

SISPM1040-582-LRT

Managed Hardened PoE++ Switch (8) 10/100/1000Base-T PoE++ Ports + (2) 100/1000Base-X SFP Slot

Web User Guide

Intellectual Property

© 2022, 2023 Lantronix, Inc. All rights reserved. No part of the contents of this publication may be transmitted or reproduced in any form or by any means without the written permission of Lantronix. *Lantronix* is a registered trademark of Lantronix, Inc. in the United States and other countries. Patented: <https://www.lantronix.com/legal/patents/>; additional patents pending.

Warranty

For details on the Lantronix warranty policy, please 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
9/28/21	G	FW VB7.20.0075: add API command "get_config_action_status" and fix API cannot delete old interface VLAN. Fix PoE Power Requested and Power Allocated not match. Add reboot the switch when DI input goes High and fix DDM information not updated. Fix DI/DO bug: after triggering DI reboot system event, Server may not receive syslog event. Fix PMD auto negotiation advertised capability info in the LLDP packet of fiber ports. Fix port can't link up when TN-EOT-CO and TN-EOT-RT copper module is inserted after rebooting switch or changing mode from force 1000M to auto. Add 'SystemDORelayOpenClose' to MIB. Fix port link up when inserting TN-EOT-CO/TN-EOT-RT copper SFP module.
9/28/22	H	FW VB7.20.0121: update RADIUS server and add two new DMS icons. Initial Lantronix rebrand. Add First Time Wizard and DHCP IP per port and update SNMP and Auth Method default settings. Add DHCP option 229 (lighting server). Add ConsoleFlow and LPM features and update DMS Google Maps API information..
11/6/23	J	FW VB7.20.0191: Change ConsoleFlow to Percepixon. Support API in HTTPS. Add DHCP per Port VLAN and update LLDP-MED Neighbor Information webpage. Allow dash character (-) for status update interval and content check interval and switch disconnect from server. Add PoE++ clarifications. Add support for two public OIDs. Automatically save Config changes to Start-Up Config in Percepixon server. Update to Dropbear 2022.82.

Contents

1	Introduction	8
1.2	About This Manual	8
1.3	Related Manuals	8
2	Web-based Management	9
2.1	Initial Login and Configuration	9
2.2	First Time Wizard	10
2.3	Startup Page	13
2.4	Webpage Controls	14
2.5	Webpage Messages	15
3	System Configuration	16
3.1	System	16
3.1.1	Information	16
3.1.2	IP	17
3.1.3	NTP	23
3.1.4	Time	25
3.1.5	Log	27
3.1.6	Digital I/O	28
3.1.7	Alarm Notification	30
3-2	Green Ethernet	34
3.2.1	Port Power Savings	34
3-3	Ports Configuration	36
3.3.1	Ports	36
3.3.2	Ports Description	38
3-4	DHCP	39
3.4.1	Server	39
3.4.2	Snooping	47
3.4.3	Relay	49
3-5	Security	51
3.5.1	Switch	51
3.5.1.1	Users	51
3-5.2	Network	82
3-5.3	AAA	117
3-6	Aggregation	122
3-6.1	Static	122
3-6.2	LACP	124
3-6.3	LACP on Air	126
3-7	Link OAM	128
3-7.1	Port Settings	128
3-7.2	Event Settings	130
3-8	Loop Protection	132
3-9	Spanning Tree	134
3-9.1	Bridge Setting	135
3-9.2	MSTI Mapping	137
3-9.3	MSTI Priorities	139
3-9.4	CIST Port	140
3-9.5	MSTI Ports	142
3-10	IPMC Profile	144
3-10.1	Profile Table	144
3-10.2	Address Entry	147
3-11	MVR	148

3-12 IPMC	150
3-12.1 IGMP Snooping	150
3-12.2 MLD Snooping	157
3-13 LLDP	163
3-13.1 LLDP	163
2-13.2 LLDP-MED	166
3-14 PoE	171
3-14.1 Configuration	171
3-14.2 Lantronix POE++ Switch PoE Classification Settings	176
3-14.3 Recommended Settings	176
3-14.4 Power Delay	177
3-14.5 Schedule Profile	178
3-14.6 PoE Auto Power Reset	179
3-14.7 Chip Reset Schedule	181
3-15 EPS	182
3-16 MEP	186
3-17 ERPS	201
3-18 MAC Table	206
3-19 VLAN Translation	208
3-19.1 Port to Group Mapping	208
3-19.2 VID Translation Mapping	210
3-20 VLANs	212
3-21 Private VLANs	215
3-21.1 Membership	215
3-22.2 Port Isolation	217
3-23 VCL	218
3-23.1 MAC-based VLAN	218
3-23.2 Protocol-based VLAN	220
3-24 Voice VLAN	225
3-24.1 Configuration	225
3-24.2 OUI	227
3-25 Ethernet Services	228
3-25.1 Ports	228
3-25.2 L2CP	230
3-25.3 Bandwidth Profiles	231
3-25.4 EVCs	233
3-25.5 ECEs	236
3-26 QoS	239
3-26.1 Port Classification	239
3-26.2 Port Policing	243
3-26.3 Queue Policing	245
3-26.4 Port Scheduler	247
3-26.5 QoS Egress Port Shapers	249
3-26.6 Port Tag Remarking	250
3-26.7 Port DSCP	252
3-26.8 DSCP-Based QoS	254
3-26.9 DSCP Translation	256
3-26.10 DSCP Classification	258
3-26.11 QoS Control List	259
3-26.12 Storm Control	264
3-27 Mirroring	265
3-28 UPnP	269
3-29 PTP	270
3-30 GVRP	277

3-30.2 Port Config	279
3-31 sFlow	280
3-32 UDLD	283
3-33 Rapid Ring / Ring To Ring / Rapid Chain	285
3-33.1 Rapid Ring Operation	286
3-33.2 Single Ring	287
3-33.3 Ring to Ring	288
3-33.4 Dual Ring	289
3-33.5 Rapid Chain	290
3-33.6 HW Setting and Status for Rings	291
3-34 PercepXion and LPM	292
3-34.1 Supported Firmware Versions	292
3-34.2 PercepXion Agent Configuration	292
3-34.3 PercepXion Upload	296
3-35 MRP	297
3-36 SMTP	301
4. Monitor	302
4.1 Monitor > System > Information	302
4-1.2 IP Status	304
4-1.3 Log	306
4-1.4 Detailed Log	308
4-2 Green Ethernet	309
4-2.1 Port Power Savings	309
4-3 Ports	310
4-3.1 Traffic Overview	310
4-3.2 QoS Statistics	311
4-3.3 QCL Status	312
4-3.4 Detailed Statistics	314
4-3.5 SFP Information	316
3-3.6 SFP Detail Info	318
4-4 Link OAM	320
4-4.1 Statistics	320
4-4.2 Port Status	322
4-4.3 Event Status	324
4-5 DHCP	327
4-5.1 Server	327
4-5.2 Snooping Table	331
4-5.3 Relay Statistics	332
4-5.4 Detailed Statistics	334
4-6 Security	336
4-6.1 Access Management Statistics	336
4-6.2 Network	337
4-6.2.1 Port Security	337
4-6.3 AAA	352
4-6.4 Switch	359
4-7 Aggregation	365
4-7.1 Status	365
4-7.2 LACP	366
4-8 Loop Protection	369
4-9 Spanning Tree	370
4-10 MVR	375
4-11 IPMC	378
3-11.1 IGMP Snooping	378

4-12 LLDP	386
4-12.1 Neighbor.....	386
4-12.2 LLDP-MED Neighbor	388
4-12.3 PoE	392
4-12.4 EEE	393
4-12.5 Port Statistics	395
4-13 Ethernet Services	397
4-13.1 EVC Statistics	397
4-14 PTP	399
4-15 PoE	406
4-16 MAC Table	408
4-17 VLANs	410
4-17.1 Membership	410
4-17.2 Ports	412
4-18 MRP	414
4-19 VCL	416
4-19.1 MAC-based VLAN.....	416
4-19.2 Protocol-based VLAN	417
4-20 sFlow	421
4-21 UDLD	423
5. Diagnostics	424
5-1 Ping	424
5-2 Ping6	426
5-3 Cable Diagnostics	428
5-4 Traceroute	430
5-5 Link OAM	432
5-5.1 MIB Retrieval.....	432
6. Maintenance.....	433
6-1 Restart Device.....	433
6-2 Reboot Schedule	434
6-3 Factory Defaults	435
6-4 Firmware	436
6-4.1 Firmware Upgrade	436
6-4.2 Firmware Selection	437
6-5 Configuration.....	439
6-5.1 Save startup-config	439
6-5.2 Download	440
6-5.3 Upload.....	442
6-5.4 Activate	444
6-5.5 Delete.....	445
6-6 Server Report.....	446
7. DMS (Device Management System)	448
7.1 DMS > Management	448
7.1.1 DMS > DMS Mode	448
7.1.2 DMS Mode – DMS Controller Switch	450
7.1.3 DMS > Management > Map API Key	451
7.1.4 DMS > Management > Device List	452
7.2 DMS > Graphical Monitoring.....	454
7.2.1 DMS > Graphical Monitoring > Topology View	454
7.2.2 DMS Firmware Upgrade Procedure.....	460
7.2.3 DMS > Graphical Monitoring > Floor View.....	462
7.2.4 DMS > Graphical Monitoring > Map View	466

7.4 DMS > Maintenance.....	470
7.4.1 DMS > Maintenance > Floor Image	470
7.4.2 DMS > Maintenance > Diagnostics.....	473
7.4.3 DMS > Maintenance > Traffic Monitor	475
7.4.4 DMS Troubleshooting	477
8. Recording Device and System Information.....	479
8.1 Product Labels	480
Appendix A. DHCP Per Port and DHCP per VLAN.....	481
A-1. Configure DHCP Per Port via the Web UI.....	481
A-2. DHCP Per Port Mode Configuration.....	482
A-3. DHCP Per Port VLAN.....	484
Appendix B. MRP Pre-Requisites and Application Examples.....	485
B-1. MRP Description.....	485
B-2. MRP Operation	485
B-3. Related Devices	486
B-4. MRP Sample Setup	486
B-5. MRP Pre-Requisites (General).....	486
B-6. MRP Web UI Configuration	487
Appendix C – G.8032 Major and Sub Rings Configuration.....	491
C-1. Introduction.....	491
C-2. Basic Concepts	491
C-3. IP Addresses	491
C-4. Sample Configuration.....	492
C-5. Testing.....	497
C-6. Config files.....	499

1 Introduction

The SISPM1040-582-LRT is a managed PoE++ switch suitable for connecting and powering devices in hardened environments. It has (8) 10/100/1000 PoE++ ports with (2) 100/1000 dual speed SFP slots. The switch can supply up to 90 Watts per port on (4) ports or 60 Watts per port on (8) ports simultaneously. The switch also includes the embedded Device Management System (DMS) software that provides the advanced tools necessary for total management of all IP addressable devices. The unique DMS provides security integrators with lower overall cost, less downtime and easier management of the entire PoE+ network. Lantronix hardened switches are certified to operate reliably in harsh environments such as those found on factory floors, outdoor enclosures or other challenging environments.

1.2 About This Manual

This manual gives specific information on how to operate and use the management functions of the switch via its web browser. This manual is intended for use by network administrators who are responsible for operating and maintaining network equipment; it assumes a basic working knowledge of general switch functions, the Internet Protocol (IP), and Hypertext Transfer Protocol (HTTP).

1.3 Related Manuals

- SISPM1040-582-LRT Quick Start Guide, 33754
- SISPM1040-582-LRT Install Guide, 33755
- SISPM1040-582-LRT Web User Guide, 33756 (this manual)
- SISPM1040-582-LRT CLI Reference, 33757
- SISPM1040-582-LRT API User Guide, 33826
- Release Notes (version specific)

For Lantronix Documentation, Firmware, App Notes, etc. go to <https://www.lantronix.com/technical-support/>. For SFP or SFP+ information see the Lantronix [SFP webpage](#).

Note that this manual provides links to third party websites for which Lantronix is not responsible. These external third party links are provided as a convenience and are for informational purposes only; they do not constitute an endorsement or an approval by Lantronix of any of the products, services, or opinions of the corporation or organization or individual. Lantronix bears no responsibility for the accuracy, legality, or content of these external sites or for subsequent links. Contact the external site for answers to questions regarding its content.

2 Web-based Management

2.1 Initial Login and Configuration

This chapter describes how to configure and manage the switch via the Web user interface. The Web UI lets you easily configure and monitor from any port of the switch all switch modules and parameters.

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

After the switch has been configured, you can browse it. For instance, type 192.168.1.77 in the address row in a browser, it will show the following screen and ask you for a username and password to login.



Figure 2.1: Login page

The default username is “admin” and the default password is “admin”. For first time use, enter the default username and password, and then click the Login button. The login process now is completed.

Note: To optimize the display effect, we recommend you use Microsoft IE 10 above, Chrome V.39 above or Firefox V.33 above and have the resolution 1920x1080.

Note: The switch has DHCP disabled by default, so if you do not have a DHCP server to provide an IP addresses to the switch, the switch defaults to IP address 192.168.1.77.



: Click to show the Login text as you enter it. Added at FW VB7.20.0191.



: Click to hide the Login text as you enter it. Added at FW VB7.20.0191.

2.2 First Time Wizard

The first time you use this device you must configure some basic settings such as password, IP address, date and time, and system information. The First Time Wizard was added at FW v 7.20.0121. Use the following procedure:

Step 1: Change default password

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

The figure shows two screenshots of the Lantronix web interface. The left screenshot is titled 'Change default password' and features a progress bar at the top with four steps: 'PASSWORD' (selected), 'IP ADDRESS', 'DATE & TIME', and 'INFORMATION'. Below the title are two text input fields for 'New password' and 'Repeat new password'. A list of requirements is provided: '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.' A blue 'Next' button is at the bottom. The right screenshot is titled 'Set IP address' and has the same progress bar. It shows 'Interface VLAN ID' set to '1', two radio buttons for 'Obtain IP address via DHCP' (unselected) and 'Set IP address manually' (selected), and text input fields for 'IP address' (192.168.1.77), 'Subnet mask' (255.255.255.0), 'Default router' (192.168.1.254), and 'DNS'. Blue 'Previous' and 'Next' buttons are at the bottom.

Figure 2-1: Change default password

Step 2: Set IP address

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

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

Click the **Next** button.

The figure shows two screenshots of the Lantronix web interface for the 'Set IP address' step. The left screenshot shows the 'Set IP address' screen with 'Set IP address manually' selected. The right screenshot shows the same screen but with 'Obtain IP address via DHCP' selected. Both screenshots have the same progress bar and input fields as described in Figure 2-1.

Figure 2-2a: Set IP address

Figure 2-2b: Set IP address

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

Step 3: Set date and time

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

Figure 2-3: Set date and time

Step 4: Set system information

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

LANTRONIX®

1 2 3 4
PASSWORD IP ADDRESS DATE & TIME INFORMATION

Set system information

System contact

System name

System location

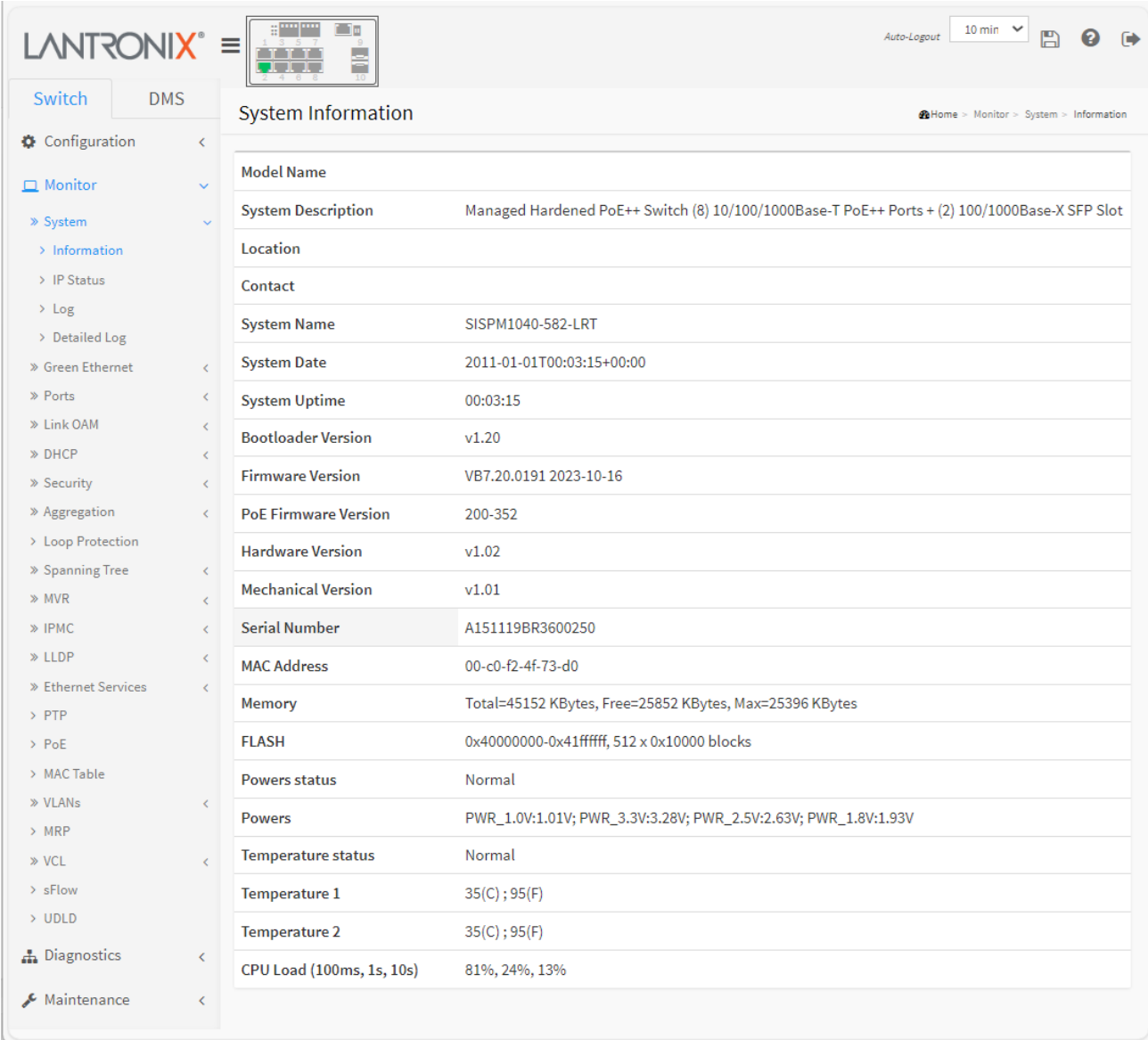
Figure 2-4: Set system information

Message: Password format error.

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

2.3 Startup Page

When logged in successfully, the startup page (Monitor > System > Information) displays as shown below. From here you can navigate to any webpage for any available function.



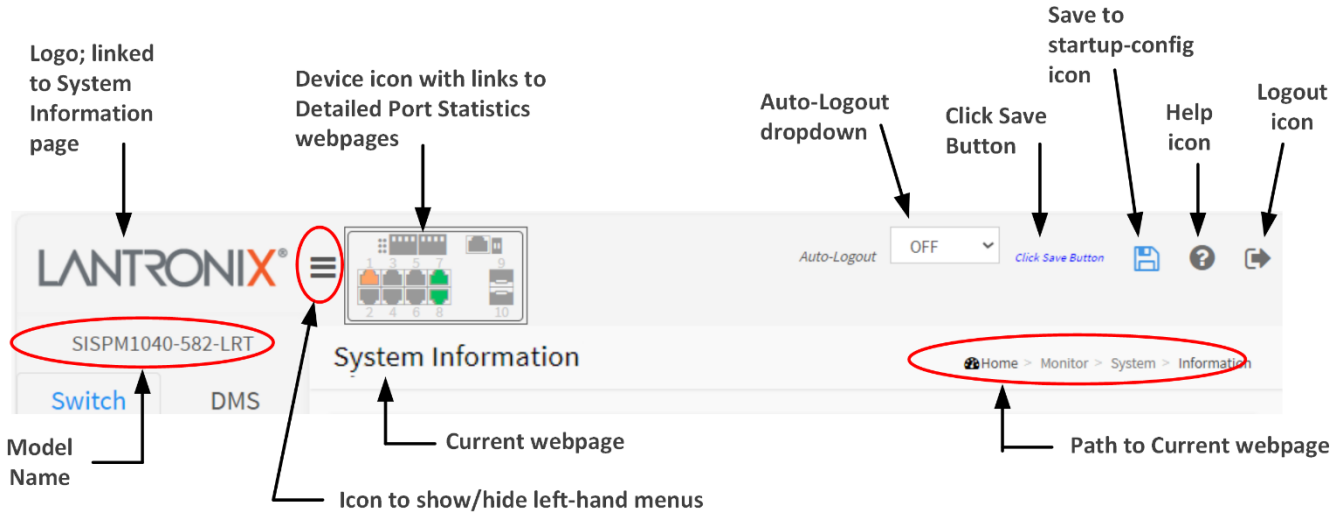
The screenshot shows the Lantronix web interface. The top navigation bar includes the Lantronix logo, a menu icon, and an Auto-Logout timer set to 10 minutes. The left sidebar contains a navigation menu with categories like Configuration, Monitor, Diagnostics, and Maintenance. The main content area is titled "System Information" and displays a table of system details.

Model Name	
System Description	Managed Hardened PoE++ Switch (8) 10/100/1000Base-T PoE++ Ports + (2) 100/1000Base-X SFP Slot
Location	
Contact	
System Name	SISPM1040-582-LRT
System Date	2011-01-01T00:03:15+00:00
System Uptime	00:03:15
Bootloader Version	v1.20
Firmware Version	VB7.20.0191 2023-10-16
PoE Firmware Version	200-352
Hardware Version	v1.02
Mechanical Version	v1.01
Serial Number	A151119BR3600250
MAC Address	00-c0-f2-4f-73-d0
Memory	Total=45152 KBytes, Free=25852 KBytes, Max=25396 KBytes
FLASH	0x40000000-0x41ffffff, 512 x 0x10000 blocks
Powers status	Normal
Powers	PWR_1.0V:1.01V; PWR_3.3V:3.28V; PWR_2.5V:2.63V; PWR_1.8V:1.93V
Temperature status	Normal
Temperature 1	35(C) ; 95(F)
Temperature 2	35(C) ; 95(F)
CPU Load (100ms, 1s, 10s)	81%, 24%, 13%

Figure 2.2: Monitor > System > Information page

2.4 Webpage Controls


The Web UI navigation controls are shown below.



Save to startup-config: Click to save changes on the web page. Click ‘Yes’ at the confirmation prompt “Are you sure you want to save running configuration to startup-config?”. Do not reset or power off the switch until the save completes.

Click Save Button: displays when a Save to startup-config can be performed. At the “Are you sure ...” prompt click the OK button. The Click Save Button then disappears until you make another webpage change.

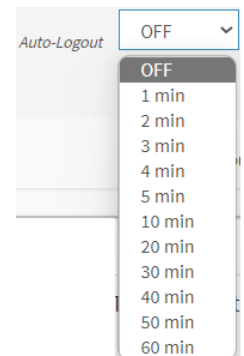


 : Logout icon : Click to log out of the switch UI.

Auto-Logout: dropdown lets you set the amount of time after a successful login before an automatic log out occurs. The selections are OFF, 1, 2, 3, 4, 5, 10 (default), 20, 30, 40, and 60 minutes (added at FW v7.10.2667).
If set to OFF, the web UI will not automatically log out at all.

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

When the Auto-Logout timeout setting is changed, it writes directly to running-config. To save the timeout change to start-up config, you must execute a save to startup-config. To examine the running-config, run the CLI command “showing running-config” or in the Web UI just log out and log back in again. To save the timeout change into startup-config, you must do a save to startup-config and then reboot the switch.



Auto-Logout summary:

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

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

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

2.5 Webpage Messages

Message: *Wrong username or password!*

Recovery: Re-try the login with the correct username and password credentials.

Message: *There are too many users in the system.*

Recovery: Try to log in later.

Message: *Update success!*

Recovery: None; if the entries are valid, this webpage message displays.

3 System Configuration

This chapter describes basic configuration tasks including System Configuration, IP, Time, IP, Syslog and NTP.

3.1 System

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

3.1.1 Information

The switch system's contact information is provided here. To set System Information in the web UI:

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

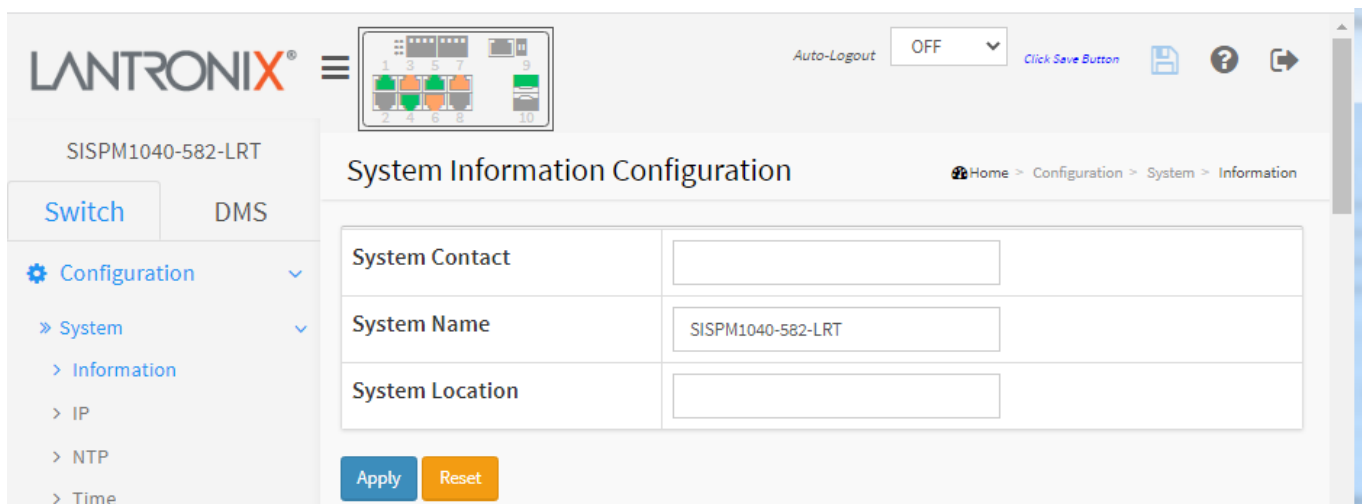


Figure 3.1.1: System Information Configuration

Parameter descriptions:

System Contact : The textual identification of the contact person for this managed node, together with information on how to contact this person. The allowed string length is 0-128 characters, and the allowed content is ASCII characters 32-126.

System name : An administratively assigned name for this managed node. By convention, this is the node's fully-qualified domain name. A domain name is a text string drawn from the alphabet (A-Za-z), digits (0-9), minus sign (-). The allowed string length is 0-255 characters.

System Location : The physical location of this node (e.g., telephone closet, 3rd floor). The allowed string length is 0 to 128 characters, and the allowed content is ASCII characters 32-126.

Buttons

Apply : Click to save changes.

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

3.1.2 IP

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

Configure switch-managed IP information on this page (e.g., IP basic settings, control IP interfaces and IP routes). The maximum number of interfaces supported is 8 and the maximum number of routes is 32.

Web Interface

To configure IP parameters in the web UI:

1. Click Configuration, System, and IP.
2. Click Add Interface to create a new Interface on the switch.
3. Click Add Route to create new Route on the switch.
4. Click Apply.

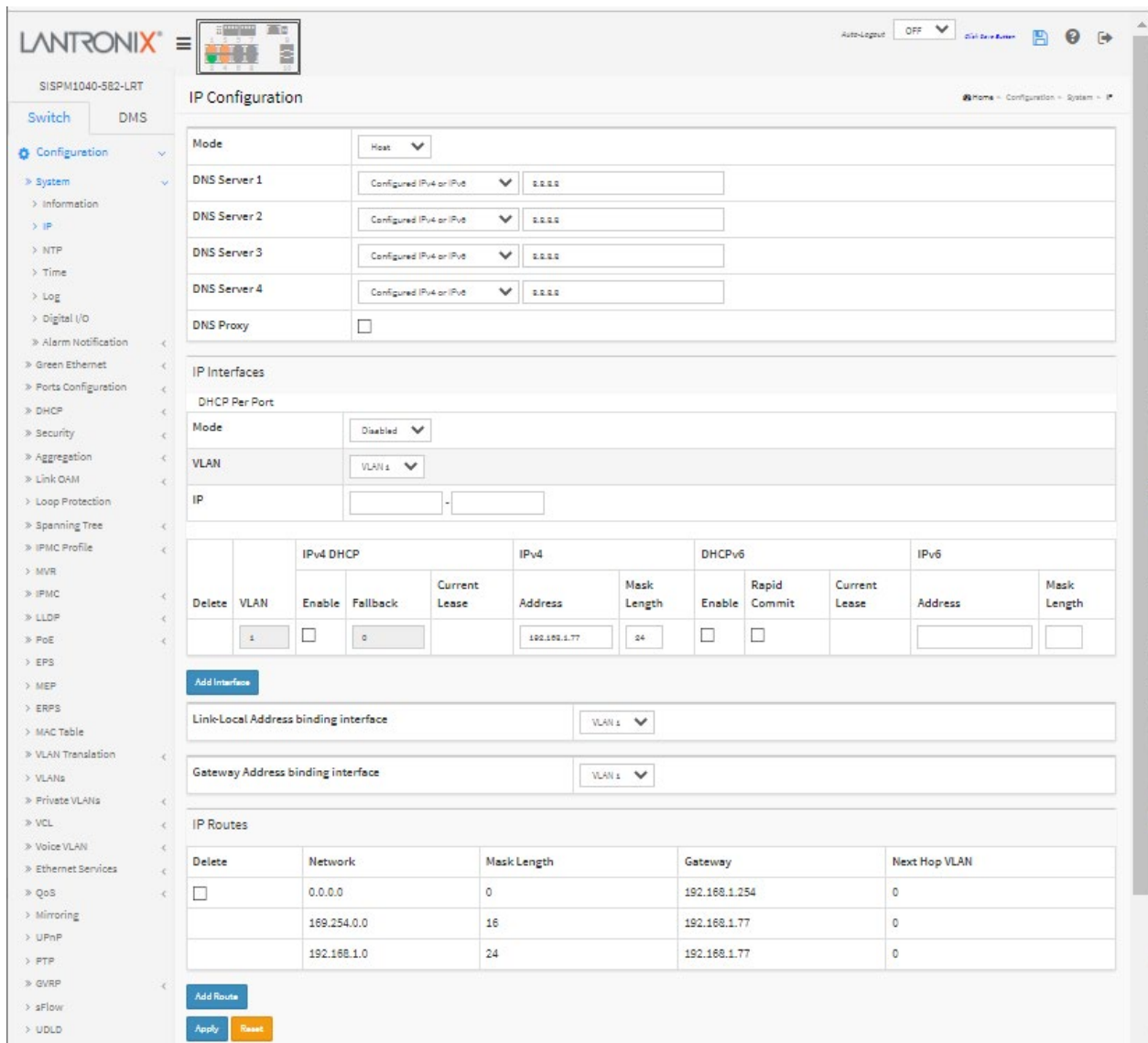


Figure 3.1.2: IP Configuration

Parameter descriptions:**IP Configuration section**

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

DNS Server : This setting controls the DNS name resolution done by the switch. There are four servers available for configuration, and the index of the server presents the preference (less index has higher priority) in doing DNS name resolution. The system selects the active DNS server from configuration in turn if the preferred server does not respond in five attempts. The following modes are supported:

- From any DHCP interfaces : The first DNS server offered from a DHCPv4 lease to a DHCPv4-enabled interface will be used.
- **No DNS server** : No DNS server will be used.
- **Configured IPv4** : Explicitly provide the valid IPv4 unicast address of the DNS Server in dotted decimal notation. Make sure the configured DNS server could be reachable (e.g., via PING) for activating DNS service.
- **From this DHCPv4 interface** : Specify from which DHCPv4-enabled interface a provided DNS server should be preferred.
- **Configured IPv6** : Explicitly provide the valid IPv6 unicast (except linklocal) address of the DNS Server. Make sure the configured DNS server could be reachable (e.g., via PING6) for activating DNS service.
- **From this DHCPv6 interface** : Specify from which DHCPv6-enabled interface a provided DNS server should be preferred.
- **From any DHCPv6 interfaces** : The first DNS server offered from a DHCPv6 lease to a DHCPv6-enabled interface will be used.

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

IP Interfaces section

DHCP Per Port Mode : Enable/Disable DHCP per port. See [Appendix A. DHCP Per Port](#) on page 476.

DHCP Per Port VLAN : Set DHCP per port VLAN (the VLAN associated with the IP interface). Only ports in this VLAN will be able to access the IP interface. This field is only available for input when creating a new interface.

DHCP Per Port IP : Define the IP range for DHCP per port.

DHCP IP per port lets you have an IP address from a DHCP pool on a switch to be statically assigned to a switchport, such that whichever device plugs into the switchport it will always be assigned that specific IP address. The IP address would be 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 technique used on most switches.

Added at FW vB.7.20.0104.

IPv4 DHCP Enabled : Enable the DHCPv4 client by checking this box. If this option is enabled, the system will configure the IPv4 address and mask of the interface using the DHCPv4 protocol. The DHCPv4 client will announce the configured System Name as hostname to provide DNS lookup.

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

The screenshot shows a configuration interface for IP Interfaces. It includes a section for DHCP Per Port with the following fields:

IP Interfaces	
DHCP Per Port	
Mode	Disabled ▼
VLAN	VLAN 1 ▼
IP	<input type="text"/> - <input type="text"/>

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

IPv4 Address : The IPv4 address of the interface in dotted decimal notation.

If DHCP is enabled, this field configures the fallback address. The field may be left blank if IPv4 operation on the interface is not desired - or no DHCP fallback address is desired.

IPv4 Mask : The IPv4 network mask, in number of bits (prefix length). Valid values are between 0 and 30 bits for an IPv4 address. If DHCP is enabled, this field 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.

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. The System accepts the valid IPv6 unicast address only, except IPv4-Compatible address and IPv4-Mapped address.

The field may be left blank if IPv6 operation on the interface is not desired.

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

Link-Local Address binding interface : 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.

Link-Local Address binding interface	VLAN 1 ▾
Gateway Address binding interface	VLAN 1 ▾

Gateway Address binding interface: DHCP client uses the DHCP protocol to get the gateway address and sets the gateway address to the interface of the binding. See the DHCP Option 3 example below.

IP Routes section

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

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

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

Next Hop VLAN (Only for IPv6) : The VLAN ID (VID) of the specific IPv6 interface associated with the gateway. The given VID ranges from 1 to 4095 and will be effective only when the corresponding IPv6 interface is valid.

If the IPv6 gateway address is is link-local, it must specify the next hop VLAN for the gateway.

If the IPv6 gateway address is not link-local, system ignores the next hop VLAN for the gateway.

Buttons

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

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

Add Interface : Click to add a new IP interface. A maximum of 8 interfaces is supported.

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

Apply : Click to save changes.

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

Message: *Subnet of VLAN 2 overlaps VLAN 1*

Message: *'Address mask length' must be an integer value between 1 and 30.*

Message: *IP address must not be a broadcast address*

Message: *ipv4 – 1.2.3.4 – Address conflict*

Message: *DHCP Per Port range (192.168.1.1 - 192.168.1.8) is not within interface subnet (192.1.2.3.4/24)*

Message: *DHCP Per Port IP range (192.168.1.1 - 192.168.1.9) is not equal to switch TP port number (8)*

Message: *DHCP Per Port IP range (192.168.1.1 - 192.168.1.) includes interface IP address (192.168.1.77)*

Message: *Invalid route - address bits outside mask: 1.2.3.4*

Message: *The value of 'Interface IP address' must be a valid IP address in dotted decimal notation ('z.y.z.w').*

The following restrictions apply:

- 1) z, y, z, and w must be decimal numbers between 0 and 255,
- 2) x must not be 0,
- 3) x must not be 127, and
- 4) x must not be greater than 223.

Example: IP configuration page with Link-Local Address binding interface VLAN and Gateway Address binding interface vlan configured:

The screenshot displays the IP Configuration page for the SISPM1040-582-LRT device. The left sidebar shows a navigation menu with 'Switch' and 'DMS' tabs, and a 'Configuration' section expanded to show various system settings. The main content area is titled 'IP Configuration' and includes the following sections:

- DNS Servers:** Four DNS Server entries (1-4) with 'Configured IPv4 or IPv6' dropdowns and '8.8.8.8' IP addresses. A 'DNS Proxy' checkbox is present.
- IP Interfaces:** A section for DHCP Per Port settings with 'Mode' set to 'Enabled' and 'IP' set to '192.168.1.1 - 192.168.1.8'. Below this is a table of IP Interfaces.
- IP Interfaces Table:**

Delete	VLAN	IPv4 DHCP			IPv4		DHCPv6		IPv6		
		Enable	Fallback	Current Lease	Address	Mask Length	Enable	Rapid Commit	Current Lease	Address	Mask Length
<input type="checkbox"/>	1	<input type="checkbox"/>	0		192.168.1.77	24	<input type="checkbox"/>	<input type="checkbox"/>			
<input type="checkbox"/>	10	<input type="checkbox"/>	0		1.1.1.4	24	<input type="checkbox"/>	<input type="checkbox"/>			

Below the table is an 'Add Interface' button. The configuration for the new interface shows:

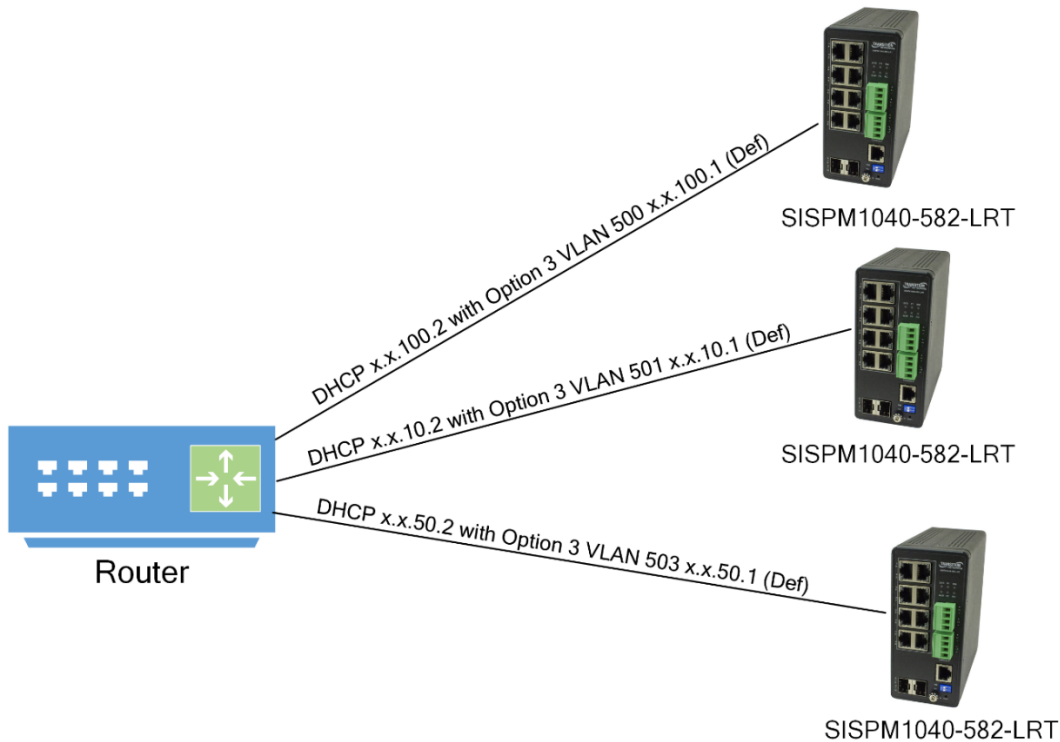
- Link-Local Address binding interface:** A dropdown menu with 'VLAN 10' selected.
- Gateway Address binding interface:** A dropdown menu with 'VLAN 10' selected.

The bottom section is titled 'IP Routes' and contains a table:

Delete	Network	Mask Length	Gateway	Next Hop VLAN
<input type="checkbox"/>	0.0.0.0	0	192.168.1.154	0
<input type="checkbox"/>	192.168.1.0	24	192.168.1.77	0

At the bottom of the page, there are 'Add Route', 'Apply', and 'Reset' buttons.

Example: DHCP Option 3: one VLAN interface gateway for the default route:



Example: DHCP Option 3 functionality on VLANs other than VLAN 1:

1. With a switch set to the factory defaults, log in and add the following IP interfaces:
 - a. VLAN 2, IPv4 DHCP enabled
 - b. VLAN 3, IPv4 DHCP enabled
2. On the Configure VLAN page, assign a Port VLAN of 2 to at least one port. Assign a Port VLAN of 3 to at least one port.
3. Delete VLAN 1 and perform a configuration save.
4. Attach a cable from a DHCP server to a VLAN 2 port.
5. Perform a switch reset and verify that a DHCP address has been obtained on VLAN 2.
6. Move the cable to a VLAN 3 port.
7. Perform a switch reset and verify that a DHCP address has been obtained on VLAN 3.
8. Repeat steps 4 – 7 resetting the switch via power cycle.

3.1.3 NTP

NTP (Network Time Protocol) is used to sync the network time based Greenwich Mean Time (GMT). If you use NTP mode and select a built-in NTP time server or manually specify an NTP server and Time Zone, the switch will sync the time a short while after you click the Apply button. Though it synchronizes the time automatically, NTP does not update the time periodically without additional processing.

Time Zone is an offset time off GMT. You must select the time zone first and then perform time sync via NTP since the switch will combine this time zone offset and updated NTP time to come out as the local time; otherwise, you will not be able to get the correct time. The switch supports a configurable time zone from -12 to +13 in 1 hour steps. The default Time zone is +8 Hrs.

Web Interface

To configure NTP in the web UI:

1. Click Configuration, System, and NTP.
2. Specify the Time parameter in manual parameters.
3. Click Apply.

The screenshot shows the Lantronix web interface for the SISPM1040-582-LRT switch. The page title is "NTP Configuration". The breadcrumb trail is "Home > Configuration > System > NTP". The left navigation menu is expanded to "Configuration" > "System" > "NTP". The main configuration area contains the following fields:

Automatic	Enabled
Server address via DHCP	
NTP Time-Sync Interval	60
Server 1	129.6.15.28
Server 2	www.ntp.org
Server 3	129.6.15.29
Server 4	
Server 5	

At the bottom of the configuration area are "Apply" and "Reset" buttons.

Figure 3.1.3: NTP Configuration

Parameter descriptions:

Automatic : Sets the automatic mode of operation. Possible modes are:

Enabled: Enable NTP client mode operation.

Disabled: Disable NTP client mode operation (default).

Server address via DHCP: Specify a list of IP addresses indicating NTP servers available to the client.

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

Server 1 to 5 : Provide the IPv4 or IPv6 address of a NTP server. 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'. In addition, it can also accept a domain name address.

Buttons

Apply : Click to save changes.

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

Message:

The input value 'Server 2 Address' (::) is not a valid IPv6 address.

The Unspecified Address must never be assigned to any node.

Message:

The value of 'Server 2 Address' (:: ::) must be a valid IPv6 address.

The symbol '::' can appear once.

Message:

The value of 'Server 2 Address' (::) must be a valid IPv6 address in 128-bit record represented as

eight fields of up to four hexadecimal digits with a colon (:) separating each field.

Message:

The format of 'Server 3 Address' is invalid.

It must either be a valid IP address in dotted decimal notation ('x.y.z.w') or a valid hostname.

A valid hostname is a string drawn from the alphabet (A-Za-z), digits (0-9), dot (.), hyphen (-).

Spaces are not allowed, the first character must be an alphanumeric character, and the first and last characters must not be a dot or hyphen.

3.1.4 Time

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

To configure Time in the web UI:

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

The screenshot displays the 'Time Configuration' web interface for a Lantronix switch. The interface is organized into several sections:

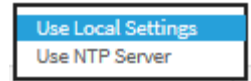
- Time Configuration:**
 - Clock Source:** A dropdown menu set to 'Use Local Settings'.
 - System Date:** A text input field containing '2023-09-06 12:19:40' with a format hint '(yyyy-mm-dd hh:mm:ss)'.
- Time Zone Configuration:**
 - Time Zone:** A dropdown menu set to 'None'.
 - Acronym:** An empty text input field with a hint '(0 - 16 characters)'.
- Daylight Saving Time Configuration:**
 - Daylight Saving Time:** A dropdown menu set to 'Disabled'.
- Start Time settings:**
 - Month:** A dropdown menu set to 'Jan'.
 - Date:** A dropdown menu set to '1'.
 - Year:** A dropdown menu set to '2014'.
 - Hours:** A dropdown menu set to '0'.
 - Minutes:** A dropdown menu set to '0'.
- End Time settings:**
 - Month:** A dropdown menu set to 'Jan'.
 - Date:** A dropdown menu set to '1'.
 - Year:** A dropdown menu set to '2097'.
 - Hours:** A dropdown menu set to '0'.
 - Minutes:** A dropdown menu set to '0'.
- Offset settings:**
 - Offset:** A text input field containing '1' with a hint '(1 - 1440) Minutes'.

At the bottom of the configuration area, there are two buttons: 'Apply' (blue) and 'Reset' (orange).

Figure 3.1.4: Time Configuration

Parameter descriptions:**Time Configuration section**

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

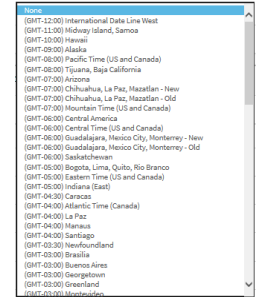


System Date : Show the current time of the system. The year of system date limits are 2011 - 2037.

Time Zone Configuration section

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

Acronym : You can set the acronym of the time zone. This is a user-configurable acronym to identify the time zone (range: up to 16 characters).

**Daylight Saving Time Configuration section**

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

Recurring Configuration section**Start time settings :**

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

End time settings :

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

Offset settings :

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

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

Buttons

Apply : Click to save changes.

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

3.1.5 Log

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 as a generalized informational, analysis and debugging messages. Syslog is supported by a wide variety of devices and receivers across multiple platforms.

To configure system log parameters in the web UI:

1. Click Configuration, System and log.
2. At the Server Mode dropdown select Enabled.
3. Specify the IP Address of the Syslog server and Port number.
4. Click Apply.

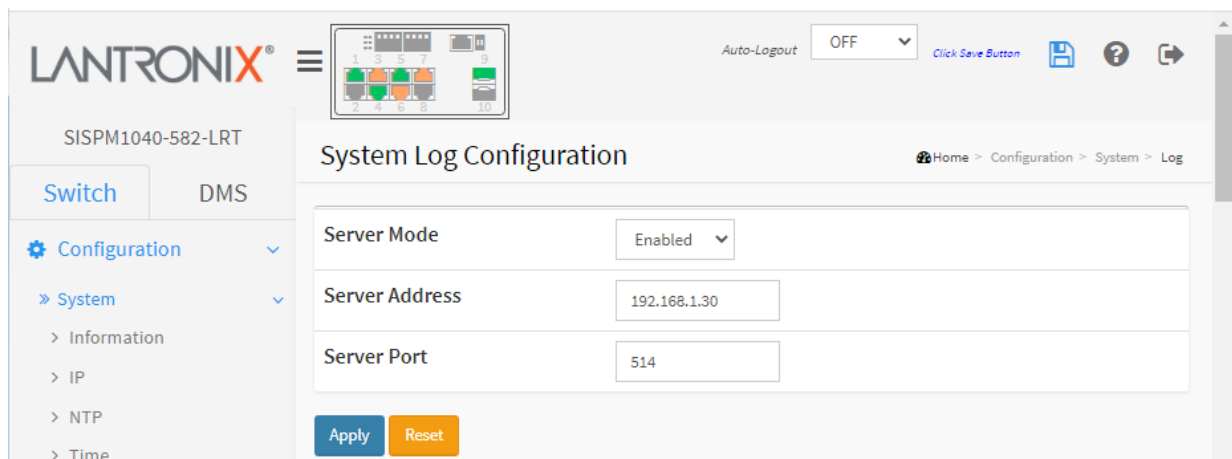


Figure 3.1.5: System Log Configuration

Parameter descriptions:

Server Mode: Select the server mode operation. When the mode operation is enabled, the syslog message will send out to syslog server. The syslog protocol is based on UDP communication and received on UDP port 514 and the syslog server will not send acknowledgments back sender since UDP is a connectionless protocol and it does not provide acknowledgments. The syslog packet is always sent out even if the syslog server does not exist. Possible modes are:

Enabled: Enable server mode operation.

Disabled: Disable server mode operation.

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

Buttons

Apply: Click to save changes.

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

3.1.6 Digital I/O

Configure the normal modes of digital input/output (DI/DO). See the *Install Guide* for DI/DO hardware configuration. To configure Digital I/O parameters in the web UI:

1. Click Configuration, System and Digital I/O.
2. Specify the Digital I/O Normal Mode and Reboot System setting.
3. Specify the DI Event Description and DO section parameters.
4. Click Apply.

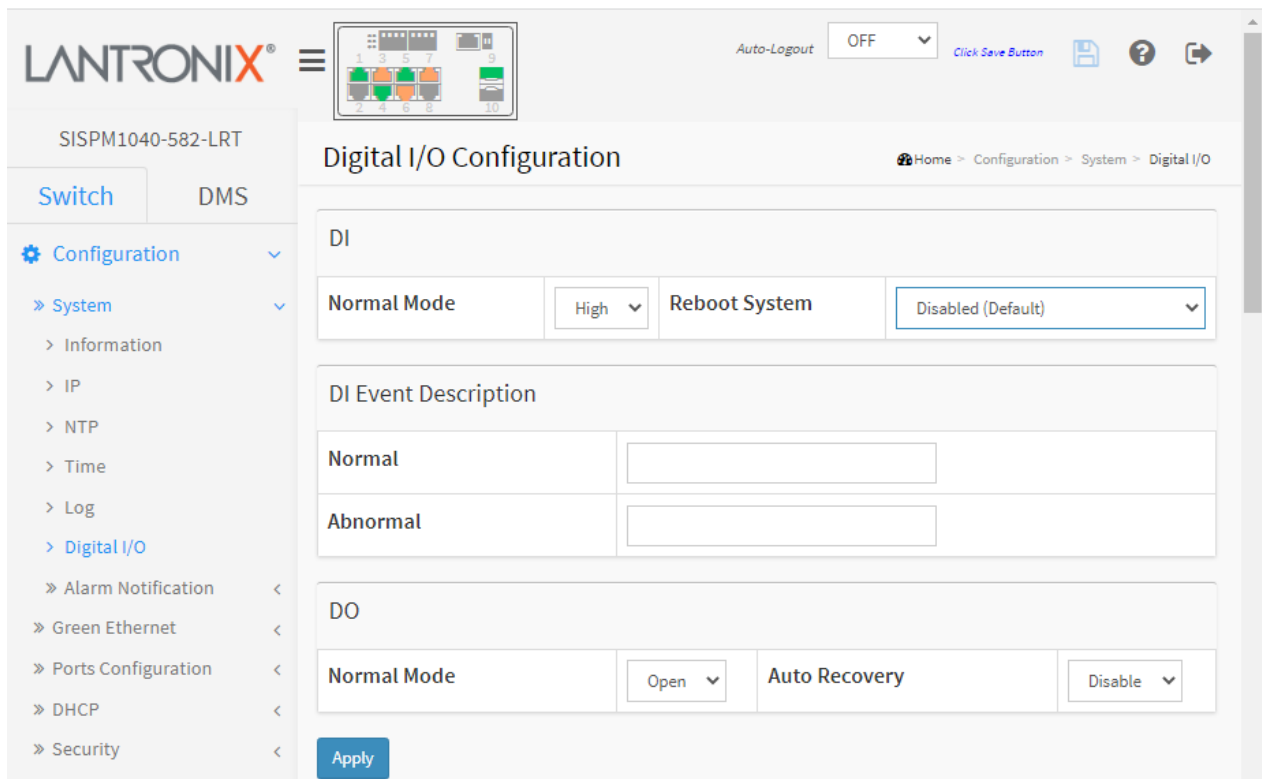


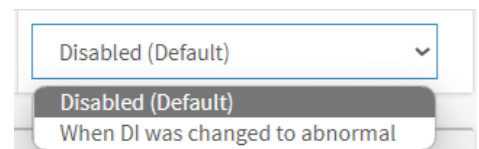
Figure 3.1.6: Digital I/O Configuration

Parameter descriptions:

DI

Normal Mode: Set the normal mode of the digital input(DI). You can set it to High or Low.

Reboot System: Set the reboot system of the digital input(DI). The default setting is Disabled (no reboot system action taken). You can set it to “When DI was changed to abnormal” to reboot the switch when DI input goes High. Added at FW v 7.20.0064/69/74.



DI Event Description

Normal: Customize event message. You can describe the event in detail.

Abnormal: Customize event message. You can describe the event in detail.

DO

Normal Mode : Set the normal mode of the digital output (DO). You can set it to Open or Close.

Auto Recovery: Enable the function of Automatic Recovery; Digital Output will automatically go back to Normal mode when Digital Input changes back to Normal mode.

Buttons

Apply : Click to save changes.

DI/DO System Log Messages:

Do Relay Status Do Relay Alarm Cut-off Apply

Do Relay Status : shows the status of digital-out relay contact.

Do Relay Alarm Cut-off: force cut off the digital-out relay contact.

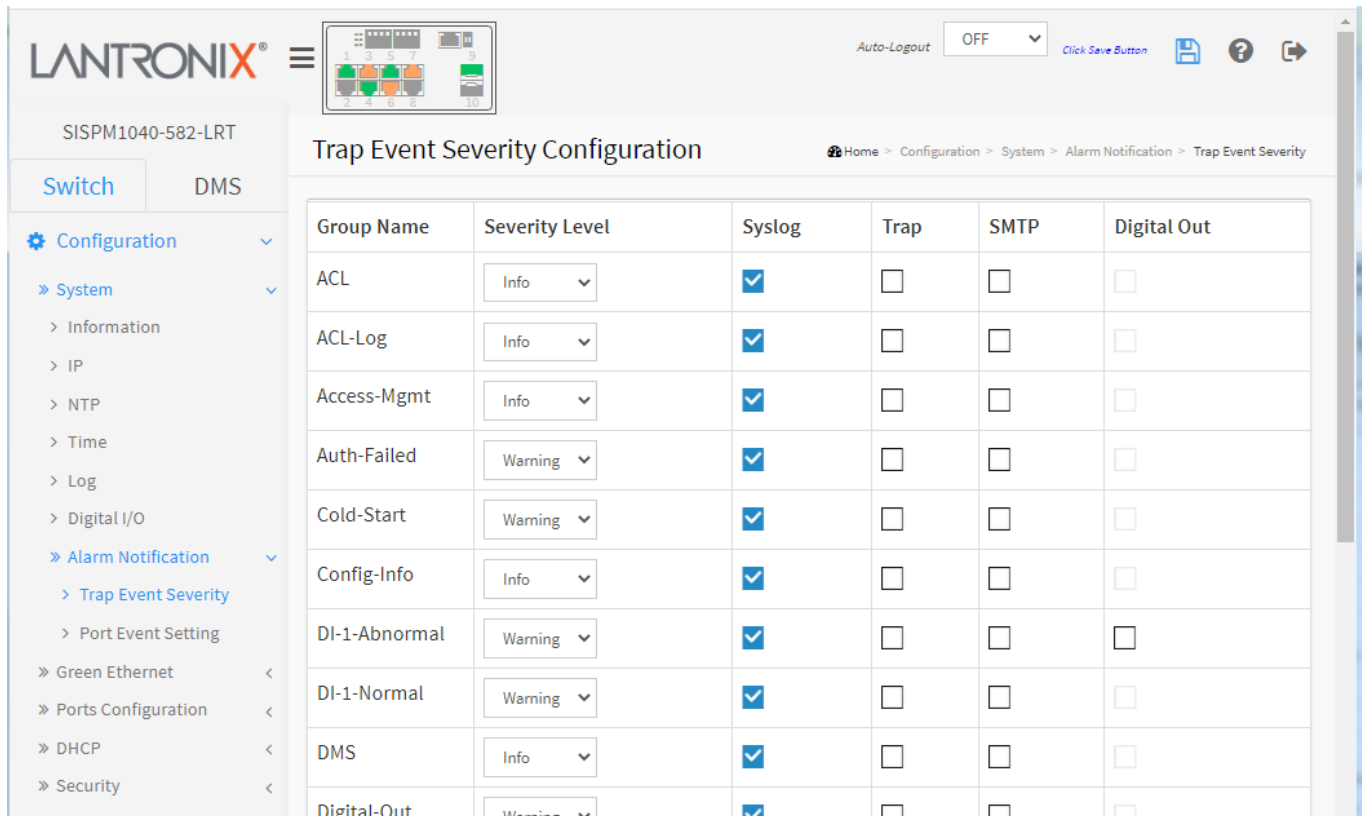
18	Warning	2021-03-26T03:00:16+00:00	DO change to abnormal
19	Warning	2021-03-26T03:00:19+00:00	DI 1 change to abnormal
20	Warning	2021-03-26T03:00:27+00:00	DO change to normal
21	Warning	2021-03-26T03:00:19+00:00	DI 1 change to normal

3.1.7 Alarm Notification

3.1.7.1 Trap Event Severity

This page lets you view and configure current trap event severity parameters. To configure Trap Event Severity in the web UI:

1. Click Configuration, System, Alarm Notification and Trap Event Severity.
2. For each Group Name, select a Severity Level, Syslog, Trap, SMTP, and Digital Out setting.
3. Click Apply.



Group Name	Severity Level	Syslog	Trap	SMTP	Digital Out
ACL	Info	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
ACL-Log	Info	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Access-Mgmt	Info	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Auth-Failed	Warning	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Cold-Start	Warning	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Config-Info	Info	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
DI-1-Abnormal	Warning	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
DI-1-Normal	Warning	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
DMS	Info	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Digital-Out	Warning	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Figure 3.1.7.1: Trap Event Severity Configuration

Parameter descriptions:

Group Name : The name identifying the severity group.

Severity Level : Every group has a severity level. The following level types are supported:

- <0> Emergency: System is unusable.
- <1> Alert: Action must be taken immediately.
- <2> Critical: Critical conditions.
- <3> Error: Error conditions.
- <4> Warning: Warning conditions.
- <5> Notice: Normal but significant conditions.
- <6> Information: Information messages.
- <7> Debug: Debug-level messages.

Syslog : Enable - Select this Group Name in Syslog.

Trap : Enable - Select this Group Name in Trap.

SMTP : Enable - Select this Group Name in SMTP.

Digital Out : Check to enable; select this Group Name in Digital Out.

Buttons

Apply : Click to save changes.

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

Group Names:

ACL	Logout	PoE-PD-On
ACL-Log	Loop-Protect	PoE-PD-Over-Current
Access-Mgmt	MRP-Event	Poe-Auto-Power-Reset
Auth-Failed	Mgmt-IP-Change	Port-Security
Cold-Start	Module-Change	Rapid-Chain-Break
Config-Info	NAS	Rapid-Ring-Break
DI-1-Abnormal	Over-Max-PoE-Power-	Rapid-Ring-Error
DI-1-Normal	Limitation	SCP-Fail
DMS	PWR-1-Off-On	SCP-Success
Digital-Out	PWR-1-On-Off	Spanning-Tree
Firmware-Upgrade	PWR-2-Off-On	Temperature
Import-Export	PWR-2-On-Off	Voltage
LACP	Password-Change	Warm-Start
Login	PoE-PD-Off	

3.1.7.2 Port Event Setting

This page is for configuring port events. To configure Port Events in the web UI:

1. Click Configuration, System, Alarm Notification and Port Event Setting.
2. Specify the Link, Traffic and Action parameters.
3. Click Apply.

Active	Port	Link		Traffic			Action				
		On	Off	Overload	Rx-Threshold (0-100%)	Traffic Duration (1-60s)	Syslog	Trap	SMTP	Digital Out	Severity
<input checked="" type="checkbox"/>		<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	0	1	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<
<input checked="" type="checkbox"/>	1	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	0	1	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Warning
<input checked="" type="checkbox"/>	2	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	0	1	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Warning
<input checked="" type="checkbox"/>	3	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	0	1	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Warning
<input checked="" type="checkbox"/>	4	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	0	1	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Warning
<input checked="" type="checkbox"/>	5	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	0	1	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Warning
<input checked="" type="checkbox"/>	6	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	0	1	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Warning
<input checked="" type="checkbox"/>	7	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	0	1	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Warning
<input checked="" type="checkbox"/>	8	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	0	1	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Warning
<input checked="" type="checkbox"/>	9	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	0	1	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Warning
<input checked="" type="checkbox"/>	10	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	0	1	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Warning

Figure 3.7.1.2: Port Event Setting

Parameter descriptions:

Active : To active the event handler of this port.

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

Link On : Event is triggered when link on.

Link Off : Event is triggered when link off.

Traffic Overload : Event is triggered when the traffic is overload.

Traffic Rx-Threshold (0-100%): Event is triggered when Rx reach this threshold.

Traffic Duration (1-60s): Event is triggered when the traffic duration reaches this value.

Action Syslog : Enable this port for Syslog.

Action Trap : Enable this port for Trap.

Action SMTP : Enable this port for SMTP.

Action Digital Out : Enable this port for Digital Out.

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.

Buttons

Apply : Click to save changes.

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

3-2 Green Ethernet

3.2.1 Port Power Savings

This page lets you configure the port power savings features. EEE is a power saving option that reduces the power usage when there is low or no traffic utilization. EEE works by powering down circuits when there is no traffic. When a port gets data to be transmitted all circuits are powered up. The time it takes to power up the circuits is named wakeup time. The default wakeup time is 17 us for 1Gbit links and 30 us for other link speeds. EEE devices must agree upon the value of the wakeup time to make sure that both the receiving and transmitting device has all circuits powered up when traffic is transmitted. The devices can exchange wakeup time information using the LLDP protocol.

EEE works for ports in auto-negotiation mode, where the port is negotiated to either 1G 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 is some overhead in turning the port down and up, more power can be saved if the traffic can be buffered until a large burst of traffic can be transmitted. Buffering traffic will give some latency in the traffic.

Web Interface

To configure a Port Power Saving Configuration in the web UI:

1. Click Configuration, Green Ethernet and Port Power Savings
2. Enable or disable the ActiPHY, PerfectReach, EEE, and EEE Urgent Queues.
3. Click Apply.

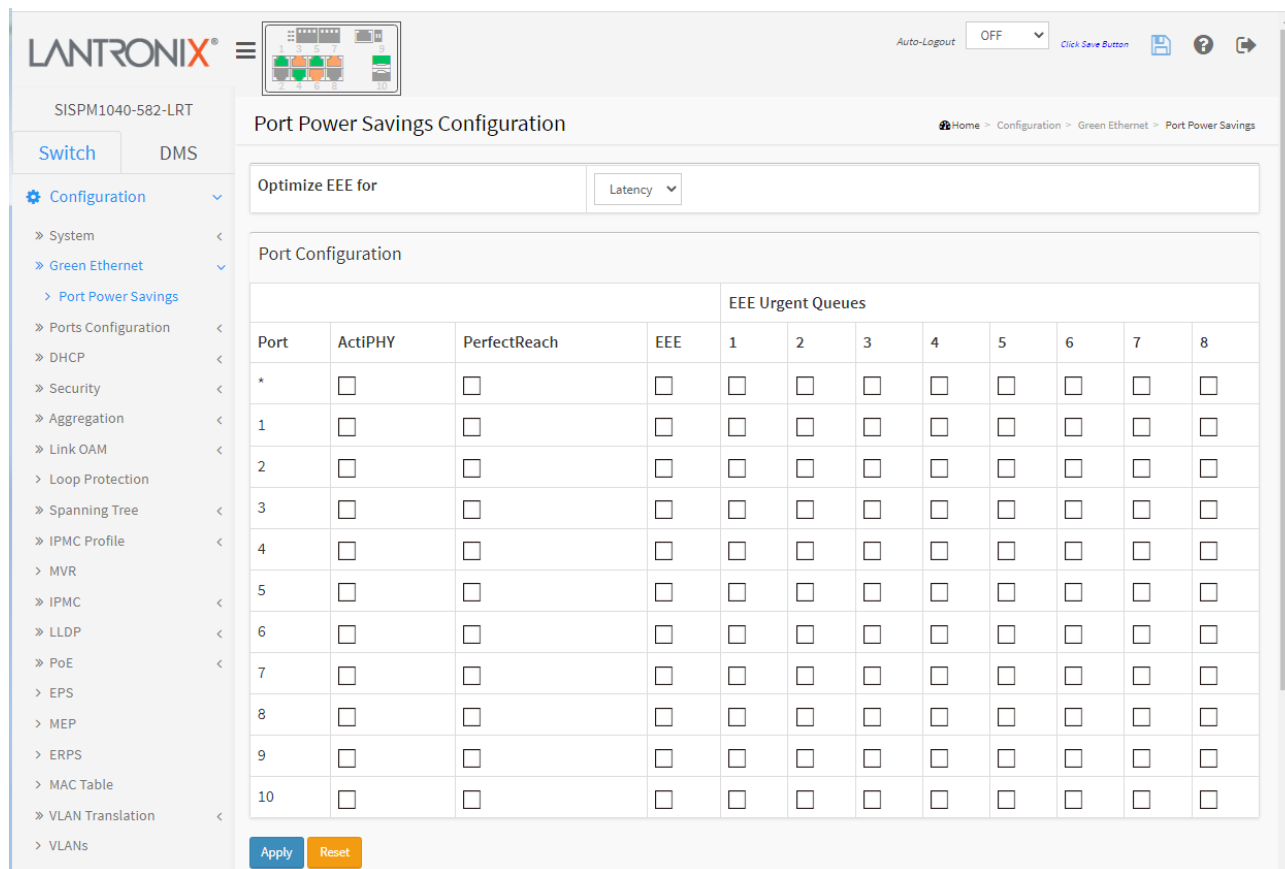


Figure 3.2.1: Port Power Savings Configuration

Parameter descriptions:

Optimize EEE for : The switch can be set to optimize EEE for either best power saving or least traffic latency.

Port : The switch port number of the logical port.

ActiPHY : Link down power savings enabled. ActiPHY works by lowering the power for a port when there is no link. The port is power up for short moment in order to determine if cable is inserted.

PerfectReach : Cable length power savings enabled. PerfectReach works by determining the cable length and lowering the power for ports with short cables.

EEE : Controls whether EEE is enabled for this switch port. For maximizing power savings, the circuit isn't started at once transmit data is ready for a port but is instead queued until a burst of data is ready to be transmitted. This will give some traffic latency.

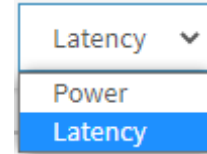
If desired it is possible to minimize the latency for specific frames, by mapping the frames to a specific queue (done with QOS), and then mark the queue as an urgent queue. When an urgent queue gets data to be transmitted, the circuits will be powered up at once and the latency will be reduced to the wakeup time.

EEE Urgent Queues : Queues set will activate transmission of frames as soon as data is available. Otherwise the queue will postpone transmission until a burst of frames can be transmitted.

Buttons

Apply : Click to save changes.

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



3-3 Ports Configuration

3.3.1 Ports

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

1. Click Configuration, Ports Configuration and Ports.
2. Specify Speed Configured, Duplex, Flow Control, Maximum Frame Size, Excessive Collision Mode and Frame Length Check parameters.
3. Click Apply.

Port	Link	Speed		Adv Duplex		Adv speed			Flow Control		Maximum Frame Size	Excessive Collision Mode	Frame Length Check	
		Current	Configured	Fdx	Hdx	10M	100M	1G	Enable	Current Rx				Current Tx
*			<input type="text" value=""/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>			9600	<input type="text" value=""/>	<input type="checkbox"/>
1	●	1Gfdx	Auto	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	9600	Restart	<input type="checkbox"/>
2	●	Down	Auto	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	9600	Restart	<input type="checkbox"/>
3	●	100fdx	Auto	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	9600	Discard	<input checked="" type="checkbox"/>
4	●	1Gfdx	Auto	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	9600	Discard	<input checked="" type="checkbox"/>
5	●	1Gfdx	Auto	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	9600	Restart	<input checked="" type="checkbox"/>
6	●	100fdx	Auto	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	9600	Discard	<input checked="" type="checkbox"/>
7	●	100fdx	Auto	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	9600	Discard	<input type="checkbox"/>

Figure 3.3.1: Ports Configuration

Parameter descriptions:

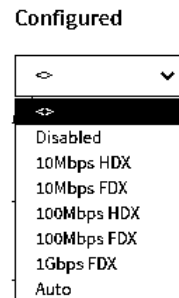
Port : This is the logical port number for this row.

Link : The current link state is displayed graphically. A green dot indicates the link is up, a red indicates the link is down, and an orange dot indicates the link is at 100fdx.

Current Link Speed : Provides the current link speed of the port (e.g., 1Gfdx, 100fdx, Down, 1Gfdx Fiber).

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

- Disabled** - Disables the switch port operation.
- Auto** - Port auto negotiating speed with the link partner and selects the highest speed that is compatible with the link partner.
- 10Mbps HDX** - Forces the cu port in 10Mbps half-duplex mode.
- 10Mbps FDX** - Forces the cu port in 10Mbps full duplex mode.
- 100Mbps HDX** - Forces the cu port in 100Mbps half-duplex mode.
- 100Mbps FDX** - Forces the cu port in 100Mbps full duplex mode.
- 1Gbps FDX** - Forces the port in 1Gbps full duplex



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

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

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

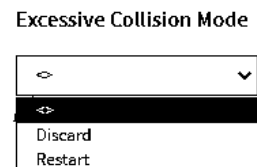


Note: The 100FX standard doesn't support Auto Negotiation, so when in 100FX mode the flow control capabilities will always be shown as "disabled".

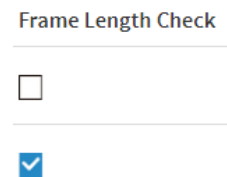
Maximum Frame Size : Enter the maximum frame size allowed for the switch port, including FCS. The range is 1518-9600 bytes.

Excessive Collision Mode : 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 dropped due to frame length mismatch.



Buttons

Apply : Click to save changes.

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

Refresh : Click to refresh the pages manually.

3.3.2 Ports Description

This page lets you set current port descriptions. To configure Port descriptions in the web UI:

1. Click Configuration, Port Configuration and Port Description.
2. Specify the detail Port alias or description an alphanumeric string describing the full name and version identification for the system's hardware type, software version, and networking application.
3. Click Apply.

The screenshot shows the Lantronix web interface for configuring port descriptions on a switch. The page title is "Port Description for Switch". The navigation menu on the left includes "Configuration", "System", "Green Ethernet", "Ports Configuration", "Ports Description", "DHCP", "Security", "Aggregation", "Link OAM", "Loop Protection", "Spanning Tree", "IPMC Profile", "MVR", "IPMC", "LLDP", "PoE", and "EPS". The main content area contains a table with 10 rows, each representing a port from 1 to 10. Each row has a "Port" column and a "Description" column. Below the table are "Apply" and "Reset" buttons.

Port	Description
1	<input type="text"/>
2	<input type="text"/>
3	<input type="text"/>
4	<input type="text"/>
5	<input type="text"/>
6	<input type="text"/>
7	<input type="text"/>
8	<input type="text"/>
9	<input type="text"/>
10	<input type="text"/>

Figure 3.3.2: Port Description

Parameter descriptions:

Port : The logical port number for this row (1-10).

Description : Enter up to 47 characters to be descriptive name for identifies this port.

Buttons

Apply : Click to save changes.

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

3-4 DHCP

This section lets you configure switch DHCP Server, Snooping, and Relay parameters.

DHCP (Dynamic Host Configuration Protocol) is used for assigning dynamic IP addresses to devices on a network. DHCP used by networked computers (clients) to obtain IP addresses and other parameters such as the default gateway, subnet mask, and IP addresses of DNS servers from a DHCP server. The DHCP server ensures that all IP addresses are unique, for example, no IP address is assigned to a second client while the first client's assignment is valid (its lease has not expired). Therefore, IP address pool management is done by the server and not by a human network administrator.

Dynamic addressing simplifies network administration because the software keeps track of IP addresses rather than requiring an administrator to manage the task. This means that a new computer can be added to a network without the hassle of manually assigning it a unique IP address.

3.4.1 Server

3.4.1.1 Mode

This page configures DHCP global mode and VLAN mode to enable/disable DHCP server per system and per VLAN. A DHCP Server is used to allocate network addresses and deliver configuration parameters to dynamically configured hosts called DHCP clients. DHCP operates based on the client-server model. When a computer or other device connects to a network, the DHCP client software sends a DHCP broadcast query requesting the necessary information. Any DHCP server on the network may service the request. The DHCP server manages a pool of IP addresses and information about client configuration parameters such as default gateway, domain name, the name servers, and time servers.

Web Interface

To configure DHCP server mode in the web UI:

1. Click Configuration, DHCP, Server and Mode.
2. Select "Enabled" in the Global Mode of DHCP Server Mode Configuration.
3. Click Add VLAN Range and enter the VID Range.
5. Click Apply.

The screenshot displays the web interface for configuring DHCP Server Mode. The breadcrumb trail is: Home > Configuration > DHCP > Server > Mode. The main content area is titled 'DHCP Server Mode Configuration'. It features a table for 'VLAN Mode' configuration with the following structure:

Delete	VLAN Range	Mode
<input type="checkbox"/>	20 - 39	Enabled
<input type="button" value="Delete"/>	<input type="text"/> - <input type="text"/>	Enabled <input type="button" value="v"/>

Below the table, there is an 'Add VLAN Range' button. At the bottom of the configuration area, there are 'Apply' and 'Reset' buttons. The left sidebar shows the navigation menu with 'DHCP' expanded to 'Server' and 'Mode' selected.

Figure 3.4.1.1: DHCP Server Mode

Parameter descriptions:

VLAN Range : Enter the VLAN range in which DHCP server is enabled. The first VLAN ID must be smaller than or equal to the second VLAN ID. However, if the VLAN range contains only one VLAN ID, then you can just enter it into either the first and second VLAN ID or both. Otherwise, to disable existed VLAN range, follow these steps:

1. Click the ADD VLAN Range button to add a new VLAN range.
2. Enter the VLAN Range that you want to disable.
3. At the Mode dropdown select Disabled.
4. Click the Apply button to apply the change.

Then you will see the disabled VLAN range is removed from the DHCP Server mode configuration page.

Mode : Indicate the operation mode per VLAN. Possible modes are:

Enabled: Enable DHCP server per VLAN.

Disabled: Disable DHCP server per VLAN.

Buttons

Delete : Check the box and click the Apply button to immediately remove the VLAN Range from the table and system.

Add VLAN Range : Click to add a new VLAN range to the table.

Apply : Click to save changes.

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

Messages: *Low VLAN 50 can not be larger than high VLAN 2.*

3.4.1.2 Excluded IP

This page configures excluded IP addresses. A DHCP server will not allocate these excluded IP addresses to DHCP clients.

To configure DHCP server excluded IP range in the web UI:

1. Click Configuration, DHCP, Server, and Excluded IP.
2. Click Add IP Range then enter a new IP Range on the switch.
3. Click Apply.

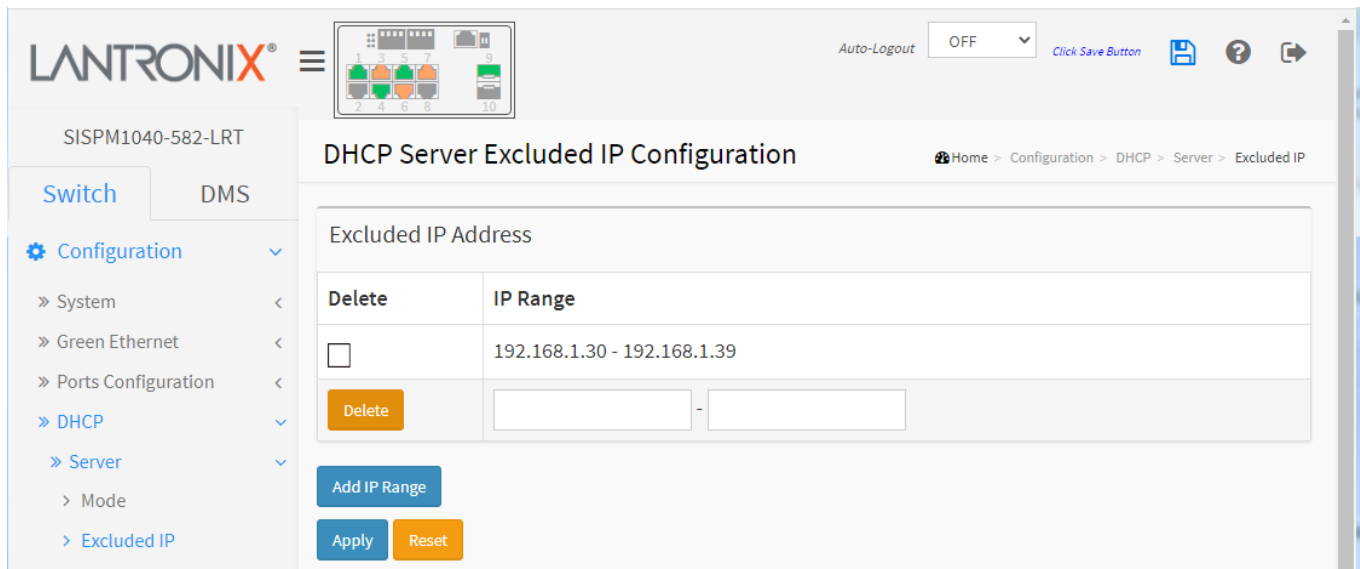


Figure 3.4.1.2: DHCP Server Excluded IP Configuration

IP Range : Define the IP range to be excluded IP addresses. The first excluded IP must be smaller than or equal to the second excluded IP. BUT, if the IP range contains only one excluded IP, then you can just input it to either one of the first and second excluded IP or both.

Buttons

Add IP Range : Click to add a new excluded IP range.

Apply : Click to save changes.

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

3.4.1.3 Pool

This page lets you manage DHCP pools. A DHCP server will allocate IP address and deliver configuration parameters to DHCP client based on the to the DHCP pool settings.

To configure a DHCP server pool in the web UI:

1. Click Configuration, DHCP, Server, and Pool.
2. Click Add New Pool then you can create new Pool on the switch.
3. Click Apply.

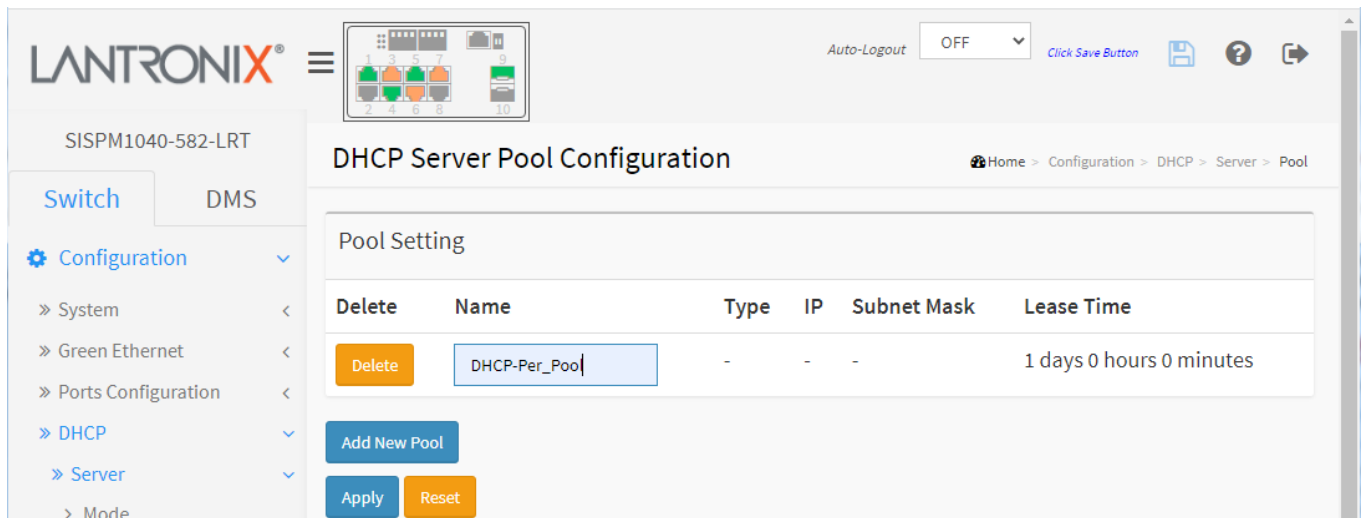


Figure 3.4.1.3: DHCP Server Pool Configuration

Parameter descriptions:

Pool Setting: Add or delete pools. Adding a pool and giving a name is to create a new pool with "default" configuration. If you want to configure all settings including type, IP subnet mask and lease time, you can click the pool name to go into the configuration page.

Name : Configure the pool name that accepts all printable characters, except white space. To configure the detail settings, click the pool name to go into the configuration page (see below).

Type : Display which type of the pool is.

Network: the pool defines a pool of IP addresses to service more than one DHCP client.

Host: the pool services for a specific DHCP client identified by client identifier or hardware address.

If "-" is displayed, it means not defined.

IP : Display network number of the DHCP address pool. If "-" is displayed, it means not defined.

Subnet Mask : Display subnet mask of the DHCP address pool. If "-" is displayed, it means not defined.

Lease Time : Display lease time of the pool.

Buttons

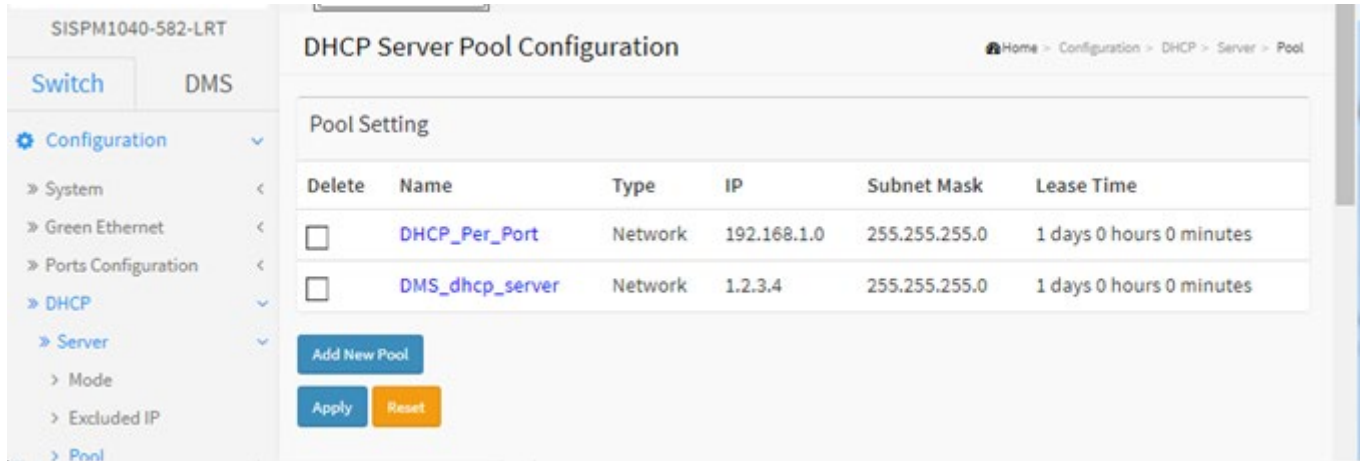
Add New Pool : Click to add a new DHCP pool.

Apply : Click to save changes.

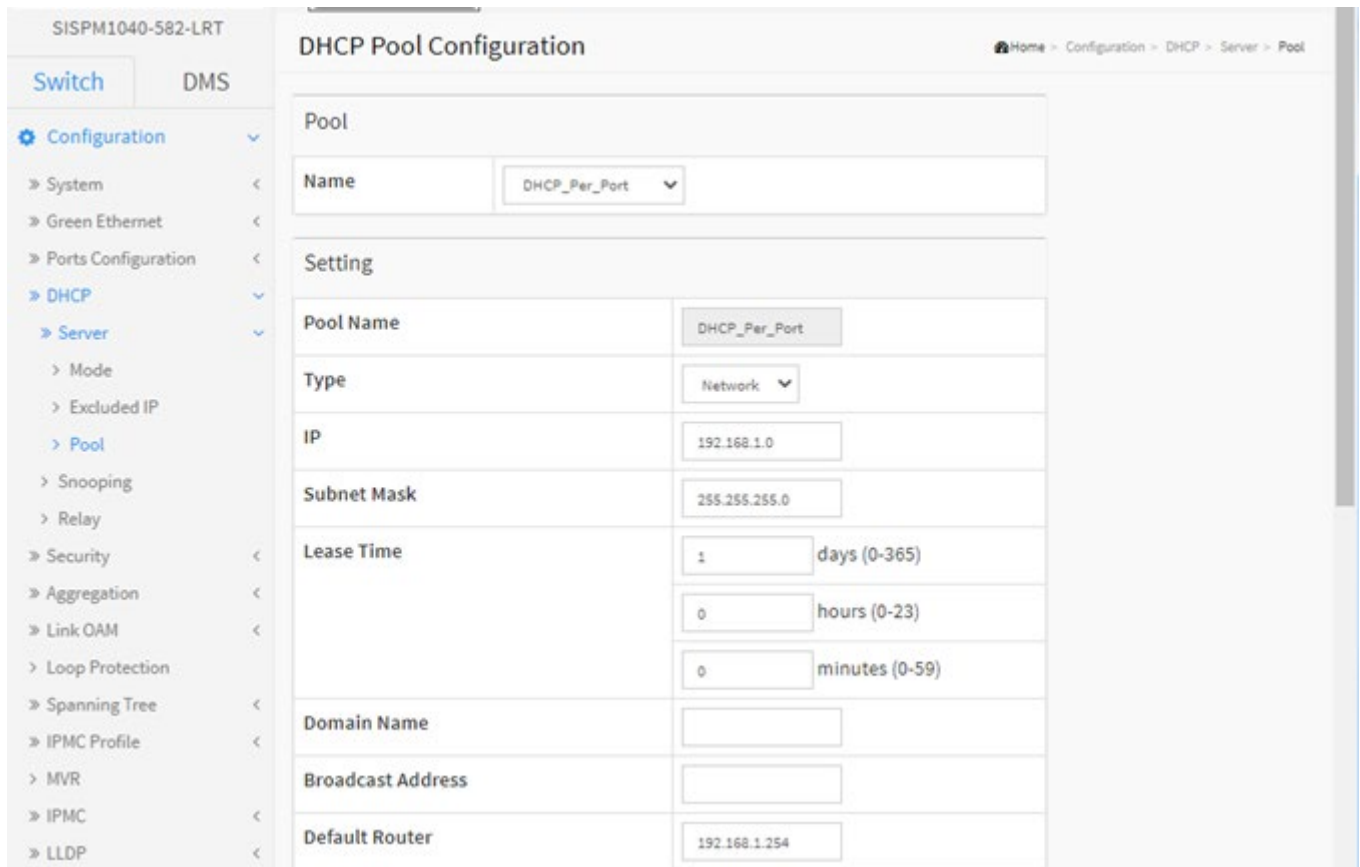
Reset : Click to undo any changes made locally and revert to previously saved values.

Configure DHCP Pool

At **Configuration > DHCP Server > Pool** click the linked name (e.g., *DHCP_Per_Port*) in the Pool Setting Name column to display the DHCP Pool Configuration page.



At the DHCP Pool Configuration page, configure the Settings:



<ul style="list-style-type: none"> » VLAN Translation < > VLANs » Private VLANs < » VCL < » Voice VLAN < » Ethernet Services < » QoS < > Mirroring > UPnP > PTP » GVRP < > sFlow > UDLD > Rapid Ring > SMTP Monitor < Diagnostics < Maintenance < 	DNS Server	<input type="text" value="8.8.8.8"/>	
		<input type="text"/>	
		<input type="text"/>	
		<input type="text"/>	
		<input type="text"/>	
	NTP Server	<input type="text"/>	
		<input type="text"/>	
		<input type="text"/>	
		<input type="text"/>	
	TFTP Server	<input type="text"/>	
	Boot File	<input type="text"/>	
	NetBIOS Node Type	None ▾	
	NetBIOS Scope	<input type="text"/>	
	NetBIOS Name Server	<input type="text"/>	
		<input type="text"/>	
	<input type="text"/>		
	<input type="text"/>		
	<input type="text"/>		
NIS Domain Name	<input type="text"/>		
NIS Server	<input type="text"/>		
	<input type="text"/>		
	<input type="text"/>		
	<input type="text"/>		
Client Identifier	None ▾		
	<input type="text"/>		
Hardware Address	<input type="text"/>		
Client Name	<input type="text"/>		
Vendor 1 Class Identifier	<input type="text"/>		
Vendor 1 Specific Information	<input type="text"/>		
Vendor 2 Class Identifier	<input type="text"/>		
Vendor 2 Specific Information	<input type="text"/>		
Vendor 3 Class Identifier	<input type="text"/>		
Vendor 3 Specific Information	<input type="text"/>		
Vendor 4 Class Identifier	<input type="text"/>		
Vendor 4 Specific Information	<input type="text"/>		
Lighting Server	<input type="text"/>		

DHCP Pool Configuration Parameters

Pool: Select a pool to configure the settings.

Name: Select a pool by pool name.

Setting: Configure pool settings.

Name: Displays the selected pool name.

Type: Specify which type of the pool is.

Network: the pool defines a pool of IP addresses to service more than one DHCP client.

Host: the pool services for a specific DHCP client identified by client identifier or hardware address.

None: no pool type specified.

Network ▾
None
Network
Host

IP: Specify network number of the DHCP address pool.

Subnet Mask: DHCP option 1. Specify subnet mask of the DHCP address pool.

Lease Time: DHCP option 51, 58 and 59. Specify lease time that allows the client to request a lease time for the IP address. If all are 0's, then it means the lease time is infinite.

Domain Name: DHCP option 15. Specify domain name that client should use when resolving hostname via DNS.

Broadcast Address: DHCP option 28. Specify the broadcast address in use on the client's subnet.

Default Router: DHCP option 3. Specify a list of IP addresses for routers on the client's subnet.

DNS Server: DHCP option 6. Specify a list of Domain Name System name servers available to the client.

NTP Server: DHCP option 42. Specify a list of IP addresses indicating NTP servers available to the client.

TFTP Server: DHCP option 66. Specify a list of TFTP servers available to the client.

Boot File: DHCP option 67. Specify a bootfile Name available to the client.

NetBIOS Node Type: DHCP option 46. Specify NetBIOS node type option to allow Netbios over TCP/IP clients which are configurable to be configured as described in [IETF RFC 1001/1002](https://www.ietf.org/rfc/rfc1001.html). The dropdown selections are None (default), B-node, P-node, M-node, and H-node.

None ▾
None
B-node
P-node
M-node
H-node

NetBIOS Scope: DHCP option 47. Specify the NetBIOS over TCP/IP scope parameter for the client as specified in RFC 1001/1002.

NetBIOS Name Server: DHCP option 44. Specify a list of NBNS name servers listed in order of preference.

NIS Domain Name: DHCP option 40. Specify the name of the client's NIS domain.

NIS Server: DHCP option 41. Specify a list of IP addresses indicating NIS servers available to the client.

Client Identifier: DHCP option 61. Specify client's unique identifier to be used when the pool is the type of host. The dropdown selections are **None** (default), **FQDN** (Fully-Qualified Domain Name), and **MAC**.

None ▾
None
FQDN
MAC

Hardware Address: Specify client's hardware(MAC) address to be used when the pool is the type of host.

Client Name: DHCP option 12. Specify the name of client to be used when the pool is the type of host.

Vendor i Class Identifier: DHCP option 60. Specify to be used by DHCP client to optionally identify the vendor type and configuration of a DHCP client. DHCP server will deliver the corresponding option 43 specific information to the client that sends option 60 vendor class identifier.

Vendor / Specific Information: DHCP option 43. Specify vendor specific information according to option 60 vendor class identifier.

Lighting Server: DHCP option 229. Specify a lighting server available to the client. This feature should be enabled for any ports used for lighting nodes as it significantly reduces the delay time between when a lighting node is connected to a port and when the switch allows network communication from the lighting node to the lighting gateway. **Note:** If multicast traffic is not allowed on your network, you can configure the network DHCP server to pass the lighting gateway server IP address in DHCP Option 229 (added at FW VB7.20.0146).

With the switch acting as DHCP Server, it will insert operation 229 into DHCP offer packets and DHCP ACK packets. After receiving DHCP discover packets, it will insert option 229 for all DHCP clients as long as the DHCP Server is configured with Option 229. This option is configurable via the UI, SNMP, and CLI.

The code for this option is 229, and its length is 4 octets:

Code Len Address

229	4	a1	a2	a3	a4
-----	---	----	----	----	----

For DHCP packet content, Option 229 is inserted between the last and before option 255.

Buttons

Apply: Click to save changes.

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

Messages:

Invalid Vendor 1 Specific Information. It must be a HEX string and begin with '0x' or '0X'.

The format of 'Hardware Address' is 'xx-xx-xx-xx-xx-xx' or 'xx.xx.xx.xx.xx.xx' or 'xxxxxxxxxxxx' (x is a hexadecimal digit).

Client identifier type is defined so value must be inputted.

3.4.2 Snooping

This page lets you configure DHCP Snooping parameters of the switch.

DHCP Snooping can prevent attackers from adding their own DHCP servers to the network. DHCP Snooping is used to block intruder on the untrusted ports of the switch device when it tries to intervene by injecting a bogus DHCP reply packet to a legitimate conversation between the DHCP client and server.

To configure DHCP snooping in the web UI:

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

The screenshot displays the Lantronix web interface for configuring DHCP Snooping. The breadcrumb trail indicates the path: Home > Configuration > DHCP > Snooping. The 'Snooping Mode' is currently set to 'Disabled'. Below this, the 'Port Mode Configuration' table lists ports 1 through 7, each with a dropdown menu set to 'Trusted'.

Port	Mode
*	<>
1	Trusted
2	Trusted
3	Trusted
4	Trusted
5	Trusted
6	Trusted
7	Trusted

Figure 3.4.2: DHCP Snooping Configuration

Parameter descriptions:

Snooping Mode : Indicates the DHCP snooping mode operation. Possible modes are:

Enabled: 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.

Disabled: Disable DHCP snooping mode operation.

Port Mode Configuration :Indicates the DHCP snooping port mode. Possible port modes are:

Trusted: Configures the port as trusted source of the DHCP messages.

Untrusted: Configures the port as untrusted source of the DHCP messages.

Buttons

Apply : Click to save changes.

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

Messages:

Client identifier type is defined so value must be inputted.

Pool's IP/netmask does not match interfaces' IP/netmask, or DHCP server mode isn't enabled on a correct VLAN range.

The format of 'Hardware Address' is 'xx-xx-xx-xx-xx-xx' or 'xx.xx.xx.xx.xx.xx' or 'xxxxxxxxxxxx' (x is a hexadecimal digit).

The value format of MAC type is 'xx-xx-xx-xx-xx-xx' or 'xx.xx.xx.xx.xx.xx' or 'xxxxxxxxxxxx' (x is a hexadecimal digit).

3.4.3 Relay

DHCP Relay is used to forward and to transfer DHCP messages between the clients and the server when they are not on the same subnet domain. DHCP option 82 enables a DHCP relay agent to insert specific information into a DHCP request packets when forwarding client DHCP packets to a DHCP server and remove the specific information from a DHCP reply packets when forwarding server DHCP packets to a DHCP client. The DHCP server can use this information to implement IP address or other assignment policies. Specifically, the option works by setting two sub-options: Circuit ID (option 1) and Remote ID (option2). The Circuit ID sub-option is supposed to include information specific to which circuit the request came in on. The Remote ID sub-option was designed to carry information relating to the remote host end of the circuit. The Remote ID is 6 bytes in length, and the value is equal the DHCP relay agents MAC address.

A DHCP relay agent is used to forward and to transfer DHCP messages between the clients and the server when they are not in the same subnet domain. It stores the incoming interface IP address in the GIADDR field of the DHCP packet. The DHCP server can use the value of GIADDR field to determine the assigned subnet. For such condition, please make sure the switch configuration of VLAN interface IP address and PVID (Port VLAN ID) correctly.

Web Interface

To configure DHCP Relay in the web UI:

1. Click Configuration, DHCP and Relay.
2. Specify the Relay Mode, Relay server, Relay Information Mode, Relay Information policy.
3. Click Apply.

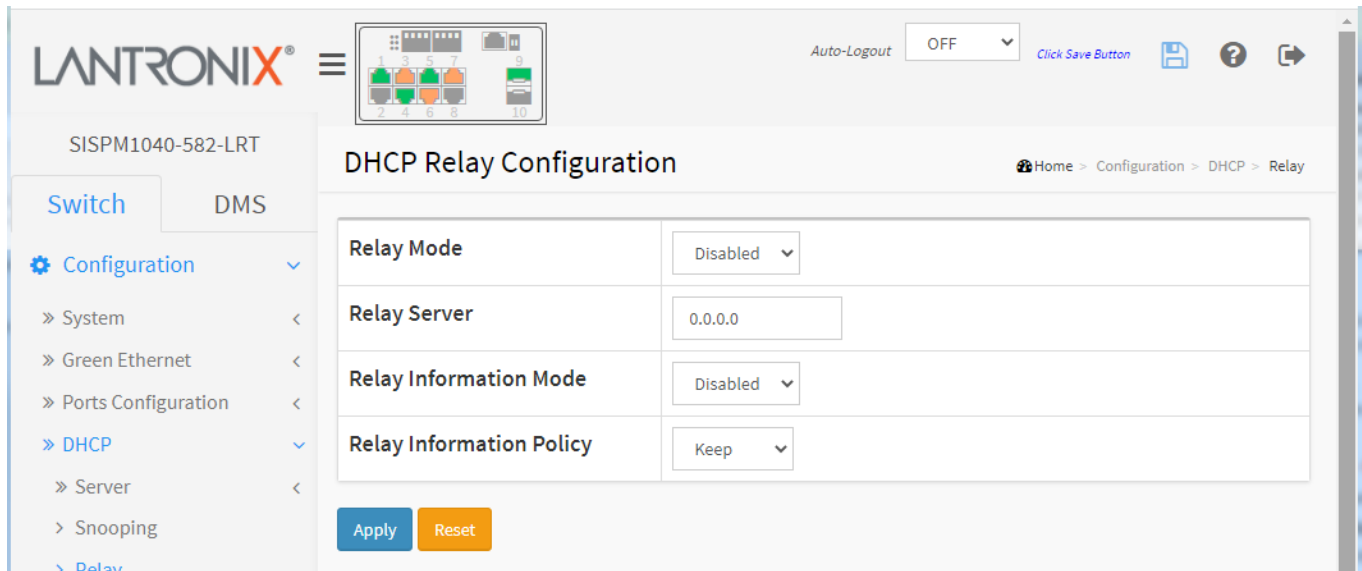


Figure 3.4.3: DHCP Relay Configuration

Parameter descriptions:

Relay Mode : Indicates the DHCP relay mode operation. Possible modes are:

Enabled: 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.

Disabled: Disable DHCP relay mode operation.

Relay Server : Indicates the DHCP relay server IP address.

Relay Information Mode : Indicates the DHCP relay information mode option operation. The Option 82 circuit ID format is "[vlan_id][module_id][port_no]". The first four characters represent the VLAN ID, the fifth and sixth characters are the module ID (in standalone device it always equals 0), and the last two characters are the port number. For example, "00030108" means the DHCP message receive form VLAN ID 3, switch ID 1, port No 8.

The option 82 remote ID value is 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 is enabled, if the agent receives a DHCP message that already contains relay agent information it will enforce the policy. The 'Replace' policy is invalid when relay information mode is disabled. Possible policies are:

Replace: Replace the original relay information when a DHCP message that already contains it is received.

Keep: Keep the original relay information when a DHCP message that already contains it is received.

Drop: Drop the package when a DHCP message that already contains relay information is received.

Buttons

Apply : Click to save changes.

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

Messages:

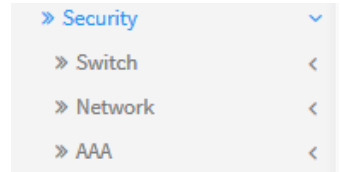
Please make sure the DHCP server connected on trust port?

Summary – How to Set Up the Switch as a DHCP Server

1. Make sure your computer IP address is on the same subnet as your switch IP subnet.
2. At Configuration > DHCP > Server > Mode click the Add VLAN Range button.
3. Enter a VLAN Range and select Enabled at the Mode dropdown.
4. Create a DHCP Server Pool. At Configuration > DHCP > Server > Pool click the Add New Pool button and enter the name of your Pool and click the Apply button.
5. Enter the Pool Name; when the next screen comes up click on the Pool Name link highlighted in blue.
6. At the DHCP > Server > Pool page click on the Type drop down and select Network, specify your network IP address and Subnet Mask; leave everything else at defaults and then click the Apply button.
7. Verify the switch is giving out IP addresses at Monitor > DHCP > Server > Binding.
8. Verify the DHCP Server setup at DMS Graphical Monitoring > Topology view.
9. Verify PoE power consumption at Monitor > PoE.

3-5 Security

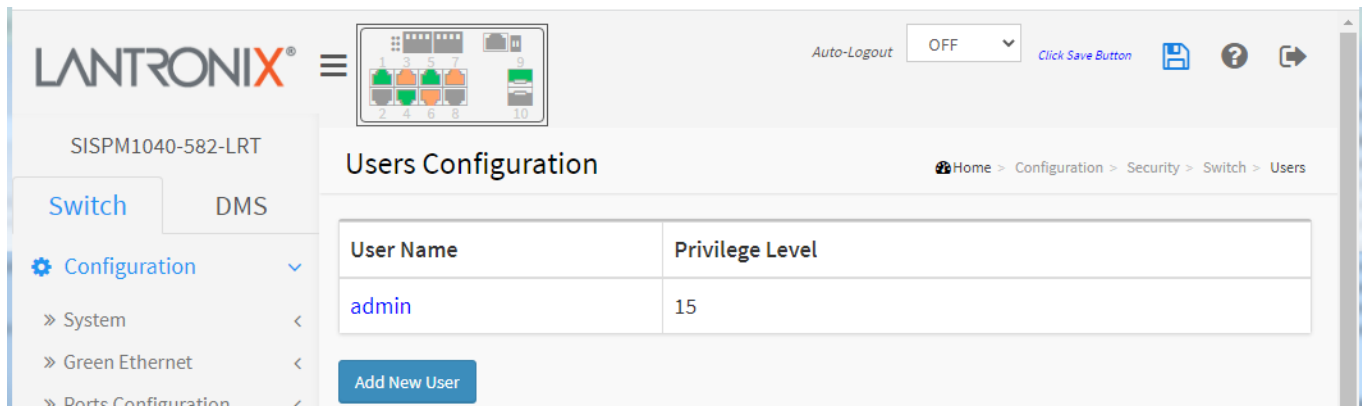
This section lets you configure the Port Security settings of the switch. Each of the main menu items (Switch, Network, and AAA) have sub-menus that let you configure a wide range of security functions (e.g., you can use the Port Security feature to restrict input to an interface by limiting and identifying MAC addresses).



3.5.1 Switch

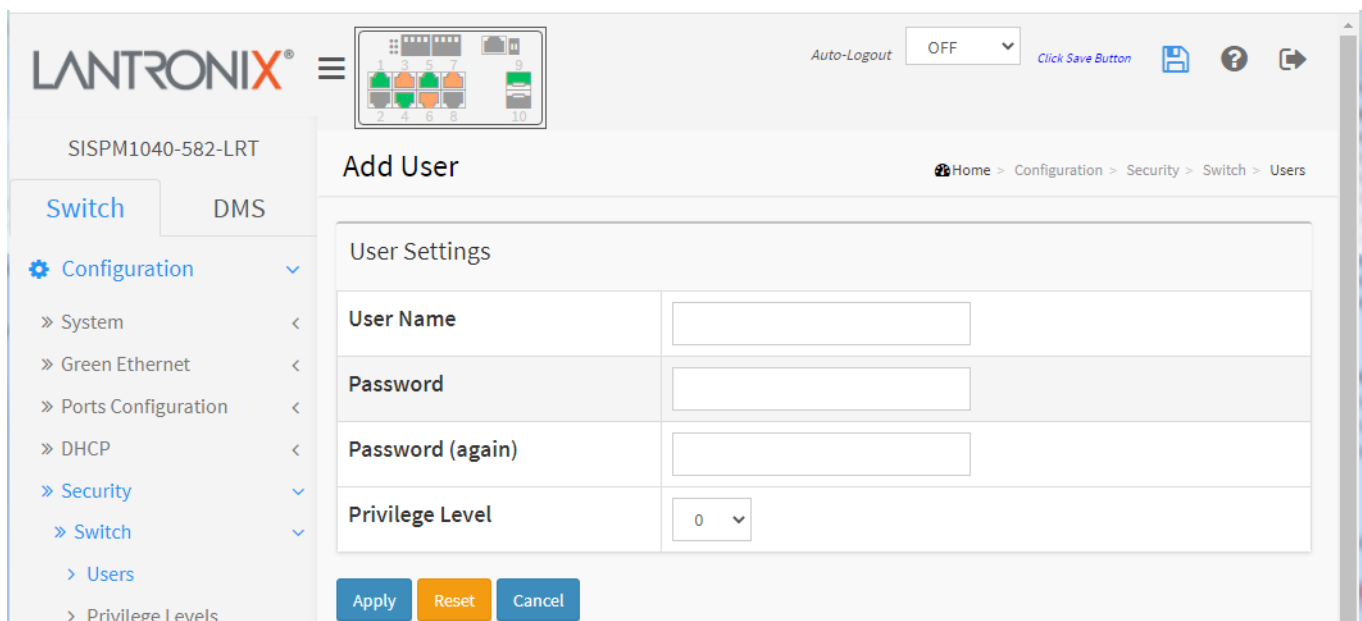
3.5.1.1 Users

This page provides an overview of the current users. Currently the only way to login as another user on the web server is to close and reopen the web browser. Initially, the Users Configuration table has one user (admin) at Privilege Level 15.



To add a User in the web UI:

1. Click Configuration, Security, Switch and Users.
2. Click Add New User.
3. Specify the User Name, Password (twice), and Privilege Level.
4. Click the Apply button to save changes to the startup-config file.



Parameter descriptions:

User Name : Enter the name identifying the user. This is also a link to Add/Edit User (see below).

Password : Enter the password of the user. The allowed string length is 0 to 31. Any printable ASCII character including the space character is accepted.

Password (again) : Enter the user password again (must match previous entry).

Privilege Level : The privilege level of the user. The allowed range is 0 to 15. If the privilege level value is 15, it can access all groups, i.e., that is granted the fully control of the device. But 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. The system maintenance level (software upload, factory defaults, etc.) needs user privilege level 15. Generally, the privilege level 15 can be used for an administrator account, privilege level 10 for a standard user account and privilege level 5 for a guest account. If a user's privilege level is too low to perform a function, the message displays "*Insufficient Privilege Level - The web page is non-accessible. Please use the valid privilege level.*" To clear the message, click a menu function that is supported by the assigned privilege level.

Buttons

Add New User : Click to add a new user.

Apply : Click to save changes.

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

Cancel: Click to undo any unsaved changes.

Edit a User

Click a linked User Name in the Users Configuration table to display the Edit User page:

The screenshot displays the 'Edit User' configuration page in the Lantronix web interface. The page title is 'Edit User' and the breadcrumb navigation is 'Home > Configuration > Security > Switch > Users'. The 'User Settings' section contains the following fields:

User Name	admin
Password
Password (again)
Privilege Level	15

At the bottom of the form are four buttons: 'Apply' (blue), 'Reset' (yellow), 'Cancel' (blue), and 'Delete User' (red). The left sidebar shows a navigation menu with 'Switch' selected and 'Users' highlighted under 'Security'.

Here you can edit a user's Password and Privilege Level. You can also delete a user from the table.

Buttons

Delete User: Delete the current user. This button is not available for new configurations (Add New User). At the confirmation prompt click the OK button.

Messages:

Can't change the privilege level since no other highest privilege account exist if change it.

3.5.1.2 Privilege Levels

This page lets you view and set privilege levels for various groups of functions. To configure Privilege Levels:

1. Click Configuration, Security, Switch and Privilege Level.
2. Specify the Privilege parameters.
3. Click Apply.

Group Name	Privilege Levels			
	Configuration Read-only	Configuration/Execute Read/write	Status/Statistics Read-only	Status/Statistics Read/write
Aggregation	5	10	5	10
Debug	15	15	15	15
DHCP	5	10	5	10
DHCPv6_Client	5	10	5	10
Diagnostics	5	10	5	10
DMS_client	5	10	5	10
DMS_server	5	10	5	10
EEE	5	10	5	10
EPS	5	10	5	10

Figure 3.5.1.2: Privilege Levels Configuration

Parameter descriptions:

Group Name : The name identifying the privilege group. In most cases, a privilege level group consists of a single module (e.g., LACP, RSTP or QoS), but a few of them contains more than one. The following description defines these privilege level groups in detail:

System: Contact, Name, Location, Timezone, Daylight Saving Time, Log.

Security: Authentication, System Access Management, Port (contains Dot1x port, MAC based and the MAC Address Limit), ACL, HTTPS, SSH, ARP Inspection, IP source guard.

IP: Everything except 'ping'.

Port: Everything except Cable Diagnostics.

Diagnostics: 'ping' and Cable Diagnostics.

Maintenance: CLI- System Reboot, System Restore Default, System Password, Configuration Save, Configuration Load and Firmware Load. Web- Users, Privilege Levels and everything in Maintenance.

Debug: Only present in CLI.

Privilege Levels : Every group has an authorization Privilege level for the following sub groups: configuration read-only, configuration/execute read-write, status/statistics read-only, and status/statistics read-write. User Privilege should be same or greater than the authorization Privilege level to have the access to that group.

Configuration Read-only: (e.g., for viewing configuration settings only).

Configuration/Execute Read/write: (e.g., for viewing and setting configuration settings).

Status/Statistics Read-only: (e.g., for viewing statistics only).

Status/Statistics Read/write: (e.g., for clearing of statistics).

Buttons

Apply : Click to save changes.

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

3.5.1.3 Auth Method

This page lets you configure how a user is authenticated when they log into the switch via one of the management client interfaces (console, telnet, ssh, http, or https). To configure Authentication Method parameters in the web UI:

1. Click Configuration, Security, Switch and Auth Method.
2. Specify the Client (console, telnet, ssh, web) which you want to monitor.
3. Specify the Authentication Method (none, local, radius, tacacs+).
4. Check Fallback.
5. Click Apply.

Authentication Method Configuration

Home > Configuration > Security > Switch > Auth Method

Authentication Method

Client	Methods			Service Port	Fallback
console	local	no	no		<input type="checkbox"/>
telnet	no	no	no	23	<input type="checkbox"/>
ssh	local	no	no	22	<input type="checkbox"/>
http	redirect	no	no	80	<input type="checkbox"/>
https	local	no	no	443	<input type="checkbox"/>

Command Authorization Method

Client	Method	Cmd Lvl	Cfg Cmd	Fallback
console	no	0	<input type="checkbox"/>	<input type="checkbox"/>
telnet	no	0	<input type="checkbox"/>	<input type="checkbox"/>
ssh	no	0	<input type="checkbox"/>	<input type="checkbox"/>
http	no			<input type="checkbox"/>
https	no			<input type="checkbox"/>

Accounting Method

Client	Method	Cmd Lvl	Exec
console	no		<input type="checkbox"/>
telnet	no		<input type="checkbox"/>
ssh	no		<input type="checkbox"/>
http	no		<input type="checkbox"/>
https	no		<input type="checkbox"/>

Apply Reset

Figure 3.5.1.3: Authentication Method Configuration

Authentication Method section : The authentication section allows you to configure how a user is authenticated when they log into the switch via one of the management client interfaces (console, telnet, ssh, http, or https).

Client : The management client for which the configuration below applies.

Methods : Method can be set to one of these values:

no: Authentication is disabled, and login is not possible.

redirect: When HTTPS is enabled, enable HTTPS automatic redirect on the switch.

local: Use the local user database on the switch for authentication.

radius: Use remote RADIUS server(s) for authentication.

tacacs: Use remote TACACS+ server(s) for authentication.

Methods that involve remote servers are timed out if the remote servers are offline. In this case the next method is tried. Each method is tried from left to right and continues until a method either approves or rejects a user. If a remote server is used for primary authentication it is recommended to configure secondary authentication as 'local'. This will enable the management client to login via the local user database if none of the configured authentication servers are alive. Note: FW vB.7.20.0106 changed the https Auth Method default setting to "local".

Service Port : The TCP port for each client service. The valid port number is 1 ~ 65534.

Fallback : Enable fallback to local authentication by checking this box. If none of the configured authentication servers are alive, the local user database is used for authentication. This is only possible if the Authentication Method is set to a value other than 'none' or 'local'

Command Authorization Method section: This section lets you limit the CLI commands available to a user.

Client : The management client for which the configuration below applies.

Method : Method can be set to one of the following values:

no: Command authorization disabled. User granted access to CLI commands according to privilege level.

tacacs: Use remote TACACS+ server(s) for command authorization. If all remote servers are offline, the user is granted access to CLI commands according to his privilege level.

Cmd Lvl : Authorize all commands with a privilege level higher than or equal to this level. Valid values are in the range 0 to 15.

Cfg Cmd : Also authorize configuration commands.

Fallback : This function is an auxiliary function of Authorization. When the switch cannot communicate with TACACS+ Server normally, it will check the right permission level of the Local Account to execute the Authorization.

Accounting Method section: This section lets you configure command and exec (login) accounting.

Client : The management client for which the configuration below applies.

Method : Method can be set to one of the following 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 0 - 15. Leave the field empty to disable command accounting.

Exec : Enable exec (login and logout) accounting.

Buttons

Apply : Click to save changes.

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

3-5.1.4 HTTPS

This page lets you configure HTTPS settings and maintain the current certificate on the switch.

To configure HTTPS parameters in the web UI:

1. Click Configuration, Security, Switch and HTTPS.
2. Specify the Certificate Maintain, Certificate Pass Phrase, and Certificate Upload.
3. Click the Choose File button to select the file to upload.
4. Click Apply.

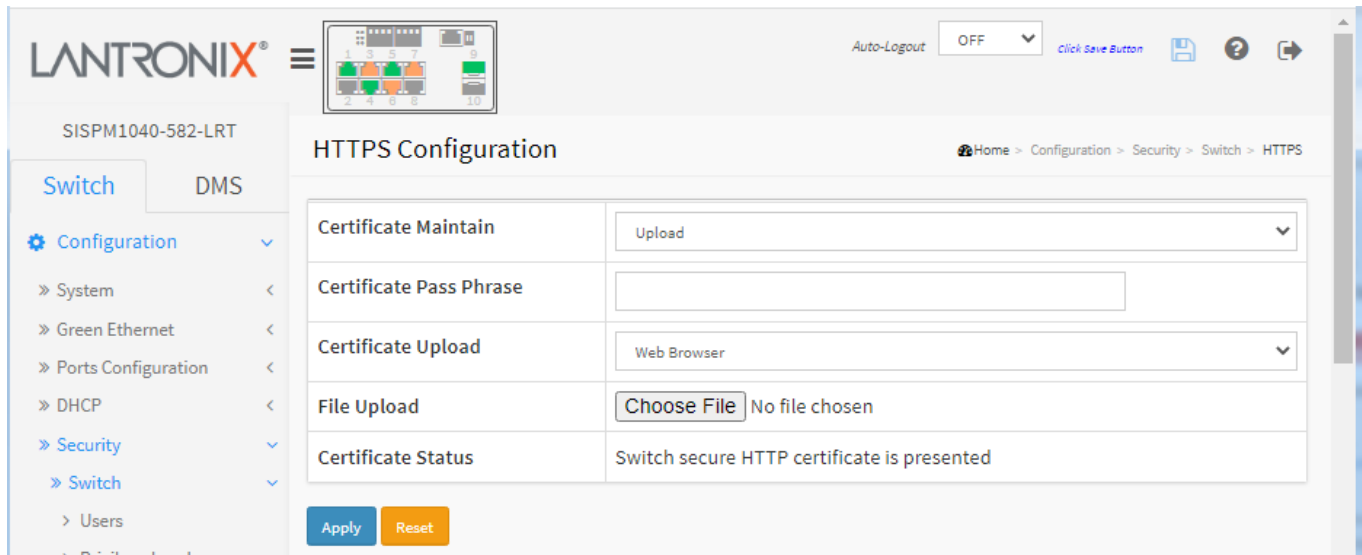


Figure 3-5.1.4: HTTPS Configuration

Parameter descriptions:

Certificate Maintain : The operation of certificate maintenance. Possible operations are:

Upload: Upload a certificate PEM file. Possible methods are: Web Browser or URL.

Generate: Generate a new self-signed RSA certificate.

Certificate Pass Phrase : Enter the pass phrase in this field if your uploading certificate is protected by a specific passphrase.

Certificate Upload : Upload a certificate PEM file into the switch. The file should contain the certificate and private key together. If you have two separated files for saving certificate and private key. Use the Linux cat command to combine them into a single PEM file. For example, `cat my.cert my.key > my.pem`.

