LANTRONIX®

SM8TAT2SA, SM16TAT2SA, SM24TAT2SA, *and* SM8TAT2SA-DC

8-/16-/24-Port Gigabit PoE+, 2-Port 100/1000 SFP Smart Managed Gigabit Ethernet PoE+ Switches

Web User Guide

Part Number 33717
Revision N September 2023

Intellectual Property

© 2022, 2023 Lantronix, Inc. All rights reserved. No part of the contents of this publication may be transmitted or reproduced in any form or by any means without the written permission of Lantronix.
Lantronix is a registered trademark of Lantronix, Inc. in the United States and other countries. All other trademarks and trade names are the property of their respective holders.

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

Warranty

For details on the Lantronix warranty policy, 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

Rev	Date	Description
K	2/23/22	Initial Lantronix rebrand at HW v1.03, Mech v1.01, FW v1.04.0041, PoE FW v200-188, and PoE MCU FW v22419. FW v1.04.0041:Fixed issue when creating Allowed VLANs on ports in Hybrid mode. Added support for alternative PHY and PoE MCU upgrade. Updated Syslog format to prevent editing of system name. Added support to show Always-On PoE status in CLI.
L	2/1/23	SM8TAT2SA FW v1.04.0079: Add ConsoleFlow and LPM support. Support DHCP per port for a particular VLAN. Change factory defaults and add SNMP mode Enabled/ Disabled selection. Change Auth Method defaults. Change Filename extension to .imgs. Remove Glossary.
M	8/24/23	FW v1.04.0095: Add DHCP option 66 support. Add ConsoleFlow On-premise support. Update DHCP per port VLAN. Update contact information. Please see the Release Notes for more information.
N	9/29/23	FW v1.04.0110: Change ConsoleFlow to Percepxion. Allow a dash character (-) for Status Update Interval and Content Check Interval. Update cert (mach10_combined.crt) file. Automatically save Configuration Update from Percepxion Explore tab and configuration of all element changes to Start-Up Config. Update Percepxion Help page.

Contents

Introduction **6**

Chapter 1 Web-based Management **8**

Chapter 2 First Time Wizard **9**

Chapter 3 System **14**

3-1 System Information 14
3-2 IP Address 16
3-2.1 IP Settings 16
3-2.1 Advanced IP Settings 18
3-2.2 IP Status 22
3-3 System Time 24
3-4 LLDP 28
3-5.1 LLDP Configuration 28
3-4.2 LLDP-MED Configuration 32
3-4.3 LLDP Neighbor 37
3-4.4 LLDP PoE 39
3-4.4 LLDP-MED Neighbor 40
3-4.5 LLDP Statistics 44
3-5 UPnP 46

Chapter 4 Port Management **47**

4-1 Port Configuration 47
4-2 Port Statistics 49
4-3 SFP Port Info 52
4-4 Energy Efficient Ethernet 54
4-5 Link Aggregation 55
4-5.1 Port 55
4-5.2 Aggregation Status 57
4-5.3 Aggregator View 58
4-5.4 Aggregation Hash Mode 60
4-5.5 LACP System Priority 61
4-6 Loop Protection 62
4-6.1 Configuration 62
4-6.2 Status 64

Chapter 5 PoE Management **65**

5-1 PoE Configuration 65
5-2 PoE Status 68
5-3 PoE Power Delay 71
5-4 PoE Auto Power Reset 72
5-5 PoE Scheduling Profile 74

Chapter 6 VLAN Management **75**

6-1 VLAN Configuration 75
6-2 VLAN Membership 78
6-3 VLAN Port Status 80
6-4 VLAN Selective QinQ 82
6-5 MAC-based VLAN 83
6-6 Protocol-based VLAN 85
6-7 IP Subnet-based VLAN 87
6-8 Private VLAN 88
6-9 Port Isolation 89
6-10 Voice VLAN 90

Chapter 7 Quality of Service **93**

7-1 Global Settings 93
7-2 Port Settings 94
7-3 Port Policing 96
7-4 Port Shaper 97
7-5 Storm Control 99
7-6 Port Scheduler 100
7-7 CoS/802.1p Mapping 101
7-8 CoS/802.1p Remarking 102
7-9 IP Precedence Mapping 103
7-10 IP Precedence Remarking 104
7-11 DSCP Mapping 105
7-12 DSCP Remarking 106

Chapter 8 Spanning Tree 107

8-1 State 108
8-2 Region Config 109
8-3 Instance View 110

Chapter 9 MAC Address Tables 118

9-1 Configuration 118
9-2 Information 120

Chapter 10 Multicast 121

10-1 IGMP Snooping 121
10-1.1 Basic Configuration 121
10-1.3 Status 126
10-1.5 IGMP SFM Information 129
10-2 MLD Snooping 131
10-2.1 Basic Configuration 131
10-2.2 VLAN Configuration 134
10-2.3 Status 136
10-2.4 Groups Information 138
10-2.5 MLD SFM Information 139
10.3 Multicast Filtering Profile 140
10.3-1 Switch > Multicast > Multicast Filtering Profile > Filtering Profile Table 140

Chapter 11 DHCP 149

11-1 Snooping 149
11-1.1 Configuration 149
11-1.2 Snooping Table 151

Chapter 12 Percepxion and LPM 159

12-1 Supported Firmware Versions 159
12-2 Percepxion Agent Configuration 159
12-3 Percepxion Upload 163

Chapter 13 Security 164

13-1 Management 164
13-1.1 Account 164
13-1.2 Privilege Level 166
13-1.3 Auth Method 167
13-1.4 Access Management 169
13-2 IEEE 802.1X 171
13-2.1 Configuration 171
13-2.2 Status 175
13-3 Port Security 177
13-3.1 Configuration 177
13-3.2 Status 179
13-6.2 SNMPv3 189

Security > SNMP > SNMPv3 > Communities 189
Security > SNMP > SNMPv3 >Users 190
Security > SNMP > SNMPv3 > Groups 191
Security > SNMP > SNMPv3 > Views 192
Security > SNMP > SNMPv3 > Access 193
13-7 RADIUS 194
13-7.1 Configuration 194
13-7.2 Status 197
13.8 RMON Configuration 201
13.9 RMON Status 205
12.10 TACACS+ Configuration 211
13.11 Access Control List 213
13.12 Access Control Status 220
13.13 Switch > Event Notification 221
13.13.1 Switch > Event Notification > SNMP Trap 221
13.13.2 Switch > Event Notification > eMail 224
13.13.3 Switch > Event Notification > Syslog 226
13.13.3.1 Syslog Configuration 226
13.13.3.2 View Log 227

Chapter 14 Diagnostics 230

14-1 Ping 230
14-2 Traceroute 232
14-3 Cable Diagnostics 233
14-4 Mirroring 235

Chapter 15 Maintenance 237

15-1 Configuration 237
15-1.1 Save running-config 237
15-1.2 Backup Configuration 239
15-1.3 Restore Configuration 241
15-1.4 Activate Configuration 243
15-1.5 Delete config 244
15-2 Restart Device 245
15-3 Restore Factory Defaults 246
15-4 Firmware 247
15-4.1 Firmware Upgrade 247
15-4.1 Firmware Selection 249

Chapter 16 DMS (Device Management System) 251

16-1 DMS Mode - DMS Controller Switch 252
16-2 DMS Mode 253
16-3 Graphical Monitoring 254
16-4 Management 267
16-4.1 Device List 267
16-4.2 MAP API Key 269
16-4 Maintenance > Floor Image 270
16-5 Maintenance > Traffic Monitor 272
16-6 DMS Troubleshooting 274

Appendix A Troubleshooting 276

General Troubleshooting Procedure 276

Appendix B DHCP Per Port 279

DHCP Per Port Mode Configuration 280
DHCP Server Mode Configuration 281
DHCP Per Port VLAN 282

Introduction

Overview

This manual describes how to configure and monitor the SMxTAT2SA via the web via its RJ-45 serial interface and Ethernet ports.

The SMxTAT2SA Smart Managed GbE PoE+ switch is the next-generation Ethernet switch offering powerful L2 features with better functionality and usability. It delivers cost-effective business and transport Ethernet services via fiber or copper connections.

The SMxTAT2SA delivers 8/16/24 (10M/100M/1G) RJ45 ports with 8 PoE+ ports (supports 802.3 at/af and total up to 130W on the SM8TAT2SA) and 2 GbE SFP ports. SMxTAT2SA provides high hardware performance and environment flexibility for SMBs and Enterprises. The embedded Device Managed System (DMS) feature makes the switch easy to use, configure, install, and troubleshoot in video surveillance, wireless access, and other SMB and Enterprise applications.

SMxTAT2SA features include:

- Compliant with IEEE 802.3at PoE+ and 802.3af PoE
- PoE configuration, Power delay, and Scheduling
- PoE Auto Power Reset
- Device Management System (Graphical Monitoring, Traffic Monitoring, and Troubleshooting)
- L2+ features for better manageability, security, QoS, and performance
- IPv4/IPv6 dual stack management
- SSH/SSL secured management
- SNMP v1/v2c/v3
- Percepxion Client support (Cloud and On-premise)
- RMON groups 1,2,3,9
- IGMP v1/v2/v3 and MLD v1/v2 Snooping
- IP Source Guard
- LACP and static link aggregation
- 802.1d (STP), 802.1w (RSTP) and 802.1s (MSTP)
- DHCP Snooping, DHCP Relay (Option 82), DHCP statistics, DHCP per Port
- Q-in-Q double tag VLAN
- GVRP dynamic VLAN
- LLDP (Link Layer Discovery Protocol)
- IEEE 802.3az Energy Efficiency
- LPM (Lantronix Provisioning Manager) support
- RADIUS and TACACS+ authentication

Ordering Information

This manual documents four similar models as described below. The models differ mainly in port count. Model differences are noted where applicable in this manual.

SKU	Description
SM8TAT2SA	PoE+ layer 2 Smart Managed Switch with Web GUI, SNMP management; PoE scheduling, APR, and DMS feature support. Port support description: (8) 10/100/1000Base-T PoE+ ports with 2 SFP ports; AC version.
SM8TAT2SA-DC	PoE+ layer 2 Smart Managed Switch with Web GUI, SNMP management; PoE scheduling, APR, and DMS feature support. Port support description: (8) 10/100/1000Base-T PoE+ ports with 2 SFP ports; DC version.

SM16TAT2SA	PoE+ layer 2 Smart Managed Switch with Web GUI, SNMP management; PoE scheduling, APR, and DMS feature support. Port support description: (16) 10/100/1000Base-T PoE+ ports with 2 SFP ports
SM24TAT2SA	PoE+ layer 2 Smart Managed Switch with Web GUI, SNMP management; PoE scheduling, APR, and DMS feature support. Port support description: (24) 10/100/1000Base-T PoE+ ports with 2 SFP ports

About This Manual

This manual gives specific information on how to operate and use the SMxTAT2SA management functions with an HTTP/HTTPs web browser. This manual is intended for use by network administrators who are responsible for operating and maintaining network equipment; it assumes a working knowledge of general switch functions, the Internet Protocol (IP), and Hypertext Transfer Protocol (HTTP).

Related Manuals

Other related manuals are listed below.

- SMxTAT2SA Quick Start Guide, 33715
- SMxTAT2SA Install Guide, 33716
- SMxTATS2A CLI Reference, 33718
- SM8TAT2SA-DC Quick Start Guide, 33813
- SM8TAT2SA-DC Install Guide, 33814
- SMxTAT2SA Unified API User Guide, 33825
- SMxTAT2SA Series Quick Start Guide 33866 Rev A (Spanish)
- Release Notes (version specific)

For Lantronix Documentation, Firmware, App Notes, etc. go to https://www.lantronix.com/technical-support/. Visit the Lantronix Web site at www.lantronix.com/support/documentation for the latest documentation. Note that this manual provides links to third party websites for which Lantronix is not responsible. These external third party links are provided as a convenience and are for informational purposes only; they do not constitute an endorsement or an approval by Lantronix of any of the products, services, or opinions of the corporation or organization or individual. Lantronix bears no responsibility for the accuracy, legality, or content of these external sites or for subsequent links. Contact the external site for answers to questions regarding its content.

Cautions and Warnings: See the Install Guide for important Cautions and Warnings.

Chapter 1 Web-based Management

Initial Configuration

This chapter describes how to configure and manage the SMxTAT2SA via the web user interface. With this facility, you can easily access and monitor through any one port of the switch all the status of the switch, including each port activity, Spanning tree status, port aggregation status, multicast traffic, VLAN and priority status, even illegal access. SMxTAT2SA default values are:

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

After the SMxTAT2SA interface has been configured, you can browse it. For instance, type 192.168.1.77 in the address row in a browser; it will show the Login screen and ask you for a username and password in order to login and access authentication.

The default Username is **admin** and default Password is **admin**. For first time use, enter the default username and password, and then click the Login button. The login process now is complete. In the login menu, you must enter the complete username and password respectively. The SMxTAT2SA allows two or more users using administrator's identity to manage this switch; the administrator to do the last setting will be the configuration to affect the system.

Note: When you login to the switch Web page to manage, type the Username **admin** and press the <tab> key. Then type the Password **admin** and press Enter. When you login to the switch Web UI, you can use IPv4 or IPv6 login to manage.
To optimize the display effect, we recommend Microsoft IE 6.0 above, Netscape V7.1 above or Firefox V1.00 above with 1024x768 resolution. See the *SMxTAT2SA Install Guide* for Web browser support.

Note: The SMxTAT2SA has the DHCP function disabled by default, so if you do not have a DHCP server to provide an IP addresses to the switch, enter the default IP address (192.168.1.77).

Figure 1: The Login page

: Show password text as it is typed. Added at FW v1.04.0079.

: Hide password text as it is typed. Added at FW v1.04.0079.

Chapter 2 First Time Wizard

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

Step 1: Change default password

Enter a new password and then enter it again. Starting at FW v1.02.1471: the Password must contain at least 8 characters, at least 1 upper case letter, 1 lower case letter and one numeric character. The new password cannot be blank or the default value. Click the **Next** button.

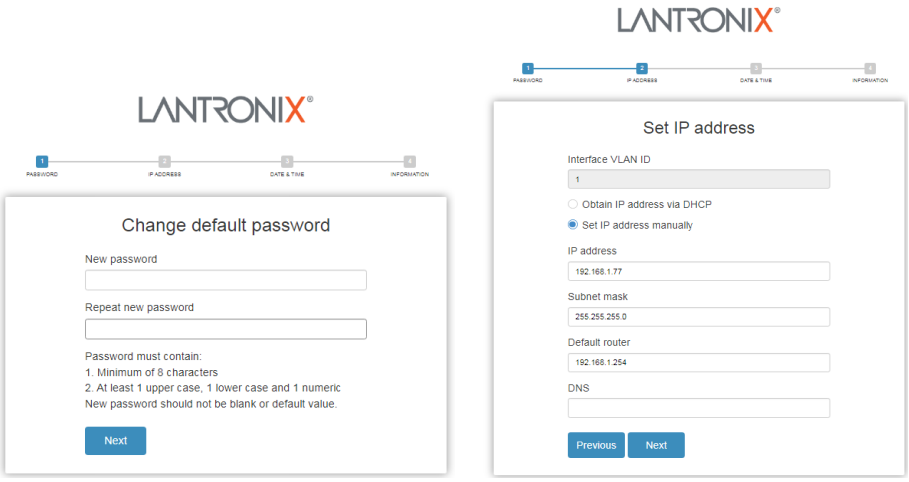


Figure 2-1: Change default password

Step 2: Set IP address

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

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

Click the **Next** button.

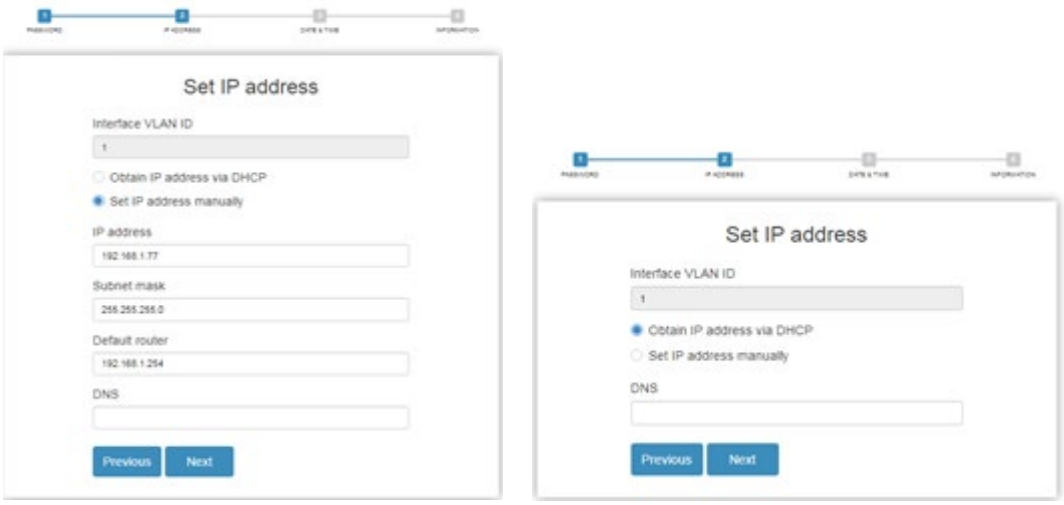


Figure 2-2a: Set IP address

Figure 2-2b: Set IP address

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

Step 3: Set date and time

Enable “Automatic 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.

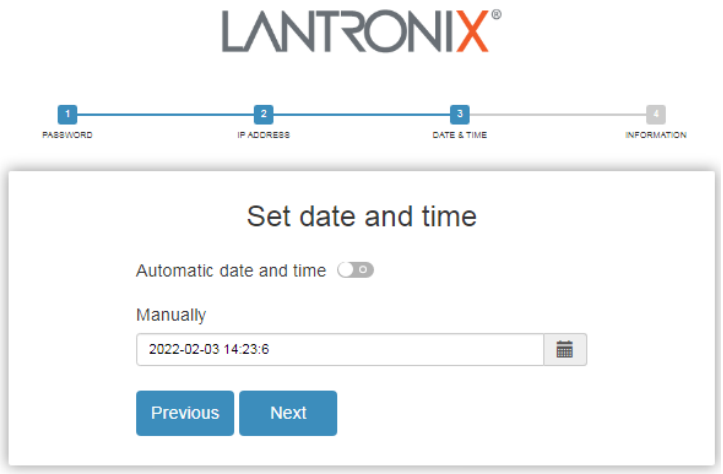


Figure 2-3: Set date and time

Step 4: Set system information

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

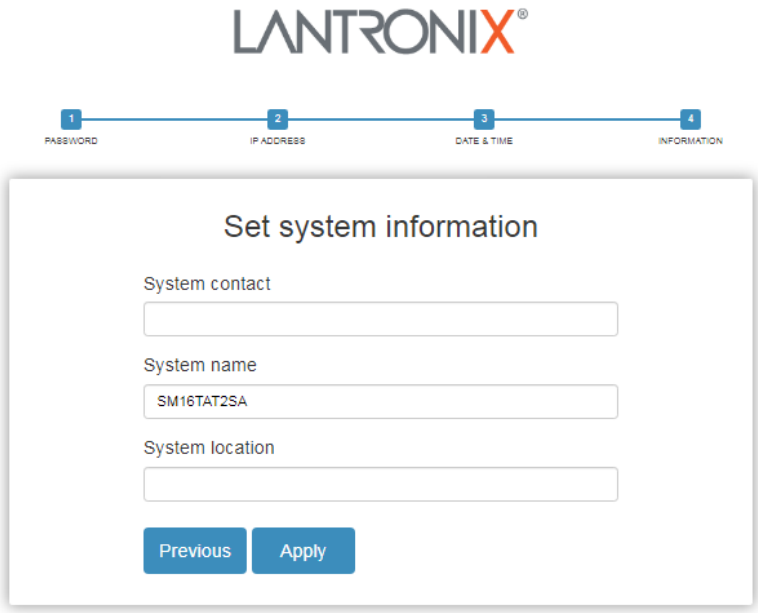


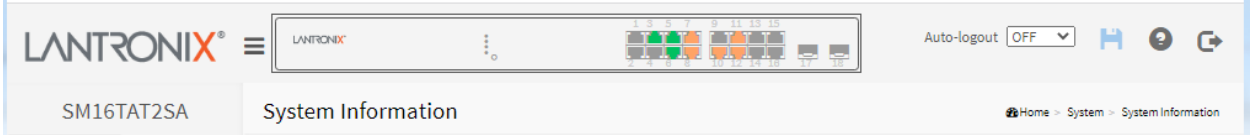
Figure 2-4: Set system information

Message: Password format error.

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

Webpage Controls

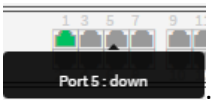
Webpage controls and icons are shown and described below.



Click the Lantronix logo to return to the Switch > System > System Information page from any page.

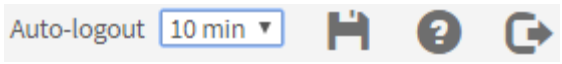
Click the icon to alternately display / hide the left hand menu bar.

Hover the cursor over any port to see its current status:

or 

.

Click on any port to display its current Detailed Port Statistics page.

Top right corner icons: 

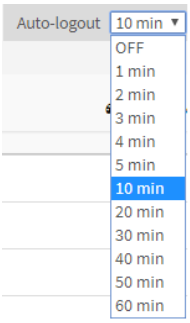
Save Configuration: Click to save parameter changes to the running-config file. Click OK when the message "*Please confirm to save current running-config file as startup-config file?*" displays. Do not reset or power off the switch until the save completes.

Help: Displays the Help page for the current webpage.

Logout: Logs you out and displays the Login prompt.

: Displays the current webpage path.

: **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 v1.02.1463). The default is 10 minutes. When set to OFF, no Auto-logout occurs.



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.

Auto-logout summary:

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

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

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

Webpage Messages

Message: *Wrong username or password!*
Recovery: Re-try the login with the correct username and password credentials.

Message: *There are too many users in the system.*
Recovery: Try to log in later.

Chapter 3 System

This chapter describes the basic configuration tasks including System Information and certain System parameters (e.g., IP Address, System Time, LLDP, UPnP).

3-1 System Information

You can enter a system name, location, and contact information here. Additional switch-related information is also provided here (e.g., Model Name, HW version, FW version, Serial Number, etc.).
To view and set System Information in the web UI:

1. Click System and System Information.
2. View the read-only parameters.
3. Enter System Name, Location, and Contact information (optional).
4. Click the Apply button.

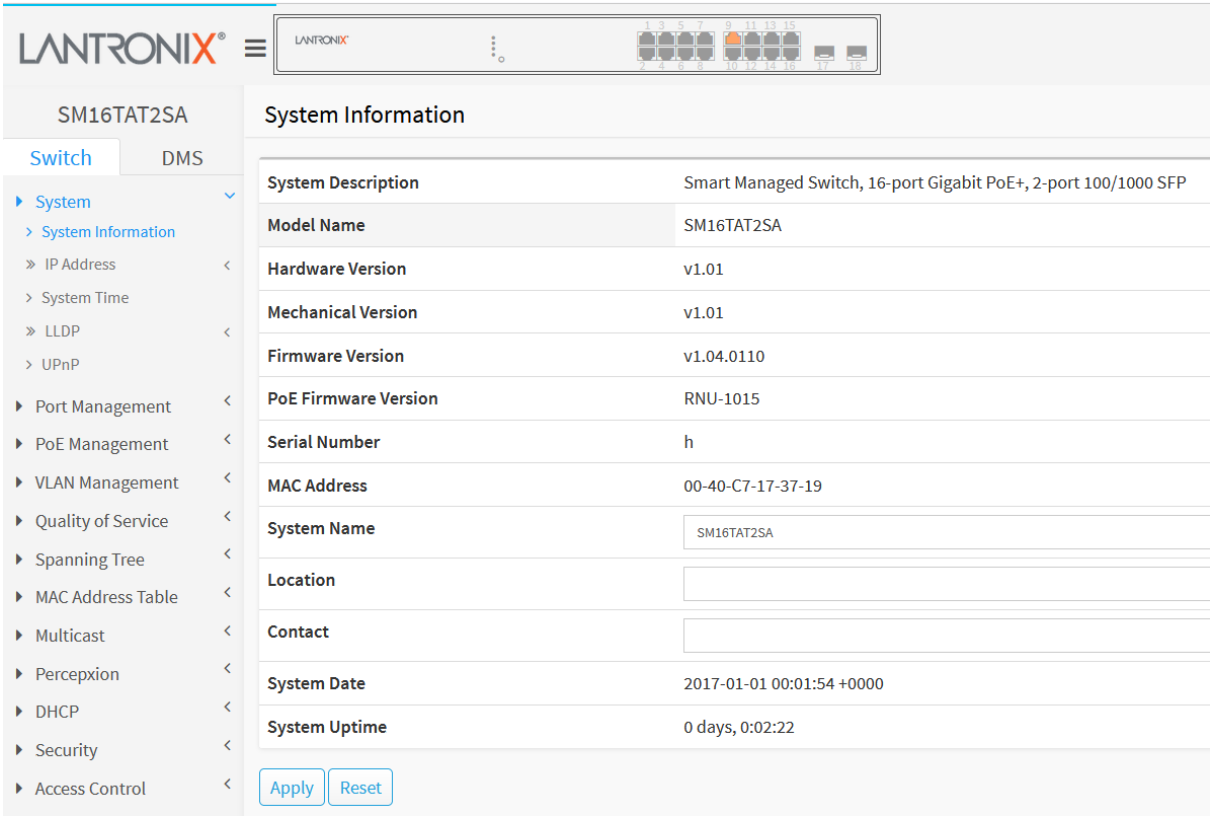


Figure 3-1: System Information (SM8TAT2SA shown)

Parameter descriptions:

System Description: e.g., Smart Managed Switch, 16-port Gigabit PoE+, 2-port 100/1000 SFP.

Model Name: the specific switch model number (i.e., SM8TAT2SA, SM8TAT2SA-DC, SM16TAT2SA, or SM24TAT2SA).

Hardware Version: the current version of hardware (e.g., v1.03).

Mechanical Version: the current mechanical version (e.g., v1.01).

Firmware Version: the current running version of switch firmware (e.g., v1.04.0110).

PoE Firmware Version: the current PoE MCU FW version (e.g., 208-211 or 220-224 or RNU-1015).

MAC Address: the switch MAC Address in the format 11-22-33-44-55-66.

Serial Number: the switch S/N (e.g., C020316AR5100024 or C021321BR4100001).

System Name: An administratively assigned name for this managed node. By convention, this is the node's fully-qualified domain name. A domain name is a text string drawn from the alphabet (A-Z, a-z), digits (0-9), minus sign (-). No space characters are permitted as part of a name. The first or last character must not be a minus sign. The allowed string length is 0-128 characters (e.g., SM8TAT2SA).

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

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

System Date: the current date and time (e.g., 2023-09-25 13:26:58 +0000).

System Uptime: the time the switch has been running since the last power cycle (e.g., 6 days, 23:28:42).

Buttons

Apply: Click to save changes.

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

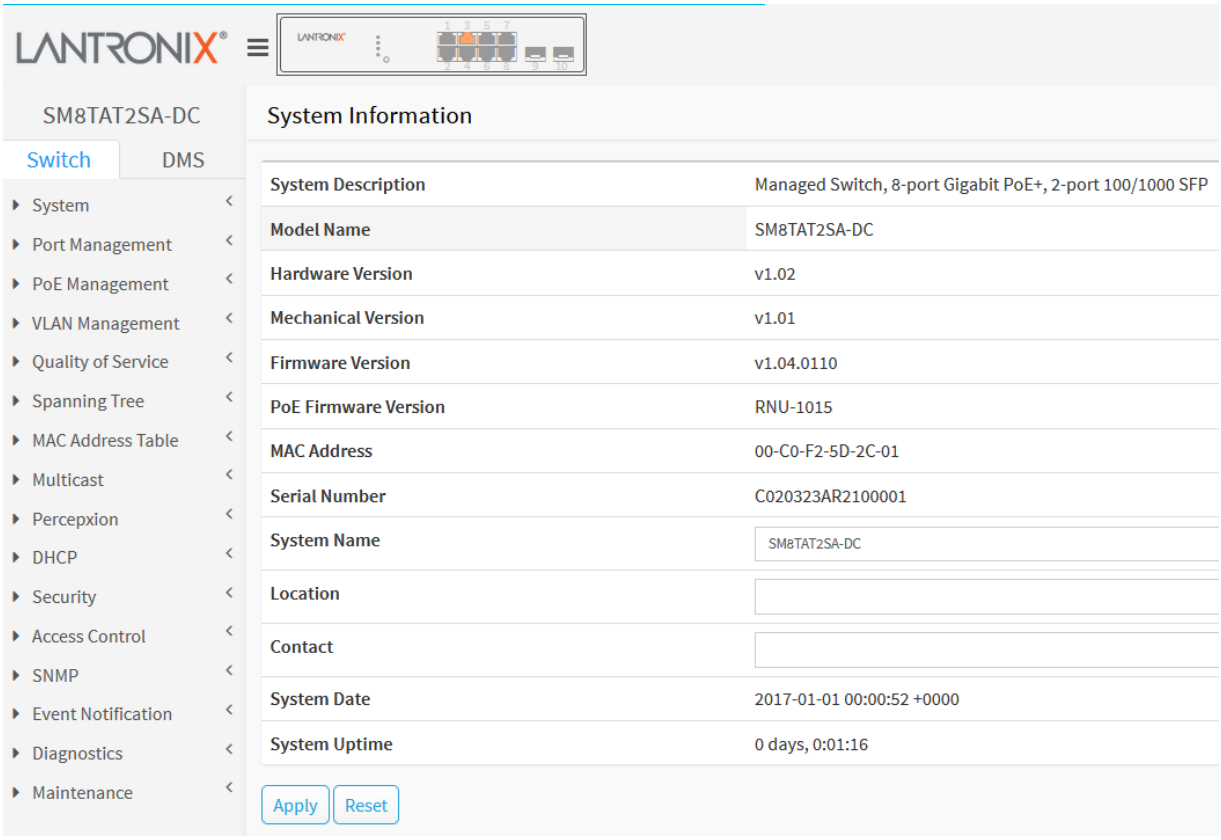


Figure 3-2: System Information (SM8TAT2SA-DC shown)

3-2 IP Address

3-2.1 IP Settings

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

To configure IP settings in the web UI:

1. Click System, IP Address, IP Settings.
2. Check the "IPv4 DHCP Client Enable" box.
3. Enter the IPv4 Address, Subnet Mask, Gateway, and DNS Server parameters.
4. Click Apply.

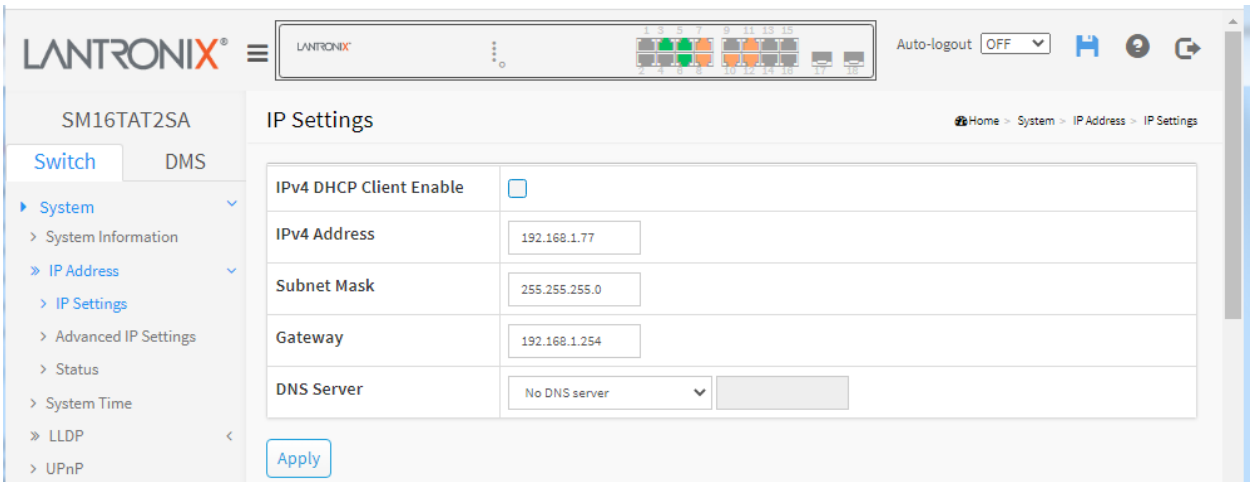


Figure 3-2.1: IP Settings page

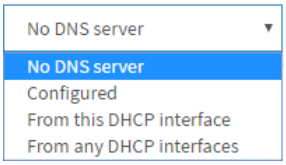
Parameter descriptions:

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

IPv4 Address: The IPv4 address of the interface in dotted decimal notation (e.g., 192.168.1.77). 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 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. User IP subnet mask of the entry (e.g., 255.255.255.0).

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



DNS Server: Select either No DNS server, Configured, From this DHCP interface, or From any DHCP interfaces. If you select "Configured", enter an IP address.
If you select "From this DHCP interface", enter a DNS Server number (configured in the following section "Advanced IP Settings".

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

No DNS server: No DNS server will be used.

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

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

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

Buttons

Apply: Click to save changes.

3-2.1 Advanced IP Settings

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

Configure switch-managed IP information on this page, including DNS server settings, IP interfaces, Link Local Address binding interface, and IP routes. You can configure up to 8 interfaces and 8 routes.

To configure advanced IP settings in the web UI:

1. Click System, IP Address, Advanced IP Settings.
2. Click Add Interface and configure the new Interface for the switch.
3. Click Add Route and configure the new route for the switch.
4. Click Apply.

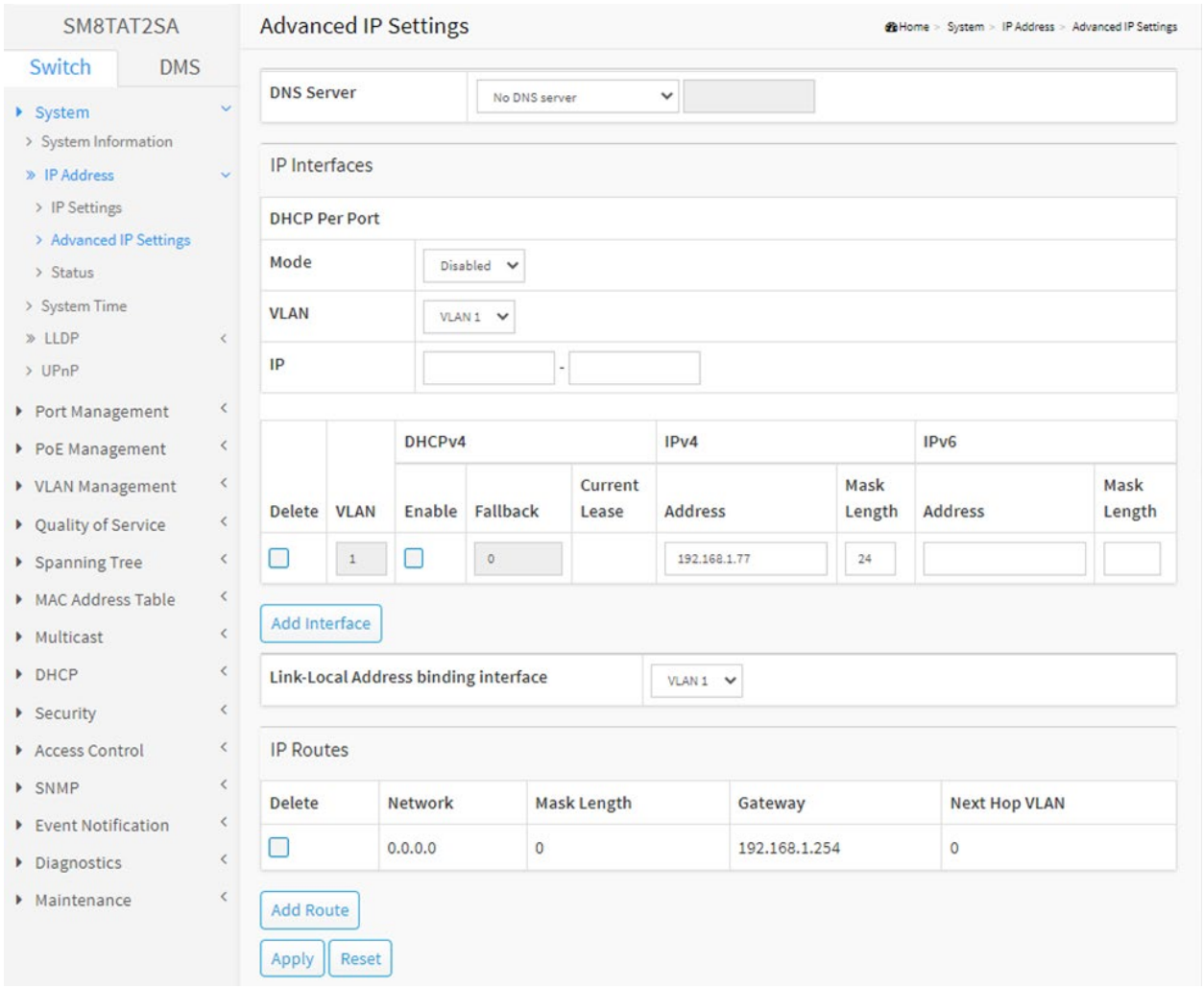


Figure 3-2.1: Advanced IP Settings

Parameter descriptions:

Advanced IP Settings

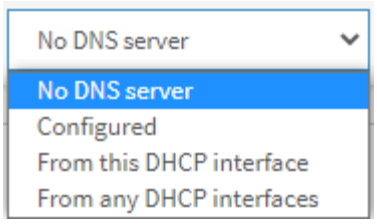
DNS Server: Controls the DNS name resolution done by the switch. These modes are supported:

No DNS server: No DNS server will be used.

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

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

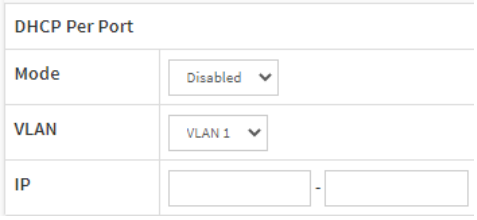
From any DHCP interfaces: The first DNS server offered from a DHCP lease to a DHCP-enabled interface will be used.



IP Interfaces

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

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



DHCP Per Port VLAN: The VLAN associated with the IP interface. Only ports in this VLAN will be able to access the IP interface. This field is only available for input when creating a new interface. This 'DHCP IP per Port' function lets you assign a static IP address from a DHCP pool to a switch port such that it will always be assigned that specific IP address. 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. (Added at FW v1.04.0079.)

DHCP Per Port IP: Define the IP range for DHCP Per Port. The range must be equal to the number of switch RJ45/TP ports (e.g., 16 for the SM16TAT2SA).

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

DHCPv4 Fallback: The number of seconds for trying to obtain a DHCP lease. After this Timeout period expires, a configured IPv4 address will be used as IPv4 interface address. A value of zero disables the fallback mechanism, such that DHCP will keep retrying until a valid lease is obtained. Legal values are 0 to 4294967295 seconds.

DHCPv4 Current Lease: For IPv4 DHCP interfaces with an active lease, this column shows the current interface address, as provided by the DHCP server.

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

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

IPv6 Address: The IPv6 address of the interface. An IPv6 address is in 128-bit records represented as eight fields of up to four hexadecimal digits with a colon separating each field (:). For example, fe80::215:c5ff:fe03:4dc7. The symbol :: is a special syntax that can be used as a shorthand way of representing multiple 16-bit groups of contiguous zeros; but it can appear only once. It can also represent a 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: 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: Configure Link-Local IP address to a different VLAN interface. The first IP interface entry is for the default value. A link-local address is a network address that is valid only for communication within the network segment or the broadcast domain that the host is connected to. Link-local addresses are not guaranteed to be unique beyond their network segment. IPv4 link-local addresses are assigned from address block 169.254.0.0/16 (169.254.0.0 - 169.254.255.255). In IPv6, they are assigned from the block fe80::/10.

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 0.0.0.0or IPv6 :: notation.

Mask Length: The destination IP network or host mask, in number of bits (prefix length). It defines how much of a network address that must match, in order to qualify for this route. Valid values are 0 - 32 bits for IPv4 routes and128 bits for IPv6 routes. Only a default route will have a mask length of 0 (as it will match anything).

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

Next Hop VLAN (Only for IPv6): The VLAN ID (VID) of the specific IPv6 interface associated with the gateway. The valid VID range is 1 - 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 8 interfaces is supported.

Add Route: Click to add a new IP route. A maximum of 8 routes is supported.

Apply: Click to save changes.

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

Messages:

Message: *ERROR: DHCP Per Port IP range (192.168.1.1 - 192.168.1.10) is not equal to switch RJ45/TP port number (16)*

Message: *Subnet overlaps with VLAN 1*

Message: *VLAN 1 used for more than one interface*

Message: *This field is required.*

Message: *Subnet of VLAN 2 overlaps VLAN 1*

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

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

Message: *ipv4 – 1.2.3.4 – Address conflict*

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

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

Message: *A static address is only used if the fall-back timeout is non-zero.*

Message: *Invalid route - address bits outside mask: 0.0.1.77*

Message: *Default route mask length must be zero.*

Message: *ERROR: Already exists*

Message: *IP address will be modify in management interface, and then use the new IP address to reconnect.*

3-2.2 IP Status

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

To display IP status in the web UI:

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

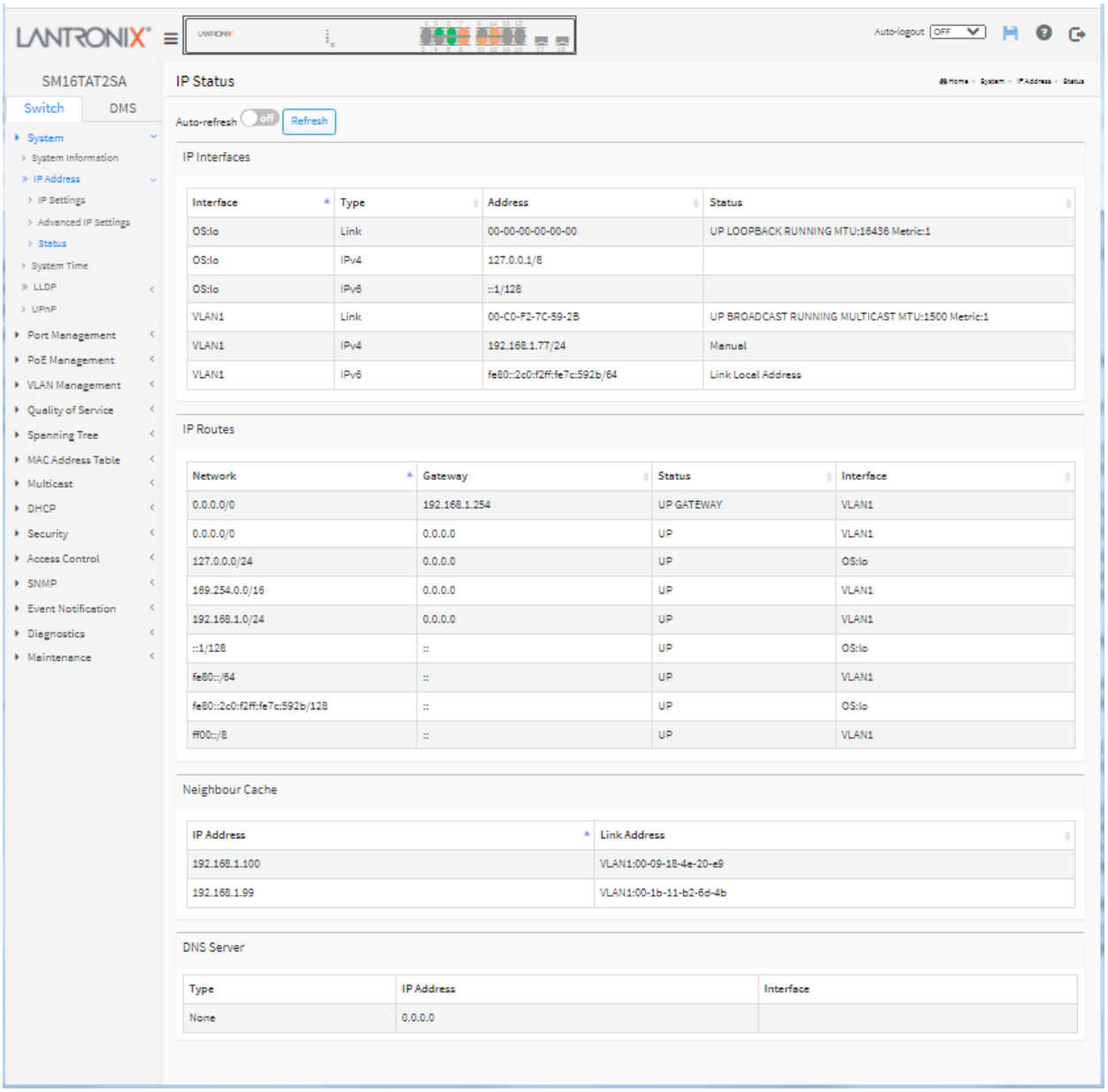


Figure 3-2.2: IP Status page

Parameter descriptions:

IP Interfaces

Interface: Shows the name of the interface (e.g., OS:lo or VLAN1).

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

Address: Shows the current address of the interface (of the given type; e.g., 192.168.1.77/24 or ::1/128 or 00-40-C7-1C-CB-6E).

Status: Shows the status flags of the interface (and/or address). For example: UP LOOPBACK RUNNING MTU:16436 Metric:1 or UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1, or Manual, or Link Local Address, or DHCP Fallback.

IP Routes

Network: Shows the destination IP network or host address of this route (e.g., 192.168.1.0/24).

Gateway: Shows the gateway address of this route (e.g., 192.168.1.254 or ::).

Status: Shows the status flags of the route (e.g., UP or UP GATEWAY).

Interface: Shows the name of the interface (e.g., OS:lo or VLAN1).

Neighbor Cache

IP Address: Show the IP address of the entry (e.g., 192.168.1.99).

Link Address: Show the Link (MAC) address for which a binding to the given IP address exists (e.g., VLAN1:00-1b-11-b2-6d-4b).

DNS Server

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

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

Interface: Show the name of the interface.

Buttons

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

Refresh: Click to manually refresh the page immediately.

3-3 System Time

The switch provides manual and automatic ways to set the system time via NTP. For manual setting, enter the "Year", "Month", "Day", "Hour" and "Minute" within the valid value range indicated for each item.

To configure Time in the web UI:

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

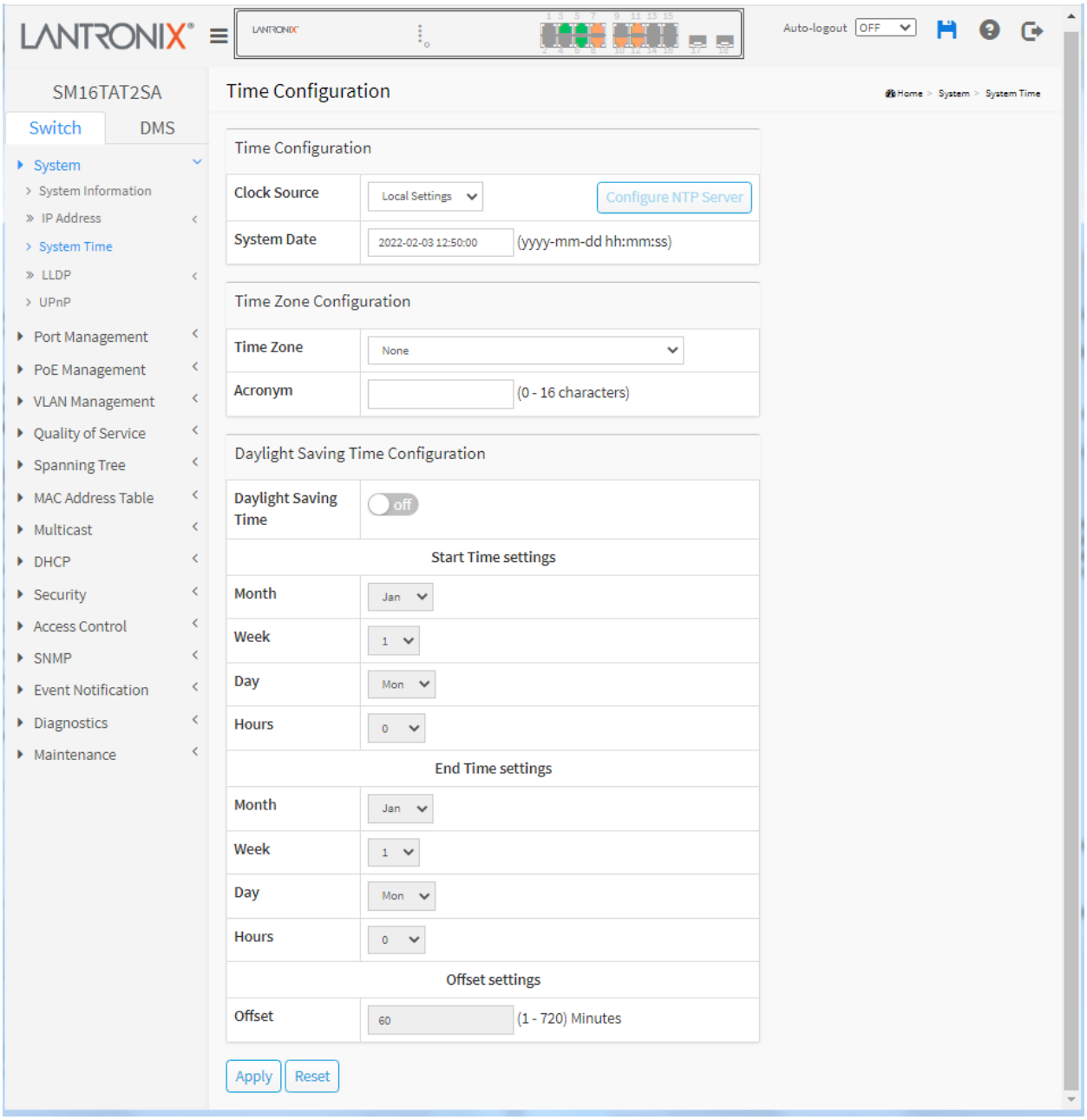


Figure 3-3: Time Configuration page

Time Configuration

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

System Date: Show the current time of the system. The year of system date must be 2000 - 2037.

Time Zone Configuration

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

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

Daylight Saving Time Configuration

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

Recurring Configuration

Start time settings:

Month - Select the starting month (Jan – Dec).

Week - Select the starting week number (1-5).

Day - Select the starting day (Mon – Sun).

Hours - Select the starting hour (0-23).

End time settings:

Month - Select the starting month (Jan – Dec).

Week - Select the starting week number (1-5).

Day - Select the starting day (Mon – Sun).

Hours - Select the starting hour (0-23).

Offset settings: Offset - Enter the number of minutes to add during Daylight Saving Time. The valid range is 1 to 1440 minutes. The default is 60 minutes.

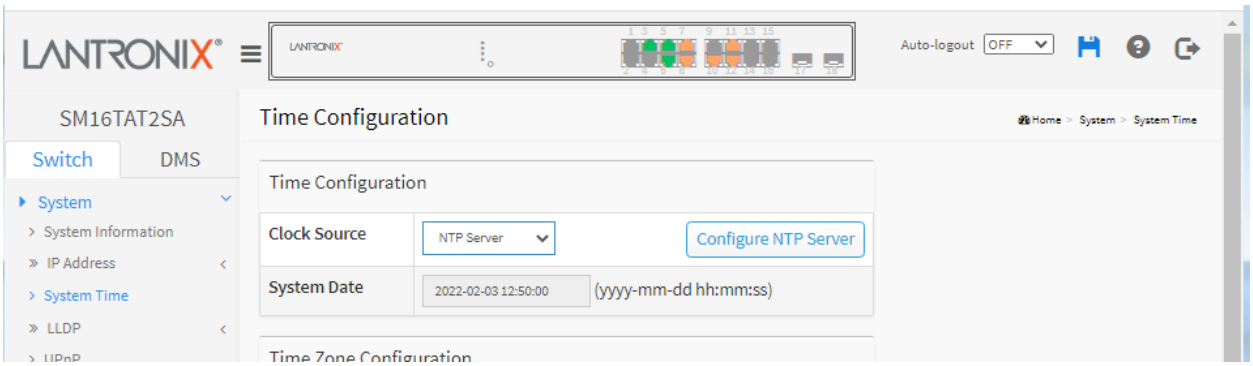
Note: The information under “Start Time Settings” and “End Time Settings” displays what you set on the “Start Time Settings” and “End Time Settings” field information.

Buttons

Apply: Click to save changes.

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

Configure NTP Server: At "**Clock Source**" select NTP Server. This enables the **Configure NTP Server** button.



Click the **Configure NTP Server** button to configure NTP server.

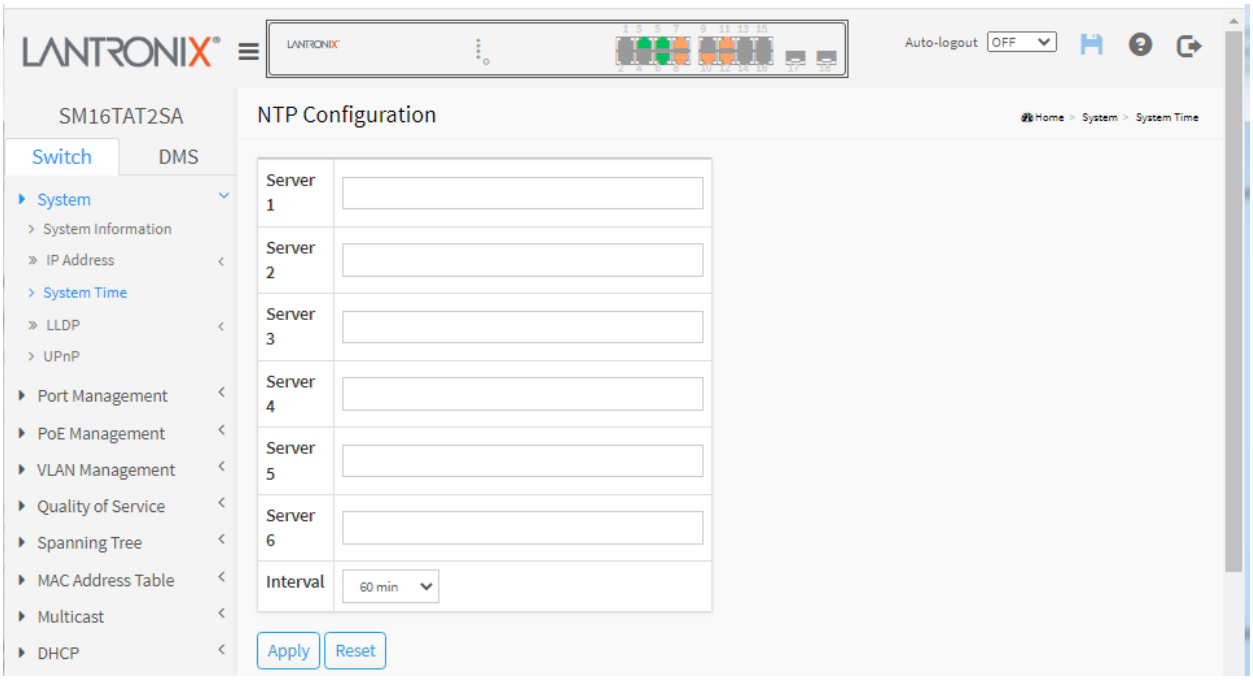


Figure 3-3: NTP Configuration page

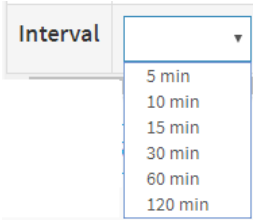
NTP (Network Time Protocol) is used to sync the network time based Greenwich Mean Time (GMT). If use the NTP mode and select a built-in NTP time server or manually specify a user-defined NTP server as well as Time Zone, the switch will sync the time in a short after pressing Apply button. Though it synchronizes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

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

Parameter descriptions:

Server 1 to 6: 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 '::' can be used as a shorthand way of representing multiple 16-bit groups of contiguous zeros; but it can only appear once. It can also represent a valid IPv4 address. For example, '::192.1.2.34'.

Interval: You can specify the time interval in seconds after which a time check and, in case of deviation, a resynchronization of the internal device clock against the specified timeserver via Network Time Protocol (NTP) should be performed.



The selections are 5 min, 10 min, 15 min, 30 min, 60 min, and 120 min.

Buttons: These buttons are displayed on the NTP page:

Apply: Click to save changes.

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

Message:
The input value 'Server 2 Address' (::)
is not a valid IPv6 address.
The Unspecified Address must never be assigned to any node.

Message:
The value of 'Server 2 Address' (:: ::)
must be a valid IPv6 address.
The symbol '::' can appear once.

Message:
The value of 'Server 2 Address' (::)
must be a valid IPv6 address in 128-bit record represented as
eight fields of up to four hexadecimal digits with a colon (:) separating
each field.

Message:
The format of 'Server 3 Address' is invalid.

It must either be a valid IP address in dotted decimal notation
('x.y.z.w') or a valid hostname.
A valid hostname is a string drawn from the alphabet (A-Za-z), digits
(0-9), dot (.), hyphen (-).
Spaces are not allowed, the first character must be an alphanumeric character,
and the first and last characters must not be a dot or hyphen.

3-4 LLDP

The switch supports the Link Layer Discovery Protocol (LLDP) which provides a standards-based method to enable switches to advertise themselves to adjacent devices and to learn about adjacent LLDP devices.

LLDP is a vendor-neutral Link Layer protocol in the Internet Protocol Suite used by network devices for advertising their identity, capabilities, and neighbors on a IEEE 802 local area network, principally wired Ethernet. The protocol is formally referred to by the IEEE as Station and Media Access Control Connectivity Discovery specified in standards document IEEE 802.1AB.

LLDP can be used as a component in network management and network monitoring applications. LLDP is also used to advertise power over Ethernet capabilities and requirements and negotiate power delivery.

LLDP-MED provides extended and automated power management of Power over Ethernet (PoE) end points. Media Endpoint Discovery is an enhancement of LLDP, known as LLDP-MED.

3-5.1 LLDP Configuration

This page lets you view and set LLDP detail parameters on a per-port basis; the settings take effect immediately.

LLDP uses System Capability Codes: B = Bridge (Switch), C = DOCSIS Cable Device, O = Other, P = Repeater, R = Router, S = Station, T = Telephone, and W = WLAN Access Point.

LLDP information is sent by devices from each of their interfaces at a fixed interval, in the form of an Ethernet frame. Each frame contains one LLDP Data Unit (LLDPDU). Each LLDPDU is a sequence of type-length-value (TLV) structures.

The Ethernet frame used in LLDP typically has its destination MAC address set to a special multicast address that 802.1D-compliant bridges do not forward. Other multicast and unicast destination addresses are permitted. The EtherType field is set to 0x88cc.

Each LLDP frame starts with the mandatory TLVs Chassis ID, Port ID, and Time-to-Live.

Web Interface

To configure LLDP:

1. Click System, LLDP, and LLDP Configuration.
2. Modify LLDP Parameters and LLDP Port Parameters.
3. Specify the information to include in the TLV field of advertised messages.
4. Click Apply.

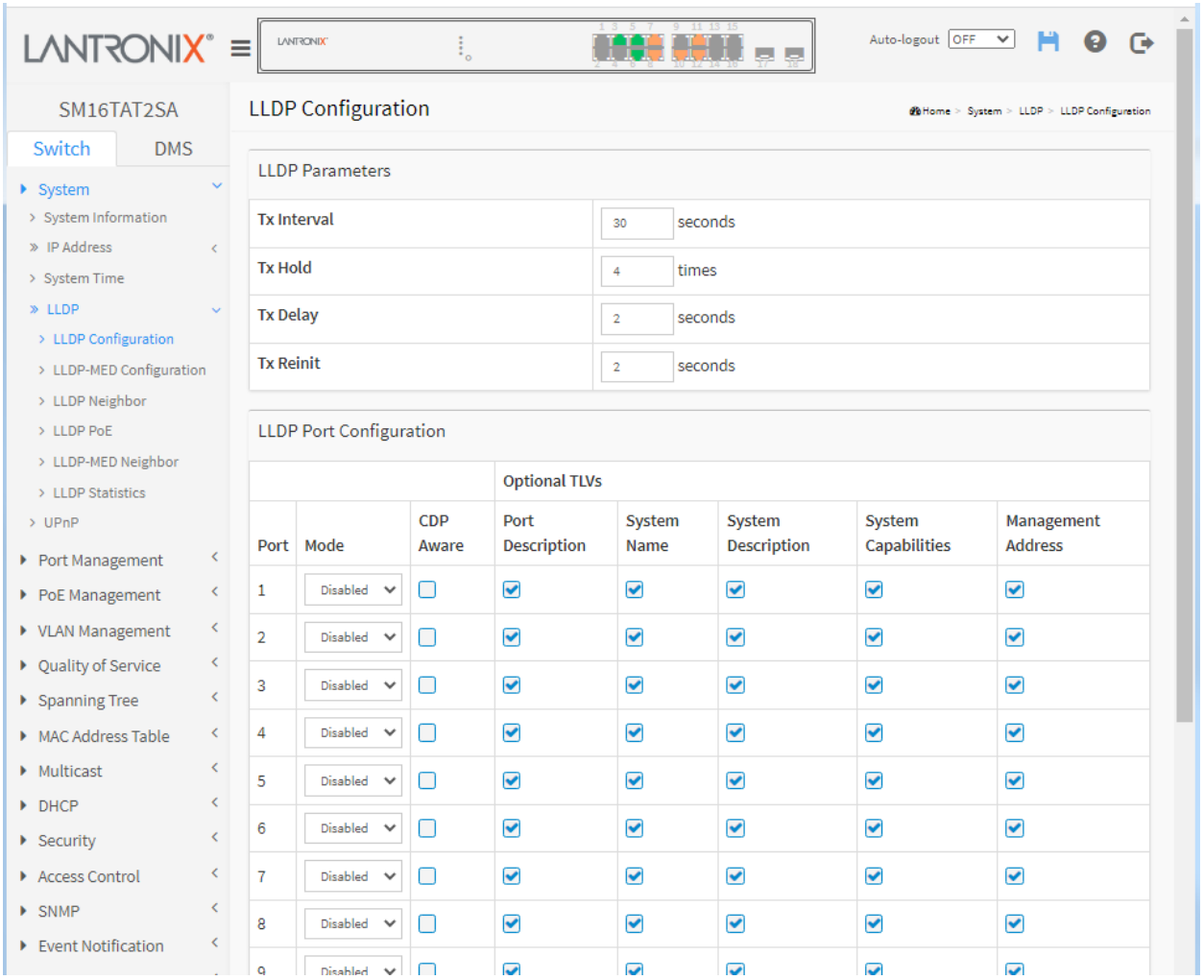


Figure 3-5.1: LLDP Configuration page

LLDP Parameters:

Tx Interval: The switch periodically transmits LLDP frames to its neighbors for having the network discovery information up-to-date. The interval between each LLDP frame is determined by the Tx Interval value. Valid values are 5 - 32768 seconds. The default is 30 seconds.

Tx Hold: Each LLDP frame contains information about how long the information in the LLDP frame will be considered valid. The LLDP information valid period is set to Tx Hold multiplied by Tx Interval seconds. Valid values are 2 - 10 times. The default is 4 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 1 - 8192 seconds. The default is 2 seconds.

Tx Reinit: When a port is disabled, LLDP is disabled or the switch is rebooted, an LLDP shutdown frame is transmitted to the neighboring units, signaling that the LLDP information isn't valid anymore. Tx Reinit controls the number of seconds between the shutdown frame and a new LLDP initialization. Valid values are 1 - 10 seconds. The default is 2 seconds.

LLDP Port Configuration: The LLDP port settings relate to the currently selected, as reflected by the page header.

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.

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

Only CDP TLVs that can be mapped to a corresponding field in the LLDP neighbors' table are decoded. All other TLVs are discarded (Unrecognized CDP TLVs and discarded CDP frames are not shown in the LLDP statistics.). CDP TLVs are mapped onto LLDP neighbors' table as shown below.

CDP TLV "Device ID" is mapped to the LLDP "Chassis ID" field.

CDP TLV "Address" is mapped to the LLDP "Management Address" field. The CDP address TLV can contain multiple addresses, but only the first address is shown in the LLDP neighbors' table.

CDP TLV "Port ID" is mapped to the LLDP "Port ID" field.

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

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

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

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

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

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

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

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

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

Buttons

Apply: Click to save changes.

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

Messages:

Tx Delay must not be larger than 1/4 of the Tx Interval value (IEEE 802.1AB-clause 10.5.4.2)

3-4.2 LLDP-MED Configuration

This page lets you configure LLDP-MED. This function applies to devices which support LLDP-MED. Media Endpoint Discovery is an LLDP enhancement, called LLDP-MED, that provides these facilities:

Auto-discovery of LAN policies (such as VLAN, Layer 2 Priority and Differentiated services (Diffserv) settings) enabling plug and play networking.
Device location discovery allows 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 is provided.
Inventory management, allowing network administrators to track their network devices, and determine their characteristics (manufacturer, software and hardware versions, and serial or asset number).

To configure LLDP-MED in the web UI:

1. Click System, LLDP, and LLDP-MED Configuration.
2. Modify Fast Start Repeat Count parameter; the default is 4.
3. Modify Coordinates Location parameters.
4. Enter Civic Address Location parameters.
5. Enter Emergency Call Service parameter.
6. Click the Add New Policy button and configure a new policy.
7. Select a Policy ID for each port.
8. Click Apply.

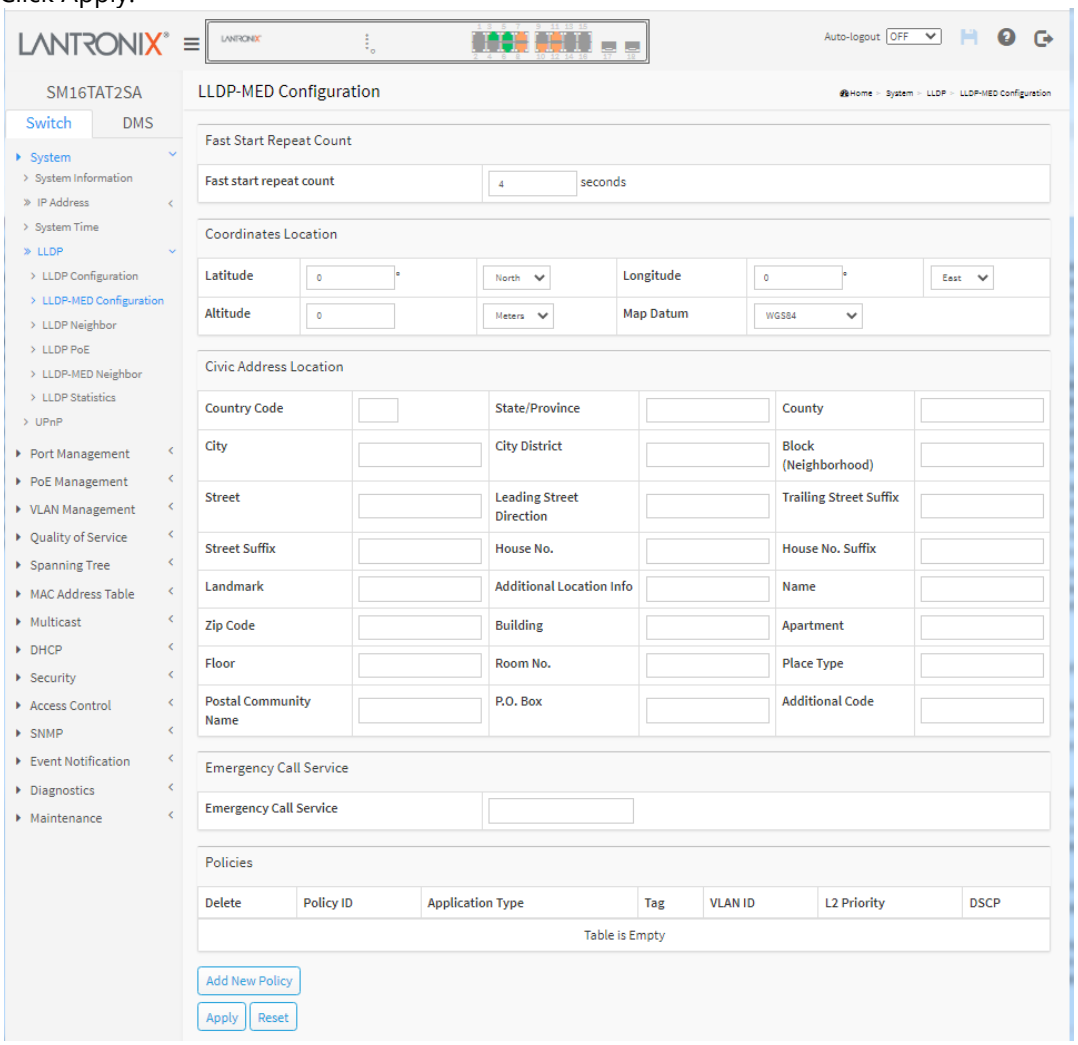


Figure 3-5.2: LLDP-MED Configuration page

Parameter descriptions:

Fast start repeat count

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

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

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

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.

Coordinates Location

Latitude: Latitude 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 normalized to within 0-180 degrees with a maximum of 4 digits. It is possible to specify the direction to either East of the prime meridian or West of the prime meridian.

Altitude: Altitude normalized to within -32767 to 32767 with a maximum of 4 digits.

It is possible to select between two altitude types (floors or meters).

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

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

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

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

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

***NAD83/MLLW*:** North American Datum 1983, CRS Code 4269, Prime Meridian Name: Greenwich;

the associated vertical datum is Mean Lower Low Water (MLLW). This datum pair is to be used when referencing locations on water/sea/ocean.

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

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

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

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

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

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

Block (Neighborhood): Neighborhood, block.

Street: Street - Example: Poppelvej.

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

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

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

House no.: House number - Example: 21.

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

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

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

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

Zip code: Postal/zip code - Example: 2791.

Building: Building (structure) - Example: Low Library.

Apartment: Unit (Apartment, suite) - Example: Apt 42.

Floor: Floor - Example: 4.

Room no. : Room number - Example: 450F.

Place type: Place type - Example: Office.

Postal community name: Postal community name - Example: Leonia.

P.O. Box: Post office box (P.O. BOX) - Example: 12345.

Additional code: Additional code - Example: 1320300003.

Emergency Call Service: Emergency Call Service (e.g., E911 and others), such as defined by TIA or NENA.

Emergency Call Service: Emergency Call Service ELIN identifier data format is defined to carry the ELIN identifier as used during emergency call setup to a traditional CAMA or ISDN trunk-based PSAP. This format consists of a numerical digit string, corresponding to the ELIN to be used for emergency calling.

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

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

The network policy attributes advertised are:

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

This network policy is potentially advertised and associated with multiple sets of application types supported on a given port. The application types specifically addressed are:

1. Voice
2. Guest Voice
3. Softphone Voice
4. Video Conferencing
5. Streaming Video
6. Control / Signaling (conditionally support a separate network policy for the media types above)

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

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

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

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

Application Type: Intended use of the application; types include:

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Port: The port number to which the configuration applies.

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

Buttons

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.

3-4.3 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. If your network device doesn't support LLDP or if LLDP is not enabled, the table displays "*No LLDP neighbor information found*".

To show LLDP neighbors:

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

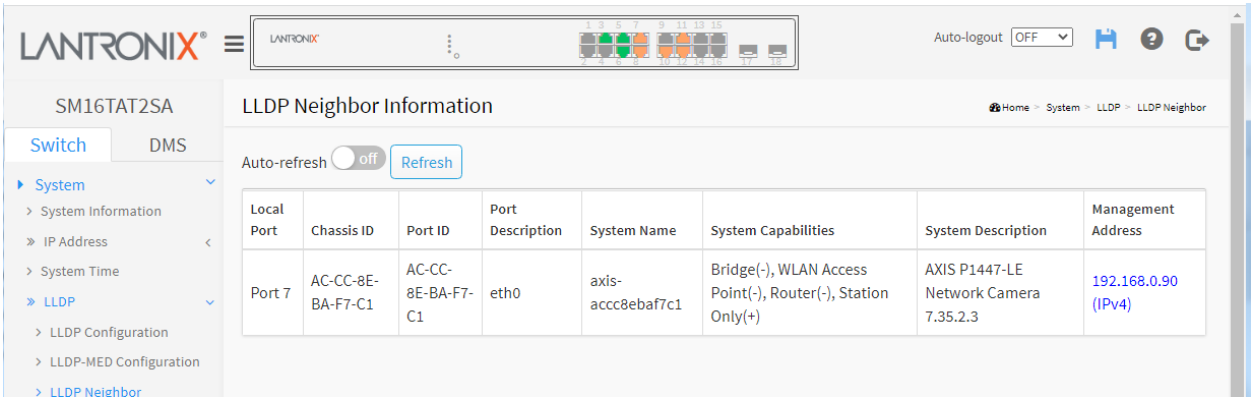


Figure 3-5.3: LLDP Neighbor Information

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: System Capabilities describes the neighbor unit's capabilities. The possible system 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 a (-).

System Description: Displays the system description.

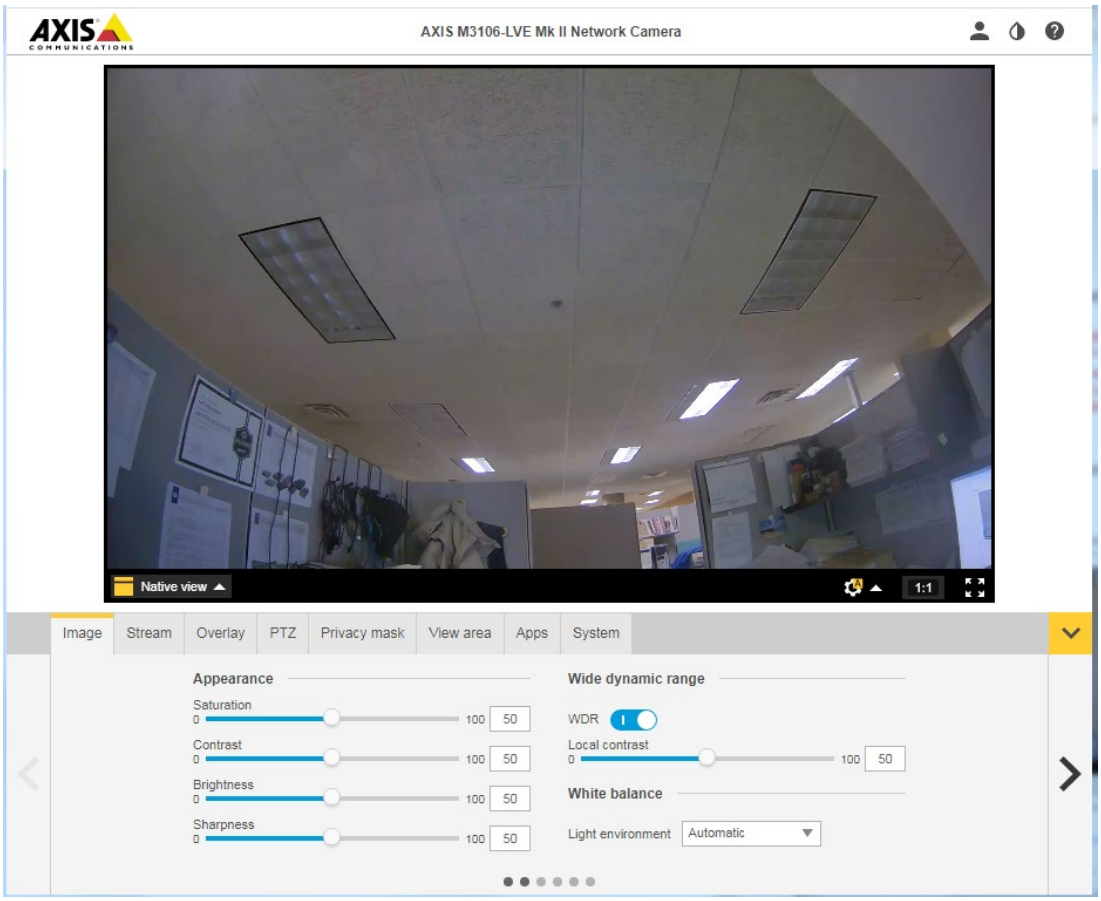
Management Address: The neighbor unit's IP address that is used for higher layer entities to assist discovery by the network management. This could for instance hold the neighbor's IP address. You can click the linked text to display the device webpage. See the example below.

Buttons

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

Refresh: Click to manually refresh the page immediately.

Example


AXIS M3106-LVE Mk II Network Camera
Native view
1:1
Image
Stream
Overlay
PTZ
Privacy mask
View area
Apps
System
Appearance
Saturation
Contrast
Brightness
Sharpness
Wide dynamic range
WDR
Local contrast
White balance
Light environment
Automatic

3-4.4 LLDP PoE

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

1. Click System, LLDP, and LLDP PoE.
2. Observe the parameters displayed.
3. Click Refresh to manually update the web page immediately.
4. Click Auto-refresh to automatically update web page every 3 seconds.

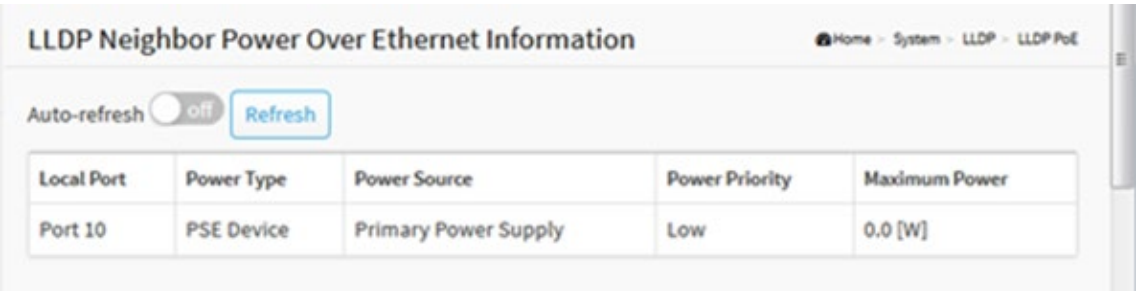


Figure 3-4.3: LLDP Neighbor Power Over Ethernet Information

Parameter descriptions:

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

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

Power Source: 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, 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 port that is sourcing the power. The three levels of power priority are ***Critical***, ***High*** and ***Low***. If the power priority is unknown it is indicated as "***Unknown***".

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

Buttons

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

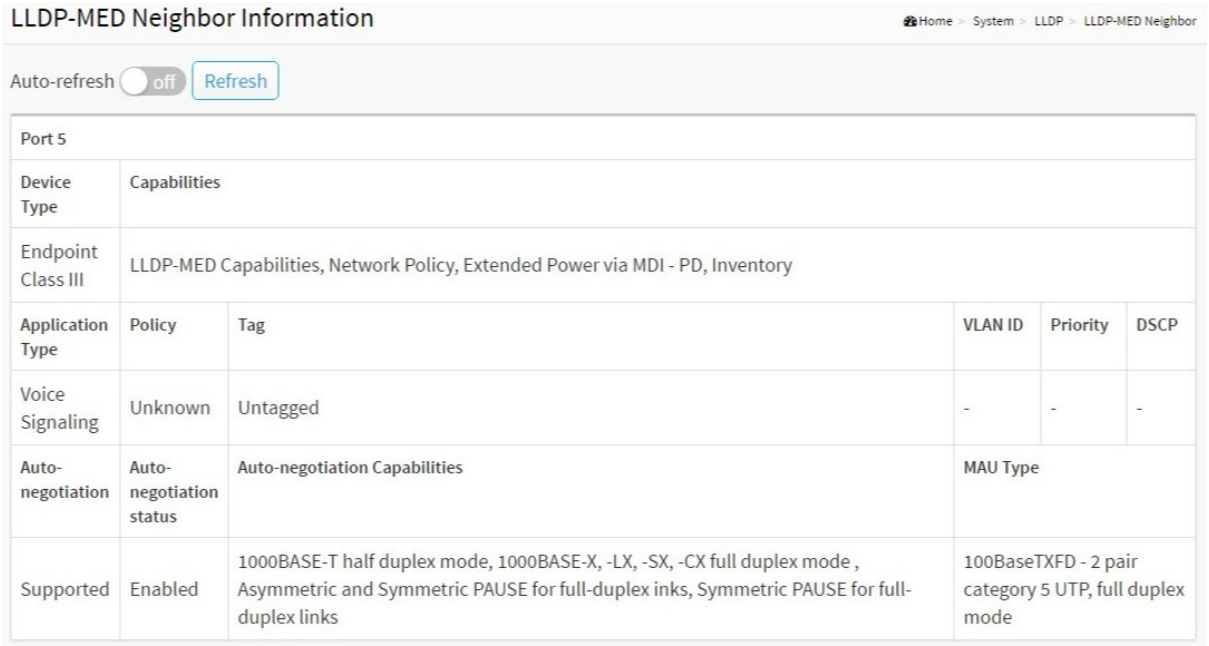
Refresh: Click to manually refresh the page immediately.

3-4.4 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 neighbor is detected. This function applies to VoIP devices which support LLDP-MED. If your network has no devices that support LLDP-MED then the table will show "*No LLDP-MED neighbor information found*".

To show LLDP-MED neighbor:

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



Port 5					
Device Type	Capabilities				
Endpoint Class III	LLDP-MED Capabilities, Network Policy, Extended Power via MDI - PD, Inventory				
Application Type	Policy	Tag	VLAN ID	Priority	DSCP
Voice Signaling	Unknown	Untagged	-	-	-
Auto-negotiation	Auto-negotiation status	Auto-negotiation Capabilities	MAU Type		
Supported	Enabled	1000BASE-T half duplex mode, 1000BASE-X, -LX, -SX, -CX full duplex mode , Asymmetric and Symmetric PAUSE for full-duplex inks, Symmetric PAUSE for full-duplex links	100BaseTXFD - 2 pair category 5 UTP, full duplex mode		

Figure 3-4.4: LLDP-MED Neighbor Iformation page

Parameter descriptions:

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

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

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

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

LLDP-MED Endpoint Device Definition: LLDP-MED Endpoint Devices, as defined in TIA-1057, are located at the IEEE 802 LAN network edge, and participate in IP communication service using the LLDP-MED framework.

Within the LLDP-MED Endpoint Device category, the LLDP-MED scheme is broken into further Endpoint Device Classes, as defined in the following.

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

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

LLDP-MED Media Endpoint (Class II): The LLDP-MED Media Endpoint (Class II) definition is applicable to all endpoint products that have IP media capabilities however may or may not be associated with a particular end user. Capabilities include all of the capabilities defined for the previous Generic Endpoint Class (Class I) and are extended to include aspects related to media streaming. Example product categories expected to adhere to this class include (but are not limited to) Voice / Media Gateways, Conference Bridges, Media Servers, and similar.
Discovery services defined in this class include media-type-specific network layer policy discovery.

LLDP-MED Communication Endpoint (Class III): The LLDP-MED Communication Endpoint (Class III) definition is applicable to all endpoint products that act as end user communication appliances supporting IP media. Capabilities include all of the capabilities defined for the previous Generic Endpoint (Class I) and Media Endpoint (Class II) classes and are extended to include aspects related to end user devices. Example product categories expected to adhere to this class include (but are not limited to) end user communication appliances, such as IP Phones, PC-based softphones, or other communication appliances that directly support the end user.
Discovery services defined in this class include provision of location identifier (including ECS / E911 information), embedded L2 switch support, inventory management.

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

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

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

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

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

Unknown: The network policy for the specified application type is currently unknown.

Defined: The network policy is defined.

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

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

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

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

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

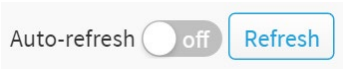
DSCP: The DSCP value to be used to provide Diffserv node behavior for the specified application type as defined in IETF RFC 2474. Contain one of 64 code point values (0 through 63).

Auto-negotiation: Identifies if MAC/PHY auto-negotiation is supported by the link partner.

Auto-negotiation status: identifies if auto-negotiation is currently enabled at the link partner.
If **Auto-negotiation** is supported and **Auto-negotiation status** is disabled, the 802.3 PMD operating mode will be determined the operational MAU type field value rather than by auto-negotiation.

Auto-negotiation Capabilities: shows the link partners MAC/PHY capabilities.

Buttons



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

Refresh: Click to manually refresh the page immediately.

3-4.5 LLDP Statistics

Two types of counters are shown. *Global* counters are counters that refer to the whole switch, while *Local* counters refer to per port counters for the switch.

To show LLDP Statistics:

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

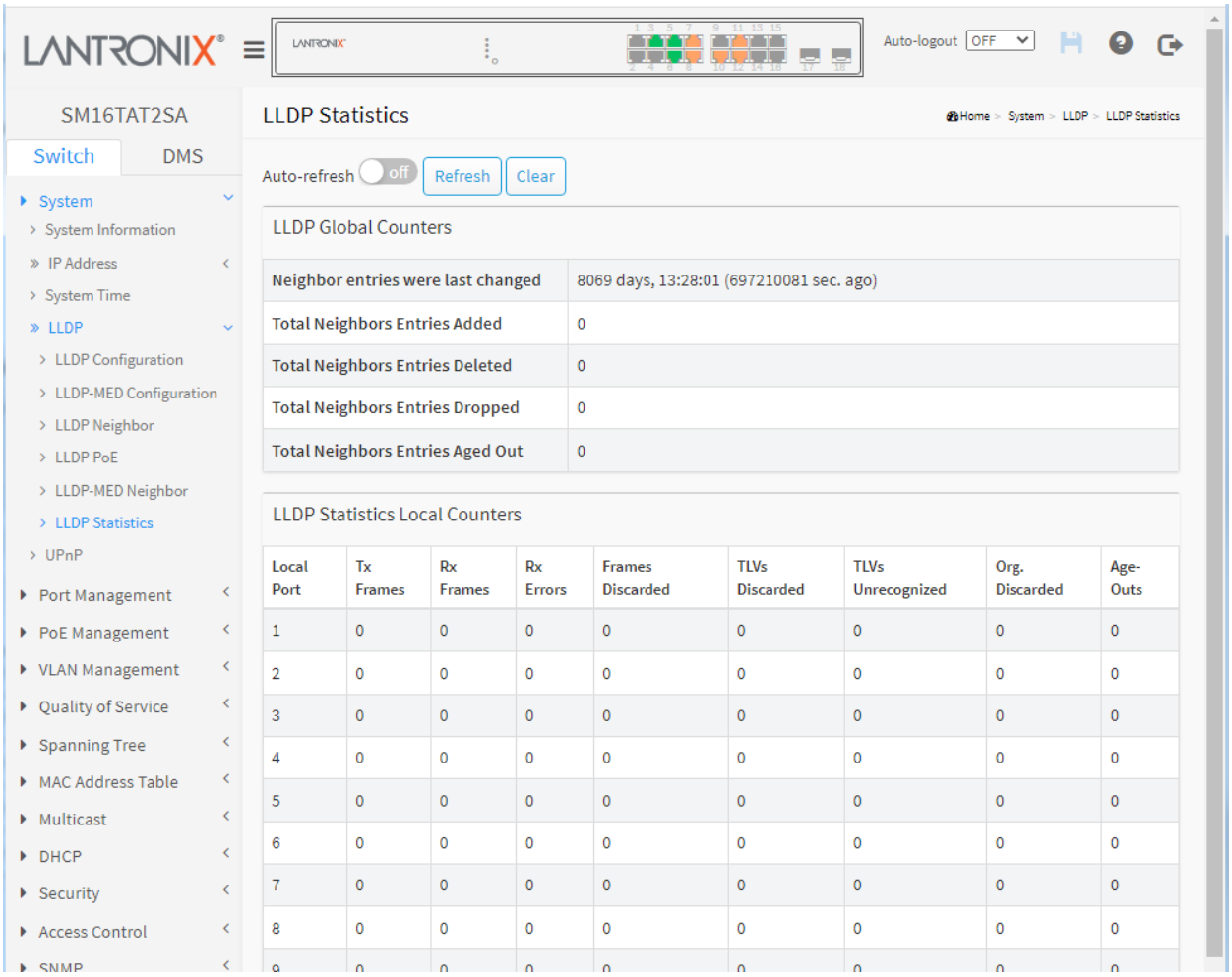


Figure 3-4.5: LLDP Statistics information

Global Counters

Neighbor entries were last changed: Shows the time when the last entry was last deleted or added. It also shows the time elapsed since the last change was detected.

