



# SM24DPB

## Managed Layer 2 Gigabit Ethernet Switch

(20) 100/1000Base-X SFP Slots + (4) 100/1000Base-X SFP/RJ-45

Combo Ports

The screenshot displays the web interface for the SM24DPB switch. The left sidebar shows navigation options like Configuration, Monitor, and Diagnostics. The main content area is titled 'System Information' and contains a table of system details. Below the table is an image of the physical switch with various components labeled.

Field	Value
Model Name	SM24DPB
System Description	Managed Switch, 20-port 100/1000 SFP, 4-port SFP/RJ-45 Combo
Location	
Contact	
System Name	SM24DPB
System Date	2011-01-01T00:03:20+00:00
System Uptime	00:03:20
Bootloader Version	v1.11e
Firmware Version	v1.11e
Hardware Version	AC 100V to 240V Power Input
Mechanical Version	
Serial Number	
MAC Address	
Memory	
FLASH	
Fan Speed	7031(rpm)
Powers	AC Power On 11.95V; DC Power On 0.00V
Temperature 1	34(C); 93(F)
Temperature 2	28(C); 82(F)
CPU Load (100ms, 1s, 10s)	0%, 10%, 3%

Physical switch components labeled in the image:

- DC 48V Power Input
- Port Status LEDs
- RST (Reset) button
- System Status LEDs
- 100/1000 SFP Ports
- 100/1000 RJ45/SFP Combo Ports
- Console Port

## Web User Guide

33682 Rev. C

## Safety Warnings and Cautions

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



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



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



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



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

### SM24DPB Managed Fiber Switch Web User Guide, 33682 Rev. C

#### Record of Revisions

Rev	Date	Description of Changes
A	5/26/16	Initial release for firmware version 6.46.
B	9/10/18	Update for FW v 6.48, update contact information. Update for FW v 6.54. Update for FW v6.54.2925 to add customized SSL certs, DMS Map View upload Google map API key function, and add port security sticky function. DMS interface can now be changed to any VLAN. Device's http port number can now be modified in the DMS device list page.
C	4/13/20	Upgrade for FW v6.54.3187 with password encryption change, add Rapid Ring, remove Force Cool Restart, add SCP feature, and add SNMP Trap over TCP. Upgrade for FW v6.54.3202 to add Traffic Monitor in DMS. FW v6.54.3359: Change DMS Topology view right side function key design. Add Click Save Button when Save Start Button on Web UI. Add message "Traffic Monitor feature is only available on Master switch". Add a field to show Aggregated Bandwidth information. Enhance Password encryption. Remove Bonjour Discovery. Add FindSwitch icon (Firefox only).

**Trademark notice:** All trademarks and registered trademarks are the property of their respective owners. All other products or service names used in this publication are for identification purposes only and may be trademarks or registered trademarks of their respective companies. All other trademarks or registered trademarks mentioned herein are the property of their respective holders.

**Copyright restrictions:** © 2016-2020 Transition Networks, Inc. All rights reserved. No part of this work may be reproduced or used in any form or by any means (graphic, electronic, or mechanical) without written permission from Transition Networks.

Address comments on this product or manual to:

#### Transition Networks Inc.

10900 Red Circle Drive, Minnetonka, MN 55343

tel: +1.952.941.7600 | toll free: 1.800.526.9267 | fax: 952.941.2322

[sales@transition.com](mailto:sales@transition.com) | [techsupport@transition.com](mailto:techsupport@transition.com) | [customerservice@transition.com](mailto:customerservice@transition.com)

Web: <https://www.transition.com>

## About This Manual

### Purpose

This manual gives specific information on how to operate and use the management functions of the SM24DPB.

### Audience

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

### FCC Caution

To assure continued compliance (e.g., use only shielded interface cables when connection to computer or peripheral devices). Any changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment. This device complies with Part 15 of the FCC Rules. Operation is subject to the Following two conditions: (1) This device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

### CE mark Warning

This is a Class B device; in a domestic environment, this product may cause radio interference, in which case the user may be required to take adequate measures.



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



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



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

### Related Manuals

The following manuals detail related switch aspects:

- SM24DPB Quick Start Guide, 33680
- SM24DPB Install Guide, 33681
- SM24DPB CLI Reference, 33683

Also, as part of the switch software, there is an online web-based help that describes the management related features. For Transition Networks Drivers, Firmware, etc. go to the [Product Support](#) webpage (login required). For Transition Networks Manuals, Brochures, Data Sheets, Specifications, etc. go to the [Support Library](#) (no registration required).

# Table of Contents

Safety Warnings and Cautions .....	ii
About This Manual .....	iii
Introduction.....	1
<b>About this Manual .....</b>	<b>1</b>
Chapter 1- Operation of Web-based Management.....	11
<b>1-1 Initial Configuration .....</b>	<b>11</b>
Chapter 2- System Configuration.....	13
<b>2-1 System .....</b>	<b>13</b>
2-1.1 Information .....	13
2-1.2 IP .....	14
2-1.3 NTP .....	17
2-1.4 Time.....	19
2-1.5 Log .....	21
<b>2-2 Ports Configuration.....</b>	<b>22</b>
2-2.1 Ports .....	22
2-3.2 Ports Description .....	24
<b>2-4 DHCP .....</b>	<b>25</b>
2-4.1 Server .....	25
2-4.1.1 Mode .....	25
2-4.1.2 Excluded IP .....	27
2-4.1.3 Pool .....	28
2-4.2 Snooping .....	30
2-4.3 Relay .....	32
<b>2-5 Security .....</b>	<b>34</b>
2-5.1 Switch .....	34
2-5.1.1 Users.....	34
2-5.1.2 Privilege Levels .....	36
2-5.1.3 Authentication Method Configuration .....	38
2-5.1.5 HTTPS.....	39
2-5.1.6 Access Management.....	41
2-5.1.7 SNMP.....	43
2-5.1.8 RMON.....	57
2-5.2 Network.....	62
2-5.2.1 Limit Control .....	62
2-5.2.2 NAS .....	65
2-5.2.3 ACL.....	72
2-5.2.4 IP Source Guard.....	84
2-5.2.5 ARP Inspection .....	87
2-5.3 AAA.....	93
2-5.3.1 RADIUS.....	93
2-5.3.2 TACACS+.....	95
<b>2-6 Aggregation .....</b>	<b>97</b>
2-6.1 Static.....	97
2-6.2 LACP.....	99
<b>2-7 Broadcast Storm Protection .....</b>	<b>101</b>
<b>2-8 Loop Protection .....</b>	<b>103</b>
<b>2-8 Spanning Tree .....</b>	<b>105</b>
2-8.1 Bridge Setting.....	105
2-8.2 MSTI Mapping.....	108
2-8.3 MSTI Priorities.....	110
2-8.4 CIST Ports .....	112

2-8.5 MSTI Ports .....	114
<b>2-9 IPMC Profile .....</b>	<b>116</b>
2-9.1 Profile Table .....	116
2-9.1.1 IPMC Profile Rule Settings Table .....	118
2-9.2 Address Entry .....	119
<b>2-10 MVR.....</b>	<b>121</b>
<b>2-11 IPMC.....</b>	<b>124</b>
2-11.1 IGMP Snooping .....	124
2-11.1.1 Basic Configuration .....	124
2-11.1.2 VLAN Configuration.....	126
2-11.1.3 Port Filtering Profile.....	128
2-11.2 MLD Snooping.....	130
2-11.2.1 Basic Configuration .....	130
2-11.2.2 VLAN Configuration.....	132
2-11.2.3 Port Group Filtering .....	134
<b>2-12 LLDP.....</b>	<b>135</b>
2-12.1 LLDP Configuration .....	135
2-12.2 LLDP-MED Configuration .....	138
<b>2-13 MAC Table .....</b>	<b>143</b>
<b>2-14 VLANs .....</b>	<b>146</b>
<b>2-15 Private VLANs .....</b>	<b>149</b>
2-15.1 VLAN Membership.....	149
2-15.2 Port Isolation.....	151
<b>2-16 VCL .....</b>	<b>152</b>
2-16.1 MAC-based VLAN.....	152
2-16.2 Protocol -based VLAN.....	154
2-16.2.1 Protocol to Group.....	154
2-16.2.2 Group to VLAN .....	156
2-16.3 IP Subnet-based VLAN .....	157
<b>2-17 Voice VLAN .....</b>	<b>158</b>
2-17.1 Configuration .....	158
2-17.2 OUI .....	160
<b>2-18 QoS .....</b>	<b>161</b>
2-18.1 Port Classification.....	161
2-18.2 Port Policing .....	163
2-18.4 Port Schedulers.....	165
2-18.5 Port Shaping.....	168
2-18.6 Port Tag Remarking.....	171
2-18.7 Port DSCP .....	174
2-18.8 DSCP-Based QoS .....	176
2-18.9 DSCP Translation .....	178
2-18.10 DSCP Classification.....	180
2-18.11 QoS Control List Configuration.....	181
2-18.12 Storm Control .....	185
2-18.13 WRED .....	187
<b>2-19 Mirroring .....</b>	<b>189</b>
<b>2-20 UPnP .....</b>	<b>191</b>
<b>2-21. GVRP .....</b>	<b>192</b>
2-21.1 Global Config.....	192
2-21.2 Port Config .....	194
<b>2-22. sFlow .....</b>	<b>196</b>
<b>2-23 SMTP Configuration .....</b>	<b>200</b>
Chapter 3. Monitor .....	202
<b>3-1 System .....</b>	<b>202</b>
3-1.1 Information .....	202

3-1.2 IP Status.....	204
3-1.3 Log .....	206
3-1.4 Detailed Log .....	208
3-1.5 Overview .....	209
<b>3-3 Ports .....</b>	<b>210</b>
3-3.1 Traffic Overview .....	210
3-3.3 QCL Status .....	213
3-3.4 Detailed Statistics.....	215
3-3.5 SFP Information.....	217
<b>3-4 DHCP .....</b>	<b>220</b>
3-4.1 Server .....	220
<b>3-4.1.1 Statistics .....</b>	<b>220</b>
<b>3-4.1.2 Binding.....</b>	<b>222</b>
<b>3-4.1.3 Declined IP .....</b>	<b>223</b>
3-4.2 Snooping Table .....	224
3-4.3 Relay Statistics.....	225
3-4.4 Detailed Statistics.....	227
<b>3-5 Security .....</b>	<b>229</b>
3-5.1 Access Management Statistics .....	229
3-5.2 Network.....	230
<b>3-5.2.1 Port Security.....</b>	<b>230</b>
<b>3-5.2.2 NAS .....</b>	<b>234</b>
<b>3-5.2.4 ARP Inspection .....</b>	<b>241</b>
<b>3-5.2.5 IP Source Guard.....</b>	<b>243</b>
3-5.3 AAA .....	244
<b>3-5.3.1 RADIUS Overview .....</b>	<b>244</b>
<b>3-5.3.2 RADIUS Details .....</b>	<b>246</b>
3-5.4 Switch .....	250
<b>3-5.4.1 RMON .....</b>	<b>250</b>
<b>3-6 LACP .....</b>	<b>257</b>
3-6.1 System Status .....	257
3-6.2 Port Status.....	258
3-6.3 Port Statistics.....	260
<b>3-7 Loop Protection .....</b>	<b>261</b>
<b>3-8 Spanning Tree .....</b>	<b>262</b>
3-8.1 Bridge Status .....	262
3-8.2 Port Status.....	263
3-8.3 Port Statistics.....	264
<b>3-9 MVR .....</b>	<b>265</b>
3-9.1 Statistics .....	265
3-9.2 MVR Channels Groups.....	266
3-9.3 MVR SFM Information .....	267
<b>3-10 IPMC .....</b>	<b>269</b>
3-10.1 IGMP Snooping .....	269
<b>3-10.1.1 Status .....</b>	<b>269</b>
<b>3-10.1.2 Group Information .....</b>	<b>271</b>
<b>3-10.1.3 IPv4 SFM Information .....</b>	<b>272</b>
3-10.2 MLD Snooping.....	274
<b>3-10.2.1 Status .....</b>	<b>274</b>
<b>3-10.2.2 Group Information.....</b>	<b>276</b>
<b>3-10.2.3 IPv6 SFM Information .....</b>	<b>277</b>
3-11.1 Neighbor .....	279
3-11.2 LLDP-MED Neighbors.....	281
3-11.3 Port Statistics .....	284
<b>3-12 MAC Table .....</b>	<b>286</b>
<b>3-13 VLANs .....</b>	<b>288</b>

3-13.1 VLAN Membership.....	288
3-13.2 VLAN Port Status.....	290
<b>3-14 VCL .....</b>	<b>292</b>
3-14.1 MAC-based VLAN.....	292
3-14.2 Protocol-based VLAN.....	293
<b>3-14.2.1 Protocol to Group.....</b>	<b>293</b>
<b>3-14.2.2 Group to VLAN .....</b>	<b>294</b>
3-14.3 IP Subnet-based VLAN.....	295
<b>3-15 sFlow .....</b>	<b>296</b>
Chapter 4. Diagnostics.....	298
<b>4-1 Ping.....</b>	<b>298</b>
<b>4-2 Ping6 .....</b>	<b>300</b>
<b>4-3 Cable Diagnostics.....</b>	<b>302</b>
<b>4-4 Traceroute .....</b>	<b>304</b>
Chapter 5. Maintenance.....	306
<b>5-1 Restart Device .....</b>	<b>306</b>
<b>5-2 Reboot Schedule .....</b>	<b>307</b>
<b>5-3 Factory Defaults .....</b>	<b>308</b>
<b>5-4 Firmware .....</b>	<b>309</b>
5-3.1 Firmware upgrade.....	309
5-3.2 Firmware Selection .....	311
<b>5-4 Configuration .....</b>	<b>313</b>
5-4.1 Save startup-config .....	313
5-4.2 Upload .....	315
5-4.3 Download .....	317
5-4.5 Delete .....	321
<b>5-5 Server Report.....</b>	<b>322</b>
Chapter 6. About DMS.....	323
<b>6-1 The DMS Tab .....</b>	<b>323</b>
DMS vs. NMS .....	323
6-2 DMS Features.....	323
Chapter 7. DMS > Mode.....	325
<b>7-1 DMS Mode .....</b>	<b>325</b>
<b>7-2 Devices List.....</b>	<b>326</b>
DMS > Management > Device List.....	326
Chapter 8. DMS > Graphical Monitoring.....	329
<b>8-1 Topology View.....</b>	<b>329</b>
.....	329
DMS > Graphical Monitoring > Topology View .....	329
<b>8-2 Floor View .....</b>	<b>334</b>
<b>8-3 Map View.....</b>	<b>337</b>
Chapter 9. DMS > Maintenance.....	340
<b>9-1 Floor Image .....</b>	<b>340</b>
DMS > Maintenance > Floor Image .....	340
<b>9-2 Diagnostics.....</b>	<b>342</b>
DMS > Maintenance > Diagnostics.....	342
DMS > Maintenance >Traffic Monitor .....	344
Chapter 10. Troubleshooting.....	346
Appendix A. Service, Warranty & Tech Support.....	347

Appendix B. Compliance Information ..... 347



# Introduction

## Overview

This manual describes how to install and connect your SM24DPB to the network and configure and monitor the SM24DPB via the web from the RJ-45 serial interface and Ethernet ports.

The SM24DPB next generation Web-managed switch from Transition Networks is a high performance Layer 2 managed switch with 48Gbps switching capacity. It provides up to 24 dual speed fiber slots.

SM24DPB features include:

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

## About this Manual

- Chapter 1 - Operation of Web-based Management
- Chapter 2 - System Configuration
- Chapter 3 - Monitor
- Chapter 4 - Diagnostics
- Chapter 5 - Maintenance
- Chapter 6 - About DMS
- Chapter 7 - DMS > Mode
- Chapter 8 - DMS > Graphical Monitoring
- Chapter 9 - DMS > Maintenance
- Chapter 10 - Troubleshooting
- Appendix A - Service, Warranty & Tech Support
- Appendix B - Compliance Information

# Chapter 1 - Operation of Web-based Management

## 1-1 Initial Configuration

This chapter describes how to configure and manage the SM24DPB via the web user interface. With this facility, you can easily access and monitor, via any port of the switch, all switch status, including each port activity, Spanning tree status, port aggregation status, multicast traffic, VLAN and priority status.

The SM24DPB default values are listed below:

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

After the SM24DPB interface has been configured you can browse it.

Type **192.168.1.77** in the address row in a browser and hit Enter. The login screen prompts you to enter a username and password in order to login.

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 is complete. In this login menu, you must enter the complete username and password respectively.

The SM24DPB allows two or more users with administrator rights to manage this switch; the most recent configuration settings will be the configuration used by the switch.



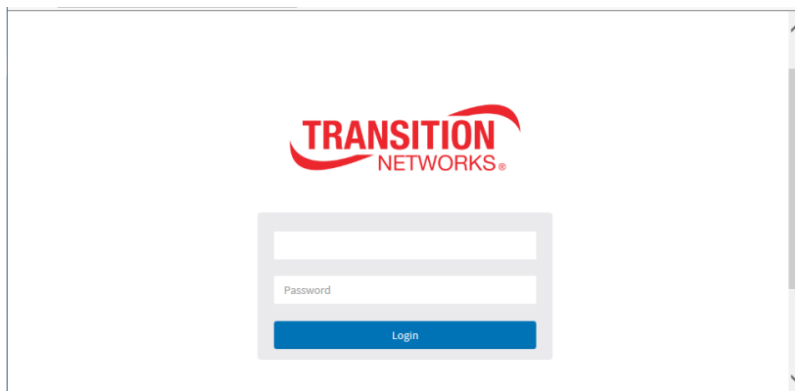
NOTE: When you login to the switch WEB/CLI to manager, you must first type the Username of admin the Password as admin, and press Enter. You can login to the SM24DPB Web UI management with IPv4 or IPv6 login to manage.

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



NOTE: The SM24DPB DHCP function is disabled by default. If you do not have a DHCP server to provide ip addresses to the switch, the switch default is IP 192.168.1.77.

**Figure 1 - Login page**



**Figure 2 - Main Menu (Startup Page)**

The startup page menu path is **Switch > Monitor > System > Information**.

SM24DPB

System Information Home > Monitor > System > Information

Model Name	SM24DPB
System Description	Managed Switch, 20-port 100/1000 SFP, 4-port SFP/RJ-45 Combo
Location	
Contact	
System Name	SM24DPB
System Date	2011-01-01T00:20:30+00:00
System Uptime	00:20:30
Bootloader Version	v1.15e
Firmware Version	v6.54.3359 2019-12-27
Hardware Version	v1.01
Mechanical Version	v1.01
Serial Number	A045116AR2200010
MAC Address	00-c0-f2-47-45-27
Memory	Total=72014 KBytes, Free=45250 KBytes, Max=43737 KBytes
FLASH	0x40000000-0x41ffff, 512 x 0x10000 blocks
Fan Speed	7031(rpm)
Powers	AC:11.95 V; DC:0.00 V
Temperature 1	33(C) ; 91(F)
Temperature 2	27(C) ; 80(F)
CPU Load (100ms, 1s, 10s)	3%, 8%, 4%

## Chapter 2 - System Configuration

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

### 2-1 System

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

#### 2-1.1 Information

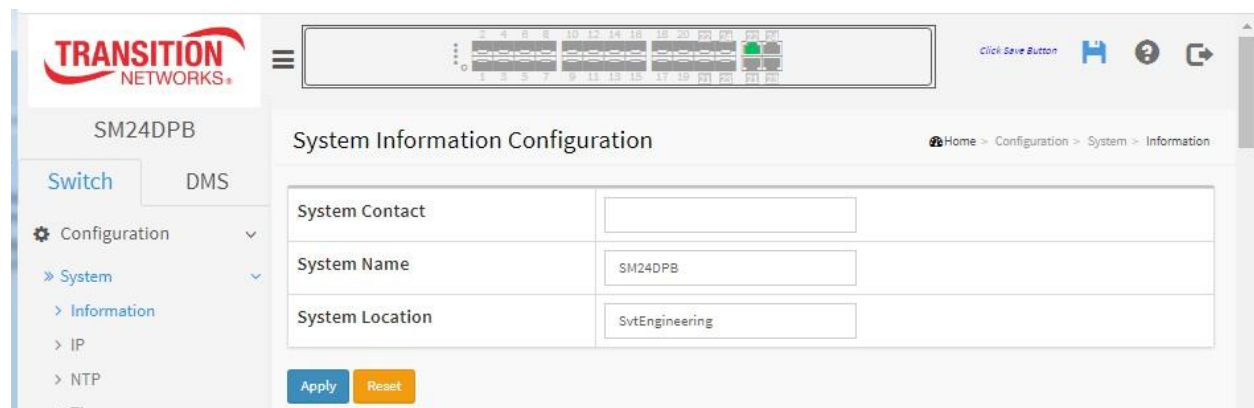
The switch system's contact information is provided here.

##### Web interface

To configure System Information in the web interface:

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

**Figure 2-1.1: System Information Configuration page**



##### Parameter descriptions:

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

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

**System Location:** The physical location of this node (e.g., telephone closet, 3rd floor). The allowed string length is 0 to 128, and the allowed content is the ASCII characters from 32 to 126.

##### Buttons

**Apply:** Click to save changes.

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

## 2-1.2 IP

The IPv4 address for the switch can 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.

Configure the switch-managed IP information on this page, and configure IP basic settings, control IP interfaces and IP routes. The maximum number of interfaces supported is 8 and the maximum number of routes is 32.

### Web Interface

To configure an IP address in the web interface:

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

**Figure 2-1.2: IP Configuration page**

The screenshot displays the IP Configuration page for a Transition Networks SM24DPB switch. The left sidebar shows the navigation menu with 'Configuration' expanded to 'System' and 'IP'. The main content area is titled 'IP Configuration' and includes the following sections:

- Mode:** A dropdown menu set to 'Router'.
- DNS Server:** A dropdown menu set to 'Configured' and a text input field containing '192.168.1.6'.
- DNS Proxy:** An unchecked checkbox.
- IP Interfaces:** A table with columns: Delete, VLAN, IPv4 DHCP (Enable, Fallback, Current Lease), IPv4 (Address, Mask Length), and IPv6 (Address, Mask Length). One interface is listed with VLAN 1, IPv4 address 192.168.1.77, and mask length 24.
- Link-Local Address binding interface:** A dropdown menu set to 'VLAN 1'.
- IP Routes:** A table with columns: Delete, Network, Mask Length, Gateway, and Next Hop VLAN. Three routes are listed: 0.0.0.0/0 with gateway 192.168.1.254, 169.254.0.0/16 with gateway 192.168.1.77, and 192.168.1.0/24 with gateway 192.168.1.77.

Buttons for 'Add Interface', 'Add Route', 'Apply', and 'Reset' are visible at the bottom of the configuration area.

### Parameter descriptions:

#### IP Configuration

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

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

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

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

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

From any DHCP interfaces
No DNS server
Configured
From this DHCP interface

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

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

### **IP Interfaces**

**Delete:** Check this checkbox to delete an existing IP interface.

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

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

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

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

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

**IPv4 Mask Length:** The IPv4 network mask, in number of bits (prefix length). Valid values are between 0 and 30 bits for a IPv4 address.

If DHCP is enabled, this field is not used. The field may also be left blank if IPv4 operation on the interface is not desired.

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

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

**IPv6 Mask Length:** The IPv6 network mask, in number of bits (prefix length). Valid values are between 1 and 128 bits for a 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 VLAN 1).

### **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 notation or a valid IPv6 notation. A default route can use the value 0.0.0.0 or IPv6 :: notation.

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

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

**Next Hop VLAN (Only for IPv6):** The VLAN ID (VID) of the specific IPv6 interface associated with the gateway.

The given VID ranges from 1 to 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 32 routes is supported.

**Apply:** Click to save changes.

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

## 2-1.3 NTP

NTP (Network Time Protocol) is used to sync to the network time based Greenwich Mean Time (GMT). If you use the NTP mode and select a built-in NTP time server or manually specify an NTP server as well as Time Zone, the switch will sync the time in a short after pressing **Apply** button. Although it synchronizes the time automatically, NTP does not update the time periodically without user 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 with the local time, otherwise, you will not able to get the correct time. The switch supports configurable time zones from -12 to +13 in one hour steps. The default Time zone offset is +8 hours.

### Web Interface

To configure NTP in the web interface:

1. Click Configuration, System, NTP.
2. Specify the NTP Server parameters on the NTP Configuration page.
3. Click Apply.
4. Specify the Time parameters on the Time Configuration page.

**Figure 2-1.3: NTP Configuration page**

Automatic	Disabled ▾
Server address via DHCP	
NTP Time-Sync Interval	60 ▾
Server address 1	<input type="text"/>
Server address 2	<input type="text"/>
Server address 3	<input type="text"/>
Server address 4	<input type="text"/>
Server address 5	<input type="text"/>

Apply Reset

### Parameter descriptions:

**Automatic** : Indicates the Automatic mode operation. Possible modes are:

**Enabled**: NTP servers available from the DHCP.

**Disabled**: NTP servers available from the config (default).

**Server address via DHCP** : Specify a list of IP addresses indicating NTP servers available to the client. Server #Provide the IPv4 or IPv6 address of a NTP server. IPv6 address is in 128-bit records represented as eight fields of up to four hexadecimal digits with a colon separating each field (:). For example, 'fe80::215:c5ff:fe03:4dc7'. The symbol '::' is a special syntax that can be used as a shorthand way of representing multiple 16-bit groups of contiguous zeros; but it can appear only once. It can also represent a legally valid IPv4 address. For example, '::192.1.2.34'.



**NTP Time-Sync Interval:** The switch is periodically transmitting NTP frames to its servers for having the network time information up-to-date. The interval between each NTP frame is determined by the NTP Time-Sync Interval value. Valid values are restricted to 5, 10, 15, 30, 60, or 120 minutes. The default is 60 minutes.

### Buttons

**Apply** – Click to save changes.

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

## 2-1.4 Time

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

### Web Interface

To configure Time in the web interface:

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

**Figure 2-1.4: Time Configuration page**

The screenshot displays the 'Time Configuration' page in the SM24DPB web interface. The page is organized into three main sections:

- Time Configuration:**
  - Clock Source:** A dropdown menu set to 'Use Local Settings'.
  - System Date:** A text input field containing '2020-02-07 15:57:22' with a format hint '(yyyy-mm-dd hh:mm:ss)'.
- Time Zone Configuration:**
  - Time Zone:** A dropdown menu set to 'None'.
  - Acronym:** A text input field with a hint '(0 - 16 characters)'.
- Daylight Saving Time Configuration:**
  - Daylight Saving Time:** A dropdown menu set to 'Disabled'.
  - Start Time settings:**
    - Month:** A dropdown menu set to 'Jan'.
    - Date:** A dropdown menu set to '1'.
    - Year:** A dropdown menu set to '2000'.
    - Hours:** A dropdown menu set to '0'.
    - Minutes:** A dropdown menu set to '0'.
  - End Time settings:**
    - Month:** A dropdown menu set to 'Jan'.
    - Date:** A dropdown menu set to '1'.
    - Year:** A dropdown menu set to '2000'.
    - Hours:** A dropdown menu set to '0'.
    - Minutes:** A dropdown menu set to '0'.
  - Offset settings:**
    - Offset:** A text input field containing '1' with a hint '(1 - 1440) Minutes'.

At the bottom of the page, there are two buttons: 'Apply' (blue) and 'Reset' (orange).

**Parameter descriptions:****Time Configuration**

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

Select "Use Local Settings" : Clock Source from Local Time.

Select "Use NTP Server" : Clock Source from NTP Server.

**System Date:** Show the current time of the system. The year of system date is limited to between 2011 and 2037.

**Time Zone Configuration**

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

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

**Daylight Saving Time Configuration**

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

**Recurring Configuration****Start time settings:**

Week - Select the starting week number.

Day - Select the starting day.

Month - Select the starting month.

Hours - Select the starting hour.

Minutes - Select the starting minute.

**End time settings:**

Week - Select the ending week number.

Day - Select the ending day.

Month - Select the ending month.

Hours - Select the ending hour.

Minutes - Select the ending minute.

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



---

**NOTE:** The "Start Time Settings" and "End Time Settings" displays what you set on the "Start Time Settings" and "End Time Settings" field information.

---

**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.

## 2-1.5 Log

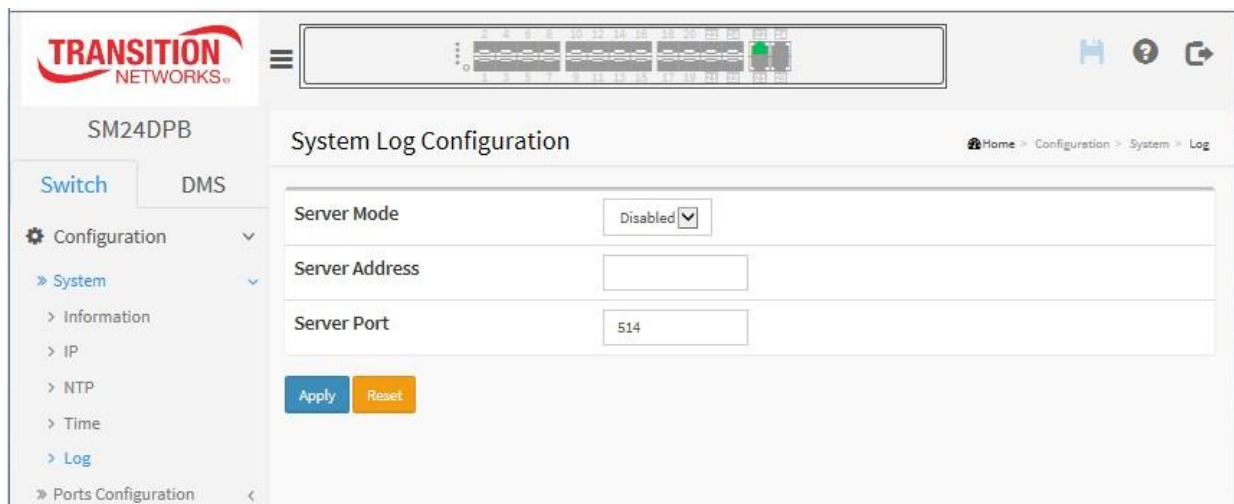
Syslog is a standard for logging program messages . It allows separation of the software that generates messages from the system that stores them and the software that reports and analyzes them. It can be used as a generalized informational, analysis and debugging messages. It is supported by a wide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

### Web Interface

To configure log configuration in the web interface:

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

**Figure2-1.5: System Log Configuration page**



### Parameter descriptions:

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

**Enabled:** Enable server mode operation.

**Disabled:** Disable server mode operation.

**Server Address :** Indicates the IPv4 hosts address of the syslog server. If the switch has the DNS feature enabled and configured, it also can be a host name.

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

### Buttons

**Apply** – Click to save changes.

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

## 2-2 Ports Configuration

This page lets you configure the Port detail parameters, enable or disable switch ports, and monitor ports' config and status.

### 2-2.1 Ports

This page lets you view and configure current port parameters.

#### Web Interface

To configure a Current Port Configuration in the web interface:

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

**Figure 2-2.1: Ports Configuration page**

Port	Link	Speed		Flow Control			Maximum Frame Size
		Current	Configured	Current Rx	Current Tx	Configured	
*			Auto			<input type="checkbox"/>	10056
1	●	Down	Auto				10056
2	●	Down	Auto				10056
3	●	Down	Auto				10056
4	●	Down	Auto				10056
5	●	Down	Auto				10056
6	●	Down	Auto				10056
18	●	Down	Auto				10056
19	●	Down	Auto				10056
20	●	Down	Auto				10056
21	●	Down	SFP_Auto_AMS	⊗	⊗	<input type="checkbox"/>	10056
22	●	1Gfdx	SFP_Auto_AMS	⊗	⊗	<input type="checkbox"/>	10056
23	●	Down	SFP_Auto_AMS	⊗	⊗	<input type="checkbox"/>	10056
24	●	Down	SFP_Auto_AMS	⊗	⊗	<input type="checkbox"/>	10056

#### Parameter descriptions:

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

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

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

**Configured Link Speed** : Selects any available link speed for the given switch port. Only the speed supported by the specific port is 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

**2.5Gbps FDX** - Forces the Serdes port in 2.5Gbps full duplex mode.

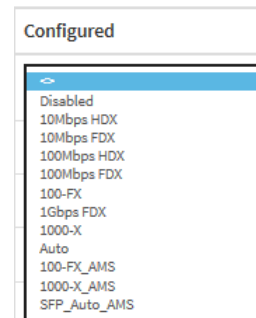
**SFP\_Auto\_AMS** - Automatically determines the speed of the SFP. There is no standardized way to do SFP auto detect, so here it is by reading the SFP rom. Due to the missing standardized way of SFP auto detect, some SFPs might not be detectable. The port is set in AMS mode. Cu port is set in Auto mode.

**100-FX** - SFP port in 100-FX speed. Cu port disabled.

**100-FX\_AMS** - Port in AMS mode. SFP port in 100-FX speed. Cu port in Auto mode.

**1000-X** - SFP port in 1000-X speed. Cu port disabled.

**1000-X\_AMS** - Port in AMS mode. SFP port in 1000-X speed. Cu port in Auto mode. Ports in AMS mode with 1000-X speed has Cu port preferred. Ports in AMS mode with 100-FX speed has fiber port preferred.



Note:  
done  
doing

**Flow Control** : When Auto Speed is selected on a port, this section indicates the flow control capability that is advertised to the link partner. When a fixed-speed setting is selected, that is what is used. The Current Rx column indicates whether pause frames on the port are obeyed, and the Current Tx column indicates whether pause frames on the port are transmitted. The Rx and Tx settings are determined by the result of the last Auto-Negotiation.

Check the configured column to use flow control. This setting is related to the setting for Configured Link Speed.

**Maximum Frame Size** : Enter the maximum frame size allowed for the switch port, including FCS.

### Buttons

**Apply** – Click to save changes.

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

**Refresh** - Click for manual refresh the Port link Status.

## 2-3.2 Ports Description

This page lets you configure the Port's alias or any descriptions for the Port Identity. You can enter an alphanumeric string describing the full name and version identification for the system's hardware type, software version, and networking application.

### Web Interface

To configure a Port Description in the web interface:

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

**Figure 2-3.1: Port Description page**

Port	Description
1	<input type="text"/>
2	<input type="text"/>
3	<input type="text"/>
4	<input type="text"/>
5	<input type="text"/>
6	<input type="text"/>
7	<input type="text"/>
8	<input type="text"/>

### Parameter descriptions:

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

**Description :** Enter up to 47 characters to be descriptive name for identifies this port.

### Buttons

**Apply** – Click to save changes.

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

## 2-4 DHCP

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

### 2-4.1 Server

#### 2-4.1.1 Mode

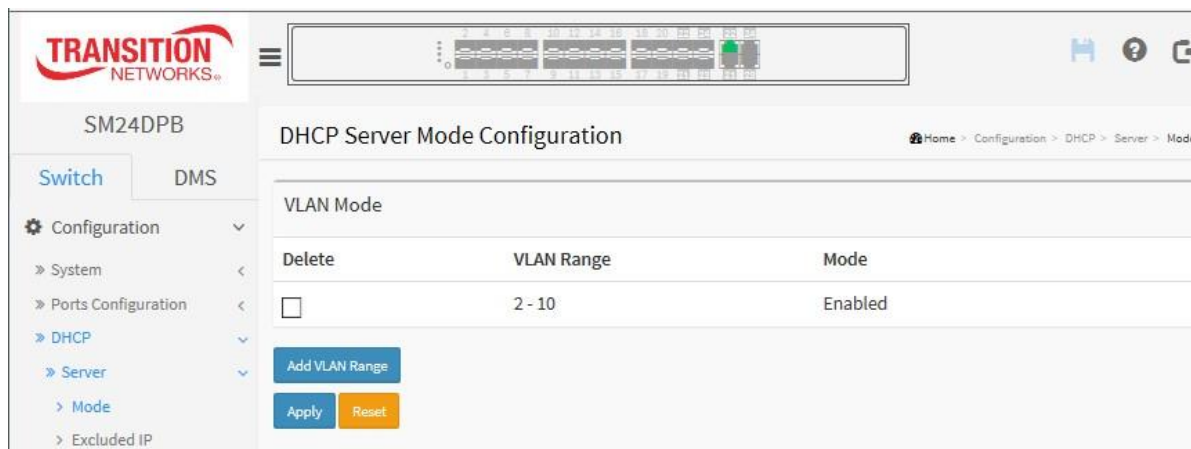
This page configures global mode and VLAN mode to enable/disable DHCP server per system and per VLAN.

#### Web Interface

To configure DHCP server mode in the web interface:

1. Click Configuration, DHCP, Server, Mode.
2. Click Add VLAN Range.
3. Select “Enabled” in the Global Mode of DHCP Server Mode Configuration.
4. Add a VLAN Range.
5. Click Apply.

**Figure 2-4.1.1: DHCP Server Mode Configuration page**



#### Parameter descriptions:

**Mode :** Configure the operation mode per system. Possible modes are:

**Enabled:** Enable DHCP server per system.

**Disabled:** Disable DHCP server per system.

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

To disable existing VLAN range, then you can follow these steps.

1. Click “Add VLAN Range” to add a new VLAN range.
2. Enter the VLAN range that you want to disable.
3. Choose Mode to be Disabled.
4. Click Apply to apply the change. The disabled VLAN range is removed from the page.



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

***Enabled:*** Enable DHCP server per VLAN.

***Disabled:*** Disable DHCP server per VLAN.

### **Buttons**

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

**Apply** - Click to save changes.

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

### 2-4.1.2 Excluded IP

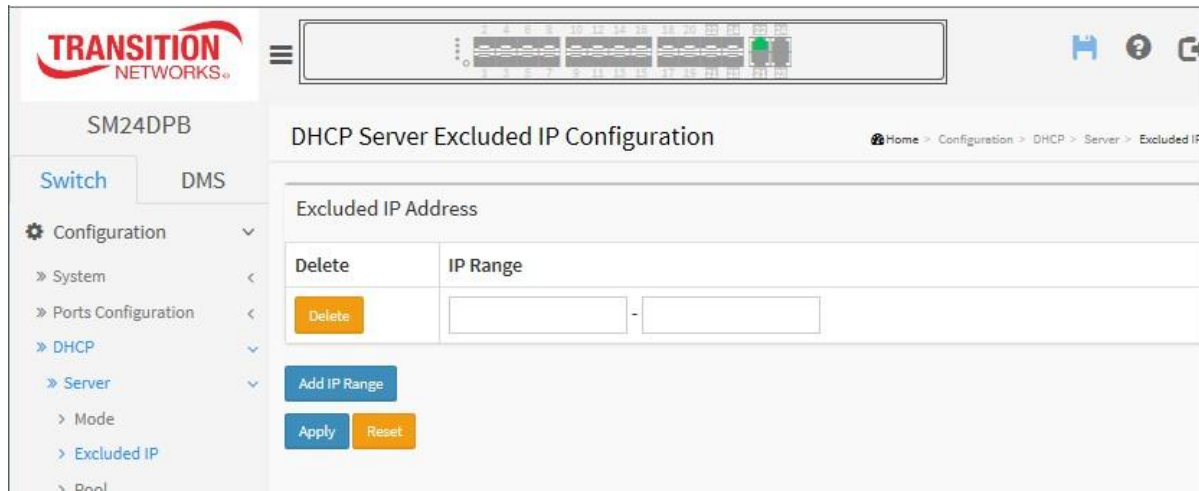
This page configures excluded IP addresses. The DHCP server will not allocate these excluded IP addresses to DHCP client.

#### Web Interface

To configure DHCP server excluded IP in the web interface:

1. Click Configuration, DHCP, Server, Excluded IP.
2. Click Add IP Range and create a new IP Range on the switch.
3. Click Apply.

**Figure 2-4.1.2: DHCP Server Excluded IP page**



#### Parameter descriptions:

**IP Range** : Define the IP range to be excluded IP addresses. The first excluded IP must be smaller than or equal to the second excluded IP. But, if the IP range contains only 1 excluded IP, then you can just input it to either one of the first and second excluded IP or both.

#### Buttons

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

**Apply** – Click to save changes.

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

### 2-4.1.3 Pool

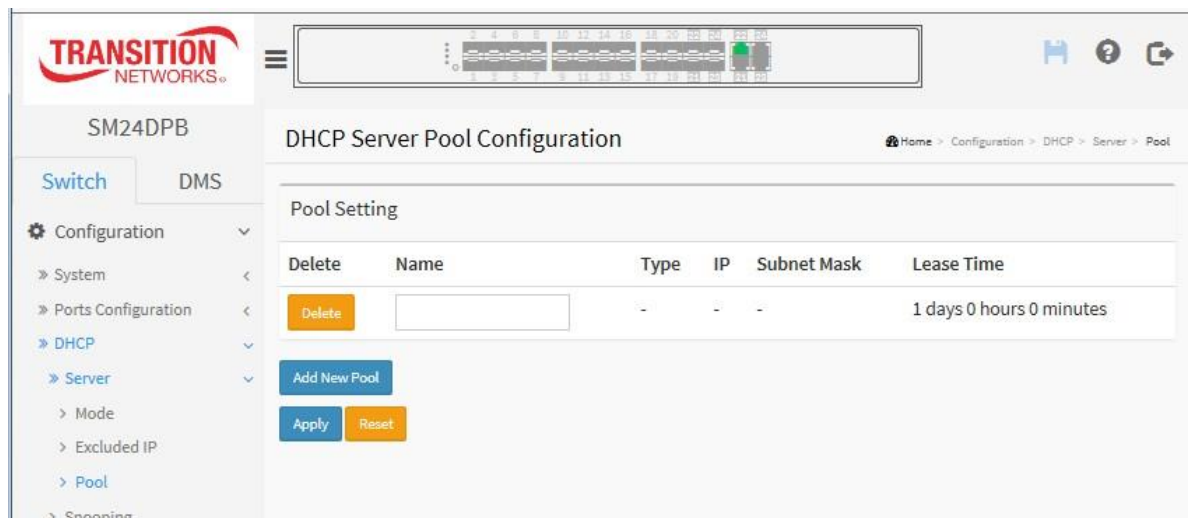
This page manages DHCP pools. According to the DHCP pool, the DHCP server will allocate IP address and deliver configuration parameters to the DHCP client.

#### Web Interface

To configure DHCP server pool in the web interface:

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

**Figure 2-4.1.1: DHCP Server Pool Configuration page**



#### Parameter descriptions:

**Pool Setting** : Add or delete pools. Adding a pool and giving a name is to create a new pool with "default" configuration. If you want to configure all settings including type, IP subnet mask and lease time, you can click the pool name to go into the configuration page.

**Name** : Configure the pool name that accepts all printable characters, except white space. If you want to configure the detail settings, you can click the pool name to go into the configuration page.

**Type** : Display which type of the pool is.

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

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

If "-" is displayed, it means not defined.

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

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

**Lease Time** : Display lease time of the pool.

#### Buttons

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

**Apply** – Click to save changes.

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

## 2-4.2 Snooping

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 switch DHCP Snooping parameters. DHCP Snooping can prevent attackers from adding their own DHCP servers to the network.

### Web Interface

To configure DHCP snooping in the web interface:

1. Click Configuration, DHCP, Snooping.
2. Select "Enabled" in the Snooping Mode dropdown.
3. Select "Trusted" as the specific port at the Mode dropdown for one or more ports.
4. Click Apply.

**Figure 2-4.2: DHCP Snooping Configuration page**

The screenshot shows the web interface for configuring DHCP Snooping on a SM24DPB switch. The breadcrumb trail is Home > Configuration > DHCP > Snooping. The 'Snooping Mode' is currently set to 'Disabled'. Below this is the 'Port Mode Configuration' table:

Port	Mode
*	↵
1	Trusted
2	Trusted
3	Trusted
4	Trusted
5	Trusted
6	Trusted
7	Trusted

### Parameter descriptions:

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

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

**Disabled:** Disable DHCP snooping mode operation.

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

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

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

## **Buttons**

**Apply** – Click to save changes.

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

### 2-4.3 Relay

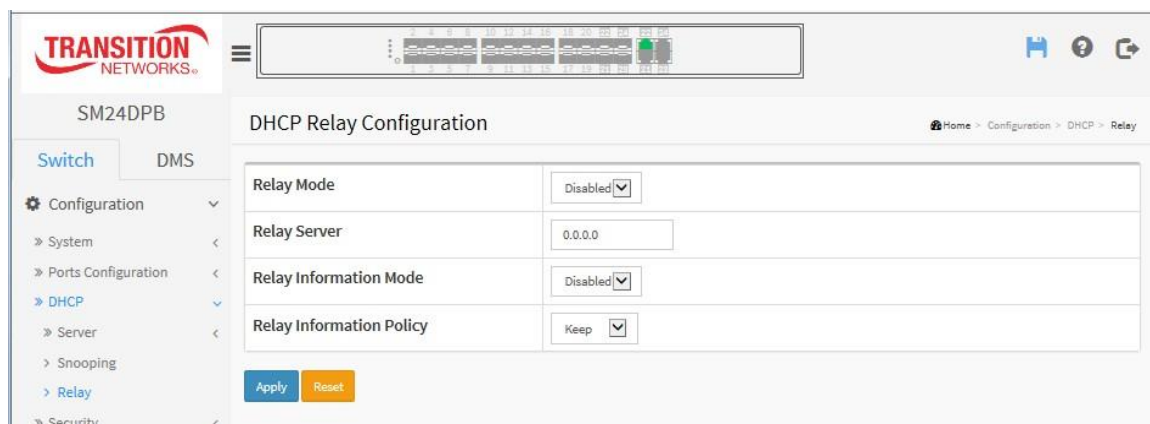
A DHCP relay agent is used to forward and to transfer DHCP messages between the clients and the server when they are not in the same subnet domain. It stores the incoming interface IP address in the GIADDR field of the DHCP packet. The DHCP server can use the value of GIADDR field to determine the assigned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

#### Web Interface

To configure DHCP Relay in the web interface:

1. Click Configuration, DHCP, Relay.
2. Specify the Relay Mode, Relay Server, Relay Information Mode, and Relay Information Policy.
3. Click Apply.

**Figure 2-4.3: DHCP Relay Configuration page**



#### Parameter descriptions:

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

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

**Disabled**: Disable DHCP relay mode operation.

**Relay Server** Indicates the DHCP relay server IP address.

**Relay Information Mode** Indicates the DHCP relay information mode option operation. The Option 82 circuit ID format is "[vlan\_id][module\_id][port\_no]". The first four characters represent the VLAN ID, the fifth and sixth characters are the module ID (in standalone device it always equals 0), and the last two characters are the port number. For example, "00030108" means the DHCP message received from VLAN ID 3, switch ID 1, port # 8. The Option 82 remote ID value is equal to the switch MAC address.

Possible modes are:

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

**Disabled**: Disable DHCP relay information mode operation.

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

Possible policies are:

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

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

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

## Buttons

**Apply** – Click to save changes.

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



## 2-5 Security

This section describes how to 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.

### 2-5.1 Switch

#### 2-5.1.1 Users

This page provides an overview of the current users. Currently the only way to login as another user on the web server is to close and reopen the browser

#### **Web Interface**

To configure User in the web interface:

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

**Figure 2-5.1.1: Users Configuration page**

The screenshot shows the 'Add User' configuration page in the SM24DPB web interface. The page has a navigation menu on the left with 'Users' selected. The main content area contains a form with the following fields:

User Settings	
User Name	<input type="text"/>
Password	<input type="password"/>
Password (again)	<input type="password"/>
Privilege Level	0 <input type="button" value="v"/>

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

#### **Parameter descriptions:**

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

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

**Password (again) :** Type the same password again in the field.

**Privilege Level :** The privilege level of the user. The allowed range is 0 to 15. If the privilege level value is 15, it can access all groups (i.e., granted full control of the device). For other values, refer to each group privilege level. User's privilege should be same or greater than the group privilege level to have the access of that group.

By default setting, most groups have privilege level 5 (read-only access); privilege level 10 has read-write access. The system maintenance (software upload, factory defaults and etc.) requires user privilege level 15. Generally, privilege level 15 can be used for an Administrator account, privilege level 10 for a standard User account, and privilege level 5 for a Guest account.

## Buttons

**Apply** – Click to save changes. You are logged out and can log in again as the new user.

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

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

After you log in again, you can go to Configuration > Security > Switch > Users again and on the Users Configuration page, click a linked User Name to display its Edit User page. Here you can change the Password and Privilege settings.

## 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).

### 2-5.1.2 Privilege Levels

This page provides an overview of the privilege levels. The switch lets you set levels of 1-15 for each feature or module.

#### Web Interface

To configure Privilege Level in the web interface:

1. Click Configuration, Security, Switch, Privilege Levels.
2. Specify the Privilege Level parameter.
3. Click Apply.

**Figure2-5.1.2: Privilege Level Configuration page**

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

#### Parameter descriptions:

**Group Name :** The name identifying the privilege group. In most cases, a privilege level group consists of a single module (e.g. LACP, RSTP or QoS), but a few of them contain more than one. These privilege level groups are defined in detail below.

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

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

**IP:** Everything except 'ping'.

**Port:** Everything except 'Diagnostic Test'.

**Diagnostics:** 'ping' and 'Diagnostic Test'.

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

**Debug:** Only present in CLI.

**Privilege Levels** Every group has an authorization Privilege level for the following sub groups: configuration read-only, configuration/execute read-write, status/statistics read-only, status/statistics read-write (e.g. for clearing of statistics). User Privilege should be same or greater than the authorization Privilege level to have the access to that group.

## **Buttons**

**Apply** – Click to save changes.

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

### 2-5.1.3 Authentication Method Configuration

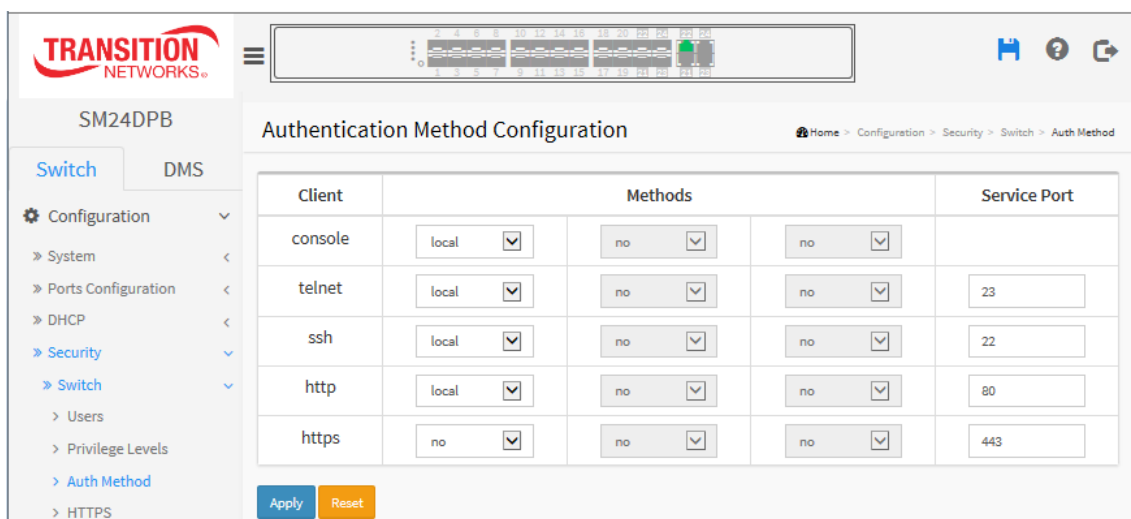
This page lets you configure a user with authentication when he logs into the switch via one of the management client interfaces.

#### Web Interface

To configure an Authentication Method via the web interface:

1. Click Configuration, Security, Switch, Auth Method.
2. Specify one or more Clients (console, telnet, ssh, http, and https) that you want to monitor.
3. Specify the Authentication Method (no, redirect, local, radius, or tacacs+).
4. Select additional Methods dropdowns and select Service Port(s).
5. Click the **Apply** button.

**Figure 2-4.1.3: Authentication Method Configuration page**



#### Parameter descriptions:

**Client:** The management client for which the configuration below applies (console, telnet, ssh, http, https). SSH is a secure communication protocol that combines authentication and data encryption to provide secure encrypted communication.

**Methods:** Authentication 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 a remote RADIUS server for authentication.
- tacacs:** use a remote TACACS+ server for authentication.



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

#### Buttons:

**Apply:** Click to save changes.

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

## 2-5.1.5 HTTPS

This page lets you configure the HTTPS settings and maintain the current certificate on the switch..

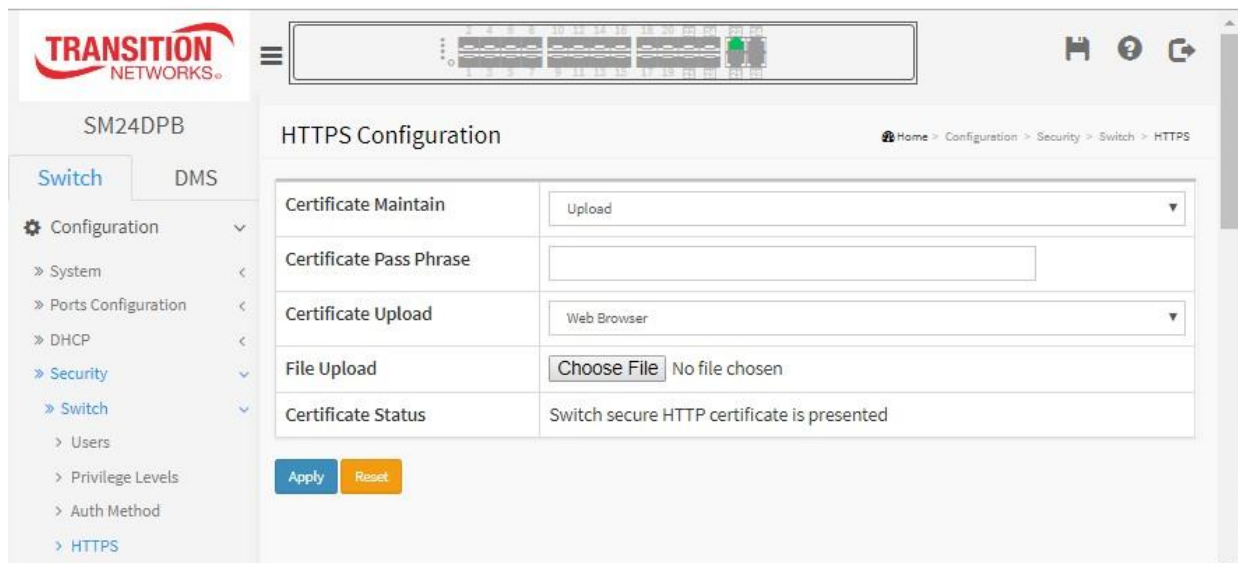
HTTPS is a secure communication protocol that combines authentication and data encryption to provide secure encrypted communication via the browser.

### Web Interface

To configure HTTPS Configuration in the web interface:

1. Select “Enabled” in the Mode of HTTPS Configuration.
2. Select “Enabled” in the Automatic Redirect of HTTPS Configuration.
3. Click Apply.

**Figure 2-5.1.5: HTTPS Configuration page**



### Parameter descriptions:

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

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

**Generate**: Generate a new self-signed RSA certificate.

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

**Certificate Upload** : Upload a certificate PEM file into the switch. The file should contain the certificate and private key together. If you have two separate files for saving certificate and private key, use the Linux cat command to combine them into a single PEM file.

For example, `cat my.cert my.key > my.pem`.

Note that the RSA certificate is recommended since most of the new browser versions have removed support for DSA in certificates (e.g. Firefox v37 and Chrome v39).

Possible methods are:

**Web Browser**: Upload a certificate via Web browser.

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

For example, tftp://10.10.10.10/new\_image\_path/new\_image.dat,  
http://username:password@10.10.10.10:80/new\_image\_path/new\_image.dat.

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

**File Upload:** Click the Choose File button to browse to and select a certificate file. Displays *No file chosen* until a file is selected.

**Certificate Status :** Displays the current status of certificate on the switch. Possible statuses are:  
*Switch secure HTTP certificate is presented.*  
*Switch secure HTTP certificate is not presented.*  
*Switch secure HTTP certificate is generating ....*

## Buttons

**Apply :** Click to save changes.

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

## 2-5.1.6 Access Management

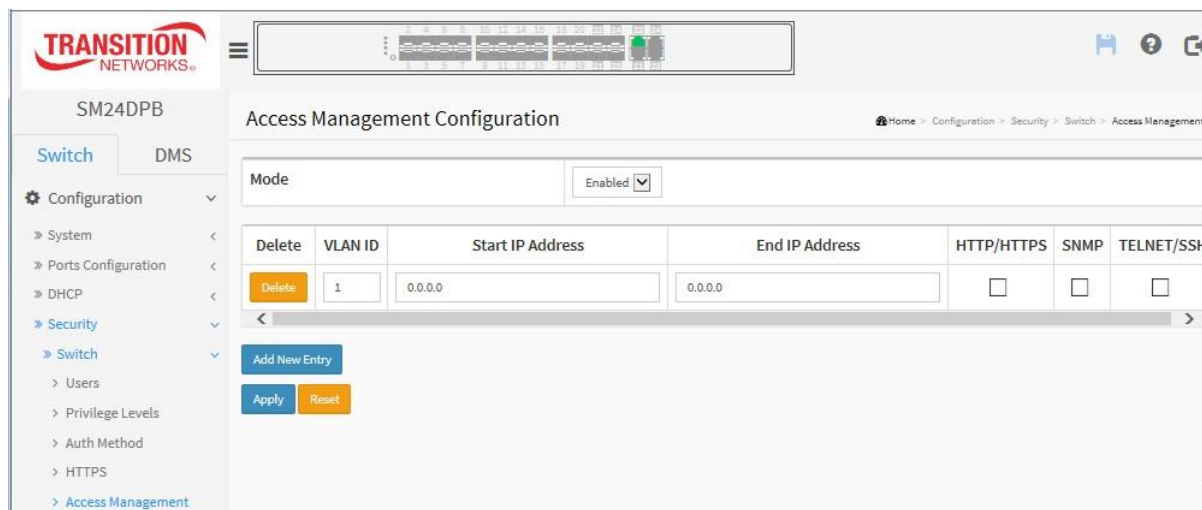
This page lets you configure access management for the switch including HTTP/HTTPS, SNMP, and TELNET/SSH. You can manage the switch over an Ethernet LAN, or over the Internet.

### Web Interface

To configure an Access Management Configuration in the web interface:

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

**Figure 2-5.1.6: Access Management Configuration page**



### Parameter descriptions:

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

**Enabled**: Enable access management mode operation.

**Disabled**: Disable access management mode operation (default).

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

**Delete** : Check to delete the entry. It will be deleted immediately.

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

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

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

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

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



**Buttons:**

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

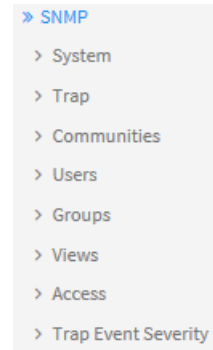
**Apply** – Click to save changes.

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

### 2-5.1.7 SNMP

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

Basically, it is passive except issuing the trap information. The switch lets you disable the SNMP agent. If you set the field SNMP “Enable”, the SNMP agent will supported MIB OIDs, including RMON MIB, can be accessed via SNMP manager. SNMP is set “Disable”, the SNMP agent will be de-activated, and the related Community Name, Trap Host IP Address, Trap and all MIB counters will be ignored.



SNMP on the between described requests

enable or start. All If the field

#### 2-5.1.7.1 System

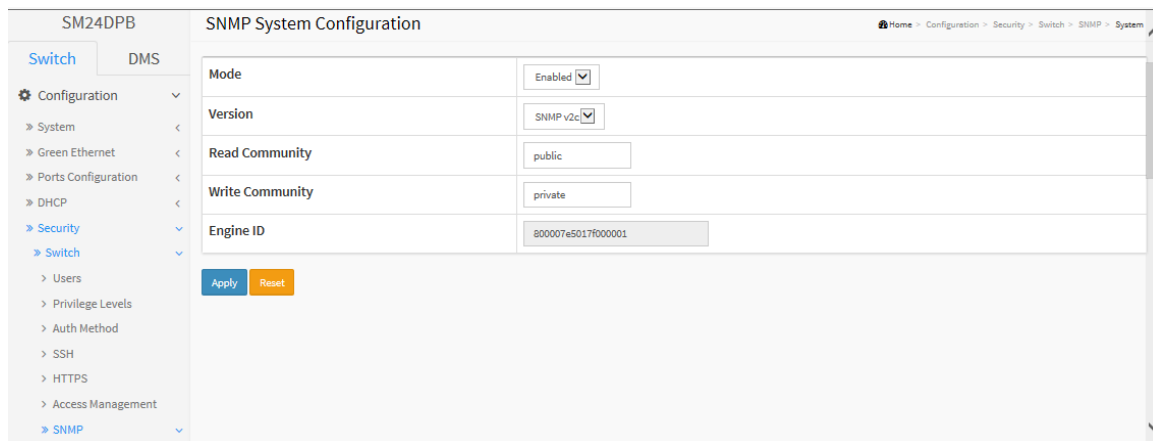
This page lets you configure SNMP System on the switch. This function is used to configure SNMP settings, community name, trap host and public traps as well as the throttle of SNMP. A SNMP manager must pass the authentication by identifying both community names, then it can access the MIB information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

#### Web Interface

To display the configure SNMP System in the web interface:

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

**Figure2-5.1.7.1: SNMP System Configuration page**



#### Parameter descriptions:

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

**Enabled:** Enable SNMP mode operation.

**Disabled:** Disable SNMP mode operation.

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

**SNMP v1:** Set SNMP supported version 1.

**SNMP v2c:** Set SNMP supported version 2c.

**SNMP v3:** Set SNMP supported version 3.

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

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

**Write Community** : Indicates the community write access string to permit access to SNMP agent. The allowed string length is 0 to 255, 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.

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

## **Buttons:**

**Apply** – Click to save changes.

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

### 2-5.1.7.2 Trap

Configure SNMP trap parameters on this page.

#### Global Settings

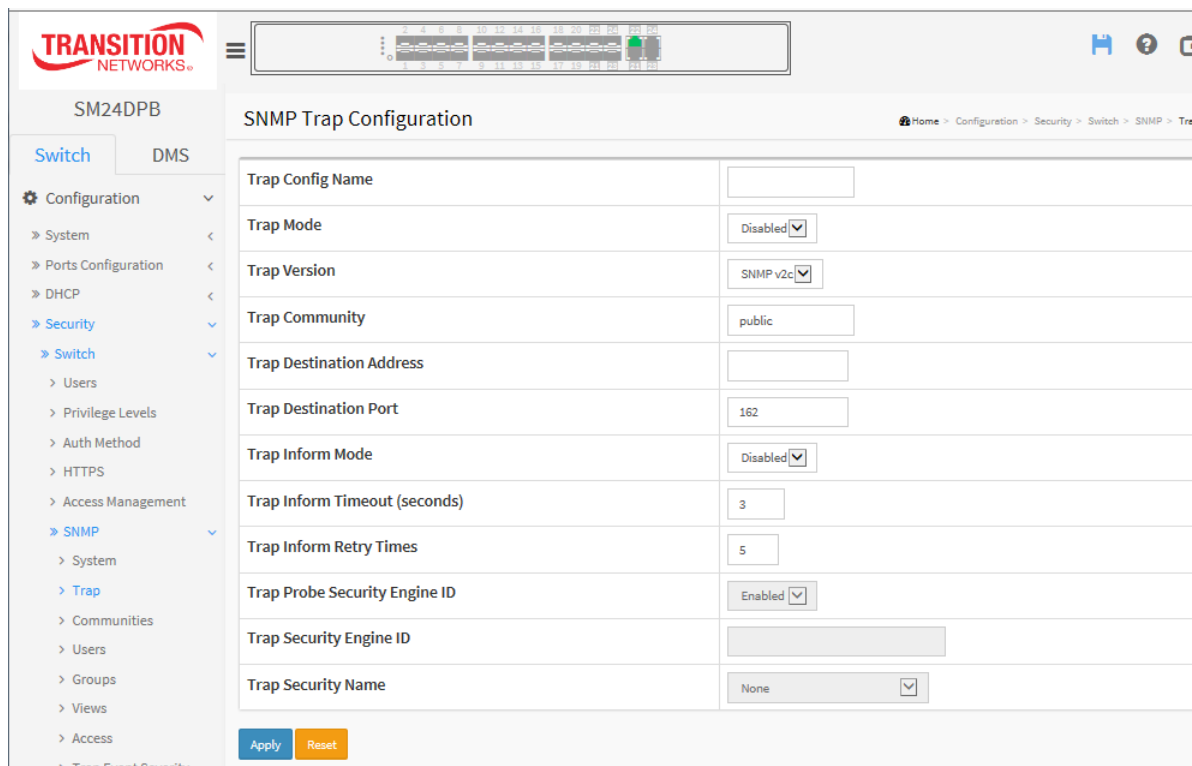
Configure SNMP trap globally on this page.

#### Web Interface

To configure SNMP Trap parameters via the web interface:

1. Click Configuration, Security, Switch, SNMP, Trap.
2. Click Add New Entry and enter the parameters to create a new SNMP Trap.
3. Click Apply.

**Figure2-5.1.7.2: SNMP Trap Configuration page**

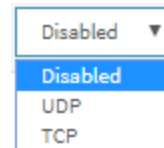


#### Global Settings

**Trap Config Name :** Enter the trap Configuration's name (the trap destination's name).

**Trap Mode :** Indicates the trap mode operation. Possible modes are:

- Disabled:** Disable SNMP trap mode operation (default).
- TCP:** Enable TCP SNMP mode operation.
- UDP:** Enable UDP SNMP mode operation.



**Trap Version :** Indicates the SNMP trap supported version. Possible versions are:

- SNMPv1:** Set SNMP trap supported version 1.
- SNMPv2c:** Set SNMP trap supported version 2c.
- SNMPv3:** Set SNMP trap supported version 3.

**Trap Community :** Indicates the community access string when sending SNMP trap packet. The allowed string length is 0 to 255, and the allowed content is ASCII characters from 33 to 126.

**Trap Destination Address :** Indicates the SNMP trap destination address. It allows a valid IP address in dotted decimal notation ('x.y.z.w').

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

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

**Trap Destination Port :** Indicates the SNMP trap destination port. SNMP Agent will send SNMP message via this port, the port range is 1-65535.

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

**Enabled:** Enable SNMP trap inform mode operation.

**Disabled:** Disable SNMP trap inform mode operation.

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

**Trap Inform Retry Times :** Indicates the SNMP trap inform retry times. The allowed range is 0 to 255.

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

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

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

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

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

## Buttons:

**Apply** – Click to save changes.

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

### 2-5.1.7.3 Communities

This page lets you configure up to four SNMPv3 communities. The Community and User Name are unique. To create a new community account, click the Add New Community button, enter the account information, and then click the Apply button.

#### Web Interface

To display the configure SNMP Communities in the web interface:

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

**Figure2-4.1.7.3: SNMP Community Security Configuration page**

Delete	Community	Source IP	Source Mask
<input type="checkbox"/>	public	0.0.0.0	0.0.0.0
<input type="checkbox"/>	private	0.0.0.0	0.0.0.0
<input type="checkbox"/>		0.0.0.0	0.0.0.0

Buttons: Add New Entry, Apply, Reset

#### Parameter descriptions:

**Delete** : Check to delete the entry. It will be deleted immediately.

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

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

**Source Mask** : Indicates the SNMP access source address mask.

#### Buttons:

**Add New Entry** – Click to add a new entry.

**Apply** – Click to save changes.

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

### 2-5.1.7.4 Users

This page lets you configure up to ten SNMPv3 users.

#### Web Interface

To configure SNMP Users via the web interface:

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

**Figure 2-5.1.7.4: SNMPv3 User Configuration page**

Delete	Engine ID	User Name	Security Level	Authentication Protocol	Authentication Password	Privacy Protocol	Privacy Password
<input type="checkbox"/>	800007e5017f000001	default_user	NoAuth, NoPriv	None	None	None	None
<input type="button" value="Delete"/>	<input type="text"/>	<input type="text"/>	Auth, Priv <input type="checkbox"/>	MDS <input type="checkbox"/>	<input type="text"/>	DES <input type="checkbox"/>	<input type="text"/>

Buttons: Add New Entry, Apply, Reset

#### Parameter descriptions:

**Delete** : Check to delete the entry. It will be deleted immediately.

**Engine ID** : An octet string identifying the engine ID that this entry should belong to. The string must contain an even number (in hexadecimal format) with number of digits between 10 and 64, but all-zeros and all-'F's are not allowed. The SNMPv3 architecture uses the User-based Security Model (USM) for message security and the View-based Access Control Model (VACM) for access control. For the USM entry, the usmUserEngineID and usmUserName are the entry's keys. In a simple agent, usmUserEngineID is always that agent's own snmpEngineID value. The value can also take the value of the snmpEngineID of a remote SNMP engine with which this user can communicate. In other words, if user engine ID equal system engine ID then it is local user; otherwise it's remote user.

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

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

**NoAuth, NoPriv:** No authentication and no privacy.

**Auth, NoPriv:** Authentication and no privacy.

**Auth, Priv:** Authentication and privacy.

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

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

**None:** No authentication protocol.

**MD5:** An optional flag to indicate that this user uses MD5 authentication protocol.

**SHA:** An optional flag to indicate that this user uses SHA authentication protocol.

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

**Authentication Password :** A string identifying the authentication password phrase. For MD5 authentication protocol, the allowed string length is 8 to 32. For SHA authentication protocol, the allowed string length is 8 to 40. The allowed content is ASCII characters 33 - 126.

**Privacy Protocol :** Indicates the privacy protocol that this entry should belong to. Possible privacy protocols are:

**None:** No privacy protocol.

**DES:** An optional flag to indicate that this user uses DES authentication protocol.

**Privacy Password :** A string identifying the privacy password phrase. The allowed string length is 8 - 32, and the allowed content is ASCII characters 33 - 126.

## Buttons:

**Add New Entry** – Click to add a new entry.

**Apply** – Click to save changes.

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

**Note:** at Firmware v6.54.3187, password encryption implemented SHA256 instead of Base64, the encryption SHA256 is directly applied after FW upgrade. After the FW is upgraded, the password is automatically converted to SHA256 so that the Username/Password of admin / admin can log in.



### 2-5.1.7.5 Group

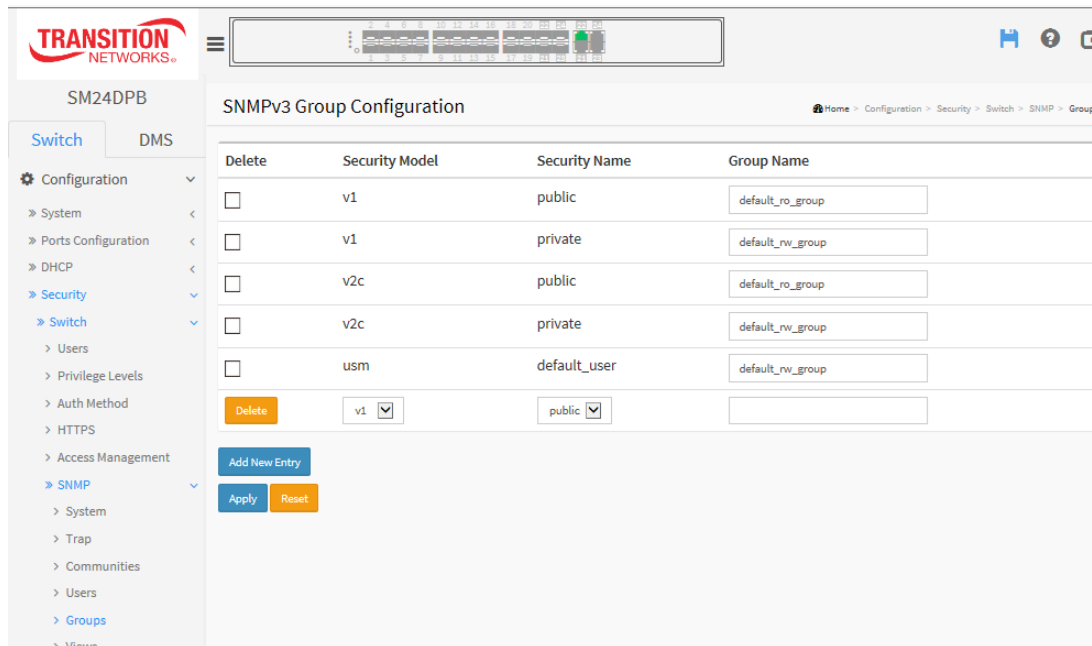
This page lets you configure SNMPv3 group. The Entry index keys are Security Model and Security Name. Max Group Number: v1: 2, v2: 2, v3:10.

#### Web Interface

To configure the SNMP Groups in the web interface:

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

**Figure 2-5.1.7.5: SNMPv3 Group Configuration page**



#### Parameter descriptions:

**Delete** : Check to delete the entry. It will be deleted immediately.

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

**v1**: Reserved for SNMPv1.

**v2c**: Reserved for SNMPv2c.

**usm**: User-based Security Model (USM).

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

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

**Buttons:**

**Add New Entry** – Click to add a new entry.

**Apply** – Click to save changes.

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

### 2-5.1.7.6 Views

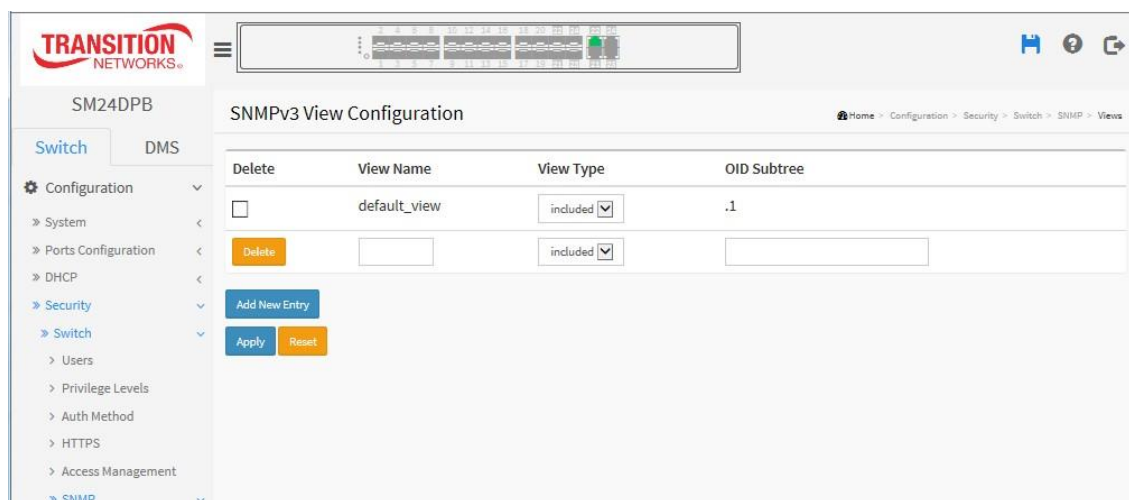
This page lets you configure up to 28 SNMPv3 Views. The Entry index keys are OID Subtree and View Name. The entry index keys are View Name and OID Subtree.

#### Web Interface

To display the configure SNMP views in the web interface:

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

**Figure 2-5.1.7.6: SNMPv3 View Configuration page**



#### Parameter descriptions:

**Delete** : Check to delete the entry. It will be deleted immediately.

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

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

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

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

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

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

#### Buttons:

**Add New Entry** – Click to add a new entry.

**Apply** – Click to save changes.

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

### 2-5.1.7.7 Access

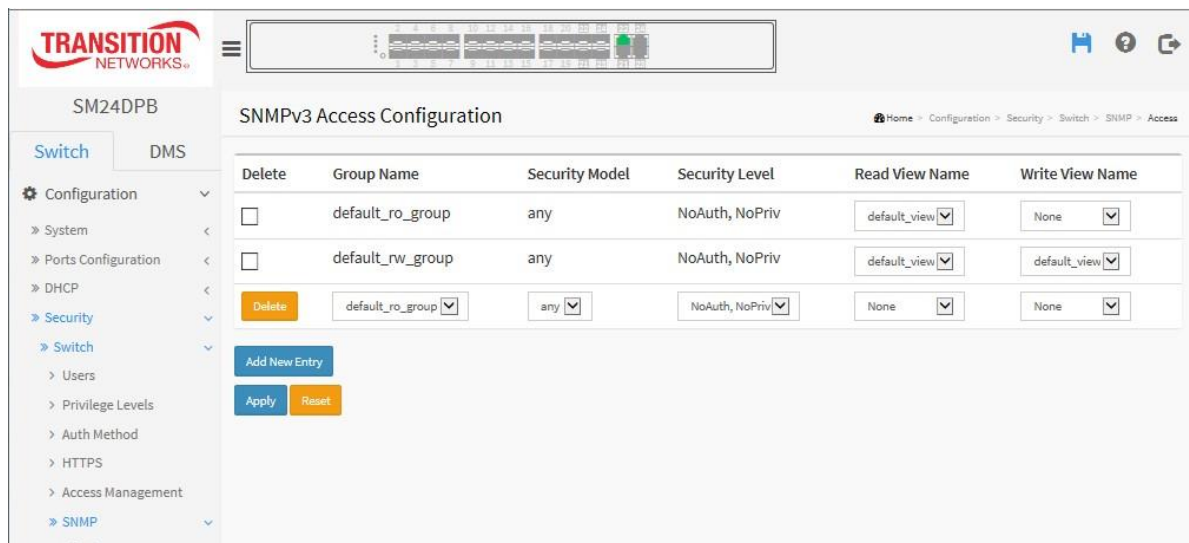
This page lets you configure up to 14 SNMPv3 accesses. The Entry index key are Group Name, Security Model and Security level.

#### Web Interface

To configure SNMP Access in the web interface:

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

**Figure 2-5.1.7.7: SNMPv3 Access Configuration page**



#### Parameter descriptions:

**Delete** : Check to delete the entry. It will be deleted immediately.

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

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

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

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

- NoAuth, NoPriv**: No authentication and no privacy.
- Auth, NoPriv**: Authentication and no privacy.
- Auth, Priv**: Authentication and privacy.

