

SM24TBT2DPA and SM24TBT2DPB

Managed Gigabit Ethernet PoE++ Switch

(24) 10/100/1000Base-T Ports + (2) 100/1000Base-X SFP/RJ-45 Combo Ports

Web User Guide

Intellectual Property

© 2022-2024 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, 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 the Lantronix web site at www.lantronix.com/about/contact.

Disclaimer

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

Revision History

Rev	Date	Description
H	4/26/22	Initial Lantronix SM24TBT2DPB release at FW vB6.64.0045. SM24TBT2DPA FW vB6.64.0043.
J	11/30/22	FW vB6.64.0079: add DHCP per port function to select a particular IP interface. Add two device icons in DMS. Change default settings: SNMP mode Disabled as factory default and change Auth Method Configuration default. Add First Time Wizard. Add DHCP option 229 support. In PoE schedule, if Start Time = End Time, reset PoE power on the ports. Update DMS Map View info. Add ConsoleFlow in web/cli/api, add CF on-premise support, add CF S/N and LPM MAC address, and support API in https. Note that SM24TBT2DPA is EoL. Note change to Power Supply monitoring.
K	7/16/24	FW VB6.64.0123: Add info on router config setup at Configuration > System > IP. Add PoE++ clarifications. Change self-signed certificate. Update to TLSv1.2 ciphers. Allow special characters in Web PoE profile name. Allow PoE mode and priority to be configured via Web UI. Update LLDP-MED Neighbor Information. Add Percepixon and LPM support. Allow configuring dash character (-) for status update interval and content check interval and switch disconnect from server. Show Operation status messages. Automatically save Config changes to Start-Up Config in Percepixon server. Remove invalid file name "mach10_combined.crt" from Config Download, Upload, Activate, and Delete pages. Add a Caution that Forcing the switch to send POE to non-POE devices can physically damage those devices. Modify Device/Product type API format. Add Capability Negotiation Definition with Percepixon Server. Fix show SNMP user command and Percepixon telemetry exchange issues. See the Release Notes for details.

Contents

Introduction	8
Safety Warnings and Cautions	9
Chapter 1 - Web-based Management Operation	10
1-1.1 Web UI Controls	11
1-1.2 First Time Wizard	13
1-1.3 Web UI Modules	16
Chapter 2 - System Configuration	17
2-1 System	17
2-1.1 Information	17
2-1.4 IP	21
2-1.3 NTP	24
2-1.4 Time	25
2-1.5 Log	27
2-2 Green Ethernet	28
2-3 Ports Configuration	30
2-3.1 Ports	30
2-3.2 Ports Description	32
2-4 DHCP	33
2-4.1 Server	33
2-4.1.1 Mode	33
2-4.1.3 Pool	36
2-5 Security	45
2-5.1 Switch	45
2-5.1.1 Users	45
2-5.1.2 Privilege Levels	47
2-5.1.3 Authentication Method	49
2-5.1.4 HTTPS Configuration	51
2-5.1.6 Access Management	53
2-5.1.8.2 History	69
2-5.2 Network	73
2-5.2.1 Limit Control	73
2-5.2.2 NAS	76
2-5.2.3 ACL	82
2-5.2.4 IP Source Guard	93
2-5.2.5 ARP Inspection	96
2-5.3 AAA	103
2-5.3.1 RADIUS	103
2-5.3.2 TACACS+	106
2-6 Aggregation	108
2-6.1 Static	108
2-6.2 LACP	110
2-7 Loop Protection	111
2-8 Spanning Tree	113
2-8.1 Bridge Setting	114
2-8.2 MSTI Mapping	116
2-8.3 MSTI Priorities	118
2-8.4 CIST Ports	119
2-8.5 MSTI Ports	121
2-9 IPMC Profile	123
2-9.1 Profile Table	123
2-9.1.1 IPMC Profile Rule Settings Table	125
2-9.2 Address Entry	126
2-10 MVR	127
2-11 IPMC	129

2-11.1 IGMP Snooping.....	129
2-11.1.1 Basic Configuration	129
2-11.1.2 VLAN Configuration.....	131
2-11.1.3 Port Filtering Profile	133
2-11.2 MLD Snooping	135
2-11.2.1 Basic Configuration	135
2-11.2.2 VLAN Configuration.....	137
2-11.2.3 Port Filtering Profile	139
2-12 LLDP	140
2-12.1 LLDP Configuration	140
2-12.2 LLDP-MED Configuration	143
2- 13 PoE	148
2- 13.3 PoE Schedule Profile.....	157
2- 13.4 PoE Auto Power Reset (PoE Auto Checking)	158
2- 13.5 PoE Chip Reset Schedule	160
2-14 MAC Table.....	161
2-15 VLANs	163
2-16 Private VLANs	166
2-16.1 Private VLAN Membership Configuration.....	166
2-16.2 Port Isolation.....	168
2-17 VCL.....	169
2-17.1 MAC-based VLAN	169
Messages:	170
2-17.2 Protocol-based VLAN	171
2-17.2.1 Protocol to Group	171
2-17.2.2 Group to VLAN.....	173
2-17.3 IP Subnet-based VLAN	174
2-18.1 Configuration	175
2-18.2 OUI	177
2-19 QoS.....	178
2-19.1 Port Classification.....	178
2-19.2 Port Policing	180
2-19.4 Port Schedulers	181
2-19.6 Port Tag Remarking.....	187
2-19.7 Port DSCP	190
2-19.8 DSCP-Based QoS	192
2-19.9 DSCP Translation	193
2-19.10 DSCP Classification	194
2-19.12 Storm Control	200
2-20 Mirroring	201
2-20 Mirroring	202
2-21 UPnP.....	203
2-22. GVRP	204
2-22.1 GVRP Config	204
2-22.2 Port Config.....	206
2-23. sFlow.....	207
2-24 Rapid Ring Configuration	210
2-25 Percepixon and LPM.....	211
2-26 SMTP Configuration	215
Chapter 3 - Monitor	216
3-1 System	216
3-1.1 Information.....	216
3-1.2 IP Status	218
3-1.3 Log.....	220
3-1.4 Detailed Log	222
3-2 Green Ethernet.....	225
3-2.1 Port Power Savings	225
3-3 Ports	226

3-3.1 Traffic Overview	226
3-3.2 QoS Statistics	227
3-3.3 QCL Status	228
3-3.4 Detailed Statistics	230
3-3.5 SFP Port Info	232
3-4 DHCP	234
3-4.1 Server	234
3-4.1.1 Statistics	234
3-4.1.2 Binding	236
3-5 Security	244
3-5.2 Network	245
3-5.2.1 Port Security	245
3-5.2.2 NAS	248
3-5.2.3 ACL Status	255
3-5.2.4 ARP Inspection	257
3-5.2.5 IP Source Guard	258
3-5.3 AAA	259
3-5.3.1 RADIUS Overview	259
3-5.4 Switch	265
3-5.4.1 RMON	265
3-6 Aggregation	272
3-6.1 Aggregation Status	272
3-6.2 LACP System Status	273
3-6.3 LACP Port Status	274
3-6.3 LACP Port Statistics	275
3-7 Loop Protection	276
3-8 Spanning Tree	277
3-8.1 Bridge Status	277
3-8.2 Port Status	280
3-8.3 Port Statistics	281
3-9 MVR	282
3-9.1 Statistics	282
3-9.2 MVR Channels Groups	283
3-10 IPMC	286
3-10.1 IGMP Snooping	286
3-10.1.1 Status	286
3-10.1.2 Group Information	288
3-10.1.3 IPv4 SFM Information	289
3-10.2 MLD Snooping	290
3-10.2.1 Status	290
3-10.2.2 Group Information	292
3-10.2.3 IPv6 SFM Information	293
3-11 LLDP	295
3-11.1 Neighbors	295
3-11.2 LLDP-MED Neighbor	297
3-11.3 PoE	304
3-11.4 EEE	305
3-11.5 Port Statistics	306
3-12 PoE	308
3-13 MAC Table	310
3-14 VLANs	312
3-14.1 VLAN Membership	312
3-13.2 VLAN Port	314
3-15 VCL	316
3-15.1 MAC-based VLAN	316
3-15.2 Protocol-based VLAN	317
3-15.2.1 Protocol to Group	317
3-15.2.2 Group to VLAN	319
3-15.3 IP Subnet-based VLAN	320

3-16 sFlow	321
Chapter 4 - Diagnostics	323
4-1 Ping	323
4-2 Ping6	324
4-3 Cable Diagnostics	325
4-4 Traceroute	327
Chapter 5 - Maintenance	329
5-1 Restart Device	329
5-2 Reboot Schedule	330
5-3 Factory Defaults	331
5-4 Firmware	332
5-4.1 Firmware Upgrade	332
5-3.2 Firmware Selection	335
5-4 Configuration	336
5-4.1 Save startup-config.....	336
5-4.3 Download.....	337
5-4.2 Upload	338
5-4.4 Activate	339
5-4.5 Delete	340
5-5 Server Report	341
Chapter 6 - DMS (Device Management System)	342
6-1 The DMS Tab	342
6-2 DMS Overview	342
6-2.1 DMS > DMS Mode > Information	343
6-4 Graphical Monitoring	346
PoE Auto Checking "AutoFill" Feature.....	351
Chapter 7 - Troubleshooting	366
Appendix A – DHCP Per Port and DHCP IP Per Port	368
Appendix B – Service, Warranty, and Tech Support	373
Appendix C –Compliance Information	373

Introduction

Product Description

The SM24TBT2DPB is a high performance Layer 2 managed switch with 52 Gbps switching capacity. It provides (24) 10/100/1000Mbps copper ports with IEEE 802.3bt PoE++ capability and (2) additional 100/1000Mbps dual speed SFP/RJ-45 combo ports. The SM24TBT2DPB complies with the latest IEEE 802.3bt PoE++ standard and supplies up to 90 Watts per port. It can provide full PoE++ output on all 24 ports when equipped with the dual hot-swappable PS-ACDC-1200 power supplies. This switch can be powered by low-line and high-line AC or DC power and Digital Electricity*, making it ideal for use in a wide variety of building applications. Model differences are noted where they apply.

Overview of this Manual

- Chapter 1 Operation of Web-based Management
- Chapter 2 System Configuration
- Chapter 3 Configuration
- Chapter 4 Monitor
- Chapter 5 Maintenance
- Chapter 6 DMS (Diagnostic Management System)
- Chapter 7 Troubleshooting
- Appendix A DHCP Per Port
- Appendix B Service, Warranty & Tech Support
- Appendix C Compliance Information

About This Manual

Purpose: This manual gives specific information on how to use the web-based management functions of the SM24TBT2DPx.

Audience: The manual is intended for use by network administrators who are responsible for operating and maintaining network equipment; consequently, it assumes a working knowledge of general switch functions, the Internet Protocol (IP), and Simple Network Management Protocol (SNMP).

Disclaimer: Lantronix does not warrant that the hardware will work properly in all environments and applications, and marks no warranty and representation, either implied or expressed, with respect to the quality, performance, merchantability, or fitness for a particular purpose. Lantronix disclaims liability for any inaccuracies or omissions that may have occurred. Information in this User Guide is subject to change without notice and does not represent a commitment on the part of Lantronix. Lantronix assumes no responsibility for any inaccuracies that may be contained in this User Guide. Lantronix makes no commitment to update or keep current the information in this User Guide and reserves the right to make improvements to this User Guide and/or to the products described in this User Guide, at any time without notice.

Related Manuals

These manuals give specific information on how to operate the web-based switch management functions:

- SM24TBT2DPA Quick Start Guide, 33736
- SM24TBT2DPA Install Guide, 33737
- SM24TBT2DPB Quick Start Guide, 33844
- SM24TBT2DPB Install Guide, 33845
- SM24TBT2DPA and DPB Web User Guide, 33738 (this manual)
- SM24TBT2DPA and DPB CLI Reference, 33739
- SM24TBT2DPA API User Guide, 33822
- Release Notes (version specific)

Go to the Lantronix [Resource Center](#) for Lantronix Firmware, Manuals, Tech Support, Knowledge Base, FAQs, etc. Note that this manual provides links to third part web sites for which Lantronix is not responsible.

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.

Chapter 1 - Web-based Management Operation

1-1 Initial Configuration

This chapter describes how to configure and manage the SM24TBT2DPx via the web user interface. The Web UI lets you easily configure and monitor switch functions from any switch port, including port activity, Spanning tree status, port aggregation status, multicast traffic, VLAN status, etc.

The default values are listed below:

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

After the SM24TBT2DPx interface configuration is finished, you can browse it. For instance, type `http://192.168.1.77` in the address row in a browser; the Login screen displays prompting you to enter a username and password in order to login and access authentication.


The default username is “admin” and password is “admin”. For first time use, enter the default username and password, and then click the <Login> button. The login process now is completed. In this login menu, you must enter the complete username and password respectively; the SM24TBT2DPx will not give you a shortcut to the username automatically.

The SM24TBT2DPx allows two or more admin users to manage this switch; the last configuration settings will be the configuration used by the system.

Note: When you login to manage the switch via Web/CLI, you must first type the Username of admin and Password admin, and then press Enter to access the Management page. When you log in to Web UI management, you can use either IPv4 or IPv6.

Note: The DHCP function is disabled by default, so if you do not have a DHCP server to provide IP addresses to the switch, the switch uses default IP address 192.168.1.77. The Login page is shown below:

LANTRONIX®

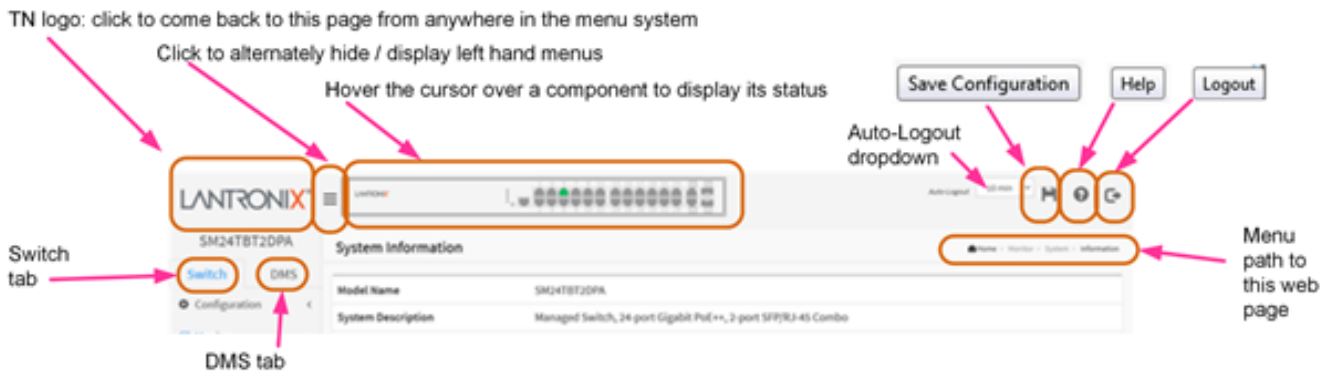


: Show Password text in entry field.



: Hide Password text in entry field (default).

The SM24TBT2DPx startup page (**Switch > Monitor > System > Information**) is shown below:

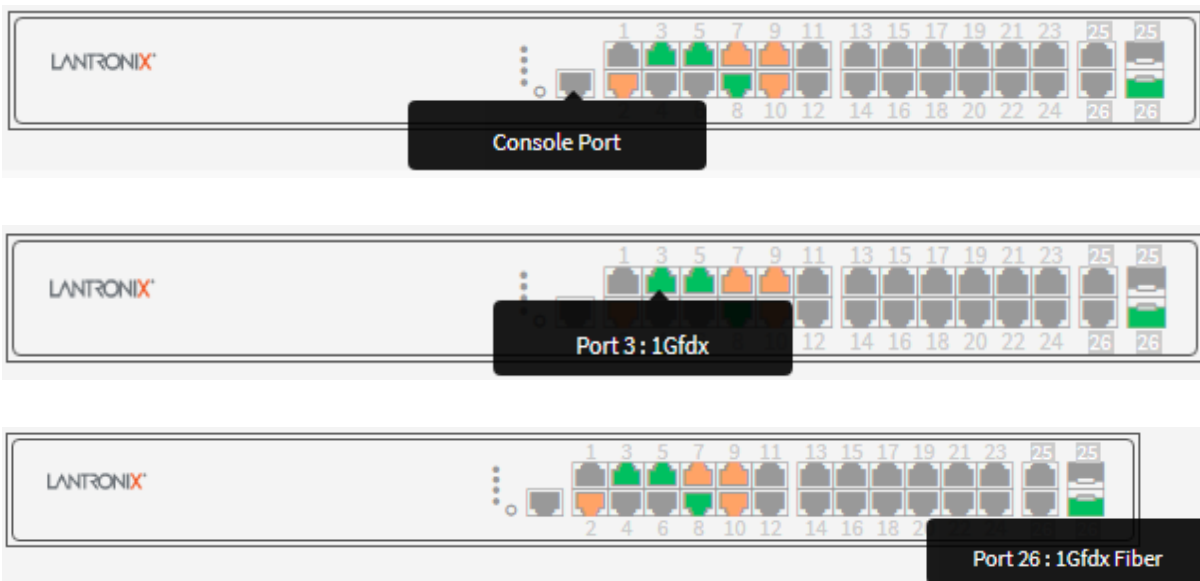


1-1.1 Web UI Controls

You can click the logo in the Web UI top left corner to come back to this page from anywhere in the menu system.

The Web UI top left corner displays an icon (☰) that alternately hides and displays the left hand menus.

The Web UI top left corner also displays a switch icon that lets you hover the cursor over a front panel component to display the status / description for that component (shown below). You can also click on a port to display that port's Detailed Port Statistics.



The Web UI top right corner displays a set of three icons (📁 ? 🏠) that let you Save Configuration, display online Help, and Logout. You can hover the cursor over any icon to display its function (Save Configuration Help Logout).

The Web UI top right corner also displays the currently displayed page's menu path (e.g., Home > Monitor > System > Information) as shown below:

🏠 Home > Monitor > System > Information

Auto-logout: The 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, 20, 30, 40, and 60 minutes (added at FW vB6.54.3494). The default is 10 minutes. When set to OFF, no Auto-logout occurs.

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

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

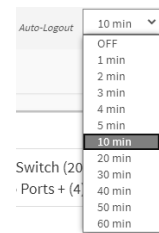
To save the timeout change to start-up config, you must execute a save to startup-config. To examine the running-config, you can run the CLI command “showing running-config” or in the Web UI just log out and log back in again.

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

In summary:

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

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



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

1-1.2 First Time Wizard

The first time you use this device you must configure some basic settings such as password, IP address, date and time, and system information. Use the following procedure:

Step 1: Change default password

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

Figure 2-1: Change default password

Step 2: Set IP address

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

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

Click the **Next** button.

Figure 2-2a: Set IP address

Set IP address

Interface VLAN ID
1

Obtain IP address via DHCP
 Set IP address manually

IP address
192.168.1.77

Subnet mask
255.255.255.0

Default router
192.168.1.254

DNS

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

[Previous](#) [Next](#)

Figure 2-2b: Set IP address

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

Step 3: Set date and time

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

Set date and time

Automatic date and time

Manually
2022-02-03 14:23:6

[Previous](#) [Next](#)

Figure 2-3: Set date and time

Step 4: Set system information

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

LANTRONIX®

1 2 3 4
PASSWORD IP ADDRESS DATE & TIME INFORMATION

Set system information

System contact

System name

System location

Figure 2-4: Set system information

Message: Password format error.

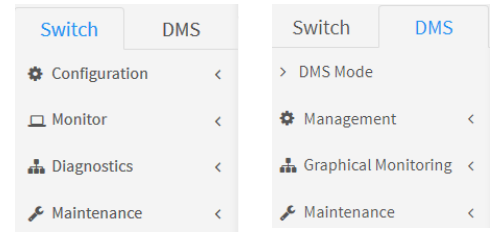
Message: The value of 'DNS' must be a valid IP address in dotted decimal notation ('x.y.z.w'). The following restrictions apply: 1) x, y, z, and w must be decimal numbers between 0 and 255, 2) x must not be 0 unless also y, z, and w are 0, 3) x must not be 127, and 4) x must not be greater than 223.

1-1.3 Web UI Modules

The SM24TBT2DPx Web UI management modules include:

Switch: Configuration, Monitor, Diagnostics, and Maintenance.

DMS: DMS Mode, Management, Graphical Monitoring, and Maintenance.



At startup, the Monitor > System > Information page displays.

LANTRONIX[®] SM24TBT2DPB

System Information

Model Name	SM24TBT2DPB
System Description	Managed Switch, 24-port Gigabit PoE++, 2-port SFP/RJ-45 Combo
Location	
Contact	
System Name	SM24TBT2DPB
System Date	2011-01-01T00:08:16+00:00
System Uptime	00:08:16
Bootloader Version	v1.15g
Firmware Version	VB6.64.0123 2024-05-27
PoE Firmware Version	200-352
Hardware Version	v3.01
Mechanical Version	v1.01
Serial Number	A206122AR2600005
MAC Address	00-c0-f2-89-a4-34
Memory	Total=70470 KBytes, Free=46899 KBytes, Max=46694 KBytes
FLASH	0x40000000-0x41fffff, 512 x 0x10000 blocks
CPU Load (100ms, 1s, 10s)	96%, 37%, 21%

The SM24TBT2DPx Web UI management modules are described in the following chapters.

Chapter 2 - System Configuration

This chapter describes basic configuration tasks including the System Information and other switch management (e.g., Power, IP, Time, Account, Syslog, NTP.)

2-1 System

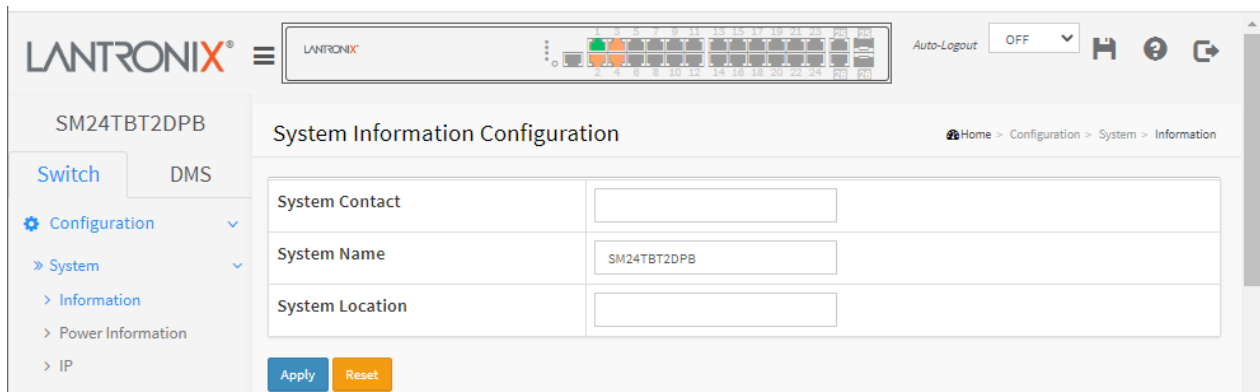
You can identify the switch by configuring the contact information, name, and location.

2-1.1 Information

Switch system contact information is provided here. To configure System Information in the web UI:

1. Click Configuration, System, Information.
2. Enter System Contact, System Name, and System Location information as desired.
3. Click Apply. The switch system information is displayed.

Figure 2-1.1: System Information Configuration page



The screenshot shows the Lantronix web interface for configuring system information on a switch. The device model is SM24TBT2DPB. The configuration page has a breadcrumb trail: Home > Configuration > System > Information. The main content area contains three rows of configuration fields:

System Contact	<input type="text"/>
System Name	<input type="text" value="SM24TBT2DPB"/>
System Location	<input type="text"/>

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

Parameter descriptions:

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

System Name: An administratively assigned name for this managed node. By convention, the system name may be the node's fully-qualified domain name. The allowed string length is 0 - 128 characters.

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

Buttons

Apply: Click to save changes.

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

2-1.2 Power Information (SM24TBT2DPA)

The SM24TBT2DPA Power Information page displays power related information for Power Supplies A and B. On the switch back panel: Left Power Module = A, Right Power Module = B. Note that the Configuration > PoE > Power Information page also has power supply settings. The screen below shows the SM24TBT2DPB with one PSU-HV power supply installed:

Power	A	B
Detected PSU	PSU-HV	PSU-HV
Power Good	Fail	Good
Power Input(AC/DC)	---	AC
Power Input Voltage (V)	0	120
FAN Speed (RPM)	0	4832
Temperature (Degree C)	27	44
Operating Mode	Boost	

Parameter descriptions:

Detected PSU: Displays the power sourcing unit that was detected (e.g., *PSU-HV* or *PSU-820* or *None*).

Power Good: Displays the power status (e.g., *Good* or *Fail*).

Power Input(AC/DC): Displays the type of power input (e.g., *AC*). Power Input is direct current or alternating current.

Power Input Voltage (V): Displays the amount of power input in Volts (e.g., *120* or *0*).

FAN Speed (RPM): Displays the fan speed in revolutions per minute (e.g., *2938* or *0*).

Temperature (Degree C): Displays the current switch temperature in degrees Celsius.

Operating Mode: At the dropdown select **Redundant** or **Boost**, where:

Redundant: Only provide Primary Power Supply up to 820W when two PSU-820 power supply modules are installed in the switch. If one power supply crashes, it can still provide enough power for system operation and also PD's operation. This is the default operating mode.

Boost: Power Supply up to 1640W when two PSU-820 power supply modules are installed in the switch. When the application total PDs' power use is over 820W, if one power supply crashes, system will be automatically rebooted due to power loading influence. After the switch finishes rebooting, it will only provide 820W to PDs.



Note that the Operating Mode setting also affects the Total PoE Available.

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 the changes.

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

2-1.2 Power Information (SM24TBT2DPB or DPB-2X)

The SM24TBT2DPB Power Information page displays power related information for Power Supplies A and B. Note that the Configuration > PoE > Power Information page also has power supply settings.

The SM24TBT2DPB ships with one PS-ACDC-1200 power supply, which lets it supply up to 90 Watts per port. The SM24TBT2DPB-2XPS, or SM24TBT2DPB with a second power supply added, can provide full PoE++ output on all 24-ports with its two hot-swappable PS-ACDC-1200 power supplies. (The PS-ACDC-1200 power supply displays as “PSU-HV” as shown below.)

See the SM24TBT2DPB Install Guide for more Power Supply Operating Mode Settings information.

When SM24TBT2DPB with two Power Supplies and Operating Mode = Redundant Mode:

The screenshot shows the Lantronix web interface for the SM24TBT2DPB. The main content area is titled "Power Information" and contains an "Auto-refresh" checkbox and a refresh icon. Below this is a table with two columns, "A" and "B", representing the two power supplies. The table lists various power-related metrics for each supply. At the bottom of the table, there is a dropdown menu for "Operating Mode" set to "Redundant", and "Apply" and "Reset" buttons.

	A	B
Detected PSU	PSU-HV	PSU-HV
Power Good	Good	Good
Power Input(AC/DC)	AC	AC
Power Input Voltage (V)	121	121
FAN Speed (RPM)	2880	3000
Temperature (Degree C)	41	42
Operating Mode	Redundant	

With Power Supply Operating Mode configured as “Redundant” Mode, the two power supplies are mutually redundant. If one of the power supplies fails, the other power supply can keep the system working normally. The PoE maximum output power of the two power supplies cannot be aggregated. The PoE maximum output Power Budget in “Redundant” Mode is equal to the PoE Budget of a single power supply.

With Power Supply Operating Mode set to Boost Mode:

- a.** When Power Supply Operating Mode is set to “Boost” mode, the power supply redundancy function will be disabled. If one of the power supplies fails, and the PoE power consumption is over the other power supply’s Max. PoE output power capability, the power supply will overload and shutdown this PoE switch.
- b.** The PoE maximum output power of the two power supplies can be aggregated. The PoE Max. PoE output Power Budget in Boost Mode is equal to the Power Supply A + Power Supply B.

SM24TBT2DPB-2XPS Power Supply Operating Mode = Redundant Mode (default):

The screenshot shows the 'Power Information' page for the SM24TBT2DPB switch. The 'Operating Mode' dropdown menu is open, showing 'Redundant' as the selected option. Below is a table of power-related metrics for Power A and Power B.

	A	B
Detected PSU	PSU-HV	PSU-HV
Power Good	Good	Good
FAN Speed (RPM)	3053	3018
Temperature (Degree C)	42	43

SM24TBT2DPB-2XPS Power Supply Operating Mode = Boost Mode Information:

The screenshot shows the 'Power Information' page for the SM24TBT2DPB switch. The 'Operating Mode' dropdown menu is set to 'Boost'. Below is a table of power-related metrics for Power A and Power B.

	A	B
Detected PSU	PSU-HV	PSU-HV
Power Good	Good	Good
FAN Speed (RPM)	2889	3024
Temperature (Degree C)	42	43

Buttons:

Apply: Click to save the 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: Click to refresh the page immediately.

Power Module Monitoring Change

SM24TBT2DPB FW VB6.64.0079 changed the way that the switch power supplies are monitored:

1. When the system is turned on and the switch finds that Power A and B are different PSUs, the management software will turn off 920W PSU output power.
2. When the system has just one PSU working, and then insert a second PSU is inserted into a power slot, if the second PSU inserted is a different than the existing PSU, the second PSU inserted will have its output power turned off.
3. When Power A and B are different PSUs, the PoE Power Budget will maintain the status quo and will not be recalculated and adjusted.
4. When Power A and B are different, then the power module Event Log and Trap are different for Power A and B.

2-1.4 IP

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

Configure the switch-managed IP information on this page (IP basic settings, control IP interfaces and IP routes). The maximum number of interfaces supported is 8 and the maximum number of routes is 32. See [Appendix A – DHCP Per Port](#) on page 368 for more DHCP Per Port information.

To configure IP parameters in the web UI:

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

Figure 2-1.2: IP Configuration page

The screenshot displays the IP Configuration page in the Lantronix web UI. The page is titled "IP Configuration" and is part of the "System" configuration for device "SM24TBT2DPB". The left sidebar shows a navigation menu with "Configuration" expanded to "System" and "IP" selected. The main content area includes the following sections:

- Mode:** Host (dropdown)
- DNS Server:** Configured (dropdown) with value 8.8.8.8
- DNS Proxy:**
- IP Interfaces:**
 - DHCP Per Port:**
 - Mode:** Disabled (dropdown)
 - VLAN:** VLAN 1 (dropdown)
 - IP:** [] - []
 - Table:**

Delete	VLAN	IPv4 DHCP		Current Lease	IPv4		IPv6	
		Enable	Fallback		Address	Mask Length	Address	Mask Length
<input type="checkbox"/>	1	<input type="checkbox"/>	0		192.168.1.77	24		
- Link-Local Address binding interface:** VLAN 1 (dropdown)
- Gateway Address binding interface:** VLAN 1 (dropdown)
- IP Routes:**

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

Buttons at the bottom include "Add Interface", "Add Route", "Apply", and "Reset".

Parameter descriptions:

IP Configuration

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

DNS Server: This setting controls the DNS name resolution done by the switch. The modes are:

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

No DNS server: No DNS server will be used.

Configured: Explicitly provide the IP address of the DNS Server in dotted decimal notation.

From this DHCP interface: Specify from which DHCP-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.

IP Interfaces

DHCP Per Port: The assign an IP address based on the switch port the device is connected to. This will speed up installations of IP cameras, cameras can be configured after they are on the network.

The per-port assignment allows you to know which IP was assigned to which camera. See [Appendix A – DHCP Per Port](#) on page 368 for more DHCP Per Port information. The parameters are:

Mode : Enable/Disable DHCP per port. The default is Disabled.

VLAN : Select a DHCP per port VLAN.

IP : Define the IP range for DHCP per port (e.g., 192.168.1.78 - 192.168.1.93).

DHCP Per Port	
Mode	Disabled ▾
VLAN	VLAN 1 ▾
IP	192.168.1.1 - 192.168.1.100

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

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

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

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

IPv4 Mask Length: The IPv4 network mask, in number of bits (prefix length). Valid values are between 0 and 30 bits for an IPv4 address. If DHCP is enabled, this field is not used. The field may also be left blank if IPv4 operation on the interface is not desired.

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

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

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

Link-Local Address binding interface: Configure Link-Local IP address to a different VLAN interface. The first IP interface entry (169.254.xx.xx) is for the default value (VLAN 1).

A link-local address is a unicast address having link-only scope that can be used to reach neighbors. All interfaces on routers must have a link-local address. Also, ADDRCONF requires that interfaces on hosts have a link-local address.

For more information see the Microsoft MSDN article [IPv6 Link-local and Site-local Addresses](#) or IETF [RFC 4861](#).

Gateway Address binding interface: A DHCP client uses the DHCP protocol to get the gateway an address and sets the gateway address to the interface of the binding.

IP Routes

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

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

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

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

Next Hop VLAN (Only for IPv6): The VLAN ID (VID) of the specific IPv6 interface associated with the gateway. The VID ranges from 1 - 4094 and will be effective only when the corresponding IPv6 interface is valid.

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

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

Buttons

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

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

Apply: Click to save changes. At the *Update success!* dialog click the **OK** button.

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

Messages:

Message: *Update success!* displays to indicate the on-screen change was applied (saved). After a series of applied changes, a checkbox (Prevent this page from creating additional dialogs) also displays; check the checkbox to apply changes without displaying this dialog box at each update. Click the **OK** button to close the dialog box.

Message: *DHCP Per Port IP range (192.168.1.1 - 192.168.1.100) includes interface IP address (192.168.1.77)* displays if you included the switch IP address in the DHCP Per Port IP range. Click the **OK** button to clear the message and enter a range that does not include the switch IP address.

Message: *Invalid DHCP Per Port IP range (-)* displays if the IP address range you entered is invalid. Click the **OK** button to clear the message and enter a range that is valid for your system and that does not include the switch IP address. You could also disable the DHCP Per Port IP feature.

Message: *DHCP Per Port IP range (1.2.3.4 - 1.5.6.7) is not within interface subnet (192.168.1.77/24)* Click the **OK** button to clear the message and enter an IP range within the switch subnet.

2-1.3 NTP

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

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

To configure NTP in the UI:

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

Figure 2-1.3: NTP Configuration page

The screenshot shows the NTP Configuration page in the Lantronix web interface. The device is identified as SM24TBT2DPA. The configuration area includes:

- Automatic:** A dropdown menu currently set to "Disabled".
- Server address via DHCP:** An empty text input field.
- NTP Time-Sync Interval:** A dropdown menu currently set to "60".
- Server address 1 to 5:** Five empty text input fields for specifying NTP server addresses.
- Buttons:** "Apply" (blue) and "Reset" (orange) buttons at the bottom of the configuration area.

Parameter descriptions:

Automatic: Indicates the NTP mode of operation. Possible modes are:

Enabled: Enable NTP client mode operation; NTP servers available from the DHCP.

Disabled: Disable NTP client mode operation; NTP servers available from the config (default).

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

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

Buttons:

Apply : Click to save changes.

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

2-1.4 Time

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

To configure Time parameters in the web UI:

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

Figure 2-1.4: Time Configuration page

The screenshot displays the 'Time Configuration' page in the Lantronix web UI. The page is titled 'Time Configuration' and includes a breadcrumb trail: Home > Configuration > System > Time. The left sidebar shows the navigation menu with 'Time' selected. The main content area is divided into several sections:

- Time Configuration:**
 - Clock Source:** A dropdown menu set to 'Use Local Settings'.
 - System Date:** A text input field containing '2022-03-15 16:54:32' with a placeholder '(yyyy-mm-dd hh:mm:ss)'.
- Time Zone Configuration:**
 - Time Zone:** A dropdown menu set to 'None'.
 - Acronym:** A text input field with a placeholder '(0 - 16 characters)'.
- Daylight Saving Time Configuration:**
 - Daylight Saving Time:** A dropdown menu set to 'Disabled'.
- Start Time settings:**
 - Month:** A dropdown menu set to 'Jan'.
 - Date:** A dropdown menu set to '1'.
 - Year:** A dropdown menu set to '2000'.
 - Hours:** A dropdown menu set to '0'.
 - Minutes:** A dropdown menu set to '0'.
- End Time settings:**
 - Month:** A dropdown menu set to 'Jan'.
 - Date:** A dropdown menu set to '1'.
 - Year:** A dropdown menu set to '2000'.
 - Hours:** A dropdown menu set to '0'.
 - Minutes:** A dropdown menu set to '0'.
- Offset settings:**
 - Offset:** A text input field containing '1' with a placeholder '(1 - 1440) Minutes'.

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

Parameter descriptions:

Time Configuration

Clock Source: There are two modes for configuring the Clock Source. Select "Use Local Settings" (default) or select "Use NTP Server" to display the NTP Server configurable parameters.

System Date: Show the current time of the system. The year of system date can be from 2011 to 2037. The format is yyyy:mm:dd hh:mm:ss (year:month:day hour:minute:second).

Time Zone Configuration

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

Acronym: Set an acronym for the time zone. This is a user configurable acronym to identify the time zone. (Range: up to 16 characters.)

Daylight Saving Time Configuration

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

Recurring Configuration

Start time settings:

Week - Select the starting week number.

Day - Select the starting day.

Month - Select the starting month.

Hours - Select the starting hour.

Minutes - Select the starting minute.

End time settings:

Week - Select the ending week number.

Day - Select the ending day.

Month - Select the ending month.

Hours - Select the ending hour.

Minutes - Select the ending minute.

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



NOTE: The entry under “Start Time Settings” and “End Time Settings” displays what you set on the “Start Time Settings” and “End Time Settings” field information.

Buttons:

Apply – Click to save changes.

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

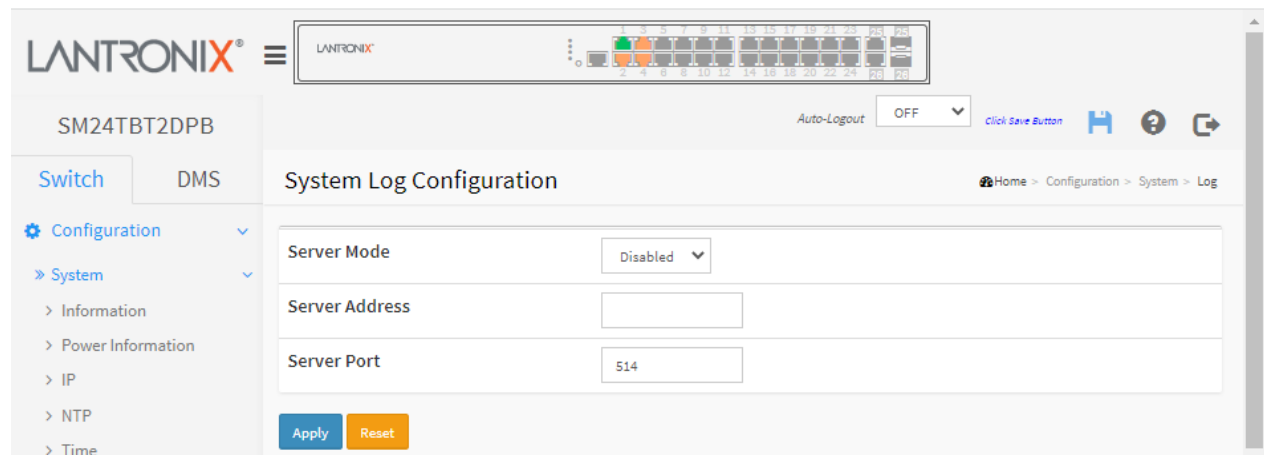
2-1.5 Log

Syslog is a standard for logging program messages. It allows separation of the software that generates messages from the system that stores them and the software that reports and analyzes them. It can also be used for generalized informational, analysis and debugging messages. Syslog is supported by a wide variety of devices and receivers across multiple platforms.

To configure Syslog in the web UI:

1. Click Configuration, System, and Log.
2. Specify the syslog server IP Address and Port number.
3. At the Server Mode dropdown, select Enabled to enable Syslog Server mode.
4. Click the Apply button.

Figure 2-1.5: System Log Configuration page



The screenshot shows the Lantronix web interface for the SM24TBT2DPB device. The page title is 'System Log Configuration'. The left sidebar shows a navigation menu with 'Configuration' and 'System' expanded. The main content area has three input fields: 'Server Mode' (a dropdown menu currently set to 'Disabled'), 'Server Address' (an empty text box), and 'Server Port' (a text box containing '514'). At the bottom of the form are two buttons: 'Apply' (blue) and 'Reset' (orange). The top of the page shows the Lantronix logo, a status bar with 'Auto-Logout OFF', and a breadcrumb trail: 'Home > Configuration > System > Log'.

Parameter descriptions:

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

Enabled: Enable server mode operation.

Disabled: Disable server mode operation.

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

Server Port: Enter the port number for the syslog server. The default is port 514.

Buttons:

Apply – Click to save changes.

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

You can view the logged messages at the **Monitor > System > Log** page.

2-2 Green Ethernet

Energy Efficient Ethernet (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 called wakeup time. The default wakeup time is 17 us for 1Gbit links and 30 us for other link speeds. EEE devices must agree on 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 Mbps full duplex mode. For ports that are not EEE-capable the corresponding EEE checkboxes are grayed out and thus impossible to enable EEE.

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

Web Interface

To configure Port Power Savings in the web UI:

1. Click Configuration, Green Ethernet, Port Power Savings.
2. At the dropdown, select to optimize EEE for either Latency or Power.
3. Enable or disable the EEE and EEE Urgent Queues for each port.
4. Click the Apply button.

Figure 2-2.1: Port Power Savings Configuration

The screenshot shows the web interface for configuring Port Power Savings on a Lantronix switch. The page title is "Port Power Savings Configuration". At the top, there is a dropdown menu labeled "Optimize EEE for" with "Latency" selected. Below this is a "Port Configuration" table with columns for "Port", "EEE", and "EEE Urgent Queues" (1 through 8). Each cell in the table contains a checkbox.

Port	EEE	EEE Urgent Queues							
		1	2	3	4	5	6	7	8
*	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
1	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
2	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
3	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
4	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
5	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
6	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
7	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
8	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Parameter descriptions:

Optimize EEE for: The switch can be set to optimize EEE for either Power (best power saving) or Latency (least traffic latency). The default is Latency.

Port: The switch port number of the logical port.

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

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

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

Buttons:

Apply – Click to save changes.

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

2-3 Ports Configuration

This section lets you configure the detailed switch Port parameters, enable or disable switch ports, and monitor the ports' status.

2-3.1 Ports

This page lets you view and configure current port parameters.

1. Click Configuration, Ports Configuration, and Ports.
2. Specify Speed Configured, Flow Control, and Maximum Frame size.
3. Click Apply.

Figure 2-3.1: Ports Configuration page

Port	Link	Speed		Flow Control			Maximum Frame Size
		Current	Configured	Current Rx	Current Tx	Configured	
*			<>			<input type="checkbox"/>	9600
1	●	1Gfdx	Auto	⊘	⊘	<input type="checkbox"/>	9600
2	●	100fdx	Auto	⊘	⊘	<input type="checkbox"/>	9600
3	●	100fdx	Auto	⊘	⊘	<input type="checkbox"/>	9600
4	●	100fdx	Auto	⊘	⊘	<input type="checkbox"/>	9600
5	●	100fdx	Auto	⊘	⊘	<input type="checkbox"/>	9600
6	●	Down	Auto	⊘	⊘	<input type="checkbox"/>	9600
7	●	Down	Auto	⊘	⊘	<input type="checkbox"/>	9600
8	●	Down	Auto	⊘	⊘	<input type="checkbox"/>	9600

Parameter descriptions:

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

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

Current Link Speed: Provides the current link speed of the port (e.g., 1Gfdx or Disabled).

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

Disabled - Disables the switch port operation.

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

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

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

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

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

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

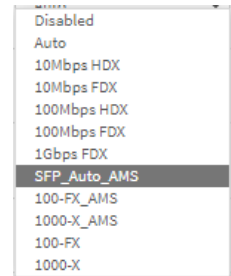
SFP_Auto_AMS - Automatically determines the speed of the SFP. Note: There is no standardized way to do SFP auto detect, so here it is done by reading the SFP rom. Due to the missing standardized way of doing SFP auto detect, some SFPs might not be detectable. The port is set to AMS mode. The copper port is set to Auto mode.

100-FX - SFP port in 100-FX speed. Copper port disabled.

100-FX_AMS - Port in AMS mode. SFP port in 100-FX speed. Copper port in Auto mode.

1000-X - SFP port in 1000-X speed. Copper port disabled.

1000-X_AMS - Port in AMS mode. SFP port in 1000-X speed. Cu port in Auto mode. Ports in AMS mode with 1000-X speed have copper port preferred. Ports in AMS mode with 100-FX speed have fiber port preferred.



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.

Maximum Frame Size: Enter the maximum frame size allowed for the switch port, including FCS. This must be an integer value of 1518 - 9600 bytes.

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 Port link Status manually.

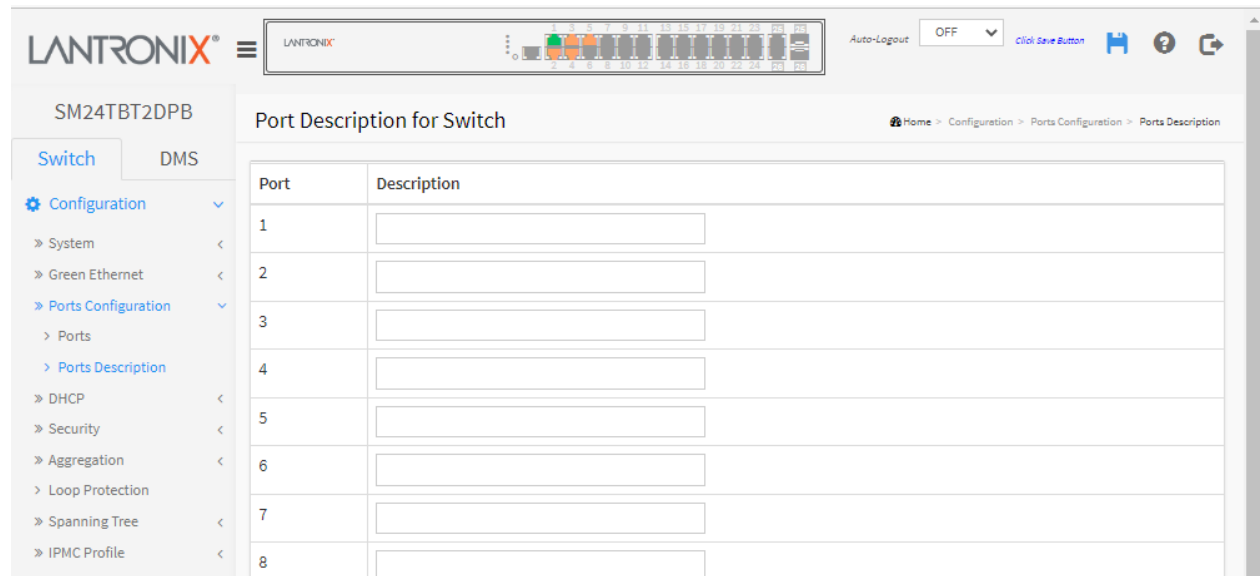
2-3.2 Ports Description

This page lets you enter ports' descriptions. You can enter an alphanumeric string describing the port name and version identification for the system's hardware type, software version, or network application.

To configure Port Descriptions in the web UI:

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

Figure 2-3.1: Port Description for Switch page



Parameter descriptions:

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

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

Buttons

Apply – Click to save changes.

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

2-4 DHCP

This page configures global mode and VLAN mode to enable/disable DHCP server per system and per VLAN.

2-4.1 Server

2-4.1.1 Mode

This page configures global mode and VLAN mode to enable/disable DHCP server per system and per VLAN. A **DHCP Server** is used to allocate network addresses and deliver configuration parameters to dynamically configured hosts called DHCP clients.

To configure DHCP server mode in the web UI:

1. Click Configuration, DHCP, Server, Mode.
2. Add VLAN Range.
3. Select "Enabled" in the Mode column.
4. Click Apply.

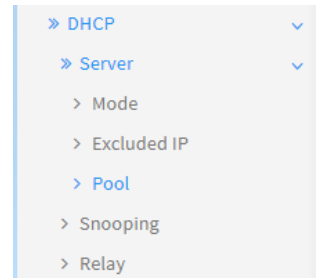
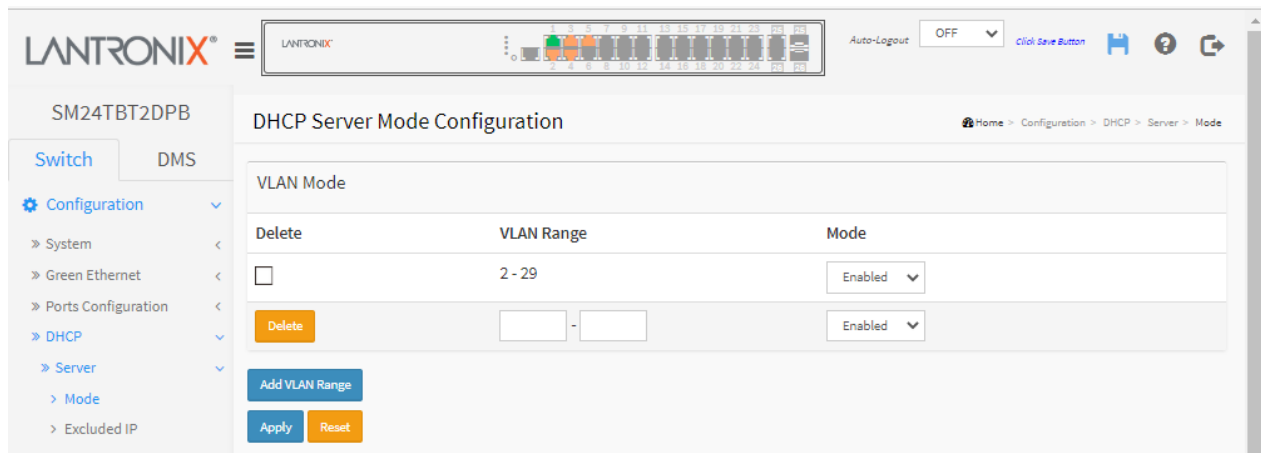


Figure 2-4.1.1: DHCP Server Mode Configuration page



Parameter descriptions:

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

Otherwise, if you want to disable an existing VLAN range, follow these steps:

1. Click "Add VLAN Range" to add a new VLAN range.
2. Input the VLAN range that you want to disable.
3. Set Mode to Disabled.
4. Click **Apply** to apply the changes. The disabled VLAN range is removed from the DHCP Server mode configuration page.

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

Enabled: Enable DHCP server per VLAN.

Disabled: Disable DHCP server per VLAN.

Buttons

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

Apply – Click to save changes.

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

Messages:

Message: *dhcp_server_pool_set(Pool2) error(-995)*

Meaning: DHCP per Port and DHCP Pool per VLAN cannot be enabled at same time; DHCP per port and DHCP pool per VLAN are mutually exclusive.

Recovery: Use either DHCP per Port or DHCP Pool per VLAN, but not both.

Message: *Update success!*

Meaning: You made changes, clicked the Apply button, and the changes were saved.

Recovery: None required.

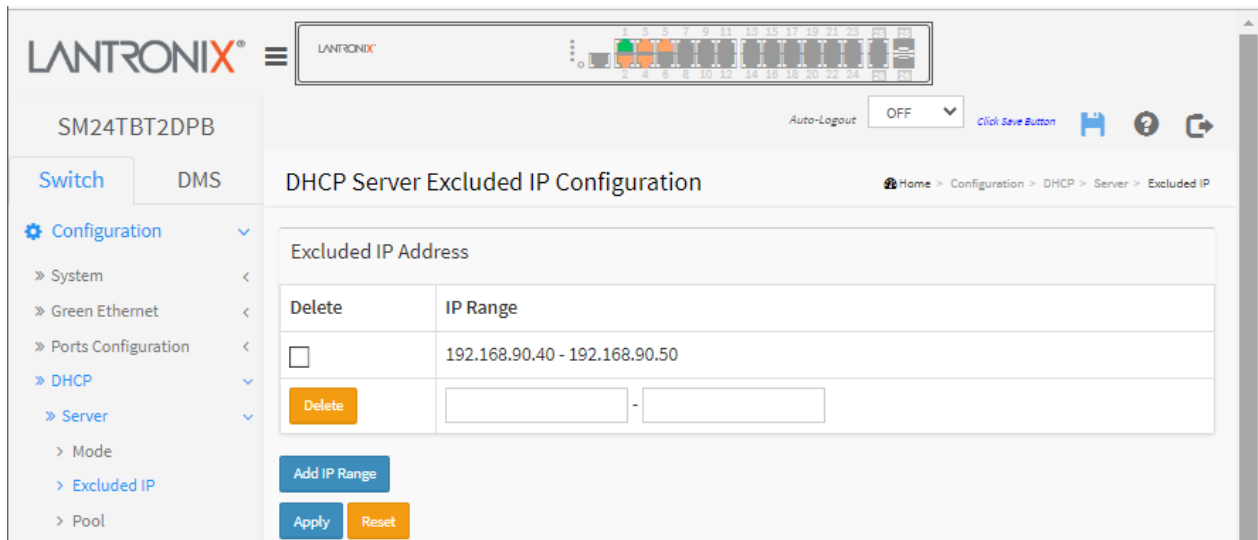
2-4.1.2 Excluded IP

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

To configure DHCP server excluded IPs in the web UI:

1. Click Configuration, DHCP, Server, Excluded IP.
2. Click Add IP Range then you can create new IP Range on the switch.
3. Click Apply.

Figure 2-4.1.2: DHCP Server Excluded IP Configuration page



Parameter descriptions:

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

Buttons

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

Apply – Click to save changes.

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

Messages:

The value of Excluded low IP address, 192.168.1.300, must be a valid IP address in dotted decimal notation ('x.y.z.w), where x, y, z, and w are decimal numbers between 0 and 255.

2-4.1.3 Pool

This page lets you manage DHCP pools. According to the DHCP pool, a DHCP server will allocate IP address and deliver configuration parameters to DHCP client. See the IANA [DHCP Parameters](#) webpage or the IETF [RFC 2132](#) webpage for DHCP option parameter descriptions.

To configure DHCP server pool in the web UI:

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

Figure 2-4.1.1: DHCP Server Pool Configuration page

The screenshot displays the 'DHCP Server Pool Configuration' page in the Lantronix web UI. The page features a navigation menu on the left with 'Configuration' expanded to 'Server' and 'Pool'. The main content area shows a table of DHCP pools. The table has columns for 'Delete', 'Name', 'Type', 'IP or IP Start', 'Subnet Mask or IP End', and 'Lease Time'. Three pools are listed: 'DHCP_per_Port', 'DHCP_per_VLAN', and 'DHCP_per_IP'. Each row has a checkbox in the 'Delete' column. Below the table are buttons for 'Add New Pool', 'Apply', and 'Reset'. The 'DHCP_per_IP' row has a 'Delete' button and a text input field containing 'DHCP_per_IP'.

Delete	Name	Type	IP or IP Start	Subnet Mask or IP End	Lease Time
<input type="checkbox"/>	DHCP_per_Port	-	-	-	1 days 0 hours 0 minutes
<input type="checkbox"/>	DHCP_per_VLAN	-	-	-	1 days 0 hours 0 minutes
<input type="checkbox"/>	DHCP_per_IP	-	-	-	1 days 0 hours 0 minutes

Parameter descriptions:

Pool Setting: Add or delete pools. Adding a pool and giving it a name to creates a new pool with a "default" configuration. To configure all settings including type, IP subnet mask and lease time, click the linked pool name to go into the pool configuration page.

Name: Configure a pool name using any printable character except the space character (e.g., DHCP-Per_Pool or DHCP_Per_Port). To configure detailed settings, click the linked pool name to go to its configuration page (see below).

Type: Display which type the pool is.

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

Host: the pool services for a specific DHCP client identified by client identifier or hardware address. If "-" is displayed, it means "not defined".

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

IP or IP Start: Enter an IP address or a starting IP Address (IP Start added at FW vB6.54.3494). See "DHCP Pool per VLAN" below.

Subnet Mask or IP End: Enter a Subnet Mask or an ending IP Address (IP End added at FW vB6.54.3494). See "DHCP Pool per VLAN" below.

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

Lease Time: Display lease time of the pool.

Buttons

Delete: Delete the selected row.

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

Apply – Click to save changes.

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

After you define a new pool and click Apply, the page re-displays with the new configuration:

Click on a Pool Setting Name from the **Configuration > DHCP > Server > Pool** menu path to display the DHCP Pool Configuration page. See the [Internet Assigned Numbers Authority](#) (IANA) webpage.

The screenshot displays the DHCP Pool Configuration page. The form includes the following fields and values:

Field	Value
Name	DHCP-Per_Pool
Pool Name	DHCP-Per_Pool
Type	Network
IP or IP Start	192.168.1.1
Subnet Mask or IP End	192.168.1.25
Lease Time	90 days (0-365)
	0 hours (0-23)
	0 minutes (0-59)
Domain Name	
Broadcast Address	
Default Router	
DNS Server	
TFTP Server	
Boot File	
NTP Server	

Parameter descriptions:

Name: Displays the selected pool name.

Type: Specify which type of the pool is.

None: no pool type.

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

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

IP: Specify network number of the DHCP address pool.

IP or IP Start: Enter an IP address or a starting IP Address (IP Start added at FW vB6.54.3494). See “DHCP Pool per VLAN” below.

Subnet Mask or IP End: Enter a Subnet Mask or an ending IP Address (IP End added at FW vB6.54.3494). See “DHCP Pool per VLAN” below.

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

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

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

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

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

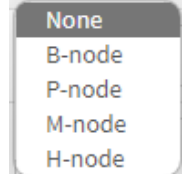
DNS Server: DHCP option 6. Specify a list of Domain Name System name servers available to the client.

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

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

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

NetBIOS Node Type: DHCP option 46. At the dropdown select a NetBIOS node type option to allow Netbios over TCP/IP clients which are configurable as described in IETF [RFC 1001](#) and [RFC 1002](#). The options are **None** (default), **B-node**, **P-node**, **M-node**, and **H-node**.



NetBIOS Scope: DHCP option 47. Specify the NetBIOS over TCP/IP scope parameter for the client as specified in IETF [RFC 1001](#) and [RFC 1002](#).

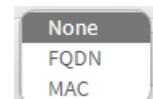
NetBIOS Name Server: DHCP option 44. Specify a list of NBNS name servers listed in order of preference.

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

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

NIS Domain Name	<input type="text"/>
NIS Server	<input type="text"/>
	<input type="text"/>
	<input type="text"/>
	<input type="text"/>
Client Identifier	None <input type="button" value="v"/> <input type="text"/>
Hardware Address	<input type="text"/>
Client Name	<input type="text"/>
Vendor 1 Class Identifier	<input type="text"/>
Vendor 1 Specific Information	<input type="text"/>
Vendor 2 Class Identifier	<input type="text"/>
Vendor 2 Specific Information	<input type="text"/>
Vendor 3 Class Identifier	<input type="text"/>
Vendor 3 Specific Information	<input type="text"/>
Vendor 4 Class Identifier	<input type="text"/>
Vendor 4 Specific Information	<input type="text"/>
Vendor 5 Class Identifier	<input type="text"/>
Vendor 5 Specific Information	<input type="text"/>
Vendor 6 Class Identifier	<input type="text"/>
Vendor 6 Specific Information	<input type="text"/>
Vendor 7 Class Identifier	<input type="text"/>
Vendor 7 Specific Information	<input type="text"/>
Vendor 8 Class Identifier	<input type="text"/>
Vendor 8 Specific Information	<input type="text"/>
Lighting Server	<input type="text"/>

Client Identifier: DHCP option 61. Specify client's unique identifier to be used when the pool is the type of host. The options are **None** (default), **FQDN** (fully-qualified domain name), and **MAC**.



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

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

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

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

Lighting Server: DHCP option 229. Specify a lighting server available to the client. This feature should be enabled for any ports used for lighting nodes as it significantly reduces the delay time between when a lighting node is connected to a port and when the switch allows network communication from the lighting node to the lighting gateway.

Note: If multicast traffic is not allowed on your network, you can configure the network DHCP server to pass the lighting gateway server IP address in DHCP Option 229. (Added at FW v7.20.0106.)

Specifications:

1. With the switch acting as DHCP Server, it will insert option 229 into DHCP offer packets and DHCP ack packets.
2. After receiving DHCP discover packets, it will insert option 229 for all DHCP clients as long as the DHCP Server is configured with Option 229.
3. The option is configurable via the UI, SNMP, and CLI, and there are Help descriptions in the Web UI and CLI.
4. The code for this option is 229, and its length is 4 octets:

Code Len Address:

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

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

Buttons

Apply – Click to save changes.

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

Messages:

Update success!

Pool type is defined so IP must be inputted.

Pool type is defined so subnet mask must be inputted.

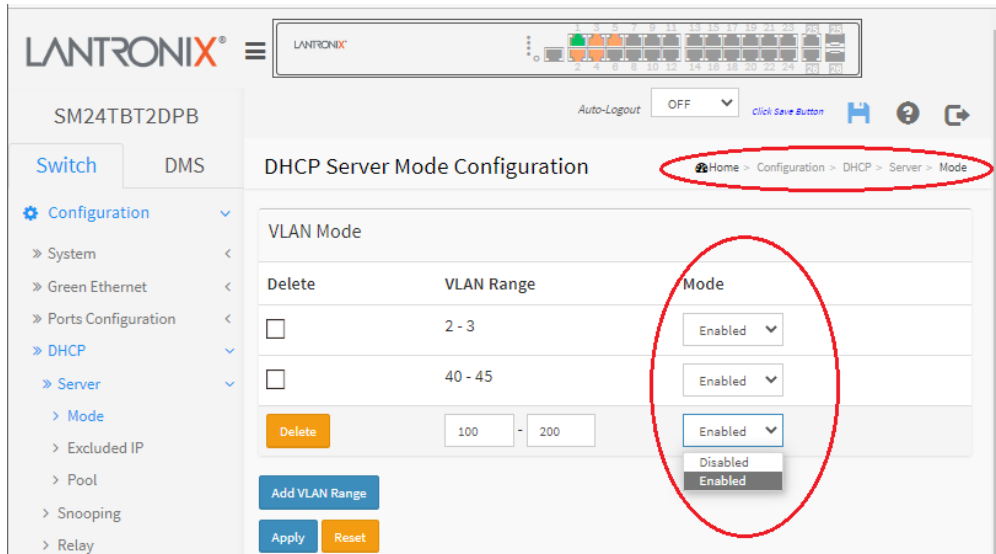
Pool's IP/netmask does not match interfaces' IP/netmask, or DHCP server mode isn't enabled on a correct VLAN range.

Pool name, POOL # 3, can not contain SPACE.

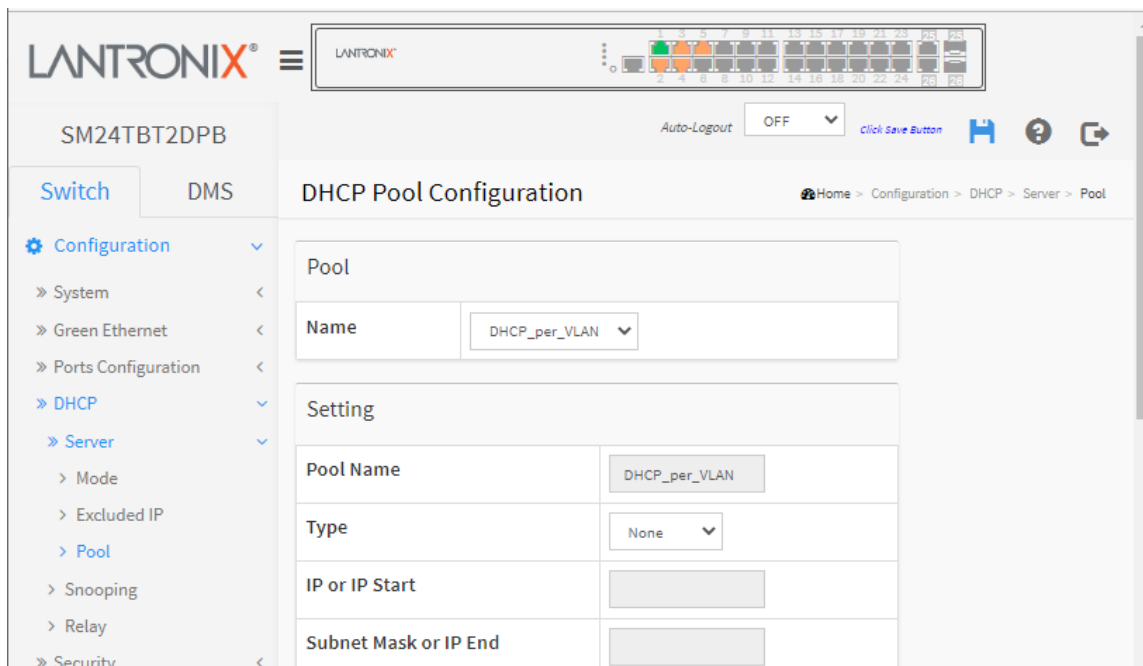
DHCP Pool per VLAN

SM24TBT2DPA switch firmware before vB6.54.3494 does not let you build a DHCP pool without creating a new IP Interface and assigning an IP Address with that same subnet in the IP Address of the pool. When you wanted to disable DHCP, the only way was to delete the VLAN Range.

With SM24TBT2DPA FW vB6.54.3494 and above you can now choose Enable or Disable at the Mode dropdown; there is no need to delete the VLAN Range. **Note:** do not operate DHCP Per Port and DHCP Pool per VLAN at the same time. If you configure entries for DHCP Pool per VLAN and then enable DHCP per Port, the configured DHCP pool will be deleted.



- Use one of two ways to configure the DHCP Address Pool:
 - Use an IP Address and a Subnet Mask, or
 - Use an IP Address Range. When the switch detects the first three digits in the Subnet Mask field, the switch will use the IP address range defined for the DHCP Address Pool.
- Set up a new DHCP Pool without setting the IP Interface and VLAN.



2-4.2 Snooping

DHCP Snooping is used to block intruders on the untrusted ports of the switch device when it tries to intervene by injecting a bogus DHCP reply packet to a legitimate conversation between the DHCP client and server.

This page lets you configure the DHCP Snooping parameters of the switch. DHCP Snooping can prevent attackers from adding their own DHCP servers to the network.

To configure DHCP snooping in the web UI:

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

Figure 2-4.2: DHCP Snooping Configuration page

The screenshot shows the Lantronix web interface for the SM24TBT2DPB switch. The main content area is titled 'DHCP Snooping Configuration'. At the top, there is a 'Snooping Mode' dropdown menu currently set to 'Disabled'. Below this is a 'Port Mode Configuration' section containing a table with two columns: 'Port' and 'Mode'. The table lists ports 1 through 6, with each port's mode set to 'Trusted'. A breadcrumb trail at the top right reads 'Home > Configuration > DHCP > Snooping'. On the left, a navigation menu is visible with 'DHCP' and 'Snooping' highlighted.

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

Parameter descriptions:

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

Enabled: Enable DHCP snooping mode operation. When DHCP snooping mode operation is enabled, the DHCP request messages will be forwarded to trusted ports and only allow reply packets from trusted ports.

Disabled: Disable DHCP snooping mode operation.

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

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

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

Buttons

Apply – Click to save changes.

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

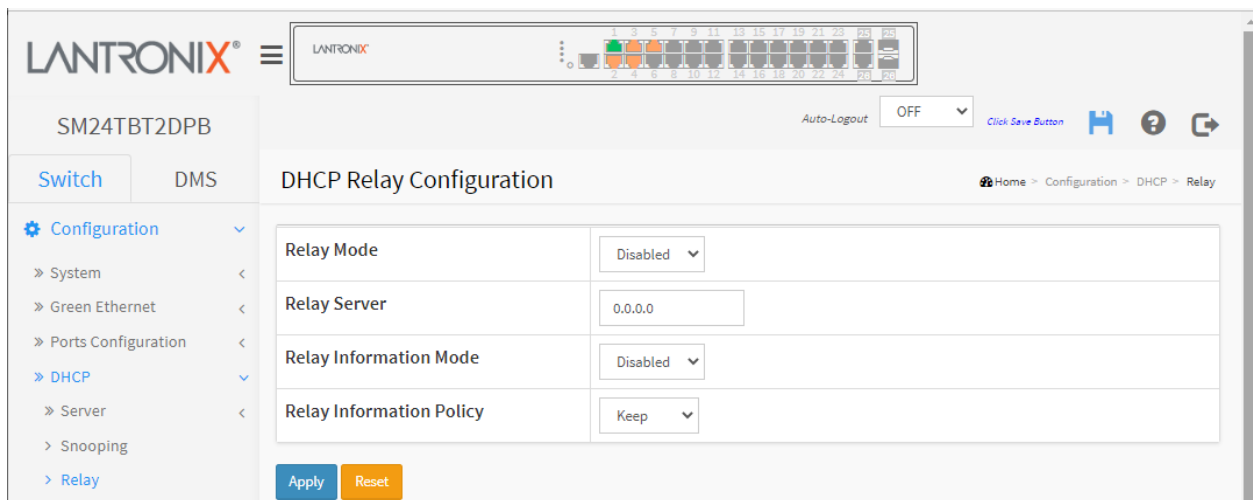
2-4.3 Relay

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

To configure DHCP Relay in the web UI:

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

Figure 2-4.3: DHCP Relay Configuration page



Parameter descriptions:

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

Enabled: Enable DHCP relay mode operation. When DHCP relay mode operation is enabled, the agent forwards and transfers DHCP messages between the clients and the server when they are not in the same subnet domain. And the DHCP broadcast message won't be flooded for security considerations.

Disabled: Disable DHCP relay mode operation.

Relay Server: Indicates the DHCP relay server IP address.

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

Possible modes are:

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

Disabled: Disable DHCP relay information mode operation.

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

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

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

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

Buttons

Apply – Click to save changes.

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

Message: *Please make sure the DHCP server connected on trust port?* displays to ensure the DHCP server is connected to a trusted port on the switch. Verify that is the case and click the **OK** button.

2-5 Security

This section lets you add, edit, and delete users and configure Switch Security settings. You can use the Port Security feature to restrict input to an interface by limiting and identifying MAC addresses.

2-5.1 Switch

2-5.1.1 Users

This page displays existing users. Currently the only way to login as another user on the web UI is to close and reopen the browser. To configure Users in the web UI:

1. Click Configuration, Security, Switch, Users.
2. Click the Add New User button.
3. Specify the User Name, Password, and Privilege Level parameters.
4. Click Apply.

Figure 2-5.1.1: Users Configuration page

The screenshot shows the Lantronix web interface for configuring a user. The breadcrumb trail is Home > Configuration > Security > Switch > Users. The 'Add User' form includes the following fields:

- User Name:** A text input field.
- Password:** A text input field.
- Password (again):** A text input field for password confirmation.
- Privilege Level:** A dropdown menu currently set to 0.

At the bottom of the form are three buttons: 'Apply' (blue), 'Reset' (orange), and 'Cancel' (blue).

Parameter descriptions:

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

Password: Type the password. The allowed string length is 0 – 255 characters, and the allowed content is ASCII characters 32 - 126.

Password (again): Type the password again. You must type the same password again in the field.

Privilege Level: The privilege level of the user. The allowed range is level 0-15. If the privilege level 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. A User's privilege should be same or greater than the group privilege level to have the access of that group. By default, most groups' privilege level 5 has the read-only access and privilege level 10 has read-write access. The system maintenance (software upload, factory defaults and 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. You are logged out of the system and can then log in again as any valid user.

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

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

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

Users Configuration page: - new user added

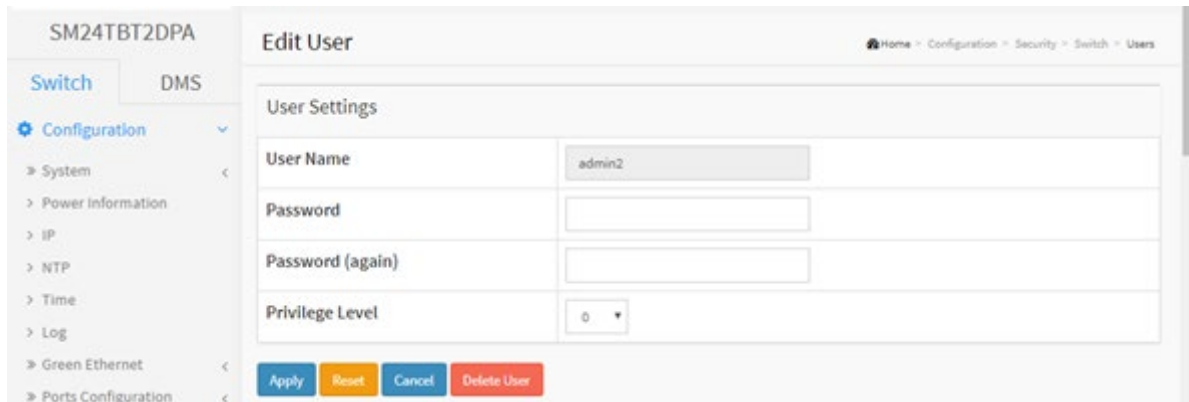
SM24TBT2DPA Users Configuration

Home > Configuration > Security > Switch > Users

User Name	Privilege Level
admin	15
jeffs	15

Add New User

Click a linked User Name to display the Edit User page:



SM24TBT2DPA Edit User

Home > Configuration > Security > Switch > Users

User Settings

User Name	admin2
Password	<input type="password"/>
Password (again)	<input type="password"/>
Privilege Level	0

Apply Reset Cancel Delete User

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

2-5.1.2 Privilege Levels

This page provides an overview of the privilege levels. The switch provides user set privilege levels for ACTIVATE, Aggregation, cloud_management, Diagnostics, EEE, GARP, GVRP, Install_Wizard, IP2, IPMC Snooping LACP, LLDP, LLDP MED, MAC Table, MRP, MVR, MVRP, Maintenance, Mirroring, Percepixon, POE, Ports, Private VLANs, QoS, R_RING, RPC, SMTP, SNMP, Security, sFlow, SMTP, Spanning Tree, System, Timer, Trap Event, Trouble_Shooting, TS_client, TS_server, UPnP, VCL, VLANs, Voice VLAN, VTUN, and XXRP. Privilege Levels range from 1 (lowest) to 15 (highest).

To configure Privilege Levels in the web UI:

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

Figure2-5.1.2: Privilege Level Configuration page

Group Name	Privilege Levels			
	Configuration Read-only	Configuration/Execute Read/write	Status/Statistics Read-only	Status/Statistics Read/write
ACTIVATE	5	10	5	10
Aggregation	5	10	5	10
cloud_management	5	10	5	10
Debug	15	15	15	15
DHCP	5	10	5	10
Dhcp_Client	5	10	5	10
Diagnostics	5	10	5	10
DMS_client	5	10	5	10
DMS_server	5	10	5	10
FFF	5	10	5	10

Parameter descriptions:

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

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

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

IP: Everything except 'ping'.

Port: Everything except Cable Diagnostics.

Diagnostics: 'ping' and Cable Diagnostics.

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

Debug: Only present in CLI.

Privilege Levels: Every group has an authorization Privilege level for the following sub-groups:

- Configuration Read-only
- Configuration/Execute Read-Write
- Status/Statistics Read-only
- Status/Statistics Read-write (e.g., for clearing of statistics)

User Privilege should be same or greater than the authorization Privilege level to have the access to that group.

Buttons

Apply – Click to save changes.

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

Messages: *The privilege level of 'Read-only' should be less or equal 'Read/write'.*

2-5.1.3 Authentication Method

This page lets you configure a user with authentication when they log into the switch via one of the management client interfaces. **SSH** (Secure **S**hell) is used to securely access the Switch. SSH is a secure communication protocol that combines authentication and data encryption to provide secure encrypted communication. **HTTPS** is used to securely access the Switch. HTTPS is a secure communication protocol that combines authentication and data encryption to provide secure encrypted communication via the browser. HTTP has no built-in security. Use HTTP redirect if you want all the requests (both HTTP and HTTPS) to be redirected on HTTPS. **Note:** starting at FW vB6.64.0079, the default is HTTPS and HTTP is redirected to HTTPS. Also, SSH is always enabled, the Telnet default is disabled, and you are given the option to enable Telnet.

To configure Authentication Methods in the web UI:

1. Specify the Client (console, telnet, ssh, http, https) which you want to monitor.
2. Specify the Authentication Method (none, local, radius, tacacs+).
3. Check Fallback.
4. Click Apply.

Figure 2-4.1.3: Authentication Method Configuration page

Client	Methods			Service Port
console	local	no	no	
telnet	no	no	no	23
ssh	local	no	no	22
http	redirect	no	no	80
https	local	no	no	443

Parameter descriptions:

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

type dropdown: select no, local, radius, or tacacs. You can also select 'redirect http to https'.

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

no: authentication is disabled and login is not possible.

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

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

radius: use a remote RADIUS server for authentication.

tacacs: use a remote TACACS+ server for authentication.

Authentication methods that involve remote servers are timed out if the remote servers are offline. In this case the next method is tried. Each method is tried from left to right and continues until a method either approves or rejects a user. If a remote server is used for primary authentication it is recommended to configure secondary authentication as 'local'. This will enable the management client to login via the local user database if none of the configured authentication servers are alive.

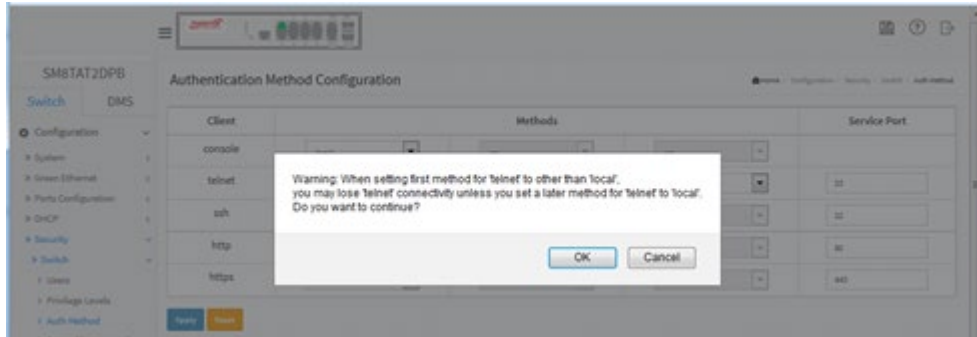
Service Port: The TCP port for each client service. A valid port number is 1 ~ 65534. The port numbers displayed are the commonly used port numbers for the client types.

Buttons:

Apply – Click to save changes.

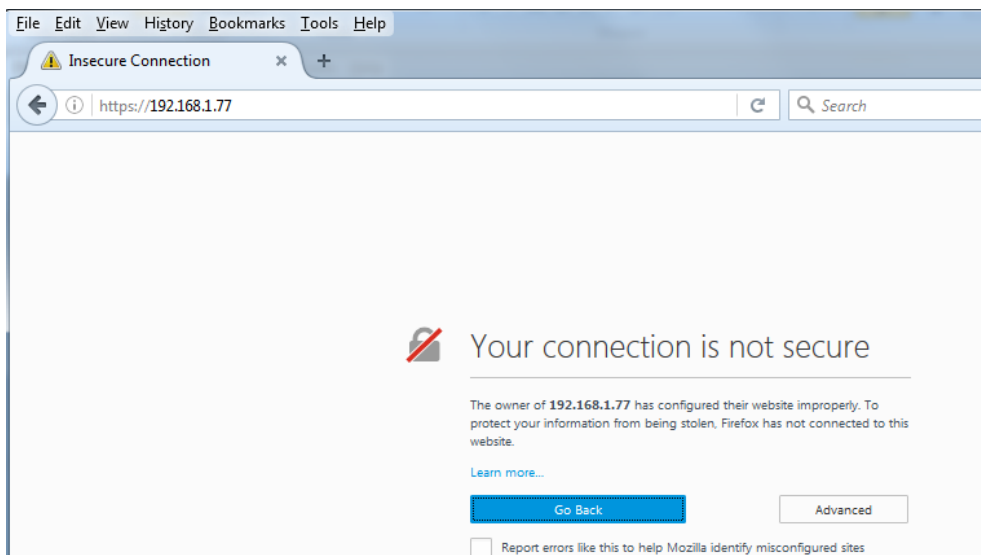
Reset - Click to undo any changes made locally and revert to previously saved values.

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



Similar messages display for other client type selections (console, telnet, ssh, http, and https).

Message: *Your connection is not secure* displays if you selected redirect as the http client login method.



Similar messages display for other web browsers. Click *Learn more*, *Go Back*, *Advanced*, or *Report errors like this*

If you select *Advanced*, then a screen displays requiring parameter entries; you must then log in again, only this time the login is at the secure site (e.g., <https://192.168.1.77/login.htm>).

2-5.1.4 HTTPS Configuration

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

1. Navigate to the Configuration > Security > Switch > HTTPS menu path.
2. Specify the Certificate operation.
3. Specify the Certificate pass phrase.
4. Select the upload method.
5. Choose a filename to upload.
6. Click Apply.

