



SISPM1040-xxxx-L3

Layer 3 Managed Hardened PoE + Switch family

SISPM1040-3248-L3 and SISPM1040-3166-L3

Web User Guide

**Part Number 33856**  
**Revision B August 2023**

## 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. All other trademarks and trade names are the property of their respective holders.

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

## Warranty

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

## Contacts

### Lantronix Corporate Headquarters

48 Discovery, Suite 250  
Irvine, CA 92618, USA  
Toll Free: 800-526-8766  
Phone: 949-453-3990  
Fax: 949-453-3995

### Technical Support

Online: <https://www.lantronix.com/technical-support/>

### Sales Offices

For a current list of our domestic and international sales offices, go to [www.lantronix.com/about/contact](http://www.lantronix.com/about/contact).

## Disclaimer

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

## Revision History

Date	Rev	Notes
6/13/22	A	Initial Lantronix release at v8.90.884, Bootloader v1_5-38e0421, PoE Firmware V 200-211HW v1.02, Mech v1.01.
8/21/23	B	SISPM1040-3248-L3 FW v 8.10.0086: view release notes for latest firmware information. Minor editorial and technical changes.

## Contents

<b>Product Description</b> .....	<b>11</b>
<b>About This Manual</b> .....	<b>11</b>
<b>Related Manuals</b> .....	<b>11</b>
<b>Safety Warnings and Cautions</b> .....	<b>11</b>
<b>Initial Switch Configuration</b> .....	<b>12</b>
Initial Switch Configuration via Web Browser .....	12
<b>Web User Interface</b> .....	<b>13</b>
Initial Configuration .....	13
Webpage Controls .....	14
<b>First Time Wizard</b> .....	<b>16</b>
<b>System</b> .....	<b>17</b>
System > Information .....	17
System > IP Address > Settings .....	19
System > IP Address > Advanced Settings .....	20
System > IP Address > Status .....	23
System > System Time .....	25
Configure NTP Server .....	27
System > LLDP > LLDP Configuration .....	28
System > LLDP > LLDP-MED Configuration .....	30
System > LLDP > LLDP Neighbor .....	36
System > LLDP > LLDP-MED Neighbor .....	37
System > LLDP > LLDP Neighbor PoE .....	40
System > LLDP > LLDP Neighbor EEE .....	41
System > LLDP > LLDP Statistics .....	43
System > UPnP .....	45
<b>Port Management</b> .....	<b>46</b>
Port Management > Port Configuration .....	46
Port Management > Port Statistics .....	49
Detailed Port Statistics .....	50
Port Management > SFP Port Info .....	52
Port Management > Energy Efficient Ethernet .....	54
Port Management > Link Aggregation > Static Configuration .....	55
Port Management > Link Aggregation > LACP Port Configuration .....	57
Port Management > Link Aggregation > System Status .....	58
Port Management > Link Aggregation > Port Status .....	59
Port Management > Link OAM > Port Settings.....	60
Detailed Link OAM Status .....	61
Port Management > Link OAM > Event Settings .....	63
Port Management > Link OAM > Statistics .....	64
Port Management > Link OAM > Event Status .....	66
Port Management > Loop Protection > Configuration .....	69
Port Management > Loop Protection > Status.....	71
Port Management > UDLD > UDLD Configuration .....	72

Port Management > UDLD > UDLD Status .....	73
Port Management > DDMI > Configuration .....	74
Port Management > DDMI > Status .....	75
<b>PoE Management.....</b>	<b>77</b>
PoE Management > PoE Configuration .....	77
PoE Management > PoE Status .....	79
PoE Management > PoE Power Delay .....	80
PoE Management > PoE Auto Checking .....	81
PoE Management > PoE Schedule Profile .....	82
PoE Management > PoE Firmware Upload .....	83
<b>VLAN Management.....</b>	<b>84</b>
VLAN Management > VLAN Configuration .....	84
VLAN Management > VLAN Membership .....	87
VLAN Management > VLAN Port Status .....	89
VLAN Management > VLAN Name .....	91
MAC-based VLAN .....	92
MAC-based VLAN Configuration .....	92
MAC-based VLAN Status .....	93
VLAN Management > Protocol-based VLAN .....	94
VLAN Management > Protocol-based VLAN > Protocol to Group .....	94
VLAN Management > Protocol-based VLAN > Group to VLAN .....	96
IP Subnet-based VLAN .....	97
VLAN Management > Stream .....	98
VLAN Management > Stream > Stream .....	98
VLAN Management > Stream > MAC Matching .....	99
VLAN Management > MRP .....	100
VLAN Management > MRP > Ports .....	100
VLAN Management > MRP > MVRP .....	101
VLAN Management > MRP > MVRP Statistics .....	102
VLAN Management > GVRP .....	103
VLAN Management > GVRP > Config .....	103
VLAN Management > Private VLAN .....	105
VLAN Management > Port Isolation .....	106
VLAN Management > Voice VLAN .....	107
VLAN Management > Voice VLAN > Configuration .....	107
VLAN Management > Voice VLAN > OUI .....	109
<b>QoS.....</b>	<b>110</b>
QoS > Port Classification .....	110
Ingress Port Tag Classification .....	112
QoS > Port Policers .....	113
QoS > Queue Policers .....	114
QoS > Port Shapers .....	115
QoS > Storm Control .....	116
QoS > Port Schedulers .....	118
QoS > Port PCP Remarking .....	122
QoS Egress Port PCP Remarking .....	123



DSCP .....	124
Port DSCP .....	124
DSCP Translation.....	125
DSCP Classification .....	126
DSCP-based QoS .....	127
Ingress Map.....	128
Egress Map .....	131
QoS Control List.....	134
QCE Configuration .....	134
Status .....	138
QoS Statistics.....	140
Detailed Port Statistics .....	141
WRED .....	143
<b>Spanning Tree.....</b>	<b>145</b>
STP Configuration.....	146
MSTI Configuration .....	148
STP CIST Port Configuration .....	149
STP Status .....	151
STP Detailed Bridge Status.....	152
Port Statistics .....	154
<b>MAC Address Table.....</b>	<b>155</b>
MAC Address Table Configuration .....	155
MAC Address Table Status.....	157
<b>Multicast .....</b>	<b>159</b>
IGMP Snooping.....	159
Basic Configuration .....	159
VLAN Configuration.....	161
Status .....	163
Groups Information.....	165
IGMP SFM Information.....	166
MLD Snooping .....	167
Basic Configuration .....	168
VLAN Configuration.....	170
Status .....	171
Groups Information.....	173
MLD SFM Information .....	174
MVR .....	175
Basic Configuration .....	175
Statistics .....	177
Groups Information.....	178
MVR SFM Information.....	179
Multicast Filtering Profile.....	180
Multicast Filtering Profile > Filtering Profile Table .....	180
Rule > Preview page .....	181
Rule > Edit page.....	182

Multicast Filtering Profile > Filtering Address Entry .....	183
<b>DHCP .....</b>	<b>184</b>
DHCP > Snooping > Snooping Configuration.....	184
DHCP > Snooping > Snooping Table .....	185
DHCP > Snooping > Detailed Statistics .....	186
DHCP > DHCPv6 > Snooping > Configuration.....	188
DHCP > DHCPv6 > Snooping > Table .....	190
DHCP > DHCPv6 Snooping > Detailed Statistics.....	191
DHCP Relay.....	192
DHCP Relay Configuration.....	192
DHCP Relay Statistics.....	194
DHCP > DHCPv6 Relay > Configuration .....	196
DHCP > DHCPv6 Relay > Status .....	197
DHCP > Server > Configuration.....	198
DHCP > Server > Status.....	199
<b>Security.....</b>	<b>200</b>
Security > Management > Account.....	200
Add New User .....	201
Edit a User.....	202
Delete a User.....	202
Security > Management > Privilege Levels .....	203
Security > Management > Auth Method .....	204
Security > Management > Access Method .....	206
Security > Management > HTTPS .....	207
Security > 802.1X > Configuration .....	208
Security > 802.1X > Status .....	214
802.1X Port Status page .....	215
Security > IP Source Guard > Configuration .....	220
Security > IP Source Guard > Static Table.....	221
Security > IP Source Guard > Dynamic Table.....	222
Security > IPv6 Source Guard > Configuration.....	223
Security > IPv6 Source Guard > Static Table .....	224
Security > IPv6 Source Guard > Dynamic Table.....	225
Security > ARP Inspection > Configuration .....	226
Security > ARP Inspection > VLAN Configuration .....	228
Security > ARP Inspection > Static Table.....	229
Security > ARP Inspection > Dynamic Table.....	230
Security > Port Security > Configuration.....	231
Security > Port Security > MAC Address.....	234
Port Security Static and Sticky MAC Addresses .....	234
Security > Port Security > Status .....	236
Port Security Status for a selected Port .....	238
Security > RADIUS > Configuration.....	239
Security > RADIUS > Status .....	241
Detailed RADIUS Authentication Statistics .....	242
Security > TACACS+ .....	249

<b>Access Control</b> .....	<b>251</b>
Access Control > ACL Ports Configuration .....	251
Access Control > Rate Limiters .....	253
Access Control > Access Control List .....	255
Access Control List Configuration page .....	255
ACE Configuration page .....	257
Access Control > ACL Status .....	266
<b>SNMP</b> .....	<b>268</b>
SNMP > SNMPv1/v2c .....	268
SNMP > SNMPv3 > Communities .....	269
SNMP > SNMPv3 > Users .....	270
SNMP > SNMPv3 > Groups .....	272
SNMP > SNMPv3 > Views .....	273
SNMP > SNMPv3 > Access .....	274
SNMP > Statistics > Configuration .....	275
SNMP > Statistics > Statistics .....	276
Detailed RMON Statistics page .....	277
SNMP > History > Configuration .....	279
SNMP > History > Status .....	280
SNMP > Alarm > Configuration .....	281
SNMP > Alarm > Status .....	283
SNMP > Event > Configuration .....	284
SNMP > Event > Status .....	285
<b>CFM</b> .....	<b>286</b>
CFM > Global .....	286
CFM > Domain .....	288
CFM > Service .....	290
CFM > MEP .....	292
CFM > MEP Status .....	295
<b>APS</b> .....	<b>297</b>
APS Configuration .....	297
APS Instance Page .....	300
APS Status .....	303
<b>ERPS</b> .....	<b>306</b>
ERPS > Control .....	306
ERPS > Status .....	310
ERPS Detailed Status for an instance .....	311
<b>Rapid Ring</b> .....	<b>314</b>
<b>MRP</b> .....	<b>315</b>
MRP > MRP Configuration .....	315
Ring Domain Configuration page .....	316
MRP > MRP Status .....	318
<b>PTP</b> .....	<b>320</b>
PTP > Configuration .....	320
PTP Clock's Configuration and Status .....	322

PTP Clock's Port Data Set Configuration .....	328
PTP > Status .....	332
PTP Clock's Configuration .....	333
PTP > 802.1AS Statistics .....	334
<b>Event Notification .....</b>	<b>336</b>
Event Notification > SNMP Trap .....	336
Event Notification > email .....	339
Event Notification > Log > Syslog .....	340
Event Notification > Log > View Log .....	341
Event Notification > Digital I/O .....	343
Event Notification > Event Configuration .....	344
<b>Router .....</b>	<b>346</b>
Router > Key-Chain .....	346
Router > Key-Chain Key-ID .....	349
Router > Access List .....	351
<b>OSPF .....</b>	<b>352</b>
OSPF > Configuration > Global Configuration .....	352
OSPF > Configuration > Network Area .....	355
OSPF > Configuration > Passive Interface .....	356
OSPF > Configuration > Stub Area .....	357
OSPF > Configuration > Area Authentication .....	358
OSPF > Configuration > Area Range .....	359
OSPF > Configuration > Interfaces .....	361
OSPF Interface Message Digest Configuration page .....	362
OSPF > Configuration > Virtual Link .....	364
OSPF Virtual Link Message Digest Configuration page .....	366
OSPF > Status .....	367
OSPF > Status > Global Status .....	367
OSPF > Status > Area Status .....	368
OSPF > Status > Neighbor Status .....	369
OSPF > Status > Interface Status .....	370
OSPF > Status > Routing Status .....	371
OSPF > Status > General Status .....	373
OSPF > Status > Router .....	375
OSPF > Status > Network .....	377
OSPF > Status > Summary .....	379
OSPF > Status > ASBR Summary .....	381
OSPF > Status > External .....	383
OSPF > Status > NSSA External .....	385
<b>OSPFv3 .....</b>	<b>387</b>
OSPFv3 > Configuration > Global Configuration .....	387
OSPFv3 > Configuration > Passive Interface .....	389
OSPFv3 > Configuration > Stub Area .....	390
OSPFv3 > Configuration > Area Range .....	391
OSPFv3 > Configuration > Interfaces .....	392

OSPFv3 > Status > Global Status .....	393
OSPFv3 > Status > Area Status .....	394
OSPFv3 > Status > Neighbor Status .....	395
OSPFv3 > Status > Interface Status .....	396
OSPFv3 > Status > Routing Status .....	397
OSPFv3 > Database > General Database .....	399
OSPFv3 > Detail Database > Router .....	401
OSPFv3 > Detail Database > Network .....	403
OSPFv3 > Detail Database > Link .....	405
OSPFv3 > Detail Database > IntraArea Prefix .....	406
OSPFv3 > Detail Database > Summary .....	407
OSPFv3 > Detail Database > ASBR Summary .....	408
OSPFv3 > Detail Database > External .....	409
<b>RIP .....</b>	<b>411</b>
RIP > Configuration > Global Configuration .....	411
RIP > Configuration > Network Configuration .....	414
RIP > Configuration > Neighbor Configuration .....	415
RIP > Configuration > Passive Interface .....	416
RIP > Configuration > Interfaces .....	417
RIP > Configuration > Offset-List .....	418
RIP > Status > Global Status .....	419
RIP > Status > Interface Status .....	420
RIP > Status > Peer Status .....	421
RIP > Status > Database .....	422
<b>Diagnostics .....</b>	<b>424</b>
Diagnostics > ICMP Ping (IPv4) .....	424
Diagnostics > ICMP Ping (IPv6) .....	426
Diagnostics > Traceroute (IPv4) .....	428
Diagnostics > Traceroute (IPv6) .....	430
Diagnostics > MIB Retrieval .....	431
Diagnostics > Cable Diagnostics .....	432
Diagnostics > Mirroring .....	434
Diagnostics > sFlow > Configuration .....	436
Diagnostics > sFlow > Statistics .....	438
<b>Maintenance .....</b>	<b>440</b>
Maintenance > Configuration .....	440
Save Startup-config .....	440
Backup Configuration .....	441
Restore Configuration .....	442
Activate Configuration .....	443
Delete Configuration File .....	444
Maintenance > Restart Device .....	444
Maintenance > Factory Defaults .....	445
Maintenance > Firmware > Firmware Upgrade .....	446
Maintenance > Firmware > Firmware Selection .....	447

<b>DMS (Device Management System)</b> .....	<b>448</b>
DMS Features .....	448
DMS > DMS Mode .....	448
DMS Information page .....	449
DMS > Management > Map API Key .....	450
DMS > Management > Device List .....	451
DMS > Graphical Monitoring > Topology View .....	453
DMS > Graphical Monitoring > Floor View .....	461
DMS > Graphical Monitoring > Map View .....	463
DMS > Maintenance > Floor Image .....	465
DMS > Maintenance > Diagnostics .....	467
DMS > Maintenance > Traffic Monitor .....	469
DMS Firmware Upgrade Procedure .....	471
DMS Troubleshooting .....	473
<b>Appendix A – DHCP Per Port Configuration</b> .....	<b>474</b>
DHCP IP per Port.....	474
Configure DHCP Per Port via the Web UI .....	474
DHCP Per Port Mode Configuration .....	475
<b>Appendix B - MRP Pre-Requisites and Application Examples</b> .....	<b>478</b>
MRP Description .....	478
MRP Operation .....	478
Related Devices .....	479
MRP Sample Setup.....	479
MRP Pre-Requisites (General) .....	479
MRP Web UI Configuration.....	480
<b>Appendix C - G.8032 Major and Sub Rings Configuration</b> .....	<b>484</b>
Introduction .....	484
Basic Concepts .....	484
IP Addresses.....	484
Sample Configuration.....	485
Testing .....	490
Config files .....	492

## Product Description

The Lantronix SISPM1040-xxxx-L3 are next generation Industrial L3+ managed GbE switches. They are affordable managed switches that provide a reliable infrastructure for your business network. These switches deliver the intelligent features you need to improve the availability of your critical business applications, protect your sensitive information, and optimize your network bandwidth to deliver information and applications more effectively. They provide the ideal combination of affordability and capabilities for entry level networking includes small business or enterprise applications and help you create a more efficient, better-connected workforce.

## About This Manual

This manual describes how to configure and manage the SISPM1040-xxxx-L3 switch using the web UI. It is intended for use by network administrators who are responsible for operating and maintaining network equipment. It assumes a strong knowledge of Ethernet switch functions, the Internet Protocol (IP), and Hypertext Transfer Protocol (HTTP).

## Related Manuals

A printed Quick Start Guide is shipped with each SISPM1040-xxxx-L3 device. For the latest information, see the [online manual](#). Note that this manual provides links to third party web sites for which Lantronix is not responsible. Related manuals include:

1. Product Support Postcard, 33504
2. SISPM1040-xxxx-L3 Quick Start Guide, 33854
3. SISPM1040-xxxx-L3 Install Guide, 33855
4. SISPM1040-xxxx-L3 Web User Guide, 33856 (this manual)
5. SISPM1040-xxxx-L3 CLI Reference, 33857
6. Release Notes (firmware version specific)

**Note:** Information in this document is subject to change without notice. All information was deemed accurate and complete at the time of publication. This manual documents the latest software/firmware version. While all screen examples may not display the latest version number, all of the descriptions and procedures reflect the latest software/firmware version, noted in the [Revision History](#) on page 2. Transition Networks is now Lantronix. Some products/firmware items are still in process of being re-branded and may still reflect the Transition Networks name/logo.

## 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.

## Initial Switch Configuration

After powering up the switch for the first time, you can perform the initial switch configuration using a web browser or CLI. For managing switch features using the CLI, refer to the CLI Reference for details.

To begin with the initial configuration stage, you must reconfigure your PC's IP address and subnet mask so as to make sure the PC can communicate with the switch. After changing PC's IP address (for example, 192.168.1.250), you can then access the Web UI of the switch using the switch's default IP address as shown below.

The initial switch configuration procedure is as follows:

**Note:** The switch factory default IP address is 192.168.1.77. The factory default Subnet Mask is 255.255.255.0.

### Initial Switch Configuration via Web Browser

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

If your PC is configured correctly, you will see the switch login page as shown below.



Web UI Login screen

If you do not see the above login page, perform the following steps:

- Refresh the web page.
  - Check to see if there is an IP conflict issue.
  - Clean browser cookies and temporary internet files.
  - Check your PC settings again and repeat step 2.
5. Enter the factory default username and password in login page and click "Login" to log into the switch.  
**Note:** The factory default Username and Password are both **admin**.



## Web User Interface

### Initial Configuration

This chapter describes how to configure and manage the switch using the web user interface. With this facility, you can easily configure and monitor, via any switch port, all switch functions, including port activity, Spanning tree, port aggregation status, multicast traffic, VLAN and priority status, etc.

Switch default values are listed below:

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

After the initial switch configuration, you can browse it. For instance, type `http://192.168.1.77` in the address row in a browser to display the Login screen which prompts for the username and password in order to login.

The default username is admin and password is admin. For first time use, enter the default username and password, and then click the Login button. The login process is complete. The Login menu requires you to enter the complete username and password; the switch will not provide a shortcut to username / password automatically. This seems inconvenient but is safer.

The switch allows two or more users with administrator rights to manage this switch. The last administrator setting will provide the configuration used by the switch.

When you log in to the switch Web UI, you can use either IPv4 or IPv6. The switch has the DHCP function disabled by default, so if you do not have DHCP server to provide IP addresses to the switch, you must use the switch default IP address of 192.168.1.77.

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

The SISPM1040-3xxx-L3 has the DHCP server function disabled by default; if you do not have a DHCP server providing IP addresses to the switch, the switch defaults to IP address 192.168.1.77.

## Webpage Controls

The Web UI navigation controls are shown and described below.



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



: Icon to show / hide left hand menu items.



: Device icon with links to

Detailed Port Statistics pages.



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



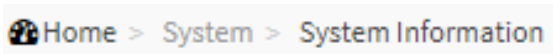
: **Save** changes on this page to the startup-config file. At the confirmation prompt “*Are you sure you want to save running configuration to startup-config?*” click the OK button. During Save operation, do not reset or power off the switch!



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



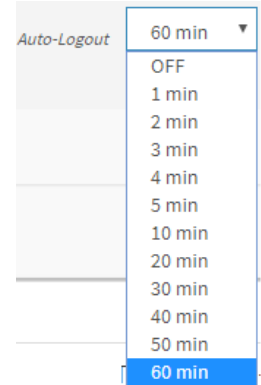
**Log out:** click to log out of the Web UI. The Login page displays again.



: **Menu path** for the currently-displayed page.



**Auto-Logout** dropdown lets you set the amount of time after a successful login before an automatic log out occurs. The selections are OFF, 1, 2, 3, 4, 5, 10 (default), 20, 30, 40, and 60 minutes. When you select an auto-logout you must click the Save button for it take effect. Save changes is retained after reboot/restart; however, if you reset the switch to factory defaults, then Auto-Logout goes back to its default of 10 min. (added at FW v8.40.1778).



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

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

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

To examine the running-config, run the CLI command “showing running-config”.

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

In other words:

- 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 save to startup-config), the timeout change will be applied to running-config immediately.
After Logout and login, the timeout setting will be the setting saved in start-up config.	After Logout and login, the timeout setting will be the setting saved in start-up configure.
After a switch reboot, the timeout setting will be the setting saved in start-up config.	After you reboot the switch, the timeout setting will be the setting saved in start-up config.

**Webpage Messages**

**Message:** *Wrong username or password!*

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

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

Recovery: Try to log in later.

## First Time Wizard

1. Change default password: enter a new password. It must contain at least 8 characters; at least 1 upper case, 1 lower case and 1 numeric character. New password should not be blank or default value. Enter the new password again and click Next.

Change default password

New password

Repeat new password

Password must contain:

1. Minimum of 8 characters
2. At least 1 upper case, 1 lower case and 1 numeric

New password should not be blank or default value.

Next

Set IP address

Obtain IP address via DHCP

Set IP address manually

IP address

Subnet mask

Default router

DNS

Previous Next

2. Set IP address: select “Obtain IP address via DHCP” or “Set IP address manually”. Enter an IP address, Subnet mask, Default router, and DNS IP address, then click Next.
3. Set Date & Time: set Automatic date and time to | (on) or 0 (off). Enter a Server Address and select a Time zone. Set date and time Manually if prompted and click Next.

Set date and time

Automatic date and time

Server Address

Time zone

None

Previous Next

4. Set Information: Set System contact, System name, and System location as desired and click Apply.
5. When the Login page displays, enter the new Username and Password, then click Login. The System Information page displays as described below.

## System

The System submenus provide basic functions, including the System Information, IP addressing, system time, LLDP, and UPnP. This is the startup page.

### System > Information

This page displays switch system information and lets you enter a system location, contact, and system name.

The screenshot shows the 'System Information' page in the Lantronix web interface. The device is identified as 'SISPM1040-3248-L3'. The page features an 'Auto-refresh' toggle set to 'off' and a 'Refresh' button. The system details are as follows:

Model Name	SISPM1040-3248-L3
System Description	Layer 3 Managed Hardened PoE+ Switch, (24) 10/100/1000Base-T PoE+ Ports + (4) 100/1000Base-X SFP + (4) 1G/10GBase-X SFP+
Location	<input type="text"/>
Contact	<input type="text"/>
System Name	<input type="text" value="SISPM1040-3248-L3"/>
System Date	2020-01-01T04:00:17+00:00
System Uptime	04:00:43
Bootloader Version	V1.05
Firmware Version	v8.10.0001 2022-04-25
PoE Firmware Version	200-211
Hardware Version	
Mechanical Version	
Serial Number	
MAC Address	02-00-c1-3e-cd-fa
Powers Status	Normal
Temperature Status	Normal
Temperature 1	45(C) ; 113(F)
Temperature 2	40(C) ; 104(F)
CPU Load (100ms, 1s, 10s)	75%, 92%, 24%

**Model Name:** Displays the factory defined model name for identification purposes (e.g., SISPM1040-3248-L3).

**System Description:** A description of the system (e.g., Layer 3 Managed Hardened PoE+ Switch, (24) 10/100/1000Base-T PoE+ Ports + (4) 100/1000Base-X SFP + (4) 1G/10GBase-X SFP+).

**Location** Edit field to define a system. The default is blank.

**Contact:** Edit field to define a system contact. The default is blank.

**System Name:** Edit field to define a system name

**System Date:** The current (GMT) system time and date in the format 2021-12-17T12:38:54+00:00. The system time is obtained through the Timing server running on the switch, if any.

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

**Bootloader Version:** Displays the current boot loader version number (e.g., 1\_5-38e0421).

**Firmware Version:** Displays the current firmware version number (e.g., v8.90.884 2022-02-16).

**PoE Firmware Version:** Displays the current PoE firmware version number (e.g., 200-211).

**Hardware Version:** Displays the hardware version of the device (e.g., v1.02).

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

**Serial Number:** Displays the unique serial number that assigned to the device (e.g., A208121BR3900001).

**MAC Address:** The MAC Address of this switch, in the format 00-c0-f2-7c-58-92.

**Powers Status:** The current status of power input (e.g., Normal).

**Temperature Status:** The current status of operating temperature (e.g., Normal).

**Temperature 1:** The temperature at sensor 1 (e.g., 37(C) ; 98(F)).

**Temperature 2:** The temperature at sensor 2 (e.g., 40(C) ; 104(F)).

**CPU Load (100ms, 1s, 10s):** Displays the cpu loading (100ms, 1s, 10s) of the system.

### Buttons

**Apply:** Click to save changes.

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

## System > IP Address > Settings

This page lets you set basic IP settings, IP interfaces, and IP routes. 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 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.

Setting	Value
IPv4 DHCP Client Enable	<input type="checkbox"/> off
IPv4 Address	192.168.1.77
Subnet Mask	255.255.255.0
Gateway	192.168.1.254
DNS Server	No DNS server

**IPv4 DHCP Client Enable:** Enable the DHCPv4 client by sliding this from **off** to **on**. If this option is enabled, the system will configure the IPv4 address and subnet mask of the interface using the DHCPv4 protocol. The DHCPv4 client will announce the configured System Name as hostname to provide DNS lookup.

**IPv4 Address:** The IPv4 address of the interface in dotted decimal notation. If DHCP is enabled, this field configures the fallback address. The field may be left blank if IPv4 operation on the interface is not desired or if no DHCP fallback address is desired.

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

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

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

**No DNS server:** No DNS server will be used.

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

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

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

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

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

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

## System > IP Address > Advanced Settings

This page lets you set more advanced IP settings, IP interfaces and IP routes. The maximum number of interfaces supported is 128 and the maximum number of routes is 128.

The screenshot shows the 'Advanced Settings' page for IP Address configuration. The 'Mode' is set to 'Host'. There are three DNS Server entries, all set to 'No DNS server'. The 'IP Interfaces' section shows 'DHCP Per Port' set to 'Disabled'. The 'DHCPv4' section has a table with columns: Delete, VLAN, Enable, Client ID, Type, IfMac, ASCII, HEX, Hostname, Fallback, Current Lease, Address, Mask Length, Enable, Rapid Commit, Current Lease, Address, Mask Length. The 'Client ID' column is highlighted with an orange box. The 'IP Routes' section has a table with columns: Delete, Network, Mask Length, Gateway, Next Hop VLAN (IPv6), Distance.

### 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. Router mode is required for Router configuration.

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

**No DNS server:** No DNS server will be used.

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

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

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

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

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

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



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

### **IP Interfaces**

**DHCP Per Port Mode:** Enable/Disable DHCP per port.

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

**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.

**DHCPv4 Client ID Type:** Specify which of the four Client Identifier types below (Auto, IF\_MAC, ASCII, or HEX) to use for the Client Identifier. See IETF [RFC-2132](#) section 9.14. This option is used by DHCP clients to specify their unique identifier. DHCP servers use this value to index their database of address bindings. This value is expected to be unique for all clients in an administrative domain.

**Auto:** The Client Identifier is set automatically (default).

**IPv4 DHCP Client ID IfMac:** The interface name of the DHCP client identifier. When DHCPv4 client is enabled and the client identifier type is 'IF\_MAC', the configured interface's hardware MAC address will be used in the DHCP option 61 field.

**IPv4 DHCP Client ID ASCII:** The ASCII string of the DHCP client identifier. When DHCPv4 client is enabled and the client identifier type is 'ASCII', the ASCII string will be used in the DHCP option 61 field.

**IPv4 DHCP Client ID HEX:** The hexadecimal string of the DHCP client identifier. When the DHCPv4 client is enabled and the client identifier type 'HEX', the hexadecimal value will be used in the DHCP option 61 field.

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

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

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

**IPv4 Address:** The IPv4 address of the interface in dotted decimal notation. If DHCP is enabled, this field configures the fallback address. The field may be left blank if IPv4 operation on the interface is not desired - or no DHCP fallback address is desired.

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

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

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

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

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

**Resolving IPv6 DAD:** The link-local address is formed from an interface identifier based on the hardware address which is supposed to be uniquely assigned. Once the DAD (Duplicate Address Detection) detects the address duplication, the operation on the interface SHOULD be disabled. At this moment, manual intervention is required to resolve the address duplication. For example, check whether the loop occurs in the VLAN or there is indeed other device occupying the same hardware address as the device in the VLAN.

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

**Link-Local Address binding interface:** Configure Link-Local IP address to a different VLAN interface. The first IP interface entry (VLAN1) is the default value.

## IP Routes

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

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

**Mask Length:** The destination IP network or host mask, in number of bits (*prefix length*). It defines how much of a network address that must match in order to qualify for this route. Valid values are 0-32 bits for IPv4 routes or 128 bits 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 link-local, it must specify the next hop VLAN for the gateway.

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

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

## **Buttons**

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

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

**Apply:** Click to save changes.

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

## **Messages:**

*DHCP Per Port IP range (192.168.1.70 - 192.168.1.77) includes interface IP address (192.168.1.77)*

*DHCP Per Port IP range (192.168.1.90 - 192.168.1.99) is not equal to switch TP port number (24)*

## System > IP Address > Status

This page displays the status of the IP protocol layer. The status is defined by the IP interfaces, the IPv6 routes and the neighbor cache (ARP cache) status.

The screenshot shows the Lantronix web interface for device SISPM1040-3166-L3. The left sidebar contains a navigation menu with categories like System, Port Management, PoE Management, VLAN Management, QoS, Spanning Tree, MAC Address Tables, Multicast, DHCP, Security, Access Control, SNMP, CFM, APS, ERPS, Rapid Ring, MRP, PTP, Event Notification, Router, OSPF, and OSPFv3. The main content area is titled 'Status' and includes an 'Auto-refresh' toggle (currently off) and a 'Refresh' button. Below this are four sections:

- IP Interfaces:** A table with columns Interface, Type, Address, and Status.
 

Interface	Type	Address	Status
VLAN 1	LINK	00-c0-f2-7c-59-7f	<UP BROADCAST MULTICAST>
VLAN 1	IPv4	169.254.225.80/16	
VLAN 1	IPv4	192.168.1.77/24	
VLAN 1	IPv6	fe80::2c0:f2ff:fe7c:597f/64	
- IP Routes:** A table with columns Network, Gateway, and Status.
 

Network	Gateway	Status
0.0.0.0/0	192.168.1.254	<UP>
169.254.0.0/16	VLAN 1	<UP>
192.168.1.0/24	VLAN 1	<UP>
- IPv6 Routes:** A table with columns Network, Gateway, and Status.
 

Network	Gateway	Status
fe80::/64	VLAN 1	<UP>
- Neighbour cache:** A table with columns IP Address and Link Address.
 

IP Address	Link Address
169.254.6.57	VLAN 1:00-09-18-4f-bc-3a
169.254.130.145	VLAN 1:ac-cc-8e-ba-f7-c1
192.168.1.99	VLAN 1:00-1b-11-b2-6d-4b

There is also a second 'Neighbour cache' section at the bottom of the page, which is currently empty.

### IP Interfaces

**Interface:** The name of the interface.

**Type:** The address type of the entry. This may be LINK, IPv4 or IPv6.

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

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

**IP Routes**

**Network:** The destination IPv4 network or host address of this route.

**Gateway:** The gateway address of this route.

**Status:** The status flags of the route.

**IPv6 Routes**

**Network:** The destination IPv4/IPv6 network or host address of this route (e.g., fe80::/64).

**Gateway:** The gateway address of this route (e.g., VLAN 1).

**Status:** The status flags of the route (e.g., <UP>).

**Neighbor cache**

**IP Address:** The IPv4/IPv6 address of the entry.

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

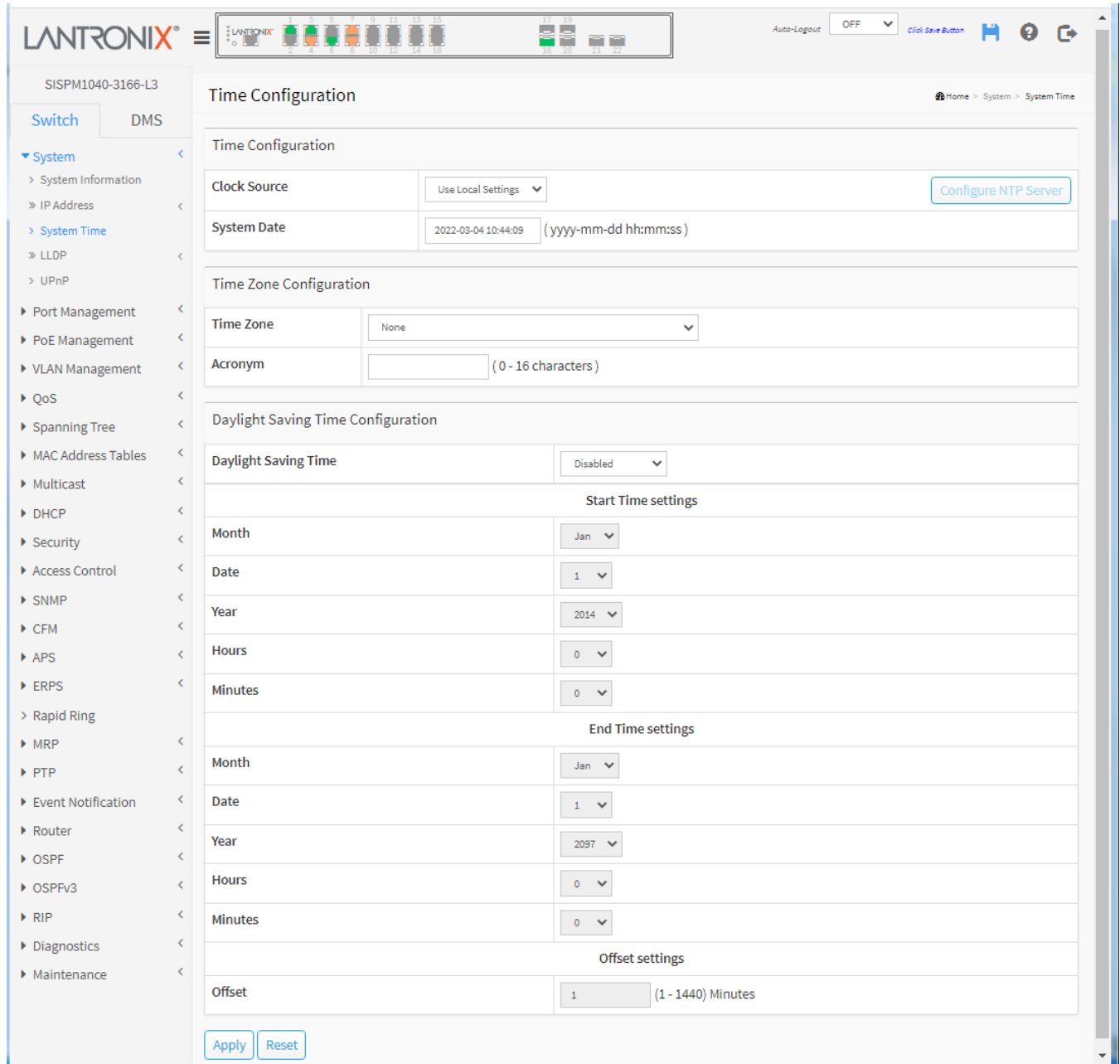
**Buttons**

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

**Refresh:** Click to refresh the page immediately.

## System > System Time

This page lets you configure Time parameters. The switch provides manual and automatic ways to set the system time via NTP. For manual setting enter the Year, Month, Day, Hour and Minute within the valid value range indicated in each item.



### Time Configuration

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

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

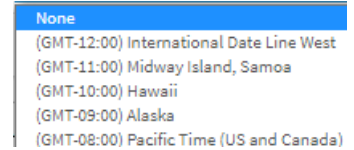
**NTP Server:** Clock Source from NTP Server.

**System Date:** Show the current datetime of the system. The year of system date can be 2011 - 2037.

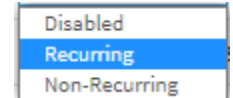
**Time Zone Configuration**

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

**Acronym:** You can set the acronym of the time zone. This is a user-configurable acronym to identify the time zone. The valid range is 0-16 characters (e.g., Pacific – Canada).

**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 'Disabled' to disable 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 Disabled.

**Recurring Configurations****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 (1 440 minutes)

**Non Recurring Configurations****Start time settings**

Month - Select the starting month.

Date - Select the starting date.

Year - Select the starting year.

Hours - Select the starting hour.

Minutes - Select the starting minute.

**End time settings**

Month - Select the ending month.

Date - Select the ending date.

Year - Select the ending year.

Hours - Select the ending hour.

Minutes - Select the ending minute.

**Offset settings**

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

## Buttons

**Configure NTP Server:** Click to display the NTP Configuration page (see below).

**Apply:** Click to save changes.

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

## Configure NTP Server

When you select “Use NTP Server” from the System > System Time menu path, the NTP Configuration page displays.

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

Time Zone is an offset time of 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 determine the local time, otherwise, you will not able to get the correct time. The switch supports configurable time zones from –12 to +13 step 1 hour.

Default Time zone: +8 Hrs.

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

**Automatic:** At the dropdown select Disabled (default) or Enabled.

**Server address via DHCP:** Not used.

**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 restricted to 5,10,15,30,60,120 minutes.

**Server #:** 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.

## System > LLDP > LLDP Configuration

This page lets you view and configure current Link Level Discovery Parameter interface settings.

LLDP is an IEEE 802.1ab standard protocol. The Link Layer Discovery Protocol(LLDP) specified in this standard allows stations attached to an IEEE 802 LAN to advertise, to other stations attached to the same IEEE 802 LAN, the major capabilities provided by the system incorporating that station, the management address or addresses of the entity or entities that provide management of those capabilities, and the identification of the stations point of attachment to the IEEE 802 LAN required by those management entity or entities. The information distributed via this protocol is stored by its recipients in a standard Management Information Base (MIB), making it possible for the information to be accessed by a Network Management System (NMS) using a management protocol such as the Simple Network Management Protocol (SNMP).

The screenshot shows the LLDP Configuration page in the Lantronix web interface. The left sidebar contains a navigation menu with categories like System, Port Management, PoE Management, VLAN Management, QoS, Spanning Tree, MAC Address Tables, Multicast, DHCP, Security, Access Control, and SNMP. The main content area is titled 'LLDP Configuration' and includes a breadcrumb trail: Home > System > LLDP > LLDP Configuration. The 'LLDP Parameters' section contains four rows of configuration fields: Tx Interval (30 seconds), Tx Hold (4 times), Tx Delay (2 seconds), and Tx Reinit (2 seconds). The 'LLDP Port Configuration' section is a table with columns for Port, Mode, CDP aware, Trap, and Optional TLVs (Port Descr, Sys Name, Sys Descr, Sys Capa, Mgmt Addr). The table lists ports 1 through 8, all with 'Enabled' mode and various TLV options checked.

Port	Mode	CDP aware	Trap	Optional TLVs				
				Port Descr	Sys Name	Sys Descr	Sys Capa	Mgmt Addr
*	↔	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
1	Enabled	<input checked="" 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"/>
2	Enabled	<input checked="" 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"/>
3	Enabled	<input checked="" 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"/>
4	Enabled	<input checked="" 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"/>
5	Enabled	<input checked="" 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"/>
6	Enabled	<input checked="" 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"/>
7	Enabled	<input checked="" 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"/>
8	Enabled	<input checked="" 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"/>

### LLDP Parameters

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

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



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

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

### **LLDP Port Configuration**

**Port:** The switch port of the logical LLDP interface.

**Mode:** Select LLDP mode:

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

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

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

**Enabled:** The switch will send out LLDP information, and will analyze LLDP information received from neighbors.

**CDP Aware:** Select CDP awareness. The CDP operation is restricted to decoding incoming CDP frames (the switch doesn't transmit CDP frames). CDP frames are only decoded if LLDP on the interface 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 interfaces have CDP awareness disabled the switch forwards CDP frames received from neighbor devices. If at least one interface has CDP awareness enabled all CDP frames are terminated by the switch.

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

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

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

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

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

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

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

### **Buttons**

**Apply:** Click to save changes.

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

## System > LLDP > LLDP-MED Configuration

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

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

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

The screenshot shows the Lantronix web interface for the LLDP-MED Configuration page. The breadcrumb trail is: Home > System > LLDP > LLDP-MED Configuration. The main configuration area includes a 'Fast Start Repeat Count' field set to 4. Below this is a 'Transmit TLVs' table with columns for Port, Capabilities, Policies, Location, PoE, and Device Type. The table lists ports 1 through 6, all with checkboxes for Capabilities, Policies, Location, and PoE checked, and a 'Connectivity' dropdown for Device Type.

Port	Capabilities	Policies	Location	PoE	Device Type
*	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<>
1	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Connectivity
2	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Connectivity
3	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Connectivity
4	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Connectivity
5	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Connectivity
6	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Connectivity

### Fast Start Repeat Count

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

With this in mind LLDP-MED defines an LLDP-MED Fast Start interaction between the protocol and the application layers on top of the protocol, in order to achieve these related properties. Initially, a Network Connectivity Device will only transmit LLDP TLVs in an LLDPDU. Only after an LLDP-MED Endpoint Device is detected, will an LLDP-MED capable Network Connectivity Device start to advertise LLDP-MED TLVs in outgoing LLDPDUs on the associated interface. 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 do not apply to links between LAN infrastructure elements, including Network Connectivity Devices, or other types of links.

**Transmit TLVs:** It is possible to select which LLDP-MED information that will be transmitted to the neighbors. When the checkbox is checked the information is included in the frame transmitted to the neighbor.

**Port:** The interface name to which the configuration applies.

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

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

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

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

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

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

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

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

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

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

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

Coordinates Location

Latitude	<input type="text" value="0"/> °	North ▾	Longitude	<input type="text" value="0"/> °	East ▾
Altitude	<input type="text" value="0"/>	Meters ▾	Map Datum	WGS84 ▾	

Civic Address Location

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

Emergency Call Service

Emergency Call Service	<input type="text"/>
------------------------	----------------------

Policies

Delete	Policy ID	Application Type	Tag	VLAN ID	L2 Priority	DSCP
No entries present						

[Add New Policy](#)

[Apply](#) [Reset](#)

**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 -2097151.9 to 2097151.9 with a maximum of 1 digits. It is possible to select between two altitude types (floors or meters).

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

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

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

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

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

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

**Civic Address Location:** IETF Geopriv Civic Address based Location Configuration Information (Civic Address LCI). The total number of characters for the combined civic address information must not exceed 250 characters.

**Note** the limitation of 250 characters:

- 1) If more than one civic address location is used, each of the additional civic address locations will use 2 extra characters in addition to the civic address location text.
- 2) The 2 letter country code is not part of the 250 characters limitation.

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

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

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

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

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

**Block (Neighborhood):** Neighborhood, block.

**Street:** Street - Example: Poppelvej.

**Leading street direction:** Leading street direction - Example: N (North).

**Trailing street suffix:** Trailing street suffix - Example: SW (South West).

**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 will be used when selecting the policies that will be mapped to the specific interfaces.

**Application Type:** Intended use of the application (one of eight types):

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

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

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

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

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

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

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

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

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

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

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

**VLAN ID:** VLAN identifier (VID) for the interface 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 IETF RFC 2475.

## Policies

**Add New Policy:** Click the button to add a new policy to the table. Specify the Application type, Tag, VLAN ID, L2 Priority and DSCP for the new policy. Click "Apply". The number of policies supported is 32.

**Policies Interface Configuration:** Every interface may advertise a unique set of network policies or different attributes for the same network policies, based on the authenticated user identity or interface configuration.

**Interface:** The interface name to which the configuration applies.

**Policy Id:** The set of policies that shall apply to a given interface. The set of policies is selected by check marking the checkboxes that corresponds to the policies.

## **Buttons**

**Apply:** Click to save changes.

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



## System > LLDP > LLDP Neighbor

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

Local Port	Chassis ID	Port ID	Port Description	System Name	System Capabilities	Management Address
GigabitEthernet 1/1	00-C0-F2-7C-59-7F	18	GigabitEthernet 1/18	SISPM1040-3166-L3	Bridge(+)	192.168.1.77 (IPv4) - if-index:18
GigabitEthernet 1/4	AC-CC-8E-BA-F7-C1	AC-CC-8E-BA-F7-C1	eth0	axis-acc8ebaf7c1	Bridge(-), WLAN Access Point(-), Router(-), Station Only(+)	192.168.0.90 (IPv4) - if-index:2
GigabitEthernet 1/18	00-C0-F2-7C-59-7F	1	GigabitEthernet 1/1	SISPM1040-3166-L3	Bridge(+)	192.168.1.77 (IPv4) - if-index:1

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

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

**Port ID:** The identification of the neighbor port.

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

**System Name:** The name advertised by the neighbor unit.

**System Capabilities:** Describes the neighbor unit's capabilities. The possible capabilities are 1. Other, 2. Repeater, 3. Bridge, 4. WLAN Access Point, 5. Router, 6. Telephone, 7. DOCSIS cable device, 8. Station only, and 9. Reserved.

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

**Management Address:** Management Address is the neighbor unit's address that is used for higher layer entities to assist discovery by the network management. For example, this could display a link to the LLDP neighbor's IP address.

### Buttons

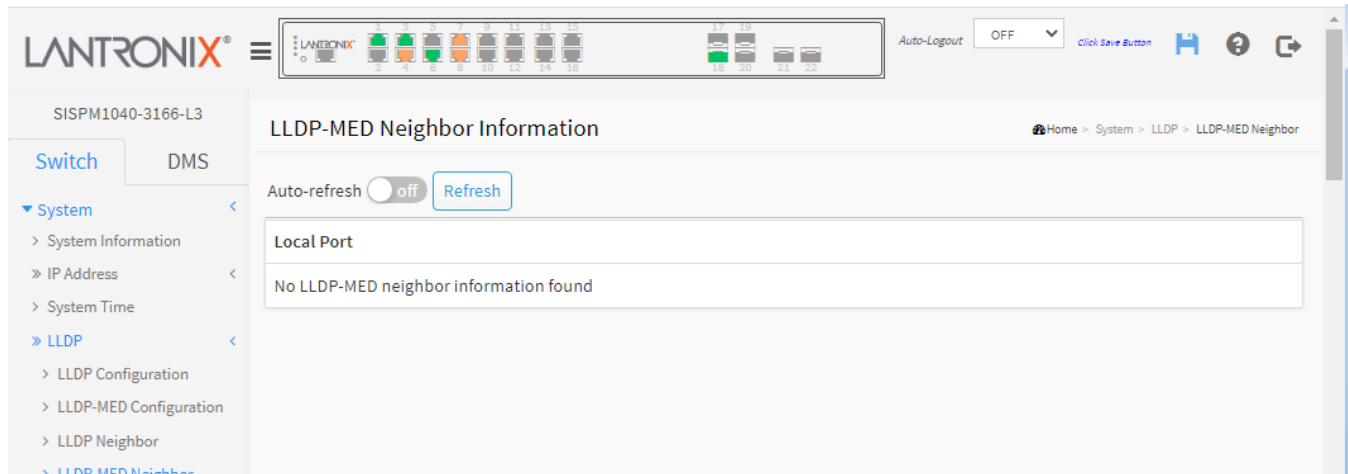
**Auto-refresh:** Check this box to refresh the page automatically every 3 seconds.

**Refresh:** Click to refresh the page.



## System > LLDP > LLDP-MED Neighbor

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



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

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

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

1. LAN Switch/Router
2. IEEE 802.1 Bridge
3. IEEE 802.3 Repeater (included for historical reasons)
4. IEEE 802.11 Wireless Access Point
5. Any device that supports the IEEE 802.1AB and MED extensions defined by TIA-1057 and can relay IEEE 802 frames via any method.

**LLDP-MED Endpoint Device Definition:** LLDP-MED Endpoint Devices, as defined in TIA-1057, are located at the IEEE 802 LAN network edge, and participate in IP communication service using the LLDP-MED framework. Within the LLDP-MED Endpoint Device category, the LLDP-MED scheme is broken into further Endpoint Device Classes, as defined in the following.

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

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

Discovery services defined in this class include LAN configuration, device location, network policy, power management, and inventory management.

**LLDP-MED Media Endpoint (Class II):** The LLDP-MED Media Endpoint (Class II) definition is applicable to all endpoint products that have IP media capabilities however may or may not be associated with a particular end user. Capabilities include all of the capabilities defined for the previous Generic Endpoint Class (Class I), and are

extended to include aspects related to media streaming. Example product categories expected to adhere to this class include (but are not limited to) Voice / Media Gateways, Conference Bridges, Media Servers, and similar.

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

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

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

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

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

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

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

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

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

**Guest Voice Signalling** - for use in network topologies that require a different policy for the guest voice 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 (known).

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

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

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

**VLAN ID:** The VLAN identifier (VID) for the interface 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 interface is used instead.

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

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

### Buttons

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

**Refresh:** Click to refresh the page.

### LLDP-MED Neighbor information Example:

LLDP-MED Neighbor Information Home > System > LLDP > LLDP-MED Neighbor

Auto-refresh  off [Refresh](#)

GigabitEthernet 1/7			
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

## System > LLDP > LLDP Neighbor PoE

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

Local Port	Power Type	Power Source	Power Priority	Maximum Power
GigabitEthernet 1/18	PSE Device	Primary Power Supply	Critical	30 [W]

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

**Power Type:** The Power Type represents whether the device is a Power Sourcing Entity (PSE) or Powered 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:** Represents the priority of the PD device, or the power priority associated with the PSE type device's interface that is sourcing the power. There are three levels of power priority. The three levels are: Critical, High and Low. If the power priority is unknown it is indicated as "Unknown"

**Maximum Power:** The Maximum Power Value contains a numerical value that indicates the maximum power in watts required by a PD device from a PSE device, or the minimum power a PSE device is capable of sourcing over a maximum length cable based on its current configuration.

The maximum allowed value is 102.3 W. If the device indicates value higher than 102.3 W, it is represented as "reserved"

### Buttons

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

**Refresh:** Click to refresh the page.

## System > LLDP > LLDP Neighbor EEE

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

By using EEE power savings can be achieved at the expense of traffic latency. This latency occurs due to that the circuits EEE 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.

The displayed table contains a row for each interface.

If the interface does not support EEE, then it displays as *"EEE not supported for this interface"*.

If EEE is not enabled on particular interface, then it displays as *"EEE not enabled for this interface"*.

If the link partner doesn't support EEE, then it displays as *"Link partner is not EEE capable"*.

Local Port	Tx Tw	Rx Tw	Fallback Receive Tw	Echo Tx Tw	Echo Rx Tw	Resolved Tx Tw	Resolved Rx Tw	EEE in Sync
GigabitEthernet 1/1	0	0	0	0	0	30	30	●
GigabitEthernet 1/4	0	0	0	0	0	30	30	●
GigabitEthernet 1/18	0	0	0	0	0	30	30	●

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

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

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

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

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

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

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

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

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

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

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

#### **Buttons**

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

**Refresh:** Click to refresh the page.

## System > LLDP > LLDP Statistics

This page provides an overview of all LLDP traffic. Two types of counters are shown. Global counters are counters that refer to the whole switch; Local counters refer to per interface counters for the currently selected switch.

**LLDP Global Counters**

Neighbor entries were last changed	2022-03-04T09:31:04+00:00 (5764 secs. ago)
Total Neighbors Entries Added	3
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	195	194	0	0	0	0	0	0
2	0	0	0	0	0	0	0	0
3	195	0	0	0	0	0	0	0
4	196	194	0	0	0	0	0	0
5	0	0	0	0	0	0	0	0
6	195	0	0	0	0	0	0	0
7	196	0	0	0	0	0	0	0
8	195	0	0	0	0	0	0	0

### 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

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

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

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

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

**Frames Discarded:** If a LLDP frame is received on a interface, 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 interface'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 LLDP frame is received with an organizationally TLV, but the TLV is not supported the TLV is discarded and counted.

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

### Buttons

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

**Refresh:** Click to refresh the page.

**Clear:** Clears the counters which have the corresponding checkbox checked.



## System > UPnP

Configure UPnP on this page. The goal of UPnP (Universal Plug and Play) is to allow devices to connect seamlessly and to simplify the implementation of networks in the home (data sharing, communications, and entertainment) and in corporate environments for simplified installation of computer components.

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

**Mode:** Indicates 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. Read only now.

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

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

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

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

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

### Buttons

**Apply:** Click to save changes.

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

# Port Management

This menu section lets you view and set port-related parameters.

## Port Management > Port Configuration

This page lets you view and set current switch port parameters.

Port	Link	Speed		Cable type	Adv Duplex		Adv speed						Flow Control			PFC		Maximum Frame Size	Excessive Collision Mode	Frame Length Check	
		Current	Configured		Fdx	Hdx	10M	100M	1G	2.5G	5G	10G	Enable	Curr Rx	Curr Tx	Enable	Priority				
*																					
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 type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	0-7	10240	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 type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	0-7	10240	Discard	<input type="checkbox"/>
3	●	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 type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	0-7	10240	Discard	<input type="checkbox"/>
4	●	100fdx	Auto		<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	0-7	10240	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 type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	0-7	10240	Discard	<input type="checkbox"/>
6	●	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 type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	0-7	10240	Discard	<input type="checkbox"/>
7	●	100fdx	Auto		<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	0-7	10240	Discard	<input type="checkbox"/>
8	●	100fdx	Auto		<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	0-7	10240	Discard	<input type="checkbox"/>
9	●	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 type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	0-7	10240	Discard	<input type="checkbox"/>
10	●	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 type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	0-7	10240	Discard	<input type="checkbox"/>
11	●	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 type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	0-7	10240	Discard	<input type="checkbox"/>
12	●	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 type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	0-7	10240	Discard	<input type="checkbox"/>
13	●	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 type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	0-7	10240	Discard	<input type="checkbox"/>
14	●	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 type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	0-7	10240	Discard	<input type="checkbox"/>
15	●	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 type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	0-7	10240	Discard	<input type="checkbox"/>
16	●	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 type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	0-7	10240	Discard	<input type="checkbox"/>
17	●	Down	Auto		<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 checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	0-7	10240		<input type="checkbox"/>
18	●	1Gfdx	Auto		<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 checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	0-7	10240		<input type="checkbox"/>
19	●	Down	Auto		<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 checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	0-7	10240		<input type="checkbox"/>
20	●	Down	Auto		<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 checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	0-7	10240		<input type="checkbox"/>
21	●	Down	10Gbps FDX	Auto	<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 checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	0-7	10240		<input type="checkbox"/>
22	●	Down	10Gbps FDX	Auto	<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 checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	0-7	10240		<input type="checkbox"/>

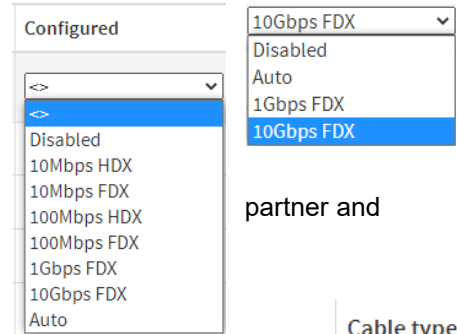
**Port:** This is the logical port number for this row.

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

**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 speeds are:

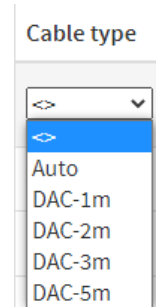
- Disabled** - Disables the switch port operation.
- 10Mbps HDX** - Forces the port in 10Mbps half duplex mode.
- 10Mbps FDX** - Forces the port in 10Mbps full duplex mode.
- 1Gbps FDX** - Forces the port in 1Gbps full duplex
- 10Gbps FDX** - Forces the port in 10Gbps full duplex mode.
- Auto** - Port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



partner and

**Cable Type:** This selection is for 10G ports only (e.g., Ports 29-32):

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



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

**Advertise Speed:** When Speed is set as Auto (auto negotiation) the port will only advertise the specified speeds (10M, 100M, 1G, 2.5G, 5G, or 10G) to the link partner. By default port will advertise all the supported speeds if speed is set as Auto.

Adv speed					
10M	100M	1G	2.5G	5G	10G

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

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

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

**Excessive Collision Mode:** Configure port transmit collision behavior. Can be either:

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

**Frame Length Check:** Configures if frames with incorrect frame length in the EtherType/Length field will be dropped. An Ethernet frame contains a field EtherType which can be used to indicate the frame payload size (in bytes) for values of 1535 and below. If the EtherType/Length field is above 1535, it indicates that the field is used as an EtherType (indicating which protocol is encapsulated in the payload of the frame). If "Frame Length Check" is enabled, frames with payload size less than 1536 bytes are dropped, if the EtherType/Length field doesn't match the actual payload length. If "frame length check" is disabled, frames are not dropped due to frame length mismatch. **Note:** No drop counters count frames dropped due to frame length mismatch

### Buttons

**Apply:** Click to save changes.

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

**Refresh:** Click to refresh the page. Any changes made locally will be undone.

**Messages:** *Both PFC and Flow Control cannot both be enabled for the same port*

## Port Management > Port Statistics

This page displays an overview of general traffic statistics for all switch ports.

The screenshot shows the 'Port Statistics' page for a Lantronix switch. The page title is 'Port Statistics' and the breadcrumb is 'Home > Port Management > Port Statistics'. There are controls for 'Auto-refresh' (set to 'off'), 'Refresh', and 'Clear'. Below this is a table titled 'Port Statistics Overview'.

Port	Packets		Bytes		Errors		Drops		Filtered
	Received	Transmitted	Received	Transmitted	Received	Transmitted	Received	Transmitted	Received
1	275	148944	63416	12214158	0	0	0	0	0
2	0	0	0	0	0	0	0	0	0
3	14980	161013	2552936	17979515	0	0	40	0	188
4	6236	145151	2268989	11273160	0	0	0	0	2
5	0	0	0	0	0	0	0	0	0
6	0	148935	0	12210442	0	0	0	0	0
7	840	148110	289056	11923152	0	0	0	0	0
8	4611	146281	2075608	11225324	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

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

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

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

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

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

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

### Buttons

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

**Refresh:** Click to refresh the page immediately.

**Clear:** Clears the counters for all ports.

## Detailed Port Statistics

When you click a linked Port number its Detailed Port Statistics display. 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.

The screenshot shows the 'Detailed Port Statistics Port 3' page. At the top, there are 'Auto-refresh' controls (off), 'Refresh', and 'Clear' buttons, along with a 'Port 3' dropdown menu. The main data is presented in a table with the following structure:

Receive Total		Transmit Total	
Rx Packets	15141	Tx Packets	162437
Rx Octets	2581229	Tx Octets	18151780
Rx Unicast	11786	Tx Unicast	15401
Rx Multicast	294	Tx Multicast	9279
Rx Broadcast	3061	Tx Broadcast	137757
Rx Pause	0	Tx Pause	0
Receive Size Counters		Transmit Size Counters	
Rx 64 Bytes	11581	Tx 64 Bytes	136605
Rx 65-127 Bytes	290	Tx 65-127 Bytes	12940
Rx 128-255 Bytes	298	Tx 128-255 Bytes	857
Rx 256-511 Bytes	53	Tx 256-511 Bytes	7834
Rx 512-1023 Bytes	2919	Tx 512-1023 Bytes	732
Rx 1024-1526 Bytes	0	Tx 1024-1526 Bytes	3469
Rx 1527- Bytes	0	Tx 1527- Bytes	0
Receive Queue Counters		Transmit Queue Counters	
Rx Q0	15141	Tx Q0	31029
Rx Q1	0	Tx Q1	0
Rx Q2	0	Tx Q2	0
Rx Q3	0	Tx Q3	0
Rx Q4	0	Tx Q4	0

### 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.

**Note 1:** Short frames are frames that are smaller than 64 bytes.

**Note 2:** 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.

**Receive MM Counters:** Rx MM Fragments: A count of received MAC frame fragments.

**Rx MM Assembly Ok:** A count of MAC frames that were successfully reassembled and delivered to MAC.

**Rx MM Assembly Errors:** A count of MAC frames with reassembly errors. The counter is incremented when the ASSEMBLY\_ERROR state of the Receive Processing State Diagram is entered.

**Rx MM SMD Errors:** A count of received MAC frames / MAC frame fragments rejected due to unknown SMD value or arriving with an SMD-C when no frame is in progress. The counter is incremented each time the BAD\_FRAG state of the Receive Processing State Diagram is entered.

**Transmit MM Counters**

**Tx MM Fragments:** A count of transmitted MAC frame fragments.

**Tx MM Hold:** A count of times MM\_CTL.request(HOLD) primitive assertion caused preemption of a preemptable MAC frame.

**Buttons**

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

**Refresh:** Click to refresh the page immediately.

**Clear:** Clears the counters for the selected port.

 : The port select box determines which port's information is displayed.

## Port Management > SFP Port Info

This page displays general SFP information and monitoring information.

The screenshot shows the 'SFP Information for Port 17' page in the Lantronix web interface. The page includes a navigation menu on the left with options like System, Port Management, PoE Management, etc. The main content area displays a table of SFP information for Port 17, with an 'Auto-refresh' toggle set to 'off' and a 'Refresh' button. The table lists various parameters such as Connector Type, Fiber Type, Tx Central Wavelength, Bit Rate, Vendor OUI, Vendor Name, Vendor P/N, Vendor Revision, Vendor Serial Number, Date Code, Temperature, Vcc, and Monitors (Mon1, Mon2, Mon3).

Parameter	Value
Connector Type	SFP or SFP Plus - LC
Fiber Type	LC
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	8672217
Date Code	091215
Temperature	48.53 C
Vcc	3.33 V
Mon1 (Bias)	14 mA
Mon2 (TX PWR)	-6.47 dBm
Mon3 (RX PWR)	-25.85 dBm

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

**Fiber Type:** Displays the fiber channel transmission media.

**Tx Central Wavelength:** Displays the nominal transmitter output wavelength in nanometers (nm).

**Bit Rate:** Displays the nominal bit rate of the transceiver.

**Vendor OUI:** Displays the vendor IEEE company ID.

**Vendor Name:** Displays the vendor name.

**Vendor P/N:** Displays the vendor part number or product name.

**Vendor Revision:** Displays the vendor'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 refresh the page immediately.

**Clear:** Clears the counters for all ports.

: The port select box determines which port's information is displayed.

**Example:** SFP Information for a DAC cable:

The screenshot shows the 'SFP Information for Port 21' page in the Lantronix web interface. The page includes a navigation sidebar on the left with categories like System, Port Management, PoE Management, VLAN Management, QoS, Spanning Tree, MAC Address Tables, Multicast, DHCP, and Security. The main content area features a table with the following SFP details:

Connector Type	SFP or SFP Plus - Copper Pigtail
Fiber Type	Reserved
Tx Central Wavelength	256
Bit Rate	10 Gbps
Vendor OUI	00-c0-f2
Vendor Name	Transition
Vendor P/N	DAC-10G-SFP-01M
Vendor Revision	G
Vendor Serial Number	18102063725
Date Code	180416
Temperature	none
Vcc	none
Mon1 (Bias)	none
Mon2 (TX PWR)	none
Mon3 (RX PWR)	none

## Port Management > Energy Efficient Ethernet

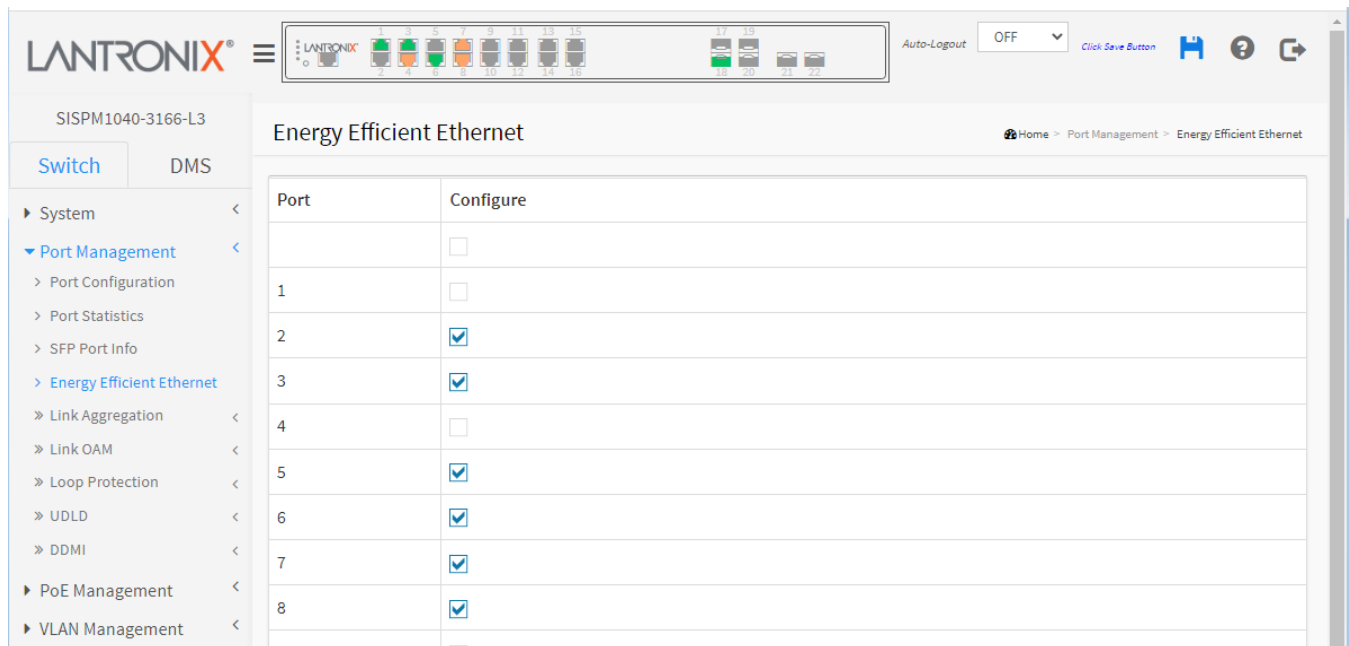
This page lets you configure the port power savings features.

EEE is a power saving option that reduces the power usage when there is low or no traffic utilization.

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



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

**Configure:** Controls whether EEE is enabled for this switch port.

### Buttons

**Apply:** Click to save changes.

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

## Port Management > Link Aggregation > Static Configuration

This page lets you configure Aggregation hash mode and the aggregation group. Aggregation involves using multiple ports in parallel to increase link speed beyond the limits of a port and to increase redundancy for higher availability. (Also *Port Aggregation, Link Aggregation*).

The screenshot shows the 'Aggregation Static Configuration' page. At the top, there are navigation tabs for 'Switch' and 'DMS'. A sidebar on the left lists various configuration categories like System, Port Management, Link Aggregation, etc. The main content area is divided into two sections: 'Hash Code Contributors' and 'Aggregation Group Configuration'.

**Hash Code Contributors:**

- Source MAC Address:
- Destination MAC Address:
- IP Address:
- TCP/UDP Port Number:

**Aggregation Group Configuration:**

Group ID	Port Members																						Group Configuration		
	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	Mode	Revertive	Max Bundle
Normal	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>			
1	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	Disabled	<input checked="" type="checkbox"/>	22
2	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	LACP (Active)	<input checked="" type="checkbox"/>	2
3	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	Static	<input checked="" type="checkbox"/>	22
4	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	LACP (Active)	<input checked="" type="checkbox"/>	2
5	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	LACP (Passive)	<input checked="" type="checkbox"/>	2
6	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	Disabled	<input checked="" type="checkbox"/>	22
7	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	Disabled	<input checked="" type="checkbox"/>	22
8	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	Disabled	<input checked="" type="checkbox"/>	22
9	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	Disabled	<input checked="" type="checkbox"/>	22

### Hash Code Contributors

**Source MAC Address:** Check the box to include the SMAC in the Hash Code. 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:** Check the box to include the DMAC in the Hash Code. 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:** Check the box to include the IP Address in the Hash Code. 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:** Check the box to include the TCP/UDP port number in the Hash Code. 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:** Column displays a row for the “Normal” group (with all Port Members selected by default) and a row for each of Group IDs 1-16 (max). Group ID "Normal" indicates there is no aggregation. Only one group ID is valid per port.

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

### Group Configuration

**Mode:** This parameter determines the mode for the aggregation group.

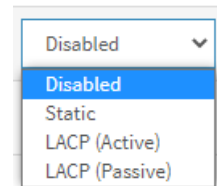
**Disabled:** The group is disabled.

**Static:** The group operates in static aggregation mode.

**LACP (Active):** The group operates in LACP active aggregation mode. See IEEE 801.AX-2014, section 6.4.1 for details. Active: Enables LACP unconditionally.

**LACP (Passive):** The group operates in LACP passive aggregation mode. See IEEE 801.AX-2014, section 6.4.1 for details. Passive: Enables LACP only when an LACP device is detected.

Mode



**Revertive:** This parameter only applies to LACP-enabled groups. It determines if the group will perform automatic link (re-)calculation when links with higher priority become available.

**Revertive mode:** When a higher priority port in active/standby configuration comes back up, it becomes active again and the current active port (if it has lower priority) becomes standby.

**Non-revertive mode:** if a port comes back up, nothing changes and traffic is not disturbed.

**Max Bundle:** This parameter only applies to LACP-enabled groups. It determines the maximum number of active bundled LACP ports allowed in an aggregation. When the number of members that have formed aggregation reach this value, remaining ports are set to standby and do not forward any frames

### **Buttons**

**Apply:** Click to save changes.

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

### **Messages:**

*Aggregation Error (set LACP config) Max bundle overflow*

*Aggregation Error (set group config) Port already in another group*

## Port Management > Link Aggregation > LACP Port Configuration

This page lets you set Link Aggregation Control Protocol port parameters. LACP is an IEEE 802.3ad standard protocol. LACP allows bundling several physical ports together to form a single logical port.

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

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

**Port:** The switch port number.

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

**Key:** The Key value incurred by the port, in the range 1-11.

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

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

**Prio:** Controls the priority of the port, range 1-65535. 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. The default is **32768**.

### Buttons

**Apply:** Click to save changes.

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

### Messages:

*LACP Error The aggregation cannot include more than 16 ports*

*LACP Error Invalid key*

*'Key' must be an integer value between 1 and 5*

## Port Management > Link Aggregation > System Status

This page provides a status overview for all LACP instances.

The screenshot shows the 'LACP System Status' page in the Lantronix web interface. The page title is 'LACP System Status' and the breadcrumb trail is 'Home > Port Management > Link Aggregation > System Status'. The page includes an 'Auto-refresh' toggle set to 'off' and a 'Refresh' button. Below this is a table with the following columns: 'Aggr ID', 'Name', 'Partner System ID', 'Partner Key', 'Partner Prio', 'Last Changed', and 'Local Ports'. The table content is empty, with the message 'No ports enabled or no existing partners' displayed in the first row. The left navigation menu shows 'Port Management' selected, with sub-items 'Port Configuration' and 'Port Statistics'. The top header shows the system ID 'SISPM1040-3166-L3' and an 'Auto-Logout' dropdown set to 'OFF'.

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

**Name:** Name of the Aggregation group ID.

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

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

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

**Last changed:** The time since this aggregation changed.

**Local Ports:** Shows which ports are a part of this aggregation for this switch.

### Buttons

**Auto-refresh:** Automatic refresh occurs every 3 seconds.

**Refresh:** Click to refresh the page immediately.

### Messages:

*No ports enabled or no existing partners*

*Group 1 member counts error!! Local aggregation must include 2-16 ports*

*Aggregation Error (set group config) LACP aggregation is enabled*

## Port Management > Link Aggregation > Port Status

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

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

**Port:** The switch port number.

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

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

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

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

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

**Partner Prio:** The partner's port priority.

### Buttons

**Auto-refresh:** Automatic refresh occurs every 3 seconds.

**Refresh:** Click to refresh the page immediately.

## Port Management > Link OAM > Port Settings

This page lets you set and view current Link OAM port parameters. OAM (Operation Administration and Maintenance) is a protocol described in ITU-T Y.1731 used to implement Carrier Ethernet functionality. MEP functions such as CC and RDI are based on this.

Port	OAM Enabled	OAM Mode	Loopback Support	Link Monitor Support	MIB Retrieval Support	Loopback Operation
*	<input type="checkbox"/>	<input type="text" value="Passive"/>	<input type="checkbox"/>	<input 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"/>

**Port:** The switch port number. Click a linked port number to display its Detailed Link OAM Status (see below).

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

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

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

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



## Buttons

**Apply:** Click to save changes.

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

## Detailed Link OAM Status

On the Link OAM Port Configuration page, click a linked port number to display its Detailed Link OAM Status. This page provides Link OAM configuration operational status. The displayed fields shows the active configuration status for the selected port.

The screenshot displays the 'Detailed Link OAM Status for Port 3' page. At the top, there is a dropdown menu for 'Port 3', an 'Auto-refresh' toggle set to 'off', and a 'Refresh' button. Below this, a table shows configuration details for PDU Permission (Receive only), Discovery State (Fault state), and Peer MAC Address (-----). A larger table below compares 'Local' and 'Peer' settings for various OAM features.

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

### Local and Peer:

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

**Unidirectional Operation Support:** This feature cannot be configured by the user. The information 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:** It represents the largest OAMPDU, in octets, supported by the DTE. This value is compared to the remotes Maximum PDU Size and the smaller of the two is used.

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

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

**Discovery State:** Displays the current state of the discovery process. Possible states are Fault state, Active state, Passive state, SEND\_LOCAL\_REMOTE\_STATE, SEND\_LOCAL\_REMOTE\_OK\_STATE, SEND\_ANY\_STATE.

### Buttons

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

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

**Refresh:** Click to refresh the page immediately.

## Port Management > Link OAM > Event Settings

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

The screenshot shows the 'Link Event Configuration for Port 1' page. At the top, there is a header with the Lantronix logo, a menu icon, and a status bar showing 'Auto-Logout OFF'. Below the header, there is a breadcrumb trail: 'Home > Port Management > Link OAM > Event Settings'. The main content area features a dropdown menu for 'Port 1' and 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	1	1
Symbol Period Error Event	1	1
Seconds Summary Event	60	1

Below the table are 'Apply' and 'Reset' buttons.

**Port:** The switch port number.

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

**Error Window:** Represents the window period in the order of 1 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 between 1-60 and its default value is '1'. Whereas Error Threshold must be between 0-4294967295 and its default value is '1'.

**Symbol Period Error Event:** 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 between 1-60 and its default value is '1'. Whereas Error Threshold must be between 0-4294967295 and its default value is '1'.

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

### Buttons

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

**Apply:** Click to save changes.

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

## Port Management > Link OAM > Statistics

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

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

The screenshot shows the 'Detailed Link OAM Statistics for Port 5' page. The interface includes a navigation menu on the left with categories like System, Port Management, and Link OAM. The main content area features a table with two columns: 'Receive Total' and 'Transmit Total'. The table lists various OAM statistics, all of which are currently at 0. The statistics include Rx and Tx OAM Information PDU's, Rx and Tx Unique Error Event Notification, Rx and Tx Duplicate Error Event Notification, Rx and Tx Loopback Control, Rx and Tx Variable Request, Rx and Tx Variable Response, Rx and Tx Org Specific PDU's, Rx and Tx Unsupported Codes, Rx and Tx Link Fault PDU's, Rx and Tx Dying Gasp, and Rx and Tx Critical Event PDU's.

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

### 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

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

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

**Refresh:** Click to refresh the page immediately.

**Clear:** Clears the counters for the selected port.

### Messages:

*Error while configuring the OAM loopback*

## Port Management > Link OAM > Event Status

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

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.

The screenshot shows the Lantronix web interface for 'SISPM1040-3166-L3'. The main content area is titled 'Detailed Link OAM Link Status for Port 1'. It features a navigation menu on the left with categories like System, Port Management, PoE Management, VLAN Management, QoS, Spanning Tree, MAC Address Tables, Multicast, DHCP, Security, Access Control, SNMP, CFM, APS, ERPS, and Rapid Ring. The main area has a dropdown for 'Port 1', an 'Auto-refresh' toggle (currently off), and a 'Refresh' button. Below this is a table with columns for 'Local Frame Error Status', 'Remote Frame Error Status', 'Local Frame Period Status', 'Remote Frame Period Status', 'Local Symbol Period Status', and 'Remote Symbol Period Status'. The table contains 24 rows of data, all showing a value of 0. The rows are: Sequence Number, Frame Error Event Timestamp, Frame error event window, Frame error event threshold, Frame errors, Total frame errors, Total frame error events, Frame Period Error Event Timestamp, Frame Period Error Event Window, Frame Period Error Event Threshold, Frame Period Errors, Total frame period errors, Total frame period error events, Symbol Period Error Event Timestamp, Symbol Period Error Event Window, Symbol Period Error Event Threshold, Symbol Period Errors, Total symbol period errors, Total Symbol period error events, Local Event Seconds Summary Status, and Remote Event Seconds Summary Status.

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

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

**Frame error event window:** This two-octet field indicates the duration of the period in 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.

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

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

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

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

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

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

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

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

**Buttons**

**Port select box:** Select which port's information to display.

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

**Refresh:** Click to refresh the page.



## Port Management > Loop Protection > Configuration

This page lets you view and set current Loop Protection parameters.

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

Port	Enable	Action	Tx Mode
*	<input type="checkbox"/>	<	<
1	<input checked="" type="checkbox"/>	Log Only	Enable
2	<input checked="" type="checkbox"/>	Shutdown Port and Log	Enable
3	<input checked="" type="checkbox"/>	Shutdown Port and Log	Enable
4	<input checked="" type="checkbox"/>	Log Only	Disable
5	<input checked="" type="checkbox"/>	Shutdown Port	Enable
6	<input checked="" type="checkbox"/>	Shutdown Port	Enable
7	<input checked="" type="checkbox"/>	Shutdown Port	Enable
8	<input checked="" type="checkbox"/>	Shutdown Port	Enable

### Global Configuration

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

**Transmission Time:** The interval between each loop protection PDU sent on each port. Valid values are 1-10 seconds. The default is 5 seconds.

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

### Port Configuration

**Port:** The switch port number of the port.

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

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

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

### Buttons

**Apply:** Click to save changes.

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

## Port Management > Loop Protection > Status

This page displays the loop protection port status the ports of the switch.

The screenshot shows the 'Loop Protection Status' page in the Lantronix web interface. The page title is 'Loop Protection Status' and the breadcrumb trail is 'Home > Port Management > Loop Protection > Status'. The device name is 'SISPM1040-3166-L3'. There are two tabs: 'Switch' (selected) and 'DMS'. A left-hand navigation menu lists various system and management options. The main content area features an 'Auto-refresh' toggle set to 'off' and a 'Refresh' button. Below this is a table with the following data:

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

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

**Action:** The currently configured port action.

**Transmit:** The currently configured port transmit mode.

**Loops:** The number of loops detected on this port.

**Status:** The current loop protection status of the port.

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

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

### Buttons

**Auto-refresh:** Check this box to enable an automatic refresh of the page every 3 seconds.

**Refresh:** Click to refresh the page immediately.

## Port Management > UDLD > UDLD Configuration

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

Port	UDLD mode	Message Interval
*	⊞	
1	Normal	7
2	Aggressive	7
3	Aggressive	7
4	Normal	7
5	Normal	7
6	Normal	7
7	Normal	7

**Port:** Port number of the switch.

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

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

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

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

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

### Buttons

**Apply:** Click to save changes.

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

## Port Management > UDLD > UDLD Status

This page displays the UDLD status of each port.

The screenshot shows the 'Detailed UDLD Status for Port 1' page. The 'UDLD Status' table is as follows:

UDLD Admin state	Enable
Device ID(local)	00-C0-F2-7C-59-7F
Device Name(local)	SISPM1040-3166-L3
Bidirectional State	Bi-directional

The 'Neighbor Status' table is as follows:

Port	Device Id	Link Status	Device Name
18	00-C0-F2-7C-59-7F	Bi-directional	SISPM1040-3166-L3

### UDLD Status

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

**Device ID(local):** The ID of Device.

**Device Name(local):** Name of the Device.

**Bidirectional State:** The current state of the port.

### Neighbor Status

**Port:** The current port of neighbor device.

**Device ID:** The current ID of neighbor device.

**Link Status:** The current link status of neighbor port.

**Device Name:** Name of the Neighbor Device.

### **Buttons**

**Auto-refresh:** Check this box to enable an automatic refresh of the page at regular intervals.

**Refresh:** Click to refresh the page immediately.

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

## Port Management > DDMI > Configuration

This page lets you configure DDMI mode and provides an overview of DDMI port parameters..

DDMI (Digital Diagnostics Monitoring Interface) provides an enhanced digital diagnostic monitoring interface for optical transceivers which allows real time access to device operating parameters.

The screenshot shows the Lantronix web interface for the SISPM1040-3166-L3 device. The page title is "DDMI Configuration". The navigation menu on the left includes "System", "Port Management", "PoE Management", "VLAN Management", and "QoS". The "Port Management" section is expanded to show "DDMI Configuration".

The main content area includes an "Auto-refresh" toggle set to "off" with a "Refresh" button. Below this is the "DDMI Configuration" section with a "Mode" toggle set to "on" and "Apply" and "Reset" buttons. The "DDMI Overview" section contains a table with the following data:

Port	Vendor	Part Number	Serial Number	Revision	Data Code	Transceiver
17	Transition	TN-SFP-SXD	8672217	0000	2009-12-15	1000BASE_SX
18	Transition	TN-10GSFP-SR	8801095	0001	2012-07-31	10G_SR
19	-	-	-	-	-	-
20	-	-	-	-	-	-
21	Transition	DAC-10G-SFP-01M	18102063725	G	2018-04-16	10G_DAC
22	-	-	-	-	-	-

### DDMI Configuration

**Mode:** Indicates the DDMI mode operation. Possible modes are:

- On:** Enable DDMI mode operation.
- Off:** Disable DDMI mode operation.

### **Buttons**

**Apply:** Click to save changes.

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

### DDMI Overview

**Port:** The DDMI port. You can click a linked Port number to display its Transceiver Information page (see below).

**Vendor:** Displays the SFP vendor name.

**Part Number:** Displays the SFP vendor part number (PN).

**Serial Number:** Displays the SFP vendor serial number (SN).

**Revision:** Indicates revision level for provided by vendor.

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

**Transceiver:** Indicates Transceiver compatibility (e.g., 10G\_SR or 1000BASE\_SX).

## Port Management > DDMI > Status

This page displays detailed DDMI information.

The screenshot shows the Lantronix web interface for device SISPM1040-3166-L3. The left sidebar contains a navigation menu with 'Port Management' expanded to 'DDMI' and 'Status'. The main content area is titled 'Transceiver Information' and includes an 'Auto-refresh' toggle (set to 'off') and a 'Refresh' button. Below this is a table of transceiver details for Port 18:

Vendor	Transition
Part Number	TN-10GSFP-SR
Serial Number	8801095
Revision	0001
Data Code	2012-07-31
Transceiver	10G_SR

Below the transceiver information is a 'DDMI Information' table with the following data:

Type	Current	High Alarm Threshold	High Warn Threshold	Low Warn Threshold	Low Alarm Threshold
Temperature(C)	44.031	90.000	85.000	0.000	-5.000
Voltage(V)	3.3216	3.6000	3.5000	3.1000	3.0000
Tx Bias(mA)	5.488	20.000	15.000	2.000	1.000
Tx Power(mW)	0.5296	1.0000	0.7943	0.1862	0.1479
Rx Power(mW)	0.1892	1.0000	0.7943	0.1023	0.0646
++ : high alarm		+ : high warning		- : low warning	
				-- : low alarm	

### Transceiver Information:

**Vendor:** Displays the SFP vendor name.

**Part Number:** Displays the SFP vendor part number (PN).

**Serial Number:** Displays the SFP vendor serial number (SN).

**Revision:** Indicates revision level provided by vendor.

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

**Transceiver:** Indicates Transceiver compatibility (e.g., 10G\_SR or 1000BASE\_SX).

### DDMI Information

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

**High Alarm Threshold:** The high alarm threshold value of temperature, voltage, TX bias, TX power, and RX power.

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

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

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

**Key:** ++ : high alarm      + : high warning      - : low warning      -- : low alarm

### Buttons

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

**Refresh:** Click to refresh the page immediately.

**Port select box:** At the dropdown select which port's data to be displayed.



## PoE Management

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

### PoE Management > PoE Configuration

This page lets you view and set current PoE port settings; it also displays the primary power supply output.

The screenshot shows the PoE Configuration page for a Lantronix switch. The interface includes a top navigation bar with the Lantronix logo and a status bar with 'Auto-Logout OFF'. A left sidebar contains a navigation menu with 'PoE Management' expanded to 'PoE Configuration'. The main content area is titled 'PoE Configuration' and contains several configuration 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 section with a 'Primary Power Supply [W]' input field set to 250.
- PoE Port Configuration:** A table with the following columns: Port, PoE Mode, PoE Schedule, Priority, Maximum Power [W], Delay Mode, and Delay Time(0~300 sec). The table lists ports 1 through 7, all with PoE Mode set to 'Enabled', PoE Schedule set to 'Disabled', and Maximum Power set to 30W.

### PoE Configuration

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

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

**Allocated** mode: In this mode the user allocates the amount of power that each port may reserve. The allocated/reserved power for each port/PD is specified in the Maximum Power fields.

**LLDP-MED** mode: This mode is similar to the Class mode expect that each port determines the amount power it reserves by exchanging PoE information using the LLDP protocol and reserves power accordingly. If no LLDP information is available for a port, the port will reserve power using the class mode. In this 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 ports priority. If two ports have the same priority the port with the highest port number is shut down.

**Reserved Power:** In this mode the ports are shut down when total reserved power 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 Configuration**

**Capacitor Detection:** Check the box to set the Capacitor Detection mode to Enabled.

### **PoE Power Supply Configuration**

**Primary Power Supply (W):** For being able to determine the amount of power the PD may use; it must be defined what amount of power a power source can deliver. Valid values are 0-370 Watts.

### **Port Configuration**

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

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

**Disabled:** PoE disabled for the port.

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

**PoE Schedule:** The PoE Schedule is defined by Schedule Profile. User can define the profiles for the scheduling.

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

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

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

**Enabled:** Enable POE Power Delay.

**Disabled:** Disable POE Power Delay.

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

### **Buttons**

**Apply:** Click to save changes.

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

## PoE Management > PoE Status

This page displays the current status for all PoE ports.

Local Port	PD class	Power Requested	Power Allocated	Power Used	Current Used	Priority	Port Status
1	1	30 [W]	30 [W]	1.7 [W]	32 [mA]	Critical	PoE turned ON
2	-	0 [W]	0 [W]	0 [W]	0 [mA]	High	No PD detected
3	-	0 [W]	0 [W]	0 [W]	0 [mA]	High	No PD detected
4	3	30 [W]	30 [W]	4.8 [W]	73 [mA]	High	PoE turned ON
5	-	0 [W]	0 [W]	0 [W]	0 [mA]	High	No PD detected
6	1	20 [W]	20 [W]	1.8 [W]	32 [mA]	Low	PoE turned ON
7	4	20 [W]	20 [W]	6.3 [W]	98 [mA]	Low	PoE turned ON
8	2	15 [W]	15 [W]	1.8 [W]	34 [mA]	Low	PoE turned ON
9	-	0 [W]	0 [W]	0 [W]	0 [mA]	Low	No PD detected

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

**PD Class:** Each PD (Powered Device) 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:** Shows the requested amount of power the PD wants to be reserved.

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

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

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

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

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

**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.

The bottom row of the table displays the total Power Requested, Power Allocated, Power Used, and Current Used

## Buttons

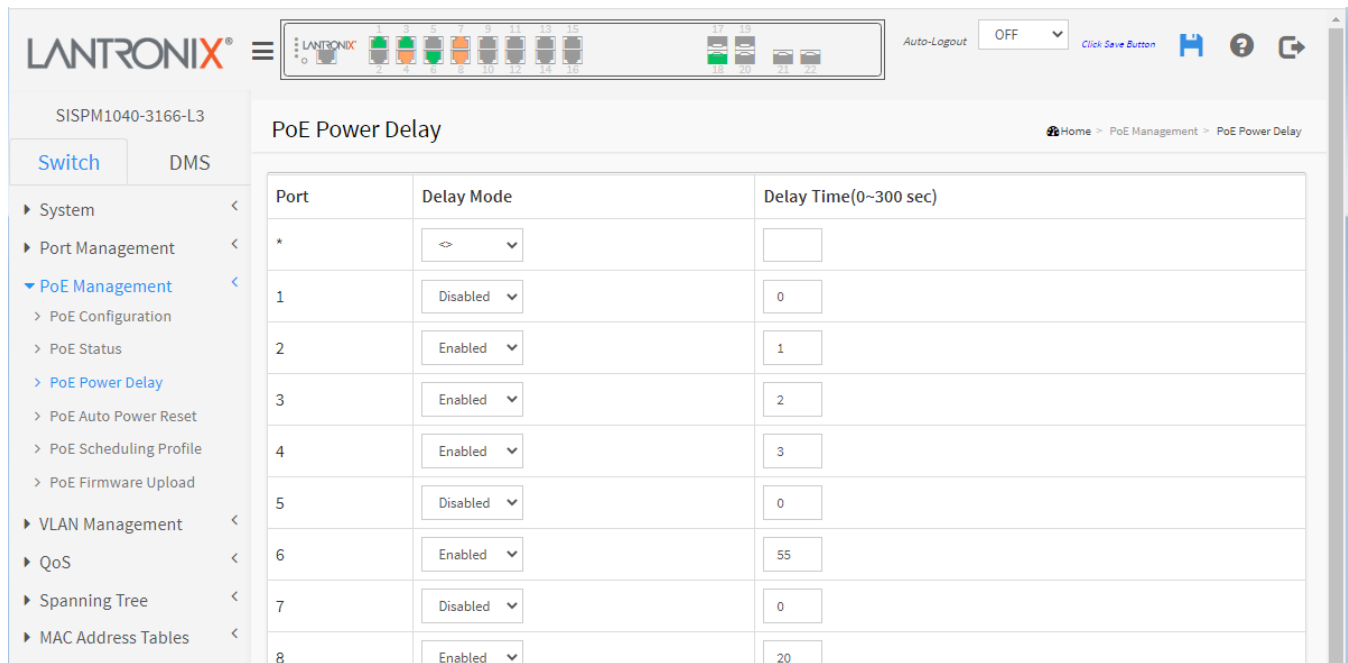
**Auto-refresh:** Check this box to refresh the page automatically every 3 seconds.

**Refresh:** Click to refresh the page.

**Note:** At SISPM1040-3248-L3 FW v 8.10.0086: Ports 25-32 do not support PoE and no longer show on PoE Status page.

## PoE Management > PoE Power Delay

This page lets you view and set the delay time of power being provided after a device rebooted.



The screenshot shows the Lantronix web interface for the SISPM1040-3166-L3 device. The page title is "PoE Power Delay". The breadcrumb navigation is "Home > PoE Management > PoE Power Delay". The left sidebar shows a navigation menu with "PoE Management" expanded to "PoE Power Delay". The main content area contains a table with the following data:

Port	Delay Mode	Delay Time(0~300 sec)
*	<input type="checkbox"/>	<input type="text"/>
1	Disabled	0
2	Enabled	1
3	Enabled	2
4	Enabled	3
5	Disabled	0
6	Enabled	55
7	Disabled	0
8	Enabled	20

**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 out of delay time. The default is 0 (no delay); the valid range is 0-300 seconds.

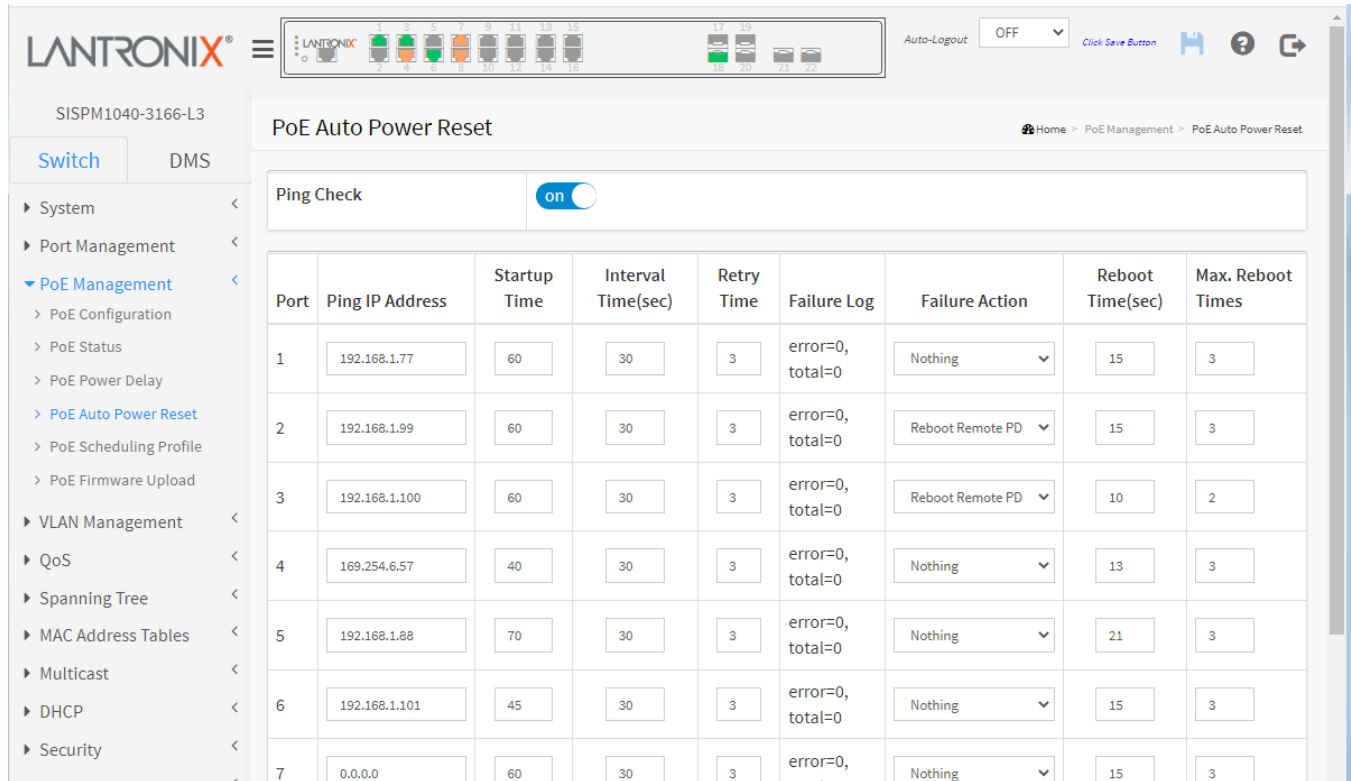
## Buttons

**Apply:** Click to save changes.

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

## PoE Management > PoE Auto Checking

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



The screenshot shows the 'PoE Auto Power Reset' configuration page. At the top, there is a 'Ping Check' toggle switch set to 'on'. Below this is a table with 7 rows, each representing a port configuration. The table columns are: Port, Ping IP Address, Startup Time, Interval Time(sec), Retry Time, Failure Log, Failure Action, Reboot Time(sec), and Max. Reboot Times.

Port	Ping IP Address	Startup Time	Interval Time(sec)	Retry Time	Failure Log	Failure Action	Reboot Time(sec)	Max. Reboot Times
1	192.168.1.77	60	30	3	error=0, total=0	Nothing	15	3
2	192.168.1.99	60	30	3	error=0, total=0	Reboot Remote PD	15	3
3	192.168.1.100	60	30	3	error=0, total=0	Reboot Remote PD	10	2
4	169.254.6.57	40	30	3	error=0, total=0	Nothing	13	3
5	192.168.1.88	70	30	3	error=0, total=0	Nothing	21	3
6	192.168.1.101	45	30	3	error=0, total=0	Nothing	15	3
7	0.0.0.0	60	30	3	error=0, total=0	Nothing	15	3

**Ping Check:** When set to **on**, the Ping Check function can detect the connection between the PoE port and the powered device. Setting to **off** will disable the detection.

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

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

**Startup Time:** When a PD has been started up, the switch will wait Startup 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 a PoE port can't ping the PD, it will try to send detection again. When this setting is reached, it will trigger failure action. The default is 3 retries; the valid range is 1-5 retry attempts.

**Failure Log:** Displays the failure loggings counter.

**Failure Action:** The action to be taken when the third fail detection.

**Nothing:** Keep Pinging the remote PD but does nothing further.

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

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

**Max. Reboot Times:** When Failure Action is Reboot Remote PD, it limits times of Reboot. The default is 3 reboot attempts, the valid range is 0-10 reboot attempts. A setting of 0 means unlimited reboots.

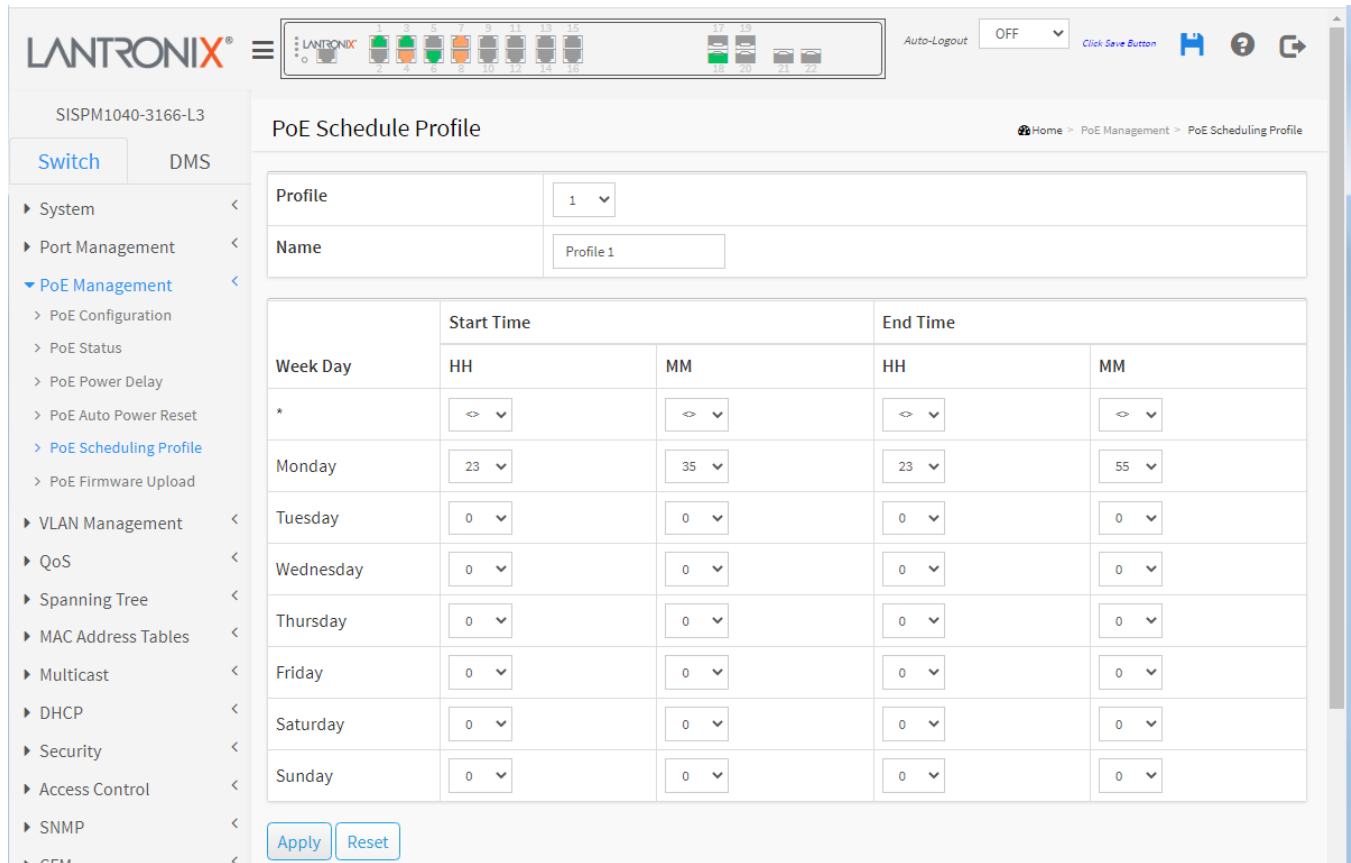
**Buttons**

**Apply:** Click to save changes.

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

**PoE Management > PoE Schedule Profile**

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



**Profile:** The index of profile. There are 16 profiles in the configuration.

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

**Week Day:** The day to schedule PoE.

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

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

**Buttons**

**Apply:** Click to save changes.

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

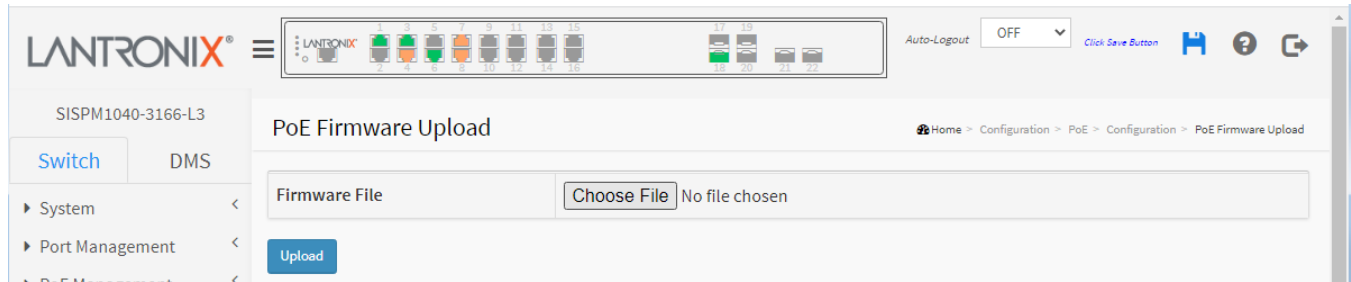
## PoE Management > PoE Firmware Upload

Navigate to the Configuration > PoE Configuration > PoE Firmware Upload menu path to display the PoE Firmware Upload page.

This page lets you browse to and select a firmware file to update the PoE firmware controlling the switch.

After the PoE firmware is uploaded, a page announces that the firmware update is initiated. After about a minute, the PoE firmware is updated and the switch restarts.

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



Click the Choose File button to browse to and select the desired PoE firmware file.

Click the Upload button to begin the upload.

The initial release was PoE Firmware Version 200-211.

## VLAN Management

A Virtual LAN (VLAN) is a method to restrict communication between switch ports. At layer 2, the network is partitioned into multiple, distinct, mutually-isolated broadcast domains.

### VLAN Management > VLAN Configuration

This page lets you set VLAN parameters on the switch. The page is divided into a global section and a per-port configuration section.

To assign a specific VLAN for management purposes, the management VLAN is used to establish an IP connection to the switch from a workstation connected to a port in the VLAN. This connection supports an SNMP or 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 at System > IP Address > Advanced Settings. Only one management VLAN can be active at a time.

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

The screenshot displays the 'VLAN Configuration' page for a Lantronix switch (SISPM1040-3166-L3). The interface includes a navigation menu on the left with 'VLAN Management' selected. The main content area is split into two sections:

- Global VLAN Configuration:**
  - Allowed Access VLANs:** A text input field containing '1-10,20,30,100-200' with a hint '(e.g. 1,2,10-13,15)'.
  - Ethertype for Custom S-ports:** A text input field containing '88A6'.
- 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			<input type="checkbox"/>				
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	
9	Access	1	C-Port	<input checked="" type="checkbox"/>	Tagged and Untagged	Untag Port VLAN	1	

### 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 the 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.

EtherType is a two-octet field in an Ethernet frame used to indicate which protocol is encapsulated in the payload of the frame and is used at the receiving end by the data link layer to determine how the payload is processed. The same field is also used to indicate the size of some Ethernet frames. See the [IANA](#) webpage.

The TPID (Tag Protocol Identifier) is a 16-bit field set to 0x8100 to identify the frame as an IEEE 802.1Q-tagged frame. This field is located at the same position as the EtherType field in untagged frames and is thus used to distinguish the frame from untagged frames. See the [IANA](#) webpage.

### **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. When a particular mode is selected, the remaining fields in that row will be either grayed out or made changeable depending on the mode in question. Grayed out fields show the value that the port will get when the mode is applied.

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

- Member of exactly one VLAN, the Port VLAN (a.k.a. Access VLAN), which by default is 1
- Accepts untagged and C-tagged frames.
- Discards all frames not classified to the Access VLAN.
- On egress all frames are transmitted untagged.

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

- By default, a trunk port is member of all VLANs (1-4095).
- The VLANs that a trunk port is member of may be limited by the use of Allowed VLANs.
- Frames classified to a VLAN that the port is not a member of are 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.

**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 the default is 1.

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

On egress, frames classified to the Port VLAN do not get tagged if Egress Tagging configuration is set to untag Port VLAN.

The Port VLAN is called an "Access VLAN" for ports in Access mode and "Native VLAN" for ports in Trunk or Hybrid mode.

**Port Type:** Ports in hybrid mode allow for changing the port type, that is, whether a frame's VLAN tag is used to classify the frame on ingress to a particular VLAN, and if so, which TPID it reacts on. Likewise, on egress, the Port Type determines the TPID of the tag, if a tag is required.

**Unaware:** On ingress, all frames, whether carrying a VLAN tag or not, get classified to the Port VLAN, and possible tags are not removed on egress.

