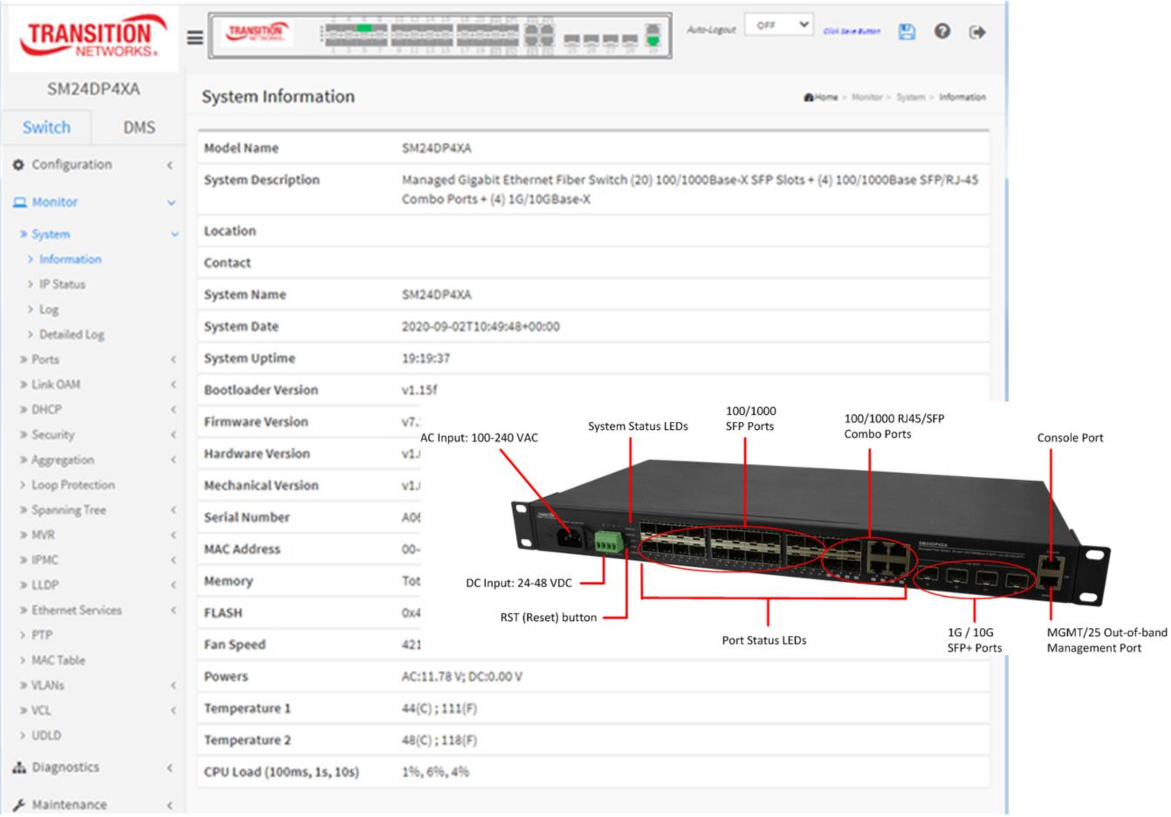
SM24DP4XA

Managed Gigabit Ethernet Fiber Switch

(20) 100/1000Base-X SFP Slots + (4) 100/1000Base SFP/RJ-45 Combo Ports + (4) 1G/10GBase-X SFP+ Slots



System Information

Model Name	SM24DP4XA
System Description	Managed Gigabit Ethernet Fiber Switch (20) 100/1000Base-X SFP Slots + (4) 100/1000Base SFP/RJ-45 Combo Ports + (4) 1G/10GBase-X
Location	
Contact	
System Name	SM24DP4XA
System Date	2020-09-02T10:49:48+00:00
System Uptime	19:19:37
Bootloader Version	v1.15f
Firmware Version	v7.
Hardware Version	v1.
Mechanical Version	v1.
Serial Number	A0
MAC Address	00-
Memory	Tot
FLASH	0x4
Fan Speed	421
Powers	AC:11.78 V; DC:0.00 V
Temperature 1	44(C) ; 111(F)
Temperature 2	48(C) ; 118(F)
CPU Load (100ms, 1s, 10s)	1%, 6%, 4%

Web User Guide

33770 Rev. D

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.

SM24DP4XA Managed Gb Fiber Ethernet Switch Web User Guide, 33770 Rev. D

Record of Revisions

Rev	Date	Description of Changes
B	6/16/20	FW v7.10.2404: display system name on Web browser tab. FW v7.10.2544: add Auto-logout and note that to use DHCP on the management port, the default PVLAN config must be changed.
C	10/16/20	FW v7.10. 2679: fix Auto-logout, Rapid Ring disable, and VLAN 1 disabled issues, add RADIUS and TACACS Key encrypt on Show Running Config and fix API Device list table.
D	3/2/21	FW v7.20.0042: Add SFTP support in CLI. Add ACL API commands. Add Gateway Address binding interface. Fix IGMP RV value under IPMC VLAN Configuration issue. Add Appendix B – G.8032 Major and Sub Rings Configuration. Have TLV IEEE802.3 MAC/ PHY configuration/status in LLDP packets. Fix download file via SolarWinds SFTP server error. Fix upgrade FW fail via SCP. Send an IEEE802.3 MAC/ PHY packet with two configuration/status TLVs when switch receives a packet with LLDP-MED.

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.

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 | techsupport@transition.com | customerservice@transition.com

Table of Contents

1. Introduction

Overview

This manual describes how to configure, monitor, test, and maintain the SM24DP4XA switch via the Web user interface (UI). This switch is a next-generation Layer 2 managed switch with 128Gbps switching capacity. It provides up to 24 dual-speed fiber slots and (4) 10Gig aggregation ports, making it an ideal switch for fiber aggregation applications. Switch features include:

- L2+ features provide better manageability, security, QoS, and performance
- Built-in DMS (Device Management System)
- Guest VLAN, voice VLAN, Port based, tag-based and Protocol based VLANs
- 802.3az Energy Efficient Ethernet standard
- 32K MAC address table and IPv6 / IPv4 Dual stack
- IEEE 802.3ah OAM, IEEE 802.1ag and Y.1731 CFM
- IEEE 1588v2 PTP
- L2/L3/L4 ACLs support MAC ACL, IP standard/extended ACL, 802.1p, Ethernet type
- ITU-T G.8031 Ethernet Linear Protection Switching (EPS)
- ITU-T G.8032 Ethernet Ring Protection Switching (ERPS)

About This Manual

This manual gives specific information on how to operate and use the Web UI management functions of the switch. 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 Http/Https protocols. Note that this manual may include links to third party websites for which Transition Networks is not responsible.

Related Manuals

A printed Quick Start Guide is shipped with each device.

For Transition Networks Drivers, Firmware, etc. go to the Product Support webpage (logon required).

For Transition Networks Manuals, Brochures, Data Sheets, etc. go to the Support Library (no logon required).