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

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

**Buttons:**

**Add New Entry** – Click to add a new entry.

**Apply** – Click to save changes.

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

### 2-5.1.7.8 Trap Event Severity

This page displays current trap event severity configurations. Trap event severity can also be configured here for ACL, ACL Log, AUTO SAVING, Access Mgmt, Auth Failed, BCS Protection, Cold Start, Config Info, DMS, Dying Gasp, FAN FAIL, Fan, Firmware Upgrade, Import Export, LACP, Link Status, Login, Logout, Loop Protect, Mgmt IP Change, Module Change, NAS, Password Change, Port Security, Temperature, Voltage, and Warm Start.

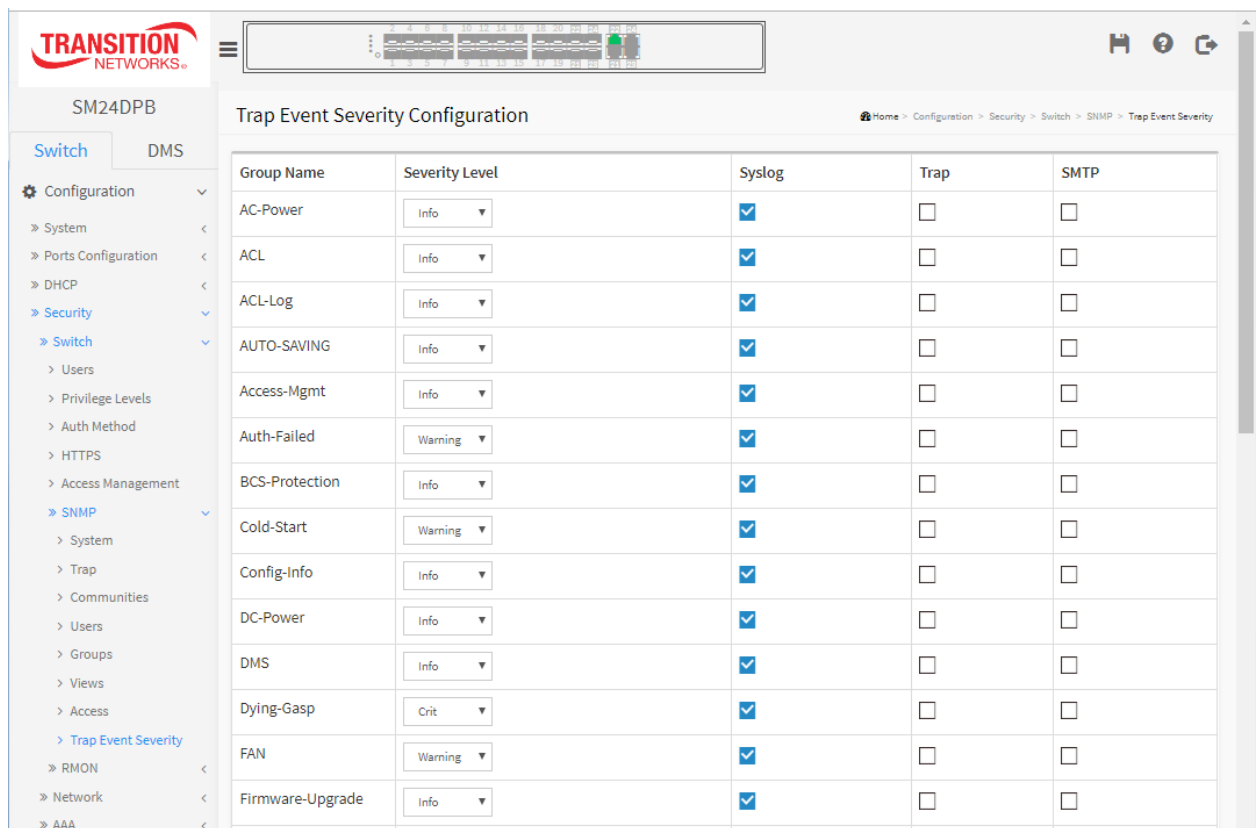
Informations can be via Syslog, SNMP Trap, and/or SMTP.

#### Web Interface

To display the configure Trap Event Severity in the web interface:

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

**Figure 2-5.1.7.8: Trap Event Severity Configuration page**



#### Parameter descriptions:

**Group Name :** The name identifying the severity group.

**Severity Level :** Every group has an severity level. These levels are supported:

- <0> **Emergency:** System is unusable.
- <1> **Alert:** Action must be taken immediately.
- <2> **Critical:** Critical condition.
- <3> **Error:** Error condition.
- <4> **Warning:** Warning condition.

- <5> **Notice**: Normal but significant condition.
- <6> **Information**: Information message.
- <7> **Debug**: Debug-level message.

**Syslog** : Check to enable this Group Name for informing in Syslog. The default is checked (Enabled).

**Trap** : Check to enable t this Group Name for informing in SNMP Traps. The default is unchecked (Disabled).

**SMTP** : Check to enable t this Group Name for informing in SMTP. The default is unchecked (Disabled).

## 2-5.1.8 RMON

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

### 2-5.1.8.1 Statistics

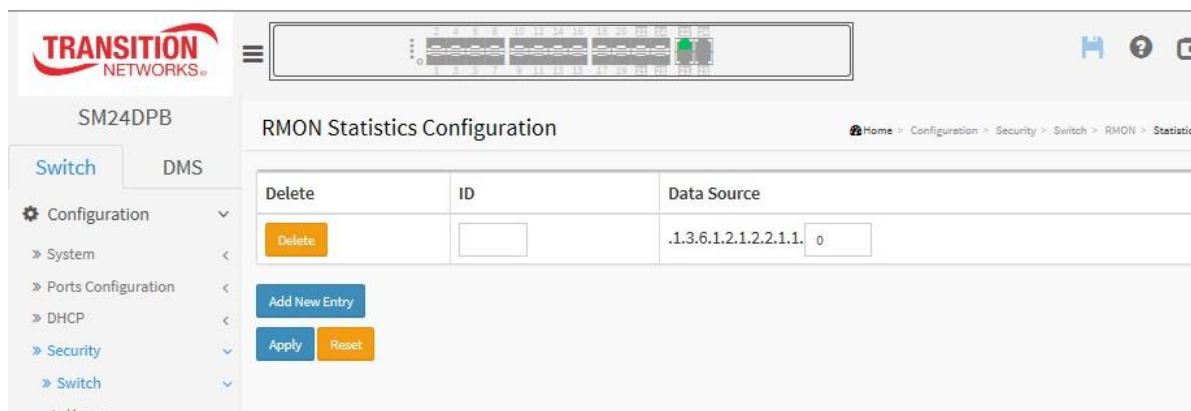
Configure RMON Statistics table on this page. The entry index key is **ID**.

#### **Web Interface**

To display the configure RMON configuration in the web interface:

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

**Figure 2-5.1.8.1: RMON Statics Configuration**



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

**Delete :** Check to delete the entry immediately.

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

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

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

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

**Buckets Granted :** The number of data are saved in the RMON.

#### **Buttons:**

**Add New Entry** – Click to add a new entry.

**Apply** – Click to save changes.

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



### 2-5.1.8.2 History

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

#### Web Interface

To display the configure RMON History in the web interface:

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

**Figure 2-5.1.8.2: RMON History Configuration**

Delete	ID	Data Source	Interval	Buckets	Buckets Granted
<input type="checkbox"/>	<input type="text"/>	.1.3.6.1.2.1.2.2.1.1	1800	50	

Buttons: Add New Entry, Apply, Reset

#### Parameter descriptions:

**Delete** : Check to delete the entry. It will be deleted immediately.

**ID** : Indicates the index of the entry. The range is from 1 to 65535.

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

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

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

**Buckets Granted** : The number of data are saved in the RMON.

#### Buttons:

**Add New Entry** – Click to add a new entry.

**Apply** – Click to save changes.

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

### 2-5.1.8.3 Alarm

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

#### Web Interface

To display the configure RMON Alarm in the web interface:

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

**Figure 2-5.1.8.3: RMON Alarm Configuration**

Delete	ID	Interval	Variable	Sample Type	Value	Startup Alarm	Rising Threshold	Rising Index	Falling Threshold	Falling Index
<input type="button" value="Delete"/>	<input type="text" value=""/>	<input type="text" value="30"/>	<input type="text" value=".1.3.6.1.2.1.2.2.1"/>	<input type="text" value="Delta"/>	<input type="text" value="0"/>	<input type="text" value="RisingOrFalling"/>	<input type="text" value="0"/>	<input type="text" value="0"/>	<input type="text" value="0"/>	<input type="text" value="0"/>

Buttons:

#### Parameter descriptions:

**Delete** : Check to delete the entry. It will be deleted immediately.

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

**Interval** : Indicates the interval in seconds for sampling and comparing the rising and falling threshold. The range is from 1 to 2<sup>31</sup>-1.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

**Absolute:** Get the sample directly.

**Delta:** Calculate the difference between samples (default).

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

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

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

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

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

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

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

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

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

#### **Buttons:**

**Add New Entry** – Click to add a new entry.

**Apply** – Click to save changes.

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

### 2-5.1.8.4 Event

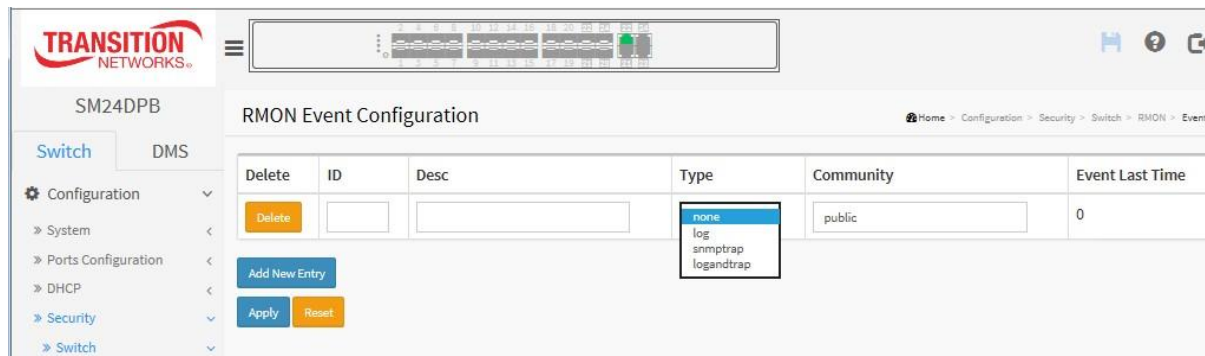
Configure the RMON Event table on this page. The entry index key is **ID**.

#### Web Interface

To display the configure RMON Event in the web interface:

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

**Figure 2-5.1.8.4: RMON Event Configuration**



#### Parameter descriptions:

These parameters are displayed on the RMON History Configuration page:

**Delete** : Check to delete the entry. It will be deleted immediately.

**ID** : Indicates the index of the entry. The range is from 1 to 65535.

**Desc** : Indicates this event, the string length is from 0 to 127, default is a null string.

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

**none**: No SNMP log is created, no SNMP trap is sent.

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

**snmptrap**: Send SNMP trap when the event is triggered.

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

**Community** : Specify the community when trap is sent, the string length is from 0 to 127, default is "public".

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

#### Buttons:

**Add New Entry** – Click to add a new entry.

**Apply** – Click to save changes.

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

## 2-5.2 Network

### 2-5.2.1 Limit Control

This page lets you configure the Port Security Limit Control. You can use the Port Security feature to restrict input to an interface by limiting and identifying MAC addresses.

#### Web Interface

To configure Port Security Limit Control in the web interface:

1. Select Configuration, Security, Network, Limit Control.
2. Select "Enabled" in the Mode of System Configuration.
3. Check Aging Enabled.
4. Set Aging Period (default is 3600 seconds).

To configure Port Configuration of Limit Control in the web interface:

1. Select "Enabled" in the Mode of Port Configuration.
2. Specify the maximum number of MAC addresses in the Limit of Port Configuration.
3. Set Action (Trap, Shutdown, or Trap & Shutdown)
4. Click Apply.

**Figure 2-5.2.1: Port Security Limit Control Configuration page**

The screenshot displays the 'Port Security Limit Control Configuration' page. The left sidebar shows a navigation menu with 'Limit Control' selected under the 'Network' section. The main content area is divided into two sections: 'System Configuration' and 'Port Configuration'.

**System Configuration:**

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

**Port Configuration Table:**

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

**Parameter descriptions:****System Configuration**

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

**Aging Enabled :** If checked, secured MAC addresses are subject to aging as discussed under Aging Period .

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

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

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

**Port Configuration**

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

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

**Limit :** The maximum number of MAC addresses that can be secured on this port. This number cannot exceed 1024. If the limit is exceeded, the corresponding action is taken.

The switch is "born" with a total number of MAC addresses from which all ports draw whenever a new MAC address is seen on a Port Security-enabled port. Since all ports draw from the same pool, it may happen that a configured maximum cannot be granted, if the remaining ports have already used all available MAC addresses.

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

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

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

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

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

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

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

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

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

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

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

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

**Sticky :** If the running config has sticky MAC address, then these MAC addresses are automatically changed to static mac address on MAC table.

**Clear :** Click the button to clear the static MAC addresses added by sticky function.

### **Buttons:**

**Refresh:** You can click to refresh the page immediately. Note that non-committed changes will be lost.

**Apply** – Click to save changes.

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

### 2-5.2.2 NAS

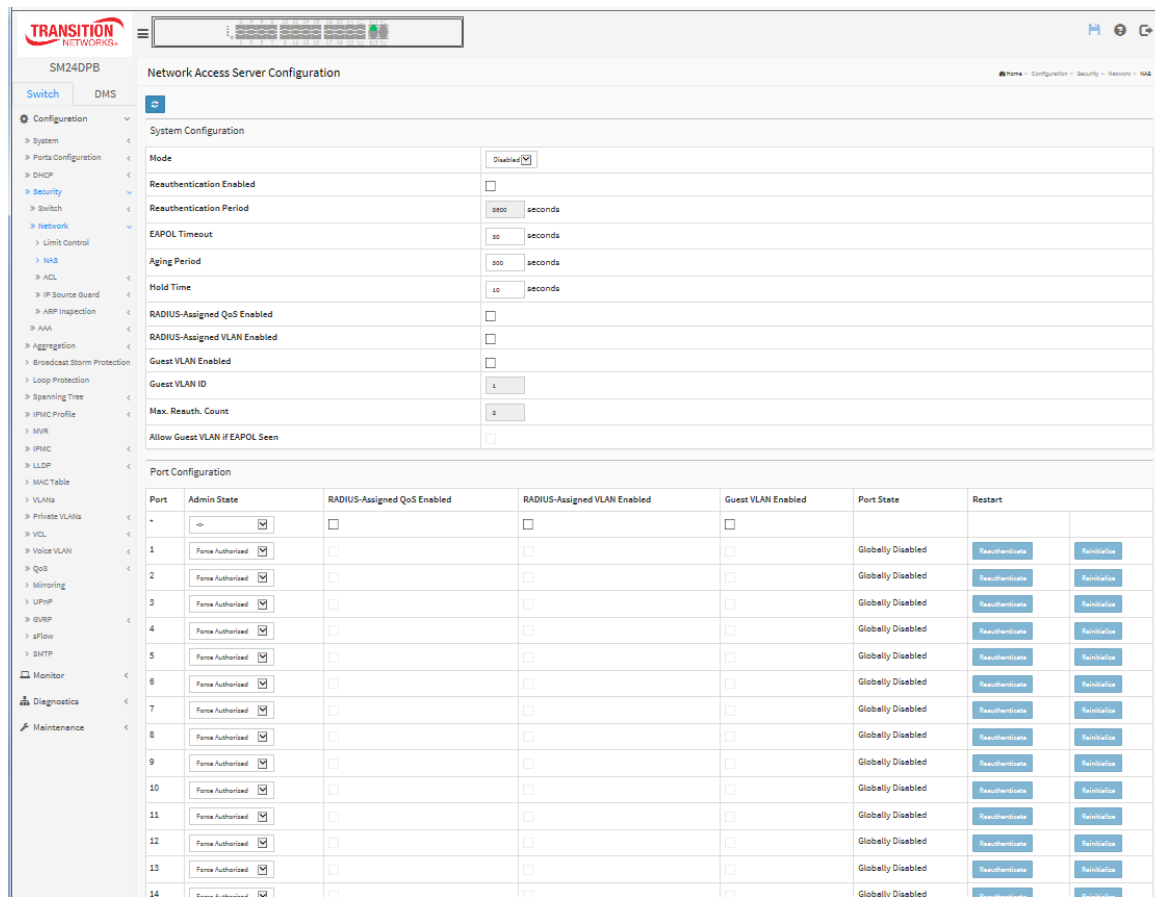
This page lets you configure switch NAS parameters. A NAS server can be employed to connect users to a variety of resources including Internet access, conference calls, printing documents on shared printers, or by simply logging on to the Internet. See IETF [RFC 2881](https://www.rfc-editor.org/rfc/rfc2881) for more information.

#### Web Interface

To configure a Network Access Server in the web interface:

1. Select Configuration, Security, Network, NAS.
2. Select "Enabled" in the Mode of Network Access Server Configuration.
3. Check Reauthentication Enabled.
4. Set Reauthentication Period (default is 3600 seconds).
5. Set EAPOL Timeout (default is 30 seconds).
6. Set Aging Period (default is 300 seconds).
7. Set Hold Time (default is 10 seconds).
8. Check RADIUS-Assigned QoS Enabled.
9. Check RADIUS-Assigned VLAN Enabled.
10. Check Guest VLAN Enabled.
11. Specify Guest VLAN ID.
12. Specify Max. Reauth. Count.
13. Check Allow Guest VLAN if EAPOL Seen.
14. Click Apply.

**Figure 2-5.2.2: NAS Configuration page**





**Parameter descriptions:**

**Mode :** Indicates if NAS 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.

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

- **Single 802.1X**
- **Multi 802.1X**
- **MAC-Based Auth.**

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

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

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

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

- **Single 802.1X**
- **Multi 802.1X**
- **MAC-Based Auth.**

If a client is denied access - either because the RADIUS server denies the client access or because the RADIUS server request times out (according to the timeout specified on the **Configuration > Security > AAA** page) - the client is put on hold in the Unauthorized state. The hold timer does not count during an on-going authentication.

In MAC-based Auth. mode, the switch will ignore new frames coming from the client during the hold time.

The Hold Time can be set to a number between 10 and 1000000 seconds.

**RADIUS-Assigned QoS Enabled :** RADIUS-assigned QoS provides a means to centrally control the traffic class to which traffic coming from a successfully authenticated supplicant is assigned on the switch. The RADIUS server must be configured to transmit special RADIUS attributes to take advantage of this feature (see RADIUS-Assigned QoS Enabled below for a detailed description)

The "RADIUS-Assigned QoS Enabled" checkbox provides a quick way to globally enable/disable RADIUS-server assigned QoS Class functionality. When checked, the individual ports' ditto setting determine whether RADIUS-assigned QoS Class is enabled on that port. When unchecked, RADIUS-server assigned QoS Class is disabled on all ports.

**RADIUS-Assigned VLAN Enabled :** RADIUS-assigned VLAN provides a means to centrally control the VLAN on which a successfully authenticated supplicant is placed on the switch. Incoming traffic will be classified to and switched on the RADIUS-assigned VLAN. The RADIUS server must be configured to transmit special RADIUS attributes to take advantage of this feature (see RADIUS-Assigned VLAN Enabled below for a detailed description).

The "RADIUS-Assigned VLAN Enabled" checkbox provides a quick way to globally enable/disable RADIUS-server assigned VLAN functionality. When checked, the individual ports' ditto setting determine whether RADIUS-assigned VLAN is enabled on that port. When unchecked, RADIUS-server assigned VLAN is disabled on all ports.

**Guest VLAN Enabled :** A Guest VLAN is a special VLAN - typically with limited network access - on which 802.1X-unaware clients are placed after a network administrator-defined timeout. The switch follows a set of rules for entering and leaving the Guest VLAN as listed below.

The "Guest VLAN Enabled" checkbox provides a quick way to globally enable/disable Guest VLAN functionality. When checked, the individual ports' ditto setting determines whether the port can be moved into Guest VLAN. When unchecked, the ability to move to the Guest VLAN is disabled on all ports.

**Guest VLAN ID :** This is the value that a port's Port VLAN ID is set to if a port is moved into the Guest VLAN. It is only changeable if the Guest VLAN option is globally enabled.

Valid values are in the range [1; 4095].

**Max. Reauth. Count :** The number of times the switch transmits an EAPOL Request Identity frame without response before considering entering the Guest VLAN is adjusted with this setting. The value can only be changed if the Guest VLAN option is globally enabled. Valid values are in the range [1; 255].

**Allow Guest VLAN if EAPOL Seen :** The switch remembers if an EAPOL frame has been received on the port for the life-time of the port. Once the switch considers whether to enter the Guest VLAN, it will first check if this option is enabled or disabled. If disabled (unchecked; default), the switch will only enter the Guest VLAN if an EAPOL frame has not been received on the port for the life-time of the port. If enabled (checked), the switch will consider entering the Guest VLAN even if an EAPOL frame has been received on the port for the life-time of the port. The value can only be changed if the Guest VLAN option is globally enabled.

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

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

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

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

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

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

or how many information exchange frames are needed for a particular method. The switch simply encapsulates the EAP part of the frame into the relevant type (EAPOL or RADIUS) and forwards it.

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



---

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

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

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

---

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

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

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

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

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

### **MAC-based Auth.:**

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

the MD5-Challenge authentication method, so the RADIUS server must be configured accordingly.

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

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

### **RADIUS-Assigned QoS Enabled :**

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

This option is only available for single-client modes, i.e.

- **Port-based 802.1X**

- **Single 802.1X**

RADIUS attributes used in identifying a QoS Class: Refer to the written documentation for a description of the RADIUS attributes needed in order to successfully identify a QoS Class. The User-Priority-Table attribute defined in RFC4675 forms the basis for identifying the QoS Class in an Access-Accept packet.

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

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

### **RADIUS-Assigned VLAN Enabled :**

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

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

This option is only available for single-client modes, i.e.

- **Port-based 802.1X**

- **Single 802.1X**

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

RADIUS attributes used in identifying a VLAN ID:

RFC2868 and RFC3580 form the basis for the attributes used in identifying a VLAN ID in an Access-Accept packet. The following criteria are used:

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

### **Guest VLAN Enabled :**

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

This option is only available for EAPOL-based modes, i.e.:

- **Port-based 802.1X**
- **Single 802.1X**
- **Multi 802.1X**

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

### **Guest VLAN Operation:**

When a Guest VLAN enabled port's link comes up, the switch starts transmitting EAPOL Request Identity frames. If the number of transmissions of such frames exceeds Max. Reauth. Count and no EAPOL frames have been received in the meanwhile, the switch considers entering the Guest VLAN. The interval between transmission of EAPOL Request Identity frames is configured with EAPOL Timeout. If Allow Guest VLAN if EAPOL Seen is enabled, the port will now be placed in the Guest VLAN. If disabled, the switch will first check its history to see if an EAPOL frame has previously been received on the port (this history is cleared if the port link goes down or the port's Admin State is changed), and if not, the port will be placed in the Guest VLAN. Otherwise it will not move to the Guest VLAN, but continue transmitting EAPOL Request Identity frames at the rate given by EAPOL Timeout.

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

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

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

**Globally Disabled:** NAS is globally disabled.

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

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

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

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

**Restart :** Two buttons are available for each row. The buttons are only enabled when authentication is globally enabled and the port's Admin State is in an EAPOL-based or MAC-based mode.

Clicking these buttons will not cause settings changed on the page to take effect.

**Reauthenticate:** Schedules a reauthentication whenever the quiet-period of the port runs out (EAPOL-based authentication). For MAC-based authentication, reauthentication will be attempted immediately.

The button only has effect for successfully authenticated clients on the port and will not cause the clients to get temporarily unauthorized.

**Reinitialize:** Forces a reinitialization of the clients on the port and thereby a reauthentication immediately. The clients will transfer to the unauthorized state while the reauthentication is in progress.

### **Buttons:**

**Apply** – Click to save changes.

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

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

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

Recovery: Click the Previous button and disable Spanning Tree at Switch > Configuration > Spanning Tree > CIST Port.

### 2-5.2.3 ACL

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

#### 2-5.2.3.1 Ports

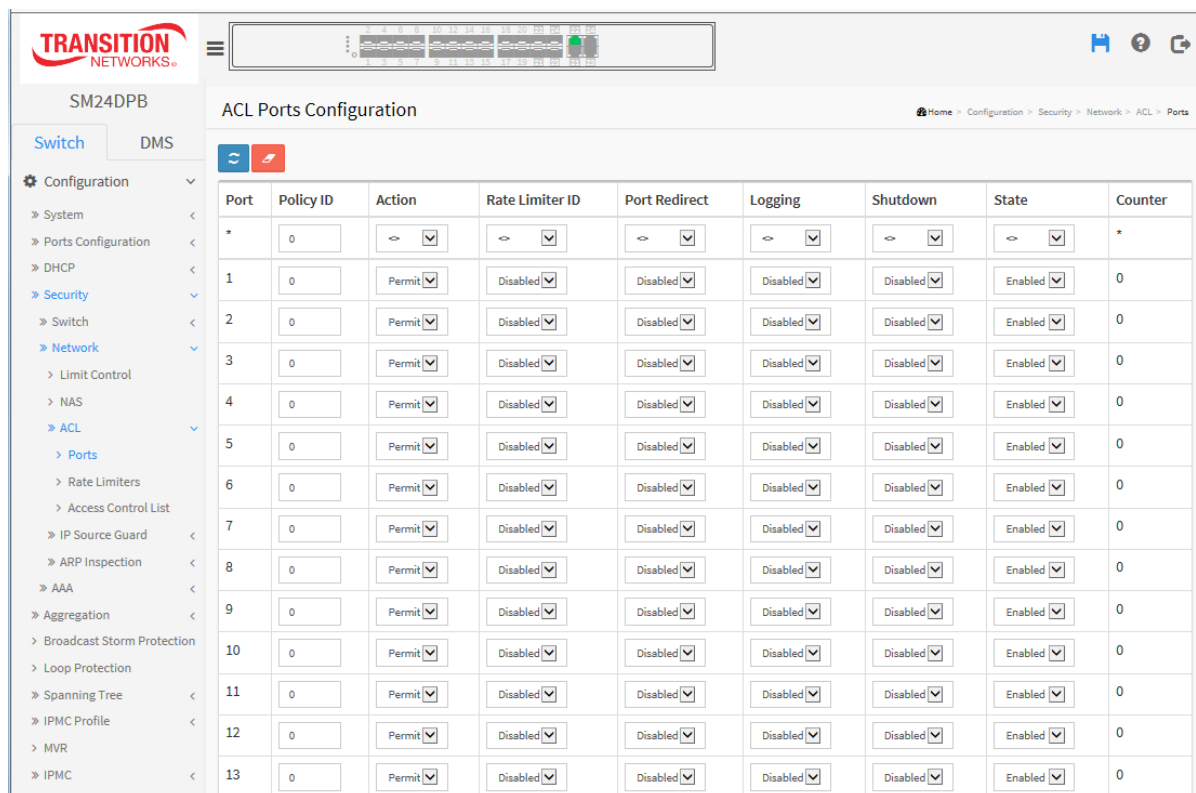
This page lets you configure the ACL parameters (ACE) of each switch port. These parameters will affect frames received on a port unless the frame matches a specific ACE

#### Web Interface

To configure the ACL Ports Configuration in the web interface:

1. Click Configuration, Security, Network, ACL, Ports.
2. Specify parameter values for port ACL settings.
3. Click the Apply button to save the settings.
4. To cancel the settings, click the Reset button to revert to previously saved values.
5. After you complete configure, you can see the Port Counters. Click Refresh to update the counter or Clear the information.

**Figure 2-5.2.3.1: ACL Ports Configuration page**



#### Parameter descriptions:

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

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

value is 1.

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

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

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

**Mirror :** Specify the mirror operation of this port. The allowed values are:

**Enabled:** Frames received on the port are mirrored.

**Disabled:** Frames received on the port are not mirrored.

The default value is "Disabled".

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

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

**Disabled:** Frames received on the port are not logged.

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

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

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

**Disabled:** Port shut down is disabled.

The default value is "Disabled".

**State :** Specify the port state of this port. The allowed values are:

**Enabled:** To reopen ports by changing the volatile port configuration of the ACL user module.

**Disabled:** To close ports by changing the volatile port configuration of the ACL user module.

The default value is "Enabled"

**Counter :** Counts the number of frames that match this ACE.

## Buttons

**Apply** – Click to save changes.

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

**Refresh, Clear** : Click to refresh the ACL Port Configuration or clear them manually.



### 2-5.2.3.2 Rate Limiters

This page lets you configure the switch's ACL Rate Limiter parameters.

#### Web Interface

To configure ACL Rate Limiter in the web interface:

1. Click Configuration, Security, Network, ACL, Rate Limiter.
2. Enter the Rate field in the range of 0 - 3276700 pps.
3. Click the Apply button to save the settings.
4. To cancel the settings click the Reset button to revert to previously saved values.

**Figure 2-5.2.3.2: ACL Rate Limiter Configuration page**

Rate Limiter ID	Rate (pps)
*	1
1	1
2	1
3	1
4	1
5	1
6	1
7	1
8	1
9	1
10	1
11	1
12	1
13	1
14	1
15	1
16	1

#### Parameter descriptions:

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

**Rate** The rate range is 0-131071 pps (packets per second).

#### Buttons

**Apply** – Click to save changes.

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


### 2-5.2.3.3 Access Control List

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

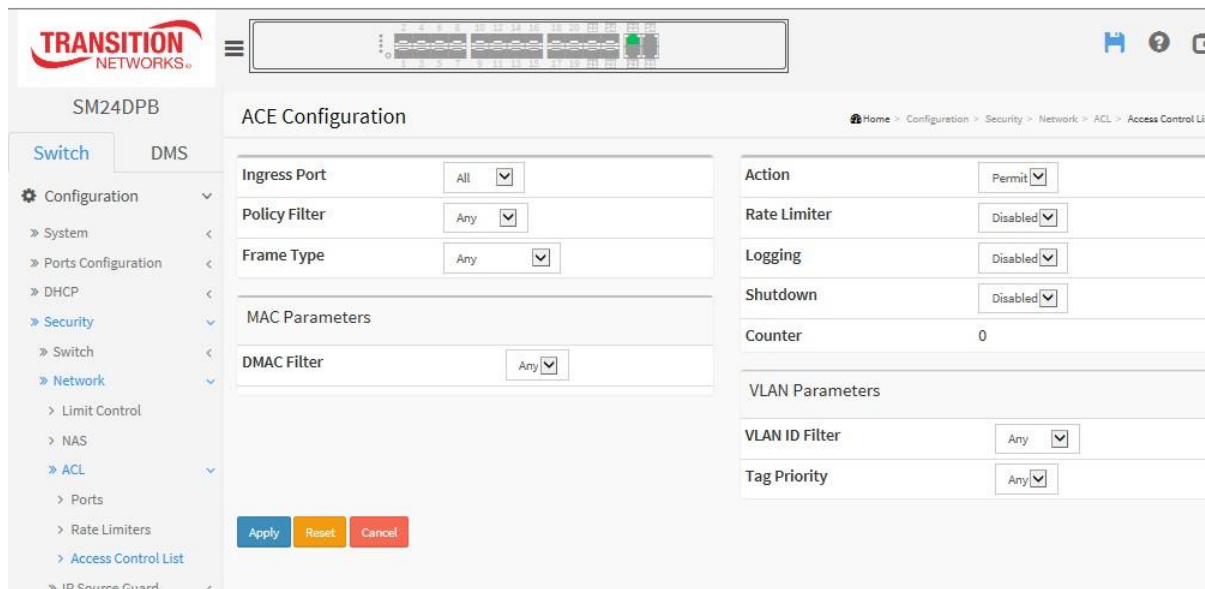
This page shows the Access Control List (ACL), which is made up of the ACEs defined on this switch. Each row describes the ACE that is defined. The maximum number of ACEs is 256 on each switch. Click on the lowest plus sign to add a new ACE to the list. The reserved ACEs used for internal protocol, cannot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

#### Web Interface

To configure Access Control List in the web interface:

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

**Figure 2-5.2.3.3: Access Control List (ACE Configuration) page**



The screenshot shows the 'ACE Configuration' page for a switch named 'SM24DPB'. The breadcrumb trail is 'Home > Configuration > Security > Network > ACL > Access Control List'. The page is split into two main columns. The left column contains 'ACE Parameters' with the following fields: 'Ingress Port' (dropdown: All), 'Policy Filter' (dropdown: Any), 'Frame Type' (dropdown: Any), 'MAC Parameters' (empty), and 'DMAC Filter' (dropdown: Any). Below these are 'Apply', 'Reset', and 'Cancel' buttons. The right column contains 'Action' (dropdown: Permit), 'Rate Limiter' (dropdown: Disabled), 'Logging' (dropdown: Disabled), 'Shutdown' (dropdown: Disabled), and 'Counter' (value: 0). Below these are 'VLAN Parameters' with 'VLAN ID Filter' (dropdown: Any) and 'Tag Priority' (dropdown: Any).

#### Parameter descriptions:

**Ingress Port :** Indicates the ingress port of the ACE. Possible values are:

**Any:** The ACE will match any ingress port.

**Policy:** The ACE will match ingress ports with a specific policy.

**Port:** The ACE will match a specific ingress port.

**Policy / Bitmask :** Indicates the policy number and bitmask of the ACE.

**Frame Type :** Indicates the frame type of the ACE. Possible values are:

**Any:** The ACE will match any frame type.

**EType:** The ACE will match Ethernet Type frames. Note that an Ethernet Type based ACE will not get matched by IP and ARP frames.

**ARP:** The ACE will match ARP/RARP frames.

**IPv4:** The ACE will match all IPv4 frames.

**IPv4/ICMP:** The ACE will match IPv4 frames with ICMP protocol.

**IPv4/UDP:** The ACE will match IPv4 frames with UDP protocol.

**IPv4/TCP:** The ACE will match IPv4 frames with TCP protocol.

**IPv4/Other:** The ACE will match IPv4 frames, which are not ICMP/UDP/TCP.

**IPv6:** The ACE will match all IPv6 standard frames.

**Action :** Indicates the forwarding action of the ACE.

**Permit:** Frames matching the ACE may be forwarded and learned.

**Deny:** Frames matching the ACE are dropped.

**Filter:** Frames matching the ACE are filtered.

**Rate Limiter :** Indicates the rate limiter number of the ACE. The allowed range is 1 to 16. When Disabled is displayed, the rate limiter operation is disabled.

**Port Copy :** Indicates the port copy operation of the ACE. Frames matching the ACE are copied to the port number. The allowed values are Disabled or a specific port number. When Disabled is displayed, the port copy operation is disabled.

**Mirror :** Specify the mirror operation of this port. The allowed values are:

**Enabled:** Frames received on the port are mirrored.

**Disabled:** Frames received on the port are not mirrored.

The default value is "Disabled".

**Logging :** Indicates the logging operation of the ACE. Possible values are:

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

**Disabled:** Frames matching the ACE are not logged.

Please note that the System Log memory size and logging rate is limited.

**Shutdown :** Indicates the port shut down operation of the ACE. Possible values are:

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

**Disabled:** Port shut down is disabled for the ACE.

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

## Modification Buttons

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



: Inserts a new ACE before the current row.



: Edits the ACE row.



: Moves the ACE up the list.



: Moves the ACE down the list.



: Deletes the ACE.



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

### MAC Parameters:

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

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

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

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

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

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

**MC**: Frame must be multicast.

**BC**: Frame must be broadcast.

**UC**: Frame must be unicast.

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

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

### VLAN Parameters:

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

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

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

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

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

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

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

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

**ARP:** Frame must have ARP opcode set to ARP.

**RARP:** Frame must have RARP opcode set to RARP.

**Other:** Frame has unknown ARP/RARP Opcode flag.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

**SIP BitMask :** When "Specific" is selected for the source IPv6 filter, you can enter a specific SIPv6 mask. The field only supported last 32 bits for IPv6 address. Notice the usage of bitmask, if the binary bit value is "0", it means this bit is "don't-care". The real matched pattern is [sipv6\_address & sipv6\_bitmask] (last 32 bits). For example, if the SIPv6 address is 2001::3 and the SIPv6 bitmask is 0xFFFFFFF0 (bit 0 is "don't-care" bit), then SIPv6 address 2001::2 and 2001::3 are applied to this rule.

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

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

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

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

#### **ICMP Parameters:**

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

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

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

**Value :** When "Specific" is selected for the ICMP filter, you can enter a specific ICMP value. The

allowed range is 0 to 255. A frame that hits this ACE matches this ICMP value.

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

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

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

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

### TCP/UDP Parameters

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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



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

**TCP PSH :** Specify the TCP "Push Function" (PSH) value for this ACE.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

**Ethernet Type Value** : When "Specific" is selected for the EtherType filter, you can enter a specific EtherType value. The allowed range is 0x600 to 0xFFFF but excluding 0x800(IPv4), 0x806(ARP) and 0x86DD(IPv6). A frame that hits this ACE matches this EtherType value.

## Buttons

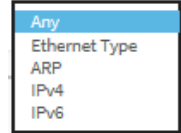
**Apply** – Click to save changes.

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

**Cancel:** Click to return to the previous page.

**Access Control List Configuration page example:**

The example below shows an instance of each Frame Type (Any, EType, ARP, IPv4, and IPv6).



SM24DPB

Access Control List Configuration

Home > Configuration > Security > Network > ACL > Access Control List

Auto-refresh  [Refresh] [Delete] [Add]

Ingress Port	Policy / Bitmask	Frame Type	Action	Rate Limiter	Port Redirect	Counter	
All	Any	EType	Permit	Disabled	Disabled	0	[+][⊖][⊕][⊗]
All	Any	ARP	Permit	Disabled	Disabled	296	[+][⊖][⊕][⊗]
All	Any	IPv4	Permit	Disabled	Disabled	809	[+][⊖][⊕][⊗]
All	Any	IPv6	Deny	1	Port 2	0	[+][⊖][⊕][⊗]
All	Any	Any	Permit	Disabled	Disabled	0	[+][⊖][⊕][⊗]
							[+]

## 2-5.2.4 IP Source Guard

This page lets you configure the IP Source Guard detail parameters of the switch. You can use the IP Source Guard configure to enable or disable with the Port of the switch.

### 2-5.2.4.1 Configuration

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

#### Web Interface

To configure an IP Source Guard Configuration in the web interface:

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

**Figure 2-5.2.4. 1: IP Source Guard Configuration page**

The screenshot shows the web interface for configuring IP Source Guard on a switch. The main heading is "IP Source Guard Configuration". At the top, there is a "Mode" dropdown menu currently set to "Disabled". Below this is a button labeled "Translate dynamic to static". The main configuration area is titled "Port Mode Configuration" and contains a table with three columns: "Port", "Mode", and "Max Dynamic Clients".

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

#### Parameter descriptions:

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

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

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

## Buttons

**Apply:** Click to save changes.

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

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

### 2-5.2.4.2 Static Table

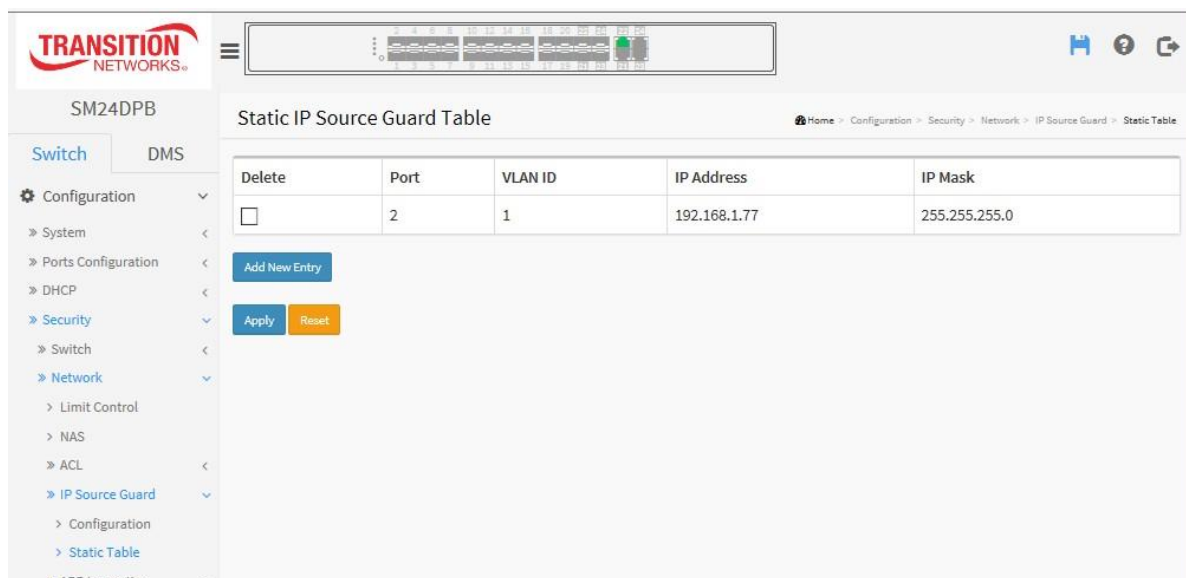
This page lets you configure the Static IP Source Guard Table parameters of the switch. You can use the Static IP Source Guard Table configure to manage the entries.

#### Web Interface

To configure a Static IP Source Guard Table Configuration in the web interface:

1. Click Configuration, Security, Network, IP Source Guard, Static Table.
2. Click “Add New Entry”.
3. Specify the Port, VLAN ID, IP Address, and IP Mask parameters.
4. Click Apply.

**Figure 2-4.2.5.2: The Static IP Source Guard Table**



#### Parameter descriptions:

**Delete** : Check to delete the entry. It will be deleted immediately.

**Port** : The logical port for the settings.

**VLAN ID** : The VLAN ID (VID) for the settings.

**IP Address** : Allowed Source IP address.

**MAC address** : Allowed Source MAC address.

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

#### Buttons:

**Apply** – Click to save changes.

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

## 2-5.2.5 ARP Inspection

This page lets you configure the ARP Inspection parameters of the switch. You can use the ARP Inspection configuration to manage the ARP table.

### 2-5.2.5.1 Configuration

This page lets you configure ARP Inspection setting including Mode (Enabled and Disabled) and Port (Enabled and Disabled).

#### Web Interface

To configure an ARP Inspection Configuration in the web interface:

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

**Figure 2-4.2.6.1: ARP Inspection Configuration page**

The screenshot displays the ARP Inspection Configuration page. At the top, the 'Mode' is set to 'Disabled'. Below this is a 'Translate dynamic to static' button. The main section is 'Port Mode Configuration', which contains a table with the following data:

Port	Mode	Check VLAN	Log Type
*	< >	< >	< >
1	Disabled	Disabled	None
2	Disabled	Disabled	None
3	Disabled	Disabled	None
4	Disabled	Disabled	None
5	Disabled	Disabled	None
6	Disabled	Disabled	None

#### Parameter descriptions:

**Mode of ARP Inspection Configuration :** Enable the Global ARP Inspection or disable the Global ARP Inspection.

**Port Mode Configuration :** Specify ARP Inspection is to be enabled on which ports. Only when both Global Mode and Port Mode on a given port are enabled, ARP Inspection is enabled on this given port. Possible modes are:

**Enabled:** Enable ARP Inspection operation.

**Disabled:** Disable ARP Inspection operation.

**Check VLAN:** If you want to inspect the VLAN configuration, you must enable the setting of "Check VLAN". The default setting of "Check VLAN" is disabled. When the setting of "Check VLAN" is disabled, the log type of ARP Inspection will refer to the port setting. And the setting of "Check VLAN" is enabled, the log type of ARP Inspection will refer to the VLAN setting. Possible setting of "Check VLAN" are:

**Enabled:** Enable check VLAN operation.

**Disabled:** Disable check VLAN operation.

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

**None:** Log nothing.

**Deny:** Log denied entries.

**Permit:** Log permitted entries.

**ALL:** Log all entries.

### **Buttons:**

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

**Apply** – Click to save changes.

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

### 2-5.2.5.2 VLAN Mode Configuration

Each page shows up to 9999 entries from the VLAN table, default being 20, selected through the "entries per page" input field. When first visited, the web page will show the first 20 entries from the beginning of the VLAN Table. The first displayed will be the one with the lowest VLAN ID found in the VLAN Table.

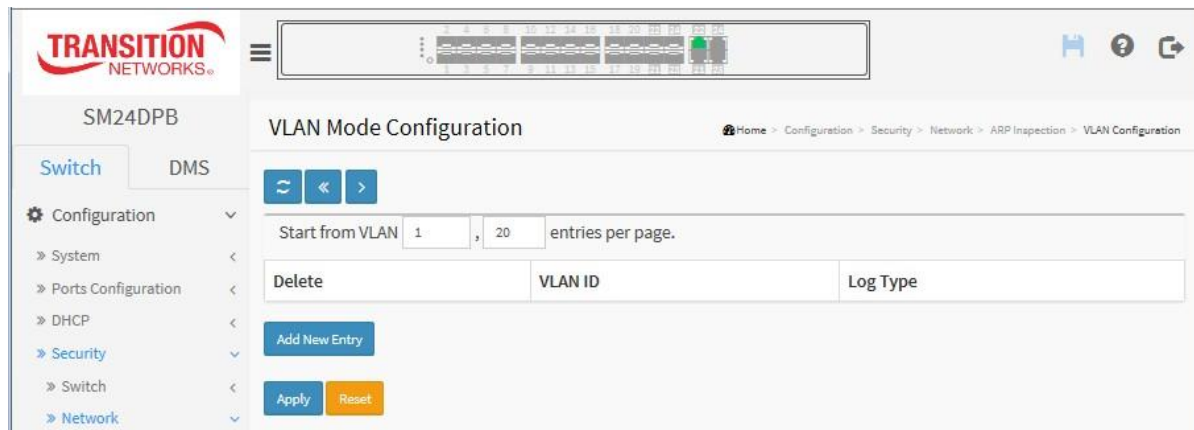
The "VLAN" input fields let you select the starting point in the VLAN Table. Clicking the > button will update the displayed table starting from that or the closest next VLAN Table match. The << will use the next entry of the currently displayed VLAN entry as a basis for the next lookup. When the end is reached the warning message is shown in the displayed table. Use the Reset button to start over.

#### Web Interface

To configure a VLAN Mode Configuration in the web interface:

1. Click "Add New Entry".
2. Specify the VLAN ID, Log Type.
3. Click Apply.

**Figure 2-4.2.6.2: VLAN Mode Configuration page**



#### Parameter descriptions:

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

Possible Log Types are:

- None:** Log nothing.
- Deny:** Log denied entries.
- Permit:** Log permitted entries.
- ALL:** Log all entries.

#### Buttons

**Add New Entry:** Click to add a new VLAN to the ARP Inspection VLAN table.

**Apply:** Click to save changes.

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



### 2-5.2.5.3 Static Table

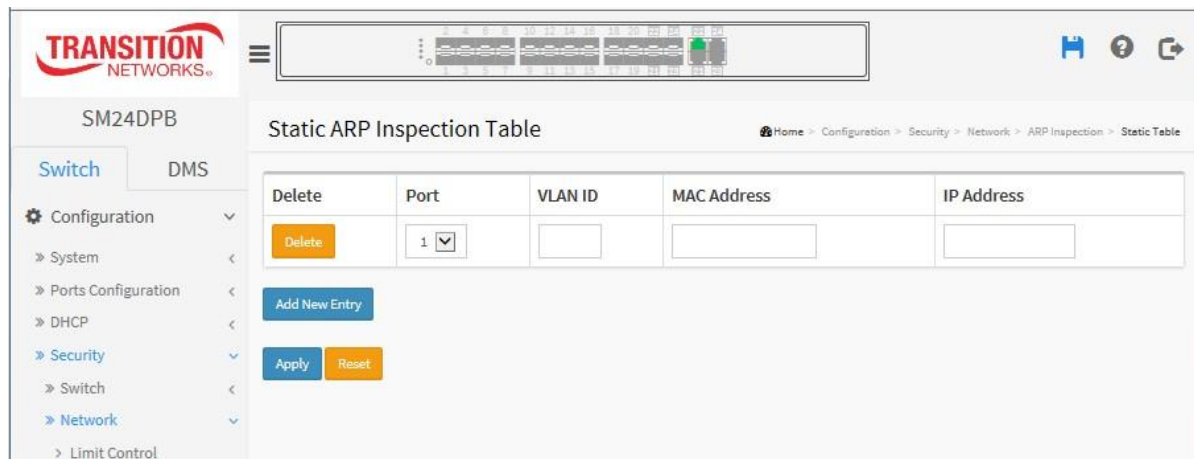
This page lets you configure the Static ARP Inspection Table parameters. You can use the Static ARP Inspection Table configure to manage the ARP entries.

#### Web Interface

To configure a Static ARP Inspection Table Configuration in the web interface:

1. Click “Add New Entry”.
2. Specify the Port, VLAN ID, MAC Address, and IP Address.
3. Click Apply.

**Figure 2-4.2.6.3: Static ARP Inspection Table**



#### Parameter descriptions:

**Delete** : Check to delete the entry. It will be deleted immediately.

**Port** : The logical port for the settings.

**VLAN ID** : The vlan id for the settings.

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

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

**Add New Entry** : Click to add a new entry to the Static ARP Inspection table. Specify the Port, VLAN ID, MAC address, and IP address for the new entry. Click Apply.

#### Buttons:

**Apply** – Click to save changes.

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

### 2-5.2.5.4 Dynamic Table

Entries in the Dynamic ARP Inspection Table are shown on this page. The Dynamic ARP Inspection Table contains up to 1024 entries, and is sorted first by port, then by VLAN ID, then by MAC address, and then by IP address.

#### Navigating the ARP Inspection Table

Each page shows up to 99 entries from the Dynamic ARP Inspection table, default being 20, selected through the "entries per page" input field. When first visited, the web page will show the first 20 entries from the beginning of the Dynamic ARP Inspection Table.

The "Start from port address", "VLAN", "MAC address" and "IP address" input fields let you select the starting point in the Dynamic ARP Inspection Table. Clicking the > button will update the displayed table starting from that or the closest next Dynamic ARP Inspection Table match. In addition, the two input fields will - upon a > button click - assume the value of the first displayed entry, allowing for continuous refresh with the same start address.

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

#### Web Interface

To configure a Dynamic ARP Inspection Table Configuration in the web interface:

1. Click Configuration, Security, Network, ARP Inspection, Dynamic Table.
2. Select Start from, VLAN, MAC address, IP address , and entries per page.
3. View the entries in the table if any exist. If none exist, the table displays "No more entries".

**Figure 2-5.2.5.4: Static ARP Inspection Table**

Delete	Port	VLAN ID	MAC Address	IP Address
<input type="checkbox"/>	1	10	11-22-33-44-55-66	192.168.1.77
<input type="checkbox"/>	2	20	11-22-33-44-55-77	192.168.1.77

**Figure 2-5.2.5.4: Dynamic ARP Inspection Table**

#### Parameter descriptions:

#### **ARP Inspection Table Columns**

**Port :** Switch Port Number for which the entries are displayed.

**VLAN ID :** VLAN-ID in which the ARP traffic is permitted.

**MAC Address :** User MAC address of the entry.

**IP Address :** User IP address of the entry.

**Translate to static :** Select the checkbox to translate the entry to a static entry.

**Buttons:**

**Apply** – Click to save changes.

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

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

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

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

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

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

### 2-5.3 AAA

This page lets you configure a AAA (Authentication, Authorization, Accounting) server to provide access control to your network. The AAA server can be a TACACS+ or RADIUS server to create and manage objects that contain settings for using AAA servers. Up to 5 servers are supported.

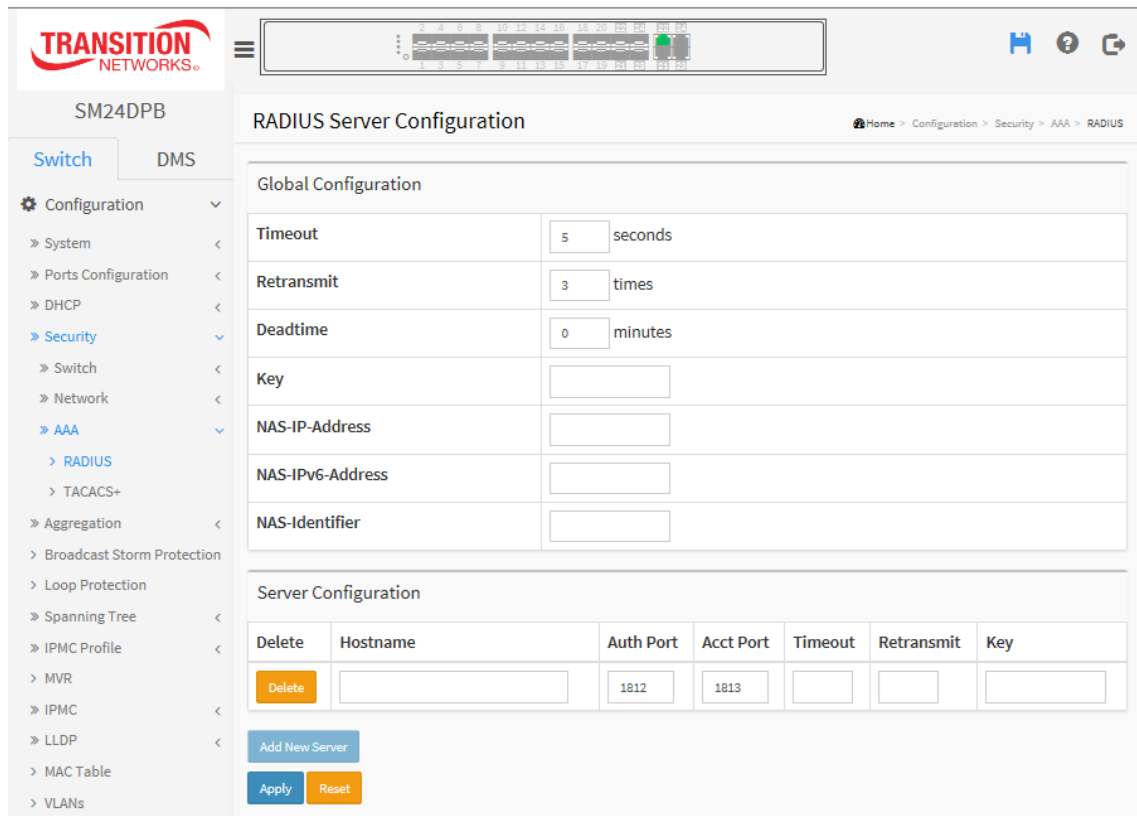
#### 2-5.3.1 RADIUS

##### Web Interface

To configure a common configuration of AAA and RADIUS in the web interface:

1. Click Configuration, Security, AAA, RADIUS.
2. Enter the Global Configuration parameters.
3. Click the Add New Server button.
4. Enter the Server Configuration parameters.
5. Click the Apply button when done to save the settings.

**Figure 2-4.3.2: RADIUS Server Configuration page**



##### Parameter descriptions:

##### **Global Configuration**

These settings are common for all of the RADIUS servers.

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

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

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

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

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

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

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

**Server Configuration**: The table has one row for each RADIUS server and these 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.

**Acct Port** : The UDP port to use on the RADIUS server for accounting.

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

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

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

**Add New Server** : Click to add a new RADIUS server. An empty row is added to the table, and the RADIUS server can be configured as needed. Up to 5 servers are supported. The **Reset** button can be used to undo the addition of the new server.

## Buttons

**Apply**: Click to save changes.

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

## 2-5.3.2 TACACS+

### Web Interface

To configure a common Configuration of AAA and TACACS+ in the web interface:

1. Click Configuration, Security, AAA, TACACS+.
2. Enter the Global Configuration parameter.
3. Click the Add New Server button.
4. Enter the Server Configuration parameters.
5. Click the Apply button when done to save the settings.

**Figure 2-5.3.2: TACACS+ Server Configuration page**

The screenshot displays the TACACS+ Server Configuration page in a web interface. The left sidebar shows a navigation tree with 'Security' expanded to 'AAA' and 'TACACS+' selected. The main content area is titled 'TACACS+ Server Configuration' and includes a breadcrumb trail: Home > Configuration > Security > AAA > TACACS+. The page is divided into two sections: 'Global Configuration' and 'Server Configuration'. The 'Global Configuration' section contains three rows of configuration parameters: 'Timeout' set to 5 seconds, 'Deadtime' set to 0 minutes, and a 'Key' field. The 'Server Configuration' section features a table with one row for a server. The table has columns for 'Delete', 'Hostname', 'Port', 'Timeout', and 'Key'. The 'Delete' column contains a 'Delete' button, and the 'Port' column contains the value '49'. Below the table are three buttons: 'Add New Server', 'Apply', and 'Reset'.

#### Parameter descriptions:

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

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

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

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

**Server Configuration:** The table has one row for each TACACS+ server and a number of columns, which are:

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

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

**Port :** The TCP port to use on the TACACS+ server for authentication.

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

value.

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

**Add New Server :** Click to add a new TACACS+ server. An empty row is added to the table, and the TACACS+ server can be configured as needed. Up to 5 servers are supported. The **Reset** button can be used to undo the addition of the new server.

## Buttons

**Apply:** Click to save changes.

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

## 2-6 Aggregation

Aggregation is used to configure the settings of Link Aggregation. You can bundle more than one port with the same speed, full duplex and the same MAC to be a single logical port, thus the logical port aggregates the bandwidth of these ports. This means you can apply your current Ethernet equipment's to build the bandwidth aggregation. For example, if there are three Fast Ethernet ports aggregated in a logical port, then this logical port has bandwidth three times as high as a single Fast Ethernet port has. **Note** that LACP and Static aggregation can not both be enabled on the same ports.

### 2-6.1 Static

Ports using Static Trunk as their trunk method can choose their unique Static Group ID to form a logic “trunked port”. The benefit of using Static Trunk method is that a port can immediately become a member of a trunk group without any handshaking with its peer port. This is also a disadvantage because the peer ports of your static trunk group may not know that they should be aggregate together to form a “logic trunked port”. Using Static Trunk on both end of a link is strongly recommended. Please also note that low speed links will stay in “not ready” state when using static trunk to aggregate with high speed links.

#### Web Interface

To configure the Trunk Aggregation Hash mode and Aggregation Group in the web interface:

1. Click Configuration, Aggregation, and Static.
2. Set the Hash Code Contributors parameters.
3. Enter Aggregation Group Configuration parameters.
4. Click Apply to save the settings.
5. To cancel the setting click the Reset button to revert to previously saved values.

**Figure 2-5.1: Aggregation Mode Configuration**

The screenshot shows the 'Aggregation Mode Configuration' page in the SM24DPB web interface. The left sidebar contains a navigation menu with 'Configuration' expanded to 'Aggregation' > 'Static'. The main content area is titled 'Aggregation Mode Configuration' and includes a breadcrumb trail: Home > Configuration > Aggregation > Static.

**Hash Code Contributors**

Source MAC Address	<input checked="" type="checkbox"/>
Destination MAC Address	<input type="checkbox"/>
IP Address	<input checked="" type="checkbox"/>
TCP/UDP Port Number	<input checked="" type="checkbox"/>

**Aggregation Group Configuration**

Group ID	Port Members																							
	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24
Normal	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
1	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
2	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
3	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
4	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
5	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
6	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
7	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>



**Parameter descriptions:****Hash Code Contributors**

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

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

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

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

**Aggregation Group Configuration**

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

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

**Buttons**

**Apply** – Click to save changes.

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

## 2-6.2 LACP

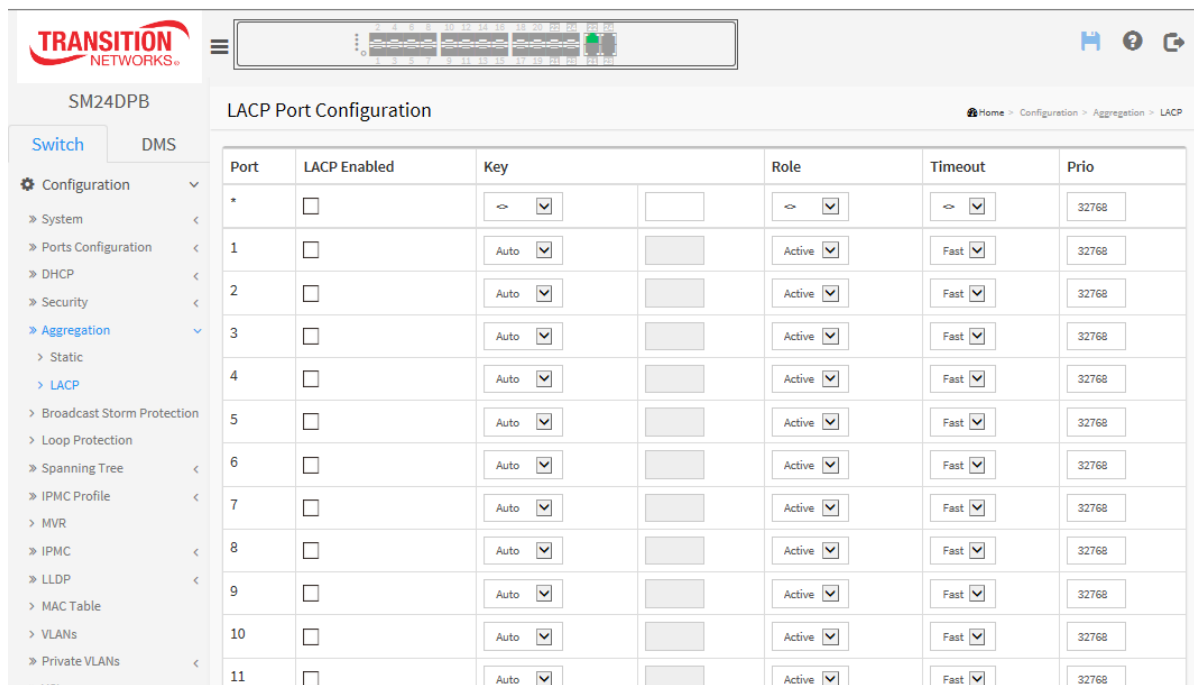
This page lets you view and configure the current LACP port configurations. An LACP trunk group with more than one ready member-port is a “real trunked” group. An LACP trunk group with only one or less than one ready member-ports is not a “real trunked” group. **Note** that LACP and Static aggregation can not both be enabled on the same ports.

### Web Interface

To configure the Trunk Aggregation LACP parameters in the web interface:

1. Click Configuration, Aggregation, LACP.
2. Enable or disable the LACP for the switch ports.
3. Select the Key parameter with Auto or Specific (default is Auto).
4. Select the Role (Active or Passive).The default is Active.
5. Select the Timeout and Priority parameters.
6. Click Apply to save the settings.
7. To cancel the settings click the Reset button to revert to previously saved values.

**Figure 2-5.2: LACP Port Configuration page**



### Parameter descriptions:

**Port :** The switch port number.

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

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

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

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

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

### **Buttons**

**Apply** – Click to save changes.

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

## 2-7 Broadcast Storm Protection

The Broadcast Storm Protection page lets you view and configure the BCS parameters.

### Web Interface

To configure the Trunk Aggregation LACP parameters in the web interface:

1. Click Configuration, BCS Protection.
2. Enable the desired ports.
3. For each enabled port, set the Action, PPS, and Timer parameters.
4. When done click the Apply button.
5. View the Status column for status changes.

**Figure 2-7.1: Broadcast Storm Protection page**

The screenshot shows the 'Broadcast Storm Protection' configuration page for SM24DPB. The page includes a navigation menu on the left and a main table with columns: Port, Enable, Action, PPS, Timer(seconds), and Status. The table lists ports from 1 to 13, with port 13 partially visible. Ports 2, 3, 4, 5, 6, 7, and 8 are enabled. The 'Status' column shows 'Activated' for ports 6, 7, and 8.

Port	Enable	Action	PPS	Timer(seconds)	Status
*	<input type="checkbox"/>	<	0	300	
1	<input type="checkbox"/>	Shutdown Port	0	300	
2	<input checked="" type="checkbox"/>	Shutdown Port	1	300	
3	<input checked="" type="checkbox"/>	Shutdown Port and Log	2	300	
4	<input checked="" type="checkbox"/>	Shutdown Port and Log	10	300	
5	<input checked="" type="checkbox"/>	Shutdown Port	20	300	
6	<input checked="" type="checkbox"/>	Shutdown Port and Log	100	120	Activated
7	<input checked="" type="checkbox"/>	Shutdown Port and Log	0	600	Activated
8	<input checked="" type="checkbox"/>	Log Only	0	300	Activated
9	<input type="checkbox"/>	Shutdown Port	0	300	
10	<input type="checkbox"/>	Shutdown Port	0	300	
11	<input type="checkbox"/>	Shutdown Port	0	300	
12	<input type="checkbox"/>	Shutdown Port	0	300	
13	<input type="checkbox"/>	Shutdown Port	0	300	

### Parameter descriptions:

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

**Enable** : Controls whether Broadcast Storm Protection is enabled on this switch port.

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

**PPS**: Broadcast Storm Protection threshold. Valid values are 0 to 1000000 packets.

**Timer(seconds)**: The period (in seconds) for which a port will be kept disabled in the event of a broadcast storm is detected (and the port action shuts down the port). Valid values are 0 to 65535 seconds.

**Status**: The current broadcast storm protection status of the port. "Activated" means the port already reached the BCS threshold setting.

## **Buttons**

**Apply:** Click to apply changes.

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

## 2-8 Loop Protection

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

### Web Interface

To configure the Loop Protection parameters in the web interface:

1. Click Configuration, Loop Protection.
2. Set the Global Configuration parameters.
3. Enable or disable Loop Protection for each port.
4. Set the Action and Tx Mode parameters for each port.
5. Click Apply to save the settings.
6. To cancel the settings click the Reset button. It will revert to previously saved values.

**Figure 2-7: Loop Protection Configuration page**

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

### Parameter descriptions:

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

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

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

will keep a port disabled (until next device restart).

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

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

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

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

**Buttons:**

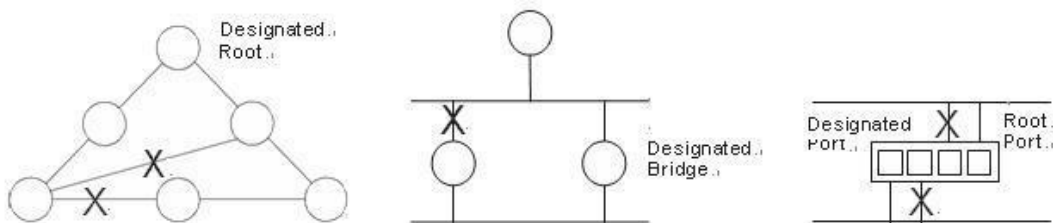
**Apply** – Click to save changes.

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

## 2-8 Spanning Tree

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



Once a stable network topology has been established, all bridges listen for Hello BPDUs (Bridge Protocol Data Units) transmitted from the Root Bridge. If a bridge does not get a Hello BPDU after a predefined interval (Maximum Age), the bridge assumes that the link to the Root Bridge is down. This bridge will then initiate negotiations with other bridges to reconfigure the network to reestablish a valid network topology.

### 2-8.1 Bridge Setting

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

#### **Web Interface**

To configure the Spanning Tree Bridge Settings parameters in the web interface:

1. Click Configuration, Spanning Tree, Bridge Settings.
2. Set the Basic Settings parameters.
3. Set the Advanced Settings parameters.
4. Click the Apply button to save the settings.
5. To cancel the settings click the Reset button. It will revert to previously saved values.



**Figure 2-8.1: STP Bridge Configuration page**

The screenshot displays the 'STP Bridge Configuration' page in the SM24DPB web interface. The page is organized into two main sections: 'Basic Settings' and 'Advanced Settings'. The 'Basic Settings' section contains six configuration items, each with a label, a value field, and a dropdown menu. The 'Advanced Settings' section contains four configuration items, each with a label and a checkbox or a value field. At the bottom of the page, there are 'Apply' and 'Reset' buttons. The left sidebar shows a navigation menu with 'Spanning Tree' expanded to 'Bridge Settings'. The top right corner shows a breadcrumb trail: 'Home > Configuration > Spanning Tree > Bridge Settings'.

Basic Settings	
Protocol Version	MSTP
Bridge Priority	32768
Forward Delay	15
Max Age	20
Maximum Hop Count	20
Transmit Hold Count	6

Advanced Settings	
Edge Port BPDU Filtering	<input type="checkbox"/>
Edge Port BPDU Guard	<input type="checkbox"/>
Port Error Recovery	<input type="checkbox"/>
Port Error Recovery Timeout	

**Parameter descriptions:****Basic Settings**

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

**Bridge Priority :** Controls the bridge priority. Lower numeric values have better priority. The bridge priority plus the MSTI instance number, concatenated with the 6-byte MAC address of the switch forms a Bridge Identifier. For MSTP operation, this is the priority of the CIST. Otherwise, this is the priority of the STP/RSTP bridge.

**Forward Delay :** The delay used by STP Bridges to transit Root and Designated Ports to Forwarding (used in STP compatible mode). Valid values are 4 - 30 seconds.

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

**Maximum Hop Count :** This defines the initial value of remaining Hops for MSTI information generated at the boundary of an MSTI region. It defines how many bridges a root bridge can distribute its BPDU information to. Valid values are 6 - 40 hops.

**Transmit Hold Count :** The number of BPDU's a bridge port can send per second. When exceeded, transmission of the next BPDU will be delayed. Valid values are in the range 1 to 10 BPDU's per second.

## **Advanced Settings**

**Edge Port BPDU Filtering** : Control whether a port explicitly configured as Edge will transmit and receive BPDUs.

**Edge Port BPDU Guard** : Control whether a port explicitly configured as Edge will disable itself upon reception of a BPDU. The port will enter the error-disabled state, and will be removed from the active topology.

**Port Error Recovery** : Control whether a port in the error-disabled state automatically will be enabled after a certain time. If recovery is not enabled, ports have to be disabled and re-enabled for normal STP operation. The condition is also cleared by a system reboot.

**Port Error Recovery Timeout** : The time to pass before a port in the error-disabled state can be enabled. Valid values are 30 - 86400 seconds (24 hours).

## **Buttons**

**Apply** : Click to save changes.

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

## 2-8.2 MSTI Mapping

When you implement an Spanning Tree protocol on the switch that the bridge instance.

The CIST is not available for explicit mapping, as it will receive the VLANs not explicitly mapped; you must set the list of VLANs mapped to the MSTI. The VLANs must be separated with a comma and/or a 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).

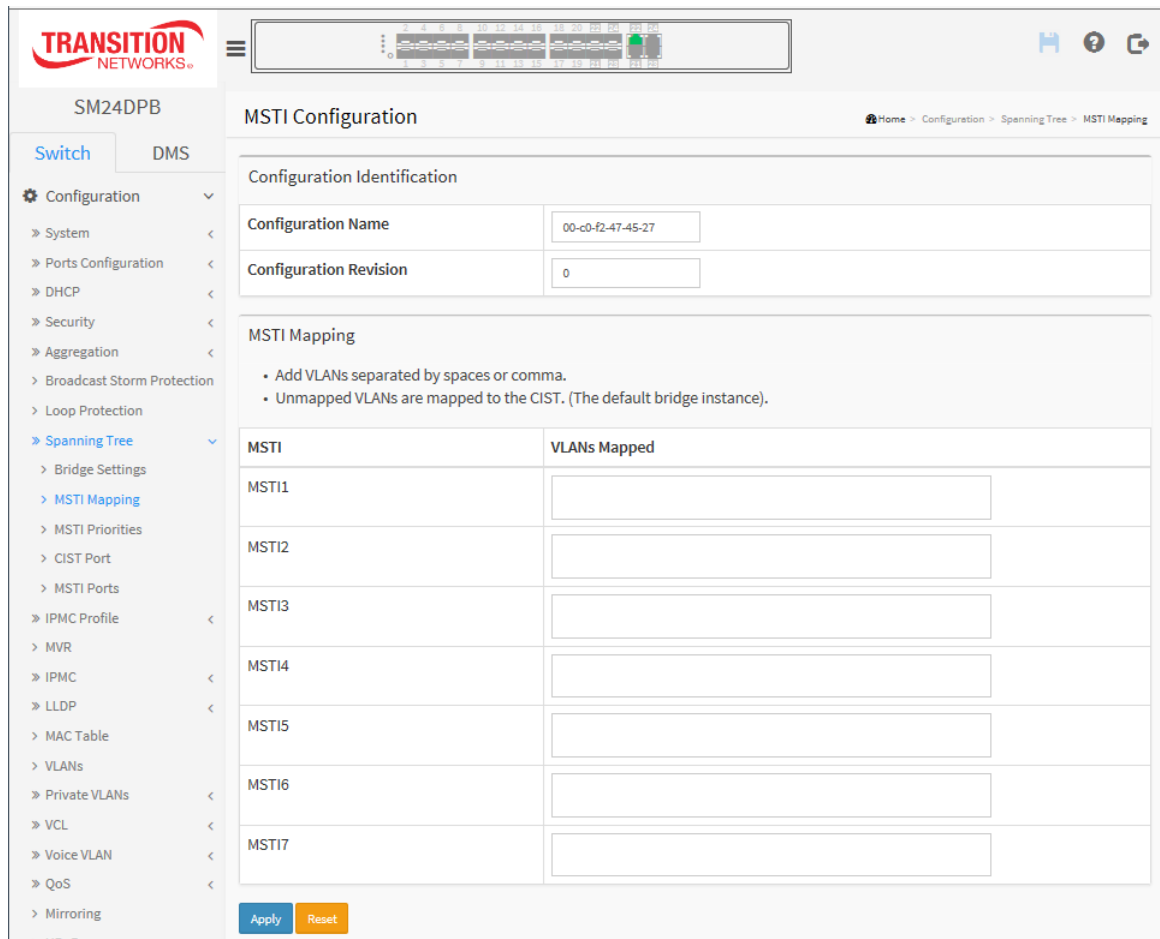
This page lets you view and configure current STP MSTI bridge instance priority parameters.

### Web Interface

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

1. Click Configuration, Spanning Tree, MSTI Mapping.
2. Specify the Configuration Identification parameters.
3. Specify the VLANs Mapped blank field(s).
4. Click Apply to save the settings.
5. To cancel the settings click the Reset button. It will revert to previously saved values.

**Figure 2-9.2: MSTI Configuration page**



***Parameter descriptions:*****Configuration Identification**

**Configuration Name:** The name identifying the VLAN to MSTI mapping. Bridges must share the name and revision (see below), as well as the VLAN-to-MSTI mapping configuration in order to share spanning trees for MSTI's (Intra-region). The name is at most 32 characters.

**Configuration Revision:** The revision of the MSTI configuration named above. This must be an integer between 0 and 65535.

***MSTI Mapping:*** Add VLANs separated by spaces or comma. Unmapped VLANs are mapped to the CIST. (The default bridge instance).

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

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

**Buttons**

**Apply :** Click to save changes.

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

### 2-8.3 MSTI Priorities

When you implement a Spanning Tree protocol on the switch that the bridge instance. The CIST is the default instance which is always active. For controls the bridge priority. Lower numeric values have higher priority. The bridge priority plus the MSTI instance number, concatenated with the 6-byte MAC address of the switch forms a Bridge Identifier.

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

#### Web Interface

To configure the Spanning Tree MSTI Priorities parameters in the web interface:

1. Click Configuration, Spanning Tree, MSTI Priorities.
2. Set the Priority for each MSTI. The valid range is 0-61440. The default is 32768.
3. Click Apply to save the settings.
4. To cancel the settings, click the Reset button to revert to previously saved values.

**Figure 2-8.3: MSTI Configuration**

The screenshot shows the web interface for the SM24DPB switch. The main content area is titled "MSTI Configuration" and contains a table for "MSTI Priority Configuration". The table has two columns: "MSTI" and "Priority". The rows are as follows:

MSTI	Priority
*	<input type="text" value="24576"/>
CIST	<input type="text" value="24576"/>
MSTI1	<input type="text" value="32768"/>
MSTI2	<input type="text" value="32768"/>
MSTI3	<input type="text" value="32768"/>
MSTI4	<input type="text" value="32768"/>
MSTI5	<input type="text" value="32768"/>
MSTI6	<input type="text" value="32768"/>
MSTI7	<input type="text" value="32768"/>

Below the table are two buttons: "Apply" (blue) and "Reset" (orange). The left sidebar shows a navigation menu with "Spanning Tree" expanded to "MSTI Priorities".

**Parameter descriptions:**

**MSTI :** The bridge instance. The CIST is the default instance, which is always active.

**Priority :** Controls the bridge priority. Lower numeric values have better priority. The bridge priority plus the MSTI instance number, concatenated with the 6-byte MAC address of the switch forms a Bridge Identifier.

**Buttons**

**Apply :** Click to save changes.

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

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

## 2-8.4 CIST Ports

When you implement a Spanning Tree protocol on the switch that the bridge instance. You need to configure the CIST Ports. This page lets you view and configure the current STP CIST port parameters.

### Web Interface

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

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

**Figure 2-8.4: STP CIST Port Configuration**

The screenshot displays the 'STP CIST Port Configuration' page in the SM24DPB web interface. The left sidebar shows the navigation menu with 'Spanning Tree' > 'CIST Port' selected. The main content area is divided into two sections:

- CIST Aggregated Port Configuration:** A table with one row. The 'STP Enabled' checkbox is checked. 'Path Cost' is set to 'Auto'. 'Priority' is 128. 'Admin Edge' is set to 'Non-Edge'. 'Auto Edge' is checked. The 'Restricted' section has 'Role', 'TCN', and 'BPDU Guard' checkboxes, all of which are unchecked. 'Point-to-point' is set to 'Forced True'.
- CIST Normal Port Configuration:** A table with seven rows, numbered 1 through 7. Each row has 'STP Enabled' checked, 'Path Cost' set to 'Auto', 'Priority' set to 128, 'Admin Edge' set to 'Non-Edge', and 'Auto Edge' checked. The 'Restricted' section has 'Role', 'TCN', and 'BPDU Guard' checkboxes, all of which are unchecked. 'Point-to-point' is set to 'Auto'.

### Parameter descriptions:

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

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

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

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

**AdminEdge:** Controls whether the operEdge flag should start as set or cleared. (The initial operEdge state when a port is initialized.)

**AutoEdge:** Controls whether the bridge should enable automatic edge detection on the bridge port. This allows operEdge to be derived from whether BPDU's are received on the port or not.

