

SM24TBT4XPA

Managed 2.5G PoE++ Switch with IEEE 1588v2
(12) 10/100/1000Base-T ports, (12) 100/1G/2.5GBase-T ports,
and (4) 1G/10G SFP+ ports

Web User Guide

Intellectual Property

© 2025 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 www.lantronix.com/about/contact.

Disclaimer

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

Revision History

| Date | Rev | Description |
|-----------|-----|---|
| 5/24/24 | A | Initial Lantronix release at FW v 8.50.0139. |
| 8/15/24 | B | FW v8.50.0149: PercepXion related adjustments and bugs fixes. <ul style="list-style-type: none">• Add Auth Method default settings.• Correct the default fallback IP address.• Disable SNMP mode by default.• Fix PoE Firmware version display and fix PoE power output issue.• Note that 10 Mbps and 10 Gbps are not supported.• Remove 'Extend PoE Mode' feature.• See the Release Notes for details. |
| 3/26/2025 | C | FW v8.50.0160: <ul style="list-style-type: none">• Update PercepXion description.• Add Web Connect feature and capability negotiation to PercepXion. HTTPS must be enabled on the switch for Web Connect.• Add support for sending syslog to PercepXion server. See the Release Notes for details. |

Cautions and Warnings

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

Warnings indicate that there is the possibility of injury to person.

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



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



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

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

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

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

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

See *Install Guide* for electrical safety warnings translated into multiple languages.

Contents

| | |
|-------------------------------------|-----------|
| Cautions and Warnings | 4 |
| 1. Introduction | 11 |
| 1-1 Overview..... | 11 |
| 1-2 Key Features | 11 |
| 1-3 About This Manual | 11 |
| 1-4 Related Manuals..... | 12 |
| 1-5 Initial Setup..... | 12 |
| 1-6 First Time Wizard..... | 13 |
| 1-7 Web UI Controls | 16 |
| 2. System | 18 |
| 2-1 System Information | 18 |
| 2-2 IP Address..... | 20 |
| 2-2.1 Settings..... | 20 |
| 2-2.2 Advanced Settings..... | 22 |
| 2-2.3 Status..... | 25 |
| 2-3 System Time | 27 |
| 2-4 LLDP | 30 |
| 2-4.1 LLDP Configuration..... | 30 |
| 2-4.2 LLDP-MED Configuration..... | 32 |
| 2-4.3 LLDP Neighbor | 39 |
| 2-4.4 LLDP-MED Neighbor | 41 |
| 2-4.5 LLDP-MED Neighbor PoE..... | 44 |
| 2-4.6 LLDP Neighbor EEE | 45 |
| 2-4.7 LLDP Statistics..... | 46 |
| 2-5 UPnP | 48 |
| 3. Port Management | 49 |
| 3-1 Port Configuration | 49 |
| 3-2 Port Statistics..... | 51 |
| 3-3 SFP Port Info | 54 |
| 3-4 Energy Efficient Ethernet | 56 |
| 3-5 Link Aggregation..... | 57 |
| 3-5.1 Static Configuration..... | 57 |
| 3-5.2 Aggregation Status | 59 |
| 3-5.3 LACP Port Configuration..... | 60 |
| 3-5.4 System Status | 60 |
| 3-5.5 Internal Status | 62 |
| 3-5.6 Neighbor Status..... | 62 |
| 3-5.7 Port Status | 63 |
| 3-6 Loop Protection | 64 |
| 3-6.1 Configuration..... | 64 |
| 3-6.2 Status..... | 66 |
| 3-7 UDLD..... | 67 |

| | |
|------------------------------------|-----------|
| 3-7.1 UDLD Configuration | 67 |
| 3-7.2 UDLD Status..... | 67 |
| 4. PoE Management..... | 69 |
| 4-1 PoE Configuration..... | 69 |
| 4-2 PoE Status..... | 71 |
| 4-3 PoE Power Delay..... | 73 |
| 4-4 PoE Auto Power Reset..... | 73 |
| 4-5 PoE Scheduling Profile | 76 |
| 4-6 PoE Chip Reset Schedule | 76 |
| 5. VLAN Management | 78 |
| 5-1 VLAN Configuration | 78 |
| 5-2 VLAN Membership | 81 |
| 5-3 VLAN Port Status | 83 |
| 5-4 VLAN Name Configuration | 85 |
| 5-5 MAC-based VLAN | 86 |
| 5-5.1 Configuration..... | 86 |
| 5-5.2 Status..... | 86 |
| 5-6 Protocol-based VLAN..... | 88 |
| 5-6.1 Protocol to Group..... | 88 |
| 5-6.2 Group to VLAN | 90 |
| 5-7 IP Subnet-based VLAN | 90 |
| 5-8 GVRP | 92 |
| 5-9 Private VLAN..... | 94 |
| 5-10 Port Isolation | 95 |
| 5-11 Voice VLAN | 96 |
| 5-11.1 Configuration | 96 |
| 5-11.2 OUI | 98 |
| 6. Quality of Service | 99 |
| 6-1 Port Classification | 99 |
| 6-2 Port Policers | 102 |
| 6-3 Port Shapers | 103 |
| 6-4 Storm Control | 105 |
| 6-5 Port Scheduler | 107 |
| 6-6 Port PCP Remarking..... | 108 |
| 6-7 DSCP | 109 |
| 6-7.1 Port DSCP | 109 |
| 6-7.2 DSCP Translation | 111 |
| 6-7.3 DSCP Classification | 113 |
| 6-7.4 DSCP-Based QoS..... | 113 |
| 6-8 QoS Control List..... | 114 |
| 6-8.1 Configuration..... | 114 |
| 6-8.2 Status..... | 119 |
| 6-9 QoS Statistics | 121 |
| 6-10 WRED | 122 |

| | |
|---------------------------------------|------------|
| 7. Spanning tree..... | 124 |
| 7-1 STP Configuration | 124 |
| 7-2 MSTI Configuration..... | 127 |
| 7-3 STP Status | 130 |
| 7-4 Port Statistics | 133 |
| 8. MAC Address Table | 134 |
| 8-1 Configuration | 134 |
| 8-2 Information..... | 136 |
| 9. Multicast..... | 137 |
| 9-1 IGMP Snooping | 137 |
| 9-1.1 Basic Configuration | 137 |
| 9-1.2 VLAN Configuration | 140 |
| 9-1.3 Status..... | 142 |
| 9-1.4 Group Information | 143 |
| 9-1.5 IGMP SFM Information | 144 |
| 9-2 MLD Snooping | 146 |
| 9-2.1 Basic Configuration | 146 |
| 9-2.2 VLAN Configuration..... | 149 |
| 9-2.3 Status..... | 151 |
| 9-2.4 Groups Information..... | 153 |
| 9-2.5 MLD SFM Information | 153 |
| 9-3 MVR | 155 |
| 9-3.1 Basic Configuration | 155 |
| 9-3.2 Statistics | 156 |
| 9-3.3 Groups Information..... | 158 |
| 9-3.4 MVR SFM Information..... | 159 |
| 9-4 Multicast Filtering Profile | 160 |
| 9-4.1 Filtering Profile Table | 160 |
| 9-4.2 Filtering Address Entry | 162 |
| 10. DHCP | 163 |
| 10-1 Snooping..... | 163 |
| 10-1.1 Configuration | 163 |
| 10-1.2 Snooping Table | 165 |
| 10-1.3 Detailed Statistics | 166 |
| 10-2 Relay | 168 |
| 10-2.1 Configuration | 168 |
| 10-2.2 Statistics | 170 |
| 10-3 Server | 172 |
| 10-3.1 Configuration | 172 |
| 10-3.2 Status..... | 172 |
| 11. Security | 173 |
| 11-1 Management | 173 |
| 11-1.1 Account | 173 |

| | |
|---------------------------------|------------|
| 11-1.2 Privilege Levels | 175 |
| 11-1.3 Auth Method | 177 |
| 11-1.4 Access Method | 179 |
| 11-1.5 HTTPS | 179 |
| 11-2 802.1X..... | 181 |
| 11-2.1 Configuration | 181 |
| 11-2.2 Status..... | 187 |
| 11-3 IP Source Guard | 189 |
| 11-3.1 Configuration | 189 |
| 11-3.2 Static Table | 190 |
| 11-3.3 Dynamic Table | 191 |
| 11-4 ARP Inspection..... | 192 |
| 11-4.1 Configuration | 192 |
| 11-4.2 VLAN Configuration..... | 194 |
| 11-4.3 Static Table | 195 |
| 11-4.4 Dynamic Table | 196 |
| 11-5 Port Security | 196 |
| 11-5.1 Configuration | 196 |
| 11-5.2 Status..... | 199 |
| 11-6 RADIUS..... | 202 |
| 11-6.1 Configuration | 202 |
| 11-6.2 Status..... | 204 |
| 11-7 TACACS+ | 208 |
| 12. Access Control | 210 |
| 12-1 Ports Configuration | 210 |
| 12-2 Rate Limiters..... | 212 |
| 12-3 Access Control List..... | 212 |
| 12-4 ACL Status..... | 222 |
| 13. SNMP | 224 |
| 13-1 Configuration..... | 224 |
| 13-2 SNMPv3 | 226 |
| 13-2.1 Communities | 226 |
| 13-2.2 Users..... | 226 |
| 13-2.3 Groups | 229 |
| 13-2.4 Views | 230 |
| 13-2.5 Access | 230 |
| 13-3 Statistics | 232 |
| 13-3.1 Configuration | 232 |
| 13-3.2 Statistics | 233 |
| 13-4 History | 235 |
| 13-4.1 Configuration | 235 |
| 13-4.2 Status..... | 235 |
| 13-5 Alarm | 237 |

| | |
|---|------------|
| 13-5.1 Configuration | 237 |
| 13-5.2 Status..... | 239 |
| 13-6 Event..... | 240 |
| 13-6.1 Configuration | 240 |
| 13-6.2 Status..... | 240 |
| 14. MEP | 242 |
| 14-1 MEP Configuration | 242 |
| 15. ERPS..... | 244 |
| 16. EPS..... | 249 |
| 17. Percepixon and LPM..... | 250 |
| 17-1 Percepixon Agent Configuration | 251 |
| 17-2 Percepixon Upload | 253 |
| 18. PTP..... | 254 |
| 18-1 Configuration..... | 254 |
| 18-2 Status..... | 262 |
| 19. Event Notification | 264 |
| 19-1 SNMP Trap..... | 264 |
| 19-2 eMail..... | 266 |
| 19-3 Log | 267 |
| 19-3.1 Syslog..... | 267 |
| 19-3.2 View Log | 267 |
| 19-4 Event Configuration..... | 270 |
| 20. Diagnostics..... | 272 |
| 20-1 Ping | 272 |
| 20-2 Traceroute | 274 |
| 20-3 Cable Diagnostics..... | 275 |
| 20-4 Mirroring | 276 |
| 20-5 sFlow..... | 277 |
| 20-5.1 Configuration | 277 |
| 20-5.2 Statistics | 279 |
| 21. Maintenance | 281 |
| 21-1 Configuration..... | 281 |
| 21-1.1 Save startup-config | 281 |
| 21-1.2 Backup | 282 |
| 21-1.3 Restore | 283 |
| 21-1.4 Activate | 283 |
| 21-1.5 Delete | 285 |
| 21-2 Restart Device | 286 |
| 21-3 Factory Defaults | 287 |
| 21-4 Firmware | 288 |
| 21-4.1 Firmware Upgrade | 288 |
| 21-4.2 Firmware Selection | 289 |

22. DMS (Device Management System)..... 290

22-1 DMS Mode - DMS Controller Switch 291

22-2 DMS Mode 292

22-3 Graphical Monitoring 293

22-3.1 Topology View 293

22-3.2 DMS Firmware Upgrade Procedure 299

22-3.3 Floor View 301

22-3.4 Map View 303

22-4 Management 305

22-4.1 Device List 305

22-4.2 MAP API Key..... 307

22-5 Maintenance > Floor Image 308

22-6 Maintenance > Diagnostics 310

22-7 Maintenance > Traffic Monitor 312

22-8 DMS Troubleshooting..... 314

1. Introduction

1-1 Overview

The Lantronix SM24TBT4XPA is a next generation industrial L2+ managed GbE PoE+ switch that provides a reliable infrastructure for your business network. This switch delivers more intelligent features that you need to improve the availability of your critical business applications, protect your sensitive information, and optimize your network bandwidth. It provides the ideal combination of affordability and capabilities for small business or enterprise applications and helps you create a more efficient, better-connected workforce.

The embedded Device Managed System (DMS) features provides users with the benefits of easy-to-use/configure/install/troubleshoot in the video surveillance, wireless access, and other SMBs and Enterprises applications. The SM24TBT4XPA is ideal to deliver management simplicity, better user experience, and lowest total cost of ownership.

1-2 Key Features

- L2 features provide better manageability, security, QoS, and performance
- IPv4/IPv6 dual stack management
- SSH/SSL secured management
- SNMP v1/v2c/v3
- RMON groups 1,2,3,9
- IGMP v1/v2 Snooping
- MLD v1/v2 Snooping
- RADIUS and TACACS+ authentication
- IP Source Guard
- DHCP Relay (Option 82)
- DHCP Snooping
- ACL and QCL for traffic filtering
- 802.1D (STP), 802.1w (RSTP) and 802.1s (MSTP)
- LACP and static link aggregation
- Q-in-Q double tag VLAN
- GVRP dynamic VLAN
- Device Managed System (DMS)
- PercepXion and LPM support

1-3 About This Manual

This GUI user guide gives specific information on how to operate and use the management functions of the SM24TBT4XPA via an HTTP/HTTPS web browser.

This manual is intended for use by network administrators who are responsible for operating and maintaining network equipment; consequently, it assumes a working knowledge of Ethernet switch functions, the Internet Protocol (IP), and Hypertext Transfer Protocol (HTTP and HTTPS).

Note that this manual provides links to third party web sites for which Lantronix is not responsible.

1-4 Related Manuals

Related manuals include:

- SM24TBT4XPA Quick Start Guide, 33875
- SM24TBT4XPA Web User Guide, 33877
- SM24TBT4XPA CLI Reference, 33878
- Release Notes (version specific)

For Lantronix Drivers, Firmware, Manuals, etc. go to the Lantronix [Technical Resource Center](https://www.lantronix.com/support/documentation). Visit the Lantronix Web site at www.lantronix.com/support/documentation for the latest documentation.

Note that this manual provides links to third party web sites for which Lantronix is not responsible.

1-5 Initial Setup

This section describes how to log in to the SM24TBT4XPA via the web UI. With this facility, you can easily access and monitor from any port of the switch.

The default values of the SM24TBT4XPA 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

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 switch will not give you a shortcut to the username automatically. This looks inconvenient but is safer.

The SM24TBT4XPA allows two or more admin users to manage this switch at the same time; whichever admin user made the last settings will present the configuration that the system will use.

When you login to the SM24TBT4XPA Web UI management, you can use IPv4 or IPv6 login to manage the switch.

Note: The SM24TBT4XPA has the DHCP function disabled by default, so if you do not have DHCP server to provide an IP address to the switch, use the default switch IP address of 192.168.1.77.

The Login page is shown below:



Figure 1-5: The Login page

1-6 First Time Wizard

When you log in to the switch the first time, a First Time Wizard displays. On subsequent power ups, you can perform switch configuration using a web browser.

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.

The figure shows two screenshots of the Lantronix web interface during the First Time Wizard. The left screenshot is titled 'Change default password' and features a progress bar at the top with four steps: 1. PASSWORD, 2. IP ADDRESS, 3. DATE & TIME, and 4. INFORMATION. The 'PASSWORD' step is currently active. The form includes two text input fields: 'New password' and 'Repeat new password'. Below these fields, a note states: 'Password must contain: 1. Minimum of 8 characters 2. At least 1 upper case, 1 lower case and 1 numeric. New password should not be blank or default value.' A blue 'Next' button is at the bottom. The right screenshot is titled 'Set IP address' and has the same progress bar, but the 'IP ADDRESS' step is active. It includes a dropdown for 'Interface VLAN ID' (set to 1), two radio buttons for 'Obtain IP address via DHCP' (unselected) and 'Set IP address manually' (selected), and text input fields for 'IP address' (192.168.1.77), 'Subnet mask' (255.255.255.0), 'Default router' (192.168.1.254), and 'DNS'. 'Previous' and 'Next' buttons are at the bottom.

Figure 1-6: Change default password

Step 2: Set IP address

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

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

Click the **Next** button.

The figure shows two screenshots of the Lantronix web interface during the First Time Wizard, both titled 'Set IP address'. The left screenshot has the same progress bar as the previous figure, with the 'IP ADDRESS' step active. It includes a dropdown for 'Interface VLAN ID' (set to 1), two radio buttons for 'Obtain IP address via DHCP' (unselected) and 'Set IP address manually' (selected), and text input fields for 'IP address' (192.168.1.77), 'Subnet mask' (255.255.255.0), 'Default router' (192.168.1.254), and 'DNS'. 'Previous' and 'Next' buttons are at the bottom. The right screenshot has the same progress bar, but the 'DATE & TIME' step is active. It includes a dropdown for 'Interface VLAN ID' (set to 1), two radio buttons for 'Obtain IP address via DHCP' (selected) and 'Set IP address manually' (unselected), and a text input field for 'DNS'. 'Previous' and 'Next' buttons are at the bottom.

Figure 1-6a: 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 1-6b: 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 data and time” or select “Manually” to set or select the desired date and time.

If you enable “Automatic data and time” then you must enter a “Server Address” and select a “Time zone”. Click the **Next** button when done.

LANTRONIX®

Set date and time

Automatic date and time ☐

Manually
2022-02-03 14:23:6

Previous Next

Figure 1-6c: 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.



The screenshot shows the Lantronix logo at the top. Below it is a progress bar with four steps: 1. PASSWORD, 2. IP ADDRESS, 3. DATE & TIME, and 4. INFORMATION. The fourth step, INFORMATION, is highlighted. Below the progress bar is a form titled 'Set system information'. The form contains three text input fields: 'System contact' (empty), 'System name' (containing 'SM16TAT2SA'), and 'System location' (empty). At the bottom of the form are two buttons: 'Previous' and 'Apply'.

Figure 1-6d: 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').

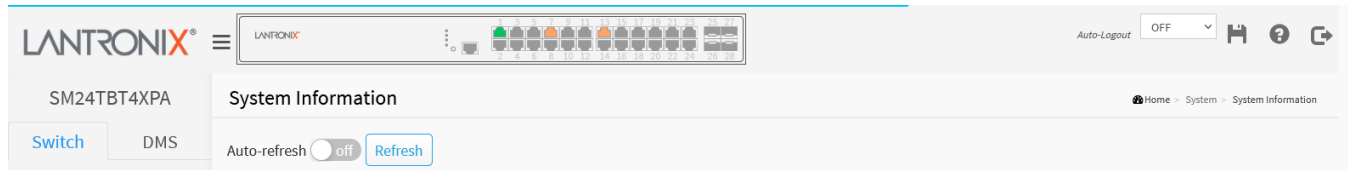
The following restrictions apply: 1) x, y, z, and w must be decimal numbers between 0 and 255, 2) x must not be 0 unless also y, z, and w are 0, 3) x must not be 127, and 4) x must not be greater than 223.


Note: The First Time Wizard only displays on the switch web GUI. If you have logged in via CLI or Console and have saved changes to the running-config file, the First Time Wizard will not display in the web UI.

The First Time Wizard displays when you use the hardware Reset button to reset the switch. Press the Reset button for over 10 seconds; when the front panel LEDs light then release the Reset button.




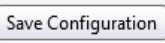


1-7 Web UI Controls

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 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 (  ).

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.

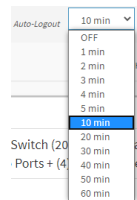
To examine the running-config, you can run the CLI command "showing running-config" or in the Web UI just log out and log back in again.

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 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 diskette icon), the changed timeout setting will be applied to running-config and start-up config immediately. | When you change the timeout setting (without save to startup-config), the timeout change will be applied to running-config immediately. |
| After Logout and login, the timeout setting will be the setting saved in start-up config. | After Logout and login, the timeout setting will be the setting saved in start-up configure. |
| After a switch reboot, the timeout setting will be the setting saved in start-up config. | After you reboot the switch, the timeout setting will be the setting saved in start-up config. |

Click Save Button [Click Save Button](#) : displays in the top right corner when a change has been made and can be saved by clicking the Save button to save the changes to the startup-config file.

2. System

This chapter describes basic information included on the System pages (e.g. Time, Account, IP, Syslog, NTP).

2-1 System Information

You can identify the system by entering a system name, location, and contact of the switch. To configure System Information in the web UI:

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

The screenshot displays the 'System Information' page in the Lantronix web UI. The left sidebar shows a navigation menu with 'System' and 'System Information' selected. The main content area lists various system parameters and their values:

| Parameter | Value |
|---------------------------|---|
| Model Name | SM24TBT4XPA |
| System Description | 12 ports 10M/100M/1G PoE+ RJ45 + 12 ports 100M/1G/2.5G PoE++ RJ45 + 4 ports 10G SFP+ (PoE 740W) |
| Location | |
| Contact | |
| System Name | SM24TBT4XPA |
| System Date | 2016-01-01T00:06:48+00:00 |
| System Uptime | 00:07:12 |
| Bootloader Version | V1.05 |
| Firmware Version | v8.50.0149 2024-05-31 |
| PoE Firmware Version | 220-355 |
| Hardware Version | v1.01 |
| Mechanical Version | v1.01 |
| Serial Number | A212121AR5000001 |
| MAC Address | 00-40-c7-1d-1c-c2 |
| Fan Speed | 1479(rpm) |
| Temperature 1 | 33(C) |
| Temperature 2 | 32(C) |
| Temperature 3 | 35(C) |
| CPU Load (100ms, 1s, 10s) | 0%, 9%, 46% |

Parameter descriptions:

Model Name: Shows the factory defined model name for identification purposes.

System Description: Displays the system description.

Location: Enter a system location for this switch.

Contact: Enter a system contact for this switch.

System Name: Enter a system name for this switch.

System Date: Displays the current (GMT) system time and date. The system time is obtained from the Timing server running on the switch, if any.

System Uptime: Displays the period the switch has been operational.

Bootloader Version: Displays the current boot loader version number.

Firmware Version: Displays the current firmware version running on this switch.

PoE Firmware Version: Displays the current firmware version running on this switch.

Hardware Version: Displays the hardware version of this switch.

Mechanical Version: Displays the mechanical version of the device.

Serial Number: The serial number of this switch.

MAC Address: The MAC Address of this switch.

Fan Speed: The current speed of the switch fan in RPMs.

Temperature 1: Displays the temperature 1 of the system.

Temperature 2: Displays the temperature 2 of the system.

CPU Load (100ms, 1s, 10s): Displays the cpu loading (100ms, 1s, 10s) of the system. The CPU load is a measure of the amount of computational work that a system performs. The CPU load is displayed for the last 100 milliseconds, one second, and 10 second periods.

Buttons

Apply: Click to save changes.

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

Refresh: Click to refresh the page immediately.

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

2-2 IP Address

The IPv4 address for the switch can be obtained via DHCP Server for VLAN 1. To manually configure an address, you must change the switch's default settings to values that are compatible with your network.

You may also need to establish a default gateway between the switch and management stations that exist on another network segment.

2-2.1 Settings

This page lets you configure basic IP settings and control IP interfaces and IP routes. To configure an IP Settings in the web UI:

1. Click System, IP Address, and Settings.
2. Enable or Disable the IPv4 DHCP Client.
3. Specify the IPv4 Address, Subnet Mask, and Gateway.
4. Select a DNS Server setting.
5. Click Apply.

The screenshot shows the Lantronix SM24TBT4XPA web interface. The top navigation bar includes the Lantronix logo, a menu icon, and a status bar with 'Auto-Logout OFF' and a 'Click Save Button' link. The left sidebar shows the navigation menu with 'System', 'IP Address', and 'Settings' selected. The main content area displays the 'Settings' page for IP Address. It features a table with the following settings:

| Setting | Value |
|-------------------------|---------------|
| IPv4 DHCP Client Enable | on |
| IPv4 Address | 172.27.100.89 |
| Subnet Mask | 255.255.255.0 |
| Gateway | 172.27.100.1 |
| DNS Server | No DNS server |

An 'Apply' button is located at the bottom left of the settings table.

Figure 2-2.1: IP Settings

Parameter descriptions:

IPv4 DHCP Client Enable: Select the switch to enable (on) or disable (off) the DHCP client. If enabled, the system will configure the IPv4 address and mask of the interface using DHCP protocol. The DHCP client will announce the configured System Name as hostname to provide DNS lookup. The default is **off**.

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.

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

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

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

No DNS server: No DNS server will be used.

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

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

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

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

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

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

No DNS server

Configured IPv4 or IPv6

From any DHCPv4 interfaces

From this DHCPv4 interface

From any DHCPv6 interfaces

From this DHCPv6 interface

Buttons

Apply: Click to save changes.

2-2.2 Advanced Settings

Configure switch-managed IP information on this page, including basic IP settings, IP interfaces, and IP routes. The maximum number of interfaces supported is 128 and the maximum number of routes is 128.

To configure Advanced Settings in the web UI:

1. Click System, IP Address, and Advanced Settings.
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.

LANTRONIX SM24TBT4XPA

Auto-Logout: OFF [Click Save Button](#)

Home > System > IP Address > Advanced Settings

Advanced Settings

Mode: Host

DNS Server 1: No DNS server

DNS Server 2: No DNS server

DNS Server 3: No DNS server

DNS Server 4: No DNS server

DNS Proxy: ☐

IP Interfaces

DHCP Per Port

Mode: Disabled

VLAN: VLAN 1

IP: -

| | | IPv4 DHCP | | | IPv4 | | IPv6 DHCP | | | IPv6 | |
|--------|------|-------------------------------------|----------|------------------|-------------|-------------|--------------------------|--------------------------|---------------|---------|-------------|
| Delete | VLAN | Enable | Fallback | Current Lease | Address | Mask Length | Enable | Rapid Commit | Current Lease | Address | Mask Length |
| | 1 | <input checked="" type="checkbox"/> | 30 | 172.27.100.89/24 | 192.168.1.1 | 24 | <input type="checkbox"/> | <input type="checkbox"/> | | | |

[Add Interface](#)

Link-Local Address binding interface: VLAN 1

IP Routes

| Delete | Network | Mask Length | Gateway | Distance/Next Hop VLAN |
|--------------------------|--------------|-------------|--------------|------------------------|
| <input type="checkbox"/> | 0.0.0.0 | 0 | 172.27.100.1 | 254 |
| | 169.254.0.0 | 16 | 192.168.1.1 | 0 |
| | 172.27.100.0 | 24 | 192.168.1.1 | 0 |

[Add Route](#)

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

Figure 2-2.2: IP Advanced Settings

Parameter descriptions:**Advanced Settings**

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

DNS Server 1-4: This setting controls the DNS name resolution done by the switch. There are four servers available for configuration, and the index of the server presents the preference (less index has higher priority) in doing DNS name resolution. The following modes are supported:

No DNS server: No DNS server will be used.

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

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

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

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

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

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

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

IP Interfaces

Delete: Check the box to remove the VLAN instance from the table.

DHCP Per Port Mode: At the dropdown select to Enable or Disable the DHCP per Port operation. The default is Disabled.

DHCP Per Port VLAN: At the dropdown select the VLAN to be associated with the IP interface. Only ports in this VLAN will be able to access the IP interface. This field is only available for input when creating a new interface. This 'DHCP IP per Port' function lets you assign a static IP address from a DHCP pool to a switch port such that it will always be assigned that specific IP address. The IP address is configured in the Interface Config settings. Note that this is binding an IP address to an interface, not to a MAC address, which is the typical binding method used on this and most other switches.

DHCP Per Port IP: Enter the IP address range for DHCP Per Port. The range must be equal to the number of switch RJ45/TP ports (24 for the SM24TBT4XPA).

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.

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

IPv4 DHCP Current Lease: For DHCP interfaces with an active lease, this column show 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 a 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.

DHCPv6Enable: Enable the DHCPv6 client by checking this box. If this option is enabled, the system will configure the IPv6 address of the interface using the DHCPv6 protocol.

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

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

IPv6 Address: The IPv6 address of the interface. A IPv6 address is in 128-bit records represented as eight fields of up to four hexadecimal digits with a colon separating each field (:). For example, fe80::215:c5ff:fe03:4dc7. The symbol :: is a special syntax that can be used as a shorthand way of representing multiple 16-bit groups of contiguous zeros; but it can appear only once. 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 1 - 128 bits for an IPv6 address. The field may be left blank if IPv6 operation on the interface is not desired.

Link-Local Address binding interface: At the dropdown select the desired VLAN (by default VLAN 1). A link-local address is a network address that is valid only for communications on a local link, i.e. within a subnetwork that a host is connected to. Link-local addresses are not guaranteed to be unique beyond their network segment. IPv4 link-local unicast addresses are assigned from address block 169.254.0.0/16 (169.254.0.0 through 169.254.255.255). In IPv6, unicast link-local addresses are assigned from the block fe80::/10.

IP Routes

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

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

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

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

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

Buttons

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

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

Apply: Click to save changes.

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

Messages:

DHCP Per Port IP range (192.168.1.1 - 192.168.1.10) includes interface IP address (192.168.1.1)

2-2.3 Status

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

To display IP status in the web UI:

1. Click System, IP Address, Status and IP Status.
2. View the IP Configuration information.

The screenshot shows the Lantronix web interface for the SM24TBT4XPA device. The 'Status' page is active, showing IP configuration details. The sidebar on the left lists various system settings, with 'IP Address' and 'Status' highlighted. The main content area has an 'Auto-refresh' toggle set to 'off' and a 'Refresh' button. Below this, three tables are displayed:

| Interface | Type | Address | Status |
|-----------|------|-----------------------------|--------------------------|
| VLAN1 | LINK | 00-c0-f2-a8-a3-bd | <UP BROADCAST MULTICAST> |
| VLAN1 | IPv4 | 172.27.100.89/24 | |
| VLAN1 | IPv6 | fe80::2c0:f2ff:fea8:a3bd/64 | |

| Network | Gateway | Status |
|--------------|-------------|--------------------|
| 169.254.0.0 | 192.168.1.1 | directly connected |
| 172.27.100.0 | 192.168.1.1 | directly connected |

| IP Address | Link Address |
|----------------|-------------------------|
| 169.254.11.154 | VLAN1:00-16-6c-d4-dd-bf |
| 169.254.101.50 | VLAN1:00-c0-f2-87-be-b5 |
| 172.27.100.1 | VLAN1:18-7a-3b-38-8e-8a |
| 172.27.100.4 | VLAN1:d8-cb-8a-8f-cb-55 |
| 172.27.100.5 | VLAN1:50-9a-4c-19-ad-0a |

Figure 2-2.3: IP Status

Parameter descriptions:

IP Interfaces

Interface: Show the name of the interface.

Type: Show the address type of the entry. This may be LINK or IPv4 or IPv6.

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

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

IP Routes

Network: Show the destination IP network or host address of this route.

Gateway: Show the gateway address of this route.

Status: Show the status flags of the route.

Neighbour cache

IP Address: Show the IP address of the entry.

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

Buttons

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

Refresh: Click to refresh the page immediately.

2-3 System Time

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

To configure Time in the web UI:

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

The screenshot displays the Lantronix web interface for the SM24TBT4XPA switch, specifically the 'Time Configuration' page. The left sidebar shows a navigation menu with 'System' and 'System Time' selected. The main content area is divided into three sections: 'Time Configuration', 'Time Zone Configuration', and 'Daylight Saving Time Configuration'. In the 'Time Configuration' section, the 'Clock Source' is set to 'Use Local Settings' (with a 'Configure NTP Server' button available), and the 'System Date' is '2016-01-01 00:07:53'. The 'Time Zone Configuration' section shows the 'Time Zone' set to 'None' and an 'Acronym' field. The 'Daylight Saving Time Configuration' section shows 'Daylight Saving Time' set to 'Disabled'. Below these are 'Start Time settings' and 'End Time settings', each with dropdowns for Month, Date, Year, Hours, and Minutes. An 'Offset settings' section shows an 'Offset' of '1' minute. At the bottom, there are 'Apply' and 'Reset' buttons.

Figure 2-3: Time configuration

Time Configuration

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

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

Time Zone Configuration

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

Acronym: User can set the acronym of the time zone. This is a user configurable acronym to identify the time zone. (Range: 0 to 16 characters.)

Daylight Savings 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).

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 starting week number.

Day - Select the starting day.

Month - Select the starting month.

Hours - Select the starting hour.

Minutes - Select the starting minute.

Offset settings:

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

Note: The information 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.

| | | |
|--------------|-------------------------|---------------------------------|
| Clock Source | <div>NTP Server ▼</div> | <div>Configure NTP Server</div> |
|--------------|-------------------------|---------------------------------|

Configure NTP Server: Click to configure NTP server when Clock Source is set to select from NTP Server.

Figure 2-3: NTP Configuration

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

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

Parameter descriptions:

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 legally 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.

2-4 LLDP

The switch supports the LLDP for current information on your switch model, The Link Layer Discovery Protocol (LLDP) provides a standards-based method for enabling switches to advertise themselves to adjacent devices and to learn about adjacent LLDP devices. The Link Layer Discovery Protocol (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.

2-4.1 LLDP Configuration

This page lets you view and configure current LLDP and port settings. To configure LLDP:

1. Click System, LLDP and 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.

LANTRONIX SM24TBT4XPA

LLDP Configuration

Home > System > LLDP > LLDP Configuration

Auto-Logout: OFF

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 | Trap | 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 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 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 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 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 type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> |

Figure 2-4.1: LLDP Configuration

Parameter descriptions:

LLDP Parameters

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

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

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

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

LLDP Port Configuration

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

Mode : Select LLDP mode:

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

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

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

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

CDP Aware : Select CDP awareness.

CDP operation is restricted to decode incoming CDP frames (the switch doesn't transmit CDP frames). CDP frames are only decoded if LLDP is enabled on the port.

Only CDPTLVs 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.).

CDPTLVs are mapped onto LLDP neighbors' table as shown below.

CDPTLV "Device ID" is mapped to the LLDP "Chassis ID" field.

CDPTLV "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.

CDPTLV "Port ID" is mapped to the LLDP "Port ID" field.

CDPTLV "Version and Platform" is mapped to the LLDP "System Description" field.

Both the CDP and LLDP support "system capabilities", but the CDP capabilities cover capabilities that are not part of the LLDP. These capabilities are shown as "others" in the LLDP neighbors' table.

If all ports have CDP awareness disabled the switch forwards CDP frames received from neighbor devices. If at least one port has CDP awareness enabled all CDP frames are terminated by the switch.

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

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

Optional TLVs

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

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

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

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

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

Buttons

Apply: Click to save changes.

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

2-4.2 LLDP-MED Configuration

Media Endpoint Discovery is an enhancement of LLDP, known as LLDP-MED, that provides the following 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, allowing network administrators to track their network devices, and determine their characteristics (manufacturer, software and hardware versions, and serial or asset number).

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

To configure LLDP-MED:




1. Click System, LLDP and LLDP-MED Configuration.
2. Modify Fast start repeat count parameter.
3. Modify Transmit TLVs parameters.
4. Modify Coordinates Location parameters.
5. Fill Civic Address Location parameters.
6. Fill Emergency Call Service parameters.
7. Add New Policy.
8. Click Apply, will show following Policy Port Configuration.
9. Select a Policy ID for each port.
10. Click Apply.

LANTRONIX®

1 3 5 7 9 11 13 15 17 19 21 23 25 27

2 4 6 8 10 12 14 16 18 20 22 24 26 28

Auto-Logout OFF



SM24TBT4XPA

LLDP-MED Configuration

Home > System > LLDP > LLDP-MED Configuration

Switch

DMS

System

System Information

IP Address

System Time

LLDP

LLDP Configuration

LLDP-MED Configuration

LLDP Neighbor

LLDP-MED Neighbor

LLDP Neighbor PoE

LLDP Neighbor EEE

LLDP Statistics

UPnP

Port Management

PoE Management

Fast Start Repeat Count

Fast start repeat count4

Transmit TLVs

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

↓↓↓↓

Coordinates Location

Latitude0°North

Longitude0°East

Altitude0Meters

Map DatumWGS84

Civic Address Location

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

Emergency Call Service

Emergency Call Service

Policies

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

[Add New Policy](#)

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

Figure 2-4.2: LLDP-MED Configuration

Parameter descriptions:

Fast start repeat count

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

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

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

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

Transmit TLVs

Port: The interface name to which the configuration applies.

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

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

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

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

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

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

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

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

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

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

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

Coordinates Location

Latitude : Latitude SHOULD be normalized to within 0-90 degrees with a maximum of 4 digits. It is possible to specify the direction to either North of the equator or South of the equator.

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

Altitude : Altitude SHOULD be normalized to within -32767 to 32767 with a maximum of 4 digits. It is possible to select between two altitude types (floors or meters).

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

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

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

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

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

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

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

Country code : The two-letter ISO 3166 country code in capital ASCII letters (e.g., DK, DE or US).

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

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

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

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

Block (Neighborhood) : Neighborhood, Block.

Street : Street -Example: Poppelvej.

Leading street direction : Leading street direction -Example: N.

Trailing street suffix : Trailing street suffix -Example: SW.

Street suffix : Street suffix -Example: Ave, Platz.

House no. : House number -Example: 21.

House no. suffix : House number suffix -Example: A, 1/2.

Landmark : Landmark or vanity address -Example: Columbia University.

Additional location info : Additional location info -Example: South Wing.

Name : Name (residence and office occupant) -Example: Flemming Jahn.

Zip code : Postal/zip code (e.g., 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 format consists of a numerical digit string, corresponding to the ELIN to be used for emergency calling.

Policies

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

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

The network policy attributes advertised are:

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

This network policy is potentially advertised and associated with multiple sets of application types supported on a given port. The application types specifically addressed are Voice, Voice Signaling, Guest Voice, Guest Voice Signaling, Softphone Voice, Video Conferencing, Streaming Video, and Video Signaling.

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

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

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

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

Application Type : Intended use of the application types:

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

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

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

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

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

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

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

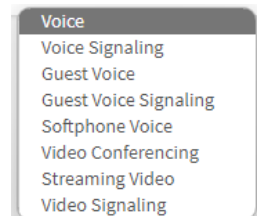
Video Signaling (conditional) - for use in network topologies that require a separate policy for the video signaling than for the video media. This application type should not be advertised if all the same network policies apply as those advertised in the Video Conferencing application policy.

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

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

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

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



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

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

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.

2-4.3 LLDP Neighbor

This page provides a status overview for all LLDP neighbors. The displayed table contains a row for each port on which an LLDP neighbor is detected. To show LLDP neighbor information:

1. Click System, LLDP and LLDP Neighbor.
2. Click the linked IP address in the Management Address column to display neighbor device information.
3. Click Refresh to manually update the web page.
4. Click Auto-refresh to automatically update the web page.

| Local Port | Chassis ID | Port ID | Port Description | System Name | System Capabilities | System Description | Management Address |
|------------------------|-------------------|---------|------------------|---------------------------------|----------------------|--|--|
| GigabitEthernet 1/1 | 18-7A-3B-38-8E-8A | 78 | 2/25 | MINNW-0001 | Bridge(+), Router(+) | Aruba JL256A 2930F-48G-PoE+-4SFP+ 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)) | 172.27.100.1 (IPv4) , fe80::1a7a:3bff:fe38:8e8a (IPv6) |
| 2.5GigabitEthernet 1/1 | E0-55-3D-84-A8-96 | 0 | wired0 | meraki admin network - wireless | | Meraki MV71 Cloud Managed Outdoor HD Dome Camera | 172.27.100.28 (IPv4) |

Figure 2-4.3: LLDP Neighbor Information

If no devices that supports LLDP in your network then the table will show *"No LLDP neighbor information found"*.

Parameter descriptions:

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

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

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

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

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

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

1. Other
2. Repeater
3. Bridge
4. WLAN Access Point
5. Router
6. Telephone
7. DOCSIS cable device
8. Station only
9. Reserved

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

Management Address : Management Address is the neighbor unit's address that is used for higher layer entities to assist discovery by the network management. This could for instance hold the neighbor's IP address.

You can click the linked IP address in the Management Address column to display neighbor device information.

Buttons

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

Refresh: Click to refresh the page immediately.

2-4.4 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-MED neighbor is detected. This function applies to devices which support LLDP-MED.

To show LLDP-MED neighbor information:

1. Click System, LLDP, and LLDP-MED Neighbor.
2. Click Refresh to manually update the web page.
3. Click Auto-refresh to automatically update the web page.

| LLDP-MED Neighbor Information | | | |
|-------------------------------|-------------------------|-------------------------------|------------------|
| GigabitEthernet 1/5 | | | |
| 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 |

Figure 2-4.4: LLDP-MED Neighbor Information

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

Parameter descriptions:

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

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

LLDP-MED Network Connectivity Device 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 the following technologies:

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

LLDP-MED Endpoint Device 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 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.

Possible capabilities are:

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

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

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

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

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, where:

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

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

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

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

DSCP : The DSCP value to be used to provide Diffserv node behavior for the specified application type as defined in IETF RFC 2474. Contains 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).

MAU Type: Displays the Medium Attachment Unit' Type or displays "*Invalid MAU Type*". See IETF RFC 4836 at iana.org/assignments/ianamau-mib/ianamau-mib

Buttons

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

Refresh: Click to refresh the page immediately.

2-4.5 LLDP-MED Neighbor PoE

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

To show LLDP neighbor PoE information:

1. Click System, LLDP, and LLDP Neighbor PoE.
2. Click Refresh for manual update web screen.
3. Click Auto-refresh for auto-update web screen.

The screenshot shows the Lantronix web interface for the SM24TBT4XPA device. The page title is "LLDP Neighbor Power Over Ethernet Information". On the left, there is a navigation menu with "System" selected, and "LLDP" is expanded. The main content area shows a table of LLDP neighbors. Above the table, there are controls for "Auto-refresh" (set to off) and a "Refresh" button. The table has five columns: Local Port, Power Type, Power Source, Power Priority, and Maximum Power. It contains two rows of data.

| Local Port | Power Type | Power Source | Power Priority | Maximum Power |
|------------------------|------------|--------------|----------------|---------------|
| GigabitEthernet 1/1 | PSE Device | Unknown | Unknown | 0 [W] |
| 2.5GigabitEthernet 1/1 | PD Device | PSE | Unknown | 22 [W] |

Figure 2-4.5: LLDP-MED Neighbor PoE information

Parameter descriptions:

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

Power Type: The Power Type represents whether the device is a Power Sourcing Entity (PSE) or Power Device (PD). If the Power Type is unknown it is represented as "Reserved".

Power Source: The Power Source represents the power source being utilized by a PSE or PD device. If the device is a PSE device it can either run on its Primary Power Source or its Backup Power Source. If it is unknown whether the PSE device is using its Primary Power Source or its Backup Power Source it is indicated as "Unknown".

If the device is a PD device it can either run on its local power supply or it can use the PSE as power source. It can also use both its local power supply and the PSE. If it is unknown what power supply the PD device is using it is indicated as "Unknown".

Power Priority: Represents the priority of the PD device, or the power priority associated with the PSE type device's interface that is sourcing the power. There are three levels of power priority. The three levels are: Critical, High, and Low. If the power priority is unknown it is indicated as "Unknown".

Maximum Power: Contains a numerical value that indicates the maximum power in watts required by a PD device from a PSE device, or the minimum power a PSE device is capable of sourcing over a maximum length cable based on its current configuration. The maximum allowed value is 102.3 W. If the device indicates value higher than 102.3 W, it is represented as "reserved".

Buttons

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

Refresh: Click to refresh the page immediately.

2-4.6 LLDP Neighbor EEE

By using EEE power savings can be achieved at the expense of traffic latency. This latency occurs because the circuits EEE turn off to save power, and 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 Tw and Rx Tw "wakeup time " to agree upon the minimum wakeup time they need.

This page provides an overview of EEE information exchanged by LLDP. To show LLDP neighbor EEE:

1. Click System, LLDP and LLDP Neighbor EEE.
2. Click Refresh to manually update the web page.
3. Click Auto-refresh to automatically update the web page.

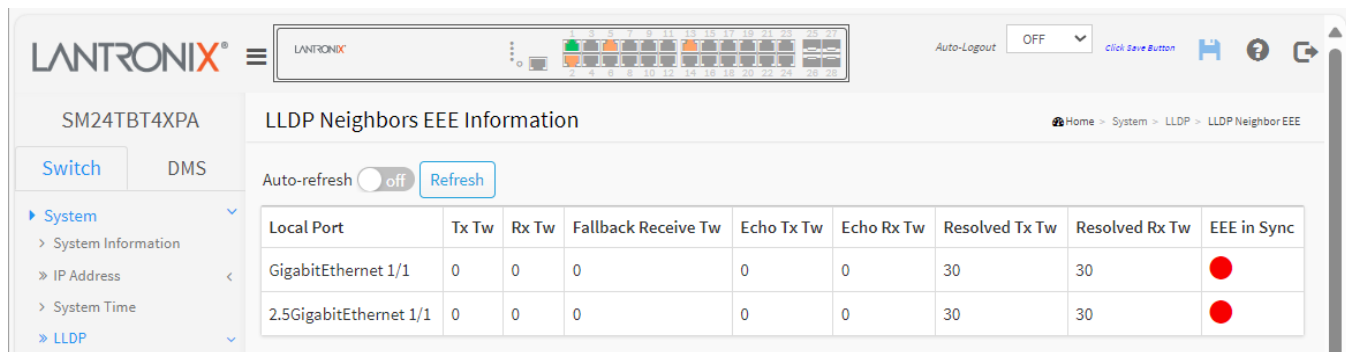


Figure 2-4.6: LLDP Neighbors EEE information

Parameter descriptions:

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

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

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

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

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

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

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

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

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

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

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

Buttons

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

Refresh: Click to refresh the page immediately.

2-4.7 LLDP Statistics

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

To show LLDP Statistics:

1. Click System, LLDP, and LLDP Statistics.
2. Click Refresh manually update the web page.
3. Click Auto-refresh to automatically update the web page.
4. Click Clear to clear all counters.

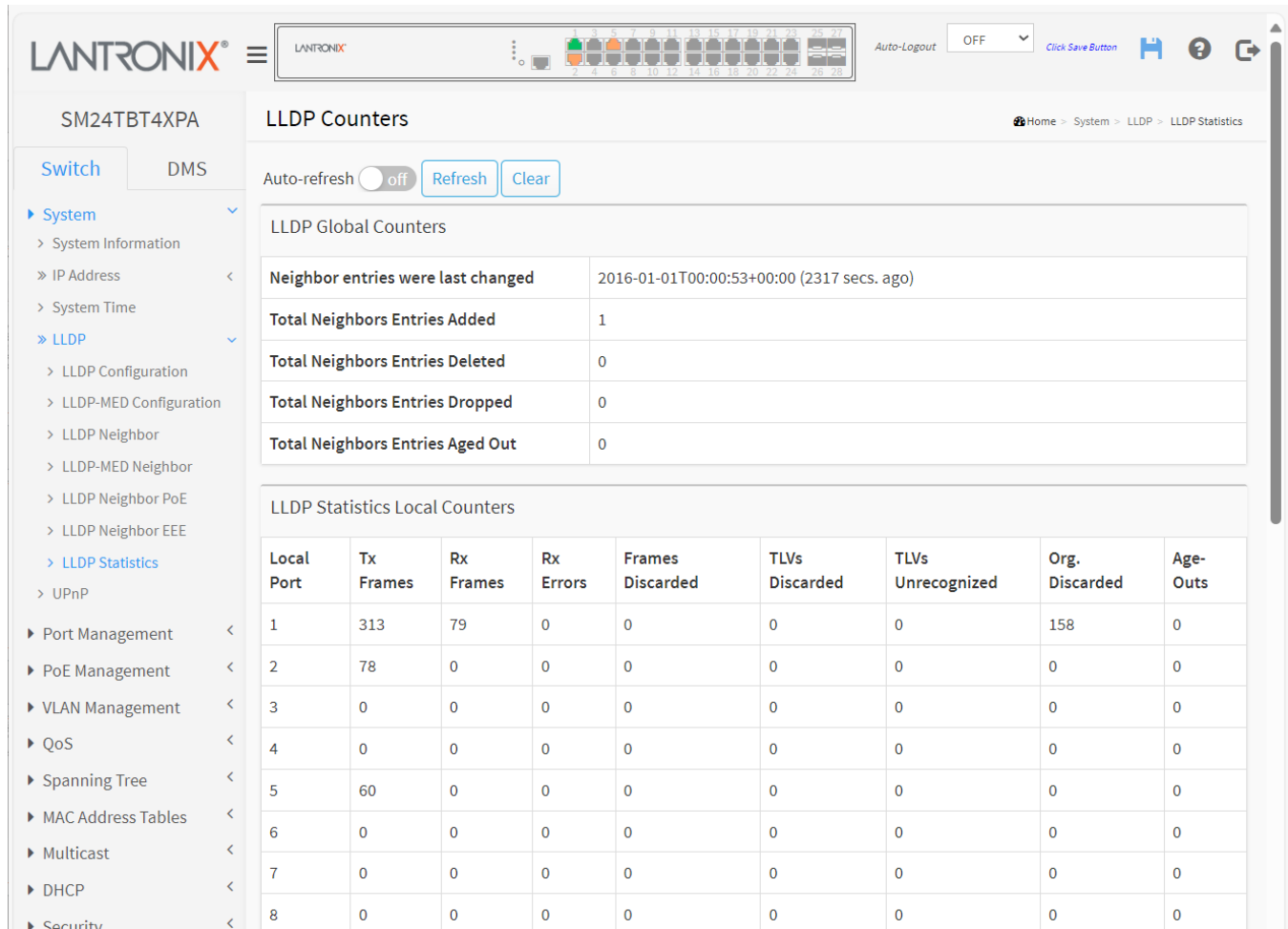


Figure 2-4.7: LLDP Statistics information

Parameter descriptions:

LLDP Global Counters

Neighbor entries were last changed at : It also 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 Neighbor Entries Added : Shows the number of new entries added since switch reboot.

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

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

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

LLDP Statistics Local Counters: The displayed table contains a row for each port. The columns hold the following information:

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

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

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

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

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

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

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

Org. Discarded : 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.

Clear: Clears the counters for the selected port.

2-5 UPnP

UPnP (Universal Plug and Play) goals are to allow devices to connect seamlessly and to simplify the implementation of networks in the home (data sharing, communications, and entertainment) and in corporate environments for simplified installation of computer components.

To configure UPnP in the web UI:

1. Click System and UPnP.
2. Select the mode (on to enable or off to disable).
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 to revert to previously saved values.

Figure 2-5: UPnP Configuration

Parameter descriptions:

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

on: Enable UPnP mode operation. When the mode is enabled, two ACEs are added automatically to trap UPnP related packets to CPU.

off: Disable UPnP mode operation (default). The ACEs are automatically removed when the mode is disabled.

TTL : Time To Live value used by UPnP to send SSDP advertisement messages. Valid values are 1 - 255. The default value is 4.

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

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

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

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

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

3. Port Management

This section lets you configure switch port parameters, enable or disable switch ports, and monitor port status.

3-1 Port Configuration

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

1. Click Port Management and Port Configuration.
2. Specify an alphanumeric string describing the port (e.g., connected hardware, software version, etc.).
3. Specify the Speed, Mode, Flow Control, and Maximum Frame Size parameters.
4. Click Apply.

The screenshot shows the 'Ports Configuration' page in the Lantronix web UI. The sidebar on the left lists various configuration options under 'System' and 'Port Management'. The main content area features a 'Refresh' button and a table with the following columns: Port, Description, Link, Speed, Mode, Flow Control (Rx Status, Tx Status, Mode), and Maximum Frame Size. The table lists ports 1 through 6. Port 1 is up at 1Gfdx. Ports 2 and 5 are up at 100fdx. Ports 3, 4, and 6 are down. The 'Link' column uses colored circles to indicate status: green for up at 1Gbps, orange for up at 10/100 Mbps, and red for down.

| Port | Description | Link | Speed | Mode | Rx Status | Tx Status | Mode | Maximum Frame Size |
|------|-------------|--------|--------|------|-----------|-----------|--------------------------|--------------------|
| * | | | | <> | | | <input type="checkbox"/> | 10240 |
| 1 | | Green | 1Gfdx | Auto | off | off | <input type="checkbox"/> | 10240 |
| 2 | | Orange | 100fdx | Auto | off | off | <input type="checkbox"/> | 10240 |
| 3 | | Red | Down | Auto | off | off | <input type="checkbox"/> | 10240 |
| 4 | | Red | Down | Auto | off | off | <input type="checkbox"/> | 10240 |
| 5 | | Orange | 100fdx | Auto | off | off | <input type="checkbox"/> | 10240 |
| 6 | | Red | Down | Auto | off | off | <input type="checkbox"/> | 10240 |

Figure 3-1: Port Configuration

Parameter descriptions:

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

Description : Enter up to 63 characters to be a descriptive name to identify this port.

Link : The current link state is displayed graphically.

Ports 1-12 and 25-28:

- Amber indicates the link is up at 10 / 100 Mbps.
- Green indicates the link is up at 1 Gbps.
- Blue indicates the link is up at 10 Gbps.
- Red indicates the link is down.

Ports 13-24:

- Amber indicates the link is up at 100 Mbps / 1 Gbps.
- Green indicates the link is up at 2.5 Gbps.
- Blue indicates the link is up at 10 Gbps.
- Red indicates the link is down.

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

Configured Link Speed Mode: 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 automatically negotiates speed with the link partner and selects the highest speed that is compatible with the link partner.

Auto (100M): Port auto negotiating speed with the link partner and selects the 100Mbps speed.

Auto (1G): Port auto negotiating speed with the link partner and selects the 1Gbps speed.

Auto (2.5G): Port auto negotiating speed with the link partner and selects the 2.5Gbps speed.

Auto (2.5G/1G): Port auto negotiating speed with the link partner and selects 2.5Gbps or 1Gbps.

Auto (2.5G/100M): Port auto negotiating speed with the link partner and selects 2.5Gbps or 100Mbps.

Auto (1G/100M): Port auto negotiating speed with the link partner and selects 1Gbps or 100Mbps.

10Mbps FDX: Forces the copper port to 10Mbps full-duplex mode.

100Mbps FDX: Forces the copper port to 100Mbps full-duplex mode.

1Gbps FDX: Forces the port to 1Gbps full duplex.

10Gbps FDX: Forces the Serdes port in 10Gbps full duplex mode.

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

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

Buttons

Refresh: Click to refresh the Port Link Status manually.

Apply: Click to save changes.

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

3-2 Port Statistics

This page provides an overview of general traffic statistics for all switch ports. To display the Port Statistics Overview in the web UI:

1. Click Port Management and Port Statistics.
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”.
4. To see the detail of port statistic click that port.

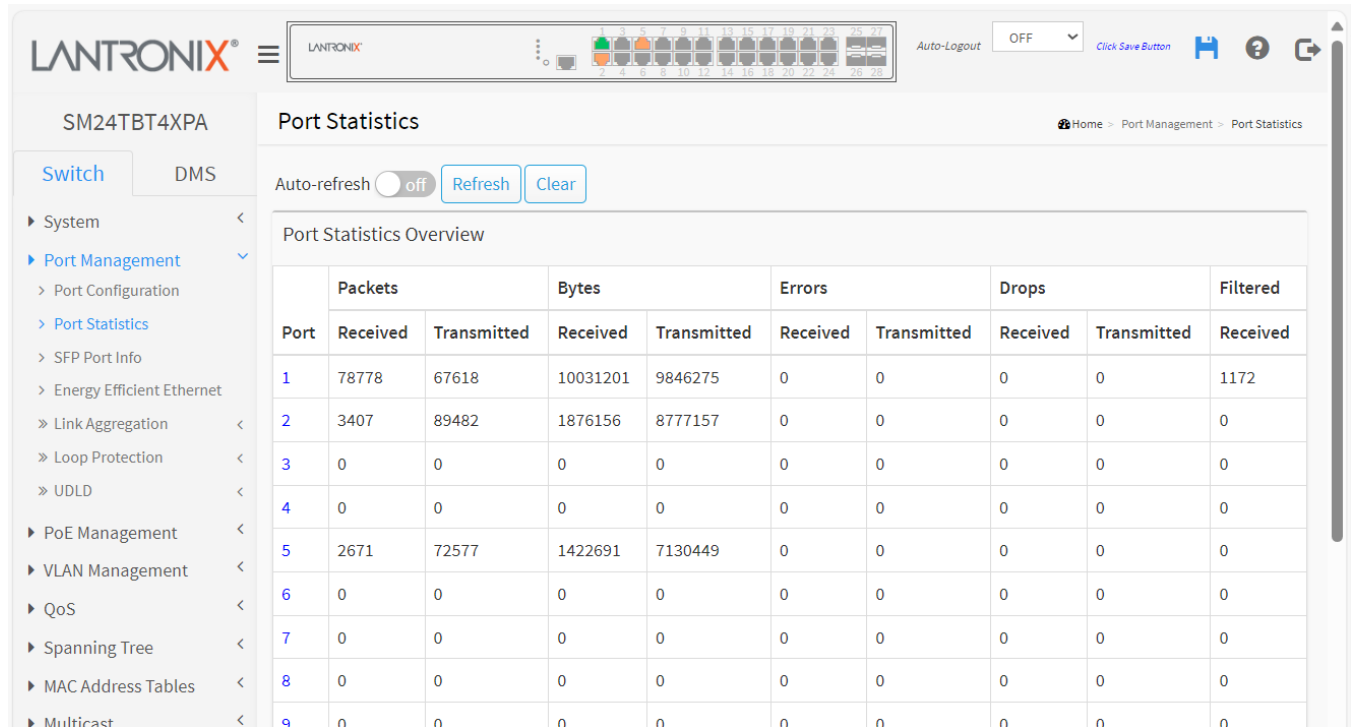


Figure 3-2: Port Statistics Overview

Parameter descriptions:

Port : The logical port for the settings contained in the same row. Click to display the port’s detailed statistics.

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

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

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

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

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

Buttons

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

Refresh: Click to refresh the page.

Clear: Clears the counters for all ports.

To see the details of a port's statistics click that 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.

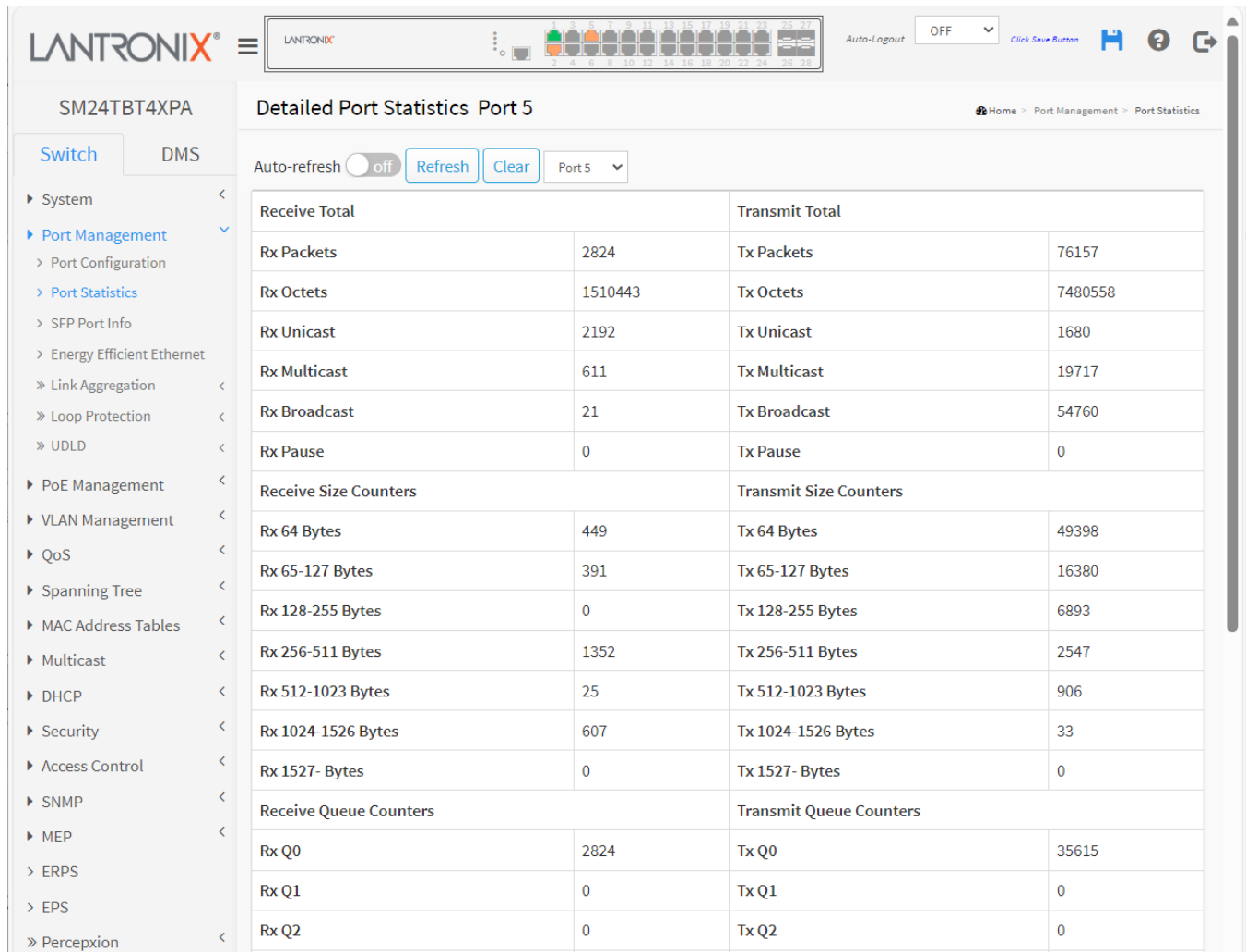


Figure 3-2: Detailed Port Statistics

Parameter descriptions:

Port Select box: Select which port to display the Port statistics with "Port-1", "Port-2", etc.

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 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 short1 frames received with valid CRC.

Rx Oversize : The number of long2 frames received with valid CRC.

Rx Fragments : The number of short1 frames received with invalid CRC.

Rx Jabber : The number of long2 frames received with invalid CRC. .

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.

Tx Oversize: The number of frames dropped due to frame oversize.

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.

3-3 SFP Port Info

This page displays detailed SFP information for SFP modules connected to the switch. The information includes Connector type, Fiber type, wavelength, bit rate, Vendor OUI, etc.

To display SFP information in the web UI:

1. Click Port Management and SFP Port Info.
2. View the SFP Information.

The screenshot shows the Lantronix web interface for the SM24TBT4XPA switch. The left sidebar contains a navigation menu with options like System, Port Management, Port Configuration, Port Statistics, SFP Port Info, Energy Efficient Ethernet, Link Aggregation, Loop Protection, UDLD, PoE Management, VLAN Management, QoS, Spanning Tree, MAC Address Tables, Multicast, DHCP, Security, and Access Control. The main content area is titled 'SFP Information for Port 25'. It features an 'Auto-refresh' toggle set to 'off' and a 'Refresh' button. Below this is a table displaying SFP details for Port 25.

| | |
|-----------------------|----------------------|
| Connector Type | SFP or SFP Plus - LC |
| Fiber Type | Reserved |
| Tx Central Wavelength | 1550 |
| Bit Rate | 10 Gbps |
| Vendor OUI | 00-c0-f2 |
| Vendor Name | Transition |
| Vendor P/N | TN-10GSFP-LR8M |
| Vendor Revision | 1.0 |
| Vendor Serial Number | TWFXPZ000 |
| Data Code | 170508 |
| Temperature | 33.01 C |
| Vcc | 3.29 V |
| Mon1 (Bias) | 83 mA |
| Mon2 (TX PWR) | 1.86 dBm |
| Mon3 (RX PWR) | none |

Figure 3-3: SFP Port Information

Parameter descriptions:

Port Select box: Select which port to display the Port statistics.

Connector Type: Displays the connector type, for instance, UTP, SC, ST, LC and so on.

Fiber Type: Displays the fiber mode, for instance, Multi-Mode, Single-Mode.

Tx Central Wavelength: Displays the fiber optical transmitting central wavelength, for instance, 850nm, 1310nm, 1550nm and so on.

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

Vendor OUI: Displays the Manufacturer's OUI code which is assigned by IEEE.

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

Vendor P/N: Displays the product name of the module manufacturer.

Vendor Rev (Revision): Displays the module revision.

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

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

Temperature: Shows the current temperature of SFP module.

Vcc: Shows the working DC voltage of SFP module.

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

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

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

Buttons

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

Refresh: Click to refresh the page.

3-4 Energy Efficient Ethernet

This page lets you view and configure the current EEE port settings.

EEE (Energy Efficient Ethernet) is defined in IEEE 802.3az. EEE is a power saving option that reduces the power usage when there is very low traffic utilization (or no traffic).

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

To configure Energy Efficient Ethernet in the web UI:

1. Click Port Management and Energy Efficient Ethernet.
2. Select enable or disable Energy Efficient Ethernet for each port.
3. Click the Apply button to save the settings.
4. To cancel the settings, click the Reset button to revert to previously saved values.