Total Neighbors Entries Added: Shows the number of new entries added since switch reboot.

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

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

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

Local Counters: The displayed table contains a row for each port. The columns display 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 to refresh the page automatically every 3 seconds.

Refresh: Click to manually refresh the page immediately.

Clear: Clears the counters for the selected port.

3-5 UPnP

The goals of UPnP (Universal Plug and Play) 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. Scroll to select the mode to enable or disable.
3. Specify the parameters in each field.
4. Click the **Apply** button to save the settings.
5. To cancel the setting click the **Reset** button to revert to previously saved values.

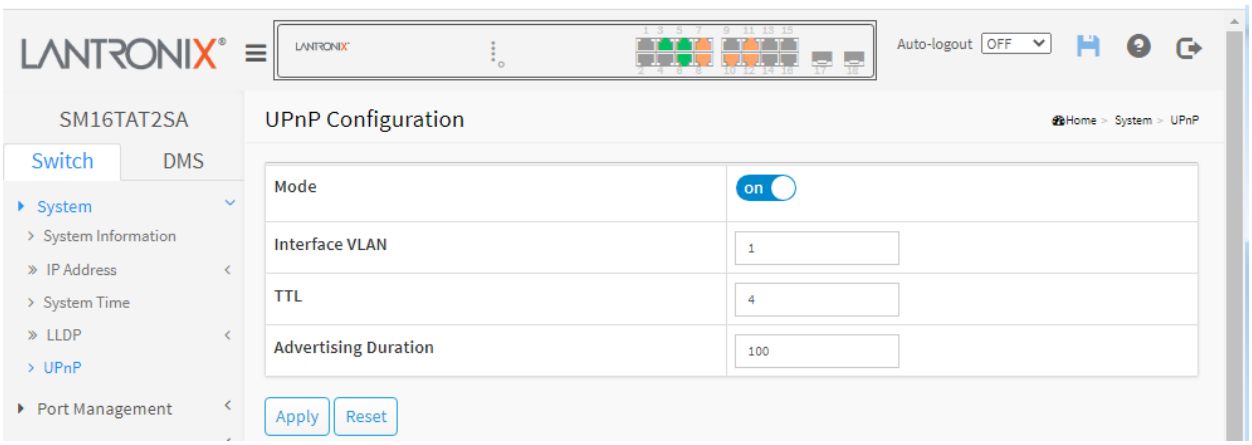


Figure 3-5: UPnP Configuration page

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

***Enabled*:** Enable UPnP mode operation.
***Disabled*:** Disable UPnP mode operation.

When Mode is enabled, two ACEs are added automatically to trap UPNP related packets to the CPU. The ACEs are automatically removed when the mode is disabled.

Interface VLAN: The Interface VLAN value is used by UPnP to send SSDP advertisement messages for the Interface VLAN. Valid values are VIDs 1 - 4095.

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

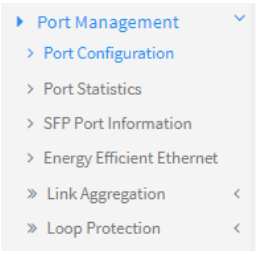
Advertising Duration: The duration, carried in SSDP packets, is used to inform a control point or control points how often it or they should receive an SSDP advertisement message from this switch. If a control point does not receive any message within the duration, it will think that the switch no longer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

Buttons

Apply: Click to save changes.

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

Chapter 4 Port Management



This section lets you view and configure switch Port functions.

4-1 Port Configuration

This page lets you view and configure current port parameters.

To set Port Configuration parameters in the web UI:

1. Click Port Management and Port Configuration.
2. Specify the Maximum Frame Size, Speed Mode, Flow Control, and Description parameters.
3. Click the Apply button.

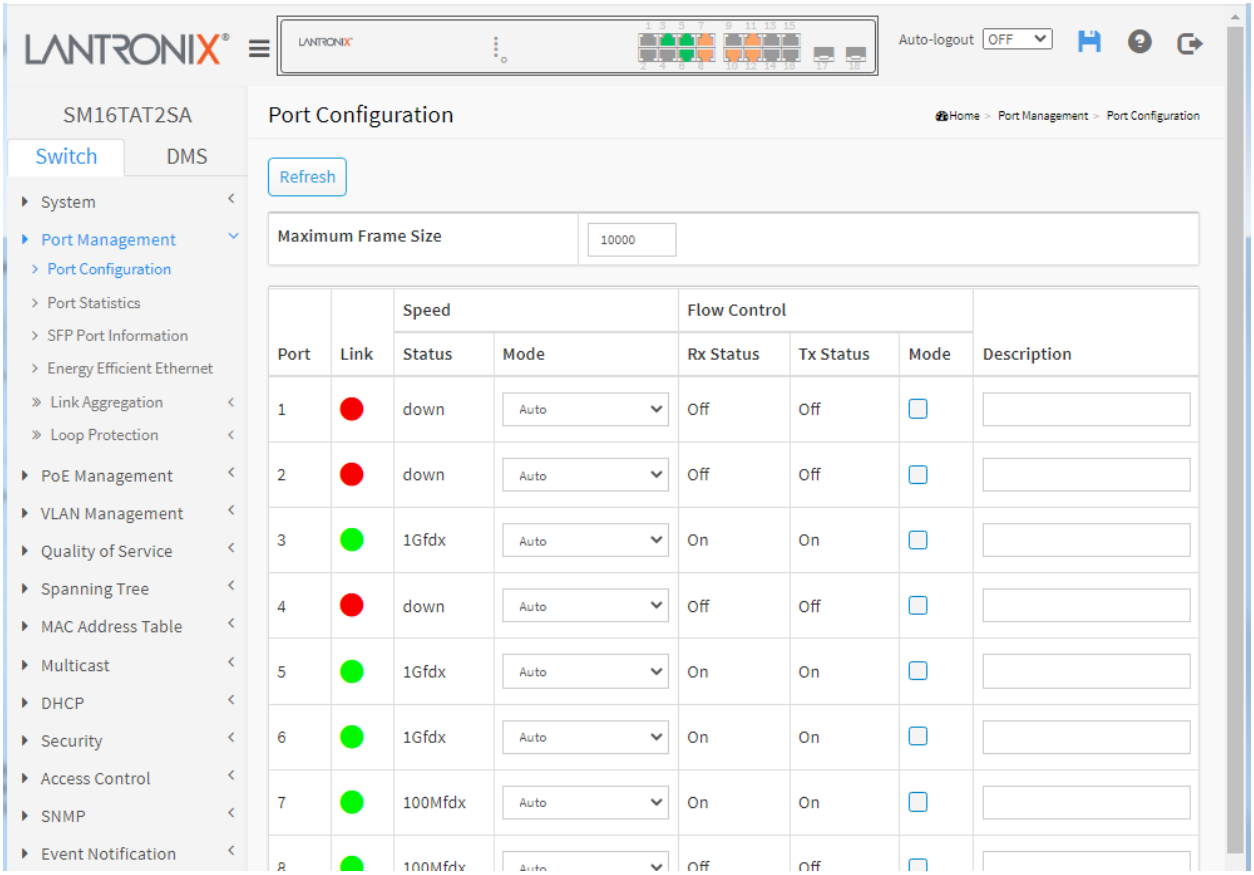


Figure 4-1: Port Configuration page

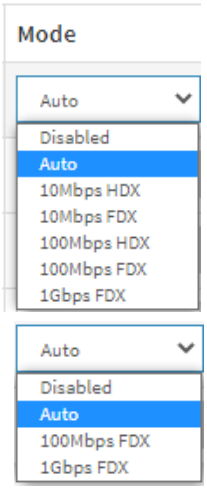
Parameter descriptions:

Maximum Frame Size : Maximum packet length filtering is examined on both receiving and transmitting ports. Enter the maximum frame size allowed for the switch port, including FCS. The valid range is 1518-10000 bytes. The default value is 10,000 bytes. FW v1.04.0009 added Maximum Frame Size setting per system in the Port Configuration.

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

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

Status: Provides the current link speed of the port if the port is up, otherwise displays 'down'.



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

Disabled - Disables the switch port operation.

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

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

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

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

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

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

Note: to power cycle an individual switch port, change the Configured Link Speed to Disabled in the drop down menu of the option highlighted below. The port LED will then go out on that port. Changing the Configured Link Speed to Auto or to the required speed will re enable the port.

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 Rx Status column indicates whether pause frames on the port are obeyed, and the Tx Status column indicates whether pause frames on the port are transmitted. The Rx and Tx Status settings are determined by the result of the last Auto-Negotiation.

Check the Flow Control Mode checkbox to use flow control. This setting is related to the setting for Configured Link Speed.

Description: Enter up to 63 characters to be descriptive name for identifies this port. Specify the detail Port alias or description; an alphanumeric string describing the full name and version identification for the system's hardware type, software version, and networking application.

Buttons

Refresh: Click to refresh the Port link Status manually.

Apply: Click to save changes.

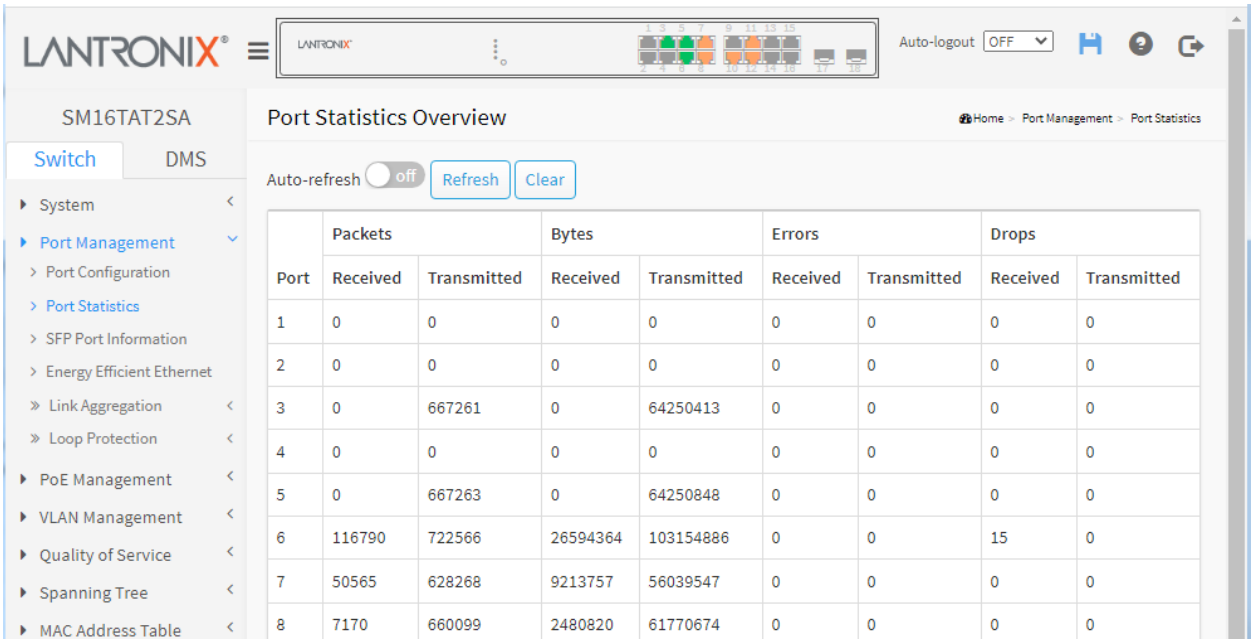
Reset: Click to undo any changes made locally and revert to previously saved values.

4-2 Port Statistics

This page displays Port statistics information and 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 select “Auto-refresh”.
3. Click “ Refresh“ to refresh the port statistics or clear all information when you click “Clear”.
4. To view detailed port statistics, click that port.



Port	Packets		Bytes		Errors		Drops	
	Received	Transmitted	Received	Transmitted	Received	Transmitted	Received	Transmitted
1	0	0	0	0	0	0	0	0
2	0	0	0	0	0	0	0	0
3	0	667261	0	64250413	0	0	0	0
4	0	0	0	0	0	0	0	0
5	0	667263	0	64250848	0	0	0	0
6	116790	722566	26594364	103154886	0	0	15	0
7	50565	628268	9213757	56039547	0	0	0	0
8	7170	660099	2480820	61770674	0	0	0	0

Figure 4-2: Port Statistics Overview page

Parameter descriptions:

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

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

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

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

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

Buttons

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

Refresh: Click to manually refresh the page immediately.

Clear: Clears the counters for all ports.

Detailed Port Statistics: Click a linked port to see its Detailed Port Statistics. 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.

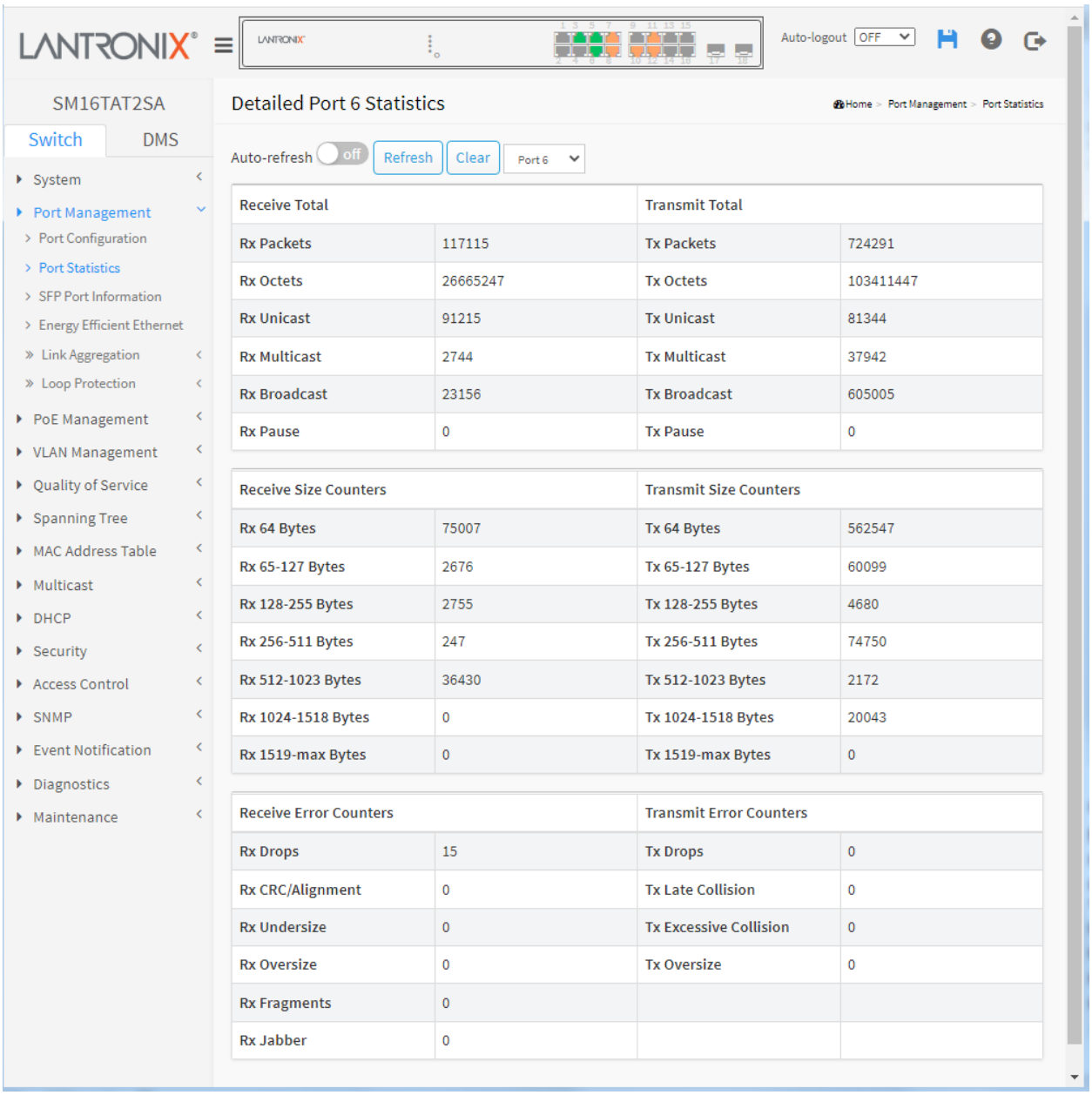


Figure 4-2: Detailed Port Statistics page

Parameter descriptions:

Receive Total and Transmit Total

Rx and Tx Packets: The number of received and transmitted (good and bad) packets.

Rx and Tx Octets: The number of received and transmitted (good and bad) bytes. Includes FCS but excludes framing bits.

Rx and Tx Unicast: The number of received and transmitted (good and bad) unicast packets.

Rx and Tx Multicast: The number of received and transmitted (good and bad) multicast packets.

Rx and Tx Broadcast: The number of received and transmitted (good and bad) broadcast packets.

Rx and Tx Pause: A count of the MAC Control frames received or transmitted on this port that have an opcode indicating a PAUSE operation.

Receive and Transmit Size Counters: The number of received and transmitted (good and bad) packets split into categories based on their respective frame sizes.

Receive Error Counters

Rx Drops: The number of frames dropped due to lack of receive buffers or egress congestion.

Rx CRC/Alignment: The number of frames received with CRC or alignment errors.

Rx Undersize: The number of short 1 frames received with valid CRC.

Rx Oversize: The number of long 2 frames received with valid CRC.

Rx Fragments: The number of short 1 frames received with invalid CRC.

Rx Jabber: The number of long 2 frames received with invalid CRC.

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

Short frames are frames that are smaller than 64 bytes.

Long frames are frames that are longer than the configured maximum frame length for this port.

Transmit Error Counters

Tx Drops: The number of frames dropped due to output buffer congestion.

Tx Late/Exc. Coll.: The number of frames dropped due to excessive or late collisions.

Buttons

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

Refresh: Click to manually refresh the page immediately.

Clear: Clears the counters for the selected port.

4-3 SFP Port Info

This page displays detailed SFP module information when an SFP is connected to the switch. The information includes Connector type, Fiber type, wavelength, bit rate, Vendor OUI, etc.

To display the SFP information in the web UI:

1. Click Port Management and SFP Port Info.
2. Use the port select dropdown to select the desired port.
3. View the displayed SFP Information.

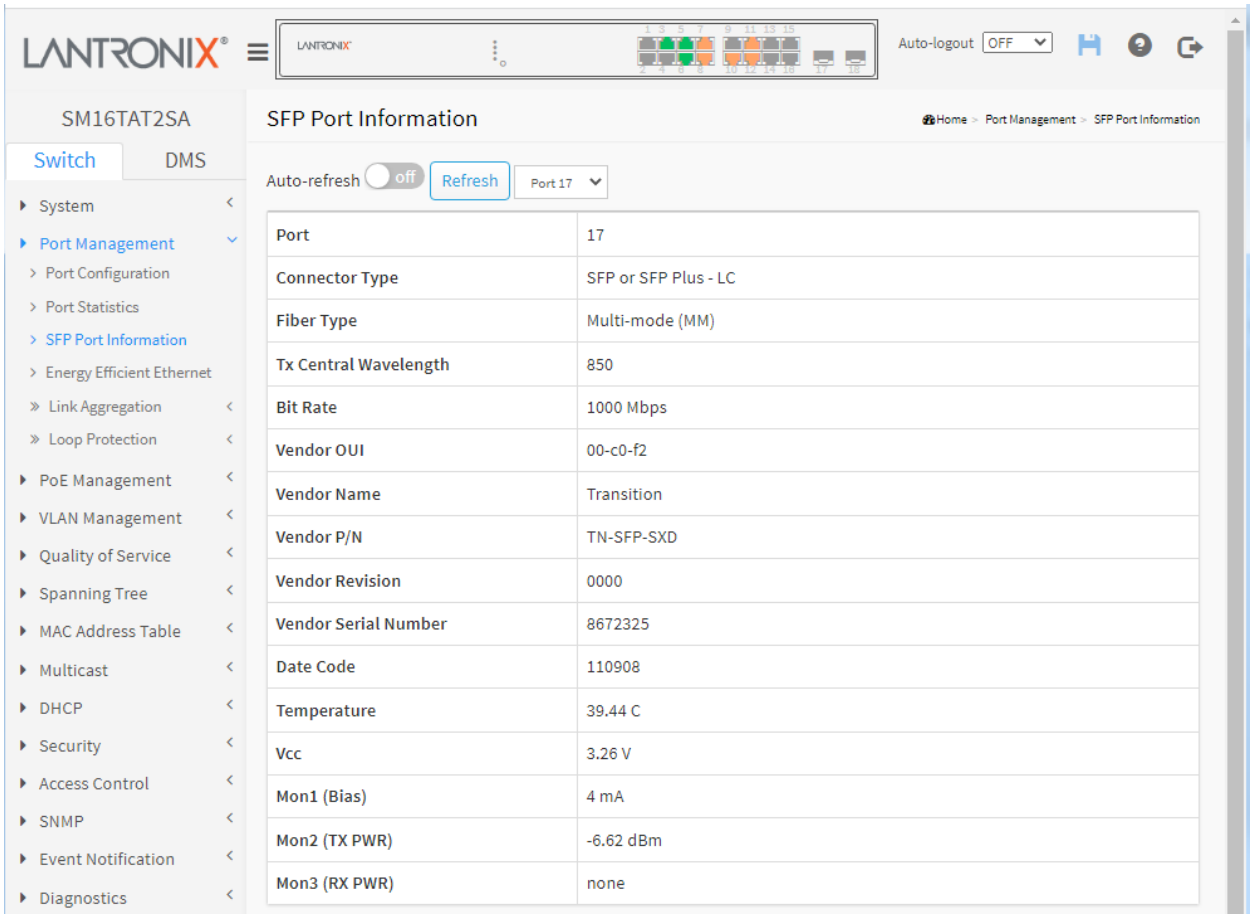


Figure 4-3: SFP Port Information page

Port select: Use the dropdown to select the port to display its Port statistics (e.g., Port 9).

Connector Type: Display the connector type (e.g., SFP, SFP Plus, Reserved - LC, SC, ST, LC, etc.).

Fiber Type: Display the fiber mode, for instance, Multi-Mode (MM) or Single-Mode (SM).

Tx Central Wavelength: Display the fiber optical transmitting central wavelength, for instance, 850nm, 1310nm, 1550nm, etc.

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

Vendor OUI: Displays the Manufacturer's OUI (Organizationally Unique Identifier) 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 naming by module manufacturer.

Vendor Revision: Displays the module revision.

Vendor 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 in milliamps.

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

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

Buttons

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

Refresh: Click to manually refresh the page immediately.

4-4 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 as 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 in order to make sure that both the receiving and transmitting device has all circuits powered up when traffic is transmitted. The devices can exchange 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. For each port select enable or disable Energy Efficient Ethernet.
3. Click the Apply button to save the settings.
4. To cancel the setting click the Reset button to revert to previously saved values.

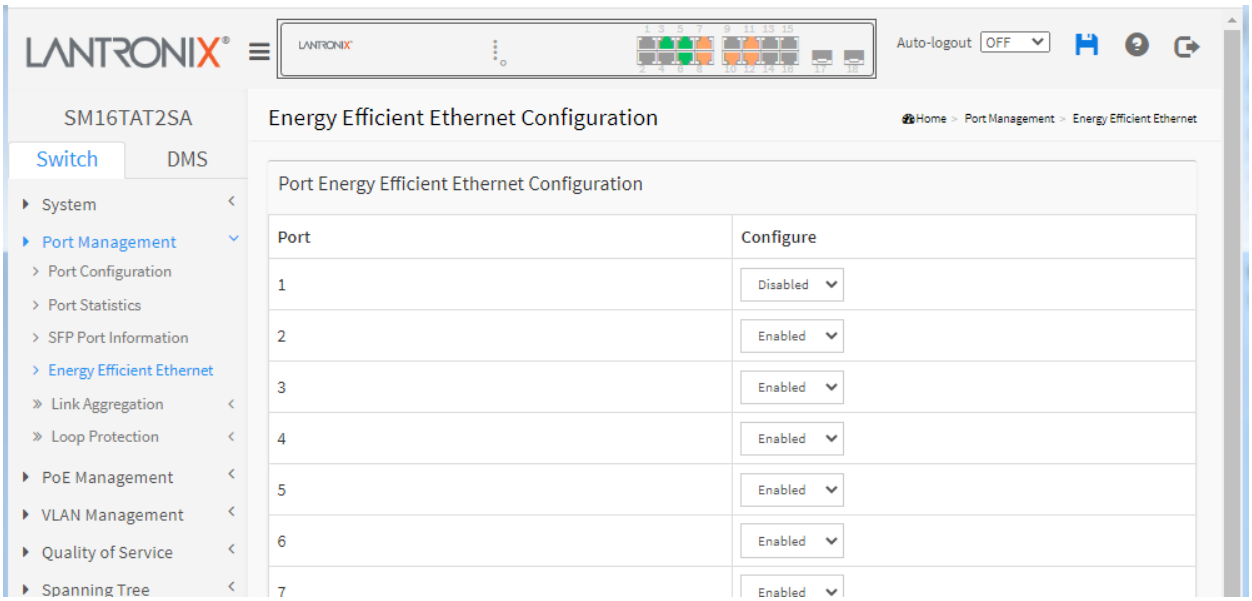


Figure 4-4: Port Energy Efficient Ethernet Configuration

Parameter descriptions:

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

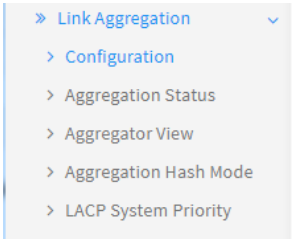
Configure: Controls whether EEE is Enabled or Disabled for each switch port.

Buttons

Apply: Click to save changes.

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

4-5 Link Aggregation



4-5.1 Port

This section describes the Port setting/status used to configure the trunk properties of each port.

To configure the trunk property of each port via the web UI:

1. Click Port Management > Link Aggregation > Port Configuration.
2. Specify the Method, Group, LACP Role and LACP Timeout.
3. Click the Apply button to save the settings.
4. To cancel the setting click the Reset button to revert to previously saved values.

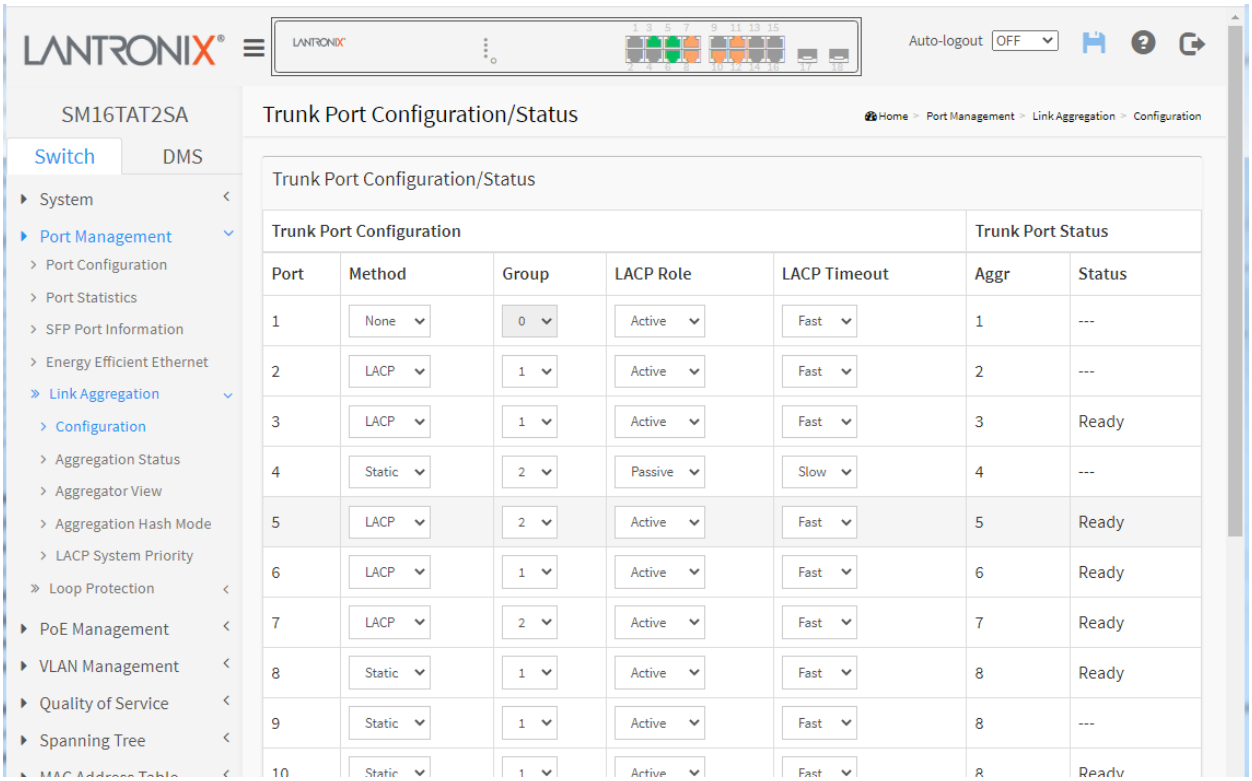


Figure 4-5.1: Trunk Port Configuration/Status page

Port Trunk Configuration:

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

Method: This determines the method a port uses to aggregate with other ports.

None: A port does not want to aggregate with any other port should choose this default setting.

LACP: A port use LACP as its trunk method to get aggregated with other ports also using LACP.

Static: A port use Static Trunk as its trunk method to get aggregated with other ports also using Static Trunk.

Group: Ports choosing the same trunking method other than "None" must be assigned a unique Group number (i.e., Group ID; valid value is 1 - 8) in order to declare that they wish to aggregate with each other.

LACP Role: This field is only referenced when a port's trunking method is LACP.

Active: An Active LACP port begins to send LACPDU to its link partner right after the LACP protocol entity started to take control of this port.

Passive: A Passive LACP port will not actively send LACPDU out before it receives an LACPDU from its link partner.

LACP Timeout: The Timeout controls the period between BPDU transmissions.

Fast: It will transmit LACP packets each second,

Slow: It will wait for 30 seconds before sending a LACP packet.

Trunk Port Status:

Aggr: Abbreviation of "aggregator". Every port is also an aggregator, and its own aggregator ID is the same as its own Port number. We can regard an aggregator as a representative of a trunking group. Ports with the same Group ID and using same trunking method will have the opportunity to aggregate to a particular aggregator port. This aggregator port is usually the port with the smallest Port No. within the trunking Group.

Status: This field represents the trunking status of a port which uses a trunking method other than "None". It also represents the management link status of a port which uses the "None" trunking method. "---" means "not ready"

Buttons

Apply: Click to save changes.

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

4-5.2 Aggregation Status

This page displays the current port trunking information from the aggregator point of status (added at FW v 1.02.1463).

To view LACP aggregation status in the web UI:

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

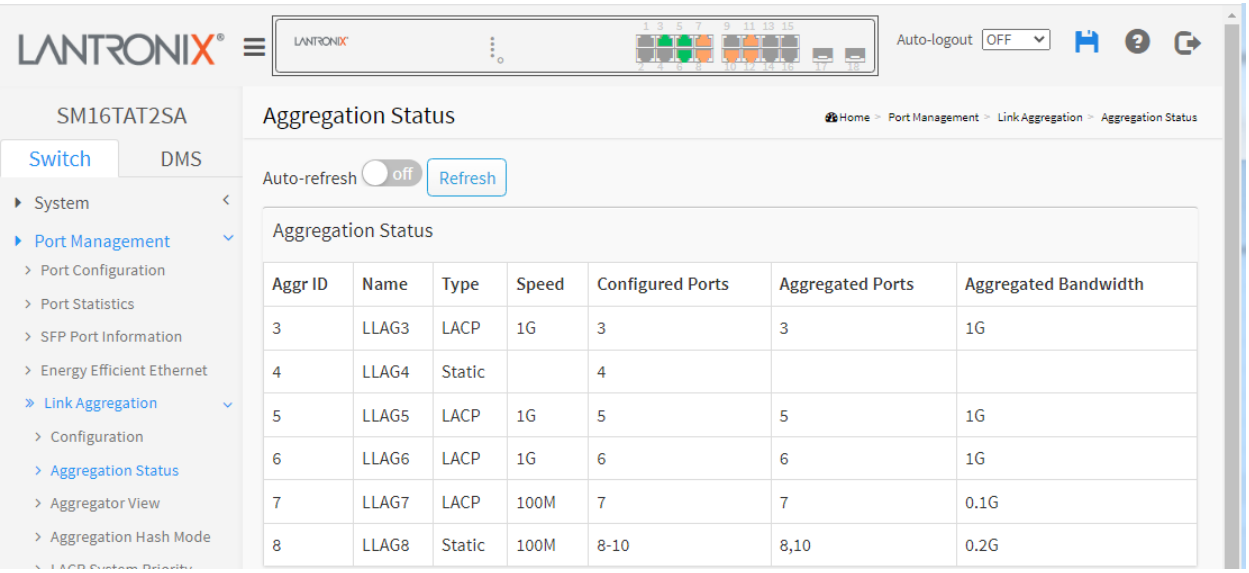


Figure 4-5.2: Port Management > Link Aggregation > Aggregation Status

Parameter descriptions:

Aggr ID: Shows the aggregator ID of aggregator ports.

Name: Show the aggregator Name of aggregator ports.

Type: Show the type a port uses to aggregate with other ports.

Speed: Show the port link speed of aggregator ports.

Configured Ports: Show all config ports of aggregator ports.

Aggregated Ports: Show all aggregated ports of aggregator ports.

Aggregated Bandwidth: Show the ports aggregated link speed bandwidth of aggregator ports.

Buttons

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

Refresh: Click to manually refresh the page immediately.

4-5.3 Aggregator View

This page displays the current port trunking information from the aggregator point of view.

To see the LACP detail in the web UI:

1. Click Port Management, Link Aggregation, and Aggregator View.
2. Click the LACP Detail radio button as required.
3. Click the LACP Detail button.

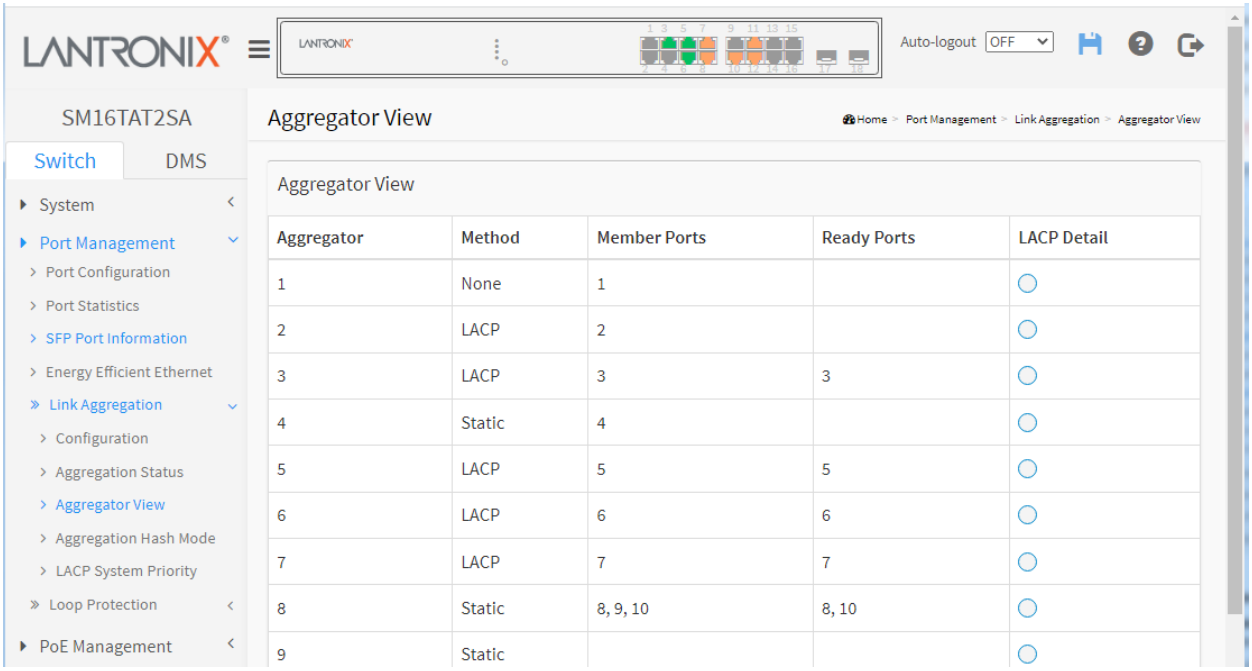


Figure 4-5.3: Aggregator View page

Parameter descriptions:

Aggregator: Shows the aggregator ID of every port. Every port is also an aggregator, and its own aggregator ID is the same as its own Port number.

Method: Show the method a port uses to aggregate with other ports.

Member Ports: Show all member ports of an aggregator (port).

Ready Ports: Show only the ready member ports within an aggregator (port).

LACP Detail: Lets you select the port that you want to see the LACP Detail.

Buttons

LACP Detail: Click this radio button to display the Aggregator Information for the selected Aggregator as described below.

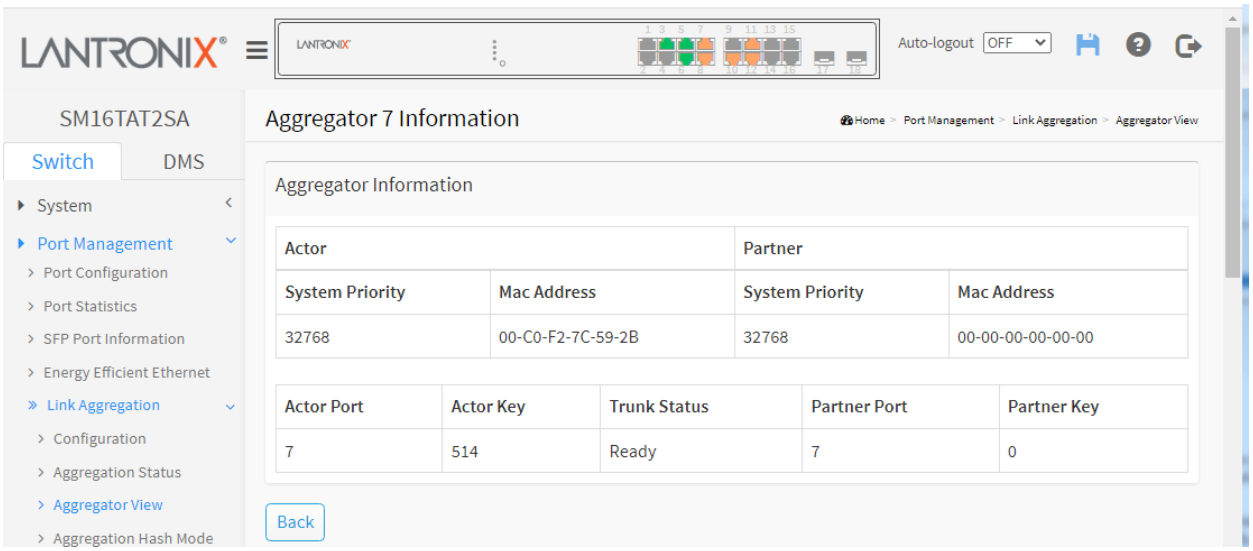


Figure 4-5.4: LACP Detail page

Actor

System Priority: Show the System Priority part of the aggregation Actor. (1-65535).

Mac Address: The system ID of the aggregation Actor.

Actor Port: The actor's port number connected to this port.

Actor Key: The Key that the actor has assigned to this aggregation ID.

Partner

System Priority: Show the System Priority part of the aggregation partner. (1-65535)

Mac Address: The system ID of the aggregation partner.

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

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

Trunk Status: This field represents the trunking status of a port which uses a trunking method other than "None". It also represents the management link status of a port which uses the "None" trunking method. "---" means "not ready".

Button

Back: Click to undo any changes made locally and return to the Aggregator View page.

Messages: *Method must be LACP and Member Ports must have a port at least.*

4-5.4 Aggregation Hash Mode

Aggregation Mode lets you select one of several Hash code contributors to calculate the destination port for the frame.

To configure the Aggregation hash mode in the web UI:

1. Click Port Management, Link Aggregation, and Aggregation Hash Mode.
2. Click Hash Code Contributors to select the mode.
3. Click the **Apply** button to save the settings.
4. To cancel the setting, click the **Reset** button to revert to previously saved values.

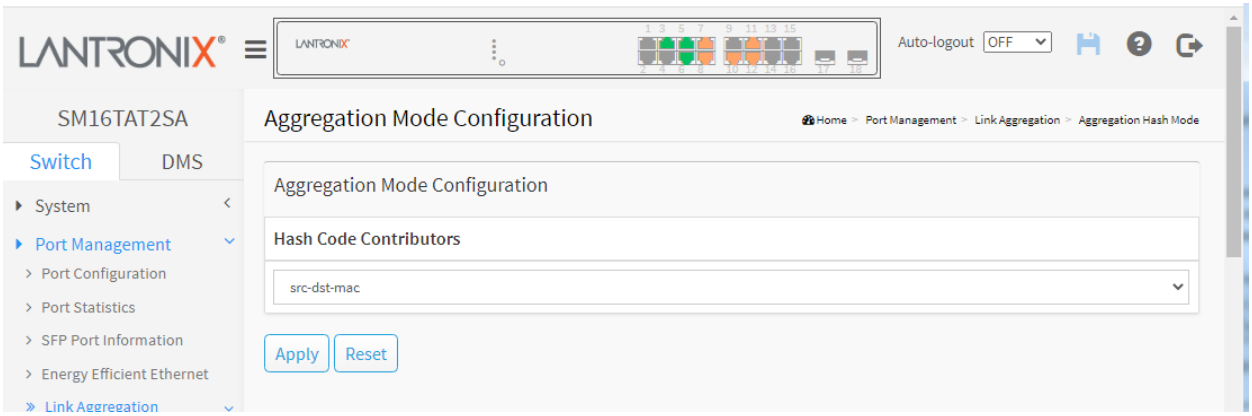
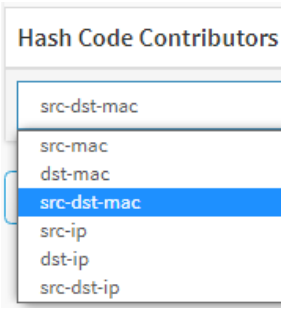


Figure 4-5.5: Aggregation Hash Mode

Hash Code Contributors



src-mac: 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.

dst-mac: 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.

src-dst-mac: Use Source MAC Address + Destination MAC Address.

src-ip: Use Source MAC Address + IP Address.

dst-ip: Use Destination MAC Address + IP Address.

src-dst-ip: Use Source MAC Address + Destination MAC Address + IP Address.

Buttons

Apply : Click to save changes.

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

4-5.5 LACP System Priority

This page lets you set the priority part of the LACP system ID. LACP will only aggregate together the ports whose peer link partners are all on a single system. Each system that supports LACP will be assigned a globally unique System Identifier for this purpose. A system ID is a 64-bit field comprising a 48-bit MAC Address and 16-bit priority value. The System Priority is configurable; its range is 1 - 65535. The default is 32768.

To configure the LACP System Priority in the web UI:

1. Click Port Management, Link Aggregation, and LACP System Priority.
2. Specify the LACP System Priority.
3. Click the **Apply** button to save the settings.
4. To cancel the setting click the **Reset** button to revert to previously saved values.

Figure 4-5.6: LACP System Priority page

Parameter descriptions:

System Priority: Show the System Priority part of a system ID (1-65535).

Buttons

Apply: Click to save changes.

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

4-6 Loop Protection

4-6.1 Configuration

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

To configure Loop Protection parameters in the web UI:

1. Click Port Management, Loop Protection, and Configuration.
2. Select "on" to enable port Loop Protection globally.
3. Click the **Apply** button to save the settings.
4. To cancel the setting, click the **Reset** button to revert to previously saved values

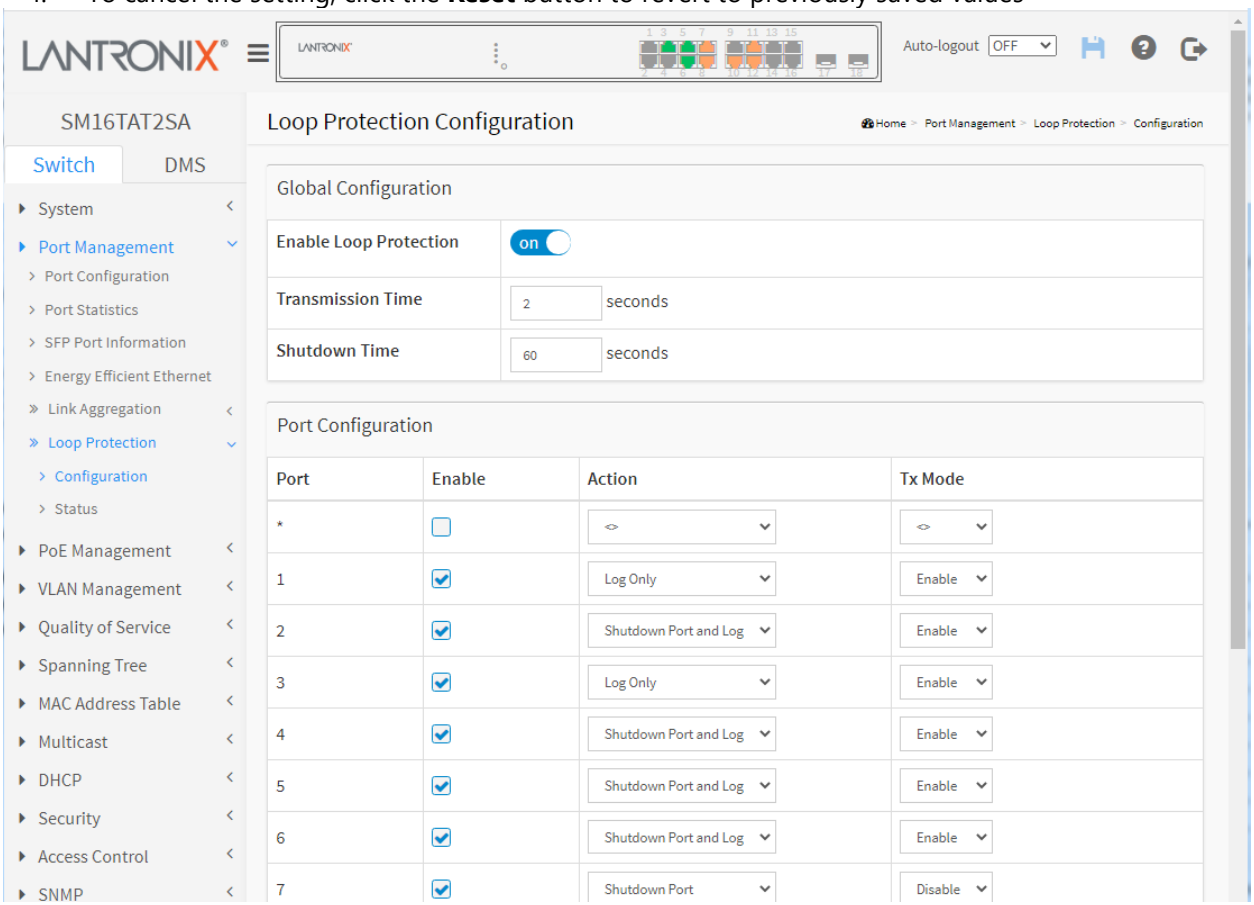


Figure 4-6.1: Loop Protection Configuration page

Global Configuration

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

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

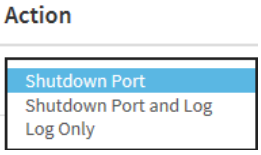
Shutdown Time: The period (in seconds) for which a port will be kept disabled in the event of a loop is detected (and the port action shuts down the port). Valid values are 0 - 604800 seconds (7 days).
A value of zero will keep a port disabled (until next device restart).

Port Configuration

Port: The switch port number of the port.

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

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



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

Buttons

Apply: Click to save changes.

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

4-6.2 Status

This section displays the loop protection port status.

To display Loop Protection status in the web UI:

1. Click Port Management, Loop Protection, and Status.
2. To automatically refresh the information, select "Auto refresh".
3. Click "Refresh" to refresh the Loop Protection Status.

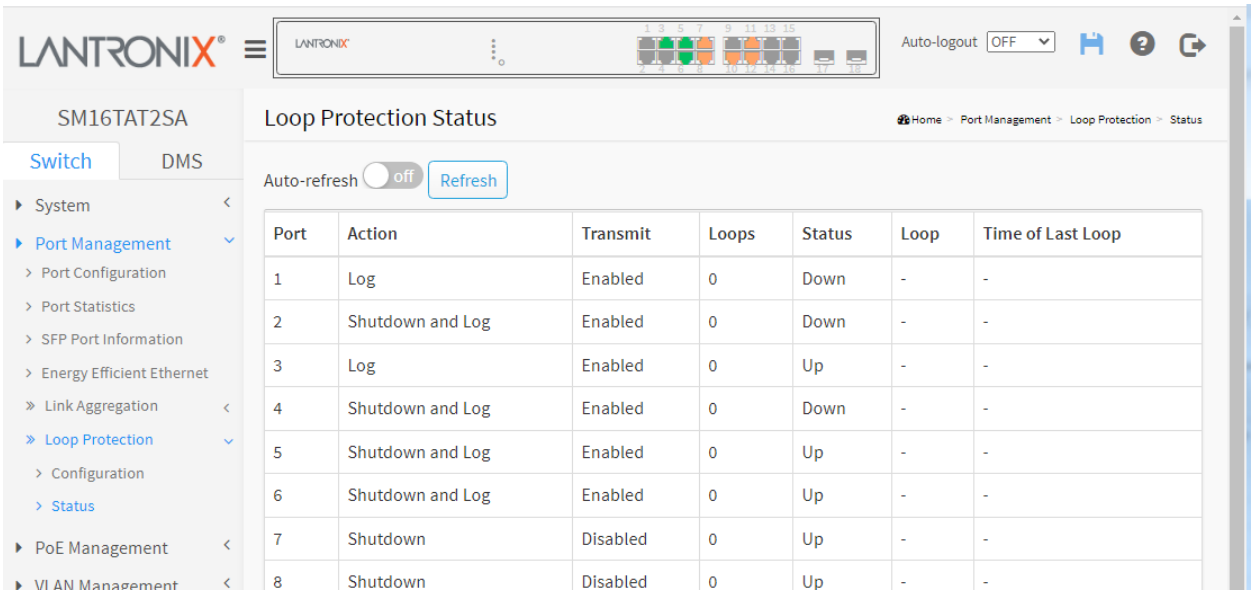


Figure 4-6.2: Loop Protection Status

Parameter descriptions:

Port: The switch port number of the logical port.

Action: The currently configured port action (Shutdown Port, Shutdown Port and Log, or Log Only).

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.

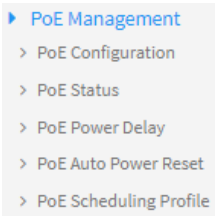
Time of Last Loop: The time of the last loop event detected.

Buttons

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

Refresh: Click to manually refresh the page immediately.

Chapter 5 PoE Management



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

5-1 PoE Configuration

This page lets you view and configure current PoE port settings and show PoE Supply power.

To configure Power over Ethernet in the web UI:

1. Click PoE Management and PoE Configuration.
2. Specify Reserved Power, Capacitor Detection, PoE Mode, PoE Schedule, Priority, and Maximum Power.
3. Click **Apply** to save the configuration.

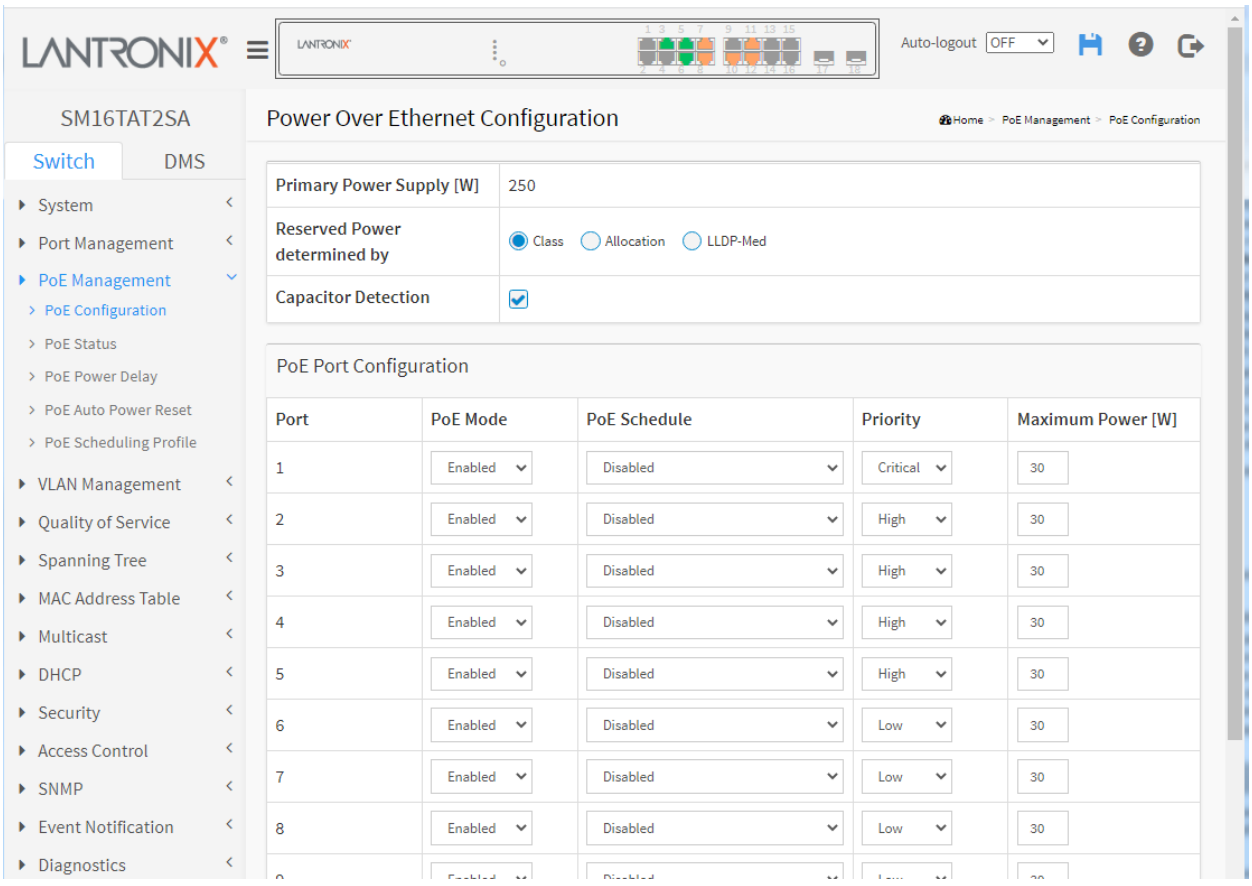


Figure 5-1: PoE Configuration

Parameter descriptions:

Primary Power Supply [W]: Displays the primary power supply power in watts (e.g., 130 Watts).

Reserved Power determined by: Radio button to select one of two modes for configuring how the ports/PDs may reserve power:

Class: The PD will negotiate PD class then feed power if the PD request power complies with the standard. If Maximum Power at the port is configured different then factory default value 30W, the PD connects the port again; the PD cannot draw more power than the new configured Maximum Power for the port. Class mode is the factory default mode. **Note**: Starting at FW v1.01.1195, when the Maximum Power per port value is changed, it will change the mode to Allocation mode. When Class mode is set, PoE allocated value will display after PoE negotiation.

Allocation: The switch will only examine power in the Maximum Power field. So once the switch receives PD request power, the switch will check Maximum Power configuration, and if the configured value is smaller than PD request power, the switch will not feed power.

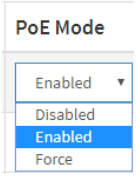
LLDP-Med: This mode is similar to the Class mode except that each port determines the amount power it reserves by exchanging PoE information using the LLDP protocol and reserves power accordingly. If no LLDP information is available for a port, the port will reserve power using the Class mode. In Class mode the Maximum Power fields have no effect for all modes: If a port uses more power than the reserved power for the port, the port is shut down.

Capacitor Detection: Check to enable or uncheck to disable the capacitor configuration. The default is disabled. Check to enable legacy IP phones support.

PoE Port Configuration

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

PoE Mode: The PoE operating mode for the port (Enabled, Disabled, or Force), where:



Disabled: PoE disabled for the port (default).

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

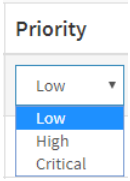
Force: The switch port powers up the linked PD without any detect/negotiate mechanism (PD limited to 30W). **Note**: Only connect PDs which support a power input of 48~56V to prevent damage to PDs. When the port changes to Force mode, the port's PoE LED will light immediately. Select ***Force*** mode for devices that do not do PoE negotiation (e.g., for a PoE DSRC RSU). **Note for first time use**: PoE Force mode is disabled by default, so you must execute the enable CLI command first. Once it's executed, Force mode displays in the Web UI.
The PoE Force mode enable CLI command is shown below:

```
# configure terminal
(config)# Special ip-cam poe-force-mode on
```

Note: Execute the CLI command to enable Force mode; the switch reboots automatically, then Force mode can start working. If you execute this command, the PoE Force mode will always be available. See the *CLI Reference* for more information.

PoE Schedule: Disable PoE Scheduling or select a PoE Schedule profile for each port.

Priority: The Priority represents the ports priority. The three levels of power priority are ***Low***, ***High*** and ***Critical***. The priority is used in the case where the remote devices require more power than the power supply can deliver. In this case the port with the lowest priority will be turned off first starting from the port with the highest port number. If both power supplies are in use and are required to provide enough power for the PoE connections that are in use, if one of the power supplies fails and there is not enough power to support all of the PoE ports that are in use, then PoE power will be fed to PoE ports with higher priority. If the ports have the same priority, the lower port number will be fed PoE power.



Maximum Power [W]: Indicates the maximum power in watts that can be delivered to a remote device. The valid range is 1-30 Watts. The default is 30 Watts.

Buttons

Apply: Click to save changes.

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

Messages

Message: *PoE Mode(Force): The switch port will power up the linked PD without any detect/negotiate mechanism(PD limited to 30W). Do you want to change this setting?*

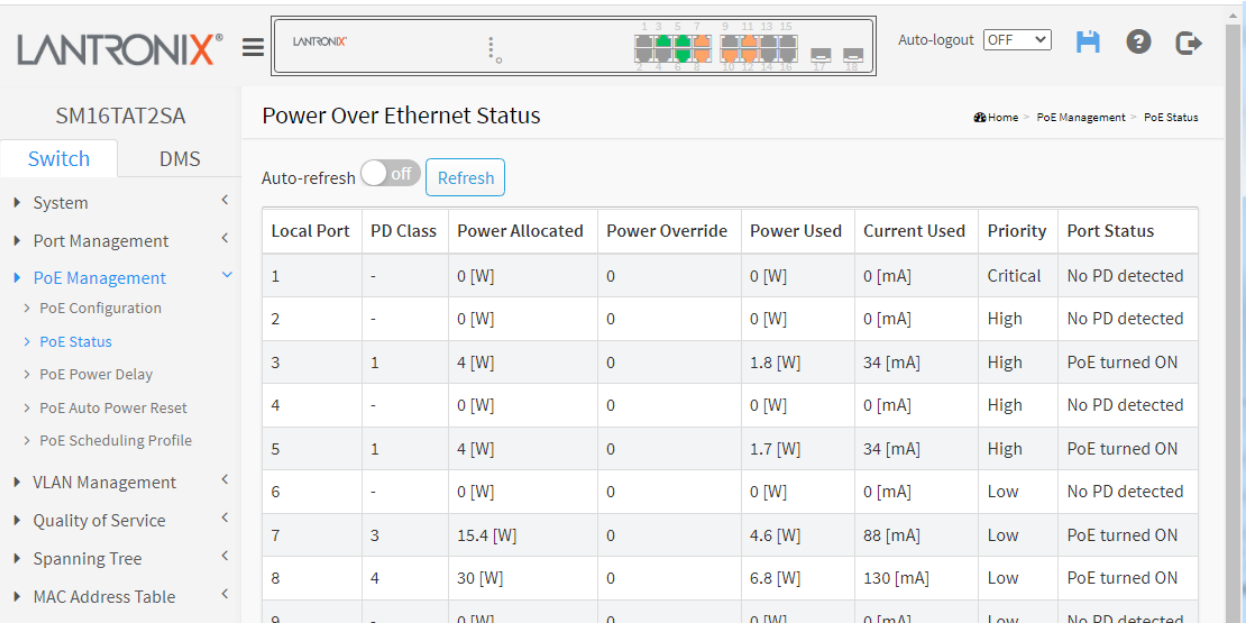
Meaning: Confirmation message ensuring that you want to make this config change.

Action: Click the **OK** button only if you are sure you want to change this setting. See the "PoE Mode" parameter description above. If you are not sure you want to change this setting, click the **Cancel** button. Added at FW v 1.01.1209.

5-2 PoE Status

This page displays the current status of all local 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 the Refresh button to refresh the page.



Local Port	PD Class	Power Allocated	Power Override	Power Used	Current Used	Priority	Port Status
1	-	0 [W]	0	0 [W]	0 [mA]	Critical	No PD detected
2	-	0 [W]	0	0 [W]	0 [mA]	High	No PD detected
3	1	4 [W]	0	1.8 [W]	34 [mA]	High	PoE turned ON
4	-	0 [W]	0	0 [W]	0 [mA]	High	No PD detected
5	1	4 [W]	0	1.7 [W]	34 [mA]	High	PoE turned ON
6	-	0 [W]	0	0 [W]	0 [mA]	Low	No PD detected
7	3	15.4 [W]	0	4.6 [W]	88 [mA]	Low	PoE turned ON
8	4	30 [W]	0	6.8 [W]	130 [mA]	Low	PoE turned ON

Figure 5-2: Power Over Ethernet Status

Parameter descriptions:

Local Port: The logical port number for this row.

PD Class: Each PD is classified according to a class that defines the maximum power the PD will use. PD Class will show by learning from the link partner no matter which "Reserved Power determined by" mode is set. If Maximum Power at the port is configured different than the factory default value of 30W, PD class still stays at the previous learned Class.

The PD Class field shows the PDs classes 0-4 where:

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 Allocated: Shows the amount of power the switch has allocated for the PD. Power gets updated to power negotiation by Class, the value assigned and displayed is forced. When Power override =1, the value is the same as the value of "Maximum Power (W)". The Switch provides power to the PD if the power required by the PD is less than this value.

Power Override: Displays **0** (override disabled) or **1** (override the default power requirement specified by the IEEE classification). The difference between the power requirement mandated by the IEEE classification and what is actually needed by the PD is returned into the global power budget for use by additional PDs. This lets you extend the switch power budget and use it more effectively. So, if you have devices that use less power than the default that will be assigned based on class, by overriding a lower value you avoid maxing out the calculated total allocation for the switch. Added at FW v 1.01.1171. When "Power Allocated" configuration value is different from the default value, displays **1**. Otherwise displays **0**.

Power Override Indicates whether the maximum power at the port has ever changed. If Maximum Power at the port is configured different than the factory default value of 30W, it displays "**1**".

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

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

Priority: The Priority shows the port's priority currently configured (e.g., ***Critical***, ***High***, or ***Low***).

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

Voltage injection: current was returned; that would affect one device at an adjacent port and cannot completely power on.

PoE turned ON : PoE power is turned on and available.

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. A port's PoE can be revoked for one of two reasons: **1**) Port power budget exceeded, or **2**) Total power budget exceeded.

No PD detected: No Powered Device 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.

PD overloaded: The PD consumed more power than the maximum limit configured for the port, based on the default, user, or CDP configuration.

Total: A combined total is displayed for each column.

Balance PoE Power Available: Displays the remaining power that can be used (Total power of switch) – (Sum of power allocated of all ports) in Watts. Added at FW v1.01.1195.

Buttons

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

Refresh: Click to manually refresh the page immediately.

Five PD Classes are defined by the IEEE standards:

Class	Usage	Classification Current [mA]	Power Range [W]	Class Description
0	Default	0–4	0.44–12.94	Classification unimplemented
1	Optional	9–12	0.44–3.84	Very Low power
2	Optional	17–20	3.84–6.49	Low power
3	Optional	26–30	6.49–12.95	Mid power
4	Valid for 802.3at (Type 2) devices, not allowed for 802.3af devices	36–44	12.95–25.50	High power

5-3 PoE Power Delay

This page lets you specify the delay time before power is provided to a port after device rebooted.

To configure Power over Ethernet Power Delay in the web interface:

1. Click PoE Management and PoE Power Delay.
2. Enable or Disable Delay Mode.
3. Specify the Delay Time.
4. Click **Apply** to apply the change.

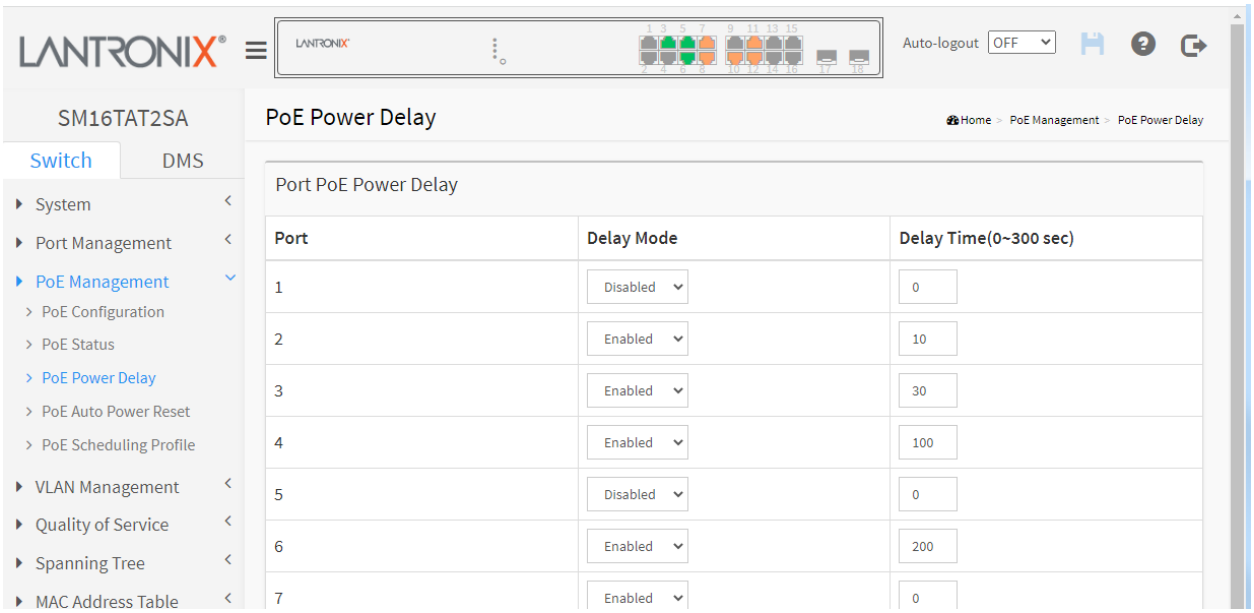


Figure 5-3: PoE Power Delay

Parameter descriptions:

Port: The port being configured; each port instance is represented by a line in the table.

Delay Mode: At the dropdown, select Enabled. The default is Disabled.

Delay Time(0~300 sec): Enter the amount of delay time (0~300 seconds). The default is 0 seconds. If Port 1 PoE Power Delay time setting is 30 seconds, it means the switch will wait 30 seconds to provide power to port 1 after the switch reboots.

Buttons

Apply : Click to save changes.

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

5-4 PoE Auto Power Reset

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

To configure Power over Ethernet Auto Power Reset in the web interface:

1. Click PoE Management and PoE Auto Power Reset.
2. Enable the Ping Check function.
4. Specify the PD's IP address, startup time, interval time, retry time, failure action, reboot time, and max reboot times.
5. Click **Apply** to apply the change.

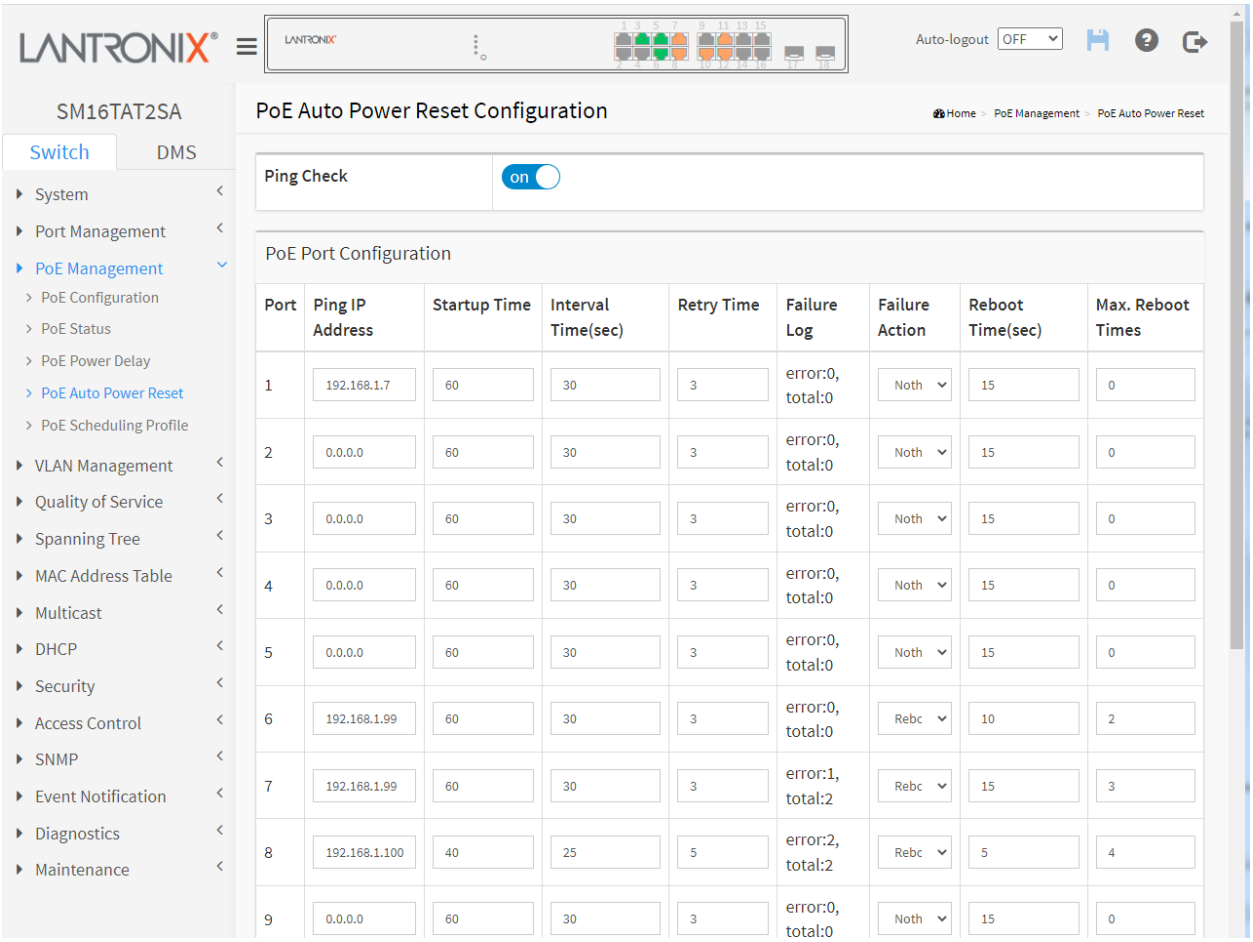


Figure 5-4: PoE Auto Power Reset Configuration

Parameter descriptions:

Ping Check: Turn the Ping Check function ***on*** to detect the connection between PoE port and powered devices (PDs). The default is ***off*** (Ping Check disabled).

Port: 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. Default: 30; range: 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 try to send detection again. When ping fails the third time, it will trigger the configured Failure Action. The default is 3 reties; the valid range is 1-5 retries.

Failure Log: Failure loggings counter.

Failure Action: The action when the third fail detection.

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

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

Reboot time(sec): When PD has been 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 the number of reboots exceeds this setting, auto checking will stop on this port until you change PoE mode without disabling in PoE configuration. The switch will issue an SNMP Trap and Log to notify this remote PD no response. If Max Reboot Times is 0, auto checking will not stop. The default is 0 reboots; the valid range is 0-10 reboots.

Buttons

Apply : Click to save changes.

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

PoE Auto Checking "AutoFill" Feature

When you enable Auto Power Reset (PoE Auto Checking) in DMS) the IP addresses of the connected devices are automatically filled in the Auto Power Reset configuration page.

1. Configure the "PoE Auto Checking" parameter at Switch > PoE Management > PoE Auto Power Reset. The default value of the "Failure Action" parameter is "Nothing".

2. Configure PoE parameters at DMS > Graphical Monitoring > Topology View. Left click on the switch icon

to display its device configuration popup. Click the PoE Config (

) icon to display the PoE Auto Checking pane.

5-5 PoE Scheduling Profile

This page lets you define profiles for PoE scheduling.

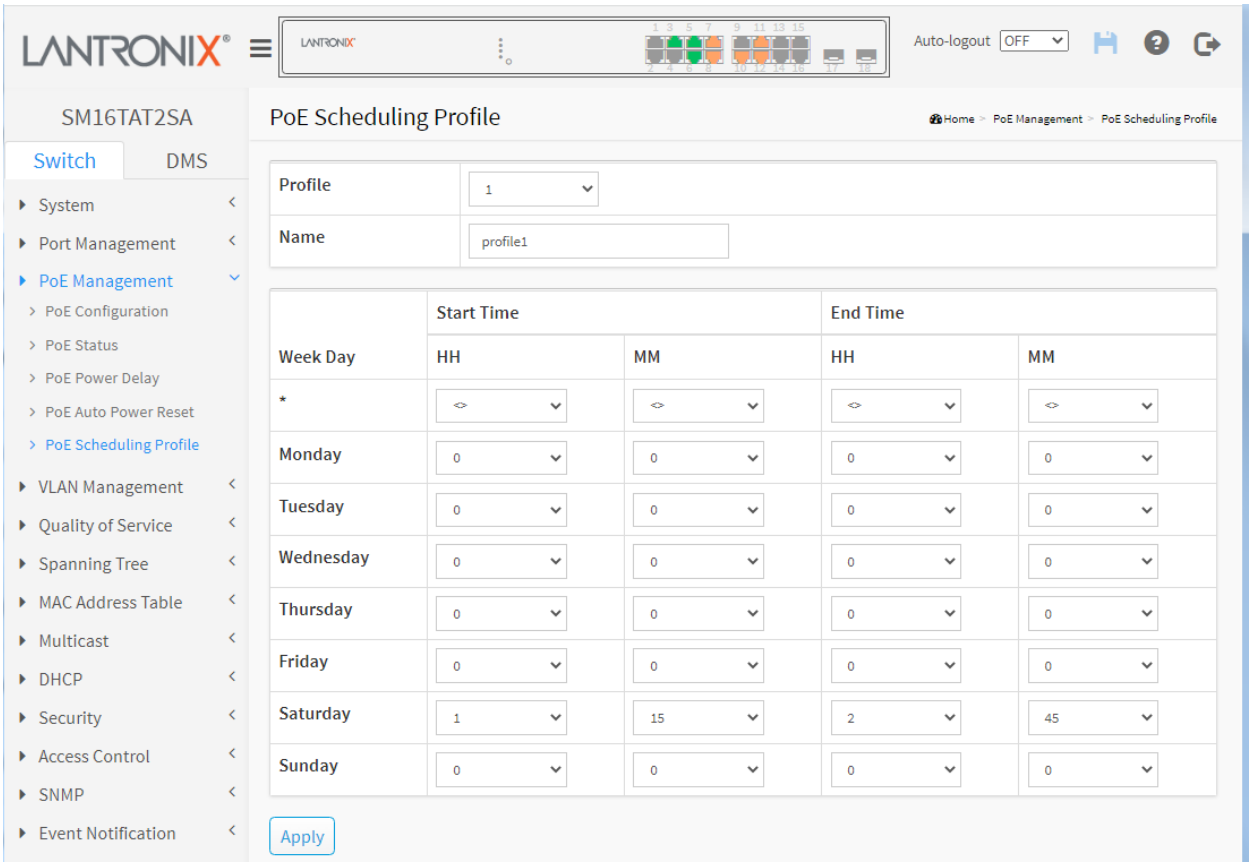


Figure 5-5: PoE Scheduling Profile

Parameters:

Profile: The index of profile. You can configure up to 16 profiles.

Name: The name of profile. The default name is "profile 1". You can define the name for identifying the profile.

Week Day: The day to schedule PoE.

Start Time: The hour (HH) and minute (MM) to start PoE. The time 00:00 means the first second of this day.

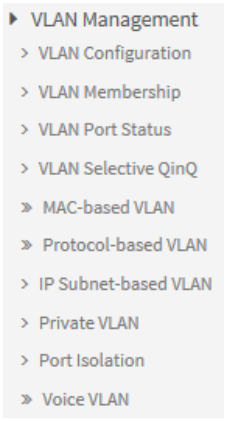
End Time: The hour (HH) and minute (MM) to stop PoE. The time 00:00 means the last second of this day.

Buttons

Apply: Click to save changes.

Messages: *End time should not be earlier than start time*

Chapter 6 VLAN Management



6-1 VLAN Configuration

This page lets you 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 membership in the web UI:

1. Click VLAN Management and VLAN Configuration.
2. Configure for existing VLANs, Ethertype, port types, ingress/egress, and allowed VLANs.
3. Click the **Apply** button.

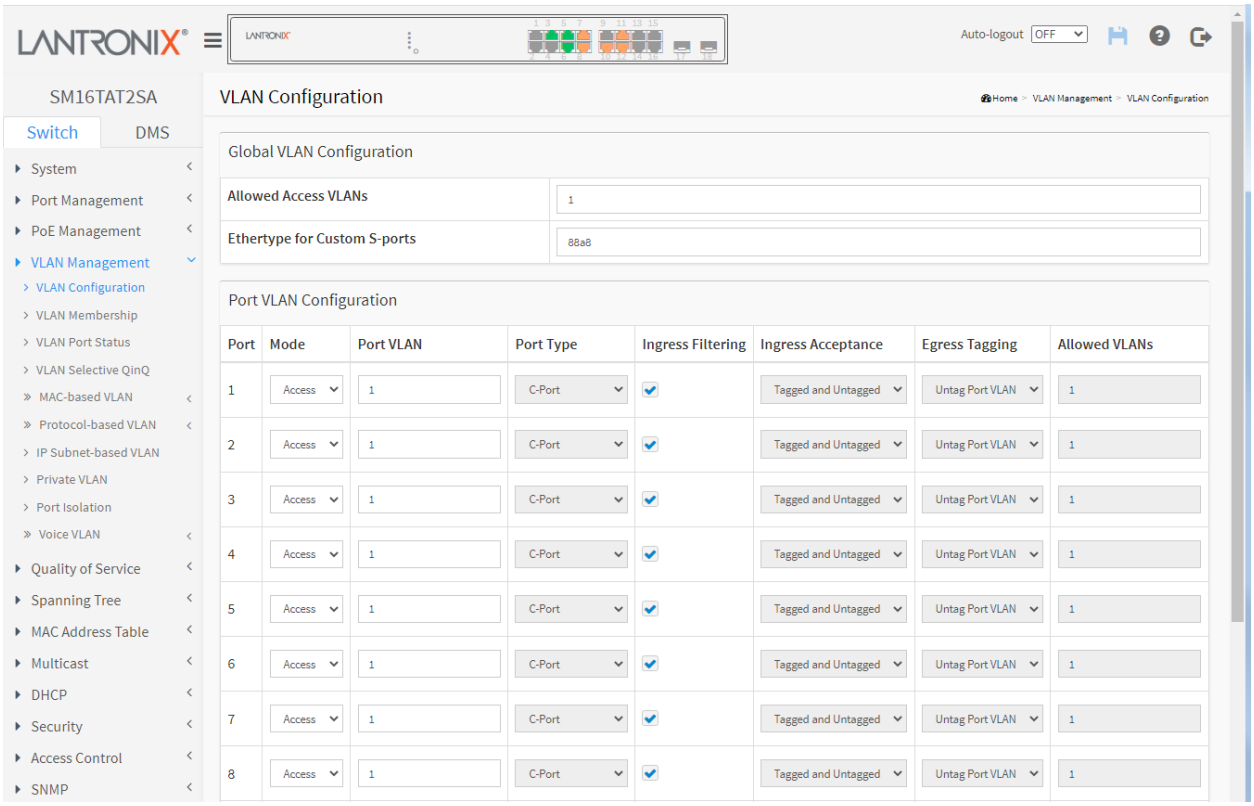


Figure 6-1: VLAN Configuration page

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 between 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 these characteristics:

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

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

- By default, a trunk port is member of all existing VLANs. This may be limited by the use of Allowed VLANs,
- unless VLAN Trunking is enabled on the port, frames classified to a VLAN that the port is not a member of will be discarded,
- by default, all frames but frames classified to the Port VLAN (a.k.a. Native VLAN) get tagged on egress. Frames classified to the Port VLAN do not get C-tagged on egress,
- egress tagging can be changed to tag all frames, in which case only tagged frames are accepted on ingress,
- VLAN trunking may be enabled.

Hybrid: Hybrid ports resemble trunk ports in many ways but 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 through 4095; the default is 1.
On ingress, frames get classified to the Port VLAN if the port is configured as VLAN unaware, the frame is untagged, or VLAN awareness is enabled on the port, but the frame is priority tagged (VLAN ID = 0).
On egress, frames classified to the Port VLAN do not get tagged if Egress Tagging configuration is set to untag Port VLAN.
The Port VLAN is called an "Access VLAN" for ports in Access mode and “Native VLAN” for ports in Trunk or Hybrid mode.

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

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

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

S-Port: On ingress, frames with a VLAN tag with TPID = 0x8100 or 0x88A8 get classified to the VLAN ID embedded in the tag. If a frame is untagged or priority tagged, the frame gets classified to the Port VLAN. If frames must be tagged on egress, they will be tagged with an S-tag.

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

Ingress Filtering: Hybrid ports allow for changing ingress filtering. Access and Trunk ports always have ingress filtering enabled.

If ingress filtering is ***enabled*** (checkbox is checked), frames classified to a VLAN that the port is not a member of get discarded.

If ingress filtering is ***disabled***, frames classified to a VLAN that the port is not a member of are accepted and forwarded to the switch engine. However, the port will never transmit frames classified to VLANs that it is not a member of.

VLAN Trunking: Trunk and Hybrid ports allow for enabling VLAN trunking. When VLAN trunking is enabled, frames classified to unknown VLANs are accepted on the port whether ingress filtering is enabled. This is useful in scenarios where a cloud of intermediary switches must bridge VLANs that haven't been created. By configuring the ports that connect the cloud of switches as trunking ports, they can seamlessly carry those VLANs from one end to the other.

Ingress Acceptance: Hybrid ports allow for changing the type of frames that are accepted on ingress.

Tagged and untagged: both tagged and untagged frames are accepted.

Tagged Only: Only tagged frames are accepted on ingress. Untagged frames are discarded.

Untagged Only: Only untagged frames are accepted on ingress. Tagged frames are discarded.

Egress Tagging: Ports in Trunk and Hybrid mode may control the tagging of frames on egress.

Untag Port VLAN: Frames classified to the Port VLAN are transmitted untagged. Other frames are transmitted with the relevant tag.

Tag All: All frames, whether classified to the Port VLAN or not, are transmitted with a tag.

Untag All: All frames, whether classified to the Port VLAN or not, are transmitted without a tag. This option is only available for ports in Hybrid mode.

Allowed VLANs: Ports in Trunk and Hybrid mode may control which VLANs they are allowed to become members of. Access ports can only be member of one VLAN, the Access VLAN. The field's syntax is identical to the syntax used in the Existing VLANs field. By default, a port may become member of all possible VLANs, and is therefore set to 1-4095. The field may be left empty, which means that the port will not be member of any of the existing VLANs, but if it is configured for VLAN Trunking it will still be able to carry all unknown VLANs.

Buttons

Apply: Click to save changes.

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

6-2 VLAN Membership

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

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 the services of the VLAN management function to configure VLAN memberships and VLAN port configurations such as PVID and UVID.

Web Interface

To configure VLAN membership in the web UI:

1. Click VLAN Management and VLAN Membership.
2. At the dropdown select which VLANs to be displayed.
3. Click Refresh to update the state.

