



SISPM1040-384-LRT-C and SISPM1040-362-LRT Managed Hardened Gigabit Ethernet PoE+ Switches

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, 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.	Comments
9/13/21	H	FW v7.20.0075: add API command get_config_action_status. Fix API cannot delete old interface vlan. Add Reboot System "When DI was changed to abnormal". Fix DDM info update issue and PoE Force mode cannot be saved issue. Fix DI/DO after triggering DI reboot system event, Server may not receive syslog event. Fix PMD auto negotiation advertised capability info is wrong in LLDP packet of fiber ports. Add 'System DO Relay Open Close' to MIB. Fix port link up when inserting TN-EOT-xx copper SFP module.
9/28/22	J	FW v7.20.0121: Add Reboot System "When DI was changed to abnormal". Fix DDM info update issue and PoE Force mode save issue. Initial Lantronix rebrand. Update RADIUS server and add two new DMS icons. 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 Client support and Lantronix Provisioning Manager (LPM). Fix ERPS Failover time bug. Update DMS Map View section.
10/10/23	K	FW v7.20.0190: Add PercepXion support and support API in https. Fix issues with Device Key, Firmware Version update, and Serial # for PercepXion and MAC address for LPM. Update features section. Add LEVEL Technical Support. Update SSH and fix FW upgrade. Add PoE Status to Device Telemetry Data. Add TLSv1.2 ciphers. Add STP 'Hello Time' description. Add public OIDs 1.3.6.1.2.1.4.20.1.2 and 1.3.6.1.2.1.4.20.1.3). Remove file name "mach10_combined.crt" from Config download, upload, activate, and delete pages. Automatically save Config changes to Start-Up Config in PercepXion server. Update LACP on Air section. Automatically save Configuration Update from PercepXion Explore tab and configuration of all element changes to Start-Up Config.

Safety Warnings and Cautions

These products are not intended for use in life support products where failure of a product could reasonably be expected to result in death or personal injury. Anyone using this product in such an application without express written consent of an officer of Lantronix does so at their own risk and agrees to fully indemnify Lantronix for any damages that may result from such use or sale.



Attention: This product, like all electronic products, uses semiconductors that can be damaged by ESD (electrostatic discharge). Always observe appropriate precautions when handling.



Note: Emphasizes important information or calls your attention to related features or instructions.



Caution: Alerts you to a potential hazard that could cause loss of data or damage the system or equipment.



Warning: Alerts you to a potential hazard that could cause personal injury.

Contents

Safety Warnings and Cautions	3
Chapter 1. Introduction.....	9
1-1 About This Manual	9
1-2 Related Documentation	9
1-3 Product Descriptions	9
1-5 Ordering Information.....	10
1-6 Web-based Management	11
1-7 Initial Configuration	11
1-8 Web Navigation	12
1-9 First Time Wizard.....	14
1-10 Menu System.....	17
Chapter 2. System Configuration	18
2-1 System.....	18
2-1.1 Information	18
2-1.2 IP.....	19
2-1.3 NTP	24
2-1.4 Time.....	26
2-1.5 Log	28
2-1.6 Digital I/O.....	29
2-1.7 Alarm Notification	30
2-2 Green Ethernet.....	34
2-2.1 Port Power Savings.....	34
2-3 Ports Configuration.....	36
2-3.1 Ports	36
2-3.2 Ports Description.....	38
2-4 DHCP.....	39
2-4.1 Server.....	39
2-4.2 Snooping	46
2-4.3 Relay	48
2-5 Security.....	50
2-5.1 Switch.....	50
2-5.2 Network	78
2-5.3 AAA	109
2-6 Aggregation	114
2-6.1 Static	114
2-6.2 LACP	116
2-6.2 LACP on Air.....	118
2-7 Link OAM.....	120
2-7.1 Port Settings.....	120
2-7.2 Event Settings	122
2-8 Loop Protection	124
2-9 Spanning Tree.....	126
2-9.1 Bridge Settings.....	126
2-9.2 MSTI Mapping.....	129
2-9.3 MSTI Priorities.....	131
2-9.4 CIST Ports.....	133
2-9.5 MSTI Ports	135
2-10 IPMC Profile	137
2-10.1 Profile Table.....	137
2-10.2 Address Entry.....	139
2-11 MVR.....	140
2-12 IPMC.....	143
2-12.1 IGMP Snooping.....	143
2-12.2 MLD Snooping	151

2-13 LLDP	159
2-13.1 LLDP	159
2-13.2 LLDP-MED	162
2-14 PoE	167
2- 14.1 Configuration	167
2- 14.2 Power Delay	170
2- 14.3 Schedule Profile	171
2- 14.4 PoE Auto Power Reset (Auto Checking)	173
2- 14.5 Chip Reset Schedule	175
2-15 EPS	176
2-16 MEP	180
Instance Data	181
Instance Configuration	182
2-17 ERPS	186
2-18 MAC Table	191
2-19 VLAN Translation	193
2- 19.1 Port to Group Mapping	193
2- 19.2 VID Translation Mapping	195
2-20 VLANs	197
2-21 Private VLANs	200
2-21.1 Membership	200
2-21.2 Port Isolation	202
2-22 VCL	203
2-22.1 MAC-based VLAN	203
2-22.2 Protocol -based VLAN	205
2-22.3 IP Subnet-based VLAN	208
2-23.1 Configuration	209
2-23.2 OUI	211
2-24 Ethernet Services	212
2-24.1 Ports	212
2-24.2 Bandwidth Profiles	215
2-24.3 EVCs	217
2-24.4 ECEs	220
2-25 QoS	227
2-25.1 Port Classification	227
2-25.2 Port Policing	230
2-25.4 Port Scheduler	232
2-25.5 Port Shaping	234
2-25.6 Port Tag Remarking	236
2-25.7 Port DSCP	239
2-25.8 DSCP-Based QoS	241
2-25.9 DSCP Translation	243
2-25.10 DSCP Classification	245
2-25.11 QoS Control List	247
2-25.12 Storm Control	251
2-26 Mirroring and Remote Mirroring	252
2-27 UPnP	256
2-28 PTP	257
2-29. GVRP	262
2-29.2 Port Config	264
2-30. sFlow	265
2-31 UDLD	267
2-32 Rapid Ring	269
2-33 PercepXion and LPM	271
Supported Firmware Versions	271
PercepXion Agent Configuration	271
PercepXion Upload	274
2-34 MRP	275
2-35 SMTP	278

Chapter 3. Monitor	280
3-1 System.....	280
3-1.1 Information	280
3-1.2 IP Status	282
3-1.3 Log	284
3-1.4 Detailed Log	286
3-2 Green Ethernet.....	287
3-2.1 Port Power Savings.....	287
3-3 Ports	288
3-3.1 Traffic Overview.....	288
3-3.2 QoS Statistics.....	290
3-3.3 QCL Status.....	291
3-3.4 Detailed Port Statistics	293
3-3.5 SFP Information	295
3-3.6 SFP Detail Info	297
3-4 Link OAM	299
3-4.1 Statistics	299
3-4.2 Port Status.....	301
3-4.3 Event Status	303
3-5 DHCP.....	306
3-5.1 Server.....	306
3-5.2 Snooping Table.....	312
3-5.3 Relay Statistics.....	313
3-5.4 Detailed Statistics.....	315
3-6 Security.....	317
3-6.1 Access Management Statistics	317
3-6.2 Network	318
3-6.3 AAA	331
3-6.4 Switch.....	338
3-7 Aggregation	345
3-7.1 Status	345
3-7.2 LACP	346
3-8 Loop Protection	349
3-9 Spanning Tree	350
3-9.1 Bridge Status.....	350
3-9.2 Port Status.....	353
3-9.3 Port Statistics	354
3-10 MVR.....	355
3-10.1 Statistics.....	355
3-10.2 MVR Channels Groups	356
3-10.3 MVR SFM Information.....	357
3-11 IPMC.....	358
3-11.1 IGMP Snooping	358
3-11.2 MLD Snooping.....	362
3-12 LLDP	366
3-12.1 Neighbor.....	366
3-12.2 LLDP-MED Neighbor	369
3-12.3 PoE.....	373
3-12.4 EEE	374
3-12.5 Port Statistics	376
3-13 Ethernet Services	378
3-13.1 EVC Statistics.....	378
3-14 PTP.....	380
3-15 PoE	387
3-16 MAC Table.....	389
3-17 VLANs.....	391
3-17.1 Membership.....	391
3-17.2 Port.....	393

3-18 MRP.....	396
3-18.1 Media Redundancy Protocol Status.....	396
3-19 VCL.....	398
3-19.1 MAC-based VLAN.....	398
3-18.2 Protocol-based VLAN.....	399
3-18.3 IP Subnet-based VLAN.....	402
3-19 sFlow.....	403
3-20 UDLD.....	405
Chapter 4. Diagnostics.....	406
4-1 Ping.....	406
4-2 Ping6.....	408
4-3 Cable Diagnostics.....	410
4-4 Traceroute.....	412
4-5 Link OAM.....	414
4-5.1 MIB Retrieval.....	414
Chapter 5. Maintenance.....	415
5-1 Restart Device.....	415
5-2 Reboot Schedule.....	416
5-3 Factory Defaults.....	417
5-4 Firmware.....	418
5-4.1 Firmware Upgrade.....	418
5-4.2 Firmware Selection.....	420
5-5 Configuration.....	422
5-5.1 Save running-config to startup-config.....	422
5-5.2 Download.....	423
5-5.3 Upload.....	425
5-5.4 Activate.....	427
5-5.5 Delete.....	430
5-6 Server Report.....	431
Chapter 6. DMS (Device Management System).....	432
6-1 DMS Introduction.....	432
6-2 About DMS Mode.....	432
6-4 DMS Icons and Controls.....	433
6-4-1 Topology View Icons / Controls.....	434
6-4-2 Device Consoles (Dashboard / Notification / Monitor).....	434
6-5 DMS Mode.....	436
6-6 Google Map API Key Configuration.....	437
6.6.1 Google Map API Key Configuration.....	437
6.6.2 Get the Google Map API Key.....	437
6-7 Device List.....	438
6.8 DMS > Maintenance > Floor Image.....	441
6.9 DMS > Maintenance > Diagnostics.....	444
Chapter 7 DMS > Graphical Monitoring.....	446
7-1 Topology View.....	446
7-2 Floor View.....	451
7-3 Map View.....	453
Chapter 8. DMS > Maintenance.....	455
8-1 Floor Image.....	455
8-2 Diagnostics.....	457
8-3 Traffic Monitor.....	459
DMS Firmware Upgrade Procedure.....	463
8-4 Troubleshooting DMS.....	465

Appendix A: Rapid Ring Operation	466
A-1 Rapid Ring Operation.....	466
A-1-1 Single Ring	466
A-1-2 Ring to Ring	468
A-1-3 Dual Ring	469
A-1-4 Rapid Chain	470
A-1-5 Hardware Setting and Status for Ring	471
A-1-6 RM and RC LED Descriptions	472
Appendix B: DHCP Per Port.....	473
Appendix C: MRP Pre-Requisites and Application Examples	477
MRP Description	477
MRP Operation	477
Related Devices.....	478
MRP Sample Setup	478
MRP Pre-Requisites (General).....	478
MRP Web UI Configuration	479
Appendix D: G.8032 Major and Sub Rings Configuration	483
Introduction	483
Basic Concepts	483
IP Addresses.....	483
Sample Configuration	484
Testing	489
Config files	491

Chapter 1. Introduction

1-1 About This Manual

This manual describes how to configure, monitor, diagnose, and maintain the SISPM1040-384-LRT-C and the SISPM1040-362-LRT via the Web UI using the RJ-45 serial interface and Ethernet ports. The SISPM1040-362-LRT and SISPM1040-384-LRT-C differ mainly in port count; differences are noted throughout this manual.

1-2 Related Documentation

These manuals give specific information on how to use the switch:

- Quick Start Guide, SISPM1040-384-LRT-C & -362-LRT, 33726
- Install Guide, SISPM1040-384-LRT-C & -362-LRT, 33727
- CLI Reference, SISPM1040-384-LRT-C & -362-LRT, 33729
- API User Guide for SISPM1040-384-LRT-C and -362-LRT, 33824
- Release Notes (version specific)

For Lantronix Drivers, Firmware, Manuals, Product Notifications, Warranty Policy & Procedures, etc. go to the Lantronix [Technical Resource Center](#).

1-3 Product Descriptions

The SISPM1040-384-LRT-C is a managed PoE+ switch suitable for connecting and powering devices in hardened environments. The SISPM1040-384-LRT-C can supply up to 30 Watts per port on all **8 ports** simultaneously. The SISPM1040-362-LRT can supply up to 30 Watts per port on all **4 ports** simultaneously.

Both switches include 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.

1-4 Features

- Device Management System (DMS)
- SSH/SSL/SCP secured management
- SNMP v1/v2c/v3
- PoE Port Config, Auto Power Reset, DHCP per Port, PoE Scheduling
- MRP (Media Redundancy Protocol)
- IGMP and MLD v1/v2/v3 Snooping
- ITU/T G.8031 EPS and G.8032 ERPS
- RADIUS and TACACS+ authentication
- PTP (Precision Time Protocol)
- PercepXion and LPM support
- Complies to IEEE 802.3at, IEEE 802.3af PoE
- DHCP Relay (Option 82)
- ACL and QCL for traffic filtering
- 802.1d (STP), 802.1w (RSTP), 802.1s (MSTP)
- LACP and static link aggregation
- Q-in-Q double tag VLAN
- GVRP dynamic VLAN
- IPv4/IPv6 dual stack management
- Rapid Ring, Ring to Ring, Dual Ring, Rapid Chain

1-5 Ordering Information

SKU	Description
SISPM1040-362-LRT	Managed Hardened PoE+ Switch; provides (4) 10/100/1000Base-T PoE+ + (2) 10/100/1000Base-T RJ-45 + (2) 100/1000Base-X SFP Slots.
SISPM1040-384-LRT-C	Managed Hardened PoE+ Switch; provides (8) 10/100/1000Base-T PoE+ RJ45 ports + (4) 100/1000Base-X SFP slots and one RJ45 Console port.
Optional Accessories (sold separately)	
PercepXion	Centralized cloud-based Management Software for PoE Switches, Remote Environment Management (REM) and IoT Gateway products. PercepXion is available as a cloud-based SAAS or On-premise. Select an annual subscription model.
SFP Modules	See Lantronix full line of SFP transceivers on our SFP webpage .
25104	Industrial Power Supply; Input: 88-264 VAC, 124-370 VDC; Output: 48~55 VDC, 5.0A, 240 Watts
25160	Industrial Power Supply; Input 90-264 VAC, 127-370 VDC; Output: 48 ~ 55 VDC, 10A, 480 Watts
PS-DC-DUAL-5624T	Industrial Power Supply; Input: 100-240 VAC, Dual 56VDC + 24V output
WMBH-01	Wall Mount Bracket
DRBH-01	Din Rail Bracket
EDCA-DIO-01	Enclosure Door Contact Alarm
OCA-P181610	18x16x10" Polycarbonate Enclosure

Services (order separately)

LS-CFCLD-1	PercepXion Cloud 1-Year Renewal
LS-CFCLD-3	PercepXion Cloud 3-Year Renewal
LS-CFCLD-5	PercepXion Cloud 5-Year Renewal
LEVEL-2-SERVICES-1	Technical Services with a technical account specialist, including LEVEL 1 Service, 1-Year. Add-On.
LEVEL-2-SERVICES-3	Technical Services with a technical account specialist, including LEVEL 1 Service, 3-Year. Add-On.
LEVEL-2-SERVICES-5	Technical Services with a technical account specialist, including LEVEL 1 Service, 5-Year. Add-On.

1-6 Web-based Management

The web user interface (Web UI) lets you quickly and easily configure and monitor all switch settings and status from any switch port.

1-7 Initial Configuration

The switch default values are:

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 initially configured you can browse it. For instance, type 192.168.1.77 in the address row in a web browser; the login page displays prompting you to enter a Username and Password

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

When you login to the switch Web UI, you can use either IPv4 or IPv6 to login.

To optimize the display effect, we recommend you use Microsoft IE 6.0 above, Netscape v7.1 above or Firefox v1.00 above and have 1024x768 resolution. The switch supports neutral web browser interface.

Note: With the DHCP function enabled, if you do not have a DHCP server to provide IP addresses to the switch, use default IP address 192.168.1.77.

The login page is shown below:



: Click to Show the Login text as entered. Added at FW v7.20.0190.



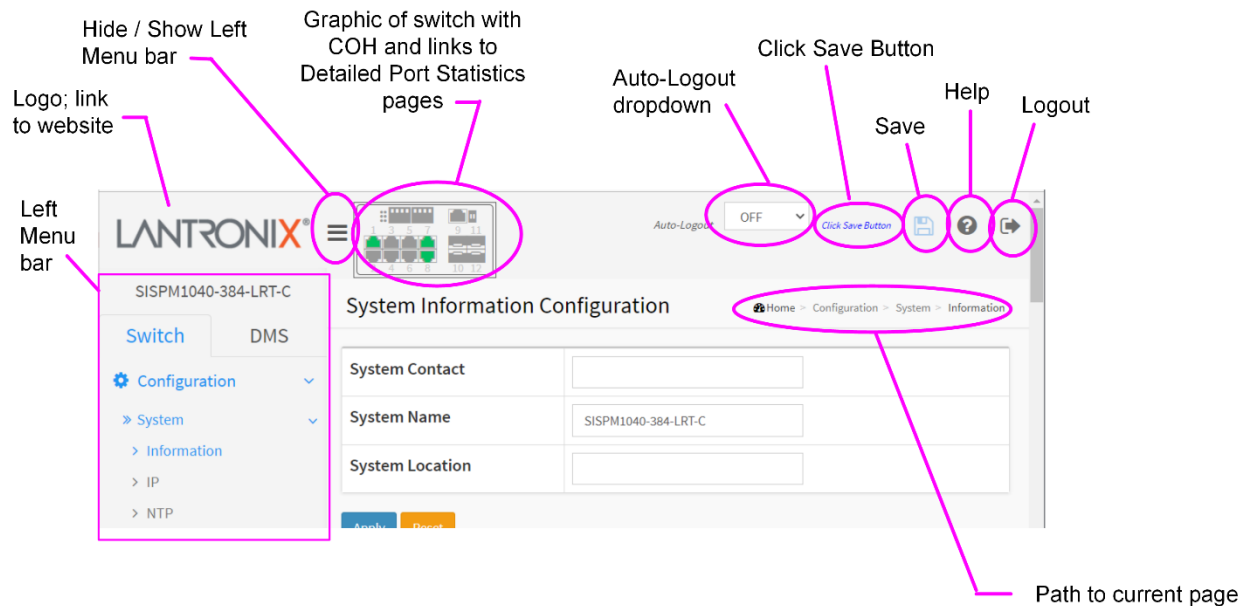
: Click to Hide the Login text as entered (default). Added at FW v7.20.0190.

On successful login, the startup page displays (Switch > Monitor > System > Information). We suggest changing the default credentials before deploying in the network.

Webpage controls are shown and described below.

1-8 Web Navigation

The Web UI navigation controls are shown below.



Click Save Button: Click Save Button: when a webpage setting is changed, the “Click Save Button” automatically pops up (added at FW v 7.10.2368).

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 v7.10.2496).

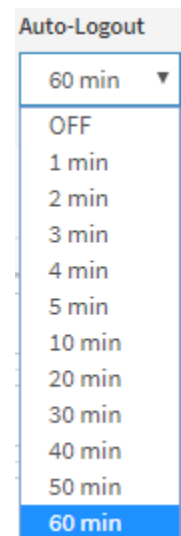
Auto-Logout Timeout: After you change the Auto-Logout timeout and then log out and log back in, the Auto-Logout timeout setting will be the setting saved to the start-up config file.

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

To save the timeout change into startup-config, you must do a save to startup-config and then reboot the switch.

In summary:

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



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

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

1-9 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 vB.7.20.0106. Use the following procedure:

Step 1: Change default password

Enter a new password and then enter it again. Starting at FW v1.02.1471: 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, IP ADDRESS, DATE & TIME, and INFORMATION. The "PASSWORD" step is highlighted. Below the title, there are two input fields: "New password" and "Repeat new password". Below these fields, there is a list of password requirements: "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, but the "IP ADDRESS" step is highlighted. It shows "Interface VLAN ID" set to "1". There are two radio button options: "Obtain IP address via DHCP" (unselected) and "Set IP address manually" (selected). Below these are input fields for "IP address" (192.168.1.77), "Subnet mask" (255.255.255.0), "Default router" (192.168.1.254), and "DNS". A blue "Previous" button and a blue "Next" button 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, both titled "Set IP address". Both have the same progress bar at the top with "IP ADDRESS" highlighted. The left screenshot shows "Obtain IP address via DHCP" selected (radio button), and "Set IP address manually" selected (radio button). Below are input fields for "IP address" (192.168.1.77), "Subnet mask" (255.255.255.0), and "Default router" (192.168.1.254). There is also a "DNS" field. A blue "Previous" button and a blue "Next" button are at the bottom. The right screenshot shows "Obtain IP address via DHCP" selected (radio button) and "Set IP address manually" unselected (radio button). Below are the "Interface VLAN ID" field (set to 1) and the "DNS" field. A blue "Previous" button and a blue "Next" button are at the bottom.

Figure 2-2a: Set IP address

Set IP address

Interface VLAN ID
1

Obtain IP address via DHCP
 Set IP address manually

IP address
192.168.1.77

Subnet mask
255.255.255.0

Default router
192.168.1.254

DNS

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

Figure 2-2b: Set IP address

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

Step 3: Set date and time

Enable “Automatic 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.

Set date and time

Automatic date and time

Manually
2022-02-03 14:23:6

Figure 2-3: Set date and time

Step 4: Set system information

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

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.

Startup Page

Model Name	SISPM1040-384-LRT-C
System Description	Managed Hardened PoE+ Switch, (8) 10/100/1000Base-T PoE+ Ports + (4) 100/1000Base-X SFP
Location	
Contact	
System Name	SISPM1040-384-LRT-C
System Date	2011-01-01T00:01:03+00:00
System Uptime	00:01:03
Bootloader Version	v1.20
Firmware Version	v7.20.0186 2023-08-25
PoE Firmware Version	104-001
Hardware Version	v1.02
Mechanical Version	v1.01
Serial Number	A074122BR1200130
MAC Address	00-c0-f2-85-54-54
Memory	Total=44716 KBytes, Free=24540 KBytes, Max=23772 KBytes
FLASH	0x40000000-0x41ffffff, 512 x 0x10000 blocks
Powers status	Normal
Powers	PWR_1.0V:0.98V; PWR_3.3V:3.29V; PWR_2.5V:2.60V; PWR_1.8V:1.93V
Temperature status	Normal
Temperature 1	42(C); 107(F)
Temperature 2	44(C); 111(F)
CPU Load (100ms, 1s, 10s)	13%, 9%, 7%

1-10 Menu System

The left menu bar items are shown below:

The screenshot displays the left-hand menu system of the web interface, organized into five main sections:

- Configuration:** A large menu with a gear icon and a dropdown arrow. It contains numerous sub-items such as 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, Mirroring, UPnP, PTP, GVRP, sFlow, UDLD, Rapid Ring, Perception, MRP, and SMTp.
- Monitor:** A menu with a monitor icon and a dropdown arrow. It contains sub-items: System, Green Ethernet, Ports, Link OAM, DHCP, Security, Aggregation, Loop Protection, Spanning Tree, MVR, IPMC, LLDP, Ethernet Services, PTP, PoE, MAC Table, VLANs, MRP, VCL, sFlow, and UDLD.
- Diagnostics:** A menu with a network icon and a dropdown arrow. It contains sub-items: Ping, Ping6, Cable Diagnostics, Traceroute, and Link OAM.
- Maintenance:** A menu with a wrench icon and a dropdown arrow. It contains sub-items: Restart Device, Reboot Schedule, Factory Defaults, Firmware (with a dropdown arrow), Firmware Upgrade, Firmware Selection, Configuration (with a dropdown arrow), Save startup-config, Download, Upload, Activate, Delete, and Server Report.
- DMS:** A menu with a switch icon and a dropdown arrow. It contains sub-items: DMS Mode, Management (with a gear icon), Map API Key, Device List, Graphical Monitoring (with a network icon), Topology View, Floor View, Map View, Maintenance (with a wrench icon), Floor Image, Diagnostics, and Traffic Monitor.

Chapter 2. System Configuration

This page lets you set System Information and IP, NTP, Time, Syslog, Digital I/O, and Alarm Notification parameters.

2-1 System

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

2-1.1 Information

This page lets you set switch system information. To configure System Information in the web UI:

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

Figure 2-1.1: System Information Configuration

The screenshot shows the Lantronix web interface for configuring system information. The main content area is titled 'System Information Configuration' and includes a breadcrumb trail: Home > Configuration > System > Information. The form contains three input fields: 'System Contact' (empty), 'System Name' (pre-filled with 'SISPM1040-384-LRT-C'), and 'System Location' (empty). Below the form are 'Apply' and 'Reset' buttons. The left sidebar shows the navigation menu with 'Configuration', 'System', 'Information', 'IP', 'NTP', and 'Time' options.

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.

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 0-128 characters.

System Location: The physical location of this node (e.g., telephone closet, 3rd floor). The allowed string length is 0–128 characters.

Buttons:

Apply – Click to save changes.

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

Messages:

System Location is empty. Do you want to proceed anyway?

2-1.2 IP

Configure switch-managed IP information on this page in terms of IP basic settings, IP interfaces, and IP routes. Up to 8 interfaces and up to 32 routes are supported. The IPv4 address for the switch can be obtained via DHCP Server for VLAN 1. To manually configure an address, you must change the switch's default settings to values that are compatible with your network. You may also need to establish a default gateway between the switch and management stations that exist on another network segment.

To configure IP parameters in the web UI:

1. Click Configuration, System, IP.
2. Select the Mode; select DNS parameters if DNS is to be used.
3. Enable and configure DHCP Per Port if it is to be used.
4. Click the Add Interface button and create a new Interface on the switch.
5. Select Link-Local Address binding interface VLAN and select Gateway Address binding interface vlan.
6. Click Add Route to create a new Route on the switch.
7. Click Apply.

Figure2-1.2: IP Configuration page

The screenshot displays the IP Configuration page in the Lantronix web UI. The page is titled "IP Configuration" and includes a navigation menu on the left with options like "Switch", "DMS", "Configuration", "System", "Information", "IP", "NTP", "Time", "Log", "Digital I/O", "Alarm Notification", "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", "Mirroring", "UPnP", "PTP", "GVRP", "sFlow", and "IPMC".

The main content area is divided into several sections:

- Mode:** Set to "Host".
- DNS Servers:** Four DNS servers are configured, each with the address "8.8.8.8".
- DNS Proxy:** A checkbox that is currently unchecked.
- IP Interfaces:**
 - DHCP Per Port:** Mode is set to "Disabled".
 - VLAN:** Set to "VLAN 1".
 - IP:** A text input field for the IP address.
- IP DHCP Table:** A table with columns for "Delete", "VLAN", "Enable", "Fallback", "Current Lease", "IPv4 Address", "Mask Length", "DHCPv6 Enable", "Rapid Commit", "Current Lease", "IPv6 Address", and "Mask Length". One row is visible for VLAN 1 with IP 192.168.1.77 and mask length 24.
- Add Interface:** A button to add a new interface.
- 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". Three routes are listed:

Delete	Network	Mask Length	Gateway	Next Hop VLAN
<input type="checkbox"/>	0.0.0.0	0	192.168.1.254	0
<input type="checkbox"/>	169.254.0.0	16	192.168.1.77	0
<input type="checkbox"/>	192.168.1.0	24	192.168.1.77	0
- Add Route:** A button to add a new route.
- Apply/Reset:** Buttons at the bottom of the page.

Parameter descriptions:**Basic Settings**

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

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

No DNS server: No DNS server will be used.

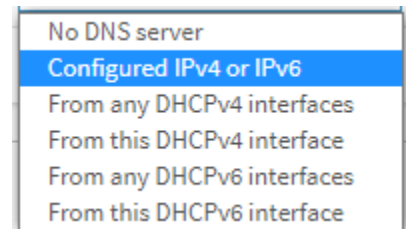
Configured IPv4 or IPv6: Explicitly provide the valid IPv4 or IPv6 (except linklocal) unicast address of the DNS Server in dotted decimal notation. Make sure the configured DNS server could be reachable (e.g. via PING) for activating DNS service.

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

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

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

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



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

IP Interfaces

DHCP per Port Mode: Select Disabled or Enabled for DHCP per Port. The default is Disabled. For more information see [Appendix B: DHCP Per Port](#) on page 473.

DHCP per Port VLAN: At the dropdown select the 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: Enter an IP address range that is within the interface subnet and equal to the switch TP port count. For more information see [Appendix B: DHCP Per Port](#) on page 473.

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

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

IPv4 DHCP Enabled : Enable the 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. Legal values are 0 to 4294967295 seconds.

IP Interfaces	
DHCP Per Port	
Mode	Enabled ▾
VLAN	VLAN 1 ▾
IP	192.168.1.1 - 192.168.1.6

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 0 - 30 bits for an IPv4 address. If DHCP is enabled, this field configures the fallback address network mask. The field may be left blank if IPv4 operation on the interface is not desired - or 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 or fe80::2c0:f2ff:fe49:4581/64. 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. 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 1-128 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 an Internet Protocol address that is intended only for communications within the segment of a local network (a link) or a point-to-point connection that a host is connected to.

Link-Local 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 'DHCP Option 3 example' below.

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

IP Routes: 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.

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

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

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

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

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

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.

Messages:

Subnet of VLAN 10 overlaps VLAN 1

Invalid route - address bits outside mask: 0.0.0.77

Invalid IPv4 Address: rt_net_3

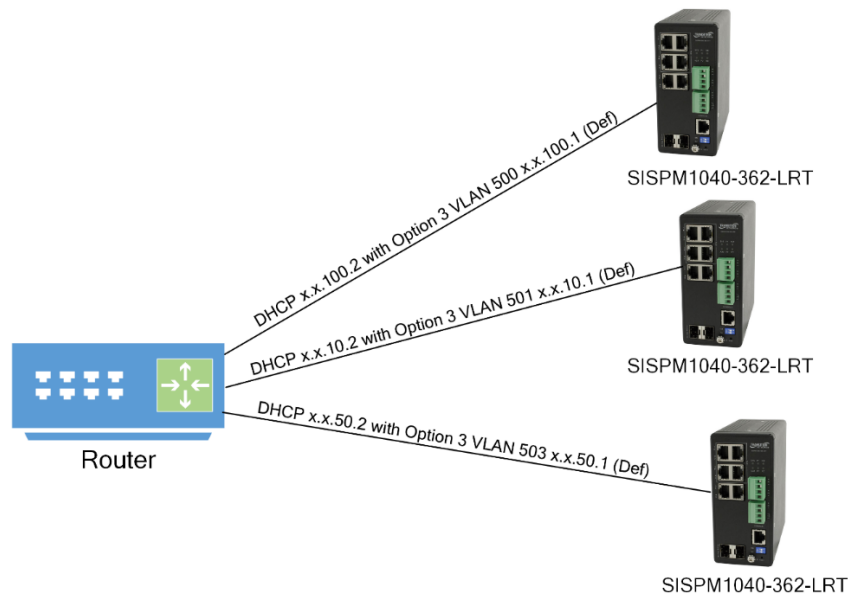
The value of 'Gateway' must be a valid IP address in dotted decimal notation ('x.y.z.w'). The following restrictions apply: 1) x, y, z, and w must be decimal numbers between 0 and 255, 2) x must not be 0, 3) x must not be 127, and 3) x must not be greater than 223.

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

The screenshot displays the 'IP Configuration' page. The 'Link-Local Address binding interface' and 'Gateway Address binding interface' are both set to 'VLAN 10'. Below, the 'IP Routes' table is shown with the following data:

Delete	Network	Mask Length	Gateway	Next Hop VLAN
<input type="checkbox"/>	0.0.0.0	0	192.168.1.254	0
<input type="checkbox"/>	0.0.0.0	0	192.168.1.254	0
<input type="checkbox"/>	169.254.0.0	16	192.168.1.77	0
<input type="checkbox"/>	192.168.1.0	24	192.168.1.77	0

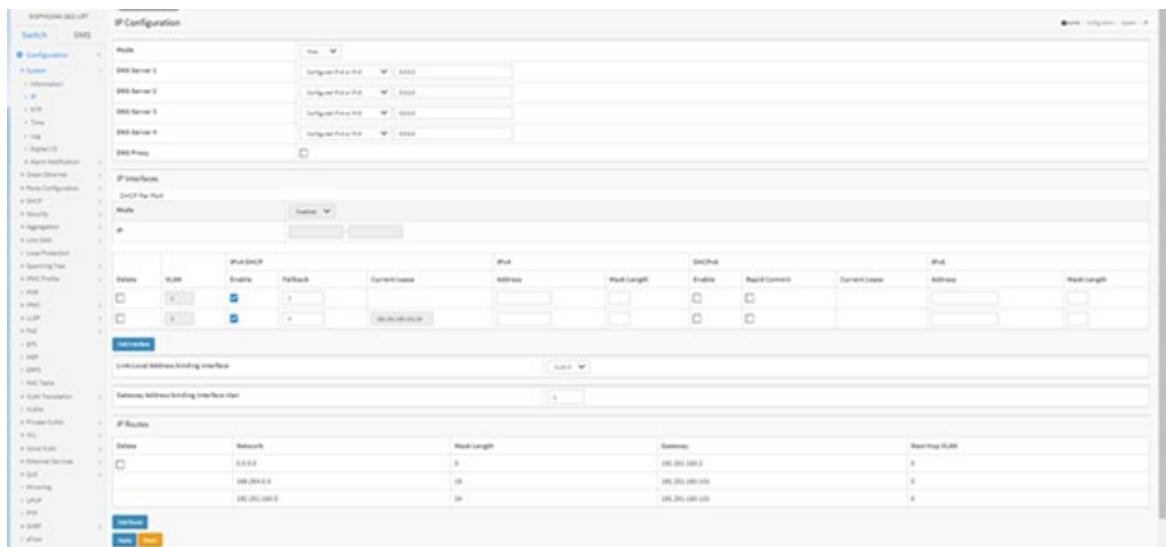
Example: DHCP Option 3: one VLAN interface gateway for the default route:



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

- With a switch set to the factory defaults, log in and add the following IP interfaces:
 - VLAN 2, IPv4 DHCP enabled
 - VLAN 3, IPv4 DHCP enabled
- 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.
- Delete VLAN 1 and perform a configuration save.
- Attach a cable from a DHCP server to a VLAN 2 port.
- Perform a switch reset and verify that a DHCP address has been obtained on VLAN 2.
- Move the cable to a VLAN 3 port.
- Perform a switch reset and verify that a DHCP address has been obtained on VLAN 3.
- Repeat steps 4 – 7 resetting the switch via power cycle.

Figure2-1.3: DHCP address obtained on VLAN 3



2-1.3 NTP

NTP (Network Time Protocol) is used to sync the network time based on Greenwich Mean Time (GMT). If using the NTP mode and select a built-in NTP time server or manually specify a user-defined NTP server as well as Time Zone, the switch will sync the time shortly after clicking the Apply button. Although NTP synchronizes the time automatically, NTP does not update the time periodically without user interaction.

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

Web Interface

To configure NTP in the web UI:

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

Figure 2-1.3: NTP Configuration

Parameter	Value
Automatic	Disabled
Server address via DHCP	
NTP Time-Sync Interval	60
Server 1	
Server 2	
Server 3	
Server 4	
Server 5	

Parameter descriptions:

Automatic : Indicates the automatic mode 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, or 120 minutes. The default is 60 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

2-1.4 Time

This page lets you set the Time, Time Zone, and Daylight Saving Time parameters.

To configure Time in the web UI:

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

Figure 2-1.4: Time Configuration

SISPM1040-384-LRT-C

Switch DMS

Configuration

System

Information

IP

NTP

Time

Log

Digital I/O

Alarm Notification

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

Mirroring

UPnP

PTP

Time Configuration

Home > Configuration > System > Time

Time Configuration

Clock Source: Use Local Settings

System Date: 2020-09-28 17:25:51 (yyyy-mm-dd hh:mm:ss)

Time Zone Configuration

Time Zone: None

Acronym: UTZ (0 - 16 characters)

Daylight Saving Time Configuration

Daylight Saving Time: Disabled

Start Time settings

Month: Jan

Date: 1

Year: 2014

Hours: 0

Minutes: 0

End Time settings

Month: Jan

Date: 1

Year: 2097

Hours: 0

Minutes: 0

Offset settings

Offset: 1 (1 - 1440) Minutes

Apply Reset

Parameter descriptions:**Time Configuration**

Clock Source: There are two modes for configuring the Clock Source:

Use Local Settings: Use to manually set Clock Source with Local Time. Note that the switch does not save the system time (using local settings) after a switch reboot.

Use NTP Server: Use to get Clock Source from an NTP Server.

System Date: Shows the current time of the system. The 'year' of system date is limited to 2011 - 2037.

Time Zone Configuration

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

Acronym: User can set the acronym of the time zone. This is a configurable acronym to identify the time zone. (Range: Up to 16 characters.)

Daylight Saving Time Configuration

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

Recurring Configuration**Start time settings:**

Week - Select the starting week number.

Day - Select the starting day.

Month - Select the starting month.

Hours - Select the starting hour.

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 (1 to 1440).

Note: The field under "Start Time Settings" and "End Time Settings" displays what you set in the "Start Time Settings" and "End Time Settings" fields.

Buttons

Apply: Click to save changes.

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

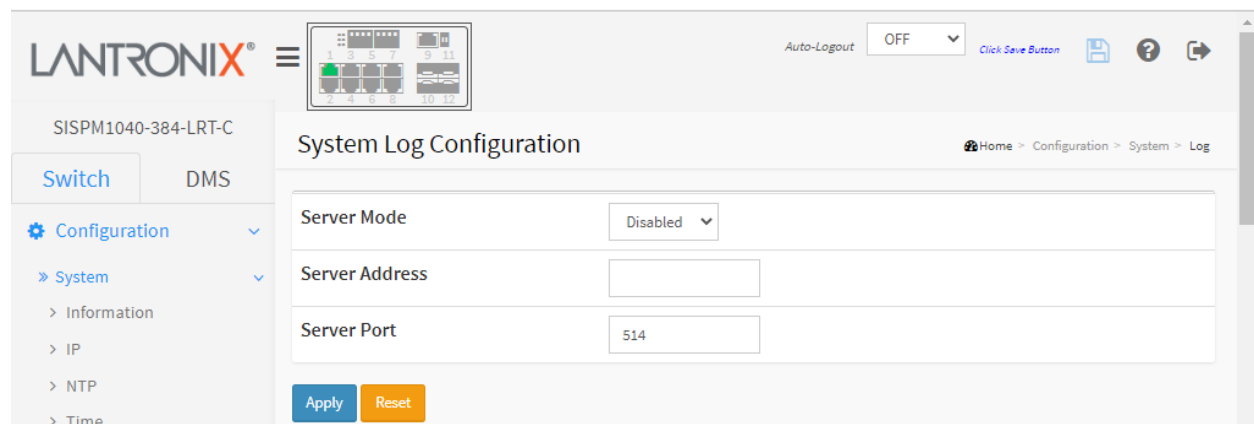
2-1.5 Log

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

To configure syslog parameters in the web UI:

1. Click Configuration, System and Log.
2. Specify the syslog parameters including IP Address of Syslog server and Port number.
3. Enable the Syslog server.
4. Click the Apply button.

Figure2-1.5: System Log Configuration



Parameter descriptions:

Server Mode : Select the server mode of operation. When the mode 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 : Enter the IPv4 hosts address of syslog server. If the switch provides a DNS feature; it also can be a host name.

Server Port: Indicates the service port of syslog server. The valid range is 1-65535. The default is port 514.

Buttons

Apply – Click to save changes.

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

2-1.6 Digital I/O

Configure the normal modes of digital input/output (DI/DO). Digital Inputs allow a microcontroller to detect logic states, and Digital Outputs allow a microcontroller to output logic states. See the Install Guide for hardware information. To configure Digital I/O parameters in the web UI:

1. Click Configuration, System and Digital I/O.
2. Specify the DI Normal Mode, Reboot System, DI Event, and the DO Normal Mode settings.
3. Click the Apply button.

Figure 2-1.6: Digital I/O Configuration

The screenshot shows the Lantronix web interface for the SISPM1040-384-LRT-C device. The main content area is titled "Digital I/O Configuration" and contains the following sections:

- DI Section:**
 - Normal Mode:** A dropdown menu set to "High".
 - Reboot System:** A dropdown menu set to "Disabled (Default)".
 - DI Event Description:** Two text input fields for "Normal" and "Abnormal" events.
- DO Section:**
 - Normal Mode:** A dropdown menu set to "Open".
 - Auto Recovery:** A dropdown menu set to "Disable".

An "Apply" button is located at the bottom left of the configuration area.

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

High : Allows the DI Normal Mode to 10V to 24V (default).

Low : Allows the DI Normal Mode to 0V to 6V .

Reboot System: Set the reboot system of the digital input (DI). You can set it to Reboot "Disabled" or Reboot "When DI was changed to abnormal." 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 7.20.0075.

DI Event Description: Customize event message. You can describe the Normal and Abnormal events in detail.

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

Open : Allows the Digital output (relay) to 0 (default).

Close : Allows the Digital output (relay) to 24VDC/1A.

Auto Recovery: Enable the Auto Recovery function. When enabled, Digital Output will automatically return to Normal mode when Digital Input changes back to Normal mode. The default is Disabled.

Buttons

Apply – Click to save changes.

2-1.7 Alarm Notification

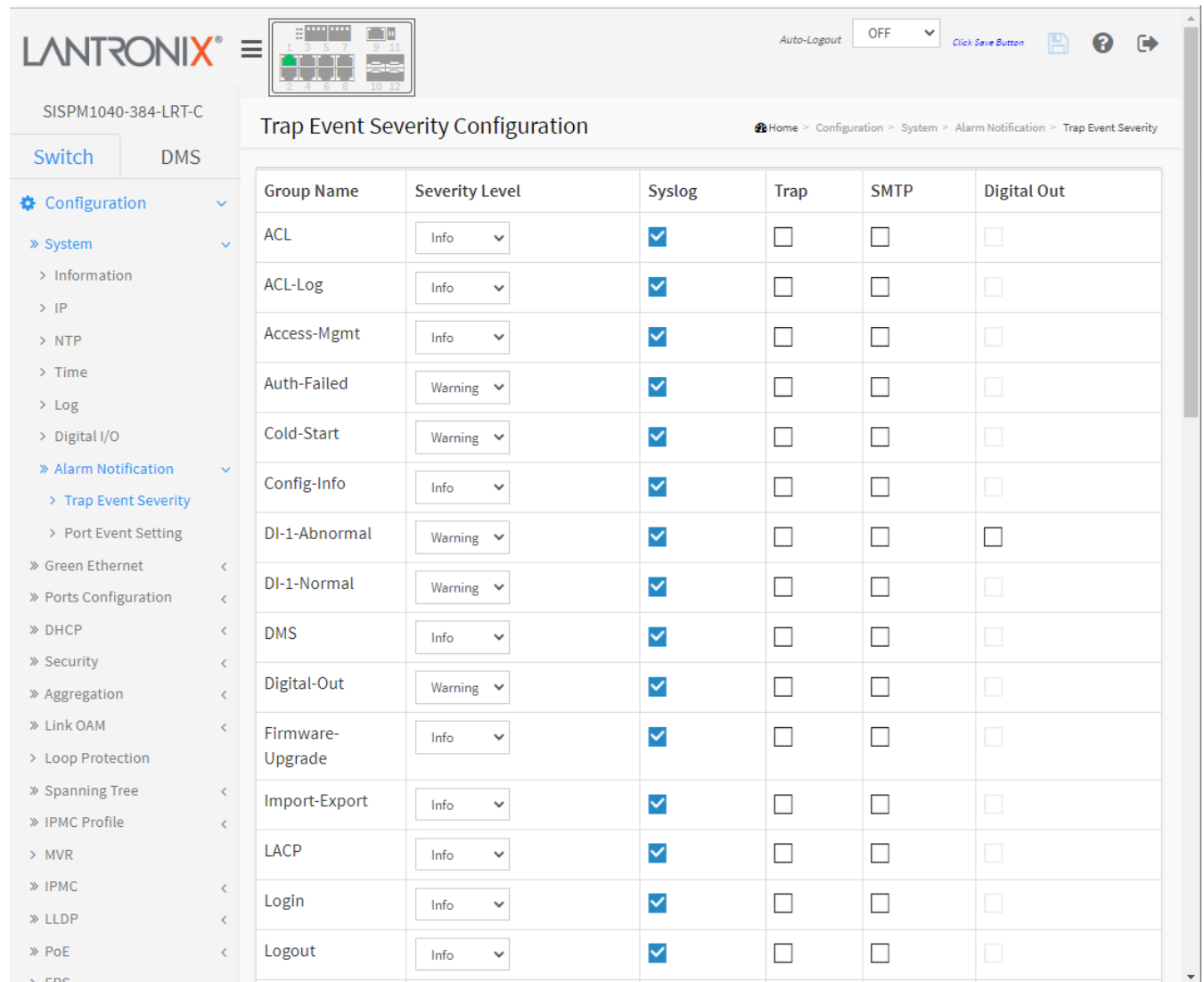
2-1.7.1 Trap Event Severity

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. Specify the Group Name, Severity Level, Syslog, Trap, SMTP, and Digital-Out.
3. Click the Apply button.

Figure 2-1.7.1: Trap Event Severity Configuration



The screenshot shows the Lantronix web interface for configuring trap event severity. The page title is "Trap Event Severity Configuration". The breadcrumb trail is "Home > Configuration > System > Alarm Notification > Trap Event Severity". The left sidebar shows the navigation menu with "Alarm Notification" > "Trap Event Severity" selected. The main content area contains a table with the following data:

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"/>
Firmware-Upgrade	Info	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Import-Export	Info	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
LACP	Info	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Login	Info	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Logout	Info	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Parameter descriptions:

Group Name : The name identifying the severity group.

Severity Level : Every group has a severity level. These Syslog levels are supported:

Emergency: System is unusable.

Alert: Action must be taken immediately.

Critical: Critical conditions.

Error: Error conditions.

Warning: Warning conditions.

Notice: Normal but significant conditions.

Information: Information messages.

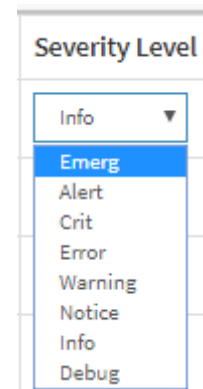
Debug: Debug-level messages.

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 : 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.

You can set Severity Level and configure for Syslog, Trap, SMTP, and/or Digital Out for these functions:

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

* Added "MRP Event" at FW v 7.10.2520.

2-1.7.2 Port Event Setting

This page is for configuring the port events. To configure Port Event Settings 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.

Figure 2-7.1.2: Port Event Setting

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"/>	Warning
<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

Parameter descriptions:

Active : Check to activate 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 : Event is triggered when Rx reaches this threshold.

Traffic Duration : Event is triggered when the traffic duration reaches this value.

Action Syslog : Enable Syslog on this port.

Action Trap : Enable SNMP Traps on this port.

Action SMTP : Enable SMTP on this port SMTP.

Action Digital Out : Enable Digital Out on this port.

Severity : Each port has a severity level. These levels are supported:

Emergency: System is unusable.

Alert: Action must be taken immediately.

Critical: Critical conditions.

Error: Error conditions.

Warning: Warning conditions (the default setting).

Notice: Normal but significant conditions.

Information: Information messages.

Debug: Debug-level messages.

Buttons

Apply – Click to save changes.

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

2-2 Green Ethernet

2-2.1 Port Power Savings

This page lets you configure the port power savings features. The EEE power saving option 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 called 'wakeup time'. The default wakeup time is 17 us for 1Gbit links and 30 us for other link speeds. EEE devices must agree upon the value of the wakeup time in order to make sure that both the receiving and transmitting device has all circuits powered up when traffic is transmitted. The devices can exchange 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.

To configure Port Power Saving 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 2-2.1: Port Power Savings Configuration

The screenshot shows the Lantronix web UI for the SISPM1040-384-LRT-C. The page title is "Port Power Savings Configuration". The breadcrumb trail is "Home > Configuration > Green Ethernet > Port Power Savings". The main configuration area has a dropdown menu for "Optimize EEE for" set to "Power". Below this is a "Port Configuration" table with columns for "Port", "ActiPHY", "PerfectReach", "EEE", and "EEE Urgent Queues" (1-8). The table contains 12 rows of port configurations.

Port	ActiPHY	PerfectReach	EEE	EEE Urgent Queues									
				1	2	3	4	5	6	7	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"/>	<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"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
2	<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"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
3	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" 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"/>
4	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
5	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<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"/>	<input checked="" type="checkbox"/>
6	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input 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"/>
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"/>	<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"/>	<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"/>	<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"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
11	<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"/>	<input type="checkbox"/>	<input type="checkbox"/>
12	<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"/>	<input type="checkbox"/>	<input type="checkbox"/>

At the bottom of the table are "Apply" and "Reset" buttons.

Parameter descriptions:

Optimize EEE for : At the dropdown set to optimize EEE for either best Power saving or least traffic Latency (the default setting).

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 as soon as 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.

2-3 Ports Configuration

2-3.1 Ports

This page lets you view and configure switch port parameters.

To configure Port Configuration parameters in the web UI:

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

Figure 2-3.1: Ports Configuration

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 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="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	Discard	<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 type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	9600	Discard	<input type="checkbox"/>
3	●	Down	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"/>
4	●	Down	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"/>
5	●	Down	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"/>
6	●	Down	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"/>
7	●	Down	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"/>
8	●	Down	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"/>
9	●	Down	Auto	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	9600		<input type="checkbox"/>
10	●	Down	Auto	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	9600		<input type="checkbox"/>

Parameter descriptions:

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

Link : The current link state is displayed graphically. Green indicates the link is up. Red indicates the link is down. Orange indicates 100fdx.

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

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

Disabled - Disables the switch port operation.

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

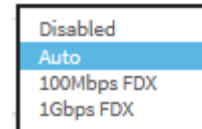
10Mbps HDX - Forces the cu port in 10Mbps half-duplex mode.

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

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

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

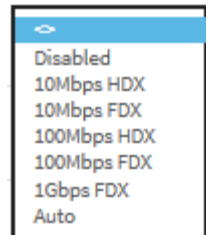
1Gbps FDX - Forces the port in 1Gbps full duplex





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

Adv Speed : When Speed is set to Auto (i.e., auto negotiation) the port will only advertise the specified speeds (**10M**, **100M**, **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 ( or ), 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 : Configure if frames with incorrect frame length in the EtherType/Length field shall 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:** Drop counters do not 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.

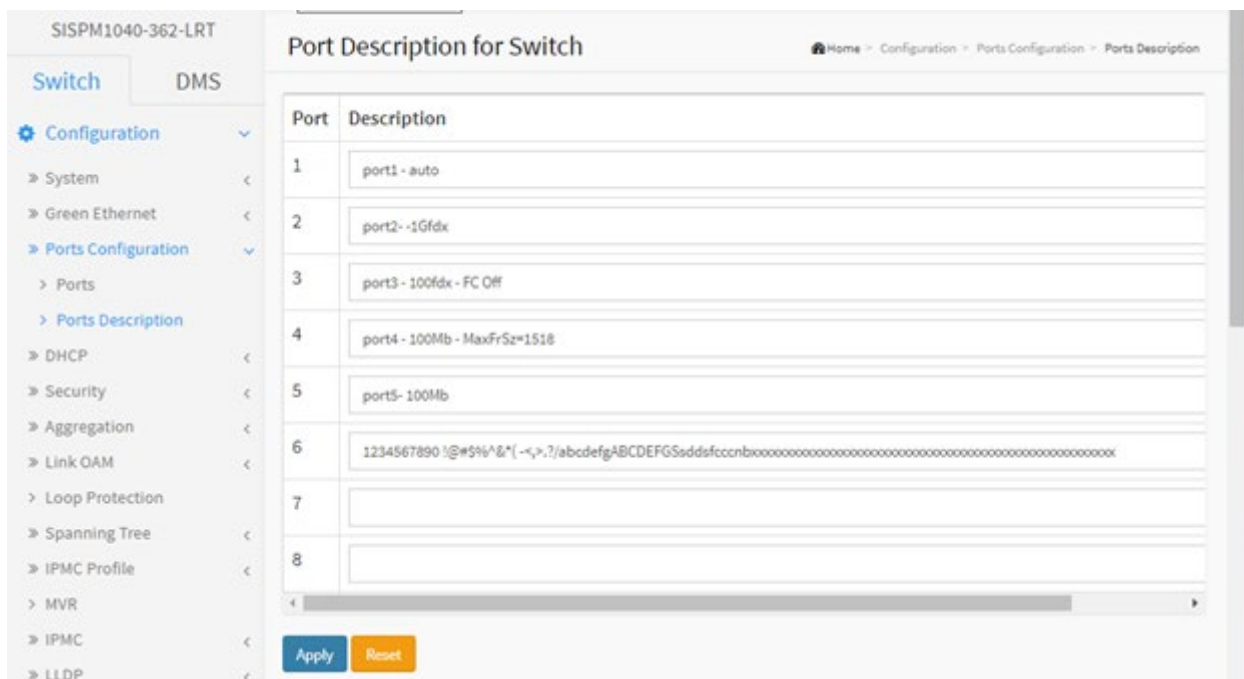
Refresh: Click to manually refresh the page immediately.

2-3.2 Ports Description

This page displays current port descriptions. To configure Port Description in the web UI:

1. Click Configuration, Port Configuration, 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.

Figure 2-3.2: Port Description



Parameter descriptions:

Port : The logical port number for this row.

Description : Enter up to 128 characters as a descriptive name to identify this port.

Buttons

Apply – Click to save changes.

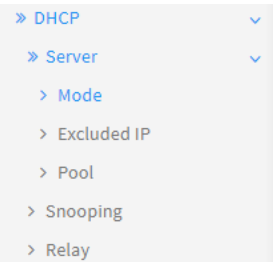
Reset- Click to undo any changes made locally and revert to previously saved values.

2-4 DHCP

This page lets you view and configure DHCP 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). Thus 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.



2-4.1 Server

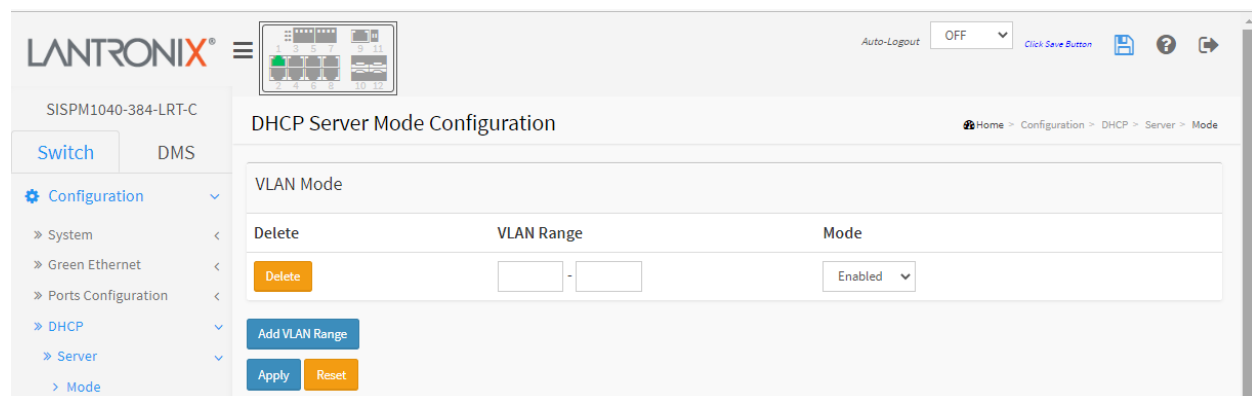
2-4.1.1 Mode

This page lets you set 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.

To configure DHCP server mode in the web UI:

1. Click Configuration, DHCP, Server, Mode.
2. Click the Add VLAN Range button.
3. Enter a valid range of VLAN IDs.
4. Select "Enabled" at the global Mode dropdown.
5. Click Apply.

Figure 2-4.1.1: DHCP Server Mode Configuration



Parameter descriptions:

Mode : Configure the operating mode of the system. Possible modes are:

Enable: Enable DHCP server per system.

Disable: Disable DHCP server per system.

VLAN Range : Indicate the VLAN range in which DHCP server is enabled or disabled. The first VLAN ID must be smaller than or equal to the second VLAN ID. However, if the VLAN range contains only 1 VLAN ID, then you can just input it into either one of the first and second VLAN ID or both.

Otherwise, to disable the existing VLAN range, follow these steps:

1. Click "Add VLAN Range" to add a new VLAN range.
2. Input the VLAN range that you want to disable.
3. At the Mode dropdown, select Enabled.
4. Click "Apply" to apply the change.

The disabled VLAN range is removed from the DHCP Server mode configuration page.

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

Enable: Enable DHCP server per VLAN.

Disable: Disable DHCP server pre VLAN.

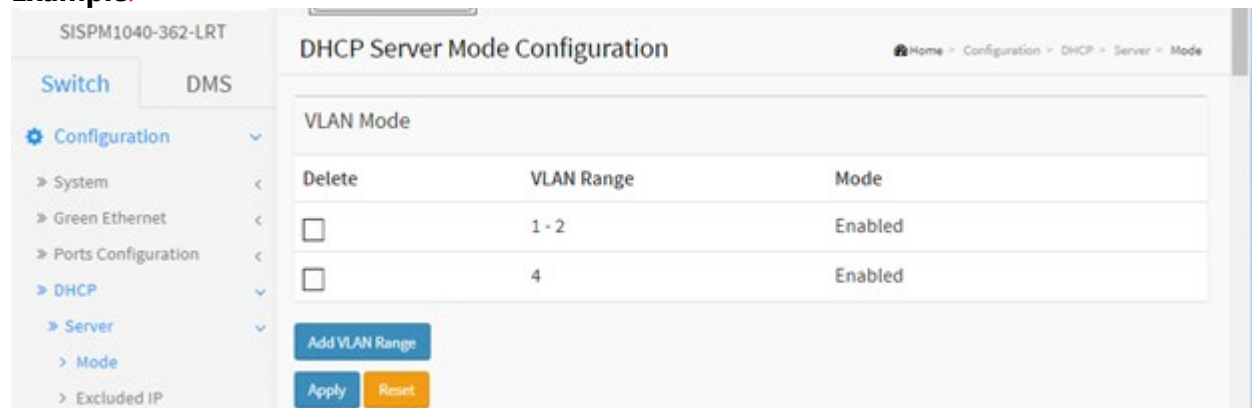
Buttons

Add VLAN Range - Click to add a new VLAN range.

Apply – Click to save changes.

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

Example:



The screenshot displays the DHCP Server Mode Configuration page for device SISPM1040-362-LRT. The page title is "DHCP Server Mode Configuration". On the left, there is a navigation menu with "Switch" and "DMS" tabs, and a "Configuration" section expanded to show "Server" > "Mode". The main content area shows a table titled "VLAN Mode" with the following data:

Delete	VLAN Range	Mode
<input type="checkbox"/>	1 - 2	Enabled
<input type="checkbox"/>	4	Enabled

Below the table, there are three buttons: "Add VLAN Range" (blue), "Apply" (blue), and "Reset" (orange). The breadcrumb trail at the top right reads: Home > Configuration > DHCP > Server > Mode.

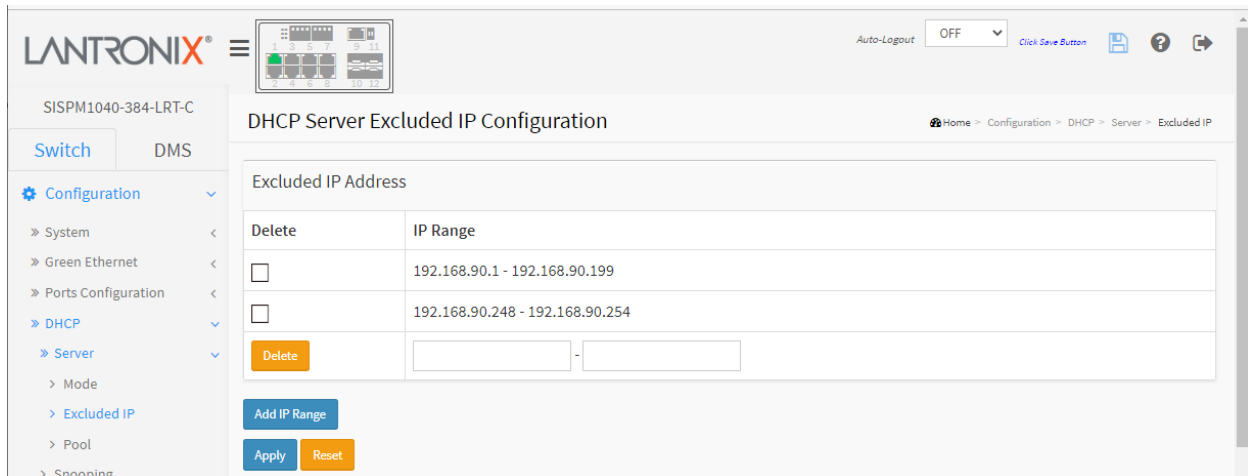
2-4.1.2 Excluded IP

This page lets you configure excluded IP addresses. A DHCP server will not allocate these excluded IP addresses to a DHCP client.

To configure DHCP server excluded IP in the web UI:

1. Click Configuration, DHCP, Server, Excluded IP
2. Click Add IP Range then enter the new Range of excluded IP addresses.
3. Click Apply.

Figure 2-4.1.2: DHCP Server Excluded IP Configuration



Parameter descriptions:

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.

Messages:

The value of Excluded low IP address, 1, must be a valid IP address in doted decimal notation (“x.y.z.w”), where x, y, z, and w are decimal numbers between 0 and 255.

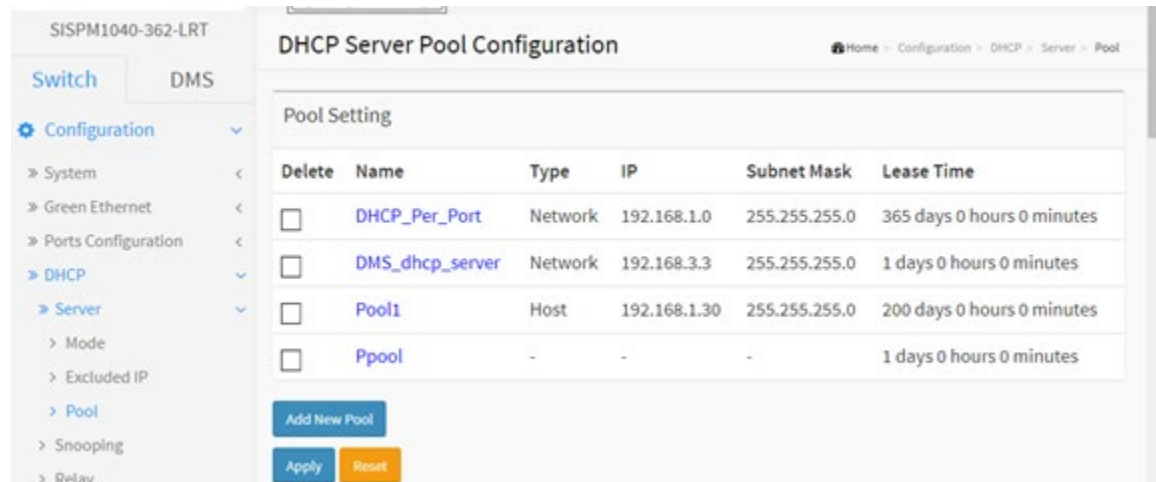
2-4.1.3 Pool

This page lets you manage DHCP pools. Based on the DHCP pool, a DHCP server will allocate IP address and deliver configuration parameters to a DHCP client.

To configure DHCP server pool in the web UI:

1. Click Configuration, DHCP, Server, Pool.
2. Click Add New Pool and configure the new Pool parameters.
3. Click Apply.

Figure 2-4.1.3: 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. To configure all pool settings including type, IP subnet mask and lease time, click the linked pool Name to go into the configuration page.

Name : 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 : Displays which type of the pool is.

None: The pool type is not yet defined (default).

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.

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

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

Lease Time : Displays the 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.

DHCP Pool Configuration Page

Click the linked Pool Name (e.g., [DHCP-Per_Port](#)) to display the DHCP Pool Configuration page.

The screenshot displays the DHCP Pool Configuration page in the Lantronix web interface. The page title is "DHCP Pool Configuration". On the left, there is a navigation menu with categories like "Configuration", "System", "Ports", "DHCP", "Services", "Users", "Integration", and "Maintenance". The main content area is a form for configuring a DHCP pool. At the top, there is a "Name" dropdown menu set to "DHCP-Per_Port". Below this is a "Saving" section with a "Pool Name" dropdown also set to "DHCP-Per_Port". The form contains several rows of input fields and dropdown menus for various parameters:

- Type:** A dropdown menu set to "Static".
- IP:** An empty input field.
- Subnet Mask:** An empty input field.
- Lease Time:** Three rows for configuring lease duration:
 - Row 1: "1" days (range 0-999).
 - Row 2: "0" hours (range 0-59).
 - Row 3: "0" minutes (range 0-59).
- Domain Name:** An empty input field.
- Broadcast Address:** An empty input field.
- Default Router:** An empty input field.
- DNS Server:** An empty input field.
- HTTP Server:** An empty input field.
- TFTP Server:** An empty input field.
- Base File:** An empty input field.
- NIS Client Name Type:** A dropdown menu set to "Static".
- NIS Client Name:** An empty input field.
- NIS Server:** An empty input field.
- Client Identifier:** A dropdown menu set to "Static".
- Hardware Address:** An empty input field.
- Client Name:** An empty input field.
- Vendor 0 Class Identifier:** An empty input field.
- Vendor 0 Option Information:** An empty input field.
- Vendor 1 Class Identifier:** An empty input field.
- Vendor 1 Option Information:** An empty input field.
- Vendor 2 Class Identifier:** An empty input field.
- Vendor 2 Option Information:** An empty input field.
- Vendor 3 Class Identifier:** An empty input field.
- Vendor 3 Option Information:** An empty input field.
- Vendor 4 Class Identifier:** An empty input field.
- Vendor 4 Option Information:** An empty input field.
- Lighting Server:** An empty input field.

 At the bottom of the form, there are "Apply" and "Save" buttons.

Parameter descriptions:

Pool:

Name: Select a pool by pool name.

Setting: Configure pool settings.

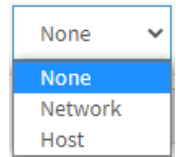
Name: Displays the selected pool name

Type: Specify the type of pool (None, Network or Host).

None: The pool type is not yet defined (default).

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.



IP: Specify the IP address 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. Valid entries are days (0-365), hours (0-23), and minutes (0-59). The default is all 0s.

Domain Name: DHCP option 15. Specify the 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. See Configuration > System > IP.

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

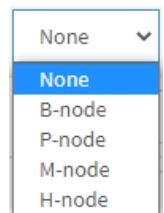
NTP Server: DHCP option 42. Specify a list of IP addresses indicating NTP servers available to the client.

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 RFC 1001/1002.

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.

IS 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.

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 1-4 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 1-4 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. (Added at FW v7.20.0106.) 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.

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 Web 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:

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

Pool type is defined so subnet mask must be inputted.

2-4.2 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, Snooping.
2. Select "Enabled" at the Snooping Mode dropdown.
3. Select "Trusted" or "Untrusted" for each port at the Mode dropdown.
4. Click Apply.

Figure 2-4.2: DHCP Snooping Configuration

The screenshot shows the web interface for configuring DHCP Snooping. The 'Snooping Mode' is currently set to 'Disabled'. The 'Port Mode Configuration' table lists ports 1 through 8, each with a 'Mode' dropdown menu. All ports are currently set to 'Trusted'.

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

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.

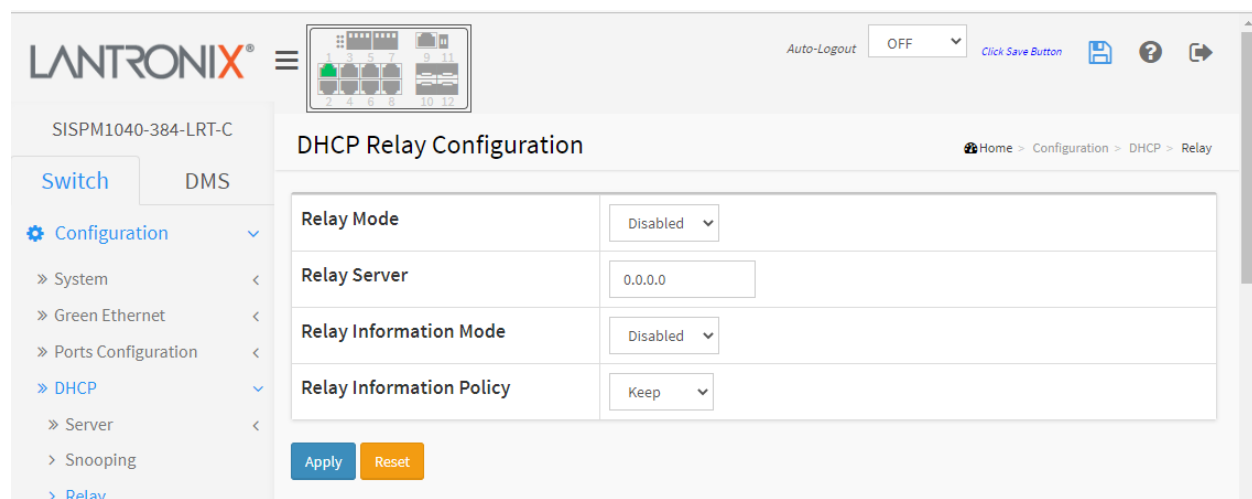
2-4.3 Relay

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

To configure DHCP Relay in the web UI:

1. Click Configuration, DHCP, Relay.
2. Specify the Relay Mode, Relay Server, Relay Information Mode, Relay Information Policy.
3. Make sure the DHCP server is connected on a trust port, and then click OK.
4. Click Apply.

Figure 2-4.3: 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 as "[vlan_id][module_id][port_no]". The first four characters represent the VLAN ID, the fifth and sixth characters are the module ID (always 0 in standalone device), and the last two characters are the port number. For example, "00030108" means the DHCP message received from VLAN ID 3, switch ID 1, port No 8. and the option 82 remote ID value is equal to the switch MAC address. Possible modes:

Enabled: Enable DHCP relay information mode operation. When DHCP relay information mode operation is enabled, the agent inserts specific information (option 82) into a DHCP message when forwarding to DHCP server and removes it from a DHCP message when transferring to DHCP client. It only works when DHCP relay operation mode is enabled.

Disabled: Disable DHCP relay information mode operation.

Relay Information Policy : Indicates the DHCP relay information option policy. When DHCP relay information mode operation is enabled, if the agent receives a DHCP message that already contains relay agent information it will enforce the policy. The 'Replace' policy is invalid when relay information mode is disabled. Possible policies are:

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

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

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

Buttons

Apply – Click to save changes.

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

Messages

Please make sure the DHCP server connected on trust port?

2-5 Security

This page lets you configure the various Security settings of the switch.

2-5.1 Switch

2-5.1.1 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 browser.

Web Interface

To configure User in the web interface:

1. Click Configuration, Security, Switch, Users. By default, the Users Configuration page displays with one User Name (admin) at Privilege Level 15.
2. Click the Add New User button.
3. Specify the User Settings parameters.
4. Click Apply.

Figure 2-5.1.1: User Settings

The screenshot shows the Lantronix web interface for the device SISPM1040-384-LRT-C. The main content area is titled 'Add User' and contains a 'User Settings' form. The form has four rows: 'User Name' with a text input field, 'Password' with a text input field, 'Password (again)' with a text input field, and 'Privilege Level' with a dropdown menu currently showing '0'. Below the form are three buttons: 'Apply' (blue), 'Reset' (orange), and 'Cancel' (blue). The left sidebar shows a navigation tree with 'Security' > 'Switch' > 'Users' selected. The top right of the interface shows 'Auto-Logout' set to 'OFF' and a 'Click Save Button' link.

Parameter descriptions:

User Name : The name identifying the user. This is also a link to Add/Edit User.

Password : The password of the user. The allowed string length is 0-31. Any printable characters including space are accepted.

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

Privilege Level : The privilege level of the user. The allowed range is 1-15. If the privilege level value is 15, it can access all groups (i.e., granted full control of the device). But other values can be set for each group privilege level. User's privilege should be same or greater than the group privilege level to have the access of that group. By default, most groups' privilege level 5 has the read-only access and privilege level 10 has the read-write access. System maintenance (software upload, factory defaults, etc.) need user privilege level 15. Generally, privilege level 15 can be used for an administrator account, privilege level 10 for a standard user account and privilege level 5 for a guest account.

Buttons

Add New User: Click to add and configure a new user.

Apply: Saves the new parameters.

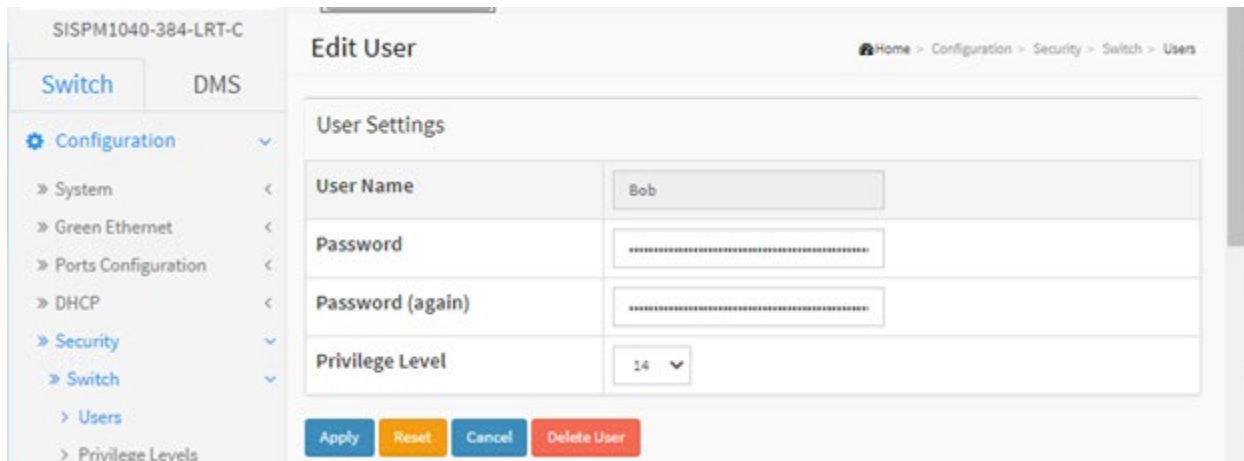
Reset: Disregards the recent parameter entries.

Cancel : Cancels the parameter changes.

After you click the Apply button, the new user is added to the User Name table.



You can click the linked User Name to display its Edit User page to let you edit a User's Password and Privilege Level:



Add/Edit User Buttons:

Apply: Click to save changes.

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

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

Delete User: Delete the current user. This button is not available for new configurations (Add New User).

2-5.1.2 Privilege Levels

This page lets you view and modify privilege levels by functions. To configure Privilege Level in the web UI:

1. Click Configuration > Security > Switch > Privilege Levels.
2. Specify the Privilege parameters.
3. Click Apply.

Figure2-5.1.2: Privilege Levels Configuration

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
ERPS	5	10	5	10
ETH_LINK_OAM	5	10	5	10

Parameter descriptions:

Group Name : The name identifying the privilege group. In most cases, a privilege level group consists of a single module (e.g. LACP, RSTP or QoS), but a few of them 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 (1-15) for the following sub groups: Configuration Read-only, Configuration/Execute Read/write, Status/Statistics Read-only, and Status/Statistics Read/write (e.g. for clearing of statistics). User Privilege should be same or greater than the authorization Privilege level to have the access to that group.

Buttons

Apply – Click to save changes.

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

2-5.1.3 Authentication Method

This page lets you configure a user with authentication when logging into the switch via one of the management client interfaces. The table has one row for each client type and several columns.

To configure Authentication Method in the web UI:

1. Click Configuration > Security > Switch > Auth Method.
2. Specify the Client (console, telnet, ssh, web) which you want to monitor. **Note:** Password security changed in FW v1.02.1415. You cannot login if downgrading the switch to older firmware versions or loading an old config file in new firmware.
3. Specify the Authentication Method (none, local, radius, tacacs+).
4. Check Fallback.
5. Click Apply.

Figure 2-5.1.3: Authentication Method Configuration

Authentication Method Configuration

Home > Configuration > Security > Switch > Auth Method

Authentication Method

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

Parameter descriptions:

Authentication Method : The Authentication Method section lets you configure how a user is authenticated when they log into the switch via one of the management client interfaces.

Client : The management client for which the configuration below applies (console, telnet, ssh, http, https).

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

no: Authentication is disabled and login is not possible.

redirect: When HTTPS is enabled at Configuration > Security > Switch > HTTPS, this enables 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.

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 : The Command Authorization Method section lets you limit the CLI commands available to a user. The table has one row for each client type and several columns:

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

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

no: Command authorization is disabled. User is granted access to CLI commands according to his 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 : The Accounting Method section lets you configure command and exec (login) accounting. The table has one row for each client type and several columns, which are:

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 in the range 0 to 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.

Messages

Message: *Warning: When setting first method for 'http' to 'redirect' and setting first method for 'https' to 'no', login via 'https' and 'http' are all not possible. Do you want to continue?*

Message: *Warning: When setting first method for 'https' to 'no', login via 'https' is not possible. Do you want to continue?*

Message: *Warning: When setting first method for 'ssh' to other than 'local', you may lose connectivity unless you set a later method for 'ssh' to 'local'. Do you want to continue?*

Message: *Auth methods updated successfully. ** Please reconnect manually if the browser fail to redirect properly.*

2-5.1.4 HTTPs

This page lets you configure HTTPS settings and maintain the current certificate on the switch. To configure HTTPS via the web UI:

1. Click Configuration > Security > Switch > HTTPS.
2. Select and enter the Certificate parameters.
3. Click the Browse button to browse to and select the certificate file to upload.
4. Click Apply.

Figure 2-5.1.5: HTTPS Configuration

Parameter descriptions:

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

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

Generate: Generate a new self-signed RSA certificate.

Certificate Pass Phrase: Enter the passphrase here if your uploading certificate is protected by a specific passphrase.

Certificate Upload: Select Web Browser or URL. Upload a certificate PEM file into the switch. The file must contain the certificate and private key together. If you have two separate files for saving certificate and private key, use the Linux cat command to combine them into a single PEM file (e.g., `cat my.cert my.key > my.pem`).

Note that the RSA certificate is recommended since most new browser versions have removed support for DSA in certificates (e.g. Firefox v37 and Chrome v39 and above). Possible “Generate” methods are:

Web Browser: Upload a certificate via Web browser.

URL: Upload a certificate via URL, the supported protocols are HTTP, HTTPS, TFTP and FTP. The URL format is:

`<protocol>://[<username>[:<password>]@]< host>[:<port>][/<path>]/<file_name>`

For example, `tftp://10.10.10.10/new_image_path/new_image.dat` or
`http://username:password@10.10.10.10:80/new_image_path/new_image.dat`

A valid file name is a text string of alpha (A-Za-z), digits (0-9), dot (.), hyphen (-), underscore (_) characters. The maximum length is 63 and hyphen must not be first character. A file name with

only '.' is not allowed.

File Upload: Browse to and select a certificate.

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.

Choose File: Click to select a certificate.