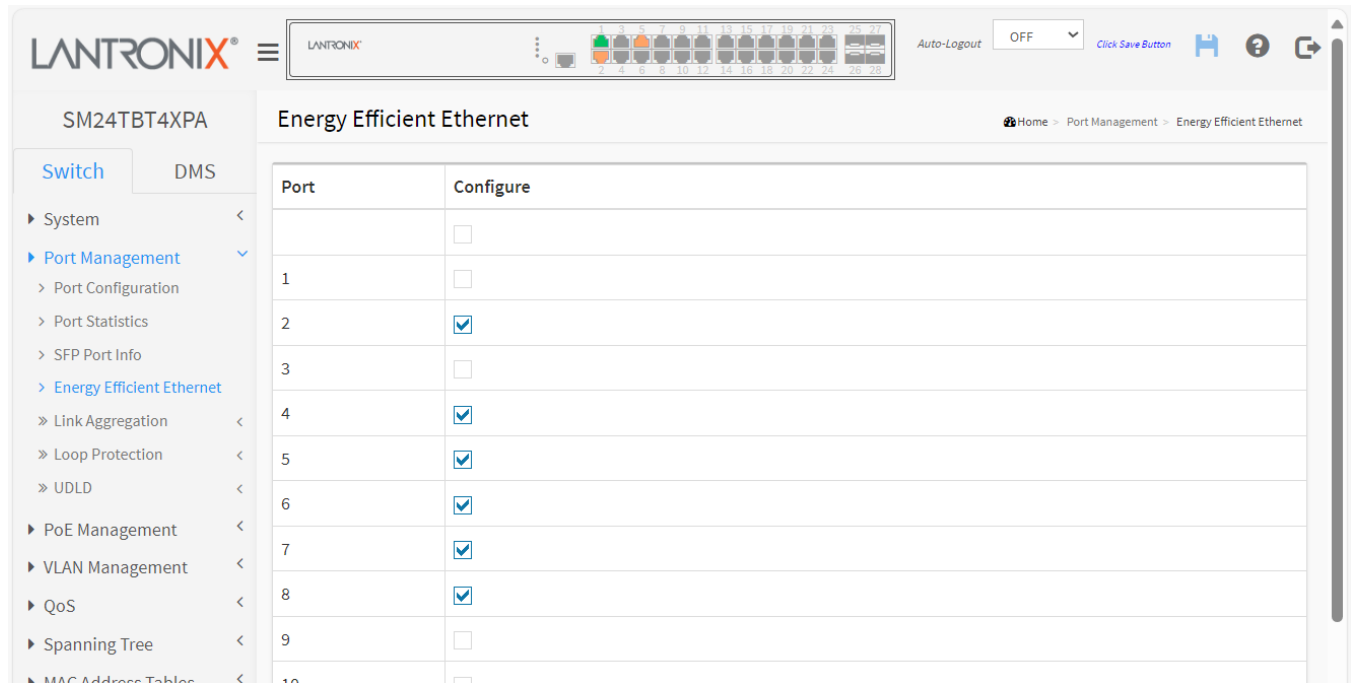


Figure 4-4: Energy Efficient Ethernet Configuration

Parameter descriptions:

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

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

Buttons

Apply: Click to save changes.

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

3-5 Link Aggregation

3-5.1 Static Configuration

This page is used to configure the Aggregation hash mode and the aggregation group. To configure the Aggregation hash mode and aggregation group in the web UI:

1. Click Port Management, Link Aggregation and Static Configuration.
2. Enable or disable the aggregation mode function.
3. Enable Aggregation Group ID and Port members.
4. Click Apply to save the settings.
5. To cancel the settings, click the Reset button to revert to previously saved values.

LANTRONIX® SM24TBT4XPA

Aggregation Static Configuration

Home > Port Management > Link Aggregation > Static Configuration

Switch DMS

System <

Port Management >

Port Configuration

Port Statistics

SFP Port Info

Energy Efficient Ethernet

Link Aggregation >

Static Configuration

Aggregation Status

LACP Configuration

System Status

Internal Status

Neighbor Status

Port Status

Loop Protection <

UDLD <

PoE Management <

VLAN Management <

QoS <

Spanning Tree <

MAC Address Tables <

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 | 27 | 28 |
|----------|----------------------------------|----------------------------------|----------------------------------|----------------------------------|----------------------------------|----------------------------------|----------------------------------|----------------------------------|----------------------------------|----------------------------------|----------------------------------|----------------------------------|----------------------------------|----------------------------------|----------------------------------|----------------------------------|----------------------------------|----------------------------------|----------------------------------|----------------------------------|----------------------------------|----------------------------------|----------------------------------|----------------------------------|----------------------------------|----------------------------------|----------------------------------|----|
| Normal | <input checked="" type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input checked="" type="radio"/> | <input checked="" type="radio"/> | <input checked="" type="radio"/> | <input checked="" type="radio"/> | <input checked="" type="radio"/> | <input checked="" type="radio"/> | <input checked="" type="radio"/> | <input checked="" type="radio"/> | <input checked="" type="radio"/> | <input checked="" type="radio"/> | <input checked="" type="radio"/> | <input checked="" type="radio"/> | <input checked="" type="radio"/> | <input checked="" type="radio"/> | <input checked="" type="radio"/> | <input checked="" type="radio"/> | <input checked="" type="radio"/> | <input checked="" type="radio"/> | <input checked="" type="radio"/> | <input checked="" type="radio"/> | |
| 1 | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | |
| 2 | <input type="radio"/> | <input checked="" type="radio"/> | <input checked="" type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | |
| 3 | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input checked="" type="radio"/> | <input checked="" type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | |
| 4 | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input checked="" type="radio"/> | <input checked="" type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | |
| 5 | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | |
| 6 | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | |
| 7 | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | |

Figure 3-5.1: Aggregation Static Configuration

Parameter descriptions:

Hash Code Contributors

Source MAC Address : The Source MAC address can be used to calculate the destination port for the frame. Check to enable the use of the Source MAC address or uncheck to disable. By default, Source MAC Address is enabled.

Destination MAC Address : The Destination MAC Address can be used to calculate the destination port for the frame. Check to enable the use of the Destination MAC Address or uncheck to disable. By default, Destination MAC Address is disabled.

IP Address : The IP address can be used to calculate the destination port for the frame. Check to enable the use of the IP Address or uncheck to disable. By default, IP Address is enabled.

TCP/UDP Port Number : The TCP/UDP port number can be used to calculate the destination port for the frame. Check to enable the use of the TCP/UDP Port Number or uncheck to disable. By default, TCP/UDP Port Number is enabled.

Aggregation Group Configuration

Group ID : Indicates the group ID for the settings contained in the same row. Group ID "Normal" indicates there is no aggregation. Only one group ID is valid per port.

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

Buttons

Apply : Click to save changes.

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

3-5.2 Aggregation Status

This page lets you view status of ports in Aggregation group(s).

1. Click Port Management, Link Aggregation and Aggregation Status.
2. View the settings.
3. Click the Auto-refresh or Refresh buttons as needed..

The screenshot shows the Lantronix SM24TBT4XPA web interface. The top header includes the Lantronix logo, a device status bar with 24 ports, and an 'Auto-Logout' dropdown set to 'OFF'. The sidebar on the left shows the navigation menu with 'Link Aggregation' selected. The main content area is titled 'Aggregation Status' and features an 'Auto-refresh' checkbox and a refresh button. Below this is a table with the following data:

| Aggr ID | Name | Type | Speed | Configured Ports | Aggregated Ports | Aggregated Bandwidth |
|---------|-------|--------|-----------|-----------------------|---------------------|----------------------|
| 2 | LLAG2 | STATIC | 100M | GigabitEthernet 1/2-3 | GigabitEthernet 1/2 | none |
| 3 | LLAG3 | STATIC | 100M | GigabitEthernet 1/4-5 | GigabitEthernet 1/5 | none |
| 4 | LLAG4 | STATIC | Undefined | GigabitEthernet 1/6-7 | none | none |

Figure 3-5.3: Aggregation Status

Parameter descriptions:

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

Name: The name of the Aggregation group ID.

Type: The type of the Aggregation group(Static or LACP).

Speed: The speed of the Aggregation group.

Configured Ports: The configured member ports of the Aggregation group.

Aggregated Ports: The aggregated member ports of the Aggregation group.

Aggregated Bandwidth: The aggregated Bandwidth of the Aggregation group.

Buttons

Auto-refresh: Automatic refresh occurs every 3 seconds.

Refresh: Click to manually refresh the page immediately.

3-5.3 LACP Port Configuration

This page lets you view and configure current LACP port parameters. To configure LACP port parameters:

1. Click Port Management, Link Aggregation and LACP Configuration.
2. Enable or disable the LACP on the port of the switch.
3. Select the Key parameter (Auto or Specific). The default is Auto.
4. Select the Role (Active or Passive). The default is Active.
5. Click Apply to save the settings.
6. To cancel the settings click the reset button to revert to previously saved values.

The screenshot shows the Lantronix web interface for the SM24TBT4XPA switch. The 'LACP Port Configuration' page is active, displaying a table for configuring LACP on various ports. The table has the following structure:

| Port | LACP Enabled | Key | Role | Timeout | Prio |
|------|--------------------------|----------------------|---|---------------------------------------|------------------------------------|
| * | <input type="checkbox"/> | <input type="text"/> | <input type="button" value="v"/> | <input type="button" value="v"/> | <input type="text" value="32768"/> |
| 1 | <input type="checkbox"/> | <input type="text"/> | Active <input type="button" value="v"/> | Fast <input type="button" value="v"/> | <input type="text" value="32768"/> |
| 2 | <input type="checkbox"/> | <input type="text"/> | Active <input type="button" value="v"/> | Fast <input type="button" value="v"/> | <input type="text" value="32768"/> |
| 3 | <input type="checkbox"/> | <input type="text"/> | Active <input type="button" value="v"/> | Fast <input type="button" value="v"/> | <input type="text" value="32768"/> |
| 4 | <input type="checkbox"/> | <input type="text"/> | Active <input type="button" value="v"/> | Fast <input type="button" value="v"/> | <input type="text" value="32768"/> |
| 5 | <input type="checkbox"/> | <input type="text"/> | Active <input type="button" value="v"/> | Fast <input type="button" value="v"/> | <input type="text" value="32768"/> |
| 6 | <input type="checkbox"/> | <input type="text"/> | Active <input type="button" value="v"/> | Fast <input type="button" value="v"/> | <input type="text" value="32768"/> |

Figure 3-5.2: LACP Configuration

Parameter descriptions:

Port : The switch port number.

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

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

Role : The Role shows the LACP activity status. The **Active** role 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 : Controls the priority of the port. If the LACP partner wants to form a larger group than is supported by this device then this parameter will control which ports will be active and which ports will be in a backup role. Lower number means greater priority.

Buttons

Apply : Click to save changes.

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

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

3-5.4 System Status

This page provides a status overview of all LACP instances. To display LACP System status in the web UI:

1. Click Port Management, Link Aggregation and System Status.
2. Check "Auto-refresh".

3. Click “Refresh” to refresh the port detailed statistics.

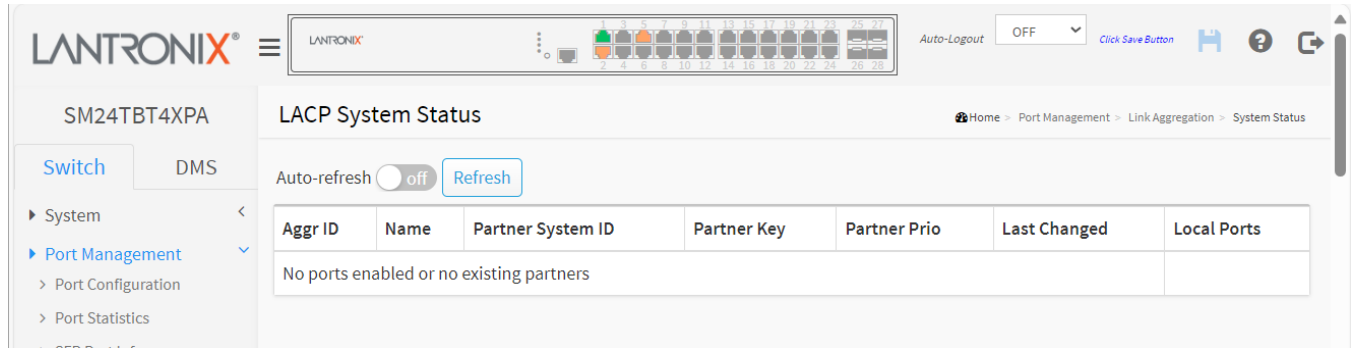


Figure 3-5.3: LACP System Status

Aggr ID : The Aggregation ID associated with this aggregation instance. For LLAG the ID is shown as 'isid: aggr-id' and for GLAGs as 'aggr-id'

Name: Name of the Aggregation group ID.

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

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

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

Last changed : The time since this aggregation changed.

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

Buttons

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

Refresh: Click to refresh the page.

3-5.5 Internal Status

This page provides a status overview for the LACP internal (i.e. local system) status for all ports. Only ports that are part of an LACP group are shown. For details on the shown parameters please refer to IEEE 801.AX-2014.

To display the LACP Internal System status in the web UI:

1. Click Port Management, Link Aggregation and Internal Status.
2. Check "Auto-refresh".
3. Click "Refresh" to refresh the page statistics.

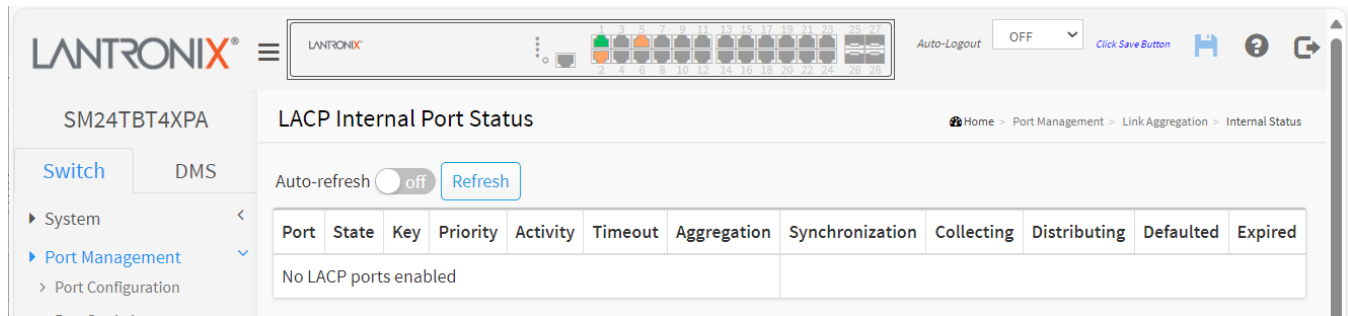


Figure 3-5.4: LACP Internal Port Status

Parameter descriptions:

Port: The switch port number.

State: The current port state:

Down: The port is not active.

Active: The port is in active state.

Standby: The port is in standby state.

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

Priority : The priority assigned to this aggregation group.

Activity: The LACP mode of the group (Active or Passive).

Timeout: The timeout mode configured for the port (Fast or Slow).

Aggregation: Show whether the system considers this link to be "aggregateable"; i.e., a potential candidate for aggregation.

Synchronization: Show whether the system considers this link to be "IN_SYNC"; i.e., it has been allocated to the correct LAG, the group has been associated with a compatible Aggregator, and the identity of the LAG is consistent with the System ID and operational Key information transmitted.

Collecting: Show if collection of incoming frames on this link is enabled.

Distributing: Show if distribution of outgoing frames on this link is enabled.

Defaulted: Show if the Actor's Receive machine is using Defaulted operational Partner information.

Expired: Show if that the Actor's Receive machine is in the EXPIRED state.

Buttons

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

Refresh: Click to refresh the page.

3-5.6 Neighbor Status

This page provides an overview of LACP neighbor status for all ports. Only ports that are part of an LACP group are shown. For details on the shown parameters please refer to IEEE 801.AX-2014. To display LACP Neighbor Port status in the web UI:

1. Click Port Management, Link Aggregation and Neighbor Status.

2. Checked "Auto-refresh".
3. Click "Refresh" to refresh the port status.

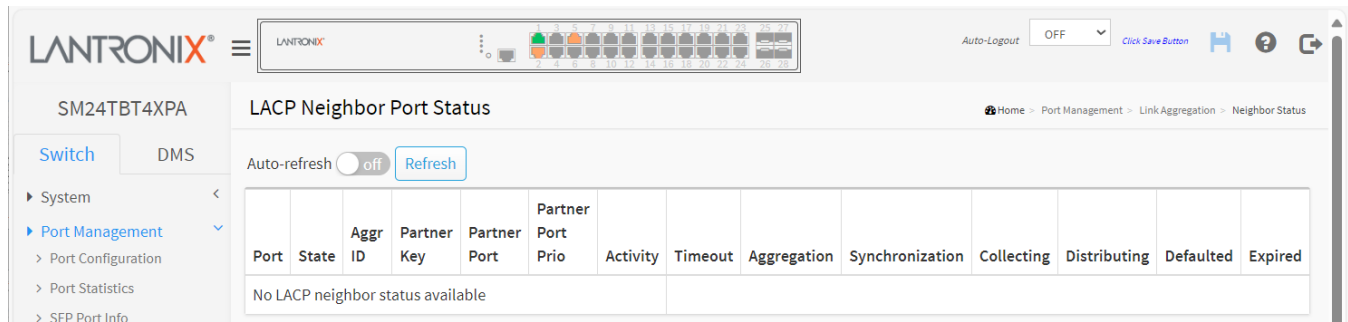


Figure 3-5.5: LACP Neighbor Port Status

Parameter descriptions:

Aggr ID: The aggregation group ID which the port is assigned to.

Port: The switch port number.

State: The current port state:

Down: The port is not active.

Active: The port is in active state.

Standby: The port is in standby state.

Partner Key: The key assigned to this port by the partner.

Partner Port: The partner port number associated with this link.

Partner Port Priority: The priority assigned to this partner port.

Activity: The LACP mode of the group (Active or Passive).

Timeout: The timeout mode configured for the port (Fast or Slow).

Aggregation: Shows if the system considers this link to be "aggregateable " (i.e., a potential candidate for aggregation).

Synchronization: Shows whether the system considers this link to be "IN_SYNC"; i.e., it has been allocated to the correct LAG, the group has been associated with a compatible Aggregator, and the identity of the LAG is consistent with the System ID and operational Key information transmitted.

Collecting: Shows if collection of incoming frames on this link is enabled.

Distributing: Shows if distribution of outgoing frames on this link is enabled.

Defaulted: Shows if the Actor's Receive machine is using Defaulted operational Partner information.

Expired: Shows if that the Actor's Receive machine is in the EXPIRED state.

Buttons

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

Refresh: Click to refresh the page.

3-5.7 Port Status

This page provides a Port Status overview for all LACP instances. To display LACP Port status in the web UI:

1. Click Port Management, Link Aggregation and Port Status.
2. If you want to auto-refresh the information then you need to evoke the "Auto-refresh".
3. Click "Refresh" to refresh the LACP Port Status.

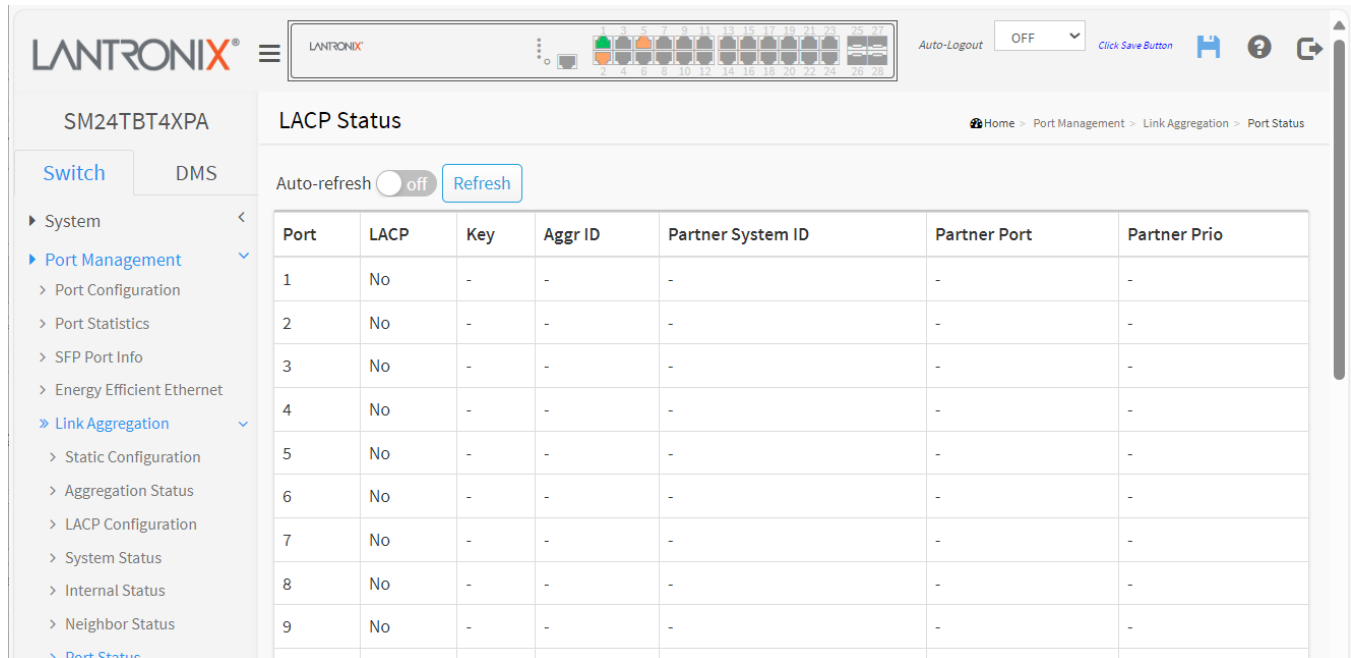


Figure 3-5.6: LACP Status

Parameter descriptions:

Port : The switch port number.

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

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

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

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

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

Partner Prio: The partner's port priority.

Buttons

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

Refresh : Click to refresh the page.

3-6 Loop Protection

3-6.1 Configuration

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

To configure Loop Protection parameters in the web UI:

1. Click Port Management, Loop Protection and Configuration.
2. Select enable or disable for port Loop Protection.
3. Click the Apply button to save the settings.
4. To cancel the settings click the Reset button to revert to previously saved values.

SM24TBT4XPA Loop Protection Configuration

Global Configuration

| | |
|------------------------|-------------------------------------|
| Enable Loop Protection | <input checked="" type="checkbox"/> |
| Transmission Time | 5 seconds |
| Shutdown Time | 180 seconds |

Port Configuration

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

Figure 3-6.1: Loop Protection Configuration

Parameter descriptions:**Global Configuration**

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

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

Shutdown Time: The period (in seconds) for which a port will be kept disabled in the event of a loop is detected (and the port action shuts down the port). Valid values are 10 to 604800 seconds (7-10 days).

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.

3-6.2 Status

This page displays the loop protection status of the switch ports. To display Loop Protection status in the web UI:

1. Click Port Management, Loop Protection, and Status.
2. To auto-refresh the information check the “Auto refresh” checkbox.
3. Click “Refresh” to refresh the page.

The screenshot shows the Lantronix SM24TBT4XPA web UI. The top header includes the Lantronix logo, a status bar with port indicators, and an Auto-Logout dropdown set to OFF. The left navigation menu is expanded to show 'Port Management' > 'Loop Protection' > 'Status'. The main content area is titled 'Loop Protection Status' and includes an 'Auto-refresh' toggle (currently off) and a 'Refresh' button. Below this is a table with the following data:

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

Figure 3-6.2: Loop Protection Status

Parameter descriptions:

Port: The switch port number of the logical port.

Action: The currently configured port action.

Transmit: The currently configured port transmit mode.

Loops: The number of loops detected on this port.

Status: The current loop protection status of the port.

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

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

Buttons

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

Refresh : Click to refresh the page.

3-7 UDLD

Unidirectional Link Detection (UDLD) is a data link layer protocol used to monitor the physical configuration of cables and detect unidirectional links. UDLD complements the Spanning Tree Protocol to eliminate switch loops.

3-7.1 UDLD Configuration

This page lets you set and view current UDLD parameters. To set UDLD parameters in the web UI:

1. Click Port Management, UDLD and UDLD Configuration.
2. Enable or disable the port UDLD.
3. Specify the Message Interval.
4. Click the Apply button to save the settings.
5. To cancel the settings click the Reset button to revert to previously saved values.

| Port | UDLD mode | Message Interval |
|------|------------|------------------|
| * | | 7 |
| 1 | Normal | 7 |
| 2 | Aggressive | 40 |
| 3 | Disable | 7 |
| 4 | Aggressive | 85 |
| 5 | Normal | 7 |
| 6 | Normal | 7 |

Figure 3-7.1: UDLD Configuration

Port: Port number of the switch.

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

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

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

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

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

Buttons

Apply : Click to save changes.

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

3-7.2 UDLD Status

This page displays the UDLD status of the ports. To display UDLD status in the web UI:

1. Click Port Management, UDLD, and UDLD Status.

2. Select port that you want to display the UDLD Status.
3. To auto-refresh the information check the “Auto refresh” checkbox.
4. Click “Refresh” to refresh the webpage.

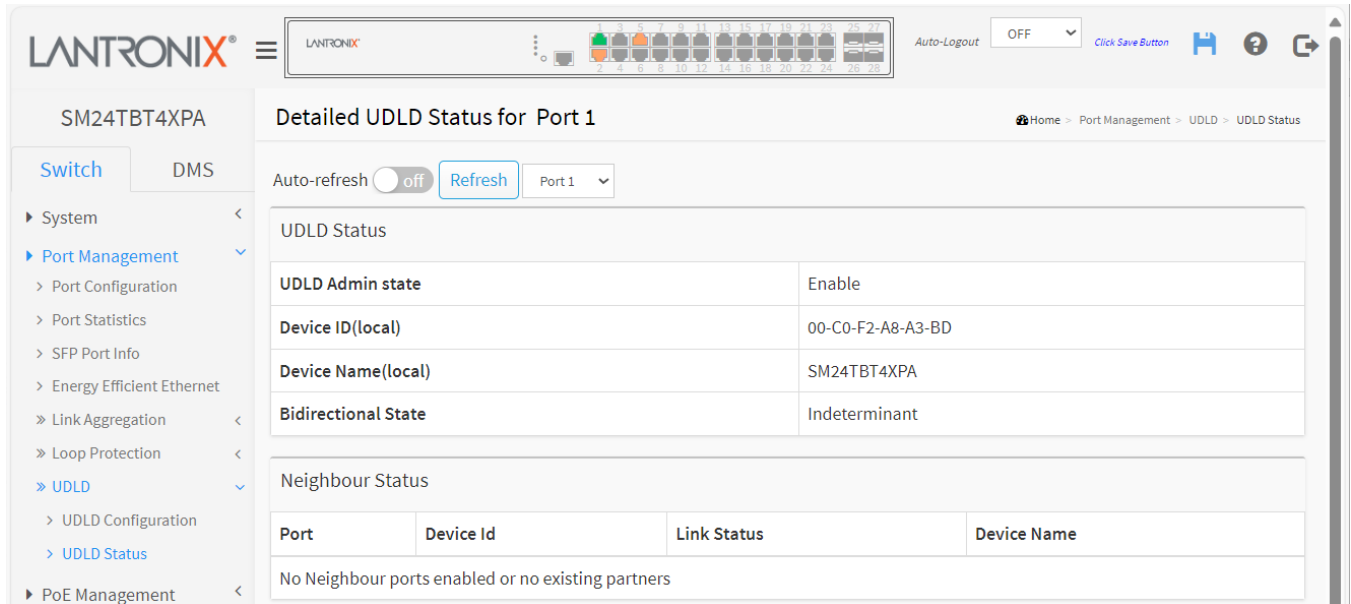


Figure 3-7.2: UDLD Status

Parameter descriptions:

UDLD Status

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

Device ID(local): The ID of Device.

Device Name(local): Name of the Device.

Bidirectional State: The current state of the port.

Neighbour Status

Port: The current port of neighbour device.

Device ID: The current ID of neighbour device.

Link Status: The current link status of neighbour port.

Device Name: Name of the Neighbour Device.

Buttons

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

Refresh: Click to refresh the page immediately.

4. PoE Management

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

4-1 PoE Configuration

This page lets you view and configure current PoE port parameters and shows PoE power information. Note that copper ports 1-12 are 10M/100M/1G PoE+ ports and ports 13-24 are 100M/1G/2.5G PoE++ ports. Ports 25-28 are 1G/10G SFP+ (fiber) ports.

To configure PoE in the web UI:

1. Click PoE Management and PoE Configuration.
2. Specify the Reserved Power determined by.
3. Specify the PoE Mode, PoE Schedule, Priority, LLDP, Legacy, Delay Mode and Delay Time.
4. Click Apply to save the configuration.
5. To cancel the settings click the Reset button to revert to previously saved values.

| Port | PoE Mode | PoE Schedule | Priority | LLDP | Legacy | Delay Mode | Delay Time(0~300 sec) |
|------|----------|--------------|----------|---------|----------|------------|-----------------------|
| * | <> | <> | <> | <> | <> | <> | 0 |
| 1 | Enabled | Disabled | Low | Enabled | Disabled | Disabled | 0 |
| 2 | Enabled | Disabled | Low | Enabled | Disabled | Disabled | 0 |
| 3 | Enabled | Disabled | Low | Enabled | Disabled | Disabled | 0 |
| 19 | 4pair60w | Disabled | Critical | Enabled | Disabled | Disabled | 0 |
| 20 | 4pair60w | Disabled | Critical | Enabled | Disabled | Disabled | 0 |
| 21 | 8023bt | Disabled | Critical | Enabled | Disabled | Disabled | 0 |
| 22 | 4pair60w | Disabled | Critical | Enabled | Disabled | Disabled | 0 |
| 23 | 4pair60w | Disabled | Critical | Enabled | Disabled | Disabled | 0 |
| 24 | 4pair60w | Disabled | Critical | Enabled | Disabled | Disabled | 0 |

Apply Reset

Figure 4-1: PoE Configuration

PoE Power Supply Configuration

PoE Firmware Version: The version of PoE MCU firmware

Primary Power Supply [W] : For being able to determine the amount of power the PD may use; it must be defined what amount of power a power source can deliver.

PoE Port Configuration

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

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

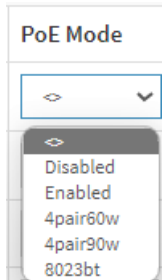
Disabled: PoE disabled for the port.

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

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)



PoE Schedule : Disable or select a PoE Schedule profile.

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

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

Legacy: Enabled means support capacitor detection to detect legacy PoE PD devices.

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

Enabled: Enable POE Power Delay.

Disabled: Disable POE Power Delay.

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

Buttons

Apply: Click to save changes.

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

4-2 PoE Status

This page displays the current status for all PoE ports. To display PoE Status in the web UI:

1. Click PoE Management and PoE Status.
2. Set "Auto-refresh" to on or off.
3. Click "Refresh" to refresh the webpage.

| Local Port | PD class | Power Requested | Power Allocated | Power Used | Current Used | Priority | Port Status |
|------------|----------|-----------------|-----------------|------------|--------------|----------|----------------|
| 1 | - | 0 [W] | 0 [W] | 0 [W] | 0 [mA] | Critical | No PD detected |
| 2 | 2 | 15 [W] | 15 [W] | 1.9 [W] | 37 [mA] | High | PoE turned ON |
| 3 | - | 0 [W] | 0 [W] | 0 [W] | 0 [mA] | High | No PD detected |
| 4 | 2 | 15 [W] | 15 [W] | 1.2 [W] | 23 [mA] | Low | PoE turned ON |
| 5 | 2 | 15 [W] | 15 [W] | 1.9 [W] | 37 [mA] | Low | PoE turned ON |
| 6 | 2 | 15 [W] | 15 [W] | 1.1 [W] | 22 [mA] | Low | PoE turned ON |
| 7 | 4 | 22 [W] | 22 [W] | 5.9 [W] | 112 [mA] | Low | PoE turned ON |
| 8 | - | 0 [W] | 0 [W] | 0 [W] | 0 [mA] | Low | No PD detected |
| 21 | - | 0 [W] | 0 [W] | 0 [W] | 0 [mA] | Low | No PD detected |
| 22 | - | 0 [W] | 0 [W] | 0 [W] | 0 [mA] | Low | No PD detected |
| 23 | - | 0 [W] | 0 [W] | 0 [W] | 0 [mA] | Low | No PD detected |
| 24 | - | 0 [W] | 0 [W] | 0 [W] | 0 [mA] | Low | No PD detected |
| Total | | 82 [W] | 82 [W] | 12 [W] | 231 [mA] | | |

Figure 4-2: PoE Status

Parameter descriptions:

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

PD Class: Each PD is classified according to a class that defines the maximum power the PD will use. Five PD Classes are defined:

- Class 0: Max. power 15.4 W
- Class 1: Max. power 4.0 W
- Class 2: Max. power 7.0 W
- Class 3: Max. power 15.4 W
- Class 4: Max. power 30.0 W

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

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

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

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

Priority: Shows the port's priority configured by the user (Low, High, or Critical).

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

PoE not available - No PoE chip found: PoE not supported for the port.

PoE turned OFF - PoE disabled: PoE is disabled by user.

PoE turned OFF - Power budget exceeded: The total requested or used power by the PDs exceeds the maximum power the Power Supply can deliver, and port(s) with the lowest priority is/are powered down.

No PD detected: No PD was detected for the port.

PoE turned OFF - PD overload: The PD has requested or used more power than the port can deliver, and is powered down.

PoE turned OFF: PD is off.

Invalid PD: PD detected, but is not working correctly.

The last row of the table displays totals for the Power Requested, Power Allocated, Power Used, and Current Used columns

Buttons

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

Refresh: Click to refresh the page immediately.

4-3 PoE Power Delay

This page lets you set the delay time of power provided after the device is rebooted. To set PoE Power Delay in the web UI:

1. Click PoE Management and PoE Power delay.
2. Enable the desired port to power.
3. Specify the power delay time on reboot.
4. Click Apply to apply the changes.

| Port | Delay Mode | Delay Time(0~300 sec) |
|------|-------------------------------|-----------------------|
| * | <input type="radio"/> Enabled | 0 |
| 1 | Disabled | 0 |
| 2 | Disabled | 0 |
| 3 | Disabled | 0 |
| 4 | Disabled | 0 |
| 5 | Disabled | 0 |
| 6 | Disabled | 0 |

Figure 4-3: PoE Power Delay

Parameter descriptions:

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

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

Enabled: Enable POE Power Delay.

Disabled: Disable POE Power Delay.

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

Buttons

Apply: Click to save changes.

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

4-4 PoE Auto Power Reset

This page lets you set the auto detection parameters to check the link status between PoE ports and PDs. When it detects a failed connection it will reboot remote the PD automatically. To configure PoE Auto Power Reset in the web UI:

1. Click PoE Management and PoE Auto Power Reset.
2. Set the Ping Check function to on.
3. Specify the PD's IP address, checking startup time, interval time, retry time, failure action and reboot time.
4. Click Apply to apply the changes.

| 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 | Reboot Remote PD | 15 | 2 |
| 3 | 0.0.0.0 | 60 | 30 | 4 | error=0, total=0 | Reboot Remote PD | 10 | 4 |
| 4 | 0.0.0.0 | 60 | 30 | 1 | error=0, total=0 | Reboot Remote PD | 20 | 3 |
| 5 | 0.0.0.0 | 60 | 30 | 3 | error=0, total=0 | Reboot Remote PD | 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 |

Figure 4-4: PoE Auto Power Reset

Parameter descriptions:

Ping Check : Enable (on) Ping Check function can detects the connection between PoE port and power device. Disable (off) will turn off ping 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 : After startup time, device will enable auto checking. The default is 30 seconds; the valid range is 30-60 seconds.

Interval Time(sec) : Device will send checking message to PD each interval time. The default is 30 seconds; the valid range is 10-120 seconds.

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

Failure Log : Failure loggings counter.

Failure Action : The action to take when the third fail is detected.

Nothing: Keep Ping the remote PD but does nothing further.

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

Reboot time(sec) : When the PD is rebooted, the PoE port restores power after the specified time. The default is 15 seconds; the valid range is 3-120 seconds.

Max. Reboot Times: When Failure Action is Reboot Remote PD, this parameter setting limits the number of reboot times. The default is 3 reboots; the valid range is 0-10 reboots. Setting to 0 means unlimited reboots.

Buttons

Apply: Click to save changes.

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

4-5 PoE Scheduling Profile

This page lets you define profiles for PoE scheduling. To configure a PoE Schedule Profile in the web UI:

1. Click PoE Management and PoE Scheduling Profile.
2. Select a profile number and specify the profile name.
3. Select Week Day and specify Start Time and End Time.
4. Click Apply to apply the changes.

LANTRONIX SM24TBT4XPA PoE Schedule Profile

Auto-Logout: OFF [Click Save Button](#)

Home > PoE Management > PoE Scheduling Profile

Profile: 1

Name: Profile 1

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

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

Figure 4-5: PoE Schedule Profile

Parameter descriptions:

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

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

Week Day: The day to schedule PoE.

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

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

4-6 PoE Chip Reset Schedule

This page lets you schedule when to reset the PoE chip. To schedule PoE chip resets in the web UI:

1. Navigate to Configuration > PoE > Chip Reset Schedule
2. At the Mode dropdown select Enabled to display the configurable parameters.
3. Set the Mode and the reset day and time
4. Click the Apply button when done.

The screenshot shows the Lantronix web interface for the SM24TBT4XPA device. The left sidebar contains a navigation menu with options like System, Port Management, PoE Management, VLAN Management, QoS, Spanning Tree, MAC Address Tables, Multicast, DHCP, Security, and Access Control. The main content area is titled 'PoE Chip Reset Schedule'. At the top, there is a 'Mode' dropdown menu set to 'Enabled'. Below this is a table for configuring the reset schedule. The table has three columns: 'Week Day', 'HH' (Hours), and 'MM' (Minutes). The rows represent the days of the week: *, Monday, Tuesday, Wednesday, Thursday, Friday, Saturday, and Sunday. Each row has dropdown menus for HH and MM. At the bottom of the table are 'Apply' and 'Reset' buttons.

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

Figure 4-6: PoE Chip Reset Schedule

Parameter descriptions:

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

Enabled: Enable PoE chip reset.

Disabled: Disable PoE chip reset (default).

Week Day: The day to reset PoE chip.

PoE Chip Reset Time: The time to reset PoE chip in hours (HH = 0-23) and minutes (MM = 0-55).

Buttons

Apply: Click to save changes.

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

5. VLAN Management

5-1 VLAN Configuration

To assign a specific VLAN for management purpose. The management VLAN is used to establish an IP connection to the switch from a workstation connected to a port in the VLAN. This connection supports a VSM, SNMP, and Telnet session. By default, the active management VLAN is VLAN 1, but you can designate any VLAN as the management VLAN using the Management VLAN window. Only one management VLAN can be active at a time.

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

To configure VLAN parameters in the web UI:

1. Click VLAN Management and VLAN Configuration.
2. Modify Global VLAN Configuration parameters.
3. Select the Mode, Port VLAN, and Port Type to enable the Port VLAN Configuration parameters.
4. Click the Apply button to save the settings.
5. To cancel the settings click the Reset button. It will revert to previously saved values.

| 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 | 2 | C-Port | <input checked="" type="checkbox"/> | Tagged and Untagged | Untag Port VLAN | 2 | |
| 4 | Trunk | 2 | C-Port | <input checked="" type="checkbox"/> | Tagged and Untagged | Untag Port VLAN | 1-4094 | 4095 |
| 5 | Hybrid | 3 | C-Port | <input checked="" type="checkbox"/> | Untagged Only | Tag All | 1,2,10-13,15 | |
| 6 | Hybrid | 3 | S-Port | <input checked="" type="checkbox"/> | Tagged Only | Untag Port VLAN | 1,2,10-13,15 | |
| 7 | Hybrid | 3 | Unaware | <input checked="" type="checkbox"/> | Tagged and Untagged | Untag Port VLAN | 1-4095 | |
| 8 | Access | 3 | C-Port | <input checked="" type="checkbox"/> | Tagged and Untagged | Untag Port VLAN | 3 | |

Figure 5-1: VLAN Configuration

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 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 adds additional port configuration features. In addition to the characteristics described for trunk ports, hybrid ports have these abilities:

- Can be configured to be VLAN tag unaware, C-tag aware, S-tag aware, or S-custom-tag aware,
- ingress filtering can be controlled,
- ingress acceptance of frames and configuration of egress tagging can be configured independently.

Port VLAN: Determines the port's VLAN ID (a.k.a. PVID). Allowed VLANs are in the range 1 - 4095, default being 1. On ingress, frames get classified to the Port VLAN if the port is configured as VLAN unaware, the frame is untagged, or VLAN awareness is enabled on the port, but the frame is priority tagged (VLAN ID = 0). On egress, frames classified to the Port VLAN do not get tagged if Egress Tagging configuration is set to untag Port VLAN. The Port VLAN is called an "Access VLAN" for ports in Access mode and Native VLAN for ports in Trunk or Hybrid mode.

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

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

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

S-Port: On ingress, frames with a VLAN tag with TPID = 0x8100 or 0x88A8 get classified to the VLAN ID

embedded in the tag. If a frame is untagged or priority tagged, the frame gets classified to the Port VLAN. If frames must be tagged on egress, they will be tagged with an S-tag.

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

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

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 Enabled VLANs field. By default, the field is left blank, which means that the port may become a member of all possible VLANs.

Buttons

Apply: Click to save changes.

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

5-2 VLAN Membership

This page provides an overview of membership status of VLAN users. To configure VLAN membership configuration in the web UI:

1. Click VLAN Management and VLAN Membership.
2. At the user select dropdown select the user to be displayed
3. Click Refresh to update the webpage.

The screenshot shows the 'VLAN Membership Status for Combined users' page. It features a sidebar with a tree view of configuration options. The main content area has a table titled 'Port Members' with 'VLAN ID' as the first column and ports 1 through 28 as subsequent columns. The table shows membership status for VLANs 1 through 11. For example, VLAN 1 is a member of ports 1 through 28. VLAN 2 is a member of ports 3 through 7. VLAN 3 is a member of ports 4 and 7. VLAN 4 is a member of ports 5 and 7. VLAN 5 is a member of ports 6 and 7. VLAN 6 is a member of ports 7 and 8. VLAN 7 is a member of ports 8 and 9. VLAN 8 is a member of ports 9 and 10. VLAN 9 is a member of ports 10 and 11. VLAN 10 is a member of ports 11 and 12. VLAN 11 is a member of ports 12 and 13.

Figure 5-2: VLAN Membership

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

The VLAN User module uses services of the VLAN management functionality to configure VLAN memberships and VLAN port configurations such as PVID and UVID. Currently we support the following VLAN user types:

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

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

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

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

MSTP : The 802.1s Multiple Spanning Tree protocol (MSTP) uses VLANs to create multiple spanning trees in a network, which significantly improves network resource utilization while maintaining a loop-free environment.

DMS: Shows DMS VLAN membership status.

VCL: Shows MAC based VLAN entries configured by various MAC based VLAN users.

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.



: Displays if a port is included in a VLAN (VLAN port).



: Displays if a port is in the forbidden port list (forbidden port).



: Displays if a port is in the forbidden port list and at the same time attempted included in the VLAN (a conflict port). The port will not be a member of the VLAN in this case.

VLAN Membership: The VLAN Membership Status Page shows the current VLAN port members for all VLANs configured by a selected VLAN User (selection will be allowed by a Combo Box). When 'Combined' users are selected, it shows this information for all the VLAN Users, and this is by default. VLAN membership allows the frames classified to the VLAN ID to be forwarded on the respective VLAN member ports.

Show entries: You can choose how many items you want to show per page.

: At the dropdown select the VLAN User. The options are Combine, Admin, Forbidden VLANs, NAS, MVRP, GVRP, MVR, Voice VLAN, MEP, RMirror and DMS.

Buttons

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

Refresh: Click to refresh the page.

First Page: Use the button to start over..

Next Page: The button will use the last entry of the currently displayed VLAN entry as a basis for the next lookup.

Combined ▼

Combined

Admin

Forbidden VLANs

NAS

MVRP

GVRP

MVR

Voice VLAN

MEP

RMirror

DMS

5-3 VLAN Port Status

The Port Status function gathers the information of all VLAN status and reports it by the order of Combined, Admin, NAS, GVRP, MVR, Voice VLAN, MSTP, DMS, VCL. To display VLAN Port Status in the web UI:

1. Click VLAN Management and VLAN Port Status.
2. Specify the user type.
3. View the Port Status information.

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

Figure 5-3: VLAN Port Status

Parameter descriptions:

VLAN USER : VLAN User module uses services of the VLAN management functionality to configure VLAN memberships and VLAN port configuration such as PVID, UVID. The following VLAN User types are supported:

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

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

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

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

MSTP :The 802.1s Multiple Spanning Tree protocol (MSTP) uses VLANs to create multiple spanning trees in a network, which significantly improves network resource utilization while maintaining a loop-free environment.

DMS: Shows DMS VLAN membership status.

VCL : shows MAC-based VLAN entries configured by various MAC-based VLAN users.

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

Port Type : Shows the Port Type. Port type can be Unaware, C-port, S-port, or Custom S-port.

If Port Type is Unaware, all frames are classified to the Port VLAN ID and tags are not removed.

C-port is Customer Port. S-port is Service port. Custom S-port is S-port with a Custom TPID.

Ingress Filtering : Shows the ingress filtering on a port. This parameter affects VLAN ingress processing. If ingress filtering is enabled and the ingress port is not a member of the classified VLAN, the frame is discarded.

Frame Type : Shows whether the port accepts all frames or only tagged frames. This parameter affects VLAN ingress processing. If the port only accepts tagged frames, untagged frames received on that port are discarded.

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

Tx Tag : Shows egress filtering frame status whether tagged or untagged.

Untagged VLAN ID: 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.

: You can choose the VLAN User.

Buttons

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

Refresh: Click to refresh the page.

5-4 VLAN Name Configuration

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

LANTRONIX®

SM24TBT4XPA

VLAN Name Configuration

Home > VLAN Management > VLAN Name

Refresh First Page Next Page

Start from VLAN , entries per page.

| VLAN ID | VLAN Name |
|---------|------------------------------------|
| 1 | default |
| 2 | <input type="text" value="VLAN2"/> |
| 3 | <input type="text" value="VLAN3"/> |
| 4 | <input type="text" value="VLAN4"/> |
| 5 | <input type="text" value="Vid 5"/> |
| 6 | <input type="text" value="VID-6"/> |
| 7 | <input type="text" value="VID_7"/> |

Figure 5-3: VLAN Name Configuration

VLAN ID: Displays the VLAN IDs.

VLAN Name: Enter a name for the VLAN. By default, VLAN 1 is named “default” and cannot be edited. Special character are allowed. The space character is not allowed.

Buttons

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

Apply: Click to save changes.

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

First Page: Updates the table starting from the first entry in the Dynamic ARP Inspection table.

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

5-5 MAC-based VLAN

5-5.1 Configuration

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

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

1. Click VLAN Management, MAC-based VLAN and Configuration.
2. Click “Add New Entry”.
3. Specify the MAC address and VLAN ID.
4. Click Apply.

The screenshot shows the LANTRONIX web interface for the SM24TBT4XPA device. The main section is titled "MAC-based VLAN Membership Configuration". It features a sidebar on the left with a tree view containing: System, Port Management, PoE Management, VLAN Management (expanded), VLAN Configuration, VLAN Membership, VLAN Port Status, VLAN Name, MAC-based VLAN (expanded), and Configuration. The top navigation bar includes "Auto-Logout OFF", "Click Save Button", and icons for home, help, and refresh. The main configuration area has an "Auto-refresh" toggle set to "off", and buttons for "Refresh", "First Page", and "Next Page". Below these is a table with columns for "Delete", "MAC Address", "VLAN ID", and "Port Members" (ports 1-28). The first row shows a MAC address of "00-00-00-00-00-00" and VLAN ID "1", with checkboxes for ports 1 through 10 checked. A second row is partially visible with a "Delete" button and an empty MAC address field. At the bottom of the table are buttons for "Add New Entry", "Apply", and "Reset".

Figure 5-4.1: MAC-based VLAN Configuration

Parameter descriptions:

MAC Address : Indicates the MAC address.

VLAN ID : Indicates the VLAN ID.

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

Buttons

Add New Entry: Click to add a new MAC-based VLAN entry. An empty row is added to the table, and the MAC-based VLAN entry can be configured as needed. Any unicast MAC address can be configured for the MAC-based VLAN entry. No broadcast or multicast MAC addresses are allowed. Valid values for a VLAN ID are 1 - 4095.

Delete: To delete a MAC-based VLAN entry, check this box and press apply.

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: Click to refresh the page.

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

5-5.2 Status

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

1. Click VLAN Management, MAC-based VLAN, and Status.
2. To auto-refresh the information click the “Auto-refresh” button.
3. Click “Refresh” to refresh the MAC-based VLAN Membership Status.

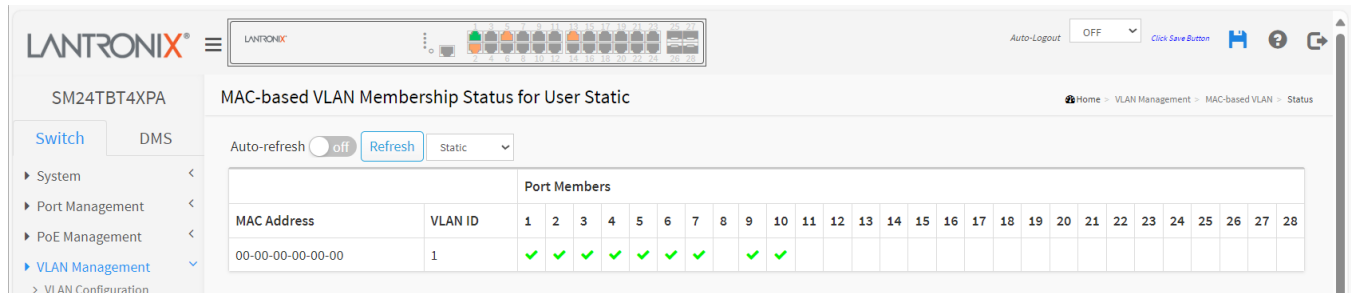


Figure 5-4.2: MAC-based VLAN Membership Status

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.

5-6 Protocol-based VLAN

This section describe Protocol -based VLAN. 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.

5-6.1 Protocol to Group

This page allows you to 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 selected stack switch unit switch.

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

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

LANTRONIX® SM24TBT4XPA

Protocol-based VLAN Configuration

Auto-refresh ☐ off [Refresh](#)

Protocol to Group Mapping Table

| Delete | Frame Type | Value | Group Name |
|--------------------------|------------|----------------|------------|
| <input type="checkbox"/> | Ethernet | 0800 | Grp1 |
| <input type="checkbox"/> | SNAP | 00-E0-2B-0001 | Grp2 |
| <input type="checkbox"/> | LLC | FF-FF | Grp3 |
| Delete | Ethernet | Etype: 0x 0800 | |

[Add New Entry](#)

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

Figure 5-5.1: Protocol to Group Mapping Table

Parameter descriptions:

Frame Type : Frame Type can have one of the following values:

1. **Ethernet**
2. **LLC**
3. **SNAP**

Note: On changing the Frame Type field, valid value of the following text field will vary depending on the new frame type you selected.

Value : Valid value that can be entered in this text field depends on the option selected from the preceding Frame Type selection menu. Below is the criteria for three different Frame Types:

Ethernet: Values in the text field when Ethernet is selected as a Frame Type is called etype. Valid values for etype range from 0x0600 to 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 value in format of xx xx xx where each pair (xx) in string 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.

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

Buttons

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

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 new entry.

Apply: Click to save changes.

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

5-6.2 Group to VLAN

This page lets you map an already configured Group Name to a VLAN. To configure Group Name to VLAN mapping in the web UI:

1. Click VLAN Management, Protocol-based VLAN, and Group to VLAN.
2. Click “Add New Entry”.
3. Specify the Group Name and VLAN ID.
4. Click Apply.

Figure 5-5.2: Group Name to VLAN Mapping Table

Parameter descriptions:

Group Name : A valid Group Name is a string of almost 16 characters. Special characters and space characters are not allowed.

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

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

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. Legal values for a VLAN ID are 1 through 4095. The button can be used to undo the addition of new entry.

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: Click to refresh the page immediately.

5-7 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.

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

1. Click VLAN Management and IP Subnet-based VLAN.
2. Click “Add New Entry”.
3. Specify IP Address, Mask Length, VLAN ID.
4. Click Apply.

The screenshot shows the Lantronix web interface for the SM24TBT4XPA device. The left sidebar contains a navigation menu with options: System, Port Management, PoE Management, VLAN Management (selected), VLAN Membership, VLAN Port Status, VLAN Name, MAC-based VLAN, Protocol-based VLAN, and IP Subnet-based VLAN. The main content area is titled 'IP Subnet-based VLAN Configuration'. It features a table with columns: Delete, IP Address, Mask Length, VLAN ID, and Port Members (ports 1-26). The first row shows an entry with IP Address 0.0.0.0, Mask Length 24, and VLAN ID 1. The checkboxes for ports 2, 4, and 5 are checked. Below the table are buttons for 'Add New Entry', 'Apply', and 'Reset'. The top right of the interface shows an 'Auto-Logout' dropdown set to 'OFF' and a 'Click Save Button' link.

Figure 5-6: IP Subnet-based VLAN Membership Configuration

Parameter descriptions:

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 to VLAN ID mapping entry. To include a port in a mapping, simply check the box. To remove or exclude the port from the mapping, make sure the box is unchecked. By default, no ports are members and all boxes are unchecked.

Buttons

Delete: To delete an IP subnet-based VLAN entry, check this box and click Apply. The entry will be

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

The IP subnet-based VLAN entry is enabled on the selected stack switch unit when you click on "Save".

The “Delete” button can be used to undo the addition of new IP subnet-based VLANs. The maximum possible IP subnet-based VLAN entries are limited to 128.

Apply: Click to save changes.

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

5-8 GVRP

The Generic Attribute Registration Protocol (GARP) provides a generic framework whereby devices in a bridged LAN, e.g. end stations and switches, can register and de-register attribute values, such as VLAN Identifiers, with each other. In doing so, the attributes are propagated to devices in the bridged LAN, and these devices form a “reachability” tree that is a subset of an active topology. GARP defines the architecture, rules of operation, state machines and variables for the registration and de-registration of attribute values.

A GARP participation in a switch or an end station consists of a GARP application component, and a GARP Information Declaration (GID) component associated with each port or the switch. The propagation of information between GARP participants for the same application in a bridge is carried out by the GARP Information Propagation (GIP) component. Protocol exchanges take place between GARP participants by means of LLC Type 1 services, using the group MAC address and PDU format defined for the GARP application concerned.

To configure GVRP in the web UI:

1. Click VLAN Management and GVRP.
2. Enable or disable GVRP.
3. Specify Join-time, Leave-time, Leave All-time, and Max VLANs.
4. Enable or disable the Mode.
5. Click Apply to save the settings.
6. To cancel the settings click the Reset button to revert to previously saved values.

LANTRONIX SM24TBT4XPA

GVRP Port Configuration

Enable GVRP: ☒ on

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

GVRP Port Configuration

| Port | Mode |
|------|--------------|
| * | GVRP enabled |
| 1 | GVRP enabled |
| 2 | GVRP enabled |
| 3 | Disabled |
| 4 | GVRP enabled |
| 5 | Disabled |
| 6 | GVRP enabled |

Figure 5-7: GVRP Configuration

Parameter descriptions:

Enable GVRP: The GVRP feature is enabled globally by checking the checkbox.

GVRP protocol timers :

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

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

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

Max VLANs : When GVRP is enabled a maximum number of VLANs supported by GVRP is specified. By default this number is 20. This number can only be changed when GVRP is turned off.

Port : The Port column shows the list of ports.

Mode: This configuration is to enable/disable GVRP Mode on a particular port locally.

Enabled: Select to Enable GVRP mode on this port.

Disabled: Select to Disable 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.

5-9 Private VLAN

The Private VLAN membership configurations for the switch can be monitored and modified here. Private VLANs can be added or deleted here. Port members of each Private VLAN can be added or removed here.

Private VLANs are based on the source port mask, and there are no connections to VLANs. This means that VLAN IDs and Private VLAN IDs can be identical. A port must be a member of both a VLAN and a Private VLAN to be able to forward packets. By default, all ports are VLAN unaware and members of VLAN 1 and Private VLAN 1.

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

VLAN Priority : Voice VLAN > MAC based VLAN > Protocol based VLAN > Tag based VLAN.

To configure Private VLANs in the web UI:

1. Click VLAN Management and Private VLAN.
2. Configure the Private VLAN membership for the switch.
3. Click Apply.

The screenshot displays the 'Private VLAN Membership Configuration' page in the Lantronix web interface. The sidebar on the left shows the navigation menu with 'VLAN Management' selected. The main content area features a table for configuring Private VLAN membership. The table has columns for 'Delete', 'PVLAN ID', and 'Port Members' (ports 1 through 27). A row for PVLAN ID 1 is shown with all port members checked. Below the table are buttons for 'Add New Private VLAN', 'Apply', and 'Reset'.

Figure 5-8: Private VLAN Membership Configuration

Parameter descriptions:

Delete: To delete a private VLAN entry, check this box.

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.

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

Buttons

Apply: Click to save changes.

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

5-10 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 having said plurality of ports, each port configured as a protected port or a non-protected port. An address table memory stores an address table having a destination address and port number pair. A forwarding map generator generates a forwarding map which is responsive to a destination address of a data packet. The method for isolating ports on a layer 2 switch comprises configuring each of the ports on the layer 2 switch as a protected port or a non-protected port. A destination address on a data packet is matched with a physical address on said layer 2 switch and a forwarding map is generated for the data packet based upon the destination address on the data packet. The data packet is then sent to the plurality of ports pursuant to the forwarding map generated based upon 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.

To configure Port Isolation in the web UI:

1. Click VLAN Management and Port Isolation.
2. Enable the ports you want to isolate.
3. Click Apply.

Figure 5-9: Port Isolation Configuration

Parameter descriptions:

Port Numbers : A check box is provided for each port of a private VLAN. When checked, port isolation is enabled on that port. When unchecked, port isolation is disabled on that port. By default, port isolation is disabled on all ports.

Buttons

Apply: Click to save changes.

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

5-11 Voice VLAN

Voice VLAN is VLAN configured specially for voice traffic. By adding the ports with voice devices attached to voice VLAN, we can perform QoS-related configuration for voice data, ensuring the transmission priority of voice traffic and voice quality.

5-11.1 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. It should be configured with its own GUI.

To configure Voice VLAN in the web UI:

1. Click VLAN Management, Voice VLAN and Configuration.
2. Select “on” in the Voice VLAN Configuration.
3. Specify VLAN ID, Aging Time, and Traffic Class.
4. Select Port Members in the Voice VLAN Configuration.
5. Specify (Mode, Security, Discovery Protocol) in the Port Configuration.
6. Click the Apply to save the settings.
7. To cancel the settings click the Reset button to revert to previously saved values.

LANTRONIX SM24TBT4XPA

Auto-Logout OFF Click Save Button

Voice VLAN Configuration

Home > VLAN Management > Voice VLAN > Configuration

Voice VLAN Configuration

| | |
|------------|-------------------------------------|
| Mode | <input checked="" type="radio"/> on |
| VLAN ID | 100 |
| Aging Time | 86400 seconds |
| Traffic | 7 (High) |

Port Configuration

| Port | Mode | Security | Discovery Protocol |
|------|----------|----------|--------------------|
| * | Disabled | <> | <> |
| 1 | Disabled | Disabled | OUI |
| 2 | Disabled | Enabled | OUI |
| 3 | Disabled | Enabled | LLDP |
| 4 | Disabled | Enabled | Both |
| 5 | Disabled | Enabled | OUI |
| 6 | Disabled | Disabled | OUI |

Figure 5-10.1: Voice VLAN Configuration

Parameter descriptions:

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

on: Enable Voice VLAN mode operation.

off: 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: Indicates the Voice VLAN traffic class. All traffic on the Voice VLAN will apply this class.

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

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

Disabled: Disjoin from Voice VLAN.

Auto: Enable auto detect mode. It detects whether there is VoIP phone attached to the specific port and configures the Voice VLAN members automatically.

Forced: Force join to Voice VLAN.

This field will be read only if STP feature is enabled. And the STP port mode will be read only if this field be set to the mode other than Disabled.

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

Enabled: Enable Voice VLAN security mode operation.

Disabled: Disable Voice VLAN security mode operation.

Port Discovery Protocol: Indicates the Voice VLAN port discovery protocol. It will only work when auto detect mode is enabled. We should enable LLDP feature before configuring discovery protocol to "LLDP" or "Both". Changing the discovery protocol to "OUI" or "LLDP" will restart auto detect process. Possible discovery protocols are:

OUI: Detect telephony device by OUI address.

LLDP: Detect telephony device by LLDP.

Both: Both OUI and LLDP.

Buttons

Apply : Click to save changes.

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

5-11.2 OUI

This page lets you set and view the Voice VLAN OUI table. The maximum entry number is 16. Modifying the OUI table will restart auto detection of the OUI (Organizationally Unique Identifier) process.

To configure Voice VLAN OUI in the web UI:

1. Click VLAN Management, Voice VLAN, and OUI
2. Select “Add New Entry” in the Voice VLAN OUI table.
3. Specify Telephony OUI and Description.
4. Click Apply.

The screenshot shows the Lantronix web interface for the SM24TBT4XPA device. The top navigation bar includes the Lantronix logo, a status bar with various indicators, and an 'Auto-Logout' dropdown set to 'OFF'. The left sidebar shows a tree view with 'VLAN Management' selected. The main content area is titled 'Voice VLAN OUI Table' and contains a table with the following structure:

| Delete | Telephony OUI | Description |
|---------------------------------------|---------------|-------------|
| <input type="button" value="Delete"/> | 00-0f-e2 | cisc0 |
| <input type="button" value="Delete"/> | | |

Below the table are three buttons: 'Add New Entry', 'Apply', and 'Reset'. The breadcrumb trail at the top right reads: Home > VLAN Management > Voice VLAN > OUI.

Figure 5-10.2: 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 IEEE. It must be 6 characters long and the input format is "xx-xx-xx" (x is a hexadecimal digit).

Description : The description of OUI address. Normally, it describes which vendor telephony device it belongs to. The allowed string length is 0 to 32 characters.

Buttons

Add New Entry : Click to add a new entry in Voice VLAN OUI table. An empty row is added to the table.

Apply: Click to save changes.

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

6. Quality of Service

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

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

6-1 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 Quality of Service and Port Classification.
2. Select QoS Ingress Port parameters.
3. Click the Apply to save the settings.
4. To cancel the settings click the Reset button. It will revert to previously saved values.
5. Click “PCP Classification” to next page “Port PCP Classification”.

| Port | Queue Priority (7 is the highest priority) | DPL | PCP | DEI | PCP Classification | DSCP Based | WRED Group |
|------|---|-----|-----|-----|--------------------|-------------------------------------|------------|
| * | <> | <> | <> | <> | | <input type="checkbox"/> | <> |
| 1 | 7 | 0 | 0 | 0 | Disabled | <input type="checkbox"/> | 1 |
| 2 | 6 | 1 | 2 | 0 | Disabled | <input checked="" type="checkbox"/> | 2 |
| 3 | 5 | 3 | 0 | 1 | Disabled | <input type="checkbox"/> | 1 |
| 4 | 4 | 1 | 5 | 0 | Disabled | <input checked="" type="checkbox"/> | 1 |
| 5 | 0 | 2 | 0 | 1 | Disabled | <input checked="" type="checkbox"/> | 1 |
| 6 | 0 | 0 | 0 | 0 | Disabled | <input type="checkbox"/> | 3 |
| 7 | 0 | 0 | 0 | 0 | Disabled | <input type="checkbox"/> | 3 |
| 8 | 0 | 0 | 0 | 0 | Disabled | <input type="checkbox"/> | 1 |

Figure 6-1: QoS Ingress Port Classification

Parameter descriptions:

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

Queue Priority: Controls the default CoS value. All frames are classified to a CoS. There is a one-to-one mapping between CoS, queue and priority. A CoS of 0 (zero) has the lowest priority.

If the port is VLAN aware, the frame is tagged and Tag Class. is enabled, then the frame is classified to a CoS that is mapped from the PCP and DEI value in the tag. Otherwise the frame is classified to the default CoS.

The classified CoS can be overruled by a QCL entry.

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

DPL: Controls the default drop precedence level. All frames are classified to a drop precedence level.

If the port is VLAN aware, the frame is tagged and Tag Class. is enabled, then the frame is classified to a DPL that is mapped from the PCP and DEI value in the tag. Otherwise the frame is classified to the default DPL.

The classified DPL can be overruled by a QCL entry.

PCP: Controls the default PCP value. All frames are classified to a PCP value. If the port is VLAN aware and the frame is tagged, then the frame is classified to the PCP value in the tag. Otherwise the frame is classified to the default PCP value.

DEI: Controls the default DEI value. All frames are classified to a DEI value. If the port is VLAN aware and the frame is tagged, then the frame is classified to the DEI value in the tag. Otherwise the frame is classified to the default DEI value.

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

WRED Group: Controls the WRED group membership.

PCP Classification: Shows the classification mode for tagged frames on this port.

Disabled: Use default CoS and DPL for tagged frames.

Enabled: Use mapped versions of PCP and DEI for tagged frames.

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.

Ingress Port PCP Classification Port 2

Port 2

Tagged Frames Settings

PCP Classification Enabled

(PCP, DEI) to (Queue Priority, DP level) Mapping

| PCP | DEI | Queue Priority | DP level |
|-----|-----|----------------|----------|
| * | * | <> | <> |
| 0 | 0 | 1 | 0 |
| 0 | 1 | 2 | 1 |
| 1 | 0 | 3 | 2 |
| 1 | 1 | 5 | 3 |
| 2 | 0 | 2 | 0 |
| 2 | 1 | 2 | 1 |
| 2 | 0 | 2 | 0 |
| 2 | 1 | 2 | 1 |
| 2 | 0 | 2 | 0 |

Parameter descriptions:

PCP Classification: Controls the classification mode for tagged frames on this port.

Disabled: Use default CoS and DPL for tagged frames.

Enabled: Use mapped versions of PCP and DEI for tagged frames.

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

Buttons

Apply : Click to save changes.

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

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

6-2 Port Policers

This page provides an overview of QoS Ingress Port Policers for all switch ports. Port Policing is useful in constraining traffic flows and marking frames above specific rates. Policing is primarily useful for data flows and voice or video flows because voice and video usually maintains a steady rate of traffic.