For SFP manuals see Transition Networks SFP webpage.

Other related manuals include:

- SM24DP4XA Quick Start Guide, 33768
- SM24DP4XA Install Guide, 33769
- SM24DP4XA Web User Guide, 33770 (this manual)
- SM24DP4XA CLI Reference, 33771
- Release Notes (version specific)

2. Web UI Management

Initial Configuration

This chapter describes how to access, configure, and monitor the switch via any switch port.

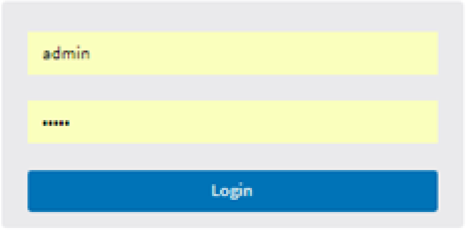
The default IP Address and sub-net mask are:

IP Address: 192.168.1.77
Subnet Mask: 255.255.255.0

The default Username, Password, and Privilege Levels are:

User Name	Password	Privilege Level
admin	admin	15
superuser	superuser	13
administrator	administrator	10
operator	operator	6
readonly	readonly	1

After the switch has been configured you can browse it. Type 192.168.1.77 in the address row of a browser and hit Enter. The Login screen displays prompting you to enter a Username and Password in order to login and access authentication.


admin

•••••

The default username is **admin** and password is **admin**. For the first time to use, please enter the default username and password, and then click the **Login** button. The login process now is completed. In this login menu, you have to input the complete username and password respectively, the switch will not give you a shortcut to username automatically. This looks inconvenient but is safer.

The switch supports a simple web management function allowing only one administrator to configure the system at the same time. If there are two or more users using administrator's identity, it will allow only the one who logs in first to configure the system. Other users, even with administrator rights, can only monitor the system. Those who have no administrator rights can only monitor the system (read only). A maximum of three users can log in simultaneously.

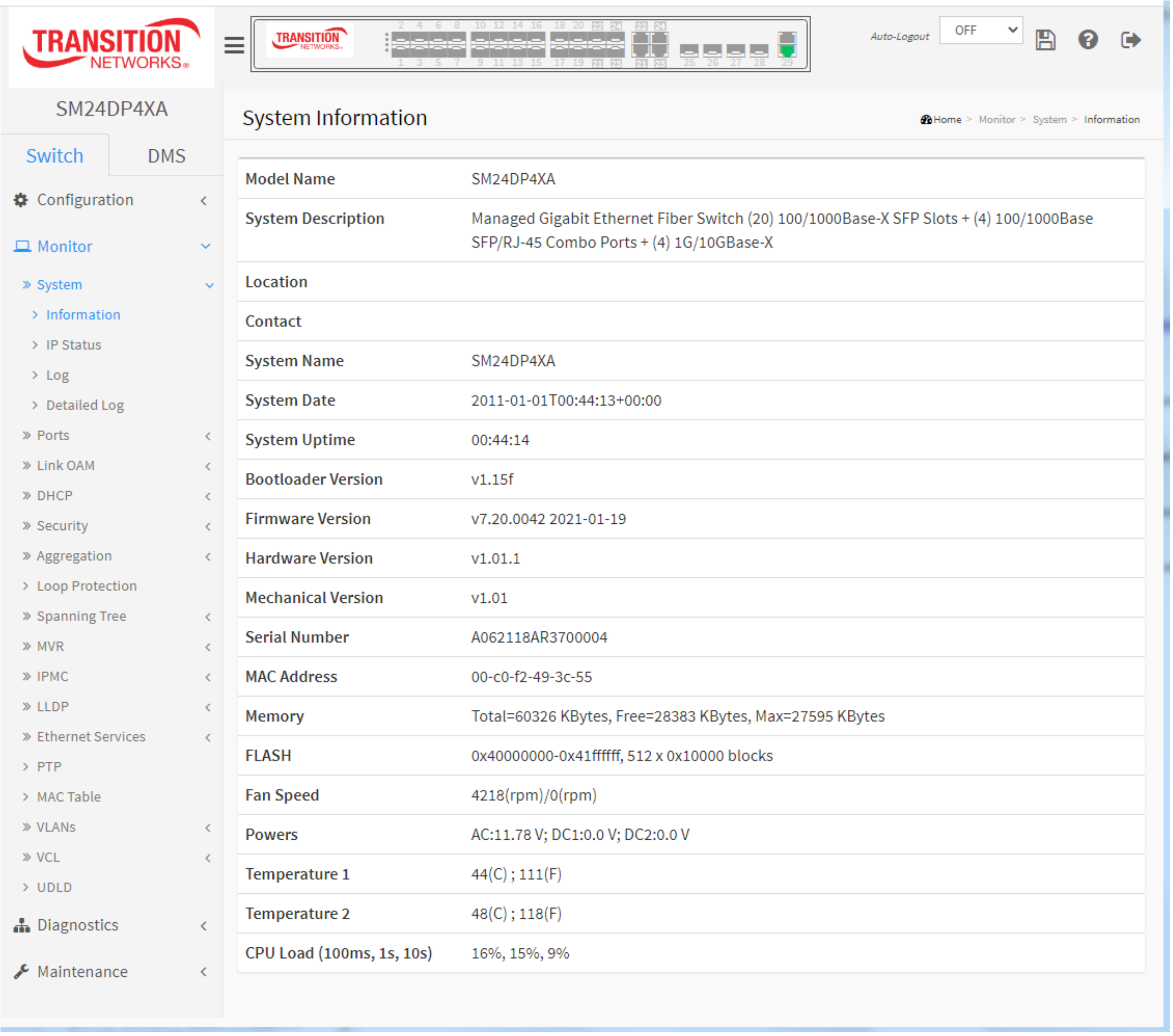
To optimize the display effect, we recommend Microsoft IE 6.0 above, Netscape v7.1 above or Firefox v1.00 above with 1024x768 resolution. The switch supports neutral web browser interface.

Note: The switch can have its IP address assigned by DHCP; If you do not use a DHCP server to provide IP addresses to the switch, use the switch default IP address 192.168.1.77.

Note: To configure function parameters you can click "help" under the web GUI and the switch will pop-up simple help content on how to set the parameters.

Startup Screen

After successful login the startup page displays (Monitor > System > Information):



System Information

Model Name	SM24DP4XA
System Description	Managed Gigabit Ethernet Fiber Switch (20) 100/1000Base-X SFP Slots + (4) 100/1000Base SFP/RJ-45 Combo Ports + (4) 1G/10GBase-X
Location	
Contact	
System Name	SM24DP4XA
System Date	2011-01-01T00:44:13+00:00
System Uptime	00:44:14
Bootloader Version	v1.15f
Firmware Version	v7.20.0042 2021-01-19
Hardware Version	v1.01.1
Mechanical Version	v1.01
Serial Number	A062118AR3700004
MAC Address	00-c0-f2-49-3c-55
Memory	Total=60326 KBytes, Free=28383 KBytes, Max=27595 KBytes
FLASH	0x40000000-0x41ffffff, 512 x 0x10000 blocks
Fan Speed	4218(rpm)/0(rpm)
Powers	AC:11.78 V; DC1:0.0 V; DC2:0.0 V
Temperature 1	44(C) ; 111(F)
Temperature 2	48(C) ; 118(F)
CPU Load (100ms, 1s, 10s)	16%, 15%, 9%

Navigation Icons

The top right side of each web page provides these icons: Auto-Logout OFF ▾ *Click Save Button* 💾 ❓ ⇨

Click Save Button : **Click Save Button**: displays when a page parameter has changed.

