Enable	Fallback	Current Lease	Address	Mask Length	Enable	Rapid Commit	Current Lease	Address	Mask Length
	1	□	0		192.168.1.77	24	□	□			

Link-Local Address binding interface	VLAN 1

Gateway Address binding interface	VLAN 1

IP Routes

Delete	Network	Mask Length	Gateway	Next Hop VLAN
□	0.0.0.0	0	192.168.1.254	0
	169.254.0.0	16	192.168.1.77	0
	192.168.1.0	24	192.168.1.77	0

Parameter descriptions: The DHCP Per Port parameters and buttons are described below.

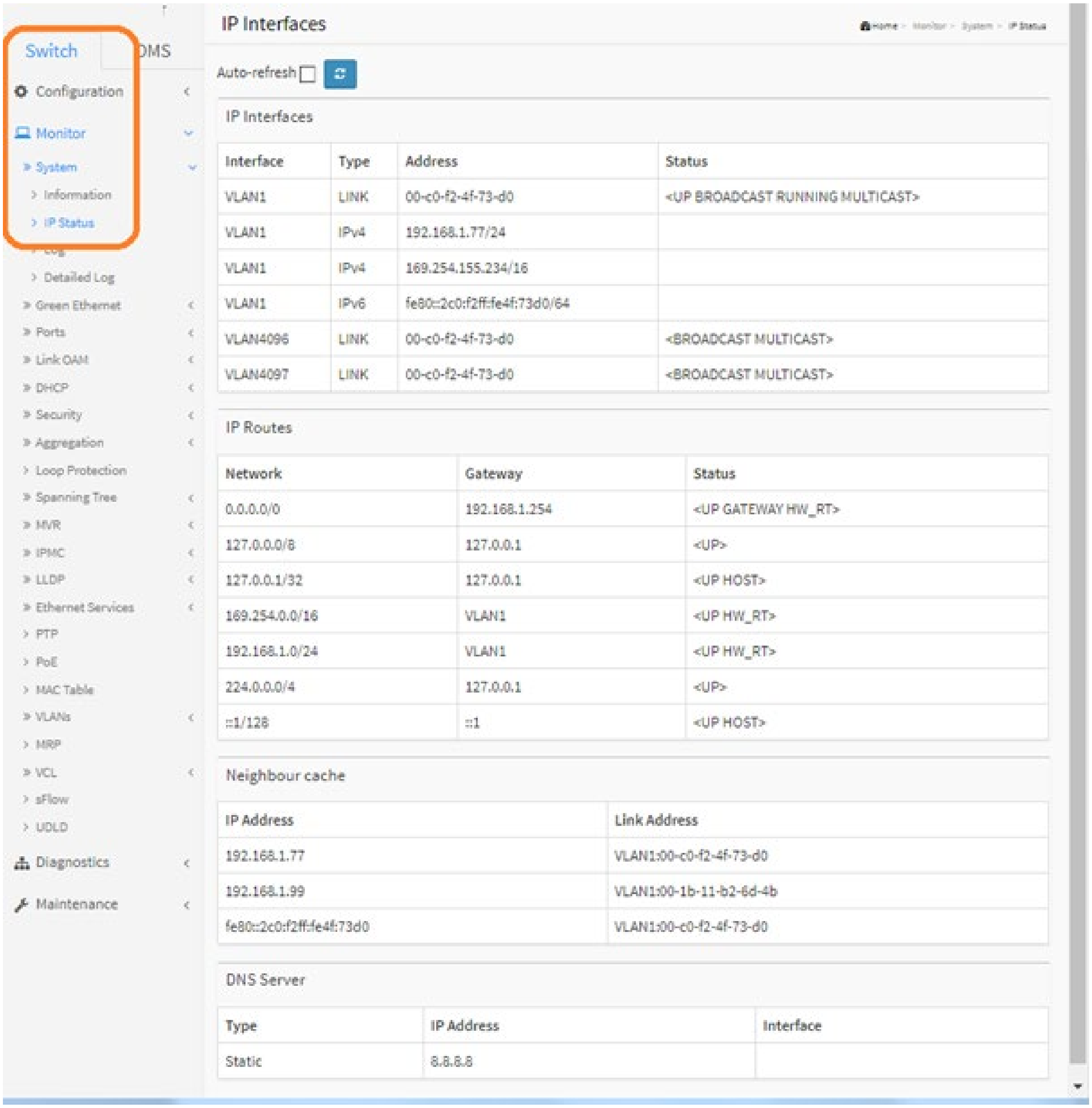
DHCP Per Port Mode: at the dropdown select **Enable** or **Disable** the DHCP Per Port function globally. The default is **Disabled**.

IP: enter the IPv4 IP address range to be used when the DHCP Per Port function is enabled (e.g., 192.168.10.20 - 192.168.10.37). The DHCP Per Port IP range must be within the interface subnet. Note that DHCP Per Port with IPv6 is not supported currently. The DHCP Per Port IP range must equal the switch port number excluding uplink ports (16).

Apply: Click to save changes to the entries. If the entries are valid, the webpage message "*Update success!*" displays. Click the **OK** button to clear the message. If any entries are invalid, an error message displays. Click the **OK** button to clear the message and enter valid values, then click the **Apply** button again.

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

To monitor DHCP Per Port status, navigate to the **Monitor** > **System** > **IP Status** menu path.



IP Interfaces

IP Interfaces

Interface	Type	Address	Status
VLAN1	LINK	00-c0-f2-4f-73-d0	<UP BROADCAST RUNNING MULTICAST>
VLAN1	IPv4	192.168.1.77/24	
VLAN1	IPv4	169.254.155.234/16	
VLAN1	IPv6	fe80::2c0:f2ff:fe4f:73d0/64	
VLAN4096	LINK	00-c0-f2-4f-73-d0	<BROADCAST MULTICAST>
VLAN4097	LINK	00-c0-f2-4f-73-d0	<BROADCAST MULTICAST>

IP Routes

Network	Gateway	Status
0.0.0.0/0	192.168.1.254	<UP GATEWAY HW_RT>
127.0.0.0/8	127.0.0.1	<UP>
127.0.0.1/32	127.0.0.1	<UP HOST>
169.254.0.0/16	VLAN1	<UP HW_RT>
192.168.1.0/24	VLAN1	<UP HW_RT>
224.0.0.0/4	127.0.0.1	<UP>
::1/128	::1	<UP HOST>

Neighbour cache

IP Address	Link Address
192.168.1.77	VLAN1:00-c0-f2-4f-73-d0
192.168.1.99	VLAN1:00-1b-11-b2-6d-4b
fe80::2c0:f2ff:fe4f:73d0	VLAN1:00-c0-f2-4f-73-d0

DNS Server

Type	IP Address	Interface
Static	8.8.8.8	

Web UI Messages

Message: Interface xx not using DHCP

Meaning: The Interface being configured does not have DHCP enabled and configured.

Recovery: **1**. Click the **OK** button to clear the webpage message. **2**. Enable and configure DHCP for the interface being configured. See DHCP Server Configuration on page 218.

Message: *'DHCP Per Port IP range (192-168-1.80 - 192-168-1.99*) is not equal to switch port number excluding uplink ports (10)

Meaning: The IPv4 IP address range entered for the DHCP Per Port function was invalid.

Recovery: **1**. Click the **OK** button to clear the webpage message. **2**. Re-configure DHCP Per Port. See the DHCP Per Port Mode Configuration section above.

Message: 'DHCP Per Port IP range (192-168-1.70 - 192-168-1.85) includes interface IP Address (192.168.1.77)

Meaning: The IPv4 IP address range entered for the DHCP Per Port function was invalid.