Possible 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>`.

tftp example: `tftp://10.10.10.10/new_image_path/new_image.dat`,

http example:

`http://username:password@10.10.10.10:80/new_image_path/new_image.dat`.

A valid file name is a text string drawn from alphabet (A-Za-z), digits (0-9), dot (.), hyphen (-), under score (_). The maximum length is 63 and hyphen must not be first character. A filename that only contains '.' is not allowed.

Note that an RSA certificate is recommended since most new web browser versions have removed support for DSA in certificates (e.g., Firefox v37 and Chrome v39).

File Upload: Click the **Choose File** button to navigate to and select a file to upload. Initially displays the message “No file chosen”.

Certificate Status : Display the current status of certificate on the switch. Possible statuses are:

Switch secure HTTP certificate is presented.

Switch secure HTTP certificate is not presented.

Switch secure HTTP certificate is generating

Buttons

Apply : Click to save changes.

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

Example: Certificate Upload via Web Browser:

The screenshot shows the Lantronix web interface for the SISPM1040-582-LRT device. The left sidebar shows the navigation menu with 'Switch' selected. The main content area is titled 'HTTPS Configuration' and contains the following fields:

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

At the bottom of the configuration area are 'Apply' and 'Reset' buttons.

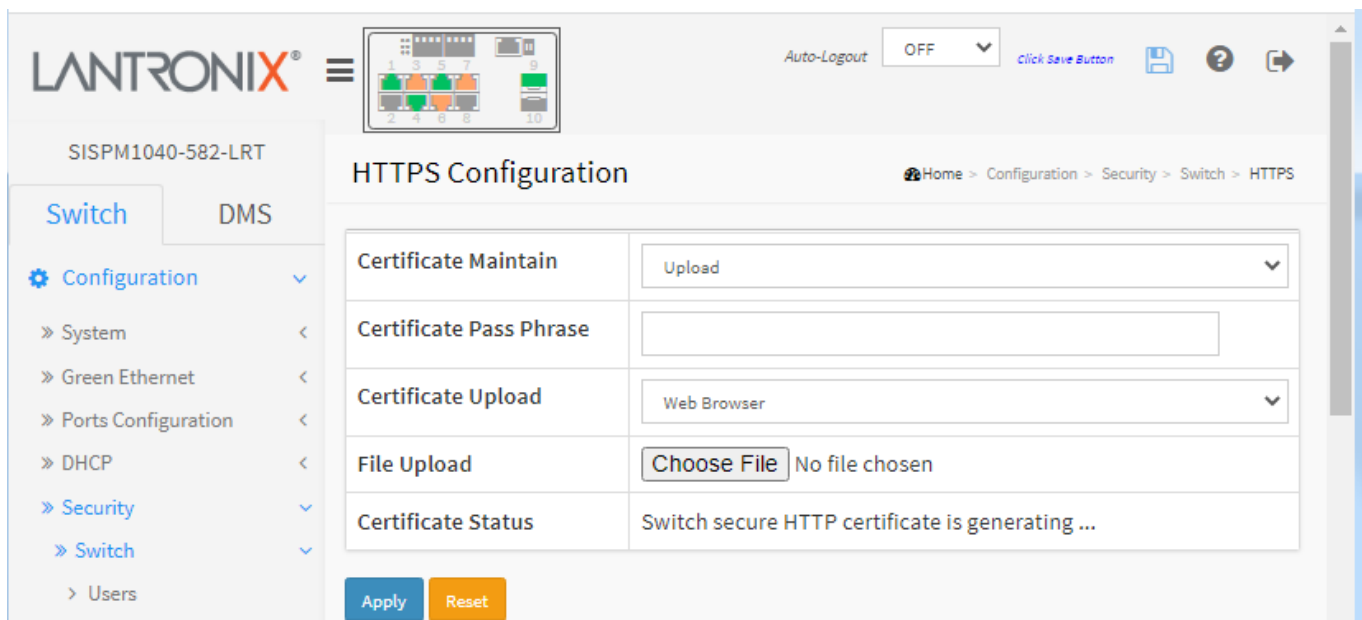
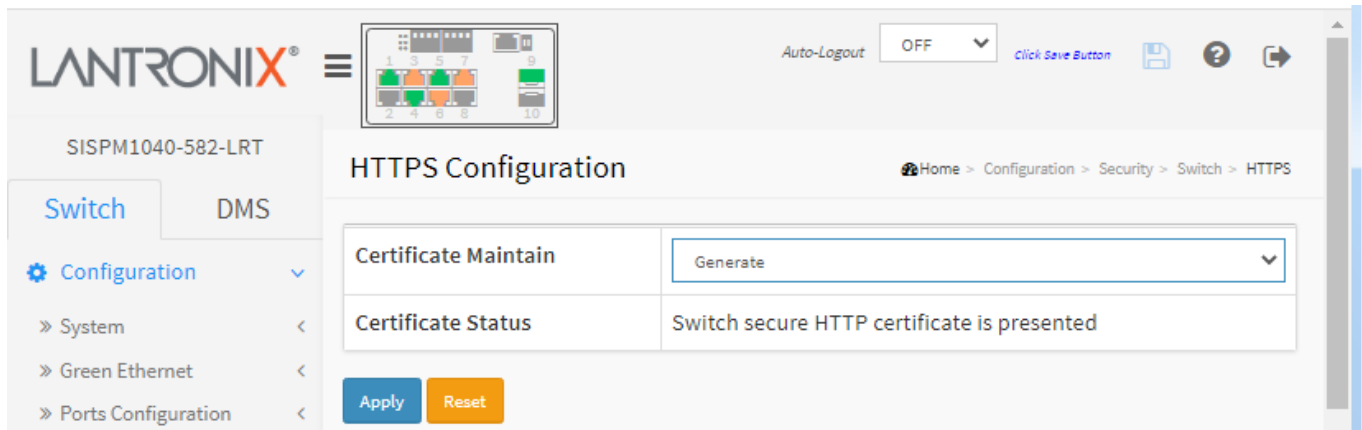
Example: Certificate Upload via URL:

The screenshot shows the Lantronix web interface for the SISPM1040-582-LRT device. The left sidebar shows the navigation menu with 'Switch' selected. The main content area is titled 'HTTPS Configuration' and contains the following fields:

Certificate Maintain	Upload
Certificate Pass Phrase
Certificate Upload	URL
URL	192.168.90.52
Certificate Status	Switch secure HTTP certificate is presented

At the bottom of the configuration area are 'Apply' and 'Reset' buttons.

Example: Generate a Certificate



Messages:

Certificate PEM file size too big

HTTPS invalid URL parameter

Please disable HTTPS mode first.

3-5.1.5 Access Management

This page lets you configure the access management table of the Switch including HTTP/HTTPS, SNMP, and TELNET/SSH. You can manage the Switch over an Ethernet LAN or over the Internet. The maximum number of entries is 16. If the application's type matches any of the access management entries, it will allow access to the switch.

To configure Access Management in the web UI:

1. Click Configuration, Security, Switch and Access Management.
2. Select "Enabled" in the Mode of Access Management Configuration.
3. Click "Add New Entry".
4. Specify the Start IP Address and End IP Address.
5. Check Access Management method (HTTP/HTTPS, SNMP, and TELNET/SSH) in the entry.
6. Click Apply.

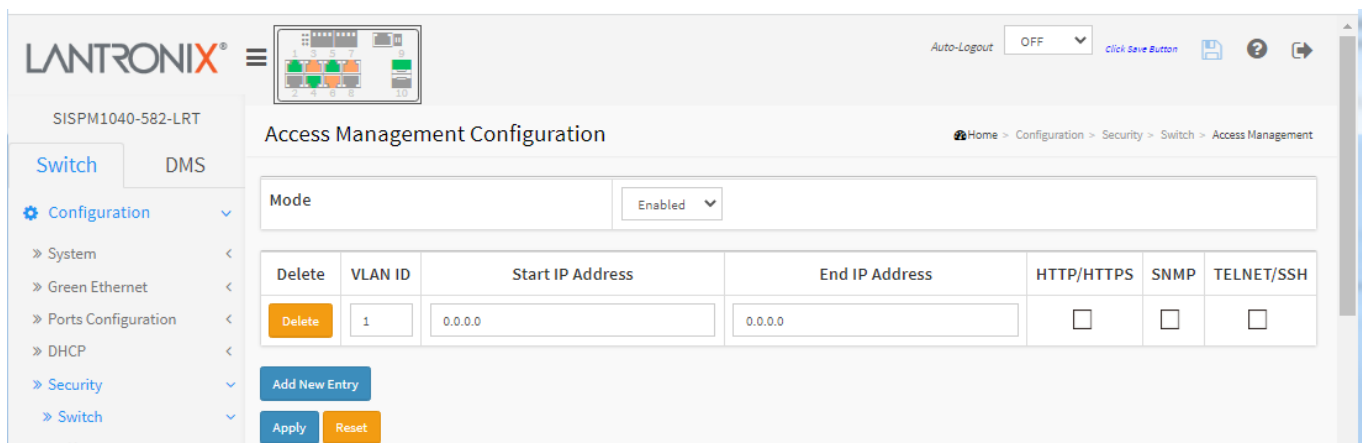


Figure 3-5.1.5: Access Management Configuration

Parameter descriptions:

Mode : Indicates the access management mode operation. Possible modes are:

Enabled: Enable access management mode operation.

Disabled: Disable access management mode operation (default).

VLAN ID : Indicates the VLAN ID for the access management entry.

Start IP address : Indicates the start IP address for the access management entry.

End IP address : Indicates the end IP address for the access management entry.

HTTP/HTTPS : Indicates that the host can access the switch from HTTP/HTTPS interface if the host IP address matches the IP address range provided in the entry.

SNMP : Indicates that the host can access the switch from SNMP interface if the host IP address matches the IP address range provided in the entry.

TELNET/SSH : Indicates that the host can access the switch from TELNET/SSH interface if the host IP address matches the IP address range provided in the entry.

Buttons

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

Add New Entry : Click to add a new access management entry. At least one allowed service must be selected.

Apply : Click to save changes.

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

3-5.1.6 SNMP

Any Network Management System (NMS) running the Simple Network Management Protocol (SNMP) can manage the Managed devices equipped with SNMP agent, provided that the Management Information Base (MIB) is installed correctly on the managed devices. The SNMP is a protocol that is used to govern the transfer of information between SNMP manager and agent and traverses the Object Identity (OID) of the management Information Base (MIB), described in the form of SMI syntax. SNMP agent is running on the switch to response the request issued by SNMP manager.

Basically, it is passive except issuing the trap information. The switch supports a switch to turn on or off the SNMP agent. If you select Enabled at the SNMP Mode dropdown, the SNMP agent will be started up. All supported MIB OIDs, including RMON MIB, can be accessed via SNMP manager. If the SNMP Mode is set to “Disabled”, the SNMP agent will be de-activated, and the related Community Names, Trap Host IP Address, Trap and all MIB counters will be ignored.

3-5.1.6.1 System

This page lets you configure SNMP mode, version, community names, and engine ID. An SNMP manager must pass the authentication by identifying both community names, then it can access the MIB information of the target device. So both parties must have the same community name. Once completing the setting, click the Apply button for the setting to take effect.

Web Interface

To configure SNMP System parameters in the web UI:

1. Click Configuration, Security, Switch, SNMP and System.
2. At the Mode dropdown, select Enable or Disable as the SNMP mode.
3. Specify the Version, Read and Write Community, and Engine ID parameters.
4. Click Apply.

Parameter	Value
Mode	Enabled
Version	SNMP v2c
Read Community	public
Write Community	private (Enabled)
Engine ID	800007e5017f000001

Figure 3-5.1.6.1: SNMP System Configuration

Parameter descriptions:

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

Enabled: Enable SNMP mode operation.

Disabled: Disable SNMP mode operation.

Version : Indicates the SNMP supported version. Possible versions are:

SNMP v1: Set SNMP supported version 1.

SNMP v2c: Set SNMP supported version 2c (the default).

SNMP v3: Set SNMP supported version 3.

Read Community : Indicates the community read access string to permit access to SNMP agent. The allowed string length is 0 to 255 characters, and the allowed content is ASCII characters 33 - 126.

The field is applicable only when SNMP version is SNMPv1 or SNMPv2c. If SNMP version is SNMPv3, the community string will be associated with SNMPv3 communities table. It provides more flexibility to configure security name than a SNMPv1 or SNMPv2c community string. In addition to community string, a particular range of source addresses can be used to restrict source subnet.

Write Community : Indicates the community write access string to permit access to SNMP agent. The allowed string length is 0 to 255 characters, and the allowed content is ASCII characters 33 - 126.

Enabled: Enable SNMP write community operation.

Disabled: Disable SNMP write community operation.

The field is applicable only when SNMP version is SNMPv1 or SNMPv2c. If SNMP version is SNMPv3, the community string will be associated with SNMPv3 communities table. It provides more flexibility to configure security name than a SNMPv1 or SNMPv2c community string. In addition to community string, a particular range of source addresses can be used to restrict source subnet.

Engine ID : Indicates the SNMPv3 engine ID. 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. Change of the Engine ID will clear all original local users.

Buttons

Apply : Click to save changes.

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

3-5.1.6.2 Trap

Configure SNMP traps on this page. To configure SNMP Trap parameters in the web UI:

1. Click Configuration, Security, Switch, SNMP and Trap.

The screenshot shows the 'Trap Configuration' page in the Lantronix web UI. The breadcrumb trail is 'Home > Configuration > Security > Switch > SNMP > Trap'. The 'Mode' dropdown is set to 'Disabled'. Below is a table for 'Trap Destination Configurations' with columns: Delete, Name, Mode, Version, Destination Address, and Destination Port. There are 'Add New Entry', 'Apply', and 'Reset' buttons.

2. On the default page, click the Add New Entry button and enter the new SNMP Trap parameters for the switch.

3. Click Apply when done.

The screenshot shows the 'SNMP Trap Configuration' page in the Lantronix web UI. The breadcrumb trail is 'Home > Configuration > Security > Switch > SNMP > Trap'. The form fields are: Trap Config Name (empty), Trap Mode (Disabled), Trap Version (SNMP v2c), Trap Community (public), Trap Destination Address (empty), Trap Destination Port (162), Trap Inform Mode (Disabled), Trap Inform Timeout (seconds) (3), Trap Inform Retry Times (5), Trap Probe Security Engine ID (Enabled), Trap Security Engine ID (empty), and Trap Security Name (None). There are 'Apply' and 'Reset' buttons.

Figure 3-5.1.6.2: SNMP Trap Configuration

Parameter descriptions:

Trap Config Name: Set the trap Configuration's name for configuring. The allowed string length is 1 – 32 characters and the allowed content is ASCII characters 33 - 126.

Trap Mode: Indicates the trap mode operation. Possible modes are:

Disabled: Disable SNMP trap mode operation (default).

TCP: Enable TCP SNMP mode operation.

UDP: Enable UDP SNMP mode operation.

Disabled ▼
Disabled
UDP
TCP

Trap Version : Indicates the SNMP trap supported version. Possible versions are:

SNMPv1: Set SNMP trap supported version 1.

SNMPv2c: Set SNMP trap supported version 2c.

SNMPv3: Set SNMP trap supported version 3.

Trap Community: Indicates the community access string when sending SNMP trap packet. The allowed string length is 0 to 255 characters, and the allowed content is ASCII characters from 33 - 126.

Trap Destination Address: Indicates the SNMP trap destination address. It allows a valid IP address in dotted decimal notation ('x.y.z.w'). It also allows a valid hostname. A valid hostname is a string drawn from the alphabet (A-Za-z), digits (0-9), dot (.), dash (-). Spaces are not allowed, the first character must be an alpha character, and the first and last characters must not be a dot or a dash. Indicates the SNMP trap destination IPv6 address. IPv6 address is in 128-bit records represented as eight fields of up to four hexadecimal digits with a colon separating each field (:). For example, 'fe80::215:c5ff:fe03:4dc7'. The symbol '::' is a special syntax that can be used as a shorthand way of representing multiple 16-bit groups of contiguous zeros; but it can appear only once. It can also represent a legally valid IPv4 address. For example, '::192.1.2.34'.

Trap Destination Port: Indicates the SNMP trap destination port. SNMP Agent will send SNMP message via this port, the port range is 1~65535.

Trap Config Name: Indicates which trap Configuration's name for configuring. The allowed string length is 1 to 32 characters, and the allowed content is ASCII characters 33-126.

Trap Inform Mode : Indicates the SNMP mode operation. Possible modes are:

Enabled: Enable SNMP mode operation.

Disabled: Disable SNMP mode operation.

Trap Inform Timeout (seconds): Indicates the SNMP trap inform timeout. The allowed range is 0-2147.

Trap Inform Retry Times: Indicates the SNMP trap inform retry times. The allowed range is 0-255.

Trap Probe Security Engine ID: Indicates the SNMP trap probe security engine ID mode of operation.

Possible values are:

Enabled: Enable SNMP trap probe security engine ID mode of operation.

Disabled: Disable SNMP trap probe security engine ID mode of operation.

Trap Security Engine ID: Indicates the SNMP trap security engine ID. SNMPv3 sends traps and informs using USM for authentication and privacy. A unique engine ID for these traps and informs is needed. When "Trap Probe Security Engine ID" is enabled, the ID will be probed automatically. Otherwise, the ID specified in this field is used. The string must contain an even number(in hexadecimal format) with number of digits between 10 and 64, but all-zeros and all-'F's are not allowed.

Trap Security Name : Indicates the SNMP trap security name. SNMPv3 traps and informs using USM for authentication and privacy. A unique security name is needed when traps and informs are enabled.

Buttons

Add New Entry : Click to add a new user.

Apply : Click to save changes.

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

Example:

The screenshot displays the 'Trap Configuration' page. On the left is a navigation menu with 'Switch' and 'DMS' tabs, and a 'Configuration' section expanded to show 'Security' > 'Switch'. The main content area has a breadcrumb trail: Home > Configuration > Security > Switch > SNMP > Trap. The 'Global Settings' section contains a 'Mode' dropdown menu currently set to 'Enabled'. The 'Trap Destination Configurations' section features a table with the following data:

Delete	Name	Mode	Version	Destination Address	Destination Port
<input type="checkbox"/>	trap1	TCP	SNMPv2c	192.168.1.30	162
<input type="checkbox"/>	trap2	TCP	SNMPv2c	192.168.1.40	162
<input type="checkbox"/>	trap3	Disabled	SNMPv2c	192.168.1.50	162

Below the table are three buttons: 'Add New Entry' (blue), 'Apply' (blue), and 'Reset' (orange).

You can click a linked Name to display its edit page.

3-5.1.6.3 Communities

This function is used to configure SNMPv3 communities. The entry index key is Community. To configure SNMP Communities in the web UI:

1. Click Configuration, Security, Switch, SNMP and Communities.
2. Click the Add New Entry button.
3. Specify the SNMP community's parameters.
4. Click Apply.
5. To modify or clear the settings click Reset.

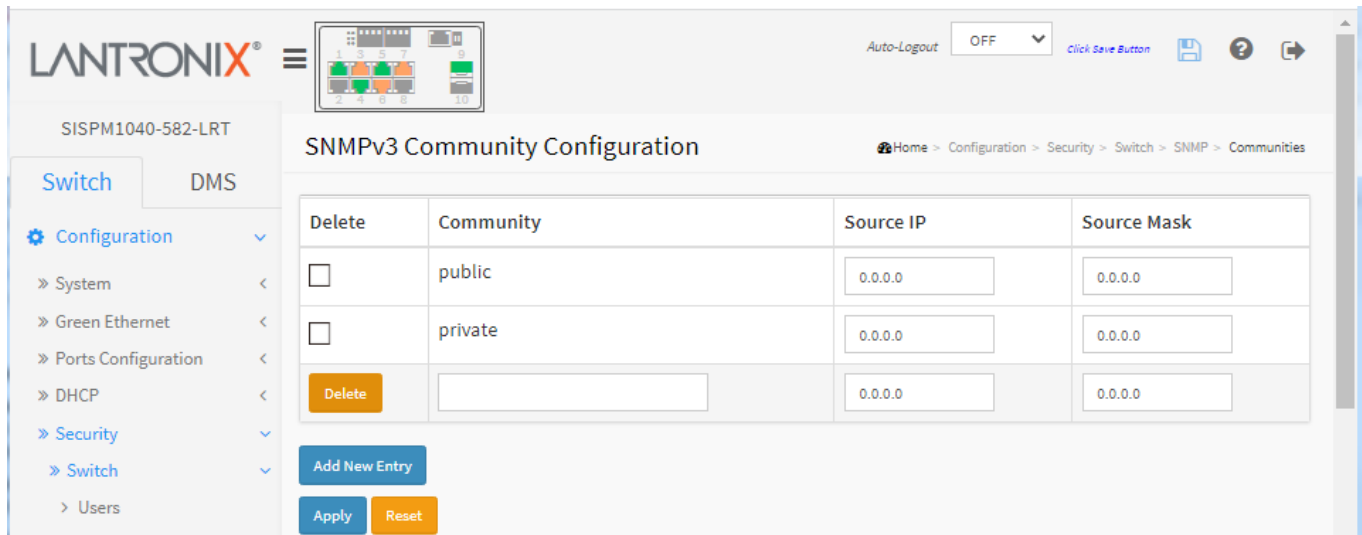


Figure 3-5.1.6.3: SNMPv3 Community Configuration

Parameter descriptions:

Community : Indicates the community access string to permit access to SNMPv3 agent. The allowed string length is 1-32 characters, and the allowed content is ASCII characters 33-126. The community string will be treated as security name and map a SNMPv1 or SNMPv2c community string.

Source IP : Indicates the SNMP access source address. A particular range of source addresses can be used to restrict source subnet when combined with source mask.

Source Mask : Indicates the SNMP access source address mask.

Buttons

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

Add New Entry : Click to add a new Community entry.

Apply : Click to save changes.

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

Example:

The screenshot displays the 'SNMPv3 Community Configuration' page in the LANTRONIX web interface. The interface includes a left-hand navigation menu with categories like 'Switch' and 'DMS'. The main content area shows a table of configurations with columns for 'Delete', 'Community', 'Source IP', and 'Source Mask'. Below the table are three buttons: 'Add New Entry', 'Apply', and 'Reset'. The breadcrumb trail at the top right indicates the path: Home > Configuration > Security > Switch > SNMP > Communities.

Delete	Community	Source IP	Source Mask
<input type="checkbox"/>	public	0.0.0.0	0.0.0.0
<input type="checkbox"/>	private	0.0.0.0	0.0.0.0
<input type="checkbox"/>	SnmpCmmnty-1	192.168.1.30	255.255.255.0
<input type="checkbox"/>	SnmpCmmnty-2	192.168.1.30	255.255.255.0
<input type="checkbox"/>	SnmpCmmnty-3	192.168.1.40	255.255.255.0
<input type="checkbox"/>	SnmpCmmnty-4	192.168.1.50	255.255.255.0
<input type="checkbox"/>	SnmpCmmnty-5	192.168.1.60	255.255.255.0
<input type="checkbox"/>	SnmpCmmnty-6	192.168.1.30	255.255.255.0
<input type="checkbox"/>	SnmpCmmnty-8	192.168.1.30	255.255.255.0
<input type="checkbox"/>	SnmpCmmnty-9	192.168.1.30	255.255.255.0

3-5.1.6.4 Users

This page lets you configure SNMPv3 users. The Entry index key is UserName. The maximum number of Users is 10. To configure SNMP Users in the web UI:

1. Click Configuration, Security, Switch, SNMP and Users.
2. Specify the Privilege parameter.
3. Click Apply.

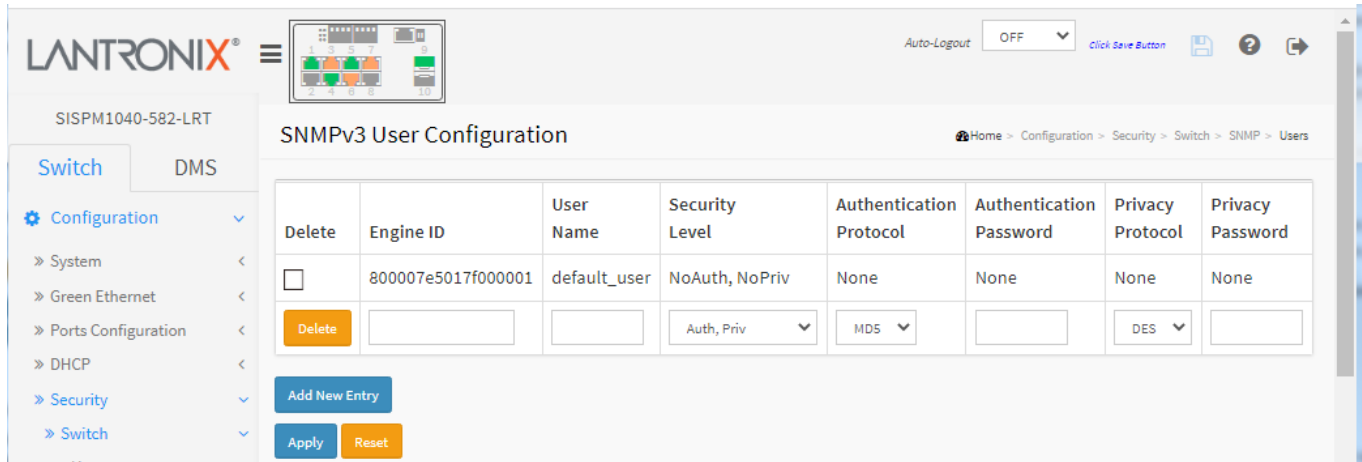


Figure 3-5.1.6.4: SNMPv3 Users Configuration

Parameter descriptions:

Engine ID : An octet string identifying the engine ID that this entry should belong to. The string must contain an even number (in hexadecimal format) with the number of digits from 10-64, but all-zeros and all-'F's are not allowed. The SNMPv3 architecture uses the User-based Security Model (USM) for message security and the View-based Access Control Model (VACM) for access control. For the USM entry, the usmUserEngineID and usmUserName are the entry's keys. In a simple agent, usmUserEngineID is always that agent's own snmpEngineID value. The value can also take the value of the snmpEngineID of a remote SNMP engine with which this user can communicate. In other words, if user engine ID equal system engine ID then it is local user; otherwise it's remote user.

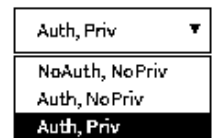
User Name : A string identifying the user name that this entry should belong to. The allowed string length is 1-32 characters, and the allowed content is ASCII characters 33-126.

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 an entry already exists. That means it must first be ensured that the value is set correctly.

Authentication Protocol : Indicates the authentication protocol that this entry should belong to. Possible authentication protocols are:

None: No authentication protocol (default_user only).

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.

MD5	▼
MD5	
SHA	

Authentication Password : A string identifying the authentication password phrase. For MD5 authentication protocol, the allowed string length is 8 to 32 characters. For SHA authentication protocol, the allowed string length is 8 to 40. The allowed content is ASCII characters 33 - 126.

Privacy Protocol : Indicates the privacy protocol that this entry should belong to. Possible privacy protocols are:

None: No privacy protocol.

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
Protocol

None

DES	▼
DES	
AES	

Privacy Password : A string identifying the privacy password phrase. The allowed string length is 8 to 32 characters, and the allowed content is ASCII characters 33 - 126.

Buttons

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

Add New Entry : Click to add a new user entry.

Apply : Click to save changes.

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

Messages:

The 'Engine ID' string must contain an even number between 10 and 64 hexadecimal digits, but all-zeros and all-'F's are not allowed

The length of 'MD5 Authentication Password' is restricted to 8 - 32

3-5.1.6.5 Groups

This page lets you configure SNMPv3 groups. The Entry index key are Security Model and Security Name. The maximum number of Groups for SNMP v1 is 2 groups, for SNMP v2 the max is 2 groups, and for SNMP v3 the max is 10 groups.

To configure SNMP Groups in the web UI:

1. Click Configuration, Security, Switch, SNMP and Groups.
2. Specify the Group Name parameters.
3. Click Apply.

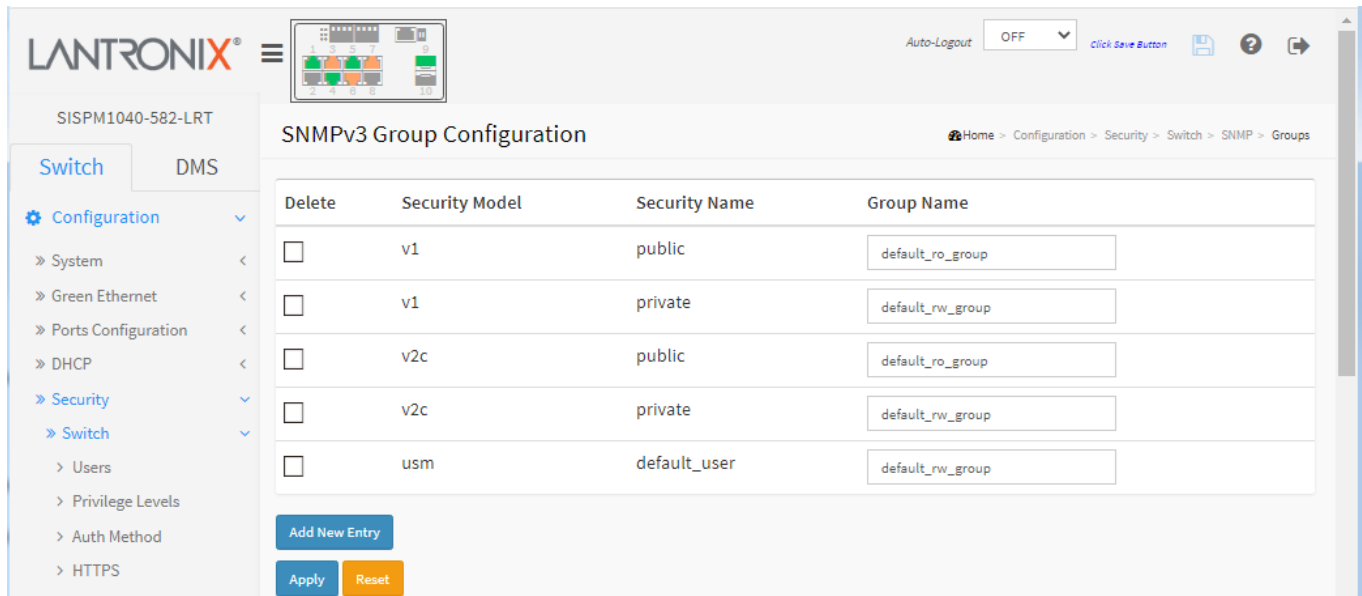


Figure 3-5.1.6.5: SNMP Groups Configuration

Parameter descriptions:

Security Model : Indicates the security model that this entry should belong to. Possible security models are:

- v1**: Reserved for SNMPv1.
- v2c**: Reserved for SNMPv2c.
- usm**: User-based Security Model (USM).

Security Name : A string identifying the security name that this entry should belong to. The allowed string length is 1 – 32 characters, and the allowed content is ASCII characters 33 - 126.

Group Name : A string identifying the group name that this entry should belong to. The allowed string length is 1 – 32 characters, and the allowed content is ASCII characters 33 - 126.

Buttons

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

Add New Entry : Click to add a new group entry.

Apply : Click to save changes.

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

3-5.1.6.6 Views

This page lets you configure SNMPv3 views. The Entry index keys are OID Subtree and View Name. The maximum number of Groups allowed is 28.

To configure SNMP Views in the web UI:

1. Click Configuration, Security, Switch, SNMP and Views.
2. Click Add New View.
3. Specify the SNMP View parameters.
4. Click Apply.

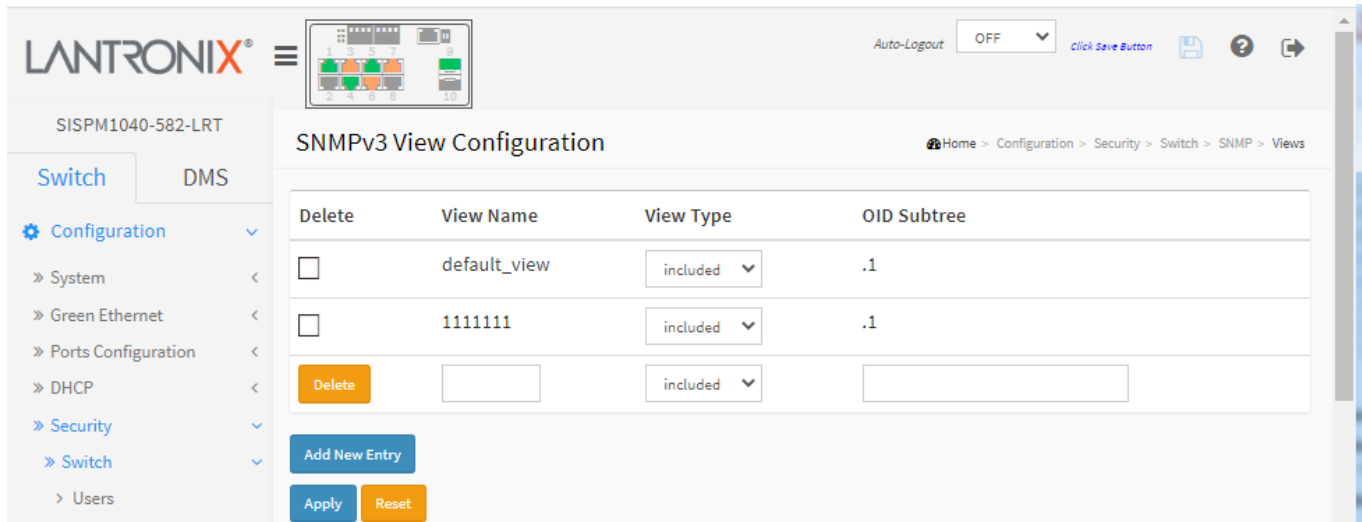


Figure 3-5.1.6.6: SNMP Views Configuration

Parameter descriptions:

View Name : A string identifying the view name that this entry should belong to. The allowed string length is 1 – 32 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 its 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 characters. The allowed string content is digital number or asterisk (*).

Buttons

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

Add New Entry : Click to add a new view entry.

Apply : Click to save changes.

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

3-5.1.6.7 Access

This page lets you configure SNMPv3 accesses. The Entry index keys are Group Name, Security Model, and Security level. The maximum number of entries is 16.

To configure SNMP Access in the web UI:

1. Click Configuration, Security, Switch, SNMP and Accesses.
2. Click Add New Access.
3. Specify the SNMP Access parameters.
4. Click Apply.
5. If you want to modify or clear the settings click Reset.

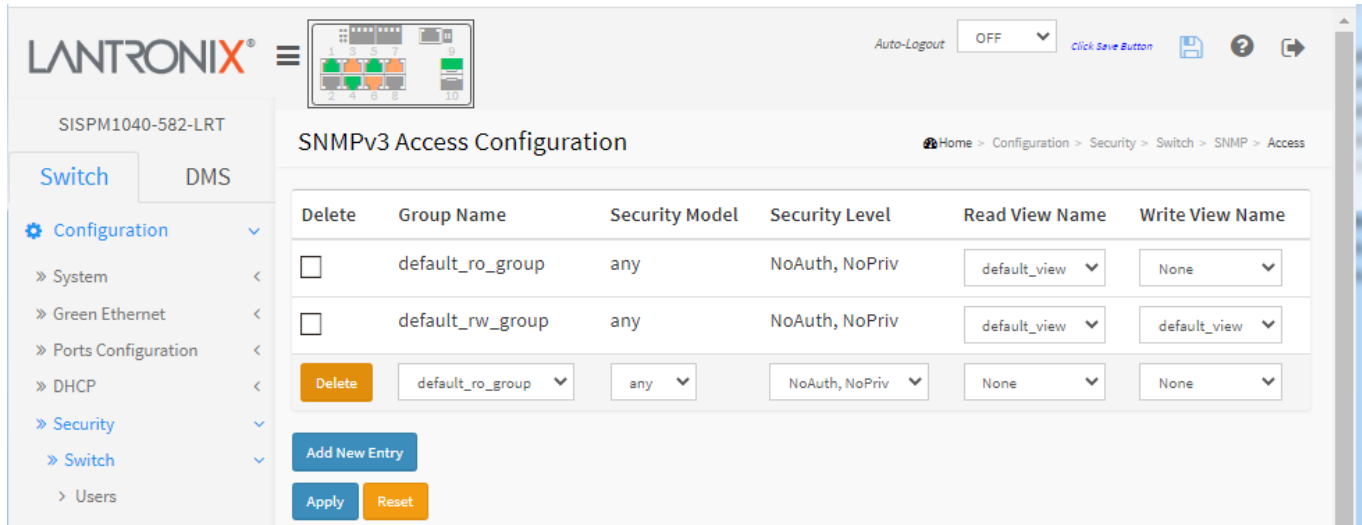


Figure 3-5.1.6.7: SNMP Access Configuration

Parameter description:

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.

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 - 32 characters, and valid 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 1-32 characters, and the allowed content is ASCII characters 33 - 126.

Buttons

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

Add New Entry : Click to add a new access entry.

Apply : Click to save changes.

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

Messages:

The maximum number of entries is 16

The entry 'default_ro_groupv1-1, any, Auth, NoPriv' already exists

3-5.1.7 RMON

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

The Remote Network Monitoring (RMON) MIB was developed by the IETF to support monitoring and protocol analysis of LANs. RMON is an industry-standard specification that provides much of the functionality offered by proprietary network analyzers.

3-5.1.7.1 Statistics

Configure RMON Statistics table on this page. The entry index key is ID. To configure RMON Statistics:

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

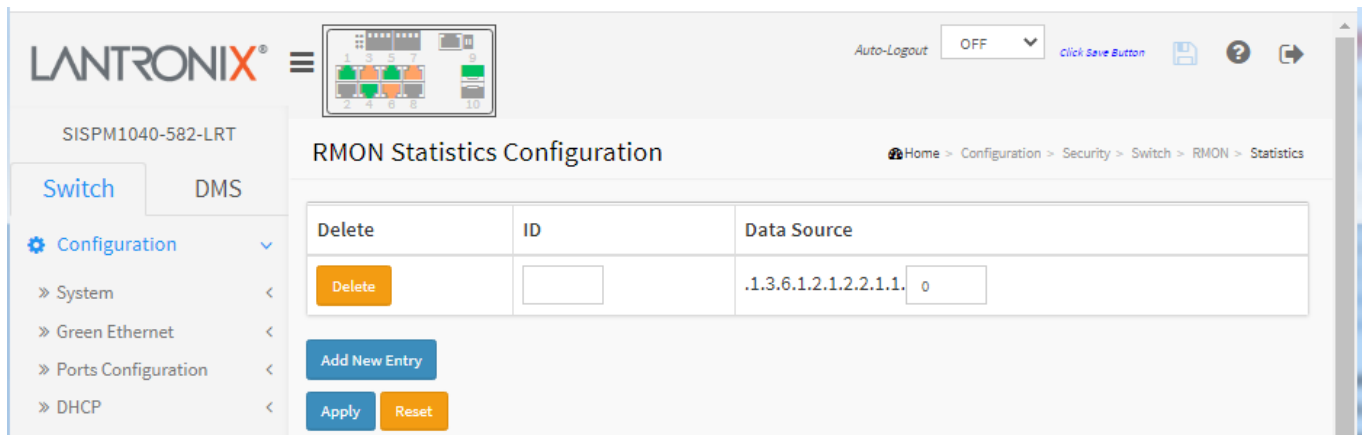


Figure 3-5.1.7.1: RMON Statics Configuration

Parameter descriptions:

ID : Indicates the index of the entry. The range is 1 – 65535 characters.

Data Source : Indicates the port ID which you want to be monitored.

Buttons

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

Add New Entry : Click to add a new community entry.

Apply : Click to save changes.

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

3-5.1.7.2 History

Configure the RMON History table on this page. The entry index key is ID. To configure RMON History in the web UI:

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

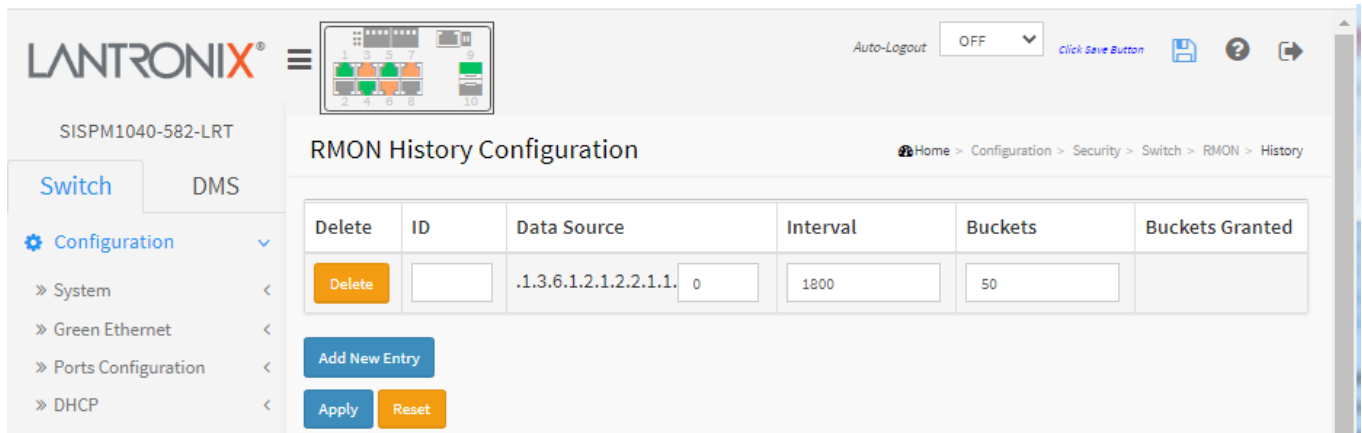


Figure 3-5.1.7.2: RMON History Configuration

Parameter descriptions:

ID : Indicates the index of the entry. The range is from 1 to 65535.

Data Source : Indicates the port ID which wants to be monitored.

Interval : Indicates the interval in seconds for sampling the history statistics data. The range is 1-3600 seconds; the default is 1800 seconds.

Buckets : Indicates the maximum data entries associated this History control entry stored in RMON. The range is 1-3600 buckets; the default value is 50 buckets.

Buckets Granted : The number of data to be saved in the RMON.

Buttons

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

Add New Entry : Click to add a new history entry.

Apply : Click to save changes.

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

3-5.1.7.3 Alarm

Configure RMON Alarm table on this page. The entry index key is ID.

Web Interface

To configure RMON Alarms in the web UI:

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

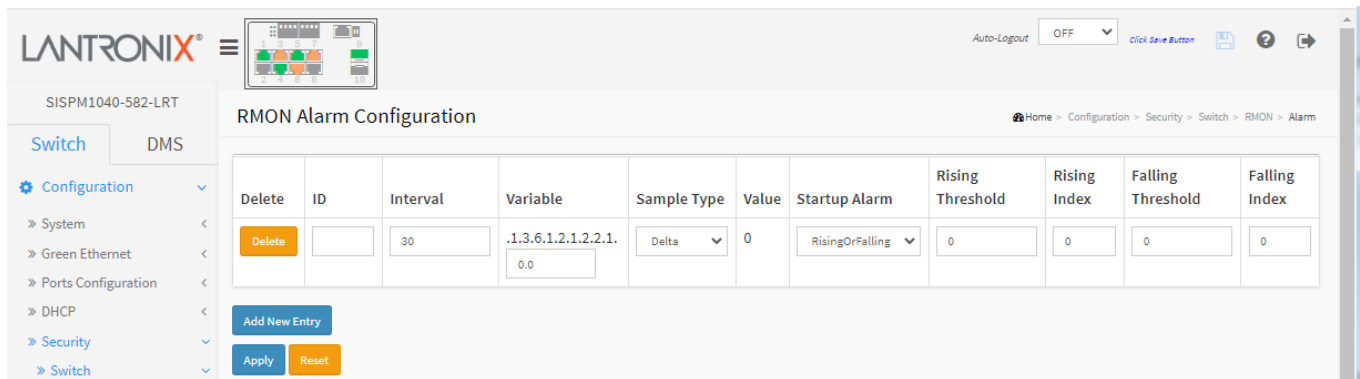


Figure 3-5.1.7.3: RMON Alarm Configuration

Parameter descriptions:

ID : Indicates the index of the entry. The range is 1 - 65535.

Interval : Indicates the interval in seconds for sampling and comparing the rising and falling threshold. The range is from 1 to $2^{31}-1$.

Variable : Indicates the particular variable to be sampled, the possible variables are:

InOctets: The total number of octets received on the interface, including framing characters.

InUcastPkts: The number of uni-cast packets delivered to a higher-layer protocol.

InNUcastPkts: The number of broad-cast and multi-cast packets delivered to a higher-layer protocol.

InDiscards: The number of inbound packets that are discarded even the packets are normal.

InErrors: The number of inbound packets that contained errors preventing them from being deliverable to a higher-layer protocol.

InUnknownProtos: the number of the inbound packets that were discarded because of the unknown or un-support protocol.

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

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

OutNUcastPkts: The number of broad-cast and multi-cast packets that request to transmit.

OutDiscards: The number of outbound packets that are discarded event the packets is normal.

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

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

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

Absolute: Get the sample directly.

Delta: Calculate the difference between samples (default).

Value : The value of the statistic during the last sampling period.

Startup Alarm : The method of sampling the selected variable and calculating the value to be compared against the thresholds; possible sample types are:

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

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

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

Rising Threshold : Rising threshold value (-2147483648-2147483647).

Rising Index : Rising event index (1-65535).

Falling Threshold : Falling threshold value (-2147483648-2147483647)

Falling Index : Falling event index (1-65535).

Buttons

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

Add New Entry : Click to add a new alarm entry.

Apply : Click to save changes.

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

Messages:

Variable value is xxx.yyy, xxx is 10-21, yyy is 1-65535

'Rising threshold' must be an integer value between 1 and 2147483647

'Rising Index' must be an integer value between 1 and 65535

'Falling threshold' must be an integer value between 1 and 2147483647

'Falling Index' must be an integer value between 1 and 65535

'Rising threshold' must be larger than 'Falling threshold'

3-5.1.7.4 Event

Configure the RMON Event table on this page. The entry index key is ID.

To configure RMON Events in the web UI:

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

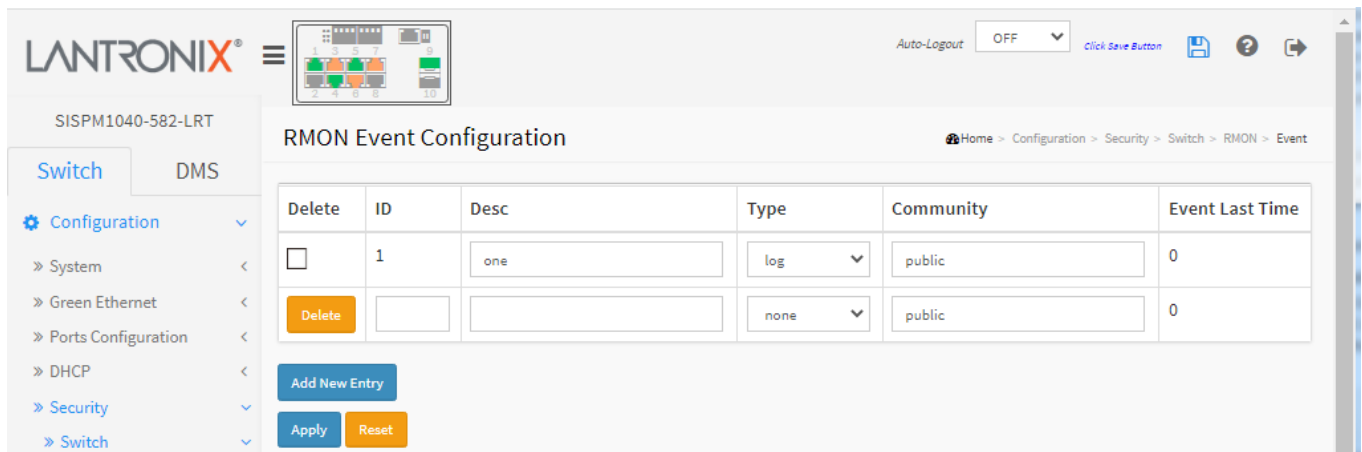


Figure 3-5.1.7.4: RMON Event Configuration

Parameter descriptions:

ID : Indicates the index of the entry. The valid range is 1 - 65535.

Desc : Indicates this event, valid string length is 0 - 127; default is a null string.

Type : Indicates the notification of the event, the possible types are:

none: No SNMP log is created; no SNMP trap is sent.

log: Create SNMP log entry when the event is triggered.

snmptrap: Send SNMP trap when the event is triggered.

logandtrap: Create SNMP log entry and sent SNMP trap when the event is triggered.

Community : Specify the community when trap is sent, valid string length is 0 - 127 characters; the default is "public".

Event Last Time : Indicates the value of sysUpTime at the time this event entry last generated an event.

Buttons

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

Add New Entry :Click to add a new event entry.

Apply : Click to save changes.

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

3-5.2 Network

3-5.2.1 Limit Control

This page lets you configure the Port Security Limit Control system and port settings. Limit Control allows for limiting the number of users on a given port. A user is identified by a MAC address and VLAN ID. If Limit Control 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. The action can be one of the four different actions as described below. The Limit Control module utilizes a lower-layer module, Port Security module, which manages MAC addresses learnt on the port.

To configure Port Security Limit Control in the web UI:

1. Click Configuration > Security > Network > Limit Control.
2. Select “Enabled” in the Mode of System Configuration.
3. Check Aging Enabled.
4. Set Aging Period (default is 3600 seconds).

To configure Port Limit Control in the web UI:

1. Select “Enabled” in the Mode of Port Configuration.
2. Specify the maximum number of MAC addresses in the Limit of Port Configuration.
3. Set Action (Trap, Shutdown, or Trap & Shutdown) and Sticky.
4. Click Apply.

The screenshot shows the 'Port Security Limit Control Configuration' page in the Lantronix web UI. The page is titled 'SISPM1040-582-LRT' and has a breadcrumb trail: Home > Configuration > Security > Network > Limit Control. The left sidebar shows the navigation menu with 'Limit Control' selected under 'Network'. The main content area is divided into two sections: 'System Configuration' and 'Port Configuration'.

System Configuration:

- Mode: Disabled (dropdown)
- Aging Enabled:
- Aging Period: 3600 seconds

Port Configuration:

Port	Mode	Limit	Action	State	Re-open	Sticky	Clear
*	↔	4	↔			↔	
1	Disabled	4	None	Disabled	Reopen	Disabled	Clear
2	Disabled	4	None	Disabled	Reopen	Disabled	Clear
3	Disabled	4	None	Disabled	Reopen	Disabled	Clear
4	Disabled	4	None	Disabled	Reopen	Disabled	Clear
5	Disabled	4	None	Disabled	Reopen	Disabled	Clear
6	Disabled	4	None	Disabled	Reopen	Disabled	Clear
7	Disabled	4	None	Disabled	Reopen	Disabled	Clear
8	Disabled	4	None	Disabled	Reopen	Disabled	Clear

Figure 3-5.2.1: Port Security Limit Control Configuration

Parameter descriptions:**System Configuration section**

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

Aging Enabled : If checked, secured MAC addresses are subject to aging as discussed under Aging Period.

Aging Period : If Aging Enabled is checked, then the aging period is controlled with this input. If other modules are using the underlying port security for securing MAC addresses, they may have other requirements to the aging period. The underlying port security will use the shorter requested aging period of all modules that use the functionality.

The Aging Period can be set to 10 - 10,000,000 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 Limit Control 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.

Port Configuration section: The table has one row for each port on the selected switch and a number of columns:

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

Mode : Controls whether Limit Control is enabled on this port. Both this and the Global Mode must be set to Enabled for Limit Control to be in effect. Notice that other modules may still use the underlying port security features without enabling Limit Control on a given port.

Limit : The maximum number of MAC addresses that can be secured on this port. This number cannot exceed 1024. If the limit is exceeded, the corresponding action is taken. The switch is "born" with a total number of MAC addresses from which all ports draw whenever a new MAC address is seen on a Port Security-enabled port. Since all ports draw from the same pool, it may happen that a configured maximum cannot be granted, if the remaining ports have already used all available MAC addresses.

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

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

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

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

- 1) Boot the switch,
- 2) Disable and re-enable Limit Control on the port or the switch,
- 3) Click the Reopen button.

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

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

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

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

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

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

Re-open button : If a port is shut down by this module, you may reopen it by clicking this button, which will only be enabled if this is the case. For other methods, refer to shut down in the Action section. **Note**: Clicking the Re-open button causes the page to be refreshed, so non-committed changes will be lost .

Sticky : If running config has sticky MAC address, then these MAC addresses are automatically set to be static MAC addresses on the MAC Table.

Clear button : Click to clear the static MAC addresses added by the sticky function.

Buttons

Refresh: Click to refresh the Port Security information manually.

Apply : Click to save changes.

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

3-5.2.2 NAS Configuration

Navigate to System > Configuration > Security > Network > NAS to display the Network Access Server Configuration page. Here you configure IEEE 802.1X and MAC-based authentication system and port parameters.

The IEEE 802.1X standard defines a port-based access control procedure that prevents unauthorized access to a network by requiring users to first submit credentials for authentication. One or more central servers, the backend servers, determine whether the user is allowed access to the network. These backend (RADIUS) servers are configured on the "Configuration > Security > AAA" page. The IEEE802.1X standard defines port-based operation, but non-standard variants overcome security limitations as shall be explored below.

MAC-based authentication allows for authentication of more than one user on the same port and doesn't require the user to have special 802.1X supplicant software installed on his system. The switch uses the user's MAC address to authenticate against the backend server. Intruders can create counterfeit MAC addresses, which makes MAC-based authentication less secure than 802.1X authentication.

To configure a Network Access Server in the web UI:

1. Click Configuration, Security, Network, and NAS.
2. Set the System Configuration section parameters.
3. Set the Port Configuration section parameters.
4. Click Apply.

The screenshot displays the 'Network Access Server Configuration' page in the Lantronix web UI. The page is divided into two main sections: 'System Configuration' and 'Port Configuration'.

System Configuration:

- Mode: Disabled
- 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
*	<>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>		
1	Force Authorized	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Globally Disabled	Reauthenticate Reinitialize
2	Force Authorized	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Globally Disabled	Reauthenticate Reinitialize
3	Force Authorized	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Globally	Reauthenticate Reinitialize

Figure 3-5.2.2: Network Access Server Configuration

Parameter descriptions: The NAS Configuration page has two sections: System Configuration and Port Configuration.

System Configuration

Mode : Indicates if NAS is globally enabled or disabled on the switch. If globally disabled, all ports are allowed forwarding of frames.

Reauthentication Enabled : If checked, successfully authenticated supplicants/clients are reauthenticated after the interval specified by the Reauthentication Period. Reauthentication for 802.1X-enabled ports can be used to detect if a new device is plugged into a switch port or if a supplicant is no longer attached. For MAC-based ports, reauthentication is only useful if the RADIUS server configuration has changed. It does not involve communication between the switch and the client, and therefore doesn't imply that a client is still present on a port (see Aging Period below).

Reauthentication Period : Determines the period, in seconds, after which a connected client must be reauthenticated. This is only active if the Reauthentication Enabled checkbox is checked. Valid values are 1 to 3600 seconds.

EAPOL Timeout : Determines the time for retransmission of Request Identity EAPOL frames. Valid values are 1- 65535 seconds. This has no effect for MAC-based ports.

Aging Period : This setting applies to the following modes (i.e., modes using the Port Security functionality to secure MAC addresses):

- Single 802.1X
- Multi 802.1X
- MAC-Based Auth.

When the NAS module uses the Port Security module to secure MAC addresses, the Port Security module needs to check for activity on the MAC address in question at regular intervals and free resources if no activity is seen within a given time 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 functionality to secure MAC addresses):

- Single 802.1X
- Multi 802.1X
- MAC-Based Auth.

If a client is denied access - either because the RADIUS server denies the client access or because the RADIUS server request times out (according to the timeout specified on the "Configuration > Security > AAA" page) - the client is put on hold in the Unauthorized state. The hold timer does not count during an on-going authentication.

In MAC-based Auth. mode, the switch will ignore new frames coming from the client during the hold time. The Hold Time can be set to a number between 10 and 1000000 seconds.

RADIUS-Assigned QoS Enabled : 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. This value can only be changed if the Guest VLAN option is globally enabled. Valid values are 1-4095.

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. This value can only be changed if the Guest VLAN option is globally enabled. Valid values are 1-255.

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

Port Configuration : The table has one row for each port on the switch and several columns:

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

Admin State : If NAS is globally enabled, this selection controls the port's authentication mode. These modes are available:

Force Authorized : In this mode, the switch will send one EAPOL Success frame when the port link comes up, and any client on the port will be allowed network access without authentication.

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).

Admin State

A dropdown menu with a downward arrow on the right. The menu is currently open, showing a list of options. The first option is selected and highlighted in black. The options are:

- Force Authorized
- Force Unauthorized
- Port-based 802.1X
- Single 802.1X
- Multi 802.1X
- MAC-based Auth.

Frames sent between the switch and the RADIUS server are RADIUS packets. RADIUS packets also encapsulate EAP PDUs together with other attributes like the switch's IP address, name, and the supplicant's port number on the switch. EAP is very flexible, in that it allows for different authentication methods, like MD5-Challenge, PEAP, and TLS. The important thing is that the authenticator (the switch) doesn't need to know which authentication method the supplicant and the authentication server are using, or how many information exchange frames are needed for a particular method. The switch simply encapsulates the EAP part of the frame into the relevant type (EAPOL or RADIUS) and forwards it.

When authentication is complete, the RADIUS server sends a special packet containing a success or failure indication. Besides forwarding this decision to the supplicant, the switch uses it to open up or block traffic on the switch port connected to the supplicant.

Note: Suppose two backend servers are enabled and that the server timeout is configured to X seconds (using the AAA configuration page), and suppose that the first server in the list is currently down (but not considered dead). Now, if the supplicant retransmits EAPOL Start frames at a rate faster than X seconds, then it will never get authenticated, because the switch will cancel on-going backend authentication server requests whenever it receives a new EAPOL Start frame from the supplicant. And since the server hasn't yet failed (because the X seconds haven't expired), the same server will be contacted upon the next backend authentication server request from the switch. This scenario will loop forever. Therefore, the server timeout should be smaller than the supplicant's EAPOL Start frame retransmission rate.

Single 802.1X : In port-based 802.1X authentication, once a supplicant is successfully authenticated on a port, the whole port is opened for network traffic. This allows other clients connected to the port (for instance through a hub) to piggy-back on the successfully authenticated client and get network access even though they really aren't authenticated. To overcome this security breach, use the Single 802.1X variant. Single 802.1X is really not an IEEE standard, but features many of the same characteristics as does port-based 802.1X. In Single 802.1X, at most one supplicant can get authenticated on the port at a time. Normal EAPOL frames are used in the communication between the supplicant and the switch. If more than one supplicant is connected to a port, the one that comes first when the port's link comes up will be the first one considered. If that supplicant doesn't provide valid credentials within a certain amount of time, another supplicant will get a chance. Once a supplicant is successfully authenticated, only that supplicant will be allowed access. This is the most secure of all the supported modes. In this mode, the Port Security module is used to secure a supplicant's MAC address once successfully authenticated.

Multi 802.1X : 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 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 meantime without affecting the RADIUS-assigned). This option is only available for single-client modes, i.e.:

- Port-based 802.1X
- Single 802.1X

RADIUS attributes used in identifying a QoS Class : The User-Priority-Table attribute defined in [RFC4675](#) forms the basis for identifying the QoS Class in an Access-Accept packet. Only the first occurrence of the attribute in the packet will be considered, and to be valid, it must follow this rule:

- All 8 octets in the attribute's value must be identical and consist of ASCII characters in the range '0' - '7', which translates into the desired QoS Class in the range 0-7.

RADIUS-Assigned VLAN Enabled : When RADIUS-Assigned VLAN is both globally enabled and enabled (checked) for a given port, the switch reacts to VLAN ID information carried in the RADIUS Access-Accept packet transmitted by the RADIUS server when a supplicant is successfully authenticated. If present and valid, the port's Port VLAN ID will be changed to this VLAN ID, the port will be set to be a member of that VLAN ID, and the port will be forced into VLAN unaware mode. Once assigned, all traffic arriving on the port will be classified and switched on the RADIUS-assigned VLAN ID. If (re-)authentication fails or the RADIUS Access-Accept packet no longer carries a VLAN ID or it's invalid, or the supplicant is otherwise no longer present on the port, the port's VLAN ID is immediately reverted to the original VLAN ID (which may be changed by the administrator in the meanwhile without affecting the RADIUS-assigned). This option is only available for single-client modes, i.e.:

- Port-based 802.1X
- Single 802.1X

For trouble-shooting VLAN assignments, use the "Monitor > VLANs > VLAN Membership and VLAN Port" pages. These pages show which modules have (temporarily) overridden the current Port VLAN configuration.

RADIUS attributes used in identifying a VLAN ID: IETF [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 has the same Tag value and fulfils these 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 these values:

Globally Disabled : NAS is globally disabled.

Link Down : NAS 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.

Reauthenticate : Schedules a reauthentication whenever the quiet-period of the port runs out (EAPOL-based authentication). For MAC-based authentication, reauthentication 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 reinitialization of the clients on the port and thereby a reauthentication immediately. The clients will transfer to the unauthorized state while the reauthentication is in progress.

Buttons

Refresh: You can click them for refresh the NAS Configuration by manual.

Apply : Click to save changes.

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

Message: *NAS Error The 802.1X Admin State must be set to Authorized for ports that are enabled for Spanning Tree*

Recovery: **1.** Click the Previous button. **2.** Disable STP for the related ports at Configuration > Spanning Tree > CIST Port.

Note: SISPM1040-582-LRT FW VB7.20.0039 adds RADIUS Server Attribute 6 - Service-Type attribute option when authenticating with RADIUS:

- For **MAC authentication**, the service-type is set to "**Call-Check**".
- For **Dot1x authentication**, the service-type is set to "**Framed**".
- For **Captive portal authentication**, the service-type is set to "**Login**". A captive portal is a web page accessed with a web browser that displays to a newly-connected network user (Wi-Fi or wired) before they are granted broader access to network resources.

3-5.2.3 ACL

An ACL (Access Control List) is used for packet filtering and also for selecting types of traffic to be analyzed, forwarded, or influenced in some way. The ACLs are divided into Ether Types (IPv4, ARP protocol, MAC and VLAN parameters, etc.).

An ACL is a list table of ACEs, containing access control entries that specify individual users or groups permitted or denied to specific traffic objects, such as a process or a program. Each accessible traffic object contains an identifier to its ACL. The privileges determine whether there are specific traffic object access rights.

AN ACE (Access Control Entry) describes access permission associated with a particular ACE ID. There are three ACE frame types (Ethernet Type, ARP, and IPv4) and two ACE actions (permit and deny). The ACE also contains many different, detailed parameter options that are available for individual application.

An ACL implementation can be quite complex, for example, when the ACEs are prioritized for the various situation. In networking, the ACL refers to a list of service ports or network services that are available on a host or server, each with a list of hosts or servers permitted or denied use of the service. ACL can generally be configured to control inbound traffic, and in this context, they are similar to firewalls.

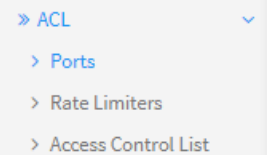
There are 3 webpages associated with the manual ACL configuration:

1. ACL > Access Control List: The web page shows the ACEs in a prioritized way, highest (top) to lowest (bottom). Default the table is empty. An ingress frame will only get a hit on one ACE even though there are more matching ACEs. The first matching ACE will take action (permit/deny) on that frame and a counter associated with that ACE is incremented. An ACE can be associated with a Policy, 1 ingress port, or any ingress port (the whole switch).

If an ACE Policy is created then that Policy can be associated with a group of ports under the "Ports" web-page. There are number of parameters that can be configured with an ACE. Read the Web page help text to get further information for each of them. The maximum number of ACEs is 64.

2. ACL > Ports: The ACL Ports configuration is used to assign a Policy ID to an ingress port. This is useful to group ports to obey the same traffic rules. Traffic Policy is created under the "Access Control List" - page. You can you also set up specific traffic properties (Action / Rate Limiter / Port copy, etc.) for each ingress port. They will though only apply if the frame gets past the ACE matching without getting matched. In that case a counter associated with that port is incremented. See the Web page help text for each specific port property.

3. ACL > Rate Limiters: This page lets you configure the rate limiters. There can be 15 different rate limiters, each ranging from 1-1024K packets per seconds. Under the "Ports" and "Access Control List" web-pages you can assign a Rate Limiter ID to the ACE(s) or ingress port(s).



3-5.2.3.1 Ports

This page lets you 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 parameters in the web UI:

1. Click Configuration, Security, Network, ACL and Ports.
2. Specify parameter values and select the correct value for port ACL setting.
3. Click Apply to save the settings.
4. To cancel the settings click the Reset button to revert to previously saved values.
5. View the Counter of the port. Click Refresh to update the counter or click Clear to clear the information.

Port	Policy ID	Action	Rate Limiter ID	EVC Policer	EVC Policer ID	Port Redirect	Mirror	Logging	Shutdown	State	Counter
*	0	<>	<>	<>	1	Disabled Port 1 Port 2	<>	<>	<>	<>	*
1	0	Permit	Disabled	Disabled	1	Disabled Port 1 Port 2	Disabled	Disabled	Disabled	Enabled	17055
2	0	Permit	Disabled	Disabled	1	Disabled Port 1 Port 2	Disabled	Disabled	Disabled	Enabled	58712
3	0	Permit	Disabled	Disabled	1	Disabled Port 1 Port 2	Disabled	Disabled	Disabled	Enabled	714
4	0	Permit	Disabled	Disabled	1	Disabled Port 1 Port 2	Disabled	Disabled	Disabled	Enabled	8962
5	0	Permit	Disabled	Disabled	1	Disabled Port 1 Port 2	Disabled	Disabled	Disabled	Enabled	0
6	0	Permit	Disabled	Disabled	1	Disabled Port 1 Port 2	Disabled	Disabled	Disabled	Enabled	0
7	0	Permit	Disabled	Disabled	1	Disabled Port 1 Port 2	Disabled	Disabled	Disabled	Enabled	0
8	0	Permit	Disabled	Disabled	1	Disabled Port 1 Port 2	Disabled	Disabled	Disabled	Enabled	0

Figure 3-5.2.3.1: ACL Ports Configuration

Parameter descriptions:

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

Policy ID : Select the policy to apply to this port. The allowed values are 1 - 8. The default value is 1.

Action : Select whether forwarding is permitted ("**Permit**") or denied ("**Deny**"). The default value is "**Permit**".

Rate Limiter ID : Select which rate limiter to apply on this port. The allowed values are Disabled or the values 1 through 16. The default value is "Disabled".

EVC Policer : Select whether EVC policer is enabled or disabled. The default value is "Disabled". Note that ACL rate limiter and EVC policer cannot both be enabled.

EVC Policer ID : Select which EVC policer ID to apply on this port. The allowed values are Disabled or the 1 - 256.

Port Redirect : Select which port frames are redirected on. The allowed values are Disabled or a specific port number and it can't be set when action is permitted. The default value is "Disabled".

Mirror : Specify the mirror operation of this port. The allowed values are:

Enabled: Frames received on the port are mirrored.

Disabled: Frames received on the port are not mirrored. The default value is "Disabled".

Logging : Specify the logging operation of this port. The allowed values are:

Enabled: Frames received on the port are stored in the System Log.

Disabled: Frames received on the port are not logged. The default value is "Disabled".

Note that the System Log memory size and logging rate is limited.

Shutdown : Specify the port shut down operation of this port. The allowed values are:

Enabled: If a frame is received on the port, the port will be disabled.

Disabled: Port shut down is disabled. The default value is "Disabled".

State : Specify the port state of this port. The allowed values are:

Enabled: To reopen ports by changing the volatile port configuration of the ACL user module.

Disabled: To close ports by changing the volatile port configuration of the ACL user module.
The default value is "Enabled"

Counter : Counts the number of frames that match this ACE.

Buttons

Refresh: Click to update the page data.

Clear : Click to clear the page data.

Apply : Click to save changes.

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

Messages:

The ACL rate limiter and EVC policer can not both be enabled.

3-5.2.3.2 Rate Limiters

This page lets you configure the switch's ACL Rate Limiter parameters. The Rate Limiter Level (1 - 16) lets you set rate limiter value in units of pps or kbps.

To configure ACL Rate Limiter in the web UI:

1. Click Configuration, Security, Network, ACL and Rate Limiter.
2. Specify the Rate and the range (0 to 3276700).
3. Select the Unit of measure (pps or kbps).
4. Click the Apply to save the settings.
5. To cancel the setting click the Reset button to revert to previously saved values.

Rate Limiter ID	Rate	Unit
*	<input type="text" value="1"/>	<input type="text" value="pps"/>
1	<input type="text" value="1"/>	<input type="text" value="pps"/>
2	<input type="text" value="1"/>	<input type="text" value="pps"/>
3	<input type="text" value="1"/>	<input type="text" value="pps"/>
4	<input type="text" value="1"/>	<input type="text" value="pps"/>
5	<input type="text" value="1"/>	<input type="text" value="pps"/>
6	<input type="text" value="1"/>	<input type="text" value="pps"/>
7	<input type="text" value="1"/>	<input type="text" value="pps"/>
8	<input type="text" value=""/>	<input type="text" value=""/>
9	<input type="text" value=""/>	<input type="text" value=""/>
10	<input type="text" value=""/>	<input type="text" value=""/>
11	<input type="text" value=""/>	<input type="text" value=""/>
12	<input type="text" value=""/>	<input type="text" value=""/>
13	<input type="text" value=""/>	<input type="text" value=""/>
14	<input type="text" value=""/>	<input type="text" value=""/>
15	<input type="text" value=""/>	<input type="text" value=""/>
16	<input type="text" value=""/>	<input type="text" value=""/>

Figure 3-5.2.3.2: ACL Rate Limiter Configuration

Parameter descriptions:

Rate Limiter ID : The rate limiter ID for the settings contained in the same row.

Rate : The allowed values are 0-3276700 in pps or 0, 100, 200, 300, ..., 100000 in kbps.

Unit : Specify the rate unit of measure. Allowed values are:

pps: packets per second.

kbps: Kbits per second.

Buttons

Apply : Click to save changes.

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

3-5.2.3.3 Access Control List

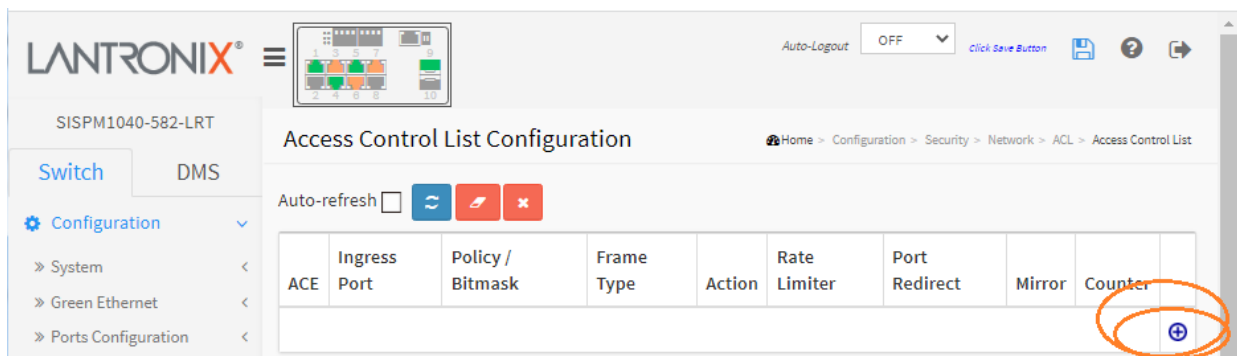
This page lets you configure Access Control List rules. This page shows the Access Control List (ACL), which is made up of the ACEs defined on this switch. Each row describes the ACE that is defined. The maximum number of ACEs is 256 on each switch.


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

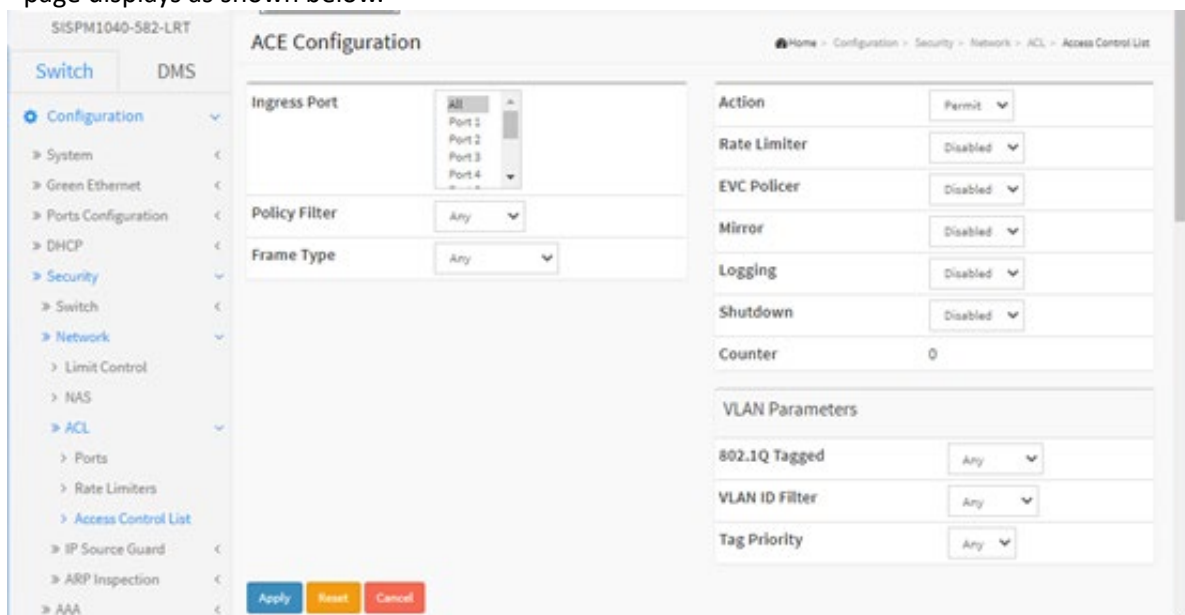
Click on the lowest plus sign to add a new ACE to the list. The reserved ACE is used for internal protocol; it cannot be edited or deleted. The sequence cannot be changed and the priority is highest.

To configure Access Control List in the web UI:

1. Click Configuration, Security, Network, ACL, and Access Control List to display the default Access Control List Configuration page:



2. Click the  button to add a new ACL, or use the other ACL modification buttons to specify the editing action (i.e., edit, delete, or move the relative position of entry in the list). The ACE Configuration page displays as shown below.



3. Specify the ACE parameters.
4. Click the Apply button to save the settings.
5. To cancel the settings, click the Reset button to revert to previously saved values.
6. When editing an entry on the ACE Configuration page, note that the Items displayed depend on various selections, such as Frame Type and IP Protocol Type. Specify the relevant parameters to be matched for this rule, and set the actions to take when a rule is matched (such as Rate Limiter, Port Copy, Logging, and Shutdown).

Parameter descriptions:

Ingress Port : Indicates the ingress port of the ACE. Possible values are:

Any: The ACE will match any ingress port.

Policy: The ACE will match ingress ports with a specific policy.

Port: The ACE will match a specific ingress port.

Policy / Bitmask : Indicates the policy number and bitmask of the ACE.

Frame Type : Select the frame type for this ACE. These frame types are mutually exclusive.

Any: Any frame can match this ACE.

Ethernet Type: Only Ethernet Type frames can match this ACE. The IEEE 802.3 describes the value of Length/Type Field specifications to be greater than or equal to 1536 decimal (equal to 0600 hexadecimal) 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.

ARP
Any
Ethernet Type
ARP
IPv4
IPv6

Action : Indicates the forwarding action of the ACE.

Permit: Frames matching the ACE may be forwarded and learned.

Deny: Frames matching the ACE are dropped.

Filter: Frames matching the ACE are filtered.

Rate Limiter : Indicates the rate limiter number of the ACE. The allowed range is 1 to 16. When Disabled is displayed, the rate limiter operation is disabled. The ACL rate limiter and EVC policer cannot both be enabled.

EVC Policer : Select whether EVC policer is enabled or disabled. The default value is "Disabled". Note that the ACL rate limiter and EVC policer cannot both be enabled.

EVC Policer ID : Select which EVC policer ID to apply on this ACE. The allowed values are Disabled or 1 - 256.

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.

Modification Buttons : You can modify each ACE (Access Control Entry) in the table using these buttons:



: Inserts a new ACE before the current row.



: Edit ACE.



: Move ACE up.



: Move ACE down.



: Delete ACE.



: The lowest plus sign adds a new ACE entry at the bottom of the ACE listings.

ACE Configuration

Ingress Port : Select the ingress port for which this ACE applies.

All: The ACE applies to all port.

Port n: The ACE applies to this port number, where n is the number of the switch port.

Policy Filter : Specify the policy number filter for this ACE.

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

Specific: If you want to filter a specific policy with this ACE, choose this value. Two field for entering a policy value and bitmask appears.

Policy Value : When "Specific" is selected for the policy filter, you can enter a specific policy value. The allowed range is 0 to 255.

Policy Bitmask : When "Specific" is selected for the policy filter, you can enter a specific policy bitmask. The allowed range is 0x0 to 0xff. Notice the usage of bitmask, if the binary bit value is "0", it means this bit is "don't-care". The real matched pattern is [policy_value & policy_bitmask]. For example, if the policy value is 3 and the policy bitmask is 0x10(bit 0 is "don't-care" bit), then policy 2 and 3 are applied to this rule.

Frame Type : Select the frame type for this ACE. These frame types are mutually exclusive.

Any: Any frame can match this ACE.

Ethernet Type: Only Ethernet Type frames can match this ACE. The IEEE 802.3 describes the value of Length/Type Field specifications to be greater than or equal to 1536 decimal (equal to 0600 hexadecimal) 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 : Specify the action to take with a frame that hits this ACE.

Permit: The frame that hits this ACE is granted permission for the ACE operation.

Deny: The frame that hits this ACE is dropped.

Filter: Frames matching the ACE are filtered.

Rate Limiter : Specify the rate limiter in number of base units. The allowed range is 1 - 16. Disabled indicates that the rate limiter operation is disabled.

EVC Policer : Select whether EVC policer is enabled or disabled. The default value is "Disabled". Note that the ACL rate limiter and EVC policer cannot both be enabled.

EVC Policer ID : Select which EVC policer ID to apply on this ACE. Allowed values are Disabled or 1 - 256.

Port Redirect : Frames that hit the ACE are redirected to the port number specified here. The rate limiter will affect these ports. The allowed range is the same as the switch port number range. Disabled indicates that the port redirect operation is disabled and the specific port number of 'Port Redirect' can't be set when action is permitted.

Mirror : Specify the mirror operation of this port. Frames matching the ACE are mirrored to the destination mirror port. The rate limiter will not affect frames on the mirror port. The allowed values are:

Enabled: Frames received on the port are mirrored.

Disabled: Frames received on the port are not mirrored. The default value is "Disabled".

Logging : Specify the logging operation of the ACE. Notice that the logging message doesn't include the 4 bytes CRC information. The allowed values are:

Enabled: Frames matching the ACE are stored in the System Log.

Disabled: Frames matching the ACE are not logged.

Note: The logging feature only works when the packet length is less than 1518 (without VLAN tags) and the System Log memory size and logging rate is limited.

Shutdown : Specify the port shut down operation of the ACE. The allowed values are:

Enabled: If a frame matches the ACE, the ingress port will be disabled.

Disabled: Port shut down is disabled for the ACE.

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

Counter : The counter indicates the number of times the ACE was hit by a frame.

MAC Parameters

SMAC Filter : (Only displays 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 "xxxxxxxxxxx" (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. Allowed values are:

Any: Any value is allowed ("don't-care").

Enabled: Tagged frame only.

Disabled: Untagged frame only.

The default value is "Any".

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

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

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

VLAN ID : When "Specific" is selected for the VLAN ID filter, you can enter a specific VLAN ID number. The allowed range is 1 to 4095. A frame that hits this ACE matches this VLAN ID value.

Tag Priority : Specify the tag priority for this ACE. A frame that hits this ACE matches this tag priority. The allowed number range is 0 to 7 or range 0-1, 2-3, 4-5, 6-7, 0-3 and 4-7. The value Any means that no tag priority is specified (tag priority is "don't-care".)

ARP Parameters

The ARP parameters can be configured when Frame Type "ARP" is selected.

ARP/RARP : Specify the available ARP/RARP opcode (OP) flag for this ACE.

Any: No ARP/RARP OP flag is specified. (OP is "don't-care".)

ARP: Frame must have ARP opcode set to ARP.

RARP: Frame must have RARP opcode set to RARP.

Other: Frame has unknown ARP/RARP Opcode flag.

Request/Reply : Specify the available Request/Reply opcode (OP) flag for this ACE.

Any: No Request/Reply OP flag is specified. (OP is "don't-care".)

Request: Frame must have ARP Request or RARP Request OP flag set.

Reply: Frame must have ARP Reply or RARP Reply OP flag.

Sender IP Filter : Specify the sender IP filter for this ACE.

Any: No sender IP filter is specified. (Sender IP filter is "don't-care".)

Host: Sender IP filter is set to Host. Specify the sender IP address in the SIP Address field that appears.

Network: Sender IP filter is set to Network. Specify the sender IP address and sender IP mask in the SIP Address and SIP Mask fields that appear.

Sender IP Address : When "Host" or "Network" is selected for the sender IP filter, you can enter a specific sender IP address in dotted decimal notation. Notice the invalid IP address configuration is acceptable too, for example, 0.0.0.0. Normally, an ACE with invalid IP address will explicitly adding deny action.

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. Notice the invalid IP address configuration is acceptable too, for example, 0.0.0.0. Normally, an ACE with invalid IP address will explicitly adding deny action.

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").

IP : 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").

Ethernet : 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").

ICMP: Select ICMP to filter IPv4 ICMP protocol frames. Extra fields for defining ICMP parameters will appear.

UDP: Select UDP to filter IPv4 UDP protocol frames. Extra fields for defining UDP parameters will appear.

TCP: Select TCP to filter IPv4 TCP protocol frames. Extra fields for defining TCP parameters will appear.

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.

IP Protocol Value : When "Specific" is selected for the IP protocol value, you can enter a specific value. The allowed range is 0 to 255. A frame that hits this ACE matches this IP protocol value.

IP TTL : Specify the Time-to-Live settings for this ACE.

zero: IPv4 frames with a Time-to-Live field greater than zero must not be able to match this entry.

non-zero: IPv4 frames with a Time-to-Live field greater than zero must be able to match this entry.

Any: Any value is allowed ("don't-care").

IP Fragment : Specify the fragment offset settings for this ACE. This involves the settings for the More Fragments (MF) bit and the Fragment Offset (FRAG OFFSET) field for an IPv4 frame.

No: IPv4 frames where the MF bit is set or the FRAG OFFSET field is greater than zero must not be able to match this entry.

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

Any: Any value is allowed ("don't-care").

IP Option : Specify the options flag setting for this ACE.

No: IPv4 frames where the options flag is set must not be able to match this entry.

Yes: IPv4 frames where the options flag is set must be able to match this entry.

Any: Any value is allowed ("don't-care").

SIP Filter : Specify the source IP filter for this ACE.

Any: No source IP filter is specified. (Source IP filter is "don't-care".)

Host: Source IP filter is set to Host. Specify the source IP address in the SIP Address field that appears.

Network: Source IP filter is set to Network. Specify the source IP address and source IP mask in the SIP Address and SIP Mask fields that appear.

SIP Address : When "Host" or "Network" is selected for the source IP filter, you can enter a specific SIP address in dotted decimal notation. Notice the invalid IP address configuration is acceptable too, for example, 0.0.0.0. Normally, an ACE with invalid IP address will explicitly adding deny action.

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. Notice the invalid IP address configuration is acceptable too, for example, 0.0.0.0. Normally, an ACE with an invalid IP address will explicitly add Deny action.

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 below.

UDP: Select UDP to filter IPv6 UDP protocol frames. Extra fields for defining UDP parameters will appear.

TCP: Select TCP to filter IPv6 TCP protocol frames. Extra fields for defining TCP parameters will appear.

Next Header Value : When "Specific" is selected for the IPv6 next header value, you can enter a specific value. The allowed range is 0 to 255. A frame that hits this ACE matches this IPv6 protocol value.

SIP Filter : Specify the source IPv6 filter for this ACE.

Any: No source IPv6 filter is specified. (Source IPv6 filter is "don't-care".)

Specific: Source IPv6 filter is set to Network. Specify the source IPv6 address and source IPv6 mask in the SIP Address fields that appear.

SIP Address : When "Specific" is selected for the source IPv6 filter, you can enter a specific SIPv6 address. The field only supports the 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. Note 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 0xFFFFFFF (bit 0 is "don't-care" bit), then SIPv6 address 2001::2 and 2001::3 is applied to this rule.

Hop Limit : Specify the hop limit settings for this ACE.

zero: IPv6 frames with a hop limit field greater than zero must not be able to match this entry.

non-zero: IPv6 frames with a hop limit field greater than zero must be able to match this entry.

Any: Any value is allowed ("don't-care").

ICMP Parameters

ICMP Type Filter : Specify the ICMP filter for this ACE.

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

Specific: If you want to filter a specific ICMP filter with this ACE, you can enter a specific ICMP value. A field for entering an ICMP value appears.

ICMP Type Value : When "Specific" is selected for the ICMP filter, you can enter a specific ICMP value. The allowed range is 0 to 255. A frame that hits this ACE matches this ICMP value.

ICMP Code Filter : Specify the ICMP code filter for this ACE.

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

Specific: If you want to filter a specific ICMP code filter with this ACE, you can enter a specific ICMP code value. A field for entering an ICMP code value appears.

ICMP Code Value : When "Specific" is selected for the ICMP code filter, you can enter a specific ICMP code value. The allowed range is 0 to 255. A frame that hits this ACE matches this ICMP code value.

TCP/UDP Parameters

TCP/UDP Source Filter : Specify the TCP/UDP source filter for this ACE.

Any: No TCP/UDP source filter is specified (TCP/UDP source filter status is "don't-care").

Specific: If you want to filter a specific TCP/UDP source filter with this ACE, you can enter a specific TCP/UDP source value. A field for entering a TCP/UDP source value appears.

Range: If you want to filter a specific TCP/UDP source range filter with this ACE, you can enter a specific TCP/UDP source range value. A field for entering a TCP/UDP source value appears.

TCP/UDP Source No. : When "Specific" is selected for the TCP/UDP source filter, you can enter a specific TCP/UDP source value. The allowed range is 0 to 65535. A frame that hits this ACE matches this TCP/UDP source value.

TCP/UDP Source Range : When "Range" is selected for the TCP/UDP source filter, you can enter a specific TCP/UDP source range value. The allowed range is 0 to 65535. A frame that hits this ACE matches this TCP/UDP source value.

TCP/UDP Destination Filter : Specify the TCP/UDP destination filter for this ACE.

Any: No TCP/UDP destination filter is specified (TCP/UDP destination filter status is "don't-care").

Specific: If you want to filter a specific TCP/UDP destination filter with this ACE, you can enter a specific TCP/UDP destination value. A field for entering a TCP/UDP destination value appears.

Range: If you want to filter a specific range TCP/UDP destination filter with this ACE, you can enter a specific TCP/UDP destination range value. A field for entering a TCP/UDP destination value appears.

TCP/UDP Destination Number : When "Specific" is selected for the TCP/UDP destination filter, you can enter a specific TCP/UDP destination value. The allowed range is 0 to 65535. A frame that hits this ACE matches this TCP/UDP destination value.

TCP/UDP Destination Range : When "Range" is selected for the TCP/UDP destination filter, you can enter a specific TCP/UDP destination range value. The allowed range is 0 to 65535. A frame that hits this ACE matches this TCP/UDP destination value.

TCP FIN : Specify the TCP "No more data from sender" (FIN) value for this ACE.

0: TCP frames where the FIN field is set must not be able to match this entry.

1: TCP frames where the FIN field is set must be able to match this entry.

Any: Any value is allowed ("don't-care").

TCP SYN : Specify the TCP "Synchronize sequence numbers" (SYN) value for this ACE.

0: TCP frames where the SYN field is set must not be able to match this entry.

1: TCP frames where the SYN field is set must be able to match this entry.

Any: Any value is allowed ("don't-care").

TCP RST : Specify the TCP "Reset the connection" (RST) value for this ACE.

0: TCP frames where the RST field is set must not be able to match this entry.

1: TCP frames where the RST field is set must be able to match this entry.

Any: Any value is allowed ("don't-care").

TCP PSH : Specify the TCP "Push Function" (PSH) value for this ACE.

0: TCP frames where the 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 ACK : Specify the TCP "Acknowledgment field significant" (ACK) value for this ACE.

0: TCP frames where the ACK field is set must not be able to match this entry.

1: TCP frames where the ACK field is set must be able to match this entry.

Any: Any value is allowed ("don't-care").

TCP URG : Specify the TCP "Urgent Pointer field significant" (URG) value for this ACE.

0: TCP frames where the URG field is set must not be able to match this entry.

1: TCP frames where the URG field is set must be able to match this entry.

Any: Any value is allowed ("don't-care").

Ethernet Type Parameters : The Ethernet Type parameters can be configured when Frame Type "Ethernet Type" is selected.

EtherType Filter : Specify the Ethernet type filter for this ACE.

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

Specific: If you want to filter a specific EtherType filter with this ACE, you can enter a specific EtherType value. A field for entering a EtherType value appears.

Ethernet Type Value : When "Specific" is selected for the EtherType filter, you can enter a specific EtherType value. The allowed range is 0x600 to 0xFFFF but excluding 0x800 (IPv4), 0x806 (ARP) and 0x86DD (IPv6). A frame that hits this ACE matches this EtherType value.

Buttons

Apply : Click to save changes.

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

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

Refresh: Click to manually refresh the page immediately.

Clear: Click to clear the ACL configuration.

Remove All : Click to remove all ACL configuration table entries. At the confirmation prompt click the OK button.

Example: Access Control List Configuration page with 5 entries with different Frame Types:

The screenshot shows the "Access Control List Configuration" page. The page title is "Access Control List Configuration" and the breadcrumb is "Home > Configuration > Security > Network > ACL > Access Control List". The page has an "Auto-refresh" checkbox and three buttons: a refresh icon, a save icon, and a delete icon. Below the buttons is a table with 5 entries. The table has columns: ACE, Ingress Port, Policy / Bitmask, Frame Type, Action, Rate Limiter, Port Redirect, Mirror, Counter, and a column with icons for edit, delete, and add. The entries are:

ACE	Ingress Port	Policy / Bitmask	Frame Type	Action	Rate Limiter	Port Redirect	Mirror	Counter	Icons
1	All	Any	EType	Permit	Disabled	Disabled	Disabled	100	⊕ ⊖ ⊗
2	All	Any	Any	Permit	Disabled	Disabled	Disabled	1103	⊕ ⊖ ⊗
3	All	Any	ARP	Permit	Disabled	Disabled	Disabled	0	⊕ ⊖ ⊗
4	All	Any	IPv4	Permit	Disabled	Disabled	Disabled	0	⊕ ⊖ ⊗
5	All	Any	IPv6	Permit	Disabled	Disabled	Disabled	0	⊕ ⊖ ⊗

3-5.2.4 IP Source Guard

This page lets you configure the IP Source Guard detail parameters of the switch. You could use the IP Source Guard configure to enable or disable with the Port of the switch.

3-5.2.4.1 Configuration

This page lets you configure IP Source Guard setting including Mode (Enabled or Disabled) and Maximum Dynamic Clients (0, 1, 2, Unlimited).

To configure IP Source Guard parameters in the web UI:

1. Click Configuration, Security, Network, IP Source Guard and Configuration.
2. Select "Enabled" at the Mode of IP Source Guard Configuration dropdown.
3. Select "Enabled" of the specific port(s) at the Port Mode dropdown.
4. Select Maximum Dynamic Clients of the specific port in the Mode column of Port Mode Configuration.
5. Click Apply.

The screenshot displays the IP Source Guard Configuration page in the Lantronix web UI. The 'Mode' is currently set to 'Disabled'. Below this, there is a 'Translate dynamic to static' button. The 'Port Mode Configuration' table is shown with the following data:

Port	Mode	Max Dynamic Clients
*	Disabled	Unlimited
1	Disabled	Unlimited
2	Disabled	Unlimited
3	Disabled	Unlimited
4	Disabled	Unlimited
5	Disabled	Unlimited
6	Disabled	Unlimited
7	Disabled	Unlimited

Figure 3-5.2.4.1: IP Source Guard Configuration

Parameter descriptions:

Mode: Enable the Global IP Source Guard or disable the Global IP Source Guard. All configured ACEs will be lost when the mode is enabled.

Port Mode Configuration : Specify IP Source Guard is enabled on which ports. Only when both Global Mode and Port Mode on a given port are enabled, IP Source Guard is enabled on this given port.

Max Dynamic Clients : Specify the maximum number of dynamic clients that can be learned on given port. This value can be **0**, **1**, **2** or **unlimited**. If the port mode is enabled and the value of max dynamic client is equal to **0** means only allow the IP packets forwarding that are matched in static entries on the specific port.

Buttons

Translate dynamic to static: Click to translate all dynamic entries to static entries.

Apply : Click to save changes.

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

3-5.2.4.2 Static Table

This page lets you configure the Static IP Source Guard Table parameters of the switch. You can use the Static IP Source Guard Table configure to manage the entries.

To configure Static IP Source Guard Table parameters in the web UI:

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

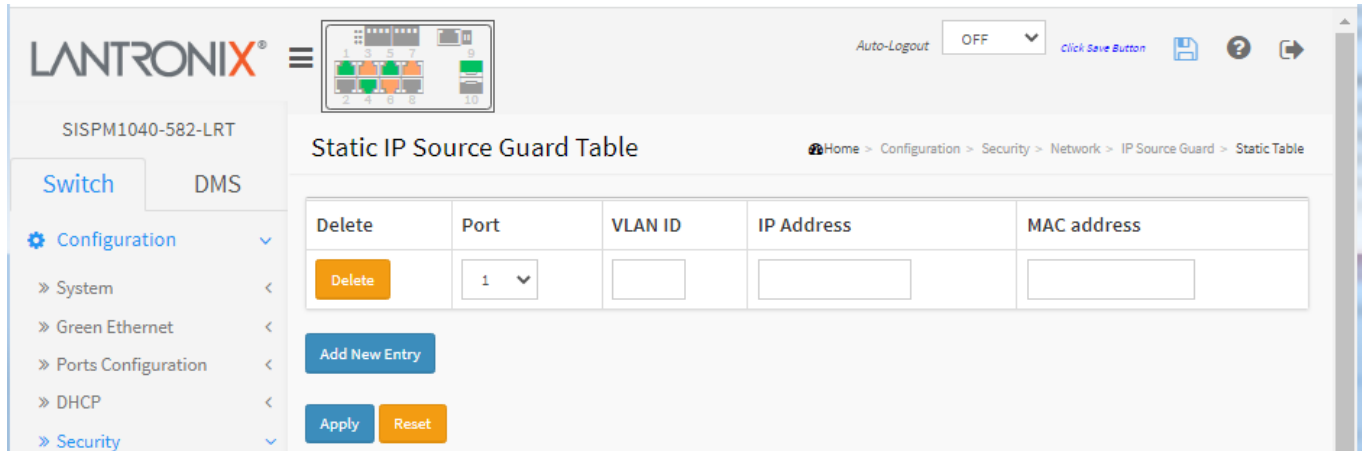


Figure 3-5.2.4.2: Static IP Source Guard Table

Parameter descriptions:

Port : The logical port for the settings.

VLAN ID : The VLAN id for the settings.

IP Address : Allowed Source IP address.

MAC address : Allowed Source MAC address.

Adding new entry : Click to add a new entry to the Static IP Source Guard table. Specify the Port, VLAN ID, IP address, and IP Mask for the new entry. Click Apply.

Buttons

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

Apply : Click to save changes.

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

3-5.2.5 ARP Inspection

This page lets you configure the ARP Inspection parameters of the switch. ARP Inspection is a secure feature. Several types of attacks can be launched against a host or devices connected to Layer 2 networks by "poisoning" the ARP caches. ARP Inspection is used to block such attacks. Only valid ARP requests and responses can go through the switch.

3-5.2.5.1 Port Configuration

Here you can configure ARP Inspection settings. To configure ARP Inspection parameters in the web UI:

1. Click Configuration, Security, Network, ARP Inspection and Port Configuration.
2. Select "Enabled" in the Mode of ARP Inspection Configuration.
3. Select "Enabled" of the specific port in the Mode of Port Mode Configuration.
4. Click Apply.

The screenshot displays the LANTRONIX web interface for the SISPM1040-582-LRT switch. The main heading is "ARP Inspection Configuration". The "Mode" is currently set to "Disabled". Below this, there is a "Translate dynamic to static" button. The "Port Mode Configuration" table is shown below, with columns for Port, Mode, Check VLAN, and Log Type. All ports (1-10) have their Mode set to "Disabled".

Port	Mode	Check VLAN	Log Type
*	<->	<->	<->
1	Disabled	Disabled	None
2	Disabled	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

At the bottom of the configuration area, there are "Apply" and "Reset" buttons.

Figure 3-5.2.5.1: ARP Inspection Configuration

Parameter descriptions:

Mode of ARP Inspection Configuration : Enable the Global ARP Inspection or disable the Global ARP Inspection.

Port Mode Configuration : Specify ARP Inspection is enabled on which ports. Only when both Global Mode and Port Mode on a given port are enabled, ARP Inspection is enabled on this given port. Possible modes are:

Enabled: Enable ARP Inspection operation.

Disabled: Disable ARP Inspection operation.

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. When the setting of "Check VLAN" is enabled, the log type of ARP Inspection will refer to the VLAN setting. Possible setting are:

Enabled: Enable check VLAN operation.

Disabled: Disable check VLAN operation.

Log Type : Only the Global Mode and Port Mode on a given port are enabled, and the setting of "Check VLAN" is disabled, the log type of ARP Inspection will refer to the port setting. The four possible log types are:

None: Log nothing.

Deny: Log denied entries.

Permit: Log permitted entries.

ALL: Log all entries.

Buttons

Translate dynamic to static : Click to translate all dynamic entries to static entries.

Apply : Click to save changes.

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

3-5.2.5.2 VLAN Configuration

Each page shows up to 9999 entries from the VLAN table, default being 20, selected through the "entries per page" input field. When first visited, the web page will show the first 20 entries from the beginning of the VLAN Table. The first displayed will be the one with the lowest VLAN ID found in the VLAN Table. The "VLAN" input fields allow the user to select the starting point in the VLAN Table. Clicking the Refresh button will update the displayed table starting from that or the closest next VLAN Table match. The > button will use the next entry of the currently displayed VLAN entry as a basis for the next lookup. When the end is reached the warning message is shown in the displayed table. Use the << button to start over.

To configure VLAN Mode parameters in the web UI:

1. Click Configuration, Security, Network, ARP Inspection, and VLAN Configuration.
2. Click Add New Entry.
3. Specify the VLAN ID, Log Type
4. Click Apply.

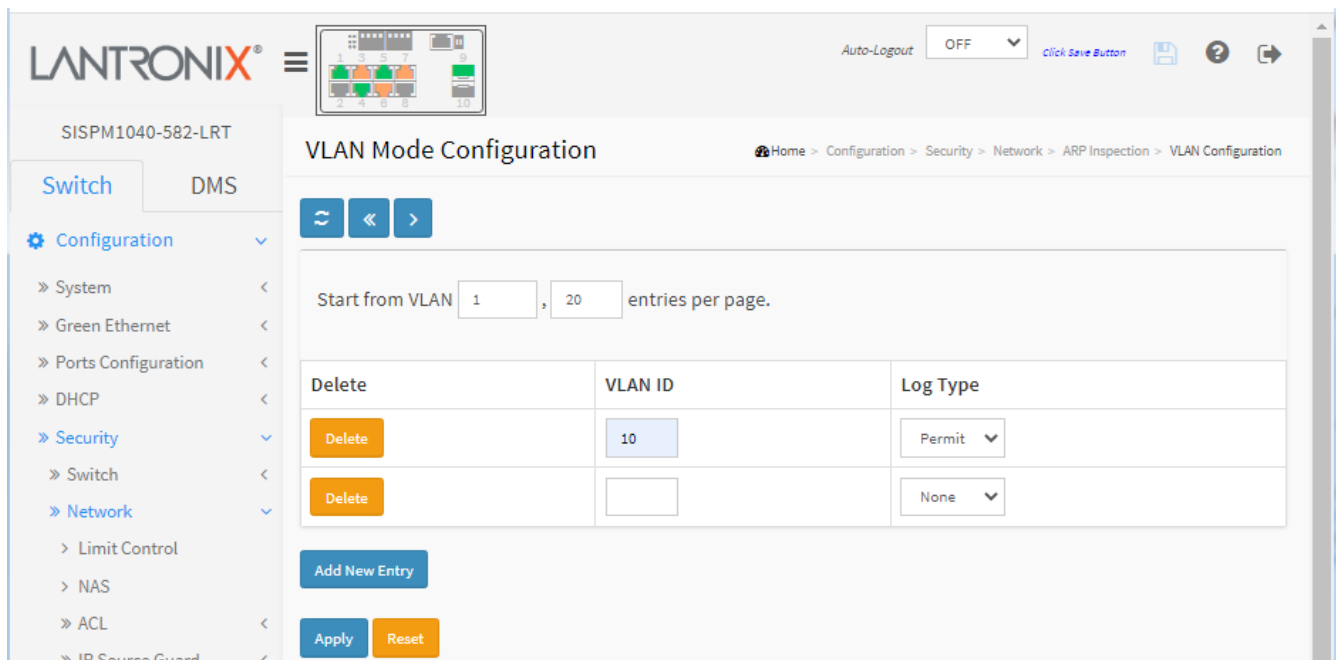


Figure 3-5.2.5.2: VLAN Mode Configuration

Parameter descriptions:

VLAN ID : Specify on which VLANs you want ARP Inspection enabled. First, you must enable the port setting on the Port Mode Configuration web page (see previous page). ARP Inspection is enabled on a given port only when both Global Mode and Port Mode for the port are enabled. Second, you can specify which VLAN will be inspected on the 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.

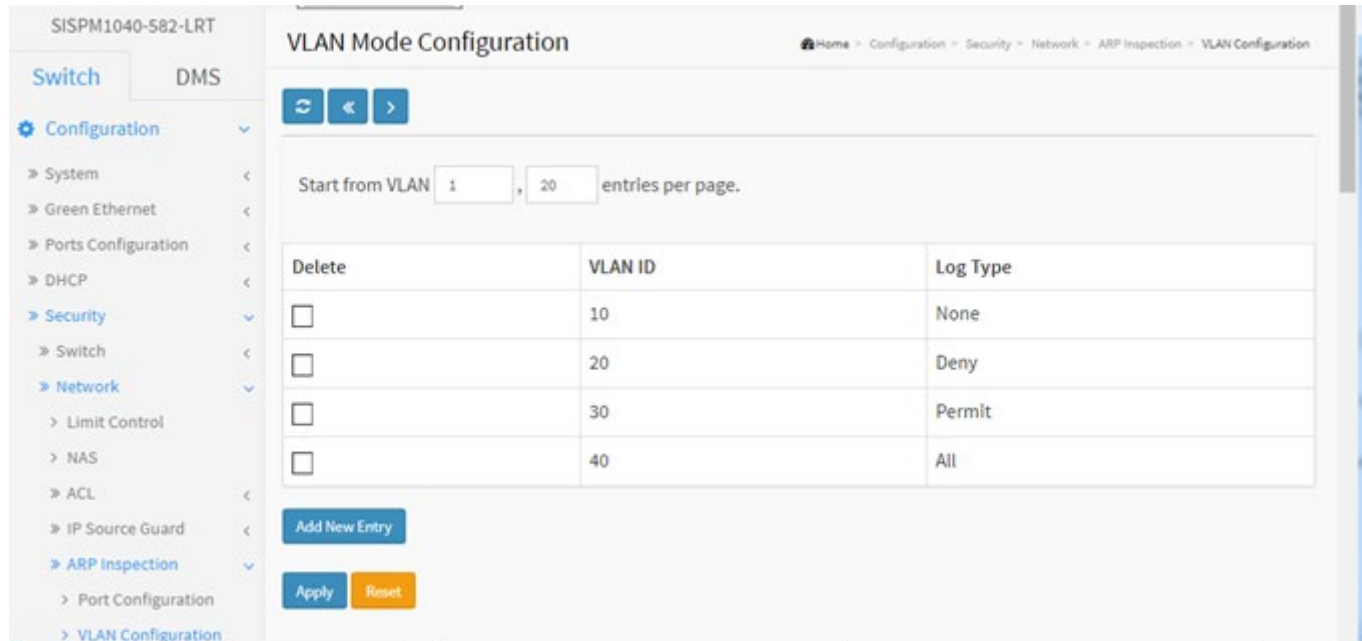
Buttons

Add New Entry : Click to add a new VLAN to the ARP Inspection VLAN table.

Apply : Click to save changes.

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

Example:



3-5.2.5.3 Static Table

This page lets you configure the Static ARP Inspection Table parameters of the switch. You can use the Static ARP Inspection Table settings to manage the ARP entries.

To configure Static ARP Inspection Table parameters in the web UI:

1. Click Configuration, Security, Network, ARP Inspection and Static Table.
2. Click Add New Entry.
3. Specify the Port, VLAN ID, IP Address, and MAC address in the entry.
4. Click Apply.

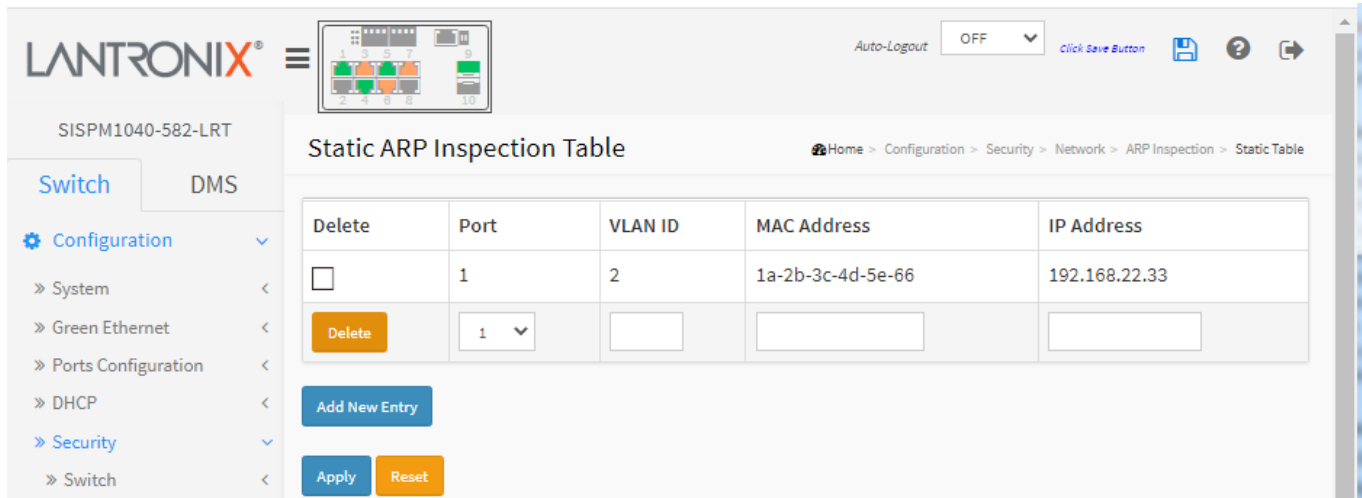


Figure 3-5.2.5.3: Static ARP Inspection Table

Parameter descriptions:

Port : The logical port for the settings.

VLAN ID : The VLAN ID (VID) for the settings.

MAC Address : Allowed Source MAC address in ARP request packets.

IP Address : Allowed Source IP address in ARP request packets.

Buttons

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 Static ARP Inspection table. Specify the Port, VLAN ID, MAC address, and IP address for the new entry. Click "Apply".

Apply : Click to save changes.

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

3-5.2.5.4 Dynamic Table

Entries in the Dynamic ARP Inspection Table are shown on this page. The Dynamic ARP Inspection Table contains up to 1024 entries, and is sorted first by port, then by VLAN ID, then by MAC address, and then by IP address.

Each page shows up to 99 entries from the Dynamic ARP Inspection table, default being 20, selected through the "entries per page" input field. When first visited, the web page will show the first 20 entries from the beginning of the Dynamic ARP Inspection Table.

The "Start from port address", "VLAN", "MAC address" and "IP address" input fields let you select the starting point in the Dynamic ARP Inspection Table. Clicking the Refresh button will update the displayed table starting from that or the closest next Dynamic ARP Inspection Table match. In addition, the two input fields will - upon a Refresh button click - assume the value of the first displayed entry, allowing for continuous refresh with the same start address.

The > 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 << button to start over.

Web Interface

To configure Dynamic ARP Inspection Table parameters in the web UI:

1. Click Configuration, Security, Network, ARP Inspection, and Dynamic Table.
2. Specify the Port, VLAN ID, IP Address, and MAC address in the entry.
3. Click Apply.

The screenshot displays the Lantronix web interface for configuring the Dynamic ARP Inspection Table. The interface includes a navigation menu on the left with options like Configuration, Security, and Network. The main content area shows the 'Dynamic ARP Inspection Table' configuration page. It features an 'Auto-refresh' checkbox and navigation buttons (refresh, back, forward). The 'Start from' section includes dropdowns for 'Port 1', 'VLAN 1', and input fields for 'MAC address' (00-00-00-00-00) and 'IP address' (0.0.0.0). Below this is an 'entries per page' input field set to 20. A 'System Configuration' table is shown with columns for Port, VLAN ID, MAC Address, IP Address, and Translate to static. The table currently displays 'No more entries'. At the bottom, there are 'Apply' and 'Reset' buttons.

Figure 3-5.2.5.4: Dynamic ARP Inspection Table

Parameter descriptions:

Port : Switch Port Number for which the entries are displayed.

VLAN ID : VLAN-ID in which the ARP traffic is permitted.

MAC Address : User MAC address of the entry.

IP Address : User IP address of the entry.

Translate to static : Select the checkbox to translate the entry to static entry.

Buttons

Apply : Click to save changes.

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

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

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

<< : Updates the table starting from the first entry in the Dynamic ARP Inspection Table.

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

3-5.3 AAA

This section lets you configure an AAA (Authentication, Authorization, and Accounting) server to provide access control to your network. The AAA server can be a TACACS+ or RADIUS server used to create and manage objects that contain settings for using AAA servers.

3-5.3.1 RADIUS

This page lets you configure up to five RADIUS servers. RADIUS (Remote Authentication Dial In User Service) is a networking protocol that provides centralized Authentication, Authorization, and Accounting ('AAA' or 'Triple A') management for users who connect and use a network service. The RADIUS server is usually a background process running on a UNIX or Microsoft Windows Server.

RADIUS uses two packet types to manage the full AAA process: Access-Request, which manages authentication and authorization; and Accounting-Request, which manages accounting. Authentication and authorization are defined in IETF [RFC 2865](#) and accounting is described by IETF [RFC 2866](#).

To configure a RADIUS server via the web UI:

1. Click Configuration, Security, AAA and RADIUS.
2. Click the Add New Server button.
3. Specify the Global and Server Configuration parameters.
4. Click Apply.

The screenshot displays the 'RADIUS Server Configuration' page in the Lantronix web interface. The page is titled 'RADIUS Server Configuration' and shows the navigation path: Home > Configuration > Security > AAA > RADIUS. The interface is split into two main sections: 'Global Configuration' and 'Server Configuration'.

Global Configuration:

- Timeout: 5 seconds
- Retransmit: 3 times
- Deadtime: 0 minutes
- Key: [masked]
- NAS-IP-Address: [empty field]
- NAS-IPv6-Address: [empty field]
- NAS-Identifier: [empty field]

Server Configuration:

Delete	Hostname	Auth Port	Acct Port	Timeout	Retransmit	Key
<input type="button" value="Delete"/>	RadSrvr1	1812	1813	60	350	admin

At the bottom of the Server Configuration section, there are three buttons: 'Add New Server', 'Apply', and 'Reset'.

Figure 3-5.3.1: RADIUS Server Configuration

Parameter descriptions:**Global Configuration**

Timeout : The number of seconds (1–1000) to wait for a reply from a RADIUS server before retransmitting the request. The default is 5 seconds.

Retransmit : The number of times (1–1000) that 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. The default is 3 retransmit times.

Deadtime : The period during which the switch will not send new requests to a RADIUS 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. The valid range is 0 - 1440 minutes. The default is 0 minutes. 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 shared between the RADIUS server and the switch (up to 63 characters long).

NAS-IP-Address (Attribute 4) : The IPv4 address to be used as attribute 4 in RADIUS Access-Request packets. If this field is left blank, the IP address of the outgoing interface is used. See “[RADIUS Attributes](#)” below.

NAS-IPv6-Address (Attribute 95) : The IPv6 address to be used as attribute 95 in RADIUS Access-Request packets. If this field is left blank, the IP address of the outgoing interface is used. See “[RADIUS Attributes](#)” below.

NAS-Identifier (Attribute 32) : The identifier - up to 255 characters long - to be used as attribute 32 in RADIUS Access-Request packets. If this field is left blank, the NAS-Identifier is not included in the packet. See “[RADIUS Attributes](#)” below.

Server Configuration: The table has one row for each RADIUS server and several columns, which are:

Hostname : The IP address or hostname of the RADIUS server.

Auth Port : The UDP port to use on the RADIUS server for authentication. The officially assigned port number for RADIUS Accounting is 1812. Note: by default, many access servers use port 1645 for authentication requests.

Note: For Windows Server information on how to configure ports that Network Policy Server (NPS) uses for Remote Authentication Dial-In User Service (RADIUS) authentication and accounting traffic see <https://docs.microsoft.com/en-us/windows-server/networking/technologies/nps/nps-udp-ports-configure#:~:text=The%20port%20values%20of%201812,and%201646%20for%20accounting%20requests>

Acct Port : The UDP port to use on the RADIUS server for accounting. The officially assigned port number for RADIUS Accounting is 1813. Note: by default, many access servers use port 1646 for accounting requests.

Timeout : This optional setting overrides the global timeout value. Leaving it blank will use the global timeout value.

Retransmit : This optional setting overrides the global retransmit value. Leaving it blank will use the global retransmit value.

Key : This optional setting overrides the global key. Leaving it blank will use the global key.

Buttons

Delete : To delete a RADIUS server entry, check this box. The entry will be deleted during the next Save.

Add New Server : Click to add a new RADIUS server. An empty row is added to the table, and the RADIUS server can be configured as needed. Up to 5 servers are supported. The Reset button can be used to undo the addition of the new server.

Apply: Click to save changes.

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

Messages:

The value of NAS-IP-Address must be a valid IP address in dotted decimal notation (x.y.z.w), where x, y, z, and w are decimal number between 0 and 255.

The input value NAS-IPv6-Address (111111111) is not a valid IPv6 address.

Hostname must be a valid hostname, unicast IPv4, or unicast IPv6 address

RADIUS Attributes

<u>Value</u>	<u>Description</u>	<u>Data Type</u>	<u>Reference</u>
4	NAS-IP-Address	ipv4addr	IETF RFC2865
32	NAS-Identifier	text	IETF RFC2865
95	NAS-IPv6-Address	ipv6addr	IETF RFC3162

The RADIUS Accounting protocol provides a protocol for carrying accounting information between a Network Access Server and a shared Accounting Server per IETF [RFC 2866](#).

See the [IANA Considerations](#) for guidance regarding IANA registration of values related to RADIUS as defined in IETF [RFC2865](#).

See your RADIUS server documents for more information.

Note: SISPM1040-582-LRT FW VB7.20.0039 adds the RADIUS Server [Attribute 6](#) - Service-Type attribute option when authenticating with RADIUS:

- For **MAC authentication**, the service-type is set to "**Call-Check**".
- For **Dot1x authentication**, the service-type is set to "**Framed**".
- For **Captive portal authentication**, the service-type is set to "**Login**". A captive portal is a web page accessed with a web browser that displays to a newly-connected network user (Wi-Fi or wired) before they are granted broader access to network resources.

3-5.3.2 TACACS+

This page lets you configure up to five TACACS+ servers. Terminal Access Controller Access Control System Plus is a networking protocol which provides access control for routers, network access servers and other networked computing devices via one or more centralized servers. TACACS+ provides separate authentication, authorization and accounting services. For more information see <https://tools.ietf.org/html/rfc8907>.

To configure a TACACS+ server in the web UI:

1. Click Configuration, Security, AAA and TACACS+.
2. Click the Add New Entry button.
3. Enter the Global Configuration parameters.
4. Enter the Server Configuration parameters.
5. Repeat steps 2 - 4 above to add another TACACS+ server.
6. Click Apply.