To configure QoS Port Policers in the web UI:

1. Click Quality of Service and Port Policers.
2. Click which port need to enable the QoS Ingress Port Policers, and configure the Rate limit condition.
3. Select the column Rate and Unit.
4. Click Apply to save the configuration.
5. To cancel the settings click the Reset button. It will revert to previously saved values.

| Port | Enable | Rate | Unit | Flow Control |
|------|-------------------------------------|------|------|-------------------------------------|
| * | <input checked="" type="checkbox"/> | 500 | < > | <input type="checkbox"/> |
| 1 | <input checked="" type="checkbox"/> | 500 | Mbps | <input type="checkbox"/> |
| 2 | <input checked="" type="checkbox"/> | 400 | fps | <input checked="" type="checkbox"/> |
| 3 | <input type="checkbox"/> | 500 | kfps | <input checked="" type="checkbox"/> |
| 4 | <input checked="" type="checkbox"/> | 500 | kfps | <input type="checkbox"/> |
| 5 | <input type="checkbox"/> | 999 | kfps | <input type="checkbox"/> |
| 6 | <input type="checkbox"/> | 500 | kfps | <input type="checkbox"/> |
| 7 | <input checked="" type="checkbox"/> | 500 | kfps | <input type="checkbox"/> |
| 8 | <input checked="" type="checkbox"/> | 500 | kfps | <input type="checkbox"/> |
| 9 | <input checked="" type="checkbox"/> | 500 | kfps | <input type="checkbox"/> |
| 10 | <input checked="" type="checkbox"/> | 500 | kfps | <input type="checkbox"/> |

Figure 6-2: QoS Ingress Port Policers Configuration

Parameter descriptions:

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

Enabled : To enable the Port(s) you need to have the QoS Ingress Port Policers function enabled.

Rate : To set the Rate limit value for this port, the default is 1000000.

Unit: Controls the unit of measure for the port policer rate as kbps, Mbps, fps or kfps.

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

Buttons

Apply: Click to save changes.

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

6-3 Port Shapers

This page lets you set QoS Egress Port Shapers for all switch ports. To configure QoS Port Shapers:

1. Click QoS and Port Shapers.
2. Select the Port to display its QoS Egress Port Shapers.
3. Specify the Queue Shaper parameters.
4. Click the Apply button to save the settings.
5. To cancel the settings click the Reset button to revert to previously saved values.

LANTRONIX® SM24TBT4XPA

QoS Egress Port Shapers

Port: Port 1

| Queue | Enable | Rate | Unit |
|-------|-------------------------------------|------|------|
| 0 | <input checked="" type="checkbox"/> | 500 | kbps |
| 1 | <input checked="" type="checkbox"/> | 625 | kbps |
| 2 | <input checked="" type="checkbox"/> | 550 | kbps |
| 3 | <input checked="" type="checkbox"/> | 500 | kbps |
| 4 | <input type="checkbox"/> | 500 | kbps |
| 5 | <input type="checkbox"/> | 500 | kbps |
| 6 | <input type="checkbox"/> | 500 | kbps |
| 7 | <input type="checkbox"/> | 500 | kbps |

Port Shaper

| Enable | Rate (kbps) | Rate-type |
|-------------------------------------|-------------|-----------|
| <input checked="" type="checkbox"/> | 500 | Line |

Apply Reset

Figure 6-3: QoS Egress Port Shapers

Parameter descriptions:

Port: The logical port for the settings contained on the page. Click on the port number in order to configure the shapers for that port.

Queue Shaper:

Queue *n*: Shows queues 0-7.

Enable: Controls whether the queue shaper is enabled for this queue on this switch port.

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

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

Port Shaper:

Enable: Checkbox to enable or disable the port shaper for the row.

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

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

Line: Specify that this shaper operates on line rate.

Data: Specify that this shaper operates on data rate.

Buttons

Apply: Click to save changes.

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

6-4 Storm Control

This page lets you configure Storm control for the switch. There is a destination lookup failure storm rate control, multicast storm rate control, and a broadcast storm rate control. These only affect flooded frames, i.e. frames with a (VLAN ID, DMAC) pair not present on the MAC Address table. The configuration indicates the permitted packet rate for unicast, multicast or broadcast traffic across the switch

To configure the Storm Control parameters in the web UI:

1. Click Quality of Service and Storm Control.
2. Select the frame type to enable storm control.
3. Set the Rate Parameters and Unit.
4. Click the port(s) to enable, and configure the Rate limit condition.
5. Click the Apply button to save the settings.
6. To cancel the settings click the Reset button to revert to previously saved values.

Global Storm Policer Configuration

| Frame Type | Enable | Rate | Unit |
|------------|-------------------------------------|------|------|
| Unicast | <input type="checkbox"/> | 10 | fps |
| Multicast | <input checked="" type="checkbox"/> | 10 | Mbps |
| Broadcast | <input checked="" type="checkbox"/> | 10 | Mbps |

Port Storm Policer Configuration

| Port | Unicast Frames | | | Broadcast Frames | | | Unknown Frames | | |
|------|-------------------------------------|------|------|-------------------------------------|------|------|-------------------------------------|------|------|
| | Enable | Rate | Unit | Enable | Rate | Unit | Enable | Rate | Unit |
| * | <input checked="" type="checkbox"/> | 500 | kbps | <input checked="" type="checkbox"/> | 500 | kbps | <input checked="" type="checkbox"/> | 500 | kbps |
| 1 | <input checked="" type="checkbox"/> | 500 | kbps | <input checked="" type="checkbox"/> | 500 | kbps | <input checked="" type="checkbox"/> | 500 | kbps |
| 2 | <input checked="" type="checkbox"/> | 500 | kbps | <input checked="" type="checkbox"/> | 500 | kbps | <input checked="" type="checkbox"/> | 500 | kbps |
| 3 | <input checked="" type="checkbox"/> | 500 | kbps | <input type="checkbox"/> | 500 | kbps | <input type="checkbox"/> | 500 | kbps |
| 4 | <input type="checkbox"/> | 500 | kbps | <input type="checkbox"/> | 500 | kbps | <input type="checkbox"/> | 500 | kbps |
| 5 | <input type="checkbox"/> | 500 | kbps | <input type="checkbox"/> | 500 | kbps | <input type="checkbox"/> | 500 | kbps |
| 6 | <input type="checkbox"/> | 500 | kbps | <input type="checkbox"/> | 500 | kbps | <input type="checkbox"/> | 500 | kbps |

Figure 6-4: Storm Control Configuration

Parameter descriptions:

Global Storm Policer Configuration: Global storm policers for the switch are configured on this page. There is a unicast storm policer, multicast storm policer, and a broadcast storm policer. These only affect flooded frames, i.e. frames with a (VLAN ID, DMAC) pair not present in the MAC Address table.

Frame Type: The frame type for which the configuration below applies.

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

Rate: Controls the rate for the global storm policer. This value is restricted to 10-13128147 when "Unit" is fps or

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

Unit: Controls the unit of measure for the global storm policer rate as fps, kfps, kbps or Mbps.

Buttons

Apply: Click to save changes.

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

6-5 Port Scheduler

This page lets you set QoS Egress Port Scheduler for all switch ports. To configure QoS Port Schedulers in the web UI:

1. Click QoS and Port Scheduler.
2. Click the Port and display the QoS Egress Port Schedulers.
3. Select Port and Scheduler Mode, and specify the Queue Shaper parameter.
4. Click the Apply button to save the settings.
5. To cancel the settings click the Reset button to revert to previously saved values.

| Port | Mode | Weight | | | | | | | |
|------|-----------------|--------|----|----|----|----|----|----|----|
| | | Q0 | Q1 | Q2 | Q3 | Q4 | Q5 | Q6 | Q7 |
| 1 | Strict Priority | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 |
| 2 | Weighted | 17 | 17 | 17 | 17 | 17 | 17 | 17 | 17 |
| 3 | Weighted | 12 | 20 | 17 | 17 | 17 | 17 | 17 | 17 |
| 4 | Weighted | 17 | 17 | 17 | 17 | 17 | 17 | 17 | 17 |
| 5 | Strict Priority | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 |
| 6 | Strict Priority | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 |
| 7 | Strict Priority | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 |
| 8 | Strict Priority | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 |
| 9 | Strict Priority | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 |
| 10 | Strict Priority | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 |

Figure 6-5: QoS Egress Port Schedulers

Parameter descriptions:

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

Mode: Select the scheduling mode for this port (Strict Priority or Weighted). If Weighted is selected, the weight must be an integer value between 1 and 100.

Qn: Shows the weight for this queue and port.

Buttons

Apply: Click to save changes.

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

6-6 Port PCP Remarking

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

1. Click Quality of Service and Port PCP Remarking.
2. Click the Port to display its QoS Port PCP Remarking.
3. Select the Port and PCP Remarking Mode and specify the parameters.
4. Click the Apply button to save the settings.
5. To cancel the settings click the Reset button to revert to previously saved values.

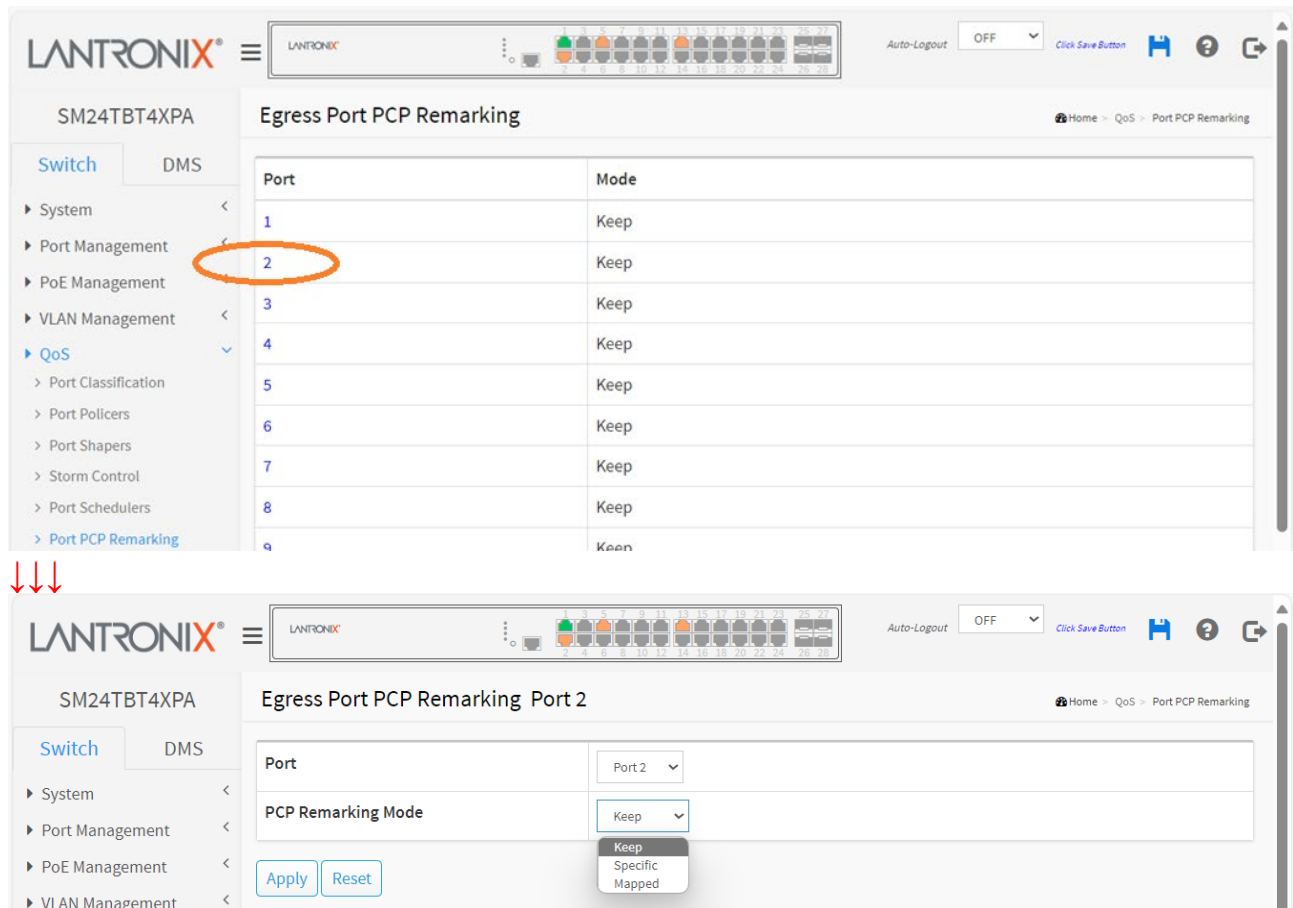


Figure 6-6: Port PCP Remarking

Parameter descriptions:

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

Mode: Shows the PCP remarking mode for this port.

Keep: Use classified PCP/DEI values.

Specific: Use default PCP/DEI values.

Mapped: Use mapped versions of CoS and DPL.

Buttons

Apply : Click to save changes.

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

6-7 DSCP

6-7.1 Port DSCP

This page lets you set the QoS Port DSCP settings for all switch ports. To configure the QoS Port DSCP parameters in the web UI:

1. Click Quality of Service, DSCP, and 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 to revert to previously saved values.

The screenshot shows the Lantronix web interface for the SM24TBT4XPA device. The main content area is titled "QoS Port DSCP Configuration". On the left, there is a sidebar with a "Switch" tab selected, showing a tree view of configuration options including System, Port Management, PoE Management, VLAN Management, QoS (selected), Port Classification, Port Policers, Port Shapers, Storm Control, Port Schedulers, Port PCP Remarking, DSCP (expanded), Port DSCP (selected), and DSCP Translation. The main table has columns for "Port", "Ingress Translate", "Ingress Classify", and "Egress Rewrite". The "Ingress Translate" column contains checkboxes, and the "Ingress Classify" column contains dropdown menus. The "Egress Rewrite" column contains dropdown menus. The table lists ports from 1 to 7, with port 1 being the default configuration.

| Port | Ingress | | Egress |
|------|-------------------------------------|-----------------------|----------------------|
| | Translate | Classify | Rewrite |
| * | <input type="checkbox"/> | <div>⌵</div> | <div>⌵</div> |
| 1 | <input type="checkbox"/> | Disable <div>⌵</div> | Enable <div>⌵</div> |
| 2 | <input checked="" type="checkbox"/> | DSCP=0 <div>⌵</div> | Enable <div>⌵</div> |
| 3 | <input checked="" type="checkbox"/> | Selected <div>⌵</div> | Remap <div>⌵</div> |
| 4 | <input checked="" type="checkbox"/> | Selected <div>⌵</div> | Remap <div>⌵</div> |
| 5 | <input checked="" type="checkbox"/> | All <div>⌵</div> | Remap <div>⌵</div> |
| 6 | <input checked="" type="checkbox"/> | DSCP=0 <div>⌵</div> | Disable <div>⌵</div> |
| 7 | <input type="checkbox"/> | Disable <div>⌵</div> | Disable <div>⌵</div> |

Figure 6-7.1: QoS Port DSCP Configuration

Parameter descriptions:

Port : The Port column shows the list of ports for which you can configure DSCP ingress and egress settings.

Ingress : In Ingress settings you can change ingress translation and classification settings for individual ports. There are two configuration parameters available in Ingress:

Translate: To enable Ingress Translation click the checkbox.

Classify: Classification for a port have 4 different values

Disable: No Ingress DSCP Classification.

DSCP=0: Classify if incoming (or translated if enabled) DSCP is 0.

Selected: Classify only selected DSCP for which classification is enabled as specified in DSCP Translation window for the specific DSCP.

All: Classify all DSCP.

Egress : 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.

6-7.2 DSCP Translation

This page lets you configure basic QoS DSCP Translation settings for the switch. DSCP translation can be done in Ingress or Egress.

To configure the DSCP Translation parameters in the web UI:

1. Click Quality of Service, DSCP, and DSCP Translation.
2. Set the Ingress Translate and Egress Remap parameters.
3. Enable or disable Classify.
4. Click the Apply button to save the settings.
5. To cancel the settings click the Reset button to revert to previously saved values.

The screenshot shows the Lantronix web UI for the SM24TBT4XPA switch. The left sidebar contains a navigation menu with the following items: System, Port Management, PoE Management, VLAN Management, QoS (expanded), Port Classification, Port Policers, Port Shapers, Storm Control, Port Schedulers, Port PCP Remarking, DSCP (expanded), Port DSCP, DSCP Translation (selected), DSCP Classification, and DSCP-Based QoS. The main content area is titled 'DSCP Translation' and contains a table with the following columns: DSCP, Ingress Translate, Classify, and Egress Remap. The table has 13 rows, with the first row being a header and the remaining 12 rows representing DSCP values from 0 to 11. The 'Classify' column has checkboxes, and the 'Egress Remap' column has dropdown menus. The 'Apply' and 'Reset' buttons are located at the bottom of the table.

| DSCP | Ingress Translate | Classify | Egress Remap |
|---------|-------------------|-------------------------------------|--------------|
| * | <> | <input type="checkbox"/> | <> |
| 0 (BE) | 0 (BE) | <input type="checkbox"/> | 0 (BE) |
| 1 | 1 | <input type="checkbox"/> | 4 |
| 2 | 2 | <input checked="" type="checkbox"/> | 8 (CS1) |
| 3 | 3 | <input checked="" type="checkbox"/> | 10 (AF11) |
| 4 | 8 (CS1) | <input checked="" type="checkbox"/> | 18 (AF21) |
| 5 | 20 (AF22) | <input checked="" type="checkbox"/> | 5 |
| 6 | 16 (CS2) | <input type="checkbox"/> | 6 |
| 7 | 7 | <input type="checkbox"/> | 7 |
| 8 (CS1) | 8 (CS1) | <input type="checkbox"/> | 8 (CS1) |
| 62 | 62 | <input type="checkbox"/> | 62 |
| 63 | 63 | <input type="checkbox"/> | 63 |

Apply Reset

Figure 6-7.2: DSCP Translation Configuration

Parameter descriptions:

DSCP : Maximum number of supported DSCP values are 64 and valid DSCP value ranges from 0 to 63.

Ingress : Ingress side DSCP can be first translated to new DSCP before using the DSCP for QoS class and DPL map. There are two configuration parameters for DSCP Translation:

Translate: DSCP at Ingress side can be translated to any of (0-63) DSCP values.

Classify: Click to enable Classification at Ingress side.

Egress : Select the DSCP value from select menu to which you want to remap. DSCP value range from 0 - 63.

Buttons

Apply : Click to save changes.

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

6-7.3 DSCP Classification

This page lets you map DSCP value to a QoS Class and DPL value. To configure the DSCP Classification parameters in the web UI:

1. Click Quality of Service, DSCP and DSCP Translation.
2. Set the DSCP parameters.
3. Click the Apply button to save the settings.
4. To cancel the settings click the Reset button to revert to previously saved values.

| Queue Priority | DSCP DP0 | DSCP DP1 | DSCP DP2 | DSCP DP3 |
|----------------|----------|----------|----------|----------|
| * | 0 (BE) | 0 (BE) | 0 (BE) | 0 (BE) |
| 0 | 0 (BE) | 0 (BE) | 0 (BE) | 0 (BE) |
| 1 | 0 (BE) | 0 (BE) | 0 (BE) | 0 (BE) |
| 2 | 0 (BE) | 0 (BE) | 0 (BE) | 0 (BE) |
| 3 | 0 (BE) | 0 (BE) | 0 (BE) | 0 (BE) |
| 4 | 0 (BE) | 0 (BE) | 0 (BE) | 0 (BE) |
| 5 | 0 (BE) | 0 (BE) | 0 (BE) | 0 (BE) |
| 6 | 0 (BE) | 0 (BE) | 0 (BE) | 0 (BE) |

Figure 6-7.3: DSCP Classification Configuration

Parameter descriptions:

Queue Priority: Actual Class of Service.

DSCP DP0: Select the classified DSCP value (0-63) for Drop Precedence Level 0.

DSCP DP1: Select the classified DSCP value (0-63) for Drop Precedence Level 1.

DSCP DP2: Select the classified DSCP value (0-63) for Drop Precedence Level 2.

DSCP DP3: Select the classified DSCP value (0-63) for Drop Precedence Level 3.

Buttons

Apply : Click to save changes.

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

6-7.4 DSCP-Based QoS

This page lets you configure DSCP-based QoS mode and set basic QoS DSCP QoS Ingress Classification settings. To configure the DSCP-based QoS Ingress Classification parameters in the web UI:

1. Click Quality of Service, DSCP and DSCP-Based QoS.
2. Enable or disable the DSCP for Trust.
3. Select Queue Priority and DPL parameters.
4. Click the Apply button to save the settings.
5. To cancel the settings click the Reset button to revert to previously saved values.

The screenshot shows the LANTRONIX web interface for the SM24TBT4XPA device. The main content area is titled "DSCP-Based QoS Ingress Classification". It features a table with four columns: DSCP, Trust, Queue Priority, and DPL. The table lists 10 DSCP values (0-9) with their corresponding Trust status (checked/unchecked), Queue Priority (0-7), and DPL (0-3).

| DSCP | Trust | Queue Priority | DPL |
|---------|-------------------------------------|----------------|-----|
| * | <input checked="" type="checkbox"/> | <> | <> |
| 0 (BE) | <input checked="" type="checkbox"/> | 0 | 1 |
| 1 | <input checked="" type="checkbox"/> | 0 | 3 |
| 2 | <input checked="" type="checkbox"/> | 2 | 2 |
| 3 | <input checked="" type="checkbox"/> | 4 | 2 |
| 4 | <input checked="" type="checkbox"/> | 7 | 0 |
| 5 | <input type="checkbox"/> | 0 | 0 |
| 6 | <input checked="" type="checkbox"/> | 0 | 0 |
| 7 | <input type="checkbox"/> | 0 | 0 |
| 8 (CS1) | <input checked="" type="checkbox"/> | 0 | 0 |
| 9 | <input type="checkbox"/> | 0 | 0 |

Figure 6-7.4: DSCP-Based QoS Ingress Classification Configuration

Parameter descriptions:

DSCP : Maximum number of supported DSCP values are 64.

Trust : Click to check if the DSCP value is trusted.

Queue Priority: Queue Priority value can be 0 - 7, where priority 7 is the highest priority.

DPL : The Drop Precedence Level (0-3).

Buttons

Apply : Click to save changes.


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

6-8 QoS Control List

6-8.1 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 Quality of Service, QoS Control List and Configuration.

2. Click the  to add a new QoS Control List.
3. Set all parameters and select the Port Members to join the QCE rules.
4. Click the Apply button to save the settings. To cancel the settings click the Reset button.

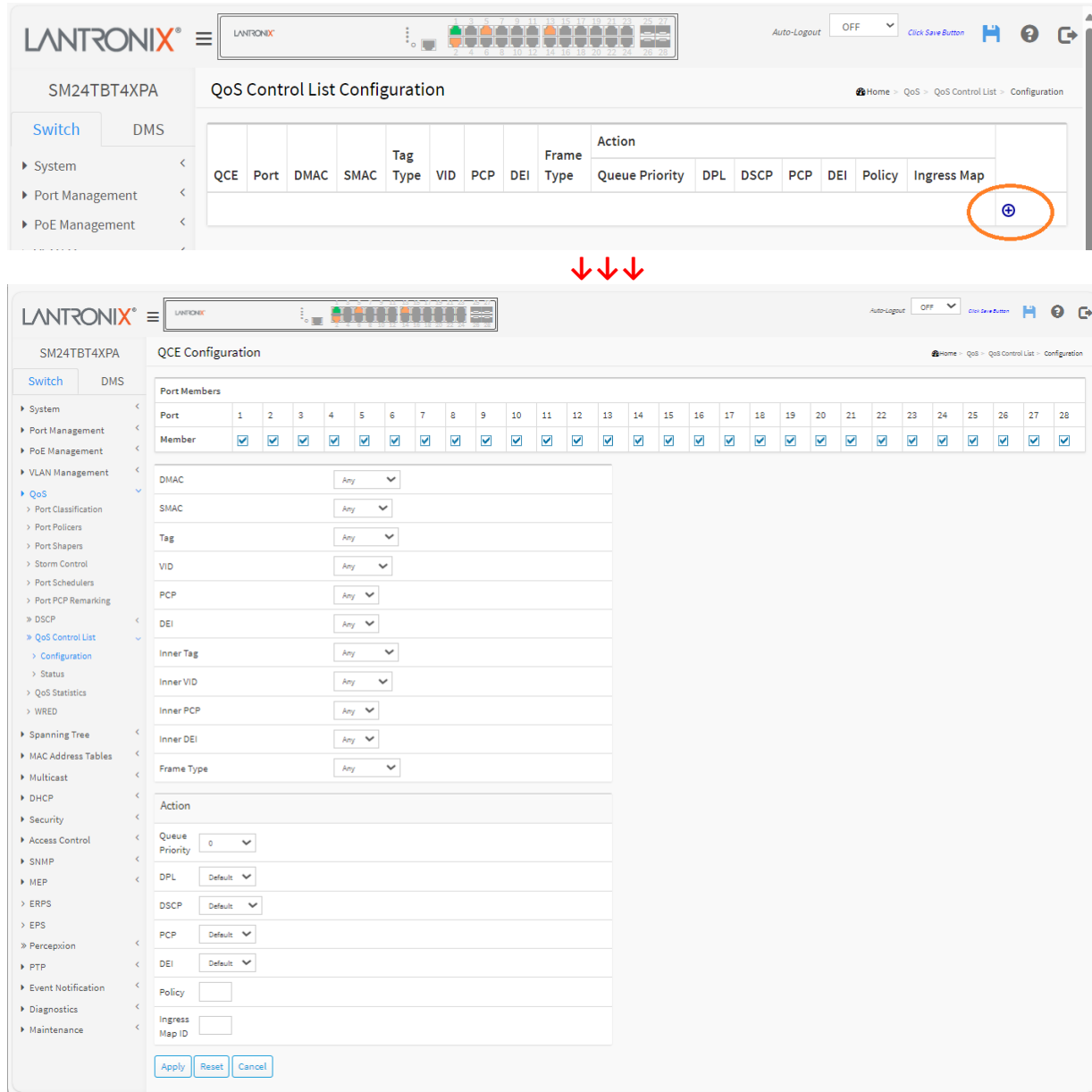


Figure 6-8.1: QoS Control List Configuration

Parameter descriptions:

QCE: Indicates the index of QCE.

Port : Indicates the list of ports configured with the QCE.

DMAC : Indicates the destination MAC address. Possible values are:

Any: Match any DMAC. The default value is 'Any'.

Unicast: Match unicast DMAC.

Multicast: Match multicast DMAC.

Broadcast: Match broadcast DMAC.

<MAC>: Match specific DMAC.

SMAC : Match specific source MAC address or 'Any'. If a port is configured to match on DMAC/DIP, this field indicates the DMAC.

Tag Type : Indicates tag type. Possible values are:

Any: Match tagged and untagged frames. The default value is 'Any'.

Untagged: Match untagged frames.

Tagged: Match tagged frames.

C-Tagged: Match C-tagged frames.

S-Tagged: Match S-tagged frames.

VID : Indicates VLAN ID, either a specific VID or range of VIDs. VID can be in the range 1-4095 or 'Any'.

PCP : Priority Code Point: Valid values of PCP are specific (0, 1, 2, 3, 4, 5, 6, 7) or range (0-1, 2-3, 4-5, 6-7, 0-3, 4-7) or 'Any'.

DEI : Drop Eligibility Indicator: Valid value of DEI are 0, 1 or 'Any'.

Frame Type : Indicates the type of frame to look for incoming frames. Possible frame types are:

Any: The QCE will match all frame type.

Ethernet: Only Ethernet frames (with Ether Type 0x600-0xFFFF) are allowed.

LLC: Only (LLC) frames are allowed.

SNAP: Only (SNAP) frames are allowed

IPv4: The QCE will match only IPV4 frames.

IPv6: The QCE will match only IPV6 frames.

Action: Indicates the classification action taken on ingress frame if parameters configured are matched with the frame's content. Possible actions are:

Queue Priority: Classify Class of Service.

DPL: Classify Drop Precedence Level.

DSCP: Classify DSCP value.

PCP: Classify PCP value.

DEI: Classify DEI value.

Policy: Classify ACL Policy number.

Ingress Map: Classify Ingress Map ID.

Port Members: Check the checkbox button to include the port in the QCL entry. By default all ports are included.

Key Parameters: Key configuration is described as below:

DMAC: Destination MAC address: Possible values are 'Unicast', 'Multicast', 'Broadcast', 'Specific' (xx-xx-xx-xx-xx-xx) or 'Any'.

SMAC: Source MAC address: xx-xx-xx-xx-xx-xx or 'Any'.

Tag: Value of Tag field can be 'Untagged', 'Tagged', 'C-Tagged', 'S-Tagged' or 'Any'.

VID: Valid value of VLAN ID can be any value in the range 1-4095 or 'Any'; user can enter either a specific value or a range of VIDs.

PCP: Valid value PCP are specific (0, 1, 2, 3, 4, 5, 6, 7) or range (0-1, 2-3, 4-5, 6-7, 0-3, 4-7) or 'Any'.

DEI: Valid value of DEI can be '0', '1' or 'Any'.

Inner Tag: Value of Inner Tag field can be 'Untagged', 'Tagged', 'C-Tagged', 'S-Tagged' or 'Any'.

Inner VID: Valid value of Inner VLAN ID can be any value in the range 1-4095 or 'Any'; enter either a specific value or a range of VIDs.

Inner PCP: Valid value of Inner PCP are specific (0, 1, 2, 3, 4, 5, 6, 7) or range (0-1, 2-3, 4-5, 6-7, 0-3, 4-7) or 'Any'.

Inner DEI: Valid value of Inner DEI can be '0', '1' or 'Any'.

Frame Type: Frame Type can have any of these values: Any, EtherType, LLC, SNAP, IPv4, or IPv6.

Note: All frame types are explained below.

Any: Allow all types of frames.

EtherType: Valid Ether Type can be 0x600-0xFFFF excluding 0x800(IPv4) and 0x86DD(IPv6) or 'Any'.

LLC: Can be:

DSAP Address: Valid DSAP (Destination Service Access Point) can vary from 0x00 to 0xFF or 'Any'.

SSAP Address: Valid SSAP(Source Service Access Point) can vary from 0x00 to 0xFF or 'Any'.

Control: Valid Control field can vary from 0x00 to 0xFF or 'Any'.

SNAP: PID: Valid PID (a.k.a, Ether Type) can be 0x0000-0xFFFF or 'Any'.

IPv4: Can be:

Protocol: IP protocol number: (0-255, 'TCP' or 'UDP') or 'Any'.

Source IP: Specific Source IP address in value/mask format or 'Any'. IP and Mask are in the format x.y.z.w where x, y, z, and w are decimal numbers between 0 and 255. When Mask is converted to a 32-bit binary string and read from left to right, all bits following the first zero must also be zero.

Destination IP: Specific Destination IP address in value/mask format or 'Any'.

IP Fragment: IPv4 frame fragmented option: 'Yes', 'No' or 'Any'.

DSCP: Diffserv Code Point value (DSCP): It can be a specific value, range of values or 'Any'. DSCP values are in the range 0-63 including BE, CS1-CS7, EF or AF11-AF43.

Sport: Source TCP/UDP port:(0-65535) or 'Any', specific or port range applicable for IP protocol UDP/TCP.

Dport: Destination TCP/UDP port:(0-65535) or 'Any', specific or port range applicable for IP protocol UDP/TCP.

IPv6: Can be:

Protocol: IP protocol number: (0-255, 'TCP' or 'UDP') or 'Any'.

Source IP: 32 LS bits of IPv6 source address in value/mask format or 'Any'.

Destination IP: Specific Destination IP address in value/mask format or 'Any'.

DSCP: Diffserv Code Point value (DSCP): It can be a specific value, range of values or 'Any'. DSCP values are in the range 0-63 including BE, CS1-CS7, EF or AF11-AF43.

Sport: Source TCP/UDP port:(0-65535) or 'Any', specific or port range applicable for IP protocol UDP/TCP.

Dport: Destination TCP/UDP port:(0-65535) or 'Any', specific or port range applicable for IP protocol UDP/TCP.

Action Parameters: Can be:

Queue Priority Class of Service: (0-7) or 'Default'.

DPL Drop Precedence Level: (0-3) or 'Default'.

DSCP DSCP: (0-63, BE, CS1-CS7, EF or AF11-AF43) or 'Default'.







PCP PCP: (0-7) or 'Default'. Note: PCP and DEI cannot be set individually.

DEI DEI:(0-1) or 'Default'.

Policy ACL Policy number: (0-127) or 'Default' (empty field).

Ingress Map Classify Ingress Map ID: (0-127) or 'Default' (empty field). 'Default' means that the default classified value is not modified by this QCE Modification.

Icons : You can modify each QCE (QoS Control Entry) in the table using the following buttons:

-  : Inserts a new QCE before the current row.
-  : Edits the QCE.
-  : Moves the QCE up the list.
-  : Moves the QCE down the list.
-  : Deletes the QCE.
-  : The lowest plus sign adds a new entry at the bottom of the QCE listings.

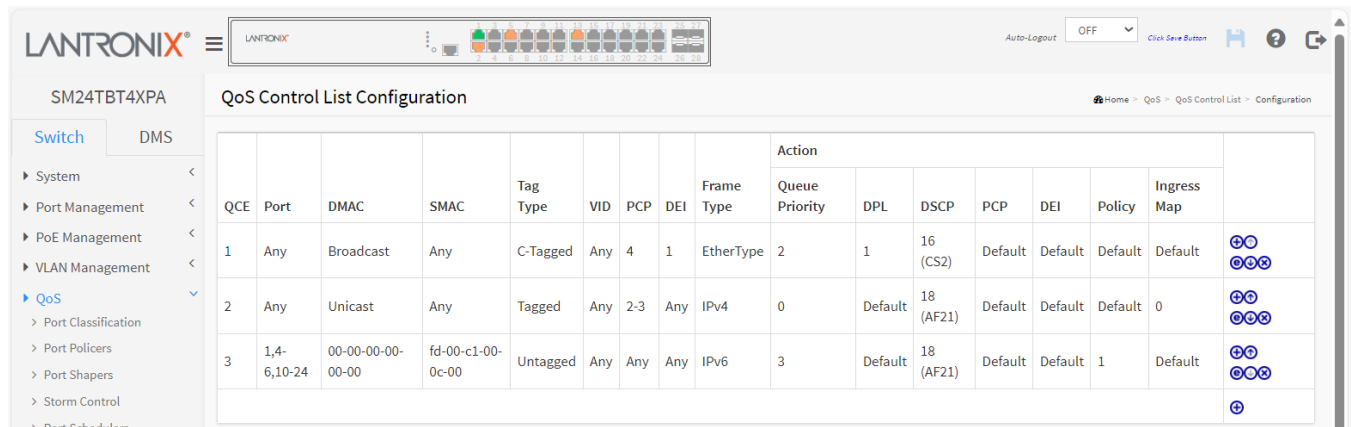
Buttons

Apply : Click to save changes.













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


Cancel : Return to the previous page without saving the configuration change.

Example:



The screenshot shows the Lantronix SM24TBT4XPA Web User Guide interface. The main content area is titled "QoS Control List Configuration". It features a table with the following columns: QCE, Port, DMAC, SMAC, Tag Type, VID, PCP, DEI, Frame Type, Queue Priority, DPL, DSCP, PCP, DEI, Policy, Ingress Map, and Action. The table contains three entries:

| QCE | Port | DMAC | SMAC | Tag Type | VID | PCP | DEI | Frame Type | Queue Priority | DPL | DSCP | PCP | DEI | Policy | Ingress Map | Action |
|-----|-------------|-------------------|-------------------|----------|-----|-----|-----|------------|----------------|---------|-----------|---------|---------|---------|-------------|---|
| 1 | Any | Broadcast | Any | C-Tagged | Any | 4 | 1 | EtherType | 2 | 1 | 16 (CS2) | Default | Default | Default | Default |     |
| 2 | Any | Unicast | Any | Tagged | Any | 2-3 | Any | IPv4 | 0 | Default | 18 (AF21) | Default | Default | Default | 0 |     |
| 3 | 1,4-6,10-24 | 00-00-00-00-00-00 | fd-00-c1-00-0c-00 | Untagged | Any | Any | Any | IPv6 | 3 | Default | 18 (AF21) | Default | Default | 1 | Default |     |

At the bottom of the table, there is a plus sign icon () to add a new entry.

6-8.2 Status

This page lets you configure and show the QCL status by different QCL users. Each row describes a 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 Quality of Service, QoS Control List, and Status.
2. Select Combined, Static, Voice VLAN or Conflict.
3. Click the "Refresh" to refresh the page.

The screenshot shows the Lantronix web interface for the SM24TBT4XPA switch. The left sidebar contains a navigation menu with options like System, Port Management, PoE Management, VLAN Management, and QoS. The main content area is titled 'QoS Control List Status' and includes a table of QCEs. The table has columns for User, QCE, Port, Frame Type, Action (Queue Priority, DPL, DSCP, PCP, DEI, Policy), and Conflict. The table shows three entries for Static QCEs.

| User | QCE | Port | Frame Type | Action | Conflict | | | | | |
|--------|-----|-------------|------------|----------------|----------|-----------|---------|---------|---------|----|
| | | | | Queue Priority | DPL | DSCP | PCP | DEI | Policy | |
| Static | 1 | Any | EtherType | 2 | 1 | 16 (CS2) | Default | Default | Default | No |
| Static | 2 | Any | IPv4 | 0 | Default | 18 (AF21) | Default | Default | Default | No |
| Static | 3 | 1,4-6,10-24 | IPv6 | 3 | Default | 18 (AF21) | Default | Default | 1 | No |

Figure 6-8.2: QoS Control List Status

Parameter descriptions:

User : Indicates the QCL user.

QCE : Indicates the index of QCE.

Port : Indicates the list of ports configured with the QCE.

Frame Type: Indicates the type of frame. Possible values are:

Any: Match any frame type.

Ethernet: Match EtherType frames.

LLC: Match (LLC) frames.

SNAP: Match (SNAP) frames.

IPv4: Match IPv4 frames.

IPv6: Match IPv6 frames.

Action: Indicates the classification action taken on ingress frame if parameters configured are matched with the frame's content. Possible actions are:

Queue Priority: Classify Class of Service.

DPL: Classify Drop Precedence Level.

DSCP: Classify DSCP value.

PCP: Classify PCP value.

DEI: Classify DEI value.

Policy: Classify ACL Policy number.

Conflict : Displays Conflict status of QCL entries. As H/W resources are shared by multiple applications, it may happen that resources required to add a QCE may not available, in that case it shows conflict status as 'Yes',

otherwise it is always 'No'. Please note that conflict can be resolved by releasing the H/W resources required to add QCL entry by pressing 'Resolve Conflict' button.

Buttons



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

Refresh: Click to refresh the page immediately.

Combined : Select the QCL status from this drop down list.

Resolve Conflict : Click to release the resources required to add QCL entry in case the conflict status for any QCL entry is 'yes'.

6-9 QoS Statistics

This page provides statistics for the different queues for all switch ports. To display the Queuing Counters in the web UI:

1. Click Quality of Service and QoS Statistics .
2. To automatically refresh the information set “Auto-refresh” to on.
3. Click “Refresh” to refresh the Queuing Counters or clear all information when you click “Clear”.

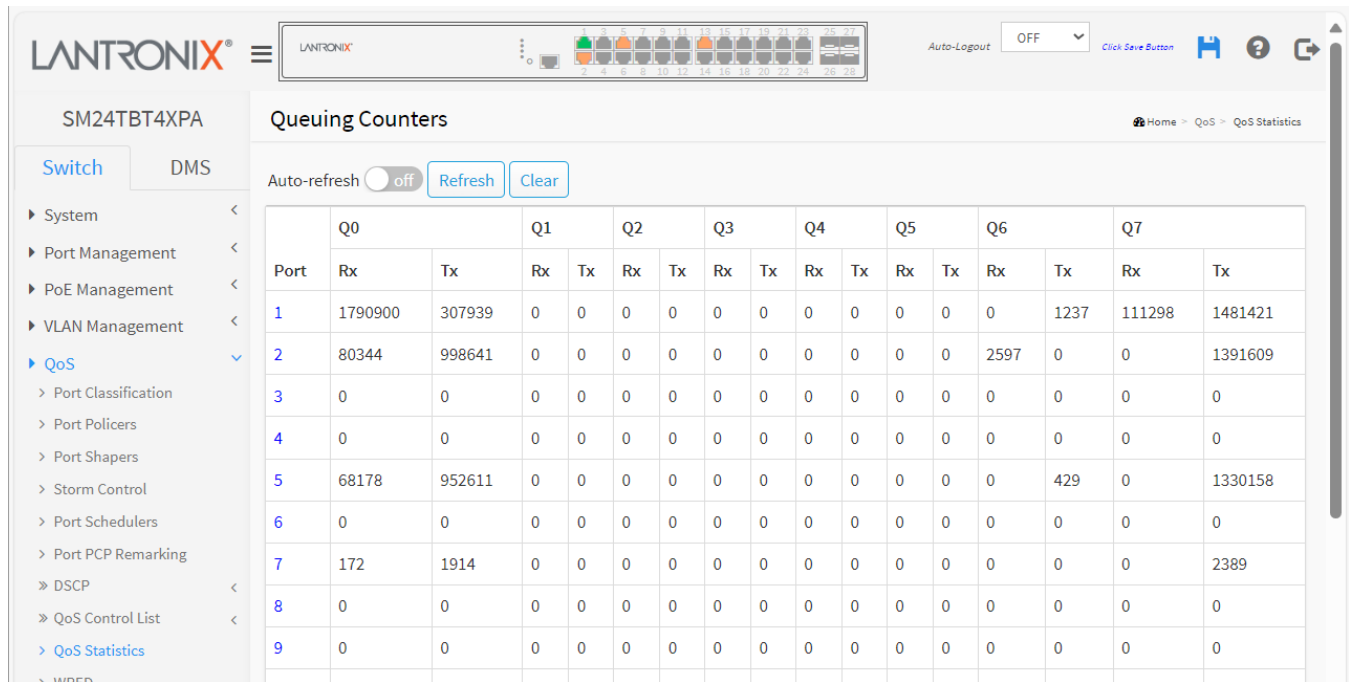


Figure 6-9: Queuing Counters Overview

Parameter descriptions:

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

Qn : Qn is the Queue number, There are 8 QoS queues per port. Q0 is the lowest priority queue.

Rx/Tx : The number of received and transmitted packets per queue.

Buttons

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

Refresh: Click to refresh the page.

Clear: Click to clear the page.

6-10 WRED

This page lets you configure Random Early Detection (RED) settings. Using different RED configurations for the queues it is possible to obtain Weighted Random Early Detection (WRED) operation between queues. The settings are global for all ports in the switch.

To configure Weighted Random Early Detection in the web UI:

1. Click Quality of Service and WRED.
2. Set all parameters and select the Weighted Random Early Detection configuration.
3. Click the Apply button to save the settings.
4. To cancel the settings click the Reset button. It will revert to previously saved values.

| Group | Queue | DPL | Enable | Min | Max | Max Unit |
|-------|-------|-----|--------------------------|-----|-----|------------------|
| 1 | 0 | 1 | <input type="checkbox"/> | 0 | 50 | Drop Probability |
| 1 | 0 | 2 | <input type="checkbox"/> | 1 | 50 | Fill Level |
| 1 | 0 | 3 | <input type="checkbox"/> | 0 | 50 | Fill Level |
| 1 | 1 | 1 | <input type="checkbox"/> | 18 | 50 | Fill Level |
| 1 | 1 | 2 | <input type="checkbox"/> | 30 | 50 | Drop Probability |
| 1 | 1 | 3 | <input type="checkbox"/> | 0 | 50 | Drop Probability |
| 1 | 2 | 1 | <input type="checkbox"/> | 0 | 50 | Fill Level |
| 1 | 2 | 2 | <input type="checkbox"/> | 0 | 50 | Drop Probability |
| 1 | 2 | 3 | <input type="checkbox"/> | 0 | 50 | Fill Level |
| 1 | 3 | 1 | <input type="checkbox"/> | 0 | 50 | Drop Probability |

Figure 6-10: Weighted Random Early Detection Configuration

Parameter descriptions:

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

Group: The WRED group number for which the configuration below applies.

Queue: The queue number (CoS) for which the configuration below applies.

DPL: The Drop Precedence Level for which the configuration below applies.

Enable: Controls whether RED is enabled for this entry.

Min: Controls the lower RED fill level threshold. If the queue filling level is below this threshold, the drop probability is zero. This value is restricted to 0-100%.

Max: Controls the upper RED drop probability or fill level threshold for frames marked with Drop Precedence Level > 0 (yellow frames). This value is restricted to 1-100%.

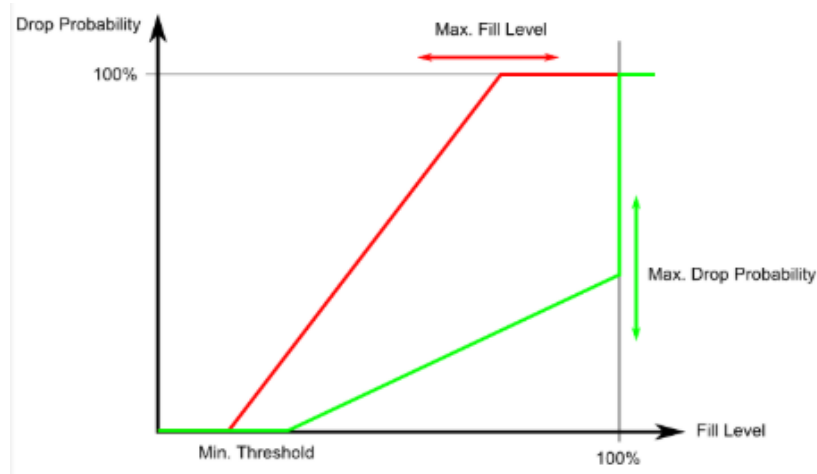
Max Unit: Selects the unit for Max. Possible values are:

Drop Probability: Max controls the drop probability just below 100% fill level.

Fill Level: Max controls the fill level where drop probability reaches 100%.

RED Drop Probability Function

The following illustration shows the drop probability versus fill level function with associated parameters.



Min is the fill level where the queue randomly start dropping frames marked with Drop Precedence Level > 0 (yellow frames). If Max Unit is 'Drop Probability' (the green line), Max controls the drop probability when the fill level is just below 100%. If Max Unit is 'Fill Level' (the red line), Max controls the fill level where drop probability reaches 100%. This configuration makes it possible to reserve a portion of the queue exclusively for frames marked with Drop Precedence Level 0 (green frames). The reserved portion is calculated as $(100 - \text{Max})\%$. Frames marked with Drop Precedence Level 0 (green frames) are never dropped. The drop probability for frames increases linearly from zero (at Min average queue filling level) to Max Drop Probability or Fill Level.

Buttons

Apply: Click to save changes.

Refresh: Click to refresh the page.

7. Spanning tree

The Spanning Tree Protocol (STP) can be used to detect and disable network loops, and to provide backup links between switches, bridges or routers. This allows the switch to interact with other bridging devices (that is, an STP-compliant switch, bridge or router) in your network to ensure that only one route exists between any two stations on the network, and provide backup links which automatically take over when a primary link goes down.

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

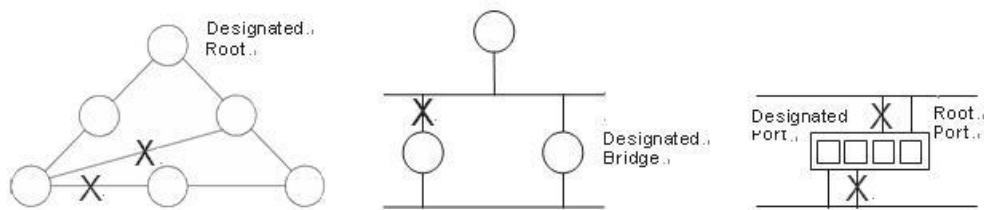


Figure 7: The Spanning Tree Protocol

Once a stable network topology has been established, all bridges listen for Hello BPDUs (Bridge Protocol Data Units) transmitted from the Root Bridge. If a bridge does not get a Hello BPDU after a predefined interval (Maximum Age), the bridge assumes that the link to the Root Bridge is down. This bridge will then initiate negotiations with other bridges to reconfigure the network to reestablish a valid network topology.

7-1 STP Configuration

This section lets you enable or disable the spanning tree protocol, and select the protocol version you want. To configure the Spanning Tree Protocol version in the web UI:

1. Click Spanning Tree and STP Configuration.
2. Select the parameters and enter the desired parameter values in blank fields in Basic Settings.
3. Enable or disable the parameters and enter the desired parameter values in the blank fields in Advanced settings.
4. Click the Apply button to save the settings.
5. To cancel the settings click the Reset button to revert to previously saved values.

LANTRONIX®

SM24TBT4XPA

STP Bridge Configuration

Home > Spanning Tree > STP Configuration

Switch DMS

System <

Port Management <

PoE Management <

VLAN Management <

QoS <

Spanning Tree >

STP Configuration

MSTI Configuration

STP Status

Port Statistics

MAC Address Tables <

Multicast <

DHCP <

Security <

Access Control <

SNMP <

MEP <

ERPS >

EPS >

PercepXion <

PTP <

Event Notification <

Diagnostics <

Maintenance <

Basic Settings

Protocol Version MSTP

Bridge Priority 32768

Hello Time 2

Forward Delay 15

Max Age 20

Maximum Hop Count 20

Transmit Hold Count 6

Advanced Settings

Edge Port BPDU Filtering ☐

Edge Port BPDU Guard ☐

Port Error Recovery ☐

Port Error Recovery Timeout

Root Guard

| Port | Root Guard |
|------|--------------------------|
| * | <input type="checkbox"/> |
| 1 | <input type="checkbox"/> |
| 2 | <input type="checkbox"/> |
| 3 | <input type="checkbox"/> |
| 4 | <input type="checkbox"/> |
| 25 | <input type="checkbox"/> |
| 26 | <input type="checkbox"/> |
| 27 | <input type="checkbox"/> |
| 28 | <input type="checkbox"/> |

Apply Reset

Figure 7-1: STP Configuration

Parameter descriptions:**Basic Settings**

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

Bridge Priority : Controls the bridge priority. Lower numeric values have better priority. The bridge priority plus the MSTI instance number, concatenated with the 6-byte MAC address of the switch forms a Bridge Identifier. For MSTP operation, this is the priority of the CIST. Otherwise, this is the priority of the STP/RSTP Bridge.

Hello Time: The interval between sending STP BPDU's. Valid values are 1 - 10 seconds, default is 2 seconds.

Note: Changing this parameter from the default value is not recommended, and may have adverse effects on your network.

Forward Delay : The delay used by STP Bridges to transit Root and Designated Ports to Forwarding (used in STP compatible mode). Valid values are 4 - 30 seconds.

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

Maximum Hop Count : This defines the initial value of remaining Hops for MSTI information generated at the boundary of an MSTI region. It defines how many bridges a root bridge can distribute its BPDU information to. Valid values are 6 - 40 hops.

Transmit Hold Count : The number of BPDU's a bridge port can send per second. When exceeded, transmission of the next BPDU will be delayed. Valid values are 1 - 10 BPDU's per second.

Advanced Settings

Edge Port BPDU Filtering : Control whether a port explicitly configured as Edge will transmit and receive BPDUs.

Edge Port BPDU Guard : Control whether a port explicitly configured as Edge will disable itself upon reception of a BPDU. The port will enter the error-disabled state, and will be removed from the active topology.

Port Error Recovery : Control whether a port in the error-disabled state automatically will be enabled after a certain time. If recovery is not enabled, ports have to be disabled and re-enabled for normal STP operation. The condition is also cleared by a system reboot.

Port Error Recovery Timeout : The time to pass before a port in the error-disabled state can be enabled. Valid values are 30 seconds - 86400 seconds (24 hours).

Buttons

Apply : Click to save changes.

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

7-2 MSTI Configuration

When you implement a Spanning Tree protocol on the switch that the bridge instance. The CIST is not available for explicit mapping, as it will receive the VLANs not explicitly mapped. Due to the reason that you need to set the list of VLANs mapped to the MSTI. The VLANs must be separated with comma and/or space. A VLAN can only be mapped to one MSTI. An unused MSTI should just be left empty (i.e. not having any VLANs mapped to it.)

This section lets you view and set current STP MSTI bridge instance priority configurations. To configure Spanning Tree MSTI in the web UI:

1. Click Spanning Tree and MSTI Configuration.
2. Specify the configuration parameters in the fields. Specify the VLANs Mapped blank field.
3. Click the Apply button to save the settings.
4. To cancel the settings click the Reset button to revert to previously saved values.
5. Click Edit to configure the STP CIST Port Configuration.

LANTRONIX SM24TBT4XPA

STP MSTI Configuration

Configuration Identification

Configuration Name: 00-c0-f2-a8-a3-bd

Configuration Revision: 0

MSTI Mapping

| Instance | VLANs Mapped | MSTI Priority | MSTI Port |
|----------|---------------------------------------|---------------|-----------|
| CIST | Unmapped VLANs are mapped to the CIST | 32768 | Edit |
| MSTI1 | Example: 2,3-5,11,13,20-40 | 32768 | Edit |
| MSTI2 | Example: 2,3-5,11,13,20-40 | 32768 | Edit |
| MSTI3 | Example: 2,3-5,11,13,20-40 | 32768 | Edit |
| MSTI4 | Example: 2,3-5,11,13,20-40 | 32768 | Edit |
| MSTI5 | Example: 2,3-5,11,13,20-40 | 32768 | Edit |
| MSTI6 | Example: 2,3-5,11,13,20-40 | 32768 | Edit |
| MSTI7 | Example: 2,3-5,11,13,20-40 | 32768 | Edit |

Apply Reset

Figure 7-2: MSTI Configuration

Configuration Identification

Configuration Name : The name identifying the VLAN to MSTI mapping. Bridges must share the name and revision (see below), as well as the VLAN-to-MSTI mapping configuration in order to share spanning trees for MSTI's (Intra-region). The name is at most 32 characters.

Configuration Revision : The revision of the MSTI configuration named above. This must be an integer between 0 and 65535.

MSTI Mapping

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

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

MSTI Priority: Controls the bridge priority. Lower numeric values have better priority. The bridge priority plus the MSTI instance number, concatenated with the 6-byte MAC address of the switch forms a Bridge Identifier.

Buttons

Apply : Click to save changes.

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

MSTI Port: Click [Edit](#) to configure the STP CIST Port Configuration:

LANTRONIX SM24TBT4XPA

STP CIST Port Configuration

Home > Spanning Tree > MSTI Configuration

CIST Aggregated Port Configuration

| Port | STP Enabled | Path Cost | Priority | Admin Edge | Auto Edge | Restricted | TCN | BPDGuard | Point-to-point |
|------|-------------------------------------|-----------|----------|------------|-----------|-------------------------------------|--------------------------|-------------------------------------|----------------|
| - | <input checked="" type="checkbox"/> | Specific | 99 | 128 | Non-Edge | <input checked="" type="checkbox"/> | <input type="checkbox"/> | <input checked="" type="checkbox"/> | Forced True |

CIST Normal Port Configuration

| Port | STP Enabled | Path Cost | Priority | Admin Edge | Auto Edge | Restricted | TCN | BPDGuard | Point-to-point |
|------|-------------------------------------|-----------|----------|------------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|----------------|
| * | <input checked="" type="checkbox"/> | Auto | | | <input checked="" type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | Auto |
| 1 | <input checked="" type="checkbox"/> | Auto | | 128 | Non-Edge | <input checked="" type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | Auto |
| 2 | <input checked="" type="checkbox"/> | Specific | 98 | 128 | Edge | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | Forced True |
| 3 | <input checked="" type="checkbox"/> | Specific | 97 | 128 | Non-Edge | <input checked="" type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | Auto |
| 4 | <input checked="" type="checkbox"/> | Auto | | 128 | Non-Edge | <input checked="" type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | Auto |
| 5 | <input checked="" type="checkbox"/> | Auto | | 128 | Non-Edge | <input checked="" type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | Auto |
| 6 | <input checked="" type="checkbox"/> | Auto | | 128 | Non-Edge | <input checked="" type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | Auto |
| 7 | <input checked="" type="checkbox"/> | Auto | | 128 | Non-Edge | <input checked="" type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | Auto |

Figure 7-2: STP CIST Port Configuration

Parameter descriptions:

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

STP Enabled : Controls whether STP is enabled on this switch port. This field will be read only if Voice VLAN feature is enabled. The Voice VLAN port mode will be read only if this field be Enabled.

Path Cost : Controls the path cost incurred by the port. The Auto setting will set the path cost as appropriate by the physical link speed, using the 802.1D recommended values. Using the Specific setting, a user-defined value can be entered. The path cost is used when establishing the active topology of the network. Lower path

cost ports are chosen as forwarding ports in favor of higher path cost ports. Valid values are 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.

7-3 STP Status

This page provides a status overview of all STP bridge instances. The displayed table contains a row for each STP bridge instance. To display STP Bridges status in the web UI:

1. Click Spanning Tree and STP Status.
2. To auto-refresh the information click “Auto-refresh”.
3. Click “Refresh” to refresh the webpage.
4. Click “CIST” to go to the next page “STP Detailed Bridge Status”.

STP Status

Auto-refresh ☐ off [Refresh](#)

| MSTI | Bridge ID | Root | | | Topology Flag | Topology Change Last |
|------|-------------------------|-------------------------|------|-------|---------------|----------------------|
| | | ID | Port | Cost | | |
| CIST | 32768.00-C0-F2-A8-A3-BD | 32768.00-C0-F2-56-1A-D8 | 1 | 20000 | Steady | 0d 19:15:42 |

STP Port Status

| Port | CIST Role | CIST State | Uptime |
|-------|----------------|------------|-------------|
| 1 | RootPort | Forwarding | 0d 21:43:55 |
| 2 | Port of LLAG2 | Forwarding | - |
| 3 | Disabled | Discarding | - |
| 4 | Disabled | Discarding | - |
| 5 | Port of LLAG3 | Forwarding | - |
| 6 | Disabled | Discarding | - |
| 7 | Disabled | Discarding | - |
| 8 | Disabled | Discarding | - |
| 26 | Disabled | Discarding | - |
| 27 | Disabled | Discarding | - |
| 28 | Disabled | Discarding | - |
| LLAG2 | DesignatedPort | Forwarding | 0d 20:44:33 |
| LLAG3 | DesignatedPort | Forwarding | 0d 20:44:33 |

Figure 7-3: STP Status

Parameter descriptions:

MSTI : The Bridge Instance. This is also a link to the STP Detailed Bridge Status.

Bridge ID : The Bridge ID of this Bridge instance.

Root ID : The Bridge ID of the currently elected root bridge.

Root Port : The switch port currently assigned the root port role.

Root Cost : Root Path Cost. For the Root Bridge it is zero. For all other Bridges, it is the sum of the Port Path Costs on the least cost path to the Root Bridge.

Topology Flag : The current state of the Topology Change Flag of this Bridge instance.

Topology Change Last : The time since last Topology Change occurred.

STP Port Status

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

CIST Role : The current STP port role of the CIST port. The port role can be one of the following values: AlternatePort, Backup Port, RootPort, DesignatedPort Disabled.

CIST State : The current STP port state of the CIST port. The port state can be one of the following values: Blocking, Learning, or Forwarding.

Uptime : The time since the bridge port was last initialized.

CIST : Click to next page "STP Detailed Bridge Status".

STP Bridge Status

Bridge Instance: The Bridge instance -CIST,MST1, ...

Bridge ID: The Bridge ID of this Bridge instance.

Root ID: The Bridge ID of the currently elected root bridge.

Root Port: The switch port currently assigned the root port role.

Root Cost: Root Path Cost. For the Root Bridge this is zero. For all other Bridges, it is the sum of the Port Path Costs on the least cost path to the Root Bridge.

Regional Root: The Bridge ID of the currently elected regional root bridge, inside the MSTP region of this bridge.*(For the CIST instance only).*

Internal Root Cost: The Regional Root Path Cost. For the Regional Root Bridge this is zero. For all other CIST instances in the same MSTP region, it is the sum of the Internal Port Path Costs on the least cost path to the Internal Root Bridge.*(For the CIST instance only).*

Topology Flag: The current state of the Topology Change Flag of this Bridge instance.

Topology Change Count: The number of times where the topology change flag has been set (during a one-second interval).

Topology Change Last: The time passed since the Topology Flag was last set.

CIST Ports & Aggregations State

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

Port ID: The port id as used by the STP protocol. This is the priority part and the logical port index of the bridge port.

Role: The current STP port role. The port role can be one of the following **values:** AlternatePort, BackupPort, 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 Autosetting, or any explicitly configured value.

Edge: The current STP port (operational) Edge Flag. An Edge Port is a switch port to which no Bridges are attached. The flag may be automatically computed or explicitly configured. Each Edge Port transits directly to the Forwarding Port State, since there is no possibility of it participating in a loop.

Point-to-Point: The current STP port point-to-point flag. A point-to-point port connects to a non-shared LAN media. The flag may be automatically computed or explicitly configured. The point-to-point properties of a port affect how fast it can transit to STP state.






Uptime: The time since the bridge port was last initialized.

Buttons

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

Refresh : Click to manually refresh the page immediately.

STP Detailed Bridge Status:

LANTRONIX®   Auto-Logout OFF [Click Save Button](#)   

SM24TBT4XPA

STP Detailed Bridge Status [Home](#) > [Spanning Tree](#) > [STP Status](#)

Auto-refresh ☐ off [Refresh](#)

STP Bridge Status

| | |
|-----------------------|-------------------------|
| Bridge Instance | CIST |
| Bridge ID | 32768.00-C0-F2-A8-A3-BD |
| Root ID | 32768.00-C0-F2-56-1A-D8 |
| Root Cost | 20000 |
| Root Port | 1 |
| Regional Root | 32768.00-C0-F2-A8-A3-BD |
| Internal Root Cost | 0 |
| Topology Flag | Steady |
| Topology Change Count | 21 |
| Topology Change Last | 0d 19:21:14 |

CIST Ports & Aggregations State

| Port | Port ID | Role | State | Path Cost | Edge | Point-to-Point | Uptime |
|-------|---------|----------------|------------|-----------|------|----------------|-------------|
| 1 | 128:001 | RootPort | Forwarding | 20000 | No | Yes | 0d 21:49:27 |
| 2 | - | Part of LLAG2 | Forwarding | | | | |
| 5 | - | Part of LLAG3 | Forwarding | | | | |
| 13 | 128:00d | DesignatedPort | Forwarding | 200000 | Yes | Yes | 0d 19:21:04 |
| LLAG2 | 128:01e | DesignatedPort | Forwarding | 99 | Yes | Yes | 0d 20:50:05 |
| LLAG3 | 128:01f | DesignatedPort | Forwarding | 99 | Yes | Yes | 0d 20:50:05 |

Switch **DMS**

- System
- Port Management
- PoE Management
- VLAN Management
- QoS
- Spanning Tree**
 - STP Configuration
 - MSTI Configuration
 - STP Status**
 - Port Statistics
- MAC Address Tables
- Multicast
- DHCP
- Security
- Access Control
- SNMP
- MEP
- ERPS
- EPS
- Percepixon
- PTP
- Event Notification
- Diagnostics
- Maintenance

7-4 Port Statistics

This page displays the STP port statistics counters of bridge ports in the switch. To display the STP Port Statistic in the web UI:

1. Click Spanning Tree and Port Statistics.
2. To auto-refresh the page click “Auto-refresh”.
3. Click “Refresh” to refresh the webpage.

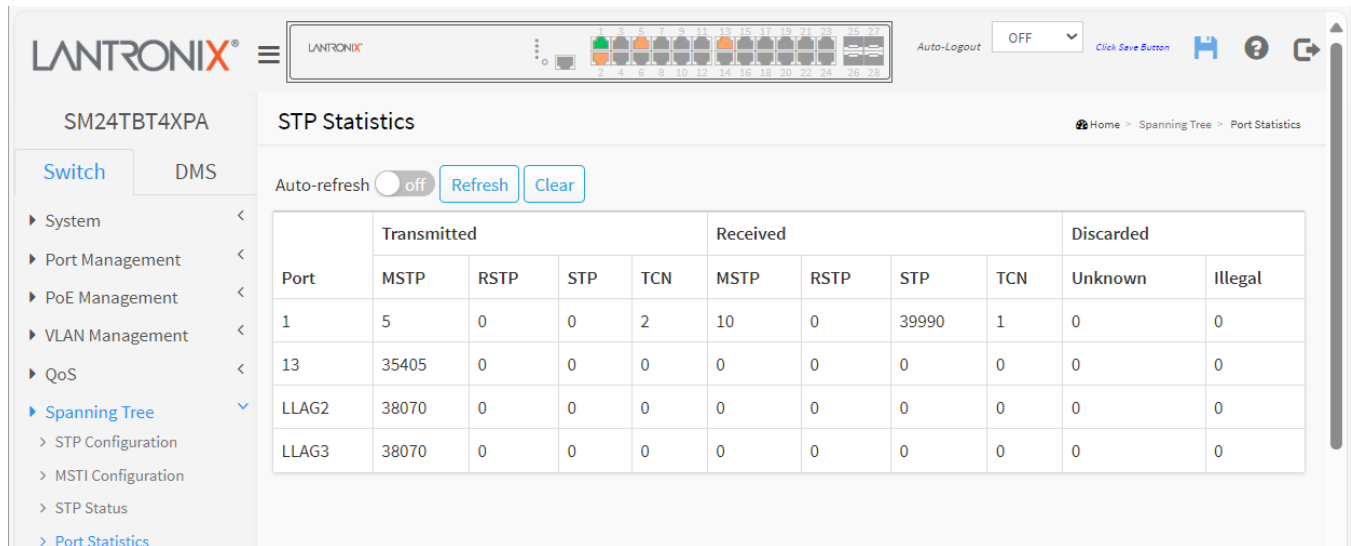


Figure 7-4: STP Port Statistics

Parameter descriptions:

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

MSTP: The number of MSTP Configuration BPDU's received/transmitted on the port.

RSTP: The number of RSTP Configuration BPDU's received/transmitted on the port.

STP : The number of legacy STP Configuration BPDU's received/transmitted on the port.