Recovery: **1**. Click the **OK** button to clear the webpage message. **2**. Re-configure DHCP Per Port.
See the DHCP Per Port Mode Configuration section above. On the screen below, the range should be something like 192-168-1.80 - 192-168-1.85 to be valid.

Message: The value of 'DNS Server' must be a valid IP address in dotted decimal notation ('x.y.z.w').

Meaning: You entered an invalid IP address for the DNS Server being configured.

Recovery: **1**. Click the **OK** button to clear the webpage message. **2**. Enter a valid IP address in the format x.y.z.w per the on-screen restrictions. See DHCP Server Configuration on page 218.

Message: 'DHCP Interface VLAN ID' must be an integer value between 1 and 4095.

Meaning: You entered an invalid VLAN ID for the DHCP Interface.

Recovery: **1**. Click the **OK** button to clear the webpage message. **2**. Enter a valid VLAN ID for the DHCP Interface (1-4095). See DHCP Server Configuration on page 218.

Message: DHCP per Port range (192.168.1.50 - 192.168.1.66) is not equal to switch TP port number (8).

Message: Update success!

Appendix B. MRP Pre-Requisites and Application Examples

You can configure Media Redundancy Protocol (MRP) parameters in the web UI at Configuration > MRP and monitor them at Monitor > MRP, or via the CLI. See the *CLI Reference* for Command Line operation.

According to ANSI, IEC 62439-2 Ed. 1.0 b:2010 is applicable to high-availability automation networks based on ISO/IEC 8802-3 / IEEE 802.3 Ethernet technology. It specifies a recovery protocol based on a ring topology, designed to react deterministically on a single failure of an inter-switch link or switch in the network, under the control of a dedicated Media Redundancy Manager (MRM) node.

Media Redundancy Protocol per IEC 62439-2 is an interoperable ring technology designed to allow a switch to connect onto a universal redundant high speed ring. MRP is self-healing and self-adjusting, requiring no operator interaction. MRP is based on the concept of standby connections for seamless redundancy.

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 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).

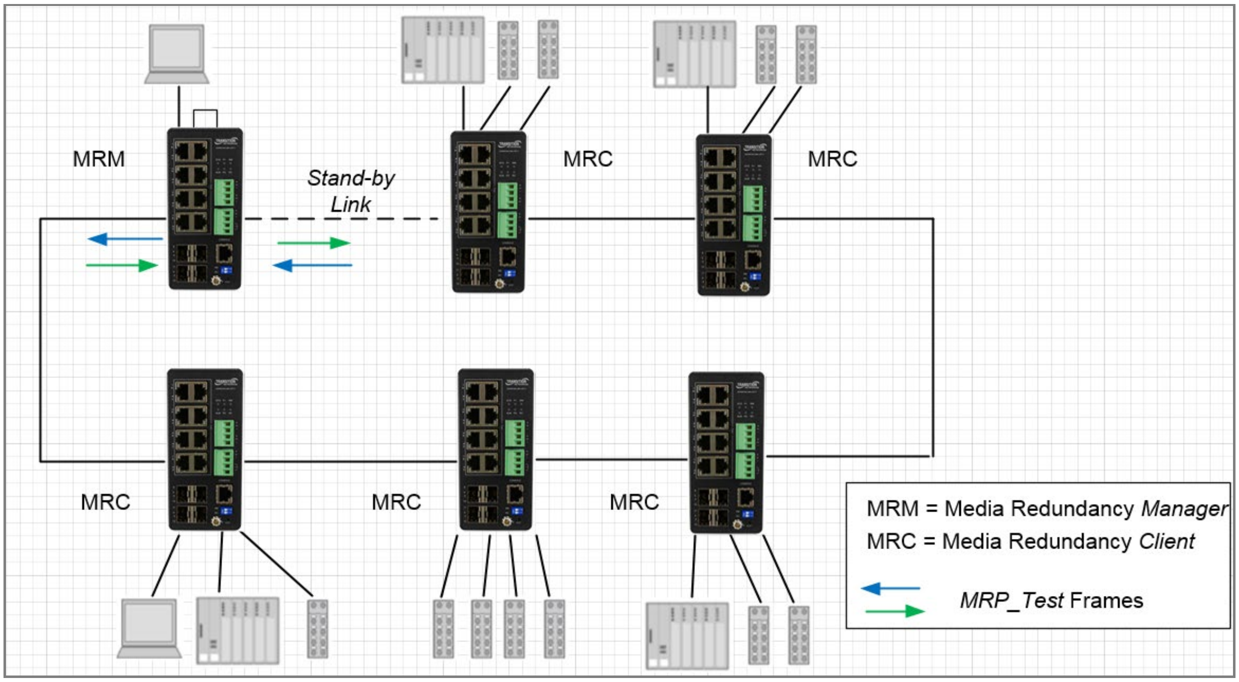

MRM
Stand-by
Link
MRC
MRC
MRC
MRC
MRC
MRM = Media Redundancy *Manager*
MRC = Media Redundancy *Client*
MRP_Test Frames

Figure: MRP Sample Setup

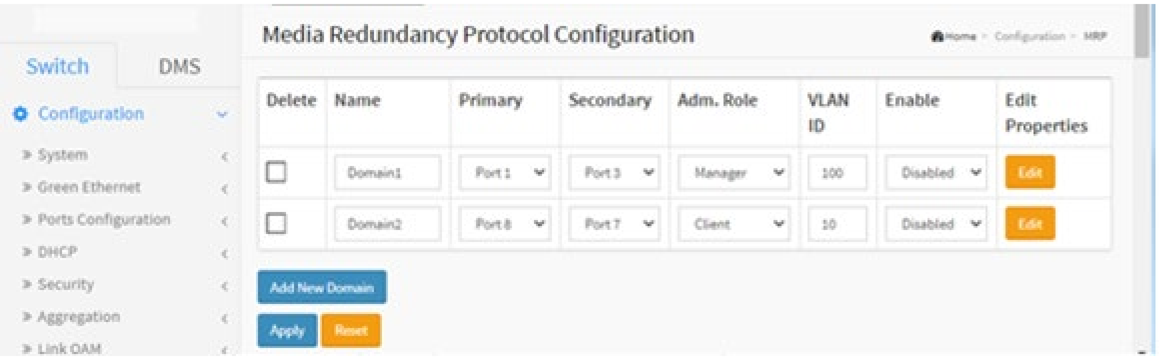
MRP Pre-Requisites (General)

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 also be disabled (G.8031 EPS, G.8032 ERPS, Rapid-Ring, Ring-To-Ring, etc.).
3. Only one MRM (Manager) is supported per ring.
4. Other pre-requisites may apply to the specific examples below.
5. One Manager Admin Role is supported.