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

**S-Port:** On egress, if frames must be tagged, they will be tagged with an S-tag. On ingress, frames with a VLAN tag with TPID = 0x88A8 or equal to the Ethertype configured for Custom-S ports get classified to the VLAN ID embedded in the tag. Priority-tagged frames are classified to the Port VLAN. If the port is configured to accept Tagged Only frames (see Ingress Acceptance below), frames without this TPID are dropped. 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.

**S-Custom-Port:** On egress, if frames must be tagged, they will be tagged with the Custom S-tag. On ingress, frames with a VLAN tag with a TPID equal to the [Ethertype configured for Custom-S ports](#) get classified to the VLAN ID embedded in the tag. Priority-tagged frames are classified to the Port VLAN. If the port is configured to accept Tagged Only frames (see Ingress Acceptance below), frames without this TPID are dropped. 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. See Port Type for a description of when a frame is considered tagged.

**Tagged Only:** Only frames tagged with the corresponding Port Type tag are accepted on ingress.

**Untagged Only:** Only untagged frames are accepted on ingress. See Port Type for a description of when a frame is considered untagged.

**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 Enabled VLANs field. By default, a Trunk or Hybrid port will become member of all VLANs and is therefore set to 1-4095. The field may be left empty, which means that the port will not become member of any VLANs.

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

## Buttons

**Apply:** Click to save changes.

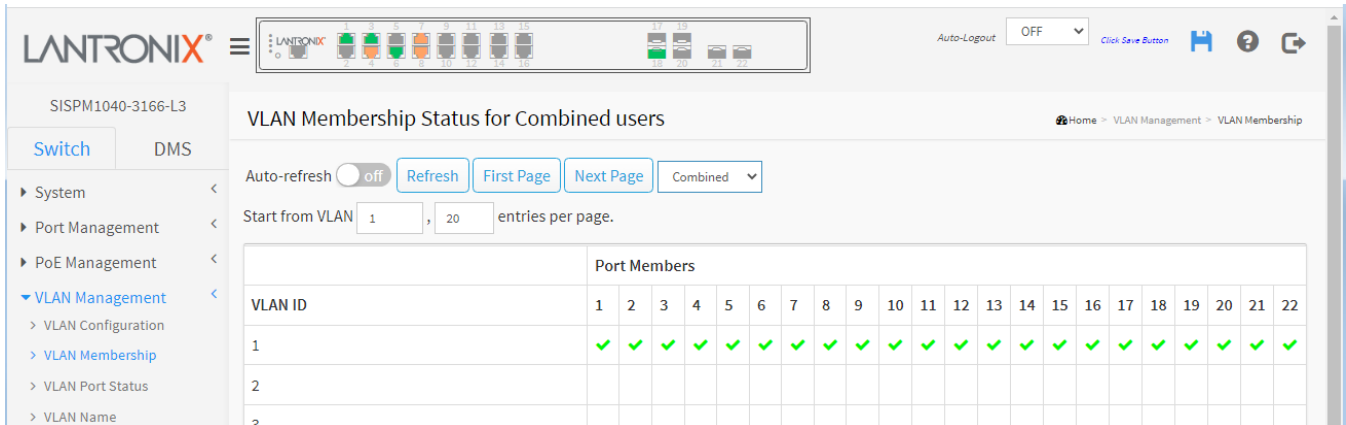
**Reset:** Click to undo any changes made locally and revert to previously saved values.

## VLAN Management > VLAN Membership

This page provides an overview of membership status of VLAN users.

Each page shows up to 99 entries from the VLAN table (the 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 "Start from VLAN" input field lets you select the starting point in the VLAN Table. Clicking the Refresh button will update the displayed table starting from that or the closest next VLAN Table match. The Next Page button 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 data exists for the selected user" is shown in the table. Use the Last Page button to start over.



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

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

**Admin:** Shows Administrative users only.

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

**MVRP:** Multiple VLAN Registration Protocol.

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

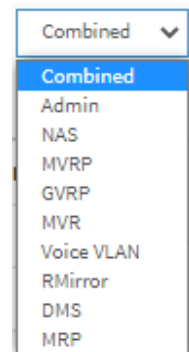
**MVR:** MVR is used to eliminate the need to duplicate multicast traffic for subscribers in each VLAN. Multicast traffic for all channels is sent only on a single (multicast) VLAN.

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

**RMirror:** Shows Remote Mirroring users only.


**DMS:** Shows DMS VLAN membership status.


**MRP:** Multiple Registration Protocol is a generic registration framework that defines the dynamic registration and de-registration of attributes across a Bridged Local Area Network.




**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, the following image will be displayed: .

If a port is in the forbidden port list, the following image will be displayed: .

If a port is in the forbidden port list and at the same time attempted to be included in the VLAN, the following image will be displayed: . The port will not be a member of the VLAN in this case.


### Buttons

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

**Refresh:** Click to refresh the page immediately.

**First Page:** Use the button to start over.

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

 : Select a VLAN Users from this drop down list. The selections are Combined (default), Admin, NAS, MVRP, GVRP, MVR, Voice VLAN, RMirror, DMS, and MRP.

## VLAN Management > VLAN Port Status

This page displays VLAN Port Status for a selected set of VLAN 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	✓	All	1	Untag All		No
2	C-Port	✓	All	1	Untag All		No
3	C-Port	✓	All	1	Untag All		No
4	C-Port	✓	All	1	Untag All		No
5	C-Port	✓	All	1	Untag All		No
6	C-Port	✓	All	1	Untag All		No
7	C-Port	✓	All	1	Untag All		No
8	C-Port	✓	All	1	Untag All		No

**VLAN User:** Various internal software modules may use VLAN services to configure VLAN port configuration on the fly. The drop-down list 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. See descriptions in the previous section.

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.

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

**Port Type:** Shows the port type (Unaware, C-Port, S-Port, S-Custom-Port) that a given user wants to configure on the port. The field is empty if not overridden by the selected user. If Port Type is Unaware, all frames are classified to the Port VLAN ID and tags are not removed.

**Ingress Filtering:** Displays whether a given user wants ingress filtering enabled or not. The field is empty if not overridden by the selected user. 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:** Displays the acceptable frame types (All, Tagged, Untagged) that a given user wants to configure on the port. The field is empty if not overridden by the selected user. Shows whether the port accepts all frames or only tagged frames. This parameter affects VLAN ingress processing. If the port only accepts tagged frames, untagged frames received on that port are discarded.

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

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

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

**Conflicts:** Two users may have conflicting requirements to a port's configuration. For instance, one user may require all frames to be tagged on egress while another requires all frames to be untagged on egress.

Since both users cannot win, this gives rise to a conflict, which is solved in a prioritized way. The Administrator has the least priority. Other software modules are prioritized according to their position in the drop-down list; the higher in the list, the higher its 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.

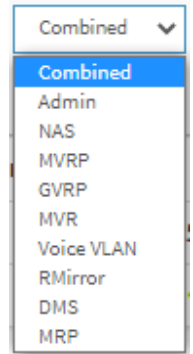
**Buttons**



: Select a VLAN User from this drop down list. The selections are Combined (default), Admin, NAS, MVRP, GVRP, MVR, Voice VLAN, RMirror, DMS, and MRP.

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

**Refresh:** Click to refresh the page immediately.



## VLAN Management > VLAN Name

Entries in the VLAN Name Configuration table are shown on this page. The VLAN Name Configuration table contains up to 4095 entries, and is sorted first by VLAN ID.

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

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

The Next Page button will use the last entry of the currently displayed table as a basis for the next lookup. When the end is reached the text "No more entries" is shown in the displayed table. Use the First Page button to start over.

SISPM1040-3166-L3

Auto-Logout OFF

Click Save Button

Switch DMS

VLAN Name Configuration

Home > VLAN Management > VLAN Name

Refresh First Page Next Page

Start from VLAN  ,  entries per page.

VLAN ID	VLAN Name
1	default
2	<input type="text" value="VID2"/>
3	<input type="text" value="VID3"/>
4	<input type="text"/>
5	<input type="text"/>
6	<input type="text"/>

**VLAN ID:** The VLAN ID.

**VLAN Name:** Entry field for a name for the VLAN.

### Buttons

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

**First Page:** Updates the table, starting with the entry after the last entry currently displayed.

**Next Page:** Updates the table starting from the first entry in the table.

**Apply:** Click to save changes.

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

## MAC-based VLAN

The MAC-based VLAN feature allows incoming untagged packets to be assigned to a VLAN and thus classify traffic based on the packet's source MAC address.

### MAC-based VLAN Configuration

The MAC address to VLAN ID mappings can be configured here. This page allows adding and deleting MAC-based VLAN Classification List entries and assigning the entries to different ports. The maximum possible MAC to VLAN ID mapping entries is 256.

The screenshot shows the 'MAC-based VLAN Membership Configuration' page in the Lantronix web interface. The page title is 'SISPM1040-3166-L3'. The navigation menu on the left includes 'Switch' and 'DMS'. The main content area has an 'Auto-refresh' toggle set to 'off' and buttons for 'Refresh', 'First Page', and 'Next Page'. Below this is a table with columns for 'Delete', 'MAC Address', 'VLAN ID', and 'Port Members' (ports 1-22). A single entry is shown with MAC address '00-00-00-00-00-00' and VLAN ID '1'. Below the table are buttons for 'Add New Entry', 'Apply', and 'Reset'.

**Delete:** To delete a MAC to VLAN ID mapping entry, click this button. The entry will be deleted from the table and from the system..

**MAC Address:** Indicates the MAC address of the mapping.

**VLAN ID:** Indicates the VLAN ID the above MAC will be mapped to.

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

#### Buttons

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

**Refresh:** Refreshes the displayed table.

**First Page:** Updates the table, starting with the entry after the last entry currently displayed.

**Next Page:** Updates the table starting from the first entry in the Dynamic ARP Inspection Table.

**Add New Entry:** Click the button to add a new MAC to VLAN ID mapping entry. An empty row is added to the table, and the mapping can be configured as needed. Any unicast MAC address can be used to configure the mapping. 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 when you click on "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.

**Apply:** Click to save changes.

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

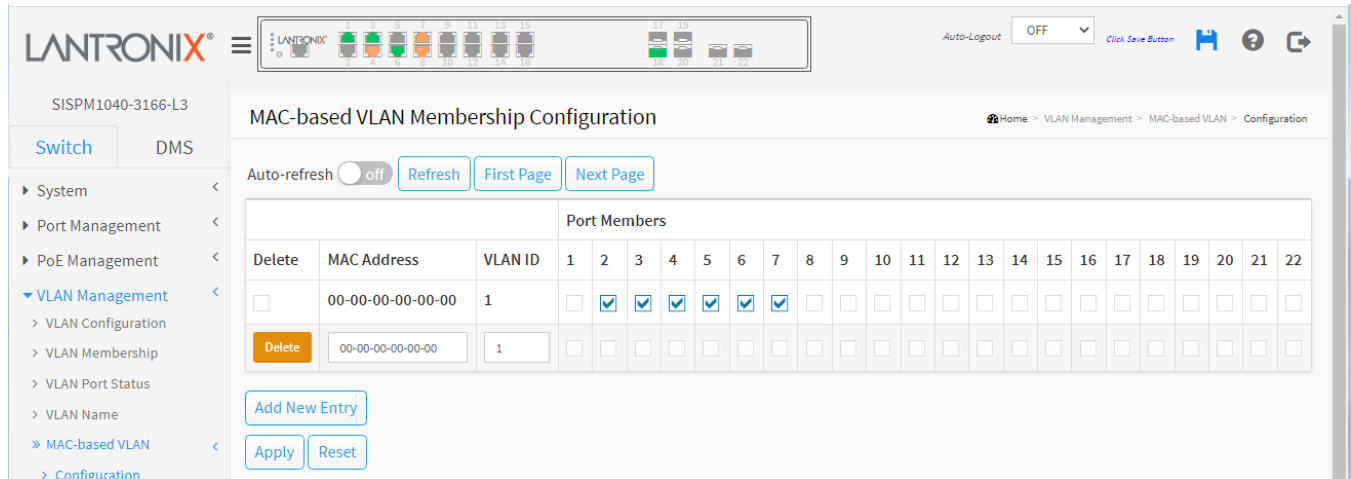


### MAC-based VLAN Status

This page shows MAC-based VLAN entries configured by various MAC-based VLAN users. The following VLAN User types are currently 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.



**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:** Refreshes the displayed table.

**User select box:** At the dropdown select the desired user (Static, NAS, DMS, or Combined).

#### Messages:

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

## VLAN Management > Protocol-based VLAN

The switch supports Ethernet, LLC, and SNAP protocols.

**LLC:** The Logical Link Control (LLC) data communication protocol layer is the upper sub-layer of the Data Link Layer (which is itself layer 2, just above the Physical Layer) in the seven-layer OSI reference model. It provides multiplexing mechanisms that make it possible for several network protocols (IP, IPX, 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.

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

This page lets you add new Protocol to Group Name mapping entries and to view and delete already mapped entries for the switch. Each protocol can be part of only one Group. The maximum possible Protocol to Group mappings is 128. Each protocol can be part of only one Group

The screenshot shows the 'Protocol-based VLAN Configuration' page in the Lantronix web interface. The page title is 'SISPM1040-3166-L3'. The navigation menu on the left includes 'System', 'Port Management', 'PoE Management', 'VLAN Management', and 'Protocol-based VLAN'. The main content area shows an 'Auto-refresh' toggle set to 'off' and a 'Refresh' button. Below this is the 'Protocol to Group Mapping Table' with the following data:

Delete	Frame Type	Value	Group Name
<input type="checkbox"/>	Ethernet	0800	Grp1
<input type="checkbox"/>	SNAP	00-E0-2B-0001	Grp2

Below the table, there is a 'Delete' button, a dropdown menu for 'Frame Type' (currently set to 'Ethernet'), and a text field for 'Etype: 0x' with the value '0800'. At the bottom of the table area are buttons for 'Add New Entry', 'Apply', and 'Reset'.

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

**Frame Type:** Frame Type can have one of the following values: Ethernet, SNAP, or LLC. **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:** Value in the text field when Ethernet is selected as a Frame Type is called etype. Valid values for etype range between 0x0600 and 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 is also comprised of two different sub-values.

a. **OUI:** OUI (Organizationally Unique Identifier) is a parameter in the format of xx-xx-xx where each pair (xx) in the string is a hexadecimal value ranging between 0x00 and 0xff.

**b. PID:** PID (Protocol ID). If OUI is hexadecimal 000000, then the protocol ID is the Ethernet type (EtherType) field value for the protocol running on top of SNAP; if 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 the value of OUI field is 00-00-00 then the value of PID will be etype (0x0600-0xffff) and if the value of OUI is other than 00-00-00 then valid values of PID will be any value between 0x0000 and 0xffff.

**Group Name:** A valid Group Name is a 16-character long string, unique for every entry, which consists of a combination of alphabets (a-z or A-Z) and integers(0-9). **Note:** Special characters and underscores (\_) are not allowed.

### Buttons

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

**Delete:** To delete an entry, check this box. The entry will be deleted during the next save.

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

**Refresh:** : Click to refresh the page immediately.

**Apply:** Click to save changes.

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

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

This page allows you to map a Group Name (already configured or to be configured in the future) to a VLAN for the switch. The maximum possible Group to VLAN mappings is 256.

The screenshot shows the 'Group Name to VLAN mapping Table' configuration page. The table has the following structure:

Delete	Group Name	VLAN ID	Port Members																				
			1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21
<input type="checkbox"/>	Grp1	10	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<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"/>	<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"/>

**Delete:** To delete a Group Name to VLAN mapping, check this box. The entry will be deleted from the switch during the next Save.

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

**VLAN ID:** Indicates the VLAN ID to which the Group Name will be mapped. Valid values are 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 the mapping, check the box. To remove or exclude the port from the mapping, make sure the box is unchecked. By default, no ports are members, and all boxes are unchecked.

### Buttons

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

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

**Refresh:** Click to refresh the page immediately.

**Apply:** Click to save changes.

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

## 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. The maximum possible IP subnet to VLAN ID mappings is 128.

The screenshot displays the 'MAC-based VLAN Membership Configuration' page in the Lantronix web interface. The interface includes a top navigation bar with the Lantronix logo, a status bar showing port indicators (1-22) and an 'Auto-Logout' dropdown set to 'OFF'. The main content area features a left-hand navigation menu with options like 'System', 'Port Management', 'PoE Management', and 'VLAN Management'. The 'VLAN Management' section is expanded to show 'MAC-based VLAN' configuration. The main configuration area has an 'Auto-refresh' toggle set to 'off', along with 'Refresh', 'First Page', and 'Next Page' buttons. A table titled 'Port Members' is present, with columns for 'Delete', 'MAC Address', 'VLAN ID', and 22 numbered ports. The table currently shows 'Currently no entries present'. Below the table are 'Add New Entry', 'Apply', and 'Reset' buttons.

**Delete:** To delete a mapping, click this button.

**IP Address:** Indicates the subnet's IP address (Any of the subnet's host addresses can be also provided here, the application will convert it automatically).

**Mask Length:** Indicates the subnet's mask length.

**VLAN ID:** Indicates the VLAN ID the subnet will be mapped to. IP Subnet to VLAN ID is a unique matching.

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

### Buttons

**Add New Entry:** Click to add a new IP subnet to VLAN ID mapping entry. An empty row is added to the table, and the mapping can be configured as needed. Any IP address/mask can be configured for the mapping. Valid values for the VLAN ID are 1 to 4095.

The IP subnet to VLAN ID mapping entry is enabled when you click on "Save". The Reset button can be used to undo the addition of new mappings.

**Apply:** Click to save changes.

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

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

**Refresh:** Refreshes the displayed table.

**Messages:** *No multicast or broadcast address allowed*

## VLAN Management > Stream

**Does not currently display in the Web UI.** A stream can be defined as all traffic that match a certain key which may contain either destination MAC, source MAC, destination IP address, or source IP address. The matching will not use all fields in the key.

### VLAN Management > Stream > Stream

This page lets you configure Stream instances.

Stream Configuration
Home > VLAN Management > Stream > Stream


Auto-refresh  off
Refresh

Stream #	OuterTag	InnerTag	Multicast	Broadcast	Protocol	
						<a href="#">+</a>

**Stream #:** The ID of Stream. The valid range is 1 - 10.

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

: Edit the Stream row.

: Delete the Stream.

: Add a new Stream.

#### Buttons

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

**Refresh:** Click to refresh the page immediately.

## VLAN Management > Stream > MAC Matching

**Does not currently display in the Web UI.** A stream can be defined as all traffic that match a certain key which may contain either destination MAC, source MAC, destination IP address, or source IP address. The matching will not use all fields in the key.

This page allows you to configure MAC/IP matching for each port. Each port can be configured to use either (source MAC/source IP address) or (destination MAC/destination IP address).

### VCL MAC matching Configuration

[Home](#) > [VLAN Management](#) > [Stream](#) > [MAC Matching](#)

Auto-refresh  off Refresh

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

Apply
Reset

**Port:** Port number of the switch.

**VCL MAC Matching:** Specify the MAC matching to be used. Possible values are:

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

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

### Buttons

**Apply:** Click to save changes.

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

## VLAN Management > MRP

This section lets you set and view Media Redundancy Protocol setting.

### VLAN Management > MRP > Ports

This page lets you set MRP generic settings for all switch ports.

The screenshot shows the 'MRP Overall Port Configuration' page in the Lantronix web interface. The page title is 'MRP Overall Port Configuration' and the breadcrumb is 'Home > VLAN Management > MRP > Ports'. The interface includes a navigation menu on the left with 'VLAN Management > MRP > Ports' selected. At the top right, there is an 'Auto-Logout' dropdown set to 'OFF' and a 'Click Save Button' link. Below the title, there is an 'Auto-refresh' toggle set to 'off' and a 'Refresh' button. The main content is a table with the following data:

Port	Join Timeout	Leave Timeout	LeaveAll Timeout	Periodic Transmission
*	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
1	<input type="text" value="20"/>	<input type="text" value="60"/>	<input type="text" value="1000"/>	<input type="checkbox"/>
2	<input type="text" value="20"/>	<input type="text" value="60"/>	<input type="text" value="1000"/>	<input type="checkbox"/>
3	<input type="text" value="20"/>	<input type="text" value="60"/>	<input type="text" value="1000"/>	<input type="checkbox"/>
4	<input type="text" value="20"/>	<input type="text" value="60"/>	<input type="text" value="1000"/>	<input type="checkbox"/>
5	<input type="text" value="20"/>	<input type="text" value="60"/>	<input type="text" value="1000"/>	<input type="checkbox"/>
6	<input type="text" value="20"/>	<input type="text" value="60"/>	<input type="text" value="1000"/>	<input type="checkbox"/>
7	<input type="text" value="20"/>	<input type="text" value="60"/>	<input type="text" value="1000"/>	<input type="checkbox"/>

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

**Join Timeout:** Controls the timeout of the Join Timer for all MRP Applications on this switch port. This value is restricted to 1-20 centiseconds.

**Leave Timeout:** Controls the timeout of the Leave Timer for all MRP Applications on this switch port. This value is restricted to 60- 300 centiseconds.

**LeaveAll Timeout:** Controls the timeout of the LeaveAll Timer for all MRP Applications on this switch port. This value is restricted to 1000- 5000 centiseconds.

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

#### Buttons

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

**Refresh:** Click to refresh the page.

**Apply:** Click to save changes.

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



## VLAN Management > MRP > MVRP

This page allows you to configure the MVRP global and per port settings altogether. The page is divided into a global section and a per-port configuration section.

The Multiple VLAN Registration Protocol defines the dynamic registration and de-registration of VLAN identifiers across a Bridged Local Area Network. It uses the MRP framework to define its operation and therefore it is also called an MRP application. The latest standard is in IEEE 802.1Q-2014.

The screenshot displays the Lantronix web interface for configuring MVRP. The top navigation bar includes the Lantronix logo, a menu icon, and a status bar with 'Auto-Logout OFF' and a 'Click Save Button' link. The main content area is titled 'MVRP Global Configuration' and includes an 'Auto-refresh' toggle set to 'off' with a 'Refresh' button. Below this, the 'Global State' is set to 'Enabled' and 'Managed VLANs' is set to '1-40'. The 'MVRP Port Configuration' section contains a table with columns for 'Port' and 'Enabled'.

Port	Enabled
*	<input type="checkbox"/>
1	<input checked="" type="checkbox"/>
2	<input checked="" type="checkbox"/>
3	<input type="checkbox"/>
4	<input checked="" type="checkbox"/>
5	<input checked="" type="checkbox"/>
6	<input checked="" type="checkbox"/>
7	<input checked="" type="checkbox"/>

### MVRP Global Configuration

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

**Managed VLANs:** This field shows the managed VLANs, i.e. the VLANs that MVRP will operate on. By default, only VLANs 1- 4094 are managed (i.e., the entire range as defined in IEEE802.1Q-2014 for MVRP). However this range can be limited by using a list syntax where the individual elements are separated by commas. Ranges are specified with a dash separating the lower and upper bound. The following example will create VLANs 1, 10, 11, 12, 13, 200, and 300: `1,10-13,200,300`. Spaces are allowed between the delimiters.

### MVRP Port Configuration

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

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

#### Buttons

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

**Refresh:** Click to refresh the page.

**Apply:** Click to save changes.

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

## VLAN Management > MRP > MVRP Statistics

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

The screenshot displays the MVRP Statistics page for a Lantronix switch. The page title is 'MVRP Statistics' and the breadcrumb trail is 'Home > VLAN Management > MVRP Statistics'. The interface includes a navigation sidebar on the left with categories like System, Port Management, PoE Management, and VLAN Management. The main content area features a table with the following data:

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

Additional controls include an 'Auto-refresh' toggle set to 'off' and a 'Refresh' button.

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

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

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

### Buttons

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

**Refresh:** Click to refresh the page immediately.

## VLAN Management > 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.

### VLAN Management > GVRP > Config

This page lets you configure GVRP global and port settings.

The screenshot displays the Lantronix web interface for configuring GVRP. The top navigation bar includes the Lantronix logo, a menu icon, and a status bar with 'Auto-Logout OFF' and a 'Click Save Button' link. The main content area is titled 'GVRP Configuration' and shows a breadcrumb trail: Home > VLAN Management > GVRP > Global Config. On the left, a sidebar menu lists various configuration options, with 'VLAN Management' expanded to show 'GVRP' and 'Global Config' selected. The main configuration area is divided into two sections: 'GVRP Configuration' and 'GVRP Port Configuration'.

**GVRP Configuration:**

- Enable GVRP:** A toggle switch is set to **on**.
- Parameter Value Table:**

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

**GVRP Port Configuration:**

Port	Mode
*	↔
1	Disabled
2	Disabled
3	Disabled
4	Disabled
5	Disabled
6	Disabled

**Enable GVRP:** The GVRP feature is globally enabled by setting the slider to **on**. The default is **off**.

#### **GVRP protocol timers:**

**Join-time** is a value in the range of 1-20cs (i.e., in units of one hundredth of a second). The default value is 20cs.

**Leave-time** is a value in the range of 60-300cs, i.e., in units of one hundredth of a second. The default is 60cs.

**LeaveAll-time** is a value in the range of 1000-5000cs, i.e. in units of one hundredth of a second. The default is 1000cs.

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

**GVRP Port Configuration:** This section 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.

**Port:** The logical port that is to be configured.

**Mode:** Mode can be either 'Disabled' or 'GVRP enabled'. These values turn the GVRP feature off or on respectively for the port in question.

## Buttons

**Apply:** Click to save changes.

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

## VLAN Management > Private VLAN

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.

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.

The screenshot displays the 'Private VLAN Membership Configuration' page. The interface includes a navigation menu on the left with options like System, Port Management, PoE Management, and VLAN Management. The main content area shows a table for configuring Private VLANs. The table has columns for 'Delete', 'PVLAN ID', and 'Port Members' (ports 1 through 22). Three rows are visible: PVLAN 1 (all ports checked), PVLAN 2 (ports 2 and 3 checked), and PVLAN 22 (ports 6, 7, 8, 9, 10, 13 checked). A 'Delete' button is next to the PVLAN 0 row. At the bottom are 'Add New Private VLAN', 'Apply', and 'Reset' buttons.

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

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

**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 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".

**Apply:** Click to save changes.

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

## VLAN Management > 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.

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

The screenshot shows the 'Port Isolation Configuration' page in the Lantronix web interface. The page title is 'Port Isolation Configuration' and the breadcrumb is 'Home > VLAN Management > Port Isolation'. The device ID is 'SISPM1040-3166-L3'. The left navigation menu includes 'System', 'Port Management', 'PoE Management', 'VLAN Management' (selected), 'VLAN Configuration', 'VLAN Membership', 'VLAN Port Status', and 'VLAN Name'. The main content area has an 'Auto-refresh' toggle set to 'off' and a 'Refresh' button. Below this is a 'Port Members' table with 22 columns representing ports 1 through 22, each with a checkbox. At the bottom of the table are 'Apply' and 'Reset' buttons.

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22
<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"/>	<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"/>

**Port Members:** A check box is provided for each port of a private VLAN.

When checked, port isolation is enabled on that port.

When unchecked, port isolation is disabled on that port. By default, port isolation is disabled on all ports.

### Buttons

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

**Refresh:** Click to refresh the page immediately.

**Apply:** Click to save changes.

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

## VLAN Management > Voice VLAN

Voice VLAN is VLAN configured specially for voice traffic. By adding 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.

### VLAN Management > Voice VLAN > Configuration

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

The screenshot displays the Lantronix web interface for configuring Voice VLAN. The top navigation bar includes the Lantronix logo, a menu icon, and a status bar with 'Auto-Logout OFF' and a 'Click Save Button' link. The main content area is titled 'Voice VLAN Configuration' and shows the following settings:

- Mode:** on (toggle)
- VLAN ID:** 1000
- Aging Time:** 86400 seconds
- Traffic:** 7 (High)

Below the configuration settings is a 'Port Configuration' table with the following columns: Port, Mode, Security, and Discovery Protocol.

Port	Mode	Security	Discovery Protocol
*	⊖	⊖	⊖
1	Disabled	Enabled	OUI
2	Auto	Enabled	LLDP
3	Forced	Enabled	Both
4	Auto	Enabled	Both
5	Forced	Enabled	LLDP
6	Auto	Disabled	OUI
7	Auto	Enabled	OUI
8	Disabled	Disabled	OUI

### Voice VLAN Configuration

**Mode:** Indicates the Voice VLAN mode operation. **Note:** You must disable the MSTP feature before you enable Voice VLAN (at Spanning Tree > MSTI Configuration) to 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 (0=Lowest priority, 7=Highest priority). All traffic on the Voice VLAN will apply this class.

### **Port Configuration**

**Port:** The port that a row can configure.

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

**Disabled:** Disjoin from Voice VLAN.

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

**Forced:** Force join to Voice VLAN.

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

**Enabled:** Enable Voice VLAN security mode operation.

**Disabled:** Disable Voice VLAN security mode operation.

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

**OUI:** Detect telephony device by OUI address. An OUI (Organizationally Unique Identifier) address is a globally unique identifier assigned to a vendor by IEEE. You can determine which vendor a device belongs to according to the OUI address which forms the first 24 bits of a MAC address.

**LLDP:** Detect telephony device by Link Level Discovery Protocol.

**Both:** Both OUI and LLDP (default).

### **Buttons**

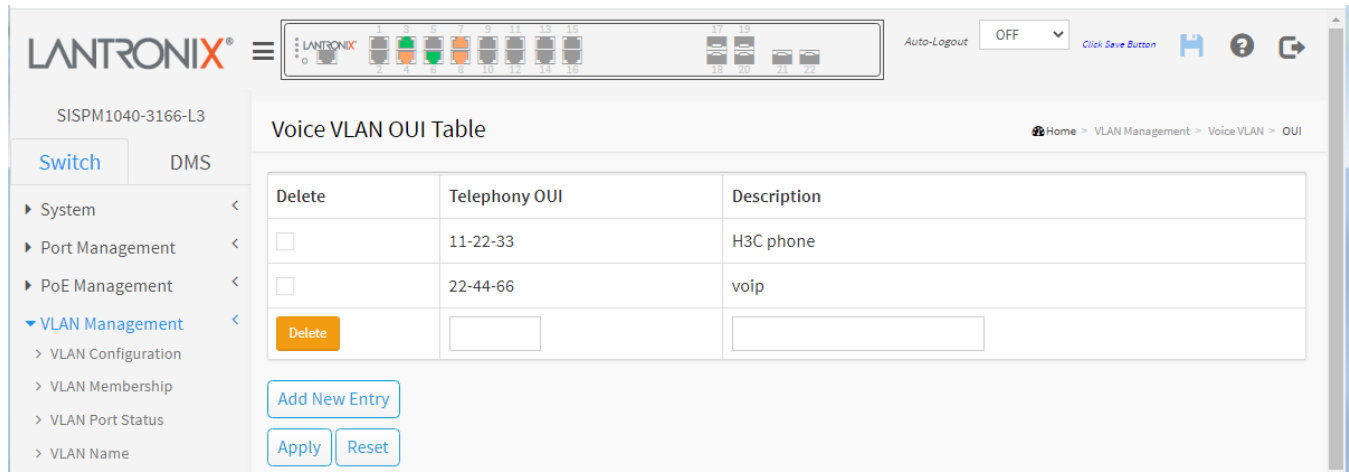
**Apply:** Click to save changes.

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



### VLAN Management > Voice VLAN > OUI

Configure Voice VLAN OUI on this page. The maximum number of entries is 16. Modifying the OUI table will restart auto detection of the OUI process.



**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 IEEE. It must be 6 characters long and the input format is "xx-xx-xx" (where x is a hexadecimal digit).

**Description:** The description of OUI address. Normally, it describes which vendor telephony device it belongs to. The allowed string length is 0 - 32 characters.

#### Buttons

**Add New Entry:** Click to add a new access management entry to the table.

**Apply:** Click to save changes.

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

## QoS

QoS (Quality of Service) is a method to guarantee a bandwidth relationship between individual applications or protocols. A communications network transports a multitude of applications and data, including high-quality video and delay-sensitive data such as real-time voice. Networks must provide secure, predictable, measurable, and sometimes guaranteed services. Achieving the required QoS becomes the secret to a successful end-to-end business solution.

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.

High flexibility is provided in 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 frame. It uses 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.

- ▼ QoS
  - > Port Classification
  - > Port Policers
  - > Queue Policers
  - > Port Shapers
  - > Storm Control
  - > Port Schedulers
  - > Port PCP Remarking
  - » DSCP
  - > Ingress Map
  - > Egress Map
  - » QoS Control List
  - > QoS Statistics
  - > WRED

### QoS > Port Classification

This page lets you configure basic QoS Classification settings for all switch ports.

The screenshot shows the 'QoS Port Classification' configuration page. The interface includes a top navigation bar with the LANTRONIX logo, a status bar with 'Auto-Logout OFF', and a breadcrumb trail 'Home > QoS > Port Classification'. On the left, there is a navigation menu with 'Switch' selected and 'DMS' as an option. The main content area contains a table for configuring QoS settings for 8 ports.

Port	Ingress									Egress	
	CoS	DPL	PCP	DEI	CoS ID	Tag Class.	DSCP Based	WRED Group	Map	Map	
*	0	0	0	0	0		<input type="checkbox"/>	1			
1	0	0	0	0	0	Disabled	<input type="checkbox"/>	1			
2	2	0	3	1	0	Disabled	<input type="checkbox"/>	2	0	50	
3	4	1	6	0	0	Disabled	<input type="checkbox"/>	3	50	125	
4	5	3	7	1	0	Disabled	<input type="checkbox"/>	1	100	300	
5	0	0	0	0	0	Disabled	<input type="checkbox"/>	1			
6	0	0	0	0	0	Disabled	<input type="checkbox"/>	1			
7	0	0	0	0	0	Disabled	<input type="checkbox"/>	1			
8	0	0	0	0	0	Disabled	<input type="checkbox"/>	1			

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

**CoS:** Controls the default CoS value. All frames are classified to a CoS. There is a one to one mapping between CoS, queue and priority. A CoS of 0 (zero) has the lowest priority. If the port is VLAN aware, the frame is tagged and Tag Class. is enabled, then the frame is classified to a CoS that is mapped from the PCP and DEI value in

the tag. Otherwise the frame is classified to the default CoS. The classified CoS can be overruled by a QCL entry. **Note:** If the default CoS has been dynamically changed, then the actual default CoS is shown in parentheses after the configured default CoS.

**DPL:** Controls the default DPL value. 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.

**CoS ID:** Controls the default CoS ID value. Every incoming frame is classified to a CoS ID, which later can be used as basis for rewriting of different parts of the frame.

**Tag Class:** Shows the classification mode for tagged frames on this port. Click the linked text to configure the mode and/or mapping (see below).

**Disabled:** Use default CoS and DPL for tagged frames.

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

**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.

**WRED Group:** Controls the WRED group membership (group 1, 2, or 3). Weighted Random Early Detection is an active queue management mechanism that provides preferential treatment of higher priority frames when traffic builds up within a queue. A frame's DPL is used as input to WRED. A higher DPL assigned to a frame results in a higher probability that the frame is dropped during times of congestion.

**Ingress Map:** Controls the Ingress Map selection through the Map ID. A valid Ingress Map ID can be 0-255. An empty field indicates no map selection.

**Egress Map:** Controls the Egress Map selection through the Map ID. A valid Egress Map ID can be 0-511. An empty field indicates no map selection.

## Buttons

**Apply:** Click to save changes.

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

## Ingress Port Tag Classification

Click on the linked text in the Tag Class. column to configure the mode and/or mapping. The classification mode for tagged frames are configured on this page.

The screenshot shows the 'Ingress Port Tag Classification' configuration page for 'Port 3'. The 'Tag Classification' is set to 'Enabled'. Below this is a table for '(PCP, DEI) to (CoS, DPL) Mapping'.

PCP	DEI	CoS	DPL
*	*	<input type="button" value="⊞"/>	<input type="button" value="⊞"/>
0	0	<input type="button" value="1"/>	<input type="button" value="2"/>
0	1	<input type="button" value="1"/>	<input type="button" value="1"/>
1	0	<input type="button" value="2"/>	<input type="button" value="2"/>
1	1	<input type="button" value="3"/>	<input type="button" value="1"/>
2	0	<input type="button" value="4"/>	<input type="button" value="3"/>
2	1	<input type="button" value="2"/>	<input type="button" value="3"/>
3	0	<input type="button" value="3"/>	<input type="button" value="0"/>
3	1	<input type="button" value="3"/>	<input type="button" value="1"/>
4	0	<input type="button" value="4"/>	<input type="button" value="0"/>

**Tag Classification:** Controls the classification mode for tagged frames on this port.

**Disabled:** Use default CoS and DPL for tagged frames.

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

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

### Buttons

**Apply:** Click to save changes.

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

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

## QoS > Port Policers

This page lets you configure the Policer settings for all switch ports. A policer can limit the bandwidth of received frames. It is located in front of the ingress queue.

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

The screenshot shows the 'Port Policers' configuration page in the Lantronix web interface. The page title is 'Port Policers' and the breadcrumb is 'Home > QoS > Port Policers'. The interface includes a navigation menu on the left with 'QoS' expanded to show 'Port Policers' selected. The main content area contains a table with the following data:

Port	Enable	Rate	Unit	Flow Control
*	<input type="checkbox"/>		<input type="text" value=""/>	<input type="checkbox"/>
1	<input type="checkbox"/>	500	kbps	<input type="checkbox"/>
2	<input checked="" type="checkbox"/>	500	kbps	<input checked="" type="checkbox"/>
3	<input checked="" type="checkbox"/>	500	kbps	<input type="checkbox"/>
4	<input checked="" type="checkbox"/>	500	Mbps	<input checked="" type="checkbox"/>
5	<input checked="" type="checkbox"/>	500	Mbps	<input checked="" type="checkbox"/>
6	<input type="checkbox"/>	500	kbps	<input checked="" type="checkbox"/>
7	<input checked="" type="checkbox"/>	500	kbps	<input type="checkbox"/>
8	<input checked="" type="checkbox"/>	500	kbps	<input type="checkbox"/>
9	<input type="checkbox"/>	500	kbps	<input type="checkbox"/>

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

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

**Rate:** Controls the rate for the port policer. This value can be 10-13128147 when "Unit" is kbps or fps, and 1-13128 when "Unit" is Mbps or kfps. The rate is internally rounded up to the nearest value supported by the port policer.

**Unit:** Controls the unit of measure for the port policer rate as kbps, Mbps, fps or kfps.

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

### Buttons

**Apply:** Click to save changes.

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

## QoS > Queue Policers

This page allows you to configure the Queue Policer settings for all switch ports.

Port	E	Queue 0			Queue 1			Queue 2			Queue 3	Queue 4	Queue 5	Queue 6	Queue 7
		Rate	Unit	E	Rate	Unit	E	Rate	Unit	Enable	Enable	Enable	Enable	Enable	
*	<input type="checkbox"/>			<input type="checkbox"/>			<input type="checkbox"/>			<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
1	<input type="checkbox"/>	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"/>	550	kbps	<input type="checkbox"/>	600	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 type="checkbox"/>	500	kbps	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
4	<input checked="" type="checkbox"/>	450	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"/>	
5	<input checked="" type="checkbox"/>	500	kbps	<input type="checkbox"/>	600	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"/>	

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

**E:** Check the box to enable or uncheck to disable the queue policer for this switch port.

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

**Unit:** Controls the unit of measure for the queue policer rate as kbps or Mbps. This field is only shown if one or more of the queue policers are enabled.

### Buttons

**Apply:** Click to save changes.

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

## QoS > Port Shapers

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

The screenshot shows the 'QoS Egress Port Shapers' configuration page. The interface includes a top navigation bar with the Lantronix logo, a hamburger menu, and a status bar showing 'Auto-Logout OFF'. A left-hand navigation menu lists various system management options, with 'QoS' and 'Port Shapers' highlighted. The main content area features a table with the following structure:

Port	Shapers							Port	
	Q0	Q1	Q2	Q3	Q4	Q5	Q6		Q7
1	-	-	-	-	-	-	-	-	-
2	-	-	-	-	-	-	-	-	-
3	-	-	-	-	-	-	-	-	-
4	-	-	-	-	-	-	-	-	-
5	-	-	-	-	-	-	-	-	-
6	-	-	-	-	-	-	-	-	-
7	-	-	-	-	-	-	-	-	-
8	-	-	-	-	-	-	-	-	-

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

**Shapers – Qn:** Shows disabled or actual queue shaper rate (e.g., "800 Mbps").

**Shapers – Port:** Shows disabled or actual port shaper rate (e.g., "800 Mbps").

### Buttons

**Apply :** Click to save changes.

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

## QoS > Storm Control

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

There is a destination lookup failure storm rate control, multicast storm rate control, and a broadcast storm rate control. These only affect flooded frames (i.e., frames with a (VLAN ID, DMAC) pair not present on the MAC Address table. The configuration indicates the permitted packet rate for unicast, multicast or broadcast traffic across the switch.

**Global Storm Policer Configuration**

Frame Type	Enable	Rate	Unit
Unicast	<input type="checkbox"/>	10	fps
Multicast	<input type="checkbox"/>	10	fps
Broadcast	<input type="checkbox"/>	10	fps

**Port Storm Policer Configuration**

Port	Unicast Frames			Broadcast Frames			Unknown Frames		
	Enable	Rate	Unit	Enable	Rate	Unit	Enable	Rate	Unit
*	<input type="checkbox"/>		<>	<input type="checkbox"/>		<>	<input type="checkbox"/>		<>
1	<input type="checkbox"/>	500	kpbs	<input type="checkbox"/>	500	kpbs	<input type="checkbox"/>	500	kpbs
2	<input type="checkbox"/>	500	kpbs	<input type="checkbox"/>	500	kpbs	<input type="checkbox"/>	500	kpbs
3	<input type="checkbox"/>	500	kpbs	<input type="checkbox"/>	500	kpbs	<input type="checkbox"/>	500	kpbs
4	<input type="checkbox"/>	500	kpbs	<input type="checkbox"/>	500	kpbs	<input type="checkbox"/>	500	kpbs
5	<input type="checkbox"/>	500	kpbs	<input type="checkbox"/>	500	kpbs	<input type="checkbox"/>	500	kpbs
6	<input type="checkbox"/>	500	kpbs	<input type="checkbox"/>	500	kpbs	<input type="checkbox"/>	500	kpbs
7	<input type="checkbox"/>	500	kpbs	<input type="checkbox"/>	500	kpbs	<input type="checkbox"/>	500	kpbs
8	<input type="checkbox"/>	500	kpbs	<input type="checkbox"/>	500	kpbs	<input type="checkbox"/>	500	kpbs

### Global Storm Policer Configuration

**Frame Type:** The frame type for which the configuration below applies.

**Enable:** Check the box to enable or uncheck to disable the global storm policer for the given Frame Type.

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

**Unit:** Controls the unit of measure for the global storm policer rate as fps, kfps, kbps or Mbps.



**Port Storm Policer Configuration**: There is a storm policer for known and unknown Unicast Frames, known and unknown Broadcast Frames, and Unknown (flooded) unicast, multicast and broadcast Frames.

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

**Enable**: Enable or disable the storm policer for this switch port.

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

**Unit**: Controls the unit of measure for the port storm policer rate as fps, kfps, kbps or Mbps.

### Buttons

**Apply**: Click to save changes.

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

## QoS > Port Schedulers

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

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

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

**Mode:** Controls which queues are scheduled as Strict Priority and which are scheduled as Weighted on this switch port.

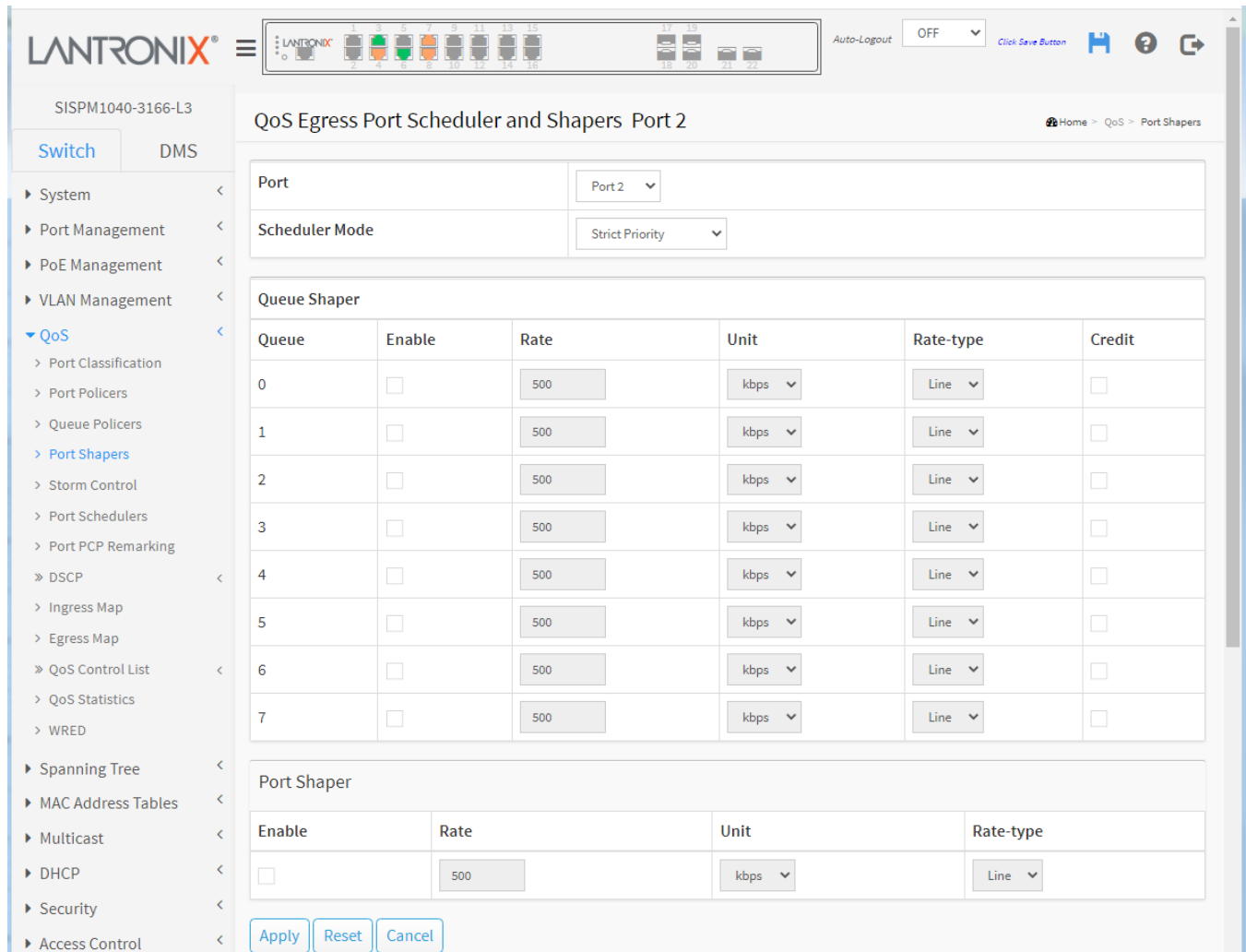
**Weight (Q0-Q7):** Set the weight for this queue in the range 1-100. This parameter is only active if Scheduler "Mode" is set to "Weighted".

### Buttons

**Apply:** Click to save changes.

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

You can click on a port number in order to configure the schedulers. This page lets you configure the Scheduler and Shapers for a specific port. The Port 2 page is shown below with Strict Priority Scheduler Mode selected:

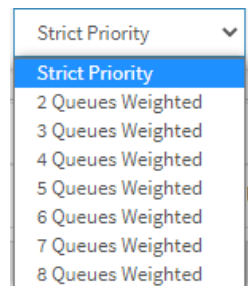


**Port:** The port number.

**Scheduler Mode:** Controls how many of the queues are scheduled as strict and how many are scheduled as weighted on this switch port. The possible selections are:

**Strict Priority:** Sets the Scheduler Mode to Strict priority (default setting).

**2-8 Queues Weighted:** Select 2 Queues Weighted – 8 Queues Weighted.



**Queue Shaper**

**Queue:** The queue number for the queue shaper.

**Enable:** Controls whether the queue shaper is enabled for this queue on this switch port.

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

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

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

**Line:** Specify that this shaper operates on line rate.

**Data:** Specify that this shaper operates on data rate.

**Credit:** Check the box if you want the queue to have credit-based shaper enabled.

The Port 2 page is shown below with 8 Queues Weighted Scheduler Mode selected:

The screenshot shows the 'QoS Egress Port Scheduler and Shapers Port 3' configuration page. The 'Port' is set to 'Port 3' and the 'Scheduler Mode' is '8 Queues Weighted'. Below this is a table for 'Queue Shaper' with 8 queues, each with a rate of 500 kbps, 'Line' rate-type, and 13% weight. A 'Port Shaper' section at the bottom is disabled with a rate of 500 kbps and 'Line' rate-type. Buttons for 'Apply', 'Reset', and 'Cancel' are at the bottom.

Queue Shaper						Queue Scheduler	
Queue	Enable	Rate	Unit	Rate-type	Credit	Weight	Percent
0	<input type="checkbox"/>	500	kbps	Line	<input type="checkbox"/>	17	13%
1	<input type="checkbox"/>	500	kbps	Line	<input type="checkbox"/>	17	13%
2	<input type="checkbox"/>	500	kbps	Line	<input type="checkbox"/>	17	13%
3	<input type="checkbox"/>	500	kbps	Line	<input type="checkbox"/>	17	13%
4	<input type="checkbox"/>	500	kbps	Line	<input type="checkbox"/>	17	13%
5	<input type="checkbox"/>	500	kbps	Line	<input type="checkbox"/>	17	13%
6	<input type="checkbox"/>	500	kbps	Line	<input type="checkbox"/>	17	13%
7	<input type="checkbox"/>	500	kbps	Line	<input type="checkbox"/>	17	13%

Port Shaper			
Enable	Rate	Unit	Rate-type
<input type="checkbox"/>	500	kbps	Line

**Queue Scheduler**

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

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

**Port Shaper**

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

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

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

**Rate-type:** The rate type of the port shaper. The allowed values are:

***Line:*** Specify that this shaper operates on line rate.

***Data:*** Specify that this shaper operates on data rate.

### **Buttons**

**Apply:** Click to save changes.

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

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

## QoS > Port PCP Remarking

This page displays QoS Egress Port PCP Remarking settings for all switch ports.

The screenshot shows the Lantronix web interface for the device SISPM1040-3166-L3. The page title is 'QoS Egress Port PCP Remarking'. The left navigation menu is expanded to 'QoS', with 'Port PCP Remarking' selected. The main content area displays a table with two columns: 'Port' and 'Mode'. The table lists ports 1 through 9, all of which are set to 'Classified' mode.

Port	Mode
<a href="#">1</a>	Classified
<a href="#">2</a>	Classified
<a href="#">3</a>	Classified
<a href="#">4</a>	Classified
<a href="#">5</a>	Classified
<a href="#">6</a>	Classified
<a href="#">7</a>	Classified
<a href="#">8</a>	Classified
<a href="#">9</a>	Classified

**Port:** The logical port for the settings contained in the same row. Click a linked port number to configure PCP remarking (see below).

**Mode:** Shows the PCP remarking mode for this port.

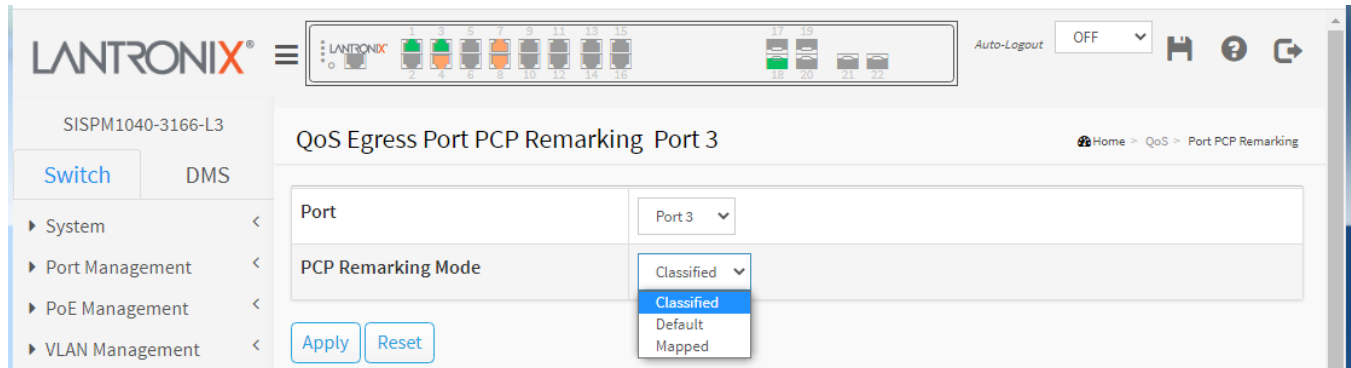
**Keep:** Use classified PCP/DEI values (default).

**Specific:** Use default PCP/DEI values.

**Mapped:** Use mapped versions of CoS and DPL.

## QoS Egress Port PCP Remarking

Click a linked port number to display the Egress Port PCP Remarking for the selected port. The Egress Port PCP Remarking for a specific port are configured on this page.



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

**PCP Remarking Mode:** Controls the PCP remarking mode for this port.

**Keep:** Use classified PCP/DEI values.

**Specific:** Use specific PCP/DEI values.

**Mapped:** Use mapped versions of CoS and DPL. DP Level 1 means 1 or higher.

**PCP/DEI Configuration** (displays only if “Specific” Mode is selected):

**Specific PCP:** At the dropdown select 0-7. The default is 0.

**Specific DEI:** At the dropdown select 0 or 1. The default is 0.

**(Queue Priority, DP level) to (PCP, DEI) Mapping** (displays only if “Mapped” Mode is selected):

**Queue Priority:** Displays two rows for each Queue Priority (0-7).

**DP level:** DP Level 1 means 1 or higher.

**PCP:** At the dropdown select 0-7.

**DEI:** At the dropdown select 0 or 1.

### Buttons

**Apply:** Click to save changes.

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

## DSCP

Differentiated Services Code Point is a field in the header of IP packets for packet classification purposes.

### Port DSCP

This page lets you configure basic QoS Port DSCP Configuration settings for all switch ports.

Port	Ingress		Egress
	Translate	Classify	Rewrite
*	<input type="checkbox"/>	<>	<>
1	<input type="checkbox"/>	Disable	Disable
2	<input type="checkbox"/>	Disable	Disable
3	<input type="checkbox"/>	Disable	Disable
4	<input type="checkbox"/>	Disable	Disable
5	<input type="checkbox"/>	Disable	Disable
6	<input type="checkbox"/>	Disable	Disable
7	<input type="checkbox"/>	Disable	Disable

**Port:** The Port column shows the list of ports for which you can configure DSCP ingress and egress settings.

**Ingress:** In Ingress settings you can change ingress translation and classification settings for individual ports. There are two configuration parameters available in Ingress: Translate and Classify:

**Translate:** To enable Ingress Translation check the checkbox.

**Classify:** Classification for a port can have one of four different values:

**Disable:** No Ingress DSCP Classification.

**DSCP=0:** Classify if incoming (or translated if enabled) DSCP is 0.

**Selected:** Classify only selected DSCP for which classification is enabled as specified in the DSCP Translation window for the specific DSCP.

**All:** Classify all DSCP.

**Egress Rewrite:** Port Egress Rewriting can be:

**Disable:** No Egress rewrite.

**Enable:** Rewrite enabled without remapping.

**Remap:** DSCP from analyzer is remapped and frame is remarked with remapped DSCP value.

### Buttons

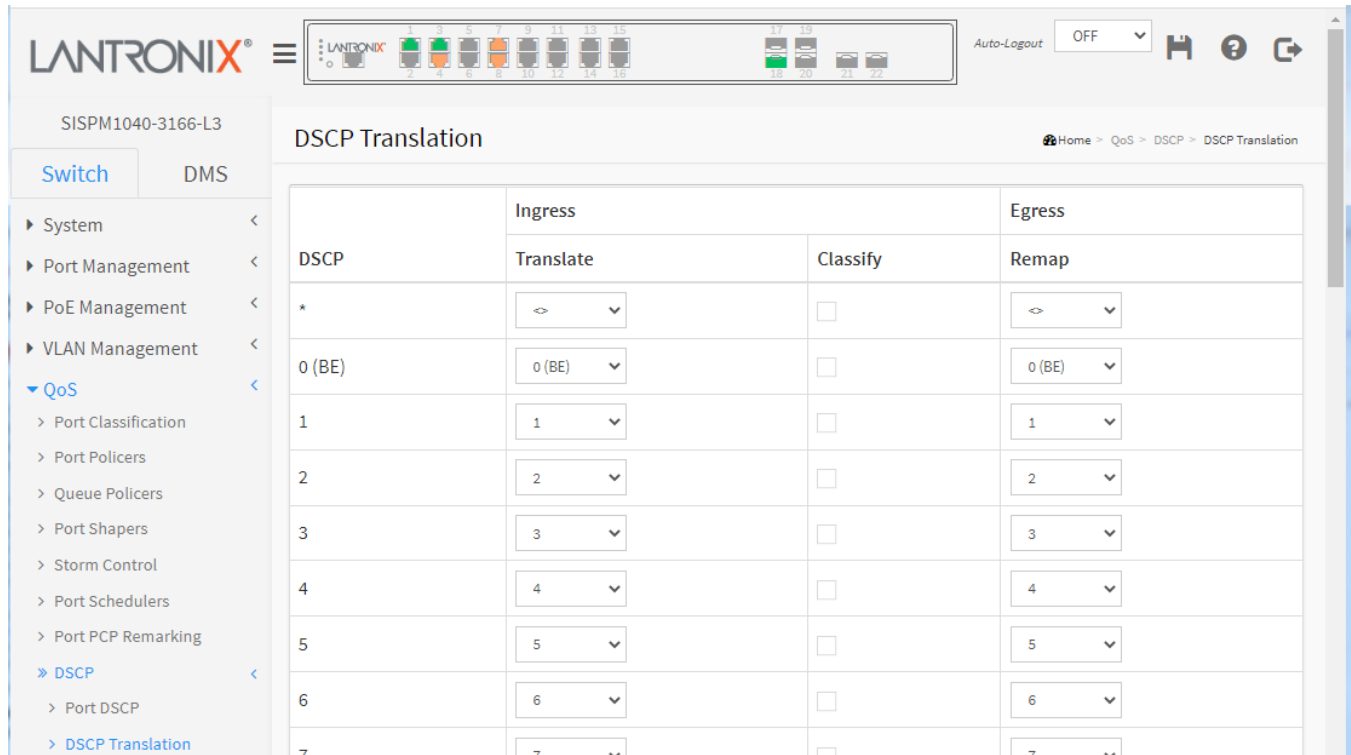
**Apply:** Click to save changes.

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



## DSCP Translation

This page allows you to configure the basic QoS DSCP Translation settings for all switches. DSCP translation can be done in Ingress or Egress.



**DSCP:** A maximum of 64 DSCP values are supported (in the range 0 - 63).

**Ingress:** Ingress side DSCP can be first translated to new DSCP before using the DSCP for CoS and DPL map. There are two configuration parameters for DSCP Translation:

**Translate:** DSCP at Ingress side can be translated to any of (0-63) DSCP values.

**Classify:** Click to enable Classification at Ingress side.

**Egress:** There is one configurable parameter for Egress side:

**Remap:** Select the DSCP value from select menu to which you want to remap. DSCP value ranges from 0 to 63.

### Buttons

**Apply:** Click to save changes.

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

## DSCP Classification

This page allows you to configure the mapping of Queue Priority and DPL to DSCP value.

CoS	DSCP DP0	DSCP DP1	DSCP DP2	DSCP DP3
*	0 (BE)	0 (BE)	0 (BE)	0 (BE)
0	0 (BE)	0 (BE)	0 (BE)	0 (BE)
1	0 (BE)	0 (BE)	0 (BE)	0 (BE)
2	0 (BE)	0 (BE)	0 (BE)	0 (BE)
3	0 (BE)	0 (BE)	0 (BE)	0 (BE)
4	0 (BE)	0 (BE)	0 (BE)	0 (BE)
5	0 (BE)	0 (BE)	0 (BE)	0 (BE)
6	0 (BE)	0 (BE)	0 (BE)	0 (BE)
7	0 (BE)	0 (BE)	0 (BE)	0 (BE)

**Queue Priority:** The actual Class of Service (COS).

**DSCP DP0:** Select the classified DSCP value (0-63) for Drop Precedence Level 0.

**DSCP DP1:** Select the classified DSCP value (0-63) for Drop Precedence Level 1.

**DSCP DP2:** Select the classified DSCP value (0-63) for Drop Precedence Level 2.

**DSCP DP3:** Select the classified DSCP value (0-63) for Drop Precedence Level 3.

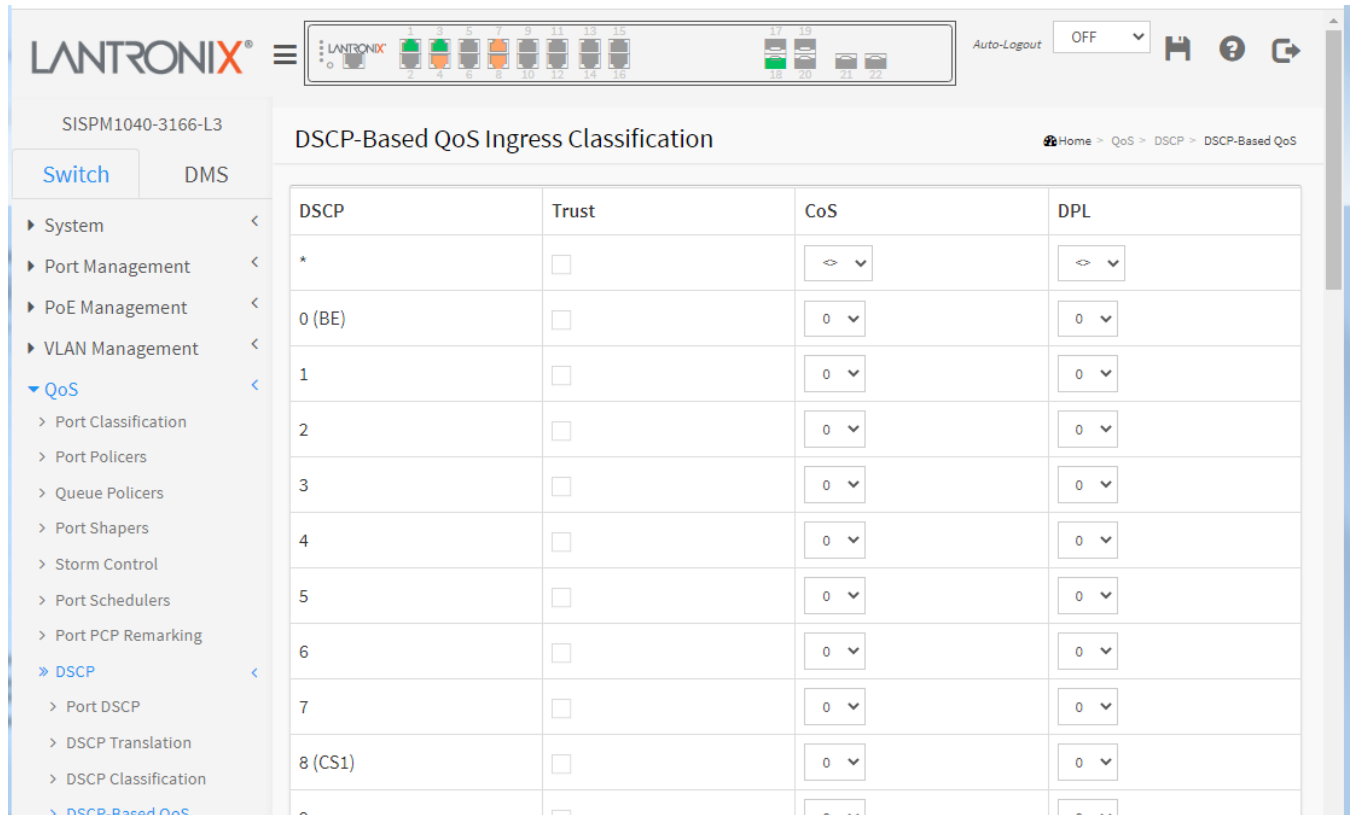
### Buttons

**Apply:** Click to save changes.

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

### DSCP-based QoS

This page lets you configure basic QoS DSCP-based QoS Ingress Classification settings for the switch.



**DSCP:** The maximum number of supported DSCP values is 64.

**Trust:** Controls whether a specific DSCP value is trusted. Only frames with trusted DSCP values are mapped to a specific CoS and DPL. Frames with untrusted DSCP values are treated as a non-IP frame.

**Queue Priority:** Queue Priority value can be 0-7 where 7 is the highest priority.

**DPL:** Drop Precedence Level (0-3)

#### Buttons

**Apply:** Click to save changes.

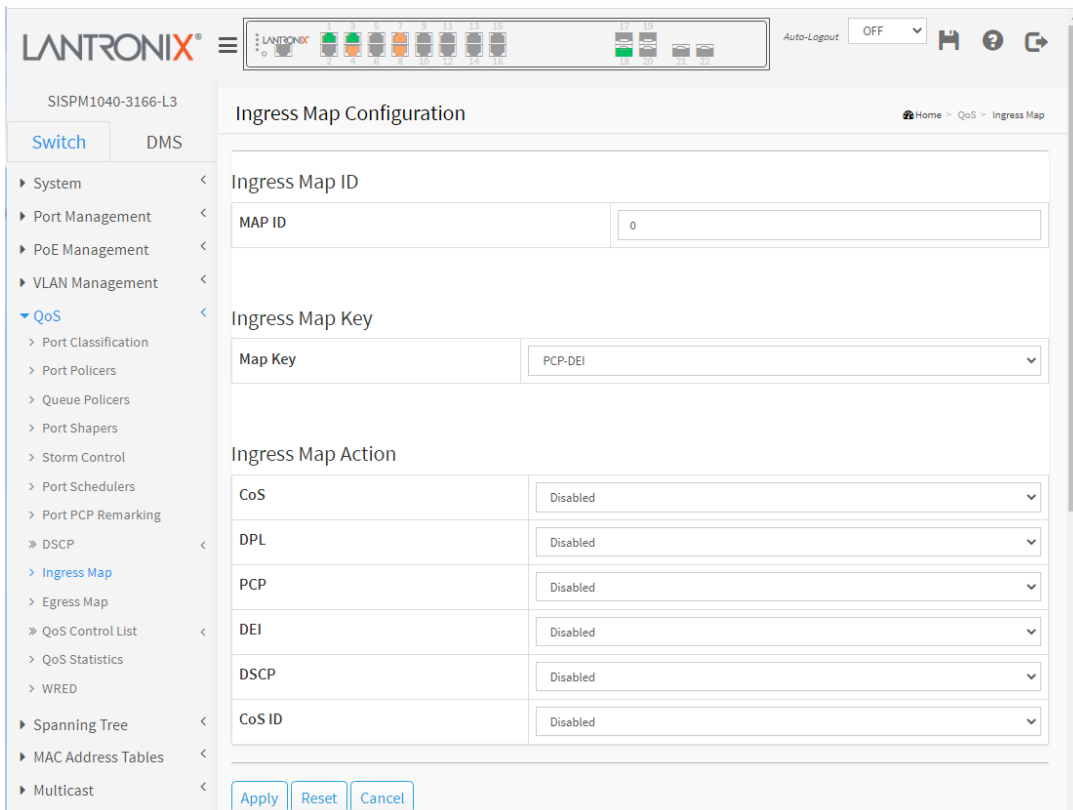
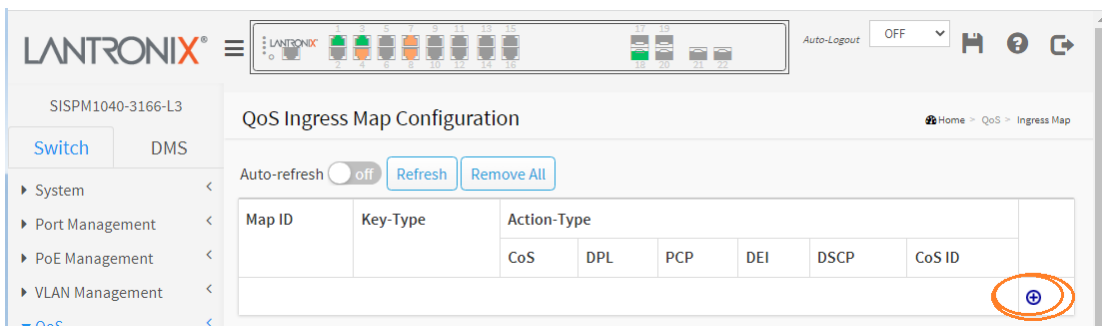
**Reset:** Click to undo any changes made locally and revert to previously saved values.

### Ingress Map

Navigate to QoS > Ingress Map to display the QoS Ingress Map Configuration page.

This page shows a table of QoS Ingress Maps which is made up of individual Map entries. Each entry has a key and an action. The key indicates which fields of the frame will be mapped to the fields specified by and according to the action. Each Map can hold a number of Map rules, or mappings between possible keys and actions. Which of those rules will be applied depends on the selection of (Key-Type, Action-Type). Each row describes a user-defined Map. The maximum number of Ingress Maps is 256. Each Ingress Map uses a number of key-entries in an internal key mapping table which has 1004 key-entries available for configuration. The consumption of key-entries by Key Type are listed as “table width” in the Key-Type parameter description below. A new Ingress Map can only be defined when there are sufficient free key-entries.

**Note:** This is just an overview of the configured Maps. You can add new Maps or edit existing Maps using the Add/Edit modification buttons. Click on the lowest plus sign (empty map entry) to add a new Ingress Map to the table.



**Ingress Map ID:** Indicates the Map (unique) ID. The valid range is 0 - 255. When in edit mode, this is non-configurable. However, it is possible to overwrite an existing mapping through the create mode.

**Ingress Map Key:** Indicates the Key type that will be used to filter the Map rules when applying the Map. As mentioned above, Map rules can have various keys, and this is to make a select set of them. Possible Key types are:

**PCP - DEI:** Use PCP/DEI as key for tagged frames and none for the rest.

**DSCP:** Use: DSCP as key for IP frames and none for the rest.

**DSCP - PCP - DEI:** Use DSCP as key for IP frames, PCP/DEI for tagged frames and none for the rest.

**Ingress Map Action :** Indicates the Action type that will be used to filter the Map rules when applying the map. As mentioned above, Map rules can have various actions available, and this is to make a select set of them.

Possible Action types are:

**CoS:** Class of Service.

**DPL:** Drop Precedence Level.

**PCP:** Priority Code Point.

**DEI:** Drop Eligible Indicator.

**DSCP:** Differentiated Services Code Point.

**CoS ID:** Class of Service ID.

### Buttons

**Apply :** Click to submit the Map configuration and move to the main Ingress Map page.

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

**Cancel :** Return to the Ingress Map page without saving the configuration changes.

**Example:** QoS Ingress Maps 0-3 configured with various Key-Types and Action-Types:

The screenshot shows the 'QoS Ingress Map Configuration' page. At the top, there's a navigation bar with 'Switch' and 'DMS' tabs, and a breadcrumb trail 'Home > QoS > Ingress Map'. Below the navigation bar, there's an 'Auto-refresh' toggle set to 'off', and 'Refresh' and 'Remove All' buttons. The main content is a table with the following data:

Map ID	Key-Type	Action-Type						
		CoS	DPL	PCP	DEI	DSCP	CoS ID	
0	PCP-DEI	Enabled	Disabled	Disabled	Disabled	Disabled	Disabled	⊕ ⊗
1	DSCP	Disabled	Enabled	Disabled	Disabled	Disabled	Disabled	⊕ ⊗
2	DSCP	Disabled	Disabled	Enabled	Enabled	Enabled	Disabled	⊕ ⊗
3	PCP-DEI	Enabled	Enabled	Enabled	Enabled	Enabled	Enabled	⊕ ⊗
								⊕

**Modification Buttons:** You can modify each Map (or add new maps) in the table using these buttons:



**Edit:** Edits the Map.



**Delete:** Deletes the Map.



**Add:** Adds a new Map in the table (can also be used to overwrite an existing Map, so use care on the Map ID).

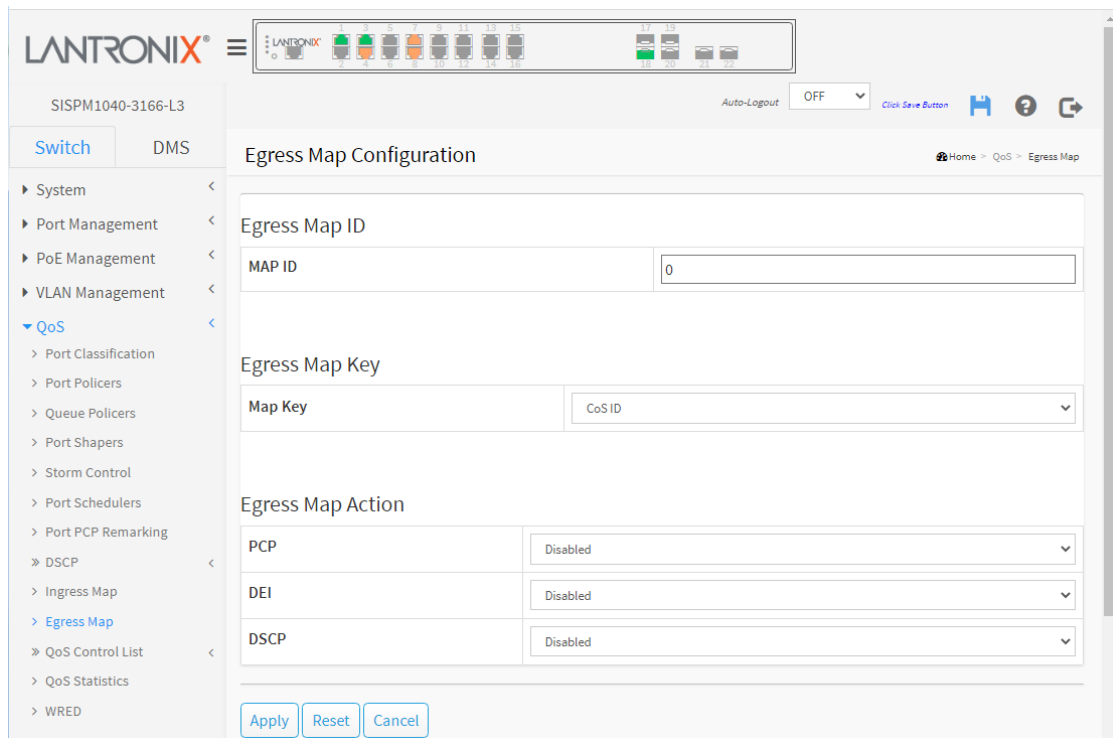
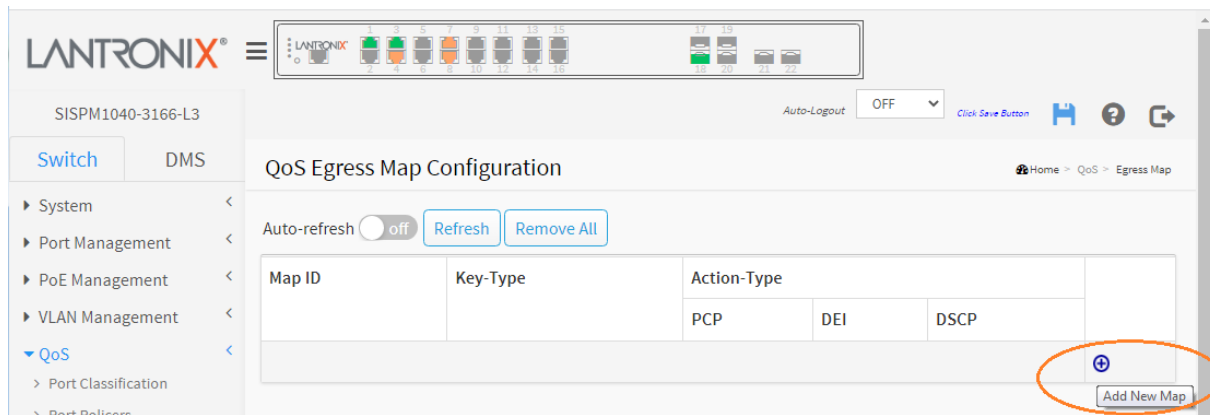
**Remove All:** Click to clear all table entries.

## Egress Map

Navigate to QoS > Egress Map to display the QoS Egress Map Configuration page.

This page shows a table of QoS Egress Maps which is made up of individual Map entries. Each entry has a key and an action. The key indicates which fields of the frame will be mapped to the fields specified by and according to the action. Each Map can hold a number of map rules, or mappings between possible keys and actions. Which of those rules will be applied depends on the selection of (Key-Type, Action-Type). Each row describes a user-defined map. The maximum number of Egress Maps is 512. Each Egress Map uses a number of key-entries in an internal key mapping table which have 960 key-entries available. The consumption of key-entries by Key Type are listed as “table width” in the Key-Type parameter description below. A new Egress Map can only be defined when there are sufficient free key-entries.

**Note:** This is just an overview of the configured Maps. You can add new Maps or edit existing Maps using the Add/Edit buttons. Click on the lowest plus sign (empty map entry) to add a new Ingress Map to the table.



**Map ID:** Indicates the Map (unique) ID. Range is 0 to 511.

**Key-Type:** Indicates the Key Type that will be used to filter the map rules when applying the map. As mentioned above, Map Rules can have various keys, and this is to make a select set of them. Possible Key types are:

**CoS ID:** Use classified COS ID as key. Table width: 1.

**CoS ID - DPL:** Use classified COS ID and DPL as key. Table width: 4.

**DSCP:** Use classified DSCP as key. Table width: 8.

**DSCP - DPL:** Use classified DSCP and DPL as key. Table width: 32.

**Action-Type:** Indicates the type of action that will be used to filter the map rules when applying the map. As mentioned above, map rules can have various actions available, and this is to make a select set of them. Possible Action types are:

**PCP:** Priority Code Point.

**DEI:** Drop Eligible Indicator.

**DSCP:** Differentiated Services Code Point.

**Modification Buttons:** It is possible to modify each map (or add new maps) in the table using these buttons:



**Edit:** Edits the map.



**Delete:** Deletes the map.



**Add:** Adds a new map in the table. Note: this button can also be used to overwrite an existing map, so use care on the Map ID.

## Buttons

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

**Refresh:** Click to refresh the page.

**Remove All:** Click to clear all table entries.

## QoS Map Rules Configuration

Maps have multiple rules inside them, and this page allows to view and configure the key and action filters that will be used when searching through the rules. To see and configure the set of rules for each map click on the Map ID (link) for each map. (Note: not the Edit button.)



**Example:** QoS Egress Map IDs 0-3 configured with various Key-Types and Action-Types:

The screenshot displays the LANTRONIX web interface for QoS Egress Map Configuration. The interface includes a navigation menu on the left, a top status bar with LANTRONIX logo and port indicators, and a main configuration area with a table of QoS Egress Maps.

**QoS Egress Map Configuration Table:**

Map ID	Key-Type	Action-Type			
		PCP	DEI	DSCP	
0	CoS ID	Enabled	Disabled	Disabled	⊕ ⊗
1	CoS ID-DPL	Enabled	Disabled	Disabled	⊕ ⊗
2	DSCP	Enabled	Disabled	Enabled	⊕ ⊗
3	DSCP-DPL	Enabled	Enabled	Enabled	⊕ ⊗
					⊕

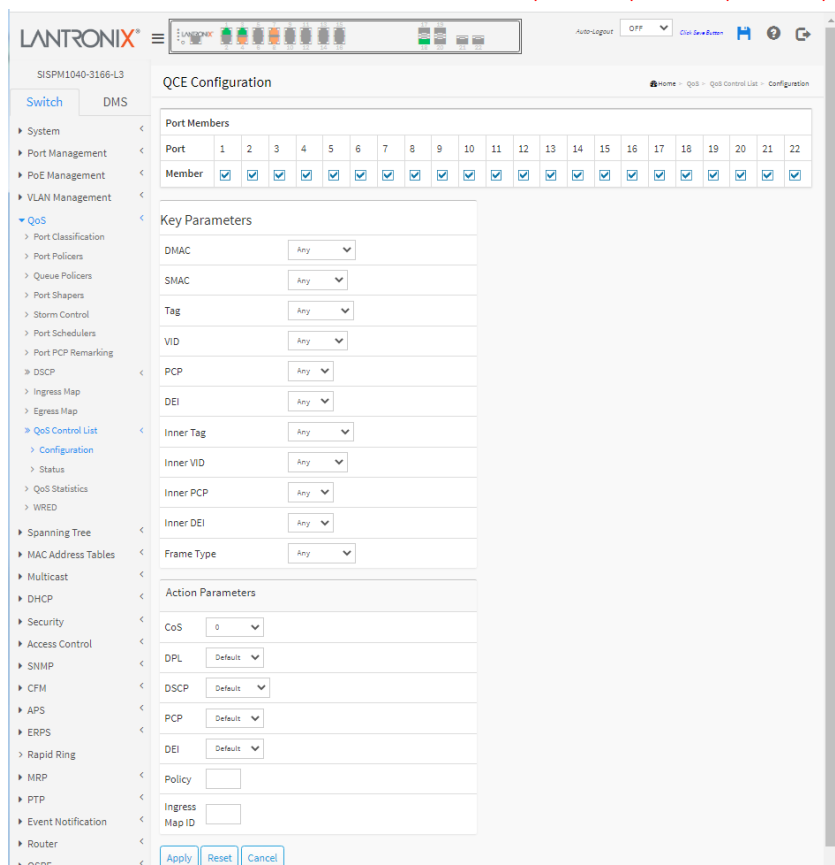
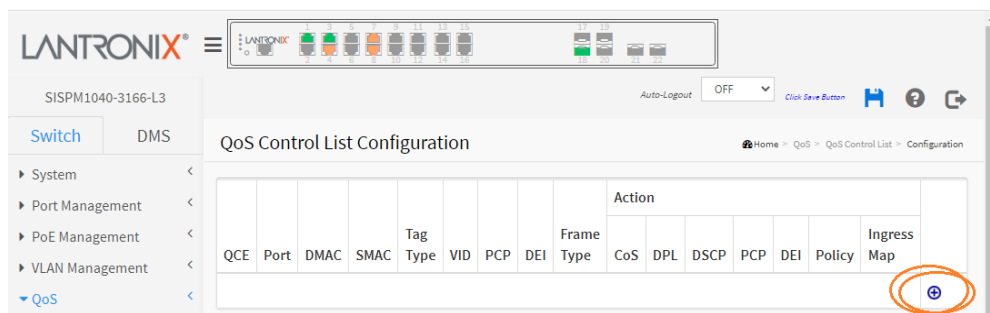
## QoS Control List

### QCE Configuration

This page shows the QoS Control List (QCL), which is made up of QCEs. Each row describes a QCE that is defined. The maximum number of QCEs is 256 per switch.

A QoS Control List is a list of QCEs. Every frame is compared against the QCEs in the list. The comparison starts with the first entry in the list and continues until there is a match between the frame and the key parameters or the end of the list is reached. If there is a match between the frame and the keys, the frame will be reclassified according to the action parameters. A QCE is a combination of keys and actions. The keys can be configured to match specific parts of a frame and the actions can be configured to override the default classified values of e.g., CoS.

Click on the lowest plus sign (+) to add a new QCE to the 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.

**Port Members:** Check the checkbox to include a port in the QCL entry. By default all ports are included .

**Key Parameters:** Key configuration is described below:

**DMAC** (Destination MAC address): Possible values are 'Unicast', 'Multicast', 'Broadcast', 'Specific' (xx-xx-xx-xx-xx-xx) or 'Any'.

**SMAC** (Source MAC address): xx-xx-xx-xx-xx-xx or 'Any'.

**Tag:** Value of Tag field can be 'Untagged', 'Tagged', 'C-Tagged', 'S-Tagged' or 'Any'.

**VID:** Valid value of VLAN ID can be any value in the range 1-4095 or 'Any'; enter either a specific value or a range of VIDs.

**PCP:** Valid value PCP are specific (0, 1, 2, 3, 4, 5, 6, 7) or range (0-1, 2-3, 4-5, 6-7, 0-3, 4-7) or 'Any'.

**DEI:** Valid value of DEI can be '0', '1' or 'Any'.

**Inner Tag:** Value of Inner Tag field can be 'Untagged', 'Tagged', 'C-Tagged', 'S-Tagged' or 'Any'.

**Inner VID:** Valid value of Inner VLAN ID can be any value in the range 1-4095 or 'Any'; user can enter either a specific value or a range of VIDs.

**Inner PCP:** Valid value of Inner PCP are specific (0, 1, 2, 3, 4, 5, 6, 7) or range (0-1, 2-3, 4-5, 6-7, 0-3, 4-7) or 'Any'.

**Inner DEI:** Valid value of Inner DEI can be '0', '1' or 'Any'.

**Frame Type:** Can have one of these values: Any, EtherType, LLC, SNAP, IPv4, or IPv6 as described below.

**1. Any:** Allow all types of frames.

**2. EtherType:** Valid Ether Type can be 0x600-0xFFFF excluding 0x800(IPv4) and 0x86DD(IPv6) or 'Any'.

**3. LLC:** The Logical Link Control (LLC) data comm protocol layer is the upper sublayer of layer 2 of the OSI model.

**DSAP Address:** Valid DSAP (Destination Service Access Point) can vary from 0x00 to 0xFF or 'Any'.

**SSAP Address:** Valid SSAP (Source Service Access Point) can vary from 0x00 to 0xFF or 'Any'.

**Control:** Valid Control field can vary from 0x00 to 0xFF or 'Any'.

**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.

**Destination IP:** Specific Destination IP address in value/mask format or 'Any'.

**IP Fragment:** IPv4 frame fragmented option: 'Yes', 'No' or 'Any'.

**DSCP:** Diffserv Code Point value (DSCP): It can be a specific value, range of values or 'Any'. DSCP values are in the range 0-63 including BE, CS1-CS7, EF or AF11-AF43.

**Sport:** Source TCP/UDP port:(0-65535) or 'Any', specific or port range applicable for IP protocol UDP/TCP.

**Dport:** Destination TCP/UDP port:(0-65535) or 'Any', specific or port range applicable for IP protocol UDP/TCP.

**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'.

**Destination IP:** Specific Destination IP address in value/mask format or 'Any'.

**DSCP:** Diffserv Code Point value (DSCP): It can be a specific value, range of values or 'Any'. DSCP values are in the range 0-63 including BE, CS1-CS7, EF or AF11-AF43.

**Sport:** Source TCP/UDP port:(0-65535) or 'Any', specific or port range applicable for IP protocol UDP/TCP.

**Dport:** Destination TCP/UDP port:(0-65535) or 'Any', specific or port range applicable for IP protocol UDP/TCP.

#### Action Parameters:

**Queue Priority:** Class of Service: (0-7) or 'Default'.

**DPL:** Drop Precedence Level: (0-3) or 'Default'.

**DSCP:** (0-63, BE, CS1-CS7, EF or AF11-AF43) or 'Default'.

**PCP:** (0-7) or 'Default'. Note: PCP and DEI cannot be set individually.

**DEI:** (0-1) or 'Default'.

**Policy:** ACL Policy number (0-127) or 'Default' (empty field).

'Default' means that the default classified value is not modified by this QCE.

#### Buttons


**Apply:** Click to save the configuration and move to main QCL page.

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

**Cancel:** Return to the previous page without saving the configuration change.

#### Modification Buttons

You can modify each QCE (QoS Control Entry) in the table using these buttons:

: Insert new QCE before the current row.

: Edit QCE.

: Move QCE up the list.

: Move QCE down the list.

: Delete QCE.

: The lowest plus sign adds a new QCE to the end of the QCE list.

#### Messages:

*PCP and DEI cannot be set individually!*

**Example:**

SISPM1040-3166-L3

QoS Control List Configuration

Home > QoS > QoS Control List > Configuration

QCE	Port	DMAC	SMAC	Tag Type	VID	PCP	DEI	Frame Type	Action								
									CoS	DPL	DSCP	PCP	DEI	Policy	Ingress Map		
1	Any	Any	Any	Any	Any	Any	Any	EtherType	0	Default	Default	Default	Default	Default	Default	Default	⊕ ⊕ ⊖ ⊖ ⊗
2	Any	Unicast	Any	Any	Any	Any	Any	IPv4	0	Default	Default	Default	Default	Default	Default	Default	⊕ ⊕ ⊖ ⊖ ⊗
3	2,5-22	Any	Any	Any	Any	Any	Any	IPv6	0	Default	Default	Default	Default	1	2	Default	⊕ ⊕ ⊖ ⊖ ⊗
																	⊕

## Status

This page shows the 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 per switch.

The screenshot shows the Lantronix web interface for a switch (SISPM1040-3166-L3). The main content area is titled "QoS Control List Status". It includes a navigation menu on the left with options like System, Port Management, PoE Management, VLAN Management, and QoS. The QoS section is expanded, showing Port Classification and Port Policers. The main table displays the following data:

User	QCE	Port	Frame Type	Action						Conflict	Ingress Map
				CoS	DPL	DSCP	PCP	DEI	Policy		
Static	1	Any	EtherType	0	Default	Default	Default	Default	Default	-	No
Static	2	Any	IPv4	0	Default	Default	Default	Default	Default	-	No
Static	3	2,5-22	IPv6	0	Default	Default	Default	Default	1	2	No

**User:** Indicates the QCL user.

**QCE:** Indicates the QCE id.

**Port:** Indicates the list of ports configured with the QCE.

**Frame Type:** Indicates the type of frame. Possible values are:

**Any:** Match any frame type.

**Ethernet:** Match EtherType frames.

**LLC:** Match (LLC) frames.

**SNAP:** Match (SNAP) frames.

**IPv4:** Match IPv4 frames.

**IPv6:** Match IPv6 frames.

**Action:** Indicates the classification action taken on ingress frame if parameters configured are matched with the frame's content. Possible actions are:

**Queue Priority:** 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. As hardware resources are shared by multiple applications. It may happen that resources required to add a QCE may not be available; in that case it shows Conflict status as 'Yes', otherwise it is always 'No'. Note that conflict can be resolved by releasing the hardware resources required to add QCL entry on pressing 'Resolve Conflict' button.

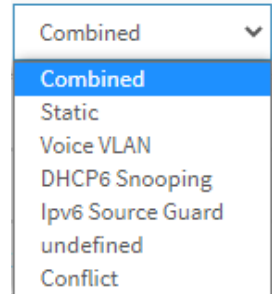
## Buttons

**QCL Status dropdown** : Select the QCL status from this drop down list.

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

**Resolve Conflict**: Click to release the resources required to add a QCL entry in case the Conflict status for any QCL entry is 'yes'.

**Refresh**: Click to refresh the page.



## QoS Statistics

This page provides statistics for the different queues for all switch ports.

The screenshot shows the 'Queuing Counters' page in the Lantronix web interface. The page title is 'Queuing Counters' and the breadcrumb is 'Home > QoS > QoS Statistics'. There is an 'Auto-refresh' toggle set to 'off' and buttons for 'Refresh' and 'Clear'. The table below shows the statistics for 11 ports (1-11) across 8 queues (Q0-Q7). Each queue has Rx and Tx columns. The data is as follows:

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	8111	269845	0	0	0	0	0	0	0	0	0	0	0	0	0	0	129205
2	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
3	256608	410448	0	0	0	0	0	0	0	0	0	0	0	0	0	0	129214
4	118531	159416	0	0	0	0	0	0	0	0	0	0	0	0	0	0	129205
5	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
6	0	80	0	0	0	0	0	0	0	0	0	0	0	0	0	0	16
7	24739	245113	0	0	0	0	0	0	0	0	0	0	0	0	0	0	129206
8	56766	213075	0	0	0	0	0	0	0	0	0	0	0	0	0	0	129205
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

**Port:** The logical port for the settings contained in each row. Click the linked port number to display its Detailed Port Statistics page (see below).

**Qn:** There are 8 QoS queues per port. Q0 is the lowest priority queue.

**Rx/Tx:** The number of received and transmitted packets per queue.

### Buttons

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

**Refresh:** Click to refresh the page immediately.

**Clear:** Clears the counters for all ports.



## Detailed Port Statistics

Click a linked port number to display its Detailed Port Statistics page. This page provides detailed traffic statistics for a selected 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.

SISPM1040-3166-L3

LANTRONIX

Auto-Logout OFF Click Save Button

Home > Port Management > Port Statistics

Switch DMS

System <

Port Management <

- Port Configuration
- Port Statistics
- SFP Port Info
- Energy Efficient Ethernet
- Link Aggregation <
- Link OAM <
- Loop Protection <
- UDLD <
- DDMI <
- PoE Management <
- VLAN Management <
- QoS <
- Spanning Tree <
- MAC Address Tables <
- Multicast <
- DHCP <
- Security <
- Access Control <
- SNMP <
- CFM <
- APS <
- ERPS <
- Rapid Ring
- MRP <
- PTP <

Detailed Port Statistics Port 1

Auto-refresh  off Refresh Clear Port 1

Receive Total		Transmit Total	
Rx Packets	8161	Tx Packets	401533
Rx Octets	1893134	Tx Octets	86461481
Rx Unicast	0	Tx Unicast	0
Rx Multicast	8161	Tx Multicast	246627
Rx Broadcast	0	Tx Broadcast	154906
Rx Pause	0	Tx Pause	0
Receive Size Counters		Transmit Size Counters	
Rx 64 Bytes	0	Tx 64 Bytes	68503
Rx 65-127 Bytes	2	Tx 65-127 Bytes	172327
Rx 128-255 Bytes	8159	Tx 128-255 Bytes	16348
Rx 256-511 Bytes	0	Tx 256-511 Bytes	144306
Rx 512-1023 Bytes	0	Tx 512-1023 Bytes	24
Rx 1024-1526 Bytes	0	Tx 1024-1526 Bytes	25
Rx 1527- Bytes	0	Tx 1527- Bytes	0
Receive Queue Counters		Transmit Queue Counters	
Rx Q0	8161	Tx Q0	271527
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

### 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.

**Note 1:** Short frames are frames that are smaller than 64 bytes.

**Note 2:** 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.

### **Receive MM Counters**

**Rx MM Fragments:** A count of received MAC frame fragments.

**Rx MM Assembly Ok:** A count of MAC frames that were successfully reassembled and delivered to MAC.

**Rx MM Assembly Errors:** A count of MAC frames with reassembly errors. The counter is incremented when the ASSEMBLY\_ERROR state of the Receive Processing State Diagram is entered.

**Rx MM SMD Errors:** A count of received MAC frames / MAC frame fragments rejected due to unknown SMD value or arriving with an SMD-C when no frame is in progress. The counter is incremented each time the BAD\_FRAG state of the Receive Processing State Diagram is entered.

### **Transmit MM Counters**

**Tx MM Fragments:** A count of transmitted MAC frame fragments.

**Tx MM Hold:** A count of times MM\_CTL.request (HOLD) primitive assertion caused preemption of a preemptable MAC frame.

### **Buttons**



: The port select box lets you select the port to be displayed.

**Refresh:** Click to refresh the page immediately.

**Clear:** Clears the counters for the selected port.

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

## WRED

This page allows you to configure the Random Early Detection (RED) settings. Through different RED configuration for the queues, it is possible to obtain Weighted Random Early Detection (WRED) operation between queues. The settings are global for all switch ports.

WRED (Weighted Random Early Detection) is an active queue management mechanism that provides preferential treatment of higher priority frames when traffic builds up within a queue. A frame's DPL is used as input to WRED. A higher DPL assigned to a frame results in a higher probability that the frame is dropped during times of congestion.

Group	Queue	DPL	Enable	Min	Max	Max Unit
1	0	1	<input checked="" type="checkbox"/>	1	40	Drop Probability
1	0	2	<input checked="" type="checkbox"/>	2	50	Fill Level
1	0	3	<input checked="" type="checkbox"/>	3	60	Fill Level
1	1	1	<input checked="" type="checkbox"/>	4	50	Drop Probability
1	1	2	<input checked="" type="checkbox"/>	5	50	Drop Probability
1	1	3	<input checked="" type="checkbox"/>	6	50	Drop Probability
1	2	1	<input type="checkbox"/>	0	50	Drop Probability

**Group:** The WRED group number for which the configuration below applies.

**Queue:** The queue number (CoS) for which the configuration below applies.

**DPL:** The Drop Precedence Level for which the configuration below applies.

**Enable:** Check the box for the RED to be enabled for this entry.

**Min:** Controls the lower RED fill level threshold. If the queue filling level is below this threshold, the drop probability is zero. This value is restricted to 0-100%.

**Max:** Controls the upper RED drop probability or fill level threshold for frames marked with Drop Precedence Level > 0 (yellow frames). This value is restricted to 1-100%.

**Max Unit:** Selects the unit for Max. Possible values are:

**Drop Probability:** Max controls the drop probability just below 100% fill level (default).

**Fill Level:** Max controls the fill level where drop probability reaches 100% (see below).

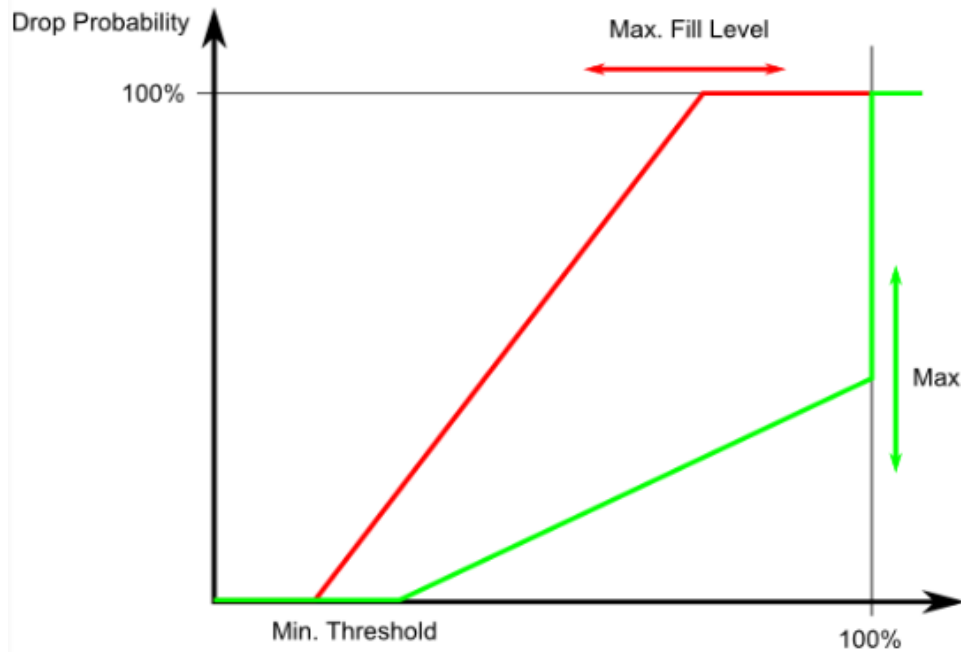
### Buttons

**Apply:** Click to save changes.

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

### RED Drop Probability Function

The figure below shows the drop probability versus fill level function with associated parameters.



#### **RED Drop Probability Function:**

**Min** is the fill level where the queue randomly start dropping frames marked with Drop Precedence Level > 0 (yellow frames).

If **Max Unit** is 'Drop Probability' (the green line), Max controls the drop probability when the fill level is just below 100%.

If **Max Unit** is 'Fill Level' (the red line), Max controls the fill level where drop probability reaches 100%. This configuration makes it possible to reserve a portion of the queue exclusively for frames marked with Drop Precedence Level 0 (green frames). The reserved portion is calculated as  $(100 - \text{Max}) \%$ .

Frames marked with Drop Precedence Level 0 (green frames) are never dropped.

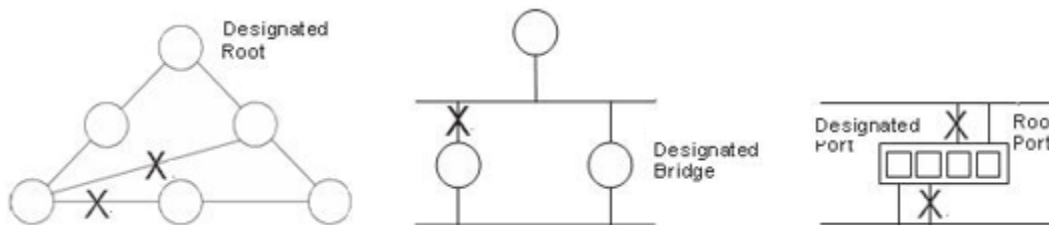
The drop probability for frames increases linearly from zero (at Min average queue filling level) to Max Drop Probability or Fill Level.

## Spanning Tree

Spanning Tree Protocols are OSI layer-2 protocols which ensure a loop free topology for any bridged LAN.

The Spanning Tree Protocol (STP) can be used to detect and disable network loops, and to provide backup links between switches, bridges or routers. This allows the switch to interact with other bridging devices (that is, an STP-compliant switch, bridge or router) in your network to ensure that only one route exists between any two stations on the network and provide backup links which automatically take over when a primary link goes down.

STP - 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.

## STP Configuration

This page lets you configure STP system settings which are used by all STP Bridge instances in the switch.

The screenshot shows the Lantronix web interface for the SISPM1040-3166-L3 switch. The main content area is titled "STP Bridge Configuration" and is divided into three sections: Basic Settings, Advanced Settings, and Root Guard.

**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 BPDUs Filtering	<input type="checkbox"/>
Edge Port BPDUs Guard	<input type="checkbox"/>
Port Error Recovery	<input type="checkbox"/>
Port Error Recovery Timeout	

**Root Guard:**

Port	Root Guard
*	<input type="checkbox"/>
1	<input type="checkbox"/>
?	<input type="checkbox"/>

### Basic Settings

**Protocol Version:** The MSTP / RSTP / 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. MSTP provides for multiple spanning tree instances, while ensuring RSTP and STP compatibility.

**Bridge Priority:** Controls the bridge priority. Lower numeric values have better priority. The bridge priority plus the MSTI instance number, concatenated with the 6-byte MAC address of the switch forms a Bridge Identifier. For MSTP operation, this is the priority of the CIST. Otherwise, this is the priority of the STP/RSTP bridge.

**Hello Time:** The interval between sending STP BPDU's. Valid values are 1 - 10 seconds; the default is 2 seconds. **Note:** Changing this parameter from the default value is not recommended and may have adverse effects on your network.

**Forward Delay:** The delay used by STP Bridges to transit Root and Designated Ports to Forwarding (used in STP compatible mode). Valid values are 4 - 30 seconds.

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

**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 6 - 40 hops.

**Transmit Hold Count:** The number of BPDU's a bridge port can send per second. When exceeded, transmission of the next BPDU will be delayed. Valid values are 1 - 10 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 30 - 86400 seconds (24 hours).

### **Root Guard**

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

**Root Guard:** Root guard allows the device to participate in STP as long as the device does not try to become the root. If root guard blocks the port, subsequent recovery is automatic. Recovery occurs as soon as the offending device ceases to send superior BPDUs.

### **Buttons**

**Apply:** Click to save changes.

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

## MSTI Configuration

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

When you implement a Spanning Tree protocol on the switch that is the bridge instance, the CIST is not available for explicit mapping, as it will receive the VLANs not explicitly mapped. So you must set the list of VLANs mapped to the MSTI. The VLANs must be separated with comma and/or space. A VLAN can only be mapped to one MSTI. An unused MSTI should just be left empty (i.e., not have any VLANs mapped to it).

Instance	VLANs Mapped	MSTI Priority	MSTI Port
CIST	Unmapped VLANs are mapped to the CIST	32768	Edit
MSTI1	Example: 2,3-5,11,13,20-40	32768	Edit
MSTI2	Example: 2,3-5,11,13,20-40	32768	Edit
MSTI3	Example: 2,3-5,11,13,20-40	32768	Edit
MSTI4	Example: 2,3-5,11,13,20-40	32768	Edit
MSTI5	Example: 2,3-5,11,13,20-40	32768	Edit
MSTI6	Example: 2,3-5,11,13,20-40	32768	Edit
MSTI7	Example: 2,3-5,11,13,20-40	32768	Edit

### 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 can have at most 32 characters.

**Configuration Revision:** The revision of the MSTI configuration named above. This must be an integer 0-65535.

### MSTI Mapping

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

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



**MSTI Priority:** Controls the bridge priority. Lower numeric values have better priority. The bridge priority plus the MSTI instance number, concatenated with the 6-byte MAC address of the switch forms a Bridge Identifier.

**Buttons**

**Edit:** In the MSTI Port column, click this to edit the MSTI ports of the instance (see STP CIST Port Configuration below).

**Apply:** Click to save changes.

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

**STP CIST Port Configuration**

In the MSTI Port column of the STP MSTI Configuration page, click the Edit button to edit the MSTI ports of the instance.

The screenshot shows the 'STP CIST Port Configuration' page in the Lantronix web interface. The left sidebar contains a navigation menu with categories like System, Port Management, PoE Management, VLAN Management, QoS, Spanning Tree, MAC Address Tables, Multicast, DHCP, Security, Access Control, SNMP, CFM, APS, ERPS, Rapid Ring, and MRP. The main content area is divided into two sections: 'CIST Aggregated Port Configuration' and 'CIST Normal Port Configuration'. Both sections contain tables with columns for Port, STP Enabled, Path Cost, Priority, Admin Edge, Auto Edge, and a 'Restricted' sub-section with Role, TCN, and BPDU Guard. The 'CIST Normal Port Configuration' table lists ports 1 through 8, with STP Enabled checked for all and Path Cost set to 'Auto'. The Priority is set to 128 for all ports, and Admin Edge is set to 'Non-Edge'. The Auto Edge is checked for all ports. The 'Restricted' section has Role and TCN unchecked, and BPDU Guard unchecked for all ports. The Point-to-point column is set to 'Auto' for all ports.

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

**STP Enabled :** Controls whether STP is enabled on this switch port. This field will be read only if Voice VLAN feature is enabled. The Voice VLAN port mode will be read only if this field be Enabled.

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

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

**AdminEdge** : Controls whether the operEdge flag should start as set or cleared. (The initial operEdge state when a port is initialized).

**AutoEdge** : Controls whether the bridge should enable automatic edge detection on the bridge port. This allows operEdge to be derived from whether BPDU's are received on the port or not.

**Restricted Role** : If enabled, causes the port not to be selected as Root Port for the CIST or any MSTI, even if it has the best spanning tree priority vector. Such a port will be selected as an Alternate Port after the Root Port has been selected. If set, it can cause lack of spanning tree connectivity. It can be set by a network administrator to prevent bridges external to a core region of the network influence the spanning tree active topology, possibly because those bridges are not under the full control of the administrator. This feature is also known as Root Guard.