The screenshot shows the 'TACACS+ Server Configuration' page in the Lantronix web UI. The page has a left sidebar with navigation options like 'Switch', 'DMS', 'Configuration', 'System', 'Green Ethernet', 'Ports Configuration', 'DHCP', 'Security', 'Switch', 'Network', 'AAA', 'RADIUS', 'TACACS+', 'Aggregation', 'Link OAM', 'Loop Protection', and 'Spanning Tree'. The main content area is titled 'TACACS+ Server Configuration' and contains two sections: 'Global Configuration' and 'Server Configuration'. The 'Global Configuration' section has three rows: 'Timeout' with a value of 5 seconds, 'Deadtime' with a value of 0 minutes, and 'Key' with a masked value of *****. The 'Server Configuration' section is a table with columns: 'Delete', 'Hostname', 'Port', 'Timeout', and 'Key'. The first row has a checkbox, 'TacSrvr1', '49', '60', and *****. Below it is a row with a 'Delete' button, an empty 'Hostname' field, '49', an empty 'Timeout' field, and an empty 'Key' field. At the bottom of the table are buttons for 'Add New Server', 'Apply', and 'Reset'.

Figure 3-5.3.2: TACACS+ Server Configuration

Parameter descriptions:

Global Configuration

Timeout : The number of seconds to wait for a reply from a TACACS+ server before it is considered to be dead. The valid range is 1 – 1000 seconds. The default is 5 seconds.

Deadtime : 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. The valid range is 0 - 1440 minutes. The default is 0 minutes. Setting the Deadtime to a value greater than 0 (zero) will enable this feature, but only if more than one server has been configured.

Key : The secret key - up to 63 characters long - shared between the TACACS+ server and the switch.

Server Configuration: The table has one row for each TACACS+ server and several columns, which are:

Hostname : The IP address or hostname of the TACACS+ server. Hostname must be a valid hostname, unicast IPv4 address, or unicast IPv6 address.

Port : The TCP port to use on the TACACS+ server for authentication; port 49 is the default.

Timeout : This optional setting overrides the global timeout value. Leaving it blank will use the global timeout value.

Key : This optional setting overrides the global key. Leaving it blank will use the global key.

Buttons

Delete : To delete a TACACS+ server entry, check this box. The entry will be deleted during the next Save.

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

Apply: Click to save changes.

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

Messages:

Authentication Error HTTPD cache has no valid entry

Hostname must be a valid hostname, unicast IPv4, or unicast IPv6 address

Meaning: You entered an invalid Key or Hostname parameter.

Recovery: **1.** Click the **Previous** button to clear the error message. **2.** Re-enter a valid Key or Hostname parameter. **3.** Continue operation.

3-6 Aggregation

The Aggregation is used to configure the settings of Link Aggregation. You can bundle more than one port with the same speed, full duplex and the same MAC to be a single logical port, thus the logical port aggregates the bandwidth of these ports. This means you can apply your current Ethernet equipment's to build the bandwidth aggregation. For example, if there are three Fast Ethernet ports aggregated in a logical port, then this logical port has bandwidth three times as high as a single Fast Ethernet port.

3-6.1 Static

Ports using Static Trunk as their trunk method can choose their unique Static Group ID to form a logic “trunked port”. The benefit of using Static Trunk method is that a port can immediately become a member of a trunk group without any handshaking with its peer port. This is also a disadvantage because the peer ports of your static trunk group may not know that they should be aggregated together to form a “logic trunked port”. Using Static Trunk on both ends of a link is strongly recommended. Please also note that low speed links will stay in “not ready” state when using static trunk to aggregate with high speed links.

To configure Trunk Aggregation Hash mode and Aggregation Group in the web UI:

1. Click Configuration, Aggregation and Static.
2. Enable or disable the Hash Code Contributors.
3. Select Aggregation Group ID and Port members.
4. Click the Apply button to save the settings, to cancel the settings click the Reset button.

The screenshot shows the 'Aggregation Mode Configuration' page in the Lantronix web UI. The page is titled 'Aggregation Mode Configuration' and is part of the 'Static' configuration section. The sidebar on the left shows the navigation menu with 'Configuration' expanded and 'Aggregation' selected. The main content area is divided into two sections: 'Hash Code Contributors' and 'Aggregation Group Configuration'.

Hash Code Contributors

Source MAC Address	<input checked="" type="checkbox"/>
Destination MAC Address	<input type="checkbox"/>
IP Address	<input checked="" type="checkbox"/>
TCP/UDP Port Number	<input checked="" type="checkbox"/>

Aggregation Group Configuration

Group ID	Port Members									
	1	2	3	4	5	6	7	8	9	10
Normal	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
1	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
2	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
3	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
4	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
5	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

At the bottom of the page, there are 'Apply' and 'Reset' buttons.

Figure 3-6.1: Aggregation Mode Configuration

Parameter descriptions:**Hash Code Contributors**

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

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

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

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

Aggregation Group Configuration

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

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

Buttons

Apply : Click to save changes.

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

Messages:

Group 1 member counts error!! Local aggregation must include 2-16 ports

Aggregation Error LACP aggregation is enabled

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

3-6.2 LACP

This page lets you view and configure the current LACP port parameters. An LACP trunk group with more than one ready member-ports is a “real trunked” group. An LACP trunk group with only one or less than one ready member-ports is not a “real trunked” group. Note that LACP and Static aggregation cannot both be enabled on the same ports at the same time.

To configure LACP Port parameters in the web UI:

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

The screenshot shows the Lantronix web interface for configuring LACP on a switch. The breadcrumb trail is Home > Configuration > Aggregation > LACP. The main content area is titled 'LACP Port Configuration' and contains a table with the following data:

Port	LACP Enabled	Key	Role	Timeout	Prio
*	<input type="checkbox"/>	<=> ▾	<=> ▾	<=> ▾	32768
1	<input type="checkbox"/>	Auto ▾	Active ▾	Fast ▾	32768
2	<input type="checkbox"/>	Auto ▾	Active ▾	Fast ▾	32768
3	<input type="checkbox"/>	Auto ▾	Active ▾	Fast ▾	32768
4	<input type="checkbox"/>	Auto ▾	Active ▾	Fast ▾	32768
5	<input type="checkbox"/>	Auto ▾	Active ▾	Fast ▾	32768
6	<input type="checkbox"/>	Auto ▾	Active ▾	Fast ▾	32768
7	<input type="checkbox"/>	Auto ▾	Active ▾	Fast ▾	32768
8	<input type="checkbox"/>	Auto ▾	Active ▾	Fast ▾	32768
9	<input type="checkbox"/>	Auto ▾	Active ▾	Fast ▾	32768
10	<input type="checkbox"/>	Auto ▾	Active ▾	Fast ▾	32768

At the bottom of the table, there are two buttons: 'Apply' (blue) and 'Reset' (orange).

Figure 3-6.2: LACP Port Configuration

Parameter descriptions:

Port : The switch port number.

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

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

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

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

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

Buttons

Apply : Click to save changes.

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

3-6.3 LACP on Air

This page lets you set up the LACP on Air ports and the Couple IP address for access management. This feature provides LACP link aggregation via a wireless AP.

In order to achieve LACP load balancing, the switch uses a link aggregation hash algorithm (Source MAC, Destination MAC, and either an IP address or a TCP/UDP port number) to determine the forwarding path within a Link Aggregation Group. This means packets are forwarded on a path over the link aggregation, but the device may be located on another path. All switches have the same behavior when using the LACP protocol with this kind of application.

To ping or access these wireless devices, LACP on AIR can help to redirect packets to the corresponding path of a device.

To configure the LACP on Air parameters in the web UI:

1. Navigate to the Configuration > Aggregation > LACP On Air menu path to display the LACP on Air webpage.
2. Enable or disable the LACP on Air for each switch port.
3. Enter a Couple IP address for access management for each port.
4. Click the Apply button.

Port	Couple IP	Couple IP	
1	Disabled	0.0.0.0	0.0.0.0
2	Disabled	0.0.0.0	0.0.0.0
3	Disabled	0.0.0.0	0.0.0.0
4	Disabled	0.0.0.0	0.0.0.0
5	Disabled	0.0.0.0	0.0.0.0
6	Disabled	0.0.0.0	0.0.0.0
7	Disabled	0.0.0.0	0.0.0.0
8	Disabled	0.0.0.0	0.0.0.0

Parameter descriptions:

Port: To control which switch port should led the access of Couple IP device management.

Couple IP: Specify the connected partners for access management. The Couple IP parameters will be the individual IP addresses of Wireless3 and Wireless4 devices in the example below.

Buttons:

Apply: Click to save changes.

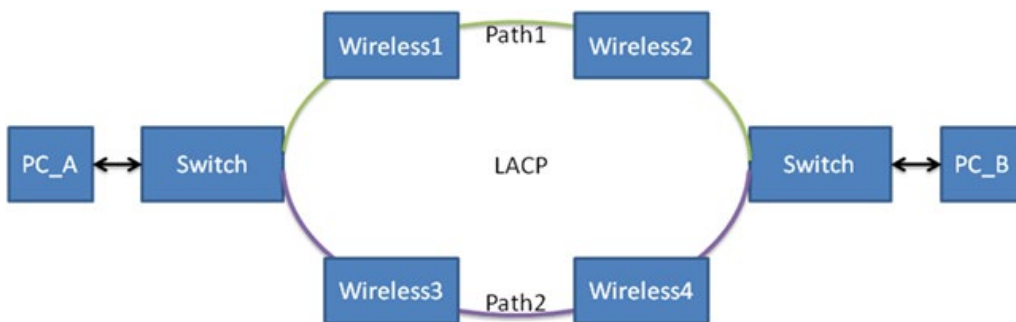
Message: *LACP Error - LACP and Static aggregation can not both be enabled on the same ports*

Meaning: Two forms of aggregation cannot be enabled at the same time.

Recovery: **1.** Click the Previous button to clear the error message. **2.** Disable either static aggregation or LACP on Air.

Example:

Suppose PC_A wants to ping to Wireless4, due to link aggregation hash algorithm, ARP and ICMP packets from PC_A will be forwarded on the Path1, but since Wireless4 is located on the Path2, it will cause the ping to fail.



After configuring LACP on AIR, PC_A can ping Wireless4 successfully, since ARP and ICMP packets will be forwarded to Path2.

3-7 Link OAM

OAM (Operation Administration and Maintenance) is a protocol described in ITU-T Y.1731 used to implement carrier Ethernet functionality. MEP functionality like CC and RDI is based on OAM.

3-7.1 Port Settings

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

To configure LOAM Port parameters in the web UI:

1. Click Configuration, Link OAM and Port Settings.
2. Select Port members.
3. Specify the Link OAM parameters.
4. Click the Apply to save the setting

The screenshot shows the Lantronix web interface for configuring Link OAM. The breadcrumb trail is Home > Configuration > Link OAM > Port Settings. The table below represents the configuration data shown in the interface.

Port	OAM Enabled	OAM Mode	Loopback Support	Link Monitor Support	MIB Retrieval Support	Loopback Operation
*	<input type="checkbox"/>	<->	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
1	<input type="checkbox"/>	Passive	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
2	<input type="checkbox"/>	Passive	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
3	<input type="checkbox"/>	Passive	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
4	<input type="checkbox"/>	Passive	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
5	<input type="checkbox"/>	Passive	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
6	<input type="checkbox"/>	Passive	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
7	<input type="checkbox"/>	Passive	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
8	<input type="checkbox"/>	Passive	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
9	<input type="checkbox"/>	Passive	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
10	<input type="checkbox"/>	Passive	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Figure 3-7.1: Link OAM Port Configuration

Parameter descriptions:

Port : The switch port number.

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

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

Active mode : DTE's 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 mode : DTE's configured in Passive mode do not initiate the Discovery process. Passive DTE's react to the initiation of the Discovery process by the remote DTE. This eliminates the possibility of passive to passive links. Passive DTE's cannot send Variable Request or Loopback Control OAMPDUs.

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

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

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

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

Buttons

Apply : Click to save changes.

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

Message:

OAM Error - Error while configuring the OAM loopback

OAM Error - Error requested configuration is not supported with the current OAM mode

Meaning: At Configuration > Link OAM > Port Settings you misconfigured a parameter.

Recovery:

1. Click the **Previous** button to clear the error dialog.
2. Navigate to **Configuration > Link OAM > Port Settings**.
3. For Loopback Support, make sure that OAM Mode is set to Active.

3-7.2 Event Settings

This page lets you configure and view the current Link OAM Link Event parameters. To configure Link Event settings in the web UI:

1. Click Configuration, Link OAM, and Event Settings.
2. Select a Port member at the Port select dropdown.
3. Specify the parameters.
4. Click the Apply button to save the settings.

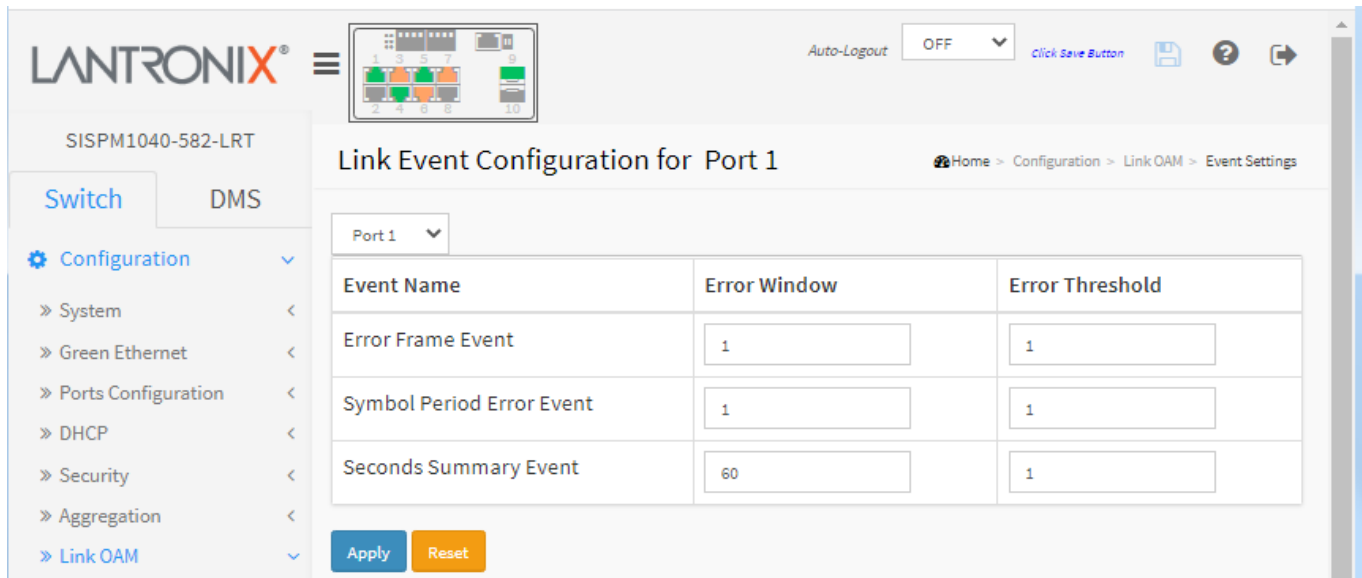


Figure 3-7.2: Event Settings

Parameter descriptions:

Port : The switch port number.

Event Name : The name of the Link Event being configured.

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

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

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

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 of 1-60 and its default value is '1'. Error Threshold must be between 0-4294967295 and its default value is '0'.

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 of 10-900 and its default value is '60'. Error Threshold must be between 0-65535 and its default value is '1'.

Buttons

Apply : Click to save changes.

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

3-8 Loop Protection

Loop Protection is used to detect the presence of traffic. The port will be locked when it receives looping Protection frames. To set Loop Protection parameters in the web UI:

1. Click Configuration and Loop Protection.
2. Select the Global and Port Loop Protection parameters.
3. Click the Apply button to save the settings.
4. To cancel the settings click the Reset button to revert to previously saved values.

The screenshot shows the 'Loop Protection Configuration' page in the Lantronix web UI. The page is titled 'Loop Protection Configuration' and is part of the 'SISPM1040-582-LRT' configuration. The page is divided into two main sections: 'Global Configuration' and 'Port Configuration'.

Global Configuration:

- Enable Loop Protection:** A dropdown menu set to 'Disable'.
- Transmission Time:** A text input field containing '5' followed by 'seconds'.
- Shutdown Time:** A text input field containing '180' followed by 'seconds'.

Port Configuration:

Port	Enable	Action	Tx Mode
*	<input checked="" type="checkbox"/>	<input type="text" value=""/>	<input type="text" value=""/>
1	<input checked="" type="checkbox"/>	Shutdown Port	Enable
2	<input checked="" type="checkbox"/>	Shutdown Port	Enable
3	<input checked="" type="checkbox"/>	Shutdown Port	Enable
4	<input checked="" type="checkbox"/>	Shutdown Port	Enable
5	<input checked="" type="checkbox"/>	Shutdown Port	Enable
6	<input checked="" type="checkbox"/>	Shutdown Port	Enable
7	<input checked="" type="checkbox"/>	Shutdown Port	Enable
8	<input checked="" type="checkbox"/>	Shutdown Port	Enable
9	<input checked="" type="checkbox"/>	Shutdown Port	Enable
10	<input checked="" type="checkbox"/>	Shutdown Port	Enable

At the bottom of the page, there are two buttons: 'Apply' (blue) and 'Reset' (orange).

Figure 3-8: Loop Protection Configuration

Parameter descriptions:**Global Configuration:**

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

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

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

Port Configuration :

Port No : The switch port number of the port.

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

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

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

Buttons

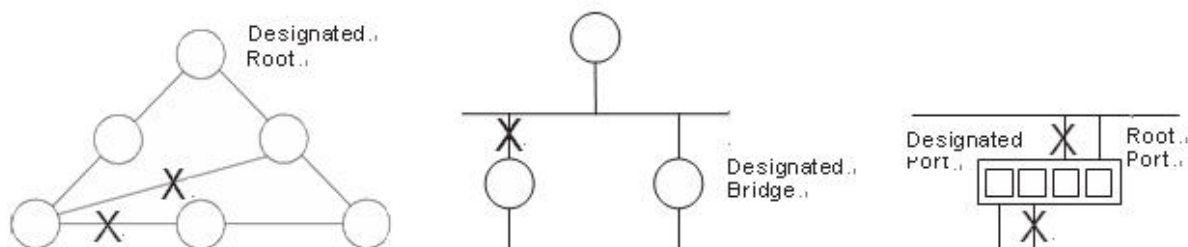
Apply : Click to save changes.

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

3-9 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 (an 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.



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.

MSTI: MSTP can generate multiple independent spanning trees in an MST region, and each spanning tree is mapped to the specific VLANs. Each spanning tree is referred to as a "multiple spanning tree instance (MSTI)".

CIST: The common and internal spanning tree (CIST) is a single spanning tree that connects all devices in a switched network. It consists of the ISTs in all MST regions and the CST.

The Spanning Tree sub parameters include Bridge Settings, MSTI Mapping, MSTI Priorities, CIST Port, and MSTI Ports as described below.

- » Spanning Tree ▾
- > Bridge Settings
- > MSTI Mapping
- > MSTI Priorities
- > CIST Port
- > MSTI Ports

3-9.1 Bridge Setting

This page lets you configure Spanning Tree Bridge and STP System settings. The STP System parameters are used by all STP Bridge instances in the switch.

To configure Spanning Tree Bridge parameters in the web UI:

1. Click Configuration, Spanning Tree and Bridge Settings.
2. Select the parameters and enter available value of parameters in blank field in Basic Settings.
3. Enable or disable the parameters and enter parameters in the blank Advanced Settings field.
4. Click the Apply button to save the settings.
5. To cancel the settings click the Reset button to revert to previously saved values.

The screenshot displays the 'STP Bridge Configuration' page in the Lantronix web UI. The page is titled 'STP Bridge Configuration' and includes a breadcrumb trail: Home > Configuration > Spanning Tree > Bridge Settings. The interface is split into two main sections: 'Basic Settings' and 'Advanced Settings'.

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	<input type="checkbox"/>
Edge Port BPDU Guard	<input type="checkbox"/>
Port Error Recovery	<input type="checkbox"/>
Port Error Recovery Timeout	

At the bottom of the configuration area, there are two buttons: 'Apply' (blue) and 'Reset' (orange). The left sidebar shows a navigation menu with 'Spanning Tree' > 'Bridge Settings' selected.

Figure 3-9.1: STP Bridge Configuration

Parameter descriptions:

Basic Settings

Protocol Version : The STP protocol version setting. Valid values are STP, RSTP and MSTP.

Bridge Priority : Controls the bridge priority. Lower numeric values have better priority. The bridge priority plus the MSTI instance number, concatenated with the 6-byte MAC address of the switch forms a Bridge Identifier. For MSTP operation, this is the priority of the CIST. Otherwise, this is the priority of the STP/RSTP Bridge.

Hello Time : The interval between sending STP BPDU's. Valid values are in the range 1 to 10 seconds, default is 2 seconds. **NOTE**: Changing this parameter from the default value is not recommended and may have adverse effects on your network.

Forward Delay : The delay used by STP Bridges to transit Root and Designated Ports to Forwarding (used in STP compatible mode). Valid values are 4 - 30 seconds.

Max Age : The maximum age of the information transmitted by the Bridge when it is the Root Bridge. Valid values are 6 - 40 seconds, and MaxAge must be $\leq (\text{FwdDelay}-1)*2$.

Maximum Hop Count : This defines the initial value of remaining Hops for MSTI information generated at the boundary of an MSTI region. It defines how many bridges a root bridge can distribute its BPDU information to. Valid values are in the range 6 to 40 hops.

Transmit Hold Count : The number of BPDU's a bridge port can send per second. When exceeded, transmission of the next BPDU will be delayed. Valid values are 1 - 10 BPDU's per second.

Advanced Settings

Edge Port BPDU Filtering : Control whether a port explicitly configured as Edge will transmit and receive BPDUs.

Edge Port BPDU Guard : Control whether a port explicitly configured as Edge will disable itself upon reception of a BPDU. The port will enter the error-disabled state and will be removed from the active topology.

Port Error Recovery : Control whether a port in the error-disabled state automatically will be enabled after a certain time. If recovery is not enabled, ports must be disabled and re-enabled for normal STP operation. The condition is also cleared by a system reboot.

Port Error Recovery Timeout : The time to pass before a port in the error-disabled state can be enabled. Valid values are between 30 and 86400 seconds (24 hours).

Buttons

Apply : Click to save changes.

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

3-9.2 MSTI Mapping

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. For that reason you must set the list of VLANs mapped to the MSTI. The VLANs must be separated with comma and/or space. A VLAN can only be mapped to one MSTI. An unused MSTI should just be left empty (i.e., not having any VLANs mapped to it).

This page lets you configure the current STP MSTI bridge instance priority parameters. To configure Spanning Tree MSTI Mapping parameters in the web UI:

1. Click Configuration, Spanning Tree, and MSTI Mapping.
2. Specify the configuration identification parameters in the field and specify the VLANs Mapped blank field.
3. Click the Apply button to save the settings.
4. To cancel the settings click the Reset button to revert to previously saved values.

The screenshot shows the Lantronix web interface for configuring MSTI Mapping. The page title is "MSTI Configuration" and the breadcrumb trail is "Home > Configuration > Spanning Tree > MSTI Mapping".

Configuration Identification

Configuration Name	00-c0-f2-49-39-30
Configuration Revision	0

MSTI Mapping

- Add VLANs separated by spaces or comma.
- Unmapped VLANs are mapped to the CIST. (The default bridge instance).

MSTI	VLANs Mapped
MSTI1	<input type="text"/>
MSTI2	<input type="text"/>
MSTI3	<input type="text"/>
MSTI4	<input type="text"/>
MSTI5	<input type="text"/>
MSTI6	<input type="text"/>
MSTI7	<input type="text"/>

Buttons: **Apply** (blue), **Reset** (orange)

Figure 3-9.2: MSTI Configuration

Parameter descriptions:**Configuration Identification**

Configuration Name : The name identifying the VLAN to MSTI mapping. Bridges must share the name and revision (see below), as well as the VLAN-to-MSTI mapping configuration in order to share spanning trees for MSTI's (Intra-region). The name is at most 32 characters.

Configuration Revision : The revision of the MSTI configuration named above. This must be an integer between 0 and 65535.

MSTI Mapping

MSTI : 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 VID (1 - 4094), or a range of VLAN IDs, each of which must be separated with comma and/or space. A VLAN can only be mapped to one MSTI. An unused MSTI should just be left empty (i.e., not have any VLANs mapped to it). For example: 2,5,20-40.

Buttons

Apply : Click to save changes.

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

3-9.3 MSTI Priorities

When you implement a Spanning Tree protocol on the switch that is the bridge instance. The CIST is the default instance which is always active to control the bridge priority. Lower numeric values have higher priority. The bridge priority plus the MSTI instance number, concatenated with the 6-byte MAC address of the switch, forms a Bridge Identifier. This page lets you configure STP MSTI bridge instance priority parameters.

To configure Spanning Tree MSTI Priorities parameters in the web UI:

1. Click Configuration, Spanning Tree and MSTI Priorities.
2. Select the Priority; the maximum is 240; the default is 128.
3. Click the Apply button to save the settings.
4. To cancel the settings click the Reset button to revert to previously saved values.

MSTI	Priority
*	32768
CIST	32768
MSTI1	32768
MSTI2	32768
MSTI3	32768
MSTI4	32768
MSTI5	32768
MSTI6	32768
MSTI7	32768

Figure 3-9.3: MSTI Configuration

Parameter descriptions:

MSTI : The bridge instance. The CIST is the default instance, which is always active.

Priority : Controls the bridge priority. Lower numeric values have better priority. The bridge priority plus the MSTI instance number, concatenated with the 6-byte MAC address of the switch forms a Bridge Identifier.

Buttons

Apply : Click to save changes.

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

3-9.4 CIST Port

This page lets you configure STP CIST port parameters for physical and aggregated ports. To configure Spanning Tree CIST Ports parameters in the web UI:

1. Click Configuration, Spanning Tree, and CIST Port.
2. Set all parameters of CIST Aggregated Port Configuration.
3. Enable or disable the STP, then set all parameters of the CIST normal Port configuration.
4. Click the Apply button to save the settings.
5. To cancel the settings click the Reset button to revert to previously saved values.

The screenshot displays the 'STP CIST Port Configuration' page in the Lantronix web UI. The page is divided into two main sections: 'CIST Aggregated Port Configuration' and 'CIST Normal Port Configuration'. Both sections contain tables with columns for Port, STP Enabled, Path Cost, Priority, Admin Edge, Auto Edge, Restricted (Role, TCN), BPDUs (Guard), and Point-to-point. The 'CIST Aggregated Port Configuration' table has one row with STP Enabled checked, Path Cost set to Auto, Priority 128, Admin Edge Non-Edge, Auto Edge checked, and various other options. The 'CIST Normal Port Configuration' table has 10 rows, each with STP Enabled checked, Path Cost set to Auto, Priority 128, Admin Edge Non-Edge, Auto Edge checked, and various other options. At the bottom, there are 'Apply' and 'Reset' buttons.

Figure 3-9.4: STP CIST Port Configuration

Parameter descriptions:

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

STP Enabled : Controls whether STP is enabled on this switch port.

Path Cost : Controls the path cost incurred by the port. The Auto setting will set the path cost as appropriate by the physical link speed, using the 802.1D recommended values. Using the Specific setting, a user-defined

value can be entered. The path cost is used when establishing the active topology of the network. Lower path cost ports are chosen as forwarding ports in favor of higher path cost ports. Valid values are 1 - 200000000.

Priority : Controls the port priority. This can be used to control priority of ports having identical port cost (see above).

operEdge (state flag) : Operational flag describing whether the port is connecting directly to edge devices. (No Bridges attached). Transition to the forwarding state is faster for edge ports (having operEdge true) than for other ports. The value of this flag is based on AdminEdge and AutoEdge fields. This flag is displayed as Edge in Monitor > Spanning Tree > STP Detailed Bridge Status.

AdminEdge : Controls whether the operEdge flag should start as set or cleared. (The initial operEdge state when a port is initialized.)

AutoEdge : Controls whether the bridge should enable automatic edge detection on the bridge port. This allows operEdge to be derived from whether BPDU's are received on the port or not.

Restricted Role : If enabled, causes the port not to be selected as Root Port for the CIST or any MSTI, even if it has the best spanning tree priority vector. Such a port will be selected as an Alternate Port after the Root Port has been selected. If set, it can cause lack of spanning tree connectivity. It can be set by a network administrator to prevent bridges external to a core region of the network influence the spanning tree active topology, possibly because those bridges are not under the full control of the administrator. This feature is also known as Root Guard.

Restricted TCN : If enabled, causes the port not to propagate received topology change notifications and topology changes to other ports. If set it can cause temporary loss of connectivity after changes in a spanning tree's active topology as a result of persistently incorrect learned station location information. It is set by a network administrator to prevent bridges external to a core region of the network, causing address flushing in that region, possibly because those bridges are not under the full control of the administrator or the physical link state of the attached LANs transits frequently.

BPDU Guard : If enabled, causes the port to disable itself upon receiving valid BPDU's. Contrary to the similar bridge setting, the port Edge status does not affect this setting. A port entering error-disabled state due to this setting is subject to the bridge Port Error Recovery setting as well.

Point to Point : Controls whether the port connects to a point-to-point LAN rather than to a shared medium. This can be automatically determined or forced either true or false. Transition to the forwarding state is faster for point-to-point LANs than for shared media.

Buttons

Apply : Click to save changes.

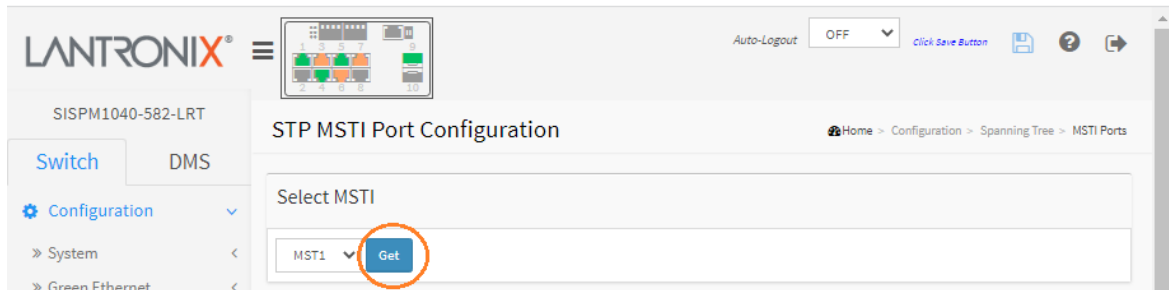
Reset : Click to undo any changes made locally and revert to previously saved values.

3-9.5 MSTI Ports

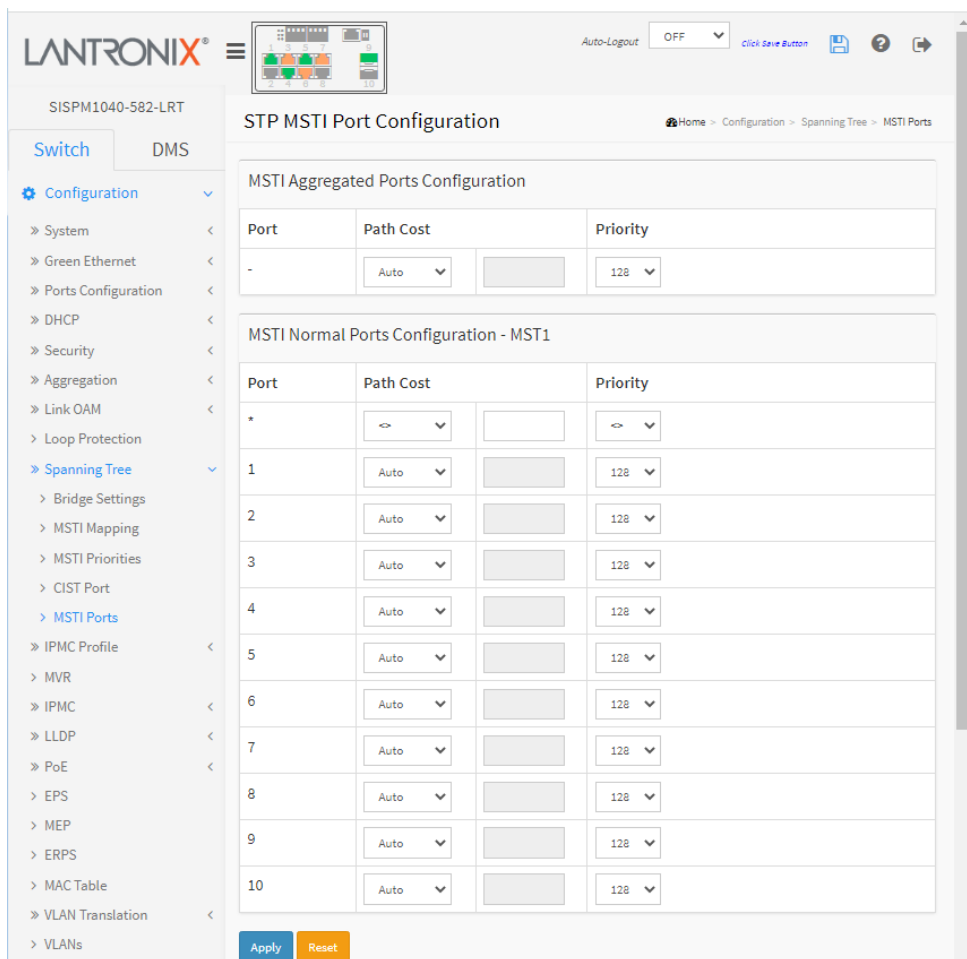
This page lets you configure STP MSTI port parameters. An MSTI port is a virtual port which is instantiated separately for each active CIST (physical) port for each MSTI instance configured on and applicable to the port. The MSTI instance must be selected before displaying actual MSTI port configuration options. It contains MSTI port settings for physical and aggregated ports.

To configure Spanning Tree MSTI Port parameters in the web UI:

1. Click Configuration, Spanning Tree, and MSTI Ports.
2. Select the MST1 or other MSTI Port.
3. Click **Get** to set the detail parameters of the MSTI Ports.



4. Set all MSTI Port parameters.
5. Click the Apply button to save the settings.
6. To cancel the settings click the Reset button to revert to previously saved values.



Parameter descriptions:

Port : The switch port number of the corresponding STP CIST (and MSTI) port.

Path Cost : Controls the path cost incurred by the port. The Auto setting will set the path cost as appropriate by the physical link speed, using the 802.1D recommended values. Using the Specific setting, a user-defined value can be entered. The path cost is used when establishing the active topology of the network. Lower path cost ports are chosen as forwarding ports in favor of higher path cost ports. Valid values are 1 - 200000000.

Priority : Controls the port priority. This can be used to control priority of ports having identical port cost (see above).

Buttons

Apply : Click to save changes.

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

3-10 IPMC Profile

This page provides IPMC Profile related configurations.

3-10.1 Profile Table

The IPMC profile is used to deploy the access control on IP multicast streams. You can create up to 64 Profiles with a maximum of 128 corresponding Rules for each Profile.

Web Interface

To configure IPMC Profile parameters in the web UI:

1. Click Configuration, IPMC Profile, and Profile Table.
2. Click the Add New IPMC Profile button.
3. Enable or disable the IPMC Profile parameter.
4. Create a profile, then click the edit button to enter the rule setting page of the designated profile.
5. Click Apply

The screenshot displays the 'IPMC Profile Configurations' web interface. On the left, a navigation menu shows 'Switch' and 'DMS' tabs, with 'Configuration' expanded to show 'IPMC Profile' and 'Profile Table'. The main content area is titled 'IPMC Profile Configurations' and includes a breadcrumb trail: Home > Configuration > IPMC Profile > Profile Table. The 'Global Profile Mode' is set to 'Enabled'. The 'IPMC Profile Table Setting' section contains a table with the following data:

Delete	Profile Name	Profile Description	Rule
<input type="checkbox"/>	Prof1	firstProfile in IPMC Profile Table	
<input type="checkbox"/>	Prof2	secondIPMCProfile	
<input type="checkbox"/>	Prof3	#3	

At the bottom of the table, there is an 'Add New IPMC Profile' button, and below that, 'Apply' and 'Reset' buttons.

Figure 2-10.1: IPMC Profile Configuration

Parameter descriptions:

Global Profile Mode : Enable/Disable the Global IPMC Profile. The system starts filtering based on profile settings only when the global profile mode is enabled.

Profile Name : The name used for indexing the profile table. Each entry has the unique name which is composed of at maximum 16 alphabetic and numeric characters. At least one alphabet must be present.

Profile Description : Additional description, which is composed of at maximum 64 alphabetic and numeric characters, about the profile. No blank or space characters are permitted as part of description. Use "_" or "-" to separate the description sentences.

Rule : When the profile is created, click the edit button to enter the rule setting page of the designated profile. Summary about the designated profile will be shown by clicking the view button. You can manage or inspect the rules of the designated profile by using the following buttons:



: List the rules associated with the designated profile.



: Adjust the rules associated with the designated profile.

Buttons

Add New IPMC Profile : Click to add new IPMC profile. Specify the name and configure the new entry. Click Apply.

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

Apply : Click to save changes.

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

IPMC Profile Rule Settings Table

This page provides the filtering rule settings for a specific IPMC profile. It displays the configured rule entries in precedence order. The first rule entry has highest priority in lookup; the last rule entry has lowest lookup priority.

Profile Name & Index	Entry Name	Address Range	Action	Log	
Prof1 1	-	~	Deny	Disable	⊕ ⊖ ⊗ ⊘

Buttons: Add Last Rule, Commit, Reset

Profile Name: The name of the designated profile to be associated. This field is not editable.

Entry Name: The name used in specifying the address range used for this rule.

Only the existing profile address entries will be chosen in the selected box. This field is not allowed to be selected as none ("-") while the Rule Settings Table is committed.

Address Range: The corresponding address range of the selected profile entry. This field is not editable and will be adjusted automatically according to the selected profile entry.

Action: Indicates the learning action upon receiving the Join/Report frame that has the group address matches the address range of the rule.

Permit: Group address matches the range specified in the rule will be learned.

Deny: Group address matches the range specified in the rule will be dropped.


Log: Indicates the logging preference upon receiving the Join/Report frame that has the group address matches the address range of the rule.


Enable: Corresponding information of the group address, that matches the range specified in the rule, will be logged.


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


Rule Management Buttons

You can manage rules and the corresponding precedence order by using these buttons:

: Insert a new rule before the current entry of rule.

: Delete the current entry of rule.

: Moves the current entry of rule up in the list.

: Moves the current entry of rule down in the list.

Buttons

Add Last Rule: Click to add a new rule in the end of the specific profile's rule list. Specify the address entry and configure the new entry. Click the "Commit" button.

Commit: Click to commit rule changes for the designated profile.

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

3-10.2 Address Entry

This page provides address range settings used in IPMC profile. The address entry is used to specify the address range that will be associated with IPMC Profile. You can create up to 128 address entries in the system.

To configure IPMC Profile Address parameters in the web UI:

1. Click Configuration, IPMC Profile and Address Entry.
2. Click the Add New Address (Range) Entry button.
3. Specify the Entry Name, Start Address, End Address.
4. Click Apply.

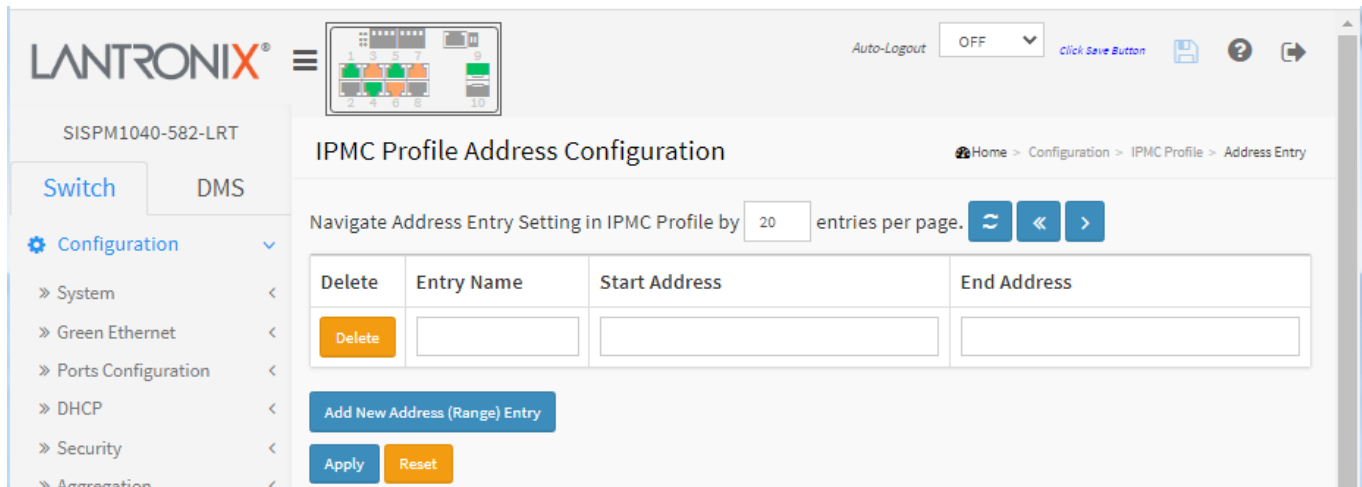


Figure 3-10.2: IPMC Profile Address Configuration

Parameter descriptions:

Entry Name : The name used for indexing the address entry table. Each entry has the unique name which is composed of at maximum 16 alphabetic and numeric characters. At least one alpha character must be present.

Start Address : The starting IPv4/IPv6 Multicast Group Address that will be used as an address range.

End Address : The ending IPv4/IPv6 Multicast Group Address that will be used as an address range.

Buttons

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

Add New Address (Range) Entry : Click to add new address range. Specify the name and configure the addresses. Click Apply when done.

Apply : Click to save changes.

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

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

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

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

3-11 MVR

The MVR (Multicast VLAN Registration) feature allows multicast traffic forwarding on Multicast VLANs. In a multicast television application, a PC or a TV 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/MLD report message to Switch A to join the appropriate multicast group address. Uplink ports that send / receive multicast data to / from the multicast VLAN are called MVR source ports. You can create up to four MVR VLANs with corresponding channel profile for each Multicast VLAN. The channel profile is defined by the IPMC Profile which provides the filtering conditions.

To configure MVR parameters in the web UI:

1. Click Configuration > MVR to display the MVR Configurations page.
2. Set the MVR mode to enable or disable and set all parameters.
3. Click the Add New MVR VLAN button, specify the VID, and configure the new entry.
4. Click the Apply button to save the settings. To cancel the settings click the Reset button.

The screenshot displays the 'MVR Configurations' page in the Lantronix web UI. The interface includes a sidebar with navigation options such as 'Switch', 'DMS', 'Configuration', 'System', 'Green Ethernet', 'Ports Configuration', 'DHCP', 'Security', 'Aggregation', 'Link OAM', 'Loop Protection', 'Spanning Tree', 'IPMC Profile', 'MVR', 'IPMC', 'LLDP', 'PoE', 'EPS', 'MEP', 'ERPS', 'MAC Table', 'VLAN Translation', 'VLANs', 'Private VLANs', 'VCL', 'Voice VLAN', 'Ethernet Services', 'QoS', and 'Mirroring'. The main content area is titled 'MVR Configurations' and contains the following sections:

- Global Setting:** MVR Mode is set to 'Enabled'.
- VLAN Interface Setting (Role [I:Inactive / S:Source / R:Receiver]):** A table with columns: Delete, MVR VID, MVR Name, IGMP Address, Mode, Tagging, Priority, LLQI, and Interface Channel Profile. The table contains one entry:

Delete	MVR VID	MVR Name	IGMP Address	Mode	Tagging	Priority	LLQI	Interface Channel Profile
<input type="checkbox"/>	1	MVRCFG1	192.168.1.99	Dynamic	Tagged	0	s	-
- Immediate Leave Setting:** A table with columns: Port and Immediate Leave. The table contains settings for ports 1 through 6:

Port	Immediate Leave
*	<<
1	Disabled
2	Enabled
3	Enabled
4	Enabled
5	Disabled
6	Disabled

Figure 3-11: MVR Configuration

Parameter descriptions:

MVR Mode : Enable/Disable the Global MVR. The Unregistered Flooding control depends on the current configuration in IGMP/MLD Snooping. It is suggested to enable Unregistered Flooding control when the MVR group table is full.

MVR VID : Specify the Multicast VLAN ID.

Caution: MVR source ports are not recommended to be overlapped with management VLAN ports.

MVR Name : MVR Name is an optional attribute to indicate the name of the specific MVR VLAN. Maximum length of the MVR VLAN Name string is 32. MVR VLAN Name can only contain alphabets or numbers. When

the optional MVR VLAN name is given, it should contain at least one alphabet. 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 from 0 to 31744. The default LLQI is 5 tenths or one-half second.

Interface Channel Setting : When the MVR VLAN is created, click the Edit symbol to expand the corresponding multicast channel settings for the specific MVR VLAN. Summary about the Interface Channel Setting (of the MVR VLAN) will be shown besides the Edit symbol.

Port : The logical port for the settings.

Port Role : Configure an MVR port of the designated MVR VLAN as one of the following roles.

Inactive: The designated port does not participate MVR operations.

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

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

Caution: MVR source ports are not recommended to be overlapped with management VLAN ports. Select the port role by clicking the Role symbol to switch the setting. **I** indicates Inactive; **S** indicates Source; **R** indicates Receiver. The default Role is Inactive.

Immediate Leave : Enable fast leave on the port. Multicast snooping Fast Leave processing allows the switch to remove an interface from the forwarding-table entry without first sending out group specific queries to the interface. The VLAN interface is pruned from the multicast tree for the multicast group specified in the original leave message. Fast-leave processing ensures optimal bandwidth management for all hosts on a switched network, even when multiple multicast groups are in use simultaneously. This processing applies to IGMP and MLD.

Buttons

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

Add New MVR VLAN : Click to add new MVR VLAN. Specify the VID, configure the new entry and click Apply.

Apply : Click to save changes.

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

3-12 IPMC

IPMC (IP MultiCast) supports IPv4 and IPv6 multicasting. IPMCv4 denotes multicast for IPv4. IPMCv6 denotes multicast for IPv6. It is used by network devices, including routers, to send error messages and operational information indicating, for example, that a requested service is not available or that a host or router could not be reached.

3-12.1 IGMP Snooping

IGMP (Internet Group Management Protocol) is a communications protocol used to manage the membership of IP multicast groups. IGMP is used by IP hosts and adjacent multicast routers to establish multicast group memberships. It is an integral part of the IP multicast specification, like ICMP for unicast connections. IGMP can be used for online video and gaming and allows more efficient use of resources when supporting these uses.

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 a broadcast packet.

A switch that supports the IGMP Snooping 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 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 enable IGMP proxy or snooping on the switch, which connects to a router closer to the root of the tree. This interface is the upstream interface. The router on the upstream interface should be running IGMP.

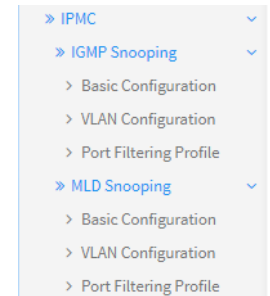
3-12.1.1 Basic Configuration

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 should be running IGMP.

Web Interface

To configure IGMP Snooping parameters in the web UI:

1. Click Configuration, IPMC, IGMP Snooping, and Basic Configuration.
2. Enable or disable which Global configuration.
3. Select which port you want to become a Router Port or enable/ disable the Fast Leave function.
4. Set the Throttling parameter.
5. Click the Apply button to save the settings.
6. To cancel the settings click the Reset button to revert to previously saved values.



SISPM1040-582-LRT

Switch DMS

Configuration

System

Green Ethernet

Ports Configuration

DHCP

Security

Aggregation

Link OAM

Loop Protection

Spanning Tree

IPMC Profile

MVR

IPMC

IGMP Snooping

Basic Configuration

VLAN Configuration

Port Filtering Profile

MLD Snooping

LLDP

PoE

EPS

MEP

ERPS

MAC Table

VLAN Translation

VLANs

Private VLANs

VCL

Voice VLAN

Ethernet Services

IGMP Snooping Configuration

Home > Configuration > IPMC > IGMP Snooping > Basic Configuration

Global Configuration

Snooping Enabled	<input checked="" type="checkbox"/>
Unregistered IPMCv4 Flooding Enabled	<input checked="" type="checkbox"/>
IGMP SSM Range	232.0.0.0 / 8
Leave Proxy Enabled	<input checked="" type="checkbox"/>
Proxy Enabled	<input checked="" type="checkbox"/>

Port Related Configuration

Port	Router Port	Fast Leave	Throttling
*	<input type="checkbox"/>	<input type="checkbox"/>	<input type="text" value=""/>
1	<input type="checkbox"/>	<input type="checkbox"/>	unlimited
2	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	2
3	<input checked="" type="checkbox"/>	<input type="checkbox"/>	unlimited
4	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	8
5	<input type="checkbox"/>	<input type="checkbox"/>	unlimited
6	<input type="checkbox"/>	<input type="checkbox"/>	unlimited
7	<input type="checkbox"/>	<input type="checkbox"/>	unlimited
8	<input type="checkbox"/>	<input type="checkbox"/>	unlimited
9	<input type="checkbox"/>	<input type="checkbox"/>	unlimited
10	<input type="checkbox"/>	<input type="checkbox"/>	unlimited

Apply Reset

Figure 3-12.1.1: IGMP Snooping Configuration

Parameter descriptions:

Global Configuration

Snooping Enabled : Enable the Global IGMP Snooping.

Unregistered IPMCv4 Flooding enabled : Enable unregistered IPMCv4 traffic flooding.

IGMP SSM Range : SSM (Source-Specific Multicast) Range allows the SSM-aware hosts and routers run the SSM service model for the groups in the address range. Format: (IP address/ sub mask)

Leave Proxy Enable: 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 : The physical Port index of the switch.

Router Port : Specify which ports act as router ports. A router port is a port on the Ethernet switch that leads towards the Layer 3 multicast device or IGMP querier. If an aggregation member port is selected as a router port, the whole aggregation will act as a router port.

Fast Leave : Enable the fast leave on the port.

Throttling : Enable to limit the number of multicast groups to which a switch port can belong.

Buttons

Apply : Click to save changes.

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

3-12.1.2 VLAN Configuration

This page lets you configure the VLAN configuration setting process integrated with the IGMP Snooping function. For each setting page shows up to 99 entries from the VLAN table, default being 20, selected through the "entries per page" input field. When first visited, the web page displays the first 20 entries from the beginning of the VLAN Table. The first displayed will be the one with the lowest VLAN ID found in the VLAN Table. The "VLAN" input fields allow the user to select the starting point in the VLAN Table. Clicking the Refresh button will update the displayed table starting from that or the next closest VLAN Table match.

Web Interface

To configure IGMP Snooping VLAN parameters in the web UI:

1. Click Configuration, IPMC, IGMP Snooping and VLAN Configuration.
2. Enable or disable Snooping and, IGMP Querier. Specify the parameters in the blank field.
3. Click the Refresh button to update the data or click << or >> to display previous entry or next entry.
4. Click the Apply button to save the setting.
5. To cancel the settings click the Reset button to revert to previously saved values.

The screenshot shows the 'IGMP Snooping VLAN Configuration' page in the Lantronix web interface. The page title is 'IGMP Snooping VLAN Configuration' and the breadcrumb trail is 'Home > Configuration > IPMC > IGMP Snooping > VLAN Configuration'. The interface includes a navigation menu on the left with options like 'Switch', 'DMS', 'Configuration', 'System', 'Green Ethernet', 'Ports Configuration', 'DHCP', 'Security', 'Aggregation', 'Link OAM', 'Loop Protection', and 'Spanning Tree'. The main content area shows a table with the following columns: Delete, VLAN ID, Snooping Enabled, Querier Election, Querier Address, Compatibility, PRI, RV, QI (sec), QRI (0.1 sec), LLQI (0.1 sec), and URI (sec). The table contains three entries for VLANs 10, 20, and 30. Below the table are buttons for 'Add New IGMP VLAN', 'Apply', and 'Reset'. The 'Start from VLAN' field is set to 1 and 'entries per page' is set to 20.

Delete	VLAN ID	Snooping Enabled	Querier Election	Querier Address	Compatibility	PRI	RV	QI (sec)	QRI (0.1 sec)	LLQI (0.1 sec)	URI (sec)
<input type="checkbox"/>	10	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	1.2.3.4	IGMP-Auto	0	2	125	100	10	1
<input type="checkbox"/>	20	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	192.168.1.99	Forced IGMPv3	1	2	125	100	10	1
<input type="checkbox"/>	30	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	0.0.0.0	IGMP-Auto	0	2	125	100	10	1

Figure 3-12.1.2: IGMP Snooping VLAN Configuration

Parameter descriptions:

VLAN ID : It displays the VLAN ID of the entry.

Snooping Enabled : Enable the per-VLAN IGMP Snooping. Only up to 32 VLANs can be selected. .

Querier Election : Enable to join IGMP Querier election in the VLAN. Disable to act as an IGMP Non-Querier.

Querier Address : Define the IPv4 address as source address used in IP header for IGMP Querier election. When the Querier address is not set, system uses IPv4 management address of the IP interface associated with this VLAN. When the IPv4 management address is not set, system uses the first available IPv4 management address. Otherwise, system uses a pre-defined value. By default, this value will be 192.0.2.1.

Compatibility : Compatibility is maintained by hosts and routers taking appropriate actions depending on the versions of IGMP operating on hosts and routers within a network. The allowed selections are IGMP-Auto, Forced IGMPv1, Forced IGMPv2, and Forced IGMPv3. The default compatibility value is IGMP-Auto.

PRI : Priority of Interface indicates the IGMP control frame priority level generated by the system. These values can be used to prioritize different classes of traffic. The allowed range is 0 (best effort) to 7 (highest), default interface priority value is 0.

Rv : Robustness Variable. The RV allows tuning for the expected packet loss on a network. The allowed range is 1 to 255; the default RV value is 2.

QI : Query Interval. The QI is the interval between General Queries sent by the Querier. The allowed range is 1 to 31744 seconds; default QI is 125 seconds.

QRI : Query Response Interval. The Max Response Time used to calculate the Max Resp Code inserted into the periodic General Queries. The allowed range is 0 to 31744 in tenths of seconds; default QRI is 100 in tenths of seconds (10 seconds).

LLQI (LMQI for IGMP) : Last Member Query Interval. The Last Member Query Time is the time value represented by the Last Member Query Interval, multiplied by the Last Member Query Count. The allowed range is 0 - 31744 in tenths of seconds; default last member query interval is 10 in tenths of a second (1 second).

URI : Unsolicited Report Interval. The Unsolicited Report Interval is the time between repetitions of a host's initial report of membership in a group. The allowed range is 0 - 31744 seconds; the default unsolicited report interval is 1 second.

Buttons

Apply : Click to save changes.

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

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

Refresh: Click to manually refresh the page immediately.

<< : Click to update the table starting from the first entry in the VLAN table (the entry with the lowest VLAN ID).

> : Click to update the table, starting with the entry after the last entry currently displayed.

2-12.1.3 Port Filtering Profile

This page lets you configure IGMP Port Group Filtering. With the IGMP filtering feature, you can exert this type of control. In some network Application environments, like the metropolitan or multiple-dwelling unit (MDU) installations, you might want to control the multicast groups to which a user on a switch port can belong.

It allows you to control the distribution of multicast services, such as IP/TV, based on some type of subscription or service plan.

With this feature, you can filter multicast joins on a per-port basis by configuring IP multicast profiles and associating them with individual switch ports. An IGMP profile can contain one or more multicast groups and specifies whether access to the group is permitted or denied. If an IGMP profile denying access to a multicast group is applied to a switch port, the IGMP join report requesting the stream of IP multicast traffic is dropped, and the port is not allowed to receive IP multicast traffic from that group. If the filtering action permits access to the multicast group, the IGMP report from the port is forwarded for normal processing.

IGMP filtering controls only IGMP membership join reports and has no relationship to the function that directs the forwarding of IP multicast traffic.

To configure IGMP Snooping Port Filtering profiles in the web UI:

1. Click Configuration, IPMC, IGMP Snooping, and Port Filtering Profile.
2. Enable Port Group Filtering. Specify the Filtering Groups in the blank field.
3. Click the Apply button to save the settings.
4. To cancel the settings click the Reset button to revert to previously saved values.

The screenshot shows the Lantronix web interface for configuring IGMP Snooping Port Filtering Profiles. The breadcrumb trail is: Home > Configuration > IPMC > IGMP Snooping > Port Filtering Profile. The page title is "IGMP Snooping Port Filtering Profile Configuration".

Port	Filtering Profile
1	-
2	-
3	-
4	-
5	-
6	-
7	-
8	-
9	-
10	-

At the bottom of the table, there are two buttons: "Apply" (blue) and "Reset" (orange).

Figure 2-12.1.3: IGMP Snooping Port Filtering Profile

Parameter descriptions:

Port : The logical port for the settings.

Filtering Profile : Select the IPMC Profile as the filtering condition for the specific port. Summary about the designated profile will be shown by clicking the view button.

Profile Management button : You can inspect the rules of the designated profile by using the following button:



: List the rules associated with the designated profile.

Buttons

Apply : Click to save changes.

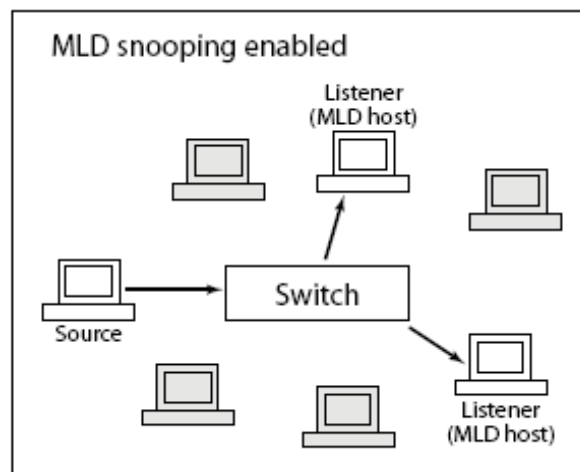
Reset : Click to undo any changes made locally and revert to previously saved values.

3-12.2 MLD Snooping

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



3-12.2.1 Basic Configuration

This page lets you configure MLD Snooping global and port-related parameters.

Web Interface

To configure MLD Snooping in the web UI:

1. Click Configuration, IPMC, MLD Snooping, and Basic Configuration.
2. Set the Global Configuration parameters.
3. Set the Port Related Configuration parameters.
4. Click the Apply button to save the settings.
5. To cancel the settings click the Reset button to revert to previously saved values.

The screenshot displays the MLD Snooping Configuration page for the SISPM1040-582-LRT device. The breadcrumb trail indicates the path: Home > Configuration > IPMC > MLD Snooping > Basic Configuration. The left navigation menu shows the current location under IPMC > MLD Snooping > Basic Configuration.

Global Configuration

Snooping Enabled	<input type="checkbox"/>
Unregistered IPMCv6 Flooding Enabled	<input checked="" type="checkbox"/>
MLD SSM Range	ff3e:: / 96
Leave Proxy Enabled	<input type="checkbox"/>
Proxy Enabled	<input type="checkbox"/>

Port Related Configuration

Port	Router Port	Fast Leave	Throttling
*	<input type="checkbox"/>	<input type="checkbox"/>	<> ▼
1	<input type="checkbox"/>	<input type="checkbox"/>	unlimited ▼
2	<input type="checkbox"/>	<input type="checkbox"/>	unlimited ▼
3	<input type="checkbox"/>	<input type="checkbox"/>	unlimited ▼
4	<input type="checkbox"/>	<input type="checkbox"/>	unlimited ▼
5	<input type="checkbox"/>	<input type="checkbox"/>	unlimited ▼
6	<input type="checkbox"/>	<input type="checkbox"/>	unlimited ▼
7	<input type="checkbox"/>	<input type="checkbox"/>	unlimited ▼

Figure 3-12.2.1: MLD Snooping Configuration

Parameter descriptions:

Snooping Enabled : Enable the Global MLD Snooping.

Unregistered IPMCv6 Flooding enabled : Enable unregistered IPMCv6 traffic flooding. The flooding control takes effect only when MLD Snooping is enabled. When MLD Snooping is disabled, unregistered IPMCv6 traffic flooding is always active in spite of this setting.

MLD SSM Range : SSM (Source-Specific Multicast) Range allows the SSM-aware hosts and routers run the SSM service model for the groups in the address (Using IPv6 Address) range.

Leave Proxy Enabled : Enable MLD Leave Proxy. This feature can be used to avoid forwarding unnecessary leave messages to the router side.

Proxy Enabled : Enable MLD Proxy. This feature can be used to avoid forwarding unnecessary join and leave messages to the router side.

Router Port : Specify which ports act as router ports. A router port is a port on the Ethernet switch that leads towards the Layer 3 multicast device or MLD querier. If an aggregation member port is selected as a router port, the whole aggregation will act as a router port.

Fast Leave : To evoke to enable the fast leave on the port.

Throttling : Enable to limit the number of multicast groups to which a switch port can belong.

Buttons

Apply : Click to save changes.

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

3-12.2.2 VLAN Configuration

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

The > button 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. Use the << button to start over.

To configure MLD Snooping VLAN in the web UI:

1. Click Configuration, IPMC, MLD Snooping and VLAN Configuration.
2. Click the Add New MLD VLAN button to add a new row to the table.
4. Specify the VLAN ID with entries per page.
5. Click "Refresh" to refresh an entry of the MLD Snooping VLAN Configuration Information.
6. Click "<< or >" to move to previous or next entry.

The screenshot shows the 'MLD Snooping VLAN Configuration' page in the Lantronix web UI. The page title is 'MLD Snooping VLAN Configuration' and the breadcrumb trail is 'Home > Configuration > IPMC > MLD Snooping > VLAN Configuration'. The page includes a navigation menu on the left with 'Switch' and 'DMS' tabs. The main content area shows a table of VLAN configurations. The table has columns for 'Delete', 'VLAN ID', 'Snooping Enabled', 'Querier Election', 'Compatibility', 'PRI', 'RV', 'QI (sec)', 'QRI (0.1 sec)', 'LLQI (0.1 sec)', and 'URI (sec)'. There are two entries in the table. The first entry has a 'Delete' button, 'VLAN ID' 10, 'Snooping Enabled' checked, 'Querier Election' checked, 'Compatibility' 'MLD-Auto', 'PRI' 1, 'RV' 2, 'QI (sec)' 125, 'QRI (0.1 sec)' 100, 'LLQI (0.1 sec)' 9, and 'URI (sec)' 1. The second entry has a 'Delete' button, 'VLAN ID' (empty), 'Snooping Enabled' unchecked, 'Querier Election' checked, 'Compatibility' 'MLD-Auto', 'PRI' 0, 'RV' 2, 'QI (sec)' 125, 'QRI (0.1 sec)' 100, 'LLQI (0.1 sec)' 10, and 'URI (sec)' 1. Below the table are buttons for 'Add New MLD VLAN', 'Apply', and 'Reset'. The page also includes an 'Auto-Logout' dropdown set to 'OFF' and a 'Click Save Button' link.

Figure 3-12.2.2: MLD Snooping VLAN Configuration

Parameter descriptions:

VLAN ID : It displays the VLAN ID of the entry.

Snooping Enabled : Enable the per-VLAN IGMP Snooping. Only up to 32 VLANs can be selected. .

Querier Election : Enable to join IGMP Querier election in the VLAN. Disable to act as an IGMP Non-Querier.

Compatibility : Compatibility is maintained by hosts and routers taking appropriate actions depending on the versions of IGMP operating on hosts and routers within a network. The allowed selections are IGMP-Auto, Forced IGMPv1, Forced IGMPv2, and Forced IGMPv3 The default Compatibility value is IGMP-Auto.

PRI : Priority of Interface; indicates the IGMP control frame priority level generated by the system. These values can be used to prioritize different classes of traffic. The allowed range is 0 (best effort) to 7 (highest); the default PRI value is 0.

Rv : Robustness Variable allows tuning for the expected packet loss on a network. The allowed range is 1 - 255; the default RV value is 2.

QI(sec) : Query Interval. The QI is the interval between General Queries sent by the Querier. The allowed range is 1 - 31744 seconds; the default query interval is 125 seconds.

QRI (0.1 sec) : Query Response Interval. The Max Response Time used to calculate the Max Resp Code inserted into the periodic General Queries. The allowed range is 0 - 31744 in tenths of seconds; the default QRI is 100 in tenths of seconds (10 seconds).

LLQI (0.1 sec) (LMQI for IGMP) : Last Member Query Interval. The Last Member Query Time is the time value represented by the Last Member Query Interval, multiplied by the Last Member Query Count. The allowed range is 0 - 31744 in tenths of seconds; default last member query interval is 10 in tenths of seconds (1 second).

URI (sec) : Unsolicited Report Interval. The Unsolicited Report Interval is the time between repetitions of a host's initial report of membership in a group. The allowed range is 0 - 31744 seconds, default unsolicited report interval is 1 second. .

Buttons

Apply : Click to save changes.

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

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

Refresh : Click them to Refresh the displayed table starting from the "VLAN" input fields.

<< : Click to update the table starting from the first entry in the VLAN table (the entry with the lowest VLAN ID).

> : Click to update the table, starting with the entry after the last entry currently displayed.

Add New MLD VLAN : Click to add a new MLD VLAN. Specify the VID and configure the new entry. Click "Save". The specific MLD VLAN starts working after the corresponding static VLAN is also created.

3-12.2.3 Port Filtering Profile

This page lets you set the Port Group Filtering in the MLD Snooping function. You can add a new filtering group and safety policy.

To configure MLD Snooping Port Group in the web UI:

1. Click Configuration, IPMC, MLD Snooping, and Port Filtering Profile.
2. Specify the Filtering Groups entries per page.
3. Click the Apply button to save the settings.
4. To cancel the settings click the Reset button to revert to previously saved values.

The screenshot shows the Lantronix web interface for configuring MLD Snooping Port Filtering Profiles. The page title is "MLD Snooping Port Filtering Profile Configuration". The breadcrumb navigation is "Home > Configuration > IPMC > MLD Snooping > Port Filtering Profile". The left sidebar shows the navigation menu with "IPMC" expanded to "MLD Snooping" and "Port Filtering Profile" selected. The main content area contains a table with 10 rows, one for each port (1-10). Each row has a "Port" column, a "Filtering Profile" column with a blue eye icon and a dropdown menu, and a "Profile Management" button (represented by a blue eye icon). At the bottom of the table are "Apply" and "Reset" buttons.

Port	Filtering Profile	Profile Management
1	[Eye Icon] [Dropdown]	[Eye Icon]
2	[Eye Icon] [Dropdown]	[Eye Icon]
3	[Eye Icon] [Dropdown]	[Eye Icon]
4	[Eye Icon] [Dropdown]	[Eye Icon]
5	[Eye Icon] [Dropdown]	[Eye Icon]
6	[Eye Icon] [Dropdown]	[Eye Icon]
7	[Eye Icon] [Dropdown]	[Eye Icon]
8	[Eye Icon] [Dropdown]	[Eye Icon]
9	[Eye Icon] [Dropdown]	[Eye Icon]
10	[Eye Icon] [Dropdown]	[Eye Icon]

Figure 3-12.2.3: MLD Snooping Port Filtering Profile Configuration

Parameter descriptions:

Port : The logical port for the settings.

Filtering Profile : Select the IPMC Profile as the filtering condition for the specific port. Summary about the designated profile will be shown by clicking the view button.

Profile Management button : You can inspect the rules of the designated profile by using the following button:



: List the rules associated with the designated profile.

Buttons

Apply : Click to save changes.

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

3-13 LLDP

The Link Layer Discovery Protocol (LLDP) provides a standards-based method for enabling switches to advertise themselves to adjacent devices and to learn about adjacent LLDP devices. LLDP is a vendor-neutral Link Layer protocol in the Internet Protocol Suite used by network devices for advertising their identity, capabilities, and neighbors on a IEEE 802 local area network, principally wired Ethernet. The protocol is formally referred to by the IEEE as Station and Media Access Control Connectivity Discovery specified in standards document [IEEE 802.1AB](http://www.ieee.org/standards/publications/IEEE%20802.1AB).

3-13.1 LLDP

This page lets you configure LLDP port settings. You can configure LLDP on a per-port basis including all detail parameters; the settings will take effect immediately. To configure LLDP in the web UI:

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

The screenshot shows the LLDP Configuration page in the Lantronix web UI. The page is titled 'LLDP Configuration' and includes a breadcrumb trail: Home > Configuration > LLDP > LLDP. The main content area is divided into two sections: 'LLDP Parameters' and 'LLDP Port Configuration'.

LLDP Parameters

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

LLDP Port Configuration

Port	Mode	CDP aware	Optional TLVs				
			Port Descr	Sys Name	Sys Descr	Sys Capa	Mgmt Addr
*	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
1	Enabled	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
2	Enabled	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
3	Enabled	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
4	Enabled	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
5	Enabled	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
6	Enabled	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
7	Enabled	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
8	Enabled	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

Figure 3-13.1: LLDP Configuration

Parameter descriptions:**LLDP Parameters**

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

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

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

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

LLDP Port Configuration

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

Mode : Select the desired LLDP mode:

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

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

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

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

CDP Aware : Select CDP (Cisco Discovery Protocol) awareness. The CDP operation is restricted to decoding 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.

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

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

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

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

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

Buttons

Apply : Click to save changes.

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

2-13.2 LLDP-MED

This page lets you configure LLDP-MED parameters that apply to VoIP devices supporting LLDP-MED. Media Endpoint Discovery is an enhancement of LLDP, known as LLDP-MED that provides:

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

To configure LLDP-MED via the Web UI:

1. Click Configuration, LLDP, LLDP-MED.
2. Set the Fast start repeat count parameter; the default is 4.
3. In the Transmit TLVs section specify the Capabilities, Policies, and Location for each port.
4. Set the Coordinates Location parameters and the Civic Address Location parameters.
5. Enter the Emergency Call Service parameters.
6. Click the Add New Policy button. In the Policies section, enter the various parameters.
7. Click the Apply button to display the Policy Port Configuration table.
8. For each port check or uncheck the Policy ID checkbox.
9. Click the Apply button to save the changes.

The screenshot displays the LLDP-MED Configuration page in the Lantronix web interface. The page is titled "LLDP-MED Configuration" and is part of the "Configuration" menu. The left sidebar shows the navigation tree with "LLDP-MED" selected. The main content area includes the following sections:

- Fast Start Repeat Count:** A text input field with the value "4".
- Transmit TLVs:** A table with columns for Port, Capabilities, Policies, Location, and PoE. All checkboxes are checked.
- Coordinates Location:** Fields for Latitude, Longitude, Altitude, and Map Datum.
- Civic Address Location:** A grid of fields for 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, and Additional code.
- Emergency Call Service:** A text input field for the Emergency Call Service.
- Policies:** A table with columns for Delete, Policy ID, Application Type, Tag, VLAN ID, L2 Priority, and DSCP. It shows "No entries present" and an "Add New Policy" button.

Figure 3-13.2: LLDP-MED Configuration

Parameter descriptions:

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

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

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

Note 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

It is possible to select which LLDP-MED information will be transmitted to the neighbors. When the checkbox is checked the information is included in the frame transmitted to the neighbor.

Port : The interface port number to which the configuration applies.

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

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

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

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

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 4 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, Prime Meridian Name: Greenwich.

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

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

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

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

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

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

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

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

Block (Neighborhood) : Neighborhood, block.

Street : Street - Example: Poppelvej.

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

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

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

House no. : House number - Example: 21.

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

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

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

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

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

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

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

Floor : Floor - Example: 4.

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

Place type : Place type - Example: Office.

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

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

Additional code : Additional code - Example: 1320300003.

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

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

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

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

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

This network policy is potentially advertised and associated with multiple sets of application types supported on a given port. The application types specifically addressed are 1. Voice, 2. Guest Voice, 3. Softphone Voice, 4. Video Conferencing, 5. Streaming Video, and 6. Control / Signaling (conditionally support a separate network policy for media types above).

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

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

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

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

Application Type : At the dropdown select Voice, Voice Signaling, Guest Voice, Guest Voice Signaling, Softphone Voice, Video Conferencing, Streaming Video, or Video Signaling. 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 Signaling (conditional) - for use in network topologies that require a different policy for the voice signaling than for the voice media. This application type should not be advertised if all the same network policies apply as those advertised in the Voice application policy.

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

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

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

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

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

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

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

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

Port Policies Configuration : Every port may advertise a unique set of network policies or different attributes for the same network policies, based on the authenticated user identity or port configuration.

Port : The port number to which the configuration applies.

Policy Id : The set of policies that will apply to a given port. The set of policies is selected by check marking the checkboxes that corresponds to the policies.

Buttons:

Apply – Click to save changes.

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

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

The Application Type dropdown is shown below.

Policies						
Delete	Policy ID	Application Type	Tag	VLAN ID	L2 Priority	DSCP
<input type="button" value="Delete"/>	0	<div style="border: 1px solid black; padding: 2px;"> Voice Voice Signaling Guest Voice Guest Voice Signaling Softphone Voice Video Conferencing Streaming Video Video Signaling </div>	Tagged <input type="button" value="v"/>	<input type="text" value="1"/>	<input type="text" value="0"/>	<input type="text" value="0"/>
<input type="button" value="Add New Policy"/>						

3-14 PoE

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.

3-14.1 Configuration

This page lets you configure the current PoE port and PoE supply parameters. To configure Power over Ethernet via the web UI (before FW VB7.10.2658):

1. Click Configuration, PoE, Configuration.
2. Specify Reserved Power determined by and Power Management Mode.
3. Check the Capacitor Detection checkbox if required.
4. In the PoE Port Configuration section, set PoE Mode, PoE Schedule, Priority, and Maximum Power for each port.
5. Click Apply.

Port	PoE Mode	PoE Schedule	Priority	Maximum Power [W]
1	Disabled	Disabled	High	30
2	Aggr	Disabled	High	30
3	Aggr	Disabled	High	30
4	Aggr	Disabled	Critical	30
5	Enabled	Disabled	Low	30
6	Enabled	Disabled	Low	30
7	Enabled	Disabled	Low	30
8	Enabled	Disabled	Low	30

Figure 3-14.1: PoE Configuration (before FW VB7.10.2658)

Parameter descriptions:

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

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

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

LLDP-MED: This mode is similar to the Class mode except that each port determines the amount power it reserves by exchanging PoE information using the LLDP protocol and reserves power accordingly. If no LLDP information is available for a port, the port will reserve power using the Class mode. In Class mode the Maximum Power fields have no effect for all modes: If a port uses more power than the reserved power for the port, the port is shut down.

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

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

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

Capacitor Detection : Check the box to enable Capacitor Detection mode for legacy device detection. Legacy PDs

refers to powered devices manufactured before the IEEE standard was finalized and do not have the expected PD signature required by the PSE's detection signal. Such PDs usually feature large capacitance as the detection signature that does not completely comply with the 802.3af specs. By enabling this option, the switch will probe for legacy PDs and if a legacy PD is detected, the switch will provide power to the PD.

PoE Power Supply Configuration section

Primary Power Supply : Note the read-only value of 480 Watts.

PoE Port Configuration section

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

PoE Mode : At the PoE Mode select the PoE operating mode for each port.

Disabled: PoE disabled for the port.

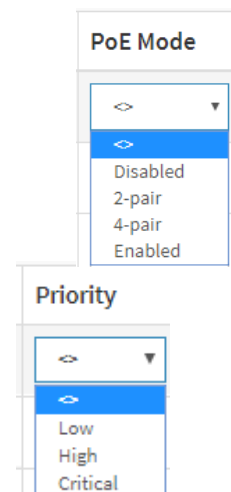
Enabled : Enables PoE IEEE 802.3bt (Class 4 PDs limited to 90W).

2-pair : The switch port will power up the linked PD using 2-pair mode.

4-pair : The switch port will power up the linked PD using 4-pair mode.

PoE Schedule : At the dropdown, select Profile 1 – Profile 16 or Disabled.

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 devices require more power than the power supply can deliver. In this case the port with the lowest priority will be turned off starting from the port with the highest port number.



Maximum Power : The Maximum Power value contains a numerical value that indicates the maximum power in watts that can be delivered to a remote device. **Note:** the PoE Maximum Power 90W Web UI settings are:

1. PoE Ports Default Setting = 60W.
2. PoE 90W setting restrictions:
 - a. The 8 ports PoE consists of 2 Ports and is divided into these four groups:
 - (1) Port 1,2
 - (2) Port 3,4
 - (3) Port 5,6
 - (4) Port 7,8
 - b. Each group of 2 Ports plus the PoE Output Power limit setting is less than or equal to 120W; the maximum per port: 90W. See the description below.

Buttons:

Apply – Click to save changes.

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

PoE Port Maximum Power Configuration Description (before FW VB7.10.2658):

PoE Port Configuration

Note Maximum Power [W] Field Settings Limitation:
Port (1+2),(3+4),(5+6),(7+8) four groups can't over 120W per group, and per port maximum is 90W.

Port	PoE Mode	PoE Schedule	Priority	Maximum Power [W]
*	<>	<>	<>	60
1	Enabled	Disabled	Low	60
2	Enabled	Disabled	Low	60
3	Enabled	Disabled	Low	60
4	Enabled	Disabled	Low	60
5	Enabled	Disabled	Low	60
6	Enabled	Disabled	Low	60
7	Enabled	Disabled	Low	60
8	Enabled	Disabled	Low	60

Apply
Reset

Group 1: Ports 1 and 2

Group 2: Ports 3 and 4

Group 3: Ports 5 and 6

Group 4: Ports 7 and 8

Four groups (Port 1+2) , (Port 3+4), (Port 5+ 6), (Port 7+ 8); maximum 120W per group; maximum 90W per port.

Note: When you click **Apply** and the settings add up to more than 120W per group, the Web UI will display the *over 120W groups* message, and these settings cannot be applied successfully.

Message: PoE Mode(Force) : The switch port will power up the linked PD without any detect/negotiate mechanism (PD limited to 90W). Do you want to Change this setting?

Message: PoE Port Configuration

Note Maximum Power [W] Field Settings Limitation:

4 groups (Port 1+2) , (Port 3+4), (Port 5+ 6), (Port 7+ 8), maximum per group: 120W, maximum per port: 90W

Web Interface

To configure Power over Ethernet via the web UI (FW VB7.10.2658 and above):

1. Click Configuration, PoE, Configuration.
2. Specify PoE Port Configuration parameters.
3. Click Apply.

The screenshot shows the Lantronix web interface for PoE configuration. The primary power supply is set to 480W. The PoE port configuration table is as follows:

Port	PoE Mode	PoE Schedule	Priority	LLDP	Legacy
*	<>	<>	<>	<>	<>
1	8023bt60w	Disabled	Low	Enabled	Disabled
2	8023bt60w	Disabled	Low	Enabled	Disabled
3	8023bt60w	Disabled	Low	Enabled	Disabled
4	8023bt60w	Disabled	Low	Enabled	Disabled
5	8023bt60w	Disabled	Low	Enabled	Disabled
6	8023bt60w	Disabled	Low	Enabled	Disabled
7	8023bt60w	Disabled	Low	Enabled	Disabled
8	8023bt60w	Disabled	Low	Enabled	Disabled

Figure 3-14.1: PoE Configuration (FW VB7.10.2658 and above)

Parameter descriptions:

Power Supply Configuration

Primary Power Supply: Displays the amount of power the PD may use; it must be defined what amount of power a power source can deliver. Valid values are 0-2000 Watts.

Port Configuration: Note Maximum Power [W] Field Settings Limitation:

4 groups (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 thus impossible to configure PoE for.

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

Disabled : PoE disabled for the port.

4pair60w : The switch port will power up the linked PD using 4-pair mode (PDs limited to 60W).

4pair90w : The switch port will power up the linked PD using 4-pair mode (PDs limited to 90W).

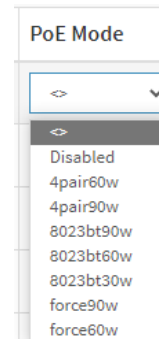
8023bt90w : Enables PoE IEEE 802.3bt (Class 8 PDs limited to 90W).

8023bt60w : Enables PoE IEEE 802.3bt (Class 8 PDs limited to 60W) (default setting).

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

force90w : Enables PoE force power (PDs limited to 90W).

force60w : Enables PoE force power (PDs limited to 60W).

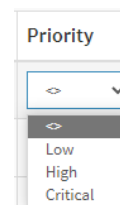


PoE Schedule: Scheduled by selecting PoE Scheduling Profile (Disabled or Profile 1-16).

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 devices 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).

**Buttons**

Apply: Click to save changes.

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

Note PoE Mode Settings Limitation: 4 groups (Port 1+2) , (Port 3+4), (Port 5+ 6), (Port 7+ 8), maximum per group: 120W, maximum per port: 90W.

Messages:

PoE Mode(Force60W) :The switch port will power up the linked PD without any detect/negotiate mechanism (PD limited to 60W). Do you want to Change this setting?

3.14-2 Lantronix POE++ Switch PoE Classification Settings

This section describes POE++ Configuration settings for different cameras or other higher powered PDs on the switch.

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.

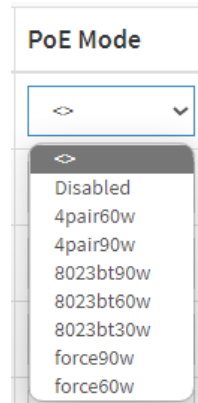
8023bt90w: Enables PoE IEEE 802.3bt (Class 8 PDs limited to 90W). Class negotiation up to 90W and supports 802.3 af/at/bt. Max power is 90W.

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). Class negotiation up to 30W and supports 802.3 af/at. 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).



3.14-3 Recommended Settings

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.

3-14.4 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. Click Configuration, PoE, Power Delay.
2. For each port set the Delay Mode and set the Delay Time.
3. Click Apply to save the changes.

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

Figure 3-14.2: PoE Power Delay

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.

Buttons:

Apply – Click to save changes.

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

3-14.5 Schedule 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. Click Configuration, PoE, and Schedule Profile.
2. Select a Profile and Profile Name.
3. Select time and day to supply power.
4. Click Apply to apply the changes.

The screenshot shows the Lantronix web UI for the SISPM1040-582-LRT device. The main content area is titled "PoE Schedule Profile". It features a "Profile" dropdown menu set to "1" and a "Name" text input field containing "Profile 1". Below this is a table for configuring the schedule by day and time.

Week Day	Start Time		End Time	
	HH	MM	HH	MM
*	<input type="text" value="0"/>	<input type="text" value="0"/>	<input type="text" value="0"/>	<input type="text" value="0"/>
Monday	<input type="text" value="0"/>	<input type="text" value="0"/>	<input type="text" value="0"/>	<input type="text" value="0"/>
Tuesday	<input type="text" value="0"/>	<input type="text" value="0"/>	<input type="text" value="0"/>	<input type="text" value="0"/>
Wednesday	<input type="text" value="0"/>	<input type="text" value="0"/>	<input type="text" value="0"/>	<input type="text" value="0"/>
Thursday	<input type="text" value="0"/>	<input type="text" value="0"/>	<input type="text" value="0"/>	<input type="text" value="0"/>
Friday	<input type="text" value="0"/>	<input type="text" value="0"/>	<input type="text" value="0"/>	<input type="text" value="0"/>
Saturday	<input type="text" value="0"/>	<input type="text" value="0"/>	<input type="text" value="0"/>	<input type="text" value="0"/>
Sunday	<input type="text" value="0"/>	<input type="text" value="0"/>	<input type="text" value="0"/>	<input type="text" value="0"/>

At the bottom of the table are "Apply" and "Reset" buttons.

Figure 3-13.3: PoE Schedule Profile

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

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

Buttons:

Apply : Click to save changes.

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

3-14.6 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 via the web UI:

1. Click Configuration, PoE, Auto Power Reset.
2. At the dropdown 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.

The screenshot shows the Lantronix web interface for configuring PoE Auto Power Reset. The page title is "PoE Auto Power Reset" and the breadcrumb trail is "Home > Configuration > PoE > Auto Power Reset". The "Ping Check" function is currently set to "Disabled". Below this is a table with 8 rows, one for each port (1-8). Each row contains fields for Port, Ping IP Address, Startup Time, Interval Time(sec), Retry Time, Failure Log, Failure Action, Reboot Time(sec), and Max. Reboot Times. The values for all ports are: Ping IP Address: 0.0.0.0, Startup Time: 60, Interval Time(sec): 30, Retry Time: 3, Failure Log: error=0, total=0, Failure Action: Nothing, Reboot Time(sec): 15, and Max. Reboot Times: 3. At the bottom of the table are "Apply" and "Reset" buttons.

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

Figure 3-14.4: PoE Auto Power Reset

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. (Feature added at FW v 7.10.2205.)



Buttons:

Apply – Click to save changes.

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

PoE Auto Checking “AutoFill” Feature

When you enable Auto Power Reset (PoE Auto Checking) in DMS, the IP addresses of the connected devices are automatically filled in the Auto Power Reset configuration page.

1. Configure the “PoE Auto Checking” parameter at Switch > PoE Management > PoE Auto Power Reset. The default value of the “Failure Action” parameter is “Nothing”.
2. Configure PoE parameters at DMS > Graphical Monitoring > Topology View. Left click on the switch icon  to display its device configuration popup. Click the PoE Config () icon to display the PoE Auto Checking pane.

3-14.7 Chip Reset Schedule

This page lets you schedule when to reset the PoE chip. To schedule PoE Chip Reset in the web UI:

1. Click Configuration, PoE, and Chip Reset Schedule.
2. At the Mode dropdown, select Enabled to display the configurable parameters.
3. Select the day(s) and time(s) for the PoE chip reset to occur.
4. Click Apply to apply the changes.

The screenshot shows the web interface for configuring the PoE Chip Reset Schedule. The mode is set to 'Enabled'. The configuration table is as follows:

Week Day	PoE Chip Reset Time	
	HH	MM
*	<input type="text" value="<"/>	<input type="text" value="<"/>
Monday	<input type="text" value="-"/>	<input type="text" value="-"/>
Tuesday	<input type="text" value="-"/>	<input type="text" value="-"/>
Wednesday	<input type="text" value="-"/>	<input type="text" value="-"/>
Thursday	<input type="text" value="-"/>	<input type="text" value="-"/>
Friday	<input type="text" value="-"/>	<input type="text" value="-"/>
Saturday	<input type="text" value="-"/>	<input type="text" value="-"/>
Sunday	<input type="text" value="-"/>	<input type="text" value="-"/>

Buttons: **Apply** (blue), **Reset** (orange)

Figure 3-14.5: PoE Chip Reset Schedule

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.

Buttons:

Apply : Click to save changes.

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

3-15 EPS

The Ethernet (Linear) Protection Switch instances are configured here. EPS (Ethernet Protection Switching) is defined in ITU/T G.8031.

To configure EPS parameters in the web UI:

1. Click Configuration and EPS.
2. Click the Add New EPS button to add a new EPS entry.
2. Specify the Ethernet Protection Switching parameters.
3. Click Apply to apply the change.

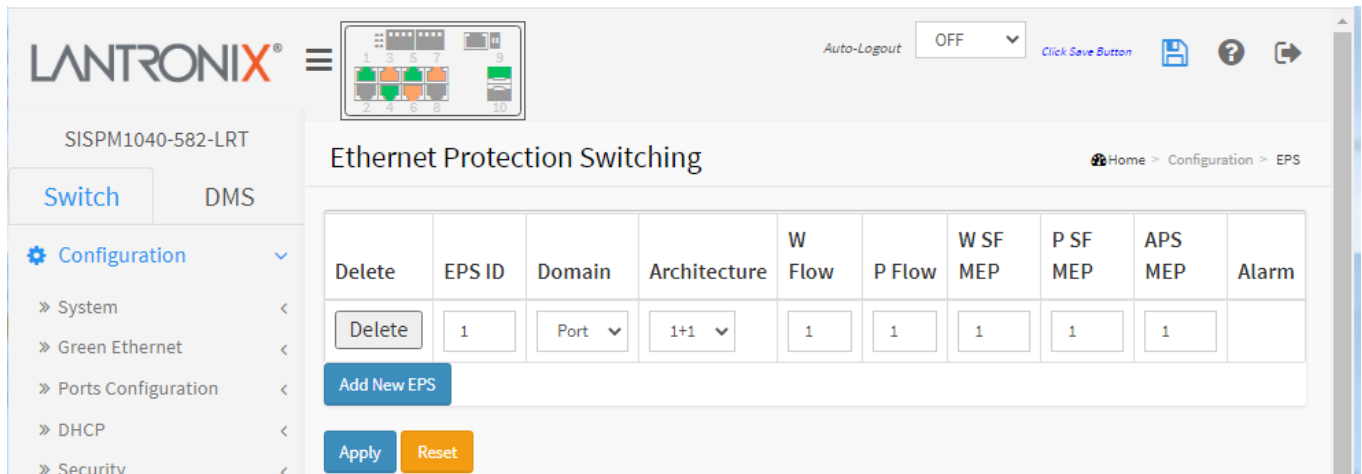


Figure 3-15: Ethernet Protection Switching

Parameter descriptions:

Delete : Check this box to mark an EPS for deletion in next save operation.

EPS ID : The ID of the EPS. Click on the ID of an EPS to enter the configuration page. The range is 1-100.

Domain : This will create an EPS in the Port Domain. 'W/P Flow' is a Port.

Architecture : At the dropdown select either:

1+1: This will create a 1+1 EPS.

1:1: This will create a 1:1 EPS.

W Flow : The working flow for the EPS - See 'Domain'. The working and protection flows cannot be equal.

P Flow : The protecting flow for the EPS - See 'Domain'.

W SF MEP : The working Signal Fail reporting MEP.

P SF MEP : The protecting Signal Fail reporting MEP.

APS MEP : The APS PDU handling MEP.

Alarm : There is an active alarm on the EPS.

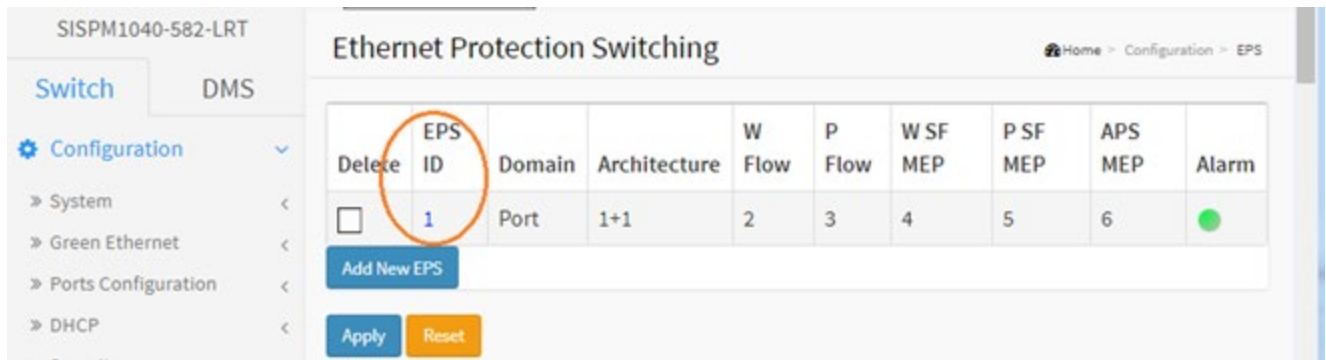
Buttons:

Add New EPS : Click to add a new EPS entry. Only one EPS can be added for each Apply operation.

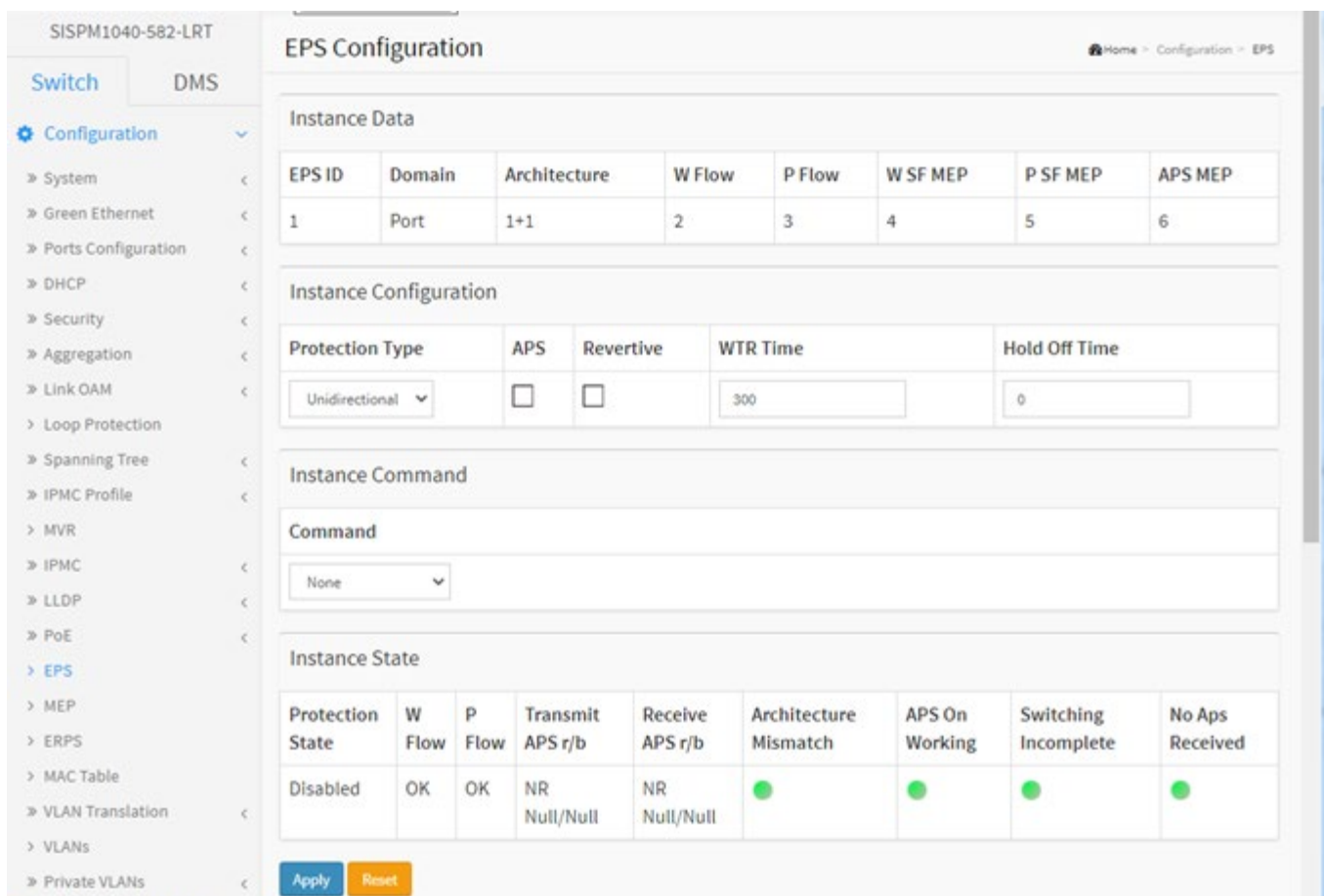
Apply : Click to save changes.

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

EPS Example:



Click the linked EPS ID to display its EPS Configuration page:



Instance Data

EPS ID : The ID of the EPS.

Domain : Port: This will create an EPS in the Port Domain. 'W/P Flow' is a Port.

Architecture :

Port: This will create a 1+1 EPS.

Port: This will create a 1:1 EPS.

W Flow : The working flow for the EPS - See 'Domain'. The working and protection flows cannot be equal.

P Flow : The protecting flow for the EPS - See 'Domain'.

W SF MEP : The working Signal Fail reporting MEP.

P SF MEP : The protecting Signal Fail reporting MEP.

APS MEP : The APS PDU handling MEP.

Instance Configuration

Configured :

Red: This EPS is only created and has not yet been configured - is not active.

Green: This EPS is configured - is active.

Protection Type :

Unidirectional: EPS in the two ends can select traffic from different working/protecting flow. This is only possible in case of 1+1 architecture.

Bidirectional: EPS in the two ends is selecting traffic from the same working/protecting flow. This requires APS enabled. This is mandatory for 1:1 architecture.

APS : The Automatic Protection Switching protocol can be enabled/disabled. This is mandatory for 1:1 architecture.

Revertive : The revertive switching to working flow can be enabled/disabled.

WTR Time : The Wait To Restore timing value to be used in revertive switching. Range is 1 to 720 seconds.

Hold Off Time : The timing value to be used to make persistent check on Signal Fail before switching. This is in 100 ms. and the max value is 100 (10 sec).

Instance Command

Command

None: There is no active local command on this instance.

Clear: The active local command will be cleared.

Lock Out: This EPS is locked to working (not active). In case of 1:N (more than one EPS with same protecting flow) - when one EPS switch to protecting flow, other EPS is enforced this command

Forced Switch: Force switch to protecting.

Manual Switch P: Manual switch to protecting.

Manual Switch W: Manual switch to working. This is only allowed in case of 'non-revertive' mode

Exercise: Exercise of the protocol - not traffic effecting. This is only allowed in case of 'Bidirectional' protection type

Freeze: This EPS is locally frozen - ignoring all input.

Lock Out Local: This EPS is locally "locked out" - ignoring local SF detected on working.

None
Clear
Lock Out
Forced Switch
Manual Switch P
Manual Switch W
Exercise
Freeze
Lock Out Local

Instance State

Protection State : EPS state according to State Transition Tables in G.8031.

W Flow : The working flow state:

OK: State of working flow is ok

SF: State of working flow is Signal Fail

SD: State of working flow is Signal Degrade (for future use)

P Flow : The protection flow state:

OK: State of protecting flow is ok

SF: State of protecting flow is Signal Fail

SD: State of protecting flow is Signal Degrade (for future use)

Transmit APS r/b : The transmitted APS according to State Transition Tables in G.8031.

Receive APS r/b : The received APS according to State Transition Tables in G.8031.

Architecture Mismatch : The architecture indicated in the received APS does not match the locally configured.

APS on working : APS is received on the working flow.

Switching Incomplete : Traffic is not selected from the same flow instance in the two ends.

No APS Received : APS PDU is not received from the other end.

Messages:

The working and protection flows are equal

Working MEP and protecting SF MEP is same instance

Invalid APS MEP instance

MEP instance must not be zero

3-16 MEP

Maintenance Entity Point (MEP) instances are configured here. A MEP is an endpoint in a Maintenance Entity Group per ITU-T Y.1731. To configure MEP parameters in the web UI:

1. Click Configuration and MEP.
2. Click the Add New MEP button.
3. Specify the Maintenance Entity Point parameters.
4. Click Apply to apply the change.

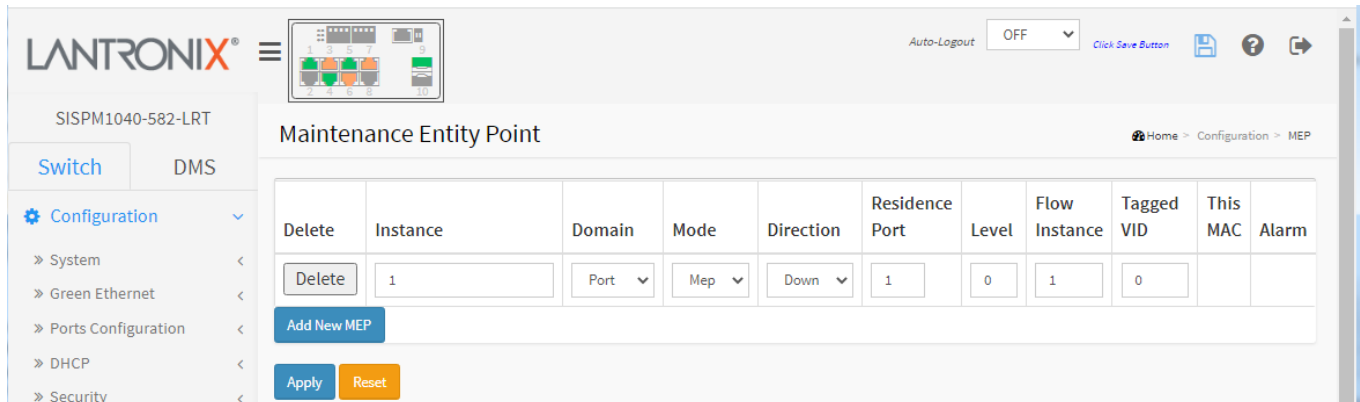


Figure 3-16: Maintenance Entity Point

Parameter descriptions:

Delete : This box is used to mark a MEP for deletion in next Save operation.

Instance : The ID of the MEP. Click on the linked ID of a MEP to enter its configuration page. The range is 1 - 100.

Domain : Select the MEP domain:

Port: This is a MEP in the Port Domain.

EVC: This is a MEP in the EVC Domain. 'Flow Instance' is an EVC. The EVC must be created

VLAN: This is a MEP in the VLAN Domain. 'Flow Instance' is a VLAN. In case of Up-MEP the VLAN must be created.

Mode : Select the mode:

MEP: This is a Maintenance Entity End Point.

MIP: This is a Maintenance Entity Intermediate Point.

Direction : Select the MEP direction:

Down: This is a Down MEP - monitoring ingress OAM and traffic on 'Residence Port'.

Up: This is a Up MEP - monitoring egress OAM and traffic on 'Residence Port'.

Residence Port : The port where MEP is monitoring - see 'Direction'. For a EVC MEP the port must be a port in the EVC. For a VLAN MEP the port must be a VLAN member.

Level : The MEG level of this MEP.

Flow Instance : The MEP is related to this flow - See 'Domain'. This is not relevant and not shown in case of Port MEP.

Tagged VID :

Port MEP: An outer C/S-tag (depending on VLAN Port Type) is added with this VID. Entering '0' means no TAG added.

EVC MEP: This is not used.

VLAN MEP: This is not used.

EVC MIP: The Subscriber VID that identifies the subscriber flow in this EVC where the MIP is active.

This MAC : The MAC of this MEP - can be used by other MEP when unicast is selected (Info only).

Alarm : There is an active alarm on the MEP.

Buttons:

Apply – Click to save changes.

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

Messages: Invalid configuration; click the OK button to clear the message and create a valid configuration.

Warning! The configuration is invalid. VLAN domain is not supported.

Warning! The configuration is invalid. EVC flow was found invalid

Warning! The configuration is invalid. VLAN was not created for this VID

Warning! The configuration is invalid. This MIP is not supported.

Only one MEP can be added for each Apply operation.

Only one peer MEP can be added for each Apply operation.

Warning! The configuration is invalid. Invalid parameter error returned from MEP

Example: A sample MEP table is shown below.

Delete	Instance	Domain	Mode	Direction	Residence Port	Level	Flow Instance	Tagged VID	This MAC	Alarm
<input type="checkbox"/>	1	Port	Mep	Down	1	0		0	00-C0-F2-4F-73-D1	●
<input type="checkbox"/>	2	Port	Mep	Down	1	0		0	00-C0-F2-4F-73-D1	●
<input type="checkbox"/>	3	Port	Mep	Down	1	0		0	00-C0-F2-4F-73-D1	●
<input type="checkbox"/>	4	Port	Mep	Down	1	0		0	00-C0-F2-4F-73-D1	●
<input type="checkbox"/>	5	Port	Mep	Down	1	0		2	00-C0-F2-4F-73-D1	●

Click a linked Instance number to display its EPS Configuration page.

Instance Data

MEP Instance : The ID of the MEP.

Domain : Select Port, EVC, or VLAN:

Port: This is a MEP in the Port Domain.

EVC: This is a MEP in the EVC Domain. 'Flow Instance' is an EVC. The EVC must be created

VLAN: This is a MEP in the VLAN Domain. 'Flow Instance' is a VLAN. In case of Up-MEP the VLAN must be created.

Mode : Select MEP or MIP:

MEP: This is a Maintenance Entity End Point.

MIP: This is a Maintenance Entity Intermediate Point.

Direction : Select UP or Down:

Down: This is a Down MEP - monitoring ingress OAM and traffic on 'Residence Port'.

Up: This is a Up MEP - monitoring egress OAM and traffic on 'Residence Port'.

Residence Port : The port where MEP is monitoring - see 'Direction'. For a EVC MEP the port must be a port in the EVC. For a VLAN MEP the port must be a VLAN member.

Level : The MEG level of this MEP.

Flow Instance : The MEP is related to this flow - See 'Domain'. This is not relevant and not shown in case of Port MEP.

Tagged VID : Port MEP: An outer C/S-tag (depending on VLAN Port Type) is added with this VID. Entering '0' means no TAG added.

EVC MEP: This is not used.

VLAN MEP: This is not used.

EVC MIP: The Subscriber VID that identifies the subscriber flow in this EVC where the MIP is active.

This MAC : The MAC of this MEP - can be used by other MEP when unicast is selected (Info only).

Instance Configuration

EVC QoS : This is only relevant for a EVC MEP. This is the QoS of the EVC and used for getting QoS counters for Loss Measurement.

Level : See help on MEP create WEB.

Format : This is the configuration of the two possible Maintenance Association Identifier formats.

ITU ICC: This is defined by ITU (Y1731 Fig. A3). 'Domain Name' is not used. 'MEG id' must be max. 13 char.

IEEE String: This is defined by IEEE (802.1ag Section 21.6.5). 'Domain Name' can be max. 16 char. 'MEG id' (Short MA Name) can be a maximum 16 char.

ITU CC ICC: This is defined by ITU (Y1731 Fig. A5). 'Domain Name' is not used. 'MEG id' must be max. 15 char.

Domain Name : This is the IEEE Maintenance Domain Name and is only used in case of 'IEEE String' format. This string can be empty giving Maintenance Domain Name Format 1 - Not present. This can be max 16 char.

MEG Id : This is either ITU MEG ID or IEEE Short MA Name - depending on 'Format'. See 'Format'. In case of ITU ICC format this must be 13 char. In case of ITU CC ICC format this must be 15 characters In case of IEEE String format this can be maximum 16 characters.

MEP Id : This value will become the transmitted two byte CCM MEP ID.

Tagged VID : This value will be the VID of a TAG added to the OAM PDU.

VOE : This will attempt to utilize VOE HW for MEP implementation. Not all platforms support VOE.

cLevel : Fault Cause indicating that a CCM is received with a lower level than the configured for this MEP.

cMEG : Fault Cause indicating that a CCM is received with a MEG ID different from configured for this MEP.

cMEP : Fault Cause indicating that a CCM is received with a MEP ID different from all 'Peer MEP ID' configured for this MEP.

cAIS : Fault Cause indicating that AIS PDU is received.

cLCK : Fault Cause indicating that LCK PDU is received.

cDEG : Fault Cause indicating that server layer is indicating Signal Degraded.

cSSF : Fault Cause indicating that server layer is indicating Signal Fail.

aBLK : The consequent action of blocking service frames in this flow is active.

aTSD : The consequent action of indicating Trail Signal Degrade is calculated.

aTSF : The consequent action of indicating Trail Signal Fail to-wards protection is active.

Delete : This box is used to mark a Peer MEP for deletion in next Save operation.

Peer MEP ID : This value will become an expected MEP ID in a received CCM - see 'cMEP'.

Unicast Peer MAC : This MAC will be used when unicast is selected with this peer MEP. Also, this MAC is used to create HW checking of receiving CCM PDU (LOC detection) from this MEP.

cLOC : Fault Cause indicating that no CCM has been received (in 3,5 periods) - from this peer MEP.

cRDI : Fault Cause indicating that a CCM is received with Remote Defect Indication - from this peer MEP.

cPeriod : Fault Cause indicating that a CCM is received with a period different what is configured for this MEP - from this peer MEP.

cPriority : Fault Cause indicating that a CCM is received with a priority different what is configured for this MEP - from this peer MEP.

Buttons

Add New Peer MEP: Click to add a new peer MEP.

Functional Configuration

Continuity Check

Enable : Continuity Check based on transmitting/receiving CCM PDU can be enabled/disabled. The CCM PDU is always transmitted as Multi-cast Class 1.

Priority : The priority to be inserted as PCP bits in TAG (if any). In case of enable of Continuity Check and Loss Measurement both implemented on SW based CCM, 'Priority' has to be the same.

Frame rate : Selecting the frame rate of CCM PDU. This is the inverse of transmission period as described in Y.1731. This value has the following uses:

- * The transmission rate of the CCM PDU.
- * Fault Cause cLOC is declared if no CCM PDU has been received within 3.5 periods - see 'cLOC'.
- * Fault Cause cPeriod is declared if a CCM PDU has been received with different period - see 'cPeriod'.

Selecting 300f/sec or 100f/sec will configure HW based CCM (if possible). Selecting other frame rates will configure SW based CCM. In case of enable of Continuity Check and Loss Measurement both implemented on SW based CCM, 'Frame Rate' has to be the same.

TLV : Enable/disable of TLV insertion in the CCM PDU.

APS Protocol

Enable : Automatic Protection Switching protocol information transportation based on transmitting/receiving R-APS/L-APS PDU can be enabled/disabled. Must be enabled to support ERPS/ELPS implementing APS. This is only valid with one Peer MEP configured.

Priority : The priority to be inserted as PCP bits in TAG (if any).

Cast : Selection of APS PDU transmitted unicast or multi-cast. The unicast MAC will be taken from the 'Unicast Peer MAC' configuration. Unicast is only valid for L-APS - see 'Type'. The R-APS PDU is always transmitted with multi-cast MAC described in G.8032.

Type : The APS PDU type:

R-APS: APS PDU is transmitted as R-APS - this is for ERPS.

L-APS: APS PDU is transmitted as L-APS - this is for ELPS.

Last Octet : This is the last octet of the transmitted and expected RAPS multi-cast MAC. In G.8031 (03/2010) a RAPS multi-cast MAC is defined as 01-19-A7-00-00-XX. In current standard the value for this last octet is '01' and the usage of other values is for further study.

TLV Configuration : Configuration of the OAM PDU TLV. Currently only TLV in the CCM is supported.

Organization Specific - OUI First : The transmitted first value in the OS TLV OUI field.

Organization Specific - OUI Second : The transmitted second value in the OS TLV OUI field.

Organization Specific - OUI Third : The transmitted third value in the OS TLV OUI field.

Organization Specific - Sub-Type : The transmitted value in the OS TLV Sub-Type field.

Organization Specific - Value : The transmitted value in the OS TLV Value field.

TLV Status : Display of the last received TLV. Currently only TLV in the CCM is supported.

CC Organization Specific - OUI First : The last received first value in the OUI field.

CC Organization Specific - OUI Second : The last received second value in the OS TLV OUI field.

CC Organization Specific - OUI Third : The last received third value in the OS TLV OUI field.

CC Organization Specific - Sub-Type : The last received value in the OS TLV Sub-Type field.

CC Organization Specific - Value : The last received value in the OS TLV Value field.

CC Organization Specific - Last RX : OS TLV was received in the last received CCM PDU.

CC Port Status – Value : The last received value in the PS TLV Value field.

CC Port Status - Last RX : PS TLV was received in the last received CCM PDU.

CC Interface Status – Value : The last received value in the IS TLV Value field.

CC Interface Status - Last RX : IS TLV was received in the last received CCM PDU.

Link State Tracking

Enable : When LST is enabled in an instance, Local SF or received 'isDown' in CCM Interface Status TLV, will bring down the residence port. Only valid in Up-MEP. The CCM rate must be 1 f/s or faster.

Buttons

Fault Management : Click to go to Fault Management page.

Performance Monitor : Click to go to Performance Monitoring page.

Fault Management page:

Parameter Descriptions:

Loop Back

Enable : Loop Back based on transmitting/receiving LBM/LBR PDU can be enabled/disabled. Loop Back is automatically disabled when all 'To Send' LBM PDU has been transmitted - waiting 5 sec. for all LBR from the end.

DEI : The Drop Eligible Indicator to be inserted as PCP bits in TAG (if any).

Priority : The priority to be inserted as PCP bits in TAG (if any).

Cast : Selection of LBM PDU transmitted unicast or multi-cast. The unicast MAC will be configured through 'Peer MEP' or 'Unicast Peer MAC'. To-towards MIP only unicast Loop Back is possible.

Peer MEP : This is only used if the 'Unicast MAC' is configured to all zero. The LBM unicast MAC will be taken from the 'Unicast Peer MAC' configuration of this peer.

Unicast MAC : This is only used if NOT configured to all zero. This will be used as the LBM PDU unicast MAC. This is the only way to configure Loop Back to-towards a MIP.

To Send : The number of LBM PDU to send in one loop test. The value 0 indicate infinite transmission (test behavior). This is HW based LBM/LBR and Requires VOE.

Size : The LBM frame size. This is entered as the wanted size (in bytes) of a un-tagged frame containing LBM OAM PDU - including CRC (four bytes).

Example when 'Size' = 64 => Un-tagged frame size = DMAC(6) + SMAC(6) + TYPE(2) + LBM PDU LENGTH(46) + CRC(4) = 64 bytes

The transmitted frame will be four bytes longer for each tag added - 8 bytes in case of a tunnel EVC.
There are two frame MAX sizes to consider.

Switch RX frame MAX size: The MAX frame size (all inclusive) accepted on the switch port of 9600 Bytes

CPU RX frame MAX size: The MAX frame size (all inclusive) possible to copy to CPU of 1526 Bytes

Consider that the Peer MEP must be able to handle the selected frame size. Consider that In case of SW based MEP, the received LBR PDU must be copied to CPU

Warning will be given if selected frame size exceeds the CPU RX frame MAX size

Frame MIN Size is 64 Bytes.

Interval : The interval between transmitting LBM PDU. In 10ms. in case 'To Send' != 0 (max 100 - '0' is as fast as possible) In 1us. in case 'To Send' == 0 (max 10.000)",

Loop Back State

Transaction ID : The transaction id of the first LBM transmitted. For each LBM transmitted the transaction id in the PDU is incremented.

Transmitted : The total number of LBM PDU transmitted.

Reply MAC : The MAC of the replying MEP/MIP. In case of multi-cast LBM, replies can be received from all peer MEP in the group. This MAC is not shown in case of 'To Send' == 0.

Received : The total number of LBR PDU received from this 'Reply MAC'.

Out Of Order : The number of LBR PDU received from this 'Reply MAC' with incorrect 'Transaction ID'.

Link Trace

Enable : Link Trace based on transmitting/receiving LTM/LTR PDU can be enabled/disabled. Link Trace is automatically disabled when all 5 transactions are done with 5 sec. interval - waiting 5 sec. for all LTR in the end. The LTM PDU is always transmitted as Multi-cast Class 2.

Priority : The priority to be inserted as PCP bits in TAG (if any).

Peer MEP : This is only used if the 'Unicast MAC' is configured to all zero. The Link Trace Target MAC will be taken from the 'Unicast Peer MAC' configuration of this peer.

Unicast MAC : This is only used if NOT configured to all zero. This will be used as the Link Trace Target MAC. This is the only way to configure a MIP as Target MAC.

Time To Live : This is the LTM PDU TTL value as described in Y.1731. This value is decremented each time forwarded by a MIP. Will not be forwarded reaching zero.

Link Trace State

Transaction ID : The transaction id is incremented for each LTM send. This value is inserted the transmitted LTM PDU and is expected to be received in the LTR PDU. Received LTR with wrong transaction id is ignored. There are five transactions in one Link Trace activated.

Time To Live : This is the TTL value taken from the LTM received by the MIP/MEP sending this LTR - decremented as if forwarded.

Mode : Indicating if it was a MEP/MIP sending this LTR.

Direction : Indicating if MEP/MIP sending this LTR is ingress/egress.

Forwarded : Indicating if MEP/MIP sending this LTR has forwarded the LTM.

Relay : The Relay action can be one of the following

MAC: The was a hit on the LT Target MAC

FDB: LTM is forwarded based on hit in the Filtering DB

MFDB: LTM is forwarded based on hit in the MIP CCM DB

Last MAC : The MAC identifying the last sender of the LBM causing this LTR - initiating MEP or previous MIP forwarding.

Next MAC : The MAC identifying the next sender of the LBM causing this LTR - MIP forwarding or terminating MEP.

Test Signal

Enable : Test Signal based on transmitting TST PDU can be enabled/disabled.

DEI : The Drop Eligible Indicator to be inserted as PCP bits in TAG (if any).

Priority : The priority to be inserted as PCP bits in TAG (if any).

Peer MEP : The TST frame destination MAC will be taken from the 'Unicast Peer MAC' configuration of this peer.

Rate : The TST frame transmission bit rate - in Megabits pr. second. Limit is 400 Mbps. This is the bit rate of a standard frame without any encapsulation. If 1 Mbps rate is selected in a EVC MEP, the added tag will give a higher bitrate on the wire.

Size : The TST frame size. This is entered as the wanted size (in bytes) of a un-tagged frame containing TST OAM PDU - including CRC (four bytes).

Example when 'Size' = 64 => Un-tagged frame size = DMAC(6) + SMAC(6) + TYPE(2) + TST PDU LENGTH(46) + CRC(4) = 64 bytes

The transmitted frame will be four bytes longer for each tag added - 8 bytes in case of a tunnel EVC.

There are two frame MAX sizes to consider.

Switch RX frame MAX size: The MAX frame size (all inclusive) accepted on the switch port of 9600 Bytes

CPU RX frame MAX size: The MAX frame size (all inclusive) possible to copy to CPU of 1526 Bytes

Consider that the Peer MEP must be able to handle the selected frame size. Consider that in order to calculate the 'RX rate' a received TST PDU must be copied to CPU

Warning will be given if selected frame size exceeds the CPU RX frame MAX size

Frame MIN Size is 64 Bytes.

Pattern : The 'empty' TST PDU has the size of 12 bytes. In order to achieve the configured frame size a data TLV will be added with a pattern.

Example when 'Size' = 64 => Un-tagged frame size = DMAC(6) + SMAC(6) + TYPE(2) + TST PDU LENGTH(46) + CRC(4) = 64 bytes

The TST PDU needs to be 46 bytes so a pattern of 46-12=34 bytes will be added.