Messages

Message: *Notice that the browser may not allow the redirect operation due to the security consideration unless the switch certificate is trusted to the browser. You need to initialize the HTTPS connection manually under this case.*

Recovery: **1.** Click the **OK** button to clear the web page message. **2.** Change HTTPS Mode to 'Disabled'.
3. Re-try the operation.

Message: *'Certificate Maintain' can't be executed if HTTPS is enabled*

Recovery: **1.** Click the **OK** button to clear the web page message. **2.** Change HTTPS Mode to 'Disabled'.
3. Re-try the operation.

Message: *Certificate PEM file size is too big.*

Meaning: A .pem file is a container format that may include just the public certificate or may include an entire certificate chain including public key, private key, and root certificates. See IETF RFCs 1421 - 1424.

Recovery: **1.** Click the **OK** button to clear the web page message. **2.** See Certificate Upload parameter above.

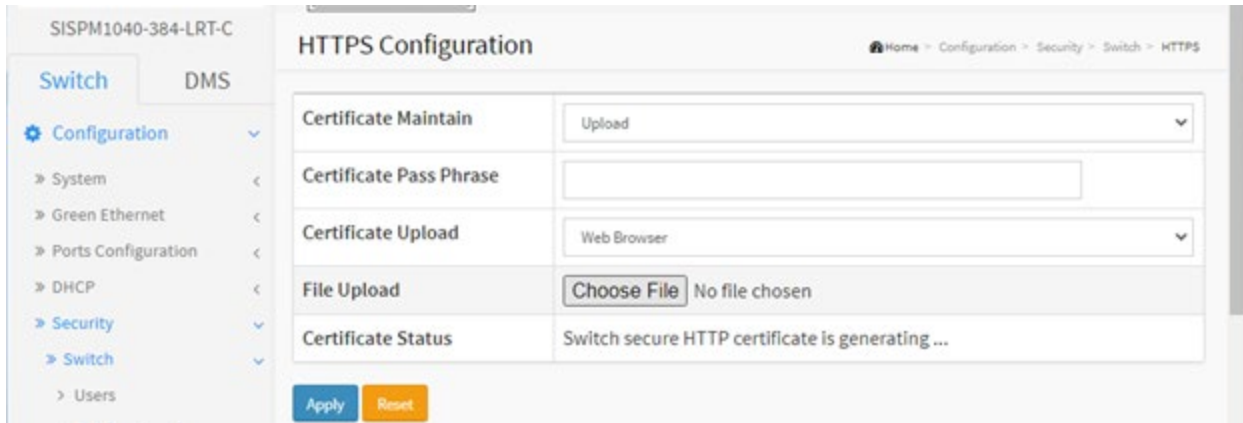
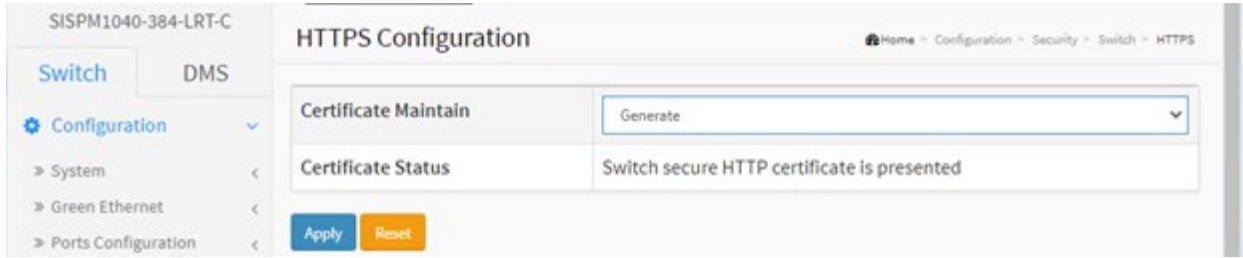
Message: *HTTPS invalid Certificate*

Recovery: **1.** Click the **OK** button to clear the web page message. **2.** See Certificate Upload parameter above.

Message: *Please disable HTTPS mode first.*

Recovery: **1.** Click the **OK** button to clear the web page message. **2.** Change HTTPS Mode to 'Disabled'.
3. Re-try the operation.

Generate a new self-signed RSA certificate:



2-5.1.6 Access Management

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

To configure Access Management via the web UI:

1. Click Configuration > Security > Switch > Access Management.
2. Select "Enabled" at the Mode dropdown.
3. Click "Add New Entry".
4. Specify the Start IP Address and End IP Address.
5. Check one or more Access Management methods (HTTP/HTTPS, SNMP, and TELNET/SSH).
6. Click Apply.

Figure 2-5.1.6: Access Management Configuration

Delete	VLAN ID	Start IP Address	End IP Address	HTTP/HTTPS	SNMP	TELNET/SSH
<input type="checkbox"/>	1	192.168.1.1	192.168.1.100	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
<input type="checkbox"/>	1	0.0.0.0	0.0.0.0	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

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).

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

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.

Note: Password security is changed in FW v1.02.1415. You cannot login if downgrading the switch to older firmware versions or loading an old config file in new firmware.

Buttons:

Add New Entry – Click to add a new access management entry.

Apply – Click to save changes.

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

Messages:

At least one allowed service must be checked.

The entry content is duplicated. (0.0.0.0 - 0.0.0.0)

2-5.1.7 SNMP

Any Network Management System (NMS) running the Simple Network Management Protocol (SNMP) can manage the Managed devices equipped with SNMP agent, provided that the Management Information Base (MIB) is installed correctly on the managed devices. The SNMP protocol is used to govern the transfer of information between 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 for issuing the trap information. The switch supports a switch to turn on or off the SNMP agent. If you set the field SNMP to “Enabled”, the SNMP agent will start up. All supported MIB OIDs, including RMON MIB, can be accessed via SNMP manager. If the field SNMP is set “Disable”, the SNMP agent will be de-activated, the related Community Name, Trap Host IP Address, Trap and all MIB counters will be ignored.

2-5.1.7.1 System

This page lets you configure SNMP System on the switch. This function is used to configure SNMP settings, community name, trap host and public traps as well as the throttle of SNMP.

An SNMP manager must pass the authentication by identifying both community names, then it can access the MIB information of the target device. So, both parties must have the same community name. When the settings are complete, click the Apply button; the settings take effect.

Web Interface

To configure SNMP System parameters in the web UI:

1. Click Configuration, Security, Switch, SNMP, System.
2. At the Mode dropdown, select Enabled to enable the SNMP function.
3. Specify the Version, Read Community, Write Community, and Engine ID.
4. Click Apply.

Figure2-5.1.7.1: SNMP System Configuration

The screenshot shows the 'SNMP System Configuration' page in the Lantronix web interface. The page includes a navigation menu on the left with 'Switch' selected. The main configuration area contains the following fields:

Mode	Enabled
Version	SNMP v2c
Read Community	public
Write Community	private <input checked="" type="checkbox"/> Enabled
Engine ID	800007e5017f000001

At the bottom of the configuration area, there are 'Apply' and 'Reset' buttons. The top right of the interface shows 'Auto-Logout OFF' and a 'Click Save Button' link.

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.

SNMP v3: Set SNMP supported version 3.

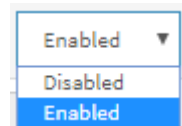
Read Community : Indicates the community read access string to permit access to SNMP agent. The allowed string length is 0 to 255, and the allowed content is the ASCII characters from 33 to 126.

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

Write Community : Indicates the community write access string to permit access to SNMP agent. The allowed string length is 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.

At the dropdown next to the field, select *Enabled* or *Disabled*. The default is Write Community Enabled.



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.

2-5.1.7.2 Trap

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

1. Click Configuration, Security, Switch, SNMP, Trap.
2. At the Global Settings “Mode” dropdown select ‘Enabled’.
3. Click Add New Entry to display the SNMP Trap Configuration page shown below.
4. Configure the new SNMP Trap on the switch and click Apply.

Figure2-5.1.7.2: SNMP Trap Configuration

Trap Config Name : Indicates which trap Configuration's name to configure. The allowed string length is 1 to 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).

UDP: Use UDP as the SNMP trap mode.

TCP: Use TCP as the SNMP trap mode.

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 (the default setting).

SNMPv3: Set SNMP trap supported version 3.

Trap Community: Indicates the community access string when sending SNMP trap packet. The allowed string length is 1-32 characters, and the allowed content is ASCII characters from 33 to 126.

Trap Destination Address : Indicates the SNMP trap destination address. It allows a valid IP address in dotted decimal notation ('x.y.z.w'). It also allows a valid hostname. A valid hostname is a string drawn from the alphabet (A-Za-z), digits (0-9), dot (.), dash (-). Spaces are not allowed, the first character must be an alpha character, and the first and last characters must not be a dot or a dash.

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

Trap Destination port : Indicates the SNMP trap destination port. An SNMP Agent will send SNMP messages via this port; the port range is 1~65535.

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

Enabled: Enable SNMP trap inform mode operation.

Disabled: Disable SNMP trap inform mode operation.

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

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

Apply – Click to save changes.

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

Messages:

The value of 'Trap Destination Address' is 0.0.0.0. Do you want to proceed anyway?

'Trap Configuration Name' string is null

Example:

Trap Configuration

Home > Configuration > Security > Switch > SNMP > Trap

Global Settings

Mode: Enabled

Trap Destination Configurations

Delete	Name	Mode	Version	Destination Address	Destination Port
<input type="checkbox"/>	trap1	UDP	SNMPv3	192.168.1.30	162
<input type="checkbox"/>	trap2	TCP	SNMPv3	192.168.1.40	162
<input type="checkbox"/>	trap3	UDP	SNMPv2c	192.168.1.50	162

Add New Entry

Apply Reset

You can click a linked Trap Name to go to its SNMP Trap Configuration page as described above.

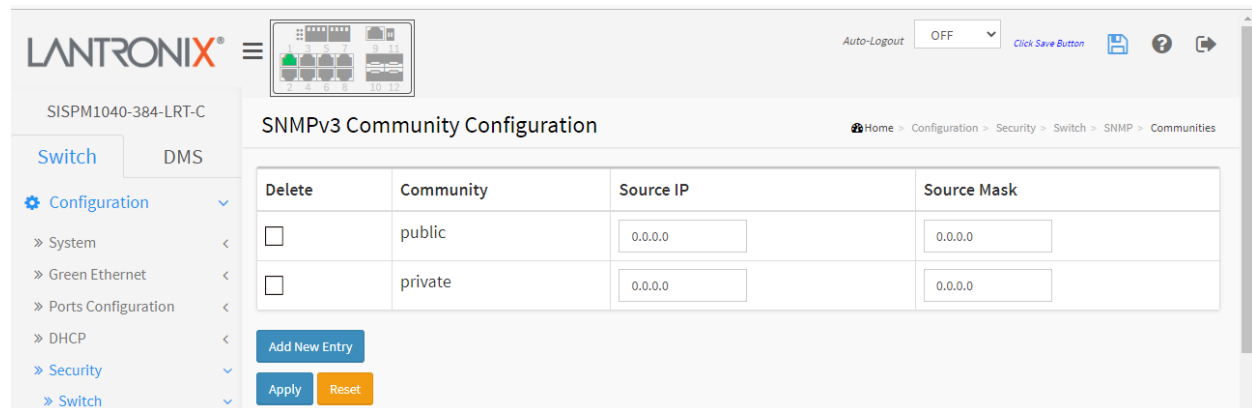
2-5.1.7.3 Communities

This function is used to configure SNMPv3 communities. The Community and UserName are unique. You can create up to four Groups.

To configure SNMP Communities in the web UI:

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

Figure2-5.1.7.3: SNMPv3 Community Configuration



Parameter descriptions:

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

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 an SNMPv1 or SNMPv2c community string.

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

Source Mask : Indicates the SNMP access source address mask.

Buttons:

Add New Entry – Click to add a new entry.

Apply – Click to save changes.

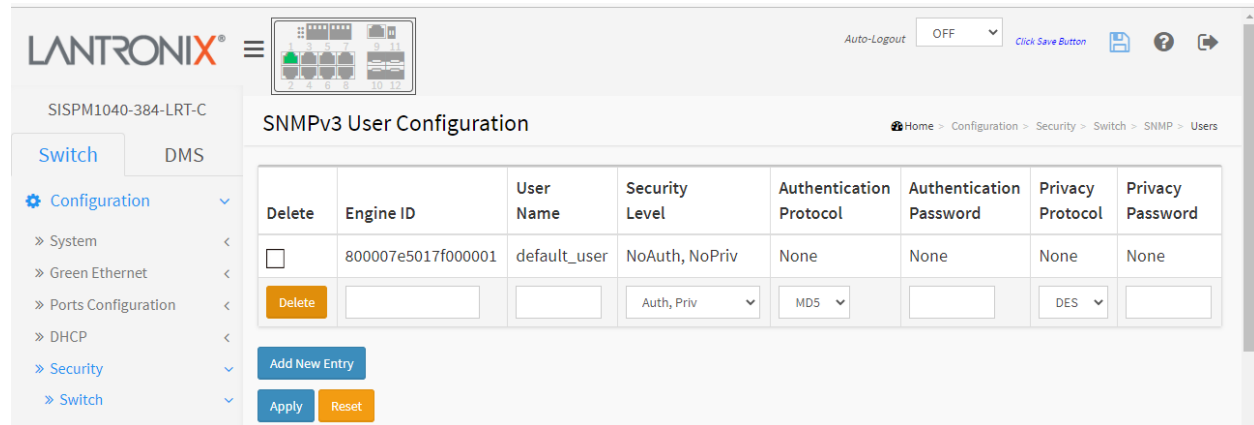
Reset- Click to undo any changes made locally and revert to previously saved values.

2-5.1.7.4 Users

This function is used to configure SNMPv3 users. The Entry index key is UserName. You can create up to 10 users. To configure SNMP Users in the web UI:

1. Click Configuration, Security, Switch, SNMP, Users.
2. Click Add New Entry.
3. Specify the Privilege parameter.
4. Click Apply.

Figure 2-5.1.7.4: SNMPv3 User Configuration



Parameter descriptions:

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

Engine ID : An octet string identifying the engine ID that this entry should belong to. The string must contain an even number (in hexadecimal format) with 10-64 digits, 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 : Sets the security model that this entry should belong to. Possible security models are:

NoAuth, NoPriv: No authentication and no privacy.

Auth, NoPriv: Authentication and no privacy.

Auth, Priv: Authentication and privacy.

The value of security level cannot be modified if entry already exists. That means it must first be ensured that the value is set correctly.

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

None: No authentication protocol.

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 an entry already exists. That means you must first ensure that the value is set correctly.

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

Buttons:

Add New Entry – Click to add a new entry.

Apply – Click to save changes.

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

Messages:

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

The length of 'DES Privacy Password' is restricted to 8 - 32

Definitions:

MD5 (Message-Digest algorithm 5) is a message digest algorithm, used cryptographic hash function with a 128-bit hash value. It was designed by Ron Rivest in 1991. MD5 is officially defined in IETF RFC 1321 (the MD5 Message-Digest Algorithm).

SHA (Secure Hash Algorithm) was designed by the National Security Agency (NSA) and published by the NIST as a U.S. Federal Information Processing Standard. Hash algorithms compute a fixed-length digital representation (known as a message digest) of an input data sequence (the message) of any length.

DES (Data Encryption Standard) provides a complete description of a mathematical algorithm for encrypting (enciphering) and decrypting (deciphering) binary coded information. Encrypting data converts it to an unintelligible form called cipher. Decrypting cipher converts the data back to its original form called plaintext. The algorithm described in this standard specifies both enciphering and deciphering operations which are based on a binary number called a "key".

AES (Advanced Encryption Standard) is the encryption key protocol applied in the 802.1i standard to improve WLAN security. It is an encryption standard by the U.S. government, which will replace DES and 3DES. AES has a fixed block size of 128 bits and a key size of 128, 192, or 256 bits.

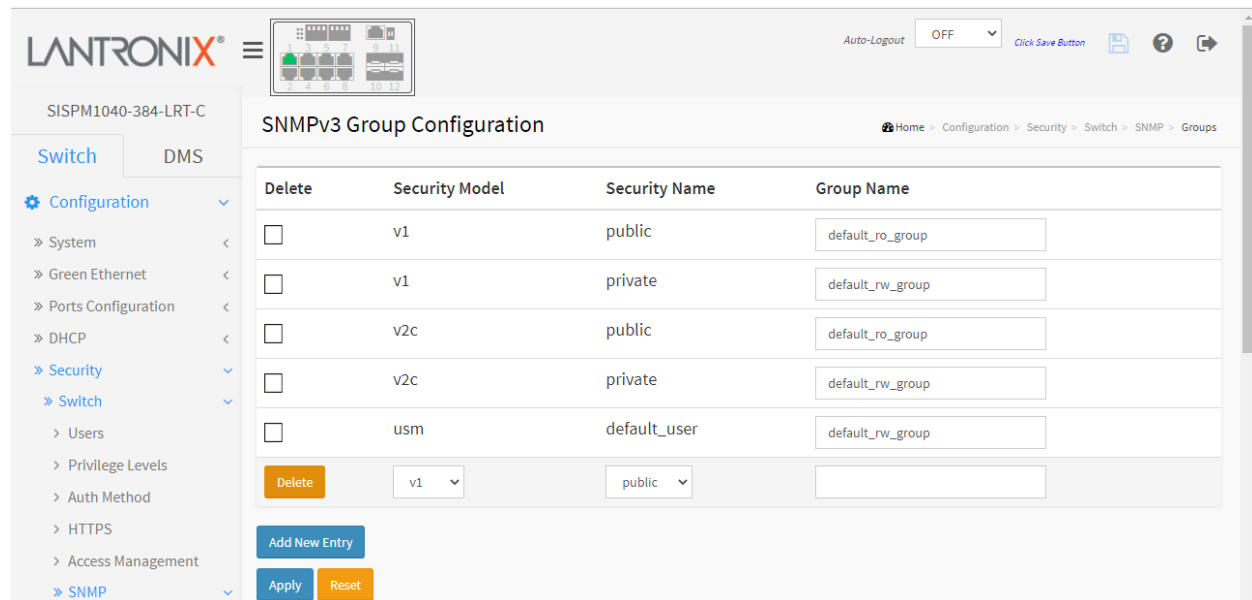
2-5.1.7.5 Group

This page lets you configure SNMPv3 Groups. The Entry index keys are Security Model and Security Name. To create a new group account, click the Add New Entry button, enter the group information, and then click the Apply button. Max Group number: **v1**: 2 groups max, **v2**: 2 groups max, **v3**: 10 groups max.

To configure SNMP Groups in the web UI:

1. Click Configuration, Security, Switch, SNMP, Groups.
2. Click the Add New Entry button.
3. Specify the privilege parameters.
4. Click Apply.

Figure 2-5.1.7.5: SNMP Group Configuration



Parameter descriptions:

Delete : Check to delete the entry immediately.

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

v1: Reserved for SNMPv1.

v2c: Reserved for SNMPv2c.

usm: User-based Security Model (USM).

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

Buttons:

Delete: Click to delete an existing entry.

Add New Entry – Click to add a new row to the table.

Apply – Click to save changes.

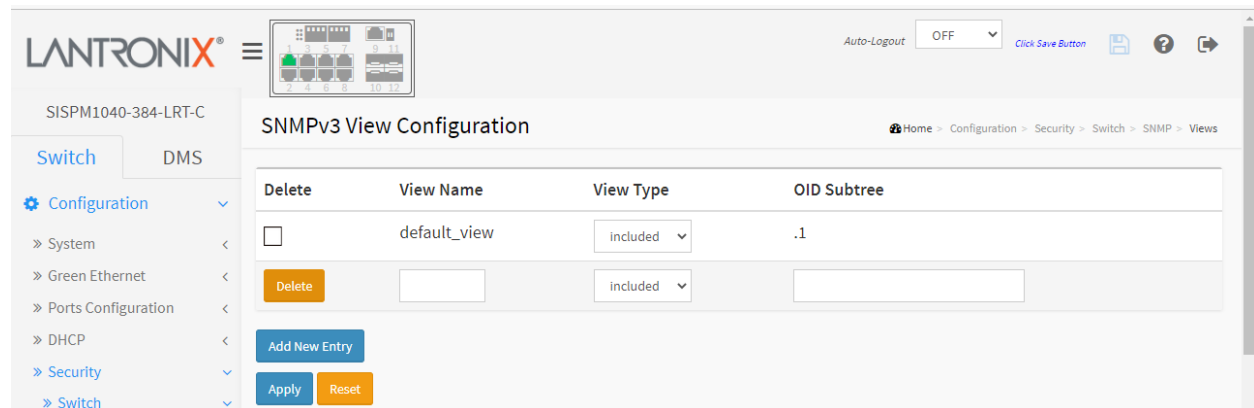
Reset- Click to undo any changes made locally and revert to previously saved values.

2-5.1.7.6 Views

This page lets you configure a maximum of 14 SNMP Views. The entry index keys are View Name and OID Subtree. To configure SNMP views in the web UI:

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

Figure 2-5.1.7.6: SNMPv3 Views Configuration



Parameter descriptions:

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

View Name : A string identifying the view name that this entry should belong to. The allowed string length is 1 – 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 to 128. The allowed string content is digital number or asterisk (*).

Buttons:

Add New Entry – Click to add a new entry.

Apply – Click to save changes.

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

2-5.1.7.7 Access

This page lets you configure SNMPv3 accesses. The Entry index key are Group Name, Security Model and Security level. You can enter a maximum of 14 SNMP Access Groups.

To create a new SNMP Access account in the web UI:

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

Figure 2-5.1.7.7: SNMPv3 Access Configuration

Delete	Group Name	Security Model	Security Level	Read View Name	Write View Name
<input type="checkbox"/>	default_ro_group	any	NoAuth, NoPriv	default_view	None
<input type="checkbox"/>	default_rw_group	any	NoAuth, NoPriv	default_view	default_view

Buttons: Delete, Add New Entry, Apply, Reset

Parameter descriptions:

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

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

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

Any: Any security model accepted(v1|v2c|usm).

v1: Reserved for SNMPv1.

v2c: Reserved for SNMPv2c.

usm: User-based Security Model (USM).

Security Level : Indicates the security model that this entry should belong to. Possible security levels are:

NoAuth, NoPriv: No authentication and no privacy.

Auth, NoPriv: Authentication and no privacy.

Auth, Priv: Authentication and privacy.

Read View Name : The name of the MIB view defining the MIB objects for which this request may request the current values. The allowed string length is 1 to 32 ASCII characters from 33 to 126.

Write View Name : The name of the MIB view defining the MIB objects for which this request may potentially set new values. The allowed string length is 1 to 32 ASCII characters from 33 to 126.

2-5.1.8 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.

2-5.1.8.1 Statistics

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

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

Figure 2-5.1.8.1: RMON Statics Configuration

Delete	ID	Data Source
<input type="checkbox"/>	1	.1.3.6.1.2.1.2.2.1.1. <input type="text" value="1"/>
<input type="checkbox"/>	2	.1.3.6.1.2.1.2.2.1.1. <input type="text" value="2"/>
<input type="checkbox"/>	3	.1.3.6.1.2.1.2.2.1.1. <input type="text" value="3"/>

Buttons: Add New Entry, Apply, Reset

Parameter descriptions: These parameters are displayed on the RMON Statistics Configuration page:

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

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

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

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

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

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

Buttons:

Add New Entry – Click to add a new entry.

Apply – Click to save changes.

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

2-5.1.8.2 History

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

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

Figure 2-5.1.8.2: RMON History Configuration

Delete	ID	Data Source	Interval	Buckets	Buckets Granted
<input type="checkbox"/>	1	.1.3.6.1.2.1.2.2.1.1. 1	1825	45	45
<input type="checkbox"/>	2	.1.3.6.1.2.1.2.2.1.1. 2	1750	52	50

Parameter descriptions: These parameters are displayed on the RMON History Configuration page:

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

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

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

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

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

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

Buttons:

Add New Entry – Click to add a new entry.

Apply – Click to save changes.

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

2-5.1.8.3 Alarm

Configure the RMON Alarm parameters on this page. The entry index key is **ID**. To display and configure RMON Alarm in the web UI:

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

Figure 2-5.1.8.3: RMON Alarm Configuration



Parameter descriptions:

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

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:

Add New Entry – Click to add a new entry.

Apply – Click to save changes.

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

Messages:

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

invalid 'datasource', invalid llag

'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

2-5.1.8.4 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, Event.
2. Click Add New Entry.
3. Specify the ID parameters.
4. Click Apply.

Figure 2-5.1.8.4: RMON Event Configuration

Delete	ID	Desc	Type	Community	Event Last Time
<input type="checkbox"/>	1	one	log	public	0
<input type="checkbox"/>	2	two	snmptrap	public	0
<input type="checkbox"/>	3	three	logandtrap	public	0
<input type="checkbox"/>			none	public	0

Buttons: Add New Entry, Apply, Reset

Parameter descriptions:

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

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

Desc : Describes this event; the string length is 0 – 127 and the default is a null string.

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

None: No SNMP log is created; an SNMP trap is sent.

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

Snmp trap: Send SNMP trap when the event is triggered.

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

Community : Specify the community when trap is sent; the string length is 0 – 127; the default is "public".

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

Buttons:

Add New Entry – Click to add a new entry.

Apply – Click to save changes.

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

2-5.2 Network

2-5.2.1 Limit Control

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

To configure System Configuration of Limit Control in the web UI:

1. Navigate to Configuration > Security > Network > Limit Control.
2. Select "Enabled" at the Mode dropdown.
3. Check Aging Enabled.
4. Set Aging Period (the default is 3600 seconds).

To configure Port Configuration of 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).
4. Click Apply.

Figure 2-5.2.1: Port Security Limit Control Configuration

The screenshot displays the 'Port Security Limit Control Configuration' web interface. It is divided into two main sections: 'System Configuration' and 'Port Configuration'.

System Configuration:

- Mode:** Enabled (dropdown menu)
- Aging Enabled:**
- Aging Period:** 3600 seconds

Port Configuration:

Port	Mode	Limit	Action	State	Re-open	Sticky	Clear
*	«»	4	«»			«»	
1	Enabled	4	None	Ready	Reopen	Enabled	Clear
2	Enabled	4	None	Ready	Reopen	Enabled	Clear
3	Enabled	4	None	Ready	Reopen	Enabled	Clear
4	Enabled	4	None	Ready	Reopen	Enabled	Clear
5	Enabled	4	None	Ready	Reopen	Enabled	Clear
6	Enabled	4	None	Ready	Reopen	Enabled	Clear
7	Enabled	4	None	Ready	Reopen	Enabled	Clear
8	Enabled	4	None	Ready	Reopen	Enabled	Clear
9	Enabled	4	None	Limit Reached	Reopen	Enabled	Clear
10	Enabled	4	None	Ready	Reopen	Enabled	Clear
11	Enabled	4	None	Ready	Reopen	Enabled	Clear
12	Enabled	4	None	Ready	Reopen	Enabled	Clear

At the bottom of the Port Configuration table, there are 'Apply' and 'Reset' buttons.

System Configuration

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

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 a number between 10 and 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

The table has one row for each port on the selected switch and a number of columns, which are:

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

Mode : Controls whether Limit Control is enabled on this port. Both Port Mode and 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 Shutdown or Trap & Shutdown.

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

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 to be static MAC addresses on the MAC table. (Added at FW v 7.10.1863.)

Clear : Click to clear the static MAC addresses added by the Sticky function. (Added at FW v 7.10.1863.)

Buttons:

Refresh: Click to manually refresh the page information immediately.

Apply: Click to save changes.

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

2-5.2.2 NAS

This page lets you configure the IEEE 802.1X and MAC-based authentication system and port settings.

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

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

NAS configuration consists of two sections: a system-level section and a port-level section.

Web Interface

1. Disable spanning tree.
2. Navigate to Configuration > Security > Network > NAS.
3. Set the System Configuration section parameters.
4. Set the Port Configuration section parameters and click Apply.

Figure 2-5.2.2: Network Access Server Configuration

Port	Admin State	RADIUS-Assigned QoS Enabled	RADIUS-Assigned VLAN Enabled	Guest VLAN Enabled	Port State	Restart
*	Force Authorized	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>		
1	Force Authorized	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Authorized	Reauthenticate Reinitialize
2	Force Authorized	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Authorized	Reauthenticate Reinitialize
3	Force Authorized	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Link Down	Reauthenticate Reinitialize
4	Force Authorized	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Authorized	Reauthenticate Reinitialize

Parameter descriptions:

System Configuration section

Mode : Select if NAS is globally enabled or disabled on the switch. If globally disabled, all ports are allowed to forward frames.

Reauthentication Enabled : If checked, successfully authenticated supplicants/clients are reauthenticated after the interval specified by the Reauthentication Period. Reauthentication for 802.1X-enabled ports can be used to detect if a new device is plugged into a switch port or if a supplicant is no longer attached.

For MAC-based ports, reauthentication is only useful if the RADIUS server configuration has changed. It does not involve communication between the switch and the client, and therefore doesn't imply that a client is still present on a port (see Aging Period below).

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

EAPOL Timeout : Determines the time for retransmission of Request Identity EAPOL frames. Valid values are in the range 1 to 255 seconds. This has no effect for MAC-based ports.

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

Single 802.1X

Multi 802.1X

MAC-Based Auth.

When the NAS module uses the Port Security module to secure MAC addresses, the Port Security module needs to check for activity on the MAC address in question at regular intervals and free resources if no activity is seen within a given period of time. This parameter controls exactly this period and can be set to a number between 10 and 1000000 seconds.

If reauthentication is enabled and the port is in an 802.1X-based mode, this is not so critical, since supplicants that are no longer attached to the port will get removed upon the next re-authentication, which will fail. But if re-authentication 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 Un-authorized 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.

Port Configuration section : The section has one row for each port on the selected switch and several columns, which are:

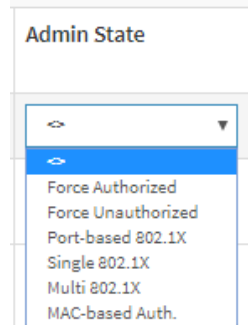
Port : The port number for which the configuration below applies.

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



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



NOTE: Suppose two backend servers are enabled and that the server timeout is configured to X seconds (using the AAA configuration page), and suppose that the first server in the list is currently down (but not considered dead).

Now, if the supplicant retransmits EAPOL Start frames at a rate faster than X seconds, then it will never get authenticated, because the switch will cancel on-going backend authentication server requests whenever it receives a new EAPOL Start frame from the supplicant.

And since the server hasn't yet failed (because the X seconds haven't expired), the same server will be contacted upon the next backend authentication server request from the switch. This scenario will loop forever. Therefore, the server timeout should be smaller than the supplicant's EAPOL Start frame retransmission rate.

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

the first one considered. If that supplicant doesn't provide valid credentials within a certain amount of time, another supplicant will get a chance. Once a supplicant is successfully authenticated, only that supplicant will be allowed access. This is the most secure of all the supported modes. In this mode, the Port Security module is used to secure a supplicant's MAC address once successfully authenticated.

Multi 802.1X: In port-based 802.1X authentication, once a supplicant is successfully authenticated on a port, the whole port is opened for network traffic. This allows other clients connected to the port (for instance through a hub) to piggy-back on the successfully authenticated client and get network access even though they really aren't authenticated. To overcome this security breach, use the Multi 802.1X variant.

Multi 802.1X is really not an IEEE standard, but features many of the same characteristics as does port-based 802.1X. Multi 802.1X is - like Single 802.1X - not an IEEE standard, but a variant that features many of the same characteristics. In Multi 802.1X, one or more supplicants can get authenticated on the same port at the same time. Each supplicant is authenticated individually and secured in the MAC table using the Port Security module.

In Multi 802.1X it is not possible to use the multicast BPDU MAC address as destination MAC address for EAPOL frames sent from the switch towards the supplicant, since that would cause all supplicants attached to the port to reply to requests sent from the switch. Instead, the switch uses the supplicant's MAC address, which is obtained from the first EAPOL Start or EAPOL Response Identity frame sent by the supplicant. An exception to this is when no supplicants are attached. In this case, the switch sends EAPOL Request Identity frames using the BPDU multicast MAC address as destination - to wake up any supplicants that might be on the port.

The maximum number of supplicants that can be attached to a port can be limited using the Port Security Limit Control functionality.

MAC-based Auth.: Unlike port-based 802.1X, MAC-based authentication is not a standard, but merely a best-practices method adopted by the industry. In MAC-based authentication, users are called clients, and the switch acts as the supplicant on behalf of clients. The initial frame (any kind of frame) sent by a client is snooped by the switch, which in turn uses the client's MAC address as both username and password in the subsequent EAP exchange with the RADIUS server. The 6-byte MAC address is converted to a string on the following form "xx-xx-xx-xx-xx-xx", that is, a dash (-) is used as separator between the lower-cased hexadecimal digits. The switch only supports the MD5-Challenge authentication method, so the RADIUS server must be configured accordingly.

When authentication is complete, the RADIUS server sends a success or failure indication, which in turn causes the switch to open up or block traffic for that particular client, using the Port Security module. Only then will frames from the client be forwarded on the switch. There are no EAPOL frames involved in this authentication, and therefore, MAC-based Authentication has nothing to do with the 802.1X standard.

The advantage of MAC-based authentication over port-based 802.1X is that several clients can be connected to the same port (e.g. through a 3rd party switch or a hub) and still require individual authentication, and that the clients don't need special supplicant software to authenticate. The advantage of MAC-based authentication over 802.1X-based authentication is that the clients don't need special supplicant software to authenticate. The disadvantage is that MAC addresses can be spoofed by malicious users - equipment whose MAC address is a valid RADIUS user can be used by anyone. Also, only the MD5-Challenge method is supported. The maximum number of clients that can be attached to a port can be limited using the Port Security Limit Control functionality.

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

Port-based 802.1X
Single 802.1X

RADIUS attributes used in identifying a QoS Class:

Refer to the written documentation for a description of the RADIUS attributes needed in order to successfully identify a QoS Class. The User-Priority-Table attribute defined in IETF [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' - '3', which translates into the desired QoS Class in the range [0; 3].

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 and Single 802.1X.

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

RADIUS attributes used in identifying a VLAN ID:

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 have the same Tag value and fulfil the following requirements (if Tag == 0 is used, the Tunnel-Private-Group-ID does not need to include a Tag):
 - Value of Tunnel-Medium-Type must be set to "IEEE-802" (ordinal 6).
 - Value of Tunnel-Type must be set to "VLAN" (ordinal 13).
 - Value of Tunnel-Private-Group-ID must be a string of ASCII chars in the range '0' - '9', which is interpreted as a decimal string representing the VLAN ID. Leading '0's are discarded. The final value must be in the range [1; 4095].

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

This option is only available for EAPOL-based modes, i.e., Port-based 802.1X, Single 802.1X, and 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 transmissions of EAPOL Request Identity frames is configured with EAPOL Timeout. If Allow Guest VLAN if EAPOL Seen is enabled, the port will now be placed in the Guest VLAN. If disabled, the switch will first check its history to see if an EAPOL frame has previously been received on the port (this history is cleared if the port link goes down or the port's Admin State is changed), and if not, the port will be placed in the Guest VLAN. Otherwise it will not move to the Guest VLAN, but continue transmitting EAPOL Request Identity frames at the rate given by EAPOL Timeout.

Once in the Guest VLAN, the port is considered authenticated, and all attached clients on the port are allowed access on this VLAN. The switch will not transmit an EAPOL Success frame when entering the Guest VLAN. While in the Guest VLAN, the switch monitors the link for EAPOL frames, and if one such frame is received, the switch immediately takes the port out of the Guest VLAN and starts authenticating the supplicant according to the port mode. If an EAPOL frame is received, the port will never be able to go back into the Guest VLAN if the "Allow Guest VLAN if EAPOL Seen" is disabled.

Port State : The current state of the port. It can undertake one of the following values:

Globally Disabled: 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:

Re-authenticate button: Click to schedule a re-authentication whenever the quiet-period of the port runs out (EAPOL-based authentication). For MAC-based authentication, re-authentication will be attempted immediately. The button only has effect for successfully authenticated clients on the port and will not cause the clients to get temporarily unauthorized.

Reinitialize button: Click to force a re-initialization of the clients on the port and thereby a re-authentication immediately. The clients will transfer to the unauthorized state while the re-authentication is in progress.

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

2-5.2.3 ACL

The switch Access Control List (ACL) 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. Here we will just go over the standard and extended access lists for TCP/IP. As you create ACEs for ingress classification, you can assign a policy for each port (1-8), however; each policy can be applied to any port. This makes it easy to determine what type of ACL policy you will be working with.

2-5.2.3.1 Ports

This page lets you configure ACL parameters (ACE) of each switch port. These parameters will affect frames received on a port unless the frame matches a specific ACE.

To configure ACL Ports in the web UI:

1. Click Configuration, Security, Network, ACL, then Ports.
2. Scroll the specific parameter value to select the correct value for port ACL setting.
3. Click the Apply button to save the setting.
4. To cancel the settings, click the Reset button to revert to previously saved values.
5. After you complete configuration, view the port Counters. Then click Refresh to update the counters or click Clear to clear the information.

Figure 2-5.2.3.1: ACL Ports Configuration

Port	Policy ID	Action	Rate Limiter ID	EVC Policer	EVC Policer ID	Port Redirect	Mirror	Logging	Shutdown	State	Counter
*	0	Deny	Deny	Deny	1	Disabled - Port 1 Port 2	Deny	Deny	Deny	Deny	*
1	0	Permit	Disabled	Disabled	1	Disabled - Port 1 Port 2	Disabled	Disabled	Disabled	Enabled	1298
2	0	Permit	Disabled	Disabled	1	Disabled - Port 1 Port 2	Disabled	Disabled	Disabled	Enabled	17197
3	0	Permit	Disabled	Disabled	1	Disabled - Port 1 Port 2	Disabled	Disabled	Disabled	Enabled	0
4	0	Permit	Disabled	Disabled	1	Disabled - Port 1 Port 2	Disabled	Disabled	Disabled	Enabled	973
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

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".

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".

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

Apply – Click to save changes.

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

Refresh: Click to immediately refresh the page manually.

Clear : Click to immediately clear the page manually.

Messages:

The parameter of 'Port Redirect' can't be set when action is permitted

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

2-5.2.3.2 Rate Limiters

This page lets you configure switch ACL Rate Limiter parameters.

1. Click Configuration, Security, Network, ACL, Rate Limiters.
2. Specify the Rate field (0 to 3276700).
3. Select the Unit of measure (pps or kbps).
4. Click the Apply button to save the settings.

Figure 2-5.2.3.2: ACL Rate Limiter Configuration

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"/>

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, ..., 1000000 in kbps.

Unit : The Unit of measure (pps or kbps).

Buttons

Apply – Click to save changes.

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

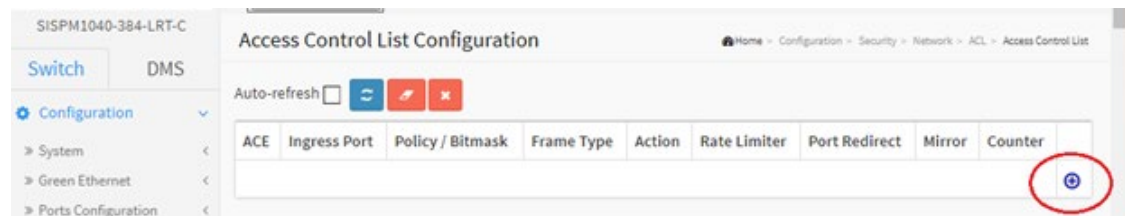
2-5.2.3.3 Access Control List

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


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

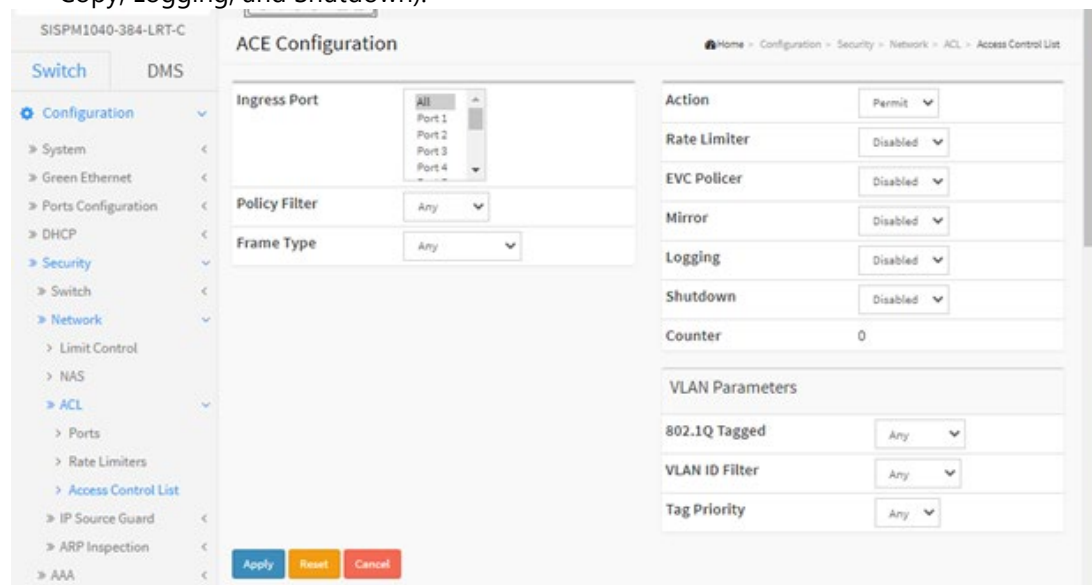
Configure an ACE (Access Control Entry) on this page. An ACE consists of several parameters. These parameters vary according to the frame type that you select. First select the ingress port for the ACE, and then select the frame type. Different parameter options are displayed depending on the frame type selected. A frame that hits this ACE matches the configuration that is defined here.

The initial Configuration > Security > Network > ACL > Access Control List page is shown below:



To configure Access Control List in the web UI:

1. Click Configuration, Security, Network, ACL, then Access Control List.
2. Click the  button to display the ACE Configuration page (shown below).
3. Specific the ACE configuration parameters.
4. Click the Apply button to save the settings.
5. When editing an entry on the ACE Configuration page, note that the parameters displayed depend on various selections, such as Frame Type and IP Protocol Type. Specify the relevant criteria 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).

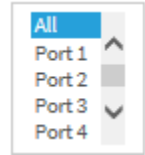


Parameter descriptions:

Ingress Port : 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, and include:

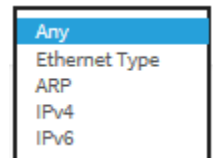
Any: Any frame can match this ACE.

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.

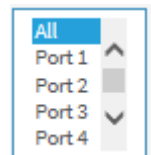
Deny: The frame that hits this ACE is dropped.

Filter: Frames matching the ACE are filtered.

Filter Port : When Action is set to 'Filter' select All port filters or select a specific port.

Rate Limiter : Specify the rate limiter in number of base units. The allowed range is **1** to **16**.

Disabled indicates that the rate limiter operation is disabled.



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 the values **1** through **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.

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



: Inserts a new ACE before the current row.



: Edits the ACE row.



: Moves the ACE up the list.



: Moves the ACE down the list.



: Deletes the ACE.



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

VLAN Parameters

802.1Q Tagged : Specify whether frames can hit the action according to the 802.1Q tagged. The allowed values are:

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

Enabled: Tagged frame only.

Disabled: Untagged frame only.

VLAN Parameters	
802.1Q Tagged	Any <input type="checkbox"/>
VLAN ID Filter	Any <input type="checkbox"/>
Tag Priority	Any <input type="checkbox"/>

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").

MAC Parameters:

SMAC Filter : (Only displayed when the frame type is Ethernet Type or ARP.) Specify the source MAC filter for this ACE.

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

Specific: To filter a specific source MAC address with this ACE, choose this value. A field for entering an SMAC value appears.

SMAC Value : When "Specific" is selected for the SMAC filter, you can enter a specific source MAC address. The legal format is "xx-xx-xx-xx-xx-xx" or "xx.xx.xx.xx.xx.xx" or "xxxxxxxxxxxx" (x is a hexadecimal digit). A frame that hits this ACE matches this SMAC value.

DMAC Filter : Specify the destination MAC filter for this ACE.

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

MC: Frame must be multicast.

BC: Frame must be broadcast.

UC: Frame must be unicast.

Specific: To filter a specific destination MAC address with this ACE. 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.

IP Parameters : The IP parameters can be configured when Frame Type "IPv4" is selected.

IP Protocol Filter : Specify the IP protocol filter for this ACE.

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

Specific: If you want to filter a specific IP protocol filter with this ACE, choose this value. A field for entering an IP protocol filter appears.

ICMP: Select ICMP to filter IPv4 ICMP protocol frames. Extra fields for defining ICMP parameters will appear. These fields are explained later in this manual.

UDP: Select UDP to filter IPv4 UDP protocol frames. Extra fields for defining UDP parameters will appear. These fields are explained later in this manual.

TCP: Select TCP to filter IPv4 TCP protocol frames. Extra fields for defining TCP parameters will appear. These fields are explained later in this manual.

IP Protocol Value : When "Specific" is selected for the IP protocol value, you can enter a specific value. The 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 invalid IP address will explicitly adding 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 in this manual.

UDP: Select UDP to filter IPv6 UDP protocol frames. Extra fields for defining UDP parameters will appear. These fields are explained later in this manual.

TCP: Select TCP to filter IPv6 TCP protocol frames. Extra fields for defining TCP parameters will appear. These fields are explained later in this manual.

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

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

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

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

SIP Address : When "Specific" is selected for the source IPv6 filter, you can enter a specific SIPv6 address. The field only supported last 32 bits for IPv6 address.

SIP BitMask : When "Specific" is selected for the source IPv6 filter, you can enter a specific SIPv6 mask. The field only supported last 32 bits for IPv6 address. Notice the usage of bitmask, if the binary bit value is "0", it means this bit is "don't-care". The real matched pattern is [sipv6_address & sipv6_bitmask] (last 32 bits). For example, if the SIPv6 address is 2001::3 and the SIPv6 bitmask is 0xFFFFFFE(bit 0 is "don't-care" bit), then SIPv6 address 2001::2 and 2001::3 are applied to this rule.

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

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

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

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

ICMP Parameters

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

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

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

ICMP Type Value : When "Specific" is selected for the ICMP filter, you can enter a specific ICMP value. The 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 PSH field is set must not be able to match this entry.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Cancel : Return to the previous page.

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

2-5.2.4 IP Source Guard

This section lets you configure detailed IP Source Guard parameters of the switch.

2-5.2.4.1 Configuration

This page lets you configure IP Source Guard setting including Mode (Enabled and Disabled) and Maximum Dynamic Clients (0, 1, 2, Unlimited). To configure IP Source Guard in the web UI:

1. Navigate to Configuration > Security > Network > IP Source Guard > Configuration.
2. Select "Enabled" in the Mode of IP Source Guard Configuration.
3. Select "Enabled" of the specific port in the Mode of Port Mode Configuration.
4. Select Maximum Dynamic Clients (0, 1, 2, Unlimited) of the specific port in the Mode of Port Mode Configuration.
5. Click Apply.

Figure 2-5.2.4.1: IP Source Guard Configuration

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

Parameter descriptions:

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

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

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

Buttons

Apply: Click to save changes.

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

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

2-5.2.4.2 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. This page shows the static IP Source Guard rules. The maximum number of rules is 112 per switch.

To configure Static IP Source Guard in the web UI:

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

Figure 2-5.2.4.2: Static IP Source Guard Table

The screenshot shows the Lantronix web interface for configuring the Static IP Source Guard Table. The page title is "Static IP Source Guard Table" and the breadcrumb trail is "Home > Configuration > Security > Network > IP Source Guard > Static Table". The interface includes a navigation menu on the left with "Configuration" expanded to show "Security" and "Switch". The main content area features a table with the following columns: Delete, Port, VLAN ID, IP Address, and MAC address. The table contains one entry with Port 1, VLAN ID 100, IP Address 192.168.1.90, and MAC address 11-22-33-44-55-66. Below the table are buttons for "Add New Entry", "Apply", and "Reset".

Delete	Port	VLAN ID	IP Address	MAC address
<input type="checkbox"/>	1	100	192.168.1.90	11-22-33-44-55-66
<input type="button" value="Delete"/>	2			

Parameter descriptions:

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

Port : The logical port for the settings.

VLAN ID : The VLAN id for the settings.

IP Address : Allowed Source IP address.

MAC address : Allowed Source MAC address.

Buttons:

Add New Entry : Click to add a new entry to the Static IP Source Guard table. Specify the Port, VLAN ID, IP address, and IP Mask for the new entry. Click the Apply button.

Apply – Click to save changes.

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

2-5.2.5 ARP Inspection

This page lets you configure the ARP Inspection parameters of the switch. ARP Inspection is a security feature. Several types of attacks can be launched against a host or devices connected to Layer 2 networks by "poisoning" the ARP caches. This feature is used to block such attacks. Only valid ARP requests and responses can go through the switch device.

2-5.2.5.1 Port Configuration

This page lets you configure ARP Inspection settings including Mode (Enabled and Disabled) and Port (Enabled and Disabled). To configure ARP Inspection in the web UI:

1. Navigate to Configuration > Security > Network > ARP Inspection > Port Configuration.
2. Select "Enabled" in the Mode of ARP Inspection Configuration.
3. Select "Enabled" for the specific port in the Mode of Port Mode Configuration.
4. Click Apply.

Figure 2-5.2.5.1: ARP Inspection Configuration

The screenshot shows the LANTRONIX web interface for ARP Inspection Configuration. The breadcrumb trail is: Home > Configuration > Security > Network > ARP Inspection > Port Configuration. The 'Mode' is currently set to 'Disabled'. A button labeled 'Translate dynamic to static' is present. Below this is the 'Port Mode Configuration' table:

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

Parameter descriptions:

Mode of ARP Inspection Configuration : Enable or disable ARP Inspection globally.

Port Mode Configuration

Mode: 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 "Check VLAN". The default is disabled. When "Check VLAN" is disabled, the log type of ARP Inspection will refer to the port setting. And if the setting of "Check VLAN" is enabled, the log type of ARP Inspection will refer to the VLAN setting. Possible setting of are:

Enabled: Enable check VLAN operation.

Disabled: Disable check VLAN operation.

Only when the Global Mode and Port Mode on a given port are enabled, and the setting of "Check VLAN" is disabled, the log type of ARP Inspection will refer to the port setting. The four log types are:

None: Log nothing.

Deny: Log denied entries.

Permit: Log permitted entries.

ALL: Log all entries.

Buttons:

Apply: Click to save changes.

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

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

2-5.2.5.2 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 uses the next entry of the currently displayed VLAN entry as a basis for the next lookup. When the end is reached a warning message is displayed in the table. Use the << button to start over.

To configure VLAN Mode in the web UI:

1. Navigate to Configuration > Security > Network > ARP Inspection > VLAN Configuration.
2. Click the Add New Entry button.
3. Specify the VLAN ID and Log Type.
4. Click Apply.

Figure 2-5.2.5.2: VLAN Mode Configuration

The screenshot displays the 'VLAN Mode Configuration' web page. At the top, there's a navigation breadcrumb: Home > Configuration > Security > Network > ARP Inspection > VLAN Configuration. Below this, there are navigation buttons: a refresh icon, a left arrow, and a right arrow. The main configuration area includes a 'Start from VLAN' field set to '1' and an 'entries per page' field set to '20'. A table lists existing VLAN configurations:

Delete	VLAN ID	Log Type
<input type="checkbox"/>	100	Deny
<input type="checkbox"/>	200	Permit
<input type="checkbox"/>	300	All
<input type="checkbox"/>	400	None

Below the table, there is a 'Delete' button, an 'Add New Entry' button, and 'Apply' and 'Reset' buttons. The 'Log Type' for the new entry is currently set to 'None'.

Parameter descriptions:

VLAN Mode Configuration : Specify ARP Inspection is enabled on which VLANs. First, you must enable the port setting on Port mode configuration web page. Only when both Global Mode and Port Mode on a given port are enabled, ARP Inspection is enabled on this given port. You can also specify which VLAN will be inspected on VLAN mode configuration web page. The log type also can be configured per VLAN setting. Possible Log types are:

None: Log nothing.

Deny: Log denied entries.

Permit: Log permitted entries.

ALL: Log all entries.

Buttons

: **Refresh**; click to update webpage information.



: **First entry**; click to go back to the first entry.



: **Next entry**; click to go to the next entry.

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.

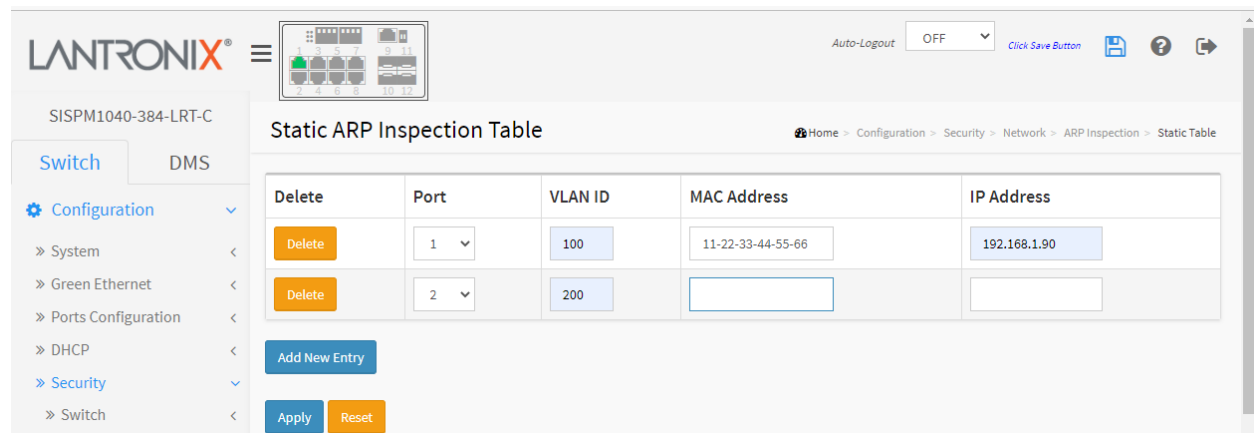
2-5.2.5.3 Static Table

This page lets you configure the Static ARP Inspection Table parameters of the switch. You can use the Static ARP Inspection table configure to manage 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 the Add New Entry button.
3. Specify the Port, VLAN ID, IP Address, and MAC address in the entry.
4. Click Apply.

Figure 2-5.2.5.3: Static ARP Inspection Table



Parameter descriptions:

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

Port : The logical port for the settings.

VLAN ID : The VLAN ID for the settings.

MAC Address : Allowed Source MAC address in ARP request packets.

IP Address : Allowed Source IP address in ARP request packets.

Buttons:

Add New Entry : Click to add a new entry to the Static ARP Inspection table.

Apply – Click to save changes.

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

2-5.2.5.4 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 via 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.

Figure 2-5.2.5.4: Dynamic ARP Inspection Table

The screenshot shows the Lantronix web interface for configuring the Dynamic ARP Inspection Table. The page title is "Dynamic ARP Inspection Table". The breadcrumb trail is "Home > Configuration > Security > Network > ARP Inspection > Dynamic Table". The configuration area includes an "Auto-refresh" checkbox and navigation buttons (refresh, back, forward). The "Start from" section has input fields for "Port" (set to Port 1), "VLAN" (set to 1), "MAC address" (set to 00-00-00-00-00-00), and "IP address" (set to 0.0.0.0), with a "20" entries per page field. Below this is a "System Configuration" table with columns: Port, VLAN ID, MAC Address, IP Address, and Translate to static. The table currently displays "No more entries". There are "Apply" and "Reset" buttons at the bottom.

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 a static entry.

Buttons:

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.

Apply – Click to save changes.

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

2-5.3 AAA

This page lets you to use an AAA (Authentication, Authorization, and Accounting) server to provide access control to your network. The AAA server can be a TACACS+ or RADIUS server.

2-5.3.1 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 RADIUS server parameters via the web UI:

1. Click Configuration, Security, AAA, and RADIUS.
2. Click the Add New Server button.
3. Specify the Global Configuration and Server Configuration parameters and click Apply.

Figure 2-5.3.1: RADIUS Server Configuration

The screenshot shows the 'RADIUS Server Configuration' page in the Lantronix web interface. The page is divided 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]
- NAS-IPv6-Address:** [Empty]
- NAS-Identifier:** [Empty]

Server Configuration:

Delete	Hostname	Auth Port	Acct Port	Timeout	Retransmit	Key
<input type="button" value="Delete"/>	[Empty]	1812	1813	[Empty]	[Empty]	[Empty]

Below the table are three buttons: 'Add New Server', 'Apply', and 'Reset'.

Parameter descriptions:

Global Configuration: These settings are common for 1-5 RADIUS servers.

Timeout: Timeout is the number of seconds, in the range 1 - 1000, to wait for a reply from a RADIUS server before retransmitting the request.

Retransmit : Retransmit is the number of times, in the range 1 - 1000, a RADIUS request is retransmitted to a server that is not responding. If the server has not responded after the last retransmit it is considered to be dead.

Deadtime : Deadtime, which can be set to 0 - 1440 minutes, is the period during which the switch will not send new requests to a server that has failed to respond to a previous request. This will stop the switch from continually trying to contact a server that it has already determined as dead. Setting the Deadtime to a value greater than 0 (zero) will enable this feature, but only if more than one server has been configured.

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

NAS-IP-Address (Attribute 4) : The IPv4 address to be used as attribute 4 in RADIUS Access-Request packets. If this field is left blank, the IP address of the outgoing interface is used.

NAS-IPv6-Address (Attribute 95) : The IPv6 address to be used as attribute 95 in RADIUS Access-Request packets. If this field is left blank, the IP address of the outgoing interface is used.

NAS-Identifier (Attribute 32) : The identifier - up to 255 characters long - to be used as attribute 32 in RADIUS Access-Request packets. If this field is left blank, the NAS-Identifier is not included in the packet.

Server Configuration: The table has one row for each RADIUS server and several columns:

Delete : To delete a RADIUS server entry, check this box. The entry will be deleted during the next Save.

Hostname : The IPv4 or IPv6 address or hostname of the RADIUS server.

Auth Port : The UDP port to use on the RADIUS server for authentication. Set to 0 to disable authentication.

Note: UDP port values of 1812 for authentication and 1813 for accounting are RADIUS standard ports defined by IETF [RFC 2865](#) and [RFC 2866](#). However, by default, many access servers use UDP ports 1645 for authentication requests and 1646 for accounting requests.

Acct Port : The UDP port to use on the RADIUS server for accounting. Set to 0 to disable accounting.

Timeout : This optional setting overrides the global timeout value. Leaving it blank will use the global timeout value.

Retransmit : This optional setting overrides the global retransmit value. Leaving it blank will use the global retransmit value.

Key : This optional setting overrides the global key. Leaving it blank will use the global key.

Buttons

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 (11111111) is not a valid 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 RFC2865. See your RADIUS server documents for more information.

Example:

Global Configuration

Timeout	5	seconds
Retransmit	3	times
Deadtime	0	minutes
Key	51164fc2a4b5e52f	
NAS-IP-Address	192.168.1.30	
NAS-IPv6-Address		
NAS-Identifier	admin	

Server Configuration

Delete	Hostname	Auth Port	Acct Port	Timeout	Retransmit	Key
<input type="checkbox"/>	RadSrvr1	1812	1813	60	350	admin
<input type="checkbox"/>	RadSrvr2	1812	1813	45	222	superuser1!2@3*
<input type="checkbox"/>	radius3	1812	1813	1	99	*****
<input type="checkbox"/>	radius4	1812	1813	1	9	obvious
<input type="checkbox"/>	radius5	1645	1646	2	2	777777-+*****

Buttons: Add New Server, Apply, Reset

2-5.3.2 TACACS+

TACACS+ (Terminal Access Controller Access Control System Plus) is a network protocol that 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. Up to five TACACS+ servers are supported.

To configure a TACACS+ server via the web UI:

1. Click Configuration, Security, AAA, and TACACS+.
2. Click the **Add New Server** button.
3. Specify the Global Configuration and Server Configuration parameters.
4. Click **Apply**.

Figure 2-5.3.2: TACACS+ Authentication Server Configuration

The screenshot shows the web interface for configuring TACACS+ servers. The breadcrumb trail is Home > Configuration > Security > AAA > TACACS+. The 'Global Configuration' section has the following fields:

Timeout	5	seconds
Deadtime	0	minutes
Key	*****	

The 'Server Configuration' section is a table with the following structure:

Delete	Hostname	Port	Timeout	Key
<input type="checkbox"/>		49		

Buttons at the bottom include 'Add New Server', 'Apply', and 'Reset'.

Parameter descriptions:

Global Configuration : These settings are common for all of the TACACS+ servers.

Timeout : Timeout is the number of seconds, in the range 1 - 1000, to wait for a reply from a TACACS+ server before it is considered to be dead. The default is 5 seconds.

Deadtime : Deadtime, which can be set to a number between 0 to 1440 minutes, is the period during which the switch will not send new requests to a server that has failed to respond to a previous request. This will stop the switch from continually trying to contact a server that it has already determined as dead. Setting the Deadtime to a value greater than 0 (zero) will enable this feature, but only if more than one server has been configured. The default is 0 minutes.

Key : The secret key - up to 63 characters long - shared between the TACACS+ server and the switch.

Server Configuration : The table has one row for each TACACS+ server and several columns, which are:

Delete : To delete a TACACS+ server entry, check this box. The entry will be deleted during the next Save.

Hostname : The IP address or hostname of the TACACS+ server.

Port : The TCP port to use on the TACACS+ server for authentication. The default is TCP port 49.

Timeout : This optional setting overrides the global timeout value. Leaving it blank will use the global timeout value. 'Timeout' must be an integer value of 1 - 1000 seconds.

Key : This optional setting overrides the global key. Leaving it blank will use the global key (up to FW v7.10.2368). The encrypted secret key - up to 63 characters long – is shared between the TACACS+ server and the switch (FW v7.10.2368 and above).

Buttons

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 five TACACS+ servers are supported. The Reset button can be used to undo the addition of the new server.

Apply: Click to save changes.

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

Messages:

Authentication Error – HTTPD cache has no valid entry

Example:

The screenshot displays the 'TACACS+ Server Configuration' page. On the left is a navigation menu with 'Switch' selected and 'DMS' as an alternative. The main content area is divided into 'Global Configuration' and 'Server Configuration'.

Global Configuration:

- Timeout:** 5 seconds
- Deadtime:** 0 minutes
- Key:** [Redacted]

Server Configuration Table:

Delete	Hostname	Port	Timeout	Key
<input type="checkbox"/>	TacSrvr1	49	60	[Redacted]
<input type="checkbox"/>	[Redacted]	49	[Redacted]	[Redacted]

Buttons at the bottom include 'Add New Server', 'Apply', and 'Reset'.

2-6 Aggregation

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 has.

Note that LACP and Static aggregation cannot both be enabled on the same ports.

2-6.1 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 aggregate together to form a "logic trunked port". Using Static Trunk on both ends of a link is strongly recommended. Also note that low speed links will stay in the "not ready" state when using static trunk to aggregate with high speed links.

To configure Aggregation via 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 and click the Apply button to save the settings.

Figure 2-6.1: Aggregation Mode Configuration

The screenshot displays the 'Aggregation Mode Configuration' web interface. On the left is a navigation menu with 'Switch' selected and 'DMS' as an option. Under 'Configuration', 'Aggregation' is expanded to show 'Static'. The main content area is titled 'Aggregation Mode Configuration' and includes a breadcrumb trail: Home > Configuration > Aggregation > Static.

The 'Hash Code Contributors' section contains the following settings:

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"/>

The 'Aggregation Group Configuration' section features a table for selecting port members:

Group ID	Port Members											
	1	2	3	4	5	6	7	8	9	10	11	12
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"/>	<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"/>	<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"/>	<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"/>	<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"/>	<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"/>	<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"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

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

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 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.

2-6.2 LACP

This page lets you view and configure 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.

To configure Trunk Aggregation LACP parameters in the web UI:

1. Click Configuration, Aggregation, LACP.
2. Enable or disable the LACP on the port of the switch.
3. At the Key dropdown select Auto or Specific. The default is Auto.
4. At the Role dropdown select Active or Passive. The default is Active.
5. At the Timeout dropdown select Fast or Slow. The default is Fast.
6. At the Prio dropdown select the priority of the port. The default is 32768.
7. Click the Apply button to save the settings.

Figure 2-6.2: LACP Port Configuration

Port	LACP Enabled	Key	Role	Timeout	Prio
*	<input checked="" type="checkbox"/>	<>	<>	<>	32768
1	<input checked="" type="checkbox"/>	Auto	Active	Fast	32768
2	<input checked="" type="checkbox"/>	Auto	Active	Fast	32768
3	<input checked="" type="checkbox"/>	Auto	Active	Fast	32768
4	<input checked="" type="checkbox"/>	Auto	Active	Fast	32768
5	<input checked="" type="checkbox"/>	Auto	Active	Fast	32768
6	<input checked="" type="checkbox"/>	Auto	Active	Fast	32768
7	<input checked="" type="checkbox"/>	Auto	Active	Fast	32768
8	<input checked="" type="checkbox"/>	Auto	Active	Fast	32768
9	<input checked="" type="checkbox"/>	Auto	Active	Fast	32768
10	<input checked="" type="checkbox"/>	Auto	Active	Fast	32768
11	<input checked="" type="checkbox"/>	Auto	Active	Fast	32768
12	<input checked="" type="checkbox"/>	Auto	Active	Fast	32768

Parameter descriptions:

Port : The switch port number.

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

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

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

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

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

2-6.2 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 switch models have the same behavior when using the LACP protocol with this kind of application.

To ping or access for 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 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	
1	Port 9	192.168.1.79	192.168.1.99
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 lead 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.

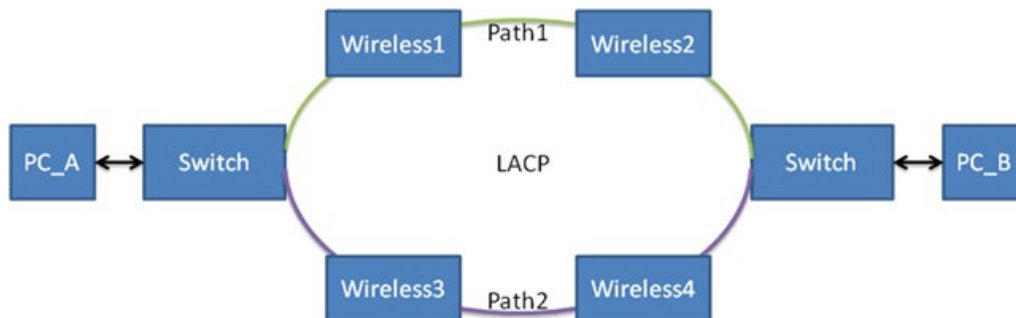
Message: *LACP Error - LACP and Static aggregation can not both be enabled on the same ports*

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.

2-7 Link OAM

2-7.1 Port Settings

This page lets you view and configure the current Link OAM port parameters. To configure LOAM Port Settings in the web UI:

1. Click Configuration, Link OAM and Port Settings.
2. For each Port select Link OAM parameters.
3. Click the Apply button to save the settings.

Figure 2-7.1: LOAM Port Configuration

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"/>

Parameter descriptions:

Port : The switch port number. You can click the linked number to display that port's Detailed Link OAM Status page.

OAM Enabled : Controls whether Link OAM is enabled on this switch port. Enabling Link OAM provides 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: 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: 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 shall not 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 MIB Retrieval is enabled for the switch port. On enabling the MIB retrieval support, the DTE supports polling of various Link OAM based MIB variables' contents. You can retrieve the local or remote OAM MIB variable data on a particular port at Diagnostics > Link OAM > MIB Retrieval.

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.

Messages

Message: *Error requested configuration is not supported with the current OAM mode*

Meaning: You tried to save an invalid Link OAM port configuration at Configuration > Link OAM > Port Settings.

Recovery: **1.** Click the **Previous** button to return to the previous page. **2.** Make sure you have made a valid configuration in terms of OAM Mode, Loopback Support, Link Monitor Support, MIB Retrieval Support, and Loopback Operation. **3.** Continue operation.

Message: *OAM Error Invalid request on this port*

Meaning: You tried to save an invalid Link OAM port configuration at Configuration > Link OAM > Port Settings.

Recovery: **1.** Click the **Previous** button to return to the previous page. **2.** Make sure you have made a valid configuration in terms of OAM Mode, Loopback Support, Link Monitor Support, MIB Retrieval Support, and Loopback Operation. **3.** Continue operation.

2-7.2 Event Settings

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

1. Click Configuration, Link OAM and Event Settings.
2. Select a Port.
3. Enter the Error Window and Threshold parameters.
4. Click the Apply button to save the settings.

Figure 2-7.2: Link Event Configuration

The screenshot shows the 'Link Event Configuration for Port 1' page. On the left is a navigation menu with 'Link OAM' selected. The main content area has a breadcrumb trail: Home > Configuration > Link OAM > Event Settings. Below the breadcrumb is a dropdown menu for 'Port 1'. A table with three columns: 'Event Name', 'Error Window', and 'Error Threshold'. The table contains three rows of data:

Event Name	Error Window	Error Threshold
Error Frame Event	<input type="text" value="1"/>	<input type="text" value="1"/>
Symbol Period Error Event	<input type="text" value="1"/>	<input type="text" value="1"/>
Seconds Summary Event	<input type="text" value="60"/>	<input type="text" value="1"/>

At the bottom of the table are 'Apply' and 'Reset' buttons.

Parameter descriptions:

Port : At the dropdown select the switch port number.

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

Error Window : Represents the window period in the order of 1 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 : The Errored 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 : The Errored Symbol Period 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 default value is '1'. Whereas 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'. Whereas 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.

Messages

Message: Error While Configuring Link Events

Recovery: **1.** Click the **Previous** button to clear the message. **2.** Re-enter valid the Error Window and Threshold parameters. **3.** Continue operation.

2-8 Loop Protection

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

To configure Loop Protection parameters in the web UI:

1. Click Configuration, Loop Protection.
2. In the Global Configuration section Enable or disable port Loop Protection and set the Transmission and Shutdown times.
3. In the Port Configuration section set the Enable, Action, and Tx Mode parameters for each port.
4. Click the Apply button to save the settings.

Figure 2-8: Loop Protection Configuration

The screenshot displays the 'Loop Protection Configuration' page in the Lantronix web UI. The page is titled 'Loop Protection Configuration' and shows the following configuration details:

Global Configuration

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

Port Configuration

Port	Enable	Action	Tx Mode
*	<input checked="" type="checkbox"/>	<>	<>
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

Parameter descriptions:

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

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

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

Port: The switch port number of the port.

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

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

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

Buttons:

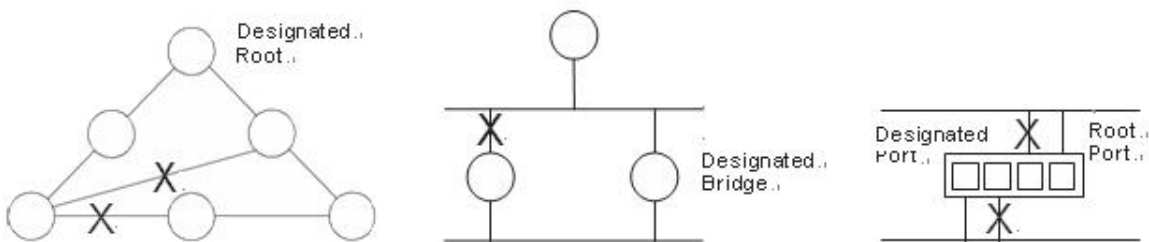
Apply – Click to save changes.

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

2-9 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 (e.g., an STP-compliant switch, bridge or router) in your network to ensure that only one route exists between any two stations on the network, and provide backup links which automatically take over when a primary link goes down.

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



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.

2-9.1 Bridge Settings

This page lets you set Spanning Tree Bridge and STP System parameters. It allows you to configure STP System settings used by all STP Bridge instance in the switch.

Web Interface

To configure Spanning Tree Bridge parameters in the web UI:

1. Click Configuration, Spanning Tree, Bridge Settings.
2. Select the parameters at the dropdowns and enter parameters in the blank fields
3. Enable or disable the parameters and enter parameters in blank fields.
4. Click the Apply button to save the settings.
5. To cancel the settings, click the Reset button to revert to previously saved values.

Figure 2-9.1: STP Bridge Configuration

The screenshot displays the 'STP Bridge Configuration' page in the Lantronix web interface. The page is titled 'STP Bridge Configuration' and includes a breadcrumb trail: Home > Configuration > Spanning Tree > Bridge Settings. The interface is divided 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 'Apply' and 'Reset' buttons.

Parameter descriptions:

Basic Settings

Protocol Version : The STP protocol version setting. Valid values are STP, RSTP and MSTP.

STP: Spanning Tree Protocol is an OSI layer-2 protocol which ensures a loop free topology for any bridged LAN. The original STP protocol is now obsolete by RSTP.

RSTP: In 1998, the IEEE with document 802.1w introduced an evolution of STP: the Rapid Spanning Tree Protocol, which provides for faster spanning tree convergence after a topology change. Standard IEEE 802.1D-2004 now incorporates RSTP and obsoletes STP, while at the same time being backwards-compatible with STP.

MSTP: In 2002, the IEEE introduced an evolution of RSTP: the Multiple Spanning Tree Protocol. The MSTP protocol provides for multiple spanning tree instances, while ensuring RSTP and STP compatibility. The standard was originally defined by IEEE 802.1s, but was later incorporated in IEEE 802.1D-2005.

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 in the range 4 to 30 seconds.

Max Age : The maximum age of the information transmitted by the Bridge when it is the Root Bridge. Valid values are in the range 6 to 40 seconds, and MaxAge must be $\leq (\text{FwdDelay}-1)*2$.

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 in the range 1 to 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 have to be disabled and re-enabled for normal STP operation. The condition is also cleared by a system reboot.

Port Error Recovery Timeout : The time to pass before a port in the error-disabled state can be enabled. Valid values are 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.

2-9.2 MSTI Mapping

This page lets you view and configure the current STP MSTI bridge instance priority configurations. When you implement a Spanning Tree protocol on the switch that the bridge instance, the CIST is not available for explicit mapping, as it will receive the VLANs not explicitly mapped, due to the fact that you must set the list of VLANs mapped to the MSTI. The VLANs must be separated with a comma and/or space.

A VLAN can only be mapped to one MSTI. An unused MSTI should just be left empty (i.e., not having any VLANs mapped to it.)

To configure Spanning Tree MSTI Mapping parameters in the web UI:

1. Click Configuration, Spanning Tree, MSTI Mapping.
2. Specify the configuration name and revision in the fields. Specify the VLANs Mapped blank field(s).
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 2-9.2: MSTI Configuration

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". The configuration area is divided into two sections: "Configuration Identification" and "MSTI Mapping".

Configuration Identification

Configuration Name	<input type="text" value="00-c0-f2-49-be-22"/>
Configuration Revision	<input type="text" value="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"/>

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

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 : The bridge instance. The CIST is not available for explicit mapping, as it will receive the VLANs not explicitly mapped.

VLANs Mapped : The list of VLANs mapped to the MSTI. The VLANs can be given as a single (xx, xx being between 1 and 4094) VLAN, or a range (xx-yy), each of which must be separated with comma and/or space. A VLAN can only be mapped to one MSTI. An unused MSTI should just be left empty (i.e., not having any VLANs mapped to it.) Example: 2,5,20-40.

Message: *MSTx: VLAN y is already mapped to MST1.*

2-9.3 MSTI Priorities

This page lets you view and configure STP MSTI bridge instance priority parameters.

When you implement a Spanning Tree protocol on the switch that the bridge instance, you must configure the MSTI priority settings. The CIST is the default instance which is always active.

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

To configure Spanning Tree MSTI Priorities in the web UI:

1. Click Configuration, Spanning Tree, MSTI Priorities.
2. Select the desired Priority. The default is 32768.
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 2-9.3: MSTI Configuration

The screenshot displays the Lantronix web interface for configuring MSTI Priorities. The page title is "MSTI Configuration" and the breadcrumb is "Home > Configuration > Spanning Tree > MSTI Priorities". The main content area is titled "MSTI Priority Configuration" and contains a table with columns "MSTI" and "Priority". The table lists MSTI instances from * to MSTI17, each with a priority value of 32768. Below the table are "Apply" and "Reset" buttons. The left sidebar shows the navigation menu with "Spanning Tree" expanded to "MSTI Priorities".

MSTI	Priority
*	<> ▼
CIST	32768 ▼
MSTI1	32768 ▼
MSTI2	32768 ▼
MSTI3	32768 ▼
MSTI4	32768 ▼
MSTI5	32768 ▼
MSTI6	32768 ▼
MSTI7	32768 ▼

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.

2-9.4 CIST Ports

This page lets you view and configure current STP CIST port settings. When you implement a Spanning Tree protocol on the switch that is the bridge instance, you must configure the CIST Ports.

To configure Spanning Tree CIST Ports parameters in the web UI:

1. Click Configuration, Spanning Tree, CIST Port.
2. Set all CIST Aggregated Port Configuration parameters.
3. Enable or disable STP, then set all CIST Normal Port Configuration parameters.
4. Click Apply to save the settings.
5. To cancel the settings, click the Reset button to revert to previously saved values.

Figure 2-9.4: STP CIST Port Configuration

The screenshot displays the 'STP CIST Port Configuration' web interface. It is divided into two main sections:

- CIST Aggregated Port Configuration:** A single row with the following fields: Port (empty), STP Enabled (checkbox), Path Cost (Auto), Priority (128), Admin Edge (Non-Edge), Auto Edge (checked), Role (checkbox), TCN (checkbox), BPDU Guard (checkbox), and Point-to-point (Forced True).
- CIST Normal Port Configuration:** A table with 12 rows, one for each port (1-12). Each row contains: Port, STP Enabled (checkbox), Path Cost (Auto), Priority (128), Admin Edge (Non-Edge), Auto Edge (checked), Role (checkbox), TCN (checkbox), BPDU Guard (checkbox), and Point-to-point (Auto).

At the bottom of the table are 'Apply' and 'Reset' buttons.

Parameter descriptions:

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

STP Enabled : Controls whether STP is enabled on this switch port.

Path Cost : Controls the path cost incurred by the port. The Auto setting will set the path cost as appropriate by the physical link speed, using the 802.1D recommended values. Using the Specific setting, a user-defined value can be entered. The path cost is used when establishing the active topology of the network. Lower path cost ports are chosen as forwarding ports in favor of higher path cost ports. Valid values are in the range 1 to 200000000.

Priority : Controls the port priority. This can be used to control priority of ports having identical port cost (see above).

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.

2-9.5 MSTI Ports

This page lets you view and configure current 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. The MSTI instance 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, MSTI Ports.
2. Scroll to select the MST1 or other MSTI Port.
3. Click the Get button to display MSTI Ports detailed parameters.
4. Set the MSTI Port Configuration parameters.
5. Click the Apply button to save the settings.

Figure 2-9.5: MSTI Port Configuration

STP CIST Port Configuration Home > Configuration > Spanning Tree > MSTI Ports

Select MSTI

MST1

STP MSTI Port Configuration Home > Configuration > Spanning Tree > MSTI Ports

MSTI Aggregated Ports Configuration

Port	Path Cost	Priority
-	Auto	128

MSTI Normal Ports Configuration - MST1

Port	Path Cost	Priority
*	∞	∞
1	Auto	128
10	Auto	128
11	Auto	128
12	Auto	128

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 in the range 1 to 200000000.

Priority : Controls the port priority. This can be used to control priority of ports having identical port cost (see above).

Buttons

Select MSTI : At the dropdown select an MSTI.

Get : Click to set the detail parameters of the selected MSTI ports.

Apply – Click to save changes.

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

2-10 IPMC Profile

This page provides IPMC Profile related configurations.