**Restricted TCN** : If enabled, causes the port not to propagate received topology change notifications and topology changes to other ports. If set it can cause temporary loss of connectivity after changes in a spanning tree's active topology as a result of persistently incorrect learned station location information. It is set by a network administrator to prevent bridges external to a core region of the network, causing address flushing in that region, possibly because those bridges are not under the full control of the administrator or the physical link state of the attached LANs transits frequently.

**BPDU Guard** :If enabled, causes the port to disable itself upon receiving valid BPDU's. Contrary to the similar bridge setting, the port Edge status does not affect this setting. A port entering error-disabled state due to this setting is subject to the bridge Port Error Recovery setting as well.

**Point to Point** : Controls whether the port connects to a point-to-point LAN rather than to a shared medium. This can be automatically determined or forced either true or false. Transition to the forwarding state is faster for point-to-point LANs than for shared media.

## Buttons

**Apply** : Click to save changes.

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

## STP Status

This page provides a status overview of all STP bridge instances. The displayed table contains a row for each STP bridge instance.

The screenshot shows the Lantronix web interface for device SISPM1040-3166-L3. The left sidebar contains a navigation menu with categories like System, Port Management, PoE Management, VLAN Management, QoS, Spanning Tree (selected), MAC Address Tables, Multicast, DHCP, Security, Access Control, SNMP, and CFM. The main content area is titled 'STP Status' and includes an 'Auto-refresh' toggle (set to off) and a 'Refresh' button. Below this is a table with columns: MSTI, Bridge ID, Root ID, Port, Cost, Topology Flag, and Topology Change Last. The table shows one instance with MSTI 'CIST', Bridge ID '32768.00-C0-F2-7C-59-7F', and Root ID '32768.00-C0-F2-7C-59-7F'. Below the table is another section titled 'STP Port Status' with a table showing columns: Port, CIST Role, CIST State, and Uptime. This table lists 8 ports with roles like DesignatedPort or Disabled and states like Forwarding or Discarding.

### STP Status

**MSTI:** The Bridge Instance. This is also a link to the STP Detailed Bridge Status (see below).

**Bridge ID:** The Bridge ID of this Bridge instance.

**Root ID:** The Bridge ID of the currently elected root bridge.

**Root Port:** The switch port currently assigned the root port role.

**Root Cost:** Root Path Cost. For the Root Bridge it is zero. For all other Bridges, it is the sum of the Port Path Costs on the least cost path to the Root Bridge.

**Topology Flag:** The current state of the Topology Change Flag of this Bridge instance.

**Topology Change Last:** The time since last Topology Change occurred.

### STP Port Status

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

**CIST Role:** The current STP port role.

**CIST State:** The current STP port state. The port state can be one of the following values: Discarding Learning Forwarding.

**Uptime:** The time since the bridge port was last initialized.

## STP Detailed Bridge Status

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 for bridge instance CIST. The page includes a navigation menu on the left with categories like System, Port Management, PoE Management, VLAN Management, QoS, Spanning Tree, MAC Address Tables, Multicast, DHCP, Security, Access Control, SNMP, CFM, APS, ERPS, Rapid Ring, MRP, PTP, Event Notification, and Router. The main content area displays the following information:

**STP Bridge Status**

Bridge Instance	CIST
Bridge ID	32768.00-C0-F2-7C-59-7F
Root ID	32768.00-C0-F2-7C-59-7F
Root Cost	0
Root Port	-
Regional Root	32768.00-C0-F2-7C-59-7F
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	20000	Yes	Yes	2d 20:26:48
3	128:003	DesignatedPort	Forwarding	20000	Yes	Yes	2d 20:26:52
4	128:004	DesignatedPort	Forwarding	200000	Yes	Yes	2d 20:26:40
7	128:007	DesignatedPort	Forwarding	200000	Yes	Yes	2d 20:26:49
8	128:008	DesignatedPort	Forwarding	200000	Yes	Yes	2d 20:26:47
18	128:012	BackupPort	Discarding	20000	No	Yes	2d 20:26:50

### 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 the following values: AlternatePort, BackupPort, RootPort, and 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**

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

**Refresh:** Click to refresh the page immediately.

## Port Statistics

This page displays the STP port statistics counters of bridge ports in the switch.

The screenshot shows the Lantronix web interface for switch SISPM1040-3166-L3. The main content area is titled "STP Statistics" and includes an "Auto-refresh" toggle set to "off", along with "Refresh" and "Clear" buttons. Below this is a table with the following data:

Port	Transmitted				Received				Discarded	
	MSTP	RSTP	STP	TCN	MSTP	RSTP	STP	TCN	Unknown	Illegal
1	122677	0	0	0	1	0	0	0	0	0
3	122687	0	0	0	0	0	0	0	0	0
4	122673	0	0	0	0	0	0	0	0	0
7	122678	0	0	0	0	0	0	0	0	0
8	122677	0	0	0	0	0	0	0	0	0
18	6	0	0	0	122677	0	0	0	0	0

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

**MSTP:** The number of MSTP BPDU's received/transmitted on the port.

**RSTP:** The number of RSTP BPDU's received/transmitted on the port.

**STP:** The number of legacy STP Configuration BPDU's received/transmitted on the port.

**TCN:** The number of (legacy) Topology Change Notification BPDU's received/transmitted on the port.

**Discarded Unknown:** The number of unknown Spanning Tree BPDU's received (and discarded) on the port.

**Discarded Illegal:** The number of illegal Spanning Tree BPDU's received (and discarded) on the port.

### Buttons

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

**Refresh:** Click to refresh the page immediately.

**Clear:** Click to reset the counters.

## MAC Address 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 frame with the corresponding SMAC address has been seen after a configurable Ageing Time.

### MAC Address Table Configuration

The MAC Address Table is configured on this page. Set timeouts for entries in the dynamic MAC Table and configure the static MAC table here.

The screenshot shows the LANTRONIX web interface for MAC Address Table Configuration. The page title is "MAC Address Table Configuration" and the breadcrumb is "Home > MAC Address Tables > Configuration".

**Aging Configuration**

- Disable Automatic Aging:
- Aging Time: 300 seconds

**MAC Table Learning**

	Port Members																					
	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22
Auto	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>
Disable	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Secure	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

**VLAN Learning Configuration**

Learning-disabled VLANs:

**Static MAC Table Configuration**

	Port Members																							
Delete	VLAN ID	MAC Address	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22
<input type="button" value="Delete"/>	<input type="text" value="1"/>	<input type="text" value="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"/>	<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: Add New Static Entry, Apply, Reset

**Aging Configuration:** By default, dynamic entries are removed from the MAC table after 300 seconds. This removal is also called “aging”.

**Disable Automatic Aging:** Check the checkbox to disable the automatic aging of dynamic entries.

**Aging Time:** Configure aging time by entering a value in seconds. The allowed range is 10 - 1000000 seconds.

**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 an unknown SMAC is received.

**Disable:** No learning is done.

**Secure:** Only static MAC entries are learned; all other frames are dropped. **Note:** Before changing to Secure learning mode, make sure that the link used for managing the switch is added to the Static Mac Table; otherwise, the management link is lost and can only be restored by using another non-secure port or by connecting to the switch via the serial interface.

### **VLAN Learning Configuration**

**Learning-disabled VLANs:** This field shows the Learning-disabled VLANs. When a NEW MAC arrives into a learning-disabled VLAN, the MAC won't be learnt. By the default, the field is empty. More VLANs may be created by using a list syntax where the individual elements are separated by commas. Ranges are specified with a dash separating the lower and upper bound. The following example will create VLANs 1, 10, 11, 12, 13, 200, and 300: 1,10-13,200,300. Spaces are allowed in between the delimiters.

**Static MAC Table Configuration:** The static entries in the MAC table are shown in this table. The static MAC table can contain up to 64 entries. The MAC table is sorted first by VLAN ID and then by MAC address.

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

**VLAN ID:** The VLAN ID of the entry.

**MAC Address:** The MAC address of the entry.

**Port Members:** Checkmarks indicate which ports are members of the entry. Check or uncheck as needed to modify the entry.

### **Buttons**

**Add New Static Entry:** Click to add a new entry to the static MAC table. Specify the VLAN ID, MAC address, and port members for the new entry. Click "Apply".

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

**Apply:** Click to save changes.

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





**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.

## Multicast

IP multicast is an internet communication method where a single data packet can be transmitted from a sender and replicated to a set of receivers.

### IGMP Snooping

IGMP snooping is a method that network switches use to identify multicast groups, which are groups of computers or devices that all receive the same network traffic. It enables switches to forward packets to the correct devices in their network. IGMP snooping lets the switch connect 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.

### Basic Configuration

This page provides IGMP Snooping related configuration.

IGMP (Internet Group Management Protocol) is a communications protocol used to manage the membership of Internet Protocol multicast groups. IGMP is used by IP hosts and adjacent multicast routers to establish multicast group memberships. It is an integral part of the IP multicast specification, like ICMP for unicast connections. IGMP can be used for online video and gaming, and allows more efficient use of resources when supporting these uses.

**Global Configuration**

Snooping Enabled	<input checked="" type="checkbox"/>
Unregistered IPMCv4 Flooding Enabled	<input checked="" type="checkbox"/>
IGMP SSM Range	232.0.0.0 / 8
Leave Proxy Enabled	<input checked="" type="checkbox"/>
Proxy Enabled	<input checked="" type="checkbox"/>

**Port Related Configuration**

Port	Router Port	Fast Leave	Throttling	Filtering Profile
*	<input type="checkbox"/>	<input type="checkbox"/>	<	<
1	<input type="checkbox"/>	<input type="checkbox"/>	unlimited	- Preview
2	<input checked="" type="checkbox"/>	<input type="checkbox"/>	3	- Preview
3	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	4	- Preview
4	<input checked="" type="checkbox"/>	<input type="checkbox"/>	unlimited	- Preview
5	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	unlimited	- Preview
6	<input checked="" type="checkbox"/>	<input type="checkbox"/>	unlimited	- Preview

**Global Configuration:**

**Snooping Enabled:** Enable the Global IGMP Snooping.

**Unregistered IPMCv4 Flooding Enabled:** Enable unregistered IPMCv4 traffic flooding. The flooding control takes effect only when IGMP Snooping is enabled. When IGMP Snooping is disabled, unregistered IPMCv4 traffic flooding is always active in spite of this setting.

**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. Assign valid IPv4 multicast address as prefix with a prefix length (from 4 to 32) for the range.

**Leave Proxy Enabled:** Enable IGMP Leave Proxy. This feature can be used to avoid forwarding unnecessary leave messages to the router side.

**Proxy Enabled:** Enable IGMP Proxy to avoid forwarding unnecessary join and leave messages to the router side.

**Port Configuration:**

**Router Port:** Specify which ports act as router ports. A router port is a port on the Ethernet switch that leads towards the Layer 3 multicast device or IGMP querier. If an aggregation member port is selected as a router port, the whole aggregation will act as a router port.

**Fast Leave:** Enable the fast leave on the port. System will remove group record and stop forwarding data upon receiving the leave message without sending last member query messages. It is recommended to enable this feature only when a single IGMPv2 host is connected to the specific port.

**Throttling:** Enable to limit the number of multicast groups to which a switch port can belong.

**Filtering Profile:** Select the profile for this port. Click to preview the page which list the rules associated with the selected profile.

**Buttons**

**Apply:** Click to save changes.

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

## VLAN Configuration

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 let you select the starting point in the VLAN Table. Clicking the Refresh button will update the displayed table starting from that or the next closest VLAN Table match.

The Next Entry 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 First Entry button to start over.

**VLAN ID:** The VLAN ID of the entry.

**Snooping Enabled:** Enable the per-VLAN IGMP Snooping. Up to 64 VLANs can be selected for IGMP Snooping.

**Querier Election:** Enable to join IGMP Querier election in the VLAN. Disable to act as an IGMP Non-Querier.

**Querier Address:** Define the IPv4 address as source address used in IP header for IGMP Querier election. When the Querier address is not set, system uses IPv4 management address of the IP interface associated with this VLAN. When the IPv4 management address is not set, system uses the first available IPv4 management address. Otherwise, system uses a pre-defined value. By default, this value will be 192.0.2.1.

**Compatibility:** Compatibility is maintained by hosts and routers taking appropriate actions depending on the versions of IGMP operating on hosts and routers within a network. The allowed selections are IGMP-Auto, Forced IGMPv1, Forced IGMPv2, and Forced IGMPv3. The default compatibility value is IGMP-Auto.

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

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

**QI (sec):** Query Interval. The QI is the interval between General Queries sent by the Querier. The allowed range is 1 to 31744 seconds; the default QI is 125 seconds.

**QRI (0.1 sec):** Query Response Interval is the Maximum Response Delay used to calculate the Maximum Response Code inserted into the periodic General Queries. The allowed range is 0 to 31744 in tenths of a second; the default QRI is 100 in tenths of a second (10 seconds).

**LLQI (0.1 sec):** (LMQI for IGMP): Last Member Query Interval is the time value represented by the LMQI, multiplied by the Last Member Query Count. The allowed range is 0 to 31744 in tenths of a second; the default LLQI is 10 in tenths of a second (1 second).

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

#### **Buttons**

**Apply** : Click to save changes.

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

**Refresh** : Refreshes the displayed table starting from the "VLAN" input fields.

**First Page** : Updates the table starting from the first entry in the VLAN Table, i.e. the entry with the lowest VLAN ID.

**Next Page** : Updates the table, starting with the entry after the last entry currently displayed.

## Status

This page provides IGMP Snooping status.

The screenshot shows the Lantronix web interface for device SISPM1040-3166-L3. The main content area is titled 'IGMP Snooping Status'. It features an 'Auto-refresh' toggle set to 'off', with 'Refresh' and 'Clear' buttons. Below this is a 'Statistics' section with a table that currently shows 'No entries'. The 'Router Port' section contains a table with 7 rows, where ports 2 through 6 are marked as 'Static' and ports 1 and 7 are marked as '-'. The left navigation menu is expanded to 'Multicast' > 'IGMP Snooping' > 'Status'.

### Statistics

**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" means the specific interface is administratively disabled.

**Queries Transmitted:** The number of Transmitted Queries.

**Queries Received:** The number of Received Queries.

**V1 Reports Received:** The number of Received V1 Reports.

**V2 Reports Received:** The number of Received V2 Reports.

**V3 Reports Received:** The number of Received V3 Reports.

**V2 Leaves Received:** The number of Received V2 Leaves.

**Router Port:** Displays which ports act as router ports. A router port is a port on the Ethernet switch that leads towards the Layer 3 multicast device or IGMP querier.

**Static** denotes the specific port is configured to be a router port.

**Dynamic** denotes the specific port is learnt to be a router port.

**Both** denote the specific port is configured or learnt to be a router port.

**Port:** Switch port number.

**Status:** Indicate whether specific port is a router port or not.

**Buttons**

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

**Refresh**: Click to refresh the page immediately.

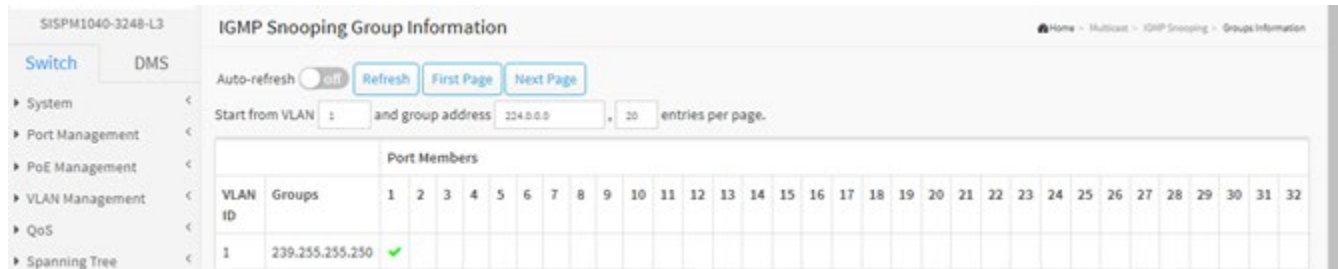
**Clear**: Clears all Statistics counters.



## Groups Information

Entries in the IGMP Group table are shown on this page. The "Start from VLAN", and "group address" input fields let you select the starting point in the IGMP Group table.

The IGMP Group Table is sorted first by VLAN ID, and then by group. This will use the last entry of the currently displayed table as a basis for the next lookup. When the end is reached the text "No more entries" is shown in the displayed table. Use the button to start over.



**VLAN ID:** VLAN ID of the group.

**Groups:** Group address of the group displayed.

**Port Members:** Ports under this group.

### Buttons

**Auto-refresh :** Click to *on* to automatically refresh the webpage every 3 seconds.

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

**First Page:** Updates the table, starting with the first entry in the IGMP Group table.

**Next Page:** Updates the table, starting with the entry after the last entry currently displayed.

## IGMP SFM Information

Entries in the IGMP SFM Information Table are shown on this page. The IGMP SFM (Source-Filtered Multicast) Information Table also contains the SSM (Source-Specific Multicast) information. This table is sorted first by VLAN ID, then by group, and then by Port. Different source addresses that belong to the same group are treated as a single entry.

**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:** The IP Address of the source. Currently, the maximum number of IPv4 source address for filtering (per group) is 8. When there is no 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 address could be handled by chip.

### Buttons

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

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

**<< :** Updates the table, starting with the first entry in the IGMP Group table.

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

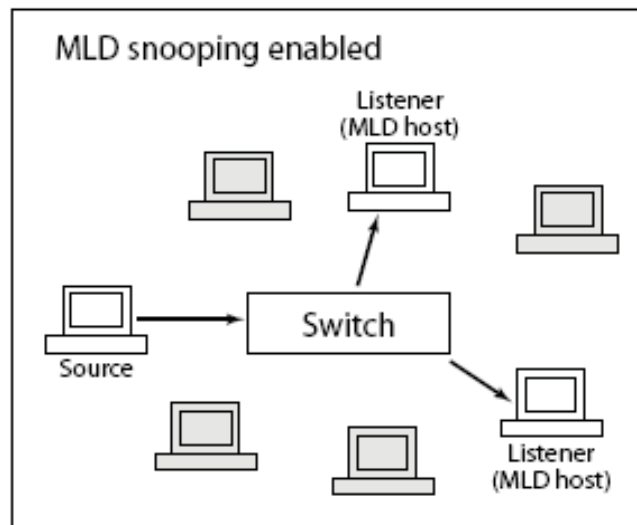
## MLD Snooping

MLD (Multicast Listener Discovery for IPv6) is used by IPv6 routers to discover multicast listeners on a directly attached link, much as IGMP is used in IPv4. The protocol is embedded in ICMPv6 instead of using a separate protocol.

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.



## Basic Configuration

This page provides MLD Snooping related configuration.

The screenshot shows the LANTRONIX web interface for the SISPM1040-3166-L3 switch. The main heading is "MLD Snooping Basic Configuration". The breadcrumb trail is "Home > Multicast > MLD Snooping > Basic Configuration".

**Global Configuration**

- Snooping Enabled:  on
- Unregistered IPMCv6 Flooding Enabled:
- MLD SSM Range: ff3e:: / 96
- Leave Proxy Enabled:
- Proxy Enabled:

**Port Related Configuration**

Port	Router Port	Fast Leave	Throttling	Filtering Profile
*	<input type="checkbox"/>	<input type="checkbox"/>	<	<
1	<input type="checkbox"/>	<input type="checkbox"/>	unlimited	- > Preview
2	<input checked="" type="checkbox"/>	<input type="checkbox"/>	unlimited	- > Preview
3	<input type="checkbox"/>	<input type="checkbox"/>	unlimited	- > Preview
4	<input checked="" type="checkbox"/>	<input type="checkbox"/>	9	- > Preview
5	<input type="checkbox"/>	<input type="checkbox"/>	unlimited	- > Preview
6	<input type="checkbox"/>	<input type="checkbox"/>	unlimited	- > Preview
7	<input type="checkbox"/>	<input type="checkbox"/>	unlimited	- > Preview

### Global Configuration

**Snooping Enabled:** Enable the Global MLD Snooping.

**Unregistered IPMCv6 Flooding Enabled:** Enable unregistered IPMCv6 traffic flooding. The flooding control takes effect only when MLD Snooping is enabled. When MLD Snooping is disabled, unregistered IPMCv6 traffic flooding is always active in spite of this setting.

**MLD SSM Range:** SSM (Source-Specific Multicast) Range allows the SSM-aware hosts and routers run the SSM service model for the groups in the address range. Assign valid IPv6 multicast address as prefix with a prefix length (from 8 to 128) for the range.

**Leave Proxy Enabled:** Enable MLD Leave Proxy. This feature can be used to avoid forwarding unnecessary leave messages to the router side.

**Proxy Enabled:** Enable MLD Proxy. This feature can be used to avoid forwarding unnecessary join and leave messages to the router side.

### **Port Related Configuration**

**Router Port:** Specify which ports act as router ports. A router port is a port on the Ethernet switch that leads towards the Layer 3 multicast device or MLD querier. If an aggregation member port is selected as a router port, the whole aggregation will act as a router port.

**Fast Leave:** Enable the fast leave on the port. The system will remove group record and stop forwarding data upon receiving the leave message without sending last member query messages. It is recommended to enable this feature only when a single MLDv1 host is connected to the specific port.

**Throttling:** Enable to limit the number of multicast groups to which a switch port can belong.

**Filtering Profile:** Select the profile for this port. Click to preview the page which list the rules associated with the selected profile.

### **Buttons**

**Apply:** Click to save changes.

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

## VLAN Configuration

This page displays the MLD Snooping VLAN Configuration table.

**Note:** Before MLD VLAN interface creation, you must enter the IP Configuration page to set up an IP interface at System > IP > Add IP Interface.

SISPM1040-3166-L3

MLD Snooping VLAN Configuration

VLAN ID	Snooping Enabled	Querier Election	Compatibility	PRI	RV	QI (sec)	QRI (0.1 sec)	LLQI (0.1 sec)	URI (sec)
1	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	MLD-Auto	0	2	125	100	10	1

Apply Reset

**VLAN ID:** The VLAN ID of the entry.

**Snooping Enabled:** Check the box to enable per-VLAN MLD Snooping. Up to 128 VLANs can be set for MLD Snooping.

**Querier Election:** Check the box to join MLD Querier election in the VLAN. Disable to act as a MLD Non-Querier.

**Compatibility:** Compatibility is maintained by hosts and routers taking appropriate actions depending on the versions of MLD operating on hosts and routers within a network. The allowed selections are MLD-Auto, Forced MLDv1, and Forced MLDv2. The default compatibility value is MLD-Auto.

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

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

**QI:** Query Interval is the interval between General Queries sent by the Querier. The allowed range is 1 - 31744 seconds; the default QI is 125 seconds.

**QRI:** Query Response Interval is the Maximum Response Delay used to calculate the Maximum Response Code inserted into the periodic General Queries. The allowed range is 0 - 31744 in tenths of a second; the default QRI is 100 in tenths of a second (10 seconds).

**LLQI:** Last Listener Query Interval is the Maximum Response Delay used to calculate the Maximum Response Code inserted into Multicast Address Specific Queries sent in response to Version 1 Multicast Listener Done messages. It is also the Maximum Response Delay used to calculate the Maximum Response Code inserted into Multicast Address and Source Specific Query messages. The allowed range is 0 - 31744 in tenths of a second. The default LLQI is 10 in tenths of a second (1 second).

**URI:** Unsolicited Report Interval is the time between repetitions of a node's initial report of interest in a multicast address. The allowed range is 0 - 31744 seconds; the default URI is 1 second.

### Buttons

**Apply:** Click to save changes.

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

## Status

This page provides MLD Snooping status and statistics.

The screenshot shows the Lantronix web interface for device SISPM1040-3166-L3. The page title is 'MLD Snooping Status'. On the left is a navigation menu with categories like System, Port Management, PoE Management, VLAN Management, QoS, Spanning Tree, MAC Address Tables, Multicast, IGMP Snooping, MLD Snooping, Basic Configuration, VLAN Configuration, Status, Groups Information, MLD SFM Information, MVR, and Multicast Filtering Profile. The main content area has an 'Auto-refresh' toggle set to 'off' with 'Refresh' and 'Clear' buttons. Below is a 'Statistics' table with columns: VLAN ID, Querier Version, Host Version, Querier Status, Queries Transmitted, Queries Received, V1 Reports Received, V2 Reports Received, and V1 Leaves Received. The table shows 'No entries'. Below that is a 'Router Port' table with columns: Port and Status. The Router Port table shows ports 1, 2, 3, 4, 5, 6, and 7 with statuses: -, Static, -, Static, -, -, and -.

### Statistics

**VLAN ID:** The VLAN ID of the entry.

**Querier Version:** Working Querier version currently.

**Host Version:** Working Host Version currently.

**Querier Status:** Shows the Querier status is "ACTIVE" or "IDLE". Shows "DISABLE" to denote the specific interface is administratively disabled.

**Queries Transmitted:** The number of Transmitted Queries.

**Queries Received:** The number of Received Queries.

**V1 Reports Received:** The number of Received V1 Reports.

**V2 Reports Received:** The number of Received V2 Reports.

**V1 Leaves Received:** The number of Received V1 Leaves.

**Router Port:** Displays which ports act as router ports. A router port is a port on the Ethernet switch that leads towards a Layer 3 multicast device or MLD querier.

**Port:** The switch port number.

**Status:** Indicates each port's status:

**Static** denotes the specific port is configured to be a router port.

**Dynamic** denotes the specific port is learnt to be a router port.

**Both** denote the specific port is configured or learned to be a router port.

**Buttons**

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

**Refresh**: Click to refresh the page immediately.

**Clear**: Clears all Statistics counters.



## Groups Information

Entries in the MLD Snooping Group Information table are shown on this page. The table is sorted first by VLAN ID, and then by group.

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 "and group address" input fields let you select the starting point in the MLD Group table.

The screenshot displays the 'MLD Snooping Group Information' page in the Lantronix web interface. The page title is 'MLD Snooping Group Information' and the breadcrumb trail is 'Home > Multicast > MLD Snooping > Groups Information'. The page includes an 'Auto-refresh' toggle set to 'off', 'Refresh', 'First Page', and 'Next Page' buttons. Below these are input fields for 'Start from VLAN' (set to 1) and 'and group address #00:'. The table below shows 'No more entries'.

		Port Members																					
VLAN ID	Groups	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22
No more entries																							

**VLAN ID:** The VLAN ID of the group.

**Groups:** The group address of the group displayed.

**Port Members:** Ports under this group.

### Buttons

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

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

**First Page:** Updates the table, starting with the first entry in the MLD Group Table.

**Next Page:** Updates the table, starting with the entry after the last entry currently displayed.

## MLD SFM Information

Entries in the MLD SFM Information Table are shown on this page. The MLD SFM (Source-Filtered Multicast) Information Table also contains the SSM (Source-Specific Multicast) information. This table is sorted first by VLAN ID, then by Group, and then by Port. Different source addresses belonging to the same group are treated as a single entry.

When first visited, the web page will show the first 20 entries from the beginning of the MLD SFM Information table. The "Start from VLAN", and "and group address" input fields let you select the starting point in the MLD SFM Information table.

The screenshot shows the Lantronix web interface for device SISPM1040-3166-L3. The page title is 'MLD SFM Information'. There are navigation buttons for 'Auto-refresh' (set to off), 'Refresh', 'First Page', and 'Next Page'. Below these are input fields for 'Start from VLAN' (value: 1), 'and group address' (value: ff00::), and 'entries per page' (value: 20). A table with the following columns is displayed: VLAN ID, Group, Port, Mode, Source Address, Type, and Hardware Filter/Switch. The table content is 'No more entries'.

**VLAN ID:** The VLAN ID of the group.

**Group:** Group address of the group displayed.

**Port:** Switch port number.

**Mode:** Indicates the filtering mode maintained per (VLAN ID, port number, Group Address) basis. It can be either Include or Exclude.

**Source Address:** IP Address of the source. Currently, the maximum number of IPv6 source address for filtering (per group) is 8. When there is no 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 IPv6 address can or cannot be handled by chip.

### Buttons

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

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

**First Page:** Updates the table starting from the first entry in the MLD SFM Information table.

**Next Page:** Updates the table, starting with the entry after the last entry currently displayed.

# MVR

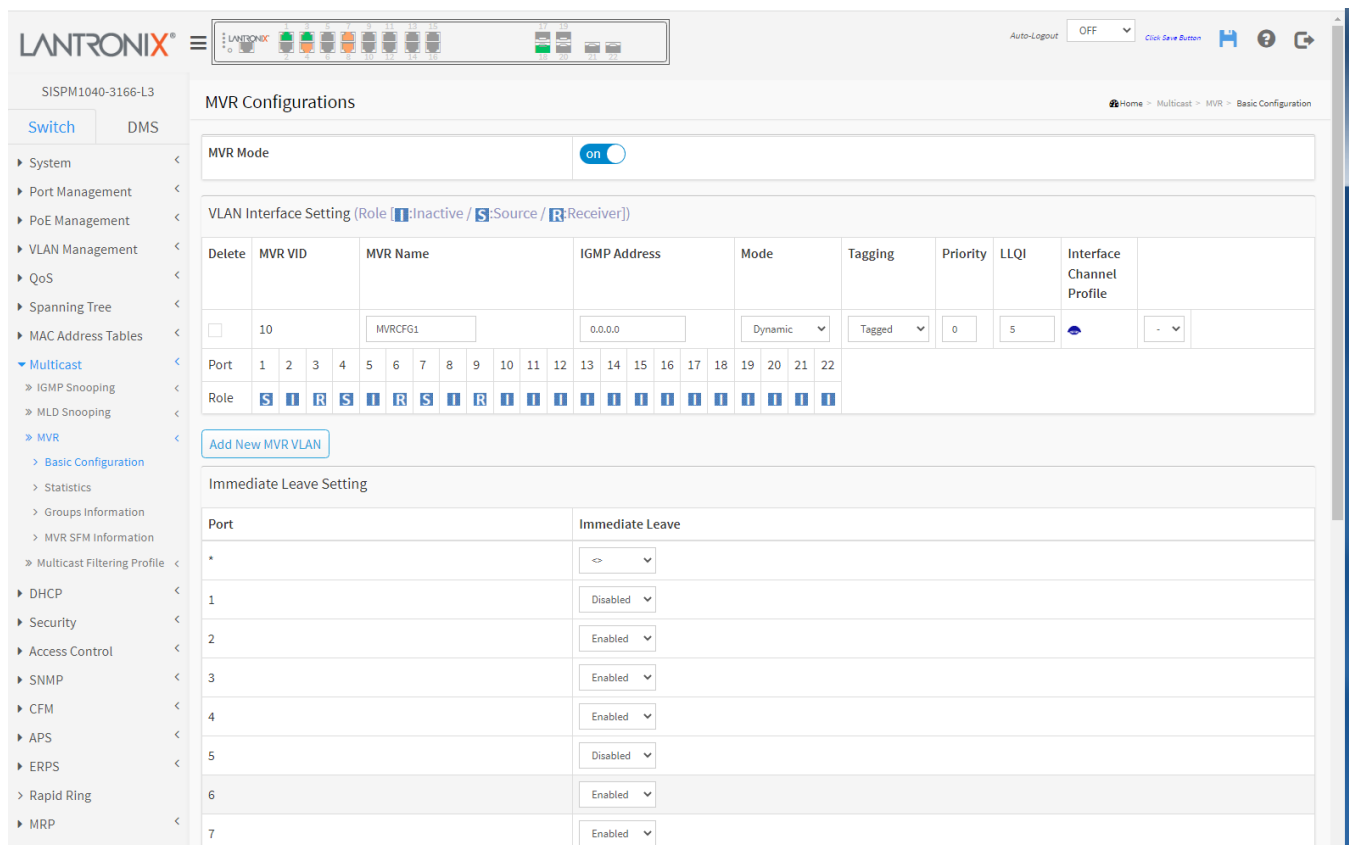
## Basic Configuration

This page provides MVR related configurations. The MVR (Multicast VLAN Registration) feature enables multicast traffic forwarding on the Multicast VLANs.

In a multicast television application, a PC or a network television or a set-top box can receive the multicast stream. Multiple set-top boxes or PCs can be connected to one subscriber port, which is a switch port configured as an MVR receiver port. When a subscriber selects a channel, the set-top box or PC sends an IGMP/MLD report message to Switch A to join the appropriate multicast group address. Uplink ports that send and receive multicast data to and from the multicast VLAN are called MVR source ports.

A maximum of four MVR VLANs with a corresponding channel profile for each Multicast VLAN is allowed. The channel profile is defined by the IPMC Profile which provides the filtering conditions.

MVR is a protocol for Layer 2 (IP)-networks that enables multicast-traffic from a source VLAN to be shared with subscriber-VLANs.



**MVR Mode:** Enable/Disable the Global MVR. The Unregistered Flooding control depends on the current configuration in IGMP/MLD Snooping. It is suggested to enable Unregistered Flooding control when the MVR group table is full.

**VLAN Interface Setting** (Role [I]:Inactive / [S]:Source / [R]:Receiver)

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

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

**MVR Name:** MVR Name is an optional attribute to indicate the name of the specific MVR VLAN. Maximum length of the MVR VLAN Name string is 16 characters (only alpha or numeric characters). 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 an IPv4 management address is not set, system uses the first available IPv4 management address. Otherwise, the 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, select the IPMC Profile as the channel filtering condition for the specific MVR VLAN. A summary of the Interface Channel Profiling (of the MVR VLAN) will be shown by clicking the View button. Profile selected for designated interface channel is not allowed to have overlapped permit group address.

**Profile Management button:** You can inspect the rules of the designated profile by using the following button:



**Navigate Profile:** List the rules associated with the designated profile.

**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 (default).

**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.

**Immediate Leave:** Enable the fast leave on the port. The system will remove group record and stop forwarding data upon receiving the leave message without sending last member query messages. It is recommended to enable this feature only when a single IGMPv2/MLDv1 host is connected to the specific port.

## Buttons

**Add New MVR VLAN:** Click to add a new MVR VLAN to the table. Specify the VID and configure the new entry.

**Apply:** Click to save changes.

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

**Message:** *MVR Interface Configuration Error Failure in SET MVR VLAN VID 200*

## Statistics

This page provides MVR Statistics information.

The screenshot shows the Lantronix web interface for device SISPM1040-3166-L3. The page title is "MVR Statistics". There is an "Auto-Logout" dropdown set to "OFF" and a "Click Save Button" link. A navigation menu on the left includes "Switch" and "DMS" sections. The main content area features an "Auto-refresh" toggle set to "off" and "Refresh" and "Clear" buttons. Below these is a table with the following data:

VLAN ID	IGMP/MLD Queries Received	IGMP/MLD Queries Transmitted	IGMPv1 Joins Received	IGMPv2/MLDv1 Reports Received	IGMPv3/MLDv2 Reports Received	IGMPv2/MLDv1 Leaves Received
10	0 / 0	0 / 0	0	0 / 0	0 / 0	0 / 0
11	0 / 0	0 / 0	0	0 / 0	0 / 0	0 / 0

**VLAN ID:** The Multicast VLAN ID.

**IGMP/MLD Queries Received:** The number of Received Queries for IGMP and MLD, respectively.

**IGMP/MLD Queries Transmitted:** The number of Transmitted Queries for IGMP and MLD, respectively.

**IGMPv1 Joins Received:** The number of Received IGMPv1 Joins.

**IGMPv2/MLDv1 Report's Received:** The number of Received IGMPv2 Joins and MLDv1 Reports, respectively.

**IGMPv3/MLDv2 Report's Received:** The number of Received IGMPv1 Joins and MLDv2 Reports, respectively.

**IGMPv2/MLDv1 Leave's Received:** The number of Received IGMPv2 Leaves and MLDv1 Dones, respectively.

### Buttons

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

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

**Clear:** Clears all Statistics counters.

## Groups Information

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 let you select the starting point in the MVR Channels (Groups) Information Table.

The screenshot displays the 'MVR Group Information' page in the Lantronix web interface. At the top, there is a navigation menu with 'Switch' and 'DMS' tabs. The main content area features an 'Auto-refresh' toggle set to 'off', and buttons for 'Refresh', 'First Page', and 'Next Page'. Below these are input fields for 'Start from VLAN' (value: 1) and 'Group Address' (value: ::), followed by a '20 entries per page' selector. A table titled 'Port Members' is shown with columns for 'VLAN ID', 'Groups', and ports 1 through 22. The table currently displays 'No more entries'.

**VLAN ID:** VLAN ID of the group.

**Groups:** Group ID of the group displayed.

**Port Members:** Ports under this group.

### Buttons

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

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

**First Page:** Updates the table starting from the first entry in the MVR Channels (Groups) Information table.

**Next Page:** Updates the table, starting with the entry after the last entry currently displayed.

## MVR SFM Information

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 let you select the starting point in the MVR SFM Information table.

**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:** The IP Address of the source. Currently, the maximum number of IP source address for filtering (per group) is 8. When there is no source filtering address, the text "None" is shown in the Source Address field.

**Type:** Indicates the Type configured. 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 or cannot be handled by the chip.

### Buttons

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

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

**First Page:** Updates the table starting from the first entry in the MVR Channels (Groups) Information table.

**Next Page:** Updates the table, starting with the entry after the last entry currently displayed.

## Multicast Filtering Profile

### Multicast Filtering Profile > Filtering Profile Table

This page provides IPMC Profile related configurations.

The IPMC profile is used to deploy the access control on IP multicast streams. You can create a maximum of 64 Profiles and a maximum of 128 corresponding Rules for each profile.

**Multicast Filtering Profile Mode:** Set to **on** (to enable) or **off** (to disable) Multicast Filtering Profile globally. The system starts filtering based on profile settings only when this global Profile Mode is **on** (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 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. Summary about the designated profile will be shown by clicking the view button. You can edit or preview the rules of the designated profile by using these buttons:

**Preview:** Preview the rules associated with the designated profile (see below).

**Edit:** Adjust the rules associated with the designated profile (see below).

#### Buttons

**Add New Filtering Profile:** Click to add new IPMC filtering profile. Specify the name and configure the new entry. Click "Apply".

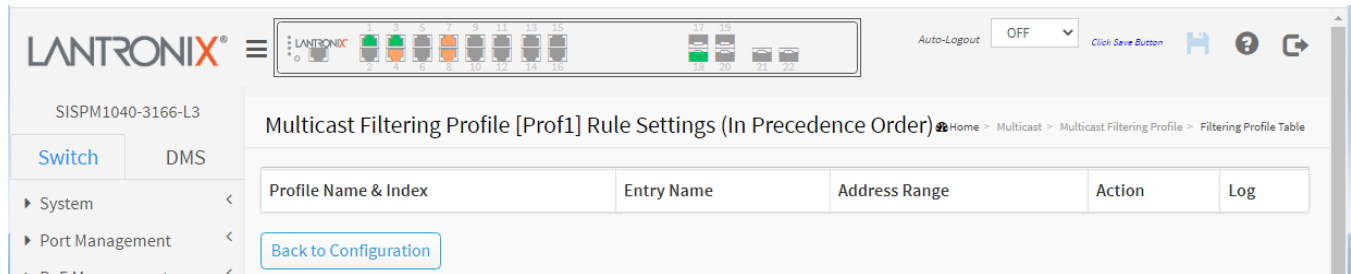
**Apply:** Click to save changes.

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



## Rule > Preview page

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. Note: the profile performs **deny** action for all groups if there is no **permit** entry is included in the profile.



**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 the following buttons:

 **Insert:** Insert a new rule before the current entry of rule.

 **Delete:** Delete the current entry of rule.

 **Up:** Moves the current entry of rule up in the list.

 **Down:** Moves the current entry of rule down in the list.

### Buttons

**Add Last Rule:** Click to add a new rule in the end of the specific profile's rule list. Specify the address entry and configure the new entry. Click "Commit" when done.

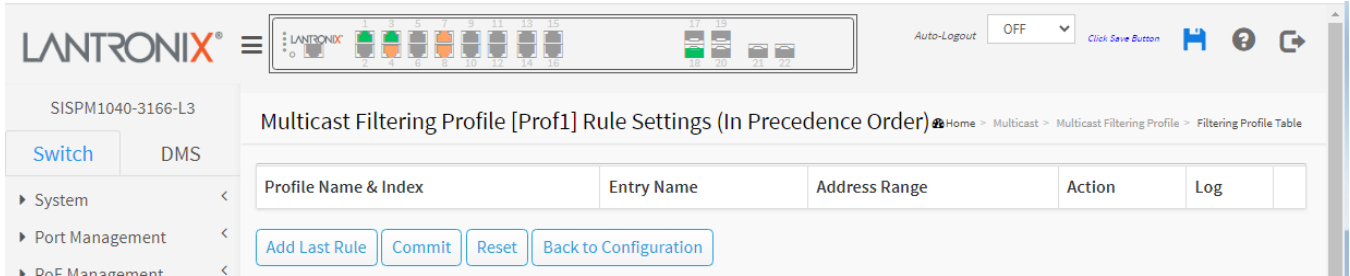
**Commit:** Click to commit rule changes for the designated profile.

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

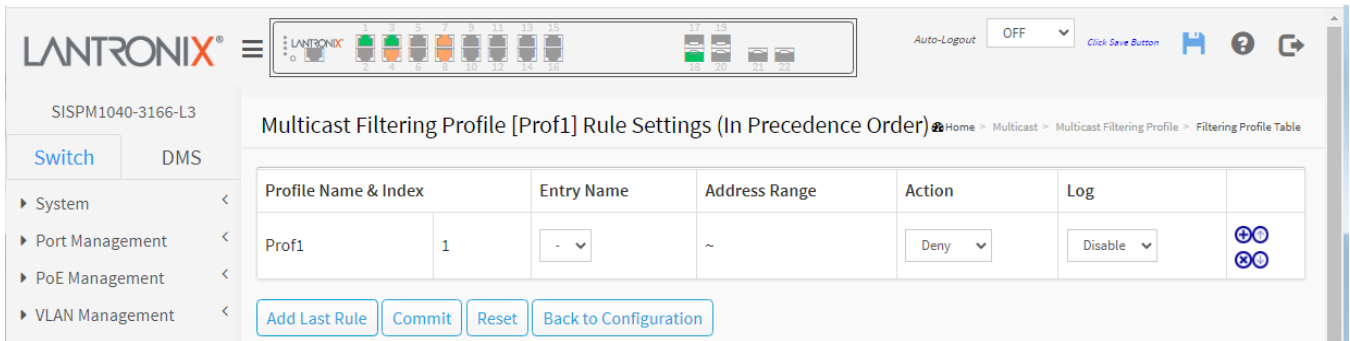
**Back to Configuration:** Go back to previous configuration page.

### Rule > Edit page

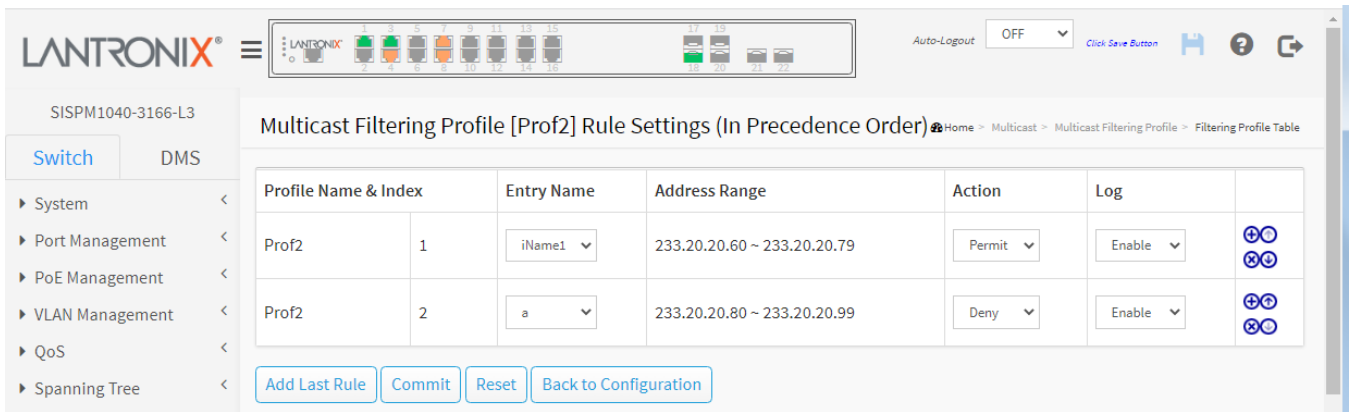
Click the Edit button to display the Multicast Filtering Profile [Prof2] Rule Settings (In Precedence Order) page:



Click the Add Last Rule button to edit the page.



### Example:



## Multicast Filtering Profile > Filtering Address Entry

This page provides address range settings used in IPMC profile.

The address entry is used to specify the address range that will be associated with IPMC Profile. You can create a maximum of 128 address entries per system.

The screenshot displays the 'Multicast Filtering Profile Address Configuration' page. At the top, there are navigation buttons: 'Refresh', 'First Entry', and 'Next Entry'. Below these, a text field indicates 'Navigate Address Entry Setting in IPMC Profile by 20 entries per page.' The main content is a table with the following structure:

Delete	Entry Name	Start Address	End Address
<input type="checkbox"/>	a	233.20.20.80	233.20.20.99
<input type="button" value="Delete"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>

Below the table, there is a button 'Add New Address (Range) Entry' and two buttons 'Apply' and 'Reset'.

**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 alphabetic and numeric characters. At least one alphabet 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 a new range of addresses. Specify the name and configure the addresses. Click the "Apply" button.

**Apply:** Click to save changes.

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

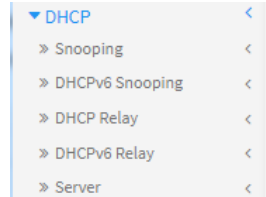
**Refresh:** Refreshes the displayed table starting from the input fields.

**First Entry:** Updates the table starting from the first entry in the IPMC Profile Address Configuration.

**Next Entry:** Updates the table, starting with the entry after the last entry currently displayed.

## DHCP

The Dynamic Host Configuration Protocol (DHCP) is a network management protocol used on Internet Protocol (IP) networks for automatically assigning IP addresses and other communication parameters to devices connected to the network using a client-server architecture. DHCP eliminates the need for individually configuring network devices manually, and consists of two network components, a centrally installed network DHCP server and client instances of the protocol stack on each computer or device. When connected to the network, and periodically thereafter, a client requests a set of parameters from the DHCP server using the [DHCP protocol](#).



### DHCP > Snooping > Snooping Configuration

Configure DHCP Snooping on this page. 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.

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

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

**on:** Enable DHCP snooping mode operation. When DHCP snooping mode operation is enabled, the DHCP request messages will be forwarded to trusted ports and only allow reply packets from trusted ports.

**off:** Disable DHCP snooping mode operation.

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

**Trusted:** Configures the port as trusted source of the DHCP messages. Trusted port can forward DHCP packets normally.

**Untrusted:** Configures the port as untrusted source of the DHCP messages. Untrusted port will discard the packets when it receive DHCP packets.

### Buttons

**Apply:** Click to save changes.

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

## DHCP > Snooping > 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.

Each page shows up to 99 entries from the Dynamic DHCP Snooping Table, default being 20, selected with the "entries per page" input field. When first visited, the webpage will show the first 20 entries from the beginning of the Dynamic DHCP snooping Table.

The "MAC Address" and "VLAN" input fields let you select the starting point in the Dynamic DHCP Snooping Table.

The screenshot shows the web interface for the Dynamic DHCP Snooping Table. At the top, there is a navigation bar with the Lantronix logo and a menu icon. Below the logo, the device model 'SISPM1040-3166-L3' is displayed. The main content area is titled 'Dynamic DHCP Snooping Table'. It features an 'Auto-refresh' toggle set to 'off', and three buttons: 'Refresh', 'First Page', and 'Next Page'. Below these buttons, there are input fields for 'Start from MAC address' (00-00-00-00-00-00), 'VLAN' (0), and 'entries per page' (20). A table with the following columns is shown: MAC Address, VLAN ID, Source Port, IP Address, IP Subnet Mask, and DHCP Server. The table currently contains the text 'No more entries'.

**MAC Address:** User MAC address of the entry.

**VLAN ID:** VLAN-ID in which 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.

**First Page:** Updates the table starting from the first entry in the Dynamic DHCP Snooping Table.

**Next Page:** Updates the table, starting with the entry after the last entry currently displayed.

## DHCP > Snooping > Detailed Statistics

This page displays statistics for DHCP snooping. Note that the normal forward per-port TX statistics are not increased if the incoming DHCP packet is done by the L3 forwarding mechanism. Also, clearing statistics on a specific port may not take effect on global statistics since it gathers statistics from a different layer.

The screenshot shows the Lantronix web interface for DHCP Detailed Statistics on Port 1. The interface includes a navigation menu on the left, a top status bar with LANTRONIX logo and port indicators, and a main content area with a table of statistics.

Navigation: Home > DHCP > Snooping > Detailed Statistics

Auto-refresh:  off   Combined

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		

### Receive and Transmit Packets

**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:** 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 coming from untrusted port.

### Buttons

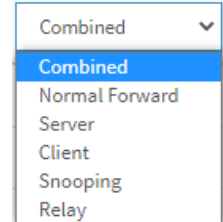
**DHCP user select box:** Select which user's information is displayed. The selections are Combined (default), Normal Forward, Server, Client, Snooping, and Relay.

**Port select box:** Select which port's information is displayed.

**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.



## DHCP > DHCPv6 > Snooping > Configuration

Configure DHCPv6 (DHCP over IPv6) Snooping on this page. 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.

The screenshot shows the Lantronix web interface for configuring DHCPv6 Snooping. The page title is "DHCPv6 Snooping Configuration". The breadcrumb trail is "Home > DHCP > DHCPv6 Snooping > Configuration".

**Switch Configuration:**

- Snooping Mode: Enabled
- Unknown IPv6 Next-Headers: Drop

**Port Configuration:**

Port	Trust Mode
*	<>
Gi 1/1	Untrusted
Gi 1/2	Untrusted
Gi 1/3	Untrusted
Gi 1/4	Untrusted
Gi 1/5	Untrusted
Gi 1/6	Untrusted

### Switch Configuration

**Snooping Mode:** Indicates the DHCPv6 snooping mode operation. Possible modes are:

**Enabled:** Enable DHCPv6 snooping mode operation. When DHCPv6 snooping mode operation is enabled, the DHCPv6 client request messages will be forwarded to trusted ports and only allow reply packets from trusted ports.

**Disabled:** Disable DHCP snooping mode operation.

**Unknown IPv6 Next-Headers:** Indicates how to treat Unknown IPv6 Next-Header values. The switch must parse all IPv6 packets to a DHCPv6 client to determine if it is in fact a DHCPv6 message. If an unknown IPv6 extension header is encountered the parsing cannot continue. See IETF [RFC 7610](#), section 5, item 3 for details. Possible options are:

**Drop:** Drop packets with unknown IPv6 extension headers. This is the most secure option but may result in traffic disruptions (default).

**Allow:** Allow packets with unknown IPv6 extension headers. This is a less secure option but prevents traffic disruptions.

**Port Configuration:** Indicates the DHCPv6 snooping port mode.

**Port:** Displays a row for each switch port in the format Gi 1/1, Gi 1/2, 10G 1/1, etc.



**Trust Mode:** Possible port Trust Modes are:

***Trusted:*** Configures the port as trusted source of the DHCPv6 messages.

***Untrusted:*** Configures the port as untrusted source of the DHCPv6 messages (default).

**Buttons:**

**Apply:** Click to save changes.

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

## DHCP > DHCPv6 > Snooping > Table

This page displays the content of the current DHCPv6 Snooping Table. This table displays the currently known DHCPv6 clients and their assigned addresses.

The screenshot shows the Lantronix web interface for the DHCPv6 Snooping Table. The page title is "DHCPv6 Snooping Table". The interface includes a navigation menu on the left with options like System, Port Management, PoE Management, VLAN Management, QoS, and Spanning Tree. The main content area shows an "Auto-refresh" toggle set to "off" and a "Refresh" button. Below this, it states "Total entries: 0" and displays an empty table with columns for Client DUID, MAC Address, Ingress Port, IAID, VLAN ID, Assigned Address, Lease Time, and DHCP Server Address.

Client DUID	MAC Address	Ingress Port	IAID	VLAN ID	Assigned Address	Lease Time	DHCP Server Address

**Client DUID:** The DHCP Unique Identifier (DUID) for the client. DHCPv6 uses this value to uniquely identify a client host instead of just using the MAC address of one of its interface ports (as DHCPv4 does).

**MAC Address:** The MAC address for the client interface port that sent the DHCPv6 message.

**Ingress Port:** The local port on the snooping switch where client messages are received.

**IAID:** Each client may contain multiple interfaces and may request addresses for each of these in the same DHCPv6 message. The Identity Association ID (IAID) value uniquely identifies the interface in the scope of the client.

**VLAN ID:** The VLAN ID which is used by the client messages.

**Assigned Address:** The address assigned to the interface identified by the IAID value.

**Lease Time:** The lease time associated with the assigned address in seconds.

**DHCP Server Address:** The IPv6 address of the DHCP server which assigned the address to the client.

### Buttons:

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

**Refresh:** Click to manually refresh the page immediately.

## DHCP > DHCPv6 Snooping > Detailed Statistics

This page displays statistics for DHCPv6 snooping. Select the desired port to display at the Selected port dropdown.

The screenshot shows the Lantronix web interface for DHCPv6 Snooping Statistics. The selected port is Gi 1/1, and the Auto-refresh toggle is off. The statistics table is as follows:

Receive Packets		Transmit Packets	
Rx Solicit	0	Tx Solicit	0
Rx Request	0	Tx Request	0
Rx InfoRequest	0	Tx InfoRequest	0
Rx Confirm	0	Tx Confirm	0
Rx Renew	0	Tx Renew	0
Rx Rebind	0	Tx Rebind	0
Rx Decline	0	Tx Decline	0
Rx Advertise	0	Tx Advertise	0
Rx Reply	0	Tx Reply	0
Rx Reconfigure	0	Tx Reconfigure	0
Rx Release	0	Tx Release	0
Rx DiscardUntrust	0		

### General Receive and Transmit Packets

The page contains both RX and TX counters for all known DHCPv6 message types. Please refer to IETF RFC 3315 for details on the various DHCPv6 message types.

### Untrusted Discards

Rx DiscardUntrust : Counter indicates the number of received DHCP server packets that have been discarded due to the port being untrusted.

### Buttons

**Selected port:**  : The port select box lets you select the port for which you want to view statistics.

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

**Refresh:** Click to refresh the page immediately.

**Clear:** Clears the counters for the selected port.

## DHCP Relay

DHCP Relay is used to forward and to transfer DHCP messages between the clients and the server when they are not on the same subnet domain.

The DHCP option 82 enables a DHCP relay agent to insert specific information into a DHCP request packets when forwarding client DHCP packets to a DHCP server and remove the specific information from a DHCP reply packets when forwarding server DHCP packets to a DHCP client. The DHCP server can use this information to implement IP address or other assignment policies. Specifically, the option works by setting two sub-options: Circuit ID (option 1) and Remote ID (option2). The Circuit ID sub-option is supposed to include information specific to which circuit the request came in on. The Remote ID sub-option was designed to carry information relating to the remote host end of the circuit.

The Circuit ID is 4 bytes long and the format is "vlan\_id" "module\_id" "port\_no". The parameter of "vlan\_id" is the first two bytes represent the VLAN ID. The parameter of "module\_id" is the third byte for the module ID (in standalone switch it always equals 0, in stackable switch it means switch ID). The parameter of "port\_no" is the fourth byte and it means the port number.

The Remote ID is 6 bytes in length, and the value is equal the DHCP relay agents MAC address.

## DHCP Relay Configuration

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

The screenshot shows the Lantronix web interface for DHCP Relay Configuration. The top navigation bar includes the Lantronix logo, a menu icon, and a status bar with "SISPM1040-3166-L3", "Auto-Logout OFF", and "Click Save Button". The left sidebar contains a navigation menu with "Switch" and "DMS" tabs, and a list of system management options. The main content area is titled "DHCP Relay Configuration" and contains the following settings:

Relay Mode	<input type="checkbox"/> off
Relay Server	<input type="text" value="0.0.0.0"/>
Relay Information Mode	Disabled
Relay Information Policy	Keep

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

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

- on:** Enable DHCP relay mode operation. When DHCP relay mode operation is enabled, the agent forwards and transfers DHCP messages between the clients and the server when they are not in the same subnet domain. And the DHCP broadcast message won't be flooded for security considerations.
- off:** Disable DHCP relay mode operation.

**Relay Server:** Enter the DHCP relay server IP address.

**Relay Information Mode:** Select the DHCP relay information mode option operation. The option 82 circuit ID format as "[vlan\_id][module\_id][port\_no]". The first four characters represent the VLAN ID, the fifth and sixth

characters are the module ID(in standalone device it always equal 0, in stackable device it means switch ID), and the last two characters are the port number. For example, "00030108" means the DHCP message receive form VLAN ID 3, switch ID 1, port No 8. And the option 82 remote ID value is equal the switch MAC address.

Possible Relay Information modes are:

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

**Disabled:** Disable DHCP relay information mode operation.

**Relay Information Policy:** Indicates the DHCP relay information option policy. When DHCP relay information mode operation is enabled, if the agent receives a DHCP message that already contains relay agent information it will enforce the policy. 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?*

## DHCP Relay Statistics

This page displays statistics for DHCP relay.

The screenshot shows the Lantronix web interface for device SISPM1040-3166-L3. The page title is 'DHCP Relay Statistics'. The interface includes a navigation menu on the left with categories like System, Port Management, PoE Management, VLAN Management, QoS, Spanning Tree, MAC Address Tables, Multicast, DHCP (highlighted), Security, Access Control, SNMP, CFM, APS, ERPS, and Rapid Ring. The DHCP section is expanded to show Configuration and Statistics. The main content area has an 'Auto-refresh' toggle set to 'off' and buttons for 'Refresh' and 'Clear'. Below this are two tables: 'Server Statistics' and 'Client Statistics'.

Server Statistics	
Transmit to Server	0
Transmit Error	1
Receive from Server	0
Receive Missing Agent Option	0
Receive Missing Circuit ID	0
Receive Missing Remote ID	0
Receive Bad Circuit ID	0
Receive Bad Remote ID	0

Client Statistics	
Transmit to Client	0
Transmit Error	0
Receive from Client	1
Receive Agent Option	0
Replace Agent Option	0
Keep Agent Option	0
Drop Agent Option	0

### Server Statistics

**Transmit to Server:** The number of packets that are relayed from client to server.

**Transmit Error:** The number of packets that resulted in errors while being sent to clients.

**Receive from Server:** The number of packets received from server.

**Receive Missing Agent Option:** The number of packets received without agent information options.

**Receive Missing Circuit ID:** The number of packets received with the Circuit ID option missing.

**Receive Missing Remote ID:** The number of packets received with the Remote ID option missing.

**Receive Bad Circuit ID:** The number of packets whose Circuit ID option did not match known circuit ID.

**Receive Bad Remote ID:** The number of packets whose Remote ID option did not match known Remote ID.

**Client Statistics**

**Transmit to Client:** The number of relayed packets from server to client.

**Transmit Error:** The number of packets that resulted in error while being sent to servers.

**Receive from Client:** The number of received packets from server.

**Receive Agent Option:** The number of received packets with relay agent information option.

**Replace Agent Option:** The number of packets which were replaced with relay agent information option.

**Keep Agent Option:** The number of packets whose relay agent information was retained.

**Drop Agent Option:** The number of packets that were dropped which were received with relay agent information.

**Buttons**

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

**Refresh:** Click to refresh the page immediately.

**Clear:** Clear all statistics.

## DHCP > DHCPv6 Relay > Configuration

This page lets you configure DHCPv6 Relay for a specified VLAN.

The screenshot shows the Lantronix web interface for DHCPv6 Relay Configuration. The interface includes a navigation menu on the left with options like System, Port Management, PoE Management, VLAN Management, QoS, and Spanning Tree. The main content area displays a table with columns for Delete, Interface, Relay Interface, and Relay Destination. Below the table are buttons for 'Add New Entry', 'Apply', and 'Reset'.

Delete	Interface	Relay Interface	Relay Destination
<input type="checkbox"/>	VLAN 1	VLAN 2	ff05::1:4

**Interface:** Displays the interface identification.

**Relay Interface:** The identification of the interface used for relaying.

**Relay Destination:** Enter an Ipv6 address represented as human readable text as specified in IETF [RFC 5952](#). This is the IPv6 address of the DHCPv6 server that requests will be relayed to. The default value 'ff05::1:3' means 'any DHCP server'.

### Buttons

**Add New Entry:** Click to add a new entry to the table.

**Apply:** Click to save changes.

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



## DHCP > DHCPv6 Relay > Status

This page shows currently configured relay agents' status and statistics.

**Dropped server packets with interface option missing:** The number of DHCPv6 Relay server packets with no interface option.

**Interface:** Interface identification. The ID of the interface that receives client requests.

**Relay Interface:** Interface identification. The ID of the interface used for relaying.

**Relay Address:** An Ipv6 address represented as human readable text as specified in RFC5952. The IPv6 address that requests will be relayed to. The default value 'ff05::1:3' means 'any DHCPv6 server'.

**Tx to server:** Integer number. Number of packets relayed to server.

**Rx from server:** Integer number. Number of packets received from server.

**Server pkts dropped:** Integer number. Number of packets from server that relay agent drops.

**Tx to client:** Integer number. Number of packets sent to client.

**Rx from client:** Integer number. Number of packets received from client.

**Client pkts dropped:** Integer number. Number of packets from client that relay agent drops.

**Clear stats:** Resets all statistics counters of relevant entry to zero.

### Buttons

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

**Refresh:** Click to refresh the page immediately.

**Clear all statistic:** Resets all statistics counters to zero.

## DHCP > Server > Configuration

This page lets you enable or disable DHCP server per system and per VLAN and configure Start IP and End IP addresses. A DHCP server will allocate these IP addresses to the DHCP client and deliver configuration parameters to DHCP client.

SISPM1040-3166-L3

LANTRONIX

Auto-Logout OFF

Click Save Button

Home > DHCP > Server > Configuration

Switch DMS

System <  
Port Management <  
PoE Management <  
VLAN Management <  
QoS <  
Spanning Tree <

### DHCP Server Configuration

Interfaces

VLAN	Mode	Start IP	End IP	Lease Time	Subnet Mask	Default Router	DNS Server
1	<input type="radio"/> on <input checked="" type="radio"/> off	0.0.0.0	0.0.0.0	86400	0.0.0.0	0.0.0.0	0.0.0.0

Apply Reset

**VLAN:** Configure the VLAN in which DHCP server is enabled or disabled. Allowed VLANs which are created in IP interfaces.

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

**on:** Enable DHCP server per VLAN.

**off:** Disable DHCP server per VLAN (default).

**Start IP and End IP:** Define the IP range. The Start IP must be smaller than or equal to the End IP.

**Lease Time:** The lease time in second. The default value is one day.

**Subnet Mask:** Configure subnet mask of the DHCP address.

**Default Router:** Configure the destination IP network or host address of the default route.

**DNS Server:** Configure the default DNS server.

### Buttons

**Apply:** Click to save changes.

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

## DHCP > Server > Status

This page displays DHCP server status.

The screenshot shows the Lantronix web interface for the DHCP Server Status page. The page title is "DHCP Server Status" and the breadcrumb is "Home > DHCP > Server > Status". The interface includes a navigation menu on the left with options like System, Port Management, PoE Management, VLAN Management, QoS, Spanning Tree, MAC Address Tables, Multicast, and DHCP. The main content area has an "Auto-refresh" toggle set to "off" and a "Refresh" button. Below this are two sections: "Interfaces" and "IP Binding Status".

VLAN	Type	Start IP	End IP	Lease Time	Subnet Mask	Default Router	DNS Server
No entries							

IP	VLAN	State	MAC	Expiration
No binding data				

### Interfaces

**VLAN:** Displays the VLAN ID of the entry.

**Type:** Displays the server type:

**Network:** to service more than one DHCP client.

**Host:** for a specific DHCP client identified by client identifier or hardware address.

**Start IP** and **End IP:** Displays the starting IP address and the ending IP address.

**Lease Time:** Displays the configured lease time.

**Subnet Mask:** Displays the configured subnet mask of the DHCP address.

**Default Router:** Displays the destination IP network or host address of this route.

**DNS Server:** Displays the configured DNS server IP address.

### IP Binding Status

**IP:** The leased IP address.

**VLAN:** The VLAN ID of the entry.

**State:** The current state of the IP address.

**MAC:** The hardware address of the device.

**Expiration:** The lease time left before it expires.

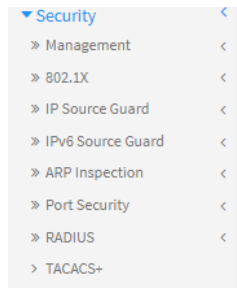
### **Buttons**

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

**Refresh:** Click to refresh the page immediately.

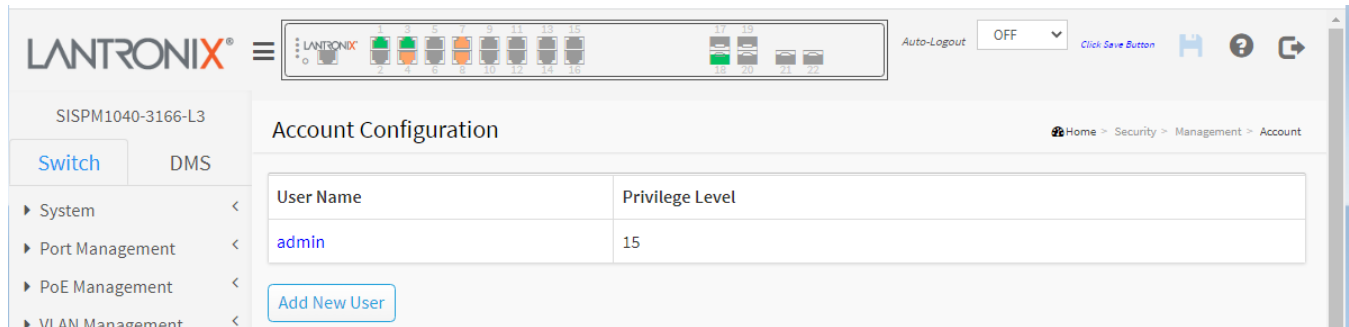
## Security

This section provides security in terms of management, 802.1X, IP Source Guard, IPv6 Source Guard, ARP inspection, Port security, RADIUS, and TACACS+.



### Security > Management > Account

This page displays an overview of current accounts, and lets you add new, and edit and delete existing users.



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

**Privilege Level:** The privilege level of the account. The allowed range is 0-15. If the privilege level value is 15, it can access all groups, i.e., that is granted the fully control of the device. But other values need to refer to each group privilege level. User's privilege should be same or greater than the group privilege level to have the access of that group. By default, most groups privilege level 5 has read-only access and privilege level 10 has read-write access. And the 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 a new user. The maximum numbers of users is 20.

## Add New User

This page lets you configure a new user account.

The screenshot shows the 'Add Account' configuration page. The 'Account Settings' section includes the following fields:

User Name	<input type="text"/>
Password	<input type="password"/>
Password (again)	<input type="password"/>
Privilege Level	0 ▼

Buttons: Apply, Reset, Cancel

**User Name:** A string identifying the user name that this entry should belong to. The allowed string length is 1 to 31 characters. A valid user name allows letters, numbers, and underscores.

**Password:** Enter the password for the user. The allowed string length is 0–31 characters. Any printable characters, including the space character, are accepted.

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

**Privilege Level:** The privilege level of the user. The allowed range is 0-15. If the privilege level value is 15, it can access all groups (i.e., granted full control of the device). But others value need to refer to each group privilege level. User's privilege should be same or greater than the group privilege level to have the access of that group. By default setting, most groups privilege level 5 has the read-only access and privilege level 10 has the read-write access. System maintenance (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

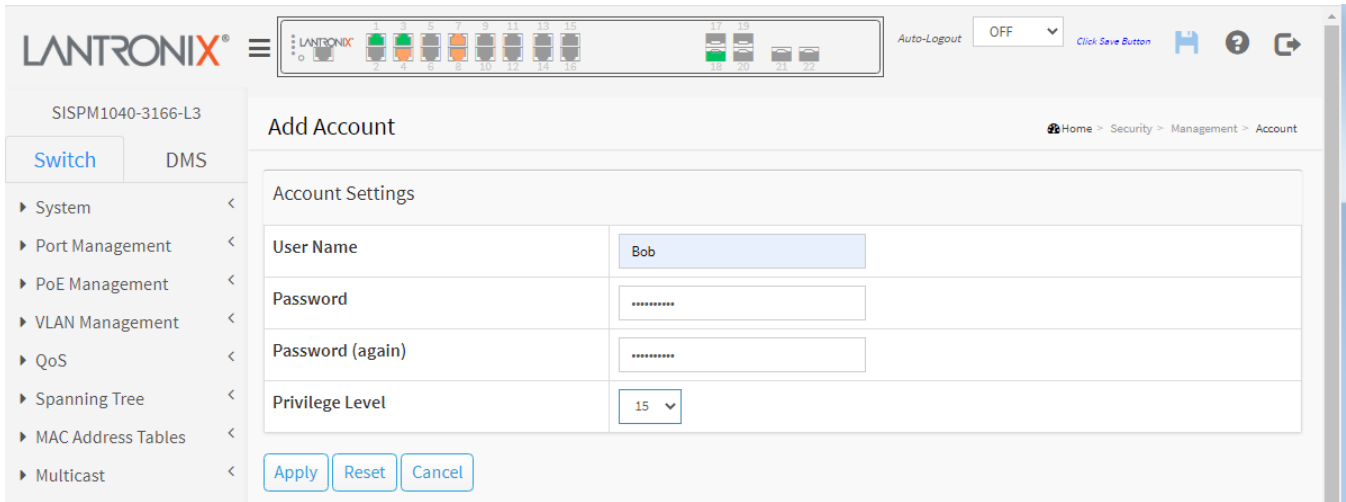
**Apply:** Click to save changes.

**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.

### Edit a User

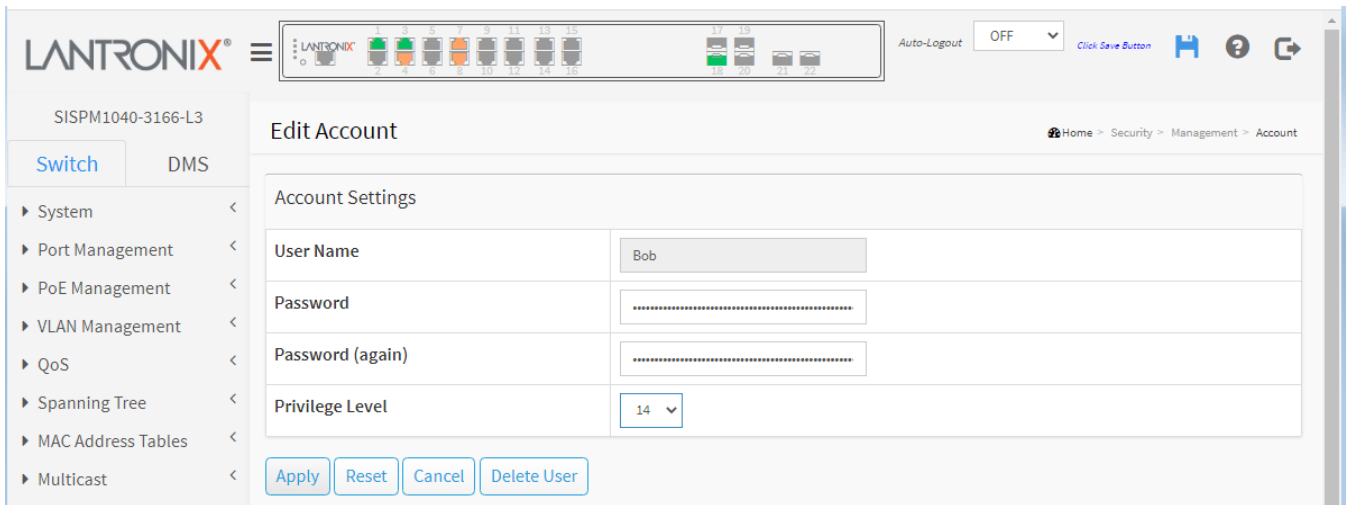
On the Account Configuration page click the linked User Name to display the Edit Account page:



1. Edit the Password and/or Privilege Level as desired.
2. Click the Apply button.
3. The Account Configuration page displays again with the edited user information.

### Delete a User

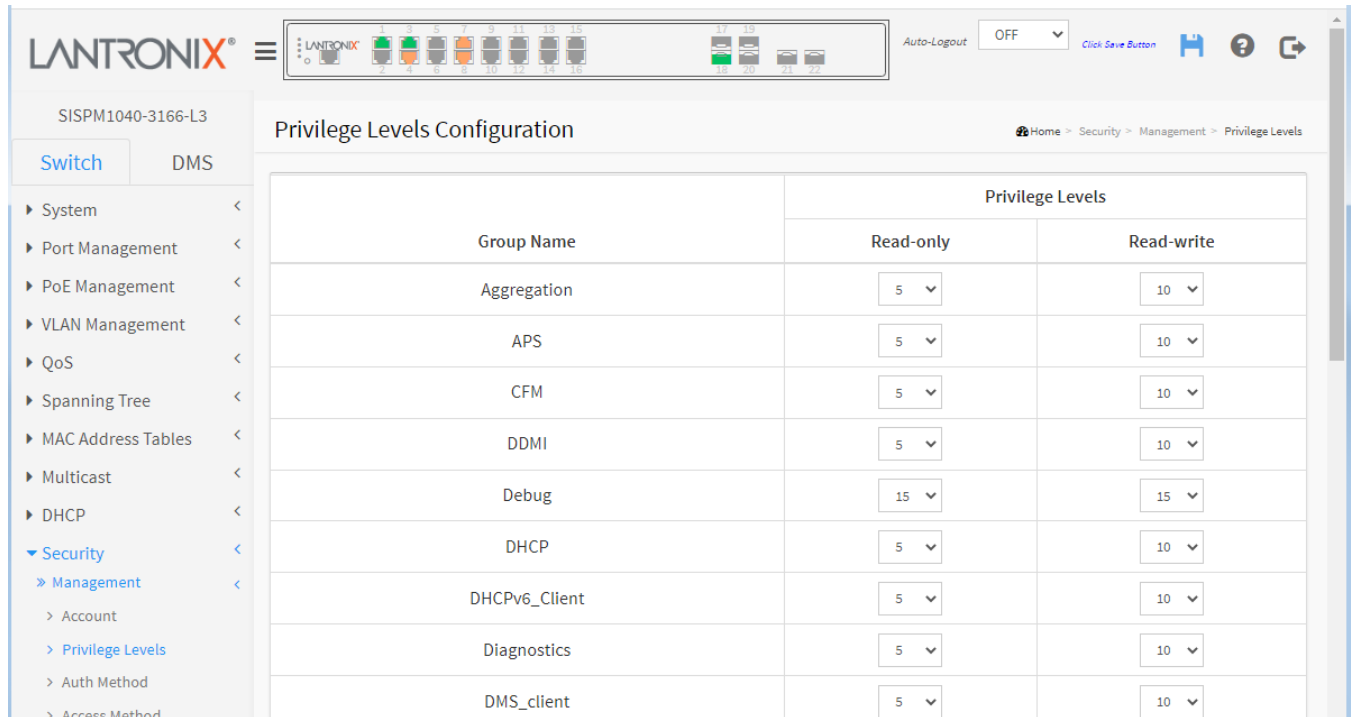
On the Account Configuration page click the linked User Name to display the Edit Account page:



1. Verify the user that you want to delete, then click the **Delete User** button to delete the user.
2. At the “Delete User” confirmation prompt click OK.
3. The Account Configuration page displays again with the user deleted.

## Security > Management > Privilege Levels

This page lets you view and set privilege levels on a per group basis.



The screenshot shows the 'Privilege Levels Configuration' page in the Lantronix web interface. The page title is 'SISPM1040-3166-L3'. The breadcrumb navigation is 'Home > Security > Management > Privilege Levels'. The page contains a table with the following data:

Group Name	Privilege Levels	
	Read-only	Read-write
Aggregation	5	10
APS	5	10
CFM	5	10
DDMI	5	10
Debug	15	15
DHCP	5	10
DHCPv6_Client	5	10
Diagnostics	5	10
DMS_client	5	10

**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, and IP source guard.

**IP:** Everything except 'ping'.

**Port:** Everything except 'Cable Diagnostics'.

**Diagnostics:** 'ping' and 'Cable Diagnostics'.

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

**Debug:** Only present in CLI.

**Privilege Levels:** The Privilege Levels can be configured between 0 to 15 (where 0 is the lowest level and 15 is the highest level) Every group has an authorization Privilege level for the following sub groups: read-only, read-write. User Privilege should be same or greater than the authorization Privilege level to have access to that function.

### Buttons

**Apply:** Click to save changes.

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

## Security > Management > Auth Method

This page lets you configure authentication, authorization, and accounting methods used when logging into the switch via one of the management client interfaces. The table has one row for each client type and several columns.

**Authentication Method Configuration**

Home > Security > Management > Auth Method

**Authentication Method**

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

**Command Authorization Method**

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

**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

### Authentication Method

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

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

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

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

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

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

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



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

**Service Port:** The network port number this client bound to provide service.

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

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

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

**no:** Command authorization 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 0-15.

**Cfg Cmd:** Also authorize configuration commands.

**Accounting Method** : This section allows you to configure command and exec (login) accounting.

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

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

**no:** Accounting is disabled.

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

**Cmd Lvl:** Enable accounting of all commands with a privilege level higher than or equal to this level. Valid values are in the range 0 to 15. Leave the field empty to disable command accounting.

**Exec:** Enable exec (login) accounting.

## Buttons

**Apply:** Click to save changes.

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

## Security > Management > Access Method

Configure access management table on this page. 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.

The screenshot shows the 'Access Method Configuration' page in the Lantronix web interface. The page title is 'SISPM1040-3166-L3'. The left sidebar shows a navigation menu with 'Switch' selected and 'DMS' as an alternative. The main content area has a 'Mode' toggle set to 'on'. Below this is a table with columns: Delete, VLAN ID, Start IP Address, End IP Address, HTTP/HTTPS, SNMP, and TELNET/SSH. There is one entry with VLAN ID 1, Start IP Address 0.0.0.0, and End IP Address 0.0.0.0. Below the table are buttons for 'Add New Entry', 'Apply', and 'Reset'. The top right of the interface shows 'Auto-Logout' set to 'OFF' and a 'Click Save Button' link.

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

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

**on:** Enable access management mode operation.

**off:** Disable access management mode operation.

**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 unicast address for the access management entry.

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

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

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

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

### Buttons

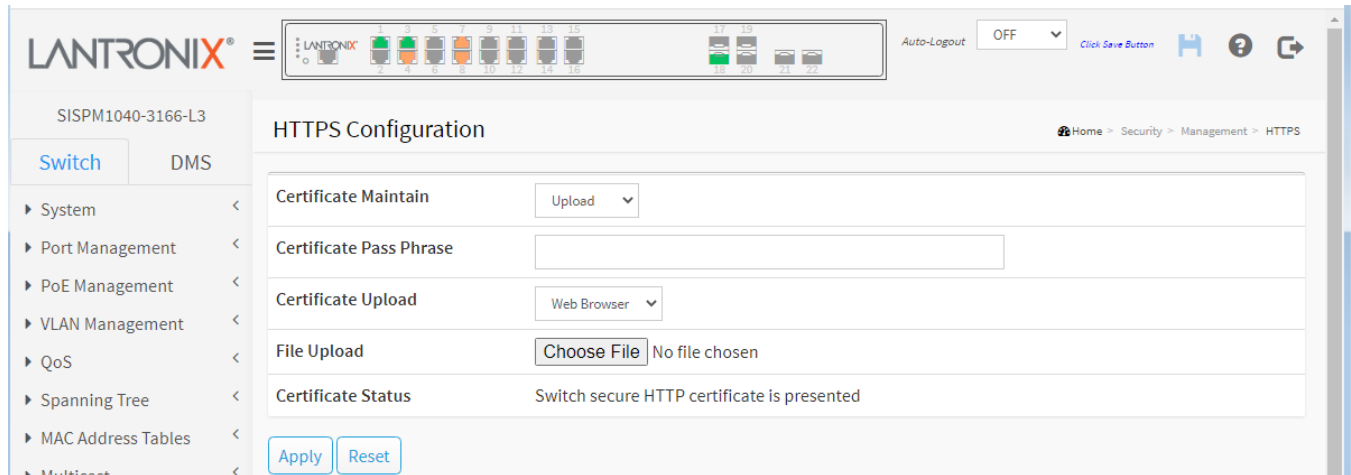
**Add New Entry:** Click to add a new access management entry.

**Apply:** Click to save changes.

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

## Security > Management > HTTPS

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



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

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

**Generate:** Generate a new self-signed RSA certificate.

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

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

**Note** that the RSA certificate is recommended since most new browser versions have removed support for DSA in certificate, e.g., Firefox v37 and Chrome v39.

Possible methods are:

**Web Browser:** Upload a certificate via Web browser.

**URL:** Upload a certificate via URL, the supported protocols are HTTP, HTTPS, TFTP and FTP. The URL format is `<protocol>://[<username>[:<password>]@]< host>[:<port>][/<path>]/<file_name>`. For example, `tftp://10.10.10.10/new_image_path/new_image.dat`, `http://username:password@10.10.10.10:80/new_image_path/new_image.dat`. A valid file name is a text string drawn from alphabet (A-Za-z), digits (0-9), dot (.), hyphen (-), under score(\_). The maximum length is 63 and hyphen must not be first character. The file name content that only contains '.' is not allowed.

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

*Switch secure HTTP certificate is presented.*

*Switch secure HTTP certificate is not presented.*

*Switch secure HTTP certificate is generating ....*

### Buttons

**Apply:** Click to save changes.

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

## Security > 802.1X > Configuration

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

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

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

The 802.1X configuration consists of two sections, system and port.

**802.1X Configuration**

System Configuration

Mode	<input type="checkbox"/> off
Reauthentication Enabled	<input type="checkbox"/>
Reauthentication Period	3600 seconds
EAPOL Timeout	30 seconds
Aging Period	300 seconds
Hold Time	10 seconds
RADIUS-Assigned QoS Enabled	<input type="checkbox"/>
RADIUS-Assigned VLAN Enabled	<input type="checkbox"/>
Guest VLAN Enabled	<input type="checkbox"/>
Guest VLAN ID	1
Max. Reauth. Count	2
Allow Guest VLAN if EAPOL Seen	<input type="checkbox"/>

Port Configuration

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

## **System Configuration**

**Mode:** Indicates if 802.1X is globally enabled (**on**) or disabled (**off**) for the switch. If globally disabled, all ports are allowed forwarding of frames.

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

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

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

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

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

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

When the 802.1X module uses the Port Security module to secure MAC addresses, the Port Security module needs to check for activity on the MAC address in question at regular intervals and free resources if no activity is seen within a given period of time. This parameter controls exactly this period and can be set to a number between 10 and 1000000 seconds.

If reauthentication is enabled and the port is in an 802.1X-based mode, this is not so critical, since supplicants that are no longer attached to the port will get removed upon the next reauthentication, which will fail. But if reauthentication is not enabled, the only way to free resources is by aging the entries.

For ports in MAC-based Auth. mode, reauthentication doesn't cause direct communication between the switch and the client, so this will not detect whether the client is still attached or not, and the only way to free any resources is to age the entry.

**Hold Time:** This setting applies to the following modes, i.e. modes using the Port Security 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 "Security > RADIUS > Configuration" page) the client is put on hold in the Unauthorized state. The hold timer does not count during an on-going authentication.

In MAC-based Auth. mode, the switch will ignore new frames coming from the client during the hold time.

The Hold Time can be set to 10- 1000000 seconds.

**RADIUS-Assigned QoS Enabled:** RADIUS-assigned QoS provides a means to centrally control the traffic class to which traffic coming from a successfully authenticated supplicant is assigned on the switch. The RADIUS server must be configured to transmit special RADIUS attributes to take advantage of this feature (see RADIUS-Assigned QoS Enabled below for a detailed description).

The "RADIUS-Assigned QoS Enabled" checkbox provides a quick way to globally enable/disable RADIUS-server assigned QoS Class functionality. When checked, the individual ports' ditto setting determines whether RADIUS-assigned QoS Class is enabled on that port. When unchecked, RADIUS-server assigned QoS Class is disabled on all ports.

**RADIUS-Assigned VLAN Enabled:** RADIUS-assigned VLAN provides a means to centrally control the VLAN on which a successfully authenticated supplicant is placed on the switch. Incoming traffic will be classified to and switched on the RADIUS-assigned VLAN. The RADIUS server must be configured to transmit special RADIUS attributes to take advantage of this feature (see RADIUS-Assigned VLAN Enabled below for a detailed description).

The "RADIUS-Assigned VLAN Enabled" checkbox provides a quick way to globally enable/disable RADIUS-server assigned VLAN functionality. When checked, the individual ports' ditto setting determines whether RADIUS-assigned VLAN is enabled on that port. When unchecked, RADIUS-server assigned VLAN is disabled on all ports.

**Guest VLAN Enabled:** A Guest VLAN is a special VLAN - typically with limited network access - on which 802.1X-unaware clients are placed after a network administrator-defined timeout. The switch follows a set of rules for entering and leaving the Guest VLAN as listed below.

The "Guest VLAN Enabled" checkbox provides a quick way to globally enable/disable Guest VLAN functionality. When checked, the individual ports' ditto setting determines whether the port can be moved into Guest VLAN. When unchecked, the ability to move to the Guest VLAN is disabled on all ports.

**Guest VLAN ID:** This is the value that a port's Port VLAN ID is set to if a port is moved into the Guest VLAN. It is only changeable if the Guest VLAN option is globally enabled. Valid values are in the range [1; 4095].

**Max. Reauth. Count:** The number of times the switch transmits an EAPOL Request Identity frame without response before considering entering the Guest VLAN is adjusted with this setting. The value can only be changed if the Guest VLAN option is globally enabled. Valid values are in the range [1; 255].

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

The value can only be changed if the Guest VLAN option is globally enabled.

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

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

**Admin State:** If 802.1X is globally enabled, this selection controls the port's authentication mode. The following 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 RADIUS configuration page) and suppose that the first server in the list is currently down (but not considered dead). Now, if the supplicant retransmits EAPOL Start frames at a rate faster than X seconds, then it will never get authenticated, because the switch will cancel on-going backend authentication server requests whenever it receives a new EAPOL Start frame from the supplicant. And since the server hasn't yet failed (because the X seconds haven't expired), the same server will be contacted upon the next backend authentication server request from the switch. This scenario will loop forever. Therefore, the server timeout should be smaller than the supplicant's EAPOL Start frame retransmission rate.

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

Single 802.1X is really not an IEEE standard, but features many of the same characteristics as does port-based 802.1X. In Single 802.1X, at most one supplicant can get authenticated on the port at a time. Normal EAPOL frames are used in the communication between the supplicant and the switch. If more than one supplicant is connected to a port, the one that comes first when the port's link comes up will be the first one considered. If that supplicant doesn't provide valid credentials within a certain amount of time, another supplicant will get a chance. Once a supplicant is successfully authenticated, only that supplicant will be allowed access. This is the most secure of all the supported modes. In this mode, the Port Security module is used to secure a supplicant's MAC address once successfully authenticated.

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

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

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

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

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

The advantage of MAC-based authentication over 802.1X-based authentication is that the clients don't need special supplicant software to authenticate. The disadvantage is that MAC addresses can be spoofed by malicious users - equipment whose MAC address is a valid RADIUS user can be used by anyone. Also, only the MD5-Challenge method is supported. The maximum number of clients that can be attached to a port can be limited using the Port Security Limit Control functionality.



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

This option is only available for single-client modes, i.e.

- Port-based 802.1X
- Single 802.1X

**RADIUS attributes used in identifying a QoS Class:** The User-Priority-Table attribute defined in RFC4675 forms the basis for identifying the QoS Class in an Access-Accept packet.

Only the first occurrence of the attribute in the packet will be considered, and to be valid, it must follow this rule:

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

**RADIUS-Assigned VLAN Enabled:** When RADIUS-Assigned VLAN is both globally enabled and enabled (checked) for a given port, the switch reacts to VLAN ID information carried in the RADIUS Access-Accept packet transmitted by the RADIUS server when a supplicant is successfully authenticated. If present and valid, the port's Port VLAN ID will be changed to this VLAN ID, the port will be set to be a member of that VLAN ID, and the port will be forced into VLAN unaware mode. Once assigned, all traffic arriving on the port will be classified and switched on the RADIUS-assigned VLAN ID.

If (re-)authentication fails or the RADIUS Access-Accept packet no longer carries a VLAN ID or it's invalid, or the supplicant is otherwise no longer present on the port, the port's VLAN ID is immediately reverted to the original VLAN ID (which may be changed by the administrator in the meanwhile without affecting the RADIUS-assigned).

This option is only available for single-client modes, i.e.

- Port-based 802.1X
- Single 802.1X

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

**RADIUS attributes used in identifying a VLAN ID:** RFC2868 and RFC3580 form the basis for the attributes used in identifying a VLAN ID in an Access-Accept packet. The following criteria are used:

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

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

This option is only available for EAPOL-based modes, i.e.:

- Port-based 802.1X
- Single 802.1X
- Multi 802.1X

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



**Guest VLAN Operation:** When a Guest VLAN enabled port's link comes up, the switch starts transmitting EAPOL Request Identity frames. If the number of transmissions of such frames exceeds Max. Reauth. Count and no EAPOL frames have been received in the meanwhile, the switch considers entering the Guest VLAN. The interval between transmission of EAPOL Request Identity frames is configured with EAPOL Timeout. If Allow Guest VLAN if EAPOL Seen is enabled, the port will now be placed in the Guest VLAN. If disabled, the switch will first check its history to see if an EAPOL frame has previously been received on the port (this history is cleared if the port link goes down or the port's Admin State is changed), and if not, the port will be placed in the Guest VLAN. Otherwise it will not move to the Guest VLAN, but continue transmitting EAPOL Request Identity frames at the rate given by EAPOL Timeout.

Once in the Guest VLAN, the port is considered authenticated, and all attached clients on the port are allowed access on this VLAN. The switch will not transmit an EAPOL Success frame when entering the Guest VLAN.

While in the Guest VLAN, the switch monitors the link for EAPOL frames, and if one such frame is received, the switch immediately takes the port out of the Guest VLAN and starts authenticating the supplicant according to the port mode. If an EAPOL frame is received, the port will never be able to go back into the Guest VLAN if the "Allow Guest VLAN if EAPOL Seen" is disabled.

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

**Globally Disabled:** 802.1X is globally disabled.

**Link Down:** 802.1X is globally enabled, but there is no link on the port.

**Authorized:** The port is in Force Authorized or a single-supplicant mode and the supplicant is authorized.

**Unauthorized:** The port is in Force Unauthorized or a single-supplicant mode and the supplicant is not successfully authorized by the RADIUS server.

**X Auth/Y Unauth:** The port is in a multi-supplicant mode. Currently X clients are authorized and Y are unauthorized.

**Restart:** Two buttons are available for each row. The buttons are only enabled when authentication is globally enabled and the port's Admin State is in an EAPOL-based or MAC-based mode. **Note:** Clicking these buttons will not cause settings changed on the page to take effect.

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

**Reinitialize:** Forces a reinitialization of the clients on the port and thereby a reauthentication immediately. The clients will transfer to the unauthorized state while the reauthentication is in progress.

## Buttons

**Refresh:** Click to refresh the page.

**Apply:** Click to save changes.

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

## Messages:

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

Click the Previous button to resolve.

## Security > 802.1X > Status

This page provides an overview of the current 802.1X port states.

The screenshot shows the Lantronix web interface for a switch (SISPM1040-3166-L3). The left sidebar contains a navigation menu with categories like System, Port Management, PoE Management, VLAN Management, QoS, Spanning Tree, MAC Address Tables, Multicast, DHCP, Security, and IP Source Guard. The main content area is titled '802.1X Status' and includes an 'Auto-refresh' toggle (currently off) and a 'Refresh' button. Below this is a table with the following data:

Port	Admin State	Port State	Last Source	Last ID	QoS Class	Port VLAN ID
1	Force Authorized	Authorized			-	
2	Force Authorized	Link Down			-	
3	Force Authorized	Authorized			-	
4	Force Authorized	Authorized			-	
5	Force Authorized	Link Down			-	
6	Force Authorized	Link Down			-	
7	Force Authorized	Authorized			-	
8	Force Authorized	Authorized			-	
9	Force Authorized	Link Down			-	
10	Force Authorized	Link Down			-	
11	Force Authorized	Link Down			-	

**Port:** The switch port number. Click to navigate to detailed 802.1X statistics for this port (see below).

**Admin State:** The port's current administrative state. Refer to 802.1X Admin State above for a description of possible values.

**Port State:** The current state of the port. Refer to 802.1X Port State above for a description of the individual states.

**Last Source:** The source MAC address carried in the most recently received EAPOL frame for EAPOL-based authentication, and the most recently received frame from a new client for MAC-based authentication.

**Last ID:** The user name (supplicant identity) carried in the most recently received Response Identity EAPOL frame for EAPOL-based authentication, and the source MAC address from the most recently received frame from a new client for MAC-based authentication.

**QoS Class:** QoS Class assigned to the port by the RADIUS server if enabled.

**Port VLAN ID:** The VLAN ID that 802.1X has put the port in. The field is blank if the Port VLAN ID is not overridden by 802.1X.

If the VLAN ID is assigned by the RADIUS server, "(RADIUS-assigned)" is appended to the VLAN ID.

If the port is moved to the Guest VLAN, "(Guest)" is appended to the VLAN ID.

### Buttons

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

**Refresh:** Click to refresh the page immediately.

## 802.1X Port Status page

Click a linked port # in the Port column of the 802.1X Status page to display the port's Status page.

This page provides detailed 802.1X statistics for a specific switch port running EAPOL-based IEEE 802.1X authentication. For MAC-based ports, it shows only selected backend server (RADIUS Authentication Server) statistics.

Use the port select box to select which port details to be displayed.

The screenshot shows the Lantronix web interface for device SISPM1040-3166-L3. The page title is "802.1X Port Status Port 1". The interface includes a navigation sidebar on the left with categories like System, Port Management, PoE Management, VLAN Management, QoS, Spanning Tree, MAC Address Tables, Multicast, DHCP, Security, and RADIUS. The main content area features an "Auto-refresh" toggle set to "off", "Refresh" and "Clear All" buttons, and a "Port 1" dropdown menu. Below these are two tables: "Port State" and "Port Counters".

Port State	
Admin State	Force Authorized
Port State	Authorized

Port Counters			
Receive EAPOL Counters		Transmit EAPOL Counters	
Total	0	Total	1
Response ID	0	Request ID	0
Responses	0	Requests	0
Start	0		
Logoff	0		
Invalid Type	0		
Invalid Length	0		

### Port State

**Admin State:** The port's current administrative state. Refer to 802.1X Admin State for a description of possible values.

**Port State:** The current state of the port. Refer to 802.1X Port State above for a description of the individual states.

**QoS Class:** The QoS class assigned by the RADIUS server. The field is blank if no QoS class is assigned.

**Port VLAN ID:** The VLAN ID that 802.1X has put the port in. The field is blank if the Port VLAN ID is not overridden by 802.1X.

If the VLAN ID is assigned by the RADIUS server, "(RADIUS-assigned)" is appended to the VLAN ID. Read more about RADIUS-assigned VLANs here.

If the port is moved to the Guest VLAN, "(Guest)" is appended to the VLAN ID. Read more about Guest VLANs here.

## **Port Counters**

**EAPOL Counters:** These supplicant frame counters are available for the following administrative states:

- Force Authorized
- Force Unauthorized
- Port-based 802.1X
- Single 802.1X
- Multi 802.1X

Direction	Name	IEEE Name	Description
RX	Total	dot1xAuthEapolFramesRx	The number of valid EAPOL frames of any type that have been received by the switch.
RX	Response ID	dot1xAuthEapolRespldFramesRx	The number of valid EAPOL Response Identity frames that have been received by the switch.
RX	Responses	dot1xAuthEapolRespFramesRx	The number of valid EAPOL response frames (other than Response Identity frames) that have been received by the switch.
RX	Start	dot1xAuthEapolStartFramesRx	The number of EAPOL Start frames that have been received by the switch.
RX	Logoff	dot1xAuthEapolLogoffFramesRx	The number of valid EAPOL Logoff frames that have been received by the switch.
RX	Invalid Type	dot1xAuthInvalidEapolFramesRx	The number of EAPOL frames that have been received by the switch in which the frame type is not recognized.
RX	Invalid Length	dot1xAuthEapLengthErrorFramesRx	The number of EAPOL frames that have been received by the switch in which the Packet Body Length field is invalid.
TX	Total	dot1xAuthEapolFramesTx	The number of EAPOL frames of any type that have been transmitted by the switch.
TX	Request ID	dot1xAuthEapolReqIdFramesTx	The number of EAPOL Request Identity frames that have been transmitted by the switch.
TX	Requests	dot1xAuthEapolReqFramesTx	The number of valid EAPOL Request frames (other than Request Identity frames) that have been transmitted by the switch.

**Backend Server Counters:** These backend (RADIUS) frame counters are available for the following administrative states:

- Port-based 802.1X
- Single 802.1X
- Multi 802.1X
- MAC-based Auth.

Direction	Name	IEEE Name	Description
RX	Access Challenges	dot1xAuthBackendAccessChallenges	802.1X-based: Counts the number of times that the switch receives the first request from the backend server following the first response from the supplicant. Indicates that the backend server has communication with the switch.  MAC-based: Counts all Access Challenges received from the backend server for this port (left-most table) or client (right-most table).
RX	Other Requests	dot1xAuthBackendOtherRequestsTo Supplicant	802.1X-based: Counts the number of times that the switch sends an EAP Request packet following the first to the supplicant. Indicates that the backend server chose an EAP-method.  MAC-based: Not applicable.  802.1X- and MAC-based: Counts the number of times that the switch receives a success indication. Indicates that the supplicant/client has successfully authenticated to the backend server.
RX	Auth. Successes	dot1xAuthBackendAuthSuccesses	802.1X- and MAC-based:  Counts the number of times that the switch receives a failure message. This indicates that the supplicant/client has not authenticated to the backend server.
RX	Auth. Failures	dot1xAuthBackendAuthFails	802.1X-based: Counts the number of times that the switch attempts to send a supplicant's first response packet to the backend server. Indicates the switch attempted communication with the backend server. Possible retransmissions are not counted.
TX	Responses	dot1xAuthBackendResponses	MAC-based: Counts all the backend server packets sent from the switch towards the backend server for a given port (left-most table) or client (right-most table). Possible retransmissions are not counted.

**Last Supplicant/Client Info:** Information about the last supplicant/client that attempted to authenticate. This information is available for the following administrative states:

- Port-based 802.1X
- Single 802.1X
- Multi 802.1X
- MAC-based Auth.

**Last Supplicant/Client Info :**

Name	IEEE Name	Description
MAC Address	dot1xAuthLastEapolFrameSource	The MAC address of the last supplicant/client.
VLAN ID -		The VLAN ID on which the last frame from the last supplicant/client was received.
Version	dot1xAuthLastEapolFrameVersion	802.1X-based: The protocol version number carried in the most recently received EAPOL frame. MAC-based: Not applicable.
Identity -		802.1X-based: The user name (supplicant identity) carried in the most recently received Response Identity EAPOL frame. MAC-based: Not applicable.

**Selected Counters**

**Selected Counters:** The Selected Counters table is visible when the port is in one of the following administrative states:

- Multi 802.1X
- MAC-based Auth.

The table is identical to and is placed next to the Port Counters table, and will be empty if no MAC address is currently selected. To populate the table, select one of the attached MAC Addresses from the section 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



: The port select box lets you select which port's information is displayed.

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

**Refresh:** Click to refresh the page immediately.

**Clear:** Click to clear the counters for the selected port. This button is available in these modes:

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

**Clear This:** Click to clear only the currently selected client's counters. This button is available in these modes:

- Multi 802.1X
- MAC-based Auth.X

## Security > IP Source Guard > Configuration

This page provides IP Source Guard related configuration.

IP Source Guard is a secure feature used to restrict IP traffic on DHCP snooping untrusted ports by filtering traffic based on the DHCP Snooping Table or manually configured IP Source Bindings. It helps prevent IP spoofing attacks when a host tries to spoof and use the IP address of another host.

The screenshot shows the IP Source Guard Configuration page. The 'Mode' is set to 'on'. Below it is a 'Translate dynamic to static' button. The 'Port Mode Configuration' table is as follows:

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

**Mode:** Set to **on** to enable the Global IP Source Guard or set to **off** to disable the Global IP Source Guard. All configured ACEs will be lost when the mode is enabled. The default is **off**.

**Port Mode Configuration:** At the dropdown enable IP Source Guard on the desired ports. Only when both Global Mode and Port Mode on a given port are enabled, IP Source Guard is enabled on this given port.

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

### Buttons

**Apply:** Click to save changes.

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

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

**Message:** The new setting of max dynamic clients on some port maybe lost some dynamic entries. Do you want to proceed anyway?



## Security > IP Source Guard > Static Table

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

The screenshot shows the Lantronix web interface for configuring Static IP Source Guard rules. The interface includes a navigation menu on the left with options like System, Port Management, PoE Management, VLAN Management, QoS, Spanning Tree, and MAC Address Tables. The main content area displays the 'Static IP Source Guard Table' with a table containing one entry. The entry has a 'Delete' checkbox, 'Port' 1, 'VLAN ID' 2, 'IP Address' 192.168.22.33, and 'MAC address' 11-22-33-44-55-66. Below the table are buttons for 'Add New Entry', 'Apply', and 'Reset'. The top of the page shows the device name 'SISPM1040-3166-L3' and 'Auto-Logout OFF'.

Delete	Port	VLAN ID	IP Address	MAC address
<input type="checkbox"/>	1	2	192.168.22.33	11-22-33-44-55-66
<input type="checkbox"/>	1			

**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 (VID) for the settings.

**IP Address:** Allowed Source IP address.

**MAC address:** Allowed Source MAC address.

### Buttons

**Add New Entry:** Click to add a new entry to the Static IP Source Guard table.

**Apply:** Click to save changes.

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

## Security > IP Source Guard > Dynamic Table

Entries in the Dynamic IP Source Guard Table are shown on this page. The Dynamic IP Source Guard Table is sorted first by port, then by VLAN ID, then by IP address, and then by MAC address.

Each page shows up to 99 entries from the Dynamic IP Source Guard table (the 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 Dynamic IP Source Guard Table.

The "Start from port address", "VLAN" and "IP address" input fields let you select the starting point in the Dynamic IP Source Guard Table.

The screenshot shows the web interface for the Dynamic IP Source Guard Table. At the top, there is a navigation menu with 'Switch' and 'DMS' tabs. The main content area is titled 'Dynamic IP Source Guard Table'. Below the title, there is an 'Auto-refresh' toggle set to 'off', and buttons for 'Refresh', 'First Page', and 'Next Page'. The 'Start from' section includes a dropdown for 'Port' (set to 'Port 1'), a text input for 'VLAN' (set to '1'), and a text input for 'IP address' (set to '0.0.0.0'). To the right, there is a text input for 'entries per page' (set to '20'). Below these controls is a table with the following columns: 'Port', 'VLAN ID', 'IP Address', and 'MAC Address'. The table currently displays 'No more entries'.

**Port:** Switch Port Number for which the entries are displayed.

**VLAN ID:** The VLAN-ID in which IP traffic is permitted.

**IP Address:** User IP address of the entry.

**MAC Address:** The Source MAC address.

### Buttons

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

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

**First Page:** Updates the table starting from the first entry in the Dynamic IP Source Guard Table.

**Next Page:** Updates the table, starting with the entry after the last entry currently displayed.

## Security > IPv6 Source Guard > Configuration

This page provides IPv6 Source Guard related configuration.

IPv6 Source Guard is a security feature used to restrict IPv6 traffic on DHCP snooping untrusted ports by filtering traffic based on the DHCPv6 Snooping Table or manually configured IPv6 Source Bindings. It helps prevent IP spoofing attacks when a host tries to spoof and use the IPv6 address of another host.

The screenshot shows the IPv6 Source Guard Configuration page in the Lantronix web interface. The page title is "IPv6 Source Guard Configuration". The "Mode" is set to "Disabled". There is a button labeled "Translate dynamic to static". Below this is a table with three columns: "Port", "Mode", and "Max Dynamic Clients".

Port	Mode	Max Dynamic Clients
*	<>	<>
Gi 1/1	Disabled	Unlimited
Gi 1/2	Disabled	Unlimited
Gi 1/3	Disabled	Unlimited
Gi 1/4	Disabled	Unlimited
Gi 1/5	Disabled	Unlimited
Gi 1/6	Disabled	Unlimited
Gi 1/7	Disabled	Unlimited
Gi 1/8	Disabled	Unlimited

**Mode:** Enable or disable IPv6 Source Guard globally.

**Port Mode Configuration:** The table shows all ports on the device. IPv6 Source Guard can be enabled or disabled on individual ports. IPv6 Source Guard is enabled on a given port only when both Global Mode and Port Mode are enabled on that port.

**Max Dynamic Clients:** This value can be 0, 1, 2 or unlimited. If the Port Mode is enabled and the value of Max Dynamic Clients is 0, only IPv6 packets that are matched in static entries on the specific port are forwarded.

### 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.

## Security > IPv6 Source Guard > Static Table

This page shows the static IPv6 Source Guard entries. The maximum number of entries is 112 per switch. At the Port dropdown, select the port to be displayed.

The screenshot displays the 'IPv6 Source Guard Static Table' configuration page. At the top, there is a navigation breadcrumb: Home > Security > IPv6 Source Guard > Static Table. The page features an 'Auto-refresh' toggle set to 'off' and a 'Refresh' button. Below these are input fields for 'Port' (a dropdown menu currently showing 'Gi 1/1'), 'VLAN ID', 'IP Address', and 'MAC Address', followed by an 'Add Entry' button. At the bottom, a table is shown with the following columns: Port, VLAN ID, IPv6 Address, and MAC Address.

**Delete:** Click entry Delete button to delete the entry.

**Port:** The logical port the entry is bound to.

**VLAN ID:** The VLAN id for the settings. If no VLAN ID is associated with the entry, this field shows 0.

**IP Address:** The allowed Source IPv6 address.

**MAC address:** Allowed Source MAC address.

### Buttons

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

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

**Add Entry:** Click to add a new entry to the Static IPv6 Source Guard table.

**Apply:** Click to save changes.

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

### Messages:

*IP address and MAC address must be filled out*

*Error: Invalid params*

## Security > IPv6 Source Guard > Dynamic Table

Entries in the Dynamic IPv6 Source Guard Table are shown on this page. All dynamic entries are shown in the table which can be scrolled up and down when the number of entries exceeds the space allotted for the table.