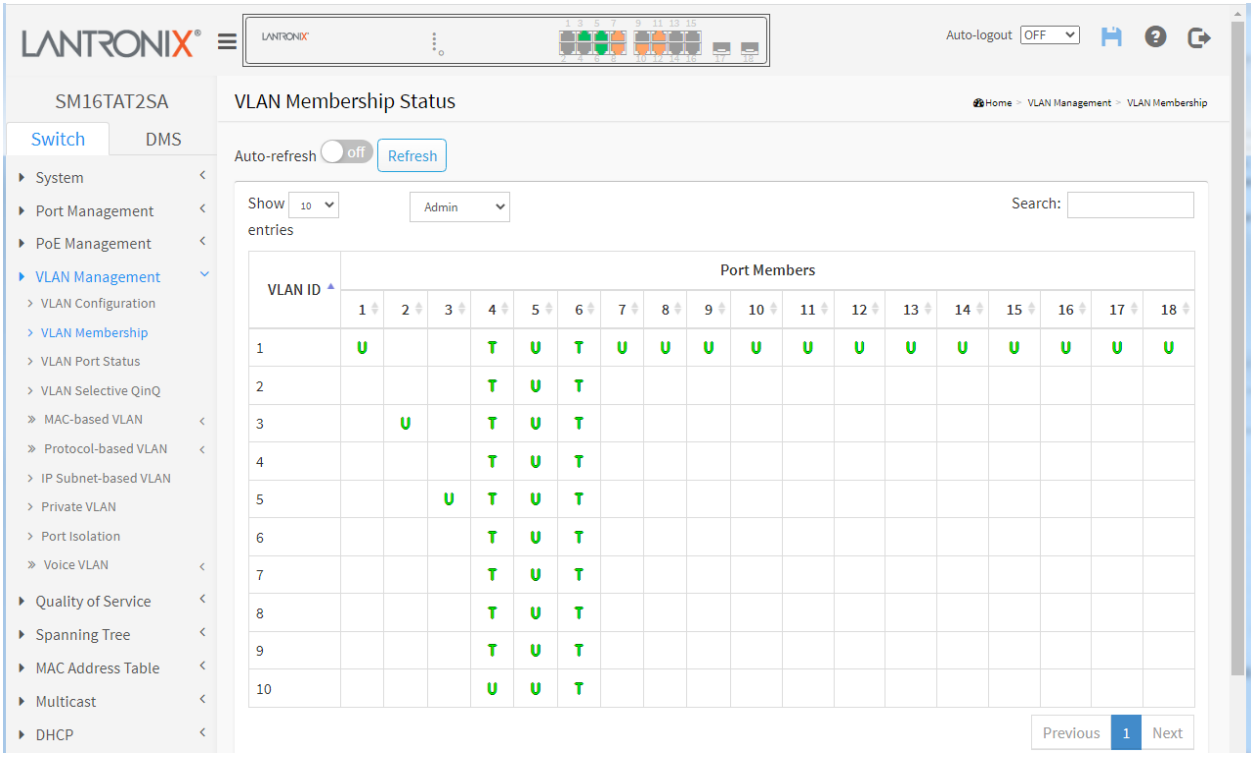


Figure 6-2: VLAN Membership Status

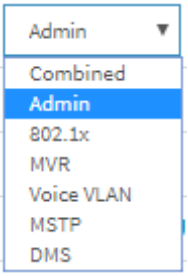
Show entries: At the dropdown you can choose how many items you want to display (10, 25, 60, or All).

VLAN USER: The VLAN User module uses the services of the VLAN management function to configure VLAN memberships and VLAN port configurations such as PVID and UVID. These VLAN user types are currently supported: Combined, Admin, 802.1x, MVR, Voice VLAN, MSTP and DMS.

The VLAN Membership Status Page shows the current VLAN port members for all VLANs configured by a selected VLAN User by using the combo box. When ALL VLAN Users are selected, it shows this information for all the VLAN Users, and this is by default. VLAN membership allows the frames classified to the VLAN ID to be forwarded on the respective VLAN member ports.

Combined: A combination of all VLAN User types.

Admin: Shows VLAN memberships configured by an administrator.



802.1x: Provides port-based authentication, which involves communications between a Supplicant, Authenticator, and an Authentication Server.

***MVR*:** Multicast VLAN Registration **(**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.

VLAN ID: VLAN ID for which the Port members are displayed.

Port Members

A row ~~of check boxes~~ for each port is displayed for each VLAN ID. If a port is included in a VLAN, an image indicating tagged (T) or untagged (U) will display. Shows egress filtering frame status whether tagged or untagged. Frames classified to the Port VLAN are transmitted tagged or untagged.

Show entries: At the dropdown choose how many items you want to view per page (10, 25, 60, or ALL).

Search: Enter text to search for the information that you want to view.

Buttons

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

Refresh: Click to manually 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.

Messages:

ERROR: Invalid allowed VLAN list (1.30)

6-3 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, and VCL.

To display VLAN Port Status in the web UI:

1. Click VLAN Management and VLAN Port Status.
2. At the dropdown, specify the user type.
3. Click Refresh to display the current Port Status information.

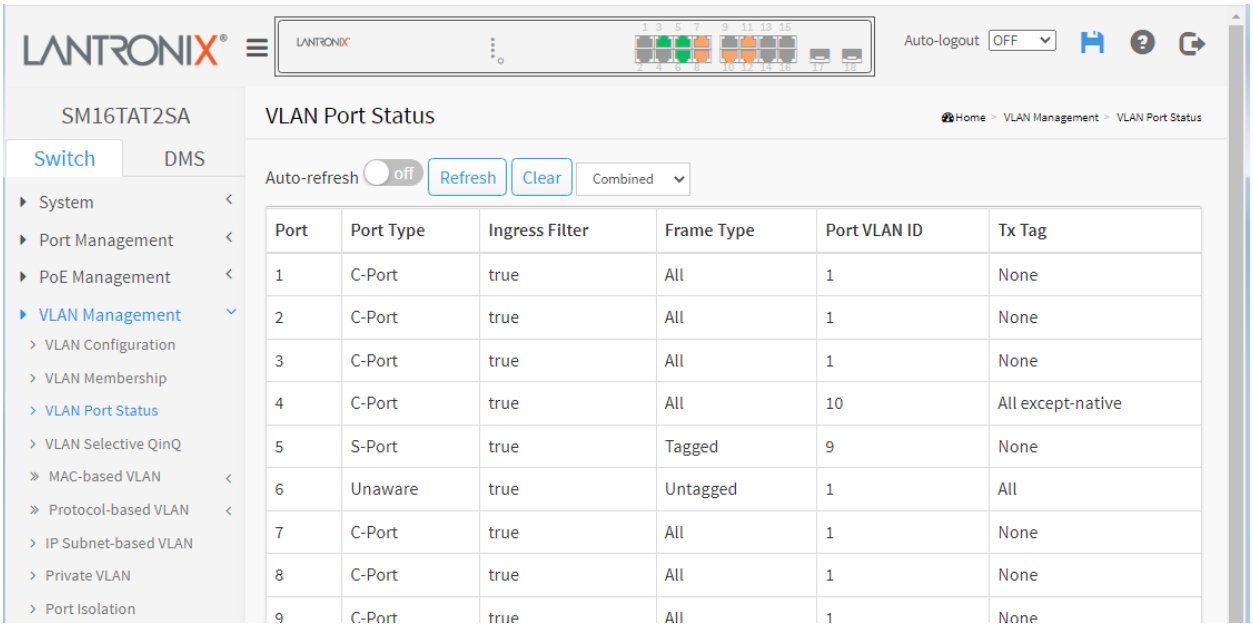
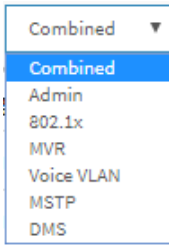


Figure 6-3: VLAN Port Status page



VLAN USER: Various internal software modules may use VLAN services to configure VLAN memberships on the fly. The drop-down list on the right allows for selecting between showing VLAN memberships as configured by an administrator (Admin) or as configured by one of these internal software modules. These VLAN User types are currently supported:

Combined: A combination of the administrator and internal software modules configuration, and basically reflects what is actually configured in hardware.

Admin: VLAN memberships as configured by an administrator.

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

GVRP: GVRP (GARP VLAN Registration Protocol or Generic VLAN Registration Protocol) facilitates control of VLANs within a larger network. GVRP conforms to the IEEE 802.1Q specification, which defines a method of tagging frames with VLAN configuration data.

MVR: Multicast VLAN Registration **(**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: Lantronix' DMS (Device Management System) is an intelligent management tool embedded in the switch to intuitively help reduce support time, cost, and effort.

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

Port Type: Shows the Port Type, which 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 Custom TPID.

Ingress Filter: Shows the ingress filtering on a port. This parameter affects VLAN ingress processing. If ingress filtering is ***true*** (enabled) and the ingress port is not a member of the classified VLAN, then the frame is discarded.

Frame Type: Shows whether the port accepts all frames or only tagged frames or all. This parameter affects VLAN ingress processing. If the port only accepts tagged frames, then 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 ***None***, ***All***, or ***All except-native***.

Buttons

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

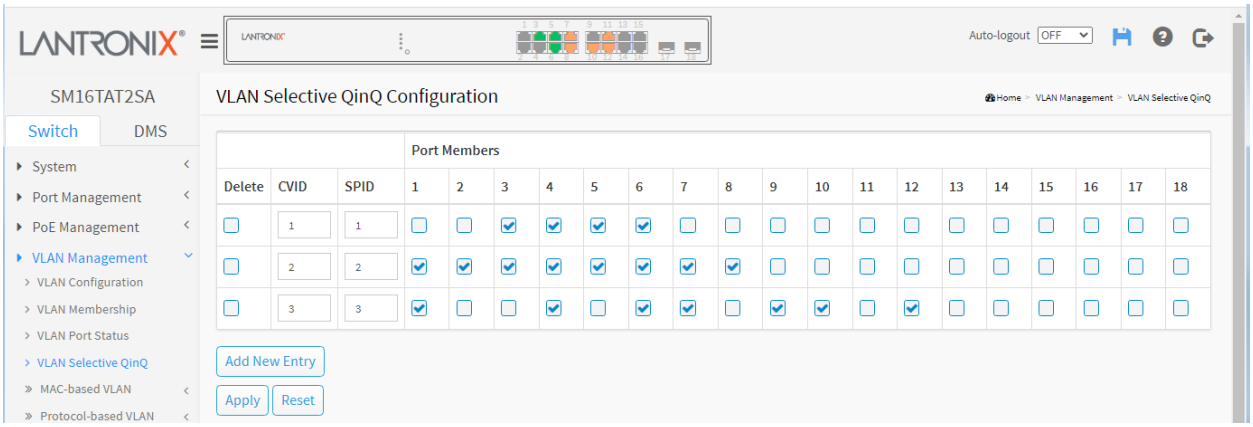
Refresh: Click to manually refresh the page immediately.

Clear: Click to clear the page.

6-4 VLAN Selective QinQ

A Q-in-Q VLAN tunnel enables a service provider to segregate the traffic of different customers in their infrastructure, while still giving the customer a full range of VLANs for their internal use by adding a second 802.1Q tag to an already tagged frame.

Navigate to Switch > VLAN Management > VLAN Selective QinQ to create new and edit existing entries.



Parameter descriptions:

Delete: To delete a private VLAN entry, check this box. The entry will be deleted during the next apply.

CVID: 1-4095; the Customer VLAN ID List to which the tagged packets will be added.

SPID: 1-4095; this configures the VLAN to join the Service Provider's VLAN as a tagged member.

Port Members: Checkmarks indicate which ports are members of the entry. Check or uncheck as needed to modify the entry.

Buttons

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

Add New Entry: Click the button to add a new instance. An empty row is added to the table, and the new member can be configured as needed. Initially displays "*Table is Empty*".

Apply: Click to save changes.

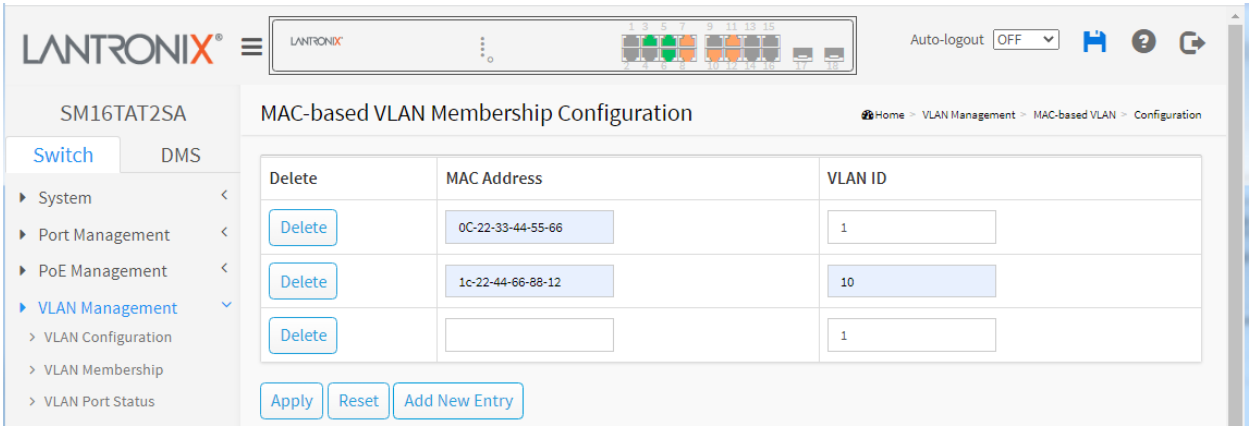
Reset: Click to undo any changes made locally and revert to previously saved values.

6-5 MAC-based VLAN

This page lets you view and configure MAC-based VLAN Memberships. Navigate to Switch > VLAN Management > MAC-based VLAN > Configuration to configure new entries and view the status of existing entries.

MAC address-based VLAN decides the VLAN for forwarding an untagged frame based on the source MAC address of the frame. A most common way of grouping VLAN members is by port, hence the name port-based VLAN. Typically, the device adds the same VLAN tag to untagged packets that are received through the same port. Later, these packets can be forwarded in the same VLAN. Port-based VLAN is easy to configure and applies to networks where the locations of terminal devices are relatively fixed. As mobile office and wireless network access gain more popularity, the ports that terminal devices use to access the networks are very often non-fixed. A device may access a network through Port A this time, but through Port B the next time. If Port A and Port B belong to different VLANs, the device will be assigned to a different VLAN the next time it accesses the network. As a result, it will not be able to use the resources in the old VLAN. On the other hand, if Port A and Port B belong to the same VLAN, after terminal devices access the network through Port B, they will have access to the same resources as those accessing the network through Port A do, which brings security issues. To provide user access and ensure data security in the meantime, the MAC-based VLAN technology is developed. MAC-based VLANs group VLAN members by MAC address. With MAC-based VLAN configured, the device adds a VLAN tag to an untagged frame according to its source MAC address. MAC-based VLANs are mostly used in conjunction with security technologies such as 802.1X to provide secure, flexible network access for terminal devices.

6-5.1 Configuration



Delete: To delete a private VLAN entry, check this box. The entry will be deleted during the next apply.

MAC Address: Enter the MAC address for the entry. Must be a valid unicast MAC address.

VLAN ID: Enter the VLAN ID (VID) for the entry (1-4095).

Buttons

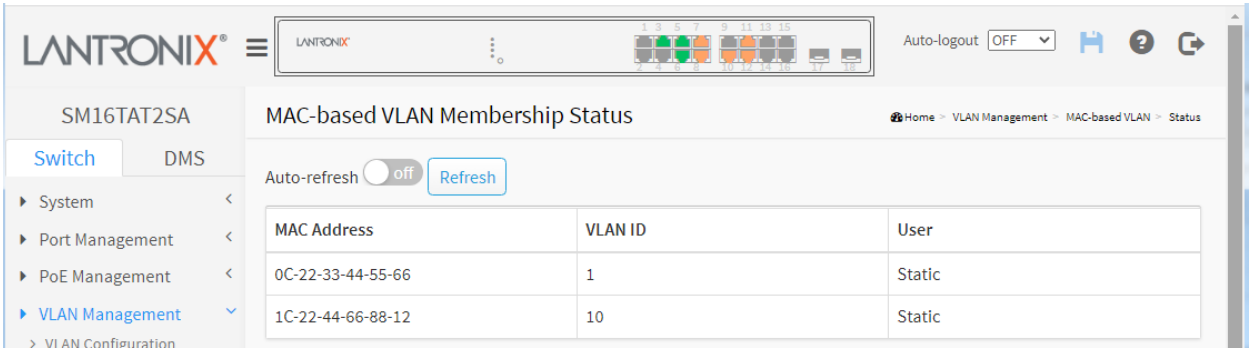
Apply: Click to save changes.

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

Add New Entry: Click the button to add a new MAC-based VLAN member. An empty row is added to the table, and the new member 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 VLAN ID values are 1-4095.

6-5.2 Status

Navigate to Switch > VLAN Management > MAC-based VLAN > Status to view existing members' status.



Parameter descriptions:

MAC Address: Displays the MAC address for the entry.

VLAN ID: Displays the VLAN ID (VID) for the entry.

User: Displays User Type for the entry (Combined, Admin, NAS, GVRP, MVR, Voice, VLAN, MSTP, DMS, or VCL).

Buttons

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

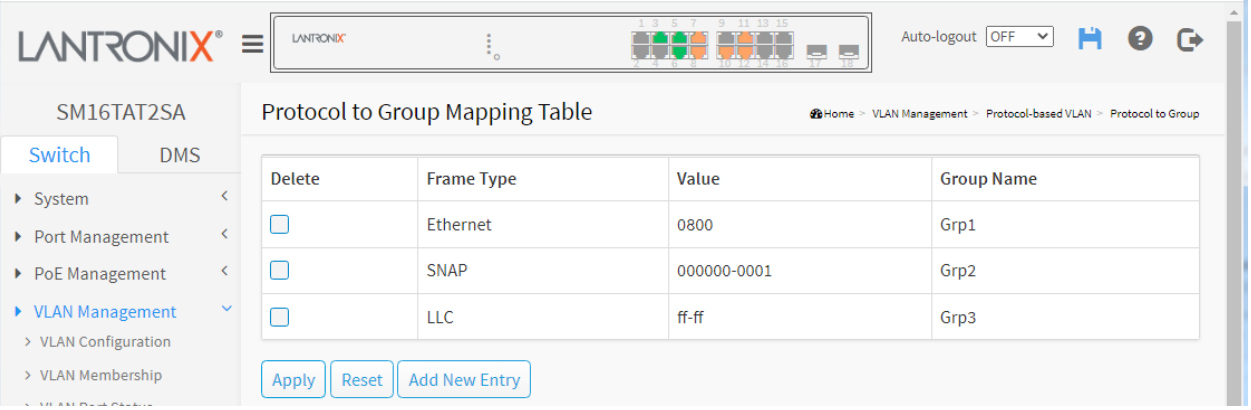
Refresh: Click to manually refresh the page immediately.

6-6 Protocol-based VLAN

6-6.1 Protocol to Group Mapping Table

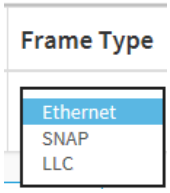
This page lets you add new protocols to Group Name (unique for each Group) mapping entries as well as allow you to see and delete already mapped entries for the switch.

Navigate to Switch > VLAN Management > Protocol-based VLAN > Protocol to Group to display the Protocol to Group Mapping Table. Here you can add new entries and view or edit existing table entries.



Parameter descriptions:

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



Frame Type: At the dropdown, select the Ethernet frame type (Ethernet, SNAP, or LLC).

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

Ethernet: Values in the text field when Ethernet is selected as a Frame Type is called etype. Valid etype values are 0x0600-0xffff

SNAP: Valid value in this case also is comprised of two different sub-values.

a. OUI: OUI (Organizationally Unique Identifier) is value in format of xx-xx-xx where each pair (xx) in string is a hexadecimal value 0x00-0xff.
b. PID: If the OUI is hexadecimal 000000, the protocol ID is the Ethernet type (EtherType) field value for the protocol running on top of SNAP; if the OUI is an OUI for a particular organization, the protocol ID is a value assigned by that organization to the protocol running on top of SNAP.

LLC: Valid value in this case is comprised of two different sub-values.

a. DSAP: 1-byte long string (0x00-0xff)
b. SSAP: 1-byte long string (0x00-0xff)

Group Name: Displays the assigned group name for each entry.

Buttons

Apply: Click to save changes.

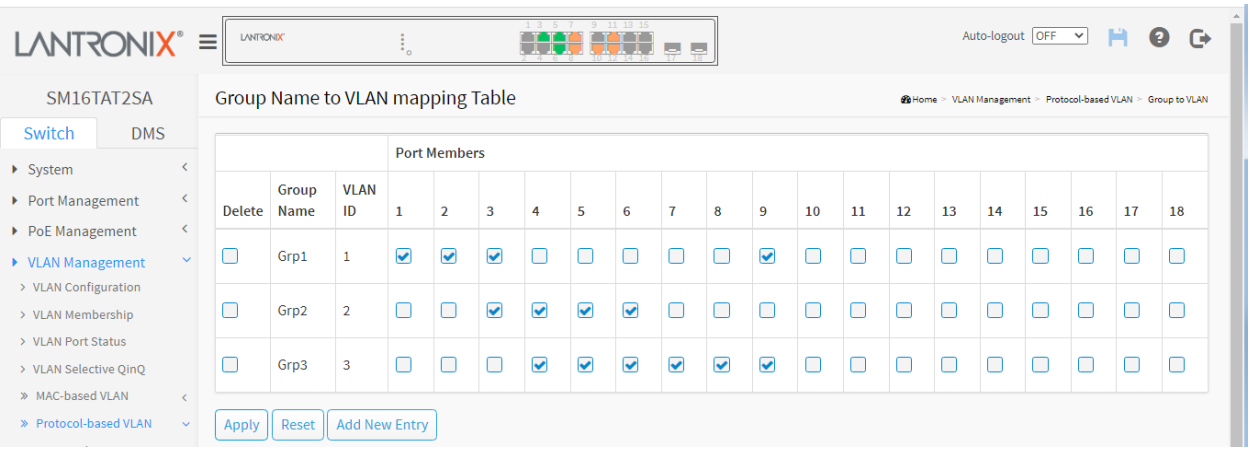
Reset: Click to undo any changes made locally and revert to previously saved values.

Add New Entry: Click the button to add a new entry. An empty row is added to the table, and the new member can be configured as needed.

6-6.2 Group Name to VLAN mapping Table

This page lets you map an already configured Group Name to a VLAN for the switch.

Navigate to Switch > VLAN Management > Protocol-based VLAN > Group to VLAN to display the Group Name to VLAN mapping Table. Add new entries and view or edit existing table entries.



Parameter descriptions:

Delete: To delete a private VLAN entry, check this box. The entry will be deleted during the next apply.

Group Name: A valid Group Name is a string of a maximum of 16 characters.

VLAN ID: Indicates the ID to which Group Name will be mapped. A valid VLAN ID can be 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

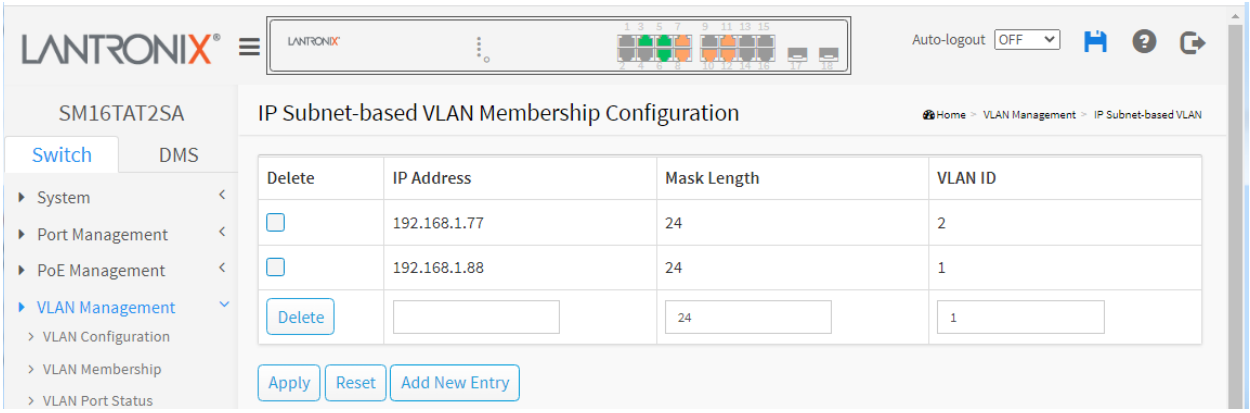
Apply: Click to save changes.

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

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

6-7 IP Subnet-based VLAN

Navigate to Switch > VLAN Management > Protocol-based VLAN > IP Subnet-based VLAN to display the IP Subnet-based VLAN Membership Configuration table. Here you can add new entries and view or edit existing table entries.



Parameter descriptions:

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

IP Address: Enter an IP address for each entry.

Mask Length: Enter the mask length for each entry.

VLAN ID: Enter the VID for this new entry (1-4095).

Buttons

Apply: Click to save changes.

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

Add New Entry: Click the button to add a new entry. An empty row is added to the table, and the new member can be configured as needed.

6-8 Private VLAN

Private VLAN membership configurations for the switch can be monitored and modified here. Private VLANs can be added or deleted here, and 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.

To configure Private VLAN membership via the web UI:

1. Click VLAN Management and Private VLAN.
2. Configure the Private VLAN port members for the switch.
3. Click the Apply button.

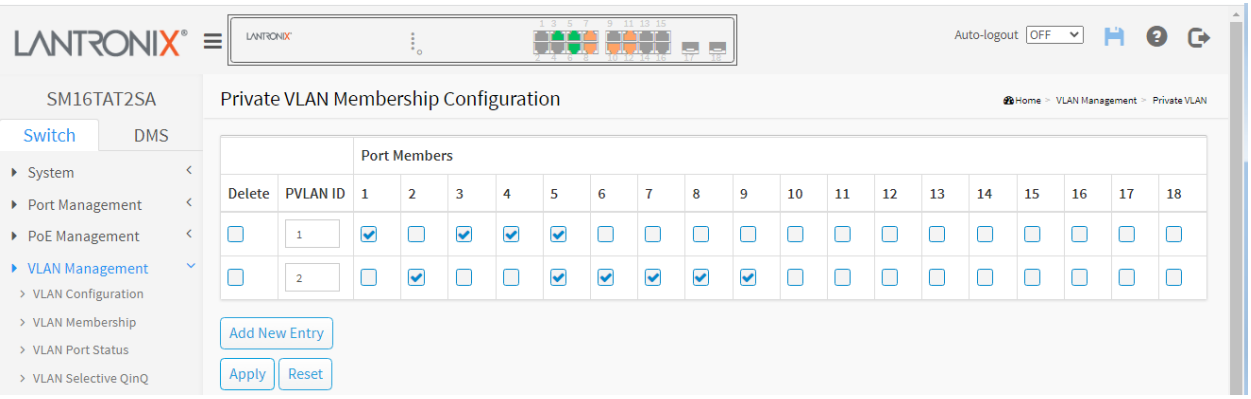


Figure 6-4: Private VLAN Membership Configuration

Parameter descriptions:

Delete: To delete a private VLAN entry, check this box. The entry will be deleted during the next apply.

PVLAN ID: Indicates the ID of this particular private VLAN.

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

Adding New Private VLAN: Click the Add New Entry button to add a new private VLAN ID. An empty row is added to the table, and the private VLAN can be configured as needed.

The Private VLAN is enabled when you click "**Apply**". The **Reset** button can be used to undo the addition of new Private VLANs.

Buttons

Apply: Click to save changes.

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

6-9 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 / port number pair.

A forwarding map generator generates a forwarding map which is responsive to a destination address of a data packet. The method for isolating ports on a layer 2 switch comprises configuring each of the ports on the layer 2 switch as a protected port or a non-protected port. A destination address on a data packet is matched with a physical address on said layer 2 switch and a forwarding map is generated for the data packet based upon the destination address on the data packet. The data packet is then sent to the plurality of ports pursuant to the forwarding map generated based on whether the ingress port was configured as a protected or non-protected port.

This page is used for enabling or disabling port isolation on ports in a Private VLAN. A port member of a VLAN can be isolated to other isolated ports on the same VLAN and Private VLAN.

To configure Port Isolation configuration in the web UI:

1. Click VLAN Management and Port Isolation.
2. Select which port(s) on which you want to enable Port Isolation.
3. Click the Apply button.

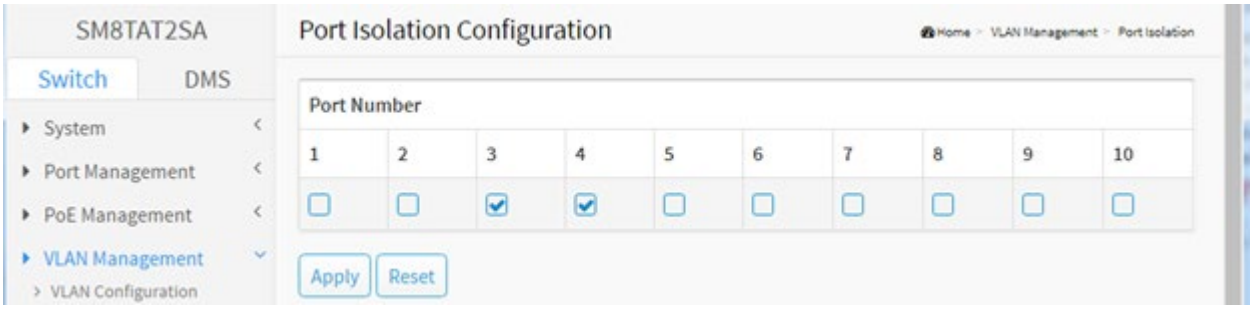


Figure 6-5: Port Isolation Configuration page

Parameter descriptions:

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

Buttons

Apply: Click to save changes.

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

6-10 Voice VLAN

The Voice VLAN feature enables voice traffic forwarding on the Voice VLAN; the switch can then classify and schedule network traffic. It is recommended that there be two VLANs on a port - one for voice and 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 through its own GUI.

6-10.1 Voice VLAN Configuration Table

To configure Voice VLAN feature parameters in the web UI:

1. Click VLAN Management, Voice VLAN, and Configuration.
2. Click the Add New Entry button.
3. Select which port(s) on which you want to configure Voice VLAN.
4. Enter VLAN ID and Aging Time and select Traffic.
5. For each Port select Mode, Security, and Discovery Protocol.
6. Click the Apply button.

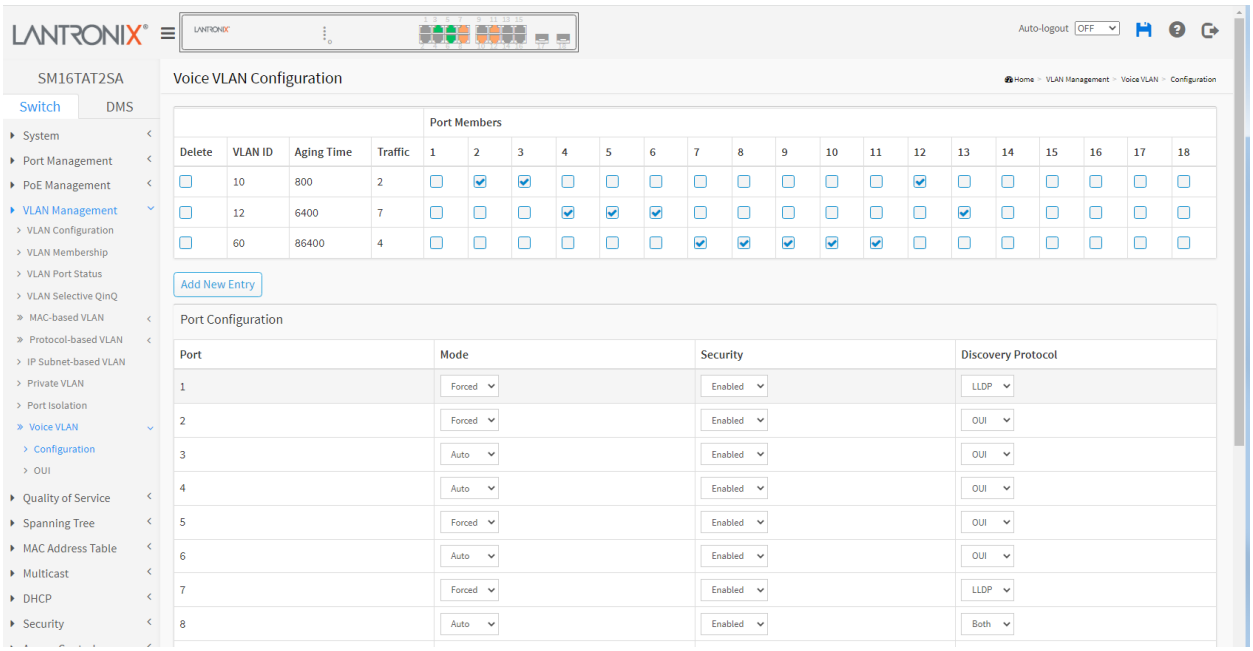


Figure 6-5: Voice VLAN Configuration page

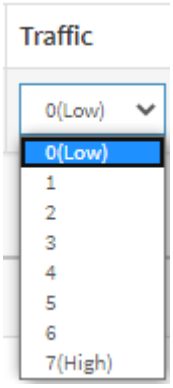
Parameter descriptions:

Voice VLAN Configuration

VLAN ID: Indicates the Voice VLAN ID. It should be a unique VLAN ID in the system and cannot equal each port PVID. It is a conflict in configuration if the value equals management VID, MVR VID, PVID etc. The allowed range is 1-4095.

Aging Time: Indicates the Voice VLAN secure learning aging time. The allowed range is 10 to 10000000 seconds. It is used when security mode or auto detect mode is enabled. In other cases, it will be based on hardware aging time. The actual aging time will be situated between the *[age_time; 2 * age_time]* interval.

Traffic: Indicates the Voice VLAN traffic class. All traffic on the Voice VLAN will apply this class. The range is 0 (Low priority) to 7 (High priority).



Port Members: Indicates the Voice VLAN port mode operation. You must disable the MSTP feature before you enable Voice VLAN. It can avoid the conflict of ingress filtering. Select which port that you want to enable the Voice VLAN mode operation.

Port Configuration

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

Mode: Indicates the Voice VLAN port mode. When the port mode isn't equal disabled, we must disable MSTP feature before we enable Voice VLAN. It can avoid the conflict of ingress filtering. Possible port modes are:

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

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

Enabled: Enable Voice VLAN security mode operation.
Disabled: Disable Voice VLAN security mode operation.

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

OUI: Detect telephony device by OUI address.
LLDP: Detect telephony device by LLDP.
Both: Both OUI and LLDP.

Buttons

Save: Click to save changes.

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

Delete: Click to do delete an existing Voice VLAN entry.

Add New Entry: Click to add a new entry in Voice VLAN configuration table.

Apply: Click to save changes.

Messages: *The VLAN ID conflict with PVID*

6-6.1 Voice VLAN OUI Configuration Table

This page lets you configure the Voice VLAN OUI table. The maximum entry number is 16. Modifying the OUI table will restart auto detection of the OUI process. An Organizationally Unique Identifier (OUI) is a 24-bit number that uniquely identifies a vendor, manufacturer, or other organization. The IEEE Public OUI list is at http://standards-oui.ieee.org/oui/oui.txt.

To configure Voice VLAN OUI in the web UI:

1. Click VLAN Management, Voice VLAN, and OUI.
2. Click the Add New Entry button.
4. Enter a Telephony OUI and Description for each instance.
5. Click the Apply button.

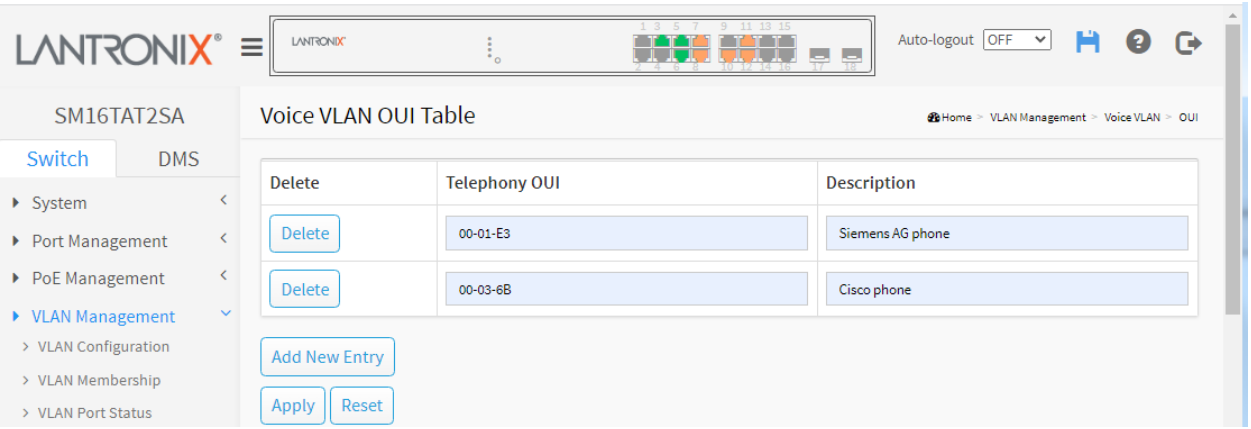


Figure 6-6: Voice VLAN OUI Table

Parameter descriptions:

Telephony OUI: A telephony OUI address is a globally unique identifier assigned to a vendor by IEEE. The OUI format is 'xx-xx-xx' (x is a hexadecimal digit). OUI examples include: 00-01-E3 (Siemens AG phones), 00-03-6B (Cisco phones), 00-0F-E2 (H3C phones), 00-60-B9 (Philips and NEC AG phones), 00-D0-1E (Pingtel phones), 00-E0-75 (Polycom phones), and 00-E0-BB (3Com phones).

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.

Delete: Click to delete an existing Voice VLAN OUI entry.

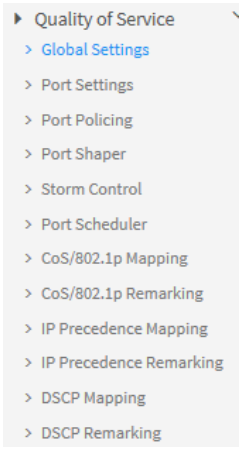
Add New Entry: Click to add a new entry in Voice VLAN OUI table. An empty row is added to the table to configure the Telephony OUI and Description.

Buttons

Save: Click to save changes.

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

Chapter 7 Quality of Service



7-1 Global Settings

Use the QoS Global Settings page to set the trust behavior for QoS basic mode. This configuration is active when the switch is in QoS basic mode. Packets entering a QoS domain are classified at the edge of the QoS domain.

To configure QoS Global Settings in the web UI:

1. Click Quality of Service and Global Settings.
2. Select the trust mode when the switch is in QoS basic mode. If a packet CoS level and DSCP tag are mapped to separate queues, the trust mode determines the queue to which the packet is assigned.
3. Click Apply to save the configuration.
4. To cancel the setting, click the Reset button to revert to previously saved values.

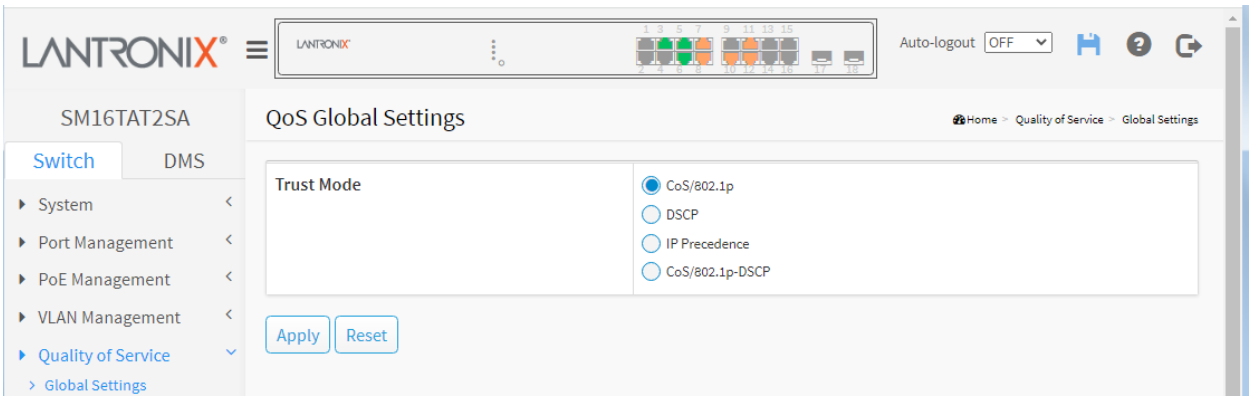


Figure 7-1: QoS Global Settings page

Trust Mode:

CoS/802.1p: Traffic is mapped to queues based on the VPT field in the VLAN tag or based on the per-port default CoS/802.1p value (if there is no VLAN tag on the incoming packet), the actual mapping of the VPT to queue can be configured on the CoS/802.1p to Queue page. This is the default setting.

DSCP: All IP traffic is mapped to queues based on the DSCP field in the IP header. The actual mapping of the DSCP to queue can be configured on the DSCP to Queue page. If traffic is not IP traffic, it is mapped to the best effort queue.

IP Precedence: Traffic is mapped to queues based on the IP precedence. The actual mapping of the IP precedence to queue can be configured on the IP Precedence to Queue page.

CoS/802.1p-DSCP: Uses the trust CoS mode for non-IP traffic and trust DSCP mode for IP traffic.

Buttons

Apply: Click to save changes.

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

7-2 Port Settings

This page lets you set QoS port parameters. To configure QoS Port Settings in the web UI:

1. Click Quality of Service and Port Settings.
2. Select Mode, Default CoS, and Source CoS, for each port.
3. Check which port(s) on which you want to enable the Remark Cos, Remark DSCP, and Remark IP Precedence.
4. Click Apply to save the configuration.
5. To cancel the setting, click the Reset button to revert to previously saved values.

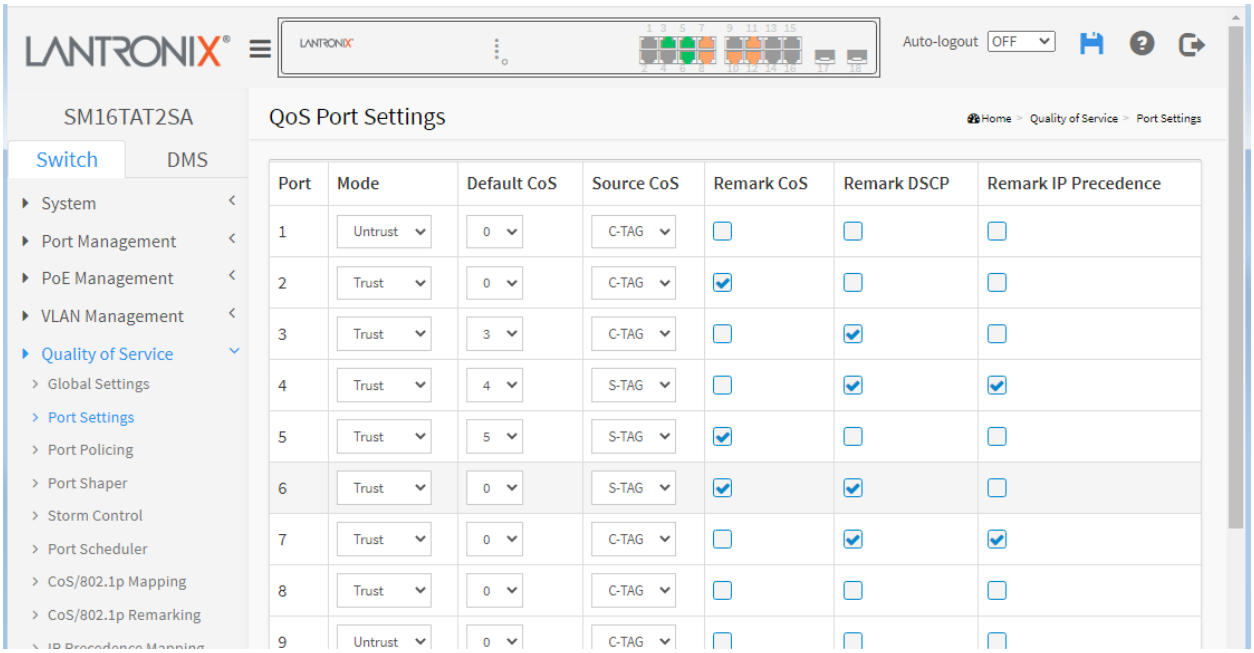


Figure 7-2: QoS Port Settings page

Parameter descriptions:

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

Mode: Select Trust or Untrust, where:

> ***Untrust*:** All ingress traffic on the port is mapped to the best effort queue and no classification/prioritization takes place (default).
>
> ***Trust*:** Port prioritize ingress traffic is based on the system wide configured trusted mode, which is either CoS/802.1p trusted mode, IP Precedence trusted mode, or DSCP trusted mode.

Default CoS: Select the default CoS value to be assigned to incoming untagged packets (0 - 7).

Source CoS: The CoS value is determined based on C-Tag or S-Tag for incoming tagged packets

Remark CoS: Click the checkbox to remark the CoS/802.1p priority for egress traffic on this port.

Remark DSCP: Click the checkbox to remark the DSCP value for egress traffic on this port.

Remark IP Precedence: Click the checkbox to remark the IP precedence for egress traffic on this port.

Note: The CoS/802.1p priority and IP Precedence, or the CoS/802.1p priority and DSCP value can be remarked simultaneously for egress traffic on a port, but the DSCP value and IP Precedence cannot be remarked simultaneously.

Buttons

Apply : Click to save changes.

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

7-3 Port Policing

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 maintain a steady rate of traffic.

To configure QoS Port Policers in the web UI:

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

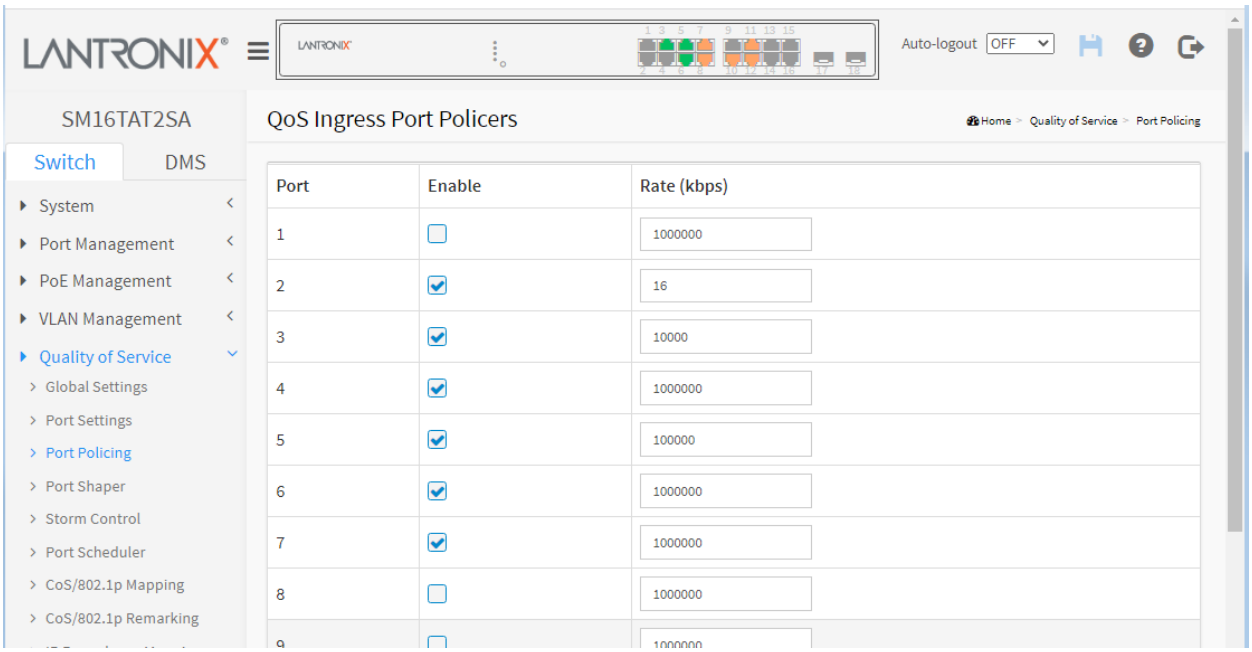


Figure 7-3: QoS Ingress Port Policers page

Parameter descriptions:

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

Enable: Check to enable for each Port you on which you want to enable the QoS Ingress Port Policers function.

Rate (kbps): Set the Rate limit value for this port. Enter a value of 16-1000000; the default is 1000000 kbps.

Buttons

Apply : Click to save changes.

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

7-4 Port Shaper

This page provides an overview of QoS Egress Port Shapers for all switch ports. To configure QoS Port Shapers in the web UI:

1. Click Quality of Service and Port Shaper.
2. Select the port to configure QoS Egress Port Shaper.
3. Click the port to enable, and configure the Rate limit condition.
4. Click Apply to save the configuration.
5. To cancel the setting, click the Reset button to revert to previously saved values.

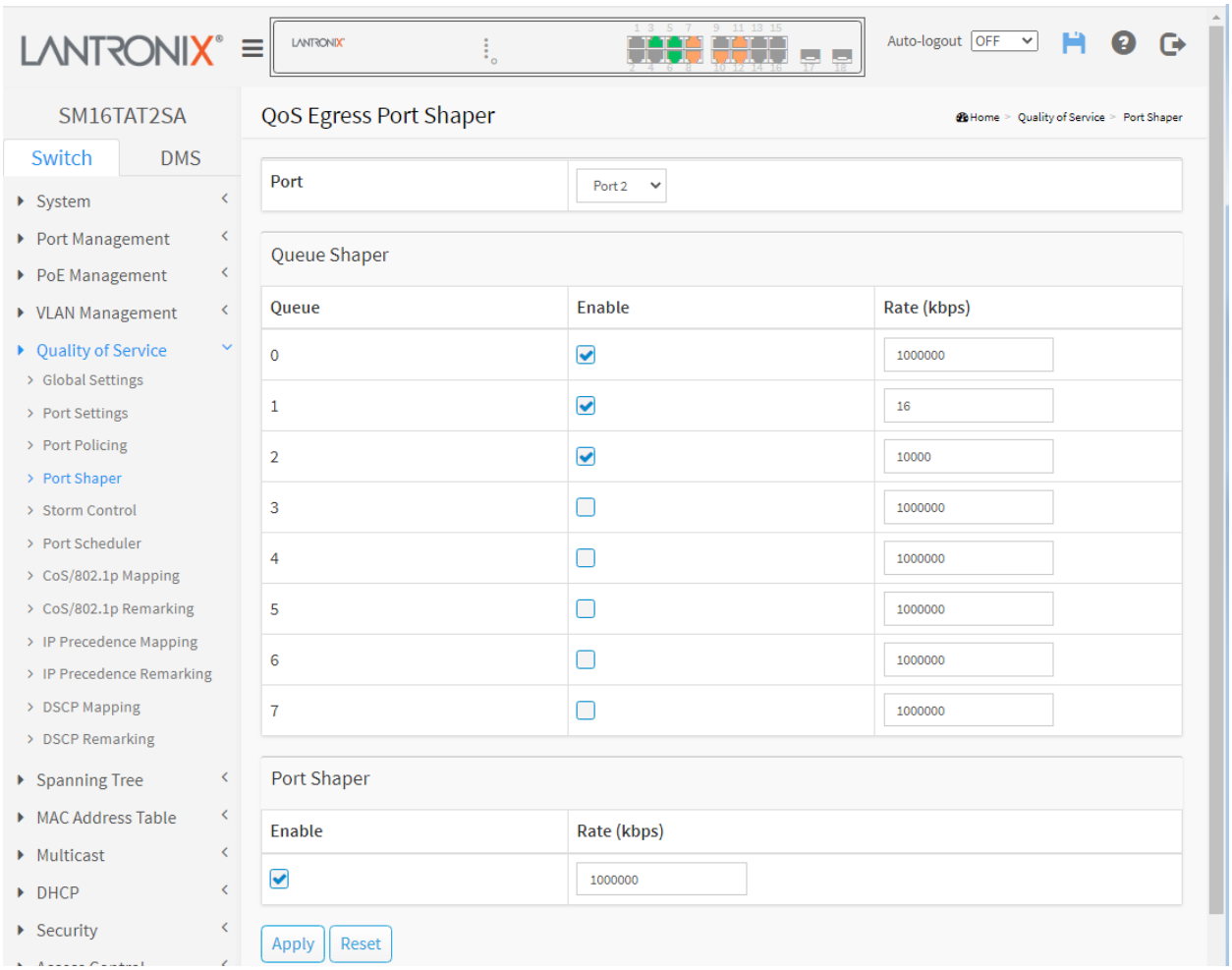


Figure 7-4: QoS Egress Port Shaper page

Parameter descriptions:

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

Queue Shaper

Queue : The queue number of the queue shaper on this switch port.

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

Rate(kbps) : Controls the rate for the queue shaper. The default value is 1000000.

Port Shaper

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

Rate(kbps) : Controls the rate for the port shaper. Valid values are 0 – 1000000. The default value is 1000000.

Buttons

Apply : Click to save changes.

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

7-5 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. You can set the permitted packet rate for Broadcast, Unknown Multicast, and Unknown Unicast traffic across the switch for each port.

To configure Storm Control parameters in the web UI:

1. Click Quality of Service and Storm Control.
2. Click the port(s) to be enabled, and configure the Rate limit condition.
4. Click the Apply button to save the settings.
5. To cancel the settings, click the Reset button to revert to previously saved values.

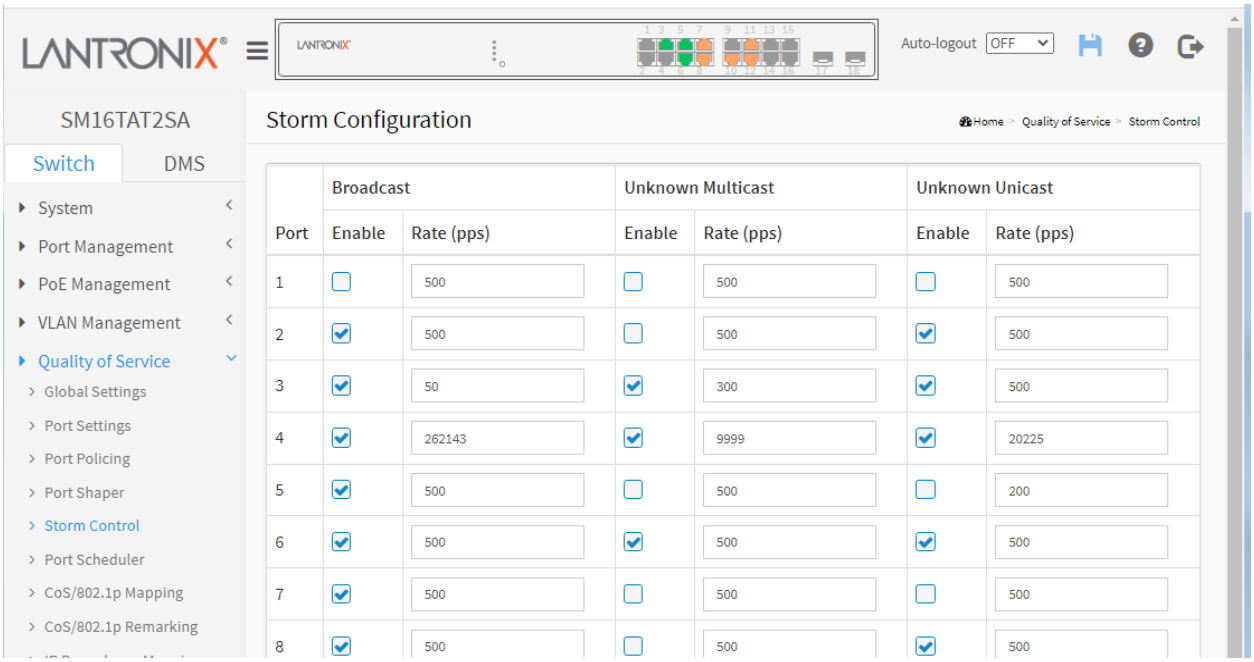


Figure 7-5: Storm Configuration page

Parameter descriptions:

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

Frame Type : The settings in a particular row apply to the frame type listed here: Broadcast, Unknown Multicast or Unknown Unicast.

Enable : Enable or disable the storm control status for the given frame type.

Rate : The rate unit in packets per second (pps). Valid values are 0 – 262143 pps.

Buttons

Apply: Click to save changes.

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

Message: *Please enter a value between 0 and 262143.*

7-6 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 Quality of Service > Port Scheduler.
2. Select Scheduler Mode for each port.
3. If you select WRR (Weighted Round Robin) or WFQ (Weighted Fair Queueing), configure Weight.
4. Click the Apply button to save the settings.
5. To cancel the setting, click the Reset button to revert to previously saved values.

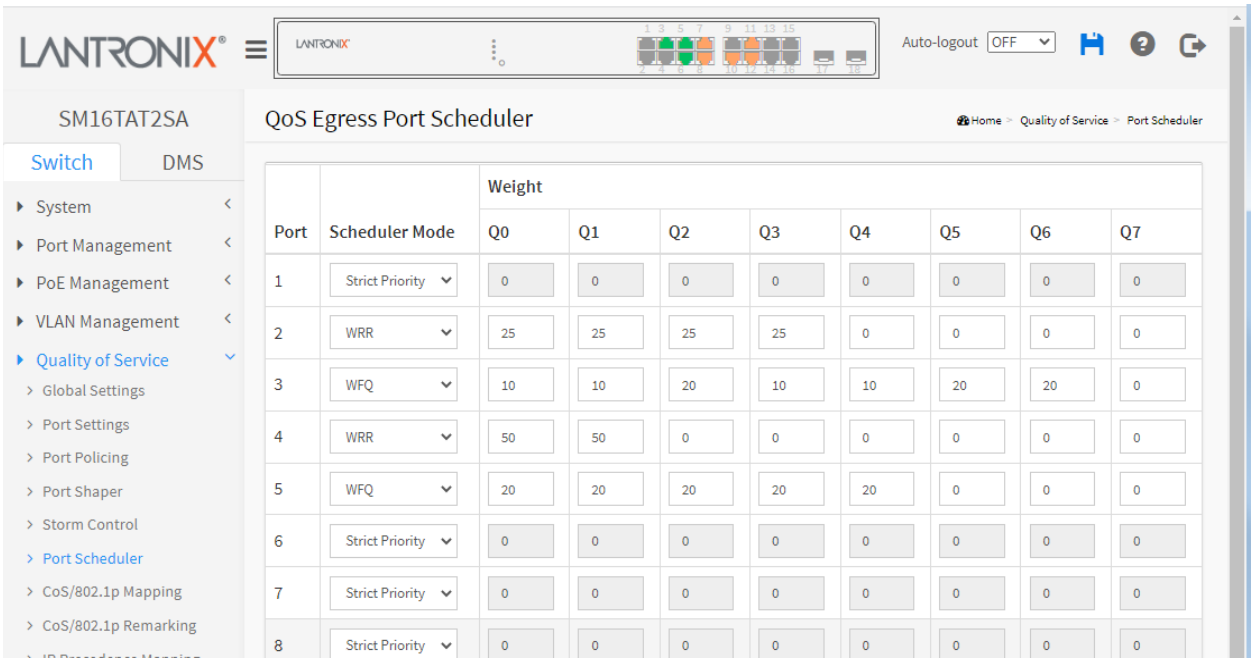
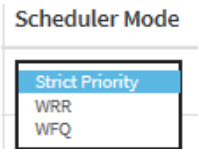


Figure 7-6: QoS Egress Port Scheduler

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

Scheduler Mode: Controls whether the scheduler mode is "Strict Priority", "WRR" or "WFQ" on this switch port.



WFQ allows specifying, for each flow, what fraction of the capacity will be given.

WRR serves a number of packets for each nonempty queue.

In a ***Strict Priority*** queue, an element with high priority is served before an element with low priority. If two elements have the same priority, they are served according to their order in the queue. This is the default setting.

Weight: Controls the weight for this queue. The default value is "0". This value is restricted to 0-127. This parameter only displays if "Scheduler Mode" is set to "Weighted" (***WRR*** or ***WFQ***).

Buttons

Apply : Click to save changes.

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

7-7 CoS/802.1p Mapping

Use the CoS/802.1p to Queue page to map 802.1p priorities to egress queues. The CoS/802.1p to Queue table determines the egress queues of the incoming packets based on the 802.1p priority in their VLAN tags. For incoming untagged packets, the 802.1p priority will be the default CoS/802.1p priority assigned to the ingress ports.

To configure the Cos/802.1p Mapping in the web UI:

1. Click Quality of Service > Cos/802.1p Mapping.
2. Select a Queue ID.
3. Click the Apply button to save the settings.
4. To cancel the setting, click the Reset button to revert to previously saved values.

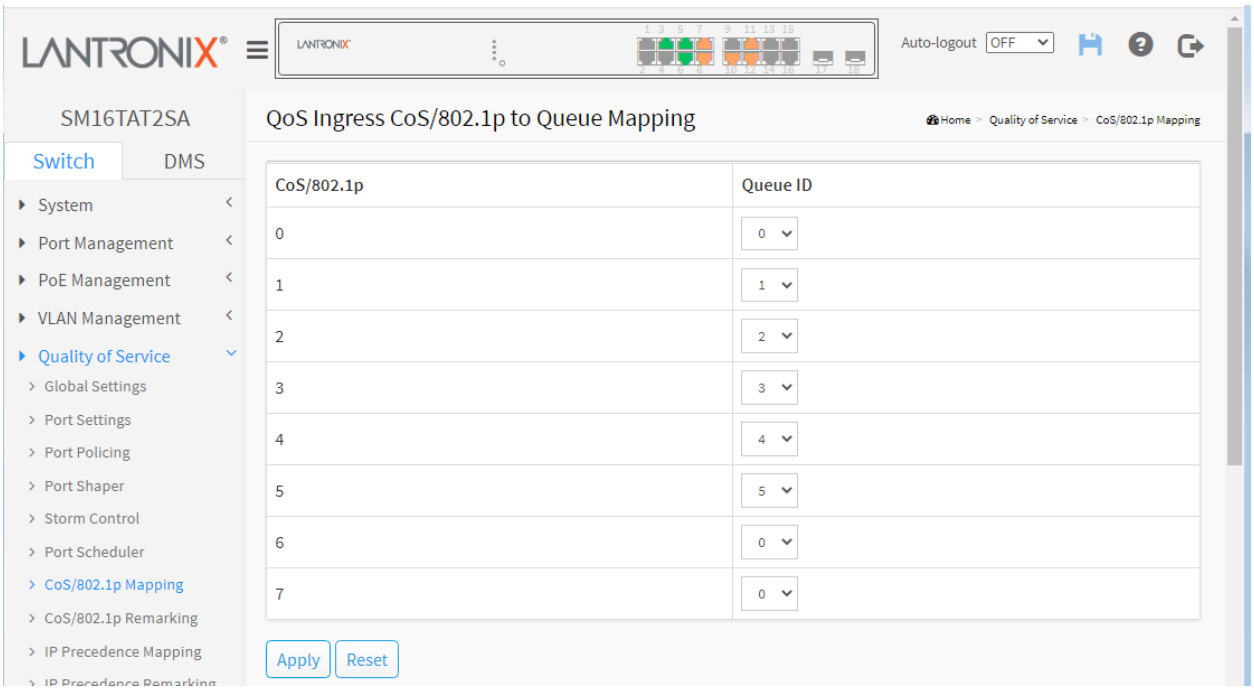


Figure 7-7: QoS Ingress CoS/802.1p to Queue Mapping

Parameter descriptions:

CoS/802.1p: Displays the 802.1p priority tag values to be assigned to an egress queue, where 0 is the lowest and 7 is the highest priority.

Queue ID: Select the egress queue to which the 802.1p priority is mapped. Eight egress queues are supported, where Queue 8 is the highest priority egress queue and Queue 1 is the lowest priority egress queue.

Buttons

Apply : Click to save changes.

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

7-8 CoS/802.1p Remarking

Use the Queues to CoS/802.1p page to remark the CoS/802.1p priority for egress traffic from each queue.

To configure Cos/802.1p Remarking in the web UI:

1. Click Quality of Service > Cos/802.1p Remarking.
2. Select CoS/802.1p.
3. Click the Apply button to save the settings.
4. To cancel the setting, click the Reset button to revert to previously saved values.

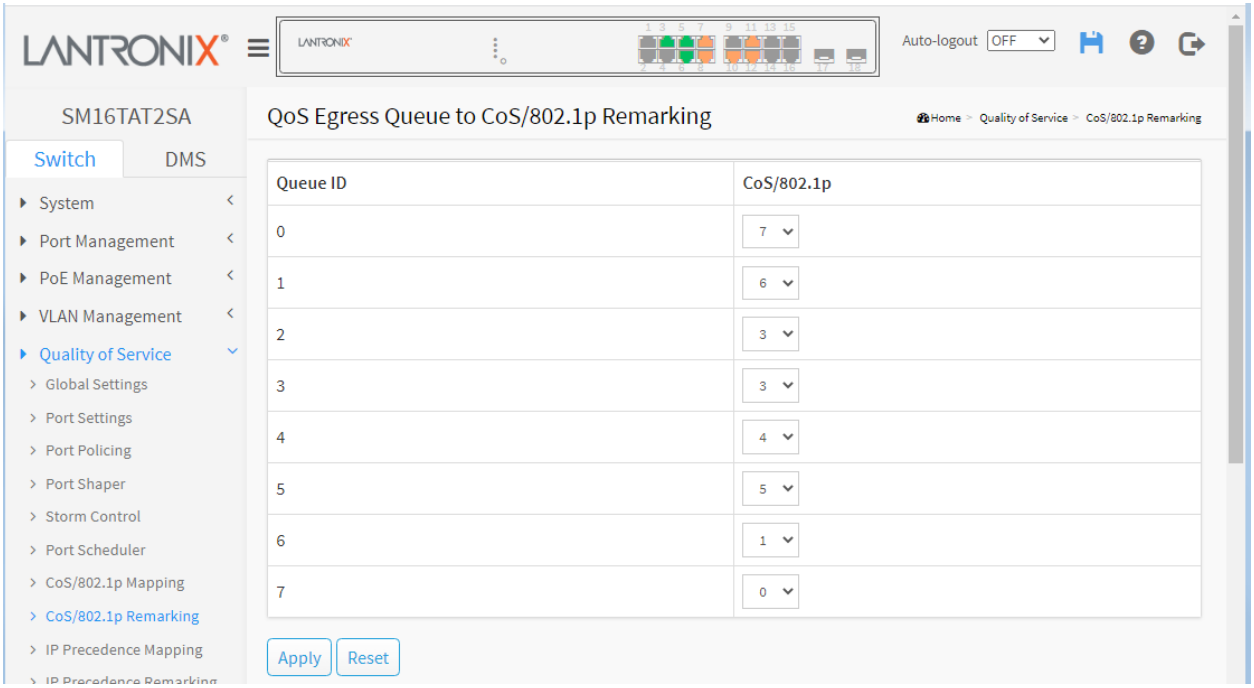


Figure 7-8: QoS Egress Queue to CoS/802.1p Remarking

Parameter descriptions:

Queue ID: Displays the Queue ID, where Queue 8 is the highest priority egress queue and Queue 1 is the lowest priority egress queue.

CoS/802.1p: For each output queue, select the CoS/802.1p priority to which egress traffic from the queue is remarked.

Buttons

Apply: Click to save changes.

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

7-9 IP Precedence Mapping

This page lets you map an IP precedence to an egress queue. To configure IP Precedence Mapping in the web UI:

1. Click Quality of Service > IP Precedence Mapping.
2. Select Queue ID.
3. Click the **Apply** button to save the settings.
4. To cancel the setting, click the **Reset** button to revert to previously saved values.

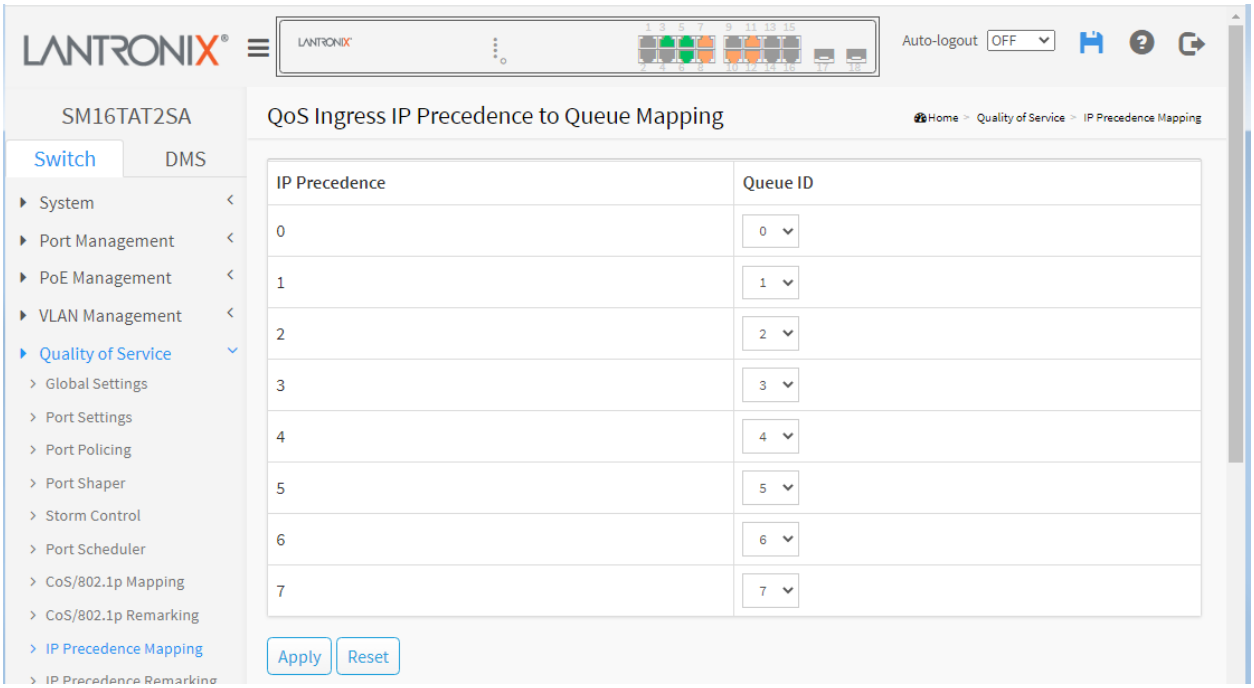


Figure 7-9: QoS Ingress IP Precedence to Queue Mapping

Parameter descriptions:

IP Precedence: Displays the IP Precedence priority tag values to be assigned to an egress queue, where 0 is the lowest priority and 7 is the highest priority.

Queue ID: Select the egress queue to which the IP precedence priority is mapped. Eight egress queues are supported, where Queue 8 is the highest priority egress queue and Queue 1 is the lowest priority egress queue.

Buttons

Apply: Click to save changes.

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

7-10 IP Precedence Remarking

This page lets you map egress queue to IP precedence. To configure IP Precedence Remarking in the web UI:

1. Click Quality of Service and IP Precedence Remarking.
2. Select IP Precedence.
3. Click the **Apply** button to save the settings.
4. To cancel the setting, click the **Reset** button to revert to previously saved values.

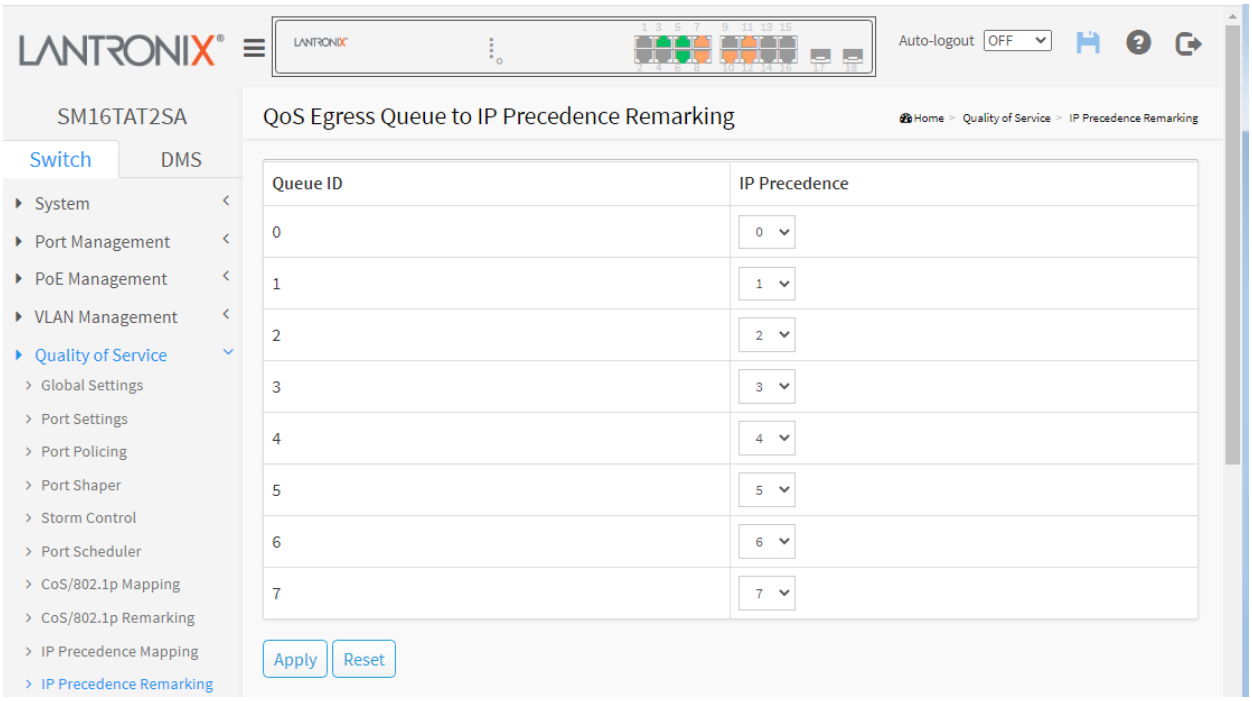


Figure 7-10: QoS Egress Queue to IP Precedence Remarking

Parameter descriptions:

Queue ID: Displays the Queue ID, where Queue 8 is the highest priority egress queue and Queue 1 is the lowest priority egress queue.

IP Precedence: For each output queue, select the IP Precedence priority to which egress traffic from the queue is remarked.

Buttons

Apply: Click to save changes.

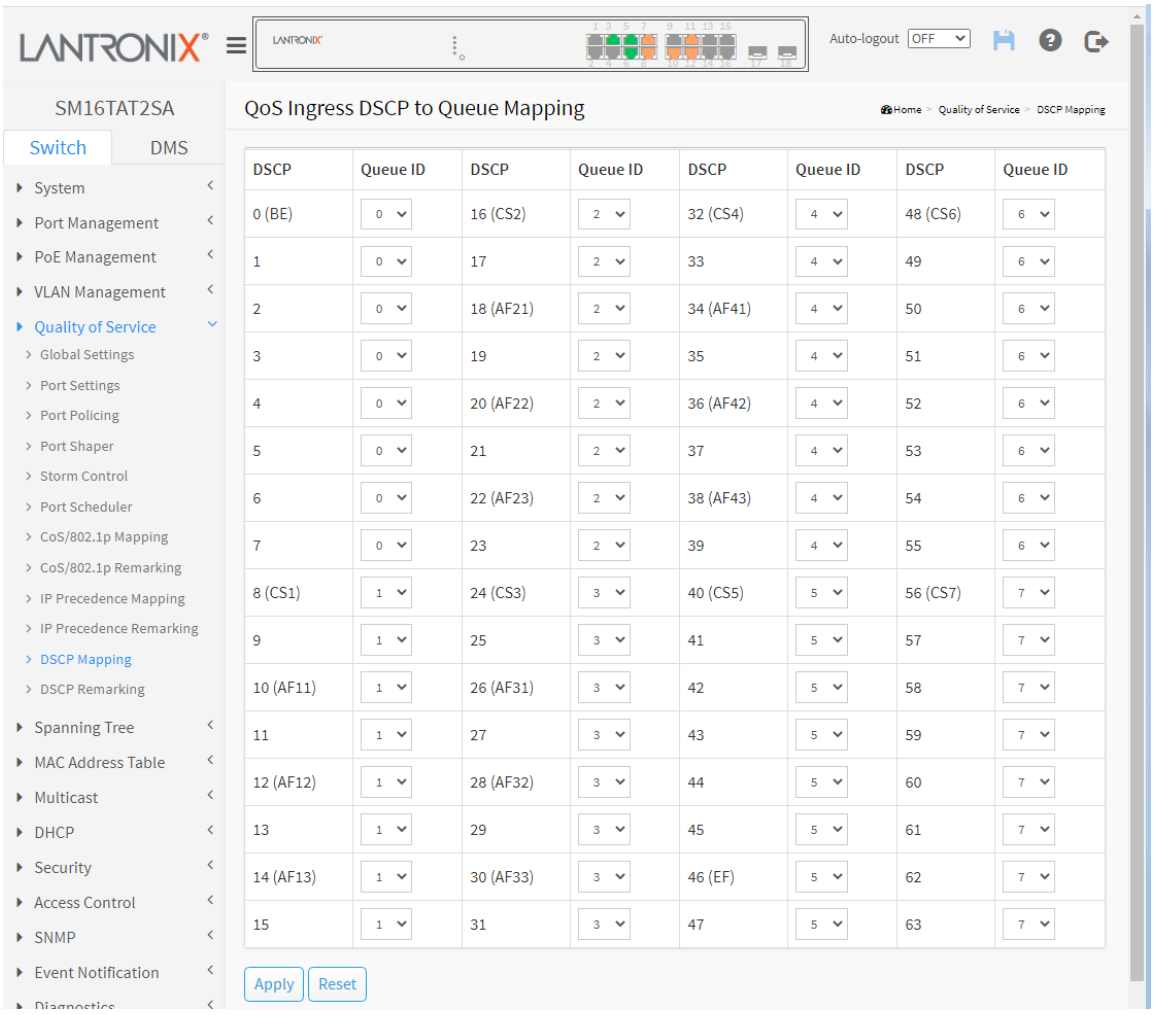
Reset: Click to undo any changes made locally and revert to previously saved values.

7-11 DSCP Mapping

Use the DSCP to Queue page to map IP DSCP to egress queues. The DSCP to Queue table determines the egress queues of the incoming IP packets based on their DSCP values. The original VLAN Priority Tag (VPT) of the packet is unchanged. It is possible to achieve the desired QoS in a network by simply changing the DSCP to Queue mapping, the queue schedule method, and bandwidth allocation.

To configure DSCP Mapping in the web UI:

1. Click Quality of Service and DSCP Mapping.
2. Select Queue ID.
3. Click the Apply button to save the settings.
4. To cancel the setting, click the Reset button to revert to previously saved values.



DSCP	Queue ID	DSCP	Queue ID	DSCP	Queue ID	DSCP	Queue ID
0 (BE)	0	16 (CS2)	2	32 (CS4)	4	48 (CS6)	6
1	0	17	2	33	4	49	6
2	0	18 (AF21)	2	34 (AF41)	4	50	6
3	0	19	2	35	4	51	6
4	0	20 (AF22)	2	36 (AF42)	4	52	6
5	0	21	2	37	4	53	6
6	0	22 (AF23)	2	38 (AF43)	4	54	6
7	0	23	2	39	4	55	6
8 (CS1)	1	24 (CS3)	3	40 (CS5)	5	56 (CS7)	7
9	1	25	3	41	5	57	7
10 (AF11)	1	26 (AF31)	3	42	5	58	7
11	1	27	3	43	5	59	7
12 (AF12)	1	28 (AF32)	3	44	5	60	7
13	1	29	3	45	5	61	7
14 (AF13)	1	30 (AF33)	3	46 (EF)	5	62	7
15	1	31	3	47	5	63	7

Figure 7-11: QoS Ingress DSCP to Queue Mapping

Parameter descriptions:

DSCP: Displays the DSCP value in the incoming packet and its associated class.

Queue ID: Select the traffic forwarding queue from the Output Queue drop-down menu to which the DSCP value is mapped.

Buttons

Apply: Click to save changes.

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

7-12 DSCP Remarking

Use the Queues to DSCP page to remark DSCP value for egress traffic from each queue.

To configure DSCP Remarking in the web UI:

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

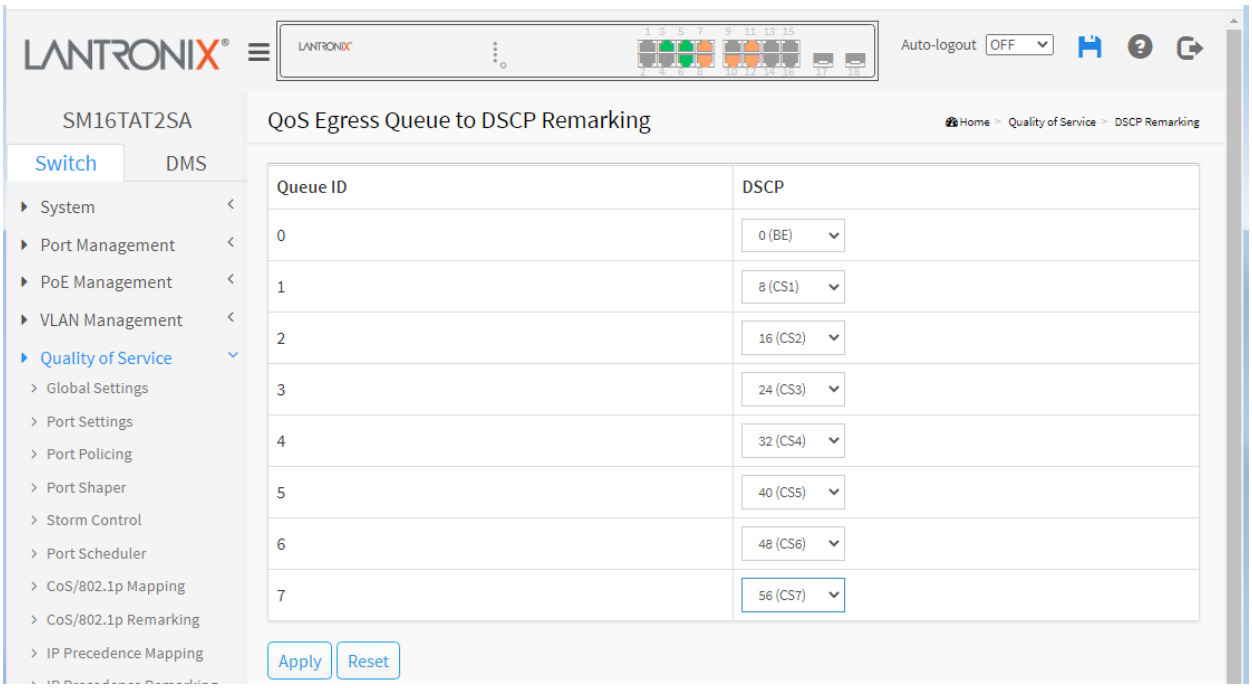


Figure 7-12: QoS Egress Queue to DSCP Remarking

Parameter descriptions:

Queue ID: Displays the Queue ID, where Queue 8 is the highest priority egress queue and Queue 1 is the lowest priority egress queue.

DSCP: For each output queue, select the DSCP priority to which egress traffic from the queue is remarked. For example, Expedited Forwarding (EF) for low-loss, low-latency traffic or Assured Forwarding (AF) which assures delivery under prescribed conditions.

Buttons

Apply: Click to save changes.

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

Chapter 8 Spanning Tree

The Spanning Tree Protocol (STP) can be used to detect and disable network loops, and to provide backup links between switches, bridges or routers. This allows the switch to interact with other bridging devices (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.

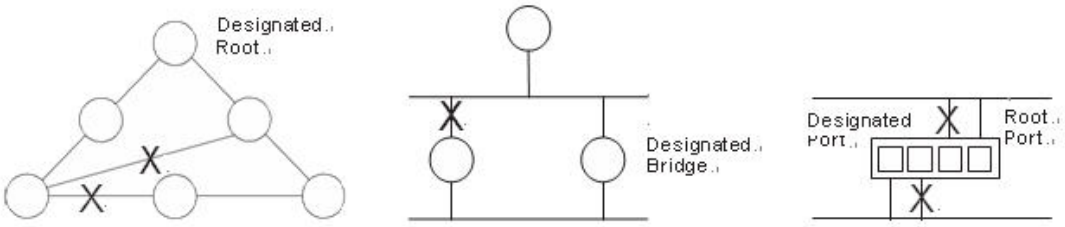


Figure 8: Spanning Tree Protocol

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.

STP network protocol builds a loop-free logical topology for Ethernet networks. The basic function of STP is to prevent bridge loops and the broadcast radiation that results from them. Spanning tree also allows a network design to include backup links providing fault tolerance if an active link fails.
STP was originally standardized as IEEE 802.1D but the functionality of spanning tree (802.1D), Rapid Spanning tree (802.1w), and Multiple Spanning tree (802.1s) has since been incorporated into IEEE 802.1Q-2014.

RSTP (Rapid Spanning Tree Protocol) was introduced as 802.1w in 2001 by the IEEE. RSTP provides significantly faster recovery in response to network changes or failures, introducing new convergence behaviors and bridge port roles to do this. RSTP was designed to be backwards-compatible with standard STP.

MSTP (Multiple Spanning Tree Protocol) was originally defined in IEEE 802.1s-2002 and later merged into IEEE 802.1Q-2005. MSTP defines an extension to RSTP to further develop the usefulness of virtual LANs (VLANs). In the standard a spanning tree that maps one or more VLANs is called “multiple spanning tree” (MST). If MSTP is implemented a spanning tree can be defined for individual VLANs or for groups of VLANs. The administrator can also define alternate paths within a spanning tree. VLANs must be assigned to a so-called multiple spanning tree instance (MSTI). Switches are first assigned to an MST region, then VLANs are mapped against or assigned to this MST. A Common Spanning Tree (CST) is an MST to which several VLANs are mapped; this group of VLANs is called MST Instance (MSTI).

8-1 State

This page lets you enable or disable MSTP; you can also select what protocol version you want. The default is Spanning Tree enabled.

To enable and configure Spanning Tree Protocol version in the web UI:

1. Click Spanning Tree and state.
2. Select "on" to enable Spanning Tree Protocol.
3. Select the Spanning Tree Protocol version.
4. Click the Apply button to save the settings.
5. To cancel the setting, click the Reset button to revert to previously saved values.

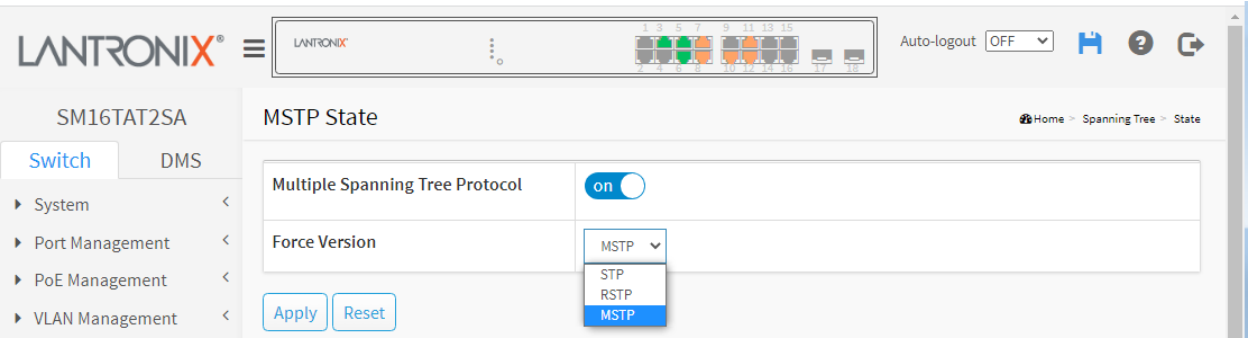


Figure 8-1: MSTP State page

Parameter descriptions:

Multiple Spanning Tree Protocol: You can select ***on*** to enable MSTP or ***off*** to disable MSTP.

Force Version: The STP protocol version setting. Valid values are ***STP***, ***RSTP*** and ***MSTP*** (see previous page for descriptions). The default is MSTP.