**Restricted Role:** If enabled, causes the port not to be selected as Root Port for the CIST or any MSTI, even if it has the best spanning tree priority vector. Such a port will be selected as an Alternate Port after the Root Port has been selected. If set, it can cause lack of spanning tree connectivity. It can be set by a network administrator to prevent bridges external to a core region of the network influence the spanning tree active topology, possibly because those bridges are not under the full control of the administrator. This feature is also known as Root Guard.

**Restricted TCN:** If enabled, causes the port not to propagate received topology change notifications and topology changes to other ports. If set it can cause temporary loss of connectivity after changes in a spanning tree's active topology as a result of persistently incorrect learned station location information. It is set by a network administrator to prevent bridges external to a core region of the network, causing address flushing in that region, possibly because those bridges are not under the full control of the administrator or the physical link state of the attached LANs transits frequently.

**BPDU Guard:** If enabled, causes the port to disable itself upon receiving valid BPDU's. Contrary to the similar bridge setting, the port Edge status does not affect this setting. A port entering error-disabled state due to this setting is subject to the bridge Port Error Recovery setting as well.

**Point to Point:** Controls whether the port connects to a point-to-point LAN rather than to a shared medium. This can be automatically determined or forced either true or false. Transition to the forwarding state is faster for point-to-point LANs than for shared media.

## Buttons

**Apply :** Click to save changes.

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



## 2-8.5 MSTI Ports

This page lets you view and configure the current STP MSTI port parameters.

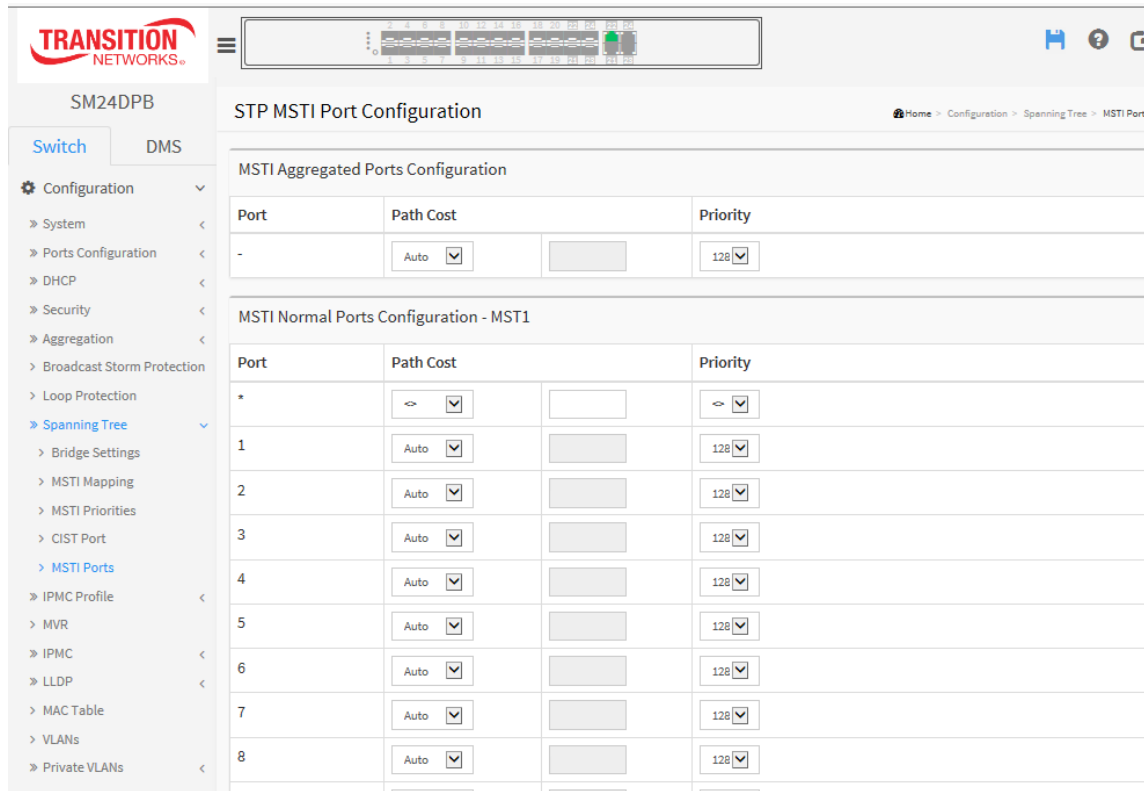
An MSTI port is a virtual port, which is instantiated separately for each active CIST (physical) port for each MSTI instance configured on and applicable to the port. The MSTI instance must be selected before displaying actual MSTI port configuration options. It contains MSTI port settings for physical and aggregated ports.

### Web Interface

To configure the Spanning Tree MSTI Port parameters in the web interface:

1. Click Configuration, Spanning Tree, MSTI Ports.
2. Select the MST1 or other MSTI Port.
3. Click **Get** to set the detail parameters of the MSTI Ports.
4. Set all MSTI Aggregated Ports Configuration parameters.
5. Set all MSTI Normal Ports Configuration parameters.
6. Click Apply to save the settings.
7. To cancel the settings click the Reset button. It will revert to previously saved values.

**Figure 2-8.5: STP CIST Port Configuration page**



### Parameter descriptions:

**Port:** The switch port number of the corresponding STP CIST (and MSTI) port.

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

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

### **Buttons**

**Apply** – Click to save changes.

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

## 2-9 IPMC Profile

This page provides IPMC Profile configuration parameters.

### 2-9.1 Profile Table

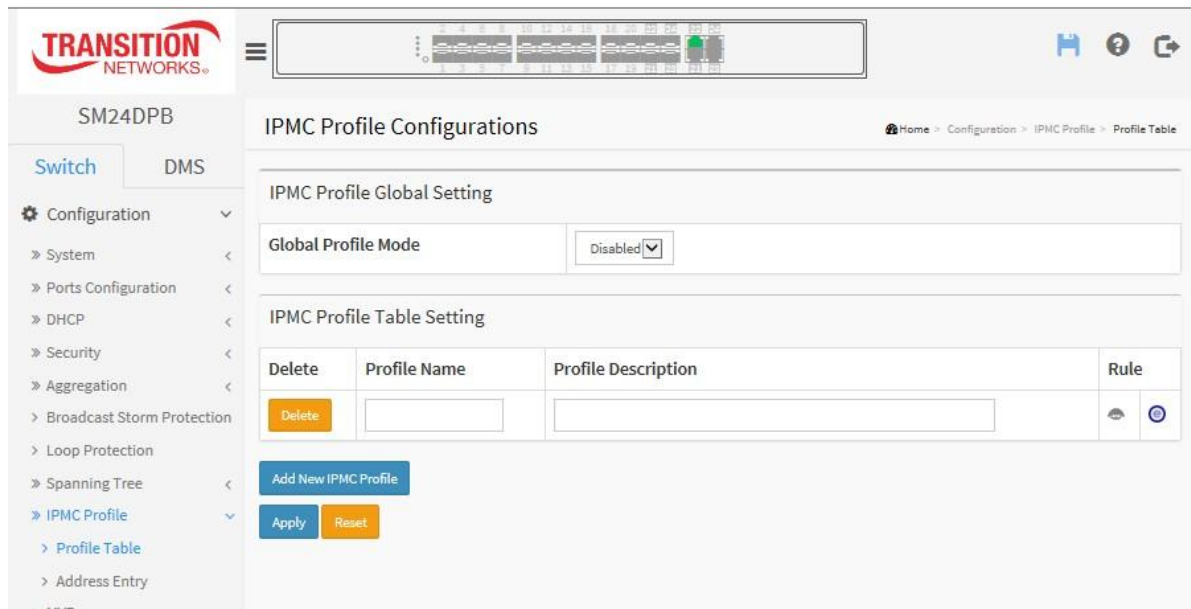
The IPMC profile is used to deploy the access control on IP multicast streams. It is allowed to create at maximum 64 Profiles with at maximum 128 corresponding rules for each.

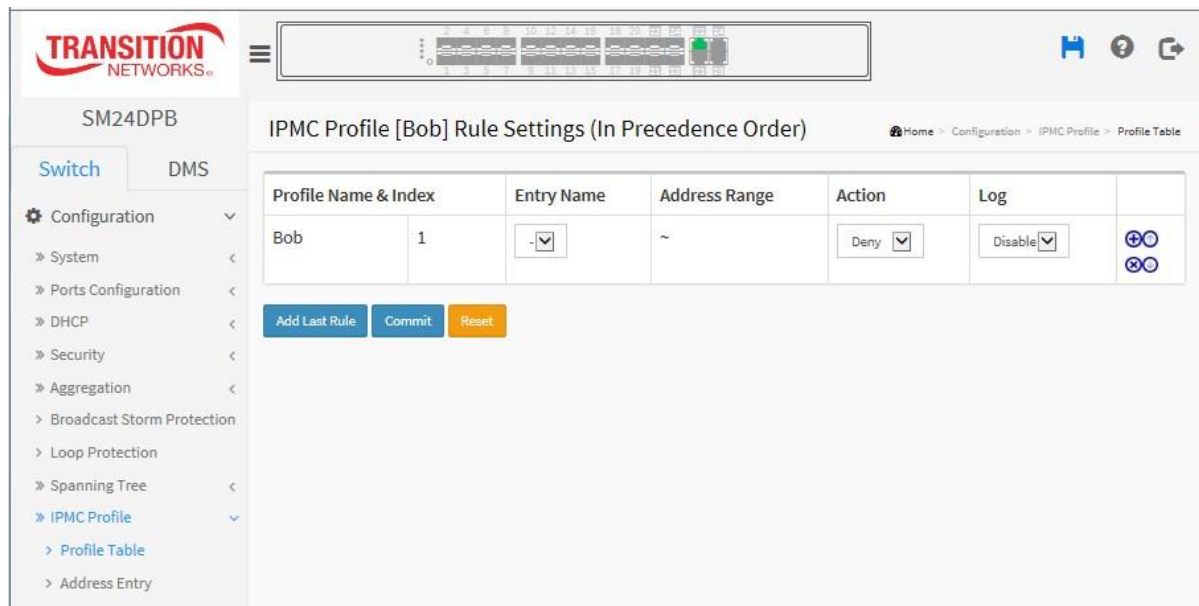
#### Web Interface

To configure the IPMC Profile Configuration in the web interface:

1. Click Configuration > IPMC Profile > Profile Table.
2. At the Global Profile Mode dropdown select Enabled.
3. In the IPMC Profile Table Setting section, click the Add New IPMC Profile button.
4. Enter a Profile Name and a Profile Description.
5. Click the Rule icon (🔗).
6. At the IPMC Profile [xxxx] Rule Settings page click the Add Last Rule button.
7. For the Profile Name & Index displayed, set the Entry Name, Address Range, Action, and Log parameters.
8. Click the Commit button.
9. Use the Edit (🔗) and List (🔗) buttons.

Figure 2-9.1: IPMC Profile Configuration page 1



**Figure 2-9.: IPMC Profile Configuration page 2****Parameter descriptions:**

**Port :** The switch port number of the corresponding STP CIST (and MSTI) port.

**Global 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.

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

**Profile Name :** The name used for indexing the profile table.

Each entry has the unique name which is composed of at maximum 16 alphabetic and numeric characters. At least one alphabet must be present.

**Profile Description :** Additional description, which is composed of at maximum 64 alphabetic and numeric characters, about the profile.

No blank or space characters are permitted as part of description. Use "\_" or "-" to separate the description sentence.

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



: List the rules associated with the designated profile.



: Edit the rules associated with the designated profile.

**Buttons**

**Add New IPMC Profile** – Click to add new IPMC profile. Specify the name and configure the new entry. Click Apply.

**Apply** – Click to save changes.

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

### 2-9.1.1 IPMC Profile Rule Settings Table

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

**Profile Name :** The name of the designated profile to be associated. This field is not editable.

**Entry Name :** The name used in specifying the address range used for this rule. Only the existing profile address entries will be chosen in the selected box. This field is not allowed to be selected as none ("-") while the Rule Settings Table is committed.

**Address Range :** The corresponding address range of the selected profile entry. This field is not editable and will be adjusted automatically according to the selected profile entry.

**Action :** Indicates the learning action upon receiving the Join/Report frame that has the group address matches the address range of the rule.

**Permit:** Group address matches the range specified in the rule will be learned.

**Deny:** Group address matches the range specified in the rule will be dropped.

**Log :** Indicates the logging preference upon receiving the Join/Report frame that has the group address matches the address range of the rule.


**Enable:** Corresponding information of the group address, that matches the range specified in the rule, will be logged.

**Disable:** Corresponding information of the group address, that matches the range specified in the rule, will not be logged.


### Rule Management Buttons

You can manage rules and the corresponding precedence order by using these buttons:

: Insert a new rule before the current entry of rule.

: Delete the current entry of rule.

: Moves the current entry of rule up in the list.

: Moves the current entry of rule down in the list.

### Buttons

**Add Last Rule** – Click to add a new rule in the end of the specific profile's rule list. Specify the address entry and configure the new entry. Click "Commit" when done.

**Commit** – Click to commit rule changes for the designated profile.

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

## 2-9.2 Address Entry

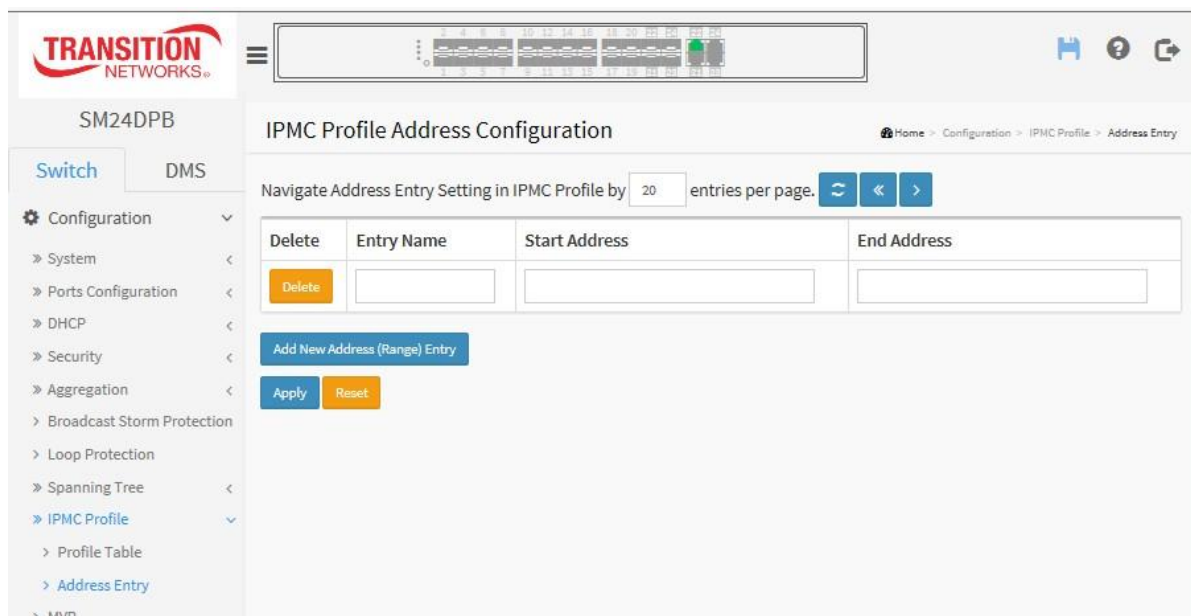
This page provides address range settings used in IPMC profile. The address entry is used to specify the address range that will be associated with IPMC Profile. You can create up to 128 address entries in the system.

### Web Interface

To configure the IPMC Profile Address Configuration in the web interface:

1. Click Configuration > IPMC Profile > Address Entry.
2. Click the Add New Address (Range) Entry button.
3. Enter the Entry Name, Start Address, and End Address parameters.
4. Click the Apply button.

**Figure 2-9.2: IPMC Profile Address Configuration page**



### Parameter descriptions:

**Delete** : Check to delete the entry.

The designated entry will be deleted during the next save.

**Entry Name** : The name used for indexing the address entry table.

Each entry has the unique name which is composed of at maximum 16 alphabetic and numeric characters. At least one alphabet must be present.

**Start Address** : The starting IPv4/IPv6 Multicast Group Address that will be used as an address range.

**End Address** : The ending IPv4/IPv6 Multicast Group Address that will be used as an address range.

### Buttons

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

**Apply** : Click to save changes.

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

<< : Updates the table starting from the first entry in the IPMC Profile Address Configuration.

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

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

## 2-10 MVR

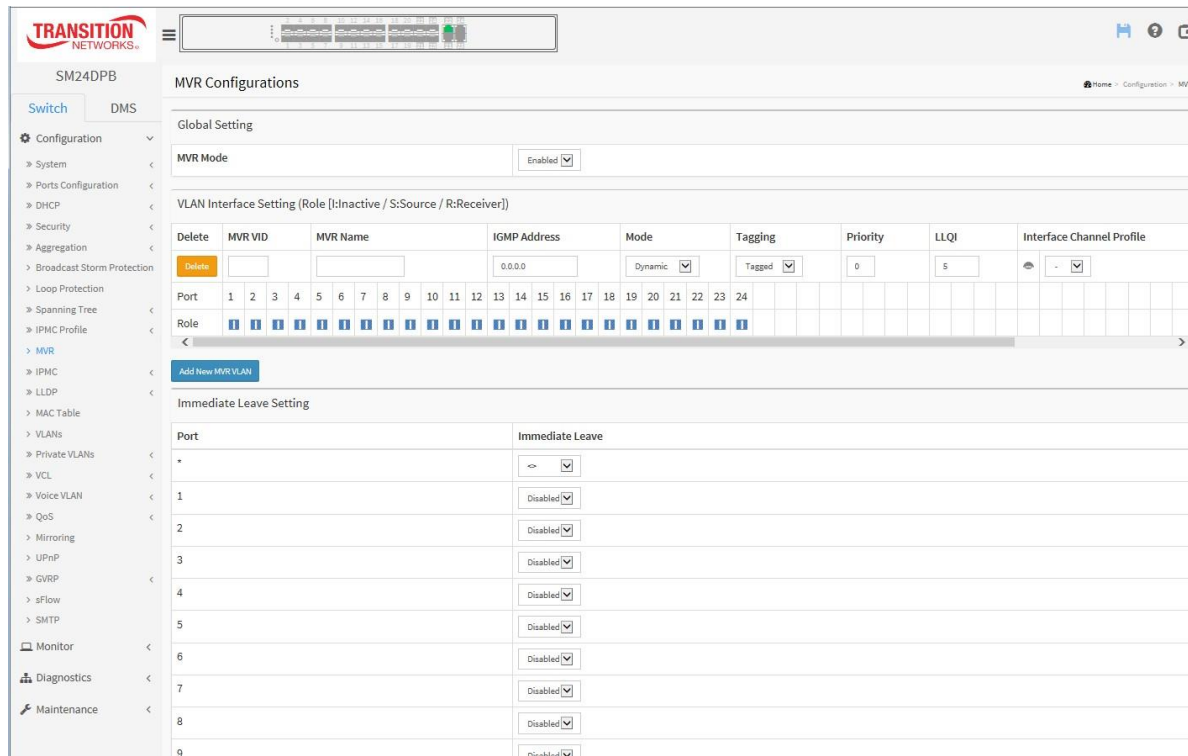
The MVR feature enables multicast traffic forwarding on the Multicast VLAN. In a multicast television application, a PC or a television with a set-top box can receive the multicast stream. Multiple set-top boxes or PCs can be connected to one subscriber port, which is a switch port configured as an MVR receiver port. When a subscriber selects a channel, the set-top box or PC sends an IGMP join message to the 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.

### Web Interface

To configure the MVR Configuration in the web interface:

1. Click Configuration, MVR.
2. Click the Add New MVR VLAN button.
3. At the MVR Mode dropdown select Enable.
4. Set all VLAN Interface Setting (Role) parameters.
5. Set the Immediate Leave Setting parameters.
6. Click Apply to save the settings.
7. To cancel the settings click the Reset button to revert to previously saved values.

Figure 2-10: MVR Configuration page 1



### Parameter descriptions:

**MVR Mode :** Enable/Disable the Global MVR. The Unregistered Flooding control depends on the current configuration in IGMP/MLD Snooping. It is suggested to enable Unregistered Flooding control when the MVR group table is full.

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



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

**MVR Name** : MVR Name is an optional attribute to indicate the name of the specific MVR VLAN. Maximum length of the MVR VLAN Name string is 32. MVR VLAN Name can only contain alphabets or numbers. When the optional MVR VLAN name is given, it should contain at least one alphabet. MVR VLAN name can be edited for the existing MVR VLAN entries or it can be added to the new entries.

**IGMP Address** : Define the IPv4 address as source address used in IP header for IGMP control frames. The default IGMP address is not set (0.0.0.0). When the IGMP address is not set, system uses IPv4 management address of the IP interface associated with this VLAN.

When the IPv4 management address is not set, system uses the first available IPv4 management address. Otherwise, system uses a pre-defined value. By default, this value will be 192.0.2.1.

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

**Tagging** : Specify whether the traversed IGMP/MLD control frames will be sent as Untagged or Tagged with MVR VID. The default is Tagged.

**Priority** : Specify how the traversed IGMP/MLD control frames will be sent in prioritized manner. The default Priority is 0.

**LLQI** : Define the maximum time to wait for IGMP/MLD report memberships on a receiver port before removing the port from multicast group membership. The value is in units of tenths of a seconds. The range is from 0 to 31744. The default LLQI is 5 tenths or one-half second.

**Interface Channel Setting** : When the MVR VLAN is created, click the Edit symbol to expand the corresponding multicast channel settings for the specific MVR VLAN. Summary about the Interface Channel Setting (of the MVR VLAN) will be shown besides the Edit symbol.

**Port** : The logical port for the settings.

**Port Role** : Configure an MVR port of the designated MVR VLAN as one of the following roles.

**Inactive:** The designated port does not participate MVR operations.

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

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

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

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

## Buttons

**Add New MVR VLAN:** Click to add new MVR VLAN. Specify the VID and configure the new entry. Click "Apply".

**Apply:** Click to save changes.

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

Figure 2-10: MVR Configuration page 2

The screenshot displays the MVR Configuration page for SM24DPB. The interface includes a navigation menu on the left with categories like Configuration, Monitor, Diagnostics, and Maintenance. The main content area is titled 'MVR Configurations' and is divided into several sections:

- Global Setting:** MVR Mode is set to 'Enabled'.
- VLAN Interface Setting (Role [I:Inactive / S:Source / R:Receiver]):** This section contains two VLAN configurations:
  - VLAN 1 (MvrCtg-1):** IGMP Address: 192.177.9.30; Mode: Compatible; Tagging: Untagged; Priority: 0; LLQI: S; Interface Channel Profile: Bob.
  - VLAN 2 (MvrCtg-2):** IGMP Address: 0.0.0.0; Mode: Dynamic; Tagging: Tagged; Priority: 0; LLQI: S; Interface Channel Profile: -.
- Port Role Matrix:** A grid showing roles for ports 1-24. For VLAN 1, ports 1-4 are Source (S), ports 5-12 are Inactive (I), and ports 13-24 are Receiver (R). For VLAN 2, all ports 1-24 are Inactive (I).
- Immediate Leave Setting:** A table for ports 1-5:

Port	Immediate Leave
*	Enabled
1	Disabled
2	Enabled
3	Enabled
4	Enabled
5	Enabled

## 2-11 IPMC

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

### 2-11.1 IGMP Snooping

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

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

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

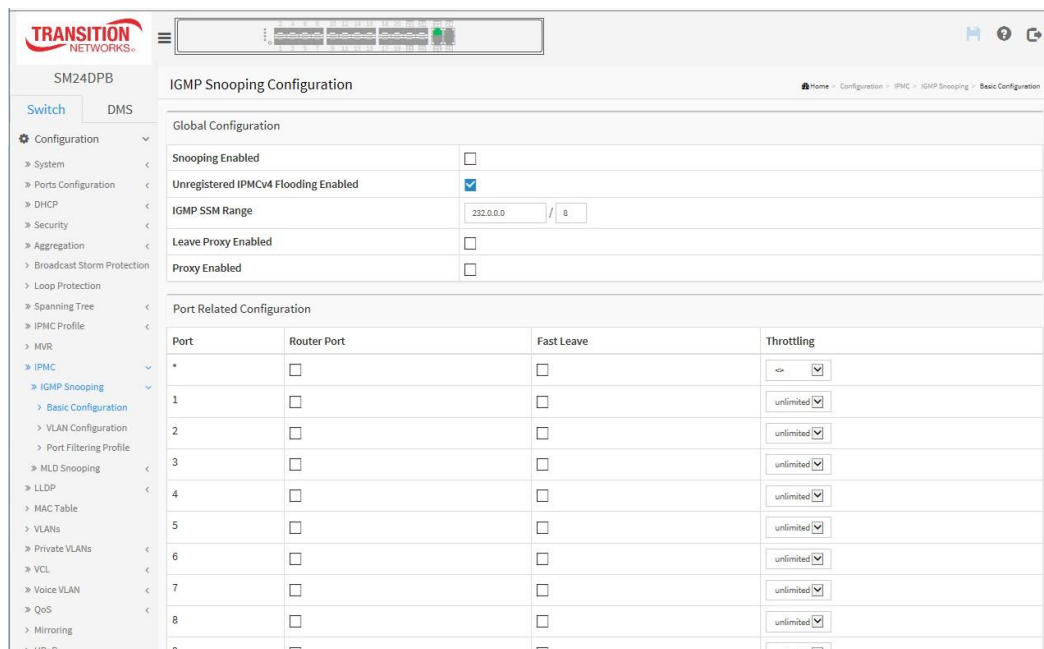
#### 2-11.1.1 Basic Configuration

This page lets you set basic IGMP snooping on the switch, which connects to a router closer to the root of the tree. This interface is the upstream interface. The router on the upstream interface must be running IGMP.

To configure IGMP Snooping parameters in the web interface:

1. Click Configuration, IPMC, IGMP Snooping, Basic Configuration.
2. Set the Global Configuration parameters.
3. Set the Port Related Configuration parameters.
4. Click Apply to save the settings.

**Figure 2-12.1.1: IGMP Snooping Configuration page**



**Parameter descriptions:****Global Configuration**

**Snooping Enabled :** Enable the Global IGMP Snooping.

**Unregistered IPMCv4 Flooding enabled :** Enable unregistered IPMCv4 traffic flooding.

**IGMP SSM Range :** SSM (Source-Specific Multicast) Range allows the SSM-aware hosts and routers run the SSM service model for the groups in the address range. Format: (IP address/ sub mask)

**Leave Proxy Enable:** Enable IGMP Leave Proxy. This feature can be used to avoid forwarding unnecessary leave messages to the router side.

**Proxy Enabled :** Enable IGMP Proxy. This feature can be used to avoid forwarding unnecessary join and leave messages to the router side.

**Port 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.

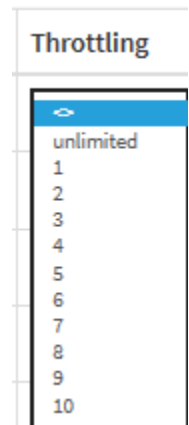
**Fast Leave :** Enable the fast leave on the port.

**Throttling :** Select the number of multicast groups to which a switch port can belong. The selections are unlimited and 1-10. The default is unlimited.

**Buttons**

**Apply:** Click to save changes.

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



### 2-11.1.2 VLAN Configuration

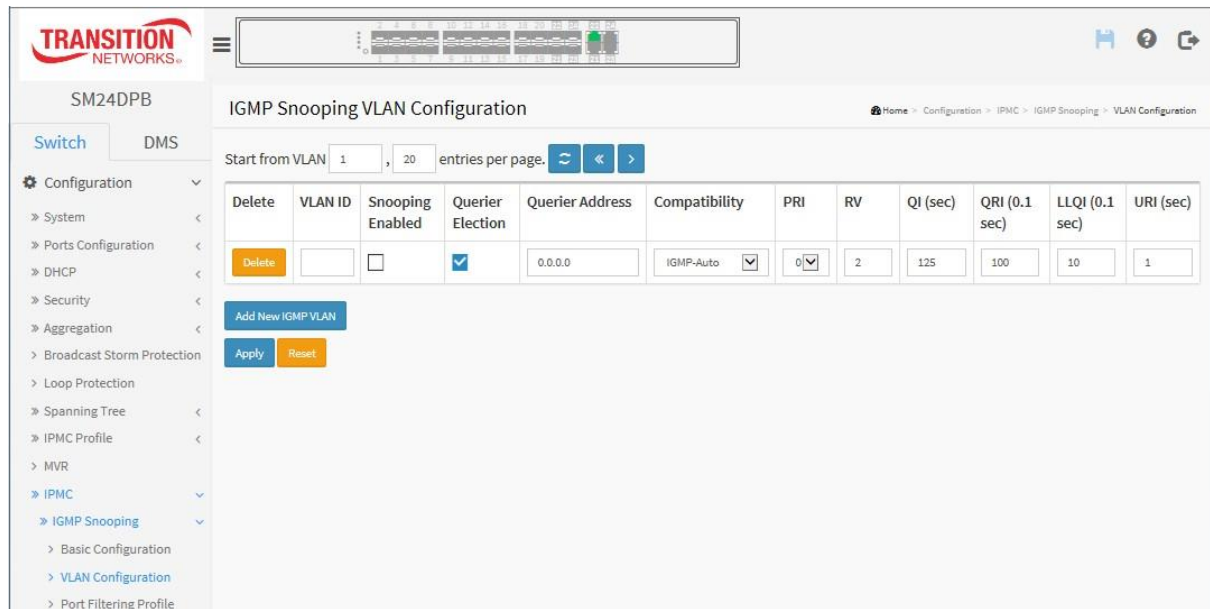
This section describes the VLAN configuration setting process integrated with the IGMP Snooping function. Each page shows up to 99 entries from the VLAN table, default being 20, selected through the "entries per page" input field. When first visited, the web page will show the first 20 entries from the 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 let you select the starting point in the VLAN Table. Clicking the > button will update the displayed table starting from that or the next closest VLAN Table match.

#### Web Interface

To configure the IGMP Snooping VLAN Configuration in the web interface:

1. Click Configuration, IPMC, IGMP Snooping, VLAN Configuration.
2. Click the Add New IGMP VLAN button.
3. Specify the IGMP Snooping VLAN Configuration parameters.
4. Click Apply to save the settings.
5. To cancel the setting, click the Reset button to revert to previously saved values.

**Figure 2-11.1.2: IGMP Snooping VLAN Configuration page**



#### Parameter descriptions:

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

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

**IGMP Snooping Enabled :** Enable the per-VLAN IGMP Snooping. Only up to 32 VLANs can be selected. .

**Querier Election :** Enable to join IGMP Querier election in the VLAN. Disable to act as an IGMP Non-Querier.

**Querier Address :** Define the IPv4 address as source address used in IP header for IGMP Querier election. When the Querier address is not set, system uses IPv4 management address of the IP interface associated with this VLAN. When the IPv4 management address is not set, system uses the first available IPv4 management address. Otherwise, system uses a pre-defined value. By default, this value will be 192.0.2.1.

**Compatibility** : Compatibility is maintained by hosts and routers taking appropriate actions depending on the versions of IGMP operating on hosts and routers within a network. The allowed selection is IGMP-Auto, Forced IGMPv1, Forced IGMPv2, Forced IGMPv3, default compatibility value is IGMP-Auto.

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

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

**QI** : Query Interval. The Query Interval is the interval between General Queries sent by the Querier. The allowed range is 1 to 31744 seconds; default query interval is 125 seconds.

**QRI** : Query Response Interval. The Max Response Time used to calculate the Max Resp Code inserted into the periodic General Queries. The allowed range is 0 to 31744 in tenths of seconds; default query response interval is 100 in tenths of seconds (10 seconds).

**LLQI (LMQI for IGMP)** : Last Member Query Interval. The 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** : 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 unsolicited report interval is 1 second. .

#### **Buttons :**

**Add New IGMP VLAN** : Click to add new IGMP VLAN. Specify the VID and configure the new entry. Click Apply. when done. The specific IGMP VLAN starts working after the corresponding static VLAN is also created.

**Apply** – Click to save changes.

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

**Refresh, |<<, >** : Click Refresh to refresh the displayed table starting from the "VLAN" input fields.

Click << to update the table starting from the first entry in the VLAN table, i.e. the entry with the lowest VLAN ID.

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

### 2-11.1.3 Port Filtering Profile

This page lets you set the IGMP Port Group Filtering. With the IGMP filtering feature, you can exert this type of control. In some network Application environments, as like the metropolitan or multiple-dwelling unit (MDU) installations, an user might want to control the multicast groups to which a user on a switch port can belong. It lets you control the distribution of multicast services, such as IP/TV, based on some type of subscription or service plan.

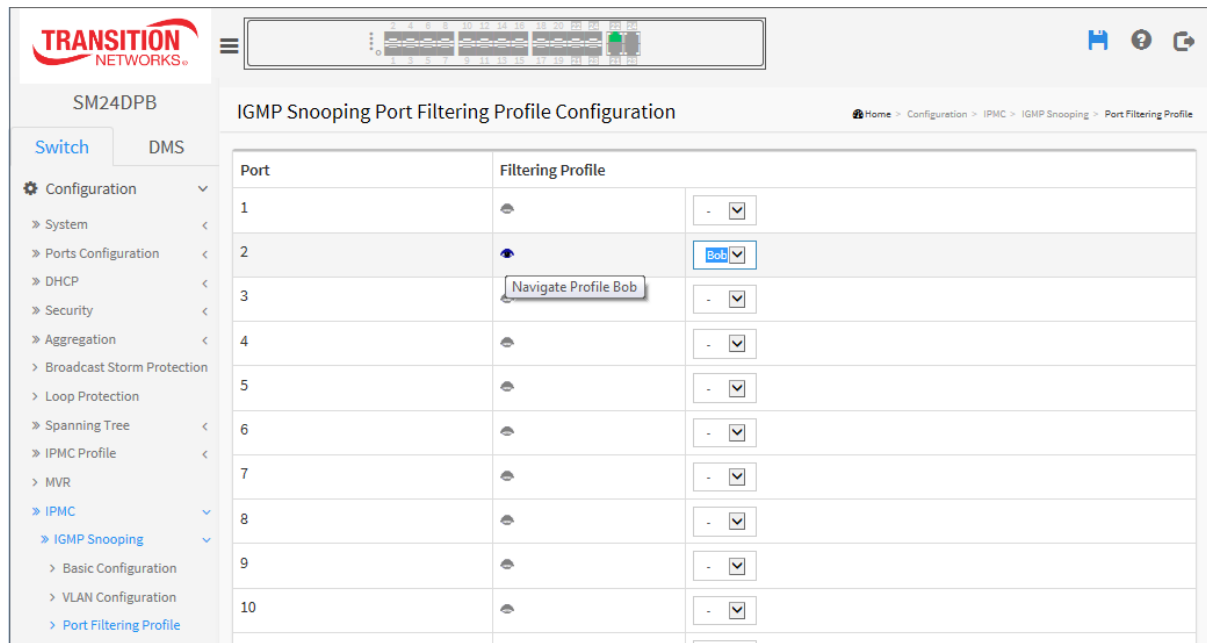
With this feature, you can filter multicast joins on a per-port basis by configuring IP multicast profiles and associating them with individual switch ports. An IGMP profile can contain one or more multicast groups and specifies whether access to the group is permitted or denied. If an IGMP profile denying access to a multicast group is applied to a switch port, the IGMP join report requesting the stream of IP multicast traffic is dropped, and the port is not allowed to receive IP multicast traffic from that group. If the filtering action permits access to the multicast group, the IGMP report from the port is forwarded for normal processing.

IGMP filtering controls only IGMP membership join reports and has no relationship to the function that directs the forwarding of IP multicast traffic.

To configure the IGMP Snooping Port Group Configuration in the web interface:

1. Click Configuration, IPMC, IGMP Snooping, Port Group Filtering.
2. Click Add New Filtering Group.
3. For each Port enable Port Group Filtering and specify the Filtering Groups.
4. Click Apply to save the setting
5. To cancel the setting click the Reset button to previously saved values.

**Figure 2-11.1.3: IGMP Snooping Port Filtering Profile Config page**



**Parameter descriptions:**

**Port :** The logical port for the settings.

**Filtering Profile :** Select the IPMC Profile as the filtering condition for the specific port. Summary about the designated profile will be shown by clicking the view button.

**Profile Management button :** You can inspect the rules of the designated profile by using the following button: : List the rules associated with the designated profile.

**Buttons:**

**Apply** – Click to save changes.

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

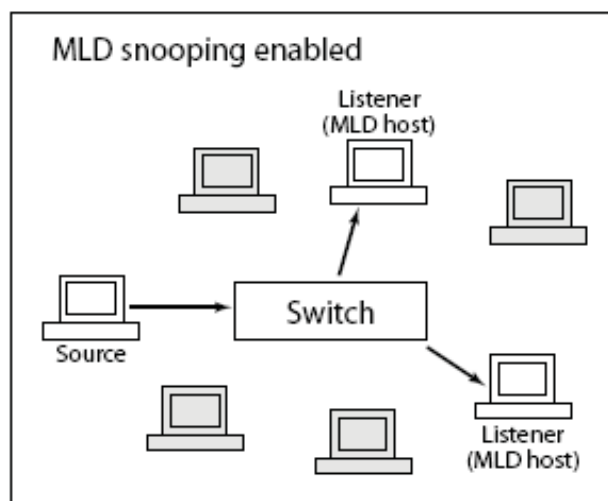


## 2-11.2 MLD Snooping

A network node that acts as a source of IPv6 multicast traffic is only an indirect participant in MLD snooping—it just provides multicast traffic, and MLD doesn't interact with it. (Note, however, that in an application like desktop conferencing a network node may act as both a source and an MLD host; but MLD interacts with that node only in its role as an MLD host.)

A source node creates multicast traffic by sending packets to a multicast address. In IPv6, addresses with the first eight bits set (that is, "FF" as the first two characters of the address) are multicast addresses, and any node that listens to such an address will receive the traffic sent to that address. Application software running on the source and destination systems cooperates to determine what multicast address to use. (Note that this is a function of the application software, not of MLD.)

When MLD snooping is enabled on a VLAN, the switch acts to minimize unnecessary multicast traffic. If the switch receives multicast traffic destined for a given multicast address, it forwards that traffic only to ports on the VLAN that have MLD hosts for that address. It drops that traffic for ports on the VLAN that have no MLD hosts.



MLD (Multicast Listener Discovery for IPv6) is used by IPv6 routers to discover multicast listeners on a directly attached link, much as IGMP is used in IPv4. The protocol is embedded in ICMPv6 instead of using a separate protocol.

### 2-11.2.1 Basic Configuration

This page lets you configure MLD Snooping basic configuration parameters.

#### **Web Interface**

To configure the MLD Snooping Configuration in the web interface:

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

**Figure 2-11.2.1: MLD Snooping Configuration page**

SM24DPB MLD Snooping Configuration

Home > Configuration > IPMC > MLD Snooping > Basic Configuration

Switch DMS

Configuration

- System
- Ports Configuration
- DHCP
- Security
- Aggregation
- Broadcast Storm Protection
- Loop Protection
- Spanning Tree
- IPMC Profile
- MVR
- IPMC
  - IGMP Snooping
  - MLD Snooping
    - Basic Configuration
    - VLAN Configuration
    - Port Filtering Profile
- LLDP
- MAC Table
- VLANs
- Private VLANs
- VCL
- Voice VLAN

Global Configuration

Snooping Enabled	<input type="checkbox"/>
Unregistered IPMCv6 Flooding Enabled	<input checked="" type="checkbox"/>
MLD SSM Range	ff3e:: / 96
Leave Proxy Enabled	<input type="checkbox"/>
Proxy Enabled	<input type="checkbox"/>

Port Related Configuration

Port	Router Port	Fast Leave	Throttling
*	<input type="checkbox"/>	<input type="checkbox"/>	< unlimited
1	<input type="checkbox"/>	<input type="checkbox"/>	unlimited
2	<input type="checkbox"/>	<input type="checkbox"/>	unlimited
3	<input type="checkbox"/>	<input type="checkbox"/>	unlimited
4	<input type="checkbox"/>	<input type="checkbox"/>	unlimited
5	<input type="checkbox"/>	<input type="checkbox"/>	unlimited
6	<input type="checkbox"/>	<input type="checkbox"/>	unlimited
7	<input type="checkbox"/>	<input type="checkbox"/>	unlimited

**Parameter descriptions:**

**Snooping Enabled:** Enable the Global MLD Snooping.

**Unregistered IPMCv6 Flooding enabled :** Enable unregistered IPMCv6 traffic flooding. The flooding control takes effect only when MLD Snooping is enabled. When MLD Snooping is disabled, unregistered IPMCv6 traffic flooding is always active in spite of this setting.

**MLD SSM Range:** SSM (Source-Specific Multicast) Range allows the SSM-aware hosts and routers run the SSM service model for the groups in the address (Using IPv6 Address) range.

**Leave Proxy Enabled:** Enable MLD Leave Proxy. This feature can be used to avoid forwarding unnecessary leave messages to the router side.

**Proxy Enabled:** Enable MLD Proxy. This feature can be used to avoid forwarding unnecessary join and leave messages to the router side.

**Fast Leave:** Check to enable the fast leave on the port.

**Router Port:** Specify which ports act as router ports. A router port is a port on the Ethernet switch that leads towards the Layer 3 multicast device or MLD querier. If an aggregation member port is selected as a router port, the whole aggregation will act as a router port.

**Throttling:** Select unlimited or 1-10 to limit the number of multicast groups to which a switch port can belong.

**Buttons:**

**Apply** – Click to save changes.

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

## 2-11.2.2 VLAN Configuration

When MLD snooping is enabled on a VLAN, the switch acts to minimize unnecessary multicast traffic. If the switch receives multicast traffic destined for a given multicast address, it forwards that traffic only to ports on the VLAN that have MLD hosts for that address. It drops that traffic for ports on the VLAN that have no MLD hosts

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

### Web Interface

To configure the MLD Snooping VLAN Configuration in the web interface:

1. Click Configuration, IPMC, MLD Snooping, VLAN Configuration
2. Specify the VLAN ID entries per page.
3. Click the Add New VLAN button and enter the MLD Snooping VLAN parameters.
4. Click the Apply button when done to save the settings.

**Figure 2-11.2.2: MLD Snooping VLAN Configuration page**

Delete	VLAN ID	Snooping Enabled	Querier Election	Compatibility	PRI	RV	QI (sec)	QRI (0.1 sec)	LLQI (0.1 sec)	URI (sec)
<input type="checkbox"/>		<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	MLD-Auto	0	2	125	100	10	1

### Parameter descriptions:

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

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

**IGMP Snooping Enabled** : Enable the per-VLAN IGMP Snooping. Up to 32 VLANs can be selected.

**Querier Election** : Enable to join IGMP Querier election in the VLAN. Disable to act as an IGMP Non-Querier.

**Querier Address** : Define the IPv4 address as source address used in IP header for IGMP Querier election. When the Querier address is not set, system uses IPv4 management address of the IP interface associated with this VLAN. When the IPv4 management address is not set, system uses the first available IPv4 management address. Otherwise, system uses a pre-defined value. By default, this value will be 192.0.2.1.

**Compatibility** : Compatibility is maintained by hosts and routers taking appropriate actions depending on the versions of IGMP operating on hosts and routers within a network. The allowed selections are IGMP-Auto, Forced IGMPv1, Forced IGMPv2, Forced IGMPv3. The default compatibility value is IGMP-Auto.

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

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

**QI** : Query Interval. The Query Interval is the interval between General Queries sent by the Querier. The allowed range is 1 - 31744 seconds; default query interval is 125 seconds.

**QRI** : Query Response Interval. The Max Response Time used to calculate the Max Resp Code inserted into the periodic General Queries. The allowed range is 0 - 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 - 31744 in tenths of seconds; default last member query interval is 10 in tenths of seconds (1 second).

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

### **Buttons :**

**Apply** – Click to save changes.

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

**Refresh**: Click to refresh the displayed table starting from the "VLAN" input fields.

**<<** : Click to update the table starting from the first entry in the VLAN table (i.e., the entry with the lowest VLAN ID).

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

### 2-11.2.3 Port Group Filtering

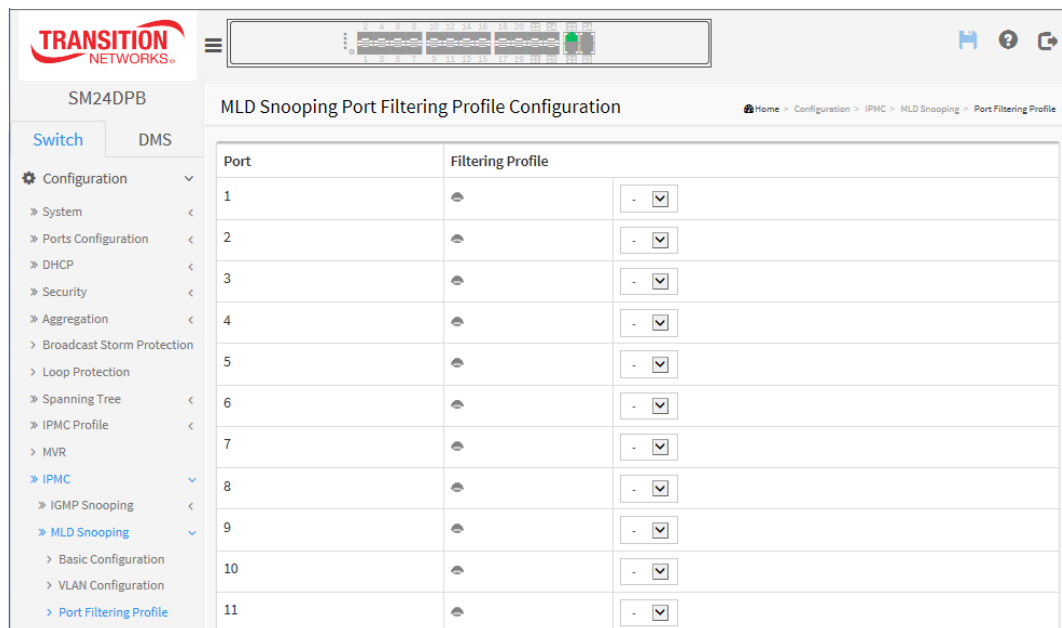
This page lets you set the Port Group Filtering in the MLD Snooping function and how to add a new filtering group and safety policy.

#### Web Interface

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

1. Click Configuration, IPMC, MLD Snooping, Port Group Filtering Configuration.
2. Click the Add New Filtering Group button.
3. Specify the Filtering Groups entries per page.
4. Enter the MLD Snooping **Port Filtering Profile** parameters.
5. Click the Apply to save the setting.
6. To cancel the setting click the Reset button to revert to previously saved values.

**Figure 2-11.2.3: MLD Snooping Port Filtering Profile Configuration**



#### Parameter descriptions:

**Port** : The logical port for the settings.

**Filtering Profile** : Select the IPMC Profile as the filtering condition for the specific port. Summary about the designated profile will be shown by clicking the view button.

**Profile Management Button** : You can inspect the rules of the designated profile by using the following button:

: List the rules associated with the designated profile.

#### Buttons:

**Apply** – Click to save changes.

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

## 2-12 LLDP

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

### 2-12.1 LLDP Configuration

You can configure LLDP parameters per-port; the settings will take effect immediately. This page lets you view and configure the current LLDP port settings.

#### Web Interface

To configure LLDP:

1. Click LLDP configuration.
2. Modify LLDP timing parameters.
3. Set the required mode for transmitting or receiving LLDP messages.
4. Specify the information to include in the TLV field of advertised messages.
5. Click Apply.

**Figure 2-13.1: LLDP Configuration page**

The screenshot displays the LLDP Configuration page in the SM24DPB web interface. The left sidebar shows the navigation menu with 'LLDP' selected. The main content area is divided into two sections: 'LLDP Parameters' and 'LLDP Port Configuration'.

**LLDP Parameters:**

Tx Interval	30	seconds
Tx Hold	4	times
Tx Delay	2	seconds
Tx Reinit	2	seconds

**LLDP Port Configuration:**

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

**Parameter descriptions:****LLDP Parameters**

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

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

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

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

**LLDP Port Configuration:**

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

**Mode :** Select LLDP mode.

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

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

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

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

**CDP Aware :** Select CDP awareness.

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 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.



## 2-12.2 LLDP-MED Configuration

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

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

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

### Web Interface

To configure LLDP-MED:

1. Click Configuration, LLDP, LLDP-MED.
2. Modify the Fast start repeat count parameter; the default is 4.
3. Modify Coordinates Location parameters.
4. Fill Civic Address Location parameters.
5. Click Add New Policy.
6. Click Apply to show the Policy Port Configuration.
7. Select a Policy ID for each port.
8. Click Apply.

Figure 2-12.2: LLDP-MED Configuration page

The screenshot displays the LLDP-MED Configuration page. On the left is a navigation menu with categories like Configuration, System, Ports, DHCP, Security, and LLDP. The main content area is titled 'LLDP-MED Configuration' and includes the following sections:

- Fast Start Repeat Count:** A text input field containing the value '4'.
- Coordinates Location:** Fields for Latitude (0), North (dropdown), Longitude (0), East (dropdown), Altitude (0), Meters (dropdown), and Map Datum (WGS84 dropdown).
- Civic Address Location:** A grid of text input fields for Country code, State/Province, County, City, City district, Block (Neighborhood), Street, Leading street direction, Trailing street suffix, Street suffix, House no., House no. suffix, Landmark, Additional location info, Name, Zip code, Building, Apartment, Floor, Room no., Place type, Postal community name, P.O. Box, and Additional code.
- Emergency Call Service:** A text input field.
- Policies:** A table with columns: Delete, Policy ID, Application Type, Tag, VLAN ID, L2 Priority, and DSCP. Below the table is an 'Add New Policy' button.

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

**Parameter descriptions:****Fast start repeat count**

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

With this in mind LLDP-MED defines an LLDP-MED Fast Start interaction between the protocol and the application layers on top of the protocol, in order to achieve these related properties. Initially, a Network Connectivity Device will only transmit LLDP TLVs in an LLDPDU. Only after an LLDP-MED Endpoint Device is detected, will an LLDP-MED capable Network Connectivity Device start to advertise LLDP-MED TLVs in outgoing LLDPDUs on the associated port. The LLDP-MED application will temporarily speed up the transmission of the LLDPDU to start within a second, when a new LLDP-MED neighbour 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 SHOULD be normalized to within 0-90 degrees with a maximum of 4 digits.

It is possible to specify the direction to either North of the equator or South of the equator.

**Longitude :** Longitude SHOULD be normalized to within 0-180 degrees with a maximum of 4 digits.

It is possible to specify the direction to either East of the prime meridian or West of the prime meridian.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

**House no.** : House number - Example: 21.

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

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

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

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

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

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

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

**Floor** : Floor - Example: 4.

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

**Place type** : Place type - Example: Office.

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

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

**Additional code** : Additional code - Example: 1320300003.

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

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

**Policies** : Network Policy Discovery enables the efficient discovery and diagnosis of mismatch issues with the VLAN configuration, along with the associated Layer 2 and Layer 3 attributes, which apply for a set of specific protocol applications on that port. Improper network policy configurations are a very significant issue in VoIP environments that frequently result in voice quality degradation or loss of service. Policies are only intended for use with applications that have specific 'real-time' network policy requirements, such as interactive voice and/or video services.

The network policy attributes advertised are:

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

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

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

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

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 immediately.

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

**Application Type :** Intended use of the application types:

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

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

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

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

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

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

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

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

policies apply as those advertised in the Video Conferencing application policy.

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

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

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

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

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

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

**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.

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

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

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

#### **Buttons:**

**Apply** – Click to save changes.

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

## 2-13 MAC Table

Switching of frames is based on the DMAC address contained in the frame. The switch builds up a table that maps MAC addresses to switch ports for knowing which ports the frames should go to (based on the DMAC address in the frame). This table contains both static and dynamic entries.

The static entries are configured by the network administrator if the administrator wants to do a fixed mapping between the DMAC address and switch ports.

The frames also contain a MAC address (SMAC address), which shows the MAC address of the equipment sending the frame. The SMAC address is used by the switch to automatically update the MAC table with these dynamic MAC addresses. Dynamic entries are removed from the MAC table if no frames with the corresponding SMAC address have been seen after a configurable age time.

To configure MAC Address Table in the web interface:

### Aging Configuration

1. Click Configuration, MAC Table.
2. Specify the Disable Automatic Aging and Aging Time.
3. Click Apply.

### MAC Table Learning

1. Click Configuration, MAC Table.
2. Specify the Port Members (Auto, Disable, Secure).
3. Click Apply.

### Static MAC Table Configuration

1. Click configuration and Add new Static entry.
2. Specify the VLAN IP and Mac address, Port Members.
3. Click Apply.

**Figure 2-13: MAC Address Table Configuration page**

The screenshot shows the 'MAC Address Table Configuration' page. It includes a sidebar with navigation options like 'Switch', 'DMS', and 'Configuration'. The main content area is divided into three sections:

- Aging Configuration:** Contains a checkbox for 'Disable Automatic Aging' and a text input for 'Aging Time' set to '300 seconds'.
- MAC Table Learning:** Features a table for 'Port Members' with columns 1-24. It has three rows: 'Auto' (all checked), 'Disable' (all unchecked), and 'Secure' (all unchecked).
- Static MAC Table Configuration:** Includes a table with columns 'Delete', 'VLAN ID', 'MAC Address', and 'Port Members' (1-24). Below the table are buttons for 'Add New Static Entry', 'Apply', and 'Reset'.

**Parameter descriptions:**

**Aging Configuration :** By default, dynamic entries are removed from the MAC table after 300 seconds. This removal is also called aging. Configure aging time by entering a value here in seconds; for example, Age time in seconds. The allowed range is 10 to 1000000 seconds.

Disable the automatic aging of dynamic entries by checking  Disable automatic aging.

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

**Auto :** Learning is done automatically as soon as a frame with unknown SMAC is received.

**Disable :** No learning is done.

**Secure :** Only static MAC entries are learned, all other frames are dropped.



**NOTE:** Make sure that the link used for managing the switch is added to the Static Mac Table before changing to secure learning mode, otherwise the management link is lost and can only be restored by using another non-secure port or by connecting to the switch via the serial interface.

**Static MAC Table Configuration :** The static entries in the MAC table are shown in this table. The static MAC table can contain 64 entries. The maximum of 64 entries is for the whole stack, and not per switch. The MAC table is sorted first by VLAN ID and then by MAC address.

**Delete :** Check to delete the entry. It will be deleted immediately.

**VLAN ID :** The VLAN ID of the entry.

**MAC Address :** The MAC address of the entry.

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

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

**Buttons:**

**Apply** – Click to save changes.

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

**Messages**

**Message:** *No port members selected for VLAN ID:1 and MAC address: 00-00-00-00-00-00. This will block the MAC address for all ports. Is this correct?*

*Meaning:* You made no entry, which will block access from all ports.

*Recovery:*

1. Click the **OK** button to clear the webpage message.
2. Enter the parameters (VLAN ID and Mac Address) as required.
3. Continue operation.

**Message:** *Entry with VLAN ID:1 and MAC address 00-00-00-00-00-00 is already in the MAC table.*

*Meaning:* You made a duplicate entry.

*Recovery:*

1. Click the **OK** button to clear the webpage message.
2. Re-enter the parameters (VLAN ID and Mac Address) as required.
3. Continue operation.
4. Log in again if necessary.



## 2-14 VLANs

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

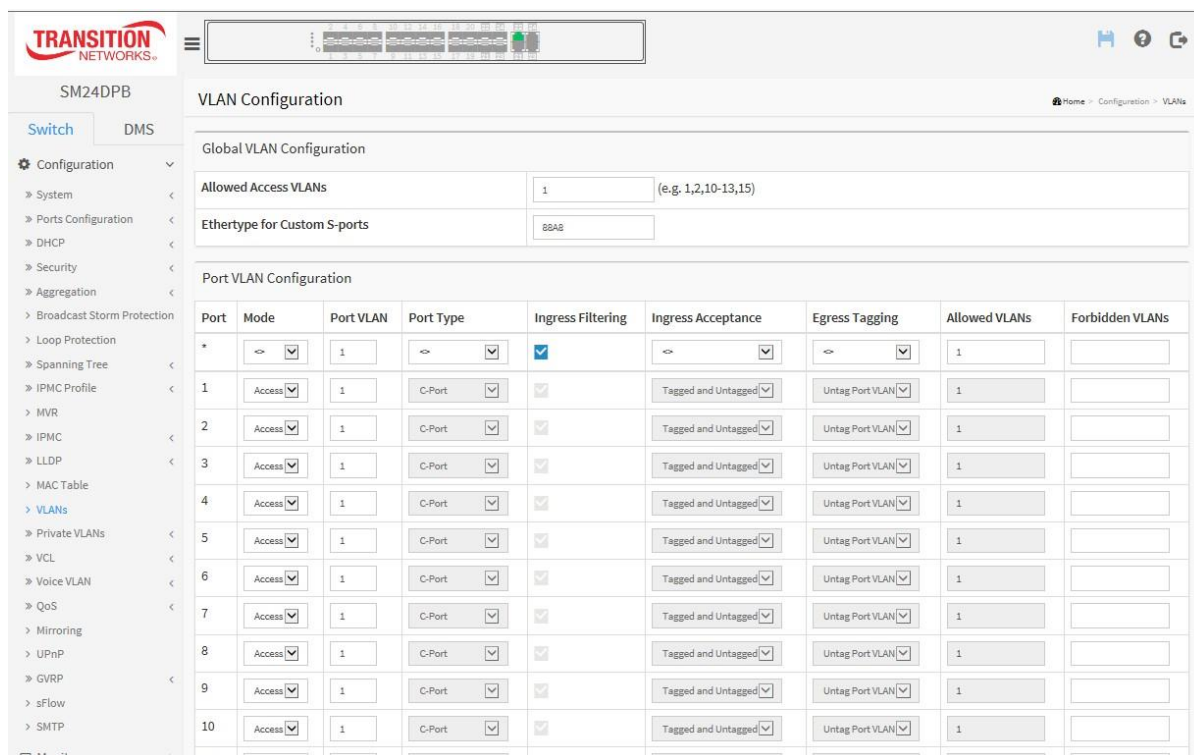
When you specify a new management VLAN, your HTTP connection to the old management VLAN is lost. For this reason, you should have a connection between your management station and a port in the new management VLAN or connect to the new management VLAN through a multi-VLAN route.

### Web Interface

To configure VLAN membership configuration in the web interface:

1. Click Configuration, VLANS.
2. Specify Global VLAN Configuration and Port VLAN Configuration parameters.
3. Click Apply.

**Figure 2-14.1: VLAN Configuration page**



### Parameter descriptions:

#### Global VLAN Configuration

**Allowed Access VLANs :** This field shows the VLANs that are created on the switch. By default, only VLAN 1 exists. More VLANs may be created by using a list syntax where the individual elements are separated by commas. Ranges are specified with a dash separating the lower and upper bound. The following example will create VLANs 1, 10, 11, 12, 13, 200, and 300: 1,10-13,200,300. Spaces are allowed in between the delimiters.

**Ethertype for Custom S-ports :** This field specifies the ethertype/TPID (specified in hexadecimal) used for Custom S-ports. The setting is in force for all ports whose Port Type is set to S-Custom-Port.

## **Port VLAN Configuration**

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

**Mode :** The port mode (default is Access) determines the fundamental behavior of the port in question. A port can be in one of three modes as described below.

Whenever a particular mode is selected, the remaining fields in that row will be either grayed out or made changeable depending on the mode in question.

Grayed out fields show the value that the port will get when the mode is applied.

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

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

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

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

**Hybrid:** Hybrid ports resemble trunk ports in many ways, but adds additional port configuration features. In addition to the characteristics described for trunk ports, hybrid ports have these abilities:

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

**Port VLAN :** Determines the port's VLAN ID (a.k.a. PVID). Allowed VLANs are 1 - 4095, default being 1.

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

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

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

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

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

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

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

**S-Custom-Port:** On ingress, frames with a VLAN tag with a TPID = 0x8100 or equal to the Ethertype configured

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

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

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

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

**VLAN Trunking** : Trunk and Hybrid ports allow for enabling VLAN trunking.

When VLAN trunking is enabled, frames classified to unknown VLANs are accepted on the port whether ingress filtering is enabled or not.

This is useful in scenarios where a cloud of intermediary switches must bridge VLANs that haven't been created. By configuring the ports that connect the cloud of switches as trunking ports, they can seamlessly carry those VLANs from one end to the other.

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

**Tagged and Untagged**: Both tagged and untagged frames are accepted.

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

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

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

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

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

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

**Allowed VLANs** : Ports in Trunk and Hybrid mode may control which VLANs they are allowed to become members of. Access ports can only be member of one VLAN, the Access VLAN.

The field's syntax is identical to the syntax used in the Existing VLANs field. By default, a port may become member of all possible VLANs, and is therefore set to **1 - 4095**.

The field may be left empty, which means that the port will not be member of any of the existing VLANs, but if it is configured for VLAN Trunking it will still be able to carry all unknown VLANs.

**Forbidden VLANs** : A port may be configured to never be member of one or more VLANs. This is particularly useful when dynamic VLAN protocols like MVRP and GVRP must be prevented from dynamically adding ports to VLANs. The trick is to mark such VLANs as forbidden on the port in question. The syntax is identical to the syntax used in the Existing VLANs field.

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

## 2-15 Private VLANs

In a private VLAN, communication between ports in that private VLAN is not permitted. A VLAN can be configured as a private VLAN.

### 2-15.1 VLAN Membership

The VLAN membership configuration for can be monitored and modified here. Up to 4096 VLANs are supported. This page allows for adding and deleting VLANs as well as adding and deleting port members of each VLAN.

#### Web Interface

To configure VLAN membership in the web interface:

1. Click Configuration, Private VLANs, and Membership.
2. Click the Add New VLAN Membership button.
3. Specify a Management VLAN ID (0~ 4094).
4. Click Apply.

**Figure 2-15.1: Private VLAN Membership Configuration page**

Private VLAN Membership Configuration		Port Members																							
Delete	PVLAN ID	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24
<input type="checkbox"/>	1	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
<input type="checkbox"/>	0	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

#### Parameter descriptions:

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

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

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

**Adding a New VLAN** : Click to add a new VLAN ID. An empty row is added to the table, and the VLAN can be configured as needed. Legal values for a VLAN ID are 1 - 4095.

The VLAN is enabled on the selected switch unit when you click on "Save". The VLAN is thereafter present on the other switch units, but with no port members. The check box is greyed out when VLAN is displayed on other switches, but you can add member ports to it.

A VLAN without any port members on any switch will be deleted when you click "Save". The **Reset** button can be used to undo the addition of new VLANs.

**Buttons:**

**Apply** – Click to save changes.

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

## 2-15.2 Port Isolation

Port Isolation provides for an apparatus and method to isolate ports on layer 2 switches on the same VLAN to restrict traffic flow. The apparatus comprises a switch having said plurality of ports, each port configured as a protected port or a non-protected port. An address table memory stores an address table having a destination address and port number pair. A forwarding map generator generates a forwarding map which is responsive to a destination address of a data packet. The method for isolating ports on a layer 2 switch comprises configuring each of the ports on the layer 2 switch as a protected port or a non-protected port. A destination address on an data packet is matched with a physical address on said layer 2 switch and a forwarding map is generated for the data packet based upon the destination address on the data packet. The data packet is then sent to the plurality of ports pursuant to the forwarding map generated based upon whether the ingress port was configured as a protected or non-protected port.

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

### Web Interface

To configure Port Isolation configuration in the web interface:

1. Click Configuration, Private VLANs, Port Isolation.
2. Select which port(s) you want to enable Port Isolation.
3. Click Apply.

**Figure 2-15.1: Port Isolation Configuration page**



### Parameter descriptions:

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

### Buttons:

**Apply** – Click to save changes.

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

## 2-16 VCL

### 2-16.1 MAC-based VLAN

MAC address-based VLAN decides the VLAN for forwarding an untagged frame based on the source MAC address of the frame.

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

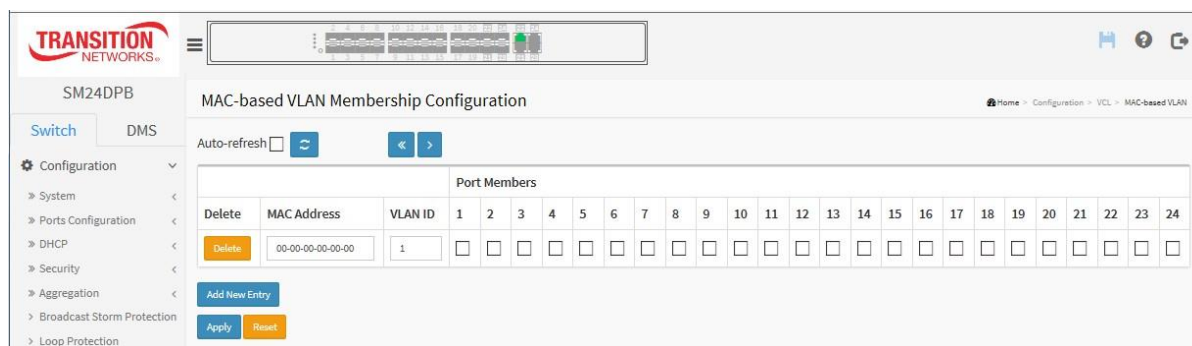
MAC-based VLANs group VLAN members by MAC address. With MAC-based VLAN configured, the device adds a VLAN tag to an untagged frame according to its source MAC address. MAC-based VLANs are mostly used in conjunction with security technologies such as 802.1X to provide secure, flexible network access for terminal devices.

#### Web Interface

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

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

**Figure 2-16.1: MAC-based VLAN Membership Configuration page**



#### Parameter descriptions:

**Delete :** To delete a MAC-based VLAN entry, check this box and click Apply. The entry will be deleted on the selected switch in the stack.

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

**VLAN ID :** Indicates the VLAN ID.

**Port Members :** A row of check boxes for each port is displayed for each MAC-based VLAN entry. To include a port in a MAC-based VLAN, check the box. To remove or exclude the port from the MAC-based VLAN, make

sure the box is unchecked. By default, no ports are members, and all boxes are unchecked.

### **Adding a New MAC-based VLAN**

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

The MAC-based VLAN entry is enabled on the selected switch unit when you click Apply.

A MAC-based VLAN without any port members on any switch unit will be deleted when you click Apply.

The **Reset** button can be used to undo the addition of new MAC-based VLANs.

### **Buttons:**

**Apply** – Click to save changes.

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



## 2-16.2 Protocol -based VLAN

This section describes Protocol -based VLAN. The switch supports Protocol include Ethernet, LLC, and SNAP protocols.

**LLC:** The Logical Link Control (LLC) data communication protocol layer is the upper sub-layer of the Data Link Layer (which is itself layer 2, just above the Physical Layer) in the seven-layer OSI reference model. It provides multiplexing mechanisms that make it possible for several network protocols (IP, IPX, Decnet and AppleTalk) to coexist within a multipoint network and to be transported over the same network media, and can also provide flow control and automatic repeat request (ARQ) error management mechanisms.

**SNAP:** The Subnetwork Access Protocol (SNAP) is a mechanism for multiplexing, on networks using IEEE 802.2 LLC, more protocols than can be distinguished by the 8-bit 802.2 Service Access Point (SAP) fields. SNAP supports identifying protocols by Ethernet type field values; it also supports vendor-private protocol identifier spaces. It is used with IEEE 802.3, IEEE 802.4, IEEE 802.5, IEEE 802.11 and other IEEE 802 physical network layers, as well as with non-IEEE 802 physical network layers such as FDDI that use 802.2 LLC.

### 2-16.2.1 Protocol to Group

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

#### Web Interface

To configure Protocol -based VLAN configuration in the web interface:

1. Click Configuration, VCL, Protocol-based VLAN, Protocol to Group.
2. Click Add New Entry.
3. Specify the Ethernet LLC SNAP Protocol and Group Name.
4. Click Apply.

**Figure 2-16.2.1: Protocol to Group Mapping Table**

The screenshot shows the 'Protocol to Group Mapping Table' configuration page. The interface includes a navigation menu on the left with options like Configuration, System, Ports Configuration, DHCP, Security, Aggregation, Broadcast Storm Protection, and Loop Protection. The main content area has a breadcrumb trail: Home > Configuration > VCL > Protocol-based VLAN > Protocol to Group. Below the breadcrumb, there is an 'Auto-refresh' checkbox and a refresh icon. The table below has the following structure:

Delete	Frame Type	Value	Group Name
<input type="checkbox"/>	Ethernet SNAP LLC	Etype: 0x 0800	

Buttons for 'Delete', 'Add New Entry', 'Apply', and 'Reset' are also visible.

#### Parameter descriptions:

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

**Frame Type :** At the dropdown select Ethernet, LLC, or SNAP.



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

**Value :** Valid value that can be entered in this text field depends on the option selected from the preceding Frame Type selection menu.

Below are the criteria for three different Frame Types:

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

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

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

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

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

a. OUI: OUI (Organizationally Unique Identifier) is value in format of xx-xx-xx where each pair (xx) in string is a hexadecimal value ranges from 0x00-0xff.

b. PID: If the OUI is hexadecimal 000000, the protocol ID is the Ethernet type (EtherType) field value for the protocol running on top of SNAP; if the OUI is an OUI for a particular organization, the protocol ID is a value assigned by that organization to the protocol running on top of SNAP.

In other words, if value of OUI field is 00-00-00 then value of PID will be etype (0x0600-0xffff) and if value of OUI is other than 00-00-00 then valid value of PID will be any value from 0x0000 to 0xffff.

**Group Name :** A valid Group Name is a unique 16-character long string for every entry which consists of a combination of alphabets (a-z or A-Z) and integers(0-9).



---

**NOTE:** Special character and underscore ( ) are not allowed.

---

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

#### **Buttons:**

**Apply** – Click to save changes.

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

**Refresh:** Click to refresh the Protocol Group Mapping information manually.

## 2-16.2.2 Group to VLAN

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

### Web Interface

To configure Group Name to VLAN mapping table in the web interface:

1. Click Configuration, VCL, Protocol-based VLAN, Group to VLAN.
2. Click the Add New Entry button.
3. Specify the Group Name and VLAN ID.
4. Click Apply.

**Figure 2-16.2.2: Group Name to VLAN mapping Table**

The screenshot shows the web interface for SM24DPB. The main content area is titled "Group Name to VLAN mapping Table". It features an "Auto-refresh" checkbox and a refresh icon. Below this is a table with the following structure:

			Port Members																							
Delete	Group Name	VLAN ID	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24
<input type="checkbox"/>	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

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

### Parameter descriptions:

**Delete** : To delete a Group Name to VLAN map entry, check this box. The entry is deleted immediately.

**Group Name** : A valid Group Name is a string of at most 16 characters which consists of a combination of alphabets (a-z or A-Z) and integers(0-9), no special character is allowed. whichever Group name you try map to a VLAN must be present in Protocol to Group mapping table and must not be already used by any other existing mapping entry on this page.

**VLAN ID** : Indicates the ID to which Group Name will be mapped. A valid VLAN ID ranges from 1-4095.

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

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

### Buttons:

**Apply** – Click to save changes.

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

**Auto-refresh** : Check to automatically refresh the device every three seconds.

**Refresh**: Click to refresh the Protocol Group Mapping information manually.

### 2-16.3 IP Subnet-based VLAN

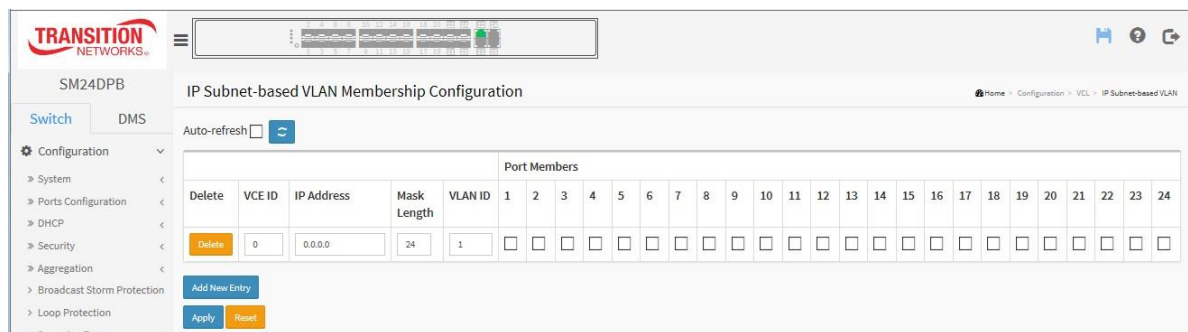
The IP subnet-based VLAN entries can be configured here. This page allows for adding, updating and deleting IP subnet-based VLAN entries and assigning the entries to different ports. This page shows only static entries. The maximum possible IP subnet-based VLAN entries are limited to 128.

#### Web Interface

To display IP subnet-based VLAN Membership to configured in the web interface:

1. Click Configuration, VCL, IP Subnet-based VLAN.
2. Click Add New Entry.
2. Specify the VCE ID, IP Address, Mask Length, VLAN ID and select Port Members.
3. Click Apply.

**Figure 2-16.3: IP Subnet-based VLAN Membership Configuration**



#### Parameter descriptions:

**Delete :** To delete a IP subnet-based VLAN entry, check this box and press Apply. The entry will be deleted.

**VCE ID :** Indicates the index of the entry. It is user configurable. Its value ranges from 0-128. If a VCE ID is 0, application will auto-generate the VCE ID for that entry. Deletion and lookup of IP subnet-based VLAN are based on VCE ID.

**IP Address :** Indicates the IP address.

**Mask Length :** Indicates the network mask length.

**VLAN ID :** Indicates the VLAN ID. VLAN ID can be changed for the existing entries.

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

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

The IP subnet-based VLAN entry is enabled on the selected switch when you click Apply.

The Delete button can be used to undo the addition of new IP subnet-based VLANs.

## 2-17 Voice VLAN

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

### 2-17.1 Configuration

The Voice VLAN feature enables voice traffic forwarding on the Voice VLAN, then the switch can classify and schedule network traffic. It is recommended that there be two VLANs on a port - one for voice, one for data. Before connecting the IP device to the switch, the IP phone should configure the voice VLAN ID correctly. It should be configured through its own GUI.

### Web Interface

To configure Voice VLAN in the web interface:

1. Click Configuration, Voice VLAN, Configuration.
2. Select "Enabled" in the Voice VLAN Configuration.
2. Specify VLAN ID, Aging Time, Traffic class.
3. Specify Port Mode, Security, and Discovery Protocol in the Port Configuration.
4. Click Apply.

**Figure 2-17.1: Voice VLAN Configuration page**

The screenshot shows the 'Voice VLAN Configuration' page. The top navigation bar includes the 'TRANSITION NETWORKS' logo and a breadcrumb trail: Home > Configuration > Voice VLAN > Configuration. The left sidebar shows a menu with 'Voice VLAN' selected and expanded to 'Configuration'. The main content area is titled 'Voice VLAN Configuration' and contains two sections:

**Voice VLAN Configuration**

Mode	Disabled
VLAN ID	1000
Aging Time	86400 seconds
Traffic	7 (High)

**Port Configuration**

Port	Mode	Security	Discovery Protocol
*	Disabled	<	<
1	Disabled	Disabled	OUI
2	Disabled	Disabled	OUI
3	Disabled	Disabled	OUI
4	Disabled	Disabled	OUI
5	Disabled	Disabled	OUI
6	Disabled	Disabled	OUI

### Parameter descriptions:

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

**Enabled:** Enable Voice VLAN mode operation.

**Disabled:** Disable Voice VLAN mode operation.

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

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

**Traffic Class :** Indicates the Voice VLAN traffic class. All traffic on the Voice VLAN will apply this class.

**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:

**Disabled:** Disjoin from Voice VLAN.

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

**Forced:** Force join to Voice VLAN.

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

**Enabled:** Enable Voice VLAN security mode operation.

**Disabled:** Disable Voice VLAN security mode operation.

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

**OUI:** Detect telephony device by OUI address.

**LLDP:** Detect telephony device by LLDP.

**Both:** Both OUI and LLDP.

#### **Buttons:**

**Apply** – Click to save changes.

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

## 2-17.2 OUI

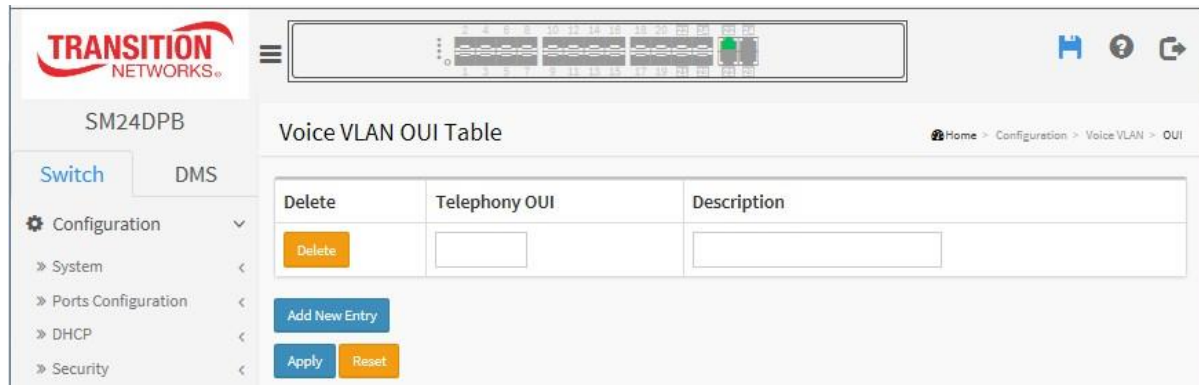
This section describes how to configure the Voice VLAN OUI table. The maximum entry number is 16. Modifying the OUI table will restart auto detection of the OUI process.

### Web Interface

To configure Voice VLAN OUI Table in the web interface:

1. Click Configuration, Voice VLAN, OUI.
2. Click the Add New Entry button in the Voice VLAN OUI table.
3. Specify Telephony OUI and Description.
4. Click Apply.

**Figure 2-17.2: The Voice VLAN OUI Table**



### Parameter descriptions:

**Delete** : Check to delete the entry. It will be deleted immediately.

**Telephony OUI** : A telephony OUI address is a globally unique identifier assigned to a vendor by IEEE. It must be 6 characters long and the input format is "xx-xx-xx" (x is a hexadecimal digit).