2-10.1 Profile Table

The IPMC profile is used to deploy the access control on IP multicast streams. You can create up to 64 Profiles and up to 128 corresponding rules for each Profile.

To configure IPMC Profile Configuration in the web UI:



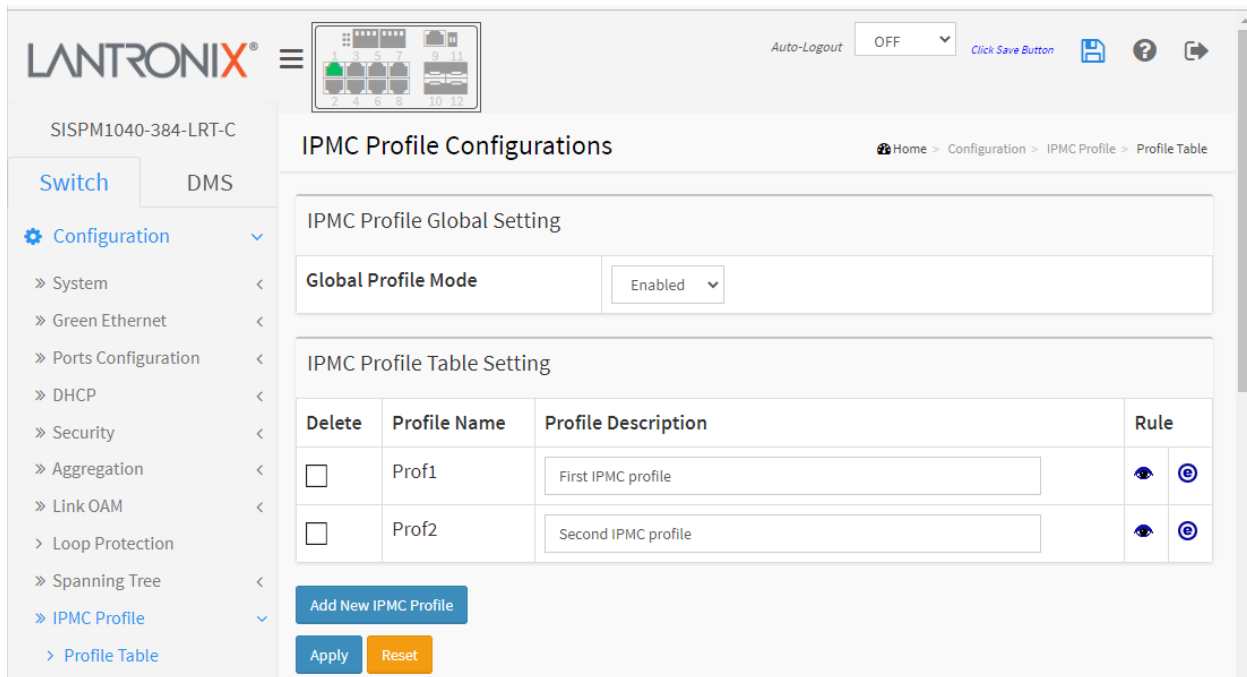




1. Click Configuration, IPMC Profile, Profile Table.
2. Enable or disable the Global IPMC Profile parameter.
3. Click the Add New IPMC Profile button to display the IPMC Profile Table.
4. Click the  button to list the rules associated with the designated profile.
5. Click the  button to adjust the rules associated with the designated profile.
6. Click the Add Last Rule button.
7. Commit
8. Click Apply.

Figure 2-10.1: IPMC Profile Configurations



The screenshot shows the web interface for configuring IPMC profiles. The main content area is titled 'IPMC Profile Configurations' and includes a breadcrumb trail: Home > Configuration > IPMC Profile > Profile Table. Under 'IPMC Profile Global Setting', the 'Global Profile Mode' is set to 'Enabled'. Below this, the 'IPMC Profile Table Setting' section contains a table with two rows:

Delete	Profile Name	Profile Description	Rule
<input type="checkbox"/>	Prof1	First IPMC profile	 
<input type="checkbox"/>	Prof2	Second IPMC profile	 

At the bottom of the table, there is a blue 'Add New IPMC Profile' button, and below that, 'Apply' and 'Reset' buttons.

Parameter descriptions:

Global Profile Mode : Enable/Disable the Global IPMC Profile. The switch starts filtering based on profile settings only when the global profile mode is enabled.

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

Profile Name : The name used for indexing the profile table. Each entry has the unique name which is composed of at maximum 16 alphabetic and numeric characters. At least one alphabet character 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 sentence.

Rule : When the profile is created, click the edit button to enter the rule setting page of the designated profile. A summary about the designated profile will be shown by clicking the view button. You can manage or inspect the rules of the designated profile by using these buttons:



: List the rules associated with the designated profile.



: Adjust the rules associated with the designated profile.

Profile Name & Index : The Profile Name (e.g., ABC above) and Index ((e.g., 1 above).

Entry Name : Select an existing entry name at the dropdown.

Address Range : displays the configured IP address range or displays the ~ symbol if none are configured.

Action : At the dropdown select the Action to be performed (Deny or Permit).

Log : At the dropdown select to Enable or Disable logging.

Buttons

Add New IPMC Profile – Click to add a new IPMC profile. Specify the name and configure the new entry, then click the Apply button.

Apply – Click to save changes.

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

Add Last Rule : Click to add the last rule to the profile.

Commit : Click to commit the changes.

Modification Buttons

You can modify the table entries 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.

Messages:

Please input valid IPv4/IPv6 multicast start address for Entry Range1.

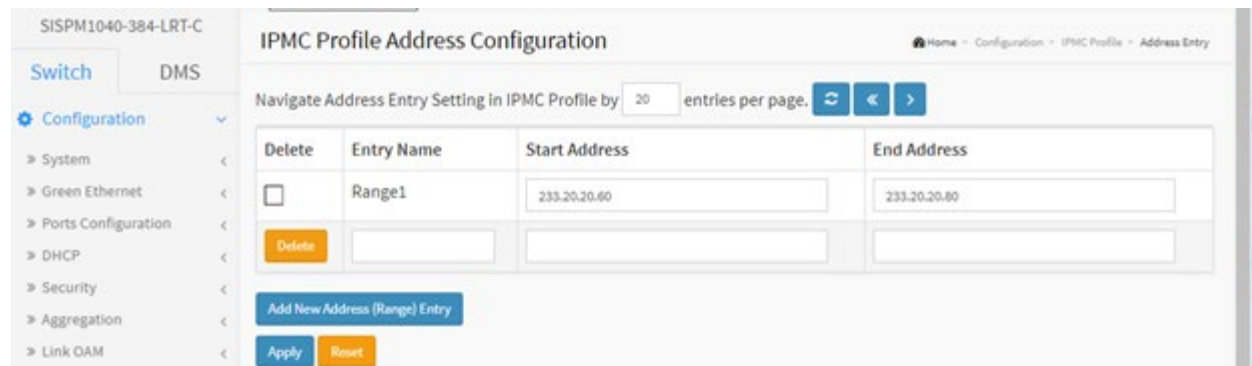
2-10.2 Address Entry

This page lets you set address ranges 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 Configuration in the web UI:

1. Click Configuration, IPMC Profile, Address Entry.
2. Specify the Entry Name, Start Address, and End Address.
3. Click Apply.

Figure 2-10.2: IPMC Profile Address Configuration



Parameter descriptions:

Delete : Check to delete the entry.

The designated entry will be deleted during the next save.

Entry Name : The name used for indexing the address entry table. Each entry has the unique name which is composed of at maximum 16 alpha 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

Add New Address (Range) Entry – Click to add new address range. Specify the name and configure the addresses. Click "Apply"

Apply – Click to save changes.

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

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.

2-11 MVR

The MVR feature enables multicast traffic forwarding on the Multicast VLAN. In a multicast television application, a PC or a television with a set-top box can receive the multicast stream. Multiple set-top boxes or PCs can be connected to one subscriber port, which is a switch port configured as an MVR receiver port. When a subscriber selects a channel, the set-top box or PC sends an IGMP join message to Switch A to join the appropriate multicast. Uplink ports that send and receive multicast data to and from the multicast VLAN are called MVR source ports.

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 via the web UI:

1. Click Configuration > MVR > Configuration to display the MVR Configuration default page.
2. In the Global Setting section set the MVR Mode to Enabled .
3. Click the Add New MVR VLAN button and configure the VLAN Interface Setting parameters.
4. Click the Apply button to save the settings
5. To cancel the settings, click the Reset button to revert to previously saved values.

Figure 2-11a: MVR Configuration (default page)

The screenshot displays the MVR Configuration web interface. The 'Global Setting' section shows 'MVR Mode' set to 'Enabled'. Below this is a table for 'VLAN Interface Setting (Role: [Inactive / S:Source / R:Receiver])'. The table has columns for 'Delete', 'MVR VID', 'MVR Name', 'IGMP Address', 'Mode', 'Tagging', 'Priority', 'LLQI', and 'Interface Channel Profile'. A 'Add New MVR VLAN' button is located below the table. At the bottom, there is an 'Immediate Leave Setting' table with columns for 'Port' and 'Immediate Leave'.

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.

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

MVR VID : Specify the Multicast VLAN ID. **Caution:** MVR source ports are not recommended to be overlapped with the Management VLAN port.

MVR Name : An optional attribute to indicate the name of the specific MVR VLAN. Maximum length of the MVR VLAN Name string is 32. MVR VLAN Name can only contain alphabets or numbers. 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.

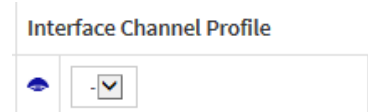
Mode : Specify the MVR mode of operation. In **Dynamic** mode, MVR allows dynamic MVR membership reports on source ports. In **Compatible** mode, MVR membership reports are forbidden on source ports. The default is **Dynamic** mode.

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 Profile : When the MVR VLAN is created, click the Edit symbol to expand the corresponding multicast channel settings for the specific MVR VLAN. A summary of 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 these roles.



Inactive: The designated port does not participate MVR operations.

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

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

Caution: MVR source ports are not recommended to be overlapped with management VLAN ports. Select the port role by clicking the Role symbol to switch the setting. I indicates Inactive; S indicates Source; R indicates Receiver. The default Role is Inactive.

Immediate Leave Setting : Enable the fast leave on the port.

Buttons

Add New MVR VLAN : Click to add a new MVR VLAN.

Apply: Click to save changes.

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

Figure 2-11b: MVR Configuration (configured page)

The screenshot displays the 'MVR Configurations' page in a web interface. On the left is a navigation menu with categories like Configuration, System, Green Ethernet, Ports Configuration, DHCP, Security, Aggregation, Link DM, 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, Mirroring, UPnP, PTP, GSRP, iFlow, UCLD, Rapid Ring, and SMTF. The main content area is titled 'MVR Configurations' and includes a breadcrumb 'Home > Configuration > MVR'. It is divided into three sections:

- Global Setting:** Contains a single field 'MVR Mode' 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. Two entries are shown:

Delete	MVR VID	MVR Name	IGMP Address	Mode	Tagging	Priority	LLQI	Interface Channel Profile
<input type="checkbox"/>	10	intMVR1	192.168.1.30	Dynamic	Tagged	0	1	
<input type="checkbox"/>	20	intMVR2	192.168.1.30	Dynamic	Tagged	0	1	
- Immediate Leave Setting:** A table with columns: Port and Immediate Leave.

Port	Immediate Leave
*	no
1	Disabled
2	Enabled
3	Enabled
4	Enabled
5	Enabled
6	Disabled
7	Disabled
8	Disabled

2-12 IPMC

ICMP (Internet Control Message Protocol) is a protocol that generated the error response, diagnostic or routing purposes. ICMP messages generally contain information about routing difficulties or simple exchanges such as time-stamp or echo transactions.

2-12.1 IGMP Snooping

This function is used to establish the multicast groups to forward the multicast packet to the member ports, and, in nature, avoids wasting the bandwidth while IP multicast packets are running over the network. This is because a switch that does not support IGMP or IGMP Snooping cannot tell the multicast packet from the broadcast packet, so it can only treat them all as the broadcast packet. Without IGMP Snooping, the multicast packet forwarding function is plain and nothing is different from broadcast packet.

A switch supported IGMP Snooping with the functions of query, report and leave, a type of packet exchanged between IP Multicast Router/Switch and IP Multicast Host, can update the information of the Multicast table when a member (port) joins or leaves an IP Multicast Destination Address. With this function, once a switch receives an IP multicast packet, it will forward the packet to the members who joined in a specified IP multicast group before.

The packets will be discarded by the IGMP Snooping if the user transmits multicast packets to the multicast group that had not been built up in advance. IGMP mode enables the switch to issue IGMP function that you enable IGMP proxy or snooping on the switch, which connects to a router closer to the root of the tree. This interface is the upstream interface. The router on the upstream interface must be running IGMP.

2-12.1.1 Basic Configuration

This section 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, Basic Configuration.
2. Enable or disable Global configuration.
3. Select the port you want to become a Router Port or enable/ disable the Fast Leave function.
4. Scroll to 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.

Figure 2-12.1.1: IGMP Snooping Configuration

Global Configuration	
Snooping Enabled	<input type="checkbox"/>
Unregistered IPMCv4 Flooding Enabled	<input checked="" type="checkbox"/>
IGMP SSM Range	232.0.0.0 / 8
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"/>	<- v
1	<input type="checkbox"/>	<input type="checkbox"/>	unlimited v
2	<input type="checkbox"/>	<input type="checkbox"/>	unlimited v
3	<input type="checkbox"/>	<input type="checkbox"/>	unlimited v
4	<input type="checkbox"/>	<input type="checkbox"/>	unlimited v
5	<input type="checkbox"/>	<input type="checkbox"/>	unlimited v
6	<input type="checkbox"/>	<input type="checkbox"/>	unlimited v
7	<input type="checkbox"/>	<input type="checkbox"/>	unlimited v
8	<input type="checkbox"/>	<input type="checkbox"/>	unlimited v

Parameter descriptions:**Global Configuration**

Snooping Enabled: Check to enable the IGMP Snooping globally.

Unregistered IPMCv4 Flooding Enabled : Check to 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 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 : Check to 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.

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.

2-12.1.2 VLAN Configuration

This page lets you configure VLAN parameters integrated with IGMP Snooping function. For each setting, the page shows up to 99 entries from the VLAN table (default is 20) selected through the "entries per page" input field. When first visited, the web page will show the first 20 entries from the beginning of the VLAN Table. The first displayed will be the one with the lowest VLAN ID found in the VLAN Table. The "VLAN" input fields let you select the starting point in the VLAN Table. Clicking the > button will update the displayed table starting from that or the next closest VLAN Table match.

To configure IGMP Snooping VLAN Configuration in the web UI:

1. Click Configuration, IPMC, IGMP Snooping, VLAN Configuration.
2. Click the Add New IGMP VLAN button.
3. Enable or disable Snooping, IGMP Querier. Specify the parameters in the blank field.
4. Click Refresh to update the data or click << or >> to display previous entry or next entry.
5. Click the Apply button to save the setting
6. To cancel the settings, click the Reset button to revert to previously saved values.

Figure 2-12.1.2: IGMP Snooping VLAN Configuration



Parameter descriptions:

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

VLAN ID : Displays the VLAN ID of the entry.

IGMP 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. When the Querier address is set, the system uses a pre-defined value. The default value is 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 selection is IGMP-Auto, Forced IGMPv1, Forced IGMPv2, Forced IGMPv3, default compatibility value is IGMP-Auto.

PRI : Priority of Interface. It indicates the IGMP control frame priority level generated by the system. These values can be used to prioritize different classes of traffic. The allowed range is 0 (best effort) to 7 (highest); the default PRI value is 0.

Rv : Robustness Variable. The Robustness Variable allows tuning for the expected packet loss on a network. The allowed range is 1 - 255; the default RV value is 2.

QI : Query Interval. The Query Interval is the interval between General Queries sent by the Querier. The allowed range is 1 to 31744 seconds; the default 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 to 31744 in tenths of seconds; the default LLQI is 10 in tenths of seconds (1 second).

URI : Unsolicited Report Interval; the time between repetitions of a host's initial report of membership in a group. The allowed range is 0 - 31744 seconds; the default URI is 1 second.

Buttons :

Add New IGMP VLAN - Click the button to add a new row to the table for configuration.

Apply – Click to save changes.

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

Refresh: Click 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, i.e. 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 set IGMP Port Group Filtering. In some network Application environments, such as metropolitan or multiple-dwelling unit (MDU) installations, you may want to control the multicast groups to which a user on a switch port can belong. This feature lets you 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 Profile parameters in the web UI:

1. Click Configuration, IPMC, IGMP Snooping, Port Filtering Profile.
2. Click the Filtering Profile icon.
3. At the dropdown, select the Filtering Profile.
4. Click the List Rules Profile Management button to display the IPMC Profile Rule Settings (In Precedence Order) for the profile.
5. Click the Apply button to save the settings.
6. To cancel the settings, click the Reset button to revert to previously saved values.

Figure 2-12.1.3: IGMP Snooping Port Filtering Profile Configuration

The screenshot displays the 'IGMP Snooping Port Filtering Profile Configuration' page. On the left is a navigation menu with 'Configuration' expanded to 'IGMP Snooping' and 'Port Filtering Profile' selected. The main area contains a table with the following data:

Port	Filtering Profile
1	-
2	Prof1
3	Prof2
4	Prof2
5	-
6	-
7	-
8	-
9	-
10	-
11	-

Parameter descriptions:

Port : The logical port for the settings.

Filtering Profile : Select the IPMC Profile as the filtering condition for the specific port. You can display a summary of the designated profile 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.

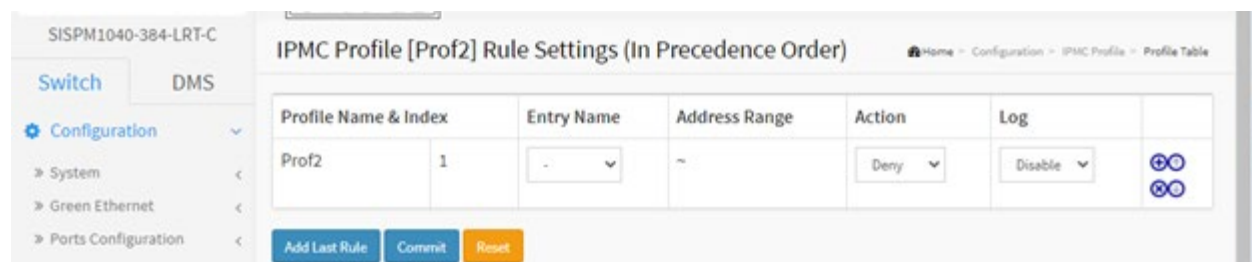
Buttons:

Apply – Click to save changes.

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

IPMC Profile [IpmcProf1] Rule Settings (In Precedence Order) page

Click the List Rules Profile Management button to display the IPMC Profile Rule Settings (In Precedence Order) for the profile. This page provides the filtering rule settings for a specific IPMC profile. It displays the configured rule entries in precedence order. First rule entry has highest priority in lookup, while the last rule entry has lowest priority in lookup.



Parameter descriptions:

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.

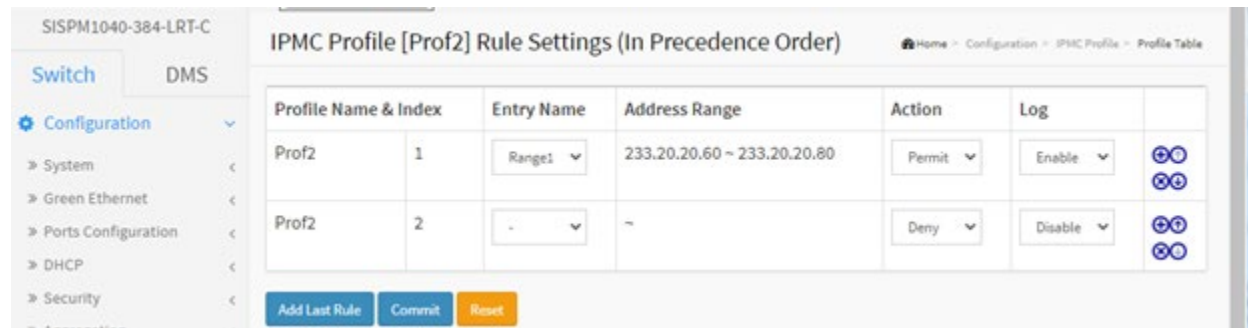
Buttons





Add New Address (Range) Entry : 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.

Apply: Click to commit rule changes for the designated profile.

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

Example:



Profile Name & Index	Entry Name	Address Range	Action	Log	
Prof2 1	Range1	233.20.20.60 ~ 233.20.20.80	Permit	Enable	 
Prof2 2	-	-	Deny	Disable	 

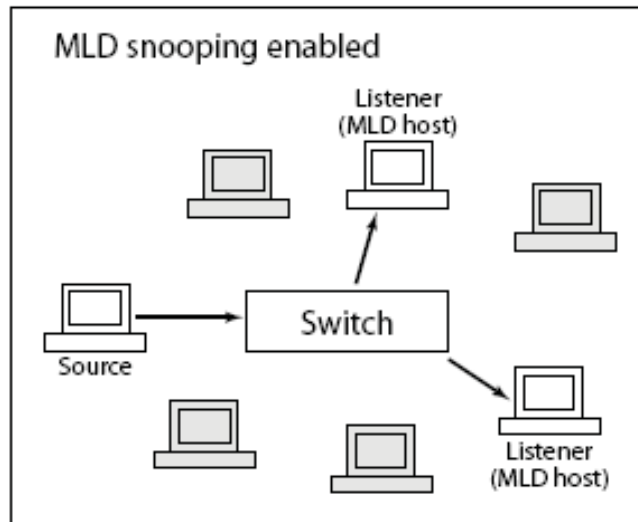
Buttons: Add Last Rule, Commit, Reset

2-12.2 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



2-12.2.1 Basic Configuration

This page lets you configure basic MLD Snooping parameters.

Web Interface

To configure MLD Snooping in the web UI:

1. Click Configuration, IPMC, MLD Snooping, Basic Configuration.
2. Enable or disable Global configuration parameters. Select the port to join Router port and Fast Leave.
3. Select the Throttling mode (unlimited or 1 - 10).
4. Click the Apply button to save the settings.
5. To cancel the setting click the Reset button to revert to previously saved values.

Figure 2-12.2.1: MLD Snooping Basic Configuration

Global Configuration

Snooping Enabled	<input type="checkbox"/>
Unregistered IPMCv6 Flooding Enabled	<input checked="" type="checkbox"/>
MLD SSM Range	#3e: / 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
8	<input type="checkbox"/>	<input type="checkbox"/>	unlimited
9	<input type="checkbox"/>	<input type="checkbox"/>	unlimited
10	<input type="checkbox"/>	<input type="checkbox"/>	unlimited
11	<input type="checkbox"/>	<input type="checkbox"/>	unlimited
12	<input type="checkbox"/>	<input type="checkbox"/>	unlimited

Apply Reset

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.

Fast Leave : To enable fast leave on the port.

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.

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.

2-12.2.2 VLAN Configuration

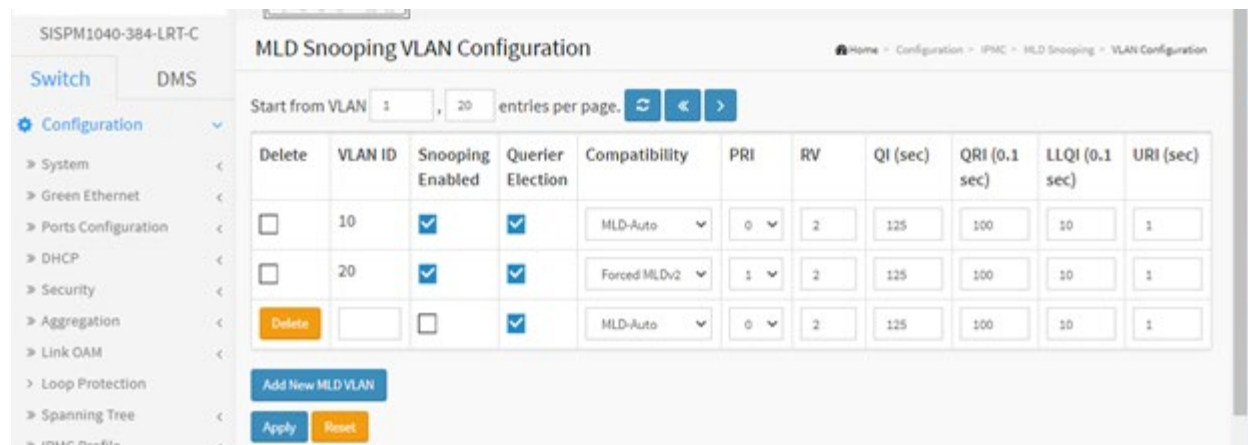
When MLD snooping is enabled on a VLAN, the switch acts to minimize unnecessary multicast traffic. If the switch receives multicast traffic destined for a given multicast address, it forwards that traffic only to ports on the VLAN that have MLD hosts for that address. It drops that traffic for ports 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 in the table. Use the > button to start over.

To configure MLD Snooping VLAN in the web UI:

1. Click Configuration, IPMC, MLD Snooping, VLAN Configuration
2. Specify the VLAN ID entries per page.
3. Click the Add New MLD VLAN button and configure the parameters.
4. Click Refresh to refresh an entry of the MLD Snooping VLAN Configuration table.
5. Click << or > to move to the previous or next entry.

Figure 2-12.2.2: MLD Snooping VLAN Configuration.



Parameter descriptions:

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

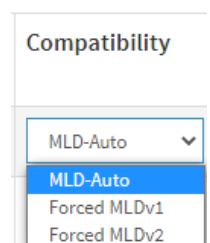
VLAN ID : It displays the VLAN ID of the entry.

Snooping Enabled : Enable per-VLAN MLD Snooping. Up to 32 VLANs can be configured.

Querier Election : Enable to join MLD 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 MLD-Auto, Forced MLDv1, Forced MLDv2. The default compatibility value is MLD-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; default robustness variable value is 2.

QI : Query Interval. The Query Interval is the interval between General Queries sent by the Querier. The allowed range is 1 to 31744 seconds; default query interval 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 query response interval is 100 in tenths of seconds (10 seconds).

LLQI (LMQI for IGMP) : Last Member Query Interval; the time value represented by the Last Member Query Interval, multiplied by the Last Member Query Count. The allowed range is 0 to 31744 in tenths of seconds; default last member query interval is 10 in tenths of seconds (1 second).

URI : Unsolicited Report Interval; the time between repetitions of a host's initial report of membership in a group. The allowed range is 0 to 31744 seconds; the default unsolicited report interval is 1 second.

Buttons :

Apply – Click to save changes.

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

Refresh: You can click 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 (i.e., the entry with the lowest VLAN ID).

> : Click to update the table, starting with the entry after the last entry currently displayed.

2-12.2.3 Port Group Filtering

This page lets you set the Port Group Filtering in the MLD Snooping function and add new filtering group and safety policy.

To configure the MLD Snooping Port Group Configuration in the web UI:

1. Click Configuration, IPMC, MLD Snooping, Port Filtering Profile.
2. Select the Filtering Profile at the dropdown.
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 2-12.2.3: MLD Snooping Port Filtering Profile Configuration


Port	Filtering Profile
1	-
2	IpmcProfile
3	IpmcProfile
4	IpmcProfile
5	-
6	-
7	-
8	-
9	-
10	-
11	-
12	-

Parameter descriptions:

Port : The logical port for the settings.

Filtering Profile : Select the IPMC Profile as the filtering condition for the specific port. A summary of the designated profile will display by clicking the View button.

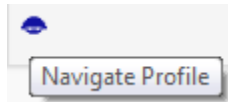
Profile Management Button : Click the View () button to inspect the rules of the designated profile:

 : 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.



: Click to navigate the Profile. This displays the “IPMC Profile [IpmcProf1] Rule Settings (In Precedence Order)” page (see below).

IPMC Profile [IpmcProf1] Rule Settings (In Precedence Order)

This page provides the filtering rule settings for a specific IPMC profile. It displays the configured rule entries in precedence order. First rule entry has highest priority in lookup, while the last rule entry has lowest priority in lookup.

Profile Name & Index	Entry Name	Address Range	Action	Log	
Prof1	1	a	233.20.20.60 ~ 233.20.20.80	Deny	Disable

Parameter descriptions:

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, and then 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.

2-13 LLDP

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

2-13.1 LLDP

This page lets you view and configure current LLDP parameters and port parameters. You can configure LLDP on a per-port and global basis and the settings will take effect immediately. To configure LLDP:

1. Click Configuration > LLDP > LLDP.
2. Modify the LLDP timing parameters.
3. Set the desired Mode for transmitting or receiving LLDP messages.
4. Enable or Disable CDP aware as required.
5. Specify the information to include in the TLV field of advertised messages and click Apply.

Figure 2-13.1: LLDP Configuration

The screenshot displays the LLDP Configuration page. On the left, a navigation menu shows 'Configuration' expanded to 'LLDP'. The main content area is titled 'LLDP Configuration' and contains two sections:

LLDP Parameters

Tx Interval	20	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 checked="" 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 checked="" 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 checked="" 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 checked="" 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 checked="" 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 checked="" 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 checked="" 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 checked="" 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 checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

Parameter descriptions:

LLDP Parameters

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

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

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

Optional TLVs

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.

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 LLDP 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 are 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.

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 of 0.0 is meaningful even outside a building and represents ground level at the given latitude and longitude. Inside a building, 0.0 represents the floor level associated with ground level at the main entrance.

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

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

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

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

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

Country code : The two-letter ISO 3166 [Country Code](#) in capital ASCII letters (e.g., 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
6. Control / Signalling (conditionally support a separate network policy for the media types above)

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

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

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

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

Application Type : Intended use of the application types:

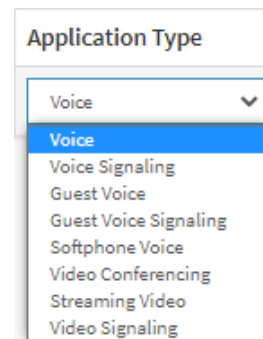
Voice - for use by dedicated IP Telephony handsets and other similar appliances supporting interactive voice services. These devices are typically deployed on a separate VLAN for ease of deployment and enhanced security by isolation from data applications.

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

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

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

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



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

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

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

Tag : 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 - 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 shall apply to a given port. The set of policies is selected by check marking the checkboxes that corresponds to the policies.

Buttons:

Add New Policy : Click to add a new policy. Specify the Application type, Tag, VLAN ID, L2 Priority and DSCP for the new policy. Click the Apply button.

Apply – Click to save changes.

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

2-14 PoE

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

See the Install Guide for PoE detection and troubleshooting information.

2- 14.1 Configuration

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

1. Click Configuration, PoE, and Configuration.
2. Specify Reserved Power determined by, Power Management Mode, and Capacitor Detection.
3. Specify PoE Mode, Schedule, Priority, and Maximum Power for each port.
4. Click Apply.

Figure 2-14.1: PoE Configuration

The screenshot shows the Lantronix web interface for PoE configuration. The breadcrumb trail is Home > Configuration > PoE > Configuration. The page is divided into several sections:

- Reserved Power determined by:** Radio buttons for Class, Allocation (selected), and LLDP-Med.
- Power Management Mode:** Radio buttons for Actual Consumption (selected) and Reserved Power.
- Capacitor Detection:** A checkbox that is currently unchecked.
- PoE Power Supply Configuration:** A text input field for Primary Power Supply [W] with the value 240.
- PoE Port Configuration:** A table with 5 columns: Port, PoE Mode, PoE Schedule, Priority, and Maximum Power [W].

Port	PoE Mode	PoE Schedule	Priority	Maximum Power [W]
*	↔	↔	↔	40
1	Enabled	Disabled	Critical	40
2	Enabled	Disabled	High	40
3	Enabled	Disabled	High	40
4	Enabled	Disabled	High	40
5	Enabled	Disabled	Low	40
6	Enabled	Disabled	Low	40
7	Enabled	Disabled	Low	40
8	Enabled	Disabled	Low	40

At the bottom of the table are 'Apply' and 'Reset' buttons.

Parameter descriptions:

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

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

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

LLDP-MED: This mode is similar to the Class mode expect that each port determines the amount power it reserves by exchanging PoE information using the LLDP protocol and reserves power accordingly. If no LLDP information is available for a port, the port will reserve power using Class mode. In LLDP-MED mode the Maximum Power fields have no effect for all modes; if a port uses more power than the reserved power for the port, the port is shut down.

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

Actual Consumption: In this mode the ports are shut down when the actual power consumption for all ports exceeds the amount of power that the power supply can deliver or if the actual power consumption for a given port exceeds the reserved power for that port. The ports are shut down according to the port's priority. If two ports have the same priority, then 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 : Checkbox to enable or disable Capacitor Detection mode. 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.

Primary Power Supply (W) : Some switches support having two PoE power supplies (Primary and Backup). One is used as primary power source, and one as backup power source. If the switch doesn't support the backup power supply, then only the primary power supply settings will be shown. In case that the primary power source fails, then the backup power source will take over. For being able to determine the amount of power the PD may use, you must define the amount of power the primary and backup power sources can deliver. The default is 240 Watts.

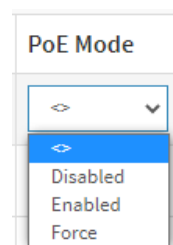
Port : This is the logical port number for this row. Ports that are not PoE-capable are grayed out and thus impossible to configure PoE for.

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

Disabled: PoE disabled for the port (default).

Enabled: PoE enabled for the port.

Force: The switch port will power up the linked PD without any detect/negotiate mechanism (PD limited to 40W). **Note:** Only connect PDs which support a power input of 48~56V to prevent damage to PDs. When the port changes to Force mode, the port's PoE LED will light immediately. Select Force mode for devices that do not do POE negotiation (e.g., for a PoE DSRC RSU).



PoE Schedule : Select the PoE scheduler – Enabled or Disabled. The default is Disabled. See the “PoE Schedule Profile” page below for schedule parameters.

Priority : The Priority represents the ports priority. There are three levels of power priority (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 turn off starting from the port with the highest port number.

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

Note: Firmware v 7.10.1237 added the PoE Force Mode feature. **Note:** only connect PDs which support power input in the range of 48~56V to prevent damage to PDs.

Firmware v7.10.1269 ~ v7.10.1329 sets the maximum PoE power of a port to 40W (adjust the register to keep PD enabled).

Messages

Message: *PoE Mode(Force): The switch port will power up the linked PD without any detect/negotiate mechanism(PD limited to 30W). Do you want to change this setting?*

Meaning: Confirmation message ensuring you want to make this config change. Added at FW v 1.01.1209.

Action: Click the **OK** button only if you are sure you want to change this setting. See the “PoE Mode” parameter description above. If you are not sure you want to change this setting, click the **Cancel** button.

2- 14.2 Power Delay

This page lets you set the delay time of PoE power provided to PDs after the switch reboots.

To configure PoE Power Delay in the web UI:

1. Click Configuration, PoE, and Power Delay.
2. On the default page select Enabled at the dropdown to display the page shown below.
3. At the Delay Mode dropdown, enable the desired ports.
4. Specify the power providing Delay Time after reboot.
5. Click Apply to apply the changes.

Figure 2-14.2: PoE Power Delay

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

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 exceeds the delay time. The default is 0 seconds; the valid range is 0-300 seconds.

2- 14.3 Schedule Profile

This page lets you schedule PoE power supply scheduling, to make PoE management easier and to save energy. To configure PoE Scheduling in the web UI:

1. Click Configuration, PoE, and Schedule Profile.
2. Select the local port and enable.
3. Select time and day to supply power.
4. Click Apply to apply the change.

Figure 2-13.3: PoE Schedule Profile

The screenshot shows the Lantronix web interface for configuring PoE Schedule Profiles. The page title is "PoE Schedule Profile" and the breadcrumb is "Home > Configuration > PoE > Schedule Profile".

Profile: A dropdown menu showing "1".

Name: A text input field containing "Profile 1".

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

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

Parameter descriptions:

Profile: Select a Profile number for this instance (1-16). There can be 16 profiles configured per switch.

Name: Enter a name for this Profile. The default name is "Profile 1". You can enter a name for identifying each profile.

Week Day: The day to schedule PoE (Monday – Sunday).

Start Time: Select the hour (HH) and Minute (MM) as 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.

2- 14.4 PoE Auto Power Reset (Auto Checking)

This page lets you specify the auto detection parameters to check the linking status between PoE ports and PDs. It automatically pings the PD on a configured schedule and if the PD does not respond to the configured number of pings, the switch toggles PoE power on the port to automatically reset the PD.

To configure PoE Auto Power Reset in the web UI:

1. Click Configuration, PoE, and Auto Power Reset.
2. Enable the Ping Check function.
3. Specify the PD's IP address, checking interval, retry time, failure action, and reboot time, and max. reboot times.
4. Click Apply to apply the changes.

Figure 2-14.4: PoE Auto Power Reset

The screenshot shows the 'PoE Auto Power Reset' configuration page in the Lantronix web UI. The page is titled 'PoE Auto Power Reset' and has a status of 'Disabled'. A table lists 8 ports with columns for Port, Ping IP Address, Startup Time, Interval Time(sec), Retry Time, Failure Log, Failure Action, Reboot Time(sec), and Max. Reboot Times. All ports are configured with IP 0.0.0.0, 60s startup, 30s interval, 3 retries, 'Nothing' failure action, 15s reboot, and 3 max reboots. 'Apply' and 'Reset' buttons are at the bottom.

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

Parameter descriptions:

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

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

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

Startup Time : When a PD has been started, the switch will wait this amount of time to do PoE Auto Power Reset. 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. The default is 30 seconds; the valid range is 10-120 seconds.

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

Failure Log : Failure loggings counter (error=x, total=y).

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. The default is 15 seconds; the valid range is 3-120 seconds.

Max. Reboot Times: When Failure Action is set to Reboot Remote PD, this setting limits the number of times to reboot the PD. The default is 3 times; the valid range is 0-10 retries. Entering 0 means unlimited reboot attempts.

Buttons:

Apply – Click to save changes.

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

Message: *W poe 19:55:52 41/poe_send_ping_check#2985: Warning: The ping ip adress has no same ip domain.*

Recovery: Make sure the PoE Auto Power Reset "Ping IP Address" parameter isn't entered for more than one port.

2- 14.5 Chip Reset Schedule

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

1. Click Configuration, PoE, and Chip Reset Schedule to display the default webpage.
2. At the Mode dropdown select Enabled to display the PoE Chip Reset table shown below.
3. Set the PoE Chip Reset Time(s).
4. Click Apply to save the changes.

Figure 2-14.5: PoE Chip Reset Schedule

The screenshot shows the Lantronix web interface for configuring the PoE Chip Reset Schedule. The page title is "PoE Chip Reset Schedule" and the mode is set to "Enabled". The configuration is as follows:

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

Buttons: **Apply** (blue), **Reset** (orange)

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 (Monday – Sunday).

PoE Chip Reset Time : The time to reset PoE chip. Select the hour (HH) and minute (MM).

Buttons:

Apply – Click to save changes.

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

2-15 EPS

The Ethernet (Linear) Protection Switch instances are configured here. EPS (Ethernet Protection Switching) is defined in ITU/T G.8031. **Note** that EPS and ERPS are standard protocols that can be used between various vendor switches. Rapid Rings protocols are only for Lantronix switches that support the Rapid Ring protocols. Note that only one EPS can be added for each Apply operation.

To configure EPS parameters in the web UI:

1. Click Configuration and EPS.
2. Click the Add New EPS button.
3. Specify the Ethernet Protection Switching parameters.
4. Click Apply to apply the changes.

Figure 2-15a: Ethernet Protection Switching

Delete	EPS ID	Domain	Architecture	W Flow	P Flow	W SF MEP	P SF MEP	APS MEP	Alarm
<input type="checkbox"/>	1	Port	1+1	1	2	3	4	5	●
<input type="checkbox"/>	2	Port	1:1	6	7	8	3	4	●

Delete	<input type="text" value="3"/>	<input type="text" value="Port"/>	<input type="text" value="1+1"/>	<input type="text" value="1"/>	<input type="text" value="1"/>	<input type="text" value="1"/>	<input type="text" value="1"/>	<input type="text" value="1"/>	
--------	--------------------------------	-----------------------------------	----------------------------------	--------------------------------	--------------------------------	--------------------------------	--------------------------------	--------------------------------	--

Buttons: **Add New EPS**, **Apply**, **Reset**

Parameter descriptions:

Delete : This box is used 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 : 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' above.

P Flow : The protecting flow for the EPS. See 'Domain' above.

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:

Apply – Click to save changes.

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

Figure 2-15b: Ethernet Protection Switching (configured)

Delete	EPS ID	Domain	Architecture	W Flow	P Flow	W SF MEP	P SF MEP	APS MEP	Alarm
<input type="checkbox"/>	1	Port	1:1	1	2	3	4	5	●
<input type="checkbox"/>	2	Port	1+1	6	7	8	9	10	●

Click on a linked EPS ID to display an EPS ID's configuration page:

EPS ID	Domain	Architecture	W Flow	P Flow	W SF MEP	P SF MEP	APS MEP
1	Port	1:1	1	2	3	4	5

Protection Type	APS	Revertive	WTR Time	Hold Off Time
Bidirectional	<input checked="" type="checkbox"/>	<input type="checkbox"/>	300	0

Protection State	W Flow	P Flow	Transmit APS r/b	Receive APS r/b	Architecture Mismatch	APS On Working	Switching Incomplete	No Aps Received
Disabled	OK	OK	NR Null/Null	NR Null/Null	●	●	●	●

Ethernet Protection Switching Configuration

This page lets you view and configure the current EPS Instance.

Instance Data

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: 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'.

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.

Instance Configuration

Configured: Displays a red dot or a green dot:

Red: This EPS is only created and has not yet been configured - is not active.

Green: This EPS is configured - is active.

Protection Type: Unidirectional or Bidirectional:

Unidirectional: EPS in the two ends can select traffic from different working/protecting flow. This is only possible in case of 1+1.

Bidirectional: EPS in the two ends is selecting traffic from the same working/protecting flow. This requires APS enabled. This is mandatory for 1:1

APS: The Automatic Protection Switching protocol can be enabled/disabled. This is mandatory for 1:1.

Revertive: The revertive switching to working flow can be enabled/disabled.

WTR Time: The Wait To Restore timing value to be used in revertive switching. 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: Forced switch to protecting.

Manual Switch P: Manual switch to protecting.

Manual Switch W: Manual switch to working. This is only allowed in case of 'non-revertive' mode

Exercise: Exercise of the protocol - not traffic effecting. This is only allowed in case of 'Bidirectional' protection type

Freeze: This EPS is locally frozen - ignoring all input.

Lock Out Local: This EPS is locally "locked out" - ignoring local SF detected on working.

Instance State

Protection State: EPS state according to State Transition Tables in G.8031.

W Flow:

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:

OK: State of protecting flow is ok.

SF: State of protecting flow is Signal Fail.

SD: State of protecting flow is Signal Degrade (for future use).

Transmit APS r/b: The transmitted APS according to State Transition Tables in G.8031.

Receive APS r/b: The received APS according to State Transition Tables in G.8031.

Architecture Mismatch: The architecture indicated in the received APS does not match the locally configured.

APS on working: APS is received on the working flow.

Switching Incomplete: Traffic is not selected from the same flow instance in the two ends.

No APS Received: APS PDU is not received from the other end.

Buttons

Apply: Click to save changes.

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

Messages:

Only one EPS can be added for each Apply operation

The working and protection flows are equal

Working MEP and protecting SF MEP is same instance

Invalid APS MEP instance

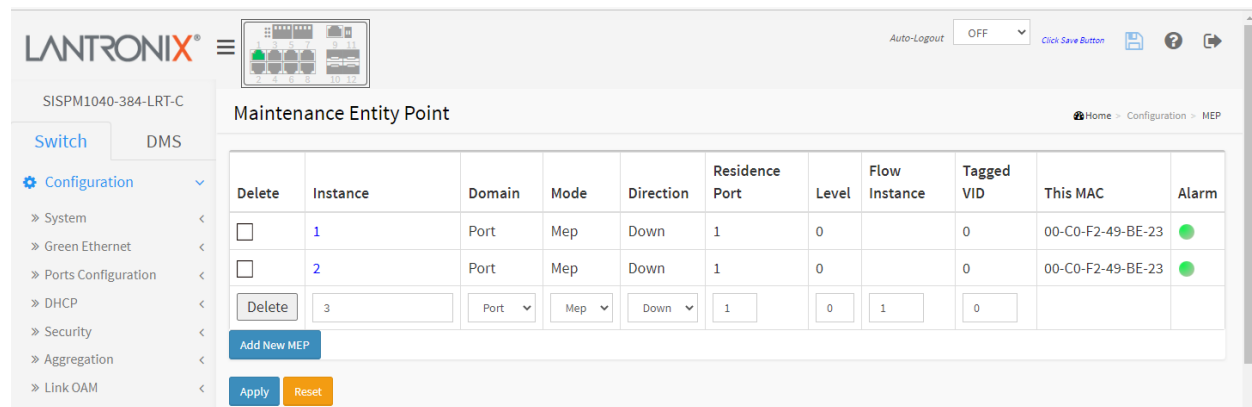
2-16 MEP

Maintenance Entity End Point (MEP) instances are configured here. A MEP is an endpoint in a Maintenance Entity Group per ITU-T Y.1731. Note that only one MEP can be added for each Apply operation.

To configure MEP parameters in the web UI:

1. Click Configuration and MEP.
2. Specify the Maintenance Entity Point parameters.
3. Click Apply to save the changes.

Figure 2-16: 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 ID of a MEP to enter the configuration page. The valid range is 1 - 100.

Domain : The domain of the MEP:

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 : Whether a MEP or a MIP:

MEP: This is a Maintenance Entity End Point.

MIP: This is a Maintenance Entity Intermediate Point.

Direction : Whether this is an Up MEP or a Down MEP.

Down: This is a Down MEP - monitoring ingress OAM and traffic on 'Residence Port'.

Up: This is an Up MEP - monitoring egress OAM and traffic on 'Residence Port'.

Residence Port : The port where MEP is monitoring - see 'Direction'. For an EVC MEP the port must be a port in the EVC. For a VLAN MEP the port must be a VLAN member.

Level : The MEG level of this MEP.

Flow Instance : The MEP is related to this flow - See 'Domain'. This is not relevant and not shown in case of Port MEP.

Tagged VID : Port MEP: An outer C/S-tag (depending on VLAN Port Type) is added with this VID. Entering '0' means no TAG added.

EVC MEP: This is not used.

VLAN MEP: This is not used.

EVC MIP: On Serval, this is the Subscriber VID that identifies the subscriber flow in this EVC where the MIP is active.

This MAC : The MAC of this MEP - can be used by other MEP when unicast is selected (Info only).

Alarm : There is an active alarm on the MEP.

Click on a linked instance number to display its configuration page:

This page lets you view and configure the current MEP Instance.

Instance Data

MEP Instance : The ID of the MEP.

Domain : The domain of the MEP:

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 : Whether a MEP or a MIP:

MEP: This is a Maintenance Entity End Point.

MIP: This is a Maintenance Entity Intermediate Point.

Direction : Whether this is an Up MEP or a Down MEP.

Down: This is a Down MEP - monitoring ingress OAM and traffic on 'Residence Port'.

Up: This is an Up MEP - monitoring egress OAM and traffic on 'Residence Port'.

Residence Port : The port where MEP is monitoring - see 'Direction'. For an EVC MEP the port must be a

port in the EVC. For a VLAN MEP the port must be a VLAN member.

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 : This value will be the VID of a TAG added to the OAM PDU.

This MAC : The MAC of this MEP - can be used by other MEP when unicast is selected (Info only).

Instance Configuration

This is the Policy number of the relevant ECE. Policy ID is used to assure that received OAM PDU is able to hit an IS2 entry. If this value is '0' IS2 rules will be created on classified VID. If this is NOT '0' IS2 rules will be created on this Policy (PAG). This must be equal to ECE Policy Number if OAM PDU will hit the ECE ISO. This is the case if an ECE is created with 'tag_type' as 'any'.

EVC QoS : This is only relevant for an 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 up to 16 characters 'MEG id' (Short MA Name) can be up to 16 characters.

ITU CC ICC: This is defined by ITU (Y1731 Fig. A5). 'Domain Name' is not used. 'MEG id' must be 15 or fewer characters.

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 up to 16 characters.

MEG Id : This is either ITU MEG ID or IEEE Short MA Name - depending on 'Format'. See 'Format'. In case of ITU ICC format this must be 13 char. In case of ITU CC ICC format this must be 15 char. In case of IEEE String format this can be max 16 char.

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' must be the same.

Frame rate : Selecting the frame rate of CCM PDU. This is the inverse of transmission period as described in Y.1731. This value has these uses:

- The transmission rate of the CCM PDU.
- Fault Cause cLOC is declared if no CCM PDU has been received within 3.5 periods - see 'cLOC'.
- Fault Cause cPeriod is declared if a CCM PDU has been received with different period - see 'cPeriod'.

Selecting 300f/sec or 100f/sec will configure HW based CCM (if possible). Selecting other frame rates will configure SW based CCM. In case of enable of Continuity Check and Loss Measurement both implemented on SW based CCM, 'Frame Rate' has to be the same.

TLV : Enable/disable of TLV insertion in the CCM PDU.

APS Protocol

Enable : Automatic Protection Switching protocol information transportation based on transmitting/receiving R-APS/L-APS PDU can be enabled/disabled. Must be enabled to support ERPS/ELPS implementing APS. This is only valid with one Peer MEP configured.

Priority : The priority to be inserted as PCP bits in TAG (if any).

Cast : Selection of APS PDU transmitted unicast or multi-cast. The unicast MAC will be taken from the 'Unicast Peer MAC' configuration. Unicast is only valid for L-APS - see 'Type'. The R-APS PDU is always transmitted with multi-cast MAC described in G.8032.

Type : either R-APS or L-APS. where:

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 Monitor page.

Apply: Click to save changes.

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

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.

Messages:

Warning! The Configuration is invalid. EVC flow was found invalid.

Warning! The Configuration is invalid. VLAN domain is not supported.

Warning! The Configuration is invalid. This MIP is not supported.

Warning! The Configuration is invalid. Invalid parameter error returned from MEP.

Only one MEP can be added for each Apply operation.

2-17 ERPS

ERPS instances are configured here. ERPS (Ethernet Ring Protection Switching) is defined in ITU/T G.8032. It provides fast protection and recovery switching for Ethernet traffic in a ring topology while also ensuring that the Ethernet layer remains loop-free. **Note** that EPS and ERPS are standard protocols that can be used between various vendor switches. Rapid Rings protocols are only for Lantronix switches that support Rapid Ring protocols. Only one ERPS can be added per Apply operation.

See "[Appendix D: G.8032 Major and Sub Rings Configuration](#)" on page 483 for a guide to ERPS configuration.

Web Interface

To configure Ethernet Ring Protection Switching 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.

Figure 2-17: Ethernet Ring Protection Switching

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	2	-	4	5	6	0	Sub	Yes	Yes	1	●
<input type="checkbox"/>	3	1	1	1	1	1	1	Major	<input type="checkbox"/>	<input type="checkbox"/>	0	●

Delete : This box is used to mark an ERPS for deletion in next Save operation.

ERPS ID : The ID of the created Protection group, It must be an integer value of 1 - 64. Up to 64 ERPS Protection Groups can be created. Click on the ID of a Protection group to enter its configuration page.

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. A "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. A "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 ERPS.

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.

Ethernet Ring Protection Switch Configuration

Click a linked ERPS ID (instance number) to display its instance configuration page. This page lets you view and configure the selected ERPS Instance.

The screenshot displays the 'ERPS Configuration 1' page. On the left is a navigation menu with 'ERPS' selected. The main content area is divided into several sections:

- Instance Data:** A table with 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, 3, 4, 1, 2, Major Ring.
- Instance Configuration:** Fields for Configured (green dot), Guard Time (900), WTR Time (3min), Hold Off Time (0), Version (v2), Revertive (checked), and VLAN config (VLAN Config).
- RPL Configuration:** RPL Role (None), RPL Port (None), and a Clear checkbox.
- Instance Command:** Command (None) and Port (None).
- Instance State:** A table with 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, (empty), (empty), (empty), 0, (green dot), (red dot), Blocked, Blocked, (green dot).

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

Parameter descriptions:**Instance Data**

ERPS ID : The ID of the Protection group.

Port 0 : This will create a Port 0 of the switch in the ring.

Port 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. A "0" in this field indicates that no Port 1 APS MEP is associated with this instance.

Ring Type : Type of Protection ring. It can be either major ring or sub-ring.

Instance Configuration

Configured : Displays a red or green dot:

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.

RPL Configuration

RPL Role : It can be either RPL owner or RPL Neighbor.

RPL Port : This allows selecting the east port or west port as the RPL block.

Clear : If the owner must be changed, then the clear check box allows clearing 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 : East port state:

OK: State of East port is ok.

SF: State of East port is Signal Fail.

Port 1 : West port state:

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 lights; otherwise the green LED lights.

Buttons

Apply: Click to save changes.

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

Messages:

'Port 0' and 'Port 1' cannot be the same

'Port 0 APS MEP' and 'Port 1 APS MEP' cannot be the same

'Port 0 SF MEP' and 'Port 1 SF MEP' can not be the same

Only one ERPS can be added for each Apply operation.

Meaning: The ERPS configuration was invalid.

Recovery: **1.** Click the **OK** button to clear the webpage message. **2.** Try the configuration again.

2-18 MAC Table

Switching of frames is based on the DMAC address contained in the frame. The switch builds a table that maps MAC addresses to switch ports for knowing which ports the frames should go to (based on the DMAC address in the frame). This table contains both static and dynamic entries. The static entries are configured by the network administrator if the administrator wants to do a fixed mapping between the DMAC address and switch ports.

The frames also contain a 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 frames with the corresponding SMAC address have been seen after a configurable age time.

To configure MAC Address table in the web UI:

Aging Configuration

1. Click Configuration, MAC Table.
2. Specify the Disable Automatic Aging and Aging Time.
3. Click Apply.

MAC Table Learning

1. Click Configuration, MAC Table.
2. Specify the Port Members (Auto, Disable, Secure).
3. Click Apply.

Static MAC Table Configuration

1. Click Configuration, MAC Table, and Add New Static Entry.
2. Specify the VLAN IP and MAC address, and Port Members.
3. Click Apply.

Figure 2-18: MAC Address Table Configuration

The screenshot displays the 'MAC Address Table Configuration' page in the Lantronix web UI. The page is divided into three main sections:

- Aging Configuration:**
 - Disable Automatic Aging:** A checkbox that is currently unchecked.
 - Aging Time:** A text input field containing '300' followed by 'seconds'.
- MAC Table Learning:**

	Port Members											
	1	2	3	4	5	6	7	8	9	10	11	12
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"/>	<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"/>	<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"/>	<input type="checkbox"/>	<input type="checkbox"/>
- Static MAC Table Configuration:**

	Port Members													
Delete	VLAN ID	MAC Address	1	2	3	4	5	6	7	8	9	10	11	12
<input type="button" value="Delete"/>	1	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"/>	<input type="checkbox"/>	<input type="checkbox"/>

Below the table are buttons for 'Add New Static Entry', 'Apply', and 'Reset'.

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 the checking Disable automatic aging checkbox.

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 maximum of 64 entries is for the whole stack, and not per switch.

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.

Adding a New Static Entry : Click to add a new entry to the static MAC table. Specify the VLAN ID, MAC address, and port members for the new entry. Click "Apply".

Buttons:

Apply – Click to save changes.

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

Message: *Error: mac address:00-00-00-00-00-00 is not multicast mac address, support only one port.*

2-19 VLAN Translation

2- 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 to display the VLAN Translation Port Configuration page.
2. Specify the Port and Group parameters.
3. Click Apply.

Figure 2-19.1: Port to Group Mapping

Port	Group Configuration	
	Default	Group ID
*	<input type="checkbox"/>	<> v
1	<input type="checkbox"/>	1 v
2	<input type="checkbox"/>	2 v
3	<input type="checkbox"/>	3 v
4	<input type="checkbox"/>	4 v
5	<input type="checkbox"/>	5 v
6	<input type="checkbox"/>	6 v
7	<input type="checkbox"/>	7 v

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 click Apply.

Group ID : The VLAN Translation mappings are organized into Groups, identified by the Group ID. This way a port is configured to use several VLAN Translation mappings easily by simply configuring it to use a given group. Then number of possible groups in a switch is equal to the number of ports present in this switch.

A port can be configured to use any of the groups, but only one at any given time. Multiple ports can be configured to use the same group. A valid Group ID is an integer value from 1 to 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 GID = 1.

Buttons:

Apply – Click to save changes.

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

2- 19.2 VID Translation Mapping

This page lets you view and configure current VLAN Translation mapping parameters.

Web Interface

To configure VID Translation Mapping in the web UI:


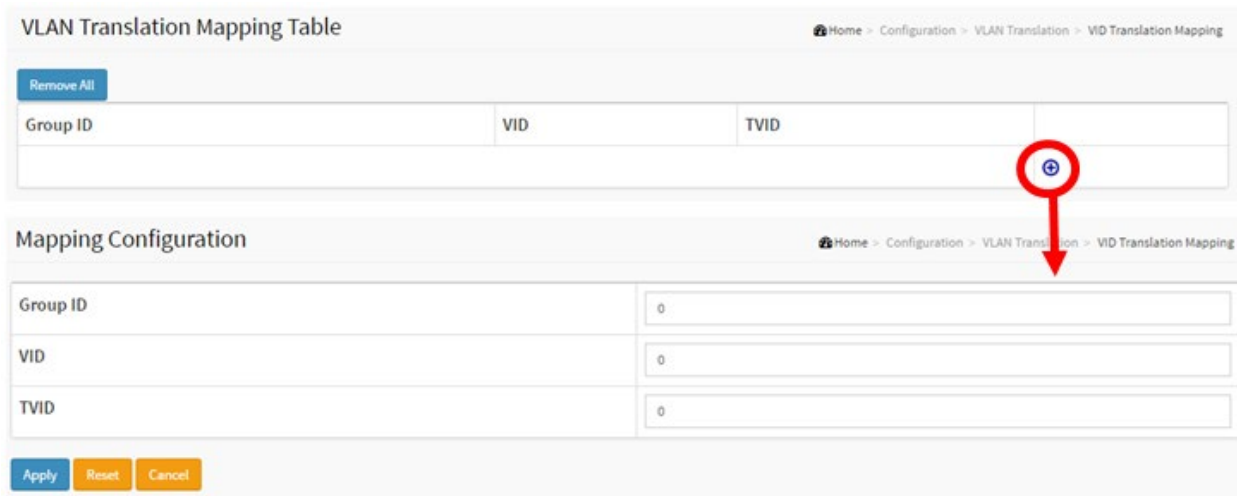
1. Click Configuration, VLAN Translation, and VID Translation Mapping.
2. Click the Add New Mapping icon ().
3. Specify the Group ID, VID, and TVID.
4. Click Apply.

Figure 2-19.2: VLAN Translation Mapping Table



Parameter descriptions:

Group ID : The VLAN Translation mappings are organized into Groups, identified by the Group ID (GID). 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 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 GID = 1.

VID : Indicates the VLAN of the mapping (i.e. 'source' VLAN). A valid VLAN ID is 1 - 4095.

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 TVID is 1 - 4095.

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.

Modification Buttons

You can modify each VLAN Translation mapping in the table using these buttons:



: Edits the mapping row.



: Deletes the mapping.



: Add New mapping.

Buttons

Remove All : Click to remove all VLAN Translation mappings

Messages : *VLAN ID and Translated VLAN ID cannot be same.*

Example:

Group ID	VID	TVID	
1	10	1	
2	20	2	

2-20 VLANs

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

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

To configure VLAN membership configuration in the web UI:

1. Click Configuration, VLANs.
2. Specify existing Allowed Access VLANs, Ethertype for Custom S-ports, and Port VLAN config.
3. Click Apply.

Figure 2-20.1: VLAN Configuration

The screenshot shows the LANTRONIX web interface for VLAN Configuration. The top navigation bar includes the LANTRONIX logo, a menu icon, and user options like 'Auto-Logout OFF' and 'Click Save Button'. The main content area is titled 'VLAN Configuration' and is divided into two sections:

- Global VLAN Configuration:**
 - Allowed Access VLANs:** A text input field containing '1' with a hint '(e.g. 1,2,10-13,15)'.
 - Ethertype for Custom S-ports:** A text input field containing '88A8'.
- Port VLAN Configuration:** A table with the following columns: Port, Mode, Port VLAN, Port Type, Ingress Filtering, Ingress Acceptance, Egress Tagging, Allowed VLANs, and Forbidden VLANs.

Port	Mode	Port VLAN	Port Type	Ingress Filtering	Ingress Acceptance	Egress Tagging	Allowed VLANs	Forbidden VLANs
*	Access	1	C-Port	<input checked="" type="checkbox"/>	Tagged and Untagged	Untag Port VLAN	1	
1	Access	1	C-Port	<input checked="" type="checkbox"/>	Tagged and Untagged	Untag Port VLAN	1	
2	Access	1	C-Port	<input checked="" type="checkbox"/>	Tagged and Untagged	Untag Port VLAN	1	
3	Access	1	C-Port	<input checked="" type="checkbox"/>	Tagged and Untagged	Untag Port VLAN	1	
4	Access	1	C-Port	<input checked="" type="checkbox"/>	Tagged and Untagged	Untag Port VLAN	1	
5	Access	1	C-Port	<input checked="" type="checkbox"/>	Tagged and Untagged	Untag Port VLAN	1	
6	Access	1	C-Port	<input checked="" type="checkbox"/>	Tagged and Untagged	Untag Port VLAN	1	
7	Access	1	C-Port	<input checked="" type="checkbox"/>	Tagged and Untagged	Untag Port VLAN	1	
8	Access	1	C-Port	<input checked="" type="checkbox"/>	Tagged and Untagged	Untag Port VLAN	1	

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 three modes as described below.

Whenever a particular mode is selected, the remaining fields in that row will be either grayed out or made changeable depending on the mode in question. Grayed out fields show the value that the port will get when the mode is applied.

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

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

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

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

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

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

Port VLAN : Determines the port's VLAN ID (a.k.a. PVID). Allowed VLANs are in the range 1 - 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 called 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.

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 a member of one or more VLANs. This is very useful when dynamic VLAN protocols like MVRP and GVRP must be prevented from dynamically adding ports to VLANs. The answer is to mark such VLANs as forbidden on the port in question. The syntax is identical to the syntax used in the Existing 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.

2-21 Private VLANs

In a Private VLAN, PVLANS provide layer 2 isolation between ports within the same broadcast domain. Isolated ports configured as part of PVLAN cannot communicate with each other. Member ports of a PVLAN can communicate with each other.

2-21.1 Membership

The Private VLAN membership configurations for the switch can be monitored and modified here. Private VLANs can be added or deleted here. Port members of each Private VLAN can be added or removed here. Private VLANs are based on the source port mask, and there are no connections to VLANs. This means that VLAN IDs and Private VLAN IDs can be identical.

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

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

Web Interface

To configure Private VLAN Membership in the web UI:

1. Click Configuration, Private VLANs, and Membership.
2. Click the Add New Private VLAN button to add a new row to the table.
3. Check the port(s) want to enable Port Members.
4. Click Apply.

Figure 2-21.1: Private VLAN Membership Configuration

The screenshot shows the 'Private VLAN Membership Configuration' page in the Lantronix web UI. The page title is 'Private VLAN Membership Configuration'. The breadcrumb trail is 'Home > Configuration > Private VLANs > Membership'. The main content area features an 'Auto-refresh' checkbox and a table for 'Private VLAN Membership Configuration'. The table has columns for 'Delete', 'PVLAN ID', and 'Port Members' (ports 1-12). The first row (PVLAN ID 1) has all port member checkboxes checked. Below the table are buttons for 'Add New Private VLAN', 'Apply', and 'Reset'.

Private VLAN Membership Configuration		Port Members											
Delete	PVLAN ID	1	2	3	4	5	6	7	8	9	10	11	12
<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 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"/>	<input type="checkbox"/>	<input 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"/>	<input type="checkbox"/>	<input type="checkbox"/>

Parameter descriptions:

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

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

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

Buttons:

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

Refresh : Click to manually refresh the page immediately.

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 "OK" to discard the incorrect entry or click "Cancel" to return to the editing and make a correction. The Private VLAN is enabled when you click "**Save**". The **Reset** button can be used to undo the addition of new Private VLANs.

Apply – Click to save changes.

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

Messages:

'Private VLAN ID' must be an integer value between 1 and 12

Private VLAN ID 2 is already in use.

At least one port must be selected to add an entry

2-21.2 Port Isolation

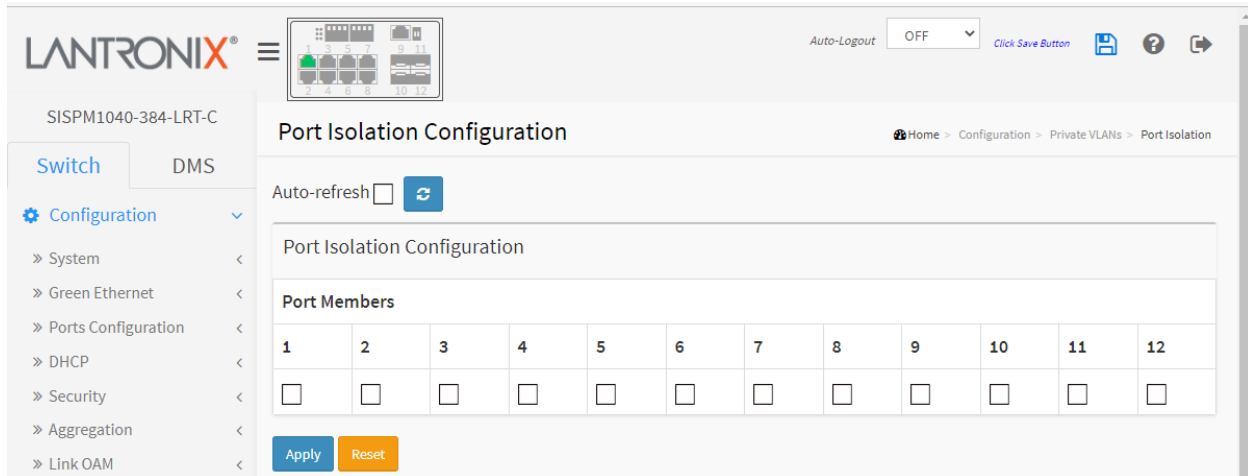
This page is used for enabling or disabling port isolation on ports in a Private VLAN.

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 VLAN, Port Isolation.
2. Select the port you want to enable Port Isolation.
3. Click Apply.

Figure 2-21.2: 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: Click to automatically refresh the page every 3 seconds.

Refresh: Click to manually refresh the page immediately.

Apply: Click to save changes.

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

2-22 VCL

VLAN Control List support includes three VLAN types (MAC address-based VLAN, Protocol-based VLAN, and IP Subnet-based VLAN).

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

A Protocol-based VLAN supports Protocols including Ethernet, LLC, and SNAP Protocols.

An IP Subnet-based VLAN provides IP subnet to VLAN ID mappings.

2-22.1 MAC-based VLAN

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

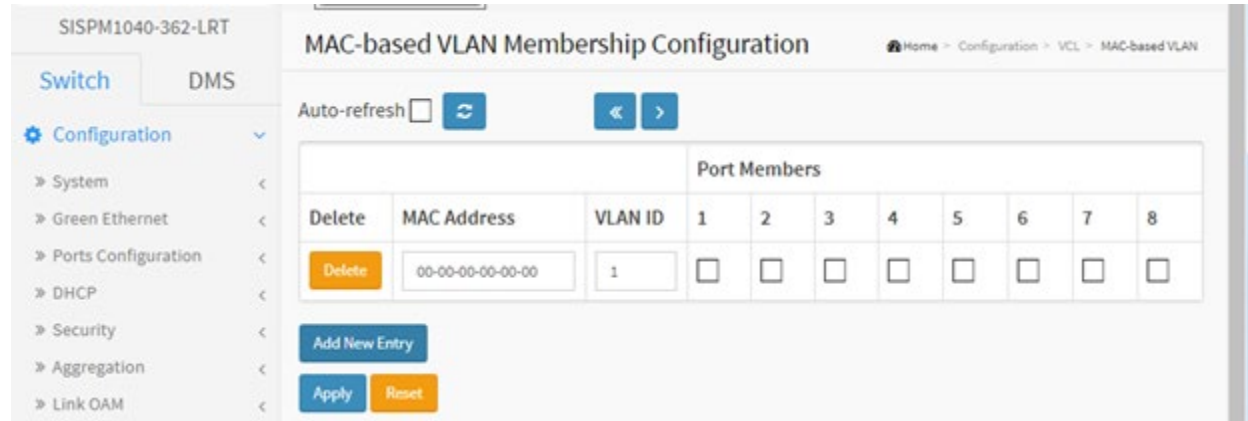
A common way of grouping VLAN members is by port, hence the name port-based VLAN. Typically, the device adds the same VLAN tag to untagged packets that are received through the same port. Later on, these packets can be forwarded in the same VLAN. Port-based VLAN is easy to configure and applies to networks where the locations of terminal devices are relatively fixed. As mobile office and wireless network access gain more popularity, the ports that terminal devices use to access the networks are very often non-fixed. A device may access a network through Port A this time, but through Port B the next time. If Port A and Port B belong to different VLANs, the device will be assigned to a different VLAN the next time it accesses the network. As a result, it will not be able to use the resources in the old VLAN. On the other hand, if Port A and Port B belong to the same VLAN, after terminal devices access the network through Port B, they will have access to the same resources as those accessing the network through Port A do, which brings security issues. To provide user access and ensure data security in the meantime, the MAC-based VLAN technology is 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 in conjunction with security technologies such as 802.1X to provide secure, flexible network access for terminal devices.

Web Interface

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

4. Click Configuration, VCL, MAC-based VLAN, and Add New Entry.
5. Specify the MAC address and VLAN ID.
6. Select the desired Port Members.
7. Click Apply.

Figure 2-22.1: MAC-based VLAN Membership Configuration**Parameter descriptions:**

Delete : To delete a MAC-based VLAN entry, check this box and click Apply. The entry will be deleted from the switch.

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. At least one port must be selected to add an entry.

Adding a New MAC-based VLAN : Click Add New Entry to add a new MAC-based VLAN entry. An empty row is added to the table, and the MAC-based VLAN entry can be configured as needed. Any unicast MAC address can be configured for the MAC-based VLAN entry. No broadcast or multicast MAC addresses are allowed. Legal values for a VLAN ID are 1 - 4095.

The MAC to VLAN ID entry is enabled on the switch unit when you click Apply.

A mapping without any port members will not be added when you click Apply.

The **Delete** button can be used to undo the addition of new mappings. The maximum possible MAC to VLAN ID mapping entries is limited to 256.

Buttons:

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

Refresh: Click to manually refresh the page immediately.

Apply – Click to save changes.

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

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

2-22.2 Protocol -based VLAN

This page lets you add new Protocol to Group Name mapping entries. Each protocol can be part of only one Group). The switch supports Ethernet, LLC, and SNAP Protocols.

LLC : The Logical Link Control (LLC) data communication protocol layer is the upper sub-layer of the Data Link Layer (which is itself layer 2, just above the Physical Layer) in the seven-layer OSI reference model. It provides multiplexing mechanisms that make it possible for several network protocols (IP, IPX, DECnet and Appletalk) to coexist within a multipoint network and to be transported over the same network media and can also provide flow control and automatic repeat request (ARQ) error management mechanisms.

SNAP : The Subnetwork Access Protocol (SNAP) is a mechanism for multiplexing, on networks using IEEE 802.2 LLC, more protocols than can be distinguished by the 8-bit 802.2 Service Access Point (SAP) fields. SNAP supports identifying protocols by Ethernet type field values; it also supports vendor-private protocol identifier spaces. It is used with IEEE 802.3, IEEE 802.4, IEEE 802.5, IEEE 802.11 and other IEEE 802 physical network layers, as well as with non-IEEE 802 physical network layers such as FDDI that use 802.2 LLC.

2-22.2.1 Protocol to Group

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

Web Interface

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

1. Click Configuration > VCL > Protocol-based VLAN > Protocol to Group.
2. Click Add New Entry.
3. Specify the Ethernet LLC SNAP Protocol and Group Name.
4. Click Apply.

Figure 2-22.2.1: Protocol to Group Mapping Table

The screenshot shows the web interface for configuring Protocol to Group Mapping. The breadcrumb path is: Home > Configuration > VCL > Protocol-based VLAN > Protocol to Group. The interface includes an 'Auto-refresh' checkbox and a refresh icon. Below this is a table titled 'Protocol to Group Mapping Table' with the following structure:

Delete	Frame Type	Value	Group Name
<input type="checkbox"/>	Ethernet	Etype: 0x 0800	

Below the table are buttons for 'Add New Entry', 'Apply', and 'Reset'.

Parameter descriptions:

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

Frame Type : Frame Type can have one of these values:

Ethernet (Ethernet II frame)

LLC (IEEE 802.2 Logical Link Control)

SNAP (IEEE 802.2 Subnetwork Access Protocol)

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

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

Below are the criteria for the three different Frame Types:

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

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 the string is a hexadecimal value of 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.

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 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.

Buttons:

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

Refresh: Click to manually refresh the page immediately.

Apply – Click to save changes.

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

2-22.2.2 Group to VLAN

This page lets you map a Group Name (already configured or to be configured in the future) to a VLAN for the switch. To set Group Name to VLAN mapping table parameters in the web UI:

1. Click Configuration > VCL > Protocol-based VLAN > Group to VLAN.
2. Click Add New Entry.
3. Specify the Group Name and VLAN ID and select Port Members.
4. Click Apply.

Figure 2-22.2.2: Group Name to VLAN Mapping Table

		Port Members								
Delete	Group Name	VLAN ID	1	2	3	4	5	6	7	8
<input type="checkbox"/>	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Parameter descriptions:

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

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

VLAN ID : Indicates the ID to which Group Name will be mapped. A valid VLAN ID 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 (all boxes are unchecked).

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, the Group Name, VLAN ID and port members can be configured as needed. Legal values for a VLAN ID are 1 through 4095. The button can be used to undo the addition of new entry.

Buttons:

Apply – Click to save changes.

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

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

Refresh: Click to manually refresh the page immediately.

2-22.3 IP Subnet-based VLAN

The IP subnet to VLAN ID mappings can be configured here. This page allows adding, updating, and deleting IP subnet to VLAN ID mapping entries and assigning them to different ports.

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

1. Click Configuration > VCL > IP Subnet-based VLAN.
2. Click 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.

Figure 2-22.3: IP Subnet-based VLAN Membership Configuration

The screenshot displays the 'IP Subnet-based VLAN Membership Configuration' page. On the left is a navigation menu with 'Configuration' expanded. The main area features an 'Auto-refresh' checkbox and a refresh icon. Below is a table with the following structure:

				Port Members											
Delete	IP Address	Mask Length	VLAN ID	1	2	3	4	5	6	7	8	9	10	11	12
<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"/>	<input type="checkbox"/>
<input type="checkbox"/>	0.0.0.0	24	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"/>	<input type="checkbox"/>	<input type="checkbox"/>

Buttons at the bottom include 'Delete', 'Add New Entry', 'Apply', and 'Reset'.

Parameter descriptions:

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

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 an 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 "Add New Entry" to add a new IP subnet-based VLAN entry. An empty row is added to the table, and the IP subnet-based VLAN entry can be configured as needed. Any IP address/mask can be configured for the IP subnet-based VLAN entry. Legal values for a VLAN ID are 1 - 4095.

The IP subnet-based VLAN entry is enabled on the switch unit when you click "Apply".

The "Delete" button can be used to undo the addition of new IP subnet-based VLANs. The maximum possible IP subnet-based VLAN entries is 128.

Message: *Subnet 0.0.0.0/x is not valid. Please use a non-zero subnet.*

2-23 Voice VLAN

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

2-23.1 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. The IP device should be configured through its own GUI.

To configure Voice VLAN in the web UI:

1. Select Configuration > Voice VLAN > Configuration.
2. Select "Enabled" Mode in the Voice VLAN Configuration.
2. Specify VLAN ID Aging Time and Traffic classification.
3. Specify (Port Mode, Security, and Discovery Protocol) in the Port Configuration section.
4. Click Apply.

Figure 2-23.1: Voice VLAN Configuration

The screenshot displays the 'Voice VLAN Configuration' web interface. On the left is a navigation menu with 'Voice VLAN' selected. The main content area is divided into two sections:

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
7	Disabled	Disabled	OUI
8	Disabled	Disabled	OUI

At the bottom of the 'Port Configuration' section are 'Apply' and 'Reset' buttons.

Parameter descriptions:

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

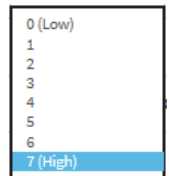
Enabled: Enable Voice VLAN mode operation.

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 to 10000000 seconds. It is used when security mode or auto detect mode is enabled. In other cases, it will be based on hardware aging time. The actual aging time will be situated between the [age_time; 2 * age_time] interval.

Traffic: Indicates the Voice VLAN traffic class. All traffic on the Voice VLAN will apply this class. The range is 0 (Low) to 7 (High). The default is 7 (High).



Port Mode : Indicates the Voice VLAN port mode. When port mode isn't set to disabled, you must disable the MSTP feature before enabling Voice VLAN to 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.



Port 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.

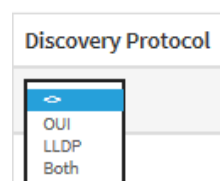
Disabled: Disable Voice VLAN security mode operation.

Port Discovery Protocol : Indicates the Voice VLAN port discovery protocol. It will only work when auto detect mode is enabled. Enable the LLDP feature before configuring discovery protocol to "LLDP" or "Both". Changing the discovery protocol to "OUI" or "LLDP" will restart the auto detect process. Possible discovery protocols are:

OUI: Detect telephony device by OUI (organizationally unique identifier) address.

LLDP: Detect telephony device by LLDP (Link Layer Discovery Protocol).

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.

2-23.2 OUI

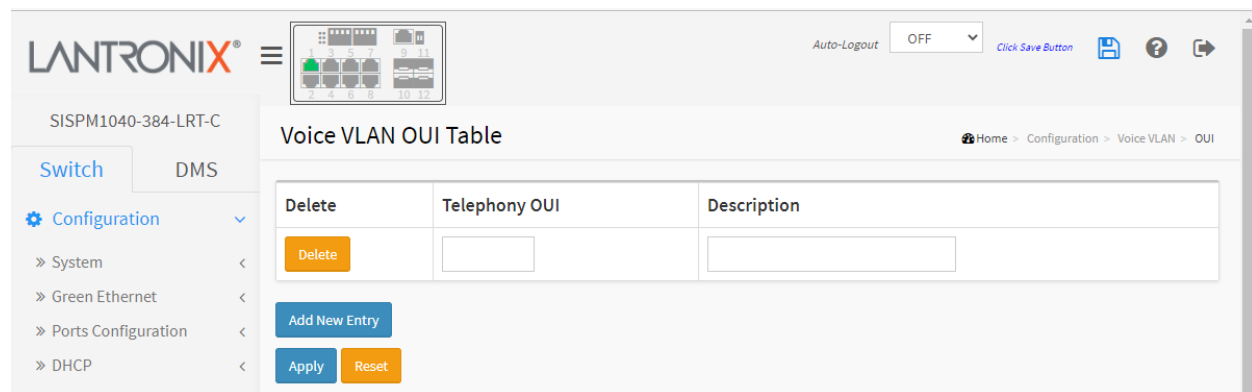
This page lets you configure Voice VLAN OUI table parameters. The maximum number of entries is 16. Modifying the OUI table will restart auto detection of the OUI process.

A Voice VLAN is a 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.