The screenshot shows the Lantronix web interface for the SISPM1040-3166-L3 switch. The page title is "IPv6 Source Guard Dynamic Table". The breadcrumb trail is "Home > Security > IPv6 Source Guard > Dynamic Table". The page includes an "Auto-refresh" toggle set to "off" and a "Refresh" button. Below these controls is a table with the following columns: "Port", "VLAN ID", "IPv6 Address", and "MAC Address".

**Port:** Switch Port Number for which the entries are displayed.

**VLAN ID:** VLAN-ID in which the IP traffic is permitted. If no VLAN-ID is associated with the entry, this field shows 0.

**IP Address:** User IPv6 address of the entry.

**MAC Address:** The Source MAC address.

### Buttons

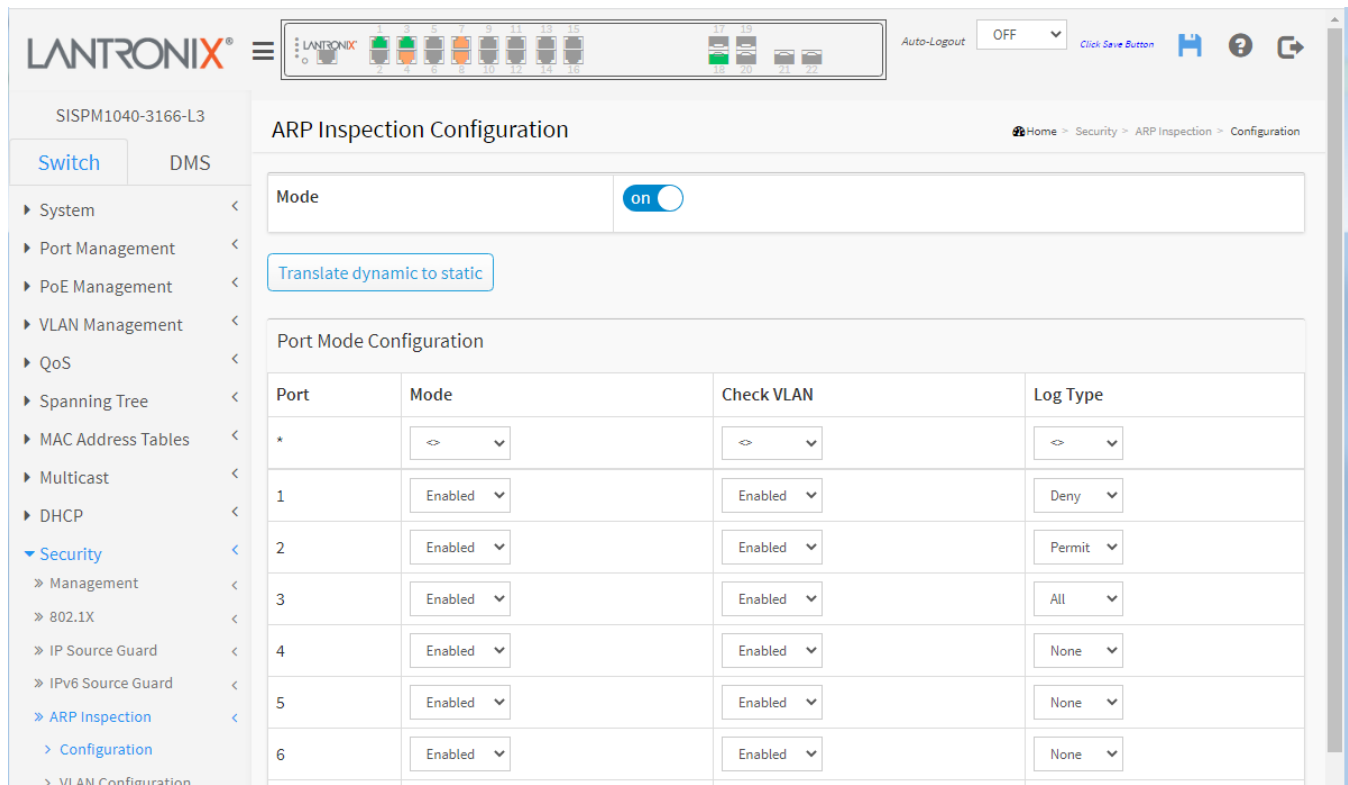
**Auto-refresh:** Check this box to refresh the page automatically every 3 seconds.

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

## Security > ARP Inspection > Configuration

This page provides ARP Inspection related configuration.

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. When enabled, only valid ARP requests and responses can go through the switch.



The screenshot shows the ARP Inspection Configuration page in the Lantronix web interface. The 'Mode' is set to 'on'. A 'Translate dynamic to static' button is visible. The 'Port Mode Configuration' table is as follows:

Port	Mode	Check VLAN	Log Type
*	<>	<>	<>
1	Enabled	Enabled	Deny
2	Enabled	Enabled	Permit
3	Enabled	Enabled	All
4	Enabled	Enabled	None
5	Enabled	Enabled	None
6	Enabled	Enabled	None

**Mode:** Set to **on** to enable ARP Inspection globally or set to **off** to 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:** To inspect the VLAN configuration, you must enable the setting of "Check VLAN". The default setting of "Check VLAN" is disabled. When the setting of "Check VLAN" is disabled, the log type of ARP Inspection will refer to the port setting. And the setting of "Check VLAN" is enabled, the log type of ARP Inspection will refer to the VLAN setting. Possible setting of "Check VLAN" are:

**Enabled:** Enable check VLAN operation.

**Disabled:** Disable check VLAN operation.

**Log Type:** 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 possible Log Types are:

**None:** Log nothing.

**Deny:** Log denied entries.

**Permit:** Log permitted entries.

**All:** Log all entries.

**Buttons**

**Apply:** Click to save changes.

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

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

## Security > ARP Inspection > VLAN Configuration

This page provides ARP Inspection related 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 "Start from VLAN" input fields let you select the starting point in the VLAN table.

**VLAN ID:** Specify which VLANs on which ARP Inspection is enabled. First, you must enable the port setting on Port mode configuration web page. Only when both Global Mode and Port Mode on a given port are enabled, ARP Inspection is enabled on this given port. Second, you can specify which VLAN will be inspected on the VLAN Mode Configuration page.

**Log Type:** The level of logging can also be configured on a per-VLAN basis. Possible log types are:

**None:** Log nothing.

**Deny:** Log denied entries.

**Permit:** Log permitted entries.

**All:** Log all entries.

### Buttons

**Add New Entry:** Click to add a new VLAN to the ARP Inspection VLAN table.

**Apply:** Click to save changes.

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

**First Entry :** Updates the table starting from the first entry in the table.

**Next Entry :** Updates the table, starting with the entry after the last entry currently displayed.

**Refresh :** Click to refresh the page immediately.

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



## Security > ARP Inspection > Static Table

This page shows the static ARP Inspection rules. The maximum number of rules is 256 per switch.

The screenshot shows the Lantronix web interface for the Static ARP Inspection Table. The interface includes a navigation menu on the left with options like System, Port Management, PoE Management, VLAN Management, and QoS. The main area displays a table with columns for Delete, Port, VLAN ID, MAC Address, and IP Address. Below the table are buttons for 'Delete', 'Add New Entry', 'Apply', and 'Reset'. The 'Delete' button is a checkbox, and the 'Port' column has a dropdown menu showing '1'.

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

**Port:** At the dropdown select the required logical port for the settings.

**VLAN ID:** Enter the VLAN ID for the settings.

**MAC Address:** Enter the allowed Source MAC address in ARP request packets.

**IP Address:** Enter the allowed Source IP address in ARP request packets.

### Buttons

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

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

**Apply:** Click to save changes.

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

## Security > ARP Inspection > Dynamic Table

Entries in the Dynamic ARP Inspection Table are shown on this page. The Dynamic ARP Inspection Table contains up to 256 entries, and is sorted first by port, then by VLAN ID, then by MAC address, and then by IP address. All dynamic entries are learning from DHCP Snooping.

Each page shows up to 99 entries from the Dynamic ARP Inspection table, default being 20, selected through the "entries per page" input field. When first visited, the web page will show the first 20 entries from the beginning of the Dynamic ARP Inspection Table.

The "Start from" port address, "VLAN", "MAC address" and "IP address" input fields let you select the starting point in the Dynamic ARP Inspection Table.

The screenshot shows the web interface for the Dynamic ARP Inspection Table. The top navigation bar includes the LANTRONIX logo, a menu icon, and a status bar with port indicators (1-22) and an Auto-Logout timer set to 10 min. The main content area is titled "Dynamic ARP Inspection Table" and includes a breadcrumb trail: Home > Security > ARP Inspection > Dynamic Table. Below the title, there is an "Auto-refresh" toggle set to "off" and three buttons: "Refresh", "First Page", and "Next Page". The configuration section includes input fields for "Start from" (Port 1), "VLAN" (1), "MAC address" (00-00-00-00-00-00), and "IP address" (0.0.0.0), followed by an "entries per page" field set to 20. 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". At the bottom of the configuration section are "Apply" and "Reset" buttons.

**Port:** Switch Port Number for which the entries are displayed.

**VLAN ID:** VLAN-ID in which the ARP traffic is permitted.

**MAC Address:** User MAC address of the entry.

**IP Address:** User IP address of the entry.

**Translate to static:** Select the checkbox to translate the entry to static entry.

### Buttons

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

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

**First Page:** Updates the table starting from the first entry in the Dynamic ARP Inspection Table.

**Next Page:** Updates the table, starting with the entry after the last entry currently displayed.

**Apply:** Click to save changes.

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

## Security > Port Security > Configuration

This page allows you to configure the Port Security global and per-port settings.

Port Security allows for limiting the number of users on a given port. A user is identified by a MAC address and VLAN ID. If Port Security is enabled on a port, the limit specifies the maximum number of users on the port. If this number is exceeded, an action is taken depending on violation mode. The violation mode can be one of the four selections described below.

Port Security configuration consists of two sections, a global and a per-port.

The screenshot displays the 'Port Security Configuration' page for device SISPM1040-3166-L3. The left sidebar shows a navigation tree with 'Security' expanded to 'Port Security' > 'Configuration'. The main content area is divided into two sections:

- System Configuration:**
  - Aging Enabled:** A toggle switch is turned 'on'.
  - Aging Period:** A text input field contains '3600' with 'seconds' to its right.
  - Hold Time:** A text input field contains '300' with 'seconds' to its right.
- Port Configuration:** A table with the following columns: Port, Mode, Limit, Violation Mode, Violation Limit, State, Re-open, Sticky, and Clear.
 

Port	Mode	Limit	Violation Mode	Violation Limit	State	Re-open	Sticky	Clear
*	<>		<>				<>	
1	Disabled	4	Protect	4	Disabled	Reopen	Disabled	Clear
2	Disabled	4	Protect	4	Disabled	Reopen	Disabled	Clear
3	Disabled	4	Protect	4	Disabled	Reopen	Disabled	Clear
4	Disabled	4	Protect	4	Disabled	Reopen	Disabled	Clear
5	Disabled	4	Protect	4	Disabled	Reopen	Disabled	Clear
6	Disabled	4	Protect	4	Disabled	Reopen	Disabled	Clear
7	Disabled	4	Protect	4	Disabled	Reopen	Disabled	Clear

### System Configuration (global configuration)

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

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

The Aging Period can be set to 10 - 10000000 seconds, with a default of 3600 seconds.

To understand why aging may be desired, consider this scenario: Suppose an end-host is connected to a third party switch or hub, which in turn is connected to a port on this switch on which Port Security is enabled. The end host will be allowed to forward if the limit is not exceeded. Now suppose that the end-host logs off or powers down. If not for aging, the end-host would still take up resources on this switch and will be allowed to forward.

To overcome this situation, enable aging. With aging enabled, a timer is started once the end-host gets secured. When the timer expires, the switch starts looking for frames from the end-host, and if such frames are not seen within the next Aging Period, the end-host is assumed to be disconnected, and the corresponding resources are freed on the switch.

**Hold Time:** The hold time - measured in seconds - is used to determine how long a MAC address is held in the MAC table if it has been found to violate the limit. The valid range is 10 - 10000000 seconds with a default of 300 seconds. The reason for holding a violating MAC address in the MAC table is primarily to ensure that the same MAC address doesn't give rise to continuous notifications (if notifications on violation count is enabled).

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

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

**Mode:** Controls whether Port Security is enabled on this port. Notice that other modules may still use the underlying port security features without enabling Port Security on a given port.

**Limit:** The maximum number of MAC addresses that can be secured on this port. This number cannot exceed 1023. The default is 4. If the limit is exceeded, an action is taken corresponding to the Violation mode.

The switch is "born" with a total number of MAC addresses from which all ports draw whenever a new MAC address is seen on a Port Security-enabled port. Since all ports draw from the same pool, it may happen that a configured maximum cannot be granted, if the remaining ports have already used all available MAC addresses.

**Violation Mode:** If Limit is reached, the switch can take one of the following actions:

**Protect:** Do not allow more than Limit MAC addresses on the port but take no further action.

**Restrict:** If Limit is reached, subsequent MAC addresses on the port will be counted and marked as violating. Such MAC addresses are removed from the MAC table when the hold time expires. At most Violation Limit MAC addresses can be marked as violating at any given time.

**Shutdown:** If Limit is reached, one additional MAC address will cause the port to be shut down. This implies that all secured MAC addresses be removed from the port, and no new addresses be learned. There are three ways to re-open the port:

- 1) In the "Configuration > Ports" page's "Configured" column, first disable the port, then restore the original mode.
- 2) Make a Port Security configuration change on the port.
- 3) Boot the switch.

**Violation Limit:** The maximum number of MAC addresses that can be marked as violating on this port. This number cannot exceed 1023. The default is 4. It is only used when Violation Mode is Restrict.

**State:** This column shows the current Port Security state of the port. The state takes one of four values:

**Disabled:** Port Security is disabled on the port.

**Ready:** The limit is not yet reached. This can be shown for all violation modes.

**Limit Reached:** Indicates that the limit is reached on this port. This can be shown for all violation modes.

**Shutdown:** Indicates that the port is shut down by Port Security. This state can only be shown if violation mode is set to Shutdown.

**Re-open:** Click the button to re-open a port that has been shut down. 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 unsaved changes will be lost.

**Sticky:** Enables sticky learning of MAC addresses on this port. When the port is in sticky mode, all MAC addresses that would otherwise have been learned as dynamic are learned as sticky.

Sticky MAC addresses are part of the running-config and can therefore be saved to startup-config. Sticky MAC addresses survive link changes (in contrast to Dynamic, which will have to be learned again). They also survive reboots if running-config is saved to startup-config.

A port can be Sticky-enabled whether Port Security is enabled on that interface. In that way, it is possible to add sticky MAC addresses in terms of management before enabling Port Security. To do that, use the "Configuration > Security > Port Security > MAC Addresses" page.

Sticky MAC (AKA, Persistent MAC learning) is a port security feature that causes an interface to retain dynamically learned MAC addresses when the switch is restarted or if the interface goes down and is brought back online.

**Enabled:** If the running config has sticky MAC addresses, then these MAC addresses are automatically to be static MAC address on MAC table.

**Disabled:** Sticky MAC addresses are not enabled.

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

### Buttons

**Apply:** Click to save changes.

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

**Refresh:** Click to refresh the page. Note that non-committed changes will be lost.

## Security > Port Security > MAC Address

### Port Security Static and Sticky MAC Addresses

This page lets you add and delete static and sticky MAC addresses managed by Port Security.

Port Security defines three types of MAC addresses, to which static and sticky can be added and removed on this page:

**Dynamic:** A MAC address learned through learn frames coming to the Port Security module while the interface in question is not in Sticky mode. Dynamic entries disappear if they age out or if the interface link goes down.

**Static:** A MAC address added by end-user through management. Static MAC addresses are not subject to aging and will be added to the MAC address table once Port Security gets enabled on the interface. Static entries are part of the running-config and will survive interface link state changes and reboots if saved to startup-config. Static entries can be added to the running-config at any time whether Port Security is enabled.

**Sticky:** When the interface is in sticky mode, all entries that would otherwise have been learned as dynamic are learned as sticky. Like static entries, sticky entries are part of the running-config and will survive interface link state changes and reboots if saved to the startup-config. Though not the intention with Sticky entries, they can be added by management to the running-config at any time whether Port Security is enabled on the interface, as long as the interface is in Sticky mode. Sticky entries will disappear if the interface is taken out of Sticky mode. The table contains one row per static or sticky MAC address.

The screenshot shows the web interface for a Lantronix switch. The main content area is titled "Port Security Static and Sticky MAC Addresses". It features a table with the following data:

Delete	Port	VLAN ID	MAC Address	Type
Delete	1	1	00:C0:F2:7C:59:91	Sticky
Delete	3	1	00:1B:11:B2:6D:4B	Sticky
Delete	4	1	AC:CC:8E:BA:F7:C1	Sticky
Delete	7	1	E0:55:3D:84:A8:96	Sticky
Delete	8	1	00:09:18:4F:BC:3A	Sticky

Below the table, there is an "Add New MAC Entry" button, and "Apply" and "Reset" buttons.

**Delete:** Press this button to remove the entry from the MAC address table (if present) and the running-config. Note that dynamic entries may be removed all-together on an interface from "Monitor > Security > Port Security > Switch" and one-by-one from "Monitor > Security > Port Security > Port".

**Port:** Displays the port number to which this MAC address is bound.

**VLAN ID:** The VLAN ID in question.

**MAC Address:** The MAC address in question.

**Type:** Displays the type of entry; it may be either Static or Sticky (see description above).

**Buttons**

**Add New MAC Entry:** Clicking this button will add a new row to the table. This new row allows for adding a static or sticky MAC address to a particular interface. When done, click the Apply button to save the changes to running-config. Note that sticky entries are normally added automatically by learning on the interface.

**Refresh:** Click to refresh the page. Note that non-committed changes will be lost.

**Apply:** Click to save changes.

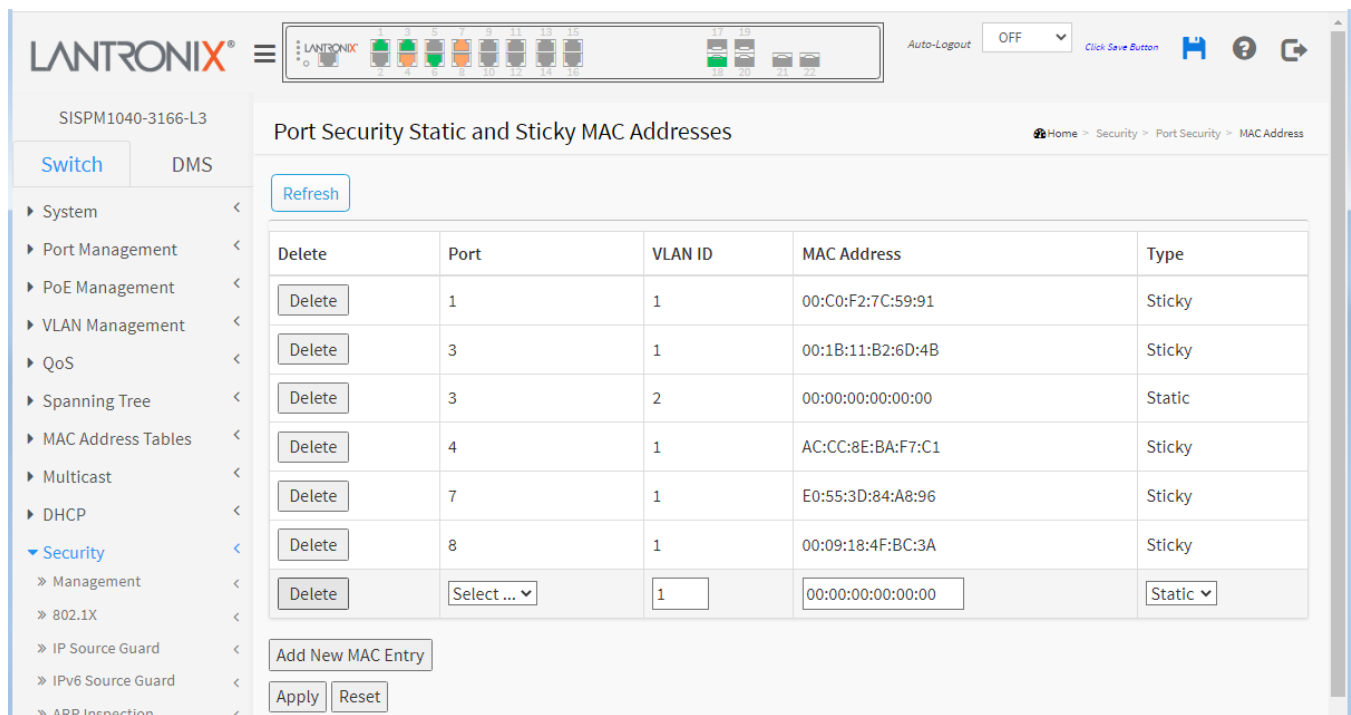
**Reset:** Click to undo any changes made locally and revert to previously saved values.

**Messages:**

*Error: The <MAC, VLAN> is already installed on another interface*

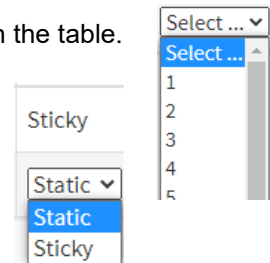
*Error: MAC address must be a unicast MAC address*

**Port Security Static and Sticky MAC Addresses Example:**



**Port select dropdown:** When adding a new MAC entry, select the desired port for the row in the table.

**Type dropdown:** When adding a new MAC entry, select the desired type for the row in the table. Select Static or Sticky; see the descriptions above.



**Messages:**

*Error: The <MAC, VLAN> is already installed on another interface*

*Error: Cannot add sticky entry on non-sticky interface*

## Security > Port Security > Status

This page shows the MAC addresses secured by the Port Security module.

Port Security may be configured both administratively and indirectly through other software modules (the so-called 'user modules').

When a user module has enabled port security on a port, the port is set up for software-based learning. In this mode, frames from unknown MAC addresses are passed on to the port security module, which in turn asks all user modules whether to allow this new MAC address to forward it 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 enabled user module chooses to block it, it will be blocked until that user module decides otherwise.

Note that if you have added Static or Sticky MAC addresses, they will show up on this page only if Port Security is enabled on the interface to which they pertain. This is done at the Security > Port Security > Configuration page.

The screenshot shows the 'Port Security Status' page in the Lantronix web interface. The page title is 'SISPM1040-3166-L3'. The navigation menu on the left includes 'System', 'Port Management', 'PoE Management', 'VLAN Management', 'QoS', 'Spanning Tree', 'MAC Address Tables', 'Multicast', 'DHCP', 'Security' (expanded), 'Management', '802.1X', 'IP Source Guard', 'IPv6 Source Guard', 'ARP Inspection', 'Port Security' (expanded), 'Configuration', 'MAC Address', and 'Status'. The main content area has a breadcrumb trail: 'Home > Security > Port Security > Status'. Below the breadcrumb is an 'Auto-refresh' toggle set to 'off' and a 'Refresh' button. The 'Port Status' table is as follows:

Port	Violation Mode	State	MAC Count		
			Current	Violating	Limit
1	Protect	Ready	1	0	4
2	Protect	Ready	0	0	4
3	Protect	Ready	2	0	4
4	Protect	Ready	1	0	4
5	Protect	Ready	0	0	4
6	Protect	Ready	0	0	4
7	Protect	Ready	1	0	4
8	Protect	Ready	1	0	4
9	Protect	Ready	0	0	4
10	Protect	Ready	0	0	4
11	Protect	Ready	0	0	4

**Port:** The table has one row for each port on the switch and several columns. This is the port number for which the row status applies. You can click a linked port number to see the status for that particular port.

**Violation Mode:** Shows the configured Violation Mode of the port. It can take one of four values:

**Disabled:** Port Security is not administratively enabled on this port.

**Protect:** Port Security is administratively enabled in Protect mode.

**Restrict:** Port Security is administratively enabled in Restrict mode.

**Shutdown:** Port Security is administratively enabled in Shutdown mode.



**State:** Shows the current state of the port. It can take one of four values:

**Disabled:** No user modules are currently using the Port Security service.

**Ready:** The Port Security service is in use by at least one user module and is awaiting frames from unknown MAC addresses to arrive.

**Limit Reached:** The Port Security service is administratively enabled, and the limit is reached.

**Shut down:** The Port Security service is administratively enabled, and the port is shut down. No MAC addresses can be learned on the port until it is administratively re-opened by administratively taking the port down and then back up on the "Configuration > Ports" page. Alternatively, the switch may be booted or reconfigured in terms of Port Security.

**MAC Count (Current, Violating, Limit):** The three columns indicate the number of currently learned MAC addresses (forwarding as well as blocked), the number of violating MAC address (only counting in Restrict mode) and the maximum number of MAC addresses that can be learned on the port, respectively.

If no user modules are enabled on the port, the Current column will show a dash (-).

If Port Security is not administratively enabled on the port, the Violating and Limit columns will show a dash (-).

### Buttons

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

**Refresh:** Click to refresh the page immediately.

## Port Security Status for a selected Port

You can click a port number to view the status for that particular port.

The Port Security Port Status page shows the MAC addresses secured by the Port Security module. Port Security may be configured both administratively and indirectly through other software modules - the so-called user modules. When a user module has enabled port security on a port, the port is set-up for software-based learning. In this mode, frames from unknown MAC addresses are passed on to the Port Security module, which in turn asks all user modules whether to allow this new MAC address to forward or block it. For a MAC address to be set in the forwarding state, all enabled user modules must unanimously agree on allowing the MAC address to forward. If only one chooses to block it, it will be blocked until that user module decides otherwise.

Note that if you have added static or sticky MAC addresses, they will show up on this page only if Port Security is enabled on the interface to which they pertain.

SISPM1040-3166-L3 Auto-Logout OFF Click Save Button

Switch DMS

Port Security Status Port 1

Auto-refresh  off Refresh Clear Port 1 Back

User Module Legend

MAC Address	VLAN ID	State	Time of Addition	Age/Hold
00-c0-f2-7c-59-91	1	Forwarding	2022-03-07T15:59:00+00:00	-

**MAC Address:** The MAC address that is seen on this port.

**VLAN ID:** The related VLAN ID.

**State:** Indicates whether the corresponding MAC address is violating (administrative user has configured the interface in "Restrict" mode and the MAC address is blocked), blocked, or forwarding.

**Time of Addition:** The date and time that the state changed.

**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 address table. Otherwise a new age period will begin.

If aging is disabled or a user module has decided to hold the MAC address indefinitely, a dash (-) will be shown.

### Buttons



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

**Refresh:** Click to refresh the page immediately.

**Clear:** Click to clear the results.

**Port Select box:** At the dropdown select which port to show status for.

**Back:** Click to return to the Port Security Status page.

## Security > RADIUS > Configuration

This page allows you to configure up to five RADIUS servers.

RADIUS (Remote Authentication Dial In User Service) is a networking protocol that provides centralized access, authorization and accounting management for computers to connect and use a network service.

**Global Configuration:** These settings are common for all of the RADIUS servers.

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

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

**Key:** The secret key - up to 63 characters long - shared between the 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 253 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/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. The officially assigned port number for RADIUS Accounting is 1812. **Note:** by default, many access servers use port 1645 for authentication requests.

**Acct Port:** The UDP port to use on the RADIUS server for accounting. Set to 0 to disable accounting. The officially assigned port number for RADIUS Accounting is 1813. **Note:** by default, many access servers use port 1646 for accounting requests.

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

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

**Key:** You can change the setting which overrides the global key. Leaving it blank won't change the current 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.

**Apply:** Click to save changes.

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

#### Messages:

*Authentication Error Invalid secret key configuration parameter*

## Security > RADIUS > Status

This page provides an overview of the status of the RADIUS servers configured on the RADIUS Server Configuration page.

#	IP Address	Authentication Port	Authentication Status	Accounting Port	Accounting Status
1	192.168.1.77	1812	Ready	1813	Ready
2	192.168.1.3	1812	Ready	1813	Ready
3			Disabled		Disabled
4			Disabled		Disabled
5			Disabled		Disabled

**#** : The RADIUS server number. Click to navigate to detailed statistics for this server (see below).

**IP Address**: The IP address of this server.

**Authentication Port**: UDP port number for authentication.

**Authentication Status**: The current status of the server. This field takes one of the following values:

**Disabled**: The server is disabled.

**Not Ready**: The server is enabled, but IP communication is not yet up and running.

**Ready**: The server is enabled, IP communication is up and running, and the RADIUS module is ready to accept access attempts.

**Dead (X seconds left)**: Access attempts were made to this server, but it did not reply within the configured timeout. The server has temporarily been disabled but will get re-enabled when the dead-time expires. The number of seconds left before this occurs is displayed in parentheses. This state is only reachable when more than one server is enabled.

**Accounting Port**: UDP port number for accounting.

**Accounting Status**: The current status of the server. This field takes one of the following values:

**Disabled**: The server is disabled.

**Not Ready**: The server is enabled, but IP communication is not yet up and running.

**Ready**: The server is enabled, IP communication is up and running, and the RADIUS module is ready to accept access attempts.

**Dead (X seconds left)**: Access attempts were made to this server, but it did not reply within the configured timeout. The server has temporarily been disabled but will get re-enabled when the dead-time expires. The number of seconds left before this occurs is displayed in parentheses. This state is only reachable when more than one server is enabled.

### Buttons

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

**Refresh**: Click to refresh the page immediately.

### Detailed RADIUS Authentication Statistics

This page provides detailed statistics for a selected RADIUS server. The statistics map closely to those specified in IETF [RFC4668 - RADIUS Authentication Client MIB](#). Use the server select box to switch between the backend servers to show details for.

The screenshot displays the 'RADIUS Authentication Statistics' page for 'Server #1'. The interface includes a navigation sidebar on the left with categories like System, Port Management, PoE Management, VLAN Management, QoS, Spanning Tree, MAC Address Tables, Multicast, DHCP, Security (highlighted), Access Control, SNMP, CFM, APS, ERPS, and Rapid Ring. The main content area features a top control bar with 'Auto-refresh' (off), 'Refresh', 'Clear', and a 'Server #1' dropdown. Below this are two tables:

RADIUS Authentication Statistics for Server #1	
Receive Packets	Transmit Packets
Access Accepts	0
Access Rejects	0
Access Challenges	0
Malformed Access Responses	0
Bad Authenticators	0
Unknown Types	0
Packets Dropped	0
Other Info	
IP Address	
State	Disabled
Round-Trip Time	0 ms

RADIUS Accounting Statistics for Server #1	
Receive Packets	Transmit Packets
Responses	0
Malformed Responses	0
Bad Authenticators	0
Unknown Types	0
Packets Dropped	0
Other Info	

**RADIUS Authentication Statistics for Server # 2:** The statistics map closely to those specified in IETF [RFC4668 - RADIUS Authentication Client MIB](#). Use the server select box to switch between the backend servers to show details for. Information is displayed both Receive Packets and Transmit Packets.

**Access Accepts :** The number of RADIUS Access-Accept packets (valid or invalid) received from the server.

**Access Rejects :** The number of RADIUS Access-Reject packets (valid or invalid) received from the server.

**Access Challenges :** The number of RADIUS Access-Challenge packets (valid or invalid) received from the server.

**Malformed Access Responses :** The number of malformed RADIUS Access-Response packets received from the server. Malformed packets include packets with an invalid length. Bad authenticators or Message Authenticator attributes or unknown types are not included as malformed access responses.

**Bad Authenticators** :The number of RADIUS Access-Response packets containing invalid authenticators or Message Authenticator attributes received from the server.

**Unknown Types** :The number of RADIUS packets that were received with unknown types from the server on the authentication port and dropped.

**Packets Dropped** :The number of RADIUS packets that were received from the server on the authentication port and dropped for some other reason.

**Access Requests** :The number of RADIUS Access-Request packets sent to the server. This does not include retransmissions.

**Access Retransmissions** :The number of RADIUS Access-Request packets retransmitted to the RADIUS authentication server.

**Pending Requests** :The number of RADIUS Access-Request packets destined for the server that have not yet timed out or received a response. This variable is incremented when an Access-Request is sent and decremented due to receipt of an Access-Accept, Access-Reject, Access-Challenge, timeout, or retransmission.

**Timeouts** :The number of authentication timeouts to the server. After a timeout, the client may retry to the same server, send to a different server, or give up. A retry to the same server is counted as a retransmit as well as a timeout. A send to a different server is counted as a Request as well as a timeout.

**IP Address** : The IP address and UDP port for the authentication server in question.

**State** :Shows the state of the server. It takes one of these values:

**Disabled** : The selected server is disabled.

**Not Ready** : The server is enabled, but IP communication is not yet up and running.

**Ready** : The server is enabled, IP communication is up and running, and the RADIUS module is ready to accept access attempts.

**Dead (X seconds left)** : Access attempts were made to this server, but it did not reply within the configured timeout. The server has temporarily been disabled but will get re-enabled when the dead-time expires. The number of seconds left before this occurs is displayed in parentheses. This state is only reachable when more than one server is enabled.

**Round-Trip Time** : The time interval (measured in milliseconds) between the most recent Access-Reply/Access-Challenge and the Access-Request that matched it from the RADIUS authentication server. The granularity of this measurement is 100 ms. A value of 0 ms indicates that there hasn't been round-trip communication with the server yet.

**RADIUS Accounting Statistics for Server #2:** The statistics map closely to those specified in RFC4670 - RADIUS Accounting Client MIB. Use the server select box to switch between the backend servers to show details for.

**Responses** : The number of RADIUS packets (valid or invalid) received from the server.

**Malformed Responses** : The number of malformed RADIUS packets received from the server. Malformed packets include packets with an invalid length. Bad authenticators or unknown types are not included as malformed access responses.

**Bad Authenticators** : The number of RADIUS packets containing invalid authenticators received from the server.

**Unknown Types** : The number of RADIUS packets of unknown types that were received from the server on the accounting port.

**Packets Dropped** : The number of RADIUS packets that were received from the server on the accounting port and dropped for some other reason.

**Requests** : The number of RADIUS packets sent to the server. This does not include retransmissions

**Retransmissions** : The number of RADIUS packets retransmitted to the RADIUS accounting server.

**Pending Requests** : The number of RADIUS packets destined for the server that have not yet timed out or received a response. This variable is incremented when a Request is sent and decremented due to receipt of a Response, timeout, or retransmission.

**Timeouts** : The number of accounting timeouts to the server. After a timeout, the client may retry to the same server, send to a different server, or give up. A retry to the same server is counted as a retransmit as well as a timeout. A send to a different server is counted as a Request as well as a timeout.

**IP Address** : IP address and UDP port for the accounting server in question.

**State** : Shows the state of the server. It takes one of the following values:

**Disabled** : The selected server is disabled.

**Not Ready** : The server is enabled, but IP communication is not yet up and running.

**Ready** : The server is enabled, IP communication is up and running, and the RADIUS module is ready to accept accounting attempts.

**Dead (X seconds left)** : Accounting attempts were made to this server, but it did not reply within the configured timeout. The server has temporarily been disabled but will get re-enabled when the dead-time expires. The number of seconds left before this occurs is displayed in parentheses. This state is only reachable when more than one server is enabled.

**Round-Trip Time** : The time interval (measured in milliseconds) between the most recent Response and the Request that matched it from the RADIUS accounting server. The granularity of this measurement is 100 ms. A value of 0 ms indicates that there hasn't been round-trip communication with the server yet.

## Buttons

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

**Refresh** : Click to refresh the page immediately.

**Clear** : Clears the counters for the selected server. The "Pending Requests" counter will not be cleared by this operation.

**Server select box**: Dropdown to select the desired server to be displayed.



**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 these values: <b>Disabled:</b> The selected server is disabled. <b>Not Ready:</b> The server is enabled, but IP communication is not yet up and running. <b>Ready:</b> The server is enabled, IP communication is up and running, and the RADIUS module is ready to accept access attempts. <b>Dead (X seconds left):</b> 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 [IETF RFC4670 - RADIUS Accounting Client MIB](#). Use the server select box to switch between the backend servers to show details for.

### Packet Counters

RADIUS accounting server packet counter. There are five receive and four transmit counters.

Direction	Name	RFC4670 Name	Description
Rx	<b>Responses</b>	radiusAccClientExtResponses	The number of RADIUS packets (valid or invalid) received from the server.
Rx	<b>Malformed Responses</b>	radiusAccClientExtMalformedResponses	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	<b>Bad Authenticators</b>	radiusAcctClientExtBadAuthenticators	The number of RADIUS packets containing invalid authenticators received from the server.
Rx	<b>Unknown Types</b>	radiusAccClientExtUnknownTypes	The number of RADIUS packets of unknown types that were received from the server on the accounting port.
Rx	<b>Packets Dropped</b>	radiusAccClientExtPacketsDropped	The number of RADIUS packets that were received from the server on the accounting port and dropped for some other reason.
Tx	<b>Requests</b>	radiusAccClientExtRequests	The number of RADIUS packets sent to the server. This does not include retransmissions.
Tx	<b>Retransmissions</b>	radiusAccClientExtRetransmissions	The number of RADIUS packets retransmitted to the RADIUS accounting server.
Tx	<b>Pending Requests</b>	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	<b>Timeouts</b>	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 these values: <b>Disabled:</b> The selected server is disabled. <b>Not Ready:</b> The server is enabled, but IP communication is not yet up and running. <b>Ready:</b> The server is enabled, IP communication is up and running, and the RADIUS module is ready to accept accounting attempts. <b>Dead (X seconds left):</b> 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 (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

**Server Select box:** At the dropdown select which RADIUS server's information to display.

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

**Refresh:** Click to refresh the page immediately.

**Clear:** Clears the counters for the selected server. The "Pending Requests" counter will not be cleared by this operation.

## Security > TACACS+

This page lets you configure up to 5 TACACS+ servers.

TACACS+ (Terminal Access Controller Access Control System Plus) is a networking protocol which provides access control for routers, network access servers and other networked computing devices via one or more centralized servers. TACACS+ provides separate authentication, authorization and accounting services.

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

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

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

**Key:** The secret key. This current key won't be shown in this field. Leaving it blank won't change the key. You can change 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:

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

**Hostname:** The IPv4/IPv6 address or hostname of the TACACS+ server.

**Port:** The TCP port to use on the TACACS+ server for authentication.

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

**Key:** You can change the setting to override the global key. Leaving it blank won't change the current key.

**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 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.

## Access Control

This section lets you set and view access control functions, including Port configuration, Rate limiters, Access Control List, and ACL status.

- ▼ Access Control
  - > Port Configuration
  - > Rate Limiters
  - > Access Control List
  - > ACL Status

### Access Control > ACL Ports Configuration

Configure the ACL parameters (ACE) of each switch port. These parameters will affect frames received on a port unless the frame matches a specific ACE.

An Access Control Entry describes access permission associated with a particular ACE ID. There are three ACE frame types (Ethernet Type, ARP, and IPv4) and two ACE actions (permit and deny). The ACE also contains many detailed, different parameter options that can be applied individually.

Port	Policy ID	Action	Rate Limiter ID	Port Redirect	Mirror	Logging	Shutdown	State	Counter
*		<>	<>	Disabled Port 1 Port 2	<>	<>	<>	<>	*
1	0	Permit	Disabled	Disabled Port 1 Port 2	Disabled	Disabled	Disabled	Enabled	0
2	0	Permit	Disabled	Disabled Port 1 Port 2	Disabled	Disabled	Disabled	Enabled	0
3	0	Permit	Disabled	Disabled Port 1 Port 2	Disabled	Disabled	Disabled	Enabled	7659
4	0	Permit	Disabled	Disabled Port 1 Port 2	Disabled	Disabled	Disabled	Enabled	1738
5	0	Permit	Disabled	Disabled Port 1 Port 2	Disabled	Disabled	Disabled	Enabled	0
6	0	Permit	Disabled	Disabled Port 1	Disabled	Disabled	Disabled	Enabled	0

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

**Policy ID:** Select the policy to apply to this port. The allowed values are 0-127. The default value is 0.

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

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

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

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

**Enabled:** Frames received on the port are mirrored.

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

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

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

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

**Note:** 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 this port. The allowed values are:

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

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

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

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

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

**Disabled:** To close ports by changing the volatile port configuration of the ACL user module. The default 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 refresh the page; any changes made locally will be undone.

**Clear:** Click to clear the counters.



## Access Control > Rate Limiters

Configure up to 16 ACL rate limiters here.

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

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

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

There are three webpages for manual ACL setup: ACL>Access Control List, ACL>Ports, and ACL>Rate Limiters.

The screenshot shows the 'ACL Rate Limiter Configuration' page in the Lantronix web interface. The page title is 'ACL Rate Limiter Configuration' and the breadcrumb trail is 'Home > Access Control > Rate Limiters'. The interface includes a navigation menu on the left with options like System, Port Management, PoE Management, VLAN Management, QoS, Spanning Tree, MAC Address Tables, Multicast, DHCP, Security, Access Control (selected), Port Configuration, Rate Limiters (selected), and Access Control List. The main content area displays a table with the following data:

Rate Limiter ID	Rate	Unit
*	<input type="text"/>	<input type="text"/>
1	<input type="text" value="1"/>	10pps
2	<input type="text" value="1"/>	10pps
3	<input type="text" value="1"/>	10pps
4	<input type="text" value="1"/>	10pps
5	<input type="text" value="1"/>	10pps
6	<input type="text" value="1"/>	10pps
7	<input type="text" value="1"/>	10pps
8	<input type="text" value="1"/>	10pps

**Rate Limiter ID:** The rate limiter ID for the settings contained in the same row and its range is 1 to 16.

**Rate:** The valid rate is 0, 10, 20, 30, ..., 5000000 in pps or 0, 25, 50, 75, ..., 10000000 in kbps.

**Unit:** Specify the rate unit. The allowed values are:

**10pps:** packets per second.

**25kbps:** Kbits per second.

### Buttons

**Apply:** Click to save changes.

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


**Messages:**

*The value of '25kbps' is restricted to 0, 1, 2, 3, ..., 400000*

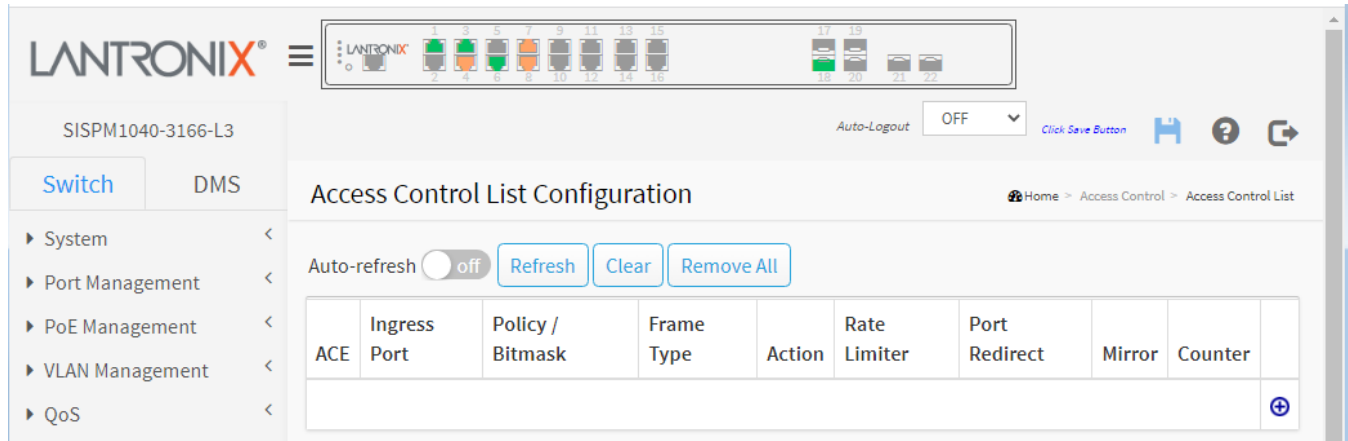
*The value of '10pps' is restricted to 0, 1, 2, 3, ..., 500000*

## Access Control > Access Control List

This page shows the Access Control List (ACL), which is made up of the ACEs defined on this switch. Each row describes the ACE that is defined. The maximum number of ACEs is 512 per switch.

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

### Access Control List Configuration page



The screenshot shows the 'Access Control List Configuration' page in the Lantronix web interface. The page title is 'Access Control List Configuration'. Below the title, there are buttons for 'Auto-refresh' (set to 'off'), 'Refresh', 'Clear', and 'Remove All'. A table with the following columns is displayed: ACE, Ingress Port, Policy / Bitmask, Frame Type, Action, Rate Limiter, Port Redirect, Mirror, and Counter. A plus sign button is located at the bottom right of the table. The left sidebar shows a navigation menu with options like System, Port Management, PoE Management, VLAN Management, and QoS. The top right corner shows 'Auto-Logout OFF' and a 'Click Save Button' link.

**ACE:** Indicates the ACE ID.

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

**All:** The ACE will match all ingress port.

**Port:** The ACE will match a specific ingress port.

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

**Frame Type:** Indicates the frame type of the ACE. Possible values are:

**Any:** The ACE will match any frame type.

**EType:** The ACE will match Ethernet Type frames. Note that an Ethernet Type based ACE will not get matched by IP and ARP frames.

**ARP:** The ACE will match ARP/RARP frames.

**IPv4:** The ACE will match all IPv4 frames.

**IPv4/ICMP:** The ACE will match IPv4 frames with ICMP protocol.

**IPv4/UDP:** The ACE will match IPv4 frames with UDP protocol.

**IPv4/TCP:** The ACE will match IPv4 frames with TCP protocol.

**IPv4/Other:** The ACE will match IPv4 frames, which are not ICMP/UDP/TCP.

**IPv6:** The ACE will match all IPv6 standard frames.

**Action:** Indicates the forwarding action of the ACE.

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

**Deny:** Frames matching the ACE are dropped.

**Filter:** Frames matching the ACE are filtered.

**Rate Limiter:** Indicates the rate limiter number of the ACE. The allowed range is 1 to 16. When Disabled is displayed, the rate limiter operation is disabled.

**Port Redirect:** Indicates the port redirect operation of the ACE. Frames matching the ACE are redirected to the port number. The allowed values are Disabled or a specific port number. When Disabled is displayed, the port redirect operation is disabled.

**Mirror:** Specify the mirror operation of this port. Frames matching the ACE are mirrored to the destination mirror port. The allowed values are:







**Enabled:** Frames received on the port are mirrored.

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

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

### Modification Buttons

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

- : Inserts a new ACE before the current row.
- : Edits the ACE row.
- : Moves the ACE up the list.
- : Moves the ACE down the list.
- : Deletes the ACE.
- : The lowest plus sign adds a new entry at the bottom of the ACE listings.

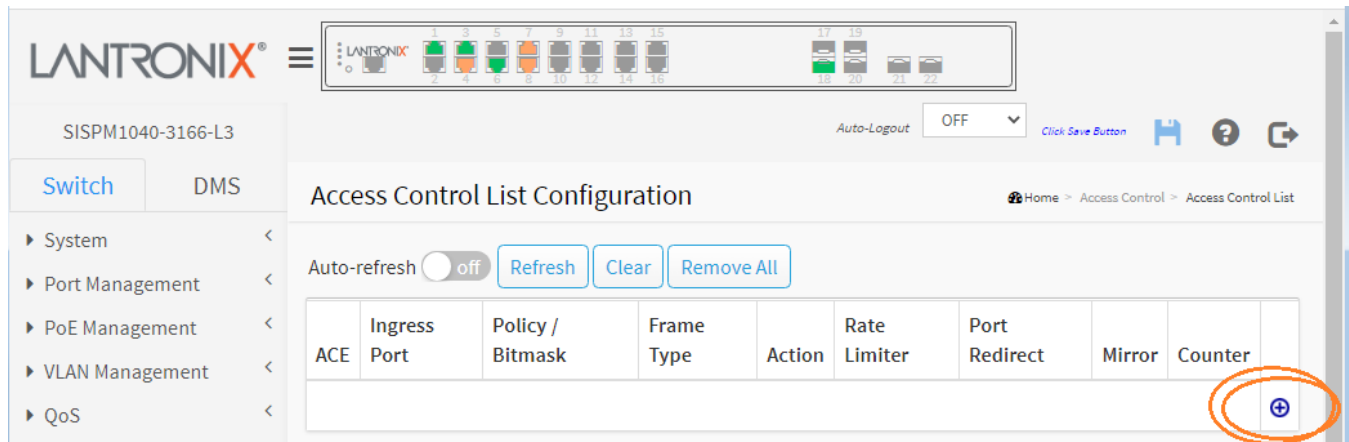
### Buttons

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

**Refresh:** Click to refresh the page; any changes made locally will be undone.

**Clear:** Click to clear the counters.

**Remove All:** Click to remove all ACEs.



The screenshot shows the 'Access Control List Configuration' page in the Lantronix web interface. The page includes a navigation menu on the left with options like System, Port Management, PoE Management, VLAN Management, and QoS. The main content area features an 'Auto-refresh' toggle set to 'off', and buttons for 'Refresh', 'Clear', and 'Remove All'. Below these is a table with columns: ACE, Ingress Port, Policy / Bitmask, Frame Type, Action, Rate Limiter, Port Redirect, Mirror, and Counter. A plus sign button is circled in orange at the bottom right of the table.

From the default page, click the Add ACE () button to display the ACE Configuration page:

## ACE Configuration page

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.

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

**All:** The ACE applies to all port.

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

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

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

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

**Policy Value:** When "Specific" is selected for the policy filter, you can enter a specific policy value. The allowed range is 0 to 127.

**Policy Bitmask:** When "Specific" is selected for the policy filter, you can enter a specific policy bitmask. The allowed range is 0x0 to 0x7f. Notice the usage of bitmask, if the binary bit value is "0", it means this bit is "don't-care". The real matched pattern is [policy\_value & policy\_bitmask]. For example, if the policy value is 3 and the policy bitmask is 0x10(bit 0 is "don't-care" bit), then policy 2 and 3 are applied to this rule.

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

**Any:** Any frame can match this ACE.

**Ethernet Type:** Only Ethernet Type frames can match this ACE. The IEEE 802.3 describes the value of Length/Type Field specifications to be greater than or equal to 1536 decimal (equal to 0600 hexadecimal) and the value should not be equal to 0x800(IPv4), 0x806(ARP) or 0x86DD(IPv6).

**ARP:** Only ARP frames can match this ACE. Notice the ARP frames won't match the ACE with ethernet type.

**IPv4:** Only IPv4 frames can match this ACE. Notice the IPv4 frames won't match the ACE with ethernet type.

**IPv6:** Only IPv6 frames can match this ACE. Notice the IPv6 frames won't match the ACE with Ethernet type.

**Action:** Specify the action to take with a frame that hits this ACE.

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

**Deny:** The frame that hits this ACE is dropped.

Filter: Frames matching the ACE are filtered.

**Filter Port:** Select the filter port for action.

**All:** The action applies to all port.

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

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

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

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

**Enabled:** Frames received on the port are mirrored.

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

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

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

**Disabled:** Frames matching the ACE are not logged.

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

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

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

**Disabled:** Port shut down is disabled for the ACE.

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

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

### **MAC Parameters**

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

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

**Specific:** If you want to filter a specific source MAC address with this ACE, choose this value. A field for entering an SMAC value appears.

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

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

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

**MC:** Frame must be multicast.

**BC:** Frame must be broadcast.

**UC:** Frame must be unicast.

**Specific:** If you want to filter a specific destination MAC address with this ACE, choose this value. A field for entering a DMAC value appears.

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

### **VLAN Parameters**

**802.1Q Tagged:** Specify whether frames can hit the action according to 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 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").

**Ethernet:** Specify whether frames can hit the action according to their ARP/RARP hardware address space (HRD) settings.

**0:** ARP/RARP frames where the HLD is not equal to Ethernet (1).

**1:** ARP/RARP frames where the HLD is equal to Ethernet (1).

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

**IP:** Specify whether frames can hit the action according to their ARP/RARP protocol address space (PRO) settings.

**0:** ARP/RARP frames where the PRO is not equal to IP (0x800).

**1:** ARP/RARP frames where the PRO is equal to IP (0x800).

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

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

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

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

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

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

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

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

**IP Protocol Value:** When "Specific" is selected for the IP protocol value, you can enter a specific value. The 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 0xFFFFFFFF(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.

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

**1:** 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 a EtherType value appears.

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

## Buttons

**Apply:** Click to save changes.

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

**Cancel:** Return to the previous page.

**Access Control List Configuration page Example:**

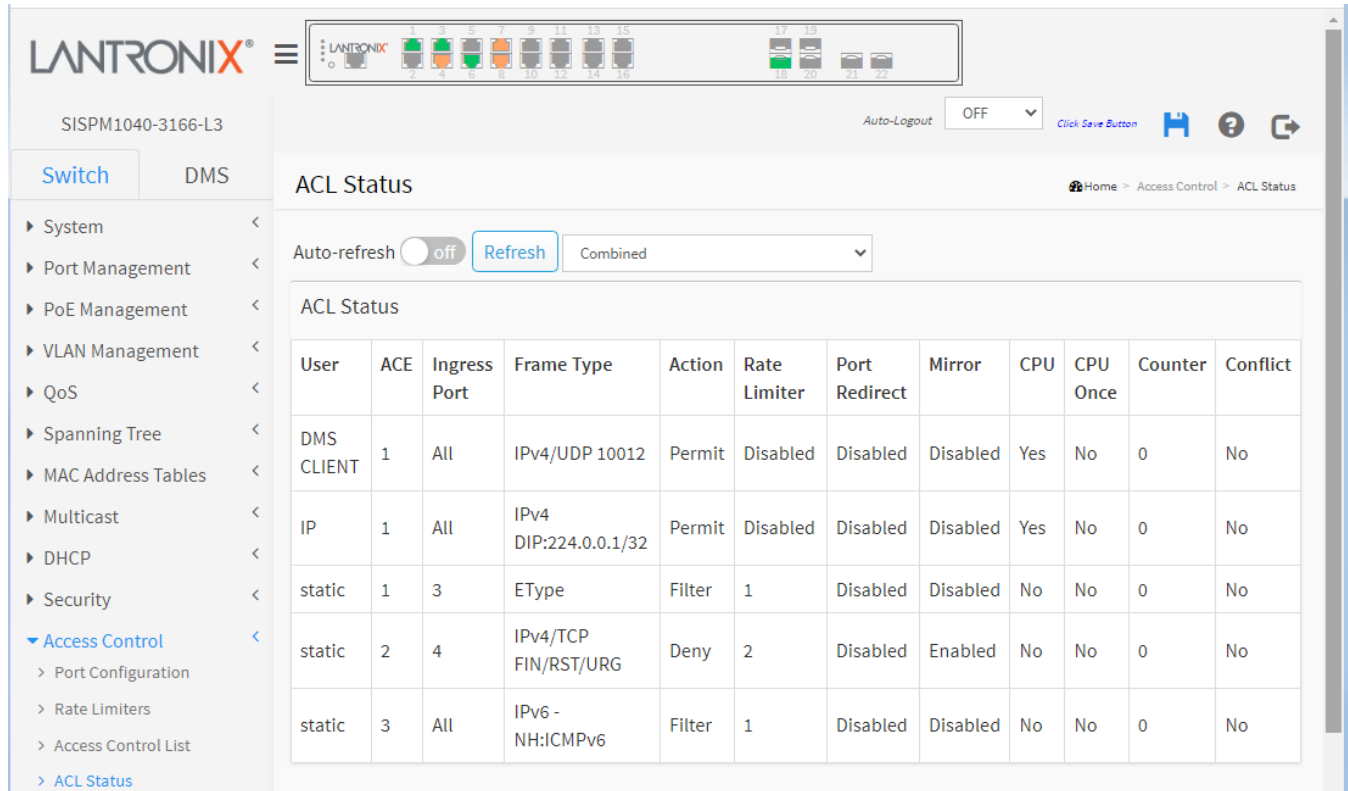
The screenshot displays the Lantronix web interface for the device SISPM1040-3166-L3. The interface is divided into several sections:

- Header:** Includes the Lantronix logo, a menu icon, and a status bar showing port status (ports 1-16 and 17-22).
- Navigation:** A left sidebar menu with options like System, Port Management, PoE Management, VLAN Management, QoS, Spanning Tree, MAC Address Tables, Multicast, DHCP, Security, and Access Control (selected).
- Page Title:** "Access Control List Configuration" with a breadcrumb trail: Home > Access Control > Access Control List.
- Controls:** An "Auto-refresh" toggle set to "off" and buttons for "Refresh", "Clear", and "Remove All".
- Table:** A table listing three ACL entries with columns for ACE, Ingress Port, Policy / Bitmask, Frame Type, Action, Rate Limiter, Port Redirect, Mirror, Counter, and action icons.

ACE	Ingress Port	Policy / Bitmask	Frame Type	Action	Rate Limiter	Port Redirect	Mirror	Counter	
1	3	Any	EType	Filter	1	Disabled	Disabled	0	⊕ ⊖ ⊕ ⊗
2	4	1 / 0x7F	IPv4/TCP FIN/RST/URG	Deny	2	Disabled	Enabled	0	⊕ ⊖ ⊕ ⊗
3	All	Any	IPv6 - NH:ICMPv6	Filter	1	Disabled	Disabled	0	⊕ ⊖ ⊕ ⊗
									⊕

## Access Control > ACL Status

This page shows the ACL status by different ACL users. Each row describes the ACE that is defined. It is a conflict if a specific ACE is not applied to the hardware due to hardware limitations. The maximum number of ACEs is 512 per switch.



The screenshot shows the Lantronix web interface for a switch (SISPM1040-3166-L3). The page title is "ACL Status". There is a navigation menu on the left with "Access Control" expanded to "ACL Status". The main content area shows a table of ACL entries. The table has the following columns: User, ACE, Ingress Port, Frame Type, Action, Rate Limiter, Port Redirect, Mirror, CPU, CPU Once, Counter, and Conflict. The table contains five rows of data:

User	ACE	Ingress Port	Frame Type	Action	Rate Limiter	Port Redirect	Mirror	CPU	CPU Once	Counter	Conflict
DMS CLIENT	1	All	IPv4/UDP 10012	Permit	Disabled	Disabled	Disabled	Yes	No	0	No
IP	1	All	IPv4 DIP:224.0.0.1/32	Permit	Disabled	Disabled	Disabled	Yes	No	0	No
static	1	3	EType	Filter	1	Disabled	Disabled	No	No	0	No
static	2	4	IPv4/TCP FIN/RST/URG	Deny	2	Disabled	Enabled	No	No	0	No
static	3	All	IPv6 - NH:ICMPv6	Filter	1	Disabled	Disabled	No	No	0	No

**User:** Indicates the ACL user (e.g., DMS CLIENT, IP, static).

**ACE:** Indicates the ACE ID on the local switch.

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

**All:** The ACE will match all ingress port.

**Port:** The ACE will match a specific ingress port.

**Frame Type:** Indicates the frame type of the ACE. Possible values are:

**Any:** The ACE will match any frame type.

**EType:** The ACE will match Ethernet Type frames. Note that an Ethernet Type based ACE will not get matched by IP and ARP frames.

**ARP:** The ACE will match ARP/RARP frames.

**IPv4:** The ACE will match all IPv4 frames.

**IPv4/ICMP:** The ACE will match IPv4 frames with ICMP protocol.

**IPv4/UDP:** The ACE will match IPv4 frames with UDP protocol.

**IPv4/TCP:** The ACE will match IPv4 frames with TCP protocol.

**IPv4/Other:** The ACE will match IPv4 frames, which are not ICMP/UDP/TCP.

**IPv6:** The ACE will match all IPv6 standard frames.

**Action:** Indicates the forwarding action of the ACE.

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

**Deny:** Frames matching the ACE are dropped.

**Filter:** Frames matching the ACE are filtered.

**Rate Limiter:** Indicates the rate limiter number of the ACE. The allowed range is 1 to 16. When Disabled is displayed, the rate limiter operation is disabled.

**Port Redirect:** Indicates the port redirect operation of the ACE. Frames matching the ACE are redirected to the port number. The allowed values are Disabled or a specific port number. When Disabled is displayed, the port redirect operation is disabled.

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

**Enabled:** Frames received on the port are mirrored.

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

**CPU:** Forward packet that 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.

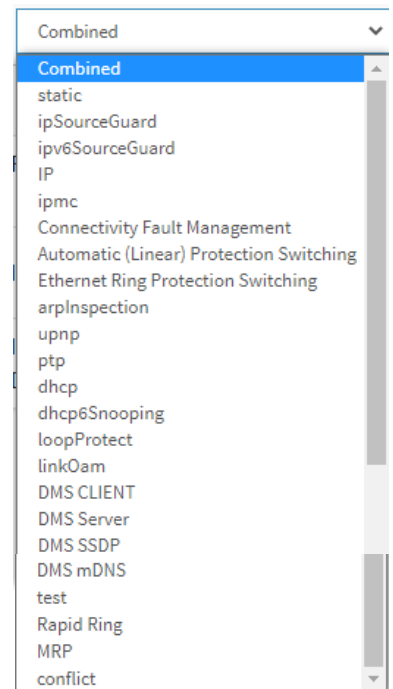
**Conflict:** Indicates the hardware status of the specific ACE. The specific ACE is not applied to the hardware due to hardware limitations.

## Buttons

**User select box:** At the dropdown select which ACL user to display. The selections are Combined, static, ipSourceGuard, ipv6SourceGuard, IP, ipmc, Connectivity Fault Management, Automatic (Linear) Protection Switching, Ethernet Ring Protection Switching, arpinspection, upnp, ptp, dhcp, dhcp6snooping, loopProtect, linkOam, DMS CLIENT, DMS Server, DMS SSDP, DMS Onvif, DMS mDNS, test, Rapid Ring, MRP, and conflict.

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

**Refresh:** Click to refresh the page.



## SNMP

SNMP (Simple Network Management Protocol) is part of the Transmission Control Protocol/Internet Protocol (TCP/IP) protocol for network management. SNMP allow diverse network objects to participate in a network management architecture. It enables network management systems to learn network problems by receiving traps or change notices from network devices implementing SNMP.

### SNMP > SNMPv1/v2c

Configure SNMPv1 and SNMPv2 on this page.

The screenshot shows the LANTRONIX web interface for the device SISPM1040-3166-L3. The main configuration area is titled 'SNMPv1/v2c Configuration'. It contains the following settings:

Mode	<input type="radio"/> off	
v1/v2c Read Community	public	Enabled
v1/v2c Write Community	private	Enabled

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

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

**on:** Enable SNMP mode operation.

**off:** Disable SNMP mode operation.

**v1/v2c Read Community:** The id that allows access to the device's data.

**v1/v2c Write Community:** The id that allows change to the device's data.

### Buttons

**Apply:** Click to save changes.

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



## SNMP > SNMPv3 > Communities

Configure SNMPv3 community table on this page. The entry index key is Community.

The screenshot shows the 'SNMPv3 Community Configuration' page in the Lantronix web interface. The page has a navigation menu on the left with options like System, Port Management, PoE Management, VLAN Management, QoS, and Spanning Tree. The main content area features a table with the following structure:

Delete	Community	Source IP	Source Mask
<input type="checkbox"/>	<input type="text"/>	<input type="text" value="0.0.0.0"/>	<input type="text" value="0.0.0.0"/>

Below the table, there are buttons for 'Add New Entry', 'Apply', and 'Reset'. The top of the page shows the device name 'SISPM1040-3166-L3' and an 'Auto-Logout' status set to 'OFF'.

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

**Community:** Indicates the security name to map the community to the SNMP Groups configuration. The allowed string length is 1 to 32, and the allowed content is ASCII characters 33-126.

**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 prefix.

**Source Mask:** Indicates the SNMP access source address network mask.

### Buttons

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

**Apply:** Click to save changes.

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

### Messages:

*The name private is not valid.*

## SNMP > SNMPv3 > Users

Configure SNMPv3 user table on this page. The entry index keys are Engine ID and User Name.

The screenshot displays the 'SNMPv3 User Configuration' page in the Lantronix web interface. The page features a navigation sidebar on the left with options like System, Port Management, PoE Management, VLAN Management, QoS, Spanning Tree, MAC Address Tables, and Multicast. The main content area shows a table with the following data:

Delete	Engine ID	User Name	Security Level	Authentication Protocol	Authentication Password	Privacy Protocol	Privacy Password
<input type="checkbox"/>	800003640300c0f27c597f	1	Auth, Priv	MD5	*****	DES	*****
<input type="checkbox"/>	800003640300c0f27c597f	2	Auth, NoPriv	SHA	*****	None	None

Below the table, there is a 'Delete' button for the selected entry, an 'Add New Entry' button, and 'Apply' and 'Reset' buttons.

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

**Engine ID:** An octet string identifying the engine ID that this entry should belong to. The string must contain an even number (in hexadecimal format) with number of digits between 10 and 64, but all-zeros and all-'F's are not allowed. The SNMPv3 architecture uses the User-based Security Model (USM) for message security and the View-based Access Control Model (VACM) for access control. For the USM entry, the `usmUserEngineID` and `usmUserName` are the entry's keys. In a simple agent, `usmUserEngineID` is always that agent's own `snmpEngineID` value. The value can also take the value of the `snmpEngineID` of a remote SNMP engine with which this user can communicate. In other words, if user engine ID 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 to 32 characters, and the allowed content is ASCII characters 33 - 126.

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

**NoAuth, NoPriv:** No authentication and no privacy.

**Auth, NoPriv:** Authentication and no privacy.

**Auth, Priv:** Authentication and privacy.

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

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

**None:** No authentication protocol.

**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 authentication protocol cannot be modified if the 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 - 40 characters. The allowed content is ASCII characters 33 - 126.

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

**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 user entry.

**Apply:** Click to save changes.

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

## SNMP > SNMPv3 > Groups

Configure up to 12 SNMPv3 groups on this page. The entry index keys are Security Model and Security Name.

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

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

**v1:** Reserved for SNMPv1.

**v2c:** Reserved for SNMPv2c.

**usm:** SNMPv3, User-based Security Model (USM).

**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.

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

### Buttons

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

**Apply:** Click to save changes.

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

### Messages:

*No available User Name, please add community or user first.*

## SNMP > SNMPv3 > Views

Configure up to 12 SNMPv3 views on this page. The entry index keys are View Name and OID Subtree.

The screenshot shows the 'SNMPv3 View Configuration' page in the Lantronix web interface. The page title is 'SNMPv3 View Configuration' and the breadcrumb is 'Home > SNMP > SNMPv3 > Views'. The interface includes a navigation menu on the left with options like System, Port Management, PoE Management, VLAN Management, QoS, Spanning Tree, MAC Address Tables, and Multicast. The main content area contains a table with the following structure:

Delete	View Name	View Type	OID Subtree
<input type="checkbox"/>	1111111	included ▼	.11
<input type="button" value="Delete"/>	<input type="text"/>	included ▼	<input type="text"/>

Below the table are buttons for 'Add New Entry', 'Apply', and 'Reset'. The 'Delete' button is located to the left of the second row of the table.

**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 it's OID subtree should overstep the 'excluded' view entry.

**OID Subtree:** The OID defining the root of the subtree to add to the named view. The allowed OID length is 1-128 characters. The allowed string content is digital number or asterisk (\*). An OID is an object identifier value, typically an address used to identify a particular device and its status.

### Buttons

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

**Apply:** Click to save changes.

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

## SNMP > SNMPv3 > Access

Configure up to 12 SNMPv3 accesses on this page. The entry index keys are Group Name, Security Model and Security Level.

The screenshot shows the 'SNMPv3 Access Configuration' page in the Lantronix web interface. The page title is 'SNMPv3 Access Configuration' and the breadcrumb is 'Home > SNMP > SNMPv3 > Access'. The interface includes a navigation menu on the left with options like System, Port Management, PoE Management, VLAN Management, QoS, Spanning Tree, MAC Address Tables, and Multicast. The main content area features a table with the following columns: Delete, Group Name, Security Model, Security Level, Read View Name, and Write View Name. Two entries are listed in the table:

Delete	Group Name	Security Model	Security Level	Read View Name	Write View Name
<input type="checkbox"/>	Grp-1	v2c	Auth, NoPriv	1111111	1111111
<input type="checkbox"/>	Grp-1	usm	Auth, Priv	1111111	1111111

Below the table are buttons for 'Add New Entry', 'Apply', and 'Reset'. The top right of the page shows 'Auto-Logout OFF' and a 'Click Save Button' link.

**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 – 32 characters, and the allowed content is ASCII characters 33 - 126.

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

**any:** Any security model accepted(v1, v2c, or usm).

**v1:** Reserved for SNMPv1.

**v2c:** Reserved for SNMPv2c.

**usm:** SNMPv3, User-based Security Model (USM).

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

**NoAuth, NoPriv:** No authentication and no privacy.

**Auth, NoPriv:** Authentication and no privacy.

**Auth, Priv:** Authentication and privacy.

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

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

### Buttons

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

**Apply:** Click to save changes.

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

## SNMP > Statistics > Configuration

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

The screenshot shows the 'RMON Statistics Configuration' page in the Lantronix web interface. The page title is 'RMON Statistics Configuration' and the breadcrumb is 'Home > SNMP > Statics > Configuration'. The device name is 'SISPM1040-3166-L3'. The page features a navigation menu on the left with options like System, Port Management, PoE Management, VLAN Management, QoS, Spanning Tree, MAC Address Tables, and Multicast. The main content area contains a table with the following data:

Delete	ID	Data Source
<input type="checkbox"/>	1	.1.3.6.1.2.1.2.2.1.1. <input type="text" value="11"/>
<input type="button" value="Delete"/>	<input type="text"/>	.1.3.6.1.2.1.2.2.1.1. <input type="text" value="0"/>

Below the table are buttons for 'Add New Entry', 'Apply', and 'Reset'. There is also an 'Auto-Logout' dropdown set to 'OFF' and a 'Click Save Button' link.

**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 is to be monitored.

### Buttons

**Add New Entry:** Click to add a new RMON statistics entry.

**Apply:** Click to save changes.

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

## SNMP > Statistics > Statistics

This page provides an overview of RMON Status entries. Each page shows up to 99 entries from the Statistics table, default being 20, selected through the "entries per page" input field. When first visited, the web page will show the first 20 entries from the beginning of the Statistics table. The first displayed will be the one with the lowest ID found in the Statistics table.

The "Start from Control Index" lets you select the starting point in the Statistics table. Clicking the Refresh button will update the displayed table starting from that or the next closest Statistics table match.

Click the Next Entry button to use the last entry of the currently displayed entry as a basis for the next lookup. When the end is reached the text "No more entries" displays in the table. Use the First Entry button to start over.

ID	Data Source (ifIndex)	Drop	Octets	Pkts	Broadcast	Multicast	CRC Errors	Under-size	Over-size	Frag.	Jabb.	Coll.	64	65 ~ 127	128 ~ 255	256 ~ 511	512 ~ 1024
1	11	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0

**ID:** Indicates the index of Statistics entry. You can click a linked ID number to display the instance's Detailed Statistics page (see below).

**Data Source (ifIndex):** The port ID which you want to be monitored.

**Drop:** The total number of events in which packets were dropped by the probe due to lack of resources.

**Octets:** The total number of octets of data (including those in bad packets) received on the network.

**Pkts:** The total number of packets (including bad packets, broadcast packets, and multicast packets) received.

**Broadcast:** The total number of good packets received that were directed to the broadcast address.

**Multicast:** The total number of good packets received that were directed to a multicast address.

**CRC Errors:** The total number of packets received that had a length (excluding framing bits but including FCS octets) of between 64 and 1518 octets, inclusive, but had either a bad Frame Check Sequence (FCS) with an integral number of octets (FCS Error) or a bad FCS with a non-integral number of octets (Alignment Error).

**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.

**64:** The total number of packets (including bad packets) received that were 64 octets in length.

**65~127:** The total number of packets (including bad packets) received that were between 65 to 127 octets in length.

**128~255:** The total number of packets (including bad packets) received that were between 128 to 255 octets in length.

**256~511:** The total number of packets (including bad packets) received that were between 256 to 511 octets in length.



**512~1023:** The total number of packets (including bad packets) received that were between 512 to 1023 octets in length.

**1024~1518:** The total number of packets (including bad packets) received that were between 1024 to 1518 octets in length.

**Buttons**

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

**Refresh:** Click to refresh the page immediately.

**First Entry:** Updates the table starting from the first entry in the Statistics table, i.e. the entry with the lowest ID.

**Next Entry:** Updates the table, starting with the entry after the last entry currently displayed.

**Detailed RMON Statistics page**

When you click a linked ID number the instance’s Detailed RMON Statistics page displays. This page provides details of a specific RMON statistics entry.

The screenshot shows the 'Detailed RMON Statistics ID 1' page. At the top, there is a navigation bar with the LANTRONIX logo, a menu icon, and a status bar showing port indicators (1-24) and a power icon. Below the navigation bar, the page title 'Detailed RMON Statistics ID 1' is displayed. On the left, there is a navigation menu with categories like System, Port Management, PoE Management, VLAN Management, QoS, Spanning Tree, MAC Address Tables, Multicast, DHCP, Security, Access Control, SNMP, and CFM. The 'SNMP' category is expanded, showing sub-items like SNMPv1/v2c, SNMPv3, Statics, Configuration, Statistics, History, Alarm, and Event. The 'Statistics' sub-item is selected. The main content area contains a table with the following data:

Receive Total	
Port	11
Drops	0
Octets	0
Pkts	0
Broadcast	0
Multicast	0
CRC/Alignment	0
Undersize	0
Oversize	0
Fragments	0
Jabber	0
Collisions	0
64 Bytes	0
65-127 Bytes	0
128-255 Bytes	0
256-511 Bytes	0
512-1023 Bytes	0
1024-1518 Bytes	0

**Port:** The port ID which wants to be monitored.

**Drop:** The total number of events in which packets were dropped by the probe due to lack of resources.

**Octets:** The total number of octets of data (including those in bad packets) received on the network.

**Pkts:** The total number of packets (including bad packets, broadcast packets, and multicast packets) received.

**Broadcast:** The total number of good packets received that were directed to the broadcast address.

**Multicast:** The total number of good packets received that were directed to a multicast address.

**CRC/Alignment:** 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.

**Fragment:** The number of frames which size is less than 64 octets received with invalid CRC.

**Jabber:** The number of frames which size is larger than 64 octets received with invalid CRC.

**Collisions:** The best estimate of the total number of collisions on this Ethernet segment.

**64:** The total number of packets (including bad packets) received that were 64 octets in length.

**65~127:** The total number of packets (including bad packets) received that were between 65 to 127 octets in length.

**128~255:** The total number of packets (including bad packets) received that were between 128 to 255 octets in length.

**256~511:** The total number of packets (including bad packets) received that were between 256 to 511 octets in length.


**512~1023:** The total number of packets (including bad packets) received that were between 512 to 1023 octets in length.

**1024~1588:** The total number of packets (including bad packets) received that were between 1024 to 1588 octets in length.

## Buttons

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

**Refresh:** Click to refresh the page immediately.

**ID Select box:** At the dropdown select the desired instance number.

## SNMP > History > Configuration

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

The screenshot shows the 'RMON History Configuration' page in the Lantronix web interface. The page title is 'RMON History Configuration' and the breadcrumb is 'Home > SNMP > History > Configuration'. The device name is 'SISPM1040-3166-L3'. The left navigation menu includes 'Switch' and 'DMS' sections. The main configuration area contains a table with the following data:

Delete	ID	Data Source	Interval	Buckets	Buckets Granted
<input type="checkbox"/>	1	.1.3.6.1.2.1.2.2.1.1. 11	1800	50	50
<input type="button" value="Delete"/>	<input type="text"/>	.1.3.6.1.2.1.2.2.1.1. 0	1800	50	

Below the table are buttons for 'Delete', 'Add New Entry', 'Apply', and 'Reset'.

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

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

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

**Interval:** Indicates the interval in seconds for sampling the history statistics data. The range is 1- 3600 seconds, and 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 buckets, and the default value is 50 buckets.

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

### Buttons

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

**Apply:** Click to save changes.

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

## SNMP > History > Status

This page provides an overview of RMON History entries. Each page shows up to 99 entries from the History table, default being 20, selected through the "entries per page" input field. When first visited, the web page will show the first 20 entries from the beginning of the History table. The first entry displayed will be the one with the lowest History Index and Sample Index found in the History table.

The "Start from History Index and Sample Index" lets you select the starting point in the History table.

**History Index:** Indicates the index of History control entry.

**Sample Index:** Indicates the index of the data entry associated with the control entry.

**Sample Start:** The value of sysUpTime at the start of the interval over which this sample was measured.

**Drop:** The total number of events in which packets were dropped by the probe due to lack of resources.

**Octets:** The total number of octets of data (including those in bad packets) received on the network.

**Pkts:** The total number of packets (including bad packets, broadcast packets, and multicast packets) received.

**Broadcast:** The total number of good packets received that were directed to the broadcast address.

**Multicast:** The total number of good packets received that were directed to a multicast address.

**CRC Errors:** The total number of packets received that had a length (excluding framing bits, but including FCS octets) of between 64 and 1518 octets, inclusive, but had either a bad Frame Check Sequence (FCS) with an integral number of octets (FCS Error) or a bad FCS with a non-integral number of octets (Alignment Error).

**Undersize:** The total number of packets received that were less than 64 octets.

**Oversize:** The total number of packets received that were longer than 1518 octets.

**Frag.:** The number of frames which size is less than 64 octets received with invalid CRC.

**Jabb.:** The number of frames which size is larger than 64 octets received with invalid CRC.

**Coll.:** The best estimate of the total number of collisions on this Ethernet segment.

**Utilization:** The best estimate of the mean physical layer network utilization on this interface during this sampling interval, in hundredths of a percent.

### Buttons

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

**Refresh:** Click to refresh the page immediately.

**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.

## SNMP > Alarm > Configuration

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

Delete	ID	Interval	Variable	Sample Type	Value	Startup Alarm	Rising Threshold	Rising Index	Falling Threshold	Falling Index
<input type="checkbox"/>	1	30	1.3.6.1.2.1.2.2.1.11.00	Delta	0	RisingOrFalling	2	1	0	0
<input type="checkbox"/>	2	30	1.3.6.1.2.1.2.2.1.21.06	Absolute	0	RisingOrFalling	4	2	3	2
<input type="checkbox"/>		30	1.3.6.1.2.1.2.2.1.0.0	Delta	0	RisingOrFalling	0	0	0	0

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

**ID:** Indicates the index of the entry. The range is from 1 to 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 (0-65535).

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

**Falling Index:** Falling event index (0-65535).

#### **Buttons**

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

**Apply:** Click to save changes.

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

#### **Messages:**

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

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

*invalid 'datasource', invalid llag*

## SNMP > Alarm > Status

This page provides an overview of RMON Alarm entries. Each page shows up to 99 entries from the Alarm table, default being 20, selected through the "entries per page" input field. When first visited, the web page 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.

ID	Interval	Variable	Sample Type	Value	Startup Alarm	Rising Threshold	Rising Index	Falling Threshold	Falling Index
1	30	.1.3.6.1.2.1.2.2.1.11.10	Delta	0	RisingOrFalling	2	1	0	0
2	30	.1.3.6.1.2.1.2.2.1.21.26	Absolute	0	RisingOrFalling	4	2	3	2

**ID:** Indicates the index of Alarm control entry.

**Interval:** Indicates the interval in seconds for sampling and comparing the rising and falling threshold.

**Variable:** Indicates the particular variable to be sampled

**Sample Type:** The method of sampling the selected variable and calculating the value to be compared against the thresholds.

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

**Startup Alarm:** The alarm that may be sent when this entry is first set to valid.

**Rising Threshold:** Rising threshold value.

**Rising Index:** Rising event index.

**Falling Threshold:** Falling threshold value.

**Falling Index:** Falling event index.

### Buttons

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

**Refresh:** Click to refresh the page immediately.

**First Entry:** Updates the table starting from the first entry in the Alarm Table, i.e. the entry with the lowest ID.

**Next Entry:** Updates the table, starting with the entry after the last entry currently displayed.

## SNMP > Event > Configuration

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

The screenshot shows the 'RMON Event Configuration' page in the Lantronix web interface. The page title is 'RMON Event Configuration' and the breadcrumb is 'Home > SNMP > Event > Configuration'. The interface includes a navigation menu on the left with options like System, Port Management, PoE Management, VLAN Management, QoS, Spanning Tree, MAC Address Tables, Multicast, and DHCP. The main content area contains a table with the following data:

Delete	ID	Desc	Type	Event Last Time
<input type="checkbox"/>	1	one	log	0
<input type="checkbox"/>	2	two	snmptrap	0
<input type="checkbox"/>	3	three	logandtrap	0

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

**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.

**Desc:** Indicates 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 and no SNMP trap is sent.

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

**snmptrap:** Send SNMP trap when the event is triggered.

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

**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 RMON event entry.

**Apply:** Click to save changes.

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



## SNMP > Event > Status

This page provides an overview of RMON Event table entries. Each page shows up to 99 entries from the Event table, default being 20, selected through the "entries per page" input field. When first visited, the web page will show the first 20 entries from the beginning of the Event table. The first entry displayed will be the one with the lowest Event Index and Log Index found in the Event table.

The "Start from Control Index" and "Sample Index" let you select the starting point in the Event table.

The screenshot displays the 'RMON Event Overview' page in the Lantronix web interface. At the top, the device name 'SISPM1040-3166-L3' is shown, along with an 'Auto-Logout' dropdown menu set to 'OFF'. A navigation menu on the left lists various system functions like System, Port Management, PoE Management, VLAN Management, QoS, and Spanning Tree. The main content area features a breadcrumb trail 'Home > SNMP > Event > Status' and a table of event entries. The table has columns for 'Event Index', 'LogIndex', 'LogTime', and 'LogDescription'. The current view shows 'No more entries'.

**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 refresh the page immediately.

**First Entry:** Updates the table starting from the first entry in the Event Table, i.e. the entry with the lowest Event Index and Log Index.

**Next Entry:** Updates the table, starting with the entry after the last entry currently displayed.

## CFM

Connectivity Fault Management (CFM) is a standard defined by IEEE802.1ag. It defines protocols and practices for OAM (Operations, Administration, and Maintenance) and is largely identical with ITU-T Recommendation Y.1731.

### CFM > Global

Configure CFM Global Configuration parameters on this page.

The screenshot shows the 'CFM Global Configuration' page in the Lantronix web interface. The page includes a navigation menu on the left with 'CFM > Global' selected. The main content area has an 'Auto-refresh' toggle set to 'off' and a 'Refresh' button. Below this is a table of configuration parameters:

Sender Id TLV	None
Port Status TLV	Enable
Interface Status TLV	Disable
Organisation Specific TLV	Disable
Organisation Specific TLV OUI	000000
Organisation Specific TLV Subtype	0
Organisation Specific TLV Value	

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

**Sender Id TLV:** Choose whether and what to use as Sender ID TLVs in CCMs generated by this switch. Can be overridden by Domain and Service level configuration. Can be **None**, **Chassis**, **Manage**, or **ChassisManage**.

**Port Status TLV:** Choose whether to send Port Status TLVs in CCMs generated by this switch. Can be overridden by Domain and Service level configuration.

**Enable:** Send Port Status TLVs in CCMs generated by this switch.

**Disable:** Do not send Port Status TLVs in CCMs generated by this switch.

**Interface Status TLV:** Choose whether to send Interface Status TLVs in CCMs generated by this switch. Can be overridden by Domain and Service level configuration.

**Enable:** Send Interface Status TLVs in CCMs generated by this switch.

**Disable:** Do not Send Interface Status TLVs in CCMs generated by this switch.

**Organisation Specific TLV:** Choose whether to send Organisation Specific TLVs in CCMs generated by this switch. Can be overridden by Domain and Service level configuration.

**Enable:** Send Organisation Specific TLVs in CCMs generated by this switch.

**Disable:** Do not send Organisation Specific TLVs in CCMs generated by this switch.

**Organisation Specific TLV OUI:** This is the three-bytes OUI transmitted with the Organization-Specific TLVs. Enter as 6 characters 0-9, a-f.

**Organisation Specific TLV Subtype:** This is the subtype transmitted with the Organization-Specific TLV. Can be any value in range [0; 255]

**Organisation Specific TLV Value:** This is the value transmitted in the Organization-Specific TLVs. Value is a printable character string of length 0-63.

### Buttons

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

**Refresh:** Click to refresh the page immediately.

**Apply:** Click to save changes.

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

### Example:

The screenshot shows the Lantronix web interface for device SISPM1040-3166-L3. The left sidebar contains a navigation menu with categories like System, Port Management, PoE Management, VLAN Management, QoS, Spanning Tree, MAC Address Tables, Multicast, DHCP, Security, Access Control, and SNMP. The 'CFM' category is expanded to show 'Global'. The main content area is titled 'CFM Global Configuration' and includes an 'Auto-refresh' toggle set to 'off' with a 'Refresh' button. Below this is a configuration table with the following fields:

Sender Id TLV	ChassisManage
Port Status TLV	Enable
Interface Status TLV	Enable
Organisation Specific TLV	Enable
Organisation Specific TLV OUI	000000
Organisation Specific TLV Subtype	1
Organisation Specific TLV Value	11-22-33-44

At the bottom of the configuration area are 'Apply' and 'Reset' buttons. The top of the interface features a LANTRONIX logo, a port status indicator (ports 1-22), an 'Auto-Logout' dropdown set to 'OFF', and a 'Click Save Button' link.

## CFM > Domain

Configure CFM Domain parameters on this page.

The screenshot shows the 'CFM Domain Configuration' page in the Lantronix web interface. The page title is 'CFM Domain Configuration' and the breadcrumb is 'Home > CFM > Domain'. The interface includes a navigation menu on the left with options like System, Port Management, PoE Management, VLAN Management, QoS, Spanning Tree, MAC Address Tables, Multicast, DHCP, and Security. The main configuration area has an 'Auto-refresh' toggle set to 'off' and a 'Refresh' button. Below this is a table with columns for 'Delete', 'Domain', 'Format', 'Name', 'Level', and 'TLV option select'. The 'TLV option select' column has sub-columns for 'Sender Id', 'Port Status', 'Interface Status', and 'Org. Specific'. Two entries are shown: 'domain1' with level 2 and 'domain2' with level 0. At the bottom of the table are 'Add New Entry', 'Apply', and 'Reset' buttons.

Delete	Domain	Format	Name	Level	TLV option select			
					Sender Id	Port Status	Interface Status	Org. Specific
*		<input type="text" value=""/>		<input type="text" value=""/>	<input type="text" value=""/>	<input type="text" value=""/>	<input type="text" value=""/>	<input type="text" value=""/>
<input type="checkbox"/>	domain1	String	DEFAULT	2	Manage	Enable	Enable	Defer
<input type="checkbox"/>	domain2	None		0	ChassisManage	Enable	Disable	Defer

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

**Domain:** Name of Domain. Value is a single word which begins with an alphabetic letter A-Z or a-z with a length of 1-15 characters.

**Format:** Select the MD name format. To mimic Y.1731 MEG IDs, use type **None**.

**None:** If format is None: Name is not used but will be set to all-zeros behind the scenes. This format is typically used by Y.1731-kind-of-PDUs.

**String:** If format is String, the Name must contain a string 1-43 characters long.

**Name:** The contents of this parameter depend on the value of the format member.

**Level:** MD/MEG level of this domain. Valid values are 0 - 7.

**About leak prevention:** Leak prevention is about discarding OAM PDUs with MEG levels lower than the MEP they hit when the OAM PDUs are ingressing the port on which the MEP resides, and to discard OAM PDUs with MEG levels at or lower than the MEP's when the OAM PDUs are ingressing other ports.

There are two categories of architectures, when it comes to leak-prevention: Those that use Shared MEG level and those that use Independent MEG level:

**Shared MEG level:** On Shared MEG level architectures, Port Down MEPs always perform level filtering no matter which VLAN ID (VID) OAM PDUs get classified to, unless the same port has a VLAN MEP on the VID in question. So if you have a Port MEP in VID X and a VLAN MEP in VID Y, an OAM frame arriving on the port and gets classified to VID X or VID Z will be handled/level-filtered by the Port MEP, whereas an OAM frame ingressing the port in VID Y will be handled by the VLAN MEP. Likewise, if the switch has a Port MEP on VID X on Port X and an OAM frame ingresses on VID Y on Port Y, it is subject to level filtering before egressing Port X, unless Port X also has a VLAN MEP on VID Y, in which case the VLAN MEP will take care of level-filtering the OAM PDU.

On Shared MEG level architectures, all Port MEPs must have the same MEG level and any VLAN MEP must have a MEG level higher than the Port MEPs' MEG level.

**Independent MEG level:** On Independent MEG level architectures, Port Down MEPs never perform level filtering on frames not classified to the MEP's VID. So if you have a Port MEP on VID X and a VLAN MEP on VID Y and an OAM frame ingresses any port on VID Z, it is not subject to handling/level-filtering by either of the two MEPs.

**This switch exhibits Independent MEG level.**

**TLV option select:**

**Sender Id:** Select the default Sender ID TLV format to be used in CCMs generated by this Domain (may be overridden in service).

**None:** Do not include Sender ID TLVs.

**Chassis:** Enable Sender ID TLV and send Chassis ID (MAC Address).

**Manage:** Enable Sender ID TLV and send Management address (IPv4 Address).

**ChassisManage:** Enable Sender ID TLV and send both Chassis ID (MAC Address) and Management Address (IPv4 Address).

**Defer:** Let the global configuration decide if Sender ID TLVs will be included (may be overridden in service).

**Port Status:** Include or exclude Port Status TLV in CCMs generated by this Domain or let higher level determine (may be overridden in Service).

**Disable:** Do not include Port Status TLVs.

**Enable:** Include Port Status TLVs.

**Defer:** Let the global configuration decide if Port Status TLVs will be included (may be overridden in Service).

**Interface Status:** Include or exclude Interface Status TLV in CCMs generated by this Domain or let higher level determine (may be overridden in Service).

**Disable:** Do not include Interface Status TLVs.

**Enable:** Include Interface Status TLVs.

**Defer:** Let the global configuration decide if Interface Status TLVs will be included (may be overridden in Service).

**Org. Specific:** Exclude Organization-Specific TLV in CCMs generated by this Domain or let higher level determine (may be overridden in Service).

**Disable:** Do not include Organization-Specific TLVs.

**Defer:** Let the global configuration decide if Organization-Specific TLVs will be included (may be overridden in Service).

**Buttons**

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

**Refresh:** Click to refresh the page immediately.

**Add New Entry:** Click to add a new Domain entry.

**Apply:** Click to save changes.

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

## CFM > Service

Configure CFM Service parameters on this page.

The screenshot shows the 'CFM Service Configuration' page in the Lantronix web interface. The page title is 'SISPM1040-3166-L3'. The left navigation menu includes System, Port Management, PoE Management, VLAN Management, QoS, Spanning Tree, MAC Address Tables, Multicast, and DHCP. The main content area has an 'Auto-refresh' toggle set to 'off' and a 'Refresh' button. Below this is a table with the following columns: Delete, Domain, Service, Format, Name, VLAN, CCM Interval, and TLV option select (Sender Id, Port Status, Interface Status, Org. Specific). The table contains two entries:

Delete	Domain	Service	Format	Name	VLAN	CCM Interval	TLV option select
<input type="checkbox"/>	domain1	Svc1	PrimaryVid	CfmDom1	10	10 ms	Sender Id: Chassis, Port Status: Enable, Interface Status: Enable, Org. Specific: Defer
<input type="checkbox"/>	domain2	svc2	Y1731 ICC	CfmDom2	1	300 Hz	Sender Id: ChassisManage, Port Status: Enable, Interface Status: Enable, Org. Specific: Disable

At the bottom of the table are buttons for 'Add New Entry', 'Apply', and 'Reset'.

**Delete:** Check to delete the entry during the next save.

**Domain:** Name of Domain under which this Service resides.

**Service:** Name of Service. Value is a single word which begins with an alphabetic letter A-Z or a-z with length 1-15.

**Format:** Select the short Service name format. This decides how the value of the Name parameter will be interpreted. To mimic Y.1731 MEG IDs, create an MD instance with an empty name and use Y1731 ICC or Y1731 ICC CC. Possible values are: **String**, **Two Octets**, **Y1731 ICC**, and **Y1731 ICC CC**. See the Name parameter below for explanations.

**Name:** The contents of this parameter depend on the value of the format member. Besides the limitations explained for each of them, the following applies in general:

If the Domain Format is **None**, the size of this cannot exceed 45 bytes.

If the Domain Format is not **None**, the size of this cannot exceed 44 bytes.

If Format is **String**, the following applies: length must be in the range [1; 44], and the Contents must be in range [32; 126].

If Format is **Two Octets**, the following applies: Name[0] and Name[1] will both be interpreted as unsigned 8-bit integers (allowing a range of [0; 255]). Name[0] will be placed in the PDU before Name[1]. The remaining available bytes in name will not be used.

If Format is **Y1731 ICC**, the following applies: length must be 13, and Contents must be in range [a-z,A-Z,0-9]. Y.1731 specifies that it is a concatenation of ICC (ITU Carrier Code) and UMC (Unique MEG ID Code): ICC: 1-6 bytes and UMC: 7-12 bytes.

In principle UMC can be any value in range [1; 127], but this API does not allow for specifying length of ICC, so the underlying code doesn't know where ICC ends and UMC starts.

The Domain Format must be **None**.

If Format is **Y1731 ICC CC**, the following applies: Length must be 15.

First 2 chars (CC): Must be amongst [A-Z]. Next 1-6 chars (ICC): Must be amongst [a-z,A-Z,0-9].

Next 7-12 chars (UMC): Must be amongst [a-z,A-Z,0-9]. There may be ONE (slash) present in name[3-7].

The Domain format must be **None**.

**VLAN:** The MA's primary VID. A primary VID of 0 means that all MEPs created within this MA will be created as port MEPs (interface MEPs). There can only be one port MEP per interface. A given port MEP may still be created with tags, if that MEP's VLAN is non-zero.

A non-zero primary VID means that all MEPs created within this MA will be created as VLAN MEPs. A given MEP may be configured with another VLAN than the MA's primary VID, but it is impossible to have untagged VLAN MEPs.

**CCM Interval:** The CCM rate of all MEPs bound to this Service.

**TLV option select:**

**Sender Id:** Default Sender ID TLV format to be used in CCMs generated by this Service.

**None:** Do not include Sender ID TLVs.

**Chassis Enable:** Sender ID TLV and send Chassis ID (MAC Address).

**Manage Enable:** Sender ID TLV and send Management address (IPv4 Address).

**ChassisManage Enable:** Sender ID TLV and send both Chassis ID (MAC Address) and Management Address (IPv4 Address).

**Defer:** Let the Domain configuration decide if Sender ID TLVs will be included.

**Port Status:** Include or exclude Port Status TLV in CCMs generated by this Service or let higher level determine.

**Disable:** Do not include Port Status TLVs.

**Enable:** Include Port Status TLVs.

**Defer:** Let the Domain configuration decide if Port Status TLVs will be included.

**Interface Status:** Include or exclude Interface Status TLV in CCMs generated by this Service or let higher level determine.

**Disable:** Do not include Interface Status TLVs.

**Enable:** Include Interface Status TLVs.

**Defer:** Let the Domain configuration decide if Interface Status TLVs will be included.

**Org. Specific:** Exclude Organization-Specific TLV in CCMs generated by this Service or let higher level determine.

**Disable:** Do not include Organization-Specific TLVs.

**Defer:** Let the Domain configuration decide if Organization-Specific TLVs will be included.

**Buttons**

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

**Refresh:** Click to refresh the page immediately.

**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:**

*Service cannot be empty*

*JSON RPC Error. (Invalid MA name length. It must be exactly 13 characters long)*

*JSON RPC Error. (Invalid params)*

## CFM > MEP

Configure CFM MEP parameters on this page. This switch supports two types of MEP: Port Down-MEPs and VLAN Down-MEPs.

**Port Down-MEPs:** In 802.1Q terminology, Port MEPs are located below the EISS entity, that is, closest to the physical port. Port MEPs are used by e.g., APS for protection purposes.

Port MEPs are created when the encompassing service has type "Port".

Port MEPs may send OAM PDUs tagged or untagged. An OAM PDU will be sent untagged only if the MEP's VLAN is set to "Inherit" (0). Any other value will cause it to be sent tagged with the port's TPID, whether or not the VLAN matches the port's PVID and that PVID is meant to be sent untagged.

**VLAN Down-MEPs:** In 802.1Q terminology, VLAN MEPs are located above the EISS entity.

This means that tagging of OAM PDUs will follow the port's VLAN configuration.

Thus, if a VLAN MEP is created on the Port's PVID and PVID is configured to be untagged, OAM PDUs will be transmitted untagged.

VLAN MEPs are created when the encompassing service has type "VLAN".

**Down-MEP creation rules:** There are a few rules to obey when creating Down-MEPs:

1. There can only be one Port MEP on the same port.
2. There can only be one VLAN MEP on the same port and VLAN.
3. A VLAN MEP must have a higher MD/MEG level than a Port MEP on the same port and VLAN.

These checks are performed automatically on administratively enabled MEPs when you change a particular MEP, change the Service Type from Port to VLAN or vice versa, or change the domain's MD/MEG level.

The screenshot shows the 'CFM Mep Configuration' page in the Lantronix web interface. The page title is 'SISPM1040-3166-L3'. The left navigation menu includes 'Switch' and 'DMS'. The main content area has an 'Auto-refresh' toggle set to 'off' and a 'Refresh' button. Below this is a table with the following columns: Delete, Domain, Service, MEPID, Direction, Port, VLAN, PCP, SMAC, Alarm Control (Level, Present, Absent), State Control (CCM, Admin), and Remote MEPID. The table contains one entry with the following values: Delete (Delete button), Domain (Select Service), Service (dropdown), MEPID (1), Direction (Down), Port (1), VLAN (1), PCP (0), SMAC (00:00:00:00:00:00), Alarm Control (Level: 2, Present: 2500, Absent: 10000), State Control (CCM: checked, Admin: unchecked), and Remote MEPID (0). There are also 'Add New Entry', 'Apply', and 'Reset' buttons at the bottom of the table.

### Parameter Descriptions:

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

**Domain:** Name of Domain under which this MEP resides.

**Service:** Name of Service under which this MEP resides.

**MEPID:** The identification of this MEP. Must be an integer [1..8091]

**Direction:** Set whether this MEP is an Up-MEP or a Down-MEP.

**Port:** Port on which this MEP resides.

**VLAN:** VLAN ID. Use the value 0 to indicate untagged traffic (implies a port MEP).

**PCP:** Choose PCP value in PDUs' VLAN tag. Not used if untagged.

**SMAC:** Set a Source MAC address to be used in CCM PDUs originating at this MEP. Must be a unicast address. Format is XX:XX:XX:XX:XX:XX. If all-zeros, the switch port's MAC address will be used instead.



**Alarm Control:** Level: If a defect is detected with a priority higher than this level, a fault alarm notification will be generated. Valid range is [1; 6] with **1** indicating that any defect will cause a fault alarm and **6** indicating that no defect can cause a fault alarm. See 802.1Q-2018, clause 20.9.5, *LowestAlarmPri*.

The possible defects and their priorities are:

<u>Short name</u>	<u>Description</u>	<u>Priority</u>
DefRDICCM	Remote Defect Indication	1
DefMACstatus	MAC Status	2
DefRemoteCCM	Remote CCM	3
DefErrorCCM	Error CCM Received	4
DefXconCCM	Cross Connect CCM Received	5

**Present:** The time in milliseconds that defects must be present before a fault alarm notification is issued. Default is 2500 ms.

**Absent:** The time in milliseconds that defects must be absent before a fault alarm notification is reset. Default is 10000 ms.

**State Control:** Check or uncheck these checkboxes:

**CCM:** Enable or disable generation of continuity-check messages (CCMs).

**Admin:** Enable or disable this MEP. When this MEP is enabled, it will check received/missing CCMs and can raise defects.

**Remote MEPID:** Specify the Remote MEP that this MEP is expected to receive CCM PDUs from. Must be an integer [0..8091] where 0 means undefined. The value of Remote MEPID must be different from the value of MEPID.

## Buttons

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

**Refresh:** Click to refresh the page immediately.

**Add New Entry:** Click to add a new MEP entry.

**Apply:** Click to save changes.

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

## Messages:

*AlarmPresentMs must be an integer value between 2500 and 10000*

*JSON RPC Error. (A Remote MEP-ID cannot be identical to this MEP's MEP-ID)*

*JSON RPC Error. (There can only be one Port MEP per interface, and another Port MEP already exists on this one)*

*MAC address must be 12 characters long*

*JSON RPC Error. (Invalid params)*

**Example:**

SISPM1040-3248-L3

Switch DMS

CFM Mep Configuration

Auto-refresh  Refresh

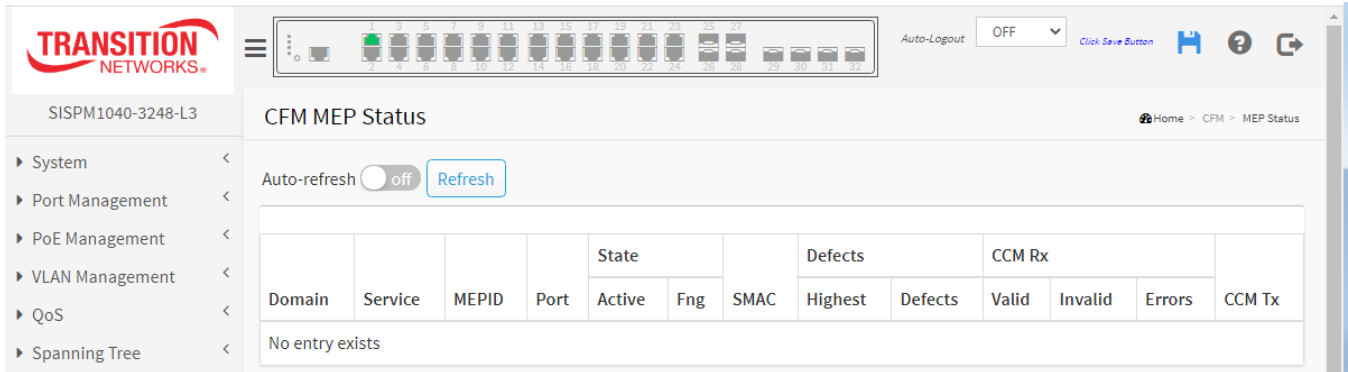
Delete	Domain	Service	MEPID	Direction	Port	VLAN	PCP	SMAC	Alarm Control			State Control		Remote MEPID
									Level	Present	Absent	CCM	Admin	
*				...	...		...		...			<input type="checkbox"/>	<input type="checkbox"/>	
<input type="checkbox"/>	domain1	Svc1	1	Down	2	30	0	000000000000	1	2500	10000	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	11
<input type="checkbox"/>	domain1	Svc1	20	Down	5	30	3	000000000000	3	2500	10000	<input checked="" type="checkbox"/>	<input type="checkbox"/>	33
<input type="checkbox"/>	domain1	c	10	Down	3	20	1	000000000000	2	2500	10000	<input type="checkbox"/>	<input checked="" type="checkbox"/>	22
<input type="checkbox"/>	domain1	w	10	Down	3	1	2	000000000000	6	2500	10000	<input checked="" type="checkbox"/>	<input type="checkbox"/>	0
<input type="checkbox"/>	domain1	w	10	Down	3	1	2	000000000000	6	2500	10000	<input checked="" type="checkbox"/>	<input type="checkbox"/>	0

Buttons: Delete, Select Service, domain1:Svc1

Buttons: Add New Entry, Apply, Reset

## CFM > MEP Status

View CFM MEP Status on this page.



**Domain:** Name of Domain under which this MEP resides.

**Service:** Name of Service under which this MEP resides.

**MEPID:** The identification of this MEP.

**Port:** Port on which this MEP resides.

**State:** The current state:

**Active** Operational state of the MEP:

- **off** : OFF. This indicates that the MEP Admin State is disabled.
- **down** : DOWN. The MEP Admin State is enabled, but an error state exists.
- **up** : UP. The MEP Admin State is enabled, and no errors and defects exist.

**Fng** : The current state of the Fault Notification Generator State Machine. Value will be one of these:

State	Description
<b>reset</b>	No defect has been present since reset timer expired or the State Machine was last reset.
<b>defect</b>	A defect is present, but not for a long enough time to be reported.
<b>reportDefect</b>	A transient state during which the defect is reported.
<b>defectReported</b>	A defect is present, and some defect has been reported.
<b>defectClearing</b>	No defect is present, but the ResetTime timer has not yet expired.

**SMAC:** This MEP's MAC address.

**Defects** : A MEP can detect and report a number of defects, and multiple defects can be present at the same time. This is indicated by one of the following letter codes.

Code	Defect	Description
-	Defect not present	No Defect present.
<b>R</b>	someRDIdefect	RDI received from at least one remote MEP.
<b>M</b>	someMACstatusDefect	Received Port Status TLV != psUp or Interface Status TLV != isUp.
<b>C</b>	someRMEPCCMdefect	Valid CCM is not received within 3.5 times CCM interval from at least one remote MEP.
<b>E</b>	errorCCMdefect	Received CCM from an unknown remote MEP-ID or CCM interval mismatch.
<b>X</b>	xconCCMdefect	Received CCM with an MD/MEG level smaller than configured or wrong MAID/MEGID (cross-connect).