Buttons

Apply: Click to save changes.

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

8-2 Region Config

This page lets you configure the basic identification of a MSTP bridge. Bridges participating in a common MST region must have the same Region Name and Revision Level.

To configure MSTP Region Config in the web UI:

1. Click Spanning Tree and Region Config.
2. Specify the Region Name and Revision Level.
3. Click the Apply button to save the settings.
4. To cancel the setting, click the Reset button to revert to previously saved values.

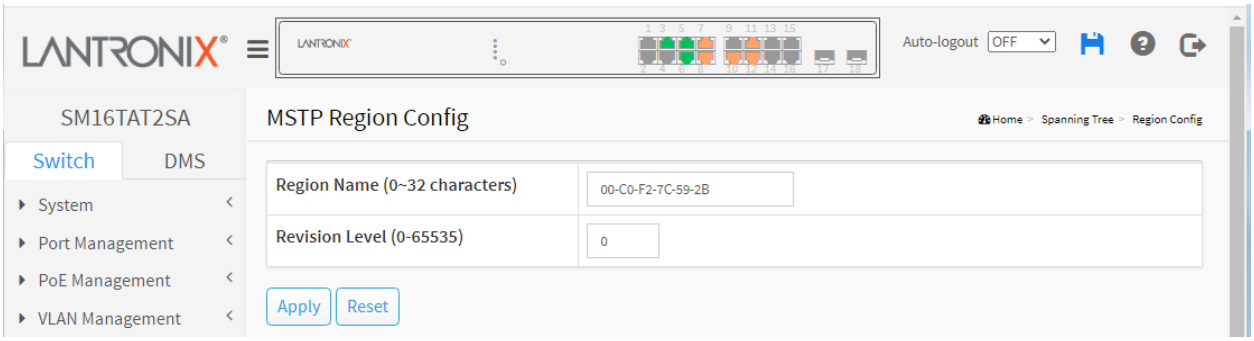


Figure 8-2: MSTP Region Config

Parameter descriptions:

Region Name (0~32 characters): 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). Enter up to 32 characters.

Revision Level (0-65535): The revision of the MSTI configuration named above. This must be an integer between 0 and 65535.

Buttons

Apply: Click to save changes.

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

8-3 Instance View

This page provides an MST instance table which includes information (VLAN membership of a MSTI) of all spanning tree instances provisioned in the particular MST region which the bridge belongs to. Through this table, additional MSTP configuration data can be applied and MSTP status can be retrieved.

To configure MSTP Instance in the web UI:

1. Click Spanning Tree and Instance View.
2. Click the Add VLAN button.
3. Specify the Instance and Port.
4. Click Instance Status and Port Status to see the detail.
5. To cancel the settings click the Delete button.

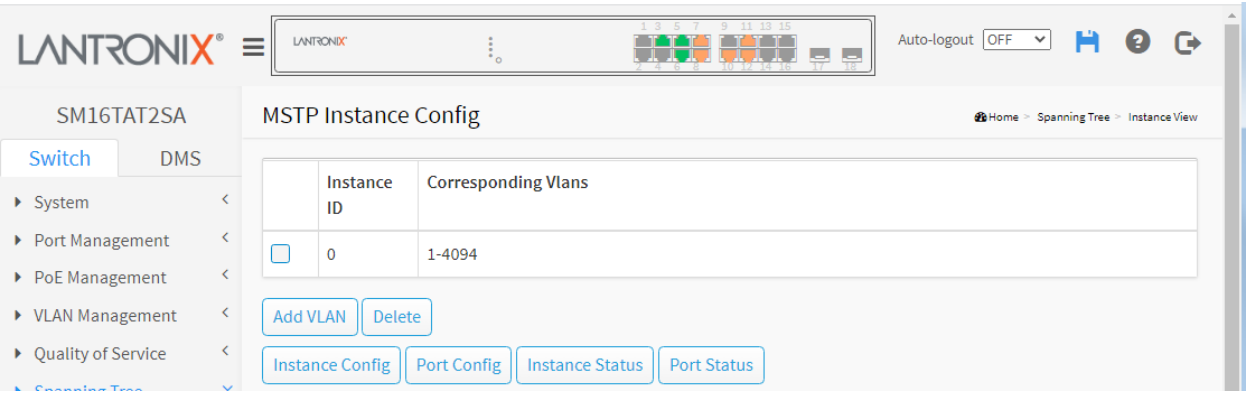


Figure 8-3a: MSTP Instance Config

Parameter descriptions:

Instance ID: Every spanning tree instance must have a unique instance ID within 0~4095. Instance 0 (CIST) always exists and cannot be deleted. Additional spanning instances (MSTIs) can be added or deleted. At least one VLAN must be provisioned for an MSTI to declare the need for the MSTI to exist.

Corresponding Vlans: 1-4095. Multiple VLANs can belong to an MSTI. All VLANs that are not provisioned through this will be automatically assigned to Instance 0 (CIST).

Buttons

Add Vlan: Click to add an MSTI and provide its VLAN members or modify VLAN members for a specific MSTI; you can add up to 63 for a total of 64.

Delete: Click to delete a selected MSTI.

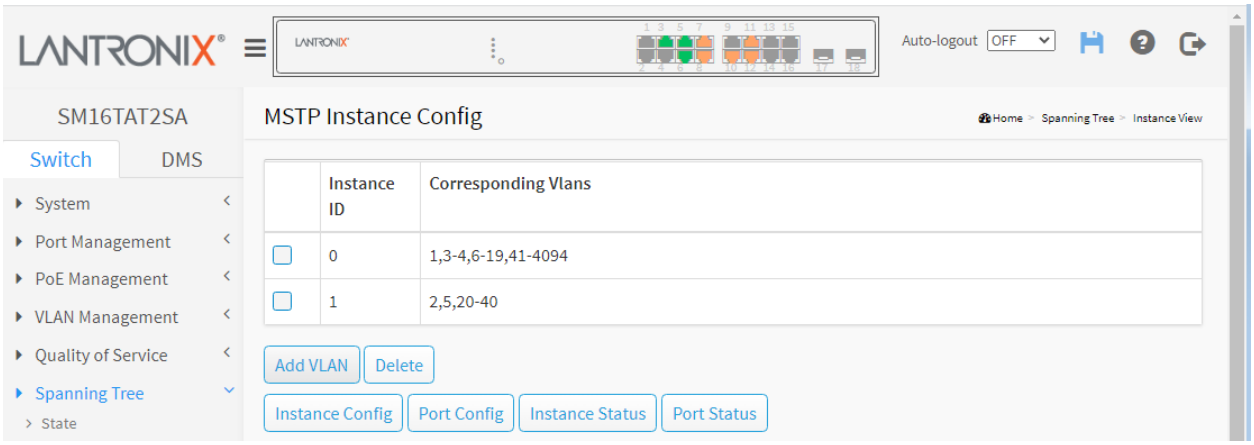
Instance Config: Click to provision spanning tree performance parameters per instance.

Port Config: Click to provision spanning tree performance parameters per instance per port.

Instance Status: Click to show the status report of a particular spanning tree instance.

Port Status: Click to show the status report of all ports regarding a specific spanning tree instance.

MSTP Create MSTI/Add Vlan Mapping:



Parameter descriptions:

Instance ID: The valid range is 1-4094.

Vlan Mapping: 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 have any VLANs mapped to it). For example: 2,5,20-40.

Buttons

Apply: Click to save changes.

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

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

Instance Config of Instance 1 :

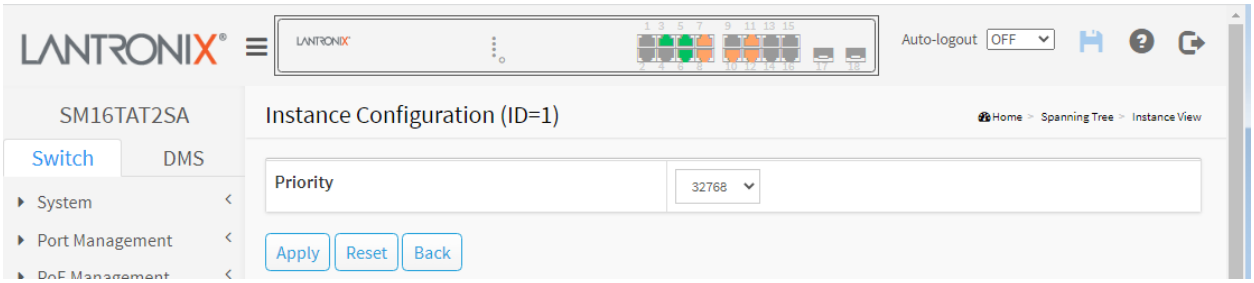


Figure 8-3b: Instance Config of Instance 1

Parameter descriptions:

Priority: The priority parameter used in the CIST (Common and Internal Spanning Tree) connection:

0 / 4096 / 8192 / 12288 / 16384 / 20480 / 24576 / 28672 / 32768 / 36864 / 40960 / 45056 / 49152 / 53248 / 57344 / 61440

MAX. Age: 6-40sec. The same definition as in the RSTP protocol.

Forward Delay: 4-30sec. The same definition as in the RSTP protocol.

MAX. Hops: 6-40sec. It's a new parameter for the multiple spanning tree protocol. It is used in the internal spanning tree instances. "CIST Remaining Hops" or "MSTI Remaining Hops" in the Spanning tree protocol message would decrease by one when the message is propagated to the neighboring bridge. If the Remaining Hops in a message is zero, the message (BPDU) would be regarded as invalid. Max Hops is used to specify the initial value of the Remaining Hops for Regional Root Bridge (Either CIST Regional Root or MSTI Regional Root).

Buttons

Apply : Click to save changes.

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

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

Port Config of Instance 1:

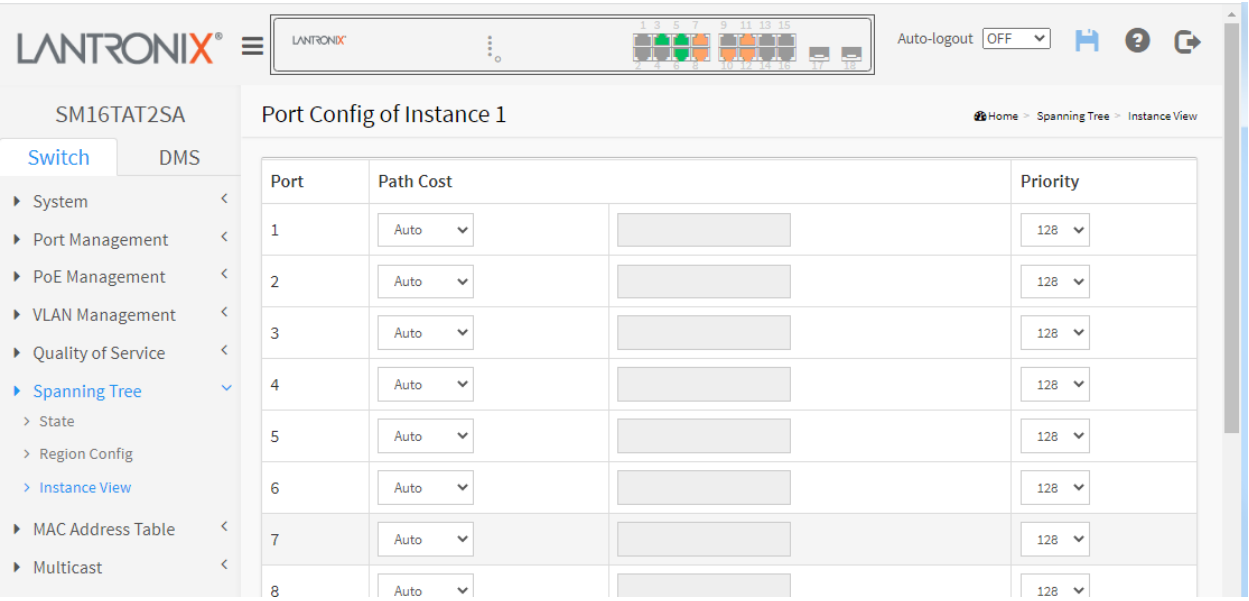


Figure 8-3c: Port Config of Instance 1

Parameter descriptions:

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

Path Cost: 1 – 200,000,000 or Auto. The same definition as in the RSTP specification. But in MSTP, this parameter can be respectively applied to ports of CIST and ports of any MSTI.

Priority: 0 / 16 / 32 / 48 / 64 / 80 / 96 / 112 / 128 / 144 / 160 / 176 / 192 / 208 / 224 / 240 . The same definition as in the RSTP specification. But in MSTP, this parameter can be respectively applied to ports of CIST and ports of any MSTI.

Admin Edge: Yes / No. The same definition as in the RSTP specification for the CIST ports. The factory

default setting is **No** (Non-Edge).

Admin P2P: Auto / True / False. The same definition as in the RSTP specification for the CIST ports.

Restricted Role: Yes / No. If "**Yes**" causes the Port not to be selected as Root Port for the CIST or any MSTI, even 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. This parameter is "**No**" by default. If set, it can cause lack of spanning tree connectivity. It is set by a network administrator to prevent bridges external to a core region of the network influencing the spanning tree active topology, possibly because those bridges are not under the full control of the administrator.

Restricted TCN: Yes / No. If "**Yes**" causes the Port not to propagate received topology change notifications and topology changes to other Ports. This parameter is "**No**" by default. If set it can cause temporary loss of connectivity after changes in a spanning trees active topology as a result of persistent incorrectly 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 status of MAC operation for the attached LANs transitions frequently.

Migration Check: The same definition as in the RSTP specification for the CIST ports. The STP Migration Check (mCheck) variable. Automatically migrate from RSTP or MSTP to STP-compatible mode.

Buttons

Apply : Click to save changes.

Back : Click to undo any changes made locally and return to the MSTP Instance Config table.

Instance Status of Instance 0 :

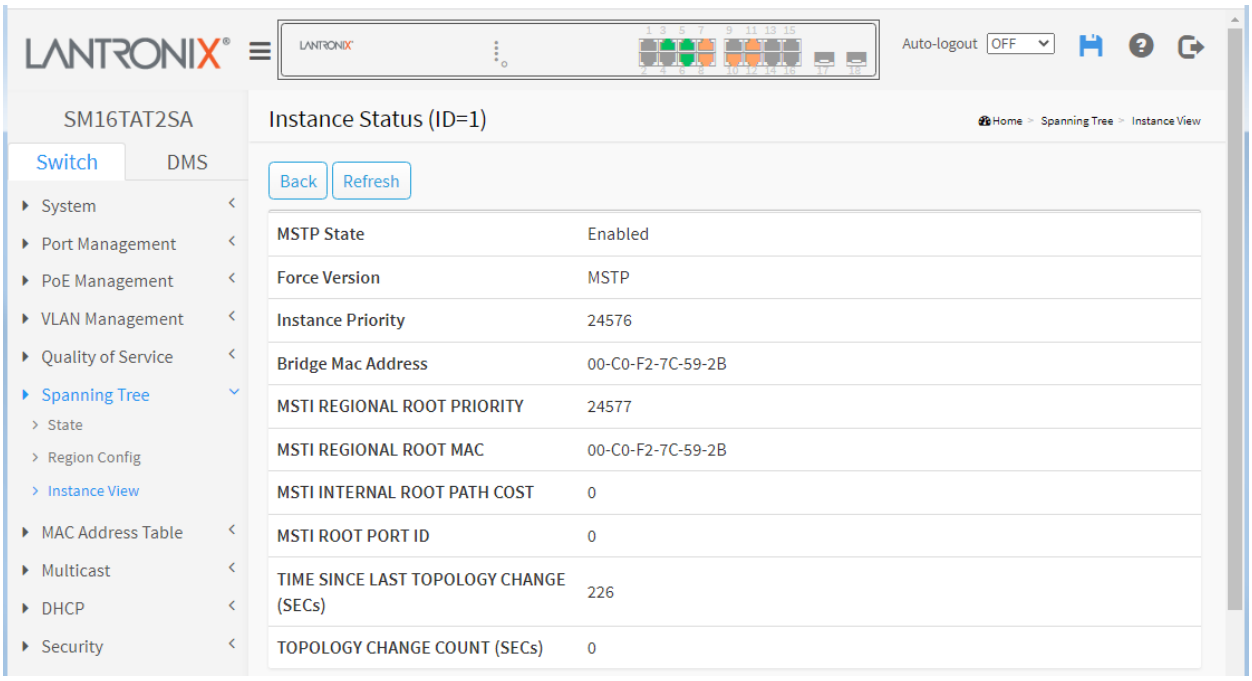


Figure 8-3d: Instance Status of Instance 1

Parameter descriptions:

MSTP State : MSTP protocol is Enable or Disable.

Force Version : Shows the current spanning tree protocol version configured.

Bridge Max Age : Shows the Max Age setting of the bridge itself.

Bridge Forward Delay : Shows the Forward Delay setting of the bridge itself.

Bridge Max Hops : Shows the Max Hops setting of the bridge itself.

Instance Priority : Spanning tree priority value for a specific tree instance (CIST or MSTI)

Bridge Mac Address : The Mac Address of the bridge itself.

CIST ROOT PRIORITY : Spanning tree priority value of the CIST root bridge

CIST ROOT MAC : Mac Address of the CIST root bridge

CIST EXTERNAL ROOT PATH COST : Root path cost value from the point of view of the bridge's MST region.

CIST ROOT PORT ID : The port ID of the bridge's root port. In MSTP, peer port of a root port may reside in different MST region or in the same MST region. The first case indicates that the root port's owner is the CIST regional root bridge.

CIST REGIONAL ROOT PRIORITY: Spanning tree priority value of the CIST regional root bridge. Note that CIST Regional Root bridge is different from CIST Root bridge. One exception is that when a bridge belonging to an MST region happens to be the root bridge of the CST (Common Spanning Tree). An MST Region in the CST can be regarded as a common RSTP bridge. The IST (Internal Spanning Tree) and MSTIs are transparent to bridges outside this region.

CIST REGIONAL ROOT MAC : Mac Address of the CIST regional root bridge.

CIST INTERNAL ROOT PATH COST : Root path cost value from the point of view of the bridges inside the IST.

CIST CURRENT MAX AGE : Max Age of the CIST Root bridge.

CIST CURRENT FORWARD DELAY : Forward Delay of the CIST Root bridge.

TIME SINCE LAST TOPOLOGY CHANGE (SECs) : Time Since Last Topology Change is the elapsed time in unit of seconds for a bunch of "Topology Change and(or) Topology Change Notification receiving" to occur. When new series of Topology Changes occur again, this counter will be reset to 0.

TOPOLOGY CHANGE COUNT (SECs) : The per spanning tree instance Topology Change Count expresses the time spent in unit of seconds since the beginning of the Spanning Tree Topology Change to the end of the STP convergence. Once there is no topology change occurring and no more topology change notification received, the Topology Change count will be reset to 0.

Buttons

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

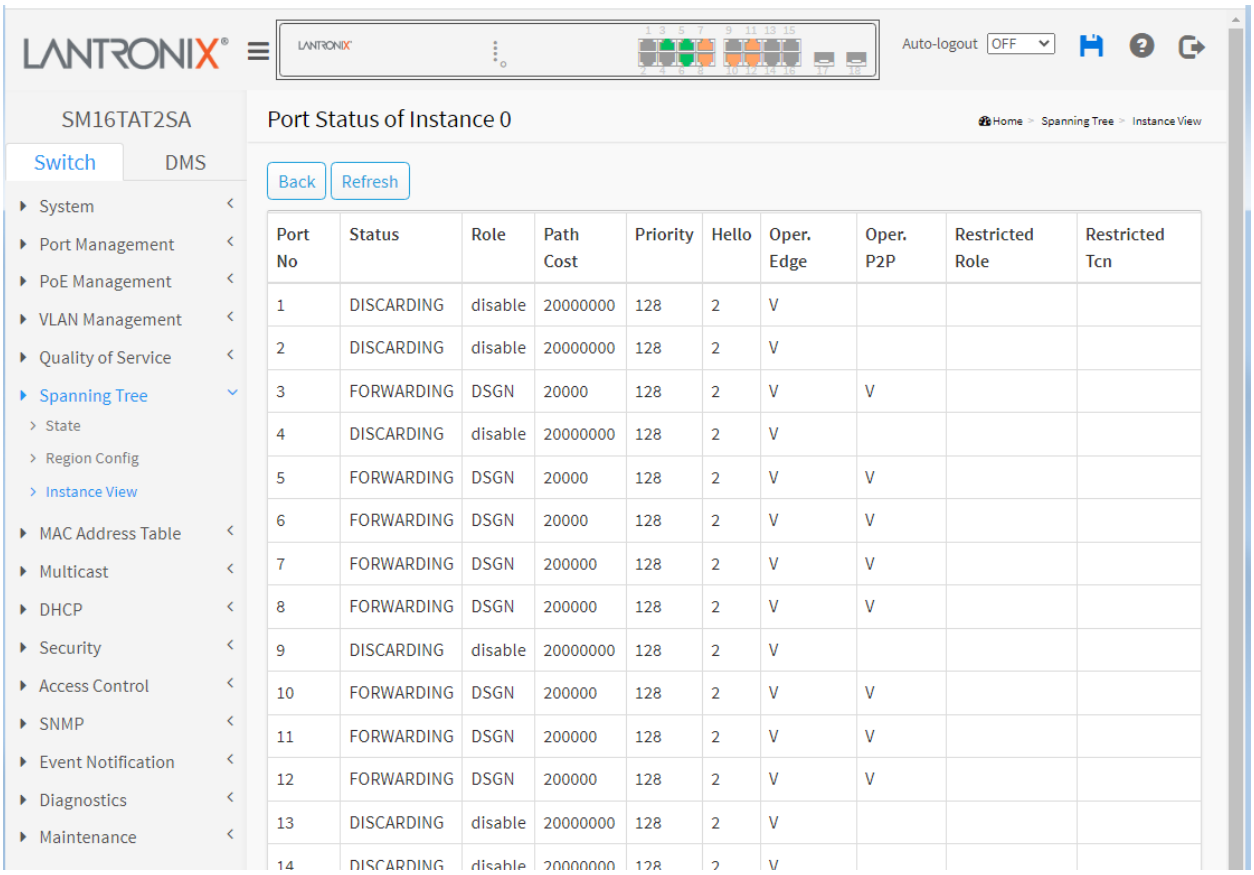
Refresh : Click to manually refresh the page immediately.

Messages:

Please choose an Instance first

MSTP disabled or force version is not MSTP

Port Status of Instance 0 :



Port No	Status	Role	Path Cost	Priority	Hello	Oper. Edge	Oper. P2P	Restricted Role	Restricted Tcn
1	DISCARDING	disable	20000000	128	2	V			
2	DISCARDING	disable	20000000	128	2	V			
3	FORWARDING	DSGN	20000	128	2	V	V		
4	DISCARDING	disable	20000000	128	2	V			
5	FORWARDING	DSGN	20000	128	2	V	V		
6	FORWARDING	DSGN	20000	128	2	V	V		
7	FORWARDING	DSGN	200000	128	2	V	V		
8	FORWARDING	DSGN	200000	128	2	V	V		
9	DISCARDING	disable	20000000	128	2	V			
10	FORWARDING	DSGN	200000	128	2	V	V		
11	FORWARDING	DSGN	200000	128	2	V	V		
12	FORWARDING	DSGN	200000	128	2	V	V		
13	DISCARDING	disable	20000000	128	2	V			
14	DISCARDING	disable	20000000	128	2	V			

Figure 8-3e: Port Status of Instance 0

Parameter descriptions:

Port No: The port number to which the configuration applies.

Status: The forwarding status. Same definition as of the RSTP specification. Possible values are "FORWARDING", "LEARNING", "DISCARDING".

Role: The role that a port plays in the spanning tree topology. Possible values are "disable"(disable port) , "alternate" (alternate port) , "backup" (backup port) , "ROOT" (root port) , "DSGN" (designated port) , and "MSTR" (master port). The last 3 are possible port roles for a port to transit to FORWARDING state

Path Cost: Displays currently resolved port path cost value for each port in a particular spanning tree instance.

Priority: Displays port priority value for each port in a particular spanning tree instance.

Hello: Per port Hello Time display. It takes the following form: *Current Hello Time/Hello Time Setting*

Oper. Edge: Whether or not a port is actually an Edge Port.

Oper. P2P: Whether or not a port is actually a Point-to-Point port.

Restricted Role: Yes / No. If "**Yes**" causes the Port not to be selected as Root Port for the CIST or any MSTI, even 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. This parameter is "**No**" by default. If set, it can cause lack of spanning tree connectivity. It is set by a network administrator to prevent bridges external to a core region of the network influencing the spanning tree active topology, possibly because those bridges are not under the full control of the administrator.

Restricted TCN: Yes / No. If "**Yes**" causes the Port not to propagate received topology change notifications and topology changes to other Ports. This parameter is "**No**" by default. If set it can cause temporary loss of connectivity after changes in a spanning trees active topology as a result of persistent incorrectly 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 status of MAC operation for the attached LANs transitions frequently.

Buttons

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

Refresh : Click to manually refresh the page immediately.

Messages

Message: *MSTP disabled or force version is not MSTP*

Recovery: Click OK to clear, change the Instance Status parameter, and continue.

Chapter 9 MAC Address Tables

9-1 Configuration

Switching of frames is based on the DMAC address contained in the frame. The switch builds a table that maps MAC addresses to switch ports for knowing which ports the frames should go to (based 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 was seen after a configurable age time.

To configure MAC Address Table in the web UI:

1. Click MAC Address Table and Configuration.
2. Specify the Disable Automatic Aging and Aging Time.
3. Configure the Port Members (Auto, Disable, Secure).
4. Click the Add New Static Entry button, and specify the VLAN ID, Mac address, Block, and Port Member parameters.
5. Click Apply.

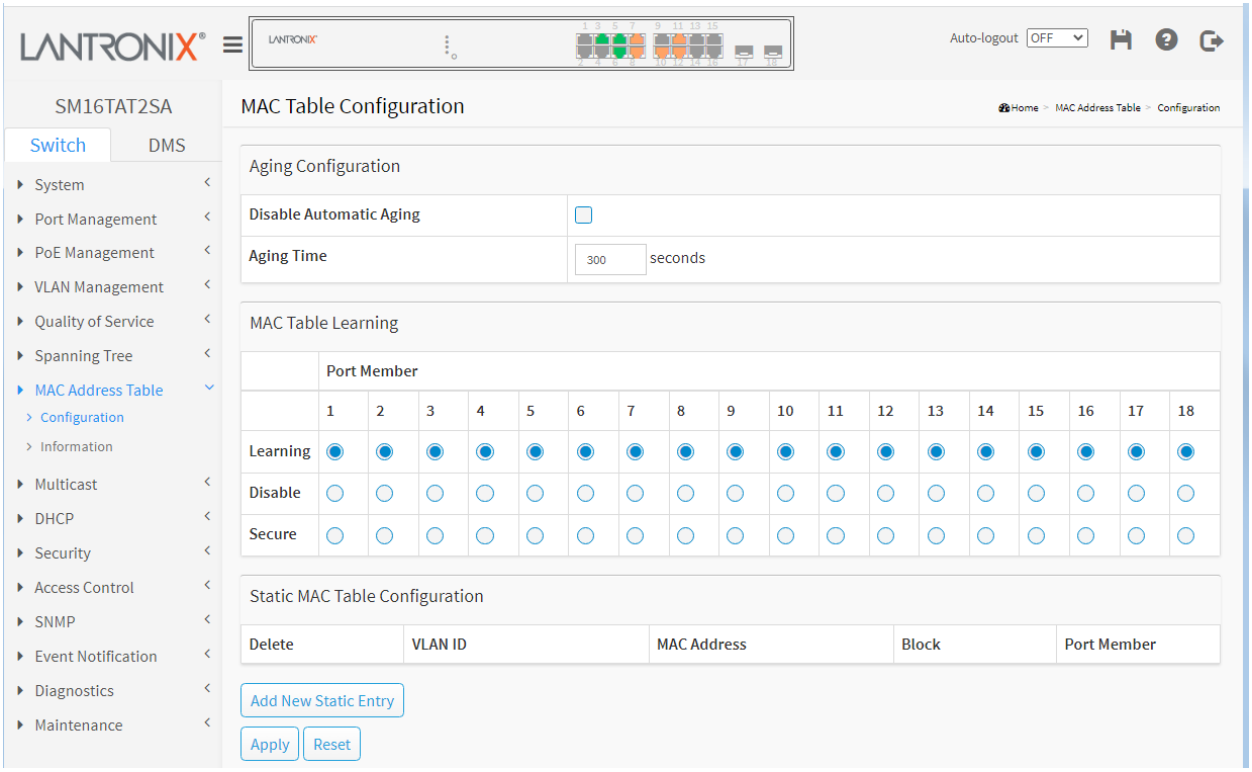


Figure 9-1: MAC Table Configuration

Parameter descriptions:

Aging Configuration: By default, dynamic entries are removed from the MAC table after 300 seconds. This removal is also called aging. Configure aging time by entering a value here in seconds. The valid range is 10 - 1000000 seconds. Disable the automatic aging of dynamic entries by checking the Disable Automatic Aging checkbox.

MAC Table Learning: If the learning mode for a given port is greyed out, another module is in control of the mode, so that it cannot be changed by the user. An example of such a module is the MAC-Based Authentication under 802.1X. Each port can do learning based upon the following settings:

Learning: 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 Telnet interface.

Static MAC Table Configuration

The static entries in the MAC table are shown in this table. The static MAC table can contain 64 entries. The MAC table is sorted first by VLAN ID and then by MAC address.

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

VLAN ID: The VLAN ID of the entry.

MAC Address: The MAC address of the entry.

Block: Click it if you want to block this mac address.

Port Member: Check radio buttons to set which ports are members of the entry. Check or uncheck as needed to modify the entry.

Buttons

Add New Static Entry: Click to add a new entry to the static MAC table. Specify the VLAN ID, MAC address, and port members for the new entry. Click "Apply".

Apply: Click to save changes.

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

9-2 Information

Entries in the MAC Table are shown on this page. The MAC Table contains up to 8192 entries, and is sorted first by VLAN ID, then by MAC address.

To display the Dynamic MAC Table in the web UI:

1. Click MAC Address Table and Information.
2. View the displayed MAC Address Table.
3. Click the buttons as required.

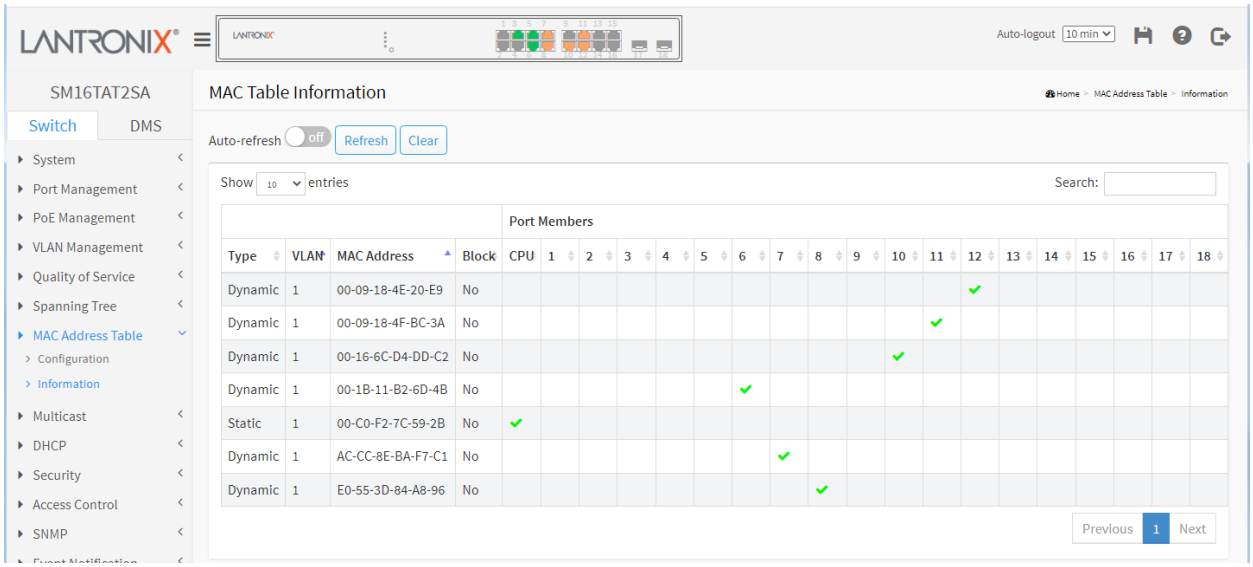


Figure 9-2: MAC Table Information

Parameter descriptions:

Aging Configuration

Show *x* entries: At the dropdown, select how many lines to display per page (10, 25, 60, 100, or 500).

Type: Indicates whether the entry is a Static or a Dynamic entry, or 802.1x, DMS.

VLAN: The VLAN ID of the entry.

MAC address: The MAC address of the entry.

Block: Whether the mac address is blocked or not.

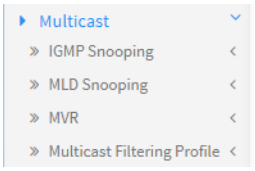
Port Members: The ports that are members of the entry.

Buttons

Auto-refresh: Check to refresh the page automatically every 3 seconds.
Refresh: Click to manually refresh the page. immediately
Clear: Click to clear the page.
Previous: Updates the system log entries, turn to the previous page.
Next: Updates the system log entries, turn to the next page.

Note: 00-40-C7-73-01-29 : your switch MAC address (for IPv4)
33-33-00-00-00-01 : Destination MAC (for IPv6 Router Advertisement) (reference IPv6 RA.JPG)
33-33-00-00-00-02 : Destination MAC (for IPv6 Router Solicitation) (reference IPv6 RS.JPG)
33-33-FF-73-01-29 : Destination MAC (for IPv6 Neighbor Solicitation) (reference IPv6 DAD.JPG)
33-33-FF-A8-01-01: your switch MAC address (for IPv6 global IP)
FF-FF-FF-FF-FF-FF: for Broadcast.

Chapter 10 Multicast



10-1 IGMP Snooping

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

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

The packets will be discarded by 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.

10-1.1 Basic Configuration

This webpage lets you set the basic IGMP snooping on the switch, which connects to a router closer to the root of the tree. This interface is the upstream interface. The router on the upstream interface should be running IGMP.

Web Interface

To configure IGMP Snooping parameters in the web UI:

1. Click Multicast, IGMP Snooping, and Basic Configuration.
2. Enable or disable the Global configuration.
3. Select the port you want to become a Router Port or enable/ disable the Fast Leave function.
4. Scroll to set the Throttling and Profile.
5. Click the Apply button to save the settings.
6. To cancel the setting, click the Reset button to revert to previously saved values.

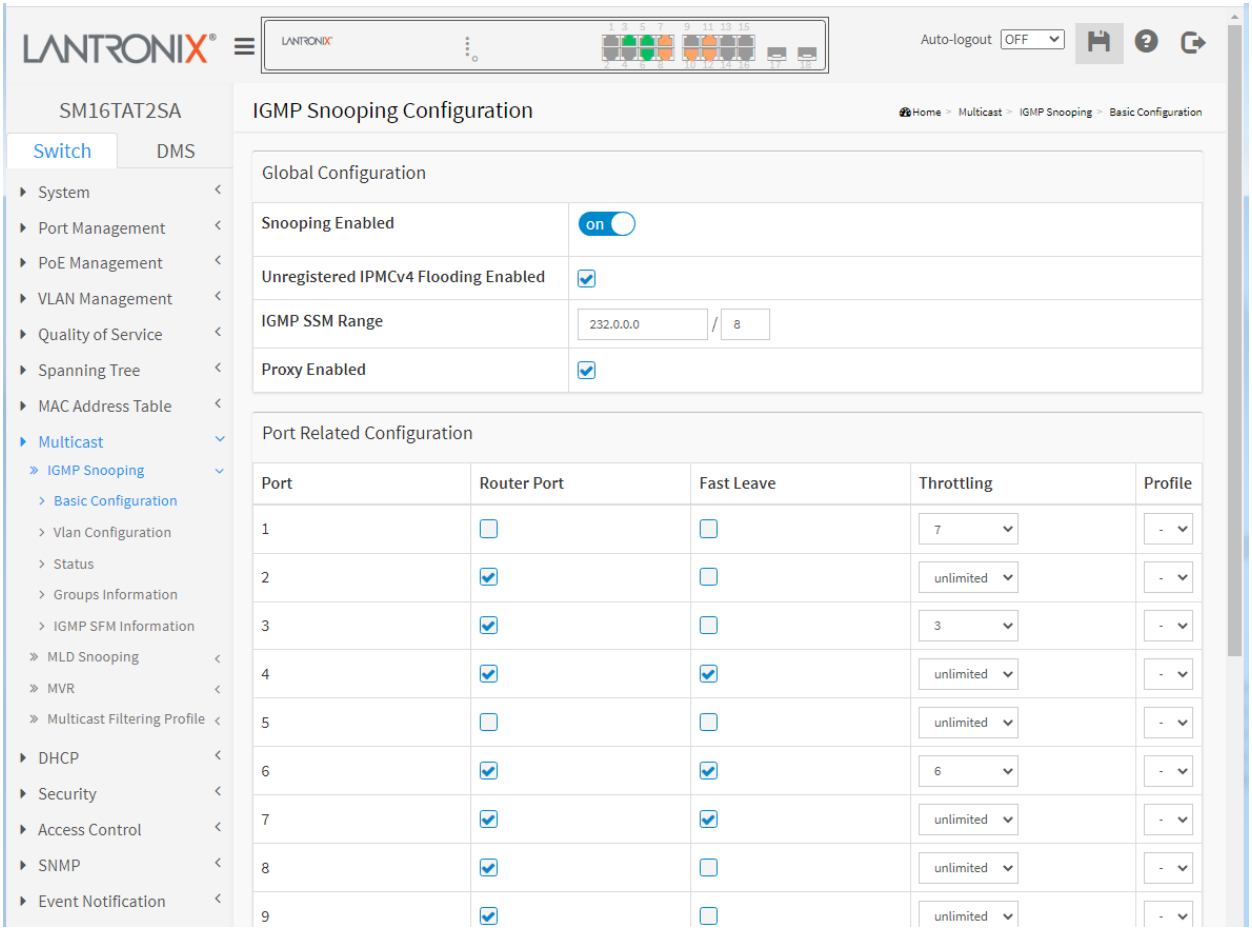


Figure 10-1.1: IGMP Snooping Configuration

Parameter descriptions:

Global Configuration

Snooping Enabled: Enable the Global IGMP Snooping.

Unregistered IPMCv4 Flooding enabled: Enable unregistered IPMCv4 traffic flooding. Unregistered IPMCv4 traffic is also called "unknown multicast". After selected, the unregistered multicast stream will be forwarded like normal packets. Once you un-selected it, an unregistered multicast stream will be discarded.

IGMP SSM Range: SSM (Source-Specific Multicast) Range lets the SSM-aware hosts and routers run the SSM service model for the groups in the address range. Format: (IP address/ sub mask).
Per IETF RFC 4607, IP version 4 (IPv4) addresses in the 232/8 (232.0.0.0 to232.255.255.255) range are designated as source-specific multicast (SSM) destination addresses and are reserved for use by source-specific applications and protocols. For IP version 6 (IPv6), the address prefix FF3x::/32 is reserved for source-specific multicast use.

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: You can select profile when you edit in Multicast Filtering Profile.

Buttons

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

Refresh: Click to manually refresh the page. immediately

10-1.2 VLAN Configuration

This page lets you set the VLAN parameters integrated for the IGMP Snooping function. Each page shows up to 99 entries from the VLAN table, default being 20, selected through the "entries per page" input field. When first visited, the web page will show the first 20 entries from the beginning of the VLAN Table. The first displayed will be the one with the lowest VLAN ID found in the VLAN Table. The "VLAN" input fields allow the user to select the starting point in the VLAN Table.

Web Interface

To configure IGMP Snooping VLAN parameters in the web UI:

1. Click Multicast, IGMP Snooping, and VLAN Configuration.
2. Click the Add New IGMP VLAN button to add a new row to the table.
3. Click the Apply button to save the settings.
4. To cancel the setting, click the Reset button to revert to previously saved values.

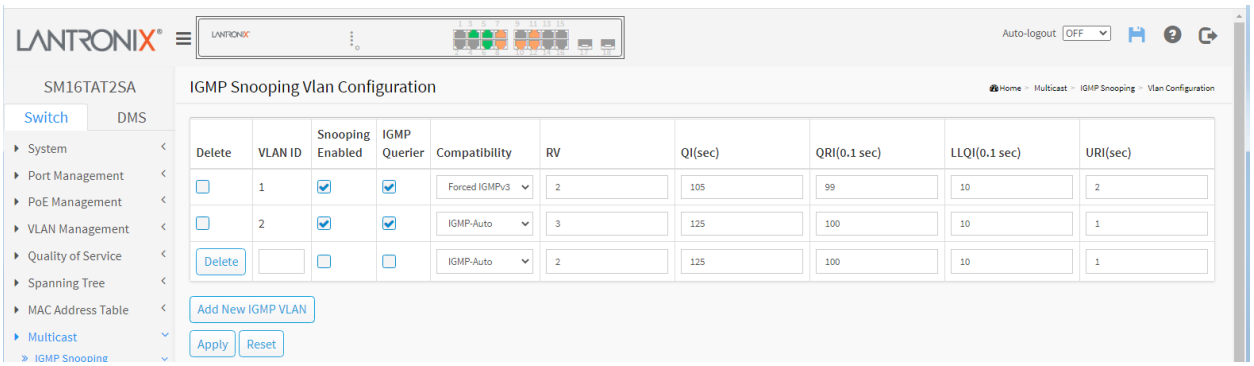


Figure 10-1.2: IGMP Snooping VLAN Configuration

Parameter descriptions:

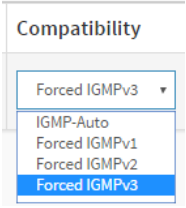
Start from Vlan: Click to refresh the displayed table starting from the "VLAN" input fields.

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

VLAN ID: Displays the VLAN ID (VID) of the entry.

Snooping Enabled: Enable the per-VLAN IGMP Snooping. Only up to 32 VLANs can be selected. .

IGMP Querier: Enable to join IGMP Querier election in the VLAN. Disable to act as an IGMP Non-Querier.



Compatibility: Compatibility is maintained by hosts and routers taking appropriate actions depending on the versions of IGMP operating on hosts and routers within a network. The allowed selections are IGMP-Auto, Forced IGMPv1, Forced IGMPv2, Forced IGMPv3. The default is IGMP-Auto.

IGMP **v1** is specified in RFC-1112; it was the first widely-deployed version and the first version to become an Internet Standard.
IGMP **v2**, specified in RFC-2236, added the ability for a host to signal desire to leave a multicast group.
IGMP **v3**, specified in RFC 3376, adds support for "source filtering", that is, the ability for a system to report interest in receiving packets *only* from specific source addresses, or from *all but* specific source addresses, sent to a particular multicast address.

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; default query interval is 125 seconds.

QRI(0.1 sec): Query Response Interval. The Max Response Time used to calculate the Max Resp Code inserted into the periodic General Queries. The allowed range is 0 to 31744 in tenths of seconds; the default QRI is 100 in tenths of a second (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 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; the default URI is 1 second.

Buttons

Add New IGMP VLAN : Click to add a new IMCP VLAN entry to the table.

Apply: Click to save changes.

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

10-1.3 Status

After you complete the IGMP Snooping configuration, you can view the IGMP Snooping Status. This page displays the IGMP Snooping detail status.

To display the IGMP Snooping status in the web UI:

1. Click Multicast, IGMP Snooping, and Status.
2. To auto-refresh the information, set "Auto-refresh" to On.
3. Click "Refresh" to refresh the IGMP Snooping Status.

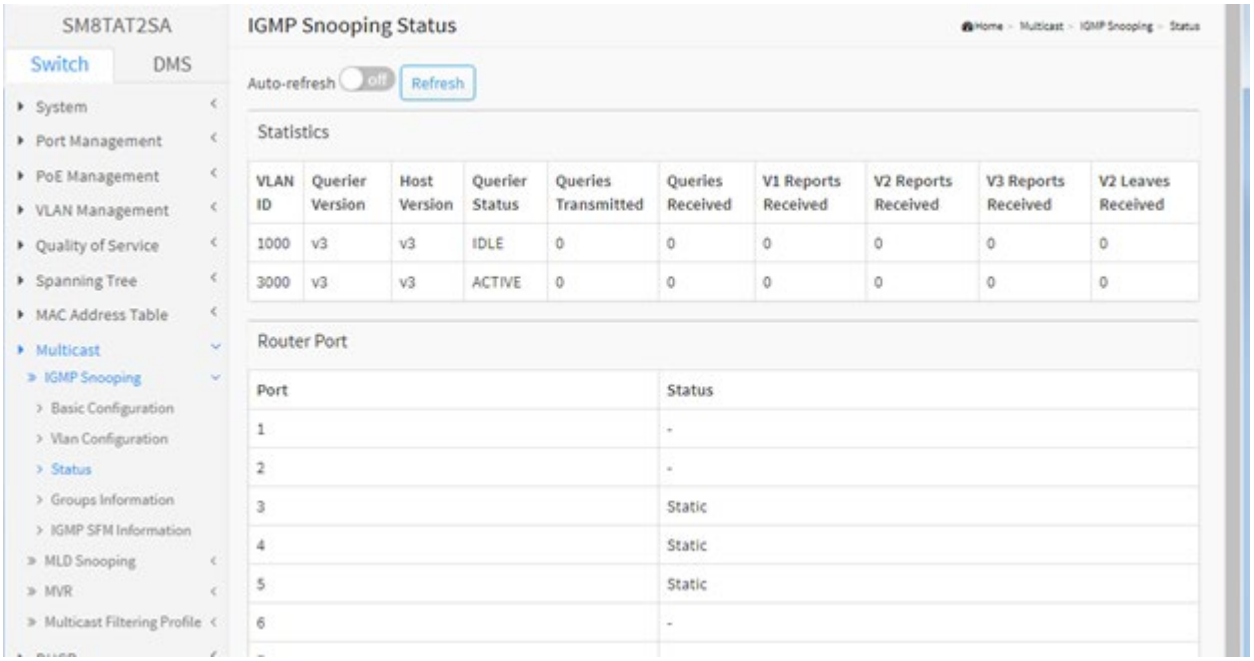


Figure 10-1.3: IGMP Snooping Status

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". "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: This section 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 to refresh the page automatically every 3 seconds.

Refresh: Click to manually refresh the page immediately.

10-1.4 Group Information

After you complete setting the IGMP Snooping function, you can view the IGMP Snooping Group Information. Entries in the IGMP Group Table are shown on this page. The IGMP Group Table is sorted first by VLAN ID, and then by group. When the end is reached the text "*No more entries*" is shown in the displayed table.

Group Member behavior: in order to be compatible with older version routers, IGMPv3 hosts must operate in version 1 and version 2 compatibility modes. IGMPv3 hosts MUST keep state per local interface regarding the compatibility mode of each attached network. A host's compatibility mode is determined from the Host Compatibility Mode variable which can be in one of three states: IGMPv1, IGMPv2 or IGMPv3. This variable is kept per interface and depends on the version of General Queries heard on that interface as well as the older querier present timers for the interface.

Web Interface

To display the IGMP Snooping Group Information in the web UI:

1. Click Multicast, IGMP Snooping, and Groups Information.
2. Specify how many entries to show in one page.
3. Click Previous or Next to change pages.

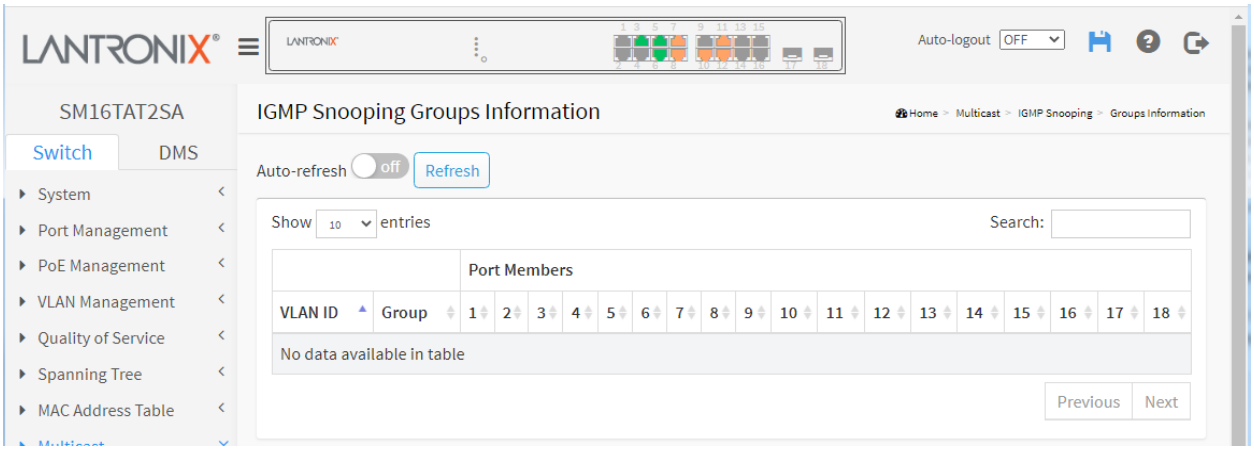


Figure 10-1.4: IGMP Snooping Groups Information

Parameter descriptions:

VLAN ID: VLAN ID of the group.

Groups: Group address of the group displayed.

Port Members: Ports under this group.

Buttons

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

Refresh : Click to manually refresh the page immediately.

Previous : Updates the system log entries, turn to the previous page.

Next : Updates the system log entries, turn to the next page.

10-1.5 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 being 20, selected through the "entries per page" input field. When first visited, the web page will show the first 20 entries from the beginning of the IGMP SFM Information table.

The "Start from VLAN", and "group" input fields allow the user to select the starting point in the IGMP SFM Information Table. Clicking the Next 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 Previous button click - assume the value of the first displayed entry, allowing for continuous refresh with the same start address.

Web Interface

To display IGMP SFM Information in the web UI:

1. Click Multicast, IGMP Snooping, and IGMP SFM Information.
2. To automatically refresh the information click “Auto-refresh”.
3. Click “Refresh” to refresh an entry of the IGMP Snooping Groups Information.
4. Click Previous or Next to change pages.

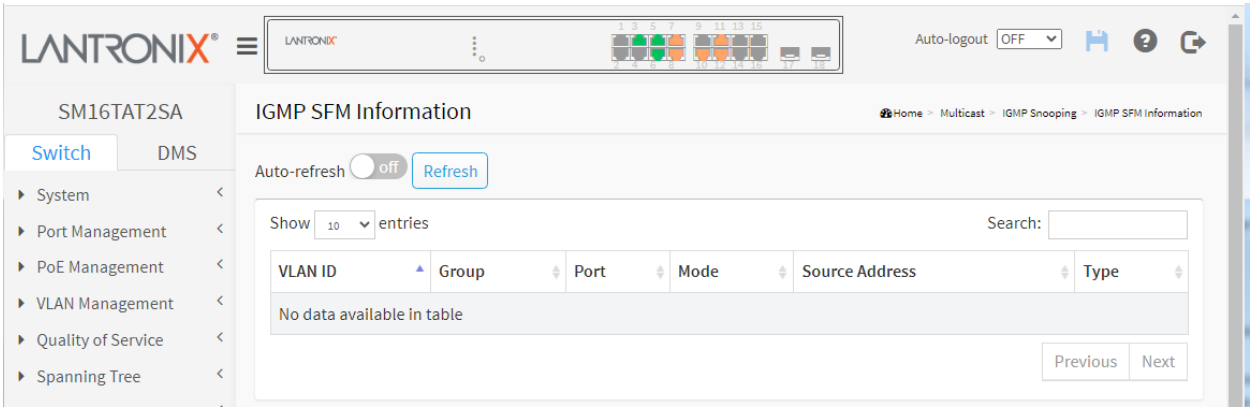


Figure 10-1.5: IGMP SFM Information

Parameter descriptions:

Search : You can search for the information that you want to view.

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

VLAN ID : VLAN ID of the group.

Group : Group address of the group displayed.

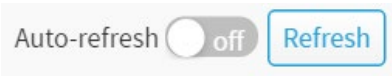
Port : Switch port number.

Mode : Indicates the filtering mode maintained per (VLAN ID, port number, Group Address) basis. It can be either Include or Exclude.

Source Address : IP Address of the source. Currently, system limits the total number of IP source addresses for filtering to be 128.

Type : Indicates the Type. It can be either ***Allow*** or ***Deny***.

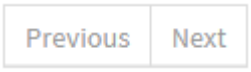
Buttons



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

Refresh : Click to manually refresh the page immediately.

Previous : Updates the system log entries, turn to the previous page.



Next : Updates the system log entries, turn to the next page.

10-2 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.

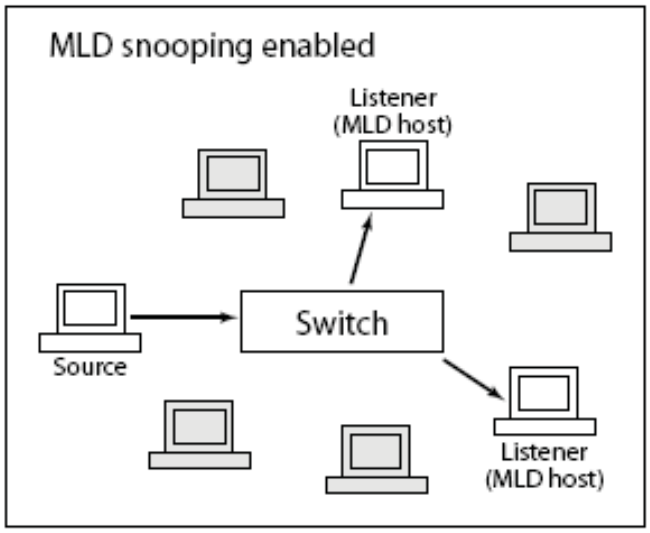


Figure 10-2: MLD Snooping enabled

10-2.1 Basic Configuration

This page let you configure the MLD Snooping basic configuration and the parameters.

Web Interface

To configure MLD Snooping in the web UI:

1. Click Multicast, MLD Snooping, and Basic Configuration.
2. Select “on” to enable Snooping globally and configure the parameters.
3. Select the port to join Router Port and Fast Leave.
4. At the Throttling mode dropdown select unlimited or 1 to 10.
5. Click the Apply button to save the settings.
6. To cancel the settings, click the Reset button to revert to previously saved values.

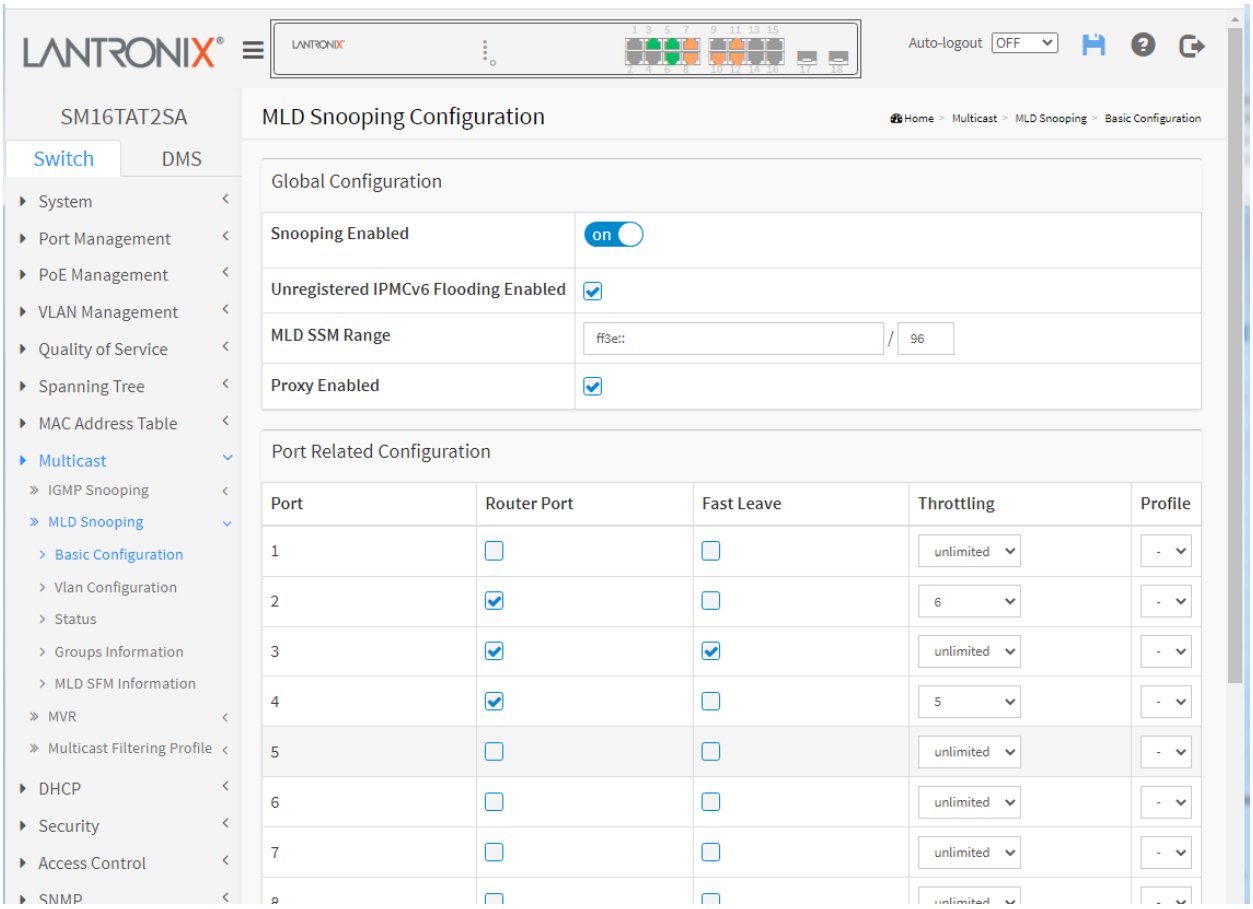


Figure 10-2.1: MLD Snooping Basic Configuration

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, then 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.

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: Check the box to enable Fast Leave on the port.

Throttling: Enable to limit the number of multicast groups to which a switch port can belong.

Profile: You can select 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.

10-2.2 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

To configure MLD Snooping VLAN in the web UI:

1. Click Multicast, MLD Snooping, and VLAN Configuration.
2. Click the Add New MLD VLAN button.
3. Specify the VLAN ID parameters.

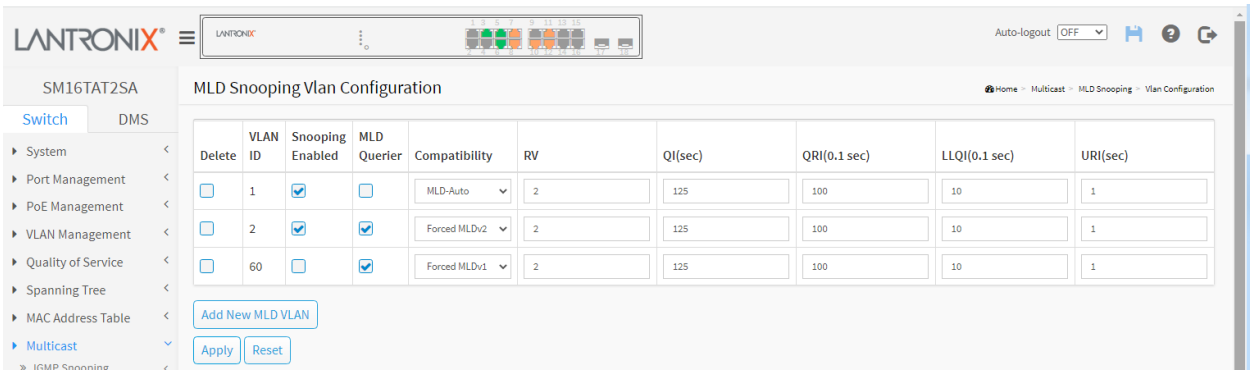


Figure 10-2.2: MLD Snooping VLAN Configuration

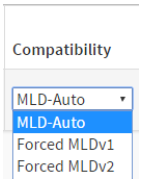
Parameter descriptions:

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

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

Snooping Enabled: Enable the per-VLAN IGMP Snooping. Up to 32 VLANs can be selected.

MLD Querier: Enable to join IGMP Querier election in the VLAN. Disable to act as an IGMP Non-Querier.



Compatibility: Compatibility is maintained by hosts and routers taking appropriate actions depending on the versions of IGMP operating on hosts and routers within a network. The allowed selections are MLD-Auto, Forced MLD v1, Forced MLD v2. The default compatibility value is MLD-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 robustness variable 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 query interval 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; default query response interval is 100 in tenths of seconds (10 seconds).

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

URI(sec): Unsolicited Report Interval. The URI 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 unsolicited report interval is 1 second.

Buttons

Add New MLD VLAN : Click to add a new instance to the table for configuration.

Apply: Click to save changes.

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

10-2.3 Status

This page lets you view MLD Snooping Status and detail information. To display MLD Snooping Status in the web UI:

1. Click Multicast, MLD Snooping, and Status.
2. To automatically refresh the information select “on” at “Auto-refresh”.
3. Click “Refresh” to refresh an entry of the MLD Snooping Status Information.

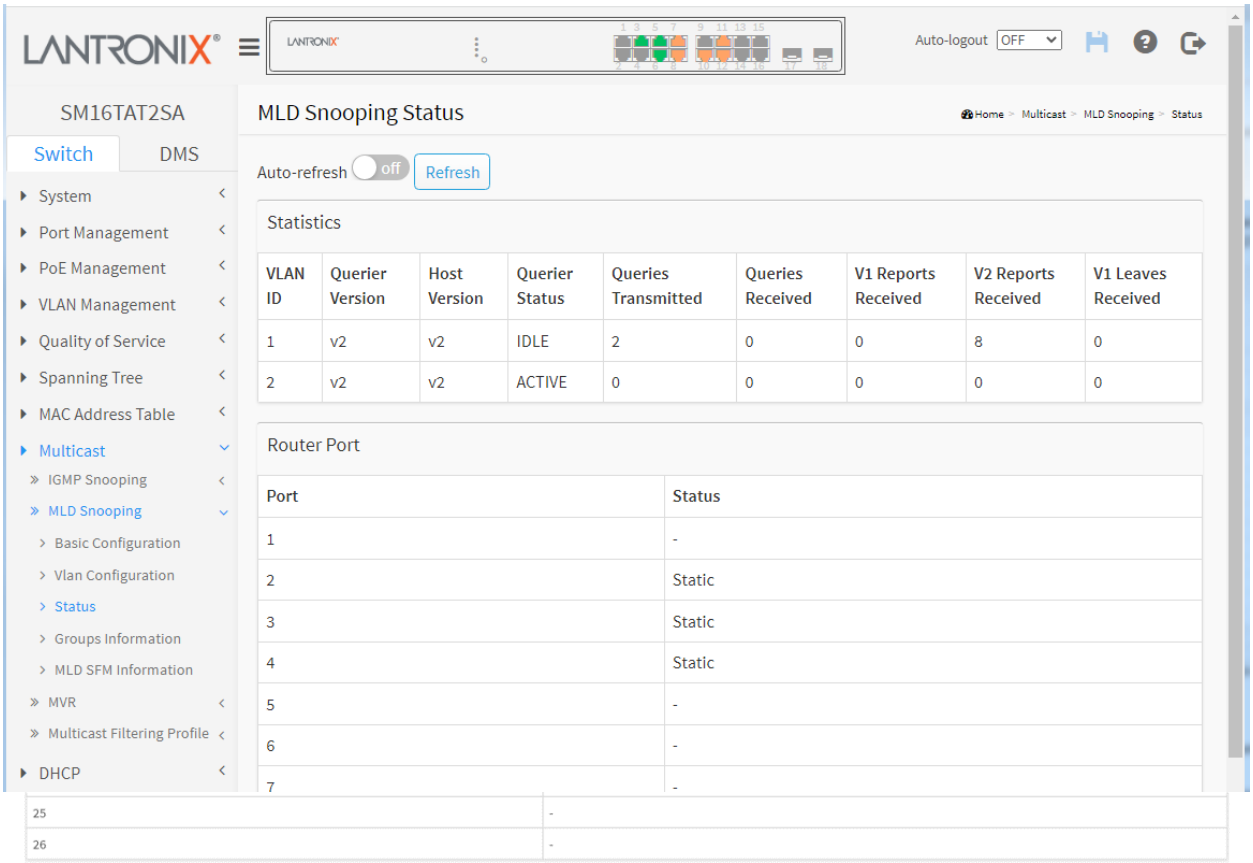


Figure 10-2.3: MLD Snooping Status

Parameter descriptions:

VLAN ID: The VLAN ID of the entry.

Querier Version: Working Querier Version currently.

Host Version: Working Host Version currently.

Querier Status : Show the Querier status is "ACTIVE" or "IDLE". "DISABLE" denotes the specific interface is administratively disabled.

Queries Transmitted: The number of Transmitted Queries.

Queries Received: The number of Received Queries.

V1 Reports Received: The number of Received V1 Reports.

V2 Reports Received: The number of Received V2 Reports.

V1 Leaves Received: The number of Received V1 Leaves.

Router Port: Display which ports act as router ports. A router port is a port on the Ethernet switch that leads towards the Layer 3 multicast device or MLD querier.

Static denotes the specific port is configured to be a router port.

Dynamic denotes the specific port is learnt to be a router port.

Both denote the specific port is configured or 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 to on to refresh the page automatically every 3 seconds.

Refresh: Click to manually refresh the page immediately.

10-2.4 Groups Information

This page lets you set MLD Snooping Groups Information. The "Start from VLAN", and "group" input fields let you select the starting point in the MLD Group Table.

Each page shows up to 99 entries from the MLD Group table, default being 20, selected through the "entries per page" input field. When first visited, the web page will show the first 20 entries from the beginning of the MLD Group Table.

To display MLD Snooping Group information in the web UI:

1. Click Multicast, MLD Snooping, and Group Information.
2. To auto-refresh the information select ”on” at “Auto-refresh”.
3. Click “Refresh” to refresh an entry of the MLD Snooping Group Information.

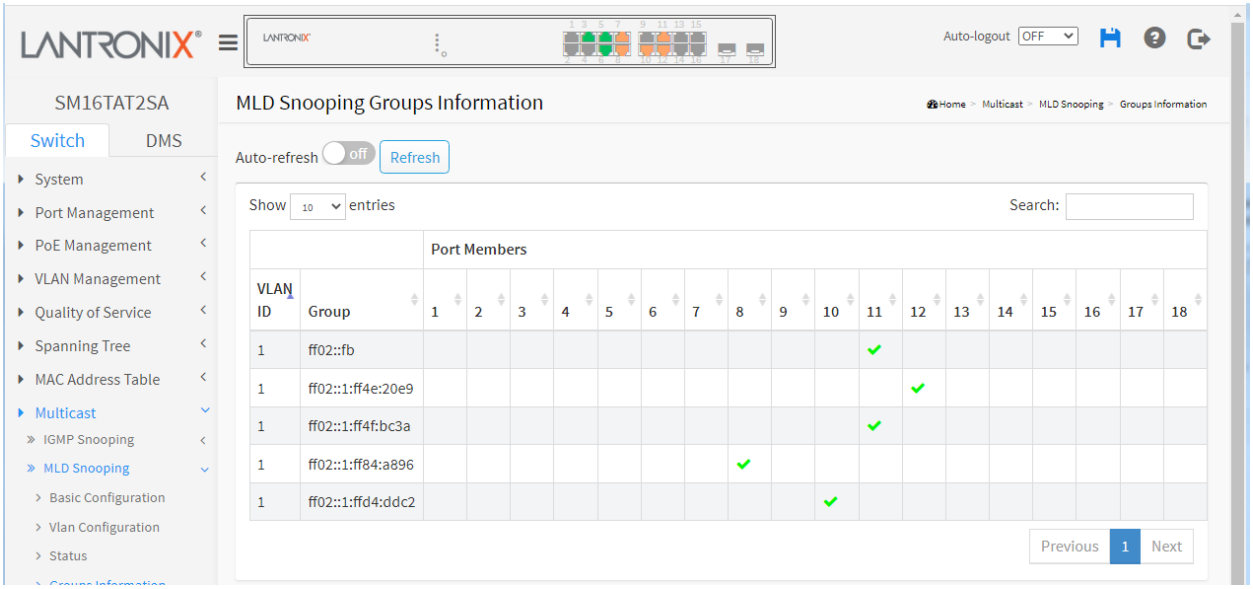


Figure 10-2.4: MLD Snooping Groups Information

Parameter descriptions:

VLAN ID: VLAN ID of the group.

Groups: Group address of the group displayed.

Port Members: Ports under this group.

Show entries: Choose how many items you want to view per page.

Buttons

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

Refresh: Click to manually refresh the page immediately.

10-2.5 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 that 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. To auto-refresh the information click Auto-refresh “On”.
3. Click “Refresh” to refresh an entry of the MLD SFM Information.

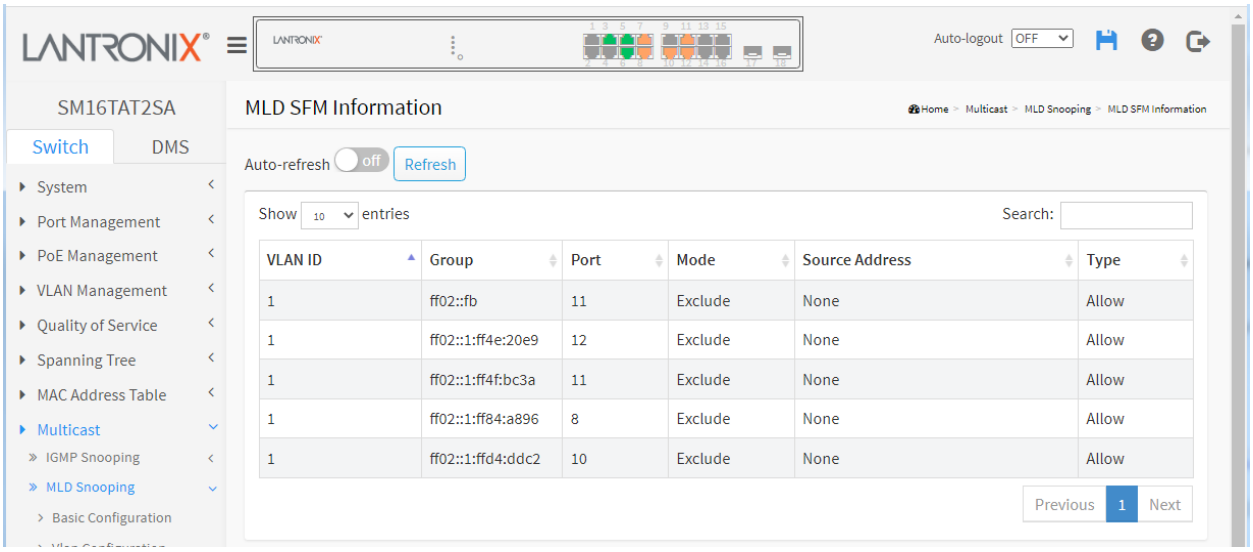


Figure 10-2.5: MLD SFM Information

Parameter descriptions:

VLAN ID: VLAN ID of the group.

Group: Group address of the group displayed.

Port: Switch port number.

Mode: Indicates the filtering mode maintained per (VLAN ID, port number, Group Address) basis. It can be either Include or Exclude.

Source Address: **The** IP Address of the source. Currently, the system limits the total number of IP source addresses for filtering to be 128.

Type: Indicates the Type. It can be either Allow or Deny.

Show entries: You can choose how many items you want to display.

Buttons

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

Refresh: Click to manually refresh the page immediately.

10.3 Multicast Filtering Profile

ICMP (Internet Control Message Protocol) generates error response, diagnostic, or routing messages. ICMP messages contain information on routing difficulties or simple exchanges such as time-stamp or echo transactions.

IGMP Snooping is used to establish the multicast groups to forward the multicast packet to the member ports. It avoids wasting the bandwidth when IP multicast packets are running over the network. A switch that does not support IGMP or IGMP Snooping cannot tell the multicast packet from the broadcast packet, so it can only treat them all as broadcast packets. Without IGMP Snooping, the multicast packet forwarding function is inactive and all packets are treated as broadcast packets.

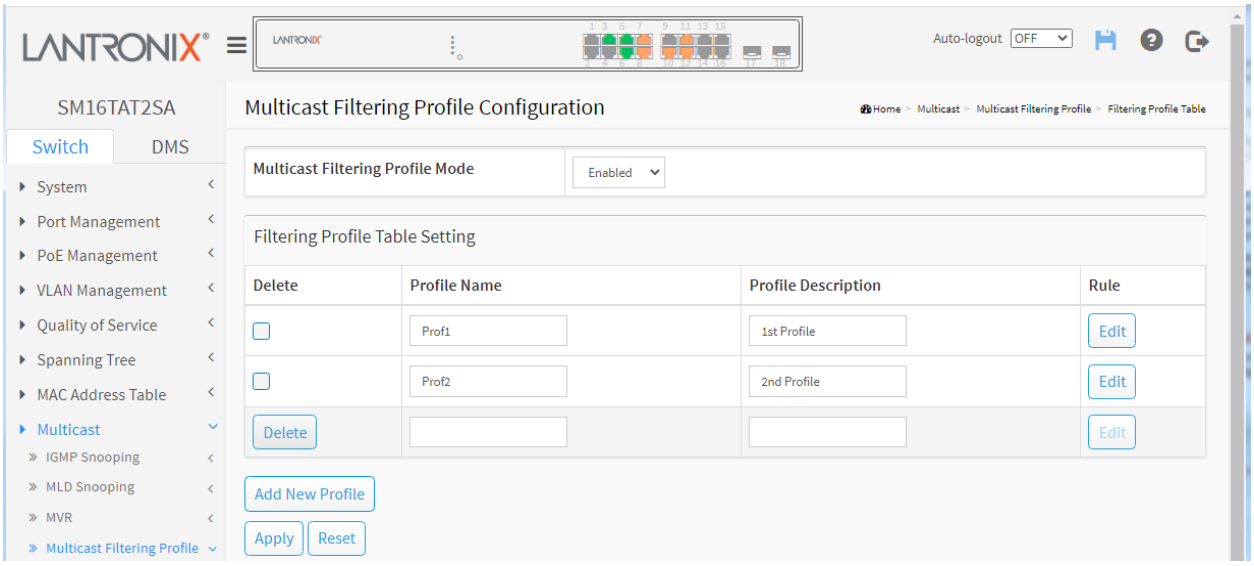
A switch that supports IGMP Snooping can query, report, and leave a packet exchanged between an IP Multicast Router/Switch and an IP Multicast Host, and can update the information of the Multicast table when a member (port) joins or leaves an IP Multicast Destination Address. With this function, once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

The packets will be discarded by IGMP Snooping if the user transmits multicast packets to the multicast group that was not 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.

10.3-1 Switch > Multicast > Multicast Filtering Profile > Filtering Profile Table

The IPMC profile is used to deploy the access control on IP multicast streams. You can create a maximum of 64 Profiles and a maximum 128 corresponding rules for each at the Multicast Filtering Profile Configuration table.

Click the Add New Profile button to display the configurable parameters.



Parameter descriptions:

Multicast Filtering Profile Mode: Enable/Disable the Global IPMC Profile. The system starts to do filtering based on profile settings only when the global profile mode is enabled. Select to Disable or Enable globally. The default is Disabled.

Filtering Profile Table Setting

Delete: Click to delete the entry. The designated entry will be deleted during the next apply.

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. Enter a name for the new IPMC profile. Avoid spaces between characters.

Profile Description: Enter a description of the new IPMC profile. Additional description, which is composed of at maximum 64 alphabetic and numeric characters, about the profile. No blank or space characters are permitted as part of description. Use "_" or "-" to separate the description sentence.

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

- List the rules associated with the designated profile.
- Adjust the rules associated with the designated profile.

Enter the parameters and click the **Apply** button, then click the **Edit** button, then click the Add Last Rule button to display the MC Filtering Profile Rule Configuration Rule Settings table (In Precedence Order).

Buttons:

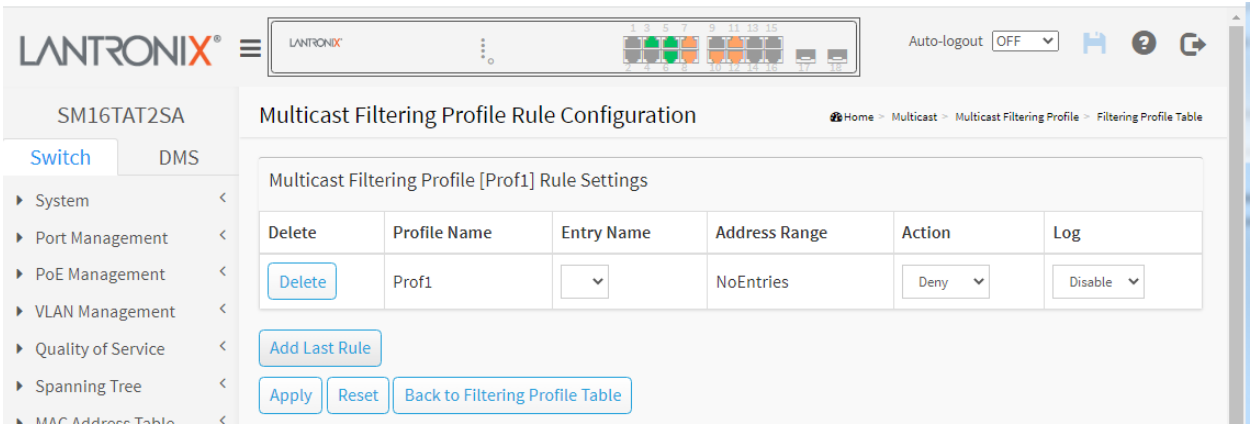
Add New Profile: Click to add new profile. Specify the name and configure the new entry.

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.

Multicast Filtering Profile Rule Configuration: At the Multicast Filtering Profile [4] Rule Settings page click the
Edit button in the Rule column of the table to display the Multicast Filtering Profile Rule Configuration table.
Click the Add Last Rule button to display the Multicast Filtering Profile Rule Configuration page:



The IPMC profile is used to deploy the access control on IP multicast streams. It is allowed to create at maximum 64 Profiles with at maximum 128 corresponding rules for each.

Parameter descriptions:

Profile Name: The name of the designated profile to be associated. This field is not editable.

Entry Name: The name used in specifying the address range used for this rule. Only the existing profile address entries will be chosen in the selected box. This field is not allowed to be selected as none ("-") while the Rule Settings Table is committed.

Address Range: The corresponding address range of the selected profile entry. This field is not editable and will be adjusted automatically according to the selected profile entry.

Action: Select 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: Select 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.

Buttons

Add Last Rule: Click to add a new rule in the end of the specific profile's rule list. Specify the address entry and configure the new entry. Click "Apply".

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

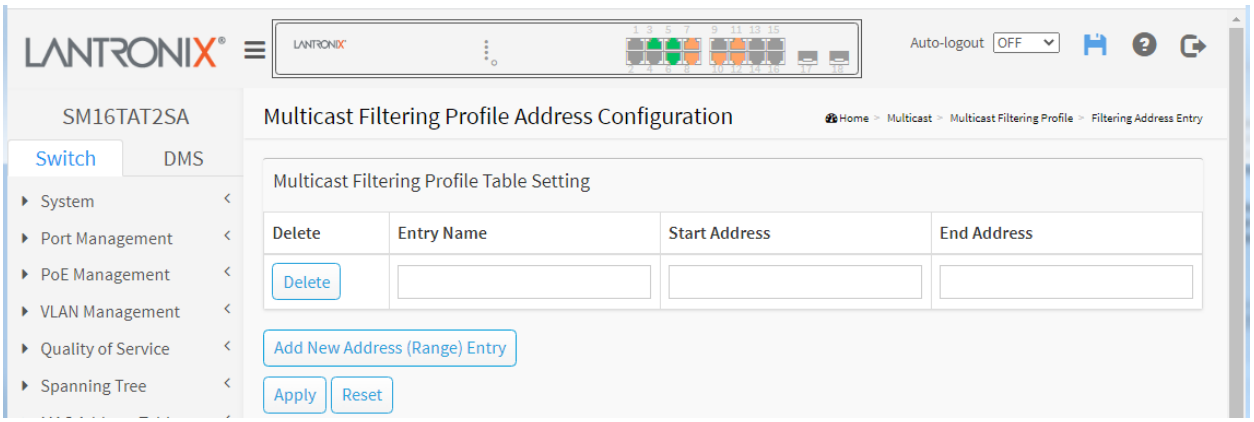
Apply: Click to save changes.

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

Back to Filtering Profile Table: Click to return to previous page with no changes.

10.3-1 Switch > Multicast > Multicast Filtering Profile > Filtering Address Entry

This page provides address range settings used in Multicast Filtering profile. The address entry is used to specify the address range that will be associated with Multicast Filtering Profile. You can create up to 128 address entries in the system.



Parameter descriptions:

Delete: Click to delete the entry. The designated entry will be deleted during the next apply.

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

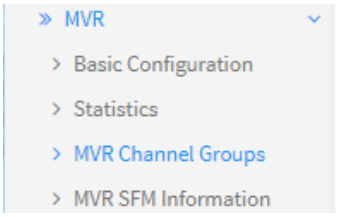
Add New Address (Range) Entry: Click to add a new address range. Specify the name and configure the addresses, then click "Apply".

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.

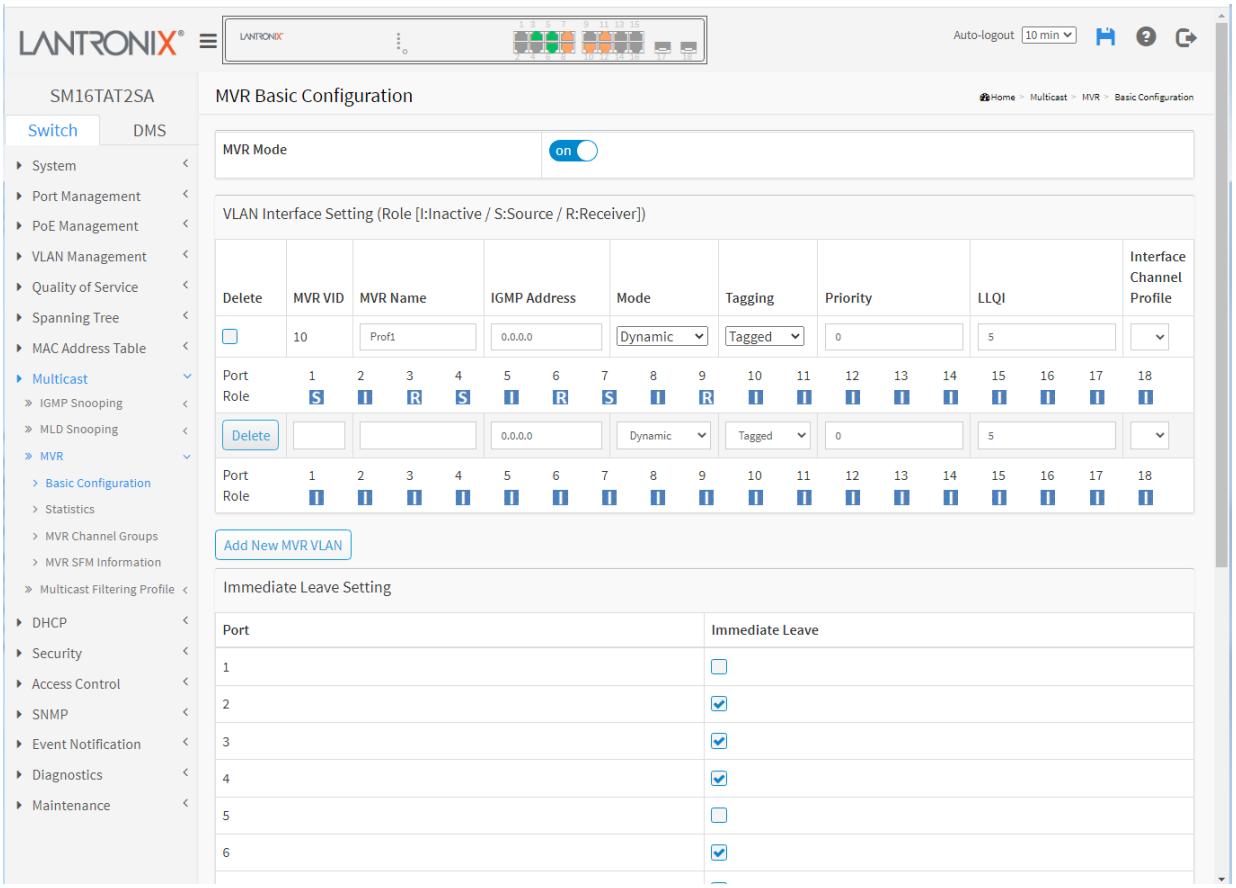
10.4 MVR



Multi VLAN Registration allows switches to automatically discover some of the VLAN information that would otherwise need to be manually configured. The MVR feature enables multicast traffic forwarding on the Multicast VLAN. In a multicast television application, a PC or a television with a set-top box can receive the multicast stream.

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

10.4-1 Switch > MVR > Basic Configuration:



Global Setting

MVR Mode: Select **on** or **off**. The default is **off**. Enable/Disable the Global MVR. The Unregistered Flooding control depends on the current configuration in IGMP/MLD Snooping. It is suggested to enable Unregistered Flooding control when the MVR group table is full.

VLAN Interface Setting (Role [I:Inactive / S:Source / R:Receiver])

MVR VID: Enter the new VLAN ID for this new MVR VLAN. Caution: MVR source ports are not recommended to be overlapped with management VLAN ports.

MVR Name: Enter a name for this new MVR VLAN. 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: e.g., 192.168.1.40. Define the IPv4 address as source address used in IP header for IGMP control frames. The default IGMP address is not set (0.0.0.0). When the IGMP address is not set, system uses IPv4 management address of the IP interface associated with this VLAN. When the IPv4 management address is not set, system uses the first available IPv4 management address. Otherwise, system uses a pre-defined value. By default, this value will be 192.0.2.1.

Mode: At the dropdown select **Dynamic** or **Compatible**. The default is **Dynamic**. 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: At the dropdown select **Tagged** or **Untagged**. The default is **Tagged**. Specify whether the traversed IGMP/MLD control frames will be sent as Untagged or Tagged with MVR VID.

Priority: Enter 0 - 7. 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: At the dropdown select an existing Profile name. When the MVR VLAN is created, select the profile to expand the corresponding multicast channel settings for the specific MVR VLAN. The file established on Filtering Profile Table.

Port: The logical port for the settings.

Port Role: For each port choose a Role; each click displays the next role (**I** = Inactive, **S** = Source role, and **R** = Receiver role). Configure an MVR port of the designated MVR VLAN as one of the following roles.

> ***Inactive***: The designated port does not participate MVR operations.
>
> ***Source***: Configure uplink ports that receive and send multicast data as source ports. Subscribers cannot be directly connected to source ports.
>
> ***Receiver***: Configure a port as a receiver port if it is a subscriber port and should only receive multicast data. It does not receive data unless it becomes a member of the multicast group by issuing IGMP/MLD messages.