To configure the Voice VLAN OUI Table in the web UI:

1. Navigate to Configuration > Voice VLAN > OUI.
2. Click the "Add New Entry" button.
3. Specify Telephony OUI and Description.
4. Click Apply.

Figure 2-23.2: Voice VLAN OUI Table



Parameter descriptions:

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

Telephony OUI : A telephony OUI address is a 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). For example, 00-01-e3 = Siemens AG Phone, 00-09-6e = Avaya.

Description : The description of OUI address. Normally, it describes which vendor telephony device it belongs to. The allowed string length is 0 to 32 characters.

Buttons:

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

Apply – Click to save changes.

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

2-24 Ethernet Services

» Ethernet Services

» Ports

» L2CP

» Bandwidth Profiles

» EVCs

» ECEs

The Configuration > Ethernet Services menu path provides sub-menus for configuring EVC Ports, L2CP, Bandwidth Profiles, EVCs, and ECEs.

2-24.1 Ports

This page lets you view and configure current EVC (Ethernet Virtual Connection) port configuration parameters. To set Port Configuration in the web UI:

1. Click Configuration, Ethernet Services, and Ports.
2. Specify DEI Mode, Tag Mode, and Address Mode.
3. Click Apply.

Figure 2-24.1: Port Configuration

The screenshot displays the 'Port Configuration' page in the Lantronix web UI. The page title is 'Port Configuration' and the breadcrumb trail is 'Home > Configuration > Ethernet Services > Ports'. The page shows a table with the following columns: Port, DEI Mode, Tag Mode, and Address Mode. The table lists ports 1 through 8, each with a DEI Mode of 'Fixed', a Tag Mode of 'Outer', and an Address Mode of 'Source'. The page also includes a navigation menu on the left, a breadcrumb trail at the top right, and a 'Click Save Button' label.

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

Parameter descriptions:

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

DEI Mode : The DEI 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:

Colored: 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.

2-42-2 L2CP Port Configuration

This page lets you view and configure EVC L2CP parameters. Layer 2 Control Protocols (L2CP) are various Ethernet control protocols such as Spanning Tree BPDUs, LACP, PAUSE Frames, etc. L2CP Frames have specific MAC DAs belonging to reserved multicast MAC address ranges. Some L2CPs have their own MAC DA assigned to them. For more details refer to IEEE 802.1Q and [MEF 10.2](#).

To configure L2CP Port parameters in the web UI:

1. Click Configuration, Ethernet Services, and L2CP.
2. Specify an L2CP Mode for each DMAC.
3. Click Apply.

Figure 2-24.1: L2CP Port Configuration

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

Parameter descriptions:


DMAC: The destination BDPUs 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

 Port select box selects the port to be configured.

Refresh: Click to manually refresh the page immediately.

Apply: Click to save changes.

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

2-24.2 Bandwidth Profiles

This page lets you view and 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.
4. Specify CIR (kbps), CBS (bytes), EIR (kbps), and EBS (bytes).
5. Click Apply.

Figure 2-24.2: Bandwidth Profiles Configuration

The screenshot shows the Lantronix web interface for the SISPM1040-384-LRT-C device. The main content area is titled "Bandwidth Profiles Configuration". It 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", "Spanning Tree", "IPMC Profile", "MVR", "IPMC", "LLDP", "PoE", "EPS", and "MEP". The main configuration area shows a table of policer profiles. The table has the following columns: Policer ID, State, Type, Policer Mode, Rate Type, CIR (kbps), CBS (bytes), EIR (kbps), and EBS (bytes). The table contains 7 rows of data, all with State set to "Disabled" and Type set to "MEF".

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

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.

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 kilobit 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.

|<< : First page; updates the table, starting with the first entry in the table.

<< : Previous page; updates the table, ending at the entry before the first entry currently displayed.

>> : Next page; updates the table, starting with the entry after the last entry currently displayed.

>>| : Last page; 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.

2-24.3 EVCs

This page displays current EVC configurations. On this system, only Provider Bridge based EVCs are supported. An Ethernet Virtual Connection (EVC) 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 EVC is an association of two or more UNIs.

To configure EVCs Control list parameters via the web UI:


1. Click Configuration, Ethernet Services, and EVCs.
2. Click the  icon to add a new entry to configure.
3. Specify NNI Ports, EVC Parameters, and Inner Tag and Outer Tag parameters.
4. Click Apply.

Figure 2-24.3: EVC Control List Configuration

The screenshot displays the EVC Control List Configuration page. The top section shows a table with columns for EVC ID, VID, IVID, Learning, Inner Tag (Type, VID Mode, VID, PCP/DEI Preservation), Outer Tag (PCP, DEI, VID), and NNI Ports. A red circle highlights a plus icon in the bottom right corner of the table. A red arrow points down to the EVC Configuration page, which shows fields for NNI Ports (checkboxes 1-8), EVC Parameters (EVC ID, VID, IVID, Learning), Inner Tag (Type, VID Mode, VLAN ID, PCP/DEI Preservation, PCP, DEI), and Outer Tag (VLAN ID).

Parameter descriptions:

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. 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 aren'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 DEI 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.

NNI Ports : The list of Network to Network Interfaces for the EVC.

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 manually 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.

Example:

The screenshot displays the 'EVC Configuration' page for device 'SISPM1040-384-LRT-C'. The interface includes a left-hand navigation menu with categories like 'Switch', 'DMS', and 'Ethernet Services'. The main content area is divided into several sections:

- NNI Ports:** A table with 12 columns representing ports. Ports 2, 3, and 4 are checked with blue checkmarks.
- EVC Parameters:** A form with the following fields:
 - EVC ID: 1
 - VID: 10
 - IVID: 11
 - Learning: Enabled (dropdown menu)
- Inner Tag:** A form with the following fields:
 - Type: S-custom-tag (dropdown menu)
 - VID Mode: Tunnel (dropdown menu)
 - VLAN ID: 100
 - PCP/DEI Preservation: Preserved (dropdown menu)
 - PCP: 1 (dropdown menu)
 - DEI: 1 (dropdown menu)
- Outer Tag:** A form with the following field:
 - VLAN ID: 12

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

2-24.4 ECEs

This page lets you view and configure EVC Control Entries (ECEs). An ECE provides rules that are ordered in a list to control the preferred classification.

To set the ECE Control List Configuration in the web UI:


1. Click Configuration, Ethernet Services, and ECEs.
2. Click the  icon to add a new entry to configure.
3. Specify ECE ID, Ingress Matching, Actions and Egress outer Tag.
4. Click Apply.

Figure 2-24.4: ECE Control List Configuration

The screenshot displays the 'ECE Control List Configuration' web interface. At the top, there are 'Refresh' and 'Remove All' buttons. Below is a table with the following columns: ECE ID, Ingress Matching (UNI Ports, Tag Type, VID, PCP, DEI, Frame Type), Actions (Direction, EVC ID, Tag Pop Count, Policy ID, Class), Egress Outer Tag (Mode, PCP/DEI Preservation, PCP, DEI), and Conflict. A red circle highlights a plus icon in the bottom right corner of the table. Below the table is the 'ECE Configuration' form, which includes sections for UNI Ports (ports 1-8), Ingress Matching (Tag Type, Frame Type), Actions (Direction, EVC ID Filter, EVC ID Value, Tag Pop Count, Policy ID, Class), NSAC Parameters (NSAC Filter, NSAC Type), and Egress Outer Tag (Mode, PCP/DEI Preservation, PCP, DEI). At the bottom of the form are 'Apply', 'Cancel', and 'Reset' buttons.

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. Possible values are:

Specific: The valid range is 0 - 4095.

Any: The ECE will match any VLAN ID.

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

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, 0-3or 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 valid 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.

Egress Outer Tag

Outer Tag Mode : The outer tag for nni-to-uni direction for the ECE. 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. 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 PCP value for the ECE. The possible range is 0 - 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.

Modification Buttons

You can modify each ECE (EVC Control Entry) in the table using the following buttons:


: Inserts a new ECE before the current row.

: Edits the ECE row.

: Moves the ECE up the list.

: Moves the ECE down the list.

: Deletes the ECE.

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

Buttons:

Refresh –Click to manually refresh the page immediately.

Remove All- Click to remove all ECEs.

ECE Configuration Parameters

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

Tag Type : The tag type for matching 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.

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

The possible values are:

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

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

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

VLAN ID Value : When "Specific" is selected for the VLAN ID filter, you can enter a specific value.

The allowed range is 0 - 4095.

VLAN ID Range : When "Range" is selected for the VLAN ID filter, you can enter a specific range.

The allowed range is 0 - 4095.

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

Any: The ECE will match any PCP value.

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

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

DEI : The DEI value for matching the ECE. It is only significant if tag type 'Tagged' is selected. Allowed 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.

IP Parameters

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

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

UDP: Specify the UDP for matching the ECE.

TCP: Specify the TCP for matching the ECE.

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

Protocol Value : When "Specific" is selected for the protocol filter, you can enter a specific value.

The allowed value is 0 - 255.

SIP/DIP Filter : The source/destination IP address for matching the ECE. It depends on by the port address mode, when port address mode is set to 'Source' then the field is used for source address. Similarly, when port address mode is set to 'Destination' then the field is used for destination address. Possible values are:

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

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

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

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

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

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

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

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

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

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

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

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

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

Any: The ECE will match any MF bit.

Non-Fragment: IPv4 frames where the MF bit is set or the FRAG OFFSET field is greater than zero must not be able to match this entry.

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

UDP/TCP Parameters

Source Port Filter : The TCP/UDP source port for matching the ECE. It only significant if protocol filter 'UDP' or 'TCP' is selected. The possible values are:

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

Specific: If you want to filter a specific TCP/UDP source port No. with this ECE, choose this value. A field for entering a specific No. appears.

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

Source Port No. : When "Specific" is selected for the source port filter, you can enter a specific value. The allowed value is 0 - 65535.

Source Port Range : When "Range" is selected for the source port filter, you can enter a specific range. The allowed range is 0 - 65535.

Destination Port Filter : The TCP/UDP destination port for matching the ECE. It only significant if protocol filter 'UDP' or 'TCP' is selected. The possible values are:

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

Specific: If you want to filter a specific TCP/UDP destination port No. with this ECE, choose this value.

A field for entering a specific No. appears.

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

Destination Port No. : When "Specific" is selected for the destination port filter, you can enter a specific value. The allowed value is 0 - 65535.

Destination Port Range : When "Range" is selected for the destination port filter, you can enter a specific range. The allowed range is 0 - 65535.

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.

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. The possible values are:

Both: Bidirectional.

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

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

EVC ID Filter : The EVC ID for the ECE. The ECE is only active when mapping to an existing EVC. Possible values are:

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

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

EVC ID Value : When "Specific" is selected for the VLAN ID filter, you can enter a specific value. The allowed value is 1 - 256.

Tag Pop Count : The ingress tag pop count for the ECE. The allowed range is 0 - 2.

Policy ID : The ACL Policy ID for the ECE for matching ACL rules. The allowed range is 0 - 255.

Class : The traffic class for the ECE. The allowed range is 0 - 7 or disabled.

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. Possible values are:

Preserved: The outer tag PCP and DEI is preserved.

Fixed: The outer tag PCP and DEI is fixed.

Outer Tag PCP : The outer tag PCP value for the ECE. The allowed range is 0 - 7.

Outer Tag DEI : The outer tag DEI value for the ECE. The allowed value is 0 or 1.

Buttons

Apply: Click to save changes.

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

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

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	1,5,7-12	C-Tagged	Any	Any	Any	Any	Both	1	2	0	2	Enabled	Fixed	0	0	No

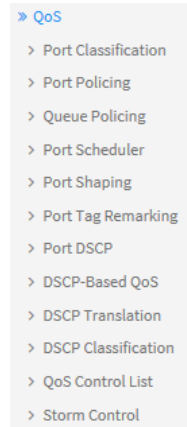
2-25 QoS

The switch supports four QoS queues per port with strict or weighted fair queuing scheduling.

It supports QoS Control Lists (QCL) for advanced programmable QoS classification, based on IEEE 802.1p, Ethertype, VID, IPv4/IPv6 DSCP and UDP/TCP ports and ranges.

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

The switch supports advanced memory control mechanisms providing excellent performance of all QoS classes under any traffic scenario, including jumbo frames. The switch provides 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.



2-25.1 Port Classification

This page lets you configure basic QoS Ingress Classification settings for all switch ports.

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.

Figure 2-25.1: QoS Ingress Port Classification

Port	CoS	DPL	PCP	DEI	Tag Class.	DSCP Based	Address Mode
*	<>	<>	<>	<>		<input type="checkbox"/>	<>
1	0	0	0	0	Disabled	<input type="checkbox"/>	Source
2	0	0	0	0	Disabled	<input type="checkbox"/>	Source
3	0	0	0	0	Disabled	<input type="checkbox"/>	Source
4	0	0	0	0	Disabled	<input type="checkbox"/>	Source
5	0	0	0	0	Disabled	<input type="checkbox"/>	Source
6	0	0	0	0	Disabled	<input type="checkbox"/>	Source
7	0	0	0	0	Disabled	<input type="checkbox"/>	Source
8	0	0	0	0	Disabled	<input type="checkbox"/>	Source

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

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

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 Tag Class. text [Disabled](#) to display the QoS Ingress Port Tag Classification page in order to configure the mode and/or mapping. See below.



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.

QoS Ingress Port Tag Classification page

When you click on the linked Tag Class. text **Disabled** the QoS Ingress Port Tag Classification page displays where you can configure Tagged Frame Settings for a port. The classification modes for tagged frames are configured on this page.

The screenshot shows the configuration page for Port 2. The 'Tag Classification' is currently set to 'Disabled'. Below this is a table for mapping PCP and DEI values to QoS classes and DP levels.

PCP	DEI	QoS class	DP level
*	*	< >	< >
0	0	1	0
0	1	1	1
1	0	0	0
1	1	0	1
2	0	2	0

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.

2-25.2 Port Policing

This section provides an overview of f QoS Ingress Port Policers for all switch ports The Port Policing is useful in constraining traffic flows and marking frames above specific rates. Policing is primarily useful for data flows and voice or video flows because voice and video usually maintains a steady rate of traffic

To set QoS Port Schedulers in the web UI:

1. Click Configuration, QoS, Port Policing.
2. Select the port to enable the QoS Ingress Port Policers and set the Rate limit condition.
3. Select the Rate limit Unit of kbps, Mbps, fps or kfps.
4. Click Apply to save the configuration.

Figure 2-25.2: QoS Ingress Port Policers

Port	Enable	Rate	Unit	Flow Control
*	<input checked="" type="checkbox"/>	500	<>	<input checked="" type="checkbox"/>
1	<input checked="" type="checkbox"/>	500	kbps	<input checked="" type="checkbox"/>
2	<input checked="" type="checkbox"/>	500	kbps	<input checked="" type="checkbox"/>
3	<input checked="" type="checkbox"/>	400	kbps	<input checked="" type="checkbox"/>
4	<input checked="" type="checkbox"/>	900	kbps	<input checked="" type="checkbox"/>
5	<input checked="" type="checkbox"/>	500	kbps	<input checked="" type="checkbox"/>
6	<input checked="" type="checkbox"/>	500	kbps	<input checked="" type="checkbox"/>
7	<input type="checkbox"/>	500	kbps	<input checked="" type="checkbox"/>
8	<input checked="" type="checkbox"/>	500	kbps	<input checked="" type="checkbox"/>
9	<input checked="" type="checkbox"/>	500	kbps	<input checked="" type="checkbox"/>

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 : Select the Port you want enabled for QoS Ingress Port Policers.

Rate : To set the Rate limit value for this port, the default is 500. Valid Rates are 100 – 3276700 kbps, 1 – 3276 Mbps, 100 – 3276700 fps, and 1 – 3276 kfps.

Unit : To scroll to 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.

2-25.3 Queue Policing

This page lets you configure the Queue Policer settings for all switch ports.

1. Click Configuration, QoS, and Queue Policing,
2. Specify the Queue Policing parameter.

Figure 2-25.3: QoS Ingress Queue Policers

The screenshot shows the Lantronix web interface for configuring QoS Ingress Queue Policers. The page title is "QoS Ingress Queue Policers" and the breadcrumb trail is "Home > Configuration > QoS > Queue Policing". 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", "Spanning Tree", "IPMC Profile", "MVR", "IPMC", "LLDP", "PoE", and "EPS".

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	Enable	Enable	Enable	Enable	Enable
*	<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	kbps	<input type="checkbox"/>	500	kbps	<input type="checkbox"/>	500	kbps	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
2	<input checked="" type="checkbox"/>	500	kbps	<input checked="" type="checkbox"/>	500	kbps	<input type="checkbox"/>	500	kbps	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
3	<input checked="" type="checkbox"/>	500	kbps	<input checked="" type="checkbox"/>	500	kbps	<input checked="" type="checkbox"/>	500	kbps	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
4	<input checked="" type="checkbox"/>	500	kbps	<input type="checkbox"/>	500	kbps	<input type="checkbox"/>	500	kbps	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
5	<input checked="" type="checkbox"/>	500	kbps	<input type="checkbox"/>	500	kbps	<input type="checkbox"/>	500	kbps	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
6	<input type="checkbox"/>	500	kbps	<input type="checkbox"/>	500	kbps	<input type="checkbox"/>	500	kbps	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
7	<input checked="" type="checkbox"/>	500	kbps	<input type="checkbox"/>	500	kbps	<input type="checkbox"/>	500	kbps	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
8	<input checked="" type="checkbox"/>	500	kbps	<input type="checkbox"/>	500	kbps	<input type="checkbox"/>	500	kbps	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Parameter descriptions:

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

E (Enable) : 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 is 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 is enabled.

Buttons:

Apply – Click to save changes.

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

2-25.4 Port Scheduler

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

Web Interface

To display the QoS Port Schedulers in the web interface:

1. Click Configuration, QoS, Port Schedulers.
2. Display the QoS Egress Port Schedulers.

Figure 2-25.4: QoS Egress Port Schedulers

The screenshot displays the QoS Egress Port Scheduler configuration interface. It is divided into three main sections:

- QoS Egress Port Schedulers Table:** A table with columns for Port, Mode, and queues Q0 through Q5. Port 1 is highlighted with a red box and a blue callout box that says "Click the Port index to set the QoS Egress Port Schedulers".
- QoS Egress Port Scheduler and Shapers Port 1 (Top):** A configuration panel for Port 1, showing "Port" set to "Port 1" and "Scheduler Mode" set to "Strict Priority".
- QoS Egress Port Scheduler and Shapers Port 1 (Bottom):** A detailed configuration panel for Port 1. It shows "Queue Shaper" and "Port Shaper" sections, both with "Enable Rate Unit Excess" checked. The Queue Shaper section displays a diagram with queues Q0 through Q7, each with a rate of 500 kbps. The Port Shaper section shows a rate of 500 kbps. A blue callout box points to the "Scheduler Mode" dropdown, stating: "If you select the scheduler mode with weighted then the screen will change as the figure shows." At the bottom are "Apply", "Reset", and "Cancel" buttons.

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.

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 "6 Queues Weighted" on this switch port.



Strict Priority
6 Queues Weighted

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". This value is restricted to 1-100. This parameter is only shown if "Scheduler Mode" is set to "6 Queues Weighted".

Queue Scheduler Percent : Shows the weight in percent for this queue. This parameter is only shown if "Scheduler Mode" is set to "6 Queues 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.

2-25.5 Port Shaping

This section provides an overview of QoS Egress Port Shapers for all switch ports.

To display the QoS Port Shapers in the web interface:

1. Click Configuration, QoS, Port Shapers.
2. Configure the QoS Egress Port Shapers.

Figure 2-25.5: QoS Egress Port Shapers

QoS Egress Port Shapers

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

QoS Egress Port Scheduler and Shapers Port 1

Port: Port 1

Scheduler Mode: Strict Priority

Queue Shaper: Enable Rate Unit Excess

Port Shaper: Enable Rate Unit

STRICT

500 kbps

500 kbps

500 kbps

500 kbps

500 kbps

500 kbps

500 kbps

500 kbps

500 kbps

500 kbps

500 kbps

Apply Reset Cancel

Parameter descriptions:

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

Mode : Shows the scheduling mode for this port.

Shapers (Qn) : Shows "disabled" or actual queue shaper rate - e.g. "800 Mbps".

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". This value is restricted to 1-100. This parameter is only shown if "Scheduler Mode" is set to "Weighted".

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

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

Port Shaper Rate : Controls the rate for the port shaper. 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 : Click to cancel unsaved changes.

2-25.6 Port Tag Remarking

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

To display the QoS Port Tag Remarking in the web interface:

1. Click Configuration, QoS, Port Tag Remarking.
2. Click a linked Port number to display the QoS Port Tag Remarking page for the selected port.
3. Set the page parameters and click the Apply button.

Figure 2-25.6: Port Tag Remarking

The screenshot displays the 'QoS Egress Port Tag Remarking' web interface. At the top, a breadcrumb trail reads 'Home > Configuration > QoS > Port Tag Remarking'. Below this is a table with two columns: 'Port' and 'Mode'. The table contains four rows, with the first row (Port 1) highlighted in blue. A red box highlights the '1' in the 'Port' column of the first row, and a blue arrow points from a text box to it. The text box contains the instruction: 'Click the Port index to set the QoS Port Tag Remarking'. Below the table, there are two configuration panels for 'Port 1'. The first panel, titled 'QoS Egress Port Tag Remarking Port 1', has a breadcrumb trail 'Home > Configuration > QoS > Port Tag Remarking'. It contains a 'Port' dropdown menu set to 'Port 1' and a 'Tag Remarking Mode' dropdown menu set to 'Classified'. Below these are 'Apply' and 'Reset' buttons. The second panel, also titled 'QoS Egress Port Tag Remarking Port 1', has the same breadcrumb trail. It contains a 'Port' dropdown menu set to 'Port 1' and a 'Tag Remarking Mode' dropdown menu set to 'Default'. Below these are 'PCP/DEI Configuration' fields: 'Default PCP' and 'Default DEI', both set to '0'. At the bottom are 'Apply' and 'Reset' buttons.

The screen below shows QoS Egress Port Tag Remarking for Port 1 with Tag Remarking Mode set to Mapped. The QoS Egress Port Tag Remarking for a specific port are configured on this page.

The screenshot shows the configuration page for QoS Egress Port Tag Remarking on Port 1. The configuration is as follows:

QoS class	DP level	PCP	DEI
*	*	<>	<>
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

Port : At the dropdown select the desired port number.

Tag Remarking Mode : Select the tag remarking mode for this port.

Classified: Use classified PCP/DEI values.

Default: Use default PCP/DEI values.

Mapped: Use mapped versions of QoS class and DP level.

The dropdown menu for Tag Remarking Mode shows the following options: Mapped (selected), Classified, Default, and Mapped.

(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.

PCP : Controls the default PCP values used when the mode is set to Default.

DEI : Controls the default DEI values used when the mode is set to Default

Buttons:

Apply – Click to save changes.

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

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.

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.

2-25.7 Port DSCP

This page lets you configure basic QoS Port DSCP settings for all switch ports.

1. Click Configuration, QoS, Port DSCP.
4. Enable or disable the Ingress Translate and select the Ingress Classify parameters.
5. Select the Egress Rewrite parameters.
6. Click the Apply button to save the settings.
7. To cancel the settings, click the Reset button to revert to previously saved values.

Figure 2-25.7: QoS Port DSCP Configuration

Port	Ingress		Egress
	Translate	Classify	Rewrite
*	<input type="checkbox"/>	<>	<>
1	<input type="checkbox"/>	Disable	Disable
2	<input checked="" type="checkbox"/>	DSCP=0	Enable
3	<input checked="" type="checkbox"/>	Selected	Remap DP Unaware
4	<input checked="" type="checkbox"/>	All	Remap DP Aware
5	<input checked="" type="checkbox"/>	Selected	Enable
6	<input type="checkbox"/>	Disable	Disable
7	<input checked="" type="checkbox"/>	Disable	Remap DP Unaware
8	<input checked="" type="checkbox"/>	Disable	Remap DP Aware

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:

1. **Translate :** To Enable the Ingress Translation click the checkbox.
2. **Classify:** Classification for a port 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.

Egress : Port Egress Rewriting can be one of three 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.

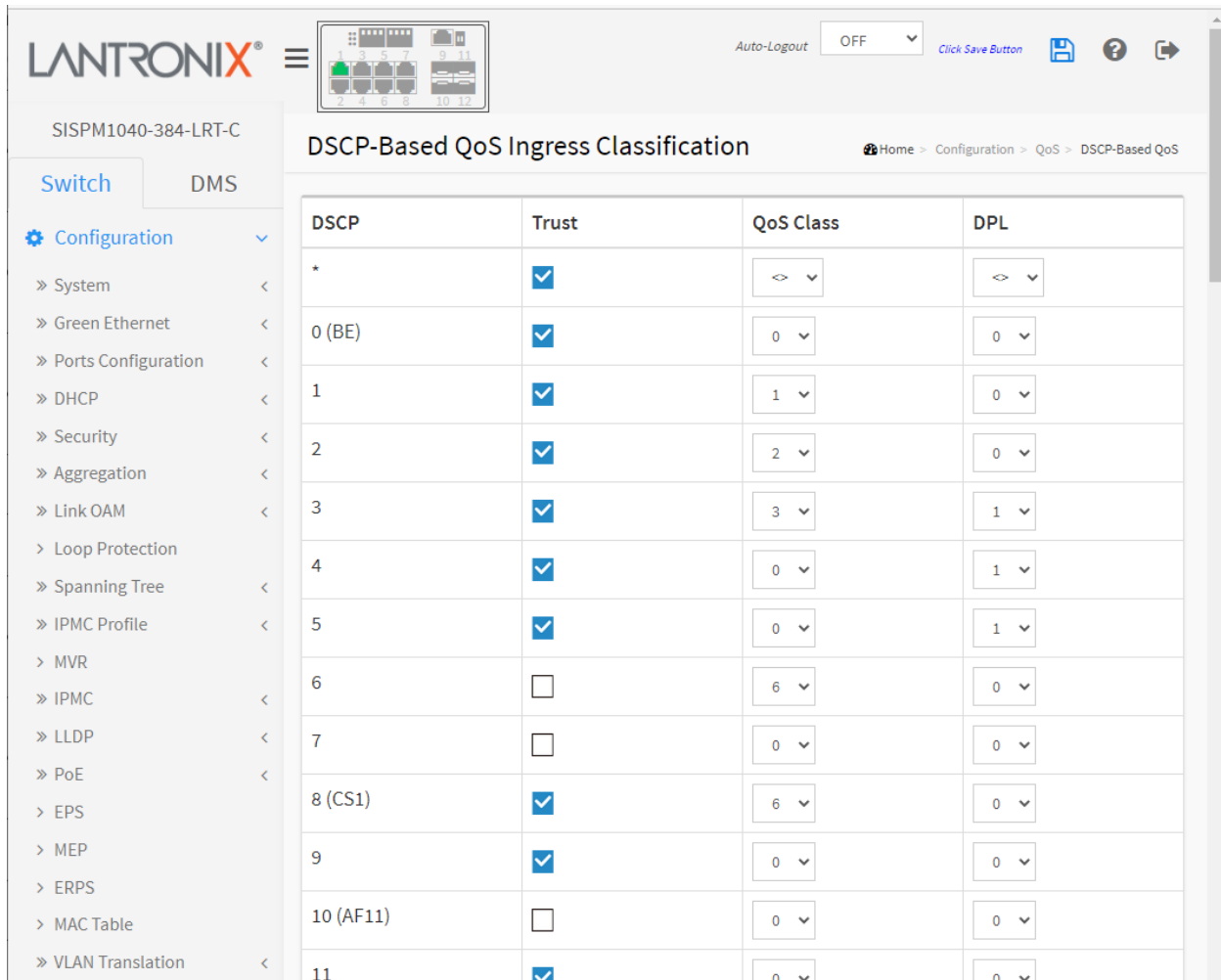
Reset- Click to undo any changes made locally and revert to previously saved values.

2-25.8 DSCP-Based QoS

This page lets you configure basic QoS DSCP-based QoS Ingress Classification settings for the switch.

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 setting.
5. To cancel the setting click the Reset button to previously saved values.

Figure 2-25.8: DSCP-Based QoS Ingress Classification



The screenshot shows the Lantronix web interface for the SISPM1040-384-LRT-C switch. The main configuration area is titled "DSCP-Based QoS Ingress Classification". A navigation menu on the left includes "Switch" and "DMS" sections. The "Configuration" menu is expanded, showing 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, and VLAN Translation. The main table is as follows:

DSCP	Trust	QoS Class	DPL
*	<input checked="" type="checkbox"/>	< >	< >
0 (BE)	<input checked="" type="checkbox"/>	0	0
1	<input checked="" type="checkbox"/>	1	0
2	<input checked="" type="checkbox"/>	2	0
3	<input checked="" type="checkbox"/>	3	1
4	<input checked="" type="checkbox"/>	0	1
5	<input checked="" type="checkbox"/>	0	1
6	<input type="checkbox"/>	6	0
7	<input type="checkbox"/>	0	0
8 (CS1)	<input checked="" type="checkbox"/>	6	0
9	<input checked="" type="checkbox"/>	0	0
10 (AF11)	<input type="checkbox"/>	0	0
11	<input checked="" type="checkbox"/>	0	0

Parameter descriptions:

DSCP : Maximum number of supported DSCP values are 64.

Trust : Click to check if the DSCP value is trusted. Controls whether a specific DSCP value is trusted. Only frames with trusted DSCP values are mapped to a specific QoS class and Drop Precedence Level. Frames with untrusted DSCP values are treated as a non-IP frame.

QoS Class : QoS Class value can be 0-7.

DPL : Drop Precedence Level (0-3).

Buttons:

Apply – Click to save changes.

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

2-25.9 DSCP Translation

This page lets you configure the basic QoS DSCP Translation settings for the switch. DSCP translation can be done in Ingress or Egress.

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.

Figure 2-25.9: DSCP Translation

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 checked="" type="checkbox"/>	1	1
2	8 (CS1)	<input checked="" type="checkbox"/>	8 (CS1)	10 (AF11)
3	10 (AF11)	<input checked="" type="checkbox"/>	3	14 (AF13)
4	13	<input checked="" 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)

Parameter descriptions:

DSCP : Maximum number of supported DSCP values is 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 the 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.

Buttons:

Apply: Click to save changes.

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

2-25.10 DSCP Classification

This page lets you configure the mapping of QoS class and Drop Precedence Level to DSCP value.

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.

DSCP (Differentiated Services Code Point) is a field in the header of IP packets for packet classification purposes.

To set DSCP Classification parameters in the web UI:

1. Click Configuration, QoS, DSCP Translation.
2. Set the DSCP parameters.
3. Click the Apply button to save the settings.

Figure 2-25.10: DSCP Classification

The screenshot shows the 'DSCP Classification' configuration page in the Lantronix web UI. The page title is 'DSCP Classification' and the breadcrumb trail is 'Home > Configuration > QoS > DSCP Classification'. The interface includes a navigation menu on the left with 'Configuration' selected. The main content area contains a table with the following data:

QoS Class	DSCP DP0	DSCP DP1
*	<>	<>
0	63	19
1	1	0 (BE)
2	2	18 (AF21)
3	3	17
4	0 (BE)	16 (CS2)
5	0 (BE)	0 (BE)
6	0 (BE)	0 (BE)
7	0 (BE)	0 (BE)

At the bottom of the table, there are 'Apply' and 'Reset' buttons.

Parameter descriptions:

QoS Class : The actual QoS class.

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.

2-25.11 QoS Control List

This page lets you edit / insert a single QoS Control Entry at a time. A QCE consists of several parameters. These parameters vary according to the frame type that you select.

This page shows the QoS Control List (QCL), which is made up of QCEs. Each row describes a QCE that is defined. You can have up to 256 QCEs per switch.

A **QCE** (QoS Control Entry) describes QoS class associated with a particular QCE ID. There are six QCE frame types: Ethernet Type, VLAN, UDP/TCP Port, DSCP, TOS, and Tag Priority. Frames are classified by one of 4 different QoS classes: "Low", "Normal", "Medium", and "High" for individual applications.

A **QCL** (QoS Control List) is a table that lists QCEs containing QoS control entries that classify to a specific QoS class on specific traffic objects. Each accessible traffic object contains an identifier to its QCL. The privileges determine specific traffic object to specific QoS class.

Web Interface

To configure the QoS Control List parameters in the web UI:


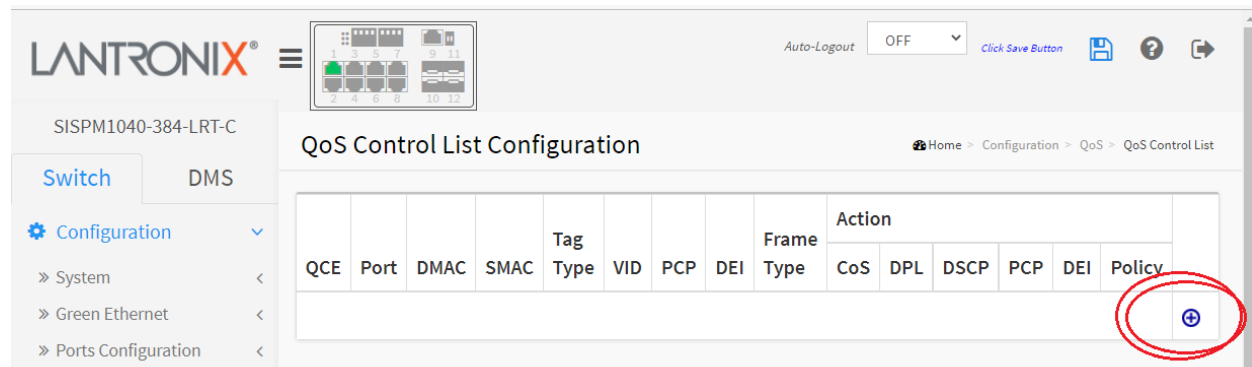
1. Click Configuration, QoS, QoS Control List.
2. Click the Add QCE icon () to add a new QoS Control List.

Figure 2-25.11: QoS Control List Configuration



The screenshot displays the Lantronix web interface for QoS Control List Configuration. The interface includes a navigation menu on the left with options like 'Switch', 'DMS', 'Configuration', 'System', 'Green Ethernet', and 'Ports Configuration'. The main content area shows a table with columns for QCE, Port, DMAC, SMAC, Tag Type, VID, PCP, DEI, Frame Type, Action, CoS, DPL, DSCP, PCP, DEI, and Policy. A red circle highlights the '+ Add QCE' button in the bottom right corner of the table.

3. Select all parameters and select the Port Member to join the QCE rules.
4. Click the Apply button to save the settings.

Figure 2-25.11: QCE Configuration

SISPM1040-384-LRT-C

QCE Configuration

Home > Configuration > QoS > QoS Control List

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**
 - Port Classification
 - Port Policing
 - Queue Policies

Port Members

1	2	3	4	5	6	7	8	9	10	11	12
<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 checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

DMAC

SMAC

Tag

VID

PCP

DEI

Frame Type

Action Parameters

CoS

DPL

DSCP

PCP

DEI

Policy

Apply Reset Cancel

Port Members: Check the checkbox button to include the port in the QCL entry. By default all ports are included.

DMAC : Indicates the destination MAC address. Possible values are:

Any: Match any DMAC. The default value is 'Any'.

Unicast: Match unicast DMAC.

Multicast: Match multicast DMAC.

Broadcast: Match broadcast DMAC.

<MAC>: Match specific DMAC.

SMAC : Match specific source MAC address or 'Any'. If a port is configured to match on DMAC/DIP, this field indicates the DMAC.

Tag: Indicates tag type. Possible values are:

Any: Match tagged and untagged frames. The default value is 'Any'.

Untagged: Match untagged frames.

Tagged: Match tagged frames.

C-Tagged: Match C-tagged frames.

S-Tagged: Match S-tagged frames.

VID : Indicates (VLAN ID), either a specific VID or range of VIDs. VID can be in the range 1-4095 or 'Any'

PCP : Priority Code Point: Valid values of PCP are specific (0, 1, 2, 3, 4, 5, 6, 7) or range(0-1, 2-3, 4-5, 6-7, 0-3, 4-7) or 'Any'.

DEI : Drop Eligible Indicator: Valid value of DEI is 0, 1 or 'Any'.

Frame Type : Select one of these values: Any, Ethernet, LLC, SNAP, IPv4, or IPv6., as explained below

1. **Any** : Allow all types of frames.
2. **EtherType** : Valid value can be **0x600 - 0xFFFF** excluding 0x800 (IPv4) and 0x86DD (IPv6) or 'Any'.
3. **LLC** : Select:

DSAP Address: Valid DSAP(Destination Service Access Point) can be 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'.

4. **SNAP** : PID Valid PID(a.k.a Ether Type) can be 0x0000-0xFFFF or 'Any'.

5. **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. 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.

6. **IPv6** : Protocol IP protocol number: (0-255, 'TCP' or 'UDP') or 'Any'.

Source IP 32 LS bits of IPv6 source address in value/mask format or 'Any'. 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.

Action Parameters : Indicates the classification action taken on ingress frame if parameters configured are matched with the frame's content. The action fields are:

CoS : Class of Service: (0-7) or 'Default'.

DP : Drop Precedence Level: (0-1) or 'Default'.

DSCP (Differentiated Services Code Point): (0-63, BE, CS1-CS7, EF or AF11-AF43) or 'Default'.

PCP (Priority Code Point) : (0-7) or 'Default'. Note: PCP and DEI cannot be set individually.

DEI (Drop Eligible Indicator): Select (0-1) or 'Default'.

Policy : ACL Policy number: (0-255) or 'Default' (empty field). 'Default' means that the default classified value is not modified by this QCE.

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.

Buttons:

Apply – Click to save changes.

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

QoS Control List Configuration Example:

The screenshot shows the Lantronix web interface for the SISPM1040-384-LRT-C switch. The main content area is titled "QoS Control List Configuration". On the left, there is a navigation menu with "Configuration" selected. The table below shows the following entries:

QCE	Port	DMAC	SMAC	Tag Type	VID	PCP	DEI	Frame Type	Action						
									CoS	DPL	DSCP	PCP	DEI	Policy	
1	Any	Any	Any	Any	Any	Any	Any	Any	0	Default	Default	Default	Default	Default	
2	Any	Any	Any	Untagged	Any	Any	Any	EtherType	1	Default	Default	Default	Default	Default	
3	Any	Any	Any	Any	Any	Any	Any	LLC	3	Default	8 (CS1)	Default	Default	1	
4	Any	Any	Any	Any	Any	Any	Any	IPv4	4	1	0 (BE)	Default	Default	1	

2-25.12 Storm Control

This page lets you configure 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 without a (VLAN ID, DMAC) pair 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 Policer 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 to revert to previously saved values.

Figure 2-25.12: Storm Policer Configuration

Frame Type	Enable	Rate	Unit
Unicast	<input checked="" type="checkbox"/>	512	kfps
Multicast	<input checked="" type="checkbox"/>	1024	kfps
Broadcast	<input type="checkbox"/>	1	fps

Parameter descriptions:

Frame Type : The settings in a particular row apply to the frame type listed here: Unicast, Multicast or Broadcast.

Enable : Enable or disable the storm control status for the given frame type.

Rate : The rate unit is packets per second (pps). Valid values are: 1, 2, 4, 8, 16, 32, 64, 128, 256, 512, 1K, 2K, 4K, 8K, 16K, 32K, 64K, 128K, 256K, 512K or 1024K, 1024K, 2048K, 4096K, 8192K, 16384K or 32768K , or 1024K. The 1 kpps is actually 1002.1 pps.

Unit : Controls the unit of measure for the global storm policer rate as fps or kfps.

Buttons:

Apply – Click to save changes.

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

2-26 Mirroring and Remote Mirroring

Mirroring is a feature for use with a switched port analyzer 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 the tagged mirrored traffic, set VLAN egress tagging as "Tag All" on the reflector port. Otherwise, to get untagged mirrored traffic, set VLAN egress tagging as "Untag ALL" on the reflector port.

To configure Mirroring in the web UI:

1. Click Configuration, Mirroring.
2. Select the Stack Global Settings and Source VLAN(s) Configuration parameters.
3. Select the Port Configuration parameters.

Figure 2-26: Mirroring & Remote Mirroring Configuration

The screenshot displays the 'Mirroring & Remote Mirroring Configuration' page in the Lantronix web UI. The interface includes a navigation menu on the left, a breadcrumb trail at the top right, and an 'Auto-Logout' dropdown set to 'OFF'. The main content area is organized into three sections:

- Stack Global Settings:**
 - Mode: Enabled
 - Type: Mirror
 - VLAN ID: 200
 - Reflector Port: Port 1
- Source VLAN(s) Configuration:**
 - Source VLANs: (Empty text input field)
- Port Configuration:**

Port	Source	Intermediate	Destination
1	Both	<input type="checkbox"/>	<input type="checkbox"/>
2	Rx only	<input type="checkbox"/>	<input checked="" type="checkbox"/>
3	Tx only	<input type="checkbox"/>	<input type="checkbox"/>
4	Disabled	<input type="checkbox"/>	<input type="checkbox"/>
5	Disabled	<input type="checkbox"/>	<input type="checkbox"/>
6	Disabled	<input type="checkbox"/>	<input type="checkbox"/>
7	Disabled	<input type="checkbox"/>	<input type="checkbox"/>

Parameter descriptions:

Global Settings

Mode : Use to **Enable/Disable** the mirror or Remote Mirroring function.

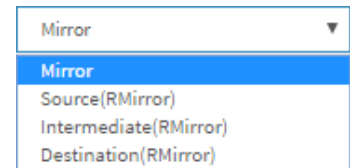
Type : Select switch type; Mirror, Source(RMirror), Intermediate(RMirror), or Destination(RMirror):

Mirror: The switch is running on mirror mode. The source port(s) and destination port are located on this switch (default).

Source: 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: 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: 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.

Note1: The reflector port needs to select only on Source switch type.

Note2: The reflector port needs to disable MAC Table learning and STP.

Note3: The reflector port only supports on pure copper ports.

Source VLAN(s) Configuration: The switch can support VLAN-based Mirroring. If you want to monitor some VLANs on the switch, you can set the selected VLANs on this field.

Note1: The Mirroring session shall have either ports or VLANs as sources, but not both.

Port Configuration for Remote Mirroring : The table is used for port role selection:

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

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.

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 needs to disable MAC Table learning.

Destination: Select destination port. This checkbox is designed for mirror or Remote mirroring. The destination port is a switched port that you receive a copy of traffic from the source port.

Note1: On mirror mode, the device only supports one destination port.

Note2: 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 must check whether or not other features are enabled or disabled. For example, the administrator has not disabled the MSTP on reflector port. All monitor traffic will be blocked on reflector port. All recommended settings are shown below and described in the online Help.

	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				



NOTE: For a given port, a frame is only transmitted once. It is therefore not possible to mirror Tx frames on the mirror port. Because of this, mode for the selected mirror port is limited to Disabled or Rx only.

Buttons:

Apply – Click to save changes.

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

2-27 UPnP

UPnP is an acronym for Universal Plug and Play. UPnP 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 in the web UI:

1. Click Configuration, UPnP.
2. Select the UPnP mode to Enabled. The default is Disabled.
3. Specify the parameters in each blank field and click the Apply button to save the settings.

Figure 2-27: UPnP Configuration

The screenshot shows the Lantronix web interface for configuring UPnP. The page title is "UPnP Configuration" and the breadcrumb is "Home > Configuration > UPnP". The "Mode" is set to "Disabled", "TTL" is "4", and "Advertising Duration" is "100". There are "Apply" and "Reset" buttons at the bottom.

Mode	Disabled
TTL	4
Advertising Duration	100

Parameter descriptions:

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

Enabled: Enable UPnP mode operation.

Disabled: Disable UPnP mode operation. When the mode is enabled, two ACEs are added automatically to trap UPnP related packets to CPU. The ACEs are automatically removed when the mode is disabled. .

TTL : The Time To Live 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. The switch sends SSDP messages periodically at the interval one-half of the advertising duration minus 30 seconds. Valid values are 66 - 86400.

Buttons:

Apply – Click to save changes.

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

2-28 PTP

This page lets you set the current Precision Time Protocol clock settings. To configure PTP in the web UI:

1. Click Configuration, PTP.
2. Set the PTP External Clock Mode parameters.
3. Click the Add New PTP Clock button to create a new clock instance.
4. Enter the Clock Instance, Device Type, and Profile parameters.
4. Click the Apply button to save the settings. You can enter multiple Clock Instances per Apply.
5. Click a linked Clock Instance and configure its parameters.

Figure 2-28: PTP Config

The screenshot shows the web UI for configuring PTP. The main configuration area is titled "PTP External Clock Mode". It contains the following parameters:

- One_PPS_Mode:** A dropdown menu set to "Disable".
- External Enable:** A dropdown menu set to "False".
- Adjust Method:** A dropdown menu set to "LTC frequency".
- Clock Frequency:** A text input field set to "1".

Below these parameters is the "PTP Clock Configuration" table:

Delete	Clock Instance	Device Type	Profile
Delete	0	Ord-Bound	No Profile
Delete	0	Ord-Bound	No Profile
Delete	0	Ord-Bound	No Profile
Delete	0	Ord-Bound	No Profile

At the bottom of the table are three buttons: "Add New PTP Clock", "Apply", and "Reset".

Parameter descriptions:

PTP External Clock Configuration

One_PPS_Mode : Selection box to select the One_pps_mode configuration, where "One_pps" means "output one pulse per second timing signal". These values are possible:

Output : Enable the 1 pps clock output.

Input : Enable the 1 pps clock input.

Disable : Disable the 1 pps clock input/output.

OutInput: Enable the 1 pps clock input/output.

Disable
Output
Input
OutInput

External Enable : Selection box to configure the External Clock output. These values are possible:

True : Enable the external clock output.

False : Disable the external clock output.

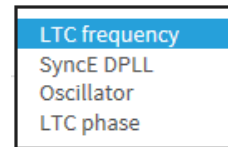
Adjust Method : Selection box to configure the Frequency adjustment configuration:

LTC frequency : Select Local Time Counter (LTC) frequency control.

SyncE-DPLL : Select SyncE DPLL 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 : Sets the Clock Frequency. The range of values is 1 – 25000000 Hz (1 - 25MHz).

PTP Clock Configuration

Delete : Check this box and click on 'Save' to delete the clock instance.

Clock Instance : Indicates the Instance of a particular Clock Instance [0..3]. Click on the Clock Instance number to edit the Clock details.

Device Type : Indicates the Type of the Clock Instance. There are five Device Types.

Ord-Bound - clock's Device Type is Ordinary-Boundary Clock.

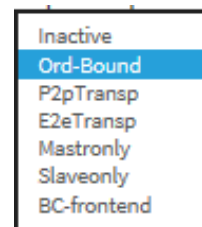
P2pTransp - clock's Device Type is Peer to Peer Transparent Clock.

E2eTransp - clock's Device Type is End to End Transparent Clock.

Masteronly - clock's Device Type is Master Only.

Slaveonly - clock's Device Type is Slave Only.

BC-frontend – clock Device Type is Boundary Clock – Front end.



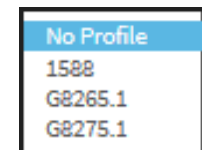
Profile: Select a timing profile:

No Profile: Do not use any PTP profile.

1588: Use [IEEE 1588](#) precision time protocol (PTP).

G8265.1: Use ITU-T [G.8265.1](#) / [Y.1365.1](#) Precision time protocol telecom profile for frequency synchronization.

G8275.1: Use [ITU-T G.8275](#) / [Y.1369](#) Architecture and requirements for packet-based time and phase distribution.



Port List : Check each port to be 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 : Displays the 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.

PTP Clock's Configuration and Status

You can click a linked Clock Instance and configure its parameters:

The screenshot displays the 'PTP Clock's Configuration and Status' page. The left sidebar shows a navigation menu with 'PTP' selected. The main content area is divided into several sections:

- Clock Type and Profile**: A table with columns for Clock Instance (0), Device Type (Mastronly), Profile (1588), and an 'Apply Profile Defaults' button.
- Port Enable and Configuration**: A 'Port Enable' section with checkboxes for ports 1 through 8, and a 'Configuration' link.
- Local Clock Current Time**: A 'PTP Time' field (1970-01-03T01:32:33+00:00 659,977,360) and a 'Clock Adjustment method' dropdown (VCO). A 'Synchronize to System Clock' button is present.
- Clock Current Data Set**: A table with columns for stpRm (0), Offset From Master (0.000,000,000), and Mean Path Delay (0.000,000,000).
- Clock Parent Data Set**: A table with columns for Parent Port ID, Port, PStat, Var, Rate, GrandMaster ID, GrandMaster Clock Quality, Pri1, and Pri2.
- Clock Default Data Set**: A table with columns for Clock ID, Device Type, 2 Step Flag, Ports, Clock Identity, Dom, and Clock Quality. Below this is a table with columns for Pri1, Pri2, Protocol, One-Way, VLAN Tag Enable, VID, PCP, and DSCP.

> UDLD	128	128	Ethernet	False	False	1	0	0
> Rapid Ring	Clock Time Properties DataSet							
> SMTP	UtcOffset	Valid	Leap59	Leap61	Time Trac	Freq Trac	PTP Time Scale	Time Source
Monitor	0	False	False	False	False	False	True	160
Diagnostics	Filter Parameters							
Maintenance	Filter Type	Delay Filter			Period	Dist		
	Basic	6			1	2		
	Servo Parameters							
	Display	P-enable	I-enable	D-enable	'P' constant	'I' constant	'D' constant	
	False	True	True	True	3	80	40	
	Unicast Slave Configuration							
	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		
	3	100	0.0.0.0		0	IDLE		
	4	100	0.0.0.0		0	IDLE		
	Apply		Reset					

Buttons:

Add New PTP Clock: Click to create a new clock instance.

Apply: Click to save the page immediately.

Reset: Click to reset the page immediately.

Ports Configuration: Click to display the PTP Clock's Port Data Set Configuration page (see below).

Apply Profile Defaults: Click to apply defaults as the parameter settings.

Synchronize to System Clock : Click to synchronize page parameters to the system clock.

PTP Clock's Port Data Set Configuration

The port data set is defined in the IEEE 1588 Standard. It holds three groups of data: the static members, the dynamic members, and configurable members which can be set here.

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	0	0	2
3	dsbl	3	0.000,000,000	0	3	0	e2e	0	0	0	0	2
4	dsbl	3	0.000,000,000	0	3	0	e2e	0	0	0	0	2

Port: Static member port Identity : Port number [1..max port no].

Stat: Dynamic member portState: Current state of the port.

MDR: Dynamic member log Min Delay Req Interval: The delay request interval announced by the master.

Peer Mean Path Del: The path delay measured by the port in P2P mode. In E2E mode this value is 0

Anv: The interval for issuing announce messages in Master state. Range is -3 to 4.

ATo: The timeout for receiving announce messages on the port. Range is 1 to 10.

Syv: The interval for issuing sync messages in master. Range is -7 to 4.

Dlm: Configurable member delayMechanism: The delay mechanism used for the port:

e2e: End to end delay measurement

p2p: Peer to peer delay measurement.

Can be defined per port in an Ordinary/Boundary clock. In a transparent clock all ports use the same delay mechanism, determined by the clock type.

MPR: The interval for issuing Delay_Req messages for the port in E2e mode. This value is announced from the master to the slave in an announce message. The value is reflected in the MDR field in the Slave The interval for issuing Pdelay_Req messages for the port in P2P mode **Note:** The interpretation of this parameter has changed from release 2.40. In earlier versions the value was interpreted relative to the Sync interval, which was a violation of the standard, so now the value is interpreted as an interval (i.e., $MPR = 0 \Rightarrow 1 \text{ Delay_Req pr sec}$, independent of the Sync rate). Range is -7 to 5.

Delay Asymmetry: If the transmission delay for a link is not symmetric, the asymmetry can be configured here, see IEEE 1588 Section 7.4.2 Communication path asymmetry Range is -100000 to 100000. Version The current implementation only supports PTP version 2.

Ingress latency: measured in ns, as defined in IEEE 1588 Section 7.3.4.2. Range is -100000 to 100000.

Egress Latency: measured in ns, as defined in IEEE 1588 Section 7.3.4.2. Range is -100000 to 100000.

PTP Troubleshooting

Problem: P2P Transparent Test Fails with another Peer Device.

Description: The Slave state never becomes locked, and no delay or offset is observed on the non-SISPM1040-3xx-LRTx Peer device. The SISPM1040-3xx-LRTx is not recognized as a PTP device by a peer PTP capable device. In a Transparent P2P test if the Master or peer device is configured, the PTP port is shown as disabled on the SISPM1040-3xx-LRTx device. If all SISPM1040-3xx-LRTx switches are used in the configuration, the PTP setup works as expected.

Workaround: **1.** Use all SISPM1040-3xx-LRTx devices if possible. **2.** Contact Technical Support.

2-29. GVRP

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

A GARP participation in a switch or an end station consists of a GARP application component, and a GARP Information Declaration (GID) component associated with each port or the switch.

The propagation of information between GARP participants for the same application in a bridge is carried out by the GARP Information Propagation (GIP) component. Protocol exchanges take place between GARP participants by means of LLC Type 1 services, using the group MAC address and PDU format defined for the GARP application concerned.

To configure GVRP in the web UI:

1. Click Configuration, GVRP, Global Config.
2. Specify Join-time, Leave-time, Leave All-time, and Max VLANs.
3. Click Apply.

Figure 2-29.1: GVRP Configuration

Parameter	Value
Enable GVRP	<input type="checkbox"/>
Join-time:	20 (1-20)
Leave-time:	60 (60-300)
LeaveAll-time:	1000 (1000-5000)
Max VLANs:	20

Parameter descriptions:

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

GVRP protocol timers

Join-time is a value in the range 1-20 in 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 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 units of centi seconds (i.e., in units of one hundredth of a second). The default is 1000.

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

Buttons:

Apply: Click to save changes.

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

2-29.2 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 ports via the web UI:

1. Click Configuration, GVRP, Port Configuration.
2. Specify the Mode for each Port.
3. Click Apply.

Figure 2-29.2: GVRP Port Configuration

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

Parameter descriptions:

Port: The logical port that is to be configured.

Mode: Select either 'Disabled' or 'GVRP enabled'. These values turn the GVRP feature off or on respectively for each individual port.

Disabled: Select to Disable GVRP mode on this port.

Enable GVRP: 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.

2-30. 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 (aka, 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. See IETF [RFC 3176](https://www.rfc-editor.org/rfc/rfc3176) for more information.

To configure the sFlow Agent in the web UI:

1. Click Configuration, sFlow.
2. Set the Agent, Receiver, and Port config 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 2-30: sFlow Configuration

SISPM1040-362-LRT

Switch DMS

sFlow Configuration

Home - Configuration - sFlow

Agent Configuration

IP Address: 127.0.0.1

Receiver Configuration

Owner: <None> [Release]

IP Address/Hostname: 0.0.0.0

UDP Port: 6343

Timeout: 0 seconds

Max. Datagram Size: 1400 bytes

Port Configuration

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

Apply Reset

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 via the Web or CLI, Owner contains <Configured through local management>.
- If sFlow is currently configured via SNMP, Owner contains a string identifying the sFlow receiver. If sFlow is configured through SNMP, all controls - except for the Release-button - are disabled to avoid inadvertent reconfiguration.

The **Release** button allows for releasing the current owner and disable sFlow sampling. The button is disabled if sFlow is currently unclaimed. If configured through SNMP, the release must be confirmed (a confirmation request will display).

IP Address/Hostname : The IP address or hostname of the sFlow receiver. Both IPv4 and IPv6 addresses are supported.

UDP Port : The UDP port on which the sFlow receiver listens to sFlow datagrams. If set to 0 (zero), the default port (6343) is used.

Timeout : The number of seconds remaining before sampling stops and the current sFlow owner is released. While active, the current time left can be updated with a click on the Refresh-button. If locally managed, the timeout can be changed on the fly without affecting any other settings.

Max. Datagram Size : The maximum number of data bytes that can be sent in a single sample datagram. This should be set to a value that avoids fragmentation of the sFlow datagrams. Valid range is 200 - 1468 bytes with default being 1400 bytes.

Port Configuration

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

Flow Sampler Enabled : Enables/disables flow sampling on this port.

Flow Sampler Sampling Rate : The statistical sampling rate for packet sampling. Set to N to sample on average 1/Nth of the packets transmitted/received on the port.

Not all sampling rates are achievable. If an unsupported sampling rate is requested, the switch will automatically adjust it to the closest achievable. This will be reported back in this field.

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 to 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.

2-31 UDLD

This page lets you view and set 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. It is 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 link.

To configure UDLD in the web UI:

1. Click Configuration, UDLD.
2. Specify UDLD mode and Message Interval.
3. Click Apply.

Figure 2-31: UDLD Port Config

Port	UDLD mode	Message Interval
*	<input type="text" value="↔"/>	<input type="text" value="7"/>
1	Disable	<input type="text" value="7"/>
2	Disable	<input type="text" value="7"/>
3	Disable	<input type="text" value="7"/>
4	Disable	<input type="text" value="7"/>
5	Disable	<input type="text" value="7"/>
6	Disable	<input type="text" value="7"/>
7	Disable	<input type="text" value="7"/>
8	Disable	<input type="text" value="7"/>

Port : Port number of the switch.

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

Disable : In disabled mode, UDLD functionality doesn't exist on the 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, disable UDLD on that port.

Message Interval : Configures the period of time between UDLD probe messages on ports that are in the advertisement phase and are determined to be bidirectional. The valid range is 7 - 90 seconds. The default value is 7 seconds. (The current 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.

2-32 Rapid Ring

This page lets you view and configure current Rapid Ring parameters. **Note:** STP must be disabled (at Configuration > Spanning Tree > CIST Port) to enable and configure Rapid Ring. See [Appendix A Rapid Ring](#) on page 466 for more information on Ring support.

To configure Rapid Ring in the web UI:

1. Click Configuration, Rapid Ring.
2. Specify the Roles, Ports, and Status.
3. Click Apply.

Figure 2-32: Rapid Ring Config

The screenshot shows the 'Rapid Ring Configuration' page in the Lantronix web UI. The page is titled 'Rapid Ring Configuration' and is part of the 'Configuration' menu. It features a sidebar with navigation options like 'Switch', 'DMS', 'Configuration', 'System', 'Green Ethernet', 'Ports Configuration', 'DHCP', 'Security', 'Aggregation', 'Link OAM', 'Loop Protection', 'Spanning Tree', 'IPMC Profile', and 'MVR'. The main content area is divided into 'Global Configuration' and 'Ring To Ring Configuration'. The 'Global Configuration' section has a table with columns for Role, 1st Ring Port, Status, 2nd Ring Port, and Status. The 'Ring To Ring Configuration' section has a table with columns for Role, Port, and Status. Both sections have 'Apply' and 'Reset' buttons at the bottom.

Parameter descriptions:

Global Configuration

Role : Select a role value.

Disabled: Rapid Ring configuration is disabled globally.

Master: Sets the role to ring master.

Member: Sets the role to ring member.

Rapid-Chain: Sets the role to failover.

Role

Disabled
Master
Member
Rapid-Chain

Port : Select the switch port number of the port. The ports should not be the same.

Status : Displays the current Rapid Ring status of the port (Forwarding, Discarding, ...).

Ring To Ring Configuration

Role : Select a role value.

Disabled: Rapid Ring configuration is disabled for ring-to-ring.

Active: Sets the role to active ring member.

Backup: Sets the role to backup ring member.

Role

Disabled
Active
Backup

Port : Select the switch port number of the port. The ports should not be the same in Global Configuration.

Status : Displays the current Rapid Ring status of the port (e.g., Forwarding, Discarding, etc.).

Buttons:

Apply : Click to save changes.

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

Example:

The screenshot shows the 'Rapid Ring Configuration' web page. On the left is a navigation menu with 'Switch' and 'DMS' tabs, and a 'Configuration' section with various options like System, Green Ethernet, Ports Configuration, DHCP, Security, Aggregation, Link OAM, Loop Protection, Spanning Tree, IPMC Profile, and MVR. The main content area is titled 'Rapid Ring Configuration' and has a breadcrumb 'Home > Configuration > Rapid Ring'. It is divided into two sections: 'Global Configuration' and 'Ring To Ring Configuration'. The 'Global Configuration' section has a table with columns: Role, 1st Ring Port, Status, 2nd Ring Port, and Status. The 'Ring To Ring Configuration' section has a table with columns: Role, Port, and Status. At the bottom of the configuration area are 'Apply' and 'Reset' buttons.

Role	1st Ring Port	Status	2nd Ring Port	Status
Master	Port 9	Forwarding	Port 8	Discarding
Member	Port 4	Discarding	Port 5	Discarding

Role	Port	Status
Active	Port 1	Discarding

Messages

Message: *Rapid Ring Configuration Error Error in port 2, STP is enable*

Meaning: You mis-configured Rapid Rings setup.

Recovery: **1.** Click the **Previous** button. **2.** Re-configure rapid ring with valid selections. **3.** Disable STP globally and per-port at Configuration > Spanning Tree > CIST Port. **4.** Continue operation.

Message: *The ports should not be same.*

Meaning: You configured at least one port for multiple Roles.

Recovery: **1.** Click the OK button to clear the webpage message. **2.** Change the port role settings. **3.** Click the **Apply** button. **4.** Continue operation.

2-33 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 or on-premise management platform that provides a single pane of glass for centralized management and automated monitoring of deployed devices, along with real-time notifications, managed APIs and data dashboards..

Lantronix Provisioning Manager (LPM) is a software application that provisions, configures and updates Lantronix devices for local site installations and deployments. LPM discovery is enabled by default and is not configurable. For more LPM information see the LPM [product page](#).

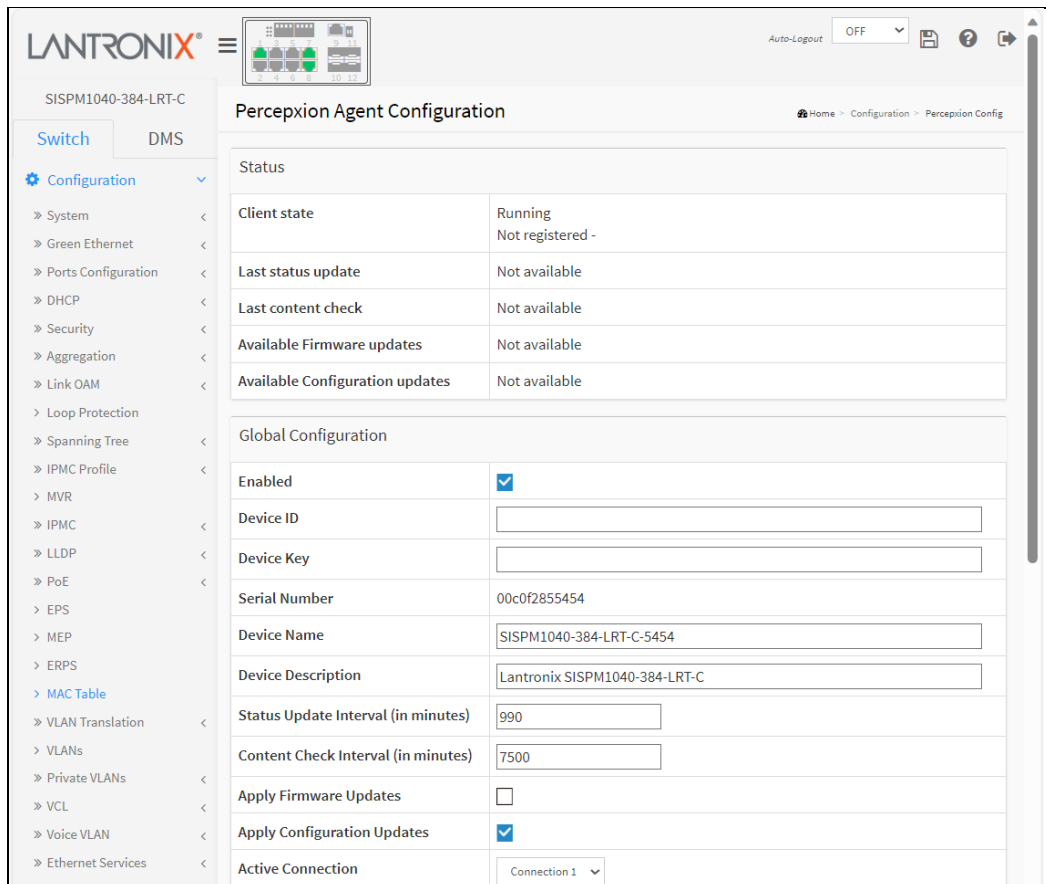
There are three pieces of information that the Percepixon client needs to complete registration and to publish data and configuration to the Percepixon server: **Device ID**, **Device Key**, and **Serial Number**. The Serial Number is always preprogrammed on the device (typically derived from the MAC 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.

Supported Firmware Versions

Devices must meet firmware requirements in order to work with Percepixon and LPM. SISPM1040-362-LRT and SISPM1040--384-LRT-C require firmware v 7.20.0190 or above.

Percepixon Agent Configuration

Go to Configuration > Percepixon > Percepixon Config to display the Percepixon Agent Configuration:



The screenshot displays the 'Percepixon Agent Configuration' page in the Lantronix web interface. The page is organized into two main sections: 'Status' and 'Global Configuration'.

Status Section:

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

Global Configuration Section:

Enabled	<input checked="" type="checkbox"/>
Device ID	<input type="text"/>
Device Key	<input type="text"/>
Serial Number	00c0f2855454
Device Name	SISPM1040-384-LRT-C-5454
Device Description	Lantronix SISPM1040-384-LRT-C
Status Update Interval (in minutes)	990
Content Check Interval (in minutes)	7500
Apply Firmware Updates	<input type="checkbox"/>
Apply Configuration Updates	<input checked="" type="checkbox"/>
Active Connection	Connection 1

Parameter descriptions:**Status:**

Client state: Displays the existing PercepXion client state (e.g., *Exited*, *Active*, *Inactive*, *Running*, or *Not Registered*).

Last status update: Displays the amount of time in minutes between status updates (1-1440 minutes or *<Not Available>*).

Last content check: Displays the amount of time in minutes between content checks; 1 minute to 90 days (in minutes) or *<Not Available>*.

Available Firmware updates: Displays a list of firmware that is available on the server. Select the firmware from this list and click Update now to upgrade or downgrade the firmware. Displays *<Not available>* if no Firmware updates are currently available.

Available Configuration updates: Displays a list of configuration that is available on the server. Select the configuration from this list and click Update now to upgrade or downgrade the firmware. Displays *<Not available>* if no configuration updates are currently available.

Global Configuration:

Enabled : Check the box to enable PercepXion globally. The default is disabled (unchecked).

Device ID: 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; up to 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 entered Device Key text.



: Click to Hide the entered Device Key text.

Serial Number : Displays the serial number of the switch in the format *11-22-33-44-55-66*. Read only.

Device Name : Enter a PercepXion Device Name for the switch of up to 32 alphanumeric characters (e.g., *SISPM1040-384-SAAS*). Device Name can have only alphanumeric (a-z, A-Z, 0-9) characters, hyphens (-), and underscores (_). Device Name must begin and end with an alphanumeric character.

Device Description : Enter a PercepXion Device Description for the switch of up to 32 alphanumeric characters (e.g., *Lantronix SISPM1040-362-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.

The screenshot shows a web interface for configuring PercepXion connections. On the left is a navigation menu with options like Mirroring, UPnP, PTP, GVRP, sFlow, UDLD, Rapid Ring, PercepXion (selected), PercepXion Config, PercepXion Upload, MRP, SMTP, Monitor, Diagnostics, and Maintenance. The main area displays two connection configuration panels, 'Connection 1' and 'Connection 2'. Each panel has a 'Connect To' dropdown set to 'Cloud', a 'Host' text field containing 'api.percepXion.ai', a 'Port' text field containing '443', and checkboxes for 'Secure Port' and 'Validate Certificates', both of which are checked. At the bottom of the panels are 'Apply' and 'Reset' buttons.

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 (Cloud or On Premise) for Connection 2. The default is Cloud. See the "Connect To" description in Connection 1 above.

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 Percepixon 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:

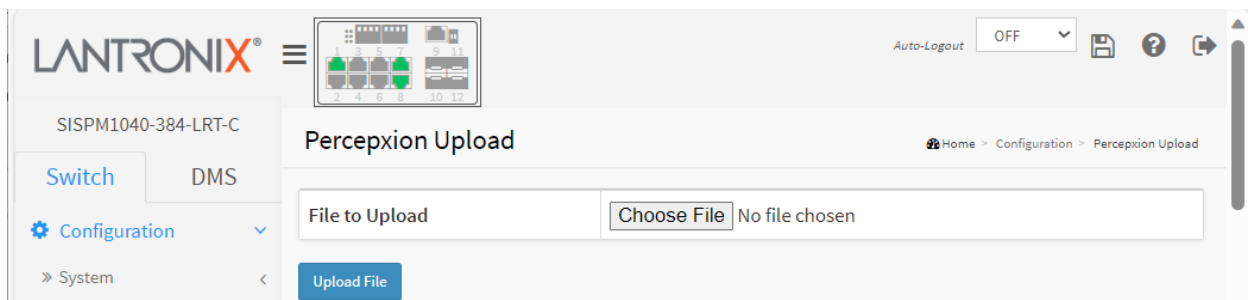
device id : 32 alphanumeric characters

5

Percepixon Upload

Navigate to Configuration > Percepixon > Percepixon Upload to display the Percepixon Upload page.

This page lets you upload a file from the web browser. Select the file to upload, then click the Upload File button.



Parameter descriptions:

Choose File: Click the button to navigate to and select the file to be uploaded.

Upload File: After a file is chosen, click the button to begin the file upload process.

Messages: No file chosen displays until you have select the file to be uploaded.

2-34 MRP

This page lets you set Media Redundancy Protocol parameters. MRP is a data network protocol standardized by the International Electrotechnical Commission as IEC 62439-2. It 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](#) for more standards information. See [Appendix C: MRP Prerequisites and Application Examples](#) on page 477.

Note: You must disable Spanning Tree at Configuration > Spanning Tree > CIST Port.

The screenshot shows the 'Media Redundancy Protocol Configuration' page in the Lantronix web interface. The page title is 'Media Redundancy Protocol Configuration' and the breadcrumb is 'Home > Configuration > MRP'. The interface includes a navigation menu on the left with 'Configuration' selected. The main content area displays a table with columns: Delete, Name, Primary, Secondary, Adm. Role, VLAN ID, Enable, and Edit Properties. Two rows are visible, both with 'Domai' as the name, 'Port 1' as the primary, 'Port 2' as the secondary, 'Undefined' as the role, '0' as the VLAN ID, and 'Disabled' as the enable status. Below the table are buttons for 'Add New Domain', 'Apply', and 'Reset'.

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

Name: A logical name for the MRP domain to 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 2 - 4094 (VLAN ID 1 is used for management).

Enable: Enable/Disable MRP protocol.

Edit: Click to edit domain properties. See "the Ring Domain Configuration" section 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.

Messages

Message: *VLAN ID is used for management*

Message: *VLAN ID is used in other ring domain*

Message: *The name is used with other 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: *Error in port 9, same with rapid ring port*

Ring Domain Configuration

Click the **Edit** button to display the Ring Domain Configuration page (Manager role shown below):

Domain settings	
Id	1
Admin Role	Manag
Name	Domain1
UUID	<input checked="" type="checkbox"/> Default FFFFFFFF-FFFF-FFFF-FFFFFFFF
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 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 is set to the role of a Media Redundancy Client (MRC). If the value is set to Manager, the entity shall be set to the role of a Media Redundancy Manager (MRM).

Name: The logical name for the MRP domain to ease the management of MRP domains.

UUID: Universally Unique Identifier belongs to the MRP domain which represents a ring.

Primary Port ID: The index of the layer 2 interface which is used as ring port 1.

Secondary Port ID: The index of the layer 2 interface which is used as ring port 2.

VLAN ID: The VLAN ID assigned to the MRP protocol. The allowed range is 0 - 4094.

Manager Priority: This parameter contains the value for the manager priority. The default is 8.

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 - 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 - 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 - 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 - 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 - 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 - 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. 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 - 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 - 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 - 10. Only MRC.

BLOCKED State Supported: This parameter specifies whether the MRC supports BLOCKED state at its ring ports. Only MRC.

Buttons

Apply: Click to save changes.

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

2-35 SMTP

The SMTP function is used to set an Alarm trap when the switch detects an alarm and then set the SMTP server to send you the alarm via e-mail. 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.
3. Click the Apply button to save the settings.
4. To cancel the setting click the **Reset** button to revert to previously saved values.

Figure 2-34: SMTP Configuration

The screenshot shows the Lantronix web interface for configuring SMTP. The page title is "SMTP Configuration". The breadcrumb trail is "Home > Configuration > SMTP". The main configuration area contains the following fields:

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"/>

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

Parameter descriptions:

Mail Server : Specify the IP Address of the server transferring your email. This is the IP address or hostname of the mail server. IP address is expressed in dotted decimal notation. This will be the device that sends out the mail for you

User Name : Specify the username of the mail server.

Password : Specify the password of the mail server.

Sender : To set the mail sender name.

Return Path : To set the mail return-path as sender mail address.

Email Address 1-6 : Email address(es) that you want to receive the alarm message.

Buttons

Apply: Click to save changes.

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

Chapter 3. Monitor

This chapter describes the monitoring functions such as System, Ports, DHCP, Security, etc.

3-1 System

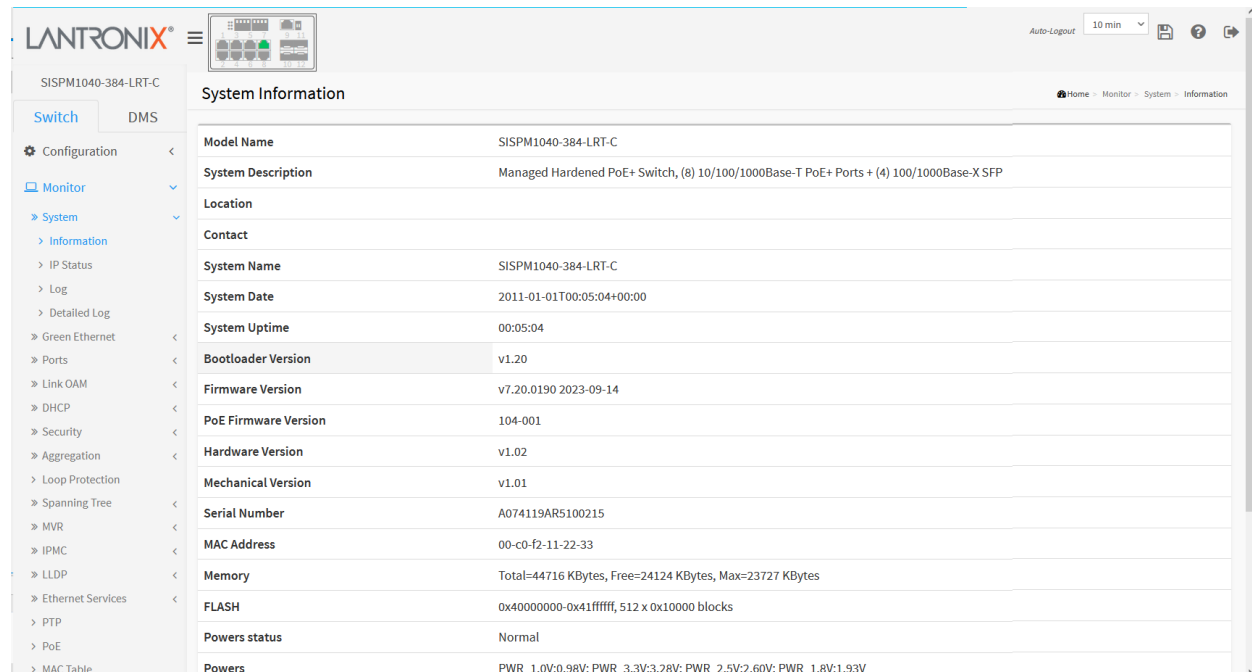
After login, the switch displays the System Information page by default. It displays basic device data, including Model Name, System Description, System Contact, System Location, Up Time, Firmware Version, and other helpful troubleshooting information.

3-1.1 Information

This page displays switch system information. To view System Information in the web UI:

1. Click Monitor, System, and Information.
2. View the displayed information such as Model Name, Firmware Version, Power status, etc.

Figure 3-1.1: System Information



System Information	
Model Name	SISPM1040-384-LRT-C
System Description	Managed Hardened PoE+ Switch, (8) 10/100/1000Base-T PoE+ Ports + (4) 100/1000Base-X SFP
Location	
Contact	
System Name	SISPM1040-384-LRT-C
System Date	2011-01-01T00:05:04+00:00
System Uptime	00:05:04
Bootloader Version	v1.20
Firmware Version	v7.20.0190 2023-09-14
PoE Firmware Version	104-001
Hardware Version	v1.02
Mechanical Version	v1.01
Serial Number	A074119AR5100215
MAC Address	00-c0-f2-11-22-33
Memory	Total=44716 KBytes, Free=24124 KBytes, Max=23727 KBytes
FLASH	0x40000000-0x41ffffff, 512 x 0x10000 blocks
Powers status	Normal
Powers	PWR_1.0V:0.98V; PWR_3.3V:3.28V; PWR_2.5V:2.60V; PWR_1.8V:1.93V

Parameter descriptions:

Model Name : Displays the factory-defined model name for identification purposes (either SISPM1040-384-LRT-C or SISPM1040-362-LRT).

System Description : Displays the system description (e.g., Managed Hardened PoE+ Switch, (8) 10/100/1000Base-T PoE+ Ports + (4) 100/1000Base-X SFP).

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 that configured in System > System Information > Configuration > System Name (e.g., SISPM1040-384-LRT-C or SISPM1040-362-LRT).

System Date : The current (GMT) system date and time in the format 2023-08-30T10:30:40+00:00. The system time is obtained through the Time server running on the switch, if any is configured.

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 : The software version of this switch (e.g., v7.20.0190 2023-09-14).

PoE Firmware Version: the running version of PoE firmware in the switch (e.g., 104-001).

Hardware Version : The hardware version of this switch (e.g., v1.02).

Mechanical Version : The mechanical version of this switch (e.g., v1.01).

Serial Number : The serial number of this switch (e.g., A084117AR0100003).

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

Memory : Displays the memory size of the system (e.g., Total=53788 KBytes, Free=36343 KBytes, Max=35318 Kbytes).

FLASH : Displays the flash size of the system (e.g., 0x40000000-0x41ffffff, 512 x 0x10000 blocks).

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

Powers: Displays the system power levels (e.g., PWR_1.0V:0.99V; PWR_3.3V:3.28V; 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 sensor # 1 (e.g., 39(C) ; 102(F)).

Temperature 2: Displays the temperature sensor # 2 (e.g., 43(C) ; 109(F)).

CPU Load (100ms, 1s, 10s): Displays the CPU loading of the system (e.g., 5%, 4%, 2%).

3-1.2 IP Status

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

To display IP interface information in the web UI:

1. Click Monitor, System and IP Status.
2. View the IP interfaces information.

Figure 3-1.2: IP Interfaces page

The screenshot shows the 'IP Interfaces' page in the web UI. The page is titled 'IP Interfaces' and has a navigation menu on the left. The main content area is divided into several sections:

- IP Interfaces Table:** A table with columns 'Interface', 'Type', 'Address', and 'Status'. It lists various VLANs and their configurations.
- IP Routes Table:** A table with columns 'Network', 'Gateway', and 'Status'. It lists various IP networks and their gateways.
- Neighbour cache Table:** A table with columns 'IP Address' and 'Link Address'. It lists various IP addresses and their corresponding link addresses.
- DNS Server Table:** A table with columns 'Type', 'IP Address', and 'Interface'. It lists various DNS servers and their interfaces.