TCN : The number of (legacy) Topology Change Notification BPDU's received/transmitted on the port.

Discarded Unknown : The number of unknown Spanning Tree BPDU's received (and discarded) on the port.

Discarded Illegal : The number of illegal Spanning Tree BPDU's received (and discarded) on the port.

Buttons

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

Refresh: Click to refresh the page immediately.

8. MAC Address Table

8-1 Configuration

Switching of frames is based on the DMAC address contained in the frame. The switch builds up a table that maps MAC addresses to switch ports for knowing which ports the frames should go to (based upon the DMAC address in the frame). This table contains both static and dynamic entries. The static entries are configured by the network administrator if the administrator wants to do a fixed mapping between the DMAC address and switch ports.

The frames also contain a MAC address (SMAC address), which shows the MAC address of the equipment sending the frame. The SMAC address is used by the switch to automatically update the MAC table with these dynamic MAC addresses. Dynamic entries are removed from the MAC table if no frame with the corresponding SMAC address have been seen after a configurable age time.

To configure MAC Address Table parameters in the web UI:

1. Click MAC Address Tables and Configuration.
2. Specify the Disable Automatic Aging and Aging Time.
3. Specify the Port Members (Auto, Disable, Secure).
4. Specify the Learning-disabled VLANs.
5. Click Add New Static Entry and specify the VLAN IP, Mac address, and Port Members..
6. Click Apply.

LANTRONIX SM24TBT4XPA MAC Address Table Configuration

Auto-Logout: OFF [Click Save Button](#) [?](#) [G](#)

Home > MAC Address Tables > Configuration

Aging Configuration

Disable Automatic Aging: ☐

Aging Time: 300 seconds

MAC Table Learning

| | Port Members | | | | | | | | | | | | | | | | | | | | | | | | | | | |
|---------|----------------------------------|----------------------------------|----------------------------------|----------------------------------|----------------------------------|----------------------------------|----------------------------------|----------------------------------|----------------------------------|----------------------------------|----------------------------------|----------------------------------|----------------------------------|----------------------------------|----------------------------------|----------------------------------|----------------------------------|----------------------------------|----------------------------------|----------------------------------|----------------------------------|----------------------------------|----------------------------------|----------------------------------|----------------------------------|----------------------------------|----------------------------------|----------------------------------|
| | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 | 19 | 20 | 21 | 22 | 23 | 24 | 25 | 26 | 27 | 28 |
| Auto | <input checked="" type="radio"/> | <input checked="" type="radio"/> | <input checked="" type="radio"/> | <input checked="" type="radio"/> | <input checked="" type="radio"/> | <input checked="" type="radio"/> | <input checked="" type="radio"/> | <input checked="" type="radio"/> | <input checked="" type="radio"/> | <input checked="" type="radio"/> | <input checked="" type="radio"/> | <input checked="" type="radio"/> | <input checked="" type="radio"/> | <input checked="" type="radio"/> | <input checked="" type="radio"/> | <input checked="" type="radio"/> | <input checked="" type="radio"/> | <input checked="" type="radio"/> | <input checked="" type="radio"/> | <input checked="" type="radio"/> | <input checked="" type="radio"/> | <input checked="" type="radio"/> | <input checked="" type="radio"/> | <input checked="" type="radio"/> | <input checked="" type="radio"/> | <input checked="" type="radio"/> | <input checked="" type="radio"/> | <input checked="" type="radio"/> |
| Disable | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> |
| Secure | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> |

VLAN Learning Configuration

Learning-disabled VLANs:

Static MAC Table Configuration

| | | | Port Members | | | | | | | | | | | | | | | | | | | | | | | | | | | |
|---------------------------------------|---------|-------------------|--------------------------|--------------------------|--------------------------|--------------------------|--------------------------|--------------------------|--------------------------|--------------------------|--------------------------|--------------------------|--------------------------|--------------------------|--------------------------|--------------------------|--------------------------|--------------------------|--------------------------|--------------------------|--------------------------|--------------------------|--------------------------|--------------------------|--------------------------|--------------------------|--------------------------|--------------------------|--------------------------|----|
| Delete | VLAN ID | MAC Address | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 | 19 | 20 | 21 | 22 | 23 | 24 | 25 | 26 | 27 | 28 |
| <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"/> | <input type="checkbox"/> | <input type="checkbox"/> | |

[Add New Static Entry](#)

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

Parameter descriptions:

Aging Configuration: By default, dynamic entries are removed from the MAC table after 300 seconds. This removal is also called 'aging'. Configure aging time by entering a value here in seconds; for example, Age time seconds. The allowed range is 10 to 1000000 seconds.

Disable: the automatic aging of dynamic entries by checking Disable automatic aging.

MAC Table Learning: If the learning mode for a given port is greyed out, another module is in control of the mode, so that it cannot be changed by the user. An example of such a module is the MAC-Based Authentication under 802.1X. Each port can do learning based 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.

VLAN Learning Configuration

Learning-disabled VLANs: This field shows the Learning-disabled VLANs. When a NEW MAC arrives into a learning-disabled VLAN, the MAC won't be learnt. By the default, the field is empty. More VLANs may be created by using a list syntax where the individual elements are separated by commas. Ranges are specified with a dash separating the lower and upper bound. The following example will create VLANs 1, 10, 11, 12, 13, 200, and 300: **1,10-13,200,300**. Spaces are allowed in between the delimiters.

Static MAC Table Configuration: The static entries in the MAC table are shown in this table. The static MAC table can contain 128 entries. The maximum is 128 entries per switch.

VLANID : The VLAN ID of the entry.

MAC Address : The MAC address of the entry.

Port Members : Checkmarks indicate which ports are members of the entry. Check or uncheck as needed to modify the entry.

Buttons

Add New Static Entry : Click to add a new entry to the static MAC table. Specify the VLAN ID, MAC address, and port members for the new entry. Click "Apply".

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

Apply: Click to save changes.

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

Messages:

At least one MAC address is invalid. The format is 'xx-xx-xx-xx-xx-xx' or 'xx.xx.xx.xx.xx.xx' or 'xxxxxxxxxxxx' (x is a hexadecimal digit).

Error: mac address:00-00-00-00-00-00 is not multicast mac address, support only one port.

9. Multicast

9-1 IGMP Snooping

This function is used to establish multicast groups to forward multicast packets to the member ports in order to avoid wasting 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 a multicast packet from a broadcast packet, so it can only treat them all as a broadcast packet. Without IGMP Snooping, the multicast packet forwarding function is no different than for broadcast packet forwarding.

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.

9-1.1 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 must be running IGMP.

To configure the IGMP Snooping parameters in the web UI:

1. Click Multicast, IGMP Snooping, and Basic Configuration.
2. Enable or disable Global configuration
3. Set the ports to become a Router Port or enable/ disable the Fast Leave function.
4. Set the Throttling and Profile parameters.
5. Click the Apply button to save the settings.
6. To cancel the settings click the Reset button to revert to previously saved values.

Global Configuration

| | |
|--------------------------------------|-------------------------------------|
| Snooping Enabled | <input checked="" type="checkbox"/> |
| Unregistered IPMCv4 Flooding Enabled | <input checked="" type="checkbox"/> |
| IGMP SSM Range | 232.0.0.0 / 8 |
| Leave Proxy Enabled | <input checked="" type="checkbox"/> |
| Proxy Enabled | <input checked="" type="checkbox"/> |

Port Related Configuration

| Port | Router Port | Fast Leave | Throttling | Filtering Profile |
|------|-------------------------------------|-------------------------------------|------------|-------------------|
| * | <input type="checkbox"/> | <input type="checkbox"/> | < > | < > |
| 1 | <input type="checkbox"/> | <input type="checkbox"/> | unlimited | - Preview |
| 2 | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | 5 | - Preview |
| 3 | <input type="checkbox"/> | <input type="checkbox"/> | unlimited | - Preview |
| 4 | <input checked="" type="checkbox"/> | <input type="checkbox"/> | 10 | - Preview |
| 5 | <input type="checkbox"/> | <input type="checkbox"/> | unlimited | - Preview |
| 6 | <input type="checkbox"/> | <input type="checkbox"/> | unlimited | - Preview |
| 7 | <input type="checkbox"/> | <input type="checkbox"/> | unlimited | - Preview |

Figure 9-1.1: IGMP Snooping Basic Configuration

Parameter descriptions:**Global Configuration**

Snooping Enabled: Enable the Global IGMP Snooping.

Unregistered IPMCv4 Flooding enabled : Enable unregistered IPMCv4 traffic flooding. Unregistered IPMCv4 traffic is so-called unknown multicast. After selected, the unregistered multicast stream will be forwarded like normal packets. Once you un-selected it, such stream will be discarded.

IGMP SSM Range : SSM (Source-Specific Multicast) Range allows the SSM-aware hosts and routers run the SSM service model for the groups in the address range. Format: (IP address/ sub mask)

Leave Proxy Enabled: Enable IGMP Leave Proxy. This feature can be used to avoid forwarding unnecessary leave messages to the router side.

Proxy Enabled : Enable IGMP Proxy. This feature can be used to avoid forwarding unnecessary join and leave messages to the router side.

Port Related Configuration

Port : It shows the physical Port index of switch.

Router Port : Specify which ports act as router ports. A router port is a port on the Ethernet switch that leads towards the Layer 3 multicast device or IGMP querier. If an aggregation member port is selected as a router port, the whole aggregation will act as a router port.

Fast Leave: Enable the fast leave on the port.

Throttling : Enable to limit the number of multicast groups to which a switch port can belong.

Profile: Select the profile for this port. Click to preview the page which list the rules associated with the selected

profile.

Buttons

Apply: Click to save changes.

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

9-1.2 VLAN Configuration

Each page shows 20 entries from the VLAN table. When first visited, the web page will show the first 20 entries from the beginning of the VLAN Table. Clicking the Refresh button will update the displayed table starting from that or the next closest VLAN Table match.

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

To configure IGMP Snooping VLAN in the web UI:

1. Click Multicast, IGMP Snooping, and VLAN Configuration.
2. Configure the parameters and click the Apply to save the setting
3. To cancel the settings click the Reset button to revert to previously saved values.
4. To add a VLAN, click System, IP Address, Advanced Settings, and click the Add Interface button.

| VLAN ID | Snooping Enabled | Querier Election | Querier Address | Compatibility | PRI | RV | QI (sec) | QRI (0.1 sec) | LLQI (0.1 sec) | URI (sec) |
|---------|-------------------------------------|-------------------------------------|-----------------|---------------|-----|----|----------|---------------|----------------|-----------|
| 1 | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | 0.0.0.0 | IGMP-Auto | 2 | 2 | 125 | 100 | 10 | 2 |

Figure 9-1.2: IGMP Snooping VLAN Configuration

Parameter descriptions:

VLAN ID: The VLAN ID of the entry

IGMP Snooping Enabled: Enable the per VLAN IGMP Snooping. Up to 64 VLANs can be selected for IGMP Snooping.

Querier Election: Enable to join IGMP Querier election in the VLAN. Disable to act as an IGMP Non Querier

Querier Address: Define the IPv4 address as source address used in IP header for IGMP Querier election. When the Querier address is not set, system uses the 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 0.0.0.0.

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.

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

QI(sec): Query Interval. The QI is the interval between General Queries sent by the Querier. The allowed range is 1 to 31744 seconds; the default QI is 125 seconds.

QRI(0.1 sec): Query Response Interval. 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 (0.1 sec) : 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(sec): Unsolicited Report Interval. The Unsolicited Report Interval is the time between repetitions of a host's initial report of membership in a group. The allowed range is 0 to 31744 seconds; the default URI is 1 second.

Buttons

Apply: Click to save changes.

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

Refresh: Refreshes the displayed table starting from the "VLAN" input fields.

First Page : Updates the table starting from the first entry in the VLAN Table (i.e., the entry with the lowest VLAN ID).

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

9-1.3 Status

This page displays the IGMP Snooping Status details. To display IGMP Snooping status in the web UI:

1. Click Multicast, IGMP Snooping, and Status.
2. To auto-refresh the information click "Auto-refresh" or click "Refresh" to refresh the page.

The screenshot shows the Lantronix web interface for the SM24TBT4XPA device. The left sidebar contains a navigation menu with categories like System, Port Management, PoE Management, VLAN Management, QoS, Spanning Tree, MAC Address Tables, Multicast, and MLD Snooping. The 'Multicast' section is expanded, showing 'IGMP Snooping' and 'Status'. The main content area is titled 'IGMP Snooping Status' and includes an 'Auto-refresh' toggle (set to 'off') and 'Refresh' and 'Clear' buttons. Below these are two tables: 'Statistics' and 'Router Port'.

| VLAN ID | Querier Version | Host Version | Querier Status | Queries Transmitted | Queries Received | V1 Reports Received | V2 Reports Received | V3 Reports Received | V2 Leaves Received |
|---------|-----------------|--------------|----------------|---------------------|------------------|---------------------|---------------------|---------------------|--------------------|
| 1 | v3 | v1 | ACTIVE | 2 | 0 | 8 | 18 | 48 | 0 |

| Port | Status |
|------|--------|
| 1 | - |
| 2 | Static |
| 3 | - |
| 4 | Static |
| 5 | - |

Figure 9-1.3: IGMP Snooping Status

Parameter descriptions:

Statistics

VLAN ID: The VLAN ID of the entry.

Querier Version : Working Querier Version currently.

Host Version : Working Host Version currently.

Querier Status : Shows the Querier status is "ACTIVE" or "IDLE". The status "DISABLE " denotes the specific interface is administratively disabled.

Queries Transmitted : The number of Transmitted Queries.

Queries Received : The number of Received Queries.

V1 Reports Received : The number of Received V1 Reports.

V2 Reports Received : The number of Received V2 Reports.

V3 Reports Received : The number of Received V3 Reports.

V2 Leaves Received : The number of Received V2 Leaves.

Router Port: Displays which ports act as router ports. A router port is a port on the Ethernet switch that leads towards the Layer 3 multicast device or IGMP querier. Static denotes the specific port is configured to be a router port. Dynamic denotes the specific port is learnt to be a router port. Both denote the specific port is configured or learnt to be a router port.

Port: Switch port number.

Status: Indicate whether specific port is a router port or not.

Buttons

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

Refresh: Click to refresh the page immediately.

9-1.4 Group Information

This page displays the IGMP Snooping Group Information table entries. The IGMP Group Table is sorted first by VLAN ID, and then by group. This will use the last entry of the currently displayed table as a basis for the next lookup. When the end is reached the text "*No more entries*" is shown in the displayed table.

To display IGMP Snooping Group Information in the web UI:

1. Click Multicast, IGMP Snooping, and Group Information.
2. Specify how many entries to show in one page.
3. To auto-refresh the information click "Auto-refresh".
4. Click "Refresh" to refresh the webpage.
5. Click First Page or Next Page to change pages.

The screenshot shows the Lantronix web interface for the SM24TBT4XPA device. The left sidebar contains a navigation menu with options: Switch, DMS, System, Port Management, PoE Management, VLAN Management, QoS, Spanning Tree, MAC Address Tables, Multicast, and IGMP Snooping. The main content area is titled "IGMP Snooping Group Information". It features a control bar with an "Auto-refresh" toggle set to "off", and buttons for "Refresh", "First Page", and "Next Page". Below this, a filter section shows "Start from VLAN 1 and group address 224.0.0.0, 20 entries per page." The main table has columns for "VLAN ID", "Groups", and "Port Members" (ports 1 through 28). The table displays three entries for VLAN 1, each with a group address and a green checkmark in the Port Members column.

| VLAN ID | Groups | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 | 19 | 20 | 21 | 22 | 23 | 24 | 25 | 26 | 27 | 28 |
|---------|-----------------|---|---|---|---|---|---|---|---|---|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|
| 1 | 224.0.1.60 | ✓ | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 1 | 239.255.102.18 | ✓ | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 1 | 239.255.255.250 | ✓ | | | | | | | | | | | | | | | | | | | | | | | | | | | |

Figure 9-1.4: IGMP Snooping Groups Information

Parameter descriptions:

Show entries: You can choose how many items you want to display.

VLAN ID : The VLAN ID of the group.

Groups : The Group address of the group displayed.

Port Members : Ports under this group.

Buttons

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

Refresh: Click to refresh the page immediately.

First Page: Updates the table, starting with the first entry in the table.

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

9-1.5 IGMP SFM Information

Entries in the IGMP SFM Information Table are shown on this page. The IGMP SFM (Source-Filtered Multicast) Information Table also contains the SSM (Source-Specific Multicast) information. This table is sorted first by VLAN ID, then by group, and then by Port. Different source addresses belong to the same group are treated as single entry.

Each page shows up to 99 entries from the IGMP SFM Information table, default = 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 allow the user to 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. The Next Page will use the last entry of the currently displayed table as a basis for the next lookup. When the end is reached the text "No more entries" is shown in the displayed table.

To display IGMP SFM Information in the web UI:

1. Click Multicast, IGMP Snooping, and IGMP SFM Information
2. To auto-refresh the information click "Auto-refresh".
3. Click "Refresh" to refresh the webpage.
4. Click First/Next Page to change page.

The screenshot shows the Lantronix web interface for the SM24TBT4XPA device. The left sidebar contains a navigation menu with options like System, Port Management, PoE Management, VLAN Management, QoS, and Spanning Tree. The main content area is titled "IGMP SFM Information". It features an "Auto-refresh" toggle set to "off", and buttons for "Refresh", "First Page", and "Next Page". Below these are input fields for "Start from VLAN" (set to 1) and "and group address" (set to 224.0.0.0), followed by a dropdown for "entries per page" (set to 20). A table displays the following data:

| VLAN ID | Group | Port | Mode | Source Address | Type | Hardware Filter/Switch |
|---------|-----------------|------|---------|----------------|------|------------------------|
| 1 | 224.0.1.60 | 1 | Exclude | None | Deny | Yes |
| 1 | 239.255.102.18 | 1 | Exclude | None | Deny | Yes |
| 1 | 239.255.255.250 | 1 | Exclude | None | Deny | Yes |

Figure 9-1.5: IGMP SFM Information

Parameter descriptions:

Show entries: You can choose how many items you want to show per page.

VLAN ID : The VLAN ID of the group.

Group : The Group address of the group displayed.

Port : Switch port number.

Mode : Indicates the filtering mode maintained per (VLAN ID, port number, Group Address) basis. It can be either Include or Exclude.

Source Address : IP Address of the source. Currently, system limits the total number of IP source addresses for filtering to be 128.

Type : Indicates the Type. It can be either Allow or Deny.

Hardware Filter/Switch: Indicates whether data plane destined to the specific group address from the source IPv4 address could be handled by the chip.

Buttons

Auto refresh : Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.

Refresh : Click to refresh the page immediately.

First Page: Updates the table starting from the first entry in the IGMP SFM Information Table.

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

9-2 MLD Snooping

Curiously enough, a network node that acts as a source of IPv6 multicast traffic is only an indirect participant in MLD snooping—it just provides multicast traffic, and MLD doesn't interact with it. (Note, however, that in an application like desktop conferencing a network node may act as both a source and an MLD host; but MLD interacts with that node only in its role as an MLD host.)

A source node creates multicast traffic by sending packets to a multicast address. In IPv6, addresses with the first eight bits set (that is, "FF" as the first two characters of the address) are multicast addresses, and any node that listens to such an address will receive the traffic sent to that address. Application software running on the source and destination systems cooperates to determine what multicast address to use. (Note that this is a function of the application software, not of MLD.)

When MLD snooping is enabled on a VLAN, the switch acts to minimize unnecessary multicast traffic. If the switch receives multicast traffic destined for a given multicast address, it forwards that traffic only to ports on the VLAN that have MLD hosts for that address. It drops that traffic for ports on the VLAN that have no MLD hosts.

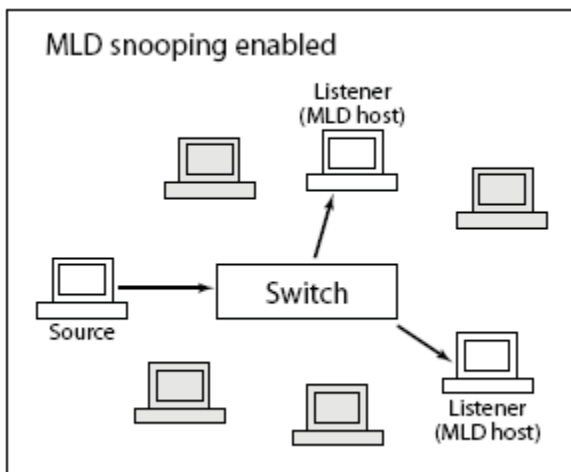


Figure 9-2: MLD Snooping Enabled

9-2.1 Basic Configuration

Here you can configure MLD Snooping basic parameters. To configure MLD Snooping in the web UI:

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

Global Configuration

| | |
|--------------------------------------|-------------------------------------|
| Snooping Enabled | <input checked="" type="checkbox"/> |
| Unregistered IPMCv6 Flooding Enabled | <input checked="" type="checkbox"/> |
| MLD SSM Range | ff3e:: / 96 |
| Leave Proxy Enabled | <input checked="" type="checkbox"/> |
| Proxy Enabled | <input checked="" type="checkbox"/> |

Port Related Configuration

| Port | Router Port | Fast Leave | Throttling | Filtering Profile |
|------|-------------------------------------|-------------------------------------|------------|-------------------|
| * | <input type="checkbox"/> | <input type="checkbox"/> | < > | < > |
| 1 | <input type="checkbox"/> | <input type="checkbox"/> | unlimited | - > Preview |
| 2 | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | 3 | - > Preview |
| 3 | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | 6 | - > Preview |
| 4 | <input type="checkbox"/> | <input type="checkbox"/> | unlimited | - > Preview |
| 5 | <input checked="" type="checkbox"/> | <input type="checkbox"/> | unlimited | - > Preview |
| 6 | <input type="checkbox"/> | <input type="checkbox"/> | unlimited | - > Preview |
| 7 | <input type="checkbox"/> | <input type="checkbox"/> | unlimited | - > Preview |

Figure 9-2.1: MLD Snooping Basic Configuration

Parameter descriptions:**Global Configuration**

Snooping Enabled : Enable the Global MLD Snooping.

Unregistered IPMCv6 Flooding enabled : Enable unregistered IPMCv6 traffic flooding. 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.

Port Related Configuration

Router Port : Specify which ports act as router ports. A router port is a port on the Ethernet switch that leads towards the Layer 3 multicast device or MLD querier. If an aggregation member port is selected as a router port, the whole aggregation will act as a router port.

Fast Leave: Enable fast leave on the port.

Throttling : Enable to limit the number of multicast groups to which a switch port can belong.

Filtering Profile : You can select a profile when you edit in Multicast Filtering Profile.

Buttons

Apply: Click to save changes.

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

9-2.2 VLAN Configuration

When MLD snooping is enabled on a VLAN, the switch acts to minimize unnecessary multicast traffic. If the switch receives multicast traffic destined for a given multicast address, it forwards that traffic only to ports on the VLAN that have MLD hosts for that address. It drops that traffic for ports on the VLAN that have no MLD hosts.

The 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.

To configure MLD Snooping VLAN in the web UI:

1. Click Multicast, MLD Snooping, and VLAN Configuration.
2. Click Add New MLD VLAN.
3. Specify the VLAN ID entries per page.

| VLAN ID | Snooping Enabled | Querier Election | Compatibility | PRI | RV | QI (sec) | QRI (0.1 sec) | LLQI (0.1 sec) | URI (sec) |
|---------|-------------------------------------|-------------------------------------|---------------|-----|----|----------|---------------|----------------|-----------|
| 1 | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | Forced MLDv2 | 2 | 2 | 125 | 100 | 10 | 1 |

Figure 9-2.2: MLD Snooping VLAN Configuration

Parameter descriptions:

VLAN ID: The VLAN ID of the entry.

MLD Snooping Enabled: Displays the VLAN ID of the entry.

Snooping Enabled : Enable per-VLAN MLD Snooping. Up to 64 VLANs can be selected for MLD Snooping.

Querier Election: Enable to join MLD Querier election in the VLAN. Disable to act as a MLD Non-Querier.

Compatibility : Compatibility is maintained by hosts and routers taking appropriate actions depending on the versions of IGMP operating on hosts and routers within a network. The allowed selections are: IGMP-Auto, Forced IGMPv1, and Forced IGMPv2. The default compatibility value is IGMP-Auto.

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

QI(sec): Query Interval. The QI is the interval between General Queries sent by the Querier. The allowed range is 1 to 31744 seconds; the default QI is 125 seconds.

QRI(0.1sec):

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 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; default LLQI is 10 in tenths of a second (1 second).

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

Buttons

Apply: Click to save changes.

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

Refresh: Refreshes the displayed table starting from the "VLAN" input fields.

First Page : Updates the table starting from the first entry in the VLAN Table, i.e. the entry with the lowest VLAN ID.

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

9-2.3 Status

This page lets you set MLD Snooping and view MLD Snooping Status and detail information. To display MLD Snooping Status in the web UI:

1. Click Multicast, MLD Snooping and Status.
2. If you want to auto-refresh the information then you need to evoke the "Auto-refresh"
3. Click "Refresh" to refresh an entry of the MLD Snooping Status Information.
- 4.

The screenshot shows the Lantronix web interface for the SM24TBT4XPA device. The left sidebar contains a navigation menu with options like System, Port Management, PoE Management, VLAN Management, QoS, Spanning Tree, MAC Address Tables, Multicast, IGMP Snooping, MLD Snooping, Basic Configuration, VLAN Configuration, Status, and Groups Information. The main content area is titled 'MLD Snooping Status' and includes an 'Auto-refresh' toggle (currently off) and 'Refresh' and 'Clear' buttons. Below these are two tables: 'Statistics' and 'Router Port'.

| VLAN ID | Querier Version | Host Version | Querier Status | Queries Transmitted | Queries Received | V1 Reports Received | V2 Reports Received | V1 Leaves Received |
|---------|-----------------|--------------|----------------|---------------------|------------------|---------------------|---------------------|--------------------|
| 1 | v2 | v2 | DISABLE | 0 | 0 | 0 | 0 | 0 |

| Port | Status |
|------|--------|
| 1 | - |
| 2 | - |
| 3 | - |
| 4 | - |
| 5 | - |

Figure 9-2.3: MLD Snooping Status

Parameter descriptions:

VLAN ID: The VLANID of the entry.

Querier Version : Working Querier Version currently.

Host Version : Working Host Version currently.

Querier Status : Show the Querier status is "ACTIVE" or "IDLE". The status "DISABLE" denotes the specific interface is administratively disabled.

Queries Transmitted : The number of Transmitted Queries.

Queries Received : The number of Received Queries.

V1 Reports Received : The number of Received V1 Reports.

V2 Reports Received : The number of Received V2 Reports.

V1 Leaves Received : The number of Received V1 Leaves.

Router Port: Displays which ports act as router ports. A router port is a port on the Ethernet switch that leads towards the Layer 3 multicast device or MLD querier.

Static denotes the specific port is configured to be a router port.

Dynamic denotes the specific port is learnt to be a router port.

Both denote the specific port is configured or learnt to be a router port.

Port: The switch port number.

Status: Indicate whether specific port is a router port or not.

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.

9-2.4 Groups Information

Entries in the MLD Group Table are shown on this page. The MLD Group Table is sorted first by VLAN ID, and then by group.

Each page shows up to 99 entries from the MLD Group table, default being 20, selected through the "entries per page" input field. When first visited, the web page will show the first 20 entries from the beginning of the MLD Group Table.

The "Start from VLAN", and "group" input fields allow the user to select the starting point in the MLD Group Table. Clicking the Refresh button will update the displayed table starting from that or the closest next MLD Group Table match. In addition, the two input fields will - upon a Refresh button click - assume the value of the first displayed entry, allowing for continuous refresh with the same start address.

The Next Page will use the last entry of the currently displayed table as a basis for the next lookup. When the end is reached the text.

To display MLD Snooping Group information in the web UI:

1. Click Multicast, MLD Snooping, and Group Information.
2. To auto-refresh the information click "Auto-refresh"
3. Click "Refresh" to refresh the webpage.
4. Click First Page or Next Page to change pages.

Figure 9-2.4: MLD Snooping Groups Information

Parameter descriptions:

VLAN ID : The VLAN ID of the group.

Groups : Group address of the group displayed.

Port Members : Ports under this group.

Show entries: Select the number of items to display per page.

Buttons

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

Refresh: Click to refresh the page immediately.

First Page: Updates the table, starting with the first entry in the table.

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

9-2.5 MLD SFM Information

Entries in the MLD SFM Information Table are shown on this page. The MLD SFM (Source-Filtered Multicast) Information Table also contains the SSM (Source-Specific Multicast) information. This table is sorted first by VLAN ID, then by group, and then by Port. Different source addresses belong to the same group are treated as single entry.

To display MLD SFM Information in the web UI:

1. Click Multicast, MLD Snooping and MLD SFM Information.
2. If you want to auto-refresh the information then you need to evoke the “Auto-refresh”.
3. Click “Refresh” to refresh an entry of the MLD SFM Information.
4. Click First/Next Page to change page.

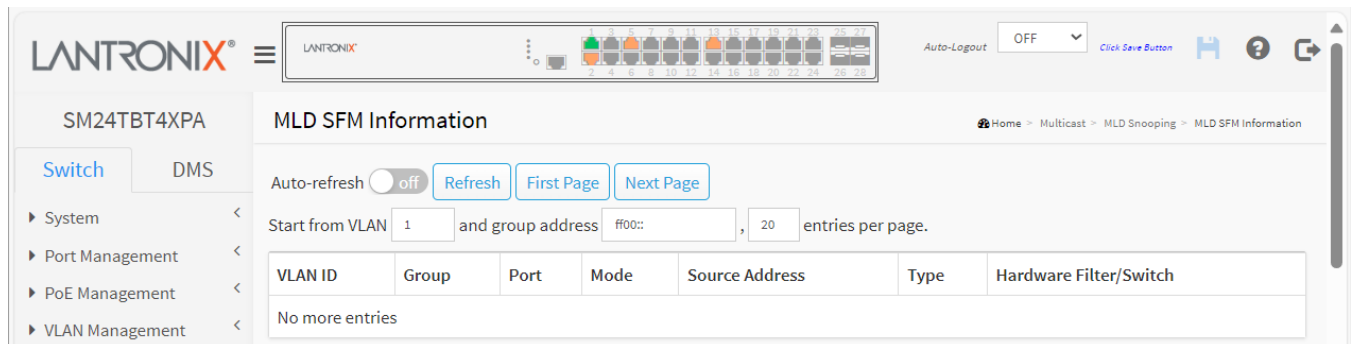


Figure 9-2.5: MLD SFM Information

Parameter descriptions:

VLAN ID : The VLAN ID of the group.

Group : The IP Multicast Group address.

Port : The Switch port number.

Mode : Indicates the filtering mode maintained per (VLAN ID, port number, Group Address) basis. It can be either Include or Exclude.

Source Address : The IP Address of the source. Currently, system limits the total number of IP source addresses for filtering to be 128.

Type : Indicates the Type. It can be either Allow or Deny.

Hardware Filter/Switch: Indicates whether data plane destined to the specific group address from the source IPv6 address could be handled by chip or not.

Buttons

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

Refresh: Click to refresh the page immediately.

First Page: Updates the table starting from the first entry in the MLD SFM Information Table.

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

9-3 MVR

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

9-3.1 Basic Configuration

To configure MVR in the web UI:

1. Click Multicast, MVR, and Basic Configuration.
2. Set the MVR mode to enable or disable and set all parameters.
3. Click “Add New MVR VLAN”.
4. Specify MVR VID, MVR Name, IGMP Address, Mode, Tagging, Priority, LLQI, Interface Channel Profile.
5. Select which port to have Immediate Leave.
6. Click the Apply button to save the settings.
7. To cancel the settings click the Reset button to revert to previously saved values

Figure 9-3.1: MVR Configuration

Parameter descriptions:

MVR Mode: Enable or Disable the MVR globally. The Unregistered Flooding control depends on the current configuration in IGMP MLD Snooping. It is suggested to enable Unregistered Flooding control when the MVR group table is full.

MVR VID: Specify the Multicast VLAN ID.

Caution: MVR source ports are not recommended to be overlapped with management VLAN ports.

MVR Name: MVR Name is an optional attribute to indicate the name of the specific MVR VLAN. Maximum length of the MVR VLAN Name string is 32. MVR VLAN Name can only contain alphabets or numbers. 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, the 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 seconds. The range is 0 - 31744. The default LLQI is 5 tenths or one-half second.

Interface Channel Profile : When the MVR VLAN is created, select the profile to expand the corresponding multicast channel settings for the specific MVR VLAN. The file is established on the Filtering Profile Table.

Port: The logical port for the settings.

Port Role: Configure an MVR port of the designated MVR VLAN as one of the following roles.

Inactive: The designated port does not participate MVR operations.

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

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

Caution: MVR source ports are not recommended to be overlapped with Management VLAN ports. Select the port role by clicking the Role symbol to switch the setting:

I indicates Inactive (default);

S indicates Source;

R indicates Receiver.

Immediate Leave: Enable fast leave on the port.

Buttons

Add New MVR VLAN: Click to add a new MVR VLAN. Specify MVR VID, MVR Name, IGMP Address, Mode, Tagging, Priority, LLQI, Interface Channel Profile. Click "Apply".

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

Apply: Click to save changes.

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

9-3.2 Statistics

This page displays MVR detail Statistics configured MVR on the switch. To display MVR Statistics in the web UI:

1. Click Multicast, MVR, and Statistics.
2. To auto-refresh the information click "Auto-refresh".
3. Click the "Refresh" button to refresh the page.

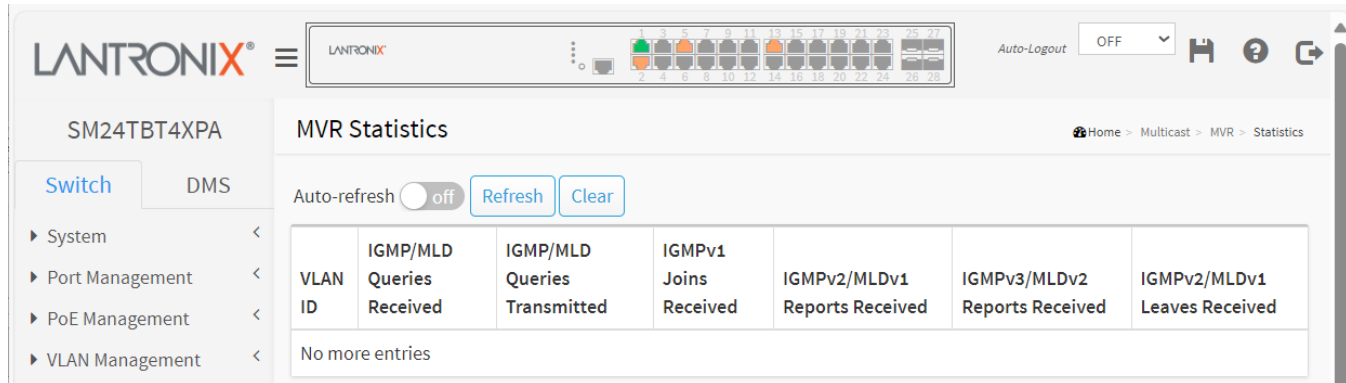


Figure 9-3.2: MVR Statistics Information

Parameter descriptions:

VLAN ID: The Multicast VLAN ID.

IGMP/MLD Queries Received: The number of Received Queries for IGMP and MLD, respectively.

IGMP/MLD Queries Transmitted: The number of Transmitted Queries for IGMP and MLD, respectively.

IGMPv1 Joins Received: The number of Received IGMPv1 Join's.

IGMPv2/MLDv1 Report's Received: The number of Received IGMPv2 Join's and MLDv1 Reports, respectively.

IGMPv3/MLDv2 Report's Received: The number of Received IGMPv3Join's and MLDv2 Reports, respectively.

IGMPv2/MLDv1 Leave's Received: The number of Received IGMPv2 Leave's and MLDv1 Dones, respectively.

Buttons

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

Refresh: Click to refresh the page immediately.

Clear: Clears all Statistics counters.

9-3.3 Groups Information

This page displays MVR Groups detail information on the switch. Entries in the MVR Group Information table are shown on this page. The MVR Group Information table is sorted first by VLAN ID, and then by group.

To display MVR Group Information in the web UI:

1. Click Multicast, MVR, and Groups Information.
2. To auto-refresh the information click “Auto-refresh”.
3. Click the “Refresh” button to refresh an entry of the MVR Groups Information.
4. Click First Page or Next Page to change page.

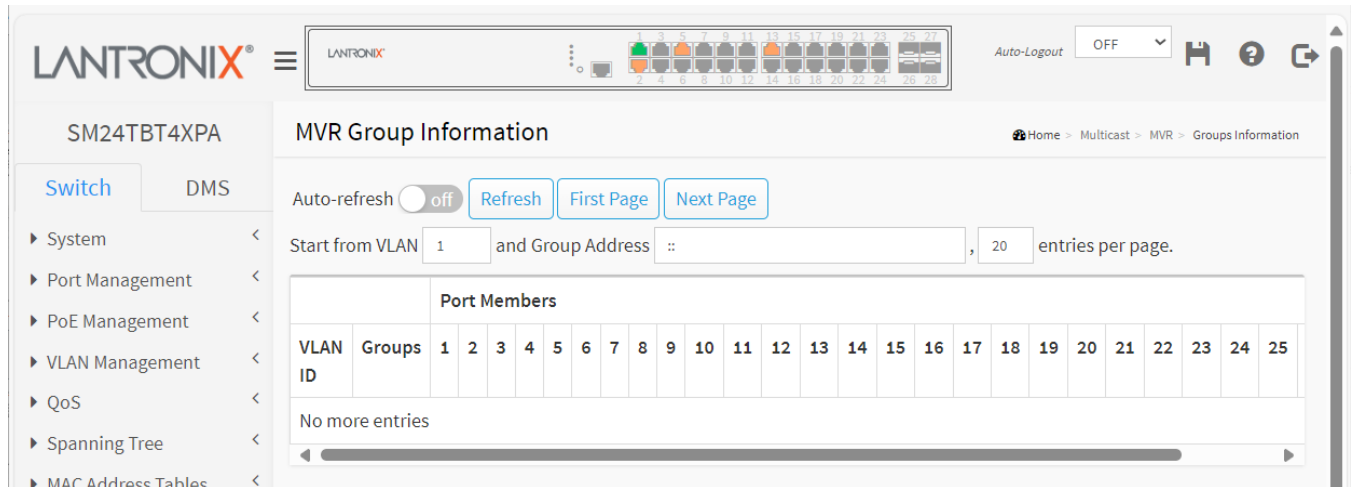


Figure 9-3.3: MVR Groups Information

Parameter descriptions:

Show entries: Choose how many items you want to display per page.

VLAN ID: The VLAN ID of the group.

Groups: The Group ID of the group displayed.

Port Members: The 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.

First Page: Updates the table starting from the first entry in the MVR Channels (Groups) Information table.

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

9-3.4 MVR SFM Information

The MVR SFM (Source-Filtered Multicast) Information Table also contains the SSM (Source-Specific Multicast) information. This table is sorted first by VLAN ID, then by group, and then by Port. Different source addresses belong to the same group are treated as single entry.

To display MVR SFM Information in the web UI:

1. Click Multicast, MVR, and MVR SFM Information.
2. To auto-refresh the information click "Auto-refresh".
3. Click "Refresh" to refresh the page.
4. Click First Page or Next Page to change pages.

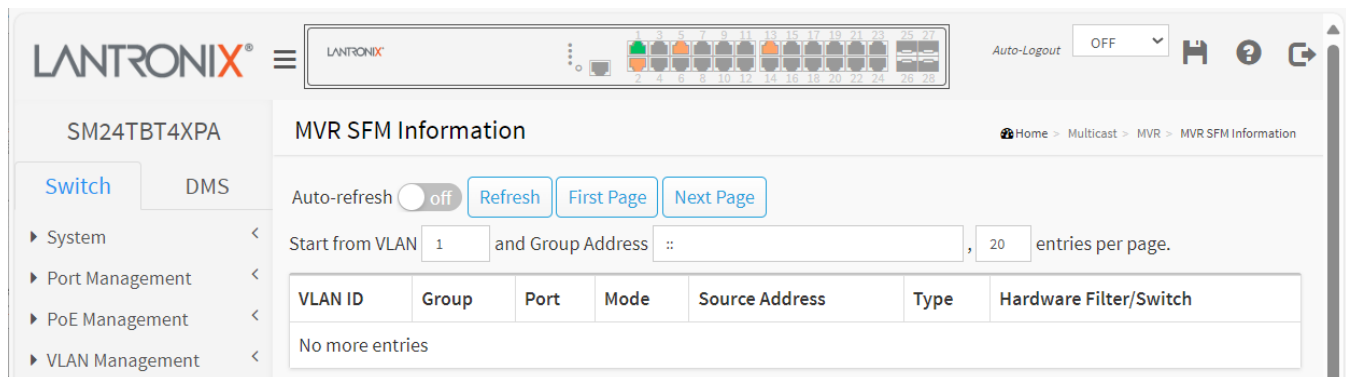


Figure 9-3.4: MVR SFM Information

Parameter descriptions:

Show entries: You can choose how many items you want to show up.

VLAN ID: VLAN ID of the group.

Group: IP Multicast Group address.

Port: The switch port number.

Mode: Indicates the filtering mode maintained per (VLAN ID, port number, Group Address) basis. It can be either *Include* or *Exclude*.

Source Address: IP Address of the source. Currently, system limits the total number of IP source addresses for filtering to be 128. When there is not any source filtering address, the text "None" is shown in the Source Address field.

Type: Indicates the Type. It can be either *Allow* or *Deny*.

Hardware Filter/Switch: Indicates whether data plane destined to the specific group address from the source IPv4/IPv6 address could be handled by the chip.

Buttons

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

Refresh: Click to refresh the page immediately.

First Page: Updates the table starting from the first entry in the MVR SFM Information Table.

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

9-4 Multicast Filtering Profile

This section provides Multicast Filtering Profile related configurations.

9-4.1 Filtering Profile Table

The IPMC profile is used to deploy access control on IP multicast streams. You can create at maximum 64 Profiles with at maximum 128 corresponding rules for each.

To configure the IPMC Profile Configuration in the web UI:

1. Click Multicast, Multicast Filtering Profile and Filtering Profile Table.
2. Set the Multicast Filtering Profile mode to enabled or disabled.
3. Click "Add New Filtering Profile".
4. Specify Profile Name, Profile Description and Rule.
5. Click the Apply button to save the settings.
6. To cancel the settings click the Reset button. It will revert to previously saved values.

Figure 9-4.1: IPMC Profile Configuration

Parameter descriptions:

Multicast Filtering Profile Mode: Enable/Disable the Multicast Filtering Profile. The switch starts to do filtering based on profile settings only when the global profile mode is enabled.

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

Profile Description: Additional description, which is composed of at maximum 64 alphabetic and numeric characters, about the profile. No blank or space characters are permitted as part of description. Use "_" or "-" to separate the description sentence.

Rule: When a 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:

Preview: Preview the rules associated with the designated profile.

Edit: Adjust the rules associated with the designated profile.

Profile Name & Index: 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: Manage rules and the corresponding precedence order by using these buttons:



Insert a new rule before the current entry of rule.

Delete the current entry of rule.

Moves the current entry of rule up in the list.

Moves the current entry of rule down in the list.

Buttons

Add New Filtering Profile: Click to add new IPMC profile. Specify the name and configure the new entry. Click "Apply".

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

Apply: Click to save changes.

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

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 "Apply".

9-4.2 Filtering Address Entry

This page provides address range settings used in IPMC profile. The address entry is used to specify the address range that will be associated with IPMC Profile. You can create up to 128 address entries in the system.

To configure IPMC Profile Address parameters in the web UI:

1. Click Multicast, Multicast Filtering Profile, and Filtering Address Entry.
2. Click "Add New Address (Range) Entry".
3. Specify Entry Name, Start Address and End Address.
4. Click the Apply button to save the settings.
5. Click "Refresh" to refresh the page.
6. Click First Entry or Next Entry to change Entry.

The screenshot shows the Lantronix web interface for the SM24TBT4XPA device. The top navigation bar includes the Lantronix logo, a status bar with various indicators, and an Auto-Logout dropdown set to OFF. The left sidebar contains a menu with categories like Switch and DMS, and sub-items such as System, Port Management, PoE Management, VLAN Management, QoS, Spanning Tree, MAC Address Tables, and Multicast. The main content area is titled 'Multicast Filtering Profile Address Configuration'. It features buttons for 'Refresh', 'First Entry', and 'Next Entry'. Below these is a text input for 'Navigate Address Entry Setting in IPMC Profile by' with a value of '20' and the text 'entries per page.'. A table with four columns is shown: 'Delete' (with a 'Delete' button), 'Entry Name', 'Start Address', and 'End Address'. Below the table is an 'Add New Address (Range) Entry' button, and at the bottom are 'Apply' and 'Reset' buttons.

Figure 9-4.2: IPMC Profile Address Configuration

Parameter descriptions:

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

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"

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

Apply: Click to save changes.

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

First Entry: Updates the table starting from the first entry in the IPMC Profile Address Configuration.

Next Entry: Updates the table, starting with the entry after the last entry currently displayed.

10. DHCP

This section describes how to configure and display the DHCP parameters of the switch.

The Dynamic Host Configuration Protocol (DHCP) is a network management protocol used on Internet Protocol (IP) networks for automatically assigning IP addresses and other communication parameters to devices connected to the network using a client-server architecture.

10-1 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.

10-1.1 Configuration

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

To configure DHCP snooping in the web UI:

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

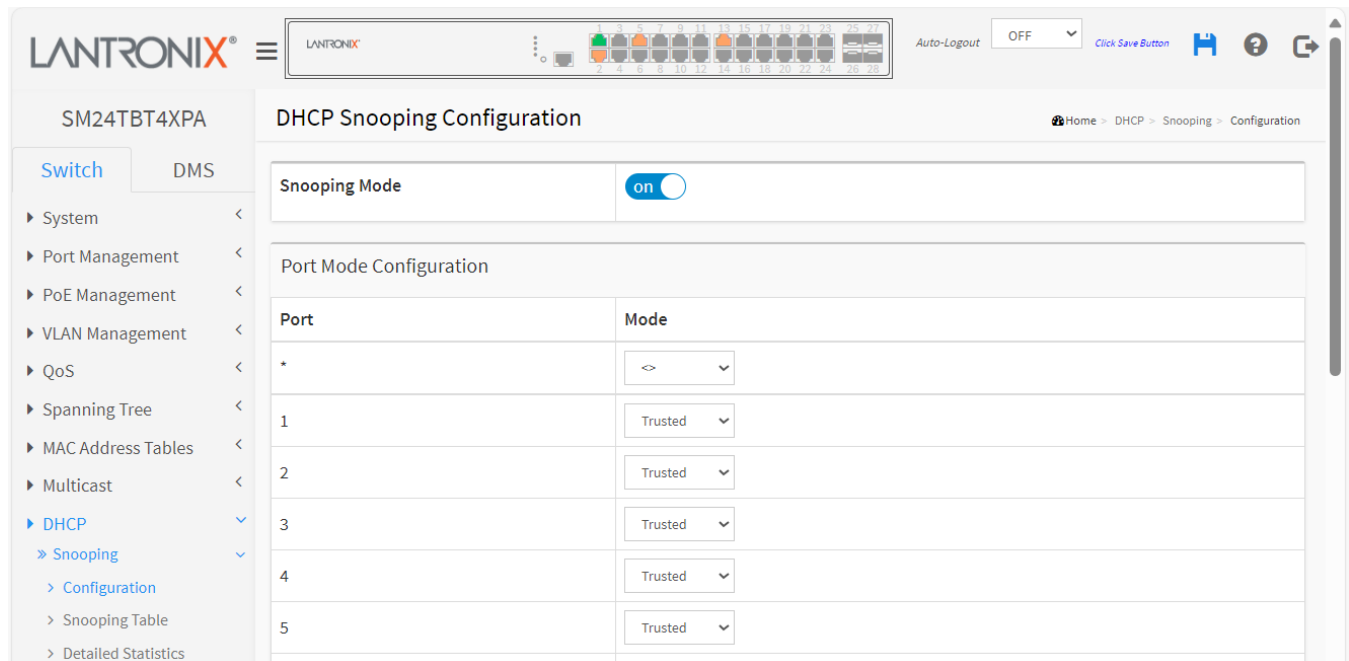


Figure 10-1.1: DHCP Snooping Configuration

Parameter descriptions:

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

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

off: Disable DHCP snooping mode operation.

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

Trusted: Configures the port as trusted source of the DHCP messages. A Trusted port can forward DHCP packets normally.

Untrusted: Configures the port as untrusted source of the DHCP messages. An Untrusted port will discard the packets when it receives DHCP packets.

Buttons

Apply: Click to save changes.

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

10-1.2 Snooping Table

This page displays the dynamic IP assigned information after DHCP Snooping mode is enabled. All DHCP clients obtained the dynamic IP address from the DHCP server will be listed in this table except for local VLAN interface IP addresses. Entries in the Dynamic DHCP Snooping Table are shown on this page.

To monitor DHCP Snooping in the web UI:

1. Click DHCP, Snooping, and Snooping table.
2. To auto-refresh the information click "Auto-refresh".
3. Click the "Refresh" button to refresh the page.
4. Click First/Next Page to change page.

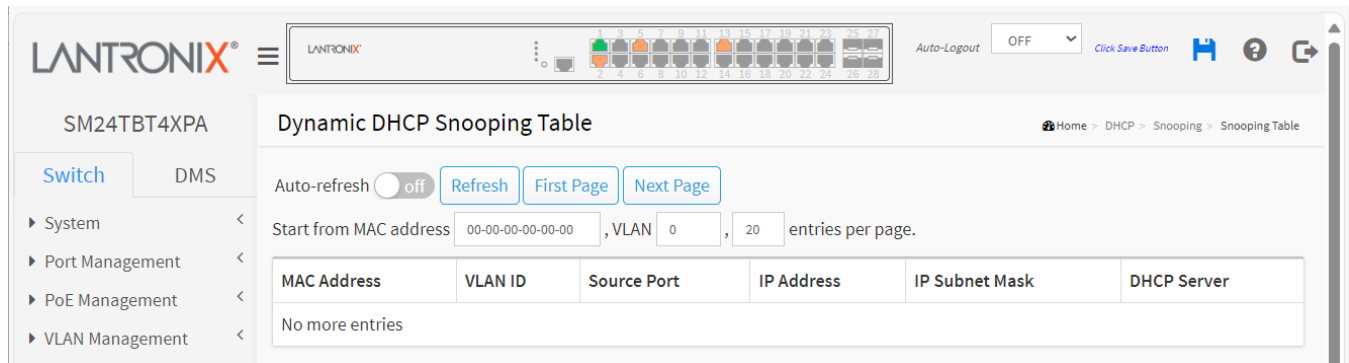


Figure 10-1.2: Dynamic DHCP Snooping Table

Parameter descriptions:

Show entries: You can choose how many items you want to display per page.

MAC Address : User MAC address of the entry.

VLAN ID : VLAN-ID in which the DHCP traffic is permitted.

Source Port: Switch Port Number for which the entries are displayed.

IP Address : User IP address of the entry.

IP Subnet Mask : User IP subnet mask of the entry.

DHCP Server : DHCP Server address of the entry.

Buttons

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

Refresh: Click to refresh the page immediately.

First Page: Updates the table starting from the first entry in the Dynamic DHCP Snooping Table.

Next Page: Updates the group information entries and turns to the next page.

10-1.3 Detailed Statistics

This page provides statistics for DHCP snooping. Note that the normal forward per-port TX statistics isn't increased if the incoming DHCP packet is done by an L3 forwarding mechanism. Clear the statistics on specific port may not take effect on global statistics since it gathers from a different layer overview.

To display DHCP statistics in the web UI:

1. Click DHCP, Snooping, and Detailed Statistics.
2. Select port that you want to display the DHCP Detailed Statistics.
3. To auto-refresh the information click "Auto-refresh".
4. To click the "Refresh" to refresh an entry of the DHCP Detailed Statistics.

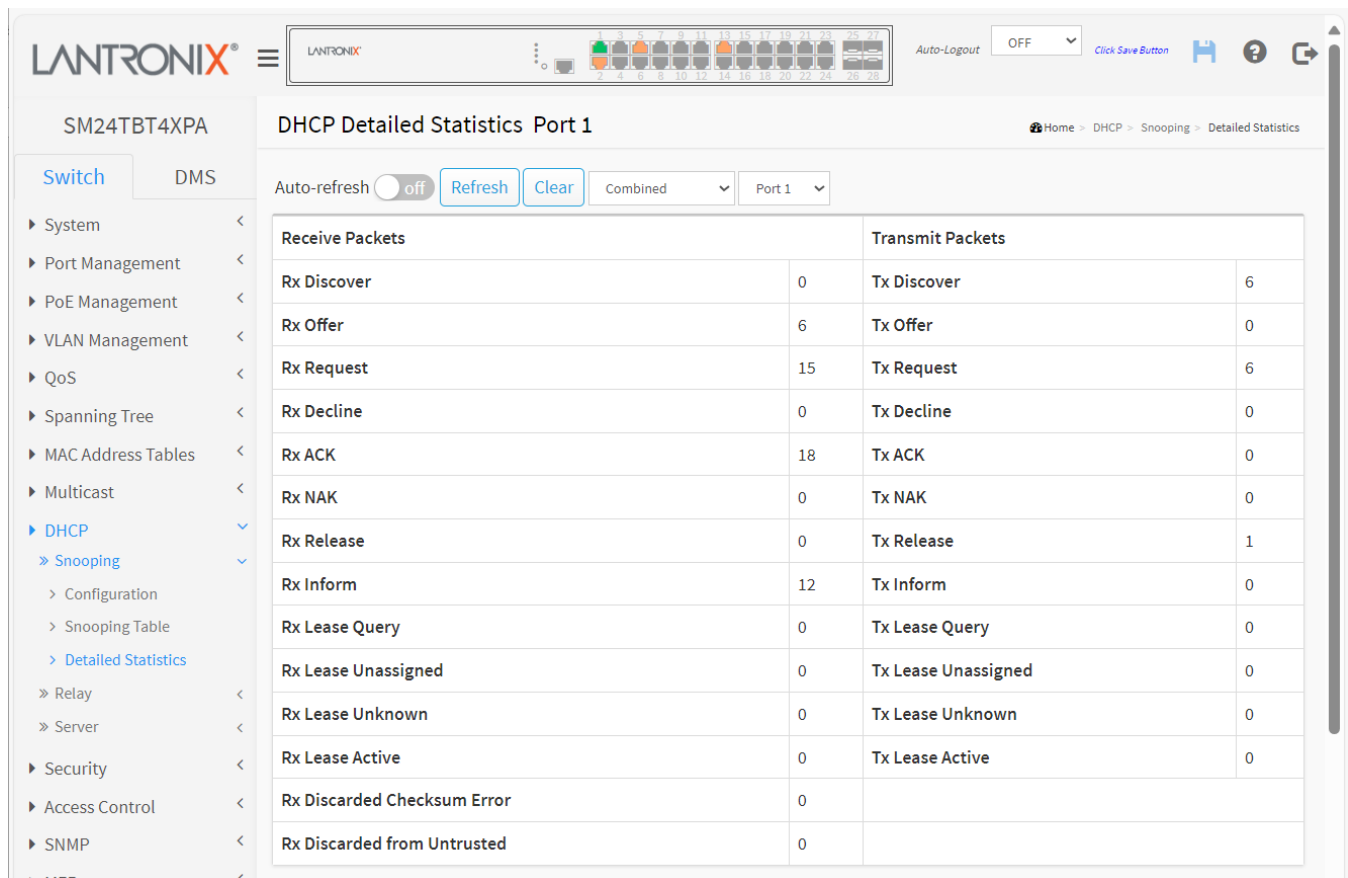


Figure 10-1.3: DHCP Detailed Statistics

Parameter descriptions:

Server Statistics

Rx and Tx Discover : The number of discover (option 53 with value 1) packets received and transmitted.

Rx and Tx Offer : The number of offer (option 53 with value 2) packets received and transmitted.

Rx and Tx Request : The number of request (option 53 with value 3) packets received and transmitted.

Rx and Tx Decline: The number of decline (option 53 with value 4) packets received and transmitted.

Rx and Tx ACK: The number of ACK (option 53 with value 5) packets received and transmitted.

Rx and Tx NAK: The number of NAK (option 53 with value 6) packets received and transmitted.

Rx and Tx Release: The number of release (option 53 with value 7) packets received and transmitted.

Rx and Tx Inform: The number of inform (option 53 with value 8) packets received and transmitted.

Rx and Tx Lease Query: The number of lease query (option 53 with value 10) packets received and transmitted.

Rx and Tx Lease Unassigned: The number of lease unassigned (option 53 with value 11) packets received and transmitted.

Rx and Tx Lease Unknown: The number of lease unknown (option 53 with value 12) packets received and transmitted. Rx and Tx Lease Active

Rx and Tx Lease Active: The number of lease active (option 53 with value 13) packets received and transmitted.

Rx Discarded checksum error: The number of discard packet that IP/UDP checksum is error.

Rx Discarded from Untrusted: The number of discarded packet 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.

10-2 Relay

10-2.1 Configuration

A DHCP relay agent is used to forward and to transfer DHCP messages between the clients and the server when they are not in the same subnet domain. It stores the incoming interface IP address in the GIADDR field of the DHCP packet. The DHCP server can use the value of GIADDR field to determine the assigned subnet. For such 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 DHCP, Relay and Configuration.
2. Specify the Relay Mode, Relay server, Relay Information Mode, Relay Information Policy.
3. Click Apply. At the prompt "Please make sure the DHCP server connected on trust port?" click OK.

DHCP Relay Configuration Home > DHCP > Relay > Configuration

| | |
|--------------------------|---------------------------------------|
| Relay Mode | <input type="radio"/> off |
| Relay Server | <input type="text" value="0.0.0.0"/> |
| Relay Information Mode | <input type="text" value="Disabled"/> |
| Relay Information Policy | <input type="text" value="Keep"/> |

Figure 10-2.1: DHCP Relay Configuration

Parameter descriptions:

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

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

off: Disable DHCP relay mode operation.

Relay Server : Indicates the DHCP relay server IP address.

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

Possible 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 of 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.

10-2.2 Statistics

This page provides statistics for DHCP relay. To monitor DHCP Relay statistics in the web UI:

1. Click DHCP, Relay, and Statistics.
2. View the DHCP relay statistics.
3. To auto-refresh the information click “Auto-refresh”.
4. Click “Refresh” to refresh the webpage.

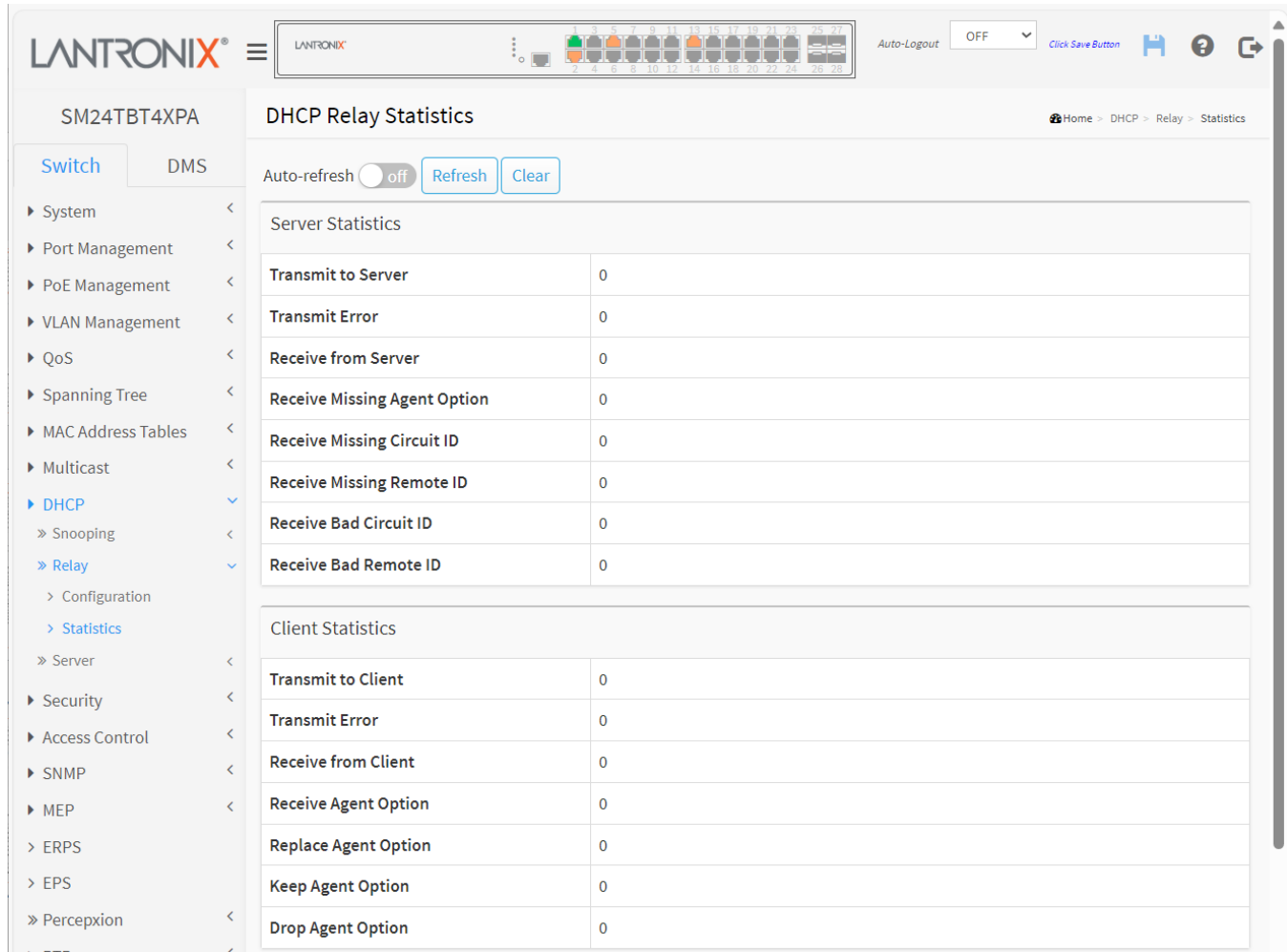


Figure 10-2.2: DHCP Relay Statistics

Server Statistics

Transmit to Server : The number of packets that are relayed from client to server.

Transmit Error : The number of packets that resulted in errors while being sent to clients.

Receive from Server : The number of packets received from server.

Receive Missing Agent Option: The number of packets received without agent information options.

Receive Missing Circuit ID : The number of packets received with the Circuit ID option missing.

Receive Missing Remote ID : The number of packets received with the Remote ID option missing.

Receive Bad Circuit ID: The number of packets whose Circuit ID option did not match known circuit ID.

Receive Bad Remote ID: The number of packets whose Remote ID option did not match known Remote ID.

Client Statistics

Transmit to Client : The number of relayed packets from server to client.

Transmit Error : The number of packets that resulted in error while being sent to servers.

Receive from Client : The number of received packets from server.

Receive Agent Option : The number of received packets with relay agent information option.

Replace Agent Option : The number of packets which were replaced with relay agent information option.

Keep Agent Option : The number of packets whose relay agent information was retained.

Drop Agent Option : The number of packets that were dropped which were received with relay agent information.

Buttons

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

Refresh: Click to refresh the page immediately.

Clear : Clear all statistics.

10-3 Server

10-3.1 Configuration

This page lets you enable/disable DHCP server per system and per VLAN, and set Start IP and End IP addresses. A DHCP server will allocate these IP addresses to a DHCP client and deliver configuration parameters to a DHCP client.

To configure DHCP Server parameters in the web UI:

1. Click DHCP, Server, and Configuration.
2. Click "Add Interface".
3. Specify VLAN, Mode, Start IP, End IP, Lease time, Subnet mask, Default router, and DNS server.
4. Click Apply.

The screenshot shows the Lantronix web interface for the SM24TBT4XPA device. The 'DHCP Server Configuration' page is active. On the left, a sidebar lists navigation options: System, Port Management, PoE Management, VLAN Management, QoS, and Spanning Tree. The main area displays a table of DHCP interfaces. The first interface is for VLAN 1, which is enabled (Mode: on). The configuration parameters are: Start IP 0.0.0.0, End IP 0.0.0.0, Lease Time 86400, Subnet Mask 0.0.0.0, Default Router 0.0.0.0, and DNS Server 0.0.0.0. 'Apply' and 'Reset' buttons are located below the table.

| VLAN | Mode | Start IP | End IP | Lease Time | Subnet Mask | Default Router | DNS Server |
|------|------|----------|---------|------------|-------------|----------------|------------|
| 1 | on | 0.0.0.0 | 0.0.0.0 | 86400 | 0.0.0.0 | 0.0.0.0 | 0.0.0.0 |

Figure 10-3.1: DHCP server configuration

Parameter descriptions:

VLAN: Configure the VLAN in which DHCP server is enabled or disabled. Allowed VLAN are in the range 1 through 4095

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

Enable: Enable DHCP server per VLAN.

Disable: Disable DHCP server per VLAN.

Start IP and End IP: Define the IP range. The Start IP must be smaller than or equal to the End IP.

Lease Time : Display lease time of the pool.

Subnet Mask : Configure subnet mask of the DHCP address.

Default router: Configure the destination IP network or host address of this route.

DNS Server: Specify DNS server.

Buttons

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

Add Interface: Click to add a new DHCP server.

Apply: Click to save changes.

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

10-3.2 Status

This page displays DHCP server status. To display DHCP server status in the web UI:

1. Click DHCP, Server, and Status.
2. To auto-refresh the information check "Auto-refresh".
3. Click the "Refresh" button to refresh the page.