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

Immediate Leave Setting

Port: The logical port for the settings.

Immediate Leave: Enable the fast leave on the port.

Buttons

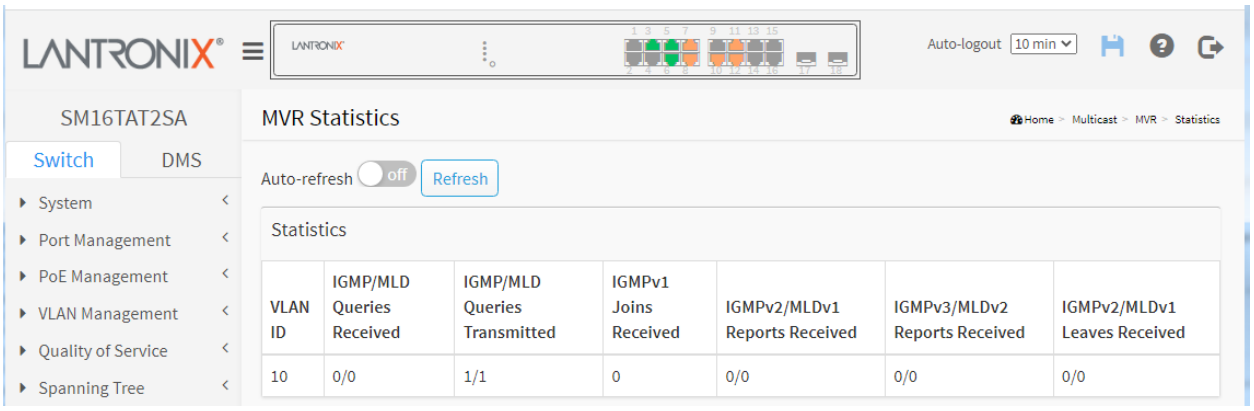
Add New MVR VLAN: Click to add a new MVR VLAN entry to the table. Specify MVR VID, MVR Name, IGMP Address, Mode, Tagging, Priority, LLQI, Interface Channel Profile. Click "Apply".

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

Apply: Click to save changes.

10.4-2 Switch > MVR > Statistics

This page displays the MVR detail Statistics that display after you have configured MVR on the switch. It provides detailed MVR Statistics Information.



VLAN ID: Displays the Multicast VID (VLAN ID).

I**GMP/MLD Queries Received**: The number of Received Queries for IGMP and MLD, respectively (e.g., x/y).

IGMP/MLD Queries Transmitted: The number of Transmitted Queries for IGMP and MLD, respectively (e.g., x/y).

IGMPv1 Joins Received: The number of Received IGMPv1 Joins (e.g., 1 Join received).

IGMPv2/MLDv1 Reports Received: The number of Received IGMPv2 Join's and MLDv1 Reports, respectively (e.g., x/y).

IGMPv3/MLDv2 Reports Received: The number of Received IGMPv3 Join's and MLDv2 Report's, respectively.(e.g., x/y).

IGMPv2/MLDv1 Leaves Received: The number of Received IGMPv2 Leave's and MLDv1 Dones, respectively (e.g., x/y).

Buttons

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

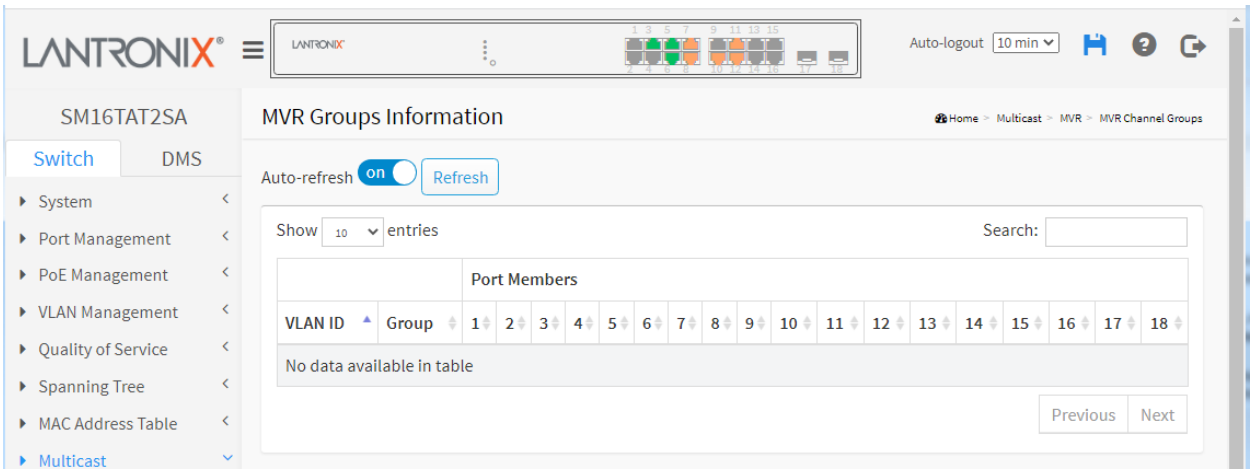
Refresh: Click to manually refresh the page immediately.

10.4-3 Switch > MVR > Group Information

This page displays MVR Groups detail information on the switch. Entries in the MVR Group Table are shown on this page. The MVR Group Table is sorted first by VLAN ID, and then by group.

Each page shows entries from the MVR Group table, default being 10, selected through the "entries per page" input field. When first visited, the web page will show the first 10 entries from the beginning of the MVR Channels (Groups) Information Table.

The "Search" input fields let you select the starting point in the MVR Channels (Groups) Information Table. It will update the displayed table starting from that or the closest next MVR Channels (Groups) Information Table match.



VLAN ID: Displays the VID (VLAN ID) of the group.

Group: Displays the Group ID of the group displayed.

Port Members: Indicates which ports are members (the Ports under this group).

Buttons

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

Search: You can search for the information that you want to see.

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

Refresh: Click to manually refresh the page immediately.

Previous: Updates the system log entries, turn to the previous page.

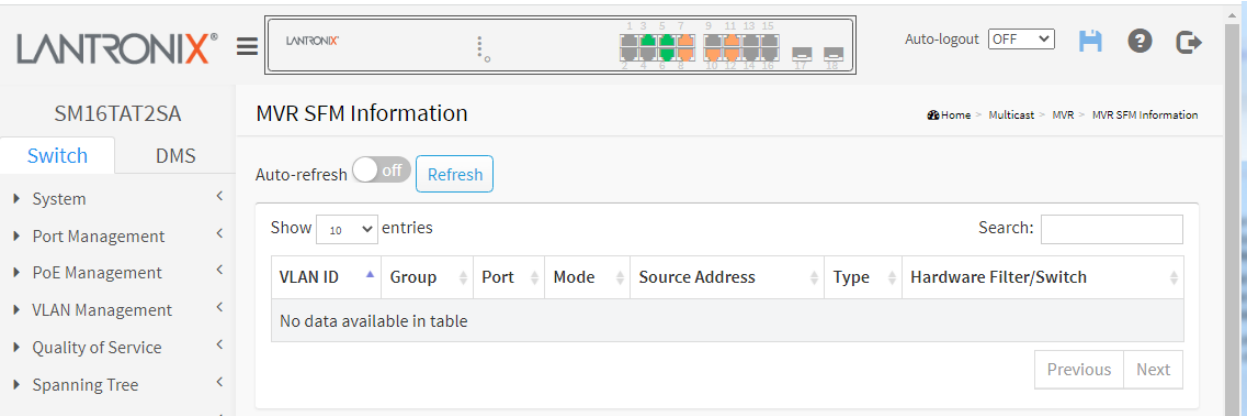
Next: Updates the system log entries, turn to the next page.

10.4-4 Switch > 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.

Each page shows up to 99 entries from the MVR SFM Information table, default being 10, selected through the "entries per page" input field. When first visited, the web page will show the first 10 entries from the beginning of the MVR SFM Information Table.

The "Search" input fields lets you select the starting point in the MVR SFM Information table. It will update the displayed table starting from that or the closest next MVR SFM Information table match.



VLAN ID: Displays the VID (VLAN ID) of the group.

Group: Displays the Group address of the group displayed.

Port: Indicates which ports are members.

Mode: Displays the filtering mode maintained per (VLAN ID, port number, Group Address) basis. It can be either Include or Exclude.

Source Address: Displays the 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: Displays the configured type (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 to refresh the page automatically every 3 seconds.

Refresh: Click to manually refresh the page immediately.

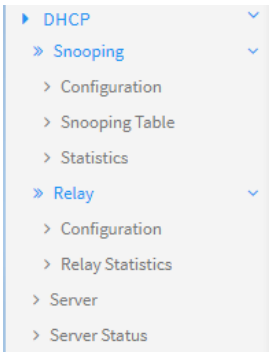
Show entries: You can choose how many items you want to show up.

Search: You can search for the information that you want to see.

Previous: Updates the system log entries, turn to the previous page.

Next: Updates the system log entries, turn to the next page.

Chapter 11 DHCP



This section lets you view and configure various DHCP parameters of the switch.
See also Appendix B DHCP Per Port on page 279.

11-1 Snooping

11-1.1 Configuration

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

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

Web Interface

To configure DHCP snooping in the web UI:

1. Click DHCP, Snooping, and Configuration.
2. Select "on" or "off" at the Snooping Mode selector.
3. Select "Trusted" or "Untrusted" for each port.
4. Click Apply.

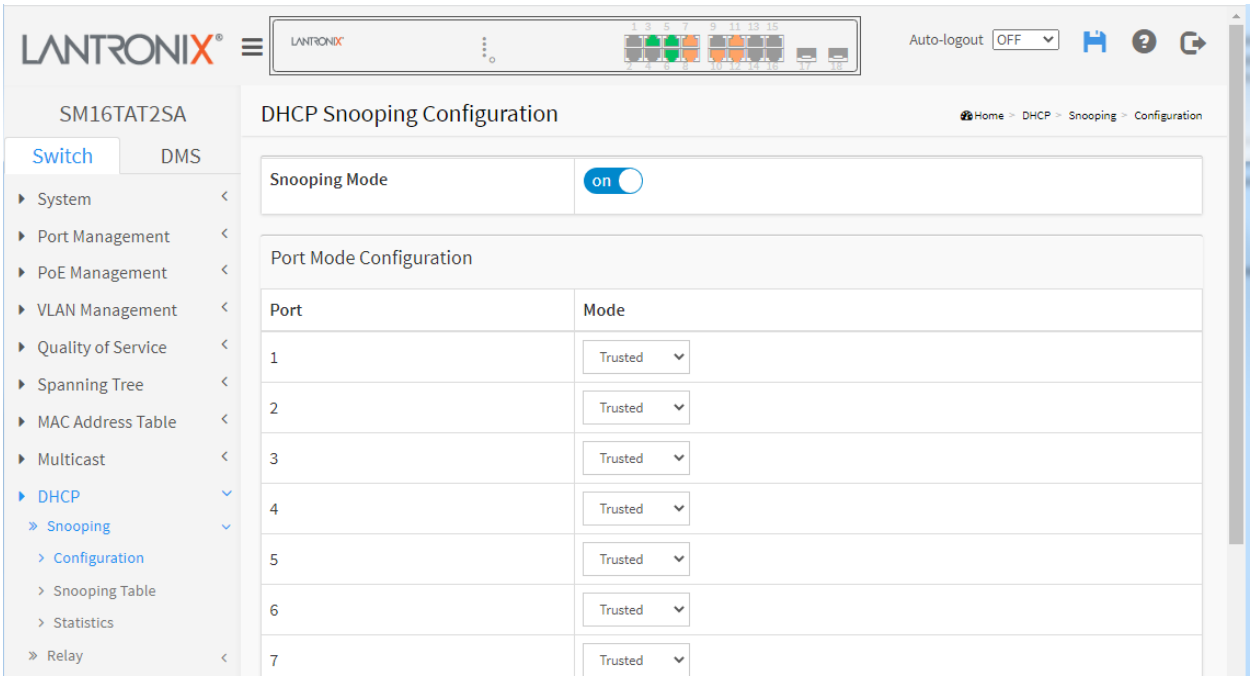


Figure 11-1.1: DHCP Snooping Configuration

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.

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

Buttons

Apply : Click to save changes.

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

11-1.2 Snooping Table

This page displays the dynamic IP assigned information after DHCP Snooping mode is disabled. All DHCP clients obtained the dynamic IP address from the DHCP server will be listed in this table except for local VLAN interface IP addresses. Entries in the Dynamic DHCP Snooping Table are shown on this page.

To view the Dynamic DHCP Snooping Table in the web UI:

1. Click DHCP, Snooping, and Snooping Table.
2. Use the buttons as needed.

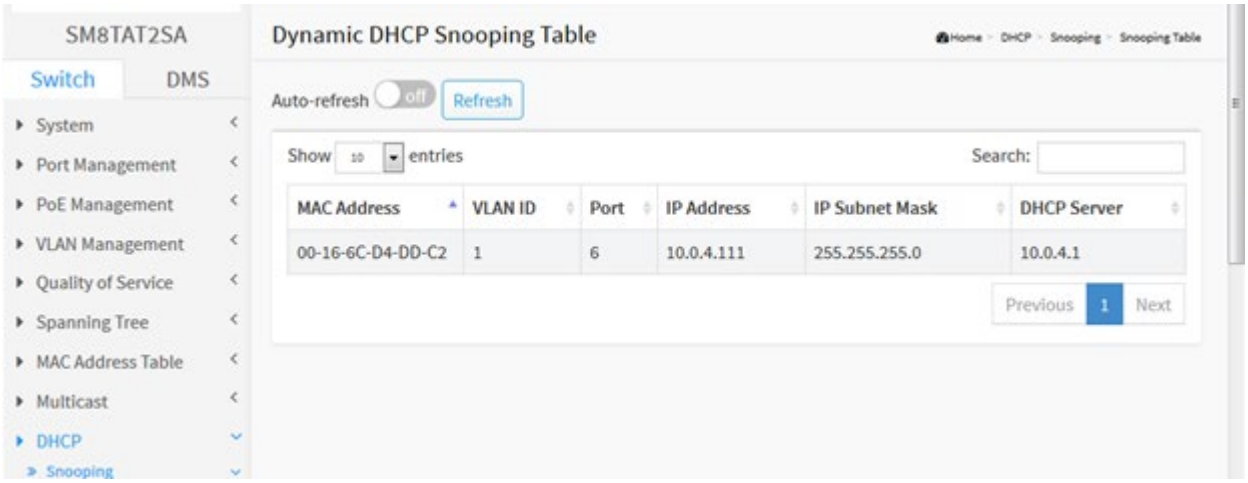


Figure 11-1.2: Dynamic DHCP Snooping Table

Parameter descriptions:

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

Search: You can search for the information that you want to see.

MAC Address: User MAC address of the entry.

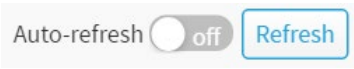
VLAN ID: VLAN-ID in which the DHCP traffic is permitted.

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 to refresh the page automatically every 3 seconds.

Refresh: Click to manually 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.

11-1.3 DHCP Detailed Statistics

This page provides statistics for DHCP snooping. Note that the normal forward per-port TX statistics are not increased if the incoming DHCP packet is done by L3 forwarding mechanism. Also, a clear of the statistics on a specific port may not take effect on global statistics since it gathers the different layer overview.

To view detailed DHCP statistics via the web UI:

1. Click DHCP, Snooping, and Detailed Statistics.
2. Use the Port select box to select the desired port.

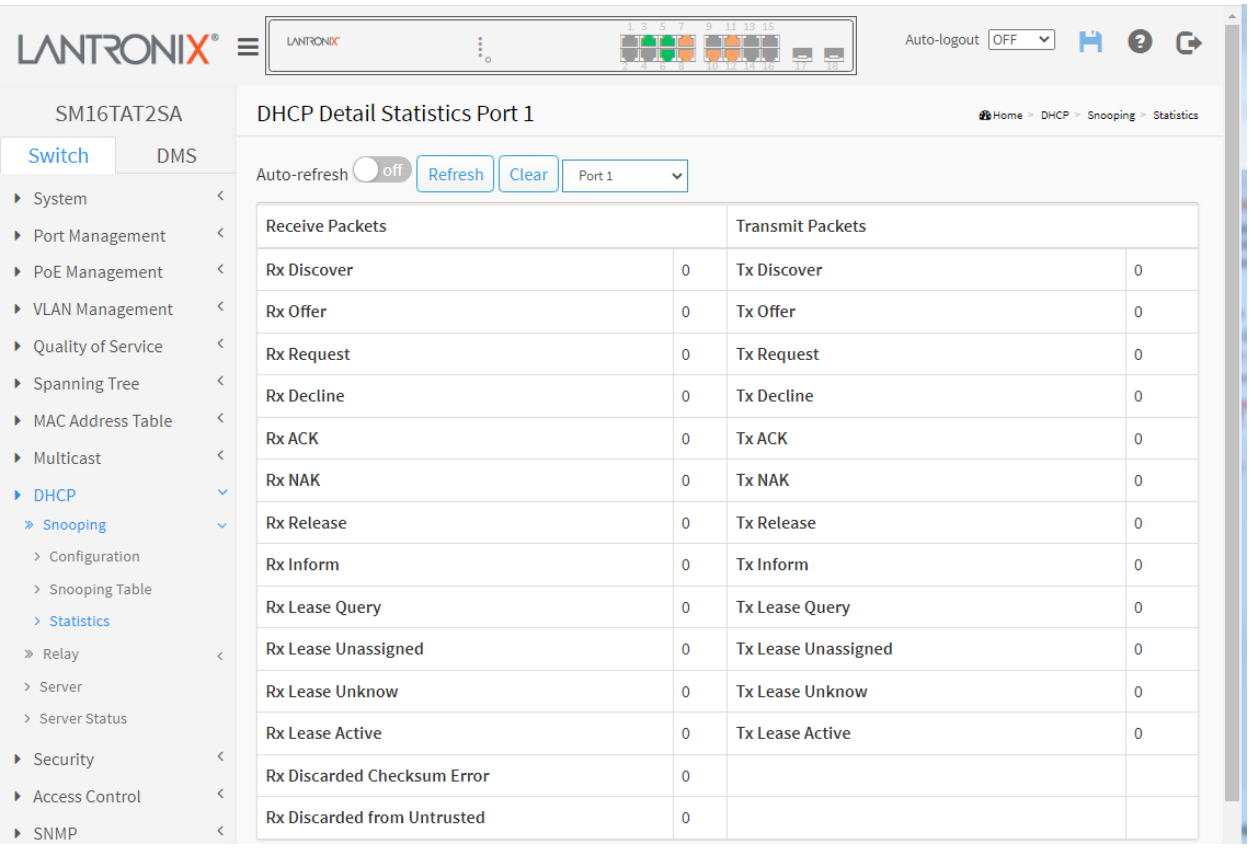


Figure 11-1.2: Dynamic DHCP Snooping Table

Parameter descriptions:

Rx and Tx Discover: The number of discover (option 53 with value 1) packets received and transmitted.

Rx and Tx Offer: The number of offer (option 53 with value 2) packets received and transmitted.

Rx and Tx Request: The number of request (option 53 with value 3) packets received and transmitted.

Rx and Tx Decline: The number of decline (option 53 with value 4) packets received and transmitted.

Rx and Tx ACK: The number of ACK (option 53 with value 5) packets received and transmitted.

Rx and Tx NAK: The number of NAK (option 53 with value 6) packets received and transmitted.

Rx and Tx Release: The number of release (option 53 with value 7) packets received and transmitted.

Rx and Tx Inform: The number of inform (option 53 with value 8) packets received and transmitted.

Rx and Tx Lease Query: The number of lease query (option 53 with value 10) packets received and transmitted.

Rx and Tx Lease Unassigned: The number of lease unassigned (option 53 with value 11) packets received and transmitted.

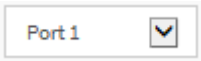
Rx and Tx Lease Unknown: The number of lease unknown (option 53 with value 12) packets received and transmitted.

Rx and Tx Lease Active: The number of lease active (option 53 with value 13) packets received and transmitted.

Rx Discarded checksum error: The number of discard packet that IP/UDP checksum is error.

Rx Discarded from Untrusted: The number of discarded packets that are coming from untrusted port.

Buttons



: Use the Port select box to select the port that you want to display the DHCP Detailed Statistics.

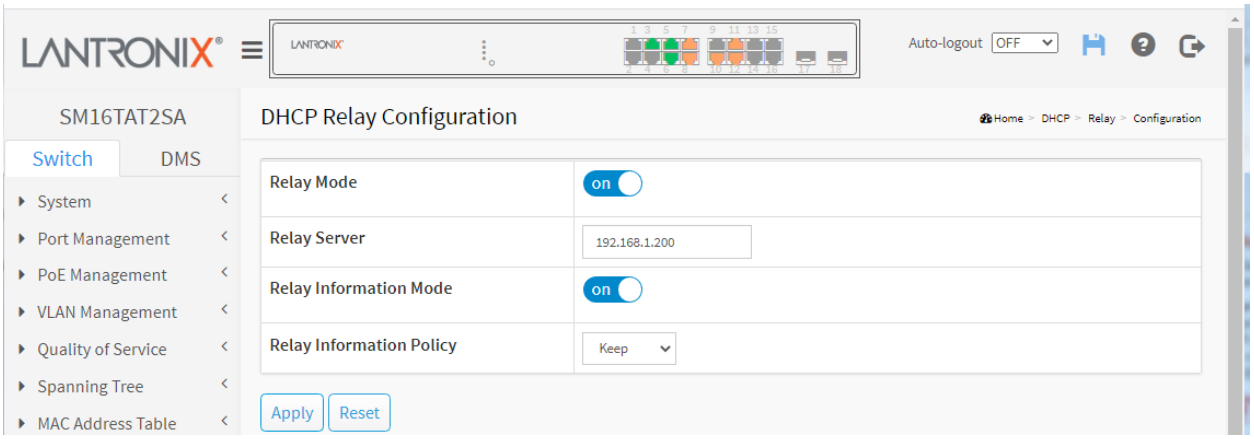
Auto-refresh: Check to refresh the page automatically every 3 seconds.

Refresh: Click to manually refresh the page immediately.

11-1.4 DHCP Relay Configuration

Navigate to the Switch > DHCP > Relay menu path to display the DHCP Relay Configuration table. Here you can configure the DHCP Relay function.

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.



Parameters:

Relay Mode: Select on or off. The default is off. Indicates the DHCP relay mode operation. Possible modes are:

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

Relay Server: Enter the DHCP Relay server IP address.

Relay Information Mode: Select on or off. The default is off. Indicates the DHCP relay information mode option operation. The option 82 circuit ID format as "[vlan_id][module_id][port_no]". The first four characters represent the VLAN ID, the fifth and sixth characters are the module ID (always 0), 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 operation.

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

Possible modes 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.

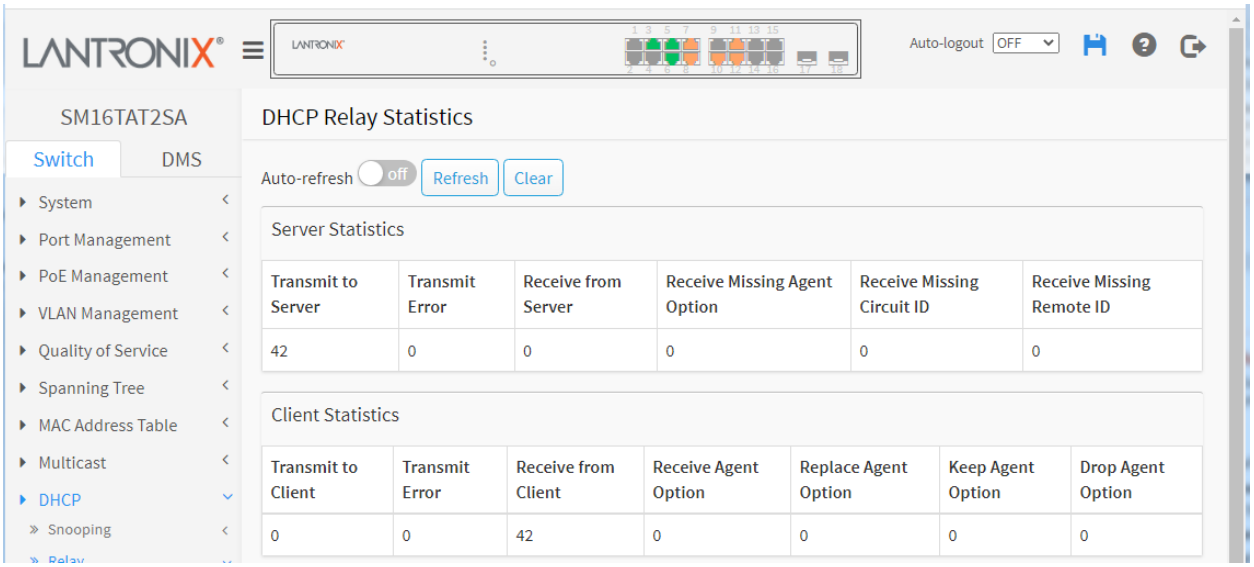
Buttons

Apply: Click to save changes.

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

11-1.5 DHCP Relay Statistics

Navigate to the Switch > DHCP > Relay > Relay Statistics menu path to display the DHCP Relay Statistics table. This page provides statistics for DHCP relay.



Server Statistics Parameters:

Transmit to Server: The number of packets that are relayed from client to server.

Transmit Error: The number of packets that resulted in error while being relayed from client to server.

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.

Client Statistics Parameters:

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 to refresh the page automatically every 3 seconds.

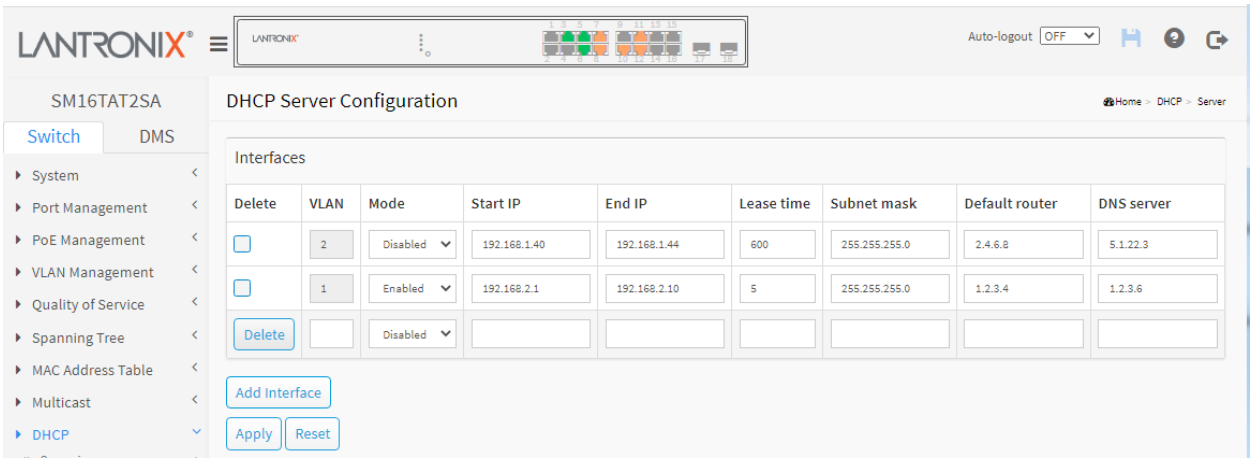
Refresh: Click to manually refresh the page immediately.

Clear: Click to clear the page data.

11-1.6 DHCP Server

Navigate to the Switch > DHCP > Server menu path to display the DHCP Server Configuration table. Here you can add and configure new DHCP servers. Click the Add Interface button to start.

This page lets you enable or disable DHCP servers per system and per VLAN and configure Start IP and End IP addresses. A DHCP server will allocate these IP addresses to the DHCP client and deliver configuration parameters to the DHCP client.



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

VLAN: Enter the VLAN ID (VID) for this instance. Configure the VLAN in which DHCP server is enabled or disabled. Allowed VLAN are in the range 1 – 4095.

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

Enable: Enable DHCP server per VLAN.

Disable: Disable DHCP server per VLAN. The default is Disabled.

Start IP: Enter the starting IP address for the range. The Start IP must be smaller than or equal to the End IP.

End IP: Enter the ending IP address for the range.

Lease time: Enter a valid DHCP lease time of the DHCP Server. Value range between 1 and 8640000 hours.

Subnet mask: Enter the Subnet mask.

Default router: Enter the default router IP address.

DNS server: Enter the destination IP network or host address of this route.

Subnet Mask: Configure subnet mask of the DHCP address.

Buttons

Add Interface: Click the button to create and configure an instance.

Apply: Click to save changes.

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

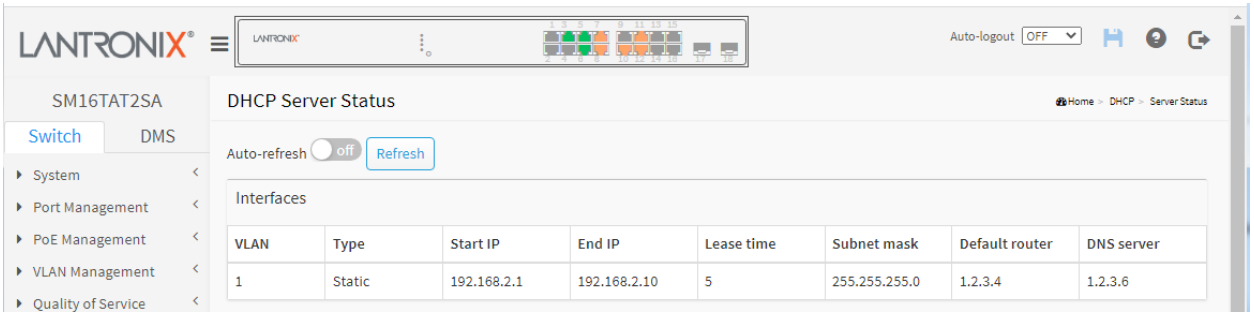
Messages:

This field is required.

ERROR: Not Found

11-1.7 DHCP Server Status

Navigate to the Switch > DHCP > Server Status menu path to display the current DHCP Server Status.



Parameters:

VLAN: The VLAN ID of the entry.

Type: Indicates the operation type per VLAN. Possible types are: Static and DMS.

Start IP and **End IP**: Display the Start IP and the End IP.

Lease time: Displays lease time of the pool.

Subnet mask: Displays subnet mask of the DHCP address.

Default router: Displays the destination IP network or host address of this route.

DNS server: Displays DNS server.

Buttons

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

Refresh: Click to manually refresh the page immediately.

Chapter 12 Percepxion and LPM

This page lets you configure Percepxion parameters. This page has four sections: the Status, Configuration, and Percepxion Connection 1 and Connection 2 sections as shown and described below.

Percepxion is Lantronix cloud-hosted or on-premise management platform that provides a single pane of glass for centralized management and automated monitoring of deployed Lantronix products, along with real-time notifications, managed APIs and data dashboards. For more information see https://www.lantronix.com/percepxion/.

Lantronix Provisioning Manager (LPM) is a software application that provisions, configures and updates Lantronix devices for local site installations and deployments. LPM discovery is enabled by default and is not configurable. For more LPM information see https://www.lantronix.com/products/lantronix-provisioning-manager/.

There are three pieces of information that the Percepxion client needs to complete registration and to publish data and configuration to the Percepxion server: Serial Number, Device ID, and Device Key. The Serial Number is always preprogrammed on the device (typically derived from the MAC address of the first Ethernet port). A new device would also be preprogrammed with the Device ID and Key.
For existing devices where the ID and Key are not pre-programmed, LPM uses Lantronix proprietary search and query protocol to get the device serial number, and then uses the switch REST API interface to set the Device ID and Device Key.

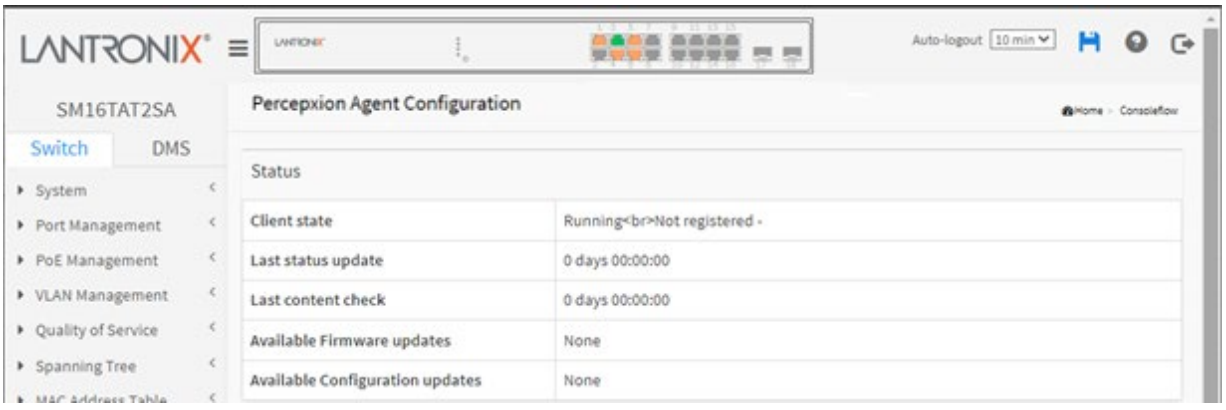
12-1 Supported Firmware Versions

Devices must meet firmware requirements in order to work with Percepxion and LPM. The SMxTAT2SA requires firmware v1.04.0110 or above.

12-2 Percepxion Agent Configuration

Navigate to Configuration > Percepxion > Percepxion Configuration to display the Percepxion Agent Configuration page:

Status section:



Parameter descriptions:

Client state: Displays the existing Percepxion client state (e.g., *Exited*, *Active, Inactive, Running,* or *Not Registered*) .

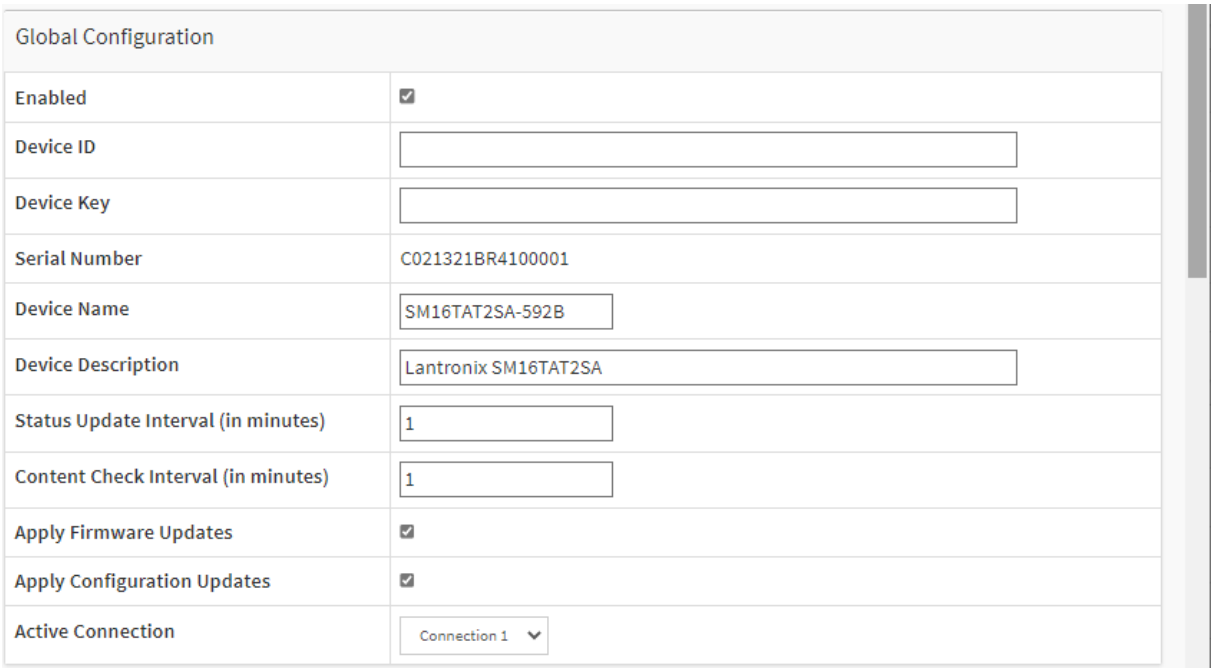
Last status update: Displays the amount of time between status updates (*e.g., 0 days 00:00:00* or *<Not Available>*).

Last content check: Displays the amount of time between content checks (e.g., e.g., 0 days 00:00:00 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 *<None>* if no Firmware updates are currently available.

Available Configuration updates: Displays a list of configuration that is available on the server. Select the configuration from this list and click Update now to upgrade or downgrade the firmware. Displays *<None>* if no configuration updates are currently available.

Global Configuration section:



Parameter descriptions:

Enabled : Check the box to enable Percepxion globally. The default is disabled (unchecked).

Device ID: Displays the switch Device ID (read only). The Device ID may be provisioned through Lantronix Provisioning manager (LPM). **Note**: The Device ID can only be provisioned once. It will persist across resets.

Device Key: Enter the key for the device; 32 alphanumeric characters. **Note**: Device Key may be configured via the Lantronix Provision Manager (LPM). The entry field shows two icons:

: Click to Show the entered Device Key text.

: Click to Hide the entered Device Key text.

Serial Number : Displays the serial number of the switch in the format *11-22-33-44-55-66*. Read only.

Device Name : Enter a Percepxion Device Name for the switch of up to 32 alphanumeric characters (e.g., *SISPM1040-384-SAAS*). Device Name can have only alphanumeric (a-z, A-Z, 0-9) characters, hyphens (-), and underscores (_). Device Name must begin and end with an alphanumeric character.

Device Description : Enter a Percepxion Device Description for the switch of up to 32 alphanumeric characters (e.g., *SISPM1040-384-LRT-C*).

Status Update Interval : Select the amount of time in minutes between status updates (1-1440 minutes). The default is 1 minute. This is the frequency that the switch updates the device status to Percepxion.

Note: at FW v1.04.0110: Allow a - (dash) character for Status Update Interval and Content Check Interval.

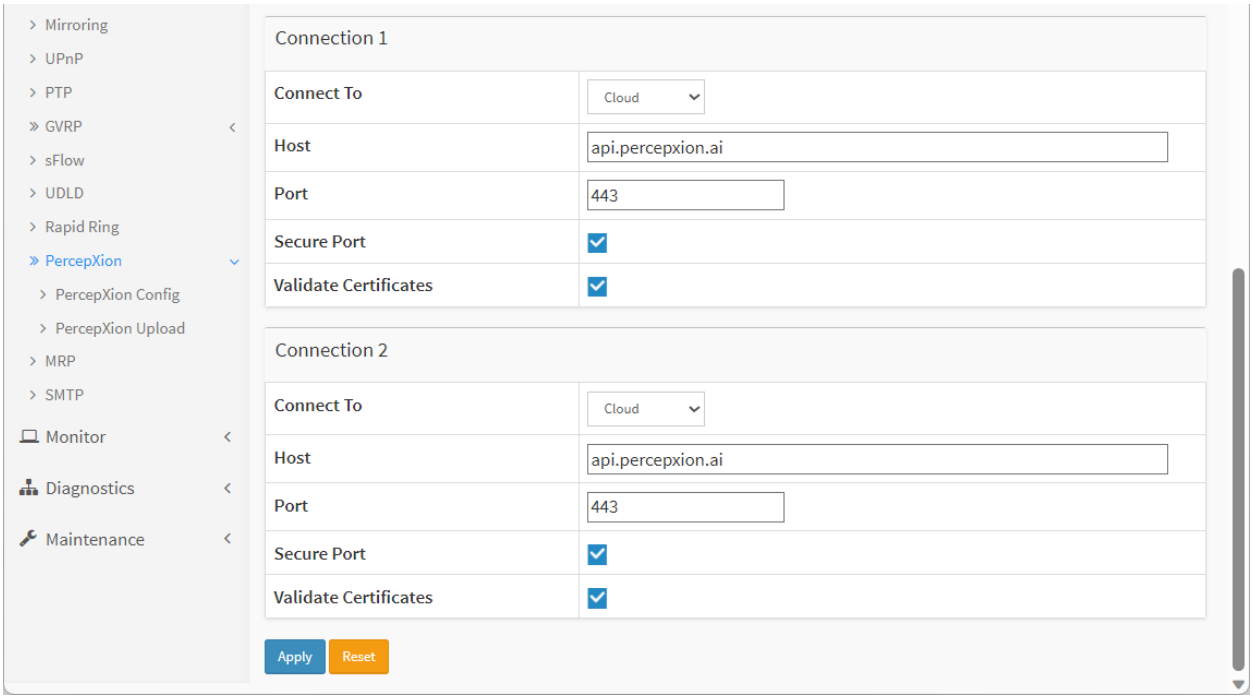
Content Check Interval : Select the amount of time in minutes between content checks (1-56160 minutes). The default is 1 minute. This is the frequency that the switch checks Percepxion for updates to configuration or firmware. The valid range is 1 hour – 2160 hours (90 days).

Apply Firmware Updates : Check the box to enable automatic switch firmware upgrades via Percepxion. The default is enabled.

Apply Configuration Updates : Check the box to enable automatic switch configuration upgrades via Percepxion. The default is enabled.

Active Connection: At the dropdown select the configuration you want to be active (i.e., *Connection 1* or *Connection 2*. The default is *Connection 1*. This is the connection to use when connecting to Percepxion. The configurable parameters for Connection 1 and Connection 2 are shown and described below.

Connection 1 and 2 sections:



Parameter descriptions:

Connection 1 :

Connect To : At the dropdown select the type of Percepxion connection to use for Connection 1 (Cloud or On-premise). The default is Cloud connection.

Host : Enter the IP address or host name of the Percepxion server for Connection 1. This is used by Percepxion to register the switch.

Port : Enter the port number for Connection 1. The default is port 443.

Secure Port : Check the box to make the selected port a secure port for Connection 1. The default is enabled.

Validate Certificates : Check the box to force using certificate validation for Connection 1. The default is enabled. To validate certificates, Secure Port must be enabled.

Connection 2 :

Connect To : At the dropdown select the type of Percepxion connection to use for Connection 2 (Cloud or On-premise). The default is Cloud connection.

Host : Enter the IP address of the Percepxion Host for Connection 2.

Port : Enter the port number for Connection 2 for Connection 2. The default is port 443.

Secure Port : Check the box to make the selected port a secure port for Connection 2. The default is enabled.

Validate Certificates : Check the box to enable using certificate validation of the Percepxion server certificates. To validate certificates, Secure Port must be enabled. The default is enabled.

Buttons

Apply : Click to apply changes.

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

Messages:

device id : 32 alphanumeric characters

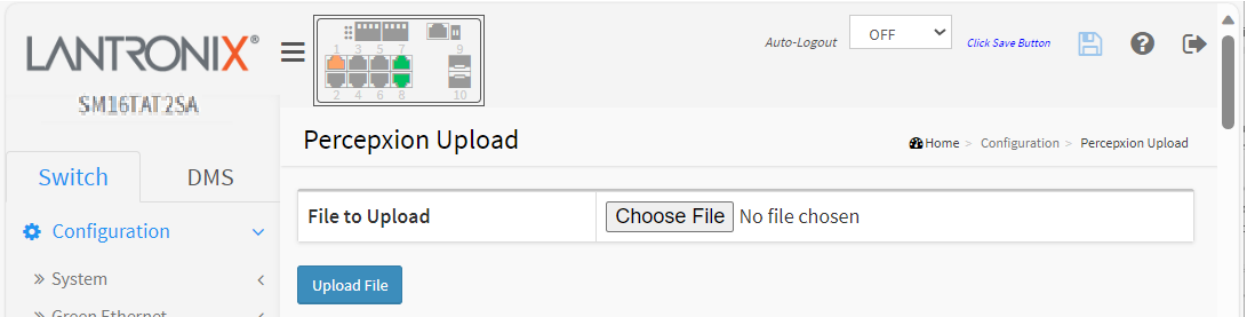
5

Status Update Interval 1 minute to 1 day (in minutes)

Content Check Interval is 1 minute to 90 days (in minutes)

12-3 Percepxion Upload

Navigate to Configuration > Percepxion > Percepxion Upload to display the Percepxion Upload page. This page lets you navigate to and select a file to upload.



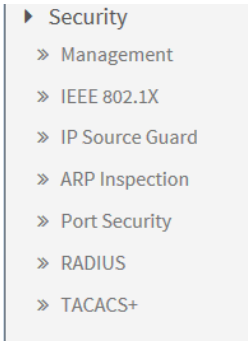
Parameter descriptions:

File to Upload: Click the Choose File button to navigate to and select a file to upload.

Upload File: Click the Upload File button to upload the chosen file.

.

Chapter 13 Security



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

13-1 Management

13-1.1 Account

This page displays current users and lets you add, edit, and delete users. Currently the only way to login as another user on the web server is to close and reopen the browser.

To add a new User via the Web UI:

1. Click Security, Management, and Account.
2. Click the Add New User button to display the Add User webpage.
3. Specify the User Name, Password (twice) and Privilege Level parameters.
4. Click Apply.

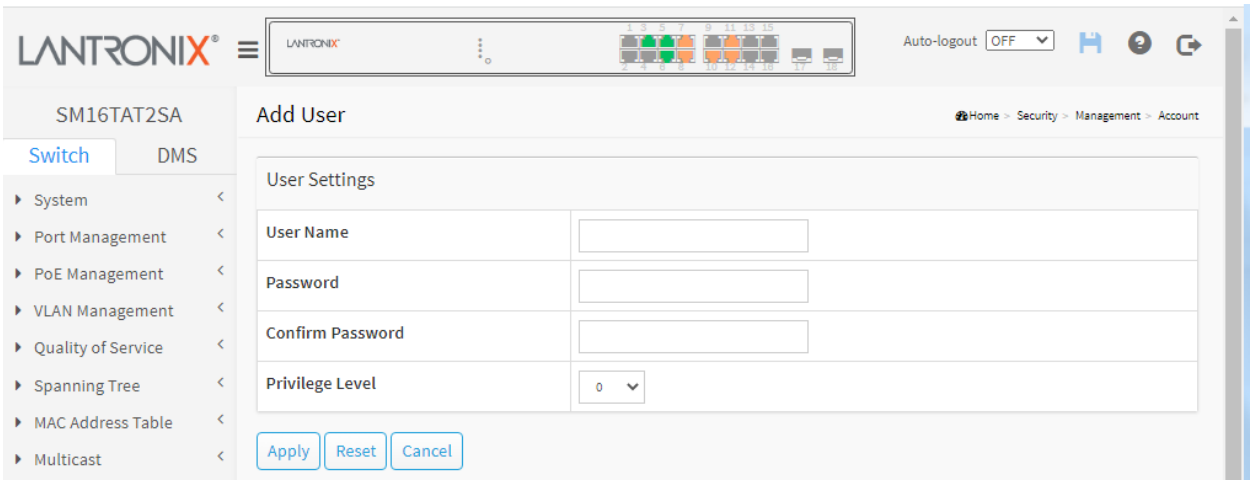


Figure 13-1.1: Account Configuration – Add User

Parameter descriptions:

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

Password: Type the password. The allowed string length is 0 – 255 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 valid 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 must refer to each group privilege level. User's privilege should be same or greater than the group privilege level to have the access of that group. By default, most groups are at privilege level 5 and have read-only access and privilege level 10 has the read-write access. The system maintenance (software upload, factory defaults and etc.) need user privilege level 15. Generally, privilege level 15 can be used for an admin account, privilege level 10 for a standard user account and privilege level 5 for a guest account.

Buttons

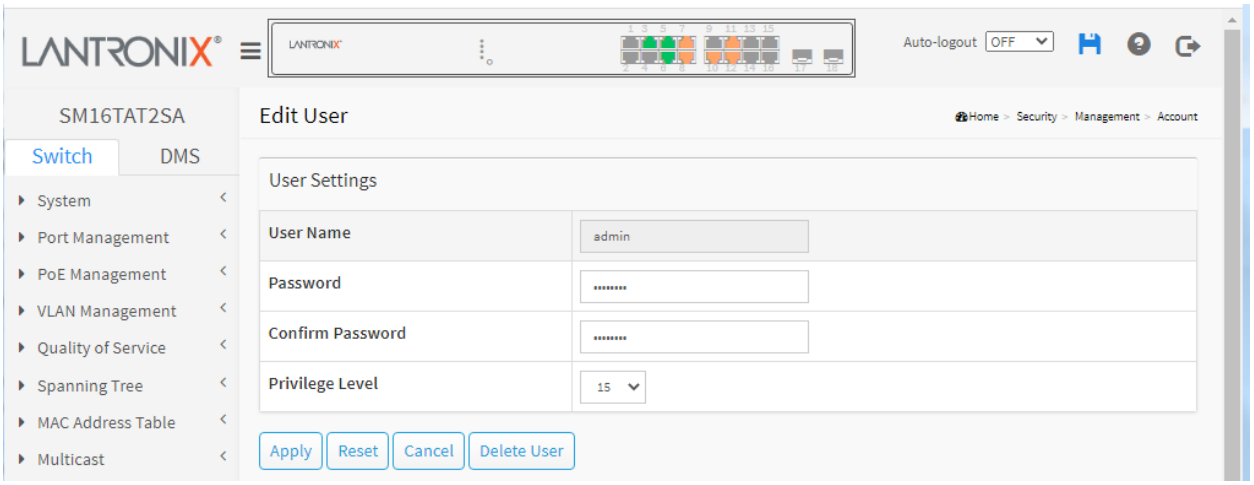
Apply: Click to save changes.

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.

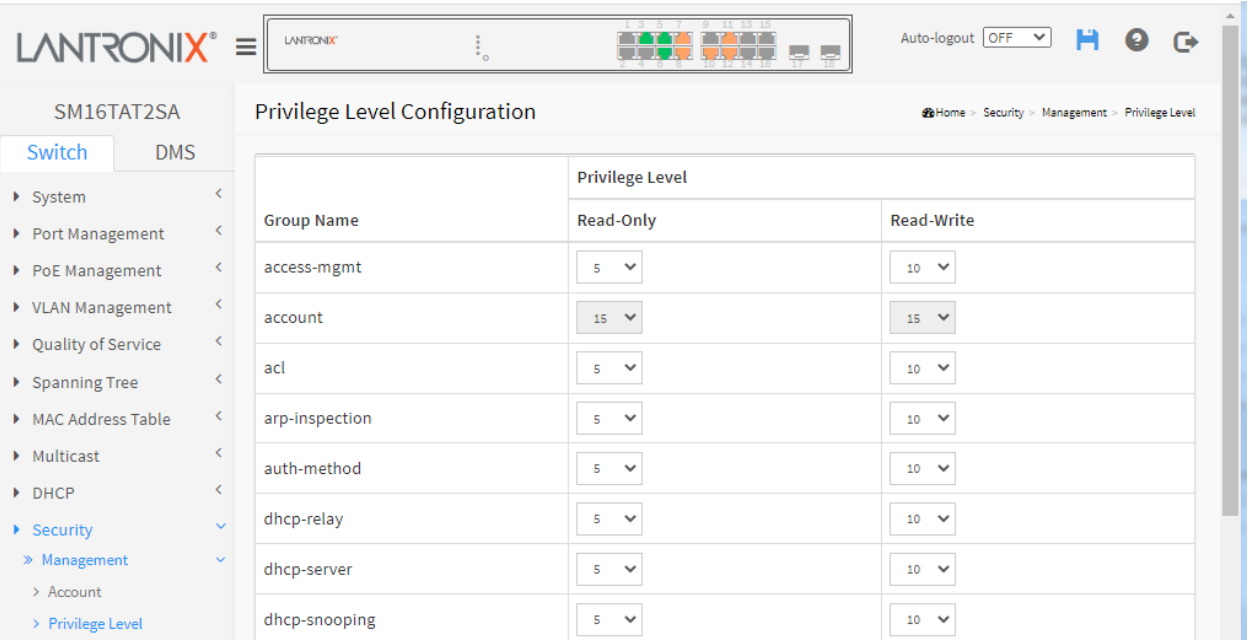
Delete User: Delete the current user. This button is not available for new configurations (Add New User).

Edit a User page:



13-1.2 Privilege Level

The Security > Management > Privilege Level menu path displays the Privilege Level Configuration table. Here you can assign Read-Only or Read-Write privilege levels for each of the major functions. This page lets you set Group Name Privilege Levels from 0 to 15.



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, STP or QoS), but a few of them contains more than one. The following description defines these privilege level groups in detail: System: Contact, Name, Location, Timezone, Daylight Saving Time, Log.

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

Read-Only: At the dropdown select a privilege level of 0-15 for any function (access-mgmt, account, arp-inspection, etc.) that you want to change from the default value.

Read-Write: At the dropdown select a privilege level of 0-15 for any function (access-mgmt, account, arp-inspection, etc.) that you want to change from the default value.

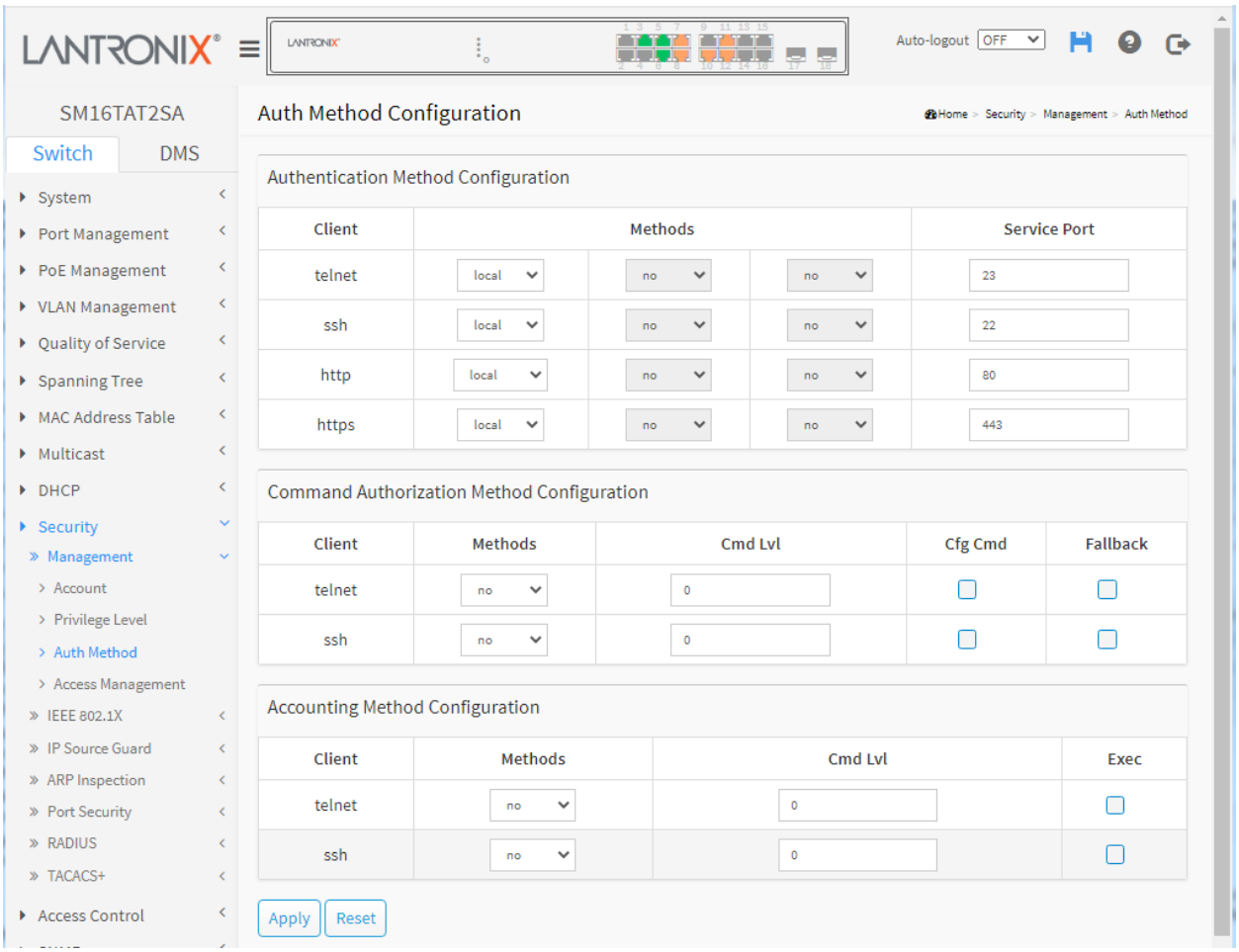
Buttons

Apply: Click to save changes.

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

13-1.3 Auth Method

The Security > Management > Auth Method menu path displays the Auth Method Configuration tables, where you can configure an authentication method (none, local, or radius) for each client (telnet, ssh, http, https). You can also configure a service port number for telnet, ssh, http, and https clients, and enable the HTTPS Redirect function on this page. The page also provides the Command Authorization Method Configuration table and the Accounting Method Configuration table.



Section descriptions:

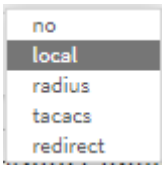
Authentication Method Configuration: The authentication section allows you to configure how a user is authenticated when he logs into the switch via one of the management client interfaces. The table has one row for each client type and several columns.

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

Accounting Method Configuration: The accounting section allows you to configure command and exec (login) accounting. The table has one row for each client type and several columns,

Parameter descriptions:

Methods: Select an authentication method (none, local, radius, or tacacs) for each client (telnet, ssh, http, https). In the Command Authorization Method Configuration table and the Accounting Method Configuration table, select a Method for telnet or ssh only (none or tacacs). The Method can be set to one of the following values:



no: Authentication is disabled and login is not possible.

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

radius: Use remote RADIUS server(s) for authentication. Remote Authentication Dial In User Service is a networking protocol that provides centralized access, authorization and accounting management for people or computers to connect and use a network service.

tacacs: Use remote TACACS+ server(s) for authentication. Terminal Access Controller Access Control System Plus. It is a networking protocol which provides access control for routers, network access servers and other networked computing devices via one or more centralized servers. TACACS+ provides separate authentication, authorization and accounting services.

redirect: enable HTTP Automatic Redirect to HTTPS (secure HTTP).

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 lets the management client login via the local user database if none of the configured authentication servers are alive.

Service Port: Enter a service port number for telnet, ssh, http, and https clients as required.

Cmd Lvl: Authorize all commands with a privilege level higher than or equal to this level. Valid values are 0 - 15. Runs accounting for all commands at the specified privilege level. Specific command level that should be authorized. Valid entries are 0 through 15.

Cfg Cmd: Check to also authorize configuration commands.

Fallback: Check the box to Enable the fallback mechanism.

Exec: Check the box to Enable exec (login) accounting. Runs accounting to determine if the user is allowed to run an EXEC shell. This facility might return user profile information such as auto command information.

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

no : accounting is disabled and login is not possible.

tacacs : use a remote TACACS server for accounting.

Cmd Lvl: Runs accounting for all commands at the specified privilege level. Specific command level that should be authorized. Valid entries are 0 through 15.

Exec: Runs accounting to determine if the user is allowed to run an EXEC shell. This facility might return user profile information such as auto command information.

Note: Password encoding changed in FW v1.02.1409. You cannot login if downgrading the switch to older firmware versions or loading an old config file in new firmware.

Buttons

Apply: Click to save changes.

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

13-1.4 Access Management

This section shows you how to configure access management table of the Switch including HTTP/HTTPS, SNMP, and TELNET/SSH. You can manage the Switch over an Ethernet LAN or over the Internet.

To configure Access Management in the web UI:

1. Click Security, Management, Access Management.
2. Select "on" in the Mode of Access Management Configuration.
3. Click "Add New Entry".
4. Checked Access Management method (HTTP/HTTPS, SNMP, and TELNET/SSH) in the entry.
5. Click Apply.

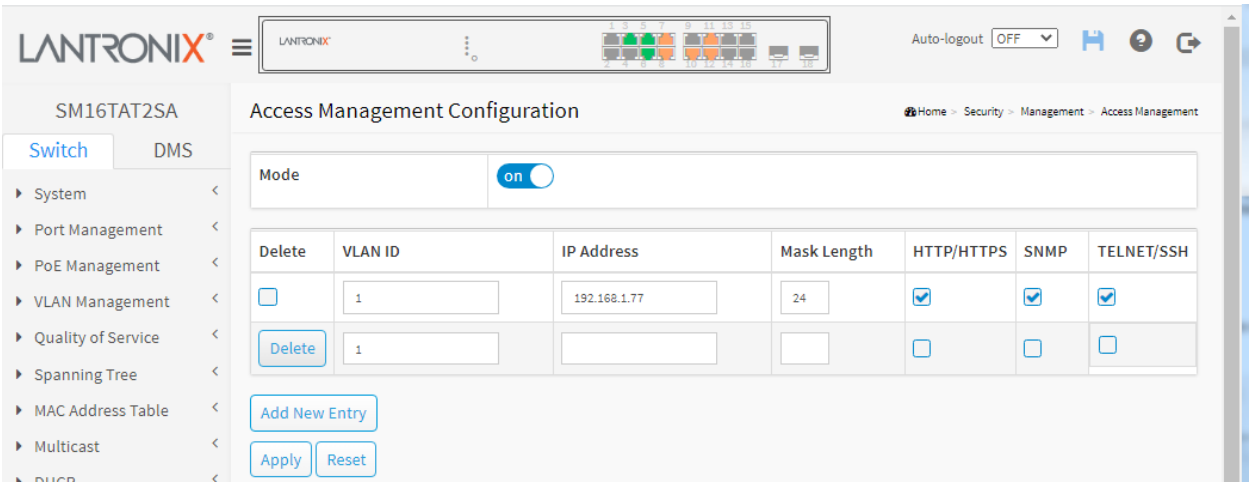


Figure 13-1.2: Access Management Configuration

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.

IP address: Enter the source IP address.

Mask Length: Enter the Mask Length (1-32).

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

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

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

Note: Firmware v1.01.1209 modified authentication method behavior for telnet/ssh/http/https. The connection is now closed if configuring the first field of Method to "none".

Note: Password encoding is changed in FW v1.02.1409. You cannot login if downgrading the switch to older firmware versions or loading an old config file in new firmware.

Buttons

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

Apply: Click to save changes.

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

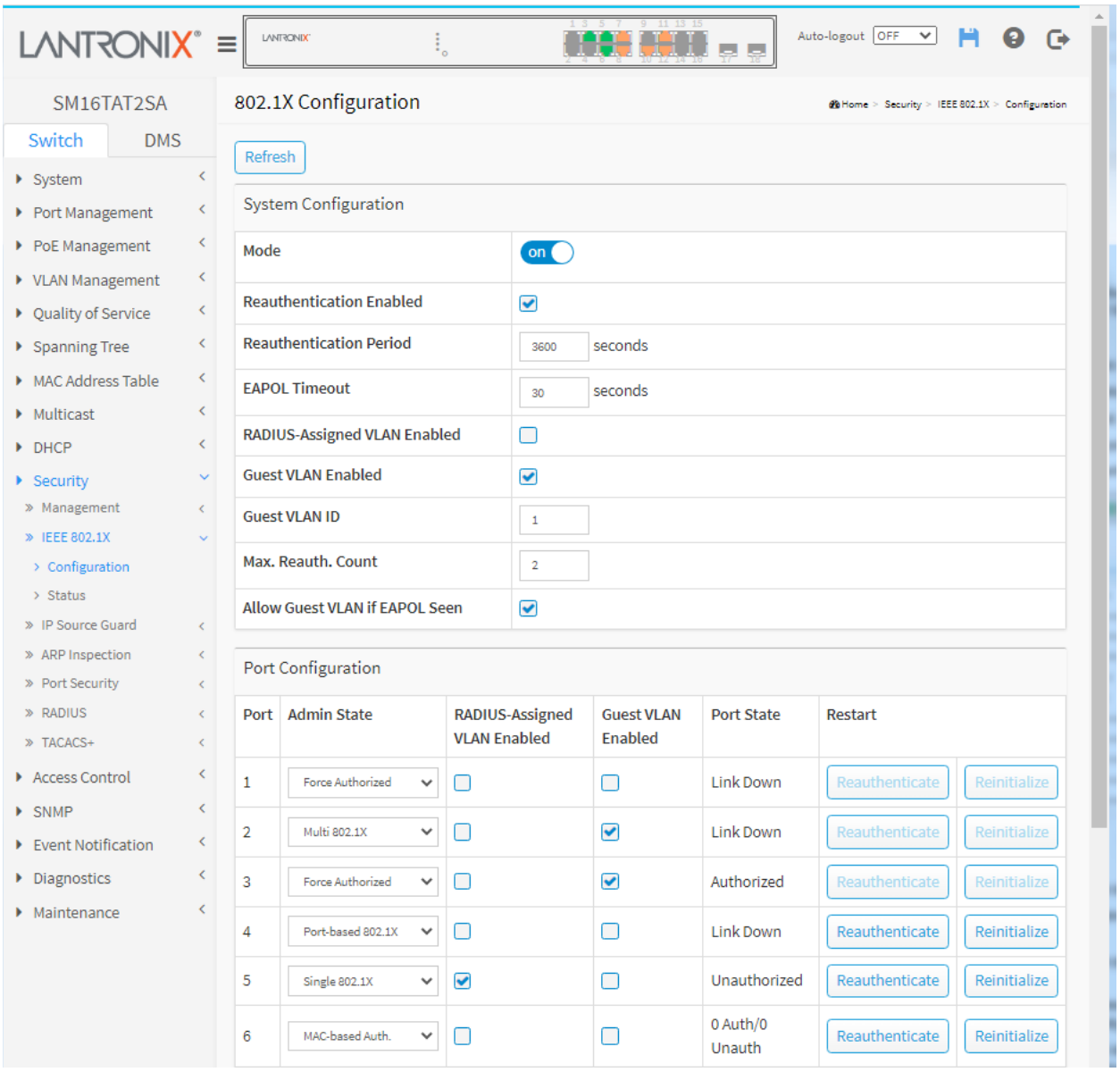
13-2 IEEE 802.1X

13-2.1 Configuration

This page lets you configure 802.1X parameters of the switch. You can use 802.1X to connect users to a variety of resources including Internet access, conference calls, printing documents on shared printers, or logging on to the Internet.

To configure IEEE 802.1X in the web UI:

1. Click Security, IEEE 802.1X, Configuration.
2. Select "on" in the Mode of IEEE 802.1X Configuration.
3. Set the System Configuration section parameters.
4. Set the Port Configuration parameters.
5. Click the Apply button to save the settings.
6. To cancel the setting click the Reset button to revert to previously saved values.



Parameter descriptions:

System Configuration

Mode: Select 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 in the range 1 to 3600 seconds.

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

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.

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 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. These modes are available:

> ***Force Authorized***: In this mode, the switch will send one EAPOL Success frame when the port link comes up, and any client on the port will be allowed network access without authentication.
>
> ***Force Unauthorized***: In this mode, the switch will send one EAPOL Failure frame when the port link comes up, and any client on the port will be disallowed network access.
>
> ***Port-based 802.1X***: In the 802.1X-world, the user is called the supplicant, the switch is the authenticator, and the RADIUS server is the authentication server. The authenticator acts as the man-in-the-middle, forwarding requests and responses between the supplicant and the authentication server. Frames sent between the supplicant and the switch are special 802.1X frames, known as EAPOL (EAP Over LANs) frames. EAPOL frames encapsulate EAP PDUs (RFC3748). Frames sent between the switch and the RADIUS server are RADIUS packets. RADIUS packets also encapsulate EAP PDUs together with other attributes like the switch's IP address, name, and the supplicant's port number on the switch. EAP is very flexible, in that it allows for different authentication methods, like MD5-Challenge, PEAP, and TLS. The important thing is that the authenticator (the switch) doesn't need to know which authentication method the supplicant and the authentication server are using, or how many information exchange frames are needed for a particular method. The switch simply encapsulates the EAP part of the frame into the relevant type (EAPOL or RADIUS) and forwards it.
>
> When authentication is complete, the RADIUS server sends a special packet containing a success or failure indication. Besides forwarding this decision to the supplicant, the switch uses it to open 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.

Guest VLAN Enabled

When Guest VLAN is both globally enabled and enabled (checked) for a given port, the switch considers moving the port into the Guest VLAN according to the rules outlined below.
This option is only available for EAPOL-based modes, i.e.:

- Port-based 802.1X
- Single 802.1X
- Multi 802.1X

For troubleshooting VLAN assignments, see "6-2 VLAN Membership" on page 78 and 6-3 VLAN Port Status on page 80**.** 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

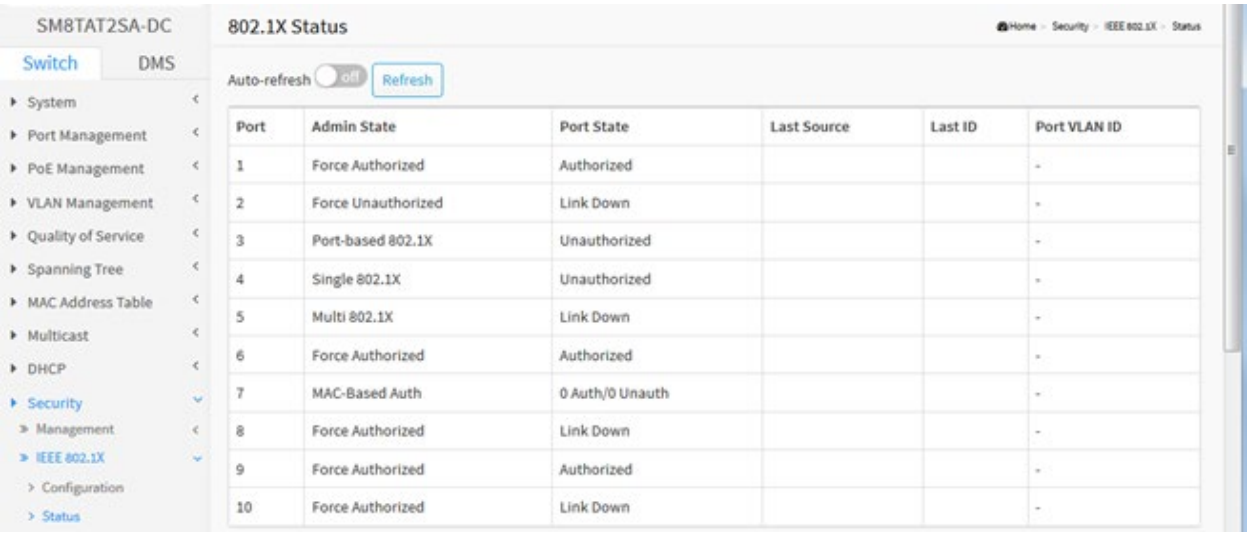
Apply : Click to save changes.

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

13-2.2 Status

This page displays 802.1X status information for each switch port. The status includes 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, Status.
2. Check "Auto-refresh" if desired.
3. Click "Refresh" to refresh the port detailed statistics.
4. Select which port that you want display 802.1X Statistics.



Port	Admin State	Port State	Last Source	Last ID	Port VLAN ID
1	Force Authorized	Authorized			-
2	Force Unauthorized	Link Down			-
3	Port-based 802.1X	Unauthorized			-
4	Single 802.1X	Unauthorized			-
5	Multi 802.1X	Link Down			-
6	Force Authorized	Authorized			-
7	MAC-Based Auth	0 Auth/0 Unauth			-
8	Force Authorized	Link Down			-
9	Force Authorized	Authorized			-
10	Force Authorized	Link Down			-

Figure 13-2.2: IEEE 802.1X Status

Parameter descriptions:

Port: The switch port number. Click to navigate to detailed 802.1X statistics for this port.

Admin State: The port's current administrative state. Refer to 802.1X Admin State above for a description of possible values.

Port State: The current state of the port. Refer to 802.1X Port State above for a description of the individual states.

Last Source: The source MAC address carried in the most recently received EAPOL frame for EAPOL-based authentication, and the most recently received frame from a new client for MAC-based authentication.

Last ID: The user name (supplicant identity) carried in the most recently received Response Identity EAPOL frame for EAPOL-based authentication, and the source MAC address from the most recently received frame from a new client for MAC-based authentication.

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. Read more about Guest VLANs here.

Buttons

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

Refresh: Click to manually refresh the page immediately.

Example: Click a linked Port number to display its individual port statistics:

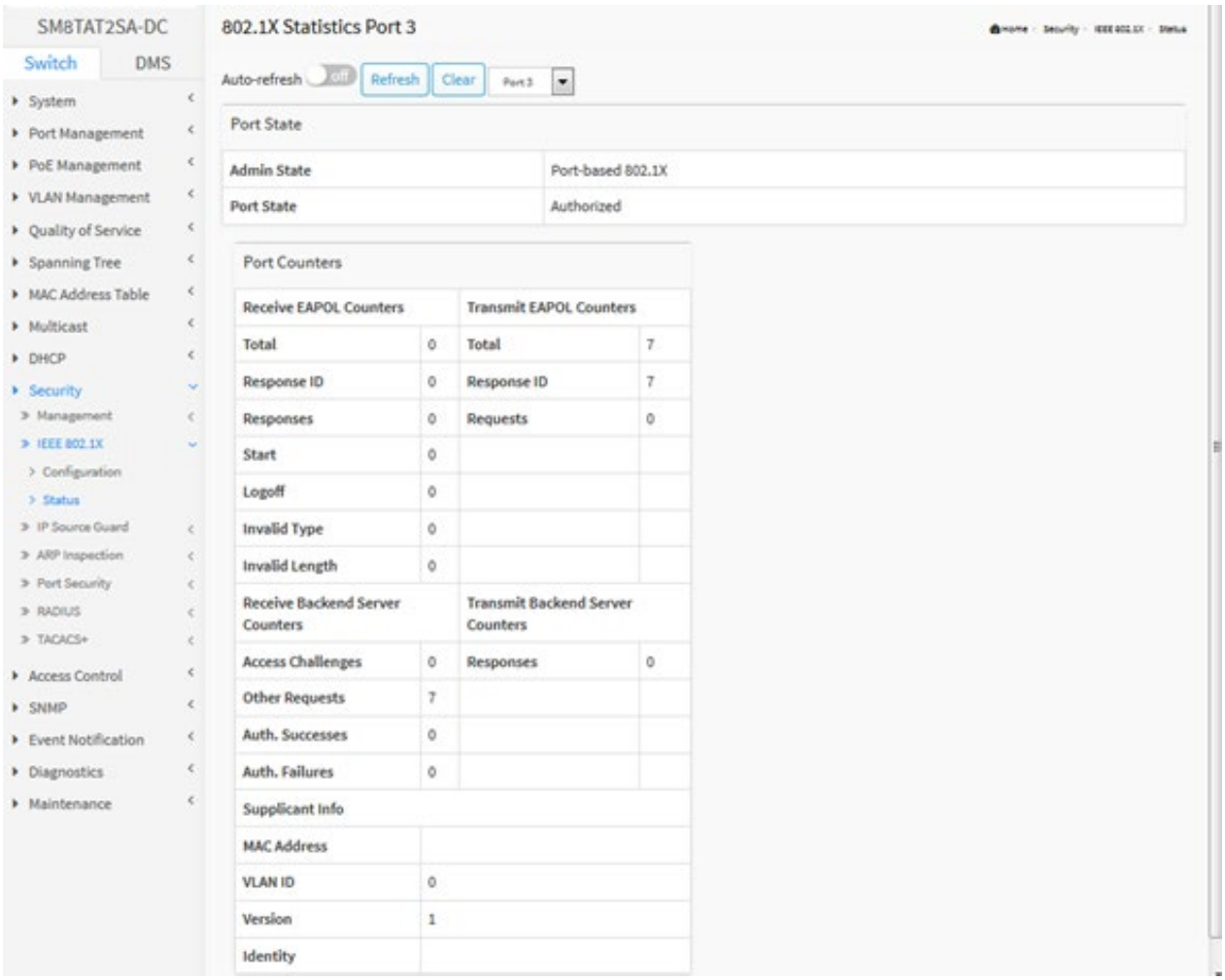


Figure 13-2.2: 802.1X Statistics

Parameter descriptions:

Port State:

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.

Port Counters: Displays Received and Transmitted EAPOL Counters, Received and Transmitted Backend Server Counters, and Supplicant Info.

Buttons:

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

Refresh: : Click to manually refresh the page immediately.

Clear: Click to clear the counters for the selected port.

Port select box: Use the dropdown to display the port for which you want to view statistics.

13-3 Port Security

13-3.1 Configuration

This page 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.

To configure Port Security parameters in the web UI:

1. Click Security, Port Security, Configuration.
2. Select "Enabled" in the Mode of System Configuration.
3. Set Mode (Enabled or Disabled), MAC Limit, and Action (Trap, Shutdown, Trap & Shutdown) for each port.
4. Click the Apply button to save the settings.
5. To cancel the settings click the Reset button to restore previously saved values.

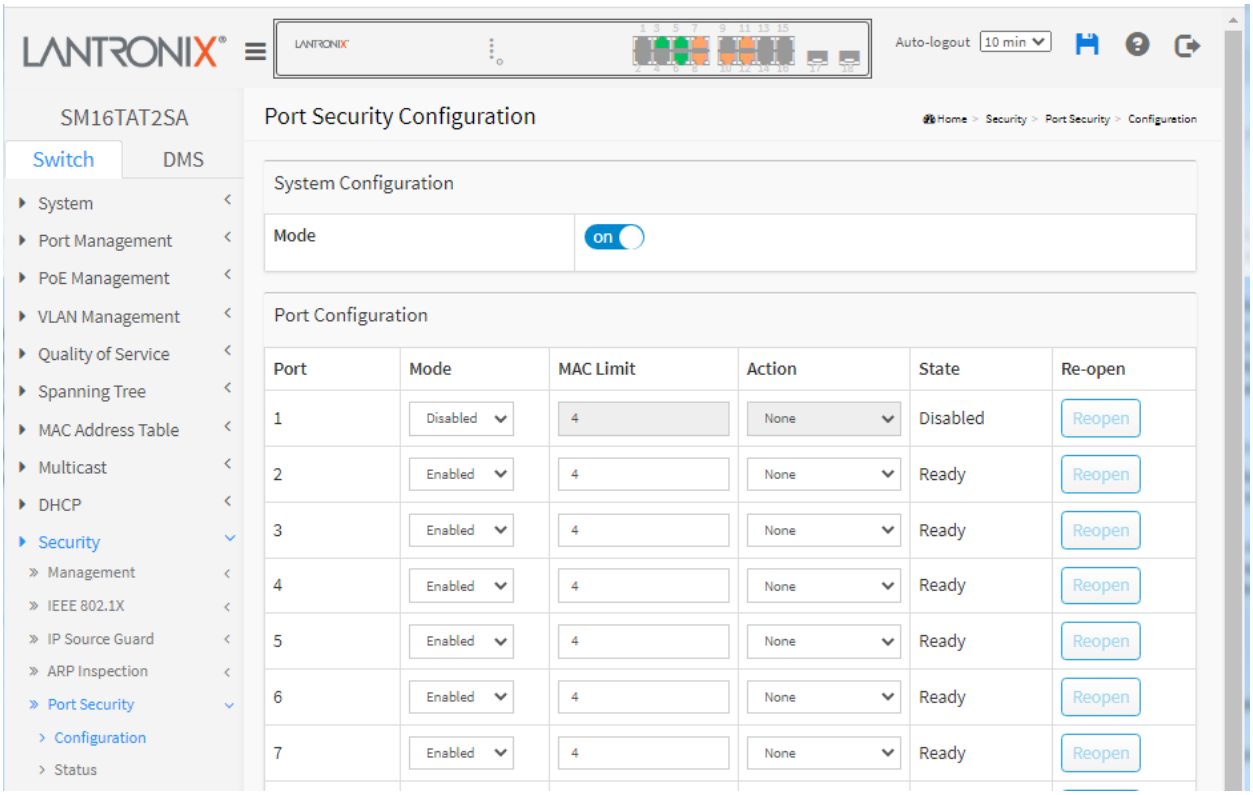


Figure 13-3.1: Port Security Configuration

System Configuration

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

Port Configuration

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. Note that other modules may still use the underlying port security features without enabling Limit Control on a given port.

MAC Limit: The maximum number of MAC addresses that can be secured on this port. This number

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Buttons

Apply: Click to save changes.

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

13-3.2 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" if desired.
3. Click "Refresh" to refresh the port detailed statistics.
4. Click the port number to see the status for the specified port.

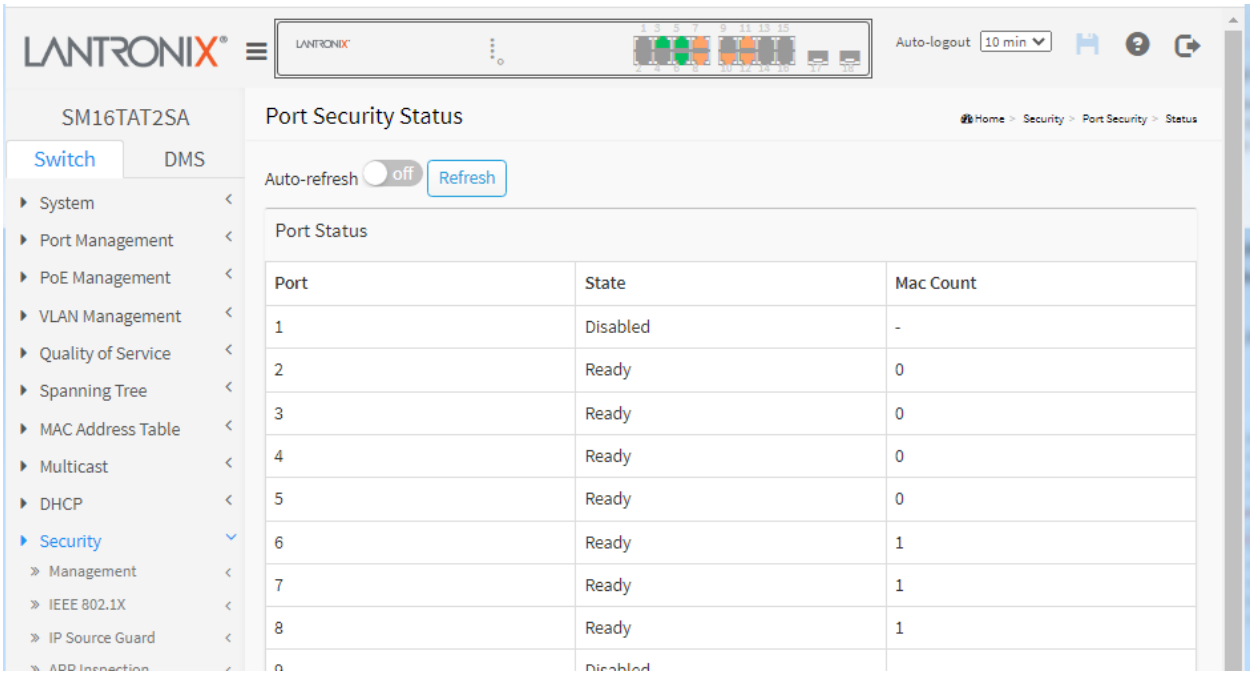


Figure 13-3.2: Port Security Status

Parameter descriptions:

Port: The port number for which the status applies. Click the port number to see the status for this particular port.

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 Reach: The Port Security service is enabled by at least the Limit Control user module, and that module has indicated that the limit is reached and no more MAC addresses should be taken in.
Shutdown: The Port Security service is enabled by at least the Limit Control user module, and that module has indicated that the limit is exceeded. No MAC addresses can be learned on the port until it is administratively re-opened on the Limit Control configuration Web-page.

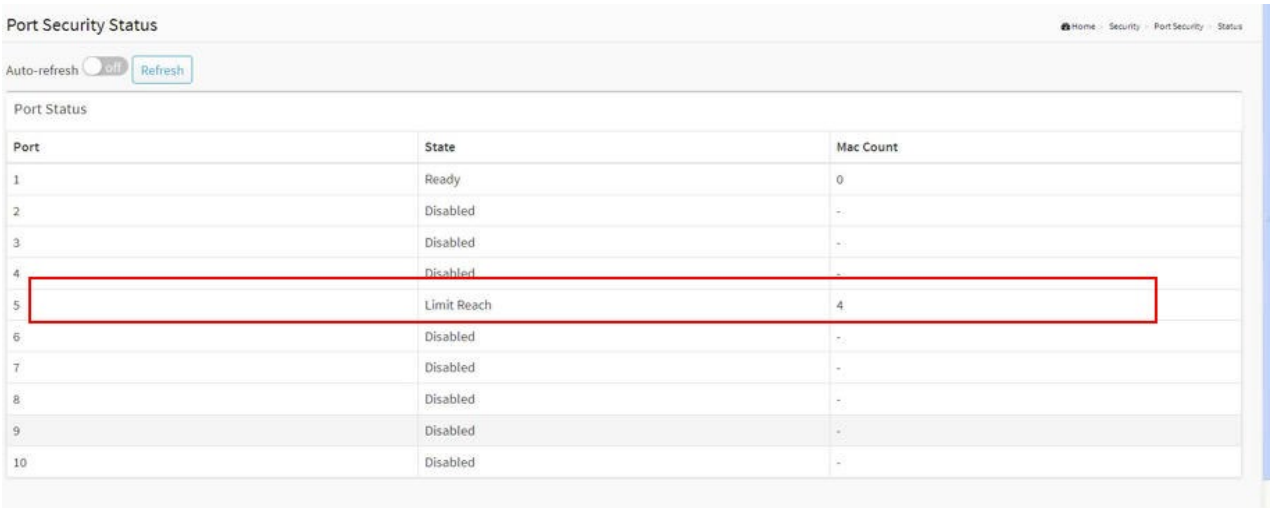
MAC Count (Current, Limit): The two columns indicate the number of currently learned MAC addresses (forwarding as well as blocked) and the maximum number of MAC addresses that can be learned on the port, respectively. If no user modules are enabled on the port, the Current column will show a dash (-).

Buttons

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

Refresh: Click to manually refresh the page immediately.