Interface	Type	Address	Status
VLAN1	LINK	00-c0-f2-49-3d-4f	<UP BROADCAST RUNNING MULTICAST>
VLAN1	IPv4	192.168.1.77/24	
VLAN1	IPv6	fe80::2c0:f2ff:fe49:3d4f/64	
VLAN2	LINK	00-c0-f2-49-3d-4f	<UP BROADCAST RUNNING MULTICAST>
VLAN2	IPv4	192.168.2.77/24	
VLAN2	IPv6	fe80::2c0:f2ff:fe49:3d4f/64	
VLAN4	LINK	00-c0-f2-49-3d-4f	<UP BROADCAST RUNNING MULTICAST>
VLAN4	IPv4	169.254.170.66/16	
VLAN4	IPv4	192.168.3.3/24	
VLAN4	IPv6	fe80::2c0:f2ff:fe49:3d4f/64	
VLAN4096	LINK	00-c0-f2-49-3d-4f	<BROADCAST MULTICAST>
VLAN4097	LINK	00-c0-f2-49-3d-4f	<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	VLAN4	<UP HW_RT>
192.168.1.0/24	VLAN1	<UP HW_RT>
192.168.2.0/24	VLAN2	<UP HW_RT>
192.168.3.0/24	VLAN4	<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-f2-49-3d-4f
192.168.1.99	VLAN1:00-1b-11-b2-6d-4b
192.168.3.3	VLAN4:00-c0-f2-49-3d-4f
fe80::2c0:f2ff:fe49:3d4f	VLAN1:00-c0-f2-49-3d-4f
fe80::2c0:f2ff:fe49:3d4f	VLAN2:00-c0-f2-49-3d-4f
fe80::2c0:f2ff:fe49:3d4f	VLAN4:00-c0-f2-49-3d-4f

Type	IP Address	Interface
Static	8.8.8.8	

Parameter descriptions:

IP Interfaces

Interface : Shows the name of the interface (e.g., VLAN1 - VLAN4097).

Type : Shows the address type of the entry. This may be LINK, IPv4 or IPv6.

Address : Shows the current address of the interface (of the given type). For example, LINK = 00-c0-f2-49-3d-4f, or IPv4 = 192.168.1.77/24, or IPv6 = fe80::2c0:f2ff:fe49:3d4f/64).

Status : Shows the status flags of the interface and/or address (e.g., <BROADCAST MULTICAST> or <UP BROADCAST RUNNING MULTICAST>).

IP Routes

Network : Shows the destination IP address or host name of this route (e.g., 0.0.0.0/0 or 92.168.1.0/24).

Gateway : Shows the gateway address of this route (e.g., 192.168.1.254 or VLAN4 or ::1).

Status : Shows the status flags of the route (e.g., <UP> or <UP GATEWAY HW_RT> or <UP HW_RT> or <UP HOST> or <HOST>).

Neighbor cache

IP Address : Displays the IP address of the entry (e.g., 192.168.3.3 or fe80::2c0:f2ff:fe49:3d4f).

Link Address : Displays the Link (MAC) address for which a binding to the IP address given exists (e.g., VLAN1:00-c0-f2-49-3d-4f or VLAN4:00-c0-f2-49-3d-4f).


DNS Server

Type: The configuration type of DNS server (e.g., Static).

IP Address : The IP address of the DNS server (e.g., 8.8.8.8).

Interface : The name of the interface if any is configured.

Buttons

Auto-refresh 

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

Refresh: Click to manually refresh the page immediately.

3-1.3 Log

This page displays the system log information of the switch.

1. Click Monitor, System, and Log.
2. View the log information.

Figure 3-1.3: System Log Information

The screenshot displays the 'System Log Information' page in the Lantronix web interface. The page title is 'System Log Information' and the breadcrumb trail is 'Home > Monitor > System > Log'. The interface includes a navigation menu on the left with options like Configuration, Monitor, System, and Log. The main content area shows the log configuration and a table of log entries.

Auto-refresh [Refresh] [Previous] [Next]

Level: All [Dropdown]

Clear Level: All [Dropdown]

Do Relay Status: On Off

Do Relay Alarm Cut-off:

The total number of entries is 16 for the given level.

Start from ID , entries per page.

ID	Level	Time	Message
1	Info	2023-08-29T14:54:28+00:00	SYS-FIRMWARE: New firmware active: SISPM1040-384-LRT-C (standalone) v7.20.0186
2	Warning	2023-08-29T14:54:37+00:00	DI 1 change to abnormal
3	Warning	2023-08-29T14:54:38+00:00	Link up on port 1
4	Info	2023-08-29T14:54:38+00:00	Password of user 'admin' was changed
5	Warning	2023-08-29T14:54:38+00:00	Switch just made a cold boot
6	Warning	2023-08-29T14:54:38+00:00	Link up on port 7
7	Warning	2023-08-29T14:54:38+00:00	Link up on port 8

Parameter descriptions:

Level : level of the system log entry. These system log levels of information are supported:

All: All levels.

Emerg: The system log entry is at the emergency level.

Alert: The system log entry is at the alert level.

Crit: The system log entry is at the critical level.

Error: The system log entry is at the error level.

Warning: The system log entry is at the warning level.

Notice: The system log entry is at the notice level.

Info: The system log entry is at the information level.

Debug: The system log entry is at the debug level.

Clear Level : The level at which to clear log messages (same as above).

Do Relay Status : Displays On (●) or Off (●) as the status of the digital-out relay contact.

Do Relay Alarm Cut-off: Click the Apply button to force cut off the digital-out relay contact.

ID : The ID number of the system log entry.

Level: The level of the system log entry; see above.

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.

<<: 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 entry to the last available entry ID.

System Log Sample

ID	Level	Time	Message
1	Info	2023-08-29T14:54:28+00:00	SYS-FIRMWARE: New firmware active: SISPM1040-384-LRT-C (standalone) v7.20.0186
2	Warning	2023-08-29T14:54:37+00:00	DI 1 change to abnormal
3	Warning	2023-08-29T14:54:38+00:00	Link up on port 1
4	Info	2023-08-29T14:54:38+00:00	Password of user 'admin' was changed
5	Warning	2023-08-29T14:54:38+00:00	Switch just made a cold boot
6	Warning	2023-08-29T14:54:38+00:00	Link up on port 7
7	Warning	2023-08-29T14:54:38+00:00	Link up on port 8
8	Info	2023-08-29T14:54:39+00:00	topologyChange
9	Info	2023-08-29T14:54:40+00:00	topologyChange
10	Info	2023-08-29T14:54:42+00:00	topologyChange
11	Warning	2023-08-29T14:54:53+00:00	DC Power 2 unavailable
12	Info	2023-08-29T14:55:29+00:00	Login passed for user 'admin'
13	Info	2023-08-30T09:34:21+00:00	Login passed for user 'admin'
14	Info	2023-08-30T09:34:23+00:00	LINK-UPDOWN: Interface Vlan 1, changed state to down.
15	Info	2023-08-30T09:34:23+00:00	LINK-UPDOWN: Interface Vlan 1, changed state to up.
16	Info	2023-08-30T09:44:52+00:00	User 'admin' logout

3-1.4 Detailed Log

This page displays detailed log information for the switch.

1. Click Monitor, System, and Detailed Log.
2. View the log information.

Figure 3-1.4: Detailed System Log Information

The screenshot shows the Lantronix web interface for device SISPM1040-384-LRT-C. The 'Monitor' > 'System' > 'Detailed Log' path is active. The log entry table is as follows:

Level	Info
Time	2011-01-01T00:00:01+00:00
Message	SYS-FIRMWARE: New firmware active: SISPM1040-384-LRT-C (standalone) v7.20.0121

Parameter descriptions:

Level: The level of the system log entry; see above.

Time : The date and time of the system log entry.

Message : The detailed message of the system log entry.

Buttons



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

<<: 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 entry to the last available entry ID.

3-2 Green Ethernet

3-2.1 Port Power Savings

This page displays the current status for EEE (Energy Efficient Ethernet).

1. Click Monitor, Green Ethernet, Port Power Savings.
2. View the displayed information.

Figure 3-2.1: Port Power Savings Status

Port	Link	EEE Cap	EEE Ena	LP EEE Cap	EEE Savings	ActiPhy Savings	PerfectReach Savings
1	●	✓	✗	✓	✗	✗	✗
2	●	✓	✗	✗	✗	✗	✗
3	●	✓	✗	✗	✗	✗	✗
4	●	✓	✗	✗	✗	✗	✗
5	●	✓	✗	✗	✗	✗	✗
6	●	✓	✗	✗	✗	✗	✗
7	●	✓	✗	✗	✗	✗	✗
8	●	✓	✗	✗	✗	✗	✗

Parameter descriptions:

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 EEE is enabled for the port (reflects the settings at the Port Power Savings configuration page).

EEE Ena : Shows if EEE is enabled for the port (reflects the settings at the Port Power Savings config 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 uSec.

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: Click to manually refresh the page immediately.

3-3 Ports

This section lets you view switch Port detail parameters.

3-3.1 Traffic Overview

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

1. Click Monitor, Ports, Traffic Overview.
2. Check the Auto-refresh checkbox to automatically refresh the page every 3 seconds.
3. Click Refresh to update the port statistics or click the Clear button to clear all information.
4. You can click a linked Port number to display its Detailed Port Statistics page (see below).

Figure 3-3.1: Port Statistics Overview

The screenshot shows the 'Port Statistics Overview' page in the Lantronix web interface. The page title is 'Port Statistics Overview' and the breadcrumb is 'Home > Monitor > Ports > Traffic Overview'. There is an 'Auto-refresh' checkbox which is currently unchecked, and a 'Click Save Button' link. The main content is a table with the following data:

Port	Packets		Bytes		Errors		Drops		Filtered
	Received	Transmitted	Received	Transmitted	Received	Transmitted	Received	Transmitted	Received
1	174358	5859947	41387218	490738661	0	0	0	0	726
2	0	65899	0	8320742	0	0	0	0	0
3	0	0	0	0	0	0	0	0	0
4	0	0	0	0	0	0	0	0	0
5	0	0	0	0	0	0	0	0	0
6	0	0	0	0	0	0	0	0	0
7	0	0	0	0	0	0	0	0	0
8	0	0	0	0	0	0	0	0	0
9	0	0	0	0	0	0	0	0	0
10	0	0	0	0	0	0	0	0	0
11	0	0	0	0	0	0	0	0	0
12	0	0	0	0	0	0	0	0	0

Parameter descriptions:

Port : The logical port for the settings contained in the same row. You can click a linked Port number to display its Detailed Port Statistics page (see below).

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

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

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

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

Filtered : The number of received frames filtered by the forwarding

Buttons

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



Refresh: Click to manually refresh the page immediately.

Clear: Clears the counters for all ports.

Detailed Port Statistics page

On the Port Statistics Overview page, you can click a linked Port number to display its Detailed Port Statistics page:

SISPM1040-384-LRT-C

Switch DMS

Configuration Monitor Ports Traffic Overview QoS Statistics QCL Status Detailed Statistics SFP Information SFP Detail Info Link OAM DHCP Security Aggregation Loop Protection Spanning Tree MVR IPAC LLDP Ethernet Services PTP PoE MAC Table VLANs MRP VCL sFlow UDLD Diagnostics Maintenance

Detailed Port Statistics Port 9

Auto-refresh Port 9

Receive Total		Transmit Total	
Rx Packets	1916547	Tx Packets	1615188
Rx Octets	202787322	Tx Octets	219559778
Rx Unicast	559742	Tx Unicast	420708
Rx Multicast	102492	Tx Multicast	103869
Rx Broadcast	1254313	Tx Broadcast	1090611
Rx Pause	0	Tx Pause	0
Receive Size Counters		Transmit Size Counters	
Rx 64 Bytes	1495450	Tx 64 Bytes	1232604
Rx 65-127 Bytes	147147	Tx 65-127 Bytes	81414
Rx 128-255 Bytes	148181	Tx 128-255 Bytes	142974
Rx 256-511 Bytes	51561	Tx 256-511 Bytes	94125
Rx 512-1023 Bytes	74195	Tx 512-1023 Bytes	49835
Rx 1024-1526 Bytes	13	Tx 1024-1526 Bytes	14236
Rx 1527- Bytes	0	Tx 1527- Bytes	0
Receive Queue Counters		Transmit Queue Counters	
Rx Q0	1916547	Tx Q0	0
Rx Q1	0	Tx Q1	0
Rx Q2	0	Tx Q2	0
Rx Q3	0	Tx Q3	0
Rx Q4	0	Tx Q4	0
Rx Q5	0	Tx Q5	0
Rx Q6	0	Tx Q6	0
Rx Q7	0	Tx Q7	1615188
Receive Error Counters		Transmit Error Counters	
Rx Drops	160	Tx Drops	0
Rx CRC/Alignment	0	Tx Late/Exc. Coll.	0
Rx Undersize	0		
Rx Oversize	0		
Rx Fragments	0		

3-3.2 QoS Statistics

This page displays the QoS detailed Queuing counters for all switch ports.

1. Click Monitor, Ports, then QoS Statistics.
2. To automatically refresh the page every 3 seconds, check the "Auto-refresh" checkbox.
3. Click "Refresh" to refresh the Queuing Counters or clear all information when you click "Clear".

Figure 3-3.2: Queuing Counters

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	174659	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	5862625
2	0	7243	0	0	0	0	0	0	0	0	0	0	0	0	0	0	61420
3	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
4	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
5	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
6	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
7	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
8	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
9	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
10	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
11	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
12	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0

Parameter descriptions:

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

Qn : The Queue number; there are 8 QoS queues per port (Q0-Q7), and Q0 is the lowest priority queue.

Rx/Tx : The number of received and transmitted packets per queue.

Buttons



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

Refresh: Click to manually refresh the page immediately.

Clear: Clears the counters for all ports.

3-3.3 QCL Status

This page displays QCL status by different QCL users. Each row describes the QCE that is defined. 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 on each switch.

To display the QoS Control List Status in the web UI:

1. Click Monitor, Ports, QCL Status.
2. To auto-refresh the information check the "Auto-refresh" checkbox.
3. At the dropdown select the User (Combined, Static, Voice VLAN, DMS, or Conflict).

Figure 3-3.3: QoS Control List Status

User	QCE	Port	Frame Type	Action							Conflict
				CoS	DPL	DSCP	PCP	DEI	Policy	Conflict	
Static	1	Any	Any	0	Default	Default	Default	Default	Default	Default	No
Static	2	Any	EtherType	1	Default	Default	Default	Default	Default	Default	No
Static	3	Any	LLC	3	Default	8 (CS1)	Default	Default	1	Default	No
Static	4	Any	IPv4	4	1	0 (BE)	Default	Default	1	Default	No

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 frame types are:

Any: The QCE will match all frame type.

Ethernet: Only Ethernet frames (with Ether Type 0x600-0xFFFF) are allowed.

LLC: Only (LLC) frames are allowed

SNAP: Only (SNAP) frames are allowed.

IPv4: The QCE will match only IPV4 frames.

IPv6: The QCE will match only IPV6 frames.

Action : Indicates the classification action taken on ingress frame if parameters configured are matched with the frame's content. Possible actions are:

CoS: Classify Class of Service.

DPL: Classify Drop Precedence Level.

DSCP: Classify DSCP value.

PCP: Classify PCP value.

DEI: Classify DEI value.

Policy: Classify ACL Policy number.

Conflict : Displays Conflict status of QCL entries. It may happen that resources required to add a QCE may not available, in that case it shows conflict status as 'Yes', otherwise it is always 'No'. Note that conflict can be resolved by releasing the H/W resources required to add QCL entry on pressing 'Resolve Conflict' button.

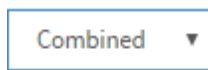
Buttons



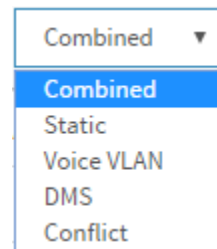
Auto-refresh: Check this box to refresh the page automatically every 3 seconds.

Refresh: Click to manually refresh the page immediately.

Resolve Conflict: Click to release the resources required to add a QCL entry, in case the Conflict status for any QCL entry is 'yes'.



: Select the QCL status from this drop down list.



3-3.4 Detailed Port 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 Port Statistics in the web UI:

1. Click Monitor, Ports, then Detailed Port Statistics.
2. At the Port Select dropdown, select the port you want to show the Detailed Port Statistics.
3. To auto-refresh the page check the “Auto-refresh” box.
4. Click “Refresh” to refresh the statistics or clear all information when you click “Clear”.

Figure 3-3.4: Detailed Port Statistics

Detailed Port Statistics Port 1			
Auto-refresh <input type="checkbox"/>		Port 1	
Receive Total		Transmit Total	
Rx Packets	260	Tx Packets	5224
Rx Octets	120394	Tx Octets	392201
Rx Unicast	84	Tx Unicast	12
Rx Multicast	103	Tx Multicast	248
Rx Broadcast	73	Tx Broadcast	4964
Rx Pause	0	Tx Pause	0
Receive Size Counters		Transmit Size Counters	
Rx 64 Bytes	92	Tx 64 Bytes	4699
Rx 65-127 Bytes	11	Tx 65-127 Bytes	411
Rx 128-255 Bytes	0	Tx 128-255 Bytes	48
Rx 256-511 Bytes	100	Tx 256-511 Bytes	29
Rx 512-1023 Bytes	17	Tx 512-1023 Bytes	32
Rx 1024-1526 Bytes	40	Tx 1024-1526 Bytes	5
Rx 1527- Bytes	0	Tx 1527- Bytes	0
Receive Queue Counters		Transmit Queue Counters	
Rx Q0	260	Tx Q0	269
Rx Q1	0	Tx Q1	0
Rx Q2	0	Tx Q2	0
Rx Q3	0	Tx Q3	0

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.

Auto-refresh: Check the Auto-refresh box to refresh the Queuing Counters automatically.



Auto-refresh   Port 1 

Buttons

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

Refresh: Click to manually refresh the page immediately.

Clear : Clears the counters for the selected port.

Port Select dropdown : select the port you want to show the Detailed Port Statistics.

3-3.5 SFP Information

This page displays general SFP monitoring information.

1. Click Monitor, Ports, then SFP Information.
2. View the displayed SFP Information.

Figure 3-3.5: SFP Information Overview

Port	Tx Central Wavelength	Bit Rate	Temperature	Vcc	Mon1 (Bias)	Mon2 (TxPwr)	Mon3 (RxPwr)
1							
2							
3							
4							
5							
6							
7	850	1000 Mbps	49.63 C	3.34 V	15 mA	-6.15 dBm	none
8	850	10 Gbps	43.91 C	3.33 V	6 mA	-2.25 dBm	-7.15 dBm

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.

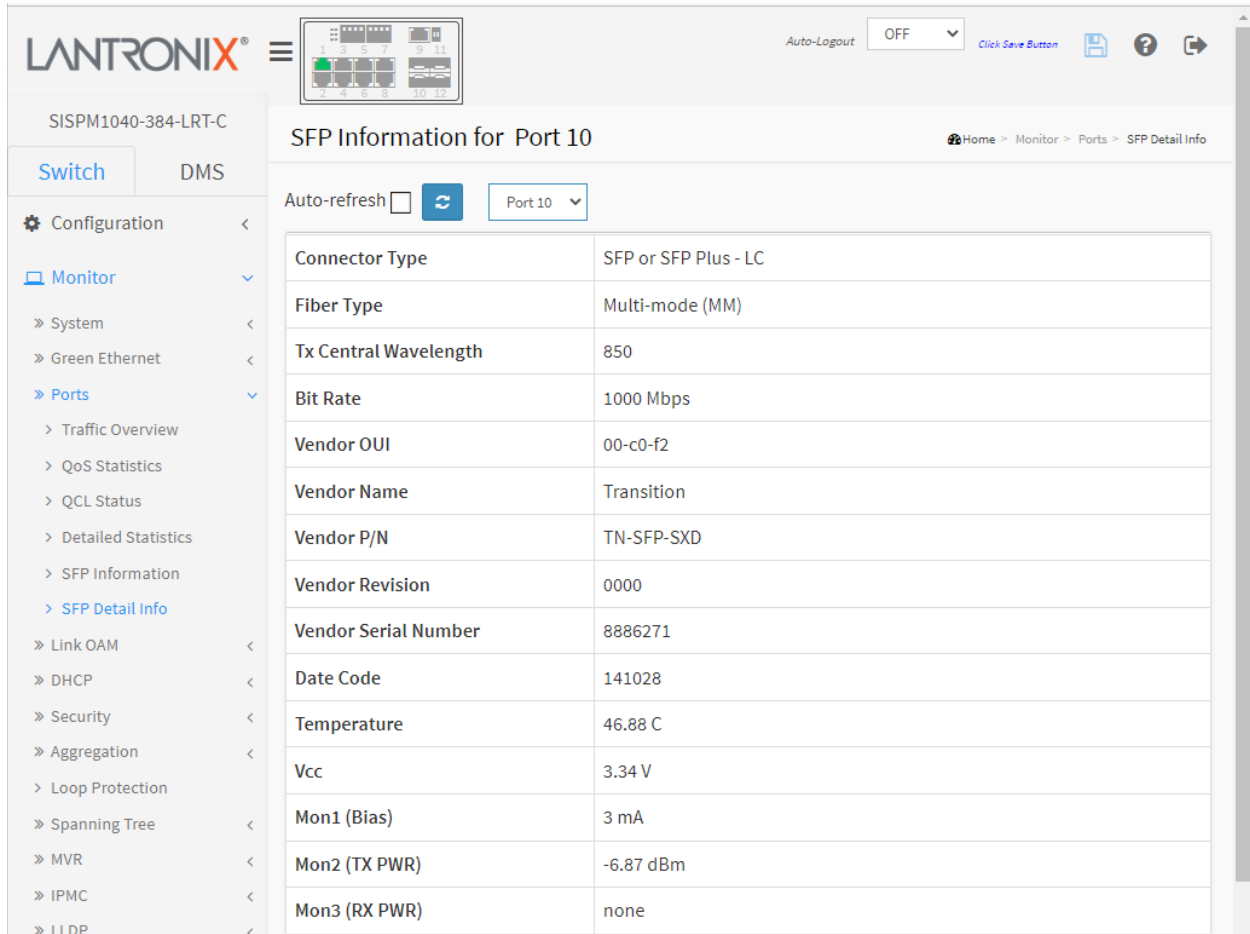
Refresh: Click to manually refresh the page immediately.

3-3.6 SFP Detail Info

This page displays detailed SFP information and monitoring information.

1. Click Monitor, Port, and SFP Detail Info.
2. Select the desired SFP port at the dropdown.
3. View the displayed SFP Information.

Figure 3-3.6: SFP Detail Info



The screenshot shows the Lantronix web interface for SFP Information for Port 10. The interface includes a navigation menu on the left, a top header with the Lantronix logo and system name (SISPM1040-384-LRT-C), and a main content area displaying SFP details for Port 10. The details are presented in a table format.

Parameter	Value
Connector Type	SFP or SFP Plus - LC
Fiber Type	Multi-mode (MM)
Tx Central Wavelength	850
Bit Rate	1000 Mbps
Vendor OUI	00-c0-f2
Vendor Name	Transition
Vendor P/N	TN-SFP-SXD
Vendor Revision	0000
Vendor Serial Number	8886271
Date Code	141028
Temperature	46.88 C
Vcc	3.34 V
Mon1 (Bias)	3 mA
Mon2 (TX PWR)	-6.87 dBm
Mon3 (RX PWR)	none

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 (e.g., Multi-mode (MM), Reserved, etc.).

Tx Central Wavelength : Displays the nominal transmitter output wavelength in nm.

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

Vendor OUI : Displays the vendor IEEE company ID.

Vendor Name : Displays the vendor name (e.g., Transition).

Vendor P/N : Displays the vendor part number or product name (e.g., TN-10GSFP-SR or TN-SFP-SXD).

Vendor Revision : Displays the vendor's 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 depends on 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 manually refresh the page immediately.

Port Select dropdown : select the port you want to show the SFP Detail Information.

3-4 Link OAM

3-4.1 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 view Link OAM Statistics in the web UI:

1. Click Monitor, Link OAM and Statistics.
2. Select the desired port to be displayed.
3. View the displayed Statistics.

Figure 3-4.1: Detailed Link OAM Statistics

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

Parameter descriptions:

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

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

Sequence Number field that is identical to the previously transmitted Event Notification OAMPDU Sequence Number.

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

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

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

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

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

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

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

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

Buttons

Port Select dropdown : select the port you want to show the Detailed Link OAM Statistics.

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

Refresh: Click to manually refresh the page immediately.

Clear: Clears the counters for the selected port.

3-4.2 Port Status

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

1. Click Monitor, Link OAM and Port Status.
2. Select the desired port.
3. View the Port Status parameters.

Figure 3-4.2: Detailed Link OAM Port Status

Local		Peer	
PDU Permission	Receive only		
Discovery State	Fault state		
Peer MAC Address	-----		
Mode	Passive	Mode	-----
Unidirectional Operation Support	Disabled	Unidirectional Operation Support	-----
Remote Loopback Support	Disabled	Remote Loopback Support	-----
Link Monitoring Support	Enabled	Link Monitoring Support	-----
MIB Retrieval Support	Disabled	MIB Retrieval Support	-----
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	-----

Parameter descriptions:

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

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 is enabled DTE supports sending Variable Response OAMPDUs.

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

Multiplexer State : When in forwarding state, the Device is forwarding non-OAMPDUs to the lower sublayer. In case of discarding, the device discards all the non-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 : 24-bit Organizationally Unique Identifier of the vendor.

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

Buttons

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

Refresh: Click to manually refresh the page immediately.

Port Select dropdown : select the port you want to show the Detailed Link OAM Port Status.

3-4.3 Event Status

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

To view the Link OAM Status in the web UI:

1. Click Monitor, Link OAM and Event Status.
2. View the Event Status parameters.

Figure 3-4.1: Detailed Link OAM Link Status

The screenshot shows the Lantronix web interface for the SISPM1040-362-LRT device. The main content area is titled 'Detailed Link OAM Link Status for Port 1'. It features a dropdown menu for 'Port 1', an 'Auto-refresh' checkbox, and a 'Refresh' button. Below this is a table with four columns: 'Local Frame Error Status', 'Remote Frame Error Status', 'Local Frame Period Status', and 'Remote Frame Period Status'. The table lists various parameters and their values, all of which are currently 0.

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

Parameter descriptions: Local Frame Error Status and Remote Frame Error Status:

Port : At the dropdown select the desired 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 32-bit unsigned integer.

Buttons

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

Refresh: Click to manually refresh the page immediately.

Port Select dropdown : select the port you want to show the Detailed Link OAM Link Status.

3-5 DHCP

3-5.1 Server

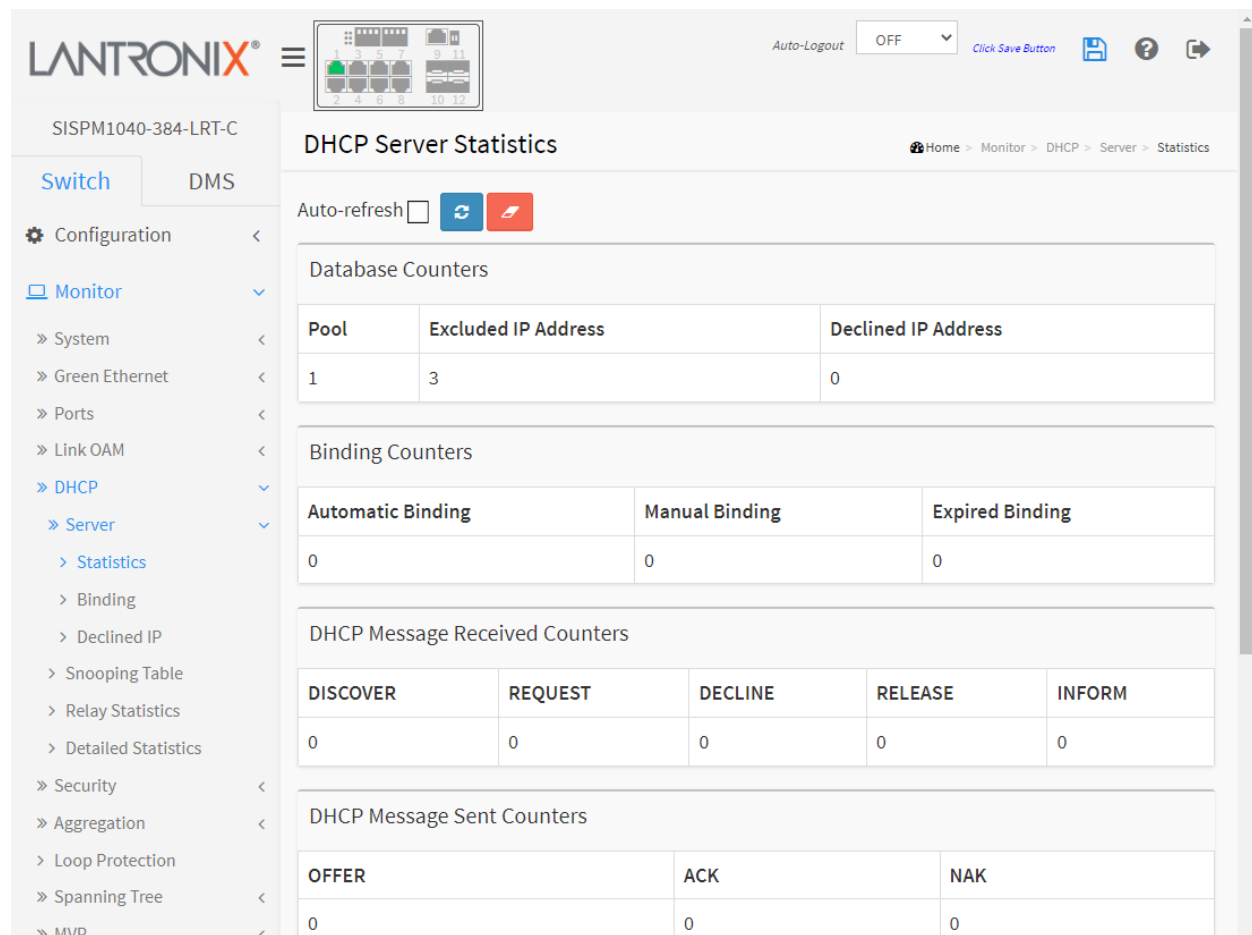
A DHCP Server is used to allocate network addresses and deliver configuration parameters to dynamically configured hosts called DHCP clients.

3-5.1.1 Statistics

This page displays the database counters and the number of DHCP messages sent and received by the DHCP server(s).

1. Click Monitor > DHCP > Server > Statistics.
2. View the displayed DHCP Server Statistics.

Figure 3-5.1.1: DHCP Server Statistics



Parameter descriptions:

Database Counters : Displays counters of various databases.

Pool : Number of pools.

Excluded IP Address : Number of excluded IP address ranges.

Declined IP Address : Number of declined IP addresses.

Binding Counters Displays counters of various databases.

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 : Displays counters of DHCP messages received by DHCP server.

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 : Displays counters of DHCP messages sent by DHCP server.

OFFER : Number of DHCP OFFER messages sent.

ACK : Number of DHCP ACK messages sent.

NAK : Number of DHCP NAK messages sent.

Buttons

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

Refresh: Click to manually refresh the page immediately.

Clear: Clears the counters for the selected port.

3-5.1.2 Binding

This page displays bindings generated for DHCP clients. A binding is a collection of configuration parameters, including at least an IP address, associated with or "bound to" a DHCP client. Bindings are managed by DHCP servers.

1. Click Monitor, DHCP, Server, and Binding.
2. View the displayed DHCP Server Binding IP table.

Figure 3-5.1.2: DHCP Server Binding IP

Delete	IP	Type	State	Pool Name	Server ID
<input type="checkbox"/>	192.168.1.4	Automatic	Committed	DHCP_Per_Port	192.168.1.77

Parameter descriptions:

IP : Displays the IP address allocated to DHCP client. Click the linked IP address text to display the DHCP Server Binding IP Data page (see below).

Type : Displays the type of binding. Possible types are Automatic, Manual, and Expired.

State : Displays the State of binding. Possible states are Committed, Allocated, and Expired.

Pool Name : Displays the pool that generates the binding.

Server ID : Displays the Server IP address to service the binding.

Buttons

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

Refresh: Click to manually 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.

DHCP Server Binding IP Data

Click the linked IP address text to display the DHCP Server Binding IP Data page. This page displays the detailed data of a binding.

The screenshot shows the DHCP Server Binding IP Data page. The left sidebar contains a navigation menu with 'Switch' selected and 'DMS' as a sub-tab. The main content area is titled 'DHCP Server Binding IP Data' and includes an 'Auto-refresh' checkbox, a 'Binding' section with an IP dropdown set to '192.168.1.4', and a 'Binding IP Data' table with various parameters.

Binding IP Data	
IP	192.168.1.4
Type	Automatic
State	Committed
Pool Name	DHCP_Per_Port
Server ID	192.168.1.77
VLAN	1
Subnet Mask	255.255.255.0
Client ID Type	MAC
Client ID Value	00-09-18-4e-20-e9
MAC Address	00-09-18-4e-20-e9
Lease Time	1 days 0 hours 0 minutes 0 seconds
Will Expired in	14 hours 3 minutes 38 seconds

Parameter descriptions:

Binding

IP : The IP address of the selected binding.

Binding IP Data : Displays data of the selected binding.

IP : The IP address allocated to a 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.

VLAN ID : VLAN ID of the interface where the DHCP client is from.

Subnet Mask : Netmask of the interface where the DHCP client is from.

Client ID Type : Type of client identifier in option 61 from DHCP client. Possible types are FQDN, MAC and -. If - is displayed, then it means DHCP client does not pack option 61 in the DHCP message.

Client ID Value : Value of client identifier in option 61 from DHCP client.

MAC Address : Hardware address in chaddr of DHCP message from DHCP client.

Lease Time : The lease time of the binding.

Will Expired in : How much remaining time until the binding will expire.

Buttons

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

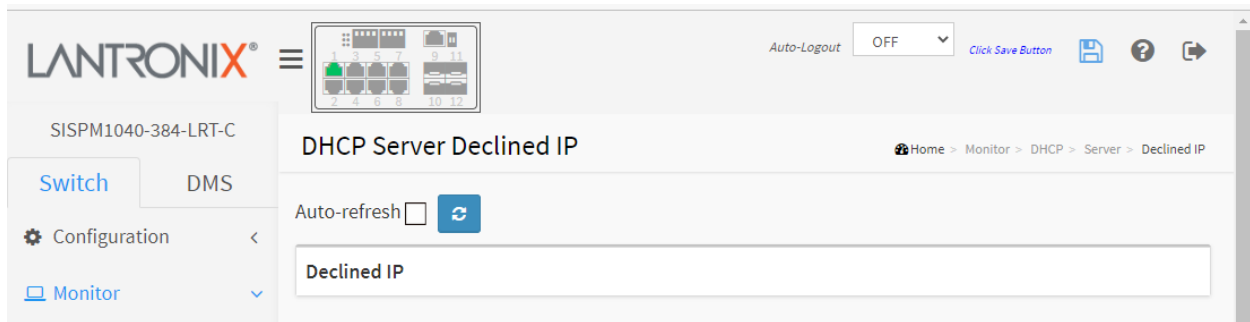
Refresh: Click to manually refresh the page immediately.

3-5.1.3 Declined IP

This page displays IP addresses declined by DHCP clients.

1. Click Monitor, DHCP, Server and Declined IP.
2. View the displayed table information.

Figure 3-5.1.3: DHCP Server Declined IP



Parameter descriptions:

Declined IP : List of IP addresses declined by DHCP clients.

Buttons

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

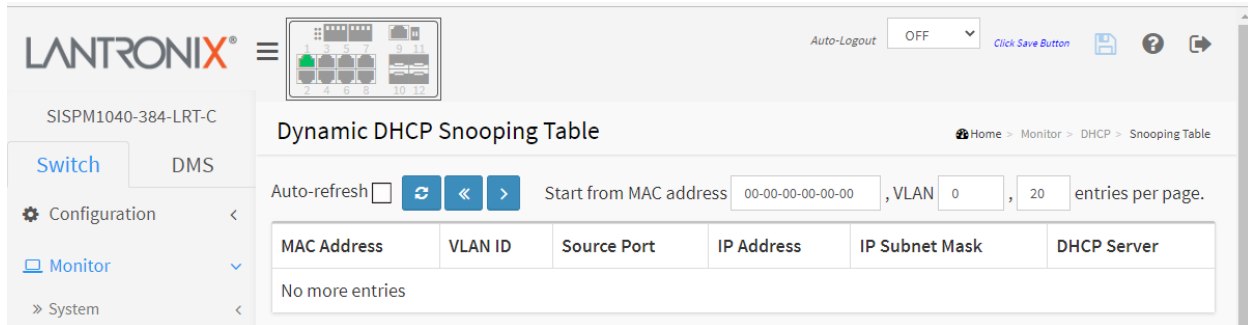
Refresh: Click to manually refresh the page immediately.

3-5.2 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.

1. Click Monitor, DHCP, and Snooping Table.
2. Check "Auto-refresh".
3. Click "Refresh" to refresh the statistics or clear all information when you click "Clear".

Figure 3-5.2: Dynamic DHCP Snooping Table



Parameter descriptions:

MAC Address : User MAC address of the entry.

VLAN ID : The 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: Refreshes the displayed table starting from the input fields.

Clear : Flushes all dynamic entries.

<< : Updates the table starting from the first entry in the Dynamic DHCP snooping Table.

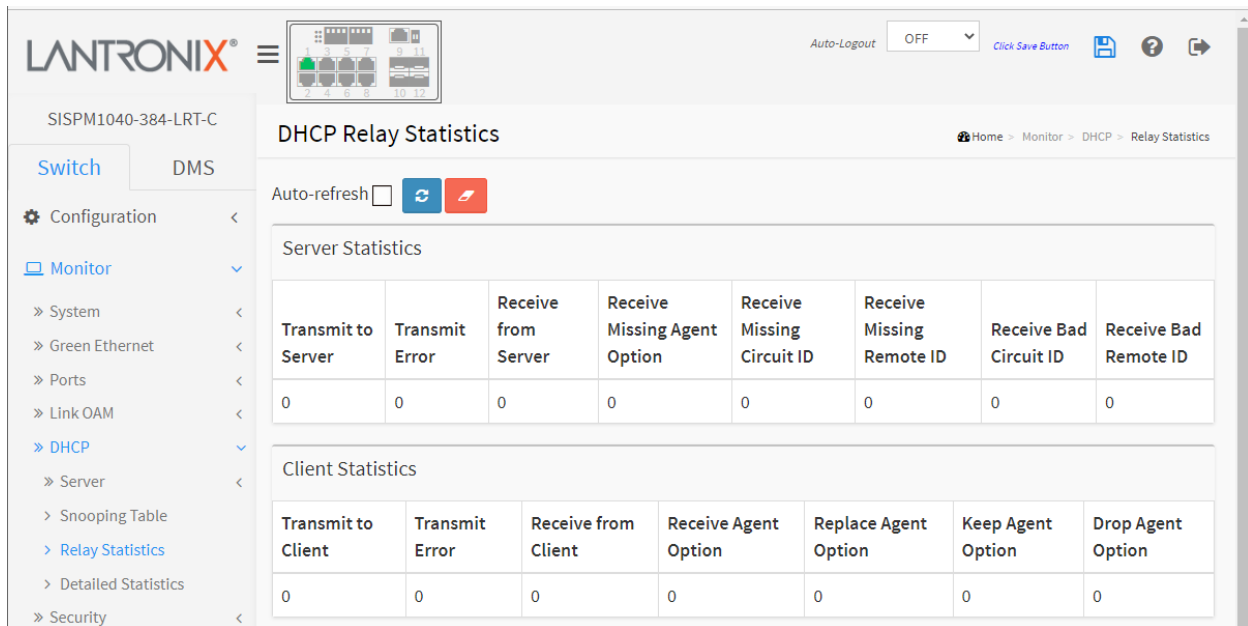
> : Updates the table, starting with the entry after the last entry currently displayed.

3-5.3 Relay Statistics

This page displays statistics for DHCP relay.

1. Click Monitor, DHCP, Relay Statistics.
2. Check "Auto-refresh" to automatically refresh the page every 3 seconds.
3. Click "Refresh" to refresh the statistics or clear all information when you click "Clear".

Figure 3-5.3: 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 a known circuit ID.

Receive Bad Remote ID : The number of packets whose Remote ID option did not match a 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: Refreshes the displayed table starting from the input fields.

Clear : Flushes all dynamic entries.

3-5.4 Detailed Statistics

This page provides statistics for DHCP snooping. Note that the normal forward per-port TX statistics are not increased if the incoming DHCP packet is done by L3 forwarding mechanism. Clearing the statistics on a specific port may not take effect on global statistics, since it gathers the different layer overview.

To monitor detailed DHCP snooping statistics in the web UI:

1. Click Monitor, DHCP, Detailed Statistics.
2. Select the set of users and the desired port at the dropdowns.
3. Check "Auto-refresh" to refresh the page automatically every 3 seconds.
4. Click "Refresh" to refresh the statistics or clear all information when you click "Clear".

Figure 3-5.4: DHCP Detailed Statistics

The screenshot shows the Lantronix web interface for monitoring DHCP statistics on Port 1. The interface includes a navigation menu on the left, a top header with the Lantronix logo and system information, and a main content area with a table of statistics.

LANTRONIX SISPM1040-384-LRT-C

Auto-Logout OFF Click Save Button

Home > Monitor > DHCP > Detailed Statistics

DHCP Detailed Statistics Port 1

Auto-refresh Refresh Clear Combined Port 1

Receive Packets		Transmit Packets	
Rx Discover	0	Tx Discover	0
Rx Offer	0	Tx Offer	0
Rx Request	0	Tx Request	0
Rx Decline	0	Tx Decline	0
Rx ACK	0	Tx ACK	0
Rx NAK	0	Tx NAK	0
Rx Release	0	Tx Release	0
Rx Inform	0	Tx Inform	0
Rx Lease Query	0	Tx Lease Query	0
Rx Lease Unassigned	0	Tx Lease Unassigned	0
Rx Lease Unknown	0	Tx Lease Unknown	0
Rx Lease Active	0	Tx Lease Active	0
Rx Discarded Checksum Error	0		
Rx Discarded from Untrusted	0		

Parameter descriptions:

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: Refreshes the displayed table starting from the input fields.

Clear : Flushes all dynamic entries.

: The DHCP user select box determines which user information is displayed. At the dropdown select Combined (default), Normal Forward, Server, Client, Snooping, or Relay.

Combined
Normal Forward
Server
Client
Snooping
Relay

: The port select box determines which port's information is displayed. The default is Port 1.

Port 1
Port 2
Port 3
Port 4
Port 5
Port 6
Port 7
Port 8

3-6 Security

3-6.1 Access Management Statistics

This page provides statistics for access management.

1. Click Monitor, Security, Access Management Statistics.
2. Check "Auto-refresh".
3. Click "Refresh" to refresh the statistics or clear all information when you click "Clear".

Figure 3-6.1: Access Management Statistics

The screenshot shows the Lantronix web interface for the device SISPM1040-384-LRT-C. The page title is "Access Management Statistics". In the top right, there is an "Auto-Logout" dropdown set to "OFF" and a "Click Save Button" link. The left sidebar shows a navigation menu with "Monitor" selected, and "Security" > "Access Management Statistics" highlighted. The main content area features an "Auto-refresh" checkbox (checked) and two buttons: a blue "Refresh" button and a red "Clear" button. Below these is a table with the following data:

Interface	Received Packets	Allowed Packets	Discarded Packets
HTTP	0	0	0
HTTPS	0	0	0
SNMP	0	0	0
TELNET	0	0	0
SSH	0	0	0

Parameter descriptions:

Interface : The interface type through which the remote host can access the switch (HTTP, HTTPS, SNMP, TELNET, and SSH).

Received Packets : Number of received packets from the interface when access management mode is enabled.

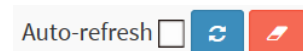
Allowed Packets : Number of allowed packets from the interface when access management mode is enabled.

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 manually refresh the page immediately.



Clear: Clears the counters for the selected port.

3-6.2 Network

3-6.2.1 Port Security

3-6.2.1.1 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 view Port Security Switch Status in the web UI:

1. Click Monitor, Security, Network, Port Security, then Switch.
2. Check "Auto-refresh".
3. Click "Refresh" to refresh the port detailed statistics.

Figure 3-6.2.1.1: Port Security Switch Status

The screenshot displays the 'Port Security Switch Status' page. At the top, there is a breadcrumb trail: Home > Monitor > Security > Network > Port Security > Switch. Below the breadcrumb, there is an 'Auto-refresh' checkbox which is checked, and a refresh icon. The page is divided into two main sections: 'User Module Legend' and 'Port Status'.

User Module Legend

User Module Name	Abbr
Limit Control	L
802.1X	8
Voice VLAN	V

Port Status

Port	Users	State	MAC Count	
			Current	Limit
1	L--	Ready	0	4
2	L--	Ready	0	4
3	L--	Ready	0	4
4	L--	Ready	0	4
5	L--	Ready	0	4
6	L--	Ready	0	4

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; used in the Users column in the port status table.

Limit Control : e.g., L.

802.1X : e.g., 8.

Voice VLAN : e.g., V.

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 linked 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) 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.

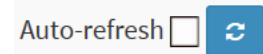
Shutdown: The Port Security service is enabled by at least the Limit Control user module, and that module has indicated that the limit is exceeded. No MAC addresses can be learned on the port until it is administratively re-opened on the Limit Control configuration Web-page.

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 manually refresh the page immediately.

Port Security Port Status for Port 9

On the Port Status page, click a linked port number to see the status for the selected port (see below).

3-6.2.1.2 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 Port Status via the web UI:

1. Click Monitor, Security, Network, Port Security, and then Port.
2. Specify the Port which you want to monitor.
3. Check "Auto-refresh".
4. Click "Refresh" to refresh the port detailed statistics.

Figure 3-6.2.1.2: Port Security Port Status

Parameter descriptions:

MAC Address and **VLAN ID** : The MAC address and VLAN ID that are 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 (-) displays.

Buttons

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

Refresh: Click to manually refresh the page immediately.

Clear : Clears the page data.

: Port Select box; Use the port select box to select which port to show status for.

3-6.2.2 NAS

3-6.2.2.1 Switch

This section shows the NAS status information of each port of the switch. The status includes Admin State Port State, Last Source, Last ID, QoS Class, and Port VLAN ID.

To view 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.

Figure 3-6.2.2.1: Network Access Server Switch Status

Port	Admin State	Port State	Last Source	Last ID	QoS Class	Port VLAN ID
1	Port-based 802.1X	Link Down			-	
2	Single 802.1X	Authorized			-	1 (Guest)
3	Multi 802.1X	Link Down			-	
4	MAC-based Auth.	Link Down			-	
5	Force Authorized	Link Down			-	
6	Force Authorized	Link Down			-	
7	Force Authorized	Link Down			-	
8	Force Authorized	Link Down			-	
9	Force Authorized	Authorized			-	
10	Force Authorized	Link Down			-	
11	Force Authorized	Link Down			-	
12	Force Authorized	Link Down			-	

Parameter descriptions:

Port : The switch port number. Click to navigate to detailed NAS statistics for this port.

Admin State : The port's current administrative state. Can be Port-based 802.1X, Single 802.1X, Multi 802.1X, MAC-based Auth. , or Force Authorized. Refer to NAS Admin State for descriptions at Configuration > Security > Network > NAS.

Port State : The current state of the port. Can be Authorized, Unauthorized, Link Down, etc. Refer to NAS Port State for descriptions at Configuration > Security > Network > NAS.

Last Source : The source MAC address carried in the most recently received EAPOL frame for EAPOL-based authentication, and the most recently received frame from a new client for MAC-based authentication.

Last ID : The user name (supplicant identity) carried in the most recently received Response Identity EAPOL frame for EAPOL-based authentication, and the source MAC address from the most recently received frame from a new client for MAC-based authentication.

QoS Class : QoS Class assigned to the port by the RADIUS server if enabled.

Port VLAN ID : The VLAN ID that 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.

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

Guest VLAN : 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.

RADIUS-Assigned VLAN : 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.

Buttons

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

Refresh: Click to manually refresh the page immediately.

3-6.2.2.2 Port

This page displays 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.

To view a port's NAS Port state and counters via the web UI:

1. Click Monitor, Security, Network, NAS, and Port.
2. Select the desired Port at the Port select dropdown.
3. Check "Auto-refresh".
4. Click "Refresh" to refresh the port detailed statistics.

Figure 3-6.2.2.2: NAS Statistics

The screenshot displays the 'NAS Statistics Port 9' web interface. At the top, there's a breadcrumb trail: Home > Monitor > Security > Network > NAS > Port. The interface includes a navigation sidebar on the left with options like Configuration, Monitor, System, Green Ethernet, Ports, Link OAM, DHCP, Security, Access Management Statistics, Network, Port Security, NAS, Switch, Port, ACL Status, and ARP Inspection. The main content area features an 'Auto-refresh' checkbox, a 'Clear' button, and a dropdown menu for 'Port 9'. Below this, the 'Port State' section contains a table with 'Admin State' (Force Authorized) and 'Port State' (Authorized). The 'Port Counters' section contains a table with 'Receive EAPOL Counters' and 'Transmit EAPOL Counters' columns, listing metrics such as Total, Response ID, Requests, Start, Logoff, Invalid Type, and Invalid Length, all with a value of 0.

Parameter descriptions:

Port State

Admin State : The port's current administrative state. Can be Port-based 802.1X, Single 802.1X, Multi 802.1X, MAC-based Auth. , or Force Authorized. Refer to NAS Admin State for descriptions at Configuration > Security > Network > NAS.

Port State : The current state of the port. Can be Authorized, Unauthorized, Link Down, etc. Refer to NAS Port State for descriptions at Configuration > Security > Network > NAS.

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. See the online help more about RADIUS-assigned VLANs.

If the port is moved to the Guest VLAN, "(Guest)" is appended to the VLAN ID. See the online help for more about Guest VLANs.

Port Counters

The screenshot shows the 'NAS Statistics Port 2' page. The 'Port State' section contains the following information:

Admin State	Single 802.1X
Port State	Authorized
QoS Class	-
Port VLAN ID	1 (Guest)

The 'Port Counters' section is divided into three main categories:

Receive EAPOL Counters		Transmit EAPOL Counters	
Total	0	Total	2
Response ID	0	Request ID	2
Responses	0	Requests	0
Start	0		
Legoff	0		
Invalid Type	0		
Invalid Length	0		

Receive Backend Server Counters		Transmit Backend Server Counters	
Access Challenges	0	Responses	0
Other Requests	2		
Auth. Successes	0		
Auth. Failures	0		

The 'Supplicant Info' section contains the following information:

MAC Address	
VLAN ID	0
Version	0
Identity	

EAPOL Counters : The supplicant frame counters are available for these administrative states:

- Force Authorized
- Force Unauthorized
- Port-based 802.1X
- Single 802.1X
- Multi 802.1X

Backend Server Counters : The backend (RADIUS) frame counters are available for these administrative states:

- Port-based 802.1X
- Single 802.1X
- Multi 802.1X
- MAC-based Auth.

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.

Selected Counters: The Selected Counters table is visible when the port is in one of these admin states:

- Multi 802.1X
- MAC-based Auth.

The table is identical to and is placed next to the Port Counters table; it 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 manually refresh the page immediately.

Clear : Click to clear the counters for the selected port. This button is available in these modes: Force Authorized, Force Unauthorized, Port-based 802.1X, and Single 802.1X.

Clear All : 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 and MAC-based Auth.X.

Clear This : Click to clear only the currently selected client counters. This button is available in these modes: Multi 802.1X and MAC-based Auth.X.

3-6.2.3 ACL Status

This page displays the ACL status by different ACL users. Each row describes the ACE that is defined. It is a conflict if a specific ACE is not applied to the hardware due to hardware limitations. The maximum number of ACEs is 256 per switch.

To display ACL status in the web UI:

1. Click Monitor, Security, Network, and ACL Status.
2. Select the desired set of users at the User Select box.
3. To automatically refresh the information every 3 seconds, check the "Auto-refresh" box.
4. Click "Refresh" to manually refresh the ACL Status immediately.

Figure 3-6.2.3: ACL Status

The screenshot shows the Lantronix web interface for device SISPM1040-384-LRT-C. The navigation menu on the left includes Configuration, Monitor, Security, and Network. The ACL Status page is active, showing a table of ACL entries. The table has 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	333	No
DMS Onvif	1	All	IPv4/UDP 10100-10107	Permit	Disabled	Disabled	Disabled	No	0	No
DMS SSDP	1	All	IPv4/UDP 1900	Permit	Disabled	Disabled	Disabled	No	11475	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	0	No
dhcp	3	All	IPv4/UDP 67 DHCP Client	Deny	Disabled	Disabled	Disabled	No	0	No
arpinspection	1	All	ARP	Deny	Disabled	Disabled	Disabled	No	699	No
mep	3	1	EType	Filter	Disabled	Disabled	Disabled	Yes	0	No
mep	2	1	EType	Filter	Disabled	Disabled	Disabled	Yes	0	No
mep	1	1	EType	Deny	Disabled	Disabled	Disabled	No	0	No

Parameter descriptions:

User : Indicates the ACL user (e.g., Rapid Ring, DMS mDNS, DMS Onvif, DMS SSDP, DMS CLIENT, dhcp, arpinspection).

ACE : Indicates the ACE ID on the local switch.

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

All: The ACE will match all ingress ports.

Port: The ACE will match a specific ingress port.

Frame Type : Indicates the frame type of the ACE. Possible values are:

Any: The ACE will match any frame type.

EType: The ACE will match Ethernet Type frames. Note that an Ethernet Type based ACE will not get matched by IP and ARP frames.

ARP: The ACE will match ARP/RARP frames.

IPv4: The ACE will match all IPv4 frames.

IPv4/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.

Frame Type examples: IPv4/UDP 10100-10107, IPv4/UDP 67 DHCP Client, IPv4/UDP 68 DHCP Server.

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.

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

Enabled: Frames received on the port are mirrored.

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

CPU : Forward packet that matched the specific ACE to CPU.

CPU Once : Forward first 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.

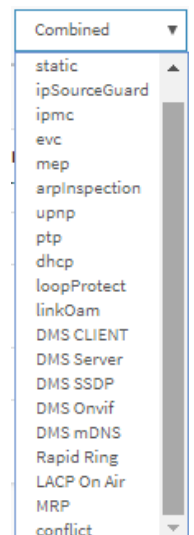
Buttons



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

Refresh: Click to manually refresh the page immediately.

User Select dropdown: View the combined set of views, or filter an individual view (Combined, static, ipSourceGuard, ipmc, evc, mep, arpinspection, upnp, ptp, dhcp, loopProtect, linkOam, DMS CLIENT, DMS Server, DMS SSDP, DMS Onvif, DMS mDNS, Rapid Ring, LACP on Air, MRP, and conflict).



3-6.2.4 ARP Inspection

This page lets you monitor 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.

To view Dynamic ARP Inspection Table parameters via 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 3-6.2.4: 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 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.

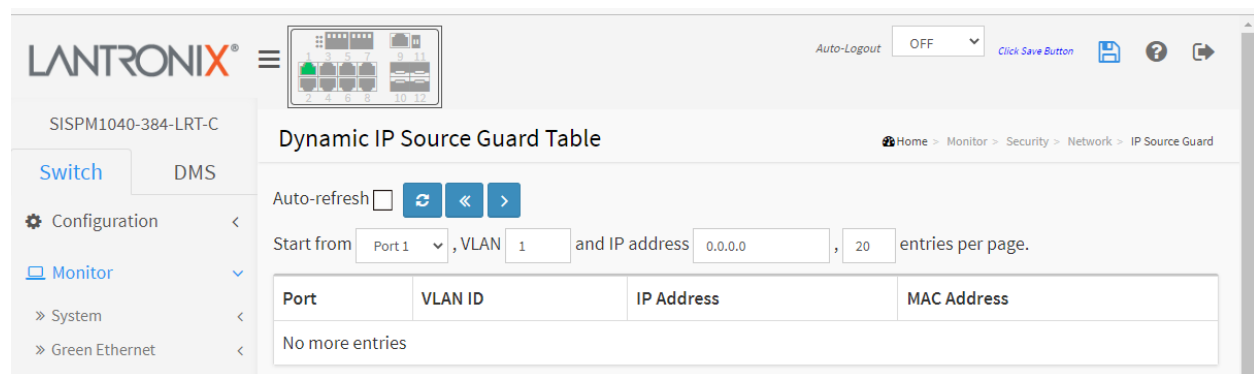
3-6.2.5 IP Source Guard

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.

To view the Dynamic IP Source Guard Table in the web UI:

1. Click Security, Network, IP Source Guard.
2. Check "Auto-refresh".
3. Click "Refresh" to refresh the port detailed statistics.
4. Specify the "Start from" port, VLAN ID, IP Address, and entries per page.

Figure 3-6.2.5: 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 : Source MAC address.

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.

3-6.3 AAA

3-6.3.1 RADIUS Overview

This page displays the status of the RADIUS servers set at Configuration > Security > AAA > RADIUS.

To view RADIUS Server Status via the web UI:

1. Click Monitor, Security, AAA, RADIUS Overview.
2. Check "Auto-refresh" or click "Refresh" to refresh the port detailed statistics.
3. Click a linked RADIUS server number to navigate to detailed statistics for the server.

Figure 3-6.3.1: RADIUS Server Status Overview

#	IP Address	Authentication Port	Authentication Status	Accounting Port	Accounting Status
1	RadSvr1	1812	Ready	1813	Ready
2	Radrvr2	1812	Ready	1813	Ready
3	radius3	1812	Ready	1813	Ready
4	radius4	1812	Ready	1813	Ready
5	radius5	1645	Ready	1646	Ready

Parameter descriptions:

: The RADIUS server number. Click to navigate to detailed statistics for this server.

IP Address : The IP address of this RADIUS server.

Authentication Port : UDP port number for authentication (e.g., 1812 or 1645).

Authentication Status : The current state of the server. This field takes one of the following values:

Disabled: The RADIUS server is disabled.

Not Ready: The RADIUS server is enabled, but IP communication is not yet up and running.

Ready: The RADIUS 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 RADIUS 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 (e.g., 1813 or 1646).

Accounting Status : The current state of the server. This field takes one of the following values:

Disabled: The server is disabled.

Not Ready: The server is enabled, but IP communication is not yet up and running.

Ready: The server is enabled, IP communication is up and running, and the RADIUS module is ready to accept access attempts.

Dead (X seconds left): Access attempts were made to this server, but it did not reply within the configured timeout. The server has temporarily been disabled but will get re-enabled when the dead-time expires. The number of seconds left before this occurs is displayed in parentheses. This state is only reachable when more than one server is enabled.

Buttons

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

Refresh: Click to manually refresh the page immediately.

3-6.3.2 RADIUS Details

This page displays detailed statistics for a particular RADIUS server.

To view RADIUS Details Configuration in the web interface:

1. Navigate to Monitor > Security > AAA > RADIUS Details.
2. At the Server select dropdown select which RADIUS Server you want to check.
3. Check "Auto-refresh".
4. Click "Refresh" to refresh the port detailed statistics or clear all information when you click "Clear".

Figure 3-6.3.2: RADIUS Authentication Statistics

The screenshot shows the RADIUS Authentication Statistics page for Server #1. The interface includes an 'Auto-refresh' checkbox, a 'Refresh' button, and a 'Server #1' dropdown menu. The main content area displays two tables: 'RADIUS Authentication Statistics for Server #1' and 'RADIUS Accounting Statistics for Server #1'. Both tables show metrics for Receive and Transmit packets, including Access Accepts, Access Rejects, Access Challenges, Malformed Access Responses, Bad Authenticators, Unknown Types, Packets Dropped, Requests, Retransmissions, Pending Requests, and Timeouts. Other info includes IP Address, State, and Round-Trip Time.

RADIUS Authentication Statistics for Server #1			
Receive Packets		Transmit Packets	
Access Accepts	0	Access Requests	0
Access Rejects	0	Access Retransmissions	0
Access Challenges	0	Pending Requests	0
Malformed Access Responses	0	Timeouts	0
Bad Authenticators	0		
Unknown Types	0		
Packets Dropped	0		
Other Info			
IP Address	RadSrvr1:1812		
State	Ready		
Round-Trip Time	0 ms		

RADIUS Accounting Statistics for Server #1			
Receive Packets		Transmit Packets	
Responses	0	Requests	0
Malformed Responses	0	Retransmissions	0
Bad Authenticators	0	Pending Requests	0
Unknown Types	0	Timeouts	0
Packets Dropped	0		
Other Info			
IP Address	RadSrvr1:1813		
State	Ready		
Round-Trip Time	0 ms		

Parameter descriptions:**RADIUS Authentication Statistics**

The statistics map closely to those specified in RFC4668 - RADIUS Authentication Client MIB. Use the server select box to switch between the backend servers to show details for.

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 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 enable an automatic refresh of the page every three seconds.

Refresh - Click to manually refresh the page immediately.

Clear - Clears the counters for the selected server. The "Pending Requests" counter will not be cleared by this operation.

3-6.4 Switch

3-6.4.1 RMON

3-6.4.1.1 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.

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*" is shown in the displayed table. Use the button to start over.

Web Interface

To view RMON Statistics in the web UI:

1. Click Monitor, Security, Switch, RMON, Statistics.
2. Specify the Start from Control Index and entries per page settings.
3. Check "Auto-refresh" or click "Refresh" to refresh the port detailed statistics.

Figure 3-6.4.1.1: RMON Statistics Status Overview

Data Source ID (if Index)	Drop	Octets	Pkts	Broadcast	Multicast	CRC Errors	Under-size	Over-size	Frag.	Jab.	Coll.	64 Bytes	65 ~ 127	128 ~ 255	256 ~ 511	512 ~ 1023	1024 ~ 1588
1	0	13339455	57225	29849	20931	0	0	0	0	0	0	35151	16	2	21461	20	575
2	0	42543217	209200	38518	6183	0	0	0	0	0	0	147073	1312	5996	123	54646	50

Parameter descriptions:

ID : Indicates the index of Statistics entry. Click a linked ID number to display the Detailed RMON Statistics page (see below).

Data Source(if Index) : The port ID monitored in each row.

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 65 - 127 octets long.

128~255 : The total number of packets (including bad packets) received that were 128 - 255 octets long.

256~511 : The total number of packets (including bad packets) received that were between 256 - 511 octets long.

512~1023 : The total number of packets (including bad packets) received that were 512 - 1023 octets long.

1024~1588 : The total number of packets (including bad packets) received that were 1024 - 1588 octets long.

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 Statistics table, i.e. the entry with the lowest ID.

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

Detailed RMON Statistics

Click on a linked ID number to display the Detailed RMON Statistics for the selected ID.

The screenshot displays the 'Detailed RMON Statistics ID 2' page. The left sidebar shows a navigation menu with 'Switch' and 'DMS' tabs. The main content area features a table of statistics for ID 2, with an 'Auto-refresh' checkbox and a refresh button. The table lists various metrics and their corresponding values.

Receive Total	
Port	2
Drops	0
Octets	42590633
Pkts	209406
Broadcast	38558
Multicast	6183
CRC/Alignment	0
Undersize	0
Oversize	0
Fragments	0
Jabber	0
Collisions	0
64 Bytes	147213
65-127 Bytes	1315
128-255 Bytes	5996
256-511 Bytes	123
512-1023 Bytes	54709
1024-1518 Bytes	50

3-6.4.1.2 History

This section 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" let you select the starting point in the History table.

To view RMON History Configuration in the web UI:

1. Click Security, Switch, RMON, History.
2. Check "Auto-refresh".
3. Click "Refresh" to refresh the statistics or clear all information when you click " Clear".

Figure 3-6.4.1.2: RMON History Overview

History Index	Sample Index	Sample Start	Drop	Octets	Pkts	Broadcast	Multicast	CRC Errors	Under-size	Over-size	Frag.	Jabb.	Coll.	Utilization
1	1	66380	0	0	0	0	0	0	0	0	0	0	0	0
1	2	68180	0	0	0	0	0	0	0	0	0	0	0	0
1	3	69980	0	0	0	0	0	0	0	0	0	0	0	0
1	4	71780	0	0	0	0	0	0	0	0	0	0	0	0
1	5	73580	0	0	0	0	0	0	0	0	0	0	0	0
1	6	75380	0	0	0	0	0	0	0	0	0	0	0	0

Parameter descriptions:

History Index : Indicates the index of History control entry. Click a linked instance to display its Detailed RMON History page (see below).

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.

Auto-refresh   

Buttons

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

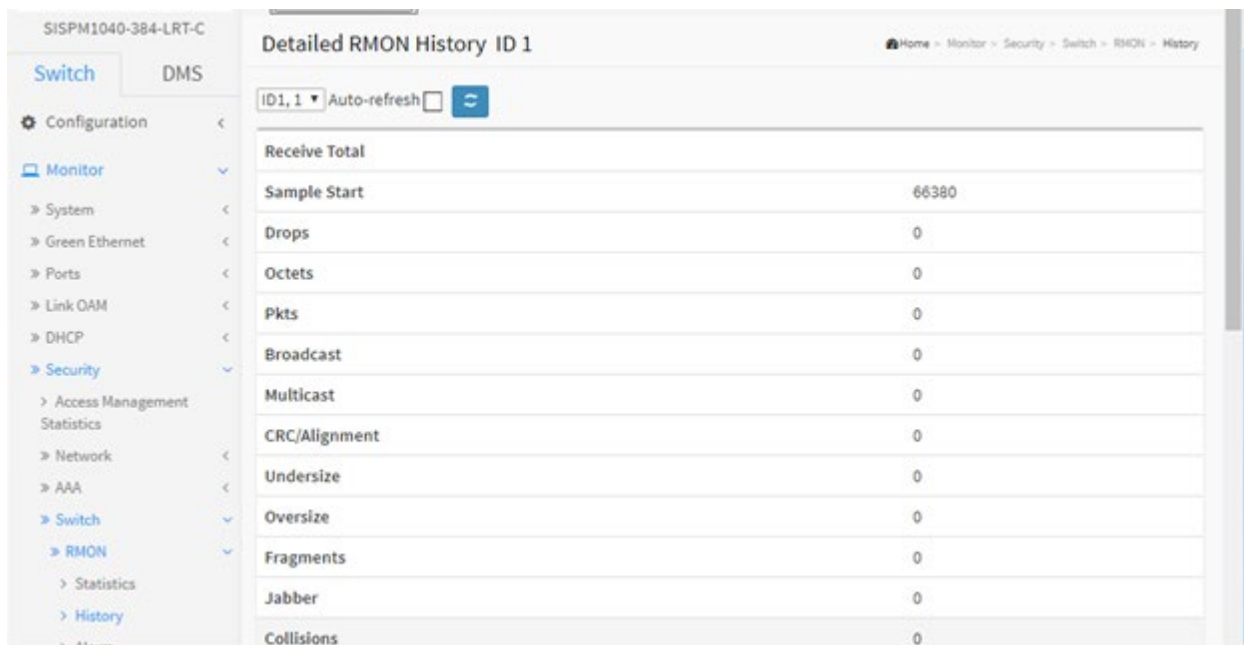
Refresh: Click to manually refresh the page immediately.

<< : First entry; updates the table starting from the first entry in the History table, i.e., the entry with the lowest History Index and Sample Index.

> : Next entry; updates the table, starting with the entry after the last entry currently displayed.

Detailed RMON History

Click a linked instance to display its Detailed RMON History page:



The screenshot shows the 'Detailed RMON History ID 1' page. The left sidebar contains a navigation menu with 'Switch' and 'DMS' tabs. The main content area displays a table with the following data:

Receive Total	
Sample Start	66380
Drops	0
Octets	0
Pkts	0
Broadcast	0
Multicast	0
CRC/Alignment	0
Undersize	0
Oversize	0
Fragments	0
Jabber	0
Collisions	0

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. Specify Port which wants to check.
2. Click Security, Switch, RMON, Alarm.
3. Check "Auto-refresh".
4. Click "Refresh" to refresh the port detailed statistics.

Figure 3-6.4.1.3: RMON Alarm Overview

ID	Interval	Variable	Sample Type	Value	Startup Alarm	Rising Threshold	Rising Index	Falling Threshold	Falling Index
1	30	.1.3.6.1.2.1.2.2.1.10.1	Delta	0	RisingOrFalling	99	9	88	8

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 manually 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.

3-6.4.1.4 Event

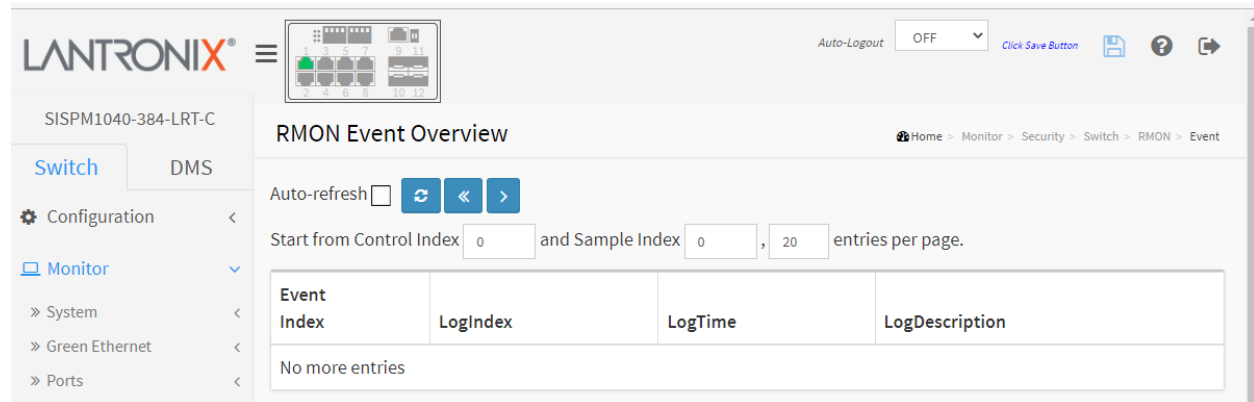
This page provides an overview of RMON Event table entries. Each page shows up to 99 entries from the Event table, default being 20, selected through the "entries per page" input field. When first visited, the web page will show the first 20 entries from the beginning of the Event table. The first entry displayed will be the one with the lowest Event Index and Log Index found in the Event table.

The "Start from Event Index and Log Index" lets you select the starting point in the Event table.

To view the RMON Event Overview in the web UI:

1. Click Security, Switch, RMON, Event.
2. Specify the Start from Control Index, Sample Index, and entries per page.
3. Check "Auto-refresh".
4. Click " Refresh" to refresh the port detailed statistics

Figure 3-6.4.1.4: RMON Event Overview



Parameter descriptions:

Event Index : Indicates the index of the event entry.

Log Index : Indicates the index of the log entry.

LogTime : Indicates Event log time

LogDescription : Indicates the Event description.

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 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

3-7 Aggregation

3-7.1 Status

This page displays the status of ports in Aggregation groups.

1. Click Monitor, Aggregation, Status.
2. Check "Auto-refresh".
3. Click "Refresh" to refresh the port detailed statistics.

Figure 3-7.1 LACP System Status



Aggr ID	Name	Type	Speed	Configured Ports	Aggregated Ports
3	LLAG3	Static	Undefined	GigabitEthernet 1/4-5	none

Parameter descriptions:

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

Name : Name of the Aggregation group.

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

Speed : 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 manually refresh the page immediately.



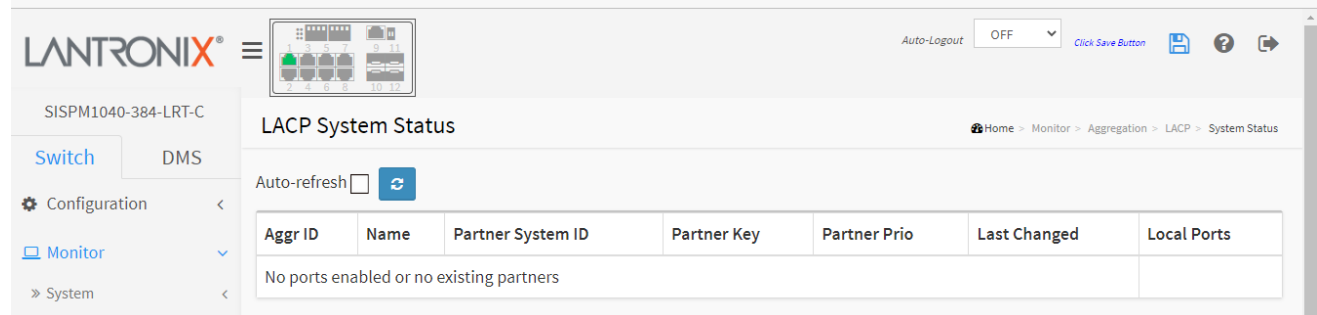
3-7.2 LACP

3-7.2.1.1 System Status

This page provides a status overview for all LACP instances.

1. Click Monitor, Aggregation, LACP, System Status.
2. To auto-refresh the information check the "Auto refresh" box.
3. Click "Refresh" to refresh the LACP Statistics.

Figure 3-7.2.1.1: 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'.

Name : Displays the Name of the Aggregation group ID.

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

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

Partner Prio : The priority of this partner.

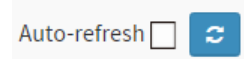
Last Changed : The time since this aggregation changed.

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 manually refresh the page immediately.



3-7.2.1.2 Port Status

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

1. Click Monitor, Aggregation, LACP, Port Status.
2. To automatically refresh the information check the "Auto refresh" box.
3. Click "Refresh" to refresh the LACP Status.

Figure 3-7.2.1.1: LACP Status

The screenshot shows the Lantronix web interface for the LACP Status page. The page title is "LACP Status" and the breadcrumb is "Home > Monitor > Aggregation > LACP > Port Status". The "Auto-refresh" checkbox is unchecked. The table below shows the LACP status for 12 ports.

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

Parameter descriptions:

Port : The switch port number.

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

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

Aggr ID : The Aggregation ID assigned to this aggregation group.

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

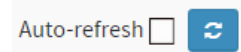
Partner Port : The partner's port number connected to this port.

Partner Prio : The partner's port priority.

Buttons

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

Refresh: Click to manually refresh the page immediately.



3-7.2.1.3 Port Statistics

This page displays LACP statistics for all ports.

1. Click Monitor, Aggregation, LACP, Port Statistics.
2. To auto-refresh the information check the "Auto refresh" box.
3. Click "Refresh" to update the LACP Statistics.

Figure 3-7.2.1.3: LACP Port Statistics

The screenshot shows the 'LACP Statistics' page in the Lantronix web interface. The page title is 'LACP Statistics' and the breadcrumb trail is 'Home > Monitor > Aggregation > LACP > Port Statistics'. There is an 'Auto-refresh' checkbox which is unchecked, followed by a refresh icon (circular arrow) and a clear icon (eraser). Below this is a table with the following data:

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
11	0	0	0	0
12	0	0	0	0

Parameter descriptions:

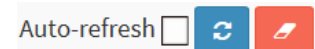
Port : The switch port number.

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 and Illegal LACP frames have been discarded at each port.

Buttons



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

Clear: Clears the counters for the selected port.

Refresh: Click to manually refresh the page immediately.

3-8 Loop Protection

This page displays the loop protection port status for all switch ports.

1. Click Monitor, Loop Protection.
2. To automatically refresh the information, check the "Auto refresh" checkbox.
3. Click "Refresh" to refresh the LACP Statistics.

Figure 3-8 : Loop Protection Status

Port	Action	Transmit	Loops	Status	Loop	Time of Last Loop
1	Log Only	Enabled	0	Down	-	-
2	Log Only	Enabled	0	Down	-	-
3	Shutdown+Log	Enabled	0	Down	-	-
4	Shutdown+Log	Enabled	0	Down	-	-
5	Shutdown	Enabled	0	Down	-	-
6	Shutdown	Enabled	0	Down	-	-
7	Shutdown	Enabled	0	Down	-	-

Parameter descriptions:

Port : The switch port number of the logical port.

Action : The currently configured port action.

Transmit : The currently configured port transmit mode.

Loops : The number of loops detected on this port.

Status : The current loop protection status of the port.

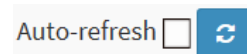
Loop : Whether a loop is currently detected on the port.

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

Buttons

Refresh: Click to manually refresh the page immediately.

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



3-9 Spanning Tree

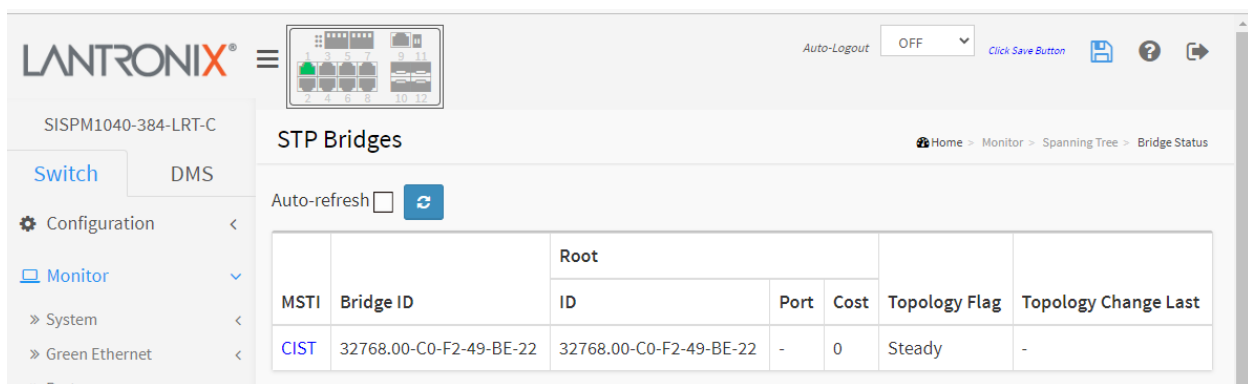
3-9.1 Bridge Status

After you complete the MSTI Port configuration you can display the Bridge Status. This page provides a status overview of all STP bridge instances. The displayed table contains a row for each STP bridge instance.

To display STP Bridges status in the web UI:

1. Click Monitor, Spanning Tree, STP Bridges.
2. To auto-refresh the information check the "Auto-refresh" checkbox.
3. Click "Refresh" to refresh the STP Bridges.
4. Click "CIST" to go to the next page "STP Detailed Bridge Status".

Figure 3-9.1: STP Bridges status



The screenshot shows the Lantronix web interface for the device SISPM1040-384-LRT-C. The page title is "STP Bridges". There is an "Auto-refresh" checkbox which is currently 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-BE-22	32768.00-C0-F2-49-BE-22	-	0	Steady	-

Parameter descriptions:

MSTI : The Bridge Instance. This is also a link to the STP Detailed Bridge Status page.

Bridge ID : The Bridge ID of this Bridge instance.

Root ID : The Bridge ID of the currently elected root bridge.

Root Port : The switch port currently assigned the root port role.

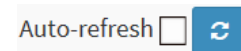
Root Cost : Root Path Cost. For the Root Bridge it is zero. For all other Bridges, it is the sum of the Port Path Costs on the least cost path to the Root Bridge.

Topology Flag : The current state of the Topology Change Flag of this Bridge instance.

Topology Change Last : The time since last Topology Change occurred.

Buttons

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



Refresh: Click to manually refresh the page immediately.

STP Detailed Bridge Status page

This page provides detailed information on a single STP bridge instance, along with port state for all active ports associated.