MRP Web UI Configuration

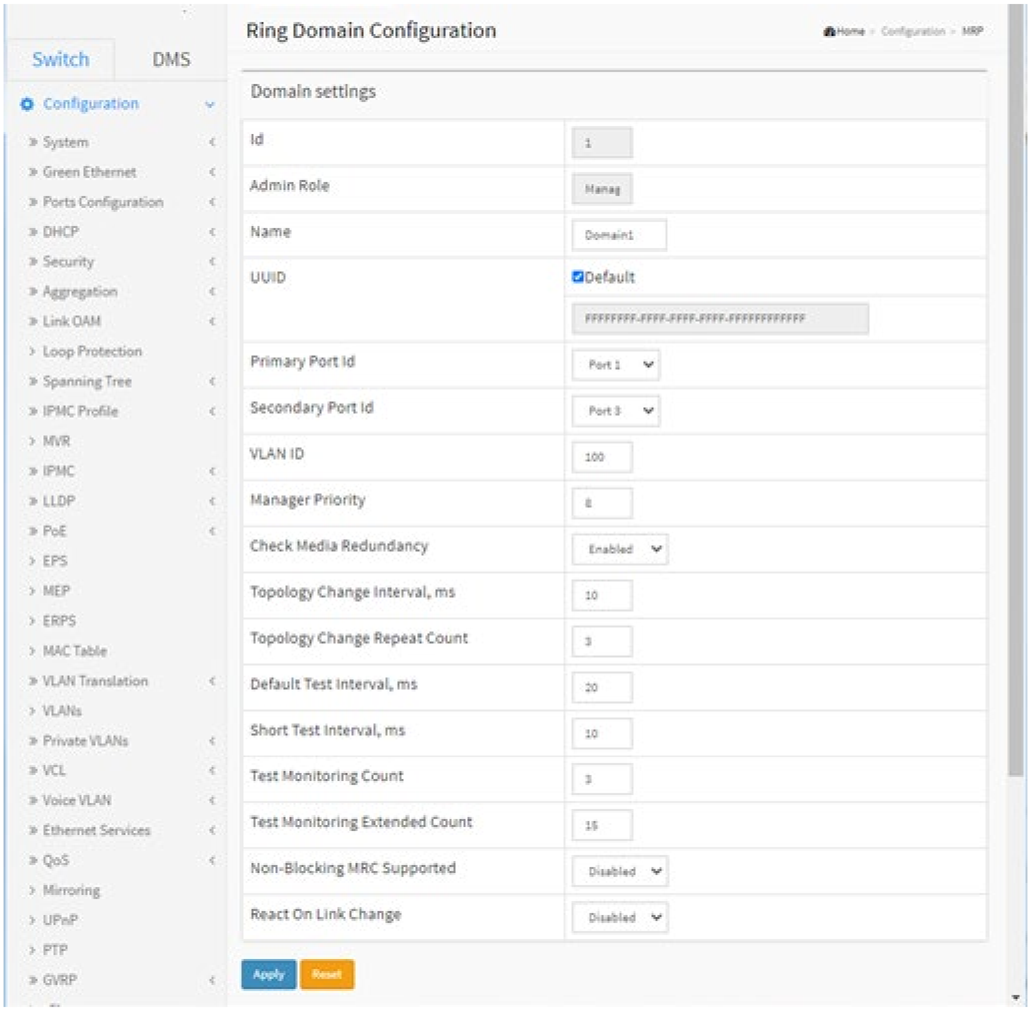
1. Go to Switch > MRP to initially configure two MRP Domains:



Media Redundancy Protocol Configuration

Delete	Name	Primary	Secondary	Adm. Role	VLAN ID	Enable	Edit Properties
□	Domain1	Port 1	Port 3	Manager	100	Disabled	Edit
□	Domain2	Port 8	Port 7	Client	10	Disabled	Edit

2. Click **Apply** to save, and then click the **Edit** button to configure the first MRP Domain (Domian1).



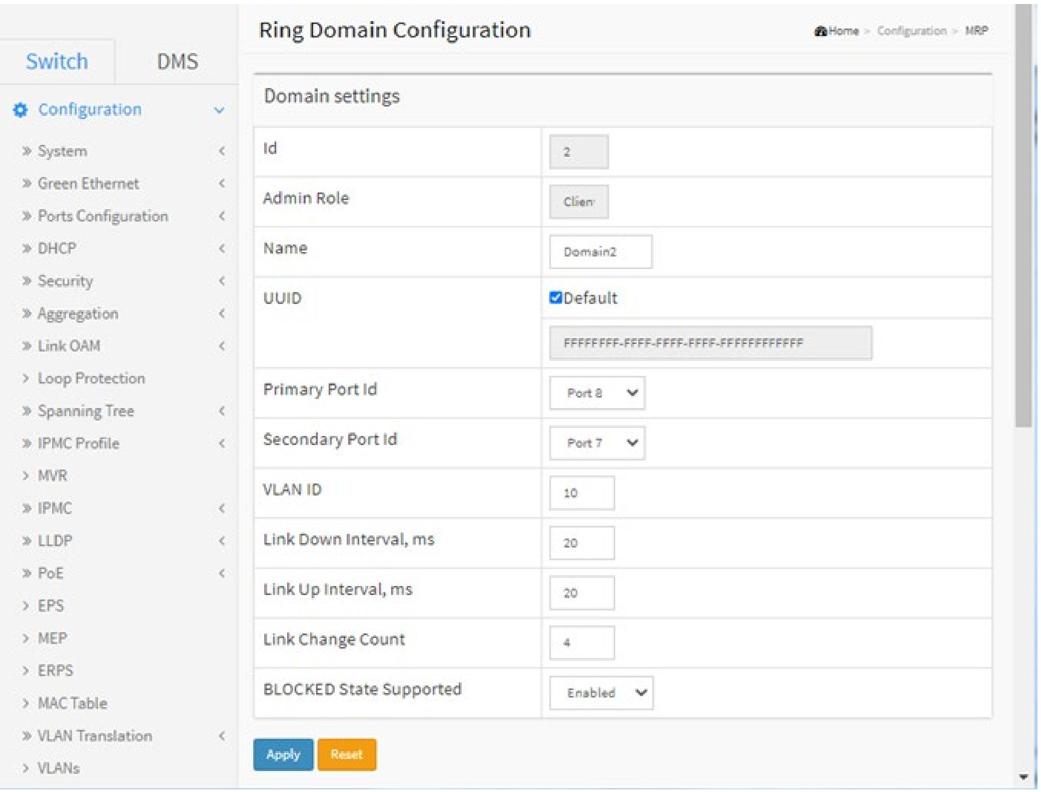
Ring Domain Configuration

Domain settings

Id	1
Admin Role	Manag
Name	Domain1
UUID	☑ Default FFFFFFFF-FFFF-FFFF-FFFF-FFFFFFFFFFFF
Primary Port Id	Port 1
Secondary Port Id	Port 3
VLAN ID	100
Manager Priority	8
Check Media Redundancy	Enabled
Topology Change Interval, ms	10
Topology Change Repeat Count	3
Default Test Interval, ms	20
Short Test Interval, ms	10
Test Monitoring Count	3
Test Monitoring Extended Count	15
Non-Blocking MRC Supported	Disabled
React On Link Change	Disabled

3. Edit the Domain Settings as required. Click **Apply** to save; the message "*Domain is enabled*" displays. Click OK to clear the webpage message. The "Media Redundancy Protocol Configuration" page displays again.

4. Click the **Edit** button to display the second MRP Domain (Domain2).



Ring Domain Configuration

Domain settings

Id	2
Admin Role	Clien
Name	Domain2
UUID	☑Default FFFFFFFF-FFFF-FFFF-FFFF-FFFFFFFFFFFF
Primary Port Id	Port 8
Secondary Port Id	Port 7
VLAN ID	10
Link Down Interval, ms	20
Link Up Interval, ms	20
Link Change Count	4
BLOCKED State Supported	Enabled

5. Edit the Domain Settings as required. Click **Apply** to save; the message “*Domain is enabled*” displays. Click **OK** to clear the webpage message.

6. When the “Media Redundancy Protocol Configuration” page displays again, verify the settings.

Example 1: MRP Manager Re-Config (Web UI)

This application example shows the MRP Manager reconfiguring the traffic path based on the client state.