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

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

### Buttons:

**Apply** – Click to save changes.

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

## 2-18 QoS

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

High flexibility in the classification of incoming frames to a QoS class. The QoS classification looks for information up to Layer 4, including IPv4 and IPv6 DSCP, IPv4 TCP/UDP port numbers, and user priority of tagged frames. This QoS classification mechanism is implemented in a QoS control list (QCL). The QoS class assigned to a frame is used throughout the device for providing queuing, scheduling, and congestion control guarantees to the frame according to what was configured for that specific QoS class.

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

- > QoS
- > Port Classification
- > Port Policing
- > Port Scheduler
- > Port Shaping
- > Port Tag Remarking
- > Port DSCP
- > DSCP-Based QoS
- > DSCP Translation
- > DSCP Classification
- > QoS Control List
- > Storm Control
- > WRED

### 2-18.1 Port Classification

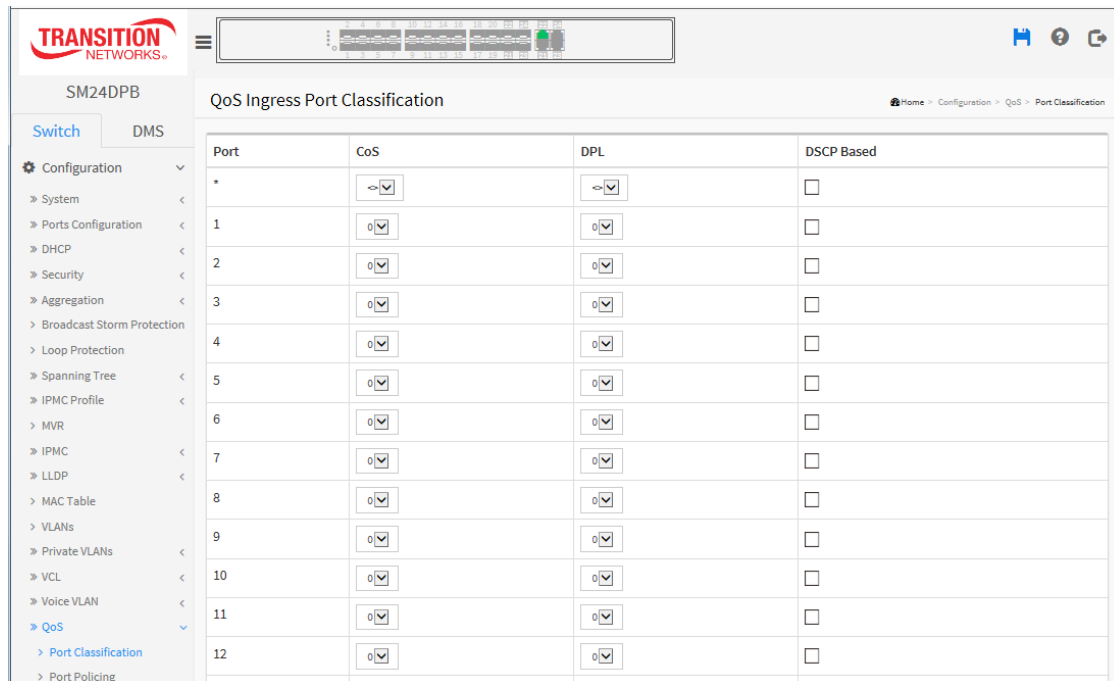
This page lets you configure the basic QoS Ingress Classification settings for all switch ports.

#### Web Interface

To configure the QoS Port Classification parameters in the web interface:

1. Click Configuration, QoS, Port Classification.
2. Select QoS class, DP Level, PCP and DEI parameters.
3. Click Apply to save the settings.
4. To cancel the setting, click the Reset button to revert to previously saved values.

**Figure 2-18.1: QoS Ingress Port Classification page**





**Parameter descriptions:**

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

**CoS :** Controls the default class of service.

All frames are classified to a CoS. There is a one to one mapping between CoS, queue and priority. A CoS of 0 (zero) has the lowest priority.

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

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

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

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

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

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

**Tag Class. :** Shows the classification mode for tagged frames on this port.

**Disabled:** Use default QoS class and DP level for tagged frames.

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

Click on the mode in order to configure the mode and/or mapping.



---

**NOTE:** This setting has no effect if the port is VLAN unaware. Tagged frames received on VLAN unaware ports are always classified to the default CoS and DPL.

---

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

**Address Mode :** The IP/MAC address mode specifying whether the QCL classification must be based on source (SMAC/SIP) or destination (DMAC/DIP) addresses on this port. Valid values are:

**Source:** Enable SMAC/SIP matching.

**Destination:** Enable DMAC/DIP matching.

**Buttons:**

**Apply** – Click to save changes.

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

## 2-18.2 Port Policing

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

### Web Interface

To display the QoS Port Schedulers in the web interface:

1. Click Configuration, QoS, Port Policing.
2. Check the checkboxes of ports to enable as QoS Ingress Port Policers
3. Enter the Rate limit condition.
4. Select the Rate limit Unit (kbps, Mbps, fps or kfps).
5. Click Apply to save the settings.

**Figure 2-18.2: QoS Ingress Port Policers page**

Port	Enabled	Rate	Unit	Flow Control
*	<input type="checkbox"/>	500	< >	<input type="checkbox"/>
1	<input type="checkbox"/>	500	kbps	
2	<input type="checkbox"/>	500	kbps	
3	<input type="checkbox"/>	500	kbps	
4	<input type="checkbox"/>	500	kbps	
5	<input type="checkbox"/>	500	kbps	
6	<input type="checkbox"/>	500	kbps	
7	<input type="checkbox"/>	500	kbps	
8	<input type="checkbox"/>	500	kbps	
9	<input type="checkbox"/>	500	kbps	
10	<input type="checkbox"/>	500	kbps	
11	<input type="checkbox"/>	500	kbps	
12	<input type="checkbox"/>	500	kbps	
13	<input type="checkbox"/>	500	kbps	

### Parameter descriptions:

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

**Enabled :** Check which port(s) you want to enable the QoS Ingress Port Policers function.

**Rate :** Set the Rate limit value for this port; the default is 500.

**Unit :** At the dropdown select the Rate unit of measure to use (kbps, Mbps, fps or kfps). The default is kbps.

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

**Buttons:**

**Apply** – Click to save changes.

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

## 2-18.4 Port Schedulers

This page lets you configure QoS Egress Port Schedulers for all switch ports.

### Web Interface

To configure the QoS Port Schedulers in the web interface:

1. Click Configuration, QoS, Port Schedulers.
2. Click the Port index to set the QoS Egress Port Schedulers.
3. Configure the QoS Egress Port Schedulers. If you select the scheduler mode with weighted then the screen will change as the figure.
4. Click Apply to save the settings.

**Figure 2-18.4: QoS Egress Port Schedulers page**

**QoS Egress Port Schedulers** Home > Configuration > QoS > Port Scheduler

Port	Mode	Q0	Q1	Q2	Q3	Q4	Q5
1	Strict Priority	-	-	-	-	-	-
2	Strict Priority	-	-	-	-	-	-
3	Strict Priority	-	-	-	-	-	-

**QoS Egress Port Scheduler and Shapers Port 1** Home > Configuration > QoS > Port Scheduler

Port: Port 1

Scheduler Mode: Strict Priority

**Queue Shaper**

Queue	Enable	Rate	Unit	Excess
*	<input type="checkbox"/>	500	<>	<input type="checkbox"/>
0	<input type="checkbox"/>	500	kbps	<input type="checkbox"/>
1	<input type="checkbox"/>	500	kbps	<input type="checkbox"/>
2	<input type="checkbox"/>	500	kbps	<input type="checkbox"/>
3	<input type="checkbox"/>	500	kbps	<input type="checkbox"/>
4	<input type="checkbox"/>	500	kbps	<input type="checkbox"/>
5	<input type="checkbox"/>	500	kbps	<input type="checkbox"/>
6	<input type="checkbox"/>	500	kbps	<input type="checkbox"/>
7	<input type="checkbox"/>	500	kbps	<input type="checkbox"/>

Port Shaper		
<b>Enable</b>	<b>Rate</b>	<b>Unit</b>
<input type="checkbox"/>	500	kbps

Apply Reset Cancel

QoS Egress Port Scheduler and Shapers Port 1

Home > Configuration > QoS > Port Scheduler

<b>Port</b>	Port 1
<b>Scheduler Mode</b>	Weighted

Queue Shaper				Queue Scheduler		
Queue	Enable	Rate	Unit	Excess	Weight	Percent
*	<input type="checkbox"/>	500	<>	<input type="checkbox"/>	17	
0	<input type="checkbox"/>	500	kbps	<input type="checkbox"/>	17	
1	<input type="checkbox"/>	500	kbps	<input type="checkbox"/>	17	
2	<input type="checkbox"/>	500	kbps	<input type="checkbox"/>	17	
3	<input type="checkbox"/>	500	kbps	<input type="checkbox"/>	17	17%
4	<input type="checkbox"/>	500	kbps	<input type="checkbox"/>	17	17%
5	<input type="checkbox"/>	500	kbps	<input type="checkbox"/>	17	17%
6	<input type="checkbox"/>	500	kbps	<input type="checkbox"/>		
7	<input type="checkbox"/>	500	kbps	<input type="checkbox"/>		

If you select "Weighted" as the scheduler mode then the screen will change as shown in the figure.

Port Shaper		
<b>Enable</b>	<b>Rate</b>	<b>Unit</b>
<input type="checkbox"/>	500	kbps

Apply Reset Cancel

**Parameter descriptions:**

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

**Mode :** Shows the scheduling mode for this port.

**Weight (Qn) :** Shows the weight for this queue and port.

**Scheduler Mode :** Controls whether the scheduler mode is "Strict Priority" or "Weighted" on this switch port.

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

**Queue Shaper Rate :** Controls the rate for the queue shaper. The default value is ?. This value is restricted

to ?-1000000 when the "Unit" is "kbps", and it is restricted to 1-? when the "Unit" is "Mbps".

**Queue Shaper Unit :** Controls the unit of measure for the queue shaper rate as "kbps" or "Mbps". The default value is "kbps".

**Queue Shaper Excess :** Controls whether the queue is allowed to use excess bandwidth.

**Queue Scheduler Weight :** Controls the weight for this queue. The default value is "17". This value is restricted to 1-100. This parameter is only shown if "Scheduler Mode" is set to "Weighted".

**Queue Scheduler Percent :** Shows the weight in percent for this queue. This parameter is only shown if "Scheduler Mode" is set to "Weighted"

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

**Port Shaper Rate :** Controls the rate for the port shaper. The default value is ?. This value is restricted to ?-1000000 when the "Unit" is "kbps", and it is restricted to 1-? when the "Unit" is "Mbps".

**Port Shaper Unit :** Controls the unit of measure for the port shaper rate as "kbps" or "Mbps". The default value is "kbps".

### **Buttons:**

**Apply** – Click to save changes.

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

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

## 2-18.5 Port Shaping

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

### Web Interface

To display the QoS Port Shapers in the web interface:

1. Click Configuration, QoS, Port Shapers.
2. Set the QoS Egress Port Shaper parameters.

**Figure 2-18.5: QoS Egress Port Shapers page**

QoS Egress Port Shapers Home > Configuration > QoS > Port Shaping

Port	Shapers							Port	
	Q0	Q1	Q2	Q3	Q4	Q5	Q6		Q7
1	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled
2	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled
3	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled

Click the Port index to set the QoS Egress Port Shapers

QoS Egress Port Scheduler and Shapers Port 1 Home > Configuration > QoS > Port Scheduler

Port: Port 1

Scheduler Mode: Strict Priority

**Queue Shaper**

Queue	Enable	Rate	Unit	Excess
*	<input type="checkbox"/>	<input style="width: 50px;" type="text" value="500"/>	<span style="border: 1px solid #ccc; padding: 2px;">&lt;&gt; ▾</span>	<input type="checkbox"/>
0	<input type="checkbox"/>	<input style="width: 50px;" type="text" value="500"/>	<span style="border: 1px solid #ccc; padding: 2px;">kbps ▾</span>	<input type="checkbox"/>
1	<input type="checkbox"/>	<input style="width: 50px;" type="text" value="500"/>	<span style="border: 1px solid #ccc; padding: 2px;">kbps ▾</span>	<input type="checkbox"/>
2	<input type="checkbox"/>	<input style="width: 50px;" type="text" value="500"/>	<span style="border: 1px solid #ccc; padding: 2px;">kbps ▾</span>	<input type="checkbox"/>
3	<input type="checkbox"/>	<input style="width: 50px;" type="text" value="500"/>	<span style="border: 1px solid #ccc; padding: 2px;">kbps ▾</span>	<input type="checkbox"/>
4	<input type="checkbox"/>	<input style="width: 50px;" type="text" value="500"/>	<span style="border: 1px solid #ccc; padding: 2px;">kbps ▾</span>	<input type="checkbox"/>
5	<input type="checkbox"/>	<input style="width: 50px;" type="text" value="500"/>	<span style="border: 1px solid #ccc; padding: 2px;">kbps ▾</span>	<input type="checkbox"/>
6	<input type="checkbox"/>	<input style="width: 50px;" type="text" value="500"/>	<span style="border: 1px solid #ccc; padding: 2px;">kbps ▾</span>	<input type="checkbox"/>
7	<input type="checkbox"/>	<input style="width: 50px;" type="text" value="500"/>	<span style="border: 1px solid #ccc; padding: 2px;">kbps ▾</span>	<input type="checkbox"/>

Port Shaper		
<b>Enable</b>	<b>Rate</b>	<b>Unit</b>
<input type="checkbox"/>	500	kbps

QoS Egress Port Scheduler and Shapers Port 1

Home > Configuration > QoS > Port Scheduler

<b>Port</b>	Port 1
<b>Scheduler Mode</b>	Weighted

Queue Shaper				Queue Scheduler	
Queue	Enable	Rate	Unit	Exces	
*	<input type="checkbox"/>	500	<>	<input type="checkbox"/>	
0	<input type="checkbox"/>	500	kbps	<input type="checkbox"/>	
1	<input type="checkbox"/>	500	kbps	<input type="checkbox"/>	17 17%
2	<input type="checkbox"/>	500	kbps	<input type="checkbox"/>	17 17%
3	<input type="checkbox"/>	500	kbps	<input type="checkbox"/>	17 17%
4	<input type="checkbox"/>	500	kbps	<input type="checkbox"/>	17 17%
5	<input type="checkbox"/>	500	kbps	<input type="checkbox"/>	17 17%
6	<input type="checkbox"/>	500	kbps	<input type="checkbox"/>	
7	<input type="checkbox"/>	500	kbps	<input type="checkbox"/>	

If you select Weighted as the scheduler mode then the screen will change as shown in the figure.

Port Shaper		
<b>Enable</b>	<b>Rate</b>	<b>Unit</b>
<input type="checkbox"/>	500	kbps

**Parameter descriptions:**

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

**Mode :** Shows the scheduling mode for this port.

**Shapers (Qn) :** Shows "disabled" or actual queue shaper rate - e.g. "800 Mbps".

**Scheduler Mode :** Controls whether the scheduler mode is "Strict Priority" or "Weighted" on this switch port.

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



**Queue Shaper Rate :** Controls the rate for the queue shaper. The default value is ?. This value is restricted to ?-1000000 when the "Unit" is "kbps", and it is restricted to 1-? when the "Unit" is "Mbps".

**Queue Shaper Unit :** Controls the unit of measure for the queue shaper rate as "kbps" or "Mbps". The default value is "kbps".

**Queue Shaper Excess :** Controls whether the queue is allowed to use excess bandwidth.

**Queue Scheduler Weight :** Controls the weight for this queue. The default value is "17". This value is restricted to 1-100. This parameter is only shown if "Scheduler Mode" is set to "Weighted".

**Queue Scheduler Percent :** Shows the weight in percent for this queue. This parameter is only shown if "Scheduler Mode" is set to "Weighted"

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

**Port Shaper Rate :** Controls the rate for the port shaper. The default value is ?. This value is restricted to 1-1000000 when the "Unit" is "kbps", and it is restricted to 1-99999 when the "Unit" is "Mbps".

**Port Shaper Unit :** Controls the unit of measure for the port shaper rate as "kbps" or "Mbps". The default value is "kbps".

**Buttons:**

**Apply** – Click to save changes.

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

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

## 2-18.6 Port Tag Remarking

This page lets you configure QoS Egress Port Tag Remarking for all switch ports.

### Web Interface

To configure QoS Port Tag Remarking in the web interface:

1. Click Configuration, QoS, Port Tag Remarking.
2. Click the Port index to set QoS Port Tag Remarking.
3. Set the QoS Egress Port Tag Remarking parameters.
4. Click the Apply button when done to save the settings.

**Figure 2-18.6: QoS Egress Port Tag Remarking page**

The screenshot displays the 'QoS Egress Port Tag Remarking' web interface. At the top, a breadcrumb trail reads 'Home > Configuration > QoS > Port Tag Remarking'. Below this is a table with two columns: 'Port' and 'Mode'. The table contains four rows, with the first and fourth rows showing 'Classified' in the 'Mode' column. A red box highlights the '1' in the first row of the 'Port' column, with a blue arrow pointing to a text box that says 'Click the Port index to set the QoS Port Tag Remarking'. Below the table are two configuration panels for 'Port 1'. The first panel has a 'Port' dropdown set to 'Port 1' and a 'Tag Remarking Mode' dropdown set to 'Classified'. The second panel has a 'Port' dropdown set to 'Port 1' and a 'Tag Remarking Mode' dropdown set to 'Default'. Both panels have 'Apply' and 'Reset' buttons at the bottom.

Port	Mode
1	Classified
2	
3	
4	Classified

**QoS Egress Port Tag Remarking Port 1**

Port: Port 1

Tag Remarking Mode: Classified

Apply Reset

**QoS Egress Port Tag Remarking Port 1**

Port: Port 1

Tag Remarking Mode: Default

PCP/DEI Configuration

Default PCP: 0

Default DEI: 0

Apply Reset

QoS Egress Port Tag Remarking Port 1

Home > Configuration > QoS > Port Tag Remarking

<b>Port</b>	Port 1 <input type="button" value="v"/>
<b>Tag Remarking Mode</b>	Mapped <input type="button" value="v"/>

(QoS class, DP level) to (PCP, DEI) Mapping

QoS class	DP level	PCP	DEI
*	*	<> <input type="button" value="v"/>	<> <input type="button" value="v"/>
0	0	1 <input type="button" value="v"/>	0 <input type="button" value="v"/>
0	1	1 <input type="button" value="v"/>	1 <input type="button" value="v"/>
1	0	0 <input type="button" value="v"/>	0 <input type="button" value="v"/>
1	1	0 <input type="button" value="v"/>	1 <input type="button" value="v"/>
2	0	2 <input type="button" value="v"/>	0 <input type="button" value="v"/>
2	1	2 <input type="button" value="v"/>	1 <input type="button" value="v"/>
3	0	3 <input type="button" value="v"/>	0 <input type="button" value="v"/>
3	1	3 <input type="button" value="v"/>	1 <input type="button" value="v"/>
4	0	4 <input type="button" value="v"/>	0 <input type="button" value="v"/>
4	1	4 <input type="button" value="v"/>	1 <input type="button" value="v"/>
5	0	5 <input type="button" value="v"/>	0 <input type="button" value="v"/>
5	1	5 <input type="button" value="v"/>	1 <input type="button" value="v"/>
6	0	6 <input type="button" value="v"/>	0 <input type="button" value="v"/>
6	1	6 <input type="button" value="v"/>	1 <input type="button" value="v"/>
7	0	7 <input type="button" value="v"/>	0 <input type="button" value="v"/>
7	1	7 <input type="button" value="v"/>	1 <input type="button" value="v"/>

Apply

**Parameter descriptions:**

**Mode :** Controls the tag remarking mode for this port.

**Classified:** Use classified PCP/DEI values.

**Default:** Use default PCP/DEI values.

**Mapped:** Use mapped versions of QoS class and DP level.

**PCP/DEI Configuration :** Controls the default PCP and DEI values used when the mode is set to Default.

**(QoS class, DP level) to (PCP, DEI) Mapping :** Controls the mapping of the classified (QoS class, DP level) to (PCP, DEI) values when the mode is set to Mapped.

**Buttons:**

**Apply** – Click to save changes.

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

**Cancel** – Click to cancel the changes.

## 2-18.7 Port DSCP

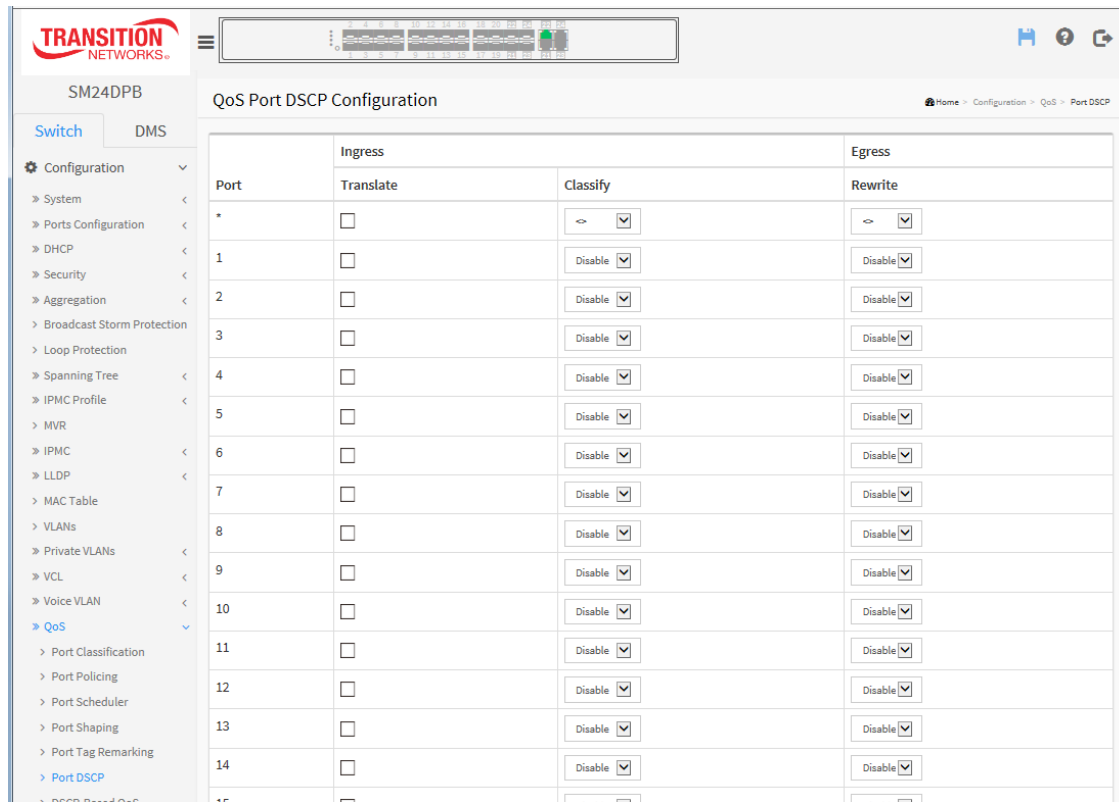
This page lets you set the QoS Port DSCP configuration settings for all switch ports.

### Web Interface

To configure the QoS Port DSCP parameters in the web interface:

1. Click Configuration, QoS, Port DSCP.
2. Enable or disable the Ingress Translate and Scroll the Classify Parameter configuration.
3. Scroll to select Egress Rewrite parameters.
4. Click Apply to save the setting.
5. To cancel the settings click the Reset button to revert to previously saved values.

**Figure 2-18.7: QoS Port DSCP Configuration page**



### Parameter descriptions:

**Port :** Column shows the list of ports which you can configure DSCP ingress and egress settings.

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

**Translate :** To Enable the Ingress Translation click the checkbox

**Classify:** Classification for a port can have one of four values:

**Disable:** No Ingress DSCP Classification.

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

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

**All:** Classify all DSCP.

**Egress** : Port Egress Rewriting can be one of these parameters:

***Disable***: No Egress rewrite.

***Enable***: Rewrite enable without remapped.

***Remap***: DSCP from analyzer is remapped and frame is remarked with remapped DSCP value.

**Buttons:**

**Apply** – Click to save changes.

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

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

**Refresh**: Click to immediately refresh the QoS Port DSCP information manually.

## 2-18.8 DSCP-Based QoS

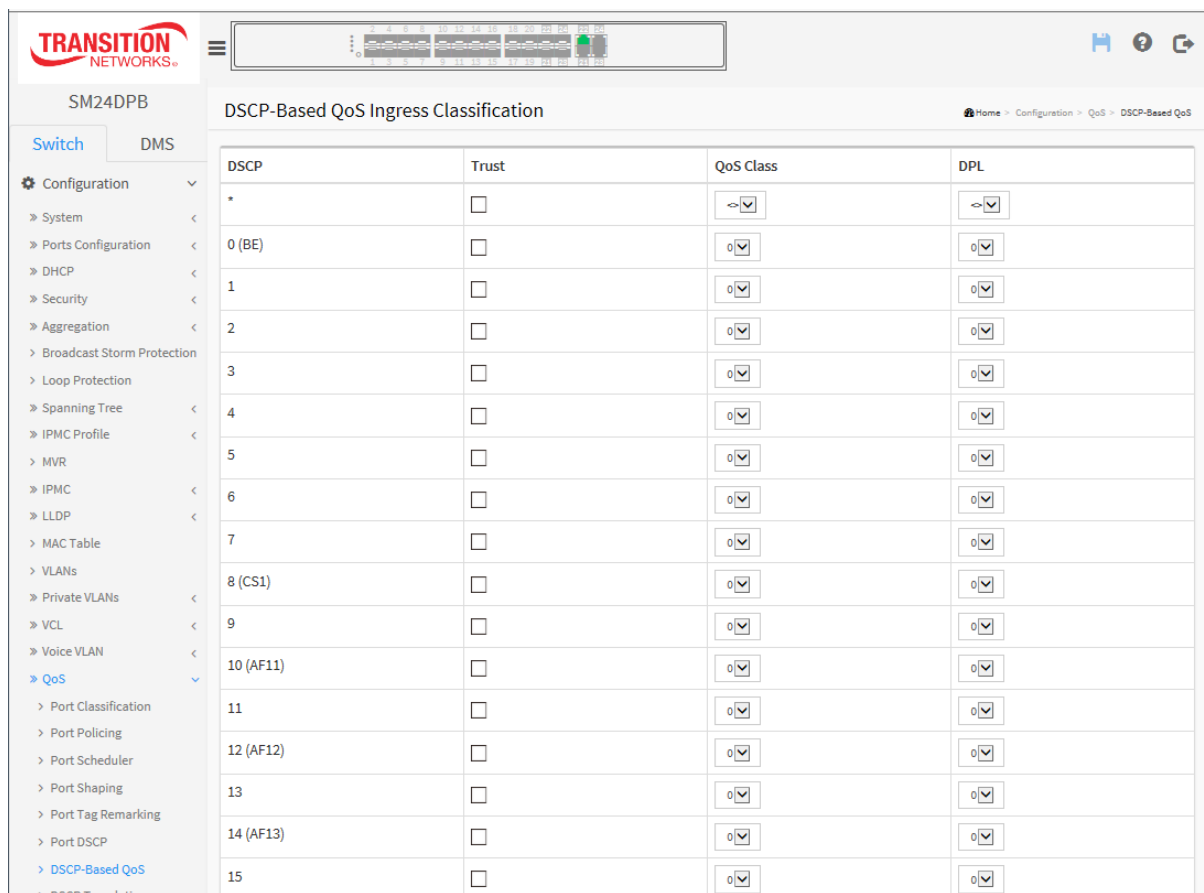
This page lets you configure basic QoS DSCP based QoS Ingress Classification settings for all switches.

### Web Interface

To configure the DSCP –Based QoS Ingress Classification parameters:

1. Click Configuration, QoS, DSCP-Based QoS.
2. Enable or disable the DSCP for Trust.
3. Scroll to select QoS Class and DPL parameters.
4. Click Apply to save the setting
5. To cancel the settings click the Reset button to revert to previously saved values.

**Figure 2-18.8: DSCP-Based QoS Ingress Classification page**



### Parameter descriptions:

**DSCP** : Maximum number of supported DSCP values are 64.

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

**QoS Class** : QoS Class value can be 0-7

**DPL** : Drop Precedence Level (0-3)

**Buttons:**

**Apply** – Click to save changes.

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

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

**Refresh**: You can click to immediately refresh the page manually.



### 2-18.9 DSCP Translation

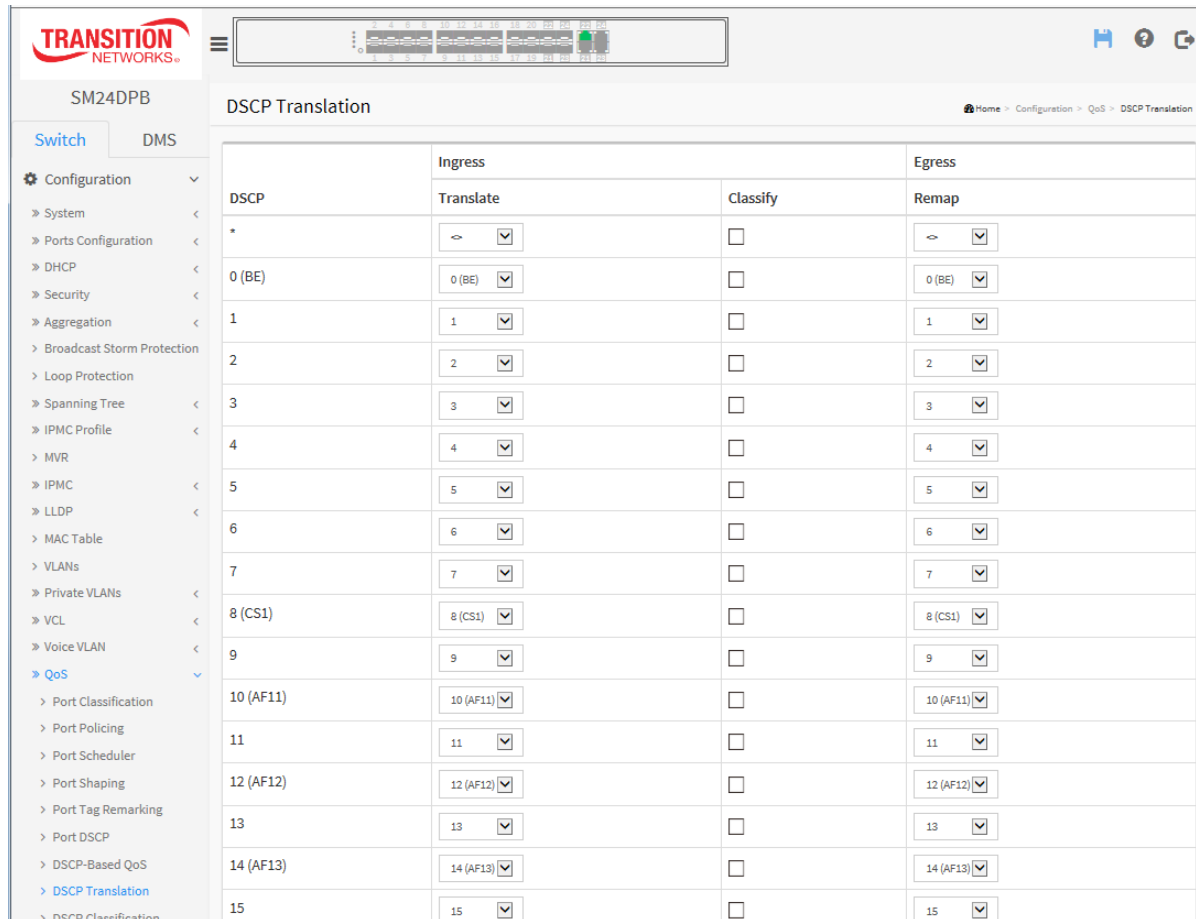
This page lets you configure the basic QoS DSCP Translation settings for the switch. DSCP translation can be done in Ingress or Egress.

#### Web Interface

To configure the DSCP Translation parameters in the web interface:

1. Click Configuration, QoS, DSCP Translation.
2. Set the Ingress Translate and Egress Remap DP0 and Remap DP1 Parameters.
3. Enable or disable Classify.
4. Click Apply to save the settings.
5. To cancel the setting click the Reset button to revert to previously saved values.

**Figure 2-18.9: DSCP Translation page**



#### Parameter descriptions:

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

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

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

**Classify :** Click to enable Classification at Ingress side.

**Egress :** There are following configurable parameters for Egress side –

**Remap DP0** : Select the DSCP value from select menu to which you want to remap. DSCP value ranges from 0 to 63

**Remap DP1** : Select the DSCP value from select menu to which you want to remap. DSCP value ranges from 0 to 63.

There is one configurable parameter for Egress side:

**Remap**: Select the DSCP value from select menu to which you want to remap. DSCP value ranges from 0 to 63.

### **Buttons:**

**Apply** – Click to save changes.

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

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

**Refresh**: Click to immediately refresh the DSCP Translation information manually.

## 2-18.10 DSCP Classification

This page lets you map DSCP value to a QoS Class and DPL value.

### Web Interface

To configure the DSCP Classification parameters in the web interface:

1. Click Configuration, QoS, DSCP Translation.
2. Set the DSCP parameters
3. Click Apply to save the settings.
4. To cancel the setting click the Reset button to revert to previously saved values.

**Figure 2-18.10: DSCP Classification page**

The screenshot shows the web interface for SM24DPB. The left sidebar contains a navigation menu with categories like Configuration, System, Ports Configuration, DHCP, Security, Aggregation, Broadcast Storm Protection, Loop Protection, Spanning Tree, IPMC Profile, MVR, IPMC, LLDP, MAC Table, VLANs, Private VLANs, VCL, Voice VLAN, QoS, Port Classification, Port Policing, Port Scheduler, Port Shaping, Port Tag Remarking, Port DSCP, DSCP-Based QoS, DSCP Translation, and DSCP Classification. The main content area is titled 'DSCP Classification' and contains a table with the following data:

QoS Class	DSCP
*	0 (BE) [v]
0	0 (BE) [v]
1	0 (BE) [v]
2	0 (BE) [v]
3	0 (BE) [v]
4	0 (BE) [v]
5	0 (BE) [v]
6	0 (BE) [v]
7	0 (BE) [v]

Below the table are two buttons: 'Apply' (blue) and 'Reset' (orange).

### Parameter descriptions:

**QoS Class** : Available QoS Class value ranges from 0 to 7. QoS Class (0-7) can be mapped to followed parameters.

**DPL** : Drop Precedence Level (0-1) can be configured for all available QoS Classes.

**DSCP** : Select DSCP value (0-63) from DSCP menu to map DSCP to corresponding QoS Class and DPL value

### Buttons:

**Apply** : Click to save changes.


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

### 2-18.11 QoS Control List Configuration

This page lets you configure QoS Control List (QCL), which is made up of the QCEs. Each row describes a QCE that is defined. The maximum number of QCEs is 256 on each switch. Click on the lowest plus sign to add a new QCE to the list.

#### Web Interface

To configure the QoS Control List parameters in the web interface:

1. Click Configuration, QoS, QoS Control List
2. Click the  to add a new QoS Control List.
3. Scroll all parameters and check the Port Member to join the QCE rules.
4. Click Apply to save the settings.
5. To cancel the settings click the Reset button to revert to previously saved values.

**Figure 2-18.11: QoS Control List Configuration page**

**Parameter descriptions:**

**QCE# :** Indicates the index of QCE.

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

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

**Any:** Match any DMAC. The default value is 'Any'.

**Unicast:** Match unicast DMAC.

**Multicast:** Match multicast DMAC.

**Broadcast:** Match broadcast DMAC.

**<MAC>:** Match specific DMAC.

**SMAC :** Match specific source MAC address or 'Any'. If a port is configured to match on DMAC/DIP, this field indicates the DMAC.

**Tag Type :** Indicates tag type. Possible values are:

**Any:** Match tagged and untagged frames.

**Untagged:** Match untagged frames.

**Tagged:** Match tagged frames.

**C-Tagged:** Match C-tagged frames.

**S-Tagged:** Match S-tagged frames.

The default value is 'Any'.

**VID :** Indicates (VLAN ID), either a specific VID or range of VIDs. VID can be 1-4095 or 'Any'

**PCP :** Priority Code Point: Valid values of PCP are specific(0, 1, 2, 3, 4, 5, 6, 7) or range(0-1, 2-3, 4-5, 6-7, 0-3, 4-7) or 'Any'.

**DEI :** Drop Eligible Indicator: Valid value of DEI are 0, 1 or 'Any'.

**Frame Type :** Indicates the type of frame to look for incoming frames. Possible frame types are:

**Any:** The QCE will match all frame type.

**Ethernet:** Only Ethernet frames (with Ether Type 0x600-0xFFFF) are allowed.

**LLC:** Only (LLC) frames are allowed.

**SNAP:** Only (SNAP) frames are allowed

**IPv4:** The QCE will match only IPV4 frames.

**IPv6:** The QCE will match only IPV6 frames.

**Action :** Indicates the classification action taken on ingress frame if parameters configured are matched with the frame's content. There are three action fields: Class, DPL and DSCP.

**Class:** Classified QoS Class; if a frame matches the QCE it will be put in the queue.

**DPL:** Drop Precedence Level; if a frame matches the QCE then DP level will set to value displayed under DPL column.

**DSCP:** If a frame matches the QCE then DSCP will be classified with the value displayed under DSCP column.

**Modification buttons :** You can modify each QCE (QoS Control Entry) in the table using these buttons:



: Inserts a new QCE before the current row.



: Edits the QCE.



: Moves the QCE up the list.



: Moves the QCE down the list.



: Deletes the QCE.



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

**Port Members :** Check the checkbox button in case you want to make any port member of the QCL entry. By default all ports will be checked.

**Key Parameters :** Key configuration are described as below:

**Tag** Value of Tag field can be 'Any', 'Untag' or 'Tag'

**VID** Valid value of VLAN ID can be any value in the range 1-4095 or 'Any'; user can enter either a specific value or a range of VIDs.

**PCP** Priority Code Point: Valid value PCP are specific(0, 1, 2, 3, 4, 5, 6, 7) or range(0-1, 2-3, 4-5, 6-7, 0-3, 4-7) or 'Any'

**DEI** Drop Eligible Indicator: Valid value of DEI can be any of values between 0, 1 or 'Any'

**SMAC** Source MAC address: 24 MS bits (OUI) or 'Any'

**DMAC** Type Destination MAC type: possible values are unicast(UC), multicast(MC), broadcast(BC) or 'Any'

**Frame Type:** can have these values: Any, Ethernet, LLC, SNAP, IPv4 or IPv6.



NOTE: All frame types are explained below:

**Any :** Allow all types of frames.

**Ethernet :** Ethernet Type Valid ethernet type can have value within 0x600-0xFFFF or 'Any', default value is 'Any'.

**LLC:** SSAP Address Valid SSAP(Source Service Access Point) can vary from 0x00 to 0xFF or 'Any', the default value is 'Any'

DSAP Address Valid DSAP(Destination Service Access Point) can vary from 0x00 to 0xFF or 'Any', the default value is 'Any'

Control Address Valid Control Address can vary from 0x00 to 0xFF or 'Any', the default value is 'Any'

**SNAP :** PID Valid PID(a.k.a ethernet type) can have value within 0x00-0xFFFF or 'Any', default value is 'Any'

**IPv4 :** Protocol IP protocol number: (0-255, TCP or UDP) or 'Any' Source IP Specific Source IP address in value/mask format or 'Any'. IP and Mask are in the format x.y.z.w where x, y, z, and w are decimal numbers between 0 and 255. When Mask is converted to a 32-bit binary string and read from left to right, all bits following the first zero must also be zero DSCP Diffserv Code Point value(DSCP): It can be specific value, range of value or 'Any'. DSCP values are in the range 0-63 including BE, CS1-CS7, EF or AF11-AF43 IP Fragment IPv4 frame fragmented option: yes|no|any

Sport Source TCP/UDP port:(0-65535) or 'Any', specific or port range applicable for IP protocol UDP/TCP

Dport Destination TCP/UDP port:(0-65535) or 'Any', specific or port range applicable for IP protocol UDP/TCP

**IPv6 :** Protocol IP protocol number: (0-255, TCP or UDP) or 'Any'.

Source IP IPv6 source address: (a.b.c.d) or 'Any', 32 LS bits

DSCP Diffserv Code Point value(DSCP): It can be specific value, range of value or 'Any'.

DSCP values are in the range 0-63 including BE, CS1-CS7, EF or AF11-AF43

Sport Source TCP/UDP port:(0-65535) or 'Any', specific or port range applicable for IP protocol UDP/TCP

---

Dport Destination TCP/UDP port:(0-65535) or 'Any', specific or port range applicable for IP protocol UDP/TCP

---

**Action Configuration :** Class QoS Class: "class (0-7)", default- basic classification

**DP :** Valid DP Level can be (0-3)", default- basic classification

**DSCP :** Valid DSCP values can be (0-63, BE, CS1-CS7, EF or AF11-AF43)

**Buttons:**

**Apply** – Click to save changes.

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

### 2-18.12 Storm Control

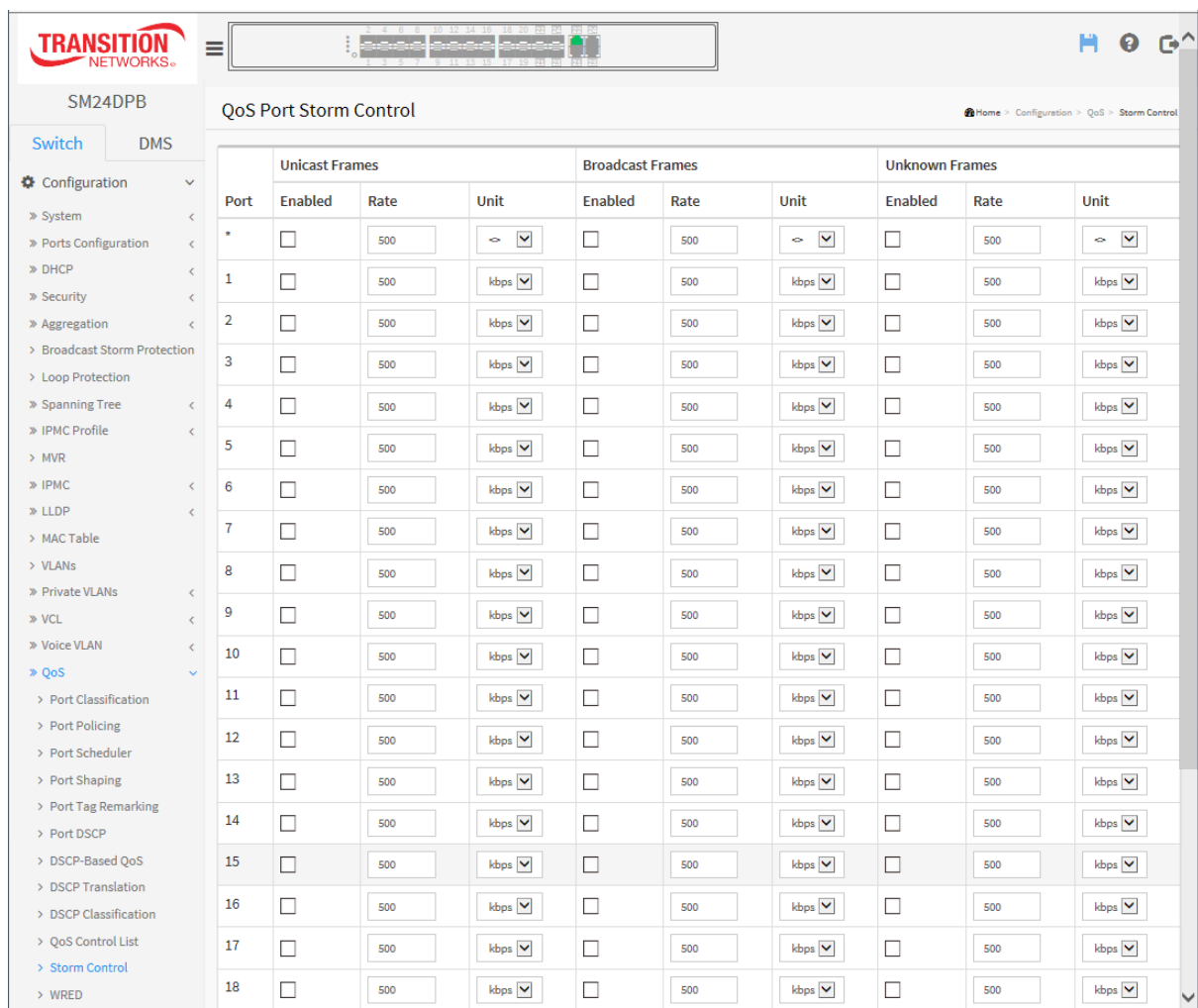
This page lets you configure Storm control. There is a unicast storm rate control, multicast storm rate control, and a broadcast storm rate control. These only affect flooded frames, i.e. frames with a (VLAN ID, DMAC) pair not present on the MAC Address table. The configuration indicates the permitted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

#### Web Interface

To configure QoS Storm Control parameters in the web interface:

1. Click Configuration, QoS, Storm Control.
2. Select the frame type to enable storm control.
3. Set the Rate parameters.
4. Click Apply to save the settings.
5. To cancel the settings click the Reset button to revert to previously saved values.

**Figure 2-18.12: QoS Port Storm Control page**



#### Parameter descriptions:

**Frame Type :** The settings in a particular row apply to the frame type ( Unicast, Multicast or Broadcast).



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

**Rate** : The rate unit is packets per second (pps). Valid values are: 1, 2, 4, 8, 16, 32, 64, 128, 256, 512, 1K, 2K, 4K, 8K, 16K, 32K, 64K, 128K, 256K, 512K or 1024K. , 1024K, 2048K, 4096K, 8192K, 16384K or 32768K, 1024K, 2048K, 4096K, 8192K, 16384K or 32768K. The 1 kpps is actually 1002.1 pps.

**Unit** : Controls the unit of measure for the storm control rate as kbps, Mbps, fps or kfps . The default value is "kbps".

**Buttons:**

**Apply** – Click to save changes immediately.

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

## 2-18.13 WRED

This page lets you configure the WRED function for the switch. This page lets you configure the Random Early Detection (RED) settings for queues 0 to 5. RED cannot be applied to queue 6 and 7. Through different RED configuration for the queues (QoS classes) it is possible to obtain Weighted Random Early Detection (WRED) operation between queues.

Weighted Random Early Detection (WRED) is an active queue management mechanism that provides preferential treatment of higher priority frames when traffic builds up within a queue. A frame's DP level is used as input to WRED. A higher DP level assigned to a frame results in a higher probability that the frame is dropped during times of congestion.

The settings are global for all ports in the switch.

### Web Interface

To configure the WRED Configuration parameters in the web interface:

1. Click Configuration, QoS, WRED.
2. Select enable or disable WRED.
3. Enter each parameter value.
4. Click Apply to save the setting
5. To cancel the setting click the Reset button to revert to previously saved values.

**Figure 2-18.13: WRED Configuration page**

Queue	Enable	Min. Threshold	Max. DP 1	Max. DP 2	Max. DP 3
0	<input type="checkbox"/>	0	1	5	10
1	<input type="checkbox"/>	0	1	5	10
2	<input type="checkbox"/>	0	1	5	10
3	<input type="checkbox"/>	0	1	5	10
4	<input type="checkbox"/>	0	1	5	10
5	<input type="checkbox"/>	0	1	5	10

### Parameter descriptions:

**Queue :** The queue number (QoS class) for which the configuration below applies.

**Enable :** Enable or disable the WRED function on the switch QoS Queue.

**Min. Threshold :** Controls the lower RED threshold. If the average queue filling level is below this threshold, the drop probability is zero. This value is restricted to 0-100.

**Max. DP1 :** Controls the drop probability for frames marked with **Drop Precedence Level 1** when the average queue filling level is 100%. This value is restricted to 0-100.

**Max. DP2 :** Controls the drop probability for frames marked with **Drop Precedence Level 2** when the average queue filling level is 100%. This value is restricted to 0-100.

**Max. DP3** : Controls the drop probability for frames marked with Drop Precedence Level 3 when the average queue filling level is 100%. This value is restricted to 0-100.

**Buttons:**

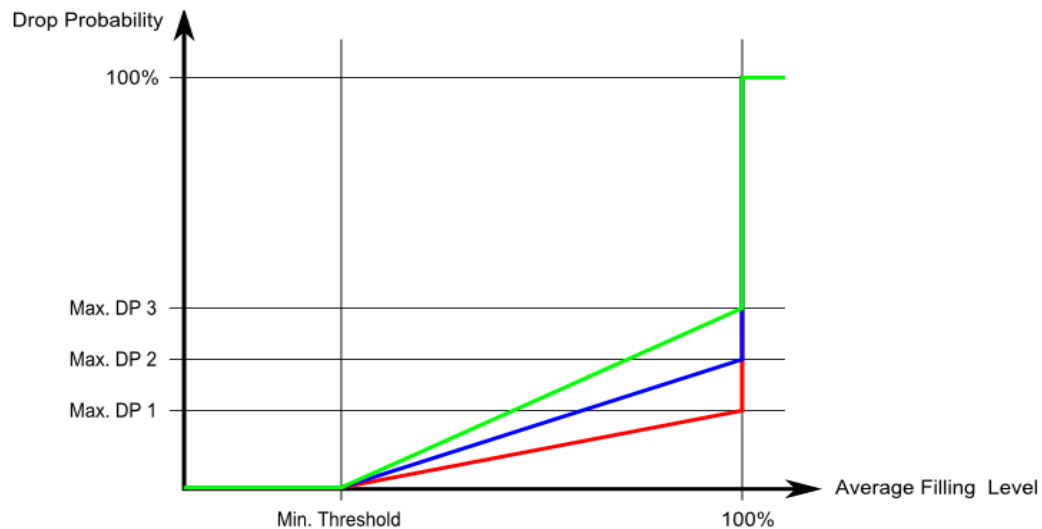
**Apply** – Click to save changes.

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



**NOTE: RED Drop Probability Function**

The figure below shows the drop probability function with associated parameters.



Max. DP 1-3 is the drop probability when the average queue filling level is 100%.

Frames marked with Drop Precedence Level 0 are never dropped. Min. Threshold is the average queue filling level where the queues randomly start dropping frames.

The drop probability for frames marked with Drop Precedence Level n increases linearly from zero (at Min. Threshold average queue filling level) to Max. DP n (at 100% average queue filling level).

## 2-19 Mirroring

Configure port Mirroring on this page.

To debug network problems, selected traffic can be copied, or mirrored, on a mirror port where a frame analyzer can be attached to analyze the frame flow.

The traffic to be copied on the mirror port is selected as follows:

- All frames received on a given port (also known as ingress or source mirroring).
- All frames transmitted on a given port (also known as egress or destination mirroring).

### Web Interface

To configure the Mirror in the web interface:

1. Click Configuration, Mirroring.
2. Select Port to mirror on which port.
3. Scroll to disabled, enable, TX Only and RX Only to set the Port mirror mode.
4. Click Apply to save the settings.
5. To cancel the settings click the Reset button to revert to previously saved values.

**Figure 2-19: Mirror Configuration page**

Port	Mode
*	↔
1	Rx only
2	Tx only
3	Enabled
4	Rx only
5	Enabled
6	Disabled
7	Disabled
8	Disabled
9	Disabled
10	Disabled

### Parameter descriptions:

**Port to mirror on :** Port to mirror also known as the mirror port. Frames from ports that have either source (rx) or destination (tx) mirroring enabled are mirrored on this port. Disabled disables mirroring.

**Mirror Port Configuration :** The following parameters are used for Rx and Tx enabling.

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

**Mode :** Select mirror mode.

**Rx only** : Frames received on this port are mirrored on the mirror port. Frames transmitted are not mirrored.

**Tx only** : Frames transmitted on this port are mirrored on the mirror port. Frames received are not mirrored.

**Disabled** : Neither frames transmitted nor frames received are mirrored.

**Enabled** : Frames received and frames transmitted are mirrored on the mirror port.



---

**NOTE:** For a given port, a frame is only transmitted once. It is therefore not possible to mirror Tx frames on the mirror port. Because of this, mode for the selected mirror port is limited to Disabled or Rx only.

---

### Buttons:

**Apply** – Click to save changes.

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

## 2-20 UPnP

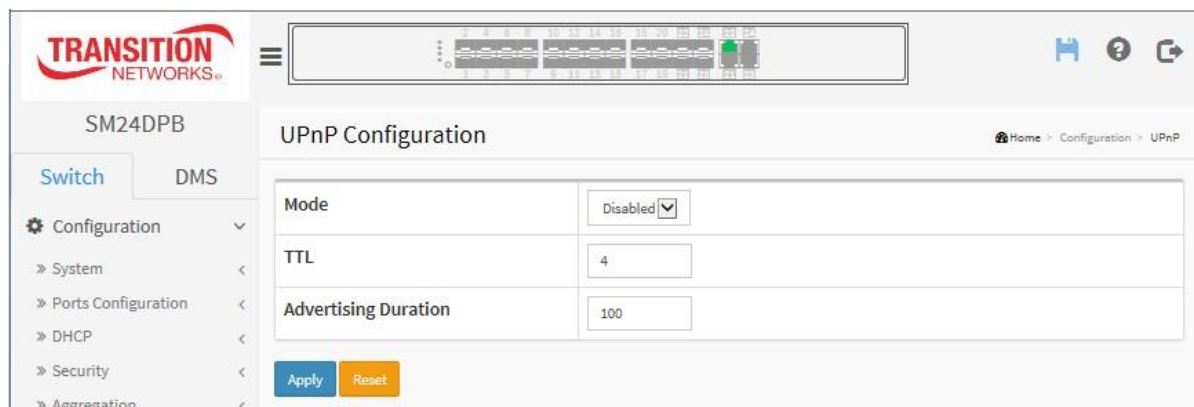
UPnP (Universal Plug and Play) allows devices to connect seamlessly and simplifies the implementation of networks in the home (data sharing, communications, and entertainment) and in corporate environments for simplified installation of computer components. **Caution:** UPnP allows clients in the local network to automatically configure the device. UPnP should only be used (enabled) if necessary and with preventive measures as it can result in high security risks for your network.

### Web Interface

To configure the UPnP Configuration in the web interface:

1. Click Configuration, UPnP
2. Scroll to select the mode to enable or disable
3. Specify the parameters in each blank field.
4. Click Apply to save the setting
5. To cancel the settings click the Reset button. It will revert to previously saved values.

**Figure 2-20: The UPnP Configuration page**



### Parameter descriptions:

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

**Enabled:** Enable UPnP mode operation.

**Disabled:** Disable UPnP mode operation.

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

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

**Advertising Duration :** The duration, carried in SSDP packets, is used to inform a control point or control points how often it or they should receive an SSDP advertisement message from this switch.

If a control point does not receive any message within the duration, it will think that the switch no longer exists.

Due to the unreliable nature of UDP, in the standard it is recommended that such refreshing of advertisements to be done at less than one-half of the advertising duration. 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.

### Buttons:

**Apply** – Click to save changes.

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

## 2-21. GVRP

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

GARP defines the architecture, rules of operation, state machines and variables for the registration and de-registration of attribute values.

A GARP participation in a switch or an end station consists of a GARP application component, and a GARP Information Declaration (GID) component associated with each port or the switch.

The propagation of information between GARP participants for the same application in a bridge is carried out by the GARP Information Propagation (GIP) component. Protocol exchanges take place between GARP participants by means of LLC Type 1 services, using the group MAC address and PDU format defined for the GARP application concerned.

### 2-21.1 Global Config

The switch stores its configuration in a number of text files in CLI format. The files are either virtual (RAM-based) or stored in flash on the switch. There are three system files:

- **running-config:** A virtual file representing the currently active config on the switch. This file is volatile.
- **startup-config:** The startup configuration for the switch, read at boot time.
- **default-config:** A read-only file with vendor-specific configuration. This file is read when the system is restored to default settings.

It is also possible to store up to two other files and apply them to running-config, thereby switching configuration.

### Web Interface

To configure the GVRP in the web interface:

1. Click Configuration, GVRP, Global Config.
2. Check the Enable GVRP checkbox.
2. Specify Join-time, Leave-time, Leave All-time, and Max VLANs.
3. Click Apply.

**Figure 2-21.1: GVRP Configuration page**

Parameter	Value
Enable GVRP	<input type="checkbox"/>
Join-time:	20 (1-20)
Leave-time:	60 (60-300)
LeaveAll-time:	1000 (1000-5000)
Max VLANs:	20

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

### **GVRP Protocol Timers**

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

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

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

### **Max VLANs**

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

### **Buttons**

**Apply** – Click to save changes.

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

**Refresh**: Click to save changes.



## 2-21.2 Port Config

This page allows you to enable or disable a port for GVRP operation.

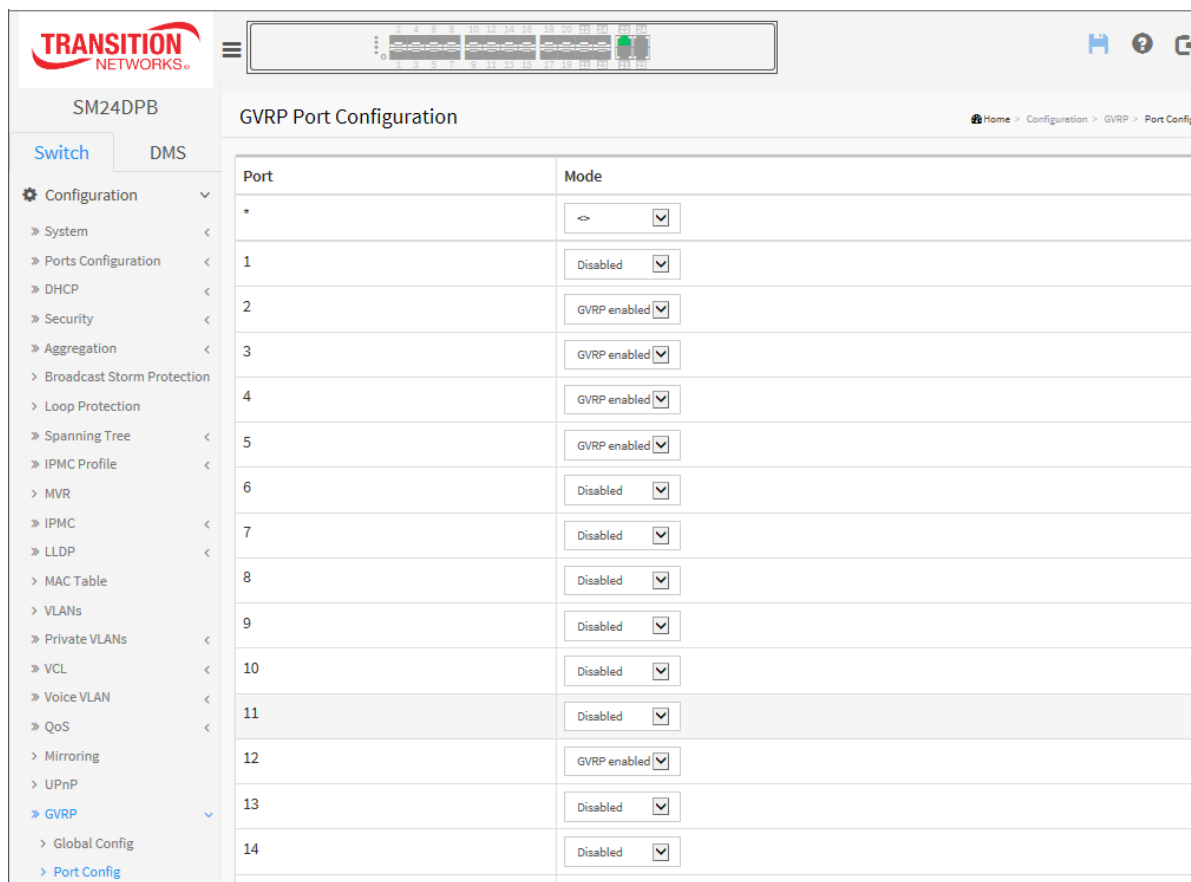
This configuration can be performed either before or after GVRP is configured globally - the protocol operation will be the same.

### Web Interface

To configure GVRP Port parameters in the web interface:

1. Click Configuration, GVRP, Port Config.
2. Specify the Mode for each port.
3. Click Apply.

**Figure 2-21.2: GVRP Port Configuration page**



### Parameter descriptions:

**Port** : The logical port that is to be configured.

**Mode** : Select either 'Disabled' or 'GVRP enabled'. These values turn the GVRP feature off or on respectively for the port in question.

## **Buttons**

**Apply** : Click to save changes.

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

## 2-22. sFlow

This page allows for configuring sFlow. The configuration is divided into two parts: Configuration of the sFlow receiver (a.k.a. sFlow collector) and configuration of per-port flow and counter samplers.

sFlow configuration is not persisted to non-volatile memory, which means that a reboot will disable sFlow sampling.

sFlow is an industry standard technology for monitoring switched networks through random sampling of packets on switch ports and time-based sampling of port counters. The sampled packets and counters (referred to as flow samples and counter samples, respectively) are sent as sFlow UDP datagrams to a central network traffic monitoring server. This central server is called an sFlow receiver or sFlow collector. Additional information can be found at <http://sflow.org>.

### Web Interface

To configure the sFlow Agent in the web interface:

1. Click Configuration, sFlow.
2. Set the Agent, Receiver, and Port Configuration parameters.
3. Click the Apply button to save the settings.
4. To cancel the settings click the Reset button to revert to previously saved values.

Figure 2-22: sFlow Configuration page

The screenshot shows the sFlow Configuration page in the SM24DPB web interface. The page is divided into three main sections: Agent Configuration, Receiver Configuration, and Port Configuration.

**Agent Configuration:**

- IP Address: 127.0.0.1

**Receiver Configuration:**

- Owner: <none> (Release button)
- IP Address/Hostname: 0.0.0.0
- UDP Port: 6343
- Timeout: 0 seconds
- Max. Datagram Size: 1400 bytes

**Port Configuration:**

Port	Flow Sampler				Counter Poller	
	Enabled	Sampler Type	Sampling Rate	Max. Header	Enabled	Interval
*	<input type="checkbox"/>	<=>	0	128	<input type="checkbox"/>	0
1	<input type="checkbox"/>	Tx	0	128	<input type="checkbox"/>	0
2	<input type="checkbox"/>	Tx	0	128	<input type="checkbox"/>	0
3	<input type="checkbox"/>	Tx	0	128	<input type="checkbox"/>	0
4	<input type="checkbox"/>	Tx	0	128	<input type="checkbox"/>	0
5	<input type="checkbox"/>	Tx	0	128	<input type="checkbox"/>	0
6	<input type="checkbox"/>	Tx	0	128	<input type="checkbox"/>	0
7	<input type="checkbox"/>	Tx	0	128	<input type="checkbox"/>	0

**Parameter descriptions:****Agent Configuration**

**IP Address :** The IP address used as Agent IP address in sFlow datagrams. It serves as a unique key that will identify this agent over extended periods of time. Both IPv4 and IPv6 addresses are supported.

**Receiver Configuration**

**Owner :** Basically, sFlow can be configured in two ways: Through local management using the Web or CLI interface or through SNMP. This read-only field shows the owner of the current sFlow configuration and assumes values as follows:

- If sFlow is currently unconfigured/unclaimed, Owner contains <none>.
- If sFlow is currently configured through Web or CLI, Owner contains <Configured through local management>.
- If sFlow is currently configured through SNMP, Owner contains a string identifying the sFlow receiver. If sFlow is configured through SNMP, all controls - except for the Release-button - are disabled to avoid inadvertent reconfiguration.

The **Release** button allows for releasing the current owner and disable sFlow sampling. The **Release** button is disabled if sFlow is currently unclaimed. If configured through SNMP, the release must be confirmed (a confirmation request will appear).

**IP Address/Hostname :** The IP address or hostname of the sFlow receiver. Both IPv4 and IPv6 addresses are supported.

**UDP Port :** The UDP port on which the sFlow receiver listens to sFlow datagrams. If set to 0 (zero), the default port (6343) is used.

**Timeout :** The number of seconds remaining before sampling stops and the current sFlow owner is released. While active, the current time left can be updated with a click on the Refresh-button. If locally managed, the timeout can be changed on the fly without affecting any other settings.

**Max. Datagram Size :** The maximum number of data bytes that can be sent in a single sample datagram. This should be set to a value that avoids fragmentation of the sFlow datagrams. Valid range is 200 to 1468 bytes with default being 1400 bytes.

**Port Configuration**

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

**Flow Sampler Enabled :** Enables/disables flow sampling on this port.

**Flow Sampler Sampling Rate :** The statistical sampling rate for packet sampling. Set to N to sample on average 1/Nth of the packets transmitted/received on the port.

Not all sampling rates are achievable. If an unsupported sampling rate is requested, the switch will automatically adjust it to the closest achievable. This will be reported back in this field.

**Flow Sampler Max. Header :** The maximum number of bytes that should be copied from a sampled packet to the sFlow datagram. Valid range is 14 to 200 bytes with default being 128 bytes. If the maximum datagram size does not take into account the maximum header size, samples may be dropped.

**Counter Poller Enabled :** Enables/disables counter polling on this port.

**Counter Poller Interval :** With counter polling enabled, this specifies the interval - in seconds - between counter poller samples.

**Buttons:**

**Apply** – Click to save changes.

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

**Release** : See description under **Owner** above.

**Refresh** : Click to refresh the page. Note that unsaved changes will be lost.

## 2-23 Rapid Ring Configuration

This page lets you configure and view current Rapid Ring parameters. STP must be disabled.

The screenshot shows the 'Rapid Ring Configuration' page for device SM24DPB. The page title is 'Rapid Ring Configuration' and the breadcrumb trail is 'Home > Configuration > Rapid > Ring'. The main content area is titled 'Global Configuration' and contains a table with the following data:

Index	Role	Port	Status
1	Master	1	Forwarding
		2	Forwarding
2	Member	3	Forwarding
		4	Forwarding
3	Member	5	Forwarding
		6	Forwarding
4	Member	7	Forwarding
		8	Forwarding
5	Member	9	Forwarding
		10	Forwarding
6	Member	11	Forwarding
		12	Forwarding
7	Disabled	13	Forwarding
		14	Forwarding
8	Disabled	15	Forwarding
		16	Forwarding
9	Disabled	17	Forwarding
		18	Forwarding
10	Disabled	19	Forwarding

**Role:** Set role value.

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

**Status:** The current Rapid Ring status of the port.

### Buttons

**Apply:** Click to apply changes.

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

**Previous:** Click to clear the message and then disable Spanning Tree at Configuration > Spanning Tree > CIST Port.

### Messages:

*Error in port 1, STP is enable*

## 2-24 SMTP Configuration

Configure SMTP (Simple Mail Transfer Protocol) on this page. Simple Mail Transfer Protocol is the message-exchange standard for the Internet.

The switch is to be configured as a client of SMTP while the server is a remote device that will receive messages from the switch that alarm events occurred.

### Web Interface

To configure the sFlow Agent in the web interface:

1. Click Configuration, SMTP.
2. Enter the Mail Server, User Name, Password, Sender, Return Path, and Email Address.
3. Click the Apply button to save the settings.
4. To cancel the settings click the Reset button to revert to previously saved values.

Figure 2-24: SMTP Configuration page

The screenshot displays the SMTP Configuration page in the Transition Networks web interface. The page title is "SMTP Configuration" and the breadcrumb trail is "Home > Configuration > SMTP". The interface includes a navigation menu on the left with "Switch" and "DMS" tabs, and a "Configuration" section expanded to show various settings. The main configuration area contains the following fields:

Mail Server	<input type="text"/>
User Name	<input type="text" value="admin"/>
Password	<input type="password" value="....."/>
Sender	<input type="text"/>
Return Path	<input type="text"/>
Email Address 1	<input type="text"/>
Email Address 2	<input type="text"/>
Email Address 3	<input type="text"/>
Email Address 4	<input type="text"/>
Email Address 5	<input type="text"/>
Email Address 6	<input type="text"/>

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

### Parameter descriptions:

**Mail Server:** The IP address or hostname of the SMTP mail server. IP address is expressed in dotted decimal notation. This will be the device that sends the e-mail out.

**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 for up to six recipients.

### **Buttons**

**Apply:** Click to apply changes.

**Reset:** Click to undo any changes made locally and revert to previously saved values.



# Chapter 3. Monitor

This chapter describes the modules that you can view (monitor) after configuring the modules as described in the previous chapter. The modules include System, Ports, Security, LACP, Spanning Tree, VLANs, etc.

## 3-1 System

After you login, the switch displays the System Information page. This page displays by default and shows basic information of the system, including Model Name, System Description, System Up Time, Firmware Version, etc.

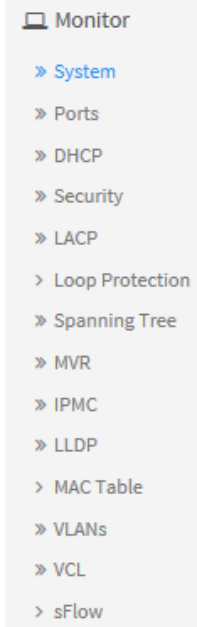
### 3-1.1 Information

The switch system information is provided here.

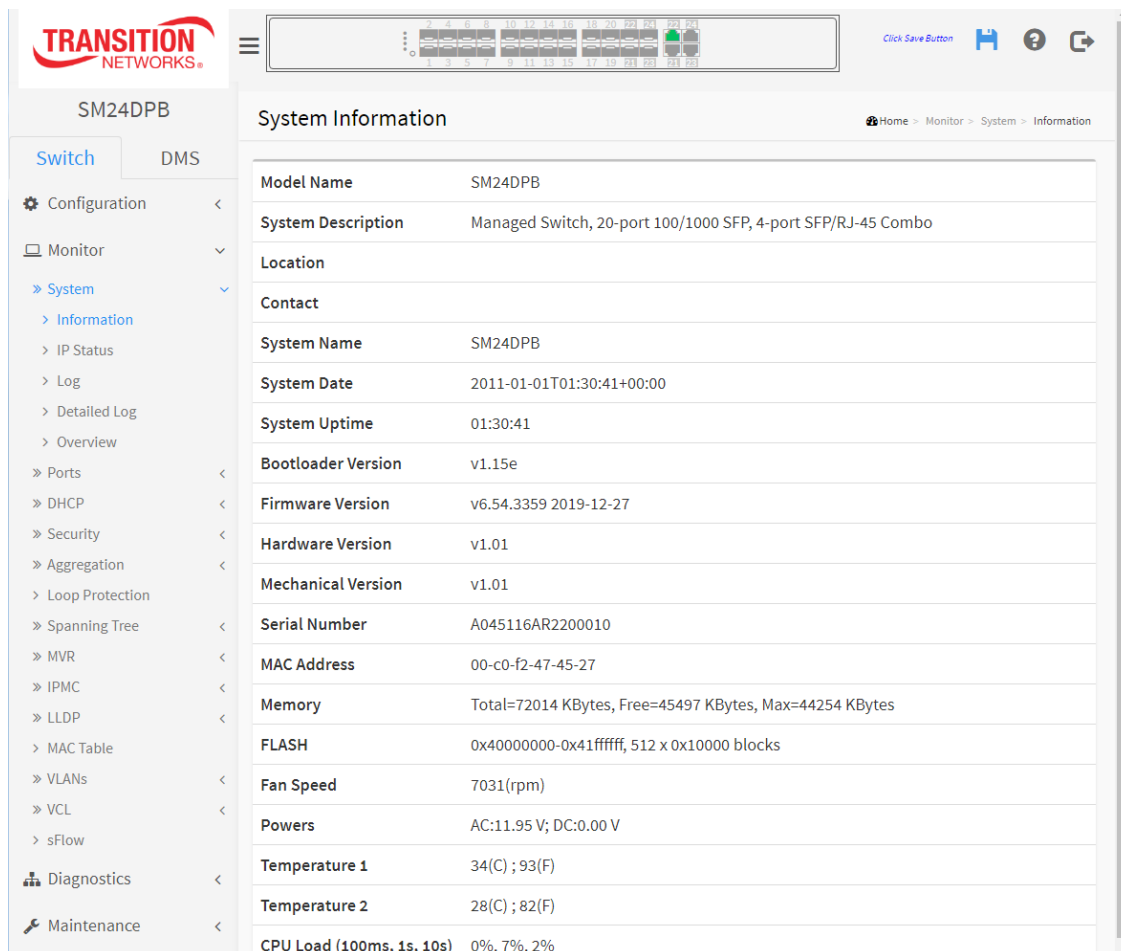
#### Web interface

To view System Information in the web interface:

1. Click Monitor, System, Information.
2. Check the information.



**Figure 3-1.1: System Information page**



**Parameter descriptions:** The information displayed on this page will be important to have available before calling Transition Networks Technical Support.

**Model Name:** Model Name displays **SM24DPB**.

**System Description :** Displays the system description (e.g., *Managed Switch, 20-port 100/1000 SFP, 4-port SFP/RJ-45 Combo*)

**Location :** The system location configured at Configuration > System > Information > System Location.

**Contact :** The system contact configured at Configuration > System > Information > System Contact.

**System Name :** Displays the system name that configured at System > System Information > Configuration > System Name. Displays SM24DPB by default.

**System Date :** The current (GMT) system time and date. The system time is obtained through the Timing server running on the switch, if any.

**System Uptime :** The period of time the device has been operational (e.g., *3d 05:11:00*).

**Bootloader Version :** Displays the current boot loader version number (e.g., *v1.15e*).

**Firmware Version :** The software version and date of this switch (e.g., *v6.54.3359 2019-12-27*).

**Hardware Version and Mechanical Version :** The hardware and mechanical version of this switch (e.g., *v1.01*).

**Serial Number :** The serial number of this switch (e.g., *A045116AR0600001*).

**MAC Address :** The MAC Address of this switch (e.g., *00-c0-f2-46-ce-fd*).

**Memory :** Displays the memory size of the system (e.g., *Total=76289 KBytes, Free=52177 KBytes, Max=51565 Kbytes*).

**FLASH :** Displays the flash size of the system (e.g., *0x40000000-0x41ffffff, 512 x 0x10000 blocks*).

**Fan Speed:** Displays the information about fan speed e.g., *7031(rpm)*.

**Powers:** The status of the AC and DC Power Supplies (for example:  
*AC Power On 11.95V ; DC Power On 0.00V (AC only) or*  
*AC Power On 0.00V ; DC Power On 11.73V (DC only) or*  
*AC Power On 11.95V ; DC Power On 11.79V (AC and DC)*

**Temperature 1:** Displays the information of temperature sensor 1 e.g., *34(C) ; 93(F)*.

**Temperature 2:** Displays the information of temperature sensor 2 e.g., *27(C) ; 80(F)*.

**CPU Load (100ms, 1s, 10s):** Displays the cpu loading (100ms, 1s, 10s) of the system.

### 3-1.2 IP Status

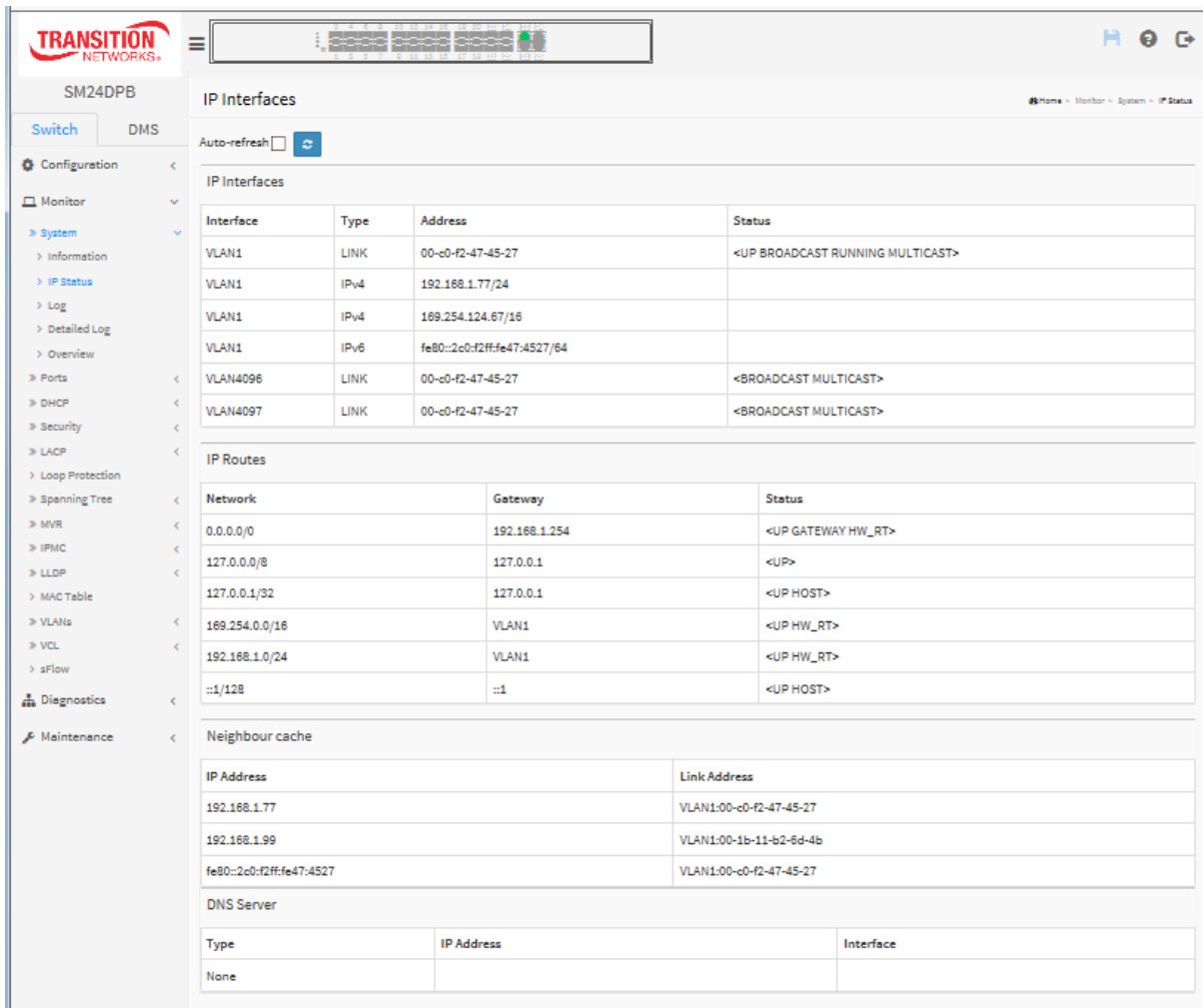
This page displays the status of the IP protocol layer. The status is defined by the IP interfaces, IP routes, Neighbor cache (ARP cache) and DNS Server status.