Example: Port State = Limit Reach, MAC Count = 4 on Port # 5

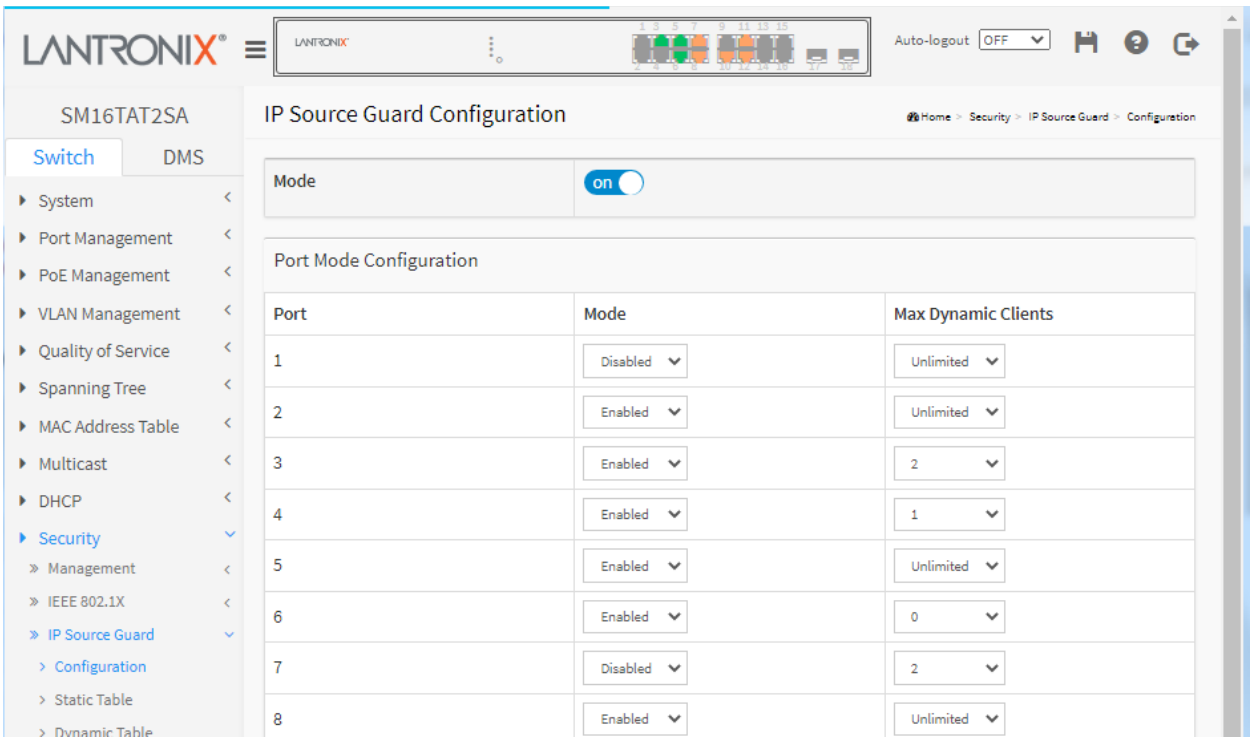


13-4 IP Source Guard

The IP Source Guard security feature restricts IP traffic on untrusted Layer 2 ports by filtering traffic based on the DHCP snooping binding database or manually configured IP source bindings. This feature helps prevent IP spoofing attacks.

13-4.1 Configuration

Navigate to Security > IP Source Guard > Configuration to configure IP Source Guard mode and port mode settings and the max dynamic clients.



Parameter descriptions:

Mode: Select the global mode (**on** or off). The default is off.

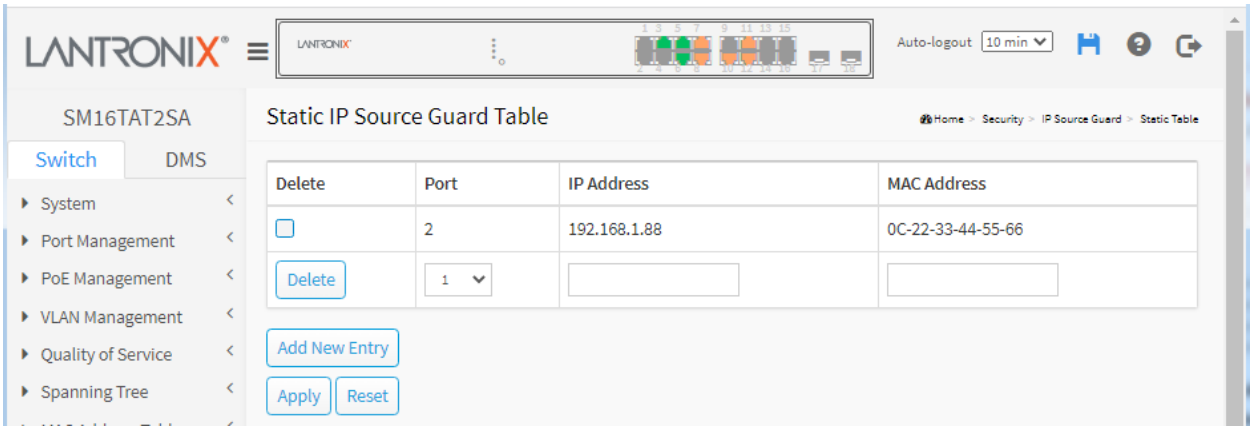
Port: A row for configuring each port.

Mode: Select the mode for each port (Enabled or Disabled). The default is Disabled.

Max Dynamic Clients: At the dropdown select 0, 1, 2, or Unlimited. The default is Unlimited.

13-4.2 Static Table

Navigate to Security > IP Source Guard > Static Table to create new Static IP Source Guard entries.



Parameter descriptions:

Add New Entry: Click the button to add a row for configuring.

Port: At the dropdown select the port to be configured.

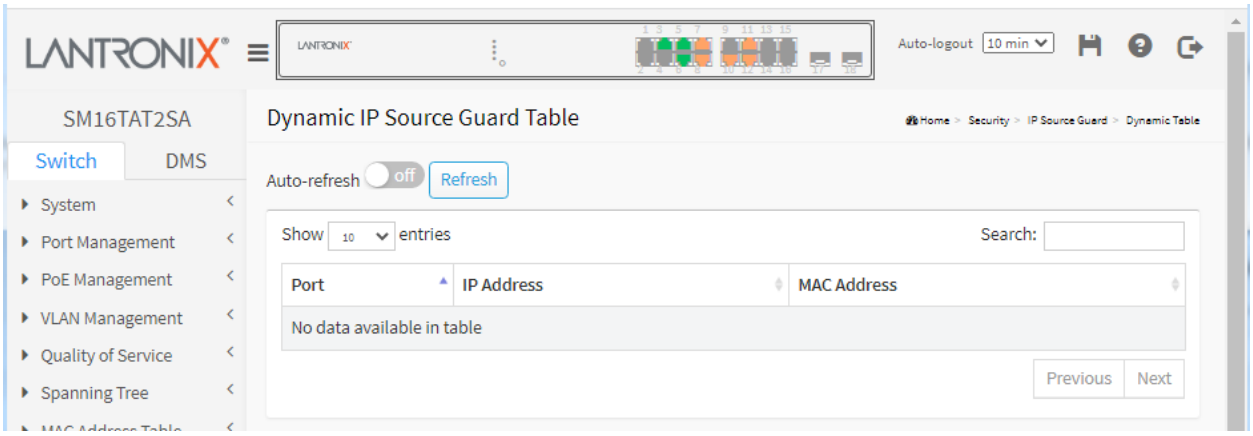
IP Address: Enter the IP address for this new entry.

MAC Address: Enter the MAC address for this new entry (must be a valid unicast MAC address).

Apply: Click the **Apply** button when done.

13-4.3 Dynamic Table

The Security > IP Source Guard > Dynamic Table displays data on existing entries. 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.



Parameters:

Port: Displays the configured port.

IP Address: Displays the IP address for the entry.

MAC Address: Displays the MAC address for the entry.

Previous: Click the button to display the previous set of entries.

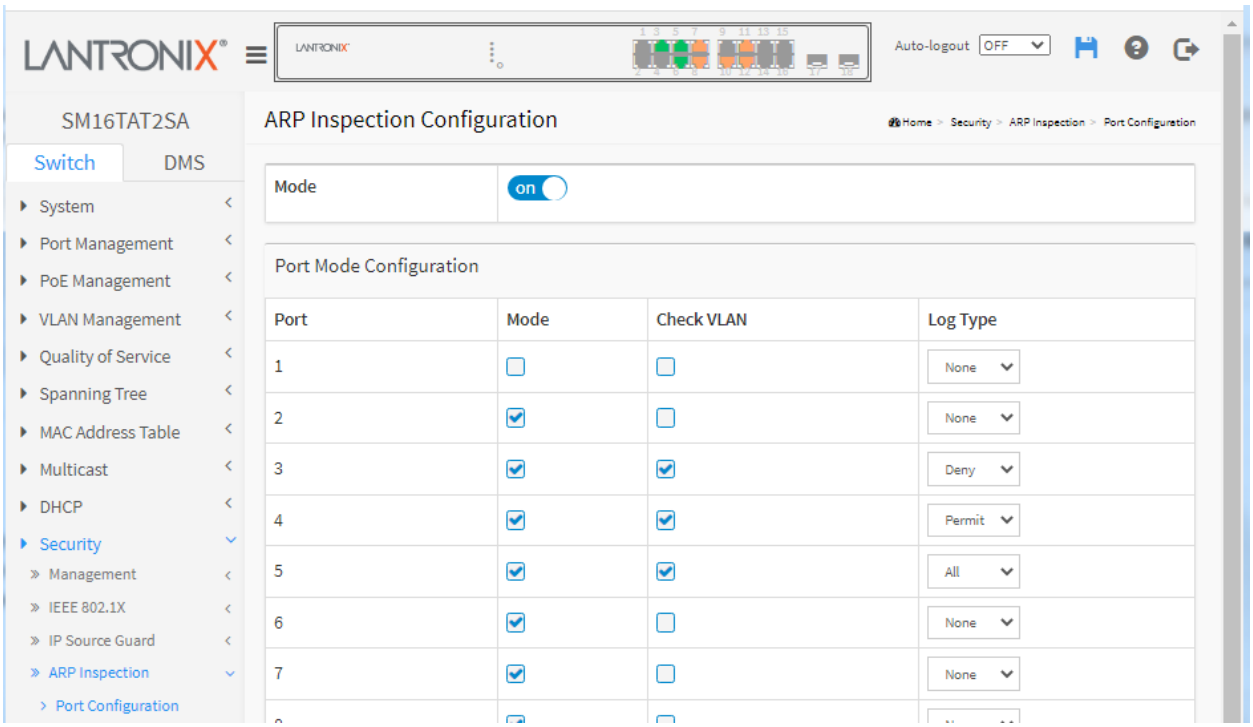
Next: Click the button to display the next set of entries.

13-5 ARP Inspection

This webpage lets you configure ARP Inspection settings including Mode (on and off) and Port (Enabled and Disabled).

13-5.1 Port Configuration

The Security > ARP Inspection > Port Configuration page displays the Port Mode Configuration table.



Parameters:

Mode: The global mode setting (***on*** or ***off***). The default is off.

Port: A row for each port to be configured.

Mode: Check the box if configured.

Check VLAN: Check the box if configured.

Log Type: Select None, Deny, Permit, or All. The default is None.

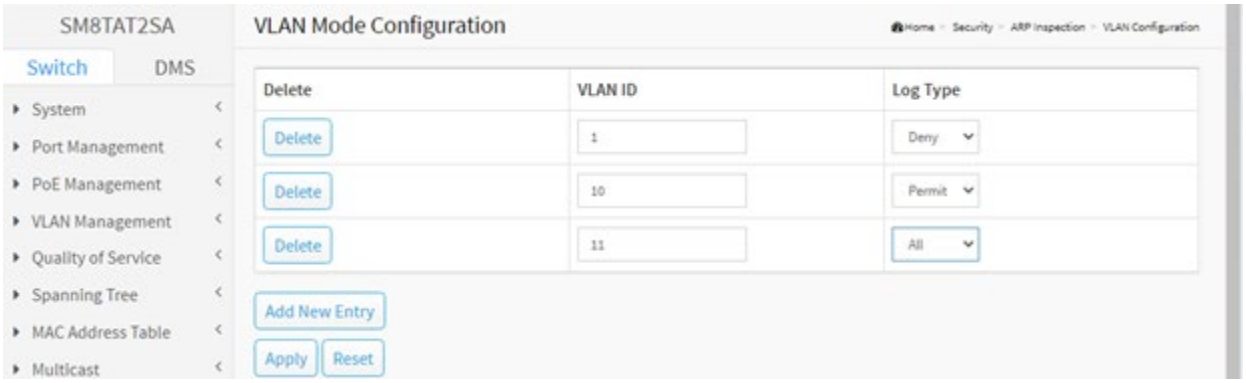
Apply: Click the button when done configuring.

13-5.2 VLAN Configuration

The Security > ARP Inspection > VLAN Configuration path displays the VLAN Mode Configuration table. Here you can 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. The log type also can be configured on per VLAN setting.



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

VLAN ID: The VID for this instance.

Log Type: Select *None*, *Deny*, *Permit*, or *All*. The default is *None*.

None: Log nothing.

Deny: Log denied entries.

Permit: Log permitted entries.

ALL: Log all entries.

Buttons

Add New Entry: Click the button to add a row for configuring.

Apply: Click the **Apply** button when done configuring.

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

13-5.3 Static Table

This page lets you configure Static ARP Inspection Table parameters of the switch. You can use the Static ARP Inspection Table to manage the ARP entries.

Navigate to the Security > ARP Inspection > Static Table menu path to display the Static ARP Inspection Table:

Port: Select the port being configured.

VLAN ID: The VID for this instance.

MAC Address: Enter the MAC address for the entry. Must be a valid unicast MAC address. This is the allowed Source MAC address in ARP request packets.

IP Address: Enter the IP address for the entry for allowed Source IP address in ARP request packets.

Buttons

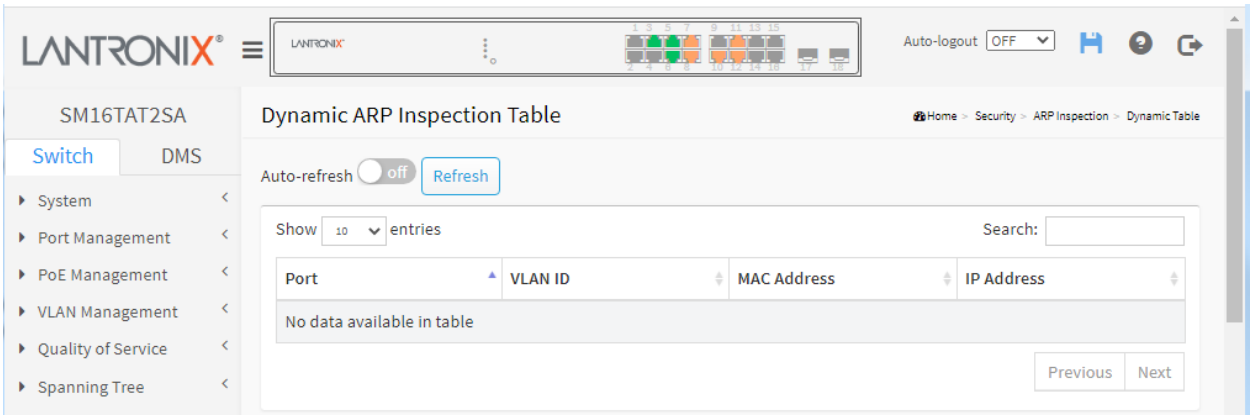
Add New Entry: Click the button to add a row for configuring a new VLAN to add to the table.

Apply: Click the button when done configuring to save changes.

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

13-5.4 Dynamic Table

Navigate to the Security > ARP Inspection > Dynamic Table menu path to display the Dynamic ARP Inspection Table. Entries in the Dynamic ARP Inspection Table are shown on this page. The Dynamic ARP Inspection Table contains up to 1024 entries, and is sorted first by port, then by VLAN ID, then by MAC address, and then by IP address.



Search: Use the Search box to search for the information that you want to see.

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

Port: Switch Port Number for which the entries are displayed.

VLAN ID: The VID for this instance. The VLAN ID in which the ARP traffic is permitted.

MAC Address: User MAC address of the entry.

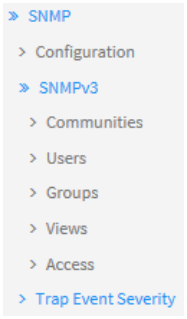
IP Address: User IP address of the entry.

Buttons:

Previous: Click the button to display the previous set of entries.

Next: Click the button to display the next set of entries.

13-6 SNMP

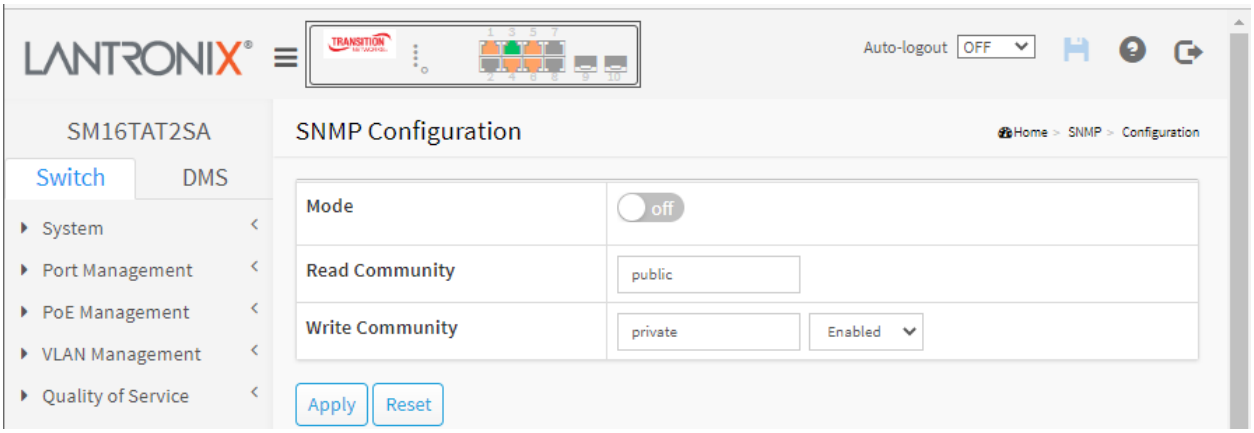


The Security > SNMP menu path lets you configure SNMP Communities, Groups, Views, and Access and Trap Event Security.

13-6.1 Configuration

Security > SNMP > Configuration

This webpage lets you configure SNMP System on the switch. This function is used to configure SNMP settings, community name, trap host and public traps as well as the throttle of SNMP.
An SNMP manager must pass the authentication by identifying both community names, then it can access the MIB information of the target device. So both parties must have the same community name.



Parameters:

Mode : Set to ***on*** to enable support for the SNMP protocol service. The default is ***off***

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 the ASCII characters from 33 to 126. The field is applicable only when SNMP version is SNMPv1 or SNMPv2c. If SNMP version is SNMPv3, the community string will be associated with SNMPv3 communities table. It provides more flexibility to configure security name than a SNMPv1 or SNMPv2c community string. In addition to community string, a particular range of source addresses can be used to restrict source subnet

Write Community: Indicates the community write access string to permit access to SNMP agent. The allowed string length is 1-31 characters, and the allowed content is the ASCII characters 33 - 126. The field is applicable only when SNMP version is SNMPv1 or SNMPv2c. If SNMP version is SNMPv3, the community string will be associated with SNMPv3 communities table. It provides more flexibility to configure security name than a SNMPv1 or SNMPv2c community string. In addition to community string, a particular range of source addresses can be used to restrict source subnet. At the dropdown you can select *Enabled* (default) or *Disabled*.

Write Mode : At the dropdown select Enabled to support community write access string to permit access to SNMP agent.

Buttons

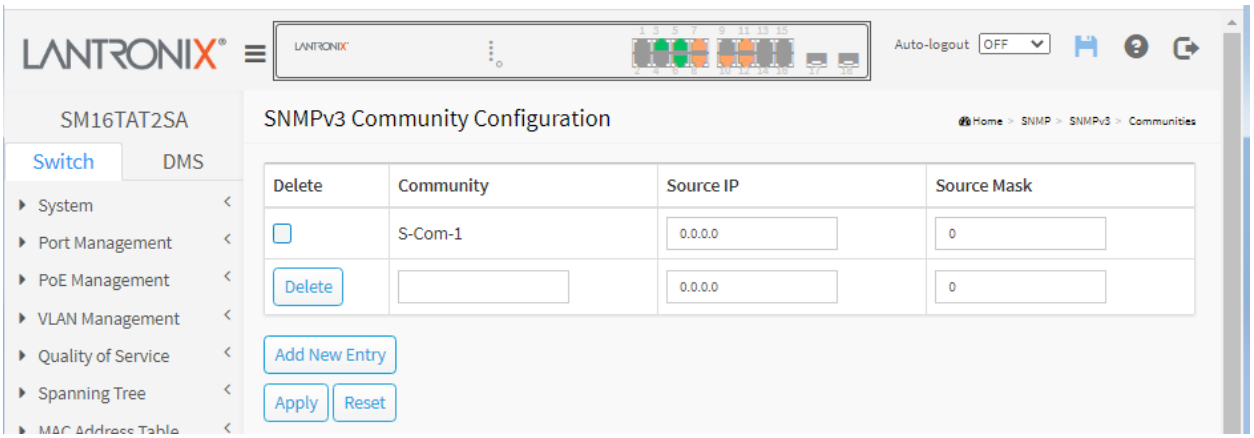
Apply: Click to save changes.

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

13-6.2 SNMPv3

Security > SNMP > SNMPv3 > Communities

The function is used to configure SNMPv3 communities. The Community is unique. To create a new community account, check the Add New Entry button, and enter the account information then click the Apply button. You can create up to six Groups.



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

Source IP: Enter the IP address for this new entry. 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: Enter the Source Mask for this new entry. Indicates the SNMP access source address mask.

Buttons:

Add New Entry: Click to add a row to the table and configure the new instance.

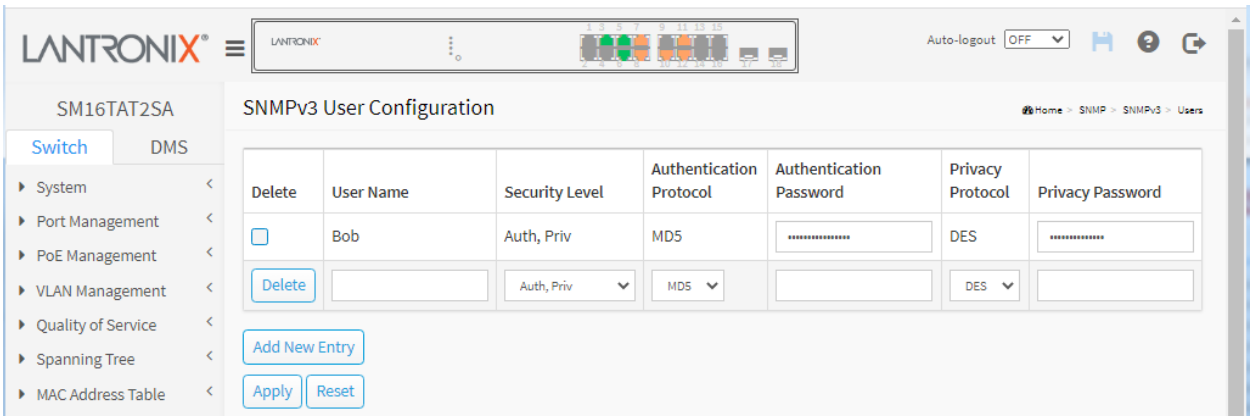
Apply: Click to save changes when done configuring.

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

Messages: *The Community ip and mask are inconsistent.*

Security > SNMP > SNMPv3 >Users

This page lets you configure SNMPv3 users. You can create up to six Users.



User Name: Enter a name for this new user entry. The allowed string length is 1-31 characters, and the allowed content is ASCII characters 33-126.

Security Level: Select the desired combination of Privacy and Authentication. Security Level indicates the security model that this entry should belong to. Possible security models are:

NoAuth, NoPriv: No authentication and no privacy.
Auth, NoPriv: Authentication and no privacy.
Auth, Priv: Authentication and privacy.

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

Authentication Protocol: If Authentication is configured, select a protocol; either: ***MD5*** (uses the Merkle–Damgård construction) or ***SHA*** (Secure Hash Algorithm). **Note**: the value of security level cannot be modified if an entry already exists. That means you must first ensure that the value is set correctly.
The length of 'SHA Authentication Password' is restricted to 8-39 characters.

Authentication Password: If Authentication is configured, enter a password for authenticating. 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 8-39 characters.
The allowed content is ASCII characters 33-126.

Privacy Protocol: If Privacy is configured, select a protocol; either **DES** (Data Encryption Standard) or **AES** (Advanced Encryption Standard). 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: If Privacy is configured, enter a password for privacy. A string identifying the privacy password phrase. The allowed string length is 8-31, and the allowed content is ASCII characters 33-126.
The length of 'Privacy Password' is restricted to 8–31 characters.

Buttons:

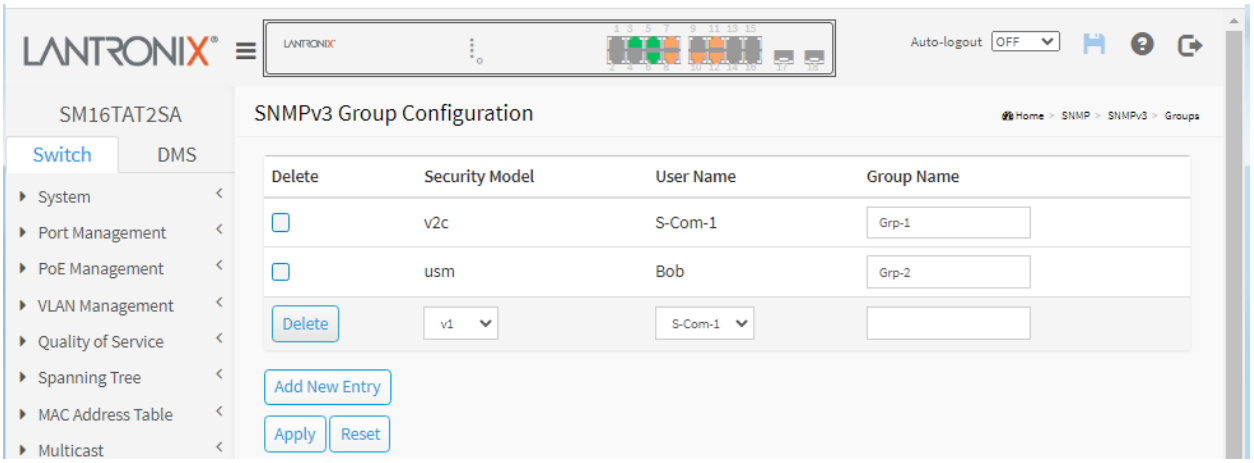
Add New Entry: Click to add a row to the table and configure the new instance.

Apply: Click to save changes when done configuring.

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

Security > SNMP > SNMPv3 > Groups

This page lets you configure SNMPv3 groups. The Entry index key are Security Model and Security Name. To create a new group account, check the Add New Group button, enter the group information, and then click the Apply button. You can create up to 12 SNMP Groups.



Security Model: Select **v1**, **v2c**, or **usm** (User-based 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).

User Name: At the dropdown select an existing User Name to become a member of this new group. A string identifying the security name that this entry should belong to. The allowed string length is 1-31 characters and the allowed content is ASCII characters 33-126.

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

Buttons:

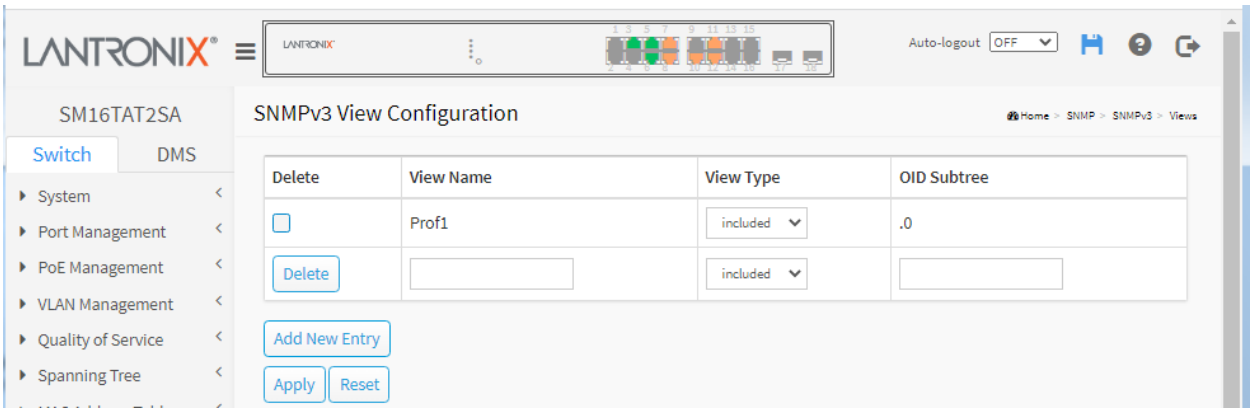
Add New Entry: Click to add a row to the table and configure the new instance.

Apply: Click to save changes when done configuring.

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

Security > SNMP > SNMPv3 > Views

The function is used to configure SNMPv3 view. The Entry index keys are OID Subtree and View Name. The maximum number of View entries is 12. The entry index keys are View Name and OID Subtree.



View Name: Enter the name for this new View. 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: Select included or excluded for this new View. 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: Enter an Object Identifier for this new View. The format is .OID1.OID2.OID3 ...
The allowed string content is digital number or asterisk (*). This is the OID defining the root of the subtree to add to the named view. The allowed OID length is 1-128.

Buttons:

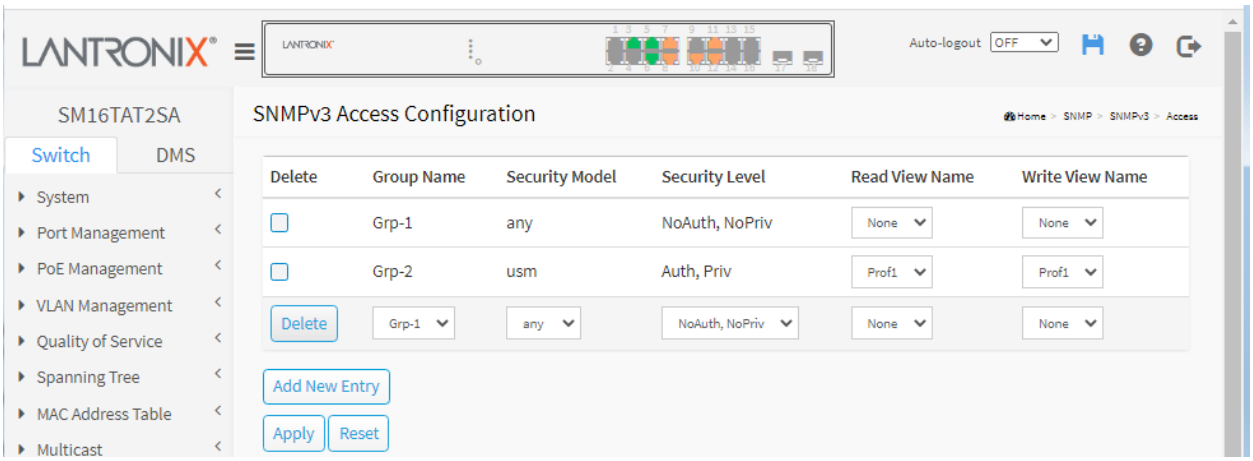
Add New Entry: Click to add a row to the table and configure the new instance.

Apply: Click to save changes when done configuring.

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

Security > SNMP > SNMPv3 > Access

This page lets you configure SNMPv3 accesses. The Entry index key are Group Name, Security Model and Security level. You can create up to 12 accesses.



Group Name: Select the name of the existing Group. 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: Select **any**, **v1**, **v2c**, or **usm** for this instance. 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: Select the level of security to be applied. 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: Select None or an existing Read View Name at the dropdown. This is 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: Select None or an existing Write View Name at the dropdown. This is 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 a new instance. An empty row is added to the table, and the new instance can be configured as needed.

Apply: Click to save changes.

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

13-7 RADIUS

13-7.1 Configuration

This page lets you configure up to five RADIUS servers:

1. Click Security, RADIUS, Configuration.
2. Set Timeout, Retransmit, Deadtime, Key, NAS-IP-Address, NAS IPv6-Address,NAS-Identifier.
3. Click "Add New Entry" to display the configurable parameters.
4. Set Global Configuration parameters.
5. Set Server Configuration parameters.
6. Click the Apply button to save the settings. To cancel the settings, click the Reset button.

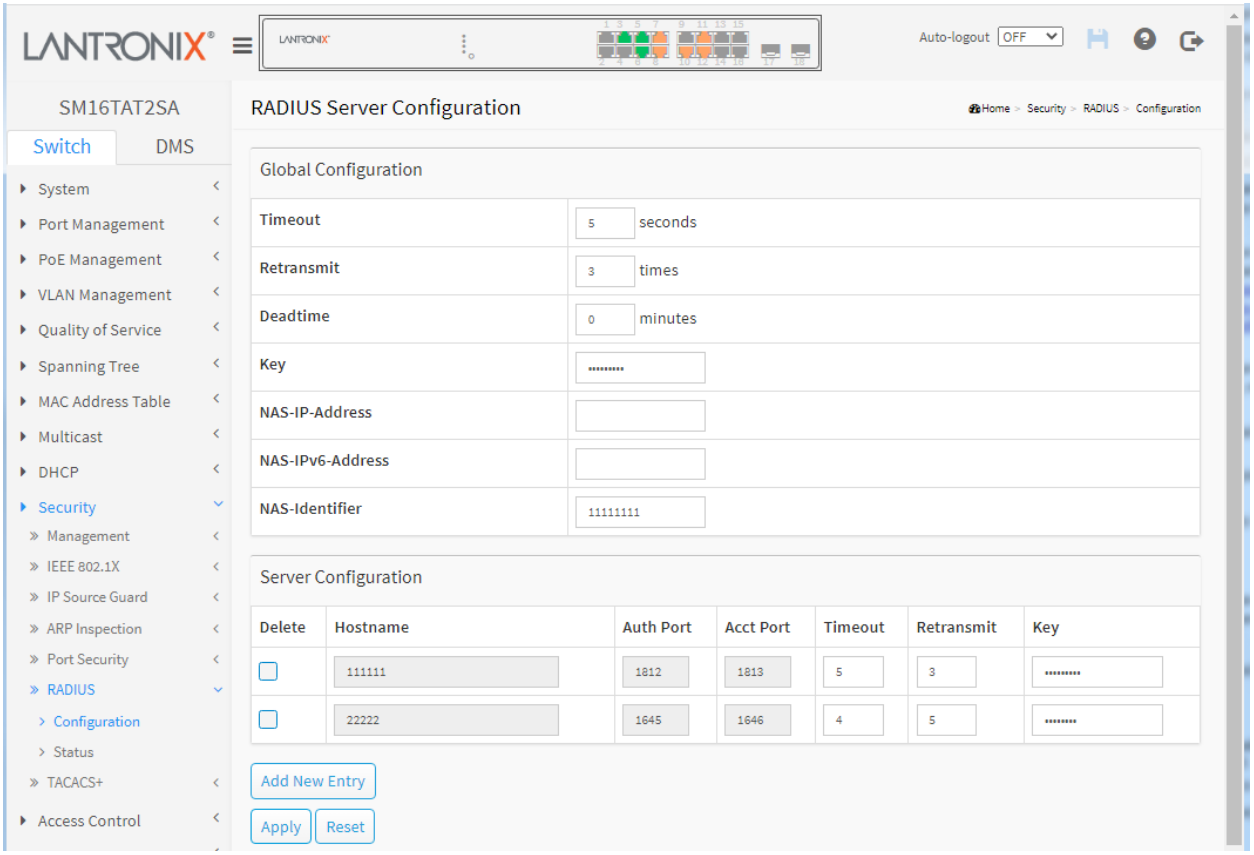


Figure 12-7.1: RADIUS Server Configuration

Global Configuration parameters: These setting are common for all of the RADIUS servers.

Timeout: The number of seconds (1 to 1000) to wait for a reply from a RADIUS server before retransmitting the request.

Retransmit: 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 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.

: Click to display the Key text as you enter it.

: Click to hide the Key text as you enter it.

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 parameters: The table has one row for each RADIUS server and a number of columns

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

Hostname: The IP address or hostname of the RADIUS server.

Auth Port : The UDP port to use on the RADIUS server for authentication. The officially assigned port number for RADIUS Authentication is 1812). Note: by default, many access servers use port 1645 for authentication requests.

> **Note**: For Windows Server information on how to configure ports that Network Policy Server (NPS) uses for Remote Authentication Dial-In User Service (RADIUS) authentication and accounting traffic see https://docs.microsoft.com/en-us/windows-server/networking/technologies/nps/nps-udp-ports-configure#:~:text=The%20port%20values%20of%201812,and%201646%20for%20accounting%20requests

Acct Port : The UDP port to use on the RADIUS server for accounting. The officially assigned port number for RADIUS Accounting is 1813. Note: by default, many access servers use port 1646 for accounting requests.

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

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

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

Buttons

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.

Apply: Click to save changes.

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

Messages:

The value of NAS-IP-Address must be a valid IP address in dotted decimal notation (x.y.z.w), where x, y, z, and w are decimal number between 0 and 255.

The input value NAS-IPv6-Address (111111111) is not a valid IPv6 address.

Hostname must be a valid hostname, unicast IPv4, or unicast IPv6 address

ERROR! Failed to set host 66 ability

RADIUS Attributes

Value	Description	Data Type	Reference
4	NAS-IP-Address	ipv4addr	IETF RFC2865
32	NAS-Identifier	text	IETF RFC2865
95	NAS-IPv6-Address	ipv6addr	IETF RFC3162

The RADIUS Accounting protocol provides a protocol for carrying accounting information between a Network Access Server and a shared Accounting Server per IETF RFC 2866.

See the IANA Considerations for guidance regarding IANA registration of values related to RADIUS as defined in IETF RFC2865.

See your RADIUS server documents for more information.

13-7.2 Status

This page displays an overview/detail of the RADIUS Authentication and Accounting servers' status to ensure the function is workable.

To display RADIUS Status in the web UI:

1. Click Security, RADIUS, and Status.
2. Select a Server line to display the detail statistics for a particular RADIUS server.

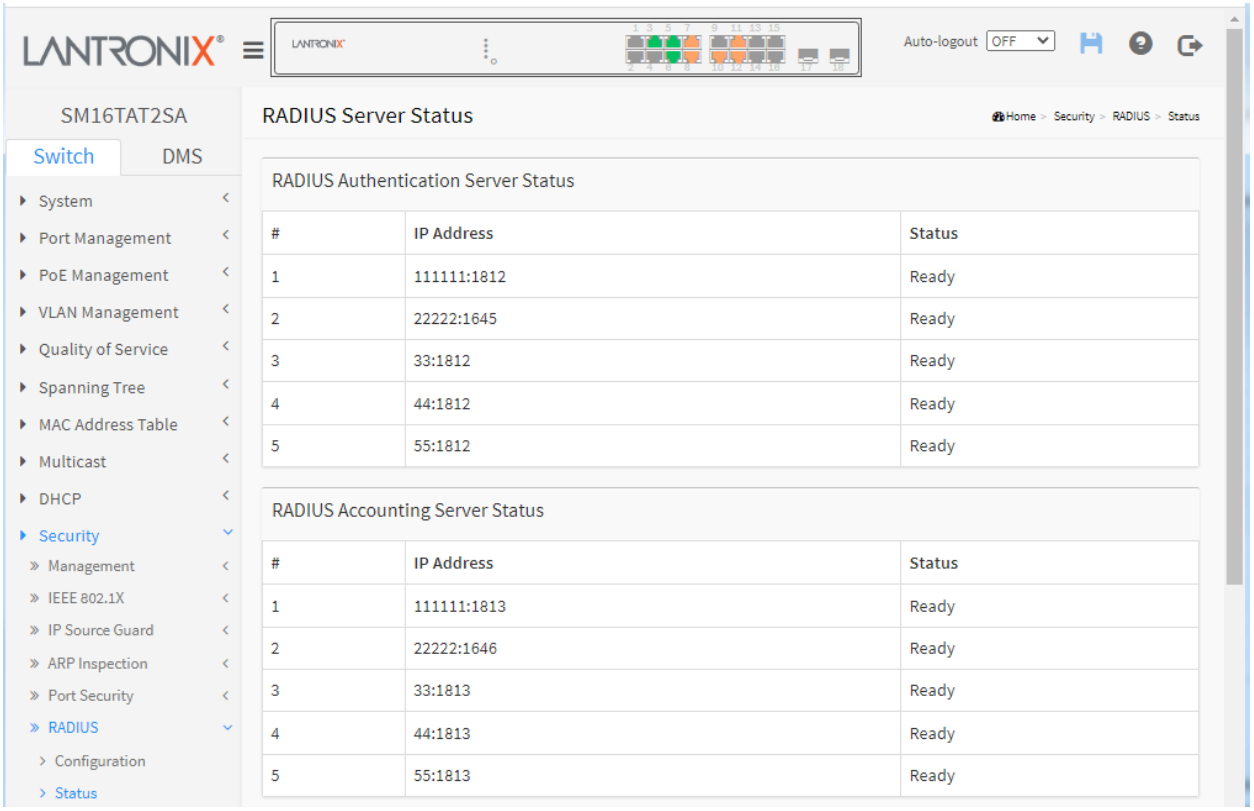


Figure 12-4.2: RADIUS Server Status

Parameter descriptions:

RADIUS Authentication Server Status

#: The RADIUS server number. Click to navigate to detailed statistics for this server (see below).

IP Address: The IP address and UDP port number (in <IP Address>:<UDP Port> notation) of this server.

State: The current state of the server. This field takes one of these values:

***Disabled*:** The server is disabled.

***Not Ready*:** The server is enabled, but IP communication is not yet up and running.

***Ready*:** The server is enabled, IP communication is up and running, and the RADIUS module is ready to accept access attempts.

***Dead (X seconds left)* :** Access attempts were made to this server, but it did not reply within the configured timeout. The server has temporarily been disabled but will get re-enabled when the dead-time expires. The number of seconds left before this occurs is displayed in parentheses. This state is only reachable when more than one server is enabled.

RADIUS Accounting Server Status

#: 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.

State : The current state of the server. This field takes one of the following values:

***Disabled*:** The server is disabled.
***Not Ready*:** The server is enabled, but IP communication is not yet up and running.
***Ready*:** The server is enabled, IP communication is up and running, and the RADIUS module is ready to accept 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.

Example: If you select Server#2 to display its RADIUS Authentication and Accounting Statistics:

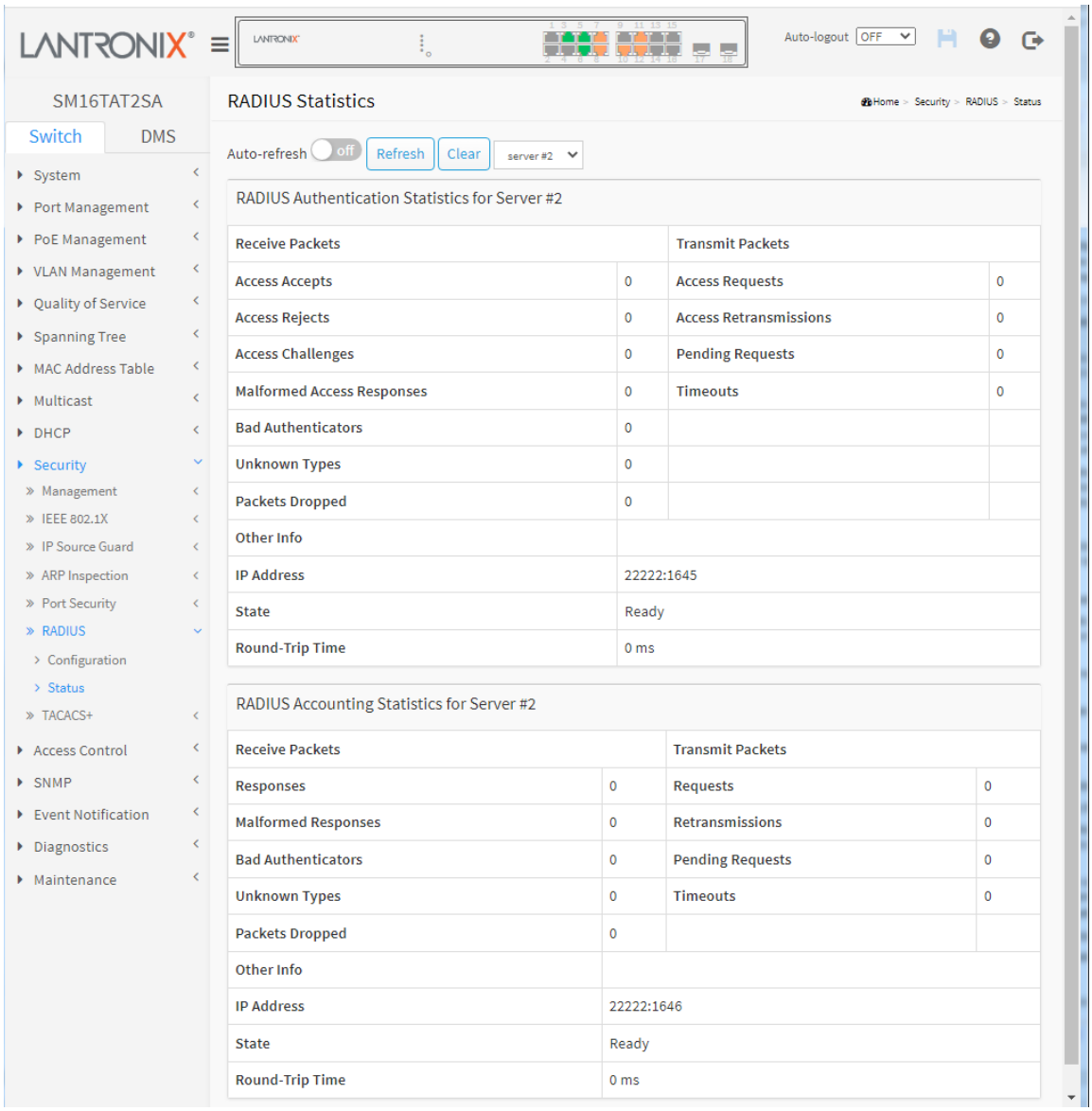


Figure 12-7.2: RADIUS Statistics

Parameter descriptions:

server #: You can select which server that you want display RADIUS.

RADIUS Authentication Statistics for Server #1: The statistics map closely to those specified in IETF RFC4668 - RADIUS Authentication Client MIB. Use the server select box to switch between the backend servers to show details for.

Access Accepts: The number of RADIUS Access-Accept packets (valid or invalid) received from the server.

Access Rejects: The number of RADIUS Access-Reject packets (valid or invalid) received from the server.

Access Challenges: The number of RADIUS Access-Challenge packets (valid or invalid) received from the server.

Malformed Access Responses: The number of malformed RADIUS Access-Response packets received from the server. Malformed packets include packets with an invalid length. Bad authenticators or Message Authenticator attributes or unknown types are not included as malformed access responses.

Bad Authenticators: The number of RADIUS Access-Response packets containing invalid authenticators or Message Authenticator attributes received from the server.

Unknown Types: The number of RADIUS packets that were received with unknown types from the server on the authentication port and dropped.

Packets Dropped: The number of RADIUS packets that were received from the server on the authentication port and dropped for some other reason.

Access Requests: The number of RADIUS Access-Request packets sent to the server. This does not include retransmissions.

Access Retransmissions: The number of RADIUS Access-Request packets retransmitted to the RADIUS authentication server.

Pending Requests: The number of RADIUS Access-Request packets destined for the server that have not yet timed out or received a response. This variable is incremented when an Access-Request is sent and decremented due to receipt of an Access-Accept, Access-Reject, Access-Challenge, timeout, or retransmission.

Timeouts: The number of authentication timeouts to the server. After a timeout, the client may retry to the same server, send to a different server, or give up. A retry to the same server is counted as a retransmit as well as a timeout. A send to a different server is counted as a Request as well as a timeout.

IP Address: 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 #x: 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.

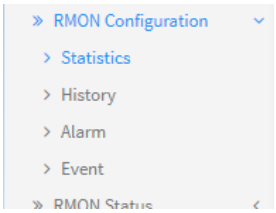
IP Address: IP address and UDP port for the accounting server in question.

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.

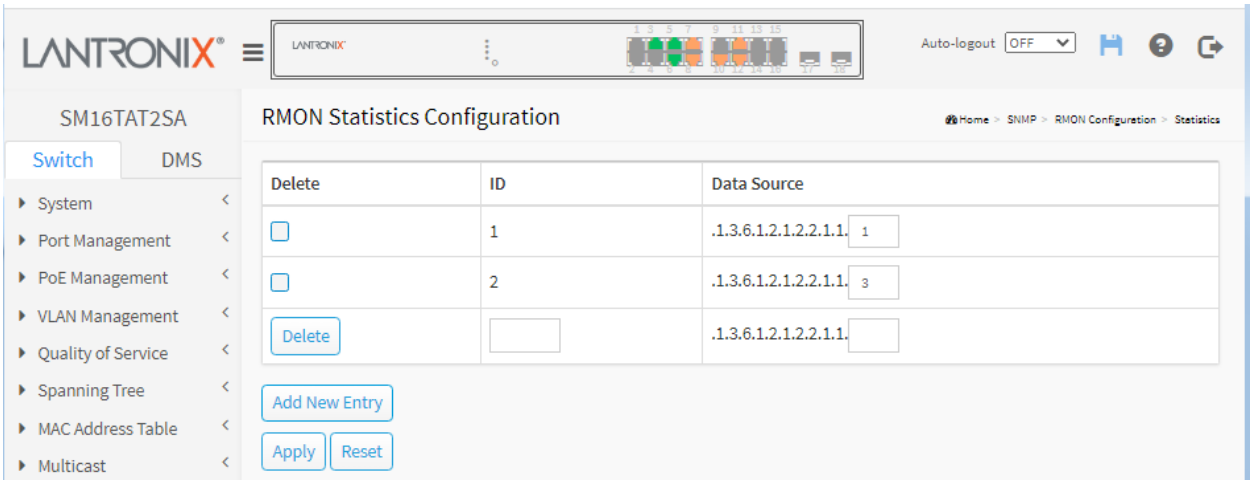
13.8 RMON Configuration



Navigate to the Switch >Security > RMON menu path to configure remote monitoring. Here you can configure and view RMON statistics, history, alarms, and events.

RMON Statistics Configuration

1. Navigate to Switch > SNMP > RMON Configuration > Statistics to display the RMON Statistics Configuration table.
2. Click the Add New Entry button.
3. Enter the desired parameters.
4. Click the Apply button to save the webpage changes to running-config.



Parameter descriptions:

Delete: Check the box to delete the table entry.

ID: Enter an ID for the instance.

Data Source: The port ID which you want to be monitored with RMON.

Buttons

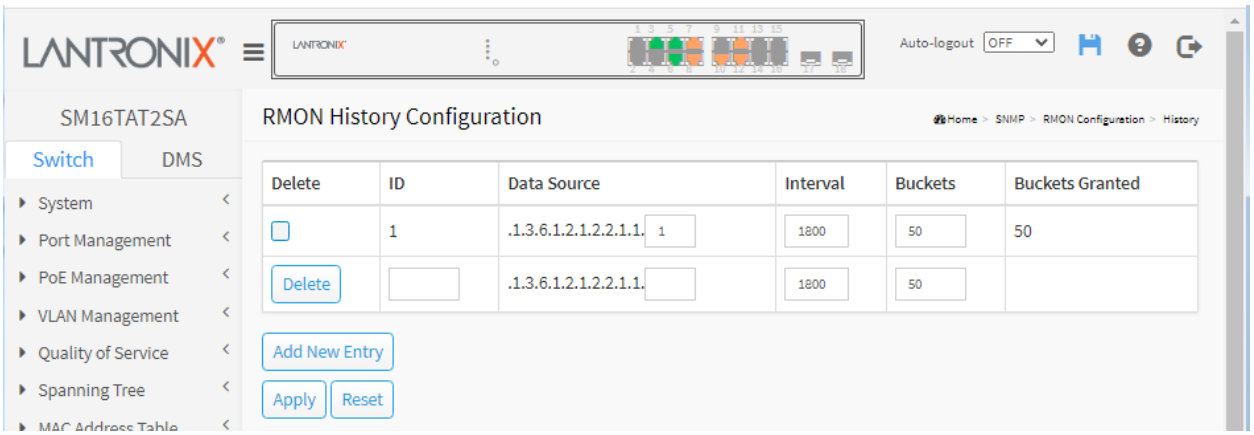
Add New Entry: Click the button to add a new row for configuring.

Apply: Click to save changes.

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

RMON History Configuration

Navigate to Switch > SNMP > RMON Configuration > History to display the RMON History Configuration page:



Delete: Check the box to delete the table entry.

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

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

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

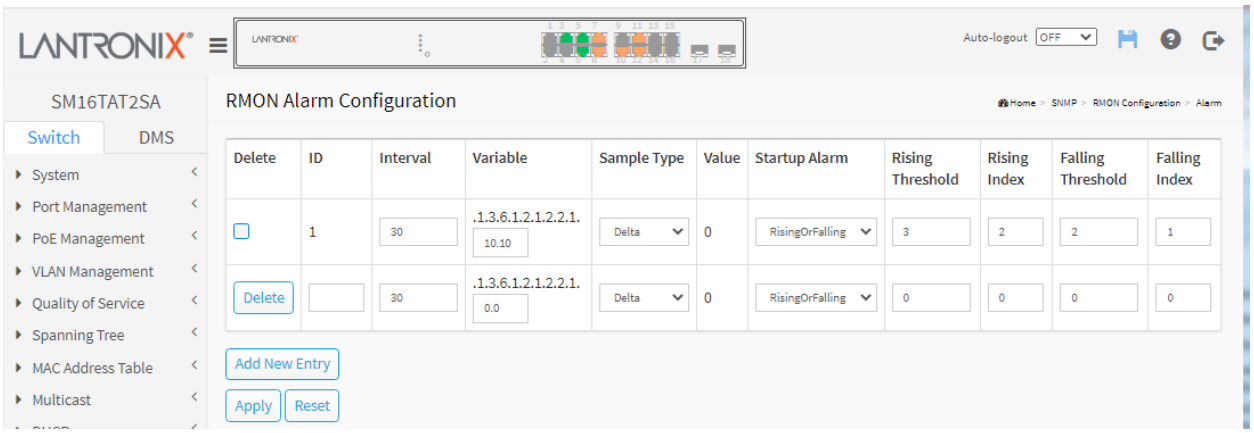
Buckets: Indicates the maximum data entries associated this History control entry stored in RMON. The valid range is 1 to 3600. The default value is 50. This is the RMON "buckets requested' value - the requested number of discrete time intervals over which data is to be saved in the part of the media-specific table associated with this historyControlEntry. When this object is created or modified, the probe should set historyControlBucketsGranted as closely to this object as is possible for the particular probe implementation and available resources. The default is 50 buckets.

Buckets Granted: The number of data saved in the RMON. The number of discrete sampling intervals over which data will be saved in the part of the media-specific table associated with this historyControlEntry.

See the RMON RFC (IETF RFC 2819) for details on the particular probe implementation and available resources.

RMON Alarm Configuration

Navigate to Switch > SNMP > RMON Configuration > Alarm to display the RMON Alarm Configuration page:



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, possible sample types are:

Delta: Delta sampling subtracts the current sample value from the last sample taken and then compares the difference to the threshold. Delta sampling is like a counter that records a value that is constantly increasing. The difference between samples of the selected variable is used when comparing against the thresholds.

Absolute: Absolute sampling compares the sample value directly to the threshold. Absolute sampling is like a gauge that records values that go up or down. An actual value of the selected variable is used when comparing against the thresholds.

Value: The value of the statistic during the last sampling period. (e.g., 72).

Startup Alarm: The alarm that may be sent when this entry is first set to valid (e.g., RisingOrFalling).

Rising Threshold: Rising threshold value.

Rising Index: Rising event index.

Falling Threshold: Falling threshold value.

Falling Index: Falling event index.

Buttons

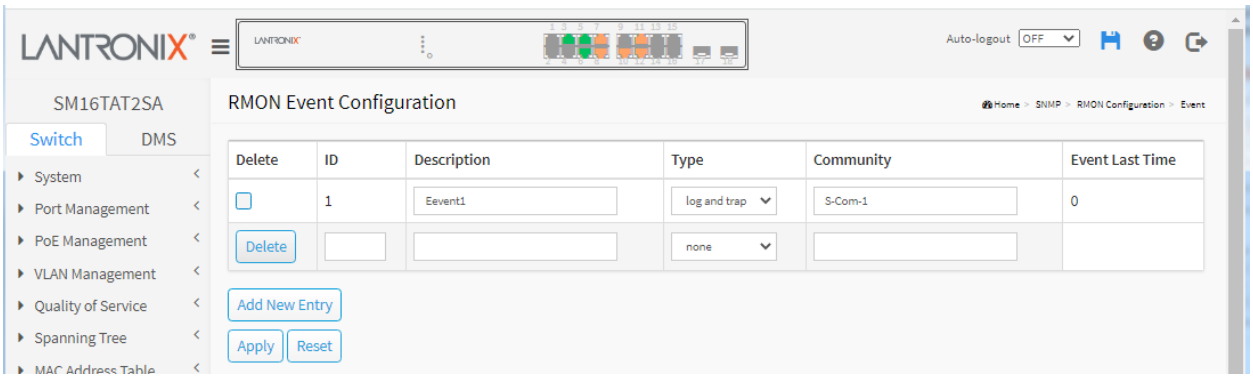
Add New Entry : Click to add new entry.

Apply : Click to save changes.

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

RMON Event Configuration

Navigate to Switch > SNMP > RMON Configuration > Event to display the RMON Event Configuration page:



ID: Enter the index of the RMON event. The valid range is 1 to 65535. Each ID entry must be unique.

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

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

none: No logging action is performed.

log: A syslog entry is added.

snmptrap: An SNMP trap event is sent.

logandtrap: A syslog entry is logged and an SNMP trap event is sent.

Community: Specify the community when a trap is sent; the string length is 0 to 127 characters. The default is "public".

Event Last Time: Indicates the value of sysUpTime at the time this event entry last generated an event (e.g., 33554560 or 33 days, 55 hours, 45 minutes, and 50 seconds).

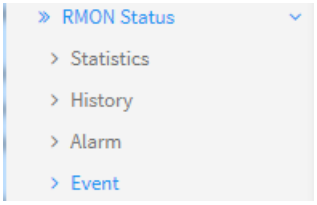
Buttons

Add New Entry : Click to add new entry.

Apply : Click to save changes.

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

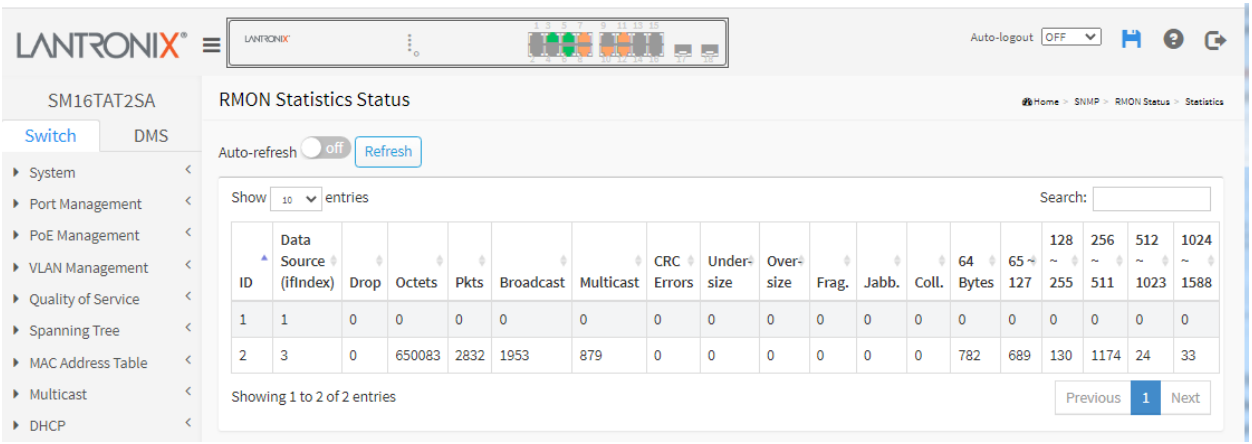
13.9 RMON Status



Navigate to the Switch > SNMP > RMON Status menu path to view RMON statistics, history, alarms, and events.

RMON Statistics Status

Navigate to Switch > SNMP > RMON Status > Statistics to display the RMON Statistics Status page:



Parameters:

ID: Indicates the index of Statistics entry.

Data Source (ifIndex): The data source which you want to be monitored.

Drop: The total number of events in which packets were dropped by the probe due to lack of resources.

Octets: The total number of octets of data (including those in bad packets) received on the network.

Pkts: The total number of packets (including bad packets, broadcast packets, and multicast packets) received.

Broad-cast: The total number of good packets received that were directed to the broadcast address.

Multi-cast: The total number of good packets received that were directed to a multicast address.

CRC Errors: The total number of packets received that had a length (excluding framing bits, but including FCS octets) of between 64 and 1518 octets.

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 with a size is less than 64 octets received with invalid CRC.

Jabb.: The number of frames which size is larger than 64 octets received with invalid CRC.

Coll.: The best estimate of the total number of collisions on this Ethernet segment.

64 Bytes: The total number of packets (including bad packets) received that were 64 octets in length.

65~127: The total number of packets (including bad packets) received that were 65 to 127 octets in length.

128~255: The total number of packets (including bad packets) received that were 128 to 255 octets long.

256~511: The total number of packets (including bad packets) received that were 256 to 511 octets long.

512~1023: The total number of packets (including bad packets) received that were 512 to 1023 octets long.

1024~1588: The total number of packets (including bad packets) received that were 1024 to 1588 octets long.

Buttons

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

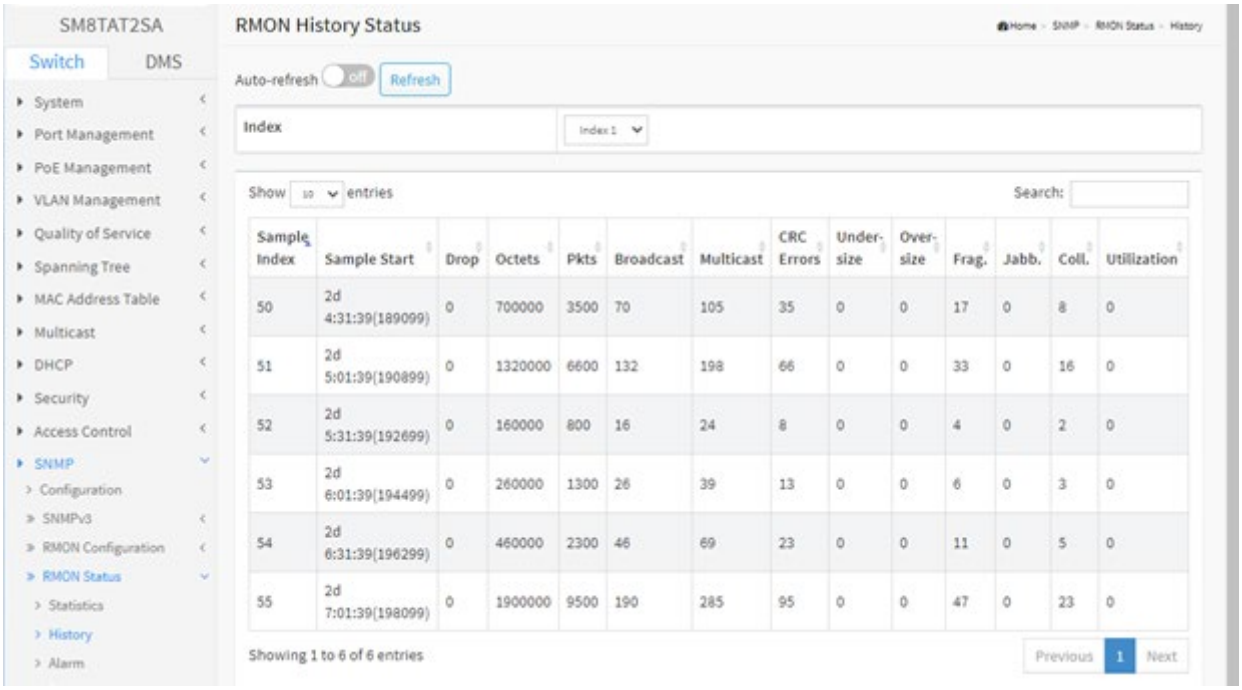
Refresh : Click to refresh the page immediately.

Previous : Updates the entries, turn to the previous page.

Next : Updates the entries, turn to the next page.

RMON History Status

Navigate to Switch > SNMP > RMON Status > History to display the RMON History Status page:



Parameters:

Sample Index: Indicates the index of the data entry associated with the control entry

Sample Start: The total number of events in which packets were dropped by the probe due to lack of resources.

Drops: 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.

Undersize: The total number of packets received that were less than 64 octets.

Oversize: The total number of packets received that were longer than 1518 octets.

Frag.: The number of frames which size is less than 64 octets received with invalid CRC.

Jabb.: The number of frames which size is larger than 64 octets received with invalid CRC.

Coll.: The best estimate of the total number of collisions on this Ethernet segment.

Utilization: The best estimate of the mean physical layer network utilization on this interface during this sampling interval, in hundredths of a percent (.01% sampling interval).

Buttons

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

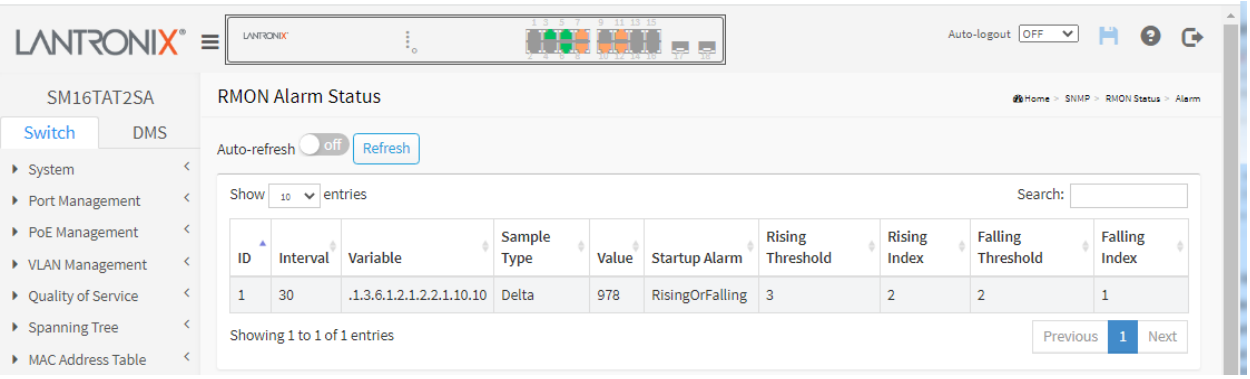
Refresh : Click to refresh the page immediately.

Previous : Updates the entries, turn to the previous page.

Next : Updates the entries, turn to the next page.

RMON Alarm Status

Navigate to Switch > SNMP > RMON Status > Alarm to display the RMON Alarm Status page:



Parameters:

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. Possible sample types are:

Delta: Delta sampling subtracts the current sample value from the last sample taken and then compares the difference to the threshold. Delta sampling is like a counter that records a value that is constantly increasing. The difference between samples of the selected variable is used when comparing against the thresholds.

Absolute: Absolute sampling compares the sample value directly to the threshold. Absolute sampling is like a gauge that records values that go up or down. An actual value of the selected variable is used when comparing against the thresholds.

Value: The value of the statistic during the last sampling period. (e.g., 72).

Startup Alarm: The alarm that may be sent when this entry is first set to valid (e.g., RisingOrFalling).

Rising Threshold: Rising threshold value.

Rising Index: Rising event index.

Falling Threshold: Falling threshold value.

Falling Index: Falling event index.

Buttons

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

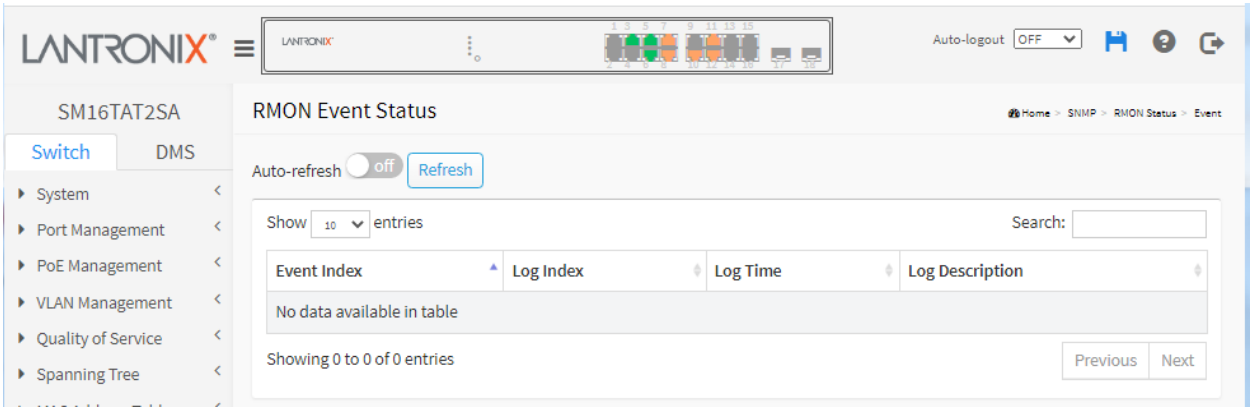
Refresh : Click to refresh the page immediately.

Previous : Updates the entries, turn to the previous page.

Next : Updates the entries, turn to the next page.

RMON Event Status

Navigate to Switch > SNMP > RMON Status > Event to display the RMON Event Status page:



Parameters:

Event Index: Indicates the index of the event entry.

Log Index: Indicates the index of the log entry.

Log Time: Indicates the time that the Event was logged.

Log Description: Indicates the Event description.

Buttons

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

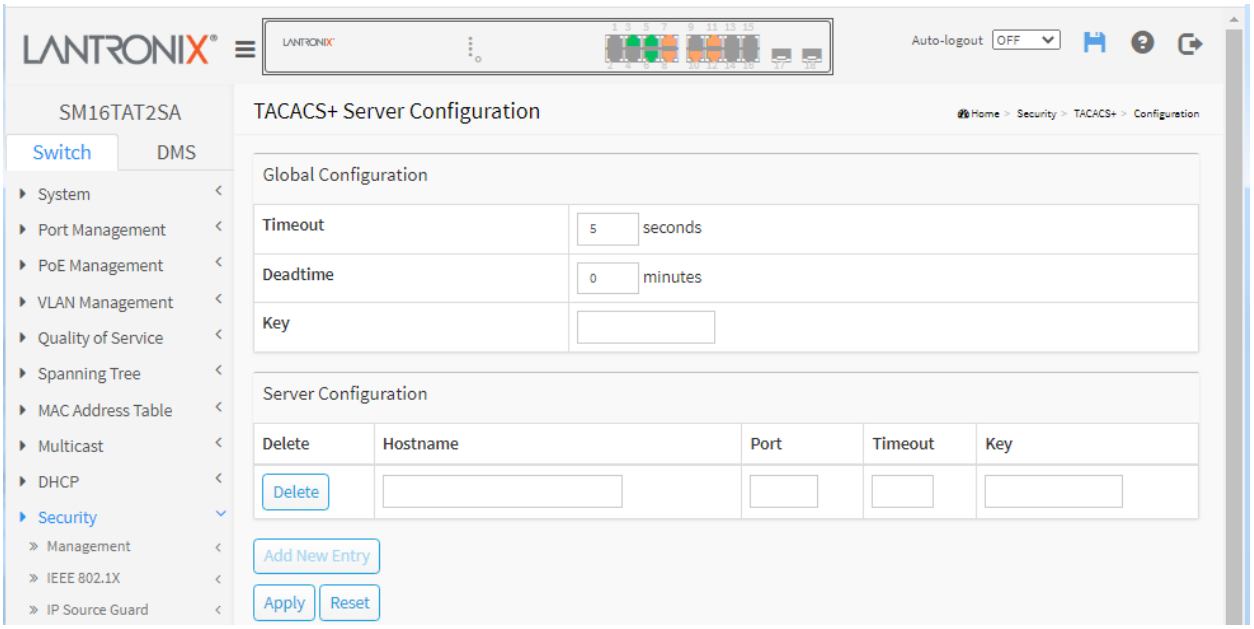
Refresh : Click to refresh the page immediately.

Previous : Updates the entries, turn to the previous page.

Next : Updates the entries, turn to the next page.

12.10 TACACS+ Configuration

Navigate to Switch >Security >TACACS+ > Configuration to display the TACACS+ Server Configuration page. Here you can configure up to six TACACS+ servers.



Global Configuration Parameters:

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

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

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

: Click to display the Key text as you enter it.

: Click to hide the Key text as you enter it.

Server Configuration Parameters:

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 for TACACS+ server for authentication.

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

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

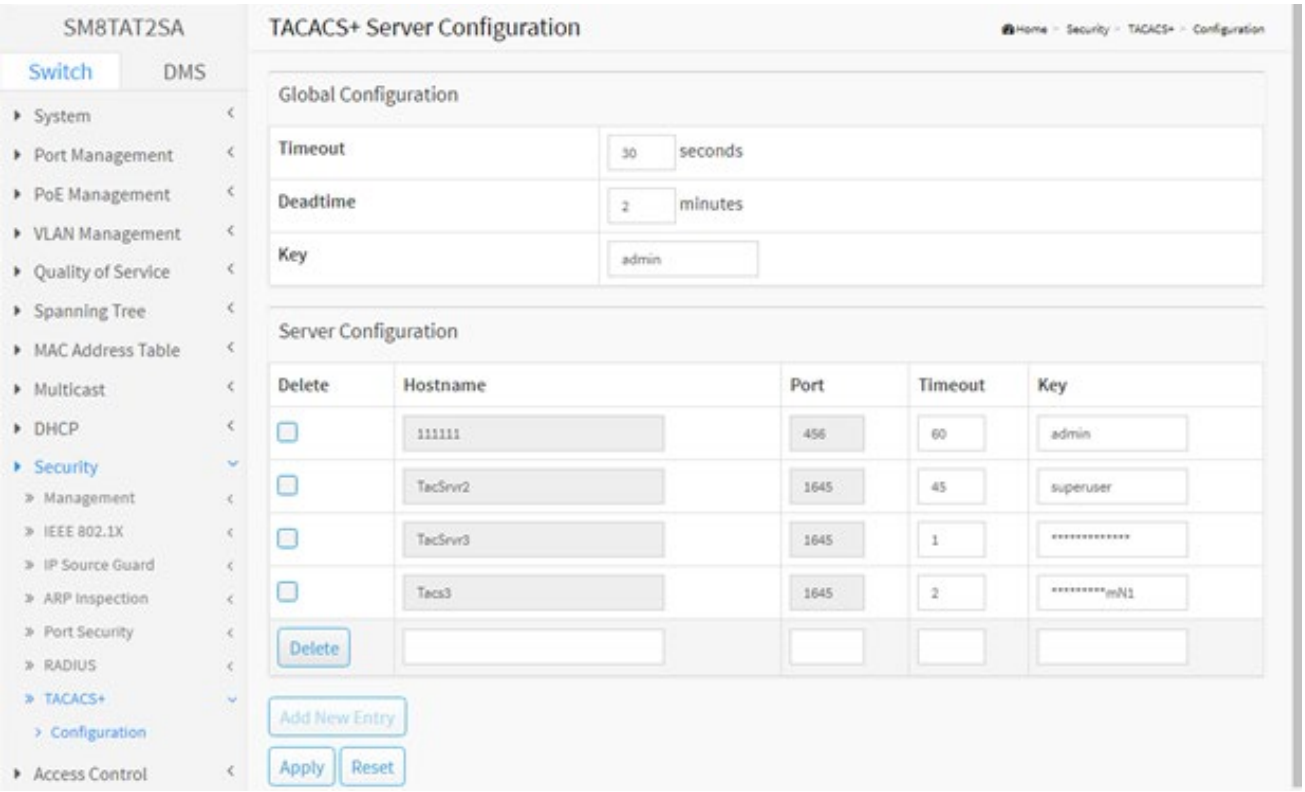
Buttons

Add New Entry: 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 6 servers are supported.

Apply: Click to save changes.

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

Example:



Messages:

Authentication Error *HTTPD cache has no valid entry*

Hostname must be a valid hostname, unicast IPv4, or unicast IPv6 address

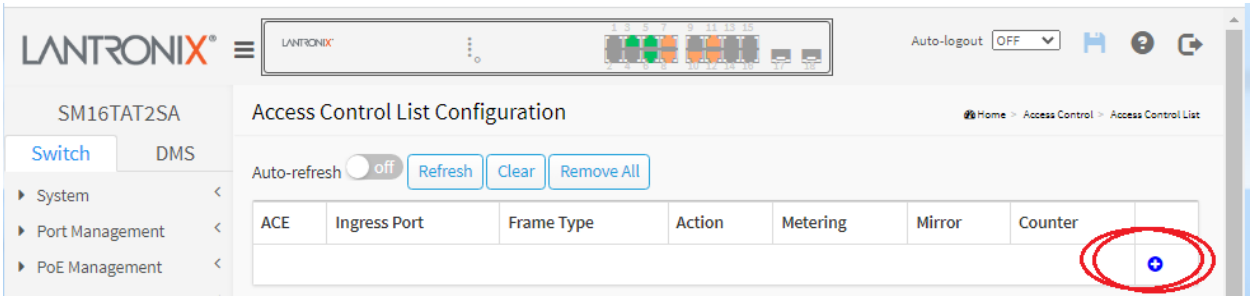
Meaning: You entered an invalid Key or Hostname parameter.

Recovery: **1.** Click the Previous button to clear the error message. **2.** Re-enter a valid Key or Hostname parameter. **3.** Continue operation.

13.11 Access Control List

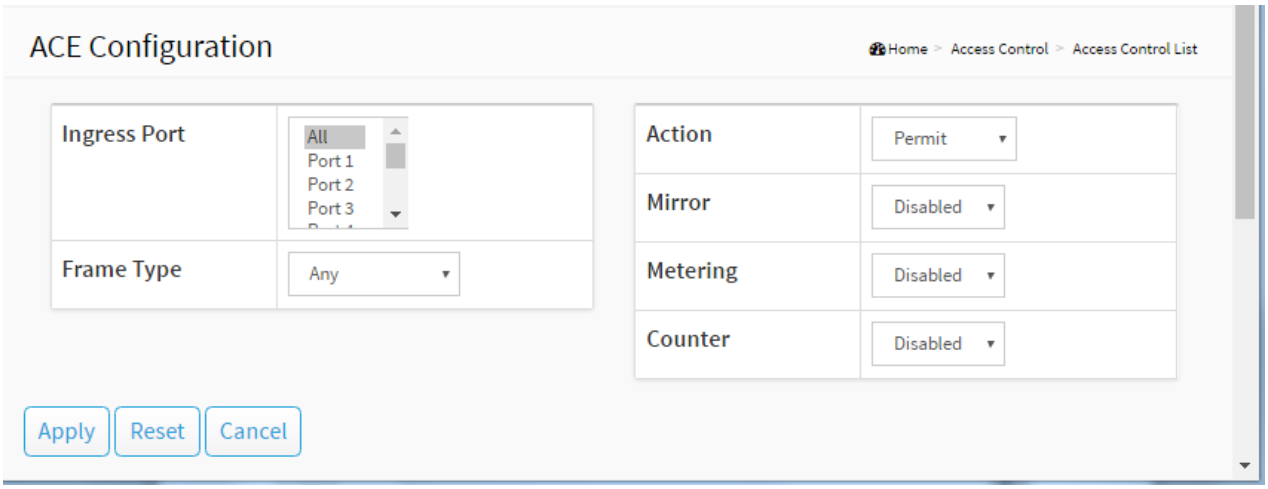
This page lets you configure Access Control List rules. An Access Control List (ACL) is a sequential list of permit or deny conditions that apply to IP addresses, MAC addresses, or other more specific criteria. This switch tests ingress packets against the conditions in an ACL one by one. A packet will be accepted as soon as it matches a permit rule or dropped as soon as it matches a deny rule. If no rules match, the frame is accepted. Other actions can also be invoked when a matching packet is found, including rate limiting, copying matching packets to another port or to the system log, or shutting down a port. This page shows the Access Control List (ACL), which is made up of the ACEs defined on this switch. Each row describes the ACE that is defined. The maximum number of ACEs is 256 on each switch. Click on the lowest plus sign to add a new ACE to the list. Reserved ACEs are used for internal protocol and cannot be edited or deleted; the order sequence cannot be changed and the priority is highest.

Navigate to Switch >Access Control List > Access Control List to display the default Access Control List Configuration page:

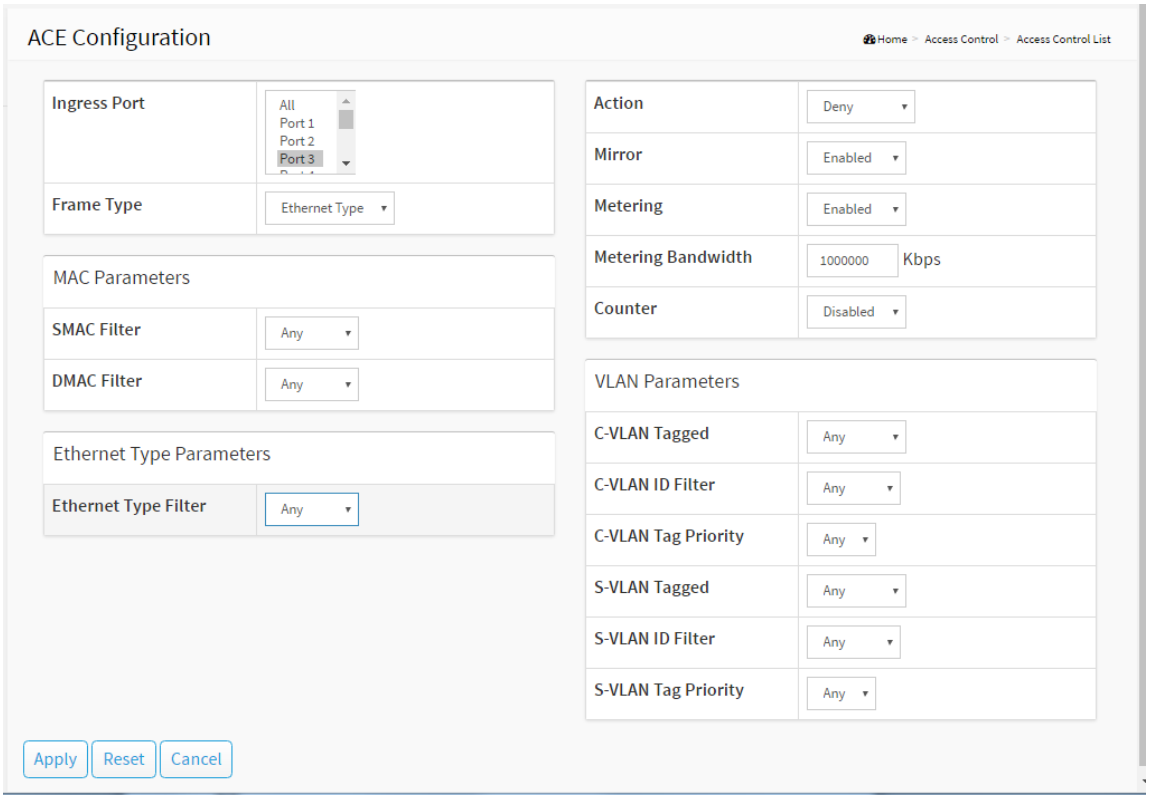


Click the icon to add an ACE from the ACE Configuration page:

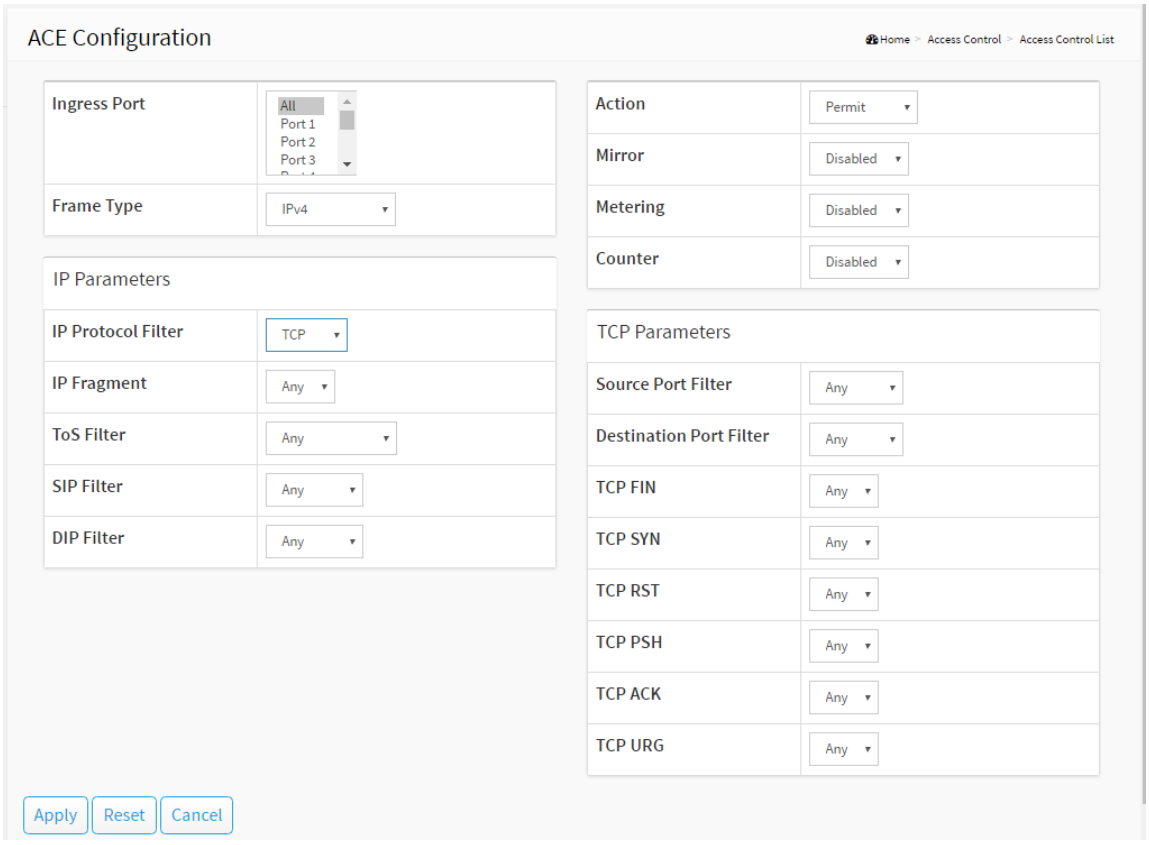
ACE Configuration / Frame Type: Any



ACE Configuration / Frame Type: Ethernet Type



ACE Configuration / Frame Type: IPv4



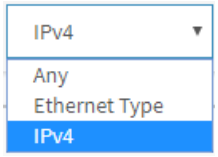
ACE Configuration Parameters:

ACE: Indicates the ACE ID.

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

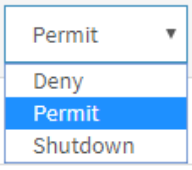
All: The ACE will match all ingress port.
Port: The ACE will match a specific ingress port.

Frame Type: Indicates the frame type of the ACE. Possible values are:
Any: The ACE will match any frame type.
Ethernet Type: The ACE will match Ethernet Type frames. Note that an Ethernet Type based ACE will not get matched by IP and ARP frames.
IPv4: The ACE will match all IPv4 frames.



Action: Indicates the forwarding action of the ACE. Possible values are:

Permit: Frames matching the ACE may be forwarded and learned.
Deny: Frames matching the ACE are dropped.
Shutdown: Specify the port shut down operation of the ACE.



Metering: Enable or disable metering mode. The default value is "Disabled".