Sample Setup: This setup includes one device with MRP enabled and has an admin role set as Manager and three clients connected in a ring topology. See the MRP Sample Setup diagram below.

Procedure:

1. Disable any other Ring technologies and disable Spanning-tree at Switch > 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' and click **Apply** to save the first domain.
6. Click **Edit** to go to the 'Ring Domain Configuration (Manager Role)' page and set a Domain name.
    - Tick the Default box for UUID.
    - Select the Primary and Secondary Port IDs.
    - Enable 'Check Media Redundancy'.
    - Leave other settings as default.
7. 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.
    - Enter the same VLAN ID as in step 4 above.
    - Link Down Interval should be 20ms. Link Up Interval should be 20ms. Link change count should be 4.
    - 'BLOCKED State Supported' must be enabled. By default, one ring port will be disabled for loop-free communication.
8. Configure ring ports to Hybrid mode on the VLAN Configuration page. Assign the VLAN ID as configured in step 4.
9. Send bi-directional traffic tagged with the VLAN ID set in step 4 above.
10. 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.
11. 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 1-11 in Example 1 above are required.

Procedure:

1. Disable any other Ring technologies and disable Spanning-tree at Switch > Spanning Tree > CIST Port.
2. Disable 'BLOCKED State Supported'.
3. Configure ring ports to Hybrid mode on the VLAN Configuration page. Assign the VLAN ID as configured in step 4 of Example 1.
4. Send bi-directional traffic tagged with the VLAN ID set in the previous step.
5. Create a failure on any one of the client ring ports by disconnecting the cable. The client ring ports will be in a forwarding state instead of blocking. The MRM should reconfigure the path within 200<500ms. The MRM will send test frames marked with a unique MAC with OUI of 00-15-4E and forwarded by the MRCs to the opposite ring ports per the interval specified.
6. Verify the MRC reacts to the reconfiguration frames as received by the MRM. The link down on the client ring port should be detected by the MRC.
7. There should be no traffic loss after path reconfiguration.

Example 3: MRP Roles Set in Web UI

Setup: This setup shows that the MRP can have both Manager and Undefined roles.

Procedure:

1. Disable any other Ring technologies and disable Spanning-tree at Configuration > Spanning Tree > CIST Port.
2. 'BLOCKED State Supported' should be enabled. By default, one ring port will be disabled for loop-free communication.
3. Configure ring ports to Hybrid mode on the VLAN Configuration page. Assign the VLAN ID as set in step 4 of Example 1.
4. Send bi-directional traffic tagged with the VLAN ID set in the previous step.
5. Create a failure on any one of the client ring ports by disconnecting the cable. The MRM should reconfigure the path within 200<500ms. The Redundancy manager will send test frames marked with a unique MAC with OUI of 00-15-4E and forwarded by the MRCs to the opposite ring ports per the interval specified.
   The disabled ring port should now be enabled and creates a new loop-free topology.
6. There should be no traffic loss after path reconfiguration.
7. On a second client set the 'BLOCKED State Supported' option to disable. The ring port will now be in a forwarding state. Cause a failure on the ring port of another device that has its blocked state disabled.
8. Verify that frames are forwarded and received by the MRC with blocking enabled. There should be no traffic loss after path reconfiguration.

Appendix C. G.8032 Major and Sub Rings Configuration

Introduction

Ethernet Ring Protection Switching (ERPS) is a protocol defined by the International Telecommunication Union - Telecommunication Standardization Sector (ITU-T) to prevent loops at Layer 2. With the standard number is ITU-T G.8032, and ERPS is also called G.8032. Generally, redundant links are used on a network to provide link backup and enhance network reliability. The use of redundant links, however, may produce loops, causing broadcast storms and rendering the MAC address table unstable. These can affect the network, where the communication quality is not good enough, and communication services might be interrupted.

ERPS provides advantages of traditional ring network technologies such as STP/RSTP/MSTP and optimizes detection mechanism to provide faster convergence. For example, the ERPS-enabled switch provides 50-ms convergence for broadcast packets. See section "17. ERPS" for general G.8032 ERPS configuration information.

Basic Concepts

There are some basic concepts that support ERPS Ring:

- **Ring Protection Link (RPL)** – Link designated by mechanism that is blocked during Idle state to prevent loop on Bridged ring.
- **RPL Owner node** – Node connected to RPL that blocks traffic on RPL during Idle state and unblocks during Protection state.
- **RPL Neighbor node** – Node connected to RPL that blocks traffic on RPL during Idle state and unblocks during Protection state (v2).
- **Link Monitoring** – Links of ring are monitored using standard ETH CC OAM messages (CFM) • Signal Fail (SF) – Signal Fail is declared when signal fail condition is detected.
- **No Request (NR)** – No Request is declared when there are no outstanding conditions (e.g., SF, etc.) on the node.
- **Ring APS (R-APS) Messages** – Protocol messages defined in Y.1731 and G.8032.
- **Automatic Protection Switching (APS) Channel** - Ring-wide VLAN used exclusively for transmission of OAM messages including R-APS messages.

IP Addresses

The sample configurations below use these IP addresses:

SISPM1040-582-LRT : 192.168.1.85

SISPM1040-384-LRT-C : 192.168.1.95

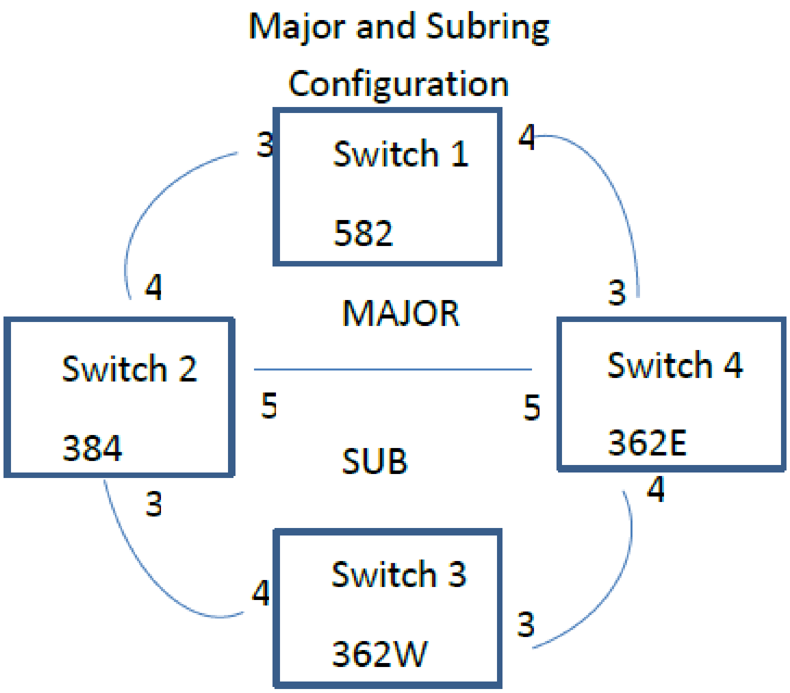
SISPM1040-362-LRT[W] : 192.168.1.125

SISPM1040-362-LRT[E] : 192.168.1.135

Sample Configuration

Major Ring and Sub Ring : 4 Switches

Major : SW#1, SW#2, SW#4; **Sub** : SW#2, SW#3, SW#4



VLANs APS Data

10,20 5

RPL Mode Major Sub Major Sub Major Sub

Owner Owner Neighbor Neighbor None None

Switch Switch Switch Switch Switch Switch

#1 #3 #2 #2 #4 #4

Switch 1 Configuration (SISPM1040-582-LRT)