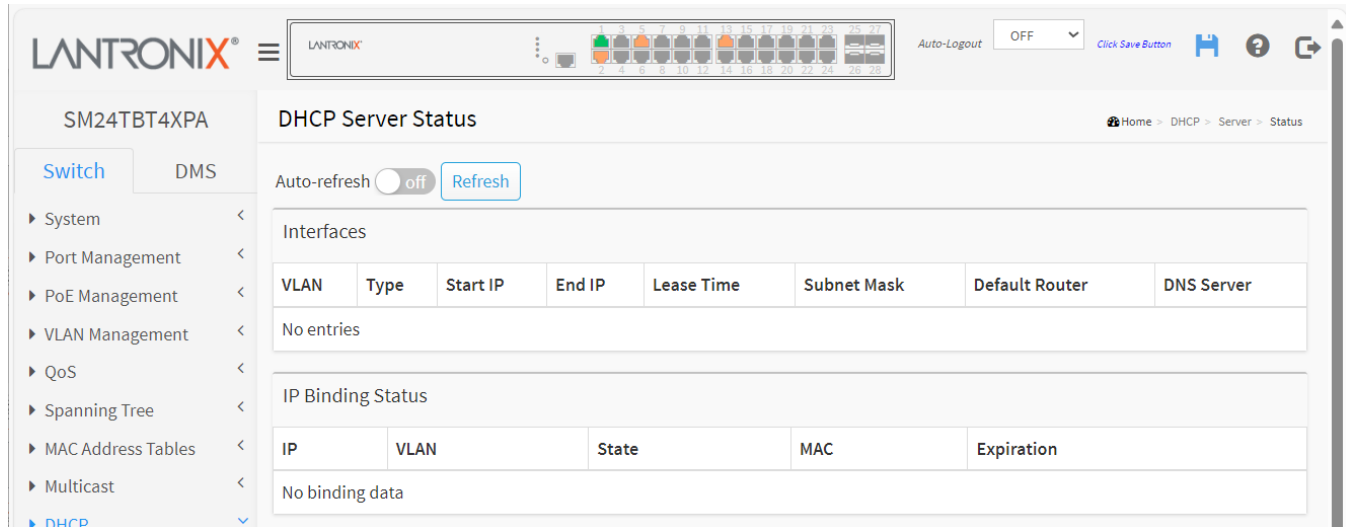


Figure 10-3.2: DHCP Server Status

Parameter descriptions:

Interfaces

VLAN: The VLAN ID of the entry.

Type: Indicate the operation type per VLAN. Possible types are: **Static** and **DMS**.

Start IP and End IP: Display the Start IP and the End IP addresses.

Lease Time : Display lease time of the pool.

Subnet Mask : Display subnet mask of the DHCP address.

Default router: Display the destination IP network or host address of this route.

DNS Server: Display DNS server.

IP Binding Status

IP: Displays the IP address of the binding.

VLAN: Displays the VLAN ID of the binding.

State: Displays the current binding state.

MAC: Displays the MAC IP address of the binding.

Expiration: Display lease expiration time.

Buttons

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

Refresh: Click to refresh the page immediately.

11. Security

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

11-1 Management

11-1.1 Account

This page provides an overview of the current users. Currently the only way to login as another user on the web server is to close and reopen the browser.

To configure Users in the web UI:

1. Click Security, Management and Account.
2. Click Add New User.
3. Specify the User Name parameters.
4. Click Apply.

The top screenshot shows the 'Account Configuration' page. It has a sidebar with 'Switch' and 'DMS' tabs, and a navigation menu with 'System', 'Port Management', and 'PoE Management'. The main content area has a breadcrumb trail 'Home > Security > Management > Account'. Below this is a table with two columns: 'User Name' and 'Privilege Level'. The table contains one row with 'admin' and '15'. There is an 'Add New User' button below the table.

The bottom screenshot shows the 'Add Account' page. It has the same sidebar and navigation menu. The breadcrumb trail is 'Home > Security > Management > Account'. The main content area has a section titled 'Account Settings' with four input fields: 'User Name', 'Password', 'Password (again)', and 'Privilege Level'. The 'Privilege Level' field is a dropdown menu currently set to '0'. There are 'Apply', 'Reset', and 'Cancel' buttons at the bottom.

Figure 11-1.1: Account Configuration > Add Account

Parameter descriptions:

User Name: The name identifying the user. You can input up to 31 characters. This is also a link to Add/Edit User.

Account Settings:

Password: Type the password. You can input up to 31 characters, and the allowed content is the 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 0 - 15. If the privilege level value is 15, it can access all groups, i.e. that is granted the fully control of the device. But others value need to refer to each group privilege level. User's privilege should be same or greater than the group privilege level to have the access of that group. By default setting, most groups privilege level 5 has the read-only access and privilege level 10 has the read-write access. And the system maintenance (software upload, factory defaults and etc.) need user privilege level 15. Generally, the privilege level 15 can be used for an administrator account, privilege level 10 for a standard user account, and privilege level 5 for a guest account.

Buttons

Apply: Click to save changes.

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

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

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

11-1.2 Privilege Levels

This page provides an overview of the privilege levels. The switch lets you set Privilege Levels for various Group Names (e.g., Aggregation, Debug, DHCP, DHCPv6_Client, Diagnostics, etc.). You can set Privilege Levels from 1 to 15 for each Group.

To configure Privilege Levels in the web UI:

1. Click Security, Management and Privilege Levels.
2. Specify the Privilege parameter.
3. Click Apply.

The screenshot shows the Lantronix web interface for the SM24TBT4XPA device. The 'Privilege Levels Configuration' page is active, displaying a table where users can set Read-only and Read-write privilege levels for different system groups. The left sidebar shows the navigation menu with 'Security' > 'Management' > 'Privilege Levels' selected.

| Group Name | Privilege Levels | |
|----------------------|------------------|------------|
| | Read-only | Read-write |
| Aggregation | 5 | 10 |
| Debug | 15 | 15 |
| DHCP | 5 | 10 |
| DHCPv6_Client | 5 | 10 |
| Diagnostics | 1 | 10 |
| DMS_client | 5 | 10 |
| DMS_Trouble_Shooting | 5 | 10 |
| DMS_Vbatch | 5 | 10 |
| EPS | 5 | 10 |
| ERPS | 5 | 10 |
| ETH_LINK_OAM | 5 | 10 |
| Firmware | 5 | 10 |
| FRR | 5 | 10 |
| Green_Ethernet | 5 | 10 |

Figure11-1.2: Privilege Level Configuration

Parameter descriptions:

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

System: Contact, Name, Location, Time zone, 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: The Privilege Levels can be configured between 0 to 15 (where 0 is lowest level and 15 is highest level). Every group has an authorization Privilege level for these sub-groups: Read-only and Read-write. User Privilege should be same or greater than the Authorization Privilege level to have the access to that function.

Buttons

Apply: Click to save changes.

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

11-1.3 Auth Method

This page lets you configure a user with auth method when they log into the switch via one of the management client interfaces. To configure Auth Method in the web UI:

1. Click Security, Management and Auth Method.
2. Specify the Client (console, telnet, ssh, http, https) which you want to monitor.
3. Specify the Methods (none, local, radius, tacacs), Service port, Cmd Lvl, Cfg Cmd, Fallback, Exec.
4. Click Apply.

Authentication Method Configuration

Home > Security > Management > Auth Method

Authentication Method

| Client | Methods | Service Port |
|---------|--|--------------|
| console | local <input type="text" value="no"/> <input type="text" value="no"/> | |
| telnet | local <input type="text" value="no"/> <input type="text" value="no"/> | 23 |
| ssh | local <input type="text" value="no"/> <input type="text" value="no"/> | 22 |
| http | redirect <input type="text" value="no"/> <input type="text" value="no"/> | 80 |
| https | local <input type="text" value="no"/> <input type="text" value="no"/> | 443 |

Command Authorization Method

| Client | Method | Cmd Lvl | Cfg Cmd |
|---------|------------------------------------|---------|--------------------------|
| console | no <input type="text" value="no"/> | 0 | <input type="checkbox"/> |
| telnet | no <input type="text" value="no"/> | 0 | <input type="checkbox"/> |
| ssh | no <input type="text" value="no"/> | 0 | <input type="checkbox"/> |

Accounting Method

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

Apply Reset

Figure 11-1.3: Authentication Method Configuration

Parameter descriptions:

Authentication Method Configuration

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

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

none : authentication is disabled and login is not possible.

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

radius : use a remote RADIUS server for authentication.

tacacs: use a remote TACACS server for authentication.

Methods that involve remote servers are timed out if the remote servers are offline. In this case the next method is tried. Each method is tried from left to right and continues until a method either approves or rejects a user. If a remote server is used for primary authentication it is recommended to configure secondary

authentication as 'local'. This will enable the management client to login via the local user database if none of the configured authentication servers are alive.

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

HTTP Redirect: Enable HTTP Automatic Redirect to HTTPS (secure HTTP).

Command Authorization Method Configuration

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

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

none : authorization is disabled and login is not possible.

tacacs: use a remote TACACS+ server for authorization.

Cmd Lvl: Runs authorization for all commands at the specified privilege level. Specific command level that should be authorized. Valid entries are 0 through 15.

Cfg Cmd: Also authorize configuration commands.

Accounting Method: The accounting section allows you to configure command and exec (login) accounting. The table has one row for each client type and a number of columns, which are:

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

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

no: Accounting is disabled.

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

Cmd Lvl: Enable accounting of all commands with a privilege level higher than or equal to this level. Valid values are 0 - 15. Leave the field empty to disable command accounting.

Exec: Enable exec (login) accounting.

Buttons

Apply: Click to save changes.

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

11-1.4 Access Method

This page lets you configure the Access Management table including HTTP/HTTPS, SNMP, and TELNET/SSH. You can manage the switch over an Ethernet LAN or over the Internet. To configure Access Method in the web UI:

1. Click Security, Management, and Access Method.
2. Select “on” as the Mode of Access Management Configuration.
3. Click “Add New Entry”.
4. Specify the VLAN ID, Start IP Address, and End IP Address.
5. Checked Access Management method (HTTP/HTTPS, SNMP, and TELNET/SSH) in the entry.
6. Click Apply.

Figure 11-1.4: Access Method Configuration

Parameter descriptions:

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

On : Enable access management mode operation.

Off : Disable access management mode operation.

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

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

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

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

HTTP/HTTPS: Indicates that the host can access the switch from an HTTP or 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.

11-1.5 HTTPS

This page lets you configure HTTPS settings and maintain the current certificate. To configure Access Management in the web UI:

1. Click Configuration, Security, Management and HTTPS.
2. Specify the Certificate Maintain, Certificate Pass Phrase, Certificate Upload parameters.
3. Click the Browse button to select the file to upload.

4. Click Apply.

The screenshot shows the Lantronix web interface for the SM24TBT4XPA device. The top navigation bar includes the Lantronix logo, a menu icon, and a status bar with 'Auto-Logout OFF' and a 'Click Save Button' link. The left sidebar has a 'Switch' tab selected, with a list of configuration categories: System, Port Management, PoE Management, VLAN Management, QoS, Spanning Tree, and MAC Address Tables. The main content area is titled 'HTTPS Configuration' and contains the following fields:

- Certificate Maintain:** A dropdown menu set to 'Upload'.
- Certificate Pass Phrase:** A text input field.
- Certificate Upload:** A dropdown menu set to 'Web Browser'.
- File Upload:** A 'Choose File' button and the text 'No file chosen'.
- Certificate Status:** A text field displaying 'Switch secure HTTP certificate is presented'.

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

Figure 11-1.5: HTTPS Configuration

Parameter descriptions:

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

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

Generate: Generate a new self-signed RSA certificate.

Certificate Pass Phrase: Enter the 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 new browser versions have removed support for DSA in certificates (e.g. Firefox v37 and Chrome v39).

Certificate Status: Displays 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.

11-2 802.1X

11-2.1 Configuration

This page lets you configure the 802.1X parameters of the switch. The 802.1X 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 IEEE 802.1X in the web UI:

1. Click Security, 802.1X, and Configuration.
2. Select “on” as the Mode of IEEE 802.1X Configuration.
3. Set the parameters as required.
4. Click the Apply button to save the settings.
5. To cancel the settings click the Reset button. It will revert to previously saved values.

LANTRONIX SM24TBT4XPA

802.1X Configuration

Home > Security > 802.1X > Configuration

System Configuration

Mode: ☒ on

Reauthentication Enabled: ☐

Reauthentication Period: 3600 seconds

EAPOL Timeout: 30 seconds

Aging Period: 300 seconds

Hold Time: 10 seconds

RADIUS-Assigned QoS Enabled: ☐

RADIUS-Assigned VLAN Enabled: ☐

Guest VLAN Enabled: ☐

Guest VLAN ID: 1

Max. Reauth. Count: 2

Allow Guest VLAN if EAPOL Seen: ☐

Port Configuration

| Port | Admin State | RADIUS-Assigned QoS Enabled | RADIUS-Assigned VLAN Enabled | Guest VLAN Enabled | Port State | Restart |
|------|----------------------|-----------------------------|------------------------------|--------------------------|-------------------|---|
| * | <input type="text"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | | |
| 1 | Force Authorized | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | Globally Disabled | Reauthenticate Reinitialize |
| 2 | Force Authorized | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | Globally Disabled | Reauthenticate Reinitialize |
| 3 | Force Authorized | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | Globally | Reauthenticate Reinitialize |

Figure 11-2.1: IEEE 802.1X Configuration

Parameter descriptions:

System Configuration

Mode : on or off. Indicates if IEEE 802.1X is globally enabled or disabled on the switch. If globally disabled, all ports are allowed forwarding of frames.

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

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

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

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

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

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

When the NAS module uses the Port Security module to secure MAC addresses, the Port Security module needs to check for activity on the MAC address in question at regular intervals and free resources if no activity is seen within a given period. This parameter controls exactly this period and can be set to a number between 10 and 1000000 seconds. If reauthentication is enabled and the port is in an 802.1X-based mode, this is not so critical, since supplicants that are no longer attached to the port will get removed upon the next reauthentication, which will fail. But if reauthentication is not enabled, the only way to free resources is by aging the entries.

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

Hold Time: This setting applies to the following modes (i.e. modes using the Port Security function to secure MAC addresses):

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

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

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

RADIUS-Assigned QoS Enabled: RADIUS-assigned QoS provides a means to centrally control the traffic class to which traffic coming from a successfully authenticated supplicant is assigned on the switch. The RADIUS server must be configured to transmit special RADIUS attributes to take advantage of this feature (see RADIUS-Assigned QoS Enabled below for a detailed description). The "RADIUS-Assigned QoS Enabled" checkbox provides a quick way to globally enable/disable RADIUS-server assigned QoS Class functionality. When checked, the individual ports' ditto setting determine whether RADIUS-assigned QoS Class is enabled on that port. When unchecked, RADIUS-server assigned QoS Class is disabled on all ports.

RADIUS-Assigned VLAN Enabled: RADIUS-assigned VLAN provides a means to centrally control the VLAN on which a successfully authenticated supplicant is placed on the switch. Incoming traffic will be classified to and switched on the RADIUS-assigned VLAN. The RADIUS server must be configured to transmit special RADIUS attributes to take advantage of this feature (see RADIUS-Assigned VLAN Enabled below for a detailed description). The "RADIUS-Assigned VLAN Enabled" checkbox provides a quick way to globally enable/disable RADIUS-server assigned VLAN functionality. When checked, the individual ports' ditto setting determines whether RADIUS-assigned VLAN is enabled on that port. When unchecked, RADIUS-server assigned VLAN is disabled on all ports.

Guest VLAN Enabled: A Guest VLAN is a special VLAN -typically with limited network access -on which 802.1X-unaware clients are placed after a network administrator-defined timeout. The switch follows a set of rules for entering and leaving the Guest VLAN as listed below. The "Guest VLAN Enabled" checkbox provides a quick way to globally enable/disable Guest VLAN functionality. When checked, the individual ports' ditto setting determines whether the port can be moved into Guest VLAN. When unchecked, the ability to move to the Guest VLAN is disabled on all ports.

Guest VLAN ID: This is the value that a port's Port VLAN ID is set to if a port is moved into the Guest VLAN. It is only changeable if the Guest VLAN option is globally enabled. Valid values are in the range [1; 4094].

Max. Reauth. Count: The number of times the switch transmits an EAPOL Request Identity frame without response before considering entering the Guest VLAN is adjusted with this setting. The value can only be changed if the Guest VLAN option is globally enabled. Valid values are in the range [1; 255].

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

Port Configuration

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

Admin State : If 802.1X is globally enabled, this selection controls the port's authentication mode. The following modes are available:

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

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

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

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

Note: Suppose two backend servers are enabled and that the server timeout is configured to X seconds (using the 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 function.

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 a 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 function.

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

This option is only available for single-client modes, i.e.:

- Port-based 802.1X
- Single 802.1X

RADIUS attributes used in identifying a QoS Class:

The User-Priority-Table attribute defined in IETF RFC4675 forms the basis for identifying the QoS Class in an Access-Accept packet. Only the first occurrence of the attribute in the packet will be considered, and to be valid, it must follow this rule:

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

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

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

This option is only available for single-client modes, i.e.

- Port-based 802.1X
- Single 802.1X

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

RADIUS attributes used in identifying a VLAN ID:

IETF RFC2868 and RFC3580 form the basis for the attributes used in identifying a VLAN ID in an Access Accept packet. The following criteria are used:

- The Tunnel Medium Type, Tunnel Type, and Tunnel Private Group ID attributes must all be present at least once in the Access Accept packet.
- The switch looks for the first set of these attributes that have the same Tag value and fulfil the following requirements (if Tag == 0 is used, the Tunnel Private Group ID does not need to include a Tag):
 - Value of Tunnel Medium Type must be set to "IEEE 802" (ordinal 6).
 - Value of Tunnel Type must be set to "VLAN" (ordinal 13).

- Value of Tunnel Private Group ID must be a string of ASCII chars in the range '0' - '9', which is interpreted as a decimal string representing the VLAN ID. Leading '0's are discarded. The final value must be in the range [1; 4095].

Guest VLAN Enabled: When Guest VLAN is both globally enabled and enabled (checked) for a given port, the switch considers moving the port into the Guest VLAN based on the rules outlined below. This option is only available for EAPOL-based modes, i.e.:

- Port-based 802.1X
- Single 802.1X
- Multi 802.1X

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

Guest VLAN Operation: When a Guest VLAN enabled port's link comes up, the switch starts transmitting EAPOL Request Identity frames. If the number of transmissions of such frames exceeds Max. Reauth. Count and no EAPOL frames have been received in the meanwhile, the switch considers entering the Guest VLAN. The interval between transmission of EAPOL Request Identity frames is configured with EAPOL Timeout. If Allow Guest VLAN if EAPOL Seen is enabled, the port will now be placed in the Guest VLAN. If disabled, the switch will first check its history to see if an EAPOL frame has previously been received on the port (this history is cleared if the port link goes down or the port's Admin State is changed), and if not, the port will be placed in the Guest VLAN. Otherwise it will not move to the Guest VLAN, but continue transmitting EAPOL Request Identity frames at the rate given by EAPOL Timeout. Once in the Guest VLAN, the port is considered authenticated, and all attached clients on the port are allowed access on this VLAN. The switch will not transmit an EAPOL Success frame when entering the Guest VLAN.

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

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

Globally Disabled: IEEE 802.1X is globally disabled.

Link Down: IEEE 802.1X is globally enabled, but there is no link on the port.

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

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

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

Restart : Two buttons are available for each row. The buttons are only enabled when authentication is globally enabled and the port's Admin State is in an EAPOL-based or MAC-based mode.

Clicking these buttons will not cause settings changed on the page to take effect.

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

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

Buttons

Apply: Click to save changes.

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

11-2.2 Status

This page displays each port's 802.1X status information, including Admin State, Port State, Last Source, Last ID and Port VLAN ID.

To display 802.1X Status in the web UI:

1. Click Security, IEEE 802.1X, and Status.
2. Check "Auto-refresh" to on.
3. Click "Refresh" to refresh the port detailed statistics.
4. Select which port that you want display 802.1X Statistics.

The screenshot shows the Lantronix web interface for the SM24TBT4XPA device. The top navigation bar includes the Lantronix logo, a port status indicator (showing ports 1-24 with various colors), and an 'Auto-Logout' dropdown set to 'OFF'. The left sidebar contains a menu with categories like System, Port Management, PoE Management, VLAN Management, QoS, Spanning Tree, MAC Address Tables, Multicast, DHCP, Security (expanded), and Status. The main content area is titled '802.1X Status' and includes an 'Auto-refresh' toggle (currently off) and a 'Refresh' button. Below this is a table with 7 columns: Port, Admin State, Port State, Last Source, Last ID, QoS Class, and Port VLAN ID. The table lists ports 1 through 10, all with 'Force Authorized' Admin State and 'Globally Disabled' Port State. The bottom of the table shows partial rows for 'N-1' and 'N'.

| Port | Admin State | Port State | Last Source | Last ID | QoS Class | Port VLAN ID |
|------|------------------|-------------------|-------------|---------|-----------|--------------|
| 1 | Force Authorized | Globally Disabled | | | - | |
| 2 | Force Authorized | Globally Disabled | | | - | |
| 3 | Force Authorized | Globally Disabled | | | - | |
| 4 | Force Authorized | Globally Disabled | | | - | |
| 5 | Force Authorized | Globally Disabled | | | - | |
| 6 | Force Authorized | Globally Disabled | | | - | |
| 7 | Force Authorized | Globally Disabled | | | - | |
| 8 | Force Authorized | Globally Disabled | | | - | |
| 9 | Force Authorized | Globally Disabled | | | - | |
| 10 | Force Authorized | Globally Disabled | | | - | |
| N-1 | Force Authorized | Globally Disabled | | | - | |
| N | Force Authorized | Globally Disabled | | | - | |

Figure 11-2.2: IEEE 802.1X Status

Parameter descriptions:

802.1X Status

Port : The switch port number. Click to navigate to detail 802.1X statistics for this port.

Admin State : The port's current administrative state. Refer to 802.1X Admin State for a description of possible values.

Port State : The current state of the port. Refer to 802.1X Port State for a description of the individual states.

Last Source : The source MAC address carried in the most recently received EAPOL frame for EAPOL-based authentication, and the most recently received frame from a new client for MAC-based authentication.

Last ID : The user name (supplicant identity) carried in the most recently received Response Identity EAPOL frame for EAPOL-based authentication, and the source MAC address from the most recently received frame from a new client for MAC-based authentication.

QoS Class: QoS Class assigned to the port by the RADIUS server if enabled.

Port VLAN ID : The VLAN ID that 802.1X has put the port in. The field is blank if the Port VLAN ID is not overridden by 802.1X.

If the VLAN ID is assigned by the RADIUS server, "(RADIUS-assigned)" is appended to the VLAN ID.

If the port is moved to the Guest VLAN, "(Guest)" is appended to the VLAN ID.

Buttons

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

Refresh: Click to refresh the page immediately.

If you select port1 to display 802.1X Statistics.

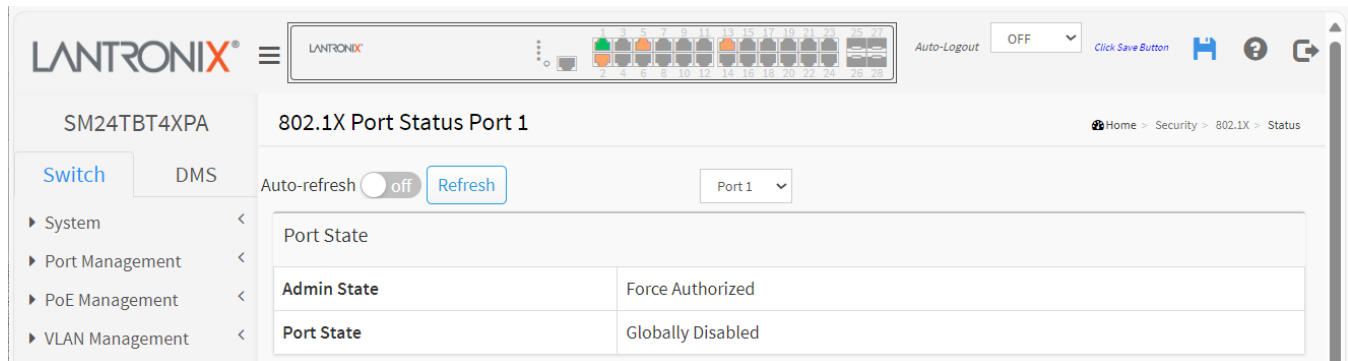


Figure 11-2.2: 802.1X Statistics Port 1

Parameter descriptions:

Port : You can select which port that you want display 802.1X Statistics.

Admin State : The port's current administrative state. Refer to 802.1X Admin State for a description of possible values.

Port State : The current state of the port. Refer to 802.1X Port State for a description of the individual states.

Buttons

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

Refresh: Click to refresh the page.

11-3 IP Source Guard

This section lets you configure IP Source Guard detail parameters.

11-3.1 Configuration

This section describes how to configure IP Source Guard settings including Mode (Enabled or Disabled) and Maximum Dynamic Clients (0, 1, 2, Unlimited).

To configure IP Source Guard parameters in the web UI:

1. Click Security, IP Source Guard, and Configuration.
2. Select “on” as the Mode of IP Source Guard Configuration.
3. Select “Enabled” of the specific port in the Mode of Port Mode Configuration.
4. Select Maximum Dynamic Clients (0, 1, 2, Unlimited) of the specific port in the Mode of Port Mode Configuration.
5. Click Apply.

LANTRONIX® SM24TBT4XPA

IP Source Guard Configuration

Auto-Logout: OFF

Click Save Button

Home > Security > IP Source Guard > Configuration

Switch DMS

System <

Port Management <

PoE Management <

VLAN Management <

QoS <

Spanning Tree <

MAC Address Tables <

Multicast <

DHCP <

Security >

» Management <

» 802.1X <

» IP Source Guard >

» Configuration >

» Static Tables <

Mode: on

Translate dynamic to static

Port Mode Configuration

| Port | Mode | Max Dynamic Clients |
|------|---------|---------------------|
| * | Enabled | 1 |
| 1 | Enabled | 1 |
| 2 | Enabled | 2 |
| 3 | Enabled | Unlimited |
| 4 | Enabled | Unlimited |
| 5 | Enabled | Unlimited |

Figure 11-3.1: IP Source Guard Configuration

Parameter descriptions:

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

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

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

Buttons

Apply: Click to save changes.

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

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

11-3.2 Static Table

This page lets you configure Static IP Source Guard parameters. To configure Static IP Source Guard parameters in the web UI:

1. Click Security, IP Source Guard, and Static Table.
2. Click "Add New Entry".
3. Specify the Port, VLAN ID, IP Address, and MAC address.
4. Click Apply.

The screenshot shows the Lantronix web interface for the SM24TBT4XPA device. The top navigation bar includes the Lantronix logo, a status bar with port indicators, and an auto-logout timer set to 10 minutes. The left sidebar shows the navigation menu with 'Switch' and 'DMS' tabs. The main content area is titled 'Static IP Source Guard Table' and includes a breadcrumb trail: Home > Security > IP Source Guard > Static Table. Below the title is a table with the following structure:

| Delete | Port | VLAN ID | IP Address | MAC address |
|--------------------------|------|---------|------------|-------------|
| <input type="checkbox"/> | 1 | 10 | | |

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

Figure 11-3.2: Static IP Source Guard Table

Parameter descriptions:

Port : The logical port for the settings.

VLAN ID: The VLAN ID (VID) for the settings.

IP Address : Allowed Source IP address.

MAC address : Allowed Source MAC address.

Buttons

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

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

Apply: Click to save changes.

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

11-3.3 Dynamic Table

Entries in the Dynamic IP Source Guard Table are shown on this page. The Dynamic IP Source Guard Table is sorted first by port, then by IP address, and then by MAC address.

To configure Dynamic IP Source Guard parameters in the web UI:

1. Click Security, IP Source Guard and Dynamic Table.
2. Check “Auto-refresh”.
3. Click “Refresh” to refresh the page.
4. Click First/Next Page to change pages.
5. Specify the Start from port, VLAN, IP Address, and entries per page.

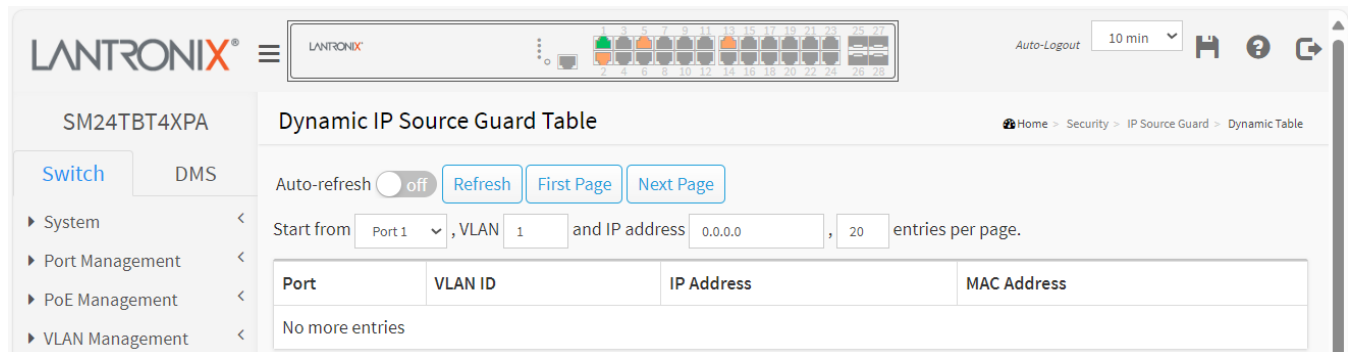


Figure 11-3.3: Dynamic IP Source Guard Table

Parameter descriptions:

Port : Switch Port Number for which the entries are displayed.

VLAN ID: The VLAN ID in which the IP traffic is permitted.

IP Address : User IP address of the entry.

MAC Address : The Source MAC address.

Show entries: You can choose how many items you want to show.

Buttons

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

Refresh: Click to refresh the page immediately.

First Page : Updates the table starting from the first entry in the Dynamic IP Source Guard Table.

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

11-4 ARP Inspection

This section describes to configure the ARP Inspection parameters of the switch. You could use the ARP Inspection configure to manage the ARP table.

11-4.1 Configuration

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

1. Click Security, ARP Inspection, and Configuration.
2. Select “on” as the Mode.
3. Select “Enabled” for the specific port(s) in the Mode of Port Mode Configuration.
4. Click Apply.

The screenshot shows the LANTRONIX web interface for the SM24TBT4XPA switch. The left sidebar contains navigation links for System, Port Management, PoE Management, VLAN Management, QoS, Spanning Tree, MAC Address Tables, Multicast, DHCP, Security, and Configuration. The main content area is titled 'ARP Inspection Configuration'. At the top, there is a 'Mode' section with a toggle switch set to 'on'. Below this is a button labeled 'Translate dynamic to static'. The 'Port Mode Configuration' table is as follows:

| Port | Mode | Check VLAN | Log Type |
|------|---------|------------|----------|
| * | <> | <> | <> |
| 1 | Enabled | Enabled | Deny |
| 2 | Enabled | Enabled | Permit |
| 3 | Enabled | Enabled | All |
| 4 | Enabled | Enabled | Permit |
| 5 | Enabled | Enabled | Deny |
| 6 | Enabled | Enabled | All |

Figure 11-4.1: ARP Inspection Configuration

Parameter descriptions:

Mode: Enable or disable Global ARP Inspection globally.

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. When "Check VLAN" is enabled, the log type of ARP Inspection will refer to the VLAN setting.

Possible "Check VLAN" settings are:

Enabled: Enable check VLAN operation.

Disabled: Disable check VLAN operation.

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

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

None: Log nothing.

Deny: Log denied entries.

Permit: Log permitted entries.

ALL: Log all entries.

Buttons

Apply: Click to save changes.

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

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

11-4.2 VLAN Configuration

Specify on which VLANs ARP Inspection is enabled. To configure VLAN Mode in the web UI:

1. Click Security, ARP Inspection, and VLAN Configuration.
2. Click "Add New Entry".
3. Specify the VLAN ID and Log Type.
4. Click Apply.
5. Click First Entry/Next Entry to change entries.

The screenshot shows the 'VLAN Mode Configuration' page in the Lantronix web UI. The left sidebar lists various configuration categories, with 'Security' expanded. The main area has a breadcrumb trail: Home > Security > ARP Inspection > VLAN Configuration. At the top of the main area are buttons for 'Refresh', 'First Entry', and 'Next Entry'. Below these is a text field 'Start from VLAN 1, 20 entries per page.' A table with three columns is shown: 'Delete', 'VLAN ID', and 'Log Type'. The table contains one entry with 'VLAN ID' 10 and 'Log Type' 'Permit'. Below the table are buttons for 'Delete', 'Add New Entry', 'Apply', and 'Reset'.

Figure 11-4.2: VLAN Mode Configuration

Parameter descriptions:

VLAN ID: Specify ARP Inspection is enabled on which VLANs. First, you must enable the port setting on Port mode configuration web page. Only when both Global Mode and Port Mode on a given port are enabled, ARP Inspection is enabled on this given port. Second, you can specify which VLAN will be inspected on VLAN mode configuration web page.

Log Type: The log type also can be configured on per VLAN setting. Possible types are:

None: Log nothing.

Deny: Log denied entries.

Permit: Log permitted entries.

ALL: Log all entries.

Buttons

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

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

Apply: Click to save changes.

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

First Entry: Updates the table starting from the first entry in the IPMC Profile Address Configuration.

Next Entry: Updates the table, starting with the entry after the last entry currently displayed.

Refresh: Click to refresh the page immediately.

11-4.3 Static Table

This page lets you configure Static ARP Inspection parameters. To configure Static ARP Inspection in the web UI:

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

The screenshot shows the Lantronix web interface for the SM24TBT4XPA device. The top navigation bar includes the Lantronix logo, a menu icon, a status bar with port indicators, and an auto-logout timer set to 10 minutes. The left sidebar shows the navigation menu with 'Switch' and 'DMS' tabs, and a list of configuration categories: System, Port Management, PoE Management, VLAN Management, and QoS. The main content area is titled 'Static ARP Inspection Table' and contains a table with the following structure:

| Delete | Port | VLAN ID | MAC Address | IP Address |
|--------------------------|------|---------|-------------|------------|
| <input type="checkbox"/> | 1 | 10 | | |

Below the table, there are three buttons: 'Add New Entry', 'Apply', and 'Reset'. The breadcrumb trail at the top right indicates the path: Home > Security > ARP Inspection > Static Table.

Figure11-4.3: Static ARP Inspection Table

Parameter descriptions:

Port : The logical port for the settings.

VLAN ID: The VLAN ID (VID) for the settings.

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

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

Buttons

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

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

Apply: Click to save changes.

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

11-4.4 Dynamic Table

Entries in the Dynamic ARP Inspection Table are shown on this page. The Dynamic ARP Inspection Table contains up to 256 entries, and is sorted first by port, then by VLAN ID, then by MAC address, and then by IP address. All dynamic entries are learned from DHCP Snooping.

To configure Dynamic ARP Inspection in the web UI:

1. Click Security, ARP Inspection, and Dynamic Table.
2. Check "Auto-refresh".
3. Click "Refresh" to refresh the port detailed statistics.
4. Click First/Next Page to change pages.
5. Specify the Start from port, VLAN, MAC Address, IP Address, and entries per page.

The screenshot shows the Lantronix web interface for the SM24TBT4XPA device. The main content area is titled "Dynamic ARP Inspection Table". It includes an "Auto-refresh" toggle set to "off", and buttons for "Refresh", "First Page", and "Next Page". Below these are input fields for "Start from" (Port 1), "VLAN" (1), "MAC address" (00-00-00-00-00-00), and "IP address" (0.0.0.0), followed by a "20" entries per page selector. A "System Configuration" section contains a table with headers: Port, VLAN ID, MAC Address, IP Address, and Translate to static. The table currently shows "No more entries". At the bottom are "Apply" and "Reset" buttons.

Figure 11-4.4: Dynamic ARP Inspection Table

Parameter descriptions:

Port: Switch Port Number for which the entries are displayed.

VLAN ID: VLAN ID in which the ARP traffic is permitted.

MAC Address: User MAC address of the entry.

IP Address: User IP address of the entry.

Show entries: Choose how many items you want to display.

Buttons

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

Refresh: Click to refresh the page immediately.

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

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

11-5 Port Security

11-5.1 Configuration

This page lets you configure switch Port Security settings. You can use the Port Security feature to restrict input to an interface by limiting and identifying MAC addresses. To configure Port Security in the web UI:

1. Click Security, Port Security and Configuration.
2. Click to Enable the Aging to specify Aging Period.
3. Set Mode(Enabled, Disabled), Limit, Violation Mode, Violation Limit for each port.
4. Click the Apply to save the setting.
5. To cancel the settings click the Reset button. It will revert to previously saved values.

Port Security Configuration

System Configuration

Aging Enabled: ☒ on

Aging Period: 3600 seconds

Hold Time: 300 seconds

Port Configuration

| Port | Mode | Limit | Violation Mode | Violation Limit | State | Re-open | Sticky | Clear |
|------|---------|-------|----------------|-----------------|-------|---------|---------|-------|
| * | <> | 4 | <> | 4 | | | <> | |
| 1 | Enabled | 4 | Protect | 4 | Ready | Reopen | Enabled | Clear |
| 2 | Enabled | 2 | Restrict | 4 | Ready | Reopen | Enabled | Clear |
| 3 | Enabled | 8 | Shutdown | 4 | Ready | Reopen | Enabled | Clear |
| 4 | Enabled | 6 | Protect | 4 | Ready | Reopen | Enabled | Clear |
| 5 | Enabled | 4 | Protect | 4 | Ready | Reopen | Enabled | Clear |
| 6 | Enabled | 4 | Protect | 4 | Ready | Reopen | Enabled | Clear |
| 7 | Enabled | 4 | Protect | 4 | Ready | Reopen | Enabled | Clear |

Figure 11-5.1: Port Security Configuration

System Configuration

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

Aging Period: If Aging Enabled is checked, then the aging period is controlled with this input. If other modules are using the underlying functionality for securing MAC addresses, they may have other requirements to the aging period. The underlying functionality will use the shorter requested aging period of all modules that have aging enabled. The Aging Period can be set to a number between 10 and 10000000 seconds with a default of 3600 seconds.

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

Hold Time: The hold time -measured in seconds -is used to determine how long a MAC address is held in the MAC table if it has been found to violate the limit. Valid range is between 10 and 1000000 seconds with a default of 300 seconds. The reason for holding a violating MAC address in the MAC table is primarily to ensure that the same MAC address doesn't give rise to continuous notifications (if notifications on violation count is enabled).

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

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

Protect: Do not allow more than Limit MAC addresses on the port, but take no further action.

Restrict: If Limit is reached, subsequent MAC addresses on the port will be counted and marked as violating. Such MAC addresses are removed from the MAC table when the hold time expires. At most Violation Limit MAC addresses can be marked as violating at any given time.

Shutdown: If Limit is reached, one additional MAC address will cause the port to be shut down. This implies that all secured MAC addresses be removed from the port, and no new addresses be learned.

There are three ways to re-open the port: 1) In the "Configuration > Ports" page's "Configured" column, first disable the port, then restore the original mode. 2) Make a Port Security configuration change on the port. 3) Boot the switch.

Violation Limit: The maximum number of MAC addresses that can be marked as violating on this port. This number cannot exceed 1023. Default is 4. It is only used when Violation Mode is Restrict.

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

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

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

Limit Reached: Indicates that the limit is reached on this port. This state 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.

Buttons

Apply: Click to save changes.

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

11-5.2 Status

This page shows the Port Security status. Port Security is a module with no direct configuration. Configuration comes indirectly from other modules - the user modules. When a user module has enabled port security on a port, the port is set-up for software-based learning. In this mode, frames from unknown MAC addresses are passed on to the port security module, which in turn asks all user modules whether to allow this new MAC address to forward or block it. For a MAC address to be set in the forwarding state, all enabled user modules must unanimously agree on allowing the MAC address to forward. If only one chooses to block it, it will be blocked until that user module decides otherwise. The status page is divided into two sections - one with a legend of user modules and one with the actual port status.

To display Port Security Status in the web UI:

1. Click Security, Port Security, and status.
2. Check "Auto-refresh".
3. Click "Refresh" to refresh the port detailed statistics.
4. Click the port number to see the status for this particular port.

The screenshot shows the Lantronix web interface for the SM24TBT4XPA device. The left sidebar contains a navigation menu with categories like System, Port Management, PoE Management, VLAN Management, QoS, Spanning Tree, MAC Address Tables, Multicast, DHCP, Security, and Management. The 'Security' category is expanded, showing 'Port Security' and its sub-items 'Configuration' and 'Status'. The 'Status' item is selected.

The main content area is titled 'Port Security Status'. It features an 'Auto-refresh' toggle set to 'off' and a 'Refresh' button. Below this is a table titled 'Port Status' with the following data:

| Port | Violation Mode | State | MAC Count | | |
|------|----------------|---------------|-----------|-----------|-------|
| | | | Current | Violating | Limit |
| 1 | Protect | Limit Reached | 4 | 0 | 4 |
| 2 | Restrict | Ready | 1 | 0 | 2 |
| 3 | Shutdown | Ready | 0 | 0 | 8 |
| 4 | Protect | Ready | 0 | 0 | 6 |
| 5 | Protect | Ready | 1 | 0 | 4 |
| 6 | Protect | Ready | 0 | 0 | 4 |
| 7 | Protect | Ready | 0 | 0 | 4 |
| 8 | Protect | Ready | 0 | 0 | 4 |
| 9 | Protect | Ready | 0 | 0 | 4 |
| 10 | Protect | Ready | 0 | 0 | 4 |
| 11 | Protect | Ready | 0 | 0 | 4 |

Figure 11-5.2: Port Security Status

Parameter descriptions:

Port : The port number for which the status applies. Click the port number to see the status for this particular port.

Violation Mode: Shows the configured Violation Mode of the port. It can take one of four values:

Disabled: Port Security is not administratively enabled on this port.

Protect: Port Security is administratively enabled in Protect mode.

Restrict: Port Security is administratively enabled in Restrict mode.

Shutdown: Port Security is administratively enabled in Shutdown mode.

State : Shows the current state of the port. It can take one of four values:

Disabled: No user modules are currently using the Port Security service.

Ready: The Port Security service is in use by at least one user module, and is awaiting frames from unknown MAC addresses to arrive.

Limit Reached: The Port Security service is 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, Violating, Limit): The three columns indicate the number of currently learned MAC addresses (forwarding as well as blocked), the number of violating MAC address (only counting in Restrict mode) and the maximum number of MAC addresses that can be learned on the port, respectively. If no user modules are enabled on the port, the Current column will show a dash (-). If Port Security is not administratively enabled on the port, the Violating and Limit columns will show a dash (-).

Buttons

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

Refresh: Click to refresh the page immediately.

Click the port number to see the status for that particular port:

LANTRONIX SM24TBT4XPA Port Security Status Port 1

Auto-refresh ☐ off Refresh Clear Port 1 Back

User Module Legend

| MAC Address | VLAN ID | State | Time of Addition | Age/Hold |
|-------------------|---------|------------|---------------------------|----------|
| 5c-ff-35-dc-0a-c1 | 1 | Forwarding | 2016-01-01T00:11:38+00:00 | - |
| 88-a4-c2-63-ce-a4 | 1 | Forwarding | 2016-01-01T00:11:38+00:00 | - |
| b0-83-fe-71-39-54 | 1 | Forwarding | 2016-01-01T00:11:39+00:00 | - |
| ff-ff-ff-ff-ff-ff | 1 | Forwarding | 2016-01-01T00:11:39+00:00 | - |

Figure 11-5.2: Port Security Status

Parameter descriptions:

MAC Address & VLAN ID : The MAC address and VLAN ID that is seen on this port. If no MAC addresses are learned, a single row stating "No MAC addresses attached" is displayed.

State : Indicates whether the corresponding MAC address is blocked or forwarding. In the blocked state, it will not be allowed to transmit or receive traffic.

Time of Addition : Shows the date and time when this MAC address was first seen on the port.

Age/Hold : If at least one user module has decided to block this MAC address, it will stay in the blocked state until the hold time (measured in seconds) expires. If all user modules have decided to allow this MAC address to forward, and aging is enabled, the Port Security module will periodically check that this MAC address still forwards traffic. If the age period (measured in seconds) expires and no frames have been seen, the MAC address will be removed from the MAC table. Otherwise a new age period will begin.

If aging is disabled or a user module has decided to hold the MAC address indefinitely, a dash (-) will be shown.

Buttons

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

Refresh: Click to refresh the page immediately.

Clear : Click to remove this particular MAC addresses from MAC table.

Port: Select port that you want to display the Port Security Status.

Back : Click to go back to the Port Security Status page.

11-6 RADIUS

11-6.1 Configuration

Up to 5 RADIUS servers are supported. To configure a RADIUS server in the web UI:

1. Click Security, RADIUS, and Configuration.
2. Set Timeout, Retransmit, Deadtime, Key, NAS-IP-Address, NAS IPv6-Address, NAS-Identifier.
3. Click “Add New Entry”.
4. Set Hostname, Auth Port, Acct Port, Timeout, Retransmit, Key.
5. Click the Apply to save the setting.
6. To cancel the settings click the Reset button to revert to previously saved values.

Figure 11-6.1: RADIUS Server Configuration

Parameter descriptions:

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

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

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

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

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

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

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

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

Server Configuration: The table has one row for each RADIUS server and a number of columns, which are:

Hostname: The IP address or hostname of the RADIUS server.

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

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

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

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

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

Buttons

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

Add New Entry : 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 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.

11-6.2 Status

This page shows an overview and details of the RADIUS Authentication and Accounting servers' status. To display RADIUS Server Status in the web UI:

1. Click Security, RADIUS, and Status.
2. View the displayed RADIUS server status.

RADIUS Server Status Home > Security > RADIUS > Status

Auto-refresh ☐ off [Refresh](#)

| # | IP Address | Authentication Port | Authentication Status | Accounting Port | Accounting Status |
|---|------------|---------------------|-----------------------|-----------------|-------------------|
| 1 | | | Disabled | | Disabled |
| 2 | | | Disabled | | Disabled |
| 3 | | | Disabled | | Disabled |
| 4 | | | Disabled | | Disabled |
| 5 | | | Disabled | | Disabled |

Figure 11-6.2: RADIUS Server Status Overview

Parameter descriptions:

: 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.

Authentication Port: The UDP port number for authentication.

Authentication Status: The current status of the server. This field takes one of the following values:

Disabled: The RADIUS server is disabled.

Not Ready: The server is enabled, but IP communication is not yet up and running.

Ready: The RADIUS server is enabled, IP communication is up and running, and the RADIUS module is ready to accept access attempts.

Dead (X seconds left): Access attempts were made to this 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 RADIUS server is enabled.

Accounting Port: UDP port number for accounting.

Accounting Status: The current status of the server. This field takes one of the following values:

Disabled: The RADIUS server is disabled.

Not Ready: The server is enabled, but IP communication is not yet up and running.

Ready: The RADIUS server is enabled, IP communication is up and running, and the RADIUS module is ready to accept access attempts.

Dead (X seconds left): Access attempts were made to this 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 RADIUS server is enabled.

Buttons

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

Refresh: Click to refresh the page immediately.

If you select Server#1 to display RADIUS Statistics:

Timeouts: The number of authentication timeouts to the server. After a timeout, the client may retry to the same server, send to a different server, or give up. A retry to the same server is counted as a retransmit as well as a timeout. A send to a different server is counted as a Request as well as a timeout.

IP Address: The IP address and UDP port for the authentication server in question.

State: Shows the state of the server. It takes one of the following values:

Disabled : The selected server is disabled.

Not Ready: The server is enabled, but IP communication is not yet up and running.

Ready: The server is enabled, IP communication is up and running, and the RADIUS module is ready to accept access attempts.

Dead (X seconds left): Access attempts were made to this server, but it did not reply within the configured timeout. The server has temporarily been disabled, but will get re-enabled when the dead-time expires. The number of seconds left before this occurs is displayed in parentheses. This state is only reachable when more than one server is enabled.

Round-Trip Time: The time interval (measured in milliseconds) between the most recent Access-Reply/Access-Challenge and the Access-Request that matched it from the RADIUS authentication server. The granularity of this measurement is 100 ms. A value of 0 ms indicates that there hasn't been round-trip communication with the server yet.

RADIUS Accounting Statistics for Server #1: The statistics map closely to those specified in RFC4670 -RADIUS Accounting Client MIB. Use the server select box to switch between the backend servers to show details for.

Responses: The number of RADIUS packets (valid or invalid) received from the server.

Malformed Responses: The number of malformed RADIUS packets received from the server. Malformed packets include packets with an invalid length. Bad authenticators or unknown types are not included as malformed access responses.

Bad Authenticators: The number of RADIUS packets containing invalid authenticators received from the server.

Unknown Types: The number of RADIUS packets of unknown types that were received from the server on the accounting port.

Packets Dropped: The number of RADIUS packets that were received from the server on the accounting port and dropped for some other reason.

Requests: The number of RADIUS packets sent to the server. This does not include retransmissions

Retransmissions: The number of RADIUS packets retransmitted to the RADIUS accounting server.

Pending Requests: The number of RADIUS packets destined for the server that have not yet timed out or received a response. This variable is incremented when a Request is sent and decremented due to receipt of a Response, timeout, or retransmission.

Timeouts: The number of accounting timeouts to the server. After a timeout, the client may retry to the same server, send to a different server, or give up. A retry to the same server is counted as a retransmit as well as a timeout. A send to a different server is counted as a Request as well as a timeout.

IP Address: IP address and UDP port for the accounting server in question.

State: Shows the state of the server. It takes one of the following values:

Disabled: The selected server is disabled.

Not Ready: The server is enabled, but IP communication is not yet up and running.

Ready: The server is enabled, IP communication is up and running, and the RADIUS module is ready to accept accounting attempts.

Dead (X seconds left): Accounting attempts were made to this server, but it did not reply within the configured timeout. The server has temporarily been disabled, but will get re-enabled when the dead-time expires. The number of seconds left before this occurs is displayed in parentheses. This state is only reachable when more than one server is enabled.

Round-Trip Time: The time interval (measured in milliseconds) between the most recent Response and the Request that matched it from the RADIUS accounting server. The granularity of this measurement is 100 ms. A value of 0 ms indicates that there hasn't been round-trip communication with the server yet.

Buttons

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

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.

11-7 TACACS+

This page allows you to configure up to 5 TACACS+ servers. To configure TACACS+ servers in the web UI:

1. Click Security and TACACS+.
2. Click "Add New Entry".
3. Specify the Timeout, Deadtime, and Key.
4. Specify the Hostname, Port, Timeout and Key in the server.
5. Click Apply.

The screenshot shows the Lantronix web interface for the SM24TBT4XPA device. The left sidebar contains a navigation menu with categories like System, Port Management, PoE Management, VLAN Management, QoS, Spanning Tree, MAC Address Tables, Multicast, DHCP, Security, Management, 802.1X, IP Source Guard, and ARP Inspection. The 'Security' category is expanded, showing 'TACACS+' as a sub-option. The main content area is titled 'TACACS+ Server Configuration'. It features a 'Global Configuration' section with three fields: 'Timeout' set to 5 seconds, 'Deadtime' set to 0 minutes, and 'Key' masked with asterisks. Below this is a 'Server Configuration' table with five columns: 'Delete', 'Hostname', 'Port', 'Timeout', and 'Key'. The table has one row with the following values: an unchecked checkbox in the 'Delete' column, '192.168.1.99' in the 'Hostname' column, '49' in the 'Port' column, '50' in the 'Timeout' column, and a masked key in the 'Key' column. Below the table are buttons for 'Add New Server', 'Apply', and 'Reset'.

Figure 11-7: TACACS+ Server Configuration

Parameter descriptions:

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

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

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

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

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

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

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

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

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

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

Buttons

Delete: This button can be used to undo the addition of the new server.

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.

Apply: Click to save changes.

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

12. Access Control

12-1 Ports Configuration

Here you can configure the ACL parameters (ACE) of each switch port. These parameters will affect frames received on a port unless the frame matches a specific ACE. To configure the ACL Ports in the web UI:

1. Click Access Control and Port Configuration.
2. Select the desired value for port ACL setting.
3. Click the Apply button to save the settings.
4. To cancel the settings click the reset button to revert to previously saved values.
5. When configuration is complete you can view the port counters and then click Refresh to update the counters or click Clear to reset the counters.

| Port | Policy ID | Action | Rate Limiter ID | Port Redirect | Mirror | Logging | Shutdown | State | Counter |
|------|-----------|--------|-----------------|------------------------------|----------|----------|----------|---------|---------|
| * | 0 | <> | <> | Disabled Port 1 Port 2 | <> | <> | <> | <> | * |
| 1 | 0 | Permit | 1 | Disabled Port 1 Port 2 | Disabled | Disabled | Disabled | Enabled | 7200 |
| 2 | 0 | Permit | 1 | Disabled Port 1 Port 2 | Disabled | Disabled | Disabled | Enabled | 261 |
| 3 | 0 | Permit | 1 | Disabled Port 1 Port 2 | Disabled | Disabled | Disabled | Enabled | 0 |
| 4 | 0 | Permit | 1 | Disabled Port 1 Port 2 | Disabled | Disabled | Disabled | Enabled | 0 |

Figure 12-1: ACL Ports Configuration

Parameter descriptions:

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

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

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

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

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

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

Enabled: Frames received on the port are mirrored.

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

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

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

Disabled: Frames received on the port are not logged.

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

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

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

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

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

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

Disabled: To close ports by changing the volatile port configuration of the ACL user module.

The default value is "Enabled"

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

Buttons

Refresh: Click to update the webpage.

Clear: Clears the counters for the selected server.

Apply: Click to save changes.

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

12-2 Rate Limiters

This page lets you configure the switch's ACL Rate Limiter parameters. The Rate Limiter Level lets you set rate limiter value and units.

To configure ACL Rate Limiter parameters in the web UI:

1. Click Access Control and Rate Limiters.
2. Set the specific Rate and Unit.
3. Click the Apply button to save the settings.
4. To cancel the settings click the reset button. It will revert to previously saved values.

The screenshot shows the Lantronix web interface for the SM24TBT4XPA switch. The 'Access Control' menu is expanded, and 'Rate Limiters' is selected. The 'ACL Rate Limiter Configuration' page displays a table with 8 rows, each representing a rate limiter. The 'Rate Limiter ID' column contains values from 1 to 8. The 'Rate' column contains the value 1 for all entries. The 'Unit' column contains the value 10pps for all entries. The interface includes a sidebar with various configuration options and a top navigation bar with the Lantronix logo and status indicators.

| Rate Limiter ID | Rate | Unit |
|-----------------|------|-------|
| * | 1 | <> |
| 1 | 1 | 10pps |
| 2 | 1 | 10pps |
| 3 | 1 | 10pps |
| 4 | 1 | 10pps |
| 5 | 1 | 10pps |
| 6 | 1 | 10pps |
| 7 | 1 | 10pps |
| 8 | 1 | 10pps |

Figure 12-2: ACL Rate Limiter Configuration

Parameter descriptions:

Rate Limiter ID : The rate limiter ID for the settings contained in the same row and its range is 1 - 16.

Rate : The valid rate is 0,10,20,30, ...,5000000 in pps or 0,25,50,75, ...,10000000 in kbps.

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

10pps: packets per second.

25kbps: Kbits per second.

Buttons


Apply: Click to save changes.

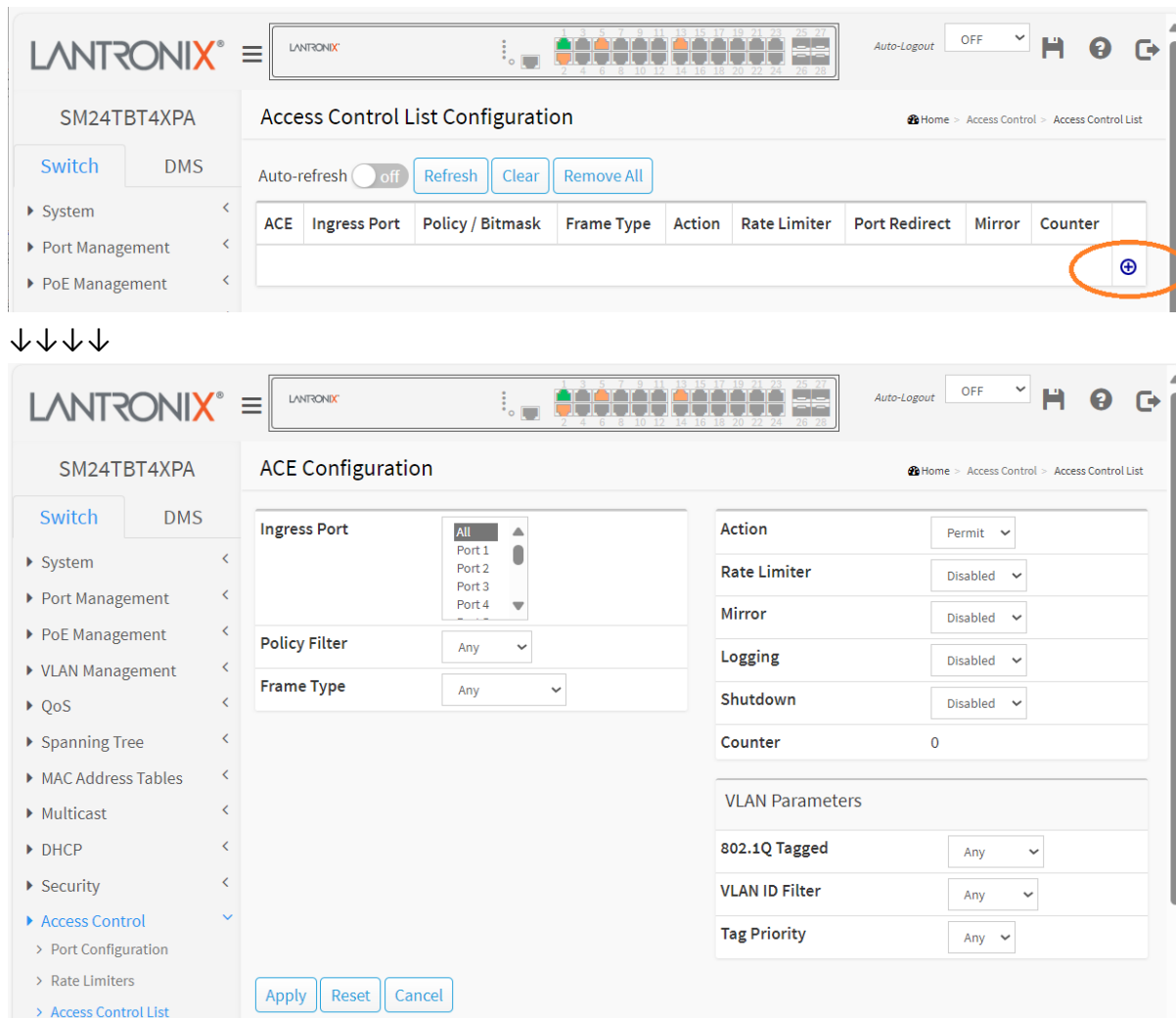
Reset: Click to undo any changes made locally and revert to previously saved values.

12-3 Access Control List

This page shows the Access Control List (ACL), which is made up of the ACEs defined on this switch. Each row describes the ACE that is defined. The maximum number of ACEs is 512 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 Access Control and Access Control List.
2. Click the  button to add a new ACL, or use the other ACL modification buttons to specify the editing action (i.e., edit, delete, or moving the relative position of entry in the list)
3. Specify the ACE parameters.
4. Click the Apply button to save the settings.
5. To cancel the settings click the reset button. It 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).



The top screenshot shows the 'Access Control List Configuration' page. It features a table with columns: ACE, Ingress Port, Policy / Bitmask, Frame Type, Action, Rate Limiter, Port Redirect, Mirror, and Counter. A plus button is circled in orange at the bottom right of the table. The bottom screenshot shows the 'ACE Configuration' page, which is a detailed form for configuring a specific ACE. It includes sections for Ingress Port (a dropdown menu), Policy Filter (Any), Frame Type (Any), Action (Permit), Rate Limiter (Disabled), Mirror (Disabled), Logging (Disabled), Shutdown (Disabled), Counter (0), and VLAN Parameters (802.1Q Tagged, VLAN ID Filter, Tag Priority).

Figure 12-3: Access Control List Configuration

Parameter descriptions:

ACE: Indicates the ACE ID.

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

Any: The ACE will match any ingress port.

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

Port: The ACE will match a specific ingress port.

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

Frame Type : Indicates the frame type of the ACE. Possible values are:

Any: The ACE will match any frame type.

EType: The ACE will match Ethernet Type frames. Note that an Ethernet Type based ACE will not get matched by IP and ARP frames.

ARP: The ACE will match ARP/RARP frames.

IPv4: The ACE will match all IPv4 frames.

IPv4/ICMP: The ACE will match IPv4 frames with ICMP protocol.

IPv4/UDP: The ACE will match IPv4 frames with UDP protocol.

IPv4/TCP: The ACE will match IPv4 frames with TCP protocol.

IPv4/Other: The ACE will match IPv4 frames, which are not ICMP/UDP/TCP.

IPv6: The ACE will match all IPv6 standard frames.

Action : Indicates the forwarding action of the ACE.

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

Deny: Frames matching the ACE are dropped.

Filter: Frames matching the ACE are filtered.

Rate Limiter : Indicates the rate limiter number of the ACE. The allowed range is 1 to 16. When Disabled is displayed, the rate limiter operation is disabled.

Port Redirect: Indicates the port redirect operation of the ACE. Frames matching the ACE are redirected to the port number. The allowed values are Disabled or a specific port number. When Disabled is displayed, the port redirect operation is disabled.

Mirror: Specify the mirror operation of this port. Frames matching the ACE are mirrored to the destination mirror port. The allowed values are:

Enabled: Frames received on the port are mirrored.

Disabled: Frames received on the port are not mirrored.

The default value is "Disabled".

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

Modification Buttons : You can modify each ACE 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.

ACE Configuration: An ACE consists of several parameters. These parameters vary according to the frame type that you select. First select the ingress port for the ACE, and then select the frame type. Different parameter options are displayed depending on the frame type selected.

A frame that hits this ACE matches the configuration that is defined here.

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

All: The ACE applies to all port.

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

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

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

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

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. Note the ARP frames won't match the ACE with ethernet type.

IPv4: Only IPv4 frames can match this ACE. Note the IPv4 frames won't match the ACE with ethernet type.

IPv6: Only IPv6 frames can match this ACE. Note 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 a 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. Can be:

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 help file.

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

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

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.

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

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

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

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

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

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

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

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

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

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

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

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

ICMP Parameters

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

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

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

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

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

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

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

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

TCP/UDP Parameters

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Buttons

Apply: Click to save changes.

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

Auto-refresh: Check to automatically refresh the information every 3 seconds.

Refresh: Click to manually refresh the page immediately.

Clear: Click to clear the ACL data.

Remove All : Remove all ACL configurations on the table.

Cancel : Click to return to the previous page.

12-4 ACL Status

This page displays ACL status by different ACL users. Each row describes an ACE that is defined. It is a Conflict if a specific ACE is not applied to the hardware due to hardware limitations. The maximum number of ACEs is 512 per switch. To display ACL Status in the web UI:

1. Click Access Control and ACL Status.
2. At the User select dropdown select the desired user set.
3. To automatically refresh the information every 3 seconds check the “Auto-refresh” checkbox.
4. Click “Refresh” to refresh the ACL Status.

The screenshot shows the Lantronix web interface for the SM24TBT4XPA device. The left sidebar contains a navigation menu with options like System, Port Management, PoE Management, VLAN Management, QoS, Spanning Tree, MAC Address Tables, Multicast, DHCP, Security, and Access Control. The main content area is titled 'ACL Status' and features an 'Auto-refresh' toggle set to 'off' and a 'Refresh' button. Below this is a table with the following columns: User, ACE, Ingress Port, Frame Type, Action, Rate Limiter, Port Redirect, Mirror, CPU, CPU Once, Counter, and Conflict. The table contains five rows of data:

| User | ACE | Ingress Port | Frame Type | Action | Rate Limiter | Port Redirect | Mirror | CPU | CPU Once | Counter | Conflict |
|------------|-----|--------------|-------------------------|--------|--------------|---------------|----------|-----|----------|---------|----------|
| DMS mDNS | 1 | All | IPv4/UDP 5353 | Permit | Disabled | Disabled | Disabled | Yes | No | 3366 | No |
| DMS Onvif | 1 | All | IPv4/UDP 10100-10227 | Permit | Disabled | Disabled | Disabled | Yes | No | 1268 | No |
| DMS SSDP | 1 | All | IPv4/UDP 1900 | Permit | Disabled | Disabled | Disabled | Yes | No | 9710 | No |
| DMS CLIENT | 1 | All | IPv4/UDP 10012 | Permit | Disabled | Disabled | Disabled | Yes | No | 0 | No |
| dhcp | 1 | All | IPv4/UDP 67 DHCP Client | Deny | Disabled | Disabled | Disabled | Yes | No | 59 | No |

Figure 12-4: ACL Status

Parameter descriptions:

User : Indicates the ACL user.

ACE: Indicates the ACE ID on local switch.

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

All: The ACE will match all ingress port.

Port: The ACE will match a specific ingress port.

Frame Type : Indicates the frame type of the ACE. Possible values are:

Any: The ACE will match any frame type.

EType: The ACE will match Ethernet Type frames. Note that an Ethernet Type based ACE will not get matched by IP and ARP frames.

ARP: The ACE will match ARP/RARP frames.

IPv4: The ACE will match all IPv4 frames.

IPv4/ICMP: The ACE will match IPv4 frames with ICMP protocol.

IPv4/UDP: The ACE will match IPv4 frames with UDP protocol.

IPv4/TCP: The ACE will match IPv4 frames with TCP protocol.

IPv4/Other: The ACE will match IPv4 frames, which are not ICMP / UDP / TCP.

IPv6: The ACE will match all IPv6 standard frames.

Action : Indicates the forwarding action of the ACE. Can be:

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 - 16. When Disabled is displayed, the rate limiter operation is disabled.

Port Redirect: Indicates the port redirect operation of the ACE. Frames matching the ACE are redirected to the port number. The allowed values are Disabled or a specific port number. When Disabled is displayed, the port redirect operation is disabled.