All Zero: Pattern will be '00000000'

All One: Pattern will be '11111111'

10101010: Pattern will be '10101010'

Test Signal State

TX frame count : The number of transmitted TST frames since last 'Clear'.

RX frame count : The number of received TST frames since last 'Clear'.

RX rate : The current received TST frame bit rate in Kbps. This is calculated on a 1 s. basis, starting when first TST frame is received after 'Clear'. The frame size used for this calculation is the first received after 'Clear'

Test time : The number of seconds passed since first TST frame received after last 'Clear'.

Clear : This will clear all Test Signal State. Transmission of TST frame will be restarted. Calculation of 'Rx frame count', 'RX rate' and 'Test time' will be started when receiving first TST frame.

Client Configuration : Only a Port MEP is able to be a server MEP with flow configuration. The Priority in the client flow is always the highest priority configured in the EVC.

Domain : The domain of the client layer flow.

Instance : Client layer flow instance numbers.

Level : Client layer level - AIS and LCK PDU transmitted in this client layer flow will be on this level.

AIS Prio : The priority to be used when transmitting AIS in each client flow. Priority resulting in highest possible PCP can be selected.

LCK Prio : The priority to be used when transmitting LCK in each client flow. Priority resulting in highest possible PCP can be selected.

AIS

Enable : Insertion of AIS signal (AIS PDU transmission) in client layer flows, can be enable/disabled.

Frame Rate : Selecting the frame rate of AIS PDU. This is the inverse of transmission period as described in Y.1731.

Protection : Selecting this means that the first 3 AIS PDU is transmitted as fast as possible - in case of using this for protection in the end point.

LOCK

Enable : Insertion of LOCK signal (LCK PDU transmission) in client layer flows, can be enable/disabled.

Frame Rate : Selecting the frame rate of LCK PDU. This is the inverse of transmission period as described in Y.1731.:

Buttons

Back : Click to go back to this MEP instance main page.

Apply : Click to save changes.

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

Performance Monitoring page:

The screenshot shows the configuration interface for a Performance Monitor instance. The left sidebar contains navigation options like Configuration, System, and Diagnostics. The main content area is titled 'Performance Monitor - Instance 1 - MEP id 1' and includes the following sections:

- Performance Monitoring Data Set:** Includes an 'Enable' checkbox.
- Loss Measurement:** Contains fields for 'Enable', 'Priority', 'Frame rate', 'Count', 'Ended', 'FLR Interval', and 'Loss Threshold'.
- Loss Measurement State:** A table with columns: Tx, Rx, Near End Loss Count, Far End Loss Count, Near End Loss Ratio, Far End Loss Ratio, and Clear.
- Loss Measurement Availability:** Includes 'Enable', 'Interval', 'FLR Threshold', and 'Maintenance' checkboxes.
- Loss Measurement Availability State:** A table with columns: Near Availability Count, Far Availability Count, Near Unavailability Count, Far Unavailability Count, Near State, and Far State.
- Loss Measurement High Loss Interval:** Includes 'Enable', 'FLR Threshold', and 'Consecutive Interval' fields.
- Loss Measurement High Loss Interval State:** A table with columns: Near Count, Far Count, Near Consecutive Count, and Far Consecutive Count.
- Loss Measurement Signal Degrade:** Includes 'Enable', 'TS Minimum', 'FLR Threshold', 'Bad Threshold', and 'Good Threshold' fields.
- Delay Measurement:** Includes 'Enable', 'Priority', 'Count', 'Peer MEP', 'Ended', 'Tx Mode', 'Calc', 'Gap', 'Count', 'Unit', 'SDUs/SE', and 'Counter Overflow Action'.
- Delay Measurement State:** A table with columns: Tx, Rx, Rx Timeout, Rx Error, Av Delay Tot, Av Delay last N, Delay Min, Delay Max, Av Delay-Var Tot, Av Delay-Var last N, Delay-Var Min, Delay-Var Max, Overflow, and Clear.
- Delay Measurement Bins:** Includes 'Measurement Bins for FD', 'Measurement Bins for IFDV', and 'Measurement Threshold'.
- Delay Measurement Bins for FD:** A table with columns: bin0, bin1, bin2 and rows: One-way, F-to-N, N-to-F, Two-way.
- Delay Measurement Bins for IFDV:** A table with columns: bin0, bin1, bin2 and rows: One-way, F-to-N, N-to-F, Two-way.

Parameter Descriptions:

Performance Monitoring Data Set

Enable : When enabled this MEP instance will contribute to the 'PM Data Set' gathered by the PM Session.

Loss Measurement

Enable : Loss Measurement based on transmitting/receiving CCM or LMM/LMR PDU can be enabled/disabled - see 'Ended'. This is only valid with one Peer MEP configured.

Priority : The priority to be inserted as PCP bits in TAG (if any). In case of enable of Continuity Check and Loss Measurement both implemented on SW based CCM, 'Priority' has to be the same.

Frame rate : Selecting the frame rate of CCM/LMM PDU. This is the inverse of transmission period as described in Y.1731. Selecting 300f/sec or 100f/sec is not valid. In case of enable of Continuity Check and Loss Measurement both implemented on SW based CCM, 'Frame Rate' has to be the same.

Cast : Selection of CCM or LMM PDU transmitted unicast or multicast. The unicast MAC will be taken from the 'Unicast Peer MAC' configuration. In case of enable of Continuity Check and dual ended Loss Measurement both implemented on SW based CCM, 'Cast' has to be the same.

Ended: Select either:

Single: Single ended Loss Measurement implemented on LMM/LMR.

Dual: Dual ended Loss Measurement implemented on SW based CCM.

FLR Interval : This is the interval in seconds where the Frame Loss Ratio is calculated.

Loss Threshold : Far end loss threshold count is incremented if a loss measurement is above this threshold.

Loss Measurement State

Near End Loss Count : The accumulated near end frame loss count - since last 'clear'.

Far End Loss Count : The accumulated far end frame loss count - since last 'clear'.

Near End Loss Ratio : The near end frame loss ratio calculated based on the near end frame loss count and far end frame transmitted - in the latest 'FLR Interval'. The result is given in percent.

Far End Loss Ratio : The far end frame loss ratio calculated based on the far end frame loss count and near end frame transmitted - in the latest 'FLR Interval'. The result is given in percent.

Clear : Set of this check and save will clear the accumulated counters and restart ratio calculation.

Loss Measurement Availability

Enable : Enable/disable of loss measurement availability.

Interval : Availability interval - number of measurements with same availability in order to change availability state.

FLR Threshold : Availability frame loss ratio threshold in per mille.

Maintenance : Enable/disable of loss measurement availability maintenance.

Loss Measurement Availability Status

Near Avail Count : Near end availability count.

Far Avail Count : Far end availability count.

Near Unavail Count : Near end unavailability count.

Far Unavail Count : Far end unavailability count.

Near State : Near end availability state.

Far State : Far end availability state.

Loss Measurement High Loss Interval

Enable : Enable/disable of loss measurement high loss interval.

FLR Threshold : High Loss Interval frame loss ratio threshold in per mille.

Consecutive Interval : High Loss Interval consecutive interval (number of measurements).

Loss Measurement High Loss Interval Status

Near Count : Near end high loss interval count (number of measurements where availability state is available and FLR is above high loss interval FLR threshold).

Far Count : Far end high loss interval count (number of measurements where availability state is available and FLR is above high loss interval FLR threshold).

Near Consecutive Count : Near end high loss interval consecutive count.

Far Consecutive Count : Far end high loss interval consecutive count.

Loss Measurement Signal Degrade

Enable : Enable/disable of loss measurement signal degrade.

TX Minimum : Minimum number of frames that must be transmitted in a measurement before frame loss ratio is tested against loss ratio threshold.

FLR Threshold : Signal Degraded frame loss ratio threshold in per mille.

Bad Threshold : Number of consecutive bad interval measurements required to set degrade state.

Good Threshold : Number of consecutive good interval measurements required to clear degrade state.

Delay Measurement

Enable : Delay Measurement based on transmitting 1DM/DMM PDU can be enabled/disabled. Delay Measurement based on receiving and handling 1DM/DMR PDU is always enabled.

Priority : The priority to be inserted as PCP bits in TAG (if any).

Cast : Selection of 1DM/DMM PDU transmitted unicast or multicast. The unicast MAC will be configured through 'Peer MEP'.

Peer MEP : This is only used if the 'Cast' is configured to Uni. The 1DM/DMR unicast MAC will be taken from the 'Unicast Peer MAC' configuration of this peer.

Way : Select either:

One-Way: One-Way Delay Measurement implemented on 1DM.

Two-Way: Two-Way Delay Measurement implemented on DMM/DMR.

Tx Mode : Select either:

Standardize: Y.1731 standardize way to transmit 1DM/DMR.

Proprietary: Vitesse proprietary way with follow-up packets to transmit 1DM/DMR.

Calc : This is only used if the 'Way' is configured to Two-way.

Round trip: The frame delay calculated by the transmitting and receiving timestamps of initiators. Frame Delay = RxTimeb-TxTimeStampf

Flow: The frame delay calculated by the transmitting and receiving timestamps of initiators and remotes. Frame Delay = (RxTimeb-TxTimeStampf)-(TxTimeStampb-RxTimeStampf)

Gap : The gap between transmitting 1DM/DMM PDU in 10ms. The range is 10 to 65535.

Count : The number of last records to calculate. The range is 10 to 2000.

Unit : The time resolution.

D2forD1 : Enable to use DMM/DMR packet to calculate one-way DM. If the option is enabled, the following action will be taken. When DMR is received, two-way delay (roundtrip or flow) and both near-end-to-far-end and far-end-to-near-end one-way delay are calculated. When DMM or 1DM is received, only far-end-to-near-end one-way delay is calculated.

Counter Overflow Action : The action to counter when overflow happens.

Delay Measurement State (One-way, F-to-N, N-to-F, Two-way):

Tx : The accumulated transmit count - since last 'clear'.

Rx : The accumulated receive count - since last 'clear'.

Rx Timeout : The accumulated receive timeout count for two-way only - since last 'clear'.

Rx Error : The accumulated receive error count - since last 'clear'. This is counting if the frame delay is larger than 1 second or if far end residence time is larger than the round trip time.

Av Delay Tot : The average total delay - since last 'clear'.

Av Delay last N : The average delay of the last n packets - since last 'clear'.

Delay Min. : The minimum delay - since last 'clear'.

Delay Max. : The maximum delay - since last 'clear'.

Av Delay-Var Tot : The average total delay variation - since last 'clear'.

Av Delay-Var last N : The average delay variation of the last n packets - since last 'clear'.

Delay-Var Min. : The minimum delay variation - since last 'clear'.

Delay-Var Max. : The maximum delay variation - since last 'clear'.

Overflow : The number of counter overflow - since last 'clear'.

Clear : Set of this check and save will clear the accumulated counters.

Far-end-to-near-end one-way delay : The one-way delay is from remote devices to the local devices. Here are the conditions to calculate this delay. 1. 1DM received. 2. DMM received with D2forD1 enabled. 3. DMR received with D2forD1 enabled.

Near-end-to-far-end one-way delay : The one-way delay is from the local devices to remote devices. The only case to calculate this delay is below. DMR received with D2forD1 enabled.

Delay Measurement Bins : A Measurement Bin is a counter that stores the number of delay measurements falling within a specified range, during a Measurement Interval.

Measurement Bins for FD : Configurable number of Frame Delay Measurement Bins per Measurement Interval.

The minimum number of FD Measurement Bins per Measurement Interval supported is 2.

The maximum number of FD Measurement Bins per Measurement Interval supported is 10.

The default number of FD Measurement Bins per Measurement Interval supported is 3.

Measurement Bins for IFDV : Configurable number of Inter-Frame Delay Variation Measurement Bins per Measurement Interval. The minimum number of FD Measurement Bins per Measurement Interval supported is 2.

The maximum number of FD Measurement Bins per Measurement Interval supported is 10. The default number of FD Measurement Bins per Measurement Interval supported is 2.

Measurement Threshold : Configurable the Measurement Threshold for each Measurement Bin. The unit for a measurement threshold is in microseconds (us). The default configured measurement threshold for a Measurement Bin is an increment of 5000 us.

Delay Measurement Bins for FD : A Measurement Bin is a counter that stores the number of delay measurements falling within a specified range, during a Measurement Interval. If the measurement threshold is 5000 us and the total number of Measurement Bins is four, for example:

Bin	Threshold	Range
bin0	0 us	0 us <= measurement < 5,000 us
bin1	5,000 us	5,000 us <= measurement < 10,000 us
bin2	10,000 us	10,000 us <= measurement < 15,000 us
bin3	15,000 us	15,000 us <= measurement < infinite us

Delay Measurement Bins for IFDV : A Measurement Bin is a counter that stores the number of delay measurements falling within a specified range, during a Measurement Interval.

If the measurement threshold is 5000 us and the total number of Measurement Bins is four, we can give an example as follows.

Bin	Threshold	Range
bin0	0 us	0 us <= measurement < 5,000 us
bin1	5,000 us	5,000 us <= measurement < 10,000 us
bin2	10,000 us	10,000 us <= measurement < 15,000 us
bin3	15,000 us	15,000 us <= measurement < infinite us

Buttons

Back : Click to go back to this MEP instance main page.

Apply : Click to save changes.

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

3-17 ERPS

ERPS instances are configured here. ERPS (Ethernet Ring Protection Switching) is defined in ITU-T G.8032. ERPS provides fast protection and recovery switching for Ethernet traffic in a ring topology while also ensuring that the Ethernet layer remains loop-free. See “[Appendix C – G.8032 Major and Sub Rings Configuration](#)” on page 491 for a guide to ERPS configuration.

Web Interface

To configure ERPS parameters in the web UI:

1. Click Configuration and ERPS.
2. Click the Add New Protection Group button.
3. Specify the Ethernet Ring Protection Switching parameters.
4. Click Apply to apply the changes.

Delete	ERPS ID	Port 0	Port 1	Port 0 APS MEP	Port 1 APS MEP	Port 0 SF MEP	Port 1 SF MEP	Ring Type	Interconnected Node	Virtual Channel	Major Ring ID	Alarm
<input type="checkbox"/>	1	1	2	3	4	5	6	Major	Yes	No	1	●
<input type="checkbox"/>	2	1	1	1	1	1	1	Sub	<input type="checkbox"/>	<input type="checkbox"/>	0	●

Figure 3-17: Ethernet Ring Protection Switching

Parameter descriptions:

Delete : This box is used to mark an EPS for deletion in next save operation.

ERPS ID: The ID of the created Protection group. It must be a number from 1 - 64. The maximum number of ERPS Protection Groups that can be created is 64. Click on a linked ERPS ID number to enter its configuration page (see below).

Port 0: This will create a Port 0 of the switch in the ring.

Port 1: This will create "Port 1" of the switch in the Ring. As inter-connected sub-ring will have only one ring port, "Port 1" is configured as "0" for inter-connected sub-ring. "0" in this field indicates that no "Port 1" is associated with this instance

Port 0 SF MEP: The Port 0 Signal Fail reporting MEP.

Port 1 SF MEP: The Port 1 Signal Fail reporting MEP. As only one SF MEP is associated with inter-connected sub-ring without virtual channel, it is configured as "0" for such ring instances. "0" in this field indicates that no Port 1 SF MEP is associated with this instance.

Port 0 APS MEP: The Port 0 APS PDU handling MEP.

Port 1 APS MEP: The Port 1 APS PDU handling MEP. As only one APS MEP is associated with inter-connected sub-ring without virtual channel, it is configured as "0" for such ring instances. "0" in this field indicates that no Port 1 APS MEP is associated with this instance.

Ring Type: Type of Protecting ring. It can be either Major ring or Sub-ring.

Interconnected Node: Interconnected Node indicates that the ring instance is interconnected. Click on the checkbox to configure this. "Yes" indicates it is an interconnected node for this instance. "No" indicates that the configured instance is not interconnected.

Virtual Channel: Sub-rings can either have virtual channel or not on the interconnected node. This is configured using "Virtual Channel" checkbox. "Yes" indicates it is a sub-ring with virtual channel. "No" indicates, sub-ring doesn't have virtual channel.

Major Ring ID: Major ring group ID for the interconnected sub-ring. It is used to send topology change updates on major ring. If ring is major, this value is same as the protection group ID of this ring.

Alarm: There is an active alarm on the ring.

Buttons:

Add New Protection Group: Click to add a new Protection group entry.

Apply : Click to save changes.

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

Click a linked ERPS ID number to display its ERPS Configuration page.

The screenshot displays the 'ERPS Configuration 1' page in a web browser. The left sidebar shows a navigation menu with 'ERPS' selected. The main content area is divided into several sections:

- Instance Data:** A table with 8 columns: ERPS ID, Port 0, Port 1, Port 0 SF MEP, Port 1 SF MEP, Port 0 APS MEP, Port 1 APS MEP, and Ring Type. The values are: 1, 1, 2, 5, 6, 3, 4, Major Ring.
- Instance Configuration:** A table with 7 columns: Configured (green dot), Guard Time (500), WTR Time (1min), Hold Off Time (0), Version (v2), Revertive (checked), and VLAN config (VLAN Config).
- RPL Configuration:** Fields for RPL Role (None), RPL Port (None), and a Clear checkbox.
- Instance Command:** Fields for Command (None) and Port (None).
- Instance State:** A table with 12 columns: Protection State, Port 0, Port 1, Transmit APS, Port 0 Receive APS, Port 1 Receive APS, WTR Remaining, RPL Unblocked, No APS Received, Port 0 Block Status, Port 1 Block Status, and FOP Alarm. The values are: Pending, OK, OK, NR BPRO, , , 0, , , Blocked, Unblocked, .

At the bottom of the configuration area, there are 'Apply' and 'Reset' buttons.

Parameter Descriptions:**Instance Data**

Port 0 : This will create a Port 0 of the switch in the ring.

Port 1 : This will create "Port 1" of the switch in the Ring. As interconnected sub-ring will have only one ring port, "Port 1" is configured as "0" for interconnected sub-ring. "0" in this field indicates that no "Port 1" is associated with this instance

Port 0 SF MEP : The Port 0 Signal Fail reporting MEP.

Port 1 SF MEP : The Port 1 Signal Fail reporting MEP. As only one SF MEP is associated with interconnected sub-ring without virtual channel, it is configured as "0" for such ring instances. "0" in this field indicates that no Port 1 SF MEP is associated with this instance.

Port 0 APS MEP : The Port 0 APS PDU handling MEP.

Port 1 APS MEP : The Port 1 APS PDU handling MEP. As only one APS MEP is associated with interconnected sub-ring without virtual channel, it is configured as "0" for such ring instances. "0" in this field indicates that no Port 1 APS MEP is associated with this instance.

Ring Type : The type of Protection ring. It can be either major ring or sub-ring.

Instance Configuration

Configured : A red or green dot displays:

Red: This ERPS is only created and has not yet been configured - is not active.

Green: This ERPS is configured - is active.

Guard Time : Guard timeout value to be used to prevent ring nodes from receiving outdated R-APS messages. The period of the guard timer can be configured in 10 ms steps between 10 ms and 2 seconds, with a default value of 500 ms

WTR Time : The Wait To Restore timing value to be used in revertive switching. The period of the WTR time can be configured by the operator in 1 minute steps between 5 and 12 minutes with a default value of 5 minutes.

Hold Off Time : The timing value to be used to make persistent check on Signal Fail before switching. The range of the hold off timer is 0 to 10 seconds in steps of 100 ms.

Version : ERPS Protocol Version - v1 or v2.

Revertive : In **Revertive** mode, after the conditions causing a protection switch has cleared, the traffic channel is restored to the working transport entity, i.e., blocked on the RPL.

In **Non-Revertive** mode, the traffic channel continues to use the RPL, if it is not failed, after a protection switch condition has cleared.

VLAN config : VLAN configuration of the Protection Group. Click on the "VLAN Config" link to configure VLANs for this protection group. See below for parameter descriptions.

RPL Configuration

RPL Role : It can be either RPL owner or RPL Neighbor.

RPL Port : This allows to select the east port or west port as the RPL block.

Clear : If the owner has to be changed, then the clear check box allows to clear the RPL owner for that ERPS ring.

Sub-Ring Configuration

Topology Change : Clicking this checkbox indicates that the topology changes in the sub-ring are propagated in the major ring.

Instance Command

Command : Administrative command. A port can be administratively configured to be in either manual switch or forced switch state.

Forced Switch : Forced Switch command forces a block on the ring port where the command is issued.

Manual Switch : In the absence of a failure or FS, Manual Switch command forces a block on the ring port where the command is issued.

Clear : The Clear command is used for clearing an active local administrative command (e.g., Forced Switch or Manual Switch).

Port : Port selection - Port0 or Port1 of the protection Group on which the command is applied.

Instance State

Protection State : ERPS state according to State Transition Tables in G.8032.

Port 0 : OK: State of East port is ok

SF: State of East port is Signal Fail

Port 1 : OK: State of West port is ok

SF: State of West port is Signal Fail

Transmit APS : The transmitted APS according to State Transition Tables in G.8032.

Port 0 Receive APS : The received APS on Port 0 according to State Transition Tables in G.8032.

Port 1 Receive APS : The received APS on Port 1 according to State Transition Tables in G.8032.

WTR Remaining : Remaining WTR timeout in milliseconds.

RPL Un-blocked : APS is received on the working flow.

No APS Received : RAPS PDU is not received from the other end.

Port 0 Block Status : Block status for Port 0 (Both traffic and R-APS block status). R-APS channel is never blocked on sub-rings without virtual channel.

Port 1 Block Status : Block status for Port 1 (Both traffic and R-APS block status). R-APS channel is never blocked on sub-rings without virtual channel.

FOP Alarm : Failure of Protocol Defect (FOP) status. If FOP is detected, red LED glows; else green LED glows.

Buttons

Apply : Click to save changes.

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

VLAN config : VLAN configuration of the Protection Group. Click on the "VLAN Config" link to configure VLANs for this protection group.

Click the **Add New Entry** button to display its config page:

The screenshot shows the 'ERPS VLAN Configuration 1' page. The table below is a representation of the data shown in the interface:

Delete	VLAN ID
<input type="checkbox"/>	10
<input type="checkbox"/>	20
<input type="checkbox"/>	30
<input type="button" value="Delete"/>	<input type="text" value="0"/>

Parameter Descriptions:

Delete : Click to delete a VLAN entry, check this box. The entry will be deleted during the next Save.

VLAN ID : Indicates the ID of this particular VLAN.

Add New Entry : Click to add a new VLAN ID. Valid VLAN ID values are 1 - 4095. The maximum number of VLANs is 63. The VLAN is enabled when you click Apply. A VLAN without any port members will be deleted when you click Apply. The **Delete** button can be used to undo the addition of new VLANs.

Buttons

Back : Click to go back to this MEP instance main page.

Apply : Click to save changes.

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

ERPS Messages:

'Port 0' and 'Port 1' can not be same

'Port 0 APS MEP' and 'Port 1 APS MEP' can not be same

Port 0 SF MEP and Port 1 SF MEP can not be same

'Port 1' must be zero

'Port 1 SF MEP' must be zero

3-18 MAC Table

Switching of frames is based upon the DMAC address contained in the frame. The switch builds up a table that maps MAC addresses to switch ports for knowing which ports the frames should go to (based upon the DMAC address in the frame). This table contains both static and dynamic entries. The static entries are configured by the network administrator to do a fixed mapping between the DMAC address and switch ports.

The frames also contain a MAC address (SMAC address), which shows the MAC address of the equipment sending the frame. The SMAC address is used by the switch to automatically update the MAC table with these dynamic MAC addresses. Dynamic entries are removed from the MAC table if no frame with the corresponding SMAC address has been seen after a configurable age time. To configure MAC Address Table:

Aging Configuration

1. Click Configuration, MAC Table.
2. Specify the Disable Automatic Aging and Aging Time.
3. Click Apply.

MAC Table Learning

1. Specify the Port Members (Auto, Disable, Secure).
2. Click Apply.

Static MAC Table Configuration

1. Click Configuration and Add New Static entry.
2. Specify the VLAN ID and Mac address and select Port Members.
3. Click Apply.

The screenshot displays the LANTRONIX web interface for MAC Address Table Configuration. The top navigation bar shows 'LANTRONIX' and 'SISPM1040-582-LRT'. The left sidebar contains a menu with 'Switch' and 'DMS' tabs, and a 'Configuration' section with various options like System, Green Ethernet, Ports Configuration, etc. The main content area is titled 'MAC Address Table Configuration' and includes the following sections:

- Aging Configuration:**
 - Disable Automatic Aging:
 - Aging Time: 300 seconds
- MAC Table Learning:**

	1	2	3	4	5	6	7	8	9	10
Auto	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Disable	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Secure	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
- Static MAC Table Configuration:**

Delete	VLAN ID	MAC Address	1	2	3	4	5	6	7	8	9	10
<input type="button" value="Delete"/>	10	00-00-00-00-00-00	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Buttons at the bottom include 'Add New Static Entry', 'Apply', and 'Reset'.

Figure 3-18: MAC Address Table Configuration

Parameter descriptions:

Aging Configuration : By default, dynamic entries are removed from the MAC table after 300 seconds. This removal is also called aging. Configure aging time by entering a value here in seconds; for example, Age time seconds. The allowed range is 10 to 1000000 seconds. Disable the automatic aging of dynamic entries by checking Disable automatic aging.

MAC Table Learning : If the learning mode for a given port is greyed out, another module is in control of the mode, so that it cannot be changed by the user. An example of such a module is the MAC-Based Authentication under 802.1X. Each port can do learning based on these 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.

Static MAC Table Configuration : The static entries in the MAC table are shown in this table. The static MAC table can contain 64 entries. The MAC table is sorted first by VLAN ID and then by MAC address.

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

VLAN ID : The VLAN ID of the entry.

MAC Address : The MAC address of the entry.

Port Members : Checkmarks indicate which ports are members of the entry. Check or uncheck as needed to modify the entry.

Buttons:

Add New Static Entry : Click to add a new entry to the static MAC table. Specify the VLAN ID, MAC address, and port members for the new entry. Click "Apply".

Apply : Click to save changes.

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

Messages:

Error: mac address:00-00-00-00-00-00 is not multicast mac address, support only one port.

3-19 VLAN Translation

3-19.1 Port to Group Mapping

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 Port to Group Mapping in the web UI:

1. Click Configuration, VLAN Translation, and Port to Group Mapping.
2. Specify the Port and Group configuration.
3. Click Apply.

The screenshot displays the 'VLAN Translation Port Configuration' page in the Lantronix web interface. The page title is 'VLAN Translation Port Configuration' and the breadcrumb trail is 'Home > Configuration > VLAN Translation > Port to Group Mapping'. The interface includes a top navigation bar with the Lantronix logo, a menu icon, and an 'Auto-Logout' dropdown set to 'OFF'. A left sidebar contains a navigation menu with 'Configuration' and 'DMS' sections. The main content area features a table for configuring port-to-group mappings. The table has three columns: 'Port', 'Default', and 'Group ID'. The 'Port' column lists ports 1 through 10, plus an asterisk for all ports. The 'Default' column has checkboxes. The 'Group ID' column has dropdown menus. At the bottom of the table are 'Apply' and 'Reset' buttons.

Port	Group Configuration	
	Default	Group ID
*	<input type="checkbox"/>	<input type="text" value="<"/>
1	<input type="checkbox"/>	<input type="text" value="1"/>
2	<input type="checkbox"/>	<input type="text" value="2"/>
3	<input type="checkbox"/>	<input type="text" value="3"/>
4	<input type="checkbox"/>	<input type="text" value="4"/>
5	<input type="checkbox"/>	<input type="text" value="5"/>
6	<input type="checkbox"/>	<input type="text" value="6"/>
7	<input type="checkbox"/>	<input type="text" value="7"/>
8	<input type="checkbox"/>	<input type="text" value="8"/>
9	<input type="checkbox"/>	<input type="text" value="9"/>
10	<input type="checkbox"/>	<input type="text" value="10"/>

Figure 3-19.1: Port to Group Mapping

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 a number of VLAN Translation mappings 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 of 1-12.

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 Group ID = 1.

Buttons:

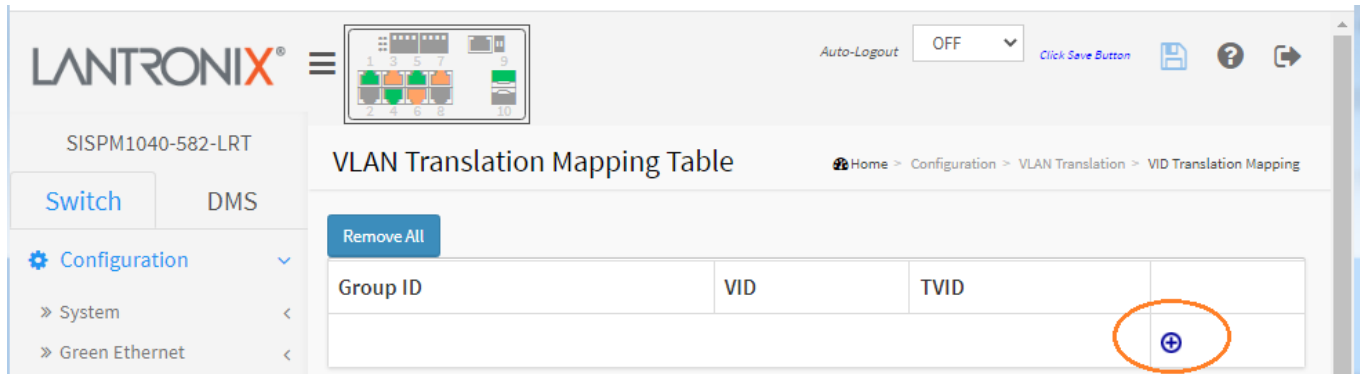
Apply : Click to save changes.

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

3-19.2 VID Translation Mapping

This page lets you view and configure current VLAN Translation Mapping parameters. To configure VID Translation Mapping in the web UI:

1. Click Configuration, VLAN Translation, and VID Translation Mapping.
2. Click the Add New Mapping button (+) to display the VLAN Translation Mapping Table entry parameters.



3. Specify the Group ID, VID, and TVID.
4. Click Apply.

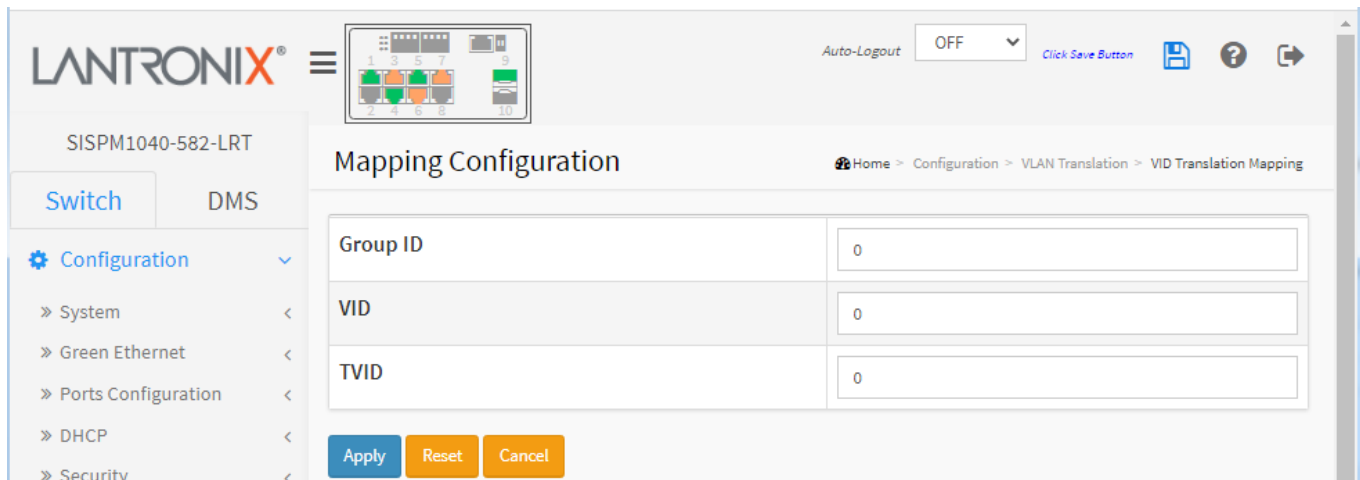


Figure 3-19.2: VLAN Translation Mapping Table

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 a number of 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 any 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.


VID : Indicates the VLAN of the mapping (i.e. 'source' VLAN). A valid VLAN ID ranges from 1 to 4095. The VID and TVID must not be the same.

TVID : Indicates the VLAN ID to which VLAN ID of an ingress frame will be translated to (granted that the mapping is enabled on the ingress port that the frame arrived at). A valid VLAN ID ranges from 1 to 4095. The VID and TVID must not be the same.

Modification Buttons

You can modify each VLAN Translation mapping in the table using these buttons:

 : Edit Mapping row.

 : Delete Mapping.

 : Add New Mapping.

Buttons:

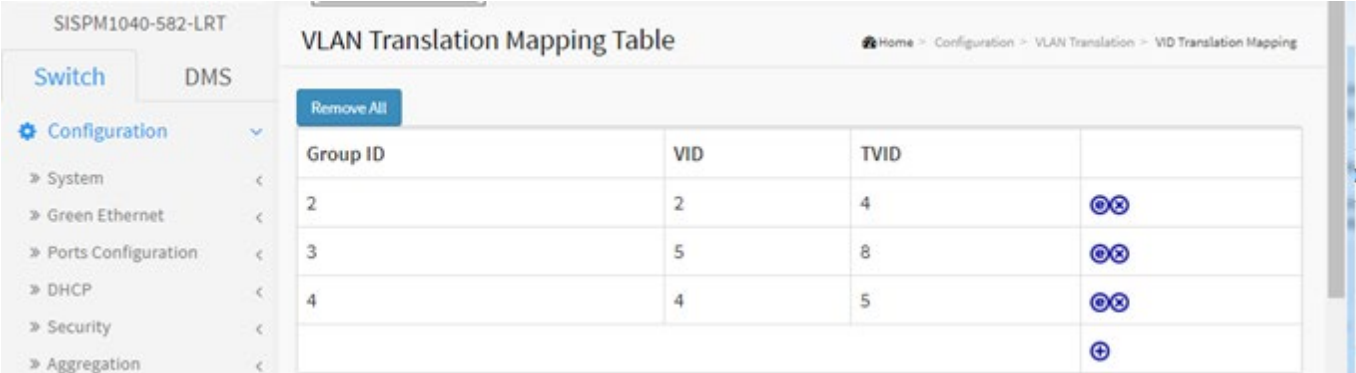
Apply : Click to save changes.








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

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

VLAN Translation Mapping Table

When you click the **Apply** button, the VLAN Translation Mapping Table displays. This page lets you create mappings of VLANs -> Translated VLANs and organize these mappings into global Groups.



Group ID	VID	TVID	
2	2	4	 
3	5	8	 
4	4	5	 
			

Buttons

Remove All: Click to remove all VLAN Translation mappings.

Messages:

'Group ID' must be an integer value between 1 and 10

VLAN ID and Translated VLAN ID cannot be same

3-20 VLANs

This page lets you set switch VLAN parameters. A Virtual LAN provides a method to restrict communication between switch ports. At layer 2, the network is partitioned into multiple, distinct, mutually isolated broadcast domains.

To configure VLAN parameters in the web UI:

1. Click Configuration, VLANs.
2. Specify Allowed Access VLANs and Ether type for Custom S-ports.
3. Specify Port VLAN Configuration parameters.
4. Click Apply.

Figure 3-20.1: VLAN Configuration

Parameter descriptions:

Global VLAN Configuration

Allowed Access VLANs : This field shows the allowed Access VLANs, i.e. it only affects ports configured as Access ports. Ports in other modes are members of all VLANs specified in the Allowed VLANs field. By default, only VLAN 1 is enabled. More VLANs may be created by using a list syntax where the individual elements are separated by commas. Ranges are specified with a dash separating the lower and upper bound. The following example will create VLANs 1, 10, 11, 12, 13, 200, and 300: 1,10-13,200,300. Spaces are allowed in between the delimiters.

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

Port VLAN Configuration

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

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

Grayed out fields show the value that the port will get when the mode is applied.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

VLAN Trunking : Trunk and Hybrid ports allow for enabling VLAN trunking. When VLAN trunking is enabled, frames classified to unknown VLANs are accepted on the port whether ingress filtering is enabled or not. This is useful in scenarios where a cloud of intermediary switches must bridge VLANs that haven't been created. By configuring the ports that connect the cloud of switches as trunking ports, they can seamlessly carry those VLANs from one end to the other.

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

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

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

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

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

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

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

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

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

The field's syntax is identical to the syntax used in the Existing VLANs field. By default, a port may become member of all possible VLANs, and is therefore set to 1-4095.

The field may be left empty, which means that the port will not be member of any of the existing VLANs, but if it is configured for VLAN Trunking it will still be able to carry all unknown VLANs.

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

Buttons:

Apply : Click to save changes.

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

3-21 Private VLANs

In a private VLAN, communication between ports in that private VLAN is not permitted. A VLAN can be configured as a private VLAN.

3-21.1 Membership

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

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

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

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

Web Interface

To configure Private VLAN Membership in the web UI:

1. Click Configuration, Private VLANs, and Membership.
2. Enable the ports want to be Port Members.
3. Click Apply.

The screenshot shows the Lantronix web interface for Private VLAN Membership Configuration. The interface includes a navigation menu on the left, a breadcrumb trail at the top right, and a main configuration area with a table for Private VLAN Membership Configuration.

Private VLAN Membership Configuration		Port Members									
Delete	PVLAN ID	1	2	3	4	5	6	7	8	9	10
<input type="checkbox"/>	1	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
<input type="checkbox"/>	0	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Figure 3-21.1: Private VLAN Membership Configuration

Parameter descriptions:

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

Private VLAN ID : Indicates the ID of this particular private VLAN. 'Private VLAN ID' must be an integer value between 1 and 10.

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

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

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

The Delete checkbox can be used to undo the addition of new Private VLANs

Buttons:

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

Refresh : Click to refresh the page immediately.

Apply : Click to save changes.

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

Messages:

'Private VLAN ID' must be an integer value between 1 and 10

3-22.2 Port Isolation

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

To configure Port Isolation in the web UI:

1. Click Configuration, Private VLANs, Port Isolation.
2. Check which ports on which you want Port Isolation to be enabled.
3. Click Apply.

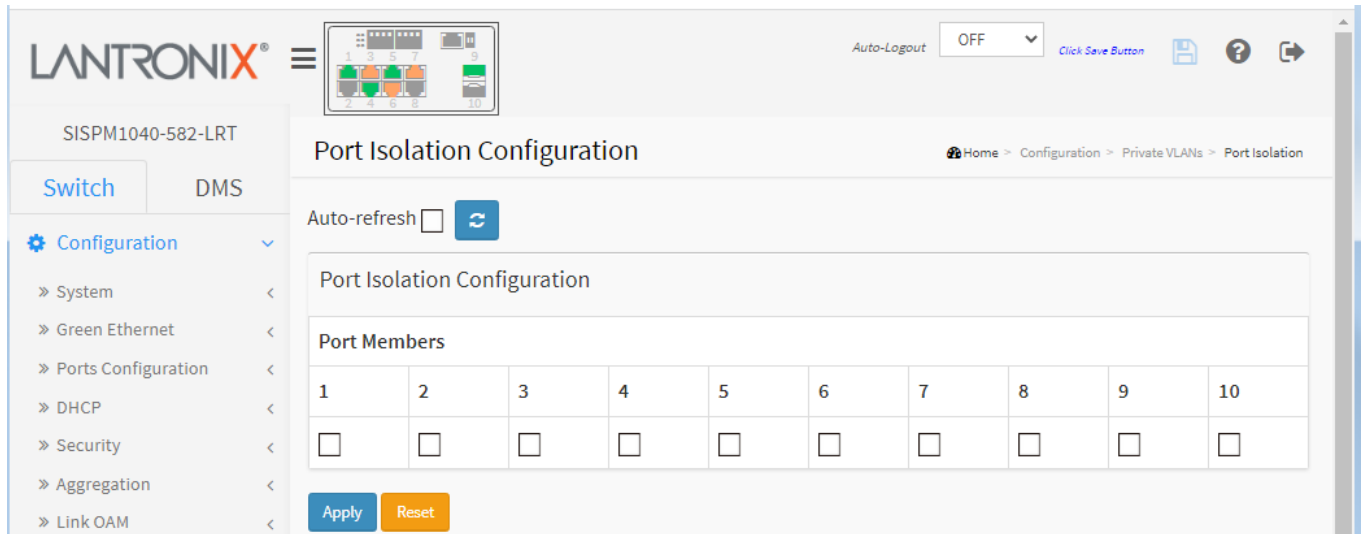


Figure 3-22.2: Port Isolation Configuration

Parameter descriptions:

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

Buttons:

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

Refresh : Click to refresh the page immediately.

Apply : Click to save changes.

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

Messages:

At least one port must be selected to add an entry

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

3-23 VCL

3-23.1 MAC-based VLAN

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

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

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

Web Interface

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

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

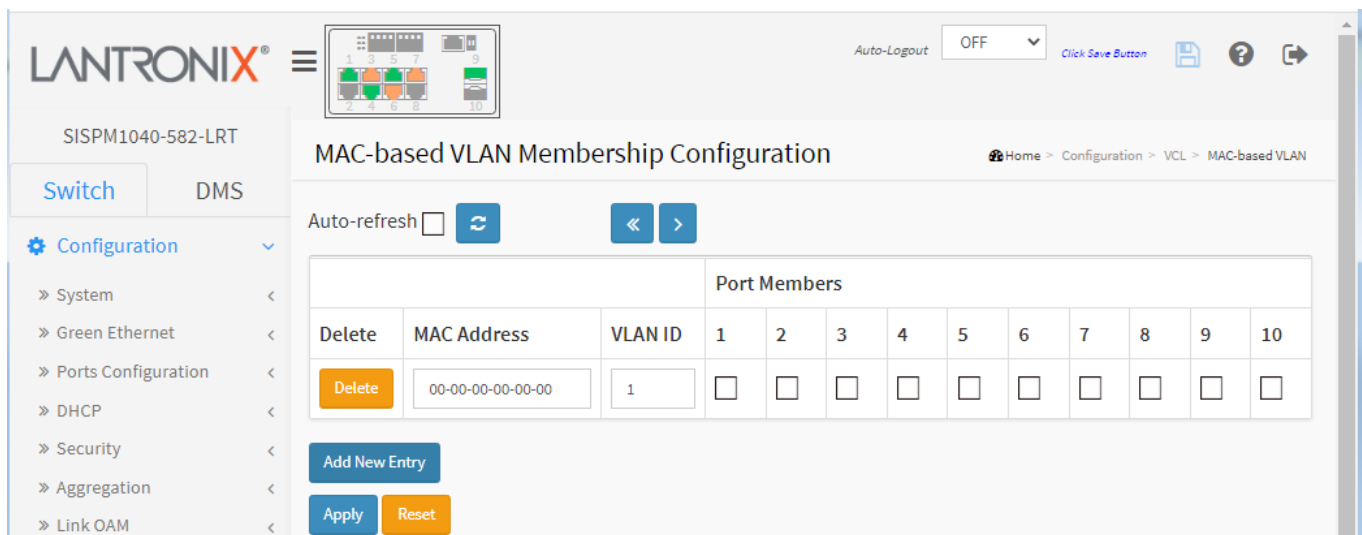


Figure 3-23.1: MAC-based VLAN Membership Configuration

Parameter descriptions:

Delete : Click to delete a MAC-based VLAN entry.

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-based VLAN entry. To include a port in a MAC-based VLAN, check the box. To remove or exclude the port from the MAC-based VLAN, make sure the box is unchecked. By default, no ports are members, and all boxes are unchecked.

Buttons:

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

The MAC-based VLAN entry is enabled on the switch when you click Apply. A MAC-based VLAN without any port members will be deleted when you click Apply. The Delete button can be used to undo the addition of new MAC-based VLANs.

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

Apply : Click to save changes immediately.

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

<< : Go to the First page.

> : Go to the Last page.

3-23.2 Protocol-based VLAN

This page lets you configure Protocol -based VLANs, including Ethernet, LLC , and SNAP protocols.

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

SNAP : The Subnetwork Access Protocol (SNAP) is a mechanism for multiplexing, on networks using IEEE 802.2 LLC, more protocols than can be distinguished by the 8-bit 802.2 Service Access Point (SAP) fields. SNAP supports identifying protocols by Ethernet type field values; it also supports vendor-private protocol identifier spaces.

It is used with IEEE 802.3, IEEE 802.4, IEEE 802.5, IEEE 802.11 and other IEEE 802 physical network layers, as well as with non-IEEE 802 physical network layers such as FDDI that use 802.2 LLC.

3-23.2.1 Protocol to Group

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

Web Interface

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

1. Click Configuration, VCL, Protocol -based VLAN configuration and add new entry.
2. Specify the Ethernet LLC SNAP Protocol and Group Name.
3. Click Apply.

The screenshot shows the 'Protocol to Group Mapping Table' configuration page in the Lantronix web interface. The page includes a navigation menu on the left with options like Configuration, System, Green Ethernet, Ports Configuration, DHCP, Security, Aggregation, Link OAM, Loop Protection, Spanning Tree, and IPMC Profile. The main content area displays a table with the following structure:

Delete	Frame Type	Value	Group Name
<input type="button" value="Delete"/>	Ethernet	Etype: 0x 0800	<input type="text"/>
<input type="button" value="Delete"/>	SNAP	OUI: 0x 00-E0-2B PID: 0x 0001	<input type="text"/>
<input type="button" value="Delete"/>	LLC	DSAP: 0x FF SSAP: 0x FF	<input type="text"/>

Below the table are buttons for 'Add New Entry', 'Apply', and 'Reset'. The page also features an 'Auto-refresh' checkbox and a refresh icon.

Figure 3-23.2.1: Protocol to Group Mapping Table

Parameter descriptions:

Delete : Click to delete a Protocol to Group Name map entry. The entry will be deleted on the switch during the next Save.

Frame Type : Frame Type can be 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.

The three different Frame Types are described below:

Ethernet: Values in the text field when Ethernet is selected as a Frame Type are called etype. Valid etype values 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 in this case also is comprised of two different sub-values.

a. OUI: OUI (Organizationally Unique Identifier) is value in format of xx-xx-xx where each pair (xx) in string is a hexadecimal value from 0x00-0xff.

b. PID: If the OUI is hexadecimal 000000, the protocol ID is the Ethernet type (EtherType) field value for the protocol running on top of SNAP; if the OUI is an OUI for a particular organization, the protocol ID is a value assigned by that organization to the protocol running on top of SNAP.

In other words, if value of OUI field is 00-00-00 then value of PID will be etype (0x0600-0xffff) and if value of OUI is other than 00-00-00 then valid value of PID will be any value from 0x0000 to 0xffff.

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

Group Name : A valid Group Name is a unique 16-character long string for every entry which consists of a combination of alphabets (a-z or A-Z) and integers (0-9).

Note: Special characters and underscore (_) are not allowed.

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

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

Buttons:

Apply : Click to save changes.

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

Refresh: Click to refresh the Protocol Group Mapping information manually.

Messages:

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

3-23.2.2 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 parameters in the web UI:

1. Click Configuration > VCL > Protocol-based VLAN > Group to VLAN.
2. Click Add New Entry and specify the Group Name, VLAN ID, and check port members.
3. Click Apply.

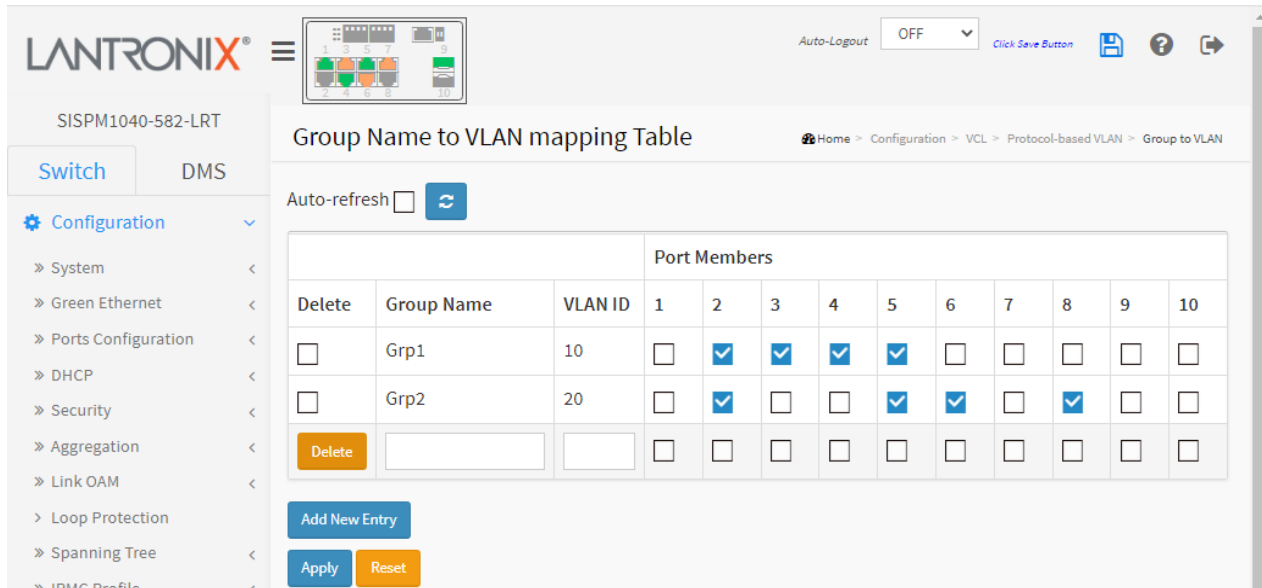


Figure 3-23.2.2: Group Name of VLAN Mapping Table

Parameter descriptions:

Delete : Click to delete a Group Name to VLAN map entry.

Group Name : A valid Group Name is a string of almost 16 characters which consists of a combination of alphabets (a-z or A-Z) and integers (0-9), no special character is allowed. Whichever Group name you try map to a VLAN must be present in Protocol to Group mapping table and must not be perused by any other existing mapping entry on this page.

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

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

Buttons:

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

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

Refresh : Click to immediately refresh the page information manually.

Apply : Click to save changes.

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

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

3-24.1 IP Subnet-based VLAN

The IP subnet-based VLAN entries can be configured here. This page allows for adding, updating and deleting IP subnet-based VLAN entries and assigning the entries to different ports. This page shows only static entries.

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

1. Click Configuration, VCL, Group Name VLAN configuration and Add New Entry.
2. Specify the VCE ID, IP Address, Mask Length, VLAN ID and select Port Members.
3. Click Apply.

The screenshot displays the 'IP Subnet-based VLAN Membership Configuration' page in the Lantronix web UI. The page title is 'IP Subnet-based VLAN Membership Configuration' and the breadcrumb trail is 'Home > Configuration > VCL > IP Subnet-based VLAN'. The page includes an 'Auto-refresh' checkbox and a refresh icon. The main configuration area is a table with the following structure:

Delete	IP Address	Mask Length	VLAN ID	Port Members										
				1	2	3	4	5	6	7	8	9	10	
<input type="checkbox"/>	1.2.3.0	24	1	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	2.4.6.0	24	2	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	0.0.0.0	24	1	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Below the table are buttons for 'Delete', 'Add New Entry', 'Apply', and 'Reset'. The 'Add New Entry' button is highlighted in blue.

Figure 3-24.3: IP Subnet-based VLAN Membership Configuration

Parameter descriptions:

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

VCE ID : Indicates the index of the entry. It is user configurable. Its value ranges from 0-128. If a VCE ID is 0, application will auto-generate the VCE ID for that entry. Deletion and lookup of IP subnet-based VLAN are based on VCE ID.

IP Address : Indicates the IP address.

Mask Length : Indicates the network mask length.

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

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

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

The IP subnet-based VLAN entry is enabled on the switch when you click Apply. The maximum possible IP subnet-based VLAN entries are limited to 128.

Buttons:

Apply : Click to save changes.

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

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

Refresh : Click to immediately refresh the page information manually.

3-24 Voice VLAN

Voice VLAN is VLAN configured specially for voice traffic. By adding the ports with voice devices attached to voice VLAN, we can perform QoS-related configuration for voice data, ensuring the transmission priority of voice traffic and voice quality.

3-24.1 Configuration

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

To configure Voice VLAN in the web UI:

1. Select Configuration, Voice VLAN, Configuration.
2. Select "Enabled" as the Mode and specify VLAN ID, Aging Time, and Traffic Class.
3. Specify Port Mode, Security, and Discovery Protocol in the Port Configuration section.
4. Click Apply.

The screenshot displays the Lantronix web interface for configuring Voice VLAN. The top navigation bar includes the Lantronix logo, a menu icon, and an Auto-Logout dropdown set to OFF. The breadcrumb trail is Home > Configuration > Voice VLAN > Configuration. The main content area is divided into two sections: Voice VLAN Configuration and Port Configuration.

Voice VLAN Configuration

Mode	Disabled
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

Figure 3-24.1: Voice VLAN Configuration

Parameter descriptions:**Voice VLAN Configuration**

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

Enabled: Enable Voice VLAN mode operation.

Disabled: Disable Voice VLAN mode operation.

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

Aging Time : Indicates the Voice VLAN secure learning aging time. The allowed range is 10 = 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 Class : Indicates the Voice VLAN traffic class. All traffic on the Voice VLAN will apply this class.

Port Configuration

Port: Indicates the port number for each row in the table.

Mode : Indicates the Voice VLAN port mode. When the port mode isn't equal disabled, we must disable MSTP feature before we enable Voice VLAN. It can avoid the conflict of ingress filtering. Possible port modes are:

Disabled: Disjoin from Voice VLAN.

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

Forced: Force join to Voice VLAN.

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

Enabled: Enable Voice VLAN security mode operation.

Disabled: Disable Voice VLAN security mode operation.

Discovery Protocol : Indicates the Voice VLAN port discovery protocol. It will only work when auto detect mode is enabled. We should enable 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: Both OUI and LLDP.

Buttons:

Apply : Click to save changes.

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

3-24.2 OUI

This page lets you configure Voice VLAN OUI table parameters. An Organizationally Unique Identifier (OUI) is a 24-bit number that uniquely identifies a vendor, manufacturer, or other organization. OUIs are purchased from the IEEE Registration Authority by the assignee (IEEE term for the vendor, manufacturer, or other organization).

The maximum entry number is 16. Modifying the OUI table will restart auto detection of the OUI process. To configure Voice VLAN OUI via the web UI:

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

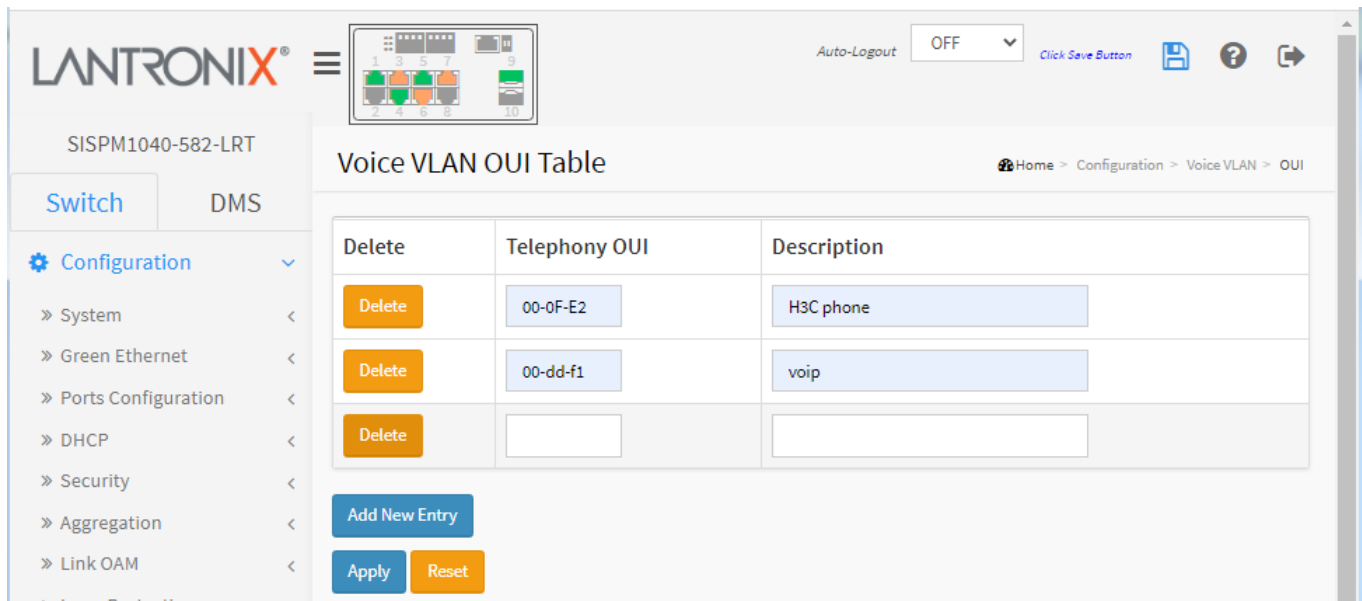


Figure 3-45.2: Voice VLAN OUI Table

Parameter descriptions:

Delete : Check to delete the entry.

Telephony OUI : A telephony OUI address is a globally 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). You can determine which vendor a device belongs to according to the OUI address which forms the first 24 bits of a MAC address.

Description : The description of OUI address. Normally, it describes which vendor telephony device it belongs to. The allowed string length is 0 – 32 characters.

Buttons:

Add New Entry : Click to add a new entry in Voice VLAN OUI table. An empty row is added to the table.

Apply : Click to save changes.

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

3-25 Ethernet Services

3-25.1 Ports

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

To configure EVC port parameters in the web UI:

1. Click Configuration, Ethernet Services, and Ports.
2. Specify DEI Mode, Tag Mode and Address Mode.
3. Click Apply.

The screenshot shows the 'Port Configuration' page in the Lantronix web UI. The page title is 'Port Configuration' and the breadcrumb is 'Home > Configuration > Ethernet Services > Ports'. The table below shows the configuration for ports 1 through 10. The 'Port' column lists ports 1-10, with a '*' for the header row. The 'DEI Mode' column is set to 'Fixed' for all ports. The 'Tag Mode' column is set to 'Outer' for all ports. The 'Address Mode' column is set to 'Source' for all ports. There are 'Apply' and 'Reset' buttons at the bottom of the table.

Port	DEI Mode	Tag Mode	Address Mode
*	<>	<>	<>
1	Fixed	Outer	Source
2	Fixed	Outer	Source
3	Fixed	Outer	Source
4	Fixed	Outer	Source
5	Fixed	Outer	Source
6	Fixed	Outer	Source
7	Fixed	Outer	Source
8	Fixed	Outer	Source
9	Fixed	Outer	Source
10	Fixed	Outer	Source

Figure 3-25.1: Port Configuration

Parameter descriptions:

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

DEI Mode : The Drop Eligible Indicator mode for an NNI port determines whether frames transmitted on the port will have the DEI field in the outer tag marked based on the color of the frame. The allowed values are:

Coloured: The DEI is 1 for yellow frames and 0 for green frames.

Fixed: The DEI value is determined by ECE rules.

Tag Mode : The tag mode specifying whether the EVC classification must be based on the outer or inner tag. This can be used on NNI ports connected to another service provider, where an outer "tunnel" tag is added together with the inner tag identifying the EVC. The allowed values are:

Inner: Enable inner tag in EVC classification.

Outer: Enable outer tag in EVC classification.

Address Mode : The IP/MAC address mode specifying whether the EVC classification must be based on source (SMAC/SIP) or destination (DMAC/DIP) addresses. The allowed values are:

Source: Enable SMAC/SIP matching.

Destination: Enable DMAC/DIP matching.

Buttons:

Apply : Click to save changes.

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

3-25.2 L2CP

This page lets you configure EVC L2CP parameters. To configure Layer 2 Control Protocol (L2CP) Port parameters in the web UI:

1. Click Configuration, Ethernet Services, and L2CP.
2. Specify DMAC and L2CP Mode.
3. Click Apply.

DMAC	L2CP Mode
*	<>
01-80-C2-00-00-00	Peer
01-80-C2-00-00-01	Peer
01-80-C2-00-00-02	Peer
01-80-C2-00-00-03	Peer
01-80-C2-00-00-04	Peer
01-80-C2-00-00-05	Peer
01-80-C2-00-00-06	Peer
01-80-C2-00-00-07	Peer
01-80-C2-00-00-08	Peer
01-80-C2-00-00-09	Peer

Figure 3-25.2: L2CP Port Configuration

Parameter descriptions:

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

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

Peer: Allow to peer L2CP frames.

Forward: Allow to forward L2CP frames.

Buttons:

Refresh-Click to refresh the page immediately.

Apply : Click to save changes.

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

3-25.3 Bandwidth Profiles

This page lets you configure EVC ingress bandwidth profile configurations. These policers may be used to limit the traffic received on UNI ports. To configure Bandwidth Profiles in the web UI:

1. Click Configuration, Ethernet Services, and Bandwidth Profiles.
2. Specify State, Type, Policer Mode, and Rate Type.
3. Click Apply.

The screenshot shows the 'Bandwidth Profiles Configuration' page in the Lantronix web UI. The page title is 'Bandwidth Profiles Configuration' and the breadcrumb trail is 'Home > Configuration > Ethernet Services > Bandwidth Profiles'. The page includes a 'Refresh' button and navigation arrows. Below the navigation is a form to set 'Start from Policer ID' (1) and 'entries per page' (20). The main content is a table with the following columns: Policer ID, State, Type, Policer Mode, Rate Type, CIR (kbps), CBS (bytes), EIR (kbps), and EBS (bytes). The table contains 8 rows of configuration entries, all with 'Disabled' state and 'MEF' type.

Policer ID	State	Type	Policer Mode	Rate Type	CIR (kbps)	CBS (bytes)	EIR (kbps)	EBS (bytes)
*	<>	<>	<>	<>	0	0	0	0
1	Disabled	MEF	Aware	Data	0	0	0	0
2	Disabled	MEF	Aware	Data	0	0	0	0
3	Disabled	MEF	Aware	Data	0	0	0	0
4	Disabled	MEF	Aware	Data	0	0	0	0
5	Disabled	MEF	Aware	Data	0	0	0	0
6	Disabled	MEF	Aware	Data	0	0	0	0
7	Disabled	MEF	Aware	Data	0	0	0	0
8	Disabled	MEF	Aware	Data	0	0	0	0

Figure 3-25.3: Bandwidth Profiles Configuration

Parameter descriptions:

Start Policer ID : The start Policer ID for displaying the table entries. The allowed range is 1 - 256.

Number of Entries : The number of entries per page. The allowed range is 2 – 256 entries.

Policer ID : The Policer ID is used to identify one of the 256 policers.

State : The administrative state of the bandwidth profile. The allowed values are:

Enabled: The bandwidth profile enabled.

Disabled: The bandwidth profile is disabled.

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

MEF: MEF ingress bandwidth profile.

Single: Single bucket policer.

Policer Mode : The color mode of the bandwidth profile. The allowed values are:

Coupled: Color-aware mode with coupling enabled.

Aware: color-aware mode with coupling disabled.

Rate Type : The rate type of the bandwidth profile. The allowed values are:

Data: Specify that this bandwidth profile operates on data rate.

Line: Specify that this bandwidth profile operates on line rate.

CIR : The Committed Information Rate of the bandwidth profile. The allowed range is 0 - 10000000 kilobits per second.

CBS : The Committed Burst Size of the bandwidth profile. The allowed range is 0 – 100000 bytes.

EIR : The Excess Information Rate for MEF type bandwidth profile. The allowed range is 0 - 10000000 kilobits per second.

EBS : The Excess Burst Size for MEF type bandwidth profile. The allowed range is 0 - 100000 bytes.

Buttons:



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

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

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

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

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

Apply- Click to save changes.


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

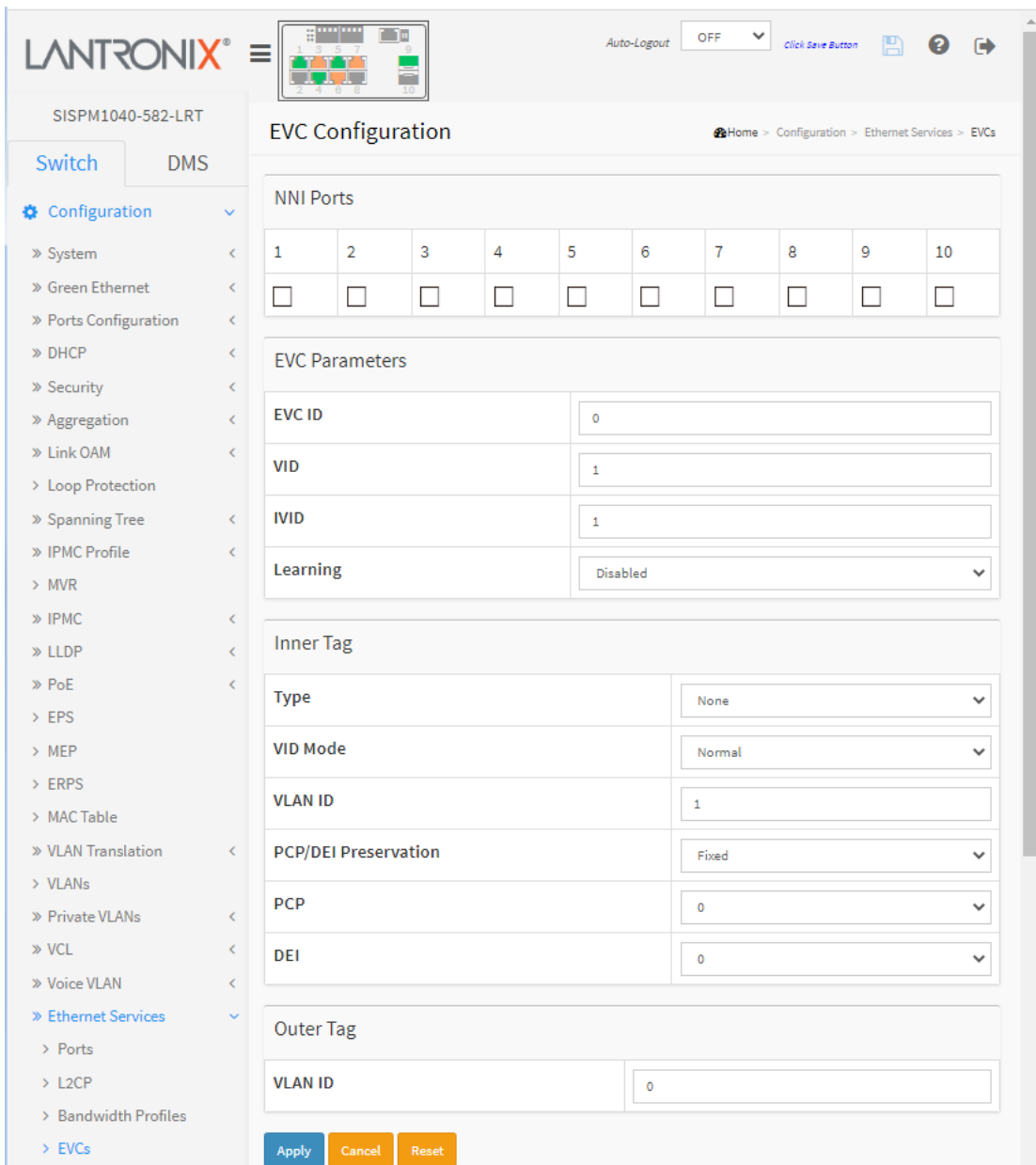
3-25.4 EVCs

This page lets you view and set EVC parameters. This system supports Provider Bridge based EVCs.

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

To configure EVC parameters in the web UI:

1. Click Configuration, Ethernet Services, and EVCs to display the default page.
2. From the default page, click the  icon to add a new EVC.
3. Specify NNI Port, EVC, Inner Tag, and Outer Tag parameters and click Apply.



The screenshot displays the 'EVC Configuration' web interface. At the top, there is a header with the Lantronix logo, a navigation menu, and a status bar showing 'Auto-Logout OFF' and 'Click Save Button'. The main content area is divided into several sections:

- NNI Ports:** A table with 10 columns representing ports 1 through 10. Each column has a checkbox below it, all of which are currently unchecked.
- EVC Parameters:** A form with the following fields:
 - EVC ID: 0
 - VID: 1
 - IVID: 1
 - Learning: Disabled (dropdown menu)
- Inner Tag:** A form with the following fields:
 - Type: None (dropdown menu)
 - VID Mode: Normal (dropdown menu)
 - VLAN ID: 1
 - PCP/DEI Preservation: Fixed (dropdown menu)
 - PCP: 0 (dropdown menu)
 - DEI: 0 (dropdown menu)
- Outer Tag:** A form with the following field:
 - VLAN ID: 0

At the bottom of the configuration area, there are three buttons: 'Apply' (blue), 'Cancel' (orange), and 'Reset' (orange).

Parameter descriptions:

NNI Ports : The list of Network to Network Interfaces for the EVC.

EVC ID : The EVC ID identifies the EVC. The range is 1 - 256.

VID : The VLAN ID in the PB network. It may be inserted in a C-tag, S-tag or S-custom tag depending on the NNI port VLAN configuration. The range is 1-4095.

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

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

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

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

Inner Tag Type : The inner tag type is used to determine whether an inner tag is inserted in frames forwarded to NNI ports. The possible values are:

None: An inner tag is not inserted.

C-tag: An inner C-tag is inserted.

S-tag: An inner S-tag is inserted.

S-custom-tag: An inner tag is inserted and the tag type is determined by the VLAN port configuration of the NNI.

Inner VID Mode : The inner VID Mode affects the VID in the inner and outer tag. The possible values are:

Normal: The VID of the two outer tags isn't swapped.

Tunnel: The VID of the two outer tags are swapped, so that the VID of the outer tag is taken from the Inner Tag configuration and the VID of the inner tag is the EVC VID. In this mode, the NNI ports are normally configured to do EVC classification based on the inner tag.

Inner Tag VID : The Inner tag VLAN ID. The allowed range is 0 - 4095.

Inner Tag PCP/DEI Preservation : The inner tag PCP and DEI preservation. The possible values are:

Preserved: The inner tag PCP and DEI is preserved.

Fixed: The inner tag PCP and DEI is fixed.

Inner Tag PCP : The inner tag PCP value. The allowed range is 0 - 7.

Inner Tag DEI : The inner tag Drop Eligible Indicator value. The allowed value is 0 or 1.

Outer Tag VID : The EVC outer tag VID for UNI ports. The allowed range is 0 - 4095.

Modification Buttons: You can modify each EVC in the table using these buttons:

: Edit the EVC row.

: Delete the EVC.

: Add New EVC.

Buttons:

Refresh –Click to refresh the page immediately.

Remove All- Click to remove all EVCs.

Apply : Click to save changes.

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

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

EVC Control List Configuration page example:

SISPM1040-582-LRT

Switch DMS

Home > Configuration > Ethernet Services > EVCs

Refresh Remove All

EVC ID	VID	IVID	Learning	Inner Tag							Outer Tag		NNI Ports	
				Type	VID Mode	VID	PCP/DEI Preservation	PCP	DEI	VID				
1	12	3	Enabled	C-tag	Normal	1	Fixed	0	0	20	2-5	⊖ ⊗		
3	6	8	Disabled	S-tag	Normal	1	Fixed	0	0	12	4,5	⊖ ⊗		
4	3	1	Disabled	S-custom-tag	Normal	1	Fixed	0	0	9	4,5,9,10	⊖ ⊗		
												⊕		


Configuration

- System
- Green Ethernet
- Ports Configuration
- DHCP
- Security
- Aggregation
- Link OAM
- Loop Protection

3-25.5 ECEs


This page lets you configure EVC Control Entries (ECEs). An ECE lists rules ordered in a list to control the preferred classification.

To configure ECE Control List Configuration in the web UI:

1. Click Configuration, Ethernet Services, and ECEs.
2. Click the  icon to display the ECE Configuration page.
3. Specify UNI Port, Ingress Matching, Actions, MAC, and Egress Outer Tag parameters.
4. Click Apply.

ECE Control List Configuration Home > Configuration > Ethernet Services > ECEs

Refresh Remove All

ECE ID	Ingress Matching					Actions					Egress Outer Tag			Conflict	
	UNI Ports	Tag Type	VID	PCP	DEI	Frame Type	Direction	EVC ID	Tag Pop Count	Policy ID	Class	Mode	PCP/DEI Preservation		PCP
															

SISPM1040-582-LRT ECE Configuration Home > Configuration > Ethernet Services > ECEs

Switch DMS

UNI Ports

1	2	3	4	5	6	7	8	9	10
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Ingress Matching

Tag Type: Any

Frame Type: Any

Actions

Direction: Both

EVC ID Filter: Specific

EVC ID Value: 1

Tag Pop Count: 1

Policy ID: 1

Class: Default

MAC Parameters

SMAC Filter: Any

DMAC Type: Any

Egress Outer Tag

Mode: Default

PCP/DEI Preservation: Fixed

PCP: 1

DEI: 1

Apply Cancel Reset

Figure 3-25.5: ECE Configuration

Parameter descriptions:

ECE ID : The ECE ID identifies the ECE. Unique ECE IDs are automatically assigned to ECEs added. The possible range is 1 - 256.

Ingress Matching

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

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

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

Untagged: The ECE will match untagged frames only.

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

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

Tagged: The ECE will match tagged frames only.

VID : The VLAN ID for the ECE. It only significant if tag type 'Tagged' is selected. The possible values are:

Specific: The range is from 0 through 4095.

Any: The ECE will match any VLAN ID.

PCP : The Priority Code Point value for the ECE. It only significant if tag type 'Tagged' is selected. Possible values:

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

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

Any: The ECE will match any PCP value.

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

Frame Type : The frame type for the ECE. The possible values are:

Any: The ECE will match any frame type.

IPv4: The ECE will match IPv4 frames only.

IPv6: The ECE will match IPv6 frames only.

Actions

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

Both: Bidirectional.

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

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

EVC ID : The EVC ID for the ECE. The ECE is only active when mapping to an existing EVC. Possible values are:

Specific: The range is from 1 through 256.

None: The ECE does not map to an EVC.

Tag Pop Count : The ingress tag pop count for the ECE. The possible range is 0 - 2.

Policy ID : The ACL Policy ID for the ECE. The range is 0 - 255.

Class : The traffic class for the ECE. The range is 0 - 7.

MAC Parameters

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

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

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

SMAC Value: When "Specific" is selected for the SMAC filter, you can enter a specific value.

The legal format is "xx-xx-xx-xx-xx-xx" or "xx.xx.xx.xx.xx.xx" or "xxxxxxxxxxxx" (x is a hexadecimal digit).

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

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

Unicast: Frame must be unicast.

Multicast: Frame must be multicast.

Broadcast: Frame must be broadcast.

Egress Outer Tag

Outer Tag Mode : The outer tag for nni-to-uni direction for the ECE. The possible values are:

Enable: Enable outer tag for nni-to-uni direction for the ECE.

Disable: Disable outer tag for nni-to-uni direction for the ECE.

Outer Tag PCP/DEI Preservation : The outer tag PCP and DEI preservation for the ECE. The possible values are:

Preserved: The outer tag PCP and DEI are preserved.

Disable: The outer tag PCP and DEI are fixed.

Outer Tag PCP : The outer tag Priority Code Point value for the ECE. The possible range is from 0 through 7.

Outer Tag DEI : The outer tag DEI value for the ECE. The possible value is 0 or 1.

Conflict : Indicates the hardware status of the specific ECE. The specific ECE is not applied to the hardware due to hardware limitations.

ECE Control List example:

ECE ID	Ingress Matching						Actions					Egress Outer Tag			Conflict		
	UNI Ports	Tag Type	VID	PCP	DEI	Frame Type	Direction	EVC ID	Tag Pop Count	Policy ID	Class	Mode	PCP/DEI Preservation	PCP		DEI	
1	None	Any	Any	Any	Any	Any	Both	1	0	0	Disabled	Disabled	Fixed	0	0	No	⊕ ⊕ ⊕ ⊕ ⊕
2	6-8	Tagged	Any	Any	Any	IPv4	UNI-to-NNI	1	1	0	Disabled	Disabled	Fixed	0	0	No	⊕ ⊕ ⊕ ⊕ ⊕

Modification Buttons

You can modify each ECE (EVC Control Entry) in the table using these buttons:

⊕: Inserts a new ECE before the current row.

ⓔ: Edits the ECE row.

⬆️: Moves the ECE up the list.

⬇️: Moves the ECE down the list.

⊗: Deletes the ECE.

⊕: The lowest plus sign adds a new entry at the bottom of the ECE listings.

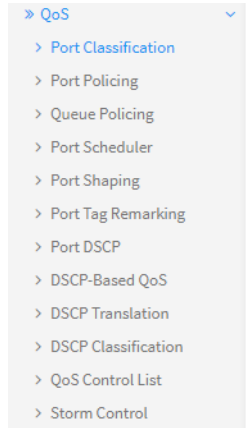
Buttons:

Refresh : Click to refresh the page immediately.

Remove All : Click to remove all ECEs.

3-26 QoS

The switch support four QoS queues per port with strict or weighted fair queuing scheduling. It supports QoS Control Lists (QCL) for advance programmable QoS classification, based on IEEE 802.1p, Ethertype, VID, IPv4/IPv6 DSCP and UDP/TCP ports and ranges. This feature 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 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. A super priority queue with dedicated memory and strict highest priority in the arbitration. The ingress super priority queue allows traffic recognized as CPU traffic to be received and queued for transmission to the CPU even when all the QoS class queues are congested.



3-26.1 Port Classification

This page lets you configure the basic QoS Ingress Classification settings for all switch ports.

To configure the QoS Ingress Port Classification in the web UI:

1. Click Configuration, QoS, Port Classification.
2. Select QoS class, DP Level, PCP and DEI parameters.
3. Click the Apply button to save the settings.
4. To cancel the settings click the Reset button to revert to previously saved values.

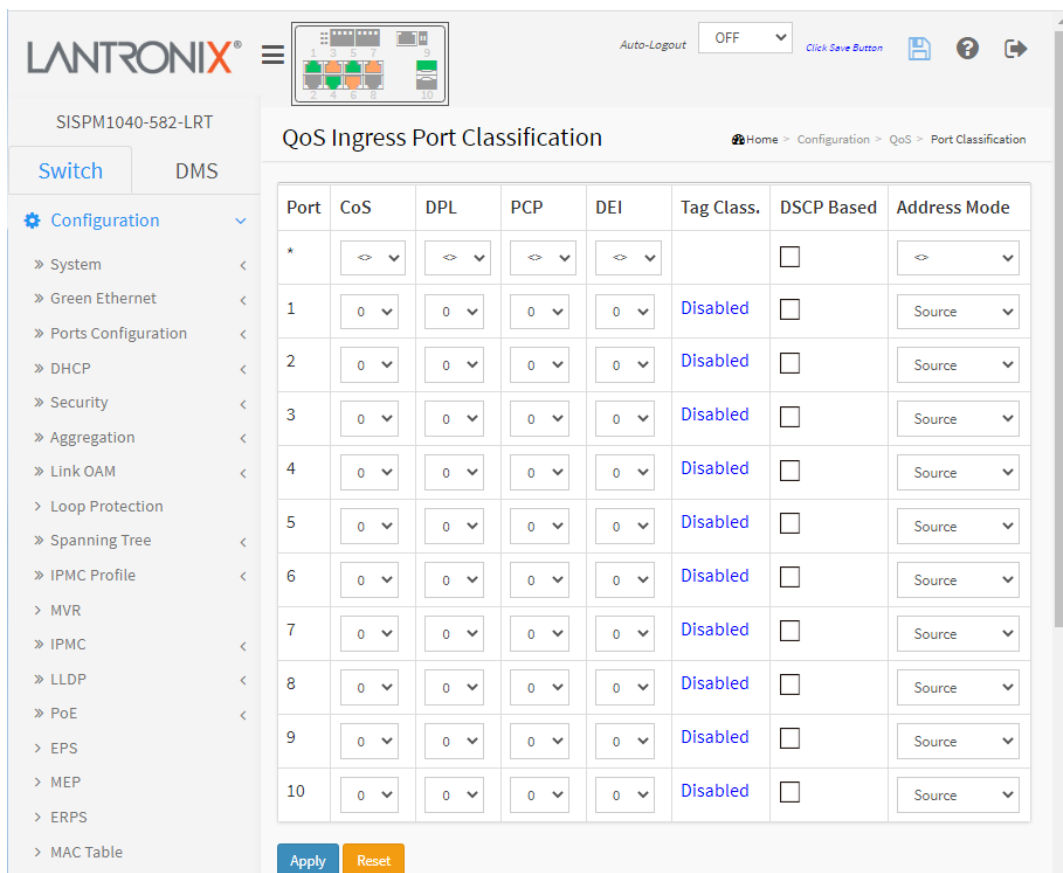


Figure 3-26.1: QoS Configuration

Parameter descriptions:

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

CoS : Controls the default class of service.

All frames are classified to a CoS. There is a one to one mapping between CoS, queue and priority. A CoS of 0 (zero) has the lowest priority.

If the port is VLAN aware, the frame is tagged and Tag Class. is enabled, then the frame is classified to a CoS that is mapped from the PCP and DEI value in the tag. Otherwise, the frame is classified to the default CoS. The classified CoS can be overruled by a QCL entry.

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

DPL : Controls the default drop precedence level.

All frames are classified to a drop precedence level.

If the port is VLAN aware, the frame is tagged and Tag Class. is enabled, then the frame is classified to a DPL that is mapped from the PCP and DEI value in the tag. Otherwise, the frame is classified to the default DPL. The classified DPL can be overruled by a QCL entry.

PCP : Controls the default Priority Code Point 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 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.

Tag Class. : Shows the classification mode for tagged frames on this port.

Disabled: Use default QoS class and DP level for tagged frames.

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

Click on the linked text [Disabled](#) to configure the mode and/or mapping.

Note: This setting has no effect if the port is VLAN unaware. Tagged frames received on VLAN unaware ports are always classified to the default CoS and DPL.

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

Address Mode : The IP/MAC address mode specifying whether the QCL classification must be based on source (SMAC/SIP) or destination (DMAC/DIP) addresses on this port. The allowed values are:

Source: Enable SMAC/SIP matching.

Destination: Enable DMAC/DIP matching.

Buttons:

Apply : Click to save changes.

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

In the Tag Class. column click the linked text [Disabled](#) to display the QoS Ingress Port Tag Classification for the selected Port. The classification mode for tagged frames are configured on this page.

QoS Ingress Port Tag Classification Port 10

Port 10

Tagged Frames Settings

Tag Classification: Disabled

(PCP, DEI) to (QoS class, DP level) Mapping

PCP	DEI	QoS class	DP level
*	*	0	0
0	0	1	0
0	1	1	1
1	0	0	0
1	1	0	1
2	0	2	0
2	1	2	1
3	0	3	0
3	1	3	1
4	0	4	0
4	1	4	1
5	0	5	0
5	1	5	1
6	0	6	0
6	1	6	1
7	0	7	0
7	1	7	1

Apply Reset Cancel

QoS Ingress Port Tag Classification for Port 10

Parameter descriptions:

Tag Classification : Controls the classification mode for tagged frames on this port.

Disabled: Use default QoS class and Drop Precedence Level for tagged frames.

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

(PCP, DEI) to (QoS class, DP level) Mapping : Controls the mapping of the classified (PCP, DEI) to (QoS class, DP level) values when Tag Classification is set to Enabled.

Buttons

Apply : Click to save changes.

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

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

Definitions

PCP (Priority Code Point) is a 3-bit field storing the priority level for the 802.1Q frame. It is also known as User Priority.

DEI (Drop Eligible Indicator) is a 1-bit field in the VLAN tag.

QoS class: Every incoming frame is classified to a QoS class, which 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. There is a one to one mapping between QoS class, queue and priority. A QoS class of 0 (zero) has the lowest priority.

DP Level (Drop Precedence Level) (DPL): Every incoming frame is classified to a Drop Precedence Level (DP level), which is used throughout the device for providing congestion control guarantees to the frame according to what was configured for that specific DP level. A DP level of 0 (zero) corresponds to 'Committed' (Green) frames and a DP level of 1 corresponds to 'Discard Eligible' (Yellow) frames.

3-26.2 Port Policing

This page lets you configure QoS Ingress Port Policers for all switch ports. Port Policing is useful in constraining traffic flows and marking frames above specific rates. Policing is primarily useful for data flows and voice or video flows because voice and video usually maintains a steady rate of traffic.

To set QoS Ingress Port Policers in the web UI:

1. Click Configuration, QoS, Port Policing.
2. Enable the ports for QoS Ingress Port Policers and type the Rate limit.
3. Select the Rate limit Unit and select Flow Control.
4. Click Apply to save the configuration.

Port	Enable	Rate	Unit	Flow Control
*	<input type="checkbox"/>	500	<>	<input type="checkbox"/>
1	<input type="checkbox"/>	500	kbps	<input type="checkbox"/>
2	<input type="checkbox"/>	500	kbps	<input type="checkbox"/>
3	<input type="checkbox"/>	500	kbps	<input type="checkbox"/>
4	<input type="checkbox"/>	500	kbps	<input type="checkbox"/>
5	<input type="checkbox"/>	500	kbps	<input type="checkbox"/>
6	<input type="checkbox"/>	500	kbps	<input type="checkbox"/>
7	<input type="checkbox"/>	500	kbps	<input type="checkbox"/>
8	<input type="checkbox"/>	500	kbps	<input type="checkbox"/>
9	<input type="checkbox"/>	500	kbps	<input type="checkbox"/>
10	<input type="checkbox"/>	500	kbps	<input type="checkbox"/>

Figure 3-26.2: QoS Ingress Port Policers

Parameter descriptions:

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

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

Rate : To set the Rate limit value for this port, the default is 500.

Unit : Select what unit of rate includes kbps, Mbps, fps and kfps. The default is kbps.

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

Buttons:

Apply –:Click to save changes.

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

3-26.3 Queue Policing

This page lets you configure the Queue Policer settings for all switch ports. To set the Queue Ingress Queue Policers in the web UI:

1. Click Configuration, QoS and Queue Policing.
2. Specify the Queue Policing parameters.

The screenshot shows the Lantronix web interface for configuring QoS Ingress Queue Policers. The page title is "QoS Ingress Queue Policers" and the breadcrumb is "Home > Configuration > QoS > Queue Policing". A table allows enabling or disabling queue policing for ports 1 through 10 across Queue 0 to Queue 7. Each cell contains a checkbox. Below the table are "Apply" and "Reset" buttons.

	Queue 0	Queue 1	Queue 2	Queue 3	Queue 4	Queue 5	Queue 6	Queue 7
Port	Enable	Enable	Enable	Enable	Enable	Enable	Enable	Enable
*	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
1	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
2	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
3	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
4	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
5	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
6	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
7	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
8	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
9	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
10	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Figure 3-26.3: Queue Policing - QoS Ingress Queue Policers

Parameter descriptions:

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

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

Rate : Controls the rate for the queue policer. This value is restricted to 100-3276700 when "Unit" is kbps, and 1-3276 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 is only shown if at least one of the queue policers are enabled.

Buttons:

Apply : Click to save changes.

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

Example:

The screenshot displays the 'QoS Ingress Queue Policers' configuration page. The interface includes a navigation menu on the left with options like 'System', 'Green Ethernet', 'Ports Configuration', etc. The main area contains a table for configuring queue policers across 11 ports (0-10) and 8 queues (0-7). Each queue configuration includes an 'Enable' checkbox, a 'Rate' field (set to 500), and a 'Unit' dropdown (set to kbps). Ports 2, 3, and 4 have their 'Enable' checkboxes checked for Queue 0. At the bottom of the table, there are 'Apply' and 'Reset' buttons.

Port	Queue 0			Queue 1			Queue 2			Queue 3			Queue 4	Queue 5	Queue 6	Queue 7	
	E	Rate	Unit	E	Rate	Unit	E	Rate	Unit	E	Rate	Unit	Enable	Enable	Enable	Enable	
*	<input type="checkbox"/>	500	<=	<input type="checkbox"/>	500	<=	<input type="checkbox"/>	500	<=	<input type="checkbox"/>	500	<=	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
1	<input type="checkbox"/>	500	kbits	<input type="checkbox"/>	500	kbits	<input type="checkbox"/>	500	kbits	<input type="checkbox"/>	500	kbits	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
2	<input checked="" type="checkbox"/>	500	kbits	<input checked="" type="checkbox"/>	500	kbits	<input type="checkbox"/>	500	kbits	<input type="checkbox"/>	500	kbits	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
3	<input checked="" type="checkbox"/>	500	kbits	<input checked="" type="checkbox"/>	500	kbits	<input checked="" type="checkbox"/>	500	kbits	<input type="checkbox"/>	500	kbits	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
4	<input checked="" type="checkbox"/>	500	kbits	<input checked="" type="checkbox"/>	500	kbits	<input type="checkbox"/>	500	kbits	<input checked="" type="checkbox"/>	500	kbits	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
5	<input type="checkbox"/>	500	kbits	<input type="checkbox"/>	500	kbits	<input type="checkbox"/>	500	kbits	<input type="checkbox"/>	500	kbits	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
6	<input type="checkbox"/>	500	kbits	<input type="checkbox"/>	500	kbits	<input type="checkbox"/>	500	kbits	<input type="checkbox"/>	500	kbits	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
7	<input type="checkbox"/>	500	kbits	<input type="checkbox"/>	500	kbits	<input type="checkbox"/>	500	kbits	<input type="checkbox"/>	500	kbits	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
8	<input type="checkbox"/>	500	kbits	<input type="checkbox"/>	500	kbits	<input type="checkbox"/>	500	kbits	<input type="checkbox"/>	500	kbits	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
9	<input type="checkbox"/>	500	kbits	<input type="checkbox"/>	500	kbits	<input type="checkbox"/>	500	kbits	<input type="checkbox"/>	500	kbits	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
10	<input type="checkbox"/>	500	kbits	<input type="checkbox"/>	500	kbits	<input type="checkbox"/>	500	kbits	<input type="checkbox"/>	500	kbits	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

3-26.4 Port Scheduler

This page lets you configure QoS Egress Port Scheduler for all switch ports. To set QoS Port Schedulers in the web UI:

1. Click Configuration, QoS, Port Schedulers.
2. Configure the QoS Egress Port Schedulers parameters and click the Apply button.

Figure 3-26.4: QoS Egress Port Schedules

Parameter descriptions:

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

Mode : Shows the scheduling mode for this port.

Weight (Qn) : Shows the weight for this queue and port.

Scheduler Mode : Controls whether the scheduler mode is "Strict Priority" or "Weighted" on this switch port.

Queue Shaper Enable : Controls whether the queue shaper is enabled for this queue on this switch port.

Queue Shaper Rate : Controls the rate for the queue shaper. The default value is 500. This value is restricted to 100-1000000 when the "Unit" is "kbps", and it is restricted to 1-13200 when the "Unit" is "Mbps".

Queue Shaper Unit : Controls the unit of measure for the queue shaper rate as "kbps" or "Mbps". The default value is "kbps".

Queue Shaper Excess : Controls whether the queue is allowed to use excess bandwidth.

Queue Scheduler Weight : Controls the weight for this queue. The default value is "17". Valid values are 1-100. This parameter is only shown if "Scheduler Mode" is set to "Weighted".

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

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

Port Shaper Rate : Controls the rate for the port shaper. The default value is 500. This value is restricted to 100-1000000 when the "Unit" is "kbps", and it is restricted to 1-13200 when the "Unit" is "Mbps".

Port Shaper Unit : Controls the unit of measure for the port shaper rate as "kbps" or "Mbps". The default value is "kbps".

Buttons:

Apply : Click to save changes.

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

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

Sample QoS Egress Port Scheduler and Shapers for Port 2 Scheduler Mode is set to "6 Queues Weighted"

The screenshot displays the Lantronix web interface for configuring QoS on Port 2. The page title is "QoS Egress Port Scheduler and Shapers Port 2". The "Scheduler Mode" is set to "6 Queues Weighted". The configuration table below shows the settings for each queue and the port shaper.

Queue Shaper	Queue Scheduler	Port Shaper
Enable Rate Unit Excess	Weight Percent	Enable Rate Unit
<input checked="" type="checkbox"/> 500 kbps <input checked="" type="checkbox"/>	17 17%	<input checked="" type="checkbox"/> 500 kbps
<input checked="" type="checkbox"/> 500 kbps <input checked="" type="checkbox"/>	17 17%	
<input checked="" type="checkbox"/> 500 kbps <input checked="" type="checkbox"/>	17 17%	
<input checked="" type="checkbox"/> 500 kbps <input checked="" type="checkbox"/>	17 17%	
<input checked="" type="checkbox"/> 500 kbps <input checked="" type="checkbox"/>	17 17%	
<input checked="" type="checkbox"/> 500 kbps <input checked="" type="checkbox"/>	17 17%	
<input checked="" type="checkbox"/> 500 kbps <input checked="" type="checkbox"/>	17 17%	
<input type="checkbox"/> 500 kbps <input type="checkbox"/>	17 17%	
<input type="checkbox"/> 500 kbps <input type="checkbox"/>	17 17%	

The diagram shows a network topology where traffic from various sources (Q1-Q8) passes through a "D W R R" (Distributed Weighted Round Robin) scheduler and then through a "S T R I C T" (Strict) scheduler before being sent to the port shaper. The port shaper is enabled and set to 500 kbps.

3-26.5 QoS Egress Port Shapers

This page lets you configure QoS Egress Port Shapers table for all switch ports. To set QoS Egress Port Shapers in the web UI:

1. Click Configuration, QoS, Port Shaping.
2. Configure the QoS Egress Port Shaper parameters.
3. Click the Apply button.

The screenshot shows the Lantronix web interface for the SISPM1040-582-LRT device. The main content area is titled "QoS Egress Port Shapers" and contains a table with the following structure:

Port	Shapers									
	Q0	Q1	Q2	Q3	Q4	Q5	Q6	Q7	Port	
1	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled
2	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled
3	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled
4	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled
5	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled
6	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled
7	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled
8	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled
9	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled
10	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled

Figure 3-26.4: QoS Egress Port Shapers

Parameter descriptions:

Port : The logical port for the settings contained in the same row. Click on the linked port number in order to configure the shapers (see below).

Shapers Qn : Shows "-" for disabled or actual queue shaper rate - e.g. "800 Mbps".

Shapers Port : Shows "-" for disabled or actual port shaper rate - e.g. "800 Mbps".

See "Sample QoS Egress Port Scheduler and Shapers" above.

3-26.6 Port Tag Remarking

This page lets you set QoS Egress Port Tag Remarking mode for each port. To set QoS Port Tag Remarking:

1. Click Configuration, QoS, Port Tag Remarking.
2. On the QoS Egress Port Tag Remarking page, click the linked Port number to display its QoS Egress Port Tag Remarking page for the selected Port.
3. Set the QoS Egress Port Tag Remarking page parameters.
4. Click Apply.

The image shows two screenshots of the web interface. The top screenshot shows the 'QoS Egress Port Tag Remarking' page with a table of ports and their modes. Port 2 is highlighted with an orange oval. A red arrow points down to the second screenshot, which shows the 'QoS Egress Port Tag Remarking Port 2' page. This page has a 'Port' dropdown set to 'Port 2' and a 'Tag Remarking Mode' dropdown set to 'Classified'. There are 'Apply' and 'Reset' buttons, and a table of other ports with their modes.

Port	Mode
1	Classified
2	Classified
3	Classified
4	Classified
5	Classified
6	Classified
7	Classified
8	Classified
9	Classified
10	Classified

Port	Mode
4	Classified
5	Classified
6	Classified
7	Classified
8	Classified
9	Classified
10	Classified

Figure 3-26.6: Port Tag Remarking for Port 2. Tag Remarking Mode = Classified

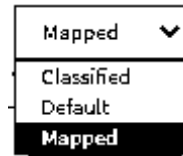
Parameter descriptions:

Mode : Controls the tag remarking mode for this port.

Classified: Use classified PCP/DEI values (default selection).

Default: Use default PCP/DEI values.

Mapped: Use mapped versions of QoS class and DP level.



PCP/DEI Configuration : Controls the default PCP and DEI values used when the mode is set to Default.

(QoS class, DP level) to (PCP, DEI) Mapping : Controls the mapping of the classified (QoS class, DP level) to (PCP, DEI) values when the mode is set to Mapped.

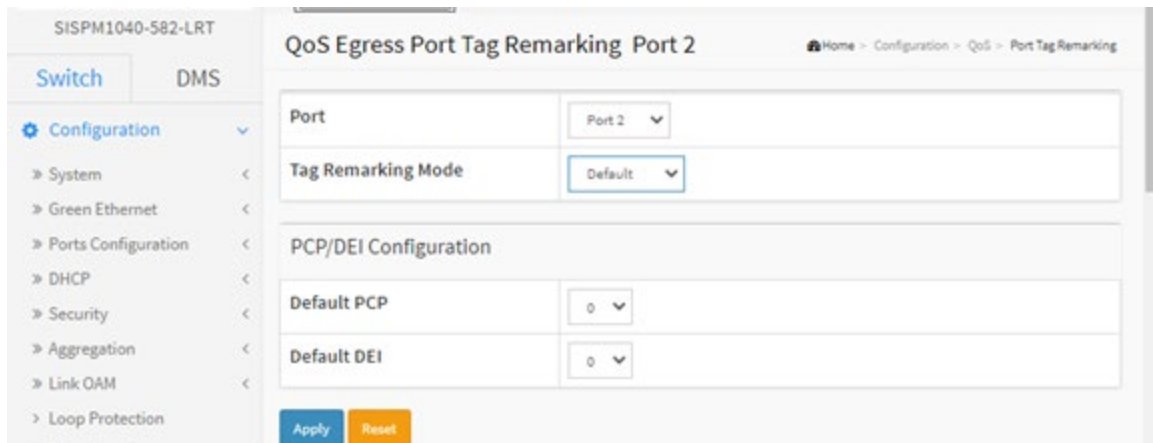
Buttons:

Apply : Click to save changes.

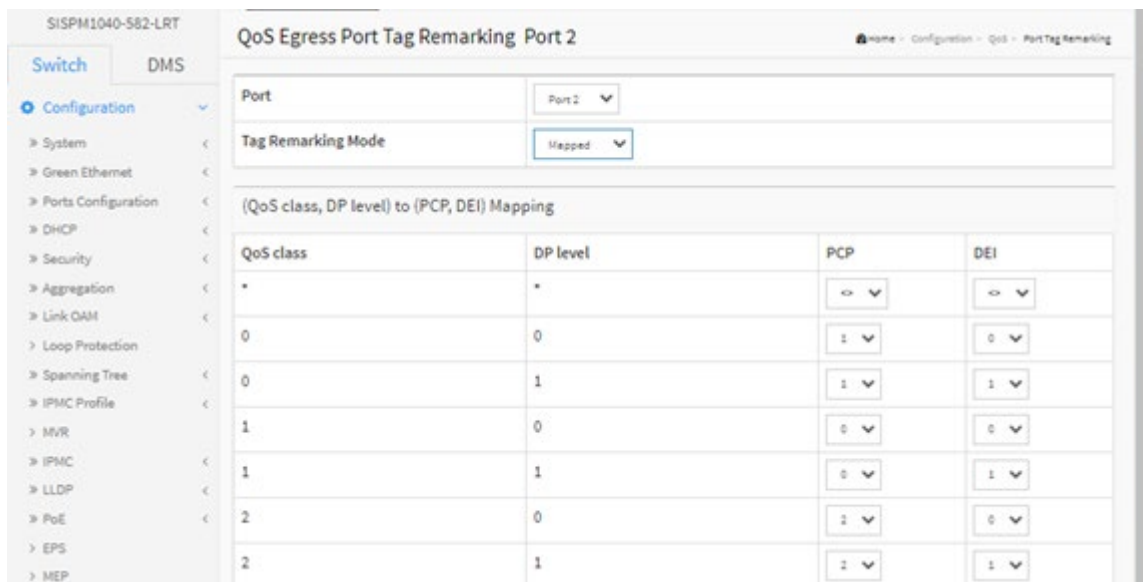
Reset : Click to undo any changes made locally and revert to previously saved values.

Cancel : Click to cancel the changes.

Port Tag Remarking for Port 2. Tag Remarking Mode = Default:



Port Tag Remarking for Port 2. Tag Remarking Mode = Mapped:



3-26.7 Port DSCP

This page lets you configure the basic QoS Port DSCP Configuration settings for all switch ports.

To configure QoS Port DSCP parameters in the web UI:

1. Click Configuration, QoS, Port DSCP.
2. Enable or disable the Ingress Translate and select the Classify parameter settings.
3. Select Egress Rewrite parameters.
4. Click the Apply button to save the settings.
5. To cancel the settings click the Reset button to revert to previously saved values.

The screenshot shows the 'QoS Port DSCP Configuration' page in the Lantronix web UI. The page title is 'QoS Port DSCP Configuration' and the breadcrumb trail is 'Home > Configuration > QoS > Port DSCP'. The left sidebar shows the navigation menu with 'Configuration' selected. The main content area contains a table with the following structure:

Port	Ingress		Egress
	Translate	Classify	Rewrite
*	<input type="checkbox"/>	<> ▾	<> ▾
1	<input type="checkbox"/>	Disable ▾	Disable ▾
2	<input type="checkbox"/>	Disable ▾	Disable ▾
3	<input type="checkbox"/>	Disable ▾	Disable ▾
4	<input type="checkbox"/>	Disable ▾	Disable ▾
5	<input type="checkbox"/>	Disable ▾	Disable ▾
6	<input type="checkbox"/>	Disable ▾	Disable ▾
7	<input type="checkbox"/>	Disable ▾	Disable ▾
8	<input type="checkbox"/>	Disable ▾	Disable ▾
9	<input type="checkbox"/>	Disable ▾	Disable ▾
10	<input type="checkbox"/>	Disable ▾	Disable ▾

At the bottom of the table, there are two buttons: 'Apply' (blue) and 'Reset' (orange).

Figure 3-26.7: QoS Port DSCP Configuration

Parameter descriptions:

Port : The Port column shows the list of ports for which you can configure DSCP ingress and egress settings.

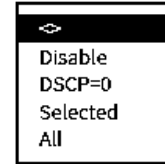
Ingress : In Ingress settings you can change ingress translation and classification settings for individual ports. There are two configuration parameters available in Ingress:

Translate : To enable Ingress Translation click the checkbox.

Classify: Classification for a port can have one of four 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.

Classify



Egress : Port Egress Rewriting can be one of these parameters:

Disable: No Egress rewrite.

Enable: Rewrite enable without remapped.

Remap: DSCP from analyzer is remapped and frame is remarked with remapped DSCP value.

Buttons:

Apply : Click to save changes.

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

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

Refresh : Click to immediately refresh the information manually.

3-26.8 DSCP-Based QoS

This page lets you configure the DSCP-Based QoS Ingress Classification settings. To set DSCP –Based QoS Ingress Classification parameters in the web UI:

1. Click Configuration, QoS, DSCP-Based QoS.
2. Enable or disable the DSCP for Trust.
3. Select QoS Class and DPL parameters.
4. Click the Apply button to save the settings.
5. To cancel the settings click the Reset button to revert to previously saved values.

DSCP	Trust	QoS Class	DPL
*	<input type="checkbox"/>	<>	<>
0 (BE)	<input type="checkbox"/>	0	0
1	<input type="checkbox"/>	0	0
2	<input type="checkbox"/>	0	0
3	<input type="checkbox"/>	0	0
4	<input type="checkbox"/>	0	0
5	<input type="checkbox"/>	0	0
6	<input type="checkbox"/>	0	0
7	<input type="checkbox"/>	0	0
8 (CS1)	<input type="checkbox"/>	0	0
9	<input type="checkbox"/>	0	0
10 (AF11)	<input type="checkbox"/>	0	0
11	<input type="checkbox"/>	0	0
12 (AF12)	<input type="checkbox"/>	0	0

Figure 3-26.8: DSCP-Based QoS Ingress Classification

Parameter descriptions:

DSCP : Maximum number of supported DSCP values are 64.

Trust : Click to check if the DSCP value is trusted.

QoS Class : QoS Class value can be 0-7. Every incoming frame is classified to a QoS class, which 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. There is a one to one mapping between QoS class, queue and priority. A QoS class of 0 (zero) has the lowest priority.

DPL : Drop Precedence Level (0-3). Every incoming frame is classified to a Drop Precedence Level (DP level), which is used throughout the device for providing congestion control guarantees to the frame according to what was configured for that specific DP level. A DP level of 0 (zero) corresponds to 'Committed' (Green) frames and a DP level of 1 corresponds to 'Discard Eligible' (Yellow) frames.

Buttons:

Apply : Click to save changes.

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

3-26.9 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 set DSCP Translation parameters in the web UI:

1. Click Configuration, QoS, DSCP Translation.
2. Set the Ingress Translate and Egress Remap DP0 and Remap DP1 Parameters.
3. Enable or disable Classify.
4. Click the Apply button to save the settings.
5. To cancel the settings click the Reset button to revert to previously saved values.

DSCP	Ingress		Egress	
	Translate	Classify	Remap DP0	Remap DP1
*	<>	<input type="checkbox"/>	<>	<>
0 (BE)	0 (BE)	<input type="checkbox"/>	0 (BE)	0 (BE)
1	1	<input type="checkbox"/>	1	1
2	2	<input type="checkbox"/>	2	2
3	3	<input type="checkbox"/>	3	3
4	4	<input type="checkbox"/>	4	4
5	5	<input type="checkbox"/>	5	5
6	6	<input type="checkbox"/>	6	6
7	7	<input type="checkbox"/>	7	7
8 (CS1)	8 (CS1)	<input type="checkbox"/>	8 (CS1)	8 (CS1)
9	9	<input type="checkbox"/>	9	9
10 (AF11)	10 (AF11)	<input type="checkbox"/>	10 (AF11)	10 (AF11)
11	11	<input type="checkbox"/>	11	11
12 (AF12)	12 (AF12)	<input type="checkbox"/>	12 (AF12)	12 (AF12)

Figure 3-26.9: DSCP Translation Configuration

Parameter descriptions:

DSCP : The maximum number of supported DSCP values are 64 and valid DSCP value ranges from 0 to 63.

Ingress : Ingress side DSCP can be first translated to new DSCP before using the DSCP for QoS class and DPL map.

There are two configuration parameters for DSCP Translation:

Translate : DSCP at Ingress side can be translated to any of (0-63) DSCP values.

Classify : Click to enable Classification at Ingress side.

Egress : There are following configurable parameters for Egress side:

Remap DP0 : Select the DSCP value from select menu to which you want to remap. DSCP value ranges from 0 to 63.

Remap DP1 : Select the DSCP value from select menu to which you want to remap. DSCP value ranges from 0 to 63.

The following configurable parameter is for the Egress side:

Remap: Select the DSCP value from select menu to which you want to remap. DSCP value ranges from 0 to 63.

Buttons:

Apply : Click to save changes.

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

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

Refresh: Click to immediately refresh the DSCP Translation information manually.

3-26.10 DSCP Classification

This page lets you configure the mapping of QoS class and Drop Precedence Level to DSCP value. To configure DSCP Classification parameters in the web UI:

1. Click Configuration, QoS, DSCP Classification.
2. Set the DSCP parameters.
3. Click the Apply button to save the settings. To cancel the settings click the Reset button to revert to previously saved values.

QoS Class	DSCP DP0	DSCP DP1
*	<>	<>
0	0 (BE)	0 (BE)
1	0 (BE)	0 (BE)
2	0 (BE)	0 (BE)
3	0 (BE)	0 (BE)
4	0 (BE)	0 (BE)
5	0 (BE)	0 (BE)
6	0 (BE)	0 (BE)
7	0 (BE)	0 (BE)

Figure 3-26.10: DSCP Classification Configuration

Parameter descriptions:

QoS Class : The actual QoS class in the range of 0 to 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.


Buttons:

Apply : Click to save changes.

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

3-26.11 QoS Control List

This page displays the QoS Control List (QCL), which is made up of QCEs. Each row 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. Click Configuration, QoS, QoS Control List.
2. Click the  icon to add a new QoS Control List.
3. Set all parameters and the Port Members to join the QCE rules.
4. Click the Apply button to save the settings. To cancel the settings click the Reset button

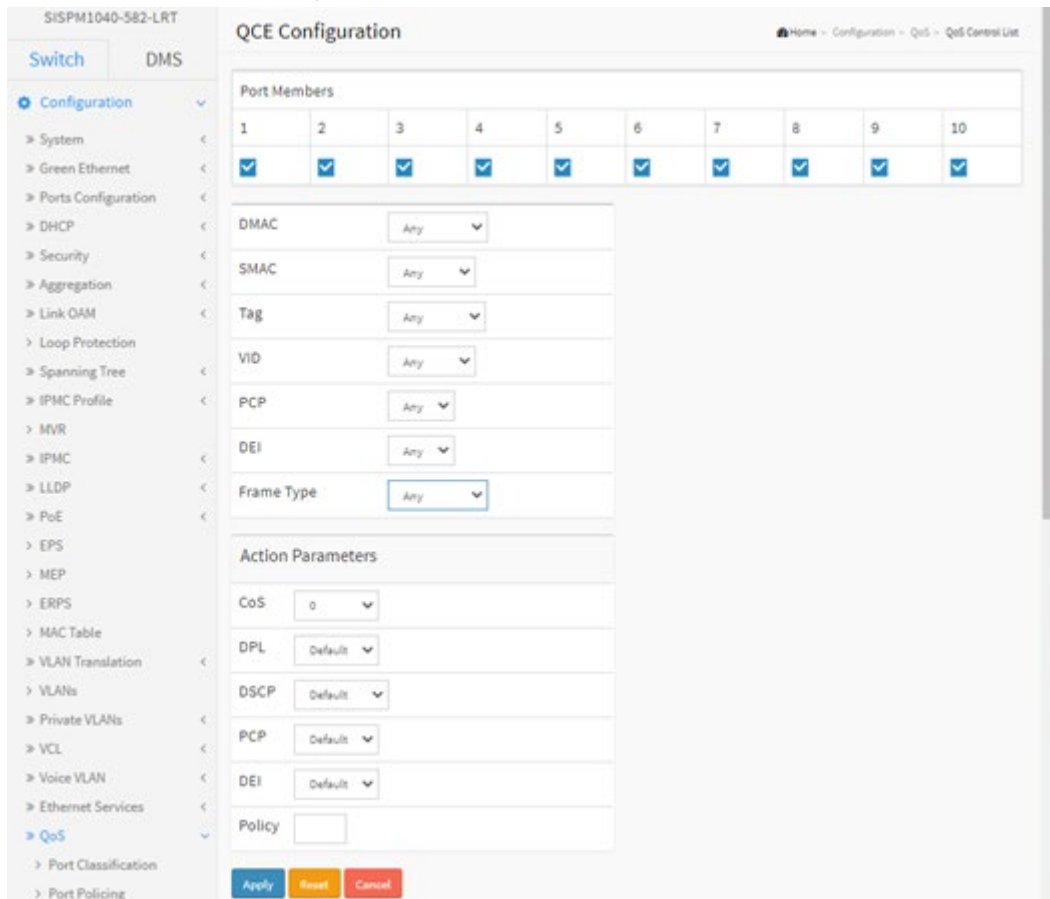
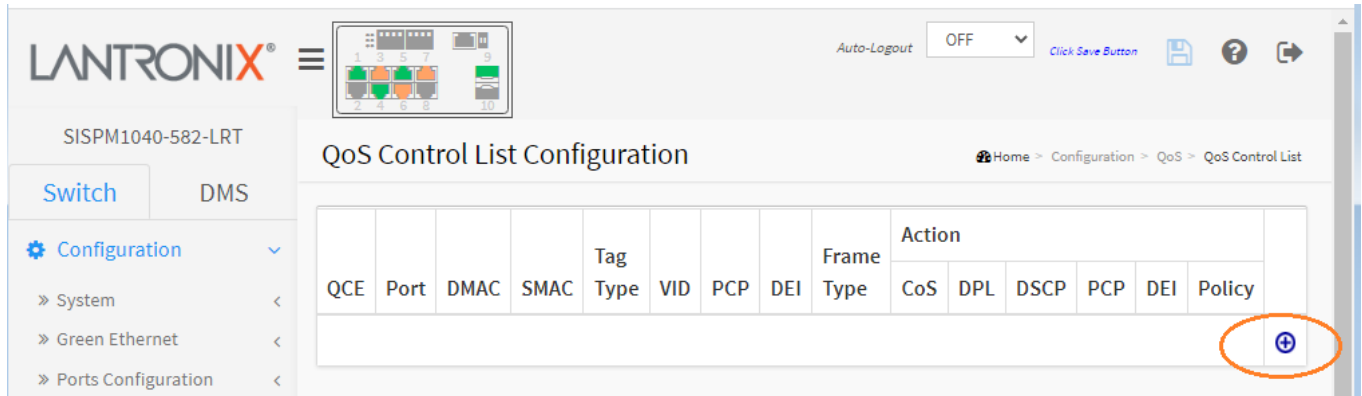


Figure 3-26.11: QoS Control List Configuration (Frame Type = Any)

Parameter descriptions:

QCE : Indicates the index of QCE.

Port : Indicates the list of ports configured with the QCE.

DMAC : Indicates the destination MAC address. Possible values are:

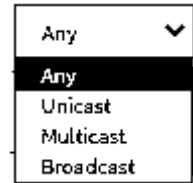
Any: Match any DMAC. The default value is 'Any'.

Unicast: Match unicast DMAC.

Multicast: Match multicast DMAC.

Broadcast: Match broadcast DMAC.

<MAC>: Match specific DMAC.



SMAC : Match specific source MAC address or 'Any'. If a port is configured to match on DMAC/DIP, this field indicates the DMAC.

Tag: Select tag type. Possible values are:

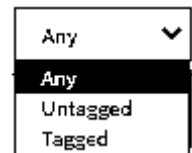
Any: Match tagged and untagged frames. The default value is 'Any'.

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 are specific (0, 1, 2, 3, 4, 5, 6, 7) or range (0-1, 2-3, 4-5, 6-7, 0-3, 4-7) or 'Any'.

DEI : Drop Eligible Indicator: Valid value of DEI are 0, 1 or 'Any'.

Frame Type : Indicates the type of frame to look for incoming frames. Possible frame types are:

Any: The QCE will match all frame type.

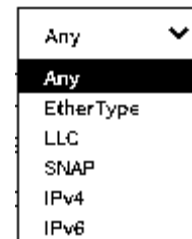
EtherType: Only Ethernet frames (with Ether Type 0x600-0xFFFF) are allowed.

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.



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, and **Policy**: Classify ACL Policy number.

Modification 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 in case you want to make any port member of the QCL entry. By default all ports will be checked.

Key Parameters : Key configuration are described as below:

Tag Value of Tag field can 'Any', 'Untag' or 'Tag'.

VID Valid value of VLAN ID can be any value in the range 1-4095 or 'Any'. You can enter either a specific value or a range of VIDs

PCP Priority Code Point: 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 Drop Eligible Indicator: Valid value of DEI can be any of values between 0, 1 or 'Any'.

SMAC Source MAC address: 24 MS bits (OUI) or 'Any'.

DMAC Type Destination MAC type: possible values are unicast (UC), multicast (MC), broadcast (BC) or 'Any'.

Frame Type : Frame Type can be Any, Ethernet, LLC, SNAP, IPv4, or IPv6. This selection determines what additional parameters are displayed. The frame types are explained below:

Any: Allow all types of frames.

EtherType: Ethernet Type Valid Ethernet type can have value within 0x600-0xFFFF or 'Any', default value is 'Any'.

LLC: SSAP Address Valid SSAP (Source Service Access Point) can vary from 0x00 to 0xFF or 'Any', the default value is 'Any'. DSAP Address Valid DSAP (Destination Service Access Point) can vary from 0x00 to 0xFF or 'Any', the default value is 'Any'. Control Address Valid Control Address can vary from 0x00 to 0xFF or 'Any', the default value is 'Any'.

SNAP : PID Valid PID(a.k.a Ethernet type) can have value within 0x00-0xFFFF or 'Any', default value is 'Any'

IPv4: Protocol IP protocol number: (0-255, TCP or UDP) or 'Any' Source IP Specific Source IP address in value/mask format or 'Any'. IP and Mask are in the format x.y.z.w where x, y, z, and w are decimal numbers between 0 and 255. When Mask is converted to a 32-bit binary string and read from left to right, all bits following the first zero must also be zero. DSCP Diffserv Code Point value (DSCP): It can be specific value, range of value or 'Any'. DSCP values are in the range 0-63 including BE, CS1-CS7, EF or AF11-AF43.

IP Fragment IPv4 frame fragmented option: yes|no|any

Sport Source TCP/UDP port:(0-65535) or 'Any', specific or port range applicable for IP protocol UDP/TCP

Dport Destination TCP/UDP port:(0-65535) or 'Any', specific or port range applicable for IP protocol UDP/TCP

IPv6 :Protocol IP protocol number: (0-255, TCP or UDP) or 'Any'.

Source IP IPv6 source address: (a.b.c.d) or 'Any', 32 LS bits.

DSCP Diffserv Code Point value (DSCP): It can be specific value, range of value or 'Any'. DSCP values are in the range 0-63 including BE, CS1-CS7, EF or AF11-AF43.

Sport Source TCP/UDP port:(0-65535) or 'Any', specific or port range applicable for IP protocol UDP/TCP.