**CCM Rx:** Can be one of these values:

**Valid:** Total number of CCMs that hit this MEP and passed the validation test.

**Invalid:** Total number of CCMs that hit this MEP and didn't pass the validation test.

**Errors:** Total number of out-of-sequence errors seen from RMEPs.

**CCM Tx:** Total number of CCM PDUs transmitted by this MEP.

**Buttons**

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

**Refresh:** Click to manually refresh the page immediately.

**Add New Entry:** Click to add a new CFM MEP entry to the table.

**Apply:** Click to save changes.

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

**Example:**

The screenshot shows the 'CFM MEP Status' page for device 'SISPM1040-3248-L3'. It includes a navigation menu on the left with categories like System, Port Management, PoE Management, VLAN Management, QoS, Spanning Tree, MAC Address Tables, and Multicast. The main content area has an 'Auto-refresh' toggle set to 'off' and a 'Refresh' button. Below is a table with the following data:


Domain	Service	MEPID	Port	State		SMAC	Defects		CCM Rx			CCM Tx
				Active	Fng		Highest	Defects	Valid	Invalid	Errors	
domain1	Svc1	1	1	●	reset	00:00:00:00:00:99	none	- - - -	0	0	0	0
domain1	Svc1	20	5	●	reset	00:C0:F2:7C:58:97	none	- - - -	0	0	0	0
domain1	c	10	3	●	reset	00:C0:F2:7C:58:95	none	- - - -	0	0	0	0
domain1	w	10	4	●	reset	CC:00:00:00:00:00	none	- - C - -	0	0	0	126

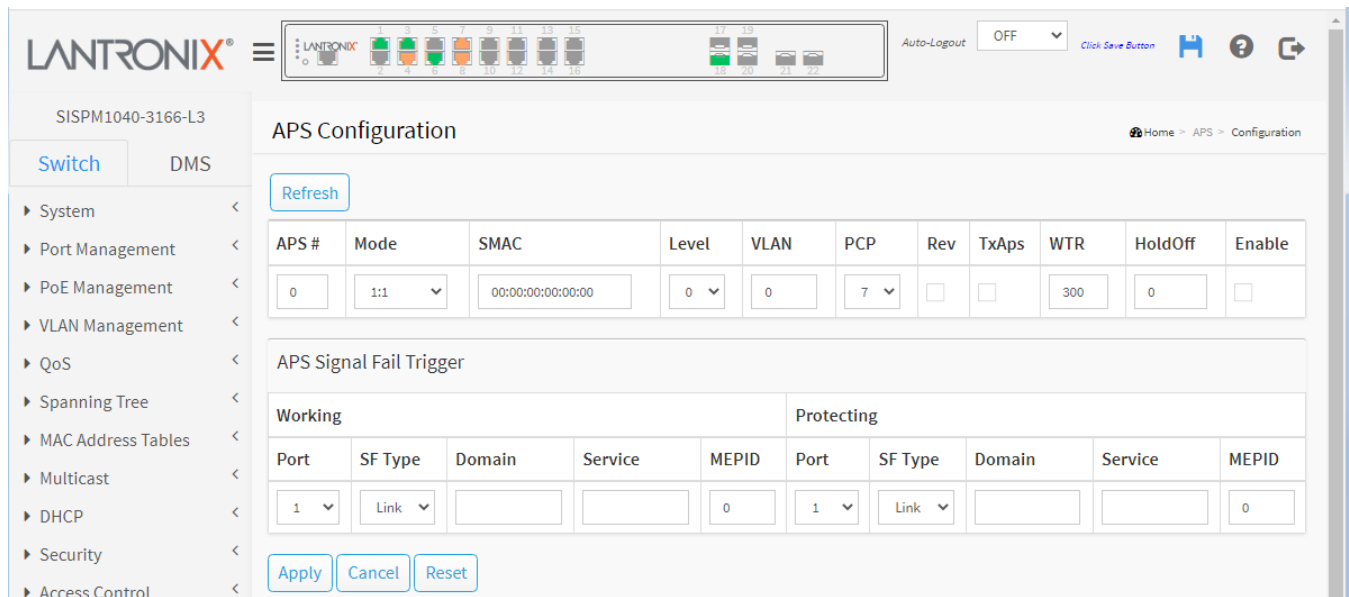
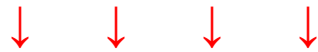
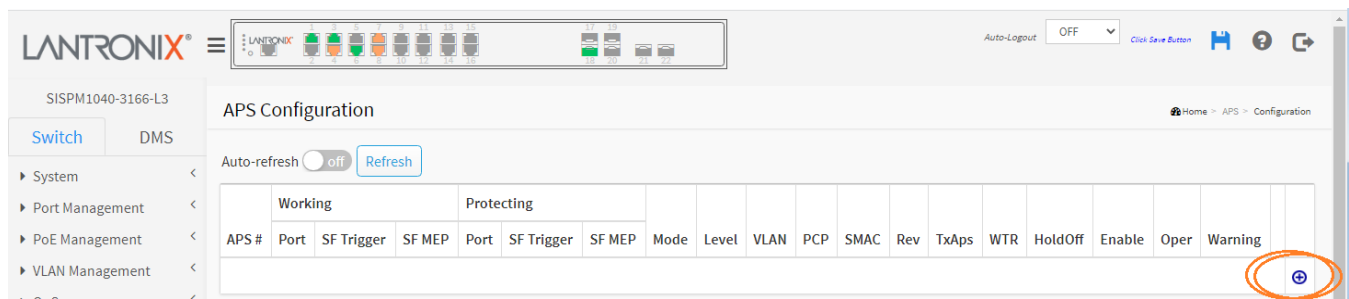
# APS

The APS module implements the protocol and linear protection switching mechanisms for point-to-point VLAN-based ETH SNC (Subnetwork Connections) in Ethernet transport networks. The APS (Automatic Protection Switching) protocol is used to ensure that switching is done bidirectionally in the two ends of a protection group, as defined in ITU-T G.8031.

This Recommendation specifies linear 1+1 protection switching architecture and linear 1:1 protection switching architecture. The linear 1+1 protection switching architecture operates with either unidirectional or bidirectional switching. The linear 1:1 protection switching architecture operates with bidirectional switching.

## APS Configuration

This page lets you create and configure an APS Instance. From the default page, click the  button to display the APS Configuration table.



### Configuration Data

**APS #:** The ID of the APS (1-32). You can create 1-32 APS instances. Click on the link to get to the APS instance page, where you can reset counters and issue commands.

**Port:** The Port this flow is attached to.

**SF Trigger:** Selects whether Signal Fail (SF) comes from the link state of a given Port, or from a Down-MEP.

**SF MEP:** The Domain::Service::MEPID (e.g., Dom3::Svc3::2) refers to a MEP instance which shall represent the Working flow. Only used when SF Trigger is MEP. The selected MEP instance does not need to exist when this APS is configured.

**Mode:** At the dropdown select 1:1, 1+1 Uni, or 1+1 Bi:

**1:1 :** This will create a 1:1 APS. In the linear 1:1 protection switching architecture, the protection transport entity is dedicated to the working transport entity. However, the normal traffic is transported either on the working transport entity or on the protection transport entity using a selector bridge at the source of the protected domain. The selector at the sink of the protected domain selects the entity which carries the normal traffic.

**1+1 Uni :** This will create a 1+1 Unidirectional APS.

**1+1 Bi :** This will create a 1+1 Bidirectional APS.

In linear 1+1 protection switching architecture, a protection transport entity is dedicated to each working transport entity. Normal traffic is copied and fed to both working and protection transport entities with a permanent bridge at the source of the protected domain. The traffic on working and protection transport entities is transmitted simultaneously to the sink of the protected domain, where a selection between the working and protection transport entities is made based on some predetermined criteria, such as server defect indication.

**Level:** MD/MEG Level (0-7).

**VLAN:** The VLAN ID used in the L-APS PDUs. 0 means untagged.

**PCP:** PCP (priority) (default 7). The PCP value used in the VLAN tag unless the L-APS PDU is untagged. Must be a value in range 0 - 7.

**SMAC:** Source MAC address used in L-APS PDUs. Must be a unicast address. If all-zeros, the switch port's MAC address will be used.

**Rev:** When checked (✓) the port recovery mode is revertive, that is, traffic switches back to the working port after the condition(s) causing a switch has cleared. In the case of clearing a command (e.g., forced switch), this happens immediately. In the case of clearing of a defect, this generally happens after the expiry of the WTR (Wait-To-Restore) timer.

When unchecked (✗) the port recovery mode is non-revertive and traffic is allowed to remain on the protect port after a switch reason has cleared.

**TxAps:** Choose whether this end transmits APS PDUs. Only used for 1+1 Unidirectional (1+1 Uni).

**WTR:** When Rev is checked, WTR (Wait-To-Restore) tells how many seconds to wait before restoring to the working port after a fault condition has cleared. Valid range 1 - 720

**HoldOff:** When a new (or more severe) defect occurs, the hold-off timer will be started, and the event will be reported after the timer expires. HoldOff time is measured in milliseconds, and valid values are 0 - 10000. The default is 0, which means immediate reporting of the defect.

**Enable:** The administrative state of this APS instance. Check to make it function normally and uncheck to make it cease functioning.

**Oper:** This field cannot be configured but it shows the operational state. You can click on the link in the APS # field to get more details on the status.

● (up) : The APS instance is functional.




● (down) : The APS instance is not functional.

**Warning:** If the operational state is Active, the APS instance is indeed active, but it may be that it doesn't run as the administrator thinks, because of configuration errors, which are reflected in the warnings below.

The Warning information is indicated by ●: no warning or ●: warning.

Use the tooltip to get detailed warning information (e.g., "No warnings. If operational state is Active, everything is fine" or "Working MEP is not found. Using link-state for SF instead").

**Configuration Buttons:** You can modify each APS in the table using these buttons:

-  **Edit:** Edit the APS row.
-  **Delete:** Delete the APS row.
-  **Add:** Add a new APS row.

**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.

**Messages:**

- JSON RPC Error. (Invalid hold-off-time. Valid range is [0; 10000] milliseconds in steps of 100 milliseconds)*
- APS # must be an integer value between 1 and 32*
- JSON RPC Error. (Working and protect ports cannot use the same interface)*
- Working Domain must not contain leading digit*
- Working Domain cannot be empty*
- Working Service must not contain leading digit*
- Protecting Domain must not contain leading digit*
- JSON RPC Error. (Another APS instance is using the same working port interface as this one)*

**APS Configuration Example:** APS # 1, 2, and 3 configured and saved.

APS #	Working			Protecting			Mode	Level	VLAN	PCP	SMAC	Rev	TxAbs	WTR	HoldOff	Enable	Oper	Warning		
	Port	SF Trigger	SF MEP	Port	SF Trigger	SF MEP														
1	1	Link		1	Link		1:1	0	0	7	00:00:00:00:00:00	X	X	300	0	X	●	●		
2	1	Link		1	Link		1+1 Uni	0	0	7	00:00:00:00:00:00	X	X	300	0	X	●	●		
3	1	Link		4	Link		1+1 Bi	2	0	4	00:00:00:00:00:00	✓	✓	300	200	✓	●	●		

## APS Instance Page

You can click on the linked APS # to display the APS Status page for the selected instance. This page lets you reset counters and issue commands.

The screenshot displays the Lantronix web interface for the APS Status page. The page title is 'APS Status' and the breadcrumb is 'Home > APS > Status'. The left navigation menu includes System, Port Management, PoE Management, VLAN Management, QoS, Spanning Tree, MAC Address Tables, Multicast, DHCP, Security, Access Control, SNMP, CFM, APS (selected), ERPS, Rapid Ring, MRP, and BTD. The main content area shows the configuration and status for APS instance 1.

**Configuration Table:**

APS #	Working			Protecting			Mode	Level	VLAN	PCP	Rev	TxAps	WTR	HoldOff	Enable
	Port	SF Trigger	SF MEP	Port	SF Trigger	SF MEP									
1	1	Link		1	Link		1:1	0	0	7	×	×	300	0	×

**Status Table:**

State	Defect state			TxAps			RxAps			Dfop				RxCnt				
	Warning	Protection	Working	Protecting	Request	ReSignal	BrSignal	Request	ReSignal	BrSignal	CM	PM	NR	TO	SMAC	TxCnt	Valid	Invalid
Administratively disabled	●	-	-	-	-	-	-	-	-	-	●	●	●	●	-	-	-	-

The page also includes an 'Auto-refresh' toggle (off) and a 'Refresh' button. Below the status table is a 'Reset Counters' button and a 'Command' section with a dropdown menu set to 'noRequest' and 'Apply', 'Reset', and 'Back' buttons.

**Configuration:** This section shows the current configuration for this APS instance. Go to the APS Configuration page for further explanation.

**Status:** This section shows the current status of the APS instance. If the Operational state is not "Active", the remaining fields are invalid.

**State, Operational:** The operational state of the APS instance. There are many ways to not have the instance active. Each of them has its own value. Only when the state is Active, will the APS instance be active and up and running. The possible values of this field are listed below:

**Administratively disabled:** Instance is inactive because it is administratively disabled.

**Active:** The instance is active and up and running.

**Internal Error:** Instance is inactive because an internal error has occurred.

**Working MEP not Found:** Instance is inactive because the Working MEP is not found.

**Protecting MEP not Found:** Instance is inactive because the Protecting MEP is not found.

**Working MEP is not administrative active:** Instance is inactive because the Working MEP is not admin enabled.

**Protecting MEP is not administrative active:** Instance is inactive because the Protecting MEP is not admin enabled.

**Working MEP is not a Down MEP:** Instance is inactive because the Working MEP is not a Down-MEP.

**Protecting MEP is not a Down MEP:** Instance is inactive because the Protecting MEP is not a Down-MEP.

**Working and Protecting MEP use the same interface:** Instance is inactive because both Working MEPs and Protecting MEPs use the same interface.



**Another instance use the same Working port:** Instance is inactive because another instance uses the same Working port.

**State, Warning:** If the operational state is Active, the APS instance is indeed active, but it may be that it doesn't run as the administrator thinks, because of configuration errors, which are reflected in the warnings below.

The Warning information is indicated by ● : no warning, ● : warning. Use the tooltip to get detailed warning information.

**State, Protection:** The possible protection group states. The letters refer to the state as described in G.8031 Annex.

*No request Working: A.*

*No request Protecting: B.*

*Lockout: C.*

*Forced Switch: D.*

*Signal fail Working: E.*

*Signal fail Protecting: F.*

*Manual switch to Protecting: G.*

*Manual switch to Working: H.*

*Wait to restore: I.*

*Do not revert: J.*

*Exercise Working: K.*

*Exercise Protecting: L.*

*Reverse request Working: M.*

*Reverse request Protecting: N.*

*Signal degrade Working: P.*

*Signal degrade Protecting: Q.*

**Defect state, Working, Protection:** The possible values of this field are shown below:

**ok:** The port defect state is OK

**sd:** The port defect state is Signal Degrade

**sf:** The port defect state is Signal Fail

**TxAps, RxAps – Request:** The possible transmitted or received APS request according to G.8031, Table 11-1.

**nr:** No Request.

**dnr:** Do Not Revert.

**rr:** Reverse Request.

**exer:** Exercise.

**wtr:** Wait-To-Restore.

**ms:** Manual Switch.

**sd:** Signal Degrade.

**sfW:** Signal Fail for Working.

**fs:** Forced Switch.

**sfP:** Signal Fail for Protect.

**lo:** Lockout.

**TxAps, ReSignal:** Transmitted requested signal according to G.8031 figure 11-2.

**TxAps, BrSignal:** Transmitted bridged signal according to G.8031 figure 11-2

**RxAps, ReSignal:** Received requested signal according to G.8031 figure 11-2

**RxAps, BrSignal:** Received bridged signal according to G.8031 figure 11-2

**Dfop:** Dfop is "Failure of Protocol defect" and the presence of a defect is indicated by ● : no defect, ● : defect.

**CM:** Configuration Mismatch (received APS PDU on working interface within last 17.5 seconds).

**PM:** Provisioning Mismatch (far and near ends are not using the same mode; bidir only)

**NR:** No Response (far end hasn't agreed on 'Requested Signal' within 50 ms; bidir only)

**TO:** Time Out (near end hasn't received a valid APS PDU within last 17.5 seconds; bidir only)

**SMAC:** Source MAC address of last received APS PDU or all-zeros if no PDU has been received.

**TxCnt:** Number of APS PDU frames transmitted.

**RxCnt, Valid:** Number of valid APS PDU frames received on the protect port.

**RxCnt, Invalid:** Number of invalid APS PDU frames received on the protect port.

**APS Command section:** At the dropdown select an APS command:

**Command:** The selections are described below:

**noRequest:** There is no active local command on this instance. Issuing this command has no effect.

**clear:** Clear a switchover, exercise request and a WTR condition.

**forceswitch:** Causes a switchover to protect if no lockout is in effect.

**manualSwitchToProtecting:** Causes a manual signal switchover from the working path to the protection path whether or not the working path signal is active.

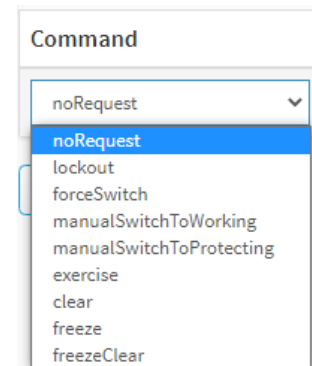
**manualSwitchToWorking:** Causes a manual signal switchover from the protection path to the working path if the protection path signal has not failed.

**exercise:** Exercise the APS instance. Use "clear" command to clear the request.

**freeze:** Freezes the state of the APS instance. While in this mode, additional near-end commands, condition changes, and received APS information are ignored. Use the command "freezeClear" to get out of this mode.

**freezeClear:** Use this command to get out of the freeze mode.

**lockout:** Lockout APS instance of protection. Use command "clear" to clear the request.



## Buttons

**Reset Counters:** Click to reset counters for this APS instance.

**Refresh:** Click to refresh the page immediately.

**Auto-refresh:** Click to automatically update page information every 3 seconds. **Note:** checking the Auto-refresh checkbox does not refresh the value of the "Command" section.

**Apply:** Click to save changes.

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

**Back:** Click to go back to webpage from which this was invoked (e.g., the APS Configuration page).

## Messages:

*JSON RPC Error. (Exercise of the APS protocol is not possible in unidirectional mode)*

*JSON RPC Error. (Exit freeze mode to enter other local requests)*

## APS Status

This page shows the current status of APS instances.

APS #	State			Defect state		TxAps			RxAps			Dfop				SMAC	RxCnt		
	Operational	Warning	Protection	Working	Protecting	Request	ReSignal	BrSignal	Request	ReSignal	BrSignal	CM	PM	NR	TO		TxCnt	Valid	Invalid
1	Active	●	Signal fail Protecting	ok	sf	sfP	0	1	nr	0	0	●	●	●	●	00:00:00:00:00:00	0	0	0
2	Administratively disabled	●	-	-	-	-	-	-	-	-	-	●	●	●	●	-	-	-	-
3	Active	●	Signal fail Protecting	ok	sf	sfP	0	1	nr	0	0	●	●	●	●	00:00:00:00:00:00	0	0	0

**APS #** : The ID of the APS. Click on the link to display the APS instance page, where you can reset counters and issue commands.

**State, Operational**: The operational state of the APS instance. There are many ways to not have the instance active. Each of them has its own value. Only when the state is Active, will the APS instance be active and up and running. If the Operational state is not "Active", the remaining fields are invalid. The possible values of this field are shown below:

**Administratively disabled**: Instance is inactive, because it is administratively disabled.

**Active**: The instance is active and up and running.

**Internal Error**: Instance is inactive, because an internal error has occurred.

**Working MEP not Found**: Instance is inactive, because the Working MEP is not found.

**Protecting MEP not Found**: Instance is inactive, because the Protecting MEP is not found.

**Working MEP is not administrative active**: Instance is inactive, because the Working MEP is not admin enabled.

**Protecting MEP is not administrative active**: Instance is inactive, because the Protecting MEP is not admin enabled.

**Working MEP is not a Down MEP**: Instance is inactive, because the Working MEP is not a Down-MEP.

**Protecting MEP is not a Down MEP**: Instance is inactive, because the Protecting MEP is not a Down-MEP.

**Working and Protecting MEP use the same interface**: Instance is inactive, because both Working MEPs and Protecting MEPs use the same interface.

**Another instance use the same Working port**: Instance is inactive because another instance uses the same Working port.

**State, Warning**: If the operational state is Active, the APS instance is indeed active, but it may be that it doesn't run as the administrator thinks, because of configuration errors, which are reflected in the warnings below.

The Warning information is indicated by ●: no warning or ●: warning. Use the tooltip to get the detailed warning information.

**State, Protection**: The possible protection group states. The letters refer to the state described in G.8031 Annex:

No request Working: **A**.

No request Protecting: **B**.

Lockout: **C**.

Forced Switch: **D**.

Signal fail Working: **E**.

Signal fail Protecting: **F**.

Manual switch to Protecting: **G**.

Manual switch to Working: **H**.

Wait to restore: **I**.  
Do not revert: **J**.  
Exercise Working: **K**.  
Exercise Protecting: **L**.  
Reverse request Working: **M**.  
Reverse request Protecting: **N**.  
Signal degrade Working: **P**.  
Signal degrade Protecting: **Q**.

**Defect state, Working, Protection:** The possible values of this field are shown below:

**ok:** The port defect state is OK  
**sd:** The port defect state is Signal Degrade  
**sf:** The port defect state is Signal Fail

**TxAps, RxAps – Request:** The possible transmitted or received APS request according to G.8031, Table 11-1.

**nr:** No Request.  
**dnr:** Do Not Revert.  
**rr:** Reverse Request.  
**exer:** Exercise.  
**wtr:** Wait-To-Restore.  
**ms:** Manual Switch.  
**sd:** Signal Degrade.  
**sfW:** Signal Fail for Working.  
**fs:** Forced Switch.  
**sfP:** Signal Fail for Protect.  
**lo:** Lockout.

**TxAps, ReSignal:** Transmitted requested signal according to G.8031 figure 11-2.

**TxAps, BrSignal:** Transmitted bridged signal according to G.8031 figure 11-2.

**RxAps, ReSignal:** Received requested signal according to G.8031 figure 11-2.

**RxAps, BrSignal:** Received bridged signal according to G.8031 figure 11-2.

**Dfop:** Dfop is "Failure of Protocol defect" and the presence of a defect is indicated by up: no defect, down: defect.

**CM:** Configuration Mismatch (received APS PDU on working interface within last 17.5 seconds).  
**PM:** Provisioning Mismatch (far and near ends are not using the same mode; bidir only)  
**NR:** No Response (far end hasn't agreed on 'Requested Signal' within 50 ms; bidir only)  
**TO:** Time Out (near end hasn't received a valid APS PDU within last 17.5 seconds; bidir only)

**SMAC:** Source MAC address of last received APS PDU or all-zeros if no PDU has been received.

**TxCnt:** Number of APS PDU frames transmitted.

**RxCnt, Valid:** Number of valid APS PDU frames received on the protect port.

**RxCnt, Invalid:** Number of invalid APS PDU frames received on the protect port.

## Buttons

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

**Refresh:** Click to manually refresh the page immediately.

**Example:** APS Status for APS # 3:

SISPM1040-3248-L3 Home - APS - Status

Switch DMS

Auto-refresh  Refresh

**Configuration**

APS #	Working			Protecting			Mode	Level	VLAN	PCP	Rev	TxAps	WTR	HoldOff	Enable
	Port	SF Trigger	SF MEP	Port	SF Trigger	SF MEP									
3	6	MEP	acs:1	3	MEP	dof:1	1+1 Bi	0	110	7	✓	✓	260	200	✓

**Status**

State			Defect state		TxAps			RxAps			Dfop				RxCnt			
Operational	Warning	Protection	Working	Protecting	Request	ReSignal	BrSignal	Request	ReSignal	BrSignal	CM	PM	NR	TD	SMAC	TxCnt	Valid	Invalid
Active	<span style="color: yellow;">●</span>	Signal fail Protecting	ok	sf	sfP	0	1	nr	0	0	<span style="color: green;">●</span>	<span style="color: green;">●</span>	<span style="color: green;">●</span>	<span style="color: red;">●</span>	00:00:00:00:00:00	0	0	0

Reset Counters

**Command**

Command

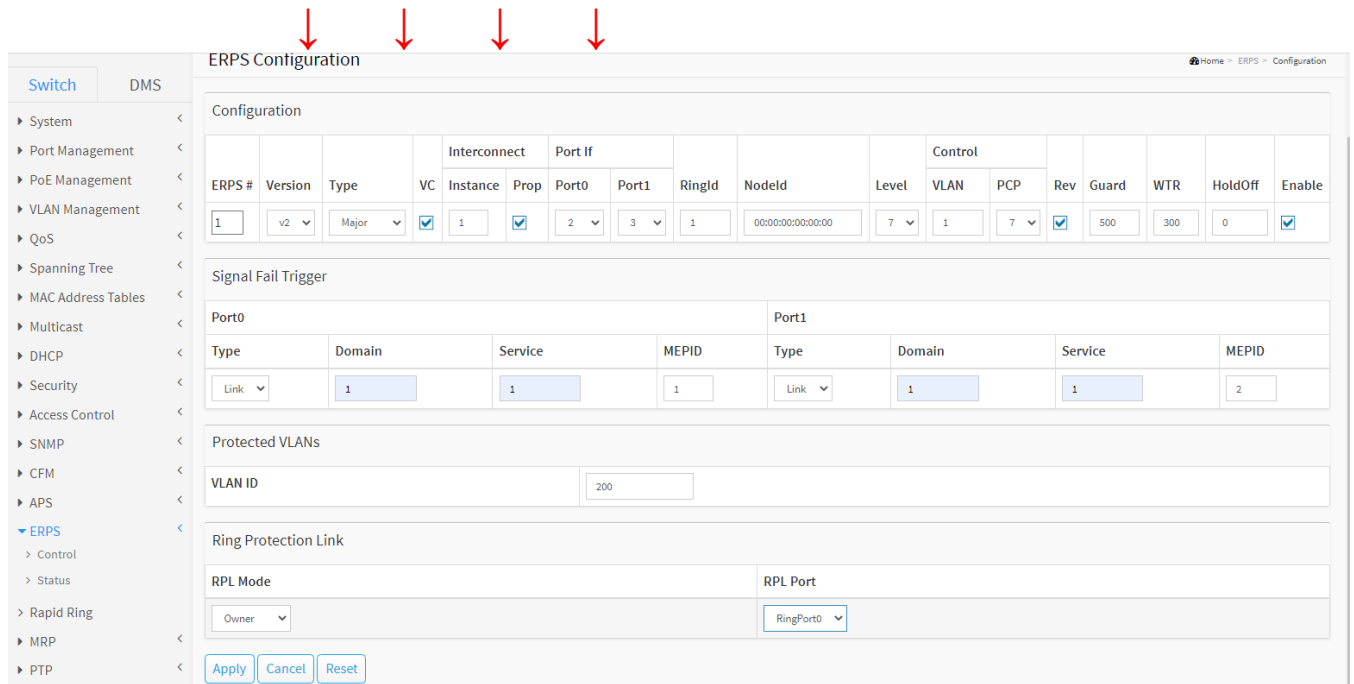
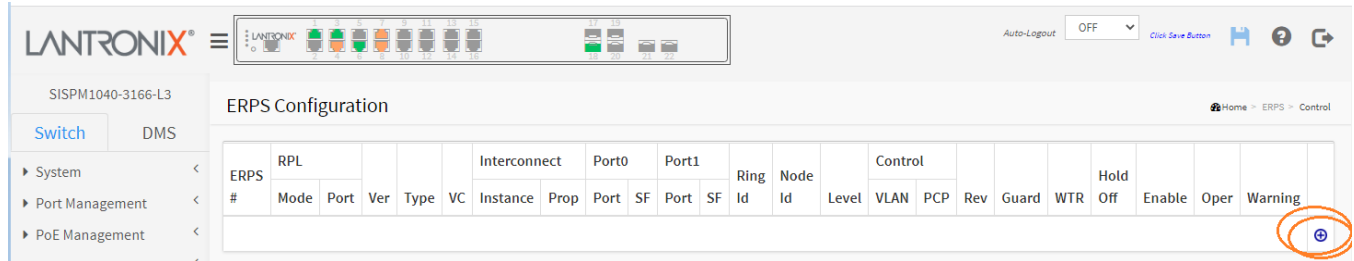
Apply Reset Back

## ERPS

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.

### ERPS > Control

ERPS instances are configured here. Click the  button to display the ERPS Configuration table.



### Configuration

**ERPS #** : The ID of ERPS. The allowed value is 1 - 64.

**Version**: ERPS protocol version (v1 and v2 are supported).

**Type**: Type of ring. Possible values are:

**Major**: ERPS major ring (G.8001-2016, clause 3.2.39)

**Sub**: ERPS sub-ring (G.8001-2016, clause 3.2.66)

**InterSub**: ERPS sub-ring on an interconnection node (G.8001-2016, clause 3.2.66)

**VC**: Controls whether to use a Virtual Channel with a sub-ring.

**Interconnect Instance**: For a sub-ring on an interconnection node, this must reference the instance ID of the ring to which this sub-ring is connected.

**Interconnect Prop:** Controls whether the ring referenced by Interconnect Instance shall propagate R-APS flush PDUs whenever this sub-ring's topology changes.

**Port If Port0:** At the dropdown select a port 0 interface (1-32).

**Port If Port1:** At the dropdown select a port 1 interface (1-32).

**Ring Id:** The Ring ID is used (along with the control VLAN) to identify R-APS PDUs as belonging to a particular ring.

**Node Id:** The Node ID is used inside the R-APS specific PDU to uniquely identify this node (switch) on the ring.

**Level:** MD/MEG Level of R-APS PDUs to transmit.

**Control VLAN:** The VLAN on which R-APS PDUs are transmitted and received on the ring ports.

**Control PCP:** The PCP value used in the VLAN tag of the R-APS PDUs.

**Rev:** Revertive (true) or Non-revertive (false) mode. In Revertive mode, after the condition(s) causing a switch have cleared, the traffic channel is restored to the working transport entity (i.e., blocked on the RPL). If a defect is cleared, the traffic channel reverts after the expiry of a WTR timer, which is used to avoid toggling protection states in the case of intermittent defects. In Non-revertive mode, the traffic channel continues to use the RPL, if it has not failed, after a switch condition has cleared.

**Guard:** Guard time in ms. Valid range is 10 - 2000 ms.

**WTR:** Wait-to-Restore time in seconds. Valid range 1 - 720 sec.

**Hold Off:** Hold off time in ms. Value is rounded down to 100ms precision. Valid range is 0 - 10000 ms.

**Enable:** The administrative state of this ERPS. Check to make it function normally and uncheck to make it cease functioning.

### **Signal Fail Trigger**

**Type:** Select whether Signal Fail (SF) comes from the link state of a given interface, or from a Down-MEP.

**Domain, Service, MEPID:** Identification of the MEP instance to provide Signal Fail, if Type is MEP.

### **Protected VLANs**

VLANs which are protected by this ring instance. At least one VLAN must be protected. Specify as a comma separated list of VLAN numbers or VLAN range (e.g., 1,4,7,30-70).

### **Ring Protection Link**

**RPL Mode:** Ring Protection Link mode. One of these:

**None:** This switch doesn't have the RPL port in the ring

**Owner:** This switch is RPL owner for the ring (G.8001-2016, clause 3.2.61)

**Neighbor:** This switch is RPL neighbor for the ring (G.8001-2016, clause 3.2.60)

**RPL Port:** Indicates whether it is port0 or port1 that is the Ring Protection Link. Not used if RPL Mode is None.

### **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.

**Messages:**

JSON RPC Error. (Port0 and Port1 cannot use the same interface)

JSON RPC Error. (Another ERPS instance has ring interfaces in common with this one and use the same control VLAN and ring ID)

JSON RPC Error. (Ring type must be "major" when using G.8032v1)

JSON RPC Error. (Ring ID must be "1" when using G.8032v1)

JSON RPC Error. (Another ERPS instance has ring interfaces and protected VLANs in common with this one)

JSON RPC Error. (An interconnected sub-ring cannot use Port1 as RPL port)

JSON RPC Error. (An interconnected sub-ring cannot reference itself as its connected ring)

Port0 Domain must not contain leading digit

**Example:** Two ERPS instances configured:

ERPS #	RPL			Ver	Type	VC	Interconnect		Port0		Port1		Ring		Control			Guard	WTR	Hold Off	Enable	Oper	Warning	
	Mode	Port	VC				Instance	Prop	Port	SF	Port	SF	Id	Node Id	Level	VLAN	PCP							Rev
1	Owner	RingPort0	v2	Major	×	0	×	2	Link	3	Link	1	00:00:00:00:00:00	7	1	7	✓	500	300	0	✓	●	●	ⓘ ⓘ
2	Neighbor	RingPort1	v2	Sub	✓	0	×	5	Link	6	Link	1	00:00:00:00:00:00	7	1	7	✓	500	300	0	✓	●	●	ⓘ ⓘ

**ERPS # :** The ID of ERPS. Valid range 1 - 64.

**Mode:** Ring Protection Link mode. Possible values:

**None:** This switch doesn't have the RPL port in the ring

**Owner:** This switch is RPL owner for the ring (G.8001-2016, clause 3.2.61)

**Neighbor:** This switch is RPL neighbor for the ring (G.8001-2016, clause 3.2.60)

**Port:** Indicates whether it is port0 or port1 that is the Ring Protection Link. Not used if RPL Mode is None.

**Ver :** The ERPS protocol version (v1 and v2 are supported).

**Type:** The type of ring. Possible values are:

**Major:** ERPS major ring (G.8001-2016, clause 3.2.39)

**Sub:** ERPS sub-ring (G.8001-2016, clause 3.2.66)

**InterSub:** ERPS sub-ring on an interconnection node (G.8001-2016, clause 3.2.66)

**VC:** Shows if a Virtual Channel with a sub-ring is in use.

**Interconnect Instance:** For a sub-ring on an interconnection node, this must reference the instance ID of the ring to which this sub-ring is connected.

**Interconnect Prop:** Shows whether the ring referenced by Interconnect Instance will propagate R-APS flush PDUs whenever this sub-ring's topology changes.

**Port0/Port1 Interface:** Interface index of ring protection Port0/Port1.

**Port0/Port1 SF:** Selects whether Signal Fail (SF) comes from the link state of a given interface, or from a Down-MEP. Possible values:

**MEP:** SF comes from Down-MEP

**Link:** SF comes from a Link state



**Ring Id:** The Ring ID is used, along with the control VLAN, to identify R-APS PDUs as belonging to a particular ring.

**Node Id:** The Node ID used inside the R-APS specific PDU to uniquely identify this node (switch) on the ring.

**Level:** MD/MEG Level of R-APS PDUs we transmit.

**Control VLAN:** The VLAN on which R-APS PDUs are transmitted and received on the ring ports.

**Control PCP:** The PCP value used in the VLAN tag of the R-APS PDUs.

**Rev:** Revertive (true) or Non-revertive (false) mode.

**Guard:** Guard time in ms. Valid range is 10 - 2000 ms.

**WTR:** "Wait-to-Restore time in seconds. Valid range is 1 - 720 sec.

**Hold Off:** Hold off time in ms. Value is rounded down to 100ms precision. Valid range is 0 - 10000 ms.

**Enable:** The administrative state of this APS ERPS. Checked means it is functioning normally and unchecked means it is not functioning.

**Oper:** The operational state of an ERPS instance:

- : Active:
- : Disabled or Internal error.

**Warning:** Operational warnings of ERPS instance:

- : No warnings
- : There are warnings, use tooltip to see.

**Configuration Buttons :** You can modify each ERPS in the table using these buttons:



**Add:** Adds new ERPS.



**Edit:** Edits the ERPS row.



**Delete:** Deletes the ERPS.

## ERPS > Status

This page shows the current status of the ERPS instances.

ERPS #	Oper	Warning	State	TxRapsActive	cFOPTo	Tx Info						Node Id	SMAC
						UpdateTimeSecs	Request	Version	Rb	Dnf	Bpr		
1	●	●	Protection	✓	✗	177664	Signal Failed	1	✗	✓	RingPort0	00:C0:F2:7C:58:92	00:00:00:00:00:00
2	●	●	Init	✗	✗	0	No Request	1	✗	✗	RingPort0	00:C0:F2:7C:58:92	00:00:00:00:00:00
3	●	●	Init	✗	✗	0	No Request	0	✗	✗	RingPort0	00:00:00:00:00:00	00:00:00:00:00:00
4	●	●	Pending	✓	✓	178793	No Request	1	✗	✗	RingPort0	00:C0:F2:7C:58:92	00:00:00:00:00:00

**ERPS #** : The ID of the ERPS. Click on a link to get to the ERPS Detailed Status for an instance page, you can reset counters and issue commands. See below.

**Oper**: The Operational state of ERPS instance.

● : Active.

● : Disabled or Internal error.

**Warning**: Operational warnings of ERPS instance.

● : No warnings.

● : There are warnings, use tooltip to see.

**State**: Specifies protection/node state of ERPS (e.g., *Init*, *Protection*, or *Warning*).

**TxRapsActive**: Specifies whether to currently transmit R-APS PDUs on ring ports (a green checkmark or a red x).

**cFOPTo**: Failure of Protocol - R-APS Rx Time Out.

**UpdateTimeSecs**: Time in seconds since boot that this structure was last updated.

**Request**: Request/state according to G.8032, table 10-3 (e.g., *Signal Failed* or *No Request*).

**Version**: Version of received/used R-APS Protocol. **0** means v1, **1** means v2, etc.

**Rb**: The RB (RPL blocked bit) of R-APS info. See Figure 10-3 of G.8032.

**Dnf**: The DNF (Do Not Flush) bit of R-APS info. See Figure 10-3 of G.8032.

**Bpr**: BPR (Blocked Port Reference) of R-APS info. See Figure 10-3 of G.8032.

**Node Id**: Node ID of this request.

**SMAC**: The Source MAC address used in the request/state.

### Buttons

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

**Refresh**: Click to manually refresh the page immediately.

## ERPS Detailed Status for an instance

On the ERPS Status page, click on a link to show the ERPS Detailed Status for that instance. Here you can reset counters and issue commands.

The screenshot shows the Lantronix web interface for device SISPM1040-3166-L3. The main content area is titled "ERPS Status" and includes an "Auto-refresh" toggle (set to "off") and a "Refresh" button. The page is divided into three main sections:

- Configuration:** A table showing the configuration for ERPS instance 1.
 

ERPS #	Ver	Type	VC	Prop	Port0	Port1	Ring Id	Node Id	Level	VLAN	PCP	Rev	Guard	WTR	HoldOff	Enable
1	v2	Major	✗	✗	2	3	1	00:00:00:00:00:00	7	1	7	✓	500	300	0	✓
- Status:** A table showing the operational status of the instance.
 

Oper	Warning	State	TxRapsActive	cFOPTo	UpdateTimeSecs	Request	Version	Rb	Dnf	Bpr	Node Id	SMAC
●	●	Protection	✓	✓	61382	Signal Failed	1	✗	✓	RingPort0	00:C0:F2:7C:59:7F	00:00:00:00:00:00
- Status Ports:** A table showing the status of individual ports.
 

Parameter	Port0	Port1
Blocked	✓	✗
Signal Fail	✓	✗
Failure of Protocol - Provisioning Mismatch	✗	✗
UpdateTimeSecs	0	0
Request state	No Request	No Request
Version of received R-APS. 0 means v1 etc	0	0
RPL blocked bit of R-APS info	✗	✗
Do Not Flush bit of R-APS info	✗	✗
Blocked Port Reference of R-APS info	RingPort0	RingPort0
Node ID of this request	00:00:00:00:00:00	00:00:00:00:00:00
Source MAC address used in the request/state	00:00:00:00:00:00	00:00:00:00:00:00

**Configuration:** This section shows the current configuration for this ERPS instance. See the ERPS Configuration page for more information.

**Status:** This section shows the current status of the ERPS instance. See the ERPS Configuration page for more information.

**Status Ports:** This section shows the current status of the ERPS instance. See the ERPS Configuration page for more information.

Counters		
Counter type	Port0	Port1
Received erroneous R-APS PDUs	0	0
Received R-APS PDUs with our own node ID	0	0
Received R-APS PDUs during guard timer	0	0
Received R-APS PDUs causing FOP-PM	0	0
Received NR R-APS PDUs	0	0
Received NR, RB R-APS PDUs	0	0
Received SF R-APS PDUs	0	0
Received FS R-APS PDUs	0	0
Received MS R-APS PDUs	0	0
Received Event R-APS PDUs	0	0
Transmitted NR R-APS PDUs	0	3
Transmitted NR, RB R-APS PDUs	0	0
Transmitted SF R-APS PDUs	0	103
Transmitted FS R-APS PDUs	0	0
Transmitted MS R-APS PDUs	0	0
Transmitted Event R-APS PDUs	0	0
Number of local signal fails	1	0
Number of FDB flushes	1	1

Reset Counters

Command

Command

No request

Apply Reset Back

**Counters:** This table shows several counters useful for debug purposes. The Counter type column indicates the counted frame attribute.

**Command:** At the dropdown select the desired command:

**No request:** There is no active local command on this instance. Issuing this command has no effect.

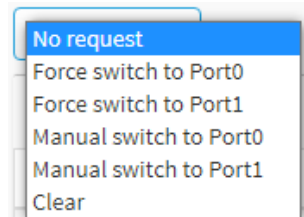
**Force switch to Port0:** Causes a forced switchover. Blocks port1 and unblocks port0.

**Force switch to Port1:** Causes a forced switchover. Blocks port0 and unblocks port1.

**Manual switch to Port0:** Causes a switchover if the signal is good and no forced switch is in effect. Blocks port1 and unblocks port0.

**Manual switch to Port1:** Causes a switchover if the signal is good and no forced switch is in effect. Blocks port0 and unblocks port1.

**Clear:** Clear a switchover (FS or MS) request and a WTB/WTR condition and force reversion even if not revertive.



**Buttons**

**Reset Counters:** Click to reset counters for this ERPS instance.

**Refresh:** Click to manually refresh the page immediately.

**Auto-refresh:** Click to **on** to refresh the page automatically every 3 seconds. **Note:** Checking Auto-refresh to **on** does not refresh the value of the "Command" selection.

**Apply:** Click to save changes.

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

**Reset :** Click to go back to the Web page from which this page was invoked.

**Counter types for Port0 and Port1:**

Received erroneous R-APS PDUs

Received R-APS PDUs with our own node ID

Received R-APS PDUs during guard timer

Received R-APS PDUs causing FOP-PM

Received NR R-APS PDUs

Received NR, RB R-APS PDUs

Received SF R-APS PDUs

Received FS R-APS PDUs

Received MS R-APS PDUs

Received Event R-APS PDUs

Transmitted NR R-APS PDUs

Transmitted NR, RB R-APS PDUs

Transmitted SF R-APS PDUs

Transmitted FS R-APS PDUs

Transmitted MS R-APS PDUs

Transmitted Event R-APS PDUs

Number of local signal fails

Number of FDB flushes

**Messages:**

*Ring Id must be an integer value between 1 and 239*

*JSON RPC Error. (Invalid instance number specified for connected ring)*

*Port0 MEPID must be an integer value between 1 and 8191*

*JSON RPC Error. (Invalid hold-off-time. Valid range is [0; 10000] milliseconds in steps of 100 milliseconds)*

*JSON RPC Error. (The control VLAN cannot be part of the protected VLANs)*

*Port0 Domain cannot be empty*

*Port0 Domain must not contain leading digit*

*Port1 Service cannot be empty*

*Port1 Service must not contain leading digit*

*Guard Time must be an integer value between 0 and 2000*

*WTR must be an integer value between 0 and 720*

*MAC address must be 12 characters long*

*HoldOff must be an integer value between 0 and 10000*

*JSON RPC Error. (Invalid params)*

*JSON RPC Error. (ERPS instance is not active)*

*JSON RPC Error. (ERPS instance is not valid)*

## Rapid Ring

This page lets you view and set current Rapid Ring parameters. **Note** that other Ring technologies (e.g., STP, MRP) must be disabled. Rapid Ring is a redundancy proprietary protocol on your network; it can be used to recover the network system from critical links failure to protect from network loops. Rapid Ring recovery time can be less than 20ms on up to 250 switches (much lower recovery time than other redundancy protocols).

Index	Role	Port	Status
1	Master	17	Discarding
		18	Discarding
2	Member	19	Discarding
		20	Discarding
3	Member	21	Discarding
		22	Discarding

### Global Configuration

**Index:** Displays the Rapid Ring Instance number (1-4).

**Role:** Set the Rapid Ring role value (Disabled, Master, or Member).

**Port:** The switch port number of the port (e.g., 25-32 or 17-22).

**Status:** The current Rapid Ring status of the port (e.g., Forwarding, Discarding).

### Buttons

**Apply:** Click to apply changes.

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

### Messages:

*Rapid Ring Configuration Error Error in port 25, STP is enable*

## MRP

### MRP > MRP Configuration

This page lets you set Media Redundancy Protocol parameters. The maximum number of entries is 2. **Note** that other Ring technologies (e.g. STP, Rapid Ring) must be disabled.

The screenshot shows the 'Media Redundancy Protocol Configuration' page in the Lantronix web interface. The page has a navigation menu on the left with options like System, Port Management, PoE Management, VLAN Management, and QoS. The main content area features a table with the following columns: Delete, Name, Primary, Secondary, Adm. Role, VLAN ID, Enable, and Edit Properties. A single domain entry is shown with the following values: Name: Domai, Primary: Port 1, Secondary: Port 2, Adm. Role: Undefined, VLAN ID: 0, Enable: Disabled. Below the table are buttons for 'Add New Domain', 'Apply', and 'Reset'. The top right of the interface shows 'Auto-Logout OFF' and a 'Click Save Button' link.

**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 (by default Domain1 and Domain2).

**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).

**Manager:** the entity will be set to the role of a Media Redundancy Manager (MRM).

**Undefined:** No role is set (default).

**VLAN ID:** The VLAN ID assigned to the MRP protocol. The allowed range is 0 - 4094.

**Enable:** Enable or Disable the MRP protocol.

**Edit Properties:** Click the Edit button to edit domain properties on the Ring Domain Configuration page (see below).

#### Buttons

**Add New Domain:** Click to add a new domain row.

**Apply:** Click to save changes.

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

## Ring Domain Configuration page

Click the Edit Properties button to display the Ring Domain Configuration page. The Manager admin role page is shown below.

Domain settings	
Id	1
Admin Role	Manag
Name	Domain1
UUID	<input checked="" type="checkbox"/> Default FFFFFFFF-FFFF-FFFF-FFFFFFFF
Primary Port Id	2
Secondary Port Id	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

### Domain settings:

**ID:** The index of the entry.

**Admin Role:** If the value is set to **Client** the entity will be set to the role of a Media Redundancy Client (MRC). If the value is set to **Manager** the entity will be set to the role of a Media Redundancy Manager (MRM). Note that some parameters only apply to the MRC role or only to the MRM role.

**Name:** A 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.

**Check Media Redundancy:** 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 or not. Only MRM.

**Link Down Interval, ms:** This parameter contains the value of the interval for sending MRP\_LinkDown frames on ring ports. The allowed range is 1 - 50. Only MRC.

**Link Up Interval, ms:** This parameter contains the value of the interval for sending MRP\_LinkUp frames on ring ports. The allowed range is 1 to 50. Only MRC.

**Link Change Count:** This parameter contains the value of the MRP\_LinkChange frame count which controls repeated transmissions of MRP\_LinkUp or MRP\_LinkDown frames. The allowed range is 1 - 10. Only MRC.

**BLOCKED State Supported:** This parameter specifies whether the MRC supports BLOCKED state at its ring ports or not. Only MRC.

## Buttons

**Apply:** Click to save changes.

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

## Messages:

*The maximum number of entries is 2*

## MRP > MRP Status

This page displays Media Redundancy Protocol status.

The screenshot shows the 'Media Redundancy Protocol Status' page. The left sidebar contains a navigation menu with 'MRP Status' selected. The main content area has an 'Auto-refresh' checkbox and a refresh icon. Below this are three sections:

- Domain Profile:** A table with columns for Name, Oper. Role, Ring State, Primary (Port, State), and Secondary (Port, State).
 

Name	Oper. Role	Ring State	Primary		Secondary	
			Port	State	Port	State
Domain1	Manager	Open	2	Not connected	3	Forwarding
Domain2	Client	-	4	Forwarding	5	Not connected
- Domain Events:** A table with columns for Timestamp, Name, Event, and Appear.
 

Timestamp	Name	Event	Appear
2022-03-08T09:15:00+00:00	Domain1	Ring Open	True
- Domain Statistics:** A table with columns for Name, MRP Transmitted Frames (Total), MRP Received Frames (Total, Error, Unrecognized), and Round Trip Delay, ms (Min, Max).
 

Name	MRP Transmitted Frames	MRP Received Frames			Round Trip Delay, ms	
	Total	Total	Error	Unrecognized	Min	Max
Domain1	2	0	0	0	0	0
Domain2	0	0	0	0	0	0

### Domain Profile

**Name:** A 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, Client, or Undefined).

**Ring State:** Ring status of the MRP entity (e.g., Open, Undefined).

**Primary:** The ifIndex (Interface Index) of the layer 2 interface which is used as ring port 1 (e.g., Not Connected, Unknown).

**Secondary:** The ifIndex (Interface Index) of the layer 2 interface which is used as ring port 2 (e.g., Forwarding).

### Domain Events

**Timestamp:** The value of sysUpTime at the time of the logged event, in the format 2020-01-01T00:27:46+00:00.

**Name:** A logical name for the MRP domain (e.g., Domain1, Domain2).

**Event:** Event type (e.g., Ring Open).

**Appear:** Event appear (true) or disappear (false).

### Domain Statistics

**Name:** The domain name.

**MRP Transmitted Frames:** The total transmitted frames.

**MRP Received Frames:** The number of total, errored, and unrecognized frames received.

**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 automatically refresh the page every 3 seconds.

**Refresh:** Click to manually refresh the page immediately.

**Clear:** Click to clear the webpage parameters.

**Messages:**

*Ring port is used*

*The name is used with other domain*

## PTP

PTP (Precision Time Protocol) is a network protocol for synchronizing the clocks of computer systems.

### PTP > Configuration

This page lets you set and view current PTP clock parameters for up to four clock instances.

#### PTP External Clock Configuration

**External Enable:** Select the External Clock output. Valid values are:

**True** : Enable the external clock output

**False** : Disable the external clock output

**Adjust Method:** Select the Frequency adjustment configuration.

**LTC** : Select Local Time Counter (LTC) frequency control.

**Auto** : Automatically select clock control, based on PTP profile and available hardware resources.

**Single** : Select SyncE DPLL frequency control, if allowed by SyncE.

**Independent** : Select an oscillator independent of SyncE for frequency control, if supported by the hardware.

**Common** : Select second DPLL for PTP, Both DPLL have the same (SyncE recovered) clock.

**Clock Frequency:** This lets you set the Clock Frequency. Possible values are 1 - 25000000 (1 - 25MHz).

#### PTP Clock Configuration

**Delete:** Check this box and click on 'Save' to delete the clock instance.

**Clock Instance:** Indicates the instance number of a particular Clock Instance [0..3]. Click on a linked Clock Instance number to edit the Clock details (see example below).

**HW Domain:** Indicates the hardware clock domain used by the clock.



**Device Type:** Indicates the Type of the Clock Instance. The Device Types are:

- Inactive:** Clock Instance is not currently active.
- Ord-Bound:** This clock's Device Type is Ordinary-Boundary Clock (default).
- P2p Transp:** This clock's Device Type is Peer to Peer Transparent Clock.
- E2e Transp:** This clock's Device Type is End to End Transparent Clock.
- Master Only:** This clock's Device Type is Master Only.
- Slave Only:** This clock's Device Type is Slave Only.
- BC-frontend:** This clock's Device Type is Boundary Clock front end.

**Device Type**

Ord-Bound ▾

- Inactive
- Ord-Bound
- P2pTransp
- E2eTransp
- Mastronly
- Slaveonly
- BC-frontend

**Profile:** Indicates the profile used by the clock. The Profile selections are:

- No Profile:** Do not use any Profile (default).
- 1588:** Use the [IEEE-1588](#) Profile.
- G8265.1:** Use the [ITU-T G.8265.1](#) Profile.
- G8275.1:** Use the [ITU-T G.8275.1](#) Profile.
- 802.1AS:** Use the [IEEE 802.1AS](#) Profile. TSN requires switches that are 802.1AS compliant to allow for priority packet scheduling.

**Profile**

No Profile ▾

- No Profile
- 1588
- G8265.1
- G8275.1
- 802.1AS

**Buttons**

**Add New Entry:** Click to create a new clock instance.

**Apply:** Click to save the page immediately.

**Reset:** Click to reset the page immediately.

**Example:** Clock details with four PTP clock instances (0-3) configured:

SISPM1040-3248-L3
PTP External Clock Mode
Home > PTP > Configuration

- ▶ System <
- ▶ Port Management <
- ▶ PoE Management <
- ▶ VLAN Management <
- ▶ QoS <
- ▶ Spanning Tree <
- ▶ MAC Address Tables <
- ▶ Multicast <
- ▶ DHCP <
- ▶ Security <
- ▶ Access Control <
- ▶ SNMP <
- ▶ CFM <
- ▶ APS <
- ▶ ERPS <
- > Rapid Ring
- ▶ MRP <

**PTP External Clock Mode**

External Enable True ▾

Adjust Method Auto ▾

Clock Frequency 10000

**PTP Clock Configuration**

Delete	Clock Instance	HW Domain	Device Type	Profile
<input type="checkbox"/>	0	0	Mastronly	1588
<input type="checkbox"/>	1	0	Slaveonly	G8265.1
<input type="checkbox"/>	2	2	Ord-Bound	No Profile
<input type="checkbox"/>	3	2	P2pTransp	802.1AS

Add New Entry
Apply
Reset

## PTP Clock's Configuration and Status

Click a linked Clock Instance to display its PTP Clock's Configuration and Status. This page lets you view and set the current PTP clock parameters.

**LANTRONIX** SISPM1040-3166-L3

Auto-Logout: OFF | [Click Here](#)

### PTP Clock's Configuration and Status

Home > PTP > Configuration

**Clock Type and Profile**

Clock Instance	HW Domain	Device Type	Profile	Apply Profile Defaults	
0	0	Mastronly	802.1AS	<input type="button" value="Apply"/>	BASIC

**Port Enable and Configuration**

Port Enable																						Configuration
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	<a href="#">Ports Configuration</a>
<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"/>	<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"/>	

**Virtual Port Enable and Configuration**

Enable	I/O Pin	Class	Accuracy	Variance	Pri1	Pri2	Local Prio
False	0	246	254	85555	128	128	128

**Local Clock Current Time**

PTP Time	Clock Adjustment method	Synchronize to System Clock
1970-01-01T17:39:56+00:00 341,516,734	Internal Timer	<input type="button" value="Synchronize to System Clock"/>

**Clock Current DataSet**

stpRm	Offset From Master	Mean Path Delay	Last GM Ph Change	Last GM FR Change	GM time base	GM change count	Last GM Change Event	Last GM Phase Change Event	Last GM Freq Change Event
0	0.000,000,000	0.000,000,000	0.000,000,000	0.000000	0	0	0	0	0

**Clock Parent DataSet**

Parent Port ID	port	PStat	Var	Rate	GrandMaster ID	GrandMaster Clock Quality	Pri1	Pri2	CRR
00:c0:f2:ff:fe:7c:59:7f	0	False	0	0	00:c0:f2:ff:fe:7c:59:7f	Cl:007 Ac:Unknwn Va:65535	246	248	0

**Clock Default DataSet**

Device Type	One-Way	2 Step Flag	Ports	Clock Identity	Dom	Clock Quality		
Mastronly	False	True	22	00:c0:f2:ff:fe:7c:59:7f	0	Cl:007 Ac:Unknwn Va:65535		
Pri1	Pri2	Local Prio	Protocol	VID	PCP	DSCP	GM Capable	sdold
246	246	128	Ethernet	1	0	0	True	0x000

**Clock Time Properties DataSet**

UtcOffset	Valid	leap59	leap61	Time Trac	Freq Trac	ptp Time Scale	Time Source
0	False	False	False	False	False	True	100
Leap Pending	Leap Date	Leap Type					
False	1970-01-01	leap61					

**Basic Filter Parameters**

Delay Filter	Period	Dist
0	1	2

**Basic Servo Parameters**

### Clock Type and Profile

**Clock Instance:** Indicates the instance number of a particular Clock Instance [0..3].

**HW Domain:** Indicates the hardware clock domain used by the clock.

**Device Type:** Indicates the Type of the Clock Instance. There are five Device Types:

**Ord-Bound** - clock's Device Type is Ordinary-Boundary Clock.

**P2p Transp** - clock's Device Type is Peer to Peer Transparent Clock.

**E2e Transp** - clock's Device Type is End to End Transparent Clock.

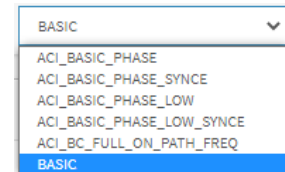
**Master Only** - clock's Device Type is Master Only.

**Slave Only** - clock's Device Type is Slave Only.

**Profile:** Indicates the profile used by the clock.

**Apply Profile Defaults:** If the clock has been configured to use a profile, clicking the 'Apply' button will reset configured values to profile defaults.

**Filter Type:** The PTP filter type determines should match the operating conditions of the network and the PTP profile.



PTP Profile	SyncE enabled (hybrid)	Filter Type	Description
1588	No	ACI_BASIC_PHASE	Requires PTP Sync and Delay_req frame rate of 16 fps or higher.
1588	Yes	ACI_BASIC_PHASE_SYNCE	Requires PTP Sync and Delay_req frame rate of 16 fps or higher.
1588	No	ACI_BASIC_PHASE_LOW	Use when the PTP Sync and Delay_req frame rate is between 1 fps to 16 fps.
1588	Yes	ACI_BASIC_PHASE_LOW_SYNCE	Use when the PTP Sync and Delay_req frame rate is between 1 fps to 16 fps.
None	No	ACI_BC_FULL_ON_PATH_FREQ	Used for Syntonized TC with basic filter.
None	No	BASIC	Basic low pass filter Servo used only for 802.1AS profile

### Port Enable and Configuration

**Port Enable:** Set check mark for each port configured for this Clock Instance.

**Configuration:** Click 'Ports Configuration' to edit the port data set for the ports assigned to this clock instance.

### Virtual Port Enable and Configuration

**Enable:** Disabled or Enabled.

**I/O Pin:** Virtual Port I/O Pin. The valid range is 0 - 3.

**Class:** Clock class value for clock as defined in IEEE Std 1588. The valid range is 0 - 255.

**Accuracy:** Clock accuracy value as defined in IEEE Std 1588. The valid range is 0 - 255.

**Variance:** The *offsetScaledLogVariance* for the clock as defined in IEEE Std 1588. The valid range is 0 - 65535.

**Pri1:** Clock priority 1 [0..255] used by the BMC master select algorithm.

**Pri2:** Clock priority 2 [0..255] used by the BMC master select algorithm.

**Local Prio:** Priority [1..255] used in the 8275.1 BMCA.

**Local Clock Current time:** Show/update local clock data:

**PTP Time:** Shows the actual PTP time with nanosecond resolution.

**Clock Adjustment Method:** Shows the actual clock adjustment method. The method depends on the available hardware.

**Synchronize to System Clock:** Activate this button to synchronize the System Clock to PTP Time.

**Clock Current Data Set:** The clock current data set is defined in the IEEE 1588 Standard. The current data set is dynamic.

**stpRm:** Steps Removed; 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

**Last GM Ph Change:** The value is the phase change that occurred on the most recent change in either grandmaster or *gmTimeBaseIndicator*.

**Last GM FR Change:** The value is the frequency change that occurred on the most recent change in either grandmaster or *gmTimeBaseIndicator*.

**GM time base:** *timeBaseIndicator* of the current grandmaster.

**GM change count:** The number of times the grandmaster has changed in a gPTP domain.

**Last GM Change Event:** The system time when the most recent grandmaster change occurred.

**Last GM Phase Change Event:** The system time when the most recent change in grandmaster phase occurred due to a change of either the grandmaster or grandmaster time base.

**Last GM Freq Change Event:** The system time when the most recent change in grandmaster frequency occurred due to a change of either the grandmaster or grandmaster time base.

**Clock Parent Data Set:** The clock parent data set is defined in the IEEE 1588 standard. The parent data set is dynamic.

**Parent Port ID:** Clock identity for the parent clock; if the local clock is not a slave, the value is the clocks own ID.

**Port:** Port Id for the parent master port.

**PStat:** Parents Stats (always false).

**Var:** It is observed parent offset scaled log variance

**Rate:** Observed Parent Clock Phase Change Rate (i.e. the slave clocks rate offset compared to the master (unit = ns per s)).

**Grand Master ID:** Clock identity for the grand master clock, if the local clock is not a slave, the value is the clocks own ID.

**Grand Master Clock Quality:** The clock quality announced by the grand master (See description of Clock Default DataSet:Clock Quality).

**Pri1:** Clock priority 1 announced by the grand master.

**Pri2:** Clock priority 2 announced by the grand master.



**CRR:** The ratio of the frequency of the grandmaster to the frequency of the Local Clock entity, expressed as fractional frequency offset.

**Clock Default Dataset:** The clock default data set is defined in the IEEE 1588 Standard. It holds three groups of data: the static members defined at clock creation time, the Dynamic members defined by the system, and the configurable members which can be set here.

**Device Type:** Indicates the Type of the Clock Instance. 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.

**One-Way:** If true, one way measurements are used. This parameter applies only to a slave. In one-way mode no delay measurements are performed (i.e., this is applicable only if frequency synchronization is needed). The Master always responds to delay requests.

**2 Step Flag:** True if two-step Sync events and Pdelay\_Resp events are used.

**Ports:** The total number of physical ports in the node.

**Clock Identity:** Shows unique clock identifier.

**Dom:** The clock domain [0..127].

**Clock Quality:** The clock quality is determined by the system, and holds 3 parts: Clock Class, Clock Accuracy and OffsetScaledLog Variance as defined in IEEE1588. The Clock Accuracy values are defined in IEEE1588 table 6 (Currently the clock Accuracy is set to 'Unknown' as default).

**Pri1:** Clock priority 1 [0..255] used by the BMC master select algorithm.

**Pri2:** Clock priority 2 [0..255] used by the BMC master select algorithm.

**Local Prio:** Priority [1..255] used in the 8275.1 BMCA.

**Protocol:** Transport protocol used by the PTP protocol engine; can be:

**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.

**IPv6Mixed:** PTP using a combination of IPv6 multicast and unicast. Currently, this is supported for only One step E2E Transparent clock.

**EthIPv4IPv6Combo:** PTP using any one of Ethernet, IPv4 or IPv6. This is supported for only one step E2E Transparent clocks.

**VID:** VLAN Identifier used for tagging the VLAN packets.

**PCP:** Priority Code Point value used for PTP frames.

**DSCP:** DSCP value used when transmitting IPv4 encapsulated packets

**GM Capable:** TRUE if the time-aware system is capable of being a Grandmaster

**Clock Time Properties Data Set:** The clock time properties data set is defined in the IEEE 1588 Standard. The data set is both configurable and dynamic (i.e., the parameters can be configured for a grandmaster). In a slave clock the parameters are overwritten by the grandmasters timing properties. The parameters are not used in the current PTP implementation. The valid values for the Time Source parameter are:

- 16** (0x10) ATOMIC\_CLOCK
- 32** (0x20) GPS
- 48** (0x30) TERRESTRIAL\_RADIO
- 64** (0x40) PTP
- 80** (0x50) NTP
- 96** (0x60) HAND\_SET
- 144** (0x90) OTHER
- 160** (0xA0) INTERNAL\_OSCILLATOR

**UtcOffset:** In systems whose epoch is UTC, it is the offset between TAI and UTC.

**Valid:** When true, the value of *currentUtcOffset* is valid

**leap59:** When true, this field indicates that last minute of the current UTC day has only 59 seconds.

**leap61:** When true, this field indicates that last minute of the current UTC day has 61 seconds.

**Time Trac:** True if the timescale and the value of *currentUtcOffset* are traceable to a primary reference.

**Freq Trac:** True if the frequency determining the timescale is traceable to a primary reference.

**ptp Time Scale:** True if the clock timescale of the grandmaster clock and false otherwise.

**Time Source:** The source of time used by the grandmaster clock.

**Leap Pending:** When true, there is a leap event pending at the date defined by *leapDate*.

**Leap Date:** The date for which the leap will occur at the end of its last minute. Date is represented as the number of days after 1970-01-01 (the latter represented as 0).

**Leap Type:** The type of leap event (i.e., leap59 or leap61).

**Servo Parameters:** The Basic clock servo uses a PID regulator to calculate the current clock rate. i.e.

$$\text{clockAdjustment} = \text{OffsetFromMaster} / \text{P constant} + \text{Integral}(\text{OffsetFromMaster}) / \text{I constant} + \text{Differential}(\text{OffsetFromMaster}) / \text{D constant}$$

**Display:** If true then Offset From Master, MeanPathDelay and clockAdjustment are logged on the debug terminal.

**P-enable:** If true the **P** part of the algorithm is included.

**I-Enable:** If true the **I** part of the algorithm is included.

**D-enable:** If true the **D** part of the algorithm is included.

**'P' constant:** [1..1000] see above.

**'I' constant:** [1..10000] see above.

**'D' constant:** [1..10000] see above.

**Filter Parameters:** The default delay filter is a low pass filter, with a time constant of  $2 \times \text{DelayFilter} \times \text{DelayRequestRate}$ .

If the DelayFilter parameter is set to 0 or the Dist parameter is 0, the delay filter uses the same algorithm as the offset filter.

The default offset filter uses a minimum offset or a mean filter method (i.e., the minimum measured offset during Period samples is used in the calculation).

The distance between two calculations is Dist periods.

**Note:** In configurations with Timestamp enabled PHYs, the period is automatically increased, if  $(\text{period} \times \text{dist} < \text{SyncPackets pr sec}/4)$  i.e., max 4 adjustments are made pr sec.

If Dist is 0 the offset is low pass filtered, the filter BW is 0.1 Hz, the filter automatically adapts to the packet rate,

If Dist is 1 the offset is averaged over the Period.

If Dist is >1 the offset is calculated using 'min' offset.

**DelayFilter:** See above.

**Period:** See above.

**dist:** See above.

**Unicast Slave Configuration:** When operating in IPv4 Unicast mode, the Slave is configured up to 5 master IP addresses. The Slave then requests Announce messages from all the configured masters. The Slave uses the BMC algorithm to select one as master clock, the Slave then requests Sync messages from the selected Master.

**Duration:** The number of seconds a Master is requested to send Announce/Sync messages. The request is repeated from the Slave each Duration/4 seconds.

**ip\_address:** IPv4 Address of the Master clock.

**grant:** The granted repetition period for the sync message.

**CommState:** The state of the communication with the master; possible values are:

**IDLE** : The entry is not in use.

**INIT** : Announce is sent to the master (Waiting for a response).

**CONN** : The master has responded.

**SELL** : The assigned master is selected as current master.

**SYNC** : The master is sending Sync messages.

## Buttons

**Apply** : Click to save changes.

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

## Messages:

*Maximum of 4 clock instances can be created.*

*Cannot create more than one new clock with a given instance number*

*Clock Instance must be an integer value between 0 and 3*

## PTP Clock's Port Data Set Configuration

The port data set is defined in the IEEE 1588 Standard. It holds three groups of data: static members, dynamic members, and configurable members which can be set here.

The screenshot shows the 'PTP Clock's Port Data Set Configuration' page in the Lantronix web interface. The page title is 'PTP Clock's Port Data Set Configuration'. The interface includes a navigation menu on the left with options like System, Port Management, PoE Management, VLAN Management, QoS, Spanning Tree, MAC Address Tables, Multicast, DHCP, Security, Access Control, SNMP, and CFM. The main content area displays a table for 'Port DataSet' with the following columns: Port, Stat, MDR, PeerMeanPathDel, Anv, ATo, Syv, DIm, MPR, Delay Asymmetry, Ingress Latency, Egress Latency, Version, Mcast Addr, Not Slave, Local Prio, and 2 Step Flag. The table contains 7 rows of data for ports 2 through 7. Below the table are 'Apply' and 'Reset' buttons.

Port	Stat	MDR	PeerMeanPathDel	Anv	ATo	Syv	DIm	MPR	Delay Asymmetry	Ingress Latency	Egress Latency	Version	Mcast Addr	Not Slave	Local Prio	2 Step Flag
2	dsbl	0	0,000,000,000	0	3	-3	p2p	0	0	0	0	2	Link-local	False	128	Clock Def.
3	lstn	0	0,000,000,000	0	3	-3	p2p	0	0	0	0	2	Link-local	False	128	Clock Def.
4	lstn	0	0,000,000,000	0	3	-3	p2p	0	0	0	0	2	Link-local	False	128	Clock Def.
5	dsbl	0	0,000,000,000	0	3	-3	p2p	0	0	0	0	2	Link-local	False	128	Clock Def.
6	lstn	0	0,000,000,000	0	3	-3	p2p	0	0	0	0	2	Link-local	False	128	Clock Def.
7	lstn	0	0,000,000,000	0	3	-3	p2p	0	0	0	0	2	Link-local	False	128	Clock Def.

### Port DataSet

**Port:** Static member port Identity : Port number [1..max port no].

**Stat:** Dynamic member *portState*: Current state of the port.

**MDR:** Dynamic member log Min Delay Req Interval: The delay request interval announced by the Master.

**Peer Mean Path Del:** The path delay measured by the port in P2P mode. In E2E mode this value is 0.

**Anv:** The interval for issuing announce messages in master state. Range is -3 to 4.

**ATo:** The timeout for receiving announce messages on the port. Range is 1 to 10.

**Syv:** The interval for issuing sync messages in master. Range is -7 to 4.

**DIm:** Configurable member delayMechanism: The delay mechanism used for the port:

**e2e** : End to end delay measurement

**p2p** : Peer to peer delay measurement.

**cp2p** : Common Peer to peer delay measurement used in 802.1AS. There will be single instance of common peer to peer delay measurement per port.

Can be defined per port in an Ordinary/Boundary clock. In a transparent clock all ports use the same delay mechanism, determined by the clock type.

**MPR:** The interval for issuing Delay\_Req messages for the port in E2e mode. This value is announced from the Master to the Slave in an announce message. The value is reflected in the MDR field in the Slave.

The interval for issuing Pdelay\_Req messages for the port in P2P mode.

**Note:** The interpretation of this parameter has changed from release 2.40. In earlier versions the value was interpreted relative to the Sync interval; this was a violation of the standard, so now the value is interpreted as an interval (i.e., MPR=0 => 1 Delay\_Req pr sec) independent of the Sync rate. The valid 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.

**Ingress latency:** Ingress latency measured in ns, as defined in IEEE 1588 Section 7.3.4.2. Range is -100000 to 100000.

**Egress Latency:** Egress latency measured in ns, as defined in IEEE 1588 Section 7.3.4.2. Range is -100000 to 100000.

**Version:** The PTP version used by this port. The current implementation only supports PTP version 2

**Mcast Addr:** Configured destination address for multicast packets (PTP Default or LinkLocal)

**Not Slave:** TRUE indicates that this interface cannot enter slave mode

**Local Prio:** 1-255, priority used in the 8275.1 BMCA

**2 Step Flag:** Option to override the 2-step option on port level \*/ // IEEE 802.1AS specific parameters are only available when the 802.1AS profile is selected. Select Clock Def., True, or False.

**Port Role:** Port role of this port.

**IsMeasDelay:** TRUE if the port is measuring link propagation delay

**As Capable:** TRUE if the time-aware system at the other end of the link is 802.1AS capable

**Neighbor rate ratio:** Calculated neighbor rate ratio expressed as the fractional frequency offset multiplied by  $2^{41}$ .

**CAnv:** Current Log Announce Interval - log2 of the current announce interval, which is either the configured initial logAnnounceInterval or the value received in a message interval request

**CSyv:** Current Log Sync Interval - log2 of the current sync interval, which is either the configured initial logSyncInterval or the value received in a message interval request

**SyncTimeIntrv:** Sync Receipt Time Interval - Time interval after which sync receipt timeout occurs if time-synchronization information has not been received during the interval.

**CMPR:** Current Log PDelay Req Interval - log2 of the current Pdelay\_Req interval, which is either the configured initial logMinPdelayReqInterval or the value received in a message interval request

**AMTE:** Acceptable Master Table Enabled - Always FALSE

**Comp rate ratio:** Current value of compute neighbor rate ratio

**Comp Mean delay:** Current value of compute Mean Link Delay

**Version Number:** IEEE 1588 PTP version number (always 2)

**NPDT:** Neighbor Prop Delay Thresh - Max allowed meanLinkDelay

**SRT:** Sync Receipt Timeout - Number of time-synchronization transmission intervals that a slave port waits without receiving synchronization information

**ALR:** Allowed Lost Responses - Number of Pdelay\_Req messages for which a valid response is not received, above which a port is considered to not be exchanging peer delay messages with its neighbor.

**AFs:** Allowed Faults - Number of allowed instances where the computed mean propagation delay exceeds the threshold meanLinkDelayThresh and/or instances where the computation of neighborRateRatio is invalid.

**useMgmtSync:** Flag to decide the value to be used for sync interval.

**SyncIntrvl:** If useMgmtSync is set, port uses this value to decide the sync packet interval, else default value is used. Range is -7 to 4.

**useMgmtAnnounce:** Flag to decide the value to be used for announce packet interval.

**AnnounceIntrvl:** If useMgmtAnnounce is set, port uses this value to decide the Announce packet interval, else default value is used. Range is -3 to 4.

**useMgmtPdelay:** Flag to decide the value to be used for announce packet interval.

**PdelayIntrvl:** If useMgmtPdelay is set, port uses this value to decide the Peer delay request packet interval , else default value is used. Range is -7 to 5.

**useMgmtGtpCapIntrvl:** Flag to decide the value to be used for gtp capable tlv signalling packet interval.

**MgmtGtpCapIntrvl:** If useMgmtGtpCapIntrvl is set, port uses this value to decide the gtp capable tlv signalling packet interval , else default value is used. Range is -24 to 24.

**GtpCapableReceiptTimeout:** Number of gPTP capable message intervals to wait without receiving from its neighbor a Signaling message containing a gPTP capable TLV, before determining that its neighbor is no longer invoking the gPTP protocol.

**initialLogGtpCapableMessageInterval:** Specifies the gPTP capable message interval when the port is initialized, and the value the gPTP capable message interval is set to when a gPTP capable TLV is received with the logGtpCapableMessageInterval field set to 126

**uMSCNRR:** useMgtSettableComputeNeighborRateRatio - This value determines the source of the value of computeNeighborRateRatio. 'True' indicates source as 'mgtSettablecomputeNeighborRateRatio'. 'false' indicates source as initial value or value set by 'LinkDelayIntervalSetting state machine'.

**MSCNRR:** mgtSettableComputeNeighborRateRatio - This value indicates the input through management interface whether to compute neighbor rate ratio or not.

**uMSCMLD\_ :** useMgtSettableComputeMeanLinkDelay - This value determines the source of the value of computeMeanLinkDelay. 'True' indicates source as 'mgtSettableComputeMeanLinkDelay'. Otherwise, Initial value or value set by LinkDelayInterval State machine is used.

**MSCMLD\_ :** mgtSettableComputeMeanLinkDelay - This value indicates the input through management interface whether to compute Mean Link Delay or not. //Common Link Delay Service parameters for 802.1AS \*/

**MLDT:** meanLinkDelayThresh - The propagation time threshold, above which a port is not considered capable of participating in the IEEE 802.1AS protocol.

**DA:** delayAsymmetry - the asymmetry in the propagation delay on the link attached to this port relative to the grandmaster time base, as defined in 8.3. If propagation delay asymmetry is not modeled, then delayAsymmetry is zero.

**iLPDRv:** initialLogPdelayReqInterval - this value is the logarithm to base 2 of the Pdelay\_Req message transmission interval used.

**uMSLPDRv:** useMgtSettableLogPdelayReqInterval - This value determines the source of 'currentLogPdelayReqInterval'. 'True' indicates source as 'mgtSettableLogPdelayReqInterval'. Otherwise, initial value or value set by LinkDelayInterval State machine is used.

**MSLPDRv:** mgtSettableLogPdelayReqInterval - This value is used if useMgtSettableLogPdelayReqInterval is true.

**iCNRR:** initialComputeNeighborRateRatio - Initial value that indicates whether neighborRateRatio is to be computed by this port.

**cm\_uMSCNRR:** useMgtSettableComputeNeighborRateRatio - This value determines the source of the value of computeNeighborRateRatio. 'True' indicates source as 'mgtSettablecomputeNeighborRateRatio'. Otherwise, initial value or value set by LinkDelayInterval state machine is used.

**cm\_MSCNRR:** mgtSettableComputeNeighborRateRatio - This value indicates the input through management interface whether to compute neighbor rate ratio or not.

**iCMLD:** initialComputeMeanLinkDelay - Initial value that indicates whether mean Link delay is computed by this port or not.

**cm\_uMSCML D:** useMgtSettableComputeMeanLinkDelay - This value determines the source of the value of computeMeanLinkDelay. 'True' indicates source as 'mgtSettableComputeMeanLinkDelay'. Otherwise, initial value or value set by LinkDelayInterval state machine is used.

**cm\_MSCMLD:** mgtSettableComputeMeanLinkDelay - This value indicates the input through management interface whether to compute Mean Link Delay or not.

**cm\_ALR:** allowedLostResponses - The number of Pdelay\_Req messages for which a valid response is not received, above which a Link Port is considered to not be exchanging peer delay messages.

**cm\_AFs:** allowedFaults - The number of faults, above which asCapableAcrossDomains is set to FALSE.

## Buttons

**Apply** : Click to save changes.

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

## PTP > Status

The PTP External Clock Mode page lets you view current PTP clock settings.

The screenshot shows the 'PTP External Clock Mode' configuration page. The 'Auto-refresh' toggle is set to 'off' with a 'Refresh' button. The 'PTP External Clock Mode' section shows: External Enable: False, Adjust Method: Auto, and Clock Frequency: 1. The 'PTP Clock Configuration' table is as follows:

Inst	ClkDom	Device Type	Port List																					
			1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22
0	0	Mastronly	✓	✓	✓	✓	✓	✓																
1	1	Slaveonly							✓	✓	✓	✓	✓											
2	2	Ord-Bound																						
3	0	E2eTransp		✓			✓		✓											✓				

### PTP External Clock Mode:

**External Enable:** Shows the current External clock output configuration:

**True** : Enable the external clock output

**False** : Disable the external clock output

**Adjust Method:** Shows the current Frequency adjustment configuration:

**LTC** : Use Local Time Counter (LTC) frequency control

**Single** : Use SyncE DPLL frequency control, if allowed by SyncE

**Independent** : Use an oscillator independent of SyncE for frequency control, if supported by the HW

**Common** : Use second DPLL for PTP, Both DPLL have the same (SyncE recovered) clock.

**Auto** : AUTO Select clock control, based on PTP profile and available HW resources.

**Clock Frequency:** Shows the current clock frequency used by the External Clock. The possible 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. See "PTP Clock's Configuration" below.

**ClkDom:** Indicates the Clock domain used by the Instance of a particular Clock Instance [0..3].

**Device Type:** Indicates the Type of the Clock Instance. There are five Device Types:

**Ord-Bound** - Clock's Device Type is Ordinary-Boundary Clock.

**P2p Transp** - Clock's Device Type is Peer to Peer Transparent Clock.

**E2e Transp** - Clock's Device Type is End to End Transparent Clock.

**Master Only** - Clock's Device Type is Master Only.

**Slave Only** - Clock's Device Type is Slave Only.



**Port List:** Shows the ports configured for that Clock Instance.

**Buttons**

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

**Refresh:** Click to refresh the page immediately.

**PTP Clock's Configuration**

Click on the Clock Instance number to display the PTP Clock's Configuration page:

The screenshot displays the 'PTP Clock's Configuration' page for device SISPM1040-0248-L3. The interface includes a navigation sidebar on the left and a main content area with several configuration sections:

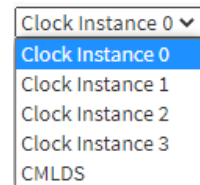
- Auto-refresh:** A toggle switch is turned off, with a 'Refresh' button next to it.
- Clock Type and Profile:** A table with columns: Clock Instance (0), HW Domain (0), Device Type (Masterly), Profile (1000), Filter Type (ACI\_BASIC\_PHASE\_LOW), and Filter Mode (PACKET).
- Local Clock Current Time:** A table with columns: PTP Time (1970-01-06T08:41:16+00:00 507,950,918), Clock Adjustment method (Internal Timer), and Ports Monitor Page (Ports Monitor).
- Clock Default DataSet:** A table with columns: Device Type (Masterly), One-Way (False), 2 Step Flag (False), Ports (32), Clock Identity (00:c0:f2:#fe:7c:5b:92), Dom (0), Clock Quality (Cl:248 Ac:Unknown Va:65535), Prio1 (128), Prio2 (128), Local Prio (128), Protocol (Ethernet), VID (1), PCP (0), and DSCP (0).
- Clock Current DataSet:** A table with columns: stpRm (0), Offset From Master (0,000,000,000), Mean Path Delay (0,000,000,000), Slave Port (0), Slave State (FREERUN), and Holdover(ppb) (N.A.).
- Clock Parent DataSet:** A table with columns: Parent Port ID (00:c0:f2:#fe:7c:5b:92), port (0), PStat (False), Var (0), Rate (0), GrandMaster ID (00:c0:f2:#fe:7c:5b:92), GrandMaster Clock Quality (Cl:248 Ac:Unknown Va:65535), Prio1 (128), and Prio2 (128).
- Clock Time Properties DataSet:** A table with columns: UtcOffset (0), Valid (False), leap59 (False), leap61 (False), Time Trac (False), Freq Trac (False), ptp Time Scale (True), and Time Source (160).
- Basic Filter Parameters:** A table with columns: DelayFilter (6), Period (1), and Dist (1).
- Basic Servo Parameters:** A table with columns: Display (False), P-enable (True), I-enable (True), D-enable (True), 'P' constant (3), 'I' constant (80), 'D' constant (40), and Gain constant (1).
- Unicast Slave Configuration:** A table with columns: Index (0-4), Duration (100), IP\_Address (0.0.0.0), Grant (0), and CommState (IDLE).

## PTP > 802.1AS Statistics

This page lets you view 802.1AS Clock Instance Specific Statistics. IEEE 802.1AS is an adaptation of PTP for use with Audio Video Bridging and Time-Sensitive Networking. TSN requires switches that are 802.1AS compliant to allow for priority packet scheduling. IEEE 802.1AS was introduced based on IEEE 1588. It specifies a profile for use of IEEE 1588-2008 for time synchronization over a virtual bridged local area network (as defined by IEEE 802.1Q). This standard enables stations attached to bridged LANs to meet the respective jitter, wander, and time synchronization requirements for time-sensitive applications.

Port	SyncCount		FollowUpCount		PdelayRequestCount		PdelayResponseCount		PdelayResponseFollowUpCount		AnnounceCount	PTPPacketDiscardCount		syncReceiptTimeoutCount		announceReceiptTimeoutCount		PdelayAllowedLostResponsesExceededCount				
	Rx	Tx	Rx	Tx	Rx	Tx	Rx	Tx	Rx	Tx		Rx	Tx	Rx	Tx	Rx	Tx	Rx	Tx			
1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
2	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
3	0	0	0	0	0	0	0	0	0	0	732	0	0	0	0	0	0	0	0	0	0	732
4	0	0	0	0	0	0	0	0	0	0	350	0	0	0	0	0	0	0	0	0	0	350
5	0	0	0	0	0	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	350	0	0	0	0	0	0	0	0	0	0	350
7	0	0	0	0	0	0	0	0	0	0	350	0	0	0	0	0	0	0	0	0	0	350
8	0	0	0	0	0	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	0	0	0	0	0
10	0	0	0	0	0	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	0	0	0	0	0
12	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
13	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
14	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0

**Instance:** At the Clock Instance dropdown select the desired instance (PTP Clock Instance 0-3) or CMLDS (Common Mean Link Delay Service). Note that the CMLDS option allows multiple PTP implementations in different domains, but sharing a physical port to use receive link delay information without repeating peer delay messages.



### 802.1AS Received counters

**SyncCount:** A counter that increments every time when synchronization information is received.

**FollowUpCount:** A counter that increments every time when a Follow Up message is received.

**PdelayRequestCount:** A counter that increments every time when a Pdelay\_Req message is received.

**PdelayResponseCount:** A counter that increments every time when a Pdelay\_Resp message is received.

**PdelayResponseFollowUpCount:** A counter that increments every time when a Pdelay\_Resp\_Follow\_Up message is received.

**AnnounceCount:** A counter that increments every time when an Announce message is received.

**PTPPacketDiscardCount:** A counter that increments every time when a PTP message is discarded.

**syncReceiptTimeoutCount:** A counter that increments every time when sync receipt timeout occurs.

**announceReceiptTimeoutCount:** A counter that increments every time when announce receipt timeout occurs.

**PdelayAllowedLostResponsesExceededCount:** A counter that increments every time the value of the variable lostResponses exceeds the value of the variable allowedLostResponses.

**802.1As Transmit Counters**

**SyncCount:** A counter that increments every time synchronization information is transmitted.

**FollowUpCount:** A counter that increments every time a Follow\_Up message is transmitted.

**PdelayRequestCount:** A counter that increments every time a Pdelay\_Req message is transmitted.

**PdelayResponseCount:** A counter that increments every time a Pdelay\_Resp message is transmitted.

**PdelayResponseFollowUpCount:** A counter that increments every time a Pdelay\_Resp\_Follow\_Up message is transmitted.

**AnnounceCount:** A counter that increments every time an Announce message is transmitted.

**Buttons**

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

**Refresh:** Click to refresh the page immediately.

**Messages:**

*Selected instance is not enabled*

## Event Notification

### Event Notification > SNMP Trap

At the default Trap Configurations page click the Add New Entry button to display the SNMP Trap Configuration page. Configure SNMP trap parameters on this page.

The screenshot shows the LANTRONIX web interface for configuring SNMP traps. The page title is "SNMP Trap Configuration" and the breadcrumb is "Home > Event Notification > SNMP Trap". The configuration form includes the following fields:

Trap Config Name	<input type="text"/>
Trap Mode	Disabled
Trap Version	SNMP v2c
Trap Community	public
Trap Destination Address	<input type="text"/>
Trap Destination Port	162
Trap Security Engine ID	800003640300c0f27c597f
Trap Security Name	None

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

**Trap Config Name:** Enter a trap Configuration name for configuring. The allowed string length is 1–32 characters, and the allowed content is ASCII characters 33-126.

**Trap Mode:** Select the SNMP mode of operation. Possible modes are:

**TCP:** Enable TCP SNMP mode operation.

**UDP:** Enable UDP SNMP mode operation.

**Disabled:** Disable SNMP mode operation.

**Trap Version:** Select the SNMP supported version. Possible versions are:

**SNMP v1:** Set SNMP supported version 1.

**SNMP v2c:** Set SNMP supported version 2c.

**SNMP v3:** Set SNMP supported version 3.

**Trap Community:** Indicates the community access string when sending SNMP trap packet. The allowed string length is 0-63 characters, and the allowed content is ASCII characters 33-126.

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

Indicates the SNMP trap destination IPv6 address. IPv6 address is in 128-bit records represented as eight fields of up to four hexadecimal digits with a colon separating each field (:). For example, 'fe80::215:c5ff:fe03:4dc7'.

The symbol '::' is a special syntax that can be used as a shorthand way of representing multiple 16-bit groups of contiguous zeros; but it can appear only once. It can also represent a legally valid IPv4 address. For example, '::192.1.2.34'.

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

**Trap Security Engine ID:** Indicates the SNMP trap security engine ID. SNMPv3 sends traps and informs using USM for authentication and privacy. A unique engine ID for these traps and informs is needed. When "Trap Probe Security Engine ID" is enabled, the ID will be probed automatically. Otherwise, the ID specified in this field is used. The string must contain an even number (in hexadecimal format) with the number of digits between 10 and 64, but all-zeros and all-Fs 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.

## Example:

Delete	Name	Mode	Version	Destination Address	Destination Port
<input type="checkbox"/>	trap1	TCP	SNMPv2c	192.168.1.30	162
<input type="checkbox"/>	trap2	UDP	SNMPv1	192.168.1.40	162
<input type="checkbox"/>	trap3	TCP	SNMPv3	192.168.1.50	162

**Name:** Displays the trap Configuration's name (e.g., the trap destination's name). Click a linked name to display the related SNMP Trap Configuration page where you can make further trap parameter edits.

**Mode:** Displays the trap destination mode operation. Possible modes are:

**TCP:** TCP SNMP trap mode operation is enabled.

**UDP:** UDP SNMP trap mode operation is enabled.

**Disabled:** Disable SNMP trap mode operation is disabled.

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

**SNMPv1:** SNMP trap version 1 is configured.

**SNMPv2c:** SNMP trap version 2c is configured.

**SNMPv3:** SNMP trap version 3 is configured.

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

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

**Destination Port:** Displays the SNMP trap destination port. The SNMP Agent will send SNMP messages via this port. The port range is 1~65535.

**Buttons**

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

**Apply:** Click to save changes.

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

## Event Notification > email

This page lets you configure SMTP (Simple Mail Transfer Protocol). SMTP is the message-exchange standard for the Internet. The switch is to be configured as a client of SMTP while the server is a remote device that will receive messages from the switch that alarm events occurred.

**Mail Server:** The IP address or hostname of the mail server. IP address is expressed in dotted decimal notation. This will be the device that sends out the mail for you

**User Name:** Specify the username on the mail server.

**Password:** Specify the password of the user on the mail server.

**Sender:** Specify the name of the sender of the alarm mail.

**Return Path:** Specify the sender email address of the alarm mail. This address will be the "from" address on the email message.

**Email Address # :** Specify the email address of the receiver.

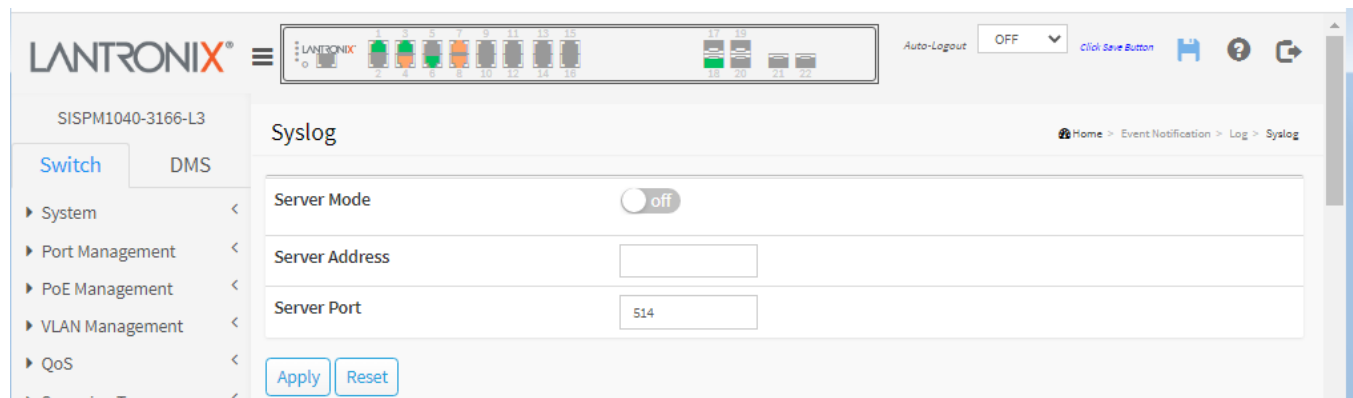
### Buttons

**Apply:** Click to apply changes.

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

## Event Notification > Log > Syslog

Configure System Log settings on this page.



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

**on:** Enable syslog server mode operation.

**off:** Disable syslog server mode operation (default).

**Server Address:** Indicates the IPv4/IPv6 host address of syslog server. If the switch uses the DNS feature, it can also be a domain name.

**Server Port:** Indicates the service port of syslog server.

### Buttons

**Apply:** Click to save changes.

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



## Event Notification > Log > View Log

The switch system log information is provided here. Each page shows a number of table entries, selected with the "Show entries" dropdown. The Search field lets you enter and search for a key word in the table.

The screenshot shows the Lantronix web interface for device SISPM1040-3166-L3. The main content area is titled "System Log Information" and features an "Auto-refresh" toggle set to "off", along with "Refresh" and "Clear" buttons. Below this, there is a "System Log" section with a "Show 50 entries" dropdown and a search field. The log entries are displayed in a table with the following columns: ID, Level, Time, and Message.

ID	Level	Time	Message
45	Informational	2020-01-01T00:03:35+00:00	LINK-UPDOWN: IP Interface VLAN 1, changed state to up.
44	Informational	2020-01-01T00:03:35+00:00	LINK-UPDOWN: IP Interface VLAN 1, changed state to up.
43	Informational	2020-01-01T00:03:35+00:00	Password of user 'admin' was changed
42	Informational	2020-01-01T00:02:17+00:00	Login passed for user 'admin' through WEB from 192.168.1.99 and authenticated by local method
41	Warning	2020-01-01T00:02:00+00:00	Bad password attempt for user 'admin' through WEB from 192.168.1.99 and authenticated by local method
40	Warning	2020-01-01T00:01:51+00:00	Bad password attempt for user 'admin' through WEB from 192.168.1.99 and authenticated by local method
39	Informational	2020-01-01T00:00:53+00:00	topologyChange
38	Informational	2020-01-01T00:00:53+00:00	DC2 Power Up
37	Informational	2020-01-01T00:00:53+00:00	AC Power Up
36	Informational	2020-01-01T00:00:53+00:00	DC1 Power Up
35	Informational	2020-01-01T00:00:53+00:00	topologyChange
34	Warning	2020-01-01T00:00:53+00:00	Switch just made a warm boot
33	Informational	2020-01-01T00:00:53+00:00	topologyChange
32	Informational	2020-01-01T00:00:53+00:00	LINK-UPDOWN: IP Interface VLAN 1, changed state to up.
31	Informational	2020-01-01T00:00:53+00:00	LINK-UPDOWN: IP Interface VLAN 1, changed state to up.
30	Warning	2020-01-01T00:00:53+00:00	Port 8 PoE PD on
29	Warning	2020-01-01T00:00:53+00:00	Port 7 PoE PD on
28	Warning	2020-01-01T00:00:53+00:00	Port 6 PoE PD on
27	Warning	2020-01-01T00:00:53+00:00	Port 4 PoE PD on

**ID:** The identification of the system log entry.

**Level:** The level of the system log entry:

**Debug** : debug level message.

**Informational** : informational message.

**Notice** : normal, but significant, condition.

**Warning** : warning condition.

**Error** : error condition.

**Crit** : critical condition.

**Alert** : action must be taken immediately.

**Emergency** : system is unusable.

**Time:** The occurred time of the system log entry.

**Message:** The detailed message of the system log entry.

### Buttons

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

**Refresh:** Updates the table entries, starting from the current entry.

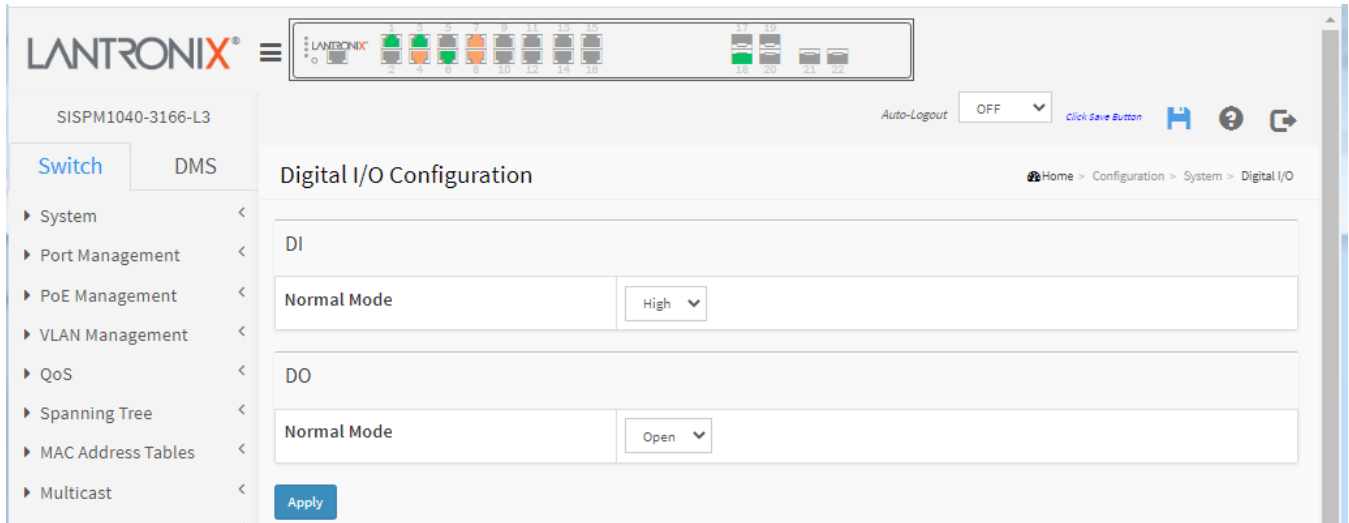
**Clear:** Flushes the selected entries.

**Previous :** Updates the system log entries, turn to the previous page.

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

## Event Notification > Digital I/O

This page lets you configure the normal modes of digital input/output (DI/DO).



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

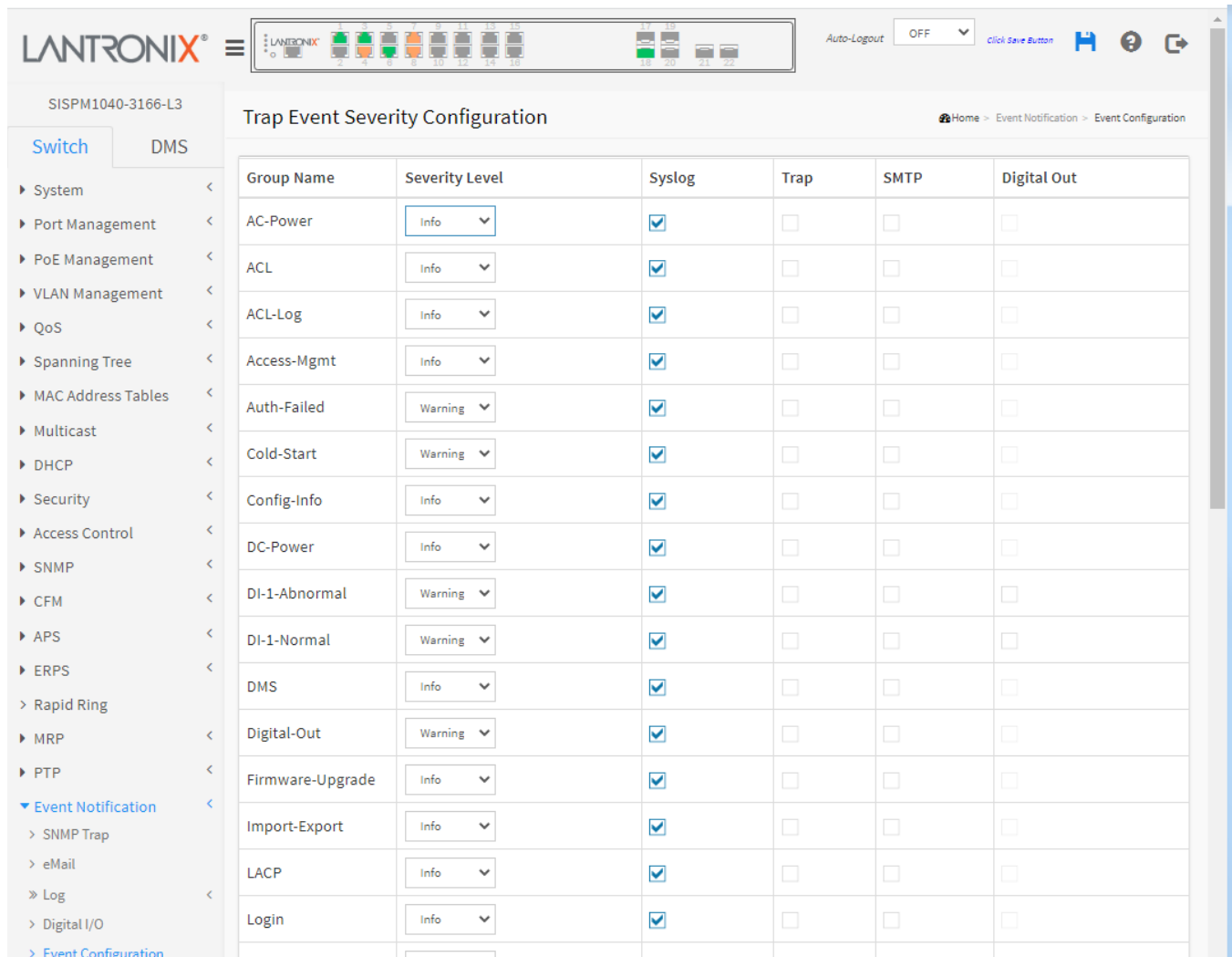
**DO Normal Mode:** Set the normal mode of the digital output(DO). You can set it to Open or Close.

### Buttons

**Apply:** Click to save the changes.

## Event Notification > Event Configuration

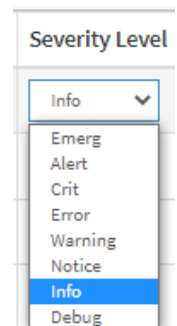
This page lets you set and view current trap event severity parameters.



**Group Name:** The name identifying the severity group.

**Severity Level:** Every group has a severity level. These level types are supported:

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



**Syslog:** Check the box to enable this Group Name in Syslog.

**Trap:** Check the box to enable this Group Name in Trap.

**SMTP:** Check the box to enable this Group Name in SMTP.

**Digital Out:** Check the box to enable this Group Name in Digital Out.

### Buttons

**Apply:** Click to apply changes.

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

## Router

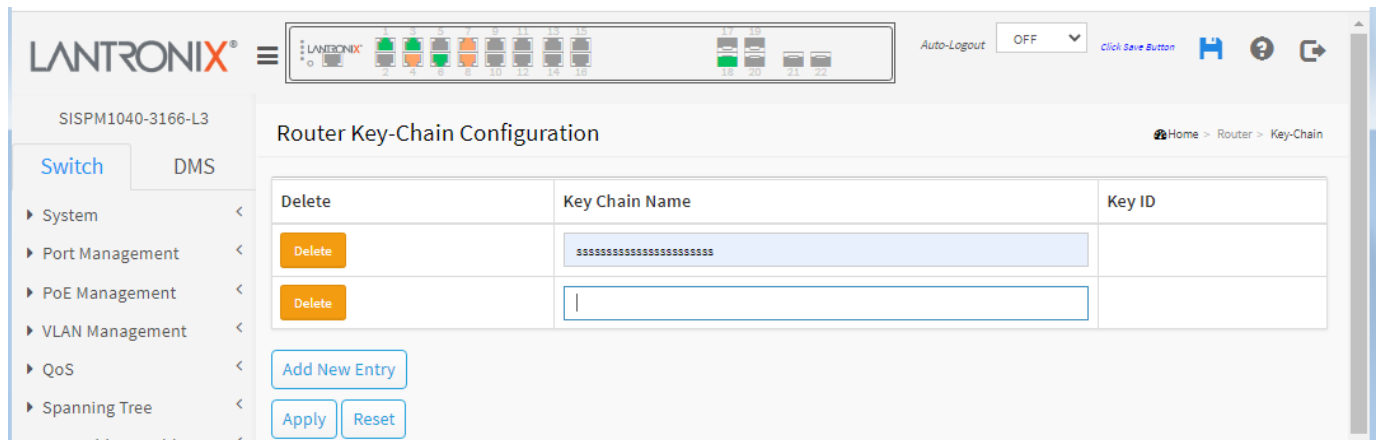
The router module lets you configure key-chain and access list parameters.

The IP Address > Advanced Settings page has a Mode dropdown to select Host or Router mode. It must be set to Router to be able to use the Router function.

### Router > Key-Chain

This page lets you set router key chain name table parameters.

A key chain is a set of keys used in succession; each has a limited lifetime. Change the keys frequently to reduce the chance of an intruder guessing a key. A key is not used during inactive time (when not activated). If a time period occurs when no key is activated, no neighbor authentication can occur, and routing updates will fail.



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

**Key Chain Name:** The name of the key-chain entry. The valid name string length is 1-31 characters and allows all printable characters excluding the space character.

**Key ID:** Click the icon to edit the key. Key ID must be an integer value of 1 - 255. The minimum length is 1.

#### Buttons

**Add New Entry:** Click to add a new entry to the table.

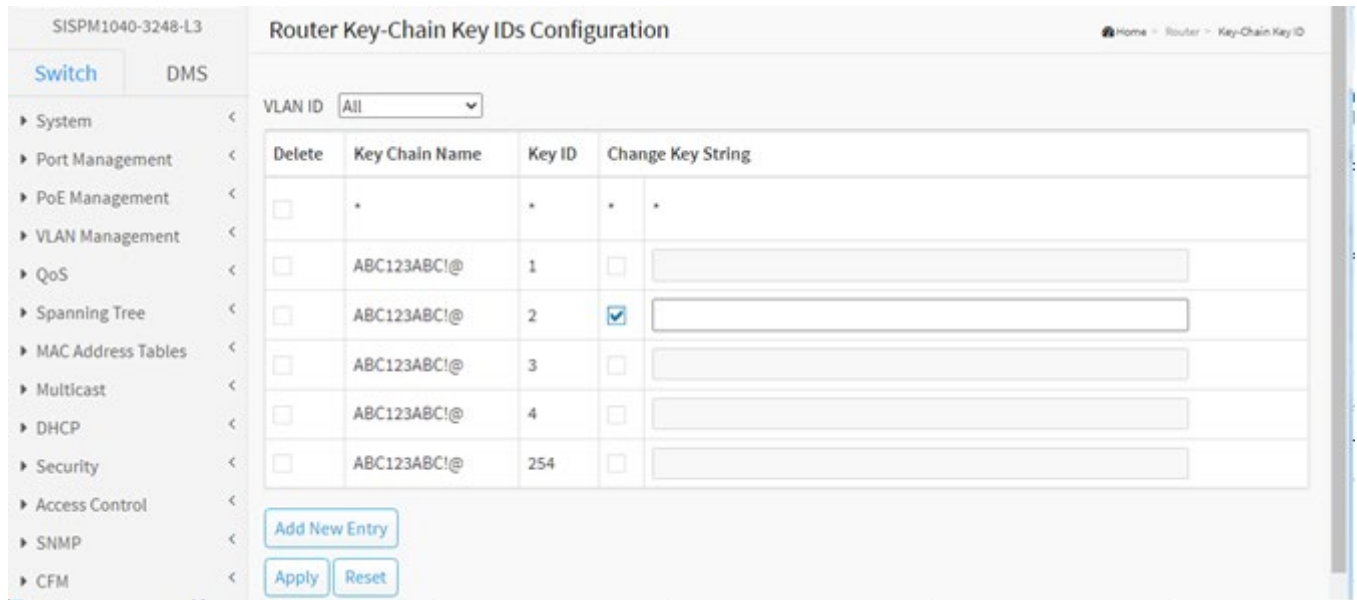
**Apply:** Click to save changes.

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

**Example 1:** Router Key-Chain Key Configuration:

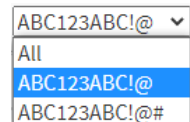


**Example 2:** Router Key-Chain Key IDs Configuration:



**VLAN ID:** At the dropdown select a VLAN ID (e.g., ABC123ABC!@) or select All.

**Change Key String:** Check the box to be able to change the existing Key String. Click the Apply button to save the change.