Figure 2-4.1.3: HTTPS Configuration page

The screenshot shows the Lantronix web interface for the SM24TBT2DPB switch. The main content area is titled "HTTPS Configuration" and contains the following fields:

Certificate Maintain	Upload
Certificate Pass Phrase	<input type="text"/>
Certificate Upload	Web Browser
File Upload	<input type="button" value="Choose File"/> No file chosen
Certificate Status	Switch secure HTTP certificate is presented

At the bottom of the configuration area are "Apply" and "Reset" buttons. The left sidebar shows a navigation menu with "Security" > "Switch" selected. The breadcrumb trail at the top right reads: Home > Configuration > Security > Switch > HTTPS.

Parameter descriptions:

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

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

Generate: Generate a new self-signed RSA certificate.

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

Certificate Upload: Upload a certificate PEM file into the switch. The file should contain the certificate and private key together. If you have two separated files for saving certificate and private key. Use the Linux cat command to combine them into a single PEM file. For example, `cat my.cert my.key > my.pem`. Note that the RSA certificate is recommended since most of the new browser versions have removed support for DSA in certificates (e.g. Firefox v37 and Chrome v39).

Possible methods are:

Web Browser: Upload a certificate via Web browser.

URL: Upload a certificate via URL, the supported protocols are HTTP, HTTPS, TFTP and FTP. The URL format is `<protocol>://[<username>[:<password>]@]< host>[:<port>][/<path>]/<file_name>`.

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

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

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

File Upload: Click the **Choose File** button and browse to and select the certificate file.

URL: Enter the URL of the file to be uploaded; only displays if URL is selected as the Certificate Upload method.

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.

Messages:

HTTPS invalid Certificate

HTTPS invalid URL parameter

file is empty

URL is empty

2-5.1.6 Access Management

This page lets you configure the Switch access management table parameters including HTTP/HTTPS, SNMP, and TELNET/SSH. You can manage the Switch over an Ethernet LAN, or over the Internet. Configure the 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.

To configure Access Management parameters in the web UI:

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

Figure 2-5.1.6: Access Management Configuration page

The screenshot shows the 'Access Management Configuration' page in the Lantronix web UI. The page title is 'Access Management Configuration' and the mode is set to 'Disabled'. A table lists access management entries with columns for Delete, VLAN ID, Start IP Address, End IP Address, HTTP/HTTPS, SNMP, and TELNET/SSH. The first entry has 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'.

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

Parameter descriptions:

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

Enabled: Enable access management mode operation.

Disabled: Disable access management mode operation.

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

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

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

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

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

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

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

Buttons:

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.

2-5.1.7 SNMP

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

SNMP is basically passive except for issuing the trap information. The switch supports a switch to turn on or off the SNMP agent. If you set the field SNMP “Enable”, SNMP agent will be started. All supported MIB OIDs, including RMON MIB, can be accessed via SNMP manager. If the field SNMP is set “Disable”, SNMP agent will be de-activated, the related Community Name, Trap Host IP Address, Trap and all MIB counters will be ignored.

2-5.1.7.1 System

This page lets you configure SNMP System on the switch. This function is used to configure SNMP settings, community name, trap host and public traps as well as the throttle of SNMP. A SNMP manager must pass the authentication by identifying both community names, then it can access the MIB information of the target device. So both parties must have the same community name. To complete the setting, click the Apply button; the setting takes effect.

Web Interface

To view and configure SNMP System parameters in the web UI:

1. Click Configuration, Security, Switch, SNMP, System.
2. At the Mode dropdown, select Enabled or Disabled for the SNMP function.
3. Specify the Version and the Engine ID.
4. Click Apply.

Figure2-5.1.7.1: SNMP System Configuration page

Mode	Disabled
Version	SNMP v2c
Read Community	public
Write Community	private
Engine ID	800007e5017f000001

Parameter descriptions:

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

Enabled: Enable SNMP mode operation (default at SM24TBT2DPB FW VB6.64.0045 and before).

Disabled: Disable SNMP mode operation (default after SM24TBT2DPB FW VB6.64.0045).

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

SNMP v1: Set SNMP support to version 1.

SNMP v2c: Set SNMP support to version 2c (default).

SNMP v3: Set SNMP support to version 3.

Read Community: Indicates the community read access string to permit access to SNMP agent.

The allowed string length is 0 to 255, and the allowed content is the ASCII characters 33-126.

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

Write Community: Indicates the community write access string to permit access to SNMP agent.

The allowed string length is 0 to 255, and the allowed content is the ASCII characters 33-126.

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

Engine ID: Indicates the SNMPv3 engine ID. The string must contain an even number (in hexadecimal format) with the number of digits between 10 and 64, but all-zeros and all-'F's are not allowed. Change of the Engine ID will clear all original local users.

Buttons:

Apply – Click to save changes.

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

2-5.1.7.2 Trap

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

1. Click Configuration, Security, Switch, SNMP, Trap.
2. At the Mode dropdown select Enabled.
3. Click the Add New Entry button.
4. Configure the SNMP Trap parameters (Name, Mode, Version, etc.).
5. Click Apply.

Figure2-5.1.7.2: SNMP Trap Configuration page

Parameter descriptions

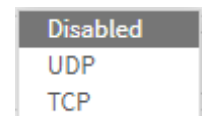
Trap Config Name: Enter a name for the SNMP trap.

Trap Mode: At the dropdown select the trap mode of operation. Possible modes are:

Disabled: Disable SNMP trap mode operation (default).

UDP: Enable UDP SNMP mode.

TCP: Enable TCP SNMP mode.



Note: FW v6.54.3104 added the SNMP Trap over TCP or UDP feature.

Trap Version: At the dropdown select the SNMP trap supported version. Possible versions are:

SNMPv1: Set SNMP trap supported version 1.

SNMPv2c: Set SNMP trap supported version 2c.

SNMPv3: Set SNMP trap supported version 3.

Trap Community: Indicates the community access string when sending SNMP trap packet.

The allowed string length is 0 - 255 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 allow a valid hostname. A valid hostname is a string drawn from the alphabet (A-Za-z), digits (0-9), dot (.), dash (-). Spaces are not allowed, the first character must be an alpha character, and the first and last characters must not be a dot or a dash.

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

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

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

Enabled: Enable SNMP trap inform mode operation.

Disabled: Disable SNMP trap inform mode operation.

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

Trap Inform Retry Times: Indicates the SNMP trap inform retry times. The valid range is 0 – 255 retries.

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

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

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

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

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

Buttons:

Apply – Click to save changes.

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

Messages:

After saving configuration, remember select the correct trap security name

The value of 'Trap Destination Address' is 0.0.0.0.

Do you want to proceed anyway?

Example: Four Trap Destination configurations:

The screenshot shows the Lantronix web interface for the SM24TBT2DPB device. The main content area is titled "Trap Configuration" and includes a "Global Settings" section with a "Mode" dropdown set to "Enabled". Below this is a "Trap Destination Configurations" table with the following data:

Delete	Name	Mode	Version	Destination Address	Destination Port
<input type="checkbox"/>	BobB	TCP	SNMPv2c	192.168.1.77	162
<input type="checkbox"/>	Trap1	TCP	SNMPv3	192.168.1.88	162
<input type="checkbox"/>	Trap2	UDP	SNMPv1	192.168.1.66	162
<input type="checkbox"/>	Trap3	UDP	SNMPv2c	192.168.1.66	162

Below the table are buttons for "Add New Entry", "Apply", and "Reset". The left sidebar shows a navigation menu with "SNMP" expanded to show "System", "Trap", and "Communities". The top right of the interface includes an "Auto-Logout" dropdown set to "OFF" and a "Click Save Button" link.

Click any linked Name to display its SNMP Trap Configuration page.

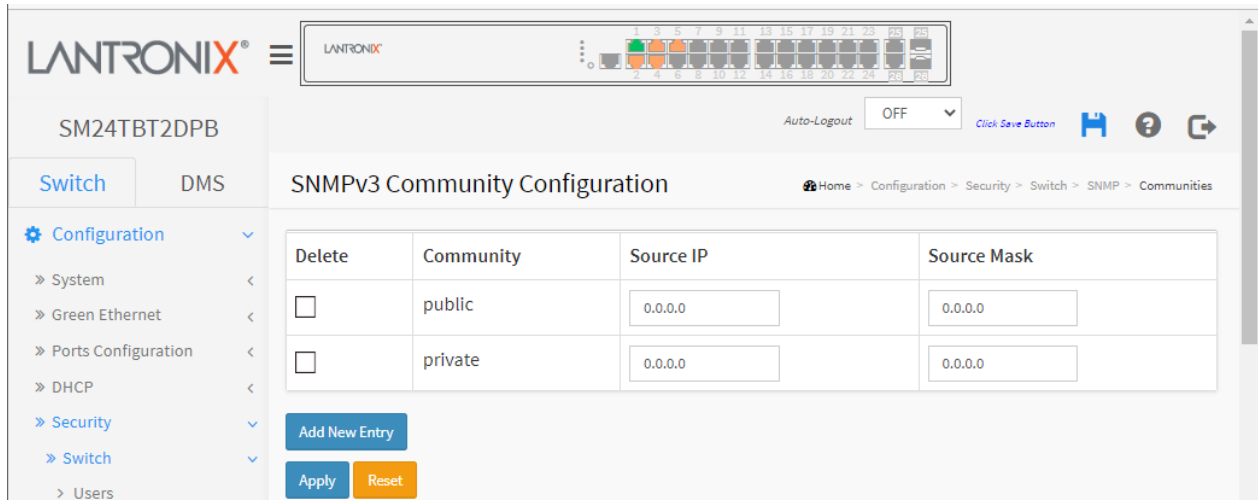
2-5.1.7.3 Communities

This page lets you configure SNMPv3 communities. The Community and User Name are unique.

To configure SNMP Communities in the web UI:

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

Figure2-4.1.7.3: SNMPv3 Community Configuration default page



Parameter descriptions:

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

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

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

Source Mask: Indicates the SNMP access source address mask.

Buttons:

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

Apply – Click to save changes.

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

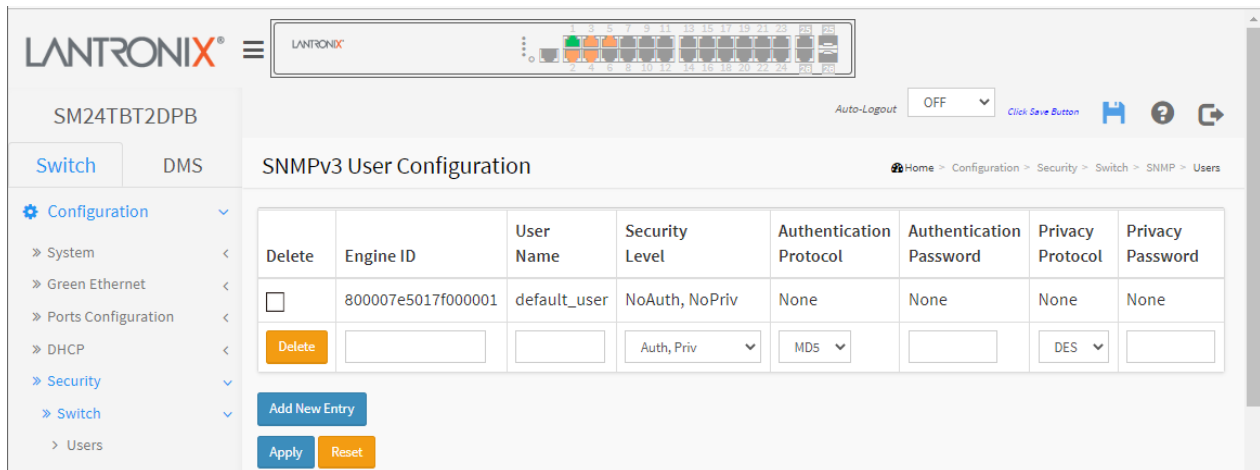
2-5.1.7.4 Users

This page lets you configure SNMPv3 users. The maximum number of Users is 10.

To configure SNMP Users in the web UI:

1. Click Configuration, Security, Switch, SNMP, Users.
2. Specify the User parameters.
3. Click Apply.

Figure 2-5.1.7.4: SNMPv3 User Configuration page



Parameter descriptions:

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

Engine ID: An octet string identifying the engine ID that this entry should belong to. The string must contain an even number (in hexadecimal format) with 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 the user engine ID equals the system engine ID then it is local user; otherwise it's remote user.

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

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

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

NoAuth, NoPriv: No authentication and no privacy.

Auth, NoPriv: Authentication and no privacy.

Auth, Priv: Authentication and privacy.

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

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

None: No authentication protocol.

MD5: An optional flag to indicate that this user uses MD5 authentication protocol. The length of 'MD5 Authentication Password' is to 8 – 32 characters.

SHA: An optional flag to indicate that this user uses SHA authentication protocol. The length of 'AES Privacy Password' is restricted to 8 – 32 characters.

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

Authentication Password: A string identifying the authentication password phrase. For MD5 authentication protocol, the allowed string length is 8 – 32 characters. For SHA authentication protocol, the allowed string length is 8 to 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. The valid length of 'DES Privacy Password' is 8 – 32 characters.

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. A confirmation prompt displays.

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

Messages:

The length of 'SHA Authentication Password' is restricted to 8 – 40

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

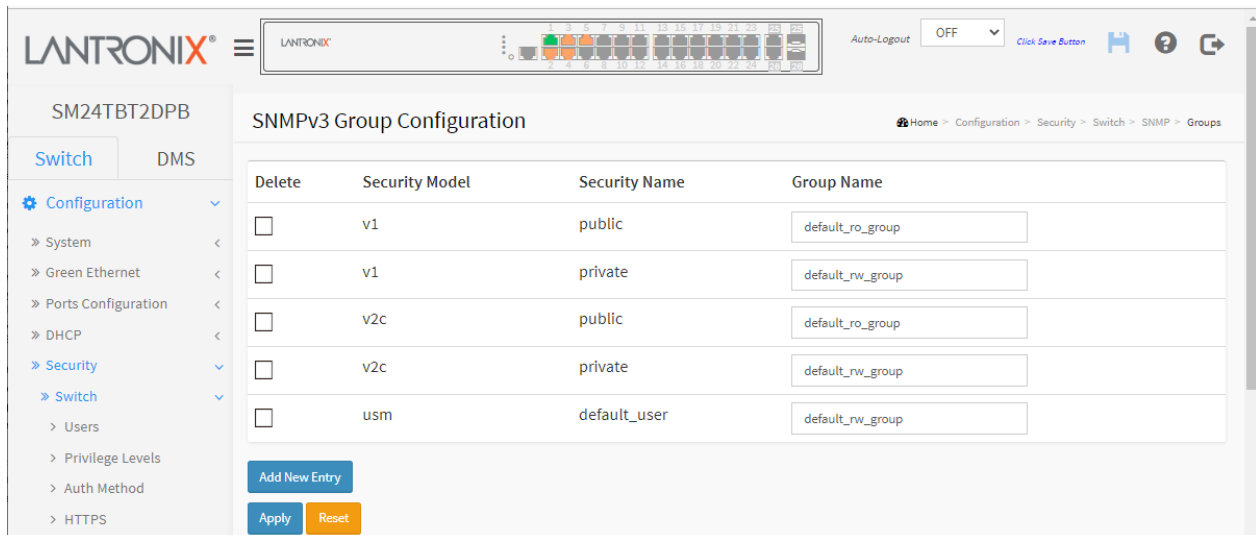
2-5.1.7.5 Groups

This page lets you configure SNMPv3 groups. The Entry index key are Security Model and Security Name. You can configure this maximum number of Groups: v1: 2, v2: 2, v3:10.

To configure SNMP Groups in the web UI:

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

Figure 2-5.1.7.5: SNMP Group Configuration default page



Parameter descriptions:

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:

v1: Reserved for SNMPv1.

v2c: Reserved for SNMPv2c.

usm: User-based Security Model (USM).

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

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

Buttons:

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: *The entry 'v1, public' already exists*

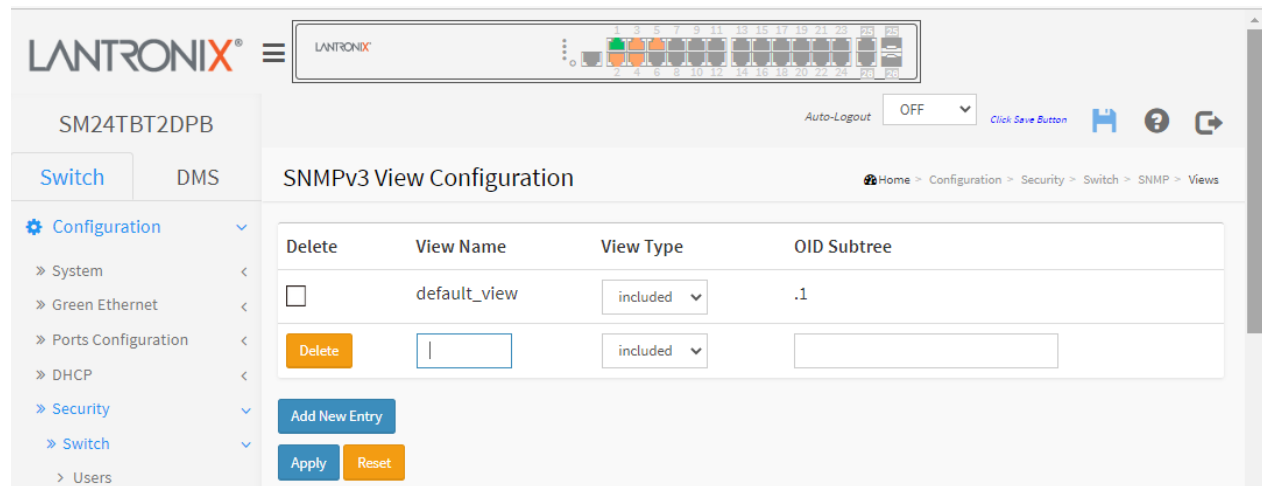
2-5.1.7.6 Views

This page lets you configure SNMPv3 View. The Entry index keys are OID Subtree and View Name. You can configure up to 28 SNMPv3 Views. The entry index keys are View Name and OID Subtree.

To configure SNMPv3 views in the web UI:

1. Click Configuration, Security, Switch, SNMP, Views.
2. Click Add New Entry.
3. Specify the SNMP View parameters.
4. Click Apply.
5. To modify or clear the setting click Reset.

Figure 2-5.1.7.6: SNMP View Configuration page



Parameter descriptions:

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

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

View Type: Indicates the view type that this entry should belong to. Possible view types are:

Included: An optional flag to indicate that this view subtree should be included.

Excluded: An optional flag to indicate that this view subtree should be excluded.

In general, if a view entry's view type is 'excluded', there should be another view entry existing with view type as 'included' and its OID subtree should overstep the 'excluded' view entry.

OID Subtree: The OID defining the root of the subtree to add to the named view. The allowed OID length is 1 - 128. The allowed string content is a digital number or an asterisk (*).

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.

Messages: *The format of 'OID Subtree' is .OID1.OID2.OID3... The allowed OID length is 1 to 128. The allowed string content is digital number or asterisk(*)*

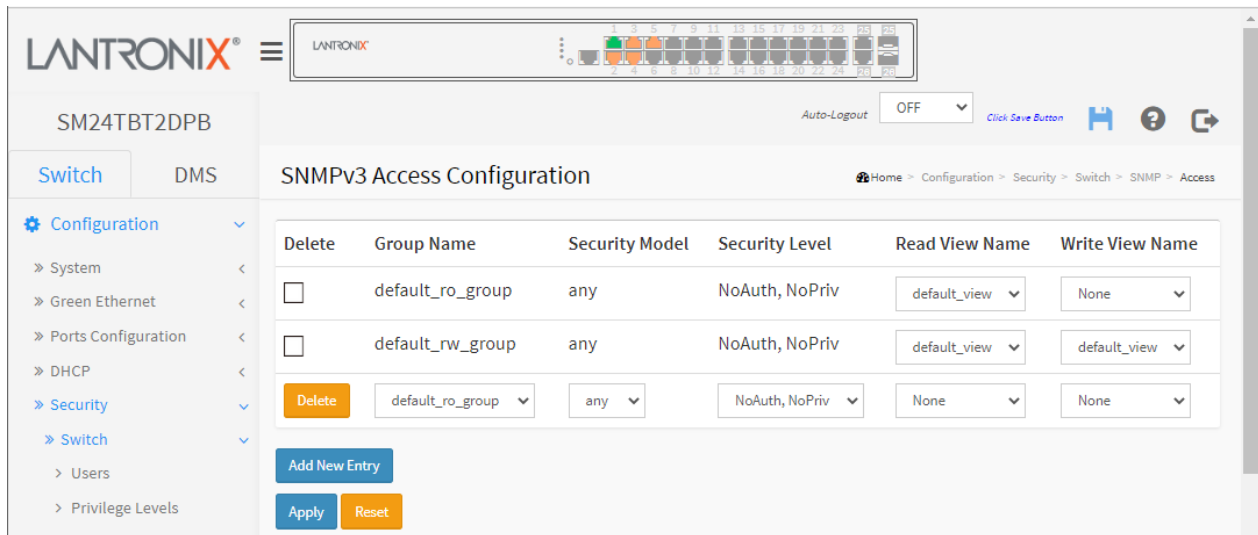
2-5.1.7.7 Access

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

To configure SNMP Access in the web U:

1. Click Configuration, Security, Switch, SNMP, Access.
2. Click Add New Entry.
3. Specify the SNMP Access parameters.
4. Click Apply.
5. To modify or clear the settings click Reset.

Figure 2-5.1.7.7: SNMP Accesses Configuration page



Parameter descriptions:

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

Group Name: A string identifying the group name that this entry should belong to. The allowed string length is 1 to 32 characters, and the allowed content is ASCII characters 33 - 126. At the dropdown select 'default_ro_group' or 'default_rw_group'.

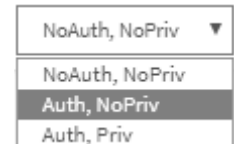
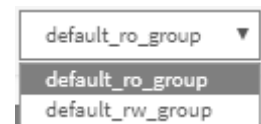
Security Model: Indicates the security model that this entry should belong to. Possible security models are:

- Any:** Any security model accepted(v1|v2c|usm).
- v1:** Reserved for SNMPv1.
- v2c:** Reserved for SNMPv2c.
- usm:** User-based Security Model (USM).

Security Level: Indicates the security model that this entry should belong to. 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 to 32 characters, and the allowed content is ASCII characters 33 - 126.



A dropdown menu with a light gray background and a thin border. The top part shows the current selection 'default_view' with a small downward arrow to its right. Below this, the menu is open, showing two options: 'None' and 'default_view'. The 'default_view' option is highlighted with a darker gray background.

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.

2-5.1.7.8 Trap Event Severity

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

1. Click Configuration, Security, Switch, SNMP, Trap Event Severity.
2. Scroll to a Group Name and select a Severity Level.
3. Click the Apply button to save the settings.
4. To cancel the setting, click the Reset button to revert to previously saved values.

Figure 2-5.1.7.8: Trap Event Severity Configuration page

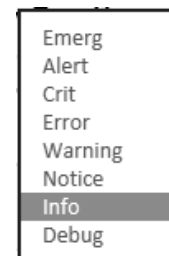
Group Name	Severity Level	Syslog	Trap	SMTP
ACL	Info	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
ACL-Log	Info	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Access-Mgmt	Info	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Auth-Failed	Warning	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Cold-Start	Warning	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Config-Info	Info	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
DMS	Info	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Firmware-Upgrade	Info	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Import-Export	Info	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
LACP	Info	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Link-Status	Warning	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Login	Info	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Logout	Info	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Parameter descriptions:

Group Name: The name identifying the severity group.

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

- <0> **Emerg:** System is unusable (Emergency).
- <1> **Alert:** Action must be taken immediately.
- <2> **Crit:** Critical condition.
- <3> **Error:** Error conditions.
- <4> **Warning:** Warning condition.
- <5> **Notice:** Normal but significant condition.
- <6> **Info:** Information message.
- <7> **Debug:** Debug-level message.



Syslog: Check to Enable - Select this Group Name in Syslog.

Trap: Enable - Select this Group Name in Trap.

SMTP: Enable - Select this Group Name in SMTP.

Digital Out: Enable - Select this Group Name in Digital I/O.

Buttons

Apply: Click to save changes.

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

2-5.1.8 RMON

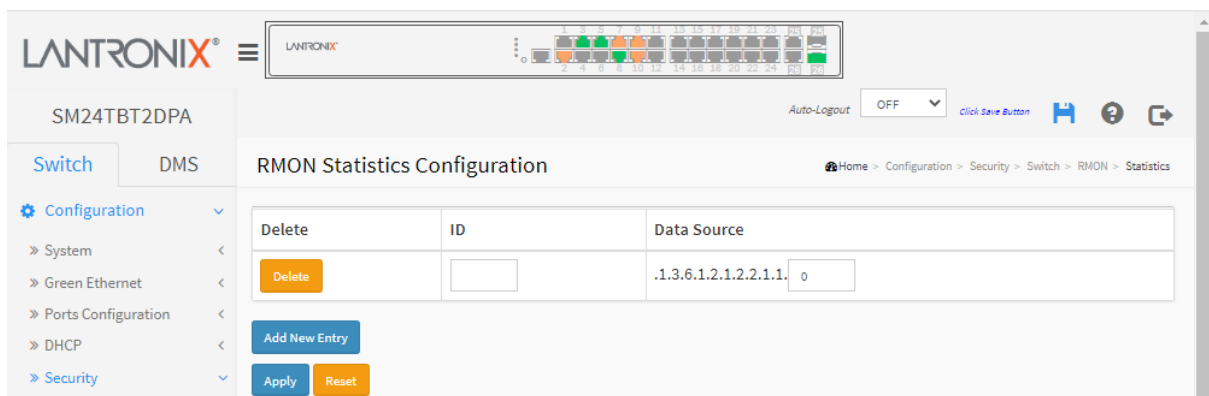
An RMON implementation typically operates in a client/server model. Monitoring devices contain RMON software agents that collect information and analyze packets. These probes act as servers and the Network Management applications that communicate with them act as clients.

2-5.1.8.1 Statistics

To configure RMON statistics in the web UI:

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

Figure 2-5.1.8.1: RMON Statistics Configuration page



Parameter descriptions:

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

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

Data Source: Indicates the port ID which you want to be monitored. 'Data Source' must be an integer value between 1 and 65535.

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 '1' already exists*

2-5.1.8.2 History

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

To configure RMON History in the web UI:

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

Figure 2-5.1.8.2: RMON History Configuration page

The screenshot shows the Lantronix web interface for the SM24TBT2DPA device. The main content area is titled "RMON History Configuration". It features 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	1800	50	50
<input type="checkbox"/>		.1.3.6.1.2.1.2.2.1.1	1800	50	

Below the table, there are buttons for "Add New Entry", "Apply", and "Reset".

Parameter descriptions:

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

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

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

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

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

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

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.

2-5.1.8.3 Alarm

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

To configure RMON Alarm in the web UI:

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

Figure 2-5.1.8.3: RMON Alarm Configuration page

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. 11.11	Delta	0	RisingOrFalling	3	3	4	5
<input type="checkbox"/>	2	30	.1.3.6.1.2.1.2.2.1. 11.11	Absolute	0	Falling	5	2	4	3
<input type="checkbox"/>	3	30	.1.3.6.1.2.1.2.2.1. 11.11	Delta	0	RisingOrFalling	7	6	5	9

Parameter descriptions:

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Absolute: Get the sample directly.

Delta: Calculate the difference between samples (default).

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

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

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

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

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

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

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

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

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

Buttons:

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

Apply – Click to save changes.

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

Messages:

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

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

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

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

invalid 'datasource', invalid llag

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

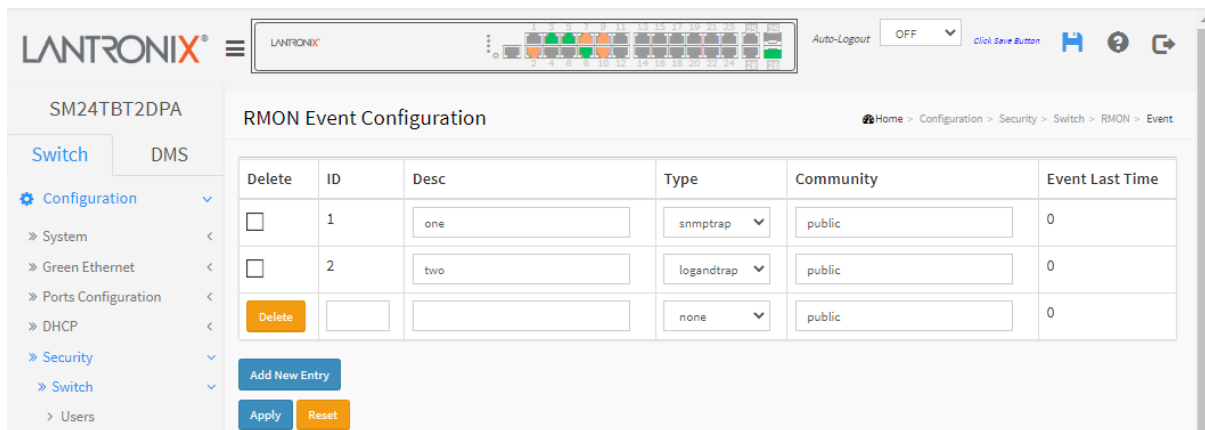
2-5.1.8.4 Event

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

To configure RMON Events in the web UI:

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

Figure 2-5.1.8.4: RMON Event Configuration page



Parameter descriptions:

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

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

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

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

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

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

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

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

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

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

Buttons:

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

Apply – Click to save changes.

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

2-5.2 Network

2-5.2.1 Limit Control

This page lets you configure the Port Security Limit Control system and port settings. Limit Control allows for limiting the number of users on a given port. A user is identified by a MAC address and VLAN ID. If Limit Control is enabled on a port, the limit specifies the maximum number of users on the port. If this number is exceeded, an action is taken. The action can be one of the four different actions as described below.

The Limit Control module utilizes a lower-layer module, Port Security module, which manages MAC addresses learned on the port. The Limit Control configuration page has two sections, a system configuration section and a port configuration section.

To configure Limit Control at the System level in the web UI:

1. Navigate to Configuration > Security > Network > Limit Control.
2. Select “Enabled” in the Mode column of the System Configuration section.
3. Check Aging Enabled and set Aging Period (default is 3600 seconds).

To configure Port level Limit Control in the web UI:

1. Select “Enabled” in the Mode column of the Port Configuration section.
2. Specify the maximum number of MAC addresses in the Limit column.
3. Set the Action (None, Trap, Shutdown, or Trap & Shutdown).
4. At the “Sticky” dropdown, select Enabled or Disabled.
5. Click the Apply button.

Figure 2-5.2.1: Port Security Limit Control Configuration page

LANTRONIX®

SM24TBT2DPB

Auto-Logout OFF

Click Save Button

Port Security Limit Control Configuration

Home > Configuration > Security > Network > Limit Control

System Configuration

Mode: Disabled

Aging Enabled:

Aging Period: 3600 seconds

Port Configuration

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

Parameter descriptions:**System Configuration**

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

Aging Enabled: If checked, secured MAC addresses are subject to aging; see [Aging Period](#) below.

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

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

To understand why aging may be desired, consider the following scenario: Suppose an end-host is connected to a 3rd party switch or hub, which in turn is connected to a port on this switch on which Limit Control is enabled. The end-host will be allowed to forward if the limit is not exceeded. Now suppose that the end-host logs off or powers down. If it wasn't for aging, the end-host would still take up resources on this switch and will be allowed to forward. To overcome this situation, enable aging. With aging enabled, a timer is started once the end-host gets secured. When the timer expires, the switch starts looking for frames from the end-host, and if such frames are not seen within the next Aging Period, the end-host is assumed to be disconnected, and the corresponding resources are freed on the switch.

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

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

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

Limit: The maximum number of MAC addresses that can be secured on this port. 'Limit' must be an integer value between 1 and 1024. If the limit is exceeded, the corresponding action is taken. The switch is "born" with a total number of MAC addresses from which all ports draw whenever a new MAC address is seen on a Port Security-enabled port. Since all ports draw from the same pool, it may happen that a configured maximum cannot be granted, if the remaining ports have already used all available MAC addresses.

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

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

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

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

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

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

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

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

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

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

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

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



NOTE: Clicking the Re-open button causes the page to be refreshed, so unsaved changes will be lost.

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

Buttons:

Refresh: Click to manually refresh the Port Security information immediately.

Apply – Click to save changes.

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

2-5.2.2 NAS

This page lets you configure the NAS parameters of the switch. The NAS server can be employed to connect users to a variety of resources including Internet access, conference calls, printing documents on shared printers, or by simply logging on to the Internet.

To configure a Network Access Server in the web UI:

1. Navigate to Configuration > Security > Network > NAS.
2. Set the “System Configuration” section parameters.
3. Set the “Port Configuration” section parameters.
4. Click Apply.

Figure 2-5.2.2: Network Access Server Configuration page

Port	Admin State	RADIUS-Assigned QoS Enabled	RADIUS-Assigned VLAN Enabled	Guest VLAN Enabled	Port State	Restart
*	<>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>		
1	Force Unauthorized	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Globally Disabled	Reauthenticate Reinitialize
2	Port-based 802.1X	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	Globally Disabled	Reauthenticate Reinitialize
3	Single 802.1X	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Globally Disabled	Reauthenticate Reinitialize
4	Multi 802.1X	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	Globally Disabled	Reauthenticate Reinitialize
5	MAC-based Auth.	<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
7	Force Authorized	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Globally	Reauthenticate Reinitialize

Parameter descriptions:

System Configuration

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

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

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

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

EAPOL Timeout: Sets the time for retransmission of Request Identity EAPOL (Extensible Authentication Protocol over LAN) frames. Valid values are in the range 1 to 255 seconds. This has no effect for MAC-based ports.

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

Single 802.1X

Multi 802.1X

MAC-Based Auth.

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

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

For ports in MAC-based Auth. mode, reauthentication doesn't cause direct communication between the switch and the client, so this will not detect whether the client is still attached or not, and the only way to free any resources is to age the entry.

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

Single 802.1X

Multi 802.1X

MAC-Based Auth.

If a client is denied access - either because the RADIUS server denies the client access or because the RADIUS server request times out (according to the timeout specified on the "Configuration > Security > AAA" page) - the client is put on hold in the Un-authorized state. The hold timer does not count during an on-going authentication. In MAC-based Auth. mode, the switch will ignore new frames coming from the client during the hold time. The Hold Time can be set to a number between 10 and 1000000 seconds.

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

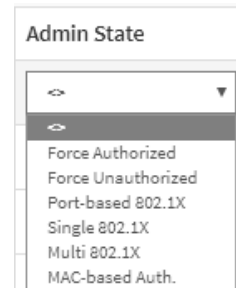
Port: The port number for which the configuration below applies.

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

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

Force Unauthorized: In this mode, the switch will send one EAPOL Failure frame when the port link comes up, and any client on the port will be disallowed network access.

Port-based 802.1X: In the 802.1X-world, the user is called the supplicant, the switch is the authenticator, and the RADIUS server is the authentication server. The authenticator acts as the man-in-the-middle, forwarding requests and responses between the supplicant and the authentication server. Frames sent between the supplicant and the switch are special 802.1X frames, known as EAPOL (EAP Over LANs) frames. EAPOL frames encapsulate EAP PDUs (RFC3748). Frames sent between the switch and the RADIUS server are RADIUS packets. RADIUS packets also encapsulate EAP PDUs together with other attributes like the switch's IP address, name, and the supplicant's port number on the switch. EAP is very flexible, in that it allows for different authentication methods, like MD5-Challenge, PEAP, and TLS. The important thing is that the authenticator (the switch) doesn't need to know which authentication method the supplicant and the authentication server are using, or how many information exchange frames are needed for a particular method. The switch simply encapsulates the EAP part of the frame into the relevant type (EAPOL or RADIUS) and forwards it.



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



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

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

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

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

Multi 802.1X: In port-based 802.1X authentication, once a supplicant is successfully authenticated on a port, the whole port is opened for network traffic. This allows other clients connected to the port

(for instance through a hub) to piggy-back on the successfully authenticated client and get network access even though they really aren't authenticated. To overcome this security breach, use the Multi 802.1X variant.

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

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

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

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

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

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

RADIUS-Assigned QoS Enabled: When RADIUS-Assigned QoS is both globally enabled and enabled (checked) on a given port, the switch reacts to QoS Class information carried in the RADIUS Access-Accept packet transmitted by the RADIUS server when a supplicant is successfully authenticated. If present and valid, traffic received on the supplicant's port will be classified to the given QoS Class. If (re-)authentication fails or the RADIUS Access-Accept packet no longer carries a QoS Class or it's invalid, or the supplicant is otherwise no longer present on the port, the port's QoS Class is immediately reverted to the original QoS Class (which may be changed by the administrator in the meanwhile without affecting the RADIUS-assigned). This option is only available for single-client modes, i.e. **Port-based 802.1X** and **Single 802.1X**.

RADIUS attributes used in identifying a QoS Class: Refer to the written documentation for a description of the RADIUS attributes needed in order to successfully identify a QoS Class.

The User-Priority-Table attribute defined in RFC4675 forms the basis for identifying the QoS Class in an Access-Accept packet.

Only the first occurrence of the attribute in the packet will be considered, and to be valid, it must follow this rule:

All 8 octets in the attribute's value must be identical and consist of ASCII characters in the range '0' - '3', which translates into the desired QoS Class in the range [0; 3].

RADIUS-Assigned VLAN Enabled: When RADIUS-Assigned VLAN is both globally enabled and enabled (checked) for a given port, the switch reacts to VLAN ID information carried in the RADIUS Access-Accept packet transmitted by the RADIUS server when a supplicant is successfully authenticated. If present and valid, the port's Port VLAN ID will be changed to this VLAN ID, the port will be set to be a member of that VLAN ID, and the port will be forced into VLAN unaware mode. Once assigned, all traffic arriving on the port will be classified and switched on the RADIUS-assigned VLAN ID.

If (re-)authentication fails or the RADIUS Access-Accept packet no longer carries a VLAN ID or it's invalid, or the supplicant is otherwise no longer present on the port, the port's VLAN ID is immediately reverted to the original VLAN ID (which may be changed by the administrator in the meanwhile without affecting the RADIUS-assigned).

This option is only available for single-client modes, i.e., **Port-based 802.1X** and **Single 802.1X**.

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

RADIUS attributes used in identifying a VLAN ID:

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 transmissions of EAPOL Request Identity frames is configured with EAPOL Timeout. If Allow Guest VLAN if EAPOL Seen is enabled, the port will now be placed in the Guest VLAN.

If disabled, the switch will first check its history to see if an EAPOL frame has previously been received on the port (this history is cleared if the port link goes down or the port's Admin State is changed), and if not, the port will be placed in the Guest VLAN. Otherwise, it will not move to the Guest VLAN but continue transmitting EAPOL Request Identity frames at the rate given by EAPOL Timeout.

Once in the Guest VLAN, the port is considered authenticated, and all attached clients on the port are allowed access on this VLAN. The switch will not transmit an EAPOL Success frame when entering the Guest VLAN.

While in the Guest VLAN, the switch monitors the link for EAPOL frames, and if one such frame is received, the switch immediately takes the port out of the Guest VLAN and starts authenticating the supplicant according to the port mode. If an EAPOL frame is received, the port will never be able to go back into the Guest VLAN if "Allow Guest VLAN if EAPOL Seen" is disabled.

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

Globally Disabled: NAS is globally disabled.

Link Down: NAS is globally enabled, but there is no link on the port.

Authorized: The port is in Force Authorized or a single-supplicant mode and the supplicant is authorized.

Unauthorized: The port is in Force Unauthorized or a single-supplicant mode and the supplicant is not successfully authorized by the RADIUS server.

X Auth/Y Unauth: The port is in a multi-supplicant mode. Currently X clients are authorized and Y clients are unauthorized.

Restart: Two buttons are available for each row. The buttons are only enabled when authentication is globally enabled and the port's Admin State is in an EAPOL-based or MAC-based mode. Clicking these buttons will not cause settings changed on the page to take effect.

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

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

Buttons:

Apply – Click to save changes.

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

Refresh: Click to refresh the NAS Configuration manually.

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

2-5.2.3 ACL

The switch Access Control List (ACL) function is used for packet filtering but also for selecting types of traffic to be analyzed, forwarded, or influenced in some way. The ACLs are divided into Ether Types, IPv4, ARP protocol, MAC and VLAN parameters, etc. Here we will just go over the standard and extended access lists for TCP/IP. As you create ACEs for ingress classification, you can assign a policy for each port, the policy number is 1-8, and however, each policy can be applied to any port. This makes it very easy to determine what type of ACL policy you will be working with.

2-5.2.3.1 Ports

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

To configure ACL Ports in the web UI:

1. Click Configuration, Security, Network, ACL, Ports.
2. Select the specific parameter values for port ACL settings.
3. Click the Apply button to save the settings.
4. To cancel the settings click the Reset button. The page will revert to previously saved values.
5. After configuration is complete, view the port Counters. Click Refresh to update the counters or click Clear to reset the counters.

Figure 2-5.2.3.1: ACL Ports Configuration page

Port	Policy ID	Action	Rate Limiter ID	Port Redirect	Mirror	Logging	Shutdown	State	Counter
*	0	Permit	Disabled	Disabled Port 1 Port 2	Disabled	Disabled	Disabled	Enabled	*
1	0	Permit	Disabled	Disabled Port 1 Port 2	Disabled	Disabled	Disabled	Enabled	631998
2	0	Permit	Disabled	Disabled Port 1 Port 2	Disabled	Disabled	Disabled	Enabled	257906
3	0	Permit	Disabled	Disabled Port 1 Port 2	Disabled	Disabled	Disabled	Enabled	57236
4	0	Permit	Disabled	Disabled Port 1 Port 2	Disabled	Disabled	Disabled	Enabled	49695
5	0	Permit	Disabled	Disabled Port 1 Port 2	Disabled	Disabled	Disabled	Enabled	114209
6	0	Permit	Disabled	Disabled Port 1 Port 2	Disabled	Disabled	Disabled	Enabled	0
7	0	Permit	Disabled	Disabled Port 1 Port 2	Disabled	Disabled	Disabled	Enabled	0
8	0	Permit	Disabled	Disabled Port 1 Port 2	Disabled	Disabled	Disabled	Enabled	0

Parameter descriptions:

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

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

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

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

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

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

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

Disabled: Frames received on the port are not logged.

The default value is "Disabled". Please note that the System Log memory size and logging rate is limited.

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

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

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

State: Specify the port state of this port. The default value is "Enabled". 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.

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 ACL Port Configuration parameters manually.

Clear: Click to clear the ACL Port Configuration parameters manually.

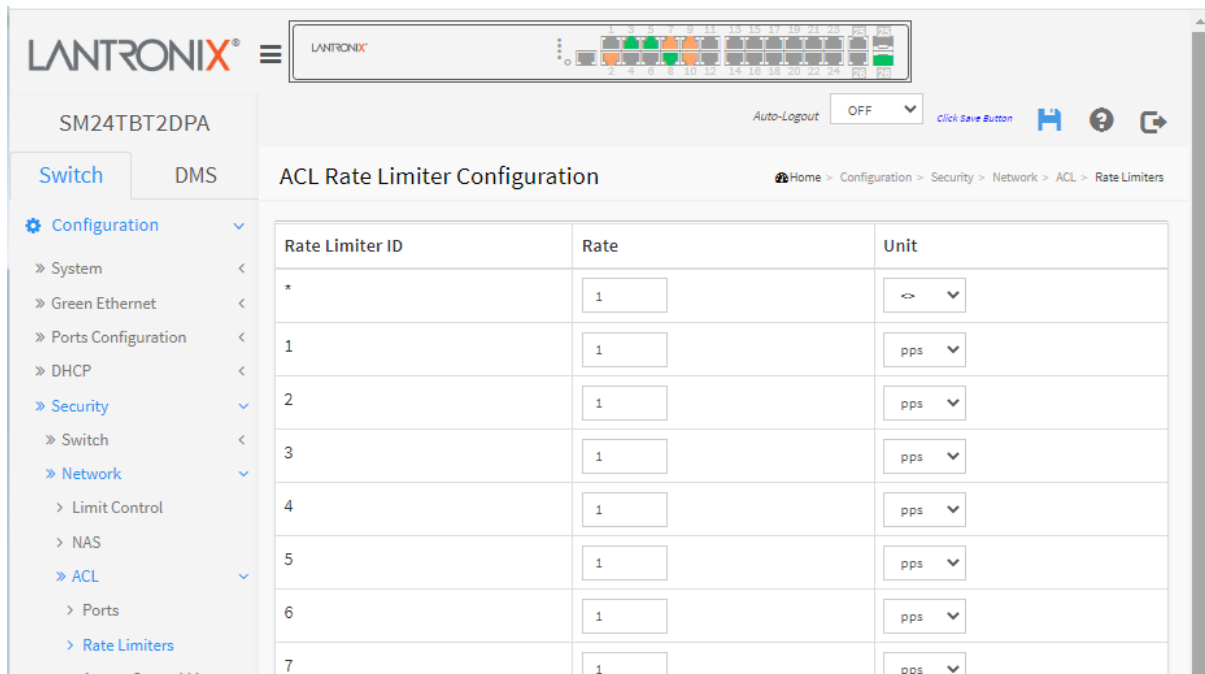
2-5.2.3.2 Rate Limiters

This page lets you configure the switch's ACL Rate Limiter parameters. The Rate Limiter Level (1 to 16) allows you to set rate limiter value and units.

To configure ACL Rate Limiter in the web UI:

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

Figure 2-5.2.3.2: ACL Rate Limiter Configuration page



Parameter descriptions:

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

Rate: The allowed values are:0-3276700 in pps or 0, 100, 200, 300, ..., 1000000 in kbps.

Unit: Specify the rate unit. The allowed values are:

pps: packets per second.

kbps: thousands of bits per second.

Buttons

Apply – Click to save changes.

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

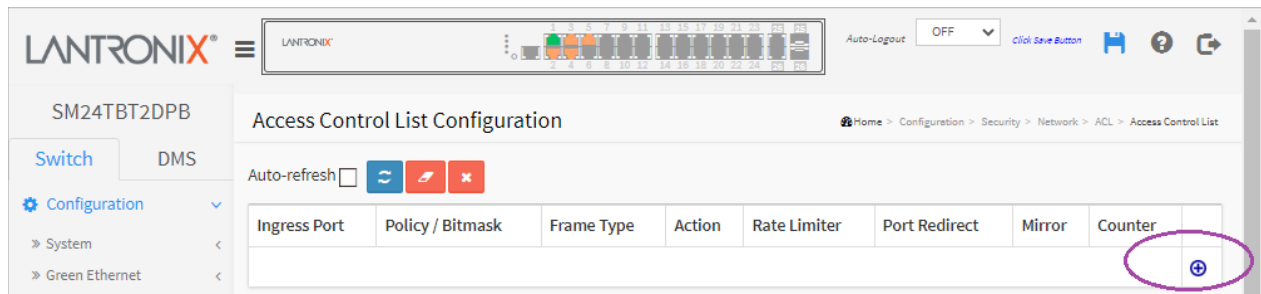
2-5.2.3.3 Access Control List

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

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. Each row describes the ACE that is defined. The maximum number of ACEs is 256 on each switch. Click on the lowest plus sign to add a new ACE to the list. The reserved ACEs used for internal protocol cannot be edited or deleted; the order sequence cannot be changed, and the priority is highest.

To configure Access Control List in the web UI:

1. Click Configuration > Security > Network > ACL > Access Control List.




2. Click the  button to add a new ACL or use the other ACL modification buttons to specify the editing action (edit, delete, or move the position of entry in the list).
3. Specify the ACE parameters.
4. Click the **Apply** button save to save the settings
5. To cancel the settings click the **Reset** button. The page will revert to previously saved values.
6. When editing an entry on the ACE Configuration page, note that the Items displayed depend on various selections, such as Frame Type and IP Protocol Type. Specify the relevant criteria to be matched for this rule and set the actions to take when a rule is matched (such as Rate Limiter, Port, Copy, Logging, and Shutdown).

Figure 2-5.2.3.3: ACE Configuration page

The screenshot shows the LANTRONIX web interface for the SM24TBT2DPB device. The main content area is titled "ACE Configuration". On the left, there is a navigation menu with "Switch" and "DMS" tabs, and a "Configuration" section expanded to show "Security" > "Network" > "ACL" > "Access Control List". The breadcrumb trail at the top right reads "Home > Configuration > Security > Network > ACL > Access Control List".

The configuration fields are as follows:

- Ingress Port:** A dropdown menu with options: All, Port 1, Port 2, Port 3, Port 4. The "All" option is selected.
- Policy Filter:** A dropdown menu with the option "Any" selected.
- Frame Type:** A dropdown menu with the option "Any" selected.
- Action:** A dropdown menu with the option "Permit" selected.
- Rate Limiter:** A dropdown menu with the option "Disabled" selected.
- Mirror:** A dropdown menu with the option "Disabled" selected.
- Logging:** A dropdown menu with the option "Disabled" selected.
- Shutdown:** A dropdown menu with the option "Disabled" selected.
- Counter:** A text input field containing the value "0".
- VLAN Parameters:**
 - 802.1Q Tagged:** A dropdown menu with the option "Any" selected.
 - VLAN ID Filter:** A dropdown menu with the option "Any" selected.
 - Tag Priority:** A dropdown menu with the option "Any" selected.

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

Parameter descriptions:

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

All: The ACE applies to all port.

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

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

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

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

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

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

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

Any: Any frame can match this ACE.

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

ARP: Only ARP frames can match this ACE. Notice the ARP frames won't match the ACE with Ethernet type.

IPv4: Only IPv4 frames can match this ACE. Notice the IPv4 frames won't match the ACE with Ethernet type.

IPv6: Only IPv6 frames can match this ACE. Notice the IPv6 frames won't match the ACE with Ethernet type.

Action: Specify the action to take with a frame that hits this ACE.

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

Deny: The frame that hits this ACE is dropped.

Filter: Frames matching the ACE are filtered.

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

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

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

Enabled: Frames received on the port are mirrored.

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

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

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

Disabled: Frames matching the ACE are not logged.

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

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

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

Disabled: Port shut down is disabled for the ACE.

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

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

MAC Parameters

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

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

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

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

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

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

MC: Frame must be multicast.

BC: Frame must be broadcast.

UC: Frame must be unicast.

Specific: If you want to filter a specific destination MAC address with this ACE, choose this value. A field for entering a DMAC value appears.

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

VLAN Parameters

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

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

Enabled: Tagged frame only.

Disabled: Untagged frame only.

The default value is "Any".

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

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

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

VLAN ID number appears.

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

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

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

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

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

ARP: Frame must have ARP opcode set to ARP.

RARP: Frame must have RARP opcode set to RARP.

Other: Frame has unknown ARP/RARP Opcode flag.

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

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

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

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

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

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

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

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

Sender IP Address: When "Host" or "Network" is selected for the sender IP filter, you can enter a specific sender IP address in dotted decimal notation.

Sender IP Mask: When "Network" is selected for the sender IP filter, you can enter a specific sender IP mask in dotted decimal notation.

Target IP Filter: Specify the target IP filter for this specific ACE.

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

Host: Target IP filter is set to Host. Specify the target IP address in the Target IP Address field that appears.

Network: Target IP filter is set to Network. Specify the target IP address and target IP mask in the Target IP Address and Target IP Mask fields that appear.

Target IP Address: When "Host" or "Network" is selected for the target IP filter, you can enter a specific target IP address in dotted decimal notation.

Target IP Mask: When "Network" is selected for the target IP filter, you can enter a specific target IP mask in dotted decimal notation.

ARP Sender MAC Match: Specify whether frames can hit the action according to their sender hardware address field (SHA) settings.

0: ARP frames where SHA is not equal to the SMAC address.

1: ARP frames where SHA is equal to the SMAC address.

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

RARP Target MAC Match: Specify whether frames can hit the action according to their target hardware address field (THA) settings.

0: RARP frames where THA is not equal to the target MAC address.

1: RARP frames where THA is equal to the target MAC address.

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

IP/Ethernet Length: Specify whether frames can hit the action according to their ARP/RARP hardware address length (HLN) and protocol address length (PLN) settings.

0: ARP/RARP frames where the HLN is not equal to Ethernet (0x06) or the (PLN) is not equal to IPv4 (0x04).

1: ARP/RARP frames where the HLN is equal to Ethernet (0x06) and the (PLN) is equal to IPv4 (0x04).

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

Ethernet: Specify whether frames can hit the action according to their ARP/RARP hardware address space (HRD) settings.

0: ARP/RARP frames where the HLD is not equal to Ethernet (1).

1: ARP/RARP frames where the HLD is equal to Ethernet (1).

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

IP: Specify whether frames can hit the action according to their ARP/RARP protocol address space (PRO) settings.

0: ARP/RARP frames where the PRO is not equal to IP (0x800).

1: ARP/RARP frames where the PRO is equal to IP (0x800).

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

SIP Address: When "Host" or "Network" is selected for the source IP filter, you can enter a specific SIP address in dotted decimal notation.

SIP Mask: When "Network" is selected for the source IP filter, you can enter a specific SIP mask in dotted

decimal notation.

DIP Filter: Specify the destination IP filter for this ACE.

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

Host: Destination IP filter is set to Host. Specify the destination IP address in the DIP Address field that appears.

Network: Destination IP filter is set to Network. Specify the destination IP address and destination IP mask in the DIP Address and DIP Mask fields that appear.

DIP Address: When "Host" or "Network" is selected for the destination IP filter, you can enter a specific DIP address in dotted decimal notation.

DIP Mask: When "Network" is selected for the destination IP filter, you can enter a specific DIP mask in dotted decimal notation.

IPv6 Parameters

The IPv6 parameters can be configured when Frame Type "IPv6" is selected.

Next Header Filter: Specify the IPv6 next header filter for this ACE.

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

Specific: If you want to filter a specific IPv6 next header filter with this ACE, choose this value. A field for entering an IPv6 next header filter appears.

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

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

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

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

ICMP Parameters

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

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

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

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

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

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

Specific: If you want to filter a specific ICMP code filter with this ACE, you can enter a specific ICMP

code value. A field for entering an ICMP code value appears.

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

TCP/UDP Parameters

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Specific: If you want to filter a specific EtherType filter with this ACE, you can enter a specific EtherType value. A field for entering 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 - 0xFFFF but excluding 0x800(IPv4), 0x806(ARP) and 0x86DD(IPv6). A frame that hits this ACE matches this EtherType value.

Modification Buttons

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



: Inserts a new ACE before the current row.



: Edits the ACE row.



: Moves the ACE up the list.



: Moves the ACE down the list.



: Deletes the ACE.



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

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.

2-5.2.4 IP Source Guard

This section lets you configure the IP Source Guard parameters of the switch. You can use IP Source Guard to enable or disable the switch ports and to specify the maximum number of dynamic clients that can be learned on given port.

2-5.2.4.1 Configuration

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

To configure IP Source Guard in the web UI:

1. Click Configuration > Security > Network > IP Source Guard > Configuration.
2. Select “Enabled” in the Mode of IP Source Guard Configuration.
3. Select “Enabled” on specific port(s) in the Mode of Port Mode Configuration.
4. Select Maximum Dynamic Clients (0, 1, 2, Unlimited) of the specific port at the Mode dropdown in the Port Mode Configuration section.
5. Click Apply.

Figure 2-5.2.4. 1: IP Source Guard Configuration page

The screenshot displays the Lantronix web interface for configuring IP Source Guard. The breadcrumb trail is: Home > Configuration > Security > Network > IP Source Guard > Configuration. The 'Mode' dropdown is currently set to 'Disabled'. A blue button labeled 'Translate dynamic to static' is visible. Below this is the 'Port Mode Configuration' table:

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

Parameter descriptions:

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

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

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

Buttons

Apply: Click to save changes.

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

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

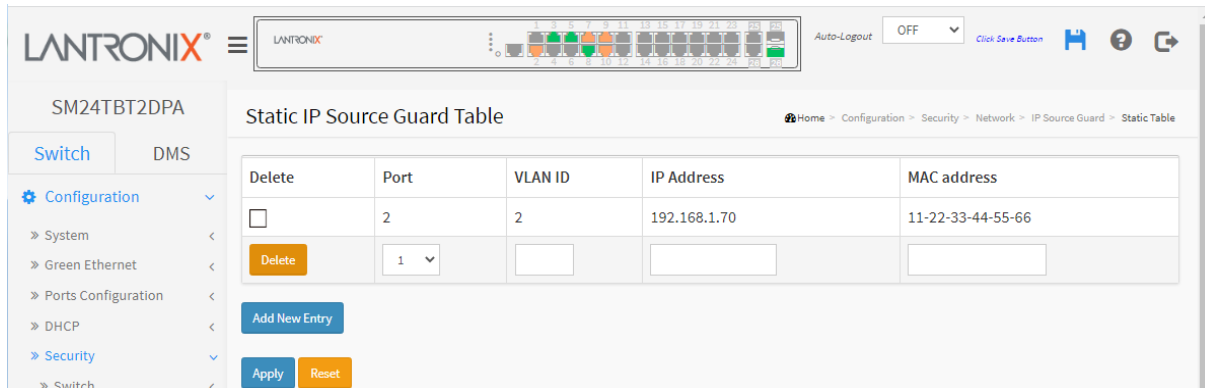
2-5.2.4.2 Static Table

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

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

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

Figure 2-4.2.5.2: Static IP Source Guard Table



Parameter descriptions:

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

Port: The logical port for the settings.

VLAN ID: The VLAN id for the settings.

IP Address: Allowed Source IP address.

MAC address: Allowed Source MAC address.

Buttons:

Apply – Click to save changes.

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

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

2-5.2.5 ARP Inspection

This section lets you configure the ARP Inspection parameters of the switch. You can use the ARP Inspection parameters to manage the ARP table.

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

2-5.2.5.1 Configuration

This page lets you configure ARP Inspection settings including Mode and Port.

1. Navigate to Configuration > Security > Network > ARP Inspection > Port Configuration.
2. Select "Enabled" at the Mode dropdown of ARP Inspection Configuration.
3. Select "Enabled" of the specific port(s) in the Mode column of the Port Mode Configuration section.
4. Click Apply.

Figure 2-4.2.6.1: ARP Inspection Configuration page

The screenshot shows the LANTRONIX web interface for the SM24TBT2DPB switch. The breadcrumb trail is: Home > Configuration > Security > Network > ARP Inspection > Port Configuration. The 'Mode' dropdown is currently set to 'Disabled'. A 'Translate dynamic to static' button is visible. The 'Port Mode Configuration' table is as follows:

Port	Mode	Check VLAN	Log Type
*	Disabled	Disabled	None
1	Disabled	Disabled	None
2	Disabled	Disabled	None
3	Disabled	Disabled	None
4	Disabled	Disabled	None
5	Disabled	Disabled	None
6	Disabled	Disabled	None
7	Disabled	Disabled	None

Parameter descriptions:

Mode of ARP Inspection Configuration: Enable the Global ARP Inspection or disable the Global ARP Inspection.

Port Mode Configuration: Specify ARP Inspection is enabled on which ports. Only when both Global Mode and Port Mode on a given port are enabled, ARP Inspection is enabled on this given port. Possible modes are:

Enabled: Enable ARP Inspection operation.

Disabled: Disable ARP Inspection operation.

Check VLAN: To inspect the VLAN configuration, enable the setting of "Check VLAN". The default setting of "Check VLAN" is disabled. When the setting of "Check VLAN" is disabled, the log type of ARP Inspection will refer to the port setting. 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 Global Mode and Port Mode on a given port are enabled, and the setting of "Check VLAN" is disabled, the log type of ARP Inspection will refer to the port setting. The four possible log types are:

None: Log nothing.

Deny: Log denied entries.

Permit: Log permitted entries.

ALL: Log all entries.

Buttons:

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

Apply – Click to save changes.

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

2-5.2.5.2 VLAN Mode 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. Only valid ARP requests and responses can go through the switch.

Each page shows up to 9999 entries from the VLAN table, default being 20, selected through the "entries per page" input field. When first visited, the web page will show the first 20 entries from the beginning of the VLAN Table. The first displayed will be the one with the lowest VLAN ID found in the VLAN Table.

The "VLAN" input fields let 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 entry) button will use the next entry of the currently displayed VLAN entry as a basis for the next lookup. When the end is reached, the warning message is shown in the displayed table. Use the << button to start over.

To configure VLAN Mode parameters in the web UI:

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

Figure 2-4.2.6.2: VLAN Mode Configuration page

Parameter descriptions:

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

- None:** Log nothing.
- Deny:** Log denied entries.
- Permit:** Log permitted entries.
- ALL:** Log all entries.

Buttons

Add New Entry: Click to add a new VLAN to the table.

Apply: Click to save changes.

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

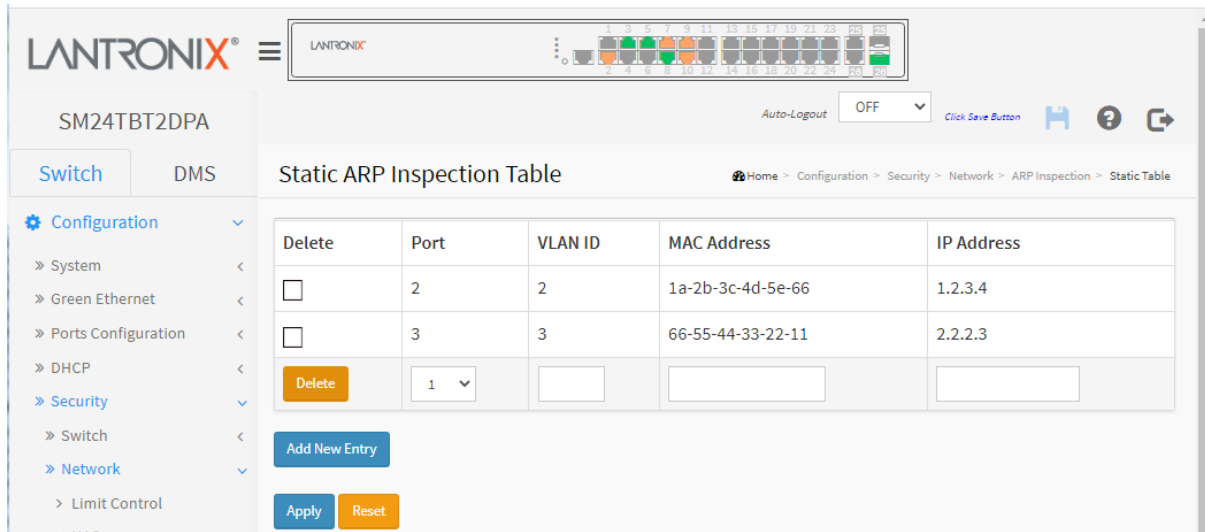
2-5.2.5.3 Static Table

This page lets you configure the Static ARP Inspection Table parameters of the switch. You could use the Static ARP Inspection Table to manage the ARP entries.

To configure Static ARP Inspection in the web UI:

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

Figure 2-4.2.6.3: Static ARP Inspection Table



Parameter descriptions:

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

Port: The logical port for the settings.

VLAN ID: The VLAN ID (VID) for the settings.

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

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

Add New Entry: Click to add a new entry to the Static ARP Inspection table. Specify the Port, VLAN ID, MAC address, and IP address for the new entry. Click "Apply".

Buttons:

Apply: Click to save changes.

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

2-5.2.5.4 Dynamic Table

Entries in the Dynamic ARP Inspection Table are shown on this page. The Dynamic ARP Inspection Table contains up to 1024 entries, and is sorted first by port, then by VLAN ID, then by MAC address, and then by IP address.

Each page shows up to 99 entries from the Dynamic ARP Inspection table, default being 20, selected through the "entries per page" input field. When first visited, the web page will show the first 20 entries from the beginning of the Dynamic ARP Inspection Table.

The "Start from port address", "VLAN", "MAC address" and "IP address" input fields lets you select the starting point in the Dynamic ARP Inspection Table. Clicking the First entry button will update the displayed table starting from that or the closest next Dynamic ARP Inspection Table match. In addition, the two input fields will - upon a First entry button click - assume the value of the first displayed entry, allowing for continuous refresh with the same start address.

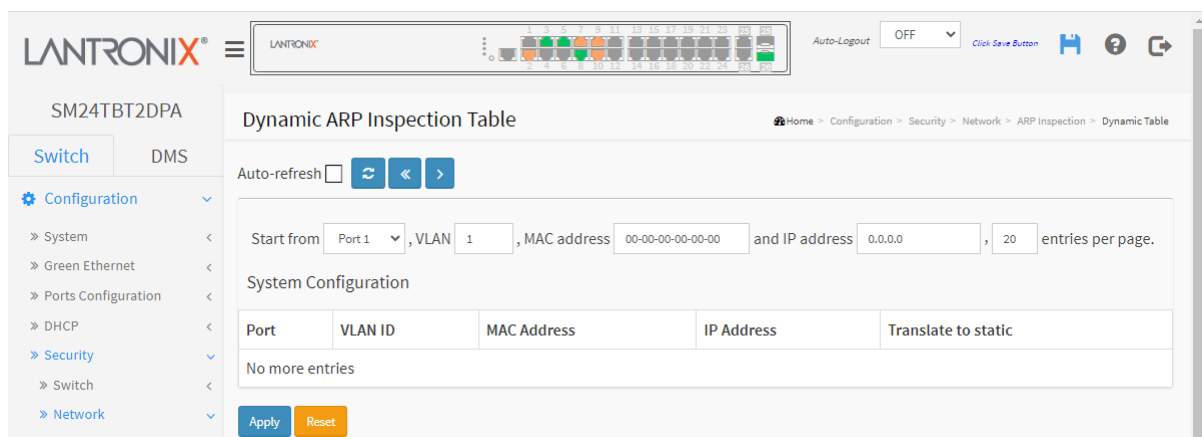
Clicking the Next entry button will use the last entry of the currently displayed table as a basis for the next lookup. When the end is reached the text "*No more entries*" is shown in the displayed table. Use the Refresh button to start over.

Web Interface

To configure Dynamic ARP Inspection in the web UI:

1. Navigate to Configuration > Security> Network> ARP Inspection> Dynamic Table.
2. Enter the Start from, VLAN, MAC address and IP address parameters.
3. Select the number of entries per page.
4. Click Apply.

Figure 2-5.2.5.4: Dynamic ARP Inspection Table



Parameter descriptions:

ARP Inspection Table Columns

Port: Switch Port Number for which the entries are displayed.

VLAN ID: VLAN-ID in which the ARP traffic is permitted.

MAC Address: User MAC address of the entry.

IP Address: User IP address of the entry.

Translate to static: Select the checkbox to translate the entry to static entry.

Buttons:

Apply: Click to save changes.

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

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

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

Save: Click to save changes.

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

<<: Updates the table starting from the first entry in the Dynamic ARP Inspection Table.

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

2-5.3 AAA

This section lets you configure an AAA (Authentication, Authorization, and Accounting) server to provide access control to your network. The AAA server can be a TACACS+ or RADIUS server to create and manage objects that contain settings for using AAA servers.

2-5.3.1 RADIUS

To configure RADIUS Server parameters via the web UI:

1. Navigate to Configuration > Security > AAA > RADIUS.
2. Enter the Global Configuration parameters.
3. Click the Add New Server button and enter the Server Configuration parameters.
4. Click the Apply button.

Figure 2-4.3.2: RADIUS Server Configuration page

The screenshot shows the 'RADIUS Server Configuration' page in the Lantronix web UI. The page is divided into two main sections: 'Global Configuration' and 'Server Configuration'.

Global Configuration:

- Timeout:** 5 seconds
- Retransmit:** 3 times
- Deadtime:** 0 minutes
- Key:** [Masked]
- NAS-IP-Address:** [Empty field]
- NAS-IPv6-Address:** [Empty field]
- NAS-Identifier:** [Empty field]

Server Configuration:

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

Buttons:

Parameter descriptions:

Global Configuration: These settings are common for all 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 (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. See “RADIUS Attributes” below.

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

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

Server Configuration: The table has one row for each RADIUS server and a number of columns:

Delete: To delete a RADIUS server entry, check this box. The entry is deleted at the next Save.

Hostname: The IP address or hostname of the RADIUS server.

Auth Port: The UDP port to use on the RADIUS server for authentication. The officially assigned port number for RADIUS Accounting is 1812. **Note:** by default, many access servers use port 1645 for authentication requests.

Note: For Windows Server information on how to configure ports that Network Policy Server (NPS) uses for Remote Authentication Dial-In User Service (RADIUS) authentication and accounting traffic see the MS [port values and accounting requests](#) document.

Acct Port: The UDP port to use on the RADIUS server for accounting. The officially assigned port number for RADIUS Accounting is 1813. **Note:** by default, many access servers use port 1646 for accounting requests.

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

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

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

Buttons

Add New Server: Click to add a new RADIUS server. An empty row is added to the table, and the RADIUS server can be configured as needed. Up to 5 servers are supported. The Reset button can be used to undo the addition of the new server.

Apply: Click to save changes.

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

Messages:

The value of NAS-IP-Address must be a valid IP address in dotted decimal notation (x.y.z.w), where x, y, z, and w are decimal number between 0 and 255.

The input value NAS-IPv6-Address (11111111) is not a valid IPv6 address.

Hostname must be a valid hostname, unicast IPv4, or unicast IPv6 address

RADIUS Attributes

<u>Value</u>	<u>Description</u>	<u>Data Type</u>	<u>Reference</u>
4	NAS-IP-Address	ipv4addr	IETF RFC2865
32	NAS-Identifier	text	IETF RFC2865
95	NAS-IPv6-Address	ipv6addr	IETF RFC3162

The RADIUS Accounting protocol provides a protocol for carrying accounting information between a Network Access Server and a shared Accounting Server per IETF [RFC 2866](#).

See the [IANA Considerations](#) for guidance regarding IANA registration of values related to RADIUS as defined in IETF [RFC2865](#).

See your RADIUS server documents for more information.

Example:

The screenshot displays the Lantronix web interface for RADIUS Server Configuration. The left sidebar shows a navigation menu with 'Security' > 'AAA' > 'RADIUS' selected. The main content area is titled 'RADIUS Server Configuration' and contains two sections:

Global Configuration

Timeout	5	seconds
Retransmit	3	times
Deadtime	0	minutes
Key	*****	
NAS-IP-Address	<input type="text"/>	
NAS-IPv6-Address	<input type="text"/>	
NAS-Identifier	<input type="text"/>	

Server Configuration

Delete	Hostname	Auth Port	Acct Port	Timeout	Retransmit	Key
<input type="checkbox"/>	RadSrv2	1845	1846	40	80	*****
<input type="checkbox"/>	RadSrv1	1812	1813	50	90	*****
<input type="checkbox"/>	RadSrv3	1812	1813	1	1000	*****
<input type="checkbox"/>	RadSrv4	1845	1846	1000	1	23456%^&*(VBNM

Buttons at the bottom: Add New Server, Apply, Reset.

2-5.3.2 TACACS+

The AAA server can be a TACACS+ server to create and manage objects that contain settings for using AAA servers. To configure TACACS+ via the web UI:

1. Navigate to Configuration > Security > AAA > TACACS+.
2. Enter the Global Configuration parameters.
3. Click the Add New Server button and enter the Server Configuration parameters.
4. Click the Apply button.

Figure 2-5.3.2: TACACS+ Server Configuration page

The screenshot shows the 'TACACS+ Server Configuration' page in the Lantronix web UI. The page has a left sidebar with navigation options like 'Switch', 'DMS', 'Configuration', 'System', 'Green Ethernet', 'Ports Configuration', 'DHCP', 'Security', 'Switch', 'Network', 'AAA', 'RADIUS', 'TACACS+', 'Aggregation', 'Loop Protection', 'Spanning Tree', 'IPMC Profile', 'MVR', 'IPMC', and 'LLDP'. The main content area is titled 'TACACS+ Server Configuration' and is divided into two sections: 'Global Configuration' and 'Server Configuration'.

Global Configuration:

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

Server Configuration:

Delete	Hostname	Port	Timeout	Key
<input type="checkbox"/>	TacSrvr2	49	45	[Masked]
<input type="checkbox"/>	TacSrvr1	49	60	[Masked]
<input type="checkbox"/>	3.4.5.6	49	1	[Masked]
<input type="checkbox"/>	[Blank]	49	[Blank]	[Blank]

At the bottom of the table, there is an 'Add New Server' button and 'Apply' and 'Reset' buttons.

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

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

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

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

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

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

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

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

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

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

Buttons

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.

2-6 Aggregation

This page lets you configure the settings of Link Aggregation. You can bundle more than one port with the same speed, full duplex and the same MAC to be a single logical port, thus the logical port aggregates the bandwidth of these ports. This means you can apply your current Ethernet equipment to build the bandwidth aggregation. For example, if there are three Fast Ethernet ports aggregated in a logical port, then this logical port has bandwidth three times as high as a single Fast Ethernet port.

2-6.1 Static

Ports using Static Trunk as their trunk method can choose their unique Static Group ID to form a logical “trunked port”. The benefit of using Static Trunk method is that a port can immediately become a member of a trunk group without any handshaking with its peer port. This is also a disadvantage because the peer ports of your static trunk group may not know that they should be aggregate together to form a “logic trunked port”. Using Static Trunk on both end of a link is strongly recommended. Please also note that low speed links will stay in “not ready” state when using static trunk to aggregate with high speed links.

To configure Trunk Aggregation Hash mode and Aggregation Group in the web UI:

1. Click Configuration, Aggregation, and then Static to display the Aggregation Mode Configuration.
2. Enable or disable the Aggregation mode function.
3. Select Aggregation Group ID and Port members.
4. Click the Apply button to save the settings.
5. To cancel the settings, click the **Reset** button to revert to previously saved values.

Figure 2-5.1: Aggregation Mode Configuration

The screenshot shows the 'Aggregation Mode Configuration' page for the SM24TBT2DPA device. The left sidebar contains a navigation menu with 'Configuration' expanded to 'Aggregation' and 'Static' selected. The main content area is titled 'Aggregation Mode Configuration' and includes a breadcrumb trail: Home > Configuration > Aggregation > Static.

Hash Code Contributors

Source MAC Address	<input checked="" type="checkbox"/>
Destination MAC Address	<input checked="" type="checkbox"/>
IP Address	<input checked="" type="checkbox"/>
TCP/UDP Port Number	<input checked="" type="checkbox"/>

Aggregation Group Configuration

Group ID	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	
Normal	<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 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 checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	
1	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<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"/>
2	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input 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"/>
3	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<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"/>
4	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
5	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<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"/>
6	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
7	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<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"/>
8	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<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"/>
9	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<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"/>

Below the table, there are input fields for Group ID (1.2.3.4), Speed (1812), Duplex (1813), and other settings. A 'Delete' button and an 'Add New Server' button are also visible.

Hash Code Contributors

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

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

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

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

Aggregation Group Configuration

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

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

Buttons

Apply – Click to save changes.

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

Messages

Message: *Group 1 member counts error!! Local aggregation must include 2-16 ports* displays if you tried to configure an aggregation of less than 2 or more than 16 ports. Click **OK** and re-configure the settings.

Message: *Aggregation Error To many members in the aggregation group* displays if an aggregation was mis-configured. Click the **Previous** button and re-configure the settings.

2-6.2 LACP

This page lets you view and change the current LACP port configuration parameters. An LACP trunk group with more than one ready member-ports is a “real trunked” group. An LACP trunk group with one or less ready member-ports is not a “real trunked” group. **Note:** LACP and Static aggregation cannot both be enabled on the same ports.

To configure LACP port parameters in the web UI:

1. Click Configuration, Aggregation, LACP.
2. Enable or disable LACP on the switch ports.
3. Select the Key parameter (Auto or Specific). The default is Auto.
3. Select the Role (Active or Passive). The default is Active.
4. Click the Apply button to save the settings.
5. To cancel the settings, click the Reset button to revert to previously saved values.

Figure 2-5.2: LACP Port Configuration

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

Port: The switch port number.

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

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

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

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

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

Buttons

Apply – Click to save changes.

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

2-7 Loop Protection

Loop Protection is used to detect the presence of traffic. When the switch receives packets (looping detection frame) with the same MAC address as itself from a port, Loop Protection occurs. The port will be locked when it receives the Loop Protection frames.

To configure Loop Protection parameters in the web UI:

1. Click Configuration, Loop Protection.
2. Enable or disable the port loop Protection.
3. Click the Apply button to save the setting.
4. To cancel the settings, click the Reset button to revert to previously saved values.

Figure 2-7: Loop Protection Configuration

The screenshot shows the 'Loop Protection Configuration' page in the Lantronix web UI. The page title is 'Loop Protection Configuration' and the breadcrumb is 'Home > Configuration > Loop Protection'. The left sidebar shows the navigation menu with 'Loop Protection' selected. The main content area is divided into two sections: 'Global Configuration' and 'Port Configuration'.

Global Configuration:

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

Port Configuration:

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

Parameter descriptions:

Global Configuration

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

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

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

Port 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

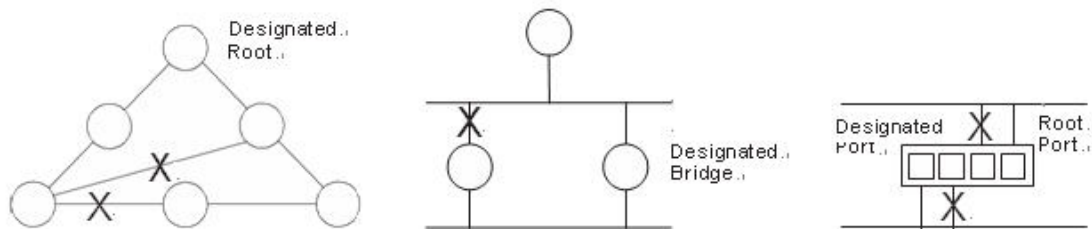
Apply – Click to save changes.

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

2-8 Spanning Tree

The Spanning Tree Protocol (STP) can be used to detect and disable network loops, and to provide backup links between switches, bridges or routers. This allows the switch to interact with other bridging devices (an STP-compliant switch, bridge or router) in your network to ensure that only one route exists between any two stations on the network and provide backup links which automatically take over when a primary link goes down.

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



Once a stable network topology has been established, all bridges listen for Hello BPDUs (Bridge Protocol Data Units) transmitted from the Root Bridge. If a bridge does not get a Hello BPDU after a predefined interval (Maximum Age), the bridge assumes that the link to the Root Bridge is down. This bridge will then initiate negotiations with other bridges to reconfigure the network to reestablish a valid network topology.

Protocol versions:

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

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

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

- > Spanning Tree
- > Bridge Settings
- > MSTI Mapping
- > MSTI Priorities
- > CIST Port
- > MSTI Ports

2-8.1 Bridge Setting

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

To configure Spanning Tree Bridge parameters in the web UI:

1. Click Configuration, Spanning Tree, Bridge Settings.
2. Select Basic Settings parameters.
3. Enable or disable parameters and enter parameters in Advanced settings.
4. Click the Apply button to save the settings.
5. To cancel the settings, click the Reset button. The page will revert to previously saved values.

Figure 2-8.1: STP Bridge Configuration

The screenshot shows the Lantronix web interface for the SM24TBT2DPB switch. The main content area is titled "STP Bridge Configuration" and is divided into two sections: "Basic Settings" and "Advanced Settings".

Basic Settings:

Protocol Version	MSTP
Bridge Priority	32768
Forward Delay	15
Max Age	20
Maximum Hop Count	20
Transmit Hold Count	6

Advanced Settings:

Edge Port BPDU Filtering	<input type="checkbox"/>
Edge Port BPDU Guard	<input type="checkbox"/>
Port Error Recovery	<input type="checkbox"/>
Port Error Recovery Timeout	<input type="text"/>

At the bottom of the configuration area, there are "Apply" and "Reset" buttons. The left sidebar shows a navigation menu with "Spanning Tree" > "Bridge Settings" selected. The top of the page shows the device name "SM24TBT2DPB" and a status bar with "Auto-Logout OFF".

Parameter descriptions:

Basic Settings

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

Bridge Priority: Controls the bridge priority. Lower numeric values have better priority. The bridge priority plus the MSTI instance number, concatenated with the 6-byte MAC address of the switch forms a Bridge Identifier. For MSTP operation, this is the priority of the CIST. Otherwise, this is the priority of the STP/RSTP Bridge.

Forward Delay: The delay used by STP Bridges to transit Root and Designated Ports to Forwarding (used in STP compatible mode). Valid values are in the range 4 to 30 seconds.

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

Maximum Hop Count: This defines the initial value of remaining Hops for MSTI information generated at

the boundary of an MSTI region. It defines how many bridges a root bridge can distribute its BPDU information to. Valid values are in the range 6 to 40 hops.

Transmit Hold Count: The number of BPDU's a bridge port can send per second. When exceeded, transmission of the next BPDU will be delayed. Valid values are in the range 1 to 10 BPDU's per second.

Advanced Settings

Edge Port BPDU Filtering: Control whether a port explicitly configured as Edge will transmit and receive BPDUs.