💾 : Save to startup-config.

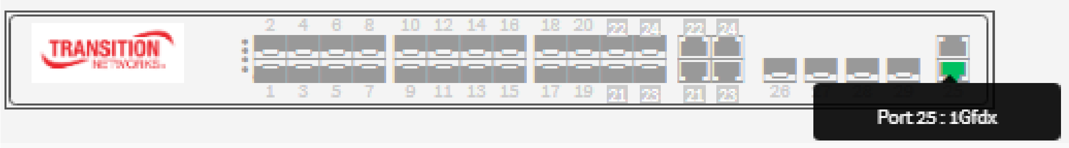
❓ : Display the Help file for this web page.

⇨ : Log out of the system.

Home > Monitor > System > Information : Shows the current menu path in the format Home > Monitor > System > Information or Home > Management > DMS Mode, etc.

☰ : The top left corner icon alternately hides and re-displays the left-hand menus and sub-menus.

Switch icon: Hover the cursor over any port to display its speed (if up) or status (if down):



Port 25 : 1Gfdx

Auto-logout 10 min ▼

: **Auto-logout**: At the dropdown select the Web UI timeout value (1, 2, 3, 4, 5, 10, 20, 30, 40, 50, 60 or OFF). Set to OFF means no automatic Web UI timeout. The default is 10 minutes.

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

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

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

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

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

In summary:

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

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

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

System Configuration

This section describes basic configuration tasks such as System Information, IP, NTP, Time, and Syslog.

2-1 *System*

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

2-1.1 Information

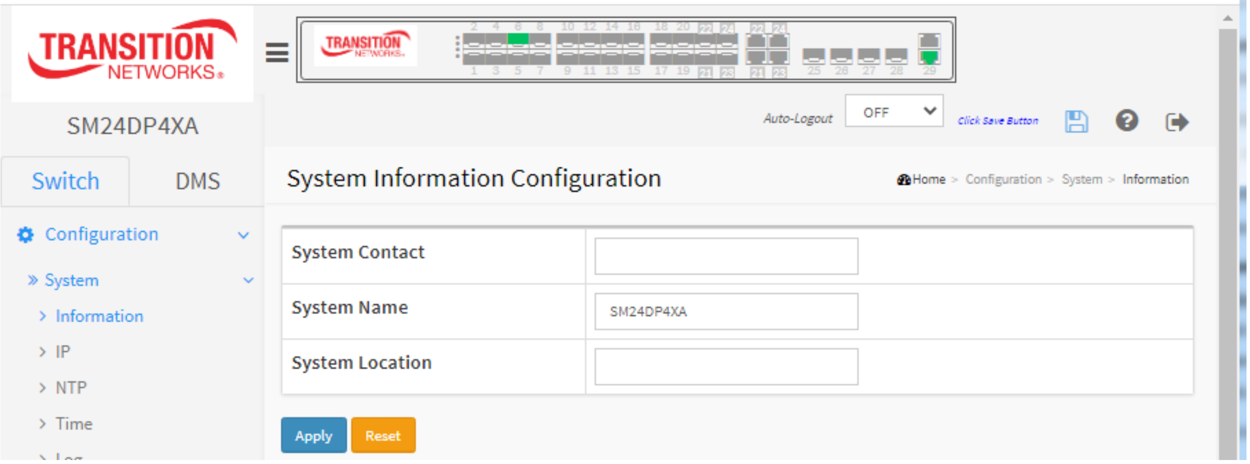
The switch system's contact information is provided here.

Web interface

To configure System Information in the web interface:

1. Click Configuration, System, Information.
2. Enter System Contact, System Name, and System Location information as desired.
3. Click Apply.

Figure 2-1.1: System Information Configuration



System Information Configuration

System Contact	
System Name	SM24DP4XA
System Location	

Parameter descriptions:

System Contact: Enter the contact person and phone number for getting help.

System Name: The model name of this device; the default is *SM24DP4XA*.

System Location: Enter the switch location.