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

Enabled: Frames received on the port are mirrored.

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

CPU : Forward packet that matched the specific ACE to CPU.

CPU Once: Forward first packet that matched the specific ACE to CPU.

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

Conflict : Indicates the hardware status of the specific ACE. The specific ACE is not applied to the hardware due to hardware limitations.

Buttons

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

Refresh: Click to manually refresh the page immediately.

13. SNMP

Any Network Management System (NMS) running the Simple Network Management Protocol (SNMP) can manage managed devices equipped with SNMP agent, provided that the Management Information Base (MIB) is installed correctly on the managed devices. SNMP is a protocol 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. An SNMP agent is running on the switch in response to a request issued by an SNMP manager.

Basically, it is passive except issuing the trap information. The switch supports a switch to turn on or off the SNMP agent. If you set the field SNMP “Enable”, SNMP agent will be started up. 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.

13-1 Configuration

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 function. An SNMP manager must pass the authentication by identifying both community names, then it can access the MIB information of the target device. So both parties must have the same community name. Once completing the settings click the Apply button and the settings takes effect.

To configure the configure SNMP System in the web UI:

1. Click SNMP and configuration.
2. Enable or Disable the SNMP function.
3. Specify the Read Community and the Write Community.
4. Click Apply.

The screenshot shows the Lantronix web interface for the SM24TBT4XPA switch. The top navigation bar includes the Lantronix logo, a menu icon, a status bar with 28 ports (ports 1-12 are green, 13-28 are grey), and an 'Auto-Logout' dropdown set to 'OFF'. The sidebar on the left has 'Switch' and 'DMS' tabs, with a list of configuration categories: System, Port Management, PoE Management, VLAN Management, and QoS. The main content area is titled 'SNMPv1/v2c Configuration'. It contains a 'Mode' section with a toggle switch set to 'on'. Below this are two rows for community configuration: 'Read Community' with a text input 'public' and a dropdown 'Enabled', and 'Write Community' with a text input 'private' and a dropdown 'Enabled'. At the bottom of the configuration area are 'Apply' and 'Reset' buttons. A breadcrumb trail at the top right reads 'Home > SNMP > SNMPv1/v2c'.

Figure 13-1: SNMP Configuration

Parameter descriptions:

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

on: Enable SNMP mode operation.

off: Disable SNMP mode operation.

Read Community: Indicates the community read access string to permit access to SNMP agent. The allowed string length is 1 - 31 characters, and the allowed content is ASCII characters 33 - 126. The field is applicable only when SNMP version is SNMPv1 or SNMPv2c. If SNMP version is SNMPv3, the community string will be associated with SNMPv3 communities table. It provides more flexibility to configure security name than a SNMPv1 or SNMPv2c community string. In addition to community string, a particular range of source addresses can be used to restrict source subnet.

Write Community: Indicates the community write access string to permit access to SNMP agent. The allowed string length is 1 to 31 characters, and the allowed content is ASCII characters 33 - 126. The field is applicable only when SNMP version is SNMPv1 or SNMPv2c. If SNMP version is SNMPv3, the community string will be associated with SNMPv3 communities table. It provides more flexibility to configure security name than a SNMPv1 or SNMPv2c community string. In addition to community string, a particular range of source addresses can be used to restrict source subnet.

Buttons

Apply: Click to save changes.

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

13-2 SNMPv3

13-2.1 Communities

Configure the SNMPv3 community table on this page. The entry index key is Community. To configure SNMP Communities in the web UI:

1. Click SNMP, SNMPv3, and Communities.
2. Click Add New Entry.
3. Specify the SNMP community parameters.
4. Click Apply.

| Delete | Community | Source IP | Source Mask |
|---------------------------------------|-----------|-----------|-------------|
| <input type="button" value="Delete"/> | v3Cmty1 | 0.0.0.0 | 0.0.0.0 |
| <input type="button" value="Delete"/> | | 0.0.0.0 | 0.0.0.0 |

Figure 13-2.1: SNMPv3 Community Configuration

Parameter descriptions:

Community: Indicates the security name to map the community to the SNMP Groups configuration. The allowed string length is 1 - 32 characters, and the allowed content is ASCII characters 33 - 126.

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

Source Mask: Indicates the SNMP access source address prefix.

Buttons

Add New Entry : Click to add new entry. Specify the name and configure the new entry. Click "Apply".

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

Apply: Click to save changes.

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

13-2.2 Users

This page lets you configure SNMPv3 users. The Entry index key is UserName. To create a new UserName account, click the Add New User button, and enter the user information then click Apply. Max Users number: 6.

To configure SNMP Users in the web UI:

1. Click SNMP, SNMPv3 and Users.
2. Click Add new entry.
3. Specify the SNMPv3 Users parameter.
4. Click Apply.

The screenshot shows the Lantronix SM24TBT4XPA web interface. The top navigation bar includes the Lantronix logo, a status bar with various indicators, and an 'Auto-Logout' dropdown set to 'OFF'. The left sidebar contains a 'Switch' tab and a 'DMS' section with expandable menu items: System, Port Management, PoE Management, VLAN Management, QoS, Spanning Tree, and MAC Address Tables. The main content area is titled 'SNMPv3 User Configuration' and features a breadcrumb trail: Home > SNMP > SNMPv3 > Users. Below the title is a table with the following columns: Delete, Engine ID, User Name, Security Level, Authentication Protocol, Authentication Password, Privacy Protocol, and Privacy Password. The table contains one entry with Engine ID '800014550300c0f2a8a3bd', User Name 'admn', Security Level 'Auth, Priv', Authentication Protocol 'MD5', and Privacy Protocol 'DES'. Below the table are buttons for 'Delete', 'Add New Entry', 'Apply', and 'Reset'.

Figure 13-2.2: SNMPv3 Users Configuration

Parameter descriptions:

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

User Name : A string identifying the user name that this entry should belong to. The allowed string length is 1 - 31 characters, and the allowed content is ASCII characters 33 - 126.

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

NoAuth, NoPriv: No authentication and no privacy.

Auth, NoPriv: Authentication and no privacy.

Auth, Priv: Authentication and privacy.

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

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

MD5: An optional flag to indicate that this user uses MD5 authentication protocol.

SHA: An optional flag to indicate that this user uses SHA authentication protocol.

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

Authentication Password : A string identifying the authentication password phrase. For MD5 authentication protocol, the allowed string length is 8 to 39. For SHA authentication protocol, the allowed string length is 8 to 39 characters. The allowed content is ASCII characters 33 - 126.

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

DES: An optional flag to indicate that this user uses DES authentication protocol.

AES: An optional flag to indicate that this user uses AES authentication protocol.

Privacy Password : A string identifying the privacy password phrase. The allowed string length is 8 to 31 characters, and the allowed content is ASCII characters 33 - 126.

Buttons

Add New Entry : Click to add new entry. Specify the name and configure the new entry. Click "Apply".

Delete : Check to delete the entry.

Apply: Click to save changes.

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

13-2.3 Groups

The function is used to configure SNMPv3 group. The Entry index key are Security Model and Security Name. To create a new group account, click the Add New Group button, an enter the group information then click Apply. The max Group number is 12. To configure SNMP Groups in the web UI:

1. Click SNMP, SNMPv3, and Groups.
2. Click Add new entry.
3. Specify the SNMP group parameter.
4. Click Apply.

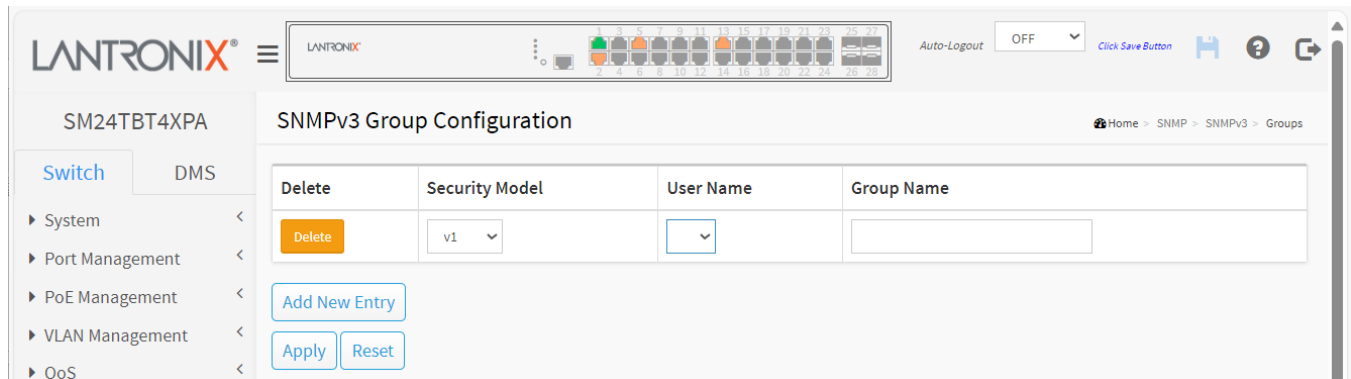


Figure 13-2.3: SNMPv3 Groups Configuration

Parameter descriptions:

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

v1: Reserved for SNMPv1.

v2c: Reserved for SNMPv2c.

usm: User-based Security Model (USM).

Security Name : A string identifying the security name that this entry should belong to. The allowed string length is 1 to 31 characters, and the allowed content is ASCII characters 33 - 126.

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

Buttons

Add New Entry : Click to add new entry. Specify the name and configure the new entry. Click "Apply".

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

Apply: Click to save changes.

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

13-2.4 Views

The function is used to configure SNMPv3 view. The Entry index keys are OID Subtree and View Name. To create a new view account, click the Add New View button, enter the view information then click Apply. The max Group number is 12. The entry index keys are View Name and OID Subtree.

To configure SNMP views in the web UI:

1. Click SNMP, SNMPv3, and Views.
2. Click Add New Entry.
3. Specify the SNMP View parameters.
4. Click Apply. If you want to modify or clear the setting then click Reset.

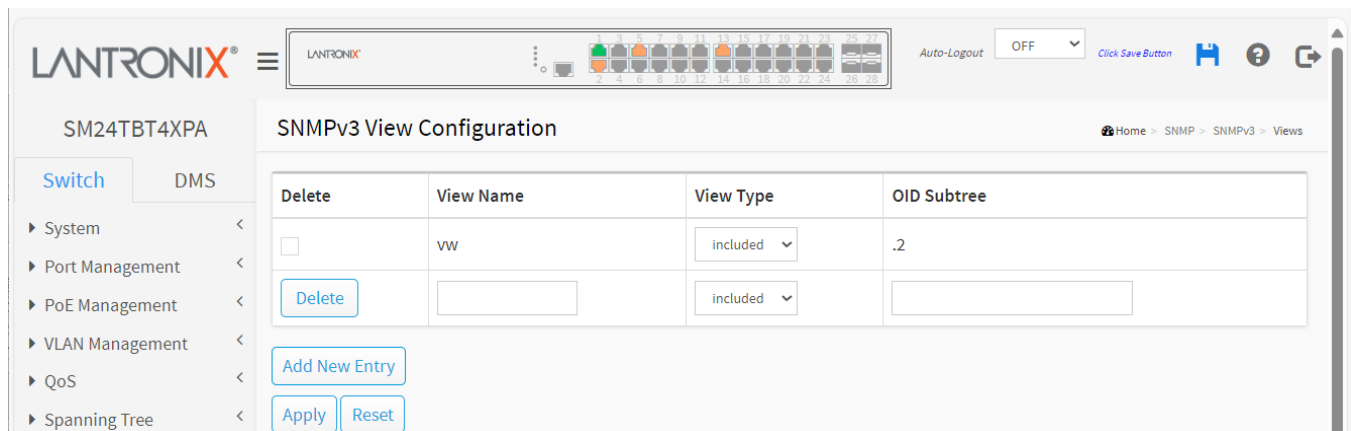


Figure 13-2.4: SNMP Views Configuration

Parameter descriptions:

View Name : A string identifying the view name that this entry should belong to. The allowed string length is 1 - 31 characters, and the allowed content is ASCII characters 33 - 126.

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

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

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

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

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

Buttons

Add New Entry : Click to add new entry. Specify the name and configure the new entry. Click "Apply".

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

Apply: Click to save changes.

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

13-2.5 Access

The function is used to configure SNMPv3 accesses. The Entry index key are Group Name, Security Model and Security level. To create a new access account, click the Add New Access button, enter the access information, and then click Apply. The max Group number is 12.

To configure SNMP Access in the web UI:

1. Click SNMP, SNMPv3, and Accesses.
2. Click Add New Entry.
3. Specify the SNMP Access parameters.
4. Click Apply. If you want to modify or clear the setting then click Reset.

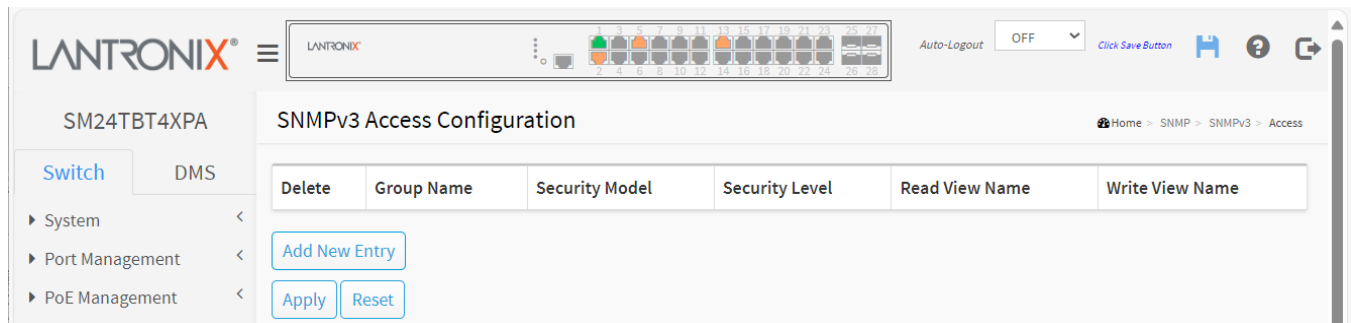


Figure 13-2.5: SNMP Accesses Configuration

Parameter descriptions:

Group Name : A string identifying the group name that this entry should belong to. The allowed string length is 1 - 31 characters, and the allowed content is ASCII characters 33 - 126.

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

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

v1: Reserved for SNMPv1.

v2c: Reserved for SNMPv2c.

usm: User-based Security Model (USM).

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

NoAuth, NoPriv: No authentication and no privacy.

Auth, NoPriv: Authentication and no privacy.

Auth, Priv: Authentication and privacy.

Read View Name : The name of the MIB view defining the MIB objects for which this request may request the current values. The allowed string length is 1 - 31 characters, and the allowed content is ASCII characters 33 - 126.

Write View Name : The name of the MIB view defining the MIB objects for which this request may potentially set new values. The allowed string length is 1 - 31 characters, and the allowed content is ASCII characters 33 - 126.

Buttons

Add New Entry : Click to add new entry. Specify the name and configure the new entry. Click "Apply".

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

Apply: Click to save changes.

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

13-3 Statistics

13-3.1 Configuration

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

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

The screenshot shows the Lantronix web interface for the SM24TBT4XPA device. The page title is "RMON Statistics Configuration". On the left, there is a sidebar with a "Switch" tab and a "DMS" tab. Under the "Switch" tab, there are several expandable sections: System, Port Management, PoE Management, VLAN Management, QoS, and Spanning Tree. The main content area contains a table with the following structure:

| Delete | ID | Data Source |
|---------------------------------------|----------------------|-------------------------|
| <input type="checkbox"/> | 1 | .1.3.6.1.2.1.2.2.1.1. 1 |
| <input type="button" value="Delete"/> | <input type="text"/> | .1.3.6.1.2.1.2.2.1.1. 0 |

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

Figure 13-3.1: RMON Statistics Configuration

Parameter descriptions:

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

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

Buttons

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

Add New Entry : Click to add a new entry.

Apply: Click to save changes.

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

13-3.2 Statistics

This page provides an overview of RMON Statistics entries. Each page shows up to 99 entries from the Statistics table, default being 20, selected through the "entries per page" input field. When first visited, the web page will show the first 20 entries from the beginning of the Statistics table. The first displayed will be the one with the lowest ID found in the Statistics table.

The "Start from Control Index" allows the user to select the starting point in the Statistics table. Clicking the Refresh button will update the displayed table starting from that or the next closest Statistics table match.

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

To display RMON Statistics Status in the web UI:

1. Click Security, RMON, Status, and Statistics.
2. Specify which Port you want to check.
3. Check "Auto-refresh".
4. Click "Refresh" to refresh the port detailed statistics.

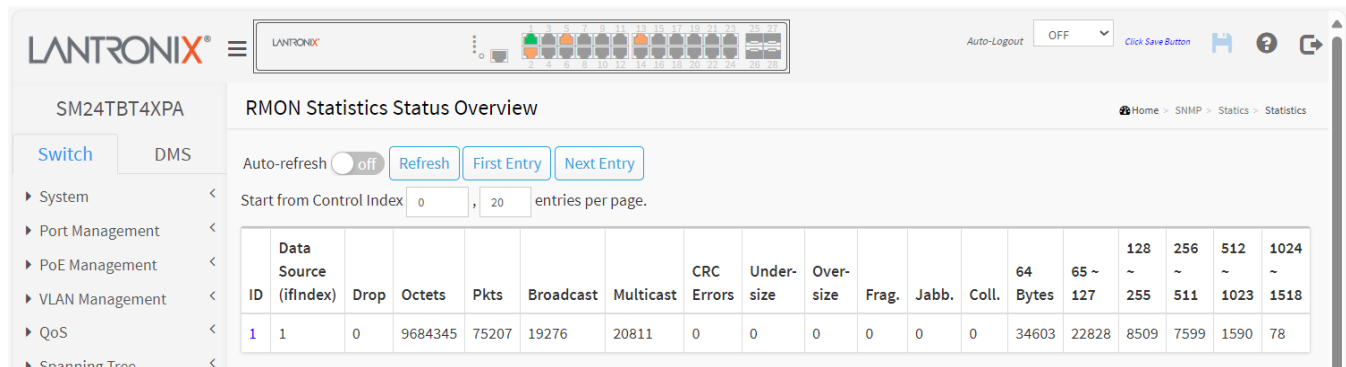


Figure 13-3.2: RMON Statistics Status Overview

Parameter descriptions:

ID: Indicates the index of Statistics entry.

Data Source(if Index): The port ID which wants to be monitored.

Drop: The total number of events in which packets were dropped by the probe due to lack of resources.

Octets: The total number of octets of data (including those in bad packets) received on the network.

Pkts: The total number of packets (including bad packets, broadcast packets, and multicast packets) received.

Broadcast: The total number of good packets received that were directed to the broadcast address.

Multicast: The total number of good packets received that were directed to a multicast address.

CRC Errors: The total number of packets received that had a length (excluding framing bits, but including FCS octets) of between 64 and 1518 octets, inclusive, but had either a bad Frame Check Sequence (FCS) with an integral number of octets (FCS Error) or a bad FCS with a non-integral number of octets (Alignment Error).

Under-size: The total number of packets received that were less than 64 octets.

Over-size: The total number of packets received that were longer than 1518 octets.

Frag.: The number of frames which size is less than 64 octets received with invalid CRC.

Jabb.: The number of frames which size is larger than 64 octets received with invalid CRC.

Coll.: The best estimate of the total number of collisions on this Ethernet segment.

64Bytes : The total number of packets (including bad packets) received that were 64 octets in length.

65~127: The total number of packets (including bad packets) received that were between 65 to 127 octets in length.

128~255: The total number of packets (including bad packets) received that were between 128 to 255 octets in length.

256~511: The total number of packets (including bad packets) received that were between 256 to 511 octets in length.

512~1023: The total number of packets (including bad packets) received that were between 512 to 1023 octets in length.

1024~1588: The total number of packets (including bad packets) received that were between 1024 to 1588 octets in length.

Search: You can search for the information that you want to see.

Show entries: Choose how many items you want to display.

Buttons

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

Refresh: Click to refresh the page immediately.

Next : Updates the system log entries, turn to the next page.

Previous: Updates the system log entries, turn to the previous page.

13-4 History

13-4.1 Configuration

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

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

Figure 13-4.1: RMON History Configuration

Parameter descriptions:

These parameters are displayed on the RMON History Configuration page:

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

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

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

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

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

Buttons

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

Add New Entry : Click to add a new entry.

Apply: Click to save changes.

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

13-4.2 Status

This page provides an overview of RMON History entries. Each page shows up to 99 entries from the History table, default being 20, selected through the "entries per page" input field. When first visited, the web page will show the first 20 entries from the beginning of the History table. The first displayed will be the one with the lowest History Index and Sample Index found in the History table.

The "Start from History Index and Sample Index" allows the user to select the starting point in the History table. Clicking the Refresh button will update the displayed table starting from that or the next closest History table match.

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

To display RMON History in the web UI:

1. Click SNMP, History, and Status.
2. Check "Auto-refresh".
3. Click "Refresh" to refresh the statistics.
4. Click First Entry/Next Entry to change Entry.

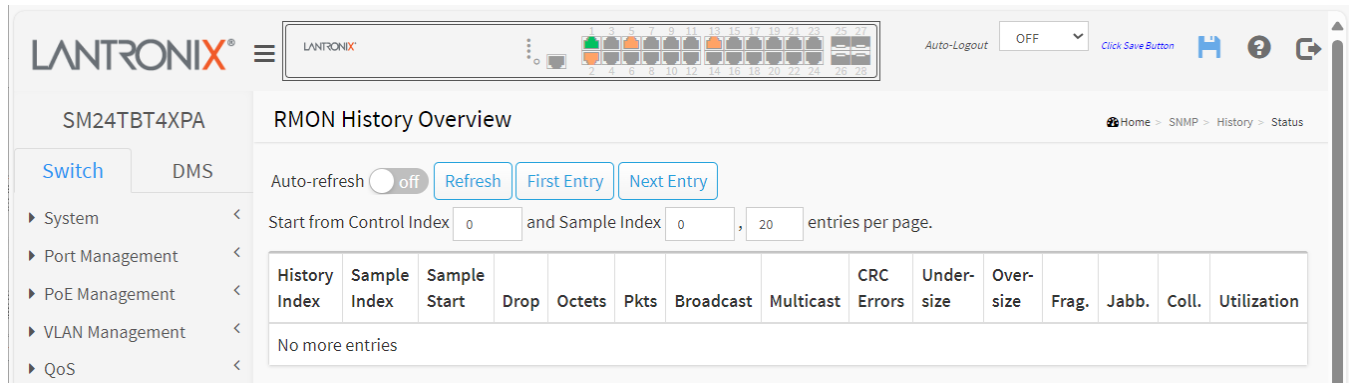


Figure 13-4.2: RMON History Overview

Parameter descriptions:

History Index: Indicates the index of History control entry.

Sample Index: Indicates the index of the data entry associated with the control entry.

Sample Start: The value of sysUpTime at the start of the interval over which this sample was measured.

Drop: The total number of events in which packets were dropped by the probe due to lack of resources.

Octets: The total number of octets of data (including those in bad packets) received on the network.

Pkts: The total number of packets (including bad packets, broadcast packets, and multicast packets).

Broadcast: The total number of good packets received that were directed to the broadcast address.

Multicast: The total number of good packets received that were directed to a multicast address.

CRC Errors: The total number of packets received that had a length (excluding framing bits, but including FCS octets) of between 64 and 1518 octets, inclusive, but had either a bad Frame Check Sequence (FCS) with an integral number of octets (FCS Error) or a bad FCS with a non-integral number of octets (Alignment Error).

Under-size: The total number of packets received that were less than 64 octets.

Over-size: The total number of packets received that were longer than 1518 octets.

Frag.: The number of frames which size is less than 64 octets received with invalid CRC.

Jabb.: The number of frames which size is larger than 64 octets received with invalid CRC.

Coll.: The best estimate of the total number of collisions on this Ethernet segment.

Utilization: The best estimate of the mean physical layer network utilization on this interface during this sampling interval, in hundredths of a percent.

Show entries: You can choose how many items you want to show.

Buttons

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

Refresh: Click to refresh the page immediately.

First Entry: Updates the table starting from the first entry in the IPMC Profile Address Configuration.

Next Entry: Updates the table, starting with the entry after the last entry currently displayed.

13-5 Alarm

13-5.1 Configuration

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

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

| Delete | ID | Interval | Variable | Sample Type | Value | Startup Alarm | Rising Threshold | Rising Index | Falling Threshold | Falling Index |
|--------------------------|----|----------|-------------------------|-------------|-------|-----------------|------------------|--------------|-------------------|---------------|
| <input type="checkbox"/> | 1 | 30 | .1.3.6.1.2.1.2.2.1.11.1 | Delta | 410 | RisingOrFalling | 4 | 1 | 3 | 2 |
| <input type="checkbox"/> | 2 | 30 | .1.3.6.1.2.1.2.2.1.12.4 | Absolute | 0 | Rising | 6 | 7 | 5 | 8 |

Figure 13-5.1: RMON Alarm Configuration

Parameter descriptions:

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

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

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

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

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

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

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

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

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

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

OutUcastPkts: The number of unicast packets that request to transmit.

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

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

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

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

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

Absolute: Get the sample directly.

Delta: Calculate the difference between samples (default).

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

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

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

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

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

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

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

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

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

Buttons

Delete : Check to delete the entry.

Add New Entry: Click to add a new entry.

Apply: Click to save changes.

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

Messages:

'ID' must be an integer value between 1 and 65535

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

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

13-5.2 Status

This page provides an overview of RMON Alarm entries. Each page shows up to 99 entries from the Alarm table, default being 20, selected through the "entries per page" input field. When first visited, the web page will show the first 20 entries from the beginning of the Alarm table. The first displayed will be the one with the lowest ID found in the Alarm table.

The "Start from Control Index" allows the user to select the starting point in the Alarm table. Clicking the Refresh button will update the displayed table starting from that or the next closest Alarm table match.

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

To display RMON Alarm Status in the web UI:

1. Click SNMP, Alarm, and Status.
2. Checked "Auto-refresh".
3. Click "Refresh" to refresh the port detailed statistics.
4. Click First Entry/Next Entry to change Entry.

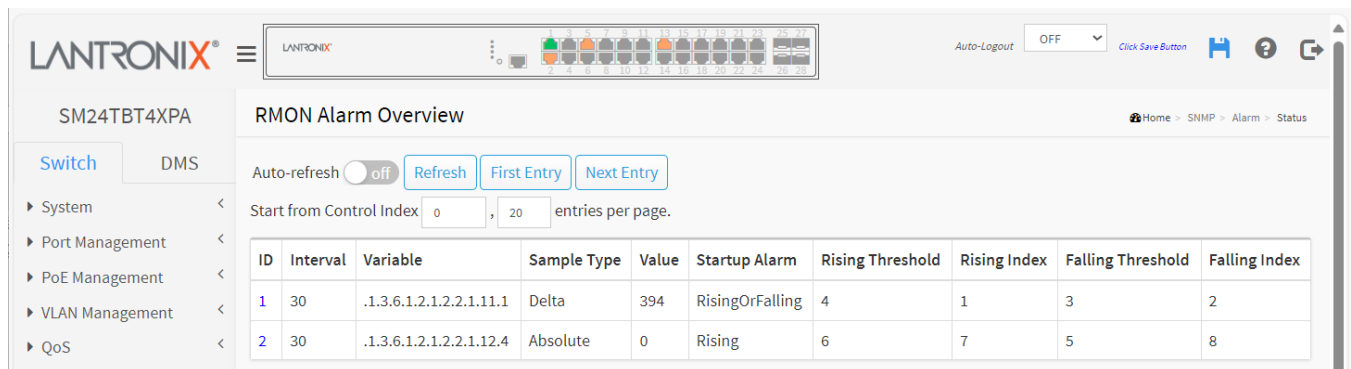


Figure 13-5.2: RMON Alarm Overview

Parameter descriptions:

ID: Indicates the index of Alarm control entry.

Interval: Indicates the interval in seconds for sampling and comparing the rising and falling threshold.

Variable: Indicates the particular variable to be sampled

Sample Type: The method of sampling the selected variable and calculating the value to be compared against the thresholds.

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

Startup Alarm: The alarm that may be sent when this entry is first set to valid.

Rising Threshold: Rising threshold value.

Rising Index: Rising event index.

Falling Threshold: Falling threshold value.

Falling Index: Falling event index.

Show entries: Choose how many items you want displayed.

Buttons

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

Refresh: Click to refresh the page immediately.

First Entry: Updates the table starting from the first entry in the IPMC Profile Address Configuration.

Next Entry: Updates the table, starting with the entry after the last entry currently displayed.

13-6 Event

13-6.1 Configuration

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

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

| Delete | ID | Desc | Type | Event Last Time |
|--------------------------|----|------|------------|-----------------|
| <input type="checkbox"/> | 1 | one | log | 4221 |
| <input type="checkbox"/> | 2 | 222 | snmptrap | 0 |
| <input type="checkbox"/> | 3 | tri | logandtrap | 0 |

Figure 13-6.1: RMON Event Configuration

Parameter descriptions:

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

Desc: Indicates this event, the string length is from 0 to 127, default is a null string.

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

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

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

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

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

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

Buttons

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

Add New Entry : Click to add a new entry.

Apply: Click to save changes.

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

13-6.2 Status

This page provides an overview of RMON Event table entries. Each page shows up to 99 entries from the Event table, default being 20, selected through the "entries per page" input field. When first visited, the web page will show the first 20 entries from the beginning of the Event table. The first displayed will be the one with the lowest Event Index and Log Index found in the Event table.

The "Start from Event Index" and "Sample Index" allows the user to select the starting point in the Event table. Clicking the Refresh button will update the displayed table starting from that or the next closest Event table match.

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

To display RMON Event Status in the web UI:

1. Click SNMP, Event, and Status.
2. Check "Auto-refresh".
3. Click "Refresh" to refresh the page data.
4. Click First Entry/Next Entry to change Entry.

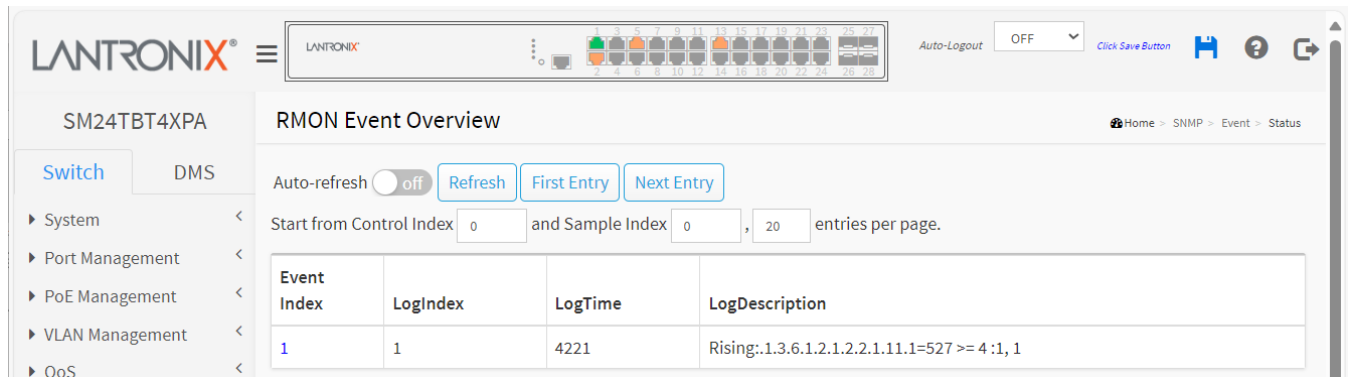


Figure 13-6.2: RMON Event Status

Parameter descriptions:

Event Index: Indicates the index of the event entry. Click the linked text to display the event's details (see below).

Log Index: Indicates the index of the log entry.

LogTime: Indicates Event log time

LogDescription: Indicates the Event description.

Show entries: Choose how many items you want displayed.

Buttons

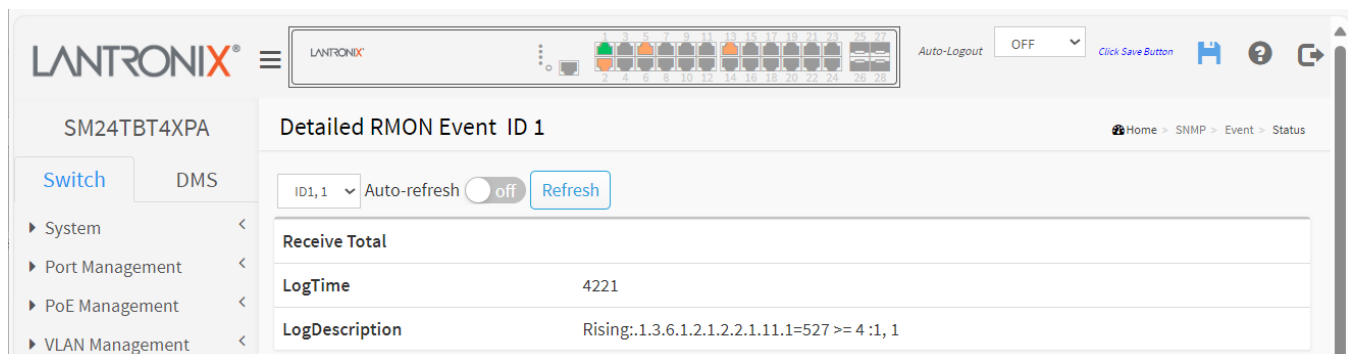
Auto-refresh: Check this box to refresh the page automatically every 3 seconds.

Refresh: Click to refresh the page immediately.

First Entry: Updates the table starting from the first entry in the IPMC Profile Address Configuration.

Next Entry: Updates the table, starting with the entry after the last entry currently displayed.

Detailed RMON Event Example:



14. MEP

14-1 MEP Configuration

The Maintenance Entity Point instances are configured here. To configure the MEP parameters in the web UI:

1. Click MEP.
2. Specify the Maintenance Entity Point parameters.
3. Click Apply to apply the change.

| Delete | Instance | Domain | Mode | Direction | Residence Port | Level | Flow Instance | Tagged VID | This MAC | Alarm |
|---------------------------------------|----------|--------|------|-----------|----------------|-------|---------------|------------|----------|-------|
| <input type="button" value="Delete"/> | 1 | Port | Mep | Down | 1 | 0 | 1 | 0 | | |

Figure 14-1: Maintenance Entity Point

Parameter descriptions:

Delete: This box is used to mark a MEP for deletion in next Save operation.

Instance: The ID of the MEP. Click on the ID of a MEP to enter the configuration page. The range is from 1-3124.

Domain: Select either:

Port: This is a MEP in the Port Domain.

VLAN: This is a MEP in the VLAN Domain. 'Flow Instance' is a VLAN. In case of Up-MEP the VLAN must be created.

Mode: Select either:

MEP: This is a Maintenance Entity End Point.

MIP: This is a Maintenance Entity Intermediate Point.

Direction: Select either:

Down: This is a Down MEP -monitoring ingress OAM and traffic on 'Residence Port'.

Up: This is a Up MEP -monitoring egress OAM and traffic on 'Residence Port'.

Residence Port: The port where MEP is monitoring -see 'Direction'. For a EVC MEP the port must be a port in the EVC. For a VLAN MEP the port must be a VLAN member.

Level: The MEG level of this MEP.

Flow Instance: The MEP is related to this flow -See 'Domain'. This is not relevant and not shown in case of a Port MEP.

Tagged VID: Select one of the following:

Port MEP: An outer C/S-tag (depending on VLAN Port Type) is added with this VID. Entering '0' means no TAG added.

EVC MEP: This is not used.

VLAN MEP: This is not used.

EVC MIP: On Serval, this is the Subscriber VID that identify the subscriber flow in this EVC where the MIP is active.

This MAC: The MAC of this MEP -can be used by other MEP when unicast is selected (Info only).

Alarm: There is an active alarm on the MEP or operational state is not "Up".

Buttons

Add New MEP: Click to add a new MEP entry.

Apply: Click to save changes.

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

Messages:

MAX number of Down-MEPs is exceeded in this flow

UP MEP/MIP is not supported in this domain

This MIP is not supported

Could not set aps config for instance 2

Example:

LANTRONIX®

SM24TBT4XPA

Maintenance Entity Point

Home > MEP > MEP Configuration

| Delete | Instance | Domain | Mode | Direction | Residence Port | Level | Flow Instance | Tagged VID | This MAC | Alarm |
|--------------------------|----------|--------|------|-----------|----------------|-------|---------------|------------|-------------------|-------|
| <input type="checkbox"/> | 1 | Port | Mep | Down | 1 | 0 | | 0 | 00-C0-F2-A8-A3-BE | ● |
| <input type="checkbox"/> | 2 | VLAN | Mep | Down | 1 | 0 | 1 | | 00-C0-F2-A8-A3-BE | ● |

Add New MEP

Apply Reset

15. ERPS

ERPS instances are configured here. Ethernet Ring Protection Switching (ERPS) is an effort at ITU-T under G.8032 Recommendation to provide sub-50ms protection and recovery switching for Ethernet traffic in a ring topology and at the same time ensuring that there are no loops formed at the Ethernet layer.

To configure Ethernet Ring Protection Switching parameters in the web UI:

1. Click ERPS.
2. Specify the Ethernet Ring Protection Switching parameters.
3. Click Apply to apply the changes.

The screenshot shows the Lantronix web interface for the SM24TBT4XPA device. The main section is titled "Ethernet Ring Protection Switching". On the left is a sidebar with navigation links: System, Port Management, PoE Management, VLAN Management, QoS, Spanning Tree, MAC Address Tables, Multicast, DHCP, and Security. The top header shows the Lantronix logo, a status bar with port indicators, and an "Auto-Logout" dropdown set to "OFF". Below the title, there's an "Auto-refresh" toggle (off) and a "Refresh" button. The main table lists ERPS instances with the following data:

| Delete | ERPS ID | Port 0 | Port 1 | Port 0 APS MEP | Port 1 APS MEP | Port 0 SF MEP | Port 1 SF MEP | Ring Type | Interconnected Node | Virtual Channel | Major Ring ID | Alarm |
|--------------------------|---------|--------|--------|----------------|----------------|---------------|---------------|-----------|--------------------------|--------------------------|---------------|------------------------------------|
| <input type="checkbox"/> | 1 | 1 | 2 | 1 | 2 | 1 | 2 | Major | No | No | 1 | ● |
| <input type="checkbox"/> | 2 | 3 | - | 5 | 6 | 7 | 0 | Sub | Yes | Yes | 1 | ● |
| <input type="checkbox"/> | 3 | 1 | 1 | 1 | 1 | 1 | 1 | Major | <input type="checkbox"/> | <input type="checkbox"/> | 0 | ● |

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

Figure 15: Ethernet Ring Protection Switching

Parameter descriptions:

Delete: This box is used to mark an EPS for deletion in next save operation.

ERPS ID: The ID of the created Protection group, It must be an integer value between 1 and 64. You can create a maximum of 64 ERPS Protection Groups. Click on the ID of a Protection group to enter its configuration page.

Port 0: This will create a Port 0 of the switch in the ring.

Port 1: This will create "Port 1" of the switch in the Ring. As interconnected sub-ring will have only one ring port, "Port 1" is configured as "0" for interconnected sub-ring. "0" in this field indicates that no "Port 1" is associated with this instance

Port 0 SF MEP: The Port 0 Signal Fail reporting MEP.

Port 1 SF MEP: The Port 1 Signal Fail reporting MEP. As only one SF MEP is associated with interconnected sub-ring without virtual channel, it is configured as "0" for such ring instances. "0" in this field indicates that no Port 1 SF MEP is associated with this instance.

Port 0 APS MEP: The Port 0 APS PDU handling MEP.

Port 1 APS MEP: The Port 1 APS PDU handling MEP. As only one APS MEP is associated with interconnected sub-ring without virtual channel, it is configured as "0" for such ring instances. "0" in this field indicates that no Port 1 APS MEP is associated with this instance.

Ring Type: Type of Protecting ring. It can be either major ring or sub-ring.

Interconnected Node: Interconnected Node indicates that the ring instance is interconnected. Click on the checkbox to configure this. "Yes" indicates it is an interconnected node for this instance. "No" indicates that the configured instance is not interconnected.

Virtual Channel: Sub-rings can either have virtual channel or not on the interconnected node. This is configured using "Virtual Channel" checkbox. "Yes" indicates it is a sub-ring with virtual channel. "No" indicates, sub-ring doesn't have virtual channel.

Major Ring ID: Major ring group ID for the interconnected sub-ring. It is used to send topology change updates on major ring. If ring is major, this value is same as the protection group ID of this ring.

Alarm: There is an active alarm on the ERPS.

Buttons

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

Refresh: Click to manually refresh the page immediately.

Add New Protection Group: Click to add a new Protection group entry.

Apply: Click to save changes.

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

Messages:

'Port 0' and 'Port 1' can not be same

Only one ERPS can be added for each Save operation

'Port 0 APS MEP' and 'Port 1 APS MEP' can not be same

Port 0 SF MEP and Port 1 SF MEP can not be same

'Port 1' must be zero

'Port 1 SF MEP' must be zero

Click on the ID of a Protection group to enter its ERPS Configuration page. This page lets you set and view the current ERPS Instance.

ERPS Configuration 1

Auto-refresh ☐ off [Refresh](#)

Instance Data

| ERPS ID | Port 0 | Port 1 | Port 0 SF MEP | Port 1 SF MEP | Port 0 APS MEP | Port 1 APS MEP | Ring Type |
|---------|--------|--------|---------------|---------------|----------------|----------------|------------|
| 1 | 1 | 2 | 1 | 2 | 1 | 2 | Major Ring |

Instance Configuration

| Configured | Guard Time | WTR Time | Hold Off Time | Version | Revertive | VLAN Config |
|-------------------------------------|------------|----------|---------------|---------|-------------------------------------|-----------------------------|
| <input checked="" type="checkbox"/> | 500 | 1min | 0 | v2 | <input checked="" type="checkbox"/> | VLAN Config |

RPL Configuration

| RPL Role | RPL Port | Clear |
|----------|----------|--------------------------|
| None | None | <input type="checkbox"/> |

Instance Command

| Command | Port |
|---------|------|
| None | None |

Instance State

| Protection State | Port 0 | Port 1 | Transmit APS | Port 0 Receive APS | Port 1 Receive APS | WTR Remaining | RPL Unblocked | No APS Received | Port 0 Block Status | Port 1 Block Status | FOP Alarm |
|------------------|--------|--------|--------------|--------------------|--------------------|---------------|-------------------------------------|-------------------------------------|---------------------|---------------------|-------------------------------------|
| Pending | OK | OK | | | | 0 | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | Blocked | Blocked | <input checked="" type="checkbox"/> |

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

Parameter descriptions:

Instance Data

ERPS ID: The ID of the created Protection group, It must be an integer value between 1 and 64. You can create a maximum of 64 ERPS Protection Groups. Click on the ID of a Protection group to enter its configuration page.

Port 0: This will create a Port 0 of the switch in the ring.

Port 1: This will create "Port 1" of the switch in the Ring. As interconnected sub-ring will have only one ring port, "Port 1" is configured as "0" for interconnected sub-ring. Enter ing a "0" in this field indicates that no "Port 1" is associated with this instance.

Port 0 SF MEP: The Port 0 Signal Fail reporting MEP.

Port 1 SF MEP: The Port 1 Signal Fail reporting MEP. As only one SF MEP is associated with interconnected sub-ring without virtual channel, it is configured as "0" for such ring instances. "0" in this field indicates that no Port 1 SF MEP is associated with this instance.

Port 0 APS MEP: The Port 0 APS PDU handling MEP.

Port 1 APS MEP: The Port 1 APS PDU handling MEP. As only one APS MEP is associated with interconnected sub-ring without virtual channel, it is configured as "0" for such ring instances. "0" in this field indicates that no Port 1 APS MEP is associated with this instance.

Ring Type: The type of Protecting ring. It can be either Major ring or Sub-ring.

Instance Configuration

Configured: Displays a red or green dot.

Red: This ERPS is only created and has not yet been configured - is not active.

Green: This ERPS is configured - is active.

Guard Time: Guard timeout value to be used to prevent ring nodes from receiving outdated R-APS messages. The period of the guard timer can be configured in 10 ms steps between 10 ms and 2 seconds, with a default value of 500 ms.

WTR Time: The Wait To Restore timing value to be used in revertive switching. The period of the WTR time can be configured by the operator in 1 minute steps between 5 and 12 minutes with a default value of 5 minutes.

Hold Off Time: The timing value to be used to make persistent check on Signal Fail before switching. The range of the hold off timer is 0 to 10 seconds in steps of 100 ms

Version: The ERPS Protocol Version - v1 or v2.

Revertive: In **Revertive** mode, after the conditions causing a protection switch has cleared, the traffic channel is restored to the working transport entity, i.e., blocked on the RPL. In **Non-Revertive** mode, the traffic channel continues to use the RPL, if it is not failed, after a protection switch condition has cleared.

VLAN config: VLAN configuration of the Protection Group. Click on the "VLAN Config" link to configure VLANs for this protection group (see below).

RPL Configuration

RPL Role: It can be either RPL owner or RPL Neighbor.

RPL Port: This allows to select the east port or west port as the RPL block.

Clear: If the owner has to be changed, then the clear check box allows to clear the RPL owner for that ERPS ring.

Sub-Ring Configuration

Topology Change: Clicking this checkbox indicates that the topology changes in the Sub-ring are propagated in the Major ring.

Instance Command

Command: Administrative command. A port can be administratively configured to be in either Manual switch or Forced switch state.

Forced Switch: Forced Switch command forces a block on the ring port where the command is issued.

Manual Switch: In the absence of a failure or FS, Manual Switch command forces a block on the ring port where the command is issued.

Clear: The Clear command is used for clearing an active local administrative command (e.g., Forced Switch or Manual Switch).

Port: Port selection - Port0 or Port1 of the protection Group on which the command is applied.

Instance State

Protection State: ERPS state according to State Transition Tables in G.8032.

Port 0: Either OK or SF:

OK: State of East port is ok

SF: State of East port is Signal Fail

Port 1: Either OK or SF:

OK: State of West port is ok

SF: State of West port is Signal Fail

Transmit APS: The transmitted APS according to State Transition Tables in G.8032.

Port 0 Receive APS: The received APS on Port 0 according to State Transition Tables in G.8032.

Port 1 Receive APS: The received APS on Port 1 according to State Transition Tables in G.8032.

WTR Remaining: Remaining WTR timeout in milliseconds.

RPL Un-blocked: APS is received on the working flow.

No APS Received: RAPS PDU is not received from the other end.

Port 0 Block Status: Block status for Port 0 (Both traffic and R-APS block status). R-APS channel is never blocked on sub-rings without virtual channel.

Port 1 Block Status: Block status for Port 1 (Both traffic and R-APS block status). R-APS channel is never blocked on sub-rings without virtual channel.

FOP Alarm: Failure of Protocol Defect (FOP) status. If FOP is detected, red LED glows; else green LED glows.

Buttons

Apply: Click to save changes.

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

Refresh: Click to refresh the page immediately.

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

ERPS VLAN Configuration

Click on the "VLAN Config" link to configure VLANs for this protection group.

To add a new VLAN, click Add the New Entry button to add a new VLAN ID to the table. Legal values for a VLAN ID are 1 - 4095. The VLAN is enabled when you click on "Apply". A VLAN without any port members will be deleted when you click "Apply". The Delete button can be used to undo the addition of new VLANs.

The screenshot shows the Lantronix web interface for the SM24TBT4XPA device. The left sidebar contains a navigation menu with the following items: System, Port Management, PoE Management, VLAN Management, QoS, Spanning Tree, and MAC Address Tables. The main content area is titled 'ERPS VLAN Configuration 1'. At the top of this section, there is an 'Auto-refresh' toggle set to 'off' and a 'Refresh' button. Below this is a table with two columns: 'Delete' and 'VLAN ID'. The table contains one row with a checkbox in the 'Delete' column and the value '100' in the 'VLAN ID' column. Below the table, there is an input field for 'VLAN ID' with the value '0'. At the bottom of the configuration area, there are four buttons: 'Add New Entry', 'Back', 'Apply', and 'Reset'.

Parameter descriptions:

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

VLAN ID: Indicates the ID of this particular VLAN.

Buttons

Apply: Click to save changes.

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

Back: Click to go back to this MEP instance main page.

Refresh: Refreshes the displayed table starting from the "VLAN ID" input fields.

16. EPS

The Ethernet (Linear) Protection Switch instances are configured here. EPS (Ethernet Protection Switching) is defined in ITU/T G.8031. To configure EPS in the web UI:

1. Click EPS.
2. Click Add New Entry.
3. Enter the parameters in each Blank field.
4. Click the Apply button to save the settings.
5. To cancel the settings click the Reset button. It will revert to previously saved values.

The screenshot shows the 'Ethernet Protection Switching' configuration page. On the left is a sidebar with navigation links: System, Port Management, PoE Management, VLAN Management, QoS, Spanning Tree, and MAC Address Tables. The top header displays the Lantronix logo, a device status bar, and an 'Auto-Logout' dropdown set to 'OFF'. The main content area features an 'Auto-refresh' toggle (currently 'off') and a 'Refresh' button. Below this is a table with columns: Delete, EPS ID, Domain, Architecture, W Flow, P Flow, W SF MEP, P SF MEP, APS MEP, and Alarm. The table contains two entries. The first entry has EPS ID '1', Domain 'Port', Architecture '1+1', and an active alarm (green dot). The second entry has EPS ID '2', Domain 'Port', Architecture '1+1', and all other fields are empty. Below the table are buttons for 'Add New Entry', 'Apply', and 'Reset'.

| Delete | EPS ID | Domain | Architecture | W Flow | P Flow | W SF MEP | P SF MEP | APS MEP | Alarm |
|--------------------------|--------|--------|--------------|--------|--------|----------|----------|---------|--------------------------------------|
| <input type="checkbox"/> | 1 | Port | 1+1 | 1 | 2 | 3 | 4 | 1 | ● |
| <input type="checkbox"/> | 2 | Port | 1+1 | 1 | 1 | 1 | 1 | 1 | |

Figure 16-1: EPS configuration

Parameter descriptions:

Delete: This box is used to mark an EPS for deletion in next Save operation.

EPS ID : The ID of the EPS. Click on the ID of an EPS to enter its configuration page. The range is 1-100.

Domain: The EPS domain.

Port: This will create an EPS in the Port Domain. 'W/P Flow' is a Port.

Architecture : Select either:

Port: This will create a 1+1 EPS (default).

Port: This will create a 1:1 EPS.

W Flow: The working flow for the EPS - See 'Domain'.

P Flow : The protecting flow for the EPS - See 'Domain'.

W SF MEP : The working Signal Fail reporting MEP.

P SF MEP : The protecting Signal Fail reporting MEP.

APS MEP: The APS PDU handling MEP.

Alarm: There is an active alarm on the EPS.

Buttons

Add New EPS : Click to add a new EPS entry.

Refresh : Click to refresh the page immediately.

Apply : Click to save changes.

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

Messages:

Only one EPS can be added for each Save operation

The working and protection flows are equal

Working MEP and protecting SF MEP is same instance

17. PercepXion and LPM

PercepXion is a cloud or on-premise portal for the centralized management of multiple Lantronix switches. A browser-based interface allows an administrator to view status, send commands, view logs and charts, and update firmware. Each Lantronix device can communicate with the cloud server or on-premise server, sending status updates and responding to commands sent by the server.

The switch requires a unique Device ID to communicate with the PercepXion portal. The ID is viewable in the PercepXion settings. If a device is not already pre-configured with the ID, the ID must be provisioned using Lantronix Provisioning Manager (LPM).

The PercepXion client follows a sequence of steps to connect to the PercepXion server, send status updates, check for firmware and configuration updates, and respond to commands from the server. This series of steps is the same each time the client starts - at boot, or if the client is enabled. Any changes to the PercepXion Device ID, or registration settings require the PercepXion client to be disabled and re-enabled for the changes to take effect.

PercepXion client registration

The client will attempt to register to the Host using the project tag and device ID. If registration fails, the client will wait and retry. The client will retry until it is successful, or the client is disabled. Registration may fail if the Project Tag is invalid, the Device ID is invalid, the Host name cannot be resolved, or the Host is not reachable. Once registration is successful, the **Client State** will display **Registered** with the date and time of registration.

Telemetry

After registration, the client will connect to the Telemetry Host (the hostname is the same as the registration host provided during registration) and perform a telemetry handshake. This handshake may request that the client publish a set of statistics at regular intervals.

Messaging and Status Updates

After the telemetry handshake, the PercepXion client will connect to the messaging host to receive messages and publish status updates. If the connection fails, the client will wait and retry. The connection may fail if the messaging host name cannot be resolved, or the messaging host is not reachable. The client publishes status update messages (changes to the device attributes) at the interval defined by **Status Update Interval**. Each time a status update is published, the **Last status update** will be updated to indicate the elapsed time since the status was sent. The client also accepts command messages from the PercepXion server to perform actions, such as reboot.

Web Connect

PercepXion allows users to make a secure connection to the switch's web interface. This connection opens the login page in the web browser. To use Web Connect, HTTPS must be enabled on the switch (HTTPS is the default). The **Web** button will be enabled in the PercepXion UI.

Firmware updates and Configuration updates

The PercepXion client checks for firmware and configuration updates at the interval defined by the **Content Check Interval**. When the client checks for firmware or configuration updates, the **Last content check** will be updated to indicate the elapsed time since the check was made. The **Available Firmware updates** and **Available Configuration updates** will indicate if an update was found on the server, or show *Not available*, if no updates were found.

Lantronix Provisioning Manager (LPM) is a software application that provisions, configures and updates Lantronix Console Managers and IoT Gateways for local site installations and deployments. LPM discovery is enabled by default and is not configurable. For more LPM information see the LPM [product page](#).

17-1 Percepixon Agent Configuration

Navigate to Configuration > Percepixon to display the Percepixon Agent Configuration page:

The screenshot shows the Lantronix web interface for the SM24TBT4XPA device. The left sidebar contains a navigation menu with options like System, Port Management, PoE Management, VLAN Management, QoS, Spanning Tree, MAC Address Tables, Multicast, DHCP, Security, Access Control, SNMP, MEP, ERPS, EPS, Percepixon (selected), PTP, Event Notification, Diagnostics, and Maintenance. The main content area is titled 'Percepixon Agent Configuration'. It features a 'Status' section with a table showing client state, last status update, last content check, and available updates. Below this is the 'Global Configuration' section with various settings like Enabled, Device ID, Device Key, Serial Number, Device Name, Device Description, Status Update Interval, Content Check Interval, Apply Firmware Updates, Apply Configuration Updates, and Active Connection.

| Status | |
|---------------------------------|--|
| Client state | Running Not registered - Couldn't resolve host name |
| Last status update | Not available |
| Last content check | Not available |
| Available Firmware updates | Not available |
| Available Configuration updates | Not available |

| Global Configuration | |
|-------------------------------------|-------------------------------------|
| Enabled | <input checked="" type="checkbox"/> |
| Device ID | 00c0f2a8a3bd3L |
| Device Key | ***** |
| Serial Number | 00c0f2a8a3bd |
| Device Name | SM24TBT4XPA-A3BD |
| Device Description | Lantronix SM24TBT4XPA |
| 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 |

Parameter descriptions:

Status:

Client state: Displays the existing Percepixon client state (e.g., *Exited*, *Active*, *Inactive*, *Running*, or *Not Registered*) .

Last status update: Displays the amount of time in minutes between status updates (1-1440 minutes or <Not Available>).

Last content check: Displays the amount of time in minutes between content checks; 1 minute to 90 days (in minutes) or <Not Available>.

Available Firmware updates: Displays a list of firmware that is available on the server. Select the firmware from this list and click Update now to upgrade or downgrade the firmware. Displays <Not available> if no Firmware updates are currently available.

Available Configuration updates: Displays a list of configuration that is available on the server. Select the configuration from this list and click Update now to upgrade or downgrade the firmware. Displays <Not available> if no configuration updates are currently available.

Global Configuration:

Enabled : Check the box to enable Percepixon globally. The default is disabled (unchecked).

Device ID: Switch Device ID. The ID is 32 alphanumeric characters. The Device ID may be provisioned through Lantronix Provisioning Manager (LPM).

Device Key: The device key provides an additional layer of security for the device. If the Device Key is not configured, it may be provisioned using Lantronix Provision Manager (LPM). Contact Lantronix Technical Support for more information on LPM.

Serial Number : Displays the serial number of the switch in the format *00c0f24f73d0*. Read only.

Device Name : Enter a Percepixon Device Name for the switch of up to 32 alphanumeric characters (e.g., *SM24TBT4XPA-A3BD*). 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 Percepixon Device Description for the switch of up to 32 alphanumeric characters (e.g., *Lantronix SM24TBT4XPA*).

Status Update Interval : Select the amount of time in minutes between updates (1-1440 minutes). The default is 1 minute. This is the frequency that the switch updates the device status to Percepixon.

Content Check Interval : Select the interval of time in minutes that the agent waits between checks for firmware or configuration updates (1-56160 minutes). The default is 1 minute. The valid range is 1 hour – 2160 hours (90 days).

Apply Firmware Updates : Check the box to enable firmware upgrades initiated by Percepixon for the switch. The device will check for updates per the frequency defined by the Content Check Interval, and if a firmware is found, the update will be downloaded and applied to the switch. The default is enabled.

Apply Configuration Updates : Check the box to enable firmware upgrades initiated by Percepixon for the switch. The device will check for updates per the frequency defined by the Content Check Interval. The default is enabled.

Active Connection: 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 Percepixon. The configurable parameters for Connection 1 and Connection 2 are shown and described below.

Connection 1 or 2 :

Connect To : At the dropdown, select **Cloud** (default) or **On-premise** as the Percepixon connection type. If Cloud is selected, the Percepixon client uses Cloud server settings. If On-Premise is selected, it uses On-Premise server settings. By default, the Percepixon active connection is Cloud.

Cloud setup connects you directly to the Percepixon server URL, allowing you to access your devices through the Internet.

On-premise setup connects you to Percepixon through your organization's network. This means you need to be physically "on-premises" to access your organization's network via Wi-Fi or may need to use a VPN connection.

Host : Enter the IP address or host name of the Percepixon server that the client registers with. The host name should start with **api**.

Port : Enter the TCP port on the registration host. The default is port 443.

Secure Port : If enabled, HTTPS (instead of HTTP) is used for registration. Enabled by default.

Validate Certificates : If enabled, use a certificate authority to validate the HTTPS certificate. To validate certificates, Secure Port must be enabled. A certificate authority file can be uploaded on the HTTPS page. If a certificate authority file is not uploaded to the switch, the client may fail to connect to the Percepixon server.

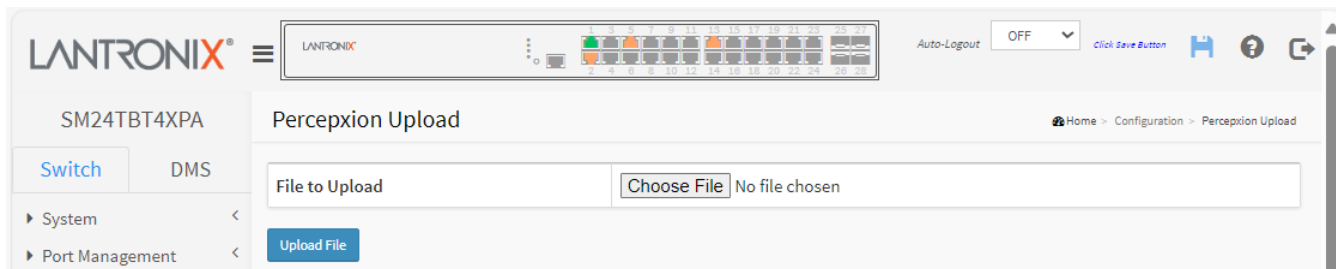
Buttons

Apply : Click to apply changes.

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

17-2 PercepXion Upload

Navigate to Configuration > PercepXion to display the PercepXion Upload page. This page lets you navigate to and select a file to upload.



Parameter descriptions:

File to Upload: Click the Choose File button to navigate to and select a file to upload a file from the web browser.

Upload File: Click the Upload File button to upload the selected file. When done, the message *"Upload successfully completed."* displays.

18. PTP

18-1 Configuration

This page lets you configure and view the current PTP clock settings. The Precision Time Protocol (PTP) is used to synchronize clocks throughout a computer network. On a local area network, it achieves clock accuracy in the sub-microsecond range, making it suitable for measurement and control systems. The switch supports the IEEE 1588v2 Precision Clock Synchronization Protocol. The first version of PTP, IEEE 1588-2002, was published in 2002. IEEE 1588-2008, also known as PTP Version 2, is not backward compatible with the 2002 version.

A maximum of 4 clock instances can be created. To configure PTP in the web UI:

1. Click PTP and Configuration.
2. Select the mode (enable or disable).
3. Specify the parameters in each blank field.
4. Click the Add New Entry button to display the PTP Clock's Configuration and Status page.
5. Set the PTP Clock's Configuration and Status parameters.
6. Click the Apply button to save the settings.
7. To cancel the settings click the Reset button to revert to previously saved values.

The screenshot shows the Lantronix web interface for the SM24TBT4XPA switch. The top header includes the Lantronix logo, a navigation menu, and status indicators like 'Auto-Logout' and 'OFF'. The left sidebar lists various configuration categories: Switch, DMS, System, Port Management, PoE Management, VLAN Management, QoS, Spanning Tree, MAC Address Tables, Multicast, DHCP, Security, Access Control, and SNMP. The main content area is titled 'PTP External Clock Mode' and contains the following configuration fields:

- PTP External Clock Mode:** A dropdown menu.
- External Enable:** A dropdown menu set to 'False'.
- Adjust Method:** A dropdown menu set to 'Auto'.
- Clock Frequency:** A text input field set to '1'.

Below these fields is a section titled 'PTP Clock Configuration' which contains a table with the following columns: Delete, Clock Instance, HW Domain, Device Type, and Profile. The table currently shows 'No Clock Instances Present'. At the bottom of the configuration area are buttons for 'Add New Entry', 'Apply', and 'Reset'.

Figure 18-1: PTP Configuration

Parameter descriptions:

PTP External Clock Configuration

External Enable: This selection box lets you configure the External Clock output. These values are possible:

True : Enable the external clock output.

False : Disable the external clock output.

Adjust Method: This selection box lets you configure the Frequency adjustment configuration:

LTC : Select Local Time Counter (LTC) frequency control.

Single : Select SyncE DPLL frequency control, if allowed by SyncE

Independent : Select an oscillator independent of SyncE for frequency control, if supported by the HW

Common : Select second DPLL for PTP, Both DPLL have the same (SyncE recovered) clock.

Auto : Automatically select clock control, based on PTP profile and available HW resources.

Clock Frequency: This will allow to set the Clock Frequency. The possible values are 1 -25000000 (1 -25MHz).

PTP Clock Configuration

Delete: Check this box and click on 'Save' to delete the clock instance.

Clock Instance: Indicates the instance number of a particular Clock Instance [0..3]. Click on the Clock Instance number to edit the Clock details.

HW Domain: Indicates the HW clock domain used by the clock.

Device Type: Indicates the Type of the Clock Instance. There are five Device Types.

Ord-Bound - clock's Device Type is Ordinary-Boundary Clock.

P2p Transp - clock's Device Type is Peer to Peer Transparent Clock.

E2e Transp - clock's Device Type is End to End Transparent Clock.

Master Only - clock's Device Type is Master Only.

Slave Only - clock's Device Type is Slave Only.

Profile: Indicates the profile used by the clock.

Buttons

Add New Entry: Click to add a new clock instance.

Apply: Click to save changes.

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

Click the Add New Entry button to display the PTP Clock's Configuration and Status page.

Page 256 of 316

Parameter descriptions:

Clock Type and Profile

Clock Instance: Indicates the instance number of a particular Clock Instance [0..3].

HW Domain: Indicates the HW clock domain used by the clock.

Device Type: Indicates the Type of the Clock Instance. There are five Device Types.

Ord-Bound - clock's Device Type is Ordinary-Boundary Clock.

P2p Transp - clock's Device Type is Peer to Peer Transparent Clock.

E2e Transp - clock's Device Type is End to End Transparent Clock.

Master Only - clock's Device Type is Master Only.

Slave Only - clock's Device Type is Slave Only.

Profile: Indicates the profile used by the clock.

Apply Profile Defaults: If the clock has been configured to use a profile, clicking the 'Apply' button will reset configured values to profile defaults.

Filter Type: The PTP filter type determines should match the operating conditions of the network and the PTP profile.

| PTP Profile | SyncE enabled (hybrid) | Filter type | Description |
|-------------|------------------------|--------------------------|---|
| 1588 | No | ACI_BASIC_PHASE | Requires PTP Sync and Delay_req frame rate of 16 fps or higher. |
| 1588 | Yes | ACI_BASIC_PHASE_SYNC | Requires PTP Sync and Delay_req frame rate of 16 fps or higher. |
| 1588 | No | ACI_BASIC_PHASE_LOW | Use when the PTP Sync and Delay_req frame rate is between 1 fps to 16 fps |
| 1588 | Yes | ACI_BASIC_PHASE_LOW_SYNC | Use when the PTP Sync and Delay_req frame rate is between 1 fps to 16 fps |
| None | No | ACI_BC_FULL_ON_PATH_FREQ | Used for Syntonized TC with basic filter. |

Port Enable and Configuration

Port Enable: Set check mark for each port configured for this Clock Instance.

Configuration: Click 'Ports Configuration' to edit the port data set for the ports assigned to this clock instance. See below.

Virtual Port Enable and Configuration

Enable: Disabled or Enabled.

I/O Pin: Virtual Port I/O Pin. The valid range is 0 to 3.

Class: Clock class value for clock as defined in IEEE Std 1588. The valid range is from 0 to 255.

Accuracy: Clock accuracy value as defined in IEEE Std 1588. The valid range is 0 to 255.

Variance: offsetScaledLogVariance for clock as defined in IEEE Std 1588. The valid range is 0 to 65535.

Pri1: Clock priority 1 [0..255] used by the BMC master select algorithm.