Dport Destination TCP/UDP port:(0-65535) or 'Any', specific or port range applicable for IP protocol UDP/TCP.

Action Parameters:

CoS: Select a Class of Service (0-7) or 'Default'.

DPL: Select a Drop Precedence Level (0-1) or 'Default'.

DSCP: Select DSCP (0-63, BE, CS1-CS7, EF or AF11-AF43) or 'Default'.

PCP: Select PCP (0-7) or 'Default'. Note: PCP and DEI cannot be set individually.

DEI: Select DEI (0-1) or 'Default'.

Policy: Enter an ACL Policy number (0-255) or 'Default' (empty field).

Note: 'Default' means that the default classified value is not modified by this QCE.

EtherType Parameters:

Ether Type: Select **Any** or **Specific**. Valid Ether Type can be 0x600-0xFFFF excluding 0x800(IPv4) and 0x86DD(IPv6) or 'Any'.

Value: 0x: Enter a value (only if Specific was selected as Ether Type above). The default is FFFF.

LLC Parameters:

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 Parameters:

PID Valid PID (a.k.a Ether Type) can be 0x0000-0xFFFF or 'Any'.

IPv4 Parameters:

Protocol: IP protocol number: ('TCP' or 'UDP' or 'Any').

SIP: 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. If a port is configured to match on DMAC/DIP, this field is the Destination IP address.

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 Parameters:

Protocol: IP protocol: 'TCP' or 'UDP' or 'Any'.

SIP: Source IP 32 LS bits of IPv6 source address in value/mask format or 'Any'. If a port is configured to match on DMAC/DIP, this field is the Destination IP address.

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.

Buttons:

Apply : Click to save changes.

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

Cancel : Return to the previous page without saving the configuration change.

Example

The sample QoS Control List Configuration table below has three QCEs configured. You can monitor QCL Status at

Monitor > Ports > QCL Status.

QCE	Port	DMAC	SMAC	Tag Type	VID	PCP	DEI	Frame Type	Action							
									CoS	DPL	DSCP	PCP	DEI	Policy		
1	Any	Broadcast	Any	Tagged	Any	Any	Any	EtherType	0	Default	Default	Default	Default	Default	Default	⊕ ⊖ ↻
2	Any	Broadcast	Any	Any	Any	2	0	IPv4	0	Default	Default	Default	Default	Default	Default	⊕ ⊖ ↻
3	Any	Any	Any	Any	Any	Any	Any	Any	0	Default	Default	Default	Default	Default	Default	⊕ ⊖ ↻
																⊕

Figure 3-26.11: QoS Control List Configuration

3-26.12 Storm Control

This page lets you configure the Storm control for the switch. There is a unicast storm rate control, multicast storm rate control, and a broadcast storm rate control. These only affect flooded frames, i.e., frames with a (VLAN ID, DMAC) pair not present on the MAC Address table. The configuration indicates the permitted packet rate for unicast, multicast or broadcast traffic across the switch.

To configure Storm Control parameters in the web UI:

1. Click Configuration, QoS, Storm Control.
2. Select the frame type to enable storm control.
3. Set the Rate and Unit parameters.
4. Click the Apply button to save the settings.
5. To cancel the settings click the Reset button.

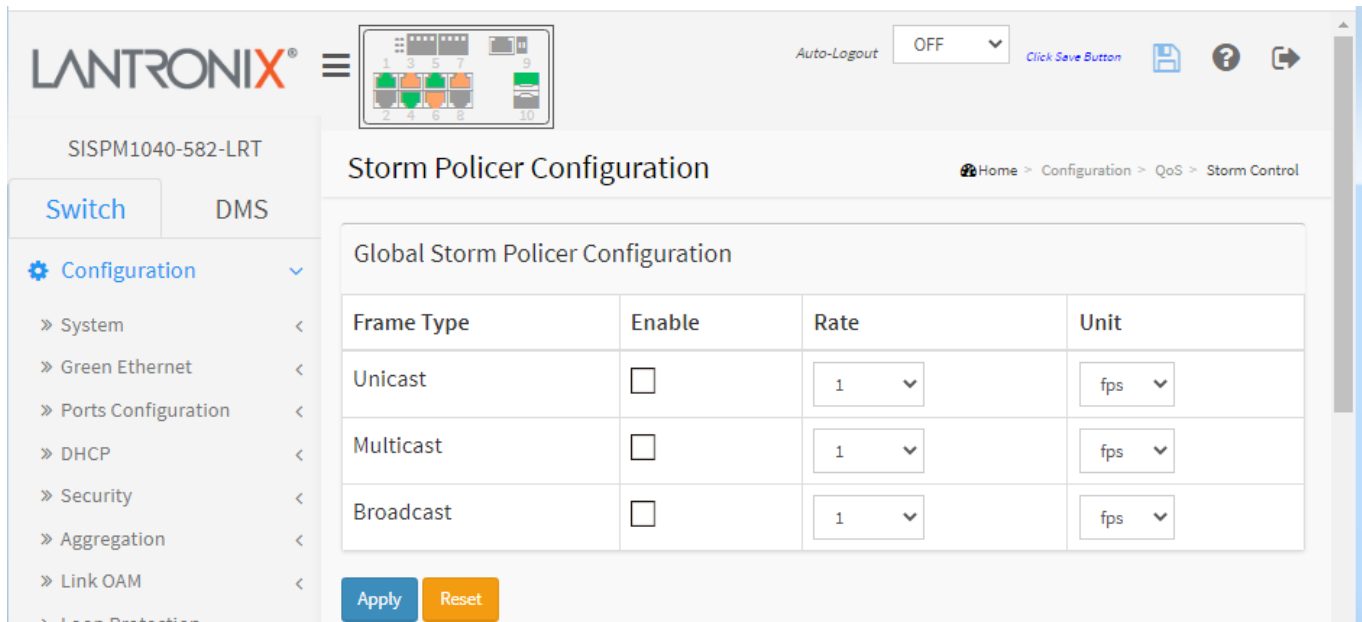


Figure 3-26.12: Global Storm Policer Configuration

Frame Type : The settings in a particular row apply to a frame type set here: Unicast, Multicast or Broadcast.

Enable : Enable or disable the storm control status for the given frame type.

Rate : Controls the rate for the global storm policer. This value can be 1-1024000 when "Unit" is fps, and 1-1024 when "Unit" is kfps. The rate is internally rounded up to the nearest value supported by the global storm policer. Valid values are: 1, 2, 4, 8, 16, 32, 64, 128, 256, 512, 1K, 2K, 4K, 8K, 16k, 32k, 64k, 128k, 256K, 512K or 1024K.

Buttons:

Apply : Click to save changes.

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

Messages: *Invalid 1024 or 1000000*

'Rate' must be an integer value between 1 and 1024 kfps.

3-27 Mirroring

Mirroring is a feature for use with a switched port analyzer. The administrator can use Mirroring to debug network problems. The selected traffic can be mirrored or copied on a destination port where a network analyzer can be attached to analyze the network traffic. Remote Mirroring is an extended function of Mirroring. It can extend the destination port in another switch, so the administrator can analyze the network traffic on the other switches.

To get tagged mirrored traffic, you must set VLAN egress tagging as "Tag All" on the reflector port.
 To get untagged mirrored traffic, you must set VLAN egress tagging as "Untag ALL" on the reflector port.

To configure mirroring in the web UI:

1. Click Configuration, Mirroring.
2. Set Stack Global Settings parameters.
3. Specify source VLANs.
4. Select Port to mirror on which port.
5. Set the Port mirror mode and click the Apply button to save the settings.

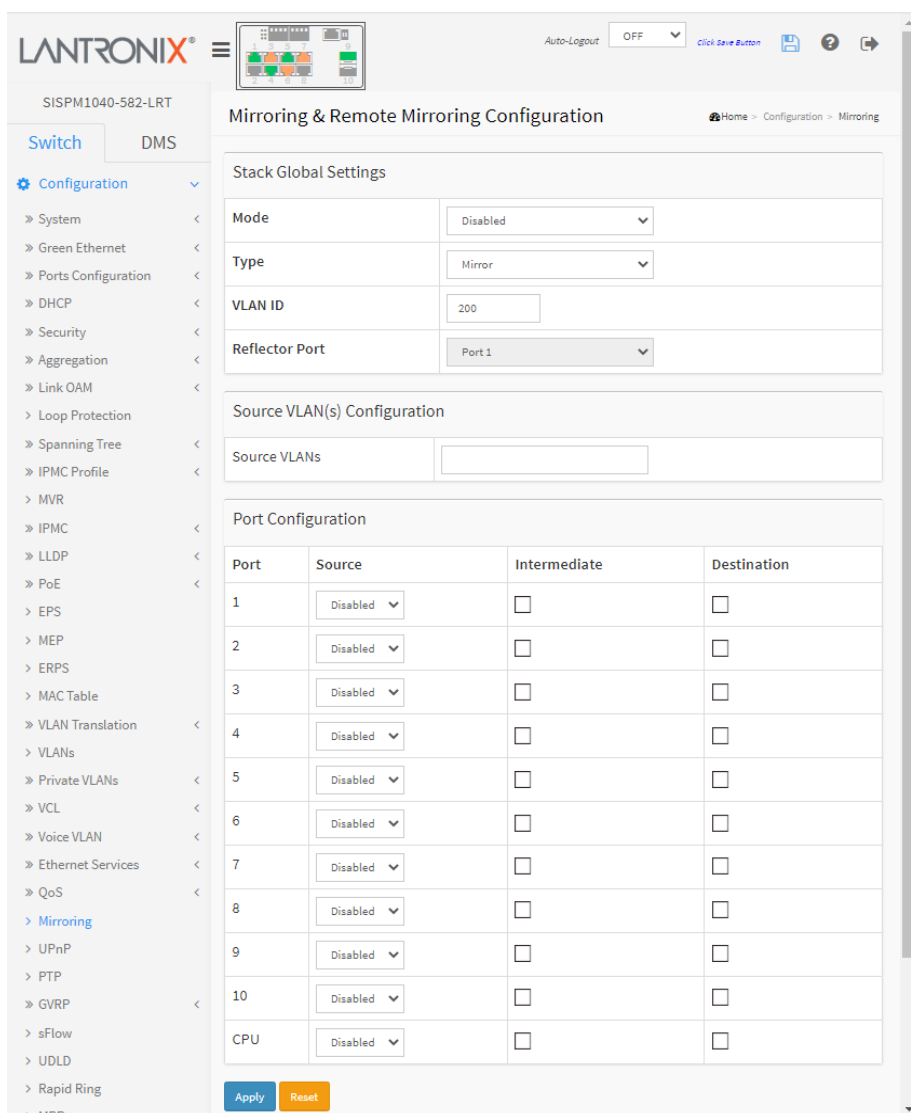


Figure 3-27: Mirroring & Remote Mirroring Configuration

Stack Global Settings:

Mode : Select Enabled or Disabled for the mirror or Remote Mirroring function.

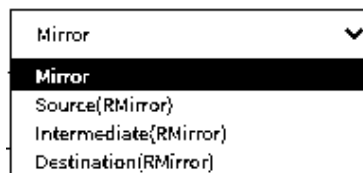
Type : Select a switch type.

Mirror : The switch is running on mirror mode. The source port(s) and destination port are located on this switch.

Source(RMirror) : The switch is a source node for monitor flow. The source port(s), reflector port and intermediate port(s) are located on this switch.

Intermediate(RMirror) : The switch is a forwarding node for monitor flow and the switch is an option node. The object is to forward traffic from source switch to destination switch. The intermediate ports are located on this switch.

Destination(RMirror) : The switch is an end node for monitor flow. The destination port(s) and intermediate port(s) are located on this switch.



VLAN ID : The VLAN ID points out where the monitor packet will copy to. The default VLAN ID is 200.

Reflector Port : The reflector port is a method to redirect the traffic to Remote Mirroring VLAN. Any device connected to a port set as a reflector port loses connectivity until the Remote Mirroring is disabled.

If you shut down a port, it cannot be a candidate for reflector port.

If you shut down the port which is a reflector port, the remote mirror function cannot work.

Note 1: The reflector port needs to select only on Source switch type.

Note 2: The reflector port needs to disable MAC Table learning and STP.

Note 3: The reflector port only supports on pure copper ports.

Source VLAN(s) Configuration : The switch supports VLAN-based Mirroring. To monitor some VLANs on the switch, you can set the selected VLANs on this field.

Note 1: The Mirroring session can have either ports or VLANs as sources, but not both.

Port Configuration : The following table is used for port role selecting.

Port : The logical port for the settings contained in the same row (1-10 and CPU).

Source : Select mirror mode.

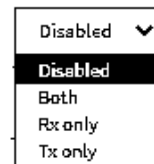
Disabled: Neither frames transmitted nor frames received are mirrored.

Both: Frames received and frames transmitted are mirrored on the Intermediate/Destination port.

Rx only: Frames received on this port are mirrored on the Intermediate/Destination port. Frames transmitted are not mirrored.

Tx only: Frames transmitted on this port are mirrored on the Intermediate/Destination port. Frames received are not mirrored.

Source



Intermediate : Select intermediate port. This checkbox is designed for Remote Mirroring. The Intermediate port is a switched port to connect to another switch. **Note:** The intermediate port must have MAC Table learning disabled.

Destination : Select destination port. This checkbox is designed for mirror or Remote Mirroring. The destination port is a switched port that receives a copy of traffic from the source port.

Note 1: In mirror mode, the device only supports one destination port.

Note 2: The destination port needs to disable MAC Table learning.

Configuration Guideline for All Features

When the switch is running in Remote Mirroring mode, the administrator also needs to check whether or not other features are enabled or disabled. For example, the administrator is not disabled the MSTP on reflector port. All monitor traffic will be blocked on reflector port. All recommended settings are as follows.

	Impact	Source port	Reflector port	Intermediate port	Destination port	Remote Mirroring VLAN
arp_inspection	High		* disabled	* disabled		
acl	Critical		* disabled	* disabled	* disabled	
dhcp_relay	High		* disabled	* disabled		
dhcp_snooping	High		* disabled	* disabled		
ip_source_guard	Critical		* disabled	* disabled	* disabled	
ipmc/igmpsnp	Critical					un-conflict
ipmc/mldsnp	Critical					un-conflict
lACP	Low				o disabled	
lldp	Low				o disabled	
mac learning	Critical		* disabled	* disabled	* disabled	
mstp	Critical		* disabled		o disabled	
mvr	Critical					un-conflict
nas	Critical		* authorized	* authorized	* authorized	
psec	Critical		* disabled	* disabled	* disabled	
qos	Critical		* unlimited	* unlimited	* unlimited	
upnp	Low				o disabled	
mac-based vlan	Critical		* disabled	* disabled		
protocol-based vlan	Critical		* disabled	* disabled		
vlan_translation	Critical		* disabled	* disabled	* disabled	
voice_vlan	Critical		* disabled	* disabled		
mrp	Low				o disabled	
mvrp	Low				o disabled	
Note:						
* -- must						
o -- optional						
Impact: Critical/High/Low:						
Critical	5 packets -> 0 packet					

High	5 packets -> 4 packets				
Low	5 packets -> 6 packets				

Buttons:

Apply : Click to save changes.

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

3-28 UPnP

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

To configure UPnP parameters in the web UI:

1. Click Configuration, UPnP.
2. Select the mode (enabled or disabled).
3. Specify the parameters in each blank field.
4. Click the Apply button to save the settings. To cancel the settings click the Reset button.

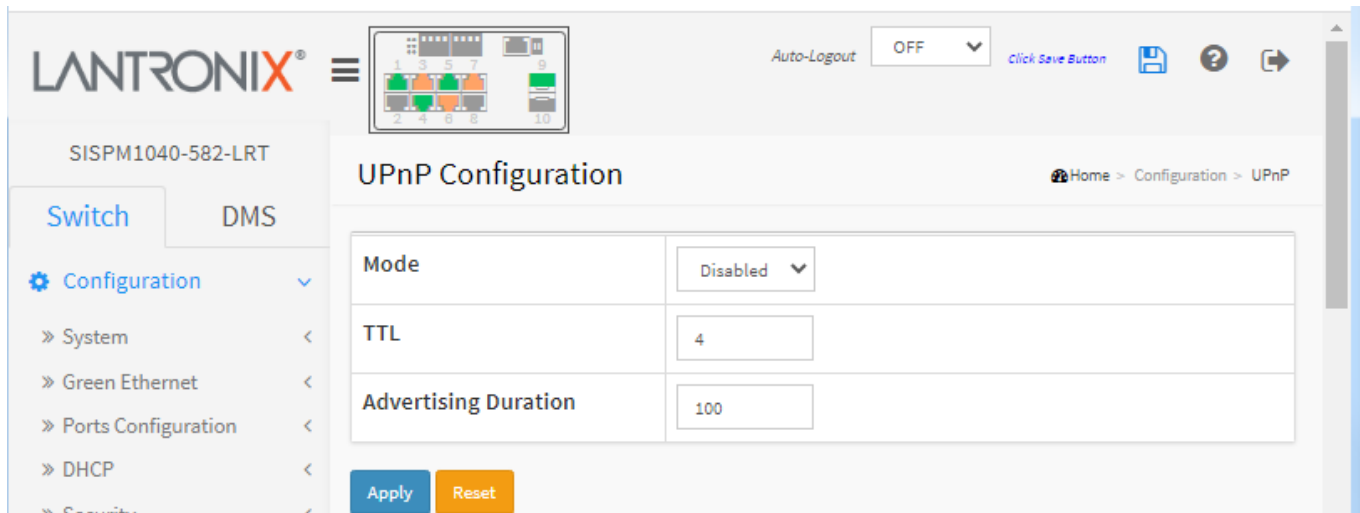


Figure 3-28: UPnP Configuration

Parameter descriptions:

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

Enabled: Enable UPnP mode operation.

Disabled: Disable UPnP mode operation.

When Mode is Enabled, two ACEs are added automatically to trap UPnP related packets to CPU. The ACEs are automatically removed when Mode is Disabled.

TTL : The TTL value is 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, in the standard it is recommended that such refreshing of advertisements to be done at less than one-half of the advertising duration. In the implementation, the switch sends SSDP messages periodically at the interval one-half of the advertising duration minus 30 seconds. Valid values are 100-86400 seconds.

Buttons:

Apply : Click to save changes.

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

3-29 PTP

This page lets you create up to four clock instances and configure PTP clock settings. PTP (Precision Time Protocol) is a network protocol for synchronizing the clocks of computer systems.

To configure PTP in the web UI:

1. Click Configuration, PTP.
2. Click the Add New PTP Clock button to create a new clock instance.
3. Select the PTP External Clock Mode section parameters.
4. Set the PTP Clock Configuration section parameters.
5. Click the Apply button to save the settings. To cancel the settings click the Reset button.

Figure 3-29: PTP Configuration

Parameter descriptions:

PTP External Clock Mode

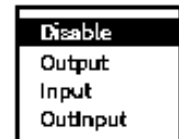
One_PPS_Mode : Selection box to select the One_pps_mode configuration. These values are possible:

Disable : Disable the 1 pps clock input and output.

Output : Enable the 1 pps clock output.

Input : Enable the 1 pps clock input.

Outinput : Enable the 1 pps clock input and output.



External Enable : This selection box will allow you to configure the External Clock output. Valid values are:

True : Enable the external clock output.

False : Disable the external clock output.

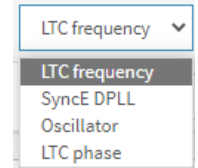
Adjust Method : This Selection box will allow you to configure the Frequency adjustment configuration.

LTC frequency : Select Local Time Counter (LTC) frequency control.

SyncE DPLL : Select SyncE Digital Phase Locked Loop frequency control, if allowed by SyncE.

Oscillator : Select an oscillator independent of SyncE for frequency control, if supported by the HW.

LTC phase : Select Local Time Counter (LTC) phase control (assumes that the frequency is locked by means of SyncE).



Clock Frequency : Set the Clock Frequency. Possible values are 1 - 25000000 (1 - 25MHz).

PTP Clock Configuration

Delete : Check this box and click on 'Save' to delete the clock instance.

Inst : Indicates the Instance of a particular Clock Instance [0..3]. Click on the Clock Instance number to edit the Clock details.

ClkDom : Indicates the Clock domain used by the Instance of a particular Clock Instance [0..3]. More instances may use the same clock domain, e.g. a Boundary clock and a Transparent clock. Only one Slave or Boundary clock is allowed within the same Clock domain.

Device Type : Indicates the Type of the Clock Instance. There are seven Device Types.

Inactive : no active clock configured.

Ord-Bound : clock's Device Type is Ordinary-Boundary Clock.

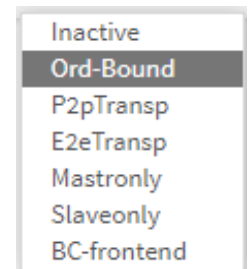
P2p Transp : clock's Device Type is Peer to Peer Transparent Clock.

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 : A boundary clock has one port in slave state, getting time from a master clock. All other ports are in master state which disseminate time to downstream slaves.



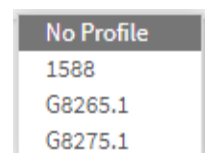
Profile : Select a profile from the dropdown:

No Profile : Do not use any profile.

1588 : Use the IEEE 1588™ Precision Time Protocol (PTP) standard profile.

G.8265.1 : Use the ITU-T G.8265.1 (ITU Telecommunications Standardization Sector) defines the "Precision time protocol telecom profile for frequency synchronization" [2]. It defines the options and attributes from IEEE 1588 to be used to deliver frequency synchronization to the end application.

G.8275.1 : Use the ITU-T G.8275.1 Precision time protocol telecom profile for phase/time synchronization with full timing support from the network.



Port List : Set check mark for each port configured for this Clock Instance. One port can only be active within one Clock domain. I.e. enabling a port which is already active in another Clock domain is rejected.

2 Step Flag : Static member: defined by the system, true if two-step Sync events and Pdelay_Resp events are used.

Clock Identity : Shows unique clock identifier.

One Way : If true, one-way measurements are used. This parameter applies only to a slave. In one-way mode no delay measurements are performed, i.e. this is applicable only if frequency synchronization is needed. The master always responds to delay requests.

Protocol : Transport protocol used by the PTP protocol engine:

Ethernet : PTP over Ethernet multicast

EthernetMixed : PTP using a combination of Ethernet multicast and unicast

IPv4Multi : PTP over IPv4 multicast

IPv4Mixed : PTP using a combination of IPv4 multicast and unicast

IPv4Uni : PTP over IPv4 unicast

Note : IPv4 unicast protocol only works in Master only and Slave only clocks. See parameter Device Type. In a unicast Slave only clock you also need configure which master clocks to request Announce and Sync messages from. See Unicast Slave Configuration.

VLAN Tag Enable : Enables the VLAN tagging for the PTP frames. **Note**: Packets are only tagged if the port is configured for VLAN tagging for the configured VLAN (i.e., the VLAN Tag Enable parameter is ignored).

VID : VLAN Identifier used for tagging the PTP frames.

PCP : Priority Code Point value used for PTP frames.

Buttons:

Add New PTP Clock : Click to create a new clock instance. See the Parameter descriptions below.

Apply : Click to save the page immediately.

Reset : Click to reset the page immediately.

When you click the linked **Clock Instance** number, the PTP Clock's Configuration and Status page displays. This page lets you view and configure the current PTP Clock's Configuration and Status settings.

The screenshot displays the 'PTP Clock's Configuration' page. The left sidebar shows navigation options like Configuration, Monitor, System, Green Ethernet, Ports, Link OAM, DHCP, Security, Aggregation, Loop Protection, Spanning Tree, MVR, IPAC, LLDP, Ethernet Services, PTP, PoE, MAC Table, VLANs, MRP, VCL, sFlow, UOLD, Diagnostics, and Maintenance. The main content area includes:

- Auto-refresh** button and **Refresh** button.
- Local Clock Current Time** section.
- PTP Time** table:

PTP Time	Clock Adjustment method	Ports Monitor Page
1970-01-01T21:55:53-00:00 623,585,700	Software	Ports Monitor
- Clock Default Data Set** table:

Clock ID	Device Type	2 Step Flag	Ports	Clock Identity	Dom	Clock Quality	Pri1	Pri2	Protocol	One-Way	VLAN Tag Enable	VID	PCP	DSCP
1	Ord-Bound	False	10	00:c0:f2:ff:fe:4f:73:d1	0	Cl:251 Acc:Unknwn Va:65535	128	128	Ethernet	False	False	1	0	0
- Clock Current Data Set** table:

stpRm	Offset From Master	Mean Path Delay	Slave Port	Slave State	Holdover(ppb)
0	0,000,000,000	0,000,000,000	0	FREERUN	N.A.
- Clock Parent Data Set** table:

Parent Port ID	Port	PStat	Var	ChangeRate	GrandMaster Identity	GrandMaster Clock Quality	Pri1	Pri2
00:c0:f2:ff:fe:4f:73:d1	0	False	0	0	00:c0:f2:ff:fe:4f:73:d1	Cl:251 Acc:Unknwn Va:65535	128	128
- Clock Time Properties Data Set** table:

UtcOffset	Valid	leap59	leap61	Time Trac	Freq Trac	PTP Time Scale	Time Source
0	False	False	False	False	False	True	160
- Servo Parameters** table:

Display	P-enable	I-enable	D-enable	'P' constant	'I' constant	'D' constant
False	True	True	True	3	80	40
- Filter Parameters** table:

Filter Type	DelayFilter	Period	Dist
Basic	6	1	2
- Unicast Slave Configuration** table:

Index	Duration	IP_Address	Grant	CommState
0	100	0.0.0.0	0	IDLE
1	100	0.0.0.0	0	IDLE
2	100	0.0.0.0	0	IDLE

Parameter descriptions:

Clock Type and Profile :

Clock Instance : The clock instance number (e.g., 0).

Device Type : The clock instance device type (e.g., Mastronly).

Profile : The clock instance profile assigned (e.g., 1588)

Apply Profile Defaults : Click the **Apply** button to save the section settings.

Port Enable and Configuration :

Port Enable : Check the desired port checkbox(es).

Configuration : Click the linked text [Ports Configuration](#) to display the PTP Clock's Port Data Set Configuration page.

Local Clock Current time : Show/update local clock data

PTP Time : Shows the actual PTP time with nanosecond resolution.

Clock Adjustment Method : Shows the actual clock adjustment method. The method depends on the available hardware.

Synchronize to System Clock : Click this button to synchronize the System Clock to PTP Time.

Ports Configuration : Click to edit the port data set for the ports assigned to this clock instance.

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 ID : An internal instance id (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.

2 Step Flag : True if two-step Sync events and Pdelay_Resp events are used.

Ports : The total number of physical ports in the node.

Clock Identity : It shows unique clock identifier.

Dom : Clock domain [0..127].

Clock Quality : The clock quality is determined by the system, and holds 3 parts: Clock Class, Clock Accuracy, and OffsetScaledLog Variance as defined in IEEE1588. The Clock Accuracy values are defined in IEEE1588 table 6 (Currently the clock Accuracy is set to 'Unknown' as default).

Pri1 : Clock priority 1 [0..255] used by the BMC master select algorithm.

Pri2 : Clock priority 2 [0..255] used by the BMC master select algorithm.

Protocol : Transport protocol used by the PTP protocol engine:

Ethernet : PTP over Ethernet multicast.

EthernetMixed : PTP using a combination of Ethernet multicast and unicast.

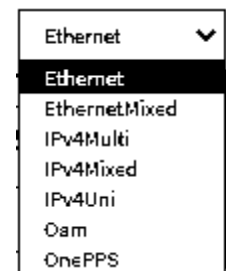
IPv4Multi : PTP over IPv4 multicast.

IPv4Mixed : PTP using a combination of IPv4 multicast and unicast.

IPv4Uni : PTP over IPv4 unicast.

Oam : Operation Administration and Maintenance protocol per ITU-T Y.1731.

OnePPS : One_pps_mode configuration. Use the One PPS signal from the switch for synchronization between the switch and PHY.



One-Way : If true, one way measurements are used. This parameter applies only to a slave. In one-way mode no delay measurements are performed, i.e. this is applicable only if frequency synchronization is needed. The master always responds to delay requests.

VLAN Tag Enable : The VLAN Tag Enable parameter is ignored, because the tagging is controlled by the VLAN configuration.

VID : VLAN Identifier used for tagging the VLAN packets.

PCP : Priority Code Point value used for PTP frames.

Clock current Data Set : The clock current data set is defined in the IEEE 1588 Standard. The current data set is dynamic.

stpRm : Steps Removed : It is the number of PTP clocks traversed from the grandmaster to the local slave clock.

Offset from Master : Time difference between the master clock and the local slave clock, measured in ns.

Mean Path Delay : The mean propagation time for the link between the master and the local slave.

Clock Parent Data Set : The clock parent data set is defined in the IEEE 1588 standard. The parent data set is dynamic.

Parent Port Identity : Clock identity for the parent clock, if the local clock is not a slave, the value is the clocks own ID.

Port : Port Id for the parent master port

PStat : Parents Stats (always false).

Var : It is observed parent offset scaled log variance

Change Rate : Observed Parent Clock Phase Change Rate. i.e. the slave clocks rate offset compared to the master. (unit = ns per s).

Grand Master Identity : Clock identity for the grand master clock, if the local clock is not a slave, the value is the clocks own id.

Grand Master Clock Quality : The clock quality announced by the grand master (See description of Clock Default DataSet:Clock Quality)

Pri1 : Clock priority 1 announced by the grand master

Pri2 : Clock priority 2 announced by the grand master.

Clock 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 default clock servo uses a PID regulator to calculate the current clock rate. i.e.

$$\text{clockAdjustment} = \text{OffsetFromMaster} / \text{P constant} + \text{Integral}(\text{OffsetFromMaster}) / \text{I constant} + \text{Differential}(\text{OffsetFromMaster}) / \text{D constant}$$

Display : If true then Offset From Master, MeanPathDelay and clockAdjustment are logged on the debug terminal

P-enable : If true the P part of the algorithm is included

I-Enable : If true the I part of the algorithm is included

D-enable : If true the D part of the algorithm is included

'P' constant : [1..1000] see above

'I' constant : [1..10000] see above

'D' constant : [1..10000] see above

Filter Parameters : The default delay filter is a low pass filter, with a time constant of $2 \times \text{DelayFilter} \times \text{DelayRequestRate}$.

If the DelayFilter parameter is set to 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 $(\text{period} \times \text{dist} < \text{SyncPackets pr sec}/4)$, i.e. max 4 adjustments are made pr sec.

If **Dist** is 1 the offset is averaged over the **Period**,

If **Dist** is >1 the offset is calculated using 'min' offset.

DelayFilter : See above

Filter Type : Shows the filter type used which can be either the basic filter or an advanced filter that can be configured to use only a fraction of the packets received (i.e. the packets that have experienced the least latency).

Period : See above

dist : See above

Height : The height of the sample window measured in microseconds (only applicable to advanced offset filter).

Percentage : The percentage of sync packets (with smallest delay) used by the offset filter (only applicable to advanced offset filter).

Reset Threshold : The threshold in micro seconds at which the offset filter will be reset, and the slave clock synchronized to the master.

Unicast Slave Configuration : When operating in IPv4 Unicast mode, the slave is configured up to 5 master IP addresses. The slave then requests Announce messages from all the configured masters. The slave uses the BMC algorithm to select one as master clock, the slave then requests Sync messages from the selected master.

Duration : The number of seconds a master is requested to send Announce/Sync messages. The request is repeated from the slave each Duration/4 seconds.

IP Address : IPv4 Address of the Master clock

Grant : The granted repetition period for the sync message

CommState : The state of the communication with the master, possible values are:

IDLE : The entry is not in use.

INIT : Announce is sent to the master (Waiting for a response).

CONN : The master has responded.

SELL : The assigned master is selected as current master.

SYNC : The master is sending Sync messages.

Buttons

Apply : Click to save changes.

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

Messages: *Maximum of 4 clock instances can be created.*

3-30 GVRP

This page lets you set global GVRP configuration parameters commonly applied to all GVRP enabled ports.

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

GVRP (GARP VLAN Registration Protocol) is a protocol for dynamically registering VLANs on ports a specified in IEEE 802.1Q-2005, clause 11. GVRP uses GARP, hence the G in GVRP.

Web Interface

To configure GVRP in the web UI:

1. Click Configuration, GVRP, Global Config.
2. Check the Enable GVRP checkbox.
3. Specify Join-time, Leave-time, Leave All-time, and Max VLANs.
4. Click Apply.

Parameter	Value
Enable GVRP	<input checked="" type="checkbox"/>
Join-time:	<input type="text" value="20"/> (1-20)
Leave-time:	<input type="text" value="60"/> (60-300)
LeaveAll-time:	<input type="text" value="1000"/> (1000-5000)
Max VLANs:	<input type="text" value="20"/>

Figure 3-30.1: GVRP Configuration

Parameter Descriptions:

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

GVRP protocol timers :

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

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

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

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

Buttons

Apply : Click to save changes.

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

3-30.2 Port Config

This page lets you enable or disable a port for GVRP operation. This configuration can be performed either before or after GVRP is configured globally; the protocol operation will be the same.

To configure GVRP Port parameters in the web UI:

1. Click Configuration, GVRP, Port Config.
2. Specify the Mode for each Port and click Apply.

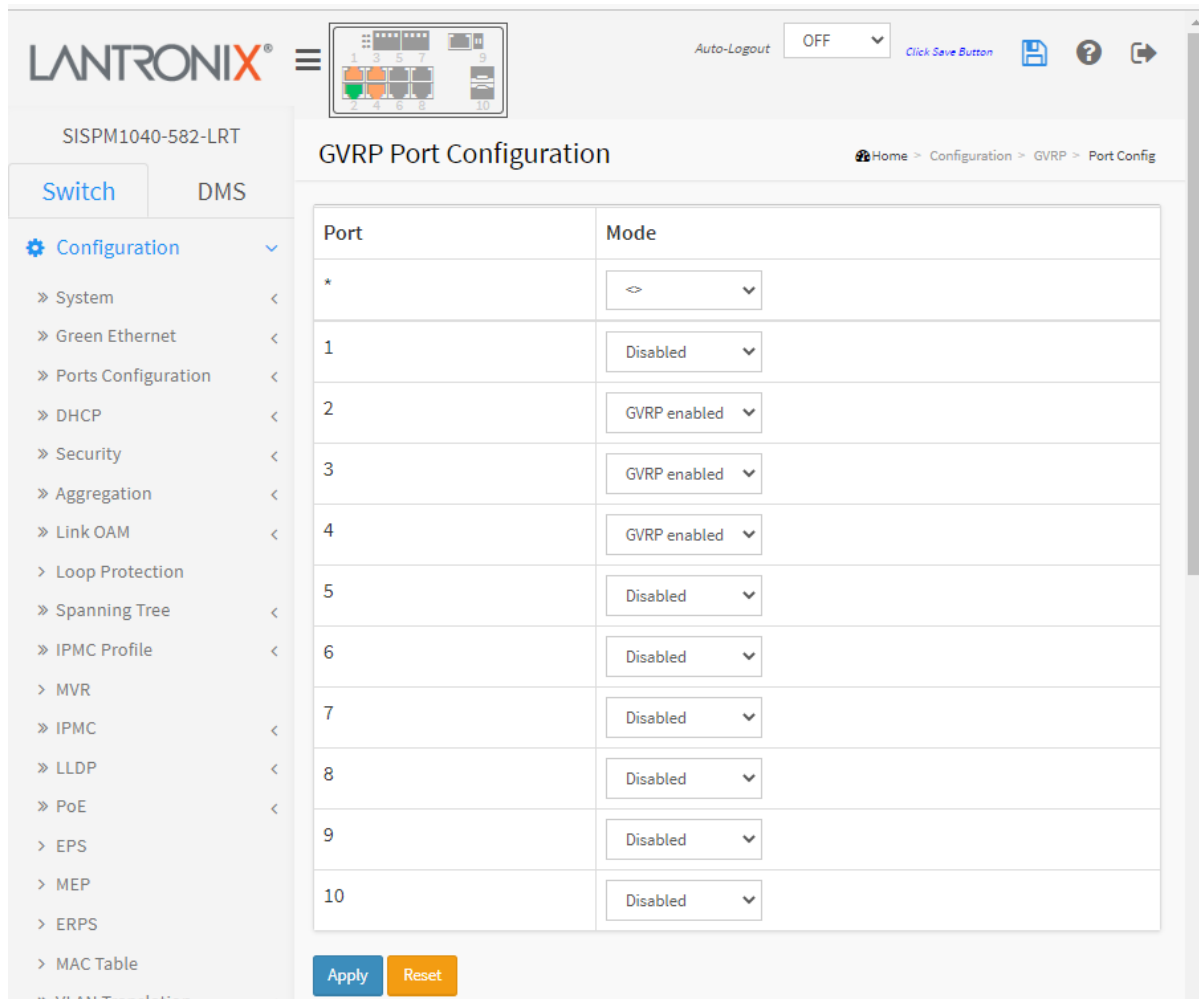


Figure 3-30.2: GVRP Port Configuration

Parameter descriptions:

Mode : Select to enable or disable GVRP Mode on a particular port.

Disabled: Select to Disable GVRP mode on this port.

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

Buttons

Apply : Click to save changes.

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

3-31 sFlow

The sFlow Collector configuration for the switch can be monitored and modified here. The configuration is divided into two parts: configuration of the sFlow receiver (a.k.a. sFlow collector) and configuration of per-port flow and counter samplers.

sFlow configuration is not persisted to non-volatile memory, which means that a reboot or master change will disable sFlow sampling.

To configure sFlow in the web UI:

1. Click Configuration, sFlow.
2. Set the Agent, Receiver, and Port parameters.
3. Click the Apply button to save the settings.
4. To cancel the settings click the Reset button to revert to previously saved values

The screenshot shows the 'sFlow Configuration' web interface. On the left is a navigation menu with 'Configuration' selected and 'sFlow' highlighted. The main content area is divided into three sections:

- Agent Configuration:** IP Address: 127.0.0.1
- Receiver Configuration:**
 - Owner: Kringar (dropdown)
 - IP Address/Hostname: 0.0.0.0
 - UDP Port: 8543
 - Timeout: 0 seconds
 - Max. Datagram Size: 1400 bytes
- Port Configuration:** A table with columns for Port, Flow Sampler (Enabled, Sampler Type, Sampling Rate, Max. Header), and Counter Poller (Enabled, Interval).

Port	Flow Sampler				Counter Poller	
	Enabled	Sampler Type	Sampling Rate	Max. Header	Enabled	Interval
*	<input type="checkbox"/>	<>	0	128	<input type="checkbox"/>	0
1	<input type="checkbox"/>	Tx	0	128	<input type="checkbox"/>	0
2	<input type="checkbox"/>	Tx	0	128	<input type="checkbox"/>	0
3	<input type="checkbox"/>	Tx	0	128	<input type="checkbox"/>	0
4	<input type="checkbox"/>	Tx	0	128	<input type="checkbox"/>	0
5	<input type="checkbox"/>	Tx	0	128	<input type="checkbox"/>	0
6	<input type="checkbox"/>	Tx	0	128	<input type="checkbox"/>	0
7	<input type="checkbox"/>	Tx	0	128	<input type="checkbox"/>	0
8	<input type="checkbox"/>	Tx	0	128	<input type="checkbox"/>	0
9	<input type="checkbox"/>	Tx	0	128	<input type="checkbox"/>	0
10	<input type="checkbox"/>	Tx	0	128	<input type="checkbox"/>	0

At the bottom of the Port Configuration table are 'Apply' and 'Reset' buttons.

Figure 3-31: sFlow Configuration

Parameter descriptions:**Agent Configuration**

IP Address : The IP address used as Agent IP address in sFlow datagrams. It serves as a unique key that will identify this agent over extended periods of time. Both IPv4 and IPv6 addresses are supported.

Receiver Configuration

Owner : Basically, sFlow can be configured in two ways: through local management using the Web or CLI interface or through SNMP. This read-only field shows the owner of the current sFlow configuration and assumes values as follows:

- If sFlow is currently unconfigured/unclaimed, Owner contains *<none>*.
- If sFlow is currently configured through Web or CLI, Owner contains *<Configured through local management>*.
- If sFlow is currently configured through SNMP, Owner contains a string identifying the sFlow receiver.
- If sFlow is configured through SNMP, all controls - except for the Release-button - are disabled to avoid inadvertent reconfiguration.

The **Release** button releases the current owner and disables sFlow sampling. The button is disabled if sFlow is currently unclaimed. If configured via SNMP, the release must be confirmed (a confirmation request displays).

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 the Refresh button. If locally managed, the timeout can be changed on the fly without affecting any other settings.

Max. Datagram Size : The maximum number of data bytes that can be sent in a single sample datagram. This should be set to a value that avoids fragmentation of the sFlow datagrams. Valid range is 200 - 1468 bytes with default being 1400 bytes.

Port Configuration

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

Flow Sampler Enabled : Enables/disables flow sampling on this port.

Sampler Type : At the dropdown select Rx, Tx, or All.

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; the default is 128 bytes. If the maximum datagram size does not take into account the maximum header size, samples may be dropped.

Counter Poller Enabled : Enables/disables counter polling on this port.

Counter Poller Interval : With counter polling enabled, this specifies the interval - in seconds - between counter poller samples.

Buttons:

Apply : Click to save changes.

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

3-32 UDLD

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

To configure UDLD in the web UI:

1. Click Configuration, UDLD.
2. Specify UDLD mode and Message Interval, then click Apply.

Port	UDLD mode	Message Interval
*	<=>	7
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

Figure 3-32: UDLD Port Configuration

Parameter descriptions:

Port : Port number of the switch.

UDLD Mode : Configures the UDLD mode on a port. Valid values are Disable, Normal and Aggressive. The 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 the ports back up you must disable UDLD on those ports.

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

Buttons:

Apply : Click to save changes.

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

3-33 Rapid Ring / Ring To Ring / Rapid Chain

This page lets you configure Rapid Ring parameters. **Note** that Rapid Ring and Ring-to-Ring can also be configured via the front panel DIP switch (i.e., without using the Web UI or CLI). See section [3-33.6 HW Setting and Status for Rings](#) on page 291 for details. Also note that you must disable STP at Configuration > Spanning Tree > CIST Port before you can configure Rapid Ring.

To configure Rapid Ring in the web UI:

1. Click Configuration, Rapid Ring.
2. Specify the Role, Ports, and Status.
3. Click Apply.

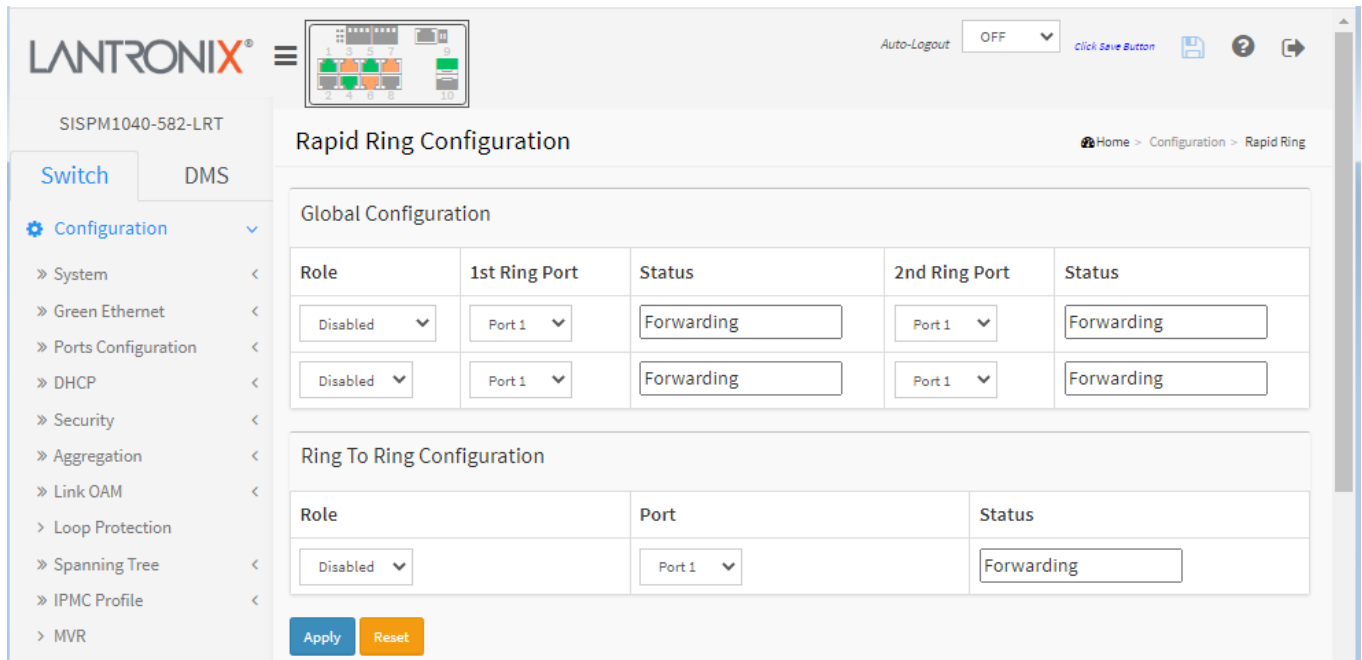


Figure 3-33: Rapid Ring Configuration

Parameter descriptions:

Global Configuration

Role : Set two roles for the first Ring Port:

Disabled : Rapid Ring is disabled globally.

Master : Ring Master.

Member : Ring Member.

Rapid-Chain : role is rapid chain.

1st Ring Port : Select a port from the dropdown.

Status : Rapid Ring status of first Ring Port (e.g., *Forwarding*, *Discarding*).

2nd Ring Port : Select another port from the dropdown.

Status : Rapid Ring status of second Ring Port (e.g., *Forwarding*, *Discarding*).

Role

Disabled	▼
Disabled	
Master	
Member	
Rapid-Chain	

Ring To Ring Configuration

Role : Set role value (Active, Backup, or Disabled).

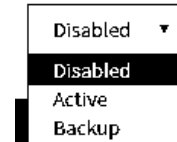
Port : The switch port number of the port.

Status : The current Ring To Ring status of the port (e.g., *Forwarding*).

Buttons:

Apply : Click to save changes.

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

Role**Messages**

Message: *Rapid Ring Configuration Error Error in port 2, STP is enable*

Recovery:

1. Click the **Previous** button.
2. Disable STP at Configuration > Spanning Tree > CIST Port.
3. Continue operation.

Message: *The ports should not be the same.*

Recovery:

1. Click the **OK** button.
2. Make sure that the 1st Ring Port, the 2nd Ring Port, and the Ring To Ring port numbers are different.
3. Continue operation.

Message: *Ring to Ring Configuration Error Error in port 1, same with rapid ring port*

Recovery:

1. Click the **Previous** button.
2. Change the Ring to Ring port number.
3. Continue operation.

3-33.1 Rapid Ring Operation

Rapid Ring is a redundancy proprietary protocol that runs on your network; it can be used to recover the network system from critical link failures so as to protect from network loops.

Many redundant or network recovery protocols defined by IEEE, such as spanning tree (STP, RSTP, MSTP) were developed to recover the network system for the connection failure, but the recovery time of Rapid Ring is can be less than 20ms for up to 250 switches, which is much less than the other redundancy protocols.

Rapid Ring supports four different applications as described below:

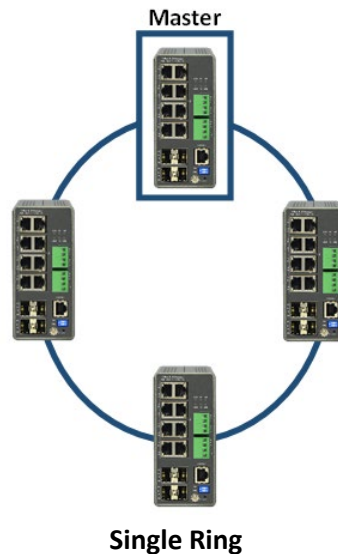
- Single Ring
- Ring to Ring
- Dual Ring
- Rapid Chain

Note: Only one redundant protocol can be used at the same time, so before you use Rapid Ring, you must disable the Spanning Tree at Configuration > Spanning Tree > CIST Port.

3-33.2 Single Ring

Single Ring is the most common ring to use, where you configure one of the switches as the “Master” and the other switches as Members of Single Ring. There are forwarding paths and a backup path on the ring master.

If one link fails, the ring will automatically activate the backup path within 20ms, recovering the network system if a critical link failure occurs.



Single Ring Configuration Procedure

- A. Select the Role (Master or Member). Only one switch can be the Master and set the other switches as Members of the Single Ring.

Rapid Ring Configuration Home > Configuration > Rapid > Ring

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

Apply Reset

- B. Configure the 1st Ring Port and 2nd Ring Port as link ports.

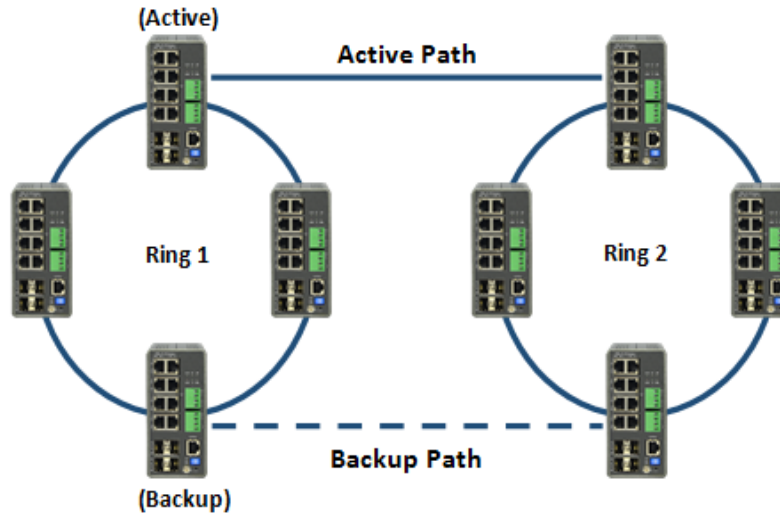
If it is Master, by default 1st Ring Port will be the active path and 2nd Ring Port is the backup path. If it is Member, 1st Ring Port and 2nd Ring Port are used to connect the link partner of the Single Ring.

- C. Check the port status (e.g., Forwarding, Discarding, etc.).

3-33.3 Ring to Ring

Ring to Ring is a flexible application to connect several single rings together. Since some device could be located in a remote area, it may not be convenient to connect all devices in the system to create on single ring.

Ring to Ring can be used to connect the devices into different single rings, they can still communicate with each other. If any path fails, Ring to Ring can be used to recover the network system within 20ms.



Ring to Ring

- A. Set up Single Ring for Ring 1 and Ring 2; see the previous section.
- B. Set the Role as Active or Backup or Disabled. Choose one specific Ring (Ring 1 or Ring 2) to set up ring-to-ring configuration. Remember to configure Active and Backup Switch connected to another ring. Only one switch can set to be the Active/ Backup, and rest of the switches should configure as Disabled.
- C. Configure Active/ Backup link port. This port should not be same as above 1st Ring Port and 2nd Ring Port.

Rapid Ring Configuration Home - Configuration - Rapid - Ring

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

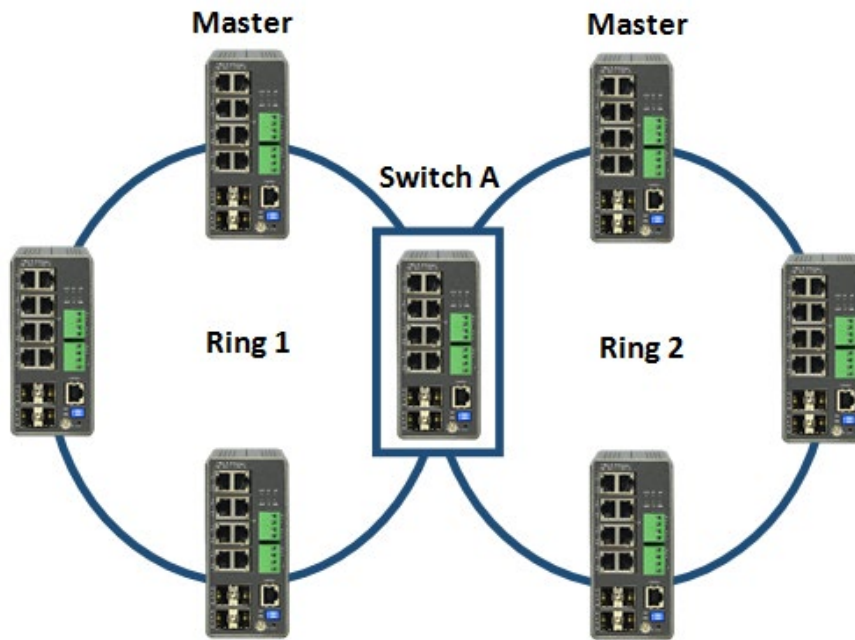
Ring To Ring Configuration

Role	Port	Status
Disabled	Port 1	Forwarding

Apply Reset

3-33.4 Dual Ring

Dual Ring is a more economical application, which uses only one switch between the two rings. This mode is ideal for applications that have inherent cabling difficulties and saves costs.



Dual Ring

- A. Set up Single Ring for Ring 1 and Ring 2, see above.
- B. Set up a second ring for switch A, see above.

Note: Switch A is not suggested to be the Master for Ring 1 or Ring 2.

Rapid Ring Configuration Home - Configuration - Rapid - Ring

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

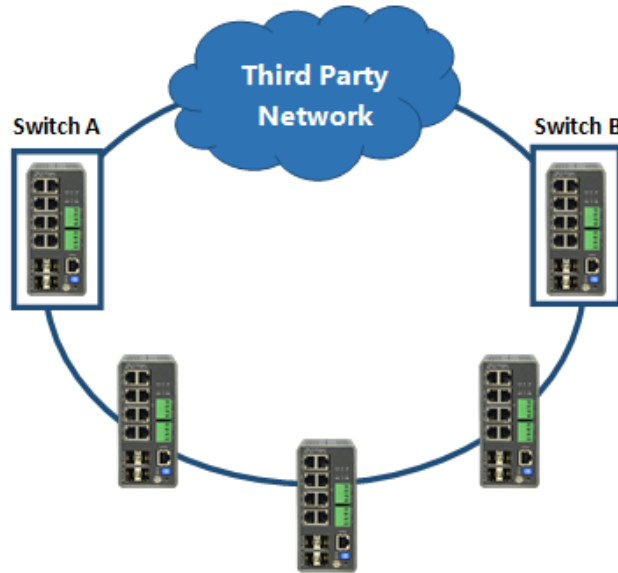
Ring To Ring Configuration

Role	Port	Status
Disabled	Port 1	Forwarding

Apply Reset

3-33.5 Rapid Chain

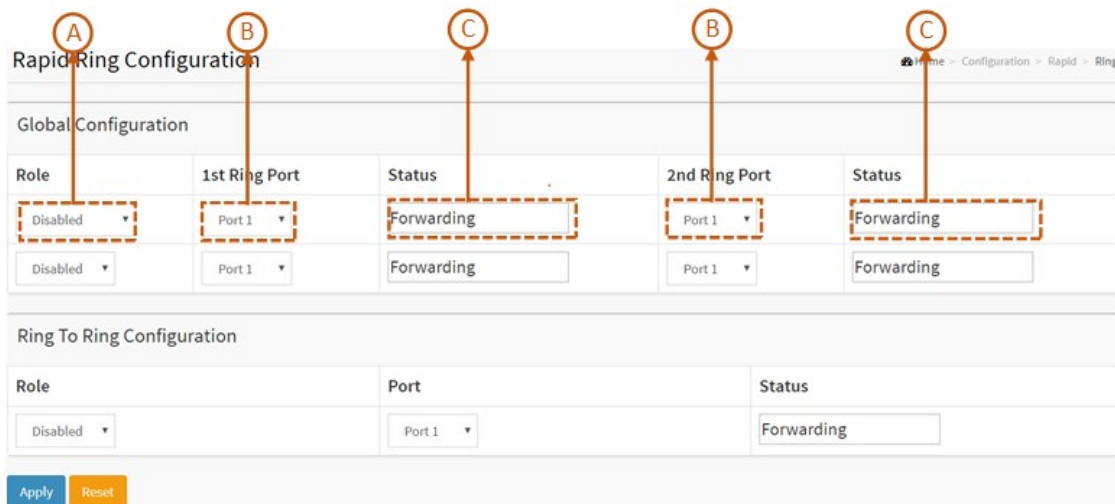
Rapid Chain is a highly flexible application for complex industrial networks. It allows our switches to be quickly and easily deployed in any type of complex redundant network with a fast recovery time. It is very easy to configure and manage.



Rapid Chain

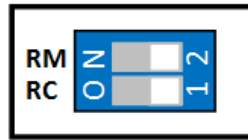
- A. Scroll the Role as Rapid-Chain or Member. Only two switches (Switch A & B) have to be set as Rapid-Chain, and the rest of the switches should set as the Members of Rapid Chain.
- B. Configure 1st Ring Port and 2nd Ring Port as link port.
 If it is Rapid-Chain, 2nd Ring Port has to connect to Third Party Network.
 If it is Member, 1st Ring Port and 2nd Ring Port is connected to link partner of the Rapid Chain.
- C. Check the port status (e.g., Forwarding, Discarding, etc.).

Note: If Rapid-Chain, one of Switch A & Switch B’s 2nd port will be backup path (the smaller MAC address).



3-33.6 HW Setting and Status for Rings

Ring Setting by DIP Switch:



DIP Switch

Configure Rapid Ring by setting the DIP Switch as described below:

Mode	RM	RC	Rapid Ring Status	1st Port	2nd Port	LED RM (Ring Master)	LED RC (Rapid Chain)
HW Control	OFF	OFF	Single Ring Member	The largest Odd Port Number	The largest Even Port Number	Lit Amber	Off
HW Control	ON	OFF	Single Ring Master	The largest Odd Port Number	The largest Even Port Number	Lit Green	Off
HW Control	OFF	ON	Rapid Chain	The largest Odd Port Number	The largest Even Port Number	Off	Lit Green (Active Path) Lit Amber (Backup Path)
SW Control	ON	ON	Rapid Ring Settings by Software	--	--	--	--

Notes:

1. The default setting of the DIP Switch is ON/ON (Software Control).
2. In HW Control mode, all Rapid Ring and Spanning Tree SW configuration from Web, Telnet and Console is "deactivated".
3. Only Single Ring and Rapid Chain are configurable by DIP Switch.
4. The largest Even/Odd ports include both fiber and copper I/O. If it is Combo, either fiber or copper can be used as ring connecting port.

LED Status (RM/RC) can refer to the table as below:

LED	Color	State	Description
RM (Ring Master)	Green	On	Ring Master has been detected in the switch.
	Amber	On	Ring Member has been detected in the switch.
	--	Off	RM Disabled.
RC (Rapid Chain)	Green	On	Rapid Chain has been detected in the switch. (Active path).
	Amber	On	Rapid Chain has been detected in the switch. (Backup path).
		Blinking	Error: There is no correspondent Rapid Chain Switch found.
	--	Off	RC Disabled.

3-34 Percepixon and LPM

This page lets you configure Percepixon parameters. This page has four sections: the Status, Configuration, Percepixon Connection 1, and Connection 2 sections as shown and described below.

Percepixon is Lantronix cloud-hosted management platform that provides a single pane of glass for centralized management and automated monitoring of all deployed Lantronix Remote Environment Management and IoT products, along with real-time notifications, managed APIs and data dashboards. For more information see <https://www.lantronix.com/percepixon/>.

Lantronix Provisioning Manager (LPM) is a software application that provisions, configures and updates Lantronix Console Managers and IoT Gateways for local site installations and deployments. LPM discovery is enabled by default and is not configurable. For more LPM information see <https://www.lantronix.com/products/lantronix-provisioning-manager/>.

There are three pieces of information that the Percepixon client needs to complete registration and to publish data and configuration to the Percepixon server: **Device ID**, **Device Key**, and **Serial Number**. The Serial Number is always preprogrammed on the device (typically derived from the MAC address of the first Ethernet port).

A new device would also be preprogrammed with the Device ID and Key. For existing devices where the ID and Key are not pre-programmed, LPM uses Lantronix proprietary search and query protocol to get the device serial number, and then uses the switch REST API interface to set the Device ID and Device Key.

3-34.1 Supported Firmware Versions

Devices must meet firmware requirements in order to work with Percepixon and LPM. SISPM1040-362-LRT and SISPM1040--582-LRT require firmware VB7.20.0191 or above.

3-34.2 Percepixon Agent Configuration

Navigate to Configuration > Percepixon to display the Percepixon Agent Configuration page. The Status section is shown and described below.

Status	
Client state	Running Not registered -
Last status update	Not available
Last content check	Not available
Available Firmware updates	Not available
Available Configuration updates	Not available

Parameter descriptions:

Status:

Client state: Displays the existing Percepixon client state (e.g., *Exited*, *Active*, *Inactive*, *Running*, or *Not Registered*) .

Last status update: Displays the amount of time in minutes between status updates (1-1440 minutes or <Not Available>).

Last content check: Displays the amount of time in minutes between content checks; 1 minute to 90 days (in minutes) or <Not Available>.

Available Firmware updates: Displays a list of firmware that is available on the server. Select the firmware from this list and click Update now to upgrade or downgrade the firmware. Displays <Not available> if no Firmware updates are currently available.

Available Configuration updates: Displays a list of configuration that is available on the server. Select the configuration from this list and click Update now to upgrade or downgrade the firmware. Displays <Not available> if no configuration updates are currently available.

Global Configuration:

<ul style="list-style-type: none"> > Loop Protection > Spanning Tree > IPMC Profile > MVR > IPMC > LLDP > PoE > EPS > MEP > ERPS > MAC Table > VLAN Translation > VLANs > Private VLANs > VCL > Voice VLAN > Ethernet Services > QoS 	<table border="1"> <thead> <tr> <th colspan="2">Global Configuration</th> </tr> </thead> <tbody> <tr> <td>Enabled</td> <td><input checked="" type="checkbox"/></td> </tr> <tr> <td>Device ID</td> <td><input type="text"/></td> </tr> <tr> <td>Device Key</td> <td><input type="text"/></td> </tr> <tr> <td>Serial Number</td> <td>00c0f2823e8b</td> </tr> <tr> <td>Device Name</td> <td>SISPM1040-582-LRT-3E8B</td> </tr> <tr> <td>Device Description</td> <td>Lantronix SISPM1040-582-LRT</td> </tr> <tr> <td>Status Update Interval (in minutes)</td> <td><input type="text" value="1"/></td> </tr> <tr> <td>Content Check Interval (in minutes)</td> <td><input type="text" value="1"/></td> </tr> <tr> <td>Apply Firmware Updates</td> <td><input checked="" type="checkbox"/></td> </tr> <tr> <td>Apply Configuration Updates</td> <td><input checked="" type="checkbox"/></td> </tr> <tr> <td>Active Connection</td> <td>Connection 1 <input type="button" value="v"/></td> </tr> </tbody> </table>	Global Configuration		Enabled	<input checked="" type="checkbox"/>	Device ID	<input type="text"/>	Device Key	<input type="text"/>	Serial Number	00c0f2823e8b	Device Name	SISPM1040-582-LRT-3E8B	Device Description	Lantronix SISPM1040-582-LRT	Status Update Interval (in minutes)	<input type="text" value="1"/>	Content Check Interval (in minutes)	<input type="text" value="1"/>	Apply Firmware Updates	<input checked="" type="checkbox"/>	Apply Configuration Updates	<input checked="" type="checkbox"/>	Active Connection	Connection 1 <input type="button" value="v"/>
Global Configuration																									
Enabled	<input checked="" type="checkbox"/>																								
Device ID	<input type="text"/>																								
Device Key	<input type="text"/>																								
Serial Number	00c0f2823e8b																								
Device Name	SISPM1040-582-LRT-3E8B																								
Device Description	Lantronix SISPM1040-582-LRT																								
Status Update Interval (in minutes)	<input type="text" value="1"/>																								
Content Check Interval (in minutes)	<input type="text" value="1"/>																								
Apply Firmware Updates	<input checked="" type="checkbox"/>																								
Apply Configuration Updates	<input checked="" type="checkbox"/>																								
Active Connection	Connection 1 <input type="button" value="v"/>																								

Enabled : Check the box to enable PercepXion globally. The default is disabled (unchecked).

Device ID: Displays the switch Device ID (read only). The Device ID may be provisioned through Lantronix Provisioning manager (LPM). **Note**: The Device ID can only be provisioned once. It will persist across resets.

Device Key: Enter the key for the device; 32 alphanumeric characters. **Note**: Device Key may be configured via the Lantronix Provision Manager (LPM). The entry field shows two icons:



: Click to Show the Device Key text as you enter it.



: Click to Hide the Device Key text as you enter it.

Serial Number : Displays the serial number of the switch in the format *00c0f24f73d0*. Read only.

Device Name : Enter a PercepXion Device Name for the switch of up to 32 alphanumeric characters (e.g., *SISPM1040-582-LRT-73D0*). Device Name can have only alphanumeric (a-z, A-Z, 0-9) characters, hyphens (-), and underscores (_). Device Name must begin and end with an alphanumeric character.

Device Description : Enter a PercepXion Device Description for the switch of up to 32 alphanumeric characters (e.g., *Lantronix SISPM1040-582-LRT*).

Status Update Interval : Select the amount of time in minutes between updates (1-1440 minutes). The default is 1 minute. This is the frequency that the switch updates the device status to PercepXion.

Content Check Interval : Select the amount of time in minutes between content checks (1-56160 minutes). The default is 1 minute. This is the frequency that the switch checks PercepXion for updates to configuration or firmware. The valid range is 1 hour – 2160 hours (90 days).

Apply Firmware Updates : Check the box to enable automatic switch firmware upgrades via PercepXion. The default is enabled.

Apply Configuration Updates : Check the box to enable automatic switch configuration upgrades via PercepXion. The default is enabled.

Active Connection: At the dropdown select the configuration you want to be active (i.e., *Connection 1* or *Connection 2*). The default is *Connection 1*. This is the connection to use when connecting to PercepXion. The configurable parameters for Connection 1 and Connection 2 are shown and described below.

Connection 1	
Connect To	Cloud
Host	api.percepXion.ai
Port	443
Secure Port	<input checked="" type="checkbox"/>
Validate Certificates	<input checked="" type="checkbox"/>

Connection 2	
Connect To	Cloud
Host	api.percepXion.ai
Port	443
Secure Port	<input checked="" type="checkbox"/>
Validate Certificates	<input checked="" type="checkbox"/>

Apply Reset

Connection 1 :

Connect To : At the dropdown, select Cloud (default) or On-premise as the PercepXion connection type for Connection 1. PercepXion is available in cloud or on-premise installation. Choose cloud or on-premise setup according to the determination of your organization. See the PercepXion [Help page](#) for more information.

Cloud setup connects you directly to the PercepXion server URL, allowing you to access your devices through the Internet.

On-premise setup connects you to PercepXion through your organization's network. This means you need to be physically "on-premises" to access your organization's network via Wi-Fi, or may need to use a VPN connection. You may later view and update on-premise setup.

Host : Enter the IP address or host name of the PercepXion server for Connection 1. This is used by PercepXion to register the switch.

Port : Enter the port number for Connection 1. The default is port 443.

Secure Port : Check the box to make the selected port a secure port for Connection 1. The default is enabled.

Validate Certificates : Check the box to force using certificate validation for Connection 1. The default is enabled. To validate certificates, Secure Port must be enabled.

Connection 2 :

Connect to: At the dropdown select the type of connection to use for Connection 1 (*Cloud* or *On Premise*). The default is *Cloud*.

Cloud : Use Lantronix centralized cloud-based Management software for Connection 2.

On Premise: Use Lantronix centralized on-premise Management software for Connection 2.

Host : Enter the IP address of the PercepXion Host for Connection 2.

Port : Enter the port number for Connection 2 for Connection 2. The default is port 443.

Secure Port : Check the box to make the selected port a secure port for Connection 2. The default is enabled.

Validate Certificates : Check the box to enable using certificate validation of the PercepXion server certificates. To validate certificates, Secure Port must be enabled. The default is enabled.

Buttons

Apply : Click to apply changes.

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

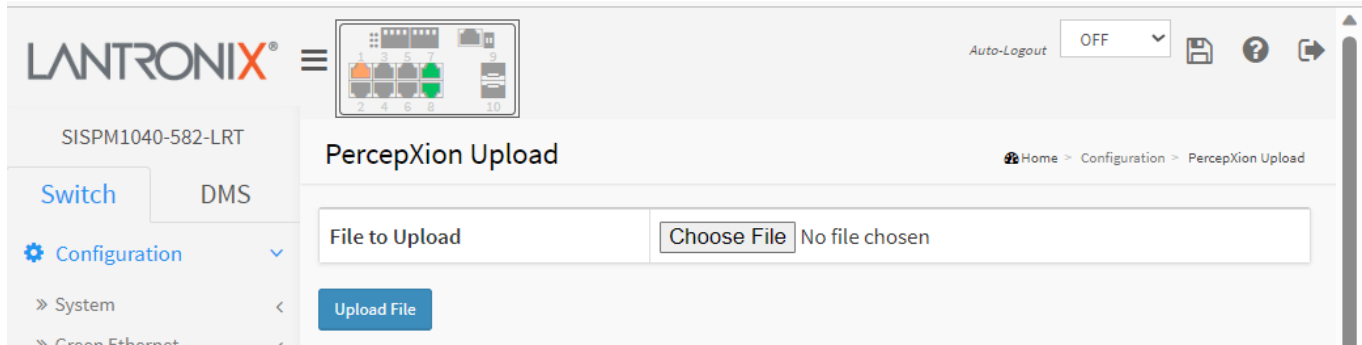
Messages:

device id : 32 alphanumeric characters

5

3-34.3 PercepXion Upload

Navigate to Configuration > PercepXion to display the PercepXion Upload page. This page lets you navigate to and select a file to upload.



Parameter descriptions:

File to Upload: Click the Choose File button to navigate to and select a file to upload a file from the web browser.

Upload File: Click the Upload File button to upload the selected file. When done, the message "Upload successfully completed." displays.

3-35 MRP

The MRP function is used to set Media Redundancy Protocol configuration. MRP is a data network protocol standardized by the International Electrotechnical Commission as IEC 62439-2. MRP allows rings of Ethernet switches to overcome any single failure with recovery time much faster than achievable with Spanning Tree Protocol. See the IETF [website](#) at for more information.

Note: You must disable Spanning Tree at Configuration > Spanning Tree > CIST Port before you can configure MRP on this page.

The maximum number of MRP entries is 2. See “Appendix B. MRP Pre-Requisites and Application Examples” on page 485 for MRP config examples.

To configure MRP in the web UI:

1. Click Configuration and MRP.
2. Click the Add New Domain button to add a new domain and configure the parameters.
3. Click Apply to save configuration.
4. Click the Edit button to enter the ring domain setting page and configure it.
5. Click Apply to save the changes.

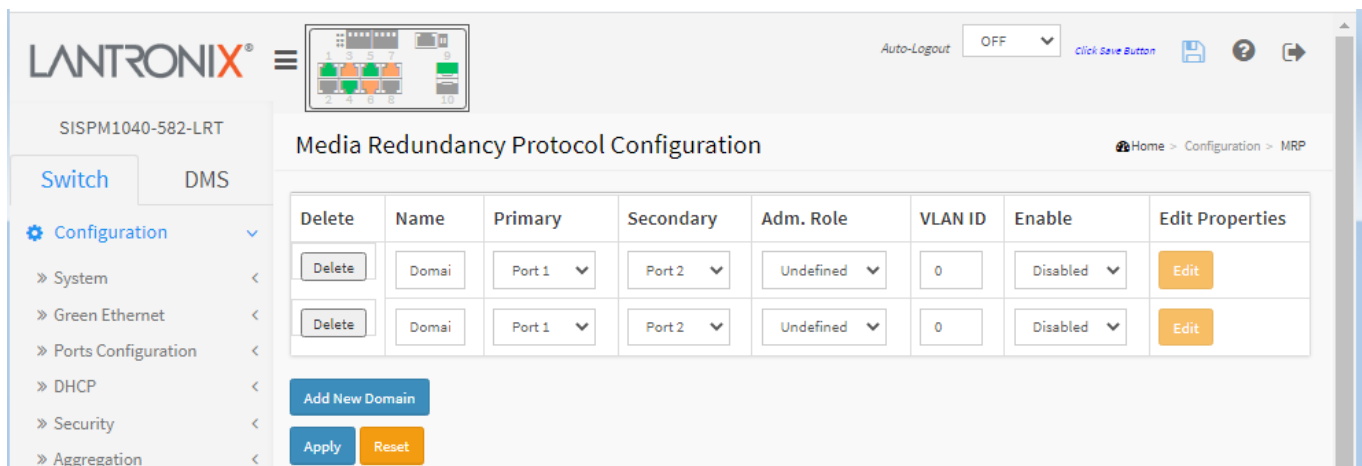


Figure 3-35: Media Redundancy Protocol Configuration

Parameter descriptions:

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

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 will be set to the role of a Media Redundancy Client (**MRC**). If the value is set to manager, the entity will be set to the role of a Media Redundancy Manager (**MRM**). The **MRM** monitors the ring topology. During normal ring operation (i.e., without ring interruption due to an error) the MRM disconnects one of its ring ports so that the ring topology becomes ‘loop free’ from a communication point of view. As soon as the ring is open due to the failure of a node and the data communication is broken, the MRM reconfigures the data paths within 200ms. It enables the disconnected ring port and creates a new loop free topology.

VLAN ID: The VLAN ID assigned to the MRP protocol. The allowed range is 0 - 4094.

Enable: Enable/Disable the MRP protocol. This must be set to Disabled for you to be able to edit Ring Domain parameters. See below.

Edit Properties: Click the Edit button to edit Ring Domain parameters. See below.

Buttons

Add New Domain: Click to add a new domain row. The maximum number of entries is 2.

Apply: Click to save changes.

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

Ring Domain Configuration

Click the Edit button to display the Ring Domain Configuration page. The MRP **Manager** page displays:

Domain settings	
Id	1
Admin Role	Manag
Name	Domain1
UUID	<input checked="" type="checkbox"/> Default FFFFFFFF-FFFF-FFFF-FFFF-FFFFFFFFFFFF
Primary Port Id	Port 2
Secondary Port Id	Port 3
VLAN ID	10
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

Apply Reset

Parameter descriptions: Note that some parameters may apply to just MRM, or just MRC, or both.

ID: The index of the entry.

Admin Role: If the value is set to client the entity will be set to the role of a Media Redundancy Client (**MRC**).

If the value is set to Manager, the entity will be set to the role of a Media Redundancy Manager (**MRM**).

Name: A logical name for the MRP domain to ease the management of MRP domains.

UUID: Universally Unique Identifier belonging to the MRP domain which represents a ring. Check or uncheck the “Default” checkbox as needed. If checked, the default UUID is used as shown above. If unchecked, enter the UUID in the entry box.

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.

Buttons

Apply: Click to save changes.

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

Messages

Message: *VLAN ID is used in other ring domain*

Message: *Domain is enabled*

Message: *The maximum number of entries is 2*

Message: *Role is undefined*

Message: *Invalid ring port*

Message: *Ring port is used*

Message: *Domain is enabled*

Message: *VLAN ID is used for management*

MRP Client page: see above for parameter descriptions.

SISPM1040-582-LRT

Switch DMS

Configuration

- System
- Green Ethernet
- Ports Configuration
- DHCP
- Security
- Aggregation
- Link OAM
- Loop Protection
- Spanning Tree
- IPMC Profile
- MVR
- IPMC
- LLDP
- PoE
- EPS
- MEP
- ERPS
- MAC Table
- VLAN Translation
- VLANs

Ring Domain Configuration

Home > Configuration > MRP

Domain settings

Id	2
Admin Role	Client
Name	Domain2
UUID	<input checked="" type="checkbox"/> Default FFFFFFFF-FFFF-FFFF-FFFFFFFF
Primary Port Id	Port 4
Secondary Port Id	Port 5
VLAN ID	10
Link Down Interval, ms	20
Link Up Interval, ms	20
Link Change Count	4
BLOCKED State Supported	Enabled

Apply Reset

3-36 SMTP

Configure SMTP (Simple Mail Transfer Protocol) on this page. Simple Mail Transfer Protocol is the message exchange standard for the Internet. The switch is to be configured as a client of SMTP while the server is a remote device that will receive messages from the switch that alarm events occurred.

To configure SMTP in the web UI:

1. Click Configuration, SMTP.
2. Specify the parameters in each blank field.
4. Click the Apply button to save the settings.
5. To cancel the settings click the Reset button to revert to previously saved values.

Parameter	Input Field
Mail Server	<input type="text"/>
User Name	<input type="text"/>
Password	<input type="text"/>
Sender	<input type="text"/>
Return Path	<input type="text"/>
Email Address 1	<input type="text"/>
Email Address 2	<input type="text"/>
Email Address 3	<input type="text"/>
Email Address 4	<input type="text"/>
Email Address 5	<input type="text"/>
Email Address 6	<input type="text"/>

Buttons:

Figure 3-36: SMTP Configuration

Parameter descriptions:

Mail Server : Specify the IP Address of the server transferring your email.

Username : Specify the username on the mail server.

Password : Specify the password on the mail server.

Sender : Set the mail sender name.

Return-Path : To set the mail return-path as sender mail address.

Email Address 1-6 : Email address that would like to receive the alarm message.

Buttons:

Apply : Click to apply changes.

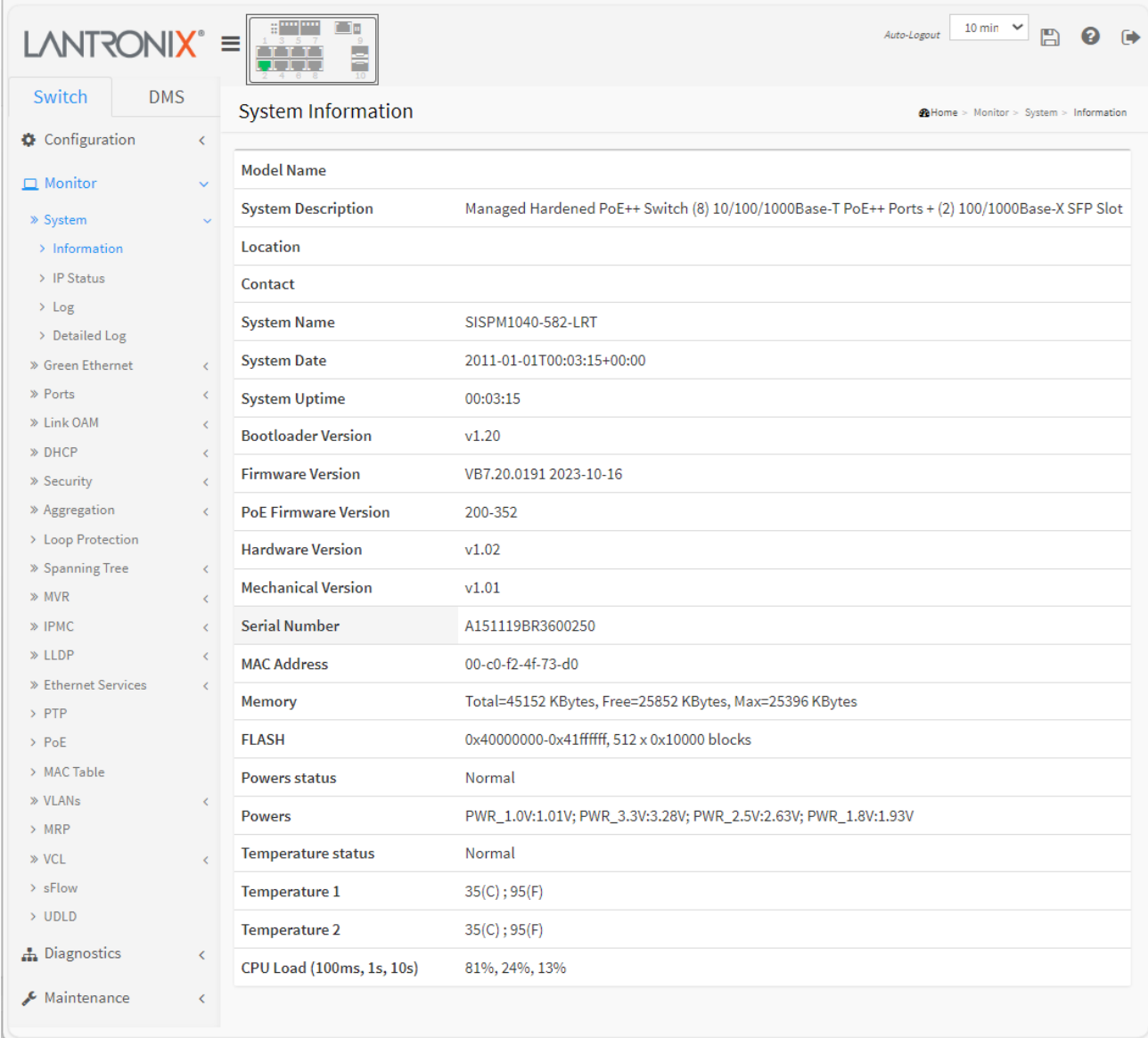
Reset : Click to discard changes.

4. Monitor

This chapter describes the Monitor menu selections, including System, Ports, DHCP, Security, Aggregation, Loop Protection, Spanning Tree, PoE, etc.

4.1 Monitor > System > Information

This page displays system information parameters. This is the startup webpage.



The screenshot shows the Lantronix web interface with the 'Monitor' menu selected. The 'System Information' page is displayed, showing the following parameters:

Model Name	
System Description	Managed Hardened PoE++ Switch (8) 10/100/1000Base-T PoE++ Ports + (2) 100/1000Base-X SFP Slot
Location	
Contact	
System Name	SISPM1040-582-LRT
System Date	2011-01-01T00:03:15+00:00
System Uptime	00:03:15
Bootloader Version	v1.20
Firmware Version	VB7.20.0191 2023-10-16
PoE Firmware Version	200-352
Hardware Version	v1.02
Mechanical Version	v1.01
Serial Number	A151119BR3600250
MAC Address	00-c0-f2-4f-73-d0
Memory	Total=45152 KBytes, Free=25852 KBytes, Max=25396 KBytes
FLASH	0x40000000-0x41ffffff, 512 x 0x10000 blocks
Powers status	Normal
Powers	PWR_1.0V:1.01V; PWR_3.3V:3.28V; PWR_2.5V:2.63V; PWR_1.8V:1.93V
Temperature status	Normal
Temperature 1	35(C); 95(F)
Temperature 2	35(C); 95(F)
CPU Load (100ms, 1s, 10s)	81%, 24%, 13%

Parameter Descriptions:

Model Name : Displays the factory defined model name for identification purposes (*SISPM1040-582-LRT*).

System Description : Displays the system description (*Managed Hardened PoE++ Switch (8) 10/100/1000Base-T PoE++ Ports + (2) 100/1000Base-X SFP Slot*).

Location : The system location configured at Configuration > System > Information > System Location.

Contact : The system contact configured at Configuration > System > Information > System Contact.

System Name : Displays the user-defined system name configured at System > System Information > Configuration > System Name.

System Date : The current (GMT) system time and date. The system time is obtained through the Timing server running on the switch, if any. The format is 2021-04-15T15:18:14+00:00.

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

Bootloader Version : Displays the current boot loader version number (e.g., *v1.20*).

Firmware Version : Displays the current firmware version number and date (e.g., *VB7.20.0191 2023-10-16*).

PoE Firmware Version : The version of PoE MCU firmware (e.g., *104-001* or *200-352*).

Hardware Version : Displays the hardware version of the device (e.g., *v1.01* or *v1.02*). The Initial version is v1.01. HW v1.02 adds 802.3bt Type 4 RJ45 1,2,3,6 PoE Power Polarity and changes the name "Non-stop PoE" to "Always On PoE".

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

Serial Number : Displays the unique serial number that assigned to the device (e.g., *A151118AR1000001* or *A151119BR3600529*).

MAC Address : The MAC Address of this switch (in the format *00-c0-f2-49-38-ff*).

Memory : Displays the memory size of the system (e.g., *Total=51155 KBytes, Free=32220 KBytes, Max=31718 Kbytes*).

FLASH : Displays the flash size of the system (e.g., *0x40000000-0x41ffffff, 512 x 0x10000 blocks*).

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

Powers : Displays the powers of the system (e.g., *PWR_1.0V:0.99V; PWR_3.3V:3.29V; PWR_2.5V:2.60V; PWR_1.8V:1.93V*).

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

Temperature 1 : Displays the temperature of temperature sensor 1 (e.g., *40(C) ; 104(F)*).

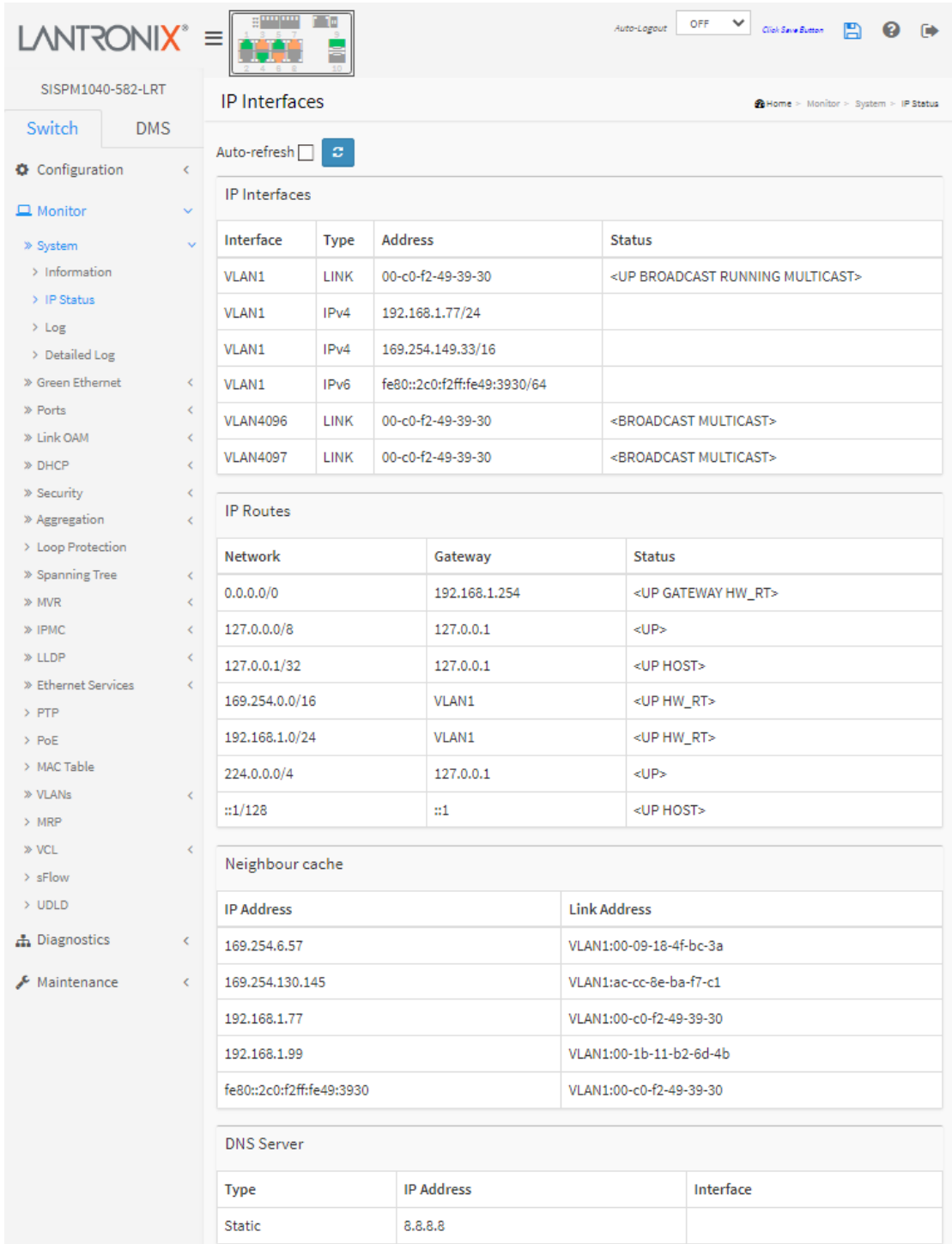
Temperature 2 : Displays the temperature of temperature sensor 2 (e.g., *40(C) ; 104(F)*).

CPU Load (100ms, 1s, 10s) : Displays the CPU loading (100ms, 1s, 10s) of the system. CPU load is a measure of the amount of computational work that a computer system performs. The load average represents the average system load over a period of time. It appears in the form of three numbers which represent the system load during the last ten seconds, one second, and 100 milliseconds.

4-1.2 IP Status

This page displays the status of the IP protocol layer. Status is provided on IP Interfaces, IP Routes, Neighbor cache, and DNS Server. To display IP interfaces in the web UI:

1. Click Monitor, System, and IP Status.
2. View the IP address information.



The screenshot shows the Lantronix web interface for the SISPM1040-582-LRT device. The left sidebar contains navigation menus for Configuration, Monitor, and Maintenance. The main content area is titled "IP Interfaces" and includes an "Auto-refresh" checkbox. Below this, there are four sections: IP Interfaces, IP Routes, Neighbour cache, and DNS Server.

IP Interfaces

Interface	Type	Address	Status
VLAN1	LINK	00-c0-f2-49-39-30	<UP BROADCAST RUNNING MULTICAST>
VLAN1	IPv4	192.168.1.77/24	
VLAN1	IPv4	169.254.149.33/16	
VLAN1	IPv6	fe80::2c0:f2ff:fe49:3930/64	
VLAN4096	LINK	00-c0-f2-49-39-30	<BROADCAST MULTICAST>
VLAN4097	LINK	00-c0-f2-49-39-30	<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
169.254.6.57	VLAN1:00-09-18-4f-bc-3a
169.254.130.145	VLAN1:ac-cc-8e-ba-f7-c1
192.168.1.77	VLAN1:00-c0-f2-49-39-30
192.168.1.99	VLAN1:00-1b-11-b2-6d-4b
fe80::2c0:f2ff:fe49:3930	VLAN1:00-c0-f2-49-39-30

DNS Server

Type	IP Address	Interface
Static	8.8.8.8	

Figure 4-1.2: IP Status

Parameter descriptions:**IP Interfaces**

Interface : Shows the name of the interface.

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

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

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

IP Routes

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

Gateway : Show the gateway address of this route.

Status : Shows the status flags of the route.

Neighbor cache

IP Address : Shows the IP address of the entry.

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

DNS Server

Type: Displays the DNS server type (e.g., Static).

IP Address: Displays the DNS server's IP address.

Interface: Displays the DNS server interface.

Buttons

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

Refresh: Click to refresh the page immediately.

4-1.3 Log

This page lets you view and configure system log information of the switch.

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 "Level" input field is used to filter the display system log entries. The "Clear Level" input field is used to specify which system log entries will be cleared. To clear specific system log entries, select the clear level first then click the Clear button.

The "Start from ID" input field allow 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, these input fields will upon a Refresh button click - assume the value of the first displayed entry, allowing for continuous refresh with the same start input field.

The >> 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 << button to start over.

To display syslog information in the web UI:

1. Click Monitor, System and Log.
2. View the log information.
3. Set the Do Relay Status and Do Relay Alarm Cut-off functions as needed.

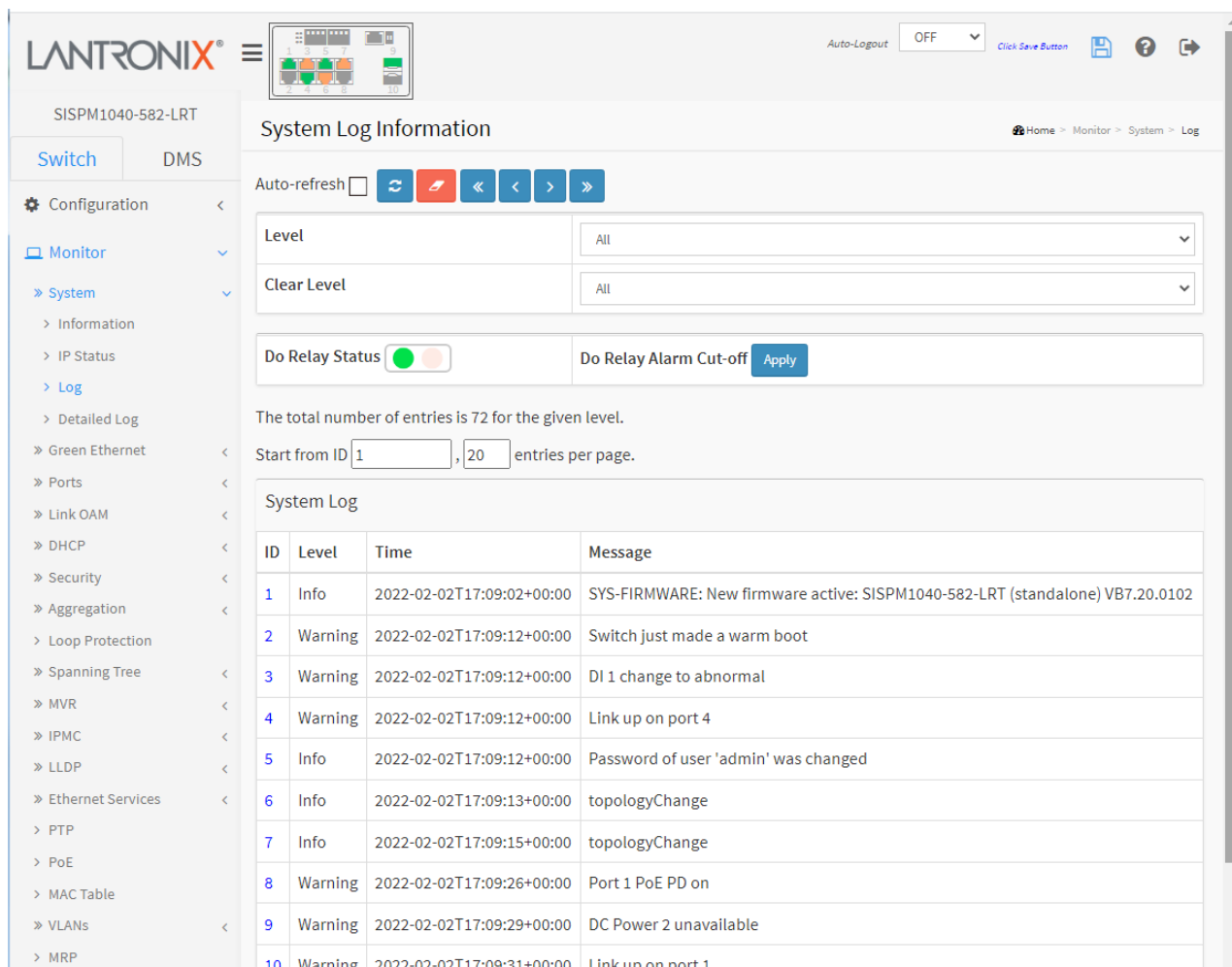


Figure 4-1.3: System Log Information

Parameter descriptions:

Level : level of the system log entry. These level types are supported:

Emerg: The system log entry is belonged emergency level.

Alert: The system log entry is belonged alert level.

Crit: The system log entry is belonged critical level.

Error: The system log entry is belonged error level.

Warning: The system log entry is belonged warning level.

Notice: The system log entry is belonged notice level.

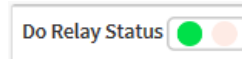
Info: The system log entry is belonged information level.

Debug: The system log entry is belonged debug level.

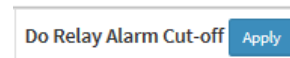
All : Display all of the level types listed above (this is the default).

Clear Level :The levels to be cleared on a Clear operation. The level types supported are listed above.

Do Relay Status : Shows the status of digital-out relay contact.



Do Relay Alarm Cut-off : Click to force a cut off the digital-out relay contact.



ID : The ID of the system log entry. Click the linked ID to display its detailed log information.

Time : Displays the log record by device time. The time of the system log entry.

Message : Displays the log detail message. The message of the system log entry.

Buttons



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

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

Clear: Flushes the selected log entries; the message “No entry exists” displays in the empty table.

<< : Updates the system log entries, starting from the first available entry ID.

< : Updates the system log entries, ending at the last entry currently displayed.

> : Updates the system log entries, starting from the last entry currently displayed.

>> : Updates the system log entries, ending at the last available entry ID.

Sample Syslog Entries

ID	Level	Time	Message
1	Notice	2011-01-01T00:00:10+00:00	LINK-UPDOWN: Interface Vlan 1, changed state to down.
2	Warning	2011-01-01T00:00:11+00:00	DI 1 change to abnormal
3	Warning	2011-01-01T00:00:11+00:00	Link up on port 1
4	Info	2011-01-01T00:00:11+00:00	Password of user 'admin' was changed
5	Warning	2011-01-01T00:00:11+00:00	Switch just made a warm boot
6	Info	2011-01-01T00:00:11+00:00	topologyChange
7	Notice	2011-01-01T00:00:15+00:00	LINK-UPDOWN: Interface Vlan 1, changed state to up.
8	Warning	2011-01-01T00:00:18+00:00	Port 4 PoE PD on
9	Warning	2011-01-01T00:00:18+00:00	Port 7 PoE PD on
10	Info	2019-06-15T02:58:00+00:00	SYS-FIRMWARE: New firmware active: SISPM1040-582-LRT (standalone) v7.10.1994

4-1.4 Detailed Log

Switch system detailed log information is provided here. To display the detailed log in the web UI:

1. Click Monitor, System and Detailed Log.
2. View the log information.

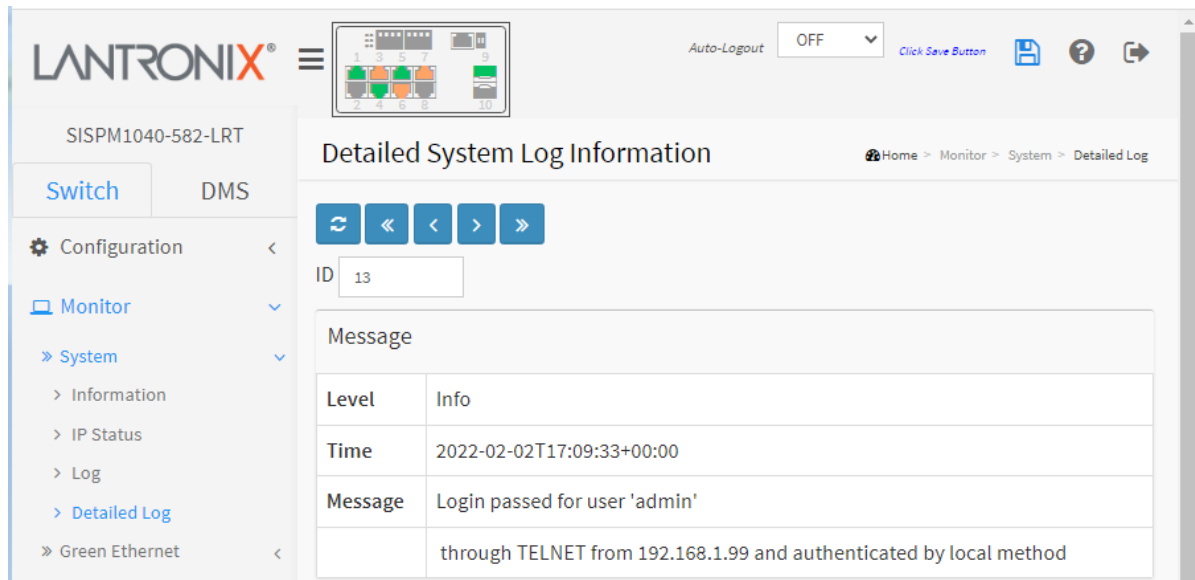


Figure 4-1.4: Detailed System Log Information

Parameter descriptions:

ID : The ID (≥ 1) of the system log entry.

Message : The detailed message of the system log entry.

Level : level of the system log entry. These level types are supported:

Emerg: The system log entry is belonged emergency level.

Alert: The system log entry is belonged alert level.

Crit: The system log entry is belonged critical level.

Error: The system log entry is belonged error level.

Warning: The system log entry is belonged warning level.

Notice: The system log entry is belonged notice level.

Info: The system log entry is belonged information level.

Debug: The system log entry is belonged debug level.

Time : Displays the log record by device time. The date and time of the system log entry.

Message : Displays the log detail message. The message of the system log entry.

Buttons

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

<<: Updates the system log entries to the first available entry ID

<: Updates the system log entry to the previously available entry ID

>: Updates the system log entry to the next available entry ID

>>: Updates the system log entry to the last available entry ID.



4-2 Green Ethernet

4-2.1 Port Power Savings

This page displays the current Port Power Savings status. To display the port power saving in the web UI:

1. Click Monitor, Green Ethernet, Port Power Savings.
2. View the displayed data.

Port	Link	EEE Cap	EEE Ena	LP EEE Cap	EEE Savings	ActiPhy Savings	PerfectReach Savings
1	●	✓	✗	✓	✗	✗	✗
2	●	✓	✗	✗	✗	✗	✗
3	●	✓	✗	✗	✗	✗	✗
4	●	✓	✗	✗	✗	✗	✗
5	●	✓	✗	✓	✗	✗	✗
6	●	✓	✗	✓	✗	✗	✗
7	●	✓	✗	✗	✗	✗	✗
8	●	✓	✗	✗	✗	✗	✗
9	●	✗	✗	✗	✗	✗	✗
10	●	✗	✗	✗	✗	✗	✗

Figure 4-2.1: Port Power Savings Status

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

Link : Shows if the link is up for the port (green = link up, red = link down).

EEE cap : Shows if the port is EEE capable.

EEE Ena : Shows if EEE is enabled for the port (reflects the settings at the Port Power Savings configuration page).

LP EEE cap : Shows if the link partner is EEE capable.

EEE Savings : Shows if the system is currently saving power due to EEE. When EEE is enabled, the system will power down if no frame has been received or transmitted in 5 uSeconds.

ActiPhy Savings : Shows if the system is currently saving power due to ActiPhy.

PerfectReach Savings : Shows if the system is currently saving power due to PerfectReach.

Buttons

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

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

4-3 Ports

The Ports sub-menus let you monitor various port parameters.

4-3.1 Traffic Overview

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

To display the Port Statistics Overview in the web UI:

1. Click Monitor, Ports, Traffic Overview.
2. You can click a linked Port number to view that port's detailed statistics.
3. Use the Auto-refresh, Refresh, or Clear buttons as needed.

The screenshot shows the 'Port Statistics Overview' page in the Lantronix web UI. The page title is 'Port Statistics Overview' and the breadcrumb is 'Home > Monitor > Ports > Traffic Overview'. There are buttons for 'Auto-refresh' (checkbox), 'Refresh' (circular arrow), and 'Clear' (eraser). The table below shows the statistics for 10 ports.

Port	Packets		Bytes		Errors		Drops		Filtered
	Received	Transmitted	Received	Transmitted	Received	Transmitted	Received	Transmitted	Received
1	7875	4472611	1598465	372965519	0	0	0	0	0
2	0	0	0	0	0	0	0	0	0
3	188902	4315098	53549534	342644423	0	0	0	0	2
4	497069	4658933	103797750	509700412	0	0	0	0	106
5	0	4440806	0	370185428	0	0	0	0	0
6	175697	4347443	82660516	340291767	0	0	0	0	0
7	25114	4416691	8687860	361878274	0	0	0	0	0
8	0	0	0	0	0	0	0	0	0
9	4440232	7877	370589304	1598711	0	0	0	0	13
10	0	0	0	0	0	0	0	0	0

Figure 4-3.1: Port Statistics Overview

Parameter descriptions:

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

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

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

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

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

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

Buttons

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

Refresh: Click to refresh the page immediately.

Clear: Clears the counters for all ports.

4-3.2 QoS Statistics

This page provides statistics for the different queues for all switch ports.

To display the Queuing Counters in the web UI:

1. Click Monitor, Ports, QoS Statistics.
2. To automatically refresh the information check the Auto-refresh checkbox.
3. Click Refresh to immediately refresh the counters or click Clear to clear all information.

The screenshot shows the 'Queuing Counters' page in the Lantronix web UI. The page title is 'Queuing Counters' and the breadcrumb is 'Home > Monitor > Ports > QoS Statistics'. There is an 'Auto-Logout' dropdown set to 'OFF', a 'Click Save Button' link, and icons for help and refresh. The left sidebar shows the navigation menu with 'Monitor' selected and 'QoS Statistics' highlighted. The main content area has an 'Auto-refresh' checkbox (unchecked) and two buttons: a blue refresh button and a red clear button. Below these is a table with 17 columns: Port, Q0 (Rx, Tx), Q1 (Rx, Tx), Q2 (Rx, Tx), Q3 (Rx, Tx), Q4 (Rx, Tx), Q5 (Rx, Tx), Q6 (Rx, Tx), and Q7 (Rx, Tx). The table contains 10 rows of data for ports 1 through 10.

Port	Q0		Q1		Q2		Q3		Q4		Q5		Q6		Q7	
	Rx	Tx	Rx	Tx	Rx	Tx	Rx	Tx	Rx	Tx	Rx	Tx	Rx	Tx	Rx	Tx
1	7876	347779	0	0	0	0	0	0	0	0	0	0	0	0	0	4125464
2	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
3	188924	215888	0	0	0	0	0	0	0	0	0	0	0	0	0	4099833
4	497167	254542	0	0	0	0	0	0	0	0	0	0	0	0	0	4405052
5	0	346709	0	0	0	0	0	0	0	0	0	0	0	0	0	4094728
6	175721	247052	0	0	0	0	0	0	0	0	0	0	0	0	0	4101011
7	25119	322754	0	0	0	0	0	0	0	0	0	0	0	0	0	4094575
8	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
9	4440865	0	0	0	0	0	0	0	0	0	0	0	0	0	0	7878
10	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0

Figure 4-3.2: Queuing Counters

Parameter descriptions:

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

Qn : The Queue number; there are 8 QoS queues per port (Q0-Q7). Q0 is the lowest priority queue.

Rx/Tx : The number of received and transmitted packets per queue.

Buttons

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

Refresh: Click to immediately refresh the page.

Clear: Clears the counters for all ports.

4-3.3 QCL Status

This page displays the QCL status of QCL users as configured at Configuration > QoS > QoS Control List.

Each row describes a defined QCE. It is a conflict if a specific QCE is not applied to the hardware due to hardware limitations. The maximum number of QCEs is 256 per switch. To display QoS Control List Status in the web UI:

1. Click Monitor, Ports, QCL Status.
2. At the User select dropdown select the set of users to display (Combined, Static, Voice VLAN, DMS, or Conflict).
3. Click the Refresh button to immediately refresh the page Information.

User	QCE	Port	Frame Type	Action						Conflict
				CoS	DPL	DSCP	PCP	DEI	Policy	
Static	1	Any	Any	0	Default	Default	Default	Default	Default	No
Static	2	Any	EtherType	3	Default	Default	Default	Default	Default	No
Static	3	Any	IPv4	0	Default	Default	Default	Default	Default	No
Voice VLAN	1	None	Any	0	Default	Default	Default	Default	Default	No

Figure 4-3.3: QoS Control List Status

Parameter descriptions:

User : Indicates the QCL user.

QCE : Indicates the index of QCE.

Port : Indicates the list of ports configured with the QCE.

Frame Type : Indicates the type of frame to look for incoming frames. 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 Drop Eligible Indicator value.

Policy: Classify ACL Policy number.

Conflict : Displays Conflict status of QCL entries (Yes or No). 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 H/W resources required to add QCL entry on pressing 'Resolve Conflict' button.

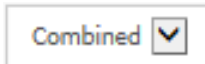
Buttons



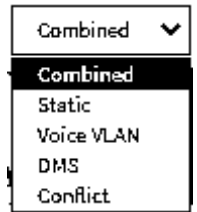
Auto-refresh: Check this box to refresh the page automatically every 3 seconds.

Refresh: Click to refresh the page immediately.

Resolve Conflict: Click to release the resources required to add QCL entry, if the Conflict status for any QCL entry is 'Yes'.



User select dropdown : Select the QCL status to be displayed from this drop down list (Combined, Static, Voice Vlan, DMS, Conflict).



4-3.4 Detailed Statistics

This page provides detailed traffic statistics for a specific switch port. Use the port select box to select which switch port details to display. The displayed counters are the totals for receive and transmit, the size counters for receive and transmit, and the error counters for receive and transmit.

To display per-port detailed Statistics Overview in the web UI:

1. Click Monitor, Ports, Detailed Port Statistics
2. Scroll the Port Index to select which port you want to show the detailed Port statistics overview.
4. To automatically refresh the information check the Auto-refresh checkbox.
5. Click Refresh to refresh the port detailed statistics or clear all information when you click Clear.

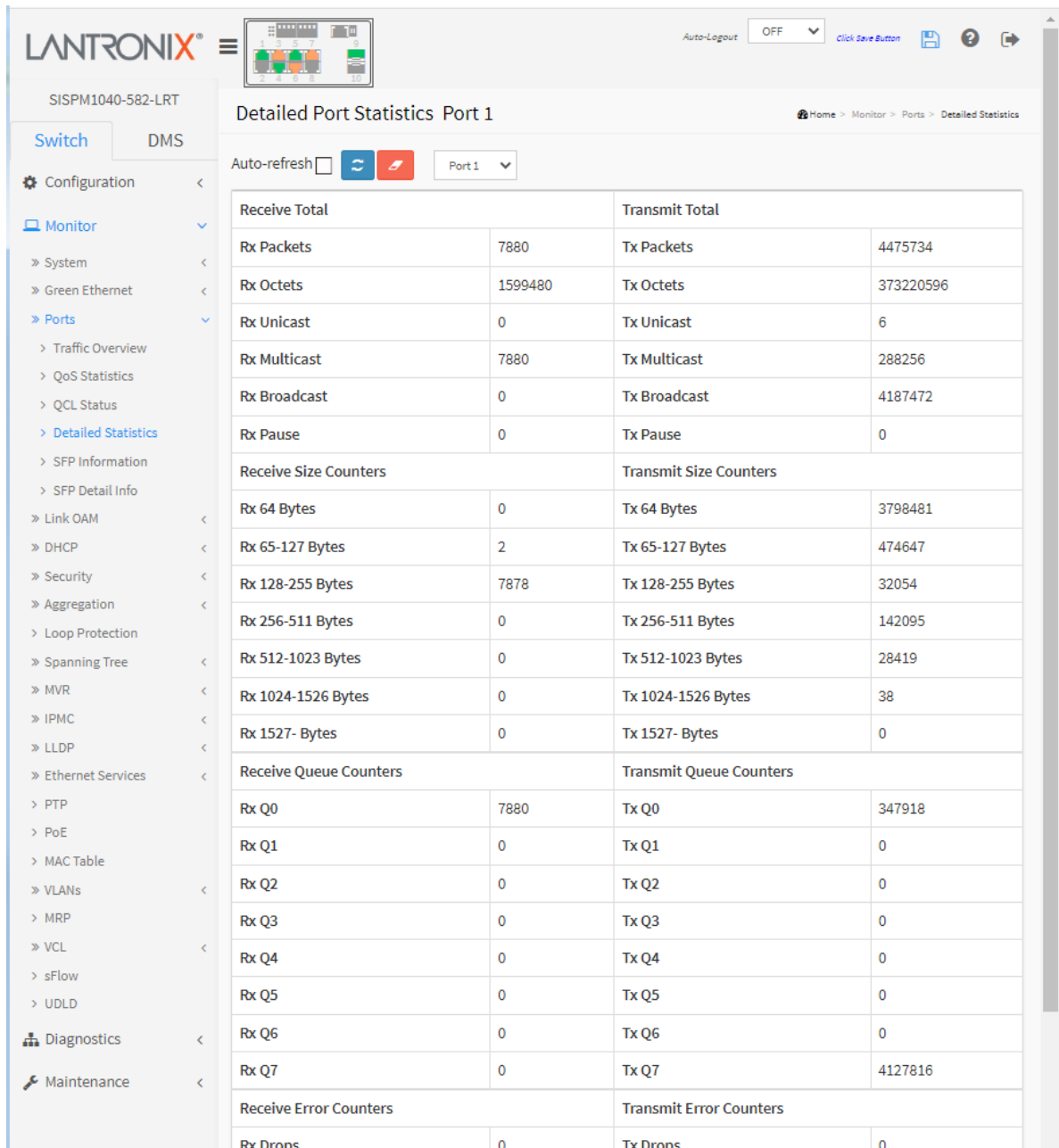


Figure 4-3.4: Detailed Port Statistics

Parameter descriptions:**Receive Total and Transmit Total** :

Rx and Tx Packets : The number of received and transmitted (good and bad) packets.

Rx and Tx Octets : The number of received and transmitted (good and bad) bytes. Includes FCS but excludes framing bits.

Rx and Tx Unicast : The number of received and transmitted (good and bad) unicast packets.

Rx and Tx Multicast : The number of received and transmitted (good and bad) multicast packets.

Rx and Tx Broadcast : The number of received and transmitted (good and bad) broadcast packets.

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

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

Receive and Transmit Queue Counters : The number of received and transmitted packets per input and output queue.

Receive Error Counters :

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

Rx CRC/Alignment : The number of frames received with CRC or alignment errors.

Rx Undersize : The number of short 1 frames received with valid CRC.

Rx Oversize : The number of long 2 frames received with valid CRC.

Rx Fragments : The number of short 1 frames received with invalid CRC.

Rx Jabber : The number of long 2 frames received with invalid CRC.

Rx Filtered : The number of received frames filtered by the forwarding process. Short frames are frames that are smaller than 64 bytes. Long frames are frames that are longer than the configured maximum frame length for this port.

Transmit Error Counters

Tx Drops : The number of frames dropped due to output buffer congestion.

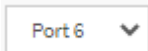
Tx Late/Exc. Coll. : The number of frames dropped due to excessive or late collisions.

Buttons

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

Refresh: Click to refresh the page immediately.

Clear: Clears the counters for the selected port.



: Port select box; use to select which port's data to view.

4-3.5 SFP Information

This page displays general SFP monitoring information. To display SFP information in the web UI:

1. Click Monitor, Ports, SFP Information.
2. View the displayed SFP Information.

The screenshot shows the Lantronix web interface for the SISPM1040-582-LRT device. The left sidebar contains a navigation menu with 'Monitor' expanded to 'Ports' and 'SFP Information' selected. The main content area displays 'SFP Information' with an 'Auto-refresh' checkbox and a refresh icon. Below is a table with the following data:

Port	Tx Central Wavelength	Bit Rate	Temperature	Vcc	Mon1 (Bias)	Mon2 (TxPwr)	Mon3 (RxPwr)
1							
2							
3							
4							
5							
6							
7							
8							
9	850	10 Gbps	51.06 C	3.32 V	5 mA	-2.77 dBm	-7.22 dBm
10	850	1000 Mbps	53.22 C	3.34 V	15 mA	-6.47 dBm	none

Figure 4-3.5: SFP Information

Parameter descriptions:

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

Tx Central Wavelength : Displays the nominal transmitter output wavelength in nm.

Bit rate : Displays the nominal bit rate of the transceiver.

Temperature : Displays the internally measured transceiver temperature. Temperature accuracy is vendor specific but must be better than 3 degrees Celsius over specified operating temperature and voltage.

Vcc : Displays the internally measured transceiver supply voltage. Accuracy is vendor specific but must be better than 3 percent of the manufacturer's nominal value over specified operating temperature and voltage. Note that in some transceivers, transmitter supply voltage and receiver supply voltage are isolated. In that case, only one supply is monitored. Refer to the device specification for more detail.

Mon1 (Bias) : Displays the measured TX bias current in uA. Accuracy is vendor specific but must be better than 10 percent of the manufacturer's nominal value over specified operating temperature and voltage.

Mon2 (TX PWR) : Displays the measured coupled TX output power in mW. Accuracy is vendor specific but must be better than 3dB over specified operating temperature and voltage. Data is assumed to be based on measurement of a laser monitor photodiode current. Data is not valid when the transmitter is disabled.

Mon3 (RX PWR) : Displays the measured received optical power in mW. Absolute accuracy is dependent upon the exact optical wavelength. For the vendor specified wavelength, accuracy should be better than 3dB over specified temperature and voltage. This accuracy should be maintained for input power levels up to the lesser of maximum transmitted or maximum received optical power per the appropriate standard. It should be maintained down to the minimum transmitted power minus cable plant loss (insertion loss or passive loss) per the appropriate standard. Absolute accuracy beyond this minimum required received input optical power range is vendor specific.

Buttons

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

Refresh: Click to refresh the page immediately.

3-3.6 SFP Detail Info

This page displays general SFP information and monitoring information. To monitor SFP Detail Information in the web UI:

1. Click Monitor, Port, and SFP Detail Info.
2. At the dropdown select the desired port.
3. View the displayed SFP Information.

The screenshot shows the Lantronix web UI for the SISPM1040-582-LRT device. The left navigation menu is expanded to 'Monitor' > 'Ports' > 'SFP Detail Info'. The main content area displays 'SFP Information for Port 9'. At the top of this section, there is an 'Auto-refresh' checkbox (unchecked) and a refresh icon, and a dropdown menu set to 'Port 9'. Below this is a table with the following data:

Connector Type	SFP or SFP Plus - LC
Fiber Type	Reserved
Tx Central Wavelength	850
Bit Rate	10 Gbps
Vendor OUI	00-c0-f2
Vendor Name	Transition
Vendor P/N	TN-10GSFP-SR
Vendor Revision	0001
Vendor Serial Number	8801095
Date Code	120731
Temperature	50.97 C
Vcc	3.32 V
Mon1 (Bias)	5 mA
Mon2 (TX PWR)	-2.77 dBm
Mon3 (RX PWR)	-7.24 dBm

Figure 4-3.6: SFP Information for a specified Port

Parameter descriptions:

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

Fiber Type : Displays the fiber channel transmission media.