VLANs Port 3 Trunk Tag All 5,10

Port 4 Trunk Tag All 5,10

STP Port 3 Disable

Port 4 Disable

MEPs Instance	Port	VLAN	MAC	MEP ID	Peer MAC	Peer MEP ID
1	3	10	00-C0-F2-49-39-5F	1	00-40-C7-1C-C7-30	4
2	4	10	00-C0-F2-49-39-60	5	00-C0-F2-53-EF-FC	5

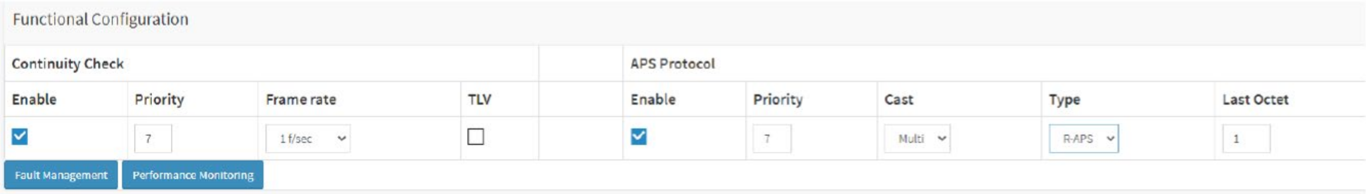
Note: All MEPs are programed the same under the Functional Configuration

Continuity Check

Check Enable – Priority: 7 – Frame rate: 1f/sec

APS Protocol

Check Enable – Priority: 7 – Cast: Multi – Type: R-APS



Functional Configuration

Continuity Check					APS Protocol				
Enable	Priority	Frame rate	TLV		Enable	Priority	Cast	Type	Last Octet
☑	7	1 f/sec	☐		☑	7	Multi	R-APS	1

ERPS

ERPS ID	Port 0	Port 1	Port 0 SF	Port 1 SF	Port 0 APS	Port 1 APS	Ring	RPL	Port	VLAN
1	1	2	1	2	1	2	Major	Owner	0	5

Switch 2 Configuration (SISPM1040-384-LRT-C)

VLANs Port 3 Trunk Tag All 5,20

Port 4 Trunk Tag All 5,10

Port 5 Trunk Tag All 5,10,20

STP Port 3 Disable

Port 4 Disable

Port 5 Disable

MEPs	Instance	Port VLAN	MAC	MEP ID	Peer MAC	Peer MEP ID
1	3	20	00-40-C7-1C-C7-2F	3	00-C0-F2-53-F0-BA	8
2	4	10	00-C0-F2-49-39-60	4	00-C0-F2-49-39-5F	1
3	5	10	00-40-C7-1C-C7-31	9	00-C0-F2-53-EF-FE	10

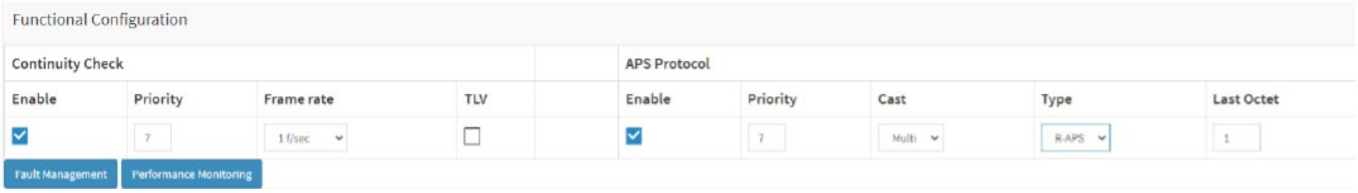
Note: All MEPs are programed the same under the Functional Configuration

Continuity Check

Check Enable – Priority: 7 – Frame rate: 1f/sec

APS Protocol

Check Enable – Priority: 7 – Cast: Multi – Type: R-APS



Functional Configuration

Continuity Check				APS Protocol				
Enable	Priority	Frame rate	TLV	Enable	Priority	Cast	Type	Last Octet
☑	7	1 f/sec	□	☑	7	Multi	R-APS	1

ERPS

ERPS ID	Port 0	Port 1	Port 0 SF	Port 1 SF	Port 0 APS	Port 1 APS	Ring	RPL	Port	VLAN
1	3	2	3	2	3	2	Major	Neighbor	1	5
2	1	0	1	0	1	0	Sub	Neighbor	0	5

Interconnect Yes, Major 1

Switch 3 Configuration (SISPM1040-362-LRT[W])

VLANs Port 3 Trunk Tag All 5,20

Port 4 Trunk Tag All 5,20

STP Port 3 Disable

Port 4 Disable

MEPs	Instance	Port	VLAN	MAC	MEP ID	Peer MAC	Peer MEP ID
1	3	20	00-C0-F2-53-F0-B9	7	00-C0-F2-53-EF-FD	6	
2	4	20	00-C0-F2-53-F0-BA	8	00-40-C7-1C-C7-2F	3	

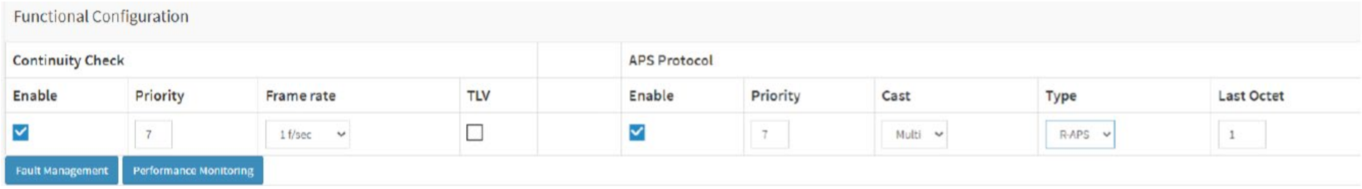
Note: All MEPs are programed the same under the Functional Configuration

Continuity Check

Check Enable – Priority: 7 – Frame rate: 1f/sec

APS Protocol

Check Enable – Priority: 7 – Cast: Multi – Type: R-APS



Functional Configuration

Continuity Check					APS Protocol				
Enable	Priority	Frame rate	TLV		Enable	Priority	Cast	Type	Last Octet
☑	7	1 f/sec	☐		☑	7	Multi	R-APS	1

ERPS

ERPS ID	Port 0	Port 1	Port 0 SF	Port 1 SF	Port 0 APS	Port 1 APS	Ring	RPL	Port	VLAN
1	1	2	1	2	1	2	Sub	Owner	1	5

Switch 4 Configuration (SISPM1040-362-LRT[E])

VLANs Port 3 Trunk Tag All 5,10

Port 4 Trunk Tag All 5,20

Port 5 Trunk Tag All 5,10,20

STP Port 3 Disable

Port 4 Disable

Port 5 Disable

MEPs Instance	Port	VLAN	MAC	MEP ID	Peer MAC	Peer MEP ID
1	3	10	00-C0-F2-53-EF-FC	5	00-C0-F2-49-39-60	2
2	4	20	00-C0-F2-53-EF-FD	6	00-C0-F2-53-F0-B9	7
3	5	10	00-C0-F2-53-EF-FE	10	00-40-C7-1C-C7-31	9