**Buttons:**

**Add New Entry:** Click to add a new entry to the table.

**Apply:** Click to save changes.

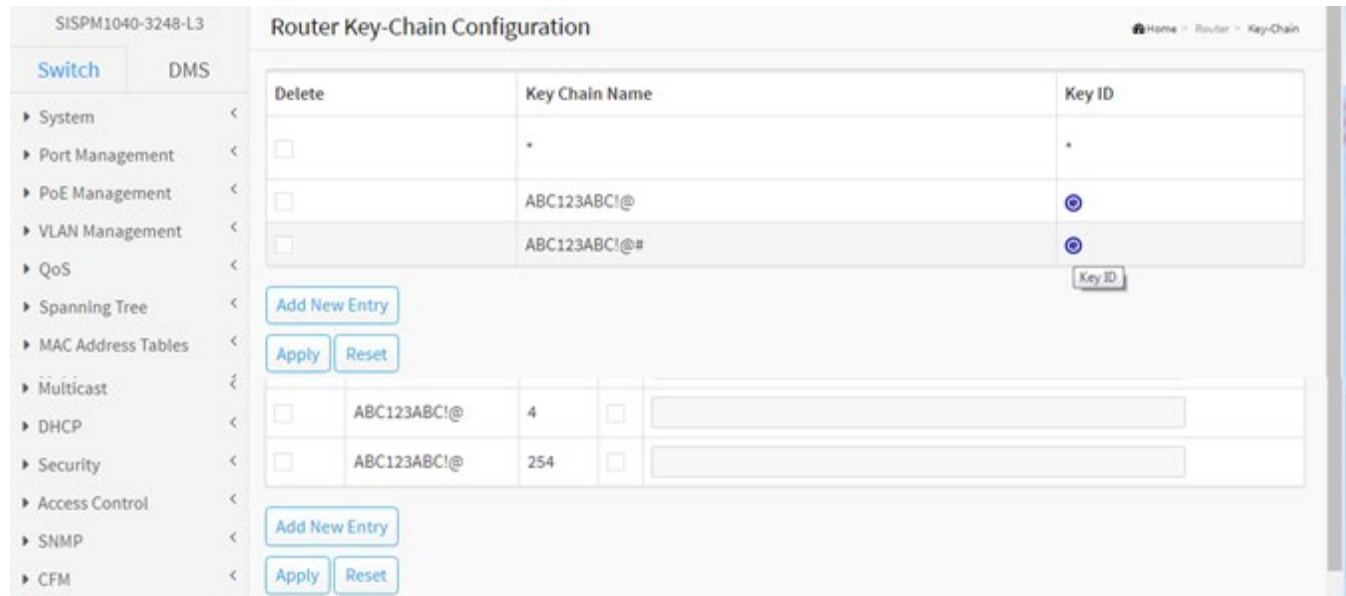
**Reset:** Click to undo any changes made locally and revert to previously saved values.


**Messages:**

*The entry {Key-Chain Name: 'ABC123ABC!@', Key ID:1} already exists.*

*Key ID must be an integer value between 1 and 255*

**Example 3:** Router Key-Chain Key IDs Configuration:



Click the key ID icon (  ) to edit the instance.



## Router > Key-Chain Key-ID

This page lets you set router key chain key ID parameters.

The screenshot shows the 'Router Key-Chain Key IDs Configuration' page. On the left is a navigation menu with categories like System, Port Management, PoE Management, VLAN Management, QoS, Spanning Tree, MAC Address Tables, Multicast, DHCP, Security, Access Control, SNMP, and CFM. The main content area has a 'VLAN ID' dropdown set to 'All'. Below this is a table with the following structure:

Delete	Key Chain Name	Key ID	Change Key String
<input type="checkbox"/>	ABC123ABC!@	4	<input type="text"/>
<input type="checkbox"/>	ABC123ABC!@	254	<input type="text"/>

Buttons for 'Add New Entry', 'Apply', and 'Reset' are located below the table.

**VLAN ID:** At the dropdown select a VLAN ID or select All.

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

**Key Chain Name:** The name of the key-chain entry. The valid name string length is 1-31 characters and allows all printable characters excluding the space character.

**Key ID:** The key chain key ID. The valid range is 1-255.

**Change Key String:** Use to change the key string (fill with plain text). The valid string length is 1-63 plain text characters.

### 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.

**Example:** Router Key-Chain Key IDs Configuration:

The screenshot shows the 'Router Key-Chain Key IDs Configuration' page. On the left is a navigation menu with categories like System, Port Management, PoE Management, VLAN Management, QoS, Spanning Tree, MAC Address Tables, Multicast, DHCP, Security, Access Control, SNMP, and CFM. The main content area has a 'VLAN ID' dropdown set to 'All'. Below it is a table with the following data:

Delete	Key Chain Name	Key ID	Change Key String
<input type="checkbox"/>	*	*	*
<input type="checkbox"/>	ABC123ABC!@	1	<input type="checkbox"/>
<input type="checkbox"/>	ABC123ABC!@	2	<input checked="" type="checkbox"/>
<input type="checkbox"/>	ABC123ABC!@	3	<input type="checkbox"/>
<input type="checkbox"/>	ABC123ABC!@	4	<input type="checkbox"/>
<input type="checkbox"/>	ABC123ABC!@	254	<input type="checkbox"/>

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

**VLAN ID:** At the dropdown select a VLAN ID (e.g., ABC123ABC!@) or select All.

**Change Key String:** Check the box to be able to change the existing Key String. Click the Apply button to save the change.

The dropdown menu shows the following options: ABC123ABC!@ (selected), All, ABC123ABC!@, and ABC123ABC!@#.

**Buttons:**

**Add New Entry:** Click to add a new entry to the table.

**Apply:** Click to save changes.

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

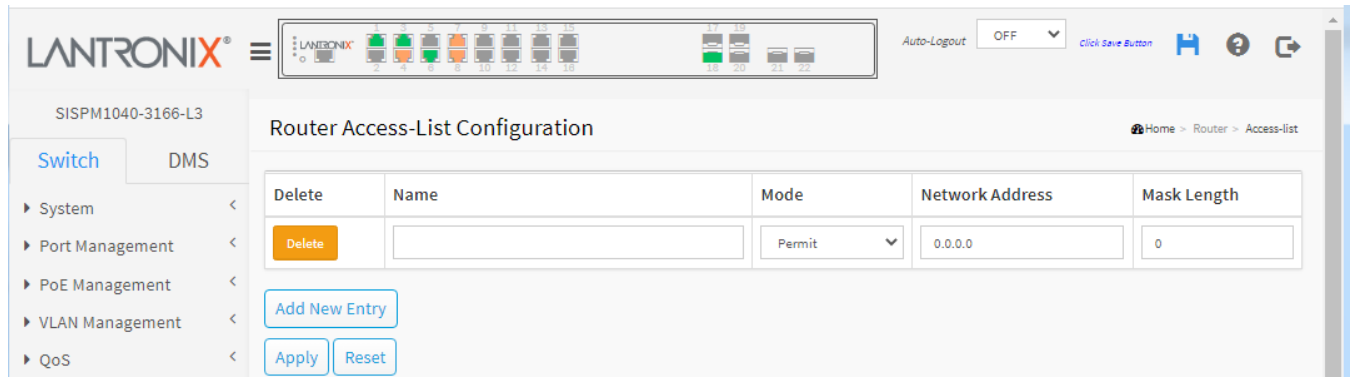
**Messages:**

*The entry {Key-Chain Name: 'ABC123ABC!@', Key ID:1} already exists.*

*Key ID must be an integer value between 1 and 255*

## Router > Access List

This page lets you set router access-list configuration parameters.



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

**Name:** The name of the access-list entry. The valid name string length is 1-31 characters and allows all printable characters excluding space characters.

**Mode:** The access right mode of the access-list entry.

**Permit:** Permit the access right.

**Deny:** Deny the access right.

**Network Address:** The IPv4 address of the access-list entry.

**Mask Length:** The network prefix size of the access-list entry. Subnet Mask Length must be an integer value of 0 - 32.

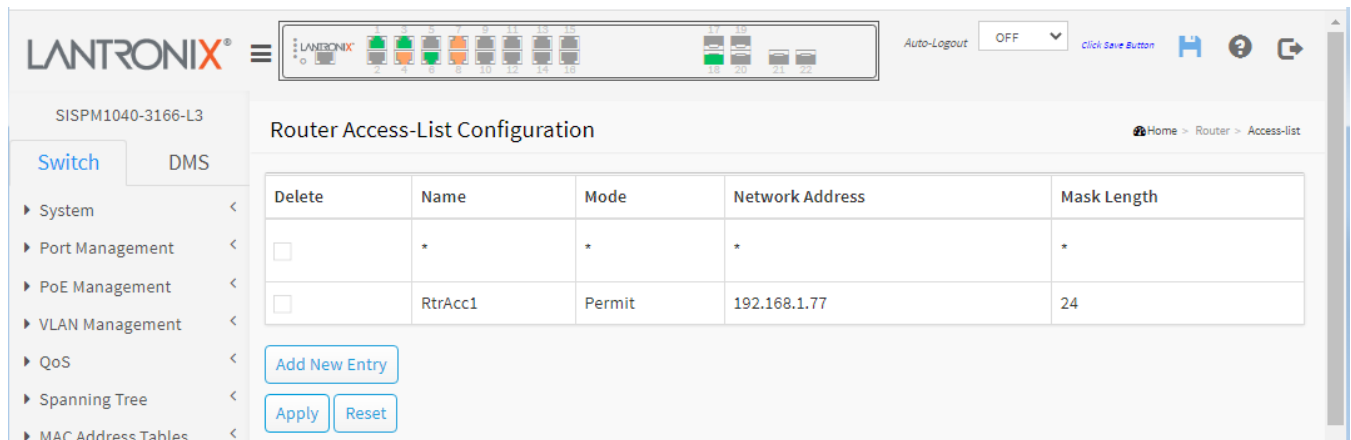
### Buttons

**Add New Entry:** Click to add a new entry to the table.

**Apply:** Click to save changes.

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

### Example:



## OSPF

Open Shortest Path First (OSPF) is a routing protocol for Internet Protocol (IP) networks. It uses a link state routing (LSR) algorithm and is an Interior Gateway Protocol (IGP), operating within a single Autonomous System (AS). It is defined as OSPF Version 2 in RFC 2328 (1998) for IPv4. The updates for IPv6 are specified as OSPF Version 3 in RFC 5340 (2008). OSPF supports the Classless Inter-Domain Routing (CIDR) address model. OSPF is a widely used IGP in large enterprise networks.

### OSPF > Configuration > Global Configuration

From the default page select Enable for the OSPF Router Mode and click Apply to display the OSPF Global Configuration page. This page lets you set common OSPF router global parameters.

The screenshot displays the 'OSPF Global Configuration' page in the Lantronix web interface. The interface includes a top navigation bar with the Lantronix logo, a status bar with 'Auto-Logout OFF', and a breadcrumb trail: 'Home > OSPF > Configuration > Global Configuration'. A left-hand navigation menu lists various system settings, with 'OSPF' and 'Configuration' highlighted. The main configuration area contains the following settings:

- OSPF Router Mode:** Set to 'Enable'.
- Router ID:** Set to 'Auto' with a value of '192.168.1.77'. The 'Specific' option is set to '0.0.0.1'.
- Default Passive Mode:** Set to 'False'.
- Default Metric:** Set to 'Auto' with a value of '0'. The 'Specific' option is set to '0'.
- Redistribute:**
  - Static:** Metric Type is 'None', Metric Value is 'Auto' (0).
  - Connected:** Metric Type is 'None', Metric Value is 'Auto' (0).
  - RIP:** Metric Type is 'None', Metric Value is 'Auto' (0).
- Stub Router:**
  - On Startup:** Mode is 'Disable', Interval is '5'.
  - On Shutdown:** Mode is 'Disable', Interval is '5'.
  - Administrative Mode:** Set to 'Disable'.
- Default Route Redistribution:** Metric Type is 'None', Metric Value is 'Auto' (0), and 'Always' is set to 'Disable'.
- Administrative Distance:** Set to '110'.

Buttons for 'Clear OSPF Process', 'Apply', and 'Reset' are visible at the bottom of the configuration area.

**OSPF Router Mode:** Enable or Disable the OSPF router mode.

**Router ID:** Set the OSPF Router ID in IPv4 address format (A.B.C.D). When the router's OSPF Router ID is changed, if there is one or more fully adjacent neighbors in current OSPF area, the new router ID will take effect after restart OSPF process. **Note** that the router ID should be unique in the Autonomous System and the value '0.0.0.0' is invalid since it is reserved for the default algorithm.

**Auto:** The default algorithm will choose the largest IP address assigned to the router.

**Specific:** User specified router ID. The allowed range is 0.0.0.1 - 255.255.255.254.

**Default Passive Mode:** Configure all interfaces as passive-interface by default. When an interface is configured as a passive-interface, sending OSPF routing updates is suppressed, so the interface does not establish adjacencies (No OSPF Hellos). The subnet of all interfaces (both passive and active) is advertised by the OSPF router.

**Default Metric:** User specified default metric value for the OSPF routing protocol. The field is significant only when the argument 'IsSpecificDefMetric' is TRUE.

**Auto:** The default metric is calculated automatically based on the routing protocols.

**Specific:** Specify the metric to be used. The allowed range is 0 to 16777214.

**Static Redistribute Metric Type:** The OSPF redistributed metric type for the static routes.

**None:** The static routes are not redistributed.

**External Type 1:** External Type 1 of the static routes.

**External Type 2:** External Type 2 of the static routes.

**Static Redistribute Metric Value:** User specified metric value for the static routes. The field is significant only when the argument 'StaticRedistIsSpecificMetric' is TRUE. The allowed range is 0 to 16777214.

**Auto:** The redistributed metric is the same as the original metric value.

**Specific:** User specified metric for the static routes.

**Connected Redistribute Metric Type:** The OSPF redistributed metric type for the connected interfaces.

**None:** The connected interfaces are not redistributed.

**External Type 1:** External Type 1 of the connected interfaces routes.

**External Type 2:** External Type 2 of the connected interfaces routes.

**Connected Redistribute Metric Value:** User specified metric value for the connected interfaces. The field is significant only when the argument 'ConnectedRedistIsSpecificMetric' is TRUE. The allowed range is 0 to 16777214.

**Auto:** The redistributed metric is the same as the original metric value.

**Specific:** User specified metric for the connected routes.

**RIP Redistribute Metric Type:** The OSPF redistributed metric type for the RIP routes. The field is significant only when the RIP protocol is supported on the device.

**None:** The RIP routes are not redistributed.

**External Type 1:** External Type 1 of the RIP routes.

**External Type 2:** External Type 2 of the RIP routes.

**RIP Redistribute Metric Value:** User specified metric value for the RIP routes. The field is significant only when the RIP protocol is supported on the device and argument 'RipRedistIsSpecificMetric' is TRUE. The allowed range is 0 to 16777214.

**Auto:** The redistributed metric is the same as the original metric value.

**Specific:** User specified metric for the RIP routes.

**Stub router during startup period:** Configures OSPF to advertise a maximum metric during startup for a configured period of time.

**Stub router on startup interval time:** User specified time interval (seconds) to advertise itself as stub area. The field is significant only when the on-startup mode is enabled. The allowed range is 5 to 86400 seconds.

**Stub router during shutdown period:** Configures OSPF to advertise a maximum metric during shutdown for a configured period of time. The device advertises a maximum metric when the OSPF router mode is disabled and notice that the mechanism also works when the device reboots but not for the 'reload default' case.

**Stub router on shutdown interval time:** User specified time interval (seconds) to wait till shutdown completed. The field is significant only when the on-shutdown mode is enabled.. The allowed range is 5-100 seconds.

**Stub router administrative mode:** Configures OSPF stub router mode administratively applied, for an indefinite period.

**Default Route Redistribution Metric Type:** The OSPF redistributed metric type for a default route.

**None:** The default route are not redistributed.

**External Type 1:** External Type 1 of the default route.

**External Type 2:** External Type 2 of the default route.

**Default Route Redistribution Metric value:** User specified metric value for a default route. The field is significant only when the argument 'DefaultRouteRedistIsSpecificMetric' is TRUE. The allowed range is 0 - 16777214.

**Auto:** The redistributed metric is the same as the original metric value.

**Specific:** User specified metric for the default route.

**Default Route Redistribution Always:** Specifies to always advertise a default route into all external-routing capable areas. Otherwise, the router only to advertise the default route when the advertising router already has a default route.

**Administrative Distance:** The OSPF administrative distance. Administrative Distance must be an integer value between 1 and 255.

## Buttons

**Clear OSPF Process:** Click to reset the current OSPF process.

**Apply:** Click to save changes.

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

## Messages:

*Administrative Distance must be an integer value between 1 and 255.*

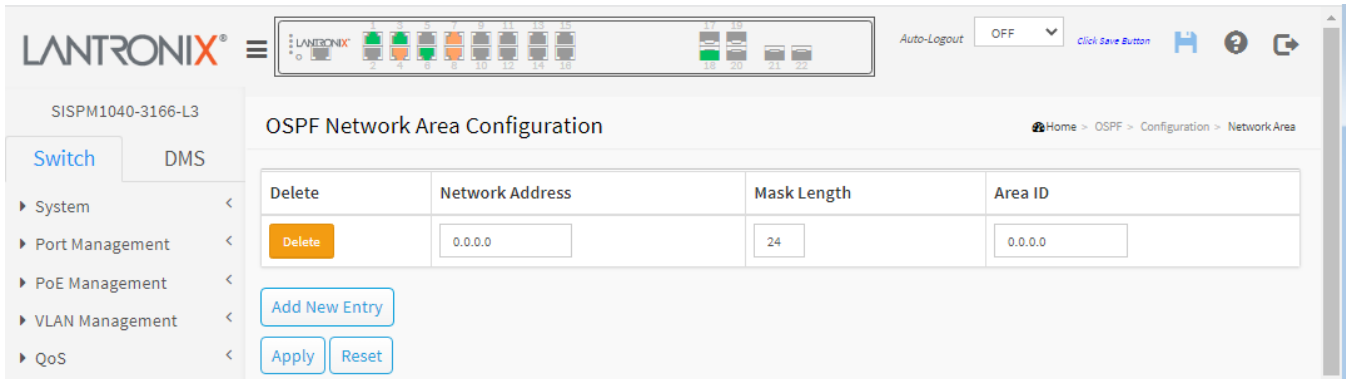
*Stub router on startup interval must be an integer value between 5 and 86400*

*Default route Redistribute Metric must be an integer value between 0 and 16777214*

*RIP Redistribute Metric must be an integer value between 0 and 16777214*

## OSPF > Configuration > Network Area

This page lets you set OSPF area parameters. It is used to specify the OSPF enabled interface(s). When OSPF is enabled on the specific interface(s), the router can provide the network information to the other OSPF routers via those interfaces.



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

**Network Address:** IPv4 network address.

**Mask Length:** IPv4 network mask length.

**Area ID:** The OSPF area ID.

### Buttons

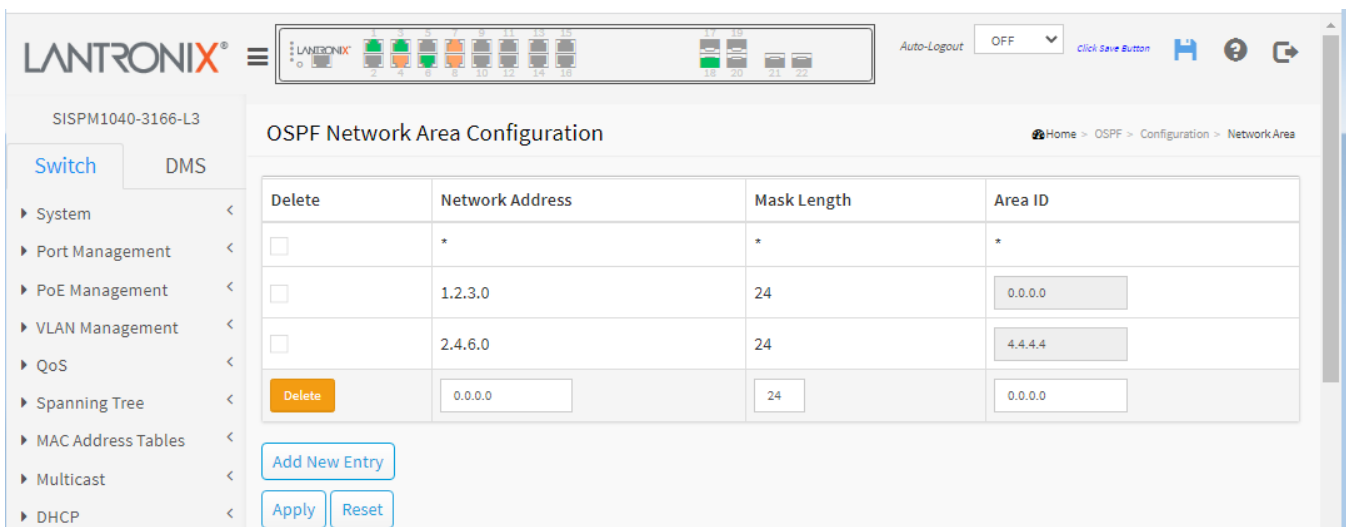
**Add New Entry:** Click to add new entry.

**Apply:** Click to save changes.

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

**Messages:** *The entry {Network Address:0.0.0.0, Mask Length:24} address range overlaps with {Network Address:0.0.0.0, Mask Length:24}.*

### Example:



## OSPF > Configuration > Passive Interface

This page lets you set OSPF router interface parameters.

Interface	Passive Interface
*	<input type="checkbox"/>
VLAN 1	<input checked="" type="checkbox"/>

**Interface:** The Interface identification.

**Passive Interface:** Check the box to enable the interface as an OSPF passive-interface.

### Buttons

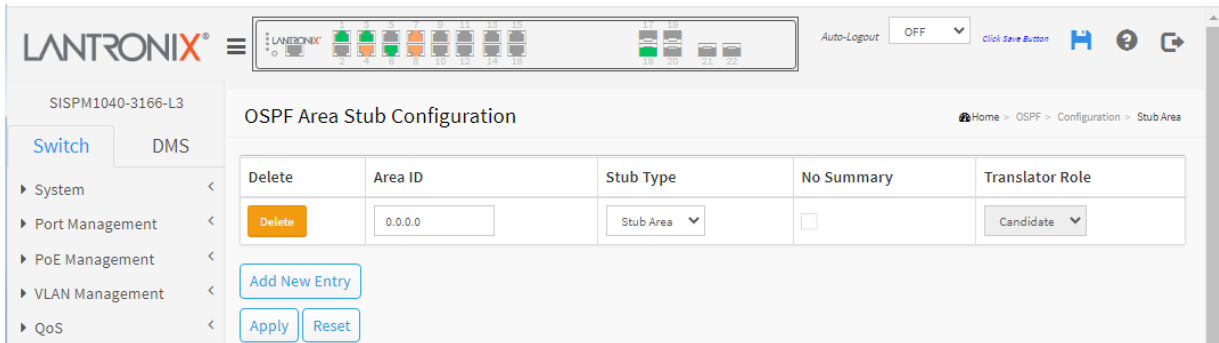
**Apply:** Click to save changes.

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



## OSPF > Configuration > Stub Area

This page lets you set OSPF stub area parameters. The configuration is used to reduce the link-state database size and therefore reduce memory and CPU requirements by forbidding some LSAs.



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

**Area ID:** The OSPF area ID.

**Stub Type:** The OSPF stub configured type.

**Stub Area:** Configure the area as stub area.

**NSSA:** Configure the area as not-so-stubby area (NSSA).

**No Summary:** The value is true to configure the inter-area routes do not inject into this stub area.

**Translator Role:** The OSPF NSSA translator role.

**Candidate:** this NSSA-ABR router will participate in the translator election.

**Never:** this NSSA-ABR router never translates.

**Always:** this NSSA-ABR router always translates.

### Buttons

**Add New Entry:** Click to add new entry.

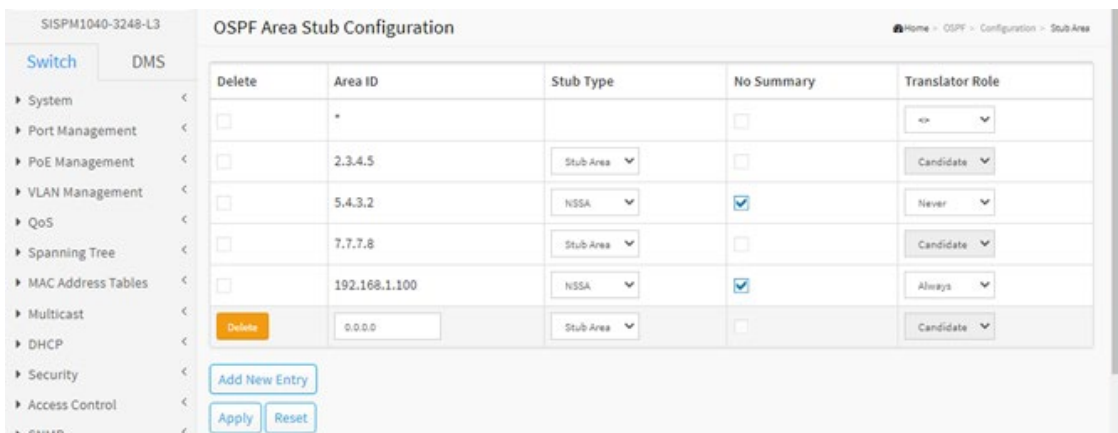
**Apply:** Click to save changes.

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

### Messages:

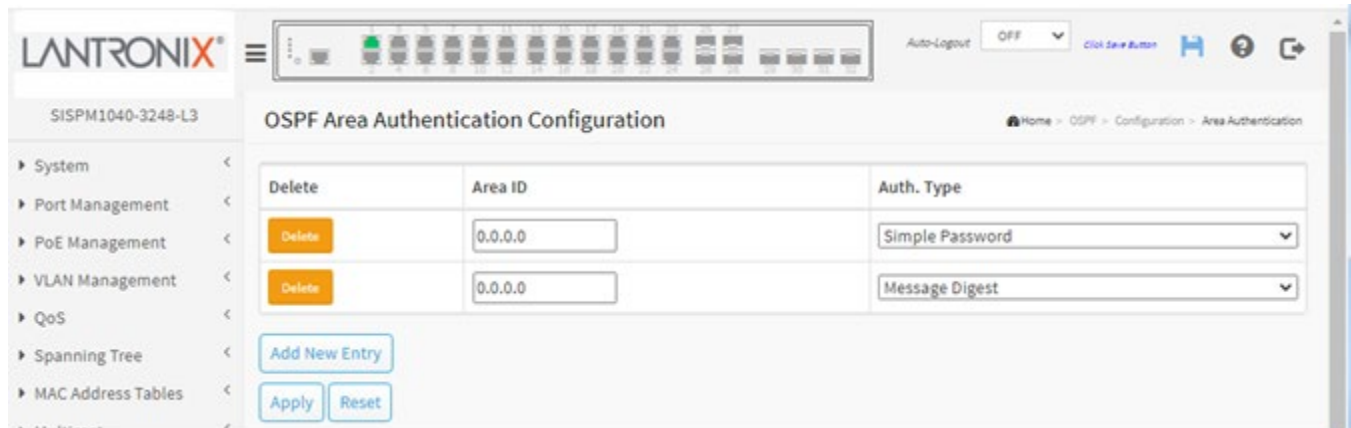
*JSON RPC Error. (Backbone can not be configured as stub area)*

### Example:



## OSPF > Configuration > Area Authentication

This page lets you set OSPF area authentication parameters. It is used to apply the authentication to all the interfaces belong to the OSPF area. No entry exists initially.



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

**Area ID:** The OSPF area ID.

**Auth. Type:** The authentication type on an area is applied to all the interfaces belong to that area. The authentication type on an IP interface or a virtual link overrides the authentication type on an area and is useful if different interfaces in the same area use different authentication types.

Specify the authentication type to be used:

**Simple Password:** Simple password authentication (default).

**Message Digest:** MD5 digest authentication.

### Buttons

**Add New Entry:** Click to add new entry.

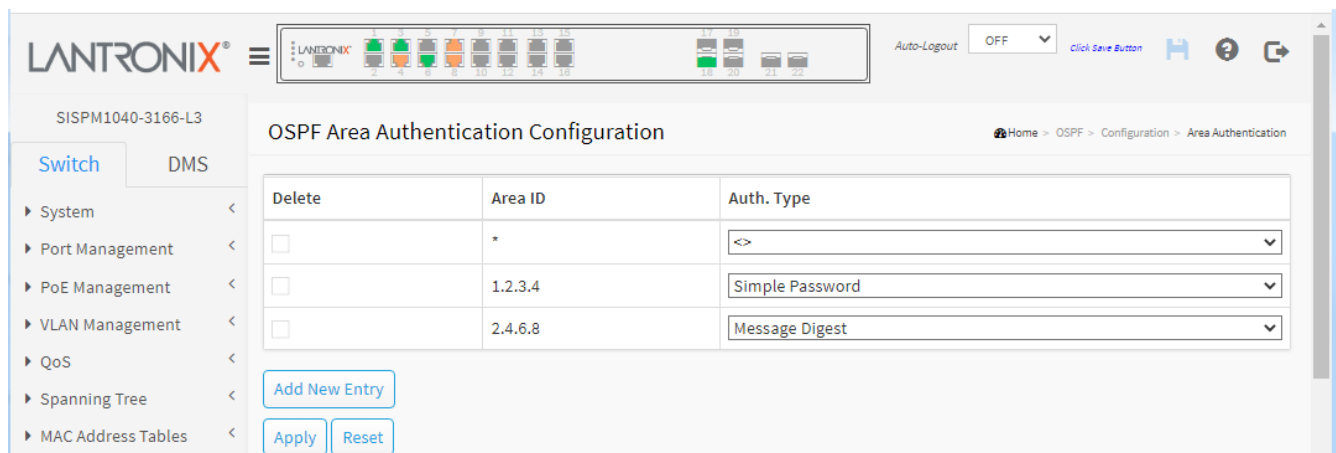
**Apply:** Click to save changes.

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

### Messages:

*The new entry {0.0.0.0} is duplicated.*

### Example:



## OSPF > Configuration > Area Range

This page lets you set OSPF area range parameters. It is used to summarize the intra area paths from a specific address range in one summary-LSA (Type-3) and advertised to other areas or configure the address range status as 'DoNotAdvertise' which suppresses the summary-LSA (Type-3).

The area range configuration is used for Area Border Routers (ABRs) and only router-LSAs (Type-1) and network-LSAs (Type-2) can be summarized.

The AS-external-LSAs (Type-5) cannot be summarized because the scope is OSPF autonomous system (AS). The AS-external-LSAs (Type-7) cannot be summarized because the feature is not supported yet.

The link-state advertisement (LSA) is a basic communication means of the OSPF routing protocol for the Internet Protocol (IP). It communicates the router's local routing topology to all other local routers in the same OSPF area. OSPF is designed for scalability, so some LSAs are not flooded out on all interfaces, but only on those that belong to the appropriate area. In this way detailed information can be kept localized, while summary information is flooded to the rest of the network. The original IPv4-only OSPFv2 and the newer IPv6-compatible OSPFv3 have broadly similar LSA types.

Delete	Area ID	Network Address	Mask Length	Advertise	Cost
<input type="checkbox"/>	0.0.0.0	0.0.0.0	24	<input checked="" type="checkbox"/>	Auto

Buttons: Add New Entry, Apply, Reset

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

**Area ID:** The OSPF area ID.

**Network Address:** IPv4 network address.

**Mask Length:** IPv4 network mask length.

**Advertise:** When the box is checked, it summarizes intra area paths from the address range in one summary-LSA (Type-3) and advertised to other areas. If the box is unchecked, the intra area paths from the address range are not advertised to other areas.

**Cost:** The cost (or metric) for this summary route. It can only be configured only when 'Specific' is selected.

**Auto:** The cost value is set to 0 automatically and cannot be configured (default).

**Specific:** Specify a cost (metric) for this summary route. The allowed range is 0 – 16777215.

### Buttons

**Add New Entry:** Click to add new entry.

**Apply:** Click to save changes.

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

**Messages:**

*JSON RPC Error. (Area range network address cannot represent default)*

*The entry {0.0.0.0, 0.0.0.0, 24} address range overlaps with {0.0.0.0, 0.0.0.0, 24}.*

*Cost must be an integer value between 0 and 16777215*

*JSON RPC Error. (Area range not-advertise and cost can not be set at the same time)*

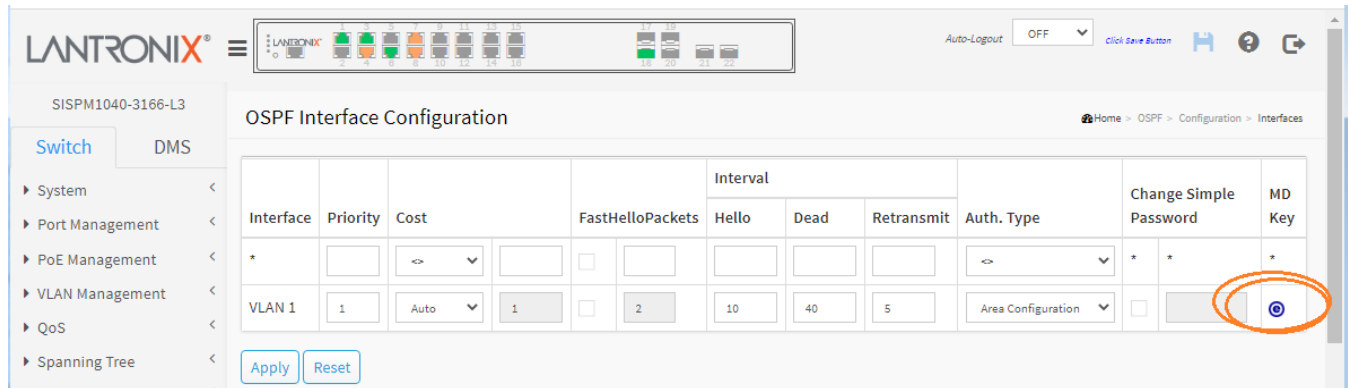
**Example:** Five Area IDs configured.

SISPM1040-3248-L3 OSPF Area Range Configuration Home > OSPF > Configuration > Area Range

Delete	Area ID	Network Address	Mask Length	Advertise	Cost
<input type="checkbox"/>	*	*	*	<input checked="" type="checkbox"/>	<< 65535
<input type="checkbox"/>	0.0.0.0	1.2.3.0	24	<input checked="" type="checkbox"/>	Specific 65535
<input type="checkbox"/>	2.3.4.5	2.1.1.0	24	<input checked="" type="checkbox"/>	Specific 16777215
<input type="checkbox"/>	9.9.9.9	9.9.9.0	24	<input checked="" type="checkbox"/>	Specific 0
<input type="checkbox"/>	192.168.1.7	192.168.2.0	24	<input checked="" type="checkbox"/>	Auto 0
<input type="checkbox"/>	192.168.1.77	192.168.1.0	24	<input checked="" type="checkbox"/>	Auto 0

## OSPF > Configuration > Interfaces

This page lets you set OSPF interface parameters.



**Interface:** The Interface identification.

**Priority:** User specified router priority for the interface. The allowed range is 0-255 and the default value is 1.

**Cost:** User specified cost for this interface. It's link state metric for the interface. The field is significant only when 'IsSpecificCost' is TRUE. The allowed range is 1-65535 and the default setting is 'Auto' cost mode.

**FastHelloPackets:** How many Hello packets will be sent per second. The allowed range is 1-10 and the default setting is disabled.

**Hello Interval:** Set the number of Hello packets to be sent per second. The allowed range is 1 to 65535 and the default value is 10 seconds.

**Dead Interval:** Set the time interval (in seconds) between hello packets. The allowed range is 1-65535 and the default value is 40 seconds.

**Retransmit Interval:** Set the time interval (in seconds) between link-state advertisement(LSA) retransmissions for adjacencies. The allowed range is 3-65535 seconds and the default value is 5 seconds.

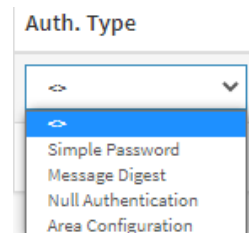
**Auth. Type:** At the dropdown select the authentication type:

**Simple Password:** It uses a plain text authentication. A password must be configured, but the password can be read by a packet sniffer (AKA, packet analyzer, protocol analyzer, network analyzer).

**Message Digest:** Use Message-Digest algorithm 5 (MD5) authentication. Keying material must also be configured. This is the most secure method.

**Null Authentication:** No authentication will be used.

**Area Configuration:** Refer to the [OSPF > Configuration > Area Authentication](#) setting on page 358.



**Change Simple Password:** It is used to change the simple password (fill with plain text). The allowed input length is 1-8 characters.


**MD Key:** Click the Edit icon (⊕) to edit the message digest key for the entry on its OSPF Interface Message Digest Configuration page (see below).

### Buttons

**Apply:** Click to save changes.

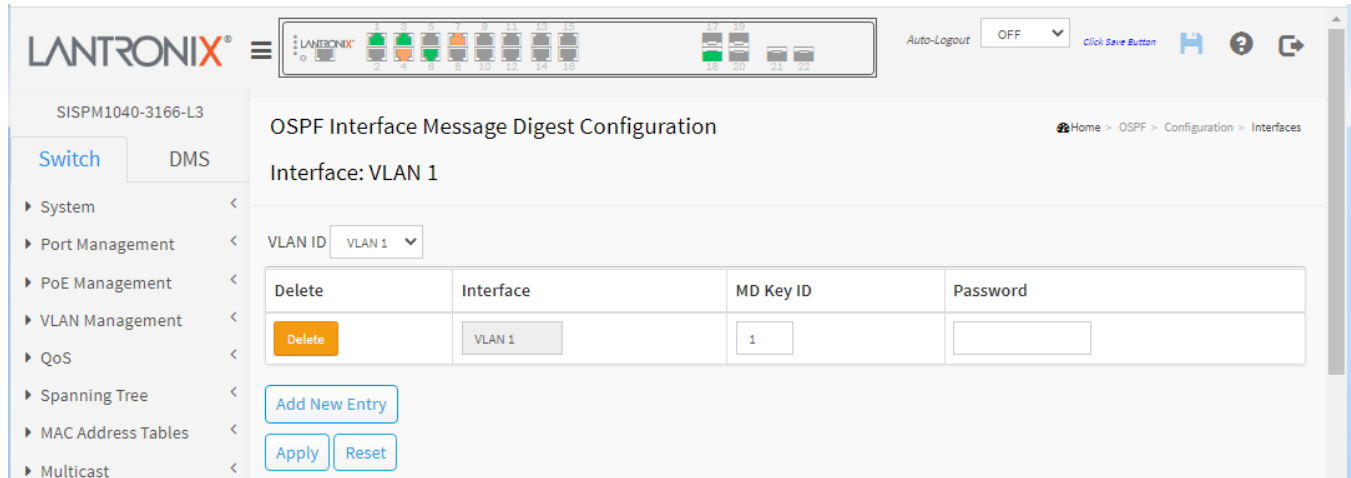
**Reset:** Click to undo any changes made locally and revert to previously saved values.

## OSPF Interface Message Digest Configuration page

In the MD Key column click the Edit icon (  ) to edit the message digest key for the entry.

This page displays the interface authentication message digest key configuration table. The listed entry sequence order is set by the Message Digest key precedence.

Click the Add New Entry button and at the dropdown select a VLAN ID.



The screenshot shows the Lantronix web interface for configuring OSPF Interface Message Digest. The page title is "OSPF Interface Message Digest Configuration" and the interface is "VLAN 1". A table displays the configuration entries:

Delete	Interface	MD Key ID	Password
<input type="button" value="Delete"/>	VLAN 1	1	<input type="text"/>

Buttons for "Add New Entry", "Apply", and "Reset" are located below the table. A "VLAN ID" dropdown menu is also present, showing "VLAN 1" selected.


**Delete:** Check to delete the entry.

**Interface:** Interface identification.

**MD Key ID:** The key ID for message digest authentication. The allowed range is 1-255.

**Password:** The message digest key. The allowed input length is 1-16 characters.

### Buttons

VLAN ID    
  
 VLAN ID dropdown: select a VLAN ID or All VLAN IDs.

**Add New Entry:** Click to add new entry to the table.

**Apply:** Click to save changes.

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

### Messages:

*The entry {Interface:VLAN 1, MD Key ID:1} already exists.*

*JSON RPC Error. (The password/key is invalid)*

*The minimum length of simple password is 1.*

**Example:**

The screenshot displays the Lantronix web management interface for a device (SISPM1040-3166-L3). The page title is "OSPF Interface Message Digest Configuration". The left sidebar shows a navigation menu with "Switch" selected. The main content area features a table with columns for "Delete", "Interface", "MD Key ID", and "Password". Below the table are buttons for "Add New Entry", "Apply", and "Reset".

Delete	Interface	MD Key ID	Password
<input type="checkbox"/>	*	*	*
<input type="checkbox"/>	VLAN 1	1	*****
<input type="checkbox"/>	VLAN 1	2	*****
<input type="checkbox"/>	VLAN 1	3	*****
<input type="button" value="Delete"/>	VLAN 1	1	

## OSPF > Configuration > Virtual Link

This page lets you set OSPF virtual link parameters. The virtual link is established between two ABRs to overcome the fact that all the areas must be connected directly to the backbone area.

Delete	Area ID	Router ID	Interval			Auth. Type	Change Simple Password	MD Key
			Hello	Dead	Retransmit			
<input type="checkbox"/>	0.0.0.0	0.0.0.0	10	40	5	Area Configuration	<input checked="" type="checkbox"/>	

Buttons: Add New Entry, Apply, Reset

**Delete:** Check to delete the entry.

**Area ID:** OSPF Area ID.

**Router ID:** OSPF router ID.

**Hello Interval:** The time interval (in seconds) between hello packets. The allowed range is 1-65535 seconds, and the default value is 10 seconds.

**Dead Interval:** The number of seconds to wait until the neighbor is declared to be dead. The allowed range is 1-65535 seconds and the default value is 40 seconds.

**Retransmit Interval:** The time interval (in seconds) between link-state advertisement(LSA) retransmissions for adjacencies. The allowed range is 3-65535 seconds, and the default value is 5 seconds.

**Auth. Type:** The authentication type on an area.

**Simple Password:** Use a plain text authentication. A password must be configured, but the password can be read by packet sniffers.

**Message Digest:** It's message-digest algorithm 5 (MD5) authentication. Keying material must also be configured. This is the most secure method.

**Null Authentication:** No authentication.

**Area Configuration:** Refer to the Area authentication setting.

**Change Simple Password:** It is used to change the simple password (fill with plain text). The allowed input length is 1 to 8 characters.

**MD Key:** Click the Edit icon (🔗) to edit the message digest key for the entry. The OSPF Virtual Link Message Digest Configuration page displays (see below).

### Buttons

**Add New Entry:** Click to add new entry.

**Apply:** Click to save changes.

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

### Messages:

*Backbone area(0.0.0.0) can not be configured as virtual link.*



**Example 1:**

SISPM1040-3248-L3 OSPF Virtual Link Configuration

Switch DMS

- System
- Port Management
- PoE Management
- VLAN Management
- QoS
- Spanning Tree
- MAC Address Tables
- Multicast
- DHCP

Delete	Area ID	Router ID	Interval			Auth. Type	Change Simple Password		MD Key
			Hello	Dead	Retransmit		<input type="checkbox"/>	<input type="text"/>	
<input type="button" value="Delete"/>	<input type="text" value="0.0.0.0"/>	<input type="text" value="0.0.0.0"/>	<input type="text" value="10"/>	<input type="text" value="40"/>	<input type="text" value="5"/>	Area Configuration	<input checked="" type="checkbox"/>	<input type="text"/>	
<input type="button" value="Delete"/>	<input type="text" value="1.2.3.4"/>	<input type="text" value="0.0.0.0"/>	<input type="text" value="10"/>	<input type="text" value="40"/>	<input type="text" value="5"/>	Simple Password	<input checked="" type="checkbox"/>	<input type="text"/>	
<input type="button" value="Delete"/>	<input type="text" value="2.4.6.8"/>	<input type="text" value="1.2.3.4"/>	<input type="text" value="10"/>	<input type="text" value="40"/>	<input type="text" value="5"/>	Area Configuration	<input checked="" type="checkbox"/>	<input type="text" value="....."/>	

**Example 2:**


SISPM1040-3248-L3 OSPF Virtual Link Configuration

Switch DMS

- System
- Port Management
- PoE Management
- VLAN Management
- QoS
- Spanning Tree
- MAC Address Tables
- Multicast
- DHCP
- Security
- Access Control

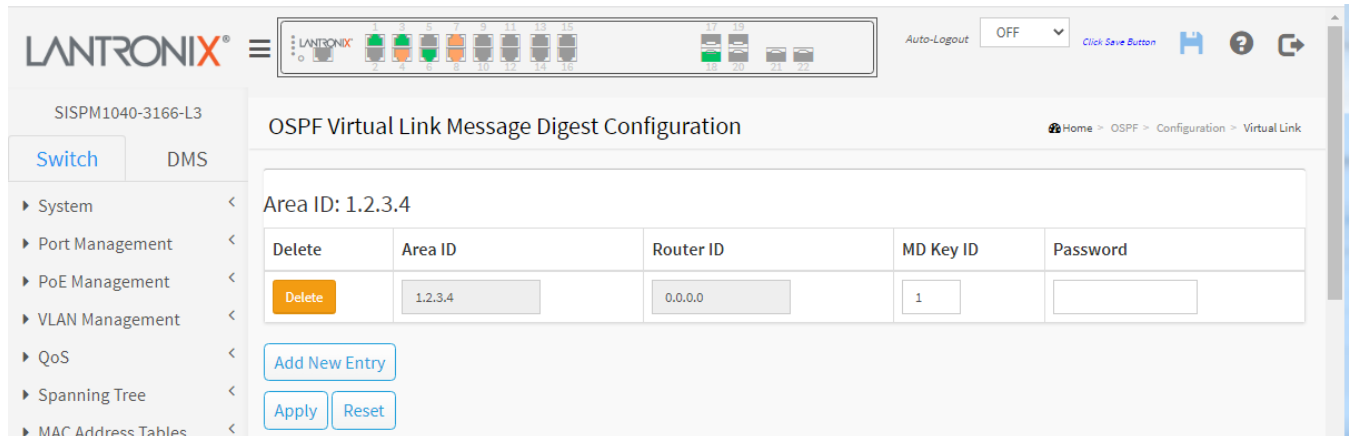
Delete	Area ID	Router ID	Interval			Auth. Type	Change Simple Password		MD Key
			Hello	Dead	Retransmit		<input type="checkbox"/>	<input type="text"/>	
<input type="checkbox"/>	*	*	<input type="text"/>	<input type="text"/>	<input type="text"/>	<>	<input type="checkbox"/>	<input type="text"/>	*
<input type="checkbox"/>	1.2.3.4	0.0.0.0	<input type="text" value="10"/>	<input type="text" value="40"/>	<input type="text" value="5"/>	Simple Password	<input type="checkbox"/>	<input type="text"/>	<input type="button" value="⊕"/>
<input type="checkbox"/>	2.3.4.9	2.3.4.99	<input type="text" value="10"/>	<input type="text" value="40"/>	<input type="text" value="5"/>	Null Authentication	<input type="checkbox"/>	<input type="text"/>	<input type="button" value="⊕"/>
<input type="checkbox"/>	2.4.6.8	1.2.3.4	<input type="text" value="10"/>	<input type="text" value="40"/>	<input type="text" value="5"/>	Message Digest	<input type="checkbox"/>	<input type="text"/>	<input type="button" value="⊕"/>
<input type="checkbox"/>	4.3.2.1	0.0.0.0	<input type="text" value="10"/>	<input type="text" value="40"/>	<input type="text" value="5"/>	Area Configuration	<input checked="" type="checkbox"/>	<input type="text"/>	<input type="button" value="⊕"/>

## OSPF Virtual Link Message Digest Configuration page

On the OSPF Virtual Link Configuration click the Edit MD Key control (  ). This page lets you set OSPF virtual link parameters.

The virtual link is established between two ABRs to overcome the fact that all the areas must be connected directly to the backbone area.

The listed entry sequence order is set by the Message Digest key precedence.



The screenshot displays the 'OSPF Virtual Link Message Digest Configuration' page. At the top, there is a navigation bar with the Lantronix logo and a menu icon. Below the logo, there are several status indicators (ports 1-22) and an 'Auto-Logout' dropdown set to 'OFF'. The main content area has a breadcrumb trail: Home > OSPF > Configuration > Virtual Link. On the left, there is a sidebar menu with options like System, Port Management, PoE Management, VLAN Management, QoS, Spanning Tree, and MAC Address Tables. The main configuration area shows 'Area ID: 1.2.3.4' and a table with the following structure:

Delete	Area ID	Router ID	MD Key ID	Password
<input type="checkbox"/>	1.2.3.4	0.0.0.0	1	

Below the table are buttons for 'Add New Entry', 'Apply', and 'Reset'.

**Delete:** Check to delete the entry.

**Area ID:** OSPF Area ID.

**Router ID:** OSPF router ID.

**MD Key ID:** The key ID for message digest authentication. The allowed range is 1-255.

**Password:** The password of message digest key, it is the plain text input field for the new entry. The allowed input length is 1- 16 plain text characters.

### Buttons

**Add New Entry:** Click to add new entry.

**Apply:** Click to save changes.

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

### Messages:

*Backbone area(0.0.0.0) can not be configured as virtual link.*

## OSPF > Status

This section provides various OSPF statuses.

### OSPF > Status > Global Status

This page displays the OSPF router status table which provides OSPF router status information.

The screenshot shows the Lantronix web interface for device SISPM1040-3166-L3. The page title is "OSPF Global Status". At the top, there is a navigation menu with "Switch" selected and "DMS" as an alternative. A sidebar on the left lists various system management options like System, Port Management, PoE Management, etc. The main content area features an "Auto-refresh" toggle set to "off", with "Refresh" and "Clear OSPF Process" buttons. Below this is a "Status Information" table.

Status Information	
Router ID	192.168.1.77
SPF Delay	200 msecs
SPF Hold Time	400 msecs
SPF Max. Wait Time	10000 msecs
Last Executed SPF Time Stamp	0 msecs
Min. LSA Interval	5 secs
Min. LSA Arrival	1000 msecs
External LSA Count	1 msecs
External LSA Checksum	0xC90
Attached Area Count	4

**Router ID:** OSPF router ID.

**SPF Delay:** Delay time (in milliseconds) of SPF calculations.

**SPF Hold Time:** Minimum hold time (in milliseconds) between consecutive SPF calculations.

**SPF Max. Wait Time:** Maximum wait time (in milliseconds) between consecutive SPF calculations.

**Last Executed SPF Time Stamp:** Time (in milliseconds) that has passed between the start of the SPF algorithm execution and the current time.

**Min. LSA Interval:** Minimum interval (in seconds) between link-state advertisements.

**Min. LSA Arrival:** Maximum arrival time (in milliseconds) of link-state advertisements.

**External LSA Count:** Number of external link-state advertisements.

**External LSA Checksum:** Number of external link-state checksum.

**Attached Area Count:** Number of areas attached for the router.

#### Buttons

**Clear OSPF Status:** Click to reset the current OSPF process.

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

**Refresh:** Click to refresh the page immediately.

## OSPF > Status > Area Status

This page displays the OSPF network area status table which provides OSPF network area status information.

Area ID	Backbone	Area Type	NSSA translator State	Active Interfaces	Auth. Type	SPF Executed Times	LSA count	Router LSA		Network LSA		Summary LSA		ASBR Summary LSA		NSSA LSA	
								Count	Checksum	Count	Checksum	Count	Checksum	Count	Checksum	Count	Checksum
0.0.0.0	Yes	Normal	disabled	0	None	0	0	0	0x0	0	0x0	0	0x0	0	0x0	0	0x0
1.2.3.4	No	Normal	disabled	0	Simple Password	0	0	0	0x0	0	0x0	0	0x0	0	0x0	0	0x0
2.4.6.8	No	Normal	disabled	0	Message Digest	0	0	0	0x0	0	0x0	0	0x0	0	0x0	0	0x0
3.3.3.3	No	Normal	disabled	0	None	0	0	0	0x0	0	0x0	0	0x0	0	0x0	0	0x0

**Area ID:** The Area ID.

**Backbone:** Indicate if it's backbone area or not.

**Area Type:** The area type (e.g., Normal, Stub, NSSA).

**NSSA translator State:** Indicate the current state of the NSSA-ABR translator which the router uses to translate Type-7 LSAs in the NSSA to Type-5 LSAs in backbone area.

**Active Interfaces:** Number of active interfaces attached in the area.

**Auth. Type:** The authentication type in the area (Simple Password, Message Digest or None).

**SPF Executed Times:** Number of times SPF algorithm has been executed for the particular area.

**LSA Count:** Number of the total LSAs for the particular area.

**Router LSA Count:** Number of the router-LSAs (Type-1) of a given type for the particular area.

**Router LSA Checksum:** The router-LSAs (Type-1) checksum.

**Network LSA Count:** Number of the network-LSAs (Type-2) of a given type for the particular area.

**Network LSA Checksum:** The network-LSAs (Type-2) checksum.

**Summary LSA Count:** Number of the summary-LSAs (Type-3) of a given type for the particular area.

**Summary LSA Checksum:** The summary-LSAs (Type-3) checksum.

**ASBR Summary LSA Count:** Number of the ASBR-summary-LSAs (Type-4) of a given type for the particular area.

**ASBR Summary LSA Checksum:** The ASBR-summary-LSAs (Type-4) checksum.

**NSSA LSA Count:** Number of the NSSA LSAs of a given type for the particular area.

**NSSA LSA Checksum:** The NSSA LSAs checksum.

### Buttons

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

**Refresh:** Click to refresh the page immediately.

## OSPF > Status > Neighbor Status

This page displays the OSPF IPv4 neighbor status table which provides OSPF neighbor status information.

The screenshot shows the Lantronix web interface for device SISPM1040-3166-L3. The main content area is titled 'OSPF Neighbor Status'. It features an 'Auto-refresh' toggle set to 'off' and a 'Refresh' button. Below this is a table with the following columns: Neighbor ID, Priority, State, Dead Time, Interface Address, and Interface. The table currently displays 'No entry exists'.

Neighbor ID	Priority	State	Dead Time	Interface Address	Interface
No entry exists					

**Neighbor ID:** The Neighbor ID.

**Priority:** The priority of OSPF neighbor. It indicates the priority of the neighbor router. This item is used when selecting the DR for the network. The router with the highest priority becomes the DR.

**State:** The state of OSPF neighbor. It indicates the functional state of the neighbor router.

**Dead Time:** Indicates the amount of time remaining that the router waits to receive an OSPF hello packet from the neighbor before declaring the neighbor down.

**Interface Address:** The IP address.

**Interface:** The network interface.

### Buttons

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

**Refresh:** Click to refresh the page immediately.

## OSPF > Status > Interface Status

This page displays the OSPF interface status table which provides the OSPF interface status information.

Interface	Interface Address	Area ID	Router ID	State	DR		BDR		Pri	Cost	Interval Configuration(sec)				Hello Timer	Neighbor	Adj Count	Passive	Transmit Delay
					ID	Address	ID	Address			Hello	Dead	Wait	Retransmit					
OSPF-VLINK 1	0.0.0.0/0	0.0.0.0	192.168.1.77	DOWN	0.0.0.0	0.0.0.0	0.0.0.0	0.0.0.0	1	10	10	40	40	5	00:00:00	0	0	false	1 sec

**Interface:** Interface identification.

**Interface Address:** The IPv4 network address.

**Area ID:** The OSPF area ID.

**Router ID:** The OSPF router ID.

**State:** The state of the link (UP or DOWN).

**DR ID:** The router ID of DR.

**DR Address:** The IP address of DR.

**BDR ID:** The router ID of BDR.

**BDR Address:** The IP address of BDR.

**Priority:** The OSPF priority; it helps determine the DR and BDR on the network to which this interface is connected.

**Cost:** The cost of the interface.

**Hello:** Hello timer; a time interval that a router sends an OSPF hello packet.

**Dead:** Dead timer is a time interval to wait before declaring a neighbor dead. The unit of time is seconds.

**Wait:** This interval is used in Wait Timer. Wait timer is a single shot timer that causes the interface to exit waiting and select a DR on the network. Wait Time interval is the same as Dead time interval.

**Retransmit:** Retransmit timer. A time interval to wait before retransmitting a database description packet that has not been acknowledged.

**Hello Timer:** Hello due timer; an OSPF hello packet will be sent on this interface after this due time.

**Neighbor:** Neighbor count; the number of OSPF neighbors discovered on this interface.

**Adj Count:** Adjacent neighbor count; the number of routers running OSPF that are fully adjacent with this router.

**Passive:** True indicates if the interface is passive interface, otherwise False.

**Transmit Delay:** The estimated time to transmit a link-state update packet on the interface.

### Buttons

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

**Refresh:** Click to refresh the page immediately.

## OSPF > Status > Routing Status

This page displays the OSPF routing status table.

Each page shows up to 999 table entries, selected through the "entries per page" input field. When first visited, the web page will show the beginning entries of this table.

The screenshot shows the Lantronix web interface for the device SISPM1040-3166-L3. The page title is "OSPF Routing Status". The interface includes a navigation menu on the left with options like System, Port Management, PoE Management, VLAN Management, QoS, Spanning Tree, and MAC Address Tables. The main content area has an "Auto-refresh" toggle set to "off" and a "Refresh" button. Below that, it shows "0 - 0 of 0 entry" with navigation arrows. Search filters include "Start from Route Type" (set to "Intra Area"), "Destination" (0.0.0.0), "Area" (0.0.0.0), and "NextHop" (0.0.0.0). There is an "entries per page" input field set to 20. A legend indicates "Codes: i - Intra-area Router Path, I - Inter-area Router Path". A table with columns: Route Type, Destination, Area, NextHop, Cost, AS Cost, Border Router Type, Interface, and IsConnected is shown, but it is empty with the text "No entry exists".

### Controls:

**Start from Route Type:** This input field lets you change the starting point of this table. At the dropdown select Intra Area, Inter Area, Border Router, External Type-1, or External Type-2. The default is Intra Area.

**Destination:** Enter the destination IP in the format 0.0.0.0/0.

**Area:** Enter the area IP in the format 0.0.0.0.

**Next Hop:** Enter the next hop IP in the format 0.0.0.0.

**Codes:** **i** - Intra-area Router Path, **I** - Inter-area Router Path.

### Parameters:

**Route Type:** The OSPF route type:

**Intra Area:** The destination is an OSPF route which is located on intra-area.

**Inter Area:** The destination is an OSPF route which is located on inter-area.

**Border Router:** The destination is a border router.

**External Type-1:** The destination is an external Type-1 route.

**External Type-2:** The destination is an external Type-2 route.

**Destination:** Network and prefix (e.g., 10.0.0.0/16) of the given route entry.

**Area:** Indicates which area the route or router can be reached via/to.

**NextHop:** Ipv4 address encoded as "a.b.c.d", where a-d is a base-10 human readable integer in the range 0-255.

**Cost:** The cost of the route.

**AS Cost:** The cost of the route within the OSPF network. It is valid for external Type-2 route and always '0' for other route types.

**Border Router Type:** The border router type of the OSPF route entry.

**i-ABR:** The border router is an ABR.

**i-ASBR:** The border router is an ASBR located on Intra-area.

**I-ASBR:** The border router is an ASBR located on Inter-area.

**i-ABR/ASBR:** The border router is an ASBR attached to at least 2 areas.

**Interface:** The interface where the IP packet is outgoing.

**IsConnected:** The destination is connected directly or not.

### Buttons

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

**Refresh:** Click to refresh the page immediately.

|<< : Updates the table entries, starting from the first available entry. If the first entry of the table is displayed, the button is disabled.

<< : Updates the table entries, ending at the entry prior to the first entry currently displayed. If the first entry of the table is displayed, the button is disabled.

>> : Updates the table entries, starting from the entry next to the last entry currently displayed. If the last entry of the table is displayed, the button is disabled.

>> | : Updates the table entries, ending at the last available entry. If the last entry of the table is displayed, the button is disabled.



## OSPF > Status > General Status

This page displays the OSPF LSA Link State Database table.

The screenshot shows the OSPF Link State Database configuration page. The search filters are: Start from Area ID (0.0.0.0), Link State Type (Network), Link State ID (0.0.0.0), and Advertising Router (0.0.0.0). The table has columns: Area ID, Link State Type, Link State ID, Advertising Router, Age (in seconds), Sequence, Checksum, and Router Link Count. The table currently shows 'No entry exists'.

**Controls:** Click the Refresh button to take effect.

**Start from Area ID:** Enter the start from area IP address in the format 0.0.0.0.

**Link State Type:** At the dropdown select Router, Network, Summary, ASBR Summary, External, or NSSA External.

**Link State ID:** Enter the link state ID in the format 0.0.0.0.

**Advertising Router:** The advertising router ID which originated the LSA.

### **Parameters:**

**Area ID:** Displays the OSPF area ID of the link state advertisement. It is not required for external LSA.

**Link State Type:** Displays the selected link state type (Router, Network, Summary, ASBR Summary, External, or NSSA External).

**Link State ID:** Displays the link state ID in the format 0.0.0.0.

**Advertising Router:** The advertising router ID which originated the LSA.

**Age (in seconds):** The time in seconds since the LSA was originated.

**Sequence:** The LS sequence number of the LSA.

**Checksum:** The checksum of the LSA contents.

**Router Link Count:** The link count of the LSA. The field is significant only when the link state type is 'Router Link State' (Type 1).

### **Buttons**

**Auto-refresh :** Check this box to refresh the page automatically every 3 seconds.

**Refresh:** Click to refresh the page immediately.

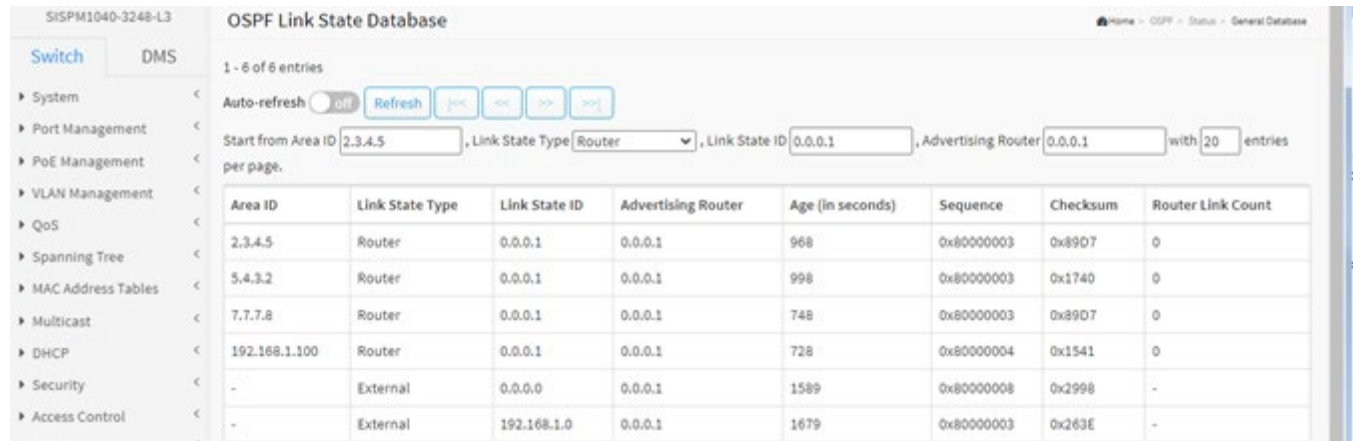
**|<< :** Updates the table entries, starting from the first available entry. If the first entry of the table is displayed, the button is disabled.

**<< :** Updates the table entries, ending at the entry prior to the first entry currently displayed. If the first entry of the table is displayed, the button is disabled.

**>> :** Updates the table entries, starting from the entry next to the last entry currently displayed. If the last entry of the table is displayed, the button is disabled.

>> | : Updates the table entries, ending at the last available entry. If the last entry of the table is displayed, the button is disabled.

### Example:



The screenshot shows the OSPF Link State Database interface. The page title is "OSPF Link State Database" and the breadcrumb is "Home - OSPF - Status - General Database". The interface includes a navigation menu on the left with categories like System, Port Management, PoE Management, VLAN Management, QoS, Spanning Tree, MAC Address Tables, Multicast, DHCP, Security, and Access Control. The main content area shows "1 - 6 of 6 entries" and a search filter with fields for "Start from Area ID" (2.3.4.5), "Link State Type" (Router), "Link State ID" (0.0.0.1), and "Advertising Router" (0.0.0.1), with "20" entries per page. A table displays the following data:

Area ID	Link State Type	Link State ID	Advertising Router	Age (in seconds)	Sequence	Checksum	Router Link Count
2.3.4.5	Router	0.0.0.1	0.0.0.1	968	0x80000003	0x8907	0
5.4.3.2	Router	0.0.0.1	0.0.0.1	998	0x80000003	0x1740	0
7.7.7.8	Router	0.0.0.1	0.0.0.1	748	0x80000003	0x8907	0
192.168.1.100	Router	0.0.0.1	0.0.0.1	728	0x80000004	0x1541	0
-	External	0.0.0.0	0.0.0.1	1589	0x80000008	0x2998	-
-	External	192.168.1.0	0.0.0.1	1679	0x80000003	0x263E	-

## OSPF > Status > Router

This page displays the OSPF LSA Router link state database information table.

The screenshot shows the 'OSPF Router Link State Database' configuration page. At the top, there's a navigation bar with 'Switch' and 'DMS' tabs. A sidebar on the left lists various management options like System, Port Management, PoE Management, etc. The main area contains search filters: 'Start from Area ID' (0.0.0.0), 'Link State Type' (Network), 'Link State ID' (0.0.0.0), and 'Advertising Router' (0.0.0.0). Below the filters is a table with columns: Area ID, Link State Type, Link State ID, Advertising Router, Age (in seconds), Options, Sequence, Checksum, Length, and Router Link Count. The table currently displays 'No entry exists'.

**Controls:** Click the Refresh button to take effect.

**Start from Area ID:** Enter the start from area IP address in the format 0.0.0.0.

**Link State Type:** At the dropdown select Router, Network, Summary, ASBR Summary, External, or NSSA External.

**Link State ID:** Enter the link state ID in the format 0.0.0.0.

**Advertising Router:** The advertising router ID which originated the LSA.

### Parameters:

**Area ID:** The OSPF area ID of the link state advertisement

**Link State Type:** The type of the link state advertisement.

**Link State ID:** The OSPF link state ID. It identifies the piece of the routing domain that is being described by the LSA.

**Advertising Router:** The advertising router ID which originated the LSA.

**Age:** The time in seconds since the LSA was originated.

**Options:** The OSPF option field, present in OSPF hello packets, which enables OSPF routers to support (or not support) optional capabilities, and to communicate their capability level to other OSPF routers.

**Sequence:** The LS sequence number of the LSA.

**Checksum:** The checksum of the LSA contents.

**Length:** The Length in bytes of the LSA.

**Router Link Count:** The link count of the LSA. The field is significant only when the link state type is 'Router Link State' (Type 1).

### Buttons

**Auto-refresh :** Check this box to refresh the page automatically every 3 seconds.

**Refresh:** Click to refresh the page immediately.

**|<< :** Updates the table entries, starting from the first available entry. If the first entry of the table is displayed, the button is disabled.

<< : Updates the table entries, ending at the entry prior to the first entry currently displayed. If the first entry of the table is displayed, the button is disabled.

>> : Updates the table entries, starting from the entry next to the last entry currently displayed. If the last entry of the table is displayed, the button is disabled.

>> | : Updates the table entries, ending at the last available entry. If the last entry of the table is displayed, the button is disabled.

**Example:**

SISPM1040-3248-L3 OSPF Router Link State Database

1 - 4 of 4 entries

Auto-refresh  Refresh << >> >>|

Start from Area ID 2.3.4.5, Link State Type Router, Link State ID 0.0.0.1, Advertising Router 0.0.0.1 with 20 entries per page.

Area ID	Link State Type	Link State ID	Advertising Router	Age (in seconds)	Options	Sequence	Checksum	Length	Router Link Count
2.3.4.5	Router	0.0.0.1	0.0.0.1	1292	0x0	0x80000003	0x89D7	24	0
5.4.3.2	Router	0.0.0.1	0.0.0.1	1322	0x8	0x80000003	0x1740	24	0
7.7.7.8	Router	0.0.0.1	0.0.0.1	1072	0x0	0x80000003	0x89D7	24	0
192.168.1.100	Router	0.0.0.1	0.0.0.1	1052	0x8	0x80000004	0x1541	24	0

## OSPF > Status > Network

This page displays the OSPF LSA Network link state database information table.

The screenshot shows the 'OSPF Network Link State Database' configuration page. The interface includes a navigation menu on the left with options like System, Port Management, PoE Management, VLAN Management, QoS, Spanning Tree, and MAC Address Tables. The main content area has a search filter section with the following fields: 'Start from Area ID' (0.0.0.0), 'Link State Type' (Network), 'Link State ID' (0.0.0.0), and 'Advertising Router' (0.0.0.0). There is also a 'with 20 entries per page' option. Below the search filters is a table with the following columns: Area ID, Link State Type, Link State ID, Advertising Router, Age (in seconds), Options, Sequence, Checksum, Length, and Network Mask. The table currently contains the text 'No entry exists'.

**Controls:** Click the Refresh button to take effect.

**Start from Area ID:** Enter the start from area IP address in the format 0.0.0.0.

**Link State Type:** At the dropdown select Router, Network, Summary, ASBR Summary, External, or NSSA External.

**Link State ID:** Enter the link state ID in the format 0.0.0.0.

**Advertising Router:** The advertising router ID which originated the LSA.

### **Parameters:**

**Area ID:** The OSPF area ID of the link state advertisement

**Link State Type:** The type of the link state advertisement.

**Link State ID:** The OSPF link state ID. It identifies the piece of the routing domain that is being described by the LSA.

**Advertising Router:** The advertising router ID which originated the LSA.

**Age:** The time in seconds since the LSA was originated.

**Options:** The OSPF option field, present in OSPF hello packets, which enables OSPF routers to support (or not support) optional capabilities, and to communicate their capability level to other OSPF routers.

**Sequence:** The LS sequence number of the LSA.

**Checksum:** The checksum of the LSA contents.

**Length:** The Length in bytes of the LSA.

**Network Mask:** Network mask length. The field is significant only when the link state type is 'Network Link State' (Type 2).

### **Buttons**

**Auto-refresh :** Check this box to refresh the page automatically every 3 seconds.

**Refresh:** Click to refresh the page immediately.

**|<< :** Updates the table entries, starting from the first available entry. If the first entry of the table is displayed, the button is disabled.

<< : Updates the table entries, ending at the entry prior to the first entry currently displayed. If the first entry of the table is displayed, the button is disabled.

>> : Updates the table entries, starting from the entry next to the last entry currently displayed. If the last entry of the table is displayed, the button is disabled.

>> | : Updates the table entries, ending at the last available entry. If the last entry of the table is displayed, the button is disabled.

## OSPF > Status > Summary

This page displays the OSPF LSA Summary link state database information table.

The screenshot shows the 'OSPF Summary Link State Database' page. It features a search interface with the following fields: 'Start from Area ID' (0.0.0.0), 'Link State Type' (Network), 'Link State ID' (0.0.0.0), and 'Advertising Router' (0.0.0.0). There are also 'Refresh', '<<', '>>', and '<<>>' buttons. The table below has the following columns: Area ID, Link State Type, Link State ID, Advertising Router, Age (in seconds), Options, Sequence, Checksum, Length, Network Mask, and Metric. The table content is 'No entry exists'.

**Controls:** Click the Refresh button to take effect.

**Start from Area ID:** Enter the start from area IP address in the format 0.0.0.0.

**Link State Type:** At the dropdown select Router, Network, Summary, ASBR Summary, External, or NSSA External.

**Link State ID:** Enter the link state ID in the format 0.0.0.0.

**Advertising Router:** The advertising router ID which originated the LSA.

### Parameters:

**Area ID:** The OSPF area ID of the link state advertisement

**Link State Type:** The type of the link state advertisement.

**Link State ID:** The OSPF link state ID. It identifies the piece of the routing domain that is being described by the LSA.

**Advertising Router:** The advertising router ID which originated the LSA.

**Age:** The time in seconds since the LSA was originated.

**Options:** The OSPF option field, present in OSPF hello packets, which enables OSPF routers to support (or not support) optional capabilities, and to communicate their capability level to other OSPF routers.

**Sequence:** The LS sequence number of the LSA.

**Checksum:** The checksum of the LSA contents.

**Length:** The Length in bytes of the LSA.

**Network Mask:** Network mask length. The field is significant only when the link state type is 'Summary/ASBR Summary Link State' (Type 3, 4).

**Metric:** User specified metric for this summary route. The field is significant only when the link state type is 'Summary/ASBR Summary Link State' (Type 3, 4).

### Buttons

**Auto-refresh :** Check this box to refresh the page automatically every 3 seconds.

**Refresh:** Click to refresh the page immediately.

|<< : Updates the table entries, starting from the first available entry. If the first entry of the table is displayed, the button is disabled.

<< : Updates the table entries, ending at the entry prior to the first entry currently displayed. If the first entry of the table is displayed, the button is disabled.

>> : Updates the table entries, starting from the entry next to the last entry currently displayed. If the last entry of the table is displayed, the button is disabled.

>> | : Updates the table entries, ending at the last available entry. If the last entry of the table is displayed, the button is disabled.



## OSPF > Status > ASBR Summary

This page displays the OSPF LSA ASBR Summary link state database information table.

The screenshot shows the Lantronix web interface for the device SISPM1040-3166-L3. The main content area is titled "OSPF ASBR Summary Link State Database". It features a search filter section with the following fields: "Start from Area ID" (0.0.0.0), "Link State Type" (Network), "Link State ID" (0.0.0.0), and "Advertising Router" (0.0.0.0). There is also a "with 20 entries per page" option. Below the search filters is a table with the following columns: Area ID, Link State Type, Link State ID, Advertising Router, Age (in seconds), Options, Sequence, Checksum, Length, Network Mask, and Metric. The table currently displays "No entry exists".

**Controls:** Click the Refresh button to take effect.

**Start from Area ID:** Enter the start from area IP address in the format 0.0.0.0.

**Link State Type:** At the dropdown select Router, Network, Summary, ASBR Summary, External, or NSSA External.

**Link State ID:** Enter the link state ID in the format 0.0.0.0.

**Advertising Router:** The advertising router ID which originated the LSA.

### **Parameters:**

**Area ID:** The OSPF area ID of the link state advertisement

**Link State Type:** The type of the link state advertisement.

**Link State ID:** The OSPF link state ID. It identifies the piece of the routing domain that is being described by the LSA.

**Advertising Router:** The advertising router ID which originated the LSA.

**Age:** The time in seconds since the LSA was originated.

**Options:** The OSPF option field, present in OSPF hello packets, which enables OSPF routers to support (or not support) optional capabilities, and to communicate their capability level to other OSPF routers.

**Sequence:** The LS sequence number of the LSA.

**Checksum:** The checksum of the LSA contents.

**Length:** The Length in bytes of the LSA.

**Network Mask:** Network mask length. The field is significant only when the link state type is 'Summary/ASBR Summary Link State' (Type 3, 4).

**Metric:** User specified metric for this summary route. The field is significant only when the link state type is 'Summary/ASBR Summary Link State' (Type 3, 4).

### **Buttons**

**Auto-refresh :** Check this box to refresh the page automatically every 3 seconds.

**Refresh:** Click to refresh the page immediately.

|<< : Updates the table entries, starting from the first available entry. If the first entry of the table is displayed, the button is disabled.

<< : Updates the table entries, ending at the entry prior to the first entry currently displayed. If the first entry of the table is displayed, the button is disabled.

>> : Updates the table entries, starting from the entry next to the last entry currently displayed. If the last entry of the table is displayed, the button is disabled.

>> | : Updates the table entries, ending at the last available entry. If the last entry of the table is displayed, the button is disabled.

## OSPF > Status > External

This page displays the OSPF LSA External link state database information table.

The screenshot shows the 'OSPF External Link State Database' configuration page. At the top, there is a navigation bar with 'LANTRONIX' and a menu icon. Below it, the device name 'SISPM1040-3166-L3' is displayed. The page has a left-hand navigation menu with options like 'Switch', 'DMS', 'System', 'Port Management', 'PoE Management', 'VLAN Management', 'QoS', 'Spanning Tree', and 'MAC Address Tables'. The main content area is titled 'OSPF External Link State Database' and includes a breadcrumb trail 'Home > OSPF > Status > External'. Below the title, it shows '0 - 0 of 0 entry'. There is an 'Auto-refresh' toggle set to 'off' and a 'Refresh' button. Search filters include 'Start from Link State Type' (set to 'Network'), 'Link State ID' (0.0.0.0), 'Advertising Router' (0.0.0.0), and 'with 20 entries per page'. A table with 12 columns is shown, but it contains the text 'No entry exists'.

**Controls:** Click the Refresh button to take effect.

**Start from Link State Type:** At the dropdown select Router, Network, Summary, ASBR Summary, External, or NSSA External.

**Link State ID:** Enter the link state ID in the format 0.0.0.0.

**Advertising Router:** The advertising router ID which originated the LSA.

### **Parameters:**

**Link State Type:** The type of the link state advertisement.

**Link State ID:** The OSPF link state ID. It identifies the piece of the routing domain that is described by the LSA.

**Advertising Router:** The advertising router ID which originated the LSA.

**Age:** The time in seconds since the LSA was originated.

**Options:** The OSPF option field, present in OSPF hello packets, which enables OSPF routers to support (or not support) optional capabilities, and to communicate their capability level to other OSPF routers.

**Sequence:** The LS sequence number of the LSA.

**Checksum:** The checksum of the LSA contents.

**Length:** The Length in bytes of the LSA.

**Network Mask:** Network mask length. The field is significant only when the link state type is 'External/NSSA External Link State' (Type 5, 7).

**Metric Type:** The External type of the LSA. The field is significant only when the link state type is 'External/NSSA External Link State' (Type 5, 7).

**Metric:** User specified metric for this summary route. The field is significant only when the link state type is 'External/NSSA External Link State' (Type 5, 7).

**Forward Address:** The IP address of forward address. The field is significant only when the link state type is 'External/NSSA External Link State' (Type 5, 7).

**Buttons**

**Auto-refresh** : Check this box to refresh the page automatically every 3 seconds.

**Refresh**: Click to refresh the page immediately.

|<< : Updates the table entries, starting from the first available entry. If the first entry of the table is displayed, the button is disabled.

<< : Updates the table entries, ending at the entry prior to the first entry currently displayed. If the first entry of the table is displayed, the button is disabled.

>> : Updates the table entries, starting from the entry next to the last entry currently displayed. If the last entry of the table is displayed, the button is disabled.

>> | : Updates the table entries, ending at the last available entry. If the last entry of the table is displayed, the button is disabled.

## OSPF > Status > NSSA External

This page displays the OSPF LSA NSSA External link state database information table.

The screenshot shows the 'OSPF NSSA External Link State Database' configuration page. The interface includes a navigation menu on the left with options like System, Port Management, PoE Management, VLAN Management, QoS, Spanning Tree, and MAC Address Tables. The main content area has a search section with the following parameters: Start from Link State Type (Network), Link State ID (0.0.0.0), Advertising Router (0.0.0.0), and 20 entries per page. Below the search section is a table with the following columns: Link State Type, Link State ID, Advertising Router, Age (in seconds), Options, Sequence, Checksum, Length, Network Mask, Metric Type, Metric, and Forward Address. The table currently displays 'No entry exists'.

**Controls:** Click the Refresh button to take effect.

**Start from Link State Type:** At the dropdown select Router, Network, Summary, ASBR Summary, External, or NSSA External.

**Link State ID:** Enter the link state ID in the format 0.0.0.0.

**Advertising Router:** The advertising router ID which originated the LSA.

### Parameters:

**Link State Type:** The type of the link state advertisement.

**Link State ID:** The OSPF link state ID. It identifies the piece of the routing domain that is being described by the LSA.

**Advertising Router:** The advertising router ID which originated the LSA.

**Age:** The time in seconds since the LSA was originated.

**Options:** The OSPF option field, present in OSPF hello packets, which enables OSPF routers to support (or not support) optional capabilities, and to communicate their capability level to other OSPF routers.

**Sequence:** The LS sequence number of the LSA.

**Checksum:** The checksum of the LSA contents.

**Length:** The Length in bytes of the LSA.

**Network Mask:** Network mask length. The field is significant only when the link state type is 'External/NSSA External Link State' (Type 5, 7).

**Metric Type:** The External type of the LSA. The field is significant only when the link state type is 'External/NSSA External Link State' (Type 5, 7).

**Metric:** User specified metric for this summary route. The field is significant only when the link state type is 'External/NSSA External Link State' (Type 5, 7).

**Forward Address:** The IP address of forward address. The field is significant only when the link state type is 'External/NSSA External Link State' (Type 5, 7).

**Buttons**

**Auto-refresh** : Check this box to refresh the page automatically every 3 seconds.

**Refresh**: Click to refresh the page immediately.

|<< : Updates the table entries, starting from the first available entry. If the first entry of the table is displayed, the button is disabled.

<< : Updates the table entries, ending at the entry prior to the first entry currently displayed. If the first entry of the table is displayed, the button is disabled.

>> : Updates the table entries, starting from the entry next to the last entry currently displayed. If the last entry of the table is displayed, the button is disabled.

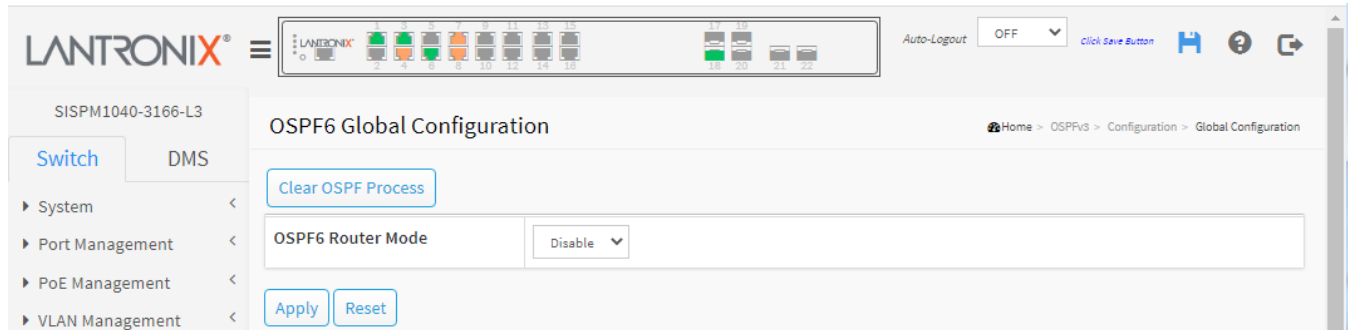
>> | : Updates the table entries, ending at the last available entry. If the last entry of the table is displayed, the button is disabled.

## OSPFv3

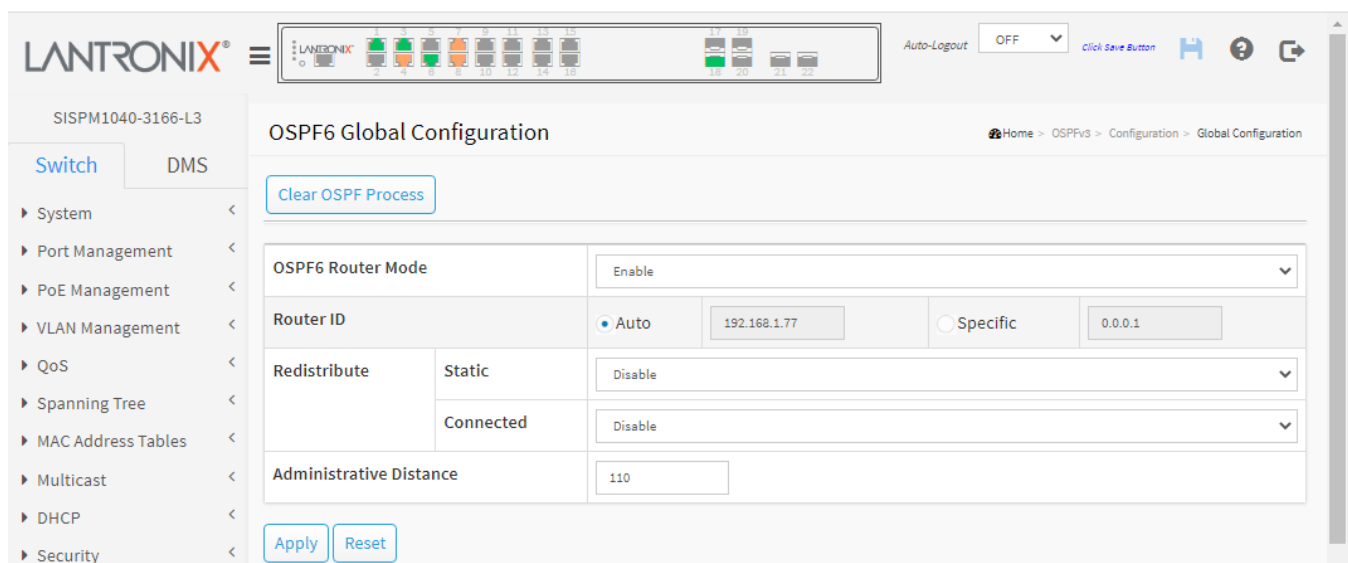
OSPF works with IPv4, and OSPFv3 works with IPv6.

### OSPFv3 > Configuration > Global Configuration

From the default OSPF6 Global Configuration page, select Enable at the dropdown, then click the Apply button.



The OSPF6 Global Configuration table displays. Here you can set OSPF6 router configuration parameters. It is a general group to configure the OSPF6 common router parameters.



**OSPF6 Router Mode:** Enable or Disable the OSPF6 router mode.

**Router ID:** The OSPF6 Router ID in IPv4 address format (A.B.C.D). When the router's OSPF6 Router ID is changed, if there is one or more fully adjacent neighbors in current OSPF6 area, the new router ID will take effect after restart OSPF6 process. Note that the router ID should be unique in the Autonomous System and value '0.0.0.0' is invalid since it is reserved for the default algorithm.

**Auto:** The default algorithm will choose the largest IP address assigned to the router.

**Specific:** User specified router ID. The allowed range is 0.0.0.1 - 255.255.255.254.

**Static Redistribute:** Set the OSPF redistribute to enabled or disabled for the static routes.

**Enable:** The static routes are redistributed.

**Disable:** The static routes are not redistributed

**Connected Redistribute:** Set the OSPF redistribute to enabled or disabled for connected route.

**Enable:** The connected interfaces are redistributed.

**Disable:** The connected interfaces are not redistributed.

**Administrative Distance:** The OSPF6 administrative distance. Administrative Distance must be an integer value of 1 - 255

## Buttons

**Clear OSPF Process:** Click to reset the current OSPF6 process.

**Apply:** Click to save changes.

**Reset:** Click to undo any changes made locally and revert to previously saved values.

## Example:

The screenshot shows the OSPF6 Global Configuration page in a web browser. The page title is "OSPF6 Global Configuration" and the breadcrumb is "Home > OSPFv3 > Configuration > Global Configuration". The page is for device "SISPM1040-3248-L3". On the left, there is a navigation menu with "Switch" selected and "DMS" as a sub-tab. The main content area has a "Clear OSPF Process" button at the top. Below it, the configuration is as follows:

OSPF6 Router Mode		Enable
Router ID		<input type="radio"/> Auto <input type="text" value="0.0.0.1"/> <input checked="" type="radio"/> Specific <input type="text" value="0.0.0.1"/>
Redistribute	Static	Enable
	Connected	Enable
Administrative Distance		99

At the bottom of the configuration area, there are "Apply" and "Reset" buttons.



## OSPFv3 > Configuration > Passive Interface

This page displays the OSPF6 router passive interface configuration table.

Interface	Area ID
*	
VLAN 1	0.0.0.0

**Interface:** Interface identification. At the dropdown select Enable.

**Area ID:** The OSPF6 interface Area ID. Only valid if Router ID is set to Specific.

### Buttons

**Apply:** Click to save changes.

**Reset:** Click to undo any changes made locally and revert to previously saved values.

## OSPFv3 > Configuration > Stub Area

This page displays the OSPF6 stub area configuration table. The configuration is used to reduce the link-state database size and thus the memory and CPU requirement by forbidding some LSAs.

The screenshot shows the LANTRONIX web interface for the SISPM1040-3166-L3 device. The main content area is titled "OSPF6 Area Stub Configuration". It features a table with the following data:

Delete	Area ID	No Summary
<input type="checkbox"/>	*	<input type="checkbox"/>
<input type="checkbox"/>	1.2.3.4	<input type="checkbox"/>
<input type="checkbox"/>	2.4.44.4	<input checked="" type="checkbox"/>

Below the table are three buttons: "Add New Entry", "Apply", and "Reset". The left sidebar shows a navigation menu with "Switch" selected and "DMS" as a sub-option. The top right corner includes an "Auto-Logout" dropdown set to "OFF" and a "Click Save Button" link.

**Delete:** Check to delete the entry. It will be deleted during the next save.

**Area ID:** The OSPF6 area ID.

**No Summary:** The value is true (checkbox checked) to configure the inter-area routes to not inject into this stub area.

### Buttons

**Add New Entry:** Click to add new entry.

**Apply:** Click to save changes.

**Reset:** Click to undo any changes made locally and revert to previously saved values.

### Messages:

*JSON RPC Error. (Backbone can not be configured as stub area)*

*The new entry {0.0.0.0} is duplicated.*

## OSPFv3 > Configuration > Area Range

This page displays the OSPF6 area range configuration table. It is used to summarize the intra area paths from a specific address range in one summary-LSA (Type-0x2003) and advertised to other areas or configure the address range status as 'DoNotAdvertise' which the summary-LSA (Type-0x2003) is suppressed.

The area range configuration is used for Area Border Routers (ABRs) and only router-LSAs (Type-0x2001) and network-LSAs (Type-0x2002) can be summarized.

The AS-external-LSAs (Type-0x4005) cannot be summarized because the scope is OSPF6 autonomous system (AS).

The AS-external-LSAs (Type-0x4007) cannot be summarized because the feature is not supported yet.

Delete	Area ID	Network Address	Mask Length	Advertise	Cost
<input type="checkbox"/>	0.0.0.0	0::0	128	<input checked="" type="checkbox"/>	Auto

**Delete:** Check to delete the entry. It will be deleted during the next save.

**Area ID:** The OSPF6 area ID.

**Network Address:** IPv6 network address.

**Mask Length:** IPv6 network mask length.

**Advertise:** When the value is true, it summarizes intra area paths from the address range in one Inter-Area Prefix LSA (Type-0x2003) and advertised to other areas. Otherwise, the intra area paths from the address range are not advertised to other areas.

**Cost:** Cost (or metric) for this summary route. It can only be configured when 'Specific' is selected.

**Auto:** Sets the cost value is set to 0 automatically and isn't allowed to be configured (default).

**Specific:** Lets you manually set the cost (or metric). The allowed range is 0 – 16777215.

### Buttons

**Add New Entry:** Click to add a new entry to the table.

**Apply:** Click to save changes.

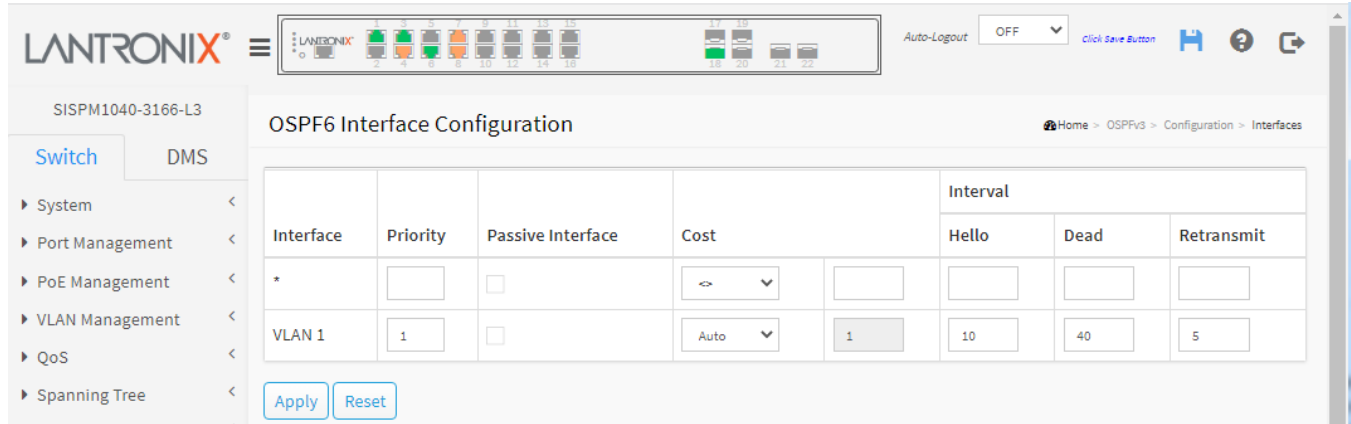
**Reset:** Click to undo any changes made locally and revert to previously saved values.

### Messages:

The input value Network address (0::0) is not a valid IPv6 address.

## OSPFv3 > Configuration > Interfaces

This page displays the OSPF6 interface configuration table.



**Interface:** Interface identification.

**Priority:** User specified router priority for the interface. The allowed range is 0- 255 and the default value is 1.

**Passive Interface:** Indicates whether the interface is passive or not

**Cost:** User specified cost for this interface. It's link state metric for the interface. The field is significant only when 'IsSpecificCost' is TRUE. The allowed range is 1- 65535 and the default setting is 'Auto' cost mode.

**Hello Interval:** How many Hello packets will be sent per second. The allowed range is 1- 65535 seconds and the default value is 10 seconds.

**Dead Interval:** The time interval (in seconds) between hello packets. The allowed range is 1-65535 seconds and the default value is 40 seconds.

**Retransmit Interval:** The time interval (in seconds) between link-state advertisement (LSA) retransmissions for adjacencies. The allowed range is 3- 65535 seconds and the default value is 5 seconds.

### Buttons

**Apply:** Click to save changes.

**Reset:** Click to undo any changes made locally and revert to previously saved values.

## OSPFv3 > Status > Global Status

This page displays the OSPF6 global status table. It provides OSPF6 router status information.

The screenshot shows the Lantronix web interface for device SISPM1040-3166-L3. The main content area is titled "OSPF6 Global Status" and includes an "Auto-refresh" toggle set to "off", a "Refresh" button, and a "Clear OSPF Process" button. Below this is a "Status Information" table.

Status Information	
Router ID	0.0.0.1
SPF Delay	200 msecs
SPF Hold Time	400 msecs
SPF Max. Wait Time	10000 msecs
Last Executed SPF Time Stamp	135782 msecs
Attached Area Count	2

**Router ID:** OSPF6 router ID.

**SPF Delay:** Delay time (in seconds) of SPF calculations.

**SPF Hold Time:** Minimum hold time (in milliseconds) between consecutive SPF calculations.

**SPF Max. Wait Time:** Maximum wait time (in milliseconds) between consecutive SPF calculations.

**Last Executed SPF Time Stamp:** Time (in milliseconds) that has passed between the start of the SPF algorithm execution and the current time.

**Attached Area Count:** Number of areas attached for the router.

### Buttons

**Auto-refresh:** Check this box to refresh the page automatically every 3 seconds.

**Refresh:** Click to refresh the page immediately.

**Clear OSPF Process:** Click to reset the current OSPF6 process.

## OSPFv3 > Status > Area Status

This page displays the OSPF6 network area status table.

OSPF6 Area Status

Auto-refresh  off [Refresh](#)

Area ID	Backbone	Area Type	Active Interfaces	SPF Executed Times	LSA count
1.2.3.4	No	Stub	1	2	1
2.4.44.4	No	Totally Stub	0	1	1

**Area ID:** The Area ID.

**Backbone:** Displays 'Yes' if it's backbone area or 'No' if it is not.

**Area Type:** The area type (e.g., Normal, Stub, or Totally Stub).

**Active Interfaces:** Number of active interfaces attached in the area.

**SPF Executed Times:** Number of times SPF algorithm has been executed for the particular area.

**LSA count:** Number of the total LSAs for the particular area.

### Buttons

**Auto-refresh:** Check this box to refresh the page automatically every 3 seconds.

**Refresh:** Click to refresh the page immediately.

### Example:

OSPF6 Area Status

Auto-refresh  off [Refresh](#)

Area ID	Backbone	Area Type	Active Interfaces	SPF Executed Times	LSA count
0.0.0.0	Yes	Normal	0	6	1
1.2.3.4	No	Totally Stub	0	3	2
2.3.4.6	No	Normal	0	4	1
3.4.5.6	No	Normal	1	5	1
192.168.1.77	No	Stub	0	1	2

## OSPFv3 > Status > Neighbor Status

This page displays the OSPF6 IPv6 neighbor status table.

The screenshot shows the Lantronix web interface for device SISPM1040-3166-L3. The main content area is titled 'OSPF6 Neighbor Status'. It includes an 'Auto-refresh' toggle set to 'off' and a 'Refresh' button. Below this is a table with the following columns: Neighbor ID, Priority, State, Dead Time, Interface Address, and Interface. The table currently displays 'No entry exists'.

Neighbor ID	Priority	State	Dead Time	Interface Address	Interface
No entry exists					

**Neighbor ID:** The Neighbor ID.

**Priority:** The priority of OSPF6 neighbor. It indicates the priority of the neighbor router. This item is used when selecting the DR for the network. The router with the highest priority becomes the DR.

**State:** The state of OSPF6 neighbor. It indicates the functional state of the neighbor router.

**Dead Time:** The Dead timer indicates the amount of time remaining that the router waits to receive an OSPF6 hello packet from the neighbor before declaring the neighbor down.

**Interface Address:** The IP address.

**Interface:** The network interface.

### Buttons

**Auto-refresh:** Check this box to refresh the page automatically every 3 seconds.

**Refresh:** Click to refresh the page immediately.

## OSPFv3 > Status > Interface Status

This page displays the OSPF6 interface status table.

The screenshot shows the Lantronix web interface for device SISPM1040-3166-L3. The page title is 'OSPF6 Interface Status'. There is an 'Auto-refresh' toggle set to 'off' and a 'Refresh' button. Below this is a 'Status Information' section containing a table with the following data:

Interface	Interface Address	Area ID	Router ID	State	DR ID	BDR ID	Pri	Cost	Interval Configuration(sec)			Passive	Transmit Delay
									Hello	Dead	Retransmit		
VLAN 1	fe80::2c0:f2ff:fe7c:597f/64	1.2.3.4	0.0.0.1	DR	0.0.0.1	0.0.0.0	1	10	10	40	5	false	1 sec

**Interface:** Interface identification (e.g., VLAN 1).

**Interface Address:** IPv6 network address.

**Area ID:** The OSPF6 area ID in the format 1.2.3.4.

**Router ID:** The OSPF6 router ID in the format 0.0.0.1

**State:** The state of the link (e.g., DR).

**DR ID:** The router ID of DR.

**BDR ID:** The router ID of BDR.

**Pri:** The OSPF6 priority. It helps determine the DR and BDR on the network to which this interface is connected.

**Cost:** The cost of the interface.

**Hello:** Hello timer. A time interval that a router sends an OSPF6 hello packet.

**Dead:** Dead timer. Dead timer is a time interval to wait before declaring a neighbor dead. The unit of time is seconds.

**Retransmit:** Retransmit timer. A time interval to wait before retransmitting a database description packet when it has not been acknowledged.

**Passive:** Displays 'true' if the interface is a passive interface or 'false' if it not.

**Transmit Delay:** The estimated time in seconds to transmit a link-state update packet on the interface.

### Buttons

**Auto-refresh:** Check this box to refresh the page automatically every 3 seconds.

**Refresh:** Click to refresh the page immediately.



## OSPFv3 > Status > Routing Status

This page displays the OSPF6 routing status table.

### Controls:

**Start from Route Type:** At the dropdown select Inter Area, Intra Area, Border Router, External Type-1, or External Type-2.

**Destination:** Enter the destination IP.

**Area:** Enter the Area IP.

**NextHop:** Enter the Next Hop IP

**Codes:** **i** - Intra-area Router Path, **I** - Inter-area Router Path

### Parameters:

**Route Type:** The OSPF6 route type:

**Intra Area:** The destination is an OSPF6 route which is located on intra-area.

**Inter Area:** The destination is an OSPF6 route which is located on inter-area.

**Border Router:** The destination is a border router.

**External Type-1:** The destination is an external Type-1 route.

**External Type-2:** The destination is an external Type-2 route.

**Destination:** Network and prefix (example 10.0.0.0/16) of the given route entry.

**Area:** It indicates which area the route or router can be reached via/to.

**NextHop:** An Ipv6 address represented as human readable text as specified in IETF [RFC 5952](#).

**Cost:** The cost of the route.

**AS Cost:** The cost of the route within the OSPF6 network. It is valid for external Type-2 route and always '0' for other route types.

**Border Router Type:** The border router type of the OSPF6 route entry.

**i-ABR:** The border router is an ABR.

**i-ASBR:** The border router is an ASBR located on Intra-area.

**I-ASBR:** The border router is an ASBR located on Inter-area.

**i-ABR/ASBR:** The border router is an ASBR attached to at least two areas.

**Interface:** The interface where the IP packet is outgoing.

**IsConnected:** The destination is connected directly or not.

**Buttons**

**Auto-refresh :** Check this box to refresh the page automatically every 3 seconds.

**Refresh:** Click to refresh the page immediately.

**|<< :** Updates the table entries, starting from the first available entry. If the first entry of the table is displayed, the button is disabled.

**<< :** Updates the table entries, ending at the entry prior to the first entry currently displayed. If the first entry of the table is displayed, the button is disabled.

**>> :** Updates the table entries, starting from the entry next to the last entry currently displayed. If the last entry of the table is displayed, the button is disabled.

**>> | :** Updates the table entries, ending at the last available entry. If the last entry of the table is displayed, the button is disabled.

**Example:**

The screenshot shows the OSPF6 Routing Status page. On the left is a navigation menu with 'Switch' selected and 'DMS' as a sub-option. The main content area includes an 'Auto-refresh' toggle set to 'off', a 'Refresh' button, and navigation buttons: '|<<', '<<', '>>', and '>>|'. Below these are search filters: 'Start from Route Type' (Intra Area), 'Destination' (1::/21), and 'Area' (1.2.34.4). A 'NextHop' field contains '::' and a note says 'with 20 entries per page.' Codes are listed as 'I - Intra-area Router Path, I - Inter-area Router Path'. A table displays the following data:

Route Type	Destination	Area	NextHop	Cost	AS Cost	Border Router Type	Interface	IsConnected
Intra Area	1::/21	1.2.34.4	::	10	-	-	VLAN 1	Connected

## OSPFv3 > Database > General Database

This page displays the OSPF6 LSA link state database information table.

Set the Start from Area ID, Link State Type, Link State ID, Advertising Router, and entries per page controls.

The screenshot shows the 'OSPF6 Link State Database' configuration page. The interface includes a navigation menu on the left with options like System, Port Management, PoE Management, VLAN Management, QoS, Spanning Tree, MAC Address Tables, and Multicast. The main content area features a search filter section with an 'Auto-refresh' toggle (set to 'off'), a 'Refresh' button, and navigation buttons (|<<, <<, >>, >>|). Below the search filters, there are input fields for 'Start from Area ID' (1.2.3.4), 'Link State Type' (Router), 'Link State ID' (0.0.0.4), and 'Advertising Router' (0.0.0.1), along with a 'with 20 entries per page' control. A table displays the following data:

Area ID	Link State Type	Link State ID	Advertising Router	Age (in seconds)	Sequence
1.2.3.4	Link	0.0.0.4	0.0.0.1	543	0x80000001
1.2.3.4	Router	0.0.0.0	0.0.0.1	475	0x80000002
2.4.44.4	Router	0.0.0.0	0.0.0.1	475	0x80000001

### Controls:

**Start from Area ID:** Enter the Area ID in the format 0.0.0.0.

**Link State Type:** At the dropdown select Router, Network, Summary, ASBR Summary, External, or NSSA External.

**Link State ID:** Enter the Link State ID in the format 0.0.0.0.

**Advertising Router:** Enter the Advertising Router IP in the format 0.0.0.0.

### Parameters:

**Area ID:** The OSPF6 area ID of the link state advertisement. It is not required for external LSA.

**Link State Type:** The type of the link state advertisement (e.g., Router, Link, or InterAreaPrefix).

**Link State ID:** The OSPF6 link state ID. It identifies the piece of the routing domain that is being described by the LSA.

**Advertising Router:** The advertising router ID which originated the LSA.

**Age (in seconds):** The time in seconds since the LSA was originated.

**Sequence:** The LS sequence number of the LSA.

### Buttons

**Auto-refresh :** Check this box to refresh the page automatically every 3 seconds.

**Refresh:** Click to refresh the page immediately.

|<< : Updates the table entries, starting from the first available entry. If the first entry of the table is displayed, the button is disabled.

<< : Updates the table entries, ending at the entry prior to the first entry currently displayed. If the first entry of the table is displayed, the button is disabled.

>> : Updates the table entries, starting from the entry next to the last entry currently displayed. If the last entry of the table is displayed, the button is disabled.

>> | : Updates the table entries, ending at the last available entry. If the last entry of the table is displayed, the button is disabled.

**Example:**

The screenshot shows the OSPF6 Link State Database interface. It includes a navigation menu on the left, a header with the device name 'SISPM1040-3248-L3' and the title 'OSPF6 Link State Database'. Below the header, there are controls for 'Auto-refresh' (set to 'off'), a 'Refresh' button, and navigation buttons '<<<', '<<', '>>', and '>>>'. The search criteria are: 'Start from Area ID' 0.0.0.0, 'Link State Type' Router, 'Link State ID' 0.0.0.0, and 'Advertising Router' 192.168.1.77, with '20' entries per page.

Area ID	Link State Type	Link State ID	Advertising Router	Age (in seconds)	Sequence
0.0.0.0	Router	0.0.0.0	192.168.1.77	937	0x80000002
1.2.3.4	Router	0.0.0.0	192.168.1.77	703	0x80000002
1.2.3.4	InterAreaPrefix	0.0.0.1	192.168.1.77	702	0x80000002
2.3.4.6	Router	0.0.0.0	192.168.1.77	640	0x80000003
3.4.5.6	Link	0.0.0.4	192.168.1.77	937	0x80000002
3.4.5.6	Router	0.0.0.0	192.168.1.77	928	0x80000002
192.168.1.77	Router	0.0.0.0	192.168.1.77	626	0x80000002
192.168.1.77	InterAreaPrefix	0.0.0.1	192.168.1.77	625	0x80000002

## OSPFv3 > Detail Database > Router

This page displays the OSPF6 LSA Router link state database information table. Set the Start from Area ID, Link State Type, Link State ID, Advertising Router, and entries per page controls.