#### Web Interface

To view the log configuration in the web interface:

1. Click Monitor, System, IP Status.
2. View the IP address information.

**Figure 3- 1.2: IP Interfaces page**



#### Parameter descriptions:

#### **IP Interfaces**

**Interface** : Shows the name of the interface (e.g., *VLAN1*).

**Type** : Shows the address type of the entry. This may be *LINK* or *IPv4*.

**Address** : Shows the current address of the interface (of the given type).

**Status** : Shows the status flags of the interface (and/or address).

***IP Routes***

**Network** : Shows the destination IP network or host address of this route.

**Gateway** : Shows the gateway address of this route.

**Status** : Shows the status flags of the route.

***Neighbour cache***

**IP Address** : Shows the IP address of the entry.

**Link Address** : Shows the Link (MAC) address for which a binding to the IP address given exist.


***DNS Server***

**Type**: e.g., *Static*

**IP Address**: e.g., *8.8.8.8*

**Interface**:

**Buttons**

Auto-refresh  

: Auto-refresh: Check this box to refresh the page automatically every 3 seconds.

**Refresh**: Click to manually refresh the page immediately.

### 3-1.3 Log

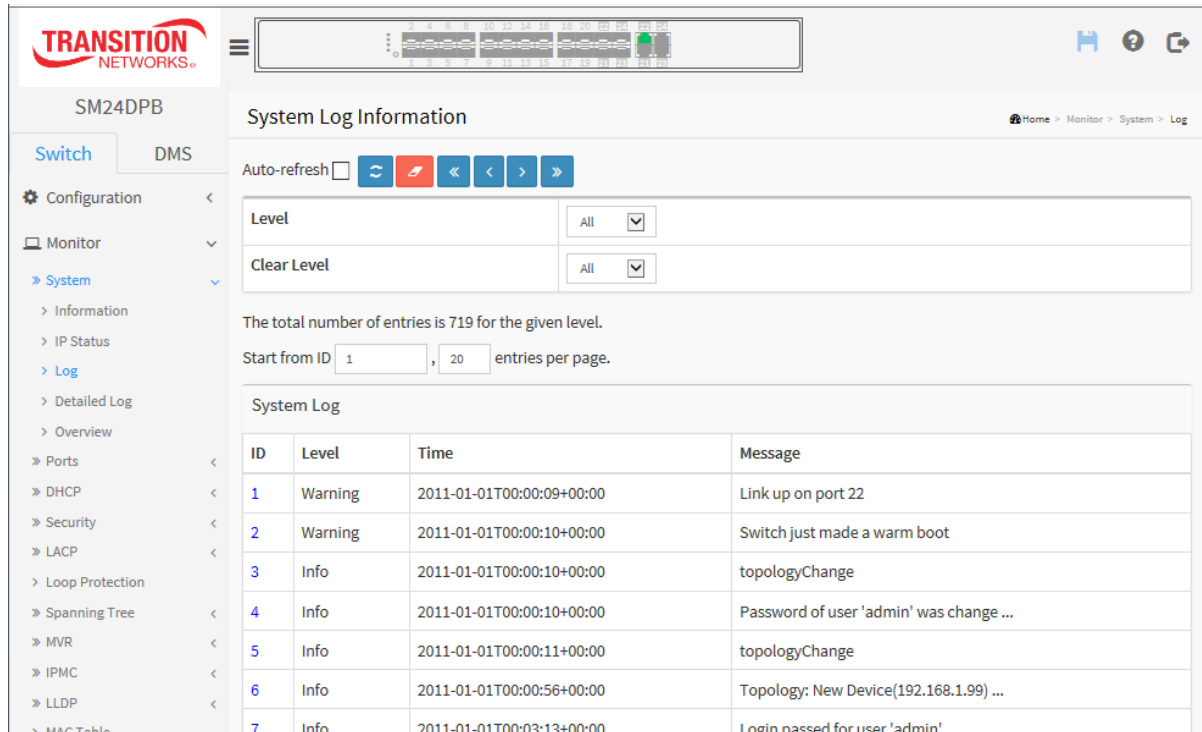
This page displays the system log parameters of the switch.

#### Web Interface

To view the syslog information in the web interface:

1. Click Monitor, System, Log.
2. View the log information.

**Figure 3- 1.3: System Log Information page**



#### Parameter descriptions:

**Auto-refresh :** Check the checkbox and the device will refresh the log automatically.

**Level:** information level of the system log entry. The following level types are supported: Emerg, Alert, Crit, Error, Warning, Notice, Info, Debug, All.

**Clear:** Clear Level for Syslog: Emerg, Alert, Crit, Error, Warning, Notice, Info, Debug, All.

**ID :** ID (>= 1) of the system log entry.

**Time :** It will display the log record by device time. The time of the system log entry.

**Message :** Displays the log detail message of the system log entry. For example, see [Syslog Message Examples](#) on the next page.

#### Buttons



**Auto-refresh:** Check this box to refresh the page automatically every 3 seconds.

**Refresh:** Updates the system log entries, starting from the current entry ID.

**Clear:** Flushes the selected log entries.

**<<:** Updates the system log entries, starting from the first available entry ID.

**< :** Updates the system log entries, ending at the last entry currently displayed.

**> :** Updates the system log entries, starting from the last entry currently displayed.

**>>:** Updates the system log entries, ending at the last available entry ID.

### Syslog Message Examples

Level	Time	Message
Warning	2011-01-01T00:00:04+00:00	Switch just made a cold boot
Warning	2011-01-01T00:00:04+00:00	Switch just made a warm boot
Info	2011-01-01T00:00:04+00:00	Password of user 'admin' was change ...
Warning	2011-01-01T00:00:05+00:00	Link up on port 22
Warning	2011-01-01T00:00:15+00:00	Power A Voltage Low, 0.00 V
Warning	2011-01-01T00:00:49+00:00	Bad password attempt for user 'admi ...
Info	2011-01-01T00:00:55+00:00	Login passed for user 'admin'
Warning	2011-01-01T01:17:37+00:00	Bad password attempt for user ''
Warning	2011-01-01T00:04:06+00:00	Power A Voltage Recovered, 11.95 V
Warning	2011-01-01T00:07:00+00:00	Power A Voltage Low, 0.00 V
Info	2011-01-01T00:14:59+00:00	User 'admin' logout
Info	2011-01-01T00:47:02+00:00	DMS: New Device(192.168.1.99) add i ...
Info	2011-01-01T00:49:35+00:00	Auto Saving
Warning	2011-01-01T03:38:22+00:00	SFP module inserted on port 1
Warning	2011-01-01T03:38:31+00:00	SFP module inserted on port 2
Warning	2011-01-01T00:00:05+00:00	Link up on port 23

### 3-1.4 Detailed Log

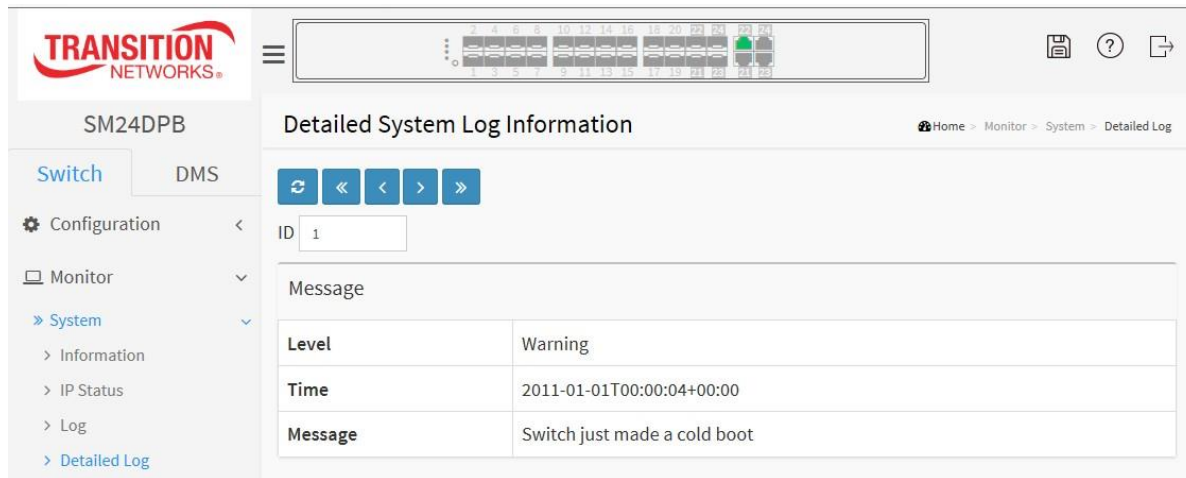
This page displays the detailed system log information.

#### Web Interface

To display the detailed log configuration in the web interface:

1. Click Monitor, System and Detailed Log.
2. View the log information.

**Figure 3- 1.4: Detailed System Log Information page**



#### Parameter descriptions:

**ID** : The ID ( $\geq 1$ ) of the system log entry.

**Message** : The detailed message of the system log entry (the Level, Time, and Message details as described above).

#### Buttons



**Refresh:** Updates the system log entries, starting from the current entry ID.

starting from the

**<<:** Updates the system log entries to the first available entry ID.

**< :** Updates the system log entry to the previous available entry ID.

**> :** Updates the system log entry to the next available entry ID.

**>>:** Updates the system log entry to the last available entry ID.

### 3-1.5 Overview

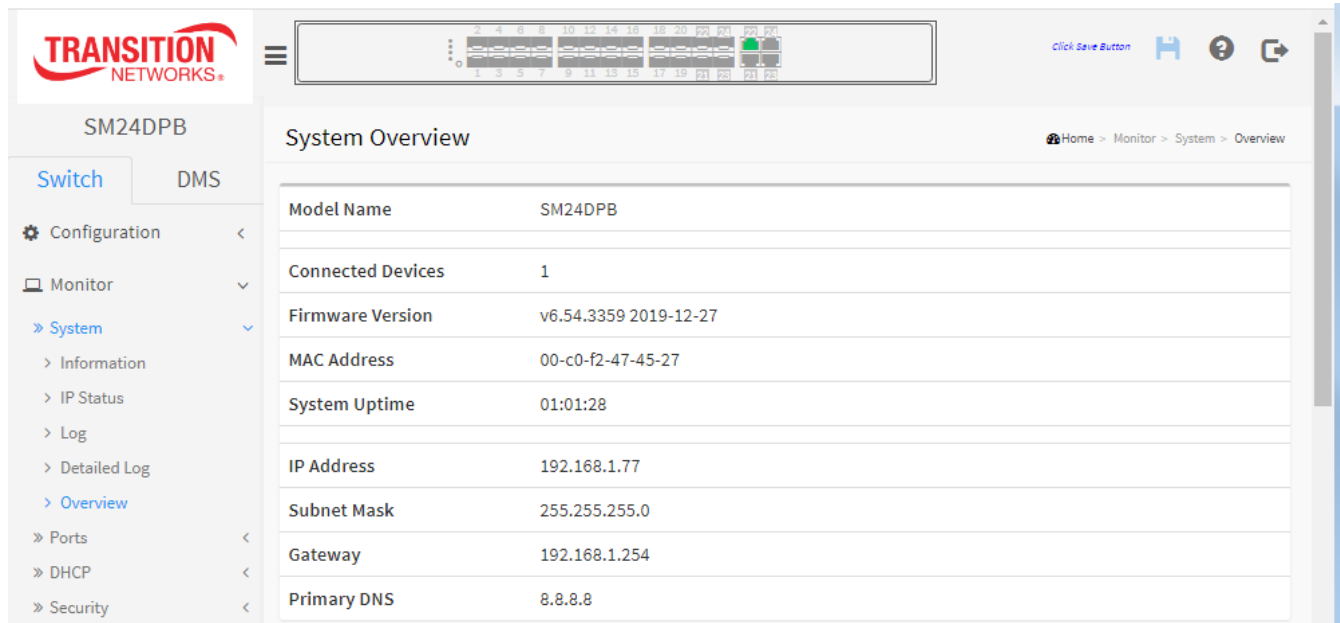
This page displays an overview of switch system parameters.

#### Web Interface

To display the system overview via the web interface:

1. Click Monitor, System, Overview.
2. View the displayed information.

**Figure 3- 1.5: System Overview page**



The screenshot shows the web interface for the SM24DPB switch. The main content area displays the 'System Overview' page with the following parameters:

Model Name	SM24DPB
Connected Devices	1
Firmware Version	v6.54.3359 2019-12-27
MAC Address	00-c0-f2-47-45-27
System Uptime	01:01:28
IP Address	192.168.1.77
Subnet Mask	255.255.255.0
Gateway	192.168.1.254
Primary DNS	8.8.8.8

#### Parameter descriptions:

**Model Name** : Displays the factory defined model name for identification purpose.

**Connected Devices** : Total of currently connected devices.

**Firmware Version** : Displays the current firmware version and date (e.g., v6.54.3202 2019-07-12).

**MAC Address** : The MAC Address of this switch (e.g., 00-c0-f2-57-45-65).

**System Uptime** : The period of time the device has been operational (e.g., 1d 00:44:05).

**IP Address** : The IPv4 or IPv6 address of the interface.

**Subnet Mask** : The IPv4 or IPv6 network mask of the interface.

**Gateway** : The IP address of the IP gateway.

**Primary DNS** : The IP address of the DNS Server if any configured.



### 3-3 Ports

This section describes how to configure the Port detail parameters, enable or disable switch Ports, and monitor the ports content or status.

- » Ports
  - > Traffic Overview
  - > QoS Statistics
  - > QCL Status
  - > Detailed Statistics
  - > SFP Information
  - > SFP Detail Info

#### 3-3.1 Traffic Overview

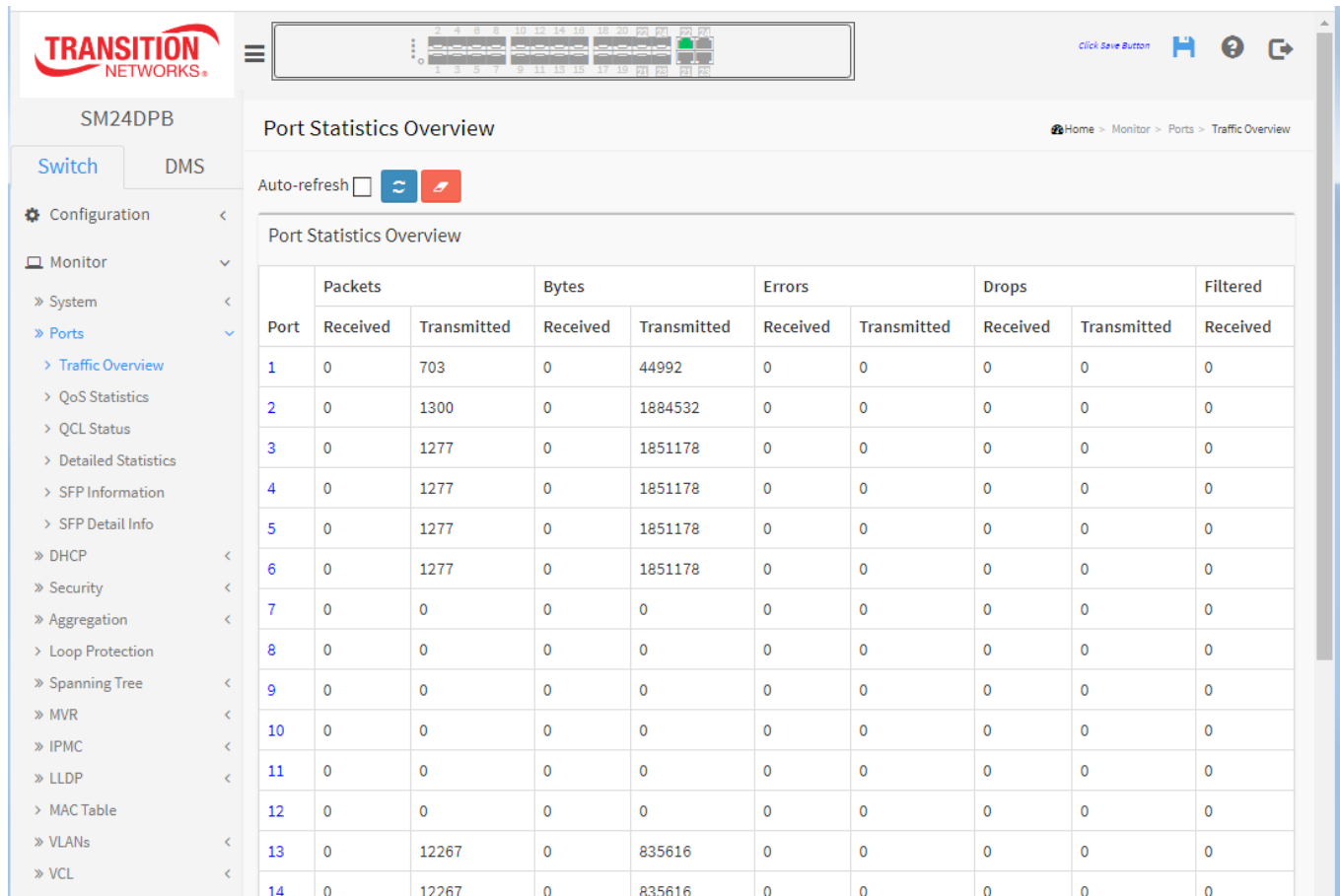
This section describes to the Port statistics information and provides overview of general traffic statistics for all switch ports.

#### Web Interface

To display the Port Statistics Overview in the web interface:

1. Click Monitor, Ports, Traffic Overview.
2. To auto-refresh check the “Auto-refresh” checkbox.
3. Click “Refresh” to refresh the port statistics or clear all information when you click “Clear”.

**Figure 3-3.1: Port Statistics Overview page**



#### Parameter descriptions:

**Port :** The logical port for the settings contained in the same row. You can click the linked port number to display that port’s detailed statistics.

**Packets :** The number of received and transmitted packets per port.

**Bytes :** The number of received and transmitted bytes per port.

**Errors :** The number of frames received in error and the number of incomplete transmissions per port.

**Drops :** The number of frames discarded due to ingress or egress congestion.

**Filtered :** The number of received frames filtered by the forwarding

## Buttons



**Auto-refresh:** Check this box to refresh the page automatically every 3 seconds.

**Refresh:** Click to immediately refresh the page manually.

**Clear:** Clears the counters for all ports.

### 3-3.2 QoS Statistics

This section describes the QoS detailed Queuing counters for a specific switch port and the different queues for all switch ports.

#### Web Interface

To display the Queuing Counters in the web interface:

1. Click Monitor, Ports, QoS Statistics.
2. To enable auto-refresh of the information check the “Auto-refresh” checkbox.
3. Click **Refresh** to refresh the pages or clear all information when you click **Clear**.

**Figure 3-3.2: Queuing Counters page**

Port	Q0		Q1		Q2		Q3		Q4		Q5		Q6		Q7	
	Rx	Tx	Rx	Tx	Rx	Tx	Rx	Tx	Rx	Tx	Rx	Tx	Rx	Tx	Rx	Tx
1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
2	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
3	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
4	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
5	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
6	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
7	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
8	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
9	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
10	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
11	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
12	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0

#### Parameter descriptions:

**Port :** The logical port for the settings contained in the same row.

**Qn :** Qn is the Queue number. There are eight QoS queues per port. Q0 is the lowest priority queue.

**Rx/Tx :** The number of received and transmitted packets per queue.

#### Buttons



**Auto-refresh:** Check this box to refresh the page automatically every 3 seconds.

**Refresh:** Click to immediately refresh the page manually.

**Clear:** Clears the counters for all ports.

### 3-3.3 QCL Status

This section describes how to configure and display the QCL status by different QCL users. Each row describes the QCE that is defined. It is a 'conflict' if a specific QCE is not applied to the hardware due to hardware limitations. The maximum number of QCEs is 256 on each switch.

#### Web Interface

To display the QoS Control List Status in the web interface:

1. Click Monitor, Ports, QCL Status.
2. To refresh the information automatically click "Auto-refresh".
3. At the User Select dropdown select Combined, Static, Voice VLAN, Surveillance, or Conflict.
4. Click the **Refresh** button to refresh an entry of the MVR Statistics Information.

**Figure 3-3.3: QoS Control List Status page**

The screenshot displays the 'QoS Control List Status' page. At the top, there is a navigation breadcrumb: Home > Monitor > Ports > QCL Status. Below the breadcrumb, there are controls for 'Auto-refresh' (checkbox), a refresh icon, a 'Resolve Conflict' button, and a dropdown menu currently set to 'Combined'. The main content is a table with the following data:

User	QCE	Port	Frame Type	Action			Conflict
				CoS	DPL	DSCP	
Static	1	2-5,7-24	IPv6	0	Default	Default	No
Static	2	1-24	Ethernet	0	Default	19	No

#### Parameter descriptions:

**User :** Indicates the QCL user.

**QCE# :** Indicates the index of QCE.

**Frame Type :** Indicates the type of frame to look for incoming frames. Possible frame types are:

**Any:** The QCE will match all frame type.

**Ethernet:** Only Ethernet frames (with Ether Type 0x600-0xFFFF) are allowed.

**LLC:** Only (LLC) frames are allowed

**SNAP:** Only (SNAP) frames are allowed.

**IPv4:** The QCE will match only IPV4 frames.

**IPv6:** The QCE will match only IPV6 frames.

**Port :** Indicates the list of ports configured with the QCE.

**Action :** Indicates the classification action taken on ingress frame if parameters configured are matched with the frame's content. There are three action fields: Class, DPL and DSCP.

**Class:** Classified QoS Class; if a frame matches the QCE it will be put in the queue.

**DPL:** Drop Precedence Level; if a frame matches the QCE then DP level will set to value displayed under DPL column.

**DSCP:** If a frame matches the QCE then DSCP will be classified with the value displayed under DSCP column.

**Conflict :** Displays Conflict status of QCL entries. It may happen that resources required to add a QCE may not be available, in that case it shows conflict status as 'Yes', otherwise it is always 'No'. Please note that conflict can be resolved by releasing the H/W resources required to add QCL entry on pressing 'Resolve Conflict' button.



**Buttons**

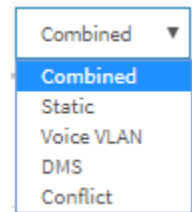
**Auto-refresh:** Check this box to refresh the page automatically every 3 seconds.

**Resolve Conflict:** Click to release the resources required to add QCL entry, in case conflict status for any QCL entry is 'yes'.

**Refresh:** Click to manually refresh the page immediately.

**Resolve Conflict :** Click to release the resources required to add QCL entry, in case the conflict status for any QCL entry is 'yes'.

**User Select dropdown :** At the dropdown select Combined, Static, Voice VLAN, DMS, or Conflict.



### 3-3.4 Detailed Statistics

This page displays detailed traffic statistics for a specific switch port. Use the port select box to select which switch port details to display.

The displayed counters are the totals for receive and transmit, the size counters for receive and transmit, and the error counters for receive and transmit.

#### Web Interface

To display the per-port detailed Statistics Overview in the web interface:

1. Click Monitor, Ports, Detailed Port Statistics.
2. Select the Port for which port you want to show the detailed Port statistics overview.
3. To auto-refresh the information check the “Auto-refresh” checkbox.
4. Click Refresh to refresh the port detailed statistics or clear all information when you click Clear.

**Figure 3-3.4: Detailed Port Statistics page**

Receive Total		Transmit Total	
Rx Packets	164034	Tx Packets	1626334
Rx Octets	26351886	Tx Octets	157807792
Rx Unicast	103459	Tx Unicast	69797
Rx Multicast	3143	Tx Multicast	74279
Rx Broadcast	57432	Tx Broadcast	1482258
Rx Pause	0	Tx Pause	0
Receive Size Counters		Transmit Size Counters	
Rx 64 Bytes	125735	Tx 64 Bytes	1469461
Rx 65-127 Bytes	1853	Tx 65-127 Bytes	79908
Rx 128-255 Bytes	3085	Tx 128-255 Bytes	15542
Rx 256-511 Bytes	10725	Tx 256-511 Bytes	26945
Rx 512-1023 Bytes	22629	Tx 512-1023 Bytes	6660
Rx 1024-1526 Bytes	7	Tx 1024-1526 Bytes	27818
Rx 1527- Bytes	0	Tx 1527- Bytes	0
Receive Queue Counters		Transmit Queue Counters	
Rx Q0	163935	Tx Q0	0
Rx Q1	0	Tx Q1	0
Rx Q2	0	Tx Q2	0
Rx Q3	0	Tx Q3	0

#### Parameter descriptions:

#### Receive Total and Transmit Total

**Rx and Tx Packets** : The number of received and transmitted (good and bad) packets.

**Rx and Tx Octets** : The number of received and transmitted (good and bad) bytes. Includes FCS, but excludes framing bits.

**Rx and Tx Unicast** : The number of received and transmitted (good and bad) unicast packets.

**Rx and Tx Multicast :** The number of received and transmitted (good and bad) multicast packets.

**Rx and Tx Broadcast :** The number of received and transmitted (good and bad) broadcast packets.

**Rx and Tx Pause :** A count of the MAC Control frames received or transmitted on this port that have an opcode indicating a PAUSE operation.

**Receive and Transmit Size Counters :** The number of received and transmitted (good and bad) packets split into categories based on their respective frame sizes.

**Receive and Transmit Queue Counters :** The number of received and transmitted packets per input and output queue.

### Receive Error Counters

**Rx Drops :** The number of frames dropped due to lack of receive buffers or egress congestion.

**Rx CRC/Alignment :** The number of frames received with CRC or alignment errors.

**Rx Undersize :** The number of short 1 frames received with valid CRC.

**Rx Oversize :** The number of long 2 frames received with valid CRC.

**Rx Fragments :** The number of short 1 frames received with invalid CRC.

**Rx Jabber :** The number of long 2 frames received with invalid CRC.

**Rx Filtered :** The number of received frames filtered by the forwarding process.

Short frames are frames that are smaller than 64 bytes.

Long frames are frames that are longer than the configured maximum frame length for this port.

### Transmit Error Counters

**Tx Drops :** The number of frames dropped due to output buffer congestion.

**Tx Late/Exc. Coll. :** The number of frames dropped due to excessive or late collisions.

**Auto-refresh:** Check the Auto-refresh button to refresh the Queuing Counters automatically.

**Upper right icon (Refresh, clear) :** You can click them for refresh the Port Detail Statistics or clear them manually.

### Buttons



**Auto-refresh:** Check this box to refresh the page automatically every 3 seconds.

**Refresh:** Click to manually refresh the page immediately.

**Clear:** Clears the counters for the selected port.

**Port Select box :** Use the port select box to select which port's details to display.

### 3-3.5 SFP Information

The **Monitor > Ports > SFP Information** menu path displays DMI (Diagnostic Monitoring Interface) and DDMI (Digital Diagnostic Monitoring Interface) data: See <ftp://ftp.seagate.com/sff/INF-8074.PDF>.

Port	Tx Central Wavelength	Bit Rate	Temperature	Vcc	Mon1 (Bias)	Mon2 (TxPwr)	Mon3 (RxPwr)
1	1550	10 Gbps	31.08 C	3.27 V	82 mA	1.86 dBm	none
2	850	10 Gbps	34.84 C	3.29 V	6 mA	-2.29 dBm	none
3	1310	100 Mbps	25.16 C	3.28 V	13 mA	-10.25 dBm	none
4	850	1000 Mbps	26.59 C	3.29 V	3 mA	-6.82 dBm	none
5							
6							

The page displays the following information for each port:

**Port:** The port number for this line of the table.

**Tx Central Wavelength:** Displays the nominal transmitter output wavelength in nm (nanometers).

**Bit Rate:** Displays the nominal bit rate of the transceiver.

**Temperature:** Displays the internally measured transceiver temperature. Temperature accuracy is vendor specific but must be better than 3 degrees Celsius over specified operating temperature and voltage.

**Vcc:** Displays the internally measured transceiver supply voltage. Accuracy is vendor specific but must be better than 3 percent of the manufacturer's nominal value over specified operating temperature and voltage. Note that in some transceivers, transmitter supply voltage and receiver supply voltage are isolated. In that case, only one supply is monitored. Refer to the device specification for more detail.

**Mon1 (Bias):** Displays the measured TX bias current in uA (microAmps). Accuracy is vendor specific but must be better than 10 percent of the manufacturer's nominal value over specified operating temperature and voltage.

**Mon2 (TX PWR):** Displays the measured coupled TX output power in mW. Accuracy is vendor specific but must be better than 3dB over specified operating temperature and voltage. Data is assumed to be based on measurement of a laser monitor photodiode current. Data is not valid when the transmitter is disabled.

**Mon3 (RX PWR):** Displays the measured received optical power in mW (milliWatts). Absolute accuracy is dependent upon the exact optical wavelength. For the vendor specified wavelength, accuracy should be better than 3dB over specified temperature and voltage. This accuracy should be maintained for input power levels up to the lesser of maximum transmitted or maximum received optical power per the appropriate standard. It should be maintained down to the minimum transmitted power minus cable plant loss (insertion loss or passive loss) per the appropriate standard. Absolute accuracy beyond this minimum required received input optical power range is vendor specific.

#### Buttons



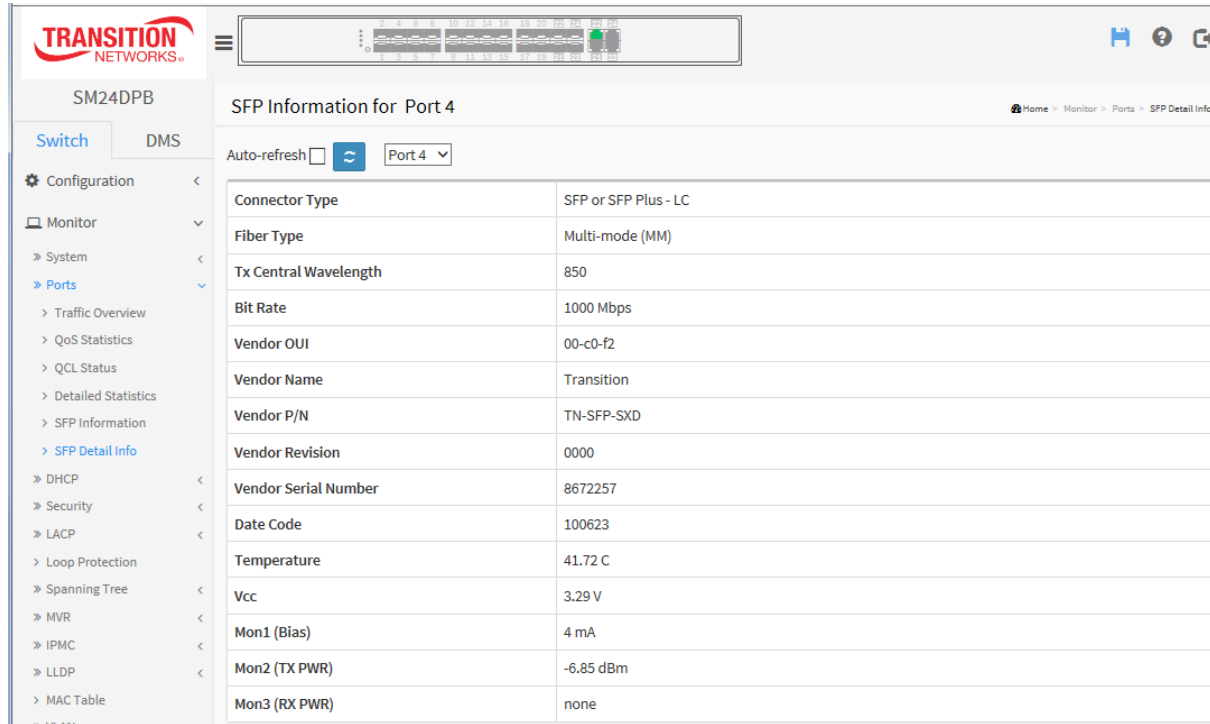
**Refresh:** Click to manually refresh the page immediately. Any changes made locally will be undone.

**Auto-refresh**  : Check this box to automatically refresh the page every 3 seconds.



### 3-3.6 SFP Detail Info

The **Monitor > Ports > SFP Detail Info** menu path displays the SFP Information page. This page displays general SFP information and monitoring information.



The screenshot shows the SFP Information page for Port 4. The page title is "SFP Information for Port 4". The breadcrumb path is "Home > Monitor > Ports > SFP Detail Info". The page includes an "Auto-refresh" checkbox and a "Port 4" dropdown menu. The main content is a table with the following parameters and values:

Connector Type	SFP or SFP Plus - LC
Fiber Type	Multi-mode (MM)
Tx Central Wavelength	850
Bit Rate	1000 Mbps
Vendor OUI	00-c0-f2
Vendor Name	Transition
Vendor P/N	TN-SFP-SXD
Vendor Revision	0000
Vendor Serial Number	8672257
Date Code	100623
Temperature	41.72 C
Vcc	3.29 V
Mon1 (Bias)	4 mA
Mon2 (TX PWR)	-6.85 dBm
Mon3 (RX PWR)	none

#### Parameter descriptions:

**Connector Type:** Displays the external optical or electrical cable connector provided as the media interface. Examples: SFP or SFP Plus - LC.

**Fiber Type:** Displays the fiber channel transmission media. Examples: Multi-mode (MM), or Single Mode (SM).

**Tx Central Wavelength:** Displays the nominal transmitter output wavelength in nanometers (e.g., 850 nm).

**Bit rate:** Displays the nominal bit rate of the transceiver (e.g., 1000 Mbps).

**Vendor OUI:** Displays the vendor IEEE company ID (Operationally Unique Identifier).

**Vendor Name:** Displays the vendor name (e.g., Transition).

**Vendor P/N:** Displays the vendor part number or product name (e.g., TN-SFP-SXD or TN-10GSFP-LR1).

**Vendor Revision:** Displays the vendor's product revision.

**Vendor Serial Number:** Displays the vendor serial number for the transceiver.

**Date Code:** Displays the vendor's manufacturing date code (e.g., 120710).

**Temperature:** Displays the internally measured transceiver temperature. Temperature accuracy is vendor specific but must be better than 3 degrees Celsius over specified operating temperature and voltage.


**Vcc:** Displays the internally measured transceiver supply voltage. Accuracy is vendor specific but must be better than 3 percent of the manufacturer's nominal value over specified operating temperature and voltage. Note that in some transceivers, transmitter supply voltage and receiver supply voltage are isolated. In that case, only one supply is monitored. Refer to the device specification for more detail.

**Mon1 (Bias):** Displays the measured TX bias current in uA. Accuracy is vendor specific but must be better than 10 percent of the manufacturer's nominal value over specified operating temperature and voltage.

**Mon2 (TX PWR):** Displays the measured coupled TX output power in mW. Accuracy is vendor specific but must be better than 3dB over specified operating temperature and voltage. Data is assumed to be based on measurement of a laser monitor photodiode current. Data is not valid when the transmitter is disabled.

**Mon3 (RX PWR):** Displays the measured received optical power in mW. Absolute accuracy is dependent upon the exact optical wavelength. For the vendor specified wavelength, accuracy should be better than 3dB over specified temperature and voltage. This accuracy should be maintained for input power levels up to the lesser of maximum transmitted or maximum received optical power per the appropriate standard. It should be maintained down to the minimum transmitted power minus cable plant loss (insertion loss or passive loss) per the appropriate standard. Absolute accuracy beyond this minimum required received input optical power range is vendor specific.

## Buttons

The port select box determines which port is affected by clicking the buttons.



**Refresh:** Click to refresh the page immediately (manually). Any changes made locally will be undone.

**Auto-refresh** : Check the Auto-refresh checkbox to enable an automatic refresh of the page at regular intervals.

## 3-4 DHCP

### 3-4.1 Server

A DHCP Server can be used to allocate network addresses and deliver configuration parameters to dynamically configured hosts called DHCP client.

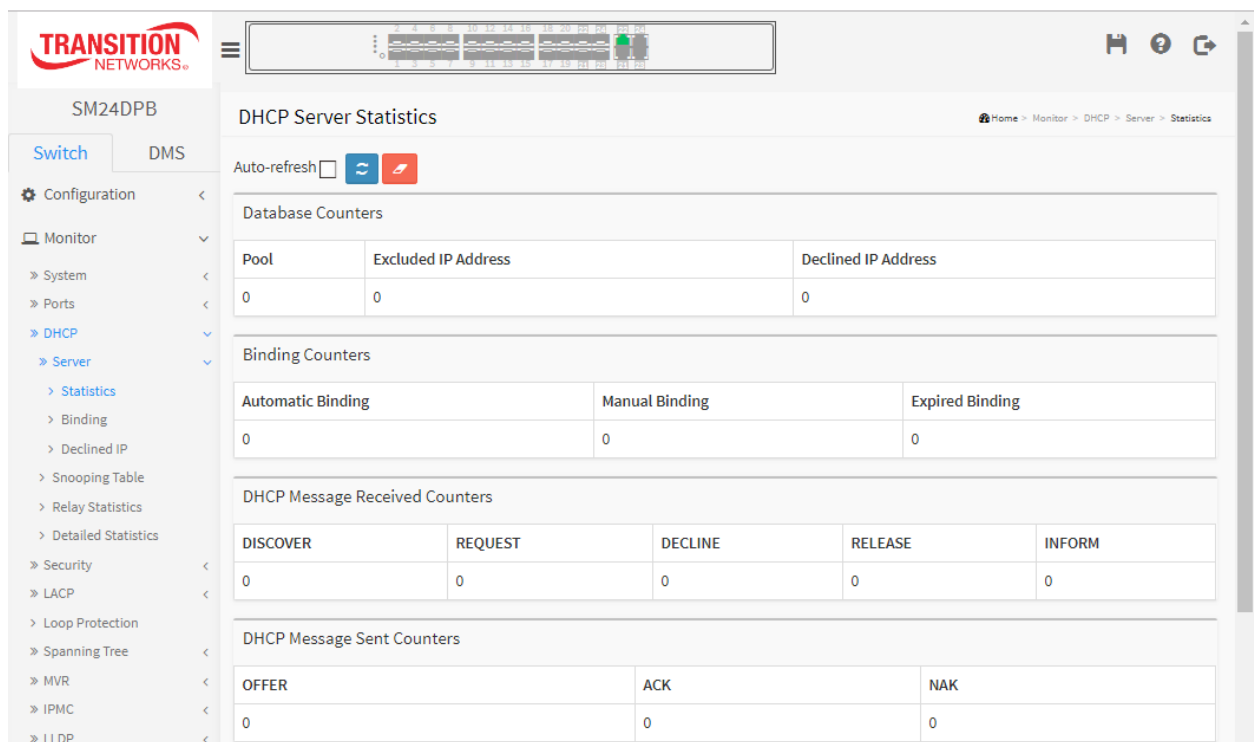
#### 3-4.1.1 Statistics

This page displays the database counters and the number of DHCP messages sent and received by DHCP server.

#### Web Interface

To view the DHCP server Statistics in the web interface click Monitor > DHCP > Server > Statistics.

**Figure 3-4.1.1: DHCP Server Statistics page**



#### Parameter descriptions:

##### **Database Counters**

**Pool:** Number of pools.

**Excluded IP Address:** Number of excluded IP address ranges.

**Declined IP Address:** Number of declined IP addresses.

##### **Binding Counters**

**Automatic Binding:** Number of bindings with network-type pools.

**Manual Binding:** Number of bindings that administrator assigns an IP address to a client. That is, the pool is of host type.

**Expired Binding:** Number of bindings that their lease time expired or they are cleared from Automatic/Manual type bindings.

**DHCP Message Received Counters**

**DISCOVER:** Number of DHCP DISCOVER messages received.

**REQUEST:** Number of DHCP REQUEST messages received.

**DECLINE:** Number of DHCP DECLINE messages received.

**RELEASE:** Number of DHCP RELEASE messages received.

**INFORM:** Number of DHCP INFORM messages received.

**DHCP Message Sent Counters**

**OFFER:** Number of DHCP OFFER messages sent.

**ACK:** Number of DHCP ACK (Acknowledge) messages sent.

**NAK:** Number of DHCP NAK (Negative Acknowledge) messages sent.

**Buttons**

**Auto-refresh :** Check this box to refresh the page automatically every 3 seconds.

**Refresh :** Click to refresh the page immediately.

**Clear:** Click to clear DHCP Message Received Counters and DHCP Message Sent Counters.

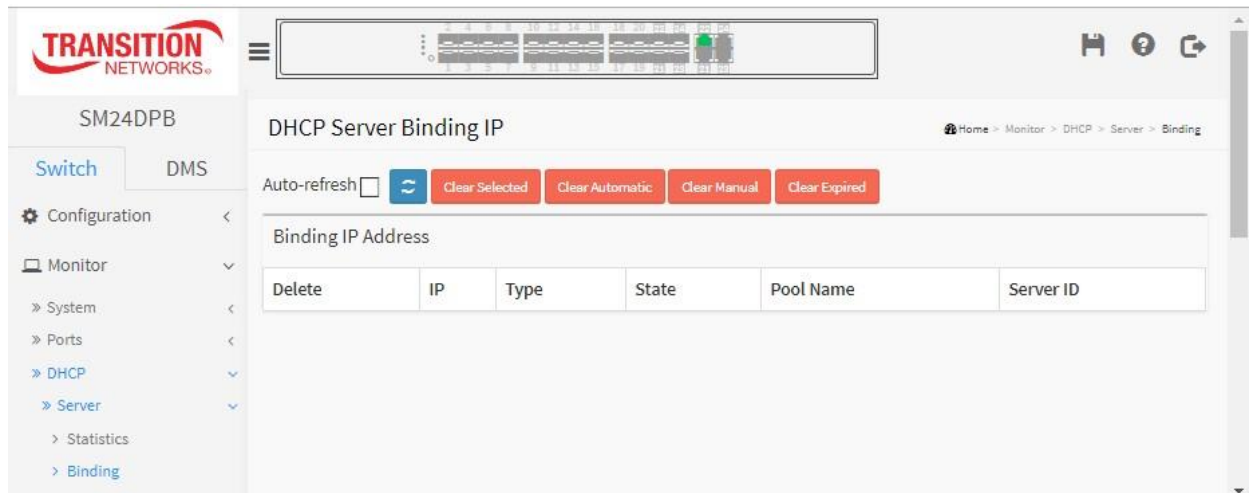
### 3-4.1.2 Binding

This page displays bindings generated for DHCP clients.

#### Web Interface

To display DHCP Server Binding IP in the web interface click Monitor, DHCP, Server and Binding.

**Figure 3-4.1.2: DHCP Server Binding IP page**



#### Parameter descriptions:

**IP:** IP address allocated to DHCP client.

**Type:** Type of binding. Possible types are Automatic, Manual, Expired.

**State:** State of binding. Possible states are Committed, Allocated, Expired.

**Pool Name:** The pool that generates the binding.

**Server ID:** Server IP address to service the binding.

#### Buttons

**Auto-refresh :** Check this box to refresh the page automatically every 3 seconds.

**Refresh :** Click to refresh the page immediately.

**Clear Selected:** Click to clear selected bindings. If the selected binding is Automatic or Manual, then it is changed to be Expired. If the selected binding is Expired, then it is freed.

**Clear Automatic :** Click to clear all Automatic bindings and Change them to Expired bindings.

**Clear Manual :** Click to clear all Manual bindings and Change them to Expired bindings.

**Clear Expired :** Click to clear all Expired bindings and free them.

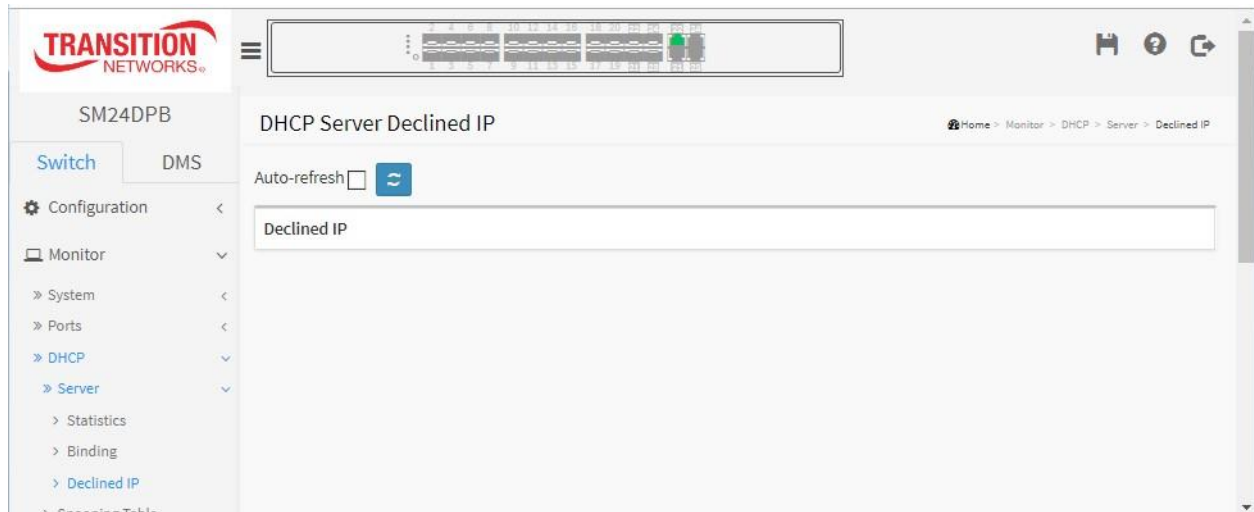
### 3-4.1.3 Declined IP

This page displays declined IP addresses.

#### **Web Interface**

To display DHCP Server Declined IP in the web interface click Monitor, DHCP, Server and Declined IP.

**Figure 3-4.1.3: The DHCP Server Declined IP page**



#### **Parameter descriptions:**

**IP:** IP address allocated to DHCP client.

**Type:** Type of binding. Possible types are Automatic, Manual, Expired.

**State:** State of binding. Possible states are Committed, Allocated, Expired.

**Pool Name:** The pool that generates the binding.

**Server ID:** Server IP address to service the binding.

#### **Buttons**

**Auto-refresh :** Check this box to refresh the page automatically every 3 seconds.

**Refresh :** Click to manually refresh the page immediately.

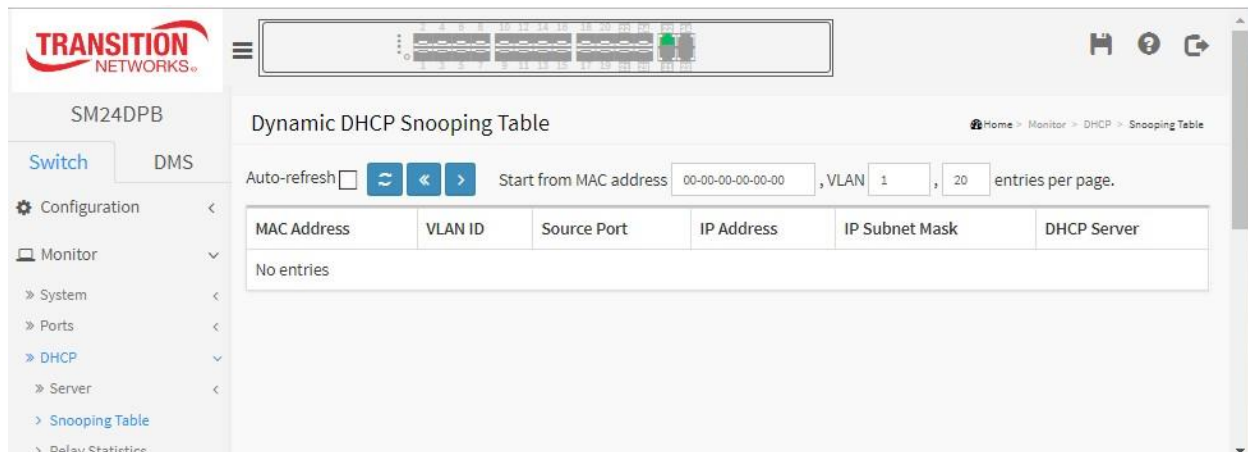
### 3-4.2 Snooping Table

This page displays the dynamic IP assigned information after DHCP Snooping mode is disabled. All DHCP clients obtained the dynamic IP address from the DHCP server will be listed in this table except for local VLAN interface IP addresses. Entries in the Dynamic DHCP Snooping Table are shown on this page.

#### Web Interface

To monitor an DHCP in the web interface click Monitor, DHCP, Snooping table.

**Figure 3-4.2: DHCP Snooping Table**



#### Parameter descriptions:

**MAC Address:** User MAC address of the entry.

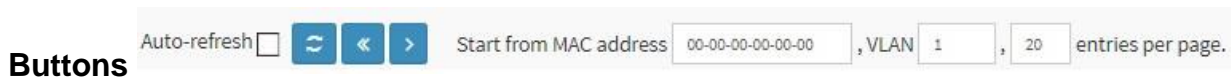
**VLAN ID:** VLAN-ID in which the DHCP traffic is permitted.

**Source Port:** Switch Port Number for which the entries are displayed.

**IP Address:** User IP address of the entry.

**IP Subnet Mask:** User IP subnet mask of the entry.

**DHCP Server Address:** DHCP Server address of the entry.



#### Buttons

**Auto-refresh:** Check this box to refresh the page automatically every 3 seconds.

**Refresh:** Refreshes the displayed table starting from the input fields.

**Clear:** Flushes all dynamic entries.

**<< :** Updates the table starting from the first entry in the Dynamic DHCP snooping Table.

**>> :** Updates the table, starting with the entry after the last entry currently displayed.

**Start from MAC address:**

**VLAN:** Enter the VLAN ID you want to view.

**entries per page:** Enter the number of entries you want to view on each page. 'entries per page' must be an integer value between 2 and 99.

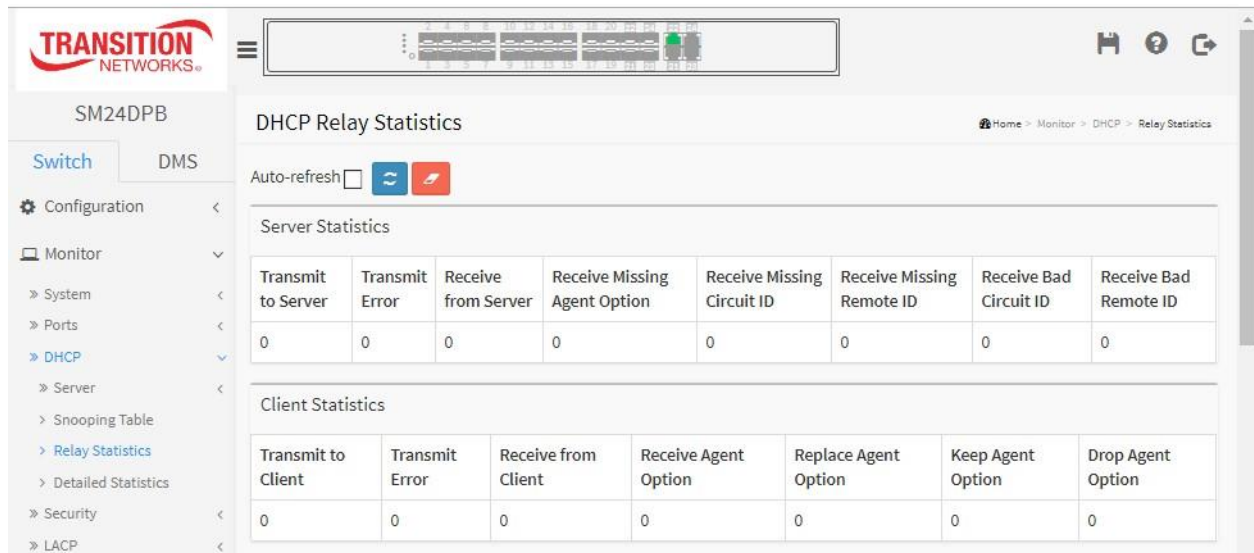
### 3-4.3 Relay Statistics

This page provides statistics for DHCP relay.

#### **Web Interface**

To monitor an DHCP Relay statistics in the web interface, Click Monitor, DHCP, Relay Statistics

**Figure 3-4.3: DHCP Relay Statistics page**



#### **Parameter descriptions:**

##### **Server Statistics**

**Transmit to Server :** The number of packets that are relayed from client to server.

**Transmit Error :** The number of packets that resulted in errors while being sent to clients.

**Receive from Server :** The number of packets received from server.

**Receive Missing Agent Option:** The number of packets received without agent information options.

**Receive Missing Circuit ID :** The number of packets received with the Circuit ID option missing.

**Receive Missing Remote ID :** The number of packets received with the Remote ID option missing.

**Receive Bad Circuit ID:** The number of packets whose Circuit ID option did not match known circuit ID.

**Receive Bad Remote ID :** The number of packets whose Remote ID option did not match known Remote ID.

##### **Client Statistics**

**Transmit to Client :** The number of relayed packets from server to client.

**Transmit Error :** The number of packets that resulted in error while being sent to servers.

**Receive from Client :** The number of received packets from server.

**Receive Agent Option :** The number of received packets with relay agent information option.

**Replace Agent Option :** The number of packets which were replaced with relay agent information option.

**Keep Agent Option :** The number of packets whose relay agent information was retained.



**Drop Agent Option :** The number of packets that were dropped which were received with relay agent information.

## Buttons

**Auto-refresh:** Check this box to refresh the page automatically every 3 seconds.

**Refresh:** Click to refresh the page immediately.

**Clear:** Clear all statistics.

### 3-4.4 Detailed Statistics

This page provides statistics for DHCP snooping. Notice that the normal forward per-port TX statistics isn't 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.

#### Web Interface

To monitor a DHCP Relay statistics in the web interface click Monitor, DHCP, Detailed Statistics.

**Figure 3-4.4: DHCP Detailed Statistics page**

Receive Packets		Transmit Packets	
Rx Discover	0	Tx Discover	0
Rx Offer	0	Tx Offer	0
Rx Request	0	Tx Request	0
Rx Decline	0	Tx Decline	0
Rx ACK	0	Tx ACK	0
Rx NAK	0	Tx NAK	0
Rx Release	0	Tx Release	0
Rx Inform	0	Tx Inform	0
Rx Lease Query	0	Tx Lease Query	0
Rx Lease Unassigned	0	Tx Lease Unassigned	0
Rx Lease Unknown	0	Tx Lease Unknown	0
Rx Lease Active	0	Tx Lease Active	0
Rx Discarded Checksum Error	0		
Rx Discarded from Untrusted	0		

#### Parameter descriptions:

**Rx and Tx Discover :** The number of discover (option 53 with value 1) packets received and transmitted.

**Rx and Tx Offer :** The number of offer (option 53 with value 2) packets received and transmitted.

**Rx and Tx Request :** The number of request (option 53 with value 3) packets received and transmitted.

**Rx and Tx Decline:** The number of decline (option 53 with value 4) packets received and transmitted.

**Rx and Tx ACK:** The number of ACK (option 53 with value 5) packets received and transmitted.

**Rx and Tx NAK:** The number of NAK (option 53 with value 6) packets received and transmitted.

**Rx and Tx Release:** The number of release (option 53 with value 7) packets received and transmitted.

**Rx and Tx Inform:** The number of inform (option 53 with value 8) packets received and transmitted.

**Rx and Tx Lease Query:** The number of lease query (option 53 with value 10) packets received and transmitted.

**Rx and Tx Lease Unassigned:** The number of lease unassigned (option 53 with value 11) packets received and transmitted.

**Rx and Tx Lease Unknown:** The number of lease unknown (option 53 with value 12) packets received and transmitted. Rx and Tx Lease Active

**Rx and Tx Lease Active:** The number of lease active (option 53 with value 13) packets received and transmitted.

**Rx Discarded checksum error:** The number of discard packet that IP/UDP checksum is error.

**Rx Discarded from Untrusted:** The number of discarded packet that are coming from untrusted port.

## Buttons

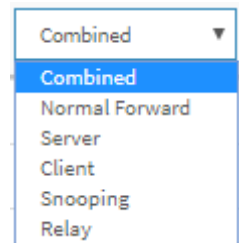
**Auto-refresh:** Check this box to refresh the page automatically every 3 seconds.

**Refresh:** Click to manually refresh the page immediately.

**Clear:** Clears the counters for the selected port.

**DHCP user select box:** determines which DHCP user's information displays on the page. You can select Combined (default), Normal Forward, Server, Client, Snooping, or Relay.

**Port select box:** determines which port is affected by clicking the buttons.



## 3-5 Security

### 3-5.1 Access Management Statistics

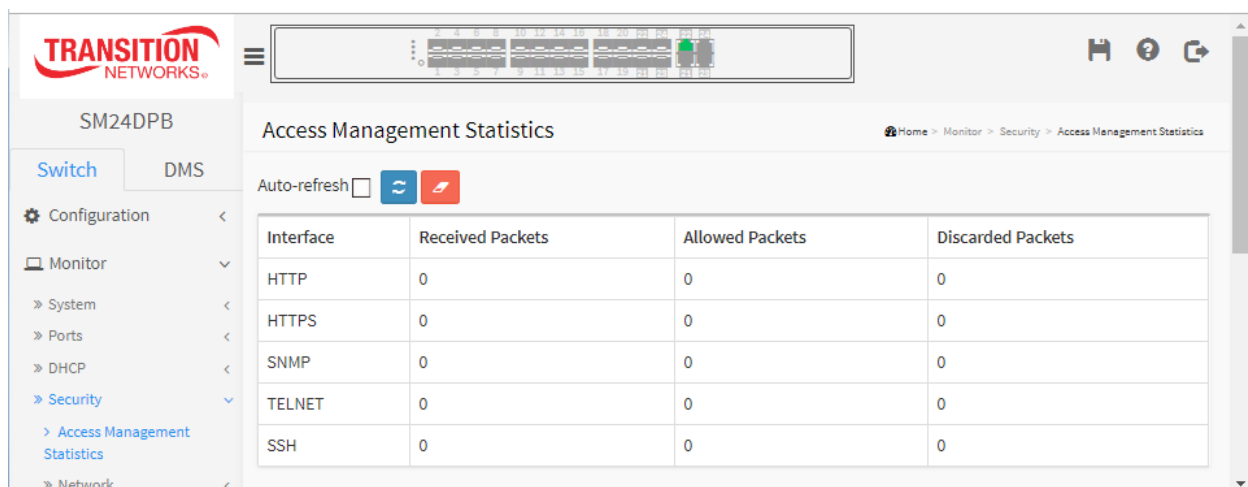
This page shows detailed statistics of the Access Management including HTTP, HTTPS, SSH, TELNET, and SSH.

#### Web Interface

To configure an Assess Management Statistics in the web interface:

1. Click Security, Access Management Statistics.
2. Check Auto-refresh.
3. Click Refresh to refresh the port detailed statistics or clear all information when you click “Clear”.

**Figure 3-5.1: Access Management Statistics page**



#### Parameter descriptions:

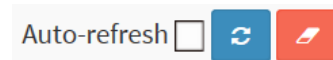
**Interface:** The interface type through which the remote host can access the switch (HTTP, HTTPS, SNMP, TELNET, SSH).

**Received Packets:** Number of received packets from the interface when access management mode is enabled.

**Allowed Packets:** Number of allowed packets from the interface when access management mode is enabled

**Discarded Packets:** Number of discarded packets from the interface when access management mode is enabled.

#### Buttons



**Auto-refresh:** Check this box to refresh the page automatically every 3 seconds.

**Refresh:** Click to manually refresh the page immediately.

**Clear:** Clears the counters for the selected port.

### 3-5.2 Network

#### 3-5.2.1 Port Security

##### 3-5.2.1.1 Switch

This page shows the Port Security status. Port Security is a module with no direct configuration.

Configuration comes indirectly from other modules - the user modules. When a user module has enabled port security on a port, the port is set-up for software-based learning. In this mode, frames from unknown MAC addresses are passed on to the port security module, which in turn asks all user modules whether to allow this new MAC address to forward or block it. For a MAC address to be set in the forwarding state, all enabled user modules must unanimously agree on allowing the MAC address to forward. If only one chooses to block it, it will be blocked until that user module decides otherwise.

The status page is divided into two sections - one with a legend of user modules and one with the actual port status.

#### Web Interface

To configure a Port Security Switch Status Configuration in the web interface:

1. Click Monitor, Security, Network, Port Security, Switch.
2. Check Auto-refresh.
3. Click Refresh to refresh the port security switch status.

**Figure 3-5.2.1.1: Port Security Switch Status page**

The screenshot displays the 'Port Security Switch Status' page. At the top, there is a navigation breadcrumb: Home > Monitor > Security > Network > Port Security > Switch. Below the breadcrumb, there is an 'Auto-refresh' checkbox and a refresh icon. The page is divided into two main sections: 'User Module Legend' and 'Port Status'.

**User Module Legend**

User Module Name	Abbr
Limit Control	L
802.1X	8
Voice VLAN	V

**Port Status**

Port	Users	State	MAC Count	
			Current	Limit
1	L--	Ready	0	4
2	L--	Ready	0	4
3	L--	Ready	0	4
4	L--	Ready	0	4
5	L--	Ready	0	4
6	L--	Ready	0	4
7	L--	Ready	0	4
8	L--	Ready	0	4

**Parameter descriptions:**

**User Module Legend:** The legend shows all user modules that may request Port Security services.

**User Module Name:** The full name of a module that may request Port Security services.

**Abbr:** A one-character abbreviation of the user module. This is used in the Users column in the port status table. ( **L** = Limit Control, **8** = 802.1X, **V** = Voice VLAN.)

**Port Status:** The table has one row for each port on the switch and a number of columns.

**Port:** The port number for which the status applies. Click the linked port number to see the status for this particular port.

**Users :** Each of the user modules has a column that shows whether that module has enabled Port Security or not. A dash (-) means that the corresponding user module is not enabled, whereas a letter indicates that the user module abbreviated by that letter (see Abbr) has enabled port security.

**State :** Shows the current state of the port. It can take one of four values:

**Disabled:** No user modules are currently using the Port Security service.

**Ready:** The Port Security service is in use by at least one user module, and is awaiting frames from unknown MAC addresses to arrive.

**Limit Reached:** The Port Security service is enabled by at least the Limit Control user module, and that module has indicated that the limit is reached and no more MAC addresses should be taken in.

**Shutdown:** The Port Security service is enabled by at least the Limit Control user module, and that module has indicated that the limit is exceeded. No MAC addresses can be learned on the port until it is administratively re-opened on the Limit Control configuration Web-page.

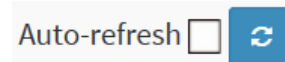
**MAC Count (Current, Limit) :** The two columns indicate the number of currently learned MAC addresses (forwarding as well as blocked) and the maximum number of MAC addresses that can be learned on the port, respectively.

If no user modules are enabled on the port, the Current column will show a dash (-).

If the Limit Control user module is not enabled on the port, the Limit column will show a dash (-).

Indicates the number of currently learned MAC addresses (forwarding as well as blocked) on the port. If no user modules are enabled on the port, a dash (-) will be shown.

## Buttons



**Auto-refresh:** Check this box to refresh the page automatically every 3 seconds.

every 3

**Refresh:** Click to manually refresh the page immediately.

### 3-5.2.1.2 Port

This page shows the MAC addresses secured by the Port Security module. Port Security is a module with no direct configuration. Configuration comes indirectly from other modules - the user modules.

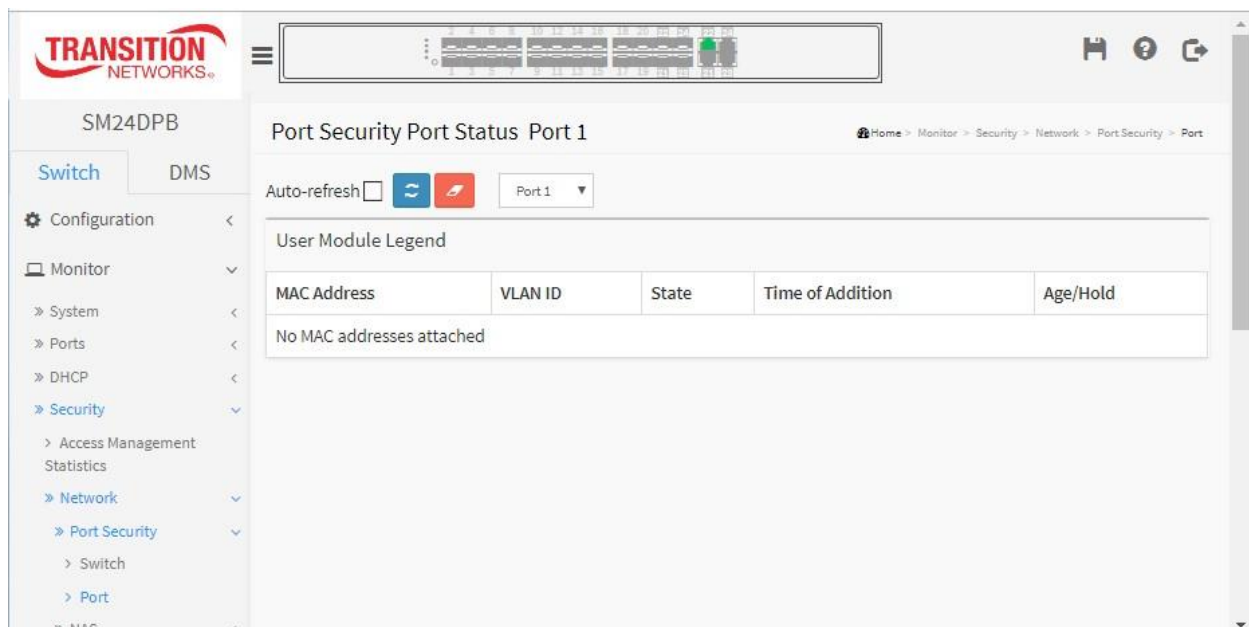
When a user module has enabled port security on a port, the port is set-up for software-based learning. In this mode, frames from unknown MAC addresses are passed on to the port security module, which in turn asks all user modules whether to allow this new MAC address to forward or block it. For a MAC address to be set in the forwarding state, all enabled user modules must unanimously agree on allowing the MAC address to forward. If only one chooses to block it, it will be blocked until that user module decides otherwise.

#### Web Interface

To display a Port Security Switch Status Configuration in the web interface:

1. Click Monitor, Security, Network, Port Security, Port.
2. Specify the Port which you want to monitor.
3. Check "Auto-refresh".
4. Click "Refresh" to refresh the port detailed statistics.

**Figure 3-5.2.1.2: Port Security Port Status page**



#### Parameter descriptions:

**MAC Address & VLAN ID :** The MAC address and VLAN ID that is seen on this port. If no MAC addresses are learned, a single row stating "No MAC addresses attached" is displayed.



**State :** Indicates whether the corresponding MAC address is blocked or forwarding. In the blocked state, it will not be allowed to transmit or receive traffic.

**Time of Addition :** Shows the date and time when this MAC address was first seen on the port.

**Age/Hold :** If at least one user module has decided to block this MAC address, it will stay in the blocked state until the hold time (measured in seconds) expires. If all user modules have decided to allow this MAC address to forward, and aging is enabled, the Port Security module will periodically check that this MAC address still forwards traffic. If the age period (measured in seconds) expires and no frames have been seen, the MAC

address will be removed from the MAC table. Otherwise a new age period will begin.

If aging is disabled or a user module has decided to hold the MAC address indefinitely, a dash (-) will be shown.

Auto-refresh    Port 1 

### Buttons

**Auto-refresh:** Check this box to refresh the page automatically every 3 seconds.

**Refresh:** Click to manually refresh the page immediately.



## 3-5.2.2 NAS

### 3-5.2.2.1 Switch

This section describes how to display NAS status information for each switch port. The status includes Admin State Port State, Last Source, Last ID, QoS Class, and Port VLAN ID.

#### Web Interface

To configure a NAS Switch Status Configuration in the web interface:

1. Click Monitor, Security, Network, NAS, Switch.
2. Check "Auto-refresh".
3. Click "Refresh" to refresh the port detailed statistics.

**Figure 3-5.2.2.1: Network Access Server Switch Status page**

Port	Admin State	Port State	Last Source	Last ID	QoS Class	Port VLAN ID
1	Force Authorized	Link Down			-	
2	Force Unauthorized	Link Down			-	
3	Port-based 802.1X	Link Down			-	
4	Single 802.1X	Link Down			-	
5	Multi 802.1X	Link Down			-	
6	MAC-based Auth.	Link Down			-	
7	Force Authorized	Link Down			-	
8	Force Authorized	Link Down			-	
9	Force Authorized	Link Down			-	

#### Parameter descriptions:

**Port :** The switch port number. Click a linked port number to display detailed NAS statistics for the port.

**Admin State :** The port's current administrative state. Refer to NAS Admin State for a description of possible values.

**Port State :** The current state of the port. Refer to NAS Port State for a description of the individual states.

**Last Source :** The source MAC address carried in the most recently received EAPOL frame for EAPOL-based authentication, and the most recently received frame from a new client for MAC-based authentication.

**Last ID :** The user name (supplicant identity) carried in the most recently received Response Identity EAPOL frame for EAPOL-based authentication, and the source MAC address from the most recently received frame from a new client for MAC-based authentication.


**QoS Class :** QoS Class assigned to the port by the RADIUS server if enabled.

**Port VLAN ID :** The VLAN ID that NAS has put the port in. The field is blank, if the Port VLAN ID is not overridden by NAS.

If the VLAN ID is assigned by the RADIUS server, "(RADIUS-assigned)" is appended to the VLAN ID. Read more

about RADIUS-assigned VLANs here.

If the port is moved to the Guest VLAN, "(Guest)" is appended to the VLAN ID. Read more about Guest VLANs here.

Auto-refresh  

### Buttons

**Auto-refresh:** Check this box to refresh the page automatically every 3 seconds.

**Refresh:** Click to refresh the page immediately (manually).

### 3-5.2.2.2 Port

This page displays detailed NAS statistics for a specific switch port running EAPOL-based IEEE 802.1X authentication. For MAC-based ports, it shows selected backend server (RADIUS Authentication Server) statistics only.

#### **Web Interface**

To display a NAS Port Statistics in the web interface:

1. Click Monitor, Security, Network, NAS, Port.
2. Check Auto-refresh.
3. Click Refresh” to refresh the port detailed statistics.

**Figure 3-5.2.2.2: NAS Statistics page**

The screenshot shows the web interface for the SM24DPB switch. The main content area is titled "NAS Statistics Port 3". It features an "Auto-refresh" checkbox and a refresh button. A dropdown menu is set to "Port 3". Below this is a table with the following data:

Port State	
Admin State	Port-based 802.1X
Port State	Link Down
QoS Class	-
Port VLAN ID	

#### **Parameter descriptions:**

##### **Port State**

**Admin State** : The port's current administrative state. Refer to NAS Admin State for a description of possible values.

**Port State** : The current state of the port. Refer to NAS Port State for a description of the individual states.

**QoS Class** : The QoS class assigned by the RADIUS server. The field is blank if no QoS class is assigned.

**Port VLAN ID** : The VLAN ID that NAS has put the port in. The field is blank if the Port VLAN ID is not overridden by NAS.

If the VLAN ID is assigned by the RADIUS server, "(RADIUS-assigned)" is appended to the VLAN ID. Read more about RADIUS-assigned VLANs here.

If the port is moved to the Guest VLAN, "(Guest)" is appended to the VLAN ID. Read more about Guest VLANs here.

## **Port Counters**

**EAPOL Counters** : These supplicant frame counters are available for these administrative states:

Force Authorized  
Force Unauthorized  
Port-based 802.1X  
Single 802.1X  
Multi 802.1X

**Backend Server Counters** : These backend (RADIUS) frame counters are available for these administrative states:

Port-based 802.1X  
Single 802.1X  
Multi 802.1X  
MAC-based Auth.

**Last Supplicant/Client Info** : Information about the last supplicant/client that attempted to authenticate. This information is available for these administrative states:

Port-based 802.1X  
Single 802.1X  
Multi 802.1X  
MAC-based Auth.

## **Selected Counters**

**Selected Counters** : The Selected Counters table is visible when the port is in one of these administrative states:

Multi 802.1X  
MAC-based Auth.

The table is identical to and is placed next to the Port Counters table, and will be empty if no MAC address is currently selected. To populate the table, select one of the attached MAC Addresses from the table below.

## **Attached MAC Addresses**

**Identity** : Shows the identity of the supplicant, as received in the Response Identity EAPOL frame. Clicking the link causes the supplicant's EAPOL and Backend Server counters to be shown in the Selected Counters table. If no supplicants are attached, it shows No supplicants attached.

This column is not available for MAC-based Auth.

**MAC Address** : For Multi 802.1X, this column holds the MAC address of the attached supplicant. For MAC-based Auth., this column holds the MAC address of the attached client.

Clicking the link causes the client's Backend Server counters to be shown in the Selected Counters table. If no clients are attached, it shows No clients attached.

**VLAN ID** : This column holds the VLAN ID that the corresponding client is currently secured through the Port Security module.

**State** : The client can either be authenticated or unauthenticated. In the authenticated state, it is allowed to forward frames on the port, and in the unauthenticated state, it is blocked. As long as the backend server hasn't successfully authenticated the client, it is unauthenticated. If an authentication fails for one or the other reason, the client will remain in the unauthenticated state for Hold Time seconds.

**Last Authentication** : Shows the date and time of the last authentication of the client (successful as well as unsuccessful).

## Buttons

**Auto-refresh:** Check this box to refresh the page every 3 seconds.

**Refresh:** Click to refresh the page immediately (manually).

**Clear:** This button is available in these modes:

- Force Authorized
- Force Unauthorized
- Port-based 802.1X
- Single 802.1X

**Clear All:** Click to clear the counters for the selected port. This button is available in these modes:

- Multi 802.1X
- MAC-based Auth.X

**Clear This:** Click to clear both the port counters and all of the attached client's counters. The "Last Client" will not be cleared, however. This button is available in these modes:

- Multi 802.1X
- MAC-based Auth.X

Click to clear only the currently selected client's counters.

### 3-5.2.3 ACL Status

This section describes how to display the ACL status by different ACL users. Each row describes the ACE that is defined. It is a conflict if a specific ACE is not applied to the hardware due to hardware limitations. The maximum number of ACEs is 512 on each switch.

#### Web Interface

To display the ACL status in the web interface:

1. Click Monitor, Network, ACL status.
2. Check Auto-refresh to refresh the page automatically every 3 seconds.
3. Click Refresh to refresh the page immediately.

**Figure 3-5.2.3: ACL Status page**

User	ACE	Ingress Port	Frame Type	Action	Rate Limiter	Port Redirect	CPU	CPU Once	Counter	Conflict
Rapid Ring	3	Port 3	IPv4/UDP 11240	Permit	Disabled	Port 4	Yes	No	0	No
Rapid Ring	4	Port 4	IPv4/UDP 11240	Permit	Disabled	Port 3	Yes	No	0	No
Rapid Ring	5	Port 5	IPv4/UDP 11240	Permit	Disabled	Port 6	Yes	No	0	No
Rapid Ring	6	Port 6	IPv4/UDP 11240	Permit	Disabled	Port 5	Yes	No	0	No
Rapid Ring	7	Port 7	IPv4/UDP 11240	Permit	Disabled	Port 8	Yes	No	0	No
Rapid Ring	8	Port 8	IPv4/UDP 11240	Permit	Disabled	Port 7	Yes	No	0	No
Rapid Ring	9	Port 9	IPv4/UDP 11240	Permit	Disabled	Port 10	Yes	No	0	No
Rapid Ring	10	Port 10	IPv4/UDP 11240	Permit	Disabled	Port 9	Yes	No	0	No
Rapid Ring	11	Port 11	IPv4/UDP 11240	Permit	Disabled	Port 12	Yes	No	0	No
Rapid Ring	12	Port 12	IPv4/UDP 11240	Permit	Disabled	Port 11	Yes	No	0	No
Rapid Ring	25	All	IPv4/UDP 11240	Permit	Disabled	Disabled	Yes	No	0	No
DMS mDNS	1	All	IPv4/UDP 5353	Permit	Disabled	Disabled	Yes	No	6	No
DMS Onvif	1	All	IPv4/UDP 10100-10227	Permit	Disabled	Disabled	Yes	No	0	No
DMS SSDP	1	All	IPv4/UDP 1900	Permit	Disabled	Disabled	Yes	No	116	No
DMS CLIENT	1	All	IPv4/UDP 10012	Permit	Disabled	Disabled	Yes	No	0	No

#### Parameter descriptions:

**User :** Indicates the ACL user.

**ACE:** Indicates the ACE ID on local switch.

**Ingress Port :** Indicates the ingress port of the ACE. Possible values are:

**All:** The ACE will match any ingress port.

**Port:** The ACE will match a specific ingress port.

**Frame Type :** Indicates the frame type of the ACE. Possible values are:

**Any:** The ACE will match any frame type.

**EType:** The ACE will match Ethernet Type frames. Note that an Ethernet Type based ACE will not get matched by IP and ARP frames.

**ARP:** The ACE will match ARP/RARP frames.

**IPv4:** The ACE will match all IPv4 frames.

**IPv4:** The ACE will match all IPv4 frames.

**IPv4/ICMP:** The ACE will match IPv4 frames with ICMP protocol.

**IPv4/UDP:** The ACE will match IPv4 frames with UDP protocol.

**IPv4/TCP:** The ACE will match IPv4 frames with TCP protocol.

**IPv4/Other:** The ACE will match IPv4 frames, which are not ICMP / UDP / TCP.

**IPv6:** The ACE will match all IPv6 standard frames.

**Action :** Indicates the forwarding action of the ACE.

**Permit:** Frames matching the ACE may be forwarded and learned.

**Deny:** Frames matching the ACE are dropped.

**Filter:** Frames matching the ACE are filtered.

**Rate Limiter :** Indicates the rate limiter number of the ACE. The allowed range is 1 to 16. When Disabled is displayed, the rate limiter operation is disabled.

**Port Redirect :** Indicates the port copy operation of the ACE. Frames matching the ACE are copied to the port number. The allowed values are Disabled or a specific port number. When Disabled is displayed, the port copy operation is disabled.

**CPU :** Forward packet that matched the specific ACE to CPU.

**CPU Once :** Forward first packet that matched the specific ACE to CPU.

**Counter :** The counter indicates the number of times the ACE was hit by a frame.

**Conflict :** Indicates the hardware status of the specific ACE. The specific ACE is not applied to the hardware due to hardware limitations.