The screenshot shows the 'STP Detailed Bridge Status' page. The left sidebar has 'Monitor' selected, with 'Spanning Tree' > 'Bridge Status' highlighted. The main content area includes an 'Auto-refresh' checkbox and a refresh icon. Below this are two sections:

STP Bridge Status

Bridge Instance	CIST
Bridge ID	32768.00-C0-F2-49-3D-4F
Root ID	32768.00-C0-F2-49-3D-4F
Root Cost	0
Root Port	-
Regional Root	32768.00-C0-F2-49-3D-4F
Internal Root Cost	0
Topology Flag	Steady
Topology Change Count	0
Topology Change Last	-

CIST Ports & Aggregations State

Port	Port ID	Role	State	Path Cost	Edge	Point-to-Point	Uptime
1	128:001	DesignatedPort	Forwarding	200000	Yes	Yes	0d 01:29:37
2	128:002	DesignatedPort	Forwarding	20000	Yes	Yes	0d 01:29:37
3	128:003	DesignatedPort	Forwarding	20000	Yes	Yes	0d 01:29:37
4	128:004	DesignatedPort	Forwarding	200000	Yes	Yes	0d 01:29:37
8	128:008	BackupPort	Discarding	20000	No	Yes	0d 01:29:37

Parameter descriptions:

STP Bridge Status

Bridge Instance : The Bridge instance - CIST, MST1, etc.

Bridge ID : The Bridge ID of this Bridge instance.

Root ID : The Bridge ID of the currently elected root bridge.

Root Port : The switch port currently assigned the root port role.

Root Cost : Root Path Cost. For the Root Bridge this is zero. For all other Bridges, it is the sum of the Port Path Costs on the least cost path to the Root Bridge.

Regional Root ; The Bridge ID of the currently elected regional root bridge, inside the MSTP region of this bridge (for the CIST instance only).

Internal Root Cost : The Regional Root Path Cost. For the Regional Root Bridge this is zero. For all other CIST instances in the same MSTP region, it is the sum of the Internal Port Path Costs on the least cost path to the Internal Root Bridge (for the CIST instance only).

Topology Flag : The current state of the Topology Change Flag of this Bridge instance.

Topology Change Count : The number of times where the topology change flag has been set (during a one-second interval).

Topology Change Last : The time passed since the Topology Flag was last set.

CIST Ports & Aggregations State

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

Port ID : The port id as used by the STP protocol. This is the priority part and the logical port index of the bridge port.

Role : The current STP port role. The port role can be one of these values: AlternatePort, BackupPort, RootPort, or DesignatedPort.

State : The current STP port state. The port state can be one of 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 manually refresh the page immediately.

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

3-9.2 Port Status

This page displays the STP CIST port status for physical ports of the switch.

To display the STP Port status in the web UI:

1. Click Monitor, Spanning Tree, Port Status.
2. To automatically refresh the information, check the "Auto-refresh" checkbox.
3. Click "Refresh" to refresh the STP ports status.

Figure 3-9.2: STP Port Status

Port	CIST Role	CIST State	Uptime
1	DesignatedPort	Forwarding	0d 01:28:23
2	DesignatedPort	Forwarding	0d 01:28:23
3	DesignatedPort	Forwarding	0d 01:28:23
4	DesignatedPort	Forwarding	0d 01:28:23
5	Disabled	Discarding	-
6	Disabled	Discarding	-
7	Disabled	Discarding	-
8	BackupPort	Discarding	0d 01:28:23

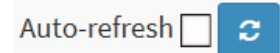
Parameter descriptions:

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 AlternatePort, Backup Port, RootPort, DesignatedPort, Disabled, or Non-STP.

CIST State : The current STP port state of the CIST port. The port state can be Blocking, Discarding, Learning, or Forwarding.

Uptime : The time since the bridge port was last initialized in days, hours, minutes, and seconds.



Buttons

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

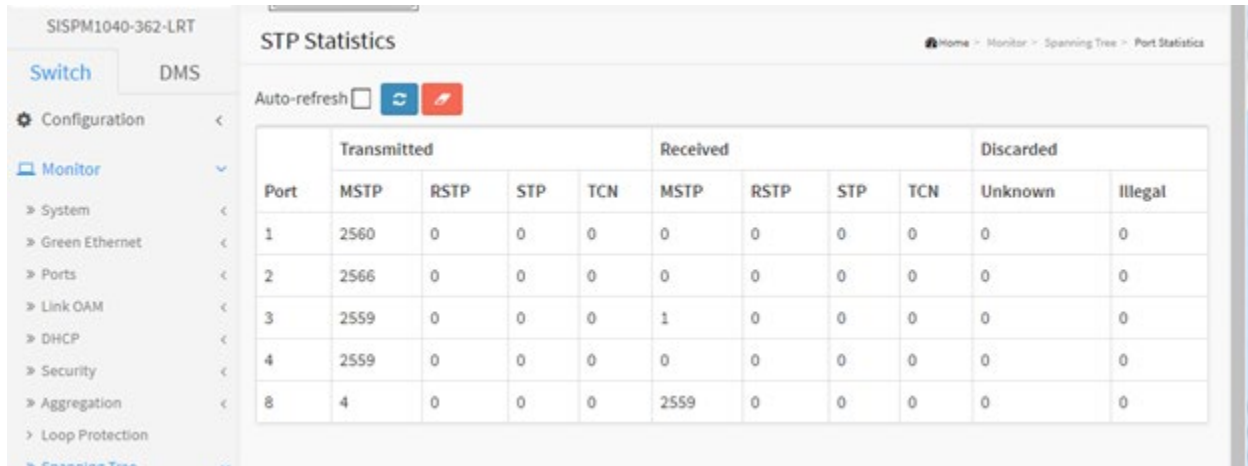
Refresh: Click to manually refresh the page immediately.

3-9.3 Port Statistics

This page displays the STP port statistics counters of bridge ports in the switch.

1. Click Monitor, Spanning Tree, Port Statistics.
2. Check the Auto-refresh box to automatically update the page.
3. Click "Refresh" to refresh the STP Bridges table.

Figure 3-9.3: STP Statistics



Port	Transmitted				Received				Discarded	
	MSTP	RSTP	STP	TCN	MSTP	RSTP	STP	TCN	Unknown	Illegal
1	2560	0	0	0	0	0	0	0	0	0
2	2566	0	0	0	0	0	0	0	0	0
3	2559	0	0	0	1	0	0	0	0	0
4	2559	0	0	0	0	0	0	0	0	0
8	4	0	0	0	2559	0	0	0	0	0

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.

Clear: Clears the counters for the selected port.

Refresh: Click to manually refresh the page immediately.

3-10 MVR

3-10.1 Statistics

This page provides MVR Statistics information.

1. Click Monitor, MVR, Statistics.
2. To auto-refresh the information check the "Auto-refresh" checkbox.
3. Click the "Refresh" to refresh an entry of the MVR Statistics Information.

Figure 3-10.1: MVR Statistics

VLAN ID	IGMP/MLD Queries Received	IGMP/MLD Queries Transmitted	IGMPv1 Joins Received	IGMPv2/MLDv1 Reports Received	IGMPv3/MLDv2 Reports Received	IGMPv2/MLDv1 Leaves Received
1	0/0	0/0	0	0/0	0/0	0/0
2	0/0	0/0	0	0/0	0/0	0/0

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.

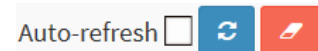
IGMPv1 Joins Received : The number of Received IGMPv1 Join's.

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.

Clear: Clears the counters for the selected port.

Refresh: Click to manually refresh the page immediately.

3-10.2 MVR Channels Groups

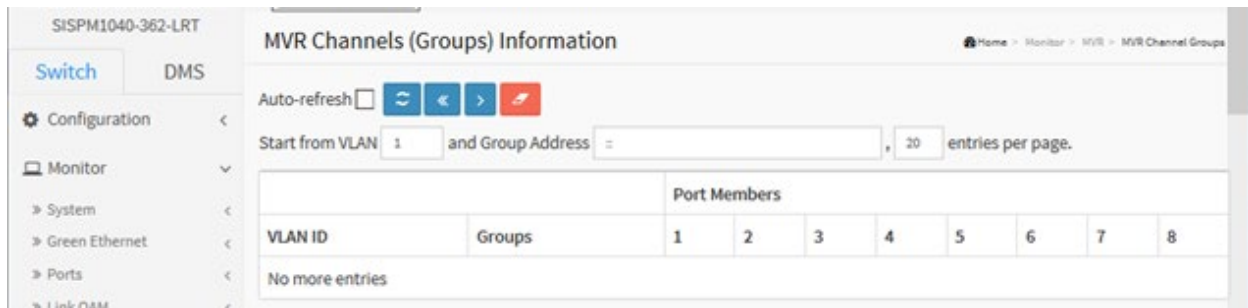
Entries in the MVR Channels (Groups) Information Table are shown on this page. The MVR Channels (Groups) Information Table is sorted first by VLAN ID, and then by group.

Each page shows up to 99 entries from the MVR Group table, default being 20, selected through the "entries per page" input field. When first visited, the web page will show the first 20 entries from the beginning of the MVR Channels (Groups) Information Table. The "Start from VLAN", and "Group Address" input fields allow the user to select the starting point in the MVR Channels (Groups) Information Table. The > 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 MVR Groups Information in the web UI:

1. Click Monitor, MVR, MVR Channel Groups.
2. To auto-refresh the information check the Auto-refresh box.
3. Click Refresh to refresh an entry of the MVR Groups Information.
4. Click << or > to move to the previous or next entry.

Figure 3-10.2: MVR Groups Information



Parameter descriptions:

VLAN ID : VLAN ID of the group.

Groups : Group ID of the group displayed.

Port Members : Ports under this group.

Buttons



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

Refresh: Click to 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 information.

3-10.3 MVR SFM Information

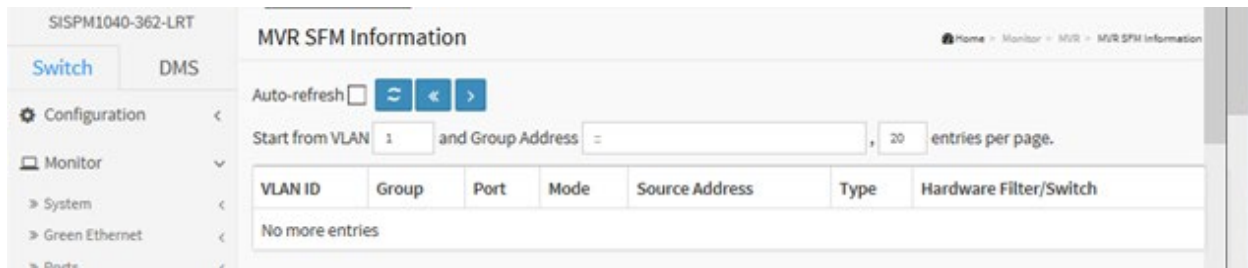
Entries in the MVR SFM Information Table are shown on this page. The MVR SFM (Source-Filtered Multicast) Information Table also contains the SSM (Source-Specific Multicast) information. This table is sorted first by VLAN ID, then by group, and then by Port. Different source addresses belong to the same group are treated as single entry.

Each page shows up to 99 entries from the MVR SFM Information Table, default being 20, selected through the "entries per page" input field. When first visited, the web page will show the first 20 entries from the beginning of the MVR SFM Information Table. The "Start from VLAN", and "Group Address" input fields allow the user to select the starting point in the MVR SFM Information Table.

To display MVR SFM Information in the web UI:

1. Click Monitor, MVR, MVR SFM Information
2. To auto-refresh the page, check the "Auto-refresh" box.
3. To click the "Refresh" to refresh an entry of the MVR Groups Information.
4. Click << or > to move to previous or next entry.

Figure 3-10.3: 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, the maximum number of IP source address for filtering (per group) is 8. 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 the 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 system log entries to the first available entry ID.

> : Updates the system log entry to the next available entry ID.

3-11 IPMC

3-11.1 IGMP Snooping

3-11.1.1 Status

This page provides IGMP Snooping status.

1. Click Monitor, IGMP Snooping, Status.
2. To auto-refresh the information check the "Auto-refresh" box.
3. Click "Refresh" to refresh the IGMP Snooping Status.
4. Click "Clear" to clear the IGMP Snooping Status.

Figure 3-11.1.1: IGMP Snooping Status

VLAN ID	Querier Version	Host Version	Querier Status	Queries Transmitted	Queries Received	V1 Reports Received	V2 Reports Received	V3 Reports Received	V2 Leaves Received
10	v3	v3	DISABLE	0	0	0	0	0	0
20	v2	v2	DISABLE	0	0	0	0	0	0

Port	Status
1	-
2	-
3	-
4	-

Parameter descriptions:

VLAN ID : The VLAN ID of the entry.

Querier Version : Working Querier Version currently.

Host Version : Working Host Version currently.

Querier Status : Shows the Querier status is "ACTIVE" or "IDLE". "DISABLE" denotes the specific interface is administratively disabled.

Queries Transmitted : The number of Transmitted Queries.

Queries Received : The number of Received Queries.

V1 Reports Received : The number of Received V1 Reports.

V2 Reports Received : The number of Received V2 Reports.

V3 Reports Received : The number of Received V3 Reports.

V2 Leaves Received : The number of Received V2 Leaves.

Router Port : 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.

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

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

Both denotes the specific port is configured or learnt to be a router port.

Port : Switch port number.

Status : Indicate whether specific port is a router port or not.

Buttons



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

Refresh: Click to manually refresh the page immediately.

Clear: Clears the counters for the selected port.

3-11.1.2 Group Information

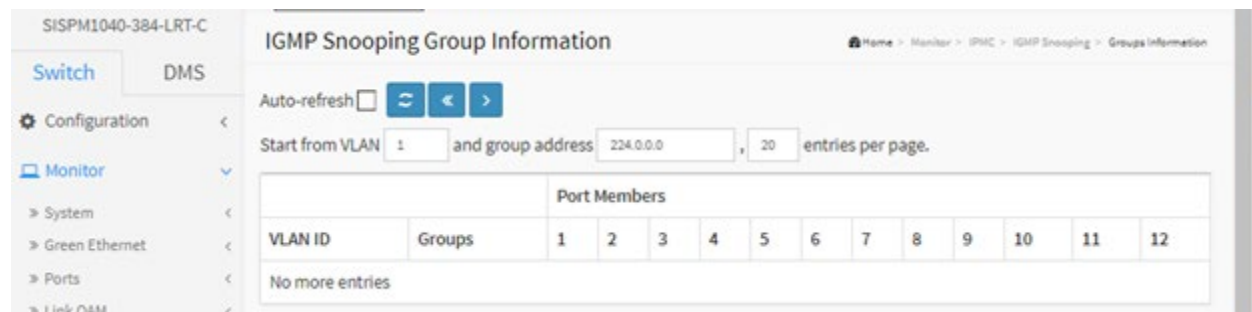
Entries in the IGMP Group Table are shown on this page. The IGMP Group Table is sorted first by VLAN ID, and then by group.

Each page shows up to 99 entries from the IGMP Group table, default being 20, selected through the "entries per page" input field. When first visited, the web page will show the first 20 entries from the beginning of the IGMP Group Table. The "Start from VLAN", and "group" input fields let you select the starting point in the IGMP Group Table.

To display IGMP Snooping Group Information in the web UI:

1. Click Monitor, IGMP Snooping, Groups Information.
2. To automatically refresh the page, check the "Auto-refresh" box.
3. Click "Refresh" to refresh the IGMP Snooping Groups Information.
4. Click << or > to move to previous or next entry.

Figure 3-11.1.2: IGMP Snooping Groups Information.



Parameter descriptions:

VLAN ID : VLAN ID of the group.

Groups : Group address of the group displayed.

Port Members : Ports under this group.

Buttons

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

Refresh: Click to 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.



3-11.1.3 IPv4 SFM Information

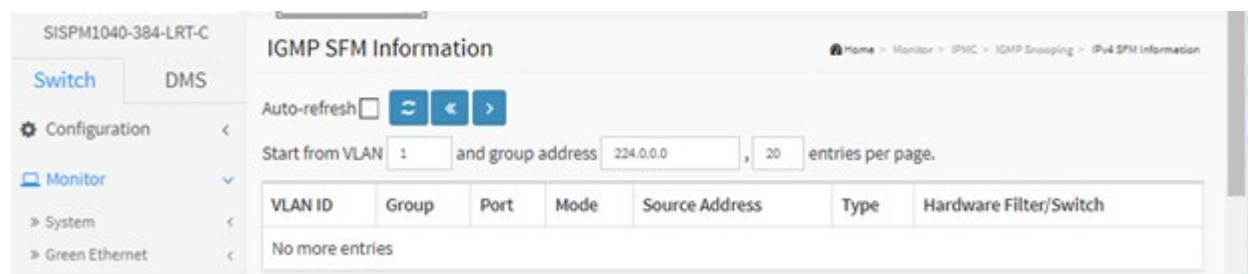
Entries in the IGMP SFM Information Table are shown on this page. The IGMP SFM (Source-Filtered Multicast) Information Table also contains the SSM (Source-Specific Multicast) information. This table is sorted first by VLAN ID, then by group, and then by Port. Different source addresses belong to the same group are treated as single entry.

Each page shows up to 99 entries from the IGMP SFM Information table, default being 20, selected through the "entries per page" input field. When first visited, the web page will show the first 20 entries from the beginning of the IGMP SFM Information Table. The "Start from VLAN", and "group address" input fields let you select the starting point in the IGMP SFM Information Table.

To display IPv4 SSM Information in the web UI:

1. Click Monitor, IPMC, IGMP Snooping, IPv4 SSM Information.
2. To automatically refresh the information, check the "Auto-refresh" button.
3. Click "Refresh" to refresh an entry of the IPv4 SFM Information.
4. Click << or > to move to previous or next entry.

Figure 3-11.1.3: IPv4 SFM Information.



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 can be handled by the 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 system log entries to the first available entry ID.

>: Updates the system log entry to the next available entry ID.

3-11.2 MLD Snooping

3-11.2.1 Status

This page displays MLD Snooping Status.

1. Click Monitor, IPMC, MLD Snooping, Status.
2. To auto-refresh the information, check the "Auto-refresh" box.
3. Click "Refresh" to refresh an entry of the MLD Snooping Status Information.
4. Click "Clear" to clear the MLD Snooping Status.

Figure 3-11.2.1: MLD Snooping Status

The screenshot shows the 'MLD Snooping Status' page. The left sidebar has 'Monitor' selected, and 'IPMC' and 'MLD Snooping' are also selected. The main content area has the title 'MLD Snooping Status' and a breadcrumb trail: Home > Monitor > IPMC > MLD Snooping > Status. There is an 'Auto-refresh' checkbox (unchecked) and two buttons (refresh and clear). Below is a 'Statistics' table with the following data:

VLAN ID	Querier Version	Host Version	Querier Status	Queries Transmitted	Queries Received	V1 Reports Received	V2 Reports Received	V1 Leaves Received
10	v2	v2	ACTIVE	3	0	0	0	0

Below the statistics is a 'Router Port' table with the following data:

Port	Status
1	-
2	Both
3	Both
4	Both
5	-
6	-

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". Shows "DISABLE" if the specific interface is administratively disabled.

Queries Transmitted : The number of Transmitted Queries.

Queries Received : The number of Received Queries.

V1 Reports Received : The number of Received V1 Reports.

V2 Reports Received : The number of Received V2 Reports.

V1 Leaves Received : The number of Received V1 Leaves.

Router Port : Display which ports act as router ports. A router port is a port on the Ethernet switch that leads towards the Layer 3 multicast device or MLD querier.

Port : The Switch port number.

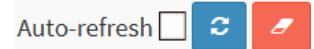
Status : Indicate whether the specific port is a router port (Static, Dynamic, or Both):

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

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

Both denotes the specific port is configured or learnt to be a router port.

Buttons



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

Clear: Clears the counters for the selected port.

Refresh: Click to manually refresh the page immediately.

3-11.2.2 Group Information

Entries in the MLD Group Table are shown on this page. The MLD Group Table is sorted first by VLAN ID, and then by group.

Each page shows up to 99 entries from the MLD Group table, default being 20, selected through the "entries per page" input field. When first visited, the web page will show the first 20 entries from the beginning of the MLD Group Table.

The "Start from VLAN", and "group" input fields allow the user to select the starting point in the MLD Group Table. Clicking the << button will update the displayed table starting from that or the closest next MLD Group Table match.

Web Interface

To display MLD Snooping Group information in the web UI:

1. Click Monitor, IPMC, MLD Snooping, Group Information.
2. Select the "Start from VLAN", "and group address", and "entries per page".
3. To automatically refresh the information, check the "Auto-refresh" box.
4. Click "Refresh" to refresh an entry of the MLD Snooping Group Information.

Figure 3-11.2.2: 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.

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.



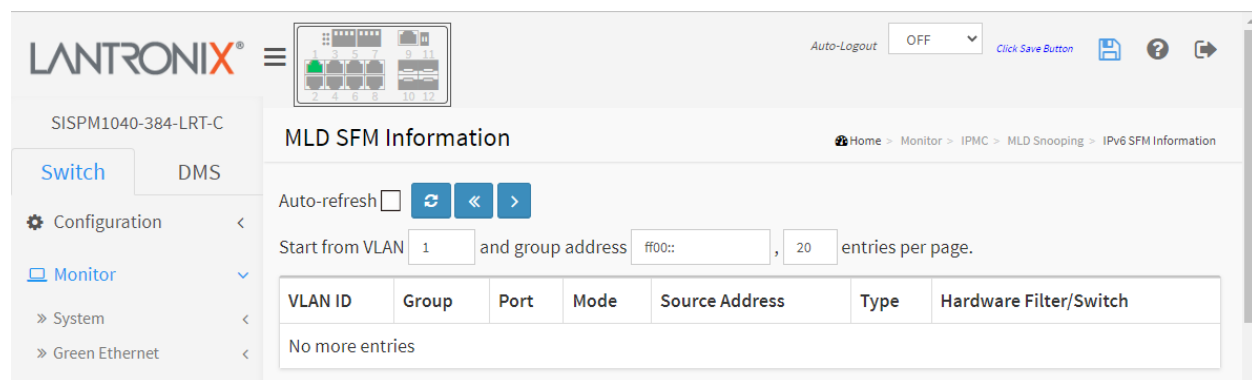
3-11.2.3 IPv6 SFM Information

Entries in the MLD SFM Information Table are shown on this page. The MLD SFM (Source-Filtered Multicast) Information Table also contains the SSM (Source-Specific Multicast) information. This table is sorted first by VLAN ID, then by group, and then by Port. Different source addresses belong to the same group are treated as single entry.

To display MLDv2 IPv6 SSM Information in the web UI:

1. Click Monitor, IPMC, MLD Snooping, IPv6 SFM Information.
2. To automatically refresh the information, check the "Auto-refresh" box.
3. Click Refresh to refresh an entry of the MLDv2 IPv6 SSM Information.
4. Click << or > to move to previous or next entry.

Figure 3-11.2.3: IPv6 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 IPv6 address could be handled by chip or not.

Buttons



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

Refresh: Click to manually refresh the page immediately.

<<: Updates the system log entries to the first available entry ID.

> : Updates the system log entry to the next available entry ID.

3-12 LLDP

3-12.1 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. **Note:** If your network has no devices that support LLDP, then the table displays “No LLDP neighbor information found”.

To show LLDP neighbors via the Web UI:

1. Click Monitor, LLDP, Neighbors.
2. Click on the IP address for a device to display its startup page.
3. Click Refresh to manually update or click Auto-refresh to automatically update the web page.

Figure 3-12.1: LLDP Neighbor Information

Local Port	Chassis ID	Port ID	Port Description	System Name	System Capabilities	System Description	Management Address
Port 1	00-C0-F2-49-3D-4F	8	GigabitEthernet 1/8	SISPM1040-362-LRT	Bridge(+)	Managed Hardened PoE+ Switch, (4) 10/100/1000Base-T PoE+ Ports + (2) 10/100/1000Base-T Ports + (2) 100/1000Base-X SFP Ports	192.168.1.77 (IPv4)
Port 3	AC-CC-8E-AD-F8-2A	AC-CC-8E-AD-F8-2A	eth0	axis-acc8eadf82a	Bridge(-), WLAN Access Point(-), Router(-), Station Only(+)	AXIS M3106-LVE Mk II Network Camera 8.30.1.1	192.168.0.90 (IPv4)
Port 8	00-C0-F2-49-3D-4F	1	GigabitEthernet 1/1	SISPM1040-362-LRT	Bridge(+)	Managed Hardened PoE+ Switch, (4) 10/100/1000Base-T PoE+ Ports + (2) 10/100/1000Base-T Ports + (2) 100/1000Base-X SFP Ports	192.168.1.77 (IPv4)

Parameter descriptions:

Local Port : The port on which the LLDP frame was received (e.g., Port 1, Port 2, etc.).

Chassis ID : The Chassis ID is the identification of the neighbor’s LLDP frames (MAC ID).

Port ID : The Remote Port ID is the identification of the neighbor port (e.g., Port Number or MAC Address).

Port Description : Port Description is the port description advertised by the neighbor device (e.g., GigabitEthernet 1/4 or eth0).

System Name : System Name is the name advertised by the neighbor device (e.g., SISPM1040-384-LRT-C or axis-acc8eadf82a).

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

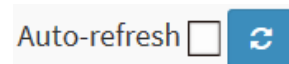
1. Other
2. Repeater
3. Bridge
4. WLAN Access Point
5. Router
6. Telephone
7. DOCSIS cable device
8. Station only
9. Reserved

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

System Description: System Description is the description advertised by the neighbor device.

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 on a linked address to display its config page (see below).

Buttons



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

Refresh: Click to manually refresh the page immediately.

LLDP Remote Device Summary Example

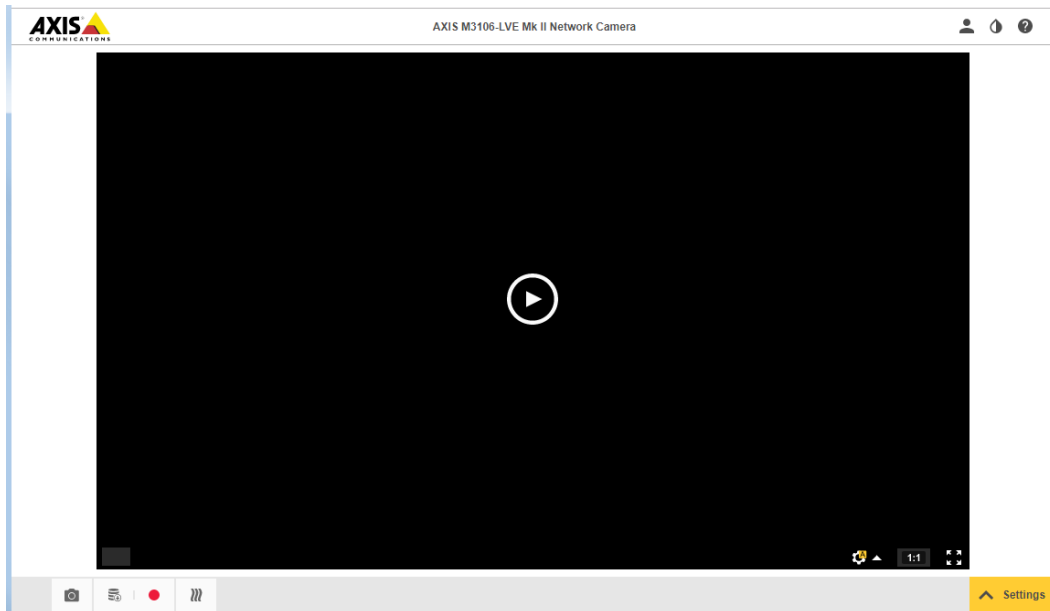
You can click on a linked IP address in the Management Address column to display its config page.

If you click on the IP address for the SISPM1040-384-LRT-C switch, the Monitor > System > Information page displays (the startup page).

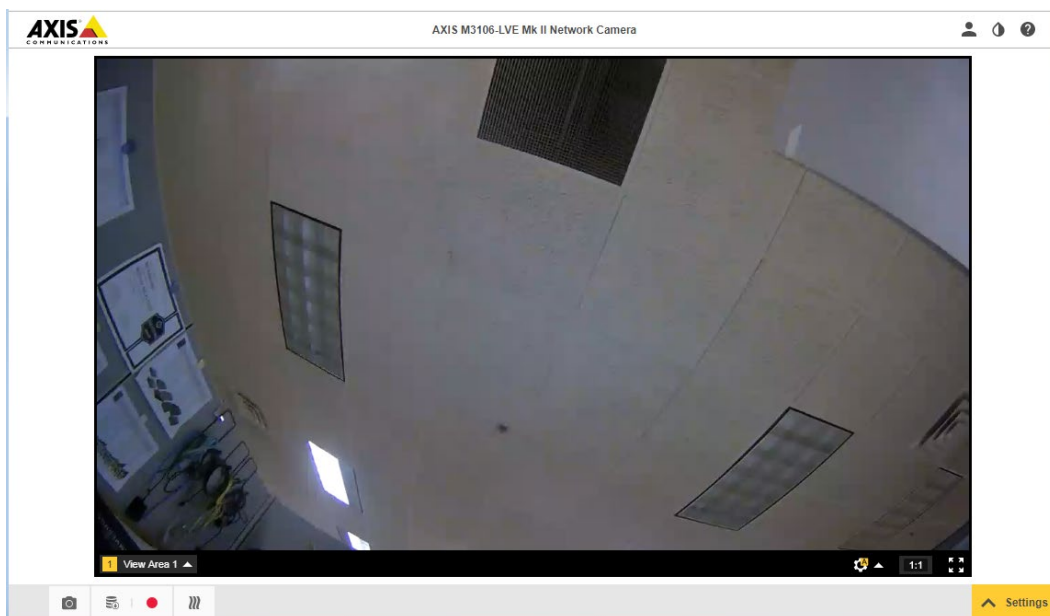
The screenshot shows the 'LLDP Neighbor Information' page with an 'Auto-refresh' checkbox and a refresh icon. Below is the 'LLDP Remote Device Summary' table:

Local Port	Chassis ID	Port ID	Port Description	System Name	System Capabilities	System Description	Management Address
Port 3	00-C0-F2-49-3D-4F	8	GigabitEthernet 1/8	SISPM1040-362-LRT	Bridge(+)	Managed Hardened PoE+ Switch, (4) 10/100/1000Base-T PoE+ Ports + (2) 10/100/1000Base-T Ports + (2) 100/1000Base-X SFP Ports	192.168.1.77 (IPv4)
Port 8	00-C0-F2-49-3D-4F	3	GigabitEthernet 1/3	SISPM1040-362-LRT	Bridge(+)	Managed Hardened PoE+ Switch, (4) 10/100/1000Base-T PoE+ Ports + (2) 10/100/1000Base-T Ports + (2) 100/1000Base-X SFP Ports	192.168.1.77 (IPv4)

In the Management Address column, if you click on the IP address of a discovered neighbor device such as a camera, that device's startup page displays.



You can now perform normal operations for the device.



3-12.2 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. Note: If your network has no devices that support LLDP-MED, the table displays the message "No LLDP-MED neighbor information found".

To show LLDP-MED neighbor:

1. Click Monitor, LLDP, LLDP-MED Neighbors.
2. Click Refresh for a manual web page update.
3. Check Auto-refresh to automatically update the web page.

Figure 3-12.2: LLDP-MED Neighbor Information

The screenshot shows the Lantronix web interface for LLDP-MED Neighbor Information. The page title is "LLDP-MED Neighbor Information" and the breadcrumb is "Home > Monitor > LLDP > LLDP-MED Neighbors". There is an "Auto-refresh" checkbox and a refresh button. The table below shows the neighbor information for Port 1.

Port 1			
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:

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 (e.g., Endpoint Class I).

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

1. LAN Switch/Router
2. IEEE 802.1 Bridge
3. IEEE 802.3 Repeater (included for historical reasons)
4. IEEE 802.11 Wireless Access Point
5. Any device that supports the IEEE 802.1AB and MED extensions defined by TIA-1057 and can relay IEEE 802 frames via any method.

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

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

Each LLDP-MED Endpoint Device Class is defined to build 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 : LLDP-MED Capabilities describes the neighborhood unit's LLDP-MED capabilities. The possible capabilities are:

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

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

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

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

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

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

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

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

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

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

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

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

Defined: The network policy is defined.

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

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

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

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

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

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

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

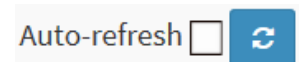
Auto-negotiation status : identifies if auto-negotiation is currently enabled at the link partner.

If Auto-negotiation is supported and Auto-negotiation status is disabled, the 802.3 PMD operating mode will be determined the operational MAU type field value rather than by auto-negotiation.

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

MAU Type : Displays the MAU (Medium Attachment Unit) Type or "Invalid MAU Type".

Buttons



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

Refresh: Click to manually refresh the page immediately.

Example:

The screenshot displays the Lantronix web management interface. At the top left is the Lantronix logo and a navigation menu. The main header shows the device model 'SISPM1040-384-LRT-C' and the page title 'LLDP-MED Neighbor Information'. A breadcrumb trail indicates the path: Home > Monitor > LLDP > LLDP-MED Neighbors. On the left, there is a sidebar with 'Switch' and 'DMS' tabs, and a menu with 'Configuration', 'Monitor', 'System', and 'Green Ethernet' options. The main content area features an 'Auto-refresh' checkbox and a refresh button. Below this is a table for 'Port 1' with columns for 'Device Type' and 'Capabilities'.

Port 1	
Device Type	Capabilities
Network Connectivity	LLDP-MED Capabilities, Extended Power via MDI - PSE

3-12.3 PoE

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

1. Click Monitor, LLDP, PoE.
2. View the displayed Power over Ethernet information.
3. Click Auto-refresh to automatically update the web page.

Figure 3-12.3: LLDP Neighbor Power Over Ethernet Information

Local Port	Power Type	Power Source	Power Priority	Maximum Power
9	PSE Device	Primary Power Supply	Low	0 [W]

Parameter descriptions:

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 Source or its Backup Power Source. If it is unknown whether the PSE device is using its Primary Power Source or its Backup Power Source it is indicated as "Unknown".

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

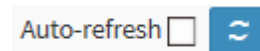
If it is unknown what power supply the PD device is using it is indicated as "Unknown".

Power Priority : Power Priority represents the priority of the PD device, or the power priority associated with the PSE type device's 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 manually refresh the page immediately.

3-12.4 EEE

This page provides an overview of EEE (Energy Efficient Ethernet) 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 turn off to save power, need time to boot up before sending traffic over the link. This time is called "wakeup time". To achieve minimal latency, devices can use LLDP to exchange information about their respective TX and RX "wakeup time " as a way to agree on the minimum wakeup time they need. **Note:** If your network has no devices enabled for EEE, then the table displays "No LLDP EEE information found".

To show LLDP EEE neighbors:

1. Click Monitor, LLDP, EEE.
2. View the discovered EEE devices.
3. Click Refresh to manually update the web page.
4. Click Auto-refresh to automatically update the web page.

Figure 3-12.4: LLDP Neighbors EEE Information

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

Parameter descriptions:

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

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

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

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

Echo Tx Tw : The link partner's Echo Tx Tw value. The respective echo values shall 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).

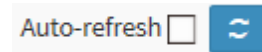
Resolved Rx Tw : The resolved Rx Tw for this link. **Note:** NOT the link partner. The resolved value that is the actual "tx wakeup time" used for this link (based on EEE information exchanged via LLDP).

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 manually refresh the page immediately.

3-12.5 Port Statistics

This page displays two types of counters. Global counters are counters that refer to the whole switch, while Local counters refer to per-port counters. To display LLDP Statistics:

1. Click Monitor, LLDP, Port Statistics.
2. View the LLDP counters and statistics.
3. Click Refresh to manually update the web page immediately.
4. Click Auto-refresh to automatically update the web page.
5. Click Clear to clear all counters.

Figure 3-12.5: LLDP Port Statistics

The screenshot shows the Lantronix web interface for device SISPM1040-384-LRT-C. The left navigation menu is expanded to 'LLDP' > 'Port Statistics'. The main content area displays 'LLDP Counters' with an 'Auto-refresh' checkbox and two buttons (refresh and clear). Below this are two tables:

LLDP Global Counters

Neighbor entries were last changed	2011-01-01T00:04:23+00:00 (344938 secs. ago)
Total Neighbors Entries Added	1
Total Neighbors Entries Deleted	0
Total Neighbors Entries Dropped	0
Total Neighbors Entries Aged Out	0

LLDP Statistics Local Counters

Local Port	Tx Frames	Rx Frames	Rx Errors	Frames Discarded	TLVs Discarded	TLVs Unrecognized	Org. Discarded	Age-Outs
1	15741	368	0	0	0	0	0	0
2	0	0	0	0	0	0	0	0
3	0	0	0	0	0	0	0	0
4	0	0	0	0	0	0	0	0
5	0	0	0	0	0	0	0	0
6	0	0	0	0	0	0	0	0

Parameter descriptions:

LLDP Global Counters

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

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

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

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

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

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

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

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

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

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

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

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

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

Org. Discarded : If an LLDP frame is received with an organizationally TLV, but the TLV is not supported, then the TLV is discarded and counted here.

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

Buttons



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

Refresh: Click to manually refresh the page immediately.

Clear: Clears the local counters. Note that All counters (including global counters) are cleared on reboot.

3-13 Ethernet Services

3-13.1 EVC Statistics

This page provides NNI port traffic statistics for the selected EVC, and shows counters for UNI ports of ECEs mapping to the EVC.

To show Ethernet Statistics:

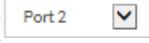
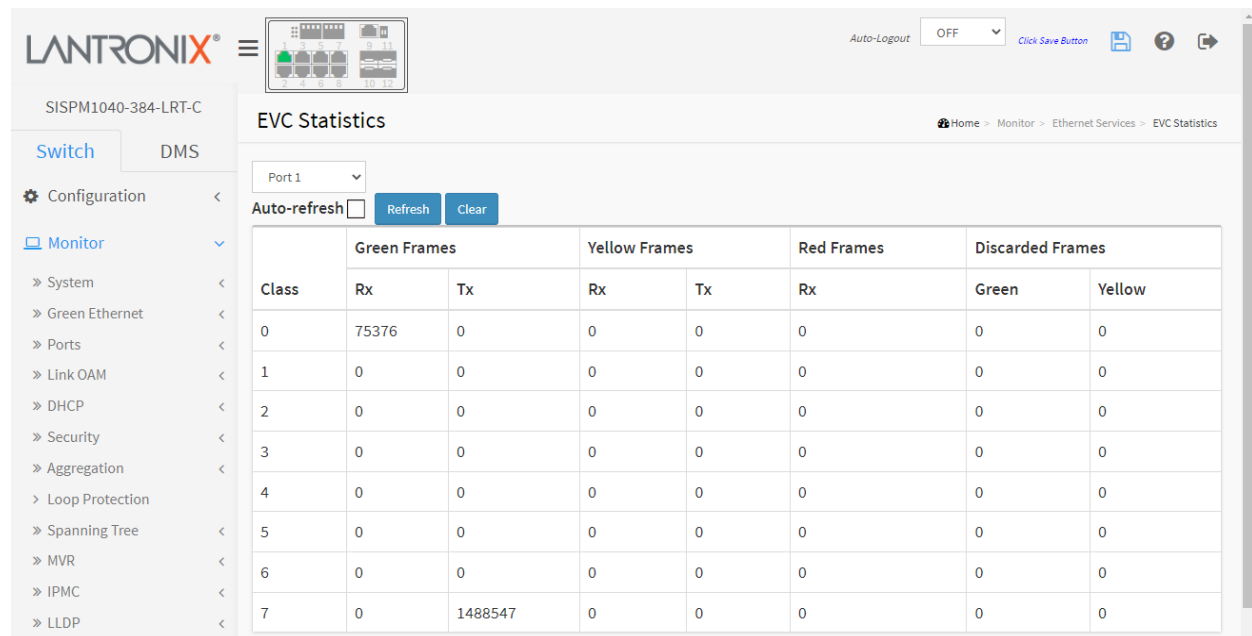
1. Click Monitor, Ethernet Services, EVC Statistics.
2. Select a port to monitor at the port select dropdown ().
3. Click Refresh to manually update the web page.
4. Click Auto-refresh to automatically update the web page.
5. Click Clear to clear all counters.

Figure 3-13.1: Ethernet Statistics



The screenshot shows the Lantronix web interface for EVC Statistics. The page title is 'EVC Statistics' and the breadcrumb is 'Home > Monitor > Ethernet Services > EVC Statistics'. The interface includes a navigation menu on the left with 'Monitor' selected. The main content area shows a dropdown menu for 'Port 1', an 'Auto-refresh' checkbox, and 'Refresh' and 'Clear' buttons. Below these is a table with the following data:

Class	Green Frames		Yellow Frames		Red Frames	Discarded Frames	
	Rx	Tx	Rx	Tx	Rx	Green	Yellow
0	75376	0	0	0	0	0	0
1	0	0	0	0	0	0	0
2	0	0	0	0	0	0	0
3	0	0	0	0	0	0	0
4	0	0	0	0	0	0	0
5	0	0	0	0	0	0	0
6	0	0	0	0	0	0	0
7	0	1488547	0	0	0	0	0

Parameter descriptions:

Class : The traffic class for the EVC (0-7).

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 in the green color.

Yellow Discarded : The number of discarded in the yellow color.

Buttons

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

Refresh: Click to manually refresh the page immediately.

Clear: Clears the counters for the selected port.



: Port select box to select the port displayed on a page.

3-14 PTP

This page lets you view current PTP clock settings.

1. Click Monitor, PTP.
2. Click Refresh to manually update the web page.
3. Click Auto-refresh to automatically update the web page.
4. Click Clear to clear all counters.
5. You can click a linked PTP clock instance number to display its PTP Clock Configuration webpage (see “PTP Clock's Configuration” on page 382).

Figure 3-14: Monitor > PTP

The screenshot shows the Lantronix web interface for device SISPM1040-384-LRT-C. The left sidebar contains a navigation menu with 'Monitor' selected. The main content area is titled 'PTP External Clock Mode' and includes a 'Refresh' button. Below this is a table for 'PTP External Clock Mode' with the following data:

Parameter	Value
One_PPS_Mode	Input
External Enable	False
Adjust Method	LTC frequency
Clock Frequency	100000

Below the table is the 'PTP Clock Configuration' section, which includes an 'Auto-refresh' checkbox and a 'Refresh' button. A table titled 'Port List' shows the configuration for four PTP clock instances across 12 ports:

Instance	Device Type	Port List											
		1	2	3	4	5	6	7	8	9	10	11	12
0	Ord-Bound		✓	✓	✓	✓	✓		✓	✓	✓		
1	P2pTransp												
2	Mastronly												
3	BC-frontend												

Parameter descriptions:

PTP External Clock Mode

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 range of values are 1 - 25000000 (1 - 25MHz).

PTP Clock Configuration

Inst : Indicates the Instance of a particular Clock Instance [0..3]. Click on the Clock Instance number to monitor the Clock details.

ClkDom : Indicates the Clock domain used by the Instance of a particular Clock Instance [0..3].

Device Type : Indicates the Type of the Clock Instance. 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 manually refresh the page immediately.

PTP Clock's Configuration

When you click a linked PTP clock instance number its PTP Clock Configuration displays:

The screenshot displays the 'PTP Clock's Configuration' page for instance 0. The interface includes a navigation menu on the left and a main content area with several data sections:

- Local Clock Current Time:** Shows PTP Time as 1870-03-01T09:59:46+00:00 042,437,832. Clock Adjustment Method is Internal Timer. Ports Monitor Page is linked.
- Clock Default Dataset:** A table with columns: Clock ID, Device Type, 2 Step Flag, Ports, Clock Identity, Dom, Clock Quality, Prio, Prio2, Protocol, One-Way, VLAN Tag Enable, VID, PCP, DSCP. Row 0: Ord-Bound, False, S2, 00:00:00:0e:49:45:81, 0, C1:006 Ac:Unknown Va:85535, S28, S28, Ethernet, False, False, 1, 0, 0.
- Clock Current Dataset:** A table with columns: stepIn, Offset From Master, Mean Path Delay, Slave Port, Slave State, Holdover(ppb). Row 0: 0, 0.000,000,000, 0.000,000,000, 0, FREERUN, N.A.
- Clock Parent Dataset:** A table with columns: Parent Port ID, Port, PStat, Var, ChangeRate, GrandMaster Identity, GrandMaster Clock Quality, Prio1, Prio2. Row 0: 00:00:00:0e:49:45:81, 0, False, 0, 0, 00:00:00:0e:49:45:81, C1:006 Ac:Unknown Va:85535, 0, S28.
- Clock Time Properties Dataset:** A table with columns: UtcOffset, Valid, leap32, leap61, Time Trac, Freq Trac, PTP Time Scale, Time Source. Row 0: 0, False, False, False, False, False, True, S80.
- Servo Parameters:** A table with columns: Display, P-enable, I-enable, D-enable, P-constant, I-constant, D-constant. Row 0: False, True, True, True, 1, 80, 40.
- Filter Parameters:** A table with columns: Filter Type, DelayFilter, Period, Dist. Row 0: Basic, 8, 1, 2.
- Unicast Slave Configuration:** A table with columns: Index, Duration, IP_Address, Grant, CommState. Rows 0-4: 0-4, 100, 0.0.0.0, 0, IDLE.

Parameter descriptions:

Local Clock Current time

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 to monitor 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 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
- ip4multi PTP over IPv4 multicast
- ip4uni 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 must 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 : 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

Slave Port : Shows which port is in slave mode. The value is 0 if no ports are in slave mode.

Slave State : Shows 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 stabilization period is 60 sec as default, it can be changed from the CLI interface.

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 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.

Note: These 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:

clockAdjustment =

OffsetFromMaster/ P constant +

Integral(OffsetFromMaster)/ I constant +

Differential OffsetFromMaster)/ D constant

Display : If true then Offset From Master, MeanPathDelay and clockAdjustment are logged in debug.

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 manually refresh the page immediately.

PTP Clock's Port Data Set Configuration

Click the linked [Ports Monitor](#) text to display the PTP Clock's Port Data Set Configuration page. The port data set is defined in the IEEE 1588 Standard.

The screenshot shows the 'PTP Clock's Port Data Set Configuration' page in the Lantronix web interface. The page includes a navigation menu on the left with options like 'Switch', 'DMS', 'Configuration', 'Monitor', 'System', 'Green Ethernet', 'Ports', 'Link OAM', 'DHCP', 'Security', 'Aggregation', 'Loop Protection', 'Spanning Tree', 'MVR', and 'IPMC'. The main content area features an 'Auto-refresh' checkbox (unchecked) and a 'Refresh' button. Below this is a table with the following data:

Port	Stat	MDR	PeerMeanPathDel	Anv	ATo	Syv	Dlm	MPR	Delay Asymmetry	Ingress Latency	Egress Latency	Version
2	dsbl	3	0.000,000,000	0	3	0	e2e	0	0.000,000,000	0.000,000,000	0.000,000,000	2
3	dsbl	3	0.000,000,000	0	3	0	e2e	0	0.000,000,000	0.000,000,000	0.000,000,000	2
4	dsbl	3	0.000,000,000	0	3	0	e2e	0	0.000,000,000	0.000,000,000	0.000,000,000	2
5	dsbl	3	0.000,000,000	0	3	0	e2e	0	0.000,000,000	0.000,000,000	0.000,000,000	2
6	dsbl	3	0.000,000,000	0	3	0	e2e	0	0.000,000,000	0.000,000,000	0.000,000,000	2
8	dsbl	3	0.000,000,000	0	3	0	e2e	0	0.000,000,000	0.000,000,000	0.000,000,000	2
9	dsbl	3	0.000,000,000	0	3	0	e2e	0	0.000,000,000	0.000,000,000	0.000,000,000	2
10	dsbl	3	0.000,000,000	0	3	0	e2e	0	0.000,000,000	0.000,000,000	0.000,000,000	2

Parameter descriptions:

Port : Port number [1..max port no]

Stat : Current state of the port (e.g., mstr, slav, dsbl).

MDR : log Min Delay Req Interval: The delay request interval announced by the master.

PeerMeanPathDel : 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., $MPR = 0 \Rightarrow 1 \text{ Delay_Req pr sec}$, independent of the Sync rate).

Delay Asymmetry : The transmission delay asymmetry for a link. See IEEE 1588 Section 7.4.2 Communication path asymmetry.

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.

Version : The current implementation only supports PTP version 2.

3-15 PoE

This page lets you view the current status for all PoE ports.

1. Click Monitor, PoE.
2. Check "Auto-refresh".
3. Click "Refresh" to refresh the page.

Figure 3-15: PoE Status

The screenshot shows the 'Power Over Ethernet Status' page in the Lantronix web interface. The page includes a navigation menu on the left with 'Monitor' selected. The main content area shows a table of PoE port status. The 'Auto-refresh' checkbox is checked, and a refresh button is present. The table data is as follows:

Local Port	PD class	Power Requested	Power Allocated	Power Used	Current Used	Priority	Port Status
1	-	0 [W]	0 [W]	0 [W]	0 [mA]	Critical	No PD detected
2	2	40 [W]	40 [W]	1.9 [W]	36 [mA]	High	PoE turned ON
3	2	40 [W]	40 [W]	1.9 [W]	36 [mA]	High	PoE turned ON
4	-	0 [W]	0 [W]	0 [W]	0 [mA]	High	No PD detected
5	-	0 [W]	0 [W]	0 [W]	0 [mA]	Low	No PD detected
6	2	40 [W]	40 [W]	2 [W]	38 [mA]	Low	PoE turned ON
7	-	0 [W]	0 [W]	0 [W]	0 [mA]	Low	No PD detected
8	-	0 [W]	0 [W]	0 [W]	0 [mA]	Low	No PD detected
Total		120 [W]	120 [W]	5.8 [W]	110 [mA]		

Parameter descriptions:

Local Port : 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 shows the PDs class. Five Classes are defined:

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

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

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

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

Current Used : The Power Used shows how much current the PD currently is using.

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

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

PoE turned ON : PD is 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.

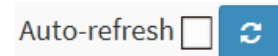
PoE turned OFF - PD overload - The PD has requested or used more power than the port can deliver and is powered down.

PoE turned OFF - PD is off.

Invalid PD - PD detected but is not working correctly.

Total: The bottom row of the table provides a sum of the Power Requested, Power Allocated, Power Used, and Current Used columns.

Buttons



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

Refresh: Click to manually refresh the page immediately.

3-16 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.

Each page shows up to 999 entries from the MAC 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 MAC Table. The first displayed entry will be the one with the lowest VLAN ID and the lowest MAC address found in the MAC Table.

The "Start from MAC address" and "VLAN" input fields let you select the starting point in the MAC Table. Clicking the "Refresh" button will update the displayed table starting from that or the next closest MAC Table match.

Web Interface

To display MAC Address Table in the web UI:

1. Click Monitor, MAC Table.
2. Specify the Start from VLAN and MAC Address.
3. View the MAC Address Table parameters.

Figure 3-16: MAC Address Table

The screenshot shows the Lantronix web interface for the device SISPM1040-384-LRT-C. The page title is "MAC Address Table". The interface includes a navigation menu on the left with "Monitor" selected. The main content area shows the "MAC Address Table" configuration and data.

Configuration options:

- Auto-refresh:
- Start from VLAN: 1
- and MAC address: 00-00-00-00-00-00
- entries per page: 20

Table Data:

Type	VLAN	MAC Address	CPU	Port Members													
				1	2	3	4	5	6	7	8	9	10	11	12		
Static	1	00-C0-F2-49-BE-22	✓														
Static	1	01-00-0C-CC-CC-CC	✓														
Static	1	33-33-00-00-00-01	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Static	1	33-33-00-00-00-02	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Static	1	33-33-FF-49-BE-22	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Static	1	FF-FF-FF-FF-FF-FF	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓

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: Refreshes the displayed table starting from the "Start from MAC address" and "VLAN" input fields.

Clear: Flushes all dynamic entries.

<<: Updates the table starting from the first entry in the MAC Table, i.e. the entry with the lowest VLAN ID and MAC address.

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

NOTE:

00-40-C7-73-01-29 : your switch MAC address (for IPv4)

33-33-00-00-00-01 : Destination MAC (for IPv6 Router Advertisement) (reference IPv6 RA.JPG)

33-33-00-00-00-02 : Destination MAC (for IPv6 Router Solicitation) (reference IPv6 RS.JPG)

33-33-FF-73-01-29 : Destination MAC (for IPv6 Neighbor Solicitation) (reference IPv6 DAD.JPG)

33-33-FF-A8-01-01: your switch MAC address (for IPv6 global IP)

FF-FF-FF-FF-FF-FF: for Broadcast.

3-17 VLANs

3-17.1 Membership

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

Each 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 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 " > " will use the last entry of the currently displayed VLAN entry as a basis for the next lookup. When the end is reached the text "No more entries" is shown in the displayed table. Use the "<<" button to start over.

To monitor VLAN membership status in the web UI:

1. Click Monitor, VLANs, Membership.
2. At the dropdown select which VLAN users to display.
3. Make a 'Start from VLAN' and an 'entries per page' selection.

Figure 3-17.1: VLAN Membership Status for Combined users

The screenshot shows the 'VLAN Membership Status for Combined users' page. The interface includes a navigation menu on the left with options like 'Switch', 'DMS', 'Configuration', 'Monitor', 'System', 'Green Ethernet', 'Ports', 'Link OAM', and 'DHCP'. The main content area features a table with the following data:

VLAN ID	Port Members											
	1	2	3	4	5	6	7	8	9	10	11	12
1	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
100	✓		✓									

VLAN User : Various internal software modules may use VLAN services to configure VLAN memberships on the fly. The drop-down list on the right allows for selecting between showing VLAN memberships as configured by an administrator (Admin) or as configured by one of these internal software modules. The "Combined" entry will show a combination of the administrator and internal software modules configuration, and basically reflects what is actually configured in hardware.

These VLAN user types are supported:

Combined: (CLI/Web/SNMP) these are referred to as static.

Admin: Select to display only Admin VLANs.

Forbidden: Select to display only Forbidden VLANs. .

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

GVRP: Select to display only GVRP VLANs. GVRP (Generic VLAN Registration Protocol or Generic VLAN Registration Protocol) is a protocol that facilitates control of VLANs within a larger network. GVRP conforms to the IEEE 802.1Q specification, which defines a method of tagging frames with VLAN configuration data.

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 : Select to display only MEP (Maintenance entity End Point VLANs).

EVC : Select to display only Ethernet Virtual Circuit VLANs.

RMirror: Select to display only Remote Mirroring VLANs.



DMS : Select to display only Device Management System (DMS) VLANs.



MRP: Select to display only MRP (Media Redundancy Protocol) VLANs.

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

Port Members : A row of check boxes for each port is displayed for each VLAN ID.

 If a port is included in a VLAN, an image  will be displayed.

 If a port is included in a Forbidden port list, an image  will be displayed.

 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 shall show the current VLAN port members for all VLANs configured by a selected VLAN User (selection shall be allowed by a Combo Box). When ALL VLAN Users are selected, it shows this information for all the VLAN Users, and this is by default. VLAN membership allows the frames classified to the VLAN ID to be forwarded on the respective VLAN member ports.

Buttons

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

Auto-refresh



Combined 

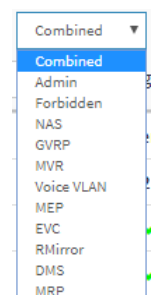
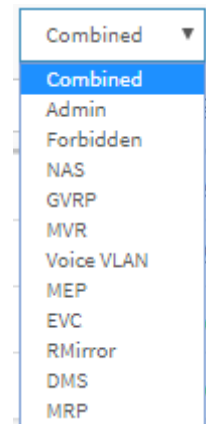
Refresh: Click to manually refresh the page immediately.

<< : Last page.

> : Next page.



: Select VLAN Users from this drop down list.



3-17.2 Port

The Port Status function gathers the information of all VLAN status and reports it for the selected user (Combined, Admin, NAS, GVRP, MVR, Voice VLAN, MSTP, ERPS, MEP, EVC, VCL, RMirror, DMS, MRP). To display VLAN Port Status in the web UI:

1. Click Monitor, VLANs, Ports.
2. At the dropdown, select the User (Combined, Admin, NAS, GVRP, MVR, Voice VLAN, MSTP, ERPS, etc.).
3. View the Port Status information.

Figure 3-17.2: VLAN Port Status for Combined users

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	Untag 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	Untag 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

Parameter descriptions:

VLAN Users: 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.

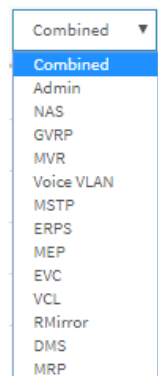
These VLAN user types are supported:

Combined: (CLI/Web/SNMP) these are referred to as static. The "Combined" entry shows a combination of the administrator and internal software modules configuration, and basically reflects what is actually configured in hardware.

Admin: Show VLAN memberships as configured by an administrator (Admin).

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

GVRP: Show VLAN memberships configured by GARP VLAN Registration Protocol.



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 : Show VLAN memberships as configured by MSTP. The Multiple Spanning Tree Protocol provides for multiple spanning tree instances, while ensuring RSTP and STP compatibility.

ERPS : Show VLAN memberships as configured by ERPS. Ethernet Ring Protection Switching per ITU/T G.8032 provides fast protection and recovery switching for Ethernet traffic in a ring topology while also ensuring that the Ethernet layer remains loop-free.

MEP : Show VLAN memberships as configured by MEP. Maintenance Entity Endpoint and is an endpoint in a Maintenance Entity Group (ITU-T Y.1731).

EVC : Show VLAN memberships as configured by Ethernet Virtual Circuit. An EVC is an association of two or more UNIs.

VCL : Show VLAN memberships as configured by VLAN Control List.

RMirror : Show VLAN memberships as configured by Mirror.

DMS : Show VLAN memberships as configured by Device Management System.

MRP : Show VLAN memberships configured by Media Redundancy Protocol.

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

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

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

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

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

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

Untagged VLAN ID : Shows UVID (untagged VLAN ID). Port's UVID determines the packet's behavior at the egress side.

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 manually refresh the page immediately.



: Select VLAN Users from this drop down list.

Messages: *No data exists for the selected user.*

3-18 MRP

3-18.1 Media Redundancy Protocol Status

This page shows MRP Domain Profile, Events, and Statistics. See [Appendix C: MRP Pre-Requisites and Application Examples](#) on page 477 for more MRP information.

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 Domain1 and Domain2.
- Domain Events:** A table listing recent events, including 'Ring Open' for Domain1.
- Domain Statistics:** A table showing the total number of frames transmitted and received for each domain.

Name	Oper. Role	Ring State	Primary		Secondary	
			Port	State	Port	State
Domain1	Manager	Open	2	Forwarding	3	Forwarding
Domain2	Client	-	4	Forwarding	5	Not connected

Timestamp	Name	Event	Appear
2011-01-01T00:00:09+00:00	Domain1	Ring Open	True
2011-01-01T01:17:47+00:00	Domain1	Ring Open	False
2011-01-01T01:17:47+00:00	Domain1	Ring Open	True

Name	MRP Transmitted Frames	MRP Received Frames			Round Trip Delay, ms	
	Total	Total	Error	Unrecognized	Min	Max
Domain1	584474	0	0	0	0	0
Domain2	0	0	0	0	0	0

Domain Profile

Name: The logical name for the MRP domain to ease the management of MRP domains.

Oper. Role: The operational role of an MRP entity per domain (Manager or Client).

Ring State: Ring status of the MRP entity (e.g., Open or – or Undefined).

Primary Port / State: The ifIndex of the layer 2 interface which is used as ring port 1.

Secondary Port / State: The ifIndex of the layer 2 interface which is used as ring port 2.

Domain Events

Timestamp: The value of sysUpTime at the time of the logged event.

Name: The logical name of the MRP domain.

Event: Event type (e.g., Ring Open).

Appear: Event appeared (True or False).

Domain Statistics

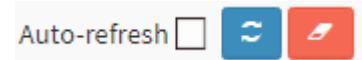
Name: The logical name of the MRP domain.

MRP Transmitted Frames: The total transmitted frames.

MRP Received Frames: The Total received frames, Error frames, and Unrecognized frames.

Round Trip Delay, ms: Round-Trip-Delay (in milliseconds) which was measured since startup. Minimum and maximum values.

Buttons



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

Refresh: Click to manually refresh the page immediately.

Clear: Click to clear (zero out) the page statistics.

3-19 VCL

3-19.1 MAC-based VLAN

This page shows MAC-based VLAN entries configured by various MAC-based VLAN users. Currently these VLAN User types are supported:

CLI/Web/SNMP: These are referred to as static.

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

DMS: Show the Device Management System type users.

Combined: Show all users.

To display MAC-based VLAN membership status in the web UI:

1. Click Monitor, VCL, MAC-based VLAN.
2. Specify the user (e.g., Static, NAS, Combined).
3. View the displayed information.

Figure 3-19.1: MAC-based VLAN Membership Status for User Static

The screenshot shows the Lantronix web interface for a device labeled 'SISPM1040-384-LRT-C'. The page title is 'MAC-based VLAN Membership Status for User Static'. There is an 'Auto-refresh' checkbox and a refresh button. A dropdown menu is set to 'Static'. Below this is a table with columns for 'MAC Address', 'VLAN ID', and 'Port Members' (1-12). The table content is 'No data exists for the user'.

Parameter descriptions:

MAC Address : Indicates the MAC address.

VLAN ID : Indicates the VLAN ID.

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

Buttons


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

Refresh: Click to manually refresh the page immediately.

User select box: At the dropdown select the set of users (Static, NAS, DMS, Combined).

Messages: *No data exists for the user*

Auto-refresh  Static 

Combined 
 Static
 NAS
 DMS
 Combined

3-18.2 Protocol-based VLAN

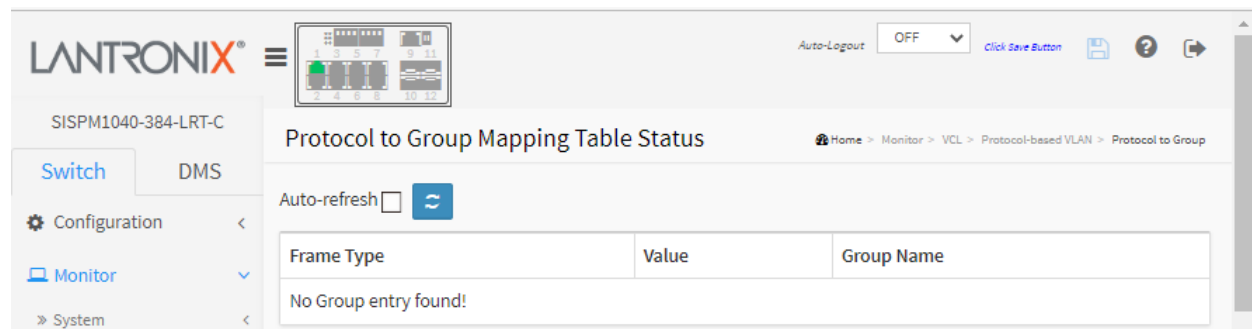
3-18.2.1 Protocol to Group

This page displays the protocols to Group Name (unique for each Group) mapping entries for the switch.

To display protocol to Group Name mapping in the web UI:

1. Click Monitor, VCL, Protocol-based VLAN, Protocol to Group.
2. Check "Auto-refresh".
3. Click "Refresh" to refresh the port detailed statistics.

Figure 3-18.2.1: 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:

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

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

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.

Buttons

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

Refresh: Click to manually refresh the page immediately.

Messages: *No Group entry found!*

3-18.2.2 Group to VLAN

This page displays the configured Group Name mapping to a VLAN for the switch.

1. Click Monitor, VCL, Group to VLAN.
2. Check "Auto-refresh".
3. Click "Refresh" to refresh the port detailed statistics.

Figure 3-17.2.2: Group Name to VLAN mapping Table

The screenshot shows the Lantronix web interface for device SISPM1040-384-LRT-C. The page title is "Group Name to VLAN mapping Table Stauts". The breadcrumb navigation is "Home > Monitor > VCL > Protocol-based VLAN > Group to VLAN". There is an "Auto-Logout" dropdown set to "OFF" and a "Click Save Button" link. The left sidebar shows "Switch" selected under "Monitor". The main content area has an "Auto-refresh" checkbox and a refresh button. Below is a table with the following structure:

Group Name	VLAN ID	Port Members											
		1	2	3	4	5	6	7	8	9	10	11	12
No Group entry found!													

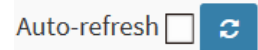
Parameter descriptions:

Group Name : A valid Group Name is a string at the most 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 the 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. The valid VLAN ID range is 1-4095.

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

Buttons



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

Refresh: Click to manually refresh the page immediately.

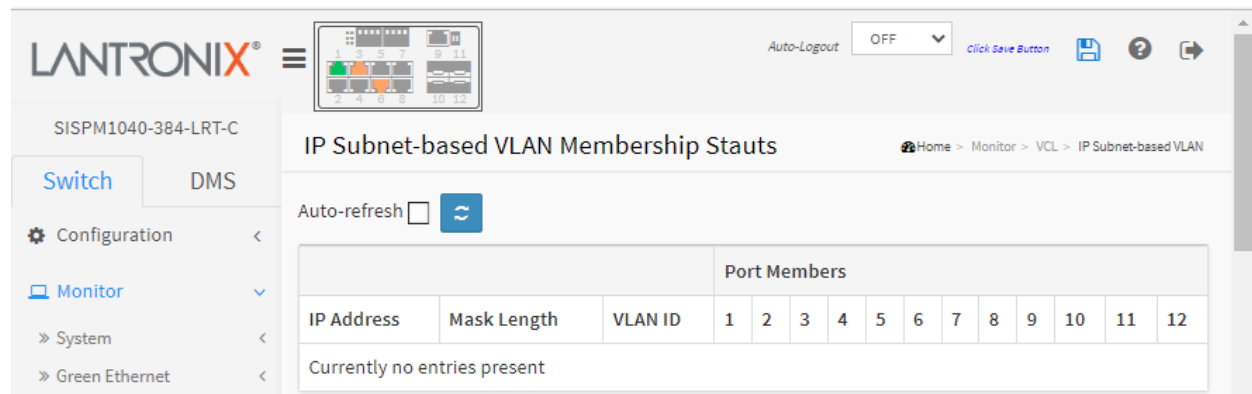
Messages: *No Group entry found!*

3-18.3 IP Subnet-based VLAN

This page shows IP subnet-based VLAN entries (only static entries).

1. Click Monitor, VCL, and IP Subnet-based VLAN.
2. Check "Auto-refresh".
3. Click "Refresh" to refresh the port detailed statistics.

Figure 3-17.3: 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, 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 an 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.

Messages:

No Group entry found!

Currently no entries present

3-19 sFlow

This page shows receiver and per-port sFlow statistics:

1. Click Monitor, sFlow.
2. View the sFlow information.
3. Use the buttons as required.

Figure 3-19: sFlow Statistics

The screenshot displays the Lantronix web interface for device SISPM1040-384-LRT-C. The page title is 'sFlow Statistics'. The left navigation menu is expanded to 'Monitor' > 'sFlow'. The main content area features an 'Auto-refresh' checkbox (unchecked) and two buttons: 'Clear Receiver' and 'Clear Ports'. Below these are two tables:

Receiver Statistics

Owner	<Configured through local management>
IP Address/Hostname	192.168.1.75
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
11	0	0	0
12	0	0	0

Parameter descriptions:**Receiver Statistics**

Owner : Shows the current owner of the sFlow configuration as one of these three values:

<**none**> : If sFlow is currently unconfigured/unclaimed, Owner contains <**none**>.

<**Configured through local management**> : If sFlow is currently configured through Web or CLI, Owner contains <**Configured through local management**>.

<**string**> : 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.

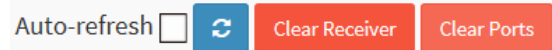
Counter Samples : The total number of counter samples sent to the sFlow receiver.

Port Statistics

Port : The port number for which the following statistics apply.

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 manually refresh the page immediately.

Clear Receiver: Clears the sFlow receiver counters.

Clear Ports: Clears the per-port counters.

3-20 UDLD

This page displays the UDLD status of the ports.

1. Click Monitor, UDLD.
2. View the UDLD information.

Figure 3-20: Detailed UDLD Status for Port 1

The screenshot displays the 'Detailed UDLD Status for Port 1' page in the Lantronix web interface. The page title is 'Detailed UDLD Status for Port 1'. Below the title, there is an 'Auto-refresh' checkbox (unchecked) and a refresh button. A dropdown menu shows 'Port 1'. The main content area is divided into two sections: 'UDLD Status' and 'Neighbour Status'. The 'UDLD Status' section contains a table with the following data:

UDLD Admin state	Enable
Device ID(local)	00-C0-F2-49-BE-22
Device Name(local)	SISPM1040-384-LRT-C
Bidirectional State	Indeterminant

The 'Neighbour Status' section contains a table with the following data:

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

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 in the format 00-40-B7-12-12-D8.

Device Name(local) : Name of the Device (e.g., SISPM1040-384-LRT-C).

Bidirectional State : The current state of the port.

Neighbor Status

Port : The current port of neighbor device.

Device ID : The current ID of neighbor device.

Link Status : The current link status of neighbor port.

Device Name : Name of the Neighbor Device.

Buttons

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

Refresh: Click to manually refresh the page immediately.

Port 1

: **Port select** box; select the port to view.

Messages: No Neighbour ports enabled or no existing partners

Chapter 4. Diagnostics

This chapter provides a set of basic system diagnosis. It let users know whether the system is healthy or needs to be fixed. The basic system check includes ICMP Ping, Link OAM, ICMPv6, and Cable Diagnostics.

4-1 Ping

This page lets you issue ICMP Ping packets to troubleshoot IPv6 connectivity issues.

1. Navigate to Diagnostics > Ping.
2. Specify ICMP Ping IP Address, Ping length, Ping count, and Ping interval.
3. Click Start.

Figure 4-1: ICMP Ping

The screenshot shows the Lantronix web interface for the SISPM1040-384-LRT-C device. The left sidebar contains navigation options: Configuration, Monitor, and Diagnostics. Under Diagnostics, there are links for Ping, Ping6, and Cable Diagnostics. The main content area is titled 'ICMP Ping' and contains a form with the following fields:

IP Address	0.0.0.0
Ping Length	56
Ping Count	5
Ping Interval	1

A 'Start' button is located below the form. The top right of the interface shows 'Auto-Logout OFF' and a 'Click Save Button' link.

IP Address : Set the IP Address of device that you want to ping.

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. Valid values are 1 - 60 times.

Ping Interval: The interval of the ICMP packet. Valid values are 0 - 30 seconds.

Start: Click the "Start" button then the switch will start to ping the device using ICMP packet size what set on the switch.

After you press **Start**, five 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.

The screenshot shows the Lantronix web interface for the SISPM1040-384-LRT-C device. The left sidebar contains navigation options: Configuration, Monitor, and Diagnostics. Under Diagnostics, there are links for Ping, Ping6, and Cable Diagnostics. The main content area is titled 'ICMP Ping Output' and contains the following text:

```
PING server 192.168.1.77, 20 bytes of data.
rcvfrom: Operation timed out
rcvfrom: Operation timed out
rcvfrom: Operation timed out
Sent 3 packets, received 0 OK, 0 bad
```

A 'New Ping' button is located below the output text. The top right of the interface shows 'Home > Diagnostics > Ping'.

Buttons

New Ping: Click to end the current ping request and return to the default Ping page.

Example

```
PING server 192.168.1.77, 22 bytes of data.  
30 bytes from 192.168.1.77: icmp_seq=0, time=0ms  
30 bytes from 192.168.1.77: icmp_seq=1, time=0ms  
Sent 2 packets, received 2 OK, 0 bad
```

4-2 Ping6

This page lets you issue ICMPv6 Ping packets to troubleshoot IPv6 connectivity issues.

1. Navigate to Diagnostics > Ping6.
2. Specify ICMPv6 Ping IP Address.
3. Specify ICMPv6 Ping Length, Count, and Interval and Egress Interface.
4. Click Start.

Figure 4-2: ICMPv6 Ping

The screenshot shows the Lantronix web interface for the SISPM1040-384-LRT-C device. The page title is "ICMPv6 Ping". The left navigation menu is expanded to "Diagnostics" > "Ping6". The main configuration area contains the following fields:

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 below the configuration fields. The top right of the interface shows "Auto-Logout" set to "OFF" and a "Click Save Button" link.

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 second to 30 seconds.

Egress Interface : 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 “Start” button then the switch will start to ping the device using the ICMPv6 packet size that was set. After you press Start, five 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.



Messages

% Unable to perform PING6 operation on VLAN 10!

% Please specify correct egress IPv6 interface.

4-3 Cable Diagnostics

This page lets you run the Cable Diagnostics. Click **Start** to run the diagnostics. This will take approximately 5 seconds. When completed, the page refreshes automatically, and you can view the cable diagnostics results in the cable status table. Note that Cable Diagnostics is only accurate for cables of length 7 -140 meters. The 10 and 100 Mbps ports will be linked down while running Cable Diagnostics, so running Cable Diagnostics on a 10 or 100 Mbps management port will cause the switch to stop responding until Cable Diagnostics are complete.

To run Cable Diagnostics in the web UI:

1. Navigate to Diagnostics > Cable Diagnostics.
2. Specify the Port you want to check.
3. Click Start and then click OK at the confirmation prompt.

Figure 4-3: Cable Diagnostics

Copper Port	Link Status	Test Result	Length
1	1G	OK	3(m)
2	Link Down	detect error or check cable length is between 7-120 meters	
3	Link Down	detect error or check cable length is between 7-120 meters	
4	Cable Diagnostics is running...		

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.

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 follow, the length has 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.

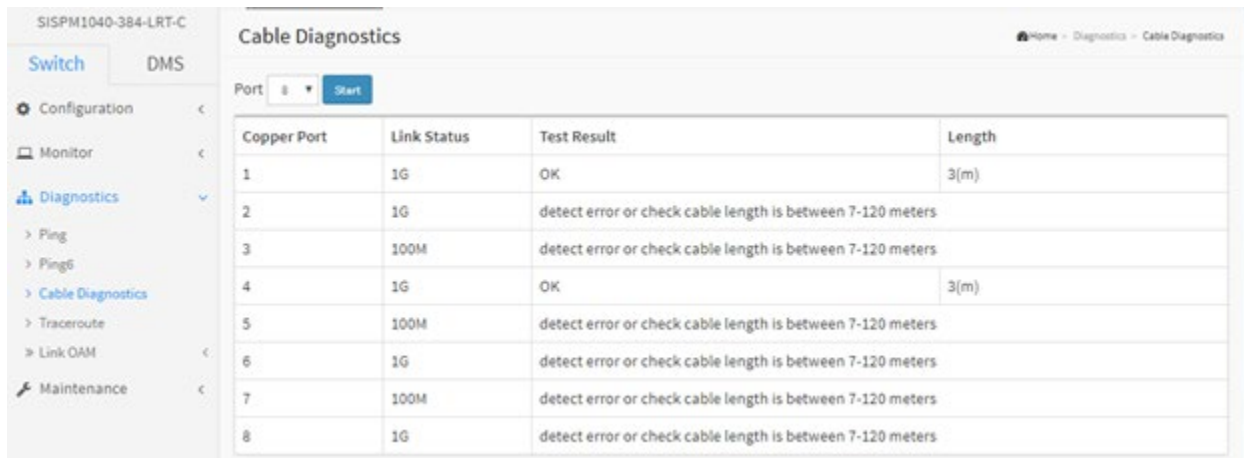
Messages

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.

cable diagnostics is running...

detect error or check cable length is between 7-120 meters

Example:



The screenshot shows the 'Cable Diagnostics' page in a web interface. The page title is 'Cable Diagnostics' and the breadcrumb is 'Home > Diagnostics > Cable Diagnostics'. There is a 'Port' dropdown menu set to '8' and a 'Start' button. Below this is a table with 4 columns: 'Copper Port', 'Link Status', 'Test Result', and 'Length'. The table contains 8 rows of data.

Copper Port	Link Status	Test Result	Length
1	1G	OK	3(m)
2	1G	detect error or check cable length is between 7-120 meters	
3	100M	detect error or check cable length is between 7-120 meters	
4	1G	OK	3(m)
5	100M	detect error or check cable length is between 7-120 meters	
6	1G	detect error or check cable length is between 7-120 meters	
7	100M	detect error or check cable length is between 7-120 meters	
8	1G	detect error or check cable length is between 7-120 meters	

4-4 Traceroute

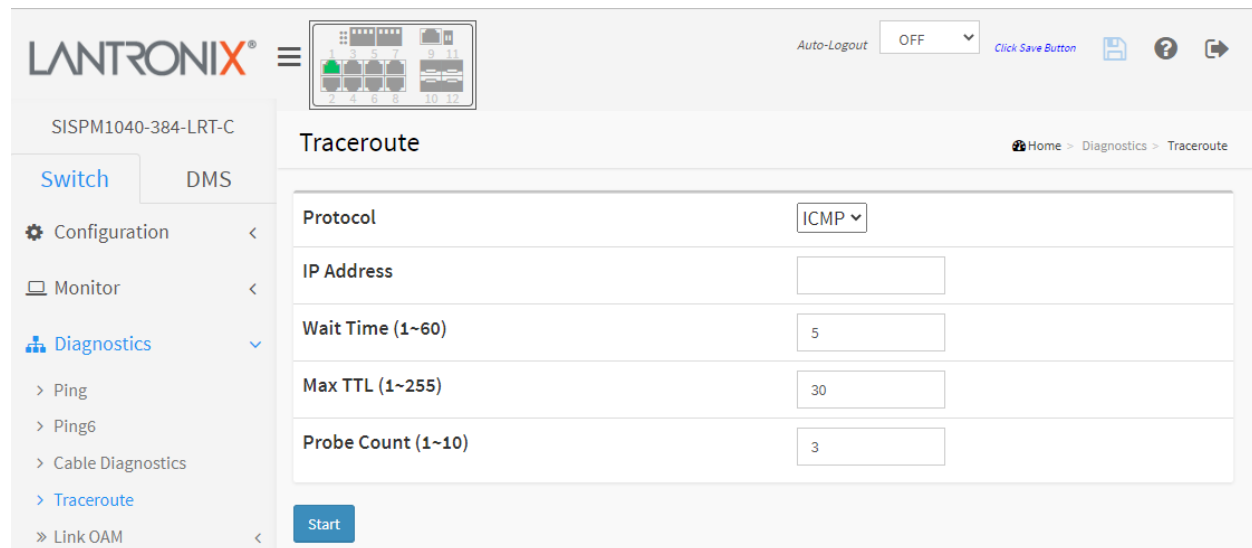
This page lets you issue ICMP, TCP, or UDP packets to diagnose network connectivity issues.

After you press the **Start** button, 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.

To configure a traceroute in the web UI:

1. Navigate to Diagnostics > Traceroute.
2. Select a Protocol.
3. Specify traceroute IP Address.
4. Specify traceroute wait time, TTL, and probe count parameters.
5. Click Start.

Figure 4-4: Traceroute



The screenshot displays the Lantronix web interface for configuring a traceroute. The top navigation bar includes the Lantronix logo, a menu icon, and an Auto-Logout dropdown set to OFF. The breadcrumb trail shows Home > Diagnostics > Traceroute. The left sidebar contains a navigation menu with options: Switch, DMS, Configuration, Monitor, Diagnostics (expanded), Ping, Ping6, Cable Diagnostics, Traceroute (selected), and Link OAM. The main content area is titled 'Traceroute' and contains a configuration form with the following fields:

Protocol	ICMP
IP Address	<input type="text"/>
Wait Time (1~60)	5
Max TTL (1~255)	30
Probe Count (1~10)	3

A blue 'Start' button is located below the form.