The screenshot shows the 'OSPF6 Router Link State Database' page. The search filters are set to: Start from Area ID: 1.2.3.4, Link State Type: Router, Link State ID: 0.0.0.0, Advertising Router: 0.0.0.1, with 20 entries per page. The table below shows two entries:

Area ID	Link State Type	Link State ID	Advertising Router	Age (in seconds)	Options	Sequence	Checksum	Length	Router Link Count
1.2.3.4	Router	0.0.0.0	0.0.0.1	560	0x17	0x80000002	0x1A18	24	0
2.4.44.4	Router	0.0.0.0	0.0.0.1	560	0x17	0x80000001	0x1F13	24	0

### Controls:

**Start from Area ID:** Enter the Area ID in the format 0.0.0.0.

**Link State Type:** At the dropdown select Router, Network, Summary, ASBR Summary, External, or NSSA External.

**Link State ID:** Enter the Link State ID in the format 0.0.0.0.

**Advertising Router:** Enter the Advertising Router IP in the format 0.0.0.0.

### Parameters:

**Area ID:** The OSPF6 area ID of the link state advertisement

**Link State Type:** The type of the link state advertisement.

**Link State ID:** The OSPF6 link state ID. It identifies the piece of the routing domain being described by the LSA.

**Advertising Router:** The advertising router ID which originated the LSA.

**Age:** The time in seconds since the LSA was originated.

**Options:** The OSPF6 option field, present in OSPF6 hello packets, which enables OSPF6 routers to support (or not support) optional capabilities, and to communicate their capability level to other OSPF6 routers.

**Sequence:** The LS sequence number of the LSA.

**Checksum:** The checksum of the LSA contents.

**Length:** The Length in bytes of the LSA.

**Router Link Count:** The link count of the LSA. This field is significant only when the link state type is 'Router Link State' (Type 1).

### Buttons

**Auto-refresh :** Check this box to refresh the page automatically every 3 seconds.

**Refresh:** Click to refresh the page immediately.

- |<< : Updates the table entries, starting from the first available entry. If the first entry of the table is displayed, the button is disabled.
- << : Updates the table entries, ending at the entry prior to the first entry currently displayed. If the first entry of the table is displayed, the button is disabled.
- >> : Updates the table entries, starting from the entry next to the last entry currently displayed. If the last entry of the table is displayed, the button is disabled.
- >>| : Updates the table entries, ending at the last available entry. If the last entry of the table is displayed, the button is disabled.

**Example:**

The screenshot displays the OSPF6 Router Link State Database. The table below shows the current data:

Area ID	Link State Type	Link State ID	Advertising Router	Age (in seconds)	Options	Sequence	Checksum	Length	Router Link Count
0.0.0.0	Router	0.0.0.0	192.168.1.77	303	0x19	0x80000003	0x4731	24	0
1.2.3.4	Router	0.0.0.0	192.168.1.77	69	0x17	0x80000003	0x3E3B	24	0
2.3.4.6	Router	0.0.0.0	192.168.1.77	6	0x19	0x80000004	0x482E	24	0
3.4.5.6	Router	0.0.0.0	192.168.1.77	294	0x19	0x80000003	0x4731	24	0
192.168.1.77	Router	0.0.0.0	192.168.1.77	1792	0x17	0x80000002	0x403A	24	0

## OSPFv3 > Detail Database > Network

This page displays the OSPF6 LSA Network link state database information table. Set the Start from Area ID, Link State Type, Link State ID, Advertising Router, and entries per page controls.

The screenshot shows the 'OSPF6 Network Link State Database' page. The search criteria are: Start from Area ID: 0.0.0.0, Link State Type: Network, Link State ID: 0.0.0.0, Advertising Router: 0.0.0.0, with 20 entries per page. The table below shows the results:

Area ID	Link State Type	Link State ID	Advertising Router	Age (in seconds)	Options	Sequence	Checksum	Length
No entry exists								

### Controls:

**Start from Area ID:** Enter the Area ID in the format 0.0.0.0.

**Link State Type:** At the dropdown select Router, Network, Summary, ASBR Summary, External, or NSSA External.

**Link State ID:** Enter the Link State ID in the format 0.0.0.0.

**Advertising Router:** Enter the Advertising Router IP in the format 0.0.0.0.

### Parameters:

**Area ID:** The OSPF6 area ID of the link state advertisement

**Link State Type:** The type of the link state advertisement.

**Link State ID:** The OSPF6 link state ID. It identifies the piece of the routing domain that is being described by the LSA.

**Advertising Router:** The advertising router ID which originated the LSA.

**Age:** The time in seconds since the LSA was originated.

**Options:** The OSPF6 option field, present in OSPF6 hello packets, which enables OSPF6 routers to support (or not support) optional capabilities, and to communicate their capability level to other OSPF6 routers.

**Sequence:** The LS sequence number of the LSA.

**Checksum:** The checksum of the LSA contents.

**Length:** The Length in bytes of the LSA.

### Buttons

**Auto-refresh:** Check this box to refresh the page automatically every 3 seconds.

**Refresh:** Click to refresh the page immediately.

**<<< :** Updates the table entries, starting from the first available entry. If the first entry of the table is displayed, the button is disabled.

<< : Updates the table entries, ending at the entry prior to the first entry currently displayed. If the first entry of the table is displayed, the button is disabled.

>> : Updates the table entries, starting from the entry next to the last entry currently displayed. If the last entry of the table is displayed, the button is disabled.

>> | : Updates the table entries, ending at the last available entry. If the last entry of the table is displayed, the button is disabled.



## OSPFv3 > Detail Database > Link

This page displays the OSPF6 LSA Link link-state database table. Set the Start from Area ID, Link State Type, Link State ID, Advertising Router, and entries per page controls.

The screenshot shows the OSPF6 Link Link State Database page. The table displays the following entry:

Area ID	Link State Type	Link State ID	Advertising Router	Age (in seconds)	Options	Sequence	Checksum	Length	Number of Links
1.2.3.4	Link	0.0.0.4	0.0.0.1	837	0x19	0x80000001	0xE3C3	44	0

**Area ID:** The OSPF6 area ID of the link state advertisement

**Link State Type:** The type of the link state advertisement.

**Link State ID:** The OSPF6 link state ID. It identifies the piece of the routing domain that is being described by the LSA.

**Advertising Router:** The advertising router ID which originated the LSA.

**Age:** The time in seconds since the LSA was originated.

**Options:** The OSPF6 option field, present in OSPF6 hello packets, which enables OSPF6 routers to support (or not support) optional capabilities, and to communicate their capability level to other OSPF6 routers.

**Sequence:** The LS sequence number of the LSA.

**Checksum:** The checksum of the LSA contents.

**Length:** The Length in bytes of the LSA.

**Number of Links:** The count of the LSA.

### Buttons

**Auto-refresh:** Check this box to refresh the page automatically every 3 seconds.

**Refresh:** Click to refresh the page immediately.

**|<< :** Updates the table entries, starting from the first available entry. If the first entry of the table is displayed, the button is disabled.

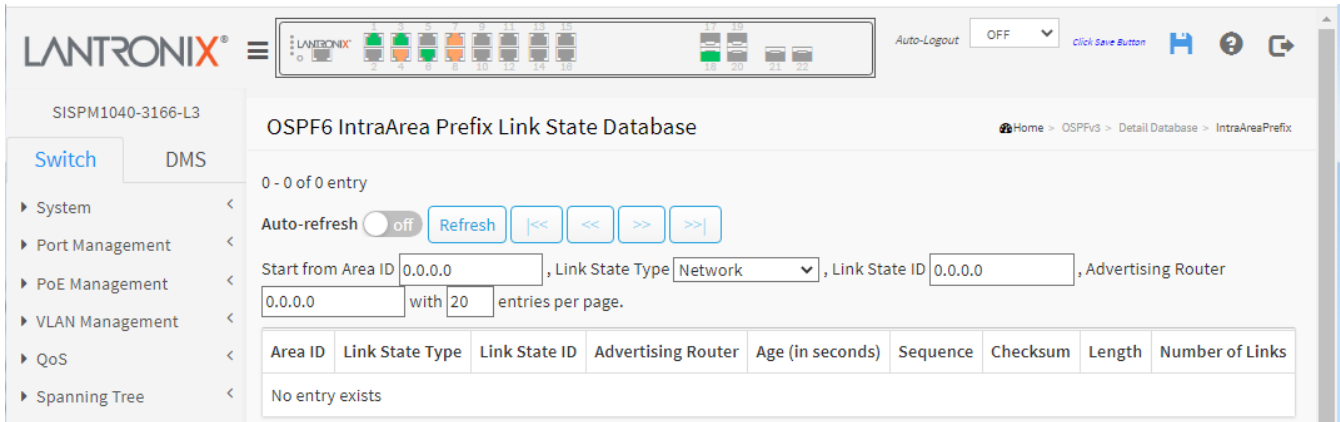
**<< :** Updates the table entries, ending at the entry prior to the first entry currently displayed. If the first entry of the table is displayed, the button is disabled.

**>> :** Updates the table entries, starting from the entry next to the last entry currently displayed. If the last entry of the table is displayed, the button is disabled.

**>> | :** Updates the table entries, ending at the last available entry. If the last entry of the table is displayed, the button is disabled.

## OSPFv3 > Detail Database > IntraArea Prefix

This page displays the OSPF6 IntraArea Prefix Link State Database. Set the Start from Area ID, Link State Type, Link State ID, Advertising Router, and entries per page controls.



**Area ID:** The OSPF6 area ID of the link state advertisement

**Link State Type:** The type of the link state advertisement.

**Link State ID:** The OSPF6 link state ID. It identifies the piece of the routing domain that is being described by the LSA.

**Advertising Router:** The advertising router ID which originated the LSA.

**Age (in seconds):** The time in seconds since the LSA was originated.

**Sequence:** The LS sequence number of the LSA.

**Checksum:** The checksum of the LSA contents.

**Length:** The Length in bytes of the LSA.

**Number of Links:** The count of the Prefixes.

### Buttons

**Auto-refresh:** Check this box to refresh the page automatically every 3 seconds.

**Refresh:** Click to refresh the page immediately.

**<<< :** Updates the table entries, starting from the first available entry. If the first entry of the table is displayed, the button is disabled.

**<< :** Updates the table entries, ending at the entry prior to the first entry currently displayed. If the first entry of the table is displayed, the button is disabled.

**>> :** Updates the table entries, starting from the entry next to the last entry currently displayed. If the last entry of the table is displayed, the button is disabled.

**>> | :** Updates the table entries, ending at the last available entry. If the last entry of the table is displayed, the button is disabled.

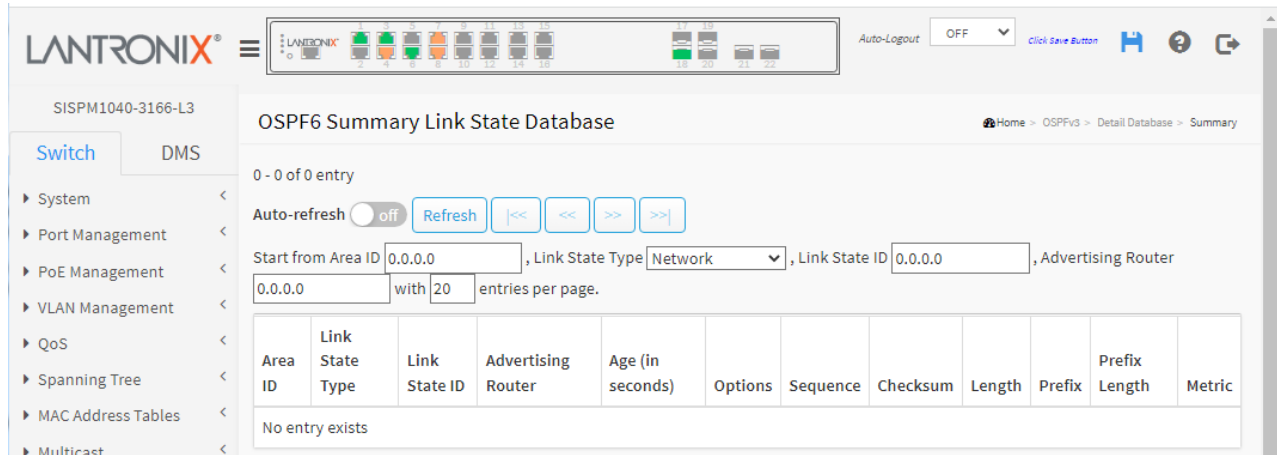
### Example:

Area ID	Link State Type	Link State ID	Advertising Router	Age (in seconds)	Sequence	Checksum	Length	Number of Links
1.2.34.4	IntraAreaPrefix	0.0.0.0	0.0.0.1	1531	0x80000001	0x23C5	40	1

## OSPFv3 > Detail Database > Summary

This page displays the OSPF6 LSA Summary link state database information table.

Set the Start from Area ID, Link State Type, Link State ID, Advertising Router, and entries per page controls.



**Area ID:** The OSPF6 area ID of the link state advertisement

**Link State Type:** The type of the link state advertisement.

**Link State ID:** The OSPF6 link state ID. It identifies the piece of the routing domain that is being described by the LSA.

**Advertising Router:** The advertising router ID which originated the LSA.

**Age (in seconds):** The time in seconds since the LSA was originated.

**Options:**

**Sequence:** The LS sequence number of the LSA.

**Checksum:** The checksum of the LSA contents.

**Length:** The Length in bytes of the LSA.

**Prefix:** IPv6 network address.

**Prefix Length:** IPv6 network mask length.

**Metric:** User specified metric for this summary route. The field is significant only when the link state type is 'External/NSSA External Link State' (Type 5, 7).

### Example:

Area ID	Link State Type	Link State ID	Advertising Router	Age (in seconds)	Options	Sequence	Checksum	Length	Prefix	Prefix Length	Metric
0.0.0.0	InterAreaPrefix	0.0.0.1	0.0.0.1	1635	0x0	0x80000001	0x7B9D	32	1::	21	10
1.0.0.9	InterAreaPrefix	0.0.0.1	0.0.0.1	183	0x0	0x80000002	0x95A6	28	::	0	0
3.0.0.0	InterAreaPrefix	0.0.0.1	0.0.0.1	138	0x0	0x80000002	0x95A6	28	::	0	0
3.0.0.0	InterAreaPrefix	0.0.0.2	0.0.0.1	1635	0x0	0x80000001	0x71A6	32	1::	21	10
10.0.0.1	InterAreaPrefix	0.0.0.1	0.0.0.1	157	0x0	0x80000002	0x95A6	28	::	0	0
10.0.0.1	InterAreaPrefix	0.0.0.2	0.0.0.1	1635	0x0	0x80000001	0x71A6	32	1::	21	10

## OSPFv3 > Detail Database > ASBR Summary

This page displays the OSPF6 LSA ASBR Summary link state database information table. Set the Start from Area ID, Link State Type, Link State ID, Advertising Router, and entries per page controls.

The screenshot shows the 'OSPF6 ASBR Summary Link State Database' page. The interface includes a navigation sidebar on the left with options like System, Port Management, PoE Management, VLAN Management, QoS, and Spanning Tree. The main area contains search filters for Area ID, Link State Type, Link State ID, and Advertising Router, along with an 'Auto-refresh' toggle and navigation buttons. The table below the filters is currently empty, displaying 'No entry exists'.

**Area ID:** The OSPF6 area ID of the link state advertisement

**Link State Type:** The type of the link state advertisement.

**Link State ID:** The OSPF6 link state ID. It identifies the piece of the routing domain being described by the LSA.

**Advertising Router:** The advertising router ID which originated the LSA.

**Age:** The time in seconds since the LSA was originated.

**Options:** The OSPF6 option field, present in OSPF6 hello packets, which enables OSPF6 routers to support (or not support) optional capabilities, and to communicate their capability level to other OSPF6 routers.

**Sequence:** The LS sequence number of the LSA.

**Checksum:** The checksum of the LSA contents.

**Length:** The Length in bytes of the LSA.

**Metric:** User specified metric for this summary route. The field is significant only when the link state type is 'Summary/ASBR Summary Link State' (Type 3, 4).

### Buttons

**Auto-refresh:** Check this box to refresh the page automatically every 3 seconds.

**Refresh:** Click to refresh the page immediately.

**|<< :** Updates the table entries, starting from the first available entry. If the first entry of the table is displayed, the button is disabled.

**<< :** Updates the table entries, ending at the entry prior to the first entry currently displayed. If the first entry of the table is displayed, the button is disabled.

**>> :** Updates the table entries, starting from the entry next to the last entry currently displayed. If the last entry of the table is displayed, the button is disabled.

**>> | :** Updates the table entries, ending at the last available entry. If the last entry of the table is displayed, the button is disabled.

## OSPFv3 > Detail Database > External

This page displays the OSPF6 LSA External link state database information table. Set the Start from Link State Type, Link State ID, Advertising Router, and entries per page controls.

The screenshot shows the 'OSPF6 External Link State Database' configuration page. The interface includes a navigation menu on the left with options like System, Port Management, PoE Management, VLAN Management, QoS, Spanning Tree, and MAC Address Tables. The main content area has a search section with the following controls:

- Auto-refresh:  off
- Refresh button
- Navigation buttons: <<, <, >, >>
- Start from Link State Type: Network (dropdown)
- Link State ID: 0.0.0.0 (input field)
- Advertising Router: 0.0.0.0 (input field)
- Entries per page: 20 (input field)

The table below the search controls is empty, showing the following headers:

Link State Type	Link State ID	Advertising Router	Age (in seconds)	Options	Sequence	Checksum	Length	Prefix	Prefix Length	Metric Type	Metric	Forward Address
No entry exists												

**Link State Type:** The type of the link state advertisement.

**Link State ID:** The OSPF6 link state ID. It identifies the piece of the routing domain that is being described by the LSA.

**Advertising Router:** The advertising router ID which originated the LSA.

**Age (in seconds):** The time in seconds since the LSA was originated.

**Options:** The OSPF6 option field, present in OSPF6 hello packets, which enables OSPF6 routers to support (or not support) optional capabilities, and to communicate their capability level to other OSPF6 routers.

**Sequence:** The LS sequence number of the LSA.

**Checksum:** The checksum of the LSA contents.

**Length:** The Length in bytes of the LSA.

**Prefix:** IPv6 network address.

**Prefix Length:** IPv6 network mask length.

**Metric Type:** The External type of the LSA. The field is significant only when the link state type is 'External/NSSA External Link State' (Type 5, 7).

**Metric:** User specified metric for this summary route. The field is significant only when the link state type is 'External/NSSA External Link State' (Type 5, 7).

**Forward Address:** The IP address of forward address. The field is significant only when the link state type is 'External/NSSA External Link State' (Type 5, 7).

### Buttons

**Auto-refresh:** Check this box to refresh the page automatically every 3 seconds.

**Refresh:** Click to refresh the page immediately.

**<<< :** Updates the table entries, starting from the first available entry. If the first entry of the table is displayed, the button is disabled.

<< : Updates the table entries, ending at the entry prior to the first entry currently displayed. If the first entry of the table is displayed, the button is disabled.

>> : Updates the table entries, starting from the entry next to the last entry currently displayed. If the last entry of the table is displayed, the button is disabled.

>> | : Updates the table entries, ending at the last available entry. If the last entry of the table is displayed, the button is disabled.

**Example:**

Link State Type	Link State ID	Advertising Router	Age (in seconds)	Options	Sequence	Checksum	Length	Prefix	Prefix Length	Metric Type	Metric	Forward Address
External	0.0.0.0	0.0.0.1	61	0x0	0x80000002	0x49B7	32	1::	21	0	0	::

## RIP

The Routing Information Protocol (RIP) prevents routing loops by implementing a limit on the number of hops allowed in a path from source to destination. The largest number of hops allowed for RIP is 15, which limits the size of networks that RIP can support. RIP uses the User Datagram Protocol (UDP) as its transport protocol and is assigned reserved port number 520.

### RIP > Configuration > Global Configuration

This page displays the RIP router global configuration table which lets you set common RIP router parameters.

The screenshot shows the 'RIP Global Configuration' page in the Lantronix web interface. The page title is 'RIP Global Configuration' and the breadcrumb is 'Home > RIP > Configuration > Global Configuration'. The interface includes a 'Clear RIP Process' button at the top left of the configuration area. The configuration is organized into several sections:

- RIP Router Mode:** A dropdown menu set to 'Disable'.
- Version:** A dropdown menu set to 'Default'.
- Timers:** A table with three rows:
 

Update	30
Invalid	180
Garbage-Collection	120
- Redistribute:** A table with three main sections:
 

Static	Mode	Disable
	Metric Value	<input checked="" type="radio"/> Auto <input type="radio"/> Specific <input type="text" value="1"/>
Connected	Mode	Disable
	Metric Value	<input checked="" type="radio"/> Auto <input type="radio"/> Specific <input type="text" value="1"/>
OSPF	Mode	Disable
	Metric Value	<input checked="" type="radio"/> Auto <input type="radio"/> Specific <input type="text" value="1"/>
- Default Metric Value:** A text input field set to '1'.
- Default Route:** A dropdown menu set to 'Disable'.
- Default Passive Mode:** A dropdown menu set to 'Disable'.
- Administrative Distance:** A text input field set to '120'.

At the bottom of the configuration area, there are 'Apply' and 'Reset' buttons.

**RIP Router Mode:** At the dropdown Enable or Disable RIP router mode:

**Enable:** Enable the RIP router mode.

**Disable:** Disable the RIP router mode (default).

**Version:** At the dropdown select the RIP version to be used:

**Default:** Base on the default version process. The router sends RIPv2 and accepts both RIPv1 and RIPv2. When the router receives either version of REQUESTS or triggered updates packets, it replies with the appropriate version.

**Version 1:** Receive/Send RIPv1 only.

**Version 2:** Receive/Send RIPv2 only.

**Update Timer:** The timer interval (in seconds) between the router sends the complete routing table to all neighboring RIP routers. The allowed range is 5 to 2147483 seconds.

**Invalid Timer:** The number of seconds after which a route will be marked invalid. The allowed range is 5 to 2147483 seconds.

**Garbage Collection Timer:** The number of seconds after which a route will be deleted. The allowed range is 5 to 2147483 seconds.

**Static Redistribute Mode:** Indicates if the router redistributes the static routes into the RIP domain or not.

**Enable:** Enable static routes redistribution.

**Disable:** Enable static routes redistribution.

**Static Redistribute Metric Value:** User specified metric value for the static routes. The field is significant only when the argument 'StaticRedistIsSpecificMetric' is TRUE. If the specific metric setting is removed while the static redistributed mode is enabled, the router will update the original static redistributed routes with metric value 16 before updates to the new metric value. The allowed range is 1 to 16.

**Auto:** The redistributed metric value; refer to redistributed default metric value.

**Specific:** User specified metric for the static routes.

**Connected Redistribute Mode:** Indicates if the router redistributes the directly connected routes with RIP not enabled into the RIP domain or not.

**Enable:** Enable connected routes redistribution.

**Disable:** Enable connected routes redistribution.

**Connected Redistribute Metric Value:** User specified metric value for the connected interfaces. The field is significant only when the argument 'ConnectedRedistIsSpecificMetric' is TRUE. If the specific metric setting is removed while the connected redistributed mode is enabled, the router will update the original connected redistributed routes with metric value 16 before updates to the new metric value. The allowed range is 1 to 16.

**Auto:** The redistributed metric value; refer to redistributed default metric value.

**Specific:** User specified metric for the connected routes.

**OSPF Redistribute Mode:** Indicate if the router redistributes the OSPF routes into the RIP domain or not. The field is significant only when the OSPF protocol is supported on the device.

**Enable:** Enable OSPF routes redistribution.

**Disable:** Enable OSPF routes redistribution.

**OSPF Redistribute Metric Value:** User specified metric value for the RIP routes. The field is significant only when the OSPF protocol is supported on the device and argument 'OspfRedistIsSpecificMetric' is TRUE. If the specific metric setting is removed while OSPF Redistribute mode is enabled, the router will update the original OSPF redistributed routes with metric value 16 before updates to the new metric value. The allowed range is 1 to 16.

**Auto:** The redistributed metric value; refer to redistributed default metric value.

**Specific:** User specified metric for the OSPF routes.

**Redistribute Default Metric Value:** The RIP default redistributed metric. It is used when the metric value isn't specified for the redistributed protocol type. The allowed range is 1 to 16.

**Redistribute Default Route:** Enable or disable RIP default route redistribution.

**Default Passive Mode:** Select Enable to set all interfaces as passive-interface by default.

**Administrative Distance:** The RIP administrative distance. The allowed range is 1 to 255. The default is 120.



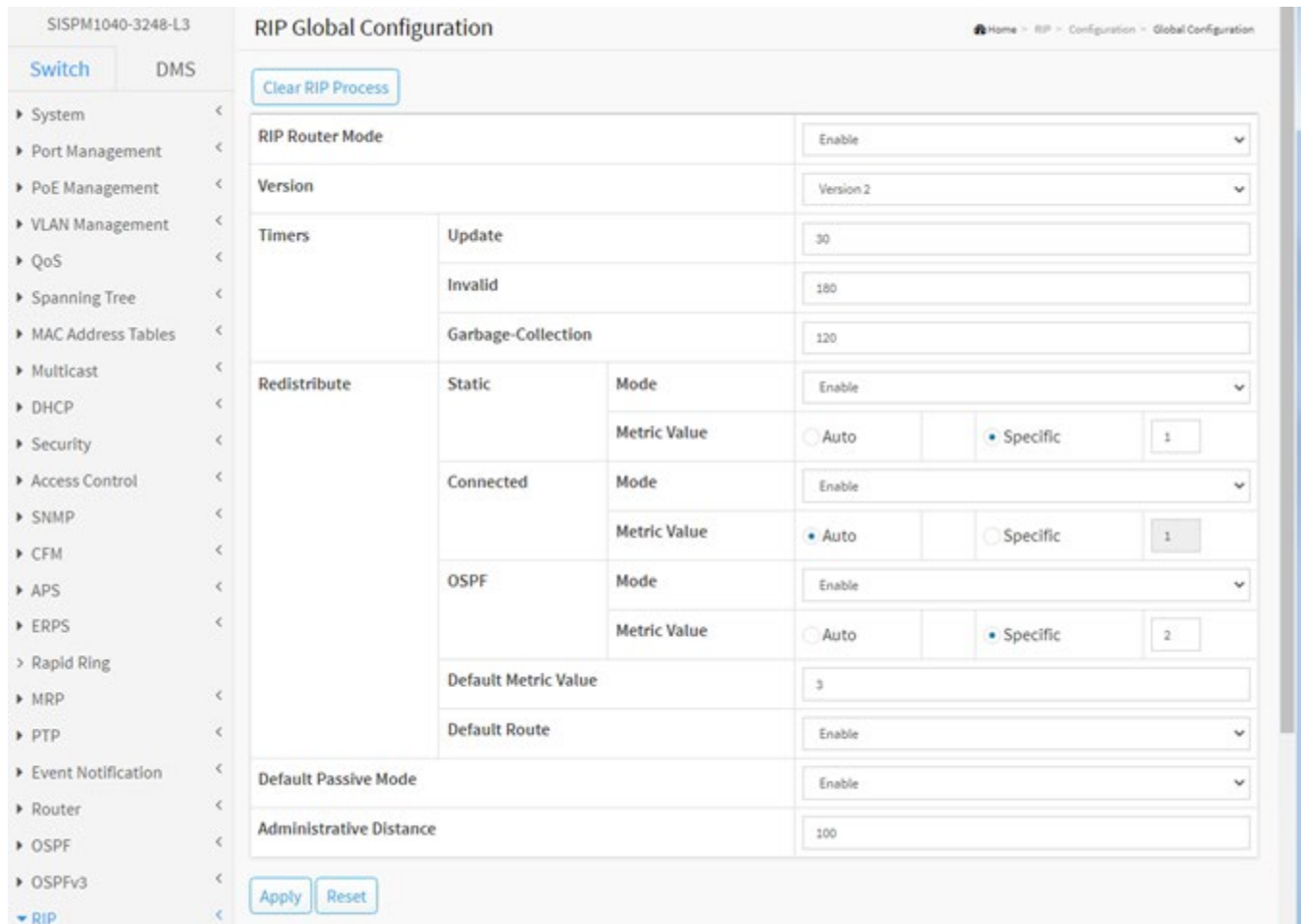
### Buttons

**Clear RIP Process:** Click to reset the current RIP process. At the “RIP process will be reset. Do you want to proceed anyway?” prompt click Yes or Cancel.

**Apply:** Click to save changes.

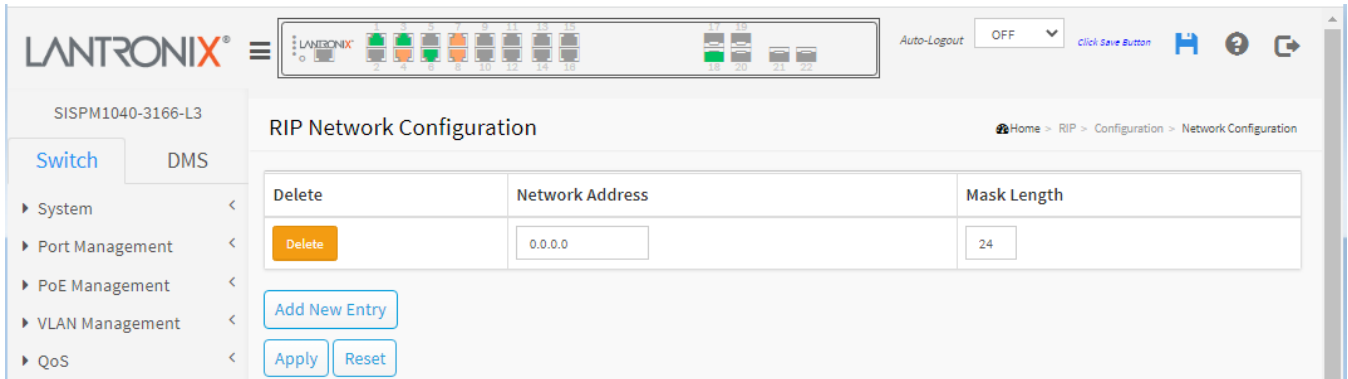
**Reset:** Click to undo any changes made locally and revert to previously saved values.

### Example:



## RIP > Configuration > Network Configuration

This page displays the RIP network configuration table. It is used to specify the RIP enabled interface(s). When RIP is enabled on the specific interface(s), the router can provide the network information to the other RIP routers via those interfaces.



**Delete:** Check to delete the entry. It will be deleted during the next save.

**Network Address:** IPv4 network address.

**Mask Length:** IPv4 network mask length.

### Buttons

**Add New Entry:** Click to add a new entry to the table.

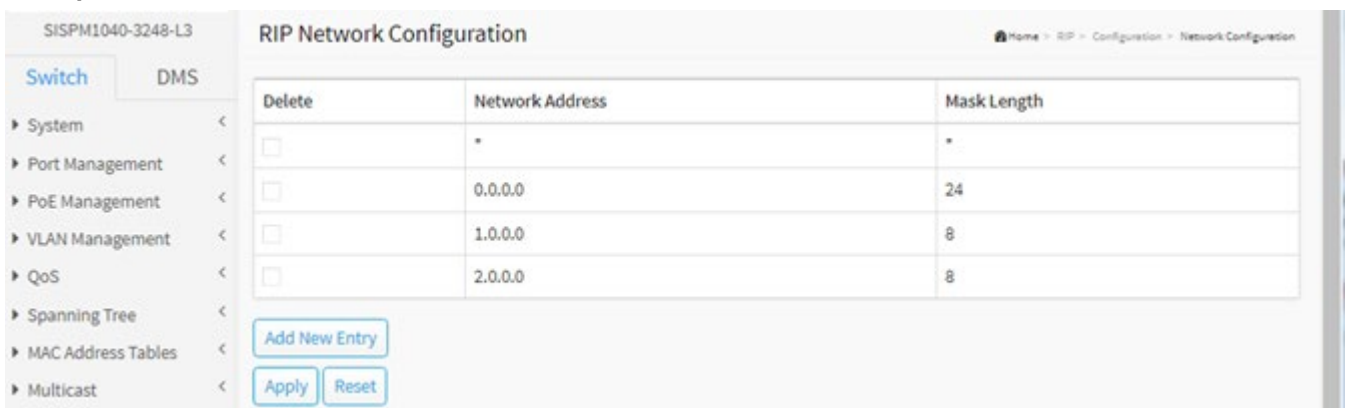
**Apply:** Click to save changes.

**Reset:** Click to undo any changes made locally and revert to previously saved values.

### Messages:

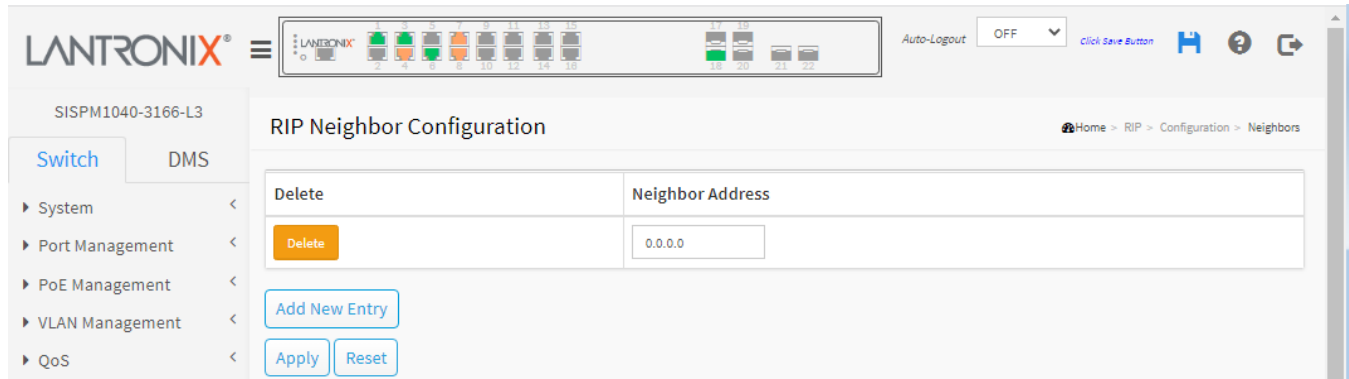
*The entry {Network Address:0.0.0.0, Mask Length:24} address range overlaps with {Network Address:0.0.0.0, Mask Length:24}.*

### Example:



### RIP > Configuration > Neighbor Configuration

This page displays the RIP neighbor connection table. It is used to configure the RIP router to send RIP updates to specific neighbors using the unicast, broadcast, or network IP address after update timer expiration.



**Delete:** Check to delete the entry. It will be deleted during the next save.

**Neighbor Address:** Ipv4 address encoded as "a.b.c.d", where a-d is a base-10 human readable integer in the range [0-255]. The neighbor address can be a unicast (excluding loopback), broadcast, or network IP address.

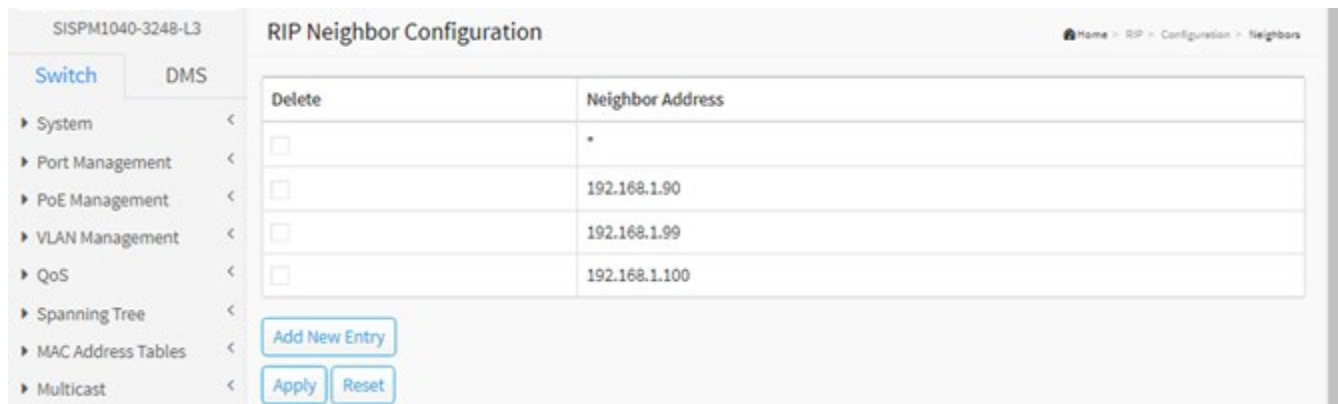
#### Buttons

**Add New Entry:** Click to add new entry.

**Apply:** Click to save changes.

**Reset:** Click to undo any changes made locally and revert to previously saved values.

#### Example:



## RIP > Configuration > Passive Interface

This page displays the RIP router interface configuration table.

Interface	Passive Interface
*	<input type="checkbox"/>
VLAN 1	<input checked="" type="checkbox"/>

**Interface:** Interface identification.

**Passive Interface:** Check the box to enable the interface as RIP passive-interface.

### Buttons

**Apply:** Click to save changes.

**Reset:** Click to undo any changes made locally and revert to previously saved values.

## RIP > Configuration > Interfaces

This page displays the RIP interface configuration table.

Interface	Send Version	Receive Version	Split Horizon Mode	Auth. Type	Change Simple Password / Key-Chain Name		
*	<	<	<	<	*	*	*
VLAN 1	Version 1 and 2	Version 2	Split Horizon	Null Authentication	<input type="checkbox"/>		

Buttons: Apply, Reset

**Interface:** Interface identification.

**Send Version:** The RIP version for the advertisement transmission on the interface.

**Version 1:** Set the RIP version to RIP v1.

**Version 2:** Set the RIP version to RIP v2.

**Version 1 and 2:** Use RIP version v1 and v2.

**Not Specified:** Do not specify a RIP receive version.

**Receive Version:** The RIP version for the advertisement reception on the interface.

**Version 1:** Set the RIP version to RIP v1.

**Version 2:** Set the RIP version to RIP v2.

**Version 1 and 2:** Use RIP version v1 and v2.

**Not Specified:** Do not specify a RIP receive version.

**Split Horizon Mode:** The split horizon mode to be used:

**Split Horizon:** To omit routes learned from one neighbor in updates sent to that neighbor.

**Poisoned Reverse:** The neighbor learned routes are included in updates sent to the neighbors but their metrics are set to infinity.

**Disabled:** Split horizon is disabled.

**Auth. Type:** The authentication type to be used:

**Simple Password:** It's using a plain text authentication. A password must be configured, but the password can be read by a packet sniffer.

**Message Digest:** It's message-digest algorithm 5 (MD5) authentication. Keying material must also be configured. This is the most secure method.

**Null Authentication:** No authentication.

**Change Simple Password:** Check the box to change the simple password (fill with plain text). The allowed input length is 1-15 printable characters excluding space character. The null string identifies none; simple password is set on the interface. **Note** that you cannot set key chain and simple password at the same time.

**Change Key-Chain Name:** It is used to change the key chain name used by MD5 authentication. The allowed input length is from 1-31 printable characters excluding space character. The null string identifies no key-chain name is set on the interface. **Note** that you cannot set key chain and simple password at the same time.

### Buttons

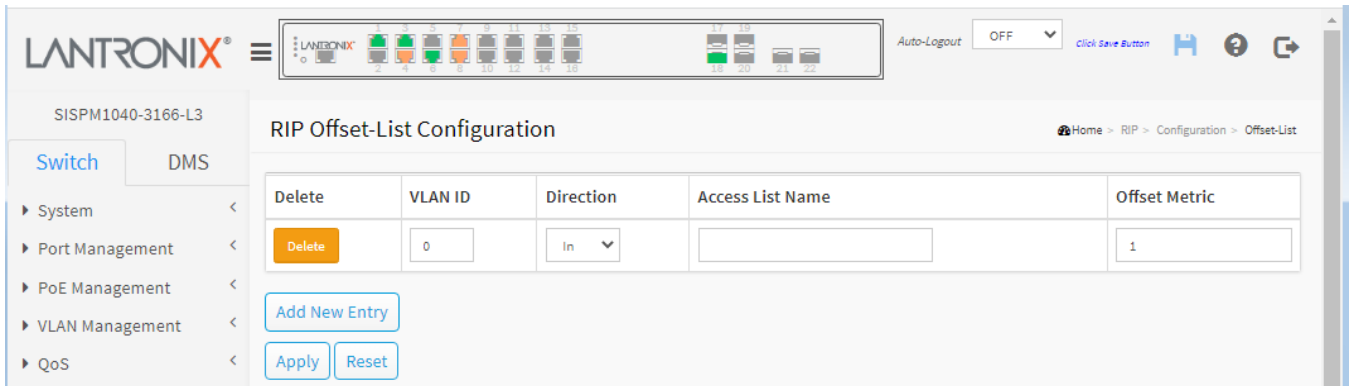
**Apply:** Click to save changes.

**Reset:** Click to undo any changes made locally and revert to previously saved values.

**Messages:** can not set key chain and simple password at the same time

### RIP > Configuration > Offset-List

This page displays the RIP offset-list configuration table.



**Delete:** Check to delete the entry. It will be deleted during the next save.

**VLAN ID:** The VLAN interface which the offset list applies to. The range is 0 - 4095. 0 means that the offset list applies to all interfaces.

**Direction:** The direction to add the offset to routing metric update.

**In:** Apply to the inbound direction (default).

**Out:** Apply to the outbound direction.

**Access List Name:** Access-list name. The valid name string length is 1-31 characters and allows all printable characters excluding the space character.

**Offset Metric:** The offset to incoming or outgoing routing metric. The allowed range is 0-16.

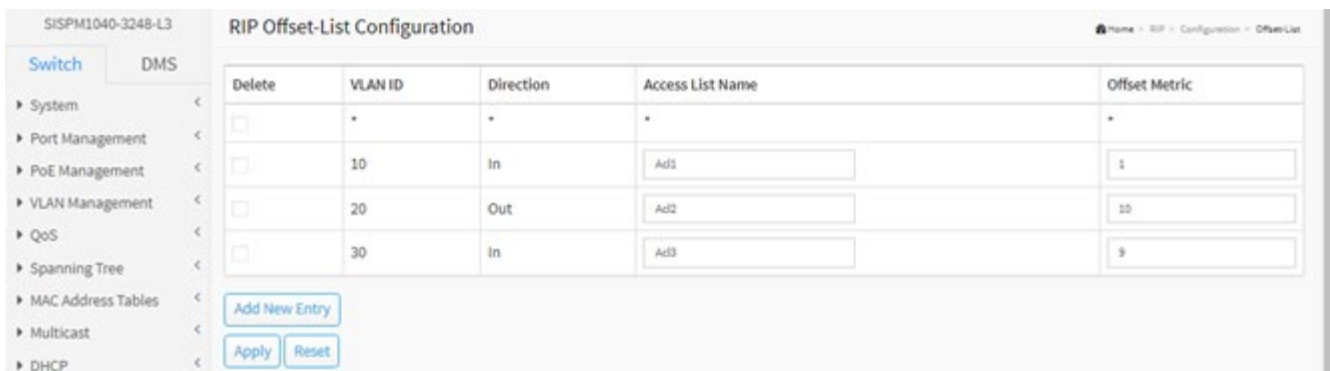
#### Buttons

**Add New Entry:** Click to add new entry to the table.

**Apply:** Click to save changes.

**Reset:** Click to undo any changes made locally and revert to previously saved values.

#### Example:



## RIP > Status > Global Status

This page displays the RIP general status information table.

The screenshot shows the 'RIP Global Status' page in the Lantronix web interface. The page has a navigation menu on the left with options like System, Port Management, PoE Management, VLAN Management, QoS, Spanning Tree, MAC Address Tables, Multicast, DHCP, Security, Access Control, SNMP, CFM, APS, and ERPS. The main content area is titled 'RIP Global Status' and includes an 'Auto-refresh' toggle set to 'off', a 'Refresh' button, and a 'Clear RIP Process' button. Below these is a 'Status Information' table.

Status Information	
Version	Default
Update Timer	30 secs
Invalid Timer	180 secs
Garbage-Collection Timer	120 secs
Next Update Time	23 secs
Redistribute Default Metric	1
Redistribute Connected	Enable
Redistribute Static	Enable
Redistribute OSPF	Enable
Administrative Distance	120

**Version:** This indicates the global RIP version. By default, the router sends RIPv2 and accepts both RIPv1 and RIPv2. When the router receives either version of REQUESTS or triggered updates packets, it replies with the appropriate version. Be aware of the RIP network class configuration when RIPv1 is involved in the topology. RIPv1 uses classful routing; the subnet information is not included in the routing updates. This limitation makes it impossible to have different-sized subnets inside of the same network class. In other words, all subnets in a network class must have the same size.

**Update Timer:** The timer interval (in seconds) between when the router sends the complete routing table to all neighboring RIP routers

**Invalid Timer:** The number of seconds after which a route will be marked invalid.

**Garbage-Collection Timer:** The number of seconds after which a route will be deleted.

**Next Update Time:** Specifies when the next round of updates will be sent out from this router in seconds.

**Redistribute Default Metric:** Indicates the default metric value of redistributed routes.

**Redistribute Connected:** Indicates the connected route is redistributed or not.

**Redistribute Static:** Shows Enable if the static route is redistributed, otherwise displays Disable.

**Redistribute OSPF:** Indicates the OSPF route is redistributed or not.

**Administrative Distance:** Indicates administrative distance value.

### Buttons

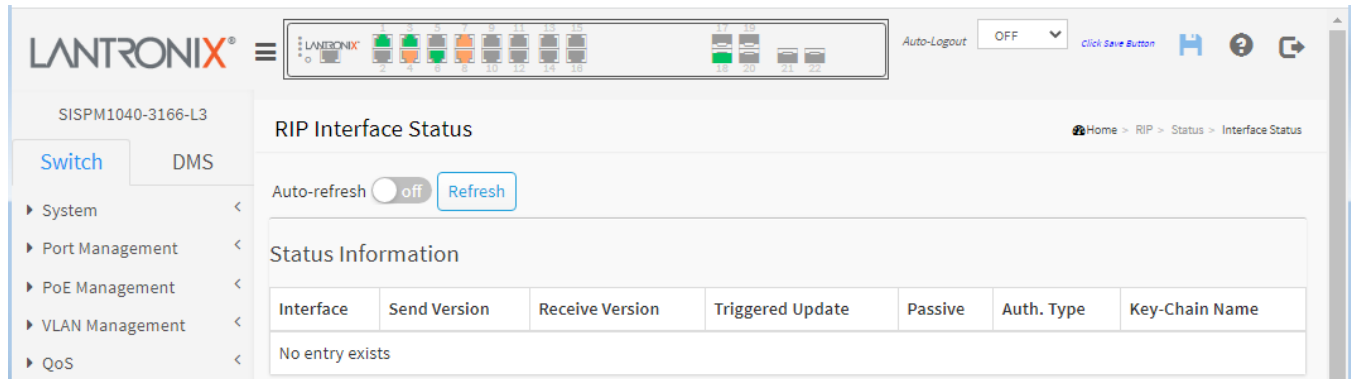
**Auto-refresh:** Check this box to refresh the page automatically every 3 seconds.

**Refresh:** Click to refresh the page immediately.

**Clear RIP Process:** Click to reset the current RIP process. At the confirmation prompt click OK or Cancel.

### RIP > Status > Interface Status

This page displays the RIP interface status information table.



**Interface:** Interface identification.

**Send Version:** The RIP version for the advertisement transmission on the interface.

**Receive Version:** The RIP version for the advertisement reception on the interface.

**Triggered Update:** Indicates if the interface has triggered update enabled (true) or disabled (false).

**Passive:** Indicates if the passive-interface is passive (true) or active (false) on the interface.

**Key-Chain Name:** Indicates if the interface is associated with a specific key-chain name.

#### Buttons

**Auto-refresh:** Check this box to refresh the page automatically every 3 seconds.

**Refresh:** Click to refresh the page immediately.

#### Example:

Status Information						
Interface	Send Version	Receive Version	Triggered Update	Passive	Auth. Type	Key-Chain Name
VLAN 1	Version 1 and 2	Version 2	true	true		



## RIP > Status > Peer Status

This page displays the RIP peer table. Set the Start from Address and entries per page controls and hit Refresh.

**Gateway:** Peer IPv4 address.

**Last Update Time:** The duration time in seconds from the time the last RIP packet received from the neighbor to now.

**Version:** The RIP version number in the header of the last RIP packet received from the neighbor.

**Received Bad Packets:** The number of RIP response packets from the neighbor that were discarded as invalid.

**Received Bad Routes:** The number of routes from the neighbor that were ignored because they were invalid.

### Buttons

**Auto-refresh:** Check this box to refresh the page automatically every 3 seconds.

**Refresh:** Click to refresh the page immediately.

**|<< :** Updates the table entries, starting from the first available entry. If the first entry of the table is displayed, the button is disabled.

**<< :** Updates the table entries, ending at the entry prior to the first entry currently displayed. If the first entry of the table is displayed, the button is disabled.

**>> :** Updates the table entries, starting from the entry next to the last entry currently displayed. If the last entry of the table is displayed, the button is disabled.

**>>| :** Updates the table entries, ending at the last available entry. If the last entry of the table is displayed, the button is disabled.

## RIP > Status > Database

This page displays the RIP Database Information table. Set the Start from Network, Next Hop, and entries per page controls then hit Refresh.

The screenshot shows the 'RIP Database Information' page in the Lantronix web interface. The page title is 'RIP Database Information' and the breadcrumb is 'Home > RIP > Status > Database'. The interface includes a navigation menu on the left with options like 'Switch', 'DMS', 'System', 'Port Management', 'PoE Management', 'VLAN Management', 'QoS', 'Spanning Tree', and 'MAC Address Tables'. The main content area shows '1 - 2 of 2 entries'. There are controls for 'Auto-refresh' (set to 'off'), a 'Refresh' button, and navigation buttons (|<<, <<, >>, >>|). Below these are input fields for 'Start from Network' (0.0.0.0 / 0), 'Next Hop' (0.0.0.0), and 'entries per page' (20). A table displays the following data:

Type	Sub-Type	Network	Next Hop	Metric	From	External Metric	Tag	Uptime
RIP	default	0.0.0.0/0	0.0.0.0	1	self		0	
Connected	redistribute	192.168.1.0/24	0.0.0.0	1	self		0	

**Type:** The protocol type of the route (e.g., RIP, Static, or Connected).

**Sub-Type:** The protocol sub-type of the route (e.g., default, static, or redistribute).

**Network:** The destination IP address and mask of the route.

**Next Hop:** The first gateway along the route to the destination.

**Metric:** The metric of the route.

**From:** Indicates the route is learned an IP address or generated from one of the local interfaces (e.g., self).

**External Metric:** The field is significant only when the route is redistributed from other protocol type, for example, OSPF. This indicates the metric value from the original redistributed source.

**Tag:** The tag of the route. It is used to provide a method of separating 'internal' RIP routes, which may have been imported from an EGP (Exterior Gateway Protocol) or another IGP (Interior Gateway Protocol). For example, routes imported from OSPF can have a route tag value which the other routing protocols can use to prevent advertising the same route back to the original protocol routing domain.

**Uptime:** The time field is significant only when the route is learned from the neighbors. When the route destination is reachable (its metric value less than 16), the uptime field means the invalid time of the route. When the route destination is unreachable (its metric value greater than 16), the uptime field means the garbage-collection time of the route.

### Buttons

**Auto-refresh:** Check this box to refresh the page automatically every 3 seconds.

**Refresh:** Click to refresh the page immediately.

|<< : Updates the table entries, starting from the first available entry. If the first entry of the table is displayed, the button is disabled.

<< : Updates the table entries, ending at the entry prior to the first entry currently displayed. If the first entry of the table is displayed, the button is disabled.

>> : Updates the table entries, starting from the entry next to the last entry currently displayed. If the last entry of the table is displayed, the button is disabled.

>>| : Updates the table entries, ending at the last available entry. If the last entry of the table is displayed, the button is disabled.

**Example:**

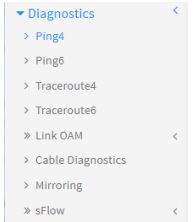
Type	Sub-Type	Network	Next Hop	Metric	From	External Metric	Tag	Uptime
Static	redistribute	0.0.0.0/0	192.168.1.254	1	self		0	
Connected	redistribute	192.168.1.0/24	0.0.0.0	1	self		0	

## Diagnostics

This section provides a set of system diagnostic test provided for troubleshooting purposes.

### Diagnostics > ICMP Ping (IPv4)

This page lets you issue ICMP (IPv4) PING packets to troubleshoot IP connectivity issues.



LANTRONIX®

SISPM1040-3166-L3

ICMP Ping (IPv4)

Fill in the parameters as needed and press "Start" to initiate the Ping session.

Hostname or IP Address	<input type="text"/>
Payload Size	<input type="text" value="56"/> bytes
Payload Data Pattern	<input type="text" value="0"/> (single byte value; integer or hex with prefix '0x')
Packet Count	<input type="text" value="5"/> packets
TTL Value	<input type="text" value="64"/>
VID for Source Interface	<input type="text"/>
Source Port Number	<input type="text"/>
IP Address for Source Interface	<input type="text"/>
Quiet (only print result)	<input type="checkbox"/>

**Hostname or IP Address:** The address of the destination host, either as a symbolic hostname or an IP Address.

**Payload Size:** Sets the size of the ICMP data payload in bytes (excluding the size of Ethernet, IP and ICMP headers). The default value is 56 bytes. The valid range is 2-1452 bytes.

**Payload Data Pattern:** Sets the pattern used in the ICMP data payload. The default value is 0. The valid range is 0-255.

**Packet Count:** sets the number of PING requests sent. The default value is 5 packets. The valid range is 1-60 packets.

**TTL Value:** Sets the Time-To-Live /TTL) field value in the IPv4 header. The default value is 64 seconds. The valid range is 1-255 seconds.

**VID for Source Interface:** This field can be used to force the test to use a specific local VLAN interface as the source interface. Leave this field empty for automatic selection based on routing configuration. **Note:** You may only specify either the VID or the IP Address for the source interface.

**Source Port Number:** This field can be used to force the test to use a specific local interface with the specified port number as the source interface. The specified port must be configured with a suitable IP address. Leave this field empty for automatic selection based on routing configuration. **Note:** You may only specify either the Source Port Number or the IP Address for the source interface.

**Address for Source Interface:** This field can be used to force the test to use a specific local interface with the specified IP address as the source interface. The specified IP address must be configured on a local interface. Leave this field empty for automatic selection based on routing configuration. **Note:** You may only specify either the VID or the IP Address for the source interface.

**Quiet (only print result):** Checking this option will not print the result of each ping request but will only show the final result.

After you press the **Start** button, ICMP packets are transmitted, and the sequence number and round trip time are displayed upon reception of a reply.

The amount of data received in an IP packet of type ICMP ECHO\_REPLY will always be 8 bytes more than the requested payload data size (the difference is the ICMP header).

The page refreshes automatically until responses to all packets are received, or until a timeout occurs.

The output from the command will look like the following:

```
PING 172.16.1.1 (172.16.1.1) from 172.16.1.10: 56 data bytes
64 bytes from 172.16.1.1: seq=0 ttl=64 time=2.034 ms
64 bytes from 172.16.1.1: seq=1 ttl=64 time=1.729 ms
64 bytes from 172.16.1.1: seq=2 ttl=64 time=1.954 ms
64 bytes from 172.16.1.1: seq=3 ttl=64 time=1.699 ms
64 bytes from 172.16.1.1: seq=4 ttl=64 time=1.916 ms

--- 172.16.1.1 ping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max = 1.699/1.866/2.034 ms

Ping session completed.
```

## Buttons

**Start:** Starts transmitting ICMP packets, and the sequence number and round trip time are displayed upon reception of a reply.

**New Ping:** After a Ping completes, click the button to start a new Ping.

## Diagnostics > ICMP Ping (IPv6)

This page lets you issue ICMPv6 PING packets to troubleshoot IPv6 connectivity issues.

**Hostname or IP Address:** The address of the destination host, either as a symbolic hostname or an IP Address.

**Payload Size:** Sets the size of the ICMP data payload in bytes (excluding the size of Ethernet, IP and ICMP headers). The default value is 56 bytes. The valid range is 2-1452 bytes.

**Payload Data Pattern:** Sets the pattern used in the ICMP data payload. The default value is 0. The valid range is 0-255.

**Packet Count:** Determines the number of PING requests sent. The default value is 5. The valid range is 1-60.

**VID for Source Interface:** This field can be used to force the test to use a specific local VLAN interface as the source interface. Leave this field empty for automatic selection based on routing configuration. **Note:** You may only specify either the VID or the IP Address for the source interface.

**Source Port Number:** This field can be used to force the test to use a specific local interface with the specified port number as the source interface. The specified port must be configured with a suitable IP address. Leave this field empty for automatic selection based on routing configuration. **Note:** You may only specify either the Source Port Number or the IP Address for the source interface.

**IP Address for Source Interface:** This field can be used to force the test to use a specific local interface with the specified IP address as the source interface. The specified IP address must be configured on a local interface. Leave this field empty for automatic selection based on routing configuration. **Note:** You may only specify either the VID or the IP Address for the source interface.

**Quiet (only print result):** Checking this option will not print the result of each ping request but will only show the final result.

After you press the **Start** button, ICMP packets are transmitted, and the sequence number and round trip time are displayed upon reception of a reply.

The amount of data received inside of an IP packet of type ICMP ECHO\_REPLY will always be 8 bytes more than the requested payload data size (the difference is the ICMP header).

The page refreshes automatically until responses to all packets are received, or until a timeout occurs.

The output from the IPv6 Ping looks like this:

```
PING 2001::01 (2001::1) from 2001::3: 56 data bytes
64 bytes from 2001::1: seq=0 ttl=64 time=2.118 ms
64 bytes from 2001::1: seq=1 ttl=64 time=2.009 ms
64 bytes from 2001::1: seq=2 ttl=64 time=1.852 ms
64 bytes from 2001::1: seq=3 ttl=64 time=2.869 ms
64 bytes from 2001::1: seq=4 ttl=64 time=1.845 ms

--- 2001::01 ping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max = 1.845/2.138/2.869 ms
```

### Buttons

**Start:** Starts transmitting ICMP packets.

**New Ping:** After a Ping completes, click the button to start a new Ping.

## Diagnostics > Traceroute (IPv4)

This page lets you perform a traceroute test over IPv4 towards a remote host. Traceroute is a diagnostic tool for displaying the route and measuring transit delays of packets across an IPv4 network.

The screenshot shows the 'Traceroute (IPv4)' configuration page in the Lantronix web interface. The page has a header with the Lantronix logo and a navigation menu on the left. The main content area contains a form with the following fields and options:

- Hostname or IP Address:** A text input field.
- DSCP Value:** A text input field with the value '0'.
- Number of Probes Per Hop:** A text input field with the value '3' and the unit 'packets'.
- Response Timeout:** A text input field with the value '3' and the unit 'seconds'.
- First TTL Value:** A text input field with the value '1'.
- Max TTL Value:** A text input field with the value '30'.
- VID for Source Interface:** A text input field.
- IP Address for Source Interface:** A text input field.
- Use ICMP instead of UDP:** A checkbox that is currently unchecked.
- Print Numeric Addresses:** A checkbox that is currently unchecked.

A 'Start' button is located at the bottom left of the form.

**Hostname or IP Address:** The destination IP Address.

**DSCP Value:** This value is used for the DSCP value in the IPv4 header. The default value is 0. The valid range is 0-63.

**Number of Probes Per Hop:** Determines the number of probes (packets) sent for each hop. The default value is 3. The valid range is 1-60.

**Response Timeout:** Determines the number of seconds to wait for a reply to a sent request. The default number is 3. The valid range is 1-86400.

**First TTL Value:** Determines the value of the Time-To-Live (TTL) field in the IPv4 header in the first packet sent. The default is 1. The valid range is 1-30.

**Max TTL Value:** Determines the maximum value of the Time-To-Live (TTL) field in the IPv4 header. If this value is reached before the specified remote host is reached the test stops. The default is 30. The valid range is 1-255.

**VID for Source Interface:** This field can be used to force the test to use a specific local VLAN interface as the source interface. Leave this field empty for automatic selection based on routing configuration. **Note:** You may only specify either the VID or the IP Address for the source interface.

**Address for Source Interface:** This field can be used to force the test to use a specific local interface with the specified IP address as the source interface. The specified IP address must be configured on a local interface. Leave this field empty for automatic selection based on routing configuration. **Note:** You may only specify either the VID or the IP Address for the source interface.

**Use ICMP instead of UDP:** By default, the **traceroute** command will use UDP datagrams. Selecting this option forces it to use ICMP ECHO packets instead.



**Print Numeric Addresses:** By default, the **tracert** command will print out hop information using a reverse DNS lookup for the acquired host IP addresses. This may slow down the display if the DNS information is not available. Selecting this option will prevent the reverse DNS lookup and force the **tracert** command to print numeric IP addresses instead.

**Buttons**

**Start:** Starts transmitting ICMP packets.

**New Traceroute:** After a traceroute completes, click the button to start a new traceroute.

**Example:**



## Diagnostics > Traceroute (IPv6)

This page lets you perform a traceroute test over IPv6 towards a remote host. Traceroute is a diagnostic tool for displaying the route and measuring transit delays of packets across an IPv6 network.

**Hostname or IP Address:** The destination IP Address.

**DSCP Value:** This value is used for the DSCP value in the IPv4 header. The default value is 0. The valid range is 0-255.

**Number of Probes Per Hop:** Determines the number of probes (packets) sent for each hop. The default value is 3. The valid range is 1-60.

**Response Timeout:** Determines the number of seconds to wait for a reply to a sent request. The default is 3. The valid range is 1-86400 seconds.

**Max TTL Value:** Determines the maximum value of the Time-To-Live (TTL) field in the IPv4 header. If this value is reached before the specified remote host is reached the test stops. The default is 255. The valid range is 1-255.

**VID for Source Interface:** This field can be used to force the test to use a specific local VLAN interface as the source interface. Leave this field empty for automatic selection based on routing configuration. **Note:** You may only specify either the VID or the IP Address for the source interface.

**Address for Source Interface:** This field can be used to force the test to use a specific local interface with the specified IP address as the source interface. The specified IP address must be configured on a local interface. Leave this field empty for automatic selection based on routing configuration. **Note:** You may only specify either the VID or the IP Address for the source interface.

**Print Numeric Addresses:** By default the **traceroute** command will print out hop information using a reverse DNS lookup for the acquired host IP addresses. This may slow down the display if the DNS information is not available. Selecting this option will prevent the reverse DNS lookup and force the **traceroute** command to print numeric IP addresses instead.

### Buttons

**Start:** Starts transmitting ICMP packets.

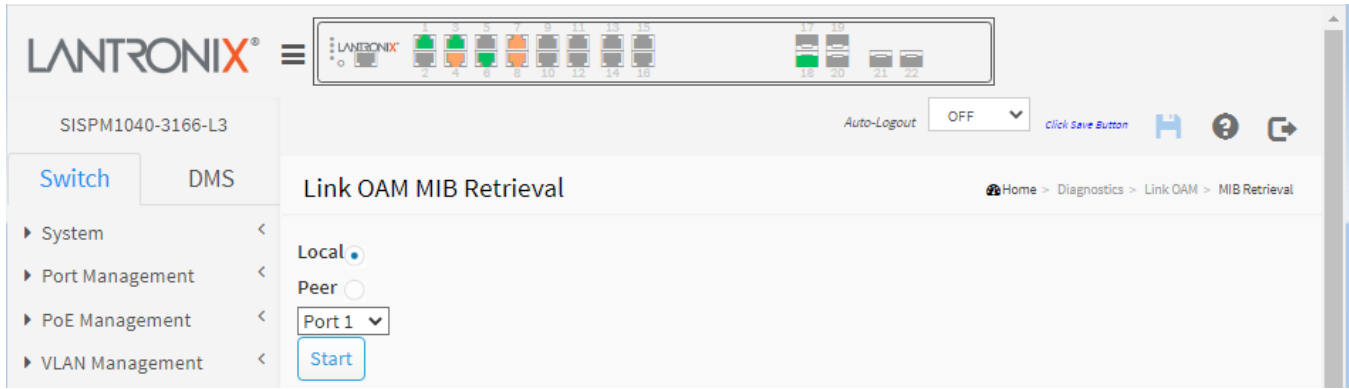
**New Traceroute:** After a traceroute completes, click the button to start a new traceroute.

## Diagnostics > MIB Retrieval

This page lets you retrieve the local or remote OAM MIB variable data on a particular port.

Select the appropriate radio button (Local or Peer)

At the dropdown select the port number of the switch to retrieve the content of interest.



Click on **Start** to retrieve the content.

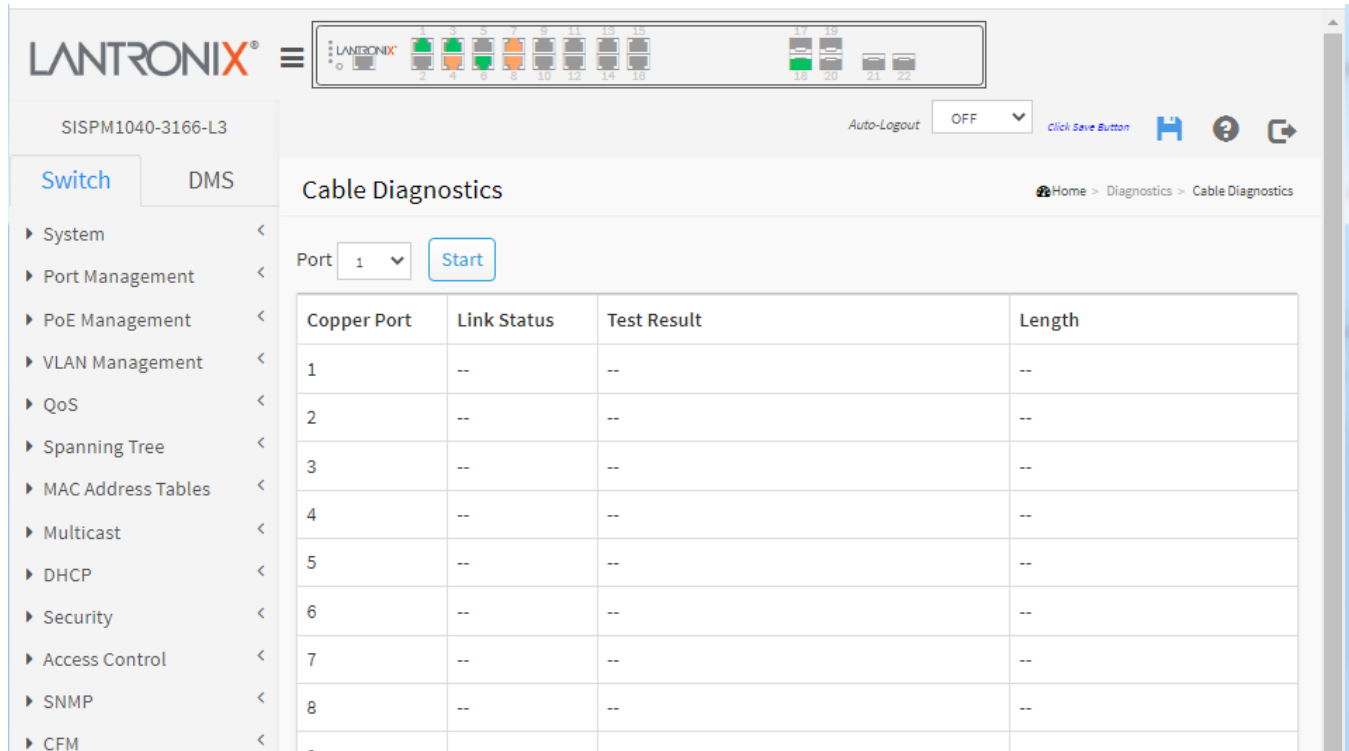
Click on **New Retrieval** to retrieve another content of interest.

## Diagnostics > Cable Diagnostics

This page is used for running the Cable Diagnostics for 10/100 and 1G copper ports.

Select the desired port and then click the Start button 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 - 120 meters with 5-meter accuracy.

10 and 100 Mbps ports will be linked down while running Cable Diagnostics. Therefore, running Cable Diagnostics on a 10 or 100 Mbps management port will cause the switch to stop responding until Cable Diagnostics is complete.



The screenshot shows the Lantronix web interface for device SISPM1040-3166-L3. The 'Cable Diagnostics' page is active, with a 'Port' dropdown set to '1' and a 'Start' button. Below the button is a table with the following data:

Copper Port	Link Status	Test Result	Length
1	--	--	--
2	--	--	--
3	--	--	--
4	--	--	--
5	--	--	--
6	--	--	--
7	--	--	--
8	--	--	--

**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.

**2.5G :** Cable is link up and correct. Speed is 2.5Gbps.

**Link Down:** Link down or cable is not correct.

**undefined:** The link status cannot be determined.

**Test Result:** Displays the result of the cable test:

**OK:** Correctly terminated pair.

**Abnormal:** Incorrectly terminated pair or link down.

**detect error or cable check length is between 7-120 meters.**

**Length:** The length (in meters) of the cable pair. The resolution is 3 meters. When Link Status is shown as follows, the length has different definitions:

**1G:** The length is the minimum value of 4-pair.

**10M/100M:** The length is the minimum value of 2-pair.

**Link Down:** The length is the minimum value of non-zero of 4-pair.

**Buttons:**

**Port select box:** At the dropdown select the port to be diagnosed.

**Start:** Press to run the diagnostics.

**Messages:**

*Cable Diagnostics is running...*

**Example:**

The screenshot shows the Lantronix web interface for device SISPM1040-3166-L3. The 'Cable Diagnostics' section is active, showing a dropdown menu for 'Port' set to '5' and a 'Start' button. Below this is a table with the following data:

Copper Port	Link Status	Test Result	Length
1	undefined	detect error or check cable length is between 7-120 meters	
2	undefined	detect error or check cable length is between 7-120 meters	
3	undefined	OK	3(m)
4	undefined	OK	3(m)
5	Cable Diagnostics is running...		
6	--	--	--

## Diagnostics > Mirroring

Mirroring is a feature for switched port analyzer. The administrator can use the Mirroring to debug network problems. The selected traffic can be mirrored or copied on a destination port where a network analyzer can be attached to analyze the network traffic.

For debugging network problems or monitoring network traffic, the switch system can be configured to mirror frames from multiple ports to a mirror port. (In this context, mirroring a frame is the same as copying the frame.)

Both incoming (source) and outgoing (destination) frames can be mirrored to the mirror port.

The screenshot shows the 'Mirror Configuration' page in the Lantronix web interface. The page title is 'SISPM1040-3166-L3'. The navigation menu on the left includes 'Switch' and 'DMS'. The main configuration area has the following sections:

- Monitor Session:** A dropdown menu set to '1'.
- Monitor destination port:** A dropdown menu set to 'Disabled'.
- Monitor Source Port Configuration:** A table with the following data:
 

Port	Mode
*	<->
1	Disabled
2	Disabled
3	Disabled
4	Disabled
5	Disabled
6	Disabled
7	Disabled

**Monitor Session:** At the dropdown select a session id to configure.

**Monitor destination port:** The destination port is an end node for monitor flow.

**Monitor Source Port Configuration:** The source node configuration for monitor flow.

**Port:** The logical port for the settings contained in the same row.

**Mode:** Select mirror mode:

**Disabled:** Neither frames transmitted nor frames received are mirrored.

**tx:** Frames transmitted on this port are mirrored on the Intermediate/Destination port. Frames received are not mirrored.

**rx:** Frames received on this port are mirrored on the Intermediate/Destination port. Frames transmitted are not mirrored.

**both:** Frames received and frames transmitted are mirrored on the Intermediate/Destination port.

**Note:** For a given port, a frame is only transmitted once. It is therefore not possible to mirror mirror port Tx frames. Because of this, the mode for the selected mirror port is limited to Disabled or rx.

### Buttons

**Apply:** Click to save changes.

**Reset:** Click to undo any changes made locally and revert to previously saved values.

## Diagnostics > sFlow > Configuration

This page lets you configure sFlow. The configuration is divided into two parts: configuration of the sFlow receiver (a.k.a. sFlow collector) and configuration of per-port flow and counter samplers. sFlow configuration is not persisted to non-volatile memory, which means that a reboot will disable sFlow sampling.

sFlow is an industry standard technology for monitoring switched networks through random sampling of packets on switch ports and time-based sampling of port counters. The sampled packets and counters (referred to as flow samples and counter samples, respectively) are sent as sFlow UDP datagrams to a central network traffic monitoring server. This central server is called an sFlow receiver or sFlow collector. Additional information can be found at <http://sflow.org>.

The screenshot shows the 'sFlow Configuration' page in the Lantronix web interface. The page is divided into three main sections: Agent Configuration, Receiver Configuration, and Port Configuration.

**Agent Configuration:**

- IP Address: 127.0.0.1

**Receiver Configuration:**

- Owner: <none> (with a Release button)
- 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"/>	<->			<input type="checkbox"/>	
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

### Agent Configuration

**IP Address:** The IP address used as Agent IP address in sFlow datagrams. It serves as a unique key that will identify this agent over extended periods of time. Both IPv4 and IPv6 addresses are supported.



## **Receiver Configuration**

**Owner:** Basically, sFlow can be configured in two ways: Through local management using the Web or CLI interface or through SNMP. This read-only field shows the owner of the current sFlow configuration and assumes values as follows:

- If sFlow is currently unconfigured/unclaimed, Owner contains <none>.
- If sFlow is currently configured through Web or CLI, Owner contains <Configured through local management>.
- If sFlow is currently configured through SNMP, Owner contains a string identifying the sFlow receiver.

If sFlow is configured through SNMP, all controls - except for the Release-button - are disabled to avoid inadvertent reconfiguration.

The **Release** button 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 appear).

**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. Valid range is 0 - 2147483647 seconds.

**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. Valid range is 1 to 32767.

**Flow Sampler Max. Header:** The maximum number of bytes that should be copied from a sampled packet to the sFlow datagram. Valid range is 14 to 200 bytes with default being 128 bytes. If the maximum datagram size does not 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. Valid range is 1 to 3600 seconds.

## **Buttons**

**Release:** 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).

**Refresh:** Click to refresh the page. Note that unsaved changes will be lost.

**Apply:** Click to save changes. Note that sFlow configuration is not persisted to non-volatile memory.

**Reset:** Click to undo any changes made locally and revert to previously saved values.

## Diagnostics > sFlow > Statistics

This page shows receiver and per-port sFlow statistics.

The screenshot shows the 'sFlow Statistics' page in the Lantronix web interface. The page title is 'sFlow Statistics' and the breadcrumb is 'Home > Diagnostics > sFlow > Statistics'. The interface includes an 'Auto-refresh' toggle set to 'off', and buttons for 'Refresh', 'Clear Receiver', and 'Clear Ports'. Below these are two tables:

Receiver Statistics	
Owner	<none>
IP Address/Hostname	0.0.0.0
Timeout	0
Tx Successes	0
Tx Errors	0
Flow Samples	0
Counter Samples	0

Port Statistics			
Port	Rx Flow Samples	Tx Flow Samples	Counter Samples
1	0	0	0
2	0	0	0
3	0	0	0
4	0	0	0
5	0	0	0
6	0	0	0
7	0	0	0
8	0	0	0

### Receiver Statistics

**Owner:** This field shows the current owner of the sFlow configuration. It assumes one of three values as follows:

- If sFlow is currently unconfigured/unclaimed, Owner contains <none>.
- If sFlow is currently configured through Web or CLI, Owner contains <Configured through local management>.
- If sFlow is currently configured through SNMP, Owner contains a string identifying the sFlow receiver.

**IP Address/Hostname:** The IP address or hostname of the sFlow receiver.

**Timeout:** The number of seconds remaining before sampling stops and the current sFlow owner is released.

**Tx Successes:** The number of UDP datagrams successfully sent to the sFlow receiver.

**Tx Errors:** The number of UDP datagrams that has failed transmission. The most common source of errors is invalid sFlow receiver IP/hostname configuration. To diagnose, paste the receiver's IP address/hostname into the Ping Web page (Diagnostics > Ping/Ping6).

**Flow Samples:** The total number of flow samples sent to the sFlow receiver.

**Counter Samples:** The total number of counter samples sent to the sFlow receiver.

**Port Statistics**

**Port:** The port number for which the following statistics applies.

**Rx and Tx Flow Samples:** The number of flow samples sent to the sFlow receiver originating from this port. Here, flow samples are divided into Rx and Tx flow samples, where Rx flow samples contains the number of packets that were sampled upon reception (ingress) on the port and Tx flow samples contains the number of packets that were sampled upon transmission (egress) on the port.

**Counter Samples:** The total number of counter samples sent to the sFlow receiver originating from this port.

**Buttons**

**Auto-refresh:** Check this box to refresh the page automatically every 3 seconds.

**Refresh:** Click to refresh the page.

**Clear Receiver:** Clears the sFlow receiver counters.

**Clear Ports:** Clears the per-port counters.

## Maintenance

This section provides maintenance configuration functions (save, backup, restore, activate, and delete) restart device, reset to factory defaults, and firmware upgrade and selection functions.

- ▼ Maintenance
  - » Configuration
    - > Save Startup-config
    - > Backup
    - > Restore
    - > Activate
    - > Delete
    - > Restart Device
    - > Factory Defaults
    - » Firmware

### Maintenance > Configuration

The switch stores its configuration in a number of text files in CLI format. The files are either virtual (RAM-based) or stored in flash on the switch.

The 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.
- **Up to 99 other files,** typically used for configuration backups or alternative configurations.

### Save Startup-config

This page lets you copy running-config to startup-config, thereby ensuring that the currently active configuration will be used at the next reboot.

The screenshot shows the 'Save Running Configuration' page in the Lantronix web interface. At the top, there is a navigation bar with the Lantronix logo, a menu icon, and a status bar showing 'Auto-Logout OFF' and a 'Click Save Button' link. Below the navigation bar, the page title is 'Save Running Configuration' and the breadcrumb trail is 'Home > Maintenance > Configuration > Save Startup-config'. On the left side, there is a sidebar menu with 'Switch' and 'DMS' tabs, and a list of configuration categories: System, Port Management, PoE Management, VLAN Management, and QoS. The main content area has a 'File Name' section with two radio buttons: 'startup-config' (selected) and 'filename' (with an adjacent text input field). At the bottom of this section is a 'Save Configuration' button.

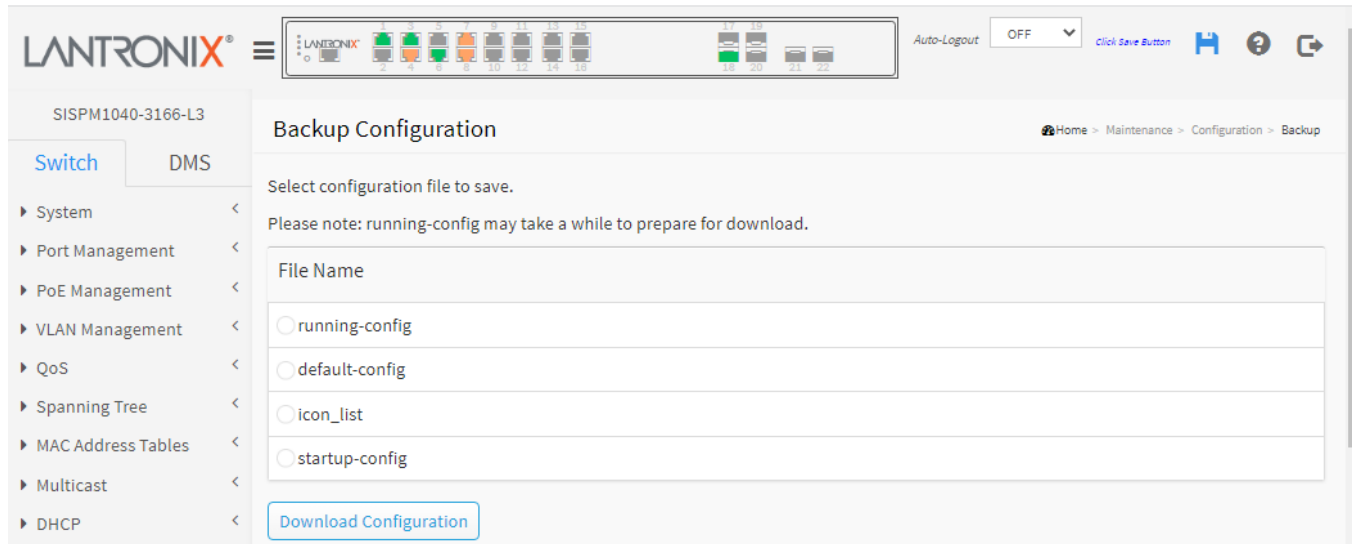
**File Name:** Tic a radio button to select a filename.

**Save Configuration:** Click the button to start the save process.

When done a message displays: *save running config to startup-config successfully*. Click the OK button to clear the message.

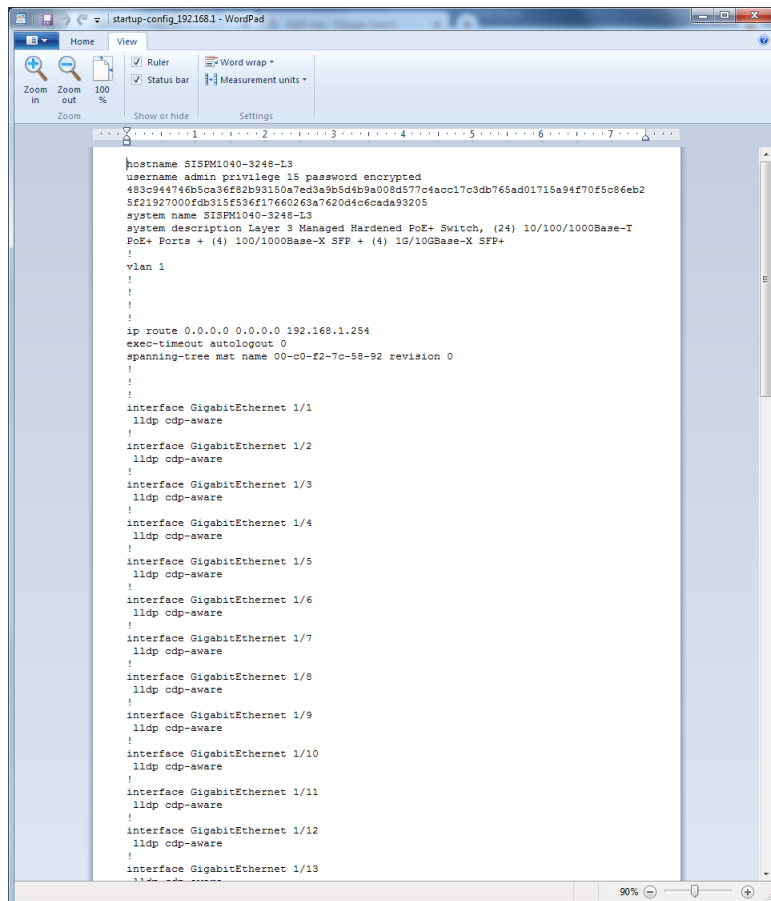
## Backup Configuration

It is possible to download any of the files on the switch to the web browser. Select the file and click the Download Configuration button. Download of running-config may take a little while to complete, as the file must be prepared for download.



**File Name:** Select a configuration file to save (e.g., running-config, default-config, icon\_list, or startup-config).

A sample startup-config file page is shown below:



## Restore Configuration

It is possible to upload a file from the web browser to all the files on the switch, except default-config which is read-only.

Select the file to upload, select the destination file on the target, then click the Upload Configuration button.

If the destination is running-config, the file will be applied to the switch configuration. This can be done in two ways:

**Replace mode:** The current configuration is fully replaced with the configuration in the uploaded file.

**Merge mode:** The uploaded file is merged into running-config.

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.

The screenshot shows the 'Restore Configuration' page in the Lantronix web interface. The page title is 'Restore Configuration' and the breadcrumb is 'Home > Maintenance > Configuration > Restore'. The 'File to Upload' field is empty, with a 'Choose File' button and 'No file chosen' text. The 'Destination File' section contains a table with the following data:

File Name	Parameters
<input type="radio"/> running-config	<input checked="" type="radio"/> Replace <input type="radio"/> Merge
<input type="radio"/> icon_list	
<input type="radio"/> startup-config	
<input type="radio"/> Create new file	<input type="text"/>

An 'Upload Configuration' button is located at the bottom of the form.

**File Name:** Select running-config (Replace or Merge), icon\_list, startup-config, or Create new file (with an entry).

Click the Upload Configuration button.

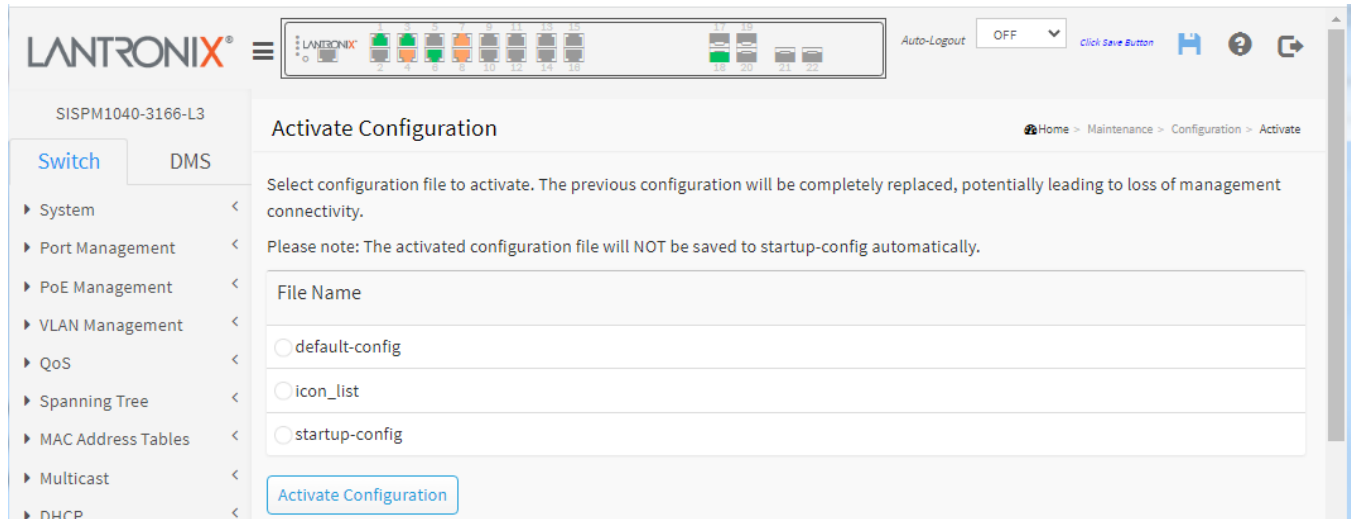
The message “*Upload successfully completed.*” displays when done.

## Activate Configuration

It is possible to activate any of the configuration files present on the switch, except for running-config which represents the currently active configuration.

Select the file to activate and click the Activate Configuration button. This will initiate the process of completely replacing the existing configuration with that of the selected file. The previous configuration will be completely replaced, potentially leading to loss of management connectivity.

**Note:** The activated configuration file will NOT be saved to startup-config automatically.

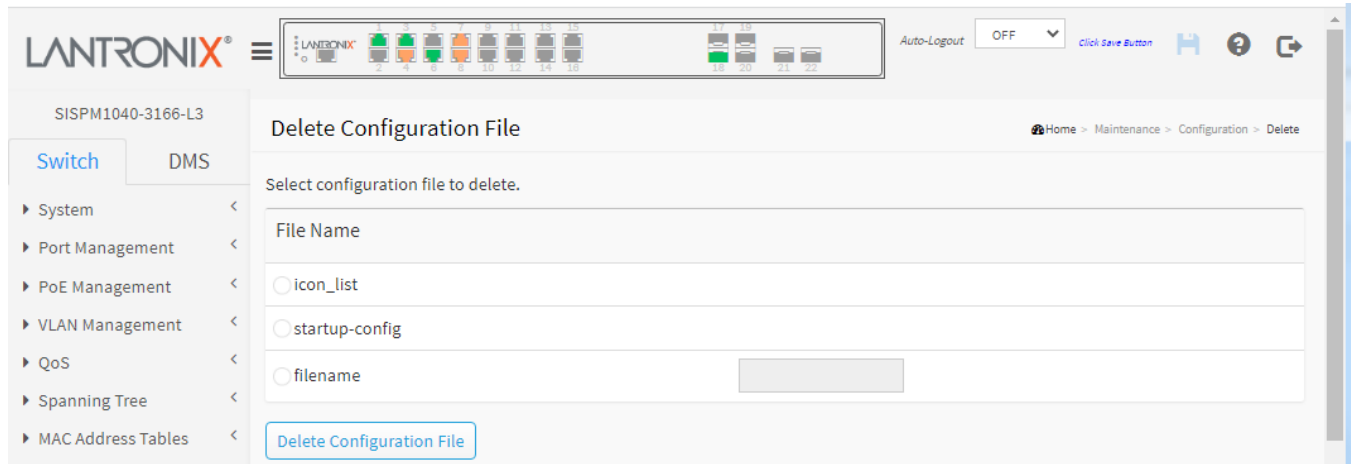


**File Name:** Select default-config, icon\_list, or startup-config.

Click the Activate Configuration button.

### Delete Configuration File

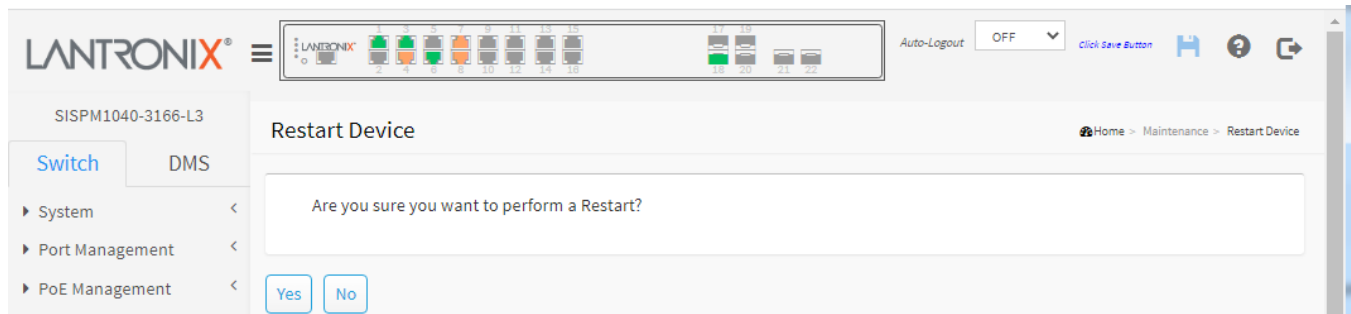
It is possible to delete any of the writable files stored in flash, including startup-config. If this is done and the switch is rebooted without a prior Save operation, this effectively resets the switch to default configuration.



1. Select a configuration file to delete.
2. Click the Delete Configuration File button.
3. At the prompt “Are you sure ...?” click the OK button.
4. The message “<filename> successfully deleted” displays.

### Maintenance > Restart Device

You can restart the switch on this page. The prompt “Are you sure you want to perform a Restart?” displays:



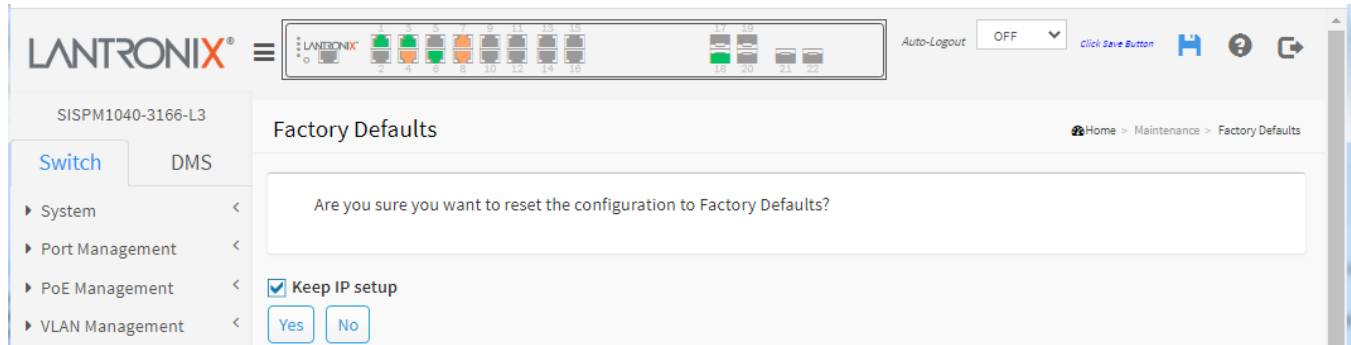
**Yes:** Click to restart device.

**No:** Click to return to the System > System Information page without restarting.



## Maintenance > Factory Defaults

You can reset the configuration of the switch on this page. The IP setup can be retained. The new configuration is available immediately, which means that no restart is necessary.



Check or uncheck the **Keep IP setup** checkbox.

At the “Are you sure you want to reset the configuration to Factory Defaults?” prompt click Yes or No.

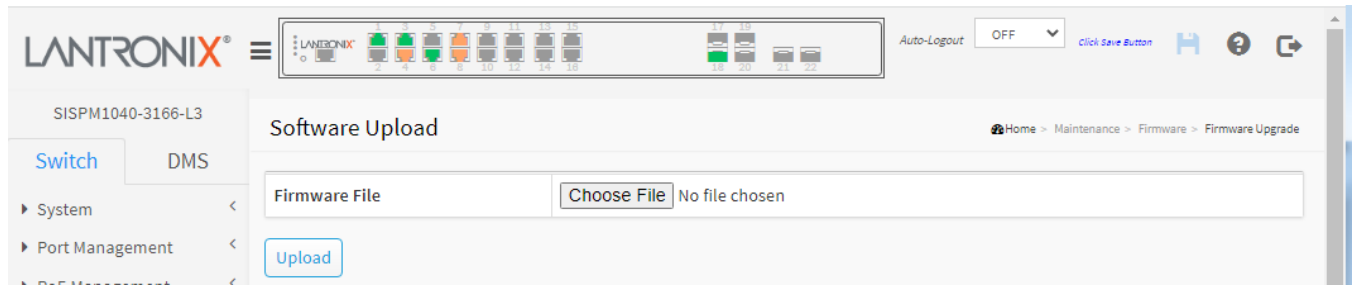
**Yes:** Click to reset the configuration to Factory Defaults.

**No:** Click to return to the System > System Information 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.

## Maintenance > Firmware > Firmware Upgrade

The Software Upload page facilitates an update of the firmware controlling the switch.

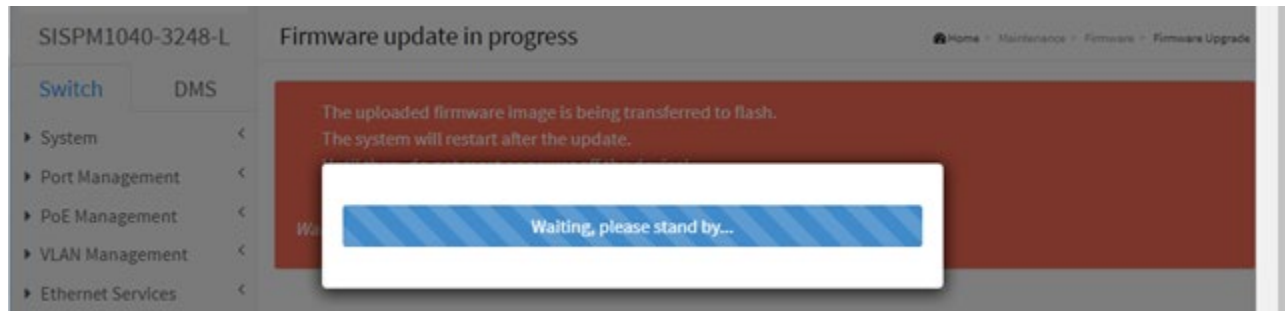


Click the **Choose File** button, browse to the location of a software image, and click the **Upload** button.

After the software image is uploaded, a page announces that the firmware update is initiated. After about a minute, the firmware is updated and the switch restarts.

**Warning:** While the firmware is being updated, Web access appears to be defunct. The front LED flashes Green/Off with a frequency of 10 Hz while the firmware update is in progress. Do not restart or power off the device at this time or the switch may fail to function afterwards.

**Messages:** *Firmware update in progress:*



## Maintenance > Firmware > Firmware Selection

The Software Image Selection page provides information about the active and alternate (backup) firmware images in the device and allows you to revert to the alternate image.

The web page displays two tables with information about the active and alternate firmware images.

**Note:** In case the active firmware image is the alternate image, only the "Active Image" table is shown. In this case, the Activate Alternate Image button is also disabled.

If the alternate image is active (due to a corruption of the primary image or by manual intervention), uploading a new firmware image to the device will automatically use the primary image slot and activate this.

The firmware version and date information may be empty for older firmware releases. This does not constitute an error.

The screenshot shows the Lantronix web interface for the device SISPM1040-3166-L3. The page title is "Software Image Selection". The breadcrumb trail is "Home > Maintenance > Firmware > Firmware Selection". The page displays two tables:

Active Image	
Image	linux
Version	SISPM1040-3166-L3 (standalone) v8.90.884
Date	2022-02-16T10:23:27+08:00

Alternate Image	
Image	linux.bk
Version	SISPM1040-3166-L3 (standalone) v8.90.696
Date	2021-10-15T15:18:02+08:00

At the bottom of the page, there are two buttons: "Activate Alternate Image" and "Cancel".

### Image Information

**Image:** The file name of the firmware image, from when the image was last updated.

**Version:** The version of the firmware image.

**Date:** The date where the firmware was produced.

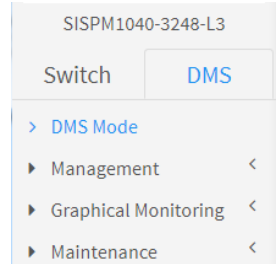
### Buttons

**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 System > System Information page.

## DMS (Device Management System)

The Device Management System (DMS) software that provides advanced tools necessary for total management of all connected network elements. The unique set of features and capabilities provide security integrators with lower overall cost, less downtime, and easier management and maintenance of an entire PoE network.

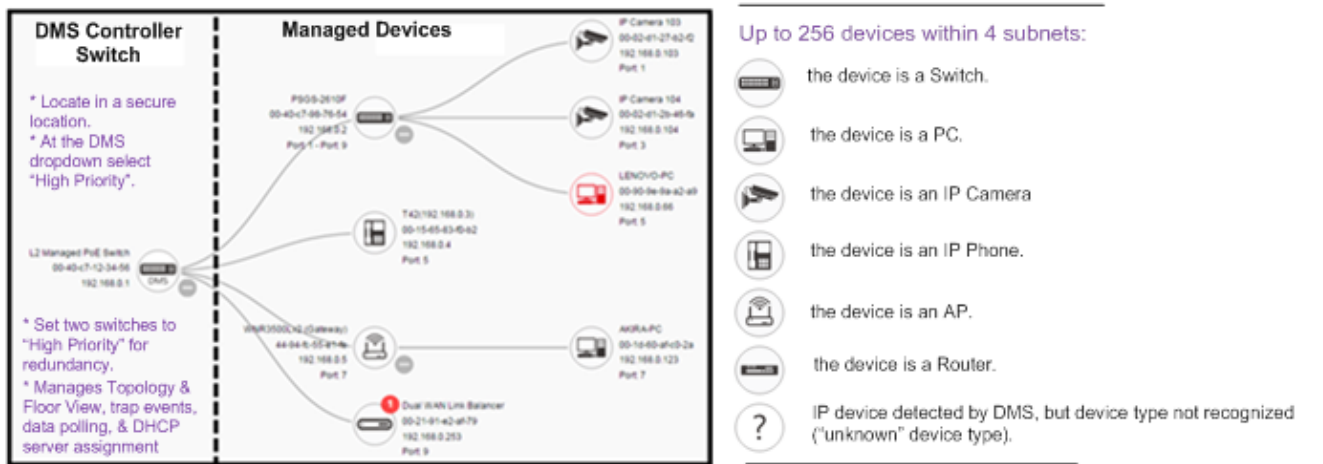


### DMS Features

- Automatically discover and remotely configure attached IP-addressable powered devices (PD)
- Graphical topology view for device management
- Floor view for device management (import JPEG drawings)
- Google Maps™ view for device management
- Auto Power Reset (APR) monitors and automatically restarts edge devices
- Troubleshoot cable and IP connection issues
- Monitor and analyze traffic by Day/Week/Port/Device
- Auto-Alarm on error conditions

### DMS > DMS Mode

- Configure DMS mode and monitor device numbers/ DMS Controller Switch IP.
- DMS is controlled by the DMS Controller switch, as specified by the DMS Mode selection.
- The DMS Controller Switch controls syncing DMS information in order to manage Topology View, Floor View, and trap event / data polling / DHCP server assignment.



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. With DHCP Server mode enabled in DMS network, the DMS Controller switch is responsible for assigning IP address for all devices.

The DMS Controller Switch will Collect, Poll, and Sync DMS information, and act as the Event Notification control center to manage all device information.

## DMS Information page

The DMS Information page lets you enable and disable DMS mode and specify DMS Controller Priority. DMS is controlled by the DMS Controller switch, as specified by the DMS Mode selection. The DMS Controller Switch controls syncing DMS information in order to manage Topology View, Floor View, and trap event / data polling / DHCP server assignment.

The screenshot shows the Lantronix web interface for the SISPM1040-3166-L3 switch. The 'DMS' tab is selected in the left sidebar. The 'Information' section contains the following configuration details:

Mode	Enabled
Controller Priority	High
Total Device	1
On-line Devices	1
Off-line Devices	0
Controller IP	0.0.0.0

An 'Apply' button is located at the bottom of the configuration table.

**Mode:** At the dropdown select Enable or Disable the DMS function globally. The default is Enabled.

**Controller Priority:** At the dropdown select a "Controller Priority" when enabling DMS:

**High:** High priority; this switch will become the "Controller" (Master) switch.

**Mid:** Mid-level priority.

**Low:** Low level priority (default).

**Non:** the switch will never become the Controller switch (default).

**Total Device:** Displays the number of IP devices that are detected and displayed in Topology view.

**On-Line Devices:** Displays the number of IP devices on-line in Topology view.

**Off-Line Devices:** Displays the number of IP devices off-line in the topology view.

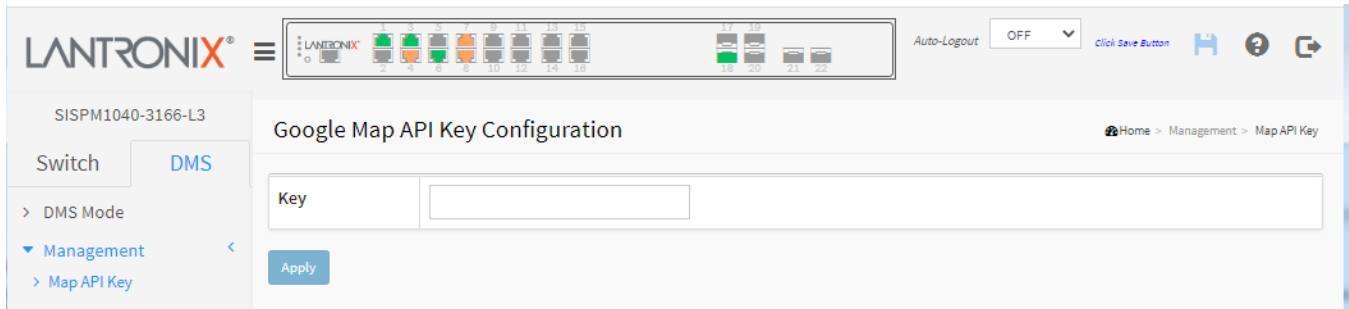
**Controller IP:** Displays the IP address of the Controller (Master) switch.

**Apply:** Click to save changes.

## DMS > Management > Map API Key

You will need a valid API key and a Google Cloud Platform billing account to access Google core product. If not, DMS Map View will not be able to load Google Maps correctly.

Visit the Google website below and follow the directions to get an API key:  
<https://developers.google.com/maps/documentation/directions/get-api-key>.



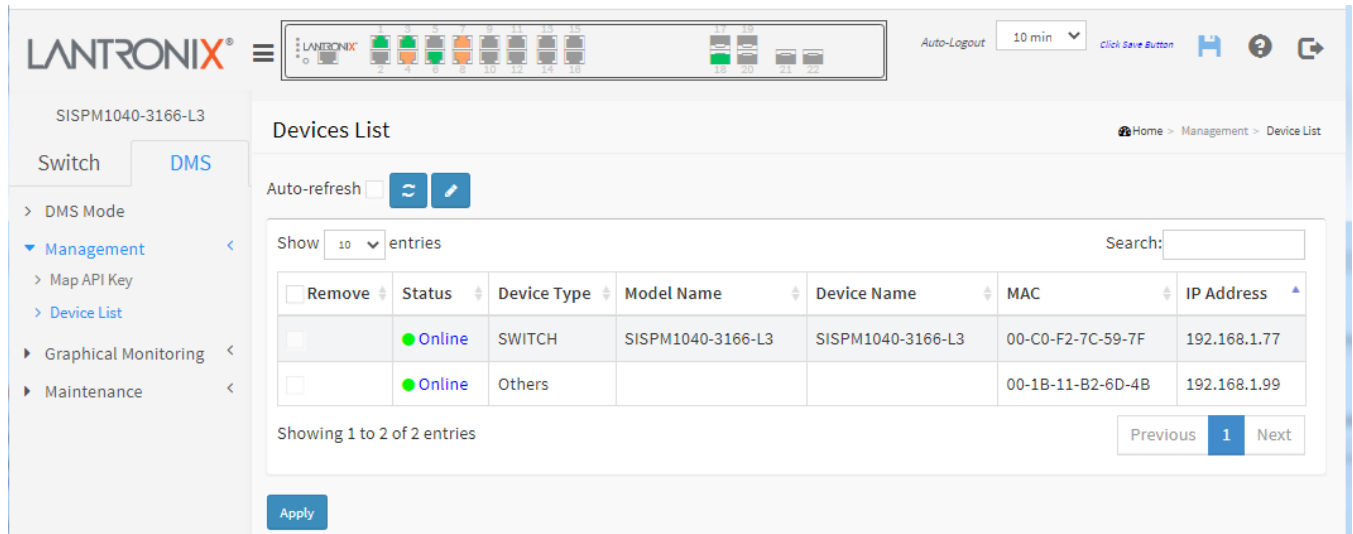
**Key:** Specify the Google API Key.