Tx Central Wavelength : Displays the nominal transmitter output wavelength in nm.

Bit rate : Displays the nominal bit rate of the transceiver.

Vendor OUI : Displays the vendor IEEE company ID.

Vendor Name : Displays the vendor name.

Vendor P/N : Displays the vendor part number or product name.

Vendor Revision : Displays the vendor product revision.

Vendor Serial Number : Displays the vendor serial number for the transceiver.

Date Code : Displays the vendor's manufacturing date code.

Temperature : Displays the internally measured transceiver temperature. Temperature accuracy is vendor specific but must be better than 3 degrees Celsius over specified operating temperature and voltage.

Vcc : Displays the internally measured transceiver supply voltage. Accuracy is vendor specific but must be better than 3 percent of the manufacturer's nominal value over specified operating temperature and voltage. Note that in some transceivers, transmitter supply voltage and receiver supply voltage are isolated. In that case, only one supply is monitored. Refer to the device specification for more detail.

Mon1 (Bias) : Displays the measured TX bias current in uA. Accuracy is vendor specific but must be better than 10 percent of the manufacturer's nominal value over specified operating temperature and voltage.

Mon2 (TX PWR) : Displays the measured coupled TX output power in mW. Accuracy is vendor specific but must be better than 3dB over specified operating temperature and voltage. Data is assumed to be based on measurement of a laser monitor photodiode current. Data is not valid when the transmitter is disabled.

Mon3 (RX PWR) : Displays the measured received optical power in mW. Absolute accuracy is dependent upon the exact optical wavelength. For the vendor specified wavelength, accuracy should be better than 3dB over specified temperature and voltage. This accuracy should be maintained for input power levels up to the lesser of maximum transmitted or maximum received optical power per the appropriate standard. It should be maintained down to the minimum transmitted power minus cable plant loss (insertion loss or passive loss) per the appropriate standard. Absolute accuracy beyond this minimum required received input optical power range is vendor specific.

Buttons

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

Refresh: Click to refresh the page immediately.

4-4 Link OAM

4-4.1 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 counters can occur at re-initialization of the management system.

To monitor Link OAM Statistics in the web UI:

1. Click Monitor, Link OAM, Statistics.
2. Use the port select box to select which port's information to display.
3. View the displayed Statistics.

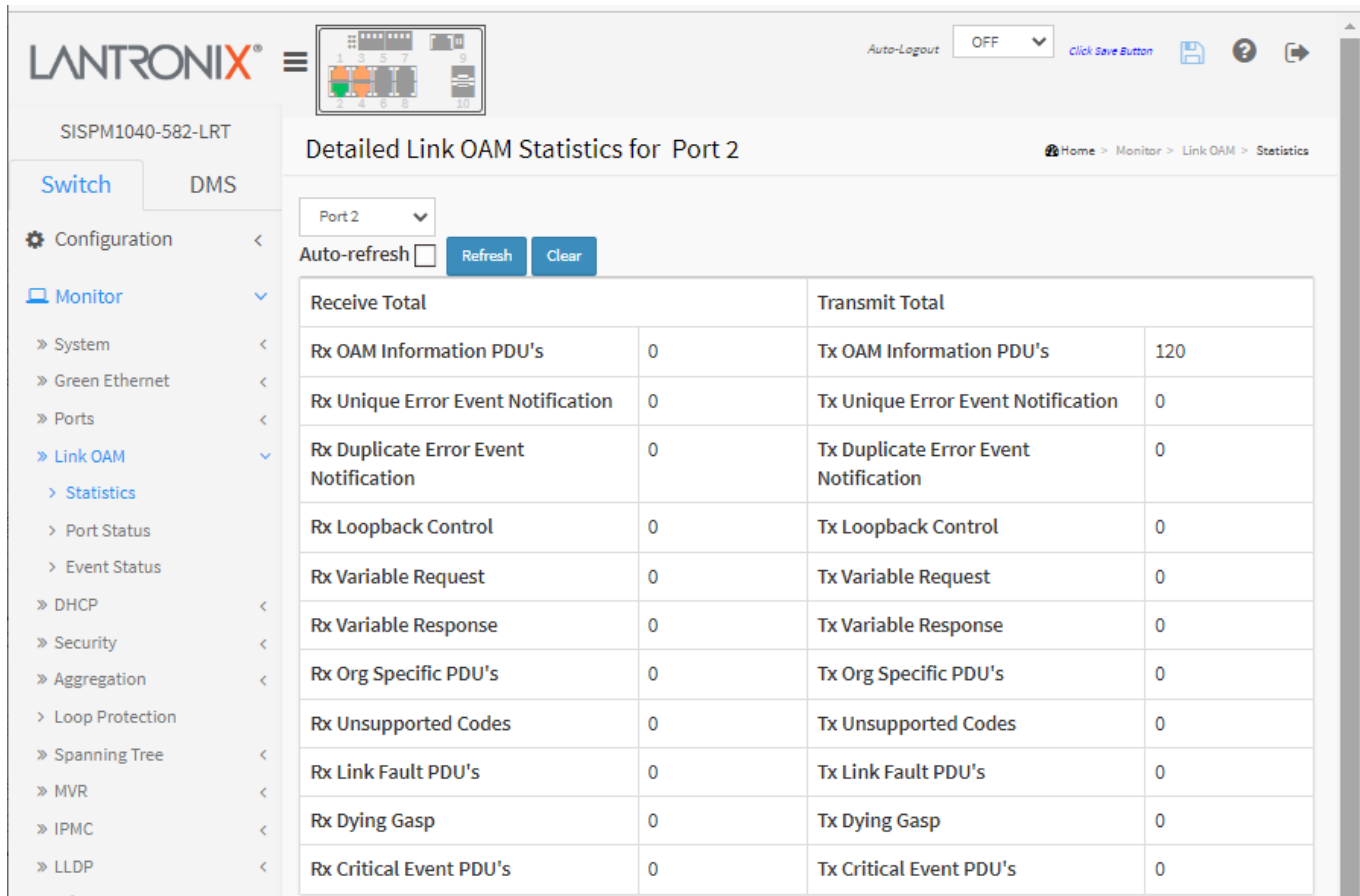


Figure 4-4.1: Detailed Link OAM Statistics

Parameter descriptions:

Receive Total and Transmit Total

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

Rx and Tx Unique Error Event Notification : 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 : 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 : The number of Loopback Control OAMPDUs received and transmitted on this interface.

Rx and Tx Variable Request : The number of Variable Request OAMPDUs received and transmitted on this interface.

Rx and Tx Variable Response : The number of Variable Response OAMPDUs received and transmitted on this interface.

Rx and Tx Org Specific PDU's : 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 PDU's : The number of Link fault PDU's received and transmitted on this interface.

Rx and Tx Dying Gasp : The number of Dying Gasp events received and transmitted on this interface.

Rx and Tx Critical Event PDU's : The number of Critical event PDUs received and transmitted on this interface.

Buttons

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

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

Clear: Clears the counters for the selected port.

Refresh: Click to refresh the page immediately.

4-4.2 Port Status

This page displays Link OAM configuration operational status. The displayed fields show the active configuration status for the selected port. To view detailed LOAM Port Status in the web UI:

1. Click Monitor, Link OAM, Port Status.
2. Use the port select box to select which port's information to display.
3. View the displayed Link OAM Status for the selected port.

The screenshot shows the 'Detailed Link OAM Status for Port 1' page. The left sidebar contains a navigation menu with 'Monitor' selected, and 'Link OAM' > 'Port Status' highlighted. The main content area features a 'Port 1' dropdown menu, an 'Auto-refresh' checkbox, and a 'Refresh' button. Below this is a table with the following data:

PDU Permission	Info exchange		
Discovery State	Active state		
Peer MAC Address	-----		
Local		Peer	
Mode	Active	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	Enabled	MIB Retrieval Support	-----
OAM PDU Size	1500	OAM PDU 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	-----

Figure 4-4.2: Detailed Link OAM Status

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", "Info exchange", or "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 if known, otherwise displays -----.

Local and Peer

Mode : The Mode in which the 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 configuration is retrieved from the PHY.

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

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

MIB Retrieval Support : If status i.e. enabled DTE supports sending Variable Response OAMPDUs.

OAM PDU Size : Represents the largest OAMPDU, in octets, supported by the DTE (e.g., 1500 octets). 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-OAMPDU's.

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 : The 24-bit Organizationally Unique Identifier (OUI) of the vendor.

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

Buttons

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

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

Refresh: Click to refresh the page immediately.

4-4.3 Event Status

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

To monitor detailed Link OAM Event Status in the web UI:

1. Click Monitor, Link OAM, Event Status.
2. Use the port select box to select which port's information to display.
3. View the displayed Link OAM Event status for the selected port.

The screenshot shows the 'Detailed Link OAM Link Status for Port 1' page. At the top, there is a 'Port 1' dropdown menu and an 'Auto-refresh' checkbox. Below this is a table with the following structure:

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

Figure 4-4.1: Link OAM Event Status

Parameter descriptions:

Port : The switch port number.

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

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

Frame error event window : This two-octet field indicates the duration of the period in terms of 100 ms intervals. 1) The default value is one second. 2) The lower bound is one second. 3) 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 in order for the event to be generated. 1) The default value is one frame error. 2) The lower bound is zero frame errors. 3) The upper bound is unspecified.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Symbol frame 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 Time Stamp : 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.

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

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

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

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

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

Buttons

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

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

Refresh: Click to refresh the page immediately.

4-5 DHCP

4-5.1 Server

DHCP Server is used to allocate network addresses and deliver configuration parameters to dynamically configured hosts called DHCP client.

4-5.1.1 Statistics

This page displays the database counters and the number of DHCP messages sent and received by DHCP server.

To display DHCP server Statistics in the web UI:

1. Click Monitor, DHCP, Server, and Statistics.
2. View the displayed information.

The screenshot shows the Lantronix web interface for the SISPM1040-582-LRT device. The left sidebar contains a navigation menu with 'Monitor' selected, and 'DHCP' > 'Server' > 'Statistics' highlighted. The main content area is titled 'DHCP Server Statistics' and includes an 'Auto-refresh' toggle (currently off) and a breadcrumb trail: Home > Monitor > DHCP > Server > Statistics.

The statistics are organized into four sections:

- Database Counters:** A table with three columns: Pool (0), Excluded IP Address (1), and Declined IP Address (0).
- Binding Counters:** A table with three columns: Automatic Binding (0), Manual Binding (0), and Expired Binding (0).
- DHCP Message Received Counters:** A table with five columns: DISCOVER (0), REQUEST (0), DECLINE (0), RELEASE (0), and INFORM (0).
- DHCP Message Sent Counters:** A table with three columns: OFFER (0), ACK (0), and NAK (0).

Figure 4-5.1.1: DHCP Server Statistics

Parameter descriptions:

Database Counters

Pool : The number of pools.

Excluded IP Address : The number of excluded IP address ranges.

Declined IP Address : The number of sec lined IP addresses.

Binding Counters

Automatic Binding : Number of bindings with network-type pools.

Manual Binding : Number of bindings that administrator assigns an IP address to a client. That is, the pool is of host type.

Expired Binding : Number of bindings that their lease time expired or they are cleared from Automatic/Manual type bindings.

DHCP Message Received Counters

DISCOVER : Number of DHCP DISCOVER messages received.

REQUEST : Number of DHCP REQUEST messages received.

DECLINE : Number of DHCP DECLINE messages received.

RELEASE : Number of DHCP RELEASE messages received.

INFORM : Number of DHCP INFORM messages received.

DHCP Message Sent Counters

OFFER : Number of DHCP OFFER messages sent.

ACK : Number of DHCP ACK messages sent.

NAK : Number of DHCP NAK messages sent.

4-5.1.2 Binding

This page displays bindings generated for DHCP clients. To display DHCP Server Binding IP in the web UI:

1. Click Monitor, DHCP, Server, and Binding.
2. View the displayed information.

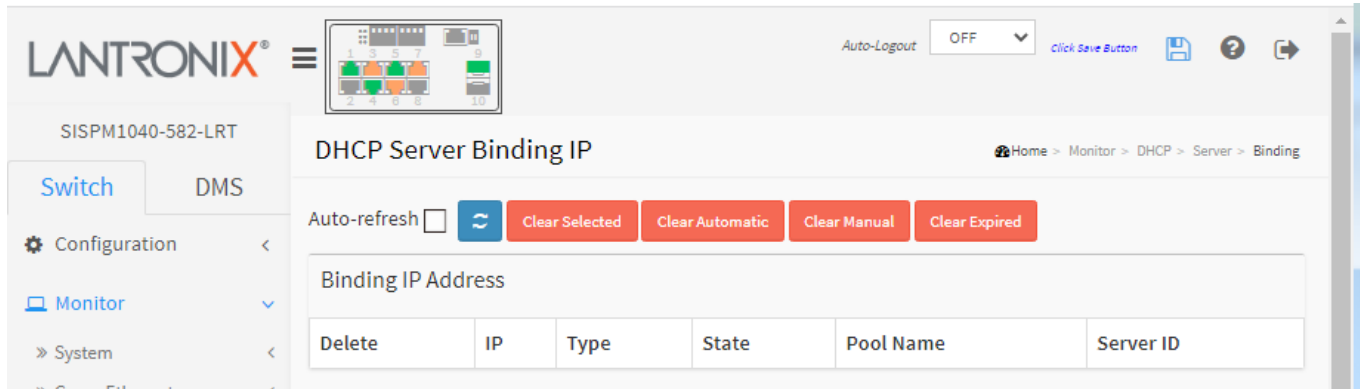


Figure 4-5.1.2: DHCP Server Binding IP

Parameter descriptions:

IP : IP address allocated to DHCP client.

Type : Type of binding. Possible types are Automatic, Manual, and Expired.

State : State of binding. Possible states are Committed, Allocated, and Expired.

Pool Name : The pool that generates the binding.

Server ID : Server IP address to service the binding.

Buttons

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

Refresh: Click to refresh the page immediately.

Clear Selected : Click to clear selected bindings. If the selected binding is Automatic or Manual, then it is changed to be Expired. If the selected binding is Expired, then it is freed.

Clear Automatic : Click to clear all Automatic bindings and Change them to Expired bindings.

Clear Manual: Click to clear all Manual bindings and Change them to Expired bindings.

Clear Expired: Click to clear all Expired bindings and free them.

4-5.1.3 Declined IP

This page displays declined IP addresses. To monitor DHCP Server Declined IP in the web UI:

1. Click Monitor, DHCP, Server, Declined IP.
2. View the displayed information.

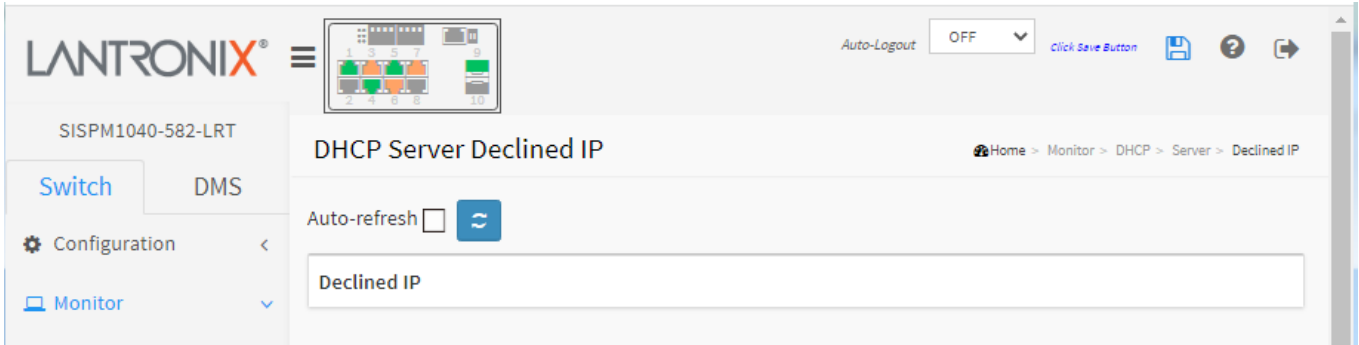


Figure 4-5.1.3: DHCP Server Declined IP

Parameter descriptions:

IP : IP address allocated to DHCP client.

Type : Type of binding. Possible types are Automatic, Manual, and Expired.

State : State of binding. Possible states are Committed, Allocated, and Expired.

Pool Name : The pool that generates the binding.

Server ID : Server IP address to service the binding.

Buttons

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

Refresh: Click to refresh the page immediately.

4-5.2 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. Click Monitor, DHCP, Snooping table
2. Check Auto-refresh.
3. Click Refresh to refresh the port detailed statistics or clear all information when you click “Clear”.

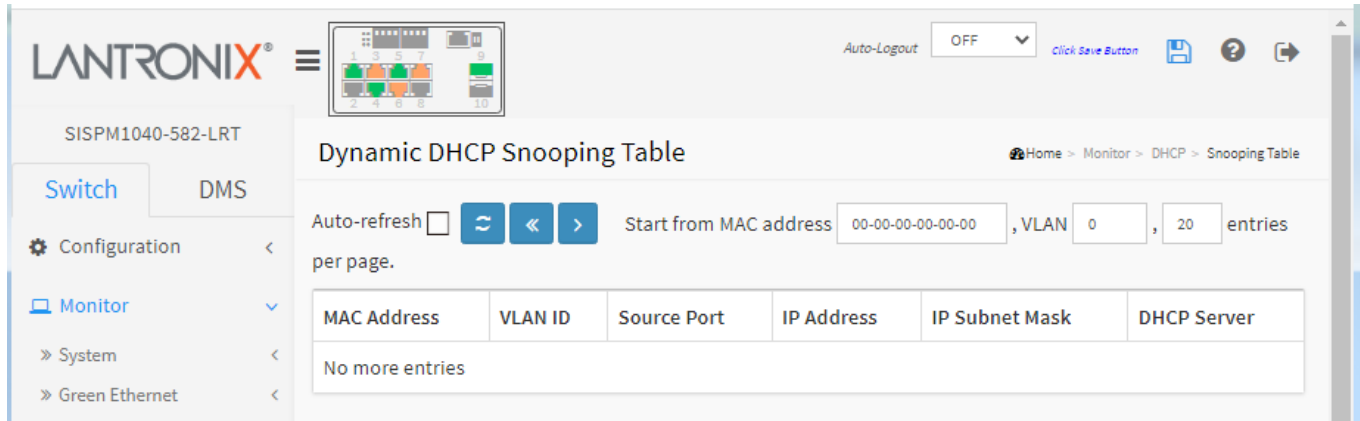


Figure 4-5.2: Dynamic DHCP Snooping Table

Parameter descriptions:

MAC Address : User MAC address of the entry.

VLAN ID : VLAN-ID in which the DHCP traffic is permitted.

Source Port: Switch Port Number for which the entries are displayed.

IP Address : User IP address of the entry.

IP Subnet Mask : User IP subnet mask of the entry.

DHCP Server Address : DHCP Server address of the entry.

Buttons

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

Refresh: Click to refresh the page immediately.

Clear: Click to

4-5.3 Relay Statistics

This page provides statistics for DHCP relay. To monitor DHCP Relay statistics in the web UI:

1. Click Monitor, DHCP, Relay Statistics.
2. Check Auto-refresh.
3. Click Refresh to refresh the port detailed statistics or clear all information when you click Clear.

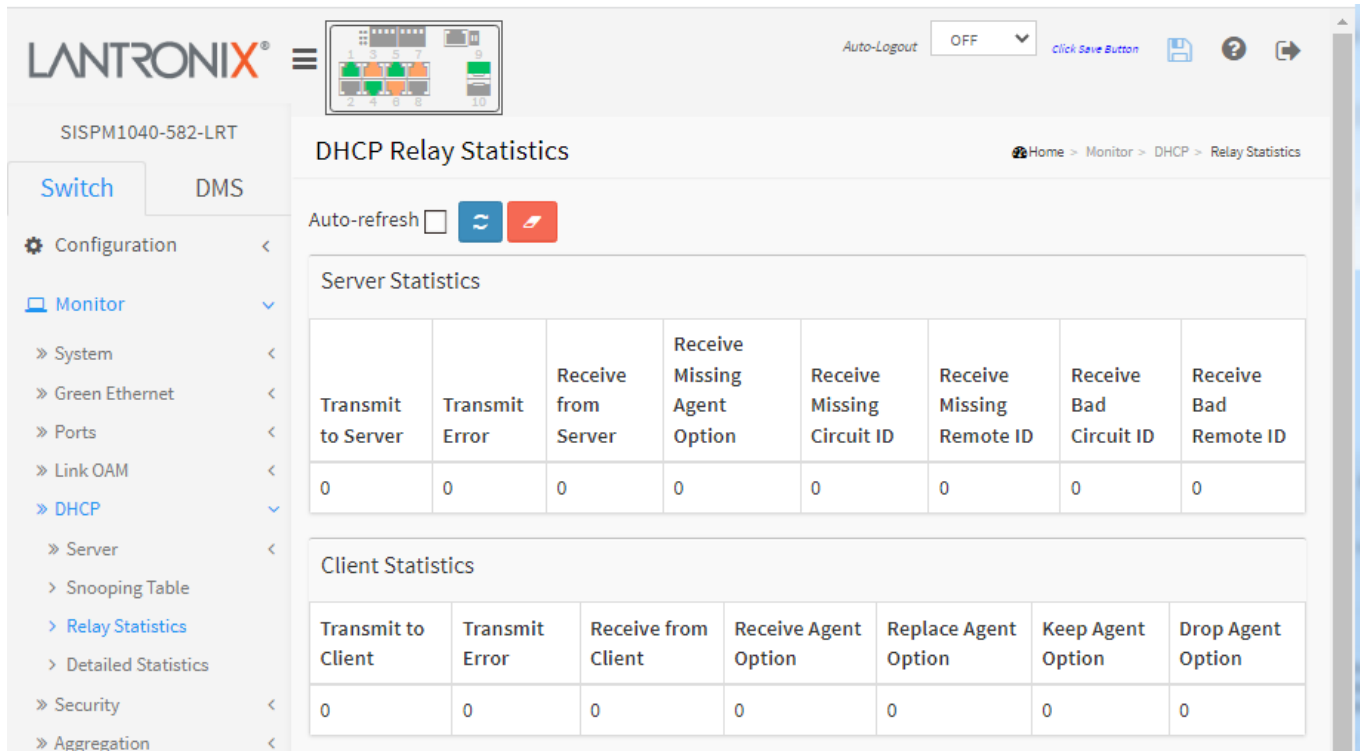


Figure 4-5.3: DHCP Relay Statistics

Parameter descriptions:

Server Statistics

Transmit to Server : The number of packets that are relayed from client to server.

Transmit Error : The number of packets that resulted in errors while being sent to clients.

Receive from Server : The number of packets received from server.

Receive Missing Agent Option: The number of packets received without agent information options.

Receive Missing Circuit ID : The number of packets received with the Circuit ID option missing.

Receive Missing Remote ID : The number of packets received with the Remote ID option missing.

Receive Bad Circuit ID: The number of packets whose Circuit ID option did not match known circuit ID.

Receive Bad Remote ID : The number of packets whose Remote ID option did not match known Remote ID.

Client Statistics

Transmit to Client : The number of relayed packets from server to client.

Transmit Error : The number of packets that resulted in error while being sent to servers.

Receive from Client : The number of received packets from server.

Receive Agent Option : The number of received packets with relay agent information option.

Replace Agent Option : The number of packets which were replaced with relay agent information option.

Keep Agent Option : The number of packets whose relay agent information was retained.

Drop Agent Option : The number of packets that were dropped which were received with relay agent information.

Buttons

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

Refresh: Click to refresh the page immediately.

Clear: Click to clear webpage statistics.

4-5.4 Detailed Statistics

This page provides statistics for DHCP snooping. Notice that the normal forward per-port TX statistics isn't increased if the incoming DHCP packet is done by L3 forwarding mechanism. Clearing the statistics on a specific port may not take effect on global statistics since it gathers the different layer overview.

To monitor DHCP Detailed statistics in the web UI:

1. Click Monitor, DHCP, Detailed Statistics
2. Check "Auto-refresh".
3. Click "Refresh" to refresh the port detailed statistics or clear all information when you click "Clear".

The screenshot shows the 'DHCP Detailed Statistics Port 1' page. At the top, there is an 'Auto-logout' dropdown set to 'OFF' and a 'Click Save Button' link. Below the header, the page title is 'DHCP Detailed Statistics Port 1' with a breadcrumb trail: Home > Monitor > DHCP > Detailed Statistics. The interface includes an 'Auto-refresh' checkbox (unchecked) and a 'Refresh' button (red). There are also dropdown menus for 'Combined' and 'Port 1'. The main content is a table with two columns: 'Receive Packets' and 'Transmit Packets'. Each column has a sub-column for the specific DHCP message type and a numerical value. All values are currently 0.

Receive Packets		Transmit Packets	
Rx Discover	0	Tx Discover	0
Rx Offer	0	Tx Offer	0
Rx Request	0	Tx Request	0
Rx Decline	0	Tx Decline	0
Rx ACK	0	Tx ACK	0
Rx NAK	0	Tx NAK	0
Rx Release	0	Tx Release	0
Rx Inform	0	Tx Inform	0
Rx Lease Query	0	Tx Lease Query	0
Rx Lease Unassigned	0	Tx Lease Unassigned	0
Rx Lease Unknown	0	Tx Lease Unknown	0
Rx Lease Active	0	Tx Lease Active	0
Rx Discarded Checksum Error	0		
Rx Discarded from Untrusted	0		

Figure 4-5.4: DHCP Detailed Statistics

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.

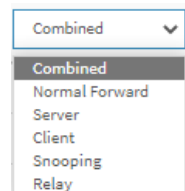
Buttons

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

Refresh: Click to refresh the page immediately.

Clear: Click to clear webpage statistics.

User Select box : Dropdown to select which user information to display (Combined, Normal Forward, Server, Client, Snooping, or Relay).



A dropdown menu with a blue border and a downward arrow. The selected item is 'Combined'. The list of items includes: Combined, Normal Forward, Server, Client, Snooping, and Relay.

Port Select box : Dropdown to select which Port's information to display.



A dropdown menu with a blue border and a downward arrow. The selected item is 'Port 1'. The list of items includes: Port 1, Port 2, Port 3, Port 4, Port 5, Port 6, Port 7, Port 8, Port 9, and Port 10.

4-6 Security

4-6.1 Access Management Statistics

This page displays statistics for access management. To monitor Access Management Statistics in the web UI:

1. Click Monitor, Security, Access Management Statistics.
2. Check “Auto-refresh”.
3. Click “Refresh” to refresh the port detailed statistics or clear all information when you click “Clear”.

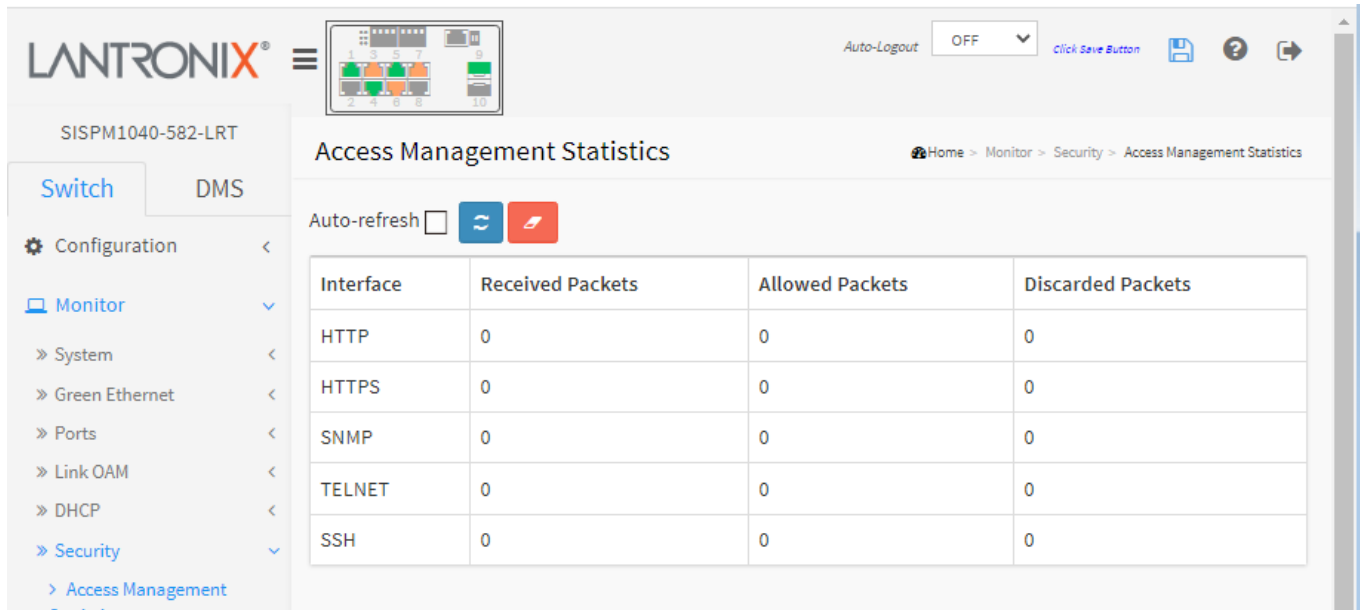


Figure 4-6.1: Access Management Statistics

Parameter descriptions:

Interface : The interface type through which the remote host can access the switch.

Received Packets : Number of received packets from the interface when access management mode is enabled.

Allowed Packets : Number of allowed packets from the interface when access management mode is enabled.

Discarded Packets : Number of discarded packets from the interface when access management mode is enabled.

Buttons

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

Refresh: Click to refresh the page immediately.

Clear: Clears the counters for the selected port.

4-6.2 Network

4-6.2.1 Port Security

4-6.2.1.1 Switch

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 chooses to block it, it will be blocked until that user module decides otherwise. The status page is divided into two sections; one with a legend of user modules and one with the actual port status.

To monitor a Port Security Switch Status Configuration in the web interface:

1. Click Monitor, Security, Network, Port Security, then Switch
2. Check “Auto-refresh”.
3. Click “Refresh” to refresh the port detailed statistics.

The screenshot shows the Lantronix web interface for the device SISPM1040-582-LRT. The page title is 'Port Security Switch Status'. The breadcrumb trail is: Home > Monitor > Security > Network > Port Security > Switch. The 'Auto-refresh' checkbox is unchecked. The 'User Module Legend' table is as follows:

User Module Name	Abbr
Limit Control	L
802.1X	8
Voice VLAN	V

The 'Port Status' table is as follows:

Port	Users	State	MAC Count	
			Current	Limit
1	---	Disabled	-	-
2	---	Disabled	-	-
3	---	Disabled	-	-
4	---	Disabled	-	-
5	---	Disabled	-	-
6	---	Disabled	-	-
7	---	Disabled	-	-
8	---	Disabled	-	-
9	---	Disabled	-	-
10	---	Disabled	-	-

Figure 4-6.2.1.1: Port Security Switch Status

Parameter descriptions:

User Module Legend : The legend shows all user modules that may request Port Security services.

User Module Name : The full name of a module that may request Port Security services.

Abbr : A one-letter abbreviation of the user module. This is used in the Users column in the port status table.

L = Limit Control, **S** = 802.1X, **V** = Voice VLAN.

Port Status : The table has one row for each port on the switch and several columns:

Port : The port number for which the status applies. Click the port number to see the status for this particular port.

Users : Each of the user modules has a column that shows whether that module has enabled Port Security or not. A '-' means that the corresponding user module is not enabled, whereas a letter indicates that the user module abbreviated by that letter (see Abbr above) has enabled port security.

State : Shows the current state of the port. It can take one of four values:

Disabled: No user modules are currently using the Port Security service.

Ready: The Port Security service is in use by at least one user module and is awaiting frames from unknown MAC addresses to arrive.

Limit Reached: The Port Security service is enabled by at least the Limit Control user module, and that module has indicated that the limit is reached, and no more MAC addresses should be taken in.

Shutdown: The Port Security service is enabled by at least the Limit Control user module, and that module has indicated that the limit is exceeded. No MAC addresses can be learned on the port until it is administratively re-opened on the Limit Control configuration Web-page.

MAC Count (Current, Limit) : The two columns indicate the number of currently learned MAC addresses (forwarding as well as blocked) 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 the Limit Control user module is not enabled on the port, the Limit column will show a dash (-).

Buttons

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

Refresh: Click to refresh the page immediately.

4-6.2.1.2 Port

This page shows the MAC addresses secured by the Port Security module. Port Security is a module with no direct configuration. Configuration comes indirectly from other modules - the user modules. When a user module has enabled port security on a port, the port is set-up for software-based learning. In this mode, frames from unknown MAC addresses are passed on to the port security module, which in turn asks all user modules whether to allow this new MAC address to forward or block it. For a MAC address to be set in the forwarding state, all enabled user modules must unanimously agree on allowing the MAC address to forward. If only one chooses to block it, it will be blocked until that user module decides otherwise.

To monitor Port Security status in the web UI:

1. Click Monitor, Security, Network, Port Security, Port.
2. Specify the Port which you want to monitor.
3. Check "Auto-refresh".
4. Click "Refresh" to refresh the port detailed statistics.

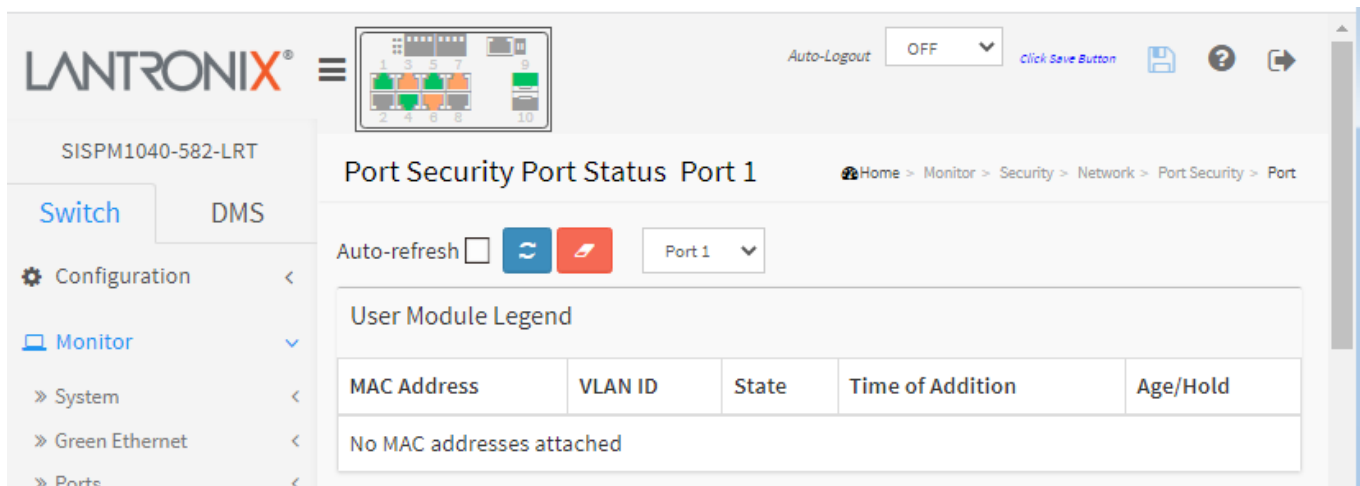


Figure 4-6.2.1.2: Port Security Port Status

Parameter descriptions:

MAC Address & VLAN ID : The MAC address and VLAN ID seen on this port. If no MAC addresses are learned, a single row stating "No MAC addresses attached" displays.

State : Indicates whether the corresponding MAC address is blocked or forwarding. In the blocked state, it will not be allowed to transmit or receive traffic.

Time of Addition : Shows the date and time when this MAC address was first seen on the port.

Age/Hold : If at least one user module has decided to block this MAC address, it will stay in the blocked state until the hold time (measured in seconds) expires. If all user modules have decided to allow this MAC address to forward, and aging is enabled, the Port Security module will periodically check that this MAC address still forwards traffic. If the age period (measured in seconds) expires and no frames have been seen, the MAC address will be removed from the MAC table. Otherwise a new age period will begin.

If aging is disabled or a user module has decided to hold the MAC address indefinitely, a dash (-) will be shown.

Buttons

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

Refresh: Click to refresh the page immediately.

Clear : Click to clear the table.

: Use the port select box to select which port to show status for.

4-6.2.2 NAS

4-6.2.2.1 Switch

This page shows each port NAS status information of the switch. The status includes Admin State Port State, Last Source, Last ID, QoS Class, and Port VLAN ID. To display NAS Switch Status in the web UI:

1. Click Monitor, Security, Network, NAS, and then Port.
2. Check Auto-refresh.
3. Click Refresh to refresh the port detailed statistics.

The screenshot shows the Lantronix web interface for the device SISPM1040-582-LRT. The main heading is "Network Access Server Switch Status". Below the heading, there is an "Auto-refresh" checkbox which is currently unchecked, and a refresh icon. A table displays the status for 10 ports. The table has the following columns: Port, Admin State, Port State, Last Source, Last ID, QoS Class, and Port VLAN ID. All ports (1 through 10) have an Admin State of "Force Authorized" and a Port State of "Globally Disabled". The Last Source, Last ID, and Port VLAN ID columns are empty for all ports. The QoS Class column contains a hyphen (-) for all ports. The left sidebar shows a navigation menu with "NAS" selected, and "Switch" highlighted under it. The top right of the interface includes an "Auto-Logout" dropdown set to "OFF", a "Click Save Button" link, and several utility icons.

Port	Admin State	Port State	Last Source	Last ID	QoS Class	Port VLAN ID
1	Force Authorized	Globally Disabled			-	
2	Force Authorized	Globally Disabled			-	
3	Force Authorized	Globally Disabled			-	
4	Force Authorized	Globally Disabled			-	
5	Force Authorized	Globally Disabled			-	
6	Force Authorized	Globally Disabled			-	
7	Force Authorized	Globally Disabled			-	
8	Force Authorized	Globally Disabled			-	
9	Force Authorized	Globally Disabled			-	
10	Force Authorized	Globally Disabled			-	

Figure 4-6.2.2.1: Network Access Server Switch Status

Parameter descriptions:

Port : The switch port number. Click a linked port number to go to the detailed NAS statistics for this port.

Admin State : The port's current administrative state. Refer to NAS Admin State for a description of possible values.

Port State : The current state of the port. Refer to NAS Port State for a description of the individual states.

Last Source : The source MAC address carried in the most recently received EAPOL (Extensible Authentication Protocol over LAN) frame for EAPOL-based authentication, and the most recently received frame from a new client for MAC-based authentication.

Last ID : The user name (supplicant identity) carried in the most recently received Response Identity EAPOL frame for EAPOL-based authentication, and the source MAC address from the most recently received frame from a new client for MAC-based authentication.

QoS Class : QoS Class assigned to the port by the RADIUS server if enabled.

Port VLAN ID : The VLAN ID that NAS has put the port in. The field is blank if the Port VLAN ID is not overridden by NAS. If the VLAN ID is assigned by the RADIUS server, "(RADIUS-assigned)" is appended to the VLAN ID.

Buttons

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

Refresh: Click to refresh the page immediately.

4-6.2.2.2 Port

This page shows detailed NAS statistics for a specific switch port running EAPOL-based IEEE 802.1X authentication. For MAC-based ports, it shows selected backend server (RADIUS Authentication Server) statistics only.

A NAS (Network Access Server) is meant to act as a gateway to guard access to a protected source. A client connects to the NAS, and the NAS connects to another resource asking whether the client's supplied credentials are valid. Based on the answer, the NAS then allows or disallows access to the protected resource. An example of a NAS implementation is IEEE 802.1X.

IEEE 802.1X is an IEEE standard for port-based Network Access Control. It provides authentication to devices attached to a LAN port, establishing a point-to-point connection or preventing access from that port if authentication fails. With 802.1X, access to all switch ports can be centrally controlled from a server, which means that authorized users can use the same credentials for authentication from any point within the network.

802.1X authentication involves three parts: a supplicant, an authenticator, and an authentication server. The supplicant is a client device (such as a laptop) that wishes to attach to the LAN/WLAN. The term 'supplicant' is also used interchangeably to refer to the software running on the client that provides credentials to the authenticator. The authenticator is a network device which provides a data link between the client and the network and can allow or block network traffic between the two, such as an Ethernet switch or wireless access point; and the authentication server is typically a trusted server that can receive and respond to requests for network access, and can tell the authenticator if the connection is to be allowed, and various settings that should apply to that client's connection or setting. Authentication servers typically run software supporting the RADIUS and EAP protocols. The authentication server software may be running on the authenticator hardware.

To view NAS Port Statistics in the web UI:

1. Click Monitor, Security, Network, NAS, then Port.
2. Use the port select box to select which port's details are to be displayed.

The screenshot shows the 'NAS Statistics Port 1' page in the web UI. The left sidebar contains a navigation menu with 'Monitor' selected, and 'Security' > 'Network' > 'NAS' > 'Port' selected. The main content area has a breadcrumb trail: Home > Monitor > Security > Network > NAS > Port. Below the breadcrumb, there are 'Auto-refresh' controls (checkbox, refresh icon, 'Clear' button) and a 'Port 1' dropdown menu. The 'Port State' section shows a table with 'Admin State' (Force Authorized) and 'Port State' (Authorized). The 'Port Counters' section shows two tables: 'Receive EAPOL Counters' and 'Transmit EAPOL Counters'. Both tables have columns for 'Total', 'Response ID', 'Responses', 'Start', 'Logoff', 'Invalid Type', and 'Invalid Length', with all values currently at 0.

Receive EAPOL Counters		Transmit EAPOL Counters	
Total	0	Total	0
Response ID	0	Request ID	0
Responses	0	Requests	0
Start	0		
Logoff	0		
Invalid Type	0		
Invalid Length	0		

Figure 4-6.2.2.2: NAS Statistics

Parameter descriptions:**Port State**

Admin State : The port's current administrative state. Refer to NAS Admin State for a description of possible values.

Port State : The current state of the port. Refer to NAS Port State for a description of the individual states.

QoS Class : The QoS class assigned by the RADIUS server. The field is blank if no QoS class is assigned.

Port VLAN ID : The VLAN ID that NAS has put the port in. The field is blank, if the Port VLAN ID is not overridden by NAS. If the VLAN ID is assigned by the RADIUS server, "(RADIUS-assigned)" is appended to the VLAN ID.

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.

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

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.

Port Counters

EAPOL Counters : These supplicant frame counters are available for these administrative states:

- Force Authorized
- Force Unauthorized
- Port-based 802.1X
- Single 802.1X
- Multi 802.1X

EAPOL Counters:

Direction	Name	IEEE Name	Description
RX	Total	dot1xAuthEapolFramesRx	The number of valid EAPOL frames of any type that have been received by the switch.
RX	Response ID	dot1xAuthEapolRespIdFramesRx	The number of valid EAPOL Response Identity frames that have been received by the switch.
RX	Responses	dot1xAuthEapolRespFramesRx	The number of valid EAPOL response frames (other than Response Identity

			frames) that have been received by the switch.
RX	Start	dot1xAuthEapolStartFramesRx	The number of EAPOL Start frames that have been received by the switch.
RX	Logoff	dot1xAuthEapolLogoffFramesRx	The number of valid EAPOL Logoff frames that have been received by the switch.
RX	Invalid Type	dot1xAuthInvalidEapolFramesRx	The number of EAPOL frames that have been received by the switch in which the frame type is not recognized.
RX	Invalid Length	dot1xAuthEapLengthErrorFramesRx	The number of EAPOL frames that have been received by the switch in which the Packet Body Length field is invalid.
TX	Total	dot1xAuthEapolFramesTx	The number of EAPOL frames of any type that have been transmitted by the switch.
TX	Request ID	dot1xAuthEapolReqIdFramesTx	The number of EAPOL Request Identity frames that have been transmitted by the switch.
TX	Requests	dot1xAuthEapolReqFramesTx	The number of valid EAPOL Request frames (other than Request Identity frames) that have been transmitted by the switch.

Backend Server Counters : These backend (RADIUS) frame counters are available for these administrative states:

- Port-based 802.1X
- Single 802.1X
- Multi 802.1X
- MAC-based Auth.

Backend Counters:

Direction	Name	IEEE Name	Description
RX	Access Challenges	dot1xAuthBackendAccessChallenges	802.1X-based: Counts the number of times that the switch receives the first request from the backend server following the first response from the supplicant. Indicates that the backend server has communication with the switch. MAC-based: Counts all Access Challenges received from the backend server for this port (left-most table) or client (right-most table).
RX	Other Requests	dot1xAuthBackendOtherRequestsTo Supplicant	802.1X-based: Counts the number of times that the switch sends an EAP Request packet following the first to the supplicant. Indicates that the backend server chose an EAP-method. MAC-based: Not applicable. 802.1X- and MAC-based: Counts the number of times that the switch receives a success indication. Indicates that the

			supplicant/client has successfully authenticated to the backend server.
RX	Auth. Successes	dot1xAuthBackendAuthSuccesses	802.1X- and MAC-based: Counts the number of times that the switch receives a failure message. This indicates that the supplicant/client has not authenticated to the backend server.
RX	Auth. Failures	dot1xAuthBackendAuthFails	802.1X-based: Counts the number of times that the switch attempts to send a supplicant's first response packet to the backend server. Indicates the switch attempted communication with the backend server. Possible retransmissions are not counted.
TX	Responses	dot1xAuthBackendResponses	MAC-based: Counts all the backend server packets sent from the switch towards the backend server for a given port (left-most table) or client (right-most table). Possible retransmissions are not counted.

Last Supplicant/Client Info : Information about the last supplicant/client that attempted to authenticate. This information is available for these administrative states:

- Port-based 802.1X
- Single 802.1X
- Multi 802.1X
- MAC-based Auth.

Last Supplicant/Client Info :

Name	IEEE Name	Description
MAC Address	dot1xAuthLastEapolFrameSource	The MAC address of the last supplicant/client.
VLAN ID -		The VLAN ID on which the last frame from the last supplicant/client was received.
Version	dot1xAuthLastEapolFrameVersion	802.1X-based: The protocol version number carried in the most recently received EAPOL frame. MAC-based: Not applicable.
Identity -		802.1X-based: The user name (supplicant identity) carried in the most recently received Response Identity EAPOL frame. MAC-based: Not applicable.

Selected Counters

Selected Counters : The Selected Counters table is visible when the port is in one of these administrative states:

- Multi 802.1X
- MAC-based Auth.

The table is identical to and is placed next to the Port Counters table, and will be empty if no MAC address is currently selected. To populate the table, select one of the attached MAC Addresses from the table below.

Attached MAC Addresses

Identity : Shows the identity of the supplicant, as received in the Response Identity EAPOL frame.

Clicking the link causes the supplicant's EAPOL and Backend Server counters to be shown in the Selected Counters table. If no supplicants are attached, it shows No supplicants attached.

This column is not available for MAC-based Auth.

MAC Address : For Multi 802.1X, this column holds the MAC address of the attached supplicant. For MAC-based Auth., this column holds the MAC address of the attached client.

Clicking the link causes the client's Backend Server counters to be shown in the Selected Counters table. If no clients are attached, it shows No clients attached.

VLAN ID : This column holds the VLAN ID that the corresponding client is currently secured through the Port Security module.

State : The client can either be authenticated or unauthenticated. In the authenticated state, it is allowed to forward frames on the port, and in the unauthenticated state, it is blocked. As long as the backend server hasn't successfully authenticated the client, it is unauthenticated. If an authentication fails for one or the other reason, the client will remain in the unauthenticated state for Hold Time seconds.

Last Authentication : Shows the date and time of the last authentication of the client (successful as well as unsuccessful).

Buttons

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

Refresh: Click to refresh the page immediately.

Clear: This button is available in the following modes:

- Force Authorized
- Force Unauthorized
- Port-based 802.1X
- Single 802.1X

Clear All: Click to clear the counters for the selected port. This button is available in these modes:

- Multi 802.1X
- MAC-based Auth.X

Clear This: Click to clear both the port counters and all of the attached client's counters. The "Last Client" will not be cleared, however. This button is available in these modes:

- Multi 802.1X
- MAC-based Auth.X

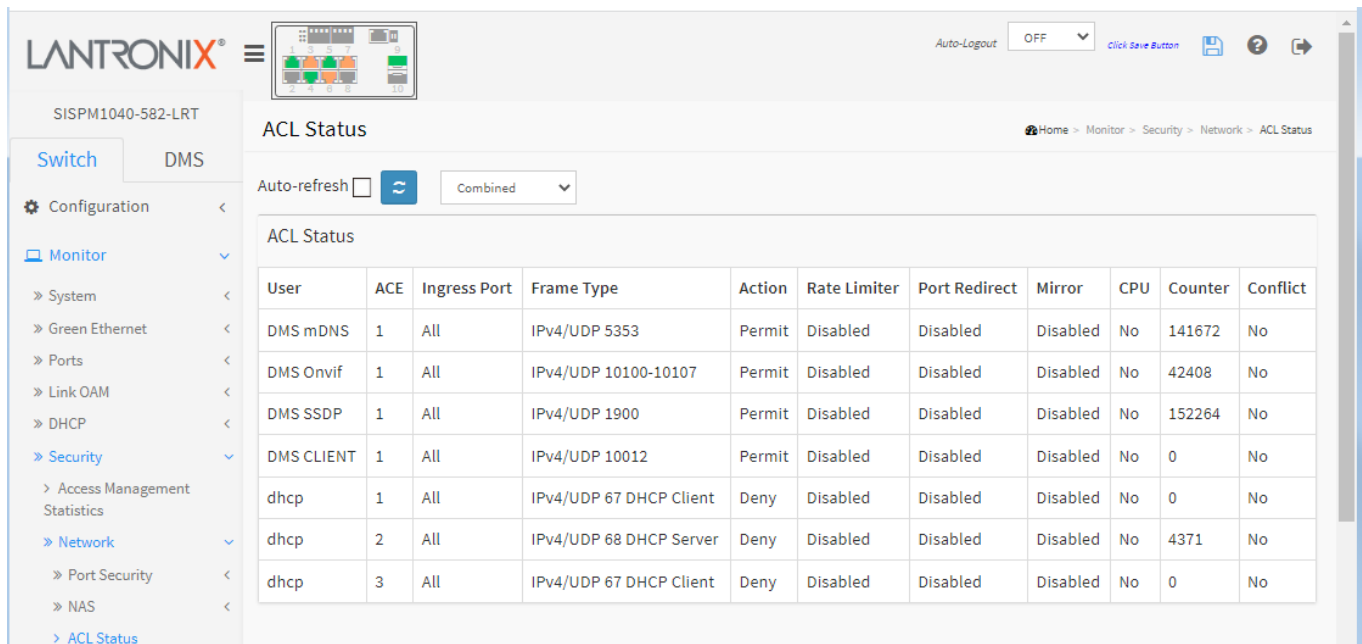
Click to clear only the currently selected client's counters.

4-6.2.3 ACL Status

This page shows the ACL status by different ACL users as configured at Configuration > QoS > QoS Control List. 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 256 per switch.

To display ACL status in the web UI:

1. Click Monitor, Security, Network, ACL Status.
2. Select the desired set of users at the User Select dropdown.
3. To automatically refresh the information every 3 seconds check the Auto-refresh checkbox.
4. Click Refresh to refresh the page immediately.



The screenshot shows the Lantronix web interface for the device SISPM1040-582-LRT. The navigation menu on the left includes Configuration, Monitor, and Security. The ACL Status page is displayed, featuring an 'Auto-refresh' checkbox and a 'Refresh' button. Below these controls is a table with the following data:

User	ACE	Ingress Port	Frame Type	Action	Rate Limiter	Port Redirect	Mirror	CPU	Counter	Conflict
DMS mDNS	1	All	IPv4/UDP 5353	Permit	Disabled	Disabled	Disabled	No	141672	No
DMS Onvif	1	All	IPv4/UDP 10100-10107	Permit	Disabled	Disabled	Disabled	No	42408	No
DMS SSDP	1	All	IPv4/UDP 1900	Permit	Disabled	Disabled	Disabled	No	152264	No
DMS CLIENT	1	All	IPv4/UDP 10012	Permit	Disabled	Disabled	Disabled	No	0	No
dhcp	1	All	IPv4/UDP 67 DHCP Client	Deny	Disabled	Disabled	Disabled	No	0	No
dhcp	2	All	IPv4/UDP 68 DHCP Server	Deny	Disabled	Disabled	Disabled	No	4371	No
dhcp	3	All	IPv4/UDP 67 DHCP Client	Deny	Disabled	Disabled	Disabled	No	0	No

Figure 4-6.2.3: ACL Status

Parameter descriptions:

User : Shows the ACL user (e.g., evc, mep, upnp, ptp).

Ingress Port : Indicates the ingress port of the ACE. Possible values are:

All: The ACE will match any ingress port.

Port: The ACE will match this 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/ICMP: The ACE will match IPv4 frames with ICMP protocol.

IPv4/UDP: The ACE will match IPv4 frames with UDP protocol.

IPv4/TCP: The ACE will match IPv4 frames with TCP protocol.

IPv4/Other: The ACE will match IPv4 frames, which are not ICMP / UDP / TCP.

IPv6: The ACE will match all IPv6 standard frames.

Action : Indicates the forwarding action of the ACE.

Permit: Frames matching the ACE may be forwarded and learned.

Deny: Frames matching the ACE are dropped.

Filter: Frames matching the ACE are filtered.

Rate Limiter : Indicates the rate limiter number of the ACE. The allowed range is 1 to 16. When Disabled is displayed, the rate limiter operation is disabled.

Port Redirect : Indicates the port copy operation of the ACE. Frames matching the ACE are copied to the port number. The allowed values are Disabled or a specific port number. When Disabled is displayed, the port copy operation is disabled.

CPU : Forward packet that matched the specific ACE to CPU.

Counter : The counter indicates the number of times the ACE was hit by a frame.

Conflict : Indicates the hardware status of the specific ACE. The specific ACE is not applied to the hardware due to hardware limitations.

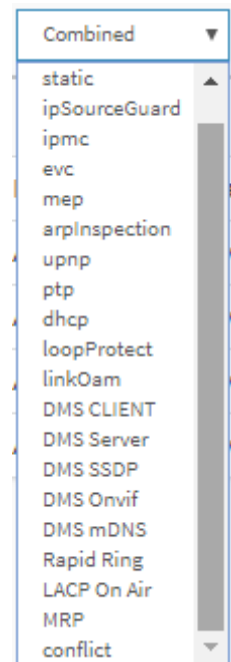
Buttons

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

Refresh: Click to refresh the page immediately.

User Select box: At the dropdown select the set of user data filtering.

The selections are Combined, static, ipSourceGuard, ipmc, evc, mep, arpInspection, upnp, ptp, dhcp, loopProtect, linkOam, DMSCLIENT, DMSServer, DMS SSDP, DMSOnvif, DMSmDNS, Rapid Ring, LACP On Air, MRP, and conflict.



4-6.2.4 ARP Inspection

This page displays the Dynamic ARP Inspection Table parameters of the switch. The Dynamic ARP Inspection Table contains up to 1024 entries, and is sorted first by port, then by VLAN ID, then by MAC address, and then by IP address.

Each page shows up to 99 entries from the Dynamic ARP Inspection table, default being 20, selected through the "entries per page" input field. When first visited, the web page will show the first 20 entries from the beginning of the Dynamic ARP Inspection Table. The "Start from port address", "VLAN", "MAC address" and "IP address" input fields let you select the starting point in the Dynamic ARP Inspection Table. Clicking the Refresh button will update the displayed table starting from that or the closest next Dynamic ARP Inspection Table match. In addition, the two input fields will - upon a Refresh button click - assume the value of the first displayed entry, allowing for continuous refresh with the same start address.

Web Interface

To view the Dynamic ARP Inspection Table in the web UI:

1. Click Monitor, Security, Network, ARP Inspection.
2. Check Auto-refresh.
3. Click Refresh to refresh the port detailed statistics.
4. Specify the Start from port, VLAN ID, MAC Address, IP Address, and entries per page.



Figure 4-6.2.4: Dynamic ARP Inspection Table

Parameter descriptions:

Port : Switch Port Number for which the entries are displayed.

VLAN ID : VLAN-ID in which the ARP traffic is permitted.

MAC Address : User MAC address of the entry.

IP Address : User IP address of the entry.

Buttons

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

Refresh: Click to refresh the page immediately.

<<: Updates the system log entries to the first available entry ID.

> : Updates the system log entry to the next available entry ID.

4-6.2.5 IP Source Guard

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 VLAN ID, then by IP address, and then by MAC address.

Web Interface

To view the Dynamic IP Source Guard Table via the web UI:

1. Click Monitor, Security, Network, IP Source Guard.
2. Check the Auto-refresh box to automatically refresh the page every 3 seconds.
3. Click Refresh to refresh the page immediately.
4. Specify the Start from port, VLAN ID, IP Address, and entries per page.

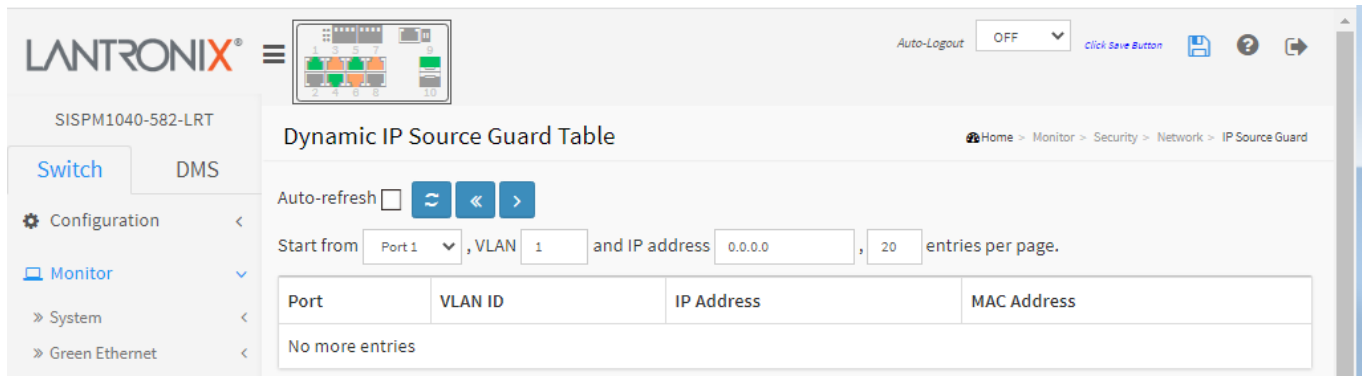


Figure 4-6.2.5: Dynamic IP Source Guard Table

Parameter descriptions:

Port : Switch Port Number for which the entries are displayed.

VLAN ID : VLAN-ID in which the IP traffic is permitted.

IP Address : User IP address of the entry.

MAC Address : The Source MAC address.

Buttons

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

Refresh: Click to refresh the page immediately.

<<: Updates to the First page.

> : Updates to the Next page.

4-6.3 AAA

4-6.3.1 RADIUS Overview

This page provides an overview of the status of the RADIUS servers configurable on the RADIUS Server Configuration page at Configuration > Security > AAA > RADIUS.

To view the RADIUS Ser Status Overview in the web UI:

1. Click Monitor, Security, AAA, RADIUS Overview.
2. Check Auto-refresh.
3. Click Refresh to refresh the page.

#	IP Address	Authentication Port	Authentication Status	Accounting Port	Accounting Status
1	RadSrvr1	1812	Ready	1813	Ready
2	1.2.3.4	1645	Ready	1646	Ready
3	3.4.5.6	1645	Ready	1813	Ready
4	radius4	1812	Ready	1646	Ready
5	radius5	1812	Ready	1813	Ready

Figure 4-6.3.1: RADIUS Server Status Overview

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 : UDP port number for authentication.

Authentication Status: The current state 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.

Accounting Port : UDP port number for accounting.

Accounting Status : The current state of the server. This field takes one of these values:

Disabled: The server is disabled.

Not Ready: The server is enabled, but IP communication is not yet up and running.

Ready: The server is enabled, IP communication is up and running, and the RADIUS module is ready to accept access attempts.

Dead (X seconds left): Access attempts were made to this server, but it did not reply within the configured timeout. The server has temporarily been disabled but will get re-enabled when the

dead-time expires. The number of seconds left before this occurs is displayed in parentheses. This state is only reachable when more than one server is enabled.

Buttons

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

Refresh: Click to refresh the page immediately.

4-6.3.2 RADIUS Details

This page displays statistics for a selected RADIUS server. To display RADIUS statistics in the web UI:

1. Click Monitor, Security, AAA, RADIUS Overview.
2. Specify which Port to check.

The screenshot displays the 'RADIUS Authentication Statistics' page for 'Server #1'. The page includes an 'Auto-refresh' toggle (disabled), a refresh button, and a server selection dropdown. The statistics are presented in two tables:

RADIUS Authentication Statistics for Server #1	
Receive Packets	Transmit Packets
Access Accepts	0
Access Rejects	0
Access Challenges	0
Malformed Access Responses	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
Malformed Responses	0
Bad Authenticators	0
Unknown Types	0
Packets Dropped	0
Other Info	
IP Address	
State	Disabled

Figure 4-6.3.2: RADIUS Authentication Statistics

RADIUS Authentication Statistics

The statistics map closely to those specified in the IETF [RFC4668 - RADIUS Authentication Client MIB](https://www.rfc-editor.org/rfc/rfc4668). Use the server select box to switch between the backend servers to show details for.

Packet Counters : RADIUS authentication server packet counter. There are seven receive and four transmit counters.

Direction	Name	RFC4668 Name	Description
Rx	Access Accepts	radiusAuthClientExtAccessAccepts	The number of RADIUS Access-Accept packets (valid or invalid) received from the server.
Rx	Access Rejects	radiusAuthClientExtAccessRejects	The number of RADIUS Access-Reject packets (valid or invalid) received from the server.
Rx	Access Challenges	radiusAuthClientExtAccessChallenges	The number of RADIUS Access-Challenge packets (valid or invalid) received from the server.
Rx	Malformed Access Responses	radiusAuthClientExtMalformedAccessResponses	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.
Rx	Bad Authenticators	radiusAuthClientExtBadAuthenticators	The number of RADIUS Access-Response packets containing invalid authenticators or Message Authenticator attributes received from the server.
Rx	Unknown Types	radiusAuthClientExtUnknownTypes	The number of RADIUS packets that were received with unknown types from the server on the authentication port and dropped.
Rx	Packets Dropped	radiusAuthClientExtPacketsDropped	The number of RADIUS packets that were received from the server on the authentication port and dropped for some other reason.
Tx	Access Requests	radiusAuthClientExtAccessRequests	The number of RADIUS Access-Request packets sent to the server. This does not include retransmissions.
Tx	Access Retransmissions	radiusAuthClientExtAccessRetransmissions	The number of RADIUS Access-Request packets retransmitted to the RADIUS authentication server.
Tx	Pending Requests	radiusAuthClientExtPendingRequests	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.
Tx	Timeouts	radiusAuthClientExtTimeouts	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.

Other Info

This section contains information about the state of the server and the latest round-trip time.

Name	RFC4668 Name	Description
IP Address	- - -	IP address and UDP port for the authentication server in question.
State	- - -	Shows the state of the server. It takes one of the following values: Disabled: The selected server is disabled. Not Ready: The server is enabled, but IP communication is not yet up and running. Ready: The server is enabled, IP communication is up and running, and the RADIUS module is ready to accept access attempts. Dead (X seconds left): Access attempts were made to this server, but it did not reply within the configured timeout. The server has temporarily been disabled but will get re-enabled when the dead-time expires. The number of seconds left before this occurs is displayed in parentheses. This state is only reachable when more than one server is enabled.
Round-Trip Time	radiusAuthClientExtRoundTripTime	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 the [IETF RFC4670 - RADIUS Accounting Client MIB](#). Use the server select box to switch between the backend servers to show details for.

Packet Counters

RADIUS accounting server packet counter. There are five receive and four transmit counters.

Direction	Name	RFC4670 Name	Description
Rx	Responses	radiusAccClientExtResponses	The number of RADIUS packets (valid or invalid) received from the server.
Rx	Malformed Responses	radiusAccClientExtMalformed 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.
Rx	Bad Authenticators	radiusAcctClientExtBadAuthenticators	The number of RADIUS packets containing invalid authenticators received from the server.
Rx	Unknown Types	radiusAccClientExtUnknownTypes	The number of RADIUS packets of unknown types that were received from the server on the accounting port.
Rx	Packets Dropped	radiusAccClientExtPacketsDropped	The number of RADIUS packets that were received from the server on the accounting port and dropped for some other reason.
Tx	Requests	radiusAccClientExtRequests	The number of RADIUS packets sent to the server. This does not include retransmissions.
Tx	Retransmissions	radiusAccClientExtRetransmissions	The number of RADIUS packets retransmitted to the RADIUS accounting server.
Tx	Pending Requests	radiusAccClientExtPendingRequests	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.
Tx	Timeouts	radiusAccClientExtTimeouts	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.

Other Info

This section contains information about the state of the server and the latest round-trip time.

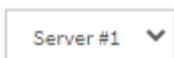
Name	RFC4670 Name	Description
IP Address	-	IP address and UDP port for the accounting server in question.
State	-	Shows the state of the server. It takes one of the following values: Disabled: The selected server is disabled. Not Ready: The server is enabled, but IP communication is not yet up and running. 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	radiusAccClientExtRoundTripTime	The time interval (measured in milliseconds) between the most recent Response and the Request that matched it from the RADIUS accounting server. The granularity of this measurement is 100 ms. A value of 0 ms indicates that there hasn't been round-trip communication with the server yet.

Buttons



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

Refresh: Click to refresh the page immediately.



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



: Clears the counters for the selected RADIUS server. The "Pending Requests" counter will not be cleared by this operation.

4-6.4 Switch

4-6.4.1 RMON

4-6.4.1.1 Statistics

This section provides an overview of RMON Statistics entries. Each page shows up to 99 entries from the Statistics table, default being 20, selected through the "entries per page" input field. When first visited, the web page will show the first 20 entries from the beginning of the Statistics table. The first displayed will be the one with the lowest ID found in the Statistics table.

To view RMON Statistics in the web UI:

1. Click Monitor, Security, Switch, RMON, Statistics.
2. Check Auto-refresh.
3. Click Refresh to refresh the page.

ID	Data Source (if Index)	Drop	Octets	Pkts	Broadcast	Multicast	CRC Errors	Under-size	Over-size	Frag.	Jabb.	Coll.	64 Bytes	65 ~ 127	128 ~ 255	256 ~ 511	512 ~ 1023	1024 ~ 1588
1	2	0	6267926	31890	5639	915	0	0	0	0	0	0	22565	796	795	18	7714	2
2	3	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0

Figure 4-6.4.1.1: RMON Statistics Status Overview

Parameter descriptions:

ID : Indicates the index of Statistics entry.

Data Source(if Index) : The port ID which wants to be monitored.

Drop : The total number of events in which packets were dropped by the probe due to lack of resources.

Octets : The total number of octets of data (including those in bad packets) received on the network.

Pkts : The total number of packets (including bad packets, broadcast packets, and multicast packets) received.

Broad-cast : The total number of good packets received that were directed to the broadcast address.

Multi-cast : 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 : The total number of packets (including bad packets) received that were 64 octets in length.

65~127 : The total number of packets (including bad packets) received that were between 65 to 127 octets in length.

128~255 : The total number of packets (including bad packets) received that were between 128 to 255 octets in length.

256~511 : The total number of packets (including bad packets) received that were between 256 to 511 octets in length.

512~1023 : The total number of packets (including bad packets) received that were between 512 to 1023 octets in length.

1024~1588 : The total number of packets (including bad packets) received that were between 1024 to 1588 octets in length.

Buttons

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

Refresh: Click to refresh the page immediately.

<< : Updates the table starting from the first entry in the Statistics table, i.e. the entry with the lowest ID.

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

4-6.4.1.2 History

This page provides an overview of RMON History entries. Each page shows up to 99 entries from the History table, default being 20, selected through the "entries per page" input field. When first visited, the web page will show the first 20 entries from the beginning of the History table. The first displayed will be the one with the lowest History Index and Sample Index found in the History table.

The "Start from History Index and Sample Index" allows the user to select the starting point in the History table.

The "Start from History Index and Sample Index" allows the user to select the starting point in the History table.

To monitor RMON history in the web UI:

1. Click Monitor, Security, Switch, RMON, History.
2. Check Auto-refresh.
3. Click Refresh to refresh the port detailed statistics or clear all information when you click Clear.

The screenshot displays the 'RMON History Overview' page in the Lantronix web UI. The page features a navigation sidebar on the left with options like 'Switch', 'DMS', 'Configuration', and 'Monitor'. The main content area shows the 'RMON History Overview' title, an 'Auto-refresh' checkbox, and input fields for 'Start from Control Index' (0) and 'Sample Index' (0), with a '20 entries per page' setting. Below this is a table with the following columns: History Index, Sample Index, Sample Start, Drop, Octets, Pkts, Broadcast, Multicast, CRC Errors, Under-size, Over-size, Frag., Jabb., Coll., and Utilization. The table currently displays 'No more entries'.

Figure 4-6.4.1.2: RMON History Overview

Parameter descriptions:

History Index : Indicates the index of History control entry.

Sample Index : Indicates the index of the data entry associated with the control entry.

Sample Start : The value of sysUpTime at the start of the interval over which this sample was measured.

Drop : The total number of events in which packets were dropped by the probe due to lack of resources.

Octets : The total number of octets of data (including those in bad packets) received on the network.

Pkts : The total number of packets (including bad packets, broadcast packets, and multicast packets) received.

Broadcast : The total number of good packets received that were directed to the broadcast address.

Multicast : The total number of good packets received that were directed to a multicast address.

CRC Errors : The total number of packets received that had a length (excluding framing bits, but including FCS octets) of between 64 and 1518 octets, inclusive, but had either a bad Frame Check Sequence (FCS) with an integral number of octets (FCS Error) or a bad FCS with a non-integral number of octets (Alignment Error).

Undersize : The total number of packets received that were less than 64 octets.

Oversize : The total number of packets received that were longer than 1518 octets.

Frag. : The number of frames which size is less than 64 octets received with invalid CRC.

Jabb. : The number of frames which size is larger than 64 octets received with invalid CRC.

Coll. : The best estimate of the total number of collisions on this Ethernet segment.

Utilization : The best estimate of the mean physical layer network utilization on this interface during this sampling interval, in hundredths of a percent.

Buttons

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

Refresh: Click to refresh the page immediately.

<< : Updates the table starting from the first entry in the History table, i.e., the entry with the lowest History Index and Sample Index

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

3-6.4.1.3 Alarm

This page provides an overview of RMON Alarm entries. Each page shows up to 99 entries from the Alarm table, default being 20, selected through the "entries per page" input field. When first visited, the web page will show the first 20 entries from the beginning of the Alarm table. The first displayed will be the one with the lowest ID found in the Alarm table. The "Start from Control Index" lets you select the starting point in the Alarm table.

To view the RMON Alarm Overview in the web UI:

1. Click Monitor, Security, Switch, RMON, Alarm.
2. Check Auto-refresh.
3. Click Refresh to refresh the port detailed statistics.

ID	Interval	Variable	Sample Type	Value	Startup Alarm	Rising Threshold	Rising Index	Falling Threshold	Falling Index
1	30	.1.3.6.1.2.1.2.2.1.10.2	Delta	38036	RisingOrFalling	5	4	3	6
2	30	.1.3.6.1.2.1.2.2.1.20.9	Delta	0	RisingOrFalling	8	5	4	7

Figure 3-6.4.1.3: RMON Alarm Overview

Parameter descriptions:

ID : Indicates the index of Alarm control entry.

Interval : Indicates the interval in seconds for sampling and comparing the rising and falling threshold.

Variable : Indicates the particular variable to be sampled

Sample Type : The method of sampling the selected variable and calculating the value to be compared against the thresholds.

Value : The value of the statistic during the last sampling period.

Startup Alarm : The alarm that may be sent when this entry is first set to valid.

Rising Threshold : Rising threshold value.

Rising Index : Rising event index.

Falling Threshold : Falling threshold value.

Falling Index : Falling event index.

Buttons

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

Refresh: Click to refresh the page immediately.

<<: Updates the table starting from the first entry in the Alarm Table, i.e. the entry with the lowest ID.

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

4-6.4.1.4 Event

This page provides an overview of RMON Event table entries. Each page shows up to 99 entries from the Event table, default being 20, selected through the "entries per page" input field. When first visited, the web page will show the first 20 entries from the beginning of the Event table. The first displayed will be the one with the lowest Event Index and Log Index found in the Event table .

The "Start from Event Index and Log Index" allows the user to select the starting point in the Event table.

To monitor the RMON Event Overview in the web UI:

1. Click Monitor, Security, Switch, RMON, Event.
2. Check Auto-refresh.
3. Click Refresh to refresh the port detailed statistics
4. Specify Port which wants to check.

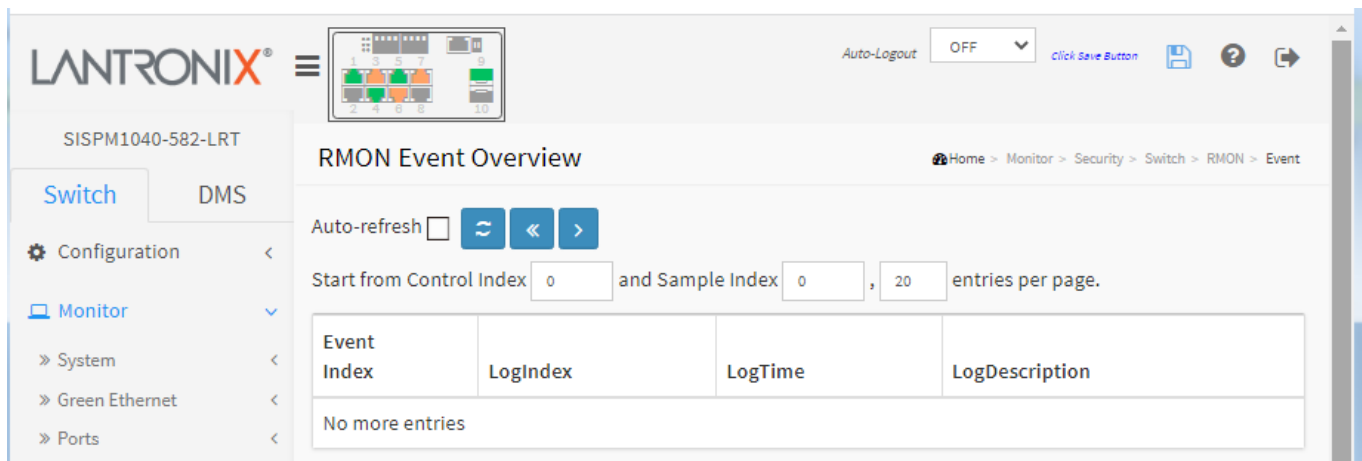


Figure 4-6.4.1.4: RMON Event Overview

Parameter descriptions:

Event Index : Indicates the index of the event entry.

LogIndex : Indicates the index of the log entry.

LogTime : Indicates Event log time

LogDescription : Indicates the Event description.

Buttons

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

Refresh: Click to refresh the page immediately.

<< : Updates the table starting from the first entry in the Event Table, i.e. the entry with the lowest Event Index and Log Index.

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

4-7 Aggregation

4-7.1 Status

This page displays the status of ports in an Aggregation group. To display Aggregation status in the web UI:

1. Click Monitor, Aggregation, Status.
2. Check “Auto-refresh”.
3. Click “Refresh” to refresh the port detailed statistics.

Aggr ID	Name	Type	Speed	Configured Ports	Aggregated Ports	Aggregated Bandwidth
1	LLAG1	Static	1G	GigabitEthernet 1/1-2	none	none
2	LLAG2	Static	100M	GigabitEthernet 1/3-4	none	none
3	LLAG3	Static	1G	GigabitEthernet 1/5-6	none	none
4	LLAG4	Static	1G	GigabitEthernet 1/7-10	GigabitEthernet 1/8,10	2G

Figure 4-7.1: Aggregation Status

Parameter descriptions:

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

Name : The name of the Aggregation group ID.

Type : The type of the Aggregation group (Static or LACP).

Speed : The speed of the Aggregation group.

Configured ports : Configured member ports of the Aggregation group.

Aggregated ports : Aggregated member ports of the Aggregation group.

Buttons

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

Refresh: Click to refresh the page immediately.

Messages:

Group 1 member counts error!! Local aggregation must include 2-16 ports

4-7.2 LACP

4-7.2.1 System Status

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

1. Click Monitor, LACP, System Status
2. To automatically refresh the information click Auto-refresh.
3. Click Refresh to refresh the LACP Status.

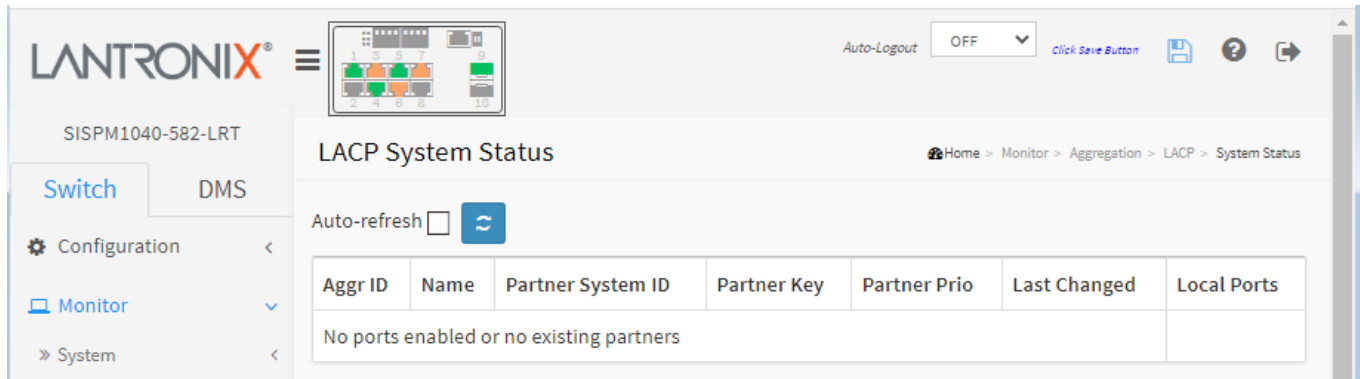


Figure 4-7.2.1: LACP System Status

Parameter descriptions:

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

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

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

Partner Prio : The priority of this partner.

Last Changed : The time since this aggregation changed.

Local Ports : Shows which ports are a part of this aggregation for this switch.

Buttons

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

Refresh: Click to refresh the page immediately.

Messages: *No ports enabled or no existing partners*

4-7.2.2 Port Status

This page displays LACP status for all ports. To display the LACP Port Status in the web UI:

1. Click Monitor, LACP, Port Status.
2. To automatically refresh the information click Auto-refresh.
3. Click Refresh to refresh the LACP Status immediately.

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

Figure 4-7.2.2: LACP Status

Parameter descriptions:

Port : The switch port number.

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

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

Aggr ID : The Aggregation ID assigned to this aggregation group.

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

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

Partner Prio : The partner's port priority.

Buttons

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

Refresh: Click to refresh the page immediately.

4-7.2.3 Port Statistics

This page provides an overview for LACP statistics for all ports. To display LACP Port Statistics in the web UI:

1. Click Monitor LACP, Port Statistics.
2. To automatically refresh the information check the Auto-refresh checkbox.
3. Click Refresh to refresh the page immediately.

The screenshot shows the Lantronix web UI for device SISPM1040-582-LRT. The page title is "LACP Statistics". A navigation menu on the left shows "Monitor" > "Aggregation" > "LACP" > "Port Statistics". The main content area has an "Auto-refresh" checkbox (unchecked) and two buttons: a blue refresh button and a red clear button. Below is a table with 5 columns: Port, LACP Received, LACP Transmitted, Discarded (Unknown), and Discarded (Illegal). The table contains 10 rows, one for each port, with all values set to 0.

Port	LACP Received	LACP Transmitted	Discarded	
			Unknown	Illegal
1	0	0	0	0
2	0	0	0	0
3	0	0	0	0
4	0	0	0	0
5	0	0	0	0
6	0	0	0	0
7	0	0	0	0
8	0	0	0	0
9	0	0	0	0
10	0	0	0	0

Figure 4-7.2.3: LACP Statistics

Parameter descriptions:

Port : The switch port number.

LACP Received : Shows how many LACP frames have been received at each port.

LACP Transmitted : Shows how many LACP frames have been sent from each port.

Discarded : Shows how many unknown or illegal LACP frames have been discarded at each port.

Buttons

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

Refresh: Click to refresh the page immediately.

Clear: Clears the counters for the selected port.

4-8 Loop Protection

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

1. Click Monitor, Loop Protection.
- 2 To automatically refresh the information check the Auto-refresh checkbox.
3. Click Refresh to refresh the status immediately.

The screenshot shows the web interface for SISPM1040-582-LRT. The main content area is titled "Loop Protection Status". Below the title, there is an "Auto-refresh" checkbox which is currently unchecked, and a refresh button. A table displays the status for 10 ports. The table has columns for Port, Action, Transmit, Loops, Status, Loop, and Time of Last Loop.

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

Figure 4-8 : Loop Protection Status

Parameter descriptions:

Port : The switch port number of the logical port.

Action : The currently configured port action.

Transmit : The currently configured port transmit mode.

Loops : The number of loops detected on this port.

Status : The current loop protection status of the port.

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

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

Buttons

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

Refresh: Click to manually refresh the page immediately.

4-9 Spanning Tree

4-9.1 Bridge Status

After you complete the MSTI Port configuration you can display the Bridge Status here. This page provides a status overview of all STP bridge instances. The displayed table contains a row for each STP bridge instance:

Web Interface

To display STP Bridges status in the web UI:

1. Click Monitor, Spanning Tree, Bridge Status.
2. To automatically refresh the information check the Auto-refresh box.
3. Click Refresh to refresh the page immediately.
4. Click “CIST” to go to the next page (STP Detailed Bridge Status).

The screenshot shows the Lantronix web interface for the device SISPM1040-582-LRT. The main content area is titled "STP Bridges" and includes an "Auto-refresh" checkbox (unchecked) and a refresh button. Below this is a table with the following data:

MSTI	Bridge ID	Root			Topology Flag	Topology Change Last
		ID	Port	Cost		
CIST	32768.00-C0-F2-49-39-30	32768.00-C0-F2-49-39-30	-	0	Steady	-

Figure 4-9.1: STP Bridges Status

Parameter descriptions:

MSTI : The Bridge Instance. This is also a link to the STP Detailed Bridge Status.

Bridge ID : The Bridge ID of this Bridge instance.

Root ID : The Bridge ID of the currently elected root bridge.

Root Port : The switch port currently assigned the root port role.

Root Cost : Root Path Cost. For the Root Bridge it is zero. For all other Bridges, it is the sum of the Port Path Costs on the least cost path to the Root Bridge.

Topology Flag : The current state of the Topology Change Flag of this Bridge instance.

Topology Change Last :

The time since last Topology Change occurred.

Buttons

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

Refresh: Click to refresh the page immediately.

When you click a linked instance in the MSTI column its STP Detailed Bridge Status page displays.

The screenshot shows the Lantronix web interface for device SISPM1040-582-LRT. The page title is "STP Detailed Bridge Status". The breadcrumb trail is "Home > Monitor > Spanning Tree > Bridge Status". The "Auto-refresh" checkbox is unchecked. The "STP Bridge Status" section contains the following data:

Parameter	Value
Bridge Instance	CIST
Bridge ID	32768.00-C0-F2-4F-73-D0
Root ID	32768.00-C0-F2-4F-73-D0
Root Cost	0
Root Port	-
Regional Root	32768.00-C0-F2-4F-73-D0
Internal Root Cost	0
Topology Flag	Steady
Topology Change Count	0
Topology Change Last	-

The "CIST Ports & Aggregations State" section contains the following table:

Port	Port ID	Role	State	Path Cost	Edge	Point-to-Point	Uptime
1	128:001	DesignatedPort	Forwarding	200000	Yes	Yes	0d 03:39:28
2	128:002	DesignatedPort	Forwarding	20000	Yes	Yes	0d 03:39:28
3	128:003	DesignatedPort	Forwarding	200000	Yes	Yes	0d 03:39:28
4	128:004	DesignatedPort	Forwarding	200000	Yes	Yes	0d 03:39:28

Parameter descriptions:

STP Bridge Status

Bridge Instance : The Bridge instance - CIST, MST1, ...

Bridge ID : The Bridge ID of this Bridge instance.

Root ID : The Bridge ID of the currently elected root bridge.

Root Port : The switch port currently assigned the root port role.

Root Cost : Root Path Cost. For the Root Bridge this is zero. For all other Bridges, it is the sum of the Port Path Costs on the least cost path to the Root Bridge.

Regional Root : The Bridge ID of the currently elected regional root bridge, inside the MSTP region of this bridge. (For the CIST instance only).

Internal Root Cost : The Regional Root Path Cost. For the Regional Root Bridge this is zero. For all other CIST instances in the same MSTP region, it is the sum of the Internal Port Path Costs on the least cost path to the Internal Root Bridge. (For the CIST instance only).

Topology Flag : The current state of the Topology Change Flag of this Bridge instance.

Topology Change Count : The number of times where the topology change flag has been set (during a one-second interval).

Topology Change Last : The time passed since the Topology Flag was last set.

CIST Ports & Aggregations State

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

Port ID : The port id as used by the STP protocol. This is the priority part and the logical port index of the bridge port.

Role : The current STP port role. The port role can be one of the following values: *AlternatePort*, *BackupPort*, and *RootPort*, *DesignatedPort*.

State : The current STP port state. The port state can be one of the following values: Discarding Learning Forwarding.

Path Cost : The current STP port path cost. This will either be a value computed from the Auto setting, or any explicitly configured value.

Edge : The current STP port (operational) Edge Flag. An Edge Port is a switch port to which no Bridges are attached. The flag may be automatically computed or explicitly configured. Each Edge Port transits directly to the Forwarding Port State, since there is no possibility of it participating in a loop.

Point-to-Point : The current STP port point-to-point flag. A point-to-point port connects to a non-shared LAN media. The flag may be automatically computed or explicitly configured. The point-to-point properties of a port affect how fast it can transit to STP state.

Uptime : The time since the bridge port was last initialized.

Buttons

Refresh: Click to refresh the page immediately.

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

4-9.2 Port Status

After you complete the STP configuration then you can display the STP Port Status (STP CIST port status for physical ports of the switch).

To display STP Port status in the web UI:

1. Click Monitor, Spanning Tree, Port Status.
2. To automatically refresh the information check Auto-refresh.
3. Click Refresh to refresh the page immediately.

The screenshot shows the Lantronix web interface for device SISPM1040-582-LRT. The main content area is titled 'STP Port Status'. Above the table, there is an 'Auto-refresh' checkbox which is currently unchecked, and a refresh icon. The table below contains the following data:

Port	CIST Role	CIST State	Uptime
1	DesignatedPort	Forwarding	2d 18:39:15
2	Disabled	Discarding	-
3	DesignatedPort	Forwarding	2d 18:39:15
4	DesignatedPort	Forwarding	2d 18:39:15
5	DesignatedPort	Forwarding	2d 18:39:15
6	DesignatedPort	Forwarding	2d 18:39:15
7	DesignatedPort	Forwarding	2d 18:39:15
8	Disabled	Discarding	-
9	BackupPort	Discarding	2d 18:39:15
10	Disabled	Discarding	-

Figure 4-9.2: STP Port Status

Parameter descriptions:

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

CIST Role : The current STP port role of the CIST port. The port role can be one of the following values: AlternatePort, Backup Port, RootPort, DesignatedPort and Disabled.

CIST State : The current STP port state of the CIST port. The port state can be one of the following values: Blocking, Learning, or Forwarding.

Uptime : The time since the bridge port was last initialized.

Buttons

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

Refresh: Click to refresh the page immediately.

4-9.3 Port Statistics

After you complete the STP configuration you can display the STP Statistics with the STP Statistics detail counters of bridge ports in the switch.

To display the STP Port statistics in the web UI:

1. Click Monitor, Spanning Tree, Port Statistics.
2. To automatically refresh the information check Auto-refresh.
3. Click Refresh to refresh the page immediately.

The screenshot shows the Lantronix web interface for the SISPM1040-582-LRT switch. The 'Spanning Tree' section is active, displaying 'Port Statistics'. The 'Auto-refresh' checkbox is unchecked. A table lists statistics for ports 1, 3, 4, 5, 6, 7, and 9. The table data is as follows:

Port	Transmitted				Received				Discarded	
	MSTP	RSTP	STP	TCN	MSTP	RSTP	STP	TCN	Unknown	Illegal
1	118838	0	0	0	1	0	0	0	0	0
3	8845	0	0	0	0	0	0	0	0	0
4	8845	0	0	0	0	0	0	0	0	0
5	8844	0	0	0	0	0	0	0	0	0
6	8845	0	0	0	0	0	0	0	0	0
7	118849	0	0	0	0	0	0	0	0	0
9	4	0	0	0	118838	0	0	0	0	0

Figure 4-9.3: STP Statistics

Parameter descriptions:

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

MSTP : The number of MSTP Configuration BPDU's received/transmitted on the port.

RSTP : The number of RSTP Configuration BPDU's received/transmitted on the port.

STP : The number of legacy STP Configuration BPDU's received/transmitted on the port.

TCN : The number of (legacy) Topology Change Notification BPDU's received/transmitted on the port.

Discarded Unknown : The number of unknown Spanning Tree BPDU's received (and discarded) on the port.

Discarded Illegal : The number of illegal Spanning Tree BPDU's received (and discarded) on the port.

Buttons

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

Refresh: Click to refresh the page immediately.

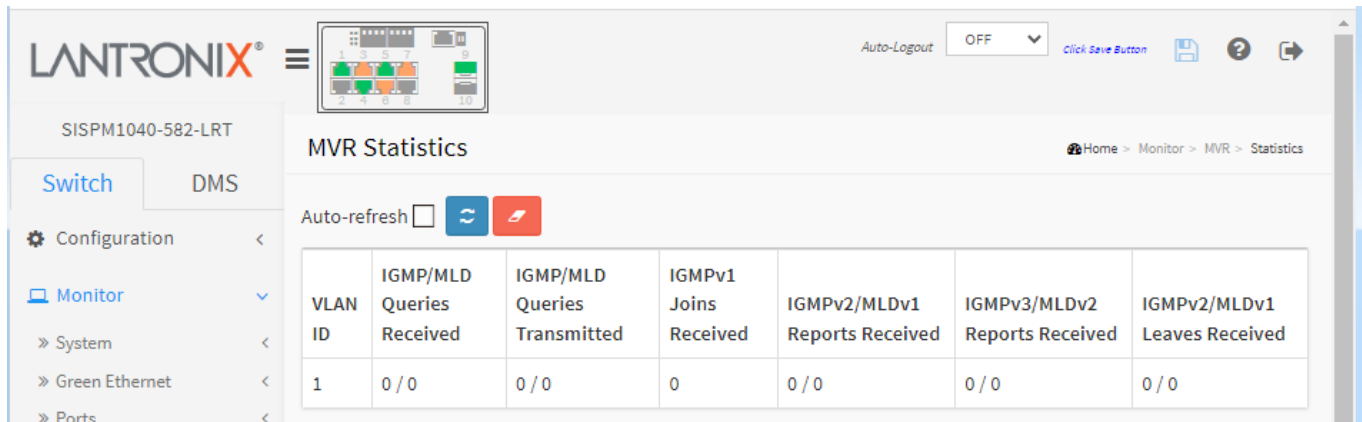
Clear: Clears the counters for the selected port.

4-10 MVR

4-10.1 Statistics

This page displays MVR detail Statistics as configured on the switch. To display MVR Statistics in the web UI:

1. Click Monitor, MVR, Statistics
2. To automatically refresh the information check Auto-refresh.
3. Click Refresh to refresh the page immediately.



The screenshot shows the Lantronix web UI for the device SISPM1040-582-LRT. The page title is 'MVR Statistics'. There is an 'Auto-refresh' checkbox which is currently unchecked, followed by a refresh icon and a clear icon. Below this is a table with the following data:

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
1	0 / 0	0 / 0	0	0 / 0	0 / 0	0 / 0

Figure 4-10.1: MVR Statistics

Parameter descriptions:

VLAN ID : The Multicast VLAN ID.

IGMP/MLD Queries Received : The number of Received Queries for IGMP and MLD, respectively.

IGMP/MLD Queries Transmitted : The number of Transmitted Queries for IGMP and MLD, respectively.

IGMPv1 Joins Received : The number of Received IGMPv1 Join's.

IGMPv2/MLDv1 Report's Received : The number of Received IGMPv2 Join's and MLDv1 Report's, respectively.

IGMPv3/MLDv2 Report's Received : The number of Received IGMPv1 Join's and MLDv2 Report's, respectively.

IGMPv2/MLDv1 Leave's Received : The number of Received IGMPv2 Leave's and MLDv1 Done's, respectively.

Buttons

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

Refresh: Click to refresh the page immediately.

Clear: Clears the counters for the selected port.

4-10.2 MVR Channels Groups

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

To display MVR Groups Information in the web UI:

1. Click Monitor, MVR, MVR Channel Groups.
2. To automatically refresh the information check Auto-refresh.
3. Click Refresh to refresh the page immediately.
4. Click << or > to move to the previous or next entry.

Figure 4-10.2: MVR Channels (Groups) Information

Parameter descriptions:

VLAN ID : VLAN ID of the group.

Groups : Group ID of the group displayed.

Port Members : Ports under this group.

Buttons

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

Refresh: Click to manually refresh the page immediately.

<<: Updates the system log entries to the first available entry ID.

> : Updates the system log entry to the next available entry ID.

Clear : Clears the page.

4-10.3 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 belonging to the same group are treated as single entry.

To display MVR SFM Information in the web UI:

1. Click Monitor, MVR, MVR SFM Information.
2. To automatically refresh the information click Auto-refresh or click Refresh to refresh the page immediately.
4. Click << or >> to move to the previous or next entry.

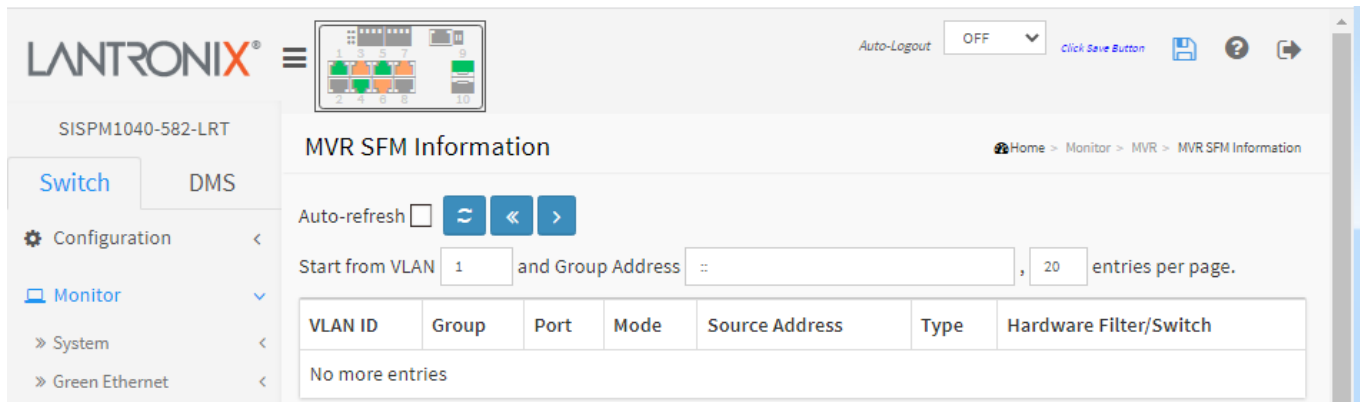


Figure 4-10.3: MVR SFM Information

Parameter descriptions:

VLAN ID : VLAN ID of the group.

Group : Group address of the group displayed.

Port : Switch port number.

Mode : Indicates the filtering mode maintained per (VLAN ID, port number, Group Address) basis. It can be either **Include** or **Exclude**.

Source Address : IP Address of the source. Currently, system limits the total number of IP source addresses for filtering to be 128. When there is no 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 can be handled by chip.

Buttons

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

Refresh: Click to refresh the page immediately.

<<: Updates the system log entries to the first available entry ID.

>> : Updates the system log entry to the next available entry ID.

4-11 IPMC

3-11.1 IGMP Snooping

4-11.1.1 Status

After you complete the IGMP Snooping configuration the switch can display the IGMP Snooping Status.

To display IGMP Snooping status in the web UI:

1. Click Monitor, IPMC, IGMP Snooping, Status.
2. To automatically refresh the information check Auto-refresh.
3. Click Refresh to refresh the page immediately.
4. Click Clear to clear the page.

The screenshot displays the IGMP Snooping Status page in the web UI. The left sidebar shows the navigation menu with 'Monitor' > 'IPMC' > 'IGMP Snooping' > 'Status' selected. The main content area is titled 'IGMP Snooping Status' and includes an 'Auto-refresh' checkbox and buttons for refresh and clear. Below this is a 'Statistics' table with columns for VLAN ID, Querier Version, Host Version, Querier Status, Queries Transmitted, Queries Received, V1 Reports Received, V2 Reports Received, V3 Reports Received, and V2 Leaves Received. The table shows two entries for VLANs 1 and 10. Below the statistics is a 'Router Port' table with columns for Port and Status, showing status for ports 1 through 10.

VLAN ID	Querier Version	Host Version	Querier Status	Queries Transmitted	Queries Received	V1 Reports Received	V2 Reports Received	V3 Reports Received	V2 Leaves Received
1	v3	v3	ACTIVE	1	1	0	0	1	0
10	v3	v3	ACTIVE	0	0	0	0	0	0

Port	Status
1	-
2	-
3	Both
4	Both
5	-
6	Both
7	-
8	-
9	Both
10	Both

Figure 4-11.1.1: IGMP Snooping Status

Parameter descriptions:

Statistics:

VLAN ID : The VLAN ID of the entry.

Querier Version : Current working Querier Version.

Host Version : Working Host Version currently.

Querier Status : Shows the Querier status is "ACTIVE" or "IDLE". "DISABLE" means the specific interface is administratively disabled.

Queries Transmitted : The number of Transmitted Queries.

Queries Received : The number of Received Queries.

V1 Reports Received : The number of Received V1 Reports.

V2 Reports Received : The number of Received V2 Reports.

V3 Reports Received : The number of Received V3 Reports.

V2 Leaves Received : The number of Received V2 Leaves.

Router Port : Display which ports act as router ports. A router port is a port on the Ethernet switch that leads towards the Layer 3 multicast device or IGMP querier.

Port : The switch port number.

Status : Indicate whether specific port is a router port or not.

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

Dynamic means the specific port is learnt to be a router port.

Both means the specific port is configured or learnt to be a router port.

Buttons

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

Refresh: Click to refresh the page immediately.

Clear: Clears the counters for the selected port.

4-11.1.2 Group Information

After you complete to set the IGMP Snooping function then you could let the switch to display the IGMP Snooping Group Information. Entries in the IGMP Group Table are shown on this page. The IGMP Group table is sorted first by VLAN ID, and then by group.

To display IGMP Snooping Group Information in the web UI:

1. Click Monitor, IPMC, IGMP Snooping, Group Information.
2. To automatically refresh the information check Auto-refresh.
3. Click Refresh to refresh the page immediately.
4. Click << or > to move to the previous or next entry.

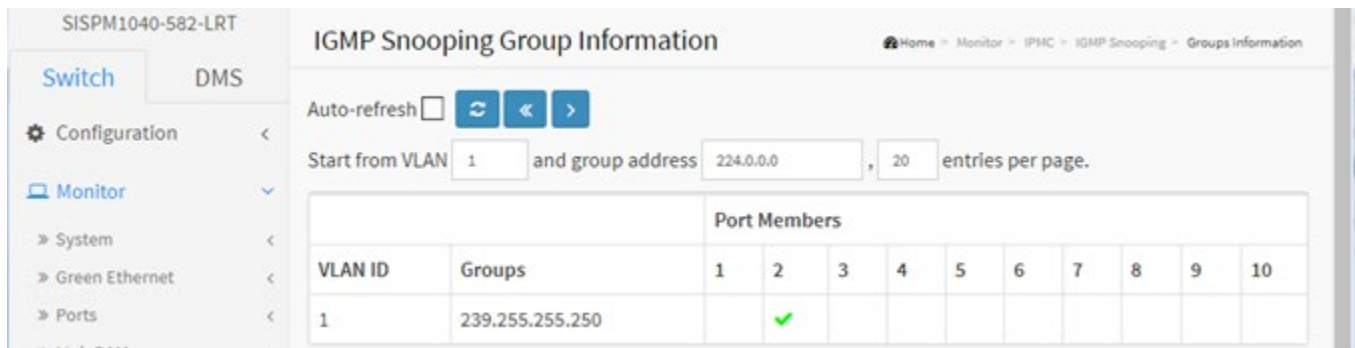


Figure 4-11.1.2: IGMP Snooping Groups Information

Parameter descriptions:

VLAN ID : The VLAN ID of the group.

Groups : The Group address of the group displayed.

Port Members : Ports under this group have a check mark (✓).

Buttons

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

Refresh: Click to refresh the page immediately.

<<: Updates the system log entries to the first available entry ID.

> : Updates the system log entry to the next available entry ID.

4-11.1.3 IPv4 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 single entry.

To display IPv4 SSM Information in the web UI:

1. Click Monitor, IGMP Snooping, IPv4 SSM Information
2. To automatically refresh the information check Auto-refresh.
3. Click Refresh to refresh the page immediately.
4. Click << or >> to move to the previous or next entry.

VLAN ID	Group	Port	Mode	Source Address	Type	Hardware Filter/Switch
1	239.255.255.250	2	Exclude	None	Deny	Yes

Figure 4-11.1.3: IPv4 SFM Information

Parameter descriptions:

VLAN ID : VLAN ID of the group.

Group : Group address of the group displayed.

Port : Switch port number.

Mode : Indicates the filtering mode maintained per (VLAN ID, port number, Group Address) basis. It can be either Include or Exclude.

Source Address : IP Address of the source. Currently, system limits the total number of IP source addresses for filtering to be 128.

Type : Indicates the Type. It can be either Allow or Deny.

Hardware Filter/Switch : Indicates whether data plane destined to the specific group address from the source IPv4 address could be handled by chip.

Buttons

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

Refresh: Click to manually refresh the page immediately.

|<< : Updates the table starting from the first entry in the IGMP SFM Information Table.

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

4-11.2 MLD Snooping

4-11.2.1 Status

This page displays MLD Snooping Status and details. To display MLD Snooping Status in the web UI:

1. Click Monitor, IPMC, MLD Snooping, Status.
2. To automatically refresh the information check Auto-refresh.
3. Click Refresh to refresh the page immediately or click Clear to clear the MLD Snooping Status.

The screenshot displays the MLD Snooping Status page. The left sidebar shows the navigation tree with 'Monitor' > 'IPMC' > 'MLD Snooping' > 'Status' selected. The main content area is titled 'MLD Snooping Status' and includes an 'Auto-refresh' checkbox, a refresh button, and a clear button. Below this are two tables: 'Statistics' and 'Router Port'.

VLAN ID	Querier Version	Host Version	Querier Status	Queries Transmitted	Queries Received	V1 Reports Received	V2 Reports Received	V1 Leaves Received
1	v2	v2	ACTIVE	1	1	0	2	0
10	v1	v1	ACTIVE	0	0	0	0	0

Port	Status
1	-
2	Both
3	Both
4	Both
5	Both
6	-
7	-
8	-
9	-
10	Dynamic

Figure 4-11.2.1: MLD Snooping Status

Parameter descriptions:

Statistics:

VLAN ID : The VLAN ID of the entry.

Querier Version : Working Querier Version currently.

Host Version : Working Host Version currently.

Querier Status : Show the Querier status is "ACTIVE" or "IDLE". "DISABLE" means 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 : Indicates whether specific port is a router port or not.

Buttons

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

Refresh: Click to refresh the page immediately.

Clear: Clears the counters for the selected port.

4-11.2.2 Group Information

This page displays the MLD Snooping Groups Information. The "Start from VLAN", and "group address" input fields let you select the starting point in the MLD Group table.

To display MLD Snooping Group information in the web UI:

1. Click Monitor, IPMC, MLD Snooping, Groups Information.
2. To automatically refresh the information check Auto-refresh.
3. Click Refresh to refresh the page immediately.
4. Click Clear to clear the page information.

VLAN ID	Groups	Port Members									
		1	2	3	4	5	6	7	8	9	10
1	ff02::fb	✓									
1	ff02::1:ff4f:bc3a	✓									
1	ff02::1:ffd4:ddc2						✓				

Figure 4-11.2.2: MLD Snooping Group Information

Parameter descriptions:

VLAN ID : VLAN ID of the group.

Groups : Group address of the group displayed.

Port Members : Ports under this group display a check mark (✓).

Buttons

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

Refresh: Click to refresh the page immediately.

<<: Updates the system log entries to the first available entry ID.

> : Updates the system log entry to the next available entry ID.

4-11.2.3 IPv6 SFM Information

This page displays MLD SFM Information table entries. The MLD SFM (Source-Filtered Multicast) Information Table also contains the SSM (Source-Specific Multicast) information. This table is sorted first by VLAN ID, then by group, and then by Port. Different source addresses belonging to the same group are treated as single entry.

To display the MLDv2 IPv6 SSM Information in the web UI:

1. Click Monitor, IPMC, MLD Snooping, IPv6 SFM Information.
2. To automatically refresh the information check Auto-refresh.
3. Click Refresh” to refresh the page immediately.
4. Click << or > to move to the previous or next entry.

VLAN ID	Group	Port	Mode	Source Address	Type	Hardware Filter/Switch
1	ff02::fb	1	Exclude	None	Deny	Yes
1	ff02::1:ff4f:bc3a	1	Exclude	None	Deny	Yes
1	ff02::1:ffd4:ddc2	6	Exclude	None	Deny	Yes

Figure 4-11.2.3: MLD SFM Information

Parameter descriptions:

VLAN ID : The VLAN ID of the group.

Group : Group address of the group displayed.

Port : Switch port number.

Mode : Indicates the filtering mode maintained per (VLAN ID, port number, Group Address) basis. It can be either Include or Exclude.

Source Address : IP Address of the source. Currently, system limits the total number of IP source addresses for filtering to be 128.

Type : Indicates the Type. It can be either Allow or Deny.

Hardware Filter/Switch : Indicates whether data plane destined to the specific group address from the source IPv6 address could be handled by chip.

Buttons

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

Refresh: Click to refresh the page immediately.

<<: Updates the system log entries to the first available entry ID.

> : Updates the system log entry to the next available entry ID.

4-12 LLDP

4-12.1 Neighbor

This page provides a status overview for all LLDP neighbors. The displayed table contains a row for each port on which an LLDP neighbor is detected. If your network has no LLDP devices then the table displays “No LLDP neighbor information found”.

To view LLDP neighbors’ information in the web UI:

1. Click Monitor, LLDP, Neighbors.
2. You can click the linked text in the Management Address column to display the device’s webpage.
3. Click Refresh to manually update the page immediately.
4. Click Auto-refresh to automatically update the page every 3 seconds.

Local Port	Chassis ID	Port ID	Port Description	System Name	System Capabilities	System Description	Management Address
Port 1	00-C0-F2-49-39-30	9	GigabitEthernet 1/9	SISPM1040-582-LRT	Bridge(+)	Managed Hardened PoE++ Switch (8) 10/100/1000Base-T PoE++ Ports + (2) 100/1000Base-X SFP Slot	192.168.1.77 (IPv4)
Port 3	AC-CC-8E-BA-F7-C1	AC-CC-8E-BA-F7-C1	eth0	axis-acc8ebaf7c1	Bridge(-), WLAN Access Point(-), Router(-), Station Only(+)	AXIS P1447-LE Network Camera 7.35.2.3	192.168.0.90 (IPv4)
Port 9	00-C0-F2-49-39-30	1	GigabitEthernet 1/1	SISPM1040-582-LRT	Bridge(+)	Managed Hardened PoE++ Switch (8) 10/100/1000Base-T PoE++ Ports + (2) 100/1000Base-X SFP Slot	192.168.1.77 (IPv4)

Figure 4-12.1: LLDP Neighbor information

Parameter descriptions:

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

Chassis ID : The MAC address of the neighbor’s LLDP frames.

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

Port Description : The port description advertised by the neighbor unit (e.g., *GigabitEthernet 1/9*).

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

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

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

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

System Description : System Description is the description advertised by the neighbor unit (e.g., *Managed Hardened PoE++ Switch (8) 10/100/1000Base-T PoE++ Ports + (2) 100/1000Base-X SFP Slot*).

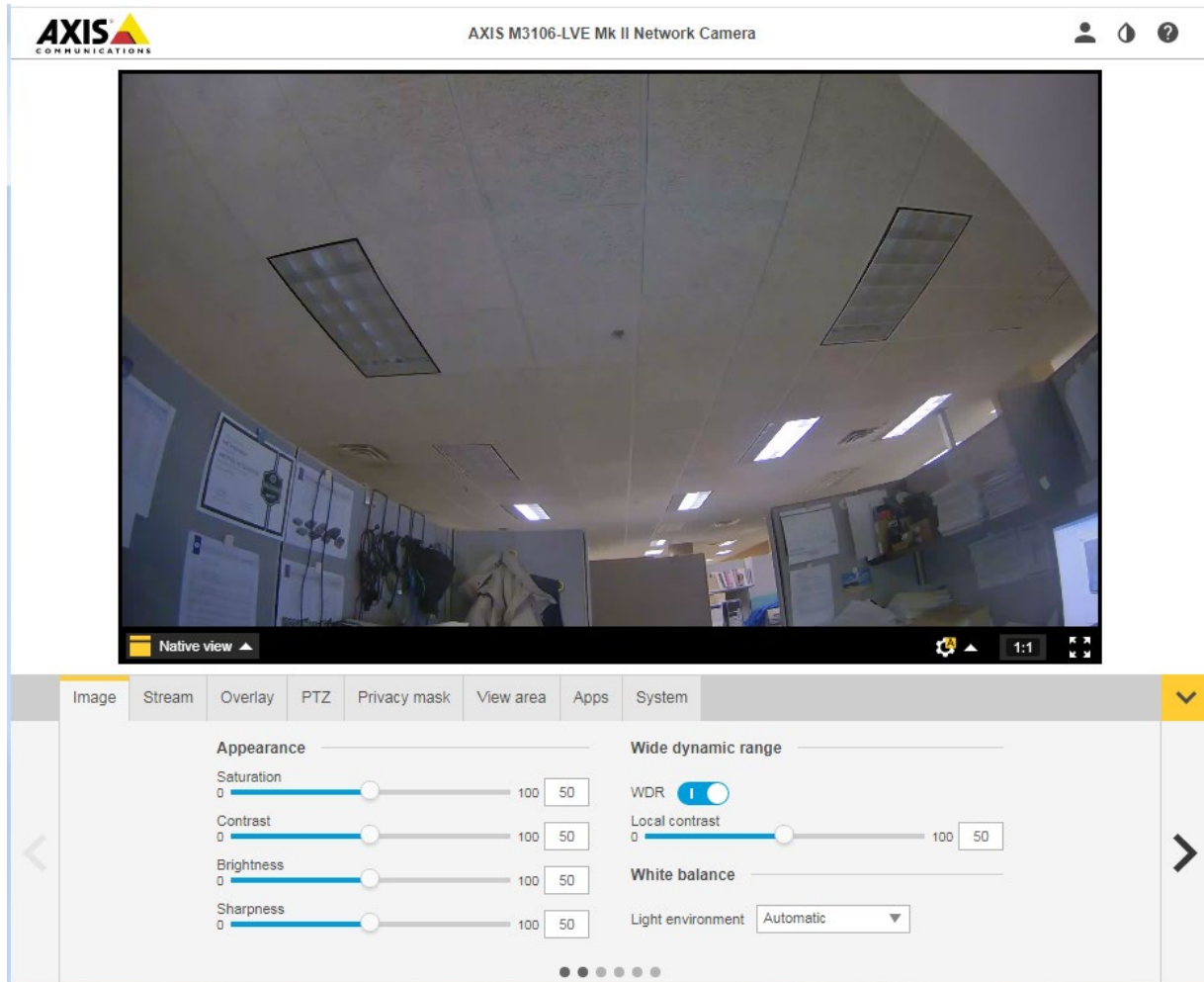
Management Address : Management Address is the neighbor unit's address that is used for higher layer entities to assist discovery by the network management. This could for instance hold the neighbor's IP address. You can click the linked text to display the device webpage. See the example below.

Buttons

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

Refresh: Click to manually refresh the page immediately.

Example



4-12.2 LLDP-MED Neighbor

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

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

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

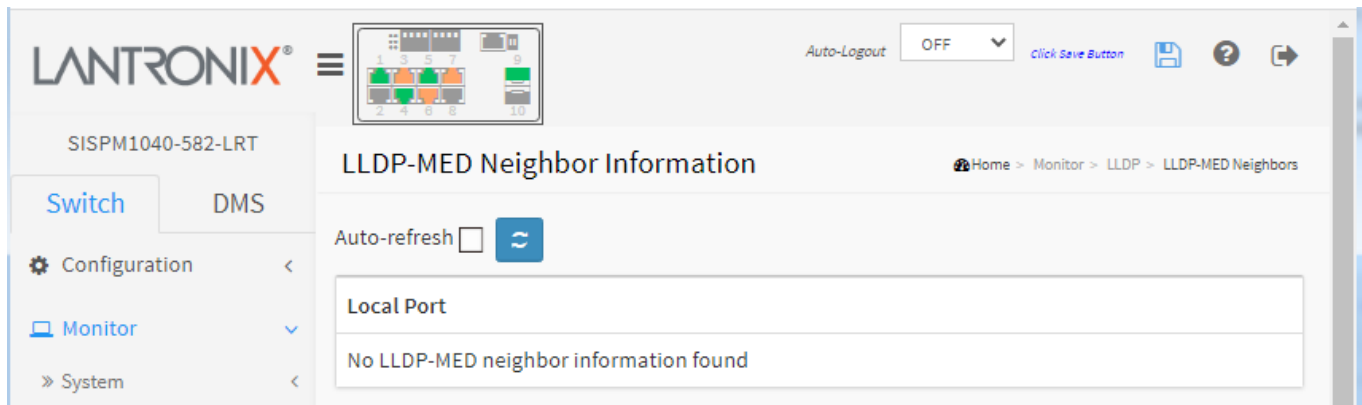


Figure 4-12.2: LLDP-MED Neighbors information

Note: If your network has no LLDP devices then the table displays “*No LLDP-MED neighbor information found*”.

Parameter descriptions: (before FW VB7.20.0171):

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

1. LAN Switch/Router
2. IEEE 802.1 Bridge
3. IEEE 802.3 Repeater (included for historical reasons)
4. IEEE 802.11 Wireless Access Point
5. Any device that supports the IEEE 802.1AB and MED extensions defined by TIA-1057 and can relay IEEE 802 frames via any method.

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

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

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

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

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

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

LLDP-MED Capabilities : The neighborhood unit's LLDP-MED capabilities, including:

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

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

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

6. Video Conferencing - for use by dedicated Video Conferencing equipment and other similar appliances supporting real-time interactive video/audio services.
7. Streaming Video - for use by broadcast or multicast based video content distribution and other similar applications supporting streaming video services that require specific network policy treatment. Video applications relying on TCP with buffering would not be an intended use of this application type.
8. Video Signaling - for use in network topologies that require a separate policy for the video signaling than for the video media.

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

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

Defined: The network policy is defined.

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

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

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

VLAN ID : VLAN ID is the VLAN identifier (VID) for the port as defined in IEEE 802.1Q-2003. A value of 1 - 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 - 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 - 63).

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

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

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

Buttons

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

Refresh: Click to manually refresh the page immediately.

LLDP-MED Neighbor Information (at FW VB7.20.0146):

Port 2			
Device Type	Capabilities		
Endpoint Class I	LLDP-MED Capabilities		
Auto-negotiation	Auto-negotiation status	Auto-negotiation Capabilities	MAU Type
Supported	Enabled	1000BASE-T full duplex mode	Invalid MAU Type

Parameter descriptions: (at FW VB7.20.0146):

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.

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

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

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

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

Auto-negotiation Capabilities : Shows the link partners MAC/PHY capabilities (e.g., *1000BASE-T full duplex mode*).

MAU Type : Displays the type of Medium Attachment Unit (e.g., *Invalid MAU Type*).

Buttons

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

Refresh : Click to refresh the page.

4-12.3 PoE

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

To show LLDP neighbor PoE information in the web UI:

1. Click Monitor, LLDP, PoE.
2. View the LLDP Power Over Ethernet Information.
3. Use the Auto-refresh and Refresh buttons as needed.

Local Port	Power Type	Power Source	Power Priority	Maximum Power
4	PSE Device	Unknown	Unknown	0 [W]
5	PSE Device	Unknown	Unknown	0 [W]
9	PSE Device	Primary Power Supply	Low	0 [W]
10	PSE Device	Primary Power Supply	Low	0 [W]

Figure 4-12.3: LLDP Neighbor Power Over Ethernet Information

Local Port : The port 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 Supply or its Backup Power Source. If it is unknown whether the PSE device is using its Primary Power Supply 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 port that is sourcing the power. There are three levels of power priority: Critical, High and Low. If the power priority is unknown it is indicated as "Unknown".