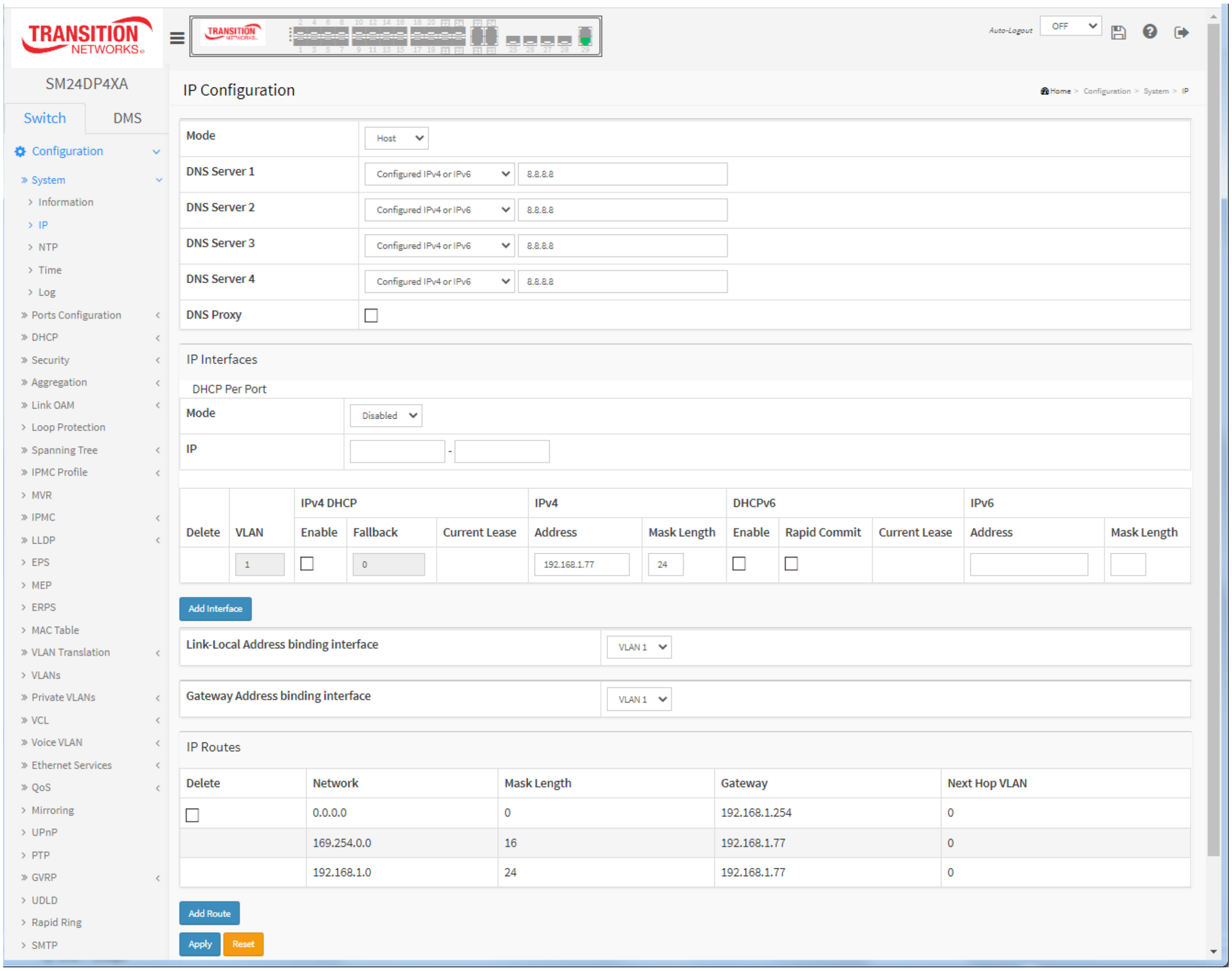
2-1.2 IP

This page lets you configure basic IP parameters and control IP interfaces and IP routes. The switch supports up to 128 interfaces is and up to 32 routes.

To configure an IP address in the web interface:

1. Click Configuration, System, IP.
2. Select the Mode and DNS server(s).
3. Click Add Interface and enter the IP Interfaces.
4. Select Link-Local Address binding interface and Gateway Address binding interface.
5. Click Add Route, enter IP Routes parameters and click Apply.

Figure2-1.2: IP Configuration



IP Configuration

Mode	Host	
DNS Server 1	Configured IPv4 or IPv6	8.8.8.8
DNS Server 2	Configured IPv4 or IPv6	8.8.8.8
DNS Server 3	Configured IPv4 or IPv6	8.8.8.8
DNS Server 4	Configured IPv4 or IPv6	8.8.8.8
DNS Proxy	□	

IP Interfaces

DHCP Per Port

Mode	Disabled
IP	-

Delete	VLAN	IPv4 DHCP			IPv4		DHCPv6			IPv6	
		Enable	Fallback	Current Lease	Address	Mask Length	Enable	Rapid Commit	Current Lease	Address	Mask Length
	1	□	0		192.168.1.77	24	□	□			

Add Interface

Link-Local Address binding interface	VLAN 1

Gateway Address binding interface	VLAN 1

IP Routes

Delete	Network	Mask Length	Gateway	Next Hop VLAN
□	0.0.0.0	0	192.168.1.254	0
	169.254.0.0	16	192.168.1.77	0
	192.168.1.0	24	192.168.1.77	0

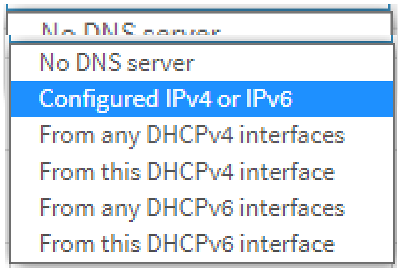
Add Route

Apply Reset

Parameter descriptions:

IP Configuration

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


No DNS server
No DNS server
Configured IPv4 or IPv6
From any DHCPv4 interfaces
From this DHCPv4 interface
From any DHCPv6 interfaces
From this DHCPv6 interface

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

- ***From any DHCPv4 interfaces*** : The first DNS server offered from a DHCPv4 lease to a DHCPv4-enabled interface will be used.
- **Configured IPv4 or IPv6** : Explicitly provide the valid IPv4 unicast address of the DNS Server in dotted decimal notation. Make sure the configured DNS server could be reachable (e.g. via PING) for activating DNS service.
- **From this DHCPv4 interface** : Specify from which DHCPv4-enabled interface a provided DNS server should be preferred.
- **Configured IPv6** : Explicitly provide the valid IPv6 unicast (except linklocal) address of the DNS Server. Make sure the configured DNS server could be reachable (e.g. via PING6) for activating DNS service.
- **From this DHCPv6 interface** : Specify from which DHCPv6-enabled interface a provided DNS server should be preferred.
- **From any DHCPv6 interfaces** : The first DNS server offered from a DHCPv6 lease to a DHCPv6-enabled interface will be used.

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

IP Interfaces

DHCP Per Port Mode: at the dropdown Enable or Disable the DHCP per port function.

DHCP Per Port IP: Enter the IP range for DHCP per port. For more information see Appendix A – DHCP Per Port on page 416.

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

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

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

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

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

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

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

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

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

IPv6 Address: The IPv6 address of the interface. An IPv6 address is in 128-bit records represented as eight fields of up to four hexadecimal digits with a colon separating each field (:). For example, fe80::215:c5ff:fe03:4dc7. The symbol :: is a special syntax that can be used as a shorthand way of representing multiple 16-bit groups of contiguous zeros; but it can appear only once. It can also represent a legally valid IPv4 address. For example, ::192.1.2.34. This field may be left blank if IPv6 operation on the interface is not desired.

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

Link-Local Address binding interface: A link-local address is an IPv6 unicast address that can be automatically configured on an interface using the link-local prefix FE80::/10 (1111 1110 10) and the interface identifier in modified EUI-64 format. See the "Next Hop VLAN" parameter description below.

Link-Local Address binding interface: VLAN 1

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

Gateway Address binding interface: 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 dotted decimal notation or a valid IPv6 notation. A default route can use the value 0.0.0.0or IPv6 :: notation.

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

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

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

Buttons

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

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

Apply: Click to save changes.

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

Messages:

Update success! displays when a config change is successfully applied (saved).

DHCP Per Port IP range (192.168.1.70 - 192.168.1.98) includes interface IP address (192.168.1.77)

DHCP Per Port IP range (192.168.1.90 - 192.168.1.98) is not equal to switch TP port number (1)

'DHCP Interface VLAN ID' must be an integer value between 1 and 4095

Invalid route - address bits outside mask: 0.0.0.77

Update success!
Please refresh this page if IPv6 address is not ready.

The input value 'IPv6 Address' (1.2.3.4)
is not a valid IPv6 address.

The value 'IPv6 Address' (2001:db8::1)
must be a valid IPv6 address in 128-bit records represented as
eight fields of up to four hexadecimal digits with a colon (:) separating
each field.

'IPv6 Mask Length' must be an integer value between 1 and 128

ipv6 – 2001:0db8:85a3:8a2e:0370:7334 – Address conflict

Default route mask length must be zero.