Edge Port BPDU Guard: Control whether a port explicitly configured as Edge will disable itself upon reception of a BPDU. The port will enter the error-disabled state and will be removed from the active topology.

Port Error Recovery: Control whether a port in the error-disabled state automatically will be enabled after a certain time. If recovery is not enabled, ports have to be disabled and re-enabled for normal STP operation. The condition is also cleared by a system reboot.

Port Error Recovery Timeout: The time to pass before a port in the error-disabled state can be enabled. Valid values are 30 - 86400 seconds (24 hours).

Buttons

Apply – Click to save changes.

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

2-8.2 MSTI Mapping

This page lets you configure and view 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 VLANs not explicitly mapped. This is why you must set the list of VLANs mapped to the MSTI. The VLANs must be separated with comma and/or space.

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

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

1. Click Configuration, Spanning Tree, MSTI Mapping
2. Specify the configuration identification parameters in the field.
3. Specify the VLANs Mapped blank field.
4. Click the Apply button to save the setting
5. To cancel the settings click the Reset button. The page will revert to previously saved values.

Figure 2-9.2: MSTI Configuration page

The screenshot shows the Lantronix web interface for the SM24TBT2DPA switch. The main content area is titled "MSTI Configuration". Under "Configuration Identification", there are two input fields: "Configuration Name" (00-c0-f2-7f-68-5b) and "Configuration Revision" (0). Below this is the "MSTI Mapping" section, which includes a list of MSTI instances (MSTI1, MSTI2, MSTI3, MSTI4) and a table with columns "MSTI" and "VLANs Mapped". The "VLANs Mapped" column is currently empty for all MSTI instances.

Parameter descriptions:

Configuration Identification

Configuration Name: The name identifying the VLAN to MSTI mapping. Bridges must share the name and revision (see below), as well as the VLAN-to-MSTI mapping configuration in order to share spanning trees for MSTI's (Intra-region). The name can have up to 32 characters.

Configuration Revision: The revision of the MSTI configuration named above. This must be an integer between 0 and 65535.

MSTI Mapping: Add VLANs separated by spaces or commas. Unmapped VLANs are mapped to the CIST (the default bridge instance).

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

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

Buttons

Apply: Click to save changes.

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

2-8.3 MSTI Priorities

When you implement a Spanning Tree protocol on the switch that the bridge instance. The CIST is the default instance which is always active. For 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

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

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

1. Click Configuration, Spanning Tree, MSTI Priorities.
2. Select the Priority; the valid range is 0-61440.
3. Click the Apply button to save the settings.
4. To cancel the settings click the Reset button. The page will revert to previously saved values.

Figure 2-8.3: MSTI Configuration page

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

Parameter descriptions:

MSTI: The bridge instance. The CIST is the default instance, which is always active.

Priority: Controls the bridge priority. Lower numeric values have better priority. The bridge priority plus the MSTI instance number, concatenated with the 6-byte MAC address of the switch, forms a Bridge Identifier.

Buttons

Apply – Click to save changes.

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

2-8.4 CIST Ports

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

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

Figure 2-8.4: STP CIST Port Configuration page

Parameter descriptions:

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

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

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

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

AdminEdge: Controls whether the operEdge flag should start as set or cleared. (The initial operEdge state when a port is initialized).

AutoEdge: Controls whether the bridge should enable automatic edge detection on the bridge port. This allows operEdge to be derived from whether BPDU's are received on the port or not.

Restricted Role: If enabled, causes the port not to be selected as Root Port for the CIST or any MSTI, even if it has the best spanning tree priority vector. Such a port will be selected as an Alternate Port after the Root Port has been selected. If set, it can cause lack of spanning tree connectivity. It can be set by a network administrator to prevent bridges external to a core region of the network influence the spanning tree active topology, possibly because those bridges are not under the full control of the administrator. This feature is also known as Root Guard.

Restricted TCN: If enabled, causes the port not to propagate received topology change notifications and topology changes to other ports. If set it can cause temporary loss of connectivity after changes in a spanning tree's active topology as a result of persistently incorrect learned station location information. It is set by a network administrator to prevent bridges external to a core region of the network, causing address flushing in that region, possibly because those bridges are not under the full control of the administrator or the physical link state of the attached LANs transits frequently.

BPDU Guard: If enabled, causes the port to disable itself upon receiving valid BPDU's. Contrary to the similar bridge setting, the port Edge status does not affect this setting. A port entering error-disabled state due to this setting is subject to the bridge Port Error Recovery setting as well.

Point to Point Controls whether the port connects to a point-to-point LAN rather than to a shared medium. This can be automatically determined or forced either true or false. Transition to the forwarding state is faster for point-to-point LANs than for shared media.

Buttons

Apply – Click to save changes.

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

2-8.5 MSTI Ports

This page lets you view and configure the current STP MSTI port configuration parameters.

An MSTI port is a virtual port, which is instantiated separately for each active CIST (physical) port for each MSTI instance configured on and applicable to the port. The MSTI instance must be selected before displaying actual MSTI port configuration options. It contains MSTI port settings for physical and aggregated ports.

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

1. Click Configuration, Spanning Tree, MSTI Ports.
2. Scroll to select the MST1 or other MSTI Port.
3. Click the **Get** button to set the detail parameters of the MSTI Ports.
4. Select all MSTI Port Configuration parameters.
5. Click the Apply button to save the settings.
6. To cancel the settings click the Reset button. The page will revert to previously saved values.

Figure 2-8.5: MSTI Port Configuration page

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

Select MSTI

MST1

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

MSTI Aggregated Ports Configuration

Port	Path Cost	Priority
-	Auto	128

MSTI Normal Ports Configuration - MST1

Port	Path Cost	Priority
*	<>	<>
1	Auto	128
16	Auto	128
17	Auto	128
18	Auto	128

Parameter descriptions:

Port: The switch port number of the corresponding STP CIST (and MSTI) port.

Path Cost: Controls the path cost incurred by the port. The Auto setting will set the path cost as appropriate by the physical link speed, using the 802.1D recommended values. Using the Specific setting, a user-defined value can be entered. The path cost is used when establishing the active topology of the

network. Lower path cost ports are chosen as forwarding ports in favor of higher path cost ports. Valid values are 1 - 200000000.

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

Buttons

Get : Click to retrieve settings for a specific MSTI.

Apply – Click to save changes.

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

2-9 IPMC Profile

This page provides IPMC Profile related configurations.

2-9.1 Profile Table

The IPMC profile is used to deploy the access control on IP multicast streams. You can create a maximum of 64 Profiles with a maximum of 128 corresponding Rules for each Profile.

To configure the IPMC Profile Configuration in the web interface:


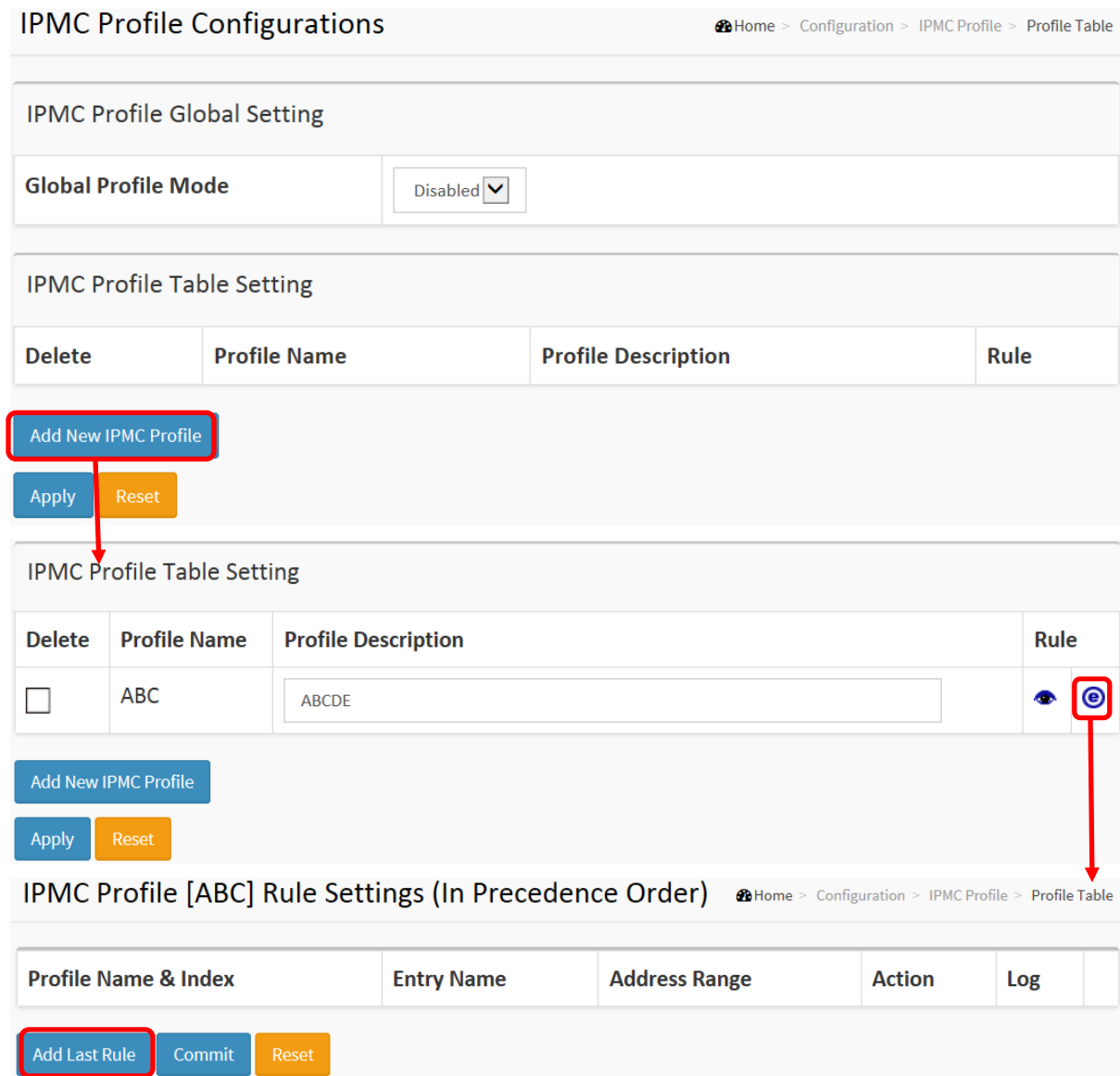
1. Navigate to Configuration > IPMC Profile > Profile Table.
2. At the Global Profile Mode dropdown select Enabled.
3. Click the Add New IPMC Profile button.
4. Enter the Profile Name and Profile Description parameters.
5. Click the Apply button.
6. In the Rule column, click the Edit Profile Rule icon ().
7. Click the Add Last Rule button.
8. Select the Entry Name, Address Range, Action, and Log parameters.

Figure 2-9.1: IPMC Profile Configurations page





IPMC Profile Configurations Home > Configuration > IPMC Profile > Profile Table

IPMC Profile Global Setting

Global Profile Mode Disabled ▾

IPMC Profile Table Setting


Delete	Profile Name	Profile Description	Rule
<input type="checkbox"/>	ABC	ABCDE	 

Add New IPMC Profile Apply Reset

IPMC Profile [ABC] Rule Settings (In Precedence Order) Home > Configuration > IPMC Profile > Profile Table

Profile Name & Index	Entry Name	Address Range	Action	Log
Add Last Rule Commit Reset				

IPMC Profile [ABC] Rule Settings (In Precedence Order) [Home](#) > [Configuration](#) > [IPMC Profile](#) > [Profile Table](#)

Profile Name & Index		Entry Name	Address Range	Action	Log	
ABC	1	<input type="text" value="-"/>	~	Deny <input type="text" value=""/>	Disable <input type="text" value=""/>	

Parameter descriptions:

Port: The switch port number of the corresponding STP CIST (and MSTI) port.

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

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

Profile Name: The name used for indexing the profile table.
Each entry has the unique name which is composed of up to 16 alphabetic and numeric characters.
At least one alphabet must be present.

Profile Description: Additional description, composed of up to 64 alphabetic and numeric characters, about the profile. No blank or space characters are permitted as part of description. Use the "_" or "-" character to separate the description sentences.

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



: List the rules associated with the designated profile.



: Adjust the rules associated with the designated profile.

Buttons

Add New IPMC Profile – Click to add new IPMC profile. Specify the name and configure the new entry. Click “Apply”.

Apply – Click to save changes.

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

Messages: *Please input valid IPv4/IPv6 multicast start address for Entry Range2.*

2-9.1.1 IPMC Profile Rule Settings Table

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

Profile Name: The name of the designated profile to be associated. This field is not editable.

Entry Name: The name used in specifying the address range used for this rule.

Only the existing profile address entries will be chosen in the selected box. This field is not allowed to be selected as none ("-") while the Rule Settings Table is committed.

Address Range: The corresponding address range of the selected profile entry. This field is not editable and will be adjusted automatically according to the selected profile entry.

Action: Indicates the learning action upon receiving the Join/Report frame that has the group address matches the address range of the rule.

Permit: Group address matches the range specified in the rule will be learned.





Deny: Group address matches the range specified in the rule will be dropped.

Log: Indicates the logging preference upon receiving the Join/Report frame that has the group address matches the address range of the rule.

Enable: Corresponding information of the group address, that matches the range specified in the rule, will be logged.

Disable: Corresponding information of the group address, that matches the range specified in the rule, will not be logged.

Rule Management Buttons: You can manage rules and the corresponding precedence order by using these buttons:

- : Insert a new rule before the current entry of rule.
- : Delete the current entry of rule.
- : Moves the current entry of rule up in the list.
- : Moves the current entry of rule down in the list.

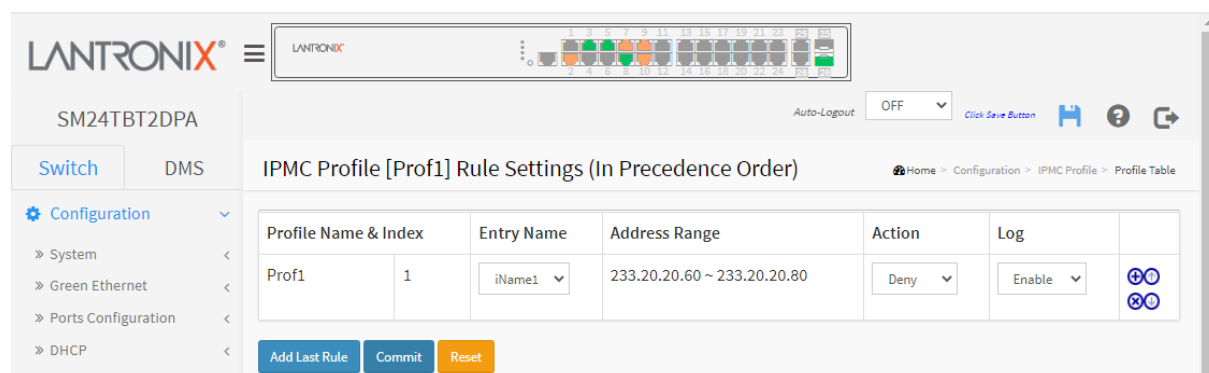
Buttons

Add Last Rule – Click to add a new rule in the end of the specific profile's rule list. Specify the address entry and configure the new entry. Click "Commit".



Commit – Click to commit rule changes for the designated profile.

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

Example:



The screenshot shows the Lantronix web interface for the SM24TBT2DPA device. The main content area displays the "IPMC Profile [Prof1] Rule Settings (In Precedence Order)" table. The table has the following structure:

Profile Name & Index	Entry Name	Address Range	Action	Log	
Prof1 1	iName1	233.20.20.60 ~ 233.20.20.80	Deny	Enable	 

Below the table are three buttons: "Add Last Rule" (blue), "Commit" (blue), and "Reset" (orange). The interface also shows a navigation menu on the left with options like "Configuration", "System", "Green Ethernet", "Ports Configuration", "DHCP", and "Security".

2-9.2 Address Entry

This page provides address range settings used in IPMC profile. The address entry is used to specify the address range that will be associated with IPMC Profile. You can create up to 128 address entries per switch.

To configure IPMC Profile Address parameters in the web UI:

The image displays two screenshots of the IPMC Profile Address Configuration web UI. The top screenshot shows the 'Add New Address (Range) Entry' button highlighted with a red box and a red arrow pointing to the 'Apply' button. The bottom screenshot shows the table with empty input fields for 'Entry Name', 'Start Address', and 'End Address'.

IPMC Profile Address Configuration Home > Configuration > IPMC Profile > Address Entry

Navigate Address Entry Setting in IPMC Profile by entries per page.

Delete	Entry Name	Start Address	End Address
<input type="button" value="Add New Address (Range) Entry"/>			
<input type="button" value="Apply"/>	<input type="button" value="Reset"/>		

IPMC Profile Address Configuration Home > Configuration > IPMC Profile > Address Entry

Navigate Address Entry Setting in IPMC Profile by entries per page.

Delete	Entry Name	Start Address	End Address
<input type="button" value="Delete"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>
<input type="button" value="Add New Address (Range) Entry"/>			
<input type="button" value="Apply"/>	<input type="button" value="Reset"/>		

Parameter descriptions:

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

Entry Name: The name used for indexing the address entry table. Each entry has the unique name which is composed of at maximum 16 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 new address range. Specify the name and configure the addresses. Click “Apply”

Apply – Click to save changes.

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

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

<< – Updates the table starting from the first entry in the IPMC Profile Address Configuration.

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

2-10 MVR

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

To configure MVR parameters in the web UI:

1. Click Configuration, MVR.
2. At the dropdown select the MVR mode (enable or disable) and scroll to set all parameters.
3. Click the Add New MVR VLAN button and configure.
4. Click the Apply button to save the setting
5. To cancel settings, click the Reset button. The page will revert to previously saved values.

Figure 2-10: MVR Configurations page

Parameter descriptions:

MVR Mode: Enable/Disable the Global MVR.

The Unregistered Flooding control depends on the current configuration in IGMP/MLD Snooping. It is suggested to enable Unregistered Flooding control when the MVR group table is full.

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

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

MVR Name: MVR Name is an optional attribute to indicate the name of the specific MVR VLAN. Maximum length of the MVR VLAN Name string is 32. MVR VLAN Name can only contain 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 the IPv4 management address is not set, system uses the first available IPv4 management address. Otherwise, system uses a pre-defined value. By default, this value will be 192.0.2.1.

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

Tagging: Specify whether the traversed IGMP/MLD control frames will be sent as Untagged or Tagged with MVR VID. The default is tagged.

Priority: Specify how the traversed IGMP/MLD control frames will be sent in prioritized manner. The default Priority is 0.

LLQI: Define the maximum time to wait for IGMP/MLD report memberships on a receiver port before removing the port from multicast group membership. The value is in units of tenths of a second. The range is 0 - 31744. The default LLQI is 5 tenths or one-half second. LLQI (Last Listener Query Interval) is the maximum response time used to calculate the Maximum Response Code inserted into Specific Queries. It is used to detect the departure of the last listener for a multicast address or source. In IGMP, this term is called LMQI (Last Member Query Interval).

Interface Channel Setting: When the MVR VLAN is created, click the Edit symbol to expand the corresponding multicast channel settings for the specific MVR VLAN. Summary about the Interface Channel Setting (of the MVR VLAN) will be shown besides the Edit symbol.

Port: The logical port for the settings.

Role: Select the port role by clicking the Role symbol to switch the setting. **I** indicates Inactive; **S** indicates Source; **R** indicates Receiver. The default Role is Inactive. Configure an MVR port of the designated MVR VLAN as one of the following roles:

Inactive: The designated port does not participate in MVR operations.

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

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

Caution: MVR source ports are not recommended to be overlapped with management VLAN ports.

Immediate Leave: Enable or disable fast leave on a port.

Enabled: the routing device leaves the multicast group immediately after the last host leaves the multicast group (host tracking enabled - the device keeps track of the hosts that send join messages).

Disabled: if one host sends a leave group message, the routing device first sends a group query to determine if another receiver responds. If no receiver responds, the routing device removes all hosts on the interface from the multicast group.

Multicast snooping Fast Leave processing allows the switch to remove an interface from the forwarding-table entry without first sending out group specific queries to the interface. The VLAN interface is pruned from the multicast tree for the multicast group specified in the original leave message. Fast-leave processing ensures optimal bandwidth management for all hosts on a switched network, even when multiple multicast groups are in use simultaneously. This processing applies to IGMP and MLD.

Buttons

Add New MVR VLAN – Click to add new MVR VLAN. Specify the VID 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.

Message: *MVR Interface Configuration Error Failure in SET MVR VLAN VID 2*

2-11 IPMC

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

2-11.1 IGMP Snooping

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

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

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

2-11.1.1 Basic Configuration

This page lets you set basic IGMP snooping on the switch, which connects to a router closer to the root of the tree. This interface is the upstream interface. The router on the upstream interface should be running IGMP.

Web Interface

To configure IGMP Snooping parameters in the web UI:

1. Click Configuration, IPMC, IGMP Snooping, Basic Configuration.
2. Enable or disable IPMC globally.
3. Select which port is to become a Router Port or enable/ disable the Fast Leave function.
4. At the Throttling dropdown, select the Throttling parameter.
5. Click the Apply button to save the settings.
6. To cancel the settings, click the Reset button. The page will revert to previously saved values.

Figure 2-12.1.1: IGMP Snooping Configuration page

LANTRONIX SM24TBT2DPA

IGMP Snooping Configuration

Global Configuration

Snooping Enabled	<input type="checkbox"/>
Unregistered IPMCv4 Flooding Enabled	<input checked="" type="checkbox"/>
IGMP SSM Range	232.0.0.0 / 8
Leave Proxy Enabled	<input type="checkbox"/>
Proxy Enabled	<input type="checkbox"/>

Port Related Configuration

Port	Router Port	Fast Leave	Throttling
*	<input type="checkbox"/>	<input type="checkbox"/>	↔
1	<input type="checkbox"/>	<input type="checkbox"/>	unlimited
2	<input type="checkbox"/>	<input type="checkbox"/>	unlimited
3	<input type="checkbox"/>	<input type="checkbox"/>	unlimited
4	<input type="checkbox"/>	<input type="checkbox"/>	unlimited
5	<input type="checkbox"/>	<input type="checkbox"/>	unlimited
6	<input type="checkbox"/>	<input type="checkbox"/>	unlimited

Parameter descriptions:

Snooping Enabled: Check the box to enable IGMP Snooping globally.

Unregistered IPMCv4 Flooding Enabled: Enable unregistered IPMCv4 traffic flooding.

IGMP SSM Range: SSM (Source-Specific Multicast) Range allows the SSM-aware hosts and routers run the SSM service model for the groups in the address range. Format: (IP address/ sub mask)

Leave Proxy Enable: Enable IGMP Leave Proxy. This feature can be used to avoid forwarding unnecessary leave messages to the router side.

Proxy Enabled: Enable IGMP Proxy. This feature can be used to avoid forwarding unnecessary join and leave messages to the router side.

Port: It shows the physical Port index of the switch.

Router Port: Specify which ports act as router ports. A router port is a port on the Ethernet switch that leads towards the Layer 3 multicast device or IGMP querier. If an aggregation member port is selected as a router port, the whole aggregation will act as a router port.

Fast Leave: Enable the fast leave on the port.

Throttling: Enable to limit the number of multicast groups to which a switch port can belong.

Buttons

Apply – Click to save changes.

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

2-11.1.2 VLAN Configuration

This page lets you set the VLAN configuration parameters integrated with IGMP Snooping function.

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 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.

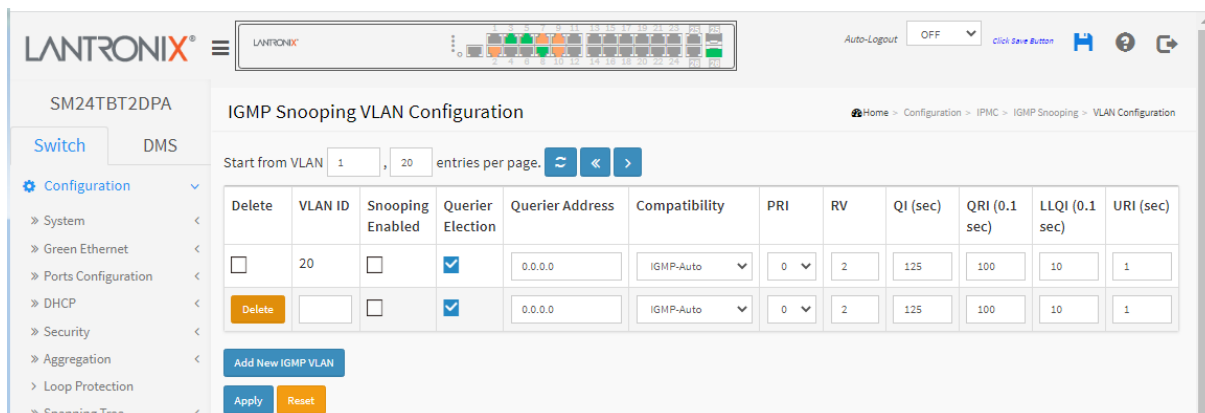
The << will use the last entry of the currently displayed entry as a basis for the next lookup. When the end is reached the text "No more entries" displays in the table. Use the > button to start over.

Web Interface

To configure IGMP Snooping VLAN parameters in the web UI:

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

Figure 2-11.1.2: IGMP Snooping VLAN Configuration page



Parameter descriptions:

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

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

IGMP Snooping Enabled: Enable the per-VLAN IGMP Snooping. Only up to 32 VLANs can be selected.

Querier Election: Enable to join IGMP Querier election in the VLAN. Disable to act as an IGMP Non-Querier.

Querier Address: Define the IPv4 address as source address used in IP header for IGMP Querier election. When the Querier address is not set, system uses IPv4 management address of the IP interface associated with this VLAN. When the IPv4 management address is not set, system uses the first available IPv4 management address. 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, Forced IGMPv3; default compatibility value is IGMP-Auto.

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

Rv: The 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: The Query Interval is the interval between General Queries sent by the Querier. The allowed range is 1 to 31744 seconds; default QI is 125 seconds.

QRI: Query Response Interval; the Max Response Time used to calculate the Max Resp Code inserted into the periodic General Queries. The allowed range is 0 to 31744 in tenths of seconds; the default QRI is 100 in tenths of seconds (10 seconds).

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

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

Buttons:

Add New IGMP VLAN - Click to add a new IGMP VLAN. Specify the VID and configure the new entry. Click "Apply". The specific IGMP VLAN starts working after the corresponding static VLAN is also created.

Apply – Click to save changes.

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

Refresh: Click to refresh the displayed table starting from the "VLAN" input fields.

<<: Click to update the table starting from the first entry in the VLAN table, i.e. the entry with the lowest VLAN ID.

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

2-11.1.3 Port Filtering Profile

This page lets you set IGMP Port Group Filtering parameters. In some network Application environments, such as metropolitan or multiple-dwelling unit (MDU) installations, a user might want to control the multicast groups to which a user on a switch port can belong. It lets you control the distribution of multicast services, such as IP/TV, based on some type of subscription or service plan.

With this feature, you can filter multicast joins on a per-port basis by configuring IP multicast profiles and associating them with individual switch ports. An IGMP profile can contain one or more multicast groups and specifies whether access to the group is permitted or denied. If an IGMP profile denying access to a multicast group is applied to a switch port, the IGMP join report requesting the stream of IP multicast traffic is dropped, and the port is not allowed to receive IP multicast traffic from that group.








If the filtering action permits access to the multicast group, the IGMP report from the port is forwarded for normal processing.

IGMP filtering controls only IGMP membership join reports and has no relationship to the function that directs the forwarding of IP multicast traffic.

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

1. Click Configuration, IPMC, IGMP Snooping, Port Group Filtering
2. Click Add new Filtering Group
3. Scroll the Port to enable the Port Group Filtering. Specify the Filtering Groups in the blank field.
4. Click Apply to save the setting
5. To cancel the settings click the Reset button. The page will revert to previously saved values.

Figure 2-11.1.3: IGMP Snooping Port Filtering Profile Configuration page

Port	Filtering Profile
1	 -
2	 -
3	 -
4	 -
5	 -
6	 -
7	 -

Parameter descriptions:

Port: The logical port for the settings.

Filtering Profile: Select the IPMC Profile as the filtering condition for the specific port. A summary of the designated profile is displayed by clicking the view () button.

Profile Management button: You can inspect the rules of the designated profile by using the following button:



: Navigate Profile; view the rules associated with the designated profile.

Buttons:

Apply – Click to save changes.

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

Example:

The screenshot displays the web management interface for the SM24TBT2DPA switch. The main title is "IGMP Snooping Port Filtering Profile Configuration". The breadcrumb trail is "Home > Configuration > IPMC > IGMP Snooping > Port Filtering Profile". The interface includes a navigation menu on the left with "Configuration" expanded to "IGMP Snooping" > "Port Filtering Profile". The main content area shows a table with 9 rows, each representing a port. The "Filtering Profile" column contains a dropdown menu for each port. Port 5 is highlighted with a blue border, and its dropdown menu is open, showing "Prof2" selected. Other ports have either "Prof1" or "-" selected.

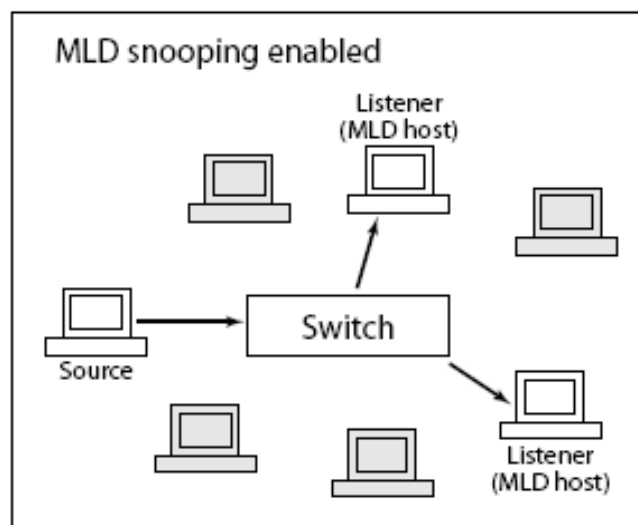
Port	Filtering Profile
1	-
2	Prof1
3	Prof1
4	Prof2
5	Prof2
6	-
7	-
8	-
9	-

2-11.2 MLD Snooping

A network node that acts as a source of IPv6 multicast traffic is only an indirect participant in MLD snooping; it just provides multicast traffic, and MLD doesn't interact with it. Note, however, that in an application like desktop conferencing a network node may act as both a source and an MLD host; but MLD interacts with that node only in its role as an MLD host.

A source node creates multicast traffic by sending packets to a multicast address. In IPv6, addresses with the first eight bits set (that is, "FF" as the first two characters of the address) are multicast addresses, and any node that listens to such an address will receive the traffic sent to that address. Application software running on the source and destination systems cooperates to determine what multicast address to use. (Note that this is a function of the application software, not of MLD.)

When MLD snooping is enabled on a VLAN, the switch acts to minimize unnecessary multicast traffic. If the switch receives multicast traffic destined for a given multicast address, it forwards that traffic only to ports on the VLAN that have MLD hosts for that address. It drops that traffic for ports on the VLAN that have no MLD hosts.



2-11.2.1 Basic Configuration

This section describes how to configure the MLD Snooping basic configuration parameters.

Web Interface

To configure MLD Snooping in the web UI:

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

Figure 2-11.2.1: MLD Snooping Configuration page

The screenshot shows the MLD Snooping Configuration page in the Lantronix web interface. The page is titled "MLD Snooping Configuration" and is part of the "Basic Configuration" section under "IPMC". The interface includes a navigation menu on the left and a main configuration area on the right.

Global Configuration

Snooping Enabled	<input type="checkbox"/>
Unregistered IPMCv6 Flooding Enabled	<input checked="" type="checkbox"/>
MLD SSM Range	ff3e:: / 96
Leave Proxy Enabled	<input type="checkbox"/>
Proxy Enabled	<input type="checkbox"/>

Port Related Configuration

Port	Router Port	Fast Leave	Throttling
*	<input type="checkbox"/>	<input type="checkbox"/>	<>
1	<input type="checkbox"/>	<input type="checkbox"/>	unlimited
2	<input type="checkbox"/>	<input type="checkbox"/>	unlimited
3	<input type="checkbox"/>	<input type="checkbox"/>	unlimited
4	<input type="checkbox"/>	<input type="checkbox"/>	unlimited
5	<input type="checkbox"/>	<input type="checkbox"/>	unlimited
6	<input type="checkbox"/>	<input type="checkbox"/>	unlimited
7	<input type="checkbox"/>	<input type="checkbox"/>	unlimited

Parameter descriptions:

Snooping Enabled: Check to enable Global MLD Snooping.

Unregistered IPMCv6 Flooding Enabled: Enable unregistered IPMCv6 traffic flooding. The flooding control takes effect only when MLD Snooping is enabled. When MLD Snooping is disabled, unregistered IPMCv6 traffic flooding is always active in spite of this setting.

MLD SSM Range: SSM (Source-Specific Multicast) Range allows the SSM-aware hosts and routers run the SSM service model for the groups in the address (Using IPv6 Address) range.

Leave Proxy Enabled: Enable MLD Leave Proxy. This feature can be used to avoid forwarding unnecessary leave messages to the router side.

Proxy Enabled: Enable MLD Proxy. This feature can be used to avoid forwarding unnecessary join and leave messages to the router side.

Router Port: Specify which ports act as router ports. A router port is a port on the Ethernet switch that leads towards the Layer 3 multicast device or MLD querier. If an aggregation member port is selected as a router port, the whole aggregation will act as a router port.

Fast Leave: Check to enable Fast leave on the port. Multicast snooping Fast Leave processing allows the switch to remove an interface from the forwarding-table entry without first sending out group specific queries to the interface. The VLAN interface is pruned from the multicast tree for the multicast group specified in the original leave message. Fast-leave processing ensures optimal bandwidth management for all hosts on a switched network, even when multiple multicast groups are in use simultaneously. This processing applies to IGMP and MLD.

Throttling: Enable to limit the number of multicast groups to which a switch port can belong (1-10 or unlimited).

2-11.2.2 VLAN Configuration

When MLD snooping is enabled on a VLAN, the switch acts to minimize unnecessary multicast traffic. If the switch receives multicast traffic destined for a given multicast address, it forwards that traffic only to ports on the VLAN that have MLD hosts for that address. It drops that traffic for ports on the VLAN that have no MLD hosts

Clicking 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 **Refresh** button to start over.

Web Interface

To configure the MLD Snooping VLAN Configuration in the web UI:

1. Click Configuration, IPMC, MLD Snooping, VLAN Configuration
2. Specify the VLAN ID with entries per page.
3. Click "Refresh" to refresh an entry of the MLD Snooping VLAN Configuration Information.
4. Click "<< or >>" to move to previous or next entry.

Figure 2-11.2.2: MLD Snooping VLAN Configuration page

Parameter descriptions:

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

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

IGMP Snooping Enabled: Enable the per-VLAN IGMP Snooping. Up to 32 VLANs can be selected.

Querier Election: Enable to join IGMP Querier election in the VLAN. Disable to act as an IGMP Non-Querier.

Querier Address: Define the IPv4 address as source address used in IP header for IGMP Querier election. When the Querier address is not set, system uses IPv4 management address of the IP interface associated with this VLAN. When the IPv4 management address is not set, system uses the first available IPv4 management address. Otherwise, system uses a pre-defined value. By default, this value will be 192.0.2.1.

Compatibility: Compatibility is maintained by hosts and routers taking appropriate actions depending on the versions of IGMP operating on hosts and routers within a network. The allowed selection is IGMP-Auto, Forced IGMPv1, Forced IGMPv2, Forced IGMPv3, default compatibility value is IGMP-Auto.

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

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

QI: Query Interval. The Query Interval is the interval between General Queries sent by the Querier. The allowed range is 1 to 31744 seconds; the default QI is 125 seconds.

QRI: Query Response Interval. The Max Response Time used to calculate the Max Resp Code inserted into the periodic General Queries. The allowed range is 0 to 31744 in tenths of a second; the default QRI is 100 in tenths of a second (10 seconds).

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

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

Buttons:

Add New MLD VLAN: Click to add new MLD VLAN. Specify the VID and configure the new entry. Click "Apply". The specific MLD VLAN starts working after the corresponding static VLAN is also created.

Apply – Click to save changes.

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

Refresh: Click to refresh the displayed table starting from the "VLAN" input fields.

<<: Click to update the table starting from the first entry in the VLAN table, i.e. the entry with the lowest VLAN ID.

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

Messages:

*MVR Interface Configuration Error
Failure in SET MVR VLAN VID 20*

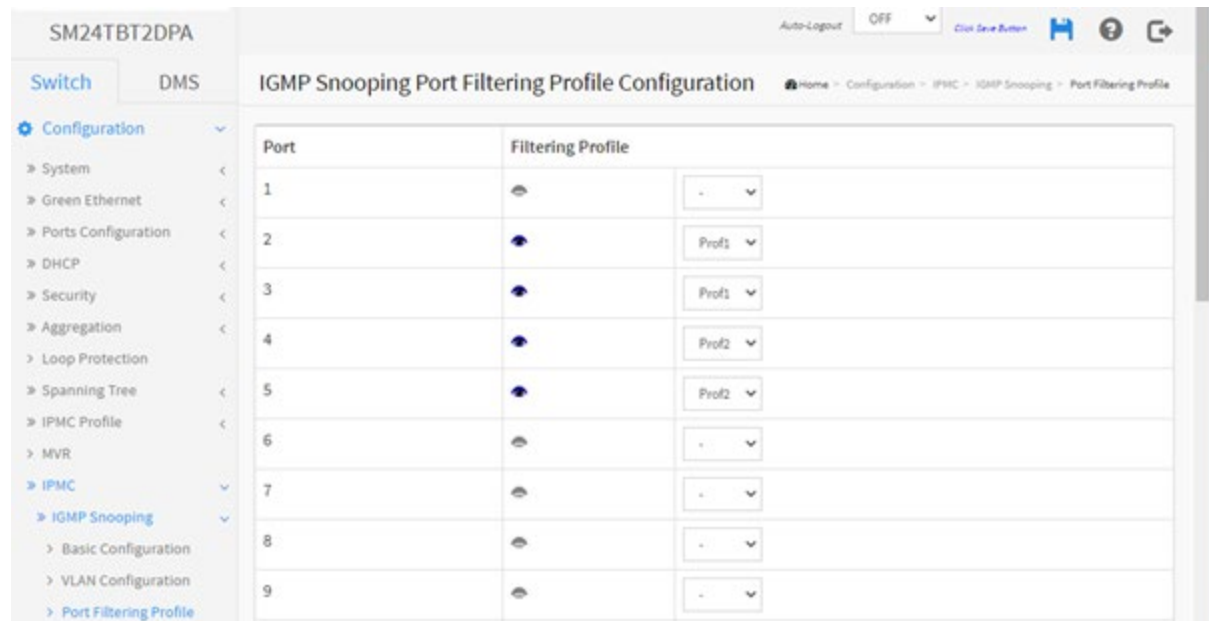
2-11.2.3 Port Filtering Profile

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

To configure MLD Snooping Port Filtering parameters in the web UI:


1. Click Configuration, IPMC, MLD Snooping, Port Filtering Profile.
2. Click the Add New Filtering Group button.
3. Specify the Filtering Groups with entries per page.
4. Click **Apply** to save the setting.
5. To cancel the settings click the **Reset** button. The page will revert to previously saved values.

Figure 2-11.2.3: MLD Snooping Port Filtering Configuration





Parameter descriptions:

Port: The logical port for the settings.

Filtering Profile: Select the IPMC Profile as the filtering condition for the specific port. Summary about the designated profile will be shown by clicking the view () button.

Navigate Profile button: You can inspect the rules of the designated profile by using the following button:

 : View the rules associated with the designated profile. The button is greyed out () if no profile name has been assigned.

Buttons:

Apply – Click to save changes.

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

2-12 LLDP

The Link Layer Discovery Protocol (LLDP) provides a standards-based way for switches to advertise themselves to adjacent devices and to learn about adjacent LLDP devices.

LLDP is a vendor-neutral Link Layer protocol in the Internet Protocol Suite used by network devices for advertising their identity, capabilities, and neighbors on a IEEE 802 local area network, principally wired Ethernet. The protocol is formally referred to by the IEEE as *Station and Media Access Control Connectivity Discovery* specified in standards document IEEE 802.1AB.

2-12.1 LLDP Configuration

This page lets you view and configure the current LLDP port settings. You can configure LLDP and detailed per-port parameters here; the settings will take effect immediately.

To configure LLDP via the Web UI:

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

Figure 2-13.1: LLDP Configuration page

The screenshot shows the Lantronix web interface for device SM24TBT2DPB. The main content area is titled 'LLDP Configuration'. It is divided into two sections: 'LLDP Parameters' and 'LLDP Port Configuration'.

LLDP Parameters:

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

LLDP Port Configuration:

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

Parameter descriptions:**LLDP Parameters**

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

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

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

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

LLDP Port Configuration

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

Mode: Select the LLDP mode:

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

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

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

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

CDP Aware: Check the box to enable CDP (Cisco Discovery Protocol) awareness. CDP operation is restricted to decoding incoming CDP frames (The switch doesn't transmit CDP frames). CDP frames are only decoded if LLDP on the port is enabled.

Only CDP TLVs that can be mapped to a corresponding field in the LLDP neighbors' table are decoded. All other TLVs are discarded (Unrecognized CDP TLVs and discarded CDP frames are not shown in the LLDP statistics.). CDP TLVs are mapped onto LLDP neighbors' table as shown below.

CDP TLV "Device ID" is mapped to the LLDP "Chassis ID" field.

CDP TLV "Address" is mapped to the LLDP "Management Address" field. The CDP address TLV can contain multiple addresses, but only the first address is shown in the LLDP neighbors' table.

CDP TLV "Port ID" is mapped to the LLDP "Port ID" field.

CDP TLV "Version and Platform" is mapped to the LLDP "System Description" field.

Both the CDP and LLDP support "system capabilities", but the CDP capabilities cover capabilities that are not part of the LLDP. These capabilities are shown as "others" in the LLDP neighbors' table.

If all ports have CDP awareness disabled the switch forwards CDP frames received from neighbor devices. If at least one port has CDP awareness enabled all CDP frames are terminated by the switch.



NOTE: When CDP awareness on a port is disabled the CDP information isn't removed immediately but gets removed when the hold time is exceeded.

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.

Note: Link Layer Discovery Protocol (LLDP) is a layer 2 Ethernet protocol for managing devices. LLDP allows an exchange of information between a PSE and a PD. This information is formatted in Type-Length-Value (TLV) format. PoE standards define TLV structures used by PSEs and PDs to signal and negotiate available power.

The type and length are fixed in size (typically 1-4 bytes), and the value field is of variable size. These fields are used:

Type: A binary code, often simply alphanumeric, which indicates the kind of field that this part of the message represents;

Length: The size of the value field (typically in bytes);

Value: Variable-sized series of bytes which contains data for this part of the message.

2-12.2 LLDP-MED Configuration

This page lets you configure LLDP-MED. This function applies to VoIP devices supporting LLDP-MED. Media Endpoint Discovery is an LLDP enhancement, known as LLDP-MED, that provides these facilities:

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

To configure LLDP-MED in the web UI:

1. Click Configuration > LLDP > MEDLLDP-MED.
2. Modify the Fast start repeat count parameter; the default is 4.
3. Modify Coordinates Location parameters.
4. Fill Civic Address Location parameters.
5. Click Add New Policy.
6. Click Apply, will show following Policy Port Configuration.
7. Select Policy ID for each port.
8. Click Apply.

Figure 2-12.2: LLDP-MED Configuration page

The screenshot displays the LLDP-MED Configuration page in the Lantronix web UI. The page is titled "LLDP-MED Configuration" and is part of the "Configuration" menu. The left sidebar shows the navigation tree with "LLDP-MED" selected. The main content area is divided into several sections:

- Fast Start Repeat Count:** A text input field containing the value "4".
- Coordinates Location:** A form with fields for Latitude (0), Longitude (0), Altitude (0), and Map Datum (WGS84). Latitude and Longitude have dropdown menus for North and East, and Altitude has a dropdown for Meters.
- Civic Address Location:** A form with multiple fields for location details: Country code, State/Province, County, City, City district, Block (Neighborhood), Street, Leading street direction, Trailing street suffix, Street suffix, House no., House no. suffix, Landmark, Additional location info, Name, Zip code, Building, Apartment, Floor, Room no., Place type, Postal community name, P.O. Box, and Additional code.
- Emergency Call Service:** A text input field for the Emergency Call Service.
- Policies:** A table with columns: Delete, Policy ID, Application Type, Tag, VLAN ID, L2 Priority, and DSCP. The table is currently empty, showing "No entries present". Below the table is a blue "Add New Policy" button.

Parameter descriptions:

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

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

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

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

Coordinates Location

Latitude: Latitude SHOULD be normalized to within 0-90 degrees with a maximum of 4 digits. It is possible to specify the direction to either North of the equator or South of the equator.

Longitude: Longitude SHOULD be normalized to within 0-180 degrees with a maximum of 4 digits. It is possible to specify the direction to either East of the prime meridian or West of the prime meridian.

Altitude: Altitude SHOULD be normalized to within -32767 to 32767 with a maximum of 4 digits. It is possible to select between two altitude types (floors or meters).

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

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

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

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

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

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

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

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

State: 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 (Neighbourhood): Neighborhood, block.

Street: Street - Example: Poppelvej.

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

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

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

House no.: House number - Example: 21.

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

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

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

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

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

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

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

Floor: Floor - Example: 4.

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

Place type: Place type - Example: Office.

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

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

Additional code: Additional code - Example: 1320300003.

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

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

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

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

The network policy attributes advertised are:

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

1. Voice
2. Guest Voice
3. Softphone Voice
4. Video Conferencing
5. Streaming Video
6. Control / Signaling (conditionally support a separate network policy for the media types above).

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

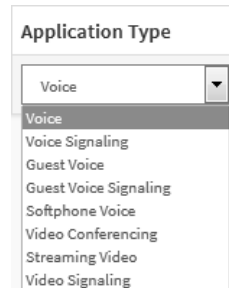
It should be noted that LLDP-MED is not intended to run on links other than between Network Connectivity Devices and Endpoints, and therefore does not need to advertise the multitude of network policies that frequently run on an aggregated link interior to the LAN.

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

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

Application Type: Intended use of the application types:

1. **Voice** - for use by dedicated IP Telephony handsets and other similar appliances supporting interactive voice services. These devices are typically deployed on a separate VLAN for ease of deployment and enhanced security by isolation from data applications.
2. **Voice Signaling** (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.
3. **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.
4. **Guest Voice Signaling** (conditional) - for use in network topologies that require a different policy for the guest voice Signaling than for the guest voice media. This application type should not be advertised if all the same network policies apply as those advertised in the Guest Voice application policy.
5. **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.
6. **Video Conferencing** - for use by dedicated Video Conferencing equipment and other similar appliances supporting real-time interactive video/audio services.
7. **Streaming Video** - for use by broadcast or multicast based video content distribution and other similar applications supporting streaming video services that require specific network policy treatment. Video applications relying on TCP with buffering would not be an intended use of this application type.
8. **Video Signaling** (conditional) - for use in network topologies that require a separate policy for the video Signaling than for the video media. This application type should not be advertised if all the same network policies apply as those advertised in the Video Conferencing application policy.



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

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

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

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

L2 Priority: The Layer 2 priority to be used for the specified application type. L2 Priority may specify one of eight priority levels (0 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: the DSCP value to be used to provide Diffserv node behavior for the specified application type as defined in IETF RFC 2474. DSCP may contain one of 64 code point values (0 through 63). A value of 0 represents use of the default DSCP value as defined in RFC 2475.

Port Policies Configuration: Every port may advertise a unique set of network policies or different

attributes for the same network policies, based on the authenticated user identity or port configuration.

Port: The port number to which the configuration applies.

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

Buttons:

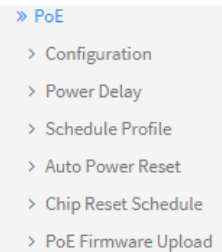
Add New Policy: Click to add a new policy. Specify the Application type, Tag, VLAN ID, L2 Priority and DSCP for the new policy. Click "Apply".

Apply : Click to save changes.

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

2- 13 PoE

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



2- 13.1 Configuration

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

Power Over Ethernet Configuration (before FW vB6.54.3576)

To configure Power over Ethernet via the web UI:

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

Figure 2-13.1: PoE Configuration page (SM24TBT2DPA before FW vB6.54.3476)

Port	PoE Mode	PoE Schedule	Priority	Capacitor Detection	Maximum Power [W]
*	<<	<<	<<	<input type="checkbox"/>	90
1	Enabled	Disabled	Low	<input type="checkbox"/>	90
2	Enabled	Disabled	Low	<input type="checkbox"/>	90
3	Enabled	Disabled	Low	<input type="checkbox"/>	90
4	Enabled	Disabled	Low	<input type="checkbox"/>	90
5	Enabled	Disabled	Low	<input type="checkbox"/>	90
6	Enabled	Disabled	Low	<input type="checkbox"/>	90
7	Enabled	Disabled	Low	<input type="checkbox"/>	90
8	Enabled	Disabled	Low	<input type="checkbox"/>	90
9	Enabled	Disabled	Low	<input type="checkbox"/>	90

Parameter descriptions: (before FW vB6.54.3476)

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; for 4, 7, 15.4 and 30 Watts. In Class mode, the Maximum Power fields have no effect.

Allocation 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 (default).

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 port's priority. If two ports have the same priority the port with the highest port number is shut down. This is the default.

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

PoE Power Supply Configuration (SM24TBT2DPA)

Primary Power Supply [W]: the maximum amount of power the primary power source can deliver (e.g., 1080 Watts with one power supply or 2160 with two power supplies). The switch can use one or two power supplies. One is used as primary power source, and one as backup power source.

If the switch does not have a second power supply installed, then only the primary power supply settings display. If two power supplies are installed, if the primary power source fails, the backup power source will take over. To be able to determine the amount of power the PD may use, it must be defined what amount of power the primary and backup power sources can deliver. Valid values are 0 - 2000 Watts.

With two power supplies installed:

The screenshot shows a web interface titled "PoE Power Supply Configuration". It contains a single input field labeled "Primary Power Supply [W]" with the value "1640" entered.

Note that the Configuration > Power Information page also has power configuration parameters.

PoE Port Configuration

Port: This is the logical port number for this row. Ports that are not PoE-capable are grayed out and cannot be configured for PoE.

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

Disabled: PoE disabled for the port.

Enabled: Enables PoE IEEE 802.3bt (Class 4 PDs limited to 90W).

2-pair: The switch port will power up the linked PD using 2-pair mode.

4-pair : The switch port will power up the linked PD using 4-pair mode.

PoE Schedule: The Poe schedule is defined by Schedule Profile. You can define the profiles for the scheduling at Configuration > PoE > Schedule Profile.

Priority: The Priority represents the ports priority. There are three levels of power priority: Low, High and Critical. The default is Low priority.

The priority is used in the case where the remote devices require more power than the power supply can deliver. In this case the port with the lowest priority will be turn off starting from the port with the highest port number.

Low is the lowest priority level. This is the default setting. Ports set to this level receive power only if all ports assigned to the other two levels are already receiving power. If there is not enough power to support all of the ports set to the Low priority level, power is provided to the ports based on port number, in ascending order.

High is the second highest priority level. Ports set to this level receive power only if all the ports set to the Critical level are already receiving power. If there is not enough power to support all of the ports set to the High priority level, power is provided to the ports based on port number, in ascending order.

Critical is the highest priority level. Ports set to this level are guaranteed power first, before any ports assigned to the other two priority levels. Ports assigned to the other priority levels receive power only

The screenshot shows a dropdown menu titled "PoE Mode". The menu is open, showing options: Disabled, 2-pair, 4-pair, and Enabled. The "2-pair" option is currently selected.

The screenshot shows a dropdown menu titled "Priority". The menu is open, showing options: Low, High, and Critical. The "Low" option is currently selected.

if all Critical ports are receiving power. Assign the most critical powered devices to Critical level. If there is not enough power to support all the ports set to Critical priority level, power is provided to the ports based on port number, in ascending order. See “[Port priority impact](#)” below.

Capacitor Detection: The PoE capacitor detection for the port; check the box to enable Capacitor Detection to support legacy PD's that were designed before the IEEE standard was finalized. The default is disabled.

Maximum Power: Set the maximum power in watts that can be delivered to a remote device. The maximum allowed value is 90 W. In Class mode and LLDP-MED mode, the Maximum Power fields have no effect.

PoE Power Note:

Power Supplies	Available PoE Power
With 2 Power Supplies	Max 90 Watts output per port. Max PoE Budget 1640 Watts. 60 Watts for (24) ports simultaneously 90 Watts for (18) ports simultaneously
With 1 Power Supply	Max PoE budget 820 Watts. 30 Watts for (24) ports simultaneously 60 Watts for (13) ports simultaneously 90 Watts for (9) ports simultaneously (see Note below)

Note: There are several ways to supply 90 Watts to the PD, mainly depending on the way the PD is requesting power. Different PDs may need to be configured different ways. When both the PSE and PD support full 802.3bt standard will be easier. Below is one way to configure the switch to provide 90W with one power supply:

1. Make sure the switch is at FW v 6.54.3178 or above and PoE FW v 208-211 (2.11) or above.
2. Set Reserved Power Determined by to Allocation.
3. Set Power Management Mode to Actual Consumption.
4. Set PoE Mode to Enabled for the switch to support PoH mode to supply 90 Watts to the PD.
5. Change the Maximum Power first (to 90W) before you click Apply.
6. Change Reserved Power Determined by to LLDP-Med then click Apply (in Class mode and LLDP-MED mode, the Maximum Power fields have no effect). If you change the Maximum Power with Allocation selected and click Apply before moving to LLDP-Med, the message *The value of 'Max. Power' is restricted to 0 - 60 watts.* displays. See the Example below.

Buttons:

Apply – Click to save changes.

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

Port priority impact:

Power-up order: After a reset, the ports are powered up based on their priority, highest to lowest, with highest (Critical) priority powering up first.

Shutdown order: When exceeding the power budget, lowest priority ports will turn off first.

Messages: *The value of 'Max. Power' is restricted to 0 - 60 watts.*

Figure 2-13.1: Power Over Ethernet Configuration page (SM24TBT2DPA FW vB6.54.3476 or newer)

Firmware vB6.54.3494 changed the PoE 802.3bt FW version to actively send the bt version of power via MDI TLVs. Reply is with the at version of power via MDI TLV if the PD is using such version of TLV, and additionally send two more bt TLVs. Firmware vB6.54.3576 adds TLV IEEE802.3 MAC/ PHY configuration/status in LLDP packets.

Parameter descriptions: (SM24TBT2DPA FW vB6.54.3476 or newer)

PoE Power Supply Configuration

Primary Power Supply [W]: the maximum amount of power the primary power source can deliver. The switch can use one or two power supplies. One is used as primary power source, and one as backup power source.

SM24TBT2DPA delivery for one PS-AC-920 is 820 Watts or 1640 Watts with two power supplies.

The SM24TBT2DPB ships with one PS-ACDC-1200 power supply, which enables up to 900W of total PoE power when connected to low-line AC or DC power or 1080W with high-line AC or DC power.

A second PS-ACDC-1200 power supply can be installed for redundancy or to provide increased PoE power - with two hot-swappable power supplies the switch can provide up to 1800W of total PoE power when connected to low-line AC or DC power or 2150W with high-line AC or DC power.

SM24TBT2DPB delivery for the PS-ACDC-1200 is AC low-line: 900W (single PS-ACDC-1200), 1,800W (dual PS-ACDC-1200) AC high-line: 1,080W (single PS-ACDC-1200), 2,160W (dual PS-ACDC-1200) HVDC low-line: 900W (single PS-ACDC-1200), 1,800W (dual PS-ACDC-1200) HVDC high-line: 1,080W (single PS-ACDC-1200), 2,160W (dual PS-ACDC-1200).

If the switch does not have a second power supply installed, then only the primary power supply settings display. If two power supplies are installed, if the primary power source fails, the backup power source will take over. To be able to determine the amount of power the PD may use, it must be defined what amount of power the primary and backup power sources can deliver. Valid values are 0 - 2000 Watts.

SM24TBT2DPA with two PS-AC-920 power supplies installed:

PoE Power Supply Configuration

Primary Power Supply [W]

Note that the Configuration > Power Information page also has power configuration parameters.

PoE Port Configuration

Port: This is the logical port number for this row. Ports that are not PoE-capable are grayed out and cannot be configured for PoE.

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

Disabled: PoE disabled for the port.

4pair60w : The switch port will power up the linked PD using 4-pair mode (PDs limited to 60W).

4pair90w : The switch port will power up the linked PD using 4-pair mode (PDs limited to 90W).

8023bt : Enables PoE IEEE 802.3bt (Class 8 PDs limited to 90W) (default).

PoE Mode

▼

- ◁
- ▷
- Disabled
- 4pair60w
- 4pair90w
- 8023bt

PoE Schedule: The Poe schedule is defined by Schedule Profile. You can define the profiles for the scheduling at Configuration > PoE > Schedule Profile.

Priority: Port prioritization is how the switch determines which ports are to receive power in the event that the needs of the PDs exceed the available power resources of the switch. There are three priority levels:

Critical: the highest priority level. Ports set to this level are guaranteed power before any ports assigned to the other two priority levels. Ports assigned to the other priority levels receive power only if all the Critical ports are receiving power. Your most critical powered devices should be assigned to this level. If there is not enough power to support all the ports set to the Critical priority level, power is provided to the ports based on port number, in ascending order.

High: the second highest level. Ports set to this level receive power only if all the ports set to the Critical level are already receiving power. If there is not enough power to support all of the ports set to the High priority level, power is provided to the ports based on port number, in ascending order.

Low: the lowest priority level. This is the default setting. Ports set to this level only receive power if all the ports assigned to the other two levels are already receiving power. As with the other levels, if there is not enough power to support all ports set to Low priority level, power is provided to the ports based on port number, in ascending order.

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

Legacy: Select Enabled or Disabled. Enabled allows support for capacitor detection to detect legacy PoE PD devices. Legacy Detection is designed to detect a variety of pre-standard PDs with wide range of input capacitance, different levels of DCDC UVLOs (undervoltage-lockout) and different startup delay times. The default is Legacy mode Disabled.

LLDP Power over Ethernet TLV (Clause 79 in 802.3 and in 802.3bt): The LLDP protocol is used to manage individual Ethernet links. The protocol is based on TLVs (Type/Length/Value). One of these TLVs is used for “organizationally specific” purposes, one of which is assigned for use by IEEE 802.3. Within this TLV, subtypes are defined that each control a set of link properties. One of these subtypes is used for PoE management and another is used for PoE measurement.

Within the PoE subtype, Clause 79 defines a number of fields used to support power negotiation between a PSE and a PD, called DLL (Data Link Layer) classification.

In addition to the “Power via MDI” TLV, an optional TLV, “Power via MDI measurements” is also defined. With this TLV the PSE and PD can exchange information about electrical conditions at their respective PI. Four different measurements are supported: voltage, current, power, and energy. The devices can independently indicate which measurements are supported, which measurement they request from the link partner, what the quality of the measurement is (expressed in an uncertainty figure), and finally the

measurement results itself. See the Ethernet Alliance "[Overview of 802.3bt - Power over Ethernet standard](#)" for more information.

SM24TBT2DPA Firmware Upgrade to FW vB6.54.3494

Once you upgrade the SM24TBT2DPA to FW vB6.54.3494, you can't fall back to the old FW version. This is because the FW upgrade includes a PoE FW upgrade to support the IEEE 802.3bt standard, so you can't downgrade to an old FW version.

PoE Mode setting between v6.54.3303 with vB6.54.3476 (and newer):

v6.54.3303	vB6.54.3476
Disabled	Disabled
Enabled (*)	4pair90w
4pair	4pair60w
2pair	8023bt (*)

Notes:

1. The PoE mode setting will be mapping according to the table above after firmware upgrade.
2. It's not allowed to downgrade to v6.54.3303 or older version after firmware upgrade to vB6.54.3476 or newer version.
3. It's not allowed to swap firmware image when the back image is v6.54.3303 or older version.

PoE Force Mode

SM24TBT2DPA FW VB6.64.0031 added the 8023bt60w, 8023bt30w, force90w, and force60w PoE Mode selections. **Caution:** using PoE 'Force' mode to force the switch to send PoE to non-PoE devices can physically damage those devices.

Port	PoE Mode	PoE Schedule	Priority	LLDP	Legacy
*	<>	<>	<>	<>	<>
1	Disabled	Disabled	Low	Enabled	Disabled
2	Disabled	Disabled	Low	Enabled	Disabled
3	Disabled	Disabled	Low	Enabled	Disabled
4	Disabled	Disabled	Low	Enabled	Disabled
5	8023bt60w	Disabled	Low	Enabled	Disabled
6	8023bt60w	Disabled	Low	Enabled	Disabled
7	8023bt60w	Disabled	Low	Enabled	Disabled
8	8023bt60w	Disabled	Low	Enabled	Disabled
9	8023bt60w	Disabled	Low	Enabled	Disabled

PoE Mode : The PoE Mode lets you set the PoE operating mode for each port:

Disabled: PoE disabled for the port.

4pair60w : The switch port will power up the linked PD using 4-pair mode (PDs limited to 60W).

4pair90w : The switch port will power up the linked PD using 4-pair mode (PDs limited to 90W).

8023bt90w : Enables PoE IEEE 802.3bt (Class 8 PDs limited to 90W).

8023bt60w : Enables PoE IEEE 802.3bt (Class 8 PDs limited to 60W).

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

force90w : Enables PoE force power (PDs limited to 90W).

force60w : Enables PoE force power (PDs limited to 60W).

Messages:

PoE Mode(Force90w) :The switch will power up the linked PD without any detect/negotiate mechanism (PD limited to 90W). Do you want to Change this setting?

PoE Mode(Force60w) :The switch will power up the linked PD without any detect/negotiate mechanism (PD limited to 60W). Do you want to Change this setting?

Action: Verify that you want to power up the linked PD without any detect/negotiate mechanism, then click the OK button. Otherwise click the Cancel button.

Lantronix POE++ Switch PoE Classification Settings

This section describes POE++ Configuration settings for different cameras or other higher powered PDs on the switch.

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

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

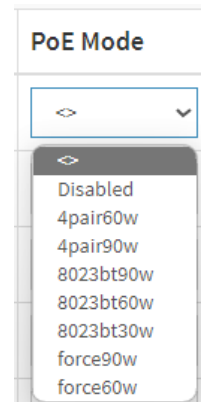
8023bt90w: Enables PoE IEEE 802.3bt (Class 8 PDs limited to 90W). Class negotiation up to 90W and supports 802.3 af/at/bt. Max power is 90W.

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

8023bt30w: Enables PoE IEEE 802.3bt (Class 8 PDs limited to 30W). Class negotiation up to 30W and supports 802.3 af/at. Max power is 30W.

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

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



3.14-3 Recommended Settings

Application	Recommended Setting
Camera is 802.3af/at.	Use 802.3bt30w mode.
Camera is not 802.3bt but requires more than 30W.	Use 802.3bt60w mode.
Camera specifies it is HPOE.	Use 4pair90w mode.

Caution: Using Force mode (forcing the switch to send POE to non-POE devices) can physically damage those devices.

2- 13.2 Power Delay

The PoE Power Delay page lets you set the delay time of power provided after the device is rebooted.

To configure Power over Ethernet delay in the web UI:

1. Click Configuration, PoE, Power Delay.
2. At the Delay Mode dropdown, enable the delay mode to delay power to the device after a reboot.
3. Specify the power providing delay time after a reboot occurs.
4. Click Apply to apply the change.

Figure 2-13.2: PoE Power Delay page

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

Parameter descriptions:

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

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

Enabled: Enable POE Power Delay.

Disabled: Disable POE Power Delay.

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

Buttons:

Apply – Click to save changes.

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

2- 13.3 PoE Schedule Profile

The PoE Schedule Profile page lets you make a schedule of PoE power supply. PoE Scheduling makes PoE management easier and saves energy. For FW VB6.64.0069 and above, on PoE schedule request, if "Start Time" is equal to "End Time", the switch will immediately reset PoE power on the selected ports. So if you configure Start Time 23:00 (Monday) and End Time 23:00 (Monday) on Profile 1, and Profile 1 is configured for port 1, at 23:00 on each Monday, port 1 will immediately reset PoE power.

To configure PoE scheduling via the web UI:

1. Click Configuration, PoE, and PoE Schedule Profile.
2. Select the local port and enable.
3. Select time and day to supply power.
4. Click Apply to apply the changes.

Figure 2-13.3: PoE Schedule Profile page

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

Parameter descriptions:

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

Name: The name of profile. The default name is "Profile #". 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.

2- 13.4 PoE Auto Power Reset (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, the switch can be set to reboot the remote PD automatically.

To set PoE Auto Power Reset in the web UI:

1. Click Configuration, PoE, Auto Power Reset.
2. At the dropdown, enable the Ping Check function.
3. Specify the PD IP address, startup time, interval, retry times, failure action, reboot time, and max reboot times.
4. Click Apply to apply the changes.

Figure 2-13.4: PoE Auto Power Reset

The screenshot shows the Lantronix web interface for the SM24TBT2DPB switch. The navigation menu on the left includes 'Switch', 'DMS', and 'Configuration'. Under 'Configuration', 'PoE' is expanded to show 'Auto Power Reset'. The main content area is titled 'PoE Auto Power Reset' and features a 'Ping Check' dropdown set to 'Disabled'. Below this is a table with 8 rows, one for each port (1-8). Each row contains input fields for 'Ping IP Address', 'Startup Time', 'Interval Time', 'Retry Time', a 'Failure Log' counter, a 'Failure Action' dropdown, 'Reboot Time', 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	0.0.0.0	60	30	3	error=0, total=0	Nothing	15	3
2	0.0.0.0	60	30	3	error=0, total=0	Nothing	15	3
3	0.0.0.0	60	30	3	error=0, total=0	Nothing	15	3
4	0.0.0.0	60	30	3	error=0, total=0	Nothing	15	3
5	0.0.0.0	60	30	3	error=0, total=0	Nothing	15	3
6	0.0.0.0	60	30	3	error=0, total=0	Nothing	15	3
7	0.0.0.0	60	30	3	error=0, total=0	Nothing	15	3
8	0.0.0.0	60	30	3	error=0, total=0	Nothing	15	3

Parameter descriptions:

Ping Check: Enable Ping Check function can detect the connection between the PoE port and the powered device. Disabled will turn off the detection.

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

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

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

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

Retry Time: When a PoE port can't ping the PD, it will try to send detection again. When the set number of retry times is reached, a failure action is triggered. Default: 3 retries; range: 1-5 retries.

Failure Log: Failure loggings counter (e.g., *error=0, total=11*).

Failure Action: The action when the third fail detection.

Nothing: Keep Pinging the remote PD but do nothing further.

Reboot Remote PD: Cut off the power on the PoE port and make the PD reboot.

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

Max. Reboot Times: When Failure Action is set to Reboot Remote PD, this setting limits the number of times the PD is rebooted. . The default is 3 reboots; the valid range: is 0-10 reboots. Entering a 0 means unlimited reboots as the failure action.

Buttons:

Apply – Click to save changes.

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

2- 13.5 PoE Chip Reset Schedule

This page lets you schedule when to reset the PoE chip. This feature lets you reset just the PoE chip, without resetting the device's CPU. To configure PoE Chip Reset Scheduling in the web UI:

1. Click Configuration, PoE, POE Chip Reset Schedule.
2. At the Mode dropdown, select Enabled to display the POE Chip Reset Schedule table.
3. Select the Week Day and PoE Chip Reset Time parameters.
4. Click Apply to save the changes.

Figure 2-13.5: PoE Chip Reset Schedule page

The screenshot shows the Lantronix web interface for configuring the PoE Chip Reset Schedule. The page title is "PoE Chip Reset Schedule" and the mode is set to "Enabled". A table allows scheduling resets by week day and time (HH and MM). Buttons for "Apply" and "Reset" are at the bottom.

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

Parameter descriptions: (only displayed when Mode is Enabled)

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

Enabled: Enable PoE chip reset.

Disabled: Disable PoE chip reset.

Week Day: The day to reset PoE chip (*, Monday, Tuesday, Wednesday, Thursday, Friday, or Saturday).

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

At the **HH** (hour) dropdown select 0-23 as the time in hours for one or more of the Days.

At the **MM** (minute) dropdown select 0-55 (in 5 minute increments) as the time in minutes for one or more of the Days.

Buttons:

Apply: Click to save changes.

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

2-14 MAC Table

Switching of frames is based on the DMAC address contained in the frame. The switch builds a table that maps MAC addresses to switch ports for knowing which ports the frames should go to (based on the DMAC address in the frame). This table contains both static and dynamic entries.

The static entries are configured by the network administrator if the administrator wants to do a fixed mapping between the DMAC address and switch ports.

The frames also contain a MAC address (SMAC address), which shows the MAC address of the equipment sending the frame. The SMAC address is used by the switch to automatically update the MAC table with these dynamic MAC addresses. Dynamic entries are removed from the MAC table if no frames with the corresponding SMAC address have been seen after a configurable age time.

Web Interface

To configure the MAC Address Table via the web UI:

Aging Configuration

1. Click Configuration.
2. Specify the Disable Automatic Aging and Aging Time.
3. Click Apply.

MAC Table Learning

1. Click Configuration.
2. Specify the Port Members (Auto, Disable, Secure).
3. Click Apply.

Static MAC Table Configuration

1. Click Configuration and Add New Static Entry.
2. Specify the VLAN IP and Mac address, Port Members.
3. Click Apply.

Figure 2-14: MAC Address Table Configuration page

LANTRONIX SM24TBT2DPB

MAC Address Table Configuration

Auto-Logout OFF

Home > Configuration > MAC Table

Switch DMS

Configuration

System

Green Ethernet

Ports Configuration

DHCP

Security

Aggregation

Loop Protection

Spanning Tree

IPMC Profile

MVR

IPMC

LLDP

PoE

MAC Table

VLANs

Private VLANs

VCL

Voice VLAN

QoS

Mirroring

UPnP

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	23	24	25	26
Auto	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Disable	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<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"/>
Secure	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<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"/>

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	23	24	25	26
<input type="button" value="Delete"/>	1	00-00-00-00-00-00	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<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"/>	

Parameter descriptions:

Aging Configuration: By default, dynamic entries are removed from the MAC table after 300 seconds. This removal is also called aging. Configure aging time by entering a value here in seconds; for example, Age time seconds. The allowed range is 10 to 1000000 seconds. Disable the automatic aging of dynamic entries by checking the Disable Automatic Aging checkbox.

MAC Table Learning: If the learning mode for a given port is greyed out, another module is in control of the mode, so that it cannot be changed by the user. An example of such a module is the MAC-Based Authentication under 802.1X. Each port can do learning based upon the following settings:

Auto: Learning is done automatically as soon as a frame with unknown SMAC is received.

Disable: No learning is done.

Secure: Only static MAC entries are learned; all other frames are dropped.



NOTE: Make sure that the link used for managing the switch is added to the Static Mac Table before changing to secure learning mode, otherwise the management link is lost and can only be restored by using another non-secure port or by connecting to the switch via the serial interface.

Static MAC Table Configuration: The static entries in the MAC table are shown in this table. The static MAC table can contain 64 entries. The maximum of entries is 64. 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 the button to add a new entry to the static MAC table. Specify the VLAN ID, MAC address, and port members for the new entry. Click "Apply".

Apply – Click to save changes.

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

Add New Static Entry - Click to add a new entry to the static MAC table.

2-15 VLANs

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

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

To configure VLAN parameters in the web UI:

1. Click Configuration, VLANs.
2. Specify Global VLAN and Port VLAN parameters.
3. Click Apply.

Figure 2-15.1: VLAN Configuration page

The screenshot shows the LANTRONIX web interface for VLAN configuration. The top navigation bar includes the LANTRONIX logo, a menu icon, and an Auto-Logout dropdown set to OFF. The main content area is titled 'VLAN Configuration' and is divided into two sections: 'Global VLAN Configuration' and 'Port VLAN Configuration'. In the Global section, 'Allowed Access VLANs' is set to '1' and 'Ethertype for Custom S-ports' is set to '88A8'. The Port section is a table with the following data:

Port	Mode	Port VLAN	Port Type	Ingress Filtering	Ingress Acceptance	Egress Tagging	Allowed VLANs	Forbidden VLANs
*	<>	1	<>	<input checked="" type="checkbox"/>	<>	<>	1	
1	Access	1	C-Port	<input checked="" type="checkbox"/>	Tagged and Untagged	Untag Port VLAN	1	
2	Access	1	C-Port	<input checked="" type="checkbox"/>	Tagged and Untagged	Untag Port VLAN	1	
3	Access	1	C-Port	<input checked="" type="checkbox"/>	Tagged and Untagged	Untag Port VLAN	1	
4	Access	1	C-Port	<input checked="" type="checkbox"/>	Tagged and Untagged	Untag Port VLAN	1	
5	Access	1	C-Port	<input checked="" type="checkbox"/>	Tagged and Untagged	Untag Port VLAN	1	
6	Access	1	C-Port	<input checked="" type="checkbox"/>	Tagged and Untagged	Untag Port VLAN	1	
7	Access	1	C-Port	<input checked="" type="checkbox"/>	Tagged and Untagged	Untag Port VLAN	1	
8	Access	1	C-Port	<input checked="" type="checkbox"/>	Tagged and Untagged	Untag Port VLAN	1	

Parameter descriptions:

Global VLAN Configuration

Allowed Access VLANs: This field shows the VLANs that are created on the switch. By default, only VLAN 1 exists. More VLANs may be created by using a list syntax where the individual elements are separated by commas. Ranges are specified with a dash separating the lower and upper bound.

The following example will create VLANs 1, 10, 11, 12, 13, 200, and 300: **1,10-13,200,300**. Spaces are allowed in between the delimiters.

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

Port VLAN Configuration

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

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

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

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

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

- By default, a trunk port is member of all existing VLANs. This may be limited by the use of Allowed VLANs,
- unless VLAN Trunking is enabled on the port, frames classified to a VLAN that the port is not a member of will be discarded,
- by default, all frames but frames classified to the Port VLAN (a.k.a. Native VLAN) get tagged on egress. Frames classified to the Port VLAN do not get C-tagged on egress,
- egress tagging can be changed to tag all frames, in which case only tagged frames are accepted on ingress,
- VLAN trunking may be enabled.

Hybrid: Hybrid ports resemble trunk ports in many ways but have additional port configuration features. In addition to the characteristics described for trunk ports, hybrid ports have these abilities:

- Can be configured to be VLAN tag unaware, C-tag aware, S-tag aware, or S-custom-tag aware,
- ingress filtering can be controlled,
- ingress acceptance of frames and configuration of egress tagging can be configured independently.

Port VLAN: Set the port's VLAN ID (a.k.a. PVID). Valid VLANs are 1 - 4095; the default is VLAN 1.

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

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

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

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

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

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

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

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

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

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

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

VLAN Trunking: Trunk and Hybrid ports allow for enabling VLAN trunking.

When VLAN trunking is enabled, frames classified to unknown VLANs are accepted on the port whether ingress filtering is enabled or not.

This is useful in scenarios where a cloud of intermediary switches must bridge VLANs that haven't been created. By configuring the ports that connect the cloud of switches as trunking ports, they can seamlessly carry those VLANs from one end to the other.

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

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

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

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

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

Untag Port VLAN: Frames classified to the Port VLAN are transmitted untagged. Other frames are transmitted with the relevant tag.

Tag All: All frames, whether classified to the Port VLAN or not, are transmitted with a tag.

Untag All: All frames, whether classified to the Port VLAN or not, are transmitted without a tag.

This option is only available for ports in Hybrid mode.

Allowed VLANs: Ports in Trunk and Hybrid mode may control which VLANs they are allowed to become members of. Access ports can only be member of one VLAN, the Access VLAN.

The field's syntax is identical to the syntax used in the Existing VLANs field. By default, a port may become member of all possible VLANs, and is therefore set to 1-4095.

The field may be left empty, which means that the port will not be member of any of the existing VLANs, but if it is configured for VLAN Trunking it will still be able to carry all unknown VLANs.

Forbidden VLANs: A port may be configured to never be member of one or more VLANs. This is particularly useful when dynamic VLAN protocols like MVRP and GVRP must be prevented from dynamically adding ports to VLANs.

The trick is to mark such VLANs as forbidden on the port in question. The syntax is identical to the syntax used in the Allowed Access VLANs field.

By default, the field is left blank, which means that the port may become a member of all possible VLANs.

Buttons:

Apply – Click to save changes.

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

2-16 Private VLANs

> Private VLANs

> Membership

> Port Isolation

In a private VLAN, communication between ports in that private VLAN is not permitted. A VLAN can be configured as a private VLAN.

2-16.1 Private VLAN Membership Configuration

The Private VLAN Membership Configuration 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 are members of VLAN 1 and Private VLAN 1.

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

To configure Private VLAN Membership parameters in the web UI:

1. Click Configuration, Private VLANs, Membership.
2. Select the ports you want to enable VLAN membership.
3. Click Apply.

Figure 2-16.1: Private VLAN Membership Configuration page

Parameter descriptions:

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

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

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.

Adding a New Private VLAN: Click the **Add New Private VLAN** button 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 **Apply**.

The **Delete** button can be used to undo the addition of new Private VLANs.

Buttons

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

Refresh: Click to refresh the page immediately.

Save: Click to save changes.

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

Add New Private VLAN: Click the button to add a new private VLAN ID. An empty row is added to the table, and the private VLAN can be configured as needed.

Example:

SM24TBT2DPA Private VLAN Membership Configuration

Auto-refresh

Private VLAN Membership Configuration

		Port Members																									
Delete	PVLAN ID	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26
<input type="checkbox"/>	1	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
<input type="checkbox"/>	2	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<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"/>	3	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<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"/>	4	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input 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"/>	5	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	6	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input 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"/>	7	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input 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 checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>

Add New Private VLAN

Apply Done

2-16.2 Port Isolation

Port Isolation provides for an apparatus and method to isolate ports on layer 2 switches on the same VLAN to restrict traffic flow. The apparatus comprises a switch with multiple ports, each port configured as a protected port or a non-protected port. An address table in 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.

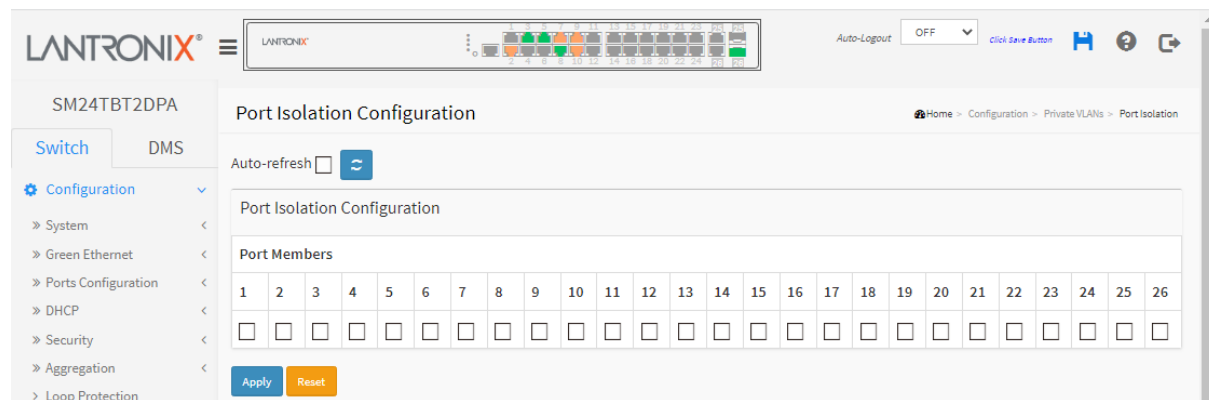
This page is used for enabling or disabling port isolation on ports in a Private VLAN. A port member of a VLAN can be isolated to other isolated ports on the same VLAN and Private VLAN.

Web Interface

To configure Port Isolation in the web UI:

1. Click Configuration, Private VLANs, Port Isolation.
2. Select which ports you want to enable Port Isolation.
3. Click Apply.

Figure 2-16.1: Port Isolation Configuration page



Parameter descriptions:

Port Members: A check box is provided for each port of a private VLAN. When checked, port isolation is enabled on that port. When unchecked, port isolation is disabled on that port. By default, port isolation is disabled (unchecked) 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.

2-17 VCL

2-17.1 MAC-based VLAN

MAC address-based VLAN decides the VLAN for forwarding an untagged frame based on the source MAC address of the frame.

A common way of grouping VLAN members is by port, hence the name port-based VLAN. Typically, the device adds the same VLAN tag to untagged packets that are received through the same port. Later on, these packets can be forwarded in the same VLAN. Port-based VLAN is easy to configure and applies to networks where the locations of terminal devices are relatively fixed. As mobile office and wireless network access gain more popularity, the ports that terminal devices use to access the networks are very often non-fixed. A device may access a network through Port A this time, but through Port B the next time. If Port A and Port B belong to different VLANs, the device will be assigned to a different VLAN the next time it accesses the network. As a result, it will not be able to use the resources in the old VLAN. On the other hand, if Port A and Port B belong to the same VLAN, after terminal devices access the network through Port B, they will have access to the same resources as those accessing the network through Port A do, which brings security issues. To provide user access and ensure data security in the meantime, the MAC-based VLAN technology is developed.