## Buttons

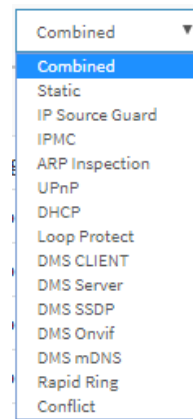


**Auto-refresh:** Check this box to refresh the page every 3 seconds.

**Refresh:** Click to manually refresh the page immediately.

**User select box:** determines which ACL user's information is displayed.

At the dropdown select Combined (default), Static, IP Source Guard, IPMC, ARP Inspection, UPnP, DHCP, Loop Protect, DMS CLIENT, DMS Server, DMS SSDP, DMS Onvif, DMS mDNS, Rapid Ring, or Conflict.



### 3-5.2.4 ARP Inspection

This page displays Dynamic ARP Inspection Table parameters of the switch. The Dynamic ARP Inspection Table contains up to 1024 entries, and is sorted first by port, then by VLAN ID, then by MAC address, and then by IP address.

Each page shows up to 99 entries from the Dynamic ARP Inspection table, default being 20, selected through the "entries per page" input field. When first visited, the web page will show the first 20 entries from the beginning of the Dynamic ARP Inspection Table.

The "Start from port address", "VLAN", "MAC address" and "IP address" input fields let you select the starting point in the Dynamic ARP Inspection Table. Clicking the > button will update the displayed table starting from that or the closest next Dynamic ARP Inspection Table match. In addition, the two input fields will - upon a << button click - assume the value of the first displayed entry, allowing for continuous refresh with the same start address.

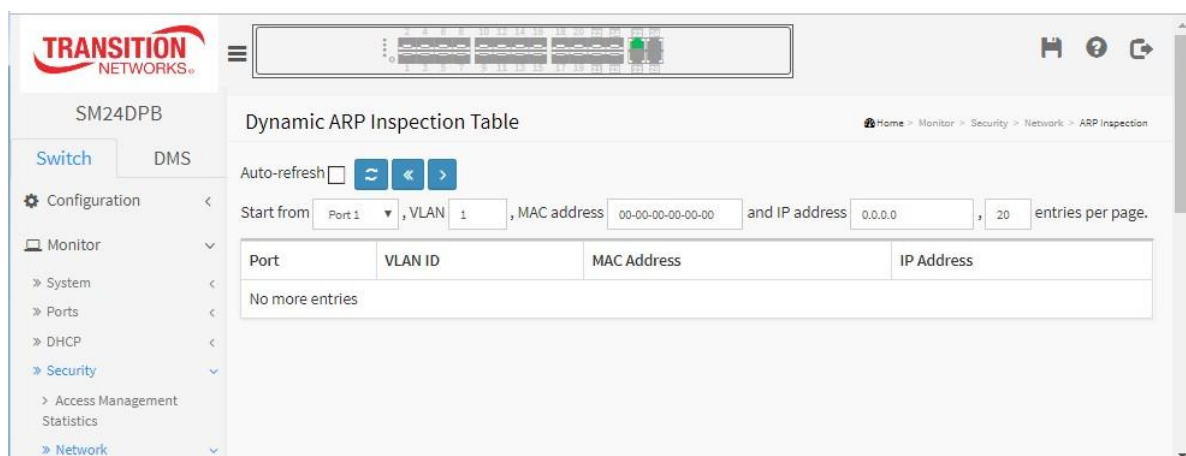
The > will use the last entry of the currently displayed table as a basis for the next lookup. When the end is reached the text "No more entries" is shown in the displayed table. Use the Refresh button to start over.

#### Web Interface

To configure a Dynamic ARP Inspection Table Configuration in the web interface:

1. Click Monitor, Security, Network, ARP Inspection.
2. Check "Auto-refresh".
3. Click "Refresh" to refresh the port detailed statistics.
4. Specify the Start from port, VLAN ID, MAC Address, IP Address, and entries per page.

**Figure 3-5.2.4: Dynamic ARP Inspection Table**



#### Parameter descriptions:

**Port :** Switch Port Number for which the entries are displayed.

**VLAN ID :** VLAN-ID in which the ARP traffic is permitted.

**MAC Address :** User MAC address of the entry.

**IP Address :** User IP address of the entry.





## Buttons

**Auto-refresh:** Check this box to refresh the page automatically every 3 seconds.

**Refresh:** Click to manually refresh the page immediately.

**<<:** Updates the system log entries to the first available entry ID.

**> :** Updates the system log entry to the next available entry ID.

### 3-5.2.5 IP Source Guard

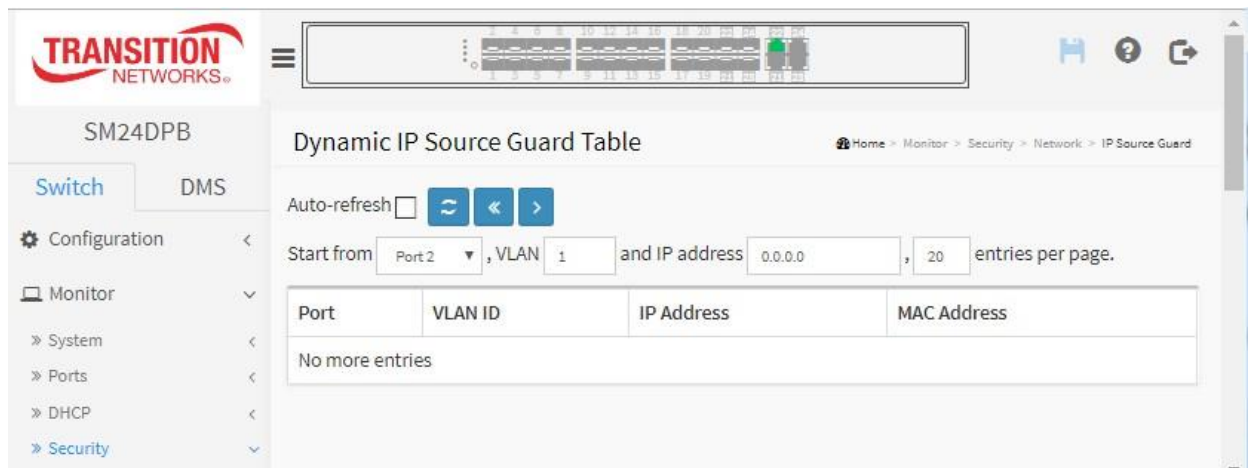
Entries in the Dynamic IP Source Guard Table are shown on this page. The Dynamic IP Source Guard Table is sorted first by port, then by VLAN ID, then by IP address, and then by MAC address.

#### **Web Interface**

To configure a Dynamic IP Source Guard Table Configuration in the web interface:

1. Click Monitor, Security, Network, IP Source Guard.
2. Check "Auto-refresh".
3. Click "Refresh" to refresh the port detailed statistics.
4. Specify the Start from port, VLAN ID, IP Address, and entries per page.

**Figure 3-5.2.5: Dynamic IP Source Guard Table**



#### **Parameter descriptions:**

**Port :** Switch Port Number for which the entries are displayed.

**VLAN ID :** VLAN-ID in which the IP traffic is permitted.

**IP Address :** User IP address of the entry.

**MAC Address :** Source MAC address.

#### **Buttons**

**Auto-refresh:** Check this box to refresh the page automatically every 3 seconds.

**Refresh:** Click to manually refresh the page immediately.

**<<:** Updates the system log entries to the first available entry ID.

**> :** Updates the system log entry to the next available entry ID.



### 3-5.3 AAA

#### 3-5.3.1 RADIUS Overview

This section shows you an overview of the RADIUS Authentication and Accounting servers status to ensure the function is workable.

#### **Web Interface**

To configure a RADIUS Overview Configuration in the web interface:

1. Click Monitor, Security, AAA, and then RADIUS Overview.
2. Check "Auto-refresh".
3. Click "Refresh" to refresh the port detailed statistics.

**Figure 3-5.3.1: RADIUS Server Status Overview page**

The screenshot displays the RADIUS Server Status Overview page. The left sidebar shows the navigation menu with 'Security' > 'AAA' > 'RADIUS Overview' selected. The main content area is titled 'RADIUS Server Status Overview' and contains two tables.

**RADIUS Authentication Server Status Overview**

#	IP Address	Status
1	0.0.0.0:0	Disabled
2	0.0.0.0:0	Disabled
3	0.0.0.0:0	Disabled
4	0.0.0.0:0	Disabled
5	0.0.0.0:0	Disabled

**RADIUS Accounting Server Status Overview**

#	IP Address	Status
1	0.0.0.0:0	Disabled
2	0.0.0.0:0	Disabled
3	0.0.0.0:0	Disabled
4	0.0.0.0:0	Disabled
5	0.0.0.0:0	Disabled

#### **Parameter descriptions:**

#### **RADIUS Authentication Server Status Overview**

**#** : 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 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 Overview**

**#** : 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.

### 3-5.3.2 RADIUS Details

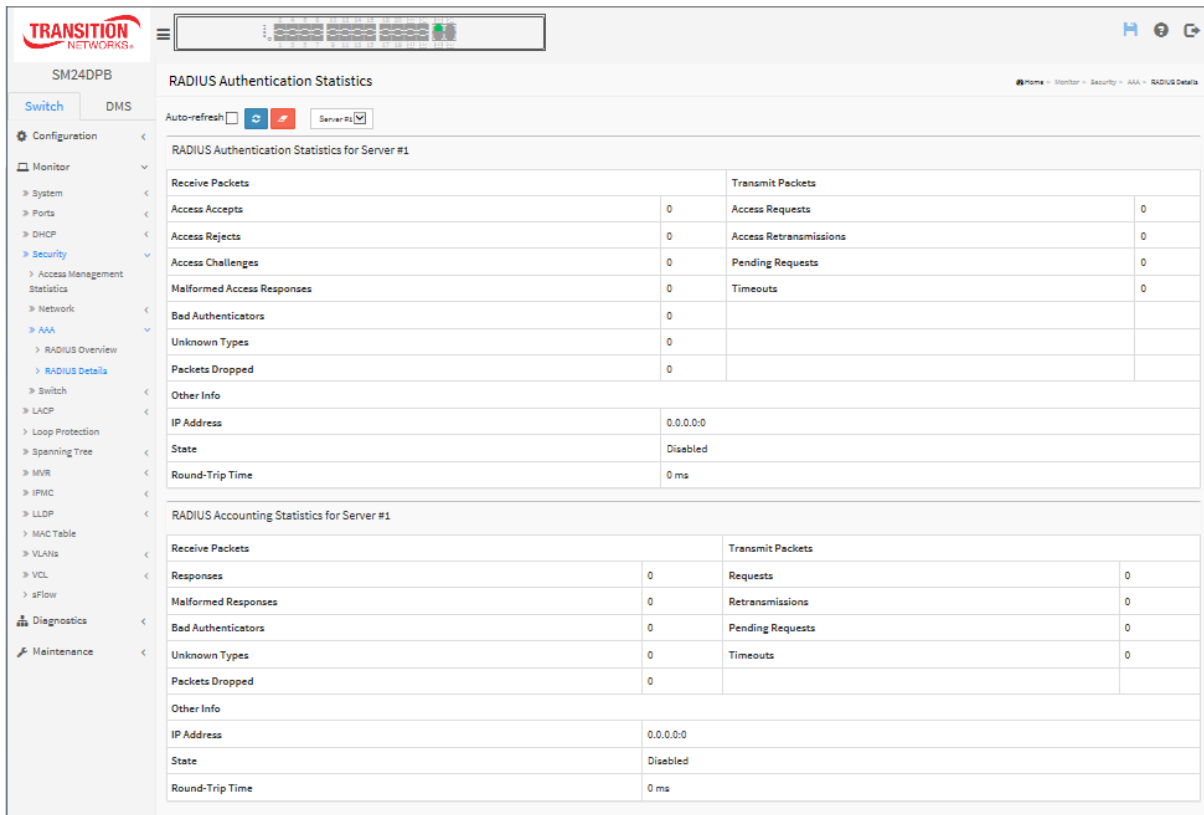
This page displays detailed statistics for a specified RADIUS server.

#### Web Interface

To display a RADIUS Details Configuration in the web interface:

1. Specify Port which you want to check.
2. Click Security, AAA, RADIUS Overview.
3. Check “Auto-refresh”.
4. Click “Refresh” to refresh the port detailed statistics or clear all information when you click “Clear”.

**Figure 3-5.3.2: RADIUS Authentication Statistics page**



#### Parameter descriptions:

#### RADIUS Authentication Statistics

The statistics map closely to those specified in RFC4668 - RADIUS Authentication Client MIB. Use the server select box to switch between the backend servers to show details for.

### Packet Counters

RADIUS authentication server packet counter. There are seven receive and four transmit counters.

Direction	Name	RFC4668 Name	Description
Rx	<b>Access Accepts</b>	radiusAuthClientExtAccessAccepts	The number of RADIUS Access-Accept packets (valid or invalid) received from the server.
Rx	<b>Access Rejects</b>	radiusAuthClientExtAccessRejects	The number of RADIUS Access-Reject packets (valid or invalid) received from the server.
Rx	<b>Access Challenges</b>	radiusAuthClientExtAccessChallenges	The number of RADIUS Access-Challenge packets (valid or invalid) received from the server.
Rx	<b>Malformed Access Responses</b>	radiusAuthClientExtMalformedAccessResponses	The number of malformed RADIUS Access-Response packets received from the server. Malformed packets include packets with an invalid length. Bad authenticators or Message Authenticator attributes or unknown types are not included as malformed access responses.
Rx	<b>Bad Authenticators</b>	radiusAuthClientExtBadAuthenticators	The number of RADIUS Access-Response packets containing invalid authenticators or Message Authenticator attributes received from the server.
Rx	<b>Unknown Types</b>	radiusAuthClientExtUnknownTypes	The number of RADIUS packets that were received with unknown types from the server on the authentication port and dropped.
Rx	<b>Packets Dropped</b>	radiusAuthClientExtPacketsDropped	The number of RADIUS packets that were received from the server on the authentication port and dropped for some other reason.
Tx	<b>Access Requests</b>	radiusAuthClientExtAccessRequests	The number of RADIUS Access-Request packets sent to the server. This does not include retransmissions.
Tx	<b>Access Retransmissions</b>	radiusAuthClientExtAccessRetransmissions	The number of RADIUS Access-Request packets retransmitted to the RADIUS authentication server.
Tx	<b>Pending Requests</b>	radiusAuthClientExtPendingRequests	The number of RADIUS Access-Request packets destined for the server that have not yet timed out or received a response. This variable is incremented when an Access-Request is sent and decremented due to receipt of an Access-Accept, Access-Reject, Access-Challenge, timeout, or retransmission.
Tx	<b>Timeouts</b>	radiusAuthClientExtTimeouts	The number of authentication timeouts to the server. After a timeout, the client may retry to the same server, send to a different server, or give up. A retry to the same server is counted as a retransmit as well as a timeout. A send to a different server is counted as a Request as well as a timeout.

### Other Info

This section contains information about the state of the server and the latest round-trip time.

Name	RFC4668 Name	Description
<b>IP Address</b>	-	IP address and UDP port for the authentication server in question.
<b>State</b>	-	Shows the state of the server. It takes one of these values: Disabled: The selected server is disabled. Not Ready: The server is enabled, but IP communication is not yet up and running. Ready: The server is enabled, IP communication is up and running, and the RADIUS module is ready to accept access attempts. Dead (X seconds left): Access attempts were made to this server, but it did not reply within the configured timeout. The server has temporarily been disabled but will get re-enabled when the dead-time expires. The number of seconds left before this occurs is displayed in parentheses. This state is only reachable when more than one server is enabled.
<b>Round-Trip Time</b>	radiusAuthClientExtRoundTripTime	The time interval (measured in milliseconds) between the most recent Access-Reply/Access-Challenge and the Access-Request that matched it from the RADIUS authentication server. The granularity of this measurement is 100 ms. A value of 0 ms indicates that there hasn't been round-trip communication with the server yet.

### RADIUS Accounting Statistics

The statistics map closely to those specified in RFC4670 - RADIUS Accounting Client MIB. Use the server select box to switch between the backend servers to show details for.

### Packet Counters

RADIUS accounting server packet counter. There are five receive and four transmit counters.

Direction	Name	RFC4670 Name	Description
Rx	<b>Responses</b>	radiusAccClientExtResponses	The number of RADIUS packets (valid or invalid) received from the server.
Rx	<b>Malformed Responses</b>	radiusAccClientExtMalformedResponses	The number of malformed RADIUS packets received from the server. Malformed packets include packets with an invalid length. Bad authenticators or unknown types are not included as malformed access responses.
Rx	<b>Bad Authenticators</b>	radiusAcctClientExtBadAuthenticators	The number of RADIUS packets containing invalid authenticators received from the server.
Rx	<b>Unknown Types</b>	radiusAccClientExtUnknownTypes	The number of RADIUS packets of unknown types that were received from the server on the accounting port.
Rx	<b>Packets Dropped</b>	radiusAccClientExtPacketsDropped	The number of RADIUS packets that were received from the server on the accounting port and dropped for some other reason.

Tx	<b>Requests</b>	radiusAccClientExtRequests	The number of RADIUS packets sent to the server. This does not include retransmissions.
Tx	<b>Retransmissions</b>	radiusAccClientExtRetransmissions	The number of RADIUS packets retransmitted to the RADIUS accounting server.
Tx	<b>Pending Requests</b>	radiusAccClientExtPendingRequests	The number of RADIUS packets destined for the server that have not yet timed out or received a response. This variable is incremented when a Request is sent and decremented due to receipt of a Response, timeout, or retransmission.
Tx	<b>Timeouts</b>	radiusAccClientExtTimeouts	The number of accounting timeouts to the server. After a timeout, the client may retry to the same server, send to a different server, or give up. A retry to the same server is counted as a retransmit as well as a timeout. A send to a different server is counted as a Request as well as a timeout.

**Other Info**

This section contains information about the state of the server and the latest round-trip time.

Name	RFC4670 Name	Description
<b>IP Address</b>	-	IP address and UDP port for the accounting server in question.
<b>State</b>	-	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.
<b>Round-Trip Time</b>	radiusAccClientExtRoundTripTime	The time interval (measured in milliseconds) between the most recent Response and the Request that matched it from the RADIUS accounting server. The granularity of this measurement is 100 ms. A value of 0 ms indicates there has been no round-trip communication with the server yet.

**Buttons:**

**Auto-refresh** –Check this box to enable an automatic refresh of the page at regular intervals.

**Refresh** - Click to refresh the page immediately.

**Clear** - Clears the counters for the selected server. The "Pending Requests" counter will not be cleared by this operation.



### 3-5.4 Switch

#### 3-5.4.1 RMON

##### 3-5.4.1.1 Statistics

This page provides an overview of RMON Statistics entries. Each page shows up to 99 entries from the Statistics table, default being 20, selected through the "entries per page" input field. When first visited, the web page will show the first 20 entries from the beginning of the Statistics table. The first displayed will be the one with the lowest ID found in the Statistics table.

The "Start from Control Index" lets you select the starting point in the Statistics table. Clicking the > button will update the displayed table starting from that or the next closest Statistics table match.

The << will use the last entry of the currently displayed entry as a basis for the next lookup. When the end is reached the text "No more entries" is shown in the displayed table. Use the Refresh button to start over.

#### Web Interface

To configure a RMON Statistics in the web interface:

1. Specify Port which want to check.
2. Click Security, Switch, RMON ,then Statistics.
3. Check "Auto-refresh".
4. Click "Refresh" to refresh the port detailed statistics.

**Figure 3-5.4.1.1: RMON Statistics Status Overview page**



#### Parameter descriptions:

**ID** : Indicates the index of Statistics entry.

**Data Source(ifIndex)** : The port ID which wants to be monitored.

**Drop** : The total number of events in which packets were dropped by the probe due to lack of resources.

**Octets** : The total number of octets of data (including those in bad packets) received on the network.

**Pkts** : The total number of packets (including bad packets, broadcast packets, and multicast packets) received.

**Broad-cast** : The total number of good packets received that were directed to the broadcast address.

**Multi-cast** : The total number of good packets received that were directed to a multicast address.

**CRC Errors** : The total number of packets received that had a length (excluding framing bits, but including FCS octets) of between 64 and 1518 octets, inclusive, but had either a bad Frame Check Sequence (FCS) with an integral number of octets (FCS Error) or a bad FCS with a non-integral number of octets (Alignment Error).

**Under-size** : The total number of packets received that were less than 64 octets.

**Over-size** : The total number of packets received that were longer than 1518 octets.

**Frag.** : The number of frames which size is less than 64 octets received with invalid CRC.

**Jabb.** : The number of frames which size is larger than 64 octets received with invalid CRC.

**Coll.** : The best estimate of the total number of collisions on this Ethernet segment.

**64** : The total number of packets (including bad packets) received that were 64 octets in length.

**65~127** : The total number of packets (including bad packets) received that were between 65 to 127 octets in length.

**128~255** : The total number of packets (including bad packets) received that were between 128 to 255 octets in length.

**256~511** : The total number of packets (including bad packets) received that were between 256 to 511 octets in length.

**512~1023** : The total number of packets (including bad packets) received that were between 512 to 1023 octets in length.

**1024~1588** : The total number of packets (including bad packets) received that were between 1024 to 1588 octets in length.

Auto-refresh    

### Buttons

**Auto-refresh:** Check this box to refresh the page automatically every 3 seconds.

**Refresh:** Click to refresh the page immediately.

**<<** : Updates the table starting from the first entry in the Statistics table, i.e. the entry with the lowest ID.

**>** : Updates the table, starting with the entry after the last entry currently displayed.

### 3-5.4.1.2 History

This section provides an overview of RMON History entries. Each page shows up to 99 entries from the History table, default being 20, selected through the "entries per page" input field. When first visited, this page shows the first 20 entries from the beginning of the History table. The first entry displayed will be the one with the lowest History Index and Sample Index found in the History table.

The "Start from History Index and Sample Index" lets you select the starting point in the History table. Clicking the > button will update the displayed table starting from that or the next closest History table match.

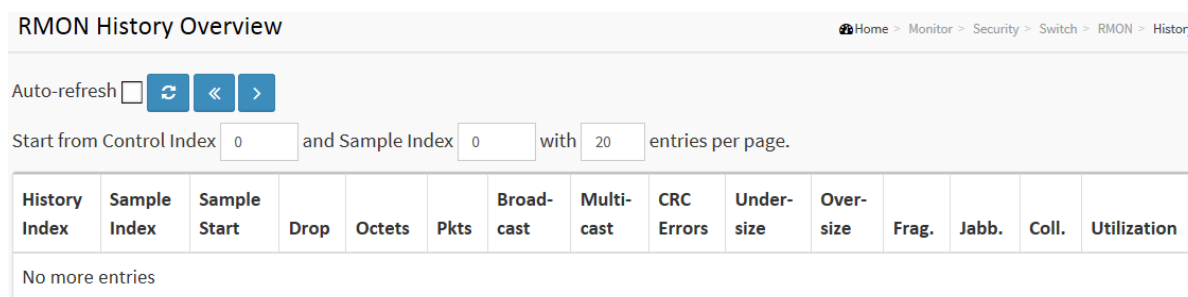
The > will use the last entry of the currently displayed entry as a basis for the next lookup. When the end is reached the text "No more entries" is shown in the displayed table. Use the Refresh button to start over.

#### Web Interface

To configure a RMON history Configuration in the web interface:

1. Specify which Port wants to check.
2. Click Security, Switch, RMON, History.
3. Check "Auto-refresh".
4. Click "Refresh" to refresh the port detailed statistics or clear all information when you click "Clear".

**Figure 3-5.4.1.2: RMON History Overview page**



#### Parameter descriptions:

**History Index :** Indicates the index of History control entry.

**Sample Index :** Indicates the index of the data entry associated with the control entry.

**Sample Start :** The value of sysUpTime at the start of the interval over which this sample was measured.

**Drop :** The total number of events in which packets were dropped by the probe due to lack of resources.

**Octets :** The total number of octets of data (including those in bad packets) received on the network.

**Pkts :** The total number of packets (including bad packets, broadcast packets, and multicast packets) received.

**Broadcast :** The total number of good packets received that were directed to the broadcast address.

**Multicast :** The total number of good packets received that were directed to a multicast address.

**CRC Errors :** The total number of packets received that had a length (excluding framing bits, but including FCS octets) of between 64 and 1518 octets, inclusive, but had either a bad Frame Check Sequence (FCS) with an integral number of octets (FCS Error) or a bad FCS with a non-integral number of octets (Alignment Error).

**Undersize :** The total number of packets received that were less than 64 octets.

**Oversize :** The total number of packets received that were longer than 1518 octets.

**Frag. :** The number of frames which size is less than 64 octets received with invalid CRC.

**Jabb.** : The number of frames which size is larger than 64 octets received with invalid CRC.

**Coll.** : The best estimate of the total number of collisions on this Ethernet segment.

**Utilization** : The best estimate of the mean physical layer network utilization on this interface during this sampling interval, in hundredths of a percent.

## Buttons



**Auto-refresh:** Check this box to refresh the page automatically every 3 seconds.

**Refresh:** Click to refresh the page immediately.

**<<** : Updates the table starting from the first entry in the History table (i.e., the entry with the lowest History Index and Sample Index).

**>** : Updates the table, starting with the entry after the last entry currently displayed.

### 3-5.4.1.3 Alarm

This page provides an overview of RMON Alarm entries. Each page shows up to 99 entries from the Alarm table, default being 20, selected through the "entries per page" input field. When first visited, the web page will show the first 20 entries from the beginning of the Alarm table. The first displayed will be the one with the lowest ID found in the Alarm table.

The "Start from Control Index" lets you select the starting point in the Alarm table. Clicking the Refresh button will update the displayed table starting from that or the next closest Alarm table match.

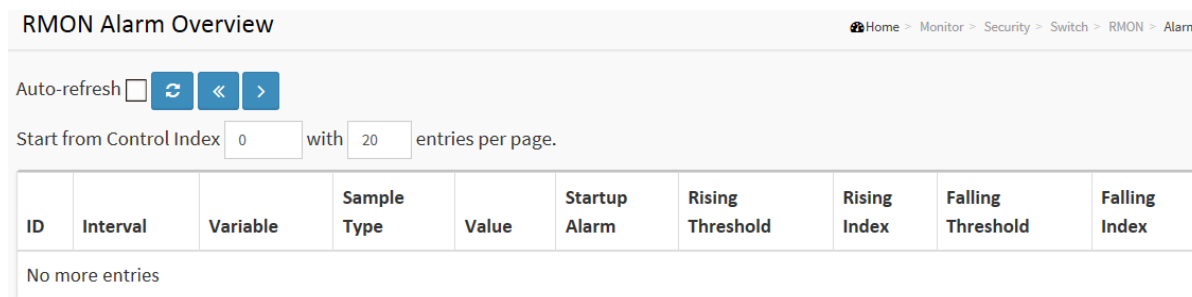
The > button will use the last entry of the currently displayed entry as a basis for the next lookup. When the end is reached the text "No more entries" is shown in the displayed table. Use the << button to start over.

#### Web Interface

To configure a RMON Alarm Overview in the web interface:

1. Click Security, Switch, RMON, Alarm.
2. Specify which Port you want to check.
3. Check Auto-refresh.
4. Click Refresh to refresh the statistics.

**Figure 3-5.4.1.3: RMON Alarm Overview page**



#### Parameter descriptions:

**ID :** Indicates the index of Alarm control entry.

**Interval :** Indicates the interval in seconds for sampling and comparing the rising and falling threshold.

**Variable :** Indicates the particular variable to be sampled

**Sample Type :** The method of sampling the selected variable and calculating the value to be compared against the thresholds.

**Value :** The value of the statistic during the last sampling period.

**Startup Alarm :** The alarm that may be sent when this entry is first set to valid.

**Rising Threshold :** Rising threshold value.

**Rising Index :** Rising event index.

**Falling Threshold :** Falling threshold value.

**Falling Index :** Falling event index.



#### Buttons

**Auto-refresh:** Check this box to refresh the page automatically every 3 seconds.

**Refresh:** Click to refresh the page immediately.

- <<: Updates the table starting from the first entry in the Alarm Table, i.e. the entry with the lowest ID.
- > : Updates the table, starting with the entry after the last entry currently displayed.

### 3-5.4.1.4 Event

This page provides an overview of RMON Event table entries. Each page shows up to 99 entries from the Event table, default being 20, selected through the "entries per page" input field. When first visited, the web page will show the first 20 entries from the beginning of the Event table. The first displayed will be the one with the lowest Event Index and Log Index found in the Event table .

The "Start from Event Index and Log Index" lets you select the starting point in the Event table. Clicking the > button will update the displayed table starting from that or the next closest Event table match.

The > will use the last entry of the currently displayed entry as a basis for the next lookup. When the end is reached the text "No more entries" is shown in the displayed table. Use the Refresh button to start over.

#### Web Interface

To configure a RMON Event Overview in the web interface:

1. Click Security, Switch, RMON, Event.
2. Check Auto-refresh.
3. Click Refresh to refresh the port detailed statistics
4. Specify which Port you want to check.

**Figure 3-5.4.1.4: RMON Event Overview page**

RMON Event Overview Home > Monitor > Security > Switch > RMON > Event

Auto-refresh  ↻ << >>

Start from Control Index  and Sample Index  with  entries per page.

Event Index	LogIndex	LogTime	LogDescription
No more entries			

#### Parameter descriptions:

**Event Index** : Indicates the index of the event entry.

**Log Index** : Indicates the index of the log entry.

**LogTime** : Indicates Event log time

**LogDescription** : Indicates the Event description.

#### Buttons

Auto-refresh  ↻ << >>

**Auto-refresh:** Check this box to refresh the page automatically every 3 seconds.

**Refresh:** Click to refresh the page immediately.

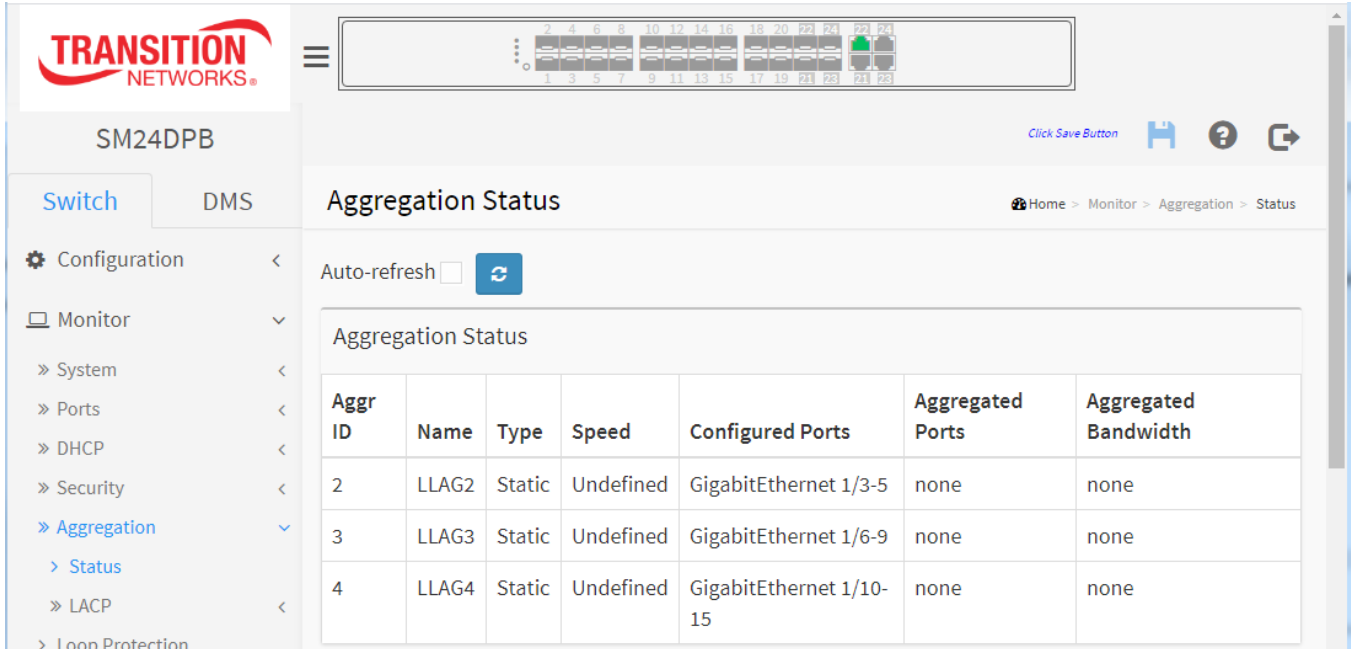
**<<** : Updates the table starting from the first entry in the Event Table, i.e. the entry with the lowest Event Index and Log Index.

**>>** : Updates the table, starting with the entry after the last entry currently displayed

## 3-6 Monitor > Aggregation > Status

### 3-6.1 System Status

This page displays the status of ports in the Aggregation group.



The screenshot shows the SM24DPB web interface. The left sidebar contains a navigation menu with 'Switch' selected and 'DMS' as a sub-option. The main content area is titled 'Aggregation Status' and includes an 'Auto-refresh' checkbox and a refresh button. Below this is a table with the following data:

Aggr ID	Name	Type	Speed	Configured Ports	Aggregated Ports	Aggregated Bandwidth
2	LLAG2	Static	Undefined	GigabitEthernet 1/3-5	none	none
3	LLAG3	Static	Undefined	GigabitEthernet 1/6-9	none	none
4	LLAG4	Static	Undefined	GigabitEthernet 1/10-15	none	none

#### Parameter descriptions:

**Aggr ID:** The Aggregation ID associated with this aggregation instance.

**Name:** Name of the Aggregation group ID.

**Type:** Type of the Aggregation group(Static or LACP).

**Speed:** Speed of the Aggregation group.

**Configured Ports:** Configured member ports of the Aggregation group.

**Aggregated Ports:** Aggregated member ports of the Aggregation group.

**Aggregated Bandwidth:** Aggregated Bandwidth of the Aggregation group.

#### Buttons

**Auto-refresh:** Click to automatically refresh the webpage every 3 seconds.

**Refresh:** Click to manually refresh the page immediately.



## 3-7 LACP

### 3-6.1 System Status

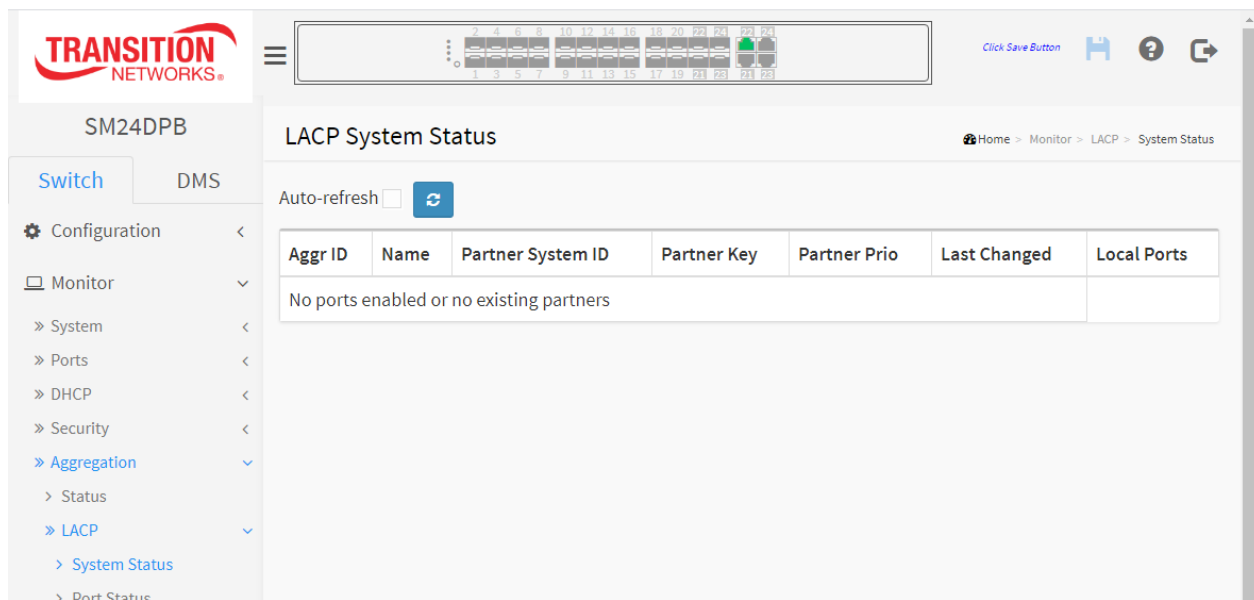
This page provides a status overview for all LACP instances.

#### Web Interface

To display the LACP System status in the web interface:

1. Click Monitor, **Aggregation**, LACP, System Status.
2. Check Auto-refresh.
3. Click Refresh to refresh the LACP system status.

**Figure 3-6.1 LACP System Status page**



#### Parameter descriptions:

**Aggr ID** : The Aggregation ID associated with this aggregation instance. For LLAG the id is shown as 'isid: aggr-id' and for GLAGs as 'aggr-id'

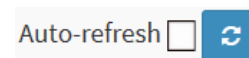
**Partner System ID** : The system ID (MAC address) of the aggregation partner.

**Partner Key** : The Key that the partner has assigned to this aggregation ID.

**Last Changed** : The time since this aggregation changed.

**Local Ports** : Shows which ports are a part of this aggregation for this switch. The format is: "Switch ID:Port".

#### Buttons



**Auto-refresh**: Check this box to refresh the page automatically every 3 seconds.

**Refresh**: Click to manually refresh the page immediately.

### 3-6.2 Port Status

This page provides a status overview for LACP status for all ports.

#### Web Interface

To display the LACP Port status in the web interface:

1. Click Monitor, LACP, Port Status.
2. Check the Auto-refresh checkbox to refresh the page automatically every 3 seconds.
3. Click "Refresh" to refresh the LACP Port Status.

**Figure 3-6.2: LACP Status page**

Port	LACP	Key	Aggr ID	Partner System ID	Partner Port	Partner Prio
1	No	-	-	-	-	-
2	No	-	-	-	-	-
3	No	-	-	-	-	-
4	No	-	-	-	-	-
5	No	-	-	-	-	-
6	No	-	-	-	-	-
7	No	-	-	-	-	-
8	No	-	-	-	-	-
9	No	-	-	-	-	-
10	No	-	-	-	-	-
11	No	-	-	-	-	-

**Port :** The switch port number.

**LACP :** 'Yes' means that LACP is enabled and the port link is up. 'No' means that LACP is not enabled or that the port link is down. 'Backup' means that the port could not join the aggregation group but will join if other port leaves. Meanwhile its LACP status is disabled.

**Key :** The key assigned to this port. Only ports with the same key can aggregate together.

**Aggr ID :** The Aggregation ID assigned to this aggregation group. IDs 1 and 2 are GLAGs while IDs 3-14 are LLAGs.

**Partner System ID :** The partner's System ID (MAC address).

**Partner Port :** The partner's port number connected to this port.

**Partner Prio:** The partner's port priority.

#### Buttons

**Auto-refresh:** Check this box to refresh the page automatically every 3 seconds.

**Refresh:** Click to refresh the page immediately.

### 3-6.3 Port Statistics

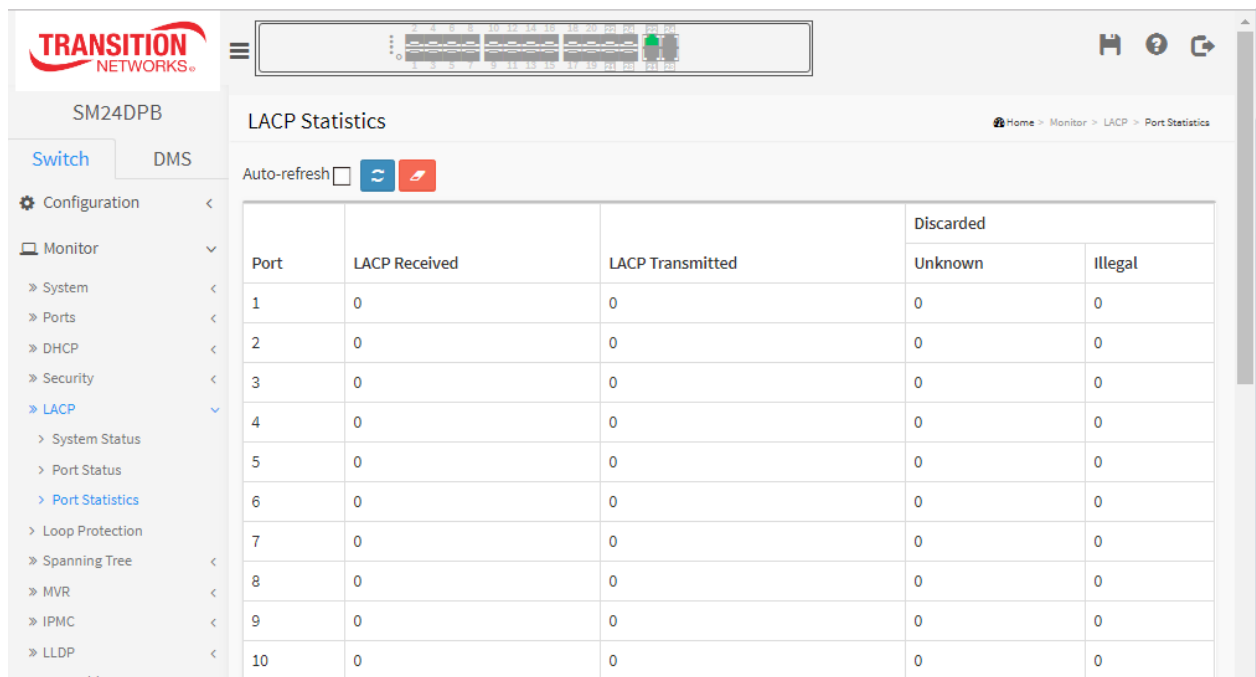
This section describes that when you complete to set LACP function on the switch then it provides a Port Statistics overview for all LACP instances.

#### Web Interface

To display the LACP Port status in the web interface:

1. Click Monitor, LACP, Port Statistics.
2. Check the Auto-refresh checkbox to refresh the page automatically every 3 seconds.
3. 3. Click Refresh to refresh the LACP Statistics immediately.

**Figure 3-6.3: LACP Statistics page**



#### Parameter descriptions:

**Port :** The switch port number.

**LACP Received :** Shows how many LACP frames have been received at each port.

**LACP Transmitted :** Shows how many LACP frames have been sent from each port.

**Discarded :** Shows how many unknown or illegal LACP frames have been discarded at each port.



#### Buttons

**Auto-refresh:** Check this box to refresh the page automatically every 3 seconds.

**Refresh:** Click to manually refresh the page immediately.

**Clear:** Clears the counters for the page.

### 3-8 Loop Protection

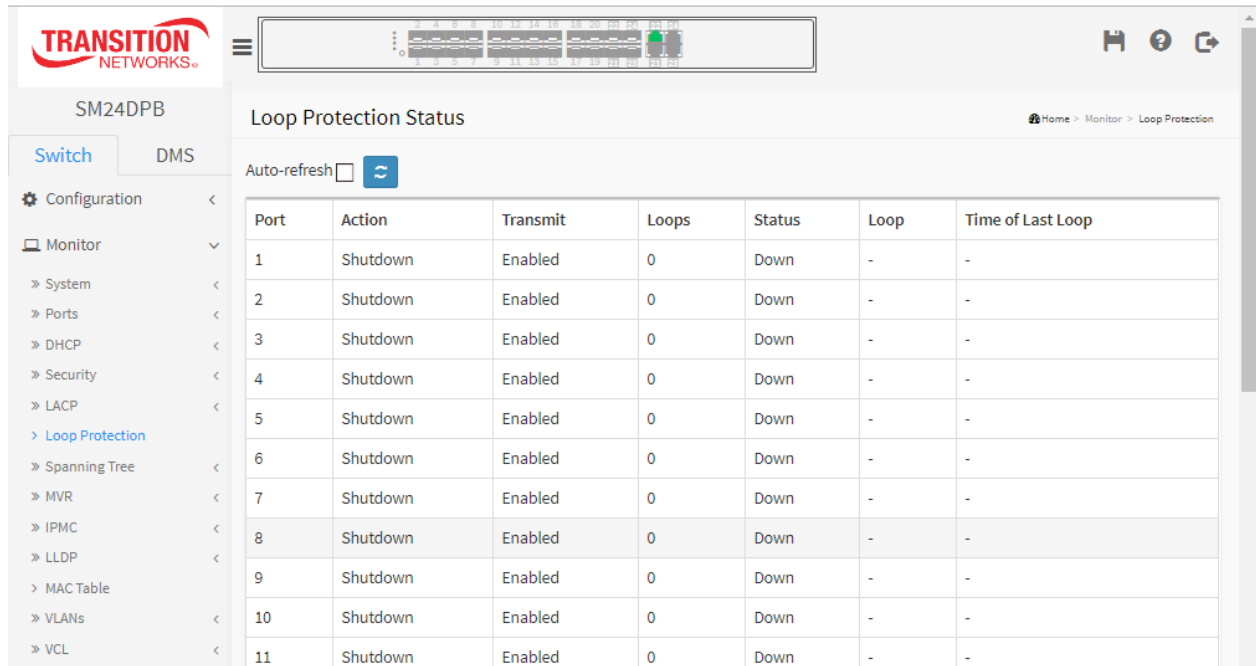
This page displays loop protection port status of the switch ports.

#### Web Interface

To display the Loop Protection status in the web interface:

1. Click Monitor, Loop Protection.
2. Check the Auto-refresh checkbox to refresh the page automatically every 3 seconds.
3. Click “Refresh” to refresh the LACP Statistics immediately (manually).

**Figure 3-7: Loop Protection Status page**



#### Parameter descriptions:

**Port :** The switch port number of the logical port.

**Action :** The currently configured port action.

**Transmit :** The currently configured port transmit mode.

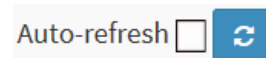
**Loops :** The number of loops detected on this port.

**Status :** The current loop protection status of the port.

**Loop :** Whether a loop is currently detected on the port.

**Time of Last Loop :** The time of the last loop event detected.

#### Buttons



**Refresh:** Click to refresh the page immediately.

**Auto-refresh:** Check this box to enable an automatic refresh of the page every 3 seconds.

## 3-9 Spanning Tree

### 3-8.1 Bridge Status

This page provides a status overview of all STP bridge instances. The table contains a row for each STP bridge instance

#### Web Interface

To display the STP Bridges status in the web interface:

1. Click Monitor, Spanning Tree, STP Bridges
2. Check the Auto-refresh checkbox to refresh the page automatically every 3 seconds.
3. Click Refresh to refresh the STP Bridges.
4. Click CIST to go to the next page "STP Detailed Bridge Status".

**Figure 3-8.1: STP Bridges status page**

The screenshot shows the web interface for SM24DPB. The left sidebar contains a navigation menu with 'Monitor' expanded to show 'Spanning Tree' and 'Bridge Status'. The main content area is titled 'STP Bridges' and includes an 'Auto-refresh' checkbox and a refresh button. Below this is a table with the following data:

MSTI	Bridge ID	Root			Topology Flag	Topology Change Last
		ID	Port	Cost		
CIST	32768.00-C0-F2-47-45-27	32768.00-C0-F2-47-45-27	-	0	Steady	-

#### Parameter descriptions:

**MSTI** : The Bridge Instance. This is also a link to the STP Detailed Bridge Status.

**Bridge ID** : The Bridge ID of this Bridge instance.

**Root ID** : The Bridge ID of the currently elected root bridge.

**Root Port** : The switch port currently assigned the root port role.

**Root Cost** : Root Path Cost. For the Root Bridge it is zero. For all other Bridges, it is the sum of the Port Path Costs on the least cost path to the Root Bridge.

**Topology Flag** : The current state of the Topology Change Flag of this Bridge instance.

**Topology Change Last** : The time since last Topology Change occurred.



#### Buttons

**Auto-refresh:** Check this box to refresh the page automatically every 3 seconds.

**Refresh:** Click to refresh the page immediately (manually).

### 3-8.2 Port Status

This page displays the STP CIST port status for physical ports of the switch.

#### Web Interface

To display the STP Port Status in the web interface:

1. Click Monitor, Spanning Tree, STP Port Status.
2. View the STP Port Status page parameters.
3. Check the Auto-refresh checkbox to cause the switch to refresh this page automatically every three seconds. Or click Refresh to refresh the page immediately.

**Figure 3-8.2: STP Port Status page**

The screenshot shows the web interface for the SM24DPB switch. The main content area is titled "STP Port Status" and includes a breadcrumb trail: Home > Monitor > Spanning Tree > Port Status. Below the title is an "Auto-refresh" checkbox (unchecked) and a refresh button. A table displays the status of 8 ports:

Port	CIST Role	CIST State	Uptime
1	Non-STP	Forwarding	-
2	Non-STP	Forwarding	-
3	Non-STP	Forwarding	-
4	Non-STP	Forwarding	-
5	Non-STP	Forwarding	-
6	Non-STP	Forwarding	-
7	Non-STP	Forwarding	-
8	Non-STP	Forwarding	-

#### Parameter descriptions:

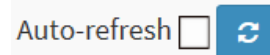
**Port :** The switch port number of the logical STP port.

**CIST Role :** The current STP port role of the CIST port. The port role can be one of the following values: *Alternate Port, Backup Port, Root Port, Designated Port, or Disabled.*

**CIST State :** The current STP port state of the CIST port. The port state can be one of the following values: *Blocking, Learning, or Forwarding.*

**Uptime :** The time since the bridge port was last initialized.

#### Buttons



**Auto-refresh:** Check this box to refresh the page automatically every 3 seconds.

**Refresh:** Click to manually refresh the page immediately.

### 3-8.3 Port Statistics

This page displays the STP port statistics counters of bridge ports in the switch.

#### Web Interface

To display the STP Port status in the web interface:

1. Click Monitor, Spanning Tree, Port Statistics.
2. Check the Auto-refresh checkbox to automatically refresh the switch every three seconds.
3. Click "Refresh" to refresh the STP Bridges immediately.

**Figure 3-8.3: STP Statistics page**



#### Parameter descriptions:

**Port :** The switch port number of the logical STP port.

**MSTP :** The number of MSTP Configuration BPDU's received/transmitted on the port.

**RSTP :** The number of RSTP Configuration BPDU's received/transmitted on the port.

**STP :** The number of legacy STP Configuration BPDU's received/transmitted on the port.

**TCN :** The number of legacy Topology Change Notification BPDU's received/transmitted on the port.

**Discarded Unknown :** The number of unknown Spanning Tree BPDU's received (and discarded) on the port.

**Discarded Illegal :** The number of illegal Spanning Tree BPDU's received (and discarded) on the port.

#### Buttons



**Auto-refresh:** Check this box to refresh the page automatically every 3 seconds.

**Refresh:** Click to manually refresh the page immediately.

**Clear:** Clears the counters for the selected port.

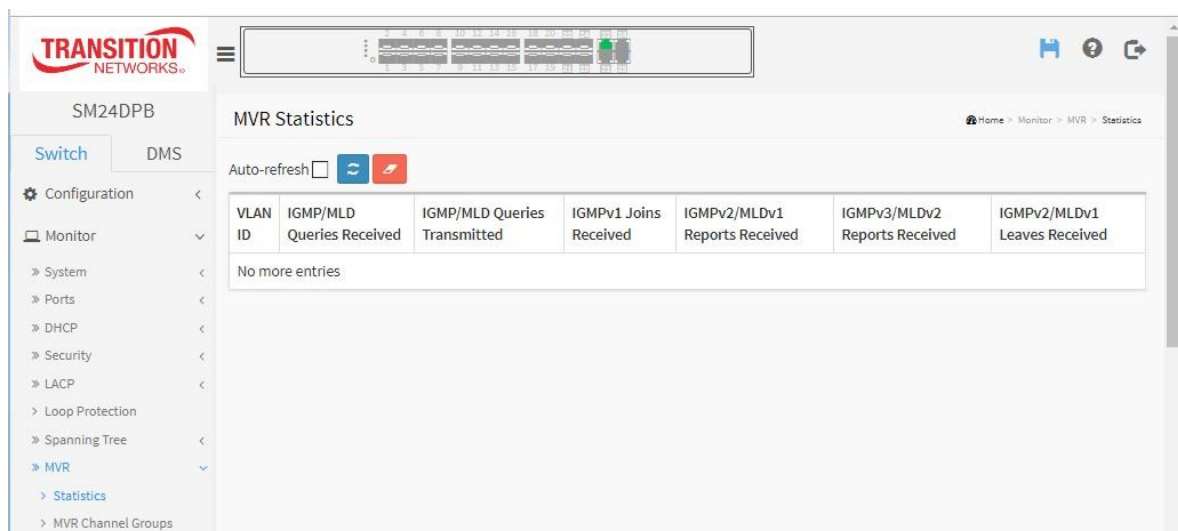
## 3-10 MVR

### 3-9.1 Statistics

This page provides detailed MVR Statistics information. To display the MVR Statistics Information in the web interface:

1. Click Monitor, MVR, Statistics
2. Check the Auto-refresh checkbox to refresh the page automatically every 3 seconds.
3. To Click the Refresh button to refresh the page immediately.

**Figure 3-9.1: MVR Statistics page**



#### **Parameter descriptions:**

**VLAN ID :** The Multicast VLAN ID.

**IGMP/MLD Queries Received :** The number of Received Queries for IGMP and MLD, respectively.

**IGMP/MLD Queries Transmitted :** The number of Transmitted Queries for IGMP and MLD, respectively.

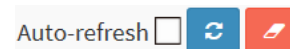
**IGMPv1 Joins Received :** The number of Received IGMPv1 Join's.

**IGMPv2/MLDv1 Report's Received :** The number of Received IGMPv2 Join's and MLDv1 Report's, respectively.

**IGMPv3/MLDv2 Report's Received :** The number of Received IGMPv1 Join's and MLDv2 Report's, respectively.

**IGMPv2/MLDv1 Leave's Received :** The number of Received IGMPv2 Leave's and MLDv1 Done's, respectively.

#### **Buttons**



**Auto-refresh:** Check this box to refresh the page automatically every 3 seconds.

**Refresh:** Click to refresh the page immediately (manually).

**Clear:** Clears the counters for the selected port.



### 3-9.2 MVR Channels Groups

This page displays MVR Groups detail information. 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 up to 99 entries from the MVR Group table, default being 20, selected through the "entries per page" input field. When first visited, the web page will show the first 20 entries from the beginning of the MVR Channels (Groups) Information table.

The "Start from VLAN", and "Group Address" input fields let you select the starting point in the MVR Channels (Groups) Information Table. Clicking the > button will update the displayed table starting from that or the closest next MVR Channels (Groups) Information Table match. In addition, the two input fields will - upon a << button click - assume the value of the first displayed entry, allowing for continuous refresh with the same start address.

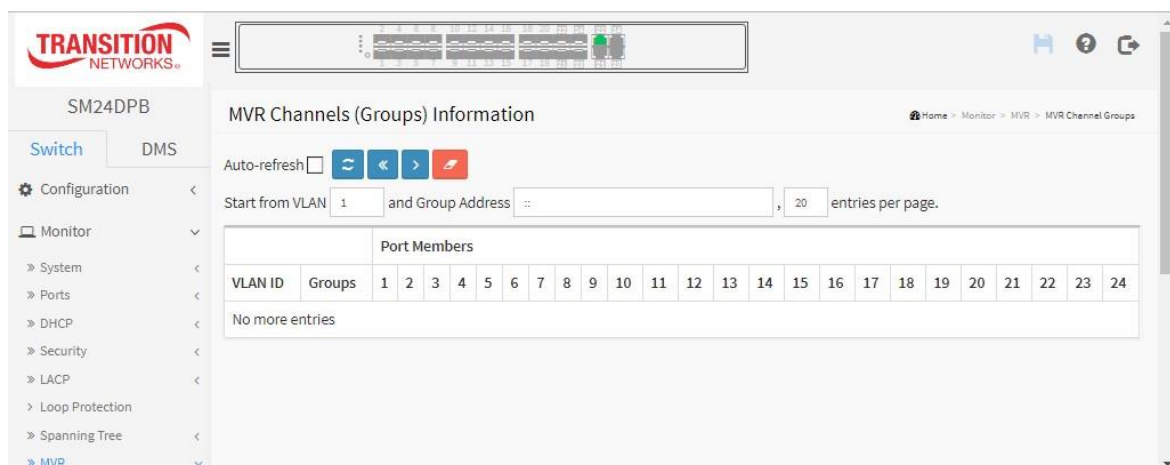
The > will use the last entry of the currently displayed table as a basis for the next lookup. When the end is reached the text "No more entries" is shown in the displayed table. Use the Refresh button to start over.

#### Web Interface

To display the MVR Groups Information in the web interface:

1. Click Monitor, MVR, Groups Information
2. Check the Auto-refresh checkbox to refresh the page automatically every 3 seconds.
3. Click the "Refresh" button to refresh an entry of the MVR Groups Information immediately.
4. Click << or > to move to previous or next entry.

**Figure 3-9.2: MVR Channels (Groups) Information page**



#### Parameter descriptions:

**VLAN ID :** VLAN ID of the group.

**Groups :** Group ID of the group displayed.

**Port Members :** Ports under this group.

#### Buttons



**Auto-refresh:** Check this box to refresh the page automatically every 3 seconds.

**Refresh:** Click to manually refresh the page immediately.

**<<:** Updates the system log entries to the first available entry ID.

**> :** Updates the system log entry to the next available entry ID.

**Clear :** Clears all Statistics counters.

### 3-9.3 MVR SFM Information

The MVR SFM (Source-Filtered Multicast) Information Table also contains the SSM (Source-Specific Multicast) information. This table is sorted first by VLAN ID, then by group, and then by Port. Different source addresses belong to the same group are treated as single entry.

Each page shows up to 99 entries from the MVR SFM Information Table, default being 20, selected through the "entries per page" input field. When first visited, the web page will show the first 20 entries from the beginning of the MVR SFM Information Table.

The "Start from VLAN", and "Group Address" input fields let you select the starting point in the MVR SFM Information Table. Clicking the > button will update the displayed table starting from that or the closest next MVR SFM Information Table match. In addition, the two input fields will - upon a button click - assume the value of the first displayed entry, allowing for continuous refresh with the same start address.

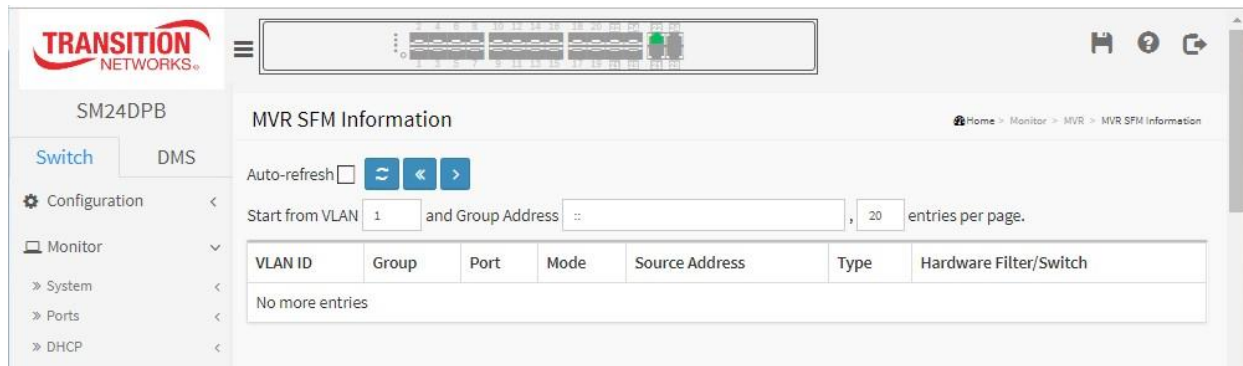
The > will use the last entry of the currently displayed table as a basis for the next lookup. When the end is reached the text "No more entries" is shown in the displayed table. Use the Refresh button to start over.

#### Web Interface

To display the MVR SFM Information in the web interface:

1. Click Monitor, MVR, MVR SFM Information.
2. Check the Auto-refresh checkbox to refresh the page automatically every 3 seconds.
3. Click the Refresh button to refresh the page immediately.
4. Click << or > to move to previous or next entry.

**Figure 3-9.2: MVR SFM Information page**



#### Parameter descriptions:

**VLAN ID** : VLAN ID of the group.

**Group** : Group address of the group displayed.

**Port** : Switch port number.

**Mode** : Indicates the filtering mode maintained per (VLAN ID, port number, Group Address) basis. It can be either Include or Exclude.

**Source Address** : IP Address of the source. Currently, system limits the total number of IP source addresses for filtering to be 128. When there is no any source filtering address, the text "None" is shown in the Source Address field.

**Type** : Indicates the Type. It can be either Allow or Deny.

**Hardware Filter/Switch** : Indicates whether data plane destined to the specific group address from the source IPv4/IPv6 address could be handled by the chip.

**Buttons**



**Auto-refresh:** Check this box to refresh the page automatically every 3 seconds.

**Refresh:** Click to manually refresh the page immediately.

**<<:** Updates the system log entries to the first available entry ID.

**> :** Updates the system log entry to the next available entry ID.

### 3-11 IPMC

#### 3-10.1 IGMP Snooping

##### 3-10.1.1 Status

After you complete the IGMP Snooping configuration, you can display IGMP Snooping Status. This section describes the IGMP Snooping detail status.



#### Web Interface

To display the IGMP Snooping status in the web interface:

1. Click Monitor, IGMP Snooping, Status.
2. Check the Auto-refresh checkbox to refresh the page automatically every 3 seconds.
3. Click the Refresh button to refresh the IGMP Snooping Status immediately.
4. Click the Clear button to clear the page. .

**Figure 3-10.1.1: IGMP Snooping Status page**

IGMP Snooping Status Home > Monitor > IPMC > IGMP Snooping > Status

Auto-refresh   

Statistics

VLAN ID	Querier Version	Host Version	Querier Status	Queries Transmitted	Queries Received	V1 Reports Received	V2 Reports Received	V3 Reports Received	V2 Leaves Received

Router Port

Port	Status
1	-
2	-
22	-
23	-
24	-

#### Parameter descriptions:

**VLAN ID** : The VLAN ID of the entry.

**Querier Version** : Working Querier Version currently.

**Host Version** : Working Host Version currently.

**Querier Status** : Shows the Querier status is "ACTIVE" or "IDLE". "DISABLE" denotes the specific interface is administratively disabled.

**Queries Transmitted** : The number of Transmitted Queries.

**Queries Received** : The number of Received Queries.

**V1 Reports Received** : The number of Received V1 Reports.

**V2 Reports Received** : The number of Received V2 Reports.

**V3 Reports Received** : The number of Received V3 Reports.

**V2 Leaves Received** : The number of Received V2 Leaves.

**Router Port** : Display which ports act as router ports. A router port is a port on the Ethernet switch that leads towards the Layer 3 multicast device or IGMP querier.

**Static** denotes the specific port is configured to be a router port.

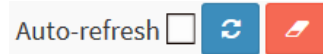
**Dynamic** denotes the specific port is learnt to be a router port.

**Both** denote the specific port is configured or learnt to be a router port.

**Port** : Switch port number.

**Status** : Indicate whether specific port is a router port or not.

## Buttons



**Auto-refresh:** Check this box to refresh the page automatically every 3 seconds.

**Refresh:** Click to manually refresh the page immediately.

**Clear:** Clears the counters for the selected port.

### 3-10.1.2 Group Information

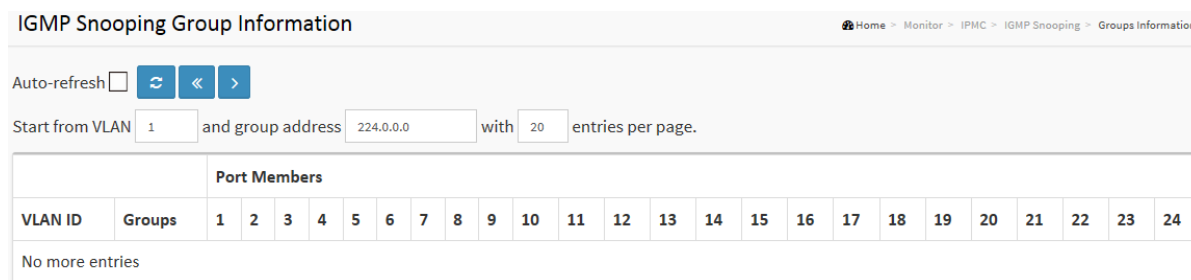
This page displays IGMP Snooping Group Information. Entries in the IGMP Group Table are shown on this page. The IGMP Group Table is sorted first by VLAN ID, and then by group. The > will use the last entry of the currently displayed table as a basis for the next lookup. When the end is reached the text "No more entries" is shown in the displayed table. Use the Refresh button to start over.

#### Web Interface

To display the IGMP Snooping Group Information in the web interface:

1. Click Monitor, IGMP Snooping, Group Information
2. Check the Auto-refresh checkbox to refresh the page automatically every 3 seconds.
3. Click Refresh to refresh the page.
4. Click << or > to move to the previous or next entry.

**Figure 3-10.1.2: IGMP Snooping Groups Information page**



#### Parameter descriptions:

Each page shows up to 99 entries from the IGMP Group table, default being 20, selected through the "entries per page" input field. When first visited, the web page will show the first 20 entries from the beginning of the IGMP Group Table.

The "Start from VLAN", and "group" input fields let you select the starting point in the IGMP Group Table. Clicking the > button will update the displayed table starting from that or the closest next IGMP Group Table match. In addition, the two input fields will - upon a button click - assume the value of the first displayed entry, allowing for continuous refresh with the same start address.

The > will use the last entry of the currently displayed table as a basis for the next lookup. When the end is reached the text "No more entries" is shown in the displayed table. Use the Refresh button to start over.

**VLAN ID** : VLAN ID of the group.

**Groups** : Group address of the group displayed.

**Port Members** : Ports under this group.



#### Buttons

**Auto-refresh:** Check this box to refresh the page automatically every 3 seconds.

**Refresh:** Click to refresh the page immediately (manually).

**<<:** Updates the system log entries to the first available entry ID.

**> :** Updates the system log entry to the next available entry ID.

### 3-10.1.3 IPv4 SFM Information

Entries in the IGMP SFM Information Table are shown on this page. The IGMP SFM (Source-Filtered Multicast) Information Table also contains the SSM (Source-Specific Multicast) information. This table is sorted first by VLAN ID, then by group, and then by Port. Different source addresses belong to the same group are treated as single entry.

#### Web Interface

To display the IPv4 SSM Information in the web interface:

1. Click Monitor, IGMP Snooping, IPv4 SSM Information.
2. Check the Auto-refresh checkbox to refresh the page automatically every 3 seconds.
3. Click the Refresh button to refresh the page.
4. Click << or > to move to the previous or next entry.

**Figure 3-10.1.3: IGMP SFM Information page**

IGMP SFM Information Home > Monitor > IPMC > IGMP Snooping > IPv4 SFM Information

Auto-refresh  ↻ ⏪ ⏩

Start from VLAN  and group address  with  entries per page.

VLAN ID	Group	Port	Mode	Source Address	Type	Hardware Filter/Switch
No more entries						

#### Parameter descriptions:

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 let you select the starting point in the IGMP SFM Information Table. Clicking the > 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 button click - assume the value of the first displayed entry, allowing for continuous refresh with the same start address.

The > will use the last entry of the currently displayed table as a basis for the next lookup. When the end is reached the text "No more entries" is shown in the displayed table. Use the Refresh button to start over.

**VLAN ID** : VLAN ID of the group.

**Group** : Group address of the group displayed.

**Port** : Switch port number.

**Mode** : Indicates the filtering mode maintained per (VLAN ID, port number, Group Address) basis. It can be either Include or Exclude.

**Source Address** : IP Address of the source. Currently, system limits the total number of IP source addresses for filtering to be 128.

**Type** : Indicates the Type. It can be either *Allow* or *Deny*.

**Hardware Filter/Switch** : Indicates whether data plane destined to the specific group address from the source IPv4 address could be handled by chip or not.

**Buttons**

**Auto-refresh:** Check this box to refresh the page automatically every 3 seconds.



**Refresh:** Click to refresh the page immediately (manually).

**<<:** Updates the system log entries to the first available entry ID.

**>:** Updates the system log entry to the next available entry ID.



### 3-10.2 MLD Snooping

#### 3-10.2.1 Status

This section describes MLD Snooping and how to display the MLD Snooping Status and detail information.

#### Web Interface

To display the MLD Snooping Status in the web interface:

1. Click Monitor, MLD Snooping, Status.
2. Check the Auto-refresh checkbox to refresh the page automatically every 3 seconds.
3. Click the Refresh button to refresh an entry of the MLD Snooping Status Information.
4. Click the Clear button to clear the page.

**Figure 3-10.2.1: MLD Snooping Status page**

MLD Snooping Status								
Auto-refresh <input type="checkbox"/>								
Statistics								
VLAN ID	Querier Version	Host Version	Querier Status	Queries Transmitted	Queries Received	V1 Reports Received	V2 Reports Received	V1 Leaves Received
Router Port								
Port	Status							
1	-							
2	-							
22	-							
23	-							
24	-							

#### 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.

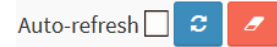
**Dynamic** denotes the specific port is learnt to be a router port.

**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 this box to refresh the page automatically every 3 seconds.

**Refresh:** Click to refresh the page immediately.

**Clear:** Clears the counters for the selected port.

### 3-10.2.2 Group Information

This section describes how to set the MLD Snooping Groups Information. The "Start from VLAN", and "group" input fields let you select the starting point in the MLD Group Table.

#### Web Interface

To display the MLD Snooping Group information in the web interface:

1. Click Monitor, MLD Snooping, Group Information.
2. Check the Auto-refresh checkbox to automatically refresh the switch every three seconds.
3. Click the Refresh button to refresh an entry of the MLD Snooping Group Information.
4. Click the Clear button to clear the page information.

**Figure 3-10.2.2: MLD Snooping Groups Information page**

MLD Snooping Group Information Home > Monitor > IPMC > MLD Snooping > Groups Information

Auto-refresh  ↻ << >>

Start from VLAN  and group address  with  entries per page.

		Port Members																							
VLAN ID	Groups	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24
No more entries																									

#### Parameter descriptions:

Each page shows up to 99 entries from the MLD Group table, default being 20, selected through the "entries per page" input field. When first visited, the web page will show the first 20 entries from the beginning of the MLD Group Table.

The "Start from VLAN", and "group" input fields let you select the starting point in the MLD Group table. Clicking the > button will update the displayed table starting from that or the closest next MLD Group Table match. In addition, the two input fields will - upon a << button click - assume the value of the first displayed entry, allowing for continuous refresh with the same start address.

The > will use the last entry of the currently displayed table as a basis for the next lookup. When the end is reached the text "No more entries" displays in the displayed table. Use the Refresh button to start over.

**VLAN ID** : VLAN ID of the group.

**Groups** : Group address of the group displayed.

**Port Members** : Ports under this group.

#### Buttons

Auto-refresh  ↻ << >>

**Auto-refresh:** Check this box to refresh the page automatically every 3 seconds.

**Refresh:** Click to refresh the page immediately.

**<<:** Updates the system log entries to the first available entry ID

**> :** Updates the system log entry to the next available entry ID

### 3-10.2.3 IPv6 SFM Information

Entries in the MLD SFM Information Table are shown on this page. The MLD SFM (Source-Filtered Multicast) Information Table also contains the SSM (Source-Specific Multicast) information. This table is sorted first by VLAN ID, then by group, and then by Port. Different source addresses belong to the same group are treated as single entry.

#### Web Interface

To display the MLDv2 IPv6 SSM Information in the web interface:

1. Click Monitor, MLD Snooping, IPv6 SFM Information.
2. Check the Auto-refresh checkbox to refresh the page automatically every 3 seconds.
3. Click the Refresh button to refresh the page information.
4. Click << or > to move to the Previous or Next entry.

**Figure 3-10.2.3: IPv6 MLD SFM Information page**

MLD SFM Information Home > Monitor > IPMC > MLD Snooping > IPv6 SFM Information

Auto-refresh  ↻ << >

Start from VLAN  and group address  with  entries per page.

VLAN ID	Group	Port	Mode	Source Address	Type	Hardware Filter/Switch
No more entries						

#### Parameter descriptions:

Each page shows up to 99 entries from the MLD SFM Information table, default being 20, selected through the "entries per page" input field. When first visited, the web page will show the first 20 entries from the beginning of the MLD SFM Information Table.

The "Start from VLAN", and "group" input fields let you select the starting point in the MLD SFM Information Table. Clicking the > button will update the displayed table starting from that or the closest next MLD SFM Information Table match. In addition, the two input fields will - upon a << button click - assume the value of the first displayed entry, allowing for continuous refresh with the same start address.

The << will use the last entry of the currently displayed table as a basis for the next lookup. When the end is reached the text "No more entries" is shown in the displayed table. Use the Refresh button to start over.

**VLAN ID** : VLAN ID of the group.

**Group** : Group address of the group displayed.

**Port** : Switch port number.

**Mode** : Indicates the filtering mode maintained per (VLAN ID, port number, Group Address) basis. It can be either Include or Exclude.

**Source Address** : IP Address of the source. Currently, system limits the total number of IP source addresses for filtering to be 128.

**Type** : Indicates the Type. It can be either Allow or Deny.

**Hardware Filter/Switch** : Indicates whether data plane destined to the specific group address from the source IPv6 address could be handled by chip or not.

Auto-refresh  ↻ << >

## Buttons

**Auto-refresh:** Check this box to refresh the page automatically every 3 seconds.

**Refresh:** Click to refresh the page immediately (manually).

**<<:** Updates the system log entries to the first available entry ID.

**> :** Updates the system log entry to the next available entry ID.

## 3-11 LLDP

### 3-11.1 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.

#### **Web Interface**

To show LLDP neighbors:

1. Click Monitor, LLDP, Neighbors.
2. Click Refresh for manual update web screen
3. Click Auto-refresh for auto-update web screen

**Figure 3-11.1: LLDP Neighbor Information page**

The screenshot shows the web interface for the SM24DPB switch. The left sidebar has a 'Monitor' section expanded, showing 'System', 'Ports', and 'DHCP'. The main content area is titled 'LLDP Neighbor Information' and includes an 'Auto-refresh' checkbox and a refresh icon. Below this is a table titled 'LLDP Remote Device Summary' with the following columns: Local Port, Chassis ID, Port ID, Port Description, System Name, System Capabilities, System Description, and Management Address. The table currently displays the text 'No neighbor information found'.



**NOTE:** If your network has no devices that support LLDP then the table will show "No LLDP neighbor information found".

#### **Parameter descriptions:**

**Local Port :** The port on which the LLDP frame was received.

**Chassis ID :** The Chassis ID is the identification of the neighbor's LLDP frames.

**Port ID :** The Remote Port ID is the identification of the neighbor port.

**Port Description :** Port Description is the port description advertised by the neighbor unit.

**System Name :** System Name is the name advertised by the neighbor unit.

**System Capabilities :** System Capabilities describes the neighbor unit's capabilities. The possible capabilities are:

- Other
- Repeater
- Bridge
- WLAN Access Point
- Router
- Telephone
- DOCSIS cable device
- Station only
- Reserved

When a capability is enabled, the capability is followed by (+). If the capability is disabled, the capability is followed by (-).

**Management Address :** Management Address is the neighbor unit's address that is used for higher layer entities to assist discovery by the network management. This could for instance hold the neighbor's IP address.

### Buttons

**Auto-refresh:** Check this box to refresh the page automatically every 3 seconds.

**Refresh:** Click to refresh the page immediately.

### 3-11.2 LLDP-MED Neighbors

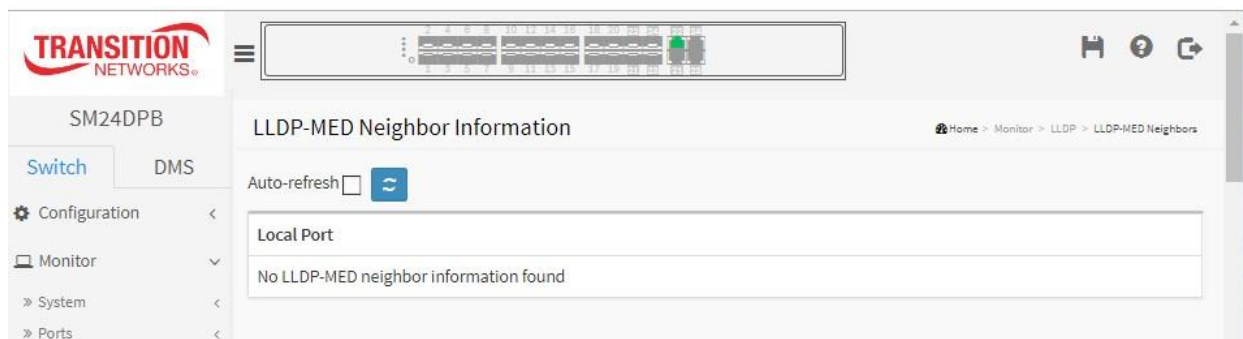
This page provides a status overview of all LLDP-MED neighbors. The displayed table contains a row for each port on which an LLDP neighbor is detected. This function applies to VoIP devices which support LLDP-MED.

#### Web Interface

To show LLDP-MED neighbor:

1. Click Monitor, LLDP, LLDP-MED Neighbor.
2. Click Refresh for manual update web screen
3. Click Auto-refresh for auto-update web screen

**Figure 3-11.2: LLDP-MED Neighbor Information page**



**NOTE:** If your network has no devices that support LLDP-MED then the table will show "No LLDP-MED neighbor information found".

#### Parameter descriptions:

**Port :** The port on which the LLDP frame was received.

**Device Type :** LLDP-MED Devices are comprised of two primary Device Types: Network Connectivity Devices and Endpoint Devices.

#### LLDP-MED Network Connectivity Device Definition

LLDP-MED Network Connectivity Devices, as defined in TIA-1057, provide access to the IEEE 802 based LAN infrastructure for LLDP-MED Endpoint Devices. An LLDP-MED Network Connectivity Device is a LAN access device based on any of these technologies:

- LAN Switch/Router
- IEEE 802.1 Bridge
- IEEE 802.3 Repeater (included for historical reasons)
- IEEE 802.11 Wireless Access Point

Any device that supports the IEEE 802.1AB and MED extensions defined by TIA-1057 and can relay IEEE 802 frames via any method.