Metering Bandwidth: Enter an integer value between 16 and 1000000 Kbps.

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.

MAC Parameters

SMAC Filter: Specify the source MAC filter for this ACE. (Only displayed when the frame type is Ethernet Type or ARP.) Any: No SMAC filter is specified. (SMAC filter status is "don't-care".) Specific: If you want to filter a specific source MAC address with this ACE, choose this value. A field for entering an SMAC value displays.

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

DMAC Filter: Specify the destination MAC filter for this ACE. Any: No DMAC filter is specified. (DMAC filter status is "don't-care".) MC: Frame must be multicast. BC: Frame must be broadcast. UC: Frame must be unicast. Specific: If you want to filter a specific destination MAC address with this ACE, choose this value. A field for entering a DMAC value displays.

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 displays.

VLAN ID: When "Specific" is selected for the VLAN ID filter, you can enter a specific VLAN ID number. The valid range is 1 to 4094. 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 valid number range is 0 to 7. The value Any means that no tag priority is specified (tag priority is "don't-care".)

IPv4 Parameters

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

IP Protocol Filter: Specify the IP protocol filter for this ACE. ***Any***: No IP protocol filter is specified ("don't-care"). ***ICMP***: Select ICMP to filter IPv4 ICMP protocol frames. Extra fields for defining ICMP parameters will appear. These fields are explained later in this section. ***UDP***: Select UDP to filter IPv4 UDP protocol frames. Extra fields for defining UDP parameters will appear. These fields are explained later in this section. ***TCP***: Select TCP to filter IPv4 TCP protocol frames. Extra fields for defining TCP parameters will display. These fields are explained later in this section. Other: If you want to filter another specific IP protocol filter with this ACE, choose this value. A field for entering an IP protocol filter displays.

IP Protocol Value: When "Specific" is selected for the IP protocol value, you can enter a specific value. The valid 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 DIP Filter, you can enter a specific DIP address in dotted decimal notation.

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

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 Parameters

Source Port 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.

Source Port 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.

Source Port 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.

Destination Port 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 displays.

Dest. Port No.: 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.

Destination Port 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: One of several TCP flag names used only when filtering TCP (urg, ack, psh, rst, syn, and 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: One of several TCP flag names used only when filtering TCP (urg, ack, psh, rst, syn, and fin). 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: One of several TCP flag names used only when filtering TCP (urg, ack, psh, rst, syn, and fin). 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: One of several TCP flag names used only when filtering TCP (urg, ack, psh, rst, syn, and fin). 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: One of several TCP flag names used only when filtering TCP (urg, ack, psh, rst, syn, and fin). 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: One of several TCP flag names used only when filtering TCP (urg, ack, psh, rst, syn, and fin). 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").

UDP Parameters

Source Port 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.

Source Port 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.

Source Port 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.

Dest. Port Filter: 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.

Destination Port 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.

Ethernet Type Parameters

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

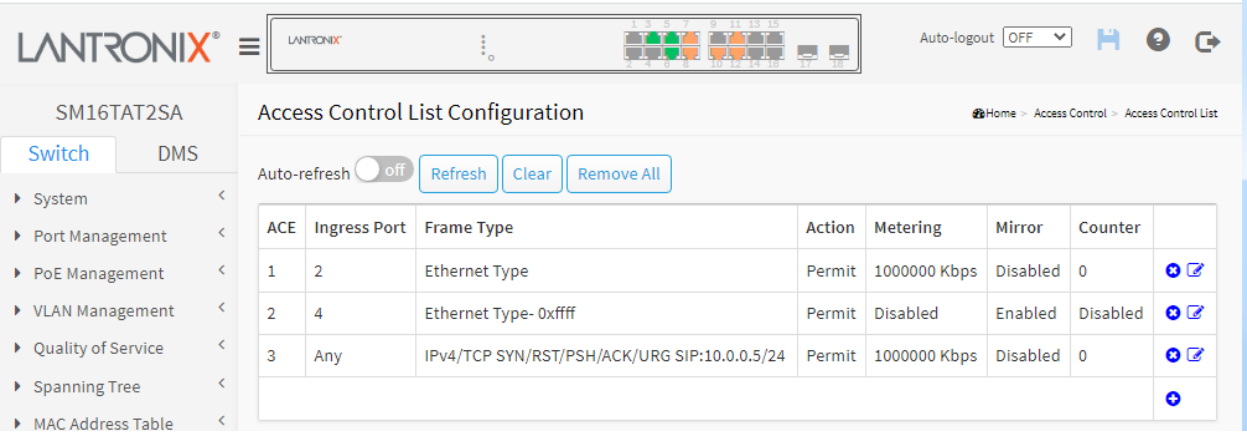
EtherType Filter: Specify the Ethernet type filter for this ACE.

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.

Example:



Control Icons

Add ACE to end of list.

Edit ACE on this line.

Delete ACE on this line.

Buttons

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

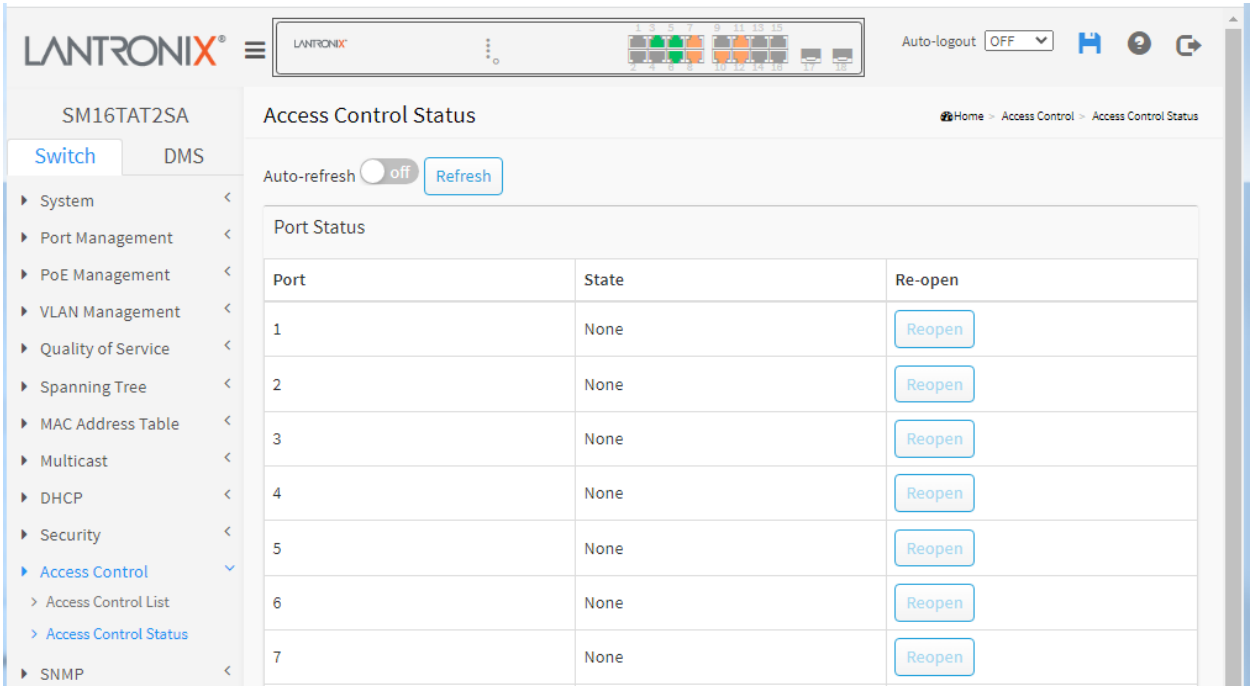
Refresh : Click to manually update webpage information immediately.

Clear : Click to clear the ACL configuration information.

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

13.12 Access Control Status

This page displays the Access Control status.



Port: The port number of the access control status.

State: Shows the current state of the port. It can take one of two values:

None: The port is normally used.
Shutdown: The port is shut down by ACL rule.

Re-open button: Click to recover the shutdown port that triggered by ACL rule.

Buttons

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

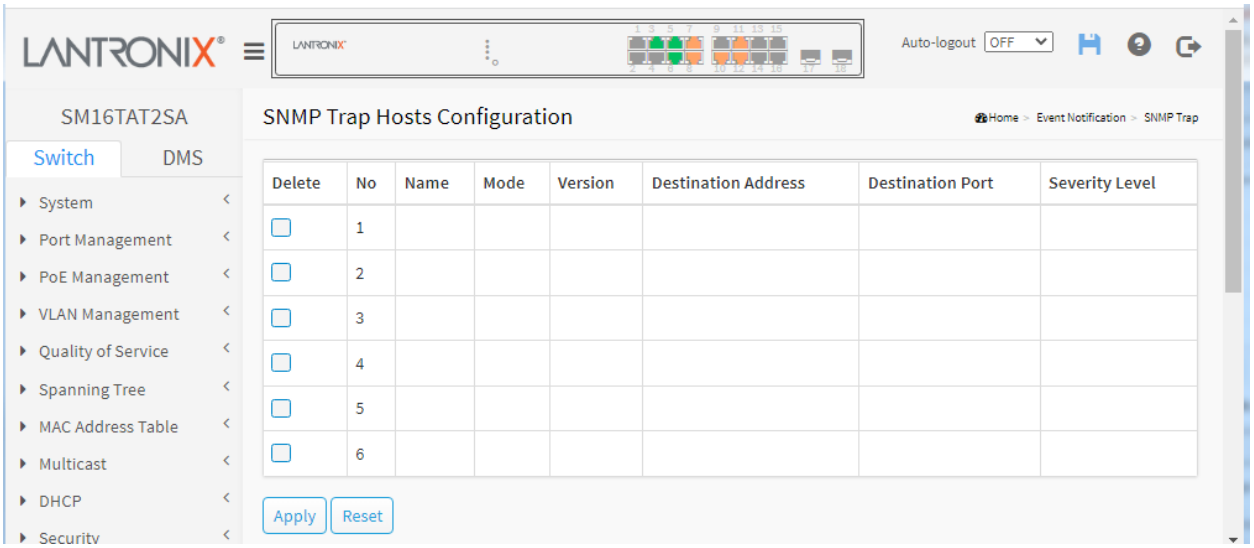
Refresh: Click to manually refresh the page immediately.

13.13 Switch > Event Notification

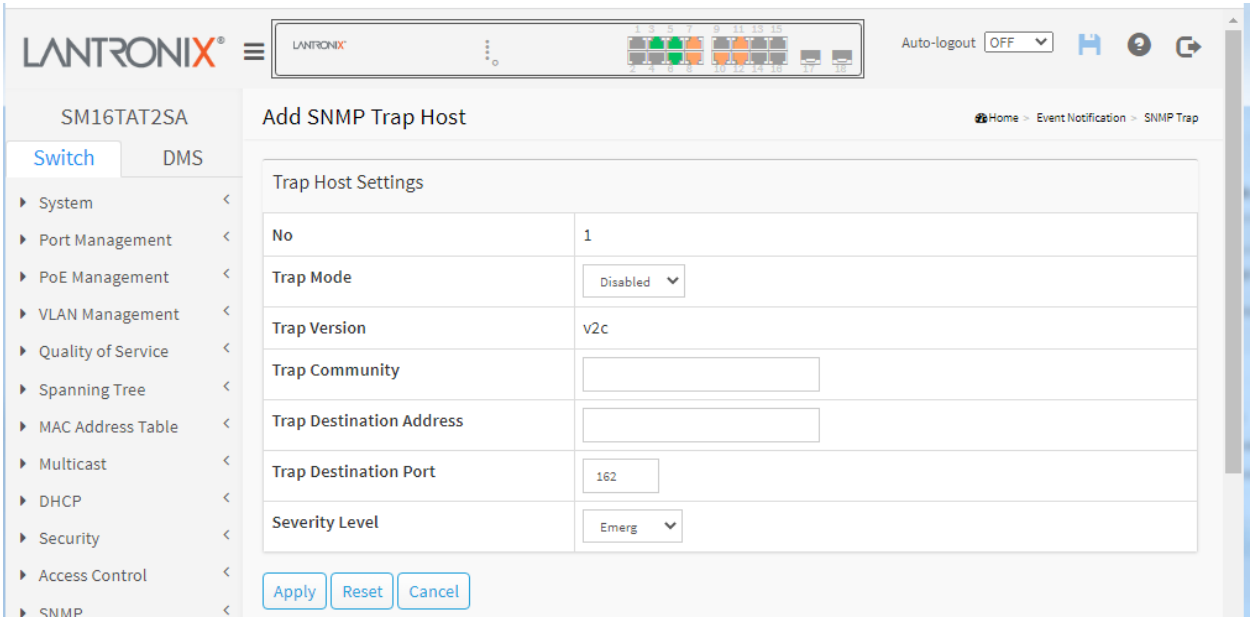
This menu path displays the SNMP Trap, Syslog, and Event Notification menu options.

13.13.1 Switch > Event Notification > SNMP Trap

Navigate to the Switch > Event Notification > SNMP Trap menu path to display the SNMP Trap Hosts Configuration table. Here you can add and configure up to six SNMP Trap hosts.



Click a line to display its configurable parameters:

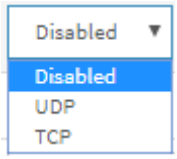


Parameters:

No: Displays the instance number for this line in the table.

Trap Name: Indicates the community access string when sending SNMP trap packet. This comes from the Trap Community parameter (see below).

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



Disabled: Disable SNMP mode operation (default).

UDP: Enable UDP SNMP mode operation.

TCP: Enable TCP SNMP mode operation.

Trap Version: The SNMP trap version. SNMP trap supports version 2c.

Trap Community: Enter the SNMP community name. This is the community access string when sending SNMP trap packet. The allowed string length is 1-32 characters, and the allowed content is ASCII characters 33 - 126. This becomes the "Name" parameter.

Trap Destination Address: Indicates the SNMP trap destination address.

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

Severity Level: At the dropdown select what level of message to send to trap server. Possible levels are:

Emerg: Emergency; System is unusable.

Alert: Action must be taken immediately.

Crit: Critical conditions.

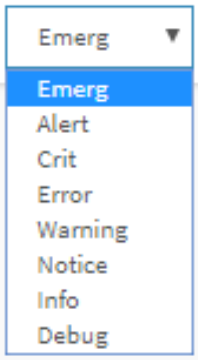
Error: Error conditions.

Warning: Warning conditions.

Notice: Normal but significant conditions.

Info: Information messages.

Debug: Debug-level messages.



Buttons

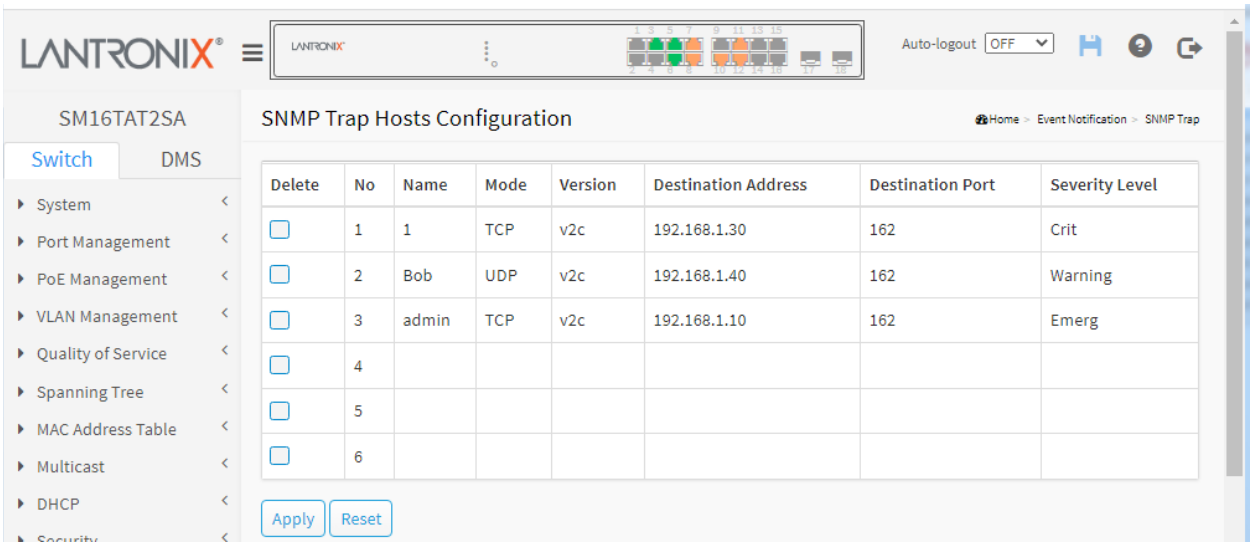
Apply: Click to save changes.

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

Cancel: Click to cancel the page edits.

Example

The screen below shows three SNMP Trap Hosts configured:



13.13.2 Switch > Event Notification > eMail

The Switch > Event Notification > eMail menu path displays the SMTP Configuration page. Configure SMTP (Simple Mail Transfer Protocol) on this page. Simple Mail Transfer Protocol is the message-exchange standard for the Internet.

The switch is to be configured as a client of SMTP while the server is a remote device that will receive messages from the switch on which the alarm events occurred.

To configure SMTP via the web UI:

1. Click Event Notification, Syslog, and eMail.
2. Specify the SMTP Configuration parameters.
3. Click Apply.

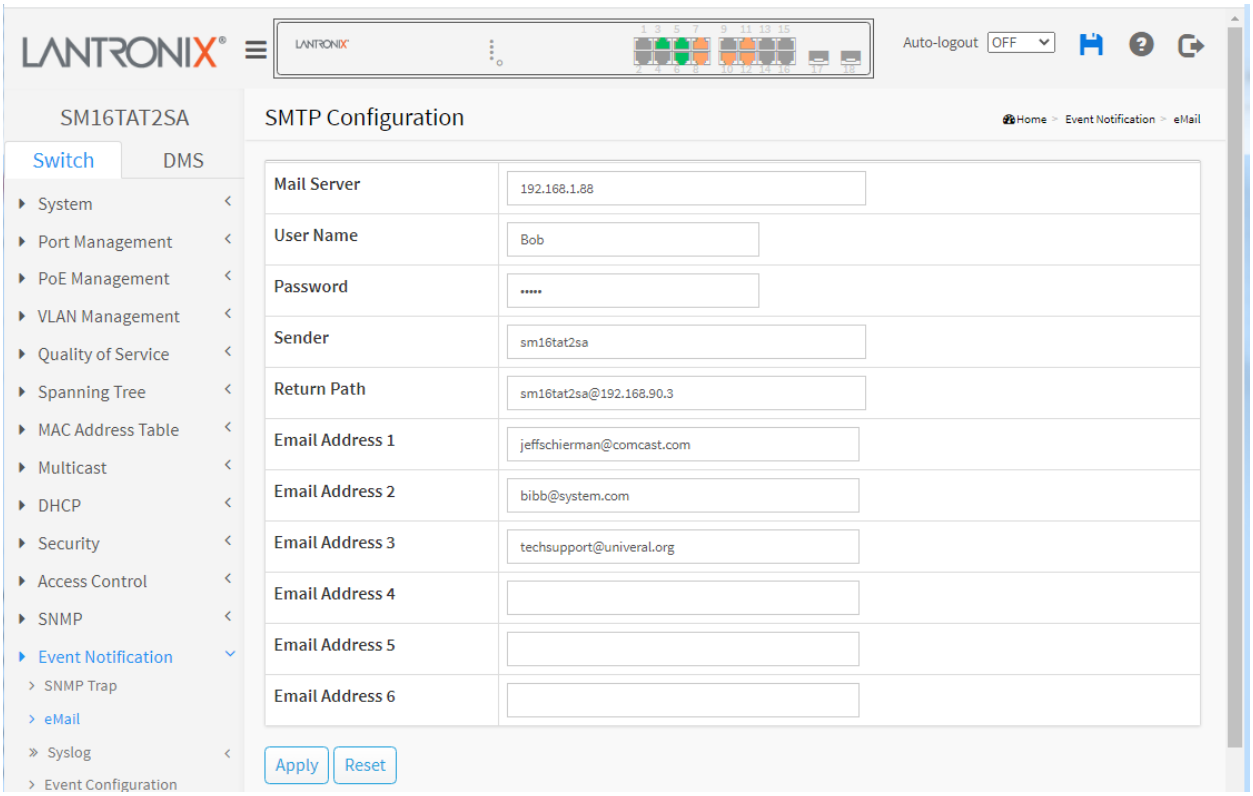


Figure 13-13.1: SMTP Configuration page

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 email 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 the email address of the receiver.

Buttons

Apply: Click to save changes.

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

13.13.3 Switch > Event Notification > Syslog

The Switch > Event Notification > Syslog menu path provides the Syslog Configuration and View Log menu options.

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

13.13.3.1 Syslog Configuration

Here you can enable System Logging and provide an IP Address for up to six Syslog servers.

To configure Syslog Configuration in the web interface:

4. Click Event Notification, Syslog, and Syslog Configuration.
5. At Mode, select "on" to enable Syslog globally.
6. Specify the syslog parameters including the IP Address of Syslog server and Port number.
7. Click Apply.

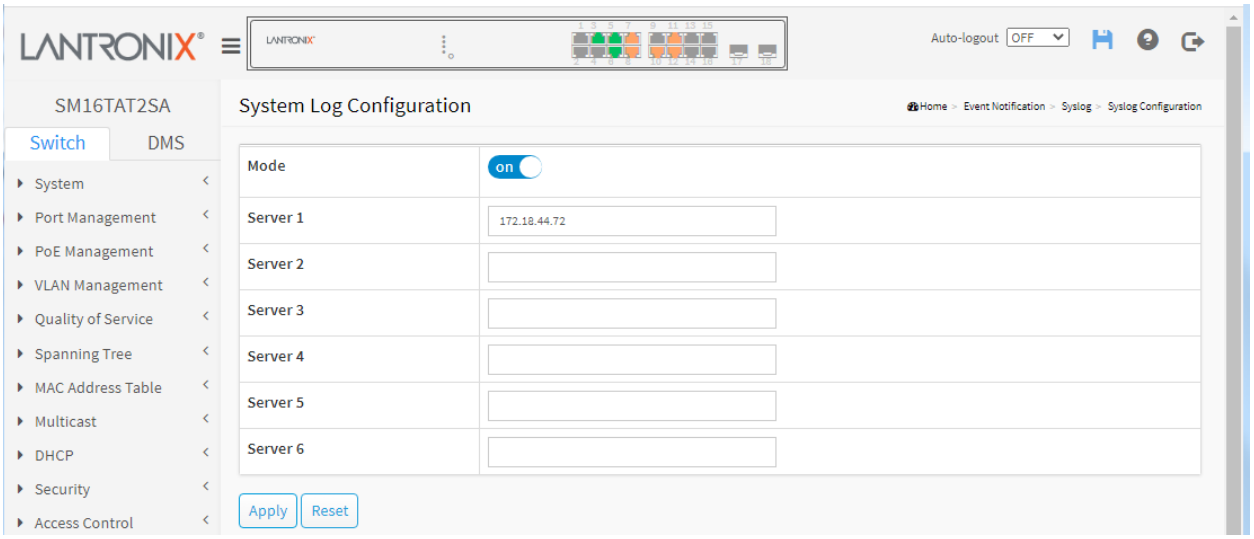


Figure 13-13.3.1: System Log Configuration page

Parameter descriptions:

Mode: Select the server mode of operation. When the mode is "on" (enabled) syslog messages will be sent out to the configured 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 to the sender since UDP is a connectionless protocol and it does not provide acknowledgments. The syslog packet is always sent out even if the syslog server does not exist. Possible modes are:

On: Enable server mode operation.

Off: Disable server mode operation.

Server 1 to 6: Indicates the IPv4 hosts address of syslog server. If the switch provides DNS, it also can be a host name (FQDN).

Buttons

Apply: Click to save changes.

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

13.13.3.2 View Log

This page displays the switch system log (Syslog) information. To display the log configuration in the web interface:

1. Click Event Notification, Syslog, and View Log.
2. Observe the log information.

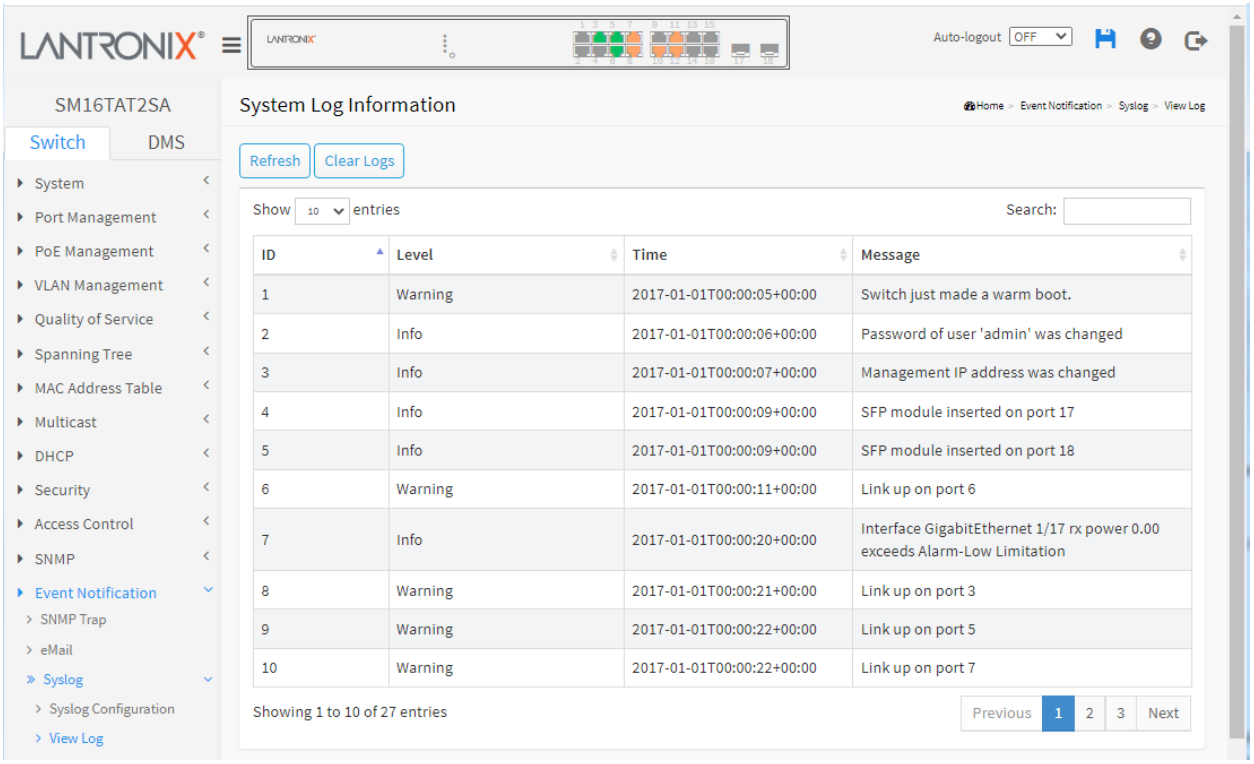


Figure 13-13.3.2: System Log Information page

Parameter descriptions:

ID: **The** ID of the system log entry.

Level: the 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 conditions.

***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 (e.g., LINK-UPDOWN).

Search: Lets you search for the information that you want to view.

Show entries: Lets you choose how many items you want to view per page (i.e., 10, 25, 60, ALL).

Buttons

Refresh: Updates the system log entries, starting from the current entry ID.

Clear Logs: Clears all the system log entries and display "*No data available in table*".

Next: Updates the system log entries, turn to the next page.

Previous: Updates the system log entries, turn to the previous page.

System Log Message Examples

Warning LINK-UPDOWN: Interface GigabitEthernet 1/1, changed state to up.

Warning WARM-START: Switch just made a warm boot.

Info LOGIN: Login passed for user 'admin'

Info LOGOUT: User '' logout

Warning SFP: Interface GigabitEthernet 1/17 rx power 0.00 exceeds Alarm-Low Limitation

Warning POE-PD-OFF: Port 3 PoE PD off

Warning LINK-UPDOWN: Interface GigabitEthernet 1/7, changed state to up.

Info SFP: Interface GigabitEthernet 1/17 rx power 0.00 exceeds Alarm-Low Limitation

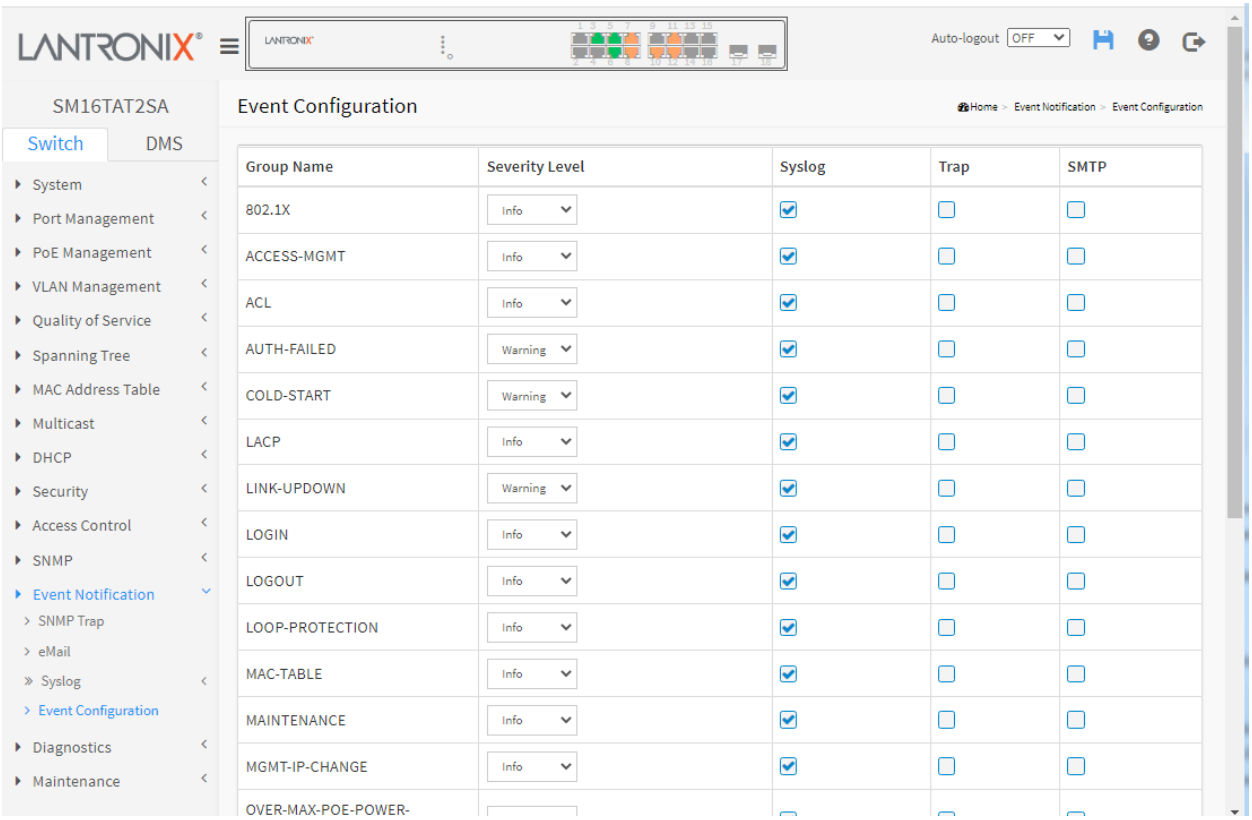
Info LACP: LACP was enabled on port 2 w ith key 1

Alert MGMT-IP-CHANGE: Management IPv4 address of interface VLAN 1 was changed

Info SFP: SFP module inserted on port 9

13.13.3 Event Configuration

The Event Notification > Event Configuration page displays the Event Configuration table. Here you can view and configure severity levels, Syslog status, and Trap status for each Group Name.



Parameters:

Group Name: The name identifying the severity group.

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

Emergency:	System is unusable.
Alert:	Action must be taken immediately.
Critical:	Critical conditions.
Error:	Error conditions.
Warning:	Warning conditions.
Notice:	Normal but significant conditions.
Information:	Information messages.
Debug:	Debug-level messages.

Syslog: Check the checkbox to enable Syslog for this Group Name.

Trap: Check the checkbox to enable Syslog for this Group Name.

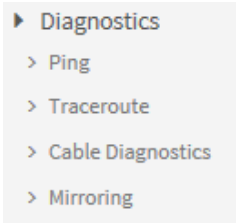
SMTP : Check the checkbox to enable SMTP email events for this Group Name.

Buttons

Apply: Click to save changes.

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

Chapter 14 Diagnostics



This module provides basic system diagnostics to help you determine system health. The diagnostics include Ping, Traceroute, Cable Diagnostics, and Mirroring.

14-1 Ping

This page lets you issue ICMP Ping packets to troubleshoot IPv4 or IPv6 connectivity issues.

To configure a PING in the web interface:

1. Click Diagnostics and Ping.
2. Specify IP Address, IP Version, Ping Length, and Ping Count.
3. Click Start.

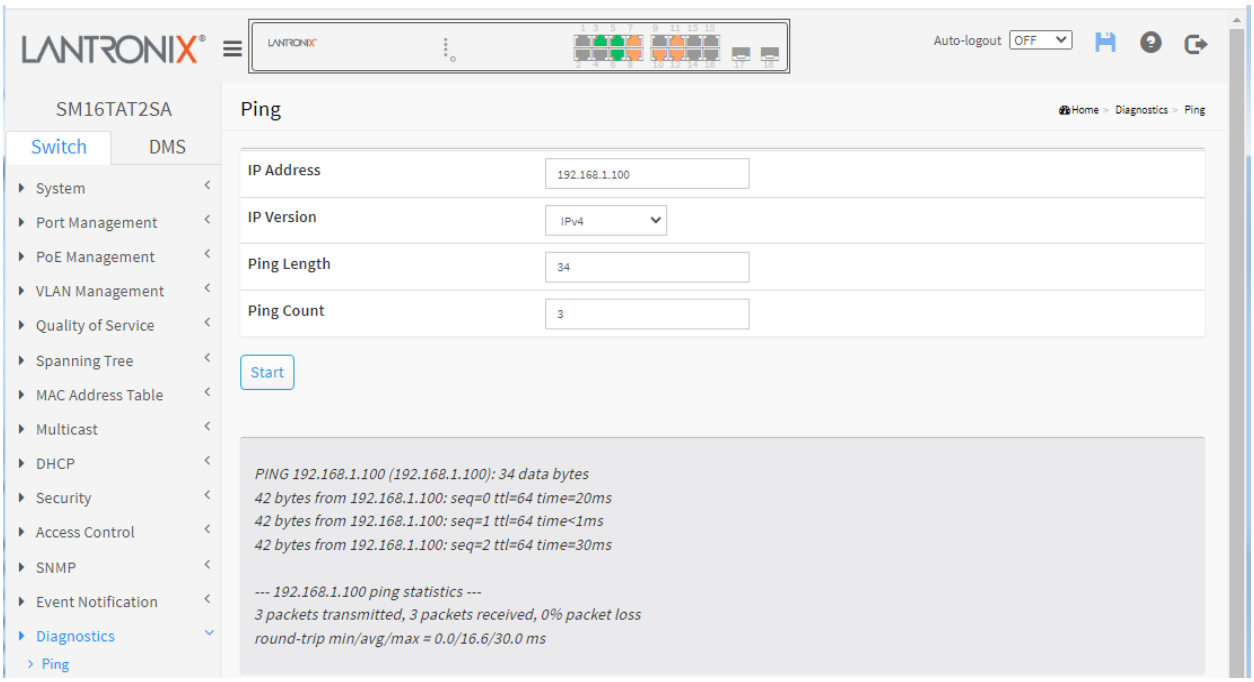
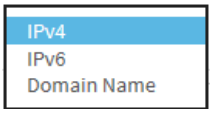


Figure 14-1: Ping Diagnostic page

Parameter descriptions:



IP Address: Enter the IP Address of the device that you want to ping.

IP Version: Select the required IP Version (IPv4, IPv6, or Domain Name).

Egress Interface: Specify an interface VLAN for sending ICMPv6 Echo packets.

Ping Length: The payload size of the ICMP packet. Values range from 1-1452 bytes.

Ping Count: The count of the ICMP packet. Values range from 1-60 times.

Start: Click the "Start" button to start to ping the target IP address.

After you press **Start**, five ICMP packets are transmitted, and the sequence number and roundtrip time are displayed upon reception of a reply. The page refreshes automatically until responses to all packets are received, or until a timeout occurs.

***Successful* Ping**:

```
PING 192.168.1.77 (192.168.1.77): 56 data bytes
64 bytes from 192.168.1.77: seq=0 ttl=64 time=0.000 ms
64 bytes from 192.168.1.77: seq=1 ttl=64 time=0.000 ms
64 bytes from 192.168.1.77: seq=2 ttl=64 time=0.000 ms
64 bytes from 192.168.1.77: seq=3 ttl=64 time=0.000 ms
64 bytes from 192.168.1.77: seq=4 ttl=64 time=0.000 ms

--- 192.168.1.77 ping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max = 0.000/0.000/0.000 ms
```

***Failed* Ping**:

```
PING 192.168.1.32 (192.168.1.32): 56 data bytes
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Request timed out.

--- 192.168.1.32 ping statistics ---
5 packets transmitted, 0 packets received, 100% packet loss
```

Messages:

Please enter a valid IP v4 address.

Please enter a valid IP v6 address.

Please enter a valid domain name address.

14-2 Traceroute

This page allows you to issue ICMP or UDP packets to diagnose network connectivity issues.

To configure a traceroute in the web UI:

1. Click Diagnostics and Traceroute.
2. Specify IP Address, IP Version, IP Protocol, Wait Time, Maximum TTL, and Probe Count.
3. Click Start.

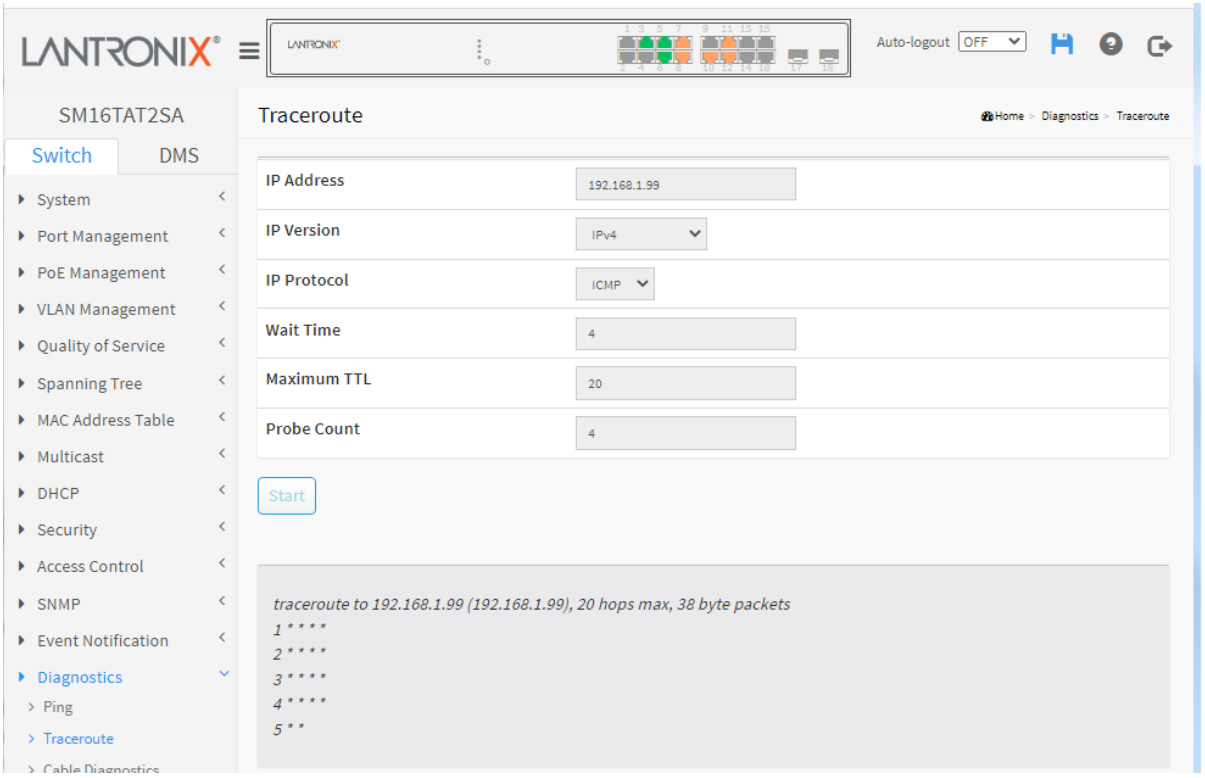


Figure 14-2: Traceroute page

Parameter descriptions:

IP Address: The destination IP Address.

IP Version: Select the IP Version (IPv4, IPv6, or Domain Name).

IP Protocol: The protocol (ICMP or UDP) packets to send.

Egress Interface: Specify an egress interface for sending traceroute packets. Only used in IPv6.

Wait Time: Set the time (in seconds) to wait for a response to a probe (default 5.0 sec). Values range from 1 to 60. The payload size of the ICMP packet. Values range from 2 bytes to 1452 bytes.

Maximum TTL: Specify the maximum number of hops (max time-to-live value) traceroute will probe. Values range from 1 to 255. The default is 30.

Probe Count: Sets the number of probe packets per hop. Valid values are 1 - 10. The default is 3.

Button

Start: Begin traceroute to the IP address that you selected.

Message: *traceroute: can't connect to remote host: Network is unreachable*

14-3 Cable Diagnostics

This section is used for running the Cable Diagnostics for copper ports. Press **Start** to run the diagnostics. This will take approximately 5 seconds. If all ports are selected, this can take approximately 15 seconds. When completed, the page refreshes automatically, and you can view the cable diagnostics results in the cable status table. Note that this is only accurate for cables of length 7 -140 meters. The 10 and 100 Mbps ports will be linked down while running the Cable Diagnostics. Running on a 10 or 100 Mbps management port will cause the switch to stop responding until it is complete.

The cable length reported could have a plus or minus 3 meter inaccuracy if the diagnostic port to be checked is link down, and it could have a plus or minus 15 meter inaccuracy if the diagnostic port to be checked is link up. Note that the port link up on 10M speed is not supported.

To run a Cable Diagnostic in the web UI:

1. Click Diagnostics and Cable Diagnostics.
2. Se the Port that you want to check.
3. Click Start.

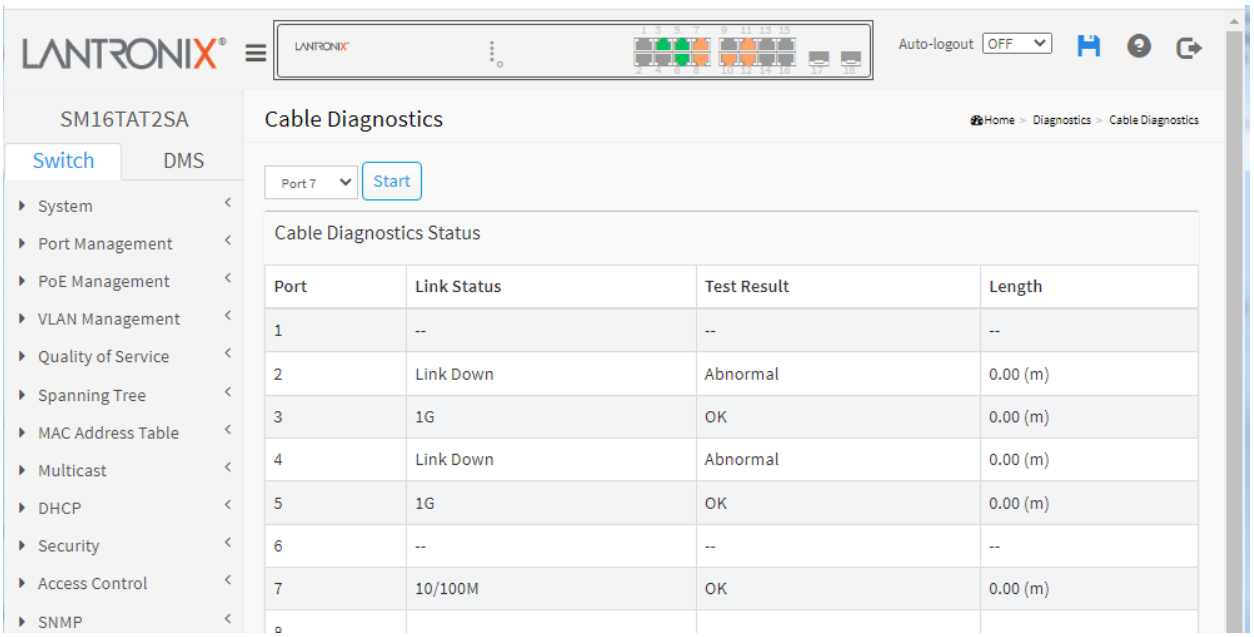


Figure 14-3: Cable Diagnostics page

Port : At the dropdown, select he port number on which you want to run Cable Diagnostics.

Cable Diagnostics Status

Port: The Port number you are requesting Cable Diagnostics.

Link Status: Provides the current link speed of the port (e.g., *1G* or *Link Down*).

Test Result: The status of the cable pair being diagnosed (e.g., *OK* or *Abnormal*)

Length: The length (in meters) of the cable pair.

Button

Start : Start cable diagnostics on the port that you selected. The message Processing... displays momentarily.

Message: *The cable length reported could have a plus or minus 3 meter inaccuracy if the diagnostic port to be checked is link down, and it could have a plus or minus 15 meter inaccuracy if the diagnostic port to be checked is link up.*
Meaning: informational message only, detailing the accuracy of the diagnostic in certain conditions.
Recovery: None; click the **OK** button and continue operation.

14-4 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 is used to monitor the traffic of the network. For example, assume that Port A and Port B are Monitoring Port and Monitored Port respectively; the traffic received by Port B will be copied to Port A for monitoring.

To configure Mirror parameters in the web UI:

1. Click Diagnostics and Mirroring.
2. At the Mode selection select on.
3. At the dropdown select the Monitor Destination Port.
4. Select Disabled, Enabled, TX Only, or RX only as the port mirror Mode for each port.
5. Click the **Apply** button to save the settings.
6. To cancel the setting click the **Reset** button to revert to previously saved values.

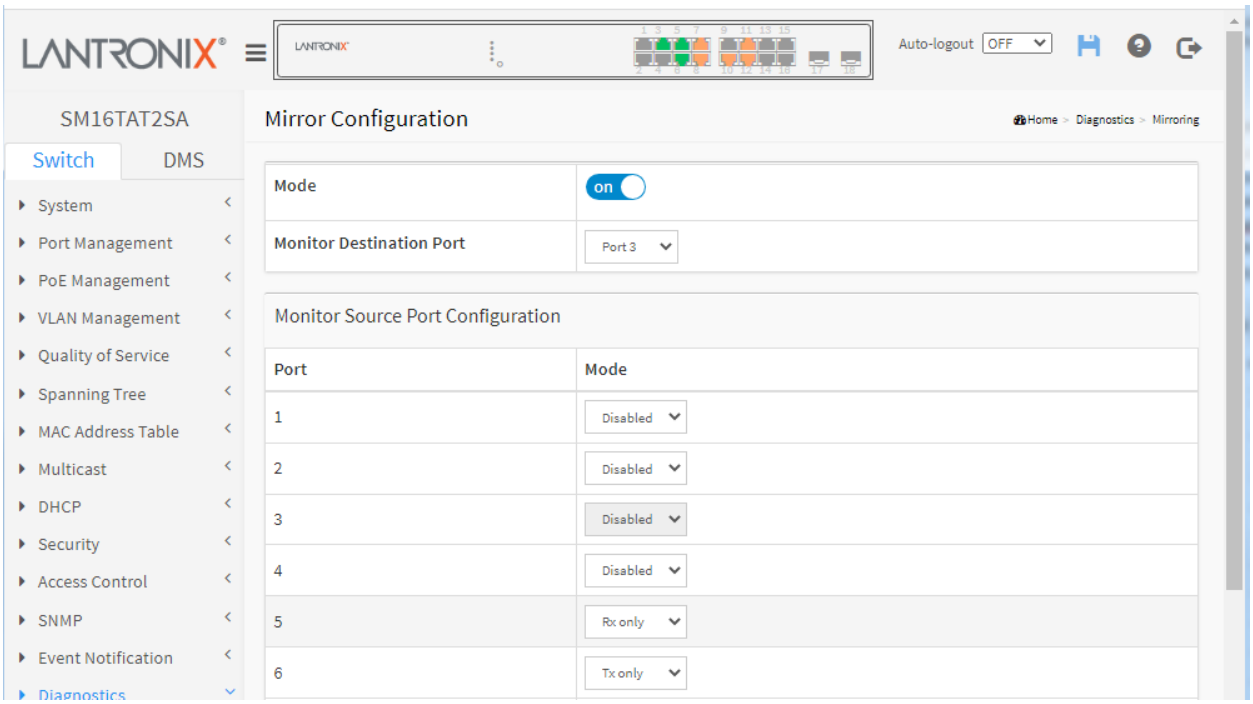


Figure 14-4: Mirror Configuration page

Mirror Configuration:

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

***on*:** Enable Mirror mode operation.

***off*:** Disable Mirror mode operation.

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.

Monitor Source Port Configuration:

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

Mode: Select mirror mode:

Rx only: Frames received on this port are mirrored on the mirror port. Frames transmitted are not mirrored.

Tx only: Frames transmitted on this port are mirrored on the mirror port. Frames received are not mirrored.

Disabled: neither frames transmitted nor frames received are mirrored.

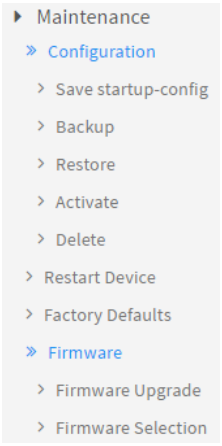
Enabled: Frames received and frames transmitted are mirrored on the mirror port.

Buttons

Apply: Click to save changes.

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

Chapter 15 Maintenance



This chapter describes the switch Maintenance configuration tasks to enhance the performance of local network including Save, Backup, Restore, Activate, Delete, Restart Device, Factory Defaults, and Firmware upgrade and Firmware Selection.

15-1 Configuration

The switch stores its configuration in a number of text files in CLI format.

The files are either virtual (RAM-based) or stored in flash on the switch.

There are three system files:

- **running-config**: A virtual file that represents the currently active configuration on the switch. This file is volatile. The config settings must be different than the default settings.
- **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.
- **mach10_combined.crt** : MACH10 is Lantronix Global Device Manager product.. A certificate file is a public-key certificate that follows the x.509 standard. The .CRT file extension is used for SSL/TLS certificates. The certificates may be encoded as binary DER or as ASCII PEM. A file with a .crt extension is a security certificate file used by secure websites for establishing secure connections from web server to a browser. Both crt and key files represent parts of a certificate; the key is the private key to the certificate and the crt is the signed certificate.

It is also possible to store up to two other files and apply them to running-config, thereby switching configuration.

15-1.1 Save running-config

This will copy the running-config to startup-config, thereby ensuring that the currently active configuration will be used at the next reboot.

To save running configuration in the web UI:

1. Click Maintenance, Configuration, Save startup-config.
2. Click Save Configuration.

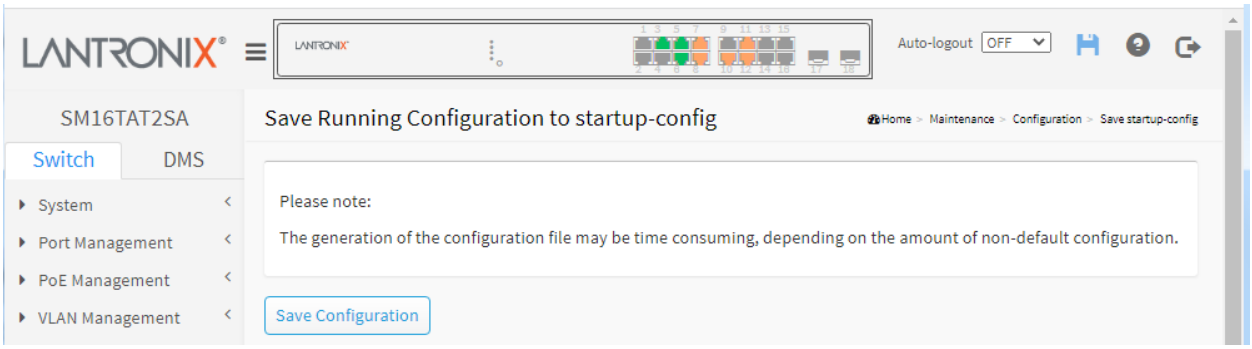
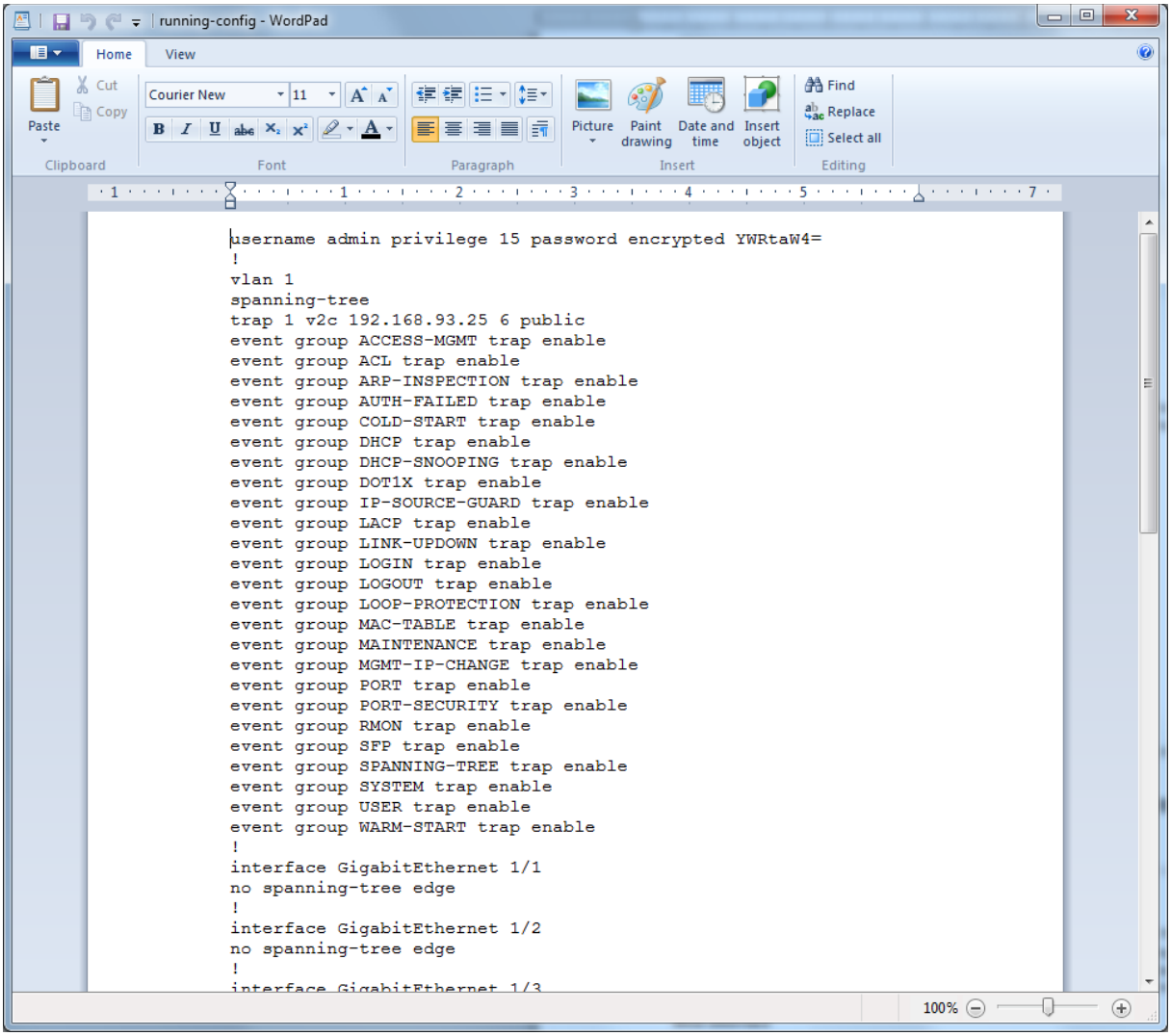


Figure 15-1.1: Save Running Config to startup-config

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 "*startup-config saved successfully.*" displays. **Note**: The generation of the configuration file may be time consuming, depending on the amount of non-default configuration.

Sample running-config file in WordPad:



15-1.2 Backup Configuration

This webpage lets you export the Switch Configuration for maintenance needs. Any current configuration files will be exported as text format.

If the file system is full (i.e., contains the three system files mentioned above plus two other files), it is not possible to create new files, but an existing file must be overwritten or another deleted first.

To back up a configuration file in the web UI:

1. Click Maintenance, Configuration, and Backup.
2. Select running-config, default-config, or startup-config for backup.
3. Click the Backup button. At the prompt select Open or Save or View Download.

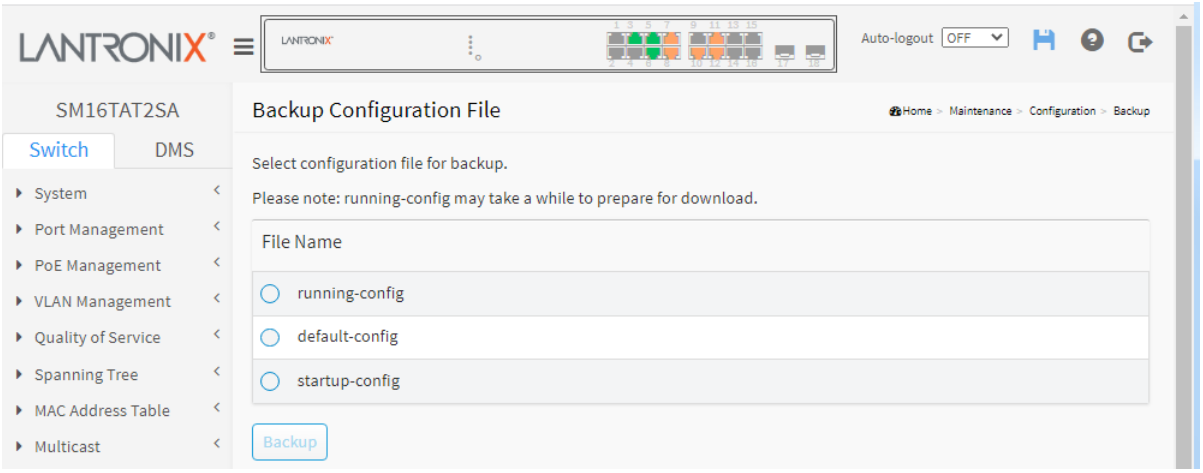


Figure 15-1.2: Backup Configuration

Parameter descriptions:

running-config: A virtual file that represents the currently active configuration on the switch. This file is volatile. The config settings must be different than the default settings.

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.

mach10_combined.crt : MACH10 is Lantronix Global Device Manager product.. A certificate file is a public-key certificate that follows the x.509 standard. The .CRT file extension is used for SSL/TLS certificates. The certificates may be encoded as binary DER or as ASCII PEM. A file with a .crt extension is a security certificate file used by secure websites for establishing secure connections from web server to a browser. Both crt and key files represent parts of a certificate; the key is the private key to the certificate and the crt is the signed certificate.

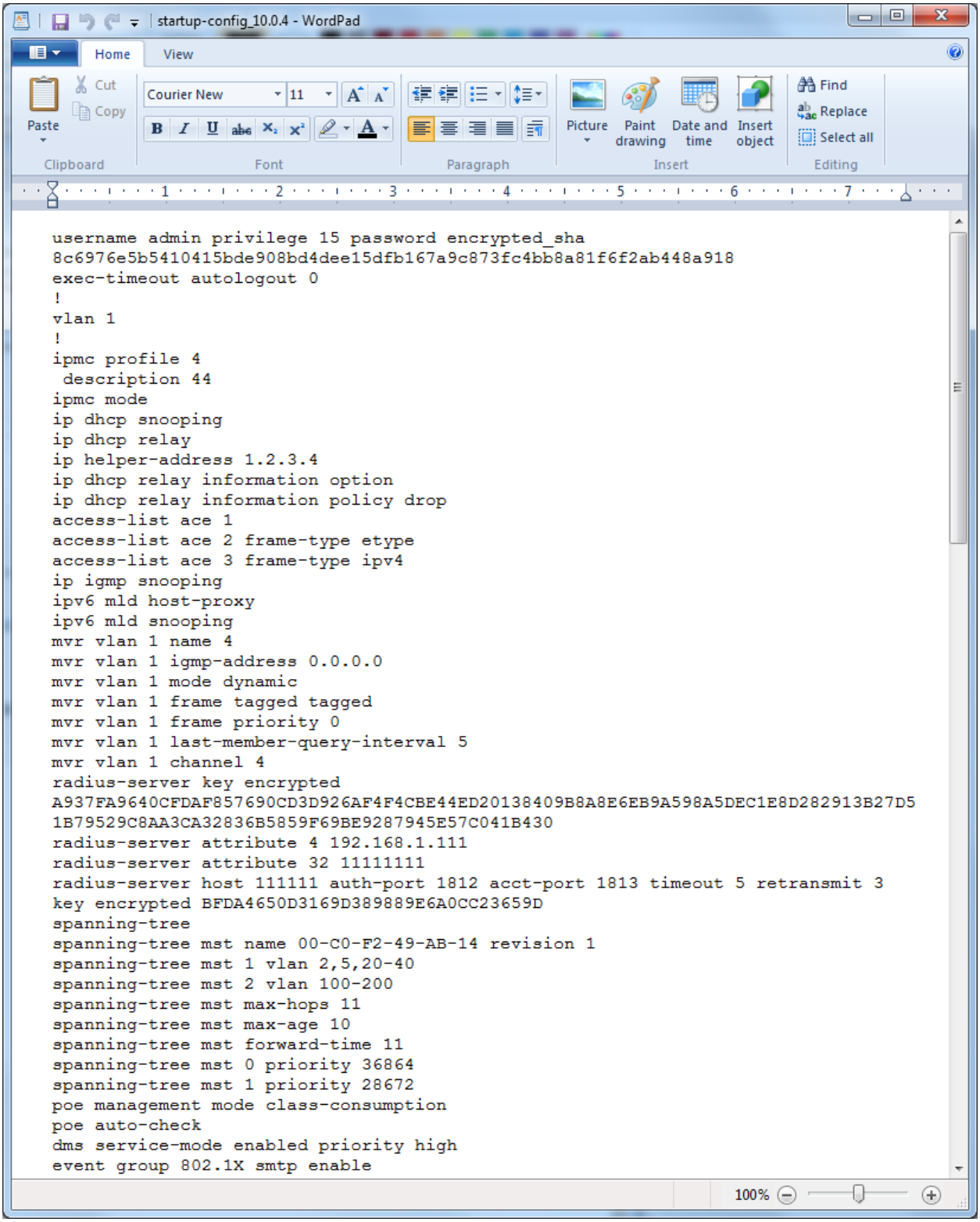
Buttons

Backup : Click the "Backup" button then the switch will start to download the configuration from flash memory to the PC or Server. **Note**: running-config may take a while to prepare for download.

Note: Starting at firmware v1.01.1201, the Backup config file name will automatically include the device's IP address and the date.

Example:

A sample startup-config page is shown below:



15-1.3 Restore Configuration

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, and select the destination file on the target.

To restore a configuration via the web UI:

1. Click Maintenance, Configuration, and Restore.
2. Browse to and select a Source File.
3. Click the Restore button.

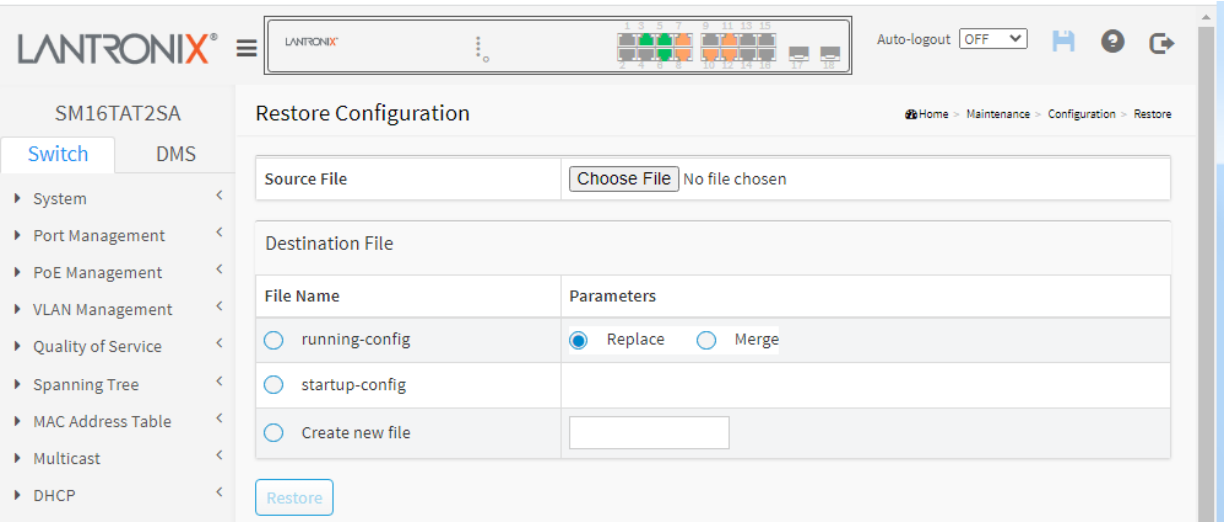


Figure 15-1.3: Restore Configuration

There are three destination file name selections:

running-config: A virtual file that represents the currently active configuration on the switch. This file is volatile. You can select "**Replace**" the existing file, or "**Merge**" the existing running-config file with the new file. If the destination is running-config, the file will be applied to the switch configuration.
This can be done in two ways:

Replace: The current configuration is fully replaced with the configuration specified in the source file.

Merge: The source file configuration is merged into running-config.

startup-config: The startup configuration for the switch, read at boot time.

mach10_combined.crt : MACH10 is Lantronix Global Device Manager product.. A certificate file is a public-key certificate that follows the x.509 standard. The .CRT file extension is used for SSL/TLS certificates. The certificates may be encoded as binary DER or as ASCII PEM. A file with a .crt extension is a security certificate file used by secure websites for establishing secure connections from web server to a browser. Both crt and key files represent parts of a certificate; the key is the private key to the certificate and the crt is the signed certificate.

Create new file: A read-only file with vendor-specific configuration. This file is read when the system is restored to default settings.

Buttons

Browse: Click the browse button to search for the configuration text file and filename.

Restore: Click the "Restore" button then the running web management PC will start to upload the configuration from the location PC configuration into the managed switch.

Message: *The config file is uploaded successfully.*

15-1.4 Activate Configuration

It is possible to activate any of the configuration files present on the switch, except for running-config which represents the currently active configuration.

To activate a configuration file in the web UI:

1. Click Maintenance, Configuration, and Activate Configuration.
2. Select the File Name to be activated.
3. Click the Activate Configuration File button. This will initiate the process of completely replacing the existing configuration with that of the selected file.

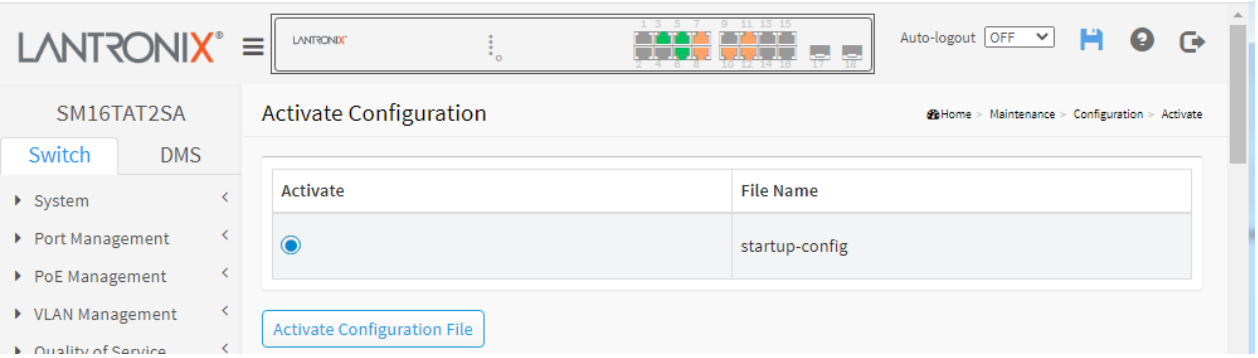


Figure 15-1.4: Activate Configuration

Parameter descriptions:

Activate: Select the radio button to activate the selected file**.**

startup-config: The startup configuration for the switch, read at boot time.

mach10_combined.crt : MACH10 is Lantronix Global Device Manager product.. A certificate file is a public-key certificate that follows the x.509 standard. The .CRT file extension is used for SSL/TLS certificates. The certificates may be encoded as binary DER or as ASCII PEM. A file with a .crt extension is a security certificate file used by secure websites for establishing secure connections from web server to a browser. Both crt and key files represent parts of a certificate; the key is the private key to the certificate and the crt is the signed certificate.

Buttons

Activate Configuration File: Click the button then the selected file will be activated and will become this switch's running configuration.

15-1.5 Delete config

It is possible to delete any of the writable files stored in flash, including startup-config. If this is done and the switch is rebooted without a prior save operation, this effectively resets the switch to its default configuration.

To delete a configuration file in the web UI:

1. Click Maintenance, Configuration, Delete config.
2. Click Delete Select.

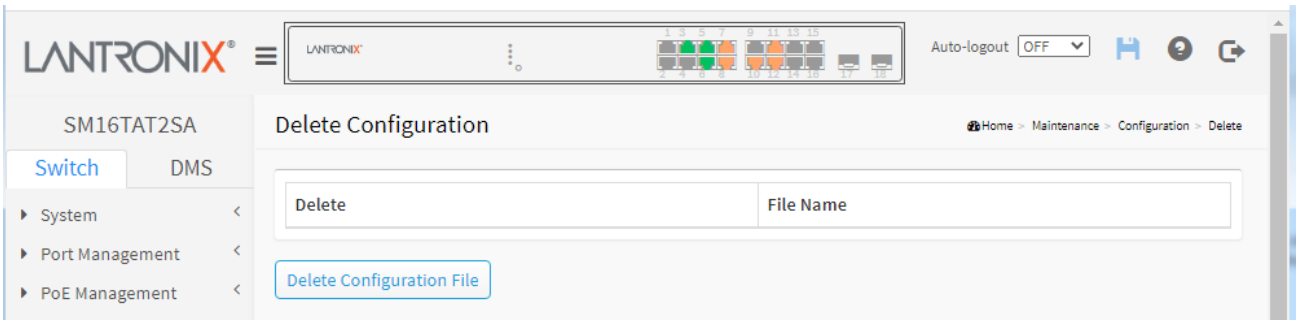


Figure 15-1.5: Delete Configuration

Parameter descriptions:

Delete: Select the file that you want to be deleted**.**

startup-config: The startup configuration for the switch, read at boot time.

mach10_combined.crt : MACH10 is Lantronix Global Device Manager product.. A certificate file is a public-key certificate that follows the x.509 standard. The .CRT file extension is used for SSL/TLS certificates. The certificates may be encoded as binary DER or as ASCII PEM. A file with a .crt extension is a security certificate file used by secure websites for establishing secure connections from web server to a browser. Both crt and key files represent parts of a certificate; the key is the private key to the certificate and the crt is the signed certificate.

Buttons

Delete Configuration File: Click the button then the selected file will be deleted.

15-2 Restart Device

This webpage lets you restart switch for any maintenance needs. Any configuration files or scripts that you saved in the switch should still be available afterwards.

To restart the device in the web UI:

1. Click Maintenance and Restart Device.
2. Check or uncheck the Always-On PoE option checkbox.
3. Click Yes.

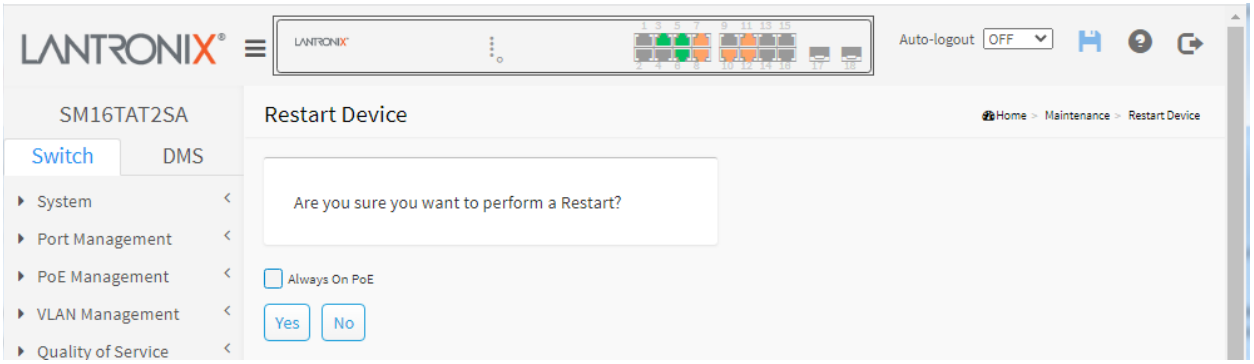


Figure 15-2: Restart Device

Parameter descriptions:

Restart Device: You can restart the switch on this page. After restart, the switch will boot normally.

Buttons

Always-On PoE: Check for the switch to maintain power to PDs during device restart. Note that the name "Non-stop PoE" changed to "Always--On PoE" at FW v1.03.1501. Always-on PoE ensures that there is uninterrupted PoE power to the PDs even when a switch is upgraded or restarted. This is critical when 24/7 surveillance cannot have any interruptions.

Yes: Click to restart the device.

No: Click to undo any restart action and return to the System Configuration page without restarting the configuration.

15-3 Restore Factory Defaults

This webpage lets you reset the Switch configuration to Factory Defaults. Any configuration files or scripts are restored to factory default values.

To reset the switch configuration to its Factory default settings in the web UI:

1. Click Maintenance and Factory Defaults.
2. Check the box if you want to keep the current IP configuration.
3. Click Yes.

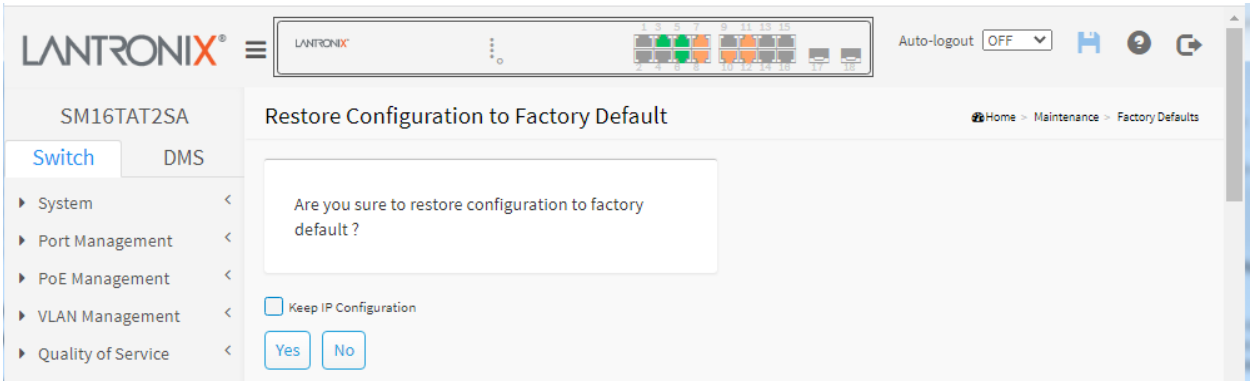


Figure 15-3: Restore Config to Factory Defaults

Buttons

Keep IP Configuration: Check if you want to keep the current IP address configuration after the restore is completed. At FW v1.02.1474 the Gateway IP address is also kept when restoring the switch to its factory defaults with the Keep IP Configuration checkbox checked.

Yes: Click the button to reset the configuration to Factory Defaults.

No: Click to undo any restore action and return to the System Configuration page without restoring the configuration.

15-4 Firmware

This webpage lets you upgrade and select Firmware. The Switch can be enhanced with value-added functions by installing firmware upgrades. **Note**: Password encoding changed in FW v1.02.1409.
You cannot login if downgrading the switch to older firmware versions or loading an old config file in new firmware. Do not restart or power off the device at this time or the switch may fail to function afterwards.

15-4.1 Firmware Upgrade

This page starts an update of the firmware controlling the switch. To upgrade switch firmware in the web UI:

1. Click Maintenance, Firmware, and Firmware Upgrade.
2. Click the Choose File button.
3. Browse to and select the file to upgrade the switch to (e.g., SM16TAT2SA_v1.04.0040_CM_202112001.tar or SM8TAT2SA_v1.04.0110_CM_202212006.tar.gz.imgs).
4. Check the Always On PoE checkbox if desired.
5. Click the Upload button. Continue operation when the message "*Firmware upgrade in progress Completed!*" displays.

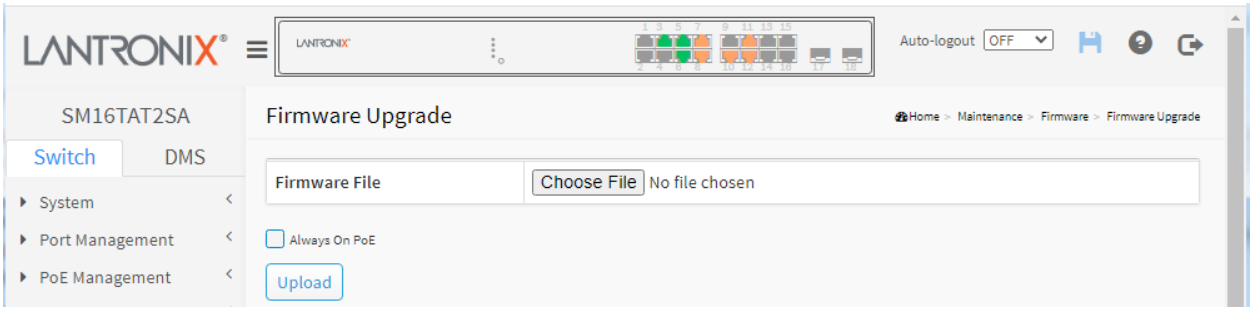


Figure 15-4.1 Software Upload page

Parameter descriptions:

Always-On PoE: Always On PoE (soft reboot) allows a warm reboot of the switch without affecting the PoE output to the PD, providing continuous power even during firmware upgrade. Note that the name "Non-stop PoE" changed to "Always-On PoE" at FW v1.03.1501. Always-on PoE ensures that there is uninterrupted PoE power to the PDs even when a switch is upgraded or restarted. This is critical when 24/7 surveillance cannot have any interruptions.

Buttons:

Choose File: Click the button to search for the Firmware filename.

Note: This page facilitates an update of the firmware controlling the switch. A Software Upload will update the managed switch to the software image at the specified location. After the software image is uploaded, a page announces that the firmware update is initiated. After about a minute, the firmware is updated and the switch restarts.

WARNING: While the firmware is being updated, Web access appears to be defunct. The front LED flashes Green/Off with a frequency of 10 Hz while the firmware update is in progress. Do not restart or power off the device at this time or the switch may fail to function afterwards.

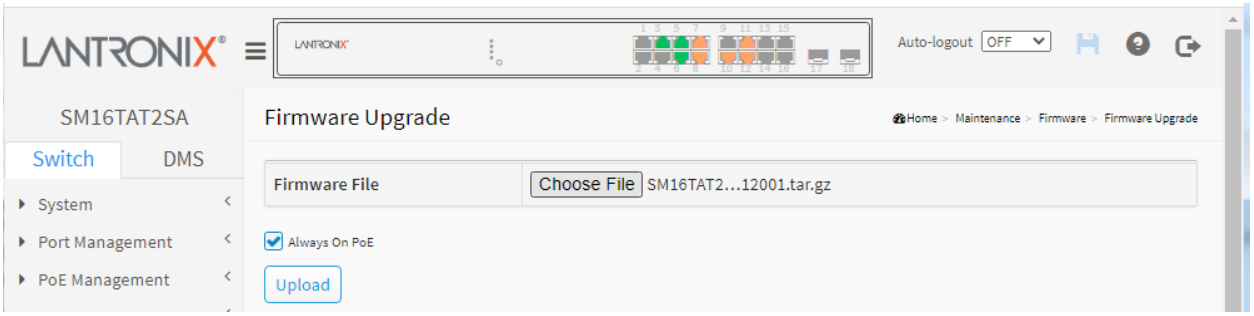


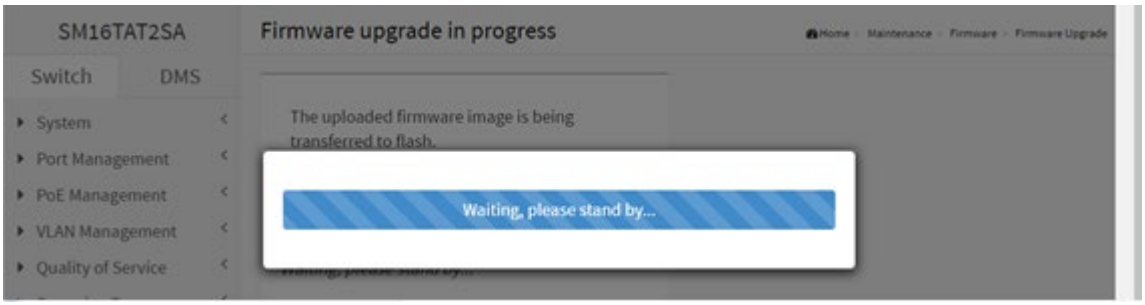
Figure 15-4.2 Firmware Upgrade page

Messages:

Message: *Error : The firmware is already update.*
Meaning: You are trying to upgrade to the current (existing) firmware version.
Recovery: Verify that you are upgrading to the latest version.

Message: *The firmware update was successful.*
Meaning: The software was successfully updated.
Recovery: None required.

Message: *Firmware upgrade in progress Waiting, please stand by...*



Meaning: While the firmware is being updated, do not restart or power off the switch or it may fail to function afterwards.
Recovery: None. Wait for the upgrade to complete.

Message: *Firmware upgrade in progress*
The uploaded firmware image is being transferred to flash.
The system will restart after the update.
Until then, do not reset or power off the device!
Waiting, please stand by…
Processing, please stand by…
Restarting, please wait …

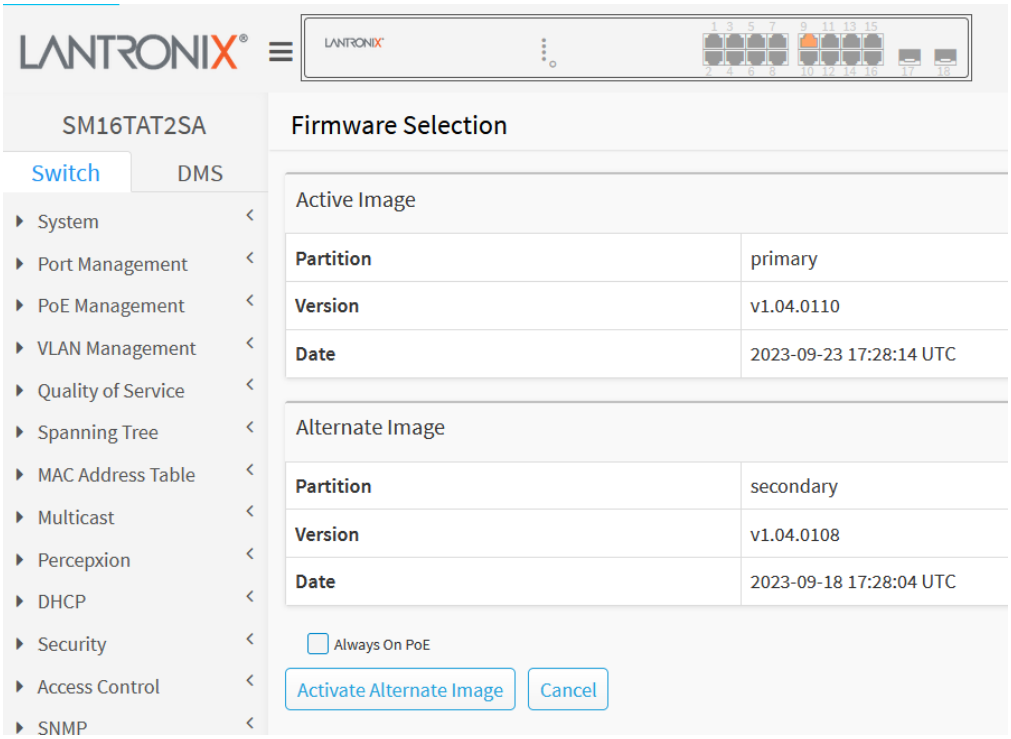
Message: *Error : The firmware image is invalid. Please use a correct firmware image.*
Meaning: You tried to upload an invalid firmware file.
Recovery: Check the file format and location. Make sure the firmware filename prefix matches your specific switch model (e.g., *sm16tat2sa*).

15-4.1 Firmware Selection

This page lets you activate an alternate firmware image. 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.

Note: Password encoding changed in FW v1.02.1409. You cannot login if downgrading the switch to older firmware versions or loading an old config file in new firmware.

1. Navigate to Maintenance > Firmware > Firmware Selection to display the Firmware Selection page.
2. Verify the Active Image and Alternate Image information.
3. Check or uncheck the Always On PoE checkbox.
4. Click the Activate Alternate Image button to swap the firmware versions.



Parameters:

Active Image

Partition: Indicates whether “primary” or “secondary” flash partition will provide the firmware upgrade image.

Version: The active firmware version (e.g., v1.04.0110).

Date: The active firmware build date (e.g., 2023-09-18 17:99:42 UTC).

Alternate Image

Partition: e.g., “secondary” firmware image.

Version: The alternate firmware version (e.g., v1.04.0106).

Date: The alternate firmware build date (e.g., 2023-09-06 12:32:55 UTC).

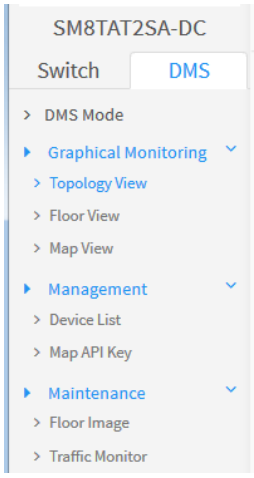
Buttons:

Always On PoE: Always On PoE (soft reboot) allows a warm reboot of the switch without affecting the PoE output to the PD, providing continuous power even during firmware upgrade. Note that the name "Non-stop PoE" changed to "Always-On PoE" at FW v1.03.1501.

Activate Alternate Image: Click the button to activate the Alternate Firmware image.

Cancel: Click to cancel the page edits.