Parameter descriptions:

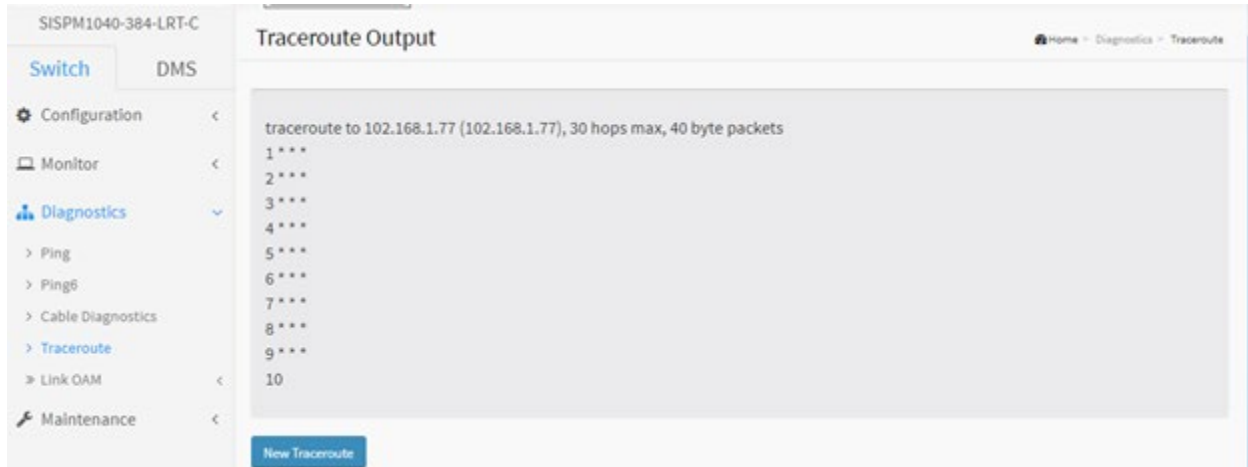
Protocol : The protocol (ICMP, UDP, or TCP) packets to send.

IP Address : The destination IP Address.

Wait Time (1-60) : Set the time (in seconds) to wait for a response to a probe (default 5.0 sec). Values range from 1 to 60. The payload size of the ICMP packet. Values range from 2 bytes to 1452 bytes.

Max TTL (1-255) : Specifies the maximum number of hops (max time-to-live value) traceroute will probe. Values range from 1 to 255 hops. The default is 30 hops.

Probe Count (1-10) : Sets the number of probe packets per hop. Values range from 1 to 10. The default is 3.

Traceroute Output Example:**Buttons**

Start: Click to start transmitting ICMP packets.

New Traceroute: Click to re-start diagnostics with PING.

4-5 Link OAM

4-5.1 MIB Retrieval

This page lets you retrieve the local or remote OAM MIB variable data on a particular port. Select the appropriate radio button and enter the port number of the switch to retrieve the content of interest. Click Start to retrieve the content. Click Previous to retrieve another content of interest.

Note that you must first enable “MIB Retrieval Support” at Configuration > Link OAM > Port Settings.

To configure Link OAM MIB Retrieval in the web UI:

1. Click Maintenance, Link OAM and Statistics.
2. View the displayed the statistics.

Figure 4-5.1: MIB Retrieval

Parameter descriptions:

Local : Select if a local device.

Peer : Select if a peer device.

Port : Enter the port number of the switch to retrieve information on.

Buttons:

Start : Click to retrieve the MIB content.

Previous : Click to retrieve another content of interest.

Messages:

*OAM Error Invalid request on this port
Port must be specified.*

Chapter 5. Maintenance

This chapter describes switch Maintenance tasks, including Restart, Reboot, Factory Defaults, Firmware upgrade/swap, Config Save/Download/Upload/Activate/Delete, and Server Report.

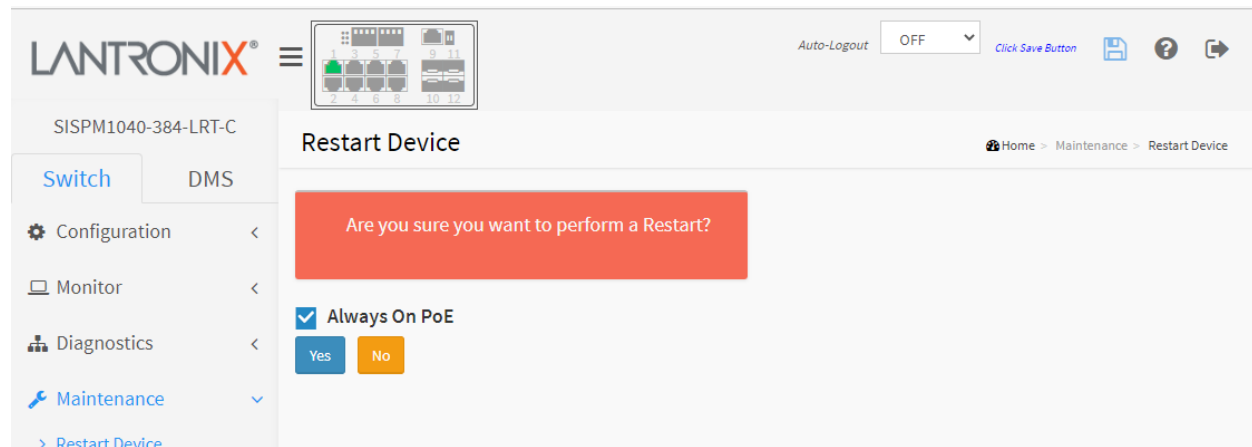
5-1 Restart Device

This page lets you restart the switch for any maintenance needs. Any configuration files or scripts that you saved in the switch should still be available afterwards.

To restart the switch in the web UI:

1. Click Maintenance, Restart Device.
2. Check the Always On PoE checkbox if needed.
3. Click Yes.

Figure 5-1: Restart Device



Parameter descriptions:

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

Always On PoE : Check the box so that when the switch warm restarts it will continue supplying PoE power to the PDs. **Note:** "Always on PoE" is de-activated in FW v7.20.0034; to get "Always on PoE" back, reload factory defaults, copy running-config to startup-config, and then refresh browser cache after finishing FW upgrade to FW v7.20.0034.

Buttons:

Yes – Click to restart the device.

No- Click to undo any restart action.

5-2 Reboot Schedule

This page lets you schedule the day and time to reboot the switch. To schedule a Reboot in the web UI:

1. Click Maintenance, Reboot Schedule.
2. At the Mode dropdown select Enabled to display the parameters table.
3. Set the Reboot Week Day and Time parameters.
4. Click Apply.

Figure 5-2: Switch Reboot Schedule

LANTRONIX®

SISPM1040-384-LRT-C

Switch Reboot Schedule

Auto-Logout OFF

Click Save Button

Home > Maintenance > Reboot Schedule

Switch DMS

Configuration <

Monitor <

Diagnostics <

Maintenance >

Restart Device

Reboot Schedule

Factory Defaults

Firmware <

Configuration <

Server Report

Mode Enabled

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

Apply Reset

Parameter descriptions:

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.

Buttons:

Apply—Click to save changes.

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

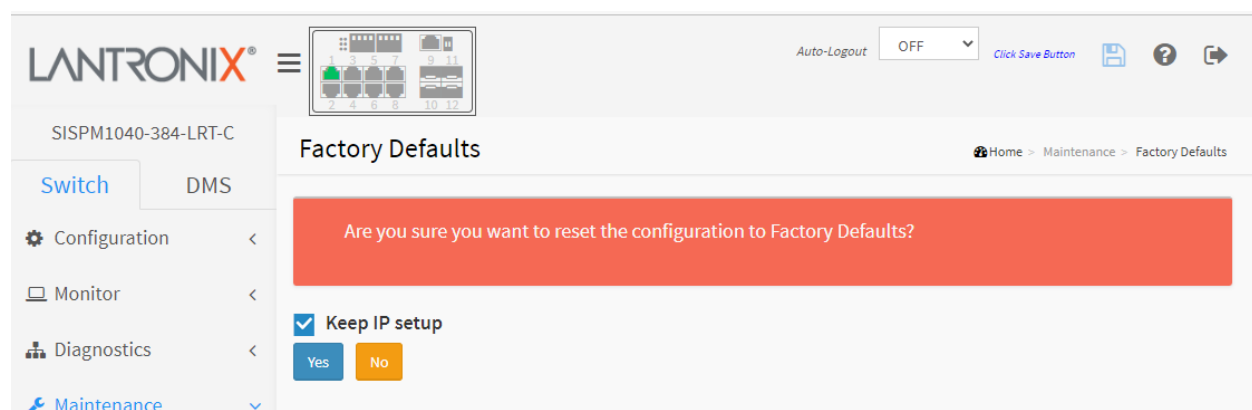
5-3 Factory Defaults

This webpage lets you reset the Switch configuration to Factory Defaults. Any configuration files or scripts will be reset to factory default values. You can reset the configuration of the switch on this page. The IP configuration may be retained. The new configuration is available immediately, which means that no restart is necessary.

To reset the switch to Factory Defaults in the web UI:

1. Click Maintenance, Factory Defaults.
2. Check the "Keep IP setup" checkbox if desired.
3. Click the Yes button.

Figure 5-2: Factory Defaults



Parameter descriptions:

Keep IP setup : Check the checkbox to keep current IP setting after the reset to factory defaults.

Buttons:

Yes – Click to "Yes" button to reset the configuration to Factory Defaults.

No - Click to return to the Port State page without resetting the configuration.

Note: Restoring factory default can also be performed by making a physical loopback between port 1 and port 2 within the first minute from switch reboot. In the first minute after boot, 'loopback' packets will be transmitted at port 1. If a 'loopback' packet is received at port 2 the switch will do a restore to default.

5-4 Firmware

This page lets you upgrade switch firmware. The switch can be enhanced with value-added functions by installing firmware upgrades. See the [SISPM1040-384-LRT-C Product](#) web page or [SISPM1040-362-LRT](#) webpage for firmware upgrade files.

5-4.1 Firmware Upgrade



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. After the software image is uploaded, a page announces that the firmware update is initiated. After about a minute, the firmware is updated and the switch restarts.



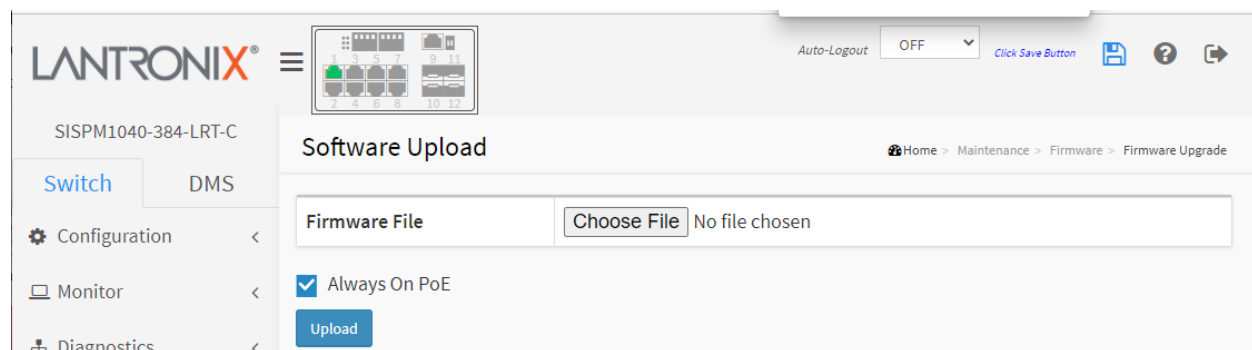
Warning: While the firmware is being updated, Web access appears to be defunct. The front LED flashes Green/Off with a frequency of 10 Hz while the firmware update is in progress. **Do not** restart or power off the device at this time or the switch may fail to function afterwards.

Web Interface

To perform a Firmware Upgrade via the web UI:

1. Click Maintenance > Firmware > Firmware Upgrade.
2. Click the Choose File button and select the firmware file to upgrade to. Verify the filename and extension (e.g., *SISPM1040-384-LRT-C_v7.20.0190_CM_202202002.imgs*).
3. Click the Upload button.

Figure 5-4.1 Firmware Upload



Parameter descriptions:

Buttons:

Choose File : Click the "Browse..." button to search for the Firmware URL and filename.

Upload: Click to start the firmware upgrade.

Always On PoE : allows a warm reboot of the switch without affecting the PoE output to the PDs, providing continuous power even during firmware upgrade.

Messages**Message:** *Success EZCM Files & Invalid Firmware Image*

The EZCM files are successfully Downloaded. The uploaded firmware image is invalid. Please use a correct firmware image. Reboot System.

Meaning: The Firmware Upgrade feature detected the wrong version but only AFTER uploading the EZCM files, causing the switch to display an incorrect model type and icon. The Firmware Upgrade feature does not check for correct file type, and can load an invalid configuration file.

Recovery: 1. Verify the filename and extension. 2. Retry the operation. 3. Contact Technical Support.

Message: *SYS-FIRMWARE: New firmware active: SISPM1040-362-LRT (standalone) v7.10.2205*

Meaning: Syslog message indicating that the firmware upgrade was successful.

Recovery: None required.

5-4.2 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. You can check the active (current) firmware version at Monitor > System > Information.

Note:

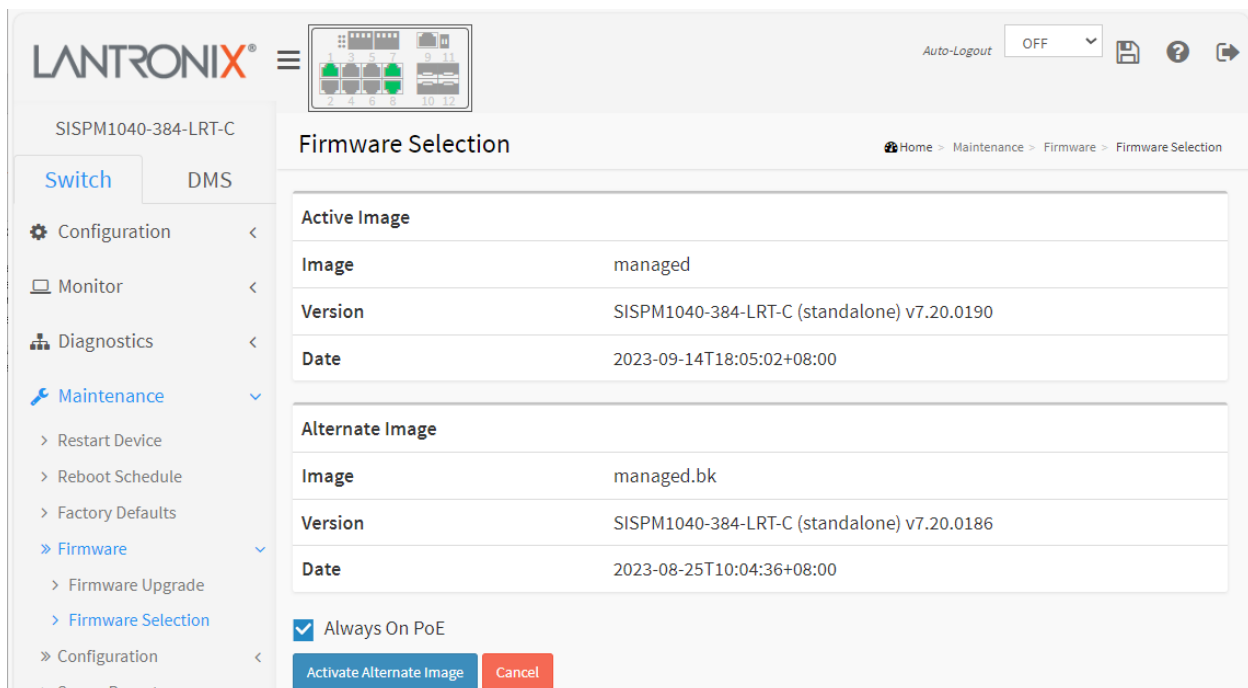
1. If the active firmware image is the alternate image, only the "Active Image" table is shown. In this case, the Activate Alternate Image button is also disabled.
2. If the alternate image is active (due to a corruption of the primary image or by manual intervention), uploading a new firmware image to the device will automatically use the primary image slot and activate this.
3. The firmware version and date information may be empty for older firmware releases. This does not constitute an error.

Web Interface

To perform a firmware selection via the web UI:

1. Click Maintenance > Firmware > Firmware Selection.
2. If desired, check the 'Always On PoE' checkbox.
3. Click the Activate Alternate Image button.
4. At the confirmation prompt (*Are you sure you want to activate the alternate software image?*) click OK.

Figure 5-4.2 Firmware Selection



The screenshot shows the Lantronix web interface for device SISPM1040-384-LRT-C. The main content area is titled "Firmware Selection" and contains two tables. The "Active Image" table lists the following details: Image (managed), Version (SISPM1040-384-LRT-C (standalone) v7.20.0190), and Date (2023-09-14T18:05:02+08:00). The "Alternate Image" table lists: Image (managed.bk), Version (SISPM1040-384-LRT-C (standalone) v7.20.0186), and Date (2023-08-25T10:04:36+08:00). Below the tables, there is a checked checkbox for "Always On PoE" and two buttons: "Activate Alternate Image" (blue) and "Cancel" (red). The left sidebar shows the navigation menu with "Maintenance" expanded to "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., *SISPM1040-384-LRT-C (standalone) v7.20.0190*).

Date : The date when the firmware was produced, in the format *2023-09-14T18:05:02+08:00*.

Always On PoE : Check this box so that when the switch warm restarts, it will continue supplying PoE power to the PDs during the firmware upgrade.

Buttons

Activate Alternate Image: Click to use the "Alternate Image". This button may be disabled depending on system state.

Cancel: Cancel activating the backup image. Navigates away from this page to the Monitor > System > Information page.

Messages:

Are you sure you want to activate the alternate software image?

System restart in progress

The system is now restarting.

Waiting, please stand by...

Processing...

5-5 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. There are three system files:

- **running-config:** A virtual file representing the currently active switch config. This file is volatile.
- **startup-config:** The startup configuration of 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.

You can also store up to two other files and apply them to the running-config, thus switching configs.

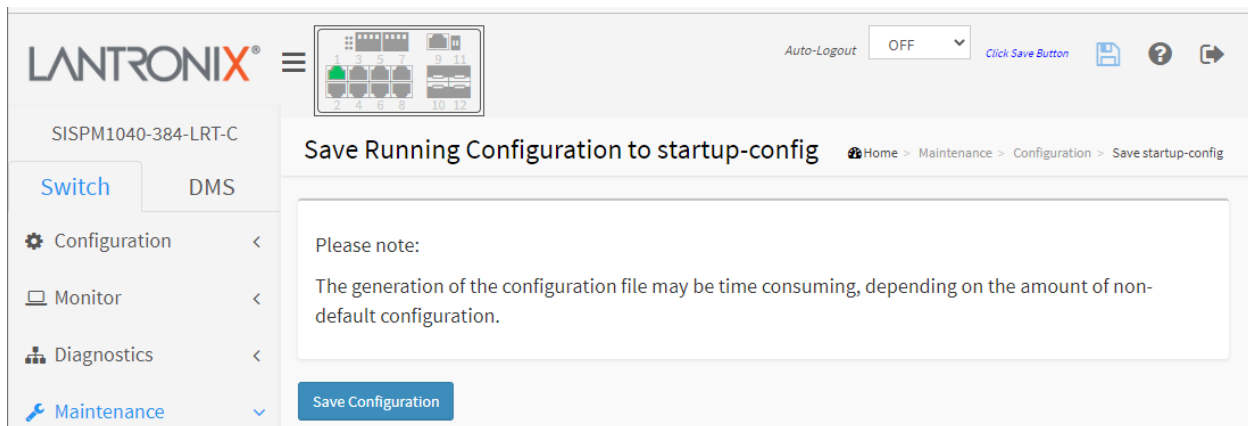
5-5.1 Save running-config to startup-config

This page lets you copy the *running-config* to the *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 via the web UI:

1. Click Maintenance > Configuration > Save startup-config.
2. Click the **Save Configuration** button.

Figure 5-5.1: Save Running Config to startup config



Buttons :

Save Configuration: Click to save configuration; the running configuration will be written to flash memory for system boot up to load this startup configuration file. The message "*startup-config saved successfully.*" displays when successfully completed.

5-5.2 Download

You can download any of the files on the switch to the web browser. 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 available files are:

running-config : A virtual file that represents the currently active switch configuration. This file is volatile. **Note:** Download of running-config may take a little while to complete, as the file must be prepared for download.

default-config : A read-only file with vendor-specific configuration. This file is read when the system is restored to default settings.

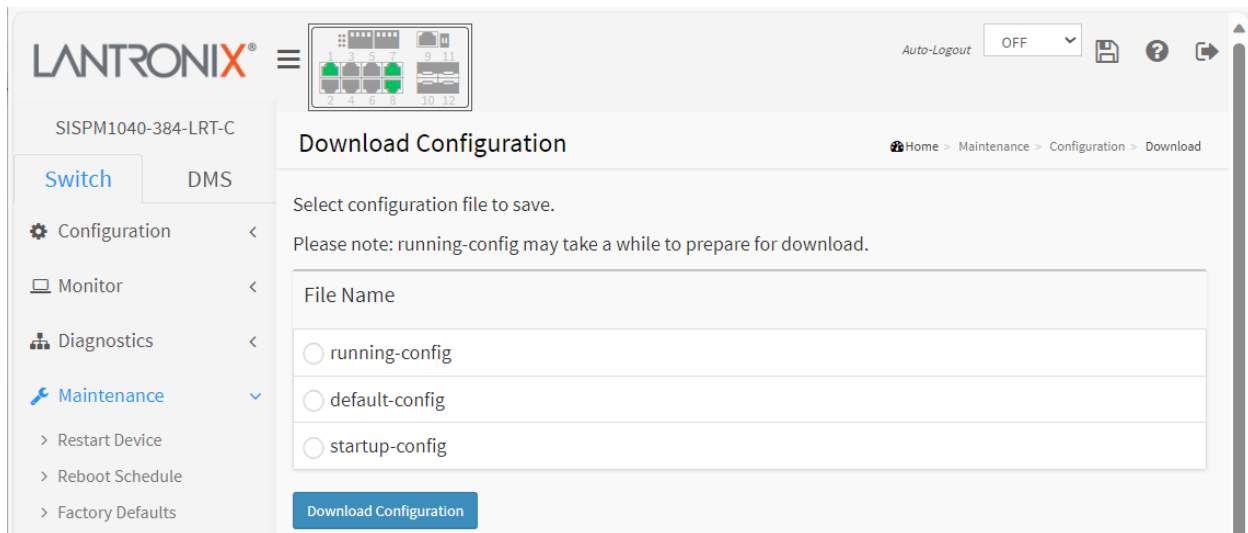
startup-config : The startup configuration for the switch, read at boot time. If this file doesn't exist at boot time, the switch will start up in its default configuration.

Up to 99 other files, typically used for configuration backups or alternative configurations, can be saved.

To download a configuration via the web UI:

1. Click Maintenance > Configuration > Download.
2. Select the desired configuration File Name to save.
3. Click the **Download Configuration** button.

Figure 5-5.2: Download Configuration

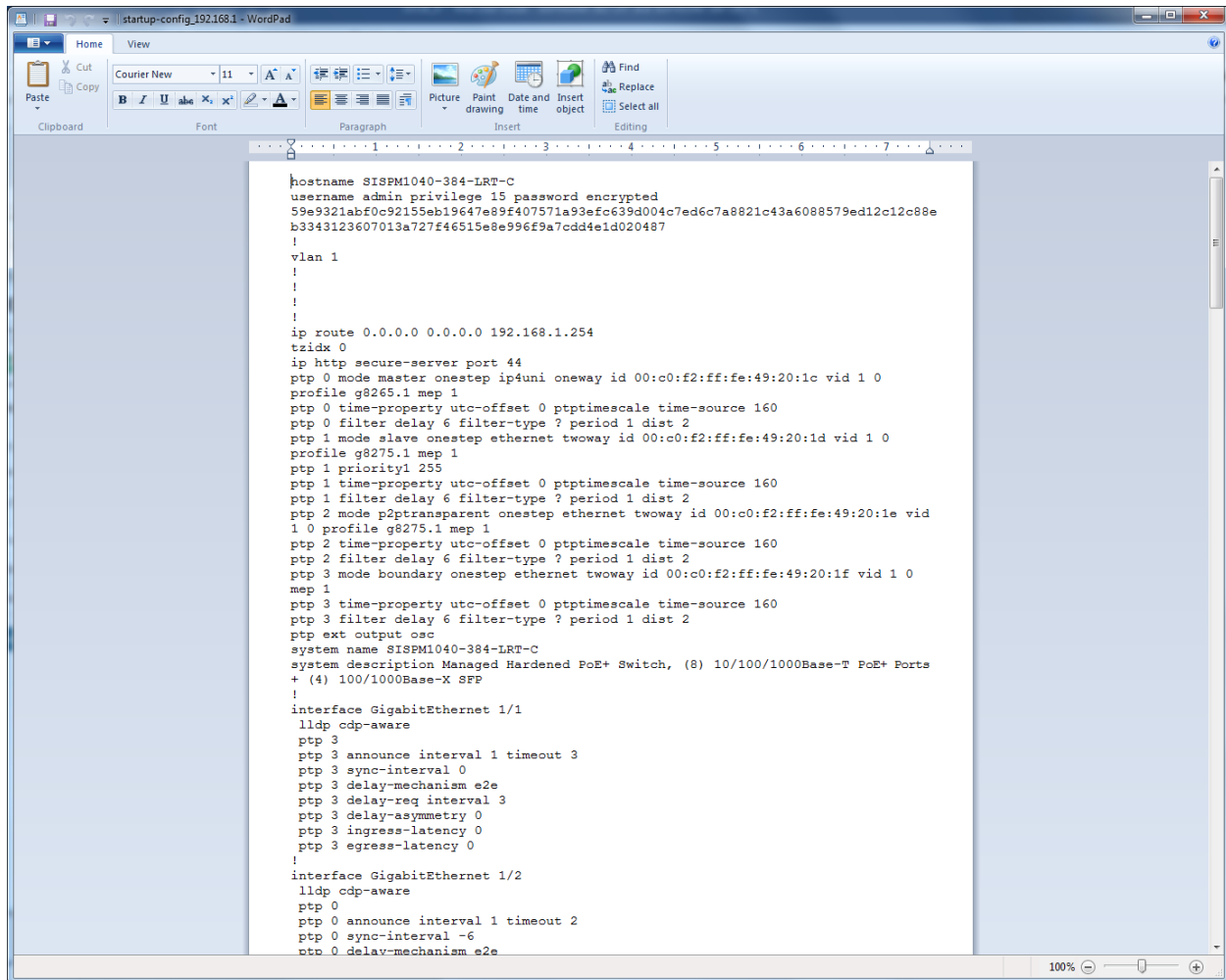


Parameter descriptions:

File Name: Select the desired configuration File Name to save.

Buttons :

Download Configuration: Click to download the saved file.

Sample Download config file:

```
hostname SISPM1040-384-LRT-C
username admin privilege 15 password encrypted
59e9321abf0c92155eb19647e89f407571a93efc639d004c7ed6c7a8821c43a6088579ed12c12c88e
b3343123607013a727f46515e8e996f9a7cdd4e1d020487
!
vlan 1
!
!
!
!
ip route 0.0.0.0 0.0.0.0 192.168.1.254
tzidx 0
ip http secure-server port 44
ptp 0 mode master onestep ip4uni oneway id 00:c0:f2:ff:fe:49:20:1c vid 1 0
profile g8265.1 mep 1
ptp 0 time-property utc-offset 0 ptptimescale time-source 160
ptp 0 filter delay 6 filter-type ? period 1 dist 2
ptp 1 mode slave onestep ethernet twoway id 00:c0:f2:ff:fe:49:20:1d vid 1 0
profile g8275.1 mep 1
ptp 1 priority1 255
ptp 1 time-property utc-offset 0 ptptimescale time-source 160
ptp 1 filter delay 6 filter-type ? period 1 dist 2
ptp 2 mode p2ptransparent onestep ethernet twoway id 00:c0:f2:ff:fe:49:20:1e vid 1 0
profile g8275.1 mep 1
ptp 2 time-property utc-offset 0 ptptimescale time-source 160
ptp 2 filter delay 6 filter-type ? period 1 dist 2
ptp 3 mode boundary onestep ethernet twoway id 00:c0:f2:ff:fe:49:20:1f vid 1 0
mep 1
PTP 3 time-property utc-offset 0 ptptimescale time-source 160
PTP 3 filter delay 6 filter-type ? period 1 dist 2
PTP ext output oac
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
lldp cdp-aware
ptp 3
ptp 3 announce interval 1 timeout 3
ptp 3 sync-interval 0
ptp 3 delay-mechanism e2e
ptp 3 delay-req interval 3
ptp 3 delay-asymmetry 0
ptp 3 ingress-latency 0
ptp 3 egress-latency 0
!
interface GigabitEthernet 1/2
lldp cdp-aware
ptp 0
ptp 0 announce interval 1 timeout 2
ptp 0 sync-interval -6
ptp 0 delay-mechanism e2e
```

5-5.3 Upload

The configuration upload function will be backed up and saved configuration from the switch's configuration into the running web browser PC. It is possible to upload any of the files on the switch to the web browser. There are three system files:

running-config : A virtual file that represents the currently active switch configuration. This file is volatile. **Note:** Upload of the *running-config* file may take a little while to complete, as the file must be prepared for upload.

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. If this file doesn't exist at boot time, the switch will start up in its default configuration.

To upload a configuration in the web UI:

1. Click Maintenance > Configuration > Upload.
2. Browse to and select the File to Upload.
3. Select the filename to be uploaded.
4. For *running-config* select the Replace or the Merge parameter.
5. Click the Upload Configuration button.

Figure 5-5.3: Upload Configuration

File Name	Parameters
<input type="radio"/> running-config	<input checked="" type="radio"/> Replace <input type="radio"/> Merge
<input type="radio"/> startup-config	
<input type="radio"/> Create new file	<input type="text"/>

Parameter descriptions:

File Name: Select one of the three system files (*running-config*, *default-config*, *startup-config*) or select Create new file. If the destination is *running-config*, the file can be applied to the switch configuration 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*.

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.

Buttons:

Choose File: Click the button and browse to and select the desired file to upload (e.g., *SISPM1040-384-LRT-C_v7.10.2121_201902019.IMGS*).

Upload Configuration: Click the “Upload” button; the running web management PC will start to upload the configuration from the managed switch configuration into the management PC; you can configure the web browser’s upload file path to keep the configuration file.

Messages:

Upload successfully completed.

5-5.4 Activate

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 available files are:

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

startup-config: The startup configuration for the switch, read at boot time. If this file doesn't exist at boot time, the switch will start up in default configuration.

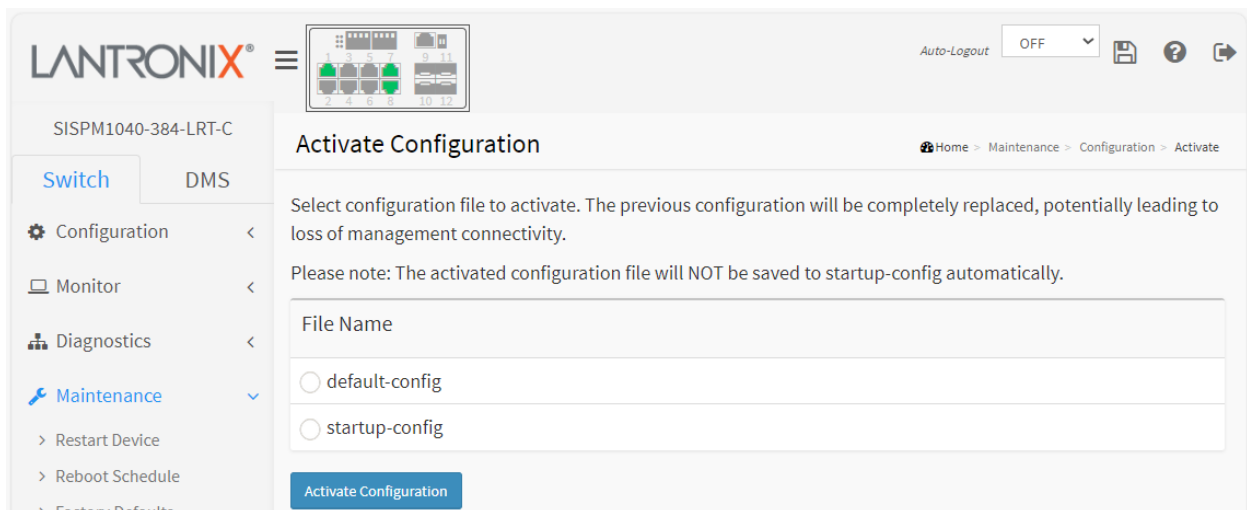
default-config: A read-only file with vendor-specific configuration. This file is read when the system is restored to default settings.

You can create up to 99 other files, typically used for configuration backups or alternate configurations.

To activate a configuration via the web UI:

1. Click Maintenance > Configuration > Activate.
2. Select the configuration file to activate. The previous configuration will be completely replaced, potentially leading to loss of management connectivity.
If no files are available, the message "No files available for activation." displays.
Please note: The activated configuration file will NOT be saved to startup-config automatically.
3. Click the **Activate Configuration** button.

Figure 5-5.4: Configuration Activation



Parameter descriptions:

File Name: Select a file to be activated:

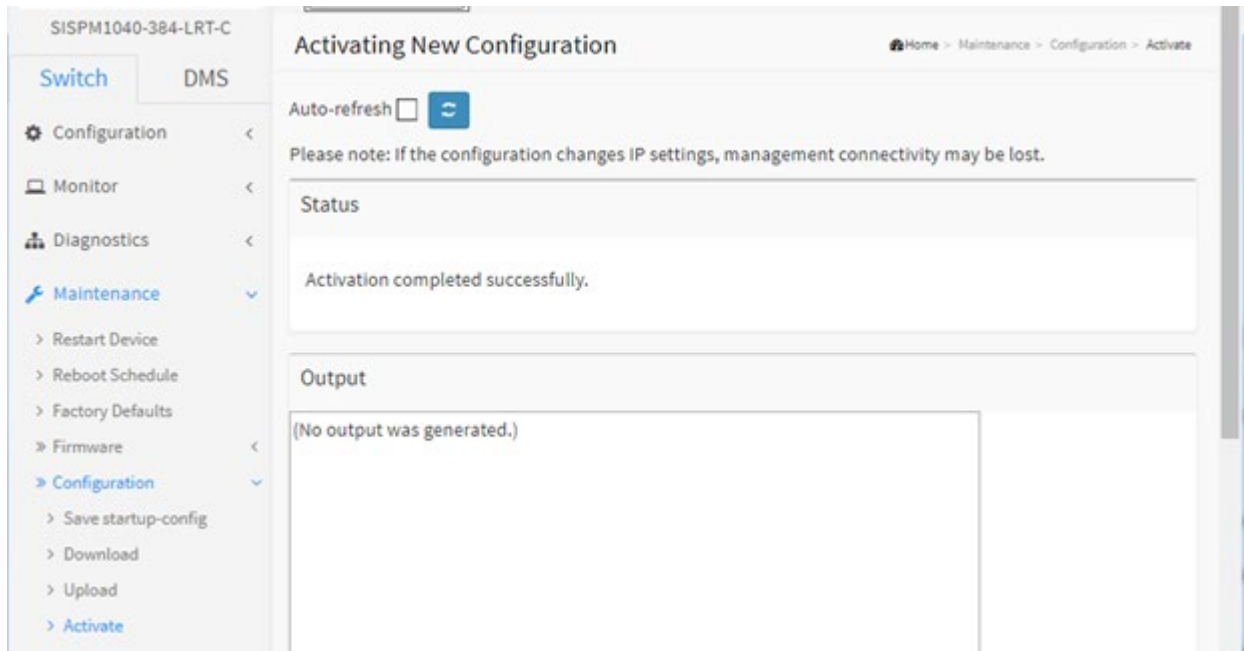
default-config: A read-only file with vendor-specific configuration. This file is read when the system is restored to default settings.

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

Buttons :

Activate Configuration: Click for the *default-config* or *startup-config* file to be activated and to become this switch's running configuration.

Example: Activation completed successfully:



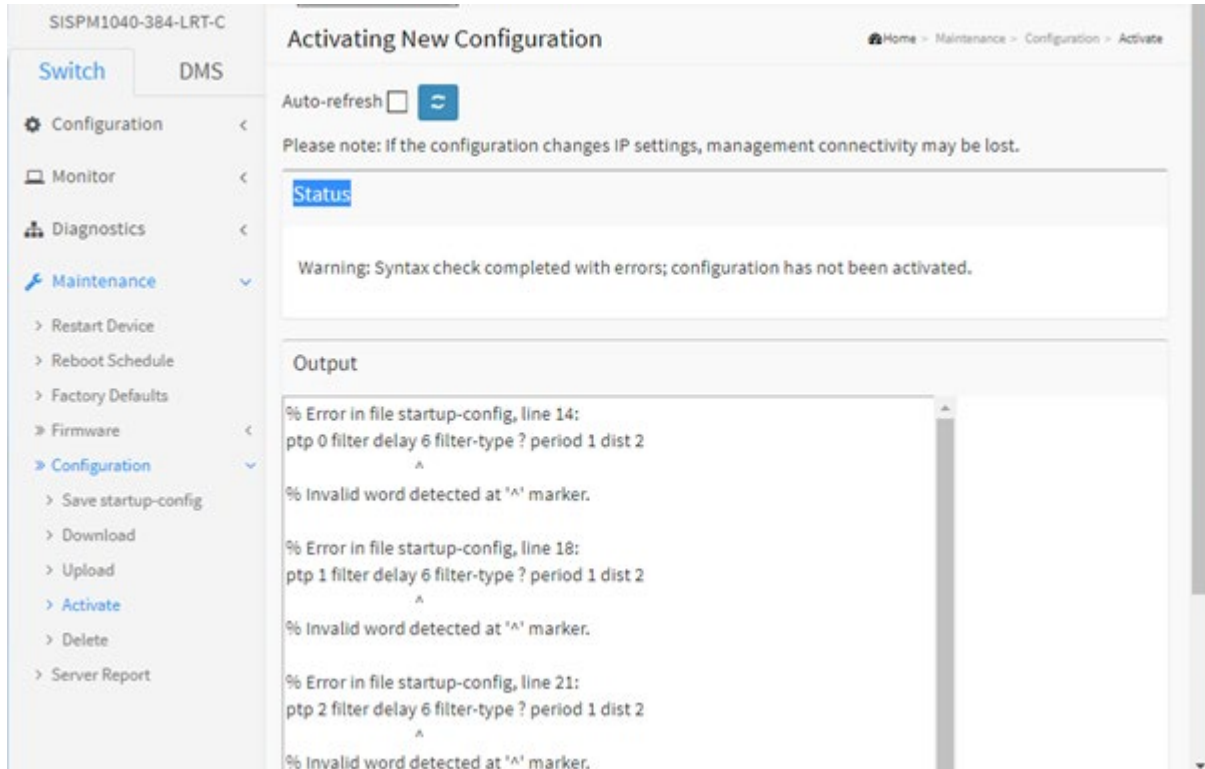
Messages:

Please note: *If the configuration changes IP settings, management connectivity may be lost.*

Status: *Activation completed successfully. The Login screen displays.*

Output: *(No output was generated.)*

Status: Warning: Syntax check completed with errors; configuration has not been activated.



Output:

```
% Error in file startup-config, line 14:
ptp 0 filter delay 6 filter-type ? period 1 dist 2
      ^
% Invalid word detected at '^' marker.
% Error in file startup-config, line 18:
ptp 1 filter delay 6 filter-type ? period 1 dist 2
      ^
% Invalid word detected at '^' marker.
% Error in file startup-config, line 21:
ptp 2 filter delay 6 filter-type ? period 1 dist 2
      ^
% Invalid word detected at '^' marker.
% Error in file startup-config, line 24:
ptp 3 filter delay 6 filter-type ? period 1 dist 2
      ^
% Invalid word detected at '^' marker.
% Syntax check done, 4 problems found.
```

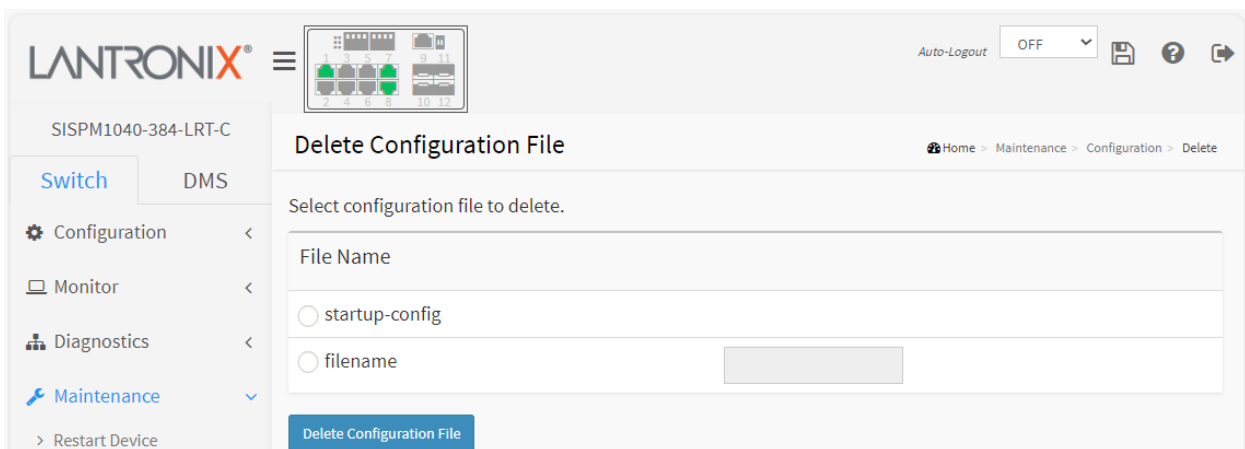
5-5.5 Delete

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 configuration file via the web UI:

1. Click Maintenance > Configuration > Delete.
2. Select the configuration file to delete. If no files are available, the message *"No files available for deletion."* displays.
3. Click the Delete Configuration File button.
4. At the prompt *"Are you sure ..."* click the OK button.

Figure 5-5.5: Delete Configuration File



Parameter descriptions:

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

filename : When selected, enter the name of the file to be deleted.

Buttons :

Delete Configuration: Click the "Delete" button then the *startup-config* file will be deleted; this effectively resets the switch to its factory default configuration.

Messages:

Delete Configuration File *Another configuration I/O operation is in progress. Please try again in a moment.*

Successfully deleted.

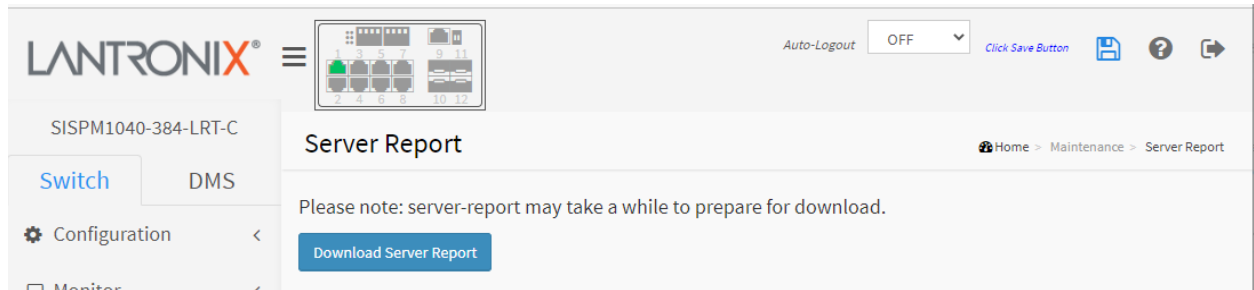
5-6 Server Report

It is possible to download a server report file from the switch to the web browser. Downloading a server report may take a little while to complete, as the file must be prepared for download.

To download a server report via the web UI:

1. Click Maintenance > Server Report.
2. Click the **Download Server Report** button.
3. At the dialog, select Open, Save, or Cancel.

Figure 5-6: Server Report



A sample Server Report text file is shown below.

```

server-report.txt
File Edit View
----- System Overview -----
Model Name: SISPM1040-384-LRT-C
Connected Devices: 3
PoE Power Consumption: 0 [W]
Total PoE Available: 240 [W]
Firmware Version: v7.20.0186 2023-08-25
MAC Address: 00-c0-f2-85-54-54
System Uptime: 22:28:20
IP Address: 172.27.195.85
Subnet Mask: 255.255.255.0
Gateway: 172.27.195.1
Primary DNS: 8.8.8.8
----- running-config -----
hostname SISPM1040-384-LRT-C
!
vlan 1
!
!
!
!
ip route 0.0.0.0 0.0.0.0 172.27.195.1
tzidx 0
exec-timeout autologout 0
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
lldp cdp-aware
!
interface GigabitEthernet 1/2
lldp cdp-aware
!
interface GigabitEthernet 1/3
lldp cdp-aware
Ln 1, Col 1 | 100% | Windows (CRLF) | UTF-8

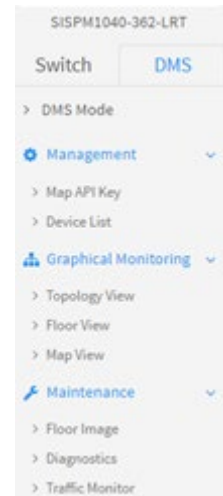
```

Chapter 6. DMS (Device Management System)

Lantronix unique Device Management System (DMS) software provides advanced tools needed for total management of all connected network elements.

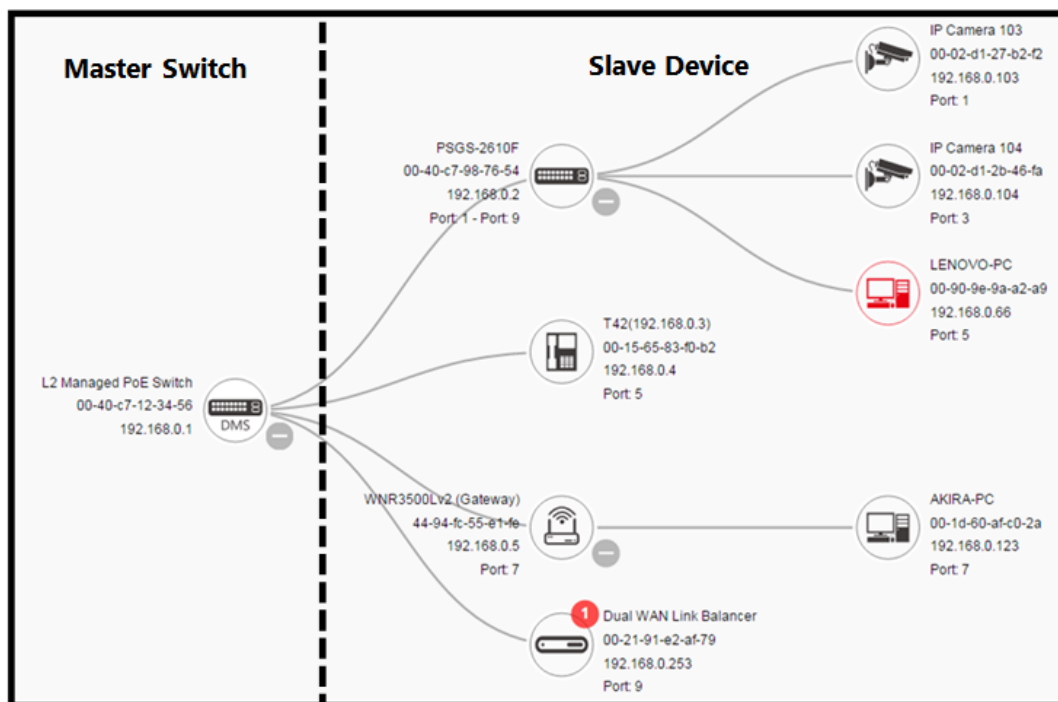
6-1 DMS Introduction

- 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.



6-2 About DMS Mode

- 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.

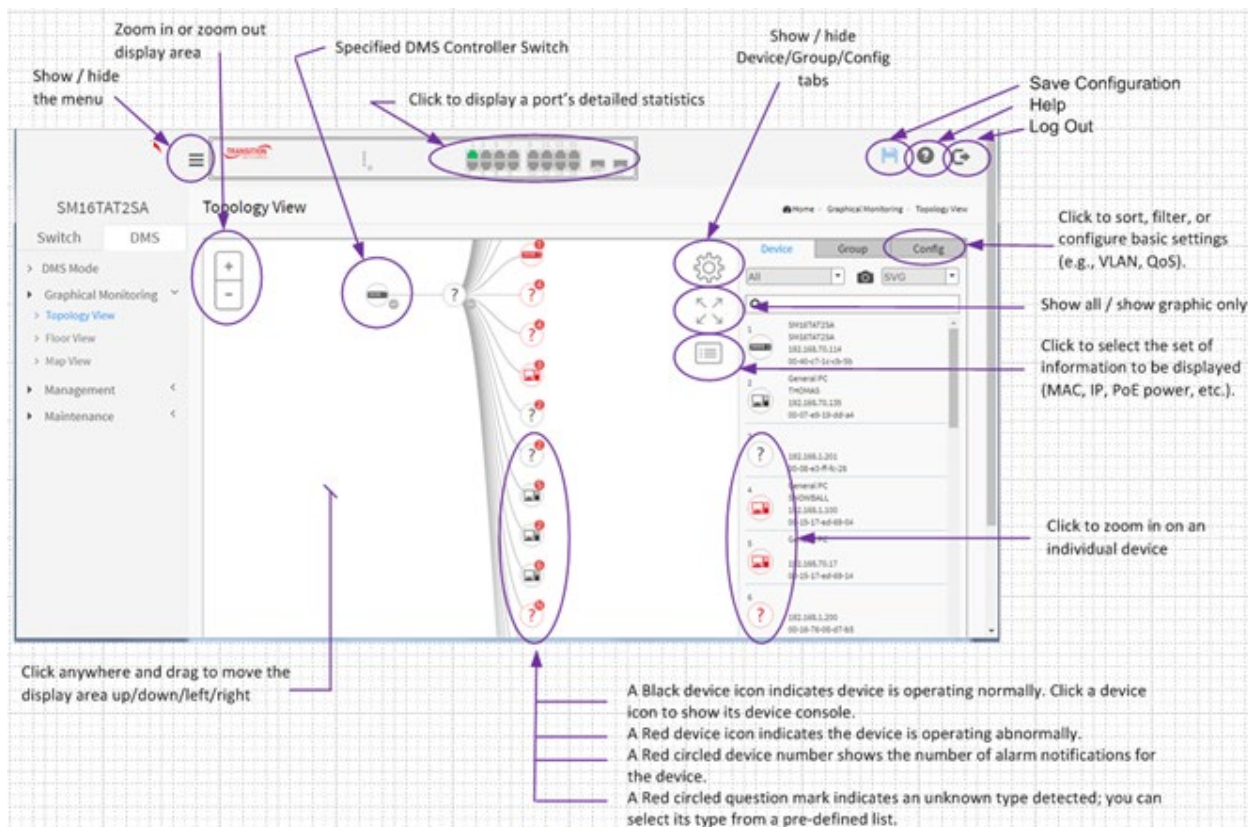


DMS Controller (Master) Switch Notes:

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 will be 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.






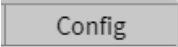
6-4 DMS Icons and Controls

The DMS Topology View icons and controls are shown below.



6-4-1 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.
 <p>40GBNIC-1 General PC 192.168.70.14 Port: 1 (0.009Mb)</p>	A Black device icon indicates device is operating normally. Click a device icon to show its device console.
 <p>SISPM1040-384-LRT-C 192.168.1.77 Port: 1 - Port: 7</p>	A Red device icon indicates the device is operating abnormally.
 <p>40GBNIC-1 General PC 192.168.70.14 Port: 1 (0.009Mb)</p>	A Red circled device number shows the number of alarm notifications for the device.
	Click this icon to select the set of information to be displayed (MAC, IP, PoE power, etc.).
	Click this icon to sort, filter, or configure basic settings (e.g., VLAN, QoS).

6-4-2 Device Consoles (Dashboard / Notification / Monitor)

Click any device icon to display the device consoles for further actions.

- Dashboard Console displays device info and related actions for the device.
- Notification Console displays alarms and logs triggered by events.
- Monitor Console displays the traffics for device health check purpose.

Dashboard Console

Device Type is displayed automatically. If an unknown type is detected, you can still select its type from a pre-defined list.

Device Name: Create your own Device Name or alias for easy management such as "1F_Lobby_Cam1".

Model Name, MAC Address, IP Address, and PoE Used are displayed automatically by DMS.

Http port: Re-assign an http port number to the device for better security.

Login icon: Click to log in the device via http for further configuration or status monitoring.

Diagnostics icon: Click to perform the cable diagnostics, to identify where the cable is broken.

PoE Reboot icon: Click to reboot the device remotely so as to recover the device back to its normal operation. At the confirmation prompt click OK.

Diagnostics icon: Click to diagnose cable status to identify where the cable break is, and check if device connection is alive by ping. The parameters are:

Connection....: A Green checkmark means the device is pinged OK. A Red x means the device cannot transmit /receive correctly. The device cannot be pinged successfully.

Cable Status....: A Green checkmark means the cable is linked OK. A Red x means the cable is not linked correctly. The distance info (in meters) displays to identify a broken cable location.

Settings Consoles (Device / Group / Config)

Click the upper right corner “Settings Icon” to search devices or configure settings:

- **Device** search console lets you sort/filter devices and export topology view.
- **Group** setting console lets you easily configure VLAN/QoS by group or OUI.
- **Config**: system settings console lets you configure global system level settings such as DHCP Server, IP Ranges, etc.

Floor View

- Anchor devices onto Floor Maps
- Find device location instantly
- 10 Maps can be stored in each Switch
- IP Surveillance/VoIP/WiFi applications
- Other features same as Topology View

Map View

- Anchor devices onto Google Maps
- Find devices instantly from Google Maps
- On-Line search by Company/Address
- Outdoor IP Cam/WiFi Applications
- Other features same as Topology View

Scan Devices on Different VLANs via DMS

1. On the IP Interfaces page, DMS will scan multiple interfaces as long as an interface is configured.
2. On the DMS Controller switch you can configure single subnet /multiple subnets. Network manager helps scan devices in others VLANs; this feature helps redirect packets to VLAN1 if you configure many VLANs but only VLAN 1 has IP interface.

The **DMS > Management** path provides the DMS Mode and Device List selections as described below.

6-5 DMS Mode

Here you can view and configure DMS mode global parameters.

1. Click DMS, DMS Mode.
2. Change the Mode and Controller Priority as required.
3. Click the Apply button to save the changes.

Figure 6-1: DMS Mode

The screenshot shows the Lantronix web interface for configuring DMS Mode. The page title is "Information" and the breadcrumb is "Home > Management > DMS Mode". The configuration table is as follows:

Mode	Enabled
Controller Priority	High
Total Device	2
On-line Devices	2
Off-line Devices	0
Controller IP	192.168.1.77

An "Apply" button is located at the bottom left of the configuration area.

Parameter descriptions:

Mode : Select the desired DMS Mode:

Enabled : DMS Mode is enabled (default).

Disabled : DMS Mode is disabled.

- Enabled
- Disabled
- Enabled

Controller Priority: Choose the priority to change the dominant status of the switch:

High: With DMS Mode enabled this device will be the Master (Controller) switch.

Mid: This switch will have medium level priority.

Low: This switch will have the lowest level priority (default).

Non: This switch will never become the Master (Controller) switch.

- Low
- High
- Mid
- Low
- Non

Total Device : The number of detected IP devices detected and displayed in Topology View.

On-line Devices : The number of detected IP devices that are currently online in Topology View.

Off-line Devices : The number of detected IP devices that are currently offline in Topology View.

Controller IP : The Master switch's IP address (e.g., 192.168.1.77).

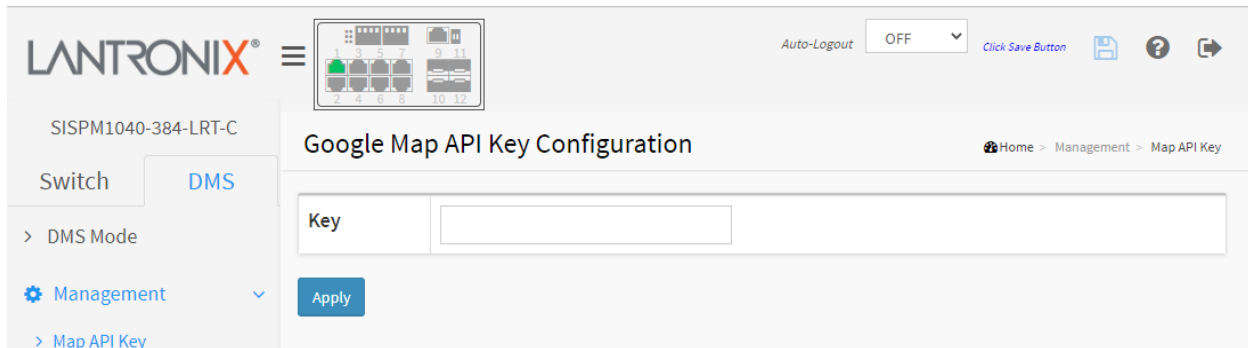
Buttons:

Apply: Click to save the parameter changes.

6-6 Google Map API Key Configuration

This page lets you set up the Google Map API Key in order to use DMS Map View for an enterprise application.

6.6.1 Google Map API Key Configuration



The screenshot shows the Lantronix web interface for the device SISPM1040-384-LRT-C. The page title is "Google Map API Key Configuration". The breadcrumb trail is "Home > Management > Map API Key". The left sidebar shows the navigation menu with "Switch" (DMS) and "Management" (Map API Key) selected. The main content area has a "Key" label and an empty text input field, followed by an "Apply" button. The top right of the interface includes an "Auto-Logout" dropdown set to "OFF", a "Click Save Button" link, and icons for help and refresh.

Key : Specify the Google Map API Key.

6.6.2 Get the Google Map API Key

- 1: Navigate to <https://developers.google.com/maps/documentation/directions/get-api-key>.
- 2: Follow the on-screen instructions.
- 3: For more information refer to the [Google Maps/Google Earth Additional Terms of Service](#) page.

6-7 Device List

You can identify the system by configuring switch contact information, name, and location. To view and set Device List parameters in the web UI:


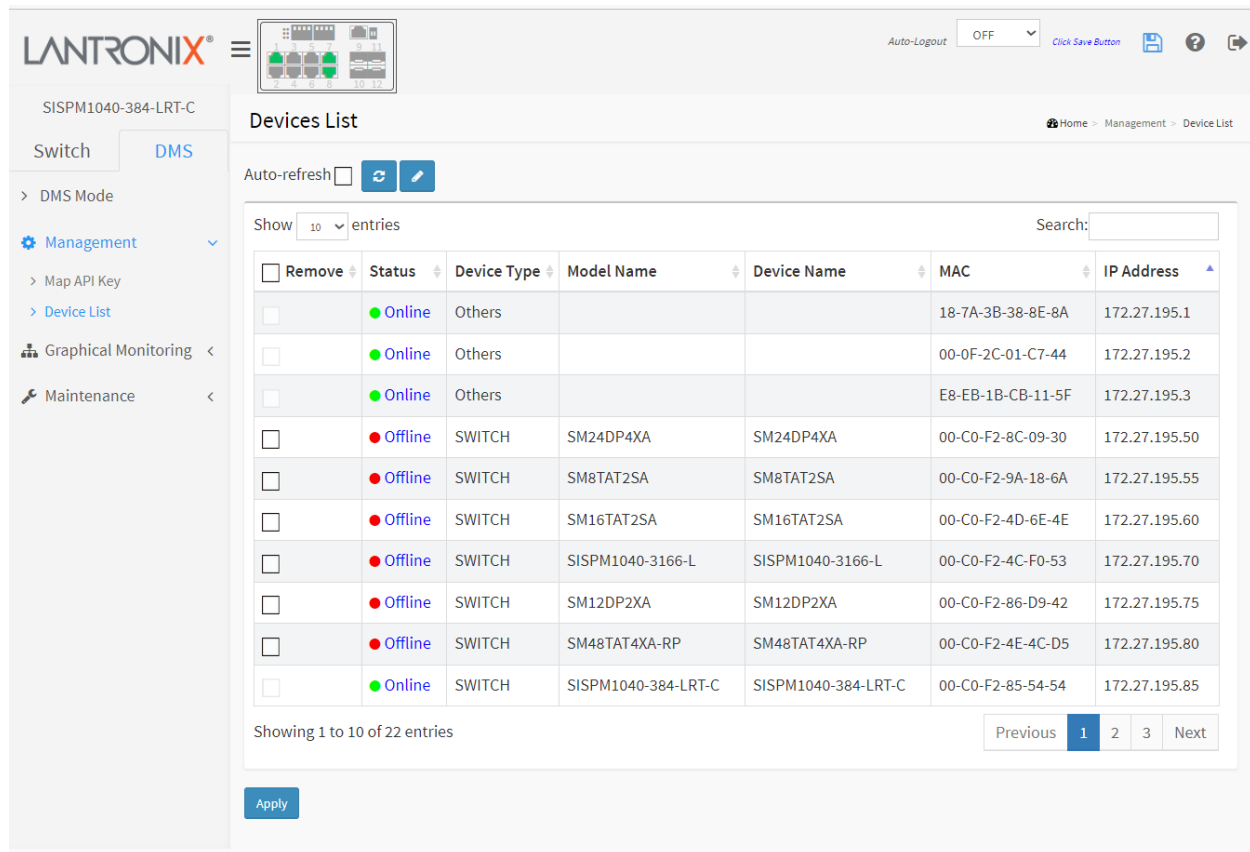
1. Click Management, Device List.
2. Click the Refresh button to refresh the page automatically.
3. Check the Auto-refresh checkbox to refresh the page every three seconds.
4. Click  to display additional fields for editing.
5. Select an Off-Line device to remove
6. In the Status column click an [Online](#) device to run diagnostics.
7. Click the Apply button to save changes.

Figure 6-2: Devices List



The screenshot shows the Lantronix web interface for the device SISPM1040-384-LRT-C. The main content area is titled "Devices List" and features an "Auto-refresh" checkbox and a refresh button. Below this is a table with 10 entries, each with a "Remove" checkbox, "Status" (Online or Offline), "Device Type", "Model Name", "Device Name", "MAC", and "IP Address". The table shows 3 Online devices and 7 Offline devices. At the bottom of the table, it says "Showing 1 to 10 of 22 entries" and includes pagination buttons for "Previous", "1", "2", "3", and "Next". An "Apply" button is located below the table.

Remove	Status	Device Type	Model Name	Device Name	MAC	IP Address
<input type="checkbox"/>	Online	Others			18-7A-3B-38-8E-8A	172.27.195.1
<input type="checkbox"/>	Online	Others			00-0F-2C-01-C7-44	172.27.195.2
<input type="checkbox"/>	Online	Others			E8-EB-1B-CB-11-5F	172.27.195.3
<input type="checkbox"/>	Offline	SWITCH	SM24DP4XA	SM24DP4XA	00-C0-F2-8C-09-30	172.27.195.50
<input type="checkbox"/>	Offline	SWITCH	SM8TAT2SA	SM8TAT2SA	00-C0-F2-9A-18-6A	172.27.195.55
<input type="checkbox"/>	Offline	SWITCH	SM16TAT2SA	SM16TAT2SA	00-C0-F2-4D-6E-4E	172.27.195.60
<input type="checkbox"/>	Offline	SWITCH	SISPM1040-3166-L	SISPM1040-3166-L	00-C0-F2-4C-F0-53	172.27.195.70
<input type="checkbox"/>	Offline	SWITCH	SM12DP2XA	SM12DP2XA	00-C0-F2-86-D9-42	172.27.195.75
<input type="checkbox"/>	Offline	SWITCH	SM48TAT4XA-RP	SM48TAT4XA-RP	00-C0-F2-4E-4C-D5	172.27.195.80
<input type="checkbox"/>	Online	SWITCH	SISPM1040-384-LRT-C	SISPM1040-384-LRT-C	00-C0-F2-85-54-54	172.27.195.85

Parameter descriptions:

Remove: Check the box and click Apply to remove Off-Line devices from the list.

Status: Device link state (Online or Offline). Linked to the device's Diagnostics page.

Device Type: The type of network connectivity devices such as PC, SWITCH, AP, IP Camera, Others.

Model Name: Device model names of the network connectivity devices (e.g., SISPM1040-384-LRT-C).

Device Name: The device name of the network connectivity devices (e.g., SISPM1040-384-LRT-C).

Edit Device Name: Device name edit (save in flash). See the button description below.

MAC: The device's MAC address.

IP Address: Device IP addresses of the network connectivity devices.

Buttons

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



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

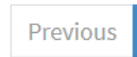


Edit Device Name: Click to display input fields for editing the Device name, HTTP port, User Name, and Password.

Show **entries** **Show # entries:** At the dropdown select how many entries to display per page (10, 25, 60, or All). The default is 10.



Apply: Click to save changes.



Previous: Click to go to the previous page (if one exists).



Next: Click to go to the next page (if one exists).

Search: **Search:** Enter text to display a search on and hit Enter. The search entry will display, or the message "No matching records found Showing 0 to 0 of 0 entries (filtered from 1 total entries)" will display. Click the **x** to exit the search.

Figure 6-3: DMS > Management > Devices List page with Edit columns displayed:

Remove	Status	Device Type	Model Name	Device Name	Edit Device Name	MAC	IP Address	Edit HTTP Port	Edit User Name	Edit User Password
<input type="checkbox"/>	Online	IP Camera	AXOS M3106-LVE Mk II - ACCCB8EADF82A	AXOS M3106-LVE Mk II - ACCCB8EADF82A	<input type="text"/>	AC-CC-8E-AD-F8-2A	169.254.124.69	80	admin	<input type="password"/>
<input type="checkbox"/>	Online	IP Camera			<input type="text"/>	00-09-18-4E-20-E9	192.168.1.4	80	admin	<input type="password"/>
<input type="checkbox"/>	Online	SWITCH	SISPM1040-362-LRT	SISPM1040-362-LRT	SISPM1040-362-LRT	00-C0-F2-49-3D-4F	192.168.1.77			
<input type="checkbox"/>	Online	Others			<input type="text"/>	00-1B-11-82-6D-4B	192.168.1.99			

Figure 6-4: Click an instance in the Status column to run a diagnostic and display the results:

The screenshot shows the 'Diagnostics' page for a device. The left sidebar contains navigation options: Management, Graphical Monitoring, Maintenance (selected), Floor Image, Diagnostics, and Traffic Monitor. The main content area has a breadcrumb trail 'Home > Maintenance > Diagnostics' and a blue 'Another Try' button. Below the button is a table with the following data:

Select	Status	Model Name	Device Name	MAC	IP Address	Version
<input checked="" type="checkbox"/>	Online	AXIS Camera	AXIS M3106-LVE Mk II - ACCC8EADF82A	AC-CC-8E-AD-F8-2A	169.254.124.69	

Below the table, there are two device status indicators. The first is a keyboard icon with IP 192.168.1.77 and MAC 00-c0-f2-49-3d-4f. The second is a camera icon with IP 169.254.124.69 and MAC ac-cc-8e-ad-f8-2a. Between these two indicators, the connection status is shown as 'Connection.....' and 'Cable status.....', both with green checkmarks.

Click the **Another Try** button to go back to the Devices List page.

See section [6.9 DMS > Maintenance > Diagnostics](#) on page [445](#) below for more information.

6.8 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.

The screenshot shows the Lantronix web interface for the Floor Image Management page. The page title is "Floor Image Management" and the breadcrumb trail is "Home > Maintenance > Floor Image". The system information at the top left is "SISPM1040-384-LRT-C". The navigation menu on the left includes "Switch", "DMS", "DMS Mode", "Management", "Graphical Monitoring", "Maintenance", "Floor Image", "Diagnostics", and "Traffic Monitor". The main content area displays file management statistics: "Maximum: 10 files", "Used: 0 file(s)", and "Free: 10 file(s)". Below this is an "Add Floor Image" section with a "Choose File" button and a "Name" input field. A table below the form shows columns for "Select", "No.", "File Name", and "Image", with the message "No information found" displayed. A "Delete" button is located at the bottom of the table.

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 restore 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.

Choose File : Click the button to navigate to and select an image from the list.

Name : Shows file name selected; only jpg and png file formats are allowed. Special characters are not allowed in the Name field.

Select : Check or uncheck the selection checkbox for action.

No. : The number of the floor image instance.

File Name : The name of the file selected (e.g., *FloorPlan 1stFloor (192.168.1.77)*).

Image : A thumbnail of the Floor Image file.

Buttons

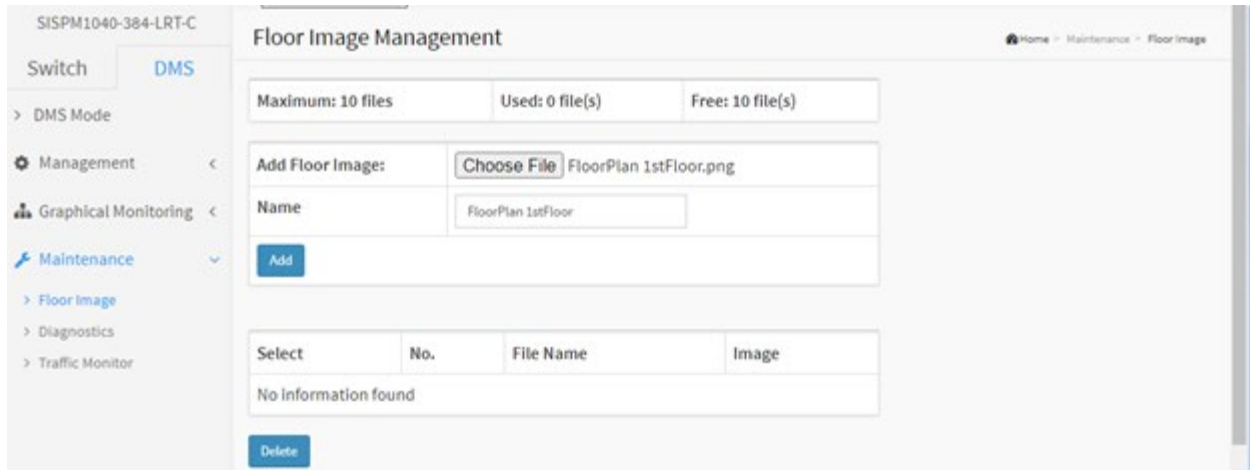
Add: Click Add to upload. When done, a snapshot will be available on screen.

Delete: To remove an existing floor map, select its checkbox and click Delete to remove.

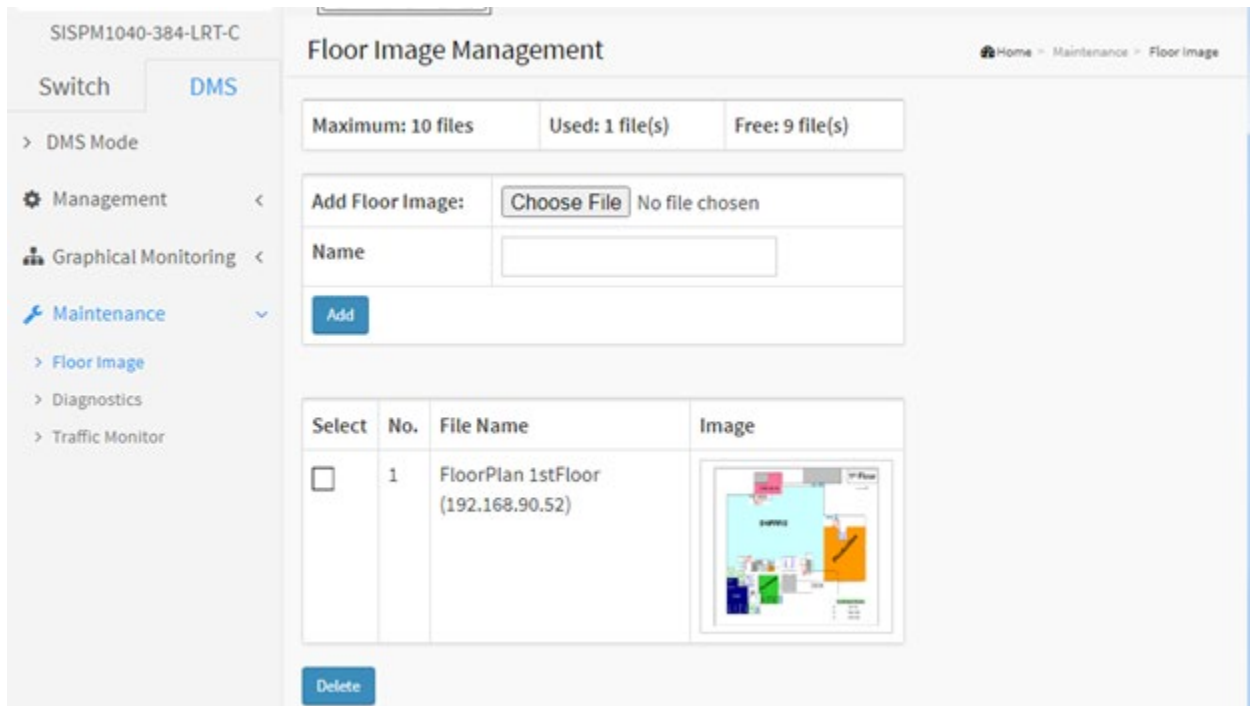
Message: File size is too big. Only 524152 bytes is available.

Examples:

A Floor Image file selected:



Selected Floor Image file added:



Three Floor Image files added:

The screenshot displays the 'Floor Image Management' interface. At the top, it shows 'Maximum: 10 files', 'Used: 3 file(s)', and 'Free: 7 file(s)'. Below this is an 'Add Floor Image' section with a 'Choose File' button and a 'No file chosen' message. A 'Name' input field is also present. A table lists the three added files, 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	FloorPlan 1stFloor (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)	

6.9 DMS > Maintenance > Diagnostics

This page provides an overview of the Diagnostics and lets you run a Connection and Cable status diagnostic.

Select	Status	Model Name	Device Name	MAC	IP Address	Version
<input type="checkbox"/>	Online			00-08-E3-FF-FC-28	192.168.90.1	
<input type="checkbox"/>	Online			00-C0-F2-00-99-DC	192.168.90.103	
<input type="checkbox"/>	Online			00-C0-F2-44-AC-EE	192.168.90.2	
<input type="checkbox"/>	Online	SM16TAT2DPA	SM16TAT2DPA	00-C0-F2-46-87-38	192.168.90.4	v6.46.1860
<input type="checkbox"/>	Online	SM8TAT2SA	SM8TAT2SA	00-C0-F2-47-A6-F8	169.254.212.71	v1.02.1476
<input type="checkbox"/>	Online	SISPM1040-3248-L	SISPM1040-3248-L	00-C0-F2-4C-43-A2	192.168.90.51	v8.40.428
<input type="checkbox"/>	Online			00-C0-F2-56-0E-FC	192.168.90.55	
<input type="checkbox"/>	Online			00-C0-F2-56-15-20	192.168.90.156	
<input type="checkbox"/>	Online			00-C0-F2-56-16-40	192.168.90.155	
<input type="checkbox"/>	Online			00-C0-F2-56-16-58	192.168.90.154	

Parameter descriptions:

Select : Check the box to select a device on which to run its Connection and Cable status diagnostic.

Status : Device Online or Offline.

Model Name : The model name of the network connectivity devices.

Device Name : The device name of the network connectivity devices.

MAC : The mac address of the device.

IP Address : The IP address of the network connectivity devices.

Version : The Version of the network connectivity devices.

Buttons

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

Search : Search for any key word you want.

Another Try : Click to leave the Diagnostics result page and go back to the DMS > Maintenance > Diagnostics page.

At DMS > Maintenance > Diagnostics, check the **Select** checkbox to run a Connection and Cable status diagnostic:

The screenshot displays the 'Diagnostics' page in the web interface. The left sidebar shows the navigation menu with 'Maintenance' selected. The main content area features a table with the following data:

Select	Status	Model Name	Device Name	MAC	IP Address	Version
<input checked="" type="checkbox"/>	Online			00-C0-F2-00-99-DC	192.168.90.103	

Below the table, there are four detailed diagnostic entries, each with a 'Connection.....' and 'Cable status.....' indicator, both showing green checkmarks:

- 192.168.90.52 00-c0-f2-49-45-81
Connection..... ●
Cable status..... ●
- 192.168.90.4 00-c0-f2-46-87-38
Connection..... ●
Cable status..... ●
- 192.168.90.51 00-c0-f2-4c-43-a2
Connection..... ●
Cable status..... ●
- 192.168.90.103 00-c0-f2-00-99-dc
Connection..... ●
Cable status..... ●

Click the **Another try** button to the DMS > Maintenance > Diagnostics page.

Diagnostics Results:

Connection..... ● : The connection diagnostic was successful (green dot).

Connection..... ● : The connection diagnostic was unsuccessful (red dot).

Cable status..... ● : The cable status diagnostic was successful (green dot).

Cable status..... ● : The cable status diagnostic was unsuccessful (red dot).

Chapter 7 DMS > Graphical Monitoring

7-1 Topology View

This page displays a graphical view of the network cluster topology. DMS can automatically discover all IP devices and display the devices in graphic networking topology view. You can manage and monitor devices in Topology View (e.g., remotely diagnose the cable connection status, auto alarm notifications of critical events, remotely reboot PoE device when it's not alive). You can use the DMS platform to solve abnormal issues anytime and anywhere by tablet or smart phone.

To configure DMS Topology View in the web UI:

1. Click DMS, Graphical Monitoring, and Topology View.


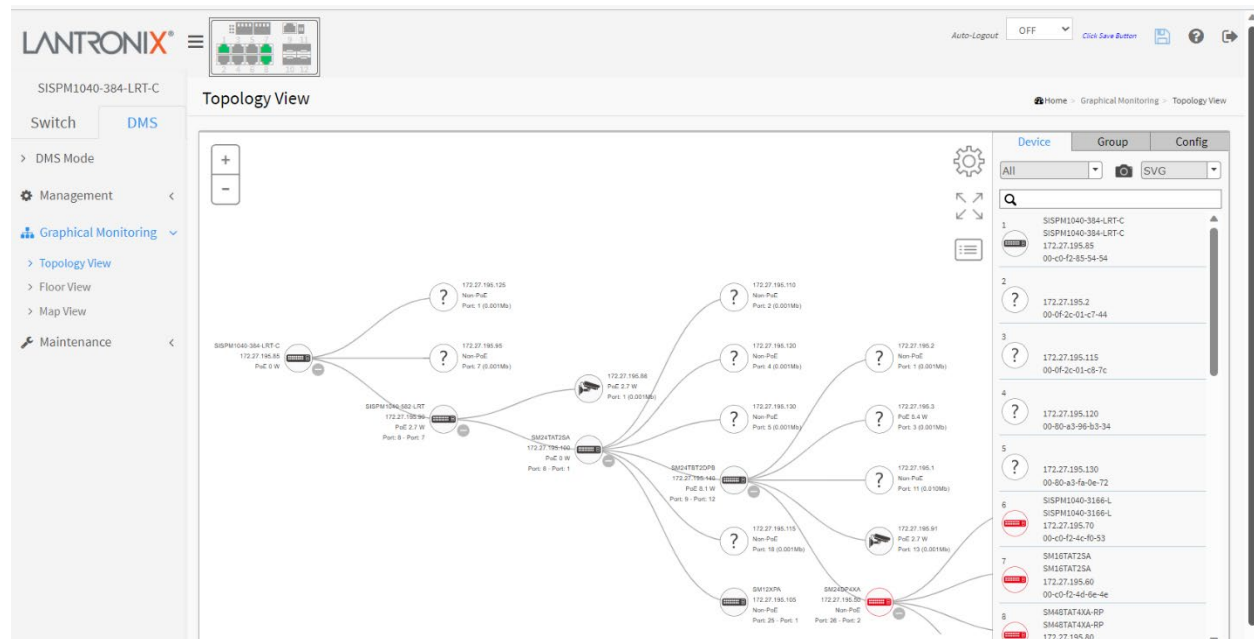
2. Click the  icon to select the display the Device, Group, and Config tabs.