**LLDP-MED Endpoint Device Definition :** LLDP-MED Endpoint Devices, as defined in TIA-1057, are located at the IEEE 802 LAN network edge, and participate in IP communication service using the LLDP-MED framework.

Within the LLDP-MED Endpoint Device category, the LLDP-MED scheme is broken into further Endpoint Device Classes, as defined in the following.

Each LLDP-MED Endpoint Device Class is defined to build upon the capabilities defined for the previous Endpoint Device Class. For-example will any LLDP-MED Endpoint Device claiming compliance as a Media Endpoint (Class II) also support all aspects of TIA-1057 applicable to Generic Endpoints (Class I), and any LLDP-MED Endpoint Device claiming compliance as a Communication Device (Class III) will also support all aspects of TIA-1057



applicable to both Media Endpoints (Class II) and Generic Endpoints (Class I).

**LLDP-MED Generic Endpoint (Class I) :** The LLDP-MED Generic Endpoint (Class I) definition is applicable to all endpoint products that require the base LLDP discovery services defined in TIA-1057, however do not support IP media or act as an end-user communication appliance. Such devices may include (but are not limited to) IP Communication Controllers, other communication related servers, or any device requiring basic services as defined in TIA-1057. Discovery services defined in this class include LAN configuration, device location, network policy, power management, and inventory management.

**LLDP-MED Media Endpoint (Class II) :** The LLDP-MED Media Endpoint (Class II) definition is applicable to all endpoint products that have IP media capabilities however may or may not be associated with a particular end user. Capabilities include all of the capabilities defined for the previous Generic Endpoint Class (Class I), and are extended to include aspects related to media streaming. Example product categories expected to adhere to this class include (but are not limited to) Voice / Media Gateways, Conference Bridges, Media Servers, and similar. Discovery services defined in this class include media-type-specific network layer policy discovery.

**LLDP-MED Communication Endpoint (Class III) :** The LLDP-MED Communication Endpoint (Class III) definition is applicable to all endpoint products that act as end user communication appliances supporting IP media. Capabilities include all of the capabilities defined for the previous Generic Endpoint (Class I) and Media Endpoint (Class II) classes, and are extended to include aspects related to end user devices. Example product categories expected to adhere to this class include (but are not limited to) end user communication appliances, such as IP Phones, PC-based softphones, or other communication appliances that directly support the end user. Discovery services defined in this class include provision of location identifier (including ECS / E911 information), embedded L2 switch support, inventory management.

**LLDP-MED Capabilities :** LLDP-MED Capabilities describes the neighborhood unit's LLDP-MED capabilities. The possible capabilities are:

- Network Policy
- Location Identification
- Extended Power via MDI - PSE
- Extended Power via MDI - PD
- Inventory
- Reserved

**Application Type :** Indicates the primary function of the application(s) defined for this network policy, advertised by an Endpoint or Network Connectivity Device. The possible application types are shown below.

**Voice** - for use by dedicated IP Telephony handsets and other similar appliances supporting interactive voice services. These devices are typically deployed on a separate VLAN for ease of deployment and enhanced security by isolation from data applications.

**Voice Signalling** - for use in network topologies that require a different policy for the voice signalling than for the voice media.

**Guest Voice** - to support a separate limited feature-set voice service for guest users and visitors with their own IP Telephony handsets and other similar appliances supporting interactive voice services.

**Guest Voice Signalling** - for use in network topologies that require a different policy for the guest voice signalling than for the guest voice media.

**Softphone Voice** - for use by softphone applications on typical data centric devices, such as PCs or laptops.

**Video Conferencing** - for use by dedicated Video Conferencing equipment and other similar appliances supporting real-time interactive video/audio services.

**Streaming Video** - for use by broadcast or multicast based video content distribution and other similar applications supporting streaming video services that require specific network policy treatment. Video applications relying on TCP with buffering would not be an intended use of this application type.

**Video Signalling** - for use in network topologies that require a separate policy for the video signalling than for the video media.

**Policy :** Policy indicates that an Endpoint Device wants to explicitly advertise that the policy is required by the device. Can be either **Defined** or **Unknown**:

**Unknown:** The network policy for the specified application type is currently unknown.

**Defined:** The network policy is defined.

**TAG :** TAG is indicative of whether the specified application type is using a tagged or an untagged VLAN. Can be Tagged or Untagged. **Untagged:** The device is using an untagged frame format and as such does not include a tag header as defined by IEEE 802.1Q-2003. **Tagged:** The device is using the IEEE 802.1Q tagged frame format.

**VLAN ID :** VLAN ID is the VLAN identifier (VID) for the port as defined in IEEE 802.1Q-2003. A value of 1 through 4094 is used to define a valid VLAN ID. A value of 0 (Priority Tagged) is used if the device is using priority tagged frames as defined by IEEE 802.1Q-2003, meaning that only the IEEE 802.1D priority level is significant and the default PVID of the ingress port is used instead.

**Priority :** Priority is the Layer 2 priority to be used for the specified application type. One of the eight priority levels (0 through 7).

**DSCP :** DSCP is the DSCP value to be used to provide Diffserv node behavior for the specified application type as defined in IETF RFC 2474. Contain one of 64 code point values (0 through 63).

**Auto-negotiation - Auto-negotiation** identifies if MAC/PHY auto-negotiation is supported by the link partner.

**Auto-negotiation status** - identifies if auto-negotiation is currently enabled at the link partner. If **Auto-negotiation** is supported and **Auto-negotiation status** is disabled, the 802.3 PMD operating mode will be determined the operational MAU type field value rather than by auto-negotiation.

**Auto-negotiation Capabilities** - shows the link partners MAC/PHY capabilities.

## Buttons

**Auto-refresh:** Check this box to refresh the page automatically every 3 seconds.

**Refresh:** Click to refresh the page immediately.

### 3-11.3 Port Statistics

Two types of counters are shown. *Global* counters are counters that refer to the whole switch, while *Local* counters refer to the per port counters for the switch.

#### Web Interface

To show LLDP Statistics:

1. Click Monitor, LLDP, Port Statistics to show LLDP counters.
2. Click Refresh for manual update web screen.
3. Click Auto-refresh for auto-update web screen.
4. Click Clear to clear all counters.

**Figure 3-11.3: LLDP Counters page**

LLDP Global Counters	
Neighbor entries were last changed	2011-01-01T00:00:00+00:00 (9433 secs. ago)
Total Neighbors Entries Added	0
Total Neighbors Entries Deleted	0
Total Neighbors Entries Dropped	0
Total Neighbors Entries Aged Out	0

LLDP Statistics Local Counters								
Local Port	Tx Frames	Rx Frames	Rx Errors	Frames Discarded	TLVs Discarded	TLVs Unrecognized	Org. Discarded	Age-Outs
1	0	0	0	0	0	0	0	0
2	0	0	0	0	0	0	0	0
3	0	0	0	0	0	0	0	0
4	0	0	0	0	0	0	0	0
21	0	0	0	0	0	0	0	0
22	129	0	0	0	0	0	0	0
23	0	0	0	0	0	0	0	0
24	0	0	0	0	0	0	0	0

#### Parameter descriptions:

##### Global Counters

**Neighbor entries were last changed at :** 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 table contains a row for each port. The columns hold the following information:

**Local Port** : The port on which LLDP frames are received or transmitted.

**Tx Frames** : The number of LLDP frames transmitted on the port.

**Rx Frames** : The number of LLDP frames received on the port.

**Rx Errors** : The number of received LLDP frames containing some kind of error.

**Frames Discarded** : If an LLDP frame is received on a port, and the switch's internal table has run full, the LLDP frame is counted and discarded. This situation is known as "Too Many Neighbors" in the LLDP standard. LLDP frames require a new entry in the table when the Chassis ID or Remote Port ID is not already contained within the table. Entries are removed from the table when a given port's link is down, an LLDP shutdown frame is received, or when the entry ages out.

**TLVs Discarded** : Each LLDP frame can contain multiple pieces of information, known as TLVs (TLV is short for "Type Length Value"). If a TLV is malformed, it is counted and discarded.

**TLVs Unrecognized** : The number of well-formed TLVs, but with an unknown type value.

**Org. Discarded** : The number of organizationally received TLVs.

**Age-Outs** : Each LLDP frame contains information about how long time the LLDP information is valid (age-out time). If no new LLDP frame is received within the age out time, the LLDP information is removed, and the Age-Out counter is incremented.



## Buttons

**Auto-refresh:** Check this box to refresh the page automatically every 3 seconds.

**Refresh:** Click to refresh the page immediately.

**Clear:** Clears the counters for the selected port.



## Buttons

**Auto-refresh:** Check this box to refresh the page automatically every 3 seconds.

**Refresh:** Click to refresh the page immediately.

**Clear:** Clears the counters for the selected port.

**<<:** Updates the system log entries to the first available entry ID.

**> :** Updates the system log entry to the next available entry ID.



---

**NOTE:**

00-40-C7-73-01-29 : your switch MAC address (for IPv4)

33-33-1-1-1-1 : Destination MAC (for IPv6 Router Advertisement)  
(reference IPv6 RA.JPG)

33-33-1-1-1-2 : Destination MAC (for IPv6 Router Solicitation) (reference  
IPv6 RS.JPG)

33-33-FF-73-01-29 : Destination MAC (for IPv6 Neighbor Solicitation)  
(reference IPv6 DAD.JPG)

33-33-FF-A8-01-01: your switch MAC address (for IPv6 global IP)

FF-FF-FF-FF-FF-FF: for Broadcast.

---

### 3-13 VLANs

#### 3-13.1 VLAN Membership

This page provides an overview of membership status of VLAN users.

Each page shows up to 99 entries from the VLAN table, default being 20, selected through the "entries per page" input field. When first visited, the web page will show the first 20 entries from the beginning of the VLAN Table. The first displayed will be the one with the lowest VLAN ID found in the VLAN Table.

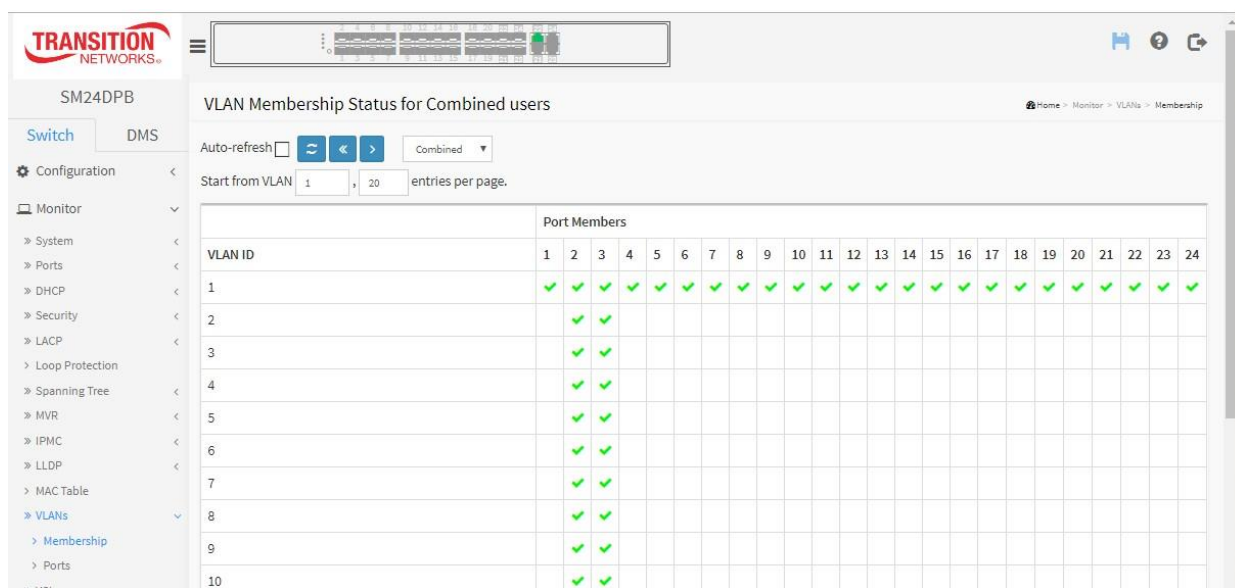
The "VLAN" input fields let you select the starting point in the VLAN Table. Clicking the **“Refresh”** button will update the displayed table starting from that or the closest next VLAN Table match. The **“ > ”** will use the last entry of the currently displayed VLAN entry as a basis for the next lookup. When the end is reached the text "No more entries" is shown in the displayed table. Use the **“ |<< ”** button to start over.

#### Web Interface

To configure VLAN membership configuration in the web interface:

1. Click Monitor, VLANs, VLAN Membership.
2. Select which VLANs to display.
3. Select the set of users to display.
4. Click Refresh to update the state.

**Figure 3-13.1: VLAN Membership Status for Combined users**



#### Parameter descriptions:

#### VLAN USER

VLAN User module uses services of the VLAN management functionality to configure VLAN memberships and VLAN port configurations such as PVID and UVID. Currently we support the following VLAN user types:

**CLI/Web/SNMP** : These are referred to as static.

**NAS** : NAS provides port-based authentication, which involves communications between a Supplicant, Authenticator, and an Authentication Server.

**MVRP** : Multiple VLAN Registration Protocol (MVRP) allows dynamic registration and deregistration of VLANs on ports on a VLAN bridged network.


**Voice VLAN** : Voice VLAN is a VLAN configured specially for voice traffic typically originating from IP phones.

**MVR** : MVR is used to eliminate the need to duplicate multicast traffic for subscribers in each VLAN. Multicast traffic for all channels is sent only on a single (multicast) VLAN.


**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.

**VLAN ID** : VLAN ID for which the Port members are displayed.

**Port Members** : A row of check boxes for each port is displayed for each VLAN ID.

If a port is included in a VLAN, an image  will be displayed.

If a port is included in a Forbidden port list, an image  will be displayed.

If a port is included in a Forbidden port list and dynamic VLAN user register VLAN on same Forbidden port, then conflict port will be displayed as .

**VLAN Membership** : The VLAN Membership Status Page shall show the current VLAN port members for all VLANs configured by a selected VLAN User (selection are allowed by a Combo Box). When ALL VLAN Users are selected, it shall show this information for all the VLAN Users, and this is by default. VLAN membership allows the frames classified to the VLAN ID to be forwarded on the respective VLAN member ports.

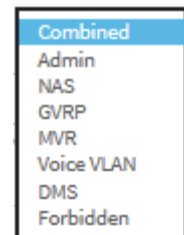
## Buttons



**Auto-refresh:** Check this box to refresh the page automatically every 3 seconds.

**Refresh:** Click to refresh the page immediately (manually).

**User select dropdown** : Select which VLANs to display:





### 3-13.2 VLAN Port Status

The Port Status gathers the information of all VLAN status and reports it in the order of Static, NAS, MVRP, MVP, Voice VLAN, MSTP, GVRP, Combined.

#### Web Interface

To display VLAN Port Status in the web interface:

1. Click Monitor, VLAN Port Status.
2. At the dropdown select the user type to display (Static NAS, MVRP, MVP, Voice VLAN, MSTP, GVRP, or Combined).
3. View the displayed Port Status information for the selected user.

**Figure 3-13.2: VLAN Port Status for Combined users**

Port	Port Type	Ingress Filtering	Frame Type	Port VLAN ID	Tx Tag	Untagged VLAN ID	Conflicts
1	C-Port	<input checked="" type="checkbox"/>	All	1	Untag PVID		No
2	C-Port	<input checked="" type="checkbox"/>	All	1	Untag PVID		No
3	C-Port	<input type="checkbox"/>	All	1	Untag PVID		No
4	C-Port	<input checked="" type="checkbox"/>	All	1	Untag PVID		No
5	C-Port	<input checked="" type="checkbox"/>	All	1	Untag PVID		No
6	C-Port	<input checked="" type="checkbox"/>	All	1	Untag PVID		No
7	C-Port	<input checked="" type="checkbox"/>	All	1	Untag PVID		No
8	C-Port	<input checked="" type="checkbox"/>	All	1	Untag PVID		No
9	C-Port	<input checked="" type="checkbox"/>	All	1	Untag PVID		No
10	C-Port	<input checked="" type="checkbox"/>	All	1	Untag PVID		No
11	C-Port	<input checked="" type="checkbox"/>	All	1	Untag PVID		No

#### Parameter descriptions:

**VLAN USER :** VLAN User module uses services of the VLAN management functionality to configure VLAN memberships and VLAN port configuration such as PVID, UVID. Currently we support following VLAN User types:

**CLI/Web/SNMP :** These are referred to as static.

**NAS :** NAS provides port-based authentication, which involves communications between a Supplicant, Authenticator, and an Authentication Server.

**Voice VLAN :** Voice VLAN is a VLAN configured specially for voice traffic typically originating from IP phones.

**MVR :** MVR is used to eliminate the need to duplicate multicast traffic for subscribers in each VLAN. Multicast traffic for all channels is sent only on a single (multicast) VLAN.

**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.

**Port :** The logical port for the settings contained in the same row.

**Port Type :** Shows the Port Type. Port type can be any of Unaware, C-port, S-port, Custom S-port.

If Port Type is Unaware, all frames are classified to the Port VLAN ID and tags are not removed. C-port is

Customer Port. S-port is Service port. Custom S-port is S-port with Custom TPID.

**Ingress Filtering** : Shows the ingress filtering on a port. This parameter affects VLAN ingress processing. If ingress filtering is enabled and the ingress port is not a member of the classified VLAN, the frame is discarded.

**Frame Type** : Shows whether the port accepts all frames or only tagged frames. This parameter affects VLAN ingress processing. If the port only accepts tagged frames, untagged frames received on that port are discarded.

**Port VLAN ID** : Shows the Port VLAN ID (PVID) that a given user wants the port to have.

The field is empty if not overridden by the selected user.

**Tx Tag** : Shows egress filtering frame status whether tagged or untagged.

**UVID** : Shows UVID (untagged VLAN ID). Port's UVID determines the packet's behavior at the egress side.

**Conflicts** : Shows status of Conflicts whether exists or not. When a Volatile VLAN User requests to set VLAN membership or VLAN port configuration, the following conflicts can occur:

- Functional Conflicts between features.
- Conflicts due to hardware limitation.
- Direct conflict between user modules.

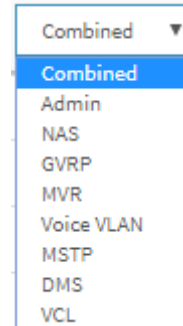
**Buttons**



**Auto-refresh:** Check this box to refresh the page automatically every 3 seconds.

**Refresh:** Click to refresh the page immediately.

**User select dropdown** : Select the user type to display (Combined, Admin, NAS, GVRP, MVR, Voice VLAN, MSTP, DMS, or VCL).



### 3-14 VCL

#### 3-14.1 MAC-based VLAN

This page shows MAC-based VLAN entries configured by various MAC-based VLAN users. Currently we support following VLAN User types:

**CLI/Web/SNMP** : These are referred to as static.

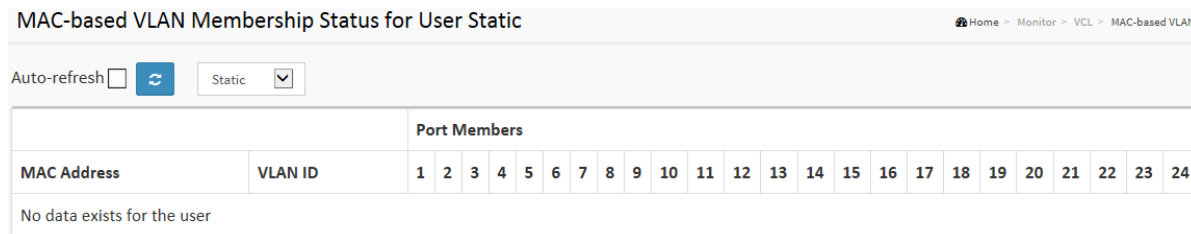
**NAS** : NAS provides port-based authentication, which involves communications between a Supplicant, Authenticator, and an Authentication Server.

#### Web Interface

To display MAC-based VLAN configuration in the web interface:

1. Click Monitor, VCL, MAC-based VLAN.
2. At the user select dropdown specify Static, NAS, DMS, or Combined.
3. Display MAC-based information.

**Figure 3-14.1: MAC-based VLAN Membership Status for User Static**



#### Parameter descriptions:

**MAC Address** : Indicates the MAC address.

**VLAN ID** : Indicates the VLAN ID.

**Port Members** : Port members of the MAC-based VLAN entry.

#### Buttons



**Auto-refresh:** Check this box to refresh the page automatically every 3 seconds.

**Refresh:** Click to refresh the page immediately.

**User select dropdown** : specify Static, NAS, DMS, or Combined.

## 3-14.2 Protocol-based VLAN

### 3-14.2.1 Protocol to Group

This page displays the protocols to Group Name (unique for each Group) mapping entries for the switch.

#### **Web Interface**

To display Protocol-based VLAN configuration in the web interface:

1. Click Monitor, VCL, Protocol to Group.
2. Check “Auto-refresh”.
3. Click “Refresh” to refresh the port detailed statistics.

**Figure 3-14.1: Protocol to Group Mapping Table Status page**

Frame Type	Value	Group Name
	No Group entry found!	

#### **Parameter descriptions:**

**Frame Type :** Frame Type can have one of these values: 1. Ethernet, 2. LLC, or 3. SNAP.



**NOTE:** On changing the Frame type field, valid value of the following text field will vary depending on the new frame type you selected.

**Value :** Valid value that can be entered in this text field depends on the option selected from the preceding Frame Type selection menu. Below are the criteria for three different Frame Types:

**Ethernet:** Values in the text field when Ethernet is selected as a Frame Type is called etype. Valid values for etype range from 0x0600 - 0xffff.

**LLC:** Valid value in this case is comprised of two different sub-values.

a. DSAP: 1-byte long string (0x00-0xff)

b. SSAP: 1-byte long string (0x00-0xff)

**SNAP:** Valid value in this case also is comprised of two different sub-values.

a. OUI: OUI (Organizationally Unique Identifier) is value in format of xx-xx-xx where each pair (xx) in string is a hexadecimal value ranges from 0x00-0xff.

b. PID: If the OUI is hexadecimal 000000, the protocol ID is the Ethernet type (EtherType) field value for the protocol running on top of SNAP; if the OUI is an OUI for a particular organization, the protocol ID is a value assigned by that organization to the protocol running on top of SNAP.

In other words, if value of OUI field is 00-00-00 then value of PID will be etype (0x0600-0xffff) and if value of OUI is other than 00-00-00 then valid value of PID will be any value from 0x0000 to 0xffff.

**Group Name :** A valid Group Name is a unique 16-character long string for every entry which consists of a combination of alphabets (a-z or A-Z) and integers(0-9).



**NOTE:** Special characters and underscore ( \_ ) are not allowed.

### 3-14.2.2 Group to VLAN

This page displays the configured Group Name to a VLAN for the switch .

#### Web Interface

To display Group to VLAN configuration in the web interface:

1. Click Monitor, VCL, Group to VLAN.
2. Check Auto-refresh.
3. Click Refresh to refresh the port detailed statistics.

**Figure 3-14.2: Group Name to VLAN mapping Table Status page**



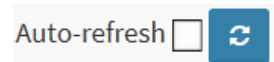
#### Parameter descriptions:

**Group Name :** A valid Group Name is a string at the most 16 characters which consists of a combination of alphabets (a-z or A-Z) and integers(0-9), no special character is allowed. whichever Group name you try map to a VLAN must be present in Protocol to Group mapping table and must not be pre-used by any other existing mapping entry on this page.

**VLAN ID :** Indicates the ID to which Group Name will be mapped. A valid VLAN ID ranges from 1-4095.

**Port Members :** A row of check boxes for each port is displayed for each Group Name to VLAN ID mapping. To include a port in a mapping, check the box. To remove or exclude the port from the mapping, make sure the box is unchecked. By default, no ports are members, and all boxes are unchecked.

#### Buttons



**Auto-refresh:** Check this box to refresh the page automatically every 3 seconds.

every 3

**Refresh:** Click to refresh the page immediately.

### 3-14.3 IP Subnet-based VLAN

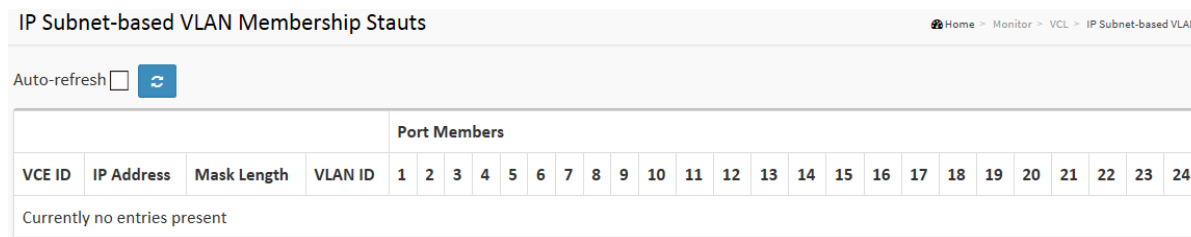
This page displays IP subnet-based VLAN entries. *This page shows only static entries.*

#### Web Interface

To display MAC-based VLAN configuration in the web interface:

1. Click Monitor, VCL, IP Subnet-based VLAN.
2. Check Auto-refresh.
3. Click Refresh to refresh the port detailed statistics.

**Figure 3-18.3: IP Subnet-based VLAN Membership Status page**



#### Parameter descriptions:

**VCE ID :** Indicates the index of the entry. It is user configurable. Its value ranges from 0-128. If a VCE ID is 0, application will auto-generate the VCE ID for that entry. Deletion and lookup of IP subnet-based VLAN are based on VCE ID.

**IP Address :** Indicates the IP address.

**Mask Length :** Indicates the network mask length.

**VLAN ID :** Indicates the VLAN ID. VLAN ID can be changed for the existing entries.

**Port Members :** A row of check boxes for each port is displayed for each IP subnet-based VLAN entry. To include a port in a IP subnet-based VLAN, check the box. To remove or exclude the port from the IP subnet-based VLAN, make sure the box is unchecked. By default, no ports are members, and all boxes are unchecked.



#### Buttons

**Auto-refresh:** Check this box to refresh the page automatically every 3 seconds.

**Refresh:** Click to refresh the page immediately.

### 3-15 sFlow

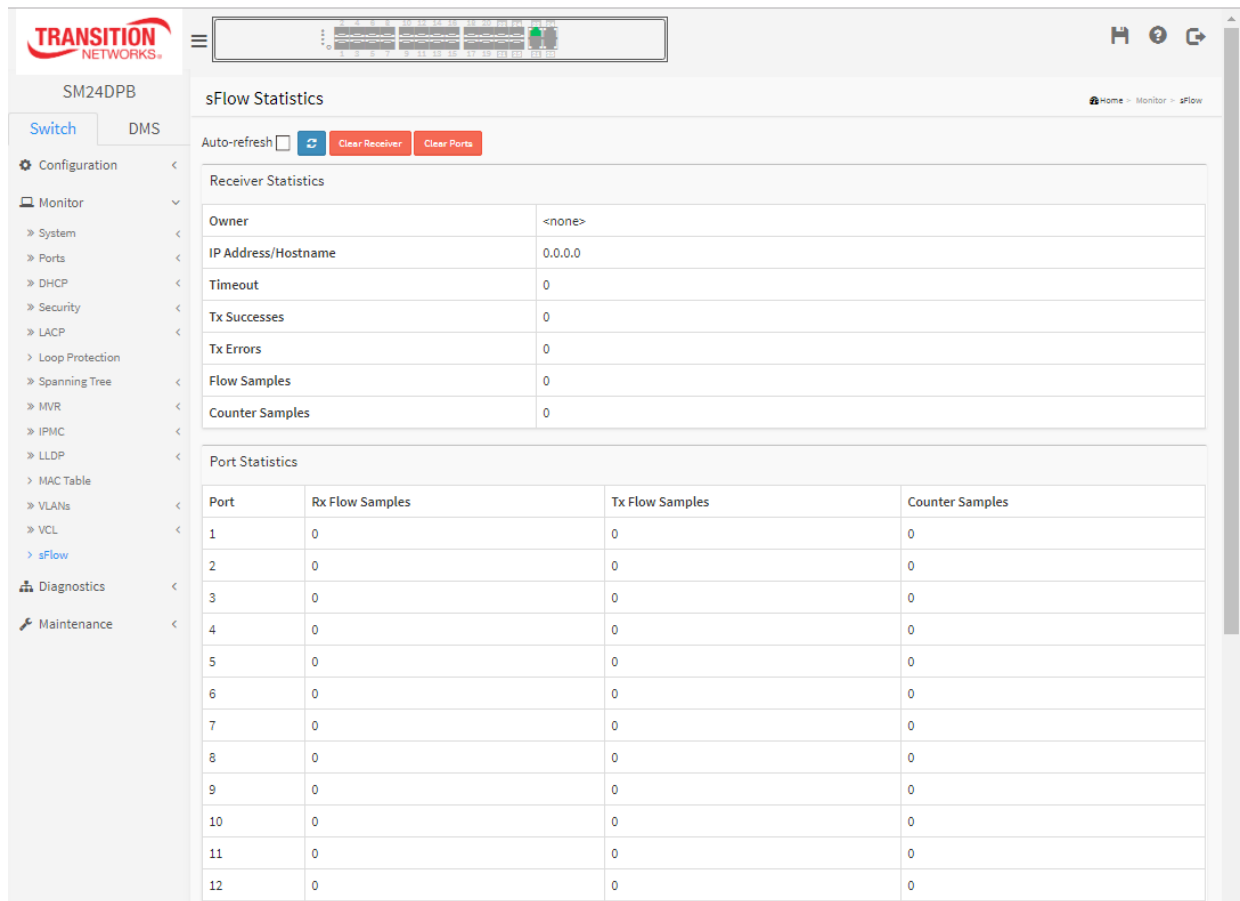
This page displays receiver and per-port sFlow statistics.

#### Web Interface

To display MAC-based VLAN configuration in the web interface:

1. Click Monitor, sFlow
2. View sFlow information.

**Figure 3-15: sFlow Statistics page**



#### Parameter descriptions:

##### Receiver Statistics

**Owner:** This field shows the current owner of the sFlow configuration. It assumes one of three values as follows:

If sFlow is currently unconfigured or unclaimed, Owner contains *<none>*.

If sFlow is currently configured through Web or CLI, Owner contains *<Configured through local management>*.

If sFlow is currently configured through SNMP, Owner contains a string identifying the sFlow receiver.

**IP Address/Hostname:** The IP address or hostname of the sFlow receiver.

**Timeout :** The number of seconds remaining before sampling stops and the current sFlow owner is released.

**Tx Successes** : The number of UDP datagrams successfully sent to the sFlow receiver.

**Tx Errors** : The number of UDP datagrams that has failed transmission. The most common source of errors is invalid sFlow receiver IP/hostname configuration. To diagnose, paste the receiver's IP address/hostname into the Ping Web page (Diagnostics > Ping/Ping6).

**Flow Samples** : The total number of flow samples sent to the sFlow receiver.

**Counter Samples** : The total number of counter samples sent to the sFlow receiver.

### **Port Statistics**

**Port** : The port number for which the following statistics applies.

**Rx and Tx Flow Samples** : The number of flow samples sent to the sFlow receiver originating from this port. Here, flow samples are divided into Rx and Tx flow samples, where Rx flow samples contains the number of packets that were sampled upon reception (ingress) on the port and Tx flow samples contains the number of packets that were sampled upon transmission (egress) on the port.

**Counter Samples** : The total number of counter samples sent to the sFlow receiver originating from this port.



### **Buttons**

**Auto-refresh:** Check this box to refresh the page automatically every 3 seconds.

**Refresh:** Click to refresh the page immediately.

**Clear Receiver:** Clears the sFlow receiver counters.

**Clear Ports:** Clears the per-port counters.



## Chapter 4. Diagnostics

This chapter provides a set of basic system diagnosis. The basic system check includes ICMP Ping, Link OAM, ICMPv6, and Cable Diagnostics.

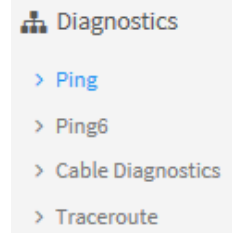
### 4-1 Ping

This page lets you issue ICMP Ping packets to troubleshoot IPv6 connectivity issues.

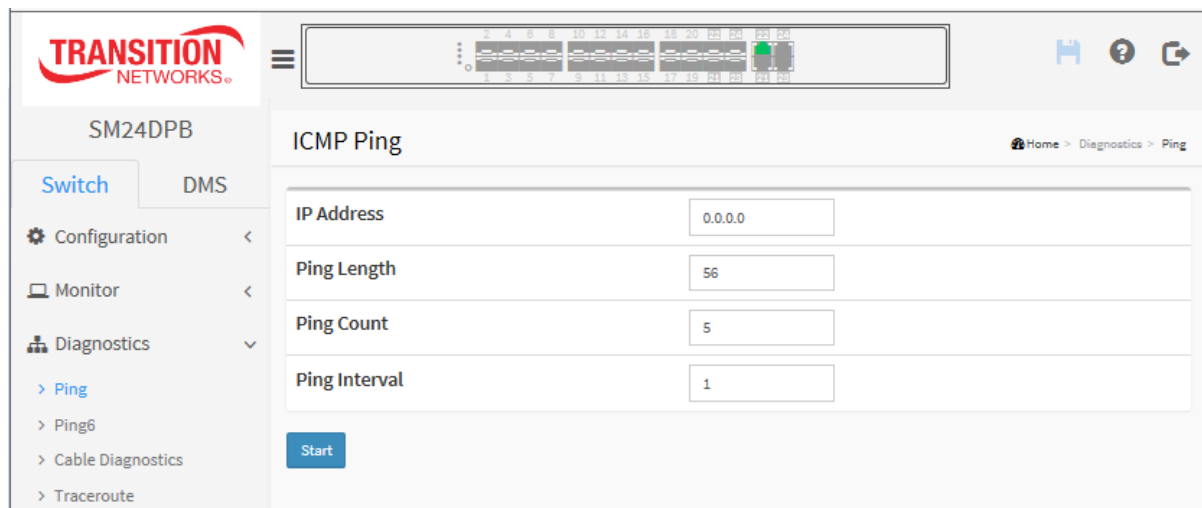
#### Web Interface

To configure an ICMP PING Configuration in the web interface:

1. Specify ICMP Ping IP Address.
2. Specify ICMP Ping Length, Count, and Interval.
3. Click Start.



**Figure 4-1: ICMP Ping page**



#### Parameter descriptions:

**IP Address :** To set the IP Address of device what you want to ping it.

**Ping Length:** The payload size of the ICMP packet. Values range from 2 bytes to 1452 bytes.

**Ping Count:** The count of the ICMP packet. Values range from 1 time to 60 times.

**Ping Interval:** The interval of the ICMP packet. Values range from 0 second to 30 seconds.

**Egress Interface (Only for IPv6):** The VLAN ID (VID) of the specific egress IPv6 interface which ICMP packet goes. The given VID ranges from 1 to 4094 and will be effective only when the corresponding IPv6 interface is valid. When the egress interface is not given, PING6 finds the best match interface for destination.

Do not specify egress interface for loopback address.

Do specify egress interface for link-local or multicast address.

#### Buttons:

**Start:** Click the **Start** button then the switch will start to ping the device using ICMP packet size what set on the switch.

After you press **Start**, 5 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.

**Sample Ping:**

```
PING6 server ::10.10.132.20
64 bytes from ::10.10.132.20: icmp_seq=0, time=0ms
64 bytes from ::10.10.132.20: icmp_seq=1, time=0ms
64 bytes from ::10.10.132.20: icmp_seq=2, time=0ms
64 bytes from ::10.10.132.20: icmp_seq=3, time=0ms
64 bytes from ::10.10.132.20: icmp_seq=4, time=0ms
Sent 5 packets, received 5 OK, 0 bad
```

**New Ping** : Click to re-start Ping diagnostic.

## 4-2 Ping6

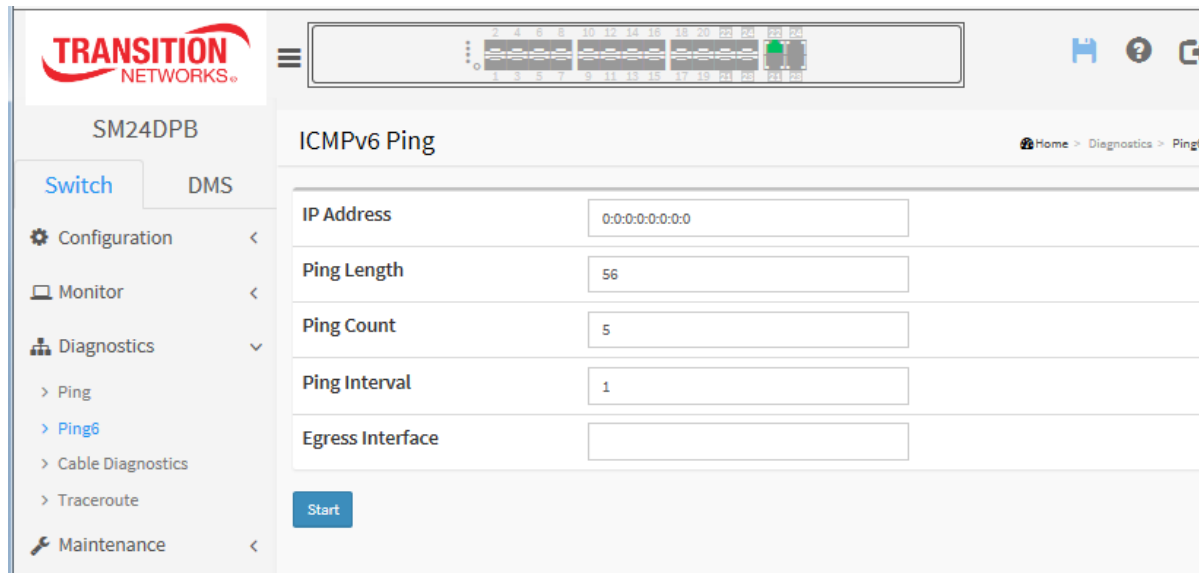
This page lets you issue ICMPv6 Ping packets to troubleshoot IPv6 connectivity issues.

### Web Interface

To configure an ICMPv6 PING Configuration in the web interface:

1. Specify ICMPv6 Ping IP Address.
2. Specify ICMPv6 Ping Length, Count and Interval, and Egress Interface.
3. Click Start.

**Figure 4-2: ICMPv6 Ping page**



### Parameter descriptions:

**IP Address** : The destination IP Address with IPv6.

**Ping Length** : The payload size of the ICMP packet. Values range from 2 bytes to 1452 bytes.

**Ping Count** : The count of the ICMP packet. Values range from 1 time to 60 times.

**Ping Interval** : The interval of the ICMP packet. Values range from 0 second to 30 seconds.

**Egress Interface** : The VLAN ID (VID) of the specific egress IPv6 interface which ICMP packet goes. The valid VID range is 1 - 4094 and will be effective only when the corresponding IPv6 interface is valid. When the egress interface is not given, PING6 finds the best match interface for destination. Do not specify egress interface for loopback address. Do specify egress interface for link-local or multicast address.

### Buttons:

**Start**: Click the **Start** button then the switch will start to ping the device using ICMPv6 packet size what set on the switch. After you press **Start**, 5 ICMPv6 packets are transmitted, and the sequence number and roundtrip time are displayed upon reception of a reply. The page refreshes automatically until responses to all packets are received, or until a timeout occurs.

**New Ping** : Click to re-start diagnostics with Ping.

**Sample Ping6:**

```
PING server 10.10.132.20
64 bytes from 10.10.132.20: icmp_seq=0, time=0ms
64 bytes from 10.10.132.20: icmp_seq=1, time=0ms
64 bytes from 10.10.132.20: icmp_seq=2, time=0ms
64 bytes from 10.10.132.20: icmp_seq=3, time=0ms
64 bytes from 10.10.132.20: icmp_seq=4, time=0ms
Sent 5 packets, received 5 OK, 0 bad
```

### 4-3 Cable Diagnostics

This page lets you run the Cable Diagnostics for 10/100 and 1G 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 Cable Diagnostics are only accurate for cables of length 7 -140 meters. 10 and 100 Mbps ports will be linked down while running Cable Diagnostics. Therefore, running Cable Diagnostics on a 10 or 100 Mbps management port will cause the switch to stop responding until Cable Diagnostics is complete.

#### Web Interface

To configure Cable Diagnostics in the web interface:

1. Specify the Port which you want to check.
2. Click Start.

**Figure 4-3: Cable Diagnostics page**

Copper Port	Link Status	Test Result	Length
21	Link Down	Abnormal	2(m)
22	1G	detect error or check cable length is between 7-120 meters	
23	Link Down	Abnormal	3(m)
24	Link Down	Abnormal	3(m)

#### Parameter descriptions:

**Port** : Dropdown to select the port for which you are requesting Cable Diagnostics.

**Copper Port** : Copper port number.

**Link Status** : The status of the cable:

**10M** : Cable is link up and correct. Speed is 10Mbps

**100M** : Cable is link up and correct. Speed is 100Mbps

**1G** : Cable is link up and correct. Speed is 1Gbps

**Link Down**: Link down or cable is not correct.

**Test Result** : Test Result of the cable:

**OK**: Correctly terminated pair

**Abnormal**: Incorrectly terminated pair or link down

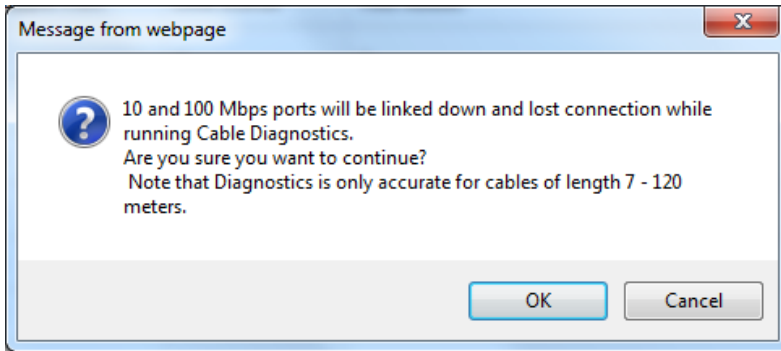
**Length** : The length (in meters) of the cable pair. The resolution is 3 meters. When Link Status is shown as follows, the length has different definitions:

**1G**: The length is the minimum value of 4-pair.

**10M/100M**: The length is the minimum value of 2-pair.

**Link Down**: The length is the minimum value of non-zero of 4-pair.

**Messages:**



**Sample Cable Diagnostics:**

TRANSITION NETWORKS

SM24DPB

Switch DMS

Configuration Monitor Diagnostics Ping Ping6 Cable Diagnostics Traceroute

Cable Diagnostics

Port: 21 Start

Copper Port	Link Status	Test Result	Length
21	Link Down	detect error or check cable length is between 7-120 meters	
22	--	--	--
23	--	--	--
24	--	--	--

### 4-4 Traceroute

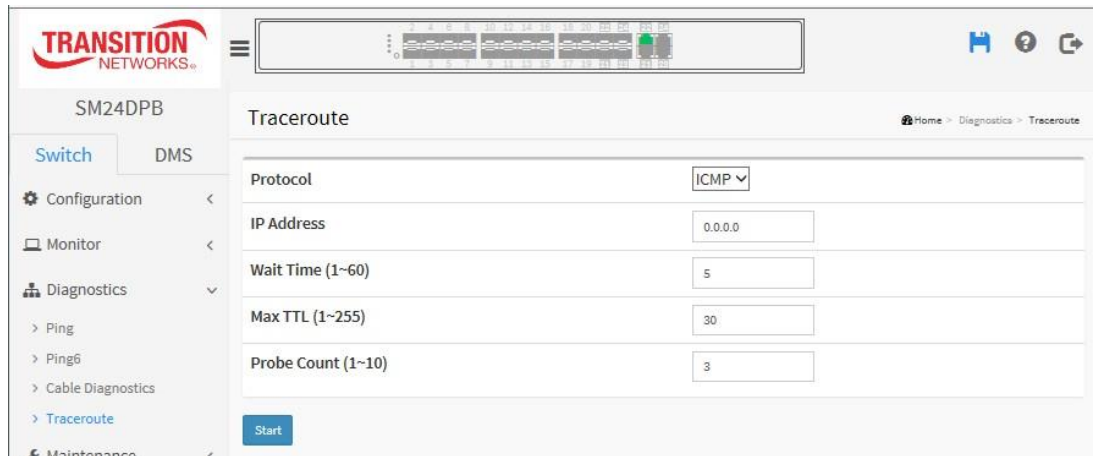
This page lets you issue ICMP, TCP, or UDP packets to diagnose network connectivity issues.

#### Web Interface

To configure Traceroute in the web interface:

1. Specify traceroute Protocol and IP Address.
2. Specify traceroute Wait Time, Max TTL, and Probe Count.
3. Click Start.

**Figure 4-4: Traceroute page**



#### Parameter descriptions:

**Protocol :** The protocol(ICMP, UDP, TCP) packets to send.

**IP Address :** The destination IP Address.

**Wait Time (1-60):** Set the time (in seconds) to wait for a response to a probe (default 5.0 sec). Values range from 1 to 60. The payload size of the ICMP packet. Values range from 2 bytes to 1452 bytes.

**Max TTL 1-255):** Specifies the maximum number of hops (max time-to-live value) traceroute will probe. Values range from 1 to 255. The default is 30.

**Probe Count (1-10):** Sets the number of probe packets per hop. Values range from 1 to 10. The default is 3.

#### Buttons

**Start :** Click to start a Traceroute.

After you press **Start**, Traceroute sends packets with gradually increasing TTL value, starting with TTL value of 1. The first router receives the packet, decrements the TTL value and drops the packet because it then has TTL value zero. The router sends an ICMP Time Exceeded message back to the source. The next set of packets are given a TTL value of 2, so the first router forwards the packets, but the second router drops them and replies with ICMP Time Exceeded. Proceeding in this way, traceroute uses the returned ICMP Time Exceeded messages to build a list of routers that packets traverse, until the destination is reached and returns an ICMP Echo Reply message. For example:

```
traceroute to 202.39.253.11 (202.39.253.11), 30 hops max, 40 byte packets
 1 192.168.10.254 ae-2-3508.edge4.Atlanta2.Level3.net. (192.168.10.254) 10 ms 10 ms 10 ms
 2 59-125-13-254.HINET-IP.hinet.net. (59.125.13.254) 20 ms 20 ms 20 ms
 3 h146.s228.ts.hinet.net. (168.95.228.146) 20 ms 10 ms 20 ms
 4 tchn-3011.hinet.net. (220.128.16.194) 20 ms TCHN-3112.hinet.net. (220.128.17.142) 20 ms tchn-3011.hinet.net. (220.128.16.202) 20 ms
 5 TPDT-3012.hinet.net. (220.128.17.6) 20 ms TPDT-3011.hinet.net. (220.128.16.10) 20 ms TPDT-3012.hinet.net. (220.128.17.6) 40 ms
 6 CHCH-3112.hinet.net. (220.128.2.13) 20 ms tchn-3011.hinet.net. (220.128.1.9) 10 ms CHCH-3112.hinet.net. (220.128.2.13) 30 ms
 7 211.22.41.237 CHCH-3112.hinet.net. (211.22.41.237) 20 ms 30 ms 30 ms
```

8 202-39-253-11.HINET-IP.hinet.net. (202.39.253.11) 10 ms 10 ms

**New Traceroute** : Click to re-start a new Traceroute.

**Sample Traceroute Output:**

The screenshot displays the web interface for a Transition Networks device (SM24DPB). The left sidebar contains navigation options: Configuration, Monitor, Diagnostics (with sub-items: Ping, Ping6, Cable Diagnostics, Traceroute), and Maintenance. The main content area is titled 'Traceroute Output' and shows the results of a traceroute to 192.168.1.77. The output consists of 10 hops, each marked with three asterisks (\*\*\*) to indicate successful completion. A 'New Traceroute' button is located at the bottom of the output area.

```
tracert to 192.168.1.77 (192.168.1.77), 30 hops max, 0 byte packets
 1 ***
 2 ***
 3 ***
 4 ***
 5 ***
 6 ***
 7 ***
 8 ***
 9 ***
10 **
```



## Chapter 5. Maintenance

This chapter describes switch Maintenance configuration tasks to enhance the performance of local network. These tasks include Restart Device, Reboot Schedule, Factory Defaults, Firmware Upgrade / Selection, Configuration Save / Download / Upload / Activate / Delete, and Server Report.

### 5-1 Restart Device

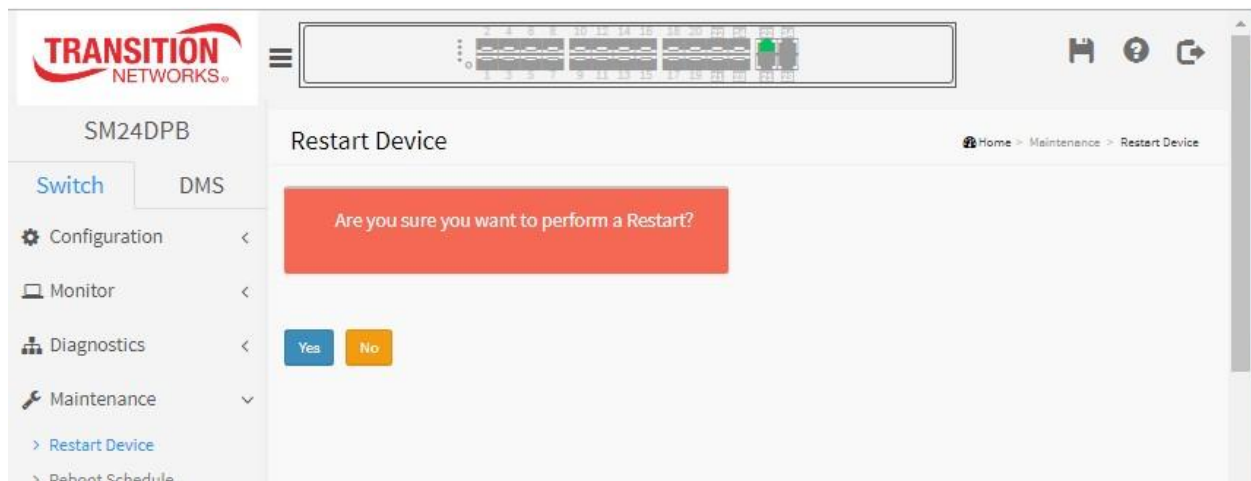
This page lets you restart the switch for maintenance needs. Any configuration files or scripts that you saved in the switch will still be available afterwards. You can restart the switch on this page. After restart, the switch will boot normally.

#### Web Interface

To configure a Restart Device in the web interface:

1. At Maintenance > Restart Device click Yes.

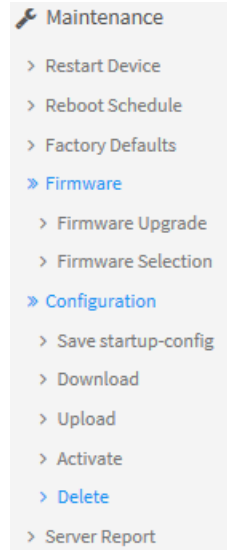
**Figure 5-1: Restart Device page**



#### Buttons:

**Yes** – Click to restart the device.

**No** – Click to undo any restart action.



## 5-2 Reboot Schedule

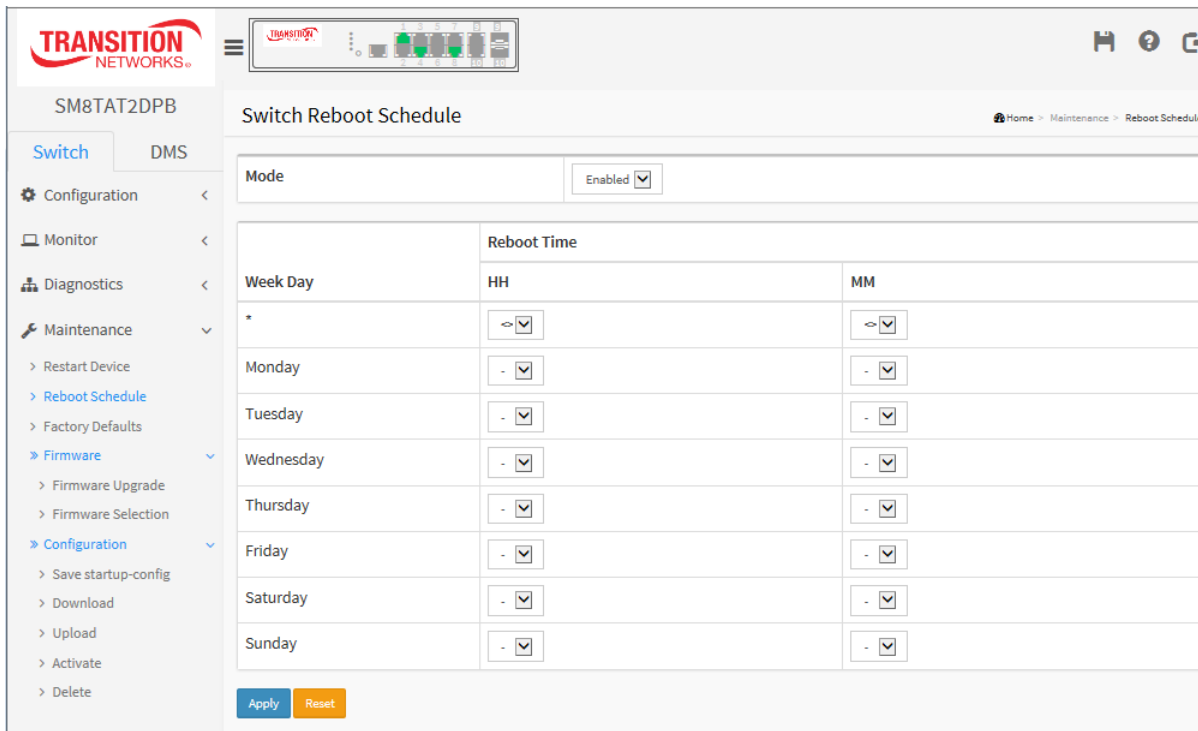
This page lets you schedule the day and time to reboot the switch.

### Web Interface

To configure a Restart Device Configuration in the web interface:

1. Click Maintenance, Reboot Schedule.
2. At the Mode dropdown select Enabled to display the configurable Switch Reboot Schedule page parameters.
3. Select the Reboot Time(s) and Day(s).
4. Click Apply.

**Figure 5-2: Reboot Schedule page**



**Mode** : Indicates the reboot scheduling mode operation. Possible modes are:

**Enabled**: Enable switch reboot scheduling.

**Disabled**: Disable switch reboot scheduling.

**Week Day** : The day to reboot this switch.

**Reboot Time** : The time to reboot the switch.

### Buttons

**Apply** : Click to save changes.

**Reset** : Click to undo any changes made locally and revert to previously saved values.

### 5-3 Factory Defaults

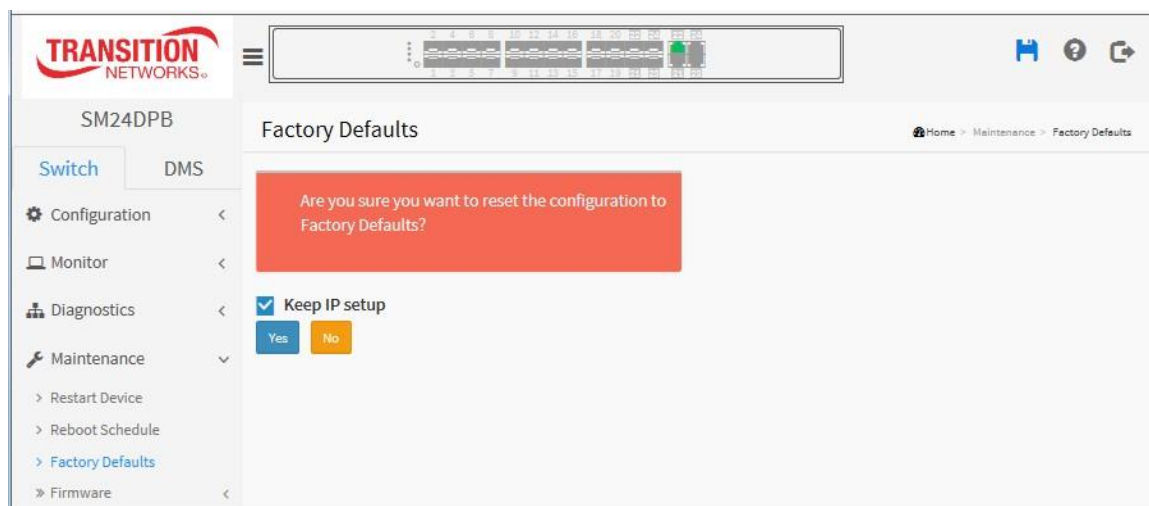
This page lets you reset the Switch configuration to Factory Defaults. Any configuration files or scripts will reset to factory default values. The new configuration is available immediately, which means that no restart is necessary.

#### Web Interface

To configure a reset to Factory Defaults in the web interface:

1. Click Maintenance, Factory Defaults.
2. Check or uncheck Keep IP setup.
3. At the “Are you sure...” prompt click Yes.

**Figure 5-3.1: Factory Defaults page**



#### Buttons:

**Keep IP setup** : Check "Keep IP setup" if you want to keep current IP setting.

**Yes** – Click to “Yes” button to reset the configuration to Factory Defaults.

**No**- Click to return to the Port State page without resetting the configuration.

**Note:** Restoring factory default can also be performed by making a physical loopback between port 1 and port 2 within the first minute from switch reboot. In the first minute after boot, 'loopback' packets will be transmitted at port 1. If a 'loopback' packet is received at port 2 the switch will do a restore to default.

## 5-4 Firmware

This section describes how to upgrade switch firmware. The switch can be enhanced with more value-added functions by installing firmware upgrades.

### 5-3.1 Firmware upgrade

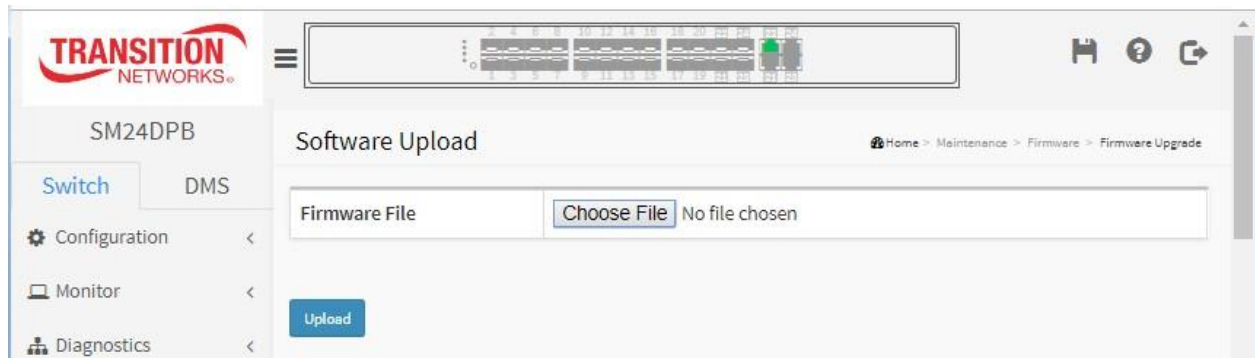
This page facilitates an update of the firmware controlling the switch.

#### **Web Interface**

To configure a Firmware Upgrade Configuration in the web interface:

1. Click Maintenance, Firmware, Firmware Upgrade.
2. Click Browse to select a firmware file to upgrade this switch.
3. Click Upload.

**Figure 5-3.1 Software Upload page**



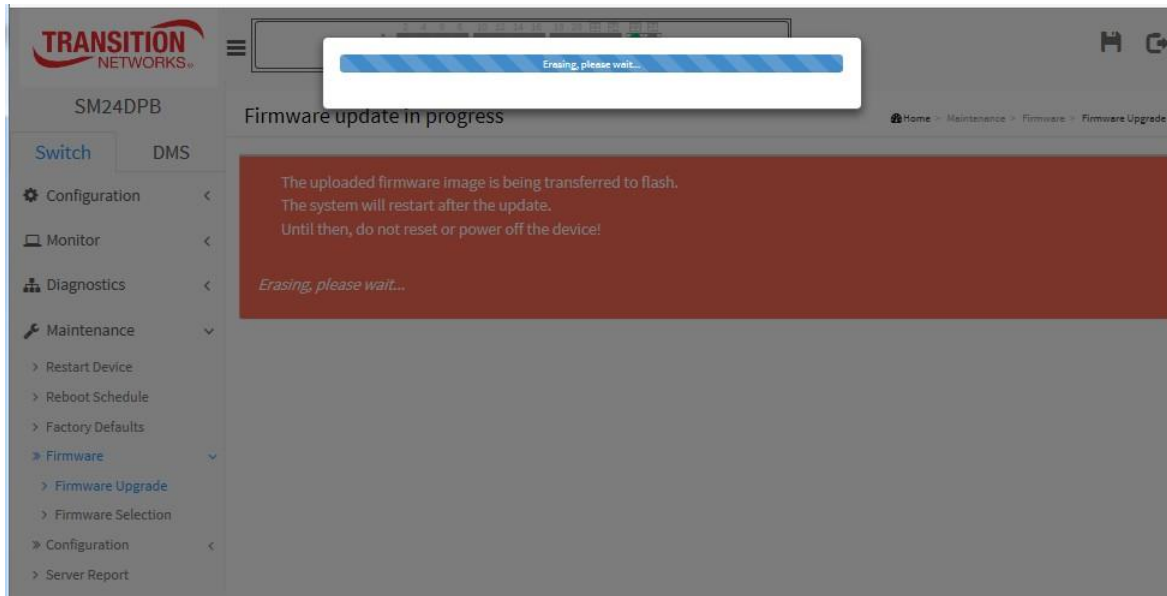
#### **Parameter descriptions:**

**Choose File :** Click the button to search the Firmware URL and filename (e.g., *SM24DPB\_v6.54.3187\_201601073*). Click the Upload button. After the software image is uploaded, a page announces that the firmware update is initiated. After about a minute, the firmware is updated and the switch restarts.



**Warning:** While the firmware is being updated, Web access appears to be defunct. The front LED flashes Green/Off with a frequency of 10 Hz while the firmware update is in progress. Do not restart or power off the device at this time or the switch may fail to function afterwards.

**During** the upgrade process a screen like the one below displays:



**After** the upgrade process the Login screen displays to let you log back in.

### 5-3.2 Firmware Selection

This page provides information about the active and alternate (backup) firmware images in the device and allows you to revert to the alternate image. The web page displays two tables with information about the active and alternate firmware images.

**Note:**

1. If the active firmware image is the alternate image, only the "Active Image" table is shown. In this case, the Activate Alternate Image button is also disabled.
2. If the alternate image is active (due to a corruption of the primary image or manually intervention), uploading a new firmware image to the device will automatically use the primary image slot and activate this.
3. The firmware version and date information may be empty for older firmware releases. This does not constitute an error.

**Web Interface**

To configure a Firmware Upgrade Configuration in the web interface:

1. Verify the active and alternate (backup) firmware information displayed.
2. Click Activate Alternate Image.

**Figure 5-3.2 Firmware Selection page**

The screenshot shows the 'Software Image Selection' page in the SM24DPB web interface. The page is divided into a left sidebar with navigation options (Switch, DMS, Configuration, Monitor, Diagnostics, Maintenance, Firmware, etc.) and a main content area. The main content area displays two tables: 'Active Image' and 'Alternate Image'. The 'Active Image' table has the following data:

Active Image	
Image	managed
Version	SM24DPB (standalone) v6.54.3359
Date	2019-12-27T22:44:14+08:00

The 'Alternate Image' table has the following data:

Alternate Image	
Image	managed.bk
Version	SM24DPB (standalone) v6.54.3202
Date	2019-07-12T05:50:42+08:00

Below the tables, there are two buttons: 'Activate Alternate Image' (blue) and 'Cancel' (red).

**Image Information**

**Image :** The flash index name of the firmware image. The name of primary (preferred) image is *managed*, and the alternate image is named *manage.bk*.

**Version :** The version of the firmware image.

**Date :** The date when the firmware was produced.

## Buttons

**Activate Alternate Image:** Click to use the “Alternate Image”. This button may be disabled depending on system state.

**Cancel:** Cancel activating the backup image and navigate away from this page.

## 5-4 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.
- **startup-config:** The startup configuration for the switch, read at boot time.
- **default-config:** A read-only file with vendor-specific configuration. This file is read when the system is restored to default settings.

It is also possible to store up to two other files and apply them to running-config, thereby switching configuration.

### 5-4.1 Save startup-config

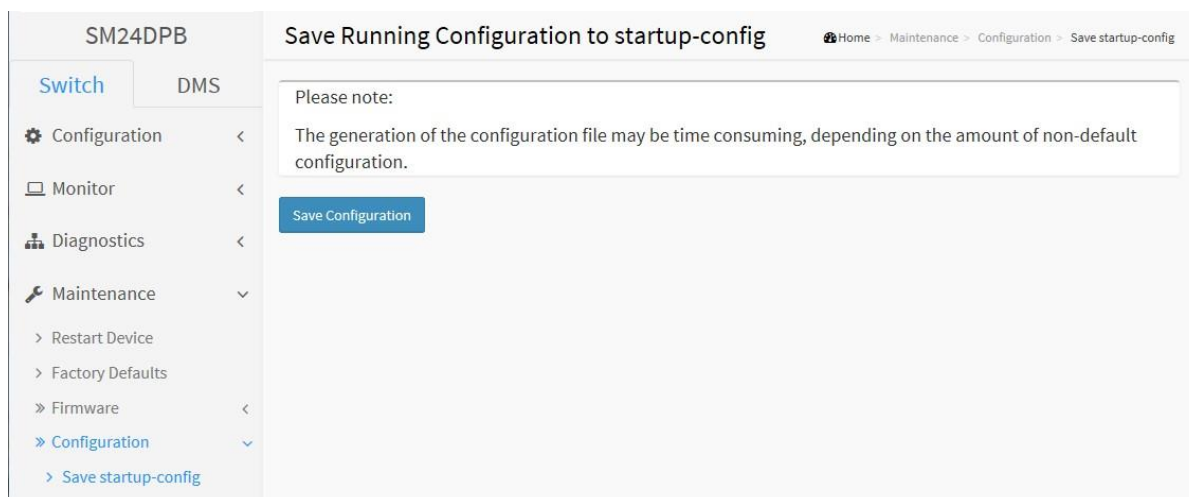
This copies the running-config to startup-config, thereby ensuring that the currently active configuration will be used at the next reboot.

#### Web Interface

To save the Running configuration to startup-config in the web interface:

1. Click Maintenance, Configuration, Save startup-config.
2. **Note:** The generation of the configuration file may be time consuming, depending on the amount of non-default configuration.
3. Click the **Save Configuration** button. The message *Save Running Configuration to startup-config startup-config saved successfully* displays to indicate a successful save.

**Figure 5-4.1: Save Startup-config page**





**Buttons :**

**Save Configuration:** Click to save configuration; the running configuration will be written to flash memory for system boot up to load this startup configuration file.

**Messages:** *Save Running Configuration to startup-config. startup-config saved successfully.*

## 5-4.2 Upload

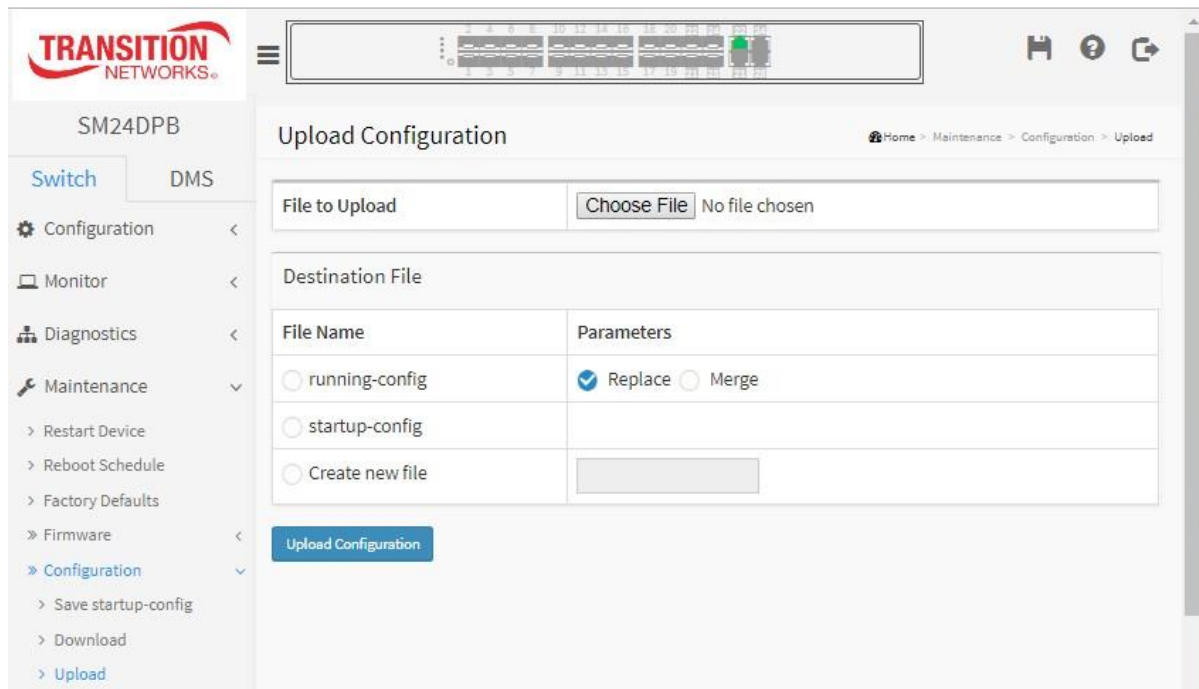
The configuration upload function will be backed up and saved configuration from the switch's configuration into the running web browser PC. It is possible to upload any of the files on the switch to the web browser. Select the file and click Upload of running-config may take a little while to complete, as the file must be prepared for upload.

### Web Interface

To upload configuration in the web interface:

1. Click Maintenance, Configuration, Upload to display the Upload Configuration page.
2. Click Browse to select a file.
3. Click the Upload Configuration button.

**Figure 5-4.2: Upload Configuration page**



The system files are:

1. **running-config:** A virtual file that represents the currently active configuration on the switch. This file is volatile. If the destination is running-config, the file will be applied to the switch configuration. This can be done in two ways:
  - Replace mode:** The current config is fully replaced with the config in the uploaded file.
  - Merge mode:** The uploaded file is merged into running-config.
2. **startup-config:** The startup configuration for the switch, read at boot time.
3. **Create new file:** A read-only file with vendor-specific configuration. The message "Upload successfully completed." should display when done.

## Buttons

**Upload Configuration:** Click the “Upload” button then the running web management PC will start to upload the configuration from the managed switch configuration into the location PC, user can configure web browser’s upload file path to keep configuration file.

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.

**Messages:** *Warning: Syntax check completed with errors; configuration has not been activated.*

### 5-4.3 Download

This page lets you export the switch configuration for maintenance needs. Any current configuration files will be exported as text format.

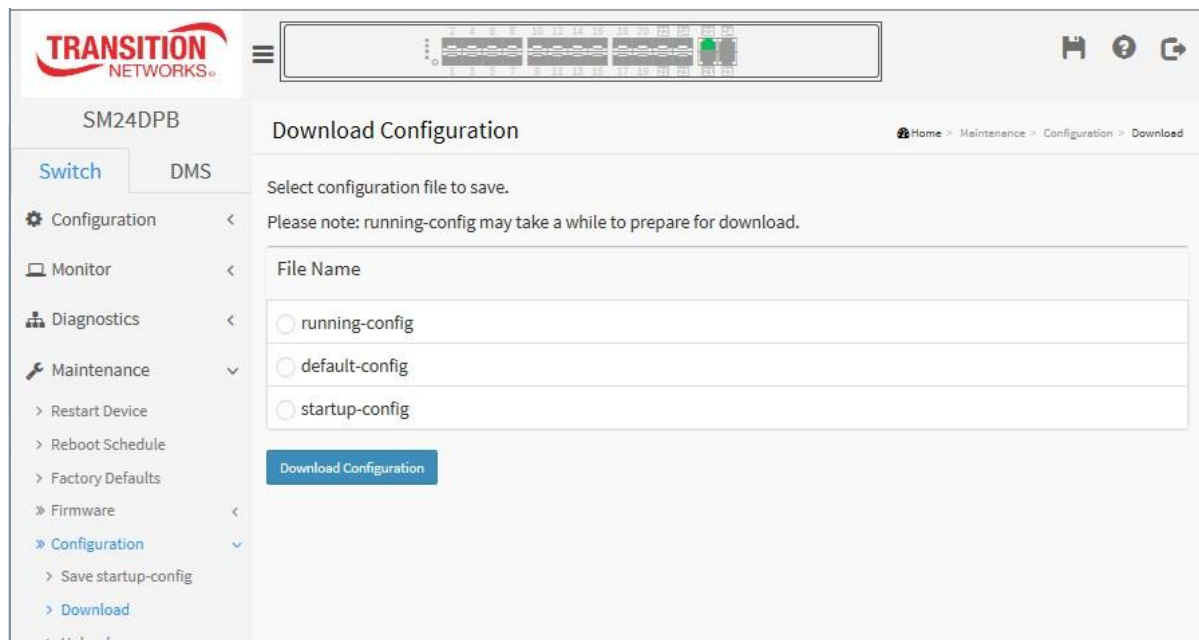
If the file system is full (i.e. contains the three system files mentioned above plus two other files), it is not possible to create new files, but an existing file must be overwritten or another deleted first.

#### **Web Interface**

To download configuration in the web interface:

1. Click Maintenance, Configuration, Download.
2. Select a File Name (running-config or default-config or startup-config).
3. Click the Download Configuration button.
4. If prompted, select Open or Save the file.

**Figure 5-4.3: Download Configuration page**

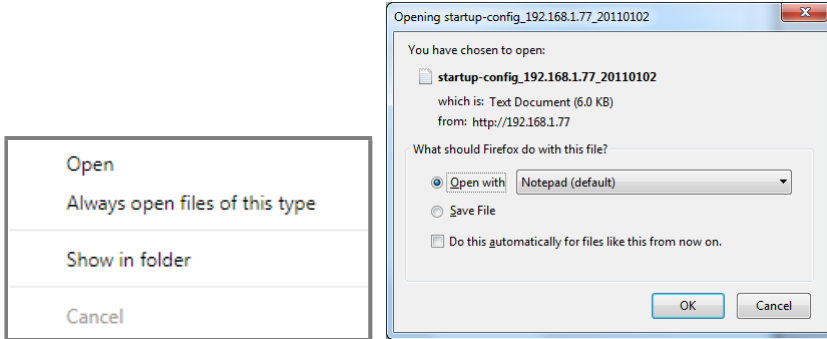


#### **Parameter descriptions:**

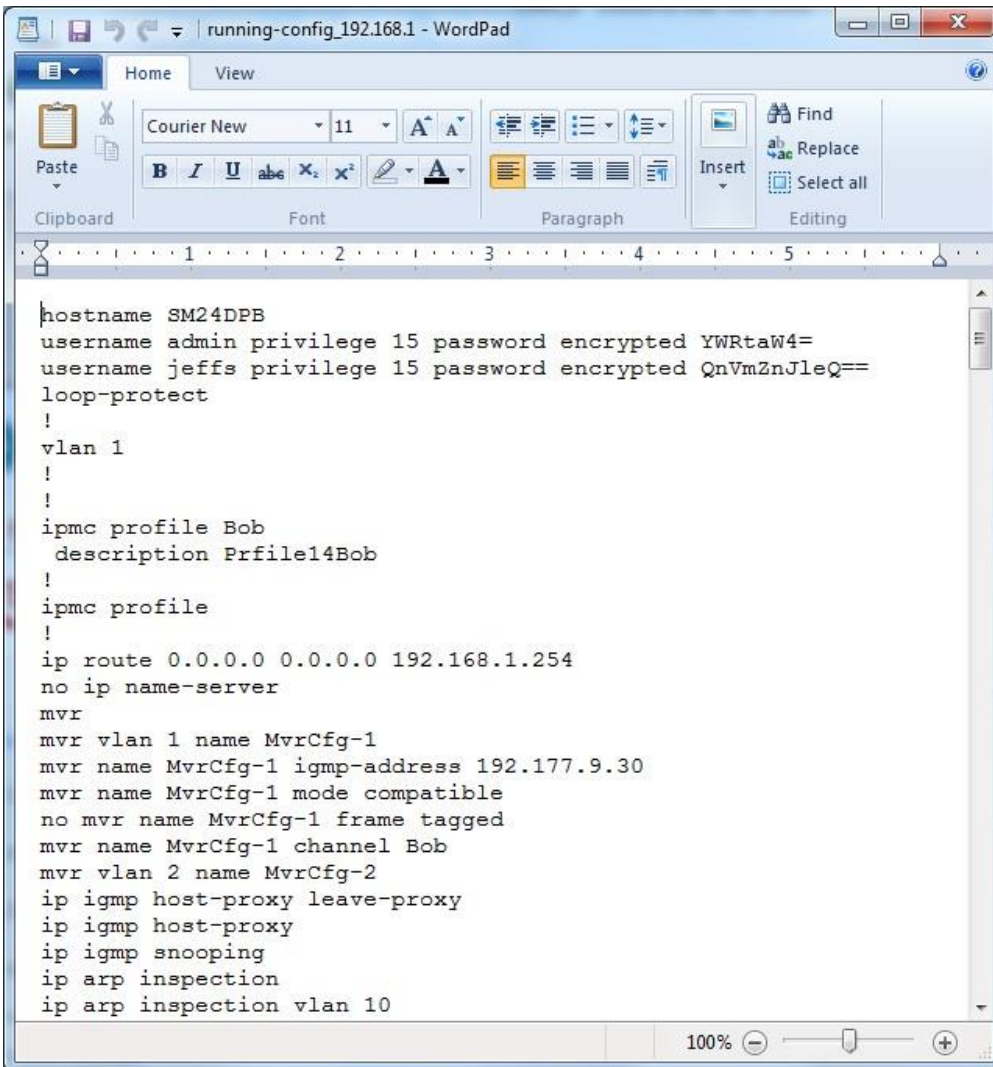
**File Name :** Check the desired radio button (e.g., running-config or default-config or startup-config).

**Download Configuration:** Click the button then the switch will start to download the configuration from configuration stored location PC or Server.