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

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

Buttons

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

Refresh: Click to refresh the page immediately.

4-12.4 EEE

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

By using EEE power savings can be achieved at the expense of traffic latency. This latency occurs due to that the circuits 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" as a way to agree on the minimum wakeup time they need.

To show LLDP neighbors EEE information in the web UI:

1. Click Monitor, LLDP, EEE to show discovered EEE devices.
2. Click Refresh to manually update the page immediately.
3. Click Auto-refresh to automatically update the page every 3 seconds.

Local Port	Tx Tw	Rx Tw	Fallback Receive Tw	Echo Tx Tw	Echo Rx Tw	Resolved Tx Tw	Resolved Rx Tw	EEE in Sync
1	0	0	0	0	0	30	30	●
3	0	0	0	0	0	30	30	●
9	0	0	0	0	0	30	30	●

Figure 4-12.4: LLDP Neighbors EEE Information

Note: If your network has no devices with EEE enabled the table will show “No LLDP EEE information found”.

Parameter descriptions:

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

Tx Tw : The link partner’s maximum time that the transmit path can hold off sending data after reassertion of LPI.

EEE uses a method called Low Power Idle (LPI) whose concept is to transmit data as fast as possible, and then return to Low-Power Idle.

Rx Tw : The link partner’s time that the 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 partner’s reflection (echo) of the remote link partners respective values. When a local link partner receives its echoed values from the remote link partner it can determine whether or not the remote link partner has received, registered and processed its most recent values. For example, if the local link partner receives

echoed parameters that do not match the values in its local MIB, then the local link partner infers that the remote link partners request was based on stale information.

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

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

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

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

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

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

Buttons

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

Refresh: Click to refresh the page immediately.

4-12.5 Port Statistics

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

To show LLDP counters in the web UI:

1. Click Monitor, LLDP, Port Statistics to show the LLDP counters.
2. Click Refresh to manually update the page immediately or
3. Click Auto-refresh to automatically update the page every 3 seconds.
4. Click Clear to clear all counters.

The screenshot shows the Lantronix web UI for device SISPM1040-582-LRT. The left sidebar contains a navigation menu with 'Monitor' selected, and 'LLDP' > 'Port Statistics' highlighted. The main content area is titled 'LLDP Counters' and includes an 'Auto-refresh' control. It displays two tables: 'LLDP Global Counters' and 'LLDP Statistics Local Counters'.

LLDP Global Counters	
Neighbor entries were last changed	2022-02-05T06:54:22+00:00 (18307 secs. ago)
Total Neighbors Entries Added	4
Total Neighbors Entries Deleted	1
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	8026	7964	0	0	0	0	0	0
2	0	0	0	0	0	0	0	0
3	7977	8300	0	0	0	0	0	0
4	8029	0	0	0	0	0	0	0
5	7966	0	0	0	0	0	0	0
6	7967	0	0	0	0	0	0	0
7	7963	0	0	0	0	0	0	0
8	0	0	0	0	0	0	0	0
9	7965	7962	0	0	0	0	7962	0
10	0	0	0	0	0	0	0	0

Figure 4-12.5: LLDP Counters

Parameter descriptions:

LLDP Global Counters

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

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

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

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

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

LLDP Statistics Local Counters

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

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

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

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

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

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

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

Org. Discarded : The number of organizationally received TLVs.

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

Buttons

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

Refresh: Click to refresh the page immediately.

Clear: Clears the counters for the selected port.

4-13 Ethernet Services

4-13.1 EVC Statistics

This page provides NNI port traffic statistics for the selected EVC. It shows counters for UNI ports of ECEs mapping to the EVC and the MPLS Pseudo-Wires counters included when the PW ID is attached to the selected EVC.

To show EVC Statistics in the web UI:

1. Click Monitor, Ethernet Statistics.
2. At the Port select dropdown select a port.
3. Click Refresh to manually update the page immediately.
4. Click Auto-refresh to automatically update the page every 3 seconds.
5. Click Clear to clear all counters

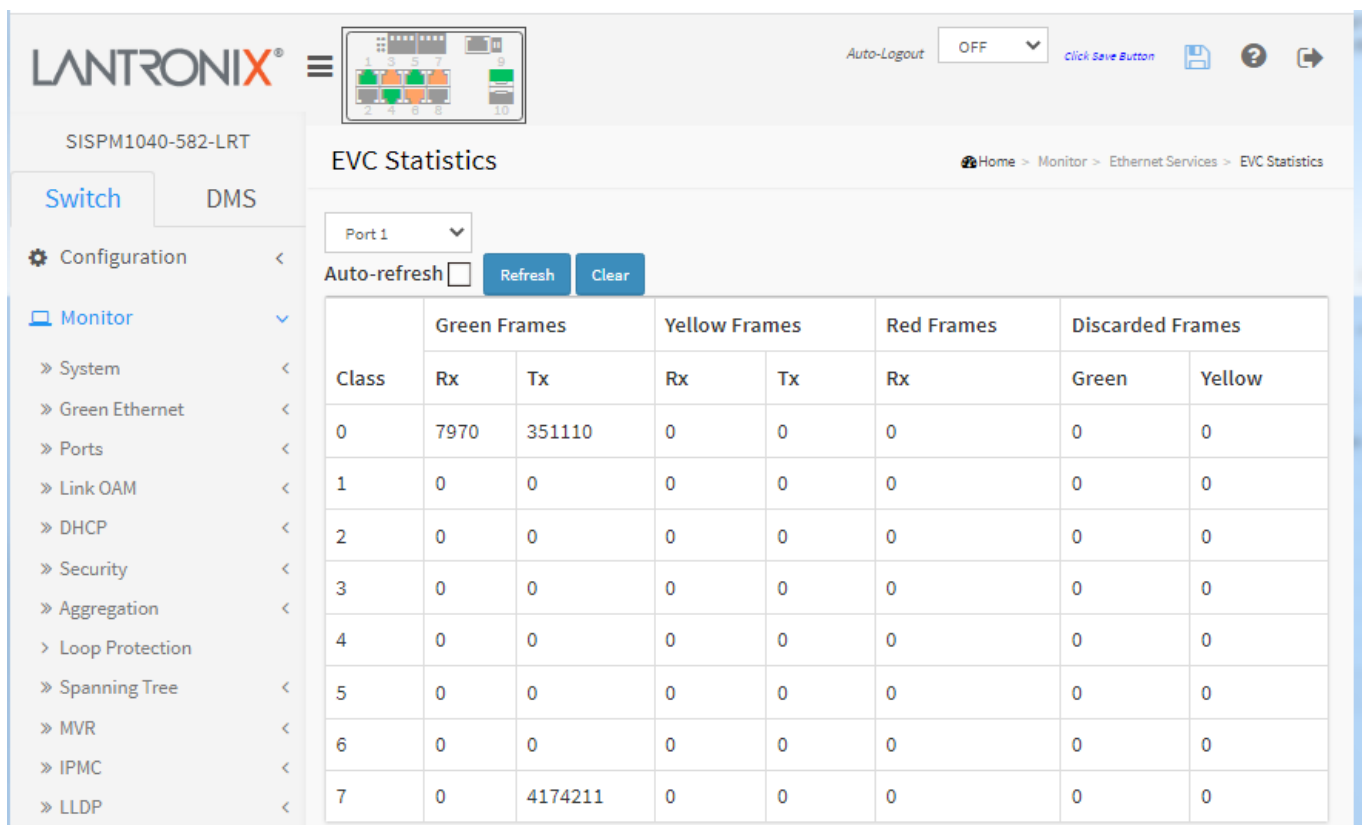


Figure 4-13.1: Ethernet Statistics

Parameter descriptions:

Class : The traffic class for the EVC.

Rx Green : The number of green frames received.

Tx Green : The number of green frames transmitted.

Rx Yellow : The number of yellow frames received.

Tx Yellow : The number of yellow frames transmitted.

Rx Red : The number of red frames received.

Green Discarded : The number of discarded green frames.

Yellow Discarded : The number of discarded yellow frames.

Buttons

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

Refresh: Click to refresh the page immediately.

Clear: Clears the counters for the selected port.

Messages:

All EVC statistics will be cleared.

Do you want to proceed anyway?

4-14 PTP

This page displays the current PTP clock settings. To show PTP parameters in the web UI:

1. Click Monitor, PTP.
2. Click Refresh to manually update the page immediately.
3. Click Auto-refresh to automatically update the page every 3 seconds.
4. Click a linked instance number to display its PTP Clock's Configuration details.

The screenshot shows the web UI for SISPM1040-582-LRT. The main content area is titled "PTP External Clock Mode". It contains a configuration table with the following data:

Parameter	Value
One_PPS_Mode	Disable
External Enable	False
Adjust Method	LTC frequency
Clock Frequency	1

Below this is the "PTP Clock Configuration" section, which includes an "Auto-refresh" checkbox (unchecked) and a "Refresh" button. Underneath is a "Port List" table:

Instance	Device Type	Port List											
		1	2	3	4	5	6	7	8	9	10		
0	Mastronly		✓	✓	✓								
1	Slaveonly				✓	✓							
2	P2pTransp						✓	✓					
3	Ord-Bound								✓	✓	✓		

Figure 4-14: PTP External Clock Mode

Parameter descriptions:

PTP External Clock Description

One_PPS_Mode : Shows the current One_pps_mode configuration:

Output : Enable the 1 pps clock output.

Input : Enable the 1 pps clock input.

Disable : Disable the 1 pps clock in/out-put.

External Enable : Shows the current External clock output configuration.

True : Enable the external clock output.

False : Disable the external clock output.

Adjust Method : Shows the current Frequency adjustment configuration.

LTC frequency : Local Time Counter (LTC) frequency control.

SyncE-DPLL : SyncE DPLL frequency control, if allowed by SyncE.

Oscillator : Oscillator independent of SyncE for frequency control, if supported by the HW.

LTC phase : Local Time Counter (LTC) phase control (assumes that the frequency is locked by means of SyncE).

Clock Frequency : Shows the current clock frequency used by the External Clock. The possible values are 1 - 25000000 (1 - 25MHz).

PTP Clock Description

Inst : Indicates the Instance of a particular Clock Instance [0..3]. Click on the Clock Instance number to monitor the Clock details. See below.

ClkDom : Indicates the Clock domain used by the Instance of a particular Clock Instance [0..3].

Device Type : Indicates the Type of the Clock Instance. There are five Device Types.

Ord-Bound - Clock's Device Type is Ordinary-Boundary Clock.

P2p Transp - Clock's Device Type is Peer to Peer Transparent Clock.

E2e Transp - Clock's Device Type is End to End Transparent Clock.

Master Only - Clock's Device Type is Master Only.

Slave Only - Clock's Device Type is Slave Only.

Port List : Shows the ports configured for that Clock Instance.

Buttons

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

Refresh: Click to refresh the page immediately.

Click on the linked Clock Instance number to view the PTP Clock's Configuration details:

The screenshot displays the 'PTP Clock's Configuration' page for a device named 'SISPM1040-582-LRT'. The interface includes a navigation sidebar on the left with categories like Configuration, Monitor, and Diagnostics. The main content area is divided into several sections:

- Local Clock Current Time:** Shows the current PTP time as 1970-01-02T02:20:55+00:00:489,857,800 and the adjustment method as Software. A 'Parts Monitor Page' link is also present.
- Clock Default DataSet:** A table with columns: Clock ID, Device Type, 2 Step Flag, Ports, Clock Identity, Dom, Clock Quality, Pri1, Pri2, Protocol, One-Way, VLAN Tag Enable, VID, PCP, DSCP. Row 1 shows ID 1, Ord-Bound, False, 10 ports, and Ethernet protocol.
- Clock Current DataSet:** A table with columns: stpRm, Offset From Master, Mean Path Delay, Slave Port, Slave State, Holdover(ppb). Row 1 shows Offset 0.000,000,000 and Slave State FREERUN.
- Clock Parent DataSet:** A table with columns: Parent Port ID, Port, PStat, Var, ChangeRate, GrandMaster Identity, GrandMaster Clock Quality, Pri1, Pri2. Row 1 shows Parent Port ID 00:c0:f2:ff:fe:49:38:00 and GrandMaster Identity 00:c0:f2:ff:fe:49:38:00.
- Port Configuration Table:** A table with columns: Port, Mode, and various status indicators. Rows 1-3 show ports 1, 2, and 3 with modes Slaveonly, P2pTransp, and Ord-Bound respectively.
- Clock Time Properties DataSet:** A table with columns: UtcOffset, Valid, leap59, leap61, Time Trac, Freq Trac, PTP Time Scale, Time Source. Row 1 shows Valid: False, PTP Time Scale: True, Time Source: 160.
- Servo Parameters:** A table with columns: Display, P-enable, I-enable, D-enable, 'P' constant, 'I' constant, 'D' constant. Row 1 shows P-enable: True, 'P' constant: 3, 'I' constant: 80, 'D' constant: 40.
- Filter Parameters:** A table with columns: Filter Type, DelayFilter, Period, Dist. Row 1 shows Filter Type: Basic, DelayFilter: 6, Period: 1, Dist: 2.
- Unicast Slave Configuration:** A table with columns: Index, Duration, IP_Address, Grant, CommState. Rows 0-4 show Index 0-4, Duration 100, IP_Address 0.0.0.0, Grant 0, and CommState IDLE.

Parameter Descriptions:

Local Clock Current time : Shows local clock data

PTP Time : Shows the actual PTP time with nanosecond resolution.

Clock Adjustment Method : Shows the actual clock adjustment method. The method depends on the available hardware.

Ports Monitor Page : Click the link to monitor the port data set for the ports assigned to this clock instance. See below.

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 configurable members which can be set here.

Clock ID : An internal instance ID (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.

2 Step Flag : True if two-step Sync events and Pdelay_Resp events are used.

Ports : The total number of physical ports in the node.

Clock Identity : Shows the unique clock identifier.

Dom : Clock domain [0..127].

Clock Quality : The clock quality is determined by the system, and holds 3 parts: Clock Class, Clock Accuracy, and OffsetScaledLog Variance as defined in IEEE1588. The Clock Accuracy values are defined in IEEE1588 table 6 (Currently the clock Accuracy is set to 'Unknown' as default).

Pri1 : Clock priority 1 [0..255] used by the BMC master select algorithm.

Pri2 : Clock priority 2 [0..255] used by the BMC master select algorithm.

Protocol : Transport protocol used by the PTP protocol engine:

Ethernet : PTP over Ethernet multicast

ip4multi : PTP over IPv4 multicast

ip4uni : PTP over IPv4 unicast

Note : IPv4 unicast protocol only works in Master only and Slave only clocks. See *Device Type* parameter.

In a unicast Slave only clock you also need configure which master clocks to request Announce and Sync messages from. See *Unicast Slave Configuration*.

One-Way : If true, one-way measurements are used. This parameter applies only to a slave. In one-way mode no delay measurements are performed (i.e., this is applicable only if frequency synchronization is needed. The master always responds to delay requests.

VLAN Tag Enable : Enables the VLAN tagging for the PTP frames. **Note**: Packets are only tagged if the port is configured for VLAN tagging for the configured VLAN (i.e., the VLAN Tag Enable parameter is ignored).

VID : VLAN Identifier used for tagging the PTP frames.

PCP : Priority Code Point value used for PTP frames.

Clock current Data Set : The clock current data set is defined in the IEEE 1588 Standard. The current data set is dynamic

stpRm : Steps Removed : The number of PTP clocks traversed from the grandmaster to the local slave clock.

Offset from master : Time difference between the master clock and the local slave clock, measured in ns.

mean Path Delay : The mean propagation time for the link between the master and the local slave

Slave Port : Shows which port is in slave mode. The value is 0 if no ports are in slave mode.

Slave State : Shows the synchronization state of the slave.

Holdover(ppb) : After the slave has been in Locked mode during the stabilization period, this value shows the actual clock offset between the freerun and the actual holdover frequency, the value is shown in parts per billion (ppb). During the stabilization period, the value is shown as N.A. The default stabilization period is 60 seconds and it can be changed from the CLI.

Clock Parent Data Set : The clock parent data set is defined in the IEEE 1588 standard. The parent data set is dynamic.

Parent Port ID : Clock identity for the parent clock, if the local clock is not a slave, the value is the clocks own id.

Port : Port Id for the parent master port

PStat : Parents Stats (always false).

Var : It is observed parent offset scaled log variance

Change Rate : Observed Parent Clock Phase Change Rate. i.e. the slave clocks rate offset compared to the master. (unit = ns per s).

Grand Master Identity : Clock identity for the grand master clock, if the local clock is not a slave, the value is the clocks own id.

Grand Master Clock Quality : The clock quality announced by the grand master (See *Clock Default DataSet:Clock Quality*).

Pri1 : Clock priority 1 announced by the grand master

Pri2 : Clock priority 2 announced by the grand master.

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 default clock servo uses a PID regulator to calculate the current clock rate. i.e.

clockAdjustment =
OffsetFromMaster/ P constant +
Integral(OffsetFromMaster)/ I constant +
Differential OffsetFromMaster)/ D constant

Display : If true then Offset From Master, MeanPathDelay and clockAdjustment are logged on the debug terminal

P-enable : If true the P part of the algorithm is included

I-Enable : If true the I part of the algorithm is included

D-enable : If true the D part of the algorithm is included

'P' constant : [1..1000] see above

'I' constant : [1..10000] see above

'D' constant : [1..10000] see above

Filter Parameters : The default delay filter is a low pass filter, with a time constant of $2 * \text{DelayFilter} * \text{DelayRequestRate}$.

If the DelayFilter parameter is set to 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.

If **Dist** is 1 the offset is averaged over the **Period**,

If **Dist** is >1 the offset is calculated using 'min' offset.

DelayFilter : See above

Filter Type : Shows the filter type used which can be either the basic filter or an advanced filter that can be configured to use only a fraction of the packets received (i.e. the packets that have experienced the least latency).

Period : See above

dist : See above

Height : The height of the sample window measured in microseconds (only applicable to advanced offset filter).

Percentage : The percentage of sync packets (with smallest delay) used by the offset filter (only applicable to advanced offset filter).

Reset Threshold : The threshold in micro seconds at which the offset filter will be reset and the slave clock synchronized to the master.

Unicast Slave Configuration : When operating in IPv4 Unicast mode, the slave is configured with up to five 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.

Duration : The number of seconds a master is requested to send Announce/Sync messages. The request is repeated from the slave each Duration/4 seconds.

IP_address : IPv4 Address of the master clock.

grant : The granted repetition period for the sync message

CommState : The state of the communication with the master, possible values are:

IDLE : The entry is not in use.

INIT : Announce is sent to the master (Waiting for a response).

CONN : The master has responded.

SELL : The assigned master is selected as current master.

SYNC : The master is sending Sync messages.

Buttons

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

Refresh: Click to refresh the page immediately.

Port 1	▼
Port 1	
Port 99	

Port Select box : Dropdown to select the current port to be displayed.

When you click the linked [Ports Monitor](#) the PTP Clock's Port Data Set Configuration page displays:

Port	Stat	MDR	PeerMeanPathDel	Anv	ATo	Syv	Dlm	MPR	Delay Asymmetry	Ingress Latency	Egress Latency	Version
2	mstr	0	0.000,000,000	0	3	0	e2e	0	0.000,000,000	0.000,000,000	0.000,000,000	2
3	mstr	0	0.000,000,000	0	3	0	e2e	0	0.000,000,000	0.000,000,000	0.000,000,000	2
4	mstr	0	0.000,000,000	0	3	0	e2e	0	0.000,000,000	0.000,000,000	0.000,000,000	2

Parameter Descriptions: The port data set is defined in the IEEE 1588 Standard.

Port Data Set :

Port : Port number [1..max port no].

Stat : Current state of the port.

MDR : log Min Delay Req Interval: The delay request interval announced by the master.

Peer Mean Path Del : The path delay measured by the port in P2P mode. In E2E mode this value is 0.

Anv : The interval for issuing announce messages in master state.

ATo : The timeout for receiving announce messages on the port.

Syv : The interval for issuing sync messages in master.

Dlm : delayMechanism: The delay mechanism used for the port:

e2e : End to end delay measurement

p2p : Peer to peer delay measurement.

MPR : The interval for issuing Delay_Req messages for the port in E2e mode. This value is announced from the master to the slave in an announce message. The value is reflected in the MDR field in the Slave. The interval for issuing Pdelay_Req messages for the port in P2P mode. **Note:** The interpretation of this parameter has changed from release 2.40. In earlier versions the value was interpreted relative to the Sync interval, this was a violation of the standard, so now the value is interpreted as an interval. I.e. MPR = 0 => 1 Delay_Req pr sec, independent of the Sync rate.

Delay Asymmetry : The transmission delay asymmetry for a link. See IEEE 1588 Section 7.4.2 Communication path asymmetry.

Version : The current implementation only supports PTP version 2.

Ingress latency : Ingress latency measured in ns, as defined in IEEE 1588 Section 7.3.4.2.

Egress Latency : Egress latency measured in ns, as defined in IEEE 1588 Section 7.3.4.2.

Buttons

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

Refresh: Click to refresh the page immediately.

4-15 PoE

This page displays the current status for all PoE ports. To display PoE port status in the web UI:

1. Click Monitor, PoE.
2. Check Auto-refresh to refresh the page automatically every 3 seconds.
3. Click Refresh to refresh the page immediately.

The screenshot shows the 'Power Over Ethernet Status' page in the Lantronix web UI. The page title is 'Power Over Ethernet Status' and the breadcrumb is 'Home > Monitor > PoE'. There is an 'Auto-refresh' checkbox and a refresh icon. Below this is a table with the following data:

Local Port	PD class	Power Requested	Power Allocated	Power Used	Current Used	Priority	Port Status
1	1	4 [W]	4 [W]	1.8 [W]	33 [mA]	Low	PoE turned ON
2	-	0 [W]	0 [W]	0 [W]	0 [mA]	Low	No PD detected
3	3	15 [W]	15 [W]	3.2 [W]	59 [mA]	Low	PoE turned ON
4	-	0 [W]	0 [W]	0 [W]	0 [mA]	Low	No PD detected
5	1	4 [W]	4 [W]	1.8 [W]	33 [mA]	Low	PoE turned ON
6	2	7 [W]	7 [W]	1.9 [W]	35 [mA]	Low	PoE turned ON
7	4	30 [W]	30 [W]	7 [W]	126 [mA]	Low	PoE turned ON
8	-	0 [W]	0 [W]	0 [W]	0 [mA]	Low	No PD detected
Total		60 [W]	60 [W]	15.7 [W]	286 [mA]		

Figure 4-15: PoE Status

Parameter descriptions:

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

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

Buttons

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

Refresh: Click to refresh the page immediately.

4-16 MAC Table

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

1. Click Monitor, MAC Table.
2. Specify the Start from VLAN and MAC address entries per page.
3. View the MAC Address Table parameters.

The screenshot shows the Lantronix web interface for the SISPM1040-582-LRT device. The 'Monitor' section is active, and the 'MAC Address Table' is displayed. The interface includes a navigation menu on the left, a top navigation bar with 'Auto-Logout' set to 'OFF', and a breadcrumb trail: Home > Monitor > MAC Table. Below the breadcrumb, there are controls for 'Auto-refresh' (unchecked), a refresh button, and navigation arrows. The main configuration area shows 'Start from VLAN' set to 1 and 'entries per page' set to 20. The MAC Address Table is a grid with columns for Type, VLAN, MAC Address, CPU, and Port Members (1-10). The table contains 12 entries with various MAC addresses and port member indicators (green checkmarks).

Type	VLAN	MAC Address	Port Members											
			CPU	1	2	3	4	5	6	7	8	9	10	
Dynamic	1	00-09-18-4F-BC-3A								✓				
Dynamic	1	00-1B-11-B2-6D-4B					✓							
Static	1	00-C0-F2-49-39-30	✓											
Dynamic	1	00-C0-F2-49-39-39		✓										
Static	1	33-33-00-00-00-01	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Static	1	33-33-00-00-00-02	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Static	1	33-33-FF-49-39-30	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Dynamic	1	AC-CC-8E-BA-F7-C1				✓								
Dynamic	1	E0-55-3D-84-A8-96									✓			
Static	1	FF-FF-FF-FF-FF-FF	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓

Figure 4-16: MAC Address Table

Parameter descriptions:

Type : Indicates whether the entry is a static 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.

Buttons



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



Refresh: Click to refresh the page immediately.



Clear: Delete all dynamic entries from the table.



<<: First page; updates the system log entries to the first available entry ID.



>: Next page; updates the system log entry to the next available entry ID.

4-17 VLANs

4-17.1 Membership

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

1. Click Monitor, VLANs, Membership.
2. Select which set of VLAN users you want to be displayed.
3. Click Refresh to update the page immediately.

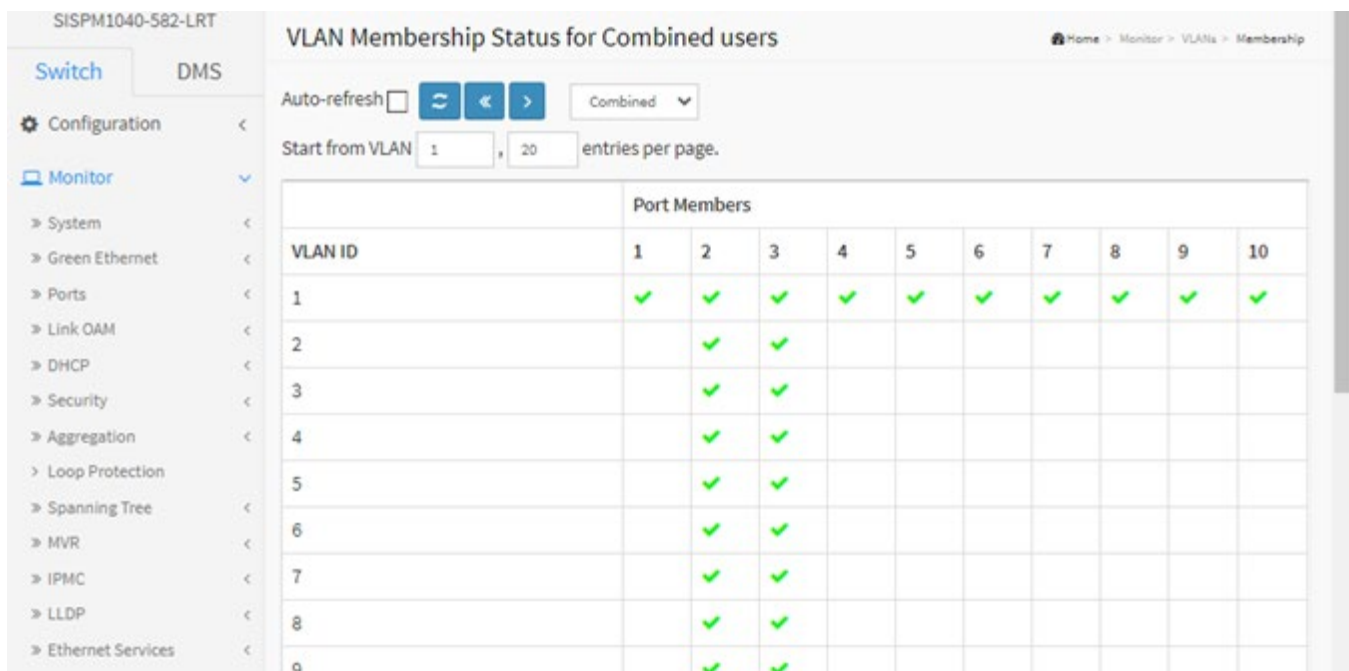


Figure 4-17.1: VLAN Membership Status for Combined users

Parameter descriptions:

VLAN User : Various internal software modules may use VLAN services to configure VLAN memberships on the fly.

The drop-down list on the right allows for selecting between showing VLAN memberships as configured by an administrator (Admin) or as configured by one of these internal software modules. These VLAN user types are supported:

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

Admin : VLAN memberships as configured by an administrator.

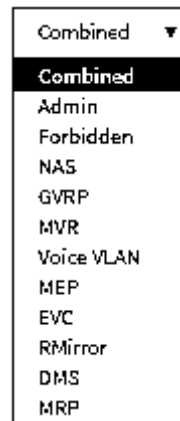
Forbidden : VLAN memberships that are forbidden VLANs.

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

GVRP : VLAN memberships configured by GVRP internal software module.

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.



MEP : VLAN memberships configured by MEP internal software module.

EVC : VLAN memberships configured by EVC internal software module.

RMirror : VLAN memberships configured by Mirroring internal software module.

DMS : VLAN memberships configured by Device Management System internal software module.

MRP : VLAN memberships configured by MRP software module.

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

Port Members : A row of check boxes for each port is displayed for each VLAN ID:




If a port is included in a VLAN, a green check mark displays.



If a port is included in a Forbidden port list, a red x displays ().



If a port is included in a Forbidden port list and dynamic VLAN user register VLAN on same Forbidden port, then conflict port will be displayed as .

VLAN Membership : 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 ALL VLAN Users are selected, it will show this information for all the VLAN Users, and this is by default. VLAN membership allows the frames classified to the VLAN ID to be forwarded on the respective VLAN member ports.

Buttons

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

Refresh: Click to refresh the page immediately.

<< : Updates the table starting from the first entry in the table.

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

Example : VLAN Membership Status for Forbidden user:

The screenshot shows the 'VLAN Membership Status for Forbidden user' page. It features a navigation menu on the left with 'Switch' and 'DMS' tabs. The main content area includes an 'Auto-refresh' checkbox, navigation buttons (refresh, left, right), a dropdown menu set to 'Forbidden', and a 'Start from VLAN' field set to '1' with '20 entries per page'. Below this is a table with columns for 'VLAN ID' and 'Port Members' (ports 1-10). The table data is as follows:

VLAN ID	1	2	3	4	5	6	7	8	9	10
100										
200										

4-17.2 Ports

This page displays information on all VLAN status and reports it by VLAN User Types.

To display VLAN Port Status in the web UI:

1. Click Monitor, VLANs, Ports.
2. At the User select dropdown select the user type (Combined, Admin, Forbidden, NAS, GVRP, etc.).
3. View the displayed Port Status information.

The screenshot shows the 'VLAN Port Status for Combined users' page. The table below represents the data shown in the interface:

Port	Port Type	Ingress Filtering	Frame Type	Port VLAN ID	Tx Tag	Untagged VLAN ID	Conflicts
1	C-Port	<input checked="" type="checkbox"/>	All	1	Tag All		No
2	C-Port	<input checked="" type="checkbox"/>	All	1	Untag All		No
3	C-Port	<input checked="" type="checkbox"/>	All	1	Untag All		No
4	C-Port	<input checked="" type="checkbox"/>	All	1	Tag All		No
5	C-Port	<input checked="" type="checkbox"/>	All	1	Untag All		No
6	C-Port	<input checked="" type="checkbox"/>	All	1	Untag All		No
7	C-Port	<input checked="" type="checkbox"/>	All	1	Untag All		No
8	C-Port	<input checked="" type="checkbox"/>	All	1	Untag All		No
9	C-Port	<input checked="" type="checkbox"/>	All	1	Untag All		No
10	C-Port	<input checked="" type="checkbox"/>	All	1	Untag All		No

Figure 4-17.2: VLAN Port Status for Static user

Parameter descriptions:

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

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

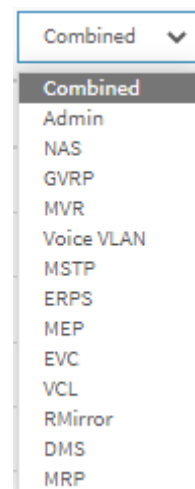
These VLAN user types are supported:

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

Admin : VLAN memberships as configured by an administrator.

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

GVRP : VLAN memberships configured by GVRP internal software module.



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 : VLAN memberships configured by MSTP internal software module.

ERPS : VLAN memberships configured by Ethernet Ring Protection Switching internal software module.

MEP : VLAN memberships configured by Maintenance Entity end Point internal software module.

EVC : VLAN memberships configured by Ethernet Virtual Circuit internal software module.

VCL : VLAN memberships configured by VLAN Control List internal software module.

RMirror : VLAN memberships configured by Mirroring internal software module.

DMS : VLAN memberships configured by Device Management System internal software module.

MRP : VLAN memberships configured by Media Redundancy Protocol internal software module.

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, Tagged, 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 egress filtering frame status whether tagged or untagged. Shows the Tx Tag requirements (Tag All, Tag PVID, Tag UVID, Untag All, Untag PVID, Untag UVID) that a given user has on a port. The field is empty if not overridden by the selected user.

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

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

Buttons

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

Refresh: Click to refresh the page immediately.

4-18 MRP

This page displays the Media Redundancy Protocol (MRP) Profile, Events, and Statistics.

MRP is a data network protocol standardized by the International Electrotechnical Commission as IEC 62439-2. MRP allows rings of Ethernet switches to overcome any single failure with recovery time much faster than achievable with Spanning Tree Protocol. MRP is suitable for most Industrial Ethernet applications.

In an MRP ring, the ring manager is named Media Redundancy Manager (MRM), while ring clients are named Media Redundancy Clients (MRCs). MRM and MRC ring ports support three status: disabled, blocked, and forwarding. Disabled ring ports drop all the received frames. Blocked ring ports drop all the received frames except the MRP control frames. Forwarding ring ports forward all the received frames.

The screenshot displays the 'Media Redundancy Protocol Status' page. On the left is a navigation menu with 'Monitor' selected. The main content area is divided into three sections:

- Domain Profile:** A table showing the configuration for two domains.
- Domain Events:** A table listing recent events, including 'Ring Open' for Domain1.
- Domain Statistics:** A table showing MRP transmitted frames, received frames (total, error, unrecognized), and round trip delay (min, max) for each domain.

Name	Oper. Role	Ring State	Primary		Secondary	
			Port	State	Port	State
Domain1	Manager	Open	1	Forwarding	2	Forwarding
Domain2	Client	-	3	Forwarding	4	Forwarding

Timestamp	Name	Event	Appear
2011-01-01T02:11:34+00:00	Domain1	Ring Open	True
2011-01-01T02:11:34+00:00	Domain1	Ring Open	False
2011-01-01T02:11:34+00:00	Domain1	Ring Open	True

Name	MRP Transmitted Frames		MRP Received Frames			Round Trip Delay, ms	
	Total		Total	Error	Unrecognized	Min	Max
Domain1	1130		0	0	0	0	0
Domain2	5		0	0	0	0	0

Domain Profile

Name: A logical name for the MRP domain to ease the management of MRP domains (e.g., *Domain1*).

Oper. Role: The operational role of an MRP entity per domain (i.e., *Manager* or *Client*).

Ring State: Ring state of the MRP entity (e.g., *Undefined*, *Not connected*, *Forwarding*).

Primary Port: The ifIndex of the layer 2 interface which is used as ring port 1 (e.g., *Open* or *-*).

Primary State: Ring status of the MRP entity (e.g., *Undefined*, *Not connected*, *Forwarding*).

Secondary Port: The ifIndex of the layer 2 interface which is used as ring port 2.

Secondary State: Ring status of the MRP entity (e.g., *Undefined*, *Not connected*, *Forwarding*).

Domain Events

Timestamp: The value of sysUpTime at the time of the logged event in the format *2020-04-15T16:01:01+00:00*.

Name: A logical name for the MRP domain (*Domain1, Domain2*).

Event: Event type (e.g., *Ring Open*).

Appear: Event *True* (appear) or *False* (disappear).

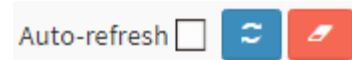
Domain Statistics

Name: The MRP domain name (*Domain1, Domain2*).

MRP Transmitted Frames: The Total number of transmitted frames for Domain1 and Domain2.

MRP Received Frames: The *Total, Error, and Unrecognized* received frames.

Round Trip Delay, (ms): Round-Trip-Delay (in milliseconds) which was measured since startup (**Minimum** and **Maximum** values).



Buttons

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

Refresh: Click to manually update the page immediately.

Clear: Click to clear the page data.

4-19 VCL

4-19.1 MAC-based VLAN

This page displays MAC-based VLAN entries configured by various MAC-based VLAN users.

To display MAC-based VLAN status in the web UI:

1. Click Monitor, VCL, MAC-based VLAN Status.
2. Specify the User type.
3. View the displayed MAC-based VLAN information.

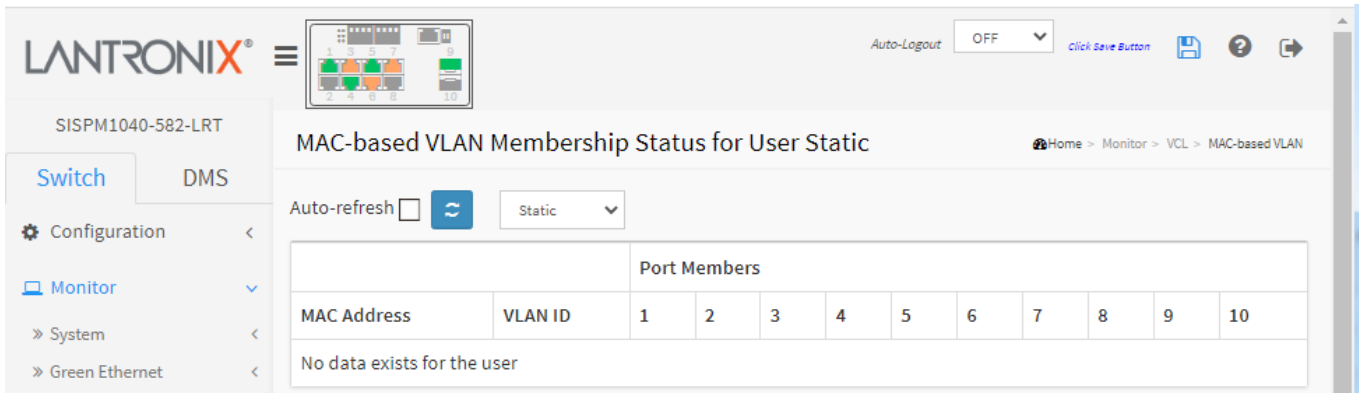


Figure 4-19.1: MAC-based VLAN Membership Status for User Static

Parameter descriptions:

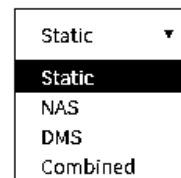
User Select dropdown: Select Static (default), NAS, DMS, or Combined.

Static : Refers to CLI/Web/SNMP as static.

NAS : Provides port-based authentication, involving communication between a Supplicant, Authenticator, and an Authentication Server.

DMS : Shows the set of current Device Management System user's data.

Combined : show a combination of all of the User types.



MAC Address : Indicates the MAC address.

VLAN ID : Indicates the VLAN ID.

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

Buttons

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

Refresh: Click to refresh the page immediately.

4-19.2 Protocol-based VLAN

4-19.2.1 Protocol to Group

This page shows the protocols to Group Name (unique for each Group) mapping entries for the switch.

To display Protocol-based VLAN configuration in the web UI:

1. Click Monitor, VCL, Protocol-based VLAN , Protocol to Group.
2. Check the Auto-refresh checkbox to refresh the page every 3 seconds.
3. Click Refresh to refresh the page immediately.

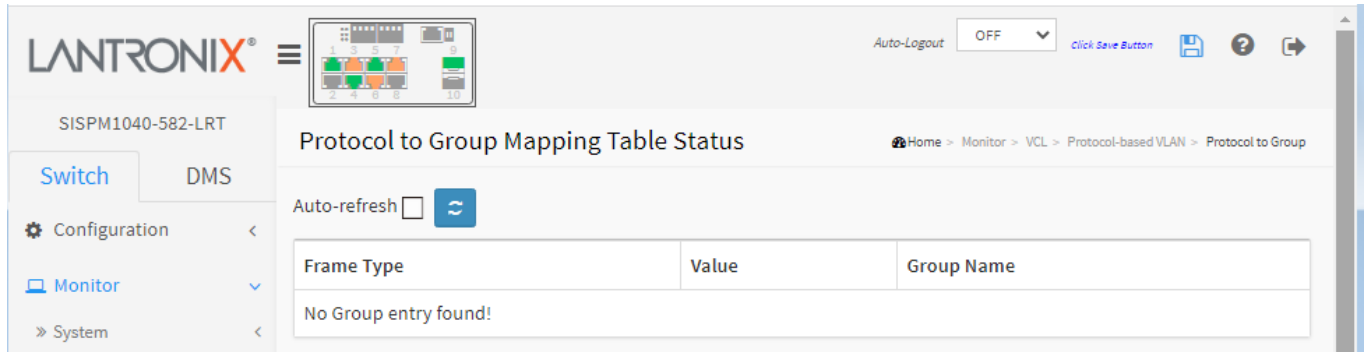


Figure 4-19.2.1: Protocol to Group Mapping Table Status

Parameter descriptions:

Frame Type : Frame Type can have one of these values: **Ethernet**, **LLC**, or **SNAP**.

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

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

1. For Ethernet: Values in the text field when Ethernet is selected as a Frame Type is called etype. Valid values for etype ranges from 0x0600-0xffff
2. For LLC: Valid value in this case is comprised of two different sub-values.
 - DSAP**: 1-byte long string (0x00-0xff)
 - SSAP**: 1-byte long string (0x00-0xff)
3. For SNAP: Valid value in this case also is comprised of two different sub-values.

OUI: OUI (Organizationally Unique Identifier) is value in format of xx-xx-xx where each pair (xx) in string is a hexadecimal value from 0x00 - 0xff.

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.

In other words, if value of OUI field is 00-00-00 then the value of PID will be etype (0x0600-0xffff) and if value of OUI is other than 00-00-00 then valid value of PID will be any value from 0x0000 to 0xffff.

Group Name : A valid Group Name is a unique 16-character long string for every entry which consists of a combination of alphabets (a-z or A-Z) and integers (0-9). **Note**: special character and underscore (_) are not allowed.

Buttons

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

Refresh: Click to refresh the page immediately.

4-19.2.2 Group to VLAN

This page displays the configured Group Name to a VLAN for the switch. To display Group Name to VLAN configuration in the web UI:

1. Click Monitor, VCL, Protocol-based VLAN, Group to VLAN.
2. Check the Auto-refresh checkbox to refresh the page every 3 seconds.
3. Click Refresh to refresh the page immediately.

The screenshot shows the Lantronix web interface for the SISPM1040-582-LRT device. The main content area is titled 'Group Name to VLAN mapping Table Status'. Below the title, there is an 'Auto-refresh' checkbox (unchecked) and a refresh icon. A table displays the mapping status for two groups, Grp1 and Grp2, across 10 ports. Green checkmarks indicate which ports are members of each group.

Group Name	VLAN ID	Port Members									
		1	2	3	4	5	6	7	8	9	10
Grp1	10		✓	✓	✓	✓					
Grp2	20		✓				✓	✓		✓	

Figure 4-19.2.2: Group Name to VLAN mapping Table Status

Parameter descriptions:

Group Name : A valid Group Name is a string of up to 16 characters which consists of a combination of alphabets (a-z or A-Z) and integers(0-9), no special character is allowed. Whichever Group name you try map to a VLAN must be present in Protocol to Group mapping table and must not be pre-used by any other existing mapping entry on this page.

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

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

Buttons

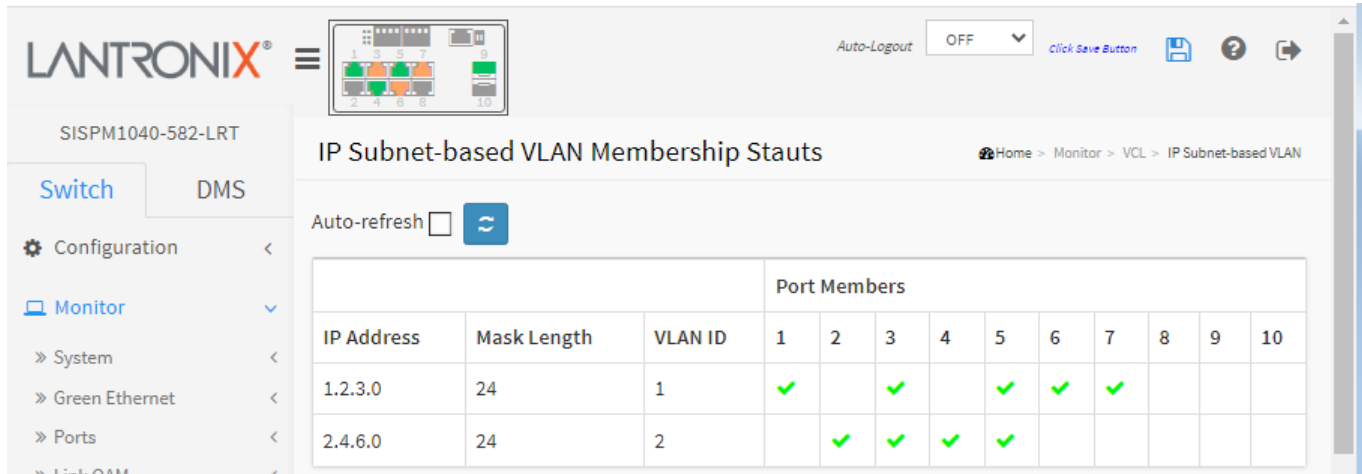
Auto-refresh: Check this box to refresh the page automatically every 3 seconds.

Refresh: Click to refresh the page immediately.

4-19.3 IP Subnet-based VLAN

The page shows IP subnet-based VLAN entries. This page shows only static entries. To display IP Subnet-based VLAN membership status in the web UI:

1. Click Monitor, VCL, and IP Subnet-based VLAN.
2. Check the Auto-refresh checkbox to refresh the page every 3 seconds.
3. Click Refresh to refresh the page immediately.



The screenshot shows the Lantronix web interface for the device SISPM1040-582-LRT. The page title is "IP Subnet-based VLAN Membership Status". There is an "Auto-refresh" checkbox which is currently unchecked, and a refresh button. Below this is a table with the following data:

IP Address	Mask Length	VLAN ID	Port Members											
			1	2	3	4	5	6	7	8	9	10		
1.2.3.0	24	1	✓		✓		✓	✓	✓					
2.4.6.0	24	2		✓	✓	✓	✓							

Figure 4-19.3: IP Subnet-based VLAN Membership Status

Parameter descriptions:

VCE ID : Indicates the index of the entry. It is user configurable. Its value ranges from 0-128. If a VCE ID is 0, the application will auto-generate the VCE ID for that entry. Deletion and lookup of IP subnet-based VLAN are based on VCE ID.

IP Address : Indicates the IP address.

Mask Length : Indicates the network mask length.

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

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

Buttons

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

Refresh: Click to manually refresh the page immediately.

4-20 sFlow

This page shows receiver and per-port sFlow statistics. To display the current sFlow configuration via the web UI:

1. Click Monitor, sFlow.
2. View the displayed sFlow information; use the buttons as needed.

The screenshot displays the 'sFlow Statistics' page in the Lantronix web UI. The page includes a navigation menu on the left with 'Monitor' selected, and a main content area with 'Receiver Statistics' and 'Port Statistics' sections. The 'Receiver Statistics' table shows fields like Owner, IP Address/Hostname, Timeout, Tx Successes, Tx Errors, Flow Samples, and Counter Samples, all with values of 0 or <none>. The 'Port Statistics' table shows columns for Port, Rx Flow Samples, Tx Flow Samples, and Counter Samples, with all values being 0 for ports 1 through 10.

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

Figure 4-20: sFlow Statistics

Receiver Statistics

Owner : This field shows the current owner of the sFlow configuration. It assumes one of these three values:

If sFlow is currently unconfigured/unclaimed, Owner contains <none>.

If sFlow is currently configured through Web or CLI, Owner contains <Configured through local management>.

If sFlow is currently configured through SNMP, Owner contains a *string* identifying the sFlow receiver.

IP Address/Hostname : The IP address or hostname of the sFlow receiver.

Timeout : The number of seconds remaining before sampling stops and the current sFlow owner is released.

Tx Successes : The number of UDP datagrams successfully sent to the sFlow receiver.

Tx Errors : The number of UDP datagrams that has failed transmission. The most common source of errors is invalid sFlow receiver IP/hostname configuration. To diagnose, paste the receiver's IP address/hostname into the Ping Web page (Diagnostics > Ping/Ping6).

Flow Samples : The total number of flow samples sent to the sFlow receiver.

Counter Samples : The total number of counter samples sent to the sFlow receiver.

Port Statistics

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

Rx and Tx Flow Samples : The number of flow samples sent to the sFlow receiver originating from this port. Here, flow samples are divided into Rx and Tx flow samples, where Rx flow samples contains the number of packets that were sampled upon reception (ingress) on the port and Tx flow samples contains the number of packets that were sampled upon transmission (egress) on the port.

Counter Samples : The total number of counter samples sent to the sFlow receiver originating from this port.

Buttons

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

Refresh: Click to refresh the page immediately.

Clear Receiver: Clears the sFlow receiver counters.

Clear Ports: Clears the per-port counters.

4-21 UDLD

This page displays the UDLD status of the ports or displays “No Neighbour ports enabled or no existing partners”. To display UDLD status in the web UI:

1. Click Monitor, UDLD.
2. At the Port Select dropdown select a port.
3. View the displayed UDLD information.

The screenshot displays the web interface for monitoring UDLD status on a specific port. The page title is 'Detailed UDLD Status for Port 6'. At the top, there is an 'Auto-refresh' checkbox and a refresh button, along with a dropdown menu set to 'Port 6'. Below this, the 'UDLD Status' section contains a table with the following data:

UDLD Admin state	Enable
Device ID(local)	00-C0-F2-49-38-FF
Device Name(local)	SISPM1040-582-LRT
Bidirectional State	Bi-directional

The 'Neighbour Status' section contains a table with the following data:

Port	Device Id	Link Status	Device Name
10	00-C0-F2-49-38-FF	Bi-directional	SISPM1040-582-LRT

Figure 4-21: Detailed UDLD Status for Port 6

UDLD Status

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

Device ID(local) : The ID of Device.

Device Name(local) : Name of the Device (*SISPM1040-582-LRT*).

Bidirectional State : The current state of the port (e.g., *Indeterminant*).

Neighbour 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 (e.g., Bi-directional).

Device Name : The name of the Neighbor Device.

Buttons

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

Refresh: Click to refresh the page immediately.

5. Diagnostics

This chapter describes system diagnostics, including Ping, Ping 6, Cable Diagnostics, Traceroute, and Link OAM.

5-1 Ping

This page lets you issue ICMP PING packets to troubleshoot IPv4 connectivity issues. To configure an ICMP Ping in the web UI:

1. Click Diagnostics, Ping.
2. Specify Ping IP Address.
3. Specify Ping Length, Count, and Interval.
4. Click the Start button.

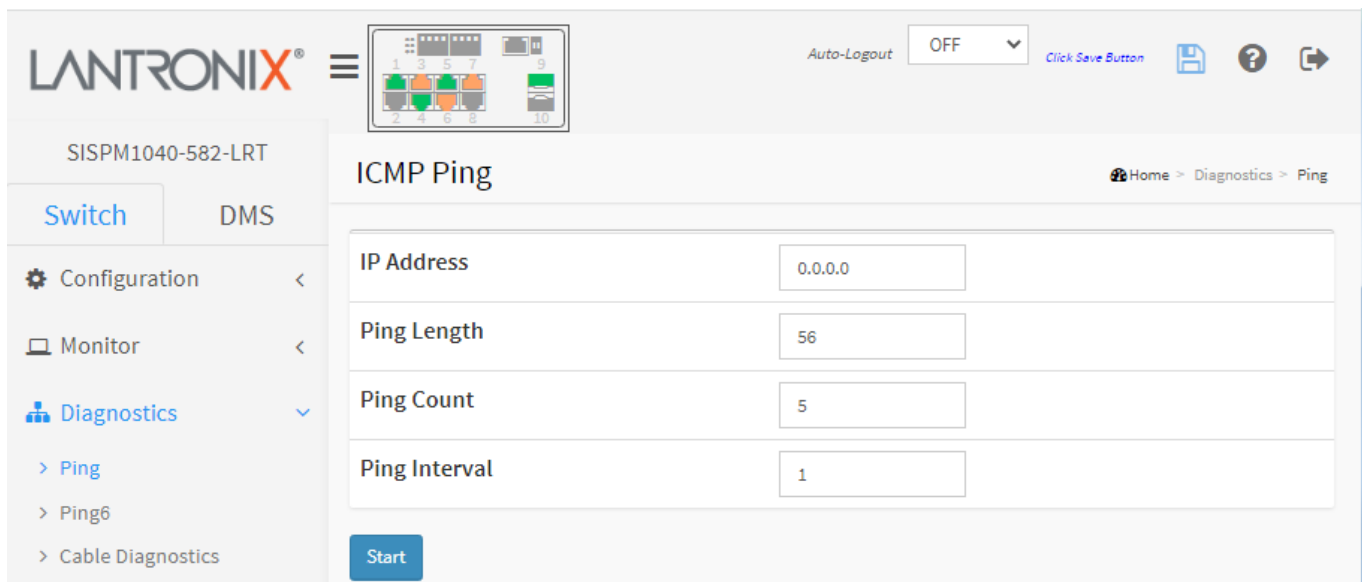


Figure 5-1: ICMP Ping

Parameter descriptions:

IP Address : To set the IP Address of device what you want to ping it.

Ping Length: The payload size of the ICMP packet. Values range from 2 bytes to 1452 bytes.

Ping Count: The count of the ICMP packet. Values range from 1 time to 60 times.

Ping Interval: The interval of the ICMP packet. Values range from 0 second to 30 seconds.

Buttons:

Start: Click the Start button then the switch will start to ping the device using ICMP packet size what set on the switch.

New Ping: After a Ping result is displayed on the ICMP Ping Output page, click this button to return to the ICMP PING page.

After you click **Start**, 5 ICMP packets are transmitted, and the sequence number and roundtrip time are displayed upon reception of a reply. The page refreshes automatically until responses to all packets are received, or until a timeout occurs.

```
PING6 server ::10.10.132.20
64 bytes from ::10.10.132.20: icmp_seq=0, time=0ms
64 bytes from ::10.10.132.20: icmp_seq=1, time=0ms
64 bytes from ::10.10.132.20: icmp_seq=2, time=0ms
64 bytes from ::10.10.132.20: icmp_seq=3, time=0ms
64 bytes from ::10.10.132.20: icmp_seq=4, time=0ms
Sent 5 packets, received 5 OK, 0 bad
```

5-2 Ping6

This page lets you issue ICMPv6 PING packets to troubleshoot IPv6 connectivity issues. To configure an ICMPv6 Ping in the web UI:

1. Click Diagnostics, Ping6.
2. Specify ICMPv6 Ping IP Address.
3. Specify ICMPv6 Ping Length, Count, and Interval.
4. Specify an Egress Interface.
5. Click the Start button.

The screenshot displays the Lantronix web interface for configuring an ICMPv6 Ping. The page title is "ICMPv6 Ping" and the breadcrumb is "Home > Diagnostics > Ping6". The configuration fields are:

IP Address	0:0:0:0:0:0:0:0
Ping Length	56
Ping Count	5
Ping Interval	1
Egress Interface	

A "Start" button is located at the bottom left of the configuration area. The left sidebar shows "Diagnostics" expanded to "Ping6".

Figure 5-2: ICMPv6 Ping

Parameter descriptions:

IP Address : The destination IP Address with IPv6

Ping Length : The payload size of the ICMP packet. Values range from 2 bytes to 1452 bytes.

Ping Count : The count of the ICMP packet. Values range from 1 time to 60 times.

Ping Interval : The interval of the ICMP packet. Values range from 0 to 30 seconds.

Egress Interface (Only for IPv6) : The VLAN ID (VID) of the specific egress IPv6 interface which ICMP packet goes.

The given VID ranges from 1 to 4094 and will be effective only when the corresponding IPv6 interface is valid.

When the egress interface is not given, PING6 finds the best match interface for destination.

Do not specify egress interface for loopback address.

Do specify egress interface for link-local or multicast address.

Buttons:

Start: Click the button for the switch to start pinging the device using ICMPv6 packet size set on the switch. After you press **Start**, 5 ICMPv6 packets are transmitted, and the sequence number and roundtrip time are displayed upon reception of a reply. The page refreshes automatically until responses to all packets are received, or until a timeout occurs.

```
PING server 10.10.132.20
64 bytes from 10.10.132.20: icmp_seq=0, time=0ms
64 bytes from 10.10.132.20: icmp_seq=1, time=0ms
64 bytes from 10.10.132.20: icmp_seq=2, time=0ms
64 bytes from 10.10.132.20: icmp_seq=3, time=0ms
64 bytes from 10.10.132.20: icmp_seq=4, time=0ms
Sent 5 packets, received 5 OK, 0 bad
```

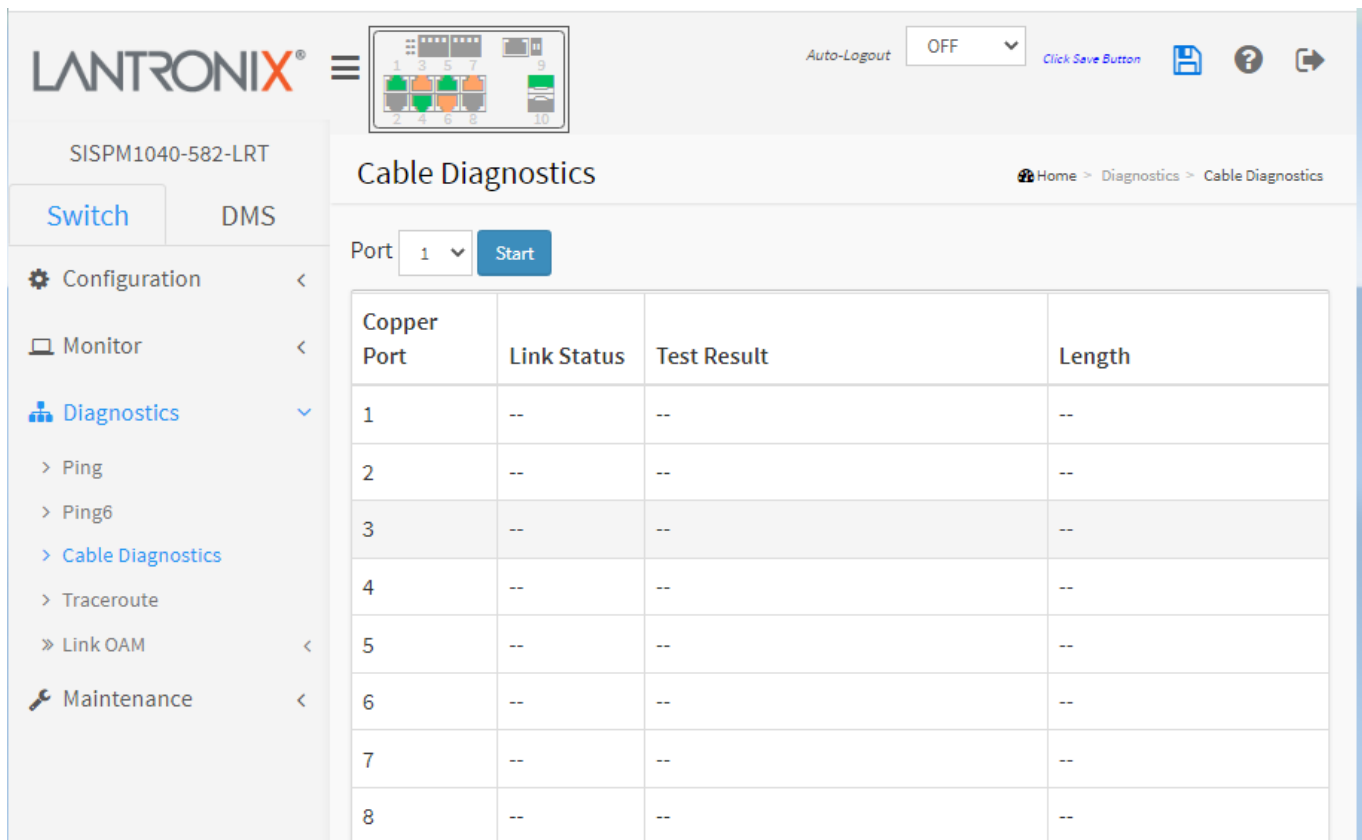
New Ping: After a Ping result is displayed on the ICMP Ping Output page, click this button to return to the ICMP PING page.

5-3 Cable Diagnostics

This page is used for running the Cable Diagnostics for 10/100 and 1G copper ports. **Note** that 10 Mbps and 100 Mbps ports will be linked down and lose connection while running Cable Diagnostics. **Note** that Diagnostics is only accurate for cables of length 7 – 120 meters.

To run a Cable Diagnostic in the web UI:

1. Click Diagnostics, Cable Diagnostics.
2. At the port select dropdown specify the Port to check.
3. Click the Start button.
4. At the confirmation message (*Are you sure... ?*) click the OK button.



The screenshot shows the Lantronix web interface for the device SISPM1040-582-LRT. The 'Cable Diagnostics' page is active, with a breadcrumb trail: Home > Diagnostics > Cable Diagnostics. A dropdown menu for 'Port' is set to '1', and a blue 'Start' button is visible. Below this is a table with the following data:

Copper Port	Link Status	Test Result	Length
1	--	--	--
2	--	--	--
3	--	--	--
4	--	--	--
5	--	--	--
6	--	--	--
7	--	--	--
8	--	--	--

Figure 5-3: Cable Diagnostics

Parameter descriptions:

Port : The port where you are requesting Cable Diagnostics.

Copper Port : Copper port number.

Link Status : The status of the cable.

10M: Cable is link up and correct. Speed is 10Mbps

100M: Cable is link up and correct. Speed is 100Mbps

1G : Cable is link up and correct. Speed is 1Gbps

Link Down: Link down or cable is not correct.

Test Result : Test Result of the cable diagnostic.

OK: Correctly terminated pair

Abnormal: Incorrectly terminated pair or link down

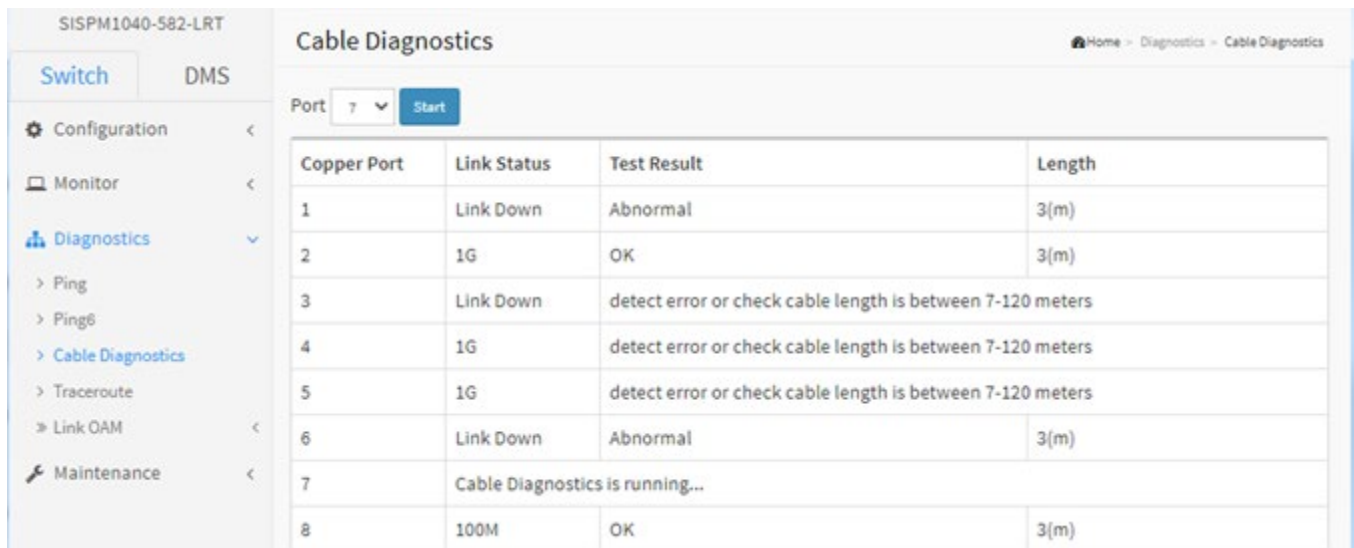
Length : The length (in meters) of the cable pair. The resolution is 3 meters. When Link Status is shown as follows, the length has a different definition.

1G: The length is the minimum value of 4-pair.

10M/100M: The length is the minimum value of 2-pair.

Link Down: The length is the minimum value of non-zero of 4-pair.

Cable Diagnostics Example:



The screenshot shows the 'Cable Diagnostics' page in a web browser. The page title is 'Cable Diagnostics' and the breadcrumb is 'Home > Diagnostics > Cable Diagnostics'. There is a 'Port' dropdown menu set to '7' and a 'Start' button. Below this is a table with the following data:

Copper Port	Link Status	Test Result	Length
1	Link Down	Abnormal	3(m)
2	1G	OK	3(m)
3	Link Down	detect error or check cable length is between 7-120 meters	
4	1G	detect error or check cable length is between 7-120 meters	
5	1G	detect error or check cable length is between 7-120 meters	
6	Link Down	Abnormal	3(m)
7	Cable Diagnostics is running...		
8	100M	OK	3(m)

Messages: 10 and 100 Mbps ports will be linked down and lost connection while running Cable Diagnostics. Are you sure you want to continue? Note that Diagnostics is only accurate for cables of length 7 – 120 meters.

5-4 Traceroute

This page lets you issue ICMP, TCP, or UDP packets to diagnose network connectivity issues. To configure a traceroute via the Web UI:

1. Click Diagnostics, Traceroute.
2. Specify the traceroute Protocol and IP Address.
3. Specify the traceroute Wait Time, Max TTL, and Probe Count.
4. Click Start.

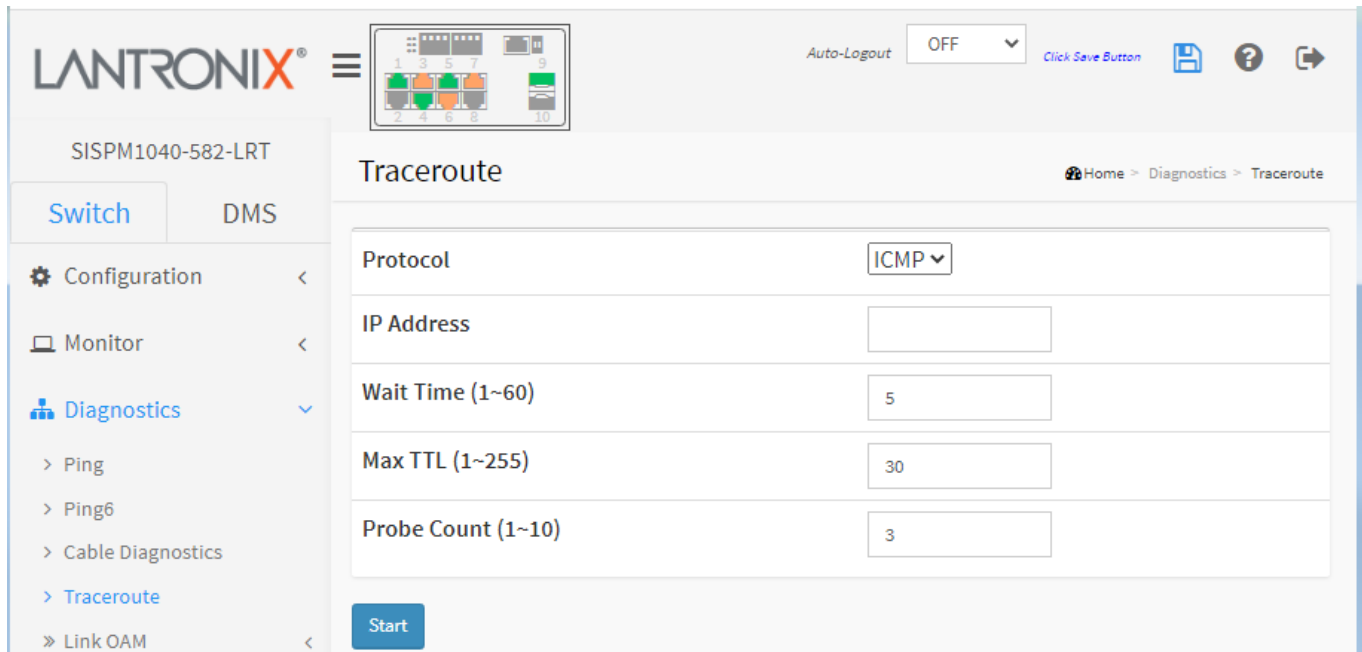


Figure 5.4-4: Traceroute

Parameter descriptions:

Protocol : The traceroute protocol (ICMP, UDP, or TCP) to use to send packets.

IP Address : The destination IP Address.

Wait Time : Set the time (in seconds) to wait for a response to a probe (default 5.0 seconds). Valid values are 1 – 60 seconds.

Max TTL : The maximum number of hops (max time-to-live value) traceroute will probe. Valid values are 1 – 255 hops. The default is 30 hops.

Probe Count : Sets the number of probe packets per hop. Valid values are 1 – 10. The default is 3 packets per hop.

Buttons :

Start : Click to start the Traceroute process.

New Traceroute : Click to re-start with a new Traceroute process.

After you press **Start**, Traceroute sends packets with gradually increasing TTL value, starting with TTL value of 1. The first router receives the packet, decrements the TTL value and drops the packet because it then has TTL value zero. The router sends an ICMP Time Exceeded message back to the source. The next set of packets are given a TTL value of 2, so the first router forwards the packets, but the second router drops them and replies with ICMP Time Exceeded. Proceeding in this way, traceroute uses the returned ICMP Time Exceeded messages to build a list of routers that packets traverse, until the destination is reached and returns an ICMP Echo Reply message.

```
traceroute to 202.39.253.11 (202.39.253.11), 30 hops max, 40 byte packets
1 192.168.10.254 ae-2-3508.edge4.Atlanta2.Level3.net. (192.168.10.254) 10 ms 10 ms 10 ms
2 59-125-13-254.HINET-IP.hinet.net. (59.125.13.254) 20 ms 20 ms 20 ms
3 h146.s228.ts.hinet.net. (168.95.228.146) 20 ms 10 ms 20 ms
4 tchn-3011.hinet.net. (220.128.16.194) 20 ms TCHN-3112.hinet.net. (220.128.17.142) 20 ms tchn-3011.hinet.net. (220.128.16.202) 20 ms
5 TPDT-3012.hinet.net. (220.128.17.6) 20 ms TPDT-3011.hinet.net. (220.128.16.10) 20 ms TPDT-3012.hinet.net. (220.128.17.6) 40 ms
6 CHCH-3112.hinet.net. (220.128.2.13) 20 ms tchn-3011.hinet.net. (220.128.1.9) 10 ms CHCH-3112.hinet.net. (220.128.2.13) 30 ms
7 211.22.41.237 CHCH-3112.hinet.net. (211.22.41.237) 20 ms 30 ms 30 ms
8 202-39-253-11.HINET-IP.hinet.net. (202.39.253.11) 10 ms 10 ms
```

Sample Traceroute Output:

SISPM1040-582-LRT

Switch DMS

Configuration <

Monitor <

Diagnostics >

> Ping

> Ping6

> Cable Diagnostics

> Traceroute

Traceroute Output

Home > Diagnostics > Traceroute

traceroute to 102.168.1.77 (102.168.1.77), 30 hops max, 140 byte packets

1***

2***

3***

4***

5*

New Traceroute

Messages:

Traceroute Output
traceroute: unknown host

Traceroute Output
traceroute to 102.168.1.77 (102.168.1.77), 30 hops max, 40 byte packets

Traceroute Output
traceroute to 102.168.1.77 (102.168.1.77), 30 hops max, 140 byte packets

5-5 Link OAM

5-5.1 MIB Retrieval

This page lets you retrieve the local or remote OAM MIB variable data on a particular port. To retrieve the Link OAM MIB information in the web UI:

1. Click Diagnostics, Link OAM, MIB Retrieval.
2. Select the Local or Peer radio button.
3. Enter the port number of the switch to retrieve the content of interest.
4. Click Start to retrieve the content.
5. View the displayed information.

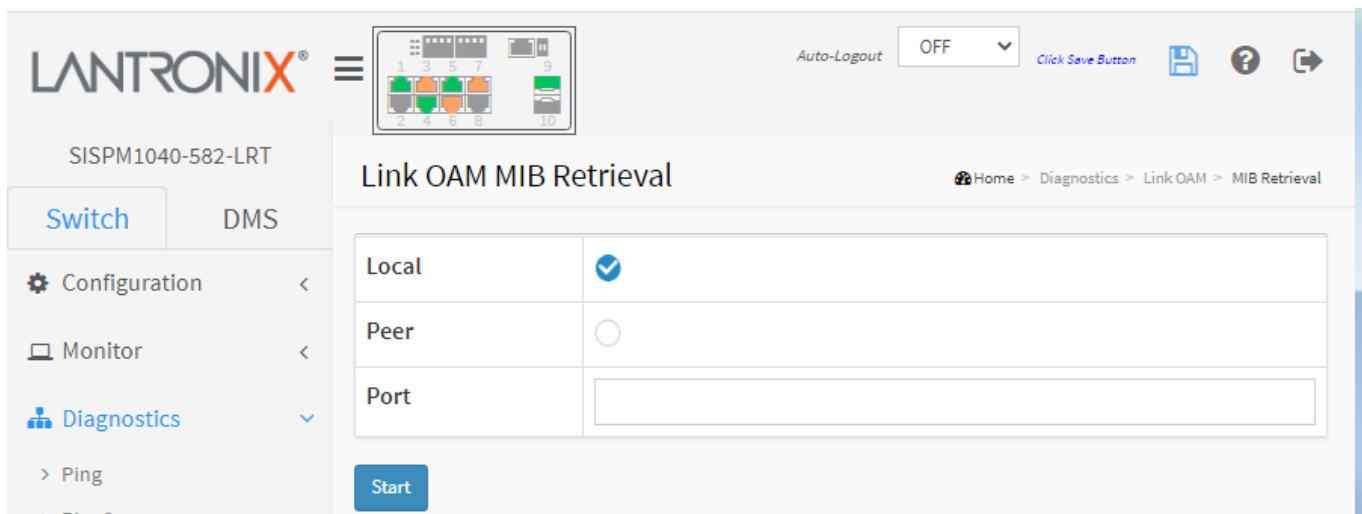


Figure 5-5.1: Link OAM MIB Retrieval

Buttons:

Start : Click to retrieve the content.

New Retrieval : Click to retrieve another content of interest.

Previous : Click to go back to the previous page.

Message: *OAM Error - Invalid request on this port*

Recovery: Click the **Previous** button and re-enter parameters.

6. Maintenance

This chapter describes the switch Maintenance configuration tasks including Restart Device, Reboot Schedule, Factory Defaults, Firmware upgrade and selection, Configuration tasks (Save/Restore, Import/Export) and Server Report.

6-1 Restart Device

This page lets you restart the switch for any maintenance needs. After restart, the switch will boot normally. Any configuration files or scripts that you saved in the switch should still be available afterwards.

To Restart the switch via the web UI:

1. Click Maintenance, Restart Device.
2. Check or uncheck the Always On PoE checkbox.
3. At the “Are you sure ...?” prompt, click Yes. After the switch restarts, the login page displays.

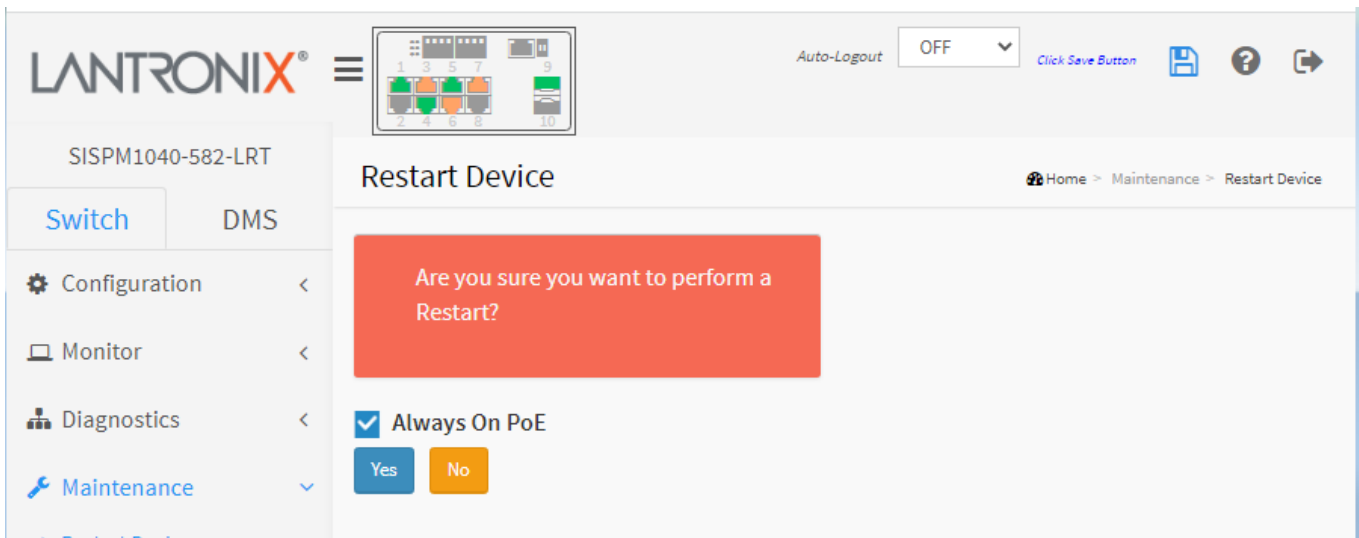


Figure 6-1: Restart Device

Parameter descriptions:

Always On PoE: If you check this box, when the switch does a warm restart, it will continue supplying PoE power to the PDs. Note: Changed from “Non-Stop PoE” to “Always On PoE” at FW VB7.10.2658. The default value is off.

Buttons:

Yes : Click to restart the switch.

No : Click to undo any restart action and return to the Monitor > System > Information page without restarting the switch.

6-2 Reboot Schedule

This page allows user to schedule the time to reboot the switch. To configure a Reboot Schedule in the web UI:

1. Click Maintenance, Reboot Schedule.
2. At the Mode dropdown, select Enabled to display the schedule data.
3. Set the reboot schedule parameters.
3. Click Apply.

The screenshot shows the 'Switch Reboot Schedule' configuration page. The 'Mode' is set to 'Enabled'. The table below shows the configuration for each day of the week:

Week Day	Reboot Time	
	HH	MM
*	<> ▾	<> ▾
Monday	- ▾	- ▾
Tuesday	- ▾	- ▾
Wednesday	- ▾	- ▾
Thursday	- ▾	- ▾
Friday	- ▾	- ▾
Saturday	- ▾	- ▾
Sunday	- ▾	- ▾

Buttons: Apply (blue), Reset (orange)

Figure 6-2: Reboot Schedule

Mode : Indicates the reboot scheduling mode of operation. Possible modes are:

Enabled: Enable switch reboot scheduling.

Disabled: Disable switch reboot scheduling.

Week Day : The day to reboot this switch.

Reboot Time : The time to reboot the switch in hours (0-23 HH) and minutes (0-55 MM).

Buttons:

Apply : Click to save changes.

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

6-3 Factory Defaults

This page lets you reset the Switch configuration to Factory Defaults. Any configuration files or scripts will return to factory default values. The new configuration is available immediately, which means that no restart is needed.

To reset the switch to Factory Defaults via the web UI:

1. Click Maintenance, Factory Defaults.
2. Check or uncheck “Keep IP setup”.
2. At the “Are you sure ...” prompt click Yes.

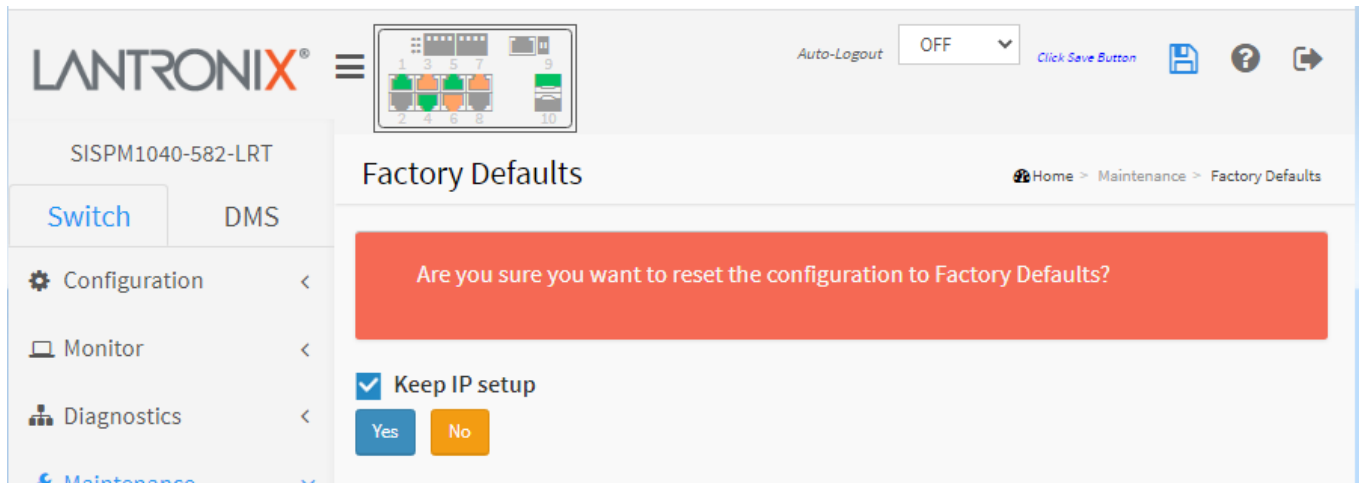


Figure 6-3: Factory Defaults

Parameter descriptions:

Keep IP setup : Check if you want to keep the current IP setting after the reset to factory defaults.

Buttons:

Yes : Click the button to reset the configuration to Factory Defaults.

No : Click to return to the Port State page without resetting the configuration.

Messages:

Are you sure you want to reset the configuration to Factory Defaults?

Configuration Factory Reset Done

The configuration has been reset. The new configuration is available immediately.

6-4 Firmware

This section lets you upgrade switch firmware or perform a firmware swap.

6-4.1 Firmware Upgrade

This page facilitates an update of the firmware controlling the switch. The switch can be enhanced with more value-added functions by installing firmware upgrades.

To perform a Firmware Upgrade via the web UI:

1. Click Maintenance, Firmware, Firmware Upgrade to display the Software Upload page.
2. Click the Choose File button to browse to and select a firmware file.
3. Check or un-check the “Always On PoE” checkbox.
4. Click Upload.

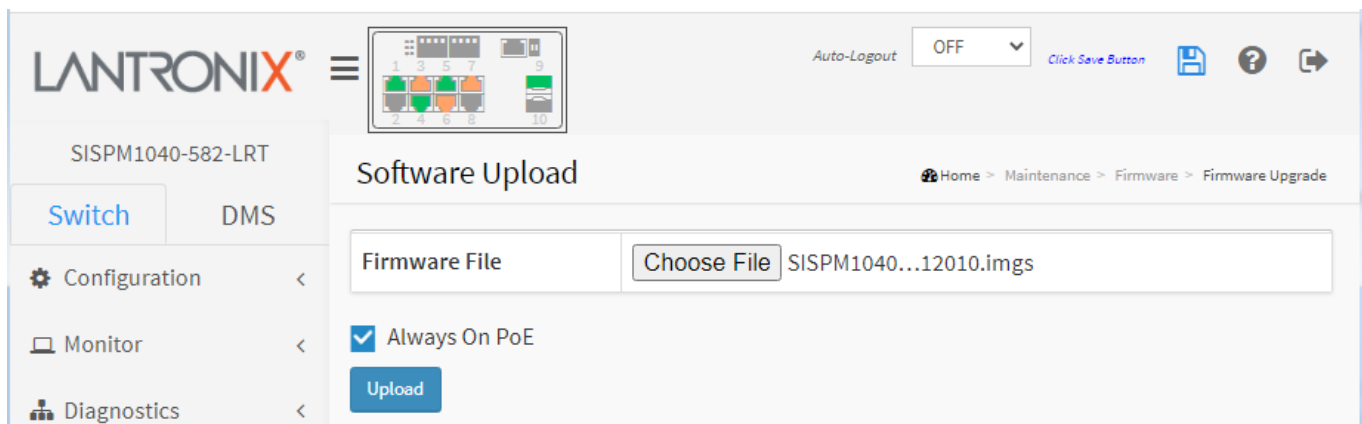


Figure 6-4.1 Software Upload

Parameter description:

Choose File : Click the button to search for and select the desired firmware filename (e.g., *SISPM1040-582-LRT_VB7.20.0191_CM_202308003.imgs*).

Note: This page facilitates an update of the firmware controlling the switch. Uploading software will update all managed switches to the location of a software image and click. 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 panel 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.

Always On PoE: If you check this box, when the switch does a warm restart, it will continue supplying PoE power to the PDs. Changed from “Non-Stop PoE” to “Always On PoE” at FW VB7.10.2658.

6-4.2 Firmware Selection

This page provides 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:

1. If the active firmware image is the same as the alternate image, only the "Active Image" table is shown. In this case the Activate Alternate Image button is disabled.
2. 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 and activate the primary image.
3. The firmware version and date information may be empty for older firmware releases. This does not constitute an error.

To perform a Firmware swap via the web UI:

1. Click Maintenance, Firmware, Firmware Selection.
2. Check or uncheck the Always On PoE checkbox.
3. Click the Activate Alternate Image button.
4. At the confirmation prompt (*Are you sure ...*) click OK. The system will restart after the update.

The screenshot shows the Lantronix web interface for the SISPM1040-582-LRT device. The main navigation menu on the left includes Configuration, Monitor, Diagnostics, and Maintenance. The Maintenance menu is expanded, showing options like Restart Device, Reboot Schedule, Factory Defaults, Firmware, and Firmware Selection. The Firmware Selection page is active, displaying the following information:

Active Image	
Image	managed
Version	SISPM1040-582-LRT (standalone) VB7.20.0191
Date	2023-10-16T18:36:32+08:00

Alternate Image	
Image	managed.bk
Version	SISPM1040-582-LRT (standalone) VB7.20.0170
Date	2023-04-06T16:45:37+08:00

Below the tables, there is an unchecked checkbox for "Always On PoE" and two buttons: "Activate Alternate Image" (blue) and "Cancel" (red).

Figure 6-4.2: Firmware Selection

Parameter descriptions:

Image : The flash index name of the firmware image. The name of primary (preferred) image is *managed*, the alternate image is named *managed.bk*.

Version : The version of the firmware image (e.g., *SISPM1040-582-LRT (standalone) VB7.20.0191*).

Date : The date and time when the firmware was produced (e.g., *2023-10-16T18:36:32+08:00*).

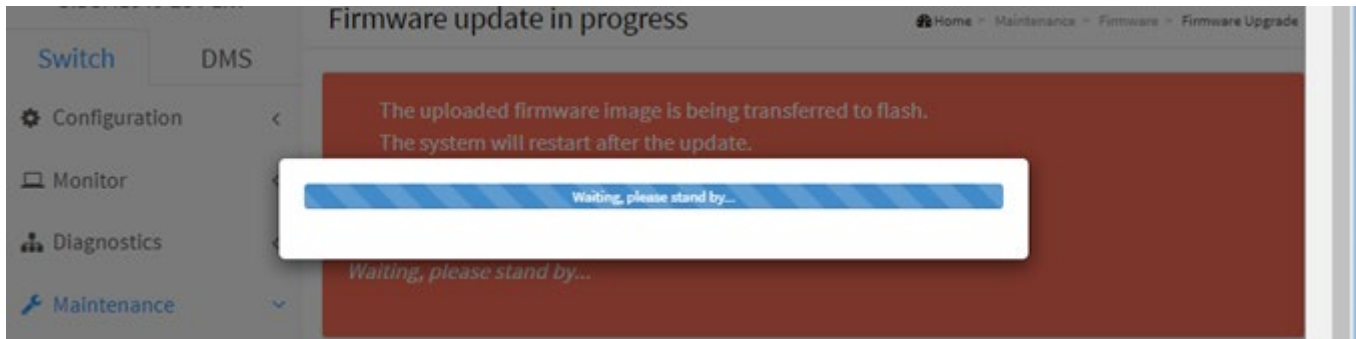
Always On PoE: If you check this box, when the switch does a warm restart, it will continue supplying PoE power to the PDs. Note: Changed from “Non-Stop PoE” to “Always On PoE” at FW VB7.10.2658. The default value is off.

Buttons

Activate Alternate Image: Click to use the “Alternate Image”. This button may be disabled depending on system state. The message “Are you sure you want to activate the alternate software image?” displays; click OK to continue.

Cancel: Click to cancel activating the backup image. Navigates away from this page to the Monitor > System > Information page.

The upgrade process displays momentarily as shown below:



6-5 Configuration

The switch stores its configuration in a number of text files in CLI format. The files are either virtual (RAM-based) or stored in flash on the switch. The system files include:

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

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

default-config: A read-only file with vendor-specific configuration. This file is read when the system is restored to default settings.

It is also possible to store up to two other files and apply them to running-config, thereby switching configuration.

6-5.1 Save startup-config

This copies the running-config to startup-config, ensuring that the currently active configuration will be used at the next reboot. Please note: The generation of the configuration file may be time consuming, depending on the amount of non-default configuration.

To save the running configuration in the web UI:

1. Click Maintenance, Configuration, Save startup-config.
2. Click the Save Configuration button.

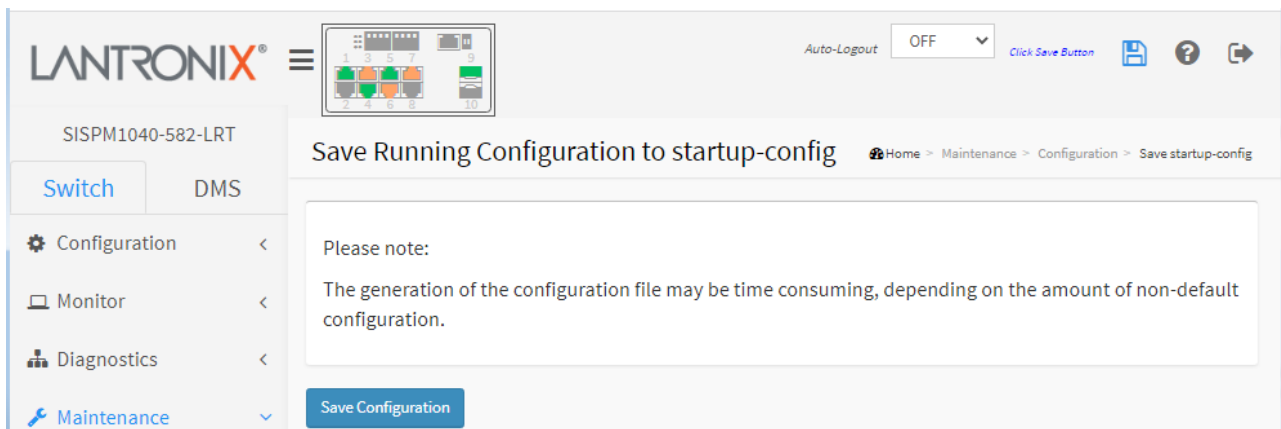


Figure 6-5.1: Save Running Configuration to startup-config

Parameter descriptions:

Buttons :

Save Configuration: Click to save the running configuration; the running configuration will be written to flash memory for system boot up to load this startup configuration file. **Note:** During Save Running configuration, do not reset or power off the switch!

Message: *startup-config saved successfully.*

Message: *Cannot commit changes to flash.*

6-5.2 Download

The switch stores its configuration in a number of text files in CLI format. The files are either virtual (RAM-based) or stored in flash on the switch. This page lets you download any of the files on the switch to the web browser.

Up to 99 other files, typically used for configuration backups or alternative configurations, can be saved.

To download a configuration file in the web UI:

1. Click Maintenance, Configuration, Download.
2. Select a firmware file.
3. Click the Download Configuration button.

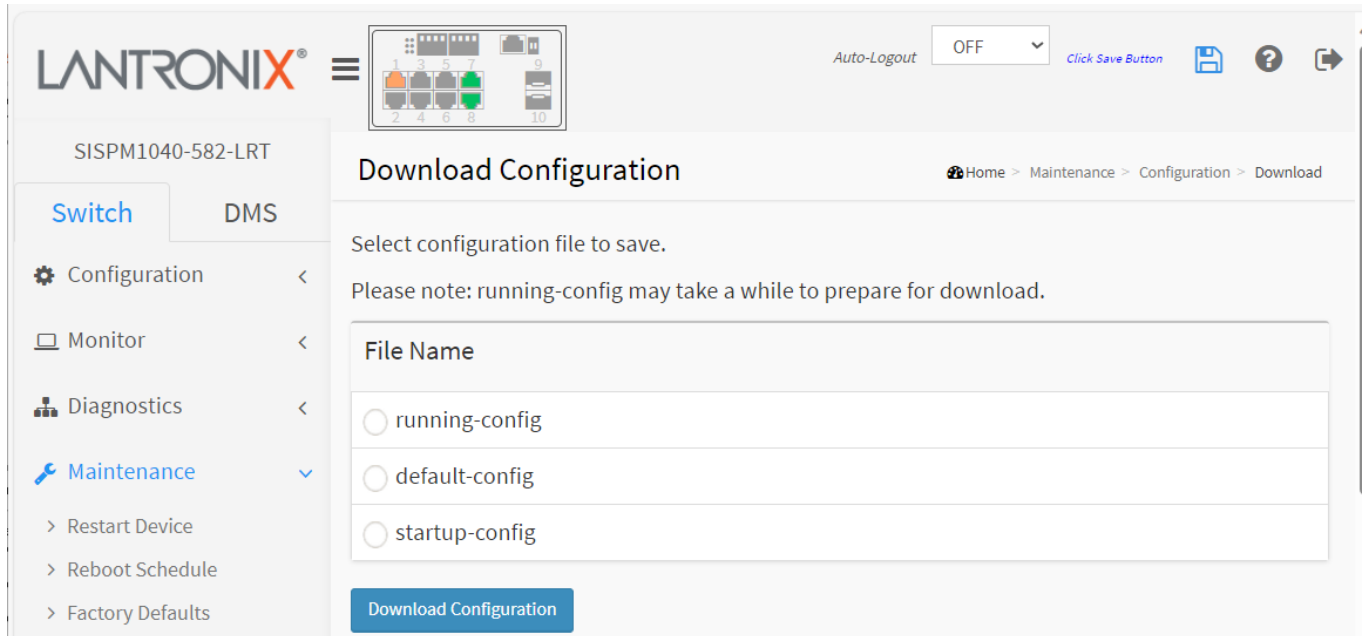


Figure 6-5.2: Download Configuration

Parameter descriptions:

running-config: A virtual file that represents the currently active configuration on the switch. This file is volatile. Download of running-config may take a little while to complete, as the file must be prepared for download.

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.

Buttons:

Download Configuration : Click to download the selected config file. The file will be named in the format *startup-config_192.168.1.77_20110103*. Check your Downloads folder to locate the files. Browser-based downloads are often placed in the downloads folder on your device in Windows. The path to the file may resemble *C:\Users\[Your User ID]\Downloads* where *C:/* indicates your device's storage drive.

Sample Default configuration file:

```
1 ..... 2 ..... 3 ..... 4 ..... 5 ..... 6 ..... 7 .....
|: Default configuration file
| -----
|
| ! This file is read and applied immediately after the system configuration is
| ! reset to default. The file is read-only and cannot be modified.
|
vlan 1
  name default

ip route 0.0.0.0 0.0.0.0 192.168.1.254
ip name-server 8.8.8.8

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

interface vlan 1
  ip address 192.168.1.1 255.255.255.0

end
```

6-5.3 Upload

The configuration upload function will upload a backed up and saved config file from the switch into the running web browser on the PC. It is possible to upload a file from the web browser to all the files on the switch, except default-config which is read-only.

Select the file and click Upload Configuration. An upload of running-config may take a while to complete, as the file must be prepared for upload. If the flash file system is full (i.e., contains *default-config* and 100 other files, usually including *startup-config*), it is not possible to create new files. Instead, an existing file must be overwritten, or another file must be deleted.

To upload a config file via the web UI:

1. Click Maintenance, Configuration, Upload.
2. Click Choose File to browse to and select a file to upload.
3. Select the name of the file to be uploaded.
4. Click the Upload Configuration button.

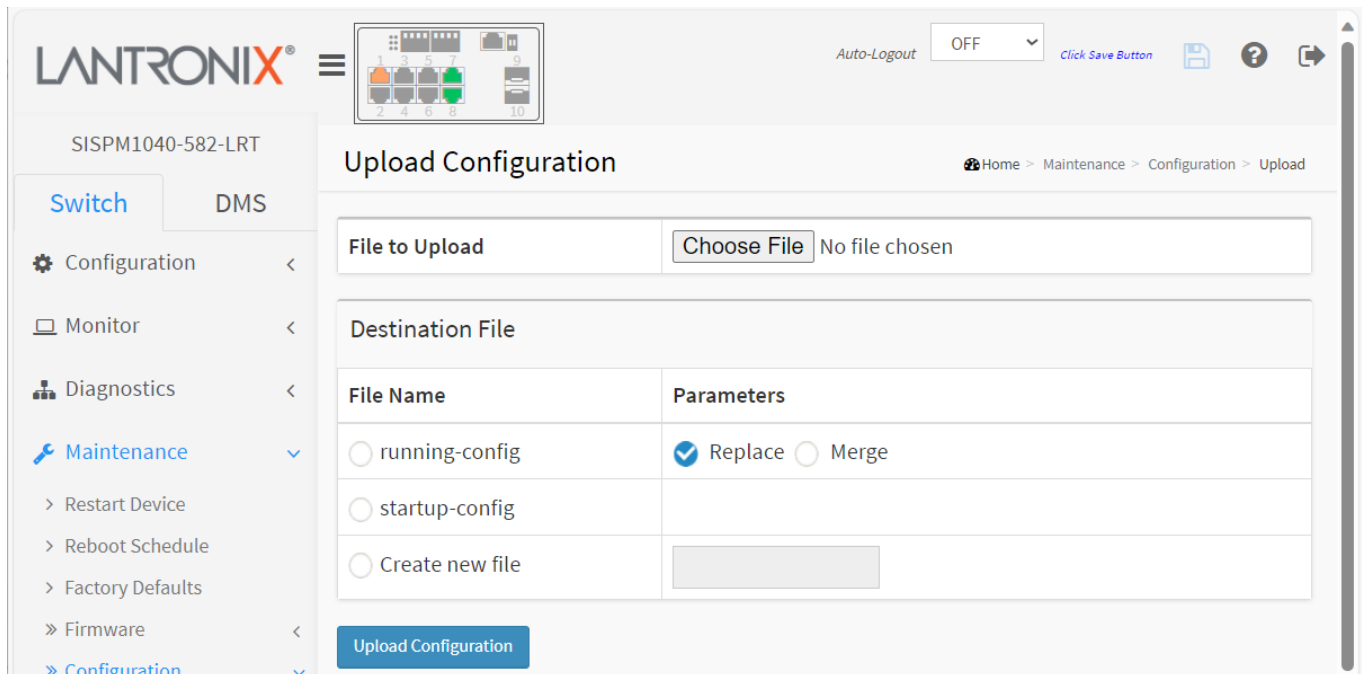


Figure 6-5.3: Upload Configuration

File to Upload: Click the **Choose File** button and browse to and select the file you want to be uploaded.

Destination File:

File Name: Select the name of the file to be uploaded:

running-config: A virtual file that represents the currently active configuration on the switch. This file is volatile. If the destination is running-config, the file will be applied to the switch configuration. This can be done in one of two ways:

Replace: The current configuration is fully replaced with the configuration in the uploaded file.

Merge: The uploaded file is merged into running-config.

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

Create new file: Lets you enter a new file and upload it.

Buttons :

Upload Configuration: Click the button then the running web management PC will start to upload the configuration from the managed switch configuration into the PC download location; you can configure the upload file path to keep the config file.

Note: Check your Downloads folder to locate the files. Browser-based downloads are often placed in the downloads folder on your device in Windows. The path to the file may resemble *C:\Users\[Your User ID]\Downloads* where *C:/* indicates your device's storage drive.

6-5.4 Activate

It is possible to activate any of the configuration files present on the switch, except for running-config which represents the currently active configuration.

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

Caution: The previous configuration will be completely replaced, potentially leading to loss of management connectivity.

Note: The activated configuration file will NOT be saved to startup-config automatically.

To activate a config file via the web UI:

1. Click Maintenance, Configuration, Activate.
2. Select the file to activate.
3. Click the Activate Configuration button.

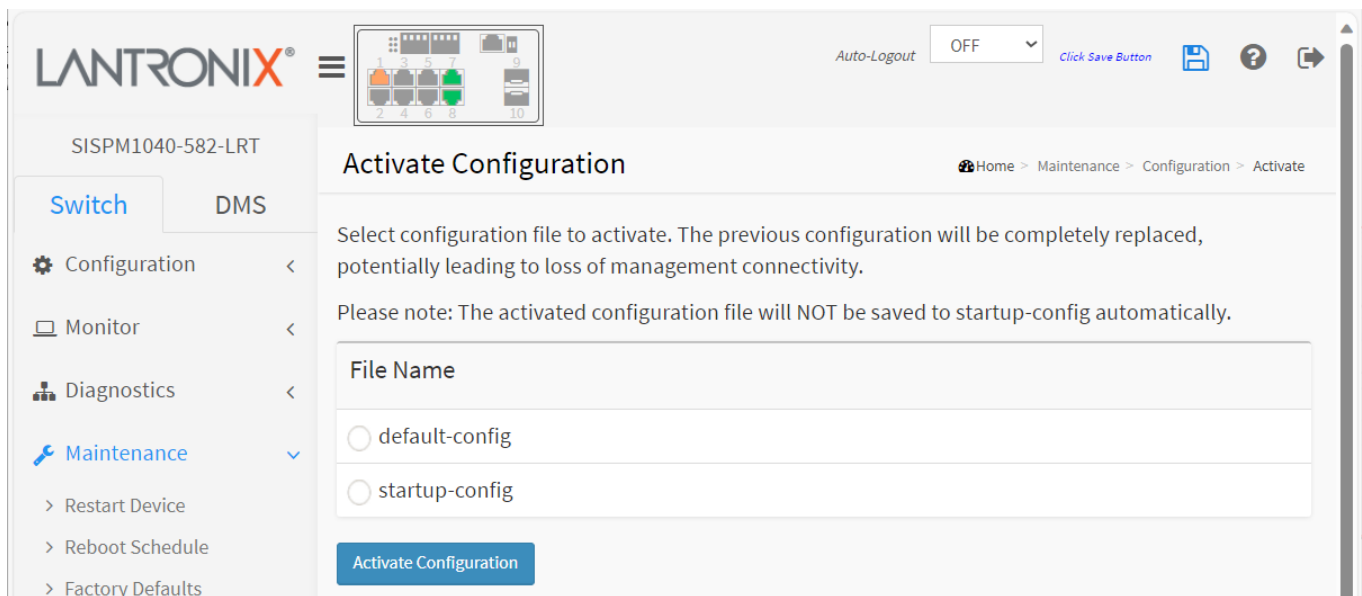


Figure 6-5.4: Configuration Activation

Parameter descriptions:

File Name:

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 :

Activate Configuration: Click the button then the default-config or startup-config file will be activated and will become this switch's running configuration. This will initiate the process of completely replacing the existing configuration with that of the selected file.

6-5.5 Delete

It is possible to delete any of the writable files stored in flash, including startup-config. If this is done and the switch is rebooted without a prior save operation, this effectively resets the switch to its default configuration.

To delete a config file from the web UI:

1. Click Maintenance, Configuration, Activate.
2. Select a File Name.
3. Click the Delete Configuration File button.
4. At the webpage message, click OK if you are sure you want to delete this file.

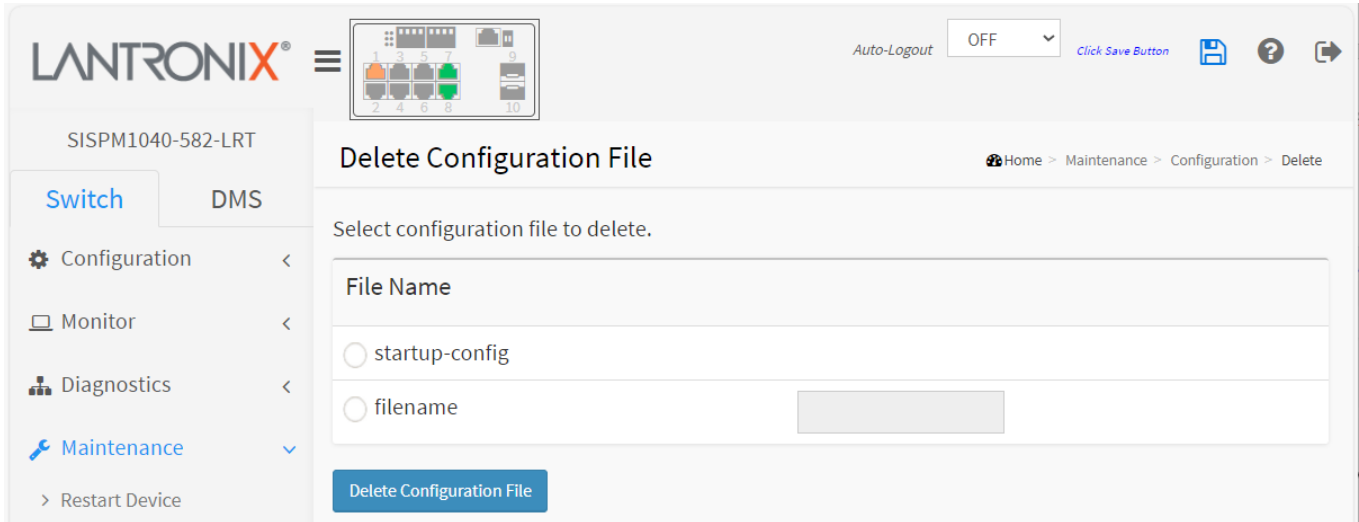


Figure 6-5.5: Delete Configuration File

File Name: Radio button to select a file to delete:

startup-config: Radio button to select the startup configuration for the switch, read at boot time.

filename : Radio button to enter a different file to be delete.

Buttons :

Delete Configuration File: Click the button then the startup-config file will be deleted, this effectively resets the switch to default configuration.

Messages:

Are you sure you want to delete startup-config_192.168.1?

Delete Configuration File

Another configuration I/O operation is in progress. Please try again in a moment.

Delete Configuration File

Successfully deleted.

6-6 Server Report

It is possible to download a server report file on the switch. Downloading the server report may take a little while to complete, as the file must be prepared for download.

To download a server report file in the web UI:

1. Click Maintenance, Configuration, Server Report.
2. Click the Server Report button.
3. At the webpage message, select whether to open or save this file.

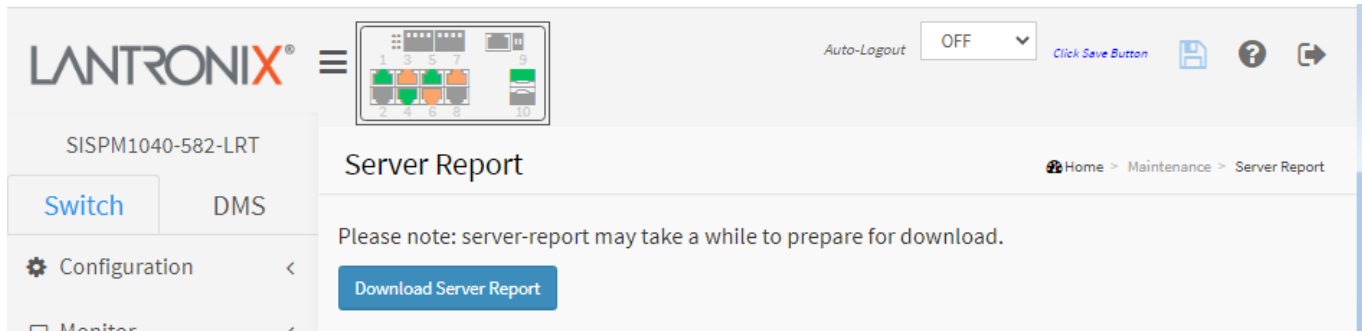


Figure 6-6: Server Report

Buttons :

Download Server Report: Click the button to download a server report file. See sample below.

Server Report Example:

```

server-report (1) - Notepad
File Edit Format View Help
----- System Overview -----
Model Name: SISPM1040-582-LRT
Connected Devices: 5
PoE Power Consumption: 9.2 [w]
Total PoE Available: 470.8 [w]
Firmware Version: vB7.20.0016 2020-10-20
MAC Address: 00-c0-f2-4f-7f-cd
System Uptime: 02:23:24
IP Address: 192.168.1.77
Subnet Mask: 255.255.255.0
Gateway: 192.168.1.254
primary DNS: 8.8.8.8
----- running-config -----
hostname SISPM1040-582-LRT!
vlan 1 !
ipmc profile prof1 description firstProfile in IPMC Profile Table!
ipmc profile ip route 0.0.0.0 0.0.0.0 192.168.1.254!
dxecc-timeout autologout 0no smp-server user
default_user engine-id 800007e5017f000001 system name SISPM1040-582-LRTsystem description Managed
Hardened PoE+ Switch (8) 10/100/1000Base-T PoE+ Ports + (2) 100/1000Base-X SFP Slot!
interface GigabitEthernet 1/1/!
interface GigabitEthernet 1/2/!
link-ooan link-ooan mode active!
interface GigabitEthernet 1/3/!
interface GigabitEthernet 1/4/!
interface GigabitEthernet 1/5/!
interface GigabitEthernet 1/6/!
interface GigabitEthernet 1/7/!
interface GigabitEthernet 1/8/!
interface GigabitEthernet 1/9/!
interface GigabitEthernet 1/10/!
interface Vlan 1 ip address 192.168.1.77
255.255.255.0!
spanning-tree aggregation spanning-tree link-type point-to-point!
line console 0!
line vty 0!
line vty 1!
line vty 5!
line vty 9!
line vty 13!
line vty 14!
line vty 15!
mp domain new 1mp 1 ringport
primary gigabitEthernet 1/1mp 1 ringport secondary gigabitEthernet 1/2mp 1 role management 1 status
enablemp domain new 2mp 2 ringport primary gigabitEthernet 1/2mp 2 ringport secondary gigabitEthernet
1/4mp 2 role clientmp 2 status enable!
end
----- System Log -----
2011-01-01T00:00:13:00:00 SISPM1040-582-LRT [ warning ] SFP module inserted on port 10 connector Type:
SFP or SFP Plus - LC Fiber Type : Reserved Tx wavelength : 850 baud Rate : 10 dbps vendor OUI
: 00-c0-f2 vendor Name : Transition vendor PN : TN-10GSP-SR vendor Rev : 0001 Vendor
SN : 102201101 date Code : 100527
2011-01-01T00:00:13:00:00 SISPM1040-582-LRT [ warning ] Switch just made a warm boot
2011-01-01T00:00:13:00:00 SISPM1040-582-LRT [ warning ] Link up on port 2
2011-01-01T00:00:13:00:00 SISPM1040-582-LRT [ warning ] DI 1 change to abnormal.
2011-01-01T00:00:14:00:00 SISPM1040-582-LRT [ info ] Password of user 'admin' was changed
2011-01-01T00:00:14:00:00 SISPM1040-582-LRT [ warning ] SFP module inserted on port 9 connector Type:
SFP or SFP Plus - LC Fiber Type : Multi-mode (OM) Tx wavelength : 850 baud Rate : 1000 Mbps
vendor OUI : 00-c0-f2 vendor Name : Transition vendor PN : TN-SFP-SXD vendor Rev
: 0000 Vendor SN : 8672105 date Code : 091027
2011-01-01T00:00:14:00:00 SISPM1040-582-LRT [ info ] topologyChange
2011-01-01T00:00:16:00:00 SISPM1040-582-LRT [ info ] topologyChange
2011-01-01T00:00:30:00:00 SISPM1040-582-LRT [ warning ] Port 1 PoE PD on
2011-01-01T00:00:30:00:00 SISPM1040-582-LRT [ warning ] Port 3 PoE PD on
2011-01-01T00:00:31:00:00 SISPM1040-582-LRT [ info ] topologyChange
2011-01-01T00:00:31:00:00 SISPM1040-582-LRT [ info ] Link up on port 10
2011-01-01T00:00:32:00:00 SISPM1040-582-LRT [ info ] topologyChange
2011-01-01T00:00:33:00:00 SISPM1040-582-LRT [ warning ] Port 4 PoE PD on
2011-01-01T00:00:33:00:00 SISPM1040-582-LRT [ warning ] Port 6 PoE PD on
2011-01-01T00:00:33:00:00 SISPM1040-582-LRT [ warning ] Port 7 PoE PD on
2011-01-01T00:00:33:00:00 SISPM1040-582-LRT [ warning ] Link up on port 1
2011-01-01T00:00:34:00:00 SISPM1040-582-LRT [ info ] topologyChange
2011-01-01T00:00:35:00:00 SISPM1040-582-LRT [ warning ] Link up on port 3
2011-01-01T00:00:35:00:00 SISPM1040-582-LRT [ warning ] DC power 2 unavailable
2011-01-01T00:00:35:00:00 SISPM1040-582-LRT [ info ] Link up on port 4
2011-01-01T00:00:35:00:00 SISPM1040-582-LRT [ info ] topologyChange
2011-01-01T00:00:35:00:00 SISPM1040-582-LRT [ info ] topologyChange
2011-01-01T00:00:36:00:00 SISPM1040-582-LRT [ info ] DMS: New Device(192.168.1.99) add in topology
2011-01-01T00:00:37:00:00 SISPM1040-582-LRT [ warning ] Link up on port 6
2011-01-01T00:00:37:00:00 SISPM1040-582-LRT [ info ] Link up on port 7
2011-01-01T00:00:37:00:00 SISPM1040-582-LRT [ info ] topologyChange
2011-01-01T00:00:39:00:00 SISPM1040-582-LRT [ info ] topologyChange
2011-01-01T00:00:39:00:00 SISPM1040-582-LRT [ info ] DMS: New Device(192.168.1.77) add in topology
2011-01-01T00:00:59:00:00 SISPM1040-582-LRT [ info ] Login passed for user 'admin' through WEB from
192.168.1.99-49830 and authenticated by local method
2011-01-01T00:00:58:00:00 SISPM1040-582-LRT [ info ] DMS: Device(SM16AT2SA) duplicate IP address
192.168.1.77
2011-01-01T00:00:58:00:00 SISPM1040-582-LRT [ info ] DMS: Device(SISPM1040-582-LRT) duplicate IP
address 192.168.1.77
2011-01-01T00:01:25:00:00 SISPM1040-582-LRT [ info ] DMS: New Device(192.168.1.100) add in topology
2011-01-01T00:01:26:00:00 SISPM1040-582-LRT [ info ] DMS: New Device(192.168.1.100) add in topology

```

Server Report parameter descriptions:

System Overview (Model Name, Connected Devices, PoE Power Consumption, Total PoE Available, Firmware Version, MAC Address, System Uptime, IP Address, Subnet Mask, Gateway, Primary DNS).

running-config (hostname, ip route, exec-timeout autologout, system name, system description, SFP Slot, etc.).

System log (e.g., Link up on port 10, Switch just made a warm boot).

System info (e.g., Model Name, System Description, Location, Contact, System Name, System Date, System Uptime, Bootloader Version, Firmware Version, Temperature status).

PoE config (Primary Power Supply [W], Port, Mode, Schedule, Priority, LLDP, Legacy support, etc.).

PoE status (Interface, PD Class, Port Status, Power Requested, Power Allocated, Power Used, PD Class, etc.).

Port status (Mode, Speed & Duplex, Flow Control, Max Frame, etc.).

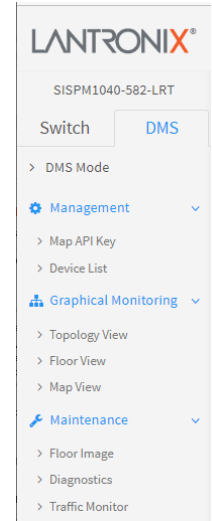
Port statistics (Rx Packets, Tx Packets, Rx Octets, Tx Octets, Rx Unicast, etc.).

7. DMS (Device Management System)

The DMS (Device Management System) is an intelligent management tool embedded in the switch to intuitively help IT/TS reduce support time, cost, and effort. In the left main menu pane, navigate to the DMS tab to display the main DMS features: DMS Mode, Management, Graphical Monitoring, and Maintenance.

DMS features include:

- DMS automatically discovers and displays all devices connected to the switch using standard networking protocols such as LLDP, UPnP, ONVIF, etc.
- DMS supports up to 256 devices within four subnets.
- DMS operates via an intuitive web GUI to allow you to:
 - Power down the IP cameras, NVRs, or any PoE devices.
 - Remotely identify the exact cable break location.
 - Detect abnormal traffic issues on IP cameras/NVR.
 - Monitor devices' status (e.g., link up, PoE power, traffic, etc.).
 - Configure VLAN/QoS intuitively for better solution quality/reliability.