Chapter 16 DMS (Device Management System)



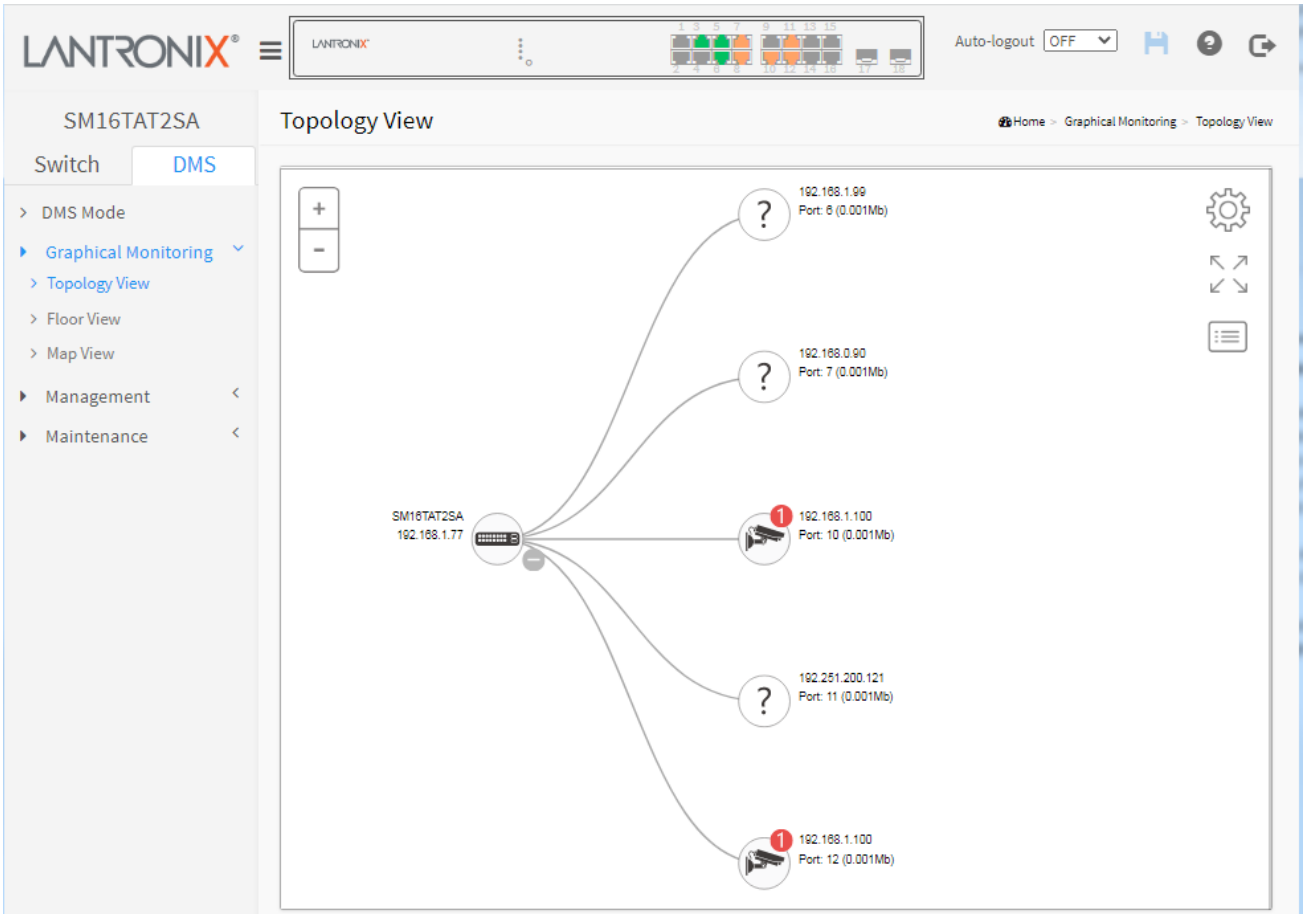
The Lantronix DMS (Device Management System) is an intelligent management tool embedded in the switch to intuitively help IT/TS in reducing support time, cost, and effort.

In the SMxTAT2SA main menu pane on the left, navigate to the DMS tab to display the main DMS features: DMS Mode, Graphical Monitoring, Management, 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.

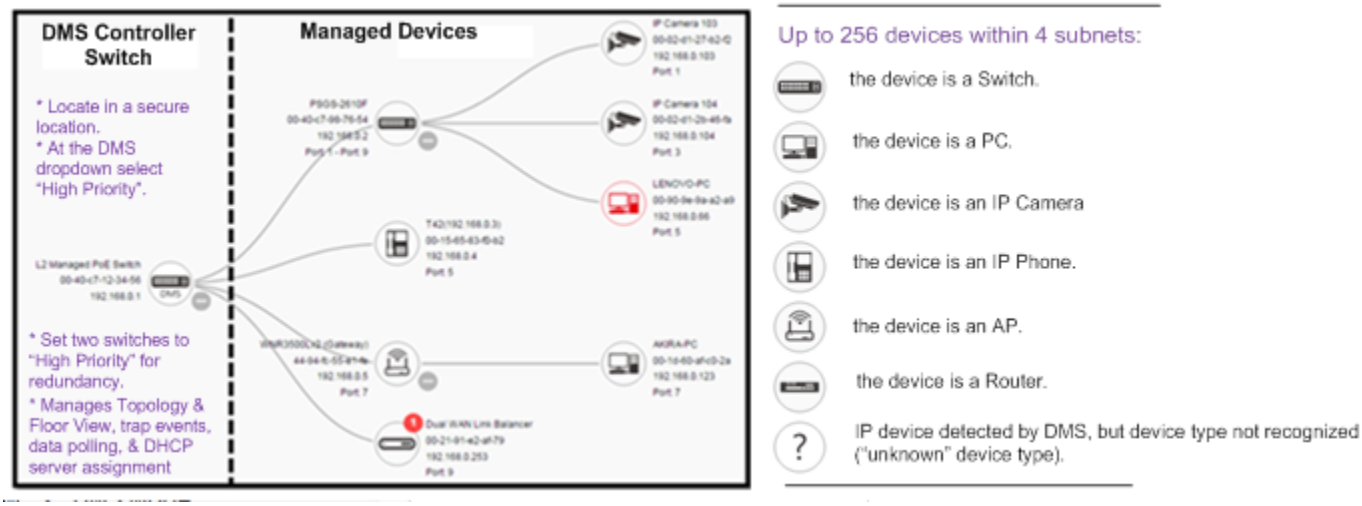
When you click the DMS tab, the default (startup) DMS webpage (DMS > Graphical Monitoring > Topology View) displays:



16-1 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.



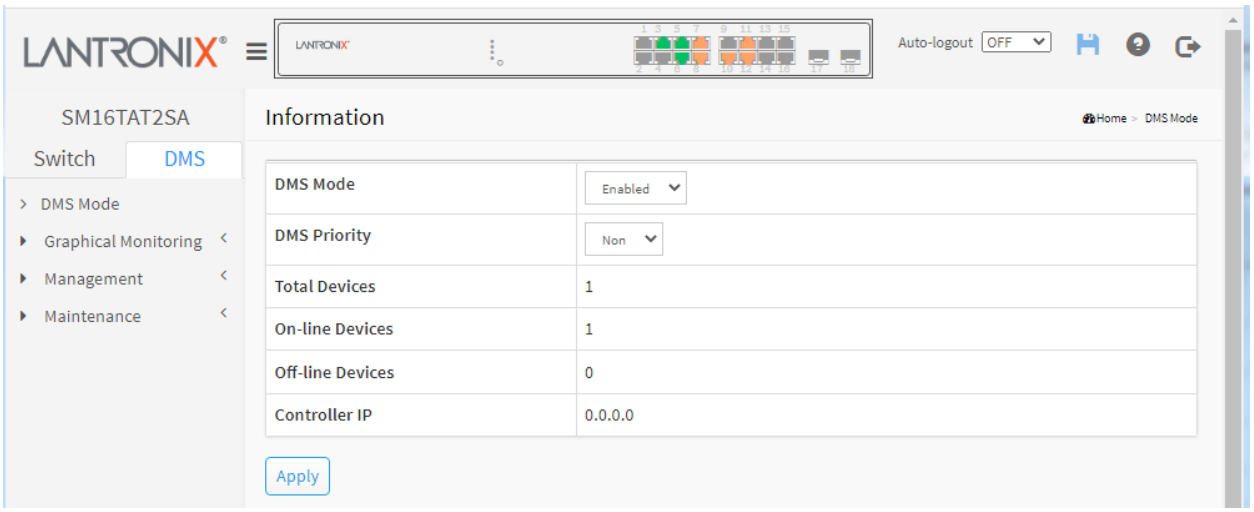
DMS Controller Switch and Managed Devices

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.

16-2 DMS Mode

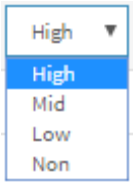
1. Click DMS > DMS Mode to display the DMS Information page.
2. At the DMS Mode dropdown select Enabled or Disabled.
3. At the DMS Priority dropdown select High, Mid, Low, or Non.
4. Click the Apply button. The DMS Information page updates.



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 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.

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.

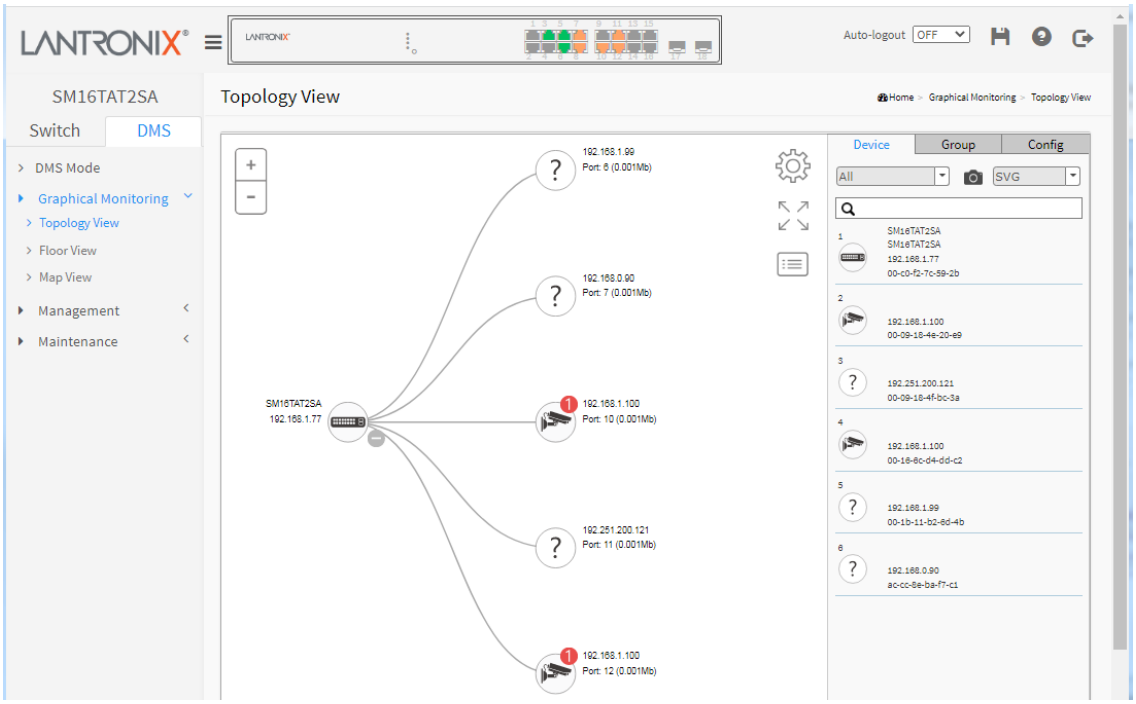
16-3 Graphical Monitoring

Navigate to the DMS > Graphical Monitoring menu path to view the options of DMS Graphical Monitoring Topology View, Floor View, and Map View.

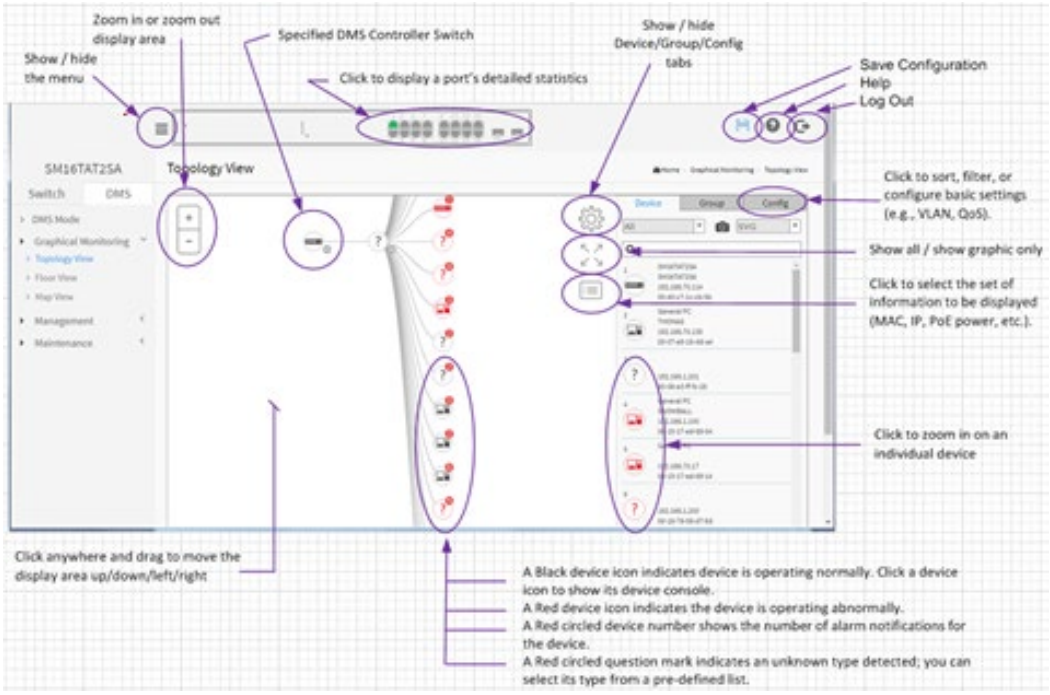
16-3.1 Topology View

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).

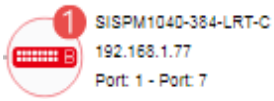
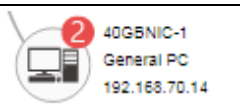


The Topology View icons and controls are shown and described below.



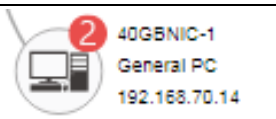
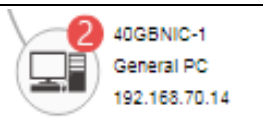
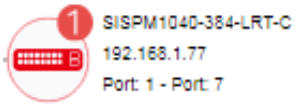
Topology View Icons / Controls

Click anywhere and drag to move the display area up /down/ left /right.

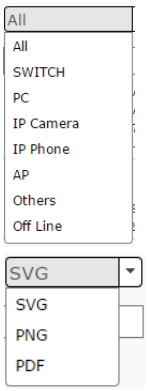
	Click “+” or “-” to zoom in or zoom out the display area.
	A Black device icon indicates device is operating normally. Click a device icon to show its device console.
	A Red device icon indicates the device is operating abnormally.
	A Red circled device number shows the number of alarm notifications 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 Cam.
	The device is an IP Phone.
	The device is a Wireless Access Point (WAP).
	The device is a Router.
	The device is an LED Light.

	Black icon: Device link up. You can select a function and check for issues.
	Red icon: Device link down. You can diagnose the link status.
	Icon with number: indicates some event has occurred (e.g. Device Off-line, IP Duplicate, etc.) on the IP device; you can click on the device icon to check events in Notification.
	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 device icon to show its device console.
	A Red device icon indicates the device is operating abnormally.

DMS Topology View parameters



Device tab parameters

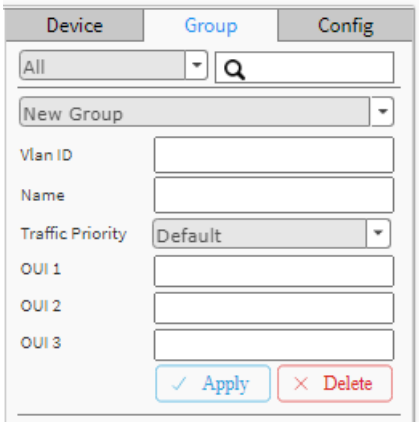
Devices dropdown: Select the device type (All, SWITCH, PC, IP Camera, IP Phone, AP, Others, or Off Line).

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 IP/MAC 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.

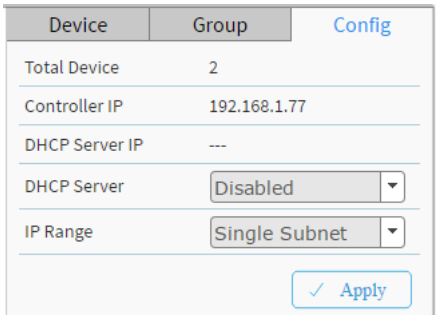
OUI 2: Enter a second Organizationally Unique Identifier.

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

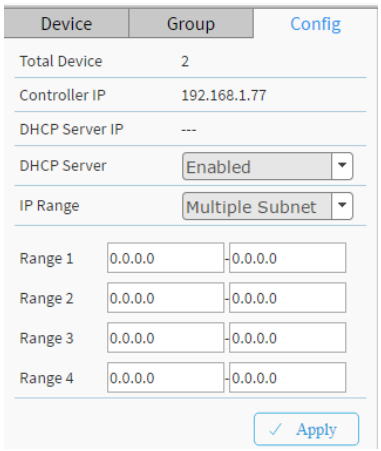


Total Device: Displays the total number of devices discovered.

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.

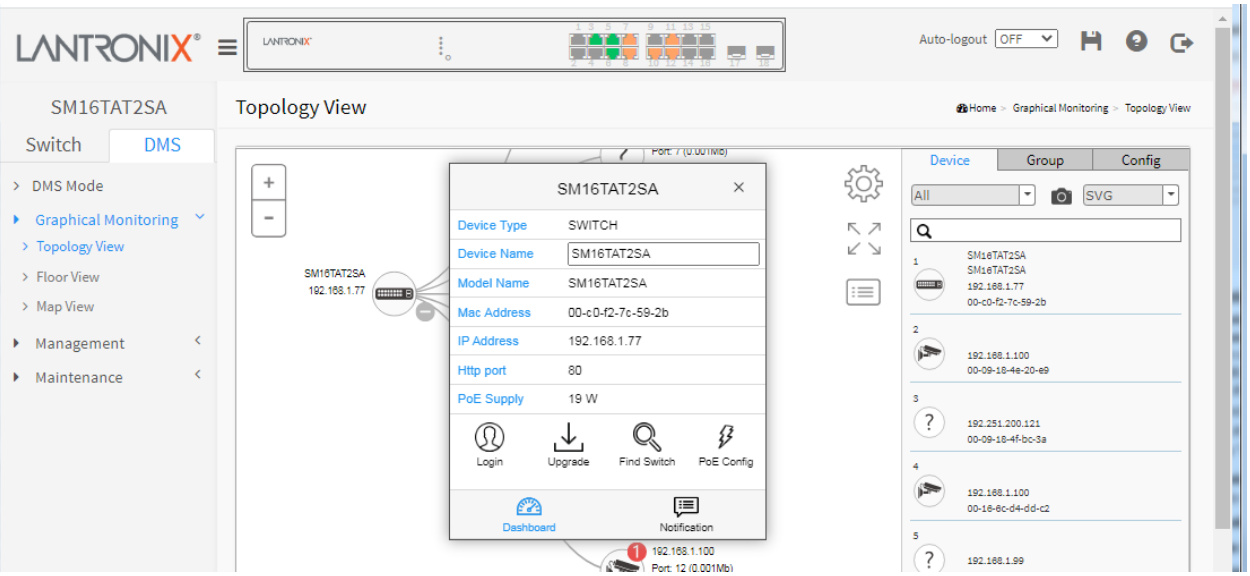


IP Range: The range type (Single Subnet or Multiple Subnet). If you select Multiple Subnet, selection fields display for Range 1 - Range 4.

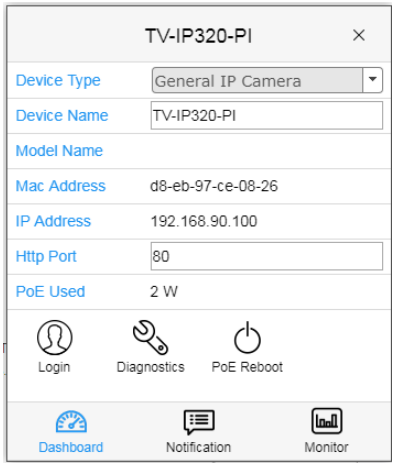
Apply: Click the button to make the changes.

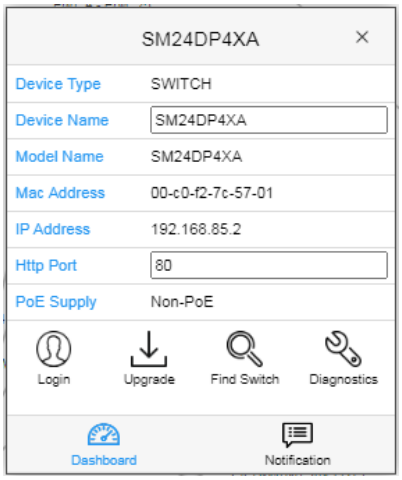
Device data

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., SM16TAT2SA. Create your own Device Name or alias for easy management such as "*1F_Lobby_Cam1*".

Model Name: e.g., SM16TAT2SA.

Mac Address: e.g., 00-40-c7-1c-cb-6e; displayed automatically by DMS.

IP Address: e.g., 192.168.1.77; displayed automatically by DMS.

Http port: e.g., 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.

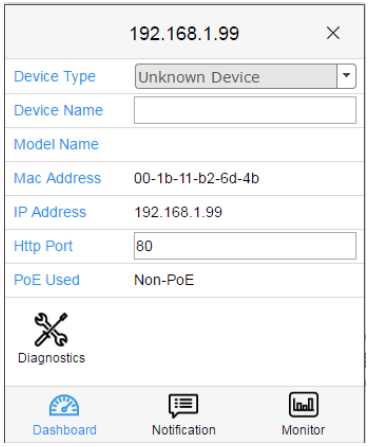
PoE Config icon: Click to display a window in which you can enable or disable PoE Auto Checking globally and enable or disable PoE Mode on a port-by-port basis.

PoE Reboot: Click to re-boot PoE.

PoE Supply and **PoE Used**: displayed automatically by DMS.

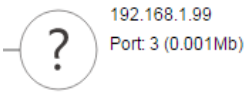
Dashboard icon: Click to display the dashboard.

Notification icon: Click to display an editable message area.



Unknown Device parameters

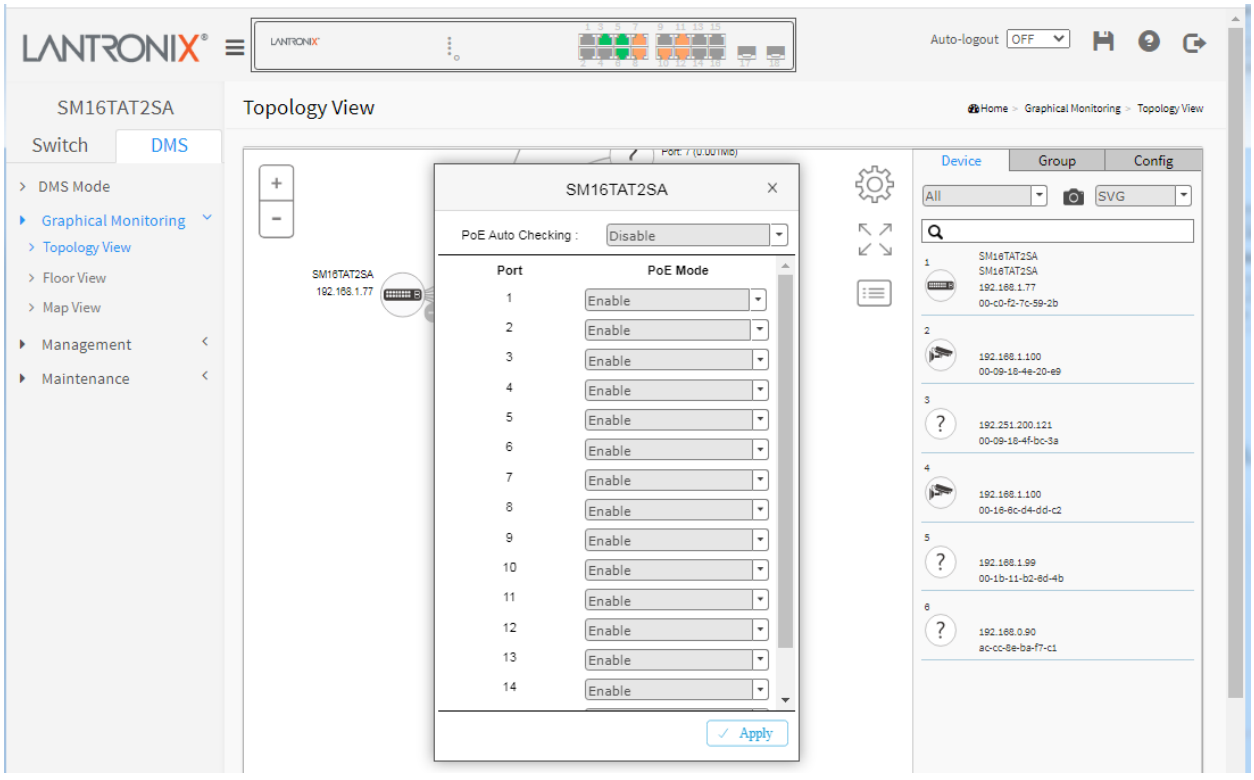
You can click on an unknown device to display its discovered data (see descriptions above). If an unknown type is detected, you can still select its type from a pre-defined list.



PoE Auto Checking "AutoFill" Feature

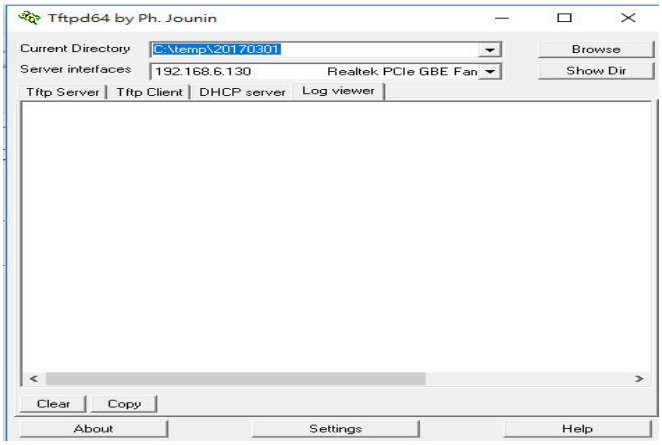
When you enable Auto Power Reset (PoE Auto Checking) in DMS, the IP addresses of the connected devices are automatically filled in the Auto Power Reset configuration page.

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 (PoE Config) icon to display the PoE Auto Checking pane:

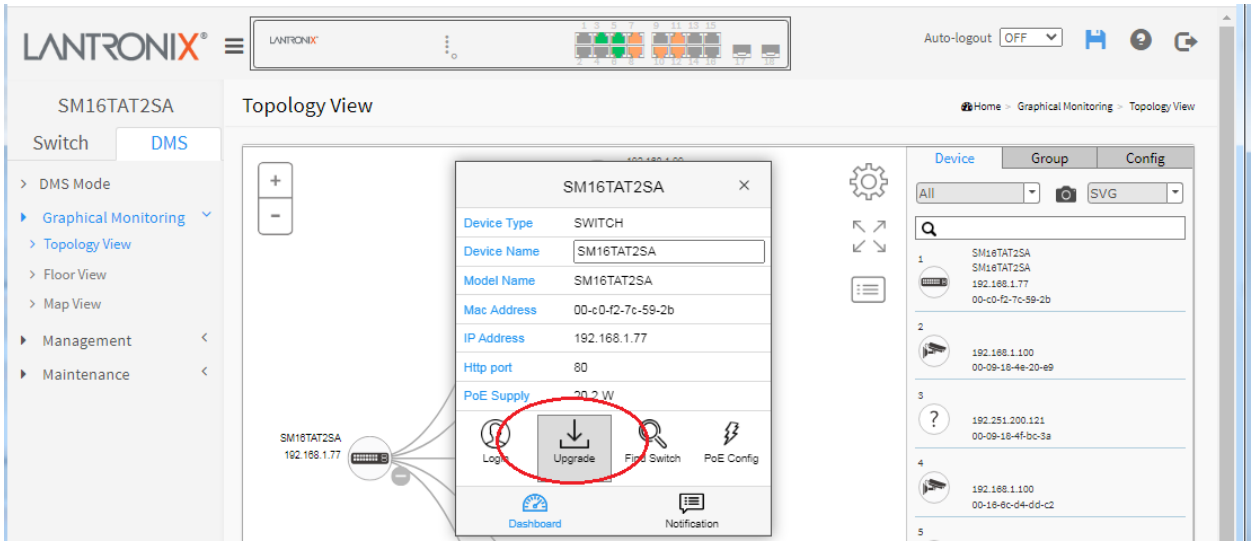


16-3.3 DMS Firmware Upgrade Procedure

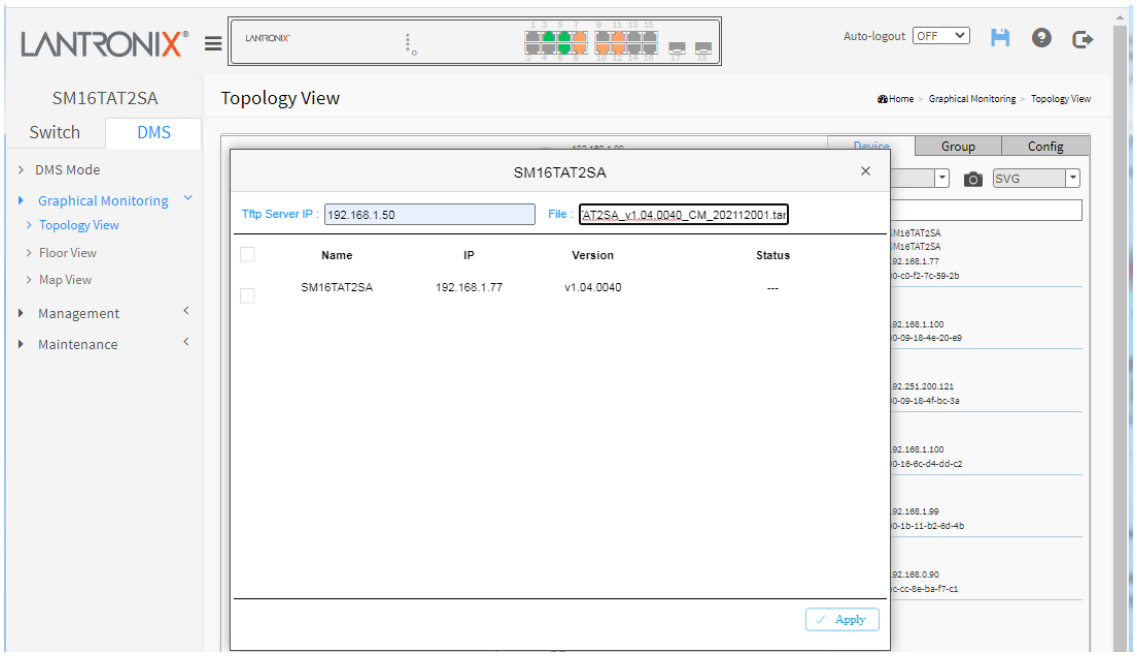
1. Navigate to the DMS > Graphical Monitoring > Topology View or Floor View menu path.
2. Click the button to display the right pane menu tabs (Entry and Config).
3. Connect all switches and make sure DMS is working.
   - Set all switches with different IP addresses and in the same IP segment.
   - Make 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.

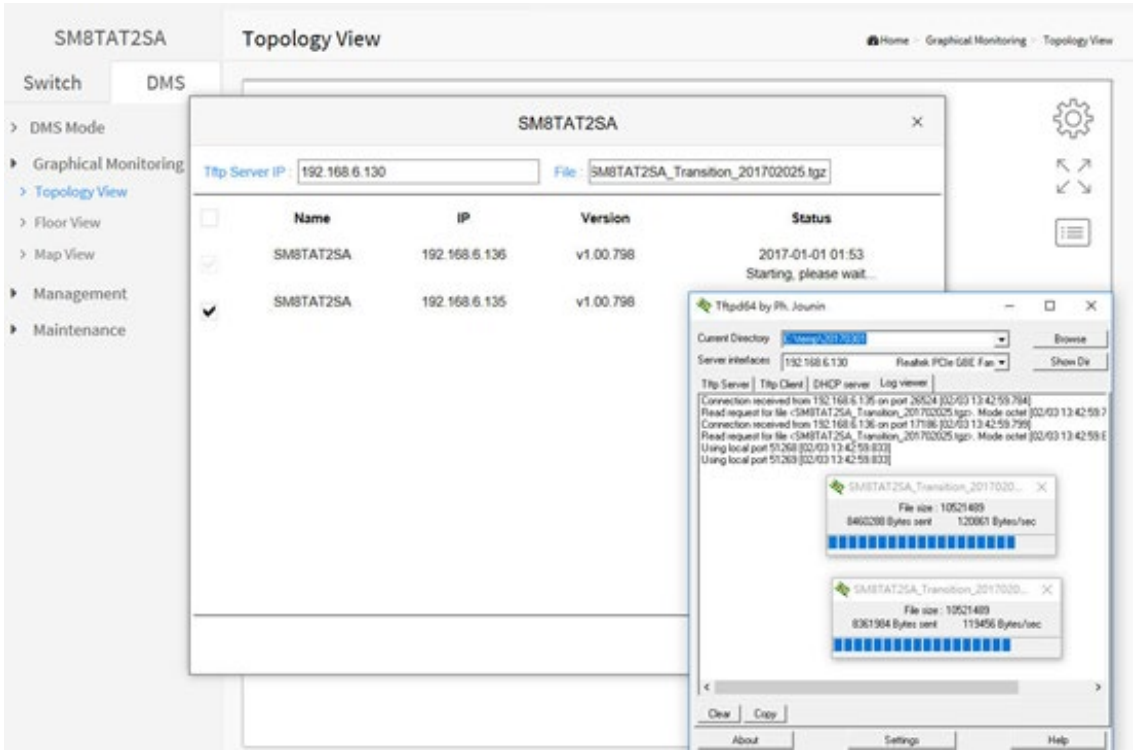


6. Enter the Tftp Server IP address and FW image name (e.g., SM16TAT2SA_v1.04.0040_CM_202112001.tar).



7. Click "Apply" to start the FW upgrade.

8. Observe the upgrade status until completion.



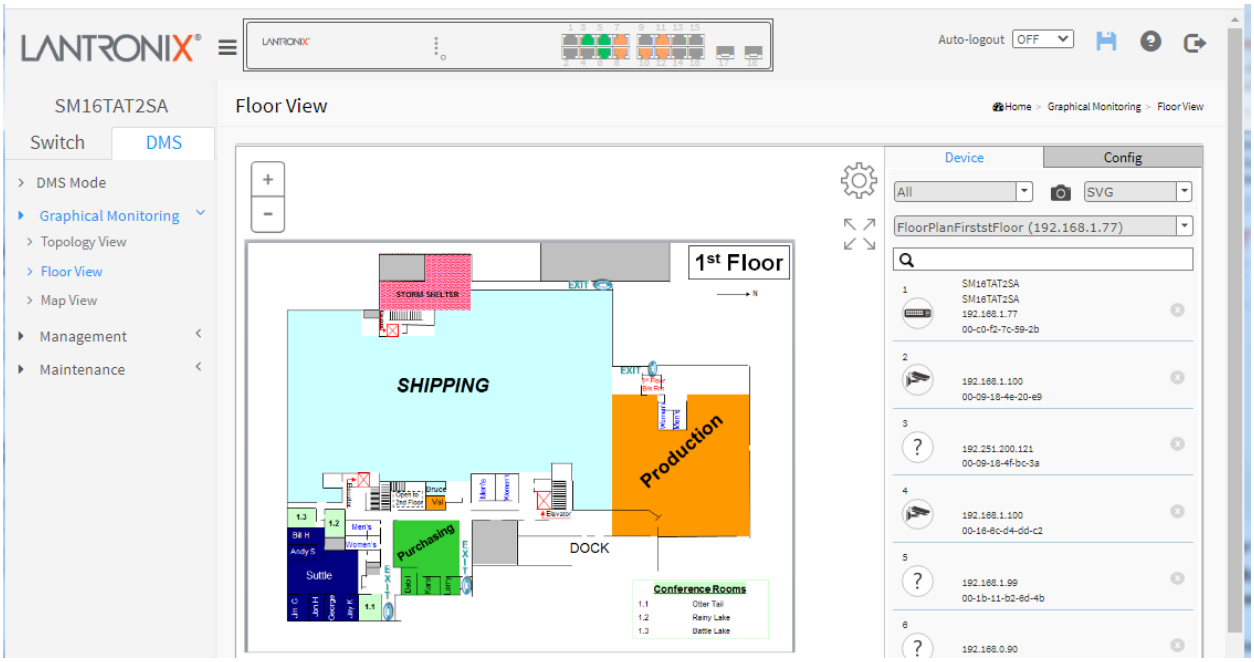
Message: *Error : Firmware download fail* displays if the TFTP Server IP address or the FW image name entered is incorrect.

16-3.4 Floor View

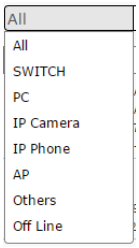
Navigate to the DMS > Graphical Monitoring > Floor View menu path. After you have added a Floor Image at DMS > Maintenance > Floor Image, the Floor View lets you:

- 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

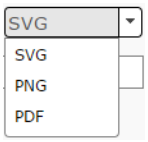


Device tab parameters

Devices dropdown: Select the device type (All, SWITCH, PC, IP Camera, IP Phone, AP, Others, or Off Line).

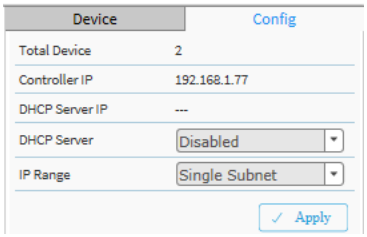
Snapshot icon: Use the icon to capture the displayed topology view.

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.

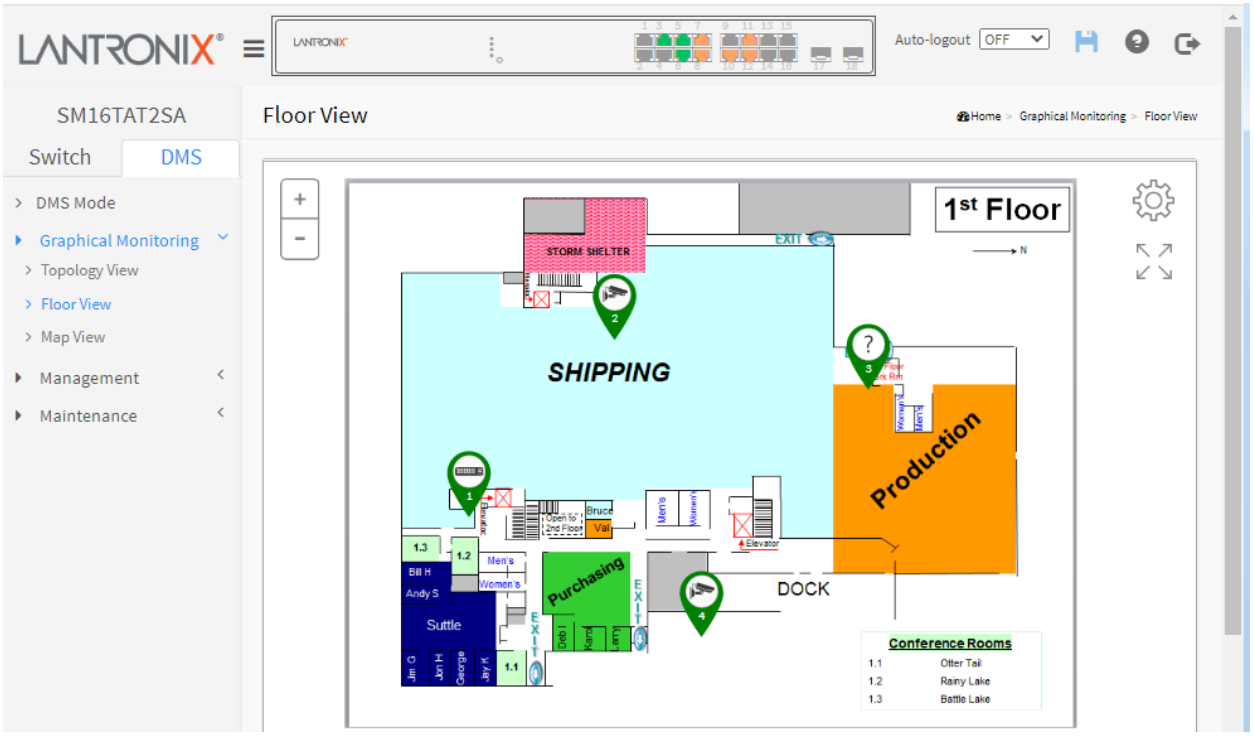
IP Range: The range type (Single Subnet or Multiple Subnet).

DHCP Server IP: Select Enabled or Disabled.

DHCP Server: Select Single Subnet or Multiple Subnet.

Apply: Click the button to save the selections.

Example: Drag and drop the devices to the desired locations:

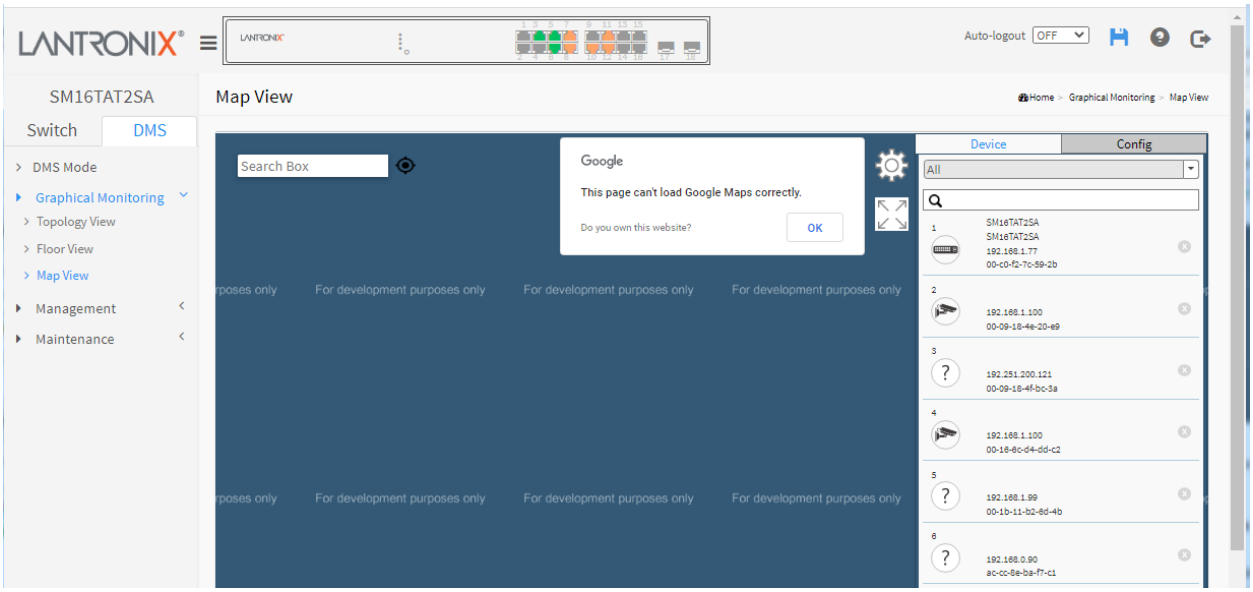


16-3.5 Map View

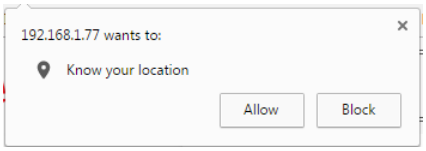
Navigate to the DMS > Graphical Monitoring > Floor View menu path. The Map View lets you:

- Anchor devices onto Google Maps
- Find devices instantly from Map
- 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.



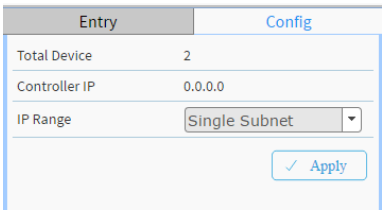
DMS Map View parameters

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:



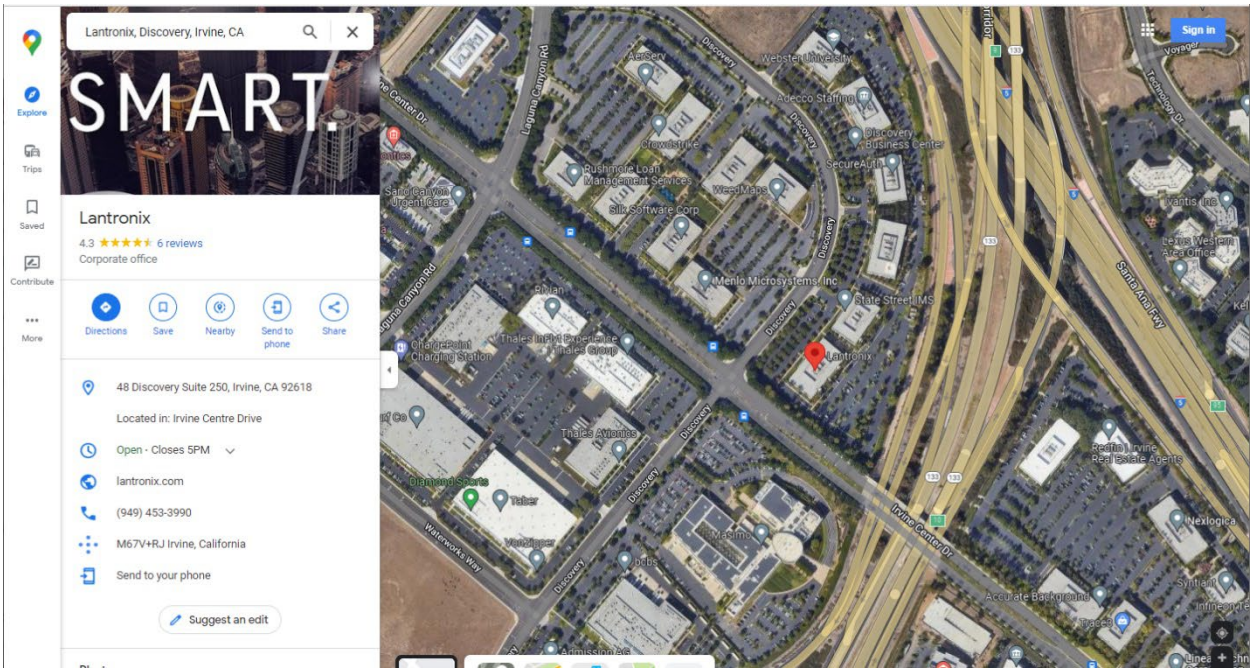
Total Device: Displays the total number of devices discovered.

Controller IP: The control device IP address in the format 0.0.0.0.

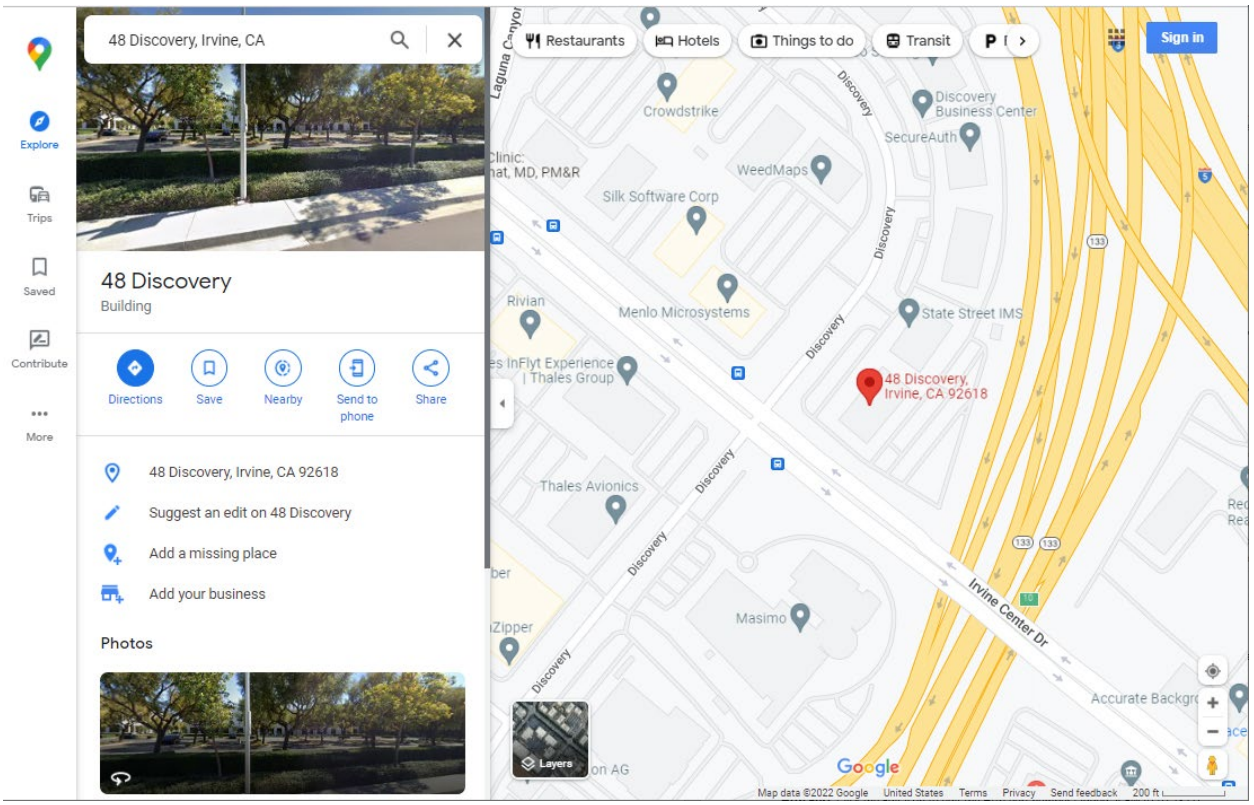
IP Range: The range type (Single Subnet or Multiple Subnet).

Apply: Click the button to save the selections.

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.

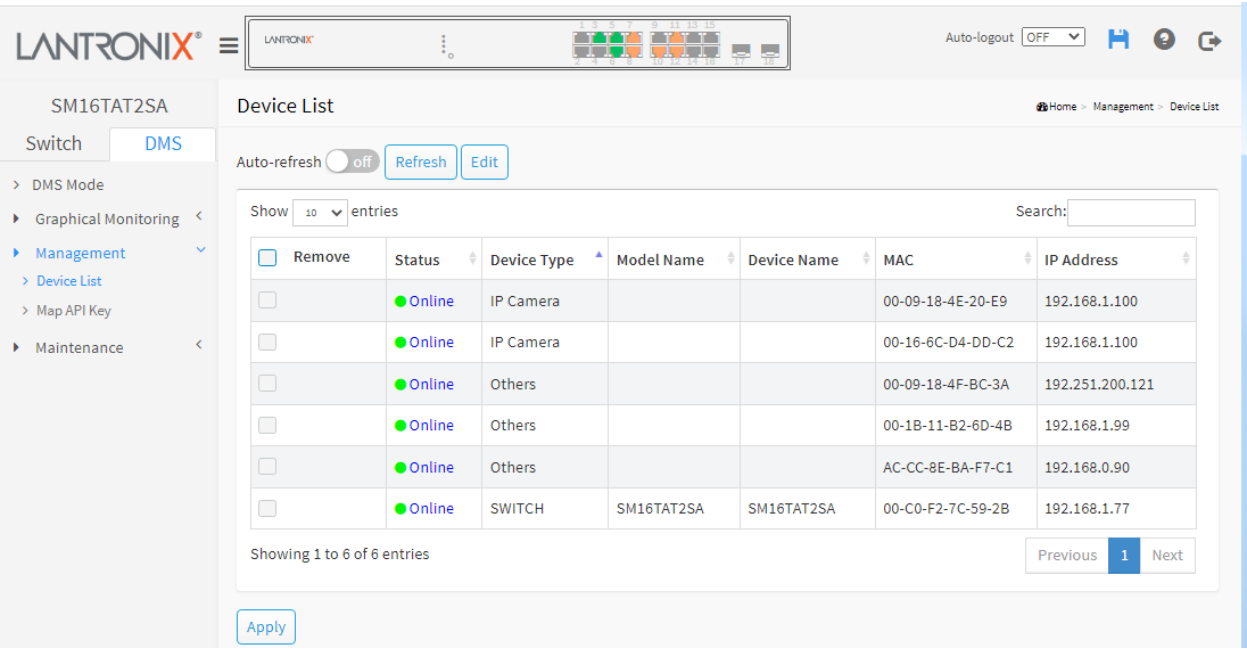
Message: *Do you own this website?*
Meaning: Click to go to the Google developers maps documentation page.

16-4 Management

Navigate to the DMS > Management menu path to view the Device List and Map API Key webpages.

16-4.1 Device List

Navigate to DMS > Management > Device List to show all devices and information detected by DMS.



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: e.g., SWITCH, IP Cameras, or Others.

Model Name: e.g., SM8TAT2SA or SM16TAT2SA or SM24TAT2SA.

Device Name: e.g., SM8TAT2SA or SM16TAT2SA or SM24TAT2SA.

MAC: e.g., 00-40-C7-1C-CB-6E.

IP Address: e.g., 192.168.1.77.

Http Port: Click the Edit icon to edit the Http Port number (added at FW v1.02.1327).

User Name: Click the Edit icon to edit the User Name (added at FW v1.02.1327).

Password: Click the Edit icon to edit the Password (added at FW v1.02.1327).

Buttons

Auto-refresh: Select **on** to automatically refresh the page every 3 seconds. The default is **off**.

Refresh: Click the button to refresh the page immediately.

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.

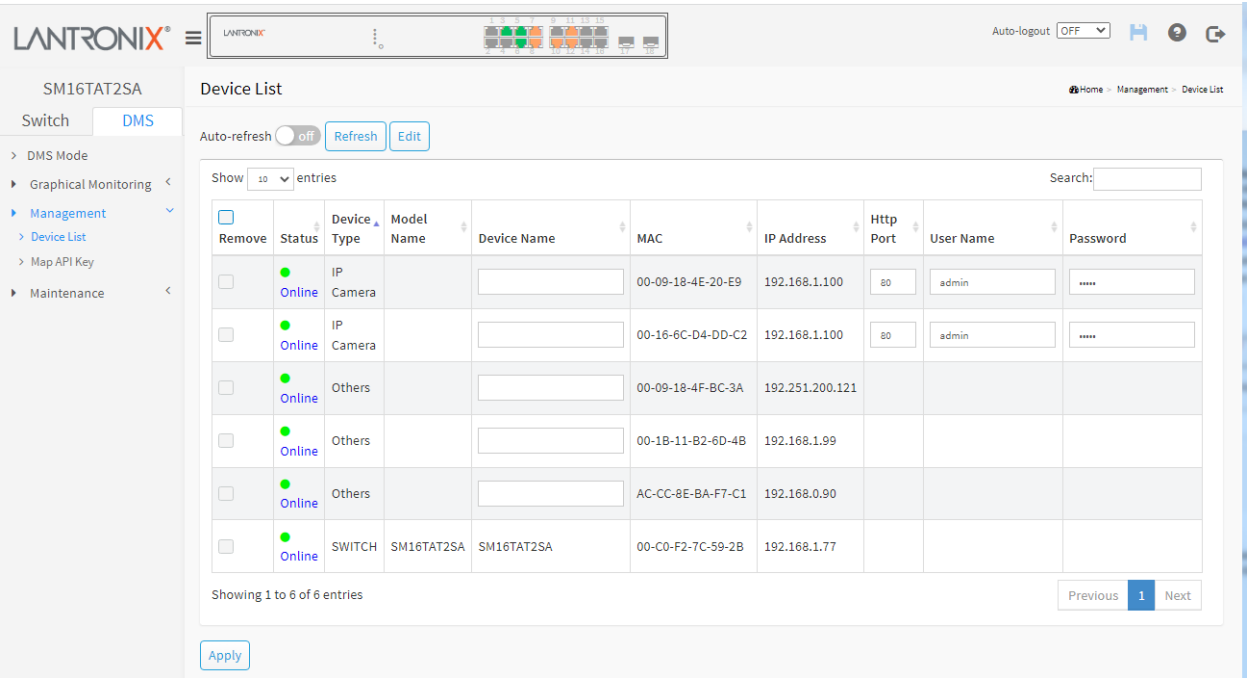
Remove: Only Offline devices provide "Remove" function to remove from DMS device list.

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:



Additional Parameter descriptions:

Device Name: Enter the desired name for this device.

Http Port: Edit the HTTP port number for this device.

User Name: Edit the Username for this device.

Password: Edit the Password for this device.

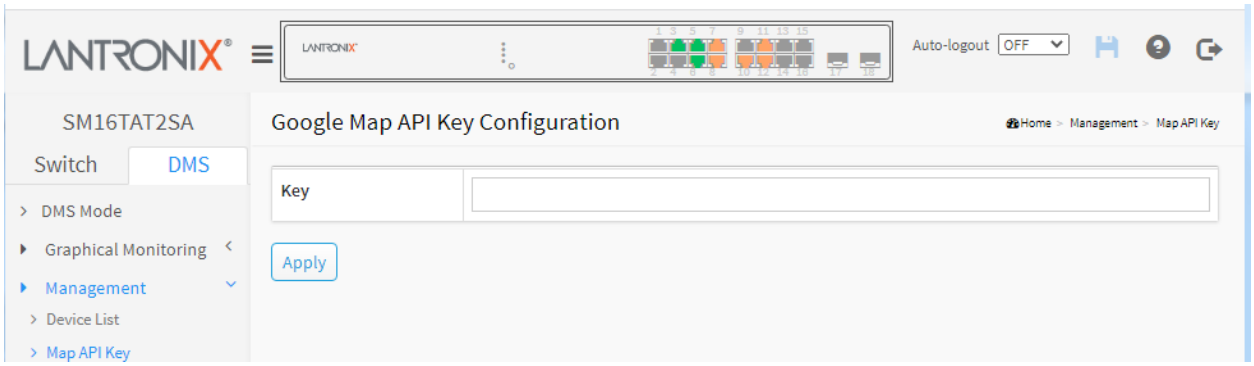
16-4.2 MAP API Key

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.

Visit the Google website below and follow the directions to get an API key:
https://developers.google.com/maps/documentation/directions/get-api-key

To configure the DMS Management API Key via the web UI:

1. Click DMS, Management, Map API Key.
2. Specify the Google Map API Key.
3. Click Apply to save the settings.



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.

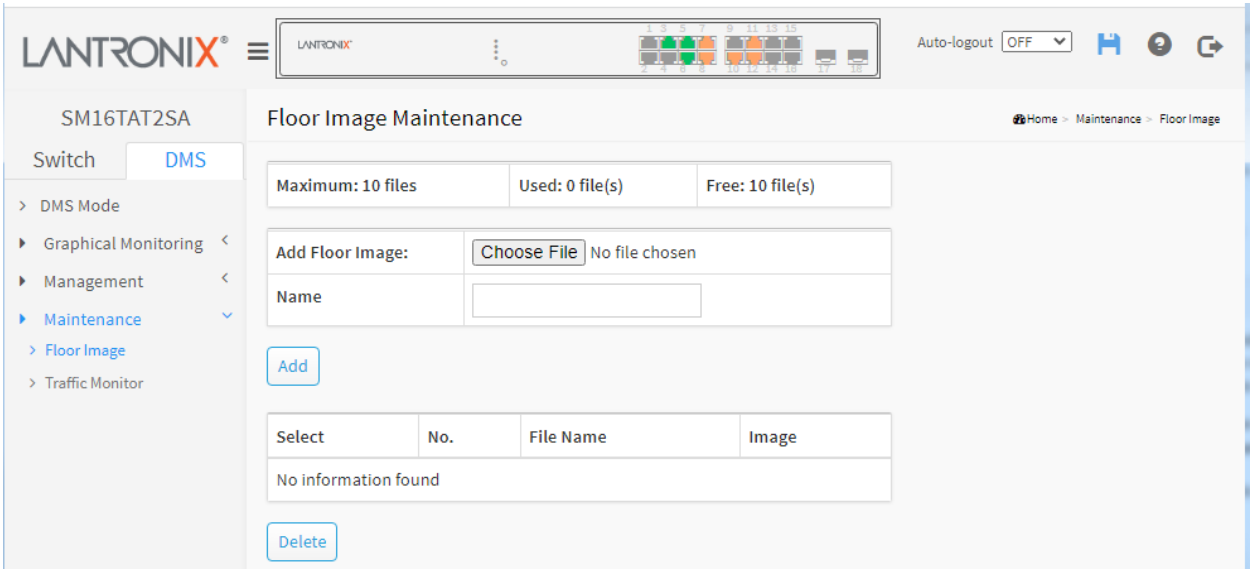
16-4 Maintenance > Floor Image

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 ae 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, Switch 2 uploaded 5 images, 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.

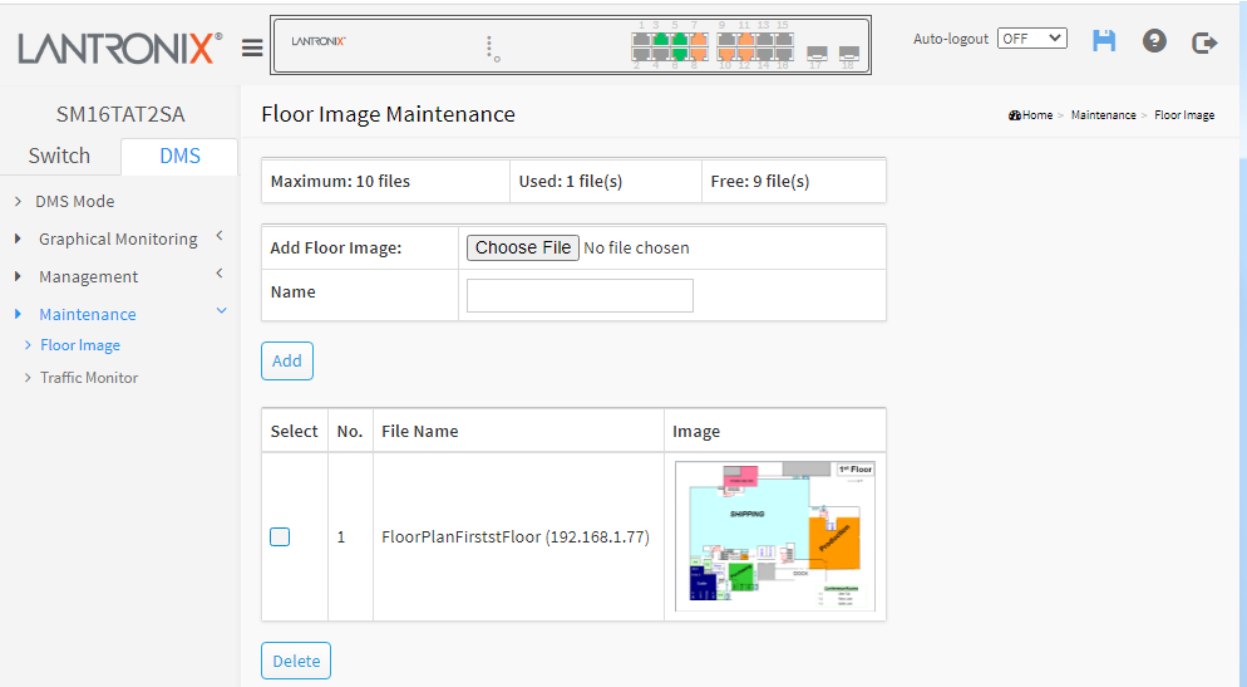
Add: Click to add the selected file.

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*):



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.

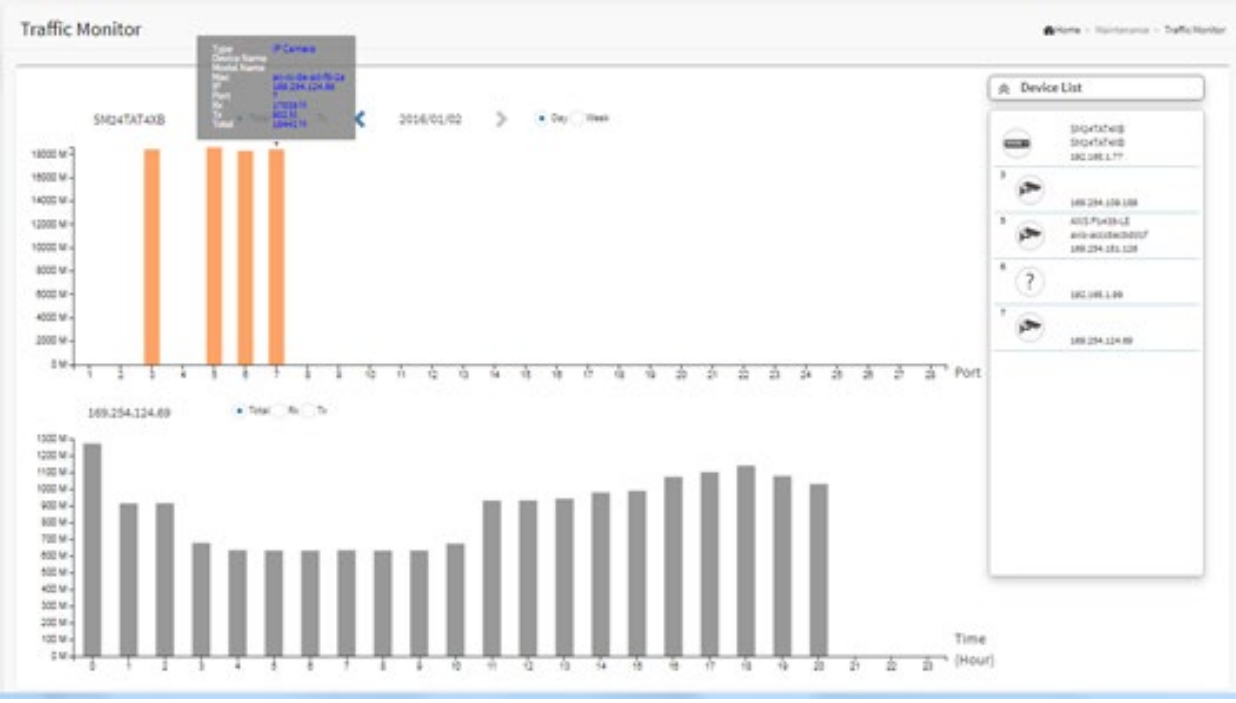
Recovery: Click the **OK** button to clear the message and choose a File Name with no special characters.

16-5 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: Select the set of data to be displayed.

< 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.

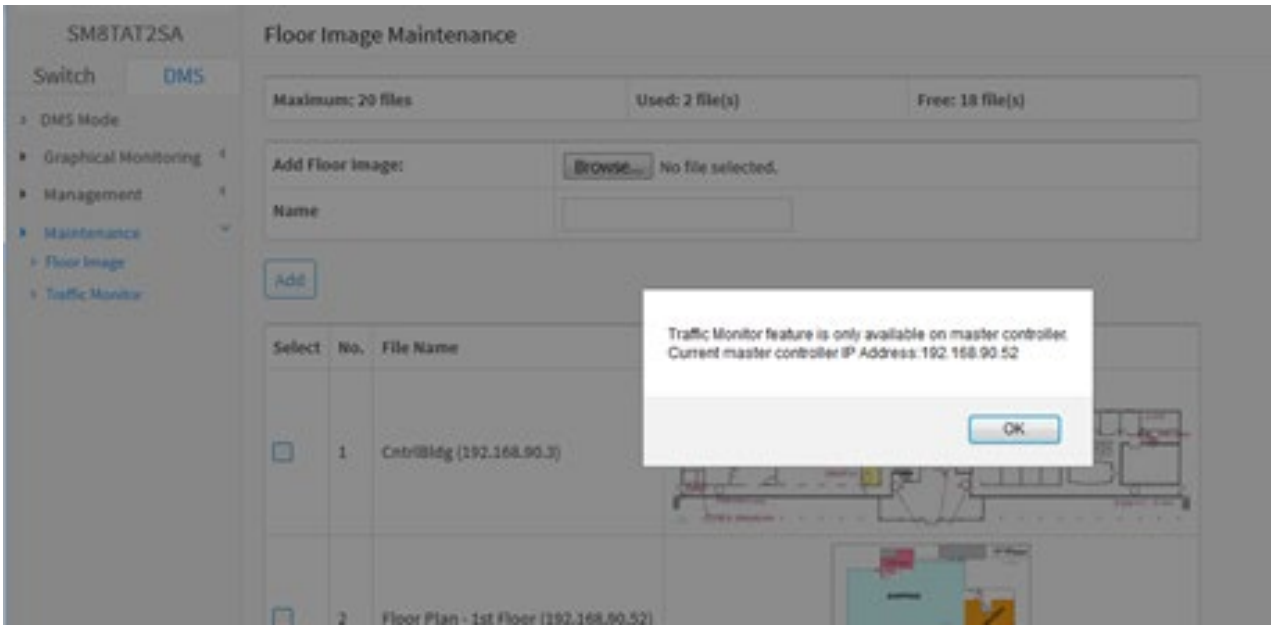
Throughput: Vertical axis shows throughput (e.g., 0 M – 18000 M or 0 M-1200 M). The unit of measure is Mbps.

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.*



16-6 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/

Appendix A Troubleshooting

Refer to the SMxTAT2SA Install Guide for install Troubleshooting, Warranty, Support, and Compliance information.

General Troubleshooting Procedure

Many problems are caused by the following situations. Check for these items first when you start troubleshooting:

1. Verify the install procedures were performed correctly. See the SMxTAT2SA Install Guide.

2. Check if the SMxTAT2SA POWER LED is Off:
   - Check connections between the switch, the power cord and the wall outlet.
   - Contact your dealer for assistance.

3. Check if the SMxTAT2SA Link LED is Off:
   - Verify that the switch and attached device are powered on.
   - Be sure the cable is plugged into the switch and corresponding device.
   - If the switch is installed in a rack, check the connections to the punch-down block and patch panel.
   - Verify that the proper cable type is used and its length does not exceed specified limits.
   - Check the adapter on the attached device and cable connections for possible defects. Replace the defective adapter or cable if necessary.

4. Make sure all devices connected to the SMxTAT2SA are configured to auto negotiate or are configured to connect at half duplex (all hubs are configured this way, for example).

5. Check the cabling:
   - Look for faulty or loose cables.
   - Look for non-standard and miswired cables.

6. Make sure you have a valid network topology:
   - Check for improper Network Topologies.
   - Make sure that your network topology contains no data path loops.

7. Check the port configuration.
   - Make sure ports have not been put into a “blocking” state by Spanning Tree, GVRP, or LACP. The normal operation of the Spanning Tree, GVRP, and LACP features may put the port in a blocking state.
   - Verify that the port has not been configured as disabled via software.

8. Make sure connected devices (e.g., SFPs, switches, hubs) are cabled, powered, and operating properly.

9. If possible, try switching modes (i.e., from Web UI to CLI, or vice versa).

10. Verify the specific function that failed (e.g., port config, PoE or VLAN management, QoS, Spanning Tree). Refer to the specific function's user manual page and online Help for details. Verify that the function you are trying to perform is supported by your particular switch model.

11. Run the tests in the Diagnostic tab of the Web UI. Verify that the interface is assigned to the correct VLAN. Use the Layer 2 traceroute. Check for spanning-tree problems such as BPDU floods or flapping mac address. Try a ping to broadcast IP address of subnet from your L3 device (Gateway).

12. Record any related error messages, conditions, and configurations for your Tech Support Specialist to consider. See below.

13. Contact Tech Support.

Record Device and System Information

After performing the troubleshooting procedures, and before calling or emailing Technical Support, please record as much information as possible to help the Tech Support Specialist.

1. Select the SMxTAT2SA **Switch** > **System** > **System Information** menu path to gather the information below or as requested by the Tech Support Specialist.
2. Record **Model**: _____

Hardware Version: _____ Firmware Version: _____

PoE Firmware Version: _____ S/N: _____

3. LED Status: _____

_____

4. Additional information for your Tech Support Specialist. See the "Troubleshooting" section above.

Your Lantronix service contract number: _____

A description of the failure: _____

_____

_____

_____

A description of any action(s) already taken to resolve the problem (e.g., change mode, reboot, etc.):

_____

_____

_____

_____

The serial and revision numbers of all involved Lantronix products in the network:

_____

_____

A description of your network environment (layout, cable type, etc.): _____

_____

_____

Network load and frame size at the time of trouble (if known): _____

The device history (i.e., have you returned the device before, is this a recurring problem, etc.):

_____

_____

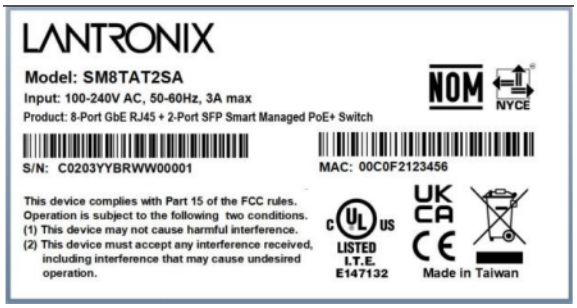
_____

_____

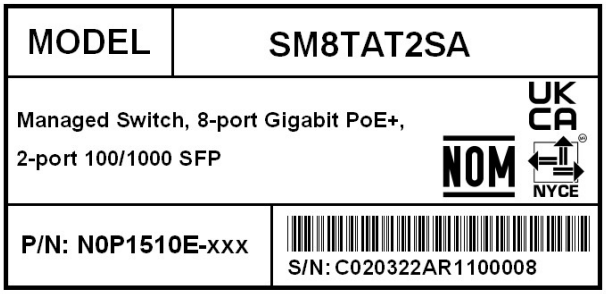
Previous Return Material Authorization (RMA) numbers: _____

_____

You can get Model, P/N, and S/N information from the Box label and the Device label:



Device Label



Box Label

Appendix B DHCP Per Port

You can configure DHCP Per Port via the CLI and Web UI. The DHCP Per Port factory default mode is Disabled. See the *CLI Reference* for CLI mode operation.

The switch's DHCP server assigns IP addresses. Clients get IP addresses in sequence and the switch assigns IP addresses on a per-port basis starting from the configured IP range. For example, if the IP address range is configured as 192.168.10.20 - 192.168.10.37 with one DHCP device connected to port 1, the client will always get IP address 192.168.10.20, then port 3 is always distributed IP address 192.168.10.22, even if port 2 is an empty port (because port 2 is always distributed IP address 192.168.10.21).

The switch does not allow a DHCP per Port pool to include the switch's address.

IP address assigned range and VLAN 1 should stay in the same subnet mask.

The configurable IP address range is allowed to configure over 18 IP addresses, but the switch always assigns one IP address per port connecting device.

The DHCP Per Port function is only supported on VLAN 1.

When the DHCP Per Port function is enabled, the switch software will automatically create the related DHCP pool named "DHCP_Per _Port".

Once the DHCP Per Port function is enabled on one switch, IPv4 DHCP client at VLAN1 mode (DMS DHCP mode), DHCP server mode are all limited to be enabled at the same time (an error message displays if attempted).

If the DHCP server pool has been configured, once you enable the DHCP Per Port function, then that DHCP server pool configuration will be overwritten.

Only for VLAN 1, clients issued DHCP packets will not be broadcast/forwarded to other ports. DHCP packets in others VLANs will be broadcast/forwarded to other ports.

The DHCP Per Port function allows the switch to connect only one DHCP client device.

DHCP-Per-Port is configured entirely on the **Switch** > **Configuration** > **System** > **IP** page, IP Interfaces window.
The feature is enabled here and an IP range (pool) is entered. The "automatic" results of this action can be displayed in:

- **Switch** > **Configuration** > **System** > **DHCP** > **Server** > **Mode** (Global Mode – Enabled, VLAN Mode - VLAN 1 created)
- **Switch** > **Configuration** > **System** > **DHCP** > **Excluded** (Excluded range created based on range entered)
- **Switch** > **Configuration** > **System** > **DHCP** > **Pool** (Pool "DHCP_Per_Port" created based on range entered)

Actual DHCP operation is monitored as normal under **System** > **Monitor** > **DHCP**.

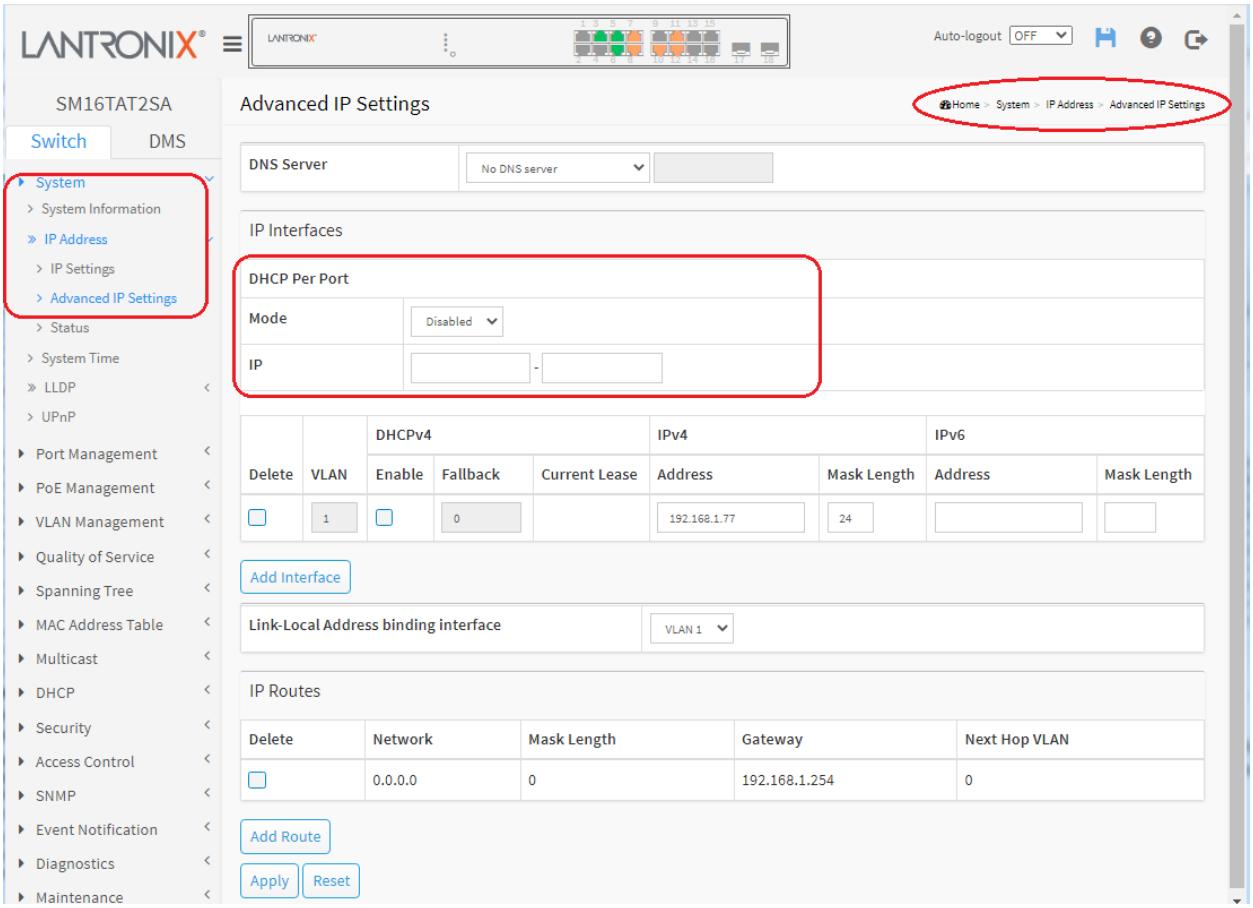
The DHCP Per Port pages and parameters are described below.

DHCP Per Port Mode Configuration

The DHCP Per Port function lets you assign an IP address based on the switch port the device is connected to. This will speed up installation of IP cameras, as the cameras can be configured after they are on the network. The DHCP Per Port assignment lets you know which IP was assigned to which camera.

Note: to prevent IP conflict, each switch can be allocated a different IP range.

To configure DHCP Per Port via the Web UI, navigate to the **System** > **IP Address** > **Advanced IP Settings** menu path.



Parameter descriptions: The DHCP Per Port parameters and buttons are described below.

DHCP Per Port Mode: at the dropdown select **Enable** or **Disable** the DHCP Per Port function globally. The default is **Disabled**.

IP: enter the IPv4 IP address range to be used when the DHCP Per Port function is enabled (e.g., 192.168.10.20 - 192.168.10.37). The DHCP Per Port IP range must be within the interface subnet. Note that DHCP Per Port with IPv6 is not supported at this time. The DHCP Per Port IP range must equal the switch port number excluding uplink ports (16).

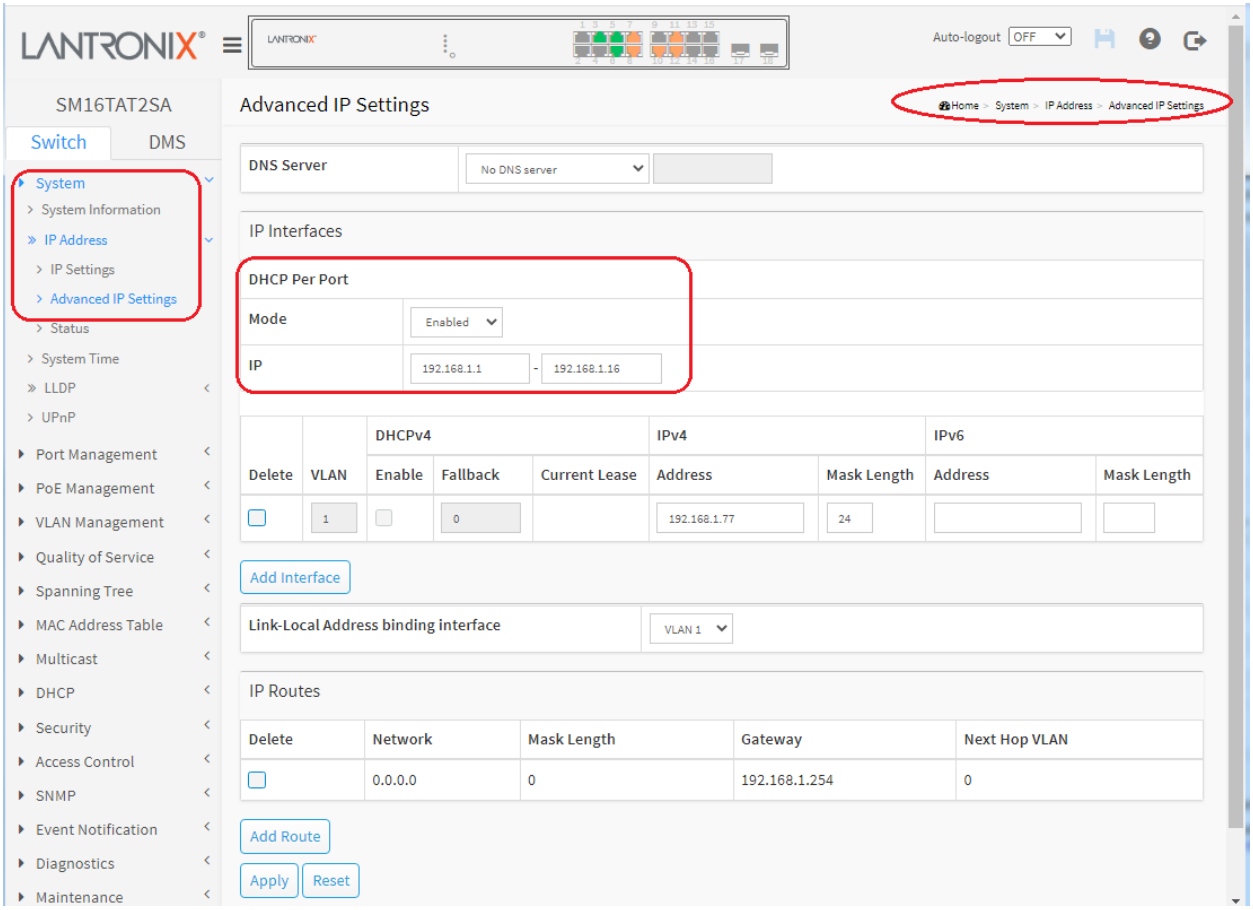
Apply: Click to save changes to the entries. If the entries are valid, the webpage message "*Update success!*" displays. Click the **OK** button to clear the message. If any entries are invalid, an error message displays. Click the **OK** button to clear the message and enter valid values, then click the **Apply** button again.

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

DHCP Server Mode Configuration

When DHCP Per Port is enabled at **Configuration** > **System** > **IP**, the checkbox and selection in the DHCP Server Mode Configuration section becomes grayed out (cannot be selected):

To monitor DHCP Per Port status, navigate to the **System > IP Address > Status** menu path.



Message: *Interface xx not using DHCP*

Meaning: The Interface being configured does not have DHCP enabled and configured.

Recovery: **1**. Click the **OK** button to clear the webpage message. **2**. Enable and configure DHCP for the interface being configured. See "DHCP Server Mode Configuration" on page 281.

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

Meaning: You entered an invalid IP address for the DNS Server being configured.

Recovery: **1**. Click the **OK** button to clear the webpage message. **2**. Enter a valid IP address in the format x.y.z.w per the on-screen restrictions. See "DHCP Server Mode Configuration" on page 281.

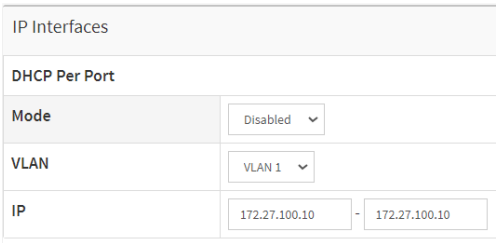
Message: *'DHCP Interface VLAN ID' must be an integer value between 1 and 4095.*

Meaning: You entered an invalid VLAN ID for the DHCP Interface.

Recovery: **1**. Click the **OK** button to clear the webpage message. **2**. Enter a valid VLAN ID for the DHCP Interface (1-4095). See "DHCP Server Mode Configuration" on page 281.

DHCP Per Port VLAN

The switch supports the DHCP IP Per Port function. It lets you have an IP address from a DHCP pool on a switch be statically assigned to a switchport, such that whichever device plugs into the switchport it will always be assigned that specific IP address. The IP address is configured in the interface config settings. Note that this is binding an IP address to an interface, not to a MAC address, which is the classic binding technique found on most switches. (Added at FW v1.04.0079.)



Navigate to Configuration > System > IP and at the dropdown select the DHCP Per Port VLAN parameter (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.

See “3-2.1 Advanced IP Settings” on page 18 for more information.

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

Technical Support
Online: techsupport@transition.com

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.