MAC-based VLANs group VLAN members by MAC address. With MAC-based VLAN configured, the device adds a VLAN tag to an untagged frame according to its source MAC address. MAC-based VLANs are mostly used in conjunction with security technologies such as 802.1X to provide secure, flexible network access for terminal devices.

Web Interface

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

1. Click Configuration, VCL, MAC-based VLAN, and Add New Entry.
2. Specify the MAC address and VLAN ID.
3. Select the Port Members.
4. Click Apply.

Figure 2-17.1: MAC-based VLAN Membership Configuration page



Parameter descriptions:

Delete: Click to do immediately delete a MAC-based VLAN entry from the table.

MAC Address: Indicates the MAC address.

VLAN ID: Indicates the VLAN ID.

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

Adding a New MAC-based VLAN: Click to add a new MAC-based VLAN entry. An empty row is added to the table, and the MAC-based VLAN entry can be configured as needed. Any unicast MAC address can be configured for the MAC-based VLAN entry. No broadcast or multicast MAC addresses are allowed. Legal values for a VLAN ID are 1 - 4095.

The MAC-based VLAN entry is enabled on the switch when you click on "Apply".
A MAC-based VLAN without any port members will be deleted when you click "Apply".

The Reset button can be used to undo the addition of new MAC-based VLANs.

Buttons:

Apply – Click to save changes.

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

Add New Entry - Click to add another entry to the table.

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

No multicast or broadcast address allowed

At least one port must be selected to add an entry

2-17.2 Protocol-based VLAN

This page lets you add new protocols to Group Name (unique for each Group) mapping entries as well as allow you to see and delete already mapped entries for the switch. Switch Protocol support includes Ethernet, LLC, and SNAP Protocols.

LLC: The Logical Link Control (LLC) data communication protocol layer is the upper sub-layer of the Data Link Layer (which is itself layer 2, just above the Physical Layer) in the seven-layer OSI reference model. It provides multiplexing mechanisms that make it possible for several network protocols (IP, IPX, Decnet and AppleTalk) to coexist within a multipoint network and to be transported over the same network media, and can also provide flow control and automatic repeat request (ARQ) error management mechanisms.

SNAP: The Subnetwork Access Protocol (SNAP) is a mechanism for multiplexing, on networks using IEEE 802.2 LLC, more protocols than can be distinguished by the 8-bit 802.2 Service Access Point (SAP) fields. SNAP supports identifying protocols by Ethernet type field values; it also supports vendor-private protocol identifier spaces. It is used with IEEE 802.3, IEEE 802.4, IEEE 802.5, IEEE 802.11 and other IEEE 802 physical network layers, as well as with non-IEEE 802 physical network layers such as FDDI that use 802.2 LLC.

2-17.2.1 Protocol to Group

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

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

1. Click Configuration, VCL, Protocol-based VLAN, and Protocol to Group.
2. Click the Add New Entry button.
3. Specify the Frame Type, Value, and Group Name parameters.
4. Click the Apply button.

Figure 2-21.2.1: Protocol to Group Mapping Table

The screenshot shows the web interface for configuring Protocol-based VLAN on a Lantronix switch. The main content area is titled "Protocol to Group Mapping Table" and contains a table with the following data:

Delete	Frame Type	Value	Group Name
<input type="checkbox"/>	LLC	FF-FF	Grp3
<input type="checkbox"/>	SNAP	00-E0-2B-0001	Grp2
<input type="checkbox"/>	Ethernet	0800	Grp1

Below the table are buttons for "Add New Entry", "Apply", and "Reset".

Parameter descriptions:

Delete: To delete a Protocol to Group Name map entry, check this box. The entry is deleted from the switch immediately.

Frame Type: Frame Type can be set to Ethernet, SNAP, or LLC as described below.



NOTE: On changing the Frame type field, the valid value of the following 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 Frame Types:

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

LLC: Valid value in this case is comprised of two different sub-values.

DSAP: 1-byte long string (0x00-0xff)

SSAP: 1-byte long string (0x00-0xff)

SNAP: Valid value in this case also is comprised of two different sub-values.

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

PID: If the OUI is hexadecimal 000000, the protocol ID is the Ethernet type (EtherType) field value for the protocol running on top of SNAP; if the OUI is an OUI for a particular organization, the protocol ID is a value assigned by that organization to the protocol running on top of SNAP. In other words, if the value of OUI field is 00-00-00 then value of PID will be etype (0x0600-0xffff) and if value of OUI is other than 00-00-00 then valid value of PID will be any value from 0x0000 to 0xffff.

Group Name: A valid Group Name is a unique 16-character long string for every entry which consists of a combination of alphabets (a-z or A-Z) and integers (0-9).



NOTE: Special characters and underscore (_) are not allowed.

Buttons:

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

Refresh: Click to manually refresh the page information immediately.

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

Apply : Click to save changes.

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

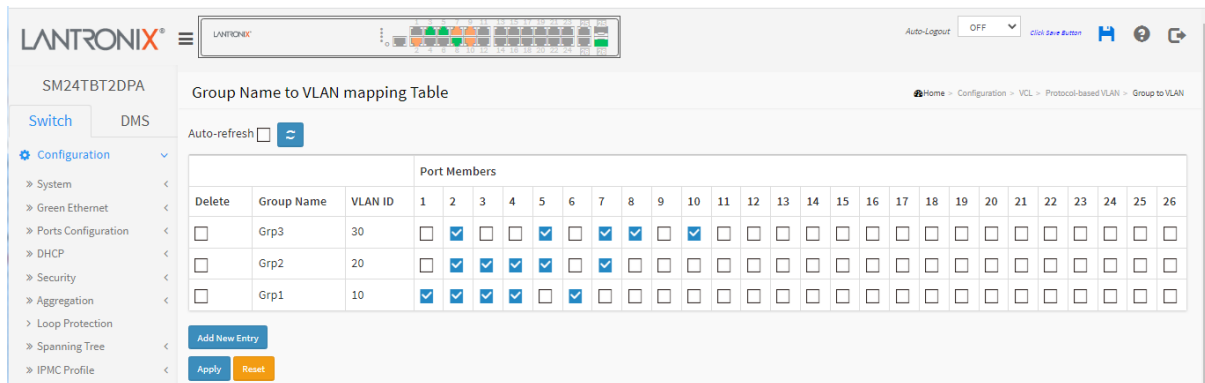
2-17.2.2 Group to VLAN

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

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

1. Click Configuration, VCL, Protocol-based VLAN, Group to VLAN.
2. Click the Add New Entry button.
2. Specify the Group Name and VLAN ID.
3. Click the Apply button.

Figure 2-21.2.2: Group Name to VLAN mapping Table



Parameter descriptions:

Delete: To delete a Group Name to VLAN map entry, check this box. The entry will be deleted from the table and from the switch immediately.

Group Name: A valid Group Name is a string of almost 16 characters which consists of a combination of alphabets (a-z or A-Z) and integers (0-9), no special character is allowed. Whichever Group name you try to map to a VLAN must be present in the Protocol to Group mapping table and must not be perused by any other existing mapping entry on this page.

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

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

Buttons:

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

Apply – Click to save changes.

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

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

Refresh: Click to manually refresh the page information immediately.

Messages:

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

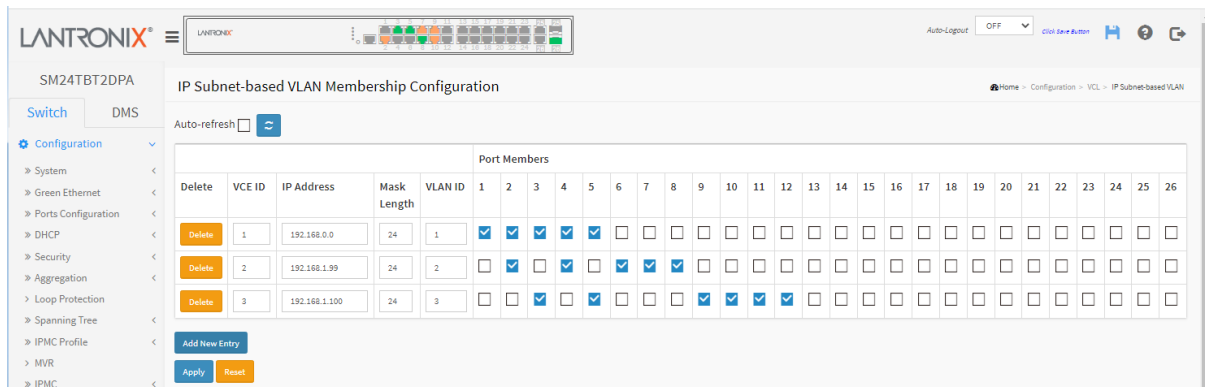
2-17.3 IP Subnet-based VLAN

The IP subnet-based VLAN entries can be configured here. This page allows for adding, updating and deleting IP subnet-based VLAN entries and assigning the entries to different ports. This page shows only static entries.

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

1. Click Configuration, VCL, IP-based VLAN.
2. Click Add New Entry.
3. Specify the VCE ID, IP Address, Mask Length, VLAN ID and select Port Members.
4. Click Apply.

Figure 2-17.3: IP Subnet-based VLAN Membership Configuration



Parameter descriptions:

Delete: To delete a IP subnet-based VLAN entry, check this box and click Apply.

VCE ID: Indicates the index of the entry. It is user configurable. Its value ranges from 0-128. If a VCE ID is 0, application will auto-generate the VCE ID for that entry. Deletion and lookup of IP subnet-based VLAN are based on VCE ID.

IP Address: Indicates the IP address. An IP address of 0.0.0.0 is not allowed.

Mask Length: Indicates the network mask length.

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

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

Buttons:

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

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 automatically refresh the page every 3 seconds.

Refresh: Click to manually refresh the page immediately.

2-18 Voice VLAN

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

2-18.1 Configuration

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

To configure Voice VLAN in the web UI:

1. Navigate to Configuration > Voice VLAN > Configuration.
2. Select “Enabled” in the Voice VLAN Configuration.
3. Specify VLAN ID, Aging Time, and Traffic Class.
4. Specify Port Mode, Security, and Discovery Protocol in the Port Configuration.
5. Click Apply.

Figure 2-18.1: Voice VLAN Configuration

The screenshot displays the Lantronix web management interface for device SM24TBT2DPA. The main content area is titled "Voice VLAN Configuration" and is divided into two sections: "Voice VLAN Configuration" and "Port Configuration".

Voice VLAN Configuration:

Mode	Enabled
VLAN ID	1
Aging Time	86400 seconds
Traffic	7 (High)

Port Configuration:

Port	Mode	Security	Discovery Protocol
*	Disabled	<>	<>
1	Disabled	Enabled	OUI
2	Disabled	Enabled	LLDP
3	Disabled	Enabled	Both
4	Disabled	Enabled	OUI
5	Disabled	Enabled	OUI
6	Disabled	Enabled	OUI

Parameter descriptions:

Mode: Indicates the Voice VLAN mode operation. **Note:** You must disable the MSTP feature before you enable Voice VLAN to avoid the conflict of ingress filtering. Otherwise, the Mode field is greyed out.

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 to 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 Class: Indicates the Voice VLAN traffic class. All traffic on the Voice VLAN will apply this class.

Mode: Indicates the Voice VLAN port mode. When the port mode isn't equal disabled, we must disable MSTP feature before we enable Voice VLAN. It can avoid the conflict of ingress filtering. Possible port modes are:

Disabled: Disjoin from Voice VLAN.

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

Forced: Force join to Voice VLAN.

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

Enabled: Enable Voice VLAN security mode operation.

Disabled: Disable Voice VLAN security mode operation.

Discovery Protocol: Indicates the Voice VLAN port discovery protocol. It will only work when Auto detect mode is enabled. You 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 (Organizationally Unique Identifier) address.

LLDP: Detect telephony device by LLDP (Link Level Discovery Protocol).

Both: Both OUI and LLDP.

Buttons:

Apply – Click to save changes.

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

Message: *The Voice VLAN ID should not equal MVR VLAN ID*

Recovery: 1. Click the OK button to clear the message.

2. Change the VLAN ID parameter described above.

2-18.2 OUI

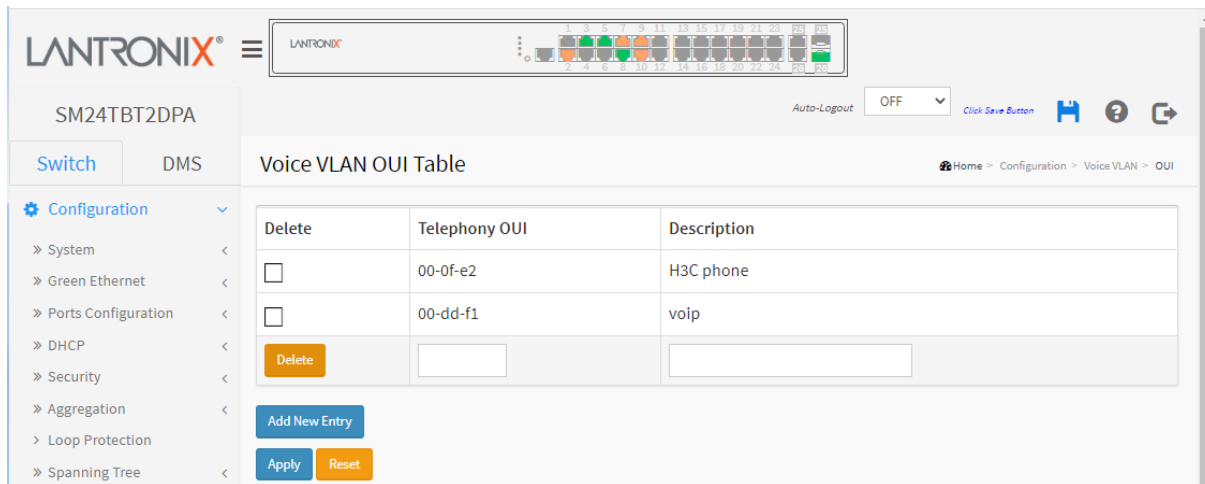
This page lets you configure the Voice VLAN OUI parameters. The maximum entry number is 16. Modifying the OUI table will restart auto detection of the OUI process.

An OUI (Organizationally Unique Identifier) 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.

To configure Voice VLAN OUI in the web UI:

1. Navigate to Configuration > Voice VLAN > OUI.
2. Click "Add New Entry" to add a line to the Voice VLAN OUI table.
3. Specify Telephony OUI and Description.
4. Click Apply.

Figure 2-18.2: Voice VLAN OUI Table



Parameter descriptions:

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

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

Description: The description of OUI address. Normally, it describes which vendor a telephony device belongs to. The allowed string length is 0-32 characters.

Buttons:

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

Apply – Click to save changes.

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

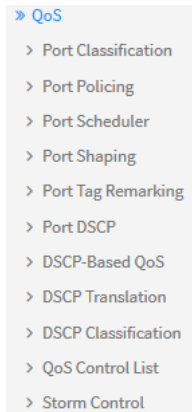
2-19 QoS

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

High flexibility in the classification of incoming frames to a QoS class.

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

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



2-19.1 Port Classification

This page lets you configure basic QoS Ingress Classification settings for all switch ports. To configure QoS Ingress Port Classification parameters in the web UI:

1. Click Configuration, QoS, Port Classification.
2. Scroll to select QoS class, DP Level, PCP and DEI parameters.
3. Click the Apply button to save the setting.
4. To cancel the settings click the Reset button. The page will revert to previously saved values.

Figure 2-19.1: QoS Ingress Port Classification page

Port	CoS	DPL	PCP	DEI	Tag Class.	DSCP Based	Address Mode
*	0	0	0	0		<input type="checkbox"/>	Source
1	0	0	0	0	Disabled	<input type="checkbox"/>	Source
2	0	0	0	0	Disabled	<input type="checkbox"/>	Source
3	0	0	0	0	Disabled	<input type="checkbox"/>	Source
4	0	0	0	0	Disabled	<input type="checkbox"/>	Source
5	0	0	0	0	Disabled	<input type="checkbox"/>	Source
6	0	0	0	0	Disabled	<input type="checkbox"/>	Source
7	0	0	0	0	Disabled	<input type="checkbox"/>	Source
8	0	0	0	0	Disabled	<input type="checkbox"/>	Source

Parameter descriptions:

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

CoS: Controls the default Class of Service. All frames are classified to a CoS. There is a one-to-one mapping between CoS, queue and priority. A CoS of 0 (zero) has the lowest priority. If the port is VLAN aware, the frame is tagged and Tag Class. is enabled, then the frame is classified to a CoS that is mapped from the PCP and DEI value in the tag. Otherwise the frame is classified to the default CoS.

The classified CoS can be overruled by a QCL entry. **Note:** If the default CoS has been dynamically changed, then the actual default CoS is shown in parentheses after the configured default CoS.

DPL: Controls the default Drop Precedence Level. All frames are classified to a drop precedence level. If the port is VLAN aware, the frame is tagged and Tag Class. is enabled, then the frame is classified to a DPL that is mapped from the PCP and DEI value in the tag. Otherwise the frame is classified to the default DPL. The classified DPL can be overruled by a QCL entry. Every incoming frame is classified to a Drop Precedence Level (DP level), which is used throughout the device for providing congestion control guarantees to the frame according to what was configured for that specific DP level. A DP level of 0 (zero) corresponds to 'Committed' (Green) frames and a DP level of 1 corresponds to 'Discard Eligible' (Yellow) frames.

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. Priority Code Point (PCP) is a 3-bit field storing the priority level for the 802.1Q frame. It is also known as User Priority.

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. Drop Eligible Indicator (DEI) is a 1-bit field in the VLAN tag.

Tag Class.: Shows the classification mode for tagged frames on this port.

Disabled: Use default QoS class and DP level for tagged frames.

Enabled: Use mapped versions of PCP and DEI for tagged frames.

Click on the mode in order to configure the mode and/or mapping.



NOTE: This setting has no effect if the port is VLAN unaware. Tagged frames received on VLAN unaware ports are always classified to the default CoS and DPL.

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

Address Mode: The IP/MAC address mode specifying whether the QCL classification must be based on source (SMAC/SIP) or destination (DMAC/DIP) addresses on this port. The allowed values are:

Source: Enable SMAC/SIP matching.

Destination: Enable DMAC/DIP matching.

Buttons:

Apply – Click to save changes.

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

2-19.2 Port Policing

This page lets you configure 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 used for data flows and voice or video flows because voice and video usually maintain a steady rate of traffic.

To set QoS Ingress Port Policers in the web UI:

1. Click Configuration, QoS, Port Policing.
2. Select which ports to enable the QoS Ingress Port Policers and type the Rate limit condition.
3. Scroll to select the Rate limit Unit (kbps, Mbps, fps or kfps).
4. Click Apply to save the configuration.

Figure 2-19.2: QoS Ingress Port Policers page

The screenshot shows the Lantronix web interface for the SM24TBT2DPB switch. The main content area is titled "QoS Ingress Port Policers" and contains a table with the following data:

Port	Enabled	Rate	Unit	Flow Control
*	<input type="checkbox"/>	500	<-	<input type="checkbox"/>
1	<input type="checkbox"/>	500	kbps	<input type="checkbox"/>
2	<input type="checkbox"/>	500	kbps	<input type="checkbox"/>
3	<input type="checkbox"/>	500	kbps	<input type="checkbox"/>
4	<input type="checkbox"/>	500	kbps	<input type="checkbox"/>
5	<input type="checkbox"/>	500	kbps	<input type="checkbox"/>
6	<input type="checkbox"/>	500	kbps	<input type="checkbox"/>
7	<input type="checkbox"/>	500	kbps	<input type="checkbox"/>
8	<input type="checkbox"/>	500	kbps	<input type="checkbox"/>

Parameter descriptions:

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

Enabled: Select which Port you need to enable the QoS Ingress Port Policers function.

Rate: To set the Rate limit value for this port, the default is 500.

Unit: To scroll to select what unit of rate includes kbps, Mbps, fps and kfps. The default is kbps.

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

Buttons:

Apply – Click to save changes.

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

2-19.4 Port Schedulers

This page lets you view and configure QoS Egress Port Schedulers for all switch ports. To configure QoS Egress Port Schedulers via the web UI:

1. Click Configuration, QoS, Port Schedulers.
2. Click a linked Port number to display its Queue Shaper page.
3. Enter the Port, Scheduler Mode, and Queue Shaper parameters.
4. Click Apply to save the changes.

Figure 2-19.4: QoS Egress Port Schedules page

QoS Egress Port Schedulers Home > Configuration > QoS > Port Scheduler

Port	Mode	Q0	Q1	Q2	Q3	Q4	Q5
1	Strict Priority	-	-	-	-	-	-
2	Strict Priority	-	-	-	-	-	-
3	Strict Priority	-	-	-	-	-	-

Click the Port index to set the QoS Egress Port Schedulers

QoS Egress Port Scheduler and Shapers Port 1 Home > Configuration > QoS > Port Scheduler

Port: Port 1

Scheduler Mode: Strict Priority

Queue Shaper

Queue	Enable	Rate	Unit	Excess
*	<input type="checkbox"/>	500	<>	<input type="checkbox"/>
0	<input type="checkbox"/>	500	kbps	<input type="checkbox"/>
1	<input type="checkbox"/>	500	kbps	<input type="checkbox"/>
2	<input type="checkbox"/>	500	kbps	<input type="checkbox"/>
3	<input type="checkbox"/>	500	kbps	<input type="checkbox"/>
4	<input type="checkbox"/>	500	kbps	<input type="checkbox"/>
5	<input type="checkbox"/>	500	kbps	<input type="checkbox"/>
6	<input type="checkbox"/>	500	kbps	<input type="checkbox"/>
7	<input type="checkbox"/>	500	kbps	<input type="checkbox"/>

Port Shaper

Enable	Rate	Unit
<input type="checkbox"/>	500	kbps

Apply Reset Cancel

QoS Egress Port Scheduler and Shapers Port 1 Home > Configuration > QoS > Port Scheduler

Port: Port 1

Scheduler Mode: **Weighted**

Queue Shaper					Queue Scheduler	
Queue	Enable	Rate	Unit	Excess	Weight	Percent
*	<input type="checkbox"/>	500	<>	<input type="checkbox"/>	17	
0	<input type="checkbox"/>	500	kbps	<input type="checkbox"/>	17	
1	<input type="checkbox"/>	500	kbps	<input type="checkbox"/>	17	
2	<input type="checkbox"/>	500	kbps	<input type="checkbox"/>	17	
3	<input type="checkbox"/>	500	kbps	<input type="checkbox"/>	17	17%
4	<input type="checkbox"/>	500	kbps	<input type="checkbox"/>	17	17%
5	<input type="checkbox"/>	500	kbps	<input type="checkbox"/>	17	17%
6	<input type="checkbox"/>	500	kbps	<input type="checkbox"/>		
7	<input type="checkbox"/>	500	kbps	<input type="checkbox"/>		

Port Shaper

Enable	Rate	Unit
<input type="checkbox"/>	500	kbps

Apply Reset Cancel

If you select the scheduler mode with **Weighted** then the screen will change as shown in the figure.

Parameter descriptions:

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

Mode: Shows the scheduling mode for this port (Strict Priority or Weighted).

Weight (Qn): Shows the weight for this queue and port.

Scheduler Mode: Controls whether the scheduler mode is "Strict Priority" or "Weighted" on this switch port.

Queue Shaper Enable: Controls whether the queue shaper is enabled for this queue on this switch port.

Queue Shaper Rate: Controls the rate for the queue shaper. The default value is 500. This value is restricted to 100-1000000 when the "Unit" is "kbps", and it is restricted to 1-13200 when the "Unit" is "Mbps".

Queue Shaper Unit: Controls the unit of measure for the queue shaper rate as "kbps" or "Mbps". The default value is "kbps".

Queue Shaper Excess: Controls whether the queue is allowed to use excess bandwidth.

Queue Scheduler Weight: Controls the weight for this queue. The default value is "17". This value is restricted to 1-100. This parameter is only shown if "Scheduler Mode" is set to "Weighted".

Queue Scheduler Percent: Shows the weight in percent for this queue. This parameter is only shown if "Scheduler Mode" is set to "Weighted".

Port Shaper Enable: Controls whether the port shaper is enabled for this switch port.

Port Shaper Rate: Controls the rate for the port shaper. The default value is 500. This value is restricted to 100-1000000 when the "Unit" is "kbps", and it is restricted to 1-13200 when the "Unit" is "Mbps".

Port Shaper Unit: Controls the unit of measure for the port shaper rate as "kbps" or "Mbps". The default value is "kbps".

Buttons:

Apply – Click to save changes.

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

Cancel - Click to undo any changes made locally and return to the previous page.

Example: QoS Egress Port Scheduler and Shapers - Port 4:

The screenshot displays the Lantronix web interface for configuring QoS on SM24TBT2DPB. The page title is "QoS Egress Port Scheduler and Shapers Port 4". The breadcrumb trail is "Home > Configuration > QoS > Port Scheduler".

Configuration Fields:

- Port:** Port 4
- Scheduler Mode:** Weighted

Queue Shaper Table:

Queue Shaper					Queue Scheduler	
Queue	Enable	Rate	Unit	Excess	Weight	Percent
*	<input type="checkbox"/>	500	<->	<input type="checkbox"/>	17	
0	<input checked="" type="checkbox"/>	500	kbps	<input checked="" type="checkbox"/>	17	17%
1	<input checked="" type="checkbox"/>	500	kbps	<input type="checkbox"/>	17	17%
2	<input checked="" type="checkbox"/>	500	kbps	<input checked="" type="checkbox"/>	17	17%
3	<input checked="" type="checkbox"/>	500	kbps	<input type="checkbox"/>	17	17%
4	<input type="checkbox"/>	500	kbps	<input type="checkbox"/>	17	17%
5	<input type="checkbox"/>	500	kbps	<input type="checkbox"/>	17	17%
6	<input type="checkbox"/>	500	kbps	<input type="checkbox"/>		
7	<input type="checkbox"/>	500	kbps	<input type="checkbox"/>		

Port Shaper Table:

Enable	Rate	Unit
<input checked="" type="checkbox"/>	500	kbps

Buttons: Apply, Reset, Cancel

2-19.5 Port Shaping

This page lets you view and configure QoS Egress Port Shapers for all switch ports. To set QoS Port Shapers in the web UI:

1. Click Configuration, QoS, Port Shapers.
2. Click a linked Port number.
3. Enter the Port, Scheduler Mode, and Queue Shaper parameters.
4. Click Apply to save the changes.

Figure 2-19.5: QoS Egress Port Shapers page

Home > Configuration > QoS > Port Shaping

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

Click the Port index to set the QoS Egress Port Shapers

Home > Configuration > QoS > Port Scheduler

Port: Port 1

Scheduler Mode: Strict Priority

Queue Shaper

Queue	Enable	Rate	Unit	Excess
*	<input type="checkbox"/>	500	<>	<input type="checkbox"/>
0	<input type="checkbox"/>	500	kbps	<input type="checkbox"/>
1	<input type="checkbox"/>	500	kbps	<input type="checkbox"/>
2	<input type="checkbox"/>	500	kbps	<input type="checkbox"/>
3	<input type="checkbox"/>	500	kbps	<input type="checkbox"/>
4	<input type="checkbox"/>	500	kbps	<input type="checkbox"/>
5	<input type="checkbox"/>	500	kbps	<input type="checkbox"/>
6	<input type="checkbox"/>	500	kbps	<input type="checkbox"/>
7	<input type="checkbox"/>	500	kbps	<input type="checkbox"/>

Port Shaper

Enable	Rate	Unit
<input type="checkbox"/>	500	kbps

Apply
Reset
Cancel

QoS Egress Port Scheduler and Shapers Port 1 Home > Configuration > QoS > Port Scheduler

Port	Port 1
Scheduler Mode	Weighted

Queue Shaper					Queue Scheduler	
Queue	Enable	Rate	Unit	Exces		
*	<input type="checkbox"/>	500	<>	<input type="checkbox"/>		
0	<input type="checkbox"/>	500	kbps	<input type="checkbox"/>		
1	<input type="checkbox"/>	500	kbps	<input type="checkbox"/>	17	17%
2	<input type="checkbox"/>	500	kbps	<input type="checkbox"/>	17	17%
3	<input type="checkbox"/>	500	kbps	<input type="checkbox"/>	17	17%
4	<input type="checkbox"/>	500	kbps	<input type="checkbox"/>	17	17%
5	<input type="checkbox"/>	500	kbps	<input type="checkbox"/>	17	17%
6	<input type="checkbox"/>	500	kbps	<input type="checkbox"/>		
7	<input type="checkbox"/>	500	kbps	<input type="checkbox"/>		

If you select the scheduler mode with wighted then the screen will change as shown in the figure.

Port Shaper		
Enable	Rate	Unit
<input type="checkbox"/>	500	kbps

Apply Reset Cancel

Parameter descriptions:

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

Shapers (Qn): Shows "disabled" or actual queue shaper rate - e.g. "800 Mbps".

Scheduler Mode: Controls whether the scheduler mode is "Strict Priority" or "Weighted" on this switch port.

Queue Shaper Enable: Controls whether the queue shaper is enabled for this queue on this switch port.

Queue Shaper Rate: Controls the rate for the queue shaper. The default value is 500. This value is restricted to 100-1000000 when the "Unit" is "kbps", and it is restricted to 1-13200 when the "Unit" is "Mbps".

Queue Shaper Unit: Controls the unit of measure for the queue shaper rate as "kbps" or "Mbps". The default value is "kbps".

Queue Shaper Excess: Controls whether the queue is allowed to use excess bandwidth.

Queue Scheduler Weight: Controls the weight for this queue. The default value is "17". This value is restricted to 1-100. This parameter is only shown if "Scheduler Mode" is set to "Weighted".

Queue Scheduler Percent: Shows the weight in percent for this queue. This parameter is only shown if "Scheduler Mode" is set to "Weighted"

Port Shaper Enable: Controls whether the port shaper is enabled for this switch port.

Port Shaper Rate: Controls the rate for the port shaper. The default value is 500. This value is restricted to 100-1000000 when the "Unit" is "kbps", and it is restricted to 1-13200 when the "Unit" is "Mbps".

Port Shaper Unit: Controls the unit of measure for the port shaper rate as "kbps" or "Mbps". The default value is "kbps".

Buttons:

Apply – Click to save changes.

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

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

2-19.6 Port Tag Remarking

This page lets you view and configure QoS Egress Port Tag Remarking for all switch ports.

To display the QoS Port Tag Remarking in the web UI:

1. Click Configuration, QoS, Port Tag Remarking.
2. Click the linked Port number.
3. At the dropdown select the Tag Remarking Mode for that port.

Figure 2-19.6: QoS Egress Port Tag Remarking page

The screenshot displays the QoS Egress Port Tag Remarking configuration page. It is divided into three main sections:

- QoS Egress Port Tag Remarking**: A table listing ports and their modes. The table has two columns: "Port" and "Mode". The first row shows "1" in the "Port" column and "Classified" in the "Mode" column. A red box highlights the "1" in the "Port" column, and a blue arrow points to it from a callout box that says "Click the Port index to set the QoS Port Tag Remarking".
- QoS Egress Port Tag Remarking Port 1**: A configuration form for Port 1. It has two fields: "Port" (set to "Port 1") and "Tag Remarking Mode" (set to "Classified"). Below the fields are "Apply" and "Reset" buttons.
- QoS Egress Port Tag Remarking Port 1**: A configuration form for Port 1 showing PCP/DEI settings. It has two fields: "Port" (set to "Port 1") and "Tag Remarking Mode" (set to "Default"). Below the fields are "Apply" and "Reset" buttons. Underneath, there is a section for "PCP/DEI Configuration" with two fields: "Default PCP" (set to "0") and "Default DEI" (set to "0"). Below these fields are "Apply" and "Reset" buttons.

QoS Egress Port Tag Remarking Port 1

Home > Configuration > QoS > Port Tag Remarking

Port	Port 1 <input type="button" value="v"/>
Tag Remarking Mode	Mapped <input type="button" value="v"/>

(QoS class, DP level) to (PCP, DEI) Mapping

QoS class	DP level	PCP	DEI
*	*	<> <input type="button" value="v"/>	<> <input type="button" value="v"/>
0	0	1 <input type="button" value="v"/>	0 <input type="button" value="v"/>
0	1	1 <input type="button" value="v"/>	1 <input type="button" value="v"/>
1	0	0 <input type="button" value="v"/>	0 <input type="button" value="v"/>
1	1	0 <input type="button" value="v"/>	1 <input type="button" value="v"/>
2	0	2 <input type="button" value="v"/>	0 <input type="button" value="v"/>
2	1	2 <input type="button" value="v"/>	1 <input type="button" value="v"/>
3	0	3 <input type="button" value="v"/>	0 <input type="button" value="v"/>
3	1	3 <input type="button" value="v"/>	1 <input type="button" value="v"/>
4	0	4 <input type="button" value="v"/>	0 <input type="button" value="v"/>
4	1	4 <input type="button" value="v"/>	1 <input type="button" value="v"/>
5	0	5 <input type="button" value="v"/>	0 <input type="button" value="v"/>
5	1	5 <input type="button" value="v"/>	1 <input type="button" value="v"/>
6	0	6 <input type="button" value="v"/>	0 <input type="button" value="v"/>
6	1	6 <input type="button" value="v"/>	1 <input type="button" value="v"/>
7	0	7 <input type="button" value="v"/>	0 <input type="button" value="v"/>
7	1	7 <input type="button" value="v"/>	1 <input type="button" value="v"/>

Apply

Reset

Parameter descriptions:

Port: At the dropdown select the desired port to configure.

Tag Remarking Mode: Controls the tag remarking mode for this port.

Classified: Use classified PCP/DEI values.

Default: Use default PCP/DEI values.

Mapped: Use mapped versions of QoS class and DP level.

PCP/DEI Configuration: Controls the default PCP and DEI values used when Mode is set to Default.

(QoS class, DP level) to (PCP, DEI) Mapping: Controls the mapping of the classified (QoS class, DP level) to (PCP, DEI) values when the mode is set to Mapped.

Buttons:

Apply – Click to save changes.

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

Cancel – Click to cancel the changes.

2-19.7 Port DSCP

This page lets you configure QoS Port DSCP parameters for all switch ports. To configure QoS Port DSCP parameters in the web UI:

1. Click Configuration, QoS, Port DSCP.
2. Enable or disable the Ingress Translate and set the Classify parameters.
3. Select Egress Rewrite parameters.
4. Click the Apply button to save the settings.
5. To cancel the settings click the Reset button. The page will revert to previously saved values.

Figure 2-19.7: QoS Port DSCP Configuration page

Port	Ingress		Egress
	Translate	Classify	Rewrite
*	<input type="checkbox"/>	<>	<>
1	<input type="checkbox"/>	Disable	Disable
2	<input checked="" type="checkbox"/>	All	Enable
3	<input checked="" type="checkbox"/>	DSCP=0	Remap DP Unaware
4	<input checked="" type="checkbox"/>	Selected	Remap DP Aware
5	<input checked="" type="checkbox"/>	All	Remap DP Aware
6	<input checked="" type="checkbox"/>	Selected	Enable
7	<input type="checkbox"/>	DSCP=0	Disable
8	<input type="checkbox"/>	Disable	Disable
9	<input checked="" type="checkbox"/>	DSCP=0	Remap DP Unaware
10	<input checked="" type="checkbox"/>	Selected	Enable

Parameter descriptions:

Port: The Port column shows the list of ports for which you can configure DSCP ingress and egress settings.

Ingress: In Ingress settings you can change ingress translation and classification settings for individual ports. There are two configuration parameters available in Ingress:

Translate: To Enable Ingress Translation check the checkbox.

Classify: The Classification for a port have one of four different values:

Disable: No Ingress DSCP Classification.

DSCP=0: Classify if incoming (or translated if enabled) DSCP is 0.

Selected: Classify only selected DSCP for which classification is enabled as specified in DSCP Translation window for the specific DSCP.

All: Classify all DSCP.

Egress: Port Egress Rewriting can be one of these parameters:

Disable: No Egress rewrite.

Enable: Rewrite enable without remapped.

Remap: DSCP from analyzer is remapped and frame is remarked with remapped DSCP value.

Buttons:

Apply – Click to save changes.

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

Auto-refresh: Check the checkbox to refresh the page information automatically every 3 seconds.

Refresh: Click to manually refresh the QoS Port DSCP information immediately.

2-19.8 DSCP-Based QoS

This page lets you configure basic QoS DSCP based QoS Ingress Classification parameters. To configure DSCP-based QoS Ingress Classification via the web UI:

1. Click Configuration, QoS, DSCP-Based QoS.
2. Enable or disable the DSCP for Trust.
3. Scroll to select QoS Class and DPL parameters.
4. Click Apply to save the settings.
5. To cancel the settings, click the Reset button. The page will revert to previously saved values.

Figure 2-19.8: DSCP-Based QoS Ingress Classification page

DSCP	Trust	QoS Class	DPL
*	<input type="checkbox"/>	< >	< >
0 (BE)	<input checked="" type="checkbox"/>	0	0
1	<input checked="" type="checkbox"/>	0	1
2	<input checked="" type="checkbox"/>	4	0
3	<input checked="" type="checkbox"/>	5	0
4	<input type="checkbox"/>	0	1
5	<input type="checkbox"/>	0	0
6	<input type="checkbox"/>	0	0
7	<input checked="" type="checkbox"/>	0	0
8 (CS1)	<input checked="" type="checkbox"/>	0	1
9	<input checked="" type="checkbox"/>	0	0

Parameter descriptions:

DSCP: The maximum number of supported DSCP values is 64.

Trust: Click to check if the DSCP value is trusted. Controls whether a specific DSCP value is trusted. Only frames with trusted DSCP values are mapped to a specific QoS class and Drop Precedence Level. Frames with untrusted DSCP values are treated as a non-IP frame.

QoS Class: QoS Class value can be 0-7.

DPL: Drop Precedence Level (0 or 1).

Buttons:

Apply – Click to save changes.

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

2-19.9 DSCP Translation

This page lets you configure the basic QoS DSCP Translation settings for the switch. DSCP translation can be done in Ingress or Egress. To configure DSCP Translation parameters in the web UI:

1. Click Configuration, QoS, DSCP Translation.
2. Scroll to set the Ingress Translate and Egress Remap DP0 and Remap DP1 Parameters.
3. Enable or disable Classify.
4. Click Apply to save the settings.

Figure 2-19.9: DSCP Translation Configuration page

DSCP	Ingress		Egress	
	Translate	Classify	Remap DP0	Remap DP1
*	<=>	<input type="checkbox"/>	<=>	<=>
0 (BE)	0 (BE)	<input checked="" type="checkbox"/>	0 (BE)	0 (BE)
1	1	<input checked="" type="checkbox"/>	1	1
2	2	<input checked="" type="checkbox"/>	2	2
3	8 (CS1)	<input type="checkbox"/>	0 (BE)	3
4	4	<input checked="" type="checkbox"/>	4	4
5	10 (AF11)	<input checked="" type="checkbox"/>	5	14 (AF13)
6	6	<input checked="" type="checkbox"/>	6	6
7	7	<input type="checkbox"/>	7	7
8 (CS1)	8 (CS1)	<input type="checkbox"/>	8 (CS1)	8 (CS1)
9	9	<input type="checkbox"/>	9	9

Parameter descriptions:

DSCP: Maximum number of supported DSCP values are 64 and valid DSCP values range from 0 to 63.

Ingress: Ingress side DSCP can be first translated to new DSCP before using the DSCP for QoS class and DPL map. There are two configuration parameters for DSCP Translation:

Translate: DSCP at Ingress side can be translated to any of (0-63) DSCP values.

Classify: Click to enable Classification at the Ingress side.

Egress: There configurable parameters for the Egress side are:

Remap DP0: Select the DSCP value to which you want to remap. DSCP value ranges from 0 to 63.

Remap DP1: Select the DSCP value to which you want to remap. DSCP value ranges from 0 to 63.

Buttons:

Apply – Click to save changes.

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

2-19.10 DSCP Classification

This page lets you configure the mapping of QoS class and Drop Precedence Level to DSCP value.

To configure DSCP Classification parameters in the web UI:

1. Click Configuration, QoS, DSCP Translation.
2. Set the DSCP Parameters.
3. Click the Apply button to save the setting.
4. To cancel the settings click the Reset button. The page will revert to previously saved values.

Figure 2-19.10: DSCP Classification page

The screenshot shows the Lantronix web interface for device SM24TBT2DPB. The main content area is titled "DSCP Classification" and contains a table with the following data:

QoS Class	DPL	DSCP
*	*	<input type="text" value=""/>
0	0	0 (BE)
0	1	0 (BE)
1	0	0 (BE)
1	1	0 (BE)
2	0	0 (BE)
2	1	0 (BE)
3	0	0 (BE)
3	1	0 (BE)
4	0	0 (BE)
4	1	0 (BE)

Parameter descriptions:

QoS Class: Actual Quality of Service class.

DPL: Actual Drop Precedence Level.

DSCP: Select the classified DSCP value (0BE-63).


Buttons

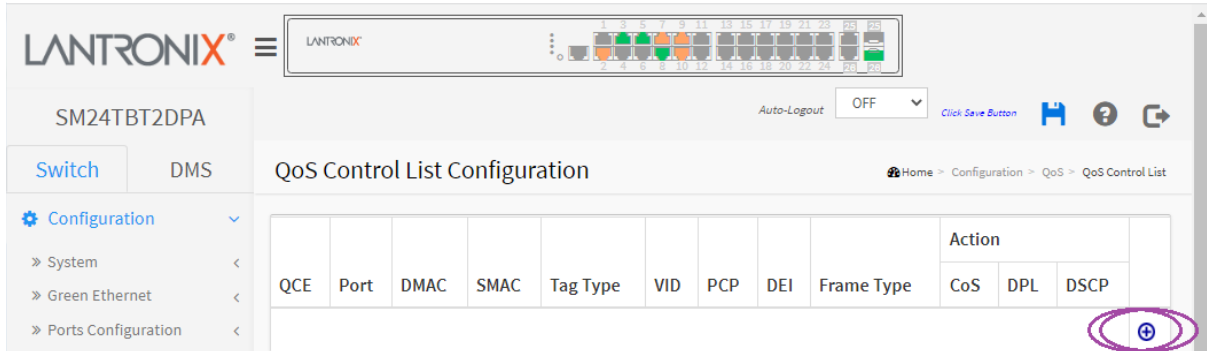
Apply: Click to save changes and apply to running-config.

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

2-19.11 QoS Control List Configuration

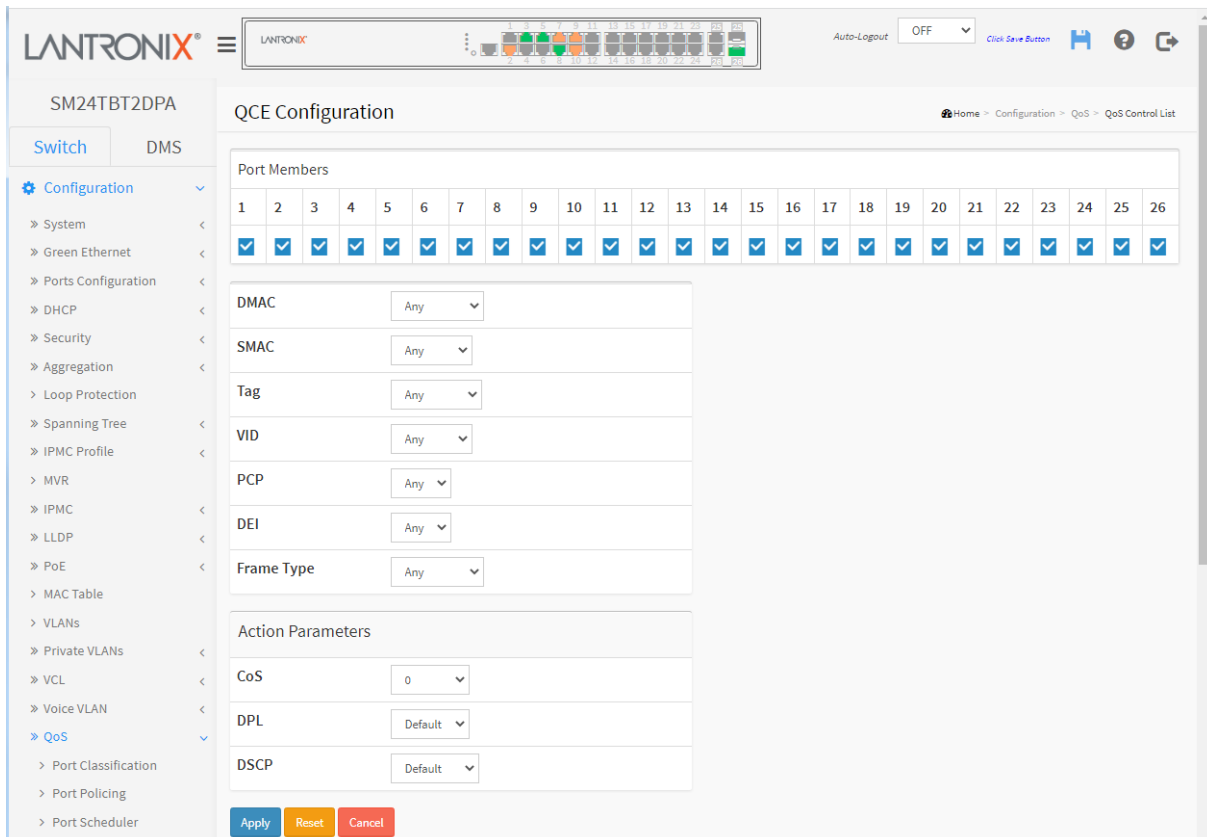
This page lets you configure QoS Control List (QCL), which is made up of the QCEs. Each row describes a QCE that is defined. The maximum number of QCEs is 256 per switch. Click on the lowest plus sign to add a new QCE to the list. To configure QoS Control List parameters in the web UI:

1. Click Configuration, QoS, QoS Control List.
2. Click the  icon to add a new QoS Control List.



The screenshot shows the 'QoS Control List Configuration' page in the Lantronix web UI. The page has a breadcrumb trail: Home > Configuration > QoS > QoS Control List. A table is displayed with the following columns: QCE, Port, DMAC, SMAC, Tag Type, VID, PCP, DEI, Frame Type, and Action (sub-columns: CoS, DPL, DSCP). A plus icon in the bottom right corner of the table is circled in purple, indicating where to click to add a new QCE.

3. Select the desired parameters and select the Port Member to join the QCE rules.
4. Click Apply to save the settings.
5. To cancel the settings, click the Reset button. The page will revert to previously saved values.



The screenshot shows the 'QCE Configuration' page in the Lantronix web UI. The page has a breadcrumb trail: Home > Configuration > QoS > QoS Control List. It features a 'Port Members' section with a grid of checkboxes for ports 1 through 26, all of which are checked. Below this are fields for DMAC, SMAC, Tag, VID, PCP, DEI, and Frame Type, each with a dropdown menu set to 'Any'. At the bottom, there are 'Action Parameters' for CoS (set to 0), DPL (set to Default), and DSCP (set to Default). Buttons for 'Apply', 'Reset', and 'Cancel' are at the bottom.

Parameter descriptions:

QCE#: Indicates the index of QCE.

Port: Indicates the list of ports configured with the QCE.

DMAC: Indicates the destination MAC address. Possible values are:

Any: Match any DMAC. The default value is 'Any'.

Unicast: Match unicast DMAC.

Multicast: Match multicast DMAC.

Broadcast: Match broadcast DMAC.

SMAC: Match a Specific source MAC address or 'Any'. If a port is configured to match on DMAC/DIP, this field indicates the DMAC.

Tag: Indicates tag type. Possible values are:

Any: Match tagged and untagged frames. The default value is 'Any'.

Untagged: Match untagged frames.

Tagged: Match tagged frames.

VID: Indicates (VLAN ID), either a specific VID or range of VIDs. VID can be in the range 1-4095 or 'Any'

PCP: Priority Code Point: Valid values of PCP are specific (0, 1, 2, 3, 4, 5, 6, 7) or range (0-1, 2-3, 4-5, 6-7, 0-3, 4-7) or 'Any'.

DEI: Drop Eligible Indicator: Valid values of DEI are 0, 1 or 'Any'.

Frame Type: Indicates the type of frame to look for incoming frames. Possible frame types are:

Any: The QCE will match all frame type.

EtherType: Only Ethernet frames (with Ether Type 0x600-0xFFFF) are allowed.

LLC: Only (LLC) frames are allowed.

SNAP: Only (SNAP) frames are allowed

IPv4: The QCE will match only IPV4 frames.

IPv6: The QCE will match only IPV6 frames.

Action Parameters: Indicates the classification action taken on ingress frame if parameters configured are matched with the frame's content. There are three action fields: CoS, DPL and DSCP.

CoS: Classified QoS Class; if a frame matches the QCE it will be put in the queue. Select Default or 0 - 7.

DPL: Drop Precedence Level; if a frame matches the QCE then DP level will set to value displayed under DPL column. Select Default, 0, or 1.

DSCP: If a frame matches the QCE then DSCP will be classified with the value displayed in the DSCP column. Select 0 (BE) – 62.

Buttons

Apply: Click to save changes and apply to the running-config.

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.

QoS Control List Configuration

This page lets you edit or 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 if you want to make any port a member of the QCL entry. By default, all ports are checked (included).

Key Parameters

DMAC: Destination MAC address: Possible values are 'Unicast', 'Multicast', 'Broadcast' or 'Any'.

SMAC: Source MAC address: xx-xx-xx-xx-xx-xx or 'Any'. If a port is configured to match on DMAC/DIP, this field is the Destination MAC address.

Tag: The value of Tag field can be 'Untagged', 'Tagged' or 'Any'.

VID Valid value of VLAN ID can be any value in the range 1-4095 or 'Any'; you can enter either a specific value or a range of VIDs.

PCP 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'.

Frame Type can have one of these values:

1. **Any**
2. **EtherType**
3. **LLC**
4. **SNAP**
5. **IPv4**
6. **IPv6**

Note: All of the Frame types are explained below.

1. **Any:** Allow all types of frames.
2. **Ether Type** Valid Ether Type can be 0x600-0xFFFF excluding 0x800(IPv4) and 0x86DD(IPv6) or 'Any'.
3. **LLC:** Logical Link Control:

SSAP Address Valid SSAP(Source Service Access Point) can vary from 0x00 to 0xFF or 'Any'.

DSAP Address Valid DSAP(Destination 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:** Subnetwork Access Protocol:

PID Valid PID (a.k.a Ether Type) can be 0x0000-0xFFFF or 'Other'.

5. **IPv4:**

Protocol IP protocol number: ('Any', 'UDP' or 'TCP' or 'Any').

Source IP Specific Source IP address in value/mask format or 'Any'. IP and Mask are in the format x.y.z.w where x, y, z, and w are decimal numbers between 0 and 255. When Mask is converted to a 32-bit binary string and read from left to right, all bits following the first zero must also be zero. If a port is configured to match on DMAC/DIP, this field is the Destination IP address.

IP Fragment IPv4 frame fragmented option: 'Yes', 'No' or 'Any'.

DSCP Diffserv Code Point value (DSCP): It can be a specific value, range of values or 'Any'. DSCP values are in the range 0-63 including BE, CS1-CS7, EF or AF11-AF43.

Sport Source TCP/UDP port:(0-65535) or 'Any', specific or port range applicable for IP protocol UDP/TCP.

Dport Destination TCP/UDP port:(0-65535) or 'Any', specific or port range applicable for IP protocol UDP/TCP.

6. IPv6:

Protocol IP protocol number: (0-255, 'TCP' or 'UDP') or 'Any'.

Source IP 32 LS bits of IPv6 source address in value/mask format or 'Any'. If a port is configured to match on DMAC/DIP, this field is the Destination IP address.

DSCP Diffserv Code Point value (DSCP): It can be a specific value, range of values or 'Any'. DSCP values are in the range 0-63 including BE, CS1-CS7, EF or AF11-AF43.

Sport Source TCP/UDP port: (0-65535) or 'Any', specific or port range applicable for IP protocol UDP/TCP.

Dport Destination TCP/UDP port: (0-65535) or 'Any', specific or port range applicable for IP protocol UDP/TCP.

Action Parameters:

CoS Class of Service: (0-7) or 'Default'.

DP Drop Precedence Level: (0-1) or 'Default'.

DSCP: (0-63, BE, CS1-CS7, EF or AF11-AF43) or 'Default'.

'Default' means that the default classified value is not modified by this QCE.

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



: Inserts a new QCE before the current row.



: Edits the QCE.



: Moves the QCE up the list.



: Moves the QCE down the list.



: Deletes the QCE.



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

Buttons

Apply: Click to save 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.

EtherType Parameters

EtherType: Select Any or Specific.

Value: 0x: If you selected Specific above, enter a value. The default is FFFF.

LLC Parameters

SSAP Address: Select Any or Specific. If you select Specific, enter a value. The default is FFFF.

DSAP Address: Select Any or Specific. If you select Specific, enter a value. The default is FFFF.

Control: Select Any or Specific. If you select Specific above, a value. The default is FFFF.

SNAP Parameters

PID: Select Any or Specific. If you select Specific above, a value. The default is FFFF.

IPv4 Parameters

Protocol: Select Any, TCP, UDP, or Other as the IPv4 protocol to use.

SIP: Select Any or Specific. If you select Specific, enter Value and Mask parameters.

IP Fragment: Select Any, Yes, or No.

DSCP: Select Any, Specific, or Range. For Specific or Range, enter additional parameters.

IPv6 Parameters

Protocol: Select Any, TCP, UDP, or Other as the IPv4 protocol to use.

SIP (32 LSB): Select Any or Specific.

DSCP: Select Any, Specific, or Range. or Specific or Range, enter additional parameters.

Example

The example below shows a QoS Control List (QCL) made up of the four QCEs (four rows, each of which describes a defined QCE).

The screenshot shows the Lantronix web interface for the SM24TBT2DPB device. The main content area is titled "QoS Control List Configuration". It features a table with the following data:

QCE	Port	DMAC	SMAC	Tag Type	VID	PCP	DEI	Frame Type	Action			
									CoS	DPL	DSCP	
1	3-19,24,26	Any	Any	Any	Any	Any	Any	Any	0	Default	Default	⊕ ⊖ ⊗
2	3-6,9,10,14-26	Unicast	Any	Untagged	Any	Any	Any	Ethernet	0	Default	Default	⊕ ⊖ ⊗
3	All	Any	Any	Any	Any	4	Any	LLC	3	Default	16 (CS2)	⊕ ⊖ ⊗
4	3-9,12-17,19,22,25	Broadcast	Any	Tagged	Any	Any	Any	IPv4	0	Default	18 (AF21)	⊕ ⊖ ⊗
												⊕

2-19.12 Storm Control

This page lets you configure the Storm control for the switch. There is a unicast storm rate control, multicast storm rate control, and a broadcast storm rate control. These only affect flooded frames, i.e. frames with a (VLAN ID, DMAC) pair not present on the MAC Address table. The configuration indicates the permitted packet rate for unicast, multicast or broadcast traffic across the switch.

To set Storm Control parameters in the web UI:

1. Click Configuration, QoS, Storm Control.
2. Select the Frame Type to enable storm control.
3. Scroll to set the Rate Parameters.
4. Click Apply to save the settings.
5. To cancel the setting, click the Reset button. The page will revert to previously saved values.

Figure 2-19.12: Storm Control Configuration page

Frame Type	Enable	Rate (pps)
Unicast	<input checked="" type="checkbox"/>	16
Multicast	<input checked="" type="checkbox"/>	64
Broadcast	<input type="checkbox"/>	1

Parameter descriptions:

Frame Type: The settings in a particular row apply to the frame type listed here: Unicast, Multicast or Broadcast.

Enable: Enable or disable storm control status for the given frame type.

Rate: The rate unit is packets per second (pps). Valid values are: 1, 2, 4, 8, 16, 32, 64, 128, 256, 512, 1K, 2K, 4K, 8K, 16K, 32K, 64K, 128K, 256K, 512K, or 1024K.

The 1 kpps is actually 1002.1 pps.

Buttons:

Apply – Click to save changes.

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

Rate (pps)

- 1
- 2
- 4
- 8
- 16
- 32
- 64
- 128
- 256
- 512
- 1K
- 2K
- 4K
- 8K
- 16K
- 32K
- 64K
- 128K
- 256K
- 512K
- 1024K

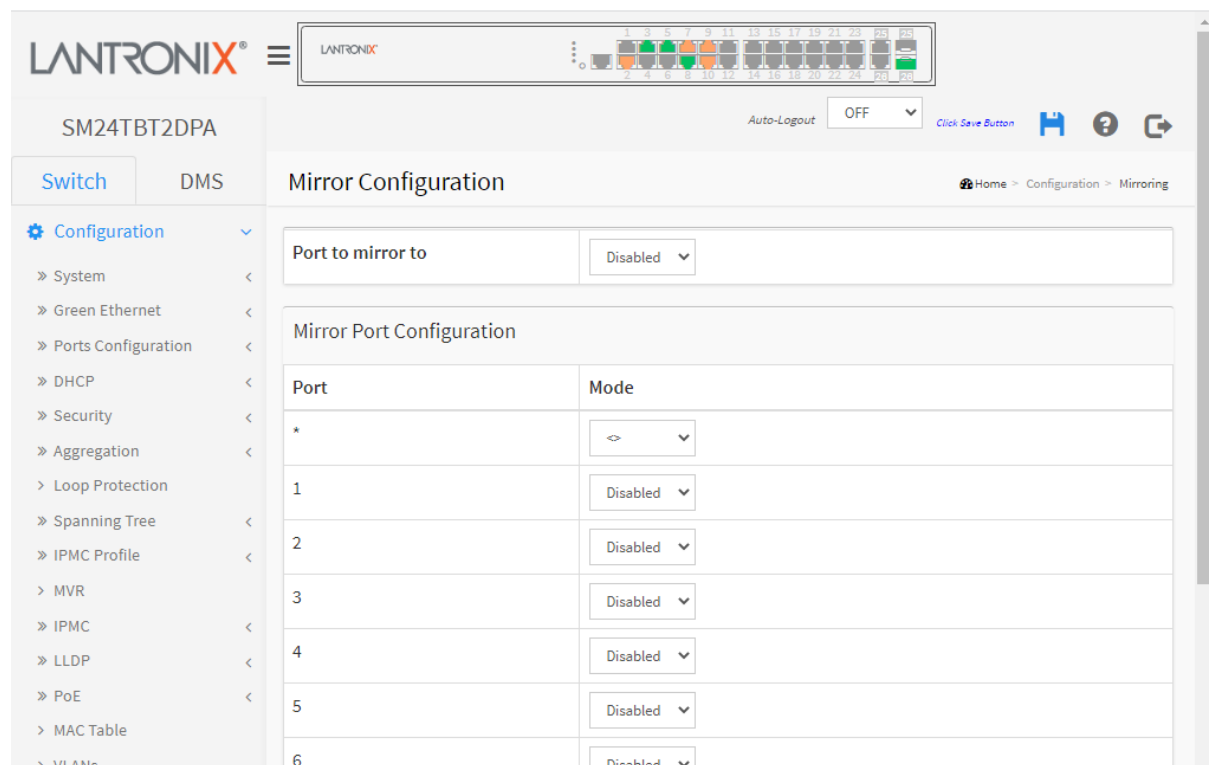
2-20 Mirroring

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.

To configure Mirroring in the web UI:

1. Click Configuration, Mirroring.
2. Scroll to select Port to mirror on which port.
3. Scroll to disabled, enable, TX Only and RX only to set the Port mirror mode.
4. Click the Apply button to save the setting.
5. To cancel the settings click the Reset button to revert to previously saved values.

Figure 2-20: Mirror Configuration page



Parameter descriptions: (before FW vB6.54.3476)

Port to mirror to: Port to mirror also known as the mirror port. Frames from ports that have either source (Rx) or destination (Tx) mirroring enabled are mirrored on this port. Disabled disables mirroring.

Mirror Port Configuration: The following table is used for Rx and Tx enabling.

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

Mode: Select mirror mode.

Rx only Frames received on this port are mirrored on the mirror port. Frames transmitted are not mirrored.

Tx only Frames transmitted on this port are mirrored on the mirror port. Frames received are not mirrored.

Disabled: Neither frames transmitted nor frames received are mirrored.

Enabled: Frames received and frames transmitted are mirrored on the mirror port.



NOTE: For a given port, a frame is only transmitted once. It is therefore not possible to mirror Tx frames on the mirror port. Because of this, the mode for the selected mirror port is limited to Disabled or Rx only.

Buttons:

Apply – Click to save changes.

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

2-20 Mirroring

Parameter descriptions: (FW vB6.54.3476 and after)

Configure port Mirroring on this page.

To debug network problems, selected traffic can be copied, or mirrored, on a mirror port where a frame analyzer can be attached to analyze the frame flow.

The traffic to be copied on the mirror port is selected as follows:

- All frames received on a given port (also known as ingress or source mirroring).
- All frames transmitted on a given port (also known as egress or destination mirroring).

Port to mirror to: Port to mirror also known as the mirror port. Frames from ports that have either source (rx) or destination (tx) mirroring enabled are mirrored on this port. Disabled disables mirroring.

2-21 UPnP

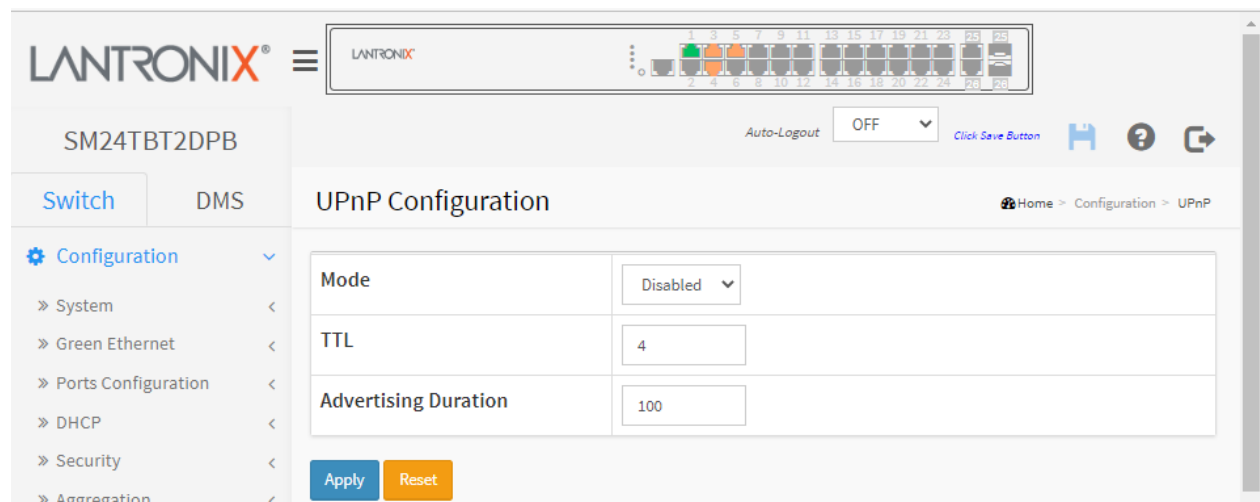
UPnP (Universal Plug and Play) allows devices to connect seamlessly and to simplify implementing networks in the home (data sharing, communications, and entertainment) and in corporate environments for simplified installation of computer components.

Caution: UPnP allows clients in the local network to automatically configure the device. UPnP should only be used (enabled) if necessary and with preventive measures as it can result in high security risks for your network.

To configure UPnP in the web UI:

1. Click Configuration, UPnP.
2. Set the mode to Enabled or Disabled.
3. Specify the parameters in each blank field.
4. Click the Apply button to save the settings.
5. To cancel the settings click the Reset button. The page will revert to previously saved values.

Figure 2-21: UPnP Configuration page



Parameter descriptions:

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

Enabled: Enable UPnP mode operation.

Disabled: Disable UPnP mode operation (default).

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 TTL value is used by UPnP to send SSDP advertisement messages. Valid values are 1 - 255.

Advertising Duration: The duration, carried in SSDP packets, is used to inform a control point or control points how often it or they should receive an SSDP advertisement message from this switch.

If a control point does not receive any message within the duration, it will think that the switch no longer exists. Due to the unreliable nature of UDP, in the standard it is recommended that such refreshing of advertisements 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 in the range 100 - 86400.

Buttons:

Apply – Click to save changes.

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

2-22. 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.

2-22.1 GVRP Config

This page lets you configure the global GVRP settings that are commonly applied to all GVRP enabled ports. To configure GVRP in the web UI:

1. Click Configuration, GVRP, Global Config.
2. Check the Enable GVRP box to enable GVRP globally.
3. Specify Join-time, Leave-time, Leave All-time, and Max VLANs.
4. Click Apply.

Figure 2-22.1: GVRP Configuration page

Parameter	Value
Enable GVRP	<input type="checkbox"/>
Join-time:	20 (1-20)
Leave-time:	60 (60-300)
LeaveAll-time:	1000 (1000-5000)
Max VLANs:	20

Parameter descriptions:

Enable GVRP: To enable the GVRP feature globally check the Enable GVRP checkbox and click the Apply button.

GVRP protocol timers:

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

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

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

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

Buttons:

Apply – Click to save changes.

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

2-22.2 Port Config

This page lets you enable a port for GVRP and configure basic GVRP settings. To configure GVRP in the web UI:

1. Click Configuration, GVRP, Port Config.
2. Specify the Mode for one or more Ports.
3. Click the Apply button.

Figure 2-22.2: GVRP Port Configuration page

The screenshot shows the Lantronix web interface for GVRP Port Configuration. The page title is "GVRP Port Configuration" and the breadcrumb trail is "Home > Configuration > GVRP > Port Config". The page features a table with the following data:

Port	Mode
*	<>
1	Disabled
2	GVRP enabled
3	GVRP enabled
4	GVRP enabled
5	GVRP enabled
6	GVRP enabled
7	Disabled
8	Disabled
9	...

Parameter descriptions:

Mode: This parameter lets you enable or disable GVRP Mode on a particular port locally.

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

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

Buttons:

Apply – Click to save changes.

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

2-23. sFlow

The sFlow Collector configuration for the switch can be monitored and modified here. The configuration is divided into two parts: configuration of the sFlow receiver (a.k.a. sFlow collector) and configuration of per-port flow and counter samplers.

sFlow configuration is not persisted to non-volatile memory, which means that a reboot or master change will disable sFlow sampling.

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>.

To configure the sFlow Agent via the web UI:

1. Click Configuration, sFlow.
2. Set the Agent, Receiver, and Port parameters.
3. Click Apply to save the settings.

Figure 2-23: sFlow Configuration page

LANTRONIX® SM24TBT2DPB

sFlow Configuration

Agent Configuration

IP Address: 127.0.0.1

Receiver Configuration

Owner: <none> [Release]

IP Address/Hostname: 0.0.0.0

UDP Port: 6343

Timeout: 0 seconds

Max. Datagram Size: 1400 bytes

Port Configuration

Port	Flow Sampler				Counter Poller	
	Enabled	Sampler Type	Sampling Rate	Max. Header	Enabled	Interval
*	<input type="checkbox"/>	<none>	0	128	<input type="checkbox"/>	0
1	<input type="checkbox"/>	Tx	0	128	<input type="checkbox"/>	0
2	<input type="checkbox"/>	Tx	0	128	<input type="checkbox"/>	0
3	<input type="checkbox"/>	Tx	0	128	<input type="checkbox"/>	0
4	<input type="checkbox"/>	Tx	0	128	<input type="checkbox"/>	0
5	<input type="checkbox"/>	Tx	0	128	<input type="checkbox"/>	0

Agent Configuration

IP Address: The IP address used as the Agent IP address in sFlow datagrams. It serves as a unique key that will identify this agent over extended periods of time. Both IPv4 and IPv6 addresses are supported.

Receiver Configuration

Owner: Basically, sFlow can be configured in two ways: through local management using the Web or CLI 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.

Max. Datagram Size: The maximum number of data bytes that can be sent in a single sample datagram. This should be set to a value that avoids fragmentation of the sFlow datagrams. Valid range is 200 to 1468 bytes with default being 1400 bytes.

Port Configuration

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

Flow Sampler Enabled: Enables/disables flow sampling on this port.

Flow Sampler Sampling Rate: The statistical sampling rate for packet sampling. Set to N to sample on average 1/Nth of the packets transmitted/received on the port.

Not all sampling rates are achievable. If an unsupported sampling rate is requested, the switch will automatically adjust it to the closest achievable. This will be reported back in this field.

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.

Buttons:

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.

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.

Messages:

'Sampling Rate' must be an integer value between 1 and 4294967295

'Interval' must be an integer value between 1 and 3600

2-24 Rapid Ring Configuration

Configure Rapid Ring and Ring To Ring parameters on this page. **Note** that Spanning Tree must be disabled on ports 25 and 26 at Configuration > Spanning Tree > CIST Port. **Note:** FW v6.54.3303 added Rapid Ring support on two uplink ports.

Before FW v6.54.3203: configure Rapid Ring and Ring To Ring parameters:

SM24TBT2DPA Rapid Ring Configuration

Global Configuration

Role	1st Ring Port	Status	2nd Ring Port	Status
Disabled	Port 1	Forwarding	Port 1	Forwarding
Disabled	Port 1	Forwarding	Port 1	Forwarding

Ring To Ring Configuration

Role	Port	Status
Disabled	Port 1	Forwarding

Apply Reset

At FW v6.54.3303 and above: configure Rapid Ring global parameters:

LANTRONIX SM24TBT2DPB Rapid Ring Configuration

Global Configuration

Index	Role	Port	Status
1	Disabled	25	Forwarding
		26	Forwarding

Apply Reset

Parameter descriptions:

Global Configuration section:

Index: Displays the instance number for this line of the table.

Role: At the dropdown assign a Rapid Ring role; either **Master**, **Member**, or **Disabled**.

Port: Displays the Port numbers 25 and 26.

Status: e.g., *Forwarding*, *Discarding*, etc.

Ring To Ring Configuration section: (only before FW v6.54.3236)

Role: At the dropdown assign a Rapid Ring role; either **Master**, **Member**, or **Disabled**.

Port: At the dropdown assign a Port.

Status: Ring status (e.g., *Forwarding*, *Discarding*, ...).

Buttons:

Apply: Click to save the changes.

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

Role

Master

Disabled

Master

Member

Role

Master

Disabled

Master

Member

2-25 PercepXion and LPM

This page lets you configure PercepXion parameters. This page has four sections: the Status, Configuration, PercepXion Connection 1, and Connection 2 sections as shown and described below.

PercepXion is Lantronix cloud-hosted management platform that provides a single pane of glass for centralized management and automated monitoring of all deployed Lantronix Remote Environment Management and IoT products, along with real-time notifications, managed APIs and data dashboards. For more information see <https://www.lantronix.com/percepXion/>.

Lantronix Provisioning Manager (LPM) is a software application that provisions, configures and updates Lantronix devices for local site installations and deployments. **Note:** LPM discovery is currently enabled by default and is not configurable. For more information see <https://www.lantronix.com/products/lantronix-provisioning-manager/>.

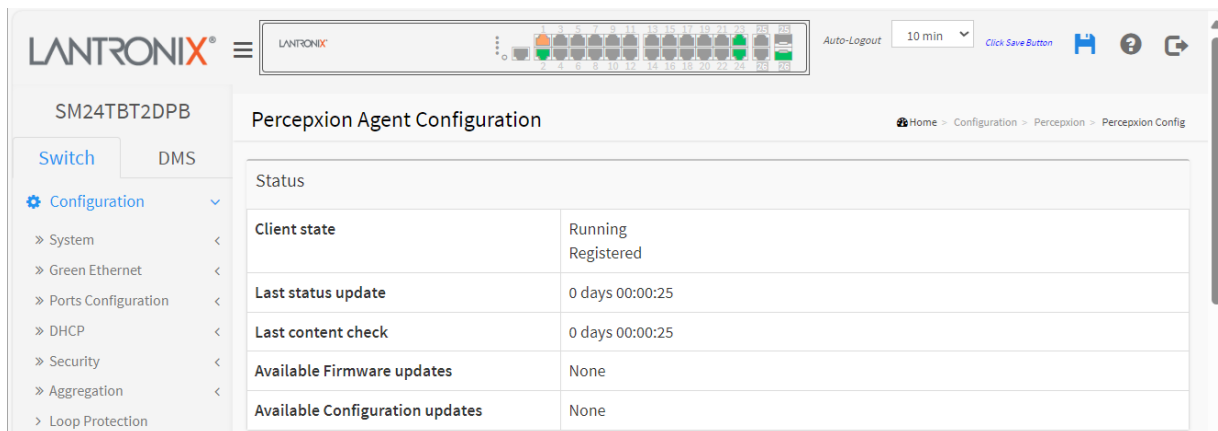
There are three pieces of information that the PercepXion client needs to complete registration and to publish data and configuration to the PercepXion server: Serial Number, Device ID, and Device Key. The Serial Number is always preprogrammed on the device (typically derived from the MAC address of the first Ethernet port). A new device would also be preprogrammed with the Device ID and Key. For existing devices where the ID and Key are not pre-programmed, LPM uses Lantronix proprietary search and query protocol to get the device serial number, and then uses the switch REST API interface to set the Device ID and Device Key.

Supported Firmware Versions

Devices must meet firmware requirements to work with PercepXion and LPM. The SM24TBT2DPA and SM24TBT2DPB require firmware **VB6.64.0123** or above.

PercepXion Agent Configuration

Navigate to Configuration > PercepXion to display the PercepXion Agent Configuration page:



The screenshot shows the Lantronix web interface for the SM24TBT2DPB device. The main content area is titled "PercepXion Agent Configuration". It features a "Status" section with a table containing the following data:

Client state	Running Registered
Last status update	0 days 00:00:25
Last content check	0 days 00:00:25
Available Firmware updates	None
Available Configuration updates	None

Parameter descriptions:

Status:

Client state: Displays the existing PercepXion client state (e.g., *Exited*, *Active*, *Inactive*, *Running*, or *Not Registered*).

Last status update: Displays the amount of time since the last status update, starting at *0 days 00:00:25*.

Last content check: Displays the amount of time since the last content check, starting at *0 days 00:00:25*.

Available Firmware updates: Displays a list of firmware that is available on the server. Select the firmware from this list and click Update now to upgrade or downgrade the firmware. Displays *None* if no Firmware updates are currently available.

Available Configuration updates: Displays a list of configuration that is available on the server. Select the configuration from this list and click Update now to upgrade or downgrade the firmware. Displays *None* if no configuration updates are currently available.

Global Configuration:

Global Configuration	
Enabled	<input checked="" type="checkbox"/>
Device ID	00c0f2838328zP
Device Key
Serial Number	00c0f2838328
Device Name	SM24TBT2DPB-8328
Device Description	Lantronix SM24TBT2DPB
Status Update Interval (in minutes)	1
Content Check Interval (in minutes)	1
Apply Firmware Updates	<input checked="" type="checkbox"/>
Apply Configuration Updates	<input checked="" type="checkbox"/>
Active Connection	Connection 1

Enabled : Check the box to enable PercepXion globally. The default is enabled (checkbox checked).

Device ID: Displays the switch Device ID (read only). The Device ID may be provisioned through Lantronix Provisioning manager (LPM). **Note**: The Device ID can only be provisioned once. It will persist across resets.

Device Key: Enter a key for the device of 32 alphanumeric characters. **Note**: Device Key may be configured via the Lantronix Provision Manager (LPM). The entry field shows two icons:



: Show the Device Key text as you enter it.



: Hide the Device Key text as you enter it.

Serial Number : Displays the serial number of the switch in the format *A206121BR1500003*. Read only.

Device Name : Enter a PercepXion Device Name for the switch of up to 32 alphanumeric characters (e.g., *SM24TBT2DPB-8328*). Device Name can have only alphanumeric (a-z, A-Z, 0-9) characters, hyphens (-), and underscores (_). Device Name must begin and end with an alphanumeric character.

Device Description : Enter a PercepXion Device Description for the switch of up to 32 alphanumeric characters (e.g., *Lantronix SM24TBT2DPB*).

Status Update Interval in minutes : Select the amount of time in minutes between updates (1-1440 minutes). The default is 1 minute. This is the frequency that the switch updates the device status to PercepXion.

Content Check Interval in minutes : Select the amount of time in minutes between content checks (1-56160 minutes). The default is 1 minute. This is the frequency that the switch checks PercepXion for updates to configuration or firmware. The valid range is 1 hour – 2160 hours (90 days).

Apply Firmware Updates : Check the box to enable automatic switch firmware upgrades via PercepXion. The default is enabled.

Apply Configuration Updates : Check the box to enable automatic switch configuration upgrades via PercepXion. The default is enabled.

Active Connection: At the dropdown select the configuration you want to be active (i.e., *Connection 1* or *Connection 2*). The default is *Connection 1*. This is the connection to use when connecting to PercepXion. The parameters for Connection 1 and Connection 2 are shown and described below.

The screenshot shows the 'PercepXion Config' page. On the left is a navigation menu with 'PercepXion Upload', 'SMTP', 'Monitor', 'Diagnostics', and 'Maintenance'. The main area is divided into two sections: 'Connection 1' and 'Connection 2'. Each section has a 'Connect To' dropdown menu (set to 'Cloud'), a 'Host' text input (containing 'api.gopercepXion.ai'), a 'Port' text input (containing '443'), a 'Secure Port' checkbox (checked), and a 'Validate Certificates' checkbox (unchecked). At the bottom of the form are 'Apply' and 'Reset' buttons.

Connection 1 :

Connect To : At the dropdown select the type of PercepXion connection to be made for Connection 1:

Cloud : Use PercepXion Cloud-based connection. The default is Cloud connection.

On Premise : Use PercepXion on-premise connection.

The dropdown menu is open, showing 'Cloud' as the selected option and 'On Premise' as an alternative option.

Host : Enter the IP address or host name of the PercepXion server for Connection 1. This is used by PercepXion to register the switch.

Port : Enter the port number for Connection 1. The default is port 443.

Secure Port : Check the box to make the selected port a secure port for Connection 1. The default is enabled.

Validate Certificates : Check the box to force using certificate validation of the PercepXion server certificates for Connection 1. The default is enabled. To validate certificates Secure Port must be enabled.

Connection 2 :

Host : Enter the IP address of the PercepXion Host for Connection 2.

Port : Enter the port number for Connection 2 for Connection 2. The default is port 443.

Secure Port : Check the box to make the selected port a secure port for Connection 2. The default is enabled.

Validate Certificates : Check the box to force using certificate validation of the PercepXion server certificates for Connection 2. The default is enabled. To validate certificates Secure Port must be enabled.

Buttons

Apply : Click to apply changes.

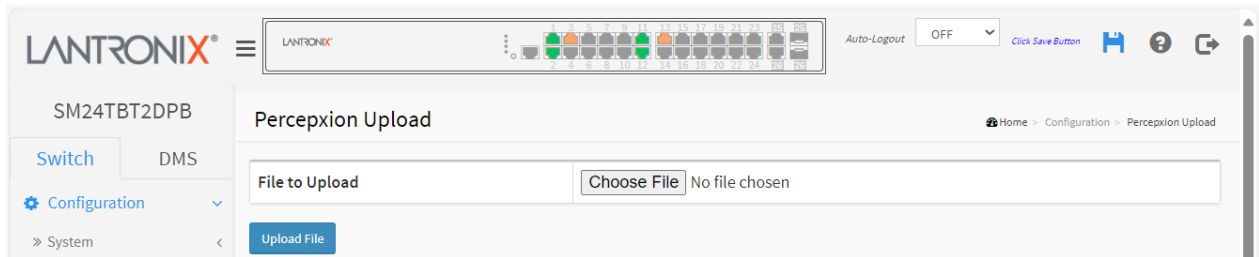
Reset : Click to undo any changes made locally and revert to previously saved values.

Messages: *device id : 32 alphanumeric characters*

5

Percepixon Upload

Navigate to Configuration > Percepixon > Upload to display the Percepixon Upload page. This page lets you upload a file from the web browser. Select the file to upload, then click the Upload File button.



Parameter descriptions:

Choose File : Click the button to navigate to and select the file to be uploaded.

Upload File : After a file is selected, click the button to perform the upload.

2-26 SMTP Configuration

Configure SMTP (Simple Mail Transfer Protocol) on this page. SMTP is the message-exchange standard for the Internet. The switch can be configured as a client of SMTP while the server is a remote device that will receive messages from the switch that alarm events occurred.

To configure SMTP in the web UI:

1. Click Configuration, SMTP Configuration.
2. Specify the parameters in each blank field.
3. Click the **Apply** button to save the settings.
4. To cancel the settings click the **Reset** button to revert to previously saved values.