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

2-1.3 NTP

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

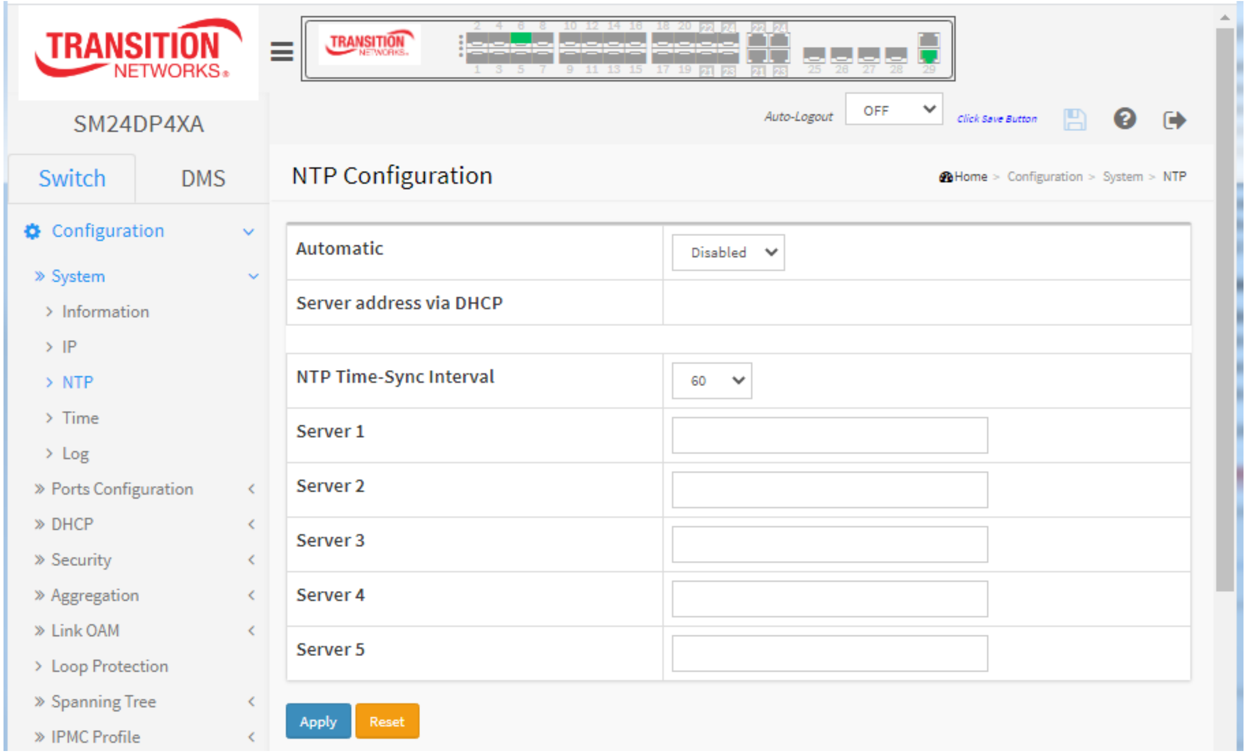
Time Zone is an offset time off GMT. You must select the time zone first and then perform time sync via NTP because the switch will combine this time zone offset and updated NTP time to come out the local time, otherwise, you will not able to get the correct time. The switch supports configurable time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

Web Interface

To configure Time in the web interface:

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

Figure 2-1.3: NTP Configuration



NTP Configuration

Automatic	Disabled
Server address via DHCP	
NTP Time-Sync Interval	60
Server 1	
Server 2	
Server 3	
Server 4	
Server 5	

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.

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

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 5, 10, 15, 30, 60, and 120 minutes.

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

Buttons

Apply : Click to save changes.

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

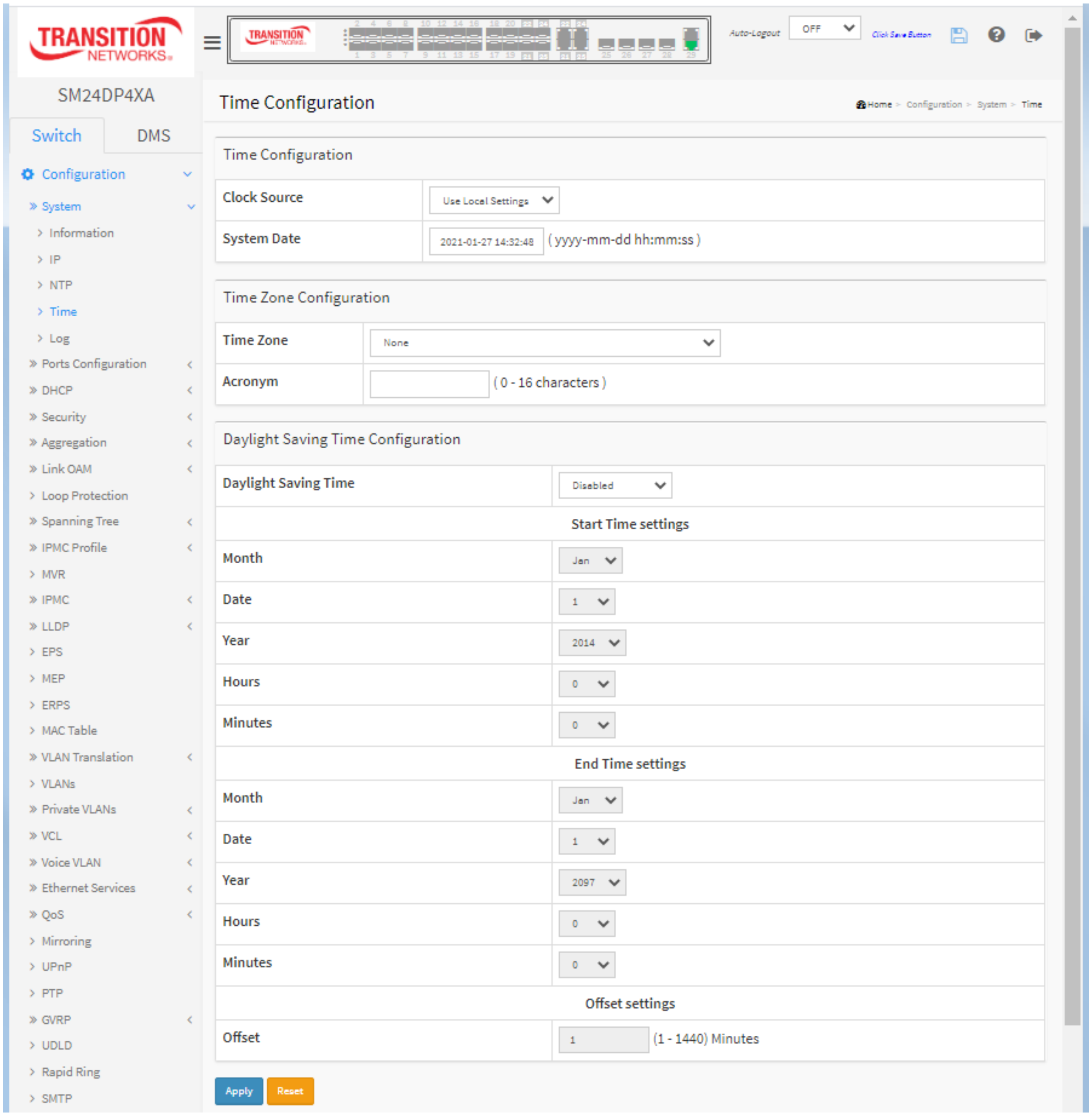
2-1.4 Time

This page lets you set Clock Source (Use Local Settings or Use NTP Server), System Date and Time, Time Zone Configuration, and Daylight Saving Time parameters.