Figure 7-1: Topology View




The Device search console displays all devices and their related information.



A : Filter devices by device type.

B : Search devices by key words full text search.

C : Save the whole view to an SVG (Scalable Vector Graphics) file.

Click the  icon again to hide the popup.

Parameter descriptions:

Login : Login to this device

Trouble shooting : Move to the troubleshooting page.

Find my switch : Allows administrators to quickly and easily find the Switch in their cabinet.

Reboot Device : Reboot the PD device.



Device Type : Select Device Type (PC, IP phone, IP cam, AP, or other device).

Control descriptions:



: Use the directional pad to scroll up, down, left, or right.



: Use the  to zoom in; use the  to zoom out. You can also use the mouse to navigate by clicking and dragging the left mouse button. Use the mouse wheel to zoom in/out.



SVG

: Save the whole View to SVG, PNG or PDF.

All

: Select the device category.





: Search for device by typing IP/MAC address or Model/Device name.



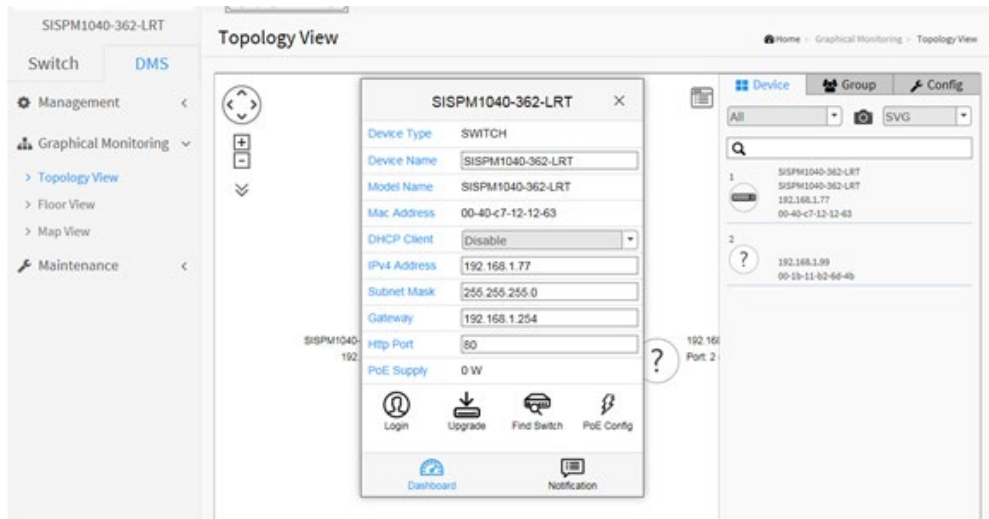
: Click to view / select the view options (Device Name, Model Name, Mac, IP, and/or PoE).



The  icon changes to  which you can click to clear the view options.

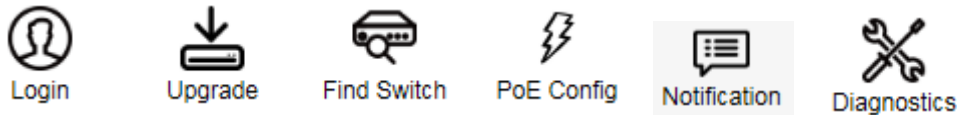
Topology View > Dashboard

Left mouse click a device to display its dashboard.



The information displayed includes Device Type, Device Name, Model Name, MAC Address, DHCP Client state, IPv4 Address, Subnet Mask, Gateway, Http Port number, and PoE Supply power.

The icons displayed include Login, Upgrade, Find Switch, PoE Config, and Notification:



Login: Click to return to the Switch > Monitor > System > Information page.

Upgrade: Lets you select a device and enter a Tftp Server IP address and a File name to upgrade to.

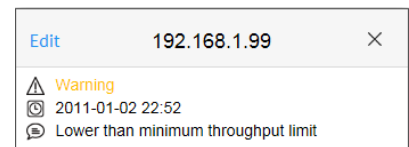
Find Switch: Lights the switch front panel LEDs momentarily.

PoE Config: Lets you configure PoE Mode and PoE Auto Checking (APR).

Notification: Displays any messages (e.g., *Lower than minimum throughput limit*). Otherwise displays "No message."




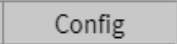
For a Device Type of "Unknown" a Diagnostics icon also displays.

Diagnostics : Click the icon to display Connection and Cable status.












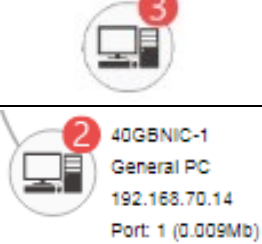






Icons / Controls

Click anywhere and drag to move the display area up /down/ left /right.

	<p>Click "+" or "-" to zoom in or zoom out the display area.</p>
	<p>Click to alternately display / hide the Device tab.</p>
	<p>Click this icon to select the set of data to be displayed (MAC, IP, PoE power, etc.).</p>
	<p>Click this icon to sort, filter, or configure basic settings (e.g., VLAN, QoS).</p>

Device Categories and Statuses

	The device is a Switch.
	The device is a general switch.
	The device is a 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.
	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.
 40GB NIC-1 General PC 192.168.70.14 Port: 1 (0.009Mb)	A Red circled device number shows the number of alarm notifications for the device.
	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.

	Icon with question mark and red N:indicates the device is not connected.
 <p>40GBNIC-1 General PC 192.168.70.14 Port: 1 (0.009Mb)</p>	A Black device icon indicates device is operating normally. Click device icon to show its device console.
 <p>SISPM1040-384-LRT-C 192.168.1.77 Port: 1 - Port: 7</p>	A Red device icon indicates the device is operating abnormally.

7-2 Floor View

This page lets an administrator place a device per time onto the custom image, which you have already uploaded (at DMS > Maintenance > Floor Image) by dragging-and-dropping markers in the device list. Ten maps can be stored per switch.

To configure DMS Floor View in the web UI:

1. Click DMS, Graphical Monitoring, Floor View.

Figure 7-2: Floor View



Control descriptions:



: Use the directional pad to scroll up, down, left, or right.

Use the to zoom in; use the to zoom out. You can also use the mouse to navigate by clicking and dragging the left mouse button. Use the mouse wheel to zoom in/out.

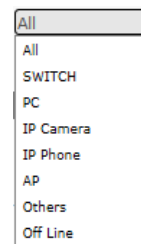


SVG

: Save the whole View to SVG, PNG or PDF.

All

: Select the device category to display (All, SWITCH, PC, IP Camera, IP Phone, AP, Others, Off Line).



: Search for device by typing IP/MAC address or Model/Device name.

Device Status



Green icon with black mark: Device link up. User can select function and check issues.



Red icon with red mark: Device link down. User can diagnose the link status.

Example: Click and drag the device icons to their desired locations:

The screenshot displays the 'Floor View' interface for the SISPM1040-384-LRT-C system. The main area shows a floor plan of the 1st floor with several rooms labeled: SHIPPING (light blue), Production (orange), DOCK, and Conference Rooms (1.1, 1.2, 1.3). There are several green location pin icons with black dots placed on the floor plan, indicating devices that are 'link up'. A right-hand panel shows a list of devices with their IP addresses and MAC addresses. The list is as follows:

Entry	Config
All	SVG
FloorPlan 1stFloor (192.168.90.52)	
Q	
1	SISPM1040-384-LRT-C SISPM1040-384-LRT-C 192.168.90.52 00-c0-42-48-45-02
2	192.168.90.1 00-08-43-8f-0c-28
3	192.168.90.101 00-c0-42-00-99-0c
4	192.168.90.2 00-c0-42-44-ec-ee
5	SH8TAT209A SH8TAT209A 192.168.90.4 00-c0-42-46-07-38
6	SH8TAT25A SH8TAT25A

7-3 Map View

Map View helps you find the location of the devices even if they are installed in different buildings. This page lets you view a realistic representation of device in the network. To find one of devices within the network, enter the device name in the search bar. Click "Device List" to hide the "Device List" on the page or show a list of devices. To configure DMS Map View in the web UI:


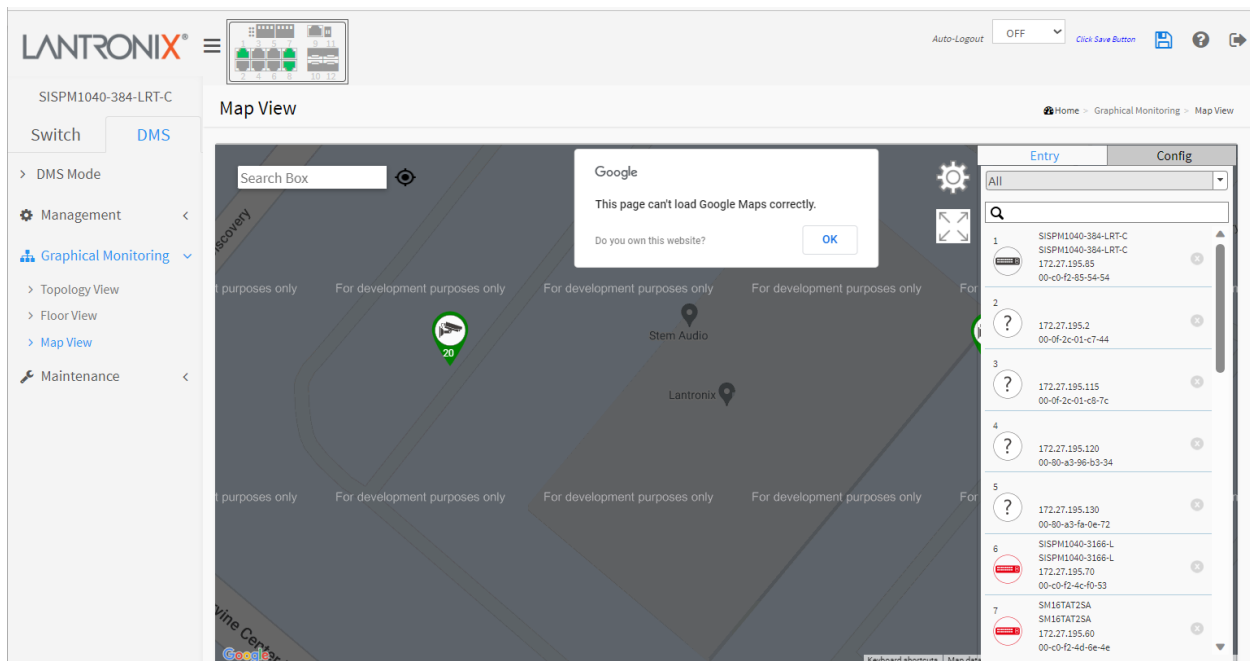


1. Click DMS, Graphical Monitoring, and Map View.
2. At the prompt, select "Allow Once".
3. Select Map or Satellite view.
4. Click the "Setting" icon () in the upper right corner; the Device Config will pop-up, with advanced search functions for the device.

Figure 7-3: Map View



: Use the directional pad to scroll up, down, left, or right.



: Use the  to zoom in; use the  to zoom out. You can also use the mouse to navigate by clicking and dragging the left mouse button. Use the mouse wheel to zoom in/out.



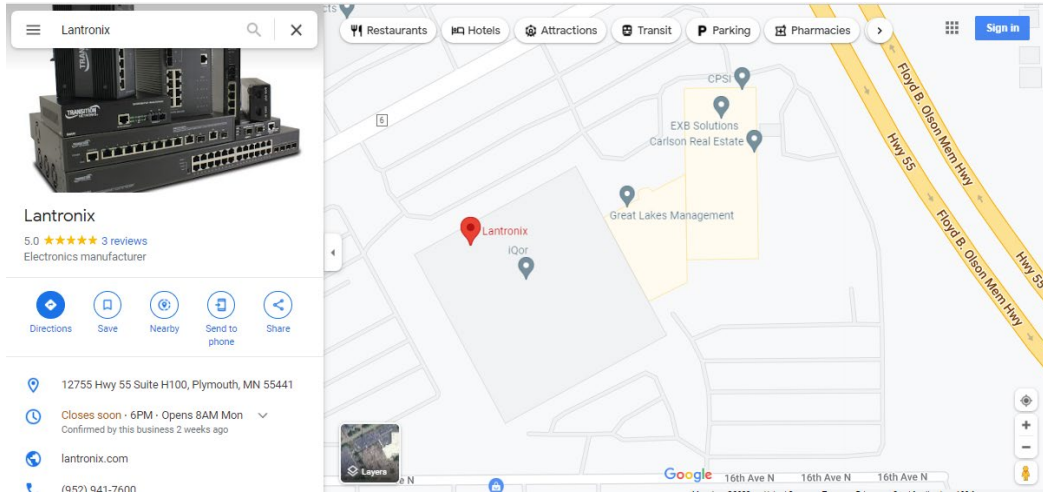
: Select the device category to display (All, SWITCH, PC, IP Camera, IP Phone, AP, Others, Off Line).



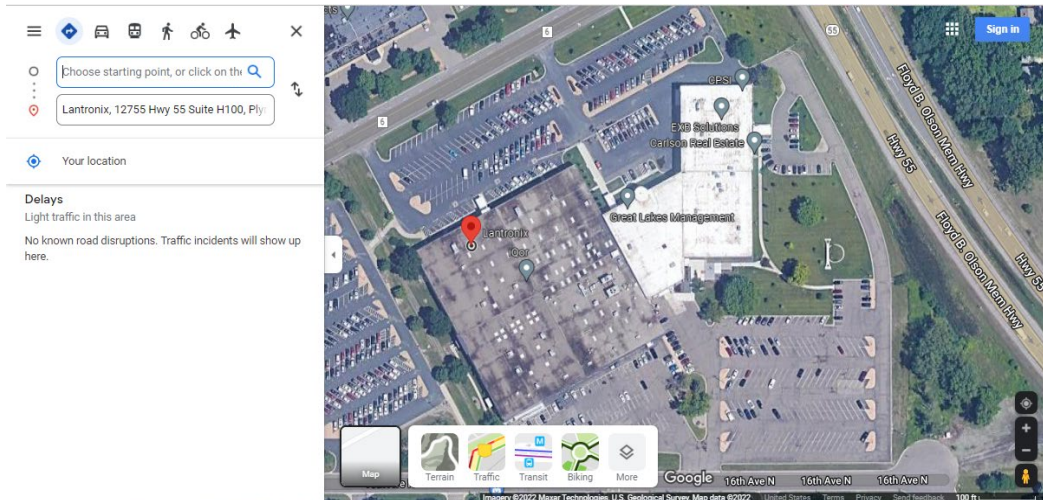
: Search for device by typing IP/MAC address or Model/Device name.

If the message "This page can't load Google Maps correctly." displays see section [6.6.1 Google Map API Key Configuration](#) on page [437](#) .

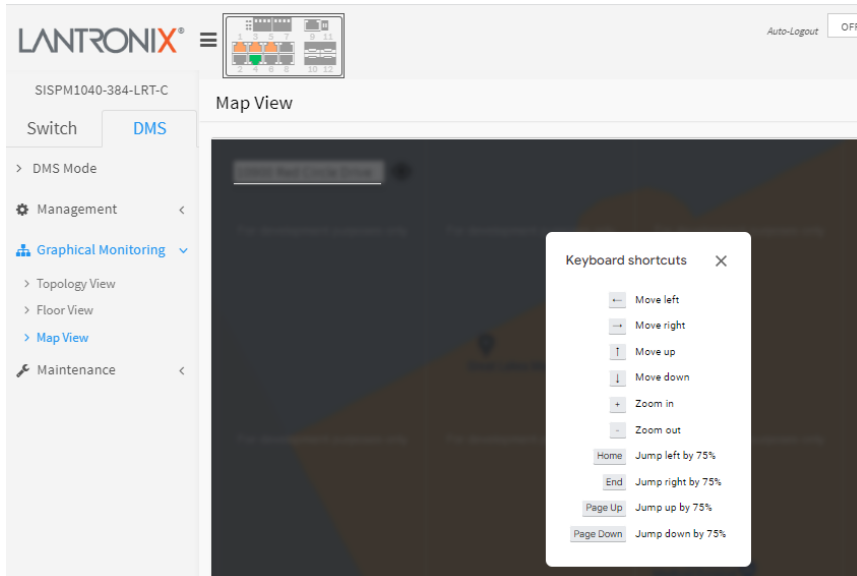
Example 1:



Example 2:



Click Keyboard shortcuts button in the lower right corner to display the keyboard shortcuts:



Chapter 8. DMS > Maintenance

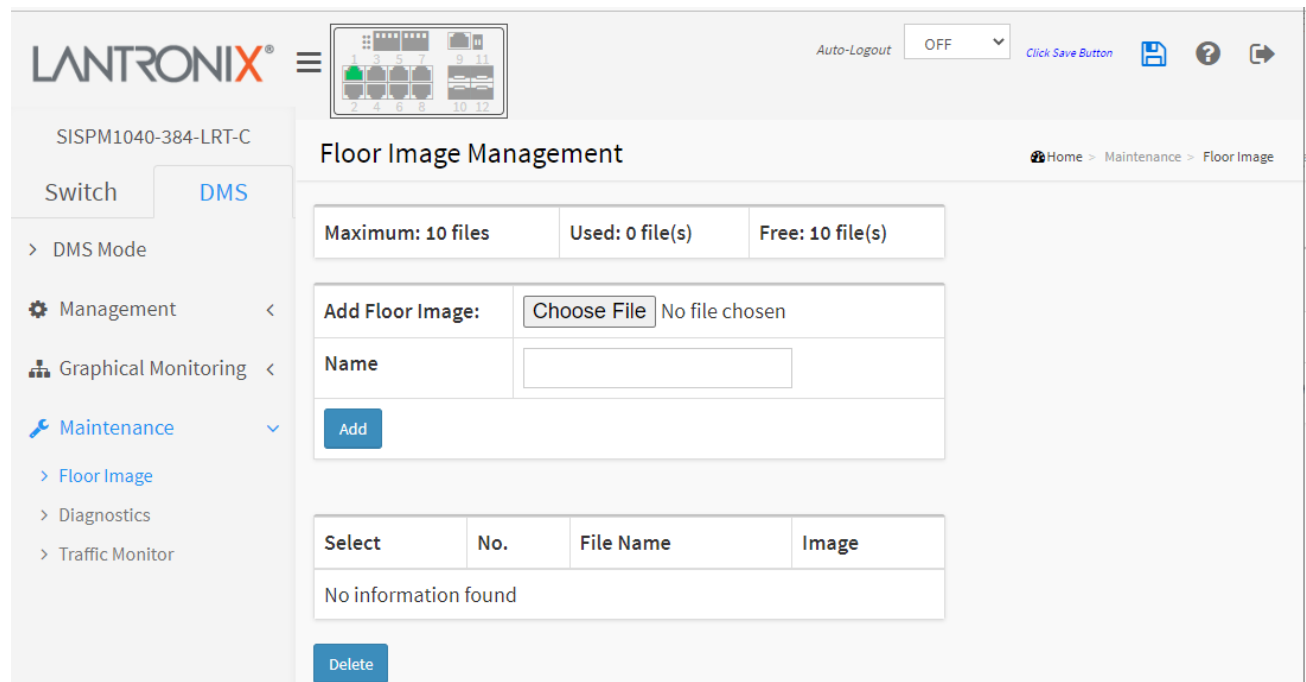
8-1 Floor Image

This page lets you add or delete a custom map or floor image. Here you can upload or manage floor map images. Up to 20 JPEG images, with a maximum of 256KB each, can be uploaded to the switch.

To configure floor image in the web UI:

1. Click DMS, Maintenance, and Floor Image.
2. Click "Browse..." to select a Floor image in your device.
3. Click Add.

Figure 8-1a: Floor Image (default)



Parameter descriptions:

Maximum: The maximum number of files that you can add (10 files).

Used: The number of files that you have added so far (e.g., 2 file(s)).

Free: The number of files that you can still add (e.g., 8 file(s)).

Add Floor Image: Click the **Choose File** button, then select and open a supported graphics file.

Name: The selected filename displays in the Name field and in the Image field.

Select: Check the box to select an instance to delete.

No.: The image instance number (1-10).

File Name: The filename of the image instance.

Image: A thumbnail of the image instance.

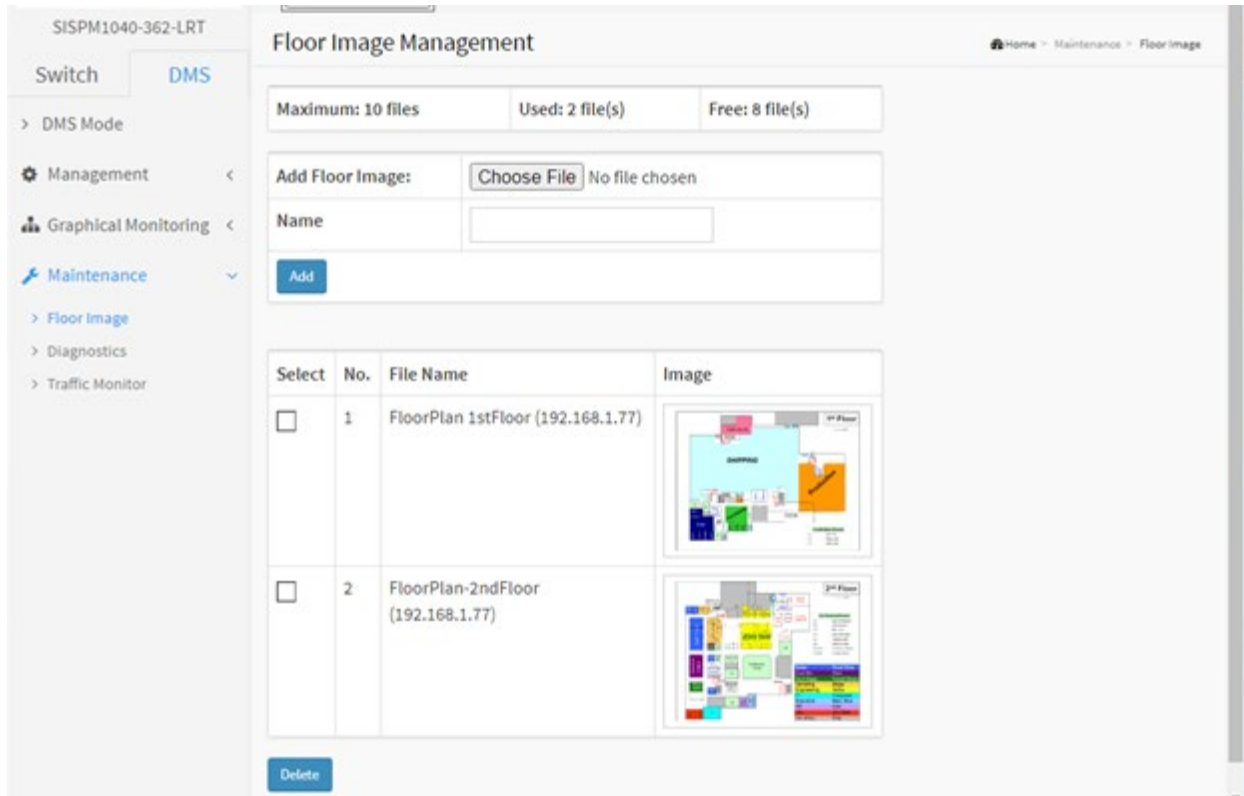
Buttons:

Add: Click to add the selected image file to the table. When done, a snapshot displays on screen.



Delete: Click to delete a selected image file from the table.

Browse: Click to open a window to browse to and select a Floor image in your device.

Figure 8-1b: Floor Image with 2 images added



The screenshot displays the 'Floor Image Management' web interface. On the left is a navigation sidebar with 'Maintenance' expanded to 'Floor Image'. The main area shows a status bar with 'Maximum: 10 files', 'Used: 2 file(s)', and 'Free: 8 file(s)'. Below this is an 'Add Floor Image' section with a 'Choose File' button and a text input field. A table below contains two entries:

Select	No.	File Name	Image
<input type="checkbox"/>	1	FloorPlan 1stFloor (192.168.1.77)	
<input type="checkbox"/>	2	FloorPlan-2ndFloor (192.168.1.77)	

A 'Delete' button is located at the bottom left of the table area.

Message: Only jpg, png are allowed

8-2 Diagnostics

This page lets you troubleshoot issues with device connected to the network. This feature is designed primarily for administrators to verify and test the link route between the switch and the device.

Here you can detect where the problem lies for a selected device. Note that the network topology must be saved for this function to work properly.

To run DMS diagnostics via the web UI:

1. Click DMS, Maintenance, Diagnostics.
2. Check a box in the Select column for a device to start the diagnostic.
3. Observe the device, connection, and cable status information displayed.

Figure 8-2: Diagnostics in progress

The screenshot shows the Lantronix web interface for the SISPM1040-384-LRT-C switch. The 'Diagnostics' page is active, showing a table of devices. The table has columns for Select, Status, Model Name, Device Name, MAC, IP Address, and Version. One device is listed with a checked 'Select' box and a green 'Online' status. Below the table, there is a visual representation of the network topology showing the connection and cable status for the selected device.

Select	Status	Model Name	Device Name	MAC	IP Address	Version
<input checked="" type="checkbox"/>	Online	General PC	MINNW1074	5C-FF-35-DC-0A-C1	192.168.1.75	

Showing 1 to 1 of 1 entries

Previous 1 Next

Visual representation of network topology:

- 192.168.1.77 00-c0-f2-49-be-22
- Connection.....*
- Cable status.....*
- 192.168.1.75 5c-ff-35-dc-0a-c1

Parameters:

Select: Select a device from the list to start its diagnostic.

Status: Device status; either Online or Offline.

Model Name: The model names of the network connectivity devices.

Device Name: The device names of the network connectivity devices.

MAC: The MAC address of each device.

IP Address: The IP address of the network connectivity devices

Version: The Version of the network connectivity devices, if available.

Buttons:

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

Search: Enter any key word you want to search for.

Another Try: Click to leave the current selection and select another device on which to start the recovery mechanism.

Status information displays as shown below:

The screenshot shows the Lantronix web interface for the SISPM1040-384-LRT-C device. The main content area is titled "Diagnostics" and features a table of device status information. The table has columns for Select, Status, Model Name, Device Name, MAC, IP Address, and Version. The first entry is selected, and its status is "Offline". Below the table, there is a graphical representation of the network topology, showing a central switch connected to several devices. The status of each connection and cable is indicated by green checkmarks or red X's.

Table Data:

Select	Status	Model Name	Device Name	MAC	IP Address	Version
<input checked="" type="checkbox"/>	Offline	SISPM1040-3166-L	SISPM1040-3166-L	00-C0-F2-4C-F0-53	172.27.195.70	v8.50.0032

Showing 1 to 10 of 21 entries

Navigation: Previous | 1 | 2 | 3 | Next

Graphical Representation:

- Device 1: 172.27.195.85, MAC 00-c0-f2-85-54-54. Connection: ✓, Cable status: ✓
- Device 2: 172.27.195.90, MAC 00-c0-f2-82-3e-8b. Connection: ✓, Cable status: ✓
- Device 3: 172.27.195.100, MAC 00-c0-f2-9a-b6-28. Connection: ✗, Cable status: ✗
- Device 4: 172.27.195.140, MAC 00-c0-f2-83-83-28. Connection: ✗, Cable status: ✗
- Device 5: 172.27.195.50, MAC 00-c0-f2-8c-09-30. Connection: ✗, Cable status: ✗
- Device 6: 172.27.195.70, MAC 00-c0-f2-4c-f0-53. Connection: ✗, Cable status: ✗

8-3 Traffic Monitor

DMS supports traffic monitoring of each port and keeps a one-week record that can be used to compare and analyze through visual charts. The page displays two different graphs for a selected device.

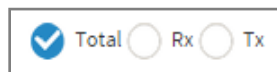
This page displays a chart of network traffic of all the devices. You can view the traffic of all ports or a specific port. Click on specific port on the traffic chart to reveal its traffic during the day. You can select to display a summary of one day or a week of traffic by selecting the check circle on top. The same applies to the selection of Tx, or Rx traffic, or a total of both. A single port's traffic is shown at the lower half of the screen.

Procedure

1. Click DMS > Maintenance > Traffic Monitor.
2. Select the parameters to display.
3. Select the device to monitor.



Parameter descriptions:



Total / Rx / Tx: Select the set of data to be displayed.



< yy/mm/dd >: Select the date of data displayed. This is the time set at Switch > Configuration > System > Time or at Switch > Configuration > System > NTP.

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 throughput (e.g., 0 M – 18000 M or 0 M-1200 M). The unit of measure is Mbps.

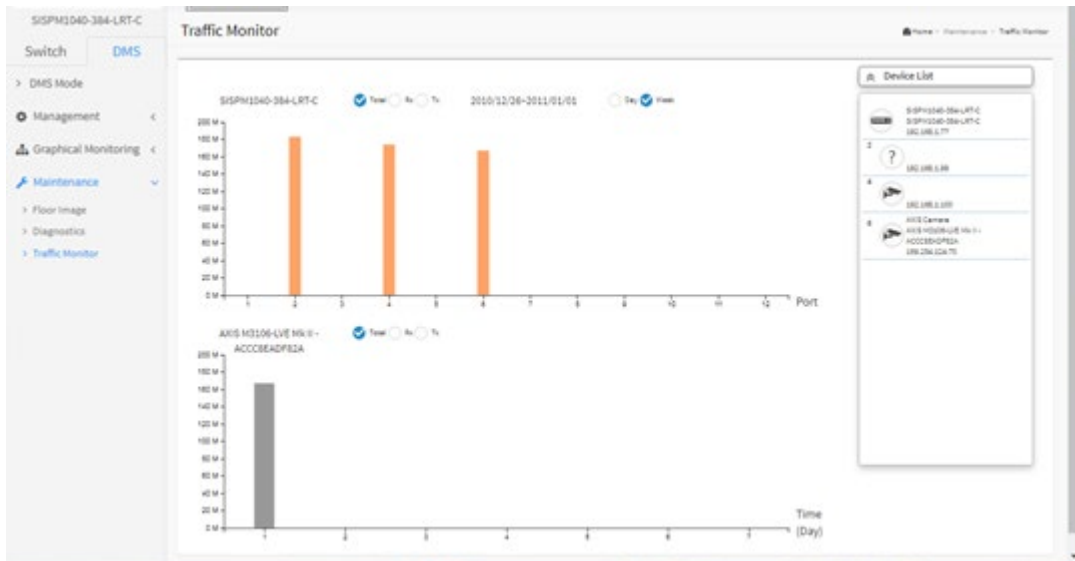
Port: Horizontal axis shows the switch port numbers.

Time (Hour): Horizontal axis shows the time elapsed in hours (0-23).

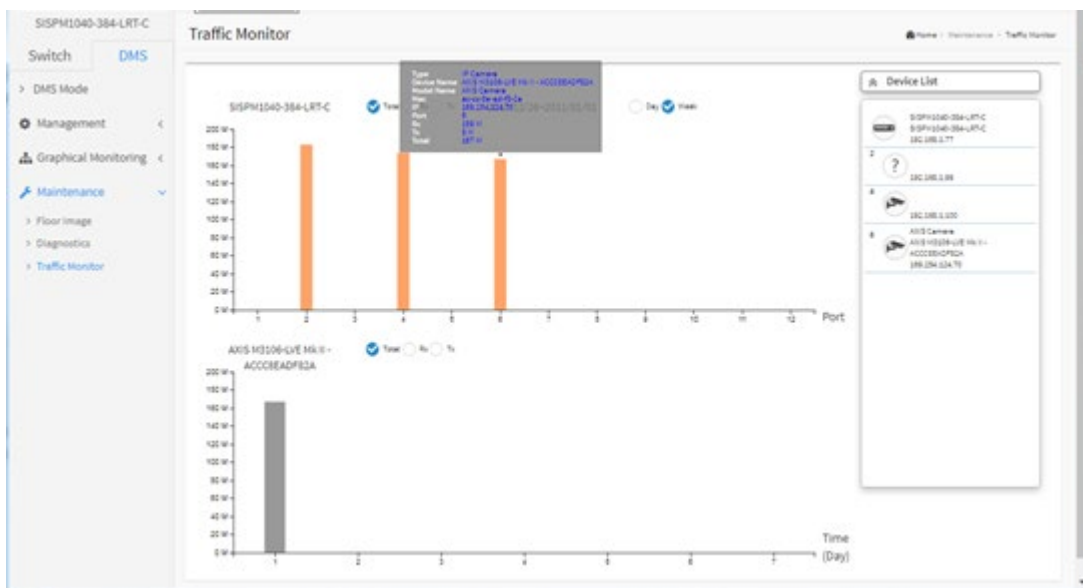
The graph's vertical axis shows throughput and the unit of measure is Mbps.

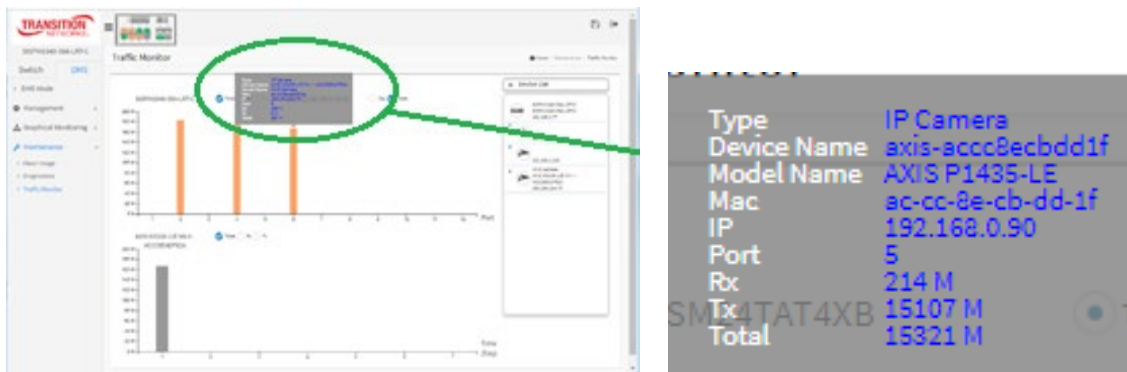
DMS Traffic Monitor Operation

1. Navigate to DMS > Maintenance > Traffic Monitor.



2. Select a device to monitor.
3. Hover the cursor over a column in the graph to view its details.





4. Click the graph column to display its axis information in the lower graph table.

Message: Traffic Monitor feature is only available on master controller.

Current master controller IP Address:0.0.0.0

Meaning: The switch must be the Master (Controller) switch (added at FW v 7.10.2307).

Recovery: Click the OK button and make this switch the Master (Controller) switch. See section “6-5 DMS Mode” on page 436.

Bandwidth vs Throughput vs Network Throughput

Bandwidth: the maximum amount of data that can go through a given medium.

Throughput: the amount of data that actually goes through that medium.

Network throughput: the amount of data that is transmitted through a given network medium over a given amount of time.

Throughput Units of Measurement

Bit: The smallest size of binary information used by computer devices (the ones and zeros in binary)

Byte: 8 bits

Megabit: 1 million bits

Megabyte: 1 million bytes

Gigabit: 1 billion bits

Gigabyte: 1 billion bytes

Mbps: Megabits per second

MBps: Megabytes per second

Gbps: Gigabits per second

GBps: Gigabytes per second

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.




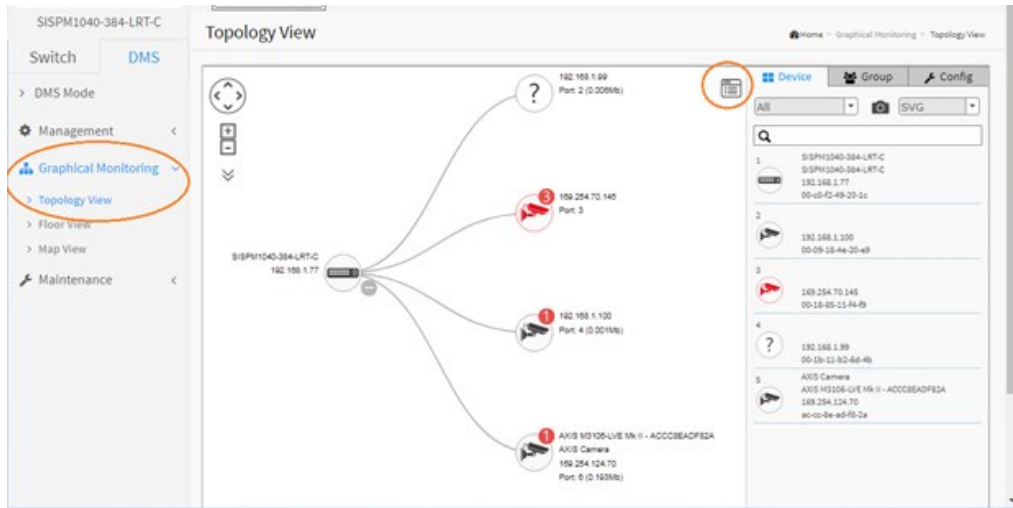
4. Click the PoE Config (PoE Config) icon to display the PoE Auto Checking pane.



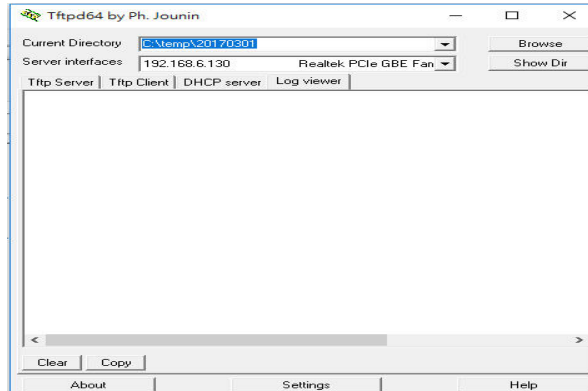
5. At the PoE Auto Checking dropdown select Enable.
6. Click the Apply button.

DMS Firmware Upgrade Procedure

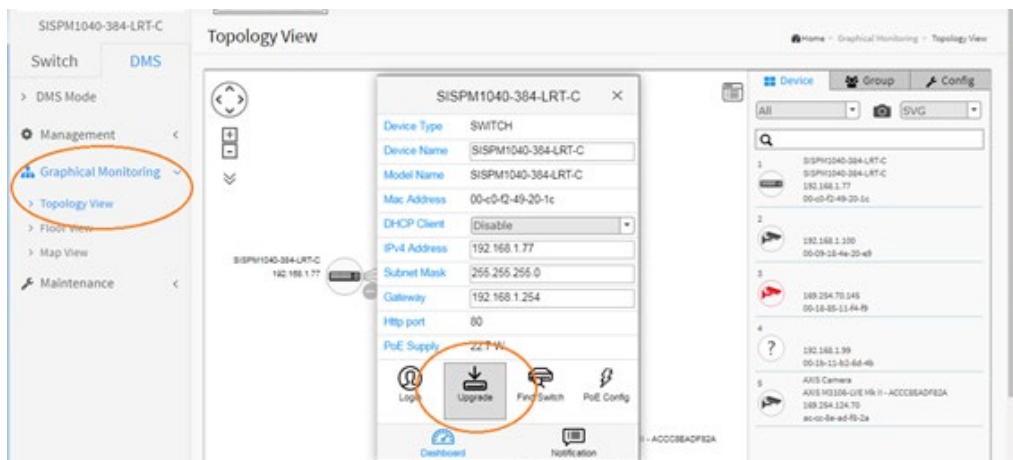
1. Navigate to the DMS > Graphical Monitoring > Topology View menu path.
2. Click the  button to display the right pane menu tabs (Device, Group, and Config).
3. Connect all switches and make sure DMS discovers and displays them.
 - Set all switches with different IP addresses and in the same IP segment.
 - Make sure gateway IP address is configured.



4. Enable the TFTP server and set the correct image path.



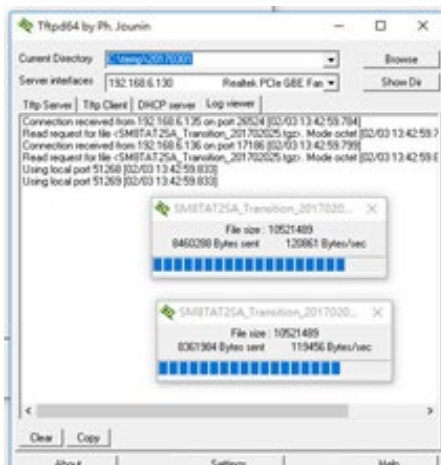
5. Click the switch icon, and then click the "Upgrade" button in the Dashboard.



- Enter the TFTP server IP address and FW file name and select the switch on which you want to upgrade the FW.



- Click "Apply" to start the FW upgrade and save to Running-config.
- Observe the upgrade status until completion.



Messages

Starting, please wait...

Error : Firmware download fail

8-4 Troubleshooting DMS

Problem: The switch lists itself as the only device in Topology View of DMS.

Problem: In DMS, the Local image shows the IP address of another switch.

Description: The switch is listed as only device in DMS Topology View in DMS; all devices are listed in DMS device list. This is usually because the switch's gateway is not configured appropriately.

Resolution: An IP Route must be configured manually. For example, a switch IP address of 192.168.1.77 should have the following IP route configured: `ip route 0.0.0.0 0.0.0.0 192.168.1.x`. Without the IP route configured, you may be unable to view all devices on the network in DMS.

1. Go to DMS > Management > DMS Mode to check if the controller IP is correct.
2. Verify that the gateway of this switch is correctly configured.
3. Verify that all connected devices are displayed in DMS Topology View.

Problem: DMS Connectivity diagnostics fails to ICMP reachable device.

Description: DMS displays a device which is reachable via ICMP ping as failing the connection status in diagnostics. Cable status displays as *OK*.

Resolution: Contact Technical Support.

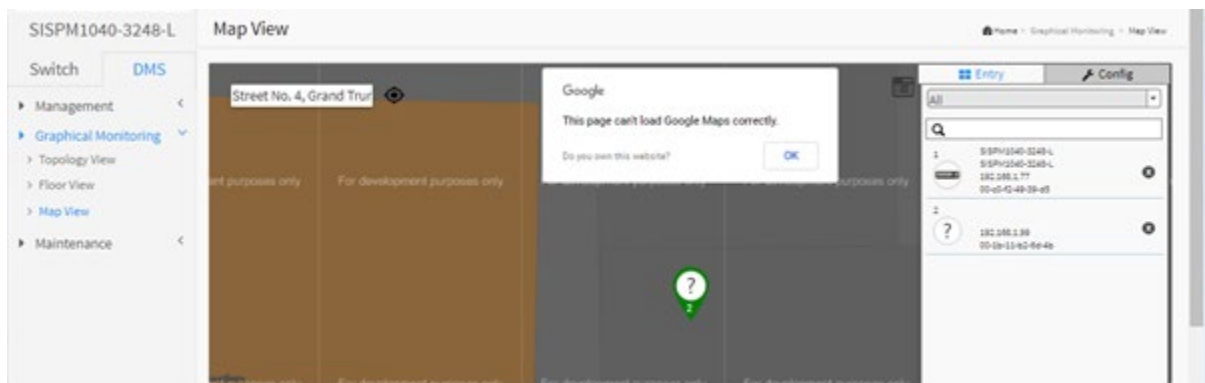
Problem: DMS will discover the device type, name and model of some cameras and hosts but others are displayed as *Unknown*.

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 does not issue any of these previously- 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.* Displays at DMS > Graphical Monitoring > Map View.

Resolution: 1. Click the OK button to clear the message. 2. See [Get the Google Map API Key](#) on page 436.



Appendix A: Rapid Ring Operation

A-1 Rapid Ring Operation

Rapid Ring is a proprietary redundancy network ring protocol. It can be used to recover the network from critical link failure to provide fault failover protection.

Many redundant or network recovery protocols are defined by IEEE, such as spanning tree (STP, RSTP, MSTP) are available to recover the network from link failures. But the recovery time to propagate broadcast packets to the failover port can take several seconds, depending on the amount of network traffic. Rapid Ring recovery is less than 20ms for up to 250 switches.

The SISPM1040-384-LRT-C and SISPM1040-362-LRT support four types of ring topology:

- Single Ring
- Ring to Ring
- Dual Ring
- Rapid Chain

The four types of Rapid Ring and how to configure them is described below.

Note: Only one redundant protocol can be used at the same time. Before you enable Rapid Ring, you must disable Spanning Tree.

A-1-1 Single Ring

Single Ring can be used to recover the network if a critical link failure occurs. With Single Ring, one of the switches must be configured as the “Master” and the other switches as Members of the single ring. Each switch will have a forwarding path and a backup path on the Ring Master. If one link fails, the ring will automatically activate the backup path within 20ms.

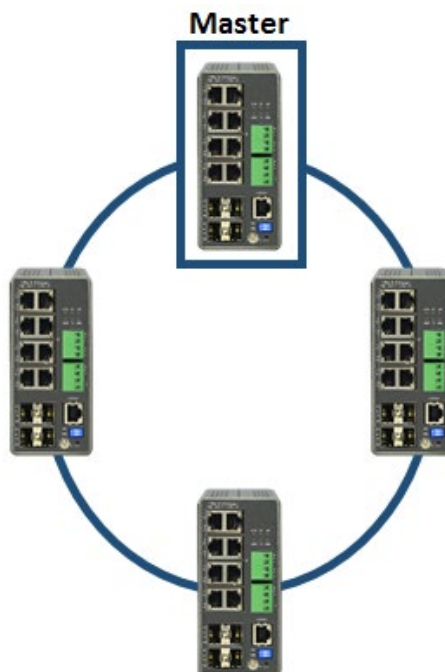


Figure 1: Single Ring

Single Ring configuration is shown and described below.

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

Figure 2: Single Ring Configuration

- Configure the Role as **Master** or **Member**. Only one switch in the single ring can be the Master and rest of the switches must be set as Members of the single ring.
- Configure 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 will be the backup path.
- If it is a Member, 1st Ring Port and 2nd Ring Port is used to connect the link partner of the Single Ring.
- Indicates port status (e.g., Forwarding, Discarding, etc.).

A-1-2 Ring to Ring

Ring to Ring is a flexible application that connects several single rings together. Since some devices could be located in a remote area, it may not be convenient to connect all devices in the system to create a 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, it can recover the network system within 20ms.

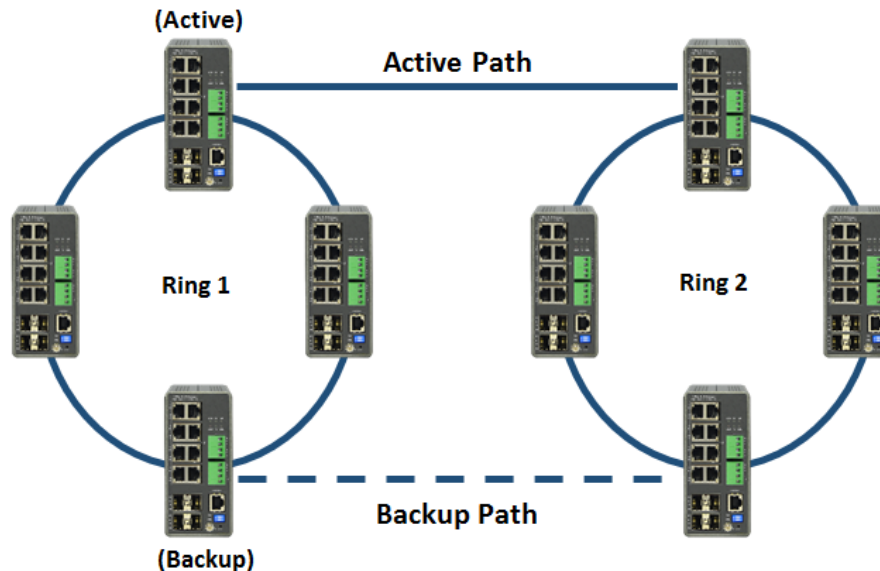


Figure 3: Ring to Ring Overview

Ring to Ring configuration is shown and described below.

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

A B C

Figure 4: Ring to Ring Configuration

- Set up Single Ring for Ring 1 and Ring 2, setting can refer to 2-1.2.
- Configure 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 be set to be the Active/ Backup, and the rest of the switches should be configured as Disabled.
- Configure Active/ Backup link port. This port should not be same as above 1st Ring Port and 2nd Ring Port.

A-1-3 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.

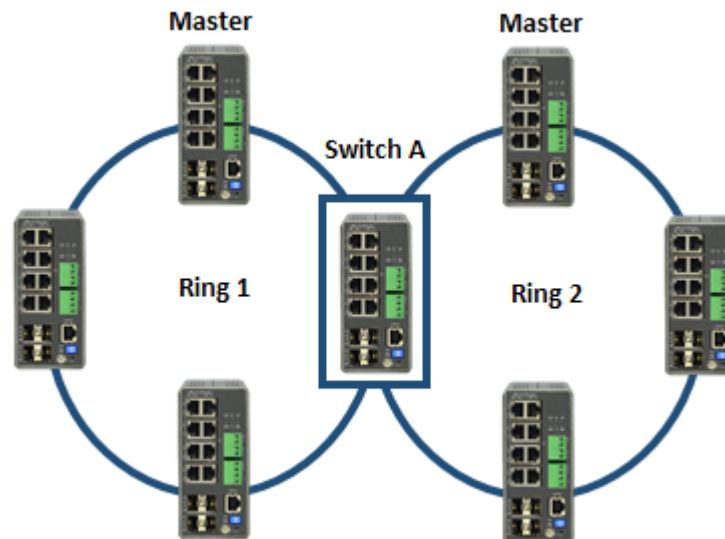


Figure 5: Dual Ring Overview

Dual Ring configuration is shown and described below.

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

Figure 6: Dual Ring Configuration

- A. Set up Single Ring for Ring 1 and Ring 2; refer to Single Ring above.
- B. Setup second ring for switch A; refer to Single Ring above.

Note: Switch A is not suggested to be the Master for Ring 1 or Ring 2.

A-1-4 Rapid Chain

Rapid Chain is a highly flexible application for complex industrial networks. It allows the switches to be quickly and easily deployed in any type of complex redundant network with a fast recovery time.

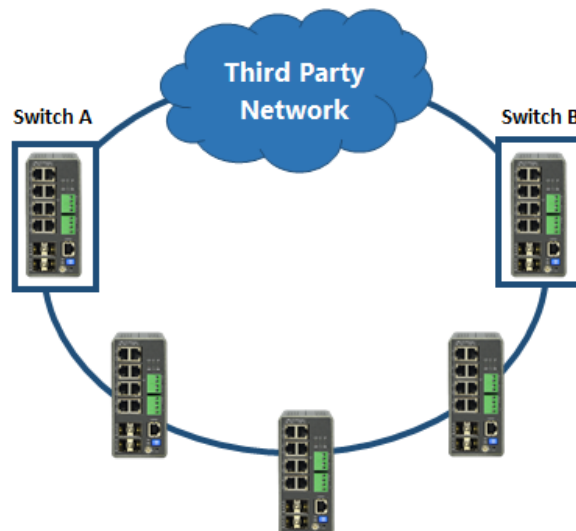


Figure 7: Rapid Chain Overview

Rapid Chain configuration is shown and described below.

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

Figure 8: Rapid Chain Configuration

- Configure the Role as **Rapid-Chain** or **Member**. Only two switches (Switch A and B) must be set as Rapid-Chain, and the rest of the switches set as the Member of Rapid Chain.
- 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.
- Indicates Port status (e.g., Forwarding, Discarding).

Note: If it is Rapid-Chain, one of Switch A and Switch B's 2nd port will be the backup path chosen by the smaller MAC address.

A-1-5 Hardware Setting and Status for Ring

Ring Setting by DIP Switch

DIP switch settings are shown and described below. Note that **RM** indicates Ring Master, and **RC** indicates Rapid Chain. See the *Install Guide* for more information.

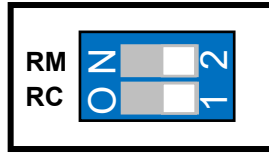


Figure 9: DIP Switch

Configure Rapid Ring by hardware DIP Switch as shown in the table below:

Table 1: DIP Switch Settings

Mode	RM	RC	Rapid Ring Status	1st Port	2nd Port	RM LED	RC LED
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	--	--	--	--

Note:

1. The DIP Switch default setting is ON/ON (software mode).
2. In hardware 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 ports. For a Combo port, either fiber or copper can be used as the Ring connecting port.

A-1-6 RM and RC LED Descriptions

The table below describes RM (Ring Master) and RC (Rapid Chain) LED status:

Table 2: LED Status

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	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: <i>There is no correspondent Rapid Chain Switch found.</i>
	--	Off	Disabled

Appendix B: DHCP Per Port

You can configure DHCP Per Port via the CLI and Web UI as described below. The DHCP Per Port factory default mode is Disabled. See the *CLI Reference* for CLI mode operation.

Configure DHCP Per Port via the Web UI

The switch's DHCP server assigns IP addresses. Clients get IP addresses in sequence and the switch assigns IP addresses on a per-port basis starting from the configured IP range. For example, if the IP address range is configured as 192.168.10.20 - 192.168.10.37 with one DHCP device connected to port 1, the client will always get IP address 192.168.10.20, then port 3 is always distributed IP address 192.168.10.22, even if port 2 is an empty port (because port 2 is always distributed IP address 192.168.10.21).

The switch does not allow a DHCP per Port pool to include the switch's address.

IP address assigned range and VLAN 1 should stay in the same subnet mask.

The configurable IP address range is allowed to configure over 18 IP addresses, but the switch always assigns one IP address per port connecting device.

When the DHCP Per Port function is enabled, the switch software will automatically create the related DHCP pool named "DHCP_Per_Port".

Once the DHCP Per Port function is enabled on one switch, IPv4 DHCP client at VLAN1 mode (DMS DHCP mode), DHCP server mode are all limited to be enabled at the same time (an error message displays if attempted).

If the DHCP server pool has been configured, once you enable the DHCP Per Port function, then that DHCP server pool configuration will be overwritten.

Only for VLAN 1, clients issued DHCP packets will not be broadcast/forwarded to other ports. DHCP packets in others VLANs will be broadcast/forwarded to other ports.

The DHCP Per Port function allows the switch to connect only one DHCP client device.

DHCP-Per-Port is configured entirely on the **Switch > Configuration > System > IP** page, IP Interfaces window.

The feature is enabled here and an IP range (pool) is entered. The "automatic" results of this action can be displayed in:

- **Switch > Configuration > System > DHCP > Server > Mode** (Global Mode – Enabled, VLAN Mode - VLAN 1 created)
- **Switch > Configuration > System > DHCP > Excluded** (Excluded range created based on range entered)
- **Switch > Configuration > System > DHCP > Pool** (Pool "DHCP_Per_Port" created based on range entered)

Actual DHCP operation is monitored as normal under **System > Monitor > DHCP**.

The DHCP Per Port pages and parameters are described below.

DHCP Per Port 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 shows the Lantronix web UI for device SISPM1040-362-LRT. The left sidebar contains a navigation menu with 'Configuration > System > IP' highlighted in red. The main content area is titled 'IP Configuration' and includes several sections:

- DNS Servers:** Four DNS Server entries, each with a dropdown for 'Configured IPv4 or IPv6' and a text field for the IP address (all set to 8.8.8.8). A 'DNS Proxy' checkbox is also present.
- IP Interfaces:** A section for 'DHCP Per Port' configuration. The 'Mode' dropdown is set to 'Disabled', the 'VLAN' dropdown is set to 'VLAN1', and the 'IP' field is empty. This section is circled in red.
- IP4 DHCP Table:** A table with columns: Delete, VLAN, Enable, Fallback, Current Lease, IPv4 Address, IPv4 Mask Length, DHCPv6 Enable, DHCPv6 Rapid Commit, DHCPv6 Current Lease, IPv6 Address, and IPv6 Mask Length. One row is visible for VLAN 1 with IP 192.168.1.77 and mask length 24.
- Link-Local Address binding interface:** A dropdown menu set to 'VLAN1'.
- Gateway Address binding interface:** A dropdown menu set to 'VLAN1'.
- IP Routes Table:** A table with columns: Delete, Network, Mask Length, Gateway, and Next Hop VLAN. Three routes are listed: 0.0.0.0 (mask 0, gateway 192.168.1.254), 169.254.0.0 (mask 16, gateway 192.168.1.77), and 192.168.1.0 (mask 24, gateway 192.168.1.77).

Parameter descriptions:

DHCP Per Port Mode: at the dropdown select **Enable** or **Disable** the DHCP Per Port function globally. The default is **Disabled**.

DHCP Per VLAN: The switch 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 VB7.20.0190.)

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).

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' selected, and 'System' and 'IP Status' highlighted. The main content area is titled 'IP Interfaces' and includes an 'Auto-refresh' button. Below this, there are two tables: 'IP Interfaces' and 'IP Routes'.

Interface	Type	Address	Status
VLAN1	LINK	00-c0-f2-49-3d-4f	<UP BROADCAST RUNNING MULTICAST>
VLAN1	IPv4	192.168.1.77/24	
VLAN1	IPv4	169.254.170.66/16	
VLAN1	IPv6	fe80::2c0:f2ff:fe49:3d4f/64	
VLAN4096	LINK	00-c0-f2-49-3d-4f	<BROADCAST MULTICAST>
VLAN4097	LINK	00-c0-f2-49-3d-4f	<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>

Buttons:

Apply: Click to save changes to the entries. If the entries are valid, the webpage message “*Update success!*” displays. Click the **OK** button to clear the message. If any entries are invalid, an error message displays. Click the **OK** button to clear the message and enter valid values, then click the **Apply** button again.

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

Web UI Messages

Message: *Interface xx not using DHCP*

Meaning: The Interface being configured does not have DHCP enabled and configured.

Recovery: **1.** Click the **OK** button to clear the webpage message. **2.** Enable and configure DHCP for the interface being configured. See “[DHCP Server Mode Configuration](#)” on page 39.

Message: *DHCP per Port range (192.168.1.50 - 192.168.1.66) is not equal to switch TP port number (8).*

Message: *'DHCP Per Port IP range (192-168-1.80 - 192-168-1.99) is not equal to switch port number excluding uplink ports (10)*

Meaning: The IPv4 IP address range entered for the DHCP Per Port function was invalid.

Recovery: **1.** Click the **OK** button to clear the webpage message. **2.** Re-configure DHCP Per Port. See the DHCP Per Port Mode Configuration section above.

Message: *'DHCP Per Port IP range (192-168-1.70 - 192-168-1.85) includes interface IP Address (192.168.1.77)*

Meaning: The IPv4 IP address range entered for the DHCP Per Port function was invalid.

Recovery: **1.** Click the **OK** button to clear the webpage message. **2.** Re-configure DHCP Per Port. See the DHCP Per Port Mode Configuration section above. On the screen 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 39.

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 39.

Message: *Update success!*

Appendix C: 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, and via the CLI. See the *CLI Reference* for Command Line operation.

According to ANSI, [IEC 62439-2 Ed. 1.0 b:2010](#) is applicable to high-availability automation networks based on [ISO/IEC 8802-3](#) / [IEEE 802.3 Ethernet technology](#). It specifies a recovery protocol based on a ring topology, designed to react deterministically on a single failure of an inter-switch link or switch in the network, under the control of a dedicated Media Redundancy Manager (MRM) node.

Media Redundancy Protocol per IEC 62439-2 is an interoperable ring technology designed to allow a switch to connect onto a universal redundant high speed ring. MRP is self-healing and self-adjusting, requiring no operator interaction. MRP is based on the concept of standby connections for seamless redundancy.

MRP Description

1. MRP operates at the MAC Layer of the Ethernet Switch.
2. The Ring Manager is called the Media Redundancy Manager (MRM).
3. Ring Clients are called Media Redundancy Clients (MRCs).
4. MRM and MRC ports support three Status Types:
 - a. *Disabled* ring ports drop all the received frames.
 - b. *Blocked* ring ports drop all the received frames except the MRP control frames.
 - c. *Forwarding* ring ports forward all the received frames.
5. Ring Reconfiguration speed is 200 ms for 50 switches on average.
6. The MRM continuously sends Watchdog Packets into the ring network to verify communication between ring points.
7. During normal operation, no packets are transmitted over the redundant link.
8. When the MRM no longer receives the Watchdog Packets it sent out, the redundant path is immediately activated, and it becomes the primary layer 2 packet path.
9. When the failed link is restored:
 - a. The MRM switches back to normal operation and the first Path becomes the primary path again.
 - b. You can configure a period of time before the MRM switches back to the primary path (to prevent the circuit from flapping if it is not stable).

MRP Operation

Normal operation: the network works in the *Ring-Closed* status. In this status, one of the MRM ring ports is blocked, while the other is forwarding. Conversely, both ring ports of all MRCs are forwarding. Loops are avoided because the physical ring topology is reduced to a logical stub topology.

Failure mode: the network works in the *Ring-Open* status. For instance, in case of failure of a link connecting two MRCs, both ring ports of the MRM are forwarding. The MRCs adjacent to the failure have a blocked and a forwarding ring port; the other MRCs have both ring ports forwarding. The physical ring topology is also a logical stub topology in the Ring-Open status.

Related Devices

MRP is implemented on Lantronix SISPM1040-384-LRT-C, SISPM1040-362-LRT, SISPM1040-582-LRT, and SISGM1040-284-LRT switches.

MRP Sample Setup

The example below shows SISPM1040-384-LRT-C switches (one MRM and five MRCs).

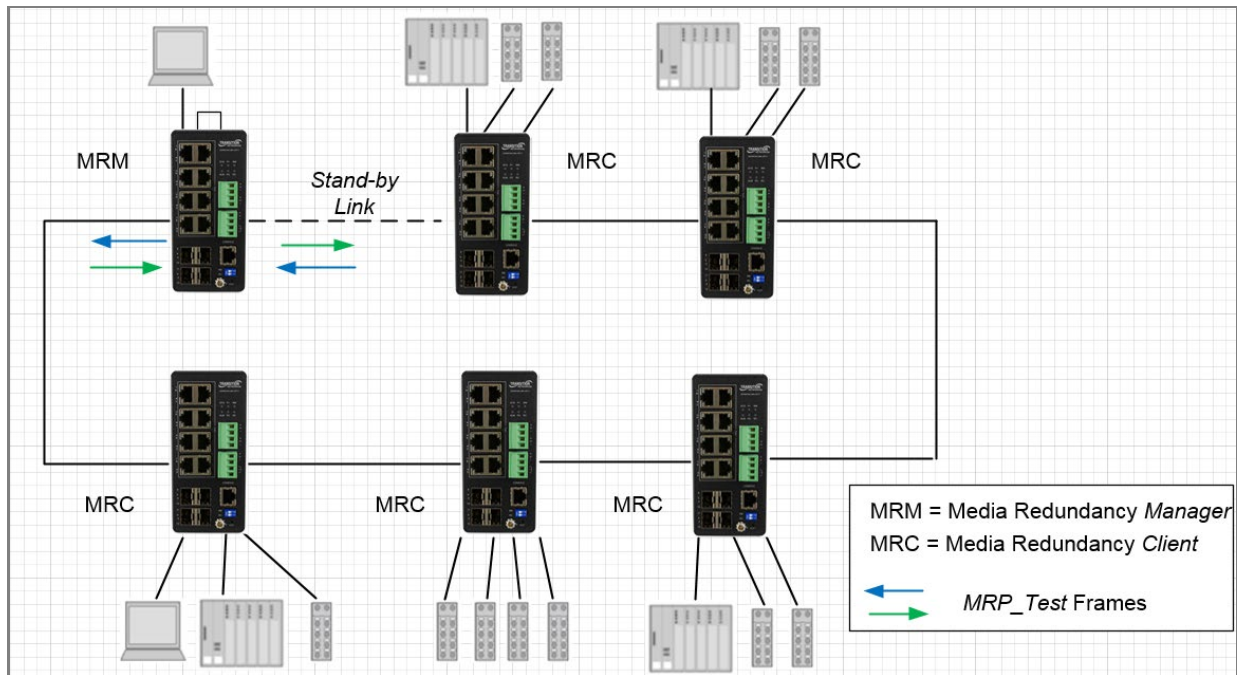


Figure: MRP Sample Setup

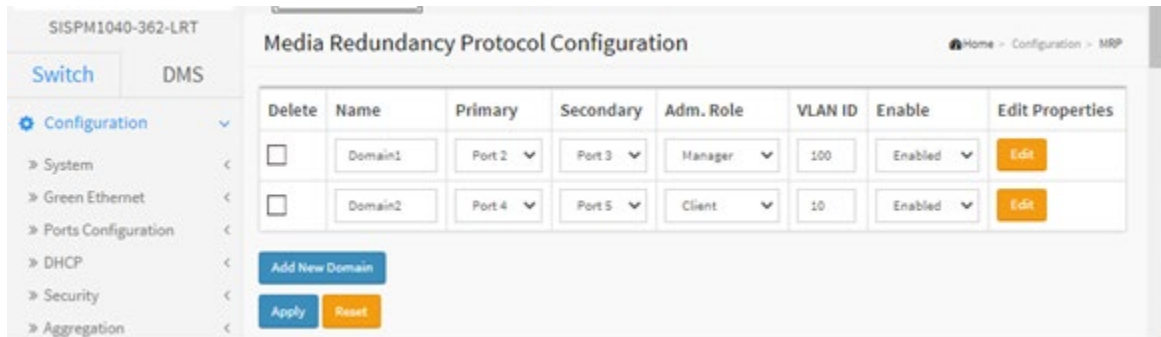
MRP Pre-Requisites (General)

The following are required to perform MRP setups.

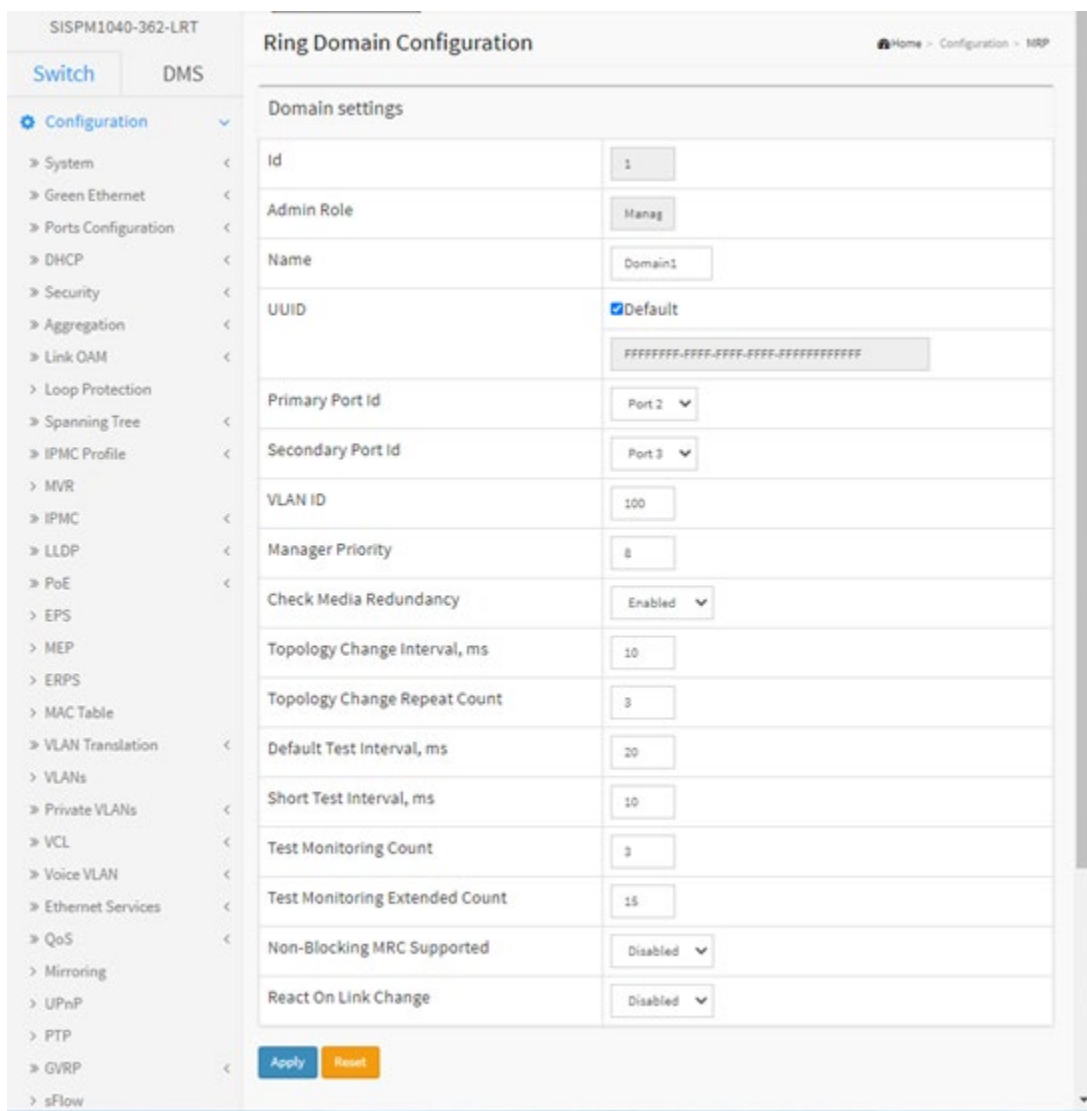
1. Spanning Tree must be disabled at Configuration > Spanning Tree > CIST Port.
2. Other Ring technologies must be disabled (G.8031 EPS, G.8032 ERPS, Rapid-Ring, Ring-To-Ring, etc.).
3. Only one MRM (Manager) is supported.
4. Other pre-requisites may apply to the specific examples below.

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 for 'SISPM1040-362-LRT'. The left sidebar shows a navigation menu with 'Configuration' expanded. The main content area is titled 'Ring Domain Configuration' and contains 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 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

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

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 D: G.8032 Major and Sub Rings Configuration

Introduction

Ethernet Ring Protection Switching (ERPS) protocol is defined by the International Telecommunication Union - Telecommunication Standardization Sector (ITU-T) to prevent loops at Layer 2. The standard number is ITU-T G.8032 (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 “2-17 ERPS” on page 186 for general G.8032 ERPS configuration information.

Basic Concepts

There are some basic concepts that support ERPS Ring:

- **Ring Protection Link (RPL)** – Link designated by mechanism that is blocked during Idle state to prevent loop on Bridged ring.
- **RPL Owner node** – Node connected to RPL that blocks traffic on RPL during Idle state and unblocks during Protection state.
- **RPL Neighbor node** – Node connected to RPL that blocks traffic on RPL during Idle state and unblocks during Protection state (v2).
- **Link Monitoring** – Links of ring are monitored using standard ETH CC OAM messages (CFM) • **Signal Fail (SF)** – Signal Fail is declared when signal fail condition is detected.
- **No Request (NR)** – No Request is declared when there are no outstanding conditions (e.g., SF, etc.) on the node.
- **Ring APS (R-APS) Messages** – Protocol messages defined in Y.1731 and G.8032.
- **Automatic Protection Switching (APS) Channel** - Ring-wide VLAN used exclusively for transmission of OAM messages including R-APS messages.

IP Addresses

The sample configurations below use these IP addresses:

SISPM1040-582-LRT : 192.168.1.85

SISPM1040-384-LRT-C : 192.168.1.95

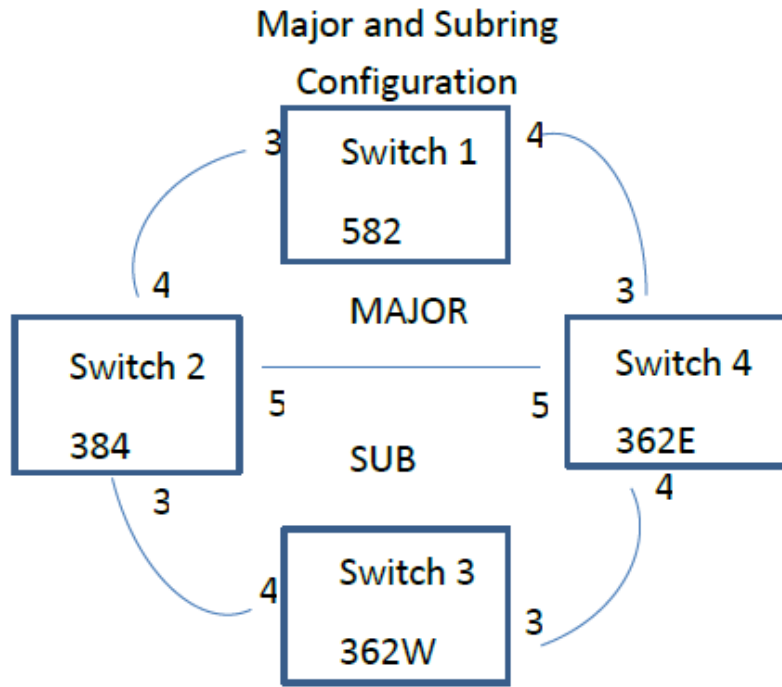
362W : 192.168.1.125

362E : 192.168.1.135

Sample Configuration

Major Ring and Sub Ring : 4 Switches

Major : SW#1, SW#2, SW#4; Sub : SW#2, SW#3, SW#4



VLANs
10,20

APS Data
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	

ERPS

ERPS ID	Port 0	Port 1	Port 0 SF	Port 1 SF	Port 0 APS	Port 1 APS	Ring	RPL	Port	VLAN
1	1	2	1	2	1	2	Major Owner		0	5

Switch 2 Configuration (SISPM1040-384-LRT-C)

VLANs	Port	Mode	Tagging	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	Mode
	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	1f/sec	<input type="checkbox"/>	<input checked="" type="checkbox"/>	7	Multi	R-APS	1

Fault Management
Performance Monitoring

ERPS

ERPS ID	Port 0 RPL	Port 1 Port	Port 0 SF VLAN	Port 1 SF	Port 0 APS	Port 1 APS	Ring
1	3	2	3	2	3	2	Major Neighbor 1
	5						
2	1	0	1	0	1	0	Sub Neighbor 0 5

Interconnect Yes, Major 1

Switch 3 Configuration (SISPM1040-362-LRT [W])

VLANs Port 3 Trunk Tag All 5,20
 Port 4 Trunk Tag All 5,20

STP Port 3 Disable
 Port 4 Disable

MEPs	Instance	Port	VLAN	MAC	MEP ID	Peer MAC	Peer MEP ID
	1	3	20	00-C0-F2-53-F0-B9	7	00-C0-F2-53-EF-FD	6
	2	4	20	00-C0-F2-53-F0-BA	8	00-40-C7-1C-C7-2F	3

Note: All MEPs are 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 RPL	Port 1 Port	Port 0 SF VLAN	Port 1 SF	Port 0 APS	Port 1 APS	Ring
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 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	Port 0	Port 1	Port 0 SF	Port 1 SF	Port 0 APS	Port 1 APS	Ring	RPL	Port VLAN
1	1	3	1	3	1	3	Major	None	5
2	2	0	2	0	2	0	Sub	None	5

Interconnect Yes, Major 1

Testing 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<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

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

Config files

running-config_192.168.1

hostname SISPM1040-362-LRT-E

```
username admin privilege 15 password encrypted
feec1d1085ff075fd03b1d2d5ab4c0befbfff0917079c8abb3a77338041bf5d6e1771bdbbd1a317ea2f42fc
2aacc8c50a8e667456d7c04099f74f8ef9dcc0fbd4
!
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_192.168.1.1**hostname SISPM1040-582-LRT**

```
logging on
logging host 192.168.1.253
username admin privilege 15 password encrypted
7073dec86c15b8a9907bb4106ef783adde46bd5b5969cc68fb55b430336bd7c80d5ded65d2fdb39abe81cc
9caa5a93620f270c21bca86e776cee9c5588bfb8c7
username superuser privilege 15 password encrypted
4643fdc71f39fd4cb955943fcaf89faca81bc650fbaeebe25a796662d5c225bf0d5ded65d2fdb39abe81cc
9c514497e27799560e488713aabaac4f167e7732ca
!
vlan 1
!
!
!
!
ip route 0.0.0.0 0.0.0.0 192.168.1.254
ntp automatic
ntp server 1 ip-address ntp1.transition.com
ntp server 2 ip-address ntp2.transition.com
clock timezone '' 9
tzidx 0
exec-timeout autologout 0
poe ping-check enable
snmp-server contact DTroxel
snmp-server location DT Office
system contact DTroxel
system name SISPM1040-582-LRT
system location DT Office
system description Managed Hardened PoE++ Switch (8) 10/100/1000Base-T PoE++ Ports +
(2) 100/1000Base-X SFP Slot
!
interface GigabitEthernet 1/1
no spanning-tree
poe ping-ip-addr 192.168.1.70
poe failure-action reboot-Remote-PD
!
interface GigabitEthernet 1/2
no spanning-tree
switchport forbidden vlan add 3,5
!
interface GigabitEthernet 1/3
no spanning-tree
switchport trunk allowed vlan 5,10
switchport trunk vlan tag native
switchport mode trunk
poe mode disable
!
interface GigabitEthernet 1/4
no spanning-tree
switchport trunk allowed vlan 5,10
switchport trunk vlan tag native
switchport mode trunk
poe mode disable
poe ping-ip-addr 192.168.1.200
!
interface GigabitEthernet 1/5
no spanning-tree
!
interface GigabitEthernet 1/6
no spanning-tree
!
interface GigabitEthernet 1/7
!
interface GigabitEthernet 1/8
```

```
poe mode disable
!
interface GigabitEthernet 1/9
 no spanning-tree
!
interface GigabitEthernet 1/10
 no spanning-tree
!
interface vlan 1
 ip address 192.168.1.85 255.255.255.0
 ip dhcp server
!
mep 1 down domain port level 4 interface GigabitEthernet 1/3
mep 1 vid 10
mep 1 peer-mep-id 4 mac 00-40-C7-1C-C7-30
mep 1 cc 7
mep 1 aps 7 raps
mep 2 down domain port level 4 interface GigabitEthernet 1/4
mep 2 mep-id 2
mep 2 vid 10
mep 2 peer-mep-id 5 mac 00-C0-F2-53-EF-FC
mep 2 cc 7
mep 2 aps 7 raps
erps 1 major port0 interface GigabitEthernet 1/3 port1 interface GigabitEthernet 1/4
erps 1 mep port0 sf 1 aps 1 port1 sf 2 aps 2
erps 1 rpl owner port0
erps 1 vlan 5
!
spanning-tree aggregation
 no spanning-tree
 spanning-tree link-type point-to-point
!
!
line console 0
!
line vty 0
!
line vty 1
!
line vty 2
!
line vty 3
!
line vty 4
!
line vty 5
!
line vty 6
!
line vty 7
!
line vty 8
!
line vty 9
!
line vty 10
!
line vty 11
!
line vty 12
!
line vty 13
!
line vty 14
!
line vty 15
```

```
!  
map-api-key AIzaSyBITuM0hDtK6nJeZPEk7jnrcGGi92EpFM  
!  
end
```

running-config_192.168.1**hostname SISPM1040-384-LRT-C**

```
username admin privilege 15 password encrypted
6593186b999f348becd63b8612ac561c114250a1a00bd38f6afb5378acb6d08c1864c59b092b0e2b29ba4f
1d559166800846cbc52c4558a90e4cdf95d3cfcfbf4
username dennis privilege 5 password encrypted
a92a5dbf4fcd2e13d35adb36d2418476e907de19a641fa7baf80b1abb2bacd8ee5dbdd44e246b88be1636d
f6b8769af790aa8721622481085e33c32e6e119dbd
!
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 AIzaSyBITuM0hDtK6nJeZPEk7jnrcGGi92EpFM
!
end
```

running-config_192.168.1**hostname SISPM1040-362-LRT-W**

```
username admin privilege 15 password encrypted
6158ed7daf39d06ded0e7c4828c3b15bb4c40673bd445afcd643295925ae425d9611d1cbe872708237571a
acc7b9237f33b01ae6866e2484009edfelfa0bf56f
!
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.