Figure 2-25: SMTP Configuration page

The screenshot shows the LANTRONIX web interface for the SM24TBT2DPB device. The page title is "SMTP Configuration". On the left, there is a navigation menu with "Switch" and "DMS" tabs, and a "Configuration" section expanded to show various settings like System, Green Ethernet, Ports Configuration, DHCP, Security, Aggregation, Loop Protection, Spanning Tree, IPMC Profile, MVR, IPMC, LLDP, PoE, MAC Table, VLANs, and Private VLANs. The main configuration area contains the following fields:

Mail Server	<input type="text"/>
User Name	<input type="text"/>
Password	<input type="text"/>
Sender	<input type="text"/>
Return Path	<input type="text"/>
Email Address 1	<input type="text"/>
Email Address 2	<input type="text"/>
Email Address 3	<input type="text"/>
Email Address 4	<input type="text"/>
Email Address 5	<input type="text"/>
Email Address 6	<input type="text"/>

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

Parameter descriptions:

Mail Server: Specify the IP Address of the server transferring your email.

Username: Specify the username on the mail server.

Password: Specify the password on the mail server.

Sender: To set the mail sender name.

Return-Path: To set the mail return-path as sender mail address.

Email Address 1-6: Email address that would like to receive the alarm message.

Buttons:

Apply: Click to apply changes.

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

Chapter 3 - Monitor

The Monitor menus display the current parameter settings for each module (e.g., System, Ports, DHCP, Security, LACP, etc.).

3-1 System

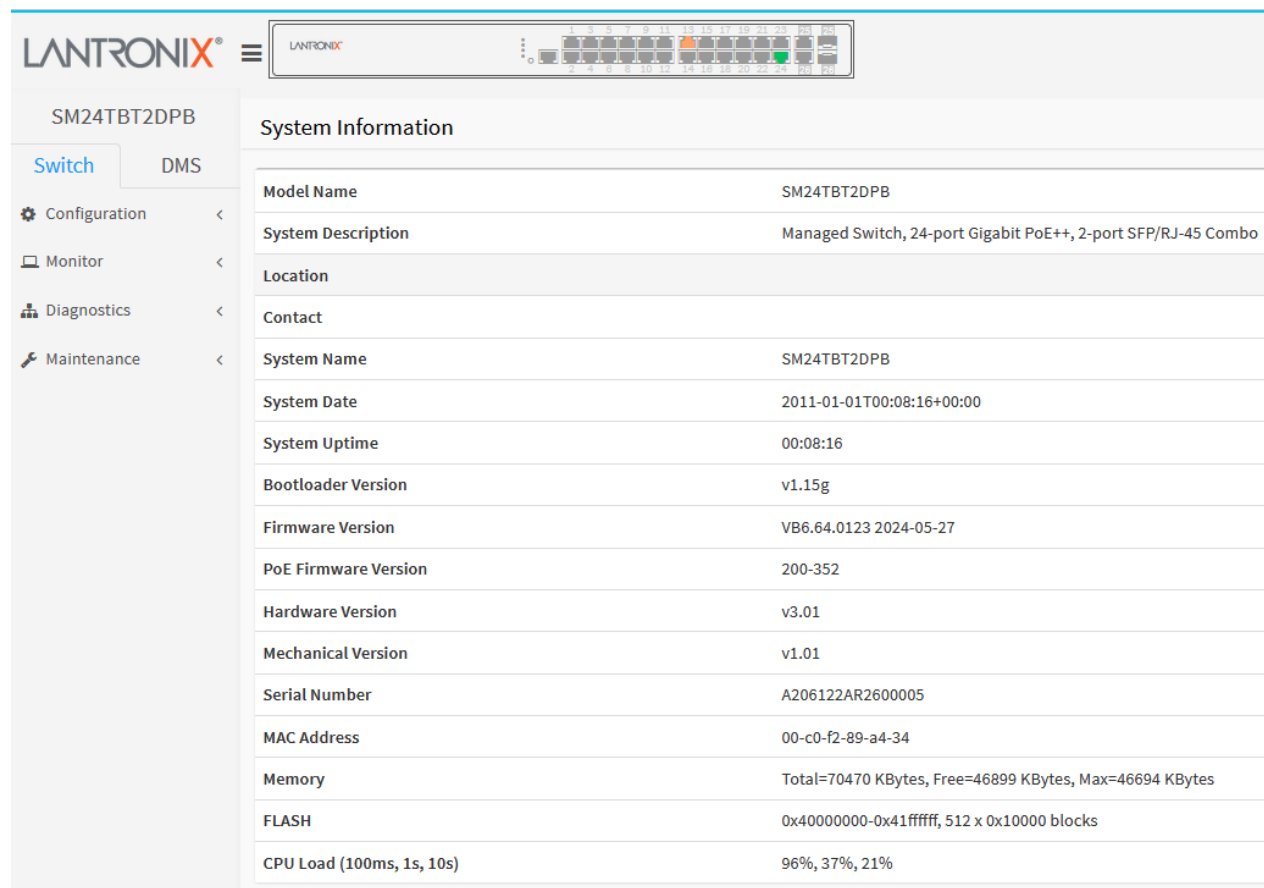
After you log in, the switch displays the System Information page. This page provides basic system information, including Model Name, System Description, Contact, Firmware Version, etc. This information is helpful when contacting Technical Support.

3-1.1 Information

Switch system information is provided here. To view System Information in the web UI:

1. Click Monitor, System, Information.
2. View the name and location of the switch, the system date, firmware version, serial number, etc.

Figure 3-1.1: System Information page (SM24TBT2DPB)



System Information	
Model Name	SM24TBT2DPB
System Description	Managed Switch, 24-port Gigabit PoE++, 2-port SFP/RJ-45 Combo
Location	
Contact	
System Name	SM24TBT2DPB
System Date	2011-01-01T00:08:16+00:00
System Uptime	00:08:16
Bootloader Version	v1.15g
Firmware Version	VB6.64.0123 2024-05-27
PoE Firmware Version	200-352
Hardware Version	v3.01
Mechanical Version	v1.01
Serial Number	A206122AR2600005
MAC Address	00-c0-f2-89-a4-34
Memory	Total=70470 KBytes, Free=46899 KBytes, Max=46694 KBytes
FLASH	0x40000000-0x41ffffff, 512 x 0x10000 blocks
CPU Load (100ms, 1s, 10s)	96%, 37%, 21%

Parameter descriptions:

Model Name: Displays the factory defined model name for identification purposes (e.g., *SM24TBT2DPB*).

System Description: Displays the system description (e.g., *Managed Switch, 24-port Gigabit PoE++, 2-port SFP/RJ-45 Combo*).

Location: Displays the location of this node that was configured at Configuration > System > Information.

Contact: Displays the text identifying the contact configured at Configuration > System > Information.

System Name: Displays the assigned name for this managed node (e.g., *SM24TBT2DPB*).

System Date: Displays the date this switch was manufactured (e.g., *2023-09-21T11:22:51+00:00*).

System Uptime: The amount of time this switch has been running in the format hh:mm:ss (e.g., *04:30:11*).

Bootloader Version: Displays the current boot loader version number (e.g., *v1.15g*).

Firmware Version: The current switch firmware version and build date (e.g., *VB6.64.0123 2024-05-14*).

PoE Firmware Version: The version of PoE MCU firmware (e.g., *200-352*).

Hardware Version: The hardware version of this switch (e.g., *v1.02*).

Mechanical Version: The mechanical versions of this switch (e.g., *v1.01*).

Serial Number: The serial number of this switch (e.g., *A137198DF789A960*).

MAC Address: The MAC Address of this switch assigned to this switch at the factory (e.g., *02-0c-41-f2-fb-f9*).

Memory: Displays the memory size of the system (e.g., *Total=74639 KBytes, Free=51138 KBytes, Max=50216 Kbytes*).

FLASH: Displays the flash size of the system (e.g., *0x40000000-0x41ffffff, 512 x 0x10000 blocks*).

CPU Load (100ms, 1s, 10s): Displays the percentage of CPU loading (100ms, 1s, 10s) of the system (e.g., *1%, 4%, 3%*).

(SM24TBT2DPB with two PS)

Power A/B Present : On the rear panel: Left Power Module = A , Right Power Module = B. Power Module A/B present status.

Power A/B Good: Power Module A/B good status.

Power A/B FAN Speed(RPM) : Power Module A/B fan speed (RPM).

Power A/B Operating Temperature (C) : Power Module A/B Operating Temperature (C).

Power Module Monitoring Change

SM24TBT2DPB FW VB6.64.0045 changed the way that the switch power supplies are monitored:

1. When the system is turned on and the switch finds that Power A and B are different PSUs, the management software will turn off 920W PSU output power.
2. When the system has just one PSU working, and then a second PSU is inserted into a power slot, if the second PSU inserted is different than the existing PSU, the second PSU inserted will have its output power turned off.
3. When Power A and B are different PSUs, the PoE Power Budget will maintain the status quo and will not be recalculated and adjusted.
4. When Power A and B are different, then the power module Event Log and Trap are different for Power A and B.

3-1.2 IP Status

This page displays the status of the IP protocol layer. The status is displayed for IP Interfaces, IP Routes, Neighbor cache (ARP cache) and DNS Server. To display IP Status in the web UI:

1. Click Monitor, System, IP Status.
2. View the IP address information.

Figure 3- 1.3: IP Status page

The screenshot shows the Lantronix web UI for device SM24TBT2DPB. The main content area is titled "IP Interfaces" and includes an "Auto-refresh" button. Below this, there are four sections: IP Interfaces, IP Routes, Neighbour cache, and DNS Server.

IP Interfaces Table:

Interface	Type	Address	Status
VLAN1	LINK	00-c0-f2-7c-58-77	<UP BROADCAST RUNNING MULTICAST>
VLAN1	IPv4	192.168.1.77/24	
VLAN1	IPv4	169.254.79.119/16	
VLAN1	IPv6	fe80::2c0:f2ff:fe7c:5877/64	
VLAN4096	LINK	00-c0-f2-7c-58-77	<BROADCAST MULTICAST>
VLAN4097	LINK	00-c0-f2-7c-58-77	<BROADCAST MULTICAST>

IP Routes Table:

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>
::1/128	::1	<UP HOST>

Neighbour cache Table:

IP Address	Link Address
169.254.7.49	VLAN1:00-09-18-4e-20-e9
169.254.11.169	VLAN1:00-16-6c-d4-dd-c2
169.254.138.213	VLAN1:ec-cc-8e-be-f7-c1
192.168.1.75	VLAN1:5c-f3-35-dc-0a-c1
192.168.1.77	VLAN1:00-c0-f2-7c-58-77
192.168.1.100	VLAN1:00-09-18-4e-20-e9
fe80::2c0:f2ff:fe7c:5877	VLAN1:00-c0-f2-7c-58-77

DNS Server Table:

Type	IP Address	Interface
Static	8.8.8.8	

IP Interfaces

Interface: Shows the name of the interface (e.g., *VLAN1*).

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

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

Status: Shows the status flags of the interface and/or address (e.g., *<UP BROADCAST RUNNING MULTICAST>* or *<BROADCAST MULTICAST>*).

IP Routes

Network: Shows the destination IP network or host address of this route.

Gateway: Shows the gateway address of this route.

Status: Shows the status flags of the route (e.g., *<UP GATEWAY HW_RT>*, *<UP>*, *<UP HOST>*, *<UP HW_RT>*).

Neighbour cache

IP Address: Shows the IP address of the entry.

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

DNS Server

Type: The DNS server type (e.g., *Static*).

IP Address: The DNS server IP address (e.g., *0.0.0.0*).

Interface: The DNS server interface.

Buttons

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

Refresh: Click to manually refresh the page immediately.

3-1.3 Log

This page displays the system log information of the switch. To display syslog information in the web UI:

1. Click Monitor, System, Log.
2. View the log information.
3. Use the control buttons as needed.

Figure 3- 1.3: System Log Information page

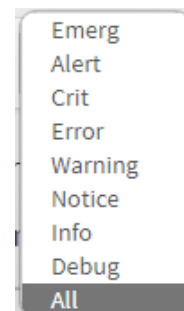
The screenshot shows the Lantronix web UI for device SM24TBT2DPB. The page title is "System Log Information". On the left is a navigation menu with "Monitor" expanded to "System" > "Log". The main area has an "Auto-refresh" checkbox and navigation buttons. Below are two dropdown menus for "Level" and "Clear Level", both set to "All". A message states "The total number of entries is 98 for the given level." and "Start from ID 1, 20 entries per page." Below this is a table titled "System Log" with columns for ID, Level, Time, and Message.

ID	Level	Time	Message
1	Warning	2011-01-01T00:00:23+00:00	Link up on port 5
2	Warning	2011-01-01T00:00:23+00:00	SFP module inserted on port 25
3	Warning	2011-01-01T00:00:23+00:00	Switch just made a warm boot
4	Warning	2011-01-01T00:00:23+00:00	SFP module inserted on port 26
5	Info	2011-01-01T00:00:23+00:00	topologyChange
6	Info	2011-01-01T00:00:23+00:00	topologyChange
7	Warning	2011-01-01T00:00:23+00:00	Power A: Inserted
8	Warning	2011-01-01T00:00:23+00:00	Power A: Fail
9	Warning	2011-01-01T00:00:23+00:00	Power A: Fan Good (0 RPM)

Parameter descriptions:

Level: The level of the system log entry. These level types are supported:

- Emerg:** Emergency level of the system log.
- Alert:** Alert level of the system log.
- Crit:** Critical level of the system log.
- Error:** Error level of the system log.
- Warning:** Warning level of the system log.
- Info:** Information level of the system log.
- Debug:** Debug level of the system log.
- All:** All levels logged and displayed (default).



Clear Level: The clear level of the system log entry. The level types supported are listed above.

ID: The instance number of the system log entry. Click a linked ID number to display its details.

Time: Displays the log record by device time. The time of the system log entry.

Message: Displays the log detail message. The message of the system log entry. For example: *Link up on port 1*, or *Switch just made a warm boot*, or *Password of user 'admin' was change ...*, *topologyChange*, *topologyChange*, *Power A: Fan Good (8873 RPM)*, *Login passed for user 'admin'*, etc.

Buttons



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



: **Refresh:** Updates the system log entries, starting from the current entry ID.



: **Clear:** Flushes the selected log entries.



: **First entry;** updates the system log entries, starting from the first available entry ID.



: **Previous entry;** updates the system log entries, ending at the last entry currently displayed.



: **Next entry;** updates the system log entries, starting from the last entry currently displayed.



: **Last entry;** updates the system log entries, ending at the last available entry ID.

Example

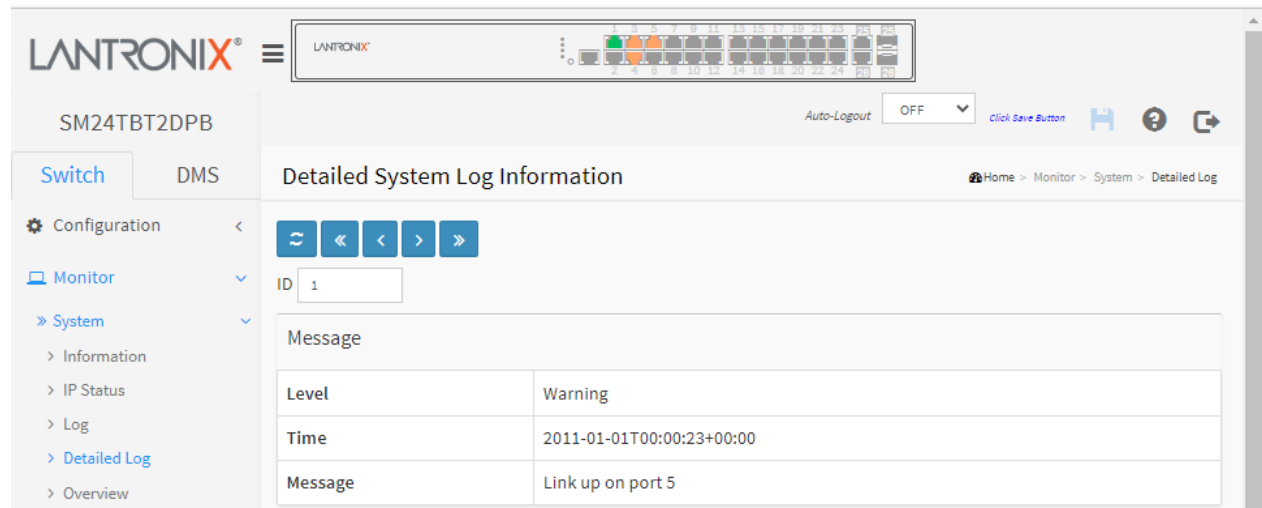
```
System Log
ID  Level   Time                               Message
1   Warning 2019-06-17T02:56:30+00:00 SFP module inserted on port 26
2   Warning 2019-06-17T02:56:31+00:00 Link up on port 1
3   Warning 2019-06-17T02:56:31+00:00 Link up on port 26
4   Warning 2019-06-17T02:56:31+00:00 Switch just made a cold boot
5   Info 2019-06-17T02:56:31+00:00 topologyChange
6   Info 2019-06-17T02:56:31+00:00 topologyChange
7   Info 2019-06-17T02:56:31+00:00 topologyChange
8   Warning 2019-06-17T02:56:31+00:00 Link up on port 2
9   Info 2019-06-17T02:56:31+00:00 Password of user 'admin' was change ...
10  Warning 2019-06-17T02:56:31+00:00 Link up on port 3
11  Warning 2019-06-17T02:56:31+00:00 SFP module inserted on port 25
12  Info 2019-06-17T02:56:32+00:00 topologyChange
13  Info 2019-06-17T02:56:34+00:00 topologyChange
14  Warning 2019-06-17T02:56:34+00:00 Power A: Removed
15  Warning 2019-06-17T02:56:34+00:00 Power A: Fail
16  Warning 2019-06-17T02:56:34+00:00 Power A: Fan Good (8898 RPM)
17  Warning 2019-06-17T02:56:34+00:00 Power A: Temperature Normal (28 C)
18  Warning 2019-06-17T02:56:34+00:00 Power B: Removed
19  Warning 2019-06-17T02:56:34+00:00 Power B: Fail
20  Warning 2019-06-17T02:56:34+00:00 Power B: Fan Good (0 RPM)
```

3-1.4 Detailed Log

This page displays more detailed log information of the switch. To display detailed log information in the web UI:

1. Click Monitor, System, and Detailed Log.
2. View the log information.

Figure 3- 1.4: Detailed System Log Information page



Parameter descriptions:

ID: The ID of the system log entry.

Message: The detailed message of the system log entry (the level, time, and message displayed).



Buttons

Refresh: Updates the system log entries, starting from the current entry ID.

<< : First Entry; updates the system log entries to the first available entry ID.

< : Previous Entry; updates the system log entry to the previously available entry ID.

> : Next Entry; updates the system log entry to the next available entry ID.

>> : Last Entry; updates the system log entry to the last available entry ID.

Messages

Info messages: e.g., topologyChange, Login passed for user 'admin', etc.

Warning messages: Switch just made a warm boot, Link up on port 1, SFP module inserted on port 25, Password of user 'admin' was change ... , Power A: Inserted, Power A: Good, Power A: Fan Good (8873 RPM), Power A: Temperature Normal (31 C), Power B: Removed, Power B: Fail, Power B: Fan Good (0 RPM), Power B: Temperature Normal (0 C), Bad password attempt for user " through TELNET from 192.168.1.99 and authenticated by local method, User 'admin' logout through HTTP from 192.168.1.99, etc.

3-1.5 System Overview

This page displays an overview of system level information of the switch. To display the System Overview page in the web UI:

1. Click Monitor, System, Overview.
2. View the system information.

Figure 3- 1.4: System Overview page

System Overview	
Model Name	SM24TBT2DPB
Connected Devices	3
PoE Power Consumption	2.5 [W]
Total PoE Available	897.5 [W]
Firmware Version	VB6.64.0117 2023-12-14
MAC Address	00-c0-f2-83-83-28
System Uptime	86d 09:08:49
IP Address	172.27.195.140
Subnet Mask	255.255.255.0
Gateway	172.27.195.1
Primary DNS	8.8.8.8

Parameter descriptions:

Model Name: Displays the factory defined model name for identification purposes (*SM24TBT2DPA*).

Connected Devices: Total number of currently connected devices (e.g., 11).

PoE Power Consumption: Displays the PoE power consumption (e.g., e.g., 3.4 [W] with one power supply or 7.3 [W] with two power supplies).

Total PoE Available: Displays the Total PoE budget available (e.g., 891.5 [W] with one power supply or 1636.7 [W] with two power supplies). See the “Operating Mode” parameter at Configuration > Power Information. Shows how much calculated power is still available in the system until it will reach the power limit: Available Power = (Power Limit – Calculated power consumption) in Watts.

Firmware Version: Displays the current firmware version number and release date (e.g., *VB6.64.0123 2024-05-14*).

MAC Address: The MAC Address of this switch (e.g., *00-40-c7-b9-20-b2*).

System Uptime: The period of time the device has been operational (e.g., *86d 09:08:49*).

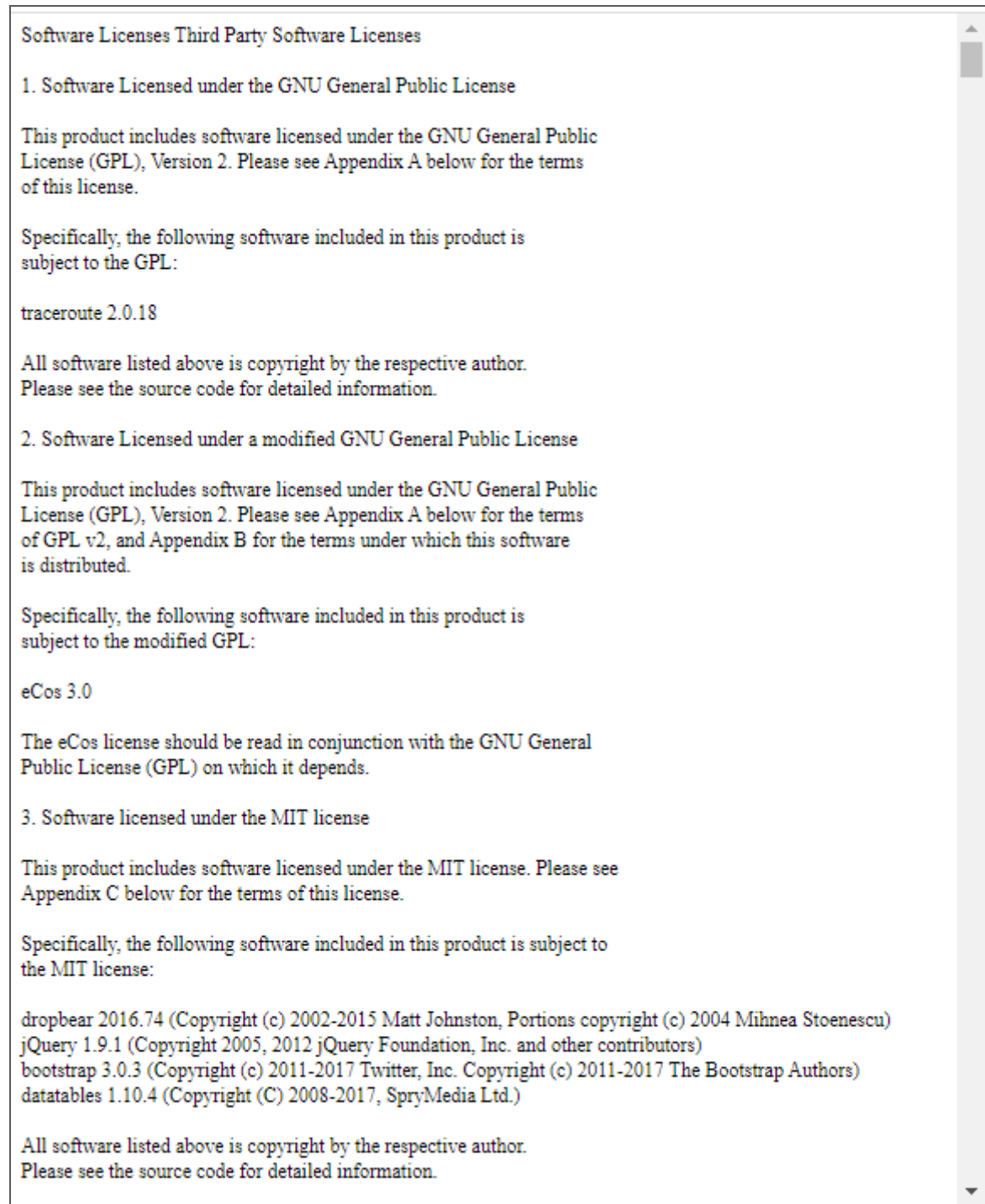
IP Address: The IPv4 or IPv6 address of the interface (e.g., *192.168.1.77*).

Subnet Mask: The IPv4 or IPv6 network mask of the interface (e.g., *255.255.255.0*).

Gateway: The IP address of the IP gateway (*192.168.1.254*)

Primary DNS: The IP address of the DNS Server.

Note that the System Overview Help provides a link to Third party licenses at the bottom of the page. Click the linked text "[Third party licenses](#)" to display the license page. A sample Third Party Software Licenses page is shown below:



Software Licenses Third Party Software Licenses

1. Software Licensed under the GNU General Public License

This product includes software licensed under the GNU General Public License (GPL), Version 2. Please see Appendix A below for the terms of this license.

Specifically, the following software included in this product is subject to the GPL:

traceroute 2.0.18

All software listed above is copyright by the respective author. Please see the source code for detailed information.

2. Software Licensed under a modified GNU General Public License

This product includes software licensed under the GNU General Public License (GPL), Version 2. Please see Appendix A below for the terms of GPL v2, and Appendix B for the terms under which this software is distributed.

Specifically, the following software included in this product is subject to the modified GPL:

eCos 3.0

The eCos license should be read in conjunction with the GNU General Public License (GPL) on which it depends.

3. Software licensed under the MIT license

This product includes software licensed under the MIT license. Please see Appendix C below for the terms of this license.

Specifically, the following software included in this product is subject to the MIT license:

dropbear 2016.74 (Copyright (c) 2002-2015 Matt Johnston, Portions copyright (c) 2004 Mihnea Stoenescu)
jQuery 1.9.1 (Copyright 2005, 2012 jQuery Foundation, Inc. and other contributors)
bootstrap 3.0.3 (Copyright (c) 2011-2017 Twitter, Inc. Copyright (c) 2011-2017 The Bootstrap Authors)
datatables 1.10.4 (Copyright (C) 2008-2017, SpryMedia Ltd.)

All software listed above is copyright by the respective author. Please see the source code for detailed information.

3-2 Green Ethernet

3-2.1 Port Power Savings

This page displays the current status for EEE (Energy Efficient Ethernet) defined in IEEE 802.3az. To view Power Savings status in the web UI:

1. Click Monitor, Green Ethernet, Port Power Savings.
2. View the displayed information.

Figure 3- 2.1: Port Power Savings Status page

Port	Link	EEE	LP EEE Cap	EEE Savings
1	●	✘	✓	✘
2	●	✘	✓	✘
3	●	✘	✘	✘
4	●	✘	✓	✘
5	●	✘	✘	✘
6	●	✘	✘	✘
7	●	✘	✘	✘
8	●	✘	✘	✘
-	-	-	-	-

Parameter descriptions:

Port: The logical (local) port number for this row.

Link: Shows if the link is up for the port (green ● = link up, red ● = link down).

EEE: Shows ✓ if EEE is enabled for the port (reflects the settings at the Port Power Savings configuration page).

LP EEE Cap: Shows ✓ if the link partner is EEE capable, otherwise shows ✘.

EEE Savings: Shows if the system is currently saving power due to EEE. When EEE is enabled, the system will power down if no frame has been received or transmitted in 5 microseconds.

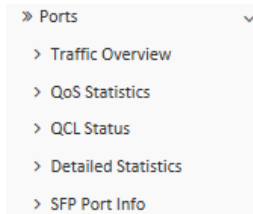
Buttons

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

Refresh: Click to refresh the page immediately.

3-3 Ports

This section displays ports traffic, QoS statistics and status, and SFP port information in the switch.



3-3.1 Traffic Overview

This page shows Port statistics information and provides an overview of general traffic statistics for all switch ports.

To display Port Statistics Overview in the web UI:

1. Click Monitor, Port, Traffic Overview.
2. To automatically refresh the page, check the “Auto-refresh” checkbox.
3. Click “Refresh” to refresh the port statistics or clear all information when you click “ Clear”.

Figure 3-3.1: Port Statistics Overview page

LANTRONIX SM24TBT2DPB

Port Statistics Overview

Auto-refresh

Port	Packets		Bytes		Errors		Drops		Filtered
	Received	Transmitted	Received	Transmitted	Received	Transmitted	Received	Transmitted	Received
1	27390	140708	7244410	25480655	0	0	0	0	68
2	4464	114762	3107768	8599300	0	0	0	0	2
3	5391	113095	1546906	8464075	0	0	0	0	39
4	4493	114790	3109706	8603042	0	0	0	0	2
5	0	0	0	0	0	0	0	0	0
6	0	0	0	0	0	0	0	0	0
7	0	0	0	0	0	0	0	0	0
8	0	0	0	0	0	0	0	0	0
9	0	0	0	0	0	0	0	0	0

Parameter descriptions:

Port: The logical port for the settings contained in the same row.

Packets: The number of received and transmitted packets per port.

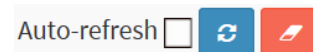
Bytes: The number of received and transmitted bytes per port.

Errors: The number of frames received in error and the number of incomplete transmissions per port.

Drops: The number of frames discarded due to ingress or egress congestion.

Filtered: The number of received frames filtered by the forwarding.

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.

3-3.2 QoS Statistics

This page displays statistics for the different QoS queues for all switch ports. To display the Queuing Counters in the web UI:

1. Click Monitor, Ports, QoS Statistics.
2. To auto-refresh the information check "Auto-refresh".
3. Click "Refresh" to refresh the Queuing Counters or clear all information when you click "Clear".

Figure 3-3.2: Queuing Counters page

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	24011	10092	0	0	0	0	0	0	0	0	0	0	0	0	0	0	206108
2	2826	2162	0	0	0	0	0	0	0	0	0	0	0	0	0	0	37133
3	6570	10092	0	0	0	0	0	0	0	0	0	0	0	0	0	0	165720
4	6593	10095	0	0	0	0	0	0	0	0	0	0	0	0	0	0	165745
5	7915	5576	0	0	0	0	0	0	0	0	0	0	0	0	0	0	166509
6	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
7	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
8	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
9	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0

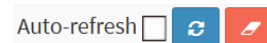
Parameter descriptions:

Port: The logical port for the settings contained in the same row.

Qn: the Queue number, There are eight QoS queues per port. Q0 is the lowest priority queue.

Rx/Tx: The number of received and transmitted packets per queue.

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.

3-3.3 QCL 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 on each switch.

To display the QoS Control List Status in the web UI:

1. Click Monitor, Ports, QCL Status.
2. At the QCL status dropdown select a status (Combined, Static, Voice VLAN, DMS, or Conflict).
3. To auto-refresh the information check the “Auto-refresh” checkbox.
4. Click the “Refresh” button to refresh the page.

Figure 3-3.3: QoS Control List Status page

User	QCE	Port	Frame Type	Action			Conflict
				CoS	DPL	DSCP	
Static	1	3-19,24,26	Any	0	Default	Default	No
Static	2	3-6,9,10,14-26	Ethernet	0	Default	Default	No
Static	3	1-26	LLC	3	Default	16 (CS2)	No
Static	4	3-9,12-17,19,22,25	IPv4	0	Default	18 (AF21)	No

Parameter descriptions:

User: Indicates the QCL user (e.g., Voice VLAN, Static, etc.).

QCE: Indicates the index of QCE.

Port: Indicates the list of ports configured with the QCE (e.g., None, 1-26, 1,3,6-26).

Frame Type: Indicates the type of frame to look for incoming frames. Possible frame types are:

Any: The QCE will match all frame type.

Ethernet: Only Ethernet frames (with Ether Type 0x600-0xFFFF) are allowed.

LLC: Only (LLC) frames are allowed

SNAP: Only (SNAP) frames are allowed.

IPv4: The QCE will match only IPV4 frames.

IPv6: The QCE will match only IPV6 frames.

Action: Indicates the classification action taken on ingress frame if parameters configured are matched with the frame's content. There are three action fields: Class, DPL and DSCP.

CoS: Classify Class of Service ; if a frame matches the QCE it will be put in the queue.

DPL: Classify Drop Precedence Level ; if a frame matches the QCE then DP level will set to value displayed under DPL column.

DSCP: Classify DSCP value; if a frame matches the QCE then DSCP will be classified with the value displayed under DSCP column.

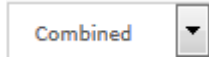
Conflict: Displays Conflict status of QCL entries. As Hardware resources are shared by multiple applications. It may happen that resources required to add a QCE may not be available, in that case it shows conflict status as 'Yes', otherwise it is always 'No'. **Note** that conflict can be resolved by releasing the Hardware resources required to add QCL entry on clicking the 'Resolve Conflict' button.

Buttons

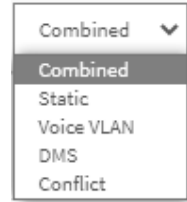
Auto-refresh: Check this box to refresh the page automatically every 3 seconds.

Refresh: Click to refresh the page immediately.

Resolve Conflict: Click to release the resources required to add QCL entry in case conflict status for any QCL entry is 'yes'.



: Select the QCL status from this drop down list.



3-3.4 Detailed Statistics

This page displays detailed traffic statistics for a specific switch port. The displayed counters are the totals for receive and transmit, the size counters for receive and transmit, and the error counters for receive and transmit.

To display per-port detailed Statistics Overview in the web UI:

1. Click Monitor, Ports, Detailed Statistics.
2. Use the port select box to select which switch port details to display.
3. To automatically refresh the information, check the “Auto-refresh” checkbox.
4. Click “Refresh” to refresh the port detailed statistics or clear all information when you click “Clear”.

Figure 3-3.4: Detailed Port Statistics page

Receive Total		Transmit Total	
Rx Packets	24494	Tx Packets	220021
Rx Octets	8159002	Tx Octets	59533509
Rx Unicast	23315	Tx Unicast	41019
Rx Multicast	1078	Tx Multicast	9445
Rx Broadcast	101	Tx Broadcast	169557
Rx Pause	0	Tx Pause	0
Receive Size Counters		Transmit Size Counters	
Rx 64 Bytes	14736	Tx 64 Bytes	158290
Rx 65-127 Bytes	947	Tx 65-127 Bytes	14766
Rx 128-255 Bytes	802	Tx 128-255 Bytes	2719
Rx 256-511 Bytes	37	Tx 256-511 Bytes	12007
Rx 512-1023 Bytes	7915	Tx 512-1023 Bytes	6609
Rx 1024-1526 Bytes	57	Tx 1024-1526 Bytes	25630
Rx 1527- Bytes	0	Tx 1527- Bytes	0
Receive Queue Counters		Transmit Queue Counters	
Rx Q0	24494	Tx Q0	10217
Rx Q1	0	Tx Q1	0
Rx Q2	0	Tx Q2	0
Rx Q3	0	Tx Q3	0

Parameter descriptions:

Receive Total and Transmit Total

Rx and Tx Packets: The number of received and transmitted (good and bad) packets.

Rx and Tx Octets: The number of received and transmitted (good and bad) bytes. Includes FCS, but excludes framing bits.

Rx and Tx Unicast: The number of received and transmitted (good and bad) unicast packets.

Rx and Tx Multicast: The number of received and transmitted (good and bad) multicast packets.

Rx and Tx Broadcast: The number of received and transmitted (good and bad) broadcast packets.

Rx and Tx Pause: A count of the MAC Control frames received or transmitted on this port that have an opcode indicating a PAUSE operation.

Receive and Transmit Size Counters: The number of received and transmitted (good and bad) packets split into categories based on their respective frame sizes.

Receive and Transmit Queue Counters: The number of received and transmitted packets per input and output queue.

Receive Error Counters

Rx Drops: The number of frames dropped due to lack of receive buffers or egress congestion.

Rx CRC/Alignment: The number of frames received with CRC or alignment errors.

Rx Undersize: The number of short 1 frames received with valid CRC.

Rx Oversize: The number of long 2 frames received with valid CRC.

Rx Fragments: The number of short 1 frames received with invalid CRC.

Rx Jabber: The number of long 2 frames received with invalid CRC.

Rx Filtered: The number of received frames filtered by the forwarding process.

Short frames are frames that are smaller than 64 bytes.

Long frames are frames that are longer than the configured maximum frame length for this port.

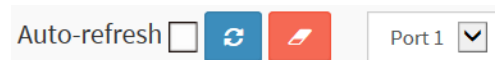
Transmit Error Counters

Tx Drops: The number of frames dropped due to output buffer congestion.

Tx Late/Exc. Coll.: The number of frames dropped due to excessive or late collisions.

Auto-refresh: Check to refresh the Queuing Counters automatically.

Buttons



Auto-refresh: Check this box to refresh the page automatically every 3 seconds.

Clear: Clears the counters for the selected port.

Refresh: Click to manually refresh the page immediately.

Port select scroll bar: At the dropdown select which port to display the Port statistics for.

3-3.5 SFP Port Info

This page displays general SFP information and monitoring information. The information includes Connector type, Fiber type, wavelength, baud rate, Vendor OUI, etc.

To display the SFP information in the web interface, click Monitor, Ports, SFP Port Info.

Figure 3-3.5: SFP Information for Port 25

The screenshot shows the 'SFP Information for Port 25' page in the Lantronix web interface. The page title is 'SFP Information for Port 25' and the breadcrumb is 'Home > Monitor > Ports > SFP Port Info'. The interface includes a navigation menu on the left with options like Configuration, Monitor, System, Green Ethernet, Ports, DHCP, Security, Aggregation, Loop Protection, Spanning Tree, MVR, IPMC, LLDP, PoE, and MAC Table. The main content area has an 'Auto-refresh' checkbox and a 'Port 25' dropdown menu. Below this is a table with the following data:

Connector Type	SFP or SFP Plus - LC
Fiber Type	Multi-mode (MM)
Tx Central Wavelength	850
Bit Rate	1000 Mbps
Vendor OUI	00-c0-f2
Vendor Name	Transition
Vendor P/N	TN-SFP-SX
Vendor Revision	0000
Vendor Serial Number	8789228
Date Code	110104
Temperature	none
Vcc	none
Mon1 (Bias)	none
Mon2 (TX PWR)	none
Mon3 (RX PWR)	none

Parameter descriptions:

Connector Type: Displays the connector type, e.g., SFP or SFP Plus-UTP, SC, ST, LC, etc.

Fiber Type: Displays the fiber mode, e.g., Multi-Mode (MM), Single-Mode (SM), SFP or SFP Plus – LC or 'Reserved'.

Tx Central Wavelength: Displays the fiber optical transmitting central wavelength (e.g., 850nm, 1310nm, 1550nm, etc.).

Bit Rate: Displays the nominal bit rate of the transceiver (e.g., 1000 Mbps or 10 Gbps).

Vendor OUI: Displays the OUI code which is assigned by IEEE (e.g., 00-c0-f2).

Vendor Name: Displays the company name of the SFP module manufacturer.

Vendor P/N: Displays the vendor part number.

Vendor Revision: Displays the SFP module revision.

Vendor Serial Number: Shows the SFP serial number assigned by (e.g., 102201101).

Date Code: Shows the date this SFP module was made (e.g., 170915).

Temperature: Shows the current temperature of the SFP module (e.g., 27.13 C). 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: Shows the working DC voltage of the SFP module (e.g., 3.33 V). 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 SFP device documentation for more detail.

Mon1 (Bias) mA: Shows the Bias current of the SFP module (e.g., 6 mA). 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): Shows the transmit power of the SFP module (e.g., -2.30 dBm). 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): Shows the receiver power of the SFP module (e.g., none). Displays the measured received optical power in mW. Absolute accuracy is dependent upon the exact optical wavelength. For the vendor specified wavelength, accuracy should be better than 3dB over specified temperature and voltage. This accuracy should be maintained for input power levels up to the lesser of maximum transmitted or maximum received optical power per the appropriate standard. It should be maintained down to the minimum transmitted power minus cable plant loss (insertion loss or passive loss) per the appropriate standard. Absolute accuracy beyond this minimum required received input optical power range is vendor specific.

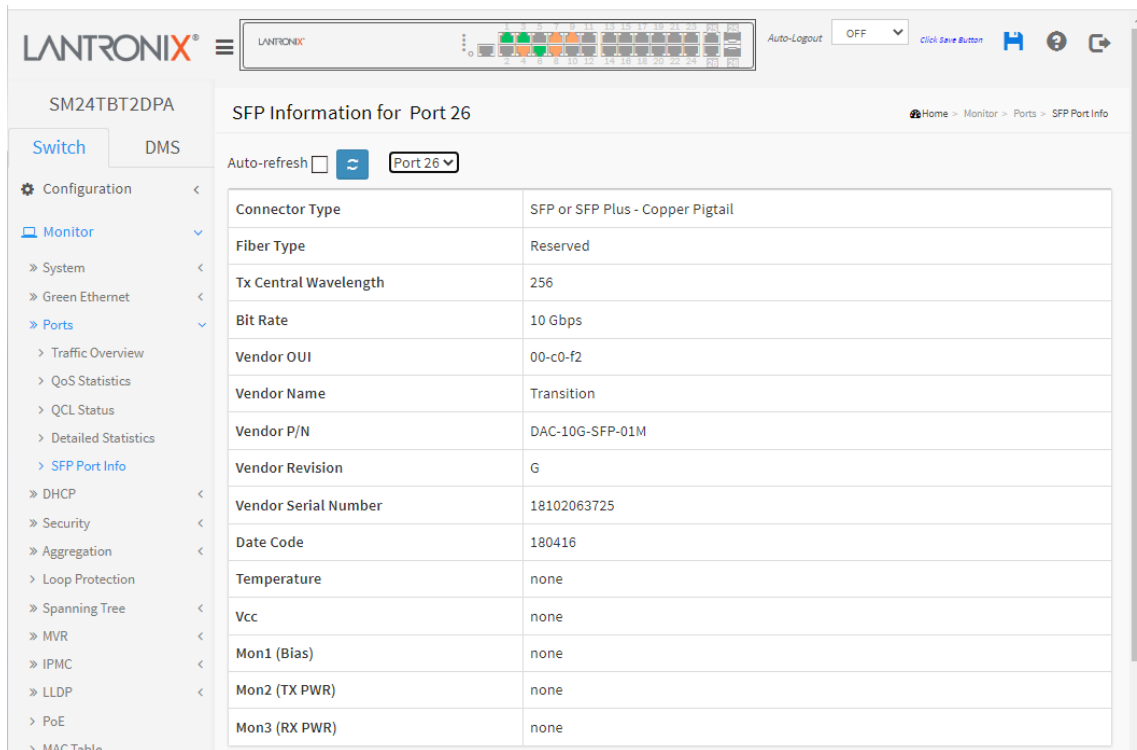
Buttons

Port 25 : The port select box determines which port is affected by clicking the buttons on a page.

Refresh: Click to refresh the page immediately. Any changes made locally will be undone.

Auto-refresh: Check this box to enable an automatic refresh of the page at regular intervals.

Example:



The screenshot shows the Lantronix web interface for the SM24TBT2DPA device. The main content area displays "SFP Information for Port 26". The interface includes a navigation menu on the left with options like Configuration, Monitor, and Ports. The SFP information is presented in a table with the following data:

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

3-4 DHCP

3-4.1 Server

A DHCP Server is used to allocate network addresses and deliver configuration parameters to dynamically configured hosts called DHCP clients.

3-4.1.1 Statistics

This page displays the database counters and the number of DHCP messages sent and received by a DHCP server. To display the DHCP Server Statistics in the Web UI:

1. Click Monitor, DHCP, Server, Statistics.
2. View the DHCP Server Statistics and use the buttons as needed.

Figure 3-4.1.1: DHCP Server Statistics page

The screenshot shows the DHCP Server Statistics page in the Lantronix Web UI. The page title is "DHCP Server Statistics" and the breadcrumb is "Home > Monitor > DHCP > Server > Statistics". The page includes an "Auto-refresh" checkbox and buttons for refresh and manual update. The data is presented in four tables:

Database Counters		
Pool	Excluded IP Address	Declined IP Address
1	0	0

Binding Counters		
Automatic Binding	Manual Binding	Expired Binding
3	0	5

DHCP Message Received Counters				
DISCOVER	REQUEST	DECLINE	RELEASE	INFORM
289	6834	0	0	482

DHCP Message Sent Counters		
OFFER	ACK	NAK
289	481	276

Parameter descriptions:

Database Counters

Pool: Number of pools.

Excluded IP Address: Number of excluded IP address ranges.

Declined IP Address: Number of declined IP addresses.

Binding Counters

Automatic Binding: Number of bindings with network-type pools.

Manual Binding: Number of bindings that administrator assigns an IP address to a client. That is, the pool is of host type.

Expired Binding: Number of bindings that their lease time expired or they are cleared from Automatic/Manual type bindings.

DHCP Message Received Counters

DISCOVER: Number of DHCP DISCOVER messages received.

REQUEST: Number of DHCP REQUEST messages received.

DECLINE: Number of DHCP DECLINE messages received.

RELEASE: Number of DHCP RELEASE messages received.

INFORM: Number of DHCP INFORM messages received.

DHCP Message Sent Counters

OFFER: Number of DHCP OFFER messages sent.

ACK: Number of DHCP ACK messages sent.

NAK: Number of DHCP NAK messages sent.

Buttons

Auto-refresh : Check this box to refresh the page automatically every 3 seconds.

Refresh: Click to manually refresh the page immediately.

Clear: Click to Clear DHCP Message Received Counters and DHCP Message Sent Counters.

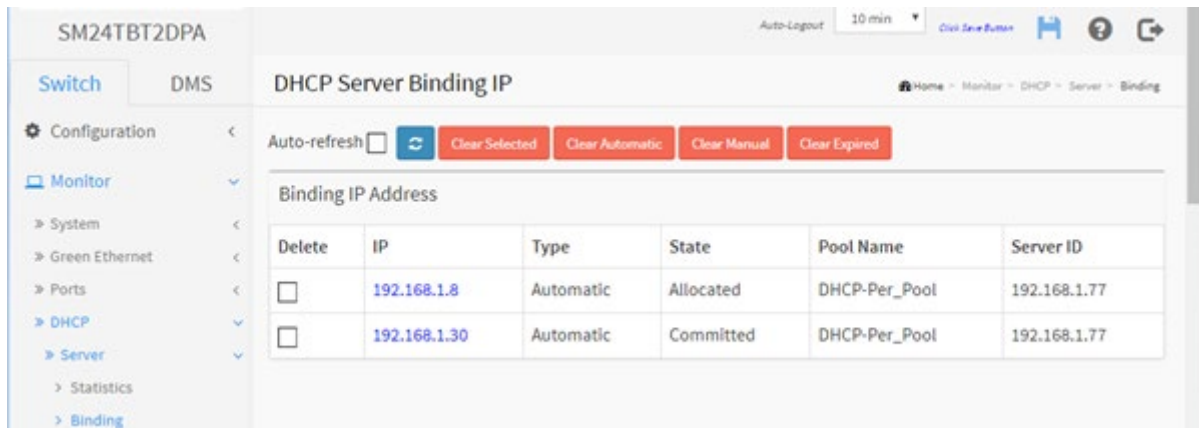
3-4.1.2 Binding

This page displays bindings generated for DHCP clients. A binding is a collection of configuration parameters, including at least an IP address, associated with or "bound to" a DHCP client. Bindings are managed by DHCP servers.

To display DHCP Server Binding IP in the web UI:

1. Click Monitor, DHCP, Server and Binding.
2. You can click a linked IP Address to display its DHCP Server Binding IP Data page.

Figure 3-4.1.2: DHCP Server Binding IP page



Parameter descriptions:

IP: The IP address allocated to DHCP client. Click a linked IP Address to display its DHCP Server Binding IP Data page. See example below.

Type: Type of binding. Possible types are Automatic, Manual, and Expired.

State: State of binding. Possible states are Committed, Allocated, and Expired.

Pool Name: The pool that generates the binding.

Server ID: Server IP address to service the binding.

Buttons

Clear Selected: Click to clear selected bindings. If the selected binding is Automatic or Manual, then it is changed to be Expired. If the selected binding is Expired, then it is freed.

Clear Automatic: Click to clear all Automatic bindings and Change them to Expired bindings.

Clear Manual: Click to clear all Manual bindings and Change them to Expired bindings.

Clear Expired: Click to clear all Expired bindings and free them.

Example: When you click a linked IP Address the DHCP Server Binding IP Data page displays:

Binding IP Data	
IP	172.27.195.3
Type	Automatic
State	Committed
Pool Name	DMS_dhcp_server
Server ID	172.27.195.140
VLAN	1
Subnet Mask	255.255.255.0
Client ID Type	MAC
Client ID Value	e8-eb-1b-cb-11-5f
MAC Address	e8-eb-1b-cb-11-5f
Lease Time	1 days 0 hours 0 minutes 0 seconds
Will Expired in	22 hours 18 minutes 56 seconds

Parameter descriptions:

Binding: Select a binding.

IP: Select IP address of the desired binding.

Binding IP Data: Displays data of the selected binding.

IP: Displays the IP address allocated to DHCP client.

Type: Displays the Type of binding. Possible types are Automatic, Manual, Expired.

State: Displays the State of binding. Possible states are Committed, Allocated, Expired.

Pool Name: Displays the pool that generated the binding.

Server ID: Displays the Server IP address to service the binding.

VLAN ID: Displays the VLAN ID of the interface where the DHCP client is from.

Subnet Mask: Displays the Netmask of the interface where the DHCP client is from.

Client ID Type: Displays the Type of client identifier in option 61 from DHCP client. Possible types are FQDN, MAC and -. If - is displayed, it means DHCP client does not pack option 61 in the DHCP message.

Client ID Value: Displays the Value of client identifier in option 61 from DHCP client.

MAC Address: Displays the Hardware address in *chaddr* of the DHCP message from DHCP client.

Lease Time: Displays the lease time of the binding.

Will Expired in: Displays the amount of time remaining until the binding will expire.

Buttons

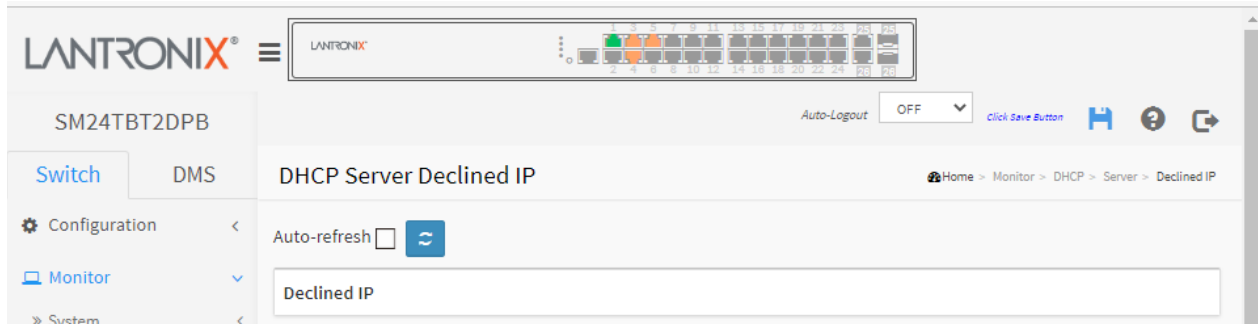
Auto-refresh: Check this box to refresh the page automatically every three seconds.

Refresh: Click to refresh the page immediately.

3-4.1.3 Declined IP

This page displays declined IP addresses. To display DHCP Server Declined IP in the web UI, click Monitor, DHCP, Server, and Declined IP.

Figure 3-4.1.3: DHCP Server Declined IP page



Parameter descriptions:

Declined IP: The IP address allocated to the DHCP client.

Buttons

Auto-refresh: Check this box to refresh the page automatically every three seconds.

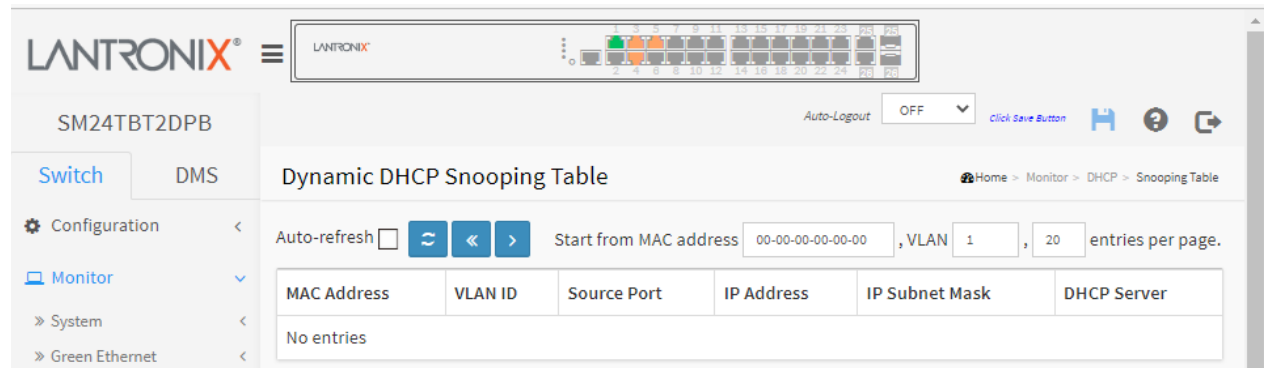
Refresh: Click to refresh the page immediately.

3-4.2 Snooping Table

This page displays the dynamic IP assigned information after DHCP Snooping mode is disabled. All DHCP clients obtained the dynamic IP address from the DHCP server will be listed in this table except for local VLAN interface IP addresses. Entries in the Dynamic DHCP Snooping Table are shown on this page.

To monitor DHCP Snooping in the web UI: click Monitor, DHCP, and Snooping Table.

Figure 3-4.2: Dynamic DHCP Snooping Table page



Parameter descriptions:

MAC Address: The user MAC address of the entry.

VLAN ID: The VLAN ID in which the DHCP traffic is permitted.

Source Port: Switch Port Number for which the entries are displayed.

IP Address: The User IP address of the entry.

IP Subnet Mask: The User IP subnet mask of the entry.

DHCP Server: The DHCP Server address of the entry.

Buttons

Auto-refresh: Check this box to refresh the page automatically every three seconds.

Refresh: Click to refresh the page immediately.

Clear: Flushes all dynamic entries.

<< : Updates the table starting from the first entry in the Dynamic DHCP snooping Table.

> : Updates the table, starting with the entry after the last entry currently displayed.

3-4.3 Relay Statistics

This page provides statistics for DHCP relay. To monitor DHCP Relay statistics in the web UI click Monitor, DHCP, Relay Statistics.

Figure 3-4.3: DHCP Relay Statistics page

The screenshot shows the Lantronix web interface for the SM24TBT2DPB device. The left sidebar contains a navigation menu with 'Monitor' selected, and 'DHCP' and 'Relay Statistics' also visible. The main content area displays 'DHCP Relay Statistics' with an 'Auto-refresh' checkbox and a refresh button. Below this are two tables: 'Server Statistics' and 'Client Statistics'. Both tables show zero values for all metrics.

Transmit to Server	Transmit Error	Receive from Server	Receive Missing Agent Option	Receive Missing Circuit ID	Receive Missing Remote ID	Receive Bad Circuit ID	Receive Bad Remote ID
0	0	0	0	0	0	0	0

Transmit to Client	Transmit Error	Receive from Client	Receive Agent Option	Replace Agent Option	Keep Agent Option	Drop Agent Option
0	0	0	0	0	0	0

Parameter descriptions:

Server Statistics

Transmit to Server: The number of packets that are relayed from client to server.

Transmit Error: The number of packets that resulted in errors while being sent to clients.

Receive from Server: The number of packets received from server.

Receive Missing Agent Option: The number of packets received without agent information options.

Receive Missing Circuit ID: The number of packets received with the Circuit ID option missing.

Receive Missing Remote ID: The number of packets received with the Remote ID option missing.

Receive Bad Circuit ID: The number of packets whose Circuit ID option did not match known circuit ID.

Receive Bad Remote ID: The number of packets whose Remote ID option did not match known Remote ID.

Client Statistics

Transmit to Client: The number of relayed packets from server to client.

Transmit Error: The number of packets that resulted in error while being sent to servers.

Receive from Client: The number of received packets from server.

Receive Agent Option: The number of received packets with relay agent information option.

Replace Agent Option: The number of packets which were replaced with relay agent information option.

Keep Agent Option: The number of packets whose relay agent information was retained.

Drop Agent Option: The number of packets 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 manually refresh the page immediately.

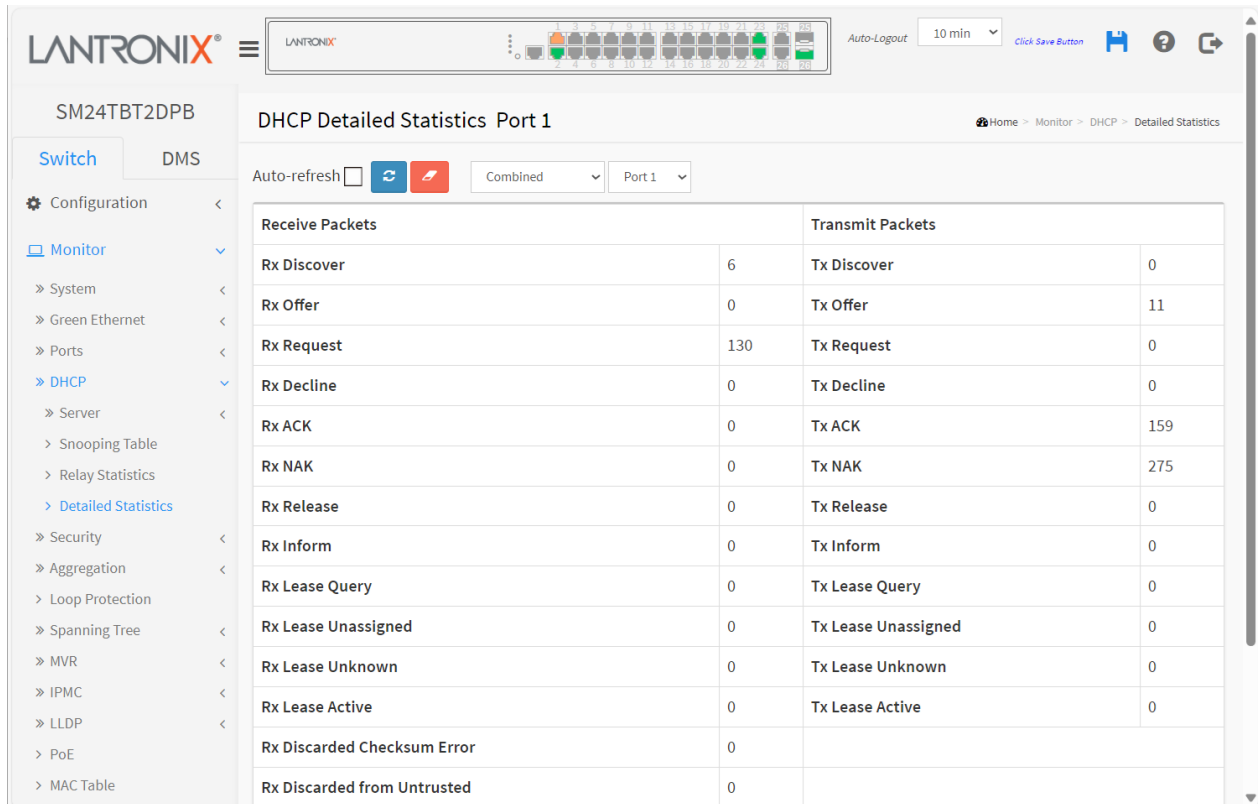
Clear: Clears all statistics.

3-4.4 Detailed Statistics

This page provides statistics for DHCP snooping. Note that the normal forward per-port TX statistics are not increased if the incoming DHCP packet is done by an L3 forwarding mechanism. Also, clearing the statistics on a specific port may not take effect on global statistics since it gathers statistics from a different layer.

To monitor DHCP detailed statistics in the web UI, click Monitor, DHCP, Detailed Statistics.

Figure 3-4.4: DHCP Detailed Statistics



Parameter descriptions:

Rx and Tx Discover: The number of discover (option 53 with value 1) packets received and transmitted.

Rx and Tx Offer: The number of offer (option 53 with value 2) packets received and transmitted.

Rx and Tx Request: The number of request (option 53 with value 3) packets received and transmitted.

Rx and Tx Decline: The number of decline (option 53 with value 4) packets received and transmitted.

Rx and Tx ACK: The number of ACK (option 53 with value 5) packets received and transmitted.

Rx and Tx NAK: The number of NAK (option 53 with value 6) packets received and transmitted.

Rx and Tx Release: The number of release (option 53 with value 7) packets received and transmitted.

Rx and Tx Inform: The number of inform (option 53 with value 8) packets received and transmitted.

Rx and Tx Lease Query: The number of lease query (option 53 with value 10) packets received and transmitted.

Rx and Tx Lease Unassigned: The number of lease unassigned (option 53 with value 11) packets received and transmitted.

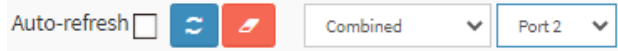
Rx and Tx Lease Unknown: The number of lease unknown (option 53 with value 12) packets received and transmitted.

Rx and Tx Lease Active: The number of lease active (option 53 with value 13) packets received and transmitted.

Rx Discarded checksum error: The number of discard packet that IP/UDP checksum is error.

Rx Discarded from Untrusted: The number of discarded packets that are coming from untrusted port.

Buttons



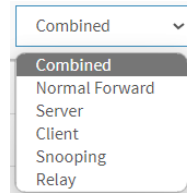
Auto-refresh : Check this box to refresh the page automatically every 3 seconds.

Refresh: Click to refresh the page immediately.

Clear: Clears the counters for the selected port.

Combined : The DHCP user select box determines which user is affected by clicking the buttons.

Port 1 : The port select box determines which port is affected by clicking the buttons.



3-5 Security

3-5.1 Access Management Statistics

This page displays detailed statistics of the Access Management including HTTP, HTTPS, SNMP, TELNET, and SSH.

To view Access Management Statistics in the web UI:

1. Click Monitor, Security, Access Management Statistics.
2. Check “Auto-refresh”.
3. Click “Refresh” to refresh the statistics or clear all information when you click “Clear”.

Figure 3-5.1: Access Management Statistics page

The screenshot shows the Lantronix web interface for the SM24TBT2DPA switch. The main content area is titled "Access Management Statistics". At the top of this section, there is an "Auto-refresh" checkbox which is currently unchecked, followed by a blue circular refresh icon and a red square clear icon. Below this is a table with the following data:

Interface	Received Packets	Allowed Packets	Discarded Packets
HTTP	0	0	0
HTTPS	0	0	0
SNMP	0	0	0
TELNET	0	0	0
SSH	0	0	0

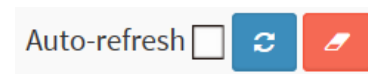
Parameter descriptions:

Interface: The interface type through which the remote host can access the switch.

Received Packets: Number of received packets from the interface when access management mode is enabled.

Allowed Packets: Number of allowed packets from the interface when access management mode is enabled.

Discarded Packets.: Number of discarded packets from the interface when access management mode is enabled.



Buttons

Auto-refresh: Check this box to refresh the page automatically every 3 seconds.

Refresh: Click to manually refresh the page immediately.

Clear: Clears the page statistics.

3-5.2 Network

3-5.2.1 Port Security

3-5.2.1.1 Switch

This page shows the Port Security Switch status. Port Security is a module with no direct configuration. Configuration comes indirectly from other modules - the user modules. When a user module has enabled port security on a port, the port is set-up for software-based learning. In this mode, frames from unknown MAC addresses are passed on to the port security module, which in turn asks all user modules whether to allow this new MAC address to forward or block it. For a MAC address to be set in the forwarding state, all enabled user modules must unanimously agree on allowing the MAC address to forward. If only one chooses to block it, it will be blocked until that user module decides otherwise.

The status page is divided into two sections - one with a legend of user modules and one with the actual port status.

Web Interface

To view Port Security Switch Status in the web UI:

1. Click Monitor, Security, Network, Port Security, Switch and view page parameters.
2. Check "Auto-refresh" or click "Refresh" to refresh the page.

Figure 3-5.2.1.1: Port Security Switch Status

The screenshot shows the web interface for SM24TBT2DPA. The page title is "Port Security Switch Status". The breadcrumb trail is "Home > Monitor > Security > Network > Port Security > Switch". The "Auto-refresh" checkbox is unchecked. The "User Module Legend" table is as follows:

User Module Name	Abbr
Limit Control	L
802.1X	8
Voice VLAN	V

The "Port Status" table is as follows:

Port	Users	State	MAC Count	
			Current	Limit
1	---	Disabled	-	-
2	--V*	Ready	0	-
3	--V*	Ready	1	-
4	--V*	Ready	0	-
5	--V*	Ready	1	-
6	--V*	Ready	0	-
7	---	Disabled	-	-

Parameter descriptions:

User Module Legend: The legend shows all user modules that may request Port Security services.

User Module Name: The full name of a module that may request Port Security services.

Abbr: A one-letter abbreviation of the user module. This is used in the Users column (described below).

Port Status: The table has one row for each port on the selected switch and several columns:

Port: The port number for which the status applies. Click the port number to see the status for this particular port.

Users: Each of the user modules has a column that shows whether that module has enabled Port Security or not. A '-' means that the corresponding user module is not enabled, whereas a letter indicates that the user module abbreviated by that letter has enabled port security. The abbreviations are: Limit Control = L, 802.1X = 8, and Voice VLAN = V.

State: Shows the current state of the port. It can take one of four values:

Disabled: No user modules are currently using the Port Security service.

Ready: The Port Security service is in use by at least one user module and is awaiting frames from unknown MAC addresses to arrive.

Limit Reached: The Port Security service is enabled by at least the Limit Control user module, and that module has indicated that the limit is reached, and no more MAC addresses should be taken in.

Shutdown: The Port Security service is enabled by at least the Limit Control user module, and that module has indicated that the limit is exceeded. No MAC addresses can be learned on the port until it is administratively re-opened on the Limit Control configuration Web-page.

MAC Count (Current, Limit): The two columns indicate the number of currently learned MAC addresses (forwarding as well as blocked) and the maximum number of MAC addresses that can be learned on the port, respectively.

If no user modules are enabled on the port, the Current column will show a dash (-).

If the Limit Control user module is not enabled on the port, the Limit column will show a dash (-).

Buttons

Auto-refresh: Check this box to refresh the page automatically every 3 seconds.

Refresh: Click to manually refresh the page immediately.

3-5.2.1.2 Port

This page displays the MAC addresses secured by the Port Security module. Port Security is a module with no direct configuration. Configuration comes indirectly from other modules - the user modules. When a user module has enabled port security on a port, the port is set-up for software-based learning. In this mode, frames from unknown MAC addresses are passed on to the port security module, which in turn asks all user modules whether to allow this new MAC address to forward or block it. For a MAC address to be set in the forwarding state, all enabled user modules must unanimously agree on allowing the MAC address to forward. If only one chooses to block it, it will be blocked until that user module decides otherwise.

To view Port Security Port Status in the web UI:

1. Click Monitor, Security, Network, Port Security, Port.
2. Specify the Port which you want to monitor.
3. Check "Auto-refresh" or click "Refresh" to refresh the port detailed statistics.

Figure 3-5.2.1.2: Port Security Port Status page

The screenshot shows the Lantronix web interface for the SM24TBT2DPB device. The main content area is titled "Port Security Port Status Port 1". It features an "Auto-refresh" checkbox (unchecked), a "Refresh" button (blue), a "Clear" button (red), and a port selection dropdown menu set to "Port 1". Below this is a "User Module Legend" table with the following data:

MAC Address	VLAN ID	State	Time of Addition	Age/Hold
5c-ff-35-dc-0a-c1	1	F	2011-01-01T00:44:25+00:00	-

Parameter descriptions:

MAC Address & VLAN ID: The MAC address and VLAN ID seen on this port. If no MAC addresses are learned, a single row stating "No MAC addresses attached" displays.

State: Indicates whether the corresponding MAC address is **B**locked or **F**orwarding. In the blocked state, it will not be allowed to transmit or receive traffic.

Time of Addition: Shows the date and time when this MAC address was first seen on the port.

Age/Hold: If at least one user module has decided to block this MAC address, it will stay in the blocked state until the hold time (measured in seconds) expires. If all user modules have decided to allow this MAC address to forward, and aging is enabled, the Port Security module will periodically check that this MAC address still forwards traffic. If the age period (measured in seconds) expires and no frames have been seen, the MAC address will be removed from the MAC table. Otherwise, a new age period will begin.

If aging is disabled or a user module has decided to hold the MAC address indefinitely, a dash (-) will be shown.



Buttons

Auto-refresh: Check this box to refresh the page automatically every 3 seconds.

Refresh: Click to refresh the page immediately.

Clear: Use the port select box to select which port to show status for.

3-5.2.2 NAS

3-5.2.2.1 Switch

This page displays port NAS status information of the switch. The status includes Admin State, Port State, Last Source, Last ID, QoS Class, and Port VLAN ID.

To view NAS Switch Status in the web UI:

1. Click Monitor, Security, Network, NAS, Port.
2. Check "Auto-refresh".
3. Click "Refresh" to refresh the port detailed statistics.

Figure 3-5.2.2.1: Network Access Server Switch Status page

The screenshot shows the Lantronix web interface for device SM24TBT2DPB. The navigation menu on the left includes Configuration, Monitor, System, Green Ethernet, Ports, DHCP, Security, Access Management, Statistics, Network, Port Security, NAS, Switch, and Port. The main content area is titled "Network Access Server Switch Status" and includes an "Auto-refresh" checkbox 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	Globally Disabled			-	
2	Force Authorized	Globally Disabled			-	
3	Force Authorized	Globally Disabled			-	
4	Force Authorized	Globally Disabled			-	
5	Force Authorized	Globally Disabled			-	
6	Force Authorized	Globally Disabled			-	
7	Force Authorized	Globally Disabled			-	
8	Force Authorized	Globally Disabled			-	
9	Force Authorized	Globally Disabled			-	

Parameter descriptions:

Port: The switch port number. Click to navigate to detailed NAS statistics for this port.

Admin State: The port's current administrative state. See section 2-5.1 Switch on page 45 for a description of possible values.

Port State: The current state of the port. Refer to NAS Port State for a description of the individual states.

Last Source: The source MAC address carried in the most recently received EAPOL frame for EAPOL-based authentication, and the most recently received frame from a new client for MAC-based authentication.

Last ID: The user name (supplicant identity) carried in the most recently received Response Identity EAPOL frame for EAPOL-based authentication, and the source MAC address from the most recently received frame from a new client for MAC-based authentication.

QoS Class: QoS Class assigned to the port by the RADIUS server if enabled.

Port VLAN ID: The VLAN ID that NAS has put the port in. The field is blank if the Port VLAN ID is not overridden by NAS.

If the VLAN ID is assigned by the RADIUS server, "(RADIUS-assigned)" is appended to the VLAN ID. See the online Help for more about RADIUS-assigned VLANs.

If the port is moved to the Guest VLAN, "(Guest)" is appended to the VLAN ID. See the online Help for more about Guest VLANs.

Buttons

Auto-refresh: Check this box to refresh the page automatically every 3 seconds.

Refresh: Click to manually refresh the page immediately.

3-5.2.2.2 Port

This page provides detailed NAS statistics for a specific switch port running EAPOL-based IEEE 802.1X authentication. For MAC-based ports, it shows selected backend server (RADIUS Authentication Server) statistics, only.

To view NAS Port Statistics in the web UI:

1. Click Monitor, Security, Network, NAS, and then Port.
2. At the Port select dropdown select the desired port.
3. Check "Auto-refresh" or click "Refresh" to refresh the port detailed statistics.

Figure 3-5.2.2.2: NAS Statistics page

The screenshot displays the 'NAS Statistics Port 1' page in the LANTRONIX web UI. The page title is 'NAS Statistics Port 1'. At the top, there is an 'Auto-logout' dropdown set to 'OFF' and a 'Clear' button. Below this, there is a 'Port 1' dropdown menu. The main content area is divided into two sections: 'Port State' and 'Port Counters'. The 'Port State' section shows 'Admin State' as 'Force Authorized' and 'Port State' as 'Authorized'. The 'Port Counters' section is divided into 'Receive EAPOL Counters' and 'Transmit EAPOL Counters', with various metrics like Total, Response ID, Requests, Start, Logoff, Invalid Type, and Invalid Length, all showing a value of 0.

Parameter descriptions:

Port State

Admin State: The port's current administrative state. Refer to NAS Admin State for a description of possible values.

Port State: The current state of the port. See section 2-5.1 Switch on page 45 for a description of possible values.

QoS Class: The QoS class assigned by the RADIUS server. The field is blank if no QoS class is assigned.

Port VLAN ID: The VLAN ID that NAS has put the port in. The field is blank if the Port VLAN ID is not overridden by NAS.

If the VLAN ID is assigned by the RADIUS server, "(RADIUS-assigned)" is appended to the VLAN ID. See the online Help for more about RADIUS-assigned VLANs here.

If the port is moved to the Guest VLAN, "(Guest)" is appended to the VLAN ID. See the online Help for more about Guest VLANs here.

Port Counters

EAPOL Counters: Supplicant frame counters are available for these administrative states: Force Authorized, Force Unauthorized, Port-based 802.1X, Single 802.1X, and 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	dot1xAuthEapolReqldFramesTx	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: Backend (RADIUS) frame counters are available for these administrative states: Port-based 802.1X, Single 802.1X, Multi 802.1X, and MAC-based Auth.

Direction	Name	IEEE Name	Description
Rx	Access Challenges	dot1xAuthBackendAccessChallenges	<p>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.</p> <p>MAC-based: Counts all Access Challenges received from the backend server for this port (left-most table) or client (right-most table).</p>
Rx	Other Requests	dot1xAuthBackendOtherRequestsToSupplicant	<p>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.</p> <p>MAC-based: Not applicable.</p>
Rx	Auth. Successes	dot1xAuthBackendAuthSuccesses	<p>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.</p>
Rx	Auth. Failures	dot1xAuthBackendAuthFails	<p>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.</p>
Tx	Responses	dot1xAuthBackendResponses	<p>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.</p> <p>MAC-based: Counts all the</p>

			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, and MAC-based Auth.

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 and MAC-based Auth.

The table is identical to and is placed next to the Port Counters table and will be empty if no MAC address is currently selected. To populate the table, select one of the attached MAC Addresses from the table.

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).

Auto-refresh  Clear  Port 1 

Buttons

Auto-refresh: Check this box to refresh the page automatically every 3 seconds.

Refresh: Click to refresh the page immediately.

Clear: This button is available in the following modes:

- Force Authorized
- Force Unauthorized
- Port-based 802.1X
- Single 802.1X

Clear All: Click to clear the counters for the selected port. This button is available in these modes:

- Multi 802.1X
- MAC-based Auth.X

Clear This: Click to clear both the port counters and all of the attached client's counters. The "Last Client" will not be cleared, however. This button is available in these modes:

- Multi 802.1X
- MAC-based Auth.X

Click to clear only the currently selected client's counters.

3-5.2.3 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 256 on each switch. To display the ACL status in the web UI:

1. Click Monitor, Security, Network, ACL Status.
2. At the User select dropdown select a user.
3. Check the “Auto-refresh” checkbox or click “Refresh” to refresh the ACL Status.

Figure 3-5.2.3: ACL Status page

The screenshot shows the Lantronix web interface for the SM24TBT2DPB device. The 'ACL Status' page is active, showing 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 entries are as follows:

User	ACE	Ingress Port	Frame Type	Action	Rate Limiter	Port Redirect	Mirror	CPU	CPU Once	Counter	Conflict
DMS mDNS	1	All	IPv4/UDP 5353	Permit	Disabled	Disabled	Disabled	Yes	No	5557	No
DMS Onvif	1	All	IPv4/UDP 10100-10107	Permit	Disabled	Disabled	Disabled	Yes	No	3960	No
DMS SSDP	1	All	IPv4/UDP 1900	Permit	Disabled	Disabled	Disabled	Yes	No	598	No
DMS CLIENT	1	All	IPv4/UDP 10012	Permit	Disabled	Disabled	Disabled	Yes	No	16	No
DHCP	1	All	IPv4/UDP 67 DHCP Client	Deny	Disabled	Disabled	Disabled	Yes	No	2881	No
DHCP	2	All	IPv4/UDP 68 DHCP Server	Deny	Disabled	Disabled	Disabled	Yes	No	0	No

Parameter descriptions:

User: Dropdown to select the ACL user (e.g., Static, IPMC, DMS CLIENT, mDNS, DMS [Onvif](#), DMS SSDP, DHCP, Loop Protect, or ARP Inspection).

Ingress Port: Indicates the ingress port of the ACE. Possible values are:

All: The ACE will match any ingress port.

Port: The ACE will match a specific ingress port.

Frame Type: Indicates the frame type of the ACE. Possible values are:

Any: The ACE will match any frame type.

EType: The ACE will match Ethernet Type frames. Note that an Ethernet Type based ACE will not get matched by IP and ARP frames.

ARP: The ACE will match ARP/RARP frames.

IPv4: The ACE will match all IPv4 frames.

IPv4: The ACE will match all IPv4 frames.

IPv4/ICMP: The ACE will match IPv4 frames with ICMP protocol.

IPv4/UDP: The ACE will match IPv4 frames with UDP protocol.

IPv4/TCP: The ACE will match IPv4 frames with TCP protocol.

IPv4/Other: The ACE will match IPv4 frames, which are not ICMP / UDP / TCP.

IPv6: The ACE will match all IPv6 standard frames.

Action: Indicates the forwarding action of the ACE.

Permit: Frames matching the ACE may be forwarded and learned.

Deny: Frames matching the ACE are dropped.

Filter: Frames matching the ACE are filtered.

Rate Limiter: Indicates the rate limiter number of the ACE. The allowed range is 1 to 16. When Disabled is displayed, the rate limiter operation is disabled.

Port Redirect: Indicates the port copy operation of the ACE. Frames matching the ACE are copied to the port number. The allowed values are Disabled or a specific port number. When Disabled displays, the port copy operation 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. It is a conflict if a specific ACE is not applied to the hardware due to hardware limitations.

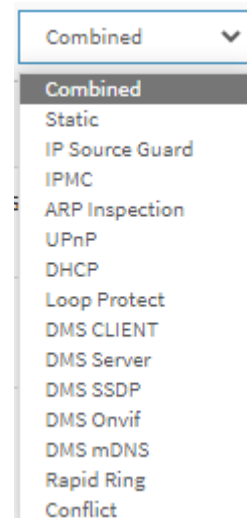
Buttons



Auto-refresh: Check this box to refresh the page automatically every 3 seconds.

Refresh: Click to refresh the page immediately.

User select box: determines which ACL user's statistics are displayed on this page.



3-5.2.4 ARP Inspection

This page displays the Dynamic ARP Inspection Table parameters. The Dynamic ARP Inspection Table contains up to 1024 entries, and is sorted first by port, then by VLAN ID, then by MAC address, and then by IP address.

Each page shows up to 99 entries from the Dynamic ARP Inspection table, default being 20, selected through the "entries per page" input field. When first visited, the web page will show the first 20 entries from the beginning of the Dynamic ARP Inspection Table.

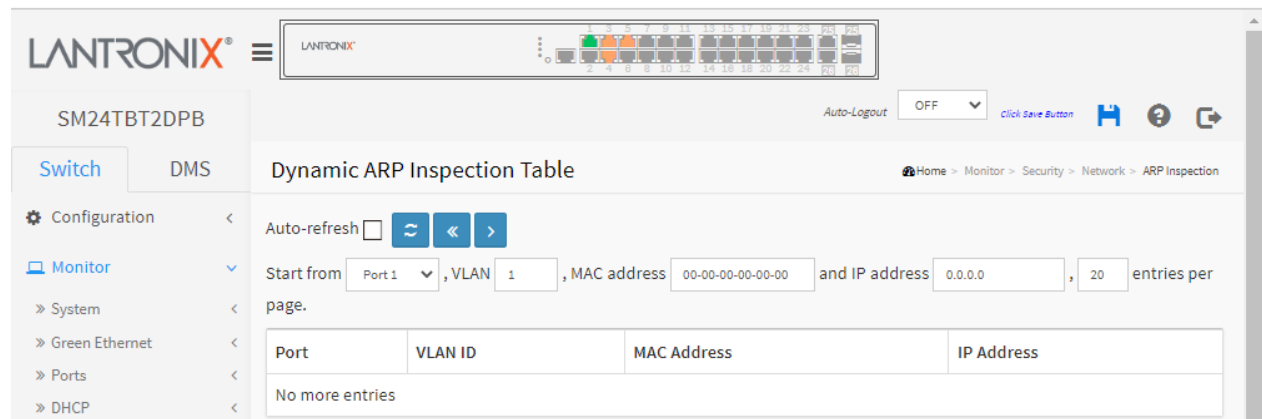
The "Start from port address", "VLAN", "MAC address" and "IP address" input fields let you select the starting point in the Dynamic ARP Inspection Table. Clicking the Refresh button will update the displayed table starting from that or the closest next Dynamic ARP Inspection Table match. In addition, the two input fields will - upon a Refresh button click - assume the value of the first displayed entry, allowing for continuous refresh with the same start address.