Pri2: Clock priority 2 [0..255] used by the BMC master select algorithm.

Local Prio: Priority [1..255] used in the 8275.1 BMCA.

Local Clock Current time: Show/update local clock data

PTP Time: Shows the actual PTP time with nanosecond resolution.

Clock Adjustment Method: Shows the actual clock adjustment method. The method depends on the available hardware.

Synchronize to System Clock: Activate this button to synchronize the System Clock to PTP Time.

Clock Current Data Set: The clock current data set is defined in the IEEE 1588 Standard. The current data set is dynamic.

stpRm: Steps Removed : It is the number of PTP clocks traversed from the grandmaster to the local slave clock.

Offset From Master: Time difference between the master clock and the local slave clock, measured in ns.

Mean Path Delay: The mean propagation time for the link between the master and the local slave

Clock Parent Data Set

The clock parent data set is defined in the IEEE 1588 standard. The parent data set is dynamic.

Parent Port ID: Clock identity for the parent clock, if the local clock is not a slave, the value is the clocks own id.

Port: Port Id for the parent master port

PStat: Parents Stats (always false).

Var: It is observed parent offset scaled log variance

Rate: Observed Parent Clock Phase Change Rate. i.e. the slave clocks rate offset compared to the master. (unit = ns per second).

Grand Master ID: Clock identity for the grand master clock, if the local clock is not a slave, the value is the clocks own id.

Grand Master Clock Quality: The clock quality announced by the grand master (See description of Clock Default DataSet:Clock Quality).

Pri1: Clock priority 1 announced by the grand master

Pri2: Clock priority 2 announced by the grand master.

Clock Default Dataset: The clock default data set is defined in the IEEE 1588 Standard. It holds three groups of data: the static members defined at clock creation time, the Dynamic members defined by the system, and the configurable members which can be set here.

Device Type: Indicates the Type of the Clock Instance. There are five Device Types.

Ord-Bound - Clock's Device Type is Ordinary-Boundary Clock.

P2p Transp - Clock's Device Type is Peer to Peer Transparent Clock.

E2e Transp - Clock's Device Type is End to End Transparent Clock.

Master Only - Clock's Device Type is Master Only.

Slave Only - Clock's Device Type is Slave Only.

One-Way: If true, one way measurements are used. This parameter applies only to a slave. In one-way mode no delay measurements are performed, i.e. this is applicable only if frequency synchronization is needed. The master always responds to delay requests.

2 Step Flag: True if two-step Sync events and Pdelay_Resp events are used

Ports: The total number of physical ports in the node

Clock Identity: It shows unique clock identifier

Dom: Clock domain [0..127].

Clock Quality: The clock quality is determined by the system, and holds 3 parts: Clock Class, Clock Accuracy and OffsetScaledLog Variance as defined in IEEE1588. The Clock Accuracy values are defined in IEEE1588 table 6 (Currently the clock Accuracy is set to 'Unknown' as default).

Pri1: Clock priority 1 [0..255] used by the BMC master select algorithm.

Pri2: Clock priority 2 [0..255] used by the BMC master select algorithm.

Local Prio: Priority [1..255] used in the 8275.1 BMCA.

Protocol: Transport protocol used by the PTP protocol engine:

- Ethernet PTP over Ethernet multicast
- EthernetMixed PTP using a combination of Ethernet multicast and unicast
- IPv4Multi PTP over IPv4 multicast
- IPv4Mixed PTP using a combination of IPv4 multicast and unicast
- IPv4Uni PTP over IPv4 unicast

VID: VLAN Identifier used for tagging the VLAN packets.

PCP: Priority Code Point value used for PTP frames.

DSCP: DSCP value used when transmitting IPv4 encapsulated packets

Clock Time Properties Data Set: The clock time properties data set is defined in the IEEE 1588 Standard. The data set is both configurable and dynamic, i.e. the parameters can be configured for a grandmaster. In a slave clock the parameters are overwritten by the grandmasters timing properties. The parameters are not used in the current PTP implementation.

The valid values for the Time Source parameter are:

16 (0x10) ATOMIC_CLOCK

32 (0x20) GPS

48 (0x30) TERRESTRIAL_RADIO

64 (0x40) PTP

80 (0x50) NTP

96 (0x60) HAND_SET

144 (0x90) OTHER

160 (0xA0) INTERNAL_OSCILLATOR

UtcOffset: In systems whose epoch is UTC, it is the offset between TAI and UTC

Valid: When true, the value of currentUtcOffset is valid

leap59: When true, this field indicates that last minute of the current UTC day has only 59 seconds.

leap61: When true, this field indicates that last minute of the current UTC day has 61 seconds.

Time Trac: True if the timescale and the value of currentUtcOffset are traceable to a primary reference.

Freq Trac: True if the frequency determining the timescale is traceable to a primary reference.

ptp Time Scale: True if the clock timescale of the grandmaster clock and false otherwise.

Time Source: The source of time used by the grandmaster clock.

Leap Pending: When true, there is a leap event pending at the date defined by leapDate.

Leap Date: The date for which the leap will occur at the end of its last minute. Date is represented as the number of days after 1970-01-01 (the latter represented as 0).

Leap Type: The type of leap event i.e. leap59 or leap61.

Unicast Slave Configuration: When operating in IPv4 Unicast mode, the slave is configured up to 5 master IP addresses. The slave then requests Announce messages from all the configured masters. The slave uses the BMC algorithm to select one as master clock, the slave then request Sync messages from the selected master.

Duration: The number of seconds a master is requested to send Announce/Sync messages. The request is repeated from the slave each Duration/4 seconds.

ip_address: IPv4 Address of the Master clock

grant: The granted repetition period for the sync message

CommState: The state of the communication with the master, possible values are:

IDLE : The entry is not in use.

INIT : Announce is sent to the master (Waiting for a response).

CONN : The master has responded.

SELL : The assigned master is selected as current master.

SYNC : The master is sending Sync messages.

Buttons

Apply: Click to save changes.

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

PTP Clock's Port Data Set Configuration: On the “PTP Clock's Configuration and Status” page, click the linked text “[Ports Configuration](#)” to display the “PTP Clock's Port Data Set Configuration” page:

Parameter descriptions: The port data set is defined in the IEEE 1588 Standard. It holds three groups of data: the static members, the dynamic members, and configurable members which can be set here.

Port: Static member port Identity : Port number [1..max port no]

Stat: Dynamic member portState: Current state of the port.

MDR: Dynamic member log Min Delay Req Interval: The delay request interval announced by the master.

Peer Mean Path Del: The path delay measured by the port in P2P mode. In E2E mode this value is 0

Anv: The interval for issuing announce messages in master state. Range is -3 to 4.

ATo: The timeout for receiving announce messages on the port. Range is 1 to 10.

Syv: The interval for issuing sync messages in master. Range is -7 to 4.

DIm: Configurable member delayMechanism: The delay mechanism used for the port:

e2e End to end delay measurement

p2p Peer to peer delay measurement.

Can be defined per port in an Ordinary/Boundary clock.

In a transparent clock all ports use the same delay mechanism, determined by the clock type.

MPR: The interval for issuing Delay_Req messages for the port in E2e mode. This value is announced from the master to the slave in an announce message. The value is reflected in the MDR field in the Slave

The interval for issuing Pdelay_Req messages for the port in P2P mode

Note: The interpretation of this parameter has changed from release 2.40. In earlier versions the value was interpreted relative to the Sync interval, this was a violation of the standard, so now the value is interpreted as an interval. I.e. $MPR = 0 \Rightarrow 1 \text{ Delay_Req pr sec}$, independent of the Sync rate. The valid range is -7 to 5.

Delay Asymmetry: If the transmission delay for a link is not symmetric, the asymmetry can be configured here, see IEEE 1588 Section 7.4.2 Communication path asymmetry. The valid range is -100000 to 100000.

Version: The current implementation only supports PTP version 2

Ingress latency: Ingress latency measured in ns, as defined in IEEE 1588 Section 7.3.4.2. The valid range is -100000 to 100000.

Egress Latency: Egress latency measured in ns, as defined in IEEE 1588 Section 7.3.4.2. The valid range is -100000 to 100000.

Version: PTP version used by this port

Mcast Addr: Configured destination address for multicast packets (PTP default or LinkLocal)

Not Slave: TRUE indicates that this interface cannot enter slave mode

Local Prio: 1-255, priority used in the 8275.1 BMCA

2 Step Flag: Option to override the 2-step option on port level *// IEEE 802.1AS specific parameters are only available when the 802.1AS profile is selected

Buttons

Apply: Click to save changes.

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

18-2 Status

This page lets you view current PTP clock parameters. To display PTP settings in the web UI:

1. Click PTP and Status.
2. Specify the PTP parameters.
3. Click Apply to apply the changes.

The screenshot shows the LANTRONIX web interface for the SM24TBT4XPA device. The left sidebar contains a navigation menu with options like System, Port Management, PoE Management, VLAN Management, QoS, Spanning Tree, MAC Address Tables, Multicast, DHCP, Security, Access Control, SNMP, MEP, ERPS, and EPS. The main content area is titled 'PTP External Clock Mode' and includes an 'Auto-refresh' toggle (currently off) and a 'Refresh' button. Below this, there are two sections: 'PTP External Clock Mode' and 'PTP Clock Configuration'.

PTP External Clock Mode

| | |
|-----------------|--------|
| External Enable | True |
| Adjust Method | Auto |
| Clock Frequency | 100000 |

PTP Clock Configuration

| Inst | ClkDom | Device Type | Port List | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
|------|--------|-------------|-----------|---|---|---|---|---|---|---|---|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|--|
| | | | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 | 19 | 20 | 21 | 22 | 23 | 24 | 25 | 26 | 27 | 28 | |
| 0 | 0 | Ord-Bound | ✓ | ✓ | ✓ | ✓ | | ✓ | ✓ | ✓ | ✓ | | | | | | | | | | | | | | | | | | | | |
| 1 | 1 | P2pTransp | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 2 | 2 | Mastronly | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 3 | 1 | Slaveonly | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |

Figure 18-2: PTP Status

Parameter descriptions:

PTP External Clock Description

External Enable: Shows the current External clock output configuration.

True : Enable the external clock output.

False : Disable the external clock output.

Adjust Method: Shows the current Frequency adjustment configuration.

LTC : Use Local Time Counter (LTC) frequency control

Single : Use SyncE DPLL frequency control, if allowed by SyncE

Independent : Use an oscillator independent of SyncE for frequency control, if supported by the HW

Common : Use second DPLL for PTP, Both DPLL have the same (SyncE recovered) clock.

Auto : Automatically select clock control, based on PTP profile and available HW resources.

Clock Frequency: Shows the current clock frequency used by the External Clock. The possible values are 1 -25000000 (1 -25MHz).

PTP Clock Description

Inst: Indicates the Instance of a particular Clock Instance [0..3]. Click on the Clock Instance number to monitor the Clock details.

ClkDom: Indicates the Clock domain used by the Instance of a particular Clock Instance [0..3].

Device Type: Indicates the Type of the Clock Instance. There are five Device Types.

Ord-Bound - Clock's Device Type is Ordinary-Boundary Clock.

P2p Transp - Clock's Device Type is Peer to Peer Transparent Clock.

E2e Transp - Clock's Device Type is End to End Transparent Clock.

Master Only - Clock's Device Type is Master Only.

Slave Only - Clock's Device Type is Slave Only.

Port List: Shows the ports configured for that Clock Instance.

Buttons

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

Refresh: Click to refresh the page immediately.

Apply: Click to save changes.

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

19. Event Notification

19-1 SNMP Trap

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

1. Click Event Notification and SNMP Trap.
2. Click Add New Entry to create a new SNMP Trap on the switch.
3. Specify SNMP Trap parameters.
4. Click Apply.

The screenshot shows the LANTRONIX web interface for the SM24TBT4XPA device. The top navigation bar includes the LANTRONIX logo, a status bar with port indicators, and an Auto-Logout dropdown set to OFF. The left sidebar shows a tree view with 'Switch' and 'DMS' as main categories, and various sub-menus like System, Port Management, PoE Management, VLAN Management, QoS, Spanning Tree, MAC Address Tables, Multicast, DHCP, Security, Access Control, and SNMP. The main content area is titled 'SNMP Trap Configuration' and contains a form with the following fields:

- Trap Config Name: Text input field.
- Trap Mode: Dropdown menu set to 'Disabled'.
- Trap Version: Dropdown menu set to 'SNMP v2c'.
- Trap Community: Text input field containing 'public'.
- Trap Destination Address: Text input field.
- Trap Destination Port: Text input field containing '162'.
- Trap Security Engine ID: Text input field containing '800014550300c0f2a8a3bd'.
- Trap Security Name: Dropdown menu set to 'None'.

At the bottom of the form are 'Apply' and 'Reset' buttons. The breadcrumb trail at the top right reads 'Home > Event Notification > SNMP Trap'.

Figure 19-1: SNMP Trap Configuration

Parameter descriptions:

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

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

on: Enable SNMP mode operation.

off: Disable SNMP mode operation.

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

SNMP v1: Set SNMP supported version 1.

SNMP v2c: Set SNMP supported version 2c.

SNMP v3: Set SNMP supported version 3.

Trap Community: Indicates the community access string when sending SNMP trap packet. The allowed string length is 0 to 63, and the allowed content is ASCII characters 33 - 126.

Trap Destination Address: Indicates the SNMP trap destination address. It allow 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. SNMP Agent will send SNMP message via this port; the port range is 1~65535.

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

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

Buttons

Add New Entry : Click to add a new entry.

Apply: Click to save changes.

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

19-2 eMail

Configure SMTP (Simple Mail Transfer Protocol) on this page. SMTP is the message-exchange standard for the Internet. The switch is to be configured as a client of SMTP while the server is a remote device that will receive messages from the switch that alarm events occurred.

To configure SMTP parameters in the web UI:

1. Click Event Notification and eMail.
2. Specify the SMTP Configuration parameters.
3. Click Apply.

Figure 19-2: SMTP Configuration

Parameter descriptions:

Mail Server: The IP address or hostname of the mail server. IP address is expressed in dotted decimal notation. This will be the device that sends out the mail for you.

User Name: Specify the username on the mail server.

Password: Specify the password of the user on the mail server.

Sender: Specify the sender name of the alarm mail.

Return Path: Specify the sender email address of the alarm mail. This address will be the "from" address on the email message.

Email Address #: Specify up to 6 receiver email addresses.

Buttons

Apply: Click to save changes.

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

19-3 Log

19-3.1 Syslog

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

To configure Syslog parameters in the web UI:

1. Click Event Notification, Log and Syslog.
2. Enable the Server Model.
3. Specify the syslog parameters.
4. Click Apply.

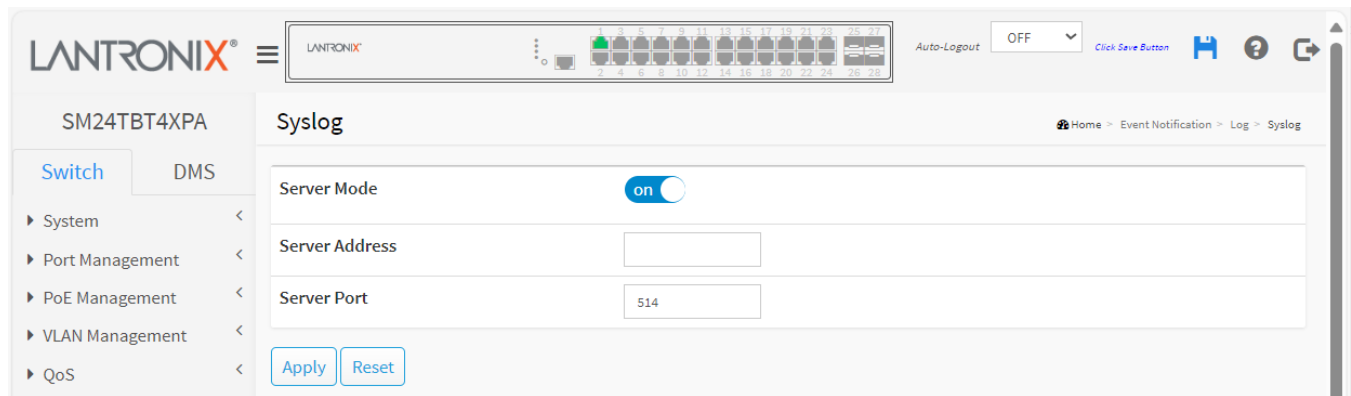


Figure 19-3.1: System Log configuration

Parameter descriptions:

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

on: Enable server mode operation.

off: Disable server mode operation.

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

Server Port: Indicates the service port of 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.

19-3.2 View Log

This page displays the system log information of the switch. To display log Information in the web UI:

1. Click Event Notification, Log, and View Log.

2. View the log information.

The screenshot shows the Lantronix web interface for the SM24TBT4XPA device. The left sidebar contains a navigation menu with options like System, Port Management, PoE Management, VLAN Management, QoS, Spanning Tree, MAC Address Tables, Multicast, DHCP, Security, Access Control, SNMP, MEP, ERPS, EPS, PercepXion, PTP, and Event Notification. The main content area is titled 'System Log Information' and includes an 'Auto-refresh' toggle (currently off), 'Refresh', and 'Clear' buttons. Below this is a 'System Log' section with a 'Show 25 entries' dropdown and a search box. A table displays the log entries with columns for ID, Level, Time, and Message.

| ID | Level | Time | Message |
|------|-------------|---------------------------|--|
| 2611 | Information | 2016-02-15T19:09:02+00:00 | DMS: New Device(172.27.100.16) add in topology |
| 2610 | Information | 2016-02-15T18:45:10+00:00 | DMS: Device(PLYWK-W10-00063 172.27.100.21) Off-line is caused by network disconnection. |
| 2609 | Information | 2016-02-15T18:33:40+00:00 | DMS: Device(PLYNB-W11-00010 172.27.100.111) On-line |
| 2608 | Information | 2016-02-15T18:33:30+00:00 | DMS: Device(PLYNB-W11-00010 172.27.100.101) Off-line is caused by network disconnection. |
| 2607 | Information | 2016-02-15T18:19:19+00:00 | DMS: New Device(172.27.100.21) add in topology |
| 2606 | Information | 2016-02-15T18:09:20+00:00 | DMS: New Device(172.27.100.101) add in topology |
| 2605 | Information | 2016-02-15T18:09:01+00:00 | DMS: Device(PLYNB-W11-00010 172.27.100.111) Off-line is caused by network disconnection. |
| 2604 | Information | 2016-02-15T18:03:52+00:00 | DMS: Device(PLYWK-W11-00054 172.27.100.103) On-line |

Figure 19-3.2: System Log Information

Parameter descriptions:

ID: ID (>= 1) of the system log entry.

Level: level of the system log entry. The following level types are supported:

Debug: debug level message.

Info: informational message.

Notice: normal, but significant, condition.

Warning: warning condition.

Error: error condition.

Crit: critical condition.

Alert: action must be taken immediately.

Emerg: system is unusable.

Time: Displays the log record by device time. The time of the system log entry.

Message: Displays the log detail message. The message of the system log entry.

Search: You can search for the information that you want to see.

Show entries: Choose how many items you want displayed per page.

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: Clear all the system log entries.

Next : Updates the system log entries, turns to the next page.

Previous: Updates the system log entries, turn to the previous page.

19-4 Event Configuration

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

1. Click Event Notification and Event Configuration.
2. Select the Group name and Severity Level.
3. Click Enable to select different trap event.
4. Click the Apply button to save the setting.
5. To cancel the settings click the Reset button. It will revert to previously saved values.

The screenshot shows the Lantronix web interface for the SM24TBT4XPA device. The top navigation bar includes the Lantronix logo, a menu icon, a status bar with various indicators, and an 'Auto-Logout' dropdown set to 'OFF'. The sidebar on the left contains a navigation menu with categories like System, Port Management, PoE Management, VLAN Management, QoS, Spanning Tree, MAC Address Tables, Multicast, DHCP, Security, Access Control, SNMP, MEP, ERPS, EPS, Perception, PTP, and Event Notification (which is currently selected). The main content area is titled 'Trap Event Severity Configuration' and contains a table with the following columns: Group Name, Severity Level, Syslog, Trap, and SMTP. The table lists 15 event groups with their respective severity levels and checkboxes for enabling Syslog, Trap, and SMTP notifications.

| 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"/> |
| FAN | 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"/> |

Figure 19-4: Trap Event Severity Configuration

Parameter descriptions:

Group Name : The name identifying the severity group (e.g., ACL, DMS, LACP).

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

<0> Emergency: System is unusable.

<1> Alert: Action must be taken immediately.

<2> Critical: Critical conditions.

<3> Error: Error conditions.

<4> Warning: Warning conditions.

<5> Notice: Normal but significant conditions.

<6> Information: Information messages.

<7> Debug: Debug-level messages.

Syslog : Select to enable this Group Name in Syslog.

Trap : Select to enable this Group Name in Trap.

SMTP: Select to enable this Group Name in SMTP.

Buttons

Apply: Click to save changes.

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

20. Diagnostics

This chapter provides a set of basic system diagnosis. These includes Ping, Traceroute, Cable Diagnostics and port mirroring.

20-1 Ping

This page let you issue ICMP Echo packets to troubleshoot IPv4/6 connectivity issues. To configure a Ping in the web UI:

1. Click Diagnostics and Ping.
2. Specify IP Address, Ping Length, Ping Count, Ping Interval and Egress Interface.
3. Click Start.

Figure 20-1: ICMP Ping

Parameter descriptions:

IP Address : Specify the target IP Address of the Ping.

Ping Length: The payload size of the ICMP packet. Values range from 2 bytes to 1452 bytes.

Ping Count: The count of the ICMP packet. 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 (Only for IPv6): The VLAN ID (VID) of the specific egress IPv6 interface which ICMP packet goes. The given VID ranges from 1 to 4094 and will be effective only when the corresponding IPv6 interface is valid. When the egress interface is not given, PING6 finds the best match interface for destination. Do not specify egress interface for loopback address. Do specify egress interface for link-local or multicast address.

Buttons

Start: Click the “Start” button to start to ping the target IP Address.

New Ping : Back to ICMP Ping page.

After you press the Start button, ICMP packets are transmitted, and the sequence number and round trip time are displayed upon reception of a reply. The amount of data received inside of an IP packet of type ICMP ECHO_REPLY will always be 8 bytes more than the requested 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

20-2 Traceroute

This page allows you to issue ICMP, TCP, or UDP packets to diagnose network connectivity issues.

To start a Traceroute in the web UI:

1. Click Diagnostics and Traceroute.
2. Specify IP Address, Wait Time, Max TTL and Probe Count.
3. Click Start.

The screenshot displays the Traceroute web interface. At the top, the title 'Traceroute' is on the left, and a breadcrumb trail 'Home > Diagnostics > Traceroute' is on the right. Below the title is a form with four rows of input fields: 'IP Address' with the value '0.0.0.0', 'Wait Time (1~60)' with the value '5' and the unit 'seconds', 'Max TTL (1~255)' with the value '30', and 'Probe Count (1~10)' with the value '3'. A blue 'Start' button is positioned below the form. Underneath the button, the title 'Traceroute' is repeated on the left, and the breadcrumb trail 'Home > Diagnostics > Traceroute' is repeated on the right. A light gray box contains the text: 'traceroute to 0.0.0.0 (0.0.0.0), 30 hops max, 38 byte packets' followed by '1 localhost (127.0.0.1) 0.135 ms 0.111 ms 0.099 ms'. At the bottom of the form is a blue 'New Traceroute' button.

Figure 20-2: Traceroute

Parameter descriptions:

IP Address : The destination IP Address.

Wait Time (1~60): Set the time (in seconds) to wait for a response to a probe (default 5.0 seconds). Valid values are 1 - 60 seconds.

Max TTL (1~255): Specify the maximum number of hops (max time-to-live value) traceroute will probe. Valid values are 1 - 255 hops. The default is 30 hops.

Probe Count (1~10): Set the number of probe packets per hop. Valid values are 1 - 10. The default is 3.

Buttons

Start: Click the button to start to traceroute the target IP Address.

New Ping : Back to Traceroute page.

20-3 Cable Diagnostics

This page lets you run Cable Diagnostics for copper ports. To configure a Cable Diagnostics in the web UI:

1. Click Diagnostics and Cable Diagnostics.
2. Specify the Port which you want to check. At the confirmation prompt click the OK button.
3. Click Start.

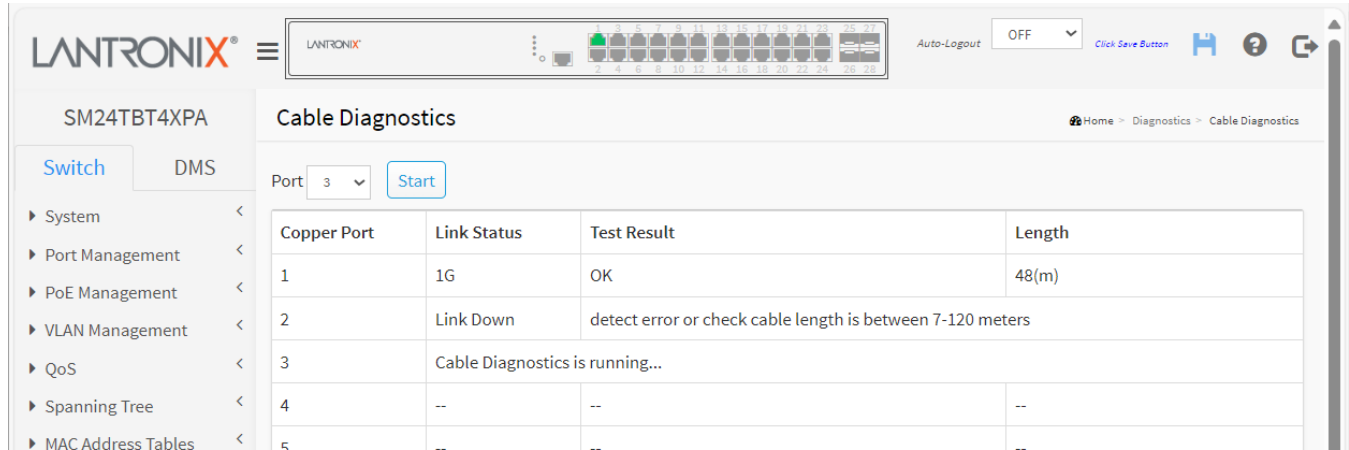


Figure 20-3: Cable Diagnostics

Parameter descriptions:

Port : The port where you are requesting Cable Diagnostics.

Copper Port: Copper port number.

Link Status: The status of the cable.

10M: Cable is link up and correct. Speed is 10Mbps

100M: Cable is link up and correct. Speed is 100Mbps

1G: Cable is link up and correct. Speed is 1Gbps

Link Down: Link down or cable is not correct.

Test Result: Test Result of the cable.

OK: Correctly terminated pair

Abnormal: Incorrectly terminated pair or link down

Length: The length (in meters) of the cable pair. The resolution is 3 meters. When Link Status is shown as follows, the length has a different definition.

1G: The length is the minimum value of 4-pair.

10M/100M: The length is the minimum value of 2-pair.

Link Down: The length is the minimum value of non-zero of 4-pair.

Button

Start : Click to start cable diagnostics on the selected port.

Messages:

10 and 100 Mbps ports will be linked down and lost connection while running Cable Diagnostics.

Are you sure you want to continue?

Note that Diagnostics is only accurate for cables of length 7-120 meters.

20-4 Mirroring

You can mirror traffic from any source port to a target port for real-time analysis. You can then attach a logic analyzer or RMON probe to the target port and study the traffic crossing the source port in a completely unobtrusive manner.

Mirror Configuration lets you monitor network traffic. For example, assume that Port A and Port B are Monitoring Port and Monitored Port respectively, so the traffic received by Port B will be copied to Port A for monitoring.

To configure the Port Mirror function in the web UI:

1. Click Diagnostics and Mirroring.
2. Select the Monitor Destination Port (Mirror Port).
3. Select a mode (disabled, enable, TX Only and RX only) for each monitored port.
4. Click the Apply button to save the settings.

Figure 20-4: Mirror Configuration

Parameter descriptions:

Monitor Session: At the dropdown select the monitor session (instance number). At the dropdown select 1-5.

Monitor destination port: Port to output the mirrored traffic. Also known as the mirror port. Frames from ports that have either source (rx) or destination (tx) mirroring enabled are mirrored on this port. Select Disabled or 1-28. The default is Disabled.

Mirror Source 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: Disabled, tx, rx, or both. The default is Disabled.

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.

Buttons

Apply: Click to save changes.

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

20-5 sFlow

20-5.1 Configuration

The sFlow Collector configuration for the switch can be monitored and modified here. The configuration is divided into two parts: Configuration of the sFlow receiver (a.k.a., sFlow collector) and configuration of per-port flow and counter samplers.

sFlow configuration is not persisted to non-volatile memory, which means that a reboot or master change will disable sFlow sampling.

To configure sFlow in the web UI:

1. Click Diagnostics, sFlow and Configuration.
2. Set the sFlow parameters.
3. Click Apply to save the setting.
4. To cancel the settings click the Reset button. It will revert to previously saved values.

LANTRONIX® SM24TBT4XPA sFlow Configuration

Home > Diagnostics > sFlow > Configuration

Switch DMS

System < Port Management < PoE Management < VLAN Management < QoS < Spanning Tree < MAC Address Tables < Multicast < DHCP < Security < Access Control < SNMP < MEP < ERPS < EPS < Perception < PTP < Event Notification < Diagnostics > Ping > Traceroute > Cable Diagnostics > Mirroring > 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"/> | <> | 0 | 128 | <input type="checkbox"/> | 0 |
| 1 | <input type="checkbox"/> | Tx | 0 | 128 | <input type="checkbox"/> | 0 |
| 2 | <input type="checkbox"/> | Tx | 0 | 128 | <input type="checkbox"/> | 0 |
| 3 | <input type="checkbox"/> | Tx | 0 | 128 | <input type="checkbox"/> | 0 |
| 4 | <input type="checkbox"/> | Tx | 0 | 128 | <input type="checkbox"/> | 0 |
| 5 | <input type="checkbox"/> | Tx | 0 | 128 | <input type="checkbox"/> | 0 |
| 6 | <input type="checkbox"/> | Tx | 0 | 128 | <input type="checkbox"/> | 0 |

Figure 20-5.1: sFlow Configuration

Parameter descriptions:

Agent Configuration

IP Address: The IP address used as Agent IP address in sFlow datagrams. It serves as a unique key that will identify this agent over extended periods of time. Both IPv4 and IPv6 addresses are supported.

Receiver Configuration

Owner: sFlow can be configured in two ways: 1) via local management using the Web or 2) CLI interface or through SNMP. This read-only field shows the owner of the current sFlow configuration and assumes values as follows:

- If sFlow is currently unconfigured/unclaimed, Owner contains <none>.
- If sFlow is currently configured through Web or CLI, Owner contains <Configured through local management>.
- If sFlow is currently configured through SNMP, Owner contains a string identifying the sFlow receiver. If sFlow is configured through SNMP, all controls - except for the Release-button - are disabled to avoid inadvertent reconfiguration.

The Release button allows for releasing the current owner and disable Flow 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 - 200 bytes with default being 128 bytes. If the maximum datagram size does not consider the maximum header size, samples may be dropped.

Counter Poller Enabled: Enables/disables counter polling on this port.

Counter Poller Interval: With counter polling enabled, this specifies the interval -in seconds -between counter poller samples.

Buttons

Apply : Click to save changes.

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

Release : See description under Owner above.

Refresh : Click to refresh the page. Note that unsaved changes will be lost.

20-5.2 Statistics

This page shows receiver and per-port sFlow statistics. To Display sFlow port statistics in the web UI:

1. Click Diagnostics, sFlow and Statistics.
2. View the sFlow information.

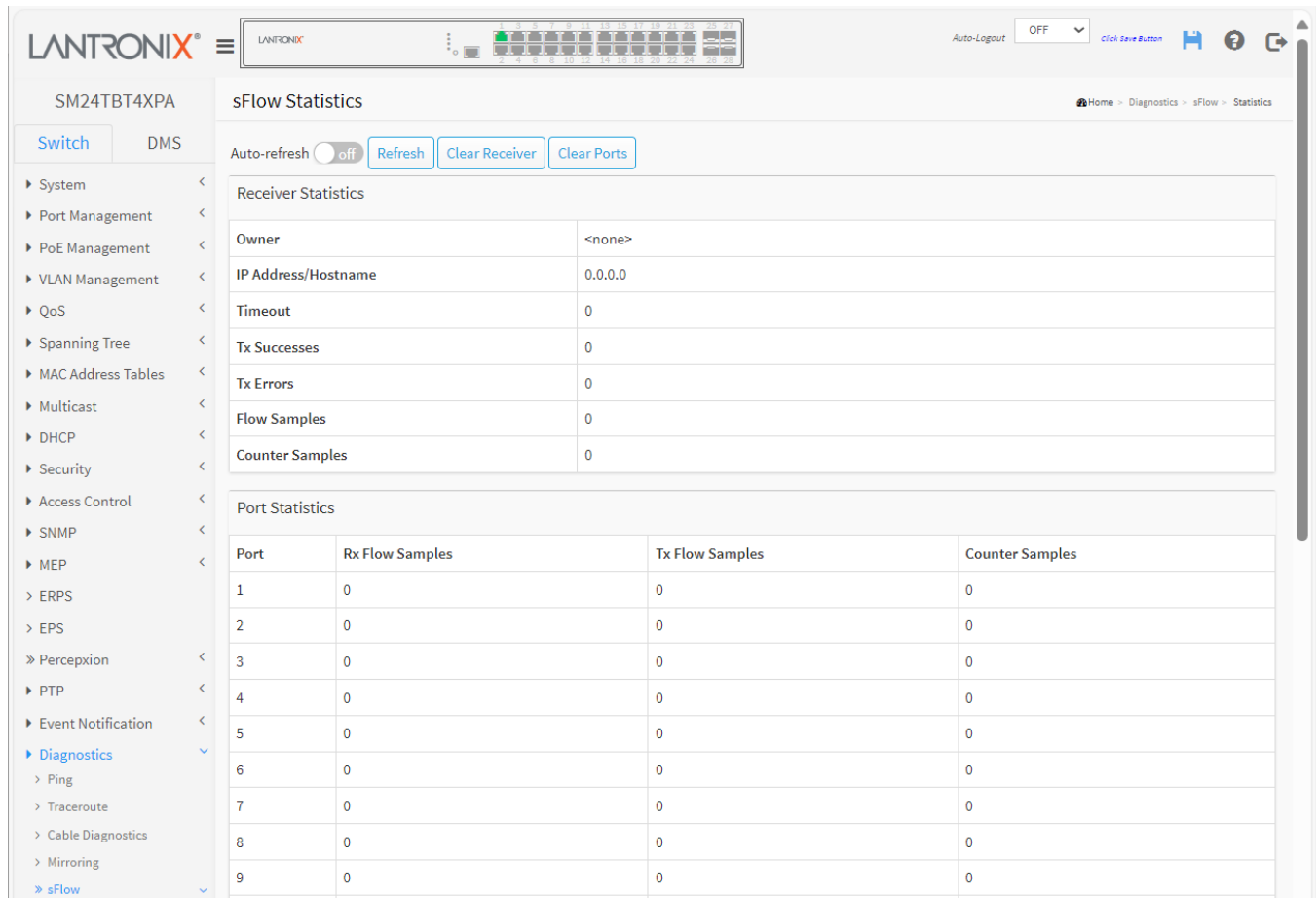


Figure 20-5.2: sFlow Statistics

Parameter descriptions:

Receiver Statistics

Owner: This field shows the current owner of the sFlow configuration. It assumes one of three values as follows:

- If sFlow is currently unconfigured/unclaimed, Owner contains <none>.
- If sFlow is currently configured through Web or CLI, Owner contains <Configured through local management>.
- If sFlow is currently configured through SNMP, Owner contains a string identifying the sFlow receiver.

IP Address/Hostname: The IP address or hostname of the sFlow receiver.

Timeout: The number of seconds remaining before sampling stops and the current sFlow owner is released.

Tx Successes: The number of UDP datagrams successfully sent to the sFlow receiver.

Tx Errors: The number of UDP datagrams that has failed transmission. The most common source of errors is invalid sFlow receiver IP/hostname configuration. To diagnose, paste the receiver's IP address/hostname into the Ping web page (Diagnostics > Ping/Ping6).

Flow Samples: The total number of flow samples sent to the sFlow receiver.

Counter Samples: The total number of counter samples sent to the sFlow receiver.

Port Statistics

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

Rx and Tx Flow Samples: The number of flow samples sent to the sFlow receiver originating from this port. Here, flow samples are divided into Rx and Tx flow samples, where Rx flow samples contains the number of packets that were sampled upon reception (ingress) on the port and Tx flow samples contains the number of packets that were sampled upon transmission (egress) on the port.

Counter Samples: The total number of counter samples sent to the sFlow receiver originating from this port.

Buttons

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

Refresh: Click to refresh the page immediately.

Clear Receiver : Clears the sFlow receiver counters.

Clear Ports : Clears the per-port counters.

21. Maintenance

This chapter describes the Maintenance configuration tasks including Save/Backup/Restore/Activate/Delete /Restart Device, Factory Defaults, Firmware upgrade, and Firmware swap.

21-1 Configuration

The switch stores its configuration in a number of files in text format. The files are either virtual (RAM-based) or stored in flash on the switch.

There are three system files:

running-config: A virtual file that represents the currently active switch configuration. 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.

21-1.1 Save startup-config

This copy running-config to startup-config, thereby ensuring that the current active configuration will be used at the next reboot. To save running configuration in the web UI:

1. Click Maintenance, Configuration, and Save Startup-config.
2. Click Save Configuration.

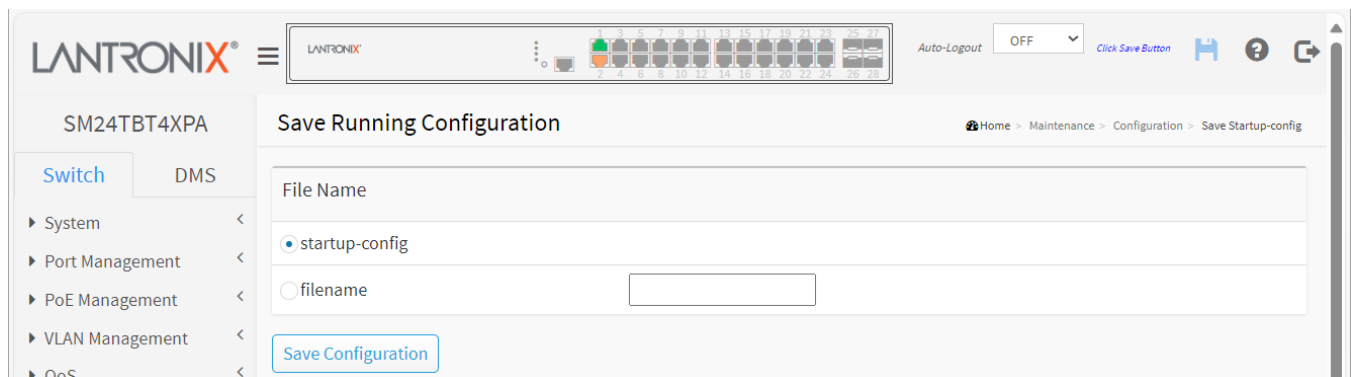


Figure 21-1.1: Save Startup Configuration

Parameter descriptions:

File Name: Select a filename or enter a filename.

Button

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. When done, the message *“save running config to startup-config successfully.”* displays.

21-1.2 Backup

This page lets you export the switch configuration for maintenance needs. Any current configuration files will be exported in text format.

The configuration files on the switch can be backed up and saved on the workstation running the web browser. It is possible to transfer any of the files on the switch to the web browser. Select the running-config may take a little while to complete, as the file must be prepared before backup.

To back up a configuration in the web UI:

1. Click Maintenance, Configuration and Backup.
2. Click Backup.

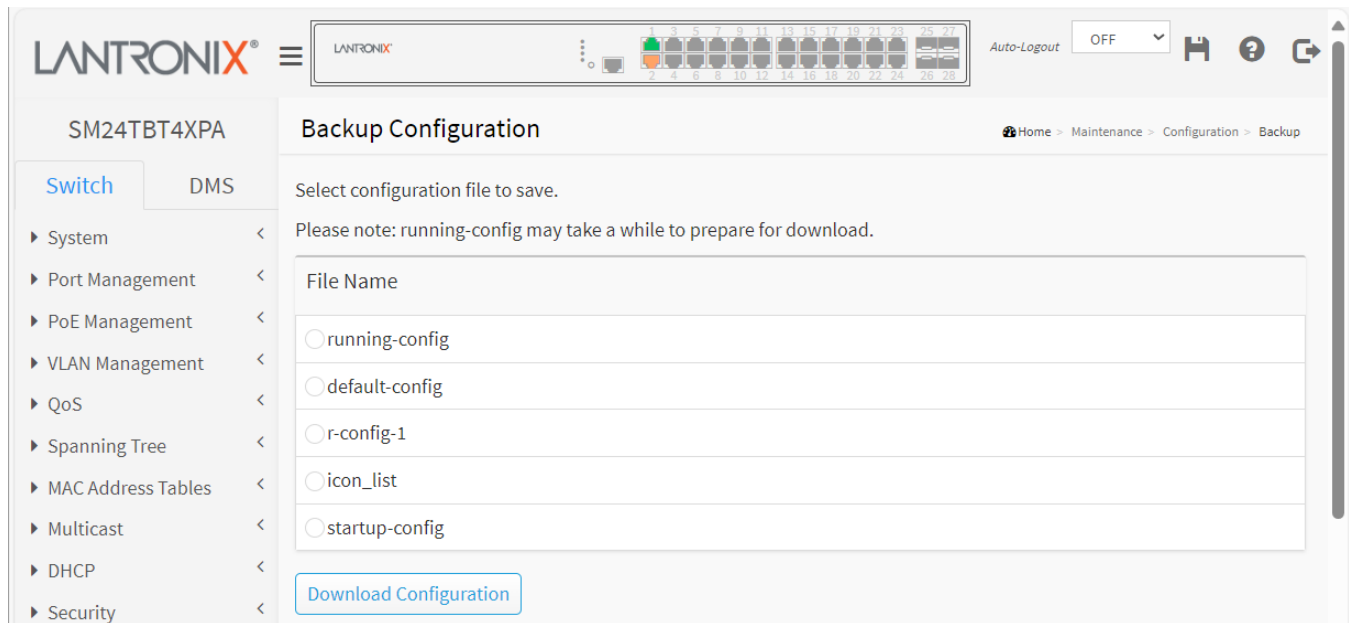


Figure 21-1.2: Backup

Parameter descriptions:

running-config: A virtual file that represents the currently active configuration on the switch. This file is volatile.

default-config: A read-only file with vendor-specific configuration. This file is read when the system is restored to default settings.

startup-config: The startup configuration for the switch, read at boot time.

Button

Download Configuration: Click the button then the switch will start to transfer the configuration file to your workstation.

21-1.3 Restore

It is possible to import a file from the web browser to all the files on the switch (except default-config, which is read-only).

Select the source file to restore then select the destination file on the target.

If the destination is running-config, the file will be applied to the switch configuration. This can be done in one of two ways:

Replace mode: The current configuration is fully replaced with the configuration specified in the source file.

Merge mode: The source file configuration is merged into running-config.

To restore a configuration in the web UI:

1. Click Maintenance, Configuration and Restore.
2. Click Restore.

The screenshot shows the 'Restore Configuration' page in the Lantronix web UI. The sidebar on the left lists various configuration categories under 'Switch' and 'DMS'. The main area is titled 'Restore Configuration' and includes a breadcrumb trail: Home > Maintenance > Configuration > Restore. The 'File to Upload' section has a 'Choose File' button and shows 'No file chosen'. The 'Destination File' section contains a table with the following data:

| File Name | Parameters |
|---------------------------------------|--|
| <input type="radio"/> running-config | <input checked="" type="radio"/> Replace <input type="radio"/> Merge |
| <input type="radio"/> r-config-1 | |
| <input type="radio"/> icon_list | |
| <input type="radio"/> startup-config | |
| <input type="radio"/> Create new file | <input type="text"/> |

At the bottom of the form is an 'Upload Configuration' button.

Figure 21-1.3: Restore Configuration

Parameter descriptions:

running-config: A virtual file that represents the currently active configuration on the switch. This file is volatile.

Replace: The current configuration is fully replaced with the configuration in the uploaded file.

Merge: The uploaded file is merged into running-config.

startup-config: The startup configuration for the switch, read at boot time.

Create New File : Click to create new files.

Buttons

Choose File: Click the button to search the configuration text file and filename

Upload Configuration: Click the button to start transfer the source file to the destination file.

21-1.4 Activate

It is possible to activate any of the configuration files present on the switch, except for running-config which represents the currently active configuration.

Select the file to activate and click Activate Configuration. This will initiate the process of completely replacing the existing configuration with that of the selected file.

Note: The previous configuration will be completely replaced, potentially leading to loss of management connectivity. The activated configuration file will NOT be save to startup-config automatically.

To activate a configuration in the web UI:

1. Click Maintenance, Configuration, and Activate.
2. Click the Activate Configuration button.

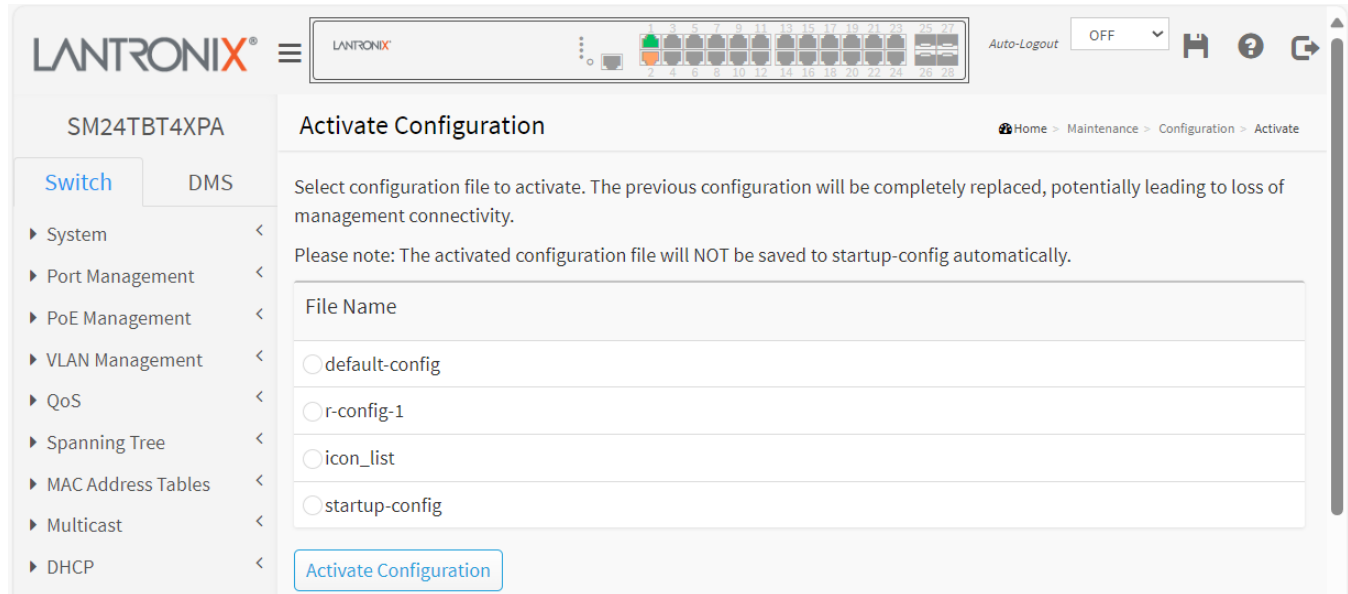


Figure 21-1.4: Activate Configuration

Parameter descriptions:

File Name: Select a filename (e.g., default-config or startup-config).

Buttons

Activate Configuration: Click the button so the selected file will be activated as the switch's running configuration.

21-1.5 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 settings.

To delete a configuration in the web UI:

1. Click Maintenance, Configuration, and Delete.
2. Select the configuration file to be deleted.
3. Click the Delete Configuration File button.

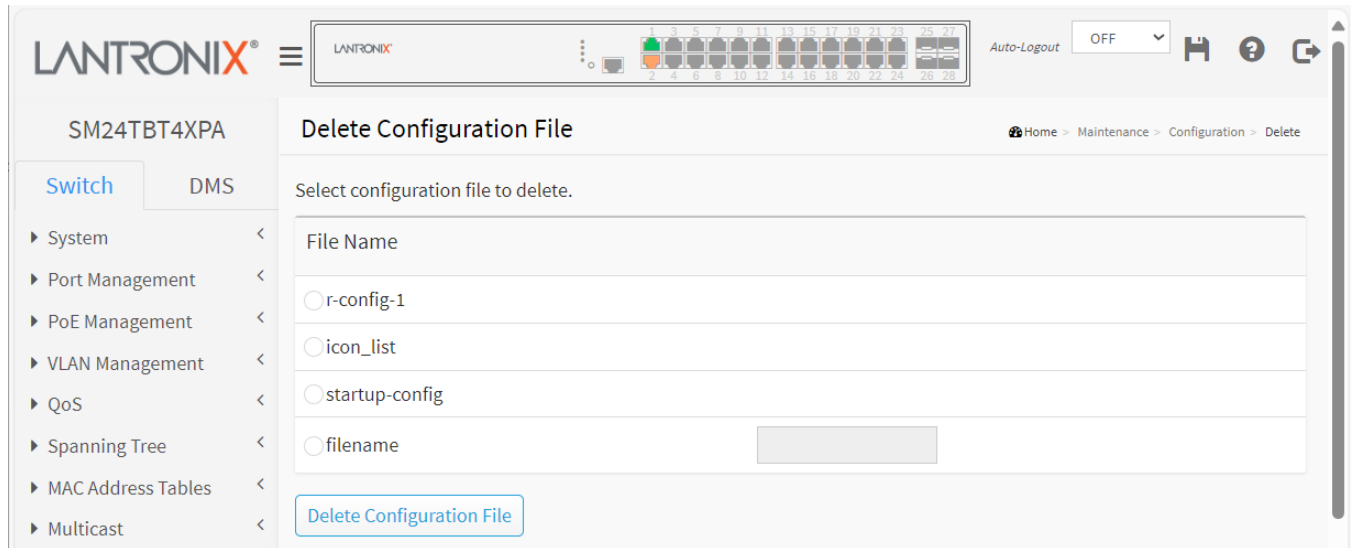


Figure 21-1.5: Delete Configuration File

Parameter descriptions:

Filename: Select the configuration file to be deleted.

Buttons

Delete Configuration File: Click the button then the selected file will be deleted.

21-2 Restart Device

This page lets you restart the switch for any maintenance needs. Any configuration files or scripts that you saved in the switch should still be available afterwards.

To Restart Device in the web UI:

1. Click Maintenance and Restart Device.
2. If desired, check the Always On PoE button (optional).
3. At the confirmation prompt click Yes.

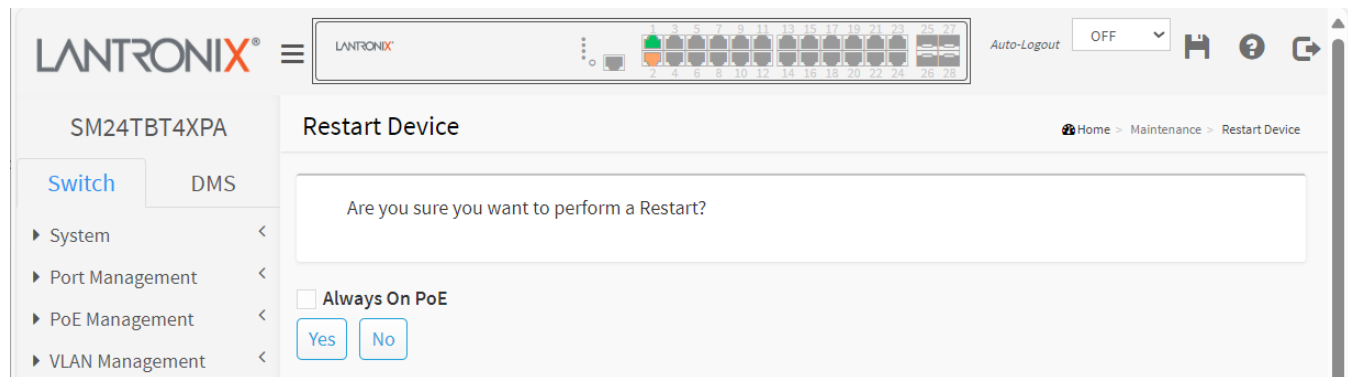


Figure 21-2: Restart Device

Parameter descriptions:

Restart Device : Click to restart the switch on this page. After restart, the switch will boot normally.

Buttons

Yes: Click to restart the switch.

No: Click to cancel the restart operation.

Always On PoE: Check this button so that when the switch does a warm restart, it will continue supplying PoE power to PDs. The default is disabled.

21-3 Factory Defaults

This page lets you restore the switch configuration to its factory default settings. To restore the switch to factory defaults in the web UI:

1. Click Maintenance and Factory Defaults.
2. Check or uncheck the box to keep the current IP configuration.
3. At the confirmation prompt click the Yes button.

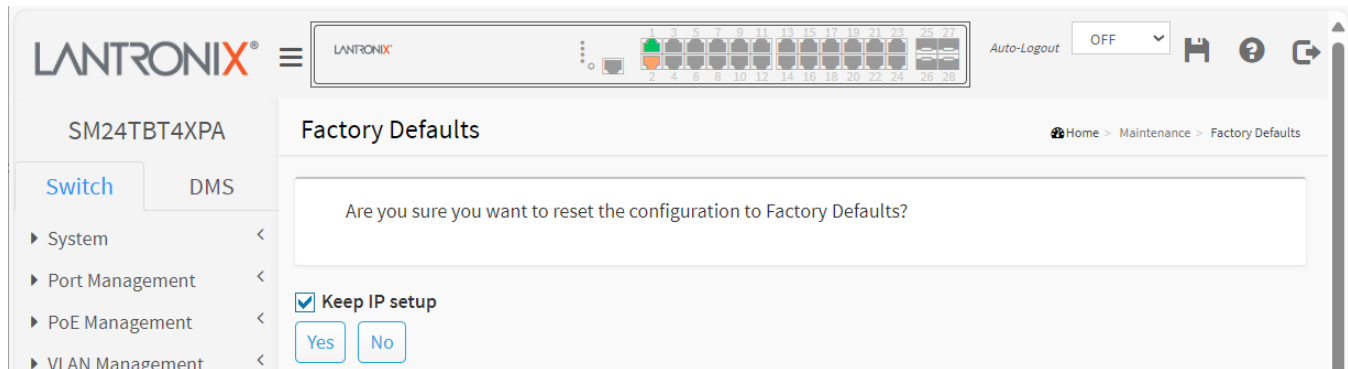


Figure 21-3: Factory Defaults

Parameter descriptions:

Keep IP Configuration: Check the box if you want to keep the current IP settings after the switch is reset.

Buttons

Yes: Click to reset the configuration to Factory Defaults.

No: Click to cancel the factory reset operation.

Messages:

Configuration Factory Reset Done

The configuration has been reset. The new configuration is available immediately.

21-4 Firmware

This section lets you upgrade switch firmware and activate an alternate firmware image.

21-4.1 Firmware Upgrade

This page lets you update the firmware controlling the switch. To update switch firmware in the web UI:

1. Click Maintenance, Firmware, and Firmware Upgrade.
2. Browse to and select the desired firmware file.
3. If desired, check the Always On PoE checkbox (optional).
4. Click the Upload button.

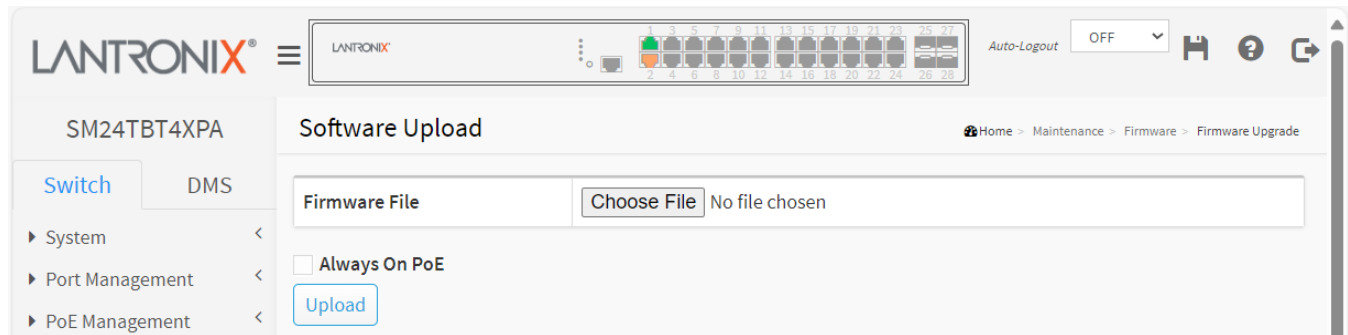


Figure 21-4.1 Firmware Upload

Parameter descriptions:

Browse: Click the button to search the firmware URL and filename.

Always On PoE: Check this button so when the switch preforms a warm restart it will continue supplying PoE power to the PDs.

Upload: Click to begin the firmware upload process.

21-4.2 Firmware Selection

This page provides information about the active and alternate (backup) firmware images in the device, and allows you to activate the alternate image.

The web page displays two tables with information about the active and alternate firmware images. To show the firmware information or swap boot firmware in the web UI:

- 1. Click Maintenance, Firmware, and Firmware Selection.
- 2. Click the Activate Alternate Image button to swap firmware versions.

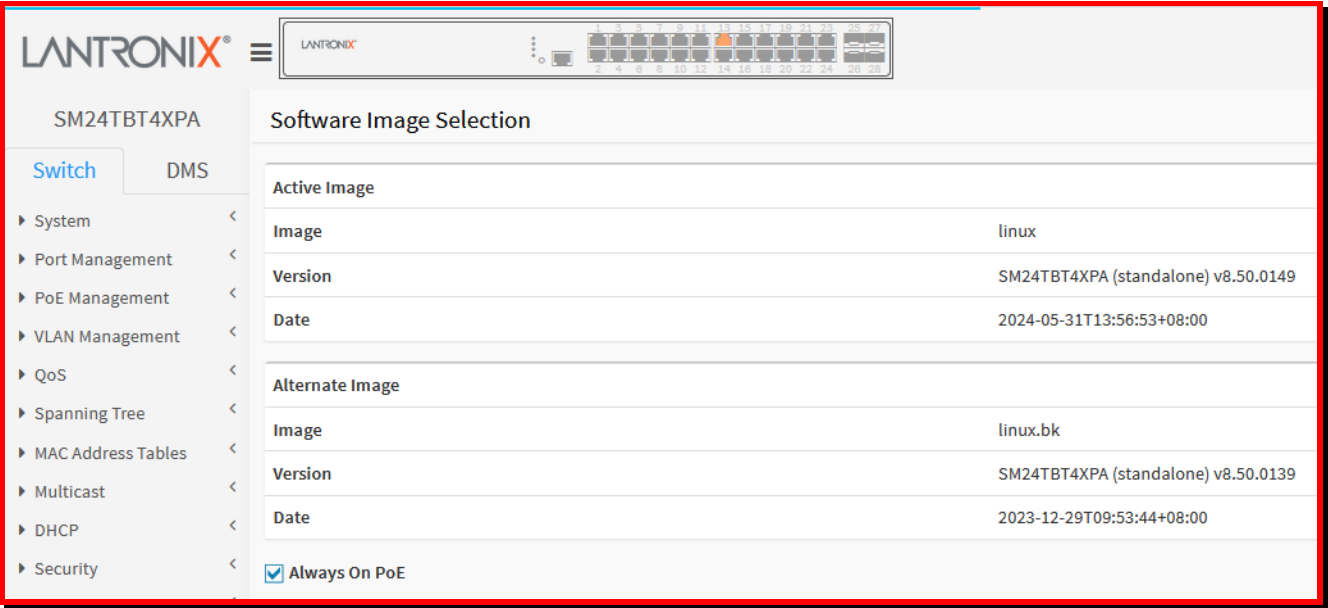


Figure 21-4.2 Firmware Selection

Image Information

Image: The file name of the firmware image, from when the image was last updated.

Version: The version of the firmware image.

Date: The date and time when the firmware was produced.

Buttons

Activate Alternate Image: Click to use the Alternate Image. This button may be disabled depending on system state.

Cancel: Click to cancel activating the alternate image and navigate away from this page.

Always On PoE: Check this button so when the switch performs a warm restart it will continue supplying PoE power to the PDs.

22. DMS (Device Management System)

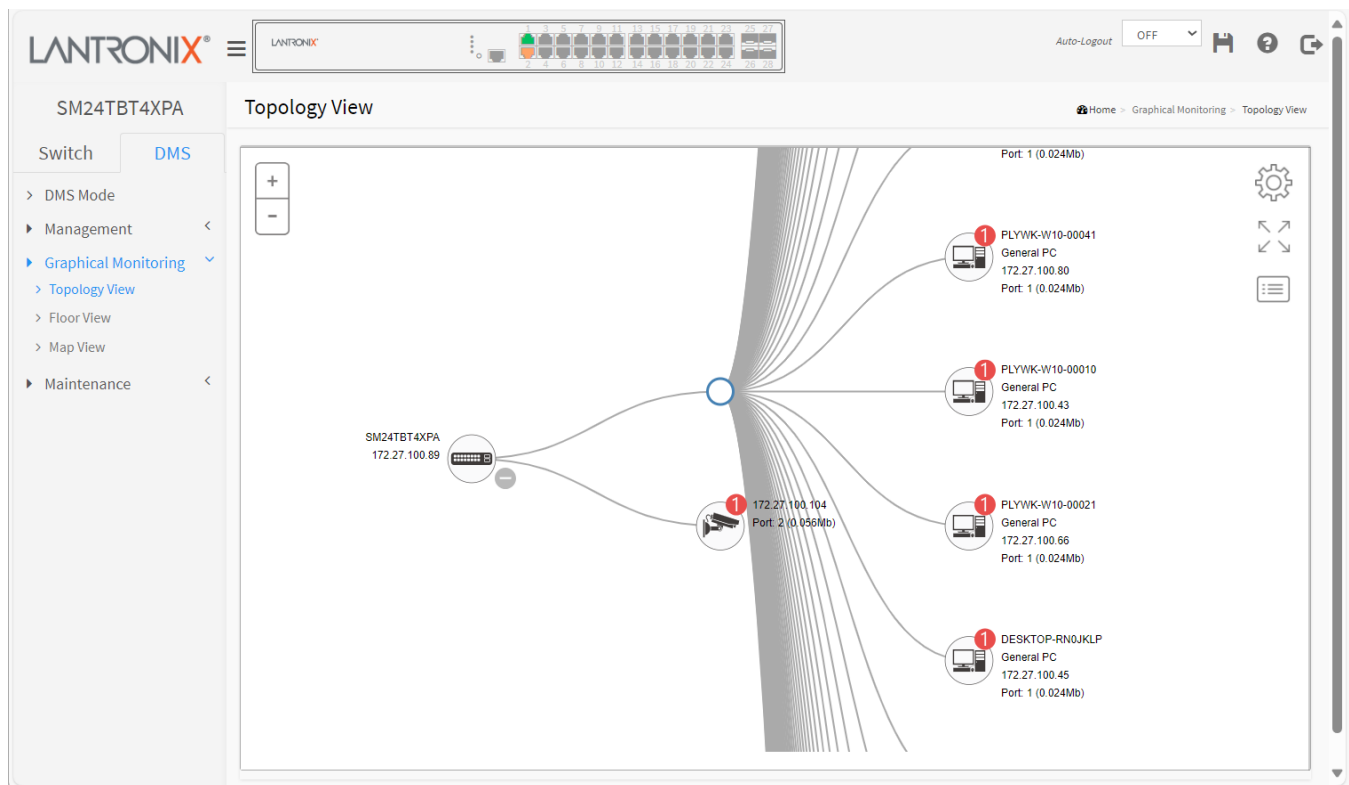
The Lantronix DMS (Device Management System) is an intelligent management tool embedded in the switch to intuitively help IT/TS in reducing support time, cost, and effort.

In the SM24TBT4XPA main menu pane on the left, navigate to the DMS tab to display the main DMS features: DMS Mode, Management, Graphical Monitoring, and Maintenance.

DMS features include:

- DMS automatically discovers and displays all devices connected to the switch using standard networking protocols such as LLDP, UPnP, [ONVIF](#), etc.
- DMS supports up to 256 devices within four subnets.
- DMS operates via an intuitive web GUI to allow you to:
 - Power down the IP cameras, NVRs, or any PoE devices.
 - Remotely identify the exact cable break location.
 - Detect abnormal traffic issues on IP cameras/NVR.
 - Monitor devices' status (e.g., link up, PoE power, traffic, etc.).
 - Configure VLAN/QoS intuitively for better solution quality/reliability.