To configure Time via the web interface:

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

Figure 2-1.5: Time Configuration



Time Configuration

Time Configuration

Clock Source	Use Local Settings
System Date	2021-01-27 14:32:48 (yyyy-mm-dd hh:mm:ss)

Time Zone Configuration

Time Zone	None
Acronym	(0 - 16 characters)

Daylight Saving Time Configuration

Daylight Saving Time	Disabled
	Start Time settings
Month	Jan
Date	1
Year	2014
Hours	0
Minutes	0
	End Time settings
Month	Jan
Date	1
Year	2097
Hours	0
Minutes	0
	Offset settings
Offset	1 (1 - 1440) Minutes

Apply Reset

Parameter descriptions:

Time Configuration

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

System Date : Shows the current system date and time in the format yyyy-mm-dd hh:mm:ss. The year entry can be 2011 - 2037.

Time Zone Configuration

Time Zone: Select the time zone where the switch is located.

Acronym: Name the time zone where the switch is located.

Daylight Saving Time Configuration

Daylight Saving: Daylight saving is adopted in some countries. If set, it will adjust the time lag or in advance in unit of hours, according to the starting date and the ending date. For example, if you set the day light saving to be 1 hour. When the time passes over the starting time, the system time will be increased one hour after one minute at the time since it passed over. And when the time passes over the ending time, the system time will be decreased one hour after one minute at the time since it passed over. Provide the Daylight savings type selection. Select “Disable”, “Recurring” or “Non-Recurring” type for Daylight saving type.

Start Time Settings: To configure when Daylight saving start date and time, the format is “YYYY-MM-DD HH:MM”.

End Time Settings: To configure when Daylight saving end date and time, the format is “YYYY-MM-DD HH:MM”.

Offset settings

Offset : Provide the Daylight saving time set offset. The offset is given in minutes east of GMT. The valid range is 1 - 1440 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.

2-1.5 Log

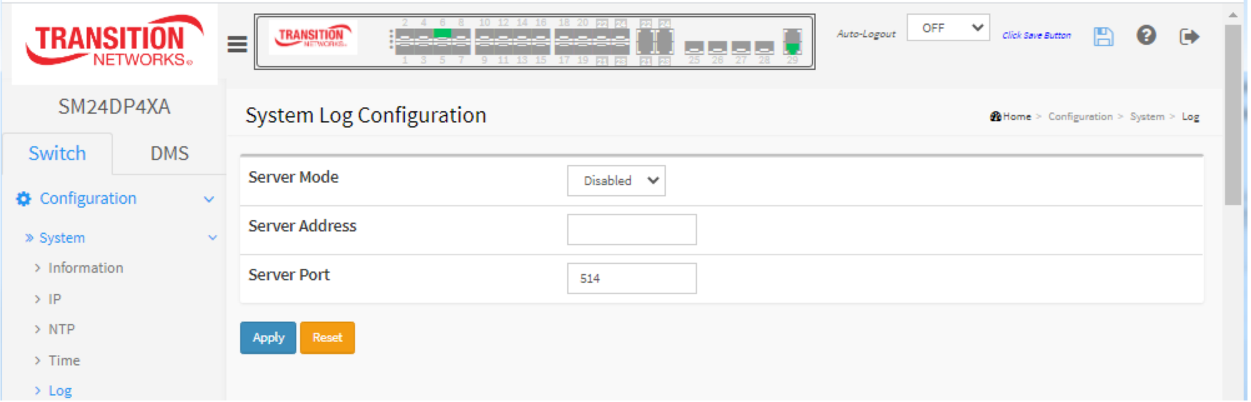
Syslog is a standard for logging program messages . It allows separation of the software that generates messages from the system that stores them and the software that reports and analyzes them. It can be used as well a generalized informational, analysis and debugging messages. It is supported by a 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 include IP Address of Syslog server and Port number.
3. At the Server Mode dropdown, select Enable to enable Syslog.
4. Click Apply.

Figure2- 6.1: System Log configuration



System Log Configuration

Server Mode	Disabled
Server Address	
Server Port	514

Parameter descriptions:

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

Enabled: Enable server mode operation.

Disabled: Disable server mode operation.

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

Server Port : Indicates the service port of syslog server. The valid port range is 1-65535.

2-2 Ports Configuration

2-2.1 Ports

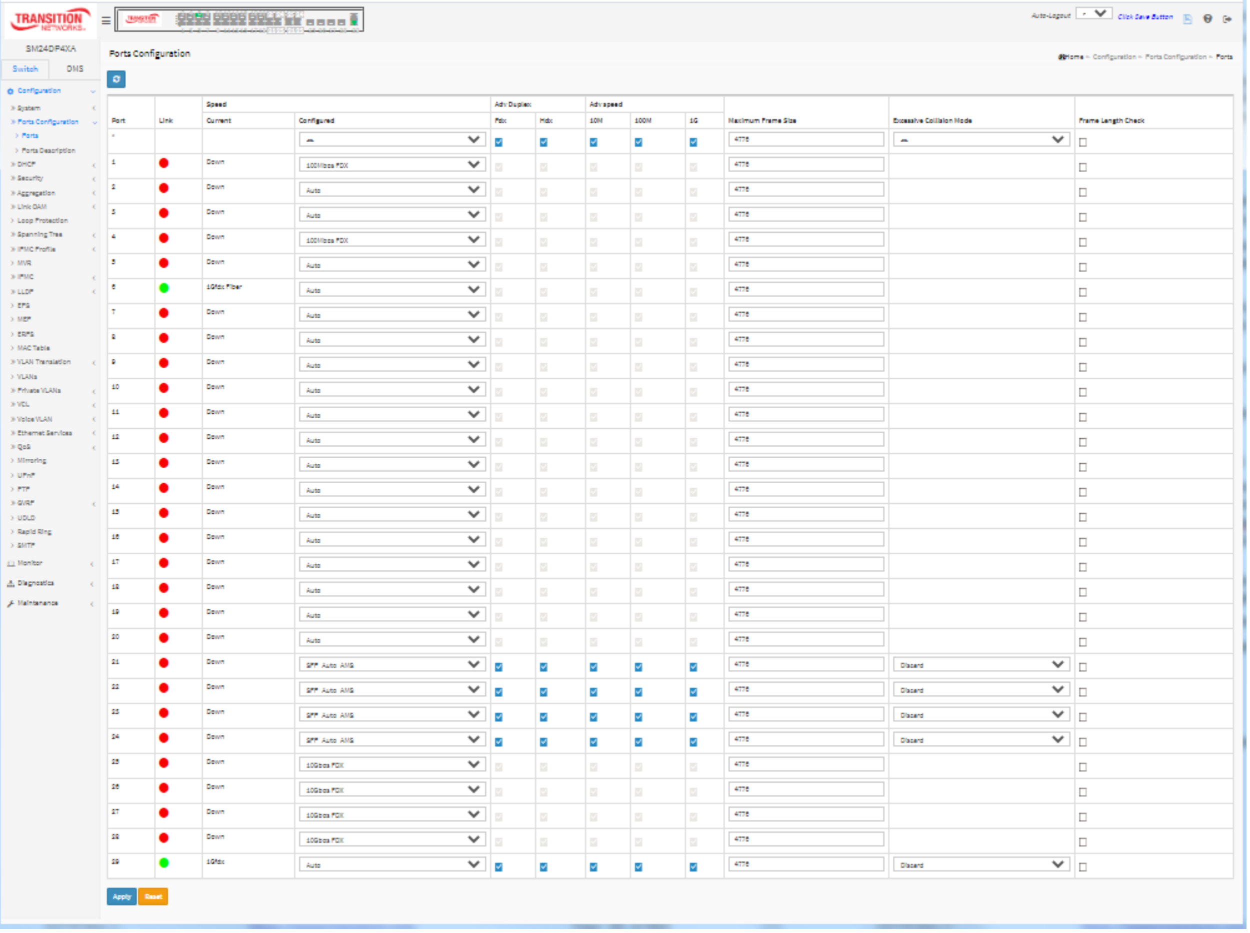
This page lets you configure Port detail parameters of the switch, enable or disable switch ports, and monitor ports content or status.