Clicking the Next entry 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" displays in the table. Use the Refresh button to start over.

To view the Dynamic ARP Inspection Table in the web UI:

1. Click Monitor, Security, Network, ARP Inspection.
2. Check "Auto-refresh".
3. Click "Refresh" to refresh the port detailed statistics.
4. Specify the Start from port, VLAN ID, MAC Address, IP Address, and entries per page.

Figure 3-5.2.4: Dynamic ARP Inspection Table page



Parameter descriptions:

Port: Switch Port Number for which the entries are displayed.

VLAN ID: VLAN-ID in which the ARP traffic is permitted.

MAC Address: User MAC address of the entry.

IP Address: User IP address of the entry.

Buttons

Auto-refresh: Check this box to refresh the page automatically every 3 seconds.

Refresh: Click to refresh the page immediately.

<<: Updates the system log entries to the first available entry ID.

>: Updates the system log entry to the next available entry ID.

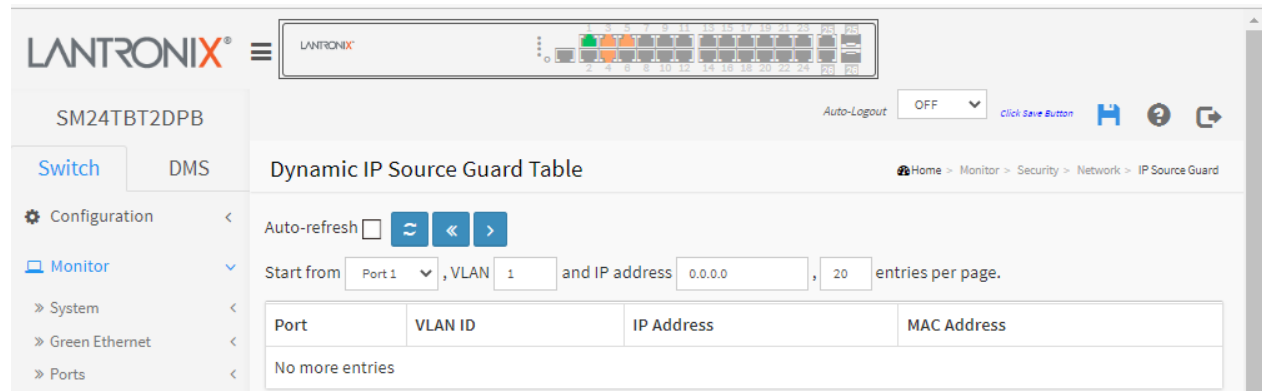
3-5.2.5 IP Source Guard

Entries in the Dynamic IP Source Guard Table are shown on this page. The Dynamic IP Source Guard Table is sorted first by port, then by VLAN ID, then by IP address, and then by MAC address.

To view the Dynamic IP Source Guard Table in the web UI:

1. Click Monitor, Security, Network, IP Source Guard.
2. Check “Auto-refresh” to refresh the page automatically or click “Refresh” to refresh the port immediately.
3. Specify the Start from port, VLAN ID, IP Address, and entries per page.

Figure 3-5.2.5: Dynamic IP Source Guard Table page



Parameter descriptions:

Port: Switch Port Number for which the entries are displayed.

VLAN ID: VLAN-ID in which the IP traffic is permitted.

IP Address: User IP address of the entry.

MAC Address: Source MAC address.



Buttons

Auto-refresh: Check this box to refresh the page automatically every 3 seconds.

Refresh: Click to refresh the page immediately.

<<: Updates the system log entries to the first available entry ID.

>: Updates the system log entry to the next available entry ID.

3-5.3 AAA

3-5.3.1 RADIUS Overview

This page displays an overview of the RADIUS Authentication and Accounting servers' status.

To view RADIUS server status in the web UI:

1. Click Monitor, Security, AAA, RADIUS Overview.
2. Check "Auto-refresh" or click "Refresh" to refresh the statistics.

Figure 3-5.3.1: RADIUS Server Status Overview page

The screenshot shows the Lantronix web interface for device SM24TBT2DPB. The main content area is titled 'RADIUS Server Status Overview' and contains two sections:

RADIUS Authentication Server Status Overview

#	IP Address	Status
1	0.0.0.0:0	Disabled
2	0.0.0.0:0	Disabled
3	0.0.0.0:0	Disabled
4	0.0.0.0:0	Disabled
5	0.0.0.0:0	Disabled

RADIUS Accounting Server Status Overview

#	IP Address	Status
1	0.0.0.0:0	Disabled
2	0.0.0.0:0	Disabled
3	0.0.0.0:0	Disabled
4	0.0.0.0:0	Disabled
5	0.0.0.0:0	Disabled

Parameter descriptions: for the RADIUS Authentication Server and the Accounting Server:

#: The RADIUS server number. Click to navigate to detailed statistics for this server.

IP Address: The IP address and UDP port number (in <IP Address>:<UDP Port> notation) of this server.

Status: The current state of the server. This field takes one of these values:

Disabled: The server is disabled.

Not Ready: The server is enabled, but IP communication is not yet up and running.

Ready: The server is enabled, IP communication is up and running, and the RADIUS module is ready to accept access attempts.

Dead (X seconds left): Access attempts were made to this server, but it did not reply within the configured timeout. The server has temporarily been disabled but will get re-enabled when the dead-time expires. The number of seconds left before this occurs is displayed in parentheses.

This state is only reachable when more than one server is enabled.

3-5.3.2 RADIUS Details

This page displays detailed statistics for a particular RADIUS server. These statistics map closely to those specified in [RFC4668 - RADIUS Authentication Client MIB](#).

To display RADIUS Authentication Statistics in the web UI:

1. Click Monitor, Security, AAA, RADIUS Overview.
2. At the dropdown select the Server # to view.
3. Check Auto-refresh or click Refresh to refresh the statistics or click Clear to clear all statistics.

Figure 3-5.3.2: RADIUS Authentication Status page

The screenshot shows the web UI for SM24TBT2DPA. The left sidebar contains a navigation menu with 'Monitor' expanded to 'Security' > 'AAA' > 'RADIUS Overview'. The main content area is titled 'RADIUS Server Status Overview' and contains two tables:

RADIUS Authentication Server Status Overview		
#	IP Address	Status
1	0.0.0.0:1812	Ready
2	0.0.0.0:1645	Ready
3	0.0.0.0:1812	Ready
4	1.2.3.4:1812	Ready
5	0.0.0.0:0	Disabled

RADIUS Accounting Server Status Overview		
#	IP Address	Status
1	0.0.0.0:1813	Ready
2	0.0.0.0:1646	Ready
3	0.0.0.0:1813	Ready
4	1.2.3.4:1813	Ready
5	0.0.0.0:0	Disabled

Parameter descriptions:

RADIUS Authentication Statistics

The status map closely to those specified in RFC4668 - RADIUS Authentication Client MIB. You can click a linked instance number to display its details.

Packet Counters

RADIUS authentication server packet counter. There are seven receive and four transmit counters.

Direction	Name	RFC4668 Name	Description
Rx	Access Accepts	radiusAuthClientExtAccess Accepts	The number of RADIUS Access-Accept packets (valid or invalid) received from the server.
Rx	Access Rejects	radiusAuthClientExtAccess Rejects	The number of RADIUS Access-Reject packets (valid or invalid) received from the server.
Rx	Access Challenges	radiusAuthClientExtAccess Challenges	The number of RADIUS Access-Challenge packets (valid or invalid) received from the server.
Rx	Malformed Access Responses	radiusAuthClientExtMalformed AccessResponses	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	radiusAuthClientExtBad Authenticators	The number of RADIUS Access-Response packets containing invalid authenticators or Message Authenticator attributes received from the server.
Rx	Unknown Types	radiusAuthClientExt UnknownTypes	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	radiusAuthClientExtAccess Requests	The number of RADIUS Access-Request packets sent to the server. This does not include retransmissions.
Tx	Access Retransmissions	radiusAuthClientExtAccess Retransmissions	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	radiusAuthClientExt 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.

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: Disabled: The selected server is disabled. Not Ready: The server is enabled, but IP communication is not yet up and running. Ready: The server is enabled, IP communication is up and running, and the RADIUS module is ready to accept access attempts. Dead (X seconds left): Access attempts were made to this server, but it did not reply within the configured timeout. The server has temporarily been disabled but will get re-enabled when the dead-time expires. The number of seconds left before this occurs is displayed in parentheses. This state is only reachable when more than one server is enabled.
Round-Trip Time	radiusAuthClientExtRoundTripTime	The time interval (measured in milliseconds) between the most recent Access-Reply/Access-Challenge and the Access-Request that matched it from the RADIUS authentication server. The granularity of this measurement is 100 ms. A value of 0 ms indicates that there hasn't been round-trip communication with the server yet.

RADIUS Accounting Statistics

The statistics map closely to those specified in RFC4670 - RADIUS Accounting Client MIB. Use the server select box to switch between the backend servers to show details for.

Packet Counters

RADIUS accounting server packet counter. There are five receive and four transmit counters.

Direction	Name	RFC4670 Name	Description
Rx	Responses	radiusAccClientExtResponses	The number of RADIUS packets (valid or invalid) received from the server.
Rx	Malformed Responses	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	Bad Authenticators	radiusAccClientExtBadAuthenticators	The number of RADIUS packets containing invalid authenticators received from the server.
Rx	Unknown Types	radiusAccClientExtUnknownTypes	The number of RADIUS packets of unknown types that were received from the server on the accounting port.
Rx	Packets Dropped	radiusAccClientExtPacketsDropped	The number of RADIUS packets that were received from the server on the accounting port and dropped for some other reason.
Tx	Requests	radiusAccClientExtRequests	The number of RADIUS packets sent to the server. This does not include retransmissions.
Tx	Retransmissions	radiusAccClientExtRetransmissions	The number of RADIUS packets retransmitted to the RADIUS accounting server.
Tx	Pending Requests	radiusAccClientExtPendingRequests	The number of RADIUS packets destined for the server that have not yet timed out or received a response. This variable is incremented when a Request is sent and decremented due to receipt of a Response, timeout, or retransmission.
Tx	Timeouts	radiusAccClientExtTimeouts	The number of accounting timeouts to the server. After a timeout, the client may retry to the same server, send to a different server, or give up. A retry to the same server is counted as a retransmit as well as a timeout. A send to a different server is counted as a Request as well as a timeout.

Other Info

This section contains information about the state of the server and the latest round-trip time.

Name	RFC4670 Name	Description
IP Address	--	IP address and UDP port for the accounting server in question.
State	--	Shows the state of the server. It takes one of the following values: Disabled: The selected server is disabled. Not Ready: The server is enabled, but IP communication is not yet up and running. Ready: The server is enabled, IP communication is up and running, and the RADIUS module is ready to accept accounting attempts. Dead (X seconds left): Accounting attempts were made to this server, but it did not reply within the configured timeout. The server has temporarily been disabled but will get re-enabled when the dead-time expires. The number of seconds left before this occurs is displayed in parentheses. This state is only reachable when more than one server is enabled.
Round-Trip Time	radiusAccClientExtRoundTripTime	The time interval (measured in milliseconds) between the most recent Response and the Request that matched it from the RADIUS accounting server. The granularity of this measurement is 100 ms. A value of 0 ms indicates that there hasn't been round-trip communication with the server yet.

Buttons:

Auto-refresh –Check this box to enable an automatic refresh of the page at regular intervals.

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.

3-5.4 Switch

3-5.4.1 RMON

3-5.4.1.1 Statistics

This page displays an overview of RMON Statistics entries. Each page shows up to 99 entries from the Statistics table, default being 20, selected through the "entries per page" input field. When first visited, the web page will show the first 20 entries from the beginning of the Statistics table. The first displayed will be the one with the lowest ID found in the Statistics table.

The "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.

Clicking 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 << button to start over.

Web Interface

To display RMON Statistics in the web UI:

1. Click Monitor, Security, Switch, RMON, Statistics.
2. Specify "Start from Control Index" and "entries per page".
3. Check "Auto-refresh" or click "Refresh" to refresh the page.

Figure 3-5.4.1.1: RMON Statistics Status Overview page

Data Source ID	Drop	Octets	Pkts	Broadcast	Multicast	CRC Errors	Under-size	Over-size	Frag.	Jabb.	Coll.	Bytes	64	65	128	256	512	1024
1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
2	256	48011126	74335	8174	145	0	0	0	0	0	0	16379	66	0	32917	0	24973	

Parameter descriptions:

ID: Indicates the index of Statistics entry.

Data Source(if Index): The port ID which wants to be monitored.

Drop: The total number of events in which packets were dropped by the probe due to lack of resources.

Octets: The total number of octets of data (including those in bad packets) received on the network.

Pkts: The total number of packets (including bad packets, broadcast packets, and multicast packets) received.

Broad-cast: The total number of good packets received that were directed to the broadcast address.

Multi-cast: The total number of good packets received that were directed to a multicast address.

CRC Errors: The total number of packets received that had a length (excluding framing bits, but including FCS octets) of between 64 and 1518 octets, inclusive, but had either a bad Frame Check Sequence (FCS) with an integral number of octets (FCS Error) or a bad FCS with a non-integral number of octets (Alignment Error).

Under-size: The total number of packets received that were less than 64 octets.

Over-size: The total number of packets received that were longer than 1518 octets.

Frag.: The number of frames less than 64 octets received with invalid CRC.

Jabb.: The number of frames 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 long.

65~127: The total number of packets (including bad packets) received that were 65 - 127 octets long.

128~255: The total number of packets (including bad packets) received that were 128 - 255 octets long.

256~511: The total number of packets (including bad packets) received that were 256 - 511 octets long.

512~1023: The total number of packets (including bad packets) received that were 512 - 1023 octets long.

1024~1588: The total number of packets (including bad packets) received that were 1024 - 1588 octets long.

Buttons



Auto-refresh: Check this box to refresh the page automatically every 3 seconds.

Refresh: Click to manually refresh the page immediately.

<< : Updates the table starting from the first entry in the Statistics table (i.e., the entry with the lowest ID).

> : Updates the table, starting with the entry after the last entry currently displayed.

3-5.4.1.2 History

This page displays an overview of RMON History entries. Each page shows up to 99 entries from the History table, default being 20, selected through the "entries per page" input field. When first visited, the web page will show the first 20 entries from the beginning of the History table. The first displayed will be the one with the lowest History Index and Sample Index found in the History table.

The "Start from History Index" and "Sample Index" let you select the starting point in the History table.

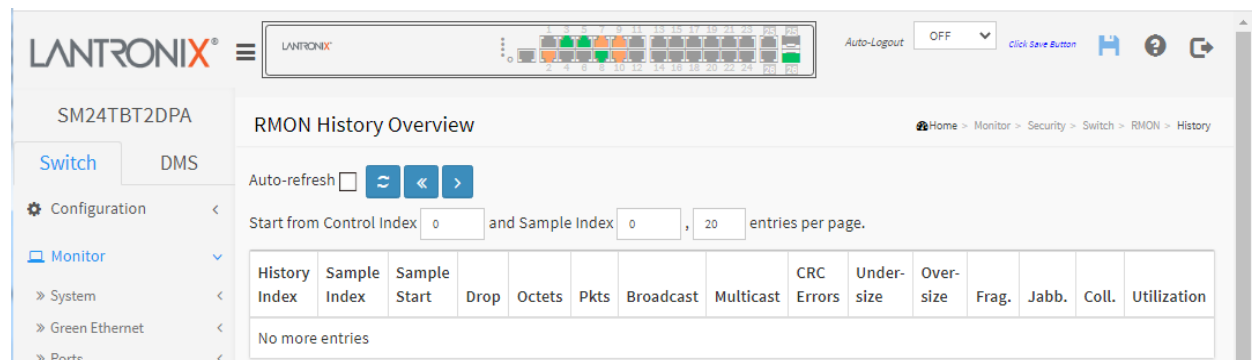
The Last Entry (>) button will use the last entry of the currently displayed entry as a basis for the next lookup. When the end is reached the text "No more entries" is shown in the displayed table. Use the << button to start over.

Web Interface

To view RMON history in the web UI:

1. Click Monitor, Security, Switch, RMON, History.
2. Specify "Start from Control index" and "Sample Index".
3. Check "Auto-refresh".
4. Click "Refresh" to refresh the statistics or clear all information when you click "Clear".

Figure 3-5.4.1.2: RMON History Overview page



Parameter descriptions:

History Index: Indicates the index of History control entry.

Sample Index: Indicates the index of the data entry associated with the control entry.

Sample Start: The value of *sysUpTime* at the start of the interval over which this sample was measured.

Drop: The total number of events in which packets were dropped by the probe due to lack of resources.

Octets: The total number of octets of data (including those in bad packets) received on the network.

Pkts: The total number of packets (including bad packets, broadcast packets, and multicast packets) received.

Broadcast: The total number of good packets received that were directed to the broadcast address.

Multicast: The total number of good packets received that were directed to a multicast address.

CRC Errors: The total number of packets received that had a length (excluding framing bits, but including FCS octets) of between 64 and 1518 octets, inclusive, but had either a bad Frame Check Sequence (FCS) with an integral number of octets (FCS Error) or a bad FCS with a non-integral number of octets (Alignment Error).

Undersize: The total number of packets received that were less than 64 octets.

Oversize: The total number of packets received that were longer than 1518 octets.

Frag.: The number of frames which size is less than 64 octets received with invalid CRC.

Jabb.: The number of frames which size is larger than 64 octets received with invalid CRC.

Coll.: The best estimate of the total number of collisions on this Ethernet segment.

Utilization: The best estimate of the mean physical layer network utilization on this interface during this sampling interval, in hundredths of a percent.

Buttons



Auto-refresh: Check this box to refresh the page automatically every 3 seconds.

Refresh: Click to refresh the page immediately.

<<: Updates the table starting from the first entry in the History table (i.e., the entry with the lowest History Index and Sample Index).

> : Updates the table, starting with the entry after the last entry currently displayed.

3-5.4.1.3 Alarm

This page displays 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.

Clicking the Refresh button will update the displayed table starting from that or the next closest Alarm table match.

The Last 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 << button to start over.

Web Interface

To monitor an RMON Alarm Overview in the web UI:

1. Click Monitor, Security, Switch, RMON, Alarm.
2. Check "Auto-refresh".
3. Click "Refresh" to refresh the port detailed statistics.

Figure 3-5.4.1.3: RMON Alarm Overview page

The screenshot shows the RMON Alarm Overview page in the web UI. The page title is "SM24TBT2DPA" and the breadcrumb trail is "Home > Monitor > Security > Switch > RMON > Alarm". The page includes a navigation menu on the left with options like Configuration, Monitor, System, Green Ethernet, Ports, and DHCP. The main content area shows the "RMON Alarm Overview" section with an "Auto-refresh" checkbox and buttons for navigation. Below this is a table with the following data:

ID	Interval	Variable	Sample Type	Value	Startup Alarm	Rising Threshold	Rising Index	Falling Threshold	Falling Index
1	30	.1.3.6.1.2.1.2.2.1.10.10	Delta	64929665	RisingOrFalling	7	8	6	5

Parameter descriptions:

ID: Indicates the index of Alarm control entry.

Interval: Indicates the interval in seconds for sampling and comparing the rising and falling threshold.

Variable: Indicates the particular variable to be sampled

Sample Type: The method of sampling the selected variable and calculating the value to be compared against the thresholds.

Value: The value of the statistic during the last sampling period.

Startup Alarm: The alarm that may be sent when this entry is first set to valid.

Rising Threshold: Rising threshold value.

Rising Index: Rising event index.

Falling Threshold: Falling threshold value.

Falling Index: Falling event index.

Buttons



Auto-refresh: Check this box to refresh the page automatically every 3 seconds.

Refresh: Click to refresh the page immediately.

<<: Updates the table starting from the first entry in the Alarm Table (i.e., the entry with the lowest ID).

>: Updates the table, starting with the entry after the last entry currently displayed.

3-5.4.1.4 Event

This page displays an overview of RMON Event table entries. Each page shows up to 99 entries from the Event table, default being 20, selected through the "entries per page" input field. When first visited, the web page will show the first 20 entries from the beginning of the Event table. The first displayed will be the one with the lowest Event Index and Log Index found in the Event table .

The "Start from Control Index and Sample Index" lets you select the starting point in the Event table. Clicking the Refresh button will update the displayed table starting from that or the next closest Event table match.

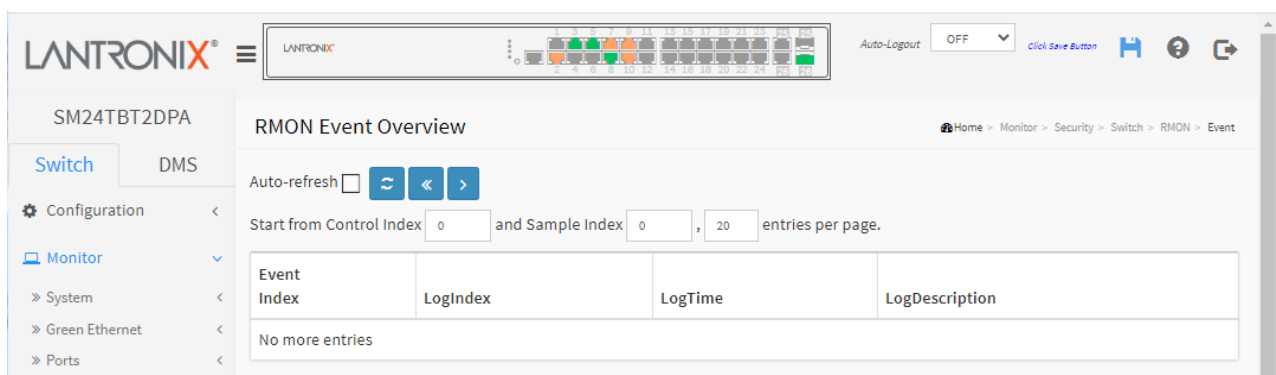
The >> button will use the last entry of the currently displayed entry as a basis for the next lookup. When the end is reached the text "No more entries" is shown in the displayed table. Use the << button to start over.

Web Interface

To monitor RMON Events in the web UI:

1. Click Monitor, Security, Switch, RMON, Event.
2. Specify "Start from Control Index ", "Sample Index", and "entries per page.".
3. Check "Auto-refresh" or click " Refresh" to refresh the port detailed statistics

Figure 3-5.4.1.4: RMON Event Overview page



Parameter descriptions:

Event Index: Indicates the index of the event entry.

Log Index: Indicates the index of the log entry.

LogTime: Indicates Event log time

LogDescription: Indicates the Event description.

Buttons



Auto-refresh: Check this box to refresh the page automatically every 3 seconds.

Refresh: Click to manually refresh the page immediately.

<< : Updates the table starting from the first entry in the Event Table (i.e., the entry with the lowest Event Index and Log Index).

> : Updates the table, starting with the entry after the last entry currently displayed.

3-6 Aggregation

3-6.1 Aggregation Status

This page displays a status overview for all aggregation group ports.

To display LACP Aggregation Status in the web UI:

1. Click Monitor, Aggregation, Status.
2. Check "Auto-refresh".
3. Click "Refresh" to refresh the port detailed statistics.

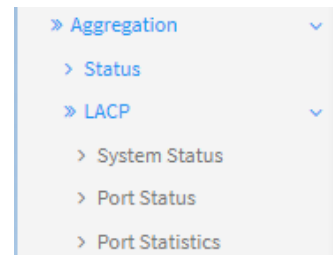


Figure 3-6.1 LACP Aggregation Status page

Aggr ID	Name	Type	Speed	Configured Ports	Aggregated Ports	Aggregated Bandwidth
1	LLAG1	Static	100M	GigabitEthernet 1/4-5	none	none
2	LLAG2	Static	1G	GigabitEthernet 1/6-8,10	GigabitEthernet 1/6-7	2G
3	LLAG3	Static	Undefined	GigabitEthernet 1/11-13	none	none
4	LLAG4	Static	Undefined	GigabitEthernet 1/14-15	none	none
6	LLAG6	Static	Undefined	GigabitEthernet 1/16-17	none	none
7	LLAG7	Static	Undefined	GigabitEthernet 1/18-20	none	none

Parameter descriptions:

Aggr ID: The Aggregation ID associated with this aggregation instance.

Name: Name of the Aggregation group ID (e.g., LLAG1).

Type: Type of the Aggregation group (Static or LACP).

Speed: Speed of the Aggregation group (e.g., 100M, 1G, undefined).

Configured Ports: Configured member ports of the Aggregation group (e.g., GigabitEthernet 1/4-5).

Aggregated Ports: Aggregated member ports of the Aggregation group (e.g., GigabitEthernet 1/6-7).

Aggregated Bandwidth: Aggregated Bandwidth of the Aggregation group (e.g., none or 2G).

Buttons

Auto-refresh: Check this box to refresh the page automatically every 3 seconds.

Refresh: Click to manually refresh the page immediately.

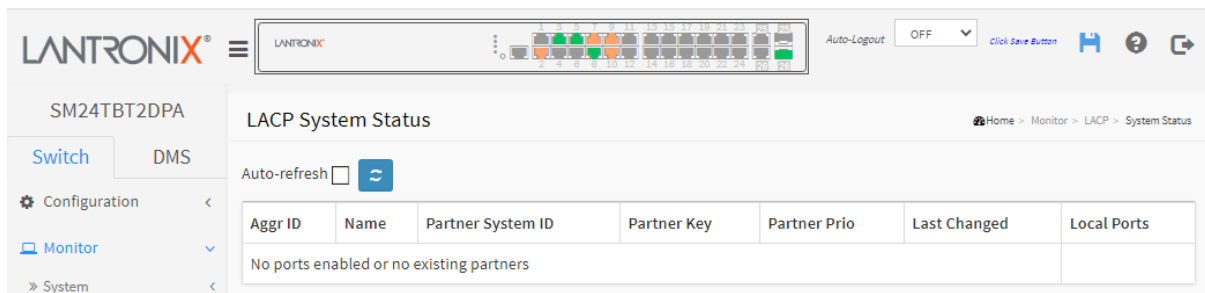
3-6.2 LACP System Status

This page displays a status overview for LACP status for all ports/partners.

To display LACP System status in the web UI:

1. Click Monitor, Aggregation, LACP, System Status.
2. To automatically refresh the information, check the “Auto-refresh” checkbox.
3. Click “Refresh” to refresh the LACP System Status.

Figure 3-6.2: LACP System Status page



Parameter descriptions:

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 of this partner.

Last Changed : The time since this aggregation changed.

Local Ports : Shows which ports are a part of this aggregation for this switch.

Buttons

Auto-refresh: Check this box to refresh the page automatically every 3 seconds.

Refresh: Click to refresh the page immediately.

3-6.3 LACP Port Status

This page displays an overview for LACP status for all ports. To display LACP Port status via the Web UI:

1. Click Monitor, Aggregation, LACP, Port Status.
2. To auto-refresh the page check the “Auto refresh” checkbox.
3. Click “Refresh” to refresh the LACP ports’ status.

Figure 3-6.3: LACP Status page

Port	LACP	Key	Aggr ID	Partner System ID	Partner Port	Partner Prio
1	No	-	-	-	-	-
2	Yes	4	-	-	-	-
3	Yes	4	-	-	-	-
4	Yes	2	-	-	-	-
5	No	-	-	-	-	-
6	Yes	3	-	-	-	-
7	Yes	3	-	-	-	-
8	No	-	-	-	-	-
9	No	-	-	-	-	-
10	No	-	-	-	-	-

Parameter descriptions:

Port: The switch port number.

LACP: 'Yes' means that LACP is enabled and the port link is up. 'No' means that LACP is not enabled or that the port link is down. 'Backup' means that the port could not join the aggregation group but will join if other port leaves; meanwhile its LACP status is disabled.

Key: The key assigned to this port. Only ports with the same key can aggregate together.

Aggr ID: The Aggregation ID assigned to this aggregation group.

Partner System ID: The system ID (MAC address) of the aggregation partner.

Partner Port: The partner's port number connected to this port.

Partner Prio: The priority of this partner.

Buttons

Auto-refresh: Check this box to refresh the page automatically every 3 seconds.

Refresh: Click to manually refresh the page immediately.

3-6.3 LACP Port Statistics

This page displays an overview of LACP statistics for all ports. To display the LACP Port status via the Web UI:

1. Click Monitor, Aggregation, LACP, Port Status.
2. To auto-refresh the page check the “Auto refresh” checkbox.
3. Click “Refresh” to refresh the LACP ports’ status.

Figure 3-6.3: LACP Statistics page

Port	LACP Received	LACP Transmitted	Discarded	
			Unknown	Illegal
1	0	0	0	0
2	0	0	0	0
3	0	466	0	0
4	0	364	0	0
5	0	0	0	0
6	0	364	0	0
7	0	364	0	0
8	0	0	0	0
9	0	0	0	0
10	0	0	0	0

Parameter descriptions:

Port: The switch port number.

LACP Received: Shows how many LACP frames have been received at each port.

LACP Transmitted: Shows how many LACP frames have been sent from each port.

Discarded: Shows how many unknown and illegal LACP frames have been discarded at each port.

Buttons

Auto-refresh: Check this box to refresh the page automatically every 3 seconds.

Refresh: Click to manually refresh the page immediately.

Clear: Clears the counters for the selected port.



3-7 Loop Protection

This page displays the loop protection port status for switch ports. To display Loop Protection status in the web UI:

1. Click Monitor, Loop Protection.
2. To automatically refresh the page, check the “Auto refresh” checkbox.
3. Click “Refresh” to refresh the statistics.

Figure 3-7: Loop Protection Status page

The screenshot shows the Lantronix web interface for the SM24TBT2DPA switch. The 'Monitor' section is active, and the 'Loop Protection' status is displayed. The 'Auto-refresh' checkbox is unchecked. The table below shows the status of 8 ports.

Port	Action	Transmit	Loops	Status	Loop	Time of Last Loop
1	Log Only	Enabled	0	Down	-	-
2	Shutdown+Log	Enabled	0	Up	-	-
3	Shutdown+Log	Enabled	0	Up	-	-
4	Log Only	Enabled	0	Down	-	-
5	Shutdown	Enabled	0	Up	-	-
6	Shutdown	Enabled	0	Down	-	-
7	Shutdown	Enabled	0	Up	-	-
8	Shutdown	Enabled	0	Up	-	-

Parameter descriptions:

Port: The switch port number of the logical port.

Action: The currently configured port action (Log Only, Shutdown, or Shutdown+Log).

Transmit: The currently configured port transmit mode (Enabled or Disabled).

Loops: The number of loops detected on this port.

Status: The current loop protection status of the port (Up or Down).

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 manually refresh the page immediately.

3-8 Spanning Tree

3-8.1 Bridge Status

This page displays a status overview of all STP bridge instances, with a row for each STP bridge instance.

To display the STP Bridges status in the web UI:

1. Click Monitor, Spanning Tree, STP Bridges.
2. Click “Refresh” to refresh the STP Bridges.
3. Click “CIST” to display the next page “STP Detailed Bridge Status”.

Figure 3-8.1: STP Bridges status page

The screenshot shows the Lantronix web interface for the SM24TBT2DPB device. The main content area is titled "STP Bridges" and includes an "Auto-refresh" checkbox (unchecked) and a refresh button. Below this is a table with the following data:

MSTI	Bridge ID	Root			Topology Flag	Topology Change Last
		ID	Port	Cost		
CIST	32768.00-C0-F2-83-83-28	32768.00-C0-F2-4C-D0-33	26	60000	Steady	31d 10:07:08

Parameter descriptions:

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.

Buttons

Auto-refresh: Check this box to refresh the page automatically every 3 seconds.

Refresh: Click to manually refresh the page immediately.

Example: Click a linked instance in the MSTI column on the STP Bridges webpage to display the STP Detailed Bridge Status page:

The screenshot shows the Lantronix web interface for device SM24TBT2DPB. The main content area is titled "STP Detailed Bridge Status" and includes an "Auto-refresh" checkbox and a refresh icon. Below this is a table of STP Bridge Status parameters:

STP Bridge Status	
Bridge Instance	CIST
Bridge ID	32768.00-C0-F2-83-83-28
Root ID	32768.00-C0-F2-4C-D0-33
Root Cost	60000
Root Port	26
Regional Root	32768.00-C0-F2-83-83-28
Internal Root Cost	0
Topology Flag	Steady
Topology Change Count	90
Topology Change Last	31d 10:08:01

Below the summary table is a section titled "CIST Ports & Aggregations State" which contains a table with the following data:

Port	Port ID	Role	State	Path Cost	Edge	Point-to-Point	Uptime
1	128:001	DesignatedPort	Forwarding	200000	Yes	Yes	54d 12:44:09
2	128:002	DesignatedPort	Forwarding	20000	Yes	Yes	34d 14:58:05
23	128:017	DesignatedPort	Forwarding	20000	Yes	Yes	45d 00:17:42
24	128:018	DesignatedPort	Forwarding	20000	No	Yes	50d 05:53:37
26	128:01a	RootPort	Forwarding	20000	No	Yes	86d 08:40:33

Parameter descriptions:

STP Bridge Status

Bridge Instance: The Bridge instance - CIST, MST1, etc.

Bridge ID: The Bridge ID of this Bridge instance.

Root ID: The Bridge ID of the currently elected root bridge.

Root Port: The switch port currently assigned the root port role.

Root Cost: Root Path Cost. For the Root Bridge this is zero. For all other Bridges, it is the sum of the Port Path Costs on the least cost path to the Root Bridge.

Regional Root: The Bridge ID of the currently elected regional root bridge, inside the MSTP region of this bridge. (For the CIST instance only.)

Internal Root Cost: The Regional Root Path Cost. For the Regional Root Bridge this is zero. For all other CIST instances in the same MSTP region, it is the sum of the Internal Port Path Costs on the least cost path to the Internal Root Bridge. (For the CIST instance only.)

Topology Flag: The current state of the Topology Change Flag of this Bridge instance.

Topology Change Count: The number of times where the topology change flag has been set (during a one-second interval).

Topology Change Last: The time passed since the Topology Flag was last set.

CIST Ports & Aggregations State

Port: The switch port number of the logical STP port.

Port ID: The port id as used by the STP protocol. This is the priority part and the logical port index of the bridge port (e.g., *128:001*).

Role: The current STP port role. The port role can be one of the following values: *AlternatePort*, *BackupPort*, *RootPort*, or *DesignatedPort*.

State: The current STP port state. The port state can be one of the following values: *Discarding*, *Learning*, or *Forwarding*.

Path Cost: The current STP port path cost. This will either be a value computed from the Auto setting, or any explicitly configured value.

Edge: The current STP port (operational) Edge Flag. An Edge Port is a switch port to which no Bridges are attached. The flag may be automatically computed or explicitly configured. Each Edge Port transits directly to the Forwarding Port State, since there is no possibility of it participating in a loop.

Point-to-Point: The current STP port point-to-point flag (*Yes* or *No*). 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 in the format *3848d 14:50:36*.

Buttons

Refresh: Click to manually refresh the page immediately.

Auto-refresh: Check this box to refresh the page automatically every 3 seconds.

3-8.2 Port Status

This page displays the STP Port Status. To display the STP Port status in the web UI:

1. Click Monitor, Spanning Tree, STP Port Status.
2. To auto-refresh the information check the “Auto-refresh” checkbox.
3. Click “Refresh” to refresh the STP Bridges.

Figure 3-8.2: STP Port Status page

The screenshot shows the Lantronix web interface for device SM24TBT2DPA. The main content area is titled "STP Port Status" and features an "Auto-refresh" checkbox (unchecked) and a refresh button. Below this is a table with the following data:

Port	CIST Role	CIST State	Uptime
1	Disabled	Discarding	-
2	DesignatedPort	Forwarding	0d 18:26:48
3	DesignatedPort	Forwarding	0d 18:26:46
4	Disabled	Discarding	-
5	DesignatedPort	Forwarding	0d 18:26:44
6	Disabled	Discarding	-
7	DesignatedPort	Forwarding	0d 18:26:35
8	DesignatedPort	Forwarding	0d 18:27:13
9	DesignatedPort	Forwarding	0d 18:26:44
10	DesignatedPort	Forwarding	0d 18:26:42
11	Disabled	Discarding	-

Parameter descriptions:

Port: The switch port number of the logical STP port.

CIST Role: The current STP port role of the CIST port. The port role can be one of these values: *AlternatePort*, *BackupPort*, *RootPort*, *DesignatedPort*, *Non-STP*, or *Disabled*.

CIST State: The current STP port state of the CIST port. The port state can be *Blocking*, *Learning*, or *Forwarding*.

Uptime: The time since the bridge port was last initialized in the format *3848d 15:00:26*.

Buttons

Auto-refresh: Check this box to refresh the page automatically every 3 seconds.

Refresh: Click to manually refresh the page immediately.

3-8.3 Port Statistics

This page displays the STP Statistics detail counters of bridge ports in the switch. To display STP Statistics in the web UI:

1. Click Monitor, Spanning Tree, Port Statistics.
2. To auto-refresh the information check the “Auto-refresh” checkbox.
3. Click “Refresh” to refresh the STP Bridges.

Figure 3-8.3: STP Statistics page

Port	Transmitted				Received				Discarded	
	MSTP	RSTP	STP	TCN	MSTP	RSTP	STP	TCN	Unknown	Illegal
1	2311694	0	0	0	0	0	0	0	0	0
2	1466734	0	0	0	0	0	0	0	0	0
23	1907572	0	0	0	0	0	0	0	0	0
24	2129765	0	0	0	5	0	0	0	0	0
26	95	0	0	0	3929451	0	0	0	0	0

Parameter descriptions:

Port: The switch port number of the logical STP port.

MSTP: The number of MSTP Configuration BPDU's received/transmitted on the port.

RSTP: The number of RSTP Configuration BPDU's received/transmitted on the port.

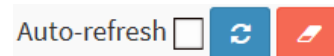
STP: The number of legacy STP Configuration BPDU's received/transmitted on the port.

TCN: The number of (legacy) Topology Change Notification BPDU's received/transmitted on the port.

Discarded Unknown: The number of unknown Spanning Tree BPDU's received (and discarded) on the port.

Discarded Illegal: The number of illegal Spanning Tree BPDU's received (and discarded) on the port.

Buttons



Auto-refresh: Check this box to refresh the page automatically every 3 seconds.

Refresh: Click to refresh the page immediately.

Clear: Clears the counters for the selected port.

3-9 MVR

3-9.1 Statistics

This page displays detailed Multi VLAN Registration Statistics configured on the switch.

To display MVR Statistics in the web UI:

1. Click Monitor, MVR, Statistics.
2. To auto-refresh the information check the “Auto-refresh” checkbox.
3. To click the “Refresh” to refresh the MVR Statistics Information.

Figure 3-9.1: MVR Statistics page

VLAN ID	IGMP/MLD Queries Received	IGMP/MLD Queries Transmitted	IGMPv1 Joins Received	IGMPv2/MLDv1 Reports Received	IGMPv3/MLDv2 Reports Received	IGMPv2/MLDv1 Leaves Received
1	0/0	0/0	0	0/0	55/27	0/0

Parameter descriptions:

VLAN ID: The Multicast VLAN identifier.

IGMP/MLD Queries Received: The number of Received Queries for IGMP and MLD, respectively.

IGMP/MLD Queries Transmitted: The number of Transmitted Queries for IGMP and MLD, respectively.

IGMPv1 Joins Received: The number of Received IGMPv1 Joins.

IGMPv2/MLDv1 Reports Received: The number of Received IGMPv2 Joins and MLDv1 Reports, respectively.

IGMPv3/MLDv2 Reports Received: The number of Received IGMPv1 Joins and MLDv2 Reports, respectively.

IGMPv2/MLDv1 Leaves Received: The number of Received IGMPv2 Leaves and MLDv1 Dones, respectively.

Buttons



Auto-refresh: Check this box to refresh the page automatically every 3 seconds.

Clear: Clears the counters for the selected port.

Refresh: Click to refresh the page immediately.

3-9.2 MVR Channels Groups

This page displays MVR Groups information. 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.

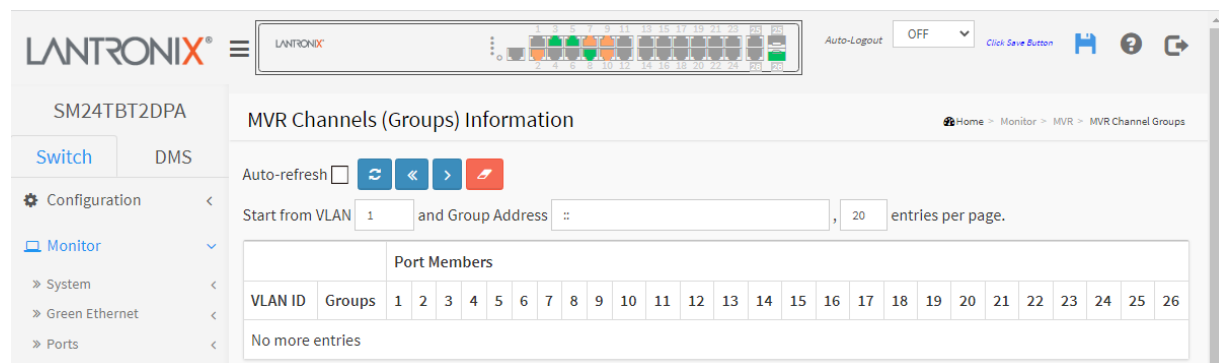
The "Start from VLAN" and "Group Address" input fields lets you select the starting point in the MVR Channels (Groups) Information Table. Clicking the Refresh button will update the displayed table starting from that or the closest next MVR Channels (Groups) Information Table match. In addition, the two input fields will - upon a Refresh button click - assume the value of the first displayed entry, allowing for continuous refresh with the same start address.

Clicking the Next entry (>) 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" displays in the displayed table. Use the << button to start over.

To display MVR Groups Information in the web UI:

1. Click Monitor, MVR, Groups Information.
2. Check the "Auto-refresh" checkbox or click "Refresh" to refresh the page.
3. Click "<< or >" to move to the previous or next entry.

Figure 3-9.2: MVR Channels (Groups) Information page



Parameter descriptions:

VLAN ID: VLAN ID of the group.

Groups: Group ID of the group displayed.

Port Members: Ports under this group.

Buttons



Auto-refresh: Check this box to refresh the page automatically every 3 seconds.

Refresh: Click to refresh the page immediately.

<<: Updates the system log entries to the first available entry ID.

>: Updates the system log entry to the next available entry ID.

3-9.3 MVR SFM Information

The MVR SFM (Source-Filtered Multicast) Information Table also contains the SSM (Source-Specific Multicast) information. This table is sorted first by VLAN ID, then by group, and then by Port. Different source addresses belonging to the same group are treated as a single entry.

Each page shows up to 99 entries from the MVR SFM Information Table (default 20) selected via the "entries per page" input field. When first visited, the web page will show the first 20 entries from the beginning of the MVR SFM Information Table.

The "Start from VLAN", and "Group Address" input fields lets you select the starting point in the MVR SFM Information Table. Clicking the Refresh button will update the displayed table starting from that or the closest next MVR SFM Information Table match. In addition, the two input fields will - upon a Refresh button click - assume the value of the first displayed entry, allowing for continuous refresh with the same start address.

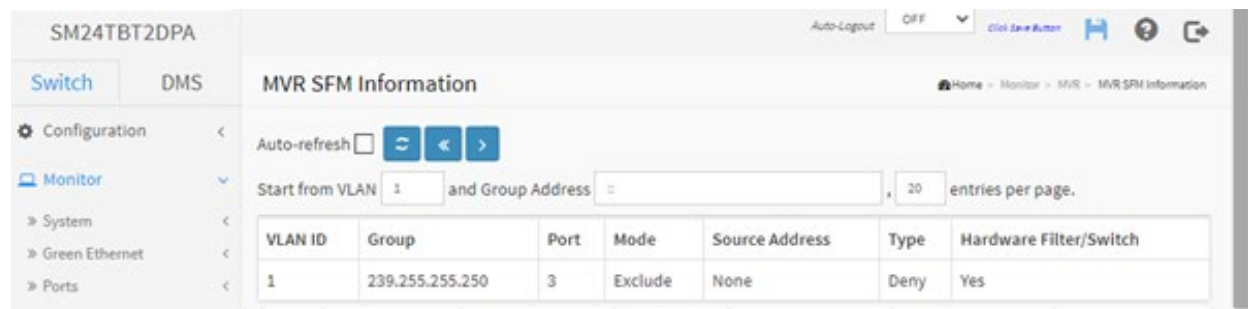
Clicking the Next entry (>>) button will use the last entry of the currently displayed table as a basis for the next lookup. When the end is reached the text "No more entries" is shown in the displayed table. Use the << button to start over.

Web Interface

To display MVR SFM Information in the web UI:

1. Click Monitor, MVR, MVR SFM Information
2. To auto-refresh the information check the "Auto.-refresh" checkbox.
3. To click "Refresh" to refresh an entry of the MVR Groups Information.
4. Click "<< or >>" to move to previous or next entry.

Figure 3-9.2: MVR SFM Information page



Parameter descriptions:

VLAN ID: The VLAN ID of the group.

Group: The IP address of the group.

Port: The Switch port number.

Mode: Indicates the filtering mode maintained per (VLAN ID, port number, Group Address) basis. The Mode can be either *Include* or *Exclude*.

Source Address: IP Address of the source. Currently, the system limits the total number of IP source addresses for filtering to be 128. 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/IPv6 address could be handled by the onboard chip 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 system log entries to the first available entry ID.

>: Updates the system log entry to the next available entry ID.

3-10 IPMC

3-10.1 IGMP Snooping

3-10.1.1 Status

This page displays the IGMP Snooping detailed status. To display IGMP Snooping status in the web UI:

1. Click Monitor, IGMP Snooping, Status.
2. Check the “Auto-refresh” checkbox or click “Refresh” to refresh the page.
3. Click “Clear” to clear the IGMP Snooping Status.

Figure 3-10.1.1: IGMP Snooping Status page

The screenshot shows the web UI for SM24TBT2DPA. The left sidebar contains a navigation menu with 'Monitor' selected, and 'IGMP Snooping' > 'Status' selected. The main content area is titled 'IGMP Snooping Status'. At the top, there is an 'Auto-refresh' checkbox which is unchecked, and a 'Refresh' button. Below this is a 'Statistics' table with the following data:

VLAN ID	Querier Version	Host Version	Querier Status	Queries Transmitted	Queries Received	V1 Reports Received	V2 Reports Received	V3 Reports Received	V2 Leaves Received
10	v3	v3	DISABLE	0	0	0	0	0	0

Below the statistics table is a 'Router Port' table:

Port	Status
1	-
2	-
3	-
4	-
5	-

Parameter descriptions:

VLAN ID: The VLAN ID of the entry.

Querier Version: Working Querier Version currently.

Host Version: Working Host Version currently.

Querier Status: Shows the Querier status as "ACTIVE" or "IDLE". Displays "DISABLE" if the specific interface is administratively disabled.

Queries Transmitted: The number of Transmitted Queries.

Queries Received: The number of Received Queries.

V1 Reports Received: The number of Received V1 Reports.

V2 Reports Received: The number of Received V2 Reports.

V3 Reports Received: The number of Received V3 Reports.

V2 Leaves Received: The number of Received V2 Leaves.

Router Port: Display which ports act as router ports. A router port is a port on the Ethernet switch that leads towards the Layer 3 multicast device or IGMP querier.

Static denotes the specific port is configured to be a router port.

Dynamic denotes the specific port is learnt to be a router port.

Both 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: Check this box to refresh the page automatically every 3 seconds.

Clear: Clears the counters for the selected port.

Refresh: Click to refresh the page immediately.

3-10.1.2 Group Information

After you complete setting the IGMP Snooping function you can have the switch display the IGMP Snooping Group Information. Entries in the IGMP Group Table are shown on this page. The IGMP Group Table is sorted first by VLAN ID, and then by group. Clicking the Next entry 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 Refresh button to start over.

Each page shows up to 99 entries from the IGMP Group table, default being 20, selected through the "entries per page" input field. When first visited, the web page will show the first 20 entries from the beginning of the IGMP Group Table.

The "Start from VLAN", and "group" input fields lets you select the starting point in the IGMP Group Table. Clicking the Refresh button will update the displayed table starting from that or the closest next IGMP Group Table match. In addition, the two input fields will - upon a Refresh button click - assume the value of the first displayed entry, allowing for continuous refresh with the same start address.

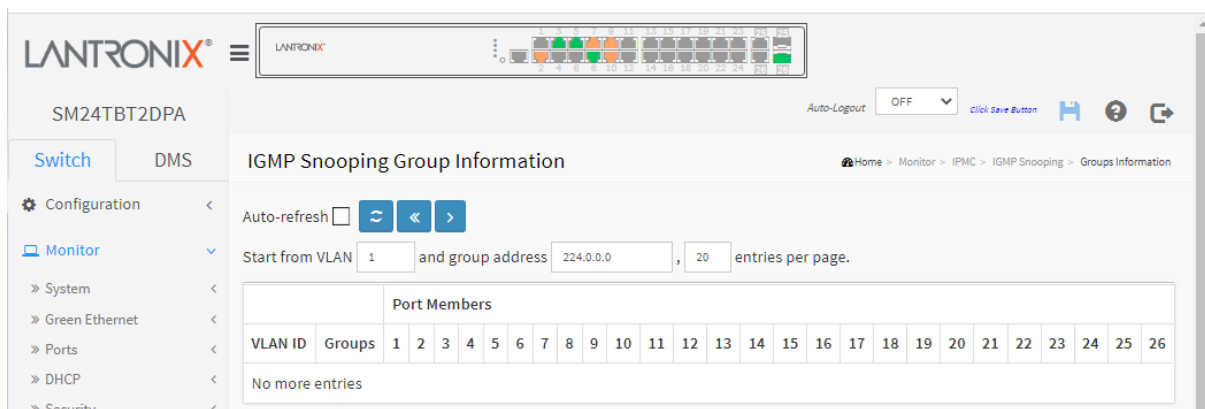
Clicking the Next entry (>>) button will use the last entry of the currently displayed table as a basis for the next lookup. When the end is reached the text "No more entries" is shown in the displayed table. Use the << button to start over.

Web Interface

To display IGMP Snooping Group Information in the web UI:

1. Click Monitor, IGMP Snooping, Group Information.
2. Check the "Auto-refresh" checkbox or click "Refresh" to refresh the page.
3. Click "<< or >>" to move to previous or next entry.

Figure 3-10.1.2: IGMP Snooping Group Information page



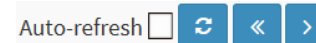
Parameter descriptions:

VLAN ID: VLAN ID of the group.

Groups: Group address of the group displayed.

Port Members: Ports under this group.

Buttons



Auto-refresh: Check this box to refresh the page automatically every 3 seconds.

Refresh: Click to refresh the page immediately.

<<: Updates the system log entries to the first available entry ID.

>>: Updates the system log entry to the next available entry ID.

3-10.1.3 IPv4 SFM Information

Entries in the IGMP SFM Information Table are shown on this page. The IGMP SFM (Source-Filtered Multicast) Information Table also contains the SSM (Source-Specific Multicast) information. This table is sorted first by VLAN ID, then by group, and then by Port. Different source addresses belong to the same group are treated as single entry.

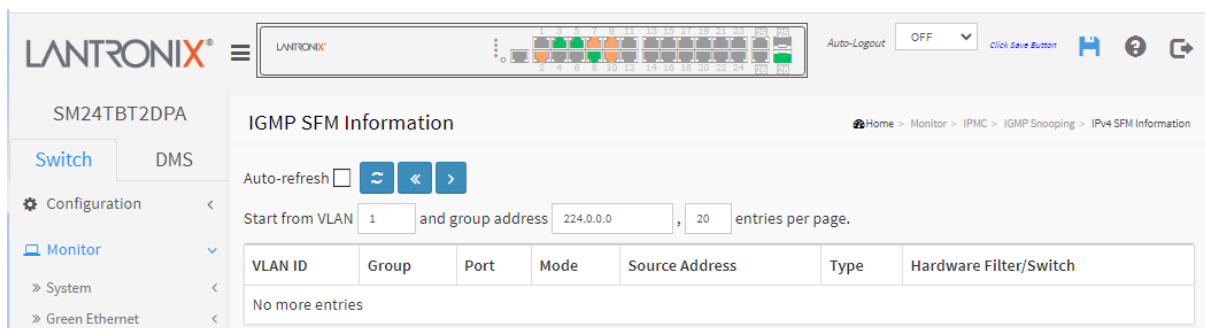
Each page shows up to 99 entries from the IGMP SFM Information table, default being 20, selected through the "entries per page" input field. When first visited, the web page will show the first 20 entries from the beginning of the IGMP SFM Information Table.

The "Start from VLAN", and "group" input fields lets you select the starting point in the IGMP SFM Information Table. Clicking the Refresh button will update the displayed table starting from that or the closest next IGMP SFM Information Table match. In addition, the two input fields will - upon a Refresh button click - assume the value of the first displayed entry, allowing for continuous refresh with the same start address.

To display IGMP SFM Information in the web UI:

1. Click Monitor, IGMP Snooping, IPv4 SSM Information.
2. Check the "Auto-refresh" checkbox or click "Refresh" to refresh the page.
4. Click << or >> to move to previous or next entry.

Figure 3-10.1.3: IGMP SFM Information



Parameter descriptions:

VLAN ID: VLAN ID of the group.

Group: Group address of the group displayed.

Port: Switch port number.

Mode: Indicates the filtering mode maintained per (VLAN ID, port number, Group Address) basis. It can be either **Include** or **Exclude**.

Source Address: IP Address of the source. Currently, the system limits the total number of IP source addresses for filtering to be 128.

Type: Indicates the Type. It can be either **Allow** or **Deny**.

Hardware Filter/Switch: Indicates whether data plane destined to the specific group address from the source IPv4 address could be handled by the chip.

Buttons

Auto-refresh: Check this box to refresh the page automatically every 3 seconds.

Refresh: Click to refresh the page immediately.

<<: Updates the system log entries to the first available entry ID.

>>: Updates the system log entry to the next available entry ID.

3-10.2 MLD Snooping

3-10.2.1 Status

This page displays MLD Snooping status. To display MLD Snooping Status in the web UI:

1. Click Monitor > IPMC > MLD Snooping > Status.
2. To auto-refresh the information check the "Auto-refresh" checkbox.
3. Click "Clear" to clear the MLD Snooping Status.

Figure 3-10.2.1: MLD Snooping Status page

The screenshot shows the web UI for SM24TBT2DPA. The main content area is titled 'MLD Snooping Status'. It features an 'Auto-refresh' checkbox which is currently unchecked. Below this is a 'Statistics' table with the following data:

VLAN ID	Querier Version	Host Version	Querier Status	Queries Transmitted	Queries Received	V1 Reports Received	V2 Reports Received	V1 Leaves Received
10	v2	v2	ACTIVE	106	0	0	0	0

Below the statistics is a 'Router Port' table:

Port	Status
1	-
2	Both
3	-
4	Both
5	-
6	-

Parameter descriptions:

VLAN ID: The VLAN ID of the entry.

Querier Version: Working Querier Version currently.

Host Version: Working Host Version currently.

Querier Status: Show the Querier status is "ACTIVE" or "IDLE". "DISABLE" denotes the specific interface is administratively disabled.

Queries Transmitted: The number of Transmitted Queries.

Queries Received: The number of Received Queries.

V1 Reports Received: The number of Received V1 Reports.

V2 Reports Received: The number of Received V2 Reports.

V1 Leaves Received: The number of Received V1 Leaves.

Router Port: Display which ports act as router ports. A router port is a port on the Ethernet switch that leads towards the Layer 3 multicast device or MLD querier.

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.

Port: Switch port number.

Status: Indicate whether specific port is a Router port or Both.

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.

3-10.2.2 Group Information

This page displays MLD Snooping Groups Information. The "Start from VLAN", and "group" input fields lets you select the starting point in the MLD Group table.

Each page shows up to 99 entries from the MLD Group table, default being 20, selected through the "entries per page" input field. When first visited, the web page will show the first 20 entries from the beginning of the MLD Group Table.

The "Start from VLAN", and "group" input fields lets you select the starting point in the MLD Snooping Group Table. Clicking the Refresh button will update the displayed table starting from that or the closest next MLD Group Table match. In addition, the two input fields will - upon a Refresh button click - assume the value of the first displayed entry, allowing for continuous refresh with the same start address.

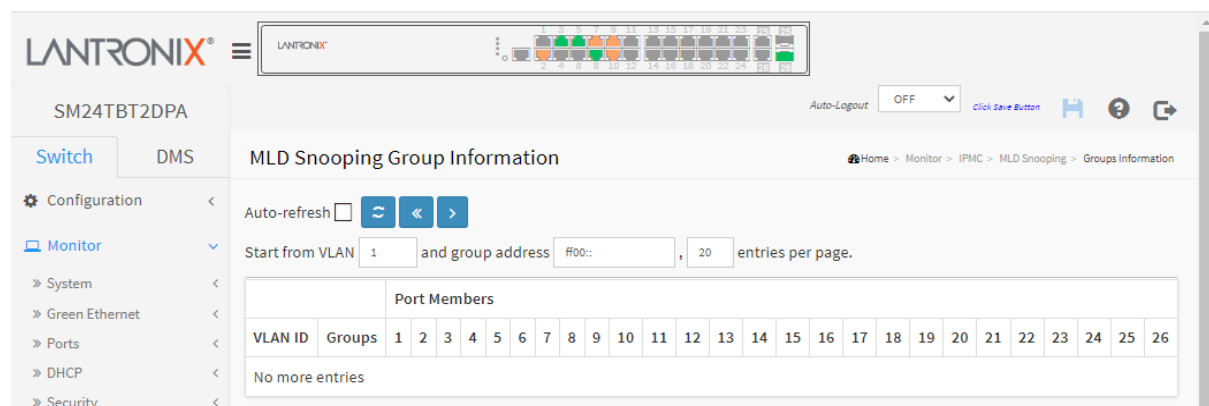
Clicking the Next entry (>>) button will use the last entry of the currently displayed table as a basis for the next lookup. When the end is reached the text "No more entries" is shown in the displayed table. Use the << button to start over.

Web Interface

To display MLD Snooping Groups information in the web UI:

1. Click Monitor, MLD Snooping, Group Information.
2. Check the "Auto-refresh" checkbox or click "Refresh" to refresh the page

Figure 3-10.2.2: MLD Snooping Groups Information page



Parameter descriptions:

VLAN ID: VLAN ID of the group.

Groups: Group address of the group displayed.

Port Members: Ports under this group.

Buttons



Auto-refresh: Check this box to refresh the page automatically every 3 seconds.

Refresh: Click to refresh the page immediately.

<<: Updates the system log entries to the first available entry ID.

>: Updates the system log entry to the next available entry ID.

3-10.2.3 IPv6 SFM Information

Entries in the MLD SFM Information Table are shown on this page. The MLD SFM (Source-Filtered Multicast) Information Table also contains the SSM (Source-Specific Multicast) information. This table is sorted first by VLAN ID, then by group, and then by Port. Different source addresses belong to the same group are treated as single entry.

Each page shows up to 99 entries from the MLD SFM Information table, default being 20, selected through the "entries per page" input field. When first visited, the web page will show the first 20 entries from the beginning of the MLD SFM Information Table.

The "Start from VLAN", and "group" input fields lets you select the starting point in the MLD SFM Information Table. Clicking the Refresh button will update the displayed table starting from that or the closest next MLD SFM Information Table match. In addition, the two input fields will - upon a Refresh button click - assume the value of the first displayed entry, allowing for continuous refresh with the same start address.

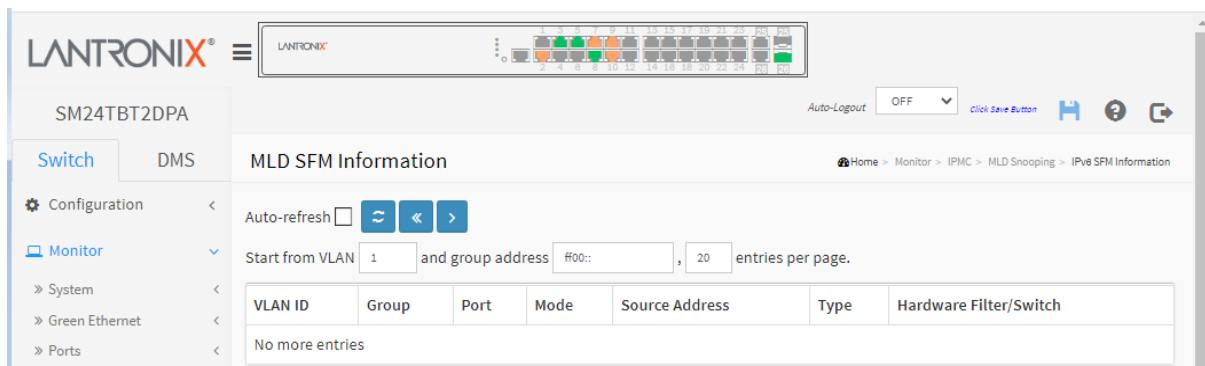
Clicking the Next entry (>) button will use the last entry of the currently displayed table as a basis for the next lookup. When the end is reached the text "No more entries" is shown in the displayed table. Use the << button to start over.

Web Interface

To display MLDv2 IPv6 SSM Information in the web UI:

1. Click Monitor, MLD Snooping, IPv6 SFM Information.
2. To auto-refresh the information check the "Auto-refresh" checkbox.
3. Click "Refresh" to refresh an entry of the MLDv2 IPv6 SSM Information.
4. Click "<< or >" to move to previous or next entry.

Figure 3-10.2.3: MLD SFM Information page



Parameter descriptions:

VLAN ID: VLAN ID of the group.

Group: Group address of the group displayed.

Port: Switch port number.

Mode: Indicates the filtering mode maintained per (VLAN ID, port number, Group Address) basis. It can be either **Include** or **Exclude**.

Source Address: IP Address of the source. Currently, system limits the total number of IP source addresses for filtering to be 128.

Type: Indicates the Type. It can be either **Allow** or **Deny**.

Hardware Filter/Switch: Indicates whether data plane destined to the specific group address from the source IPv6 address could be handled by the chip.

Buttons



Auto-refresh: Check this box to refresh the page automatically every 3 seconds.

Refresh: Click to refresh the page immediately.

<<: Updates the system log entries to the first available entry ID.

>: Updates the system log entry to the next available entry ID.

3-11 LLDP

3-11.1 Neighbors

This page provides a status overview of all LLDP neighbors. The LLDP Remote Device Summary table contains a row for each port on which an LLDP neighbor is detected. If your network has no devices that support LLDP, then the table displays “No LLDP neighbor information found”. To show LLDP neighbors:

1. Click Monitor, LLDP, Neighbors.
2. Click Refresh to manually update the webpage or click Auto-refresh to automatically update the webpage every 3 seconds.

Figure 3-11.1: LLDP Neighbors Information

Local Port	Chassis ID	Port ID	Port Description	System Name	System Capabilities	System Description	Management Address
Port 3	00-C0-F2-7F-68-5B	26	Port #26	SM24TBT2DPA	Bridge(+)	Managed Switch, 24-port Gigabit PoE++, 2-port SFP/RJ-45 Combo	192.168.1.77 (IPv4)
Port 7	AC-CC-8E-BA-F7-C1	AC-CC-8E-BA-F7-C1	eth0	axis- accc8ebaf7c1	Bridge(-), WLAN Access Point(-), Router(-), Station Only(+)	AXIS P1447-LE Network Camera 7.35.2.3	192.168.0.90 (IPv4)
Port 26	00-C0-F2-7F-68-5B	3	Port #3	SM24TBT2DPA	Bridge(+)	Managed Switch, 24-port Gigabit PoE++, 2-port SFP/RJ-45 Combo	192.168.1.77 (IPv4)

Parameter descriptions:

Local Port: The port on which the LLDP frame was received.

Chassis ID: The identification of the neighbor’s LLDP frames.

Port ID: The Remote Port ID is the identification of the neighbor port (a switch port # or the MAC address or the neighbor device).

Port Description: The port description advertised by the neighbor unit (e.g., *Port # 4* or *eth0*).

System Name: The name advertised by the neighbor unit (e.g., SM24TBT2DPA or an IP camera model number).

System Capabilities: Displays the neighbor unit's capabilities (e.g., Other, Repeater, Bridge, WLAN Access Point, Router, Telephone, DOCSIS cable device, Station only, and Reserved).

+ : When a capability is enabled, the capability is followed by (+).

- : If the capability is disabled, the capability is followed by a (-).

System Description: Displays a description of the neighbor device (e.g., *Managed Switch ...*, *Network Camera ...*, etc.).

Management Address: The neighbor unit's IP address that is used for higher layer entities to assist discovery by the network management. This could show the neighbor’s IP address and provide a link to the device. If you click the linked IP address a login page displays to let you log in to and set up the discovered neighbor device. Sample screens are shown below.

Buttons

Auto-refresh: Check this box to refresh the page automatically every 3 seconds.

Refresh: Click to refresh the page immediately.

Sample Screens

LANTRONIX SM24TBT2DPB LLDP Neighbor Information

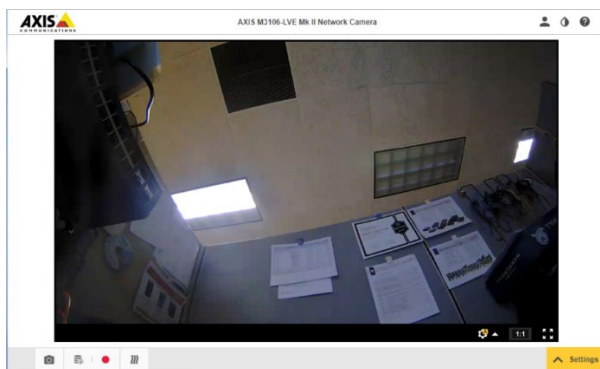
Auto-refresh

Local Port	Chassis ID	Port ID	Port Description	System Name	System Capabilities	System Description	Management Address
Port 1	5C-FF-35-DC-0A-C1	5C-FF-35-DC-0A-C1					
Port 2	AC-CC-8E-A7-02-65	AC-CC-8E-A7-02-65	eth0	axis-acc8ea70265	Bridge(-), WLAN Access Point(-), Router(-), Station Only(+)	AXIS Q1645 Network Camera 7.35.2.1	192.251.200.181 (IPv4)
Port 5	AC-CC-8E-BA-F7-C1	AC-CC-8E-BA-F7-C1	eth0	axis-acc8ebaf7c1	Bridge(-), WLAN Access Point(-), Router(-), Station Only(+)	AXIS P1447-LE Network Camera 7.35.2.3	192.168.0.90 (IPv4)

LANTRONIX SM24TBT2DPB LLDP Neighbor Information

Auto-refresh

Local Port	Chassis ID	Port ID	Port Description	System Name	System Capabilities	System Description	Management Address
Port 1	E8-EB-1B-CB-11-5F	POE PD	inspeXtor			sysDescr.0 = STRING: <<Port_Desc: inspeXtor; HW_REV: Rev 120219.0; VENDOR: inspeXtor; SERIAL_NUM: 15258; MODEL: 90-watt; FW_REV: Rev 120219.0>>	172.27.195.2 (IPv4)
Port 23	00-C0-F2-9A-B6-28	24	Port #24	SM24TAT2SA	Bridge(+)	Smart Managed Switch, 24-port Gigabit PoE+, 2-port 100/1000 SFP	172.27.195.100 (IPv4)
Port 24	18-7A-3B-38-8E-8A	77	2/24	MINNW-0001	Bridge(+), Router(+)	Aruba JL256A 2930F-48G-PoE+-45FP+ Switch, revision WC.16.11.0016, ROM WC.16.01.0010 (/ws/swbuildm/rel_beluru_qaoff/code/build/lvm/swbuildm_rel_beluru_qaoff_rel_beluru)	172.27.195.1 (IPv4)
Port 26	00-C0-F2-8C-09-30	2	SM24TBT2DPB	SM24DP4XA	Bridge(+)	Managed Gigabit Ethernet Fiber Switch (20) 100/1000Base-X SFP Slots + (4) 100/1000Base SFP/RJ-45 Combo Ports + (4) 1G/10GBase-X	172.27.195.50 (IPv4)



AXIS M3106-LVE Mk II Network Camera

Appearance settings:

- Saturation: 0 to 100
- Contrast: 0 to 100
- Brightness: 0 to 100
- Sharpness: 0 to 100
- Wide dynamic range: (ON)
- Local contrast: 0 to 100
- White balance: (OFF)
- Light environment: Automatic

3-11.2 LLDP-MED Neighbor

This page provides a status overview of all LLDP-MED neighbors. The displayed table contains a row for each port on which an LLDP neighbor is detected. This function applies to devices which support LLDP-MED. If your network without any device supports LLDP-MED, then the table will show “*No LLDP-MED neighbor information found*”. To show LLDP-MED neighbor information:

1. Click Monitor, LLDP, LLDP-MED Neighbor.
2. Click Refresh for a manual page update or click Auto-refresh for an automatic page update every 3 seconds.

Figure 3-11.2: LLDP-MED Neighbor Information page (before FW v 6.54.0.0R0046)

LLDP-MED Neighbor Information				
Auto-refresh <input type="checkbox"/>				
Port 2				
Device Type	Capabilities			
Endpoint Class II	LLDP-MED Capabilities, Network Policy, Location Identification, Extended Power via MDI - PSE, Extended Power via MDI - PD, Inventory			
Auto-negotiation	Auto-negotiation status	Auto-negotiation Capabilities		MAU Type
Supported	Enabled	1000BASE-T full duplex mode, 1000BASE-T half duplex mode, 100BASE-TX full duplex mode, 100BASE-TX half duplex mode, 100BASE-T full duplex mode, 10BASE-T half duplex mode		1000BaseTFD - Four-pair Category 5 UTP, full duplex mode

Parameter descriptions:

Port: The port on which the LLDP frame was received.

Device Type: LLDP-MED Devices are comprised of two primary Device Types: Network Connectivity Devices and Endpoint Devices.

LLDP-MED Network Connectivity Device 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:

- LAN Switch/Router
- IEEE 802.1 Bridge
- IEEE 802.3 Repeater (included for historical reasons)
- IEEE 802.11 Wireless Access Point

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 neighborhood unit's LLDP-MED capabilities. The possible capabilities are LLDP-MED capabilities, Network Policy, Location Identification, Extended Power via MDI – PSE, Extended Power via MDI – PD, Inventory, or Reserved.

Application Type: Application Type indicating the primary function of the application(s) defined for this network policy, advertised by an Endpoint or Network Connectivity Device. The possible application types are shown below.

Voice - for use by dedicated IP Telephony handsets and other similar appliances supporting interactive voice services. These devices are typically deployed on a separate VLAN for ease of deployment and enhanced security by isolation from data applications.

Voice Signaling - for use in network topologies that require a different policy for the voice Signaling than for the voice media.

Guest Voice - to support a separate limited feature-set voice service for guest users and visitors with their own IP Telephony handsets and other similar appliances supporting interactive voice services.

Guest Voice Signaling - 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 Signaling - for use in network topologies that require a separate policy for the video Signaling than for the video media.

Policy: Indicates that an Endpoint Device wants to explicitly advertise that the policy is required by the device. Can be either Defined or Unknown. Unknown: The network policy for the specified application type is currently unknown. Defined: The network policy is defined.

TAG: indicates whether the specified application type is using a tagged or an untagged VLAN. Can be Tagged or Untagged.

Untagged: The device is using an untagged frame format and as such does not include a tag header as defined by IEEE 802.1Q-2003.

Tagged: The device is using the IEEE 802.1Q tagged frame format.

VLAN ID: The VLAN identifier (VID) for the port as defined in IEEE 802.1Q-2003. A value of 1 through 4094 is used to define a valid VLAN ID. A value of 0 (Priority Tagged) is used if the device is using priority tagged frames as defined by IEEE 802.1Q-2003, meaning that only the IEEE 802.1D priority level is significant and the default PVID of the ingress port is used instead.

Priority: The Layer 2 priority to be used for the specified application type. One of the eight priority levels (0 through 7).

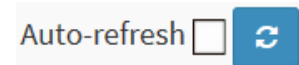
DSCP: The DSCP value to be used to provide Diffserv node behavior for the specified application type as defined in IETF RFC 2474. Contain one of 64 code point values (0 - 63).

Auto-negotiation identifies if MAC/PHY auto-negotiation is supported by the link partner.

Auto-negotiation status identifies if auto-negotiation is currently enabled at the link partner. If Auto-negotiation is supported and Auto-negotiation status is disabled, the 802.3 PMD operating mode will be determined the operational MAU type field value rather than by auto-negotiation.

Auto-negotiation Capabilities shows the link partners MAC/PHY capabilities (e.g., *1000BASE-T full duplex mode, 1000BASE-T half duplex mode, 100BASE-TX full duplex mode, 100BASE-TX half duplex mode, 100BASE-T full duplex mode, 10BASE-T half duplex mode*).

MAU Type : A Medium Attachment Unit (MAU) transceiver converts signals on an Ethernet cable to and from Attachment Unit Interface (AUI) signals (e.g., *1000BaseTFD - Four-pair Category 5 UTP, full duplex mode*).



Buttons

Auto-refresh: Check this box to refresh the page automatically every 3 seconds.

Refresh: Click to refresh the page immediately.

Figure 3-11.3a: LLDP-MED Neighbor Information page (FW v 6.54.0.0R0046 to VB6.64.0107)

LLDP-MED Neighbor Information					
Auto-refresh <input type="checkbox"/>					
Port 1					
Device Type		Capabilities			
Endpoint Class I		LLDP-MED Capabilities			
Auto-negotiation	Auto-negotiation status	Auto-negotiation Capabilities	MAU Type		
Supported	Enabled	1000BASE-T full duplex mode	Invalid MAU Type		

Parameter descriptions:

Port : The port on which the LLDP frame was received.

Device Type : LLDP-MED Devices are comprised of two primary Device Types: *Network Connectivity Devices* and *Endpoint Devices*. For example: *Endpoint Class I*.

Capabilities : describes the neighbor unit's LLDP-MED capabilities. The possible capabilities are:

1. LLDP-MED capabilities
2. Network Policy
3. Location Identification
4. Extended Power via MDI - PSE
5. Extended Power via MDI - PD
6. Inventory
7. Reserved

Auto-negotiation : 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 : Auto-negotiation Capabilities shows the link partners MAC/PHY capabilities. For example: *1000BASE-T full duplex mode*.

MAU Type : A Medium Attachment Unit (MAU) transceiver converts signals on an Ethernet cable to and from Attachment Unit Interface (AUI) signals (e.g., *1000BaseTFD - Four-pair Category 5 UTP, full duplex mode* or *Invalid MAU Type*).

Buttons

Auto-refresh: Check this box to refresh the page automatically every 3 seconds.

Refresh: Click to refresh the page immediately.

Figure 3-11.3b: LLDP-MED Neighbor Information page (FW VB6.64.0101 and after)

This page provides a status overview of all LLDP-MED neighbors. The displayed table contains a row for each port on which an LLDP neighbor is detected. This function applies to VoIP devices which support LLDP-MED.

The screenshot shows the Lantronix web interface for the SM24TBT2DPB device. The main content area is titled "LLDP-MED Neighbor Information" and includes an "Auto-refresh" checkbox and a refresh icon. A table displays the LLDP-MED neighbor information for Port 3.

Port 3							
Device Type	Capabilities						
Network Connectivity	LLDP-MED Capabilities, Extended Power via MDI - PD						
Application Type	Policy	Tag	VLAN ID	Priority	DSCP		
Reserved	Defined	Untagged	-	-	0		
Auto-negotiation	Auto-negotiation status	Auto-negotiation Capabilities		MAU Type			
Supported	Enabled	1000BASE-T full duplex mode, 100BASE-TX full duplex mode, 100BASE-TX half duplex mode, 100BASE-T full duplex mode, 10BASE-T half duplex mode		No internal MAU, view from AUI			

Parameter descriptions:

Port: The port on which the LLDP frame was received.

Device Type: LLDP-MED Devices are comprised of two primary **Device Types:** Network Connectivity Devices and Endpoint Devices.

LLDP-MED Network Connectivity Device 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 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: 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.

1. Voice - for use by dedicated IP Telephony handsets and other similar appliances supporting interactive voice services. These devices are typically deployed on a separate VLAN for ease of deployment and enhanced security by isolation from data applications.
2. Voice Signalling - for use in network topologies that require a different policy for the voice signalling than for the voice media.
3. Guest Voice - to support a separate limited feature-set voice service for guest users and visitors with their own IP Telephony handsets and other similar appliances supporting interactive voice services.
4. Guest Voice Signalling - for use in network topologies that require a different policy for the guest voice signalling than for the guest voice media.
5. Softphone Voice - for use by softphone applications on typical data centric devices, such as PCs or laptops.
6. Video Conferencing - for use by dedicated Video Conferencing equipment and other similar appliances supporting real-time interactive video/audio services.
7. Streaming Video - for use by broadcast or multicast based video content distribution and other similar applications supporting streaming video services that require specific network policy treatment. Video applications relying on TCP with buffering would not be an intended use of this application type.
8. Video Signalling - for use in network topologies that require a separate policy for the video signalling than for the video media.

Policy: Indicates that an Endpoint Device wants to explicitly advertise that the policy is required by the device. Can be either Defined or Unknown

Unknown: The network policy for the specified application type is currently unknown.

Defined: The network policy is defined.

Tag: Indicates of whether the specified application type is using a tagged or an untagged VLAN. Can be Tagged or Untagged.

Untagged: The device is using an untagged frame format and as such does not include a tag header as defined by IEEE 802.1Q-2003.

Tagged: The device is using the IEEE 802.1Q tagged frame format.

VLAN ID: The VLAN identifier (VID) for the port as defined in IEEE 802.1Q-2003. A value of 1 through 4094 is used to define a valid VLAN ID. A value of 0 (Priority Tagged) is used if the device is using priority tagged frames as defined by IEEE 802.1Q-2003, meaning that only the IEEE 802.1D priority level is significant and the default PVID of the ingress port is used instead.

Priority: The Layer 2 priority to be used for the specified application type. One of the eight priority levels (0 - 7).

DSCP: DSCP is the DSCP value to be used to provide Diffserv node behavior for the specified application type as defined in IETF RFC 2474. Contain one of 64 code point values (0 - 63).

Auto-negotiation: identifies if MAC/PHY auto-negotiation is supported by the link partner.

Auto-negotiation status: Identifies if auto-negotiation is currently enabled at the link partner. If Auto-negotiation is supported and Auto-negotiation status is disabled, the 802.3 PMD operating mode will be determined 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 immediately.

3-11.3 PoE

This page provides a status overview for all LLDP PoE neighbors. The displayed table contains a row for each port on which an LLDP PoE neighbor is detected.

To show LLDP PoE neighbor information:

1. Click Monitor, LLDP, PoE.
2. View the LLDP Neighbor Power Over Ethernet Status Information.
3. Check Auto-refresh or click Refresh to refresh the page immediately.

Figure 3-11.3: LLDP Neighbor Power Over Ethernet Information

Local Port	Power Type	Power Source	Power Priority	Maximum Power
1	PD Device	PSE	Low	71.3 [W]
23	PSE Device	Primary Power Supply	Low	287.9 [W]
24	PSE Device	Unknown	Unknown	0 [W]

Parameter descriptions:

Local Port: The port for this switch on which the LLDP frame was received.

Power Type: The Power Type represents whether the device is a Power Sourcing Entity (PSE) or Power Device (PD). If the Power Type is unknown it is represented as "Reserved".

Power Source: The Power Source represents the power source being utilized by a PSE or PD device. If the device is a **PSE** device it can either run on its Primary Power Source or its Backup Power Source. If it is not known whether the PSE device is using its Primary Power Source or its Backup Power Source it is indicated as "**Unknown**".

If the device is a **PD** device it can either run on its local power supply or it can use the PSE as power source. It can also use both its local power supply and the PSE.

If it is unknown what power supply the PD device is using it is indicated as "**Unknown**".

Power Priority: Power Priority represents the priority of the PD device, or the power priority associated with the PSE type device's port that is sourcing the power. There are three levels of power priority. 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 a value higher than 102.3 W, it is represented as "reserved".

Buttons

Auto-refresh: Check this box to refresh the page automatically every 3 seconds.

Refresh: Click to refresh the page immediately.

3-11.4 EEE

This page provides an overview of Energy Efficient Ethernet information exchanged by LLDP.

By using EEE power savings can be achieved at the expense of traffic latency. This latency occurs due to that the circuits EEE turn off to save power, need time to boot up before sending traffic over the link. This time is called "wakeup time". To achieve minimal latency, devices can use LLDP to exchange information about their respective TX and RX "wakeup time", as a way to agree upon the minimum wakeup time they need. If your network has no devices with EEE enabled, then the table will show "No LLDP EEE information found".