### Buttons

**Apply:** Click to save changes.

### DMS > Management > Device List

This page provides an overview of the devices list. It initially displays with seven columns:



**Remove:** Remove off-line device from the list.

**Status:** Device Online or Offline. You can click the linked text to display the Maintenance > Diagnostics page.

**Device Type:** The type of the network connectivity devices such as PC, SWITCH, AP, IP Cam, IP Phone, or Others.

**Model Name:** The model name of the network connectivity device.

**Device Name:** The device name of the network connectivity device.

**MAC:** The mac address of the device.

**IP Address:** The IP address of the network connectivity devices.

#### Buttons

**Auto-refresh:** Check this box to refresh the page automatically every 3 seconds.


**Refresh:** Refreshes the displayed table starting from the input fields.

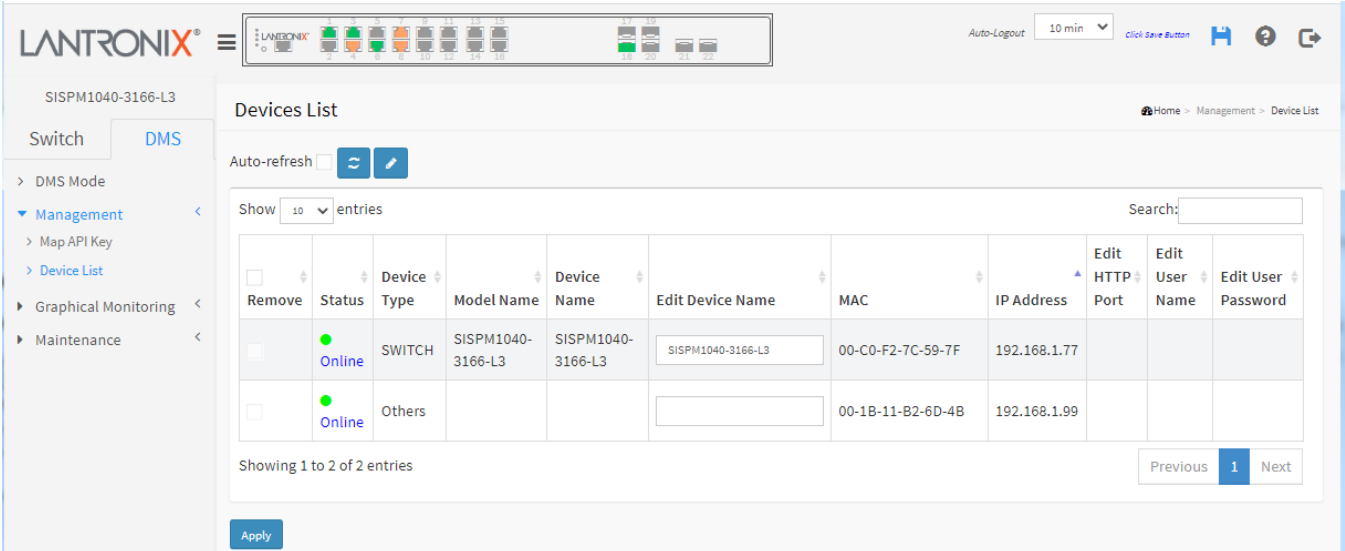


**Edit Device Name:** Add the input fields for editing the device names and the HTTP ports (see below).

**Apply:** Click to save changes.

**Devices List with added input columns:**

When you can click the  **Edit Device Name** button, the Devices List page displays with four additional columns:



The screenshot shows the Lantronix web interface for the device SISPM1040-3166-L3. The 'Devices List' page is displayed, featuring an 'Auto-refresh' checkbox and a refresh button. The table below shows two devices with their respective details and edit options.

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	SWITCH	SISPM1040-3166-L3	SISPM1040-3166-L3	<input type="text" value="SISPM1040-3166-L3"/>	00-C0-F2-7C-59-7F	192.168.1.77			
<input type="checkbox"/>	Online	Others			<input type="text"/>	00-1B-11-B2-6D-4B	192.168.1.99			

Showing 1 to 2 of 2 entries

Previous 1 Next

Apply

**Edit Device Name:** Entry field to edit a device's Name.

**Edit HTTP Port:** Entry field to edit a device's HTTP port number.

**Edit User Name:** Entry field to edit a device's user name.

**Edit User Password:** Entry field to edit a device's user password.

**Buttons:**

**Auto-refresh:** Check this box to refresh the page automatically every 3 seconds.

**Refresh:** Refreshes the displayed table starting from the input fields.

 **Edit Device Name:** Add the input fields for editing the device names and the http ports (see below).

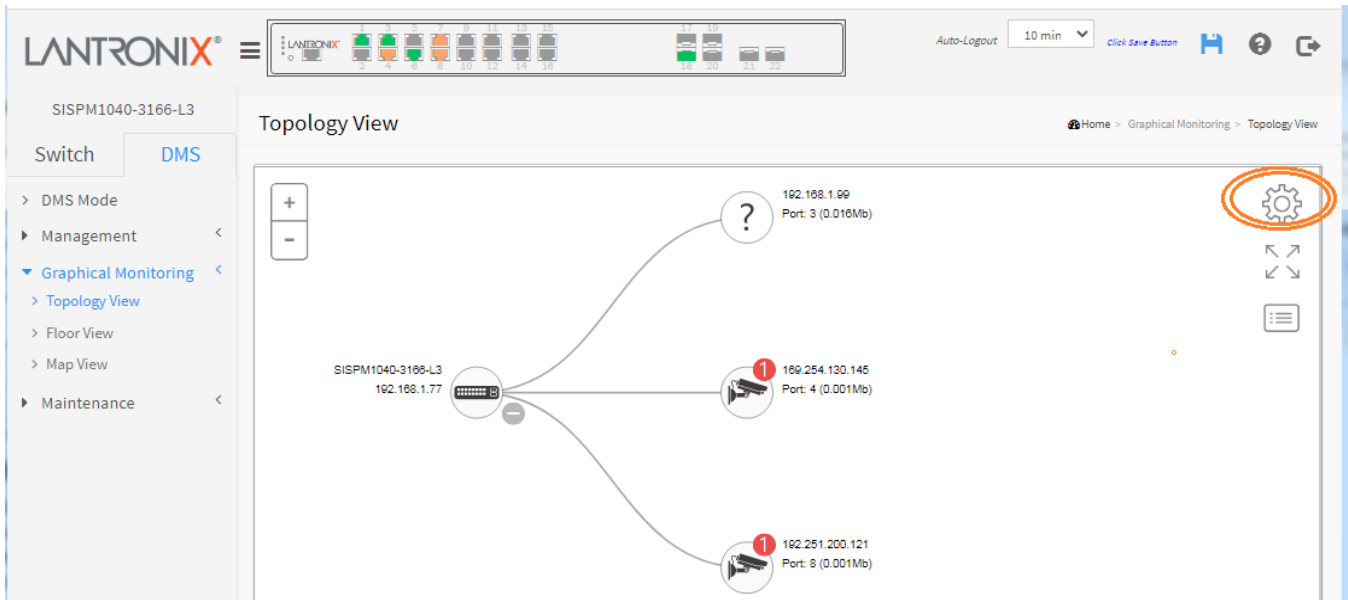
**Apply:** Click to save changes.



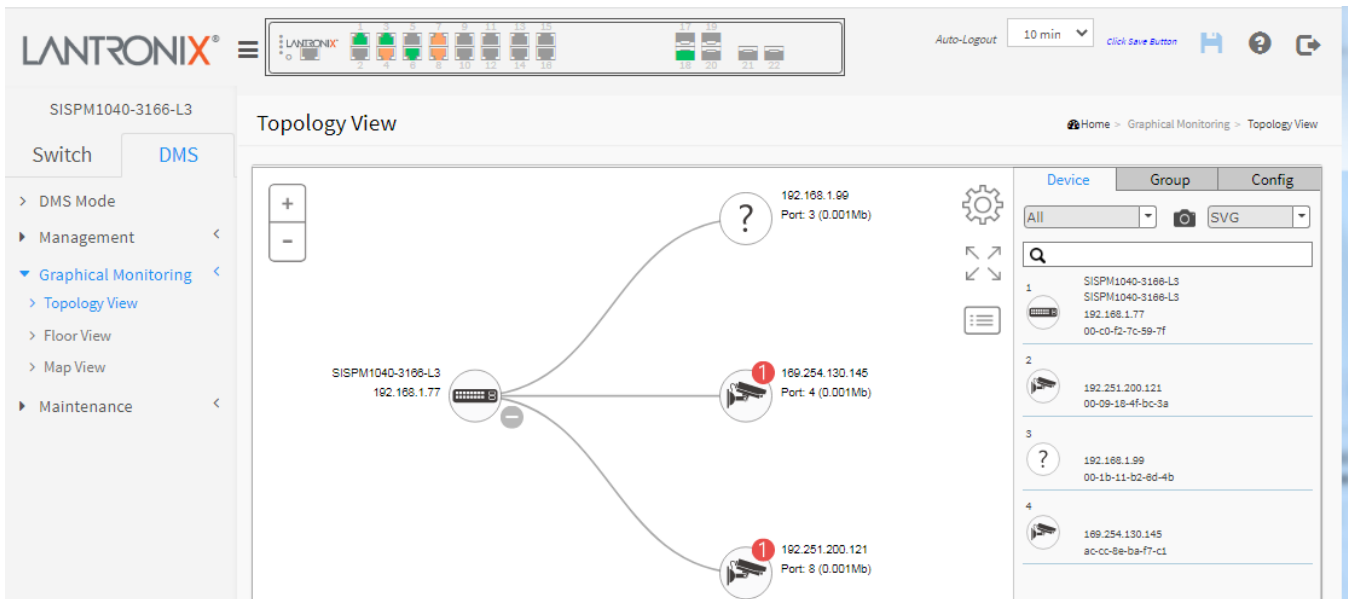
### DMS > Graphical Monitoring > Topology View

DMS can automatically discover all IP devices and display the devices by graphic networking topology view. You can manage and monitor them in the Topology View, such as to remotely diagnose the cable connection status, auto alarm notifications on critical events, and remotely reboot a PoE device. You can use the DMS platform to solve abnormal issues anytime and anywhere by tablet or smart phone and keep the network functioning smoothly.

Click Graphical Monitoring > Topology View to see a visual representation of the network topology:



Click the Setting icon (  ) to display additional right-hand menu items:





: Icon with plus and minus marks to let you zoom in and zoom out of Topology view. You can scroll up/down with mouse to achieve the same purpose.

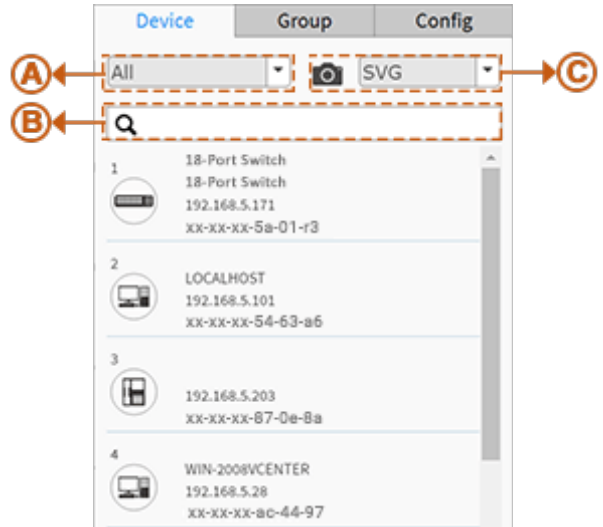


In the upper right corner, there is a "Setting" icon. When you click the icon, it will pop-up Device, Group, Config, export topology view and advanced search functions for the topology.

### Device Search Console

Functions:

- A** Filter devices by Device Type
- B** Search devices by key words full text search
- C** Save the whole View to SVG, PNG or PDF

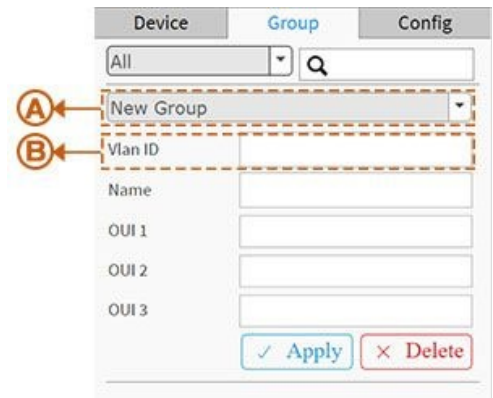


### Group Setting Console

- Uses MAC-based VLAN to isolate groups.
- One IP device only can join one VLAN group.

Functions:

- A** Group devices by filtering, searching, clicking device icons, or specifying OUI.
- B** Assign VLAN ID or Name to Group.



### System Setting Console

Functions:

- A** Shows how many IP devices are detected and displayed in Topology view.
- B** Shows the Master IP.
- C** Single Subnet: DMS is based on the Master switch's IP address. Here the subnet means "255.255.255.0"

Multiple Subnet: Provides 4 ranges for inputting manually. In this case, we suggest you adjust the switch subnet mask to "255.255.0.0" also to avoid IP devices that can't be recognized.

Device	Group	Config
Total Device	20	
Controller IP	192.168.5.171	
IP Range	Multiple Subnet	
Range 1	0.0.0.0	0.0.0.0
Range 2	0.0.0.0	0.0.0.0
Range 3	0.0.0.0	0.0.0.0
Range 4	0.0.0.0	0.0.0.0

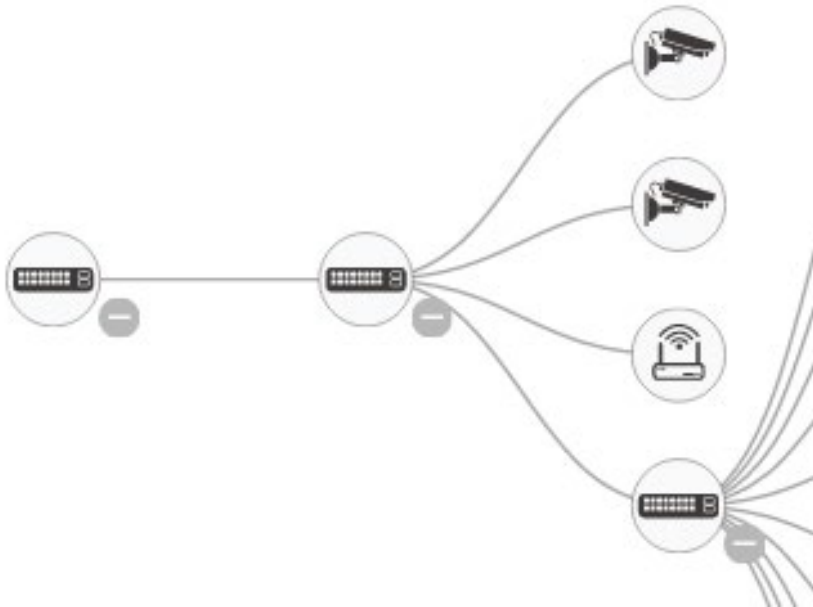


**Icon with screen view type:** Click it to change to Full Screen View of Topology or return to the Normal View.



**Icon with information list:** Select what kind of information should be shown on the topology view of each device. Up to three items can be selected.

### Device Tree View



## Device Categories



The device is a Switch.



The device is a PC.



The device is an IP Camera.



The device is an IP Phone.



The device is an Access Point.



The device is a Router.



Icon with question mark: The IP device is detected by DMS, but the device type can't be recognized, and will be classified as an "Unknown" device type.

## Device Status



**Icon with black mark:** Device link up. User can select function and check issues.










**Icon with red mark:** Device link down. User can diagnose the link status.



**Icon with number:** An event has occurred (e.g., Device Off-line, IP Duplicate, etc.) on the IP device. Click on the device icon to check Events in Notification.

## Device Consoles

Left-click any device icon to display the device consoles for further actions.

Test		×
Device Type	IP Cam	
Device Name	<input type="text" value="Test"/>	
Model Name	Test	
Mac Address	xx-xx-xx-02-26-48	
IP Address	192.168.0.103	
Http Port	<input type="text" value="80"/>	
PoE Used	2.8 W	
		
Login	Diagnostics	Streaming
		
Reboot		
		
Dashboard	Notification	Monitor

**Dashboard Console:** displays device info and related actions for the device.

Different device types support different function:

If an IP device is recognized as DMS switch, it will support "Upgrade" and "Find Switch" function.

If an IP device is recognized as PoE device, it will support more "Reboot" function in addition to "Upgrade".

If an IP device is recognized as IP Cam via ONVIF protocol, it will support "Streaming" function.

**Device Type:** Can be displayed automatically. If an unknown type is detected, you can still select type from a pre-defined list. Device Types include **PC** (General PC), **IP Camera** (General IP Cam), **IP Phone** (General IP Phone, Cisco SPA303), **AP** (General AP), and **Others** (Mobile Device, General Switch, Internet Gateway, IP PBX, NAS, Printer, NVR, VMS, Unknown Device).

**Device Name:** Create your own Device Name or alias for easy management such as, 1F\_Lobby\_Cam1.

**Model Name, MAC Address, IP Address, Subnet Mask, Gateway, PoE Supply and PoE Used** are displayed automatically by DMS.

**HTTP Port:** Re-assign HTTP port number to the device for better security.



Login

**Login:** Click the Login Action Icon to log in the device via HTTP for further configuration or status monitoring.



Upgrade

**Upgrade:** Click it to upgrade software version.



Find Switch

**Find Switch:** When this feature is activated, the switch LEDs will all flicker for 15 seconds.



**Diagnostics** **Diagnostics:** Click Diagnostic Action Icon to perform the cable diagnostics, to exam where the broken cable is, and check if the device connection is alive or not by ping.

- **Cable Status:**
  - **Green icon:** Cable is connected correctly.
  - **Red icon:** Cable is not connected correctly. User can check the distance info (XX meters) to identify the broken cable location.
- **Connection:**
  - **Green icon:** Device is pinged correctly.
  - **Red icon:** Device is not transmitted /receiving data correctly. Which means it might not be pinged successfully.



**Reboot** **Reboot:** Click Reboot Action Icon to reboot the device remotely so as recover the device back to its normal operation.



**Streaming** **Streaming:** Click Streaming Action Icon to display the video images streaming if the device supports this feature.



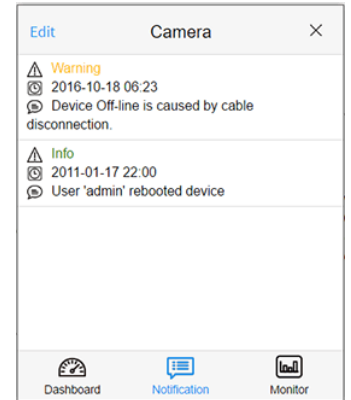
**Parent Node** **Parent Node:** When DMS switch detects more than two IP devices from the same port, switch can't resolve this IP device's layout, instead, it will show a blank node to present this situation. User can use "Parent Node" function to adjust layout in Dashboard.

**Notification Console:** Displays alarms and logs triggered by events. For example:

**Warning:** <date> Device Off-line is caused by cable disconnection.

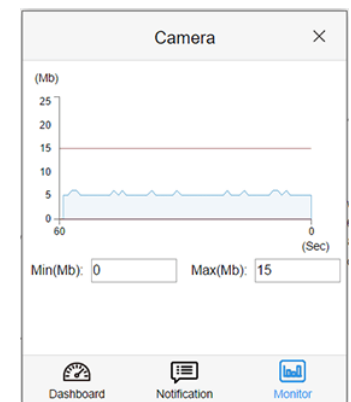
**Info** <date> User 'admin' rebooted device

No Message




**Monitor Console:** It displays the traffics for device health check purpose.

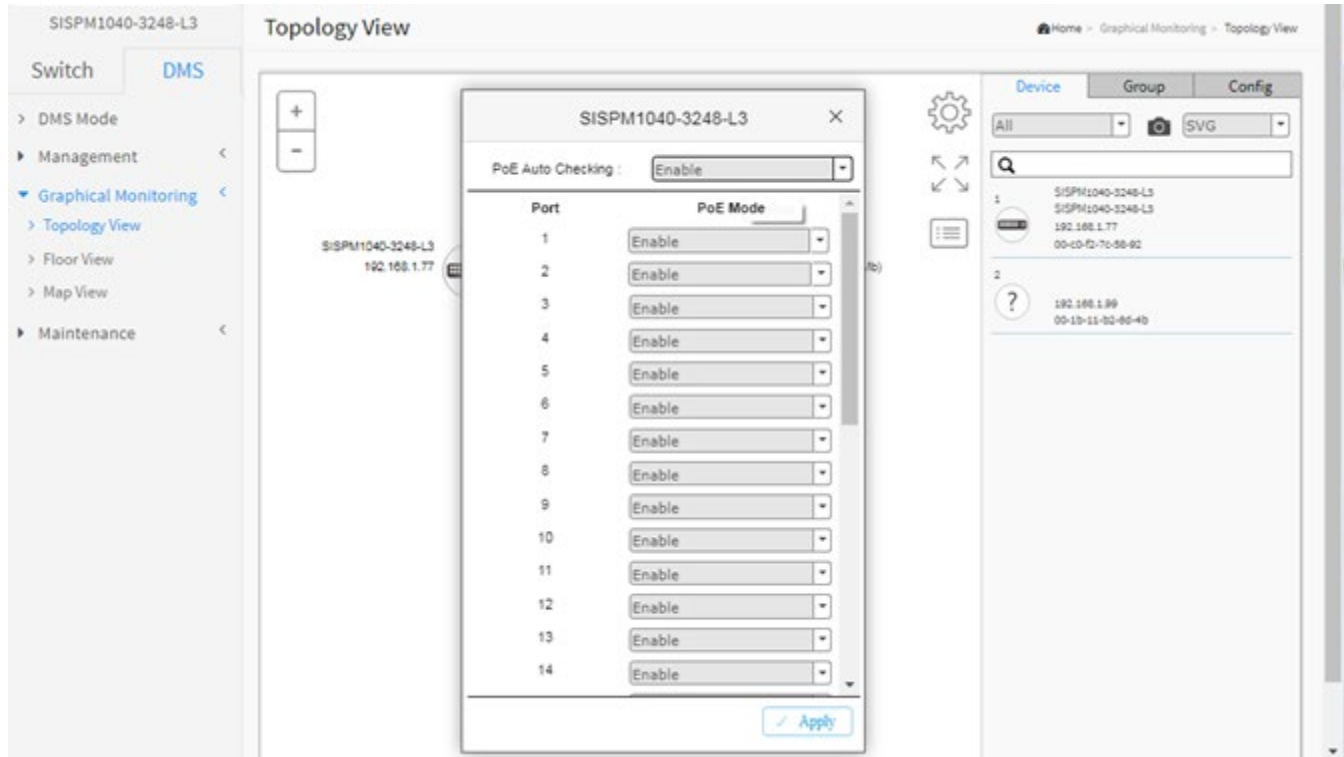
- For each IP device except DMS switches, you can set a threshold of throughput for IP devices, and get notification when throughput is lower or higher than settings.
- If both values are "0", it means the function is disabled.
- Polling interval is 1 second; when the page is closed, the Polling interval will change to around 5 seconds.



### PoE Auto Checking “AutoFill” Feature

When you enable Auto power reset (PoE auto checking) in DMS, the IP addresses of the connected devices are automatically filled on the Auto Power Reset configuration page.

1. Configure the “PoE Auto Checking” parameter at Switch > PoE Management > PoE Auto Checking. The default value of the “Failure Action” parameter is “Reboot Remote PD”. Note that “PoE Auto Checking” is called “PoE Auto Power Reset” in earlier firmware versions.
2. Configure PoE parameters at DMS > Graphical Monitoring > Topology View. Left click on the switch icon to display its device configuration popup. Click the PoE Config (  ) icon to display the PoE Auto Checking pane:

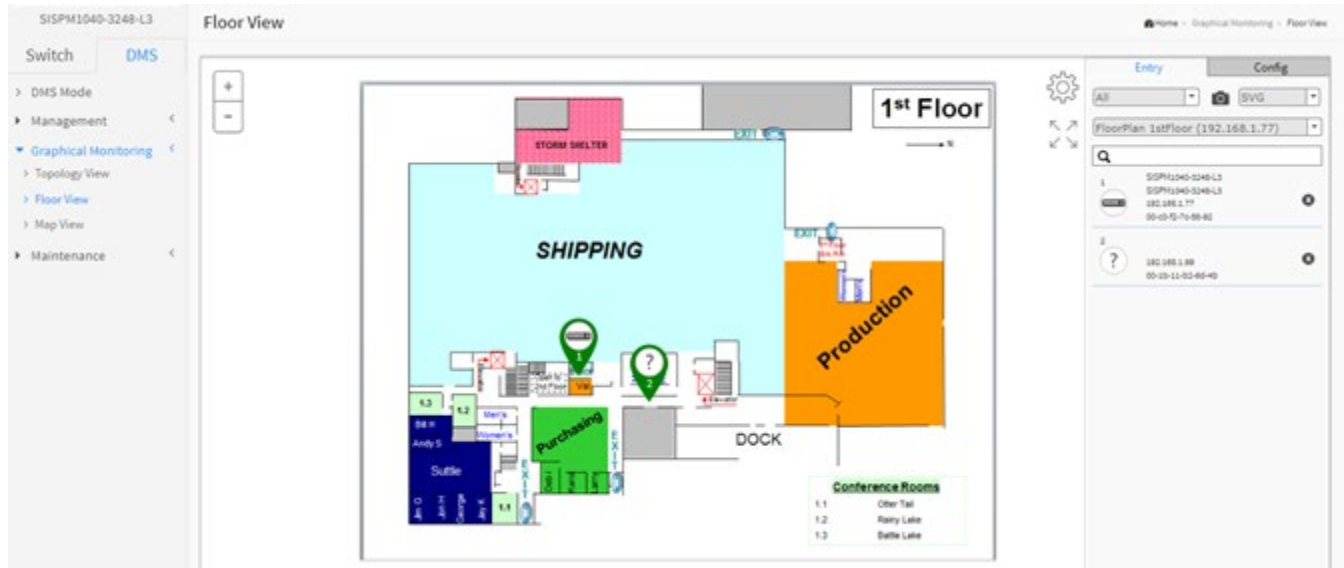




### DMS > Graphical Monitoring > Floor View

This page displays the graphical image created at DMS > Maintenance > Floor Image. Initially, no Floor View images are displayed. Go to [DMS > Maintenance > Floor Image](#) on page 465 to upload floor images.

The Floor View lets you easily plan IP devices installation locations by dragging the uploaded floor images into place.



Icon with plus and minus marks: Zoom in and zoom out the floor view, user can scroll up/down with mouse to achieve the same purpose.



There is a "Setting icon" in the upper right corner. When you click the icon, it will pop-up Device, Config, export floor view and advanced search functions for the device.

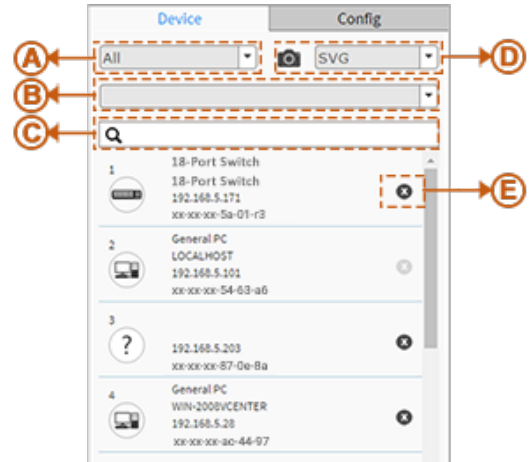


Icon with screen view type: Click it to change to Full Screen view of Floor or return to the Normal View.

### Device Search Console

**Functions:**

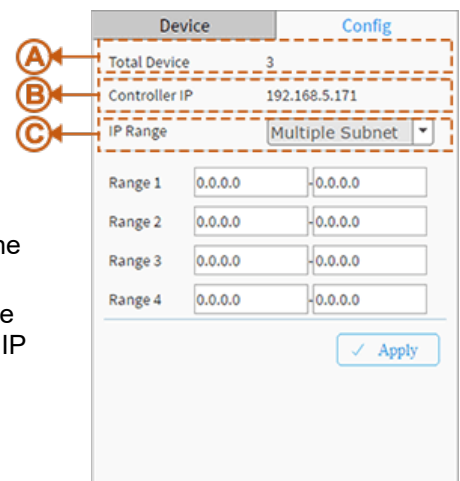
- A. Filter devices by Device Type
- B. Select floor images
- C. Search devices by key words full text search
- D. Save the whole View to SVG, PNG or PDF
- E. Remove a device from all floor view images



### System Setting Console

**Functions:**

- A. Shows how many IP devices are detected and displayed in the topology view.
- B. Shows the Master switch's IP address.
- C. Single Subnet: DMS will base on the master switch's IP address. Here the subnet means "255.255.255.0".  
Multiple Subnet: To provide 4 ranges for inputting manually. (In the case, we suggest you adjust the switch's subnet mask to "255.255.0.0" also to avoid IP devices that can't be recognized.)



### Floor View

- Anchor devices onto Floor Maps
- Find device location instantly
- 10 Maps can be stored per Switch
- IP Surveillance/VoIP/WiFi applications
- Other features same as Topology View
- To place and remove a device icon:
  - Select a device and click its icon from the device list.
  - The device icon will show on the floor image's default location.
  - Click and hold left mouse to drag-and-drop the icon to the correct location on the Floor View.
  - Click cross sign on the right side of device icon to remove a device from all Floor View images.

### Device Status



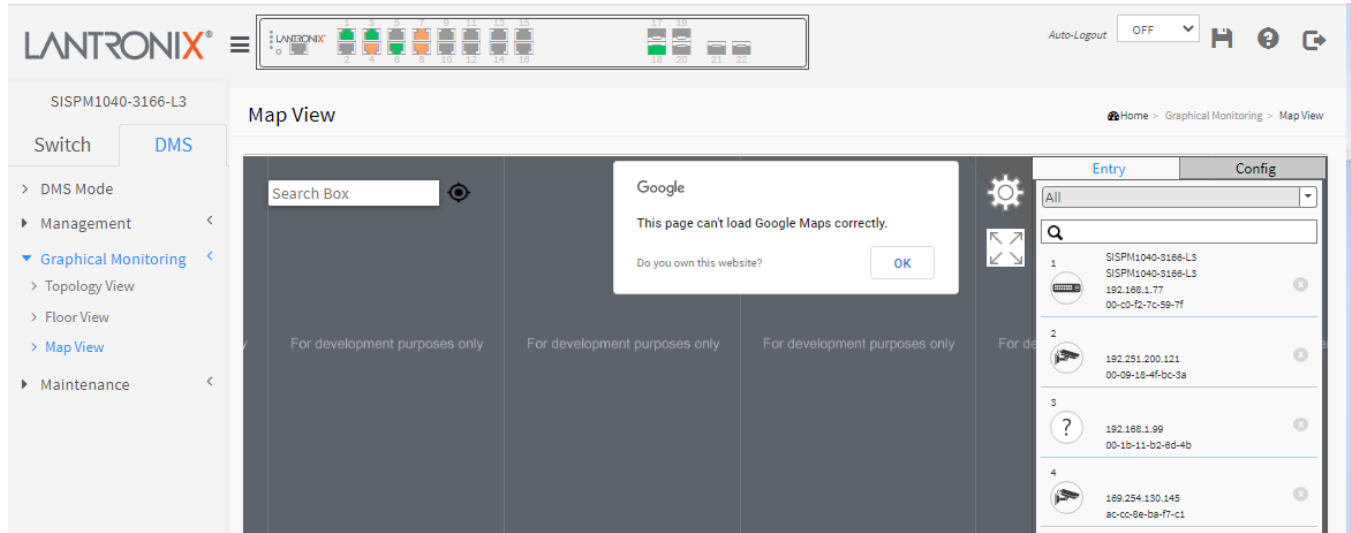
Icon with black mark: Device link up. User can select function and check issues.




Icon with red mark: Device link down. User can diagnose the link status.

## DMS > Graphical Monitoring > Map View

This page helps you find the location of devices even when they are installed in a different building. You can place a device icon on the Map View and navigate using Google Maps. You need a valid API key and a Google Cloud Platform billing account to access a Google core product. If not, DMS Map View will not be able to load Google Maps correctly. See [DMS > Management > Map API Key](#) on page 450.

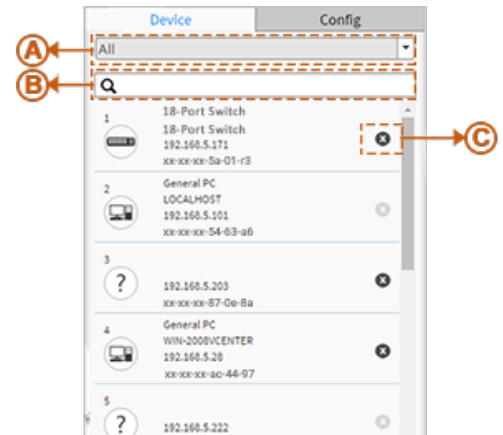


 There is a "Settings icon in the upper right corner. When you click the icon, it will pop-up Device, Config, export floor view and advanced search functions for the device.

### 1. Device Search Console

**Function:**

- A. Filter devices by Device Type
- B. Search devices by key words full text search
- C. Remove a device from Map view



### 2. System Setting Console

**Function:**

- A. Shows how many IP devices are detected and displayed in the topology view.

B. Shows the Master switch's IP address.

C. Single Subnet: DMS will base on the master switch's IP address. Here the subnet means "255.255.255.0".

Multiple Subnet: To provide 4 ranges for inputting manually. (In the case, we will suggest user to adjust switch's subnet mask to "255.255.0.0" also to avoid IP devices can't be recognized.)



Icon with screen view type: Click it to change to Full Screen View of the Map View page or return to the Normal View.

### Map View

- Anchor Devices onto Google Maps.
- Find Devices Instantly from Map View.
- On-Line Search Company/Address.
- Outdoor IP Cam/WiFi Applications.
- Other Features same as Topology View
- To place and remove a device icon
  - Select a device and click its icon from the device list.
  - The device icon will show on the map's default location.
  - Click and hold left mouse to drag-and-drop the icon to the correct location on the Map View.
  - Click the cross sign on the right side of device icon to remove a device from Map View.

### Device Status



Icon with black mark: Device link up. You can select functions and check issues.



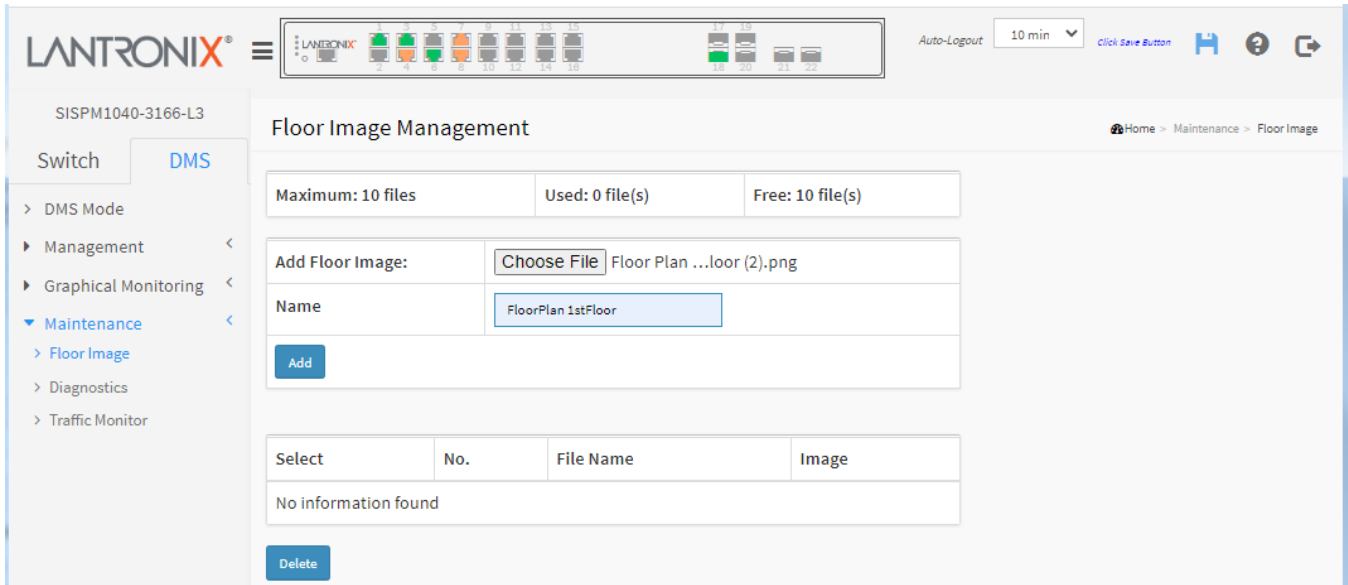
Icon with red mark: Device link down. You can diagnose the link status.

**Message:** *This page can't load Google Maps correctly.*

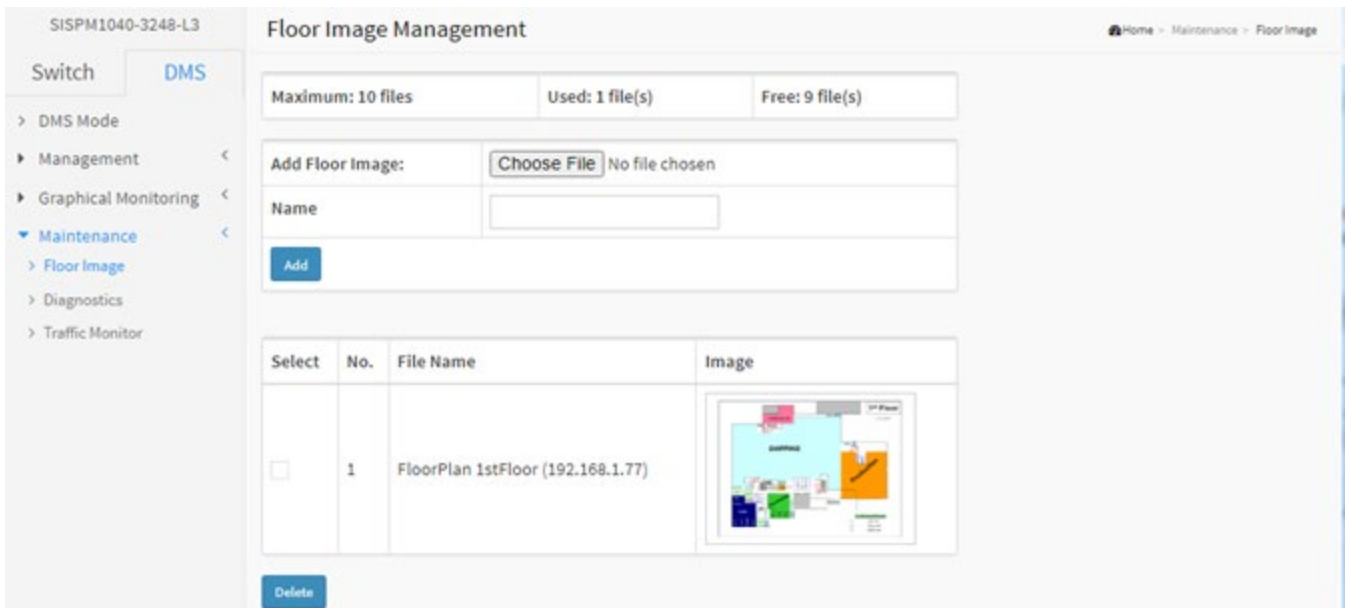
Recovery: See DMS > Management > Map API Key on page [450](#).

### DMS > Maintenance > Floor Image

This page lets you upload and manage floor map images. You can upload up to 20 JPEG or PNG images, each a maximum of 256KB in size.



1. At the default Floor Image Management page click the Choose File icon.
2. Navigate to and select a JPEG or PNG image.
3. Enter a Name and click the Add button to display the selected image:



**Select** : Check the checkbox to select an image from the list.

**No.:** Floor Image instance number (maximum 10 image files).

**File Name** : Displays the file name information (e.g., *Floor Plan - 1st Floor (192.168.1.77)*).

**Image:** Displays a thumbnail of the floor image.

### Buttons

**Add:** Click Add to upload. When done, a snapshot will be available on screen.

**Delete:** If you need to remove an existing floor map, select its checkbox and click Delete to remove.

**Messages:** *Only jpg, png are allowed* displays if you selected a file type other than JPG or PNG. Click OK to clear the message and select a PNG or JPG file.

### Example:

SISPM1040-3248-L3

Home > Maintenance > FloorImage

Switch **DMS**

> DMS Mode

> Management <

> Graphical Monitoring <

> Maintenance <

> Floor Image

> Diagnostics




> Traffic Monitor

Floor Image Management

Maximum: 10 files    Used: 3 file(s)    Free: 7 file(s)

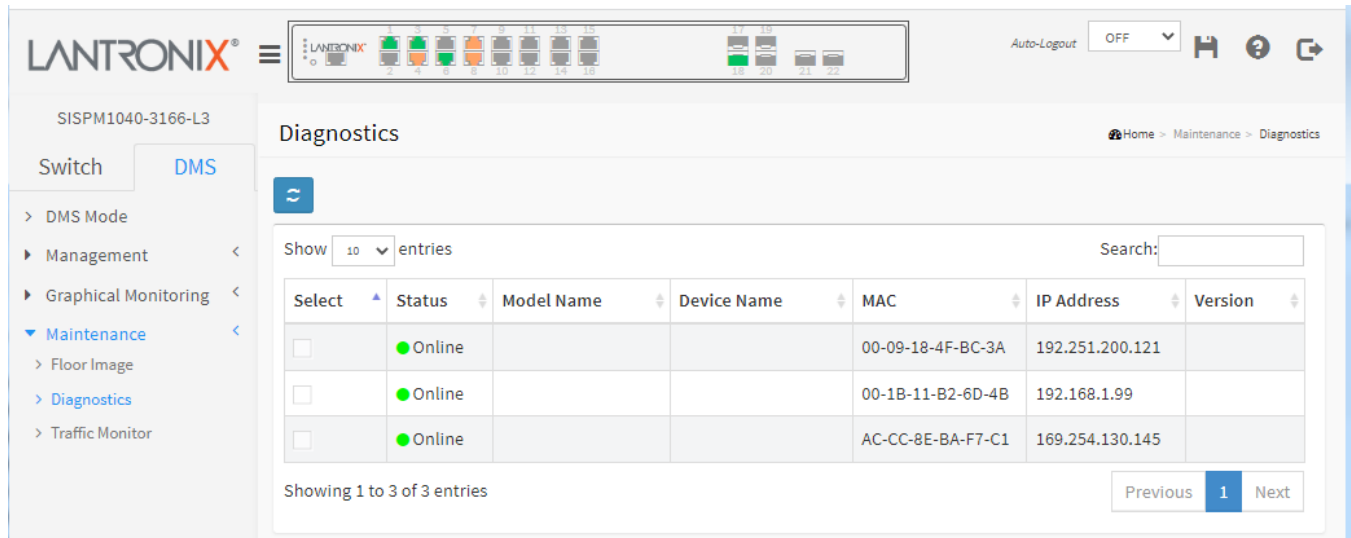
Add Floor Image:  No file chosen

Name

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)	

## DMS > Maintenance > Diagnostics

This page lets you run a diagnostic test on a selected device.



**Select:** Select an on-line device from the list. The diagnostic test starts.

**Status:** Device Online or Offline.

**Model Name:** The model name of the network connectivity devices.

**Device Name:** The device name of the network connectivity devices.

**MAC:** The mac address of the device.

**IP Address:** The IP address of the network connectivity devices.

**Version:** The Version of the network connectivity devices.

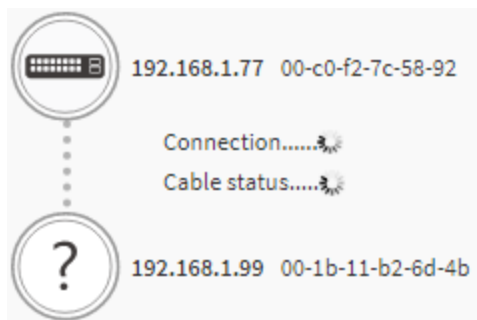
### Buttons

**Refresh:** Refreshes the displayed table starting from the input fields.

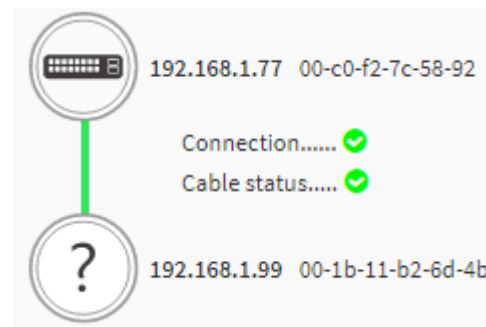
**Show x entries:** At the dropdown select the number of devices to display per page.

**Search:** Enter a key word to search for.

**Another Try:** When a diagnostic test completes, click the button to clear the page and run another diagnostic test.



**Diagnostic In process**



**Diagnostic Completed**

### Example

The screenshot shows the Lantronix web interface for a switch (SISPM1040-3166-L3) in DMS mode. The 'Diagnostics' page is active, displaying a table of device entries. The table has columns for Select, Status, Model Name, Device Name, MAC, IP Address, and Version. One entry is shown as 'Online' with IP 192.168.1.99 and MAC 00-1B-11-B2-6D-4B. Below the table, there are two circular icons representing device status: one with a keyboard icon and one with a question mark icon, each with associated IP and MAC addresses and connection/cable status indicators.

Select	Status	Model Name	Device Name	MAC	IP Address	Version
<input checked="" type="checkbox"/>	Online			00-1B-11-B2-6D-4B	192.168.1.99	

Showing 1 to 3 of 3 entries

192.168.1.77 00-c0-f2-7c-59-7f  
Connection.....  
Cable status.....

192.168.1.99 00-1b-11-b2-6d-4b

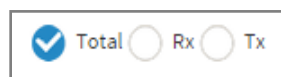


### DMS > Maintenance > Traffic Monitor

This page displays a visual chart of network traffic of all the devices. Numbers are shown in Mbit/s.

To view the traffic of all the ports or just a specific port; click on a specific port on the traffic chart to reveal its traffic during the day.

You can select to display a summary of a day's or a week's traffic by selecting the check circle on top. The same applies to the selection of Rx Tx traffic. A single port's traffic is shown at the lower half of the screen.



**Total / Rx / Tx:** Select the set of data to be displayed. The default is Total.



**< yy/mm/dd >:** Select the date of data displayed.

**Day / Week:** Select a day's worth of data or a week's worth of data to be displayed.

**Device List:** Displays the set of discovered devices.

**Throughput:** Vertical axis shows the device throughput (e.g., 0 M-18000 M or 0 M-1200 M).

**Port:** Horizontal axis shows the switch port numbers.

**Time (Hour):** Horizontal axis shows the time elapsed in hours (0-23).

Hover the mouse cursor over a column in the table to display its specific parameters:




**Message:** “Traffic Monitor feature is only available on master switch” added at FW v8.40.1523.

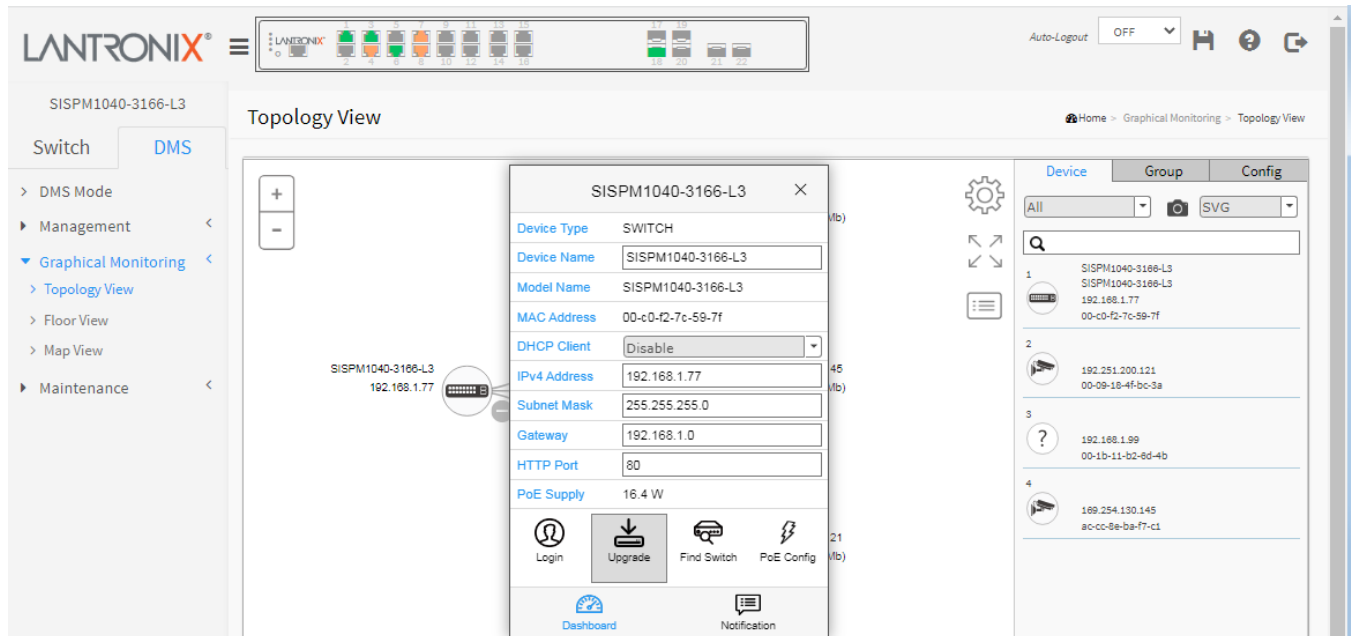
Meaning: You clicked on “Traffic Monitor” at DMS > Traffic Monitor, but this switch is not the DMS Controller (Master) Switch.

Recovery: Either make this switch the DMS Controller (Master) Switch or use the designated DMS Controller (Master) Switch for traffic monitoring. See “[DMS Information page](#)” on page 449.

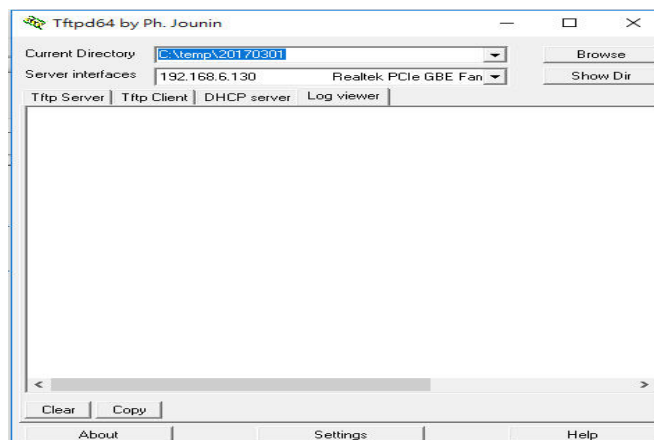
## DMS Firmware Upgrade Procedure

To upgrade a device's firmware via DMS:

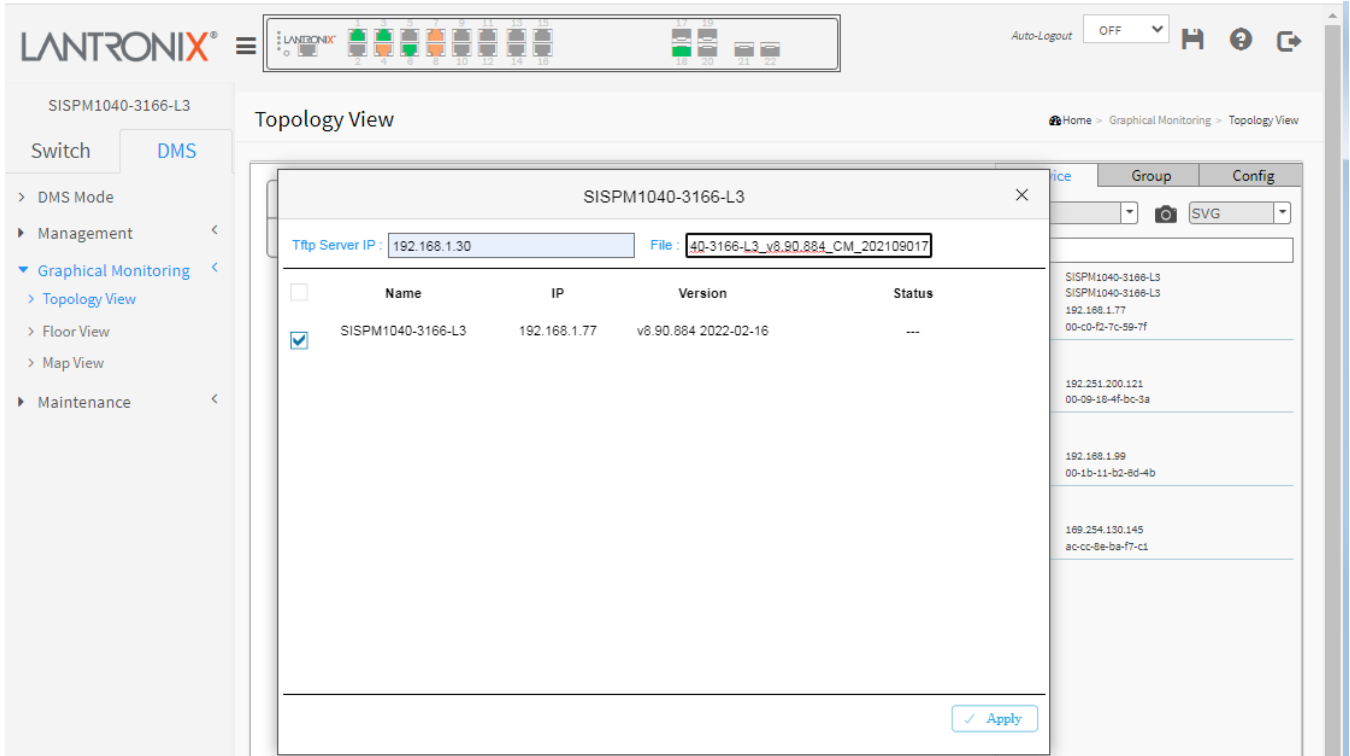
1. Navigate to the DMS > Graphical Monitoring > Topology View menu path.
2. Click the  button to display the right pane menu tabs (Device, Group, and Config).
3. Connect all switches and make sure DMS is working.
  - Set all switches with different IP addresses and in the same IP segment.
  - Make sure gateway IP address is configured.
4. Left-click the desired device icon to display the options:



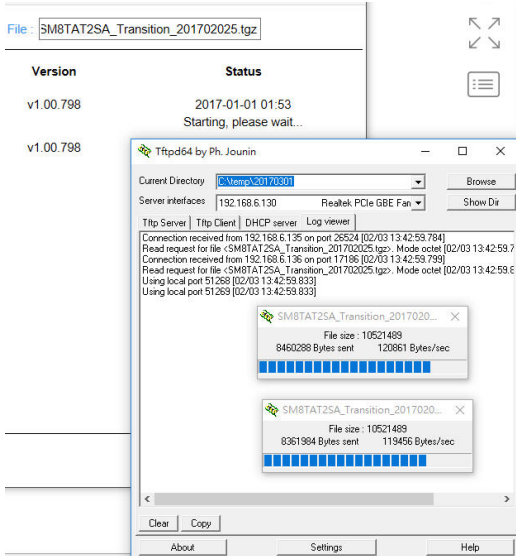
5. Enable the TFTP server and set the correct image path.



6. Click the switch icon, and then click the “Upgrade” button in the Dashboard.
7. Enter the TFTP server IP address and FW file name, and select the switch on which you want to upgrade the FW.



- 8. Click “Apply” to start the FW upgrade and save to Running-config.
- 9. Observe the upgrade status until completion.



### Messages

*Starting, please wait...*

*Error : Firmware download fail*

## DMS Troubleshooting

**Problem:** The switch lists itself as the only device in Topology View of DMS.

**Problem:** In DMS, the Local image shows the IP address of another switch.

**Description:** The switch is listed as only device in DMS Topology View in DMS; all devices are listed in DMS device list. This is usually because the switch's gateway is not configured appropriately.

**Resolution:** An IP Route must be configured manually. For example, a switch IP address of 192.168.1.77 should have the following IP route configured: ip route 0.0.0.0 0.0.0.0 192.168.1.x. Without the IP route configured, you may be unable to view all devices on the network in DMS.

1. Go to DMS > Management > DMS Mode to check if the controller IP is correct.
2. Verify that the gateway of this switch is correctly configured.
3. Verify that all connected devices are displayed in DMS Topology View.

**Problem:** DMS Connectivity diagnostics fails to ICMP reachable device.

**Description:** DMS displays a device which is reachable via ICMP ping as failing the connection status in diagnostics. Cable status displays as OK.

**Resolution:** Contact Technical Support.

**Problem:** DMS will discover the device type, name and model of some cameras and hosts but others are displayed as *Unknown*.

**Description:** When a device is detected by DMS, the device's information (such as type, model name...etc.) can be recognized via LLDP (e.g. Switch), UPnP (e.g. AP), **ONVIF** (e.g. IP cam), NBNS (e.g. PC) packets if the device supports these protocols. So if the device display as *Unknown*, that means this device do not issue above mentioned protocol for DMS to recognize.

**Resolution:** You can manually assign and configure the device type and name for the unknown devices. See the Topology View > Dashboard or the Topology View section.

**Message:** This page can't load Google Maps correctly. See DMS > Graphical Monitoring > Map View on page 463 above.

The screenshot displays the Lantronix web management interface. At the top, the 'LANTRONIX' logo is visible on the left, and 'Auto-Logout OFF' is on the right. The main navigation menu on the left includes 'Switch', 'DMS', 'DMS Mode', 'Management', 'Graphical Monitoring', and 'Topology View'. The 'DMS' section is currently active. The central area is titled 'Map View' and contains a search box and a Google Maps error message: 'This page can't load Google Maps correctly. Do you own this website? OK'. On the right side, there is a table with columns 'Entry' and 'Config'. The table contains one entry for 'SISPM1040-3166-L3' with IP address '192.168.1.77'.

## Appendix A – DHCP Per Port Configuration

You can configure DHCP Per Port via the Web UI as described below.

### *DHCP IP per Port*

This function lets you assign a static IP address from a DHCP pool to a switch port such that it will always be assigned that specific IP address.

The IP address would be configured in the Interface Config settings.

Note that this is binding an IP address to an interface, not to a MAC address (the typical binding method used on this and most other switches).

### *Configure DHCP Per Port via the Web UI*

The switch's DHCP server assigns IP addresses. Clients get IP addresses in sequence and the switch assigns IP addresses on a per-port basis starting from the configured IP range. For example, if the IP address range is configured as 192.168.10.20 - 192.168.10.37 with one DHCP device connected to port 1, the client will always get IP address 192.168.10.20, then port 3 is always distributed IP address 192.168.10.22, even if port 2 is an empty port (because port 2 is always distributed IP address 192.168.10.21).

The switch does not allow a DHCP per Port pool to include the switch's address.

IP address assigned range and VLAN 1 should stay in the same subnet mask.

The configurable IP address range is allowed to configure over 18 IP addresses, but the switch always assigns one IP address per port connecting device.

The DHCP Per Port function is only supported on VLAN 1.

When the DHCP Per Port function is enabled, the switch software will automatically create the related DHCP pool named "DHCP\_Per\_Port".

Once the DHCP Per Port function is enabled on one switch, IPv4 DHCP client at VLAN1 mode (DMS DHCP mode), DHCP server mode are all limited to be enabled at the same time (an error message displays if attempted).

If the DHCP server pool has been configured, once you enable the DHCP Per Port function, then that DHCP server pool configuration will be overwritten.

Only for VLAN 1, clients issued DHCP packets will not be broadcast/forwarded to other ports. DHCP packets in others VLANs will be broadcast/forwarded to other ports.

The DHCP Per Port function allows the switch to connect only one DHCP client device.

DHCP-Per-Port is configured entirely on the **Switch > Configuration > System > IP** page, IP Interfaces window.

The feature is enabled here and an IP range (pool) is entered. The "automatic" results of this action can be displayed in:

- **Switch > Configuration > System > DHCP > Server > Mode** (Global Mode – Enabled, VLAN Mode - VLAN 1 created)
- **Switch > Configuration > System > DHCP > Excluded** (Excluded range created based on range entered)
- **Switch > Configuration > System > DHCP > Pool** (Pool "DHCP\_Per\_Port" created based on range entered)

Actual DHCP operation is monitored as normal under **System > Monitor > DHCP**.

The DHCP Per Port pages and parameters are described below.

## DHCP Per Port Mode Configuration

The DHCP Per Port function lets you assign an IP address based on the switch port the device is connected to. This will speed up installation of IP cameras, as the cameras can be configured after they are on the network. The DHCP Per Port assignment lets you know which IP was assigned to which camera.

**Note:** to prevent IP conflict, each switch can be allocated a different IP range.

To configure DHCP Per Port via the Web UI, navigate to the **Configuration > System > IP** menu path.

The screenshot shows the 'IP Configuration' page in the Lantronix Web UI. The left sidebar has 'Switch' selected, and 'Configuration' is expanded to show 'System' and 'IP'. The main content area is titled 'IP Configuration' and includes the following sections:

- Mode:** Host
- DNS Server 1-4:** Each set to 'Configured IPv4 or IPv6' with a default IP of 8.8.8.8.
- DNS Proxy:** Unchecked.
- IP Interfaces:**
  - DHCP Per Port Mode:** Enabled
  - IP:** 192.168.1.1 - 192.168.1.8
- Table:**

Delete	VLAN	IPv4 DHCP		IPv4		DHCPv6		IPv6			
		Enable	Fallback	Current Lease	Address	Mask Length	Enable	Rapid Commit	Current Lease	Address	Mask Length
<input type="checkbox"/>	1	<input type="checkbox"/>	0		192.168.1.77	24	<input type="checkbox"/>	<input type="checkbox"/>			
- Link-Local Address binding interface:** VLAN 1
- Gateway Address binding interface:** VLAN 1
- IP Routes:**

Delete	Network	Mask Length	Gateway	Next Hop VLAN
<input type="checkbox"/>	0.0.0.0	0	192.168.1.254	0
	169.254.0.0	16	192.168.1.77	0
	192.168.1.0	24	192.168.1.77	0

**Parameter descriptions:** The DHCP Per Port parameters and buttons are described below.

**DHCP Per Port Mode:** at the dropdown select **Enable** or **Disable** the DHCP Per Port function globally. The default is **Disabled**.

**IP:** enter the IPv4 IP address range to be used when the DHCP Per Port function is enabled (e.g., 192.168.10.20 - 192.168.10.37). The DHCP Per Port IP range must be within the interface subnet. Note that DHCP Per Port with IPv6 is not supported at this time. The DHCP Per Port IP range must equal the switch port number excluding uplink ports (e.g., 16).

**Apply:** Click to save changes to the entries. If the entries are valid, the webpage message “Update success!” displays. Click the **OK** button to clear the message. If any entries are invalid, an error message displays. Click the **OK** button to clear the message and enter valid values, then click the **Apply** button again.

**Reset:** Click to undo any changes made locally and revert to previously saved values.

To monitor DHCP Per Port status, navigate to the **Monitor > System > IP Status** menu path.

The screenshot shows the 'IP Status' page in the Lantronix web interface. The left sidebar is expanded to 'Switch', and 'IP Status' is selected. The main content area displays the following information:

**IP Interfaces**

Interface	Type	Address	Status
VLAN1	LINK	00-c0-f2-4f-73-d0	<UP BROADCAST RUNNING MULTICAST>
VLAN1	IPv4	192.168.1.77/24	
VLAN1	IPv4	169.254.155.234/16	
VLAN1	IPv6	fe80::2c0:f2ff:fe4f:73d0/64	
VLAN4096	LINK	00-c0-f2-4f-73-d0	<BROADCAST MULTICAST>
VLAN4097	LINK	00-c0-f2-4f-73-d0	<BROADCAST MULTICAST>

**IP Routes**

Network	Gateway	Status
0.0.0.0/0	192.168.1.254	<UP GATEWAY HW_RT>
127.0.0.0/8	127.0.0.1	<UP>
127.0.0.1/32	127.0.0.1	<UP HOST>
169.254.0.0/16	VLAN1	<UP HW_RT>
192.168.1.0/24	VLAN1	<UP HW_RT>
224.0.0.0/4	127.0.0.1	<UP>
::1/128	::1	<UP HOST>

**Neighbour cache**

IP Address	Link Address
192.168.1.77	VLAN1:00-c0-f2-4f-73-d0
192.168.1.99	VLAN1:00-1b-11-b2-6d-4b
fe80::2c0:f2ff:fe4f:73d0	VLAN1:00-c0-f2-4f-73-d0

**DNS Server**

Type	IP Address	Interface
Static	8.8.8.8	



**Web UI Messages****Message:** *Interface xx not using DHCP***Meaning:** The Interface being configured does not have DHCP enabled and configured.**Recovery:** **1.** Click the **OK** button to clear the webpage message. **2.** Enable and configure DHCP for the interface being configured.**Message:** *'DHCP Per Port IP range (192-168-1.80 - 192-168-1.99) is not equal to switch port number excluding uplink ports (10)***Meaning:** The IPv4 IP address range entered for the DHCP Per Port function was invalid.**Recovery:** **1.** Click the **OK** button to clear the webpage message. **2.** Re-configure DHCP Per Port. See the DHCP Per Port Mode Configuration section above.**Message:** *'DHCP Per Port IP range (192-168-1.70 - 192-168-1.85) includes interface IP Address (192.168.1.77)***Meaning:** The IPv4 IP address range entered for the DHCP Per Port function was invalid.**Recovery:** **1.** Click the **OK** button to clear the webpage message. **2.** Re-configure DHCP Per Port.

See the DHCP Per Port Mode Configuration section above. On the screen below, the range should be something like 192-168-1.80 - 192-168-1.85 to be valid.

**Message:** *The value of 'DNS Server' must be a valid IP address in dotted decimal notation ('x.y.z.w').***Meaning:** You entered an invalid IP address for the DNS Server being configured.**Recovery:** **1.** Click the **OK** button to clear the webpage message. **2.** Enter a valid IP address in the format x.y.z.w per the on-screen restrictions.**Message:** *'DHCP Interface VLAN ID' must be an integer value between 1 and 4095.***Meaning:** You entered an invalid VLAN ID for the DHCP Interface.**Recovery:** **1.** Click the **OK** button to clear the webpage message. **2.** Enter a valid VLAN ID for the DHCP Interface (1-4095).**Message:** *DHCP per Port range (192.168.1.50 - 192.168.1.66) is not equal to switch TP port number (8).***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.

## Appendix B - MRP Pre-Requisites and Application Examples

You can configure Media Redundancy Protocol (MRP) parameters via the Web UI at Configuration > MRP and monitor them at Monitor > MRP, or via the CLI. See the *CLI Reference* for Command Line operation.

According to ANSI, [IEC 62439-2 Ed. 1.0 b:2010](#) is applicable to high-availability automation networks based on [ISO/IEC 8802-3](#) / [IEEE 802.3 Ethernet technology](#). It specifies a recovery protocol based on a ring topology, designed to react deterministically on a single failure of an inter-switch link or switch in the network, under the control of a dedicated Media Redundancy Manager (MRM) node.

Media Redundancy Protocol per IEC 62439-2 is an interoperable ring technology designed to allow a switch to connect onto a universal redundant high speed ring. MRP is self-healing and self-adjusting, requiring no operator interaction. MRP is based on the concept of standby connections for seamless redundancy.

### 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 at FW v7.10.2368 for SISPM1040-384-LRT-C, SISPM1040-362-LRT, SISPM1040-582-LRT, SISGM1040-284-LRT, SISPM1040-3166-L, and SISPM1040-3248-L.

## MRP Sample Setup

The example below shows SISPM1040-384-LRT-C switches (one MRM and five MRCs).

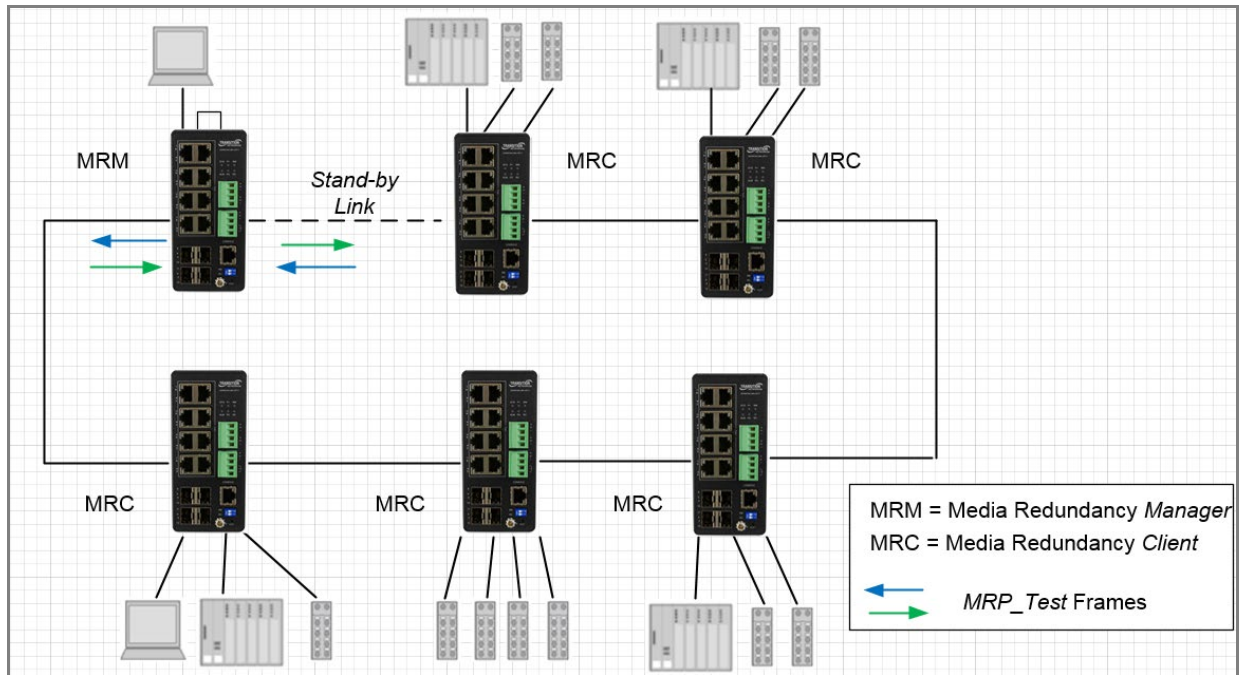


Figure: MRP Sample Setup

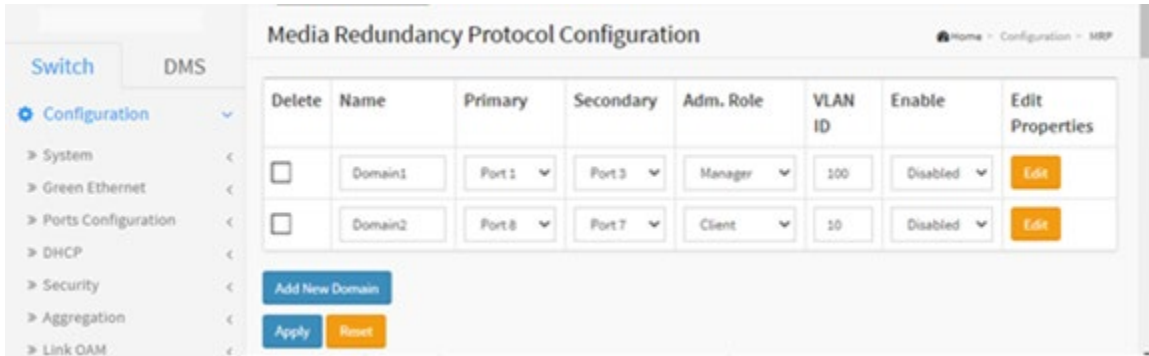
## MRP Pre-Requisites (General)

The following are required to perform MRP setups.

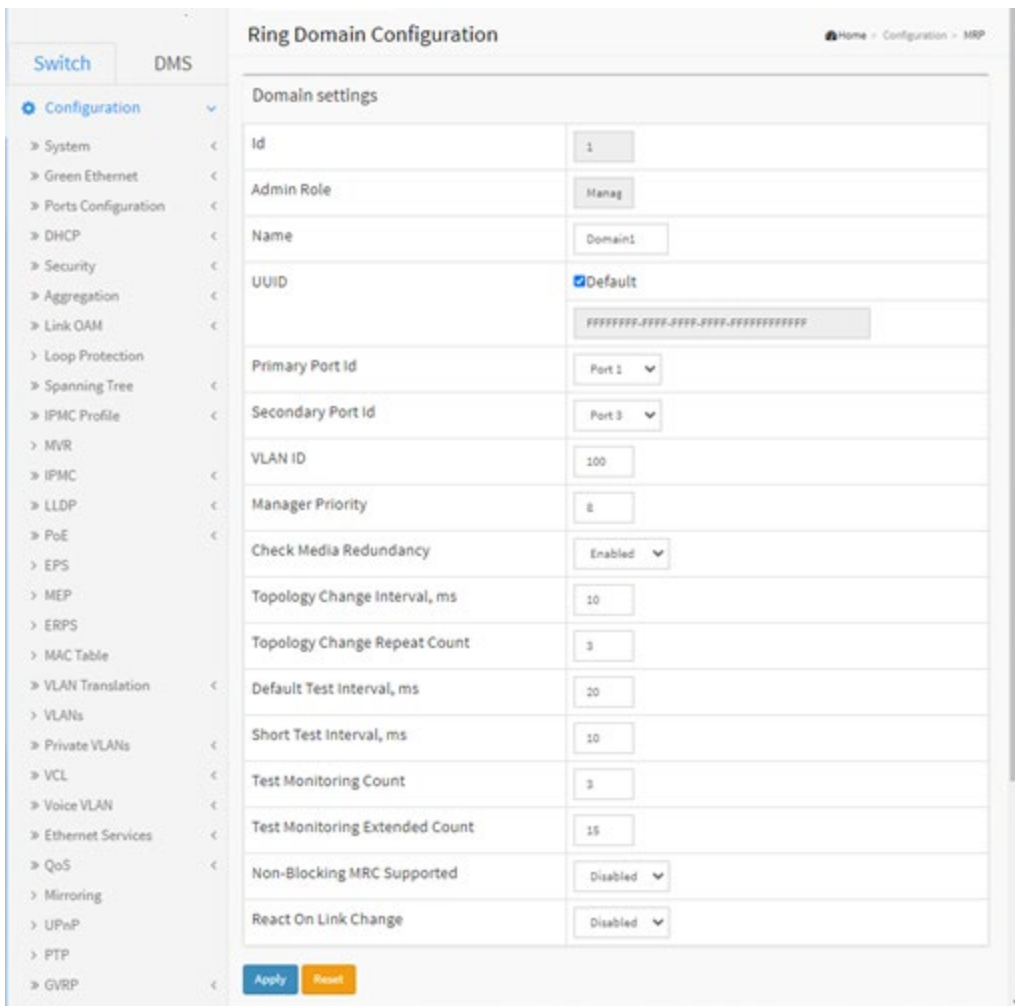
1. Spanning Tree must be disabled at Configuration > Spanning Tree > CIST Port.
2. Other Ring technologies must also be disabled (G.8031 EPS, G.8032 ERPS, Rapid-Ring, Ring-To-Ring, etc.).
3. Only one MRM (Manager) is supported per ring.
4. Other pre-requisites may apply to the specific examples below.
5. One Manager Admin Role is supported.

## MRP Web UI Configuration

1. 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 (Domian1).



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).

Domain settings	
Id	2
Admin Role	Client
Name	Domain2
UUID	<input checked="" type="checkbox"/> Default FFFFFFFF-FFFF-FFFF-FFFF-FFFFFFFFFFFFFF
Primary Port Id	Port 8
Secondary Port Id	Port 7
VLAN ID	10
Link Down Interval, ms	20
Link Up Interval, ms	20
Link Change Count	4
BLOCKED State Supported	Enabled

Apply Reset

5. Edit the Domain Settings as required. Click Apply to save; the message *“Domain is enabled”* displays. Click OK to clear the webpage message.

6. When the *“Media Redundancy Protocol Configuration”* page displays again, verify the settings.

### Example 1: MRP Manager Re-Config (Web UI)

This application example shows the MRP Manager reconfiguring the traffic path based on the client state.

**Sample Setup:** This setup includes one device with MRP enabled and has an admin role set as Manager and three clients connected in a ring topology. See the MRP Sample Setup diagram below.

#### Procedure:

1. Disable any other Ring technologies and disable Spanning-tree at Configuration > Spanning Tree > CIST Port.
2. For the device acting as MRM click 'Add New Domain' button to configure the MRP instance in the 'Media Redundancy Protocol Configuration' page.
3. Assign the first ring port under 'Primary' and the second ring port under 'Secondary'.
4. Set the Administrative Role to 'Manager' under 'Adm. Role'. Assign any VLAN ID from 2-4094.
5. Set the instance to 'enable'.
6. Go to the 'Ring Domain Configuration (Manager Role)' page and set a Domain name.
7. Tick the Default box for UUID.
8. Select the Primary and Secondary Port IDs.
9. Enable 'Check Media Redundancy'.
10. Leave other settings as default.
11. For the devices acting as MRCs in the 'Ring Domain Configuration (Client Role)' page assign the first Primary and Secondary Port IDs for the ring ports.
12. Enter the same VLAN ID as in step 4 above.
13. Link Down Interval should be 20ms. Link Up Interval should be 20ms. Link change count should be 4.
14. 'BLOCKED State Supported' must be enabled. By default, one ring port will be disabled for loop-free communication.
15. Configure ring ports to Hybrid mode on the VLAN Configuration page. Assign the VLAN ID as configured in step 4.
16. Send bi-directional traffic tagged with the VLAN ID set in step 4 above.
17. Create a failure on any one of the client ring ports by disconnecting the cable. The MRM should reconfigure the path within 200<500ms. The Redundancy Manager will send test frames marked with a unique MAC with OUI of 00-15-4E and forwarded by the MRCs to the opposite ring ports per the interval specified.  
The disabled ring port should now be enabled, creating a new loop-free topology.
18. There should be no traffic loss after path reconfiguration.

### Example 2: Non-Blocking MRC State Recognized by MRM (Web UI)

This application example shows a Non-blocking MRC state is recognized by the MRM.

Setup: This setup and steps 1-18 in Example 1 above are required.

#### Procedure:

1. Disable any other Ring technologies and disable Spanning-tree at Configuration > Spanning Tree > CIST Port.
2. Disable 'BLOCKED State Supported'.
3. Configure ring ports to Hybrid mode on the VLAN Configuration page. Assign the VLAN ID as configured in step 4 of Example 1.
4. Send bi-directional traffic tagged with the VLAN ID set in the previous step.
5. Create a failure on any one of the client ring ports by disconnecting the cable. The client ring ports will be in a forwarding state instead of blocking. The MRM should reconfigure the path within 200<500ms. The MRM will send test frames marked with a unique MAC with OUI of 00-15-4E and forwarded by the MRCs to the opposite ring ports per the interval specified.
6. Verify the MRC reacts to the reconfiguration frames as received by the MRM. The link down on the client ring port should be detected by the MRC.
7. There should be no traffic loss after path reconfiguration.

### Example 3: MRP Roles Set in Web UI

Setup: This setup shows that the MRP can have both Manager and Undefined roles.

#### Procedure:

1. Disable any other Ring technologies and disable Spanning-tree at Configuration > Spanning Tree > CIST Port.
2. 'BLOCKED State Supported' should be enabled. By default, one ring port will be disabled for loop-free communication.
3. Configure ring ports to Hybrid mode on the VLAN Configuration page. Assign the VLAN ID as set in step 4 of Example 1.
4. Send bi-directional traffic tagged with the VLAN ID set in the previous step.
5. Create a failure on any one of the client ring ports by disconnecting the cable. The MRM should reconfigure the path within 200<500ms. The Redundancy manager will send test frames marked with a unique MAC with OUI of 00-15-4E and forwarded by the MRCs to the opposite ring ports per the interval specified. The disabled ring port should now be enabled and creates a new loop-free topology.
6. There should be no traffic loss after path reconfiguration.
7. On a second client set the 'BLOCKED State Supported' option to disable. The ring port will now be in a forwarding state. Cause a failure on the ring port of another device that has its blocked state disabled.
8. Verify that frames are forwarded and received by the MRC with blocking enabled. There should be no traffic loss after path reconfiguration.

## Appendix C - G.8032 Major and Sub Rings Configuration

### Introduction

Ethernet Ring Protection Switching (ERPS) is a protocol defined by the International Telecommunication Union - Telecommunication Standardization Sector (ITU-T) to prevent loops at Layer 2. With the standard number is ITU-T G.8032, and ERPS is also called G.8032. Generally, redundant links are used on a network to provide link backup and enhance network reliability. The use of redundant links, however, may produce loops, causing broadcast storms and rendering the MAC address table unstable. These can affect the network, where the communication quality is not good enough, and communication services might be interrupted.

ERPS provides advantages of traditional ring network technologies such as STP/RSTP/MSTP and optimizes detection mechanism to provide faster convergence. For example, the ERPS-enabled switch provides 50-ms convergence for broadcast packets. See “[ERPS](#)” on page [306](#) for general G.8032 ERPS configuration information.

### Basic Concepts

There are some basic concepts that support ERPS Ring:

- **Ring Protection Link (RPL)** – Link designated by mechanism that is blocked during Idle state to prevent loop on Bridged ring.
- **RPL Owner node** – Node connected to RPL that blocks traffic on RPL during Idle state and unblocks during Protection state.
- **RPL Neighbor node** – Node connected to RPL that blocks traffic on RPL during Idle state and unblocks during Protection state (v2).
- **Link Monitoring** – Links of ring are monitored using standard ETH CC OAM messages (CFM) • Signal Fail (SF) – Signal Fail is declared when signal fail condition is detected.
- **No Request (NR)** – No Request is declared when there are no outstanding conditions (e.g., SF, etc.) on the node.
- **Ring APS (R-APS) Messages** – Protocol messages defined in Y.1731 and G.8032.
- **Automatic Protection Switching (APS) Channel** - Ring-wide VLAN used exclusively for transmission of OAM messages including R-APS messages.

### IP Addresses

The sample configurations below use these IP addresses:

SISPM1040-582-LRT : 192.168.1.85

SISPM1040-384-LRT-C : 192.168.1.95

362W : 192.168.1.125

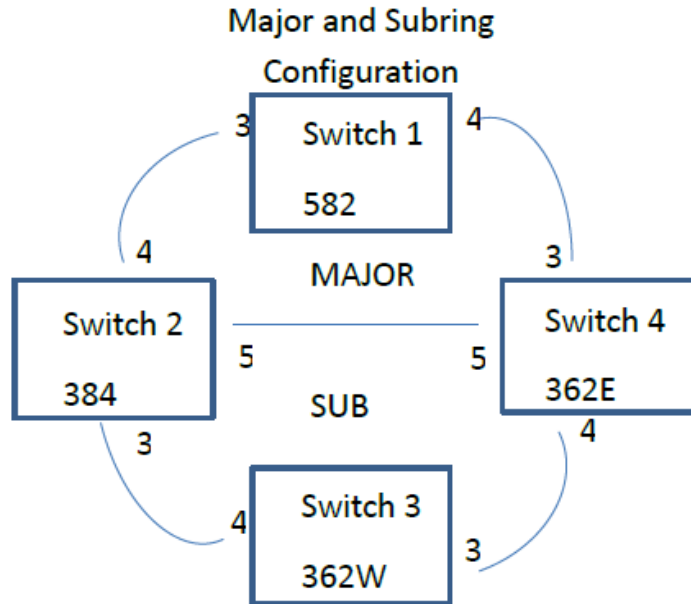
362E : 192.168.1.135



## Sample Configuration

Major Ring and Sub Ring : 4 Switches

Major : SW#1, SW#2, SW#4; Sub : SW#2, SW#3, SW#4



**VLANs**

**APS**      **Data**  
 10,20      5

**RPL Mode**

<b><u>Major</u></b>	<b><u>Sub</u></b>	<b><u>Major</u></b>	<b><u>Sub</u></b>	<b><u>Major</u></b>	<b><u>Sub</u></b>		
Owner	Owner	Neighbor	Neighbor		None	None	
Switch	Switch	Switch	Switch		Switch	Switch	
#1	#3	#2	#2	#4	#4		

**Switch 1 Configuration (SISPM1040-582-LRT)**

<b>VLANs</b>	Port 3	Trunk	Tag All	5,10
	Port 4	Trunk	Tag All	5,10
<b>STP</b>	Port 3	Disable		
	Port 4	Disable		

<b>MEPs</b>	Instance	Port	VLAN	MAC	MEP ID	Peer MAC	Peer MEP ID
	1	3	10	00-C0-F2-49-39-5F	1	00-40-C7-1C-C7-30	4
	2	4	10	00-C0-F2-49-39-60	5	00-C0-F2-53-EF-FC	5

**Note:** All MEPs are programmed the same under the Functional Configuration

**Continuity Check**

Check Enable – Priority: 7 – Frame rate: 1f/sec

**APS Protocol**

Check Enable – Priority: 7 – Cast: Multi – Type: R-APS

Functional Configuration									
Continuity Check				APS Protocol					
Enable	Priority	Frame rate	TLV	Enable	Priority	Cast	Type	Last Octet	
<input checked="" type="checkbox"/>	7	1f/sec	<input type="checkbox"/>	<input checked="" type="checkbox"/>	7	Multi	R-APS	1	

[Fault Management](#) [Performance Monitoring](#)

<b>ERPS</b>	ERPS ID	Port 0	Port 1	Port 0 SF	Port 1 SF	Port 0 APS	Port 1 APS	Ring	RPL	Port	VLAN
	1	1	2	1	2	1	2	Major	Owner	0	5

**Switch 2 Configuration (SISPM1040-384-LRT-C)**

**VLANS**  
 Port 3 Trunk Tag All 5,20  
 Port 4 Trunk Tag All 5,10  
 Port 5 Trunk Tag All 5,10,20

**STP**  
 Port 3 Disable  
 Port 4 Disable  
 Port 5 Disable

MEPs	Instance	Port	VLAN	MAC	MEP ID	Peer MAC	Peer MEP ID
	1	3	20	00-40-C7-1C-C7-2F	3	00-C0-F2-53-F0-BA	8
	2	4	10	00-C0-F2-49-39-60	4	00-C0-F2-49-39-5F	1
	3	5	10	00-40-C7-1C-C7-31	9	00-C0-F2-53-EF-FE	10

**Note:** All MEPs are programed the same under the Functional Configuration

**Continuity Check**

Check Enable – Priority: 7 – Frame rate: 1f/sec

**APS Protocol**

Check Enable – Priority: 7 – Cast: Multi – Type: R-APS

Functional Configuration									
Continuity Check				APS Protocol					
Enable	Priority	Frame rate	TLV	Enable	Priority	Cast	Type	Last Octet	
<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 VLAN	Port 1	Port 0 SF	Port 1 SF	Port 0 APS	Port 1 APS	Ring	RPL	Port
1	3 5	2	3	2	3	2	Major	Neighbor	1
2	1 5	0	1	0	1	0	Sub	Neighbor	0

Interconnect Yes, Major 1

**Switch 3 Configuration (SISPM1040-362-LRT[W])**

**VLANs**            Port 3    Trunk Tag All 5,20  
                      Port 4    Trunk Tag All 5,20

**STP**             Port 3    Disable  
                      Port 4    Disable

MEPs	Instance	Port	VLAN	MAC	MEP ID	Peer MAC	Peer MEP ID
	1	3	20	00-C0-F2-53-F0-B9	7	00-C0-F2-53-EF-FD	6
	2	4	20	00-C0-F2-53-F0-BA	8	00-40-C7-1C-C7-2F	3

**Note:** All MEPs are programed the same under the Functional Configuration

**Continuity Check**

Check Enable – Priority: 7 – Frame rate: 1f/sec

**APS Protocol**

Check Enable – Priority: 7 – Cast: Multi – Type: R-APS

Functional Configuration									
Continuity Check				APS Protocol					
Enable	Priority	Frame rate	TLV	Enable	Priority	Cast	Type	Last Octet	
<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	2	1	2	1	2	Sub	Owner	1	5

### Switch 4 Configuration (SISPM1040-362-LRT[E])

<b>VLANS</b>	Port 3	Trunk	Tag All	5,10
	Port 4	Trunk	Tag All	5,20
	Port 5	Trunk	Tag All	5,10,20

<b>STP</b>	Port 3	Disable
	Port 4	Disable
	Port 5	Disable

<b>MEPs</b>	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	

#### ERPS

ERPS ID	Port 0	Port 1	Port 0 SF	Port 1 SF	Port 0 APS	Port 1 APS	Ring	RPL	Port VLAN
1	1	3	1	3	1	3	Major	None	5
2	2	0	2	0	2	0	Sub	None	5

Interconnect Yes, Major 1

## Testing

### Testing Pings from Switch 4 to Switch 1 – Major Ring

#### Failing Major ring, No lost pings

```
C:\Users\dennist>ping 192.168.1.85 -t
Pinging 192.168.1.85 with 32 bytes of data:
Reply from 192.168.1.85: bytes=32 time<1ms TTL=64
Reply from 192.168.1.85: bytes=32 time<1ms TTL=64
Reply from 192.168.1.85: bytes=32 time<1ms TTL=64
Reply from 192.168.1.85: bytes=32 time<1ms TTL=64
Reply from 192.168.1.85: bytes=32 time<1ms TTL=64
Reply from 192.168.1.85: bytes=32 time<1ms TTL=64
Reply from 192.168.1.85: bytes=32 time<1ms TTL=64
Reply from 192.168.1.85: bytes=32 time<1ms TTL=64
Reply from 192.168.1.85: bytes=32 time<1ms TTL=64
Reply from 192.168.1.85: bytes=32 time<1ms TTL=64
Reply from 192.168.1.85: bytes=32 time<1ms TTL=64
Reply from 192.168.1.85: bytes=32 time<1ms TTL=64
Reply from 192.168.1.85: bytes=32 time<1ms TTL=64
Reply from 192.168.1.85: bytes=32 time<1ms TTL=64
Reply from 192.168.1.85: bytes=32 time<1ms TTL=64
Reply from 192.168.1.85: bytes=32 time<1ms TTL=64
Reply from 192.168.1.85: bytes=32 time<1ms TTL=64
Reply from 192.168.1.85: bytes=32 time<1ms TTL=64
Reply from 192.168.1.85: bytes=32 time<1ms TTL=64
Reply from 192.168.1.85: bytes=32 time<1ms TTL=64
Reply from 192.168.1.85: bytes=32 time<1ms TTL=64
Reply from 192.168.1.85: bytes=32 time<1ms TTL=64
Reply from 192.168.1.85: bytes=32 time<1ms TTL=64
Reply from 192.168.1.85: bytes=32 time<1ms TTL=64
Reply from 192.168.1.85: bytes=32 time<1ms TTL=64
Reply from 192.168.1.85: bytes=32 time<1ms TTL=64
Reply from 192.168.1.85: bytes=32 time<1ms TTL=64
Reply from 192.168.1.85: bytes=32 time<1ms TTL=64
Reply from 192.168.1.85: bytes=32 time<1ms TTL=64
Reply from 192.168.1.85: bytes=32 time<1ms TTL=64
Reply from 192.168.1.85: bytes=32 time=5ms TTL=64 ←-----
Reply from 192.168.1.85: bytes=32 time<1ms TTL=64 Cable Disconnect
Reply from 192.168.1.85: bytes=32 time=3ms TTL=64 ←-----
Reply from 192.168.1.85: bytes=32 time<1ms TTL=64
Reply from 192.168.1.85: bytes=32 time=1ms TTL=64
Reply from 192.168.1.85: bytes=32 time<1ms TTL=64
Reply from 192.168.1.85: bytes=32 time<1ms TTL=64
Reply from 192.168.1.85: bytes=32 time<1ms TTL=64
Reply from 192.168.1.85: bytes=32 time=1ms TTL=64
Reply from 192.168.1.85: bytes=32 time<1ms TTL=64
Reply from 192.168.1.85: bytes=32 time<1ms TTL=64
Ping statistics for 192.168.1.85:
Packets: Sent = 45, Received = 45, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 0ms, Maximum = 5ms, Average = 0ms
```



## Config files

### running-config\_192.168.1

```
hostname SISPM1040-362-LRT-E
username admin privilege 15 password encrypted
feec1d1085ff075fd03b1d2d5ab4c0befbfff0917079c8abb3a77338041bf5d6e1771bdbbd1a317ea2f42fc2aacc8c
50a8e667456d7c04099f74f8ef9dcc0fbd4
!
vlan 1
!
!
!
!
ip route 0.0.0.0 0.0.0.0 192.168.1.254
tzidx 0
exec-timeout autologout 0
snmp-server location DT Lab Ring
system name SISPM1040-362-LRT-E
system location DT Lab Ring
system description Managed Hardened PoE+ Switch, (4) 10/100/1000Base-T PoE+ Ports + (2)
10/100/1000Base-T Ports + (2) 100/1000Base-X SFP Ports
!
interface GigabitEthernet 1/1
!
interface GigabitEthernet 1/2
!
interface GigabitEthernet 1/3
no spanning-tree
switchport trunk allowed vlan 5,10
switchport trunk vlan tag native
switchport mode trunk
poE mode disable
!
interface GigabitEthernet 1/4
no spanning-tree
switchport trunk allowed vlan 5,20
switchport trunk vlan tag native
switchport mode trunk
poE mode disable
!
interface GigabitEthernet 1/5
no spanning-tree
switchport trunk allowed vlan 5,10,20
switchport trunk vlan tag native
switchport mode trunk
!
interface GigabitEthernet 1/6
!
interface GigabitEthernet 1/7
!
interface GigabitEthernet 1/8
!
interface vlan 1
ip address 192.168.1.135 255.255.255.0
ip dhcp server
!
mep 1 down domain port level 4 interface GigabitEthernet 1/3
mep 1 mep-id 5
mep 1 vid 10
mep 1 peer-mep-id 2 mac 00-C0-F2-49-39-60
mep 1 cc 7
mep 1 aps 7 raps
```



```
mep 2 down domain port level 4 interface GigabitEthernet 1/4
mep 2 mep-id 6
mep 2 vid 20
mep 2 peer-mep-id 7 mac 00-C0-F2-53-F0-B9
mep 2 cc 7
mep 2 aps 7 raps
mep 3 down domain port level 4 interface GigabitEthernet 1/5
mep 3 mep-id 10
mep 3 vid 10
mep 3 peer-mep-id 9 mac 00-40-C7-1C-C7-31
mep 3 cc 7
mep 3 aps 7 raps
erps 1 major port0 interface GigabitEthernet 1/3 port1 interface GigabitEthernet 1/5
erps 1 mep port0 sf 1 aps 1 port1 sf 3 aps 3
erps 1 vlan 5
erps 2 sub port0 interface GigabitEthernet 1/4 interconnect 1
erps 2 mep port0 sf 2 aps 2
erps 2 vlan 5
!
spanning-tree aggregation
  spanning-tree link-type point-to-point
!
!
line console 0
!
line vty 0
!
line vty 1
!
line vty 2
!
line vty 3
!
line vty 4
!
line vty 5
!
line vty 6
!
line vty 7
!
line vty 8
!
line vty 9
!
line vty 10
!
line vty 11
!
line vty 12
!
line vty 13
!
line vty 14
!
line vty 15
!
!
end
```

**running-config\_192.168.1****hostname SISPM1040-582-LRT**

```
logging on
logging host 192.168.1.253
username admin privilege 15 password encrypted
7073dec86c15b8a9907bb4106ef783adde46bd5b5969cc68fb55b430336bd7c80d5ded65d2fdb39abe81cc9caa5a9
3620f270c21bca86e776cee9c5588bfb8c7
username superuser privilege 15 password encrypted
4643fdc71f39fd4cb955943fcaf89faca81bc650fbaeebe25a796662d5c225bf0d5ded65d2fdb39abe81cc9c51449
7e27799560e488713aabaac4f167e7732ca
!
vlan 1
!
!
!
!
ip route 0.0.0.0 0.0.0.0 192.168.1.254
ntp automatic
ntp server 1 ip-address ntp1.transition.com
ntp server 2 ip-address ntp2.transition.com
clock timezone ' ' 9
tzidx 0
exec-timeout autologout 0
poE ping-check enable
snmp-server contact DTroxel
snmp-server location DT Office
system contact DTroxel
system name SISPM1040-582-LRT
system location DT Office
system description Managed Hardened PoE++ Switch (8) 10/100/1000Base-T PoE++ Ports + (2)
100/1000Base-X SFP Slot
!
interface GigabitEthernet 1/1
no spanning-tree
poE ping-ip-addr 192.168.1.70
poE failure-action reboot-Remote-PD
!
interface GigabitEthernet 1/2
no spanning-tree
switchport forbidden vlan add 3,5
!
interface GigabitEthernet 1/3
no spanning-tree
switchport trunk allowed vlan 5,10
switchport trunk vlan tag native
switchport mode trunk
poE mode disable
!
interface GigabitEthernet 1/4
no spanning-tree
switchport trunk allowed vlan 5,10
switchport trunk vlan tag native
switchport mode trunk
poE mode disable
poE ping-ip-addr 192.168.1.200
!
interface GigabitEthernet 1/5
no spanning-tree
!
interface GigabitEthernet 1/6
no spanning-tree
!
```

```
interface GigabitEthernet 1/7
!
interface GigabitEthernet 1/8
 poe mode disable
!
interface GigabitEthernet 1/9
 no spanning-tree
!
interface GigabitEthernet 1/10
 no spanning-tree
!
interface vlan 1
 ip address 192.168.1.85 255.255.255.0
 ip dhcp server
!
mep 1 down domain port level 4 interface GigabitEthernet 1/3
mep 1 vid 10
mep 1 peer-mep-id 4 mac 00-40-C7-1C-C7-30
mep 1 cc 7
mep 1 aps 7 raps
mep 2 down domain port level 4 interface GigabitEthernet 1/4
mep 2 mep-id 2
mep 2 vid 10
mep 2 peer-mep-id 5 mac 00-C0-F2-53-EF-FC
mep 2 cc 7
mep 2 aps 7 raps
erps 1 major port0 interface GigabitEthernet 1/3 port1 interface GigabitEthernet 1/4
erps 1 mep port0 sf 1 aps 1 port1 sf 2 aps 2
erps 1 rpl owner port0
erps 1 vlan 5
!
spanning-tree aggregation
 no spanning-tree
 spanning-tree link-type point-to-point
!
!
line console 0
!
line vty 0
!
line vty 1
!
line vty 2
!
line vty 3
!
line vty 4
!
line vty 5
!
line vty 6
!
line vty 7
!
line vty 8
!
line vty 9
!
line vty 10
!
line vty 11
!
line vty 12
```

```
!  
line vty 13  
!  
line vty 14  
!  
line vty 15  
!  
map-api-key AIzaSyBITuM0hDtK6nJeZPEk7jnrcoGGi92EpFM  
!  
end
```

**running-config\_192.168.1****hostname SISPM1040-384-LRT-C**

```
username admin privilege 15 password encrypted
6593186b999f348becd63b8612ac561c114250a1a00bd38f6afb5378acb6d08c1864c59b092b0e2b29ba4f1d55916
6800846cbc52c4558a90e4cdf95d3cfcbf4
username dennis privilege 5 password encrypted
a92a5dbf4fcd2e13d35adb36d2418476e907de19a641fa7baf80b1abb36d2bacd8ee5dbdd44e246b88be1636df6b8769
af790aa8721622481085e33c32e6e119dbd
!
vlan 1
!
!
!
!
ip route 0.0.0.0 0.0.0.0 192.168.1.254
tzidx 0
exec-timeout autologout 0
poe ping-check enable
access-list ace 2 ingress interface GigabitEthernet 1/2 action deny
access-list ace 1 next 2 ingress interface GigabitEthernet 1/2 frame-type ipv4-tcp dport 443
system name SISPM1040-384-LRT-C
system description Managed Hardened PoE+ Switch, (8) 10/100/1000Base-T PoE+ Ports + (4)
100/1000Base-X SFP
!
interface GigabitEthernet 1/1
 no spanning-tree
 lldp cdp-aware
 poe ping-ip-addr 192.168.1.100
 poe failure-action reboot-Remote-PD
!
interface GigabitEthernet 1/2
 no spanning-tree
 lldp cdp-aware
 speed 1000
 duplex full
!
interface GigabitEthernet 1/3
 no spanning-tree
 switchport trunk allowed vlan 5,20
 switchport trunk vlan tag native
 switchport mode trunk
 lldp cdp-aware
 poe mode disable
!
interface GigabitEthernet 1/4
 no spanning-tree
 switchport trunk allowed vlan 5,10
 switchport trunk vlan tag native
 switchport mode trunk
 lldp cdp-aware
 poe mode disable
!
interface GigabitEthernet 1/5
 no spanning-tree
 switchport trunk allowed vlan 5,10,20
 switchport trunk vlan tag native
 switchport mode trunk
 lldp cdp-aware
 poe mode disable
!
interface GigabitEthernet 1/6
 no spanning-tree
```

```
lldp cdp-aware
!
interface GigabitEthernet 1/7
lldp cdp-aware
!
interface GigabitEthernet 1/8
lldp cdp-aware
!
interface GigabitEthernet 1/9
no spanning-tree
switchport trunk allowed vlan 1,50,100
switchport trunk vlan tag native
lldp cdp-aware
!
interface GigabitEthernet 1/10
no spanning-tree
lldp cdp-aware
!
interface GigabitEthernet 1/11
no spanning-tree
lldp cdp-aware
!
interface GigabitEthernet 1/12
no spanning-tree
lldp cdp-aware
!
interface vlan 1
ip address 192.168.1.95 255.255.255.0
ip dhcp server
!
mep 1 down domain port level 4 interface GigabitEthernet 1/3
mep 1 mep-id 3
mep 1 vid 20
mep 1 peer-mep-id 8 mac 00-C0-F2-53-F0-BA
mep 1 cc 7
mep 1 aps 7 raps
mep 2 down domain port level 4 interface GigabitEthernet 1/4
mep 2 mep-id 4
mep 2 vid 10
mep 2 peer-mep-id 1 mac 00-C0-F2-49-39-5F
mep 2 cc 7
mep 2 aps 7 raps
mep 3 down domain port level 4 interface GigabitEthernet 1/5
mep 3 mep-id 9
mep 3 vid 10
mep 3 peer-mep-id 10 mac 00-C0-F2-53-EF-FE
mep 3 cc 7
mep 3 aps 7 raps
erps 1 major port0 interface GigabitEthernet 1/5 port1 interface GigabitEthernet 1/4
erps 1 mep port0 sf 3 aps 3 port1 sf 2 aps 2
erps 1 rpl neighbor port1
erps 1 vlan 5
erps 2 sub port0 interface GigabitEthernet 1/3 interconnect 1
erps 2 mep port0 sf 1 aps 1
erps 2 rpl neighbor port0
erps 2 vlan 5
!
spanning-tree aggregation
no spanning-tree
spanning-tree link-type point-to-point
!
!
line console 0
```

```
!  
line vty 0  
!  
line vty 1  
!  
line vty 2  
!  
line vty 3  
!  
line vty 4  
!  
line vty 5  
!  
line vty 6  
!  
line vty 7  
!  
line vty 8  
!  
line vty 9  
!  
line vty 10  
!  
line vty 11  
!  
line vty 12  
!  
line vty 13  
!  
line vty 14  
!  
line vty 15  
!  
map-api-key AIzaSyBITuM0hDtK6nJeZPEk7jnrcGGi92EpFM  
!  
end
```

**running-config\_192.168.1****hostname SISPM1040-362-LRT-W**

```
username admin privilege 15 password encrypted
6158ed7daf39d06ded0e7c4828c3b15bb4c40673bd445afcd643295925ae425d9611d1cbe872708237571aacc7b92
37f33b01ae6866e2484009edfe1fa0bf56f
!
vlan 1
!
!
!
!
ip route 0.0.0.0 0.0.0.0 192.168.1.254
tzidx 0
exec-timeout autologout 0
snmp-server location DT Lab Ring
system name SISPM1040-362-LRT-W
system location DT Lab Ring
system description Managed Hardened PoE+ Switch, (4) 10/100/1000Base-T PoE+ Ports + (2)
10/100/1000Base-T Ports + (2) 100/1000Base-X SFP Ports
!
interface GigabitEthernet 1/1
!
interface GigabitEthernet 1/2
!
interface GigabitEthernet 1/3
no spanning-tree
switchport trunk allowed vlan 5,20
switchport trunk vlan tag native
switchport mode trunk
poE mode disable
!
interface GigabitEthernet 1/4
no spanning-tree
switchport trunk allowed vlan 5,20
switchport trunk vlan tag native
switchport mode trunk
poE mode disable
!
interface GigabitEthernet 1/5
!
interface GigabitEthernet 1/6
!
interface GigabitEthernet 1/7
!
interface GigabitEthernet 1/8
!
interface vlan 1
ip address 192.168.1.125 255.255.255.0
ip dhcp server
!
mep 1 down domain port level 4 interface GigabitEthernet 1/3
mep 1 mep-id 7
mep 1 vid 20
mep 1 peer-mep-id 6 mac 00-C0-F2-53-EF-FD
mep 1 cc 7
mep 1 aps 7 raps
mep 2 down domain port level 4 interface GigabitEthernet 1/4
mep 2 mep-id 8
mep 2 vid 20
mep 2 peer-mep-id 3 mac 00-40-C7-1C-C7-2F
mep 2 cc 7
mep 2 aps 7 raps
```



```
erps 1 sub port0 interface GigabitEthernet 1/3 port1 interface GigabitEthernet 1/4
erps 1 mep port0 sf 1 aps 1 port1 sf 2 aps 2
erps 1 rpl owner port1
erps 1 vlan 5
!
spanning-tree aggregation
  spanning-tree link-type point-to-point
!
!
line console 0
!
line vty 0
!
line vty 1
!
line vty 2
!
line vty 3
!
line vty 4
!
line vty 5
!
line vty 6
!
line vty 7
!
line vty 8
!
line vty 9
!
line vty 10
!
line vty 11
!
line vty 12
!
line vty 13
!
line vty 14
!
line vty 15
!
!
end
```

**Lantronix 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](http://www.lantronix.com/about/contact).