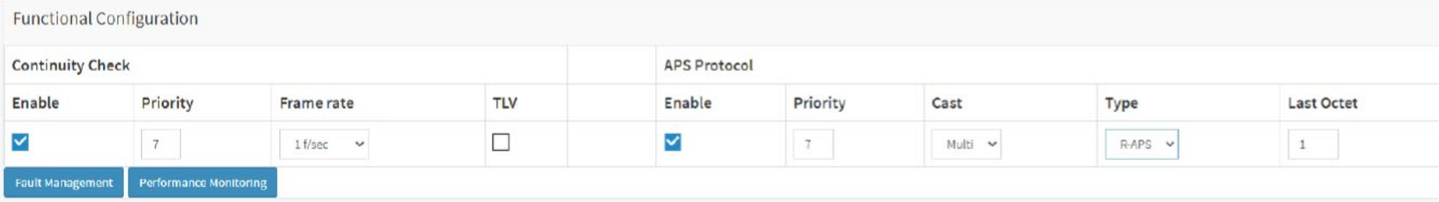
Note: All MEPs are programed the same under the Functional Configuration

Continuity Check

Check Enable – Priority: 7 – Frame rate: 1f/sec

APS Protocol

Check Enable – Priority: 7 – Cast: Multi – Type: R-APS



Functional Configuration

Continuity Check					APS Protocol				
Enable	Priority	Frame rate	TLV		Enable	Priority	Cast	Type	Last Octet
☑	7	1 f/sec	□		☑	7	Multi	R-APS	1

ERPS

ERPS ID	Port 0	Port 1	Port 0 SF	Port 1 SF	Port 0 APS	Port 1 APS	Ring	RPL	Port VLAN
1	1	3	1	3	1	3	Major	None	5
2	2	0	2	0	2	0	Sub	None	5

Interconnect Yes, Major 1

Testing

Testing Pings from Switch 4 to Switch 1 – Major Ring

Failing Major ring, No lost pings

```
C:\Users\dennist>ping 192.168.1.85 -t
Pinging 192.168.1.85 with 32 bytes of data:
Reply from 192.168.1.85: bytes=32 time<1ms TTL=64
Reply from 192.168.1.85: bytes=32 time<1ms TTL=64
Reply from 192.168.1.85: bytes=32 time<1ms TTL=64
Reply from 192.168.1.85: bytes=32 time<1ms TTL=64
Reply from 192.168.1.85: bytes=32 time<1ms TTL=64
Reply from 192.168.1.85: bytes=32 time<1ms TTL=64
Reply from 192.168.1.85: bytes=32 time<1ms TTL=64
Reply from 192.168.1.85: bytes=32 time<1ms TTL=64
Reply from 192.168.1.85: bytes=32 time<1ms TTL=64
Reply from 192.168.1.85: bytes=32 time<1ms TTL=64
Reply from 192.168.1.85: bytes=32 time<1ms TTL=64
Reply from 192.168.1.85: bytes=32 time<1ms TTL=64
Reply from 192.168.1.85: bytes=32 time<1ms TTL=64
Reply from 192.168.1.85: bytes=32 time<1ms TTL=64
Reply from 192.168.1.85: bytes=32 time<1ms TTL=64
Reply from 192.168.1.85: bytes=32 time<1ms TTL=64
Reply from 192.168.1.85: bytes=32 time<1ms TTL=64
Reply from 192.168.1.85: bytes=32 time<1ms TTL=64
Reply from 192.168.1.85: bytes=32 time=1ms TTL=64
Reply from 192.168.1.85: bytes=32 time<1ms TTL=64
Reply from 192.168.1.85: bytes=32 time<1ms TTL=64
Reply from 192.168.1.85: bytes=32 time<1ms TTL=64
Reply from 192.168.1.85: bytes=32 time<1ms TTL=64
Reply from 192.168.1.85: bytes=32 time<1ms TTL=64
Reply from 192.168.1.85: bytes=32 time<1ms TTL=64
Reply from 192.168.1.85: bytes=32 time<1ms TTL=64
Reply from 192.168.1.85: bytes=32 time<1ms TTL=64
Reply from 192.168.1.85: bytes=32 time<1ms TTL=64
Reply from 192.168.1.85: bytes=32 time<1ms TTL=64
Reply from 192.168.1.85: bytes=32 time=5ms TTL=64  ←----------------------
Reply from 192.168.1.85: bytes=32 time<1ms TTL=64  Cable Disconnect
Reply from 192.168.1.85: bytes=32 time=3ms TTL=64  ←----------------------
Reply from 192.168.1.85: bytes=32 time<1ms TTL=64
Reply from 192.168.1.85: bytes=32 time=1ms TTL=64
Reply from 192.168.1.85: bytes=32 time<1ms TTL=64
Reply from 192.168.1.85: bytes=32 time<1ms TTL=64
Reply from 192.168.1.85: bytes=32 time=1ms TTL=64
Reply from 192.168.1.85: bytes=32 time<1ms TTL=64
Reply from 192.168.1.85: bytes=32 time<1ms TTL=64
Ping statistics for 192.168.1.85:
Packets: Sent = 45, Received = 45, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 0ms, Maximum = 5ms, Average = 0ms
```

Testing Pings from Switch 4 to Switch 3 – Sub Ring

Fail Subring, No lost pings

```
C:\Users\dennist>ping 192.168.1.125 -t
Pinging 192.168.1.125 with 32 bytes of data:
Reply from 192.168.1.125: bytes=32 time=1ms TTL=64
Reply from 192.168.1.125: bytes=32 time<1ms TTL=64
Reply from 192.168.1.125: bytes=32 time<1ms TTL=64
Reply from 192.168.1.125: bytes=32 time<1ms TTL=64
Reply from 192.168.1.125: bytes=32 time<1ms TTL=64
Reply from 192.168.1.125: bytes=32 time<1ms TTL=64
Reply from 192.168.1.125: bytes=32 time<1ms TTL=64
Reply from 192.168.1.125: bytes=32 time<1ms TTL=64
Reply from 192.168.1.125: bytes=32 time<1ms TTL=64
Reply from 192.168.1.125: bytes=32 time<1ms TTL=64
Reply from 192.168.1.125: bytes=32 time<1ms TTL=64
Reply from 192.168.1.125: bytes=32 time<1ms TTL=64
Reply from 192.168.1.125: bytes=32 time<1ms TTL=64
Reply from 192.168.1.125: bytes=32 time=1ms TTL=64
Reply from 192.168.1.125: bytes=32 time<1ms TTL=64
Reply from 192.168.1.125: bytes=32 time<1ms TTL=64
Reply from 192.168.1.125: bytes=32 time<1ms TTL=64
Reply from 192.168.1.125: bytes=32 time<1ms TTL=64
Reply from 192.168.1.125: bytes=32 time<1ms TTL=64
Reply from 192.168.1.125: bytes=32 time<1ms TTL=64
Reply from 192.168.1.125: bytes=32 time<1ms TTL=64
Reply from 192.168.1.125: bytes=32 time=7ms TTL=64   ←---------------------
Reply from 192.168.1.125: bytes=32 time<1ms TTL=64   Cable Disconnect
Reply from 192.168.1.125: bytes=32 time<1ms TTL=64
Reply from 192.168.1.125: bytes=32 time<1ms TTL=64
Reply from 192.168.1.125: bytes=32 time<1ms TTL=64
Reply from 192.168.1.125: bytes=32 time<1ms TTL=64
Reply from 192.168.1.125: bytes=32 time<1ms TTL=64
Reply from 192.168.1.125: bytes=32 time<1ms TTL=64
Reply from 192.168.1.125: bytes=32 time=1ms TTL=64
Reply from 192.168.1.125: bytes=32 time<1ms TTL=64
Reply from 192.168.1.125: bytes=32 time=1ms TTL=64
Reply from 192.168.1.125: bytes=32 time<1ms TTL=64
Reply from 192.168.1.125: bytes=32 time<1ms TTL=64
Reply from 192.168.1.125: bytes=32 time<1ms TTL=64
Reply from 192.168.1.125: bytes=32 time<1ms TTL=64
Reply from 192.168.1.125: bytes=32 time<1ms TTL=64
Reply from 192.168.1.125: bytes=32 time<1ms TTL=64
Reply from 192.168.1.125: bytes=32 time<1ms TTL=64
Ping statistics for 192.168.1.125:
Packets: Sent = 41, Received = 41, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 0ms, Maximum = 7ms, Average = 0ms
```