**Messages:** (Web browser dependent)



**Sample Download Output:**



## 5-4.4 Activate

It is possible to activate any of the configuration files present on the switch, except for running-config which represents the currently active configuration.

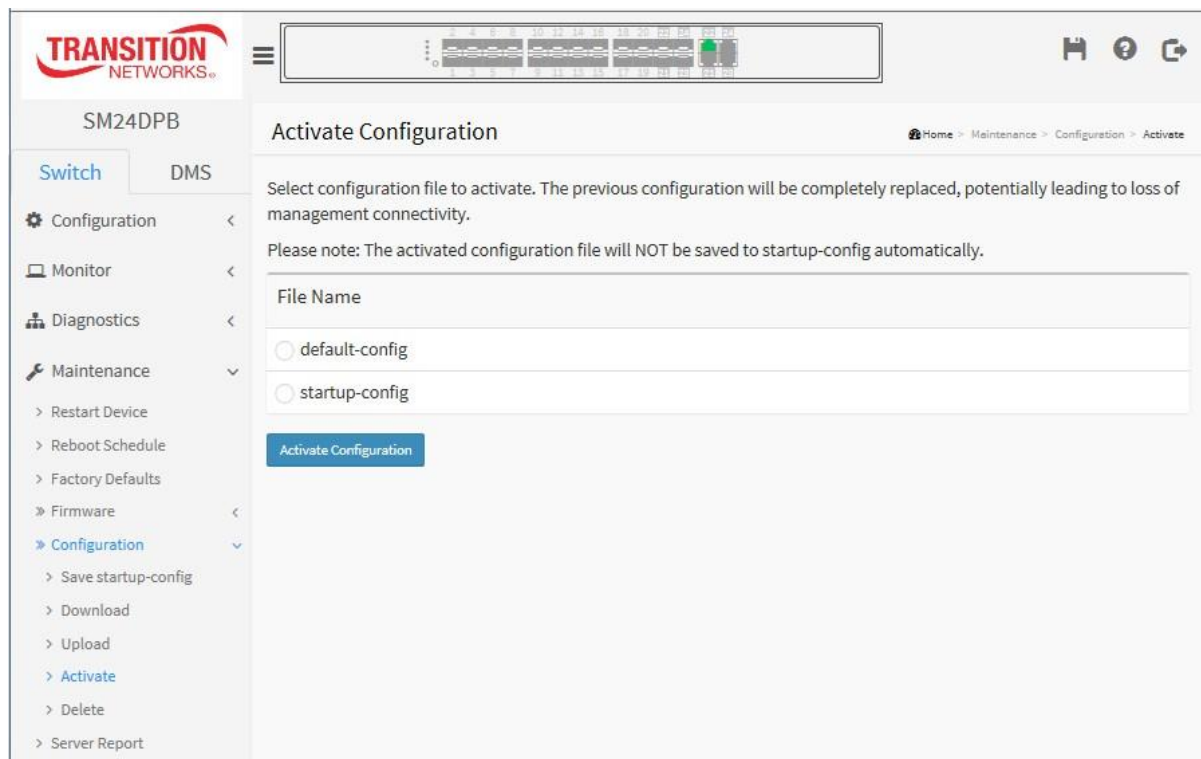
Select the file to activate and click the **Activate Configuration** button. This will initiate the process of completely replacing the existing configuration with that of the selected file.

### Web Interface

To activate configuration in the web interface:

1. Click Maintenance, Configuration, Activate.
2. Select configuration file to activate (default-config or startup-config). The previous configuration will be completely replaced, potentially leading to loss of management connectivity.
3. Please note: The activated configuration file will NOT be saved to startup-config automatically.
4. Click the **Activate Configuration** button.

**Figure 5-4.4: Activate Configuration page**



System files include:

**default-config:** A read-only file with vendor-specific configuration. This file is read when the system is restored to default settings.

**startup-config:** The startup configuration for the switch, read at boot time.

**Buttons :**

**Activate Configuration:** Click the “Activate” button then the default-config or startup-config file will be activated and to be this switch's running configuration.

The Login page displays and you must log in again to continue.

**Messages:** If no files are available to activate the message “*No files available for activation.*” displays.



### 5-4.5 Delete

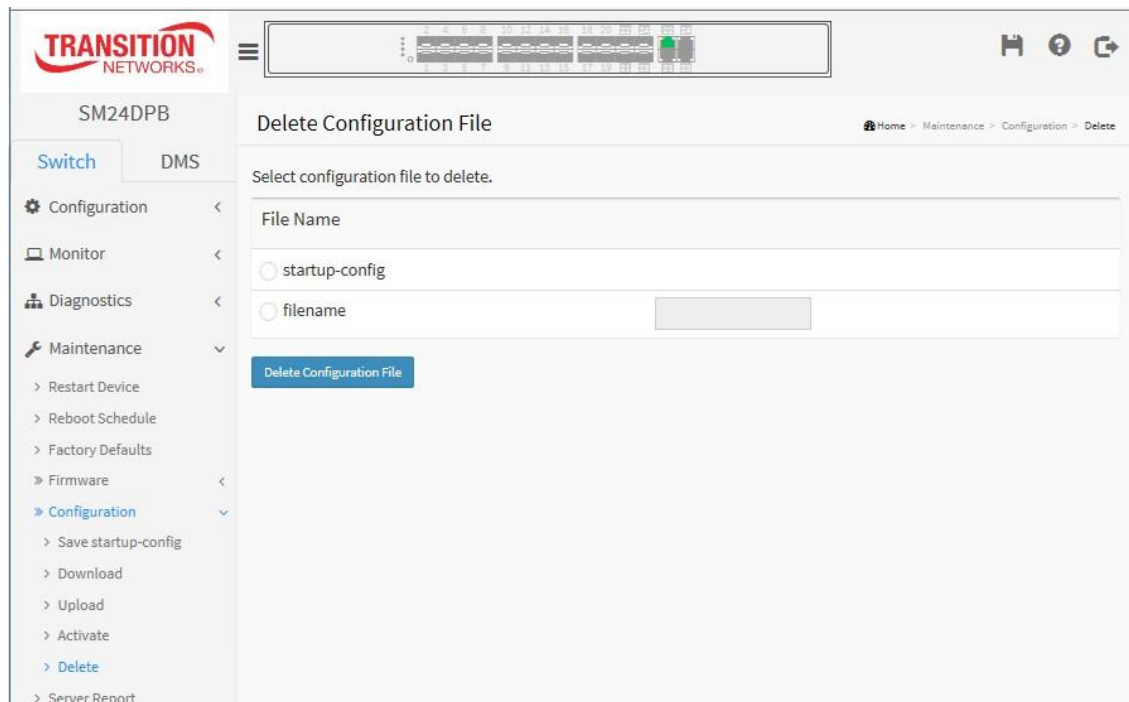
It is possible to delete any of the writable files stored in flash, including startup-config. If this is done and the switch is rebooted without a prior save operation, this effectively resets the switch to its factory default configuration.

#### Web Interface

To delete configuration in the web interface:

1. Click Maintenance, Configuration, Delete.
2. Select the configuration file to delete (*startup-config* or enter another *filename*).
3. Click the **Delete Configuration File** button.
4. At the “Are you sure ...” message click **Yes**.

**Figure 5-4.5: Delete Configuration File page**



There is one system file and one optional filename entry option:

1. **startup-config**: The startup configuration for the switch, read at boot time.
2. **filename** : radio button to enter an existing file to delete.

#### Buttons:

**Delete Configuration File:** Click the button to delete the startup-config file or the entered *filename*; this effectively resets the switch to default configuration.

#### Messages:

*Could not delete file "default-config".*



## 5-5 Server Report

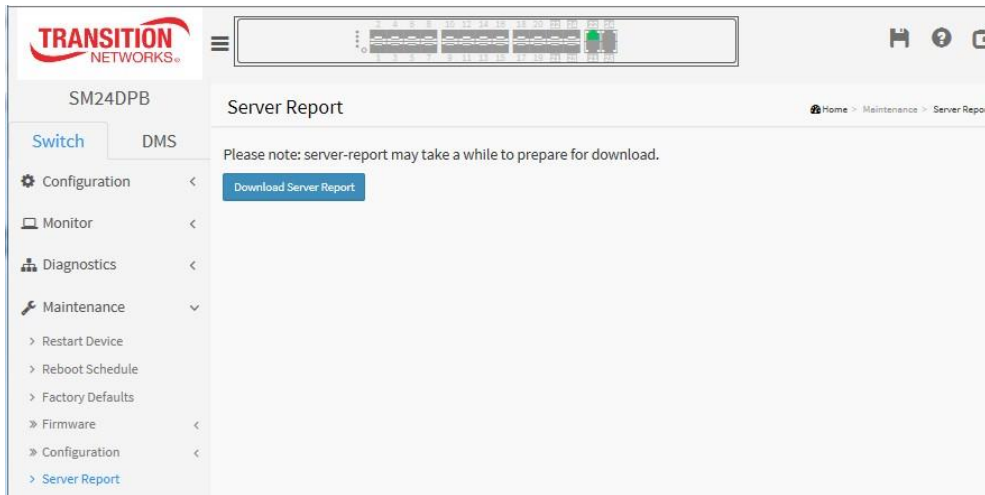
It is possible to download a server report text file on the switch to the web browser.

### Web Interface

To delete configuration in the web interface:

1. Click Maintenance, Server Report. Note: server-report may take a while to prepare for download.
2. Click the **Download Server Report** button.
3. At the dialog box select Open or Save.

Figure 5-5.1: Server Report page



### Sample Output:

```

server-report - Notepad
File Edit Format View Help
----- System Overview -----
Model Name: SM24DPB
Connected Devices: 1
Firmware Version: v6.54.2925 2018-07-31
MAC Address: 00-c0-f2-47-45-27
System uptime: 1d 03:52:47
IP Address: 192.168.1.1
Subnet Mask: 255.255.255.0
Gateway: 192.168.1.254
Primary DNS:
----- running-config -----
hostname sw0apalooop-protectv1an11!ipac profile Bob description Prfl1c4db!ipac profile!ip route 0.0.0.0
0.0.0.0 192.168.1.254 no ip name-server mvr v1an 1 name Mvrcfg-1mvr name Mvrcfg-1 igmp-address 192.177.9.30mvr
name Mvrcfg-1 mode compat!bno mvr name Mvrcfg-1 frame taggedmvr name Mvrcfg-1 channel Bobmvr v1an 2 name
Mvrcfg-1ip igmp host-proxy leave-proxyip igmp host-proxyip igmp snooping!ip arp inspection!ip arp inspection v1an
10!ip arp inspection v1an 30 logging permit!ip verify source!ip source binding interface GigabitEthernet 1/2 1
192.168.1.77 255.255.255.0mp auto-mactctz!id Qaggregation mode smac smac ip portspanning-tree mode rstp
spanning-tree edge bpdu-filterspanning-tree edge bpdu-guardspanning-tree recovery interval 60spanning-tree mst 0
priority 245!spanning-tree mst 1 v1an 10-100smrp-server view 2ndview 2 includeaccess-list ace success-list ace
4 next 3 dmac-type multicast frame-type ipvs action deny rate-limiter 1 redirect interface GigabitEthernet 1/2
logging shutdownaccess-list ace 3 next 4 frame-type ipv4access-list ace 2 next 3 frame-type arpaaccess-list ace 1
next 2 frame-type etypport-security aging port-security gvrp max-vlans 200pr time 10!in-time 20 leave-time 90
leave-all-time 1500system name SM24DPBsystem description Managed switch, 20-port 100/1000 SFP, 4-port SFP/8J-45
Combo!interface GigabitEthernet 1/1 spanning-tree mst 1 cost 500000 spanning-tree mst 1 port-priority 48 loop-
protect action log mvr name Mvrcfg-1 type source port-security sticky port-security !interface
GigabitEthernet 1/2 spanning-tree edge spanning-tree link-type point-to-point spanning-tree restricted-role
spanning-tree restricted-ctn spanning-tree bpdu-guard spanning-tree mst 0 cost 500000 spanning-tree mst 0 port-
priority 64 loop-protect action log no loop-protect tx-mode mvr immediate-leave ip igmp snooping max-groups 2 !p
igmp snooping router no ip arp inspection trust ip arp inspection check-vlan ip arp inspection logging permit
ip verify source ip verify source limit 2 port-security sticky port-security port-security violation trap-
shutdown aggregation group 1 gvrp broadcast-storm-protection broadcast-storm-protection pps 1!interface
GigabitEthernet 1/3 loop-protect action shutdown log no loop-protect tx-mode mvr immediate-leave mvr name
Mvrcfg-1 type receiver ip igmp snooping max-groups 3 ip igmp snooping router ip igmp snooping immediate-leave
no ip arp inspection trust ip arp inspection check-vlan ip arp inspection logging all speed auto duplex auto
port-security sticky port-security port-security violation shutdown aggregation group 1 gvrp broadcast-
storm-protection broadcast-storm-protection action both broadcast-storm-protection pps 2!interface
GigabitEthernet 1/4 loop-protect action shutdown log no loop-protect tx-mode mvr immediate-leave mvr name
Mvrcfg-1 type source ip igmp snooping max-groups 8 ip igmp snooping router ip igmp snooping immediate-leave
port-security sticky port-security port-security violation trap aggregation group 2 gvrp broadcast-storm-
protection broadcast-storm-protection action both broadcast-storm-protection pps 10!interface GigabitEthernet
1/5 loop-protect action shutdown log no loop-protect tx-mode mvr immediate-leave mvr name Mvrcfg-1 type source
ip igmp snooping router port-security sticky port-security port-security violation shutdown aggregation
group 2 gvrp broadcast-storm-protection broadcast-storm-protection pps 20!interface GigabitEthernet 1/6 loop-
protect action shutdown log mvr immediate-leave mvr name Mvrcfg-1 type receiver port-security sticky port-
security violation trap-shutdown aggregation group 3 broadcast-storm-protection broadcast-
storm-protection action both broadcast-storm-protection pps 100 broadcast-storm-protection timer 120!interface
GigabitEthernet 1/7 mvr immediate-leave larp port-security sticky port-security port-security violation
broadcast-storm-protection action log!interface GigabitEthernet 1/9 port-security sticky port-security
!interface GigabitEthernet 1/4 port-security sticky port-security !interface GigabitEthernet 1/22 port-security sticky
port-security aggregation group 2 gvrp!interface GigabitEthernet 1/13 port-security sticky port-security !
interface GigabitEthernet 1/24 port-security sticky port-security !interface GigabitEthernet 1/25 port-
security sticky port-security !interface GigabitEthernet 1/16 port-security sticky port-security
!interface GigabitEthernet 1/17 port-security sticky port-security !interface GigabitEthernet 1/18 port-
security sticky port-security !interface GigabitEthernet 1/19 port-security sticky port-security
!interface GigabitEthernet 1/20 port-security sticky port-security !interface GigabitEthernet 1/21 port-
security sticky port-security !interface GigabitEthernet 1/22 port-security sticky port-security
00:1b:1b:2:6c:4b v1an 1 port-security !interface GigabitEthernet 1/23 port-security sticky port-security !
!interface GigabitEthernet 1/24 port-security sticky port-security !interface v1an 1 ip address 192.168.1.77
255.255.255.0!spanning-tree aggregation spanning-tree link-type point-to-point!!line console 0!line vty 0!line
vty 1!line vty 2!line vty 3!line vty 4!line vty 5!line vty 6!line vty 7!line vty 8!line vty 9!line vty 10!line
vty 11!line vty 12!line vty 13!line vty 14!line vty 15!end
----- System Log -----
    
```

## Chapter 6. About DMS

### 6-1 The DMS Tab

The Transition Networks 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 SM24DPB main menu pane on the left, navigate to the DMS tab to display the main DMS features: Management, Graphical Monitoring, and Maintenance.

### DMS vs. NMS

Compared to an NMS, the DMS is more useful, usable, efficient, and cost-effective.

<b>DMS:</b> Device Management System	<b>NMS:</b> Network Management System
<ul style="list-style-type: none"> <li><input type="checkbox"/> Embedded in Switches, No Extra Server</li> <li><input type="checkbox"/> Intuitive and Easy to Use</li> <li><input type="checkbox"/> Work with All Third Party IP Devices</li> <li><input type="checkbox"/> <i>Free</i> Software License</li> <li><input type="checkbox"/> Failover Mechanism in Any Switch</li> </ul>	<ul style="list-style-type: none"> <li><input type="checkbox"/> Need Extra Server Hardware Cost</li> <li><input type="checkbox"/> Need Training and Experiences to Use</li> <li><input type="checkbox"/> Works Only with Owned-Brand Products</li> <li><input type="checkbox"/> Need License-Based Pricing</li> <li><input type="checkbox"/> Single Point of Failure</li> </ul>

### 6-2 DMS Features

#### Topology View:

- Auto Discover All Types of IP Devices - IP, MAC, Port, Device Type, Device Name
- On-Line Search, Sort, and Edit - by IP, MAC, Port, Type, Name
- Auto Detect Device Status Real Time - Link Status, Trap Events, Alarm Notification
- Troubleshooting Cables & Devices - Cabling Status and Device Check-Alive
- Reboot Remote Devices
- Single Sign-On Login
- Export View Pages to Files
- Auto Provisioning and more

#### Floor View:

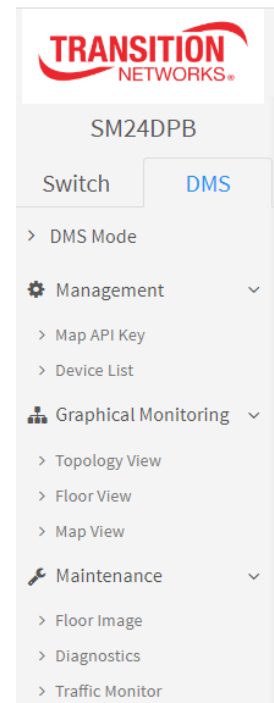
- Anchor Devices onto Floor Maps
- Find Devices Instantly by Floor View
- 10 Maps can be Stored in Each Switch
- IP Surveillance/VoIP/WiFi Applications
- Other Features same as Topology View

#### Map View:

- Anchor Devices onto Google Map
- Find Devices Instantly by Google View
- On-Line Search Company/Address
- Outdoor IP Surveillance/WiFi Applications
- Other Features same as Topology View

#### Traffic Monitor:

- Monitor Traffic and Packets of Devices
- Analyze by Day/Week/Port/Device
- Perform Health Check by Threshold
- Auto Alarm if Abnormal Condition Met
- Customized Behaviors per Request



**Diagnostics:**

- One Click to Diagnose Cable Status
- One Click to Check Device Alive
- Identify Bad Cable Connection Instantly
- Reboot Remote Devices
- to Resume Operation Remotely
- Customized Behaviors per Request

**Troubleshooting Tool (Find My Switch):**

- One Click to Identify the Switch Location, all LEDs of the Switch Blink when Activated
- A DMS Feature and Mobile Apps Available
- Help IT/TS to Locate Devices Easily in a Complicated Network Environment

**DMS Notes**

- DHCP Server Global mode will be disabled when changing gateway IP from DMS page.
- With DMS enabled, VLAN port role will be changed when the port state becomes link down.

The following chapters describe the DMS features in detail.

## Chapter 7. DMS > Mode

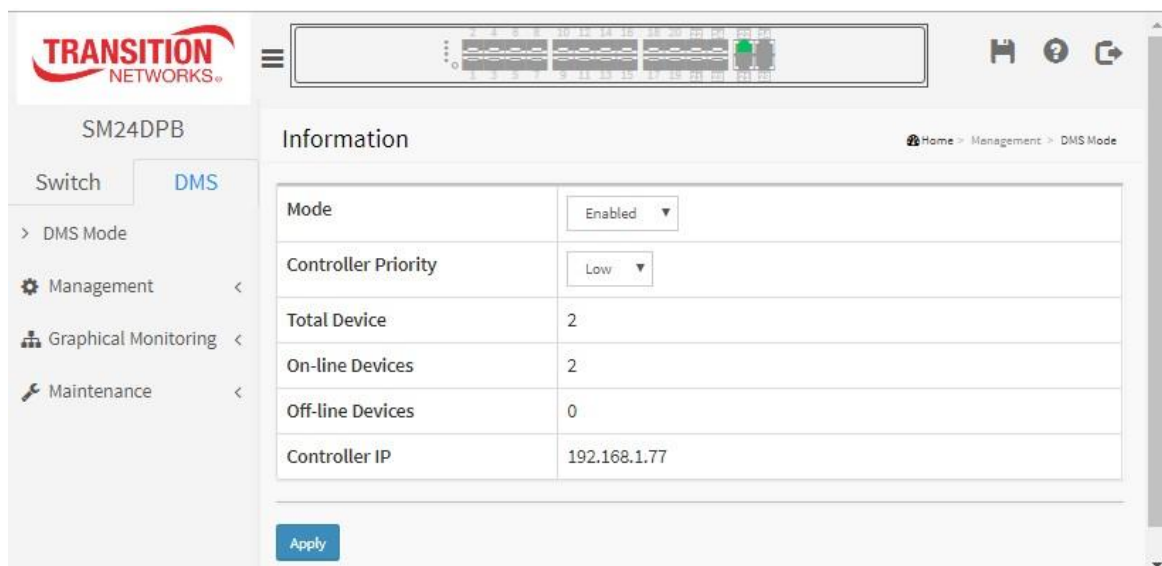
### 7-1 DMS Mode

The DMS Mode page lets you define the switch DMS mode and Controller priority.

#### Web interface

To configure DMS Mode in the web interface:

1. Click the DMS tab.
2. At Mode dropdown select Enabled (default) or Disabled.
3. At the Controller Priority dropdown select a level of control for this switch.
4. Click the Apply button.



#### Parameter descriptions:

**Mode** : Enable/Disable the DMS function. Or you can choose "High" priority to make this switch the Master switch. 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.

**Controller Priority**: Choose "Controller Priority" when enabling DMS:

**High**: Makes this switch the Controller (master) switch.

**Mid**: Gives this switch a medium level of control.

**Low**: Gives this switch a low level of control.

**Non**: This switch will never become the Controller (master) switch.

**Total Device** : Shows how many IP devices are detected and displayed in Topology view.

**On-Line Devices** : Shows how many IP devices on-line in Topology view.

**Off-Line Device** : Shows how many IP devices off-line in Topology view.

**Controller IP** : Shows the Controller (Master) switch's IP address.




## 7-2 Devices List

This page provides an overview of discovered devices.

### DMS > Management > Device List

### Web interface

To configure Devices List in the DMS tab of the web interface:

1. Click DMS, Management, Devices List.
2. Click  to refresh Devices List.
3. Check the  Auto-refresh checkbox to refresh the information automatically.
4. Click  to edit Device Name and HTTP Port.
5. Check the Remove checkbox to move the device to Offline status.
6. Click  to save changes.

### Parameter descriptions:

**Remove** : Remove off-line device from the list.

**Status** : Device Online or Offline.

**Device Type**: The type of the network connectivity devices such as PC, SWITCH, AP, IP Cam, IP Phone or Others.

**Model Name** : The model name of the network connectivity devices.

**Device Name** : The device name of the network connectivity devices.

**MAC** : The mac address of the device.

**IP Address** : The IP address of the network connectivity devices.

### Buttons

**Auto-refresh:** Check this box to refresh the page automatically every 3 seconds.

**Refresh :** Refreshes the displayed table starting from the input fields.

**Edit Device Name :** Add the input fields for editing the device names and the http ports.

**Apply :** Click to save changes.

**Figure 7-2: Sample Devices List**

The screenshot shows a web interface titled "Devices List" with a breadcrumb trail "Home > Management > Device List". It features an "Auto-refresh" checkbox, a refresh icon, and a search box. Below is a table with 9 entries. The table has columns: Remove (checkbox), Status (Online/Offline), Device Type, Model Name, Device Name, MAC, and IP Address. The status of each device is indicated by a colored dot (green for Online, red for Offline). At the bottom, there is a pagination control showing "Showing 1 to 9 of 9 entries" and "Previous 1 Next" buttons, along with an "Apply" button.

Remove	Status	Device Type	Model Name	Device Name	MAC	IP Address
<input type="checkbox"/>	Online	AP	NETGEAR, WNR3500Lv2	WNR3500Lv2 (Gateway)	44-94-FC-55-E1-FE	192.168.0.5
<input type="checkbox"/>	Online	IP Phone	Yealink T42	T42(192.168.0.3)	00-15-65-83-F0-B2	192.168.0.4
<input type="checkbox"/>	Online	Others	D-LINK DI-LB604	Dual WAN Link Balancer	00-21-91-E2-AF-79	192.168.0.253
<input type="checkbox"/>	Online	PC	AKIRA-PC	AKIRA-PC	00-1D-60-AF-C0-2A	192.168.0.123
<input type="checkbox"/>	Offline	PC	LENOVO-PC	LENOVO-PC	00-90-9E-9A-A2-A9	192.168.0.66
<input type="checkbox"/>	Online	SWITCH	PSGS-2610F	L2 Managed PoE Switch	00-40-C7-12-34-56	192.168.0.1
<input type="checkbox"/>	Online	SWITCH	PSGS-2610F	PSGS-2610F	00-40-C7-98-76-54	192.168.0.2

### Parameter descriptions:

**Remove:** Check to remove Off-line devices from the device.

**Status:** Device link state (Online / Offline). Click the linked status to display the related **DMS > Maintenance > Diagnostics** page.

**Model Name:** Device model name.

**Device Name:** Device name.

**Edit Device Name:** Device name edit (save in flash).

**MAC:** Device MAC address.

**IP Address:** Device IP address, hyper-link re-direct to device website.

**Version:** Device firmware version.

### Devices List sub-tab Use Notes

- Use the "Auto Refresh" to automatically refresh the page.
- Use the "Refresh button" to refresh the page immediately one time.
- "Edit Device Name" can edit device name.(Not including Switch )
- "Show" can select 10 / 25 / 60 / All entries to be displayed per page.
- The "Search box" can search any part of Status / Device Type / Model Name / Device Name / MAC / IP Address.

- ❑ The device can not be removed when its status is Online.
- ❑ The device can be removed when its status is Offline.
- ❑ More than two Offline devices can be removed at the same time.
- ❑ You can "Sort" by Status / Device Type / Model Name / Device Name / MAC / IP Address.
- ❑ You can Remove / Status / Device Type / Model Name / Device Name / MAC / IP Address.

**Figure 7-2: Devices List** with Edit Device Name button clicked:

The screenshot shows the 'Devices List' page in the SM24DPB web interface. The table contains the following data:

Remove	Status	Device Type	Model Name	Device Name	Edit Device Name	MAC	IP Address	Edit Http Port	Edit User Name	Edit User Password
<input type="checkbox"/>	Online	SWITCH	SM24DPB	SM24DPB	SM24DPB	00-C0-F2-47-45-27	192.168.1.77			
<input type="checkbox"/>	Online	Others			<input type="text"/>	00-1B-11-B2-6D-4B	192.168.1.99			

Showing 1 to 2 of 2 entries

Previous 1 Next

Apply


# Chapter 8. DMS > Graphical Monitoring

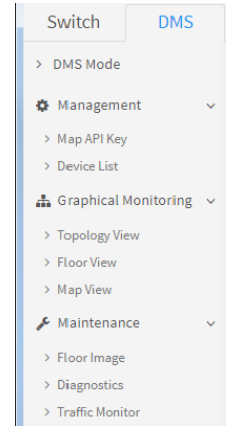
## 8-1 Topology View

This page displays a view of the topology in a cluster of networks.

### Web interface

To configure DMS Topology View in the web interface:

1. Click DMS, Graphical Monitoring, and Topology View.
2. Click  to select the display information in Topology View.



### DMS > Graphical Monitoring > Topology View

You can left mouse click a device icon to display its current parameters. The parameters include Device Type (e.g., SWITCH), Device Name (SM24DPB), Model Name (SM24DPB), Mac Address (e.g., 00-40-c7-1c-b6-46), IP Address (e.g., 192.168.1.77), and PoE (e.g., 0 W) parameters, and the Login, Find Switch, Diagnostics, Dashboard, and Notification icons.

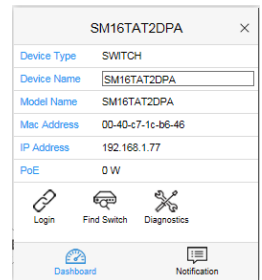
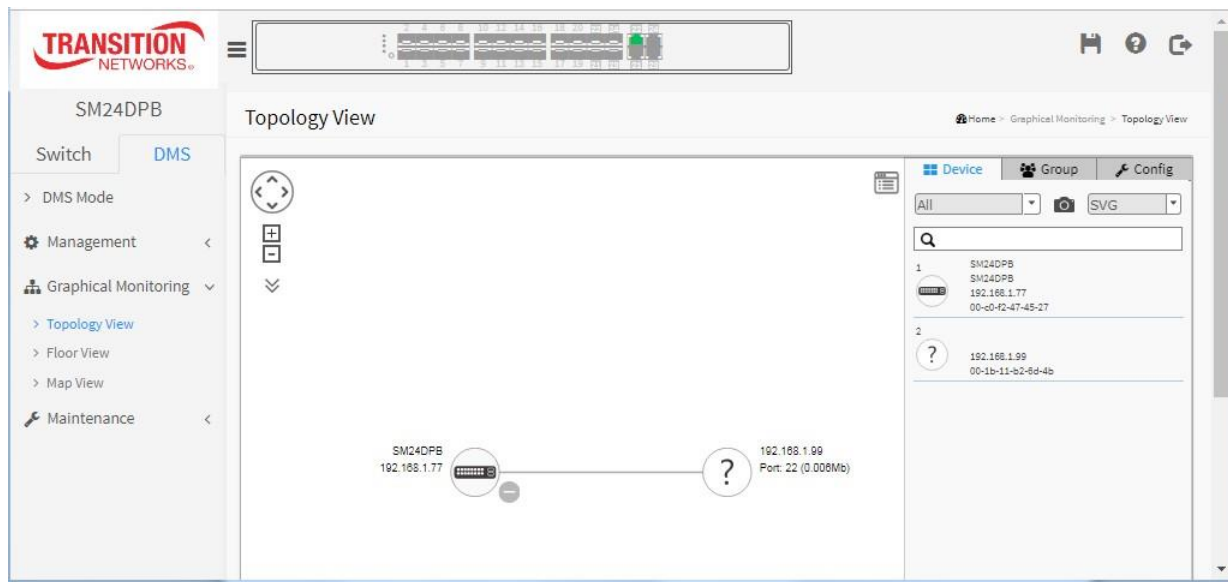

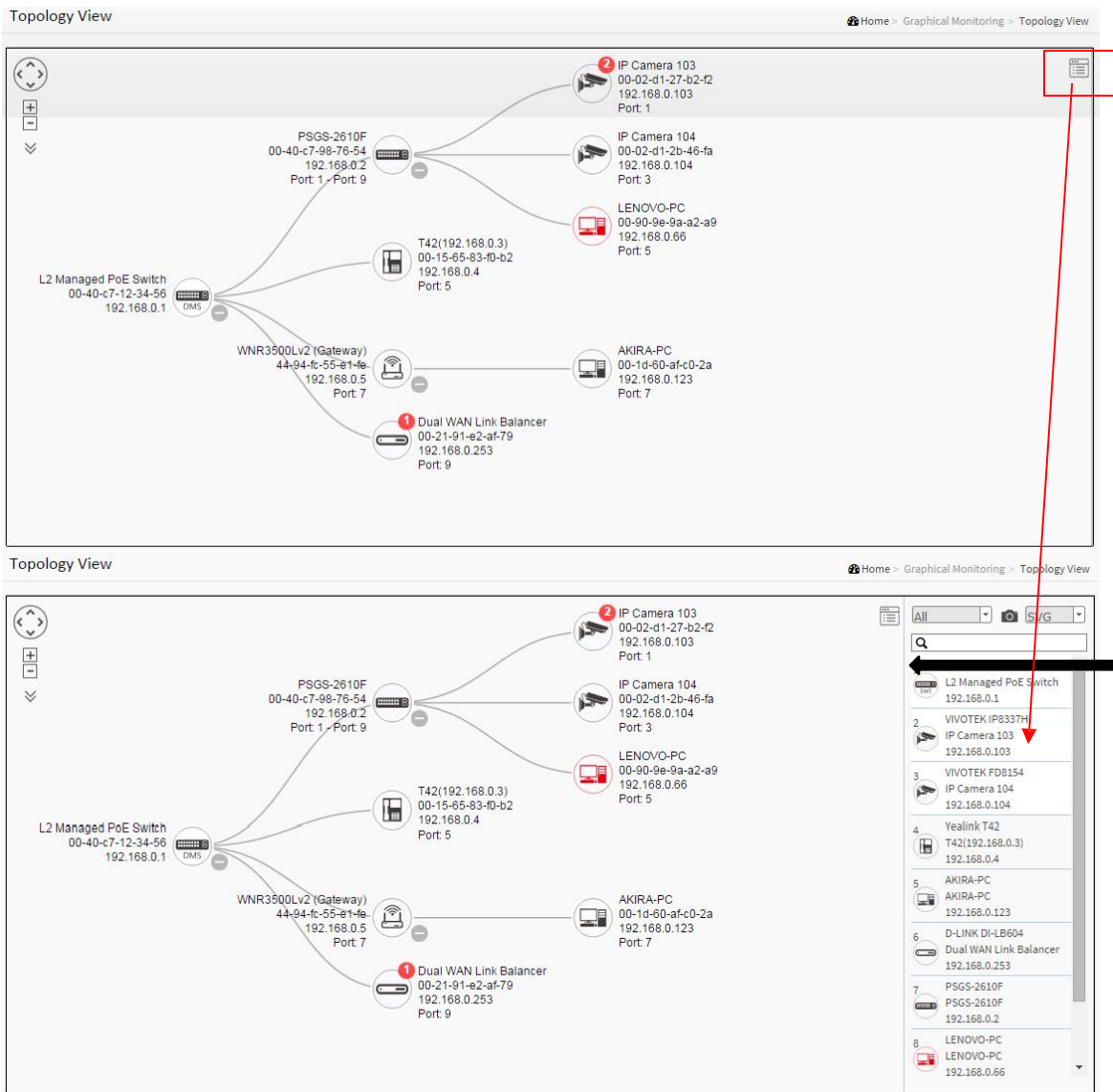


Figure 8-1: Topology View





You can click the  icon (top right corner of the screen) to toggle between displaying and hiding the right-hand properties column.



**Parameter descriptions:**

**Login :** Login to this device.

**Trouble shooting :** Move to trouble shooting page.

**Find my switch :** Allows administrators to quickly and easily find the Switch in their cabinet.

**Reboot Device :** Reboot the PD device.

**Device Type :** Select Device Type to PC, IP phone, IP cam, AP or other device.



: Use the directional pad to scroll up, down, left, or right.



: Use the slider to zoom in/out. Alternatively, use the mouse to navigate by clicking and dragging the left mouse button. Use the mouse wheel to zoom in/out.



: Save the whole View to SVG, PNG or PDF file format.



: Select the device category (ALL, SWITCH, PC, IP Cam, IP Phone, AP, Others, Off Line).



: Search for device by typing IP/MAC address or Model/Device name.

## Graphical Monitoring > Topology View sub-tab Use Notes

### General Test Function

- The link up SWITCH / PC / IP Cam / IP Phone / AP can show device image in display panel.
- Use the "Direction button" to move the display panel.
- Use the "Zoom button" to zoom-in or zoom-out display panel.
- Use the "Mouse wheel" scrolling causes zoom-in or zoom-out Display panel.
- Use "Mouse wheel" scrolling zoom out to min zoom will hiding device information.
- Use the "Pull down menu" to select three items Device Name / Model Name / Mac / IP / PoE, and then device image will show the selected items.
- The device image color indicators are OnLine --> black / OffLine --> red.
- The device image "+ / -" can show / hide the down train members.
- The device image shows Dashboard / Notification / Monitor function and shows the Device Name in the title.

### Dashboard Function

- Use the Parent node to manually add the parent node in "Parent Node".
- Only device OffLine can be "Removed".
- Only an unknown device can select "Device Type".
- The "Device Name" can change device name on SWITCH / PC / IP Cam / IP Phone / AP / Others.
- The "Http Port" can change http port on PC / IP Cam / IP Phone / AP / Others.
- The "PoE Used" can show PoE value / Non-PoE on PC / IP Cam / IP Phone / AP / Others.
- The "PoE Supply" can show the Power Used on the Switch.
- The "Find Switch" will light the switch for 15 seconds when SWITCH OnLine or OffLine.
- The "Diagnostics" check connection / cable status on SWITCH / PC / IP Cam / IP Phone / AP / Others.
- "Streaming" can show live video streaming when IP Cam is OnLine (browser support required)
- "Streaming" can't show live video streaming when IP Cam is OffLine.
- Verify "Reboot" can reboot device on IP Cam/IP Phone/AP/Others, when the device is OnLine only.

### Notification Function

- The "Messages Dot" can show the total number of messages, and over 9 messages become N Dot .
- The "messages note" can show Level / Date & Time / Information. You can "Edit" and "Delete" messages.

### Monitor Function

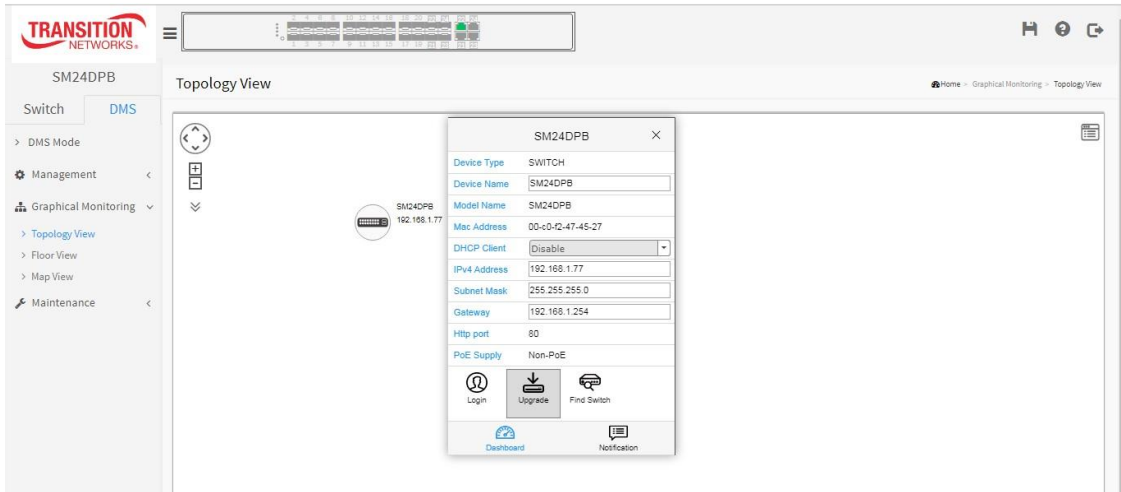
- Use "Monitor" to show device traffic immediately on PC / IP Cam / IP Phone / AP / Others.
- The "Monitor" line colors are limit setting -> red / traffic-> blue / X-coordinate, Y-coordinate -> black.
- "Monitor" can set a minimum / maximum number of traffic on PC / IP Cam / IP Phone / AP / Others.
- Device traffic out of range can show Messages Dot , if device traffic continued out of range just send one time.

Global setting

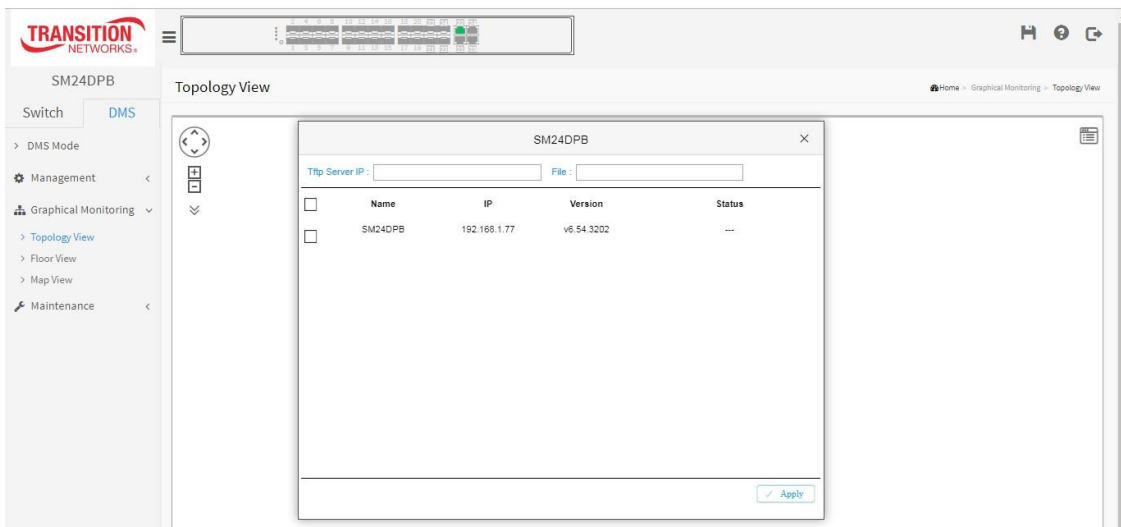
- The "Global settings button" can show or hidden Device / Group / Config.
- "Type select" ALL / SWITCH / PC / IP Cam / IP Phone / AP / Others / Off Line only show belong the type device at the devices list and display panel in "Device".
- "Snapshot" can store SVG / PNG / PDF file to a topology record in "Device".
- The "Search box" can search any part of Status / Device Type / Model Name / Device Name / MAC / IP Address in "Device".
- "Devices list" can show Device Name / Model Name / IP / Mac in "Device".
- "Devices list" device color: OnLine -> black / OffLine -> red in "Device".
- "Devices list image" can find the device location in topology, and use blue circle to mark device than move to the center position in "Device".
- "Type select" ALL / SWITCH / PC / IP Cam / IP Phone / AP / Others / Off Line only show the type of device at topology view in "Group".

## Upgrade Firmware from DMS > Graphical Monitoring > Topology View

1. Have a TFTP Server running and configured.
2. Navigate to DMS > Graphical Monitoring > Topology View.
3. Left click the SM24DPB icon to display the option pane:



4. Click the Upgrade button to display the firmware upgrade table.



5. Enter the Tftp Server IP address, enter the filename (e.g., *SM24DPB\_v6.54.3202\_201601073.imgs*) and click the Apply button.
6. Wait a few moments for the upgrade to successfully complete.

**Messages:** *Error : Firmware download fail.*

## 8-2 Floor View

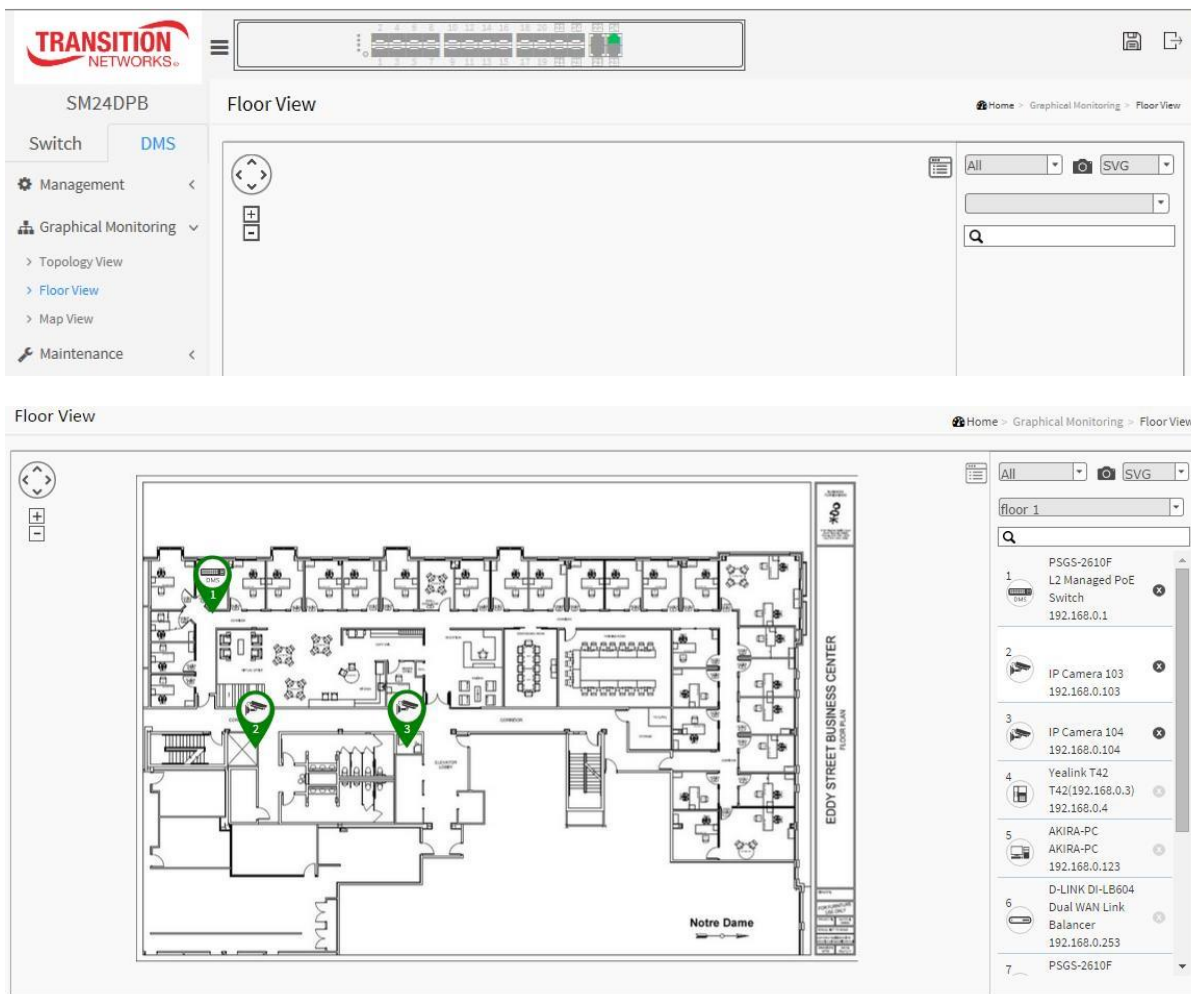
This page lets you place a device per time onto the custom image, which you have already uploaded by dragging-and-dropping markers in the device list. Here you can easily plan IP devices installation location onto the custom uploaded floor images.

### Web interface

To configure DMS Floor View in the web interface:

1. Click DMS, Graphic Monitoring, Floor View.

**Figure 8-2: Floor View**



: Use the directional pad to scroll up, down, left, or right.



: Use the slider to zoom in/out. Alternatively, you can use the mouse to navigate by clicking and dragging the left mouse button. Use the mouse wheel to zoom in/out.



: SnapShot; save the whole View to SVG, PNG or PDF



: Select the device category.



: Search for device by typing IP/MAC address or Model/Device name.

## Graphical Monitoring > Floor View sub-tab Use Notes

### General Test Function

- The floor image can show in display panel by add image from maintenance floor image.
- Use the "Direction button" to move around the display panel.
- Use the "Zoom button" to zoom-in or zoom-out display panel.
- The "Mouse wheel" scrolling causes zoom-in or zoom-out display panel.
- Press the left mouse button to move the Floor Image / Device Marker Bubble.
- The "Device Marker Bubble" colors are: Green --> OnLine device / red --> OffLine device, and if already added will become blue and show the location.
- "Device Marker Bubble" can keep the location when refresh / reload page.
- "Switch Bubble" can show Login / Upgrade / Find Switch / Remove in "Dashboard".
- "PC Bubble" can show Diagnostics / Remove in "Dashboard".
- "IP Cam Bubble" can show Login / Diagnostics / Streaming / Reboot / Remove in "Dashboard".
- "IP Phone Bubble" can show Login / Diagnostics / Reboot / Remove in "Dashboard".
- "AP Bubble" can show Login / Diagnostics / Reboot / Remove in "Dashboard".
- "Others Bubble" can show Login / Diagnostics in "Dashboard".
- The SWITCH / PC / IP Cam / IP Phone / AP / Others Bubble can show messages in "Notification".
- The PC / IP Cam / IP Phone / AP / Others Bubble can also show device traffic immediately in "Monitor".

### Global setting

- Type select ALL / SWITCH / PC / IP Cam / IP Phone / AP / Others / Off Line only show belong the type device at the devices list and display panel in "Entry".
- "Snapshot" can store SVG / PNG / PDF file to a topology record in "Entry".
- The floor image can be selected at floor image pool, and Name / IP is correctly in "Entry".
- The floor image can be shared to all switches, If there are more than two switches.
- The "Search box" can search any part of Status / Device Type / Model Name / Device Name / MAC / IP Address in "Entry".
- The "Devices list" can show Device Name / Model Name / IP / Mac in "Entry".
- The "Devices list" can show the black color to the OnLine device and red color to the OffLine device in "Entry".
- The "Devices list" can add / delete Device Marker Bubble, already added devices Black / can add devices Gray in "Entry".

**Example:** Three Floor Images added:

The screenshot displays the 'Floor Image Management' page in the SM24DPB web interface. The page includes a navigation sidebar on the left with options like 'Switch', 'DMS', 'Management', 'Graphical Monitoring', and 'Maintenance'. The main content area shows a file management section with a status bar indicating 'Maximum: 10 files', 'Used: 3 file(s)', and 'Free: 7 file(s)'. Below this is a form to 'Add Floor Image' with a 'Choose File' button and a 'Name' input field. A table lists three existing floor plans, each with a 'Select' checkbox, a 'No.' column, a 'File Name' column, and an 'Image' column. The table data is as follows:

Select	No.	File Name	Image
<input type="checkbox"/>	1	Floor Plan - 1st Floor (192.168.1.77)	
<input type="checkbox"/>	2	Floor Plan - 2nd Floor (192.168.1.77)	
<input type="checkbox"/>	3	Floor Plan - 3rd Floor (192.168.1.77)	

At the bottom of the table, there is a 'Delete' button.

### 8-3 Map View

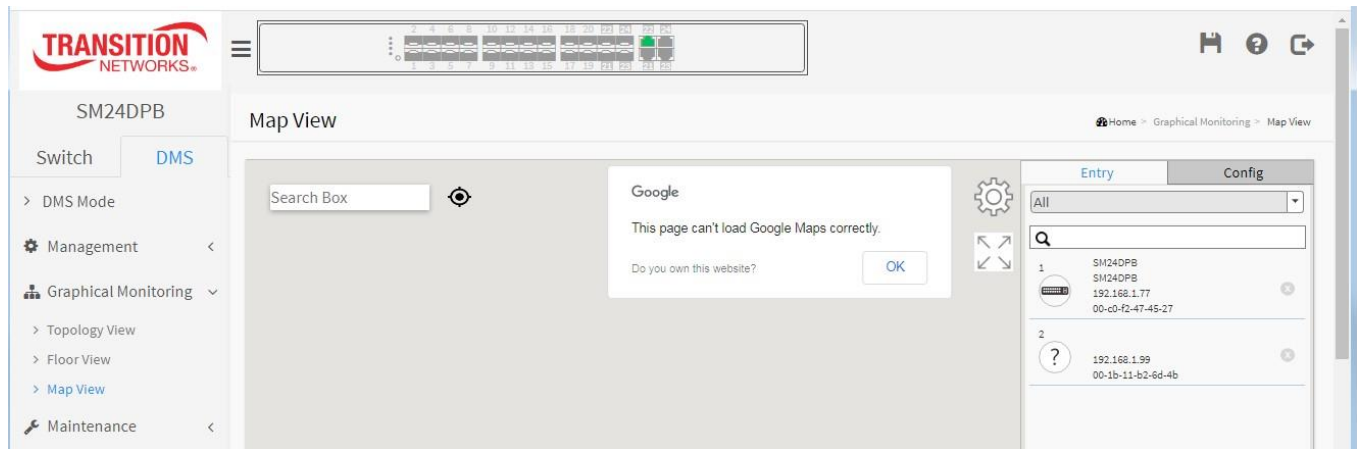
This page lets you view a realistic representation of device in the network. To find one of devices within the network, enter the device name in the search bar. Click "Device List" to hide the "Device List" on the page or show a list of devices.

#### Web interface

To configure DMS Map View in the web interface:

1. Click DMS, Graphical Monitoring, Map View.

**Figure 8-3: Map View**



: Use the directional pad to scroll up, down, left, or right.



: Use the slider to zoom in/out. Alternatively, you can use the mouse to navigate by clicking and dragging the left mouse button. Use the mouse wheel to zoom in/out.



: Select the device category.



: Search for device by typing IP/MAC address or Model/Device name.

**Message:** 192.168.1.77 wants to track your physical location.



Select *Allow once*, or *Always allow*, or *Always deny and don't tell me*. If allowed, the Map View displays, with the option to display a Satellite view.

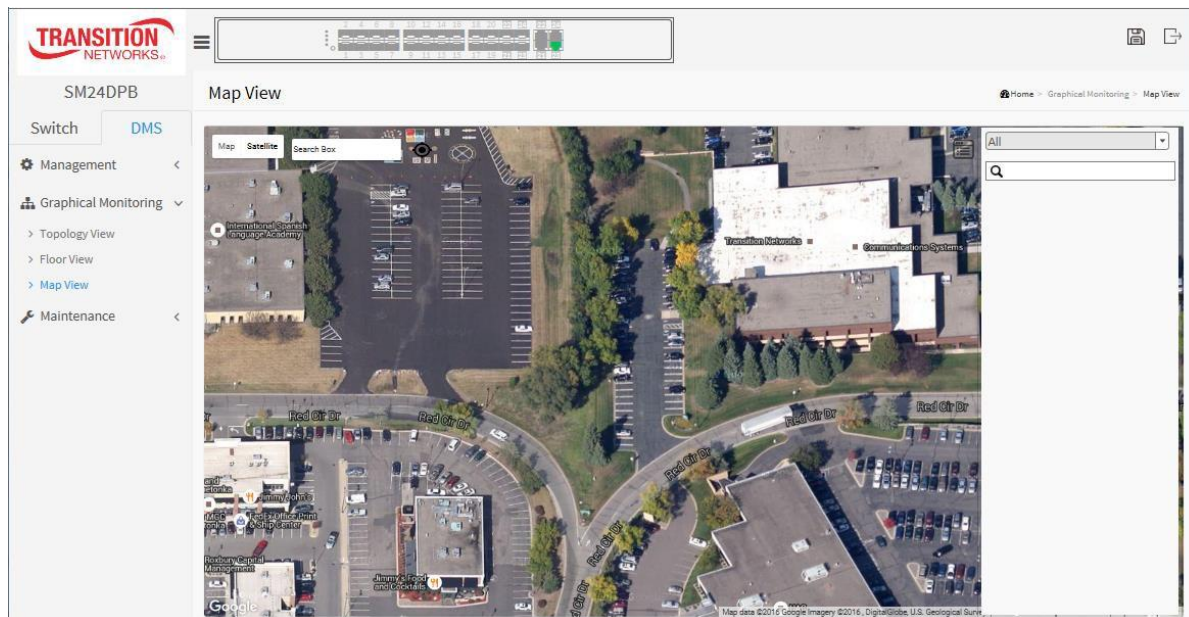


**Graphical Monitoring > Map View sub-tab Use Notes**

General Test Function

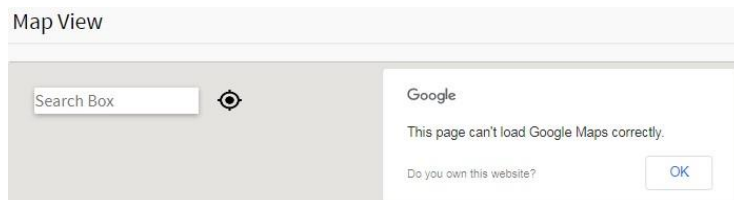
- The Map / Earth can change display panel type and show map in display panel.
- The "Search Box" can find the address of any location.
- The "Location icon" can locate the position of network machine room.
- Use the "Zoom button" to zoom-in or zoom-out display panel.
- The "Mouse wheel" scrolling causes zoom-in or zoom-out display panel.
- The "yellow Pegman icon" can see Street View (Street View might not be available in all regions).
- The "SWITCH Bubble" can show Login / Upgrade / Find Switch / Remove in "Dashboard".
- The "PC Bubble" can show Diagnostics / Remove in "Dashboard".
- The "IP Cam Bubble" can show Login / Diagnostics / Streaming / Reboot / Remove in "Dashboard".
- The "IP Phone Bubble" can show Login / Diagnostics / Reboot / Remove in "Dashboard".
- The "AP Bubble" can show Login / Diagnostics / Reboot / Remove in "Dashboard".
- The "Others Bubble" can show Login / Diagnostics in "Dashboard".
- The SWITCH / PC / IP Cam / IP Phone / AP / Others Bubble can show messages in "Notification"
- The PC / IP Cam / IP Phone / AP / Others Bubble can show device traffic immediately in "Monitor"

**Figure 8-3: Satellite View**



**Map View Troubleshooting**

**Message:** This page can't load Google Maps correctly



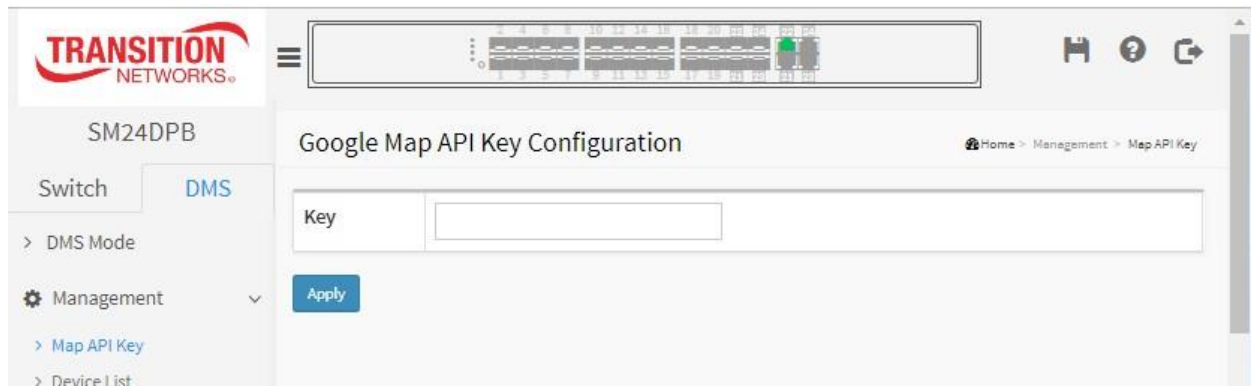
**Meaning:** There is a problem with Google Maps. If loading over 25,000 maps loaded per day over the network, request a new key from <https://developers.google.com/maps/documentation/directions/get-api-key> then apply the new key at the page for displaying the map view completely. See the [Google Account Changes webpage](#).

**Recovery:** Click the OK button to clear message and go to "Google Map API Key Configuration" below.

## Google Map API Key Configuration

You need a valid API key and a Google Cloud Platform billing account to access Google core product. If not, DMS Map View will not be able to load Google Map correctly. Please visit the Google website below and follow the on-screen directions to get an API key:

<https://developers.google.com/maps/documentation/directions/get-api-key>



### Parameter descriptions:

**Key** : Specify the Google API Key.

### Buttons

**Apply** : Click to save changes.

## Chapter 9. DMS > Maintenance

### 9-1 Floor Image

This page lets an administrator add or delete a custom map or floor image. You can upload or manage floor map images. Due to the limitation of the flash memory, up to 20 JPEG images, each of a max. of 256KB size, can be uploaded to the switch.

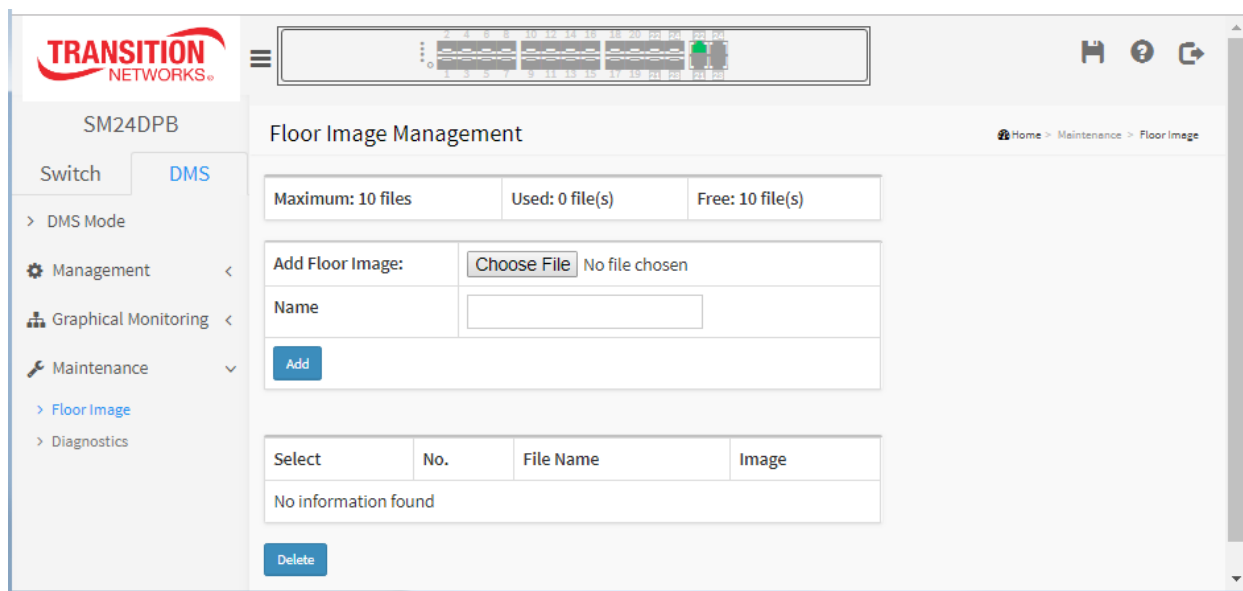
#### DMS > Maintenance > Floor Image

##### Web interface

To configure DMS Information in the web interface:

1. Click DMS, Maintenance, Floor Image.
2. Click "Browse..." to select a Floor image in your device.
3. Click Add.

Figure 9-1: Floor Image Management



##### Parameter descriptions:

**Maximum:** e.g., select up to 10 floor image files.

**Used:** the number of floor image files currently in use e.g., 0 file(s).

**Free:** the number of floor image files currently in use e.g., 10 file(s).

**Add Floor Image:** Click the Choose File button and browse to and select one of up to 10 floor image files in .JPG or .PNG file format. The add image size must be less than 524152 bytes in size.

**Name:** enter a name for this floor image file (e.g., which switch the image belongs in). No special characters are allowed.

### Buttons

**Add:** Click Add to upload. When done, a snapshot will be available on screen.

**Delete:** If you need to remove an existing floor map, select its checkbox and click Delete to remove.

### Graphical Monitoring > Map View sub-tab Use Notes

#### Floor Image Use Notes

- You can add an image in the floor image pool and show in floor view.
- Images can't be added with the same name on one switch.
- You can add up to ten images over ten files on one switch.
- With add image you must edit Image / Name at the same time.
- The add image type is restricted to Jpg / Png.
- The add image size must be less than 524152 bytes.
- More than two Floor Images can be deleted at the same time.

#### Floor Image Management Example:

The screenshot displays the 'Floor Image Management' interface. At the top, it shows the 'TRANSITION NETWORKS' logo and a navigation breadcrumb: Home > Maintenance > Floor Image. The main content area is titled 'Floor Image Management' and includes a summary of file usage: 'Maximum: 10 files', 'Used: 3 file(s)', and 'Free: 7 file(s)'. Below this is an 'Add Floor Image' section with a 'Choose File' button and a 'Name' input field. A table below lists three existing floor plans:

Select	No.	File Name	Image
<input type="checkbox"/>	1	Floor Plan - 1st Floor (192.168.1.77)	
<input type="checkbox"/>	2	Floor Plan - 2nd Floor (192.168.1.77)	
<input type="checkbox"/>	3	Floor Plan - 3rd Floor (192.168.1.77)	

A 'Delete' button is located at the bottom left of the table area.

## 9-2 Diagnostics

The **DMS > Diagnostics** page lets you troubleshoot any issue you have with device connected to the network. This feature is designed primarily for administrators to verify and test the link route between the switch and the device. A troubleshooting solution is provided by the system so that administrators can detect where the problem lies. Note that the topology of network needs to be saved for this function to work properly.

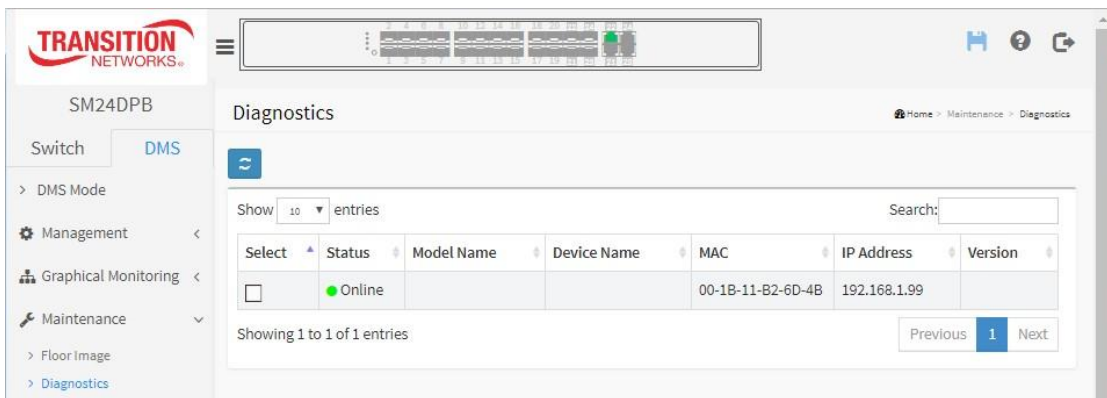
### DMS > Maintenance > Diagnostics

#### Web interface

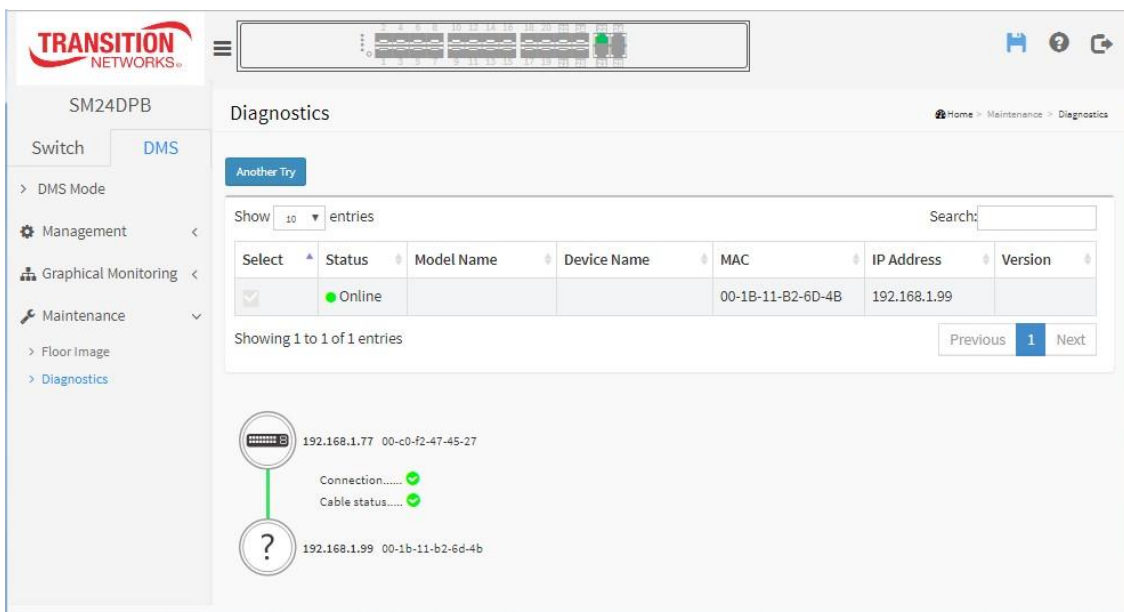
To configure DMS Information in the web interface:

1. Click DMS, Maintenance, Diagnostics.
2. Check the Select checkbox for a device to start the recover Mechanism.

Figure 9-2: Device Status



Check the **Select** checkbox to display Connection and Cable status:



Click the **Another Try** button to attempt another discovery.

**Parameter descriptions:**

**Select** : Select an off-line device from the list. Check the Select checkbox to display entries.

**Status** : The current device status (*Online* or *Offline*).

**Model Name** : The model name of the network connectivity devices (e.g., *SM24DPB*).

**Device Name** : The device name of the network connectivity devices (e.g., *SM24DPB*).

**MAC** : The MAC address of the device.

**IP Address** : The IP address of the network connectivity devices.

**Version** : The SW version of the network connectivity devices.

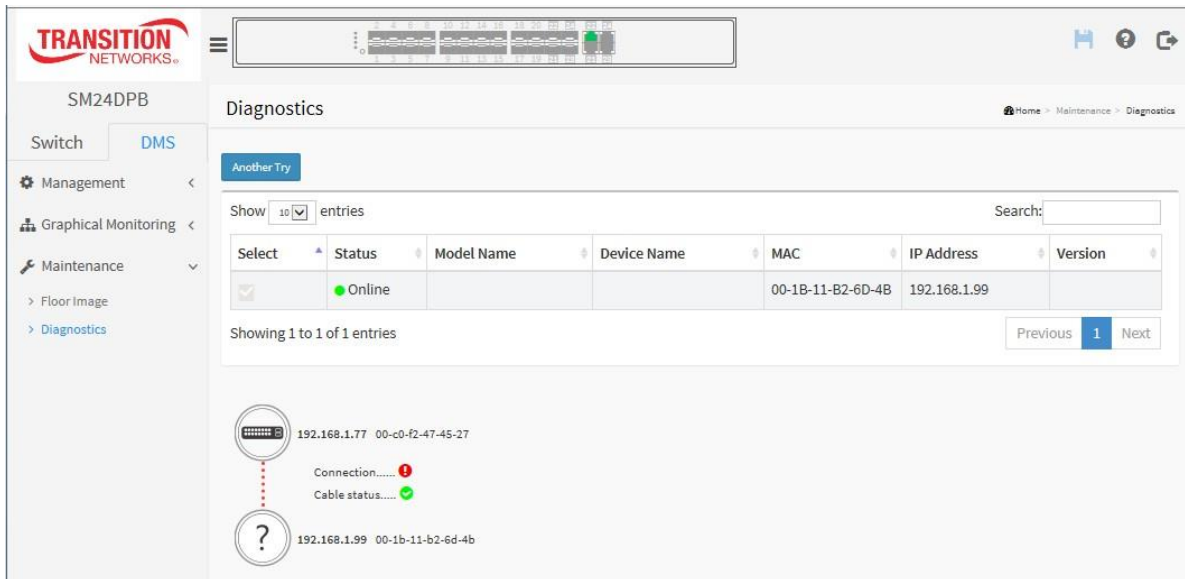
**Buttons**

**Refresh** : Refreshes the displayed table starting from the input fields.

**Search** : Search for a key word.

**Diagnostics Use Notes**

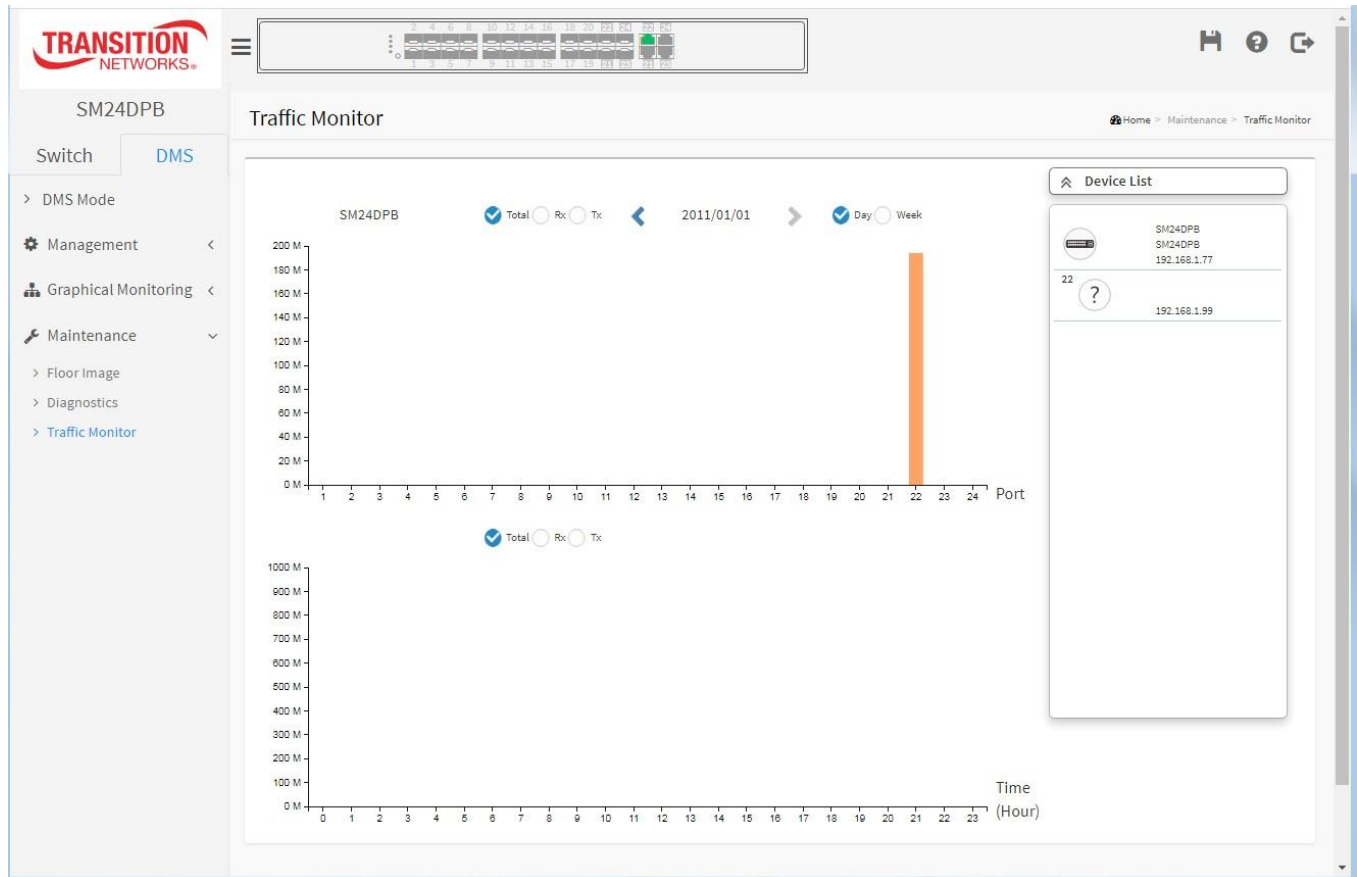
- The Search box can search any part of Status / Model Name / Device Name / MAC / IP Address / Version.
- You can Sort by Status / Model Name / Device Name / MAC / IP Address / Version.
- The Selected item can check for Connection / Cable status at one time.
- Use the Another Try button to return to the Diagnostics page.



### DMS > Maintenance > Traffic Monitor

DMS support traffic monitoring of each port and keeps a one week record that can be used to compare and analyze through a visual chart.

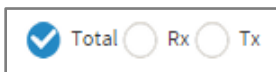
This page displays a visual chart of network traffic of all the devices. Numbers are shown in Mbit/s. You can view the traffic of all the ports or a specific port. Click on specific port on the traffic chart to reveal its traffic during the day. You can select to display a summary of a day's or a week's traffic by selecting the check circle on top. The same applies to the selection of Rx Tx traffic. A single port's traffic is shown at the lower half of the screen.



### Procedure

1. Click **DMS > Maintenance > Traffic Monitor**.
2. Select the parameters to display.
3. Select the device to monitor.

### Parameter descriptions:



: Use to select Tx, Rx or both information to display in this page.



: Use to select a day or week of information to display on this page.

## **DMS Troubleshooting**

**Problem:** The switch lists itself as the only device in Topology View of DMS.

**Problem:** In DMS, the Local image shows the IP address of another switch.

*Description:* The switch is listed as only device in DMS Topology View in DMS; all devices are listed in DMS device list. This is usually because the switch's gateway is not configured appropriately.

*Resolution:* An IP Route must be configured manually. For example, a switch IP address of 192.168.1.77 should have the following IP route configured: ip route 0.0.0.0 0.0.0.0 192.168.1.x. Without the IP route configured, you may be unable to view all devices on the network in DMS.

1. Go to DMS >Management >DMS Mode to check if the controller IP is correct.
2. Verify that the gateway of this switch is correctly configured.
3. Verify that all connected devices are displayed in DMS Topology View.

**Problem:** DMS Connectivity diagnostics fails to ICMP reachable device.

*Description:* DMS displays a device which is reachable via ICMP ping as failing the connection status in diagnostics. Cable status displays as *OK*.

*Resolution:* Contact Transition Networks 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.

**Problem:** When the SM24DPB is used with an older web browser such as Internet Explorer 8, the left side navigation window does not display.

*Solution:* The issue is related to web browser compatibility. Please try to upgrade to IE10 for better support, or use Firefox or Google Chrome instead of IE8.



## Chapter 10. Troubleshooting

Most problems are caused by the following situations. Check for these items first when you start troubleshooting:

1. Verify the install procedures were performed correctly. See the related Install Guide.
2. Check if the SM24DPB 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 SM24DPB 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 SM24DPB 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. Record any related error messages, conditions, configurations for your Tech Support Specialist to consider.
9. Contact Transition Networks Tech Support. See below.

### **Transition Networks Inc.**

10900 Red Circle Drive, Minnetonka, MN 55343

Telephone: +1-952-941-7600 / Toll Free: 800-526-9267 / Fax: 952-941-2322

E-Mail: [customerservice@transition.com](mailto:customerservice@transition.com) / [techsupport@transition.com](mailto:techsupport@transition.com)

## Appendix A. Service, Warranty & Tech Support

See the *SM24DPB Install Guide* for related information.

## Appendix B. Compliance Information

See the *SM24DPB Install Guide* for related information.



Transition Networks

10900 Red Circle Drive

Minnetonka, MN 55343 USA

Tel: 952- 941-7600 or 1-800-526-9267

Fax: 952-941-2322

Copyright© 2016-2020 Transition Networks. All rights reserved. Printed in the U.S.A.

SM24DPB Managed Fiber Switch Web User Guide 33682 Rev. C