Web Interface

To configure Port Configuration parameters via the web interface:

1. Click Configuration, Port, then Configuration.
2. Specify Speed, Duplex, Max Frame size, Excessive Collision Mode and Frame Length Check.
3. Click Apply.

Figure 2-2.1: Port Configuration



Ports Configuration

Port	Link	Speed		Adv Duplex		Adv speed			Maximum Frame Size	Excessive Collision Mode	Frame Length Check
		Current	Configured	Fdx	Hdx	10M	100M	1G			
*			<>	☑	☑	☑	☑	☑	4778	<>	□
1	🔴	Down	100Mbps FDX	☑	☑	☑	☑	☑	4778		□
2	🔴	Down	Auto	☑	☑	☑	☑	☑	4778		□
3	🔴	Down	Auto	☑	☑	☑	☑	☑	4778		□
4	🔴	Down	100Mbps FDX	☑	☑	☑	☑	☑	4778		□
5	🔴	Down	Auto	☑	☑	☑	☑	☑	4778		□
6	🟢	1Gfdx Fiber	Auto	☑	☑	☑	☑	☑	4778		□
7	🔴	Down	Auto	☑	☑	☑	☑	☑	4778		□
8	🔴	Down	Auto	☑	☑	☑	☑	☑	4778		□
9	🔴	Down	Auto	☑	☑	☑	☑	☑	4778		□
10	🔴	Down	Auto	☑	☑	☑	☑	☑	4778		□
11	🔴	Down	Auto	☑	☑	☑	☑	☑	4778		□
12	🔴	Down	Auto	☑	☑	☑	☑	☑	4778		□
13	🔴	Down	Auto	☑	☑	☑	☑	☑	4778		□
14	🔴	Down	Auto	☑	☑	☑	☑	☑	4778		□
15	🔴	Down	Auto	☑	☑	☑	☑	☑	4778		□
16	🔴	Down	Auto	☑	☑	☑	☑	☑	4778		□
17	🔴	Down	Auto	☑	☑	☑	☑	☑	4778		□
18	🔴	Down	Auto	☑	☑	☑	☑	☑	4778		□
19	🔴	Down	Auto	☑	☑	☑	☑	☑	4778		□
20	🔴	Down	Auto	☑	☑	☑	☑	☑	4778		□
21	🔴	Down	SFP Auto AMS	☑	☑	☑	☑	☑	4778	Discard	□
22	🔴	Down	SFP Auto AMS	☑	☑	☑	☑	☑	4778	Discard	□
23	🔴	Down	SFP Auto AMS	☑	☑	☑	☑	☑	4778	Discard	□
24	🔴	Down	SFP Auto AMS	☑	☑	☑	☑	☑	4778	Discard	□
25	🔴	Down	10Gbps FDX	☑	☑	☑	☑	☑	4778		□
26	🔴	Down	10Gbps FDX	☑	☑	☑	☑	☑	4778		□
27	🔴	Down	10Gbps FDX	☑	☑	☑	☑	☑	4778		□
28	🔴	Down	10Gbps FDX	☑	☑	☑	☑	☑	4778		□
29	🟢	1Gfdx	Auto	☑	☑	☑	☑	☑	4778	Discard	□

Parameter descriptions:

Port : The logical port number for this row.

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

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

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

Disabled - Disables the switch port operation.

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

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

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

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

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

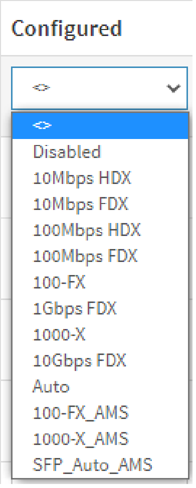
1Gbps FDX : Forces the port in 1Gbps full duplex

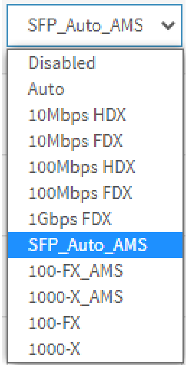
SFP_Auto_AMS : Automatically determines the speed of the SFP. Note: There is no standardized way to do SFP auto detect, so here it is done by reading the SFP ROM. Due to no standardized way of doing SFP auto detect, some SFPs might not be detectable. The port is set in AMS mode. Cu port is set in Auto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

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

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

Ports in AMS mode with 1000-X speed have Copper port preferred.
Ports in AMS mode with 100-FX speed have Fiber port preferred.





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

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

Maximum Frame Size : Enter the maximum frame size allowed for the switch port, including FCS. The valid range is 1518-4776 bytes. The default is 4776 bytes.

Excessive Collision Mode : Configure port transmit collision behavior.

Discard: Discard frame after 16 collisions (default).

Restart: Restart backoff algorithm after 16 collisions.

Frame Length Check : Configures if frames with incorrect frame length in the EtherType/Length field shall be dropped. An Ethernet frame contains a field EtherType which can be used to indicate the frame payload size (in bytes) for values of 1535 and below. If the EtherType/Length field is above 1535, it indicates that the field is used as an EtherType (indicating which protocol is encapsulated in the payload of the frame).

If "frame length check" is enabled, frames with payload size less than 1536 bytes are dropped, if the EtherType/Length field doesn't match the actual payload length.

If "frame length check" is disabled, frames are not dropped due to frame length mismatch.

Note: No drop counters count frames dropped due to frame length mismatch.

Buttons

Apply : Click to save changes.