Config files

running-config_192.168.1

```
hostname SISPM1040-362-LRT-E
username admin privilege 15 password encrypted feec1d1085ff075fd03b1d2d5ab4c0befbff0917079c8abb3a77338041bf5d6e1771bdbbd1a317ea2f42fc2aacc8c50a8e667456d7c04099f74f8ef9dcc0fbd4
!
vlan 1
!
!
!
!
ip route 0.0.0.0 0.0.0.0 192.168.1.254
tzidx 0
exec-timeout autologout 0
snmp-server location DT Lab Ring
system name SISPM1040-362-LRT-E
system location DT Lab Ring
system description Managed Hardened PoE+ Switch, (4) 10/100/1000Base-T PoE+ Ports + (2) 10/100/1000Base-T Ports + (2) 100/1000Base-X SFP Ports
!
interface GigabitEthernet 1/1
!
interface GigabitEthernet 1/2
!
interface GigabitEthernet 1/3
 no spanning-tree
 switchport trunk allowed vlan 5,10
 switchport trunk vlan tag native
 switchport mode trunk
 poe mode disable
!
interface GigabitEthernet 1/4
 no spanning-tree
 switchport trunk allowed vlan 5,20
 switchport trunk vlan tag native
 switchport mode trunk
 poe mode disable
```

```
!
interface GigabitEthernet 1/5
 no spanning-tree
 switchport trunk allowed vlan 5,10,20
 switchport trunk vlan tag native
 switchport mode trunk
!
interface GigabitEthernet 1/6
!
interface GigabitEthernet 1/7
!
interface GigabitEthernet 1/8
!
interface vlan 1
 ip address 192.168.1.135 255.255.255.0
 ip dhcp server
!
mep 1 down domain port level 4 interface GigabitEthernet 1/3
mep 1 mep-id 5
mep 1 vid 10
mep 1 peer-mep-id 2 mac 00-C0-F2-49-39-60
mep 1 cc 7
mep 1 aps 7 raps
mep 2 down domain port level 4 interface GigabitEthernet 1/4
mep 2 mep-id 6
mep 2 vid 20
mep 2 peer-mep-id 7 mac 00-C0-F2-53-F0-B9
mep 2 cc 7
mep 2 aps 7 raps
mep 3 down domain port level 4 interface GigabitEthernet 1/5
mep 3 mep-id 10
mep 3 vid 10
mep 3 peer-mep-id 9 mac 00-40-C7-1C-C7-31
mep 3 cc 7
mep 3 aps 7 raps
erps 1 major port0 interface GigabitEthernet 1/3 port1 interface GigabitEthernet 1/5
erps 1 mep port0 sf 1 aps 1 port1 sf 3 aps 3
erps 1 vlan 5
erps 2 sub port0 interface GigabitEthernet 1/4 interconnect 1
erps 2 mep port0 sf 2 aps 2
erps 2 vlan 5
!
spanning-tree aggregation
 spanning-tree link-type point-to-point
!
!
line console 0
!
line vty 0
!
line vty 1
!
line vty 2
!
line vty 3
!
line vty 4
!
line vty 5
!
line vty 6
!
line vty 7
!
line vty 8
!
line vty 9
!
line vty 10
!
line vty 11
!
line vty 12
!
line vty 13
!
```

```
line vty 14
!
line vty 15
!
!
end
```

running-config_192.168.1

```
hostname SISPM1040-582-LRT
logging on
logging host 192.168.1.253
username admin privilege 15 password encrypted
7073dec86c15b8a9907bb4106ef783adde46bd5b5969cc68fb55b430336bd7c80d5ded65d2fdb39abe81cc9caa5a
93620f270c21bca86e776cee9c5588bfb8c7
username superuser privilege 15 password encrypted
4643fdc71f39fd4cb955943fcaf89faca81bc650fbaeebe25a796662d5c225bf0d5ded65d2fdb39abe81cc9c514497e
27799560e488713aabaac4f167e7732ca
!
vlan 1
!
!
!
!
ip route 0.0.0.0 0.0.0.0 192.168.1.254
ntp automatic
ntp server 1 ip-address ntp1.transition.com
ntp server 2 ip-address ntp2.transition.com
clock timezone '' 9
tzidx 0
exec-timeout autologout 0
poe ping-check enable
snmp-server contact DTroxel
snmp-server location DT Office
system contact DTroxel
system name SISPM1040-582-LRT
system location DT Office
system description Managed Hardened PoE++ Switch (8) 10/100/1000Base-T PoE++ Ports + (2) 100/1000Base-X
SFP Slot
!
interface GigabitEthernet 1/1
 no spanning-tree
 poe ping-ip-addr 192.168.1.70
 poe failure-action reboot-Remote-PD
!
interface GigabitEthernet 1/2
```

```
 no spanning-tree
 switchport forbidden vlan add 3,5
!
interface GigabitEthernet 1/3
 no spanning-tree
 switchport trunk allowed vlan 5,10
 switchport trunk vlan tag native
 switchport mode trunk
 poe mode disable
!
interface GigabitEthernet 1/4
 no spanning-tree
 switchport trunk allowed vlan 5,10
 switchport trunk vlan tag native
 switchport mode trunk
 poe mode disable
 poe ping-ip-addr 192.168.1.200
!
interface GigabitEthernet 1/5
 no spanning-tree
!
interface GigabitEthernet 1/6
 no spanning-tree
!
interface GigabitEthernet 1/7
!
interface GigabitEthernet 1/8
 poe mode disable
!
interface GigabitEthernet 1/9
 no spanning-tree
!
interface GigabitEthernet 1/10
 no spanning-tree
!
interface vlan 1
 ip address 192.168.1.85 255.255.255.0
 ip dhcp server
```

```
!
mep 1 down domain port level 4 interface GigabitEthernet 1/3
mep 1 vid 10
mep 1 peer-mep-id 4 mac 00-40-C7-1C-C7-30
mep 1 cc 7
mep 1 aps 7 raps
mep 2 down domain port level 4 interface GigabitEthernet 1/4
mep 2 mep-id 2
mep 2 vid 10
mep 2 peer-mep-id 5 mac 00-C0-F2-53-EF-FC
mep 2 cc 7
mep 2 aps 7 raps
erps 1 major port0 interface GigabitEthernet 1/3 port1 interface GigabitEthernet 1/4
erps 1 mep port0 sf 1 aps 1 port1 sf 2 aps 2
erps 1 rpl owner port0
erps 1 vlan 5
!
spanning-tree aggregation
 no spanning-tree
 spanning-tree link-type point-to-point
!
!
line console 0
!
line vty 0
!
line vty 1
!
line vty 2
!
line vty 3
!
line vty 4
!
line vty 5
!
line vty 6
!
```

```
line vty 7
!
line vty 8
!
line vty 9
!
line vty 10
!
line vty 11
!
line vty 12
!
line vty 13
!
line vty 14
!
line vty 15
!
map-api-key AIzaSyBItuM0hDtK6nJeZPEk7jnrcoGGi92EpFM
!
end
```