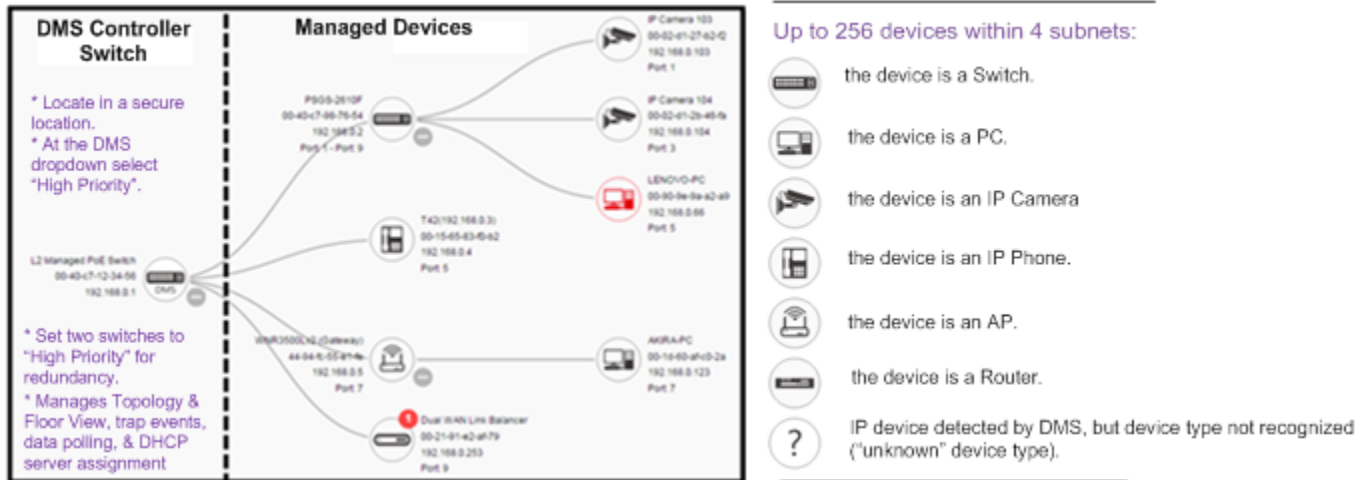
When you click the DMS tab, the default (startup) DMS webpage (DMS > Graphical Monitoring > Topology View) displays:



22-1 DMS Mode - DMS Controller Switch

You can configure DMS mode and monitor device numbers/ DMS Controller Switch IP.

- DMS is controlled by the DMS Controller switch, as specified by DMS Mode selection.
- The DMS Controller Switch is in charge of syncing DMS information in order to manage Topology View, Floor View, and trap event / data polling / DHCP server assignment.



DMS Controller Switch and Managed Devices

Note:

1. If there are more than two Switches set as High-priority or no High-priority mode switch, the Switch with the longer system uptime will be the DMS Controller switch. If two switches have same up time, the switch with the smaller MAC address will be assigned as the DMS Controller Switch.
2. You can set two switches to High Priority for Controller Switch redundancy.
3. The DMS Controller Switch should be put in a secure location such as a server room, with access and authority limited to IT staff.
4. The DMS Controller Switch is the center of IP / Event management to operate the DMS:
 - a. When enabled DHCP Server mode in DMS network, the DMS Controller switch is responsible for assigning IP address for all devices.
 - b. The DMS Controller Switch will Collect, Poll, and Sync DMS information, and act as the Event Notification control center to manage all device information.

22-2 DMS Mode

1. Click DMS > DMS Mode to display the DMS Information page.
2. At the DMS Mode dropdown select Enabled or Disabled.
3. At the DMS Priority dropdown select High, Mid, Low, or Non.
4. Click the Apply button. The DMS Information page updates.

LANTRONIX® SM24TBT4XPA

Information

Home > DMS Mode

Switch DMS

> DMS Mode

► Management <

► Graphical Monitoring <

► Maintenance <

| | |
|---------------------|---------------|
| Mode | Enabled |
| Controller Priority | Low |
| Total Device | 101 |
| On-line Devices | 93 |
| Off-line Devices | 8 |
| Controller IP | 172.27.100.89 |

Apply

DMS Mode Information parameters

DMS Mode: At the dropdown select Enabled or Disabled. The default is Enabled.

DMS Priority: At the dropdown select High, Mid, Low, or Non.

High: Choose "High" to make this switch the DMS Controller switch (Master switch).

Mid: Makes this switch a middle (medium) priority.

Low: Makes this switch a low priority (default).

Non: This switch will never become the Controller switch (Master switch). This is the default setting.

Low

High

Mid

Low

Non

Total Devices: Displays the Total / On-line/ Off-line Devices count in the DMS network (read only).

On-line Devices: Displays the total number of discovered devices that are currently on line (e.g., 3).

Off-line Devices: Displays the total number of discovered devices that are currently off line (e.g., 1).

Controller IP: Displays the active DMS Controller Switch's IP Address (read only).

DMS Mode Buttons


Apply: Click to save changes.

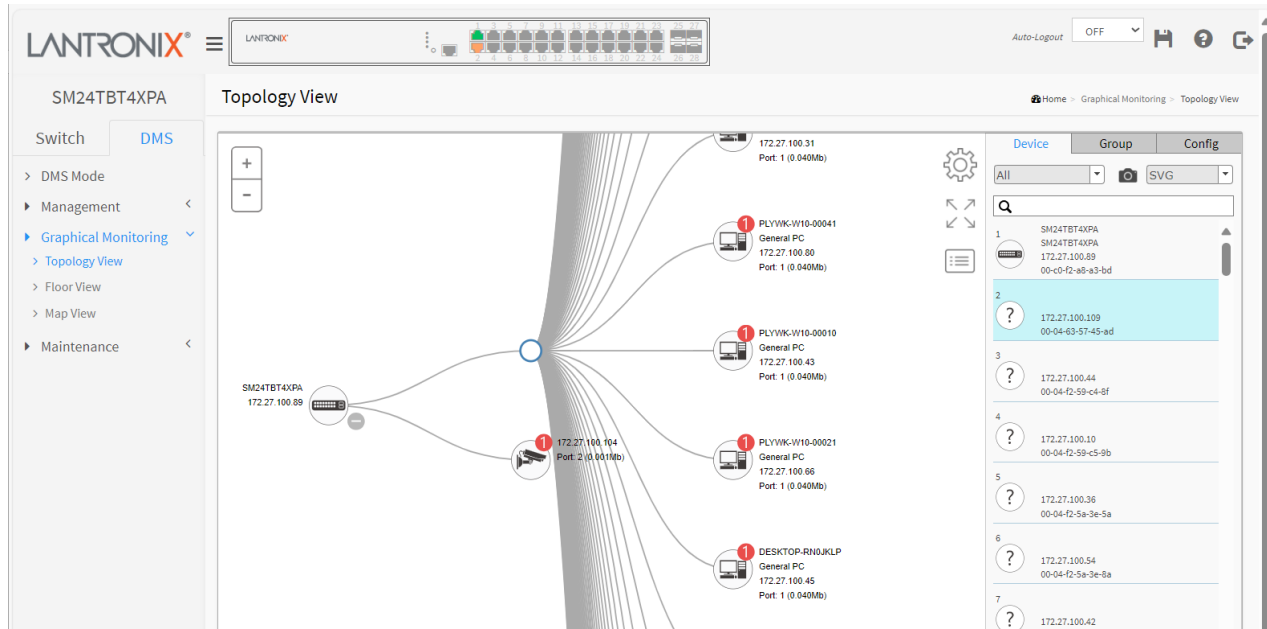
22-3 Graphical Monitoring

Navigate to the DMS > Graphical Monitoring menu path to view the options of DMS Graphical Monitoring Topology View, Floor View, and Map View.

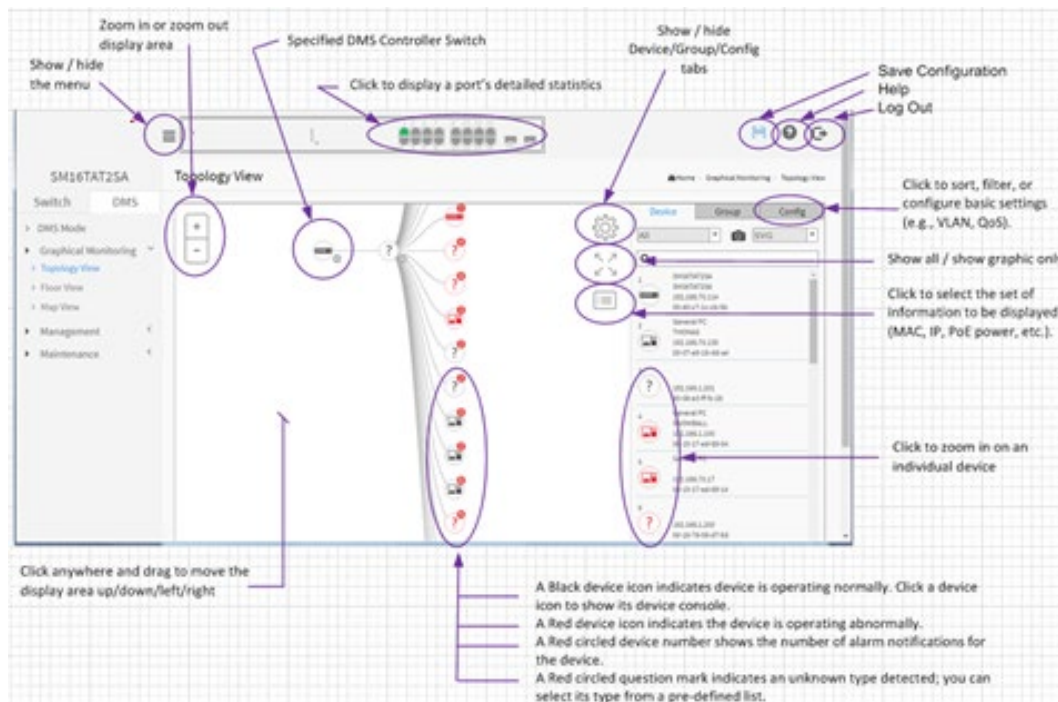
22-3.1 Topology View

Navigate to the DMS > Graphical Monitoring > Topology View menu path. Note that FW v1.02.1327 adds automatic logout when the screen is idle for over 10 minutes on the DMS Topology View page.

Click the  button to display the right pane menu tabs (Device, Group, and Config).



The Topology View icons and controls are shown and described below.







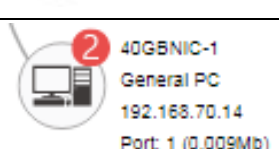

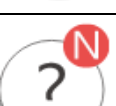
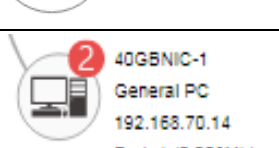
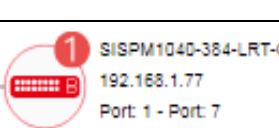
Topology View Icons / Controls

Click anywhere and drag to move the display area up /down/ left /right.

| | |
|--|---|
| | Click "+" or "-" to zoom in or zoom out the display area. |
| | A Black device icon indicates device is operating normally. Click a device icon to show its device console. |
| | A Red device icon indicates the device is operating abnormally. |
| | A Red circled device number shows the number of alarm notifications for the device. |
| | Click this icon to select the set of information to be displayed (MAC, IP, PoE power, etc.). |
| | Click this icon to sort, filter, or configure basic settings (e.g., VLAN, QoS). |

Device Categories and Statuses


| | |
|--|--|
| | The device is a Switch. |
| | The device is a General switch. |
| | The device is a PC. |
| | The device is an IP Camera. |
| | The device is an IP Phone. |
| | The device is a Wireless Access Point (WAP). |
| | The device is a Router. |

| | |
|---|--|
|  | The device is an LED Light. |
|  | Black icon: Device link up. You can select a function and check for issues. |
|  | Red icon: Device link down. You can diagnose the link status. |
|  | Icon with number: indicates some event has occurred (e.g. Device Off-line, IP Duplicate, etc.) on the IP device; you can click on the device icon to check events in Notification. |
|  | A Red circled device number shows the number of alarm notifications for the device. |
|  | Icon with question mark: Unknown Device; the IP device is detected by DMS, but the device type can't be recognized and will be classified as an 'Unknown' device type. |
|  | Icon with question mark and red N: indicates the device is 'Unknown' and is not connected. |
|  | A Black device icon indicates device is operating normally. Click the device icon to show its device console. |
|  | A Red device icon indicates the device is operating abnormally. |

DMS Topology View parameters

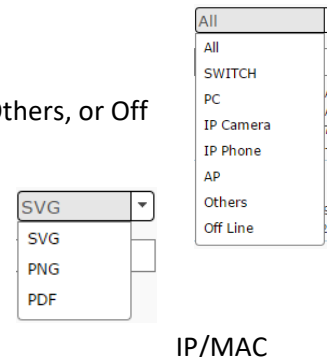
Device tab parameters

Devices dropdown: Select the device type (All, SWITCH, PC, IP Camera, IP Phone, AP, Others, or Off Line).

Snapshot icon: Use the  icon to capture the displayed topology view.

File format: Select the graphics file type (SVG, PNG, or PDF).

Search box: Use the to search for a device by typing address or Model/Device name.



Group tab parameters

Vlan ID: Enter a VLAN ID (VID) for the new group (1-4095).

Name: Enter a name for the new group.

Traffic Priority: At the dropdown select Default or 0 (Low) – 7 (High).

OUI 1: Enter an Organizationally Unique Identifier.

OUI 2: Enter a second Organizationally Unique Identifier.

OUI 3: Enter a third Organizationally Unique Identifier.

Apply: Click when done entering the new group data.

Delete: Click to close the new group configuration dialog.

Config tab parameters

Total Device: Displays the total number of devices discovered.

Controller IP: The control device IP address in the format 0.0.0.0.

DHCP Server IP: The IP address of the configured DHCP Server; otherwise --- if no DHCP Server is configured.

DHCP Server: At the dropdown select Enabled or Disabled. The default is Disabled.

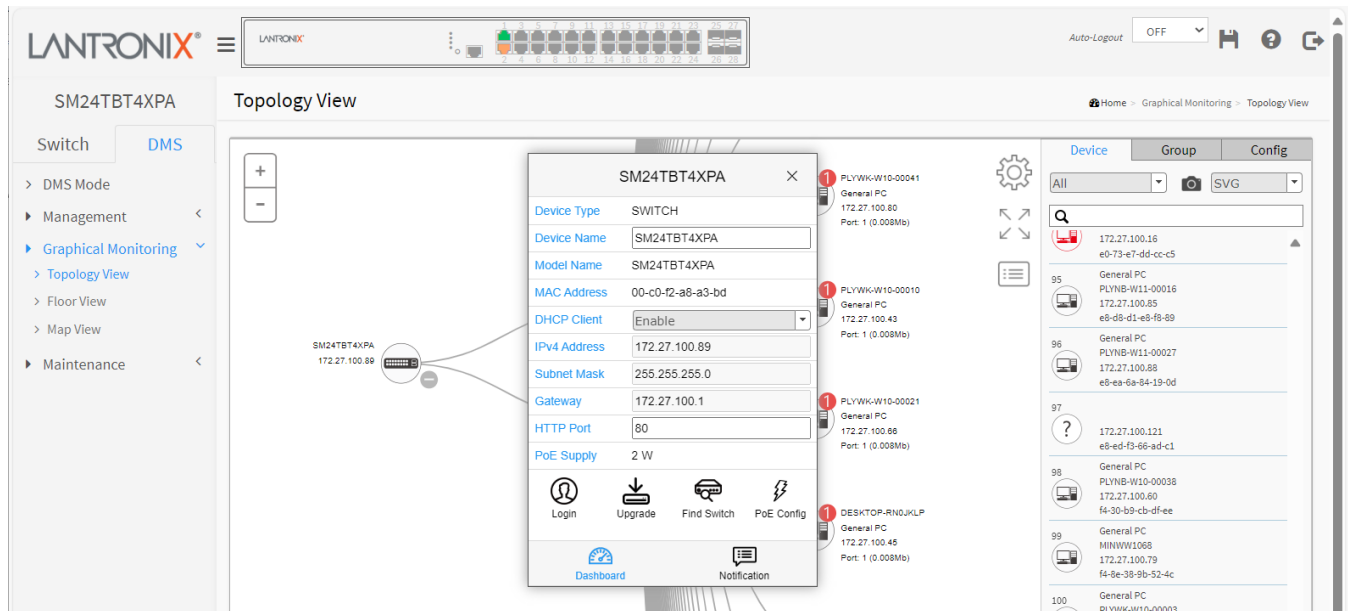
IP Range: The range type (Single Subnet or Multiple Subnet).

If you select Multiple Subnet, selection fields display for Range 1 - Range 4.

Apply: Click the button to make the changes.

Device data

Click a device in the Topology View to display its discovered data:



Device data parameters

Device Type: e.g., SWITCH, PC, IP Camera, IP Phone, AP (Access Point). Device Type is displayed automatically. If an unknown type is detected, you can still select its type from a pre-defined list. An IP device recognized as a DMS Control switch supports "Upgrade" and "Find Switch" functions.

An IP device recognized as a PoE device supports "Upgrade" and "Reboot" functions.

An IP device recognized as an IP Camera via the [ONVIF](#) protocol will support the "Streaming" function.

Device Name: e.g., SM24TBT4XPA. Create your own Device Name or alias for easy management such as "1F_Lobby_Cam1".

Model Name: e.g., SM24TBT4XPA.

Mac Address: e.g., 00-40-c7-1c-cb-6e; displayed automatically by DMS.

IP Address: e.g., 192.168.1.77; displayed automatically by DMS.

Http port: e.g., port 80.

PoE Used: e.g., 2 Watts; displayed automatically by DMS.

PoE Supply: e.g., PoE or non-PoE.

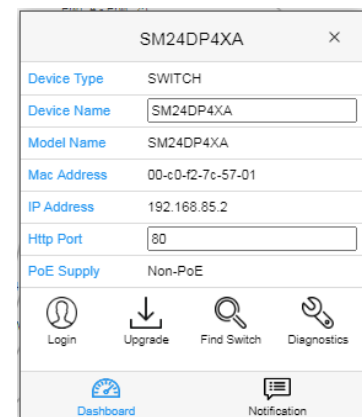
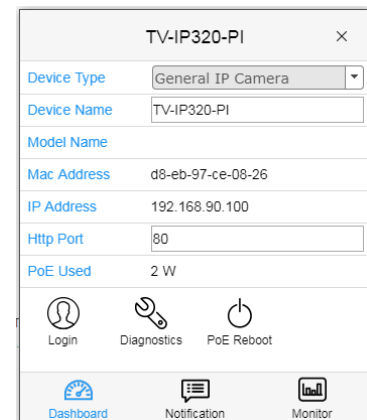
Login icon: Click to display the login window.

Upgrade icon: Click to display a window in which you can enter a Tftp Server IP address and the name of a firmware file to upgrade to.

Find Switch icon: Click to flash the device LEDs for 15 seconds to help find the device. Click **OK** to clear the message.

Parent Node / Undo Parent: click to toggle between switching the selected device with its parent node device and back.

PoE Config icon: Click to display a window in which you can enable or disable PoE Auto Checking globally and enable or disable PoE Mode on a port-by-port basis.



PoE Reboot: Click to re-boot PoE.

PoE Supply and **PoE Used:** displayed automatically by DMS.

Dashboard icon: Click to display the dashboard.

Notification icon: Click to display an editable message area.

Unknown Device parameters

You can click on an unknown device to display its discovered data (see descriptions above). If an unknown type is detected, you can still select its type from a pre-defined list.



| 192.168.1.99 | |
|--|-------------------|
| Device Type | Unknown Device |
| Device Name | |
| Model Name | |
| Mac Address | 00-1b-11-b2-6d-4b |
| IP Address | 192.168.1.99 |
| Http Port | 80 |
| PoE Used | Non-PoE |
| Diagnostics | |
| <div> Dashboard Notification Monitor </div> | |

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” parameter can be set to “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 () icon to display the PoE Auto Checking pane:

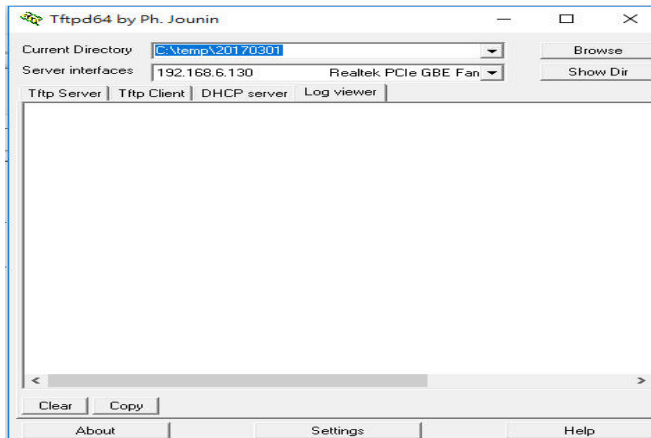
The screenshot displays the Lantronix web interface for the SM24TBT4XPA switch. The left sidebar shows the navigation menu with 'DMS Mode' selected. The main area is titled 'Topology View'. A device configuration popup for 'SM24TBT4XPA' is open, showing the following details:

- Device Type: SWITCH
- Device Name: SM24TBT4XPA
- Model Name: SM24TBT4XPA
- MAC Address: 00-c0-f2-a8-a3-bd
- DHCP Client: Enable
- IPv4 Address: 172.27.100.89
- Subnet Mask: 255.255.255.0
- Gateway: 172.27.100.1
- HTTP Port: 80
- PoE Supply: 2 W

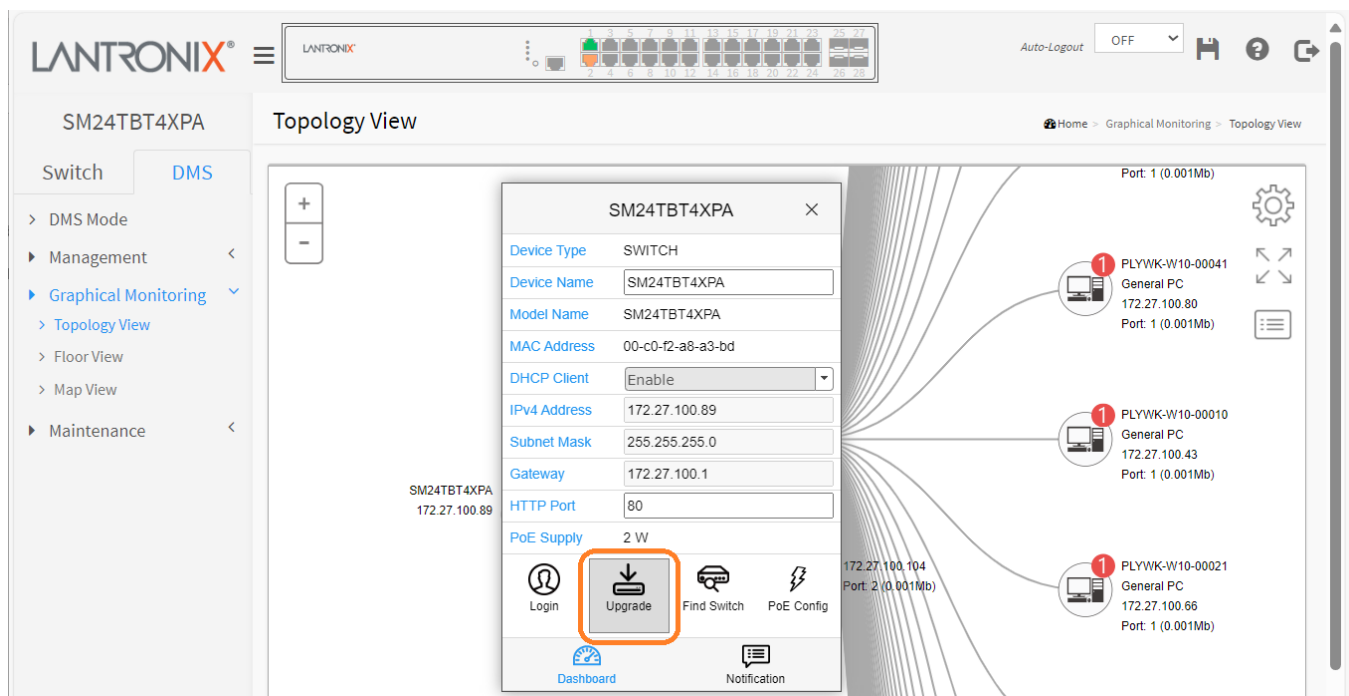
The popup also includes icons for Login, Upgrade, Find Switch, and PoE Config (highlighted with a red box). At the bottom of the popup are icons for Dashboard and Notification. The background shows a network topology with a switch icon and several connected devices, including three 'General PC' devices (PLYWK-W10-00041, PLYWK-W10-00010, PLYWK-W10-00021) connected to Port 1 (0.001Mb).

22-3.2 DMS Firmware Upgrade Procedure

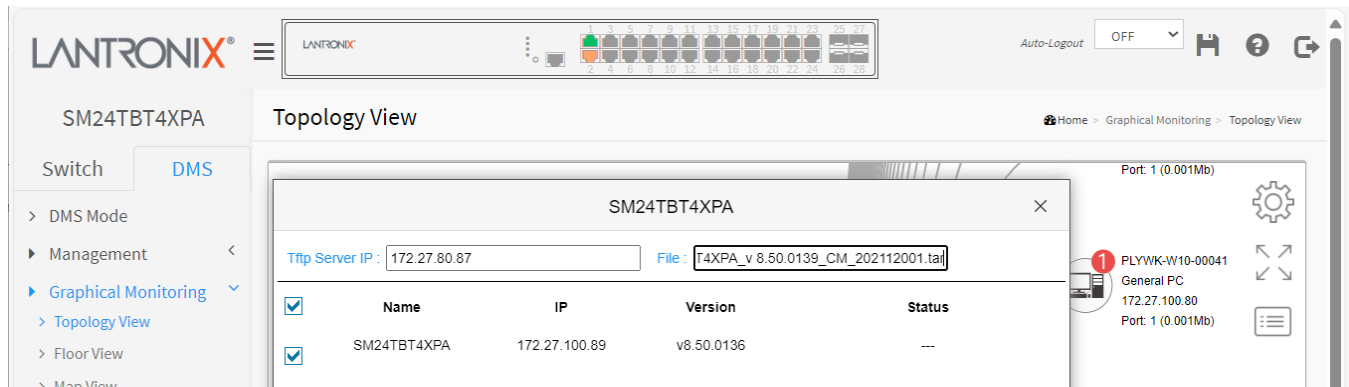
1. Navigate to the DMS > Graphical Monitoring > Topology View or Floor View menu path.
2. Click the  button to display the right pane menu tabs (Entry and Config).
3. Connect all switches and make sure DMS is working.
 - Set all switches with different IP addresses and in the same IP segment.
 - Make sure gateway IP address is configured.
4. Enable the TFTP server and set the correct image path.



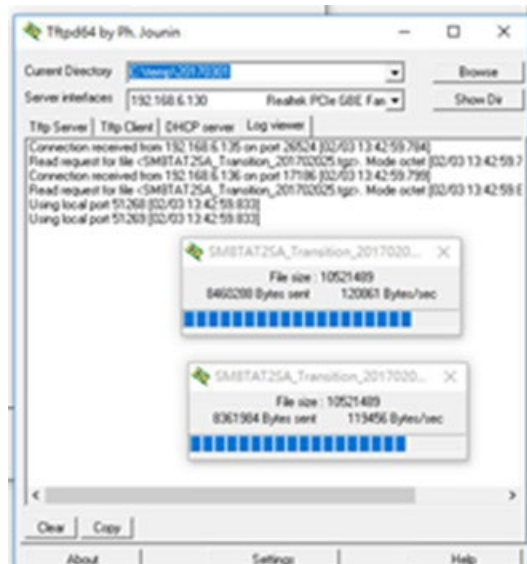
5. Click switch's icon, then click the "Upgrade" button in the Dashboard.



6. Enter a Tftp Server IP address and FW image name (e.g., *SM24TBT4XPA_v 8.50.0139_CM_202112001.tar*).



7. Click “Apply” to start the FW upgrade.
8. Observe the upgrade status until completion.




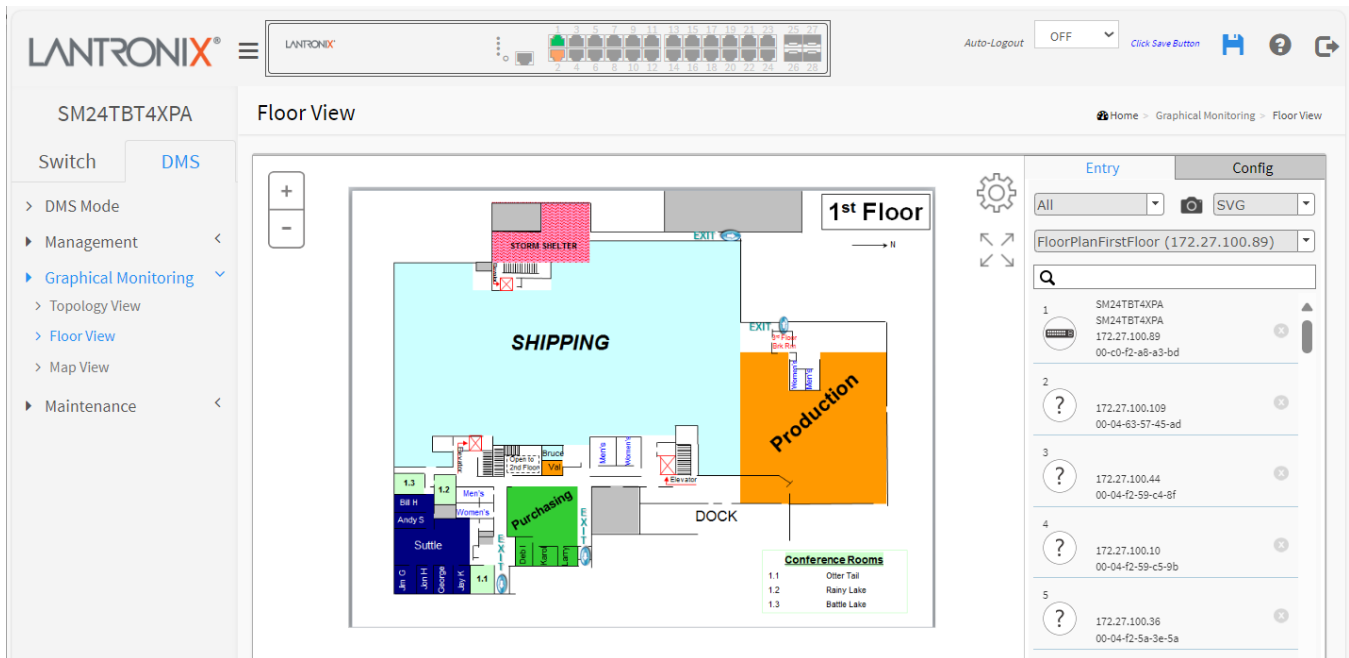
Message: *Error : Firmware download fail* displays if the TFTP Server IP address or the FW image name entered is incorrect.

22-3.3 Floor View

Navigate to the DMS > Graphical Monitoring > Floor View menu path. After you have added a Floor Image at DMS > Maintenance > Floor Image, the Floor View lets you:

- Drag and drop (anchor) devices onto Floor Maps
- Find device location instantly
- Store up to 10 Maps per Switch
- IP Surveillance/VoIP/WiFi applications
- Other features same as Topology View


Click the  button to display the right pane menu tabs (Entry and Config).




DMS Floor View parameters

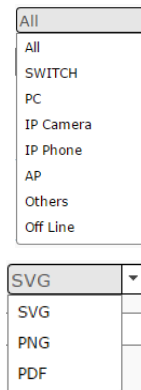
Device tab parameters

Devices dropdown: Select the device type (All, SWITCH, PC, IP Camera, IP Phone, AP, Others, or Off Line).

Snapshot icon: Use the  icon to capture the displayed topology view.

File format: Select the graphics file type (.SVG, .PNG, or .PDF).

Search box: Use the  to search for a device by typing IP/MAC address or Model/Device name.



Config tab parameters

Total Device: Displays the total number of devices discovered.

Controller IP: The control device IP address in the format 0.0.0.0.

DHCP Server IP: The IP address of the DHCP server if DHCP Server is set to Enabled.

DHCP Server: Select Enabled or Disabled.

IP Range: The range type (Single Subnet or Multiple Subnet).

Apply: Click the button to save the selections.

| Device | Config |
|--|---------------|
| Total Device | 2 |
| Controller IP | 192.168.1.77 |
| DHCP Server IP | --- |
| DHCP Server | Disabled |
| IP Range | Single Subnet |
| <input type="button" value="✓ Apply"/> | |

Example: Drag and drop the devices to the desired locations:

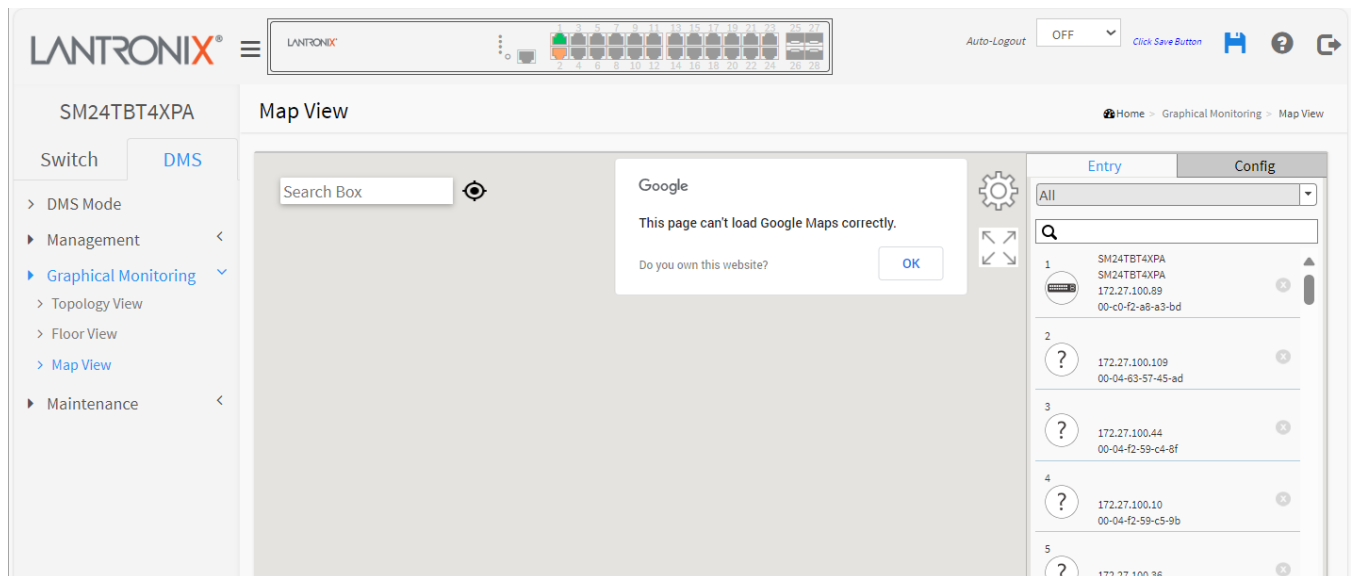
The screenshot shows the Lantronix web interface for the SM24TBT4XPA device. The top navigation bar includes 'Home', 'Graphical Monitoring', and 'Floor View'. The left sidebar contains a 'Switch' tab and a 'DMS' tab, with a list of navigation options: DMS Mode, Management, Graphical Monitoring (selected), Topology View, Floor View, Map View, and Maintenance. The main area displays the 'Floor View' of the '1st Floor'. The floor plan includes a 'SHIPPING' area, a 'Production' area, a 'Purchasing' area, a 'Dock', and 'Conference Rooms'. A 'Storm Shelter' is also indicated. A list of discovered devices is shown on the right, including their IP addresses and MAC addresses. The interface also features a top navigation bar with 'Home', 'Graphical Monitoring', and 'Floor View' links.

22-3.4 Map View

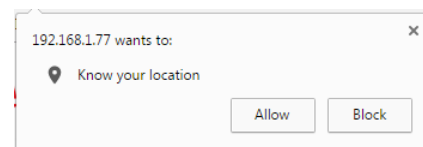
Navigate to the DMS > Graphical Monitoring > Map View menu path. The Map View lets you:

- Anchor devices onto Google Maps
- Find devices instantly from Google Maps
- Search on-Line by Company/Address
- Run outdoor IP Cam/WiFi applications
- Other features same as Topology View

Click the  button to display the right pane menu tabs (Device and Config).




If the message “192.168.1.77 wants to know your location” displays, click the **Allow** button.



DMS Map View parameters

Device tab:

Devices dropdown: Select the device type (All, SWITCH, PC, IP Camera, IP Phone, AP, Others, or Off Line).

Search box: Use the  to search for a device by typing IP/MAC address or Model/Device name.

Config tab parameters:

Total Device: Displays the total number of devices discovered.

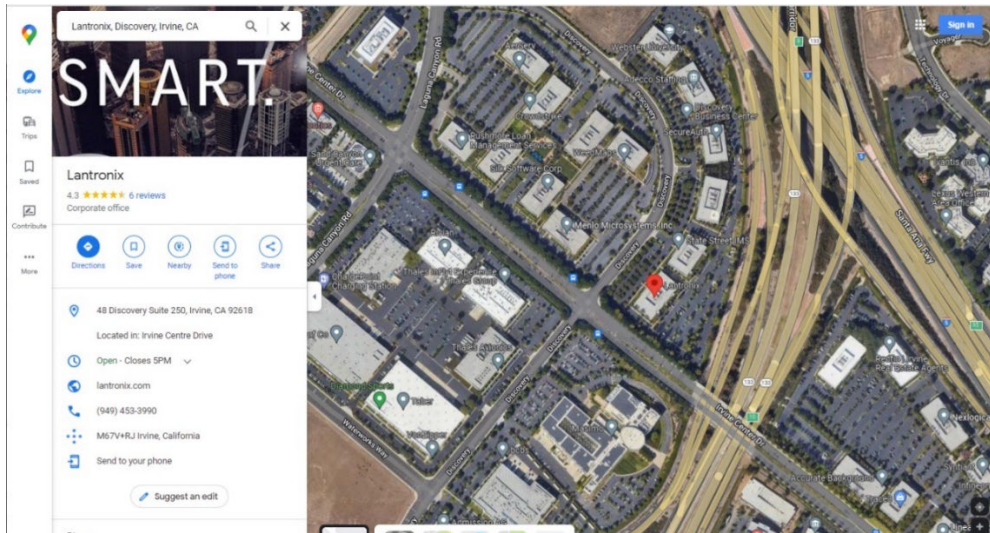
Controller IP: The control device IP address in the format 0.0.0.0.

IP Range: The range type (Single Subnet or Multiple Subnet).

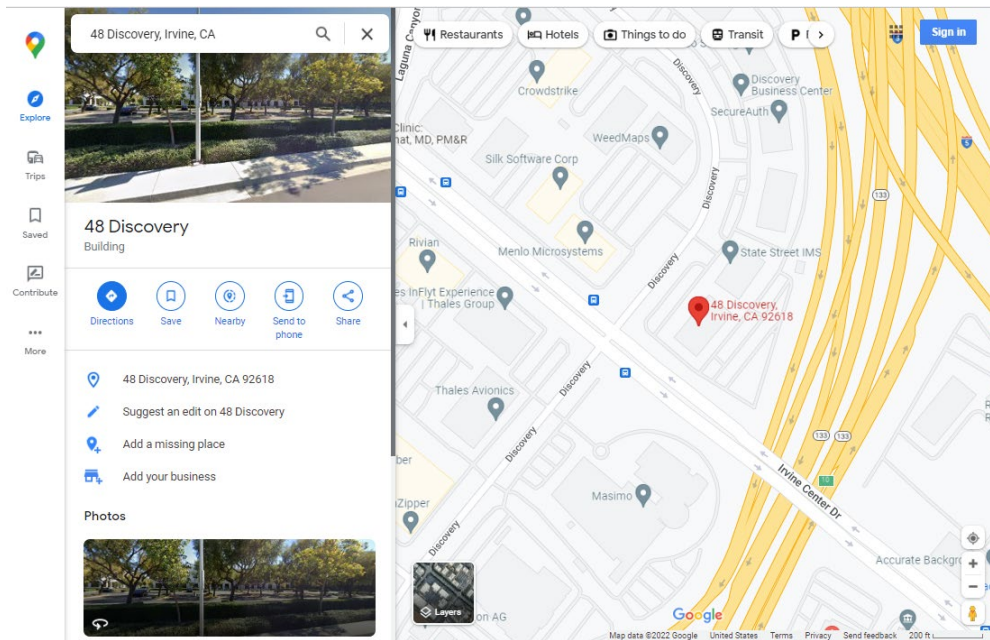
Apply: Click the button to save the selections.

| Entry | Config |
|--|---------------|
| Total Device | 2 |
| Controller IP | 0.0.0.0 |
| IP Range | Single Subnet |
| <input type="button" value="✓ Apply"/> | |

Satellite View: From DMS > Graphical Monitoring > Map View you can click **Satellite** to replace the Map View with a satellite view:



Click the linked text [View on Google Maps](#) and enter an address:



Message: This page can't load Google Maps correctly.

Meaning: Click OK to clear the message.

Message: Do you own this website?

Meaning: Click to go to the Google developers maps [documentation page](#).

22-4 Management

Navigate to the DMS > Management menu path to view the Device List and Map API Key webpages.

22-4.1 Device List

Navigate to DMS > Management > Device List to show all devices and information detected by DMS.

The screenshot shows the Lantronix SM24TBT4XPA web interface. The top navigation bar includes the Lantronix logo, a menu icon, and a status bar with 'Auto-Logout OFF' and a 'Click Save Button' link. The left sidebar shows the navigation menu with 'DMS Mode' expanded, and 'Management' selected. The main content area is titled 'Devices List' and shows a table of detected devices. The table has columns for 'Remove', 'Status', 'Device Type', 'Model Name', 'Device Name', 'MAC', and 'IP Address'. The table displays 10 entries, all with 'Online' status. A search bar and pagination controls are also visible.

| Remove | Status | Device Type | Model Name | Device Name | MAC | IP Address |
|--------------------------|--------|-------------|------------|-----------------|-------------------|---------------|
| <input type="checkbox"/> | Online | Others | | | D8-EC-5E-BC-9A-78 | 10.10.10.100 |
| <input type="checkbox"/> | Online | Others | | | 18-7A-3B-38-8E-8A | 172.27.100.1 |
| <input type="checkbox"/> | Online | Others | | | 00-C0-F2-7B-69-34 | 172.27.100.2 |
| <input type="checkbox"/> | Online | PC | General PC | PLYWK-W10-00048 | D8-CB-8A-8F-CB-55 | 172.27.100.4 |
| <input type="checkbox"/> | Online | PC | General PC | PLYWK-W10-00064 | 50-9A-4C-19-AD-0A | 172.27.100.5 |
| <input type="checkbox"/> | Online | PC | General PC | PLYWK-W7-00002 | 6C-3B-E5-23-0F-FE | 172.27.100.8 |
| <input type="checkbox"/> | Online | Others | | | C4-63-FB-00-23-95 | 172.27.100.9 |
| <input type="checkbox"/> | Online | Others | | | 00-04-F2-59-C5-9B | 172.27.100.10 |
| <input type="checkbox"/> | Online | PC | General PC | PLYWK-W10-00051 | 5C-60-BA-60-EA-22 | 172.27.100.11 |
| <input type="checkbox"/> | Online | Others | | | 00-C0-F2-96-12-11 | 172.27.100.12 |

Showing 1 to 10 of 102 entries

Previous 1 2 3 4 5 ... 11 Next

Apply

DMS > Management > Device List parameters

Show x entries: At the dropdown select the number of devices to list per page (10, 25, 60, or All). The default is 10 entries per page.

Remove: Check the box to delete the table entry at the next Apply. Only Offline devices can be removed from the DMS Device List.

Status: e.g., Online or Offline.

Device Type: The kind of device detected by DMS (e.g., SWITCH, IP Cameras, or Others).

Model Name: The model number of the device detected by DMS (e.g., SM24TBT4XPA or General PC).

Device Name: The name of the device detected by DMS (e.g., SM24TBT4XPA).

MAC: The MAC address of the device that DMS detected (e.g., 00-40-C7-1C-CB-6E).

IP Address: The IP address of the device that DMS detected (e.g., 192.168.1.77).

Http Port: Click the Edit icon to edit the Http Port number.

User Name: Click the Edit icon to edit the User Name.

Password: Click the Edit icon to edit the Password.

Edit: Click the button to display the table in editable form. Click the **Edit** icon to edit the Device Name, Http Port, User Name, and Password. This function can also be configured in the Dashboard of Topology view. There is no HTTP connection function for Unknown Device and PC type devices, so the UI doesn't provide "Edit HTTP port" function for configuring it. See below.

Show xx entries: At the dropdown select how many entries to show per page (10, 25, 60, or All).

Search: Enter key word(s) to search for on the page.

Remove: Only Offline devices provide "Remove" function to remove from DMS device list.

Previous: Click to display the previous set of entries (if any exist).

Next: Click to display the next set of entries (if any exist).

Apply: Click to save changes.

You can click the **Edit** button to show additional fields for editing:

The screenshot shows the 'Devices List' page in the Lantronix web interface. The top navigation bar includes the Lantronix logo, a status bar with 'Auto-Logout OFF', and a 'Click Save Button' link. The left sidebar shows the 'DMS Mode' selected, with 'Management' expanded to show 'Device List'. The main content area has a 'Devices List' title and a search bar. Below the search bar is a table with columns: Remove, Status, Device Type, Model Name, Device Name, Edit Device Name, MAC, IP Address, Edit HTTP Port, Edit User Name, and Edit User Password. The table lists several devices, including 'Others' and 'General PC' types, all with 'Online' status. A 'Show 10 entries' dropdown is located above the table.

| 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 | Others | | | | D8-EC-5E-BC-9A-78 | 10.10.10.100 | | | |
| <input type="checkbox"/> | Online | Others | | | | 18-7A-3B-38-8E-8A | 172.27.100.1 | | | |
| <input type="checkbox"/> | Online | Others | | | | 00-C0-F2-7B-69-34 | 172.27.100.2 | | | |
| <input type="checkbox"/> | Online | PC | General PC | PLYWK-W10-00048 | PLYWK-W10-00048 | D8-CB-8A-8F-CB-55 | 172.27.100.4 | | | |
| <input type="checkbox"/> | Online | PC | General PC | PLYWK-W10-00064 | PLYWK-W10-00064 | 50-9A-4C-19-AD-0A | 172.27.100.5 | | | |
| <input type="checkbox"/> | Online | PC | General PC | PLYWK-W7-00002 | PLYWK-W7-00002 | 6C-3B-E5-23-0F-FE | 172.27.100.8 | | | |
| <input type="checkbox"/> | Online | Others | | | | C4-63-FB-00-23-95 | 172.27.100.9 | | | |

Additional Parameter descriptions:

Edit Device Name: Enter the a name for this device.

Edit HTTP Port: Edit the HTTP port number for this device.

Edit User Name: Edit the Username for this device.

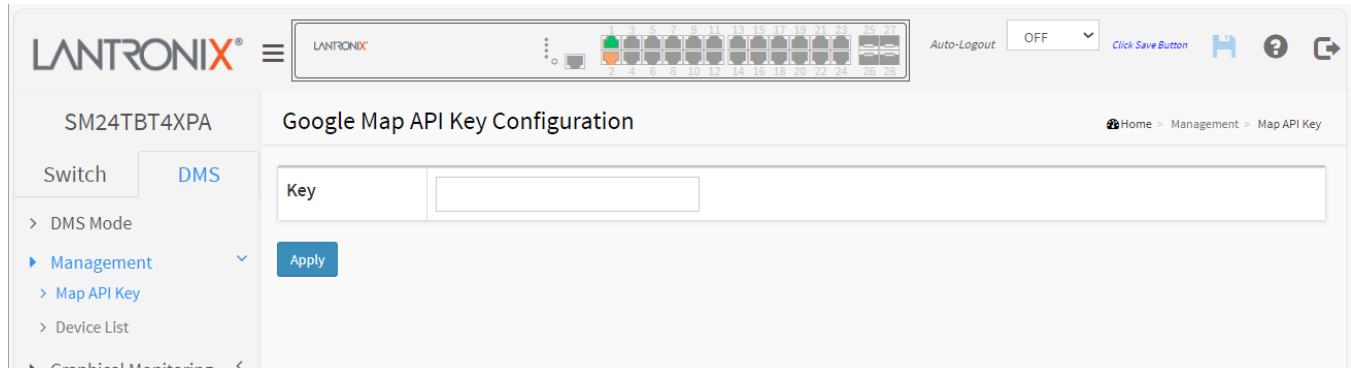
Edit User Password: Edit the Password for this device.

22-4.2 MAP API Key

Navigate to DMS > Management > Map API Key menu path to display the Google Map API Key Configuration page. You need a valid API key and a Google Cloud Platform billing account to access Google core products. If not, DMS Map View will not be able to load Google Map correctly.

To configure the DMS Management API Key via the web UI:

1. Click DMS, Management, Map API Key.
2. Visit the Google website below and follow the directions to get an API key:
<https://developers.google.com/maps/documentation/directions/get-api-key>
3. Enter your Google Map API Key.
4. Click Apply to save the settings.



The screenshot shows the Lantronix web interface for the SM24TBT4XPA device. The top navigation bar includes the Lantronix logo, a menu icon, a status bar with 28 LEDs, an 'Auto-Logout' dropdown set to 'OFF', and links for 'Click Save Button', a home icon, a help icon, and a share icon. The left sidebar shows the navigation menu with 'Switch' and 'DMS' tabs. Under 'DMS', there are links for 'DMS Mode', 'Management' (selected), 'Map API Key' (selected), 'Device List', and 'Graphical Monitoring'. The main content area is titled 'Google Map API Key Configuration' and contains a 'Key' label, a text input field, and an 'Apply' button. A breadcrumb trail at the top right reads 'Home > Management > Map API Key'.

Parameter descriptions

Key: Enter the Google API Key. To use the Google Maps Embed API, you must register your app project on the Google API Console and get a Google API key which you can add to your app or website.

Buttons

Apply: Click to save changes.

22-5 Maintenance > Floor Image

Navigate to DMS > Maintenance > Floor Image to display the Floor Image Maintenance page. This page lets you add or delete a floor image.

Each DMS switch provides 10 files space for uploading. Only JPG and PNG formats are supported. File size is limited to 256KB.

All DMS switches' floor image in the same network can be shared together. For example, if Switch 1 has uploaded 10 floor images, and Switch 2 has uploaded 5 images, then the total of 15 floor images can be shared and selected on all DMS switches in the same network.

File name will attach IP address to let you know on which DMS switch the floor image is stored.

Parameter descriptions:

Maximum: x files: By default this field displays "Maximum: 10 files". With each switch added and discovered, the maximum value increases by 10. For example, if only two switches are connected to each other, the maximum number of files will increase from 10 to 20 (on both switches). But once the connection is removed and after an approximate 1 minute wait, the maximum number of files will restore to 10.

The maximum number of images displayed is additive. When the switch is stand alone with no connections to other DMS switches, the number displayed is 10. As other DMS switches are added, the field is incremented by 10 for each one.

Used: x file(s): The number of files that have already been uploaded.

Free: x file(s): The number of files that can be uploaded before reaching the maximum number of images.

Add Floor Image: Click **Choose File** and browse to and select a File Name to add.

Add: Click to add the selected file.

Select: Displays the selected image name.

No.: Displays the instance number.

File Name: Displays the selected file name.

Image: Displays the selected image. Image added (*FloorPlanFirstFloor*):

The screenshot displays the Lantronix web interface for the SM24TBT4XPA device. The top navigation bar includes the Lantronix logo, a status bar with various indicators, and links for Auto-Logout, Click Save Button, and help icons. The left sidebar shows the 'SM24TBT4XPA' configuration menu with options like Switch, DMS, and Maintenance. The main area is titled 'Floor Image Management' and shows file usage statistics: Maximum: 20 files, Used: 1 file(s), Free: 19 file(s). Below this is a form to 'Add Floor Image' with a 'Choose File' button and a text field for the name. A table lists the current floor images, with one entry: 'FloorPlanFirstFloor (172.27.100.89)' which is associated with a floor plan image. A 'Delete' button is located at the bottom of the table.

Message: 192.168.1.77 says: Insufficient Space. Only x files available.

Meaning: The file is too large or no file exists.

Recovery: Click the **OK** button to clear the message and choose a new File Name to add.

Message: Special Characters are not allowed in Name.

Meaning: The Floor Image filename has special characters (dash, space, numbers, etc.) which are not allowed.

Recovery: Click the **OK** button to clear the message and choose a File Name with no special characters.

22-6 Maintenance > Diagnostics

DMS supports network diagnostic between devices.

The screenshot shows the Lantronix web interface for the SM24TBT4XPA device. The 'Diagnostics' page is active, displaying a table of network connectivity devices. The table has columns for 'Select', 'Status', 'Model Name', 'Device Name', 'MAC', 'IP Address', and 'Version'. All devices listed are 'Online'. The interface includes a sidebar with navigation options and a top navigation bar showing the current path: Home > Maintenance > Diagnostics.

| Select | Status | Model Name | Device Name | MAC | IP Address | Version |
|--------------------------|--------|------------|-------------|-------------------|----------------|---------|
| <input type="checkbox"/> | Online | | | 00-04-63-57-45-AD | 172.27.100.109 | |
| <input type="checkbox"/> | Online | | | 00-04-F2-59-C4-8F | 172.27.100.44 | |
| <input type="checkbox"/> | Online | | | 00-04-F2-59-C5-9B | 172.27.100.10 | |
| <input type="checkbox"/> | Online | | | 00-04-F2-5A-3E-5A | 172.27.100.36 | |
| <input type="checkbox"/> | Online | | | 00-04-F2-5A-3E-8A | 172.27.100.54 | |
| <input type="checkbox"/> | Online | | | 00-04-F2-5A-3E-96 | 172.27.100.42 | |
| <input type="checkbox"/> | Online | | | 00-04-F2-5A-41-6F | 172.27.100.38 | |
| <input type="checkbox"/> | Online | | | 00-04-F2-5A-43-47 | 172.27.100.63 | |
| <input type="checkbox"/> | Online | | | 00-04-F2-8E-C2-39 | 172.27.100.52 | |
| <input type="checkbox"/> | Online | | | 00-0C-29-81-7B-90 | 192.168.15.203 | |

Showing 1 to 10 of 101 entries

Previous 1 2 3 4 5 ... 11 Next

Parameter descriptions:

Select: Select off-line device from the list.

Status: Device Online or Offline.

Model Name: The model name of the network connectivity devices.


Device Name: The device name of the network connectivity devices.

MAC: The mac address of the device.

IP Address: The IP address of the network connectivity devices.

Version: The Version of the network connectivity devices.

Buttons

: Refreshes the displayed table starting from the input fields.

Show entries: At the dropdown select the number of entries to be displayed per page (10, 25, 60, or All).

Search: Search for any key word you want.

Previous: Click to show the previous set of entries.

Next: Click to show the next set of entries.

Select a device in the Device column to run the diagnostic:

LANTRONIX® SM24TBT4XPA

Switch DMS

> DMS Mode
> Management
> Graphical Monitoring
▶ Maintenance
 > Floor Image
 > Diagnostics
 > Traffic Monitor

Diagnosics

Another Try

Show 10 entries Search:

| Select | Status | Model Name | Device Name | MAC | IP Address | Version |
|-------------------------------------|--------|------------|-------------|-------------------|----------------|---------|
| <input checked="" type="checkbox"/> | Online | | | 00-04-63-57-45-AD | 172.27.100.109 | |

Showing 1 to 10 of 101 entries

Previous 1 2 3 4 5 ... 11 Next

172.27.100.89 00-c0-f2-a8-a3-bd

Connection.....
Cable status.....

? 172.27.100.109 00-04-63-57-45-ad

When the diagnostic is complete the Connection and Cable status display:

LANTRONIX® SM24TBT4XPA

Switch DMS

> DMS Mode
> Management
> Graphical Monitoring
▶ Maintenance
 > Floor Image
 > Diagnostics
 > Traffic Monitor

Diagnosics

Another Try

Show 10 entries Search:

| Select | Status | Model Name | Device Name | MAC | IP Address | Version |
|-------------------------------------|--------|------------|-------------|-------------------|----------------|---------|
| <input checked="" type="checkbox"/> | Online | | | 00-04-63-57-45-AD | 172.27.100.109 | |

Showing 1 to 10 of 101 entries

Previous 1 2 3 4 5 ... 11 Next

172.27.100.89 00-c0-f2-a8-a3-bd

Connection.....
Cable status.....

? 172.27.100.109 00-04-63-57-45-ad

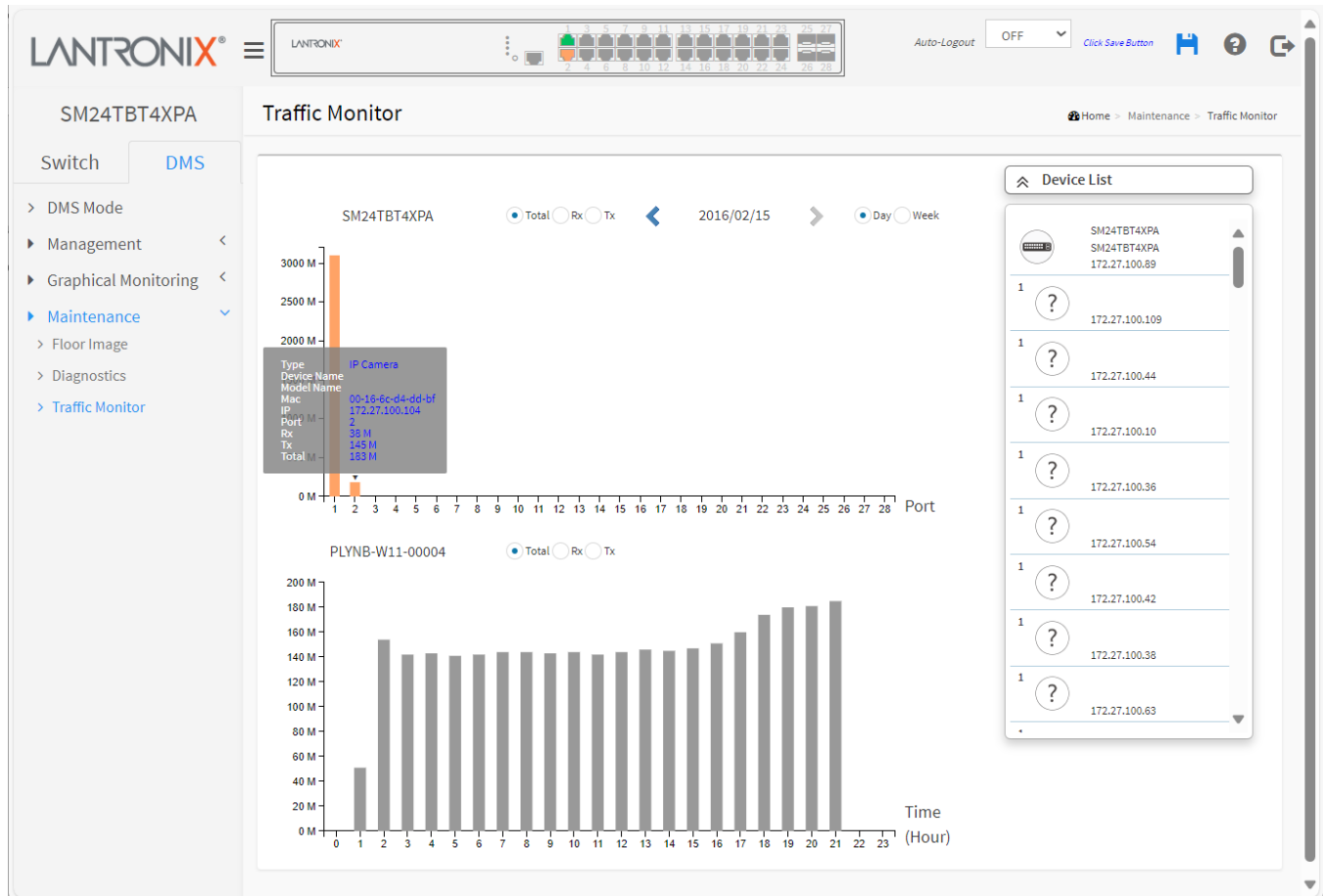
Click the **Another Try** button to return to the initial Diagnostics page.

22-7 Maintenance > Traffic Monitor

DMS supports traffic monitoring of each port and keeps a one-week record that can be used to compare and analyze with visual charts. The page displays two different graphs for a selected device.

Procedure

1. Click DMS > Maintenance > Traffic Monitor.
2. Select the parameters to display.
3. Select the device to monitor.



Parameter descriptions:

☒ Total ☐ Rx ☐ Tx

Total / Rx / Tx: Select the set of data to be displayed.

☒ Day ☐ Week

< yy/mm/dd >: Select the date of data displayed.

Day / Week: Select a day's worth of data or a week's worth of data to be displayed.

Device List: Displays the set of discovered devices.

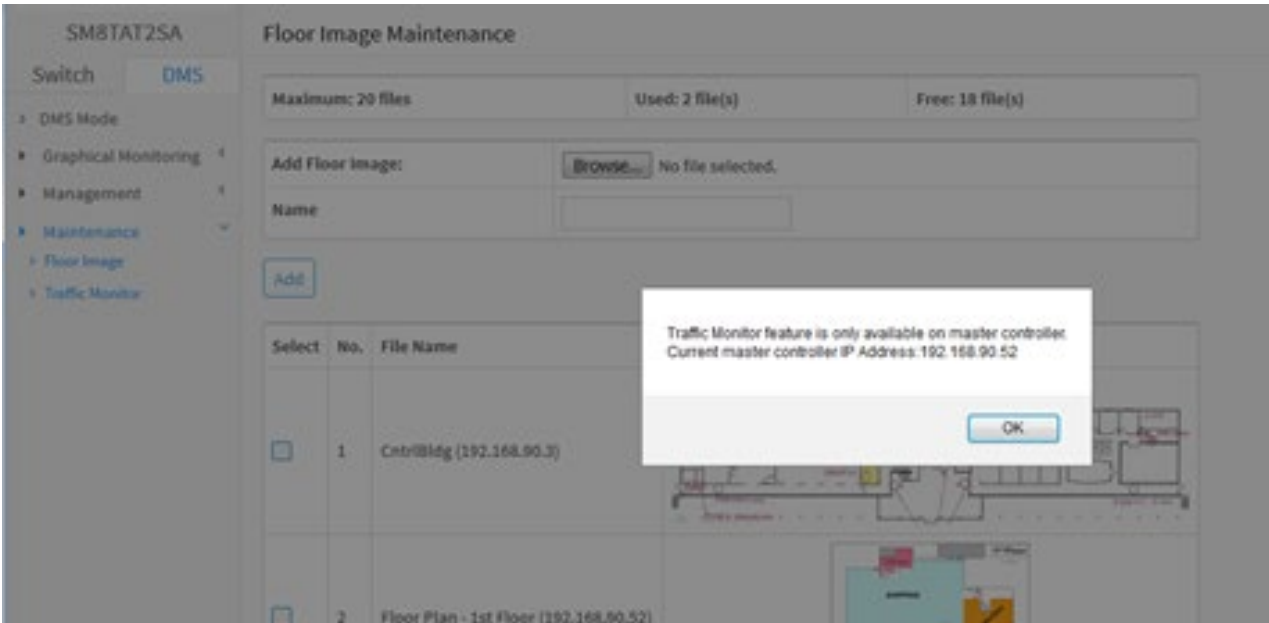
Throughput: Vertical axis shows throughput (e.g., 0 M – 18000 M or 0 M-1200 M). The unit of measure is Mbps.

Port: Horizontal axis shows the switch port numbers.

Time (Hour): Horizontal axis shows the time elapsed in hours (0-23).

The graph's vertical axis shows throughput and the unit of measure is Mbps.

Message: Traffic Monitor feature is only available on master controller. Current master controller IP Address: 192.168.90.52.



22-8 DMS Troubleshooting

Problem: The switch lists itself is the only device in Topology View of DMS.

Problem: In DMS, the Local image shows the IP address of another switch.

Description: The switch is listed as only device in DMS Topology View in DMS; all devices are listed in DMS device list. This is usually because the switch's gateway is not configured appropriately.

Resolution: An IP Route must be configured manually. For example, a switch IP address of 192.168.1.77 should have the following IP route configured: ip route 0.0.0.0 0.0.0.0 192.168.1.x. Without the IP route configured, you may be unable to view all devices on the network in DMS.

1. Go to DMS > Management > DMS Mode to check if the controller IP is correct.
2. Verify that the gateway of this switch is correctly configured.
3. Verify that all connected devices are displayed in DMS Topology View.

Problem: DMS Connectivity diagnostics fails to ICMP reachable device.

Description: DMS displays a device which is reachable via ICMP ping as failing the connection status in diagnostics. Cable status displays as *OK*.

Resolution: Contact Technical Support.

Problem: DMS will discover the device type, name and model of some cameras and hosts but others are displayed as *Unknown*.

Description: When a device is detected by DMS, the device's information (such as type, model name...etc.) can be recognized via LLDP (e.g. Switch), UPnP (e.g. AP), [ONVIF](#) (e.g. IP cam), NBNS (e.g. PC) packets if the device supports these protocols. So if the device display as *Unknown*, that means this device do not issue above mentioned protocol for DMS to recognize.

Resolution: You can manually assign and configure the device type and name for the unknown devices. See the Topology View > Dashboard or the Topology View section.

Message: This page can't load Google Maps correctly.

Recovery:

1. Click the **OK** button to clear the message.
2. Navigate to DMS > Management > Map API Key.
3. See "16-4.2 MAP API Key" on page 268.
4. Click the linked text "Do you own this website?" to display the Google [API Key and Billing Errors Troubleshooting](#) page.
5. For help on finding error messages, see the section on [checking errors in your browser](#).
6. See the Google [Maps Platform FAQ](#) for more information.

Problem: The switch cannot discover / display devices in DMS mode.

Solution: **1.** Make sure DMS Mode = Enabled and DMS Priority = High. **2.** Refresh the web browser page. **3.** Update web browser cache. **4.** Open a new web browser window.

Issue: IE Tab fix for Chrome-Firefox - DMS Topology view issue.

Description: In order to log into a camera on a switch with PoE+ or PoE++ from the DMS Topology View window from a browser other than Internet Explorer, you must have an “IE Tab” extension installed. This is needed for both Chrome and Firefox. IE Tab is an extension for the Google Chrome and Mozilla Firefox web browsers that lets you view pages using the Internet Explorer layout engine.

Recovery:

Google Chrome: <https://chrome.google.com/webstore/detail/ie-tab/hehijbfgiekmjfkfjpbkbammjbdenadd?hl=en-US>

Firefox: <https://addons.mozilla.org/en-US/firefox/addon/open-in-internet-explorer/>

**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.