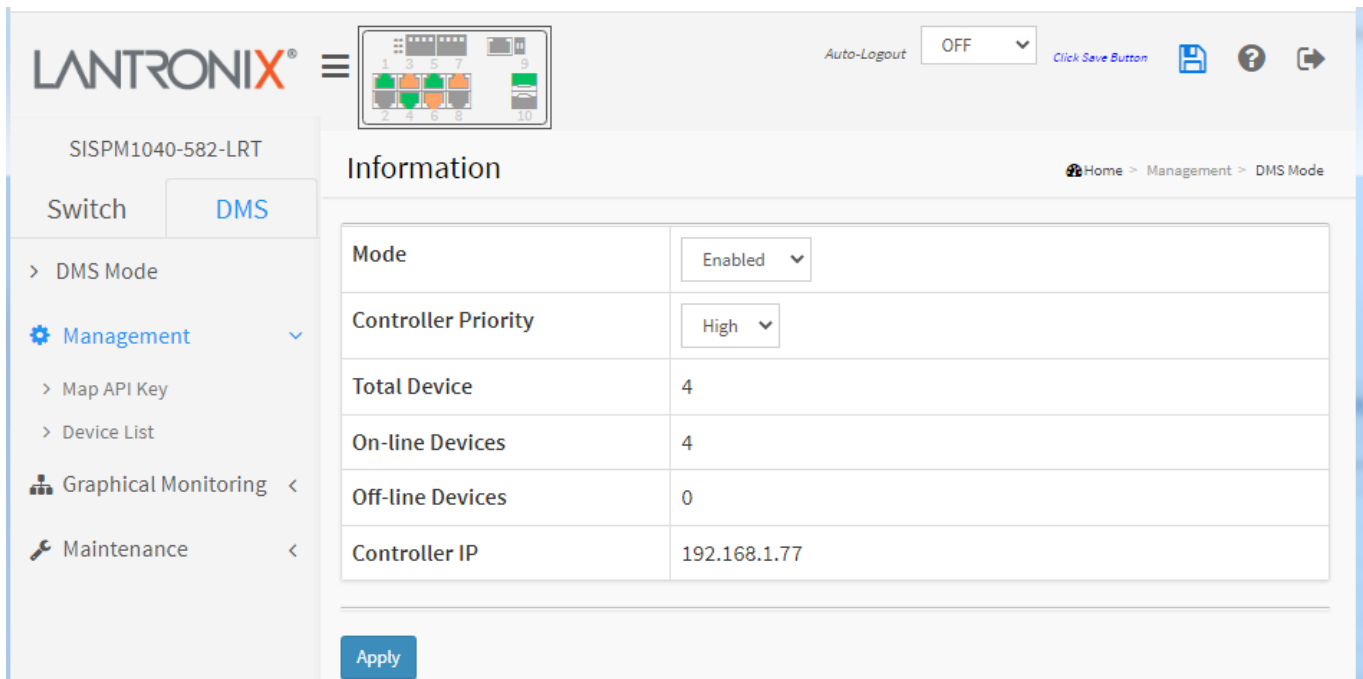


7.1 DMS > Management

At DMS > Management you can select MAP API Key and Device List.

7.1.1 DMS > DMS Mode

DMS > DMS Mode displays the DMS Information page as shown below.



Parameter Descriptions:

Mode: At the dropdown select **Enabled** or **Disabled**. The default is Enabled.

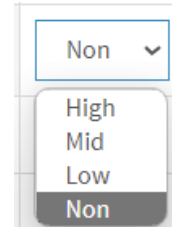
Controller Priority: Choose "Controller Priority" when enabling DMS. You can choose the priority to change the dominant status of the switch.

High: This switch with "High Priority" selected will become the DMS Controller Switch (master switch).

Mid: This switch will have mid-level priority.

Low: This switch will have low-level priority (default).

Non: This switch will never become the DMS Controller Switch (master switch).



Total Device: Displays the Total / On-line/ Off-line Devices count in the DMS network (read only).

On-line Devices: Displays the total number of discovered devices that are currently on line (e.g., 7).

Off-line Devices: Displays the total number of discovered devices that are currently off line (e.g., 1).

Controller IP: Displays the active DMS Controller Switch's IP Address (read only).

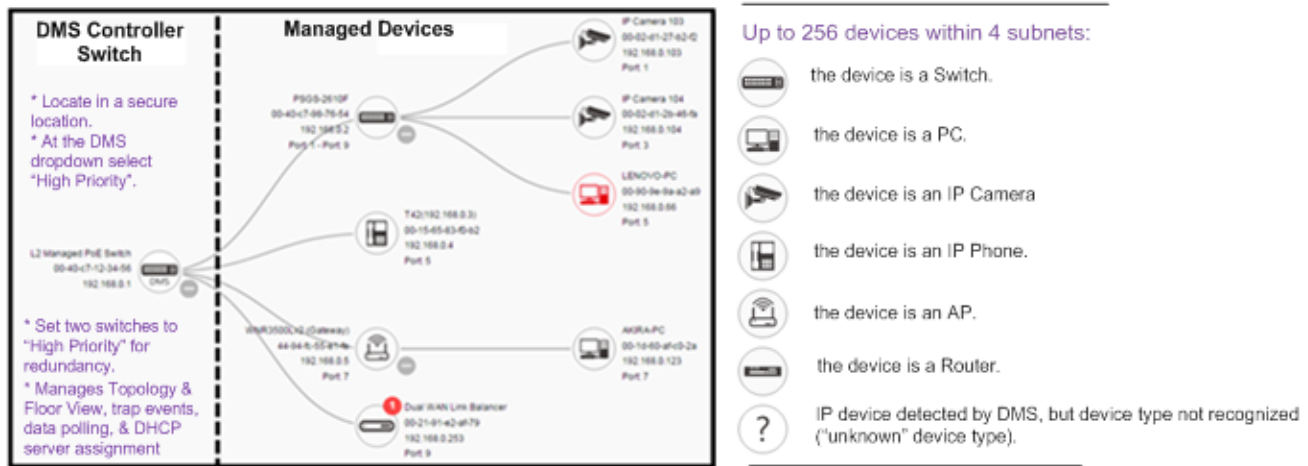
Buttons

Apply : Click to save changes.

7.1.2 DMS Mode – DMS Controller Switch

The Switch with “High Priority” selected will become the DMS Controller Switch (the master switch).

- Configure DMS mode and monitor device numbers/ DMS Controller Switch IP.
- DMS is controlled by the DMS Controller switch, as specified by DMS Mode selection.
- The DMS Controller Switch is in charge of syncing DMS information in order to manage Topology View, Floor View, and trap event / data polling / DHCP server assignment.



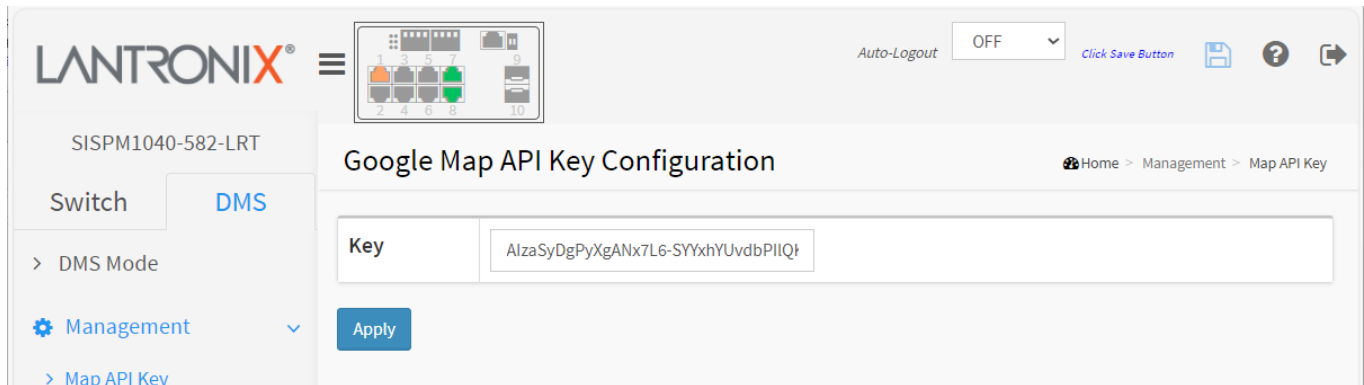
DMS Controller Switch and Managed Devices

Note:

1. If there are more than two Switches set as High-priority or no High-priority mode switch, the Switch with the longer system uptime will be selected as the DMS Controller switch. If two switches have same up time, the switch with the smaller MAC address will be assigned as the DMS Controller Switch.
2. You can set two switches to High Priority for Controller Switch redundancy.
3. The DMS Controller Switch should be put in a secure location such as a server room, with access/authority limited to IT staff.
4. The DMS Controller Switch is the center of IP / Event management to operate the DMS:
 - a. When enabled DHCP Server mode in DMS network, the DMS Controller switch is responsible for assigning IP address for all devices.
 - b. The DMS Controller Switch will Collect, Poll, and Sync DMS information, and act as the Event Notification control center to manage all device information.

7.1.3 DMS > Management > Map API Key

You need a valid API key and a Google Cloud Platform billing account to access Google core product. If not, DMS Map View will not be able to load Google Map correctly. Please visit the Google website below and following the directions to get API key: <https://developers.google.com/maps/documentation/directions/get-api-key>.



Parameter description:

Key: Specify the Google API Key. To use the Google Maps Embed API, you must register your app project on the Google API Console and get a Google API key which you can add to your app or website.

An administrator can request a new key from

<https://developers.google.com/maps/documentation/directions/get-api-key> then apply the new key at the page for displaying the map view completely.

Google APIs is a set of application programming interfaces (APIs) developed by Google which allow communication with Google Services and their integration to other services. Examples of these include Search, Gmail, Translate or Google Maps. Third-party apps can use these APIs to take advantage of or extend the functionality of the existing services.

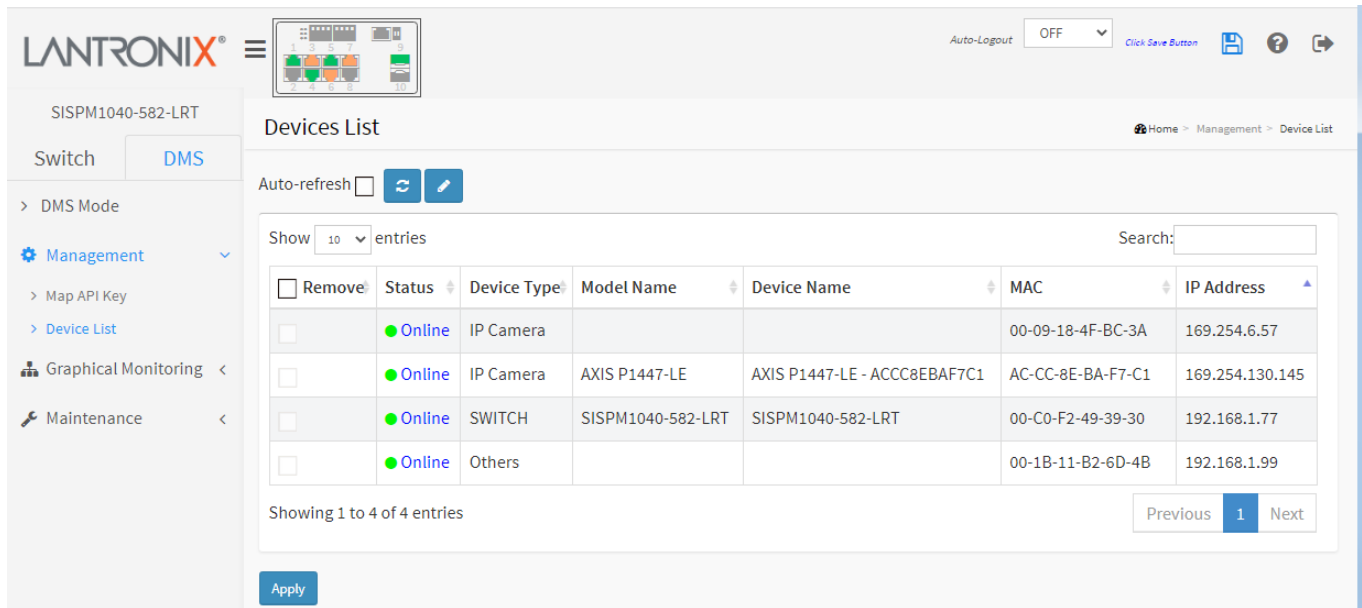
Use of some of the APIs requires authentication and authorization using the OAuth 2.0 protocol. OAuth 2.0 is a simple protocol. To start, it is necessary to obtain credentials from the Developers Console. Then the client app can request an access token from the Google Authorization Server and use that token for authorization when accessing a Google API service. From Wikipedia.

Button

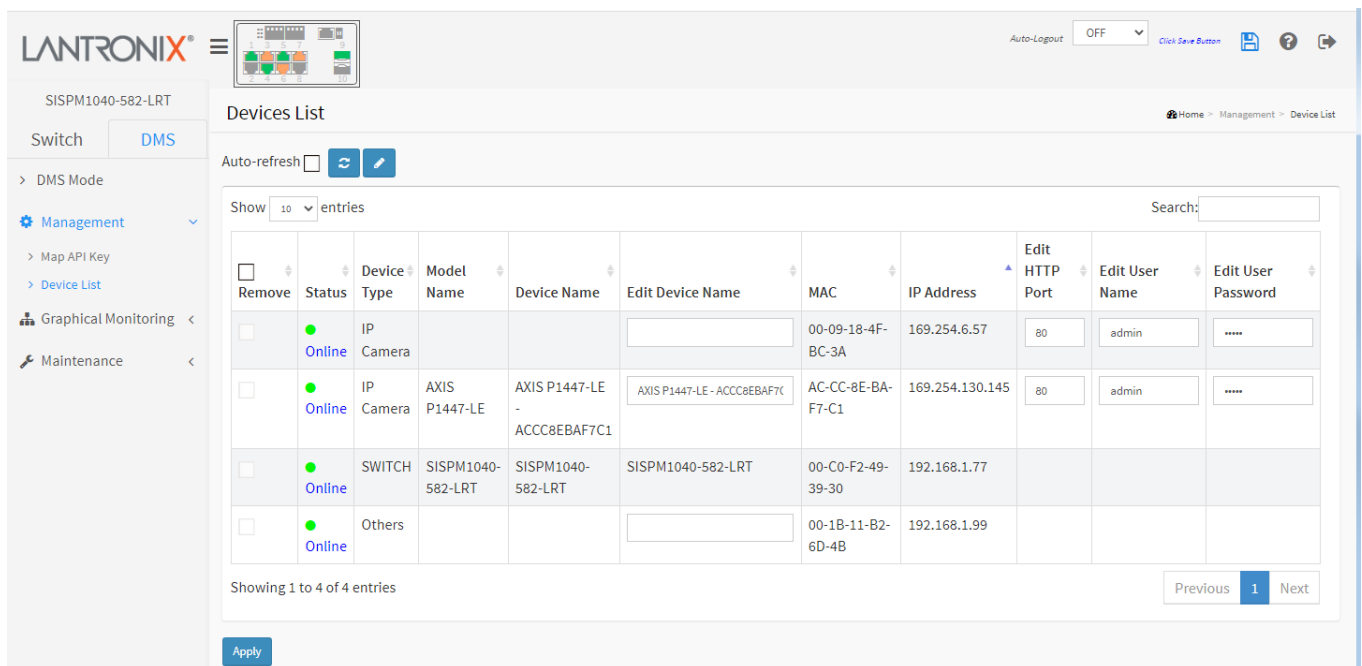
Apply : Click to save changes.

7.1.4 DMS > Management > Device List

This page provides an overview of the DMS device list. The default page displays with 6 columns:



When you click the  (Edit Device Name) icon, the table displays with 11 columns:



Parameter Descriptions:

Remove: Check to remove an off-line device from the list.

Status: Displays the device status (Online or Offline). Click a linked instance to display its diagnostic (see below).

Device Type: Displays the type of the network connected devices: General PC, General IP Cam, General IP Phone, Cisco SPA303, General AP, or Others (Mobile Device, General Switch, Internet Gateway, IP PBX, NAS, Printer, NVR, VMS, LED Light, Mini fridge, Shade or Unknown Device).

Model Name: The model name of the network connectivity devices.

Device Name: The device name of the network connectivity devices (editable).

Edit Device Name: When displayed, lets you change the current device name to a new one.

MAC: The mac address of the device.

IP Address: The IP address of the network connectivity devices (editable).

Edit HTTP Port: When displayed, lets you change the current device HTTP port number to a new one.

Edit User Name: When displayed, lets you change the current user name to a new one.

Edit User Password: When displayed, lets you change the current user's password to a new one.

Buttons

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

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



Edit Device Name: Click to toggle display of the input fields for editing the device name, HTTP port, User Name, and Password fields.

Apply: Click to save changes.

Click a linked [Online](#) instance to display its diagnostic results:

The screenshot shows the Lantronix web interface for the SISPM1040-582-LRT device. The main content area is titled "Diagnostics" and includes a table with the following data:

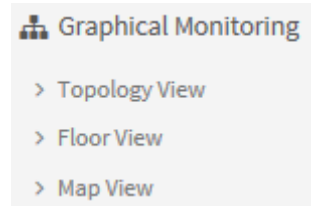
Select	Status	Model Name	Device Name	MAC	IP Address	Version
<input checked="" type="checkbox"/>	● Online			00-09-18-4F-BC-3A	169.254.6.57	

Below the table, there are two device status cards. The first card shows an IP address of 192.168.1.77 and a MAC address of 00-c0-f2-49-39-30. The second card shows an IP address of 169.254.6.57 and a MAC address of 00-09-18-4f-bc-3a. Both cards indicate a "Connection....." and "Cable status....." with green checkmarks.


See section "[7.3.2 DMS > Maintenance > Diagnostics](#)" below for more information.

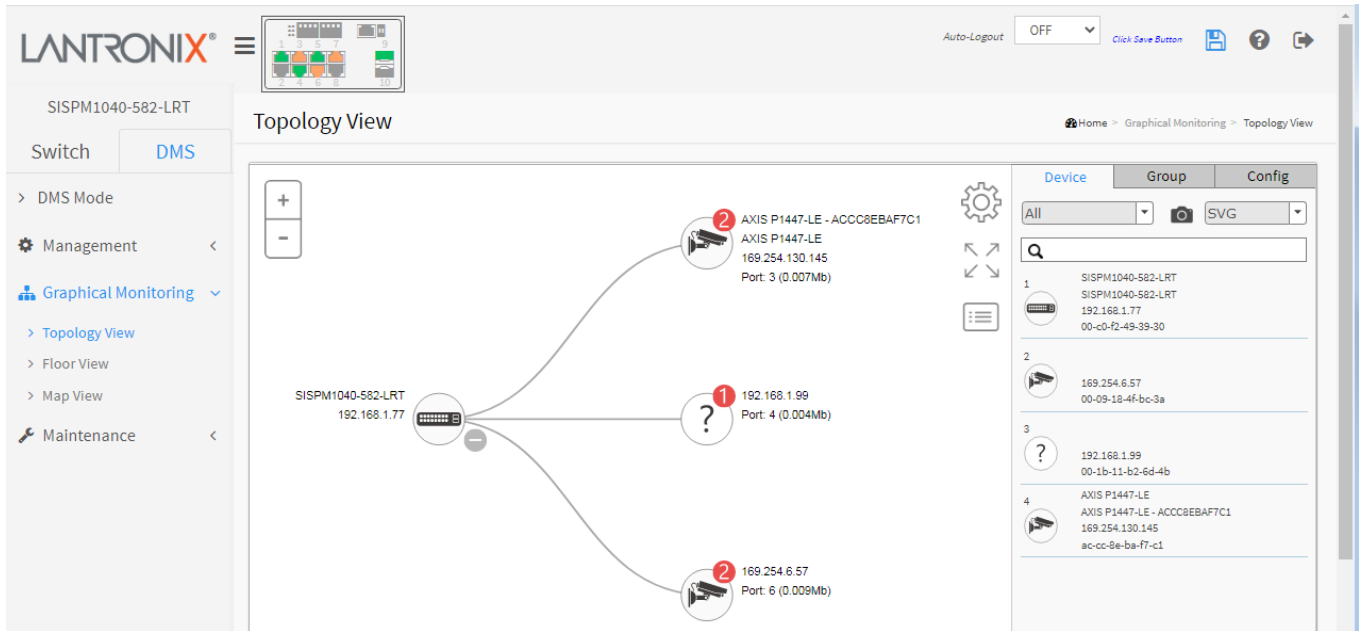
7.2 DMS > Graphical Monitoring

At DMS > Graphical Monitoring you can select Topology View, Floor View, and Map View.






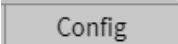
7.2.1 DMS > Graphical Monitoring > Topology View

Navigate to the DMS > Graphical Monitoring > Topology View menu path. Click the  button to display the right pane menu tabs (Device, Group, and Config).





















Topology View Icons / Controls

Click anywhere and drag to move the display area up /down/ left /right.

	Click “+” or “-” to zoom in or zoom out the display area.
	Click to alternately display / hide the Device tab.
	Click this icon to select the set of data to be displayed (MAC, IP, PoE power, etc.).
	Click this icon to sort, filter, or configure basic settings (e.g., VLAN, QoS).

Device Categories and Statuses

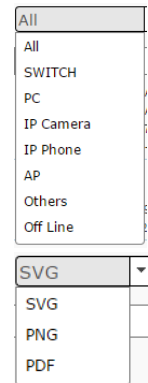
	The device is an SISPM1040-582-LRT switch.
	The device is a General switch.
	The device is a General PC.
	The device is an IP Cam.
	The device is an IP Phone.
	The device is a Wireless Access Point (WAP).
	The device is a Router.
	The device is an LED Light.
	The device is a Mini fridge.
	The device is a Shade.
	Black icon: Device link up. You can select a function and check for issues.
	Red icon: Device link down. You can diagnose the link status.
	Icon with number: indicates some event has occurred (e.g. Device Off-line, IP Duplicate, etc.) on the IP device; you can click on the device icon to check events in Notification.


 <p>40GBNIC-1 General PC 192.168.70.14 Port: 1 (0.009Mb)</p>	<p>A Red circled device number shows the number of alarm notifications for the device.</p>
	<p>Icon with question mark: Unknown Device; the IP device is detected by DMS, but the device type can't be recognized which will be classified as an unknown device type.</p>
	<p>Icon with question mark and red N indicates the device is unknown and is not connected.</p>
 <p>40GBNIC-1 General PC 192.168.70.14 Port: 1 (0.009Mb)</p>	<p>A Black device icon indicates device is operating normally. Click device icon to show its device console.</p>
 <p>SISPM1040-384-LRT-C 192.168.1.77 Port: 1 - Port: 7</p>	<p>A Red device icon indicates the device is operating abnormally.</p>

DMS Topology View parameters

Device tab parameters

Devices dropdown: Select the device type (All, SWITCH, PC, IP Camera, IP Phone, AP, Others, or Off Line).



Snapshot icon: Use the  icon to capture the displayed topology view.

File format: Select the graphics file type (SVG, PNG, or PDF).

Search box: Use the to search for a device by typing IP/MAC address or Model/Device name.

Group tab parameters

Vlan ID: Enter a VLAN ID (VID) for the new group (2-4095). 'VLAN ID' must be an integer value between 2 and 4095.

Name: Enter a name for the new group.

Traffic Priority: At the dropdown select 0 (Low) - 7 (High).

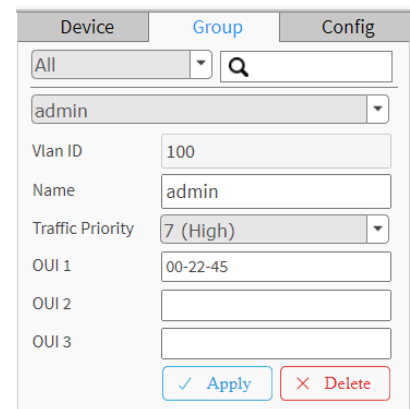
OUI 1: Enter an Organizationally Unique Identifier.

OUI 2: Enter a second Organizationally Unique Identifier.

OUI 3: Enter a third Organizationally Unique Identifier.

Apply: Click when done entering the new group data.

Delete: Click to close the new group configuration dialog.



Config tab parameters

Total Device: Displays the total number of devices discovered.

Controller IP: The control device IP address in the format 0.0.0.0.

DHCP Server IP: The IP address of the configured DHCP Server; otherwise, if no DHCP Server is configured.

DHCP Server: At the dropdown select Enabled or Disabled. The default is Disabled.

IP Range: The range type (Single Subnet or Multiple Subnet). If you select Multiple Subnet, selection fields display for IP Range 1 - Range 4.

Apply: Click the button to make the changes.

Device	Group	Config
Total Device	16	
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	192.168.1.254
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

Device data

Click a device in the Topology View to display its discovered data:

The screenshot shows the Lantronix web interface. On the left is a navigation menu with options like Management, Graphical Monitoring, and Maintenance. The main area is titled 'Topology View' and shows a network diagram with a switch icon labeled 'SISPM1040-582-LRT 192.168.1.77'. A pop-up window displays the configuration for this device:

SISPM1040-582-LRT	
Device Type	SWITCH
Device Name	SISPM1040-582-LRT
Model Name	SISPM1040-582-LRT
MAC Address	00-c0-f2-49-39-30
DHCP Client	Disable
IPv4 Address	192.168.1.77
Subnet Mask	255.255.255.0
Gateway	192.168.1.254
HTTP port	80
PoE Supply	17.1 W

Below the configuration are icons for Login, Upgrade, Find Switch, and PoE Config. At the bottom of the pop-up are links for Dashboard and Notification. On the right side of the interface, there is a 'Device' list table:

Device	Group	Config
All		
1	SISPM1040-582-LRT SISPM1040-582-LRT 192.168.1.77 00-c0-f2-49-39-30	
2	169.254.6.57 00-09-18-4f-bc-3a	
3	192.168.1.99 00-1b-11-b2-6d-4b	
4	AXIS P1447-LE AXIS P1447-LE - ACCC8EBAF7C1 169.254.130.145 ac-cc-8e-ba-f7-c1	

Device data parameters

Device Type: e.g., SWITCH, PC, IP Camera, IP Phone, AP (Access Point). **Device Type** is displayed automatically. If an unknown type is detected, you can still select its type from a pre-defined list. An IP device recognized as a DMS Control switch supports "Upgrade" and "Find Switch" functions.

An IP device recognized as a PoE device supports "Upgrade" and "Reboot" functions.

An IP device recognized as an IP Camera via the [ONVIF](#) protocol will support the "Streaming" function.

Device Name: e.g., SM16TAT2SA. Create your own Device Name or alias for easy management such as "1F_Lobby_Cam1".

Model Name: e.g., SM16TAT2SA.

Mac Address: e.g., 00-40-c7-1c-cb-6e; displayed automatically by DMS.

IP Address: e.g., 192.168.1.77; displayed automatically by DMS.

Http port: e.g., 80

PoE Used: displayed automatically by DMS (e.g., 2 Watts or Non-PoE).

Login icon: Click to display the login window.

Upgrade icon: Click to display a window in which you can enter a Tftp Server IP address and the name of a firmware file to upgrade to.

Find Switch icon: Click to flash the device LEDs for 15 seconds to help find the device. Click **OK** to clear the message.

Parent Node / Undo Parent: click to switch the selected device from its parent node device and back.

Remove: Click to remove an Off-line device.

PoE Config icon: Click to display a window in which you can enable or disable PoE Auto Checking globally and enable or disable PoE Mode on a port-by-port basis.

PoE Reboot: Click to re-boot PoE. Click OK at the confirmation prompt.

PoE Supply and PoE Used: displayed automatically by DMS.

Dashboard icon: Click to display the dashboard.

Notification icon: Click to display an editable message area.

Unknown Device parameters

You can click on an unknown device (?) to display its discovered data (see descriptions above). If an unknown type is detected, you can still select its type from the pre-defined list.

Monitor Console: Displays device traffic for health check purposes. 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.




The screenshot shows the 'Unknown Device' parameters form for IP address 192.168.1.99. The form includes the following fields:

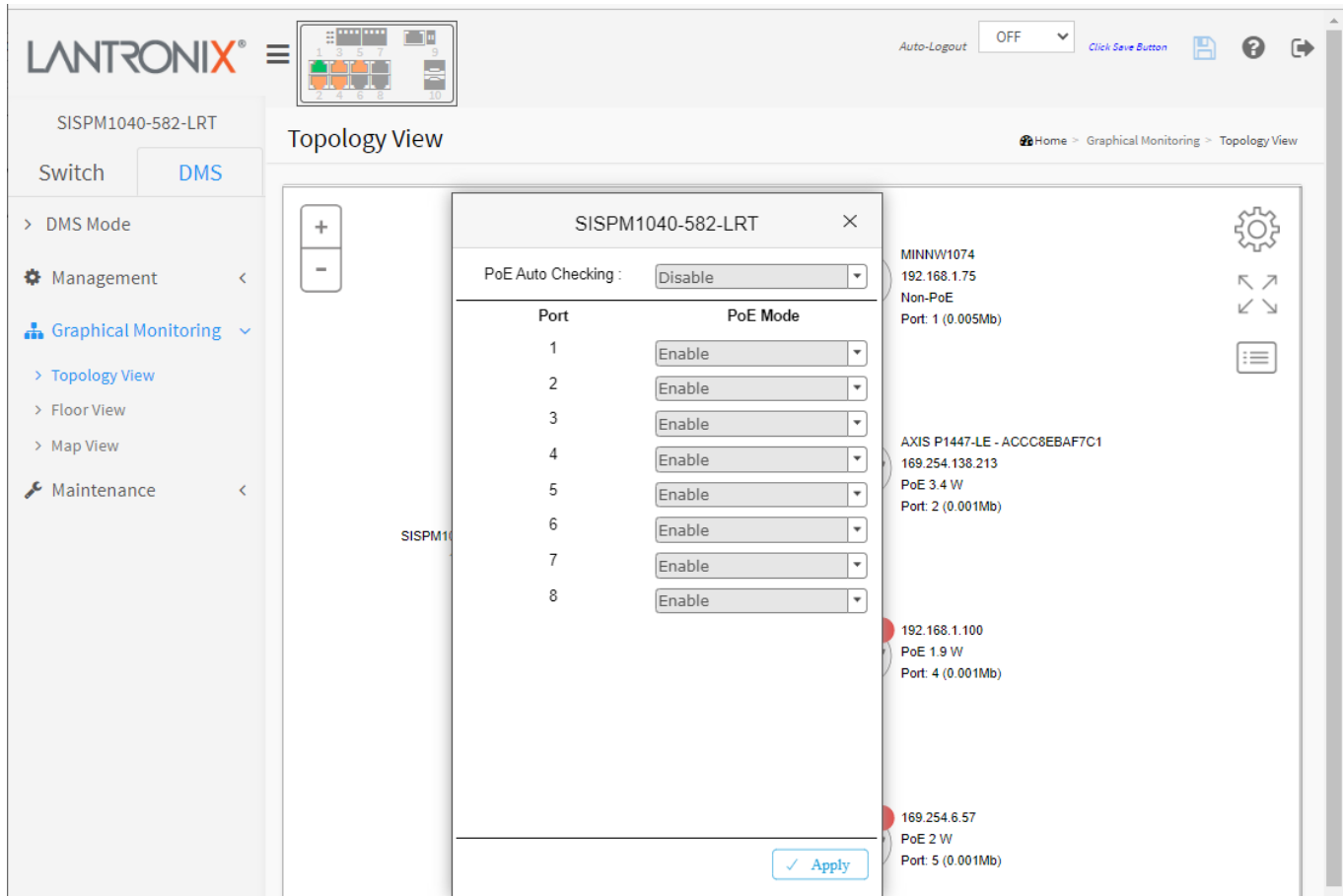
- Device Type: Unknown Device (dropdown)
- Device Name: (empty text field)
- Model Name: (empty text field)
- Mac Address: 00-1b-11-b2-6d-4b
- IP Address: 192.168.1.99
- Http Port: 80
- PoE Used: Non-PoE
- Diagnostics: (wrench icon)

At the bottom, there are three icons: 'Dashboard', 'Notification', and 'Monitor'.

PoE Auto Power Reset “AutoFill” Feature

When you enable Auto Power Reset (PoE Auto Checking) in DMS, the IP addresses of the connected devices are automatically filled in the Auto Power Reset configuration page.

1. Configure the “PoE Auto Power Reset” parameter at Switch > PoE Management > PoE Auto Power Reset. The default value of the “Failure Action” parameter is “Nothing”.
2. Configure PoE parameters at DMS > Graphical Monitoring > Topology View.
3. Left click on the switch icon to display its device configuration popup.
4. Click the PoE Config () icon to display the PoE Auto Checking pane.




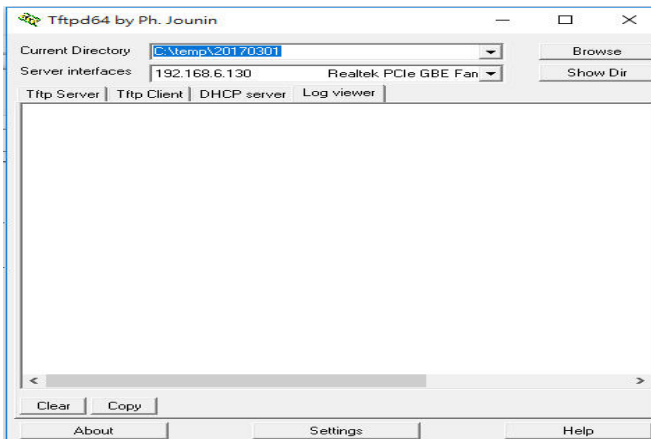
The screenshot displays the Lantronix web interface for the SISPM1040-582-LRT switch. The main navigation menu on the left includes 'Management', 'Graphical Monitoring', and 'Maintenance'. The 'Graphical Monitoring' section is expanded to show 'Topology View'. A configuration popup for the switch is open, showing the 'PoE Auto Checking' dropdown set to 'Disable'. Below this, a table lists ports 1 through 8, each with a 'PoE Mode' dropdown set to 'Enable'. An 'Apply' button is located at the bottom right of the popup. The background shows the 'Topology View' of the switch with several connected devices listed on the right side.

Port	PoE Mode
1	Enable
2	Enable
3	Enable
4	Enable
5	Enable
6	Enable
7	Enable
8	Enable

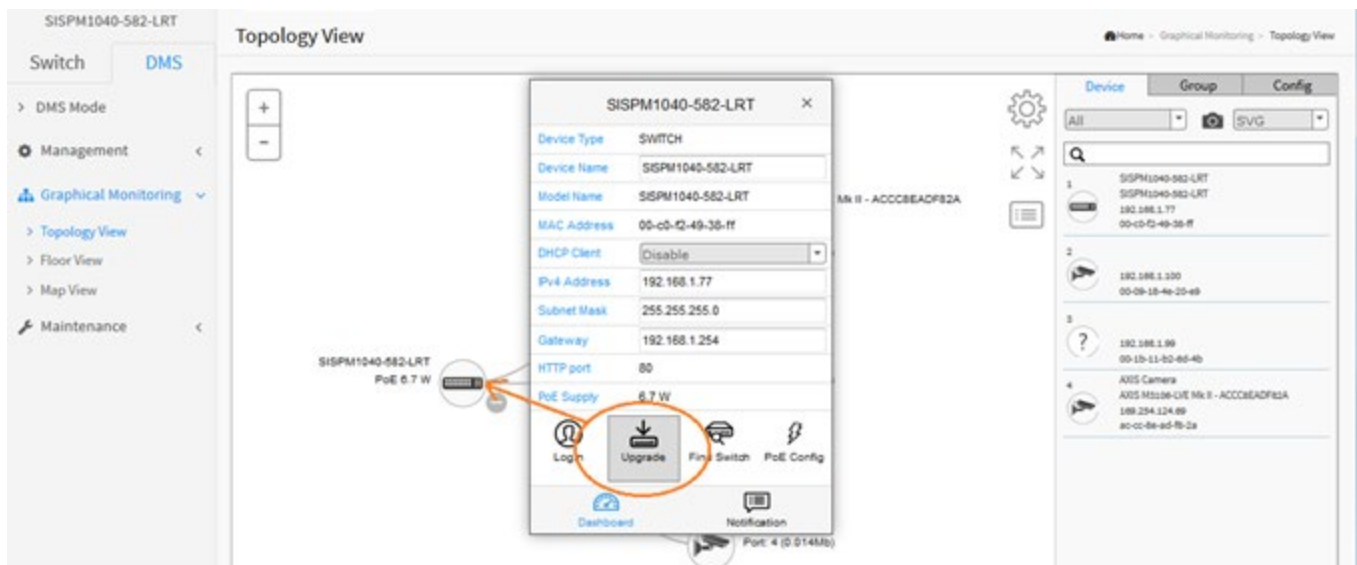
5. At the PoE Auto Checking dropdown select Enable.
6. Click the Apply button.

7.2.2 DMS Firmware Upgrade Procedure

1. Navigate to the DMS > Graphical Monitoring > Topology View or Floor View menu path.
2. Click the  button to display the right pane menu tabs (Entry and Config).
3. Connect all switches and make sure DMS is working.
 - Set all switches with different IP addresses and in the same IP segment.
 - Make sure gateway IP address is configured.
4. Enable the TFTP server and set the correct image path.



5. Click switch's icon, then click the "Upgrade" button in the Dashboard.



- Enter TFTP Server IP address and FW image name and select the switch on which you want to upgrade the FW.

The screenshot shows the Lantronix web interface for the SISPM1040-582-LRT device. The 'Topology View' window is open, displaying the configuration for a firmware upgrade. The TFTP Server IP is set to 192.168.1.77, and the File is set to RT_VB7.20.0146_CM_202202003.img. A table lists the device details, and an 'Apply' button is visible at the bottom right of the configuration window.

Name	IP	Version	Status
SISPM1040-582-LRT	192.168.1.77	VB7.20.0146	---

- Click "Apply" to start the Firmware upgrade. The message "Starting, please wait..." displays.
- Observe the upgrade status until completion.


Message: *Error : Firmware download fail* displays if the TFTP Server IP address or the FW image name entered is incorrect.

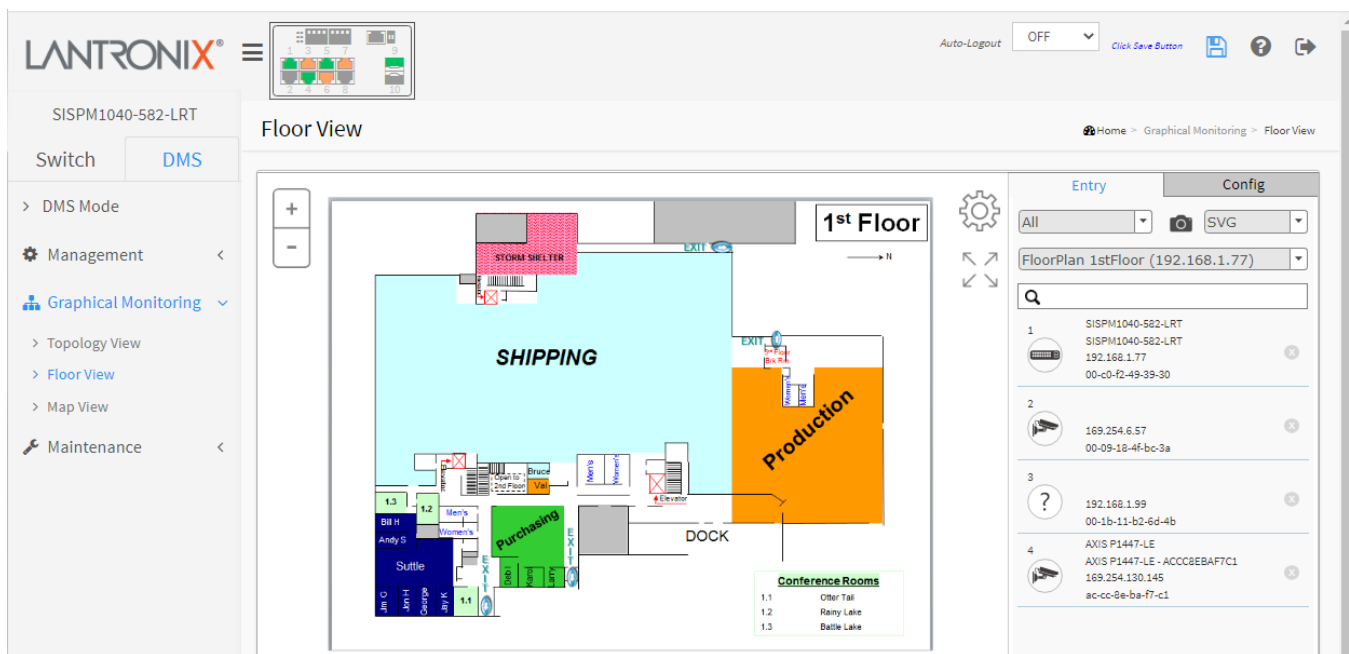
7.2.3 DMS > Graphical Monitoring > Floor View

Navigate to the DMS > Graphical Monitoring > Floor View menu path. You must first add one or more Floor Images at DMS > Maintenance > Floor Image.

The Floor View lets you:

- Drag and drop (anchor) devices onto Floor Maps
- Find device location instantly
- Store up to 10 Floor Maps per Switch
- Support IP Surveillance/VoIP/WiFi applications
- Other features same as Topology View


Click the  button to display the right pane menu tabs (Entry and Config).



DMS Floor View parameters

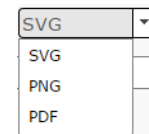
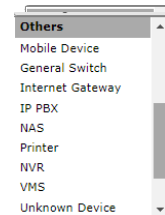
Entry tab parameters

Devices dropdown: Select the device type: **PC** (General PC), **IP Camera** (General IP Cam), **IP Phone** (General IP Phone, Cisco SPA303), **AP** (General AP), **Others** (Mobile Device, General Switch, Internet Gateway, IP PBX, NAS, Printer, NVR, VMS, Unknown Device, LED Light, LED Light, Mini fridge, Shade).

Snapshot icon: Use the  icon to capture the displayed Floor view.

File format: Select the graphics file type (SVG, PNG, or PDF).

Search box: Use the to search for a device by typing IP/MAC address or Model/Device name.



Config tab parameters

Total Device: Displays the total number of devices discovered.

Master Controller IP: The control device IP address in the format 0.0.0.0.

IP Range: The range type (Single Subnet or Multiple Subnet).

DHCP Server IP: Select Enabled or Disabled.

DHCP Server: Select Single Subnet or Multiple Subnet.

Apply: Click the button to save the selections.

Device	Config
Total Device	2
Controller IP	192.168.1.77
DHCP Server IP	---
DHCP Server	Disabled
IP Range	Single Subnet
<input type="button" value="✓ Apply"/>	

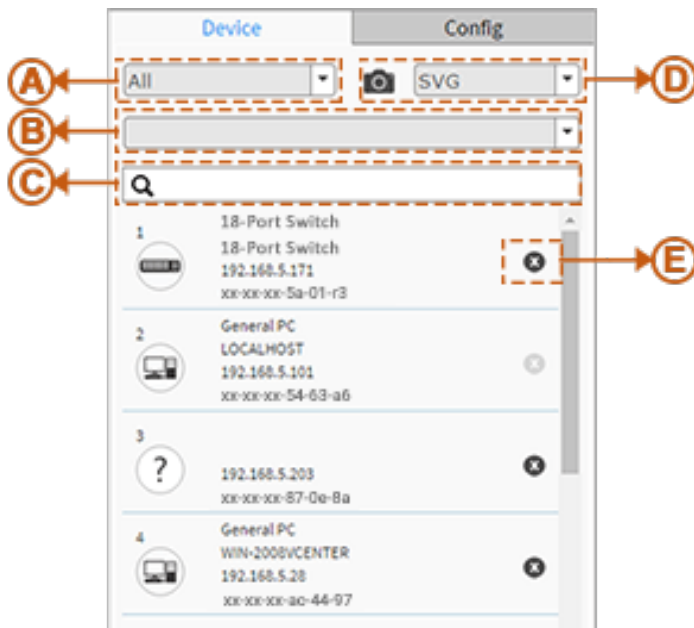


Icons with plus and minus marks: Zoom in and zoom out the floor view, user can scroll up/down with mouse to achieve the same purpose.



In the upper right corner, there is a "Setting icon". When user clicks the icon, it will pop-up Device, Config, export floor view and advanced search functions for the device.

1. 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

2. System Setting Console

The screenshot shows a configuration interface with two tabs: "Device" and "Config". The "Config" tab is active. Three callouts labeled A, B, and C point to specific fields:

- A** points to the "Total Device" field, which has the value "3".
- B** points to the "Controller IP" field, which has the value "192.168.5.171".
- C** points to the "IP Range" dropdown menu, which is currently set to "Multiple Subnet".

Below the dropdown, there are four rows labeled "Range 1" through "Range 4". Each row contains two input fields for IP addresses, both currently set to "0.0.0.0". At the bottom right of the configuration area is an "Apply" button with a checkmark icon.

Function

A. Shows how many IP devices are detected and displayed in the topology view.

B. Shows the Master IP.

C. Single or Multiple Subnet:

Single Subnet: DMS will base on the master switch's IP address. Here the subnet means "255.255.255.0"

Multiple Subnet: To provide 4 ranges for inputting manually. (In this case, we suggest you adjust the switch's subnet mask to "255.255.0.0" also to avoid IP devices can't be recognized.)

Device Status



Black icon with green outline: Device link up. You can select functions and check issues.



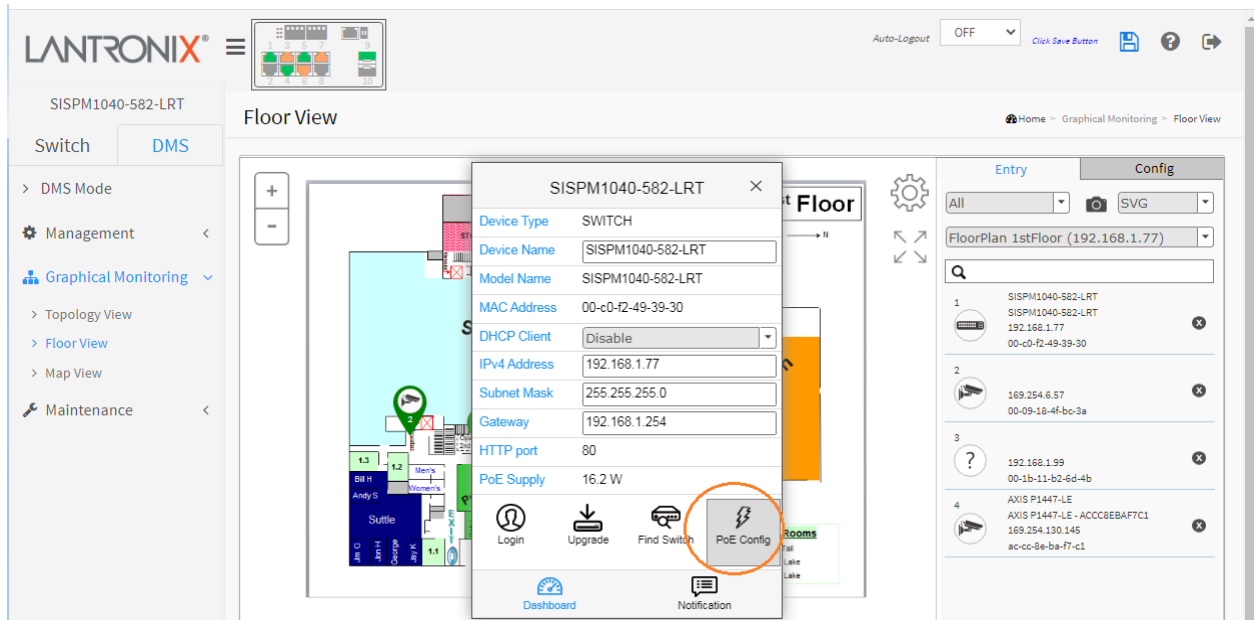
Red icon with red outline: Device link down. You can diagnose the link status.



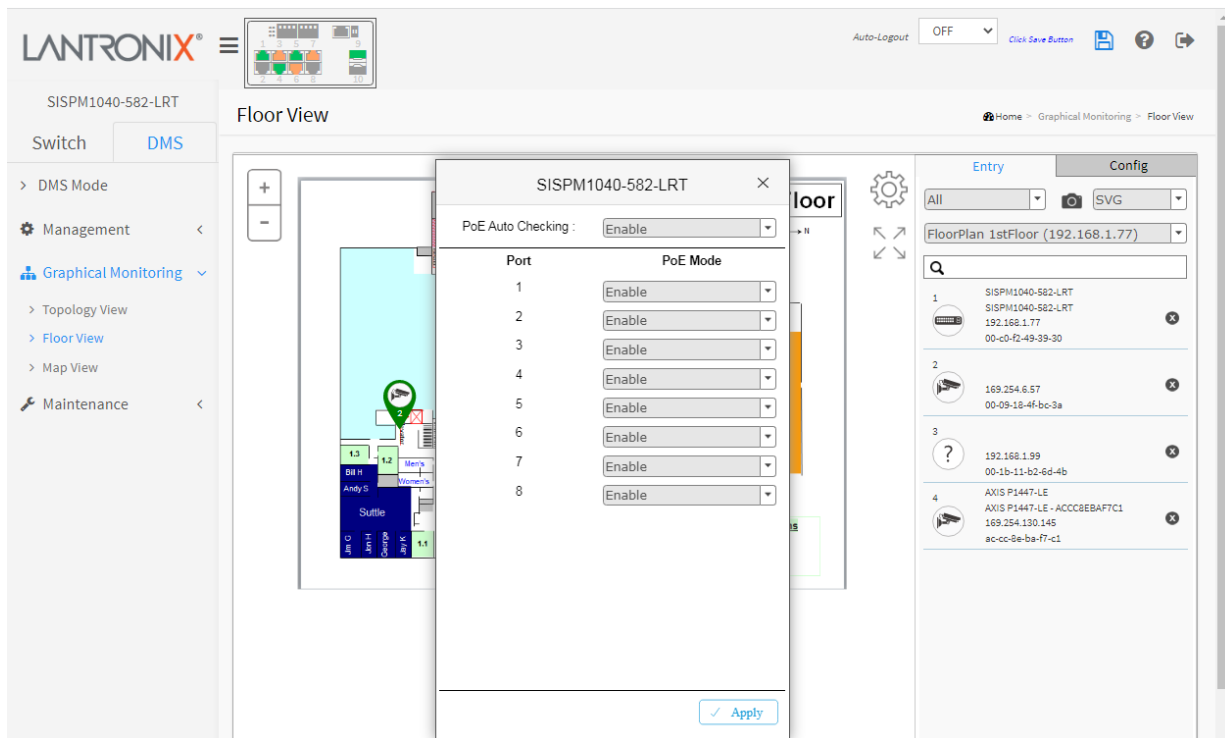
Black icon with number: Issues exist on IP device; click picture to check event log.

7.2.3.1 PoE Auto Checking

1. At **DMS > Graphical Monitoring > Floor View** click on a device.
2. At the device's dialog, click the **PoE Config** button.

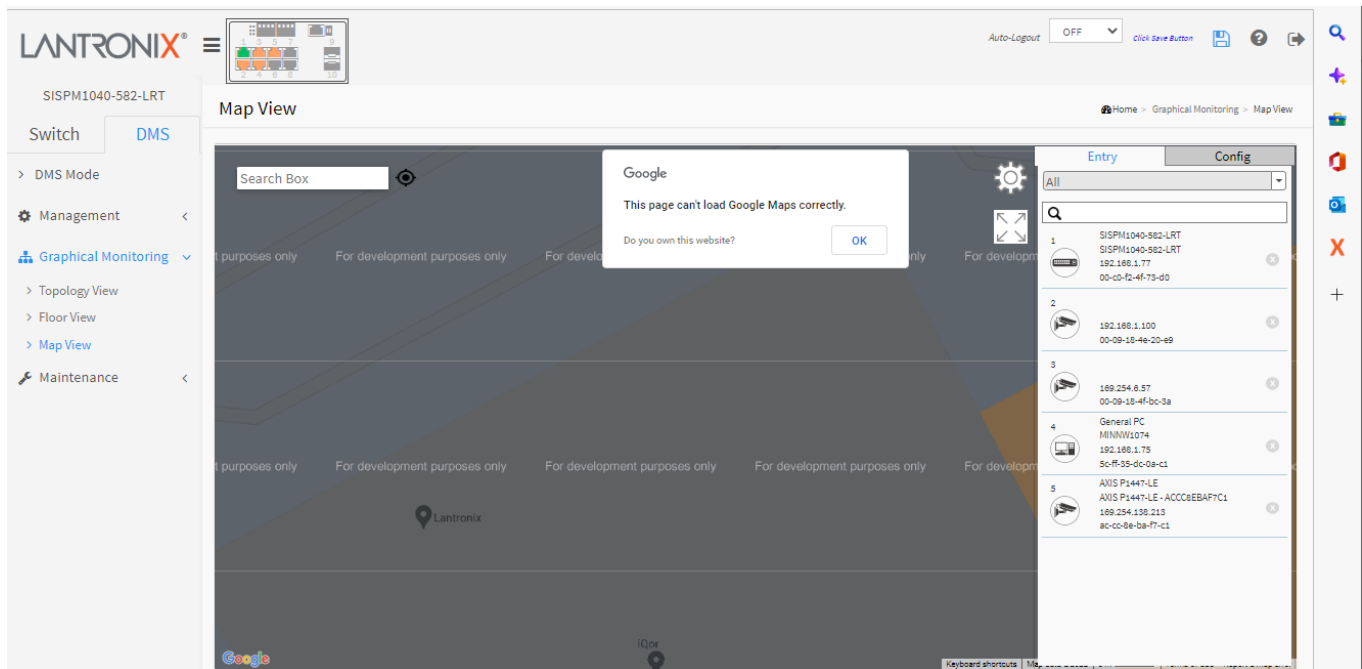


3. At the PoE Auto Checking dropdown select Enable.
4. For each port select a PoE Mode (Enable or Disable). The default is Disabled.
5. Click the **Apply** button.



7.2.4 DMS > Graphical Monitoring > Map View

Navigate to the DMS > Graphical Monitoring > Map View menu path. Here you can find the location of the devices even they are installed in different building. You can place device icons on the Map View and navigate by Google Maps. If the page displays the message *"This page can't load Google Maps correctly."* click the OK button and go to [7.1.3 DMS > Management > Map API Key](#) on page 451.



Parameter Descriptions:

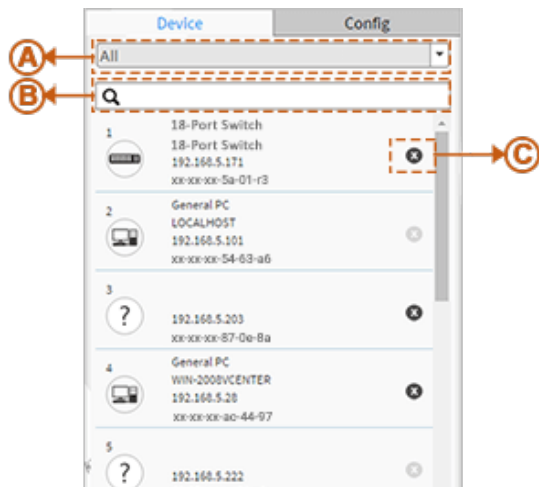


There is a "Setting" icon in the upper right corner which you can click to pop-up Entry, Config, and advanced search functions for the device.

Search box : enter some text in the (an address, company name, city, etc.) and hit Enter to display a map of the requested data.



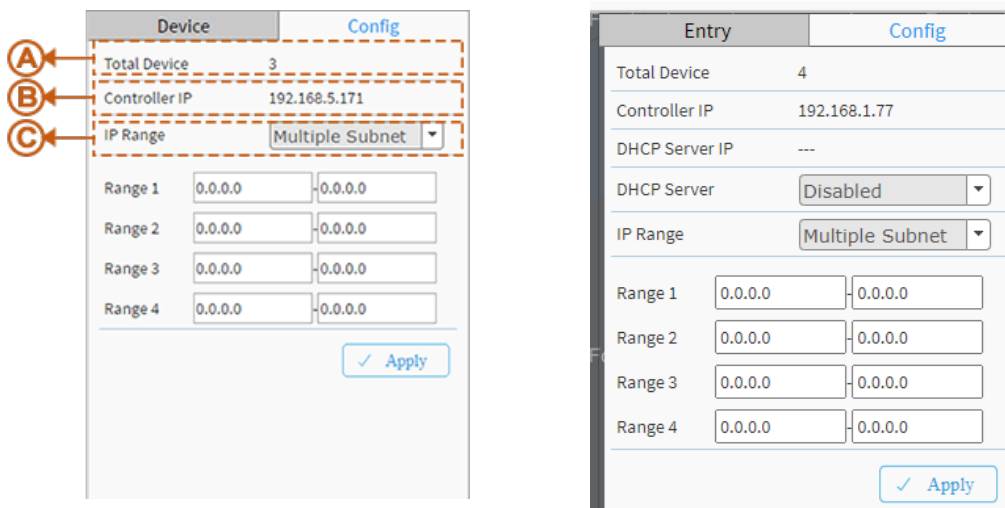
1. Device Search Console



Function

- A. Filter devices by Device Type.
- B. Search devices by key words full text search.
- C. Remove a device from Map View.

2. System Setting Console



Function

Total Device: Shows how many IP devices are detected and displayed in Topology view.

Controller IP: Shows the Master (Controller) IP address.

DHCP Server IP: Shows the IP address of the DHCP server (if enabled).

DHCP Server: Select Disabled or Enabled as the DHCP server state.

IP Range: Single or Multiple Subnet. Single Subnet: DMS will be based 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 this case we suggest you adjust switch's subnet mask to "255.255.0.0" also to avoid IP devices that can't be recognized).

Map View Functions

- Anchor Devices onto Google Maps.
- Find Devices Instantly from a Map.
- On-Line Search Company/Address.
- Outdoor IP Cam/WiFi Applications.
- Other features same as Topology View
- To place and remove a device icon
 - To select a device, click its icon in the device list.
 - The device icon will show on the map's default location.
 - Click and hold left mouse to drag-and-drop the icon to the correct location on the Map View.
 - Click the cross sign on the right side of the device icon to remove a device from Map View.

Device Status



Black Icon: Device link up. You can select a function and check issues.



Red Icon: Device link down. You can diagnose the link status.

Satellite View: From DMS > Graphical Monitoring > Map View you can click Satellite to replace the Map View with a satellite view:

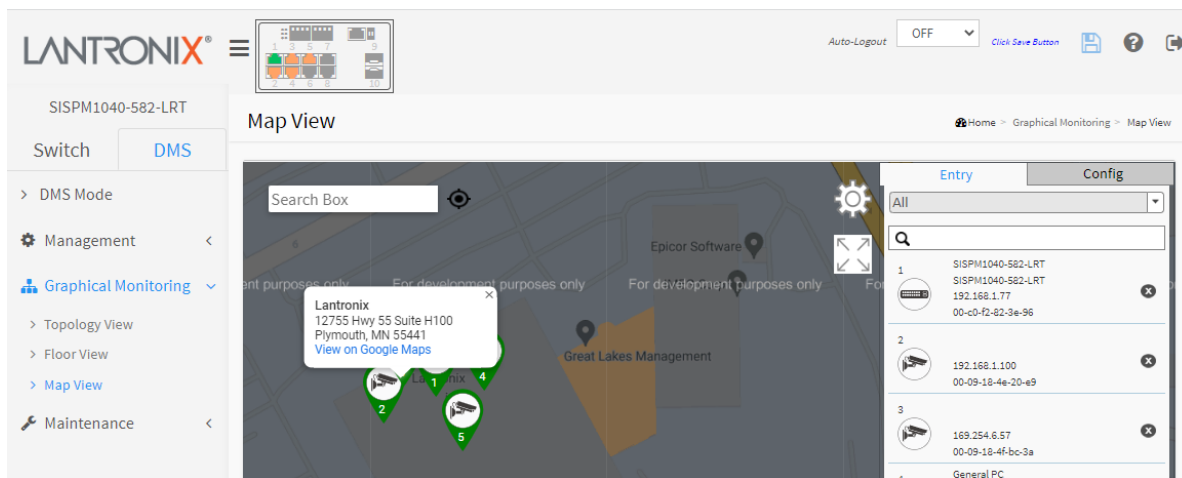


Message: *Do you own this website?*

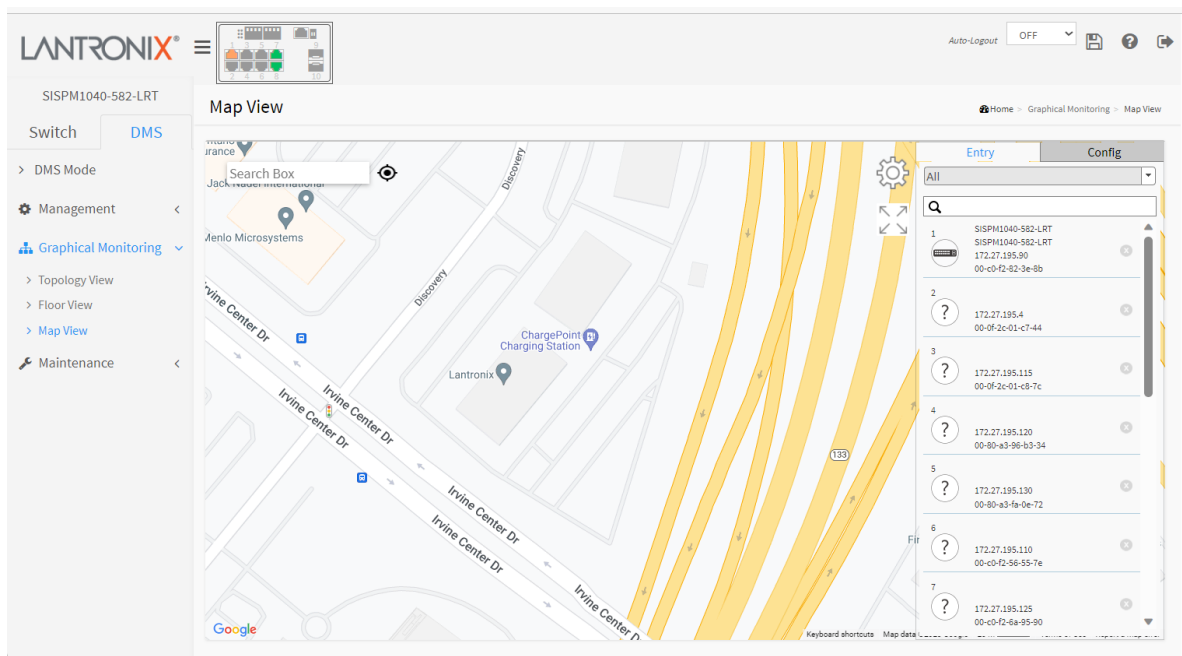
Meaning: If you are NOT the website owner, there are no steps you can take to fix any of these errors. However, you may want to notify the site owner if possible.

Recovery:

1. Click the linked text *Do you own this website?* to view the Google Maps Platform support page at https://developers.google.com/maps/documentation/javascript/error-messages?utm_source=maps_js&utm_medium=degraded&utm_campaign=keyless#api-key-and-billing-errors
2. Click the OK button to clear the message and continue operation.

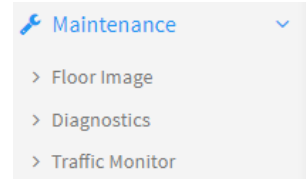
Example 1:

Click the linked text [View on Google Maps](#) to view the various map presentations and use the available tool (e.g., Satellite view, Layers, Browse Street View Images, Zoom, Sign In, etc.).

Example 2:

7.4 DMS > Maintenance

At DMS > Graphical Maintenance you can select Floor Image, Diagnostics, and Traffic Monitor.



7.4.1 DMS > Maintenance > Floor Image

Navigate to the DMS > Maintenance > Floor Image menu path to display the Floor Image Management page. This page lets you upload and manage floor map images.

You can then plan IP devices' installation location onto the custom uploaded floor images at DMS > Graphical Monitoring > Floor View.

Parameter Descriptions:

Maximum: x files: By default this field displays "Maximum: 10 files". With each switch added and discovered, the maximum value increases by 10. For example, if only two switches are connected to each other, the maximum number of files will increase from 10 to 20 (on both switches). But once the connection is removed and after an approximate 1 minute wait, the maximum number of files will go back to 10.

The maximum number of images displayed is additive. When the switch is stand alone with no connections to other DMS switches, the number displayed is 10. As other DMS switches are added, the field is incremented by 10 for each one.

Used: x file(s): The number of files that have already been uploaded.

Free: x file(s): The number of files that can be uploaded before reaching the maximum number of images.

Add Floor Image: Click the Browse... button to navigate to and select a .jpg or .png file.

Select: Select the checkbox to select an image from the list. Only jpg, png are allowed.

Name: Shows the selected file name.

Buttons

Browse... : Click to browse to and select an existing Floor Image file.

Add: Click Add to upload. When done, a snapshot displays. See the Example below.

Delete: To remove an existing floor map, select its checkbox and click Delete to remove.

Message: *Only jpg, png are allowed*

Meaning: The selected floor image must be a JPG or PNG file.

Recovery: **1.** Click the **OK** button to clear the message. **2.** Click the **Choose File** button and select a graphics file with an extension of .JPG or .PNG.

Message: *Add file fail, file name already exist!*

Meaning: You tried to load the same floor image again.

Recovery: **1.** Click the **Previous** button to clear the message. **2.** Try loading a different floor image.




Example: Maximum: 10 files Used: 1 file(s) Free: 9 file(s)

The screenshot shows the 'Floor Image Management' interface. At the top, it displays file statistics: Maximum: 10 files, Used: 1 file(s), and Free: 9 file(s). Below this, there is a section for adding a new floor image. It includes a 'Browse...' button, a text input field for 'Name', and an 'Add' button. A table below the form lists the existing floor image: 'FloorPlan1stFloor (192.168.1.77)' with a 'Select' checkbox. An 'Image' column shows a thumbnail of the floor plan. A 'Delete' button is located at the bottom left of the table area.

Select	No.	File Name	Image
<input type="checkbox"/>	1	FloorPlan1stFloor (192.168.1.77)	

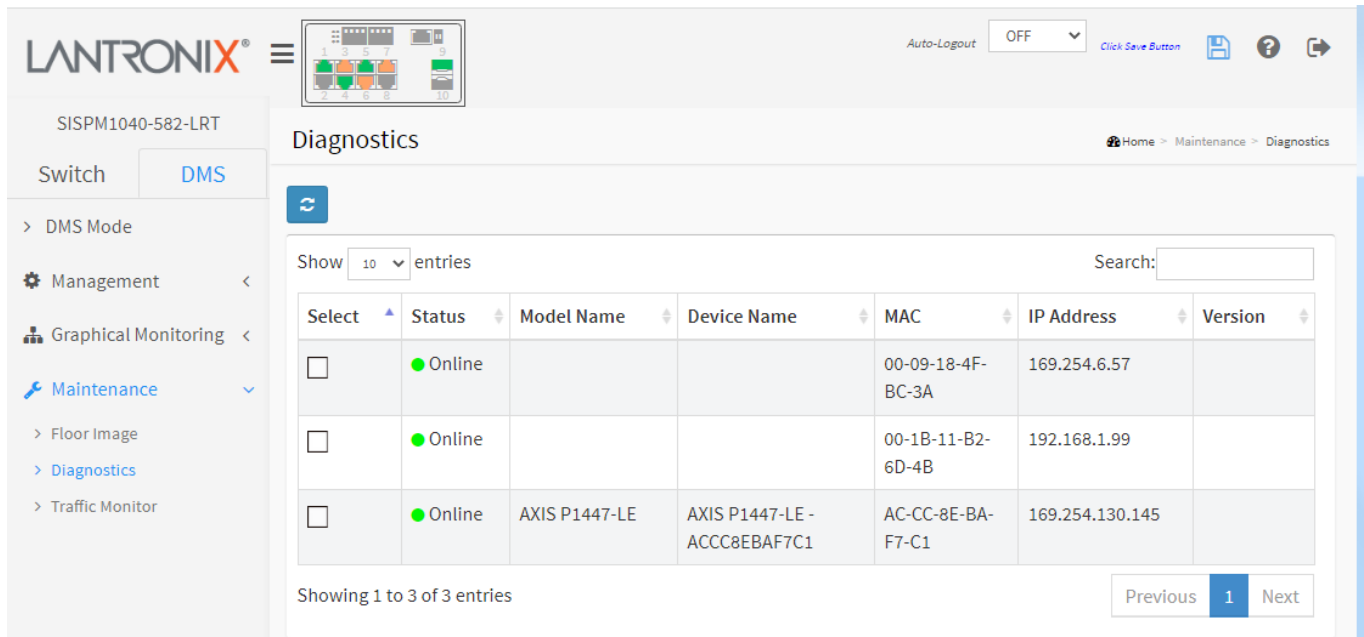
Example: Maximum: 10 files, Used: 3 file(s); Free: 7 file(s)

The screenshot displays the 'Floor Image Management' interface. At the top, it shows storage statistics: 'Maximum: 10 files', 'Used: 3 file(s)', and 'Free: 7 file(s)'. Below this is a form to 'Add Floor Image' with a 'Browse...' button and a 'Name' input field. A table lists three existing floor plans, each with a 'Select' checkbox, a 'No.' column, a 'File Name' column, and an 'Image' column. A 'Delete' button is located at the bottom left of the table area.

Select	No.	File Name	Image
<input type="checkbox"/>	1	FloorPlan1stFloor (192.168.1.77)	
<input type="checkbox"/>	2	FloorPlan-2ndFloor (192.168.1.77)	
<input type="checkbox"/>	3	Floor Plan - 3rd Floor (192.168.1.77)	

7.4.2 DMS > Maintenance > Diagnostics

Navigate to the DMS > Maintenance > Diagnostics menu path to display the Diagnostics page.



Parameter Descriptions:

Select : Check to select a device from the list. See the Example below for diagnostics results.

Status : Device is Online or Offline.

Model Name : The model name of the network connectivity devices.


Device Name : The device name of the network connectivity devices.

MAC : The mac address of the device.

IP Address : The IP address of the network connectivity devices.

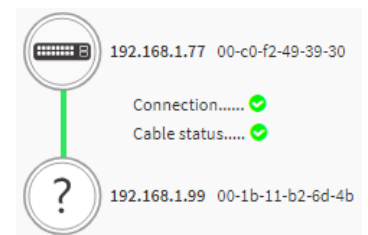
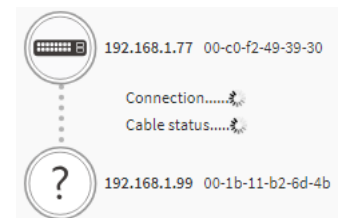
Version : The Version of the network connectivity devices.

Buttons

 : Refreshes the displayed table starting from the input fields.

Search : Search for any key word you want.

Another Try: Click to leave the diagnostic result page.



Diagnostics Page Example: Connection and Cable Status good:

The screenshot shows the Lantronix web interface for the SISPM1040-582-LRT device. The left sidebar contains navigation options: DMS Mode, Management, Graphical Monitoring, Maintenance, Floor Image, Diagnostics, and Traffic Monitor. The main content area is titled 'Diagnostics' and features a table with columns: Select, Status, Model Name, Device Name, MAC, IP Address, and Version. The first entry is selected and shows a green 'Online' status. Below the table, a detailed view for the selected entry shows a keyboard icon, IP address 192.168.1.77, MAC address 00-c0-f2-49-39-30, and green checkmarks for 'Connection.....' and 'Cable status.....'. A second entry with a camera icon, IP address 169.254.6.57, and MAC address 00-09-18-4f-bc-3a is also visible.

IP connection and physical cable testing is performed and shows that both tests have failed (two red X characters shown right) Testing shows cable is disconnected/broken and the distance from the switch for troubleshooting. A distance of 0m means the cable has been unplugged from the switch.

The screenshot shows a 'Diagnostics' window with a keyboard icon, IP address 192.168.1.75, and red 'X' marks for 'Connection.....' and 'Cable length is 60m, broken at 0m'. A camera icon and IP address 192.168.1.105 are also visible.

7.4.3 DMS > Maintenance > Traffic Monitor

Navigate to the DMS > Maintenance > Traffic Monitor menu path to display the Traffic Monitor page.

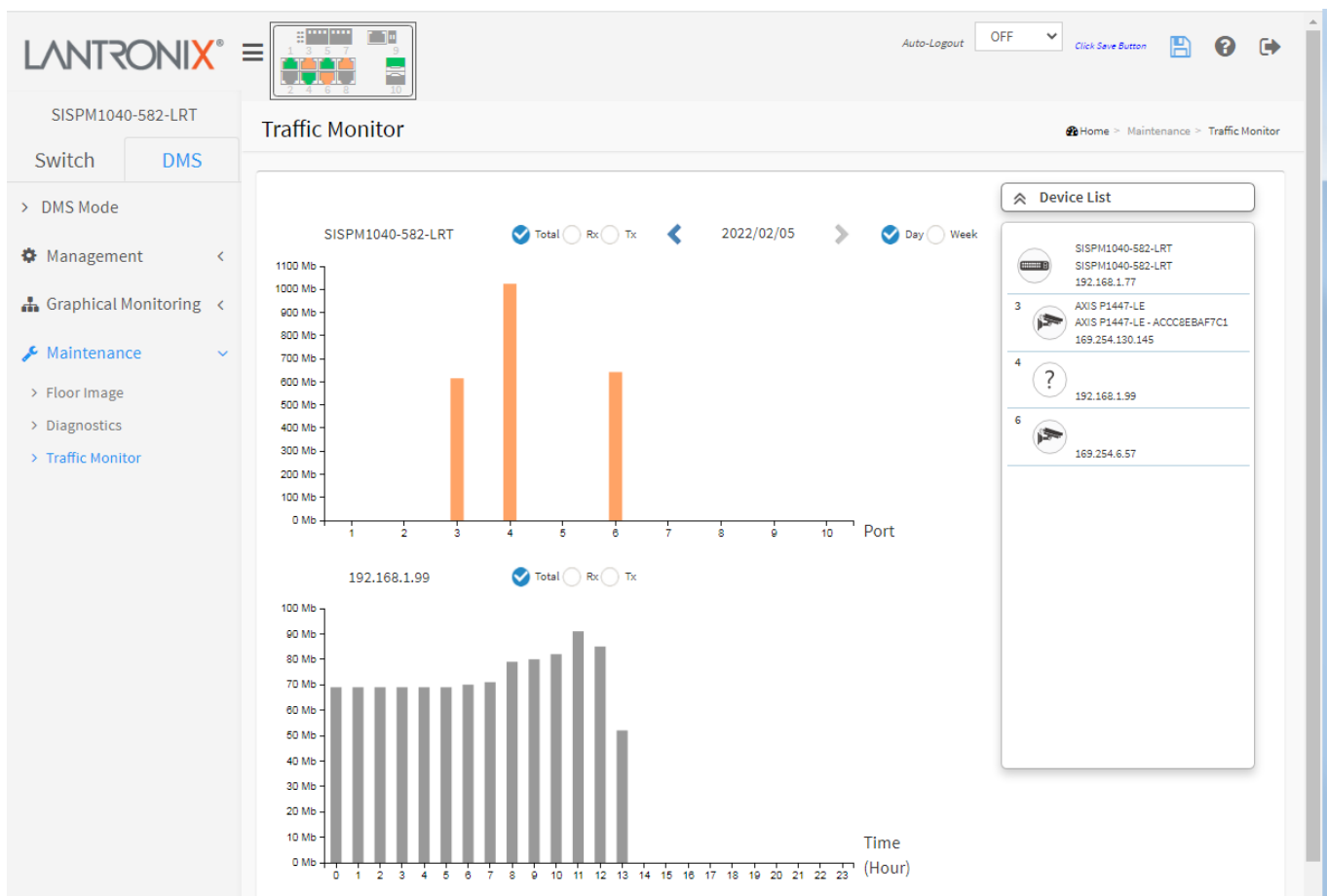
This page displays charts of network traffic of all the devices managed by the Controller switch. Note that FW v7.10.2205 added Traffic Monitor back to DMS.

To view Traffic Monitor data in the web UI:

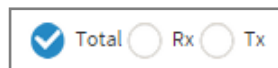
1. Click DMS, Maintenance, Traffic Monitor.
2. Select the displayed detail (Total, Rx, or Tx).
3. Select the date of monitored traffic to display.
4. Select the amount of monitored traffic to display (Day or Week).
5. View the monitored traffic displayed.

Click a chart column to display a device's second chart.

This page displays a chart of network traffic of all discovered devices. Numbers are shown in Mbit/s. You can view the traffic of all ports or a specific port. Click on 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.



Parameter Descriptions:



Total / Rx / Tx: Select the set of data to be displayed. The default is Total.



< yy/mm/dd >: Select the date of data displayed.

Day / Week: Select a day’s worth of data or a week’s worth of data to be displayed.

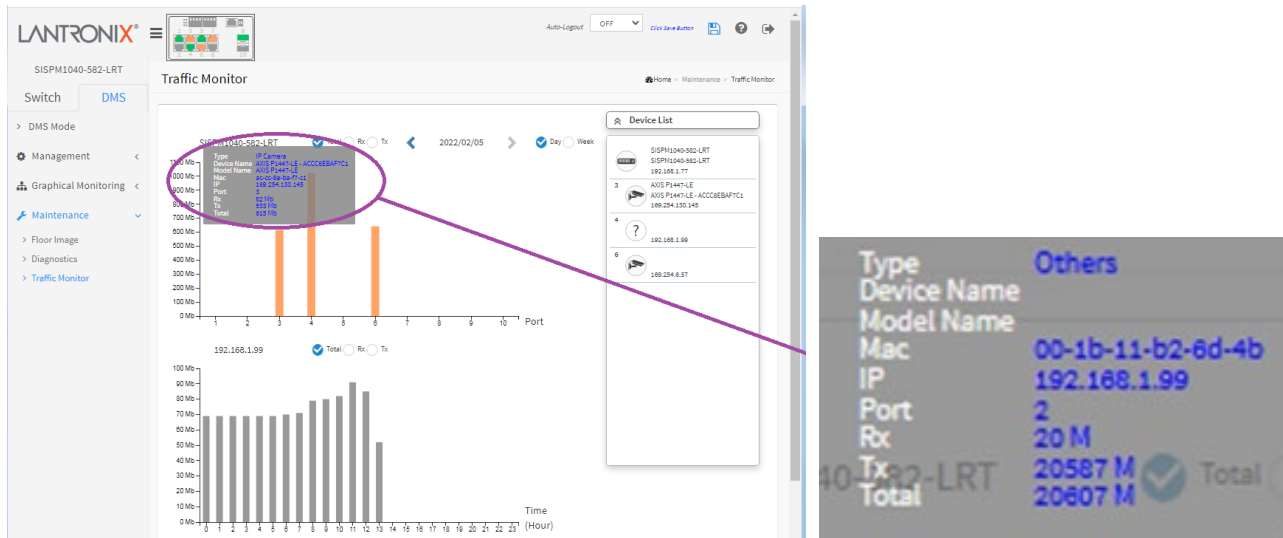
Device List: Displays the set of discovered devices.

Throughput: Vertical axis shows the device throughput (e.g., 0 M – 18000 M or 0 M-1200 M).

Port: Horizontal axis shows the switch port numbers.

Time (Hour): Horizontal axis shows the time elapsed in hours (0-23).

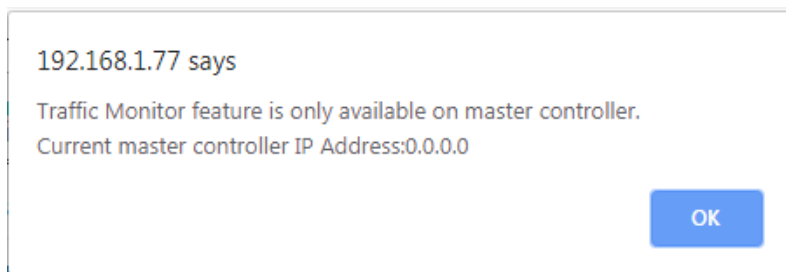
Hover the mouse pointer over a bar on the graph to display its information.



Message: *Traffic Monitor is only available on master controller. Current master controller IP Address:0.0.0.0.*

Meaning: You tried to view DMS Traffic Monitor on a switch that is not the current DMS Master (Controller) switch.

Recovery: **1.** Click the OK button to clear the message. **2.** Either make this switch the DMS Master or view Traffic Monitor from the assigned DMS Master switch.



7.4.4 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 the 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 reach an 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.

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.*

Meaning: If loading over 25,000 maps loaded per day over the network, request a new key from <https://developers.google.com/maps/documentation/directions/get-api-key> then apply the new key at the page for displaying the map view completely. See the [Google Account Changes webpage](#).

Recovery:

1. Click the **OK** button to clear the message.
2. Navigate to DMS > Management > Map API Key.
3. See [7.1.3 DMS > Management > Map API Key](#) on page 451.
4. Click the linked text "Do you own this website?" to display the Google [API Key and Billing Errors Troubleshooting](#) page.
5. For help on finding error messages, see the section on [checking errors in your browser](#).
6. See the Google [Maps Platform FAQ](#) for more information.

Message: *Traffic Monitor feature is only available on master controller. Current master controller IP Address: x.x.x.x.*

Meaning: This switch cannot function as the Master (Controller) switch.

Recovery: See [7.1.1 DMS > DMS Mode](#) on page 448.

Issue: IE Tab fix for Chrome-Firefox - DMS Topology view issue.

Description: In order to log into a camera on a switch with PoE+ or PoE++ from the DMS Topology View window from a browser other than Internet Explorer, you must have an “IE Tab” extension installed. This is needed for both Chrome and Firefox. IE Tab is an extension for the Google Chrome and Mozilla Firefox web browsers that lets you view pages using the Internet Explorer layout engine.

Recovery:

Google Chrome: <https://chrome.google.com/webstore/detail/ie-tab/hehijbfgiekmjfkfjpbkbammjbdenadd?hl=en-US>

Firefox: <https://addons.mozilla.org/en-US/firefox/addon/open-in-internet-explorer/>

8. Recording Device and System Information

After performing the troubleshooting procedures, and before calling or emailing Technical Support, please record as much information as possible in order to help the Tech Support Engineer.

1. Select the Configuration > System > Information menu path. From the CLI, use the show commands to gather the information below or as requested by the Support Engineer.

2. Model Name: _____ System Date: _____
Serial # _____ Firmware Version: _____
PoE Firmware Version: _____ Hardware Version: _____

3. LED Status: _____

4. Provide additional information to your Tech Support Specialist. See the "Troubleshooting" section above.

Your Lantronix service contract number: _____

Describe the failure: _____

A description of any action(s) already taken to resolve the problem (e.g., changing mode, rebooting, etc.):

The model #, serial # and rev of all involved Lantronix products in the network: _____

A description of your network environment (PDs, cable type, etc.): _____

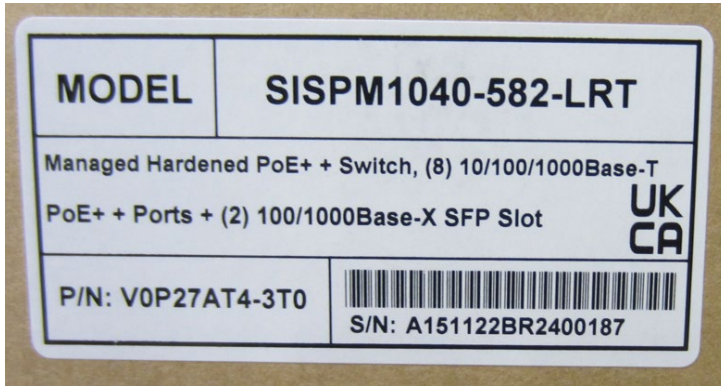
The device history (i.e., have you returned the device before, is this a recurring problem, etc.): _____

Any previous Return Material Authorization (RMA) numbers: _____

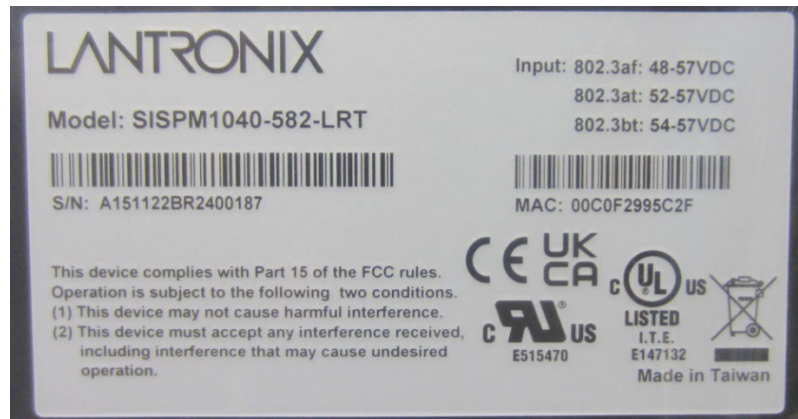
Attach any screen captures, config files, diagnostic results, server reports, etc. _____

8.1 Product Labels

The shipping box and the device label also provide Information you can record to help the Lantronix Tech Support Engineer.



Box Labels



Device Label

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.

A-1. Configure DHCP Per Port via the Web UI

The switch's DHCP server assigns IP addresses. Clients get IP addresses in sequence and the switch assigns IP addresses on a per-port basis starting from the configured IP range. For example, if the IP address range is configured as 192.168.10.20 - 192.168.10.37 with one DHCP device connected to port 1, the client will always get IP address 192.168.10.20, then port 3 is always distributed IP address 192.168.10.22, even if port 2 is an empty port (because port 2 is always distributed IP address 192.168.10.21).

The switch does not allow a DHCP per Port pool to include the switch's address.

IP address assigned range and VLAN 1 should stay in the same subnet mask.

The configurable IP address range is allowed to configure over 18 IP addresses, but the switch always assigns one IP address per port connecting device.

When the DHCP Per Port function is enabled, the switch software will automatically create the related DHCP pool named "DHCP_Per_Port".

Once the DHCP Per Port function is enabled on one switch, IPv4 DHCP client at VLAN1 mode (DMS DHCP mode), DHCP server mode are all limited to be enabled at the same time (an error message displays if attempted).

If the DHCP server pool has been configured, once you enable the DHCP Per Port function, then that DHCP server pool configuration will be overwritten.

Only for VLAN 1, clients issued DHCP packets will not be broadcast/forwarded to other ports. DHCP packets in others VLANs will be broadcast/forwarded to other ports.

The DHCP Per Port function allows the switch to connect only one DHCP client device.

DHCP-Per-Port is configured entirely on the **Switch > Configuration > System > IP** page, IP Interfaces window.

The feature is enabled here and an IP range (pool) is entered. The "automatic" results of this action can be displayed in:

- **Switch > Configuration > System > DHCP > Server > Mode** (Global Mode – Enabled, VLAN Mode - VLAN 1 created)
- **Switch > Configuration > System > DHCP > Excluded** (Excluded range created based on range entered)
- **Switch > Configuration > System > DHCP > Pool** (Pool "DHCP_Per_Port" created based on range entered)

Actual DHCP operation is monitored as normal under **System > Monitor > DHCP**.

The DHCP Per Port pages and parameters are described below.

A-2. DHCP Per Port Mode Configuration

The DHCP Per Port function lets you assign an IP address based on the switch port the device is connected to. This will speed up installation of IP cameras, as the cameras can be configured after they are on the network. The DHCP Per Port assignment lets you know which IP was assigned to which camera.

Note: to prevent IP conflict, each switch can be allocated a different IP range.

To configure DHCP Per Port via the Web UI, navigate to the **Configuration > System > IP** menu path.

The screenshot displays the Lantronix web interface for configuring DHCP Per Port. The left sidebar shows the navigation menu with 'Configuration > System > IP' highlighted. The main content area shows the 'IP Configuration' page with the following sections:

- DNS Servers:** Four DNS Server entries, each with a dropdown menu set to 'Configured IPv4 or IPv6' and a text input field containing '8.8.8.8'. A 'DNS Proxy' checkbox is present and unchecked.
- IP Interfaces:** A section for 'DHCP Per Port' configuration, highlighted with an orange box. It includes:
 - Mode:** A dropdown menu set to 'Disabled'.
 - VLAN:** A dropdown menu set to 'VLAN 1'.
 - IP:** Two empty text input fields separated by a hyphen.
- IP Interfaces Table:** A table with columns for 'Delete', 'VLAN', 'IPv4 DHCP' (Enable, Fallback, Current Lease), 'IPv4' (Address, Mask Length), 'DHCPv6' (Enable, Rapid Commit, Current Lease), and 'IPv6' (Address, Mask Length). The first row shows VLAN 1, IPv4 DHCP disabled, Fallback 0, IPv4 address 172.27.195.90, Mask Length 24, and DHCPv6 disabled.
- Link-Local Address binding interface:** A dropdown menu set to 'VLAN 1'.
- Gateway Address binding interface:** A dropdown menu set to 'VLAN 1'.
- IP Routes Table:** A table with columns for 'Delete', 'Network', 'Mask Length', 'Gateway', and 'Next Hop VLAN'. It lists three routes:

Delete	Network	Mask Length	Gateway	Next Hop VLAN
<input type="checkbox"/>	0.0.0.0	0	172.27.195.1	0
<input type="checkbox"/>	169.254.0.0	16	172.27.195.90	0
<input type="checkbox"/>	172.27.195.0	24	172.27.195.90	0

Parameter descriptions: The DHCP Per Port parameters and buttons are described below.

DHCP Per Port Mode: at the dropdown select **Enable** or **Disable** the DHCP Per Port function globally. The default is **Disabled**.

IP: enter the IPv4 IP address range to be used when the DHCP Per Port function is enabled (e.g., 192.168.10.20 - 192.168.10.37). The DHCP Per Port IP range must be within the interface subnet. Note that DHCP Per Port with IPv6 is not supported at this time. The DHCP Per Port IP range must equal the switch port number excluding uplink ports (16).

Apply: Click to save changes to the entries. If the entries are valid, the webpage message *"Update success!"* displays. Click the **OK** button to clear the message. If any entries are invalid, an error message displays. Click the **OK** button to clear the message and enter valid values, then click the **Apply** button again.

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

To monitor DHCP Per Port status, navigate to the **Monitor > System > IP Status** menu path.

The screenshot displays the 'IP Status' page in the LANTRONIX web interface. The left sidebar shows the navigation menu with 'Monitor' and 'System' highlighted, and 'IP Status' selected. The main content area is titled 'IP Interfaces' and includes an 'Auto-refresh' checkbox. Below this, there are three tables: 'IP Interfaces', 'IP Routes', and 'Neighbour cache'. At the bottom, there is a 'DNS Server' table.

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>

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>

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

Type	IP Address	Interface
Static	8.8.8.8	

Web UI Messages

Message: *Interface xx not using DHCP*

Meaning: The Interface being configured does not have DHCP enabled and configured.

Recovery: **1.** Click the **OK** button to clear the webpage message. **2.** Enable and configure DHCP for the interface being configured. See “[DHCP Server Mode Configuration](#)” on page 35.

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. The range should be something like 192-168-1.80 - 192-168-1.85 to be valid.

Message: *The value of ‘DNS Server’ must be a valid IP address in dotted decimal notation (‘x.y.z.w’).*

Meaning: You entered an invalid IP address for the DNS Server being configured.

Recovery: **1.** Click the **OK** button to clear the webpage message. **2.** Enter a valid IP address in the format x.y.z.w per the on-screen restrictions. See “[DHCP Server Mode Configuration](#)” on page 35.

Message: *‘DHCP Interface VLAN ID’ must be an integer value between 1 and 4095.*

Meaning: You entered an invalid VLAN ID for the DHCP Interface.

Recovery: **1.** Click the **OK** button to clear the webpage message. **2.** Enter a valid VLAN ID for the DHCP Interface (1-4095). See “[DHCP Server Mode Configuration](#)” on page 35.

Message: *DHCP per Port range (192.168.1.50 - 192.168.1.66) is not equal to switch TP port number (8).*

Meaning: You entered an invalid range of IP addresses for DHCP per port.

Recovery: **1.** Click the **OK** button to clear the webpage message. **2.** Enter a valid IP range of IP addresses for DHCP per port.

Message: *Update success!*

Meaning: The update effort completed successfully.

Recovery: None required.

A-3. DHCP Per Port VLAN

The SM24TBT2DPB supports the DHCP IP Per Port function. It lets you have an IP address from a DHCP pool on a switch be statically assigned to a switchport, such that whichever device plugs into the switchport it will always be assigned that specific IP address. The IP address is configured in the interface config settings. Note that this is binding an IP address to an interface, not to a MAC address, which is the classic binding technique found on most switches. (Added at FW VB7.20.0140.)

Appendix B. MRP Pre-Requisites and Application Examples

You can configure Media Redundancy Protocol (MRP) parameters via the Web UI at Configuration > MRP and monitor them at Monitor > MRP, or via the CLI. See the *CLI Reference* for Command Line operation.

According to ANSI, [IEC 62439-2 Ed. 1.0 b:2010](#) is applicable to high-availability automation networks based on [ISO/IEC 8802-3](#) / [IEEE 802.3 Ethernet technology](#). It specifies a recovery protocol based on a ring topology, designed to react deterministically on a single failure of an inter-switch link or switch in the network, under the control of a dedicated Media Redundancy Manager (MRM) node.

Media Redundancy Protocol per IEC 62439-2 is an interoperable ring technology designed to allow a switch to connect onto a universal redundant high speed ring. MRP is self-healing and self-adjusting, requiring no operator interaction. MRP is based on the concept of standby connections for seamless redundancy.

B-1. MRP Description

1. MRP operates at the MAC Layer of the Ethernet Switch.
2. The Ring Manager is called the Media Redundancy Manager (MRM).
3. Ring Clients are called Media Redundancy Clients (MRCs).
4. MRM and MRC ports support three Status Types:
 - a. *Disabled* ring ports drop all the received frames.
 - b. *Blocked* ring ports drop all the received frames except the MRP control frames.
 - c. *Forwarding* ring ports forward all the received frames.
5. Ring Reconfiguration speed is 200 ms for 50 switches on average.
6. The MRM continuously sends Watchdog Packets into the ring network to verify communication between ring points.
7. During normal operation, no packets are transmitted over the redundant link.
8. When the MRM no longer receives the Watchdog Packets it sent out, the redundant path is immediately activated, and it becomes the primary layer 2 packet path.
9. When the failed link is restored:
 - a. The MRM switches back to normal operation and the first Path becomes the primary path again.
 - b. You can configure a period of time before the MRM switches back to the primary path (to prevent the circuit from flapping if it is not stable).

B-2. MRP Operation

Normal operation: the network works in the *Ring-Closed* status. In this status, one of the MRM ring ports is blocked, while the other is forwarding. Conversely, both ring ports of all MRCs are forwarding. Loops are avoided because the physical ring topology is reduced to a logical stub topology.

Failure mode: the network works in the *Ring-Open* status. For instance, in case of failure of a link connecting two MRCs, both ring ports of the MRM are forwarding. The MRCs adjacent to the failure have a blocked and a forwarding ring port; the other MRCs have both ring ports forwarding. The physical ring topology is also a logical stub topology in the Ring-Open status.

B-3. Related Devices

MRP is implemented at FW v7.10.2368 for SISPM1040-384-LRT-C, SISPM1040-362-LRT, SISPM1040-582-LRT, SISGM1040-284-LRT, SISPM1040-3166-L, and SISPM1040-3248-L.

B-4. MRP Sample Setup

The example below shows SISPM1040-384-LRT-C switches (one MRM and five MRCs).

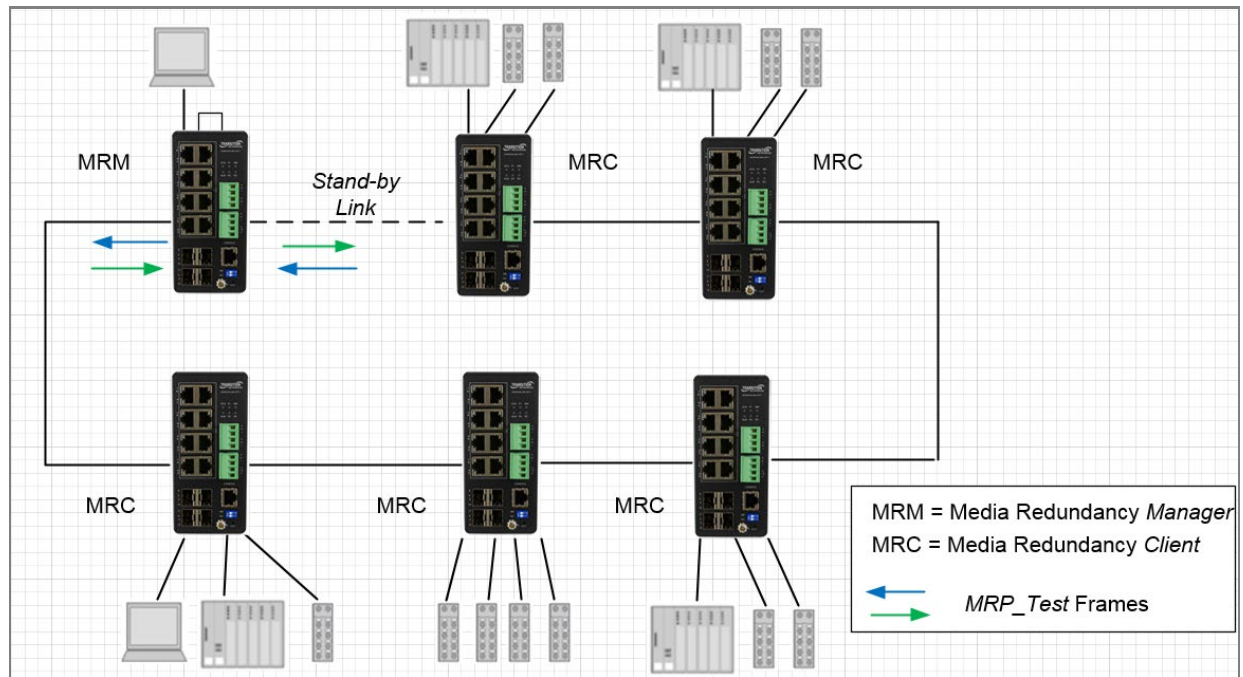


Figure: MRP Sample Setup

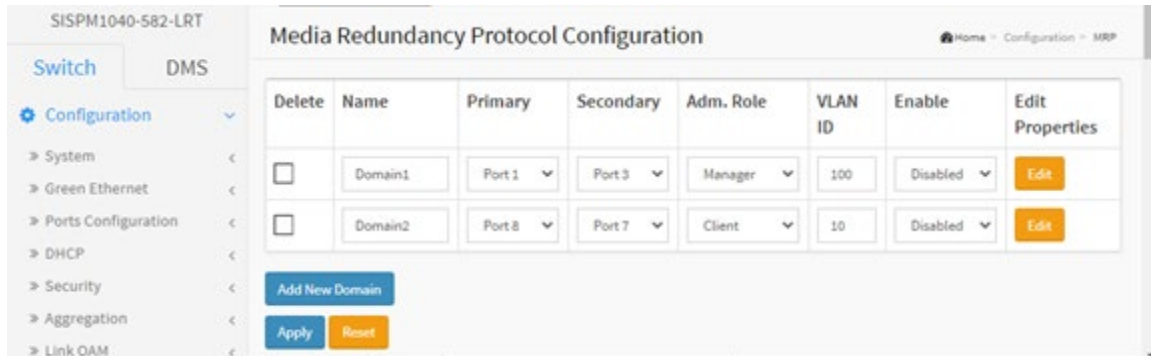
B-5. MRP Pre-Requisites (General)

The following are required to perform MRP setups.

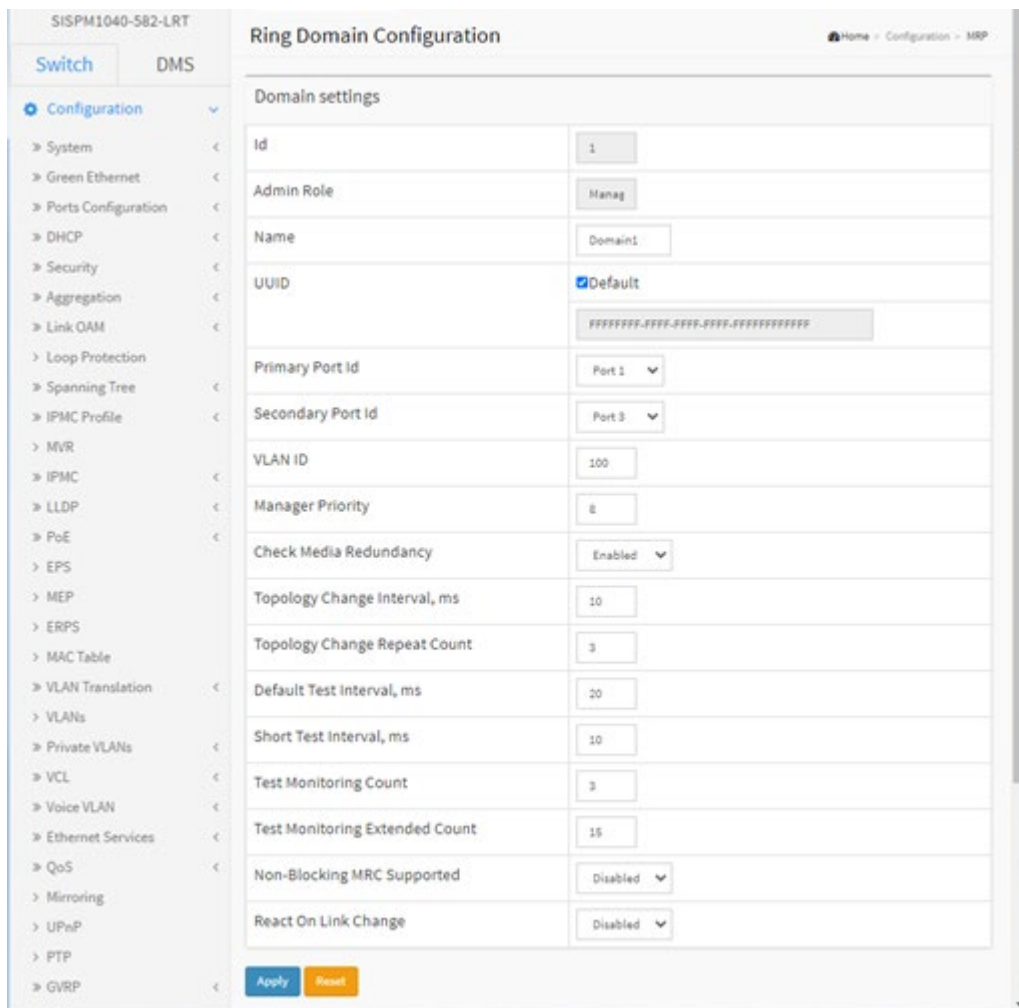
1. Spanning Tree must be disabled at Configuration > Spanning Tree > CIST Port.
2. Other Ring technologies must also be disabled (G.8031 EPS, G.8032 ERPS, Rapid-Ring, Ring-To-Ring, etc.).
3. Only one MRM (Manager) is supported per ring.
4. Other pre-requisites may apply to the specific examples below.
5. One Manager Admin Role is supported.

B-6. MRP Web UI Configuration

1. Navigate to Switch > Configuration > MRP to initially configure two MRP Domains:



2. Click Apply to save, and then click the Edit button to configure the first MRP Domain (Domain1).



3. Edit the Domain Settings as required. Click Apply to save; the message "Domain is enabled" displays. Click OK to clear the webpage message. The "Media Redundancy Protocol Configuration" page displays again.

4. Click the Edit button to display the second MRP Domain (Domian2).

The screenshot displays the 'Ring Domain Configuration' page. On the left is a navigation menu with 'Switch' and 'DMS' tabs, and a 'Configuration' section expanded to show various settings like System, Green Ethernet, Ports Configuration, DHCP, Security, Aggregation, Link OAM, Loop Protection, Spanning Tree, IPMC Profile, MVR, IPMC, LLDP, PoE, EPS, MEP, ERPS, MAC Table, VLAN Translation, and VLANs. The main content area is titled 'Ring Domain Configuration' and shows a 'Domain settings' table. The table has the following fields and values:

Domain settings	
Id	2
Admin Role	Client
Name	Domain2
UUID	<input checked="" type="checkbox"/> Default FFFFFFFF-FFFF-FFFF-FFFFFFFF
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

At the bottom of the configuration area are 'Apply' and 'Reset' buttons.

5. Edit the Domain Settings as required. Click Apply to save; the message “Domain is enabled” displays. Click OK to clear the webpage message.

6. When the “Media Redundancy Protocol Configuration” page displays again, verify the settings.

Example 1: MRP Manager Re-Config (Web UI)

This application example shows the MRP Manager reconfiguring the traffic path based on the client state.

Sample Setup: This setup includes one device with MRP enabled and has an admin role set as Manager and three clients connected in a ring topology. See the MRP Sample Setup diagram below.

Procedure:

1. Disable any other Ring technologies and disable Spanning-tree at Configuration > Spanning Tree > CIST Port.
2. For the device acting as MRM click 'Add New Domain' button to configure the MRP instance in the 'Media Redundancy Protocol Configuration' page.
3. Assign the first ring port under 'Primary' and the second ring port under 'Secondary'.
4. Set the Administrative Role to 'Manager' under 'Adm. Role'. Assign any VLAN ID from 2-4094.
5. Set the instance to 'enable'.
6. Go to the 'Ring Domain Configuration (Manager Role)' page and set a Domain name.
7. Tick the Default box for UUID.
8. Select the Primary and Secondary Port IDs.
9. Enable 'Check Media Redundancy'.
10. Leave other settings as default.
11. For the devices acting as MRCs in the 'Ring Domain Configuration (Client Role)' page assign the first Primary and Secondary Port IDs for the ring ports.
12. Enter the same VLAN ID as in step 4 above.
13. Link Down Interval should be 20ms. Link Up Interval should be 20ms. Link change count should be 4.
14. 'BLOCKED State Supported' must be enabled. By default, one ring port will be disabled for loop-free communication.
15. Configure ring ports to Hybrid mode on the VLAN Configuration page. Assign the VLAN ID as configured in step 4.
16. Send bi-directional traffic tagged with the VLAN ID set in step 4 above.
17. Create a failure on any one of the client ring ports by disconnecting the cable. The MRM should reconfigure the path within 200<500ms. The Redundancy manager will send test frames marked with a unique MAC with OUI of 00-15-4E and forwarded by the MRCs to the opposite ring ports per the interval specified. The disabled ring port should now be enabled, creating a new loop-free topology.
18. There should be no traffic loss after path reconfiguration.

Example 2: Non-Blocking MRC State Recognized by MRM (Web UI)

This application example shows a Non-blocking MRC state is recognized by the MRM.

Setup: This setup and steps 1-18 in Example 1 above are required.

Procedure:

1. Disable any other Ring technologies and disable Spanning-tree at Configuration > Spanning Tree > CIST Port.
2. Disable 'BLOCKED State Supported'.
3. Configure ring ports to Hybrid mode on the VLAN Configuration page. Assign the VLAN ID as configured in step 4 of Example 1.
4. Send bi-directional traffic tagged with the VLAN ID set in the previous step.
5. Create a failure on any one of the client ring ports by disconnecting the cable. The client ring ports will be in a forwarding state instead of blocking. The MRM should reconfigure the path within 200<500ms. The MRM will send test frames marked with a unique MAC with OUI of 00-15-4E and forwarded by the MRCs to the opposite ring ports per the interval specified.
6. Verify the MRC reacts to the reconfiguration frames as received by the MRM. The link down on the client ring port should be detected by the MRC.
7. There should be no traffic loss after path reconfiguration.

Example 3: MRP Roles Set in Web UI

Setup: This setup shows that the MRP can have both Manager and Undefined roles.

Procedure:

1. Disable any other Ring technologies and disable Spanning-tree at Configuration > Spanning Tree > CIST Port.
2. 'BLOCKED State Supported' should be enabled. By default, one ring port will be disabled for loop-free communication.
3. Configure ring ports to Hybrid mode on the VLAN Configuration page. Assign the VLAN ID as set in step 4 of Example 1.
4. Send bi-directional traffic tagged with the VLAN ID set in the previous step.
5. Create a failure on any one of the client ring ports by disconnecting the cable. The MRM should reconfigure the path within 200<500ms. The Redundancy manager will send test frames marked with a unique MAC with OUI of 00-15-4E and forwarded by the MRCs to the opposite ring ports per the interval specified. The disabled ring port should now be enabled and creates a new loop-free topology.
6. There should be no traffic loss after path reconfiguration.
7. On a second client set the 'BLOCKED State Supported' option to disable. The ring port will now be in a forwarding state. Cause a failure on the ring port of another device that has its blocked state disabled.
8. Verify that frames are forwarded and received by the MRC with blocking enabled. There should be no traffic loss after path reconfiguration.

Appendix C – G.8032 Major and Sub Rings Configuration

C-1. 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 “3-17 ERPS” on page 201 for general G.8032 ERPS configuration information.

C-2. 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.

C.3. IP Addresses

The sample configurations below use these IP addresses:

SISPM1040-582-LRT : 192.168.1.85

SISPM1040-384-LRT-C : 192.168.1.95

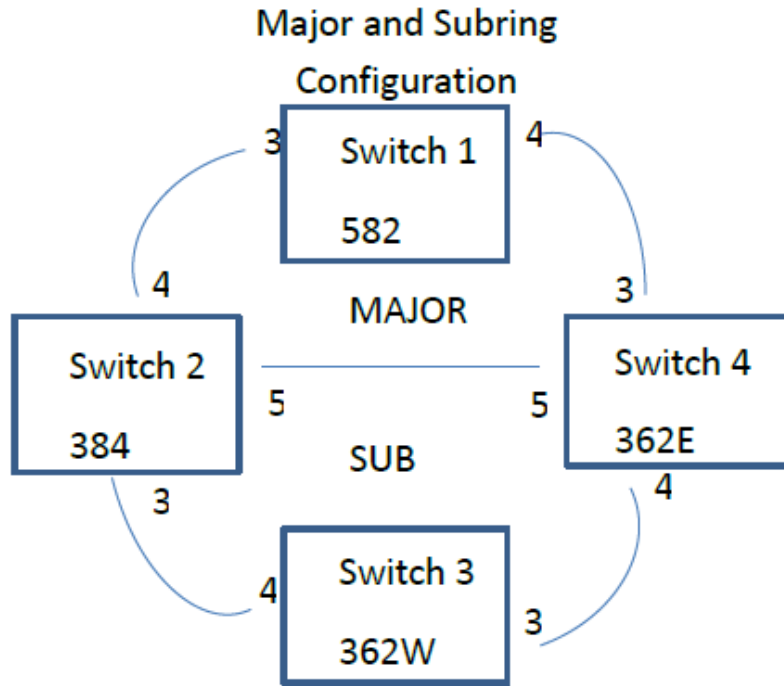
362W : 192.168.1.125

362E : 192.168.1.135

C-4. 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

<u>Major</u>	<u>Sub</u>	<u>Major</u>	<u>Sub</u>	<u>Major</u>	<u>Sub</u>
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 programmed 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	
<input checked="" type="checkbox"/>	7	1f/sec	<input type="checkbox"/>	<input checked="" type="checkbox"/>	7	Multi	R-APS	1	

[Fault Management](#) [Performance Monitoring](#)

ERPS

ERPS ID	RPL	Port 0 Port	Port 1 VLAN	Port 0 SF	Port 1 SF	Port 0 APS	Port 1 APS	Ring
1	1	2	5	1	2	1	2	
Major	Owner	0						

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 programmed 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
<input checked="" type="checkbox"/>	7	1 f/sec	<input type="checkbox"/>	<input checked="" type="checkbox"/>	7	Multi	R-APS	1

Fault Management
Performance Monitoring

ERPS

ERPS ID	Port 0 Port	Port 0 VLAN	Port 1	Port 0 SF	Port 1 SF	Port 0 APS	Port 1 APS	Ring	RPL
1	3	5	2	3	2	3	2	Major	Neighbor
2	1	5	0	1	0	1	0	Sub	Neighbor

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 programmed 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	
<input checked="" type="checkbox"/>	7	1 f/sec	<input type="checkbox"/>	<input checked="" type="checkbox"/>	7	Multi	R-APS	1	

ERPS

ERPS ID	Port 0 Port	Port 0 VLAN	Port 1	Port 0 SF	Port 1 SF	Port 0 APS	Port 1 APS	Ring	RPL
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 prograded 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	
<input checked="" type="checkbox"/>	7	1 f/sec	<input type="checkbox"/>	<input checked="" type="checkbox"/>	7	Multi	R-APS	1	

Fault Management Performance Monitoring

ERPS

ERPS ID	Port 0	Port 1	Port 0 SF	Port 1 SF	Port 0 APS	Port 1 APS	Ring	RPL	Port
1	1	3	1	3	1	3	Major	None	5
2	2	0	2	0	2	0	Sub	None	5

Interconnect Yes, Major 1

C-5. 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<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
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
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
```

```
←-----
```

Cable Disconnect

```
←-----
```

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
```

```
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
```

←-----
Cable Disconnect

C-6. Config files

running-config_192.168.1

```
hostname SISPM1040-362-LRT-E
username admin privilege 15 password encrypted
feec1d1085ff075fd03b1d2d5ab4c0befbfff0917079c8abb3a77338041bf5d6e1771bdbbd1a317ea2f42fc2aacc8c5
0a8e667456d7c04099f74f8ef9dcc0fbd4
!
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
7073dec86c15b8a9907bb4106ef783adde46bd5b5969cc68fb55b430336bd7c80d5ded65d2fdb39abe81cc9caa5a93
620f270c21bca86e776cee9c5588bfb8c7
username superuser privilege 15 password encrypted
4643fdc71f39fd4cb955943fcdf89faca81bc650fbaeebe25a796662d5c225bf0d5ded65d2fdb39abe81cc9c514497
e27799560e488713aabaac4f167e7732ca
!
vlan 1
!
!
!
!
ip route 0.0.0.0 0.0.0.0 192.168.1.254
ntp automatic
ntp server 1 ip-address ntp1.lantronixn.com
ntp server 2 ip-address ntp2.lantronix.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
6593186b999f348becd63b8612ac561c114250a1a00bd38f6afb5378acb6d08c1864c59b092b0e2b29ba4f1d559166
800846cbc52c4558a90e4cdf95d3cfcbf4
username dennis privilege 5 password encrypted
a92a5dbf4fcd2e13d35adb36d2418476e907de19a641fa7baf80b1abb2bacd8ee5dbdd44e246b88be1636df6b8769a
f790aa8721622481085e33c32e6e119dbd
!
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
6158ed7daf39d06ded0e7c4828c3b15bb4c40673bd445afcd643295925ae425d9611d1cbe872708237571aacc7b923
7f33b01ae6866e2484009edfelfa0bf56f
!
vlan 1
!
!
!
!
ip route 0.0.0.0 0.0.0.0 192.168.1.254
tzidx 0
exec-timeout autologout 0
snmp-server location DT Lab Ring
system name SISPM1040-362-LRT-W
system location DT Lab Ring
system description Managed Hardened PoE+ Switch, (4) 10/100/1000Base-T PoE+ Ports + (2)
10/100/1000Base-T Ports + (2) 100/1000Base-X SFP Ports
!
interface GigabitEthernet 1/1
!
interface GigabitEthernet 1/2
!
interface GigabitEthernet 1/3
no spanning-tree
switchport trunk allowed vlan 5,20
switchport trunk vlan tag native
switchport mode trunk
poE mode disable
!
interface GigabitEthernet 1/4
no spanning-tree
switchport trunk allowed vlan 5,20
switchport trunk vlan tag native
switchport mode trunk
poE mode disable
!
interface GigabitEthernet 1/5
!
interface GigabitEthernet 1/6
!
interface GigabitEthernet 1/7
!
interface GigabitEthernet 1/8
!
interface vlan 1
ip address 192.168.1.125 255.255.255.0
ip dhcp server
!
mep 1 down domain port level 4 interface GigabitEthernet 1/3
mep 1 mep-id 7
mep 1 vid 20
mep 1 peer-mep-id 6 mac 00-C0-F2-53-EF-FD
mep 1 cc 7
mep 1 aps 7 raps
mep 2 down domain port level 4 interface GigabitEthernet 1/4
mep 2 mep-id 8
mep 2 vid 20
mep 2 peer-mep-id 3 mac 00-40-C7-1C-C7-2F
mep 2 cc 7
mep 2 aps 7 raps
erps 1 sub port0 interface GigabitEthernet 1/3 port1 interface GigabitEthernet 1/4
```

```
erps 1 mep port0 sf 1 aps 1 port1 sf 2 aps 2
erps 1 rpl owner port1
erps 1 vlan 5
!
spanning-tree aggregation
  spanning-tree link-type point-to-point
!
!
line console 0
!
line vty 0
!
line vty 1
!
line vty 2
!
line vty 3
!
line vty 4
!
line vty 5
!
line vty 6
!
line vty 7
!
line vty 8
!
line vty 9
!
line vty 10
!
line vty 11
!
line vty 12
!
line vty 13
!
line vty 14
!
line vty 15
!
!
end
```


**Lantronix Corporate Headquarters**

48 Discovery, Suite 250
Irvine, CA 92618, USA
Toll Free: 800-526-8766
Phone: 949-453-3990
Fax: 949-453-3995

Technical Support

Online: <https://www.lantronix.com/technical-support/>

Sales Offices

For a current list of our domestic and international sales offices, go to the Lantronix web site at www.lantronix.com/about/contact.