running-config_192.168.1

```
hostname SISPM1040-384-LRT-C
username admin privilege 15 password encrypted
6593186b999f348becd63b8612ac561c114250a1a00bd38f6afb5378acb6d08c1864c59b092b0e2b29ba4f1d5591
66800846cbc52c4558a90e4cdf95d3cfcbf4
username dennis privilege 5 password encrypted
a92a5dbf4fcd2e13d35adb36d2418476e907de19a641fa7baf80b1abb2bacd8ee5dbdd44e246b88be1636df6b876
9af790aa8721622481085e33c32e6e119dbd
!
vlan 1
!
!
!
!
ip route 0.0.0.0 0.0.0.0 192.168.1.254
tzidx 0
exec-timeout autologout 0
poe ping-check enable
access-list ace 2 ingress interface GigabitEthernet 1/2 action deny
access-list ace 1 next 2 ingress interface GigabitEthernet 1/2 frame-type ipv4-tcp dport 443
system name SISPM1040-384-LRT-C
system description Managed Hardened PoE+ Switch, (8) 10/100/1000Base-T PoE+ Ports + (4) 100/1000Base-X
SFP
!
interface GigabitEthernet 1/1
 no spanning-tree
 lldp cdp-aware
 poe ping-ip-addr 192.168.1.100
 poe failure-action reboot-Remote-PD
!
interface GigabitEthernet 1/2
 no spanning-tree
 lldp cdp-aware
 speed 1000
 duplex full
!
interface GigabitEthernet 1/3
 no spanning-tree
 switchport trunk allowed vlan 5,20
 switchport trunk vlan tag native
 switchport mode trunk
 lldp cdp-aware
 poe mode disable
!
interface GigabitEthernet 1/4
 no spanning-tree
 switchport trunk allowed vlan 5,10
 switchport trunk vlan tag native
 switchport mode trunk
 lldp cdp-aware
 poe mode disable
!
interface GigabitEthernet 1/5
 no spanning-tree
 switchport trunk allowed vlan 5,10,20
 switchport trunk vlan tag native
 switchport mode trunk
 lldp cdp-aware
 poe mode disable
!
interface GigabitEthernet 1/6
 no spanning-tree
 lldp cdp-aware
!
interface GigabitEthernet 1/7
 lldp cdp-aware
!
interface GigabitEthernet 1/8
 lldp cdp-aware
!
interface GigabitEthernet 1/9
 no spanning-tree
 switchport trunk allowed vlan 1,50,100
 switchport trunk vlan tag native
 lldp cdp-aware
!
```

```
interface GigabitEthernet 1/10
 no spanning-tree
 lldp cdp-aware
!
interface GigabitEthernet 1/11
 no spanning-tree
 lldp cdp-aware
!
interface GigabitEthernet 1/12
 no spanning-tree
 lldp cdp-aware
!
interface vlan 1
 ip address 192.168.1.95 255.255.255.0
 ip dhcp server
!
mep 1 down domain port level 4 interface GigabitEthernet 1/3
mep 1 mep-id 3
mep 1 vid 20
mep 1 peer-mep-id 8 mac 00-C0-F2-53-F0-BA
mep 1 cc 7
mep 1 aps 7 raps
mep 2 down domain port level 4 interface GigabitEthernet 1/4
mep 2 mep-id 4
mep 2 vid 10
mep 2 peer-mep-id 1 mac 00-C0-F2-49-39-5F
mep 2 cc 7
mep 2 aps 7 raps
mep 3 down domain port level 4 interface GigabitEthernet 1/5
mep 3 mep-id 9
mep 3 vid 10
mep 3 peer-mep-id 10 mac 00-C0-F2-53-EF-FE
mep 3 cc 7
mep 3 aps 7 raps
erps 1 major port0 interface GigabitEthernet 1/5 port1 interface GigabitEthernet 1/4
erps 1 mep port0 sf 3 aps 3 port1 sf 2 aps 2
erps 1 rpl neighbor port1
erps 1 vlan 5
erps 2 sub port0 interface GigabitEthernet 1/3 interconnect 1
erps 2 mep port0 sf 1 aps 1
erps 2 rpl neighbor port0
erps 2 vlan 5
!
spanning-tree aggregation
 no spanning-tree
 spanning-tree link-type point-to-point
!
!
line console 0
!
line vty 0
!
line vty 1
!
line vty 2
!
line vty 3
!
line vty 4
!
line vty 5
!
line vty 6
!
line vty 7
!
line vty 8
!
line vty 9
!
line vty 10
!
line vty 11
!
line vty 12
!
```

```
line vty 13
!
line vty 14
!
line vty 15
!
map-api-key AIzaSyBItuM0hDtK6nJeZPEk7jnrcoGGi92EpFM
!
end
```

running-config_192.168.1

```
hostname SISPM1040-362-LRT-W
username admin privilege 15 password encrypted 6158ed7daf39d06ded0e7c4828c3b15bb4c40673bd445afcd643295925ae425d9611d1cbe872708237571aacc7b9237f33b01ae6866e2484009edfe1fa0bf56f
!
vlan 1
!
!
!
!
ip route 0.0.0.0 0.0.0.0 192.168.1.254
tzidx 0
exec-timeout autologout 0
snmp-server location DT Lab Ring
system name SISPM1040-362-LRT-W
system location DT Lab Ring
system description Managed Hardened PoE+ Switch, (4) 10/100/1000Base-T PoE+ Ports + (2) 10/100/1000Base-T Ports + (2) 100/1000Base-X SFP Ports
!
interface GigabitEthernet 1/1
!
interface GigabitEthernet 1/2
!
interface GigabitEthernet 1/3
 no spanning-tree
 switchport trunk allowed vlan 5,20
 switchport trunk vlan tag native
 switchport mode trunk
 poe mode disable
!
interface GigabitEthernet 1/4
 no spanning-tree
 switchport trunk allowed vlan 5,20
 switchport trunk vlan tag native
 switchport mode trunk
 poe mode disable
!
```

```
interface GigabitEthernet 1/5
!
interface GigabitEthernet 1/6
!
interface GigabitEthernet 1/7
!
interface GigabitEthernet 1/8
!
interface vlan 1
 ip address 192.168.1.125 255.255.255.0
 ip dhcp server
!
mep 1 down domain port level 4 interface GigabitEthernet 1/3
mep 1 mep-id 7
mep 1 vid 20
mep 1 peer-mep-id 6 mac 00-C0-F2-53-EF-FD
mep 1 cc 7
mep 1 aps 7 raps
mep 2 down domain port level 4 interface GigabitEthernet 1/4
mep 2 mep-id 8
mep 2 vid 20
mep 2 peer-mep-id 3 mac 00-40-C7-1C-C7-2F
mep 2 cc 7
mep 2 aps 7 raps
erps 1 sub port0 interface GigabitEthernet 1/3 port1 interface GigabitEthernet 1/4
erps 1 mep port0 sf 1 aps 1 port1 sf 2 aps 2
erps 1 rpl owner port1
erps 1 vlan 5
!
spanning-tree aggregation
 spanning-tree link-type point-to-point
!
!
line console 0
!
line vty 0
!
line vty 1
```

```
!
line vty 2
!
line vty 3
!
line vty 4
!
line vty 5
!
line vty 6
!
line vty 7
!
line vty 8
!
line vty 9
!
line vty 10
!
line vty 11
!
line vty 12
!
line vty 13
!
line vty 14
!
line vty 15
!
!
end
```