To show LLDP neighbors EEE information:

1. Click Monitor, LLDP, and then click EEE to show discover EEE devices.
2. Click Refresh for manual update the web page.
3. Click Auto-refresh for auto-update the web page.

Figure 3-11.4: LLDP Neighbors EEE information

Local Port	Tx Tw	Rx Tw	Fallback Receive Tw	Echo Tx Tw	Echo Rx Tw	Resolved Tx Tw	Resolved Rx Tw	EEE in Sync
26	17	17	17	17	17	30	30	●

Parameter descriptions:

Local Port: The port on which LLDP frames are received or transmitted.

Tx Tw: The link partner's maximum time that transmit path can hold off sending data after reassertion of LPI.

Rx Tw: The link partner's time that receiver would like the transmitter to hold off to allow time for the receiver to wake from sleep.

Fallback Receive Tw: The link partner's fallback receive Tw. A receiving link partner may inform the transmitter of an alternate desired Tw_sys_tx. Since a receiving link partner is likely to have discrete levels for savings, this provides the transmitter with additional information that it may use for a more efficient allocation. Systems that do not implement this option default the value to be the same as that of the Receive Tw_sys_tx.

Echo Tx Tw: The link partner's Echo Tx Tw value. The respective echo values will be defined as the local link partner's reflection (echo) of the remote link partners respective values. When a local link partner receives its echoed values from the remote link partner it can determine whether or not the remote link partner has received, registered and processed its most recent values. For example, if the local link partner receives echoed parameters that do not match the values in its local MIB, then the local link partner infers that the remote link partners request was based on stale information.

Echo Rx Tw: The link partner's Echo Rx Tw value.

Resolved Tx Tw: The resolved Tx Tw for this link. Note: NOT the link partner. The resolved value that is the actual "tx wakeup time" used for this link (based on EEE information exchanged via LLDP).

Resolved Rx Tw: The resolved Rx Tw for this link. Note: NOT the link partner. The resolved value that is the actual "tx wakeup time" used for this link (based on EEE information exchanged via LLDP).

EEE in Sync: Shows whether the switch and the link partner have agreed on wake times.

Red - Switch and link partner have not agreed on wakeup times.

Green - Switch and link partner have agreed on wakeup times.

3-11.5 Port Statistics

Two types of counters are shown. *Global* counters are counters that refer to the whole switch, while *Local* counters refer to per-port counters for the switch.

To show LLDP counters:

1. Click Monitor, LLDP, Port Statistics to show the LLDP counters.
2. Click Refresh for manual update web screen or click Auto-refresh for auto-update web screen.
3. Click Clear to clear all counters.

Figure 3-11.5: LLDP Counters page

The screenshot shows the Lantronix web interface for the SM24TBT2DPB switch. The main content area is titled "LLDP Counters" and includes an "Auto-refresh" control. Below this, there are two sections: "LLDP Global Counters" and "LLDP Statistics Local Counters".

LLDP Global Counters

Neighbor entries were last changed	2011-03-27T05:13:00+00:00 (181923 secs. ago)
Total Neighbors Entries Added	21
Total Neighbors Entries Deleted	17
Total Neighbors Entries Dropped	0
Total Neighbors Entries Aged Out	14

LLDP Statistics Local Counters

Local Port	Tx Frames	Rx Frames	Rx Errors	Frames Discarded	TLVs Discarded	TLVs Unrecognized	Org. Discarded	Age-Outs
1	45095	50584	0	0	0	0	35632	13
2	54758	0	0	0	0	0	0	0
3	0	0	0	0	0	0	0	0
4	0	0	0	0	0	0	0	0
5	0	0	0	0	0	0	0	0
6	0	0	0	0	0	0	0	0
7	0	0	0	0	0	0	0	0
8	0	0	0	0	0	0	0	0
9	0	0	0	0	0	0	0	0

Parameter descriptions:

LLDP Global Counters

Neighbor entries were last changed: Shows the time when the last entry was last deleted or added. It also shows the time elapsed since the last change was detected.

Total Neighbors Entries Added: Shows the number of new entries added since switch reboot.

Total Neighbors Entries Deleted: Shows the number of new entries deleted since switch reboot.

Total Neighbors Entries Dropped: Shows the number of LLDP frames dropped due to the entry table being full.

Total Neighbors Entries Aged Out: Shows the number of entries deleted due to Time-To-Live expiring.

LLDP Statistics Local Counters : The displayed table contains a row for each port

Local Port: The port on which LLDP frames are received or transmitted.

Tx Frames: The number of LLDP frames transmitted on the port.

Rx Frames: The number of LLDP frames received on the port.

Rx Errors: The number of received LLDP frames containing some kind of error.

Frames Discarded: If an LLDP frame is received on a port, and the switch's internal table has run full, the LLDP frame is counted and discarded. This situation is known as "Too Many Neighbors" in the LLDP standard. LLDP frames require a new entry in the table when the Chassis ID or Remote Port ID is not already contained within the table. Entries are removed from the table when a given port's link is down, an LLDP shutdown frame is received, or when the entry ages out.

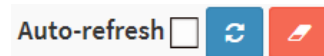
TLVs Discarded: Each LLDP frame can contain multiple pieces of information, known as TLVs (Type Length Values). If a TLV is malformed, it is counted and discarded.

TLVs Unrecognized: The number of well-formed TLVs, but with an unknown type value.

Org. Discarded: The number of organizationally received TLVs.

Age-Outs: Each LLDP frame contains information about how long time the LLDP information is valid (age-out time). If no new LLDP frame is received within the age out time, the LLDP information is removed, and the Age-Out counter is incremented.

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. All counters (including global counters) are cleared upon reboot.

3-12 PoE

This page displays the current status for all PoE ports. To display the PoE Status via the web UI:

1. Click Monitor, PoE.
2. Check “Auto-refresh” or click “Refresh” to refresh the port detailed statistics.

Figure 3-12: Power Over Ethernet Status page

Local Port	PD class	Power Requested	Power Allocated	Power Used	Current Used	Priority	Port Status
1	-	0 [W]	0 [W]	0 [W]	0 [mA]	Low	No PD detected
2	2	7 [W]	7 [W]	1.9 [W]	36 [mA]	Low	PoE turned ON
3	1	4 [W]	4 [W]	1.5 [W]	29 [mA]	Low	PoE turned ON
4	-	0 [W]	0 [W]	0 [W]	0 [mA]	Low	No PD detected
5	1	4 [W]	4 [W]	1.4 [W]	27 [mA]	Low	PoE turned ON
6	-	0 [W]	0 [W]	0 [W]	0 [mA]	Low	No PD detected
7	3	15 [W]	15 [W]	3.8 [W]	71 [mA]	Low	PoE turned ON
8	-	0 [W]	0 [W]	0 [W]	0 [mA]	Low	No PD detected
9	4	30 [W]	30 [W]	6.1 [W]	114 [mA]	Low	PoE turned ON
10	2	7 [W]	7 [W]	1.9 [W]	36 [mA]	Low	PoE turned ON

Parameter descriptions:

Local Port: This is the logical port number for this row.

PD Class: Each PD is classified according to a class that defines the maximum power the PD will use. The PD Class shows the PDs class. Eight Classes are defined:

Class 1: Max. power 4.0 W	Class 5: Max. power 45.0 W
Class 2: Max. power 7.0 W	Class 6: Max. power 60.0 W
Class 3: Max. power 15.4 W	Class 7: Max. power 75.0 W
Class 4: Max. power 30.0 W	Class 8: Max. power 90.0 W

Power Requested: The requested amount of power the PD wants to be reserved.

Power Allocated: 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 (Low, High, or Critical).

Port Status: Shows the port's current PoE status. The status can be one of these values:

PoE turned ON - PoE is detected and enabled for this port.

PoE not available - No PoE chip found : PoE not supported for the port.

PoE turned OFF - PoE disabled : PoE is disabled administratively (by a 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.

Detecting PoE chipset : The switch has not yet detected the current PoE status for this port.

Total : At the bottom of the table a row displays with sums of the 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 immediately.

Port Status = Detecting PoE chipset: click Refresh to update page.

The screenshot shows the 'Power Over Ethernet Status' page for the SM24TBT2DPA switch. The interface includes a navigation menu on the left with options like Configuration, Monitor, System, Green Ethernet, Ports, DHCP, Security, Aggregation, Loop Protection, Spanning Tree, MVR, IPMC, LLDP, PoE, and MAC Table. The main content area has a title 'Power Over Ethernet Status' and a breadcrumb trail 'Home - Monitor - PoE'. Below the title is an 'Auto-refresh' checkbox and a refresh button. The table below shows the status of 11 ports, all of which are currently 'Detecting PoE chipset'.

Local Port	PD class	Power Requested	Power Allocated	Power Used	Current Used	Priority	Port Status
1	-	0 [W]	0 [W]	0 [W]	0 [mA]	Low	Detecting PoE chipset
2	-	0 [W]	0 [W]	0 [W]	0 [mA]	Low	Detecting PoE chipset
3	-	0 [W]	0 [W]	0 [W]	0 [mA]	Low	Detecting PoE chipset
4	-	0 [W]	0 [W]	0 [W]	0 [mA]	Low	Detecting PoE chipset
5	-	0 [W]	0 [W]	0 [W]	0 [mA]	Low	Detecting PoE chipset
6	-	0 [W]	0 [W]	0 [W]	0 [mA]	Low	Detecting PoE chipset
7	-	0 [W]	0 [W]	0 [W]	0 [mA]	Low	Detecting PoE chipset
8	-	0 [W]	0 [W]	0 [W]	0 [mA]	Low	Detecting PoE chipset
9	-	0 [W]	0 [W]	0 [W]	0 [mA]	Low	Detecting PoE chipset
10	-	0 [W]	0 [W]	0 [W]	0 [mA]	Low	Detecting PoE chipset
11	-	0 [W]	0 [W]	0 [W]	0 [mA]	Low	Detecting PoE chipset

3-13 MAC Table

Entries in the MAC Table are shown on this page. The MAC Table contains up to 8192 entries and is sorted first by VLAN ID, then by MAC address.

Each page shows up to 999 entries from the MAC table, default being 20, selected through the "entries per page" input field. When first visited, the web page will show the first 20 entries from the beginning of the MAC Table. The first displayed will be the one with the lowest VLAN ID and the lowest MAC address found in the MAC Table.

The "Start from MAC address" and "VLAN" input fields let you select the starting point in the MAC Table. Clicking the Refresh button will update the displayed table starting from that or the closest next MAC Table match. In addition, the two input fields will - upon a Refresh button click - assume the value of the first displayed entry, allowing for continuous refresh with the same start address.

The >> button will use the last entry of the currently displayed VLAN/MAC address pairs as a basis for the next lookup. When the end is reached the text "No more entries" is shown in the displayed table. Use the << button to start over.

To display the MAC Address Table in the web UI:

1. Click Monitor, Dynamic MAC Table.
2. Specify the VLAN and MAC Address.
3. View the MAC Address Table.

Figure 3- 12: MAC Address Table

			Port Members																										
Type	VLAN	MAC Address	CPU	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26
Static	1	00-09-18-4E-20-E9					✓																						
Static	1	00-16-6C-D4-DD-C2			✓																								
Static	1	00-C0-F2-7C-58-77	✓																										
Static	1	33-33-00-00-00-01	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Static	1	33-33-00-00-00-02	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Static	1	33-33-FF-7C-58-77	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Static	1	5C-FF-35-DC-0A-C1		✓																									
Static	1	AC-CC-8E-BA-F7-C1				✓																							
Static	1	FF-FF-FF-FF-FF-FF	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓

Parameter descriptions:

Type: Indicates whether the entry is a Static or a Dynamic entry.

VLAN: The VLAN ID of the entry.

MAC Address: The MAC address of the entry.

Port Members: The ports that are members of the entry have a green checkmark.

Buttons

Auto-refresh: Check this box to refresh the page automatically every 3 seconds.



Refresh: Refreshes the displayed table starting from the "Start from MAC address" and "VLAN" input fields.

Clear: Flushes all dynamic entries.

<< : Updates the table starting from the first entry in the MAC Table (i.e., the entry with the lowest VLAN ID and MAC address).

> : Updates the table, starting with the entry after the last entry currently displayed.

NOTE:

00-40-C7-73-01-29: your switch MAC address (for IPv4)

33-33-00-00-00-01: Destination MAC (for IPv6 Router Advertisement) (reference IPv6 RA.JPG)

33-33-00-00-00-02: Destination MAC (for IPv6 Router Solicitation) (reference IPv6 RS.JPG)

33-33-FF-73-01-29: Destination MAC (for IPv6 Neighbor Solicitation) (reference IPv6 DAD.JPG)

33-33-FF-A8-01-01: your switch MAC address (for IPv6 global IP)

FF-FF-FF-FF-FF-FF: for Broadcast.

3-14 VLANs

3-14.1 VLAN Membership

This page provides an overview of membership status of VLAN users. VLAN membership allows the frames classified to the VLAN ID to be forwarded on the respective VLAN member ports.

The VLAN Membership Status Page shows the current VLAN port members for all VLANs configured by a selected VLAN User (selection allowed by the Combo box). When "Combined" VLAN Users is selected, it shows this information for all the VLAN Users, and this is by default.

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 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. Clicking the >> 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. Click the << button to start over.

To view VLAN membership status in the web UI:

1. Click Monitor, VLANs, VLAN Membership.
2. At the Users dropdown choose which VLAN users to display.
3. Click Refresh to update the state.

Figure 3-14.1: VLAN Membership Status for Combined users

The screenshot shows the Lantronix web interface for the SM24TBT2DPB device. The main content area is titled "VLAN Membership Status for Combined users". It features a navigation menu on the left with options like Configuration, Monitor, System, Green Ethernet, Ports, DHCP, and Security. The main area includes an "Auto-refresh" checkbox, a refresh button, and a dropdown menu set to "Combined". Below this, there is a "Start from VLAN" input field set to "1" and "entries per page" set to "20". The main table displays the following data:

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	22	23	24	25	26
1	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓

Parameter descriptions:

VLAN user: Various internal software modules may use VLAN services to configure VLAN memberships on the fly. The drop-down list on the right allows for selecting between showing VLAN memberships as configured by an administrator (Admin) or as configured by one of these internal software modules.

The following VLAN user types are currently supported:

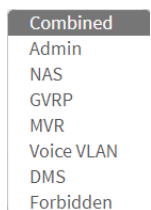
Combined: The "Combined" entry shows a combination of the administrator and internal software modules configuration, and basically reflects what is actually configured in hardware.

Admin: Only Admin users will be displayed.

NAS: NAS provides port-based authentication, which involves communications between a Supplicant, Authenticator, and an Authentication Server.

GVRP: Only GVRP users will be displayed.

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.



DMS: Only Diagnostic Monitoring Service users will be displayed.



Forbidden: Only forbidden users will be displayed.

VLAN ID: VLAN ID for which the Port members are displayed.

Port Members: A row of check boxes for each port is displayed for each VLAN ID.

 If a port is included in a VLAN, an image  will be displayed.

 If a port is included in a Forbidden port list, an image  will be displayed.

 If a port is included in a Forbidden port list and dynamic VLAN user register VLAN on same Forbidden port, then conflict port will be displayed as .

Buttons

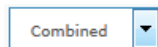


Auto-refresh: Check this box to refresh the page automatically every 3 seconds.

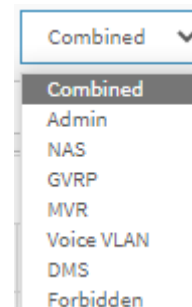
Refresh: Click to refresh the page immediately.

<<: Updates the system log entries to the first available entry ID.

>: Updates the system log entry to the next available entry ID.



: Select VLAN Users from this drop down list (shown right).



3-13.2 VLAN Port

The function Port Status gathers the information of all VLAN status and reports it in the order of Static, NAS, MVRP, MVP, Voice VLAN, MSTP, GVRP, Combined. To display VLAN Port Status in the web UI:

1. Click Monitor, VLANs, Ports.
2. At the dropdown, select the set of users to display (Combined, Admin, NAS, GVRP, MVR, Voice VLAN, MSTP, DMS, or VCL).
3. Display Port Status information.

Figure 3-13.2: VLAN Port Status for Combined users

Port	Port Type	Ingress Filtering	Frame Type	Port VLAN ID	Tx Tag	Untagged VLAN ID	Conflicts
1	C-Port	<input checked="" type="checkbox"/>	All	1	Untag PVID		No
2	C-Port	<input checked="" type="checkbox"/>	All	1	Untag PVID		No
3	C-Port	<input checked="" type="checkbox"/>	All	1	Untag PVID		No
4	C-Port	<input checked="" type="checkbox"/>	All	1	Untag PVID		No
5	C-Port	<input checked="" type="checkbox"/>	All	1	Untag PVID		No
6	C-Port	<input checked="" type="checkbox"/>	All	1	Untag PVID		No
7	C-Port	<input checked="" type="checkbox"/>	All	1	Untag PVID		No
8	C-Port	<input checked="" type="checkbox"/>	All	1	Untag PVID		No
9	C-Port	<input checked="" type="checkbox"/>	All	1	Untag PVID		No

Parameter descriptions:

VLAN USER: Various internal software modules may use VLAN services to configure VLAN memberships on the fly. The drop-down list on the right allows for selecting between showing VLAN memberships as configured by an administrator (Admin) or as configured by one of these internal software modules.

These VLAN User types are currently supported:

Combined: The "Combined" entry will show a combination of the administrator and internal software modules configuration, and basically reflects what is actually configured in hardware.

Admin: only Admin users will be displayed.

NAS: NAS provides port-based authentication, which involves communications between a Supplicant, Authenticator, and an Authentication Server.

GVRP: only GVRP users will be displayed.

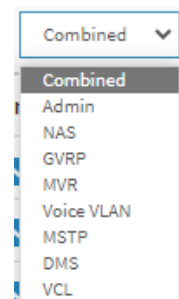
MVR: MVR is used to eliminate the need to duplicate multicast traffic for subscribers in each VLAN. Multicast traffic for all channels is sent only on a single (multicast) VLAN.

Voice VLAN: Voice VLAN is a VLAN configured specially for voice traffic typically originating from IP phones.

MSTP : only Multiple Spanning Tree Protocol users will be displayed.

DMS: Only Diagnostic Monitoring Service users will be displayed.

Forbidden: only VLAN Control List users will be displayed.



Port: The logical port for the settings contained in the same row.

Port Type: Shows the port type (Unaware, C-Port, S-Port, S-Custom-Port.) that a given user wants to configure on the port. The field is empty if not overridden by the selected user.

Ingress Filtering: Shows whether a given user wants ingress filtering enabled or not. The field is empty if not overridden by the selected user.

Frame Type: Shows the acceptable frame types (All, Tagged, Untagged) that a given user wants to configure on the port. The field is empty if not overridden by the selected user.

Port VLAN ID: Shows the Port VLAN ID (PVID) that a given user wants the port to have. The field is empty if not overridden by the selected user.

Tx Tag: Shows the Tx Tag requirements (Tag All, Tag PVID, Tag UVID, Untag All, Untag PVID, Untag UVID) that a given user has on a port. The field is empty if not overridden by the selected user.

Untagged VLAN ID: If Tx Tag is overridden by the selected user and is set to Tag or Untag UVID, then this field will show the VLAN ID the user wants to tag or untag on egress. The field is empty if not overridden by the selected user.

Conflicts: Two users may have conflicting requirements to a port's configuration. For instance, one user may require all frames to be tagged on egress while another requires all frames to be untagged on egress. Since both users cannot win, this gives rise to a conflict, which is solved in a prioritized way. The Administrator has the least priority. Other software modules are prioritized according to their position in the drop-down list: The higher in the list, the higher priority.

If conflicts exist, it will be displayed as "Yes" for the "Combined" user and the offending software module.

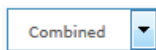
The "Combined" user reflects what is actually configured in hardware.

Buttons

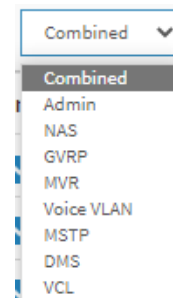


Auto-refresh: Check this box to refresh the page automatically every 3 seconds.

Refresh: Click to refresh the page immediately.



: Select VLAN Users from this drop down list (shown right).

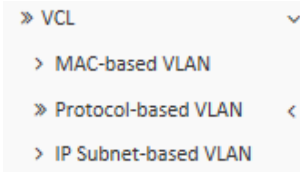


Messages: *No data exists for the selected user*

3-15 VCL

3-15.1 MAC-based VLAN

This page shows MAC-based VLAN entries configured by various MAC-based VLAN users. The following VLAN User types are currently supported:



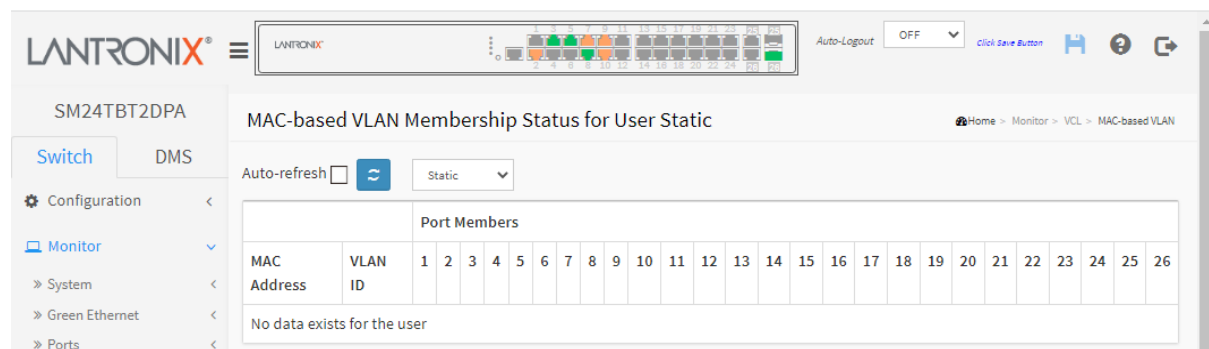
CLI/Web/SNMP: These are referred to as “Static” users.

NAS: NAS provides port-based authentication, which involves communications between a Supplicant, Authenticator, and an Authentication Server.

To display MAC-based VLAN configuration via the web UI:

1. Click Monitor, VCL, MAC-based VLAN.
2. At the dropdown specify the VLAN user type (Static, NAS, DMS, or Combined).
3. View the MAC-based information. A message displays if No data exists for the user.

Figure 3-15.1: MAC-based VLAN Membership Status for User Static



Parameter descriptions:

MAC Address: Indicates the MAC address.

VLAN ID: Indicates the VLAN ID.

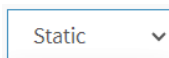
Port Members: Port members of the MAC-based VLAN entry.

Buttons

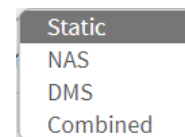


Auto-refresh : Check this box to refresh the page automatically every 3 seconds.

Refresh : Click to refresh the page immediately.



: Select VLAN Users from this drop down list (shown right).



3-15.2 Protocol-based VLAN

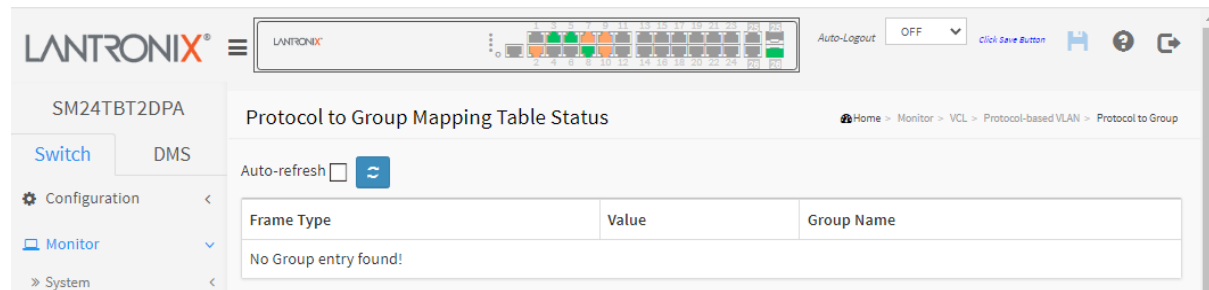
3-15.2.1 Protocol to Group

This page shows the protocols to Group Name (unique for each Group) mapping entries for the switch.

To display Protocol-based VLAN configuration in the web UI:

1. Click Monitor > VCL > Protocol-based VLAN > Protocol to Group.
2. Check "Auto-refresh".
3. Click "Refresh" to refresh the page data.

Figure 3-15.1.1: Protocol to Group Mapping Table Status page



Parameter descriptions:

Frame Type: Frame Type can have one of these values:

1. Ethernet
2. LLC
3. SNAP



NOTE:

On changing the Frame type field, the valid value of the following text field will vary depending on the new Frame Type you selected.

Value: Valid value that can be entered in this text field depends on the option selected from the preceding Frame Type selection menu. Below are the criteria for three different Frame Types:

Ethernet: Values in the text field when Ethernet is selected as a Frame Type is called etype. Valid values for etype ranges from 0x0600 - 0xffff

LLC: Valid value in this case is comprised of two different sub-values.

DSAP: 1-byte long string (0x00-0xff)

SSAP: 1-byte long string (0x00-0xff)

SNAP: Valid value in this case also is comprised of two different sub-values.

OUI: Organizationally Unique Identifier, in the format xx-xx-xx where each pair (xx) is a hexadecimal value ranges from 0x00-0xff.

PID: If the OUI is hexadecimal 000000, the protocol ID is the Ethernet type (EtherType) field value for the protocol running on top of SNAP; if the OUI is an OUI for a particular organization, the protocol ID is a value assigned by that organization to the protocol running on top of SNAP.

In other words, if value of OUI field is 00-00-00 then value of PID will be etype (0x0600-0xffff) and if value of OUI is other than 00-00-00 then valid value of PID will be any value from 0x0000 to 0xffff.

Group Name: A valid Group Name is a unique 16-character long string for every entry which consists of a combination of alphabet characters (a-z or A-Z) and integers (0-9).



NOTE: special characters and underscore (_) are not allowed.

Buttons

Auto-refresh: Check this box to refresh the page automatically every 3 seconds.

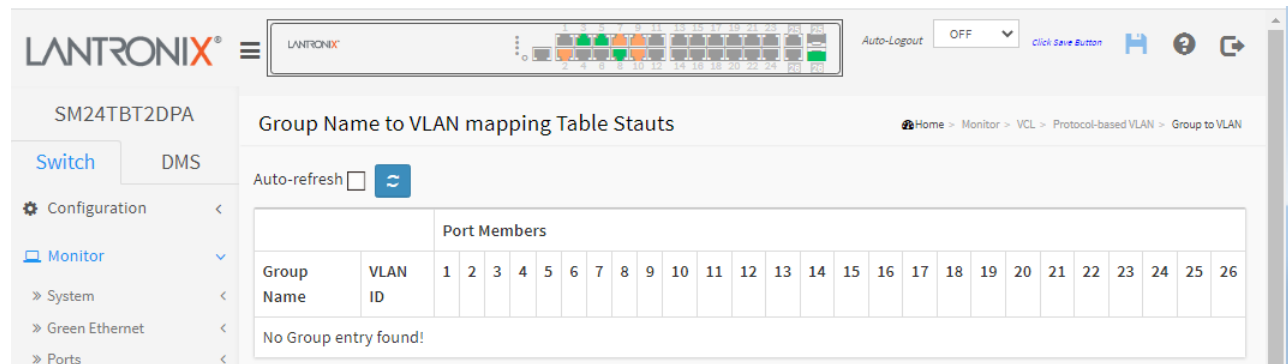
Refresh: Click to refresh the page immediately.

3-15.2.2 Group to VLAN

This page displays the configured Group Name to a VLAN for the switch. To display the Group to VLAN mapping in the web UI:

1. Click Monitor, VCL, Group to VLAN.
2. Check "Auto-refresh".
3. Click "Refresh" to refresh the port detailed statistics.

Figure 3-15.2.2: Group Name to VLAN mapping Table Status page



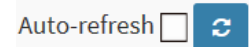
Parameter descriptions:

Group Name: A valid Group Name is a string at the most 16 characters consisting of a combination of alphabet characters (a-z or A-Z) and integers (0-9); no special characters are allowed. Whichever Group name you try, a map to a VLAN must be present in the Protocol to Group mapping table and must not be pre-used by any other existing mapping entry on this page.

VLAN ID: Indicates the ID to which Group Name will be mapped. A valid VLAN ID ranges from 1-4095.

Port Members: A row of check boxes for each port is displayed for each Group Name to VLAN ID mapping. To include a port in a mapping, check the box. To remove or exclude the port from the mapping, make sure the box is unchecked. By default, no ports are members, and all boxes are unchecked.

Buttons



Auto-refresh: Check this box to refresh the page automatically every 3 seconds.

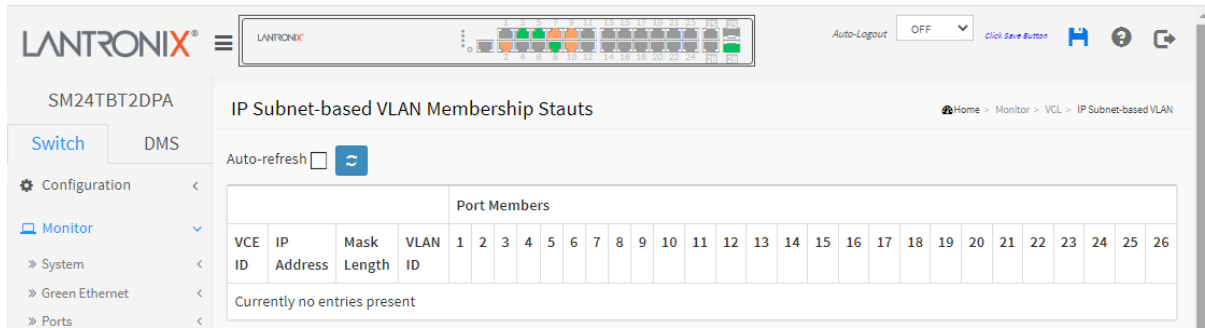
Refresh: Click to refresh the page immediately.

3-15.3 IP Subnet-based VLAN

This page shows IP subnet-based VLAN entries (only static entries). To display IP subnet-based VLAN configuration in the web UI:

1. Click Monitor, VCL, and IP Subnet-based VLAN.
2. Check “Auto-refresh”.
3. Click “Refresh” to refresh the port detailed statistics.

Figure 3-15.3: IP Subnet-based VLAN Membership Status page



Parameter descriptions:

VCE ID: Indicates the index of the entry. It is user configurable. Its value ranges from 0-128. If a VCE ID is 0, the switch will auto-generate the VCE ID for that entry. Deletion and lookup of IP subnet-based VLAN are based on VCE ID.

IP Address: Indicates the IP address.

Mask Length: Indicates the network mask length.

VLAN ID: Indicates the VLAN ID. VLAN ID can be changed for the existing entries.

Port Members: A row of check boxes for each port is displayed for each IP subnet-based VLAN entry. To include a port in an IP subnet-based VLAN, check the box. To remove or exclude the port from the IP subnet-based VLAN, make sure the box is unchecked. By default, no ports are members, and all boxes are unchecked.

Buttons

Auto-refresh: Check this box to refresh the page automatically every 3 seconds.

Refresh: Click to refresh the page immediately.

3-16 sFlow

This page shows receiver and per-port sFlow statistics. To display sFlow Statistics in the Web UI:

1. Click Monitor, sFlow.
2. View sFlow information.
3. Use the buttons as needed.

Figure 3-16: sFlow Statistics page

The screenshot displays the sFlow Statistics page in the Lantronix Web UI. The page is titled "sFlow Statistics" and includes a navigation menu on the left with options like Configuration, Monitor, and Diagnostics. The main content area is divided into two sections: Receiver Statistics and Port Statistics.

Receiver Statistics

Owner	<none>
IP Address/Hostname	0.0.0.0
Timeout	0
Tx Successes	0
Tx Errors	0
Flow Samples	0
Counter Samples	0

Port Statistics

Port	Rx Flow Samples	Tx Flow Samples	Counter Samples
1	0	0	0
2	0	0	0
3	0	0	0
4	0	0	0
5	0	0	0
6	0	0	0
7	0	0	0

Receiver Statistics

Owner: This field shows the current owner of the sFlow configuration. It assumes one of three values:

1. If sFlow is currently unconfigured/unclaimed, Owner contains <none>.
2. If sFlow is currently configured through Web or CLI, Owner contains <Configured through local management>.
3. If sFlow is currently configured through SNMP, Owner contains a string identifying the sFlow receiver.

IP Address/Hostname: The IP address or hostname of the sFlow receiver.

Timeout: The number of seconds remaining before sampling stops and the current sFlow owner is released.

Tx Successes: The number of UDP datagrams successfully sent to the sFlow receiver.

Tx Errors: The number of UDP datagrams that has failed transmission. The most common source of errors is invalid sFlow receiver IP/hostname configuration. To diagnose, paste the receiver's IP address/hostname into the Ping Web page (Diagnostics > Ping > Ping6).

Flow Samples: The total number of flow samples sent to the sFlow receiver.

Counter Samples: The total number of counter samples sent to the sFlow receiver.

Port Statistics

Port: The port number for which the following statistics applies.

Rx and Tx Flow Samples: The number of flow samples sent to the sFlow receiver originating from this port. Here, flow samples are divided into Rx and Tx flow samples, where Rx flow samples contains the number of packets that were sampled upon reception (ingress) on the port and Tx flow samples contains the number of packets that were sampled upon transmission (egress) on the port.

Counter Samples: The total number of counter samples sent to the sFlow receiver originating from this port.



Buttons

Auto-refresh: Check this box to refresh the page automatically every 3 seconds.

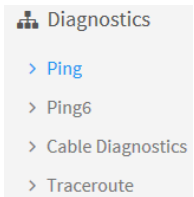
Refresh: Click to refresh the page immediately.

Clear Receiver: Clears the sFlow receiver counters.

Clear Ports: Clears the per-port counters.

Chapter 4 - Diagnostics

This chapter describes the system diagnostics that let you know if the system is healthy or needs to be fixed. The diagnostics include ICMP Ping, Ping6, Cable Diagnostics, and Traceroute.

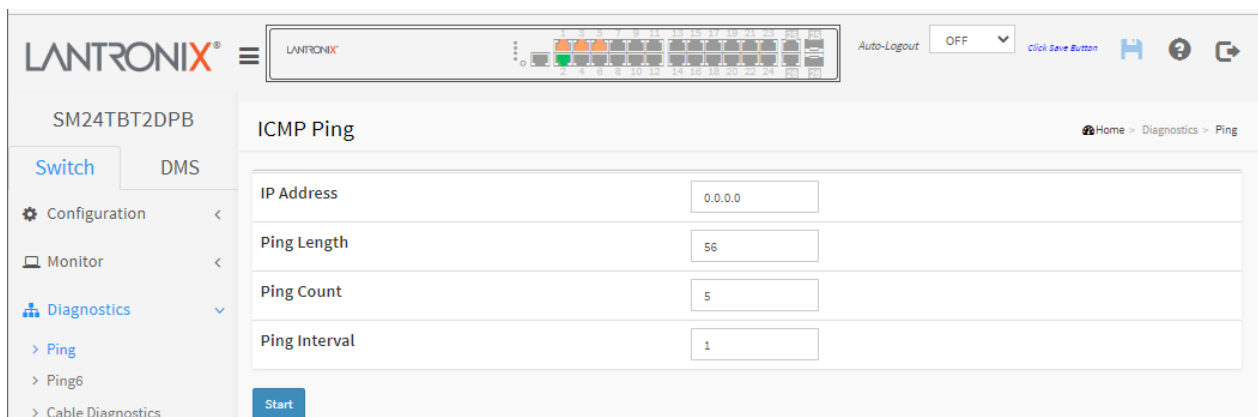


4-1 Ping

This page lets you issue ICMP PING packets to troubleshoot IP connectivity issues. To configure an ICMP PING in the web UI:

1. Navigate to Switch > Diagnostics > Ping.
2. Specify ICMP PING IP Address.
3. Specify ICMP PING Size.
4. Click Start.

Figure 4-1: ICMP Ping page



Parameter descriptions:

IP Address: Set the IP Address of the device you want to ping.

Ping Length: The payload size of the ICMP packet. Valid values range are 2 - 1452 bytes.

Ping Count: The count of the ICMP packet. Valid values are 1 time - 60 times.

Ping Interval: The interval of the ICMP packet. Valid values are 0 - 30 seconds.

Start: Click the **Start** button and the switch will start to ping the device using ICMP packet size what set on the switch. ICMP packets are transmitted, and the sequence number and round trip time are displayed upon reception of a reply. The amount of data received inside of an IP packet of type ICMP ECHO_REPLY will always be 8 bytes more than the requested data space (the ICMP header). The page refreshes automatically until responses to all packets are received, or until a timeout occurs.

```

PING server 10.10.132.20, 56 bytes of data.
64 bytes from 10.10.132.20: icmp_seq=0, time=0ms
64 bytes from 10.10.132.20: icmp_seq=1, time=0ms
64 bytes from 10.10.132.20: icmp_seq=2, time=0ms
64 bytes from 10.10.132.20: icmp_seq=3, time=0ms
64 bytes from 10.10.132.20: icmp_seq=4, time=0ms
Sent 5 packets, received 5 OK, 0 bad
  
```

4-2 Ping6

This page lets you issue ICMPv6 PING packets to troubleshoot IPv6 connectivity issues. To configure an ICMPv6 Ping in the web UI:

1. Navigate to Diagnostics > Ping6.
2. Specify ICMPv6 IP Address, Ping Length, Ping Count, Ping Interval, and Egress Interface.
3. Click Start.

Figure 4-2: ICMPv6 Ping page

Parameter descriptions: You can configure the properties of the issued ICMP packets:

IP Address: The destination IP Address with IPv6

Ping Length: The payload size of the ICMP packet. Values range from 2 bytes to 1452 bytes.

Ping Count: The count of the ICMP packet. Values range from 1 time to 60 times.

Ping Interval: The interval of the ICMP packet. Values range from 0 second to 30 seconds.

Egress Interface: The VLAN ID of the specific egress IPv6 interface where ICMP packet goes. The VID range is 1 - 4094 and will be effective only when the corresponding IPv6 interface is valid. When the egress interface is not given, PING6 finds the best match interface for destination. Do not specify egress interface for loopback address. Do specify egress interface for link-local or multicast address.

Start: Click the **Start** button and the switch will start to ping the device using ICMPv6 packet size what set on the switch. ICMPv6 packets are transmitted, and the sequence number and round trip time are displayed upon reception of a reply. The page refreshes automatically until responses to all packets are received, or until a timeout occurs.

```

PING6 server ff02::2, 56 bytes of data.
64 bytes from fe80::219:5bff:fe2f:b47: icmp_seq=0, time=10ms
64 bytes from fe80::215:58ff:feed:69dd: icmp_seq=0, time=10ms
64 bytes from fe80::219:5bff:fe2f:b47: icmp_seq=1, time=0ms
64 bytes from fe80::215:58ff:feed:69dd: icmp_seq=1, time=0ms
64 bytes from fe80::219:5bff:fe2f:b47: icmp_seq=2, time=0ms
64 bytes from fe80::215:58ff:feed:69dd: icmp_seq=2, time=0ms
64 bytes from fe80::219:5bff:fe2f:b47: icmp_seq=3, time=0ms
64 bytes from fe80::215:58ff:feed:69dd: icmp_seq=3, time=0ms
64 bytes from fe80::219:5bff:fe2f:b47: icmp_seq=4, time=0ms
64 bytes from fe80::215:58ff:feed:69dd: icmp_seq=4, time=0ms
Sent 5 packets, received 10 OK, 0 bad
  
```

4-3 Cable Diagnostics

This page is used for running the Cable Diagnostics for 10/100 and 1G copper ports.

Press Start to run the diagnostics. This will take approximately 5 seconds. When completed, the page refreshes automatically, and you can view the cable diagnostics results in the cable status table. Note that Cable Diagnostic is only accurate for cables of length 7 - 120 meters with 5-meter accuracy.

The 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.

Web Interface

To run a Cable Diagnostics check via the web UI:

1. Navigate to Diagnostics > Cable Diagnostics.
2. At the Port dropdown, specify the Copper Port which you want to check.
3. Click the Start button. If a webpage message displays, click OK to continue.

Figure 4-3: Cable Diagnostics page

Copper Port	Link Status	Test Result	Length
1	100M	OK	3(m)
2	1G	OK	3(m)
3	100M	detect error or check cable length is between 7-120 meters	
4	Cable Diagnostics is running...		

Parameter descriptions:

Port: At the Port dropdown, select the port for which you are requesting Cable Diagnostics.

Copper Port: The Copper Port number to test.

Link Status: The status of the cable:

10M: Cable is link up and correct. Speed is 10Mbps

100M: Cable is link up and correct. Speed is 100Mbps

1G: Cable is link up and correct. Speed is 1Gbps

Link Down: Link down or cable is not correct.

Test Result: Test Result of the cable:

OK: Correctly terminated pair

Abnormal: Incorrectly terminated pair or link down

Length: The length (in meters) of the cable pair. The resolution is 3 meters. When Link Status is shown as follows, the length has different definition.

1G: The length is the minimum value of 4-pair.

10M/100M: The length is the minimum value of 2-pair.

Link Down: The length is the minimum value of non-zero of 4-pair.

Message: After you select a copper port and click **Start**, the following message displays:

10 and 100 Mbps ports will be linked down and lost connection while running Cable Diagnostics.

Are you sure to continue?

Note that Diagnostics is only accurate for cables of length 1 – 120 meters.

Verify that you want to continue and click the **OK** button to continue. Otherwise click **Cancel**.

The message “Cable Diagnostic is running...” displays while the test is running.

Example:

The screenshot shows the Lantronix web interface for the SM24TBT2DPB device. The main content area is titled "Cable Diagnostics" and includes a "Port" dropdown menu set to "6" and a "Start" button. Below this is a table with the following data:

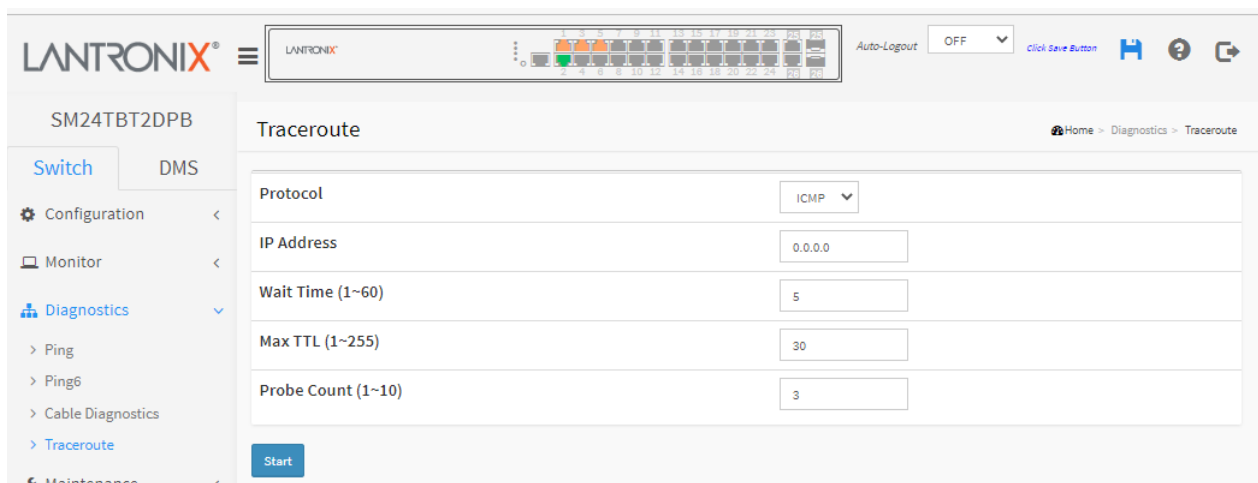
Copper Port	Link Status	Test Result	Length
1	1G	OK	3(m)
2	100M	OK	3(m)
3	100M	detect error or check cable length is between 7-120 meters	
4	100M	OK	3(m)
5	100M	OK	6(m)
6	Link Down	detect error or check cable length is between 7-120 meters	

4-4 Traceroute

This page lets you issue ICMP, TCP, or UDP packets to diagnose network connectivity issues. To configure an ICMPv6 PING in the web UI:

1. Navigate to Diagnostics > Traceroute.
2. Specify Traceroute Protocol, IP Address, Wait Time, Max TTL, and Probe Count.
3. Click Start.

Figure 4-4: Traceroute page



Parameter descriptions:

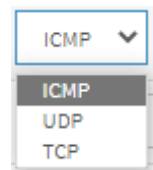
Protocol: At the dropdown select the protocol (ICMP, UDP, or TCP) to send packets.

IP Address: Enter the destination IP Address.

Wait Time: Set the time (in seconds) to wait for a response to a probe (default 5.0 seconds). Valid values are 1 - 60.

Max TTL: Specify the maximum number of hops (max time-to-live value) traceroute will probe. Valid values are 1-255 seconds. The default is 30 seconds.

Probe Count: Sets the number of probe packets per hop. Valid values are 1-10 packets. The default is 3 packets.



Buttons

Start : Click to begin the Traceroute.

New Traceroute : Click the button to end the Traceroute.

When the parameters are entered, click the **Start** button to begin the Traceroute.

Observe the Traceroute Output:



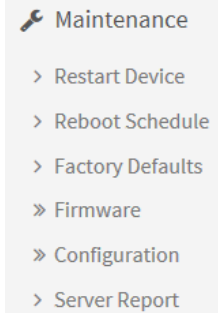
Click the **New Traceroute** button to end the Traceroute.

Traceroute Output

```
traceroute to 0.0.0.0 (0.0.0.0), 30 hops max, 40 byte packets
1 * * *
2 * * *
3 * * *
4 * * *
5 * * *
6 * * *
7 * * *
8 * * *
9 * * *
10 * * *
11 * * *
12 * * *
13 * * *
14 * * *
15 * * *
16 *
```


Chapter 5 - Maintenance

This chapter describes the switch Maintenance configuration tasks, including Restart Device, Reboot Schedule, Factory Defaults, Firmware Upgrade, Configuration, and Server Report.

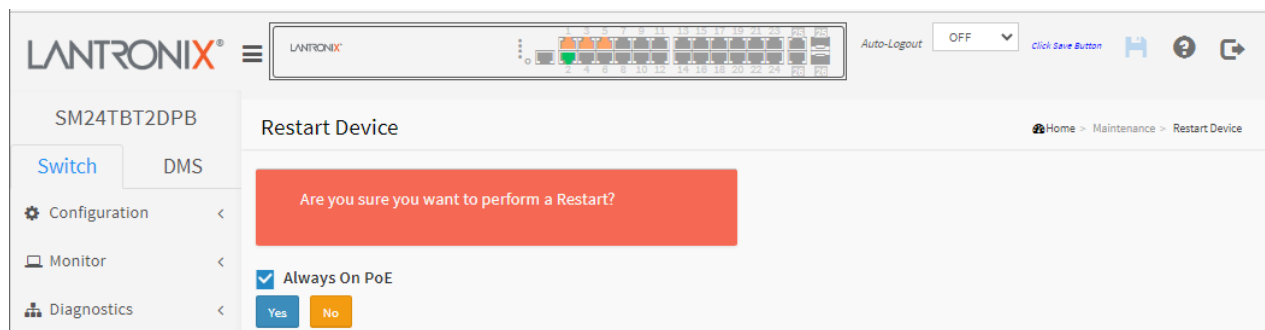


5-1 Restart Device

You can restart the on this page. After restart, the switch will boot normally. To Restart the switch in the web UI:

1. Click Maintenance, Restart Device.
2. Check or uncheck the Always On PoE checkbox as desired.
3. At the “Are you sure..?” prompt, select an option if desired, and then click Yes.

Figure 5-1: Restart Device page



Parameter descriptions:

Note: SM24TBT2DPA FW v6.54.3104 removed the Force Cool Restart checkbox from this page.

Always On PoE: If you check this button, during switch warm restart, it will continue providing PoE power to the PDs. **Note 1:** It will take 75 - 80 seconds to have PoE++ power on the ports to power PDs again if the switch makes a cold restart. The "Always on PoE" feature has no effect on this time.

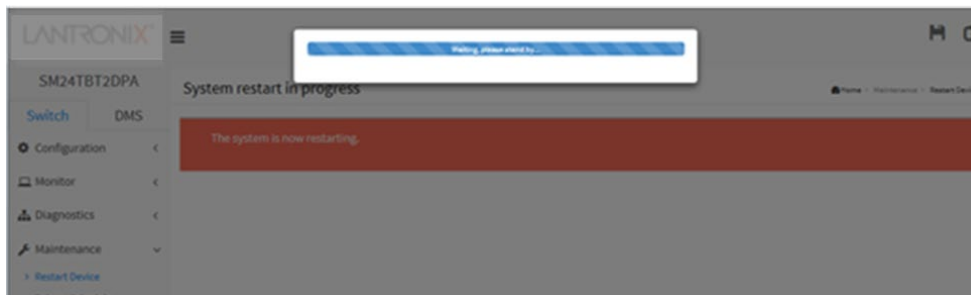
Note 2: The “Ultra-fast PoE” feature improves PoE startup time; it provides PoE output to attached PDs within five seconds after a cold start.

Buttons:

Yes: Click to restart the device.

No: Click to return to the Port State page without restarting.

Wait while the Restart occurs:



Wait a couple of minutes. If necessary, refresh the Browser and log back in to the switch.

5-2 Reboot Schedule

This page lets you schedule the day and time to reboot the switch. To set the switch Reboot Schedule in the web UI:

1. Click Maintenance, Reboot Schedule.
2. At the Mode dropdown select Enabled to display the reboot schedule parameters.
3. Enter the reboot schedule parameters and click Apply.

Figure 5-2: Switch Reboot Schedule page

The screenshot shows the 'Switch Reboot Schedule' configuration page in the Lantronix web UI. The page title is 'Switch Reboot Schedule' and the mode is set to 'Enabled'. The configuration is as follows:

Week Day	Reboot Time	
	HH	MM
*	<>	<>
Monday	12	55
Tuesday	1	0
Wednesday	-	-
Thursday	-	-
Friday	-	-
Saturday	-	-
Sunday	-	-

Buttons: Apply (blue), Reset (orange)

Parameter descriptions:

Mode: Indicates the reboot scheduling mode operation. Possible modes are:

Enabled: Enable switch reboot scheduling.

Disabled: Disable switch reboot scheduling (default).

Week Day: The day to reboot this switch.

Reboot Time: The time to reboot the switch in hours (HH) and minutes (MM).

Buttons

Apply: Click to save changes.

Reset: Click to undo any changes made locally and revert to previously saved values.

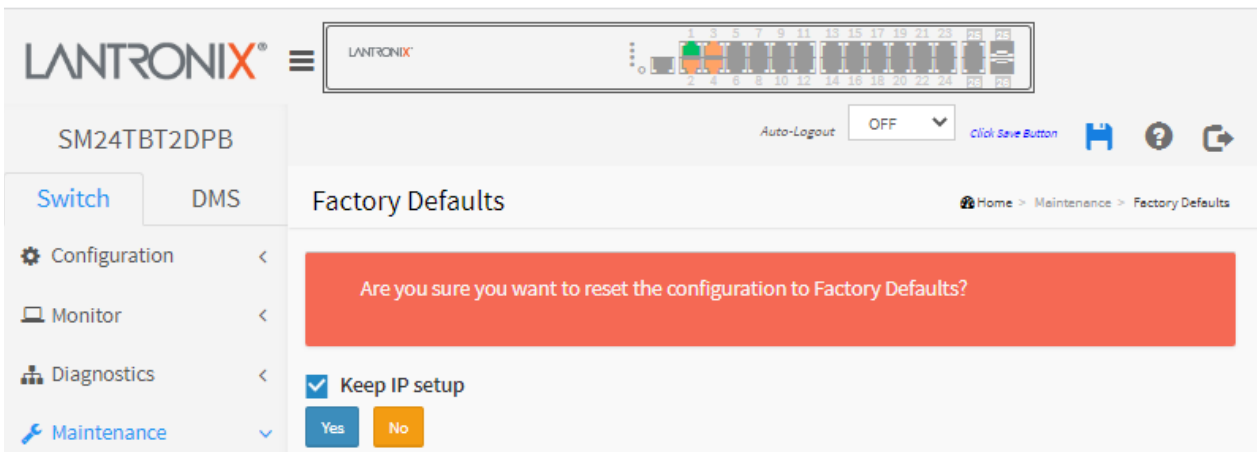
5-3 Factory Defaults

You can reset the configuration of the switch on this page. The IP configuration is retained if desired. The new configuration is available immediately (no restart is necessary).

To reset the switch to Factory Defaults in the web UI:

1. Click Maintenance, Factory Defaults.
2. Check the "Keep IP setup" checkbox if you want to retain the current VLAN1 IP setting.
3. At the "Are you sure..?" prompt, click Yes.

Figure 5-3: Factory Defaults page



Parameter descriptions:

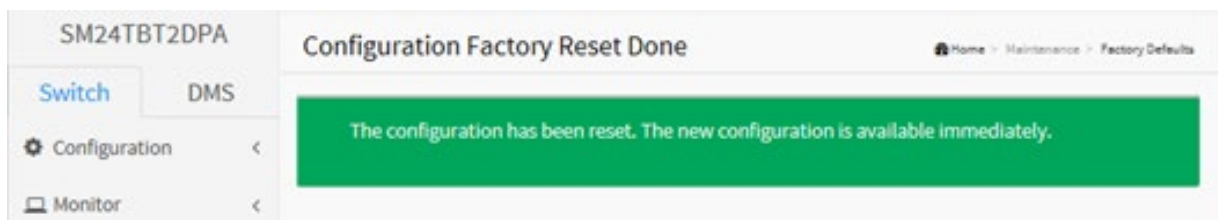
Keep VLAN1 IP setup: Check the checkbox if you want to keep the current VLAN1 IP setting.

Yes: Click to reset the configuration to Factory Defaults.

No: Click to return to the Port State page without resetting the configuration.

Note: Restoring factory defaults 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 values.

When the configuration has been reset, the new configuration is available immediately.



Click any menu item and log back in to continue.

5-4 Firmware

This section describes how to upgrade Firmware. The switch can be enhanced with more value-added functions by installing firmware upgrades.

5-4.1 Firmware Upgrade

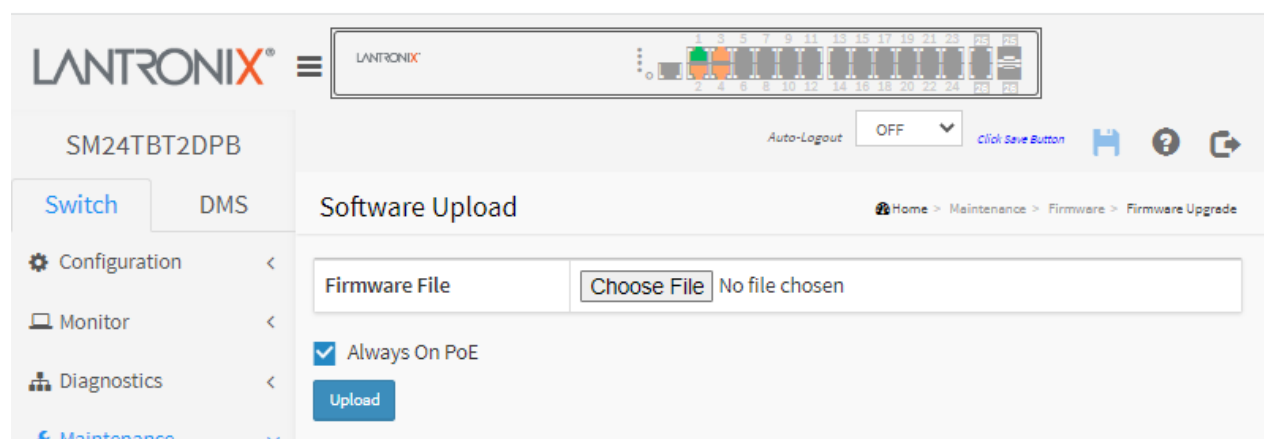
The Software Upload page facilitates an update of the firmware controlling the switch. To perform a Firmware Upgrade via the web UI:

1. Navigate to Maintenance > Firmware > Firmware Upgrade.
2. Click **Choose File** to browse to and select the firmware file to upgrade your switch.
3. Check the Always On PoE software upload option as required.
4. Click the Upload button.
5. 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 lost. The green front panel LED flashes at 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.

Figure 5-3.1 Software Upload page



Parameter descriptions:

Choose File: Click the button to search for the Firmware filename to be uploaded. The file format is "VB6.64.0123/SM24TBT2DPB_SYS_VB6.64.0123".

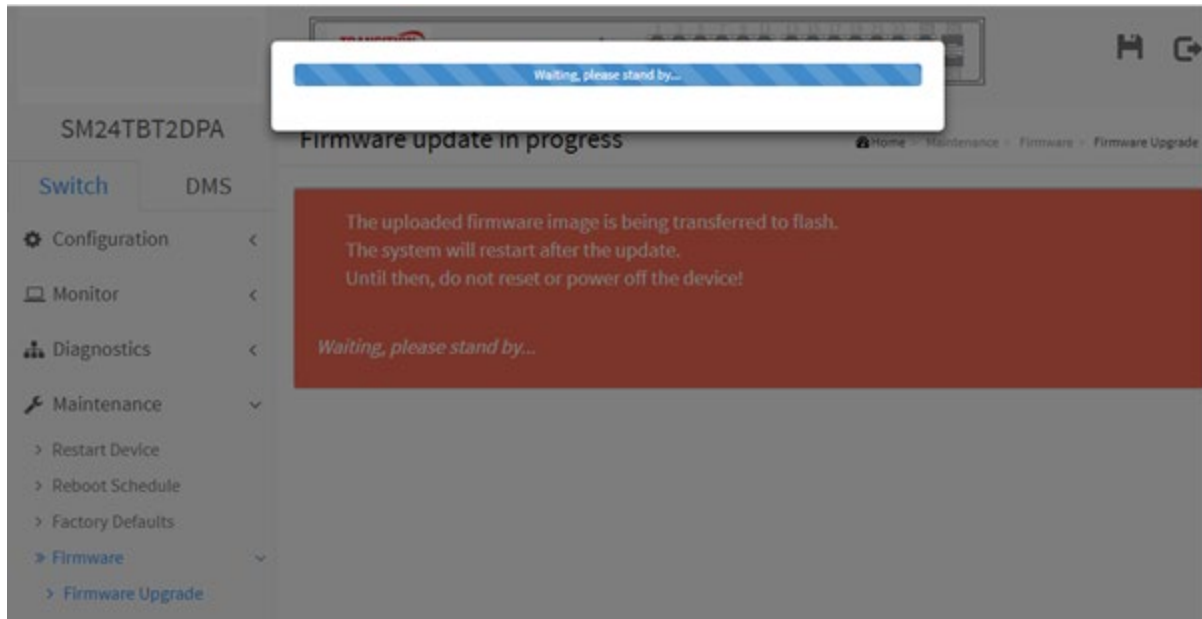
Note: SM24TBT2DPA FW v6.54.3104 removed the Force Cool Restart checkbox from this page.

Always On PoE: Check this button, then during the switch warm restart, it will continue providing PoE power to the PDs. **Note 1:** It will take 75 - 80 seconds to have PoE++ power on the ports to power PDs again if the switch makes a cold restart. The "Always on PoE" feature has no effect on this time.

Note 2: The "Ultra-fast PoE" feature improves PoE startup time; it provides PoE output to attached PDs within five seconds after a cold start.

Upload: Click to start the software upload process.

The Firmware update in progress screen is shown below.



When the Firmware update successfully completes, the startup page (**Monitor > System > Information**) displays.

Message: *Firmware/EZCM Upgrade Result*

The EZCM files are successfully updated.

The uploaded firmware image is invalid. Please use a correct firmware image.

Rebooting system!

Meaning: The Firmware update failed due to an invalid firmware file.

Recovery: When the message clears and the switch has rebooted, click away from the current menu path, log back in to the switch web UI, and then try the firmware upgrade again with a valid firmware filename.

Message: *Firmware upgrade in progress*

The system will restart after the update.

Until then, do not reset or power off the device!

Erasing, please stand by...

Meaning: When the Firmware upgrade is done, the last line of the message changes to “*Completed!*”.

Recovery: You may need to refresh the web page to clear the “*Completed!*” message.

Firmware Upgrade to **SM24TBT2DPA FW v6.54.3303**

To perform a Firmware Upgrade to FW v6.54.3303 via the web UI:

The recommended upgrade procedure is to upgrade from v6.54.3104 to v6.54.3303B and then to v6.54.3303.

1. Navigate to Maintenance > Firmware > Firmware Upgrade.
2. Click Choose File to browse to and select the firmware file v6.54.3303B to upgrade your switch.
3. Select the Non-Stop PoE / Always On PoE software upload option as required.
4. Click the Upload button and wait for the upgrade to complete.
5. Verify the upgrade succeeded; see “[Firmware Selection](#)” below.
6. Repeat steps 2-5 for FW v6.54.3303.

Firmware Upgrade to FW vB6.54.3494

Once you upgrade the SM24TBT2DPA to FW vB6.54.3494, you can't fall back to the old FW version. This is because the FW upgrade includes a PoE FW upgrade to support the IEEE 802.3bt standard, so you can't downgrade to an old FW version.

PoE Mode setting between v6.54.3303 with vB6.54.3476 (and newer)

v6.54.3303	vB6.54.3476
Disabled	Disabled
Enabled (*)	4pair90w
4pair	4pair60w
2pair	8023bt (*)

Notes:

1. The PoE mode setting will be mapped according to the table above after firmware upgrade.
2. It's not allowed to downgrade to v6.54.3303 or older version after firmware upgrade to vB6.54.3476 or newer version.
3. It's not allowed to swap firmware image when the back image is v6.54.3303 or older version.

5-3.2 Firmware Selection

This page provides information about the active and alternate (backup) firmware images in the device and lets you revert to the alternate image. The page displays two tables with information about the active and alternate firmware images. **Note:**

1. If the active firmware image is the alternate image, only the "Active Image" table is shown. In this case, the Activate Alternate Image button is also disabled.
2. If the alternate image is active (due to a corruption of the primary image or by manual intervention), uploading a new firmware image to the device will automatically use the primary image slot and activate this.
3. The firmware version and date information may be empty for older firmware releases. This does not constitute an error.

To swap Firmware images in the web UI:

1. At Maintenance > Firmware > Firmware Selection verify the displayed version.
2. If desired, check the Always On PoE checkbox.
3. Click the Activate Alternate Image button.

Figure 5-3.2 Software Image Selection page

Active Image	
Image	managed
Version	SM24TBT2DPB (standalone) VB6.64.0123
Date	2024-05-27T17:24:27+08:00

Alternate Image	
Image	managed.bk
Version	SM24TBT2DPB (standalone) VB6.64.0117
Date	2023-12-14T11:09:25+08:00

Image: The flash index name of the firmware image. The name of the active (current) image is *managed*, the alternate image is named *managed.bk*.

Version: The version of the firmware image (e.g., *SM24TBT2DPB (standalone) VB6.64.0123*).

Date: The date and time when the firmware was produced (e.g., *2024-05-27T16:02:35+08:00*).

Always On PoE : check the box For the switch to maintain PoE power to PDs during software operation. If you check this button, when the switch warm restarts, it will continue providing PoE power to the PDs.

Note 1: It takes 75 - 80 seconds to have PoE++ power on the ports to power PDs again if the switch makes a cold restart. The "Always on PoE" feature has no effect on this time. **Note 2:** The "Ultra-fast PoE" feature improves PoE startup time; providing PoE output to attached PDs within 5 seconds after a cold start.

Buttons:

Activate Alternate Image: Click to activate the "Alternate Image". This button may be disabled depending on system state.

Cancel: Cancels activating the backup image and navigates to the Monitor > System > Information page.

5-4 Configuration

- » Configuration
 - > Save startup-config
 - > Download
 - > Upload
 - > Activate
 - > Delete

This section lets you save, download, upload, activate, and/or delete a config file.

The switch stores its configuration in a number of text files in CLI format. The files are either virtual (RAM-based) or stored in flash on the switch. The system files 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.

default-config: A read-only file with vendor-specific configuration. This file is read when the system is restored to default settings.

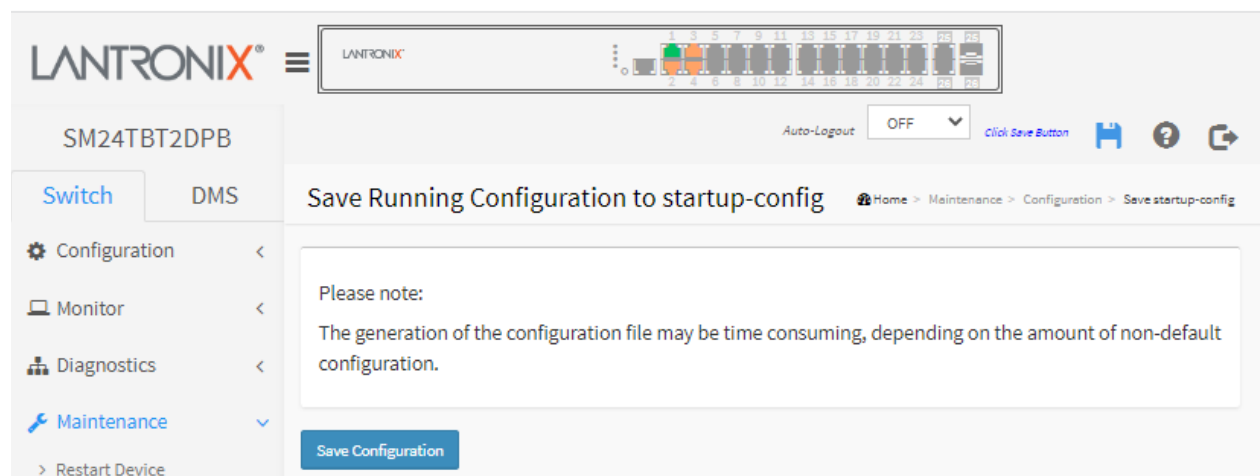
It is also possible to store up to two other files and apply them to running-config, thereby switching configuration. **Note:** The generation of the configuration file may be time consuming, depending on the amount of non-default configuration.

5-4.1 Save startup-config

This copies the running-config to startup-config, thereby ensuring that the currently active configuration will be used at the next reboot. To save the running configuration in the web UI:

1. Navigate to Switch > Maintenance > Configuration > Save Startup-config.
2. Click the Save Configuration button.

Figure 5-4.1: Save Startup Configuration page



Buttons:

Save Configuration: Click to save configuration; the running configuration will be written to flash memory for system boot up to load this startup configuration file.

Messages:

*Save Running Configuration to startup-config
startup-config saved successfully.*

5-4.3 Download

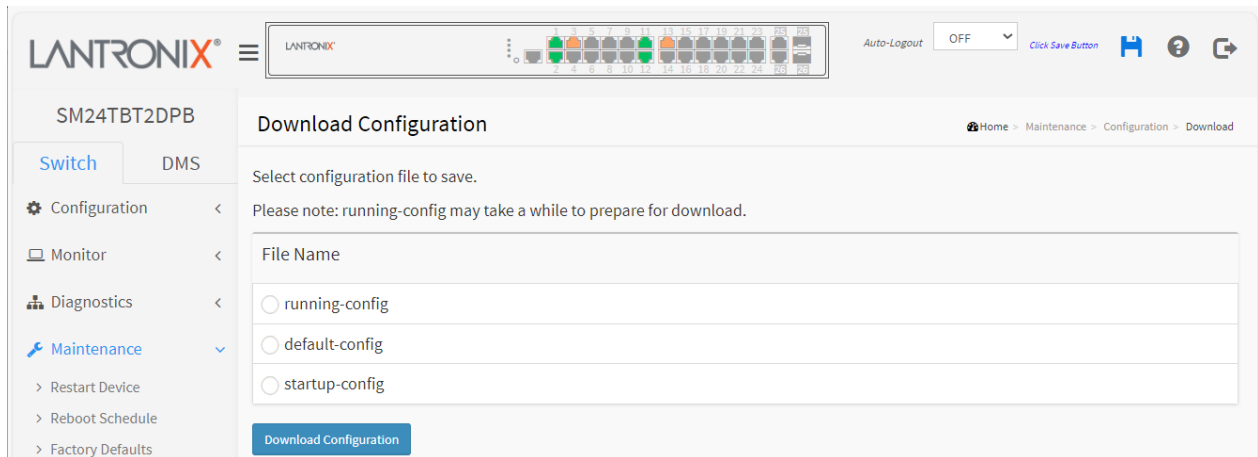
It is possible to download any of the files on the switch to the web browser. Select the file and click the Download Configuration button.

Download of running-config may take a little while to complete, as the file must be prepared for download.

To download a configuration file in the web UI:

1. Select the Configuration file to save.
2. Click the Download Configuration button.
3. Click the Apply button.
4. Select Open, Open Folder, or View Downloads.

Figure 5-4.2: Configuration Download page



Parameter descriptions: The system files are:

running-config: A virtual file that represents the currently active configuration on the switch. This file is volatile.

default-config: A read-only file with vendor-specific configuration. This file is read when the system is restored to default settings.

startup-config: The startup configuration for the switch, read at boot time.

Buttons:

Download Configuration: Select the file and click the **Download Configuration** button.

Prompts:



5-4.2 Upload

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. If the destination is running-config, the file will be applied to the switch configuration. This can be done in two ways:

Replace: The current configuration is fully replaced with the configuration in the uploaded file.

Merge: The uploaded file is merged into running-config.

If the file system is full (i.e., contains the three system files mentioned above plus two other files), it is not possible to create new files, but an existing file must be overwritten or another deleted first.

To upload a configuration in the web UI:

1. Navigate to Switch > Maintenance > Configuration > Upload.
2. Browse to and select the file to upload.
3. Select the destination file on the target.
4. For the running-config file select *Replace* or *Merge*.
5. Click the Upload Configuration button.

Figure 5-4.3: Upload Configuration page

File Name	Parameters
<input type="radio"/> running-config	<input checked="" type="radio"/> Replace <input type="radio"/> Merge
<input type="radio"/> startup-config	
<input type="radio"/> Create new file	<input type="text"/>

Parameter descriptions: The system 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.

Create new file: Select and enter a filename to upload.

Buttons

Upload Configuration: Click then the running web management PC will start to upload the configuration from the managed switch configuration into the location PC; you can configure web browser's upload file path to keep the configuration file.

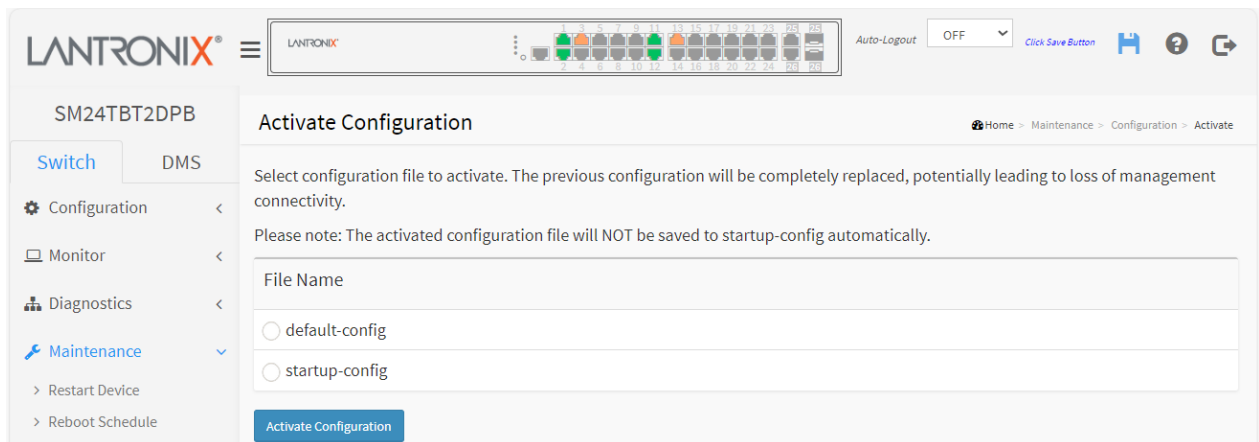
5-4.4 Activate

It is possible to activate any of the configuration files present on the switch, except for `running-config` which represents the currently active configuration.

To activate a configuration in the web UI:

1. Select the configuration file to activate (*default-config* or *startup-config*).
2. 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.

Figure 5-4.4: Activate Configuration page



Parameter descriptions: The system files are:

default-config: A read-only file with vendor-specific configuration. This file is read when the system is restored to default settings.

startup-config: The startup configuration for the switch, read at boot time.

Buttons:

Activate Configuration: Click the button and the *default-config* or *startup-config* file will be activated and will become this switch's running configuration.

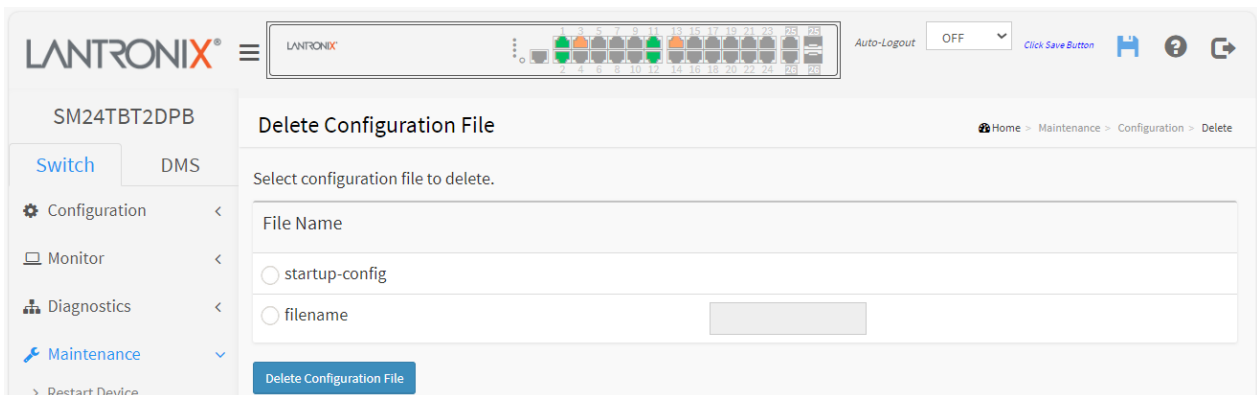
5-4.5 Delete

It is possible to delete any of the writable files stored in flash, including startup-config. If this is done and the switch is rebooted without a prior Save operation, this effectively resets the switch to its default configuration.

To delete a configuration file via the web UI:

1. Navigate to Maintenance > Configuration > Delete.
2. Select *startup-config* or select the *filename* radio button and enter a filename to be deleted.
3. Click the **Delete Configuration File** button.
4. At the *Are you sure...?* prompt, select **Yes** to delete the file.

Figure 5-4.5: Delete Configuration File page



Parameter descriptions:

File Name: There is one system file and one optional file selection:

startup-config: The startup configuration for the switch, read at boot time.

filename: select the radio button and enter a valid (existing) filename to be deleted.

Buttons:

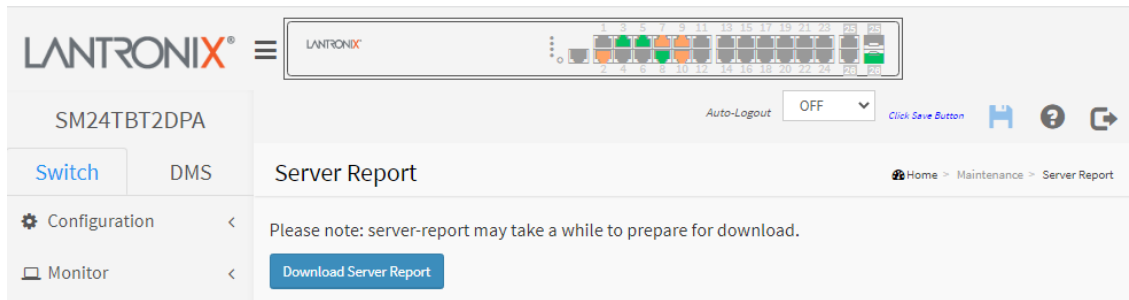
Delete Configuration File: Click this button to delete the startup-config file; this effectively resets the switch to its default configuration.

5-5 Server Report

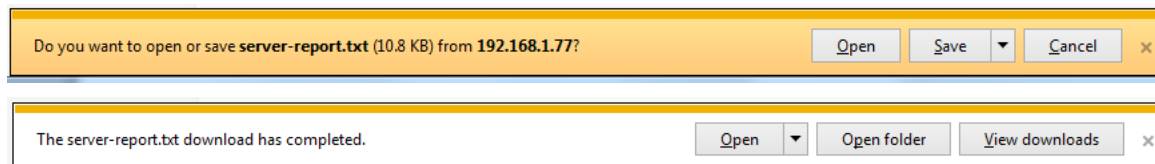
You can download a system report file on the switch to the web browser. The *Server Report* includes system overview, running-config and log information. A download of *system-report* may take a little while to complete, as the file must be prepared for download.

1. Navigate to Switch > Maintenance > Server Report menu path.
2. Click the Download Server Report button.
3. Select Open, Save, or Cancel. If you select Open, the file opens in MS Word.
If you select Save, you have the options to Open, Open folder, or View downloads.

Figure 5-5.1: Server Report page



Messages:



A server report includes sections of information such as System Overview (Connected Devices, PoE Power Consumption, Total PoE Available, etc.), running-config, System log, System info, PoE config, PoE status, Port status, and Port statistics.

5-4.5 Sample Downloaded Server Report Page

```

server-report - Notepad
File Edit Format View Help
----- System Overview -----
Model Name: SM24TBT2DPA
Connected Devices: 0
PoE Power Consumption: 0 [W]
Total PoE Available: 820 [W]

Firmware Version: v6.54.2776 2018-01-31
MAC Address: 00-c0-f2-49-38-6a
System Uptime: 00:45:53

IP Address: 192.168.1.77
Subnet Mask: 255.255.255.0
Gateway: 192.168.1.254
Primary DNS: 8.8.8.8

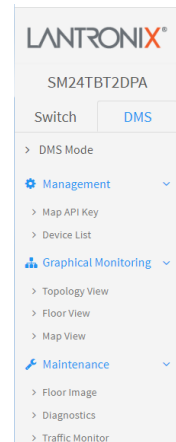
----- running-config -----
hostname SM24TBT2DPA username admin privilege 15 password encrypted YWrtaw4=
!vlan 1!!ip route 0.0.0.0 0.0.0.0 192.168.1.254 tzid 0
system name SM24TBT2DPA
system description Managed Switch, 24-port Gigabit PoE+, 2-port SFP/RJ-45 Combo!
interface GigabitEthernet 1/1 poe power limit 90.0!
interface GigabitEthernet 1/2 poe power limit 90.0!
interface GigabitEthernet 1/3 poe power limit 90.0!
interface GigabitEthernet 1/4 poe power limit 90.0!
interface GigabitEthernet 1/5 poe power limit 90.0!
interface GigabitEthernet 1/6 poe power limit 90.0!
interface GigabitEthernet 1/7 poe power limit 90.0!
interface GigabitEthernet 1/8 poe power limit 90.0!
interface GigabitEthernet 1/9 poe power limit 90.0!
interface GigabitEthernet 1/10 poe power limit 90.0!
interface GigabitEthernet 1/11 poe power limit 90.0!
interface GigabitEthernet 1/12 poe power limit 90.0!
interface GigabitEthernet 1/13 poe power limit 90.0!
interface GigabitEthernet 1/14 poe power limit 90.0!
interface GigabitEthernet 1/15 poe power limit 90.0!
interface GigabitEthernet 1/16 poe power limit 90.0!
interface GigabitEthernet 1/17 poe power limit 90.0!
interface GigabitEthernet 1/18 poe power limit 90.0!
interface GigabitEthernet 1/19 poe power limit 90.0!
interface GigabitEthernet 1/20 poe power limit 90.0!
interface GigabitEthernet 1/21 poe power limit 90.0!
interface GigabitEthernet 1/22 poe power limit 90.0!
interface GigabitEthernet 1/23 poe power limit 90.0!
interface GigabitEthernet 1/24 poe power limit 90.0!
interface GigabitEthernet 1/25!
interface GigabitEthernet 1/26!
interface vlan 1 ip address 192.168.1.77 255.255.255.0!
spanning-tree aggregation spanning-tree

```

Chapter 6 - DMS (Device Management System)

6-1 The DMS Tab

The Lantronix DMS (Device Management System) is an intelligent management tool embedded in the switch to intuitively help IT/TS in reducing support time, cost, and effort. In the SM24TBT2DPA main menu pane on the left, click the DMS tab to display the main DMS functions: DMS Mode, Management, Graphical Monitoring, and Maintenance.

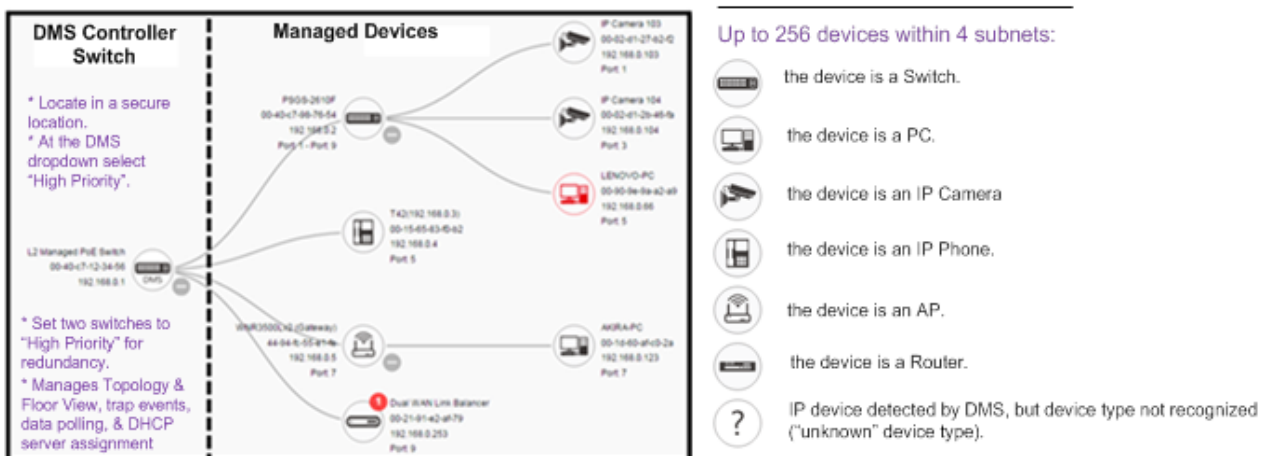


6-2 DMS Overview

The embedded Device Management System is designed to be extremely easy to use, manage, and install IP Phones, IP Cameras, WAPs, etc. for enterprise applications.

DMS operates by a “Master switch” elected from one of the switches. The Master (“Controller” or “High Priority”) switch automatically discovers all types of IP device information and diagnoses all cable and device status on topology. Any member of the DMS switch can be the Master switch.

You can deploy IP devices via Topology/ Floor/ Map View to installation locations, run Diagnostics and view Traffic Monitor, and check link status and monitor throughput.



DMS Controller Switch and Managed Devices

DMS Controller Switch Notes:

- 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.
- You can set two switches to High Priority for Controller Switch redundancy.
- The DMS Controller Switch should be put in a secure location such as a server room, with access/authority limited to IT staff.
- The DMS Controller Switch is the center of IP / Event management for DMS operation:
 - When enabled DHCP Server mode in DMS network, the DMS Controller switch will be 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.

6-2.1 DMS > DMS Mode > Information

The first time you access the DMS tab, the DMS Mode Information page displays with DMS Mode Disabled. **Note:** at SM24TBT2DPA FW v6.54.3104 the DMS mode behavior was changed to default Mode = Enabled and default Controller Priority = Low. At SM24TBT2DPA FW v6.54.3135 Controller Priority modes (High/Low/Mid/Non) were introduced.

The screenshot shows the Lantronix web interface for SM24TBT2DPB. The left sidebar contains navigation options: DMS Mode, Management (with sub-options Map API Key and Device List), Graphical Monitoring, and Maintenance. The main content area is titled 'Information' and contains a table with the following data:

Mode	Enabled
Controller Priority	High
Total Device	5
On-line Devices	5
Off-line Devices	0
Controller IP	192.168.1.77

An 'Apply' button is located at the bottom left of the configuration area.

Parameter descriptions:

DMS Mode: Enable or Disable the DMS function. The default is Enabled.

Controller Priority: Select the Controller priority when enabling DMS:

High: Select "High" Priority to make this device the DMS Master ("Controller") switch.

Mid: Select "Mid" to assign a middle level priority.

Low: Select "Low" to assign the lowest level priority (default).

Non: This switch will never become the DMS Master ("Controller") switch.



Total Devices: Shows how many IP devices are detected and displayed in the topology view.

On-Line Devices: Shows how many IP devices on-line in the topology view.

Off-Line Device: Shows how many IP devices off-line in the topology view.

Controller IP: Shows the IP address of the assigned DMS Master (Controller) switch.

Buttons

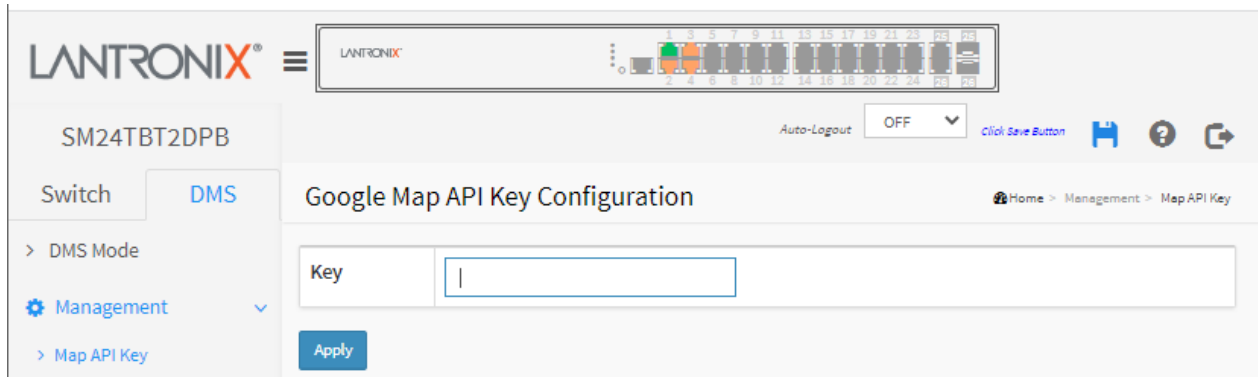
Apply: Click to save changes to the running-config file.

6-3 Management

6-3.1 Google Maps API Key Configuration

You need a valid API key and a Google Cloud Platform billing account to access Google core product. If not, DMS Map View will not be able to load Google Maps correctly. Visit the Google website below and follow the directions to get a Google Maps API key:

<https://developers.google.com/maps/documentation/directions/get-api-key>



The screenshot shows the Lantronix web interface for the SM24TBT2DPB device. The page is titled "Google Map API Key Configuration". On the left, there is a navigation menu with "DMS Mode" selected and "Management" expanded to show "Map API Key". The main content area has a "Key" label and an empty text input field. Below the input field is a blue "Apply" button. At the top right, there is an "Auto-Logout" dropdown set to "OFF" and a "Click Save Button" link. The breadcrumb trail is "Home > Management > Map API Key".

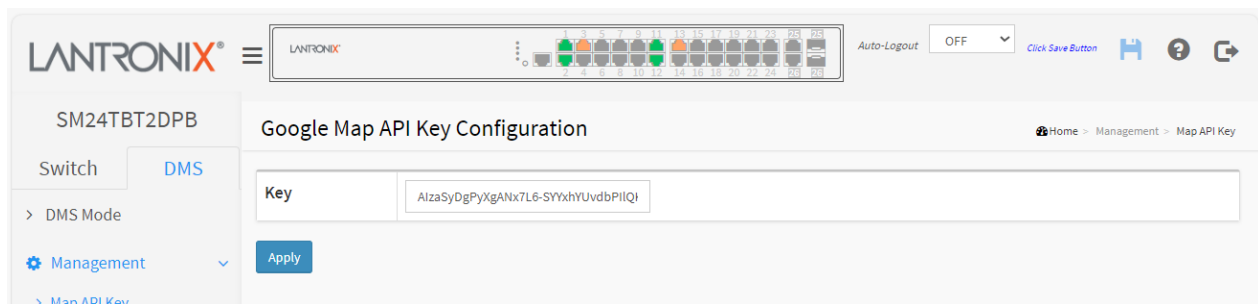
Parameters:

Key: Specify the Google API Key.

Buttons

Apply: Click to save changes.

Example:



The screenshot shows the same Lantronix web interface as above, but now the "Key" field is populated with the example key: "AlzaSyDgPyXgANx7L6-SYxxhYUvdbPllQI". The "Apply" button remains visible below the input field. All other interface elements, including the navigation menu and top right controls, are identical to the previous screenshot.

6-3.2 Device List

The devices in the same subnet with the DMS switch will be listed in the Devices List.

LANTRONIX SM24TBT2DPB

Switch **DMS**

> DMS Mode

Management

> Map API Key

> Device List

Graphical Monitoring

Maintenance

Auto-refresh

Show 10 entries Search:

<input type="checkbox"/> Remove	Status	Device Type	Model Name	Device Name	MAC	IP Address
<input type="checkbox"/>	Online	IP Camera	AXIS P1447-LE	AXIS P1447-LE - ACCC8EBAF7C1	AC-CC-8E-BA-F7-C1	169.254.138.213
<input type="checkbox"/>	Online	PC	General PC	MINNW1074	5C-FF-35-DC-0A-C1	192.168.1.75
<input type="checkbox"/>	Online	SWITCH	SM24TBT2DPB	SM24TBT2DPB	00-C0-F2-7C-58-77	192.168.1.77
<input type="checkbox"/>	Online	IP Camera			00-09-18-4E-20-E9	192.168.1.100
<input type="checkbox"/>	Online	IP Camera			00-16-6C-D4-DD-C2	192.168.1.100

Showing 1 to 5 of 5 entries

Previous 1 Next

Apply

Procedure

1. Click **DMS > Management > Device List**. Select to remove a device if necessary.
2. By default, seven columns display in the table.
3. Click the Edit Device Name icon () to display four additional (editable) table columns (see Example Below).
4. Edit the Device Name, Http Port, User Name, and/or User Password as desired.
5. Click Apply.



Note: Click a column heading to sort by Mac address, or IP address, etc.

Example: Five devices discovered, with eleven columns displayed (four editable table columns).

LANTRONIX SM24TBT2DPB

Switch **DMS**

> DMS Mode

Management

> Map API Key

> Device List

Graphical Monitoring

Maintenance

Auto-refresh

Show 10 entries Search:

<input type="checkbox"/> Remove	Status	Device Type	Model Name	Device Name	Edit Device Name	MAC	IP Address	Edit HTTP Port	Edit User Name	Edit User Password
<input type="checkbox"/>	Online	IP Camera	AXIS P1447-LE	AXIS P1447-LE - ACCC8EBAF7C1	AXIS P1447-LE - ACCC8EBAF7C1	AC-CC-8E-BA-F7-C1	169.254.138.213	80	admin	****
<input type="checkbox"/>	Online	PC	General PC	MINNW1074	MINNW1074	5C-FF-35-DC-0A-C1	192.168.1.75			
<input type="checkbox"/>	Online	SWITCH	SM24TBT2DPB	SM24TBT2DPB	SM24TBT2DPB	00-C0-F2-7C-58-77	192.168.1.77			
<input type="checkbox"/>	Online	IP Camera				00-09-18-4E-20-E9	192.168.1.100	80	admin	****
<input type="checkbox"/>	Online	IP Camera				00-16-6C-D4-DD-C2	192.168.1.100	80	admin	****

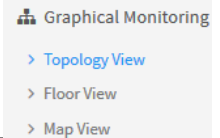
Showing 1 to 5 of 5 entries

Previous 1 Next

Apply

6-4 Graphical Monitoring

Navigate to the DMS tab > Graphical Monitoring, Topology View menu path to monitor Topology/ Floor/ Map view. The global buttons are described below.



Button / Icon	Function
	Click to show or hide the pop up device list.
SVG	Save the whole View to SVG, PNG or PDF.
All	Select the device you want to be displayed.
Q	Type the key word you want to search.

6-4.1 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 Topology View (e.g., remotely diagnose cable connection status, auto alarm notifications on critical events, remotely reboot PoE device when it's not alive, etc.). You can apply the DMS platform to resolve issues anytime and anywhere by tablet or smart phone, and keep the network working smoothly.

In the DMS tab, click Graphical Monitoring, Topology View to display a visual representation of the network

topology. Click to show the pop up device list.

Device Icons:



Icon with black mark: Device link up; you can select a function and check issues.




Icon with red mark: Device link down; you can diagnose the link status.




Icon with numbers: If issues on IP devices click picture to check event log.

Procedure

1. Click Topology View.

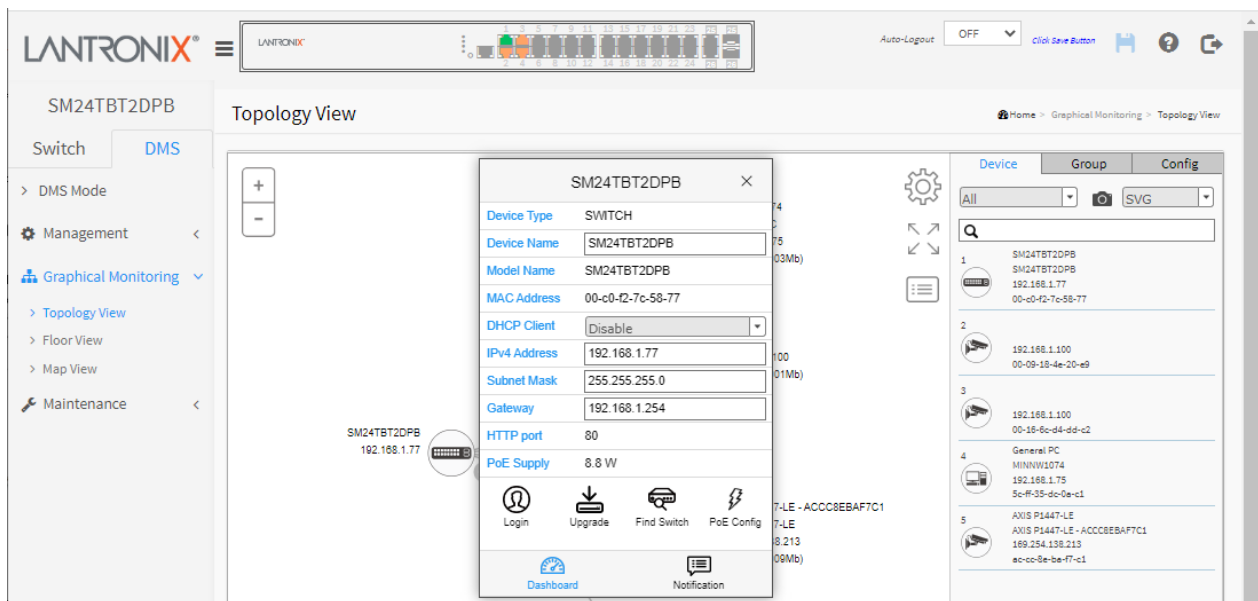
2. Click  to show the pop up device list.

3.. Click  to select each device to display information; up to three can be selected.

4. Click the Snapshot icon () to save a copy of topology view and transfer the format to SVG, PNG or PDF file format.

Graphical Monitoring > Topology View > Device Tab

Click a device to display its parameters and icons.



The screenshot displays the Lantronix web interface. The main area shows a network topology view with a central device labeled 'SM24TBT2DPB' and IP address '192.168.1.77'. A pop-up window for this device is open, showing the following parameters:

SM24TBT2DPB	
Device Type	SWITCH
Device Name	SM24TBT2DPB
Model Name	SM24TBT2DPB
MAC Address	00-c0-f2-7c-58-77
DHCP Client	Disable
IPv4 Address	192.168.1.77
Subnet Mask	255.255.255.0
Gateway	192.168.1.254
HTTP port	80
PoE Supply	8.8 W

Below the parameters are icons for Login, Upgrade, Find Switch, and PoE Config. At the bottom of the pop-up are links for Dashboard and Notification. On the right side of the interface, there is a 'Device' tab with a search bar and a list of devices, including the selected SM24TBT2DPB and several General PCs and AXIS IP cameras.

Device Tab Parameters and Icons

Device Type: **PC** (General PC), **IP Camera** (General IP Cam), **IP Phone** (General IP Phone, Cisco SPA303), **AP** (General AP), **Others** (Mobile Device, General Switch, Internet Gateway, IP PBX, NAS, VMS, Unknown Device, LED Light, Mini fridge, Shade).

Device Name: e.g., SM24TBT2DPA or other device.

Model Name: e.g., SM24TBT2DPA or other model.

Mac Address: e.g., 00-40-c7-fe-07-df

DHCP Client: dropdown to select Disable or Enable. The default is disabled.

IPv4 Address: e.g., 192.168.1.77

Subnet Mask: e.g., 255.255.255.0

Gateway: e.g., 192.168.1.254

Http Port: e.g., 80

PoE Supply: e.g., 9 W

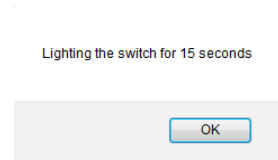
Login: click the button to return to the startup screen.

Upgrade: click the button to display the firmware upgrade dialog.

Find Switch: click the button to light the front panel port LEDs for 15 seconds.

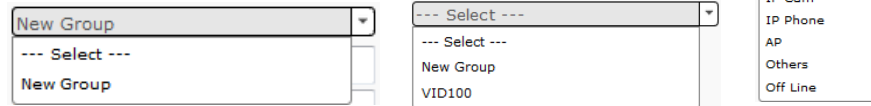
Dashboard: click the button to display the dashboard data.

Notification: click the button to display notification messages if any exist.

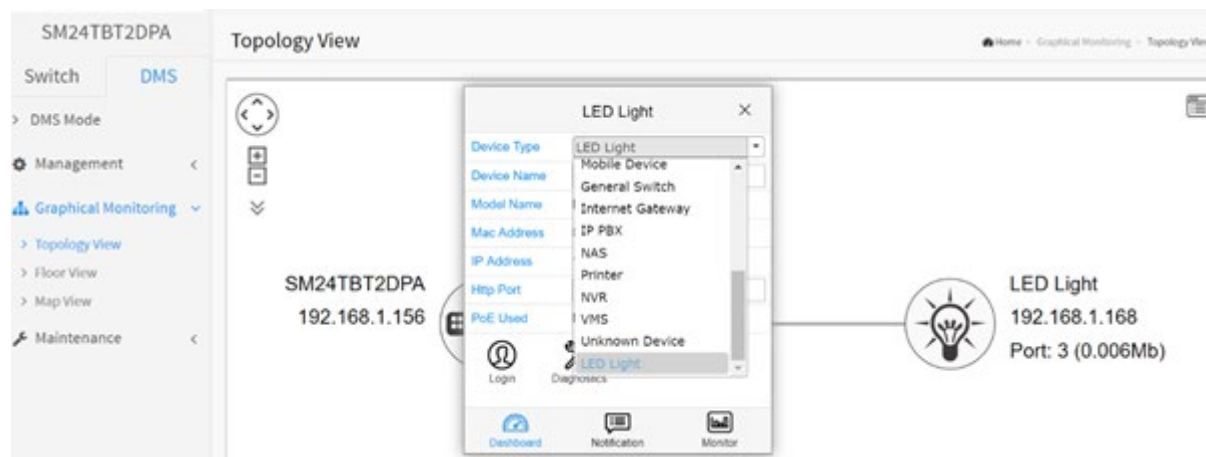
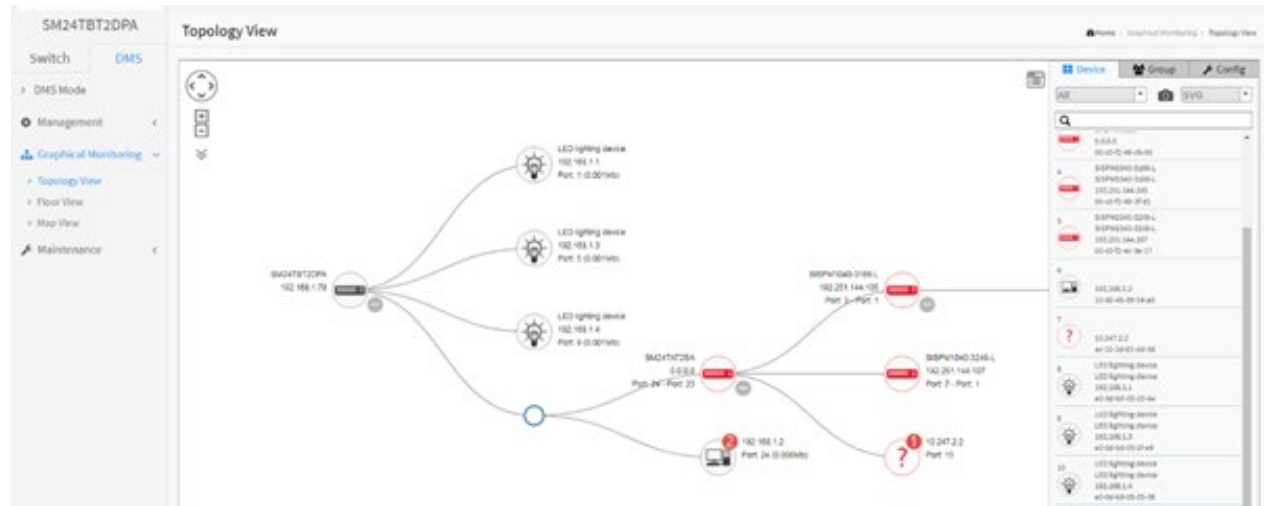


Graphical Monitoring > Topology View > Group Tab

At the Groups dropdown, select a Group (ALL, SWITCH, PC, IP Cam, IP Phone, AP, Others, or Off Line).



At the New Group or Existing Groups dropdown, select New and enter a Vlan ID, Name, Traffic Priority, OUI(s), and then click the **Apply** button.



Group Tab Parameters and Icons

At the group name dropdown select an existing Group Name or select New Group to create a new one.

Vlan ID: enter the VLAN ID (VID; 1-4094).

Name: enter a Group name.

Traffic Priority: at the dropdown select Default, 0 (Low), 1, 2, 3, 4, 5, 6, or 7 (High) as the priority for traffic for this Group.

OUI 1 - 3: enter 1-3 Organizationally Unique Identifiers. When DMS detects the MAC address range of E0-0D-B9-xx-xx-xx, it will identify the device as LED lighting in topology view (e.g., E0-0D-B9 is the vendor OUI of CREE LED light).

Buttons:

Apply: Click to save the configured parameters.

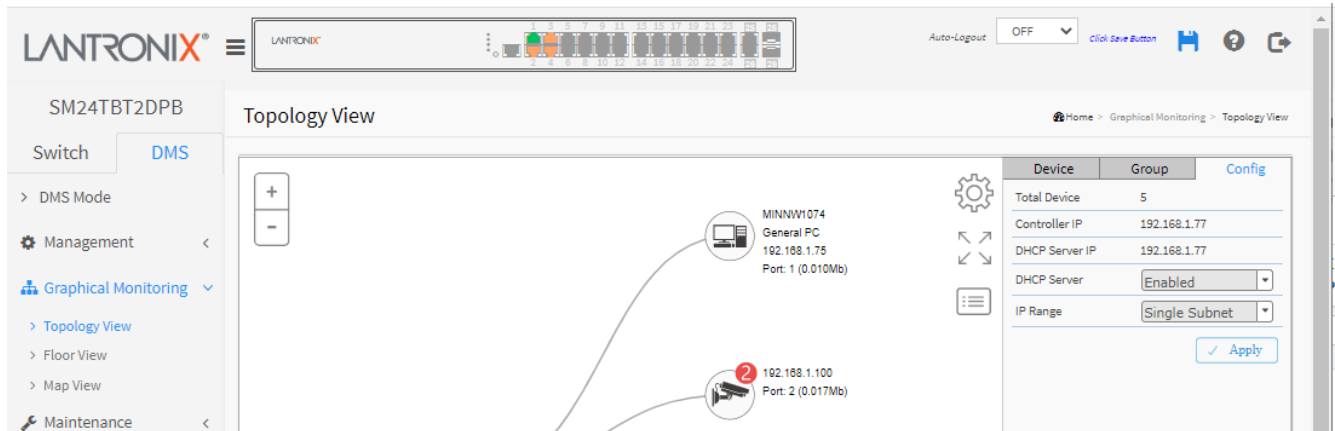
Delete: Click to delete the parameters.

The screenshot shows a web interface for configuring a group. At the top, there is a breadcrumb trail: Home > Graphical Monitoring > Topology View. Below this, there are three tabs: Device, Group (selected), and Config. A search bar with a dropdown menu set to 'All' and a search icon is present. Below the search bar, there is a dropdown menu showing 'admin 10 2 sec'. The main configuration area contains the following fields:

- Vlan ID: 100
- Name: admin 10 2 sec
- Traffic Priority: 3
- OUI 1: 00-22-45
- OUI 2: (empty)
- OUI 3: (empty)

At the bottom right of the configuration area, there are two buttons: 'Apply' (with a checkmark icon) and 'Delete' (with an 'X' icon).

Graphical Monitoring > Topology View > Config Tab



Config Tab Parameters and Icons

Device Type: PC (General PC), IP Camera (General IP Cam), IP Phone (General IP Phone, Cisco SPA303), AP (General AP), **Others** (Mobile Device, General Switch, Internet Gateway, IP PBX, NAS, Printer, NVR, VMS, Unknown Device, LED Light, Mini fridge, Shade).

Device Name and Model Name: e.g., SM24TBT2DPA or SM24TBT2DPB.

Mac Address: e.g., 00-40-c7-fe-07-df

DHCP Client: dropdown to select *Disable* or *Enable*. The default is *Disabled*.

IPv4 Address: e.g., 192.168.1.77

Subnet Mask: e.g., 255.255.255.0

Gateway: e.g., 192.168.1.254

Http Port: e.g., 80

PoE Supply: e.g., 0 W

Login: click the button to return to the startup screen.

Upgrade: click the button to display the firmware upgrade dialog.

Find Switch: click the button to light the front panel port LEDs for 15 seconds.

Dashboard: click the button to display the dashboard data.

Notification: click the button to display notification messages, if any exist.

Total Device: the number of devices discovered (e.g., 2).

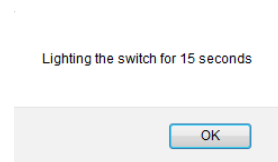
Controller IP: the master IP address (e.g., 192.168.1.77).

DHCP Server IP: if one is configured, otherwise displays "---".

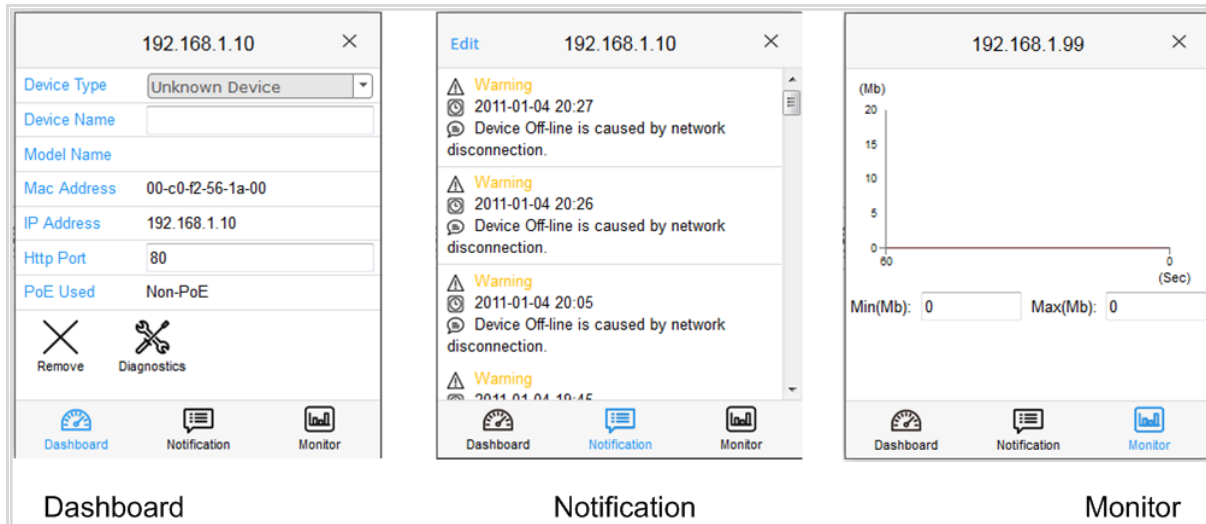
DHCP Server: at the dropdown select *Disabled* or *Enabled*. The default is *Disabled*.

IP Range: at the dropdown select *Single Subnet* or *Multiple Subnet*. If you select *Multiple Subnets*, you must also enter one or more Range parameters.

Click the **Apply** button when done.



Sample Dashboard, Notification, and Monitor dialog boxes are shown below:



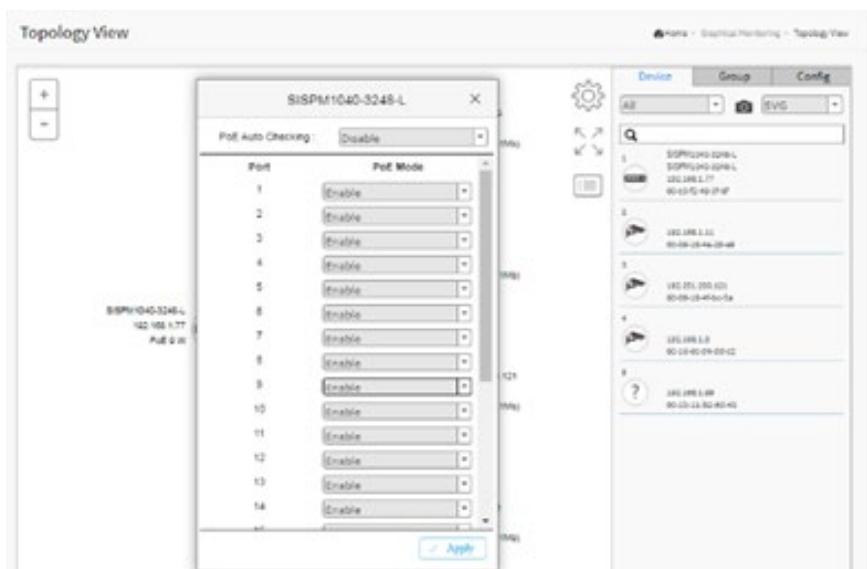
PoE Auto Checking “AutoFill” Feature

When you enable Auto Power Reset (PoE Auto Checking) in DMS, the IP addresses of the connected devices are automatically filled in the Auto Power Reset configuration page.











1. Configure the “PoE Auto Checking” parameter at Switch > PoE Management > PoE Auto Checking. The “Failure Action” parameters are “Reboot Remote PD” or “Nothing”.
2. Configure PoE parameters at DMS > Graphical Monitoring > Topology View. Left click on the switch



icon to display its device configuration popup. Click the PoE Config (PoE Config) icon to display the PoE Auto Checking pane:



Device Types (Device Categories)

 <p>: The device is a switch.</p>	 <p>: The device is a PC.</p>
 <p>: The device is an IP Camera</p>	 <p>: The device is an IP Phone.</p>
 <p>: The device is a WAP</p>	 <p>: The device is a Router.</p>
 <p>: The device is an LED Light.</p>	 <p>: The device is a Mini fridge.</p>
 <p>: The device is a Shade.</p>	 <p>: 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" type.</p>

Device Status



: Icon with black mark: Device link up; you can select function and check issues.



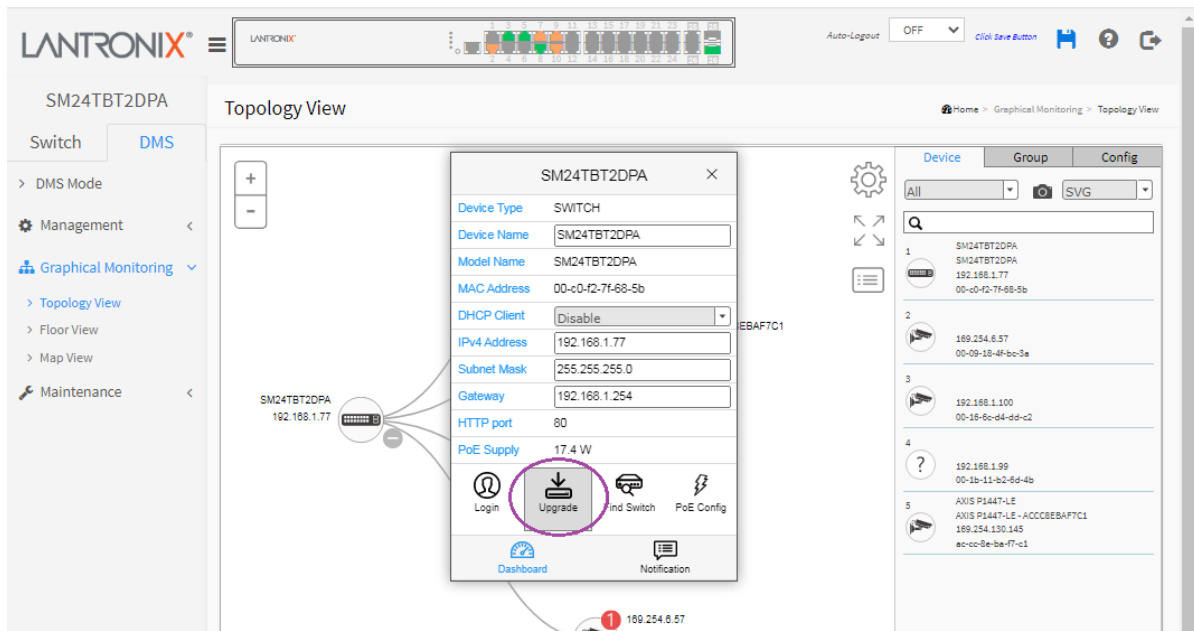
: Icon with red mark: Device link down; you can diagnose link issues.



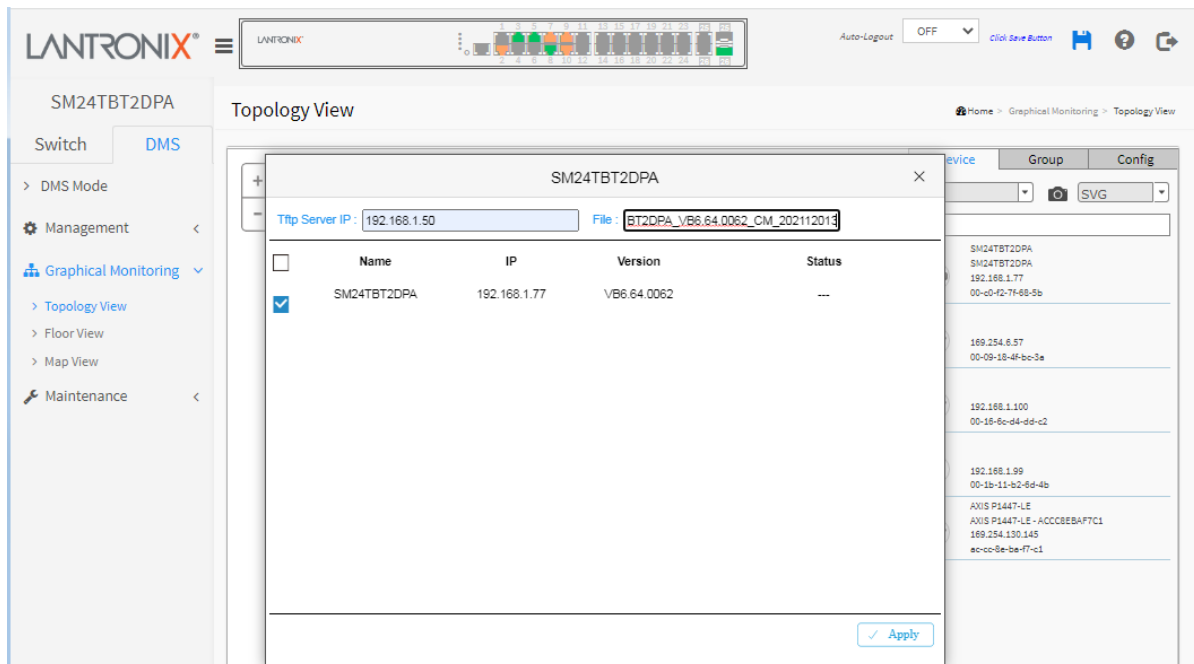
: Icon with number: An event occurred (Device Offline, IP Duplicate, etc.) on the IP device. You can click the device icon and check events in Notification.

Upgrade Firmware Procedure

1. At DMS > Graphical Monitoring > Topology View left mouse click on the SM24TBT2DPB icon to display the Config tab.



2. Click the Upgrade button to display the upgrade table.



3. Check the SM24TBT2DPA checkbox.
4. Enter the Tftp Server IP address (e.g., 192.168.1.50).
5. Enter the firmware upgrade File (e.g., SM24TBT2DPA_VB6.64.0107_CM_202112013).
6. Click the Apply button to Save to running-config file. The message "Starting, please wait..." displays momentarily.
7. Wait for the firmware upgrade File to be successfully loaded.


Messages: *Error : Firmware download fail* displays if unsuccessful.

6-4.2 Floor View



This page lets you easily plan IP device installation locations onto the custom uploaded image by dragging-and-dropping markers in the Device list. You must first load one or more floor images at DMS > Maintenance > Floor Image (see [6-5.1 Floor Image](#) on page 364).

You can place the device icon on the install location and print the page for future reference. To place an icon, click the IP device from the Devices List then drag and drop onto the floor view.

Procedure

1. At **DMS > Maintenance > Floor Image** add a Floor Image file (so it will be available for use in the “Floor View” page).
2. Click Floor View.
3. Click Device List.
4. Select and click a device.
5. Drag the device to the desired location.
6. Click  to save the floor view to SVG, PNG, or PDF file format.

Entry Tab Parameters and Icons

- Click  to show or hide the pop up device list.
- Click  to Save the whole View to SVG, PNG or PDF.
- Click and select the device you would like to show up.
- Click and type the key word you would like to search.

Config Tab Parameters

Total Device: the number of devices discovered (e.g., 2).

Master Controller IP: the master IP address (e.g., 192.168.1.77)

DHCP Server IP: if one is configured, otherwise displays “---”.

DHCP Server: at the dropdown select *Disabled* or *Enabled*. The default is *Disabled*.

IP Range: at the dropdown select *Single Subnet* or *Multiple Subnet*. If you select *Multiple Subnets*, you must also enter one or more Range parameters.

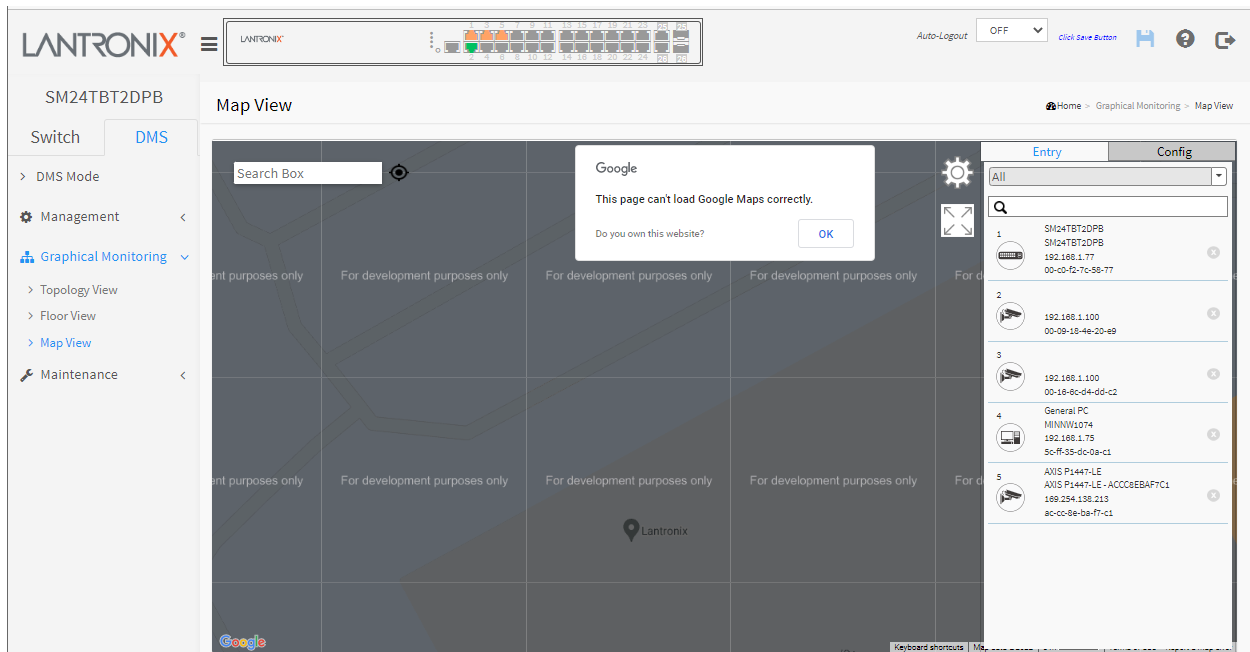
Range 1-4: Displays the configured range of IP addresses.

Apply: Click to apply the settings to the running-config file.

Entry		Config
Total Device	2	
Master Controller IP	192.168.1.77	
DHCP Server IP	---	
DHCP Server	Disabled	
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
<input type="button" value="Apply"/>		

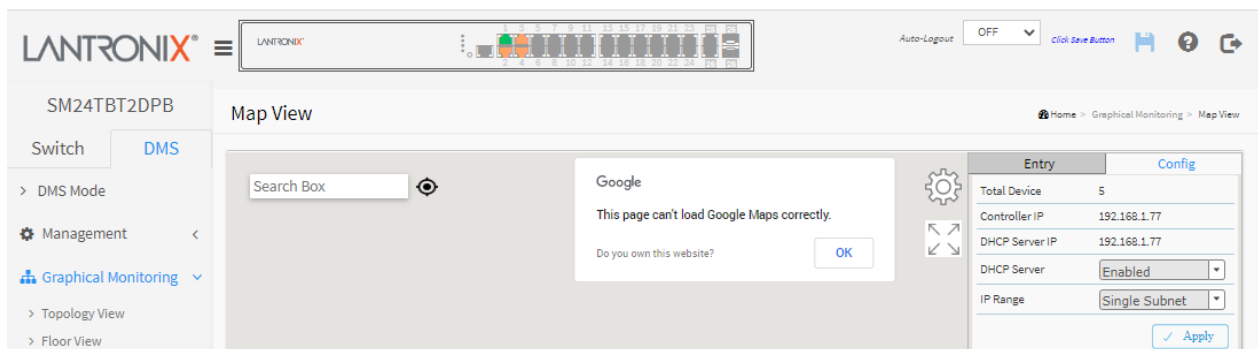
6-4.4 Map View

You can monitor and manage each device by DMS, and help the user find the location of the devices even if they are installed in a different building. You can place the device icons on the Map View which is navigated by Google Maps.



1. Click Map View and click *Always*.
2. Click a device in the Entry tab list.
3. Select and click a device (📍).
4. Drag the device to the desired location.

Config Tab:



Message: *Would you like to share your location with this site?*

Response: Select *Always*, *Never*, or *Not Now*.

Message: *This page can't load Google Maps correctly.*

Recovery:

1. Click the OK button to clear the message.
2. Navigate to DMS > Mode > Map API Key.
3. See section “6-3.1 Google Maps API Key Configuration” on page 343.

Message: *Do you own this website?*

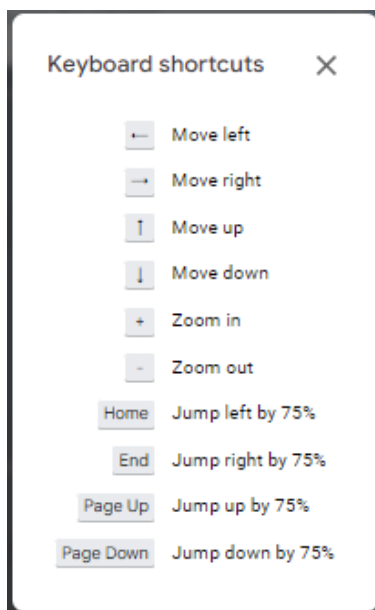
Meaning: If you are NOT the website owner, there are no steps you can take to fix any of these errors. However, you may want to notify the site owner if possible.

Recovery:

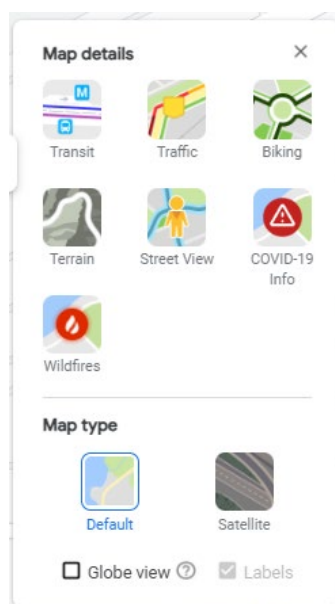
1. Click the linked text *Do you own this website?* to view the Google Maps Platform support page at https://developers.google.com/maps/documentation/javascript/error-messages?utm_source=maps_js&utm_medium=degraded&utm_campaign=keyless#api-key-and-billing-errors
2. Click the OK button to clear the message and continue operation.

Navigation Tools

Keyboard Shortcuts:



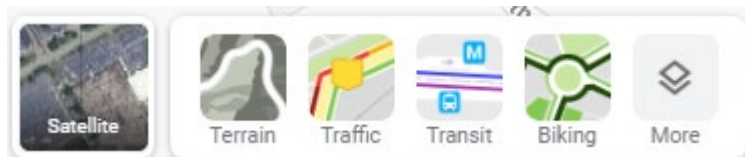
Map Details:



Map data ©2022 United States Terms Privacy Send feedback 100 ft

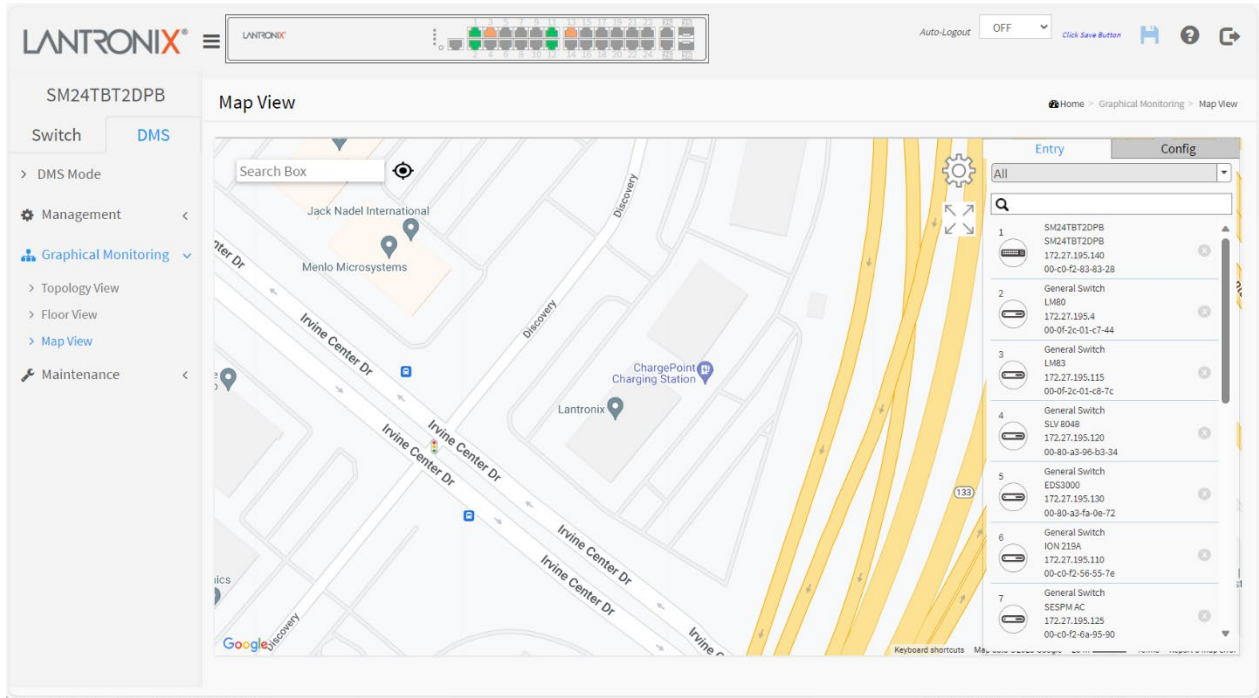


: Show Your Location (top), Zoom Out/Zoom In, Browse Street View Images (bottom)



: View Selections

Example:



6-5 Maintenance

6-5.1 Floor Image

The Floor Image Management page lets you manage and maintain the flow view image. Navigate to DMS > Maintenance > Floor Image to display the Floor Image Management page. Here you can add or delete one or more floor image maps.

LANTRONIX SM24TBT2DPB

Auto-Logout OFF Click Save Button

Home > Maintenance > Floor Image

Maximum: 10 files Used: 0 file(s) Free: 10 file(s)

Add Floor Image: Choose File FloorPlan 1stFloor.png

Name FloorPlan 1stFloor

Add

Select	No.	File Name	Image
No information found			

Delete

1. Click **DMS > Management > Floor View**.
2. Select a floor image (image size: 512KB, File type: .jpg or .png).
3. Click **Add** to add the new floor image.

LANTRONIX SM24TBT2DPB

Auto-Logout OFF Click Save Button

Home > Maintenance > Floor Image

Maximum: 10 files Used: 1 file(s) Free: 9 file(s)

Add Floor Image: Choose File No file chosen

Name

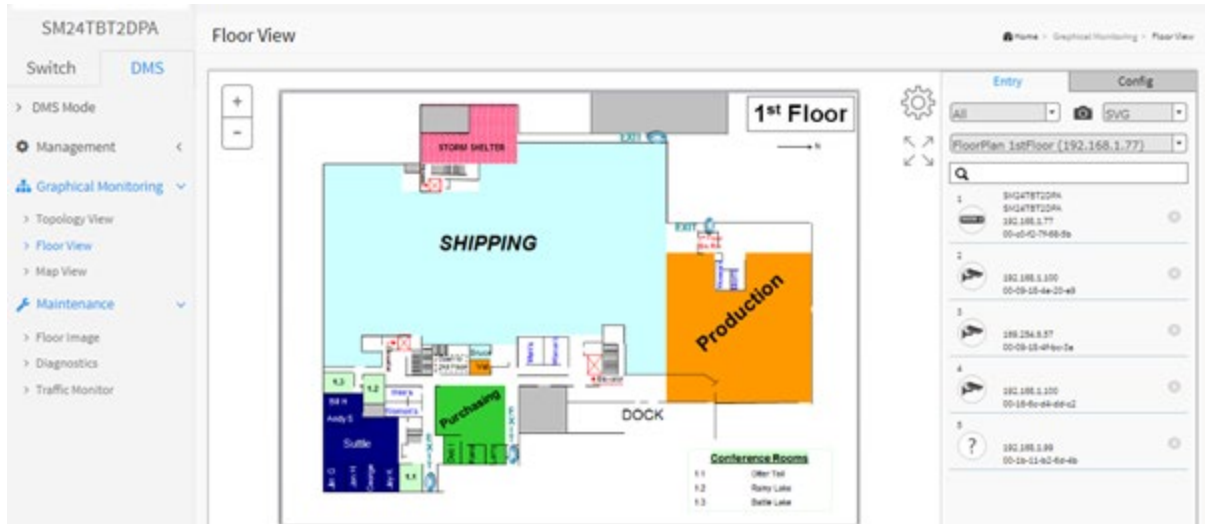
Add

Select	No.	File Name	Image
<input type="checkbox"/>	1	FloorPlan 1stFloor (192.168.1.77)	

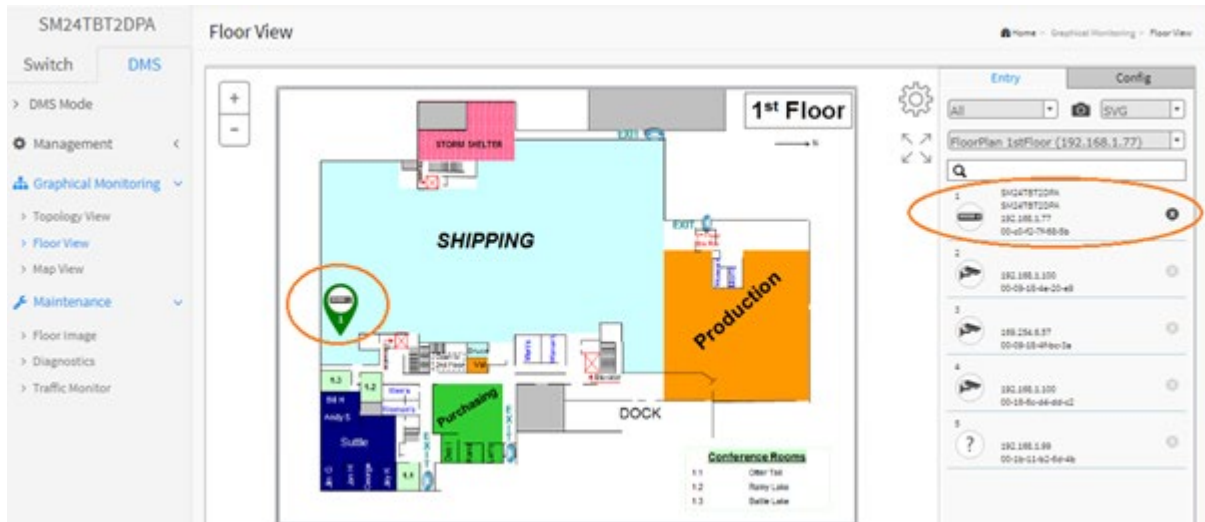
Delete

4. You can now place device icons on the Floor View page. See “6-4.2 Floor View” on page 332.

5. To open the new floor image, you can navigate to **DMS > Graphical Monitoring > Floor View**:



6. Left mouse click a device to display its icon on the Floor View. Drag the device icon to the desired location:



Message: 192.168.1.77 is not responding due to a long-running script.






Meaning: At Floor View you

Recovery: Click the **Stop script** button and continue operation.

Example: three floor images added:

The screenshot shows the Lantronix web interface for the SM24TBT2DPA switch. The page is titled "Floor Image Management" and is part of the "Maintenance" section. It displays the following information:

- Maximum: 10 files, Used: 3 file(s), Free: 7 file(s)
- Add Floor Image: Choose File (No file chosen)
- Name: [Empty text box]
- Add button
- Table with 4 columns: Select, No., File Name, Image
- Table content:

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)	
- Delete button

You can now select a floor image to view at DMS > Graphical Monitoring > Floor View.

6-4.2 Diagnostics

This feature lets you verify and test the link route between switches and devices. You can use this feature to remotely diagnose all IP device status and decrease troubleshooting time.

This page lets you diagnose the connection status of IP devices in the network.

LANTRONIX SM24TBT2DPA

Switch DMS

> DMS Mode

Management <

Graphical Monitoring <

Maintenance >

> Floor Image

> Diagnostics

> Traffic Monitor

Auto-Logout OFF Click Save Button

Home > Maintenance > Diagnostics

Diagnosics

Show 10 entries Search:

Select	Status	Model Name	Device Name	MAC	IP Address	Version
<input type="checkbox"/>	Online			00-09-18-4F-BC-3A	169.254.6.57	
<input type="checkbox"/>	Online			00-16-6C-D4-DD-C2	192.168.1.100	
<input type="checkbox"/>	Online			00-1B-11-B2-6D-4B	192.168.1.99	
<input type="checkbox"/>	Online	AXIS P1447-LE	AXIS P1447-LE - ACCC8EBAF7C1	AC-CC-8E-BA-F7-C1	169.254.130.145	

Showing 1 to 4 of 4 entries

Previous 1 Next

1. Click **DMS > Maintenance > Diagnostics**.
2. Select a device to troubleshoot.
3. View the selected device's information (example below).

LANTRONIX SM24TBT2DPB

Switch DMS

> DMS Mode

Management <

Graphical Monitoring <

Maintenance >

> Floor Image

> Diagnostics

> Traffic Monitor

Auto-Logout 10 min Click Save Button

Home > Maintenance > Diagnostics

Diagnosics

Another Try

Show 10 entries Search:

Select	Status	Model Name	Device Name	MAC	IP Address	Version
<input checked="" type="checkbox"/>	Online	SISPM1040-582-LRT	SISPM1040-582-LRT	00-C0-F2-82-3E-8B	172.27.195.90	VB7.20.0191

Showing 1 to 10 of 13 entries

Previous 1 2 Next

172.27.195.140 00-c0-f2-83-83-28

Connection..... ✓
Cable status..... ✓

172.27.195.100 00-c0-f2-9a-b6-28

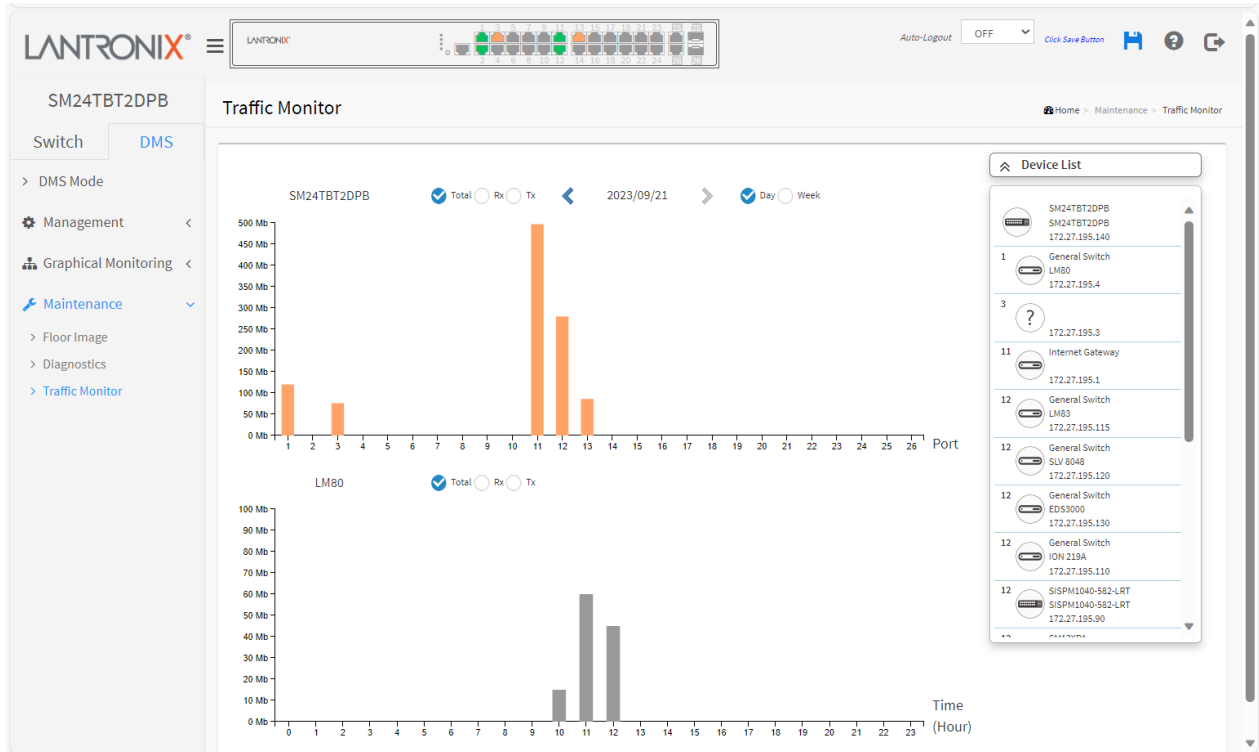
Connection..... ✓
Cable status..... ✓

172.27.195.90 00-c0-f2-82-3e-8b

When done, click the **Another Try** button to troubleshoot another device.

6-4.3 Traffic Monitor

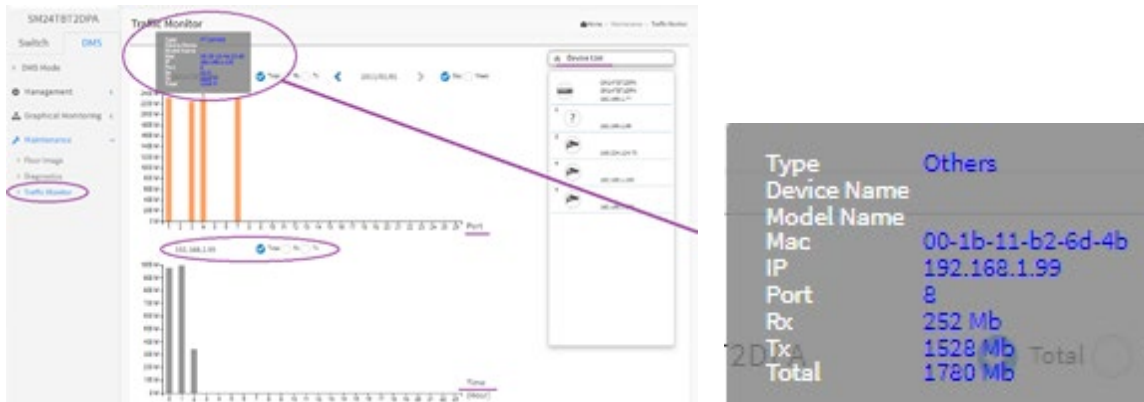
This page displays a visual chart of network traffic of all the devices. Numbers are shown in Mbit/s. To view the traffic through all the ports or a specific port, click on specific port on the traffic chart to reveal its traffic during the day. You can select to display a summary of a day's or a week's traffic by selecting the check circle on top. The same applies to the selection of Rx Tx traffic. A single port's traffic is shown at the lower half of the screen.



Procedure

1. Click **DMS > Maintenance > Traffic Monitor**.
2. View the numbers in Mbit/s.
3. To view the traffic through all the ports or a specific port, click on specific port on the traffic chart to reveal its traffic during the day.
4. 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.

Example



6-4.4 DMS Troubleshooting

Problem: The switch lists itself as the only device in Topology View of DMS.

Problem: In DMS, the Local image shows the IP address of another switch.

Description: The switch is listed as 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: IP cameras connected to a PoE+ or PoE++ switch but cannot log into the cameras directly via DMS Topology View.

Resolution: In order to log into a camera on a switch with PoE+ or PoE++ from DMS > Graphical Monitoring > Topology View from a browser other than IE, you must have an "IE Tab" extension installed. This is needed for both [Chrome](#) and [Firefox](#). IE Tab is an extension for the Google Chrome and Mozilla Firefox web browsers that lets you view pages using the Internet Explorer layout engine.

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 [6-4.1 Google Maps API Key Configuration](#) on page [361](#).

The screenshot shows the Lantronix DMS web interface for switch SM24TBT2DPB. The interface includes a navigation menu on the left with options like 'Switch', 'DMS', 'Management', 'Graphical Monitoring', and 'Maintenance'. The main area is titled 'Map View' and displays a map. A Google error dialog box is overlaid on the map, stating 'This page can't load Google Maps correctly.' and 'Do you own this website?'. On the right side, there is a table listing discovered devices:

Entry	Config
1	SM24TBT2DPB SM24TBT2DPB 192.168.1.77 00-c0-f2-7c-98-77
2	192.168.1.100 00-09-18-4e-20-e9
3	192.168.1.100 00-18-8c-04-d5-c2
4	General PC MINNW1074 192.168.1.75 5c-f9-35-0c-08-c1
5	AXIS P1447-LE AXIS P1447-LE - ACC08EBAFTC1 189.254.138.213 ac-cc-8e-08-f7-c1

Message: *Traffic Monitor feature is only available on master controller. Current master controller IP Address:192.168.xx.xx. See [Maintenance > Traffic Monitor](#) on page 368 above.*

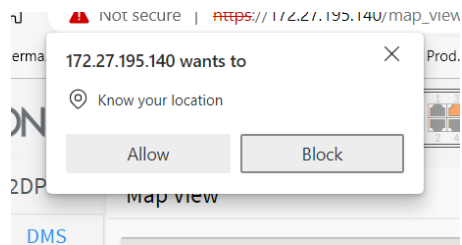
Problem: Some switches don't display DMS Topology View.

Description: With several switches installed, a few of them do not display the network Topology View.

Resolution: This may be due to having different firmware on the devices. Upgrade so that the firmware levels are all the same on these units.

Message: *<site IP> wants to Know your location*

Recovery: Select Allow or Block reporting your current location.



Chapter 7 - Troubleshooting

7-1 Troubleshooting Procedure

Most problems are caused by the following situations. Check for these items first when you start troubleshooting:

1. Verify the install procedures were performed correctly. See the related Install Guide.
2. Check if the SM24TBT2DPx POWER LED is Off:
 - Check connections between the switch, the power cord and the wall outlet.
3. Check if the SM24TBT2DPx Link LED is Off:
 - Verify that the switch and attached device are powered on.
 - Be sure the cable is plugged into the switch and corresponding device.
 - If the switch is installed in a rack, check the connections to the punch-down block and patch panel.
 - Verify that the proper cable type is used and its length does not exceed specified limits.
 - Check the adapter on the attached device and cable connections for possible defects. Replace the defective adapter or cable if necessary.
 - Use the **Mode/Reset** button to change LED mode, reset the switch, or restore to defaults. See the Install Guide for details.
4. Make sure all devices connected to the SM24TBT2DPA are configured to auto negotiate or are configured to connect at half duplex (all hubs are configured this way, for example).
5. Check the cabling:
 - Look for faulty or loose cables.
 - Look for non-standard and mis-wired cables.
6. Make sure you have a valid network topology:
 - Check for improper Network Topologies.
 - Make sure that your network topology contains no data path loops.
7. Check the port configuration:
 - Make sure ports have not been put into a “blocking” state by Spanning Tree, GVRP, or LACP. The normal operation of the Spanning Tree, GVRP, and LACP features may put the port in a blocking state.
 - Verify that the port has not been configured as disabled via software.
8. Review section [7-2 Troubleshooting Q&A](#) on page [372](#) below.
9. Check the Release Notes for your FW version. Note any known issues and check for a more current FW version to upgrade to.
10. Record any related error messages, conditions, and configurations for your Tech Support Specialist to consider.
11. Contact Tech Support.

7-2 Troubleshooting Q&A

Q1. Can you reset to factory defaults by creating a physical loop between ports 1 and 2?

A1. The switch supports buzzer and LED status at looping conditions only (not reloading factory defaults per-se).

Q2. The switch supports the use of one or two power supplies, and they are not identified. Is a Power Supply required to be installed in a particular slot at all times, and is the other slot for the optional second power supply?

A2. You can use one power supply in either slot. Use both power supplies if required to provide enough power for the PoE connections that are in use.

Q3. If both power supplies are in use and are required to provide enough power for the PoE connections that are in use, what happens if one of the power supplies fails and there is not enough power to support all of the PoE ports that are in use?

A3. PoE power will be fed to PoE ports with higher priority. If the ports have the same priority, the lower port number will be fed PoE power.

Q4: There is a mismatch of information regarding power requested vs. power allocated on the SM24TBT2DPA. With PD class 2 IP cameras connected to the switch, the switch shows power requested of 90 W and power allocated of 90 W. It should actually show not more than 6.49 W requested or 7 W allocated when using PD class 2. The SM24TBT2DPA however does classify the PD class and the power usage correctly. Comparing the SM24TBT2DPA to the SM24TAT2SA shows the difference.

A4: The SM24TBT2DPA factory default setting is different than the SM24TAT2SA factory default setting. See the Power over Ethernet Status screenshot below. Set the “Reserved Power determined by” parameter to “Class” mode.

Local Port	PD-class	Power Requested	Power Allocated	Power Used	Current Used	Priority	Port Status
1	-	0.2W	0.2W	0.2W	0.2W	Low	No PD detected
2	-	0.2W	0.2W	0.2W	0.2W	Low	No PD detected
3	-	0.2W	0.2W	0.2W	0.2W	Low	No PD detected
4	-	0.2W	0.2W	0.2W	0.2W	Low	No PD detected
5	-	0.2W	0.2W	0.2W	0.2W	Low	No PD detected
6	-	90.2W	90.2W	6.17W	21.04W	Low	PoE Limited On
7	-	0.2W	0.2W	0.2W	0.2W	Low	No PD detected
8	-	0.2W	0.2W	0.2W	0.2W	Low	No PD detected
9	-	0.2W	0.2W	0.2W	0.2W	Low	No PD detected
10	-	0.2W	0.2W	0.2W	0.2W	Low	No PD detected
11	-	0.2W	0.2W	0.2W	0.2W	Low	No PD detected
12	-	0.2W	0.2W	0.2W	0.2W	Low	No PD detected
13	-	0.2W	0.2W	0.2W	0.2W	Low	No PD detected
14	-	0.2W	0.2W	0.2W	0.2W	Low	No PD detected
15	-	0.2W	0.2W	0.2W	0.2W	Low	No PD detected
16	-	0.2W	0.2W	0.2W	0.2W	Low	No PD detected

Power Over Ethernet Status (SM24TBT2DPA)

Appendix A – DHCP Per Port and DHCP IP Per Port

You can configure DHCP Per Port via the CLI and Web UI as described below. The DHCP Per Port factory default mode is Disabled. See the *SM24TBT2DPx CLI Reference* for CLI mode operation. **Note:** do not operate DHCP Per Port and DHCP Pool per VLAN at the same time. If you configure entries for DHCP Pool per VLAN and then enable DHCP per Port, the configured DHCP pool will be deleted.

Configure DHCP Per Port

The switch's DHCP server assigns IP addresses. Clients get IP addresses in sequence and the switch assigns IP addresses on a per-port basis starting from the configured IP range. For example, if the IP address range is configured as 192.168.10.20 - 192.168.10.37 with one DHCP device connected to port 1, the client will always get IP address 192.168.10.20, then port 3 is always distributed IP address 192.168.10.22, even if port 2 is an empty port (because port 2 is always distributed IP address 192.168.10.21).

The switch does not allow a DHCP per Port pool to include the switch's address.

IP address assigned range and VLAN 1 should stay in the same subnet mask.

The configurable IP address range is allowed to configure over 18 IP addresses, but the switch always assigns one IP address per port connecting device.

When the DHCP Per Port function is enabled, the switch software will automatically create the related DHCP pool named "DHCP_Per_Port".

Once the DHCP Per Port function is enabled on one switch, IPv4 DHCP client at VLAN1 mode (DMS DHCP mode), DHCP server mode are all limited to be enabled at the same time (an error message displays if attempted).

If the DHCP server pool has been configured, once you enable the DHCP Per Port function, then that DHCP server pool configuration will be overwritten.

Only for VLAN 1, clients issued DHCP packets will not be broadcast/forwarded to other ports. DHCP packets in others VLANs will be broadcast/forwarded to other ports.

The DHCP Per Port function allows the switch to connect only one DHCP client device.

DHCP-Per-Port is configured entirely on the **Switch > Configuration > System > IP** page, IP Interfaces window.

The feature is enabled here and an IP range (pool) is entered. The "automatic" results of this action can be displayed in:

- **Switch > Configuration > System > DHCP > Server > Mode** (Global Mode – Enabled, VLAN Mode - VLAN 1 created)
- **Switch > Configuration > System > DHCP > Excluded** (Excluded range created based on range entered)
- **Switch > Configuration > System > DHCP > Pool** (Pool "DHCP_Per_Port" created based on range entered)

Actual DHCP operation is monitored as normal under **System > Monitor > DHCP**.

The DHCP Per Port pages and parameters are described below.

DHCP per Port Mode Configuration

The DHCP per Port function lets you assign an IP address based on the switch port the device is connected to. This will speed up installation of IP cameras, as the cameras can be configured after they are on the network. The DHCP Per Port assignment lets you know which IP was assigned to which camera. **Note:** to prevent IP conflict, each switch can be allocated a different IP range.

To configure DHCP Per Port via the Web UI, navigate to the **Configuration > System > IP** menu path.

The screenshot displays the Lantronix web interface for configuring DHCP Per Port. The breadcrumb path **Home > Configuration > System > IP** is highlighted. The left sidebar shows the navigation menu with **Configuration** and **IP** selected. The main configuration area is titled **IP Configuration** and includes the following sections:

- DHCP Per Port:**
 - Mode: Disabled
 - VLAN: VLAN 1
 - IP: [Empty field]
- IP4 DHCP Table:**

Delete	VLAN	Enable	Fallback	Current Lease	IPv4 Address	Mask Length	IPv6 Address	Mask Length
<input type="checkbox"/>	1	<input type="checkbox"/>	0		192.168.1.77	24		
- Link-Local Address binding interface:** VLAN 1
- Gateway Address binding interface:** VLAN 1
- IP Routes Table:**

Delete	Network	Mask Length	Gateway	Next Hop VLAN
<input type="checkbox"/>	0.0.0.0	0	192.168.1.254	0
<input type="checkbox"/>	169.254.0.0	16	192.168.1.77	0
<input type="checkbox"/>	192.168.1.0	24	192.168.1.77	0

Parameter descriptions:

Mode: at the dropdown select **Enable** or **Disable** the DHCP Per Port function globally. The default is **Disabled**.

VLAN: at the dropdown select the desired VLAN for DHCP Per Port operation.

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 (24).

DHCP Per Port VLAN

The SM24TBT2DPB supports the DHCP IP Per Port function. It lets you have an IP address from a DHCP pool on a switch be statically assigned to a switchport, such that whichever device plugs into the switchport it will always be assigned that specific IP address. The IP address is configured in the interface config settings. Note that this is binding an IP address to an interface, not to a MAC address, which is the classic binding technique found on most switches.

DHCP Per Port VLAN: The VLAN associated with the IP interface. Only ports in this VLAN will be able to access the IP interface. This field is only available for input when creating a new interface. This 'DHCP IP per Port' function lets you assign a static IP address from a DHCP pool to a switch port such that it will always be assigned that specific IP address. (Added at FW vB6.64.0079.)

Buttons

Add Interface : Click to add a new IP interface. A maximum of 8 interfaces is supported.

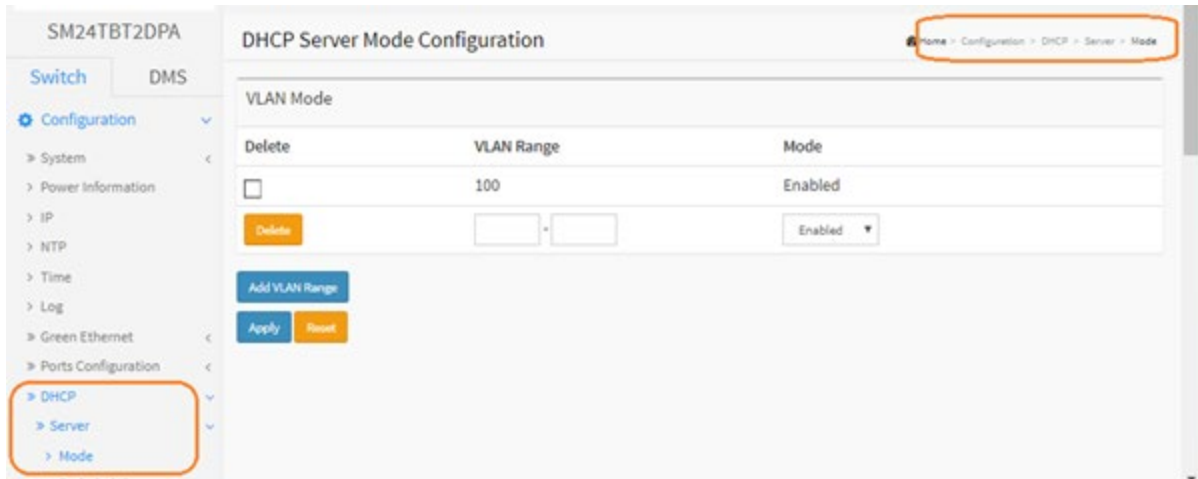
Add Route : Click to add a new IP route. A maximum of 32 routes is supported.

Apply: Click to save changes 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.

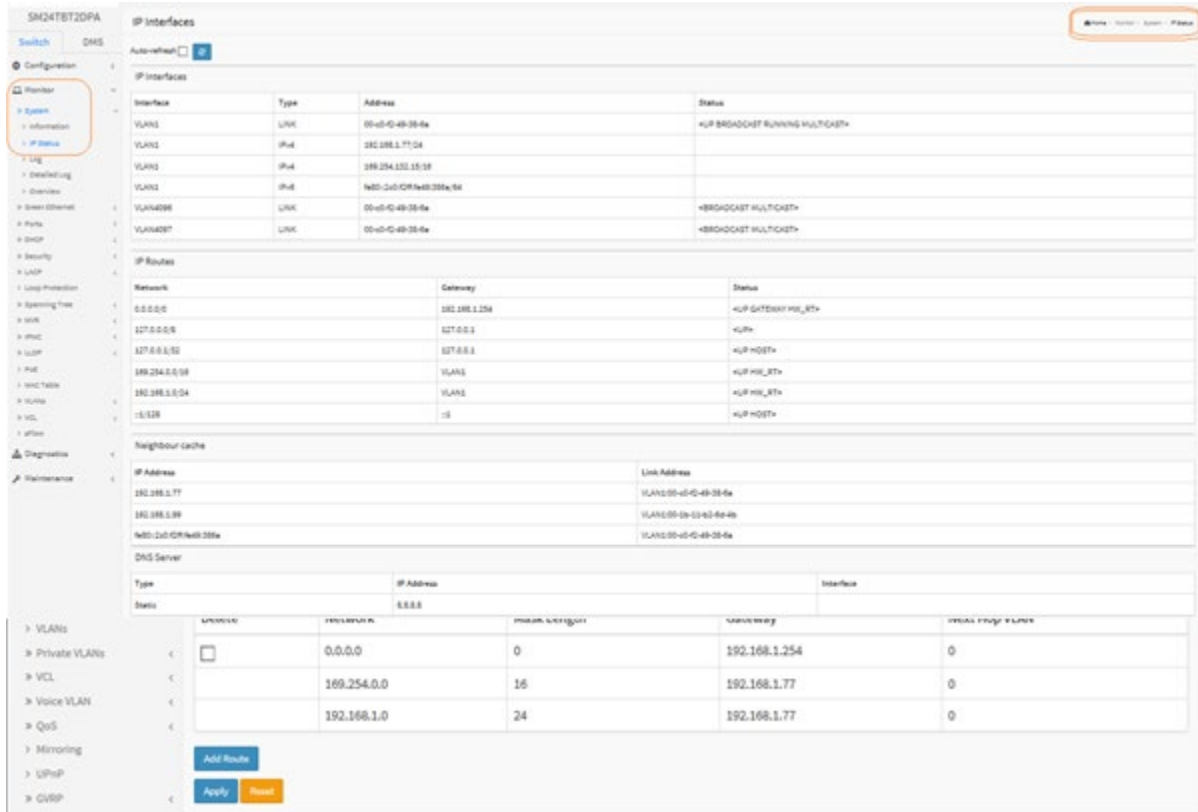
Reset: Click to undo any changes made locally and revert to previously saved values.

DHCP Server Mode Configuration

When DHCP Per Port is enabled and configured at **Configuration > System > IP**, the checkbox and selection in the DHCP Server Mode Configuration section at **Configuration > DHCP > Server > Mode** will become gray (cannot be selected):



To monitor DHCP Per Port status, navigate to the **Monitor > System > IP Status** menu path.



DHCP per Port Mode Web UI Messages

Message: *Interface xx not using DHCP*

Meaning: The Interface being configured does not have DHCP enabled and configured.

Recovery: **1.** Click the **OK** button to clear the webpage message. **2.** Enable and configure DHCP for the interface being configured. See “[DHCP Server Mode Configuration](#)” on page [375](#).

Message: *'DHCP Per Port IP range (192-168-1.80 - 192-168-1.99) is not equal to switch port number excluding uplink ports (10)*

Meaning: The IPv4 IP address range entered for the DHCP Per Port function was invalid.

Recovery: **1.** Click the **OK** button to clear the webpage message. **2.** Re-configure DHCP Per Port. See the [DHCP Per Port Mode Configuration](#) section above.

Message: *'DHCP Per Port IP range (192-168-1.70 - 192-168-1.85) includes interface IP Address (192.168.1.77)*

Meaning: The IPv4 IP address range entered for the DHCP Per Port function was invalid.

Recovery: **1.** Click the **OK** button to clear the webpage message. **2.** Re-configure DHCP Per Port. See the [DHCP Per Port Mode Configuration](#) section above. On the screen below, the range should be something like 192-168-1.80 - 192-168-1.85 to be valid.

Message: *The value of 'DNS Server' must be a valid IP address in dotted decimal notation ('x.y.z.w').*

Meaning: You entered an invalid IP address for the DNS Server being configured.

Recovery: **1.** Click the **OK** button to clear the webpage message. **2.** Enter a valid IP address in the format x.y.z.w per the on-screen restrictions. See “[DHCP Server Mode Configuration](#)” on page [376](#).

Message: *'DHCP Interface VLAN ID' must be an integer value between 1 and 4095.*

Meaning: You entered an invalid VLAN ID for the DHCP Interface.

Recovery: **1.** Click the **OK** button to clear the webpage message. **2.** Enter a valid VLAN ID for the DHCP Interface (1-4095). See “[DHCP Server Mode Configuration](#)” on page [376](#).

Message: *Subnet of VLAN 1 overlaps VLAN 2*

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 – Service, Warranty, and Tech Support

See the *SM24TBT2DPA Install Guide* or the *SM24TBT2DPB Install Guide* for related information.

Appendix C –Compliance Information

See the *SM24TBT2DPA Install Guide* or the *SM24TBT2DPB Install Guide* for related information.

**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

<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.