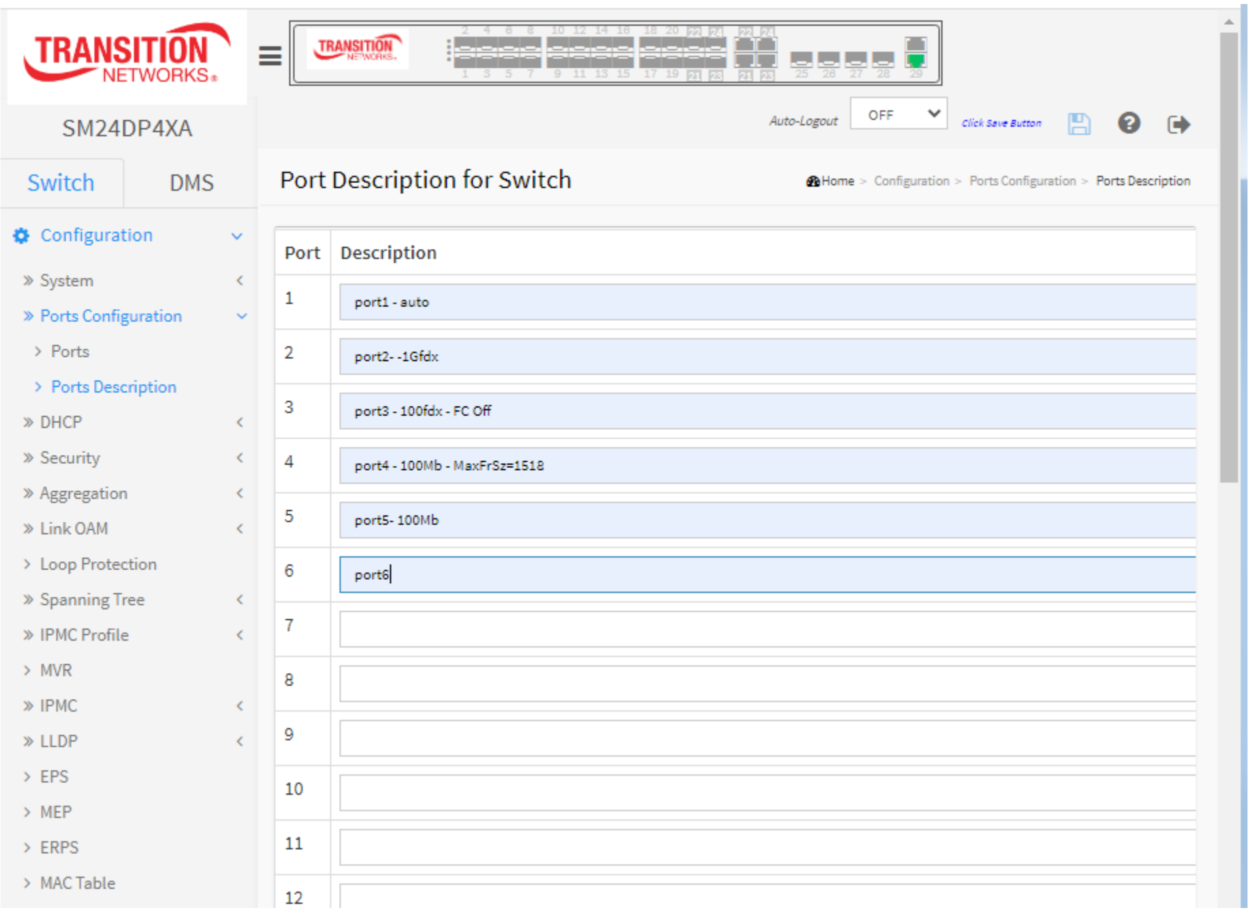
Reset: Click to undo any changes made locally and revert to previously saved values.

Refresh: Click to refresh the Port link Status manually.

2-2.1 Ports Description

This page lets you enter a port description.

Figure 2-2.1: Port Description for Switch



Port Description for Switch

Port	Description
1	port1 - auto
2	port2- -1Gfdx
3	port3 - 100fdx - FC Off
4	port4 - 100Mb - MaxFrSz=1518
5	port5- 100Mb
6	port6
7	
8	
9	
10	
11	
12	

Parameter descriptions:

Port : The logical port number for this row.

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

Buttons

Apply : Click to apply changes.

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

2-3 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.

2-3.1 Server

2-3.1.1 Mode

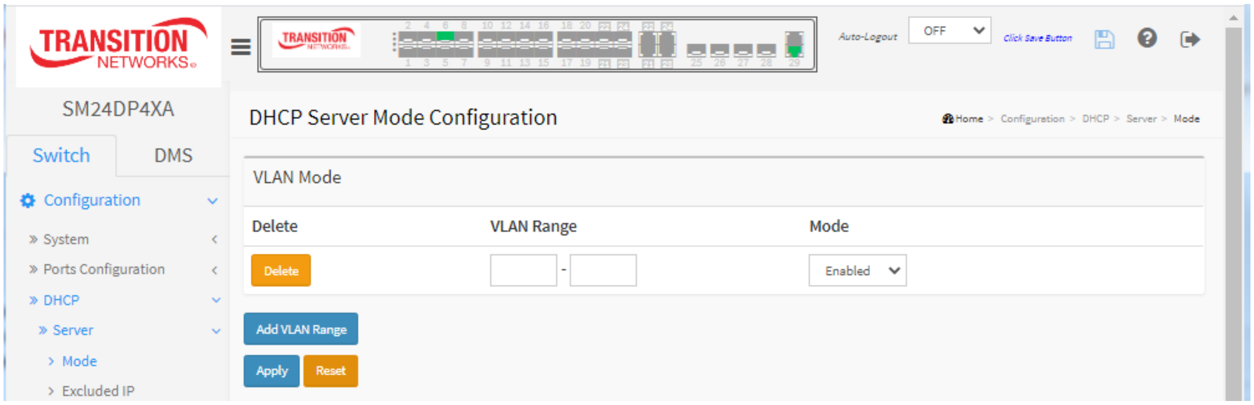
This page configures global mode and VLAN mode to enable/disable DHCP server per system and per VLAN.

Web Interface

To configure DHCP server mode in the web interface:

1. Click Configuration, DHCP, Server, Mode.
2. Click Add VLAN Range.
3. Enter a valid range of VLAN IDs
4. Select “Enabled” at the Mode dropdown.
5. Click Apply.

Figure 2-4.1.1: DHCP Server Mode Configuration



DHCP Server Mode Configuration

VLAN Mode

Delete	VLAN Range	Mode
Delete	-	Enabled

Parameter descriptions:

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 only 1 VLAN ID, then you can enter it into either the first or second VLAN ID or both.

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

1. Click the Add VLAN Range button to add a new VLAN range.
2. Input the VLAN range that you want to disable.
3. At the Mode dropdown select Disabled.
4. Press Apply to apply the change. The disabled VLAN range is removed from the DHCP Server mode configuration page.

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

Enabled: Enable DHCP server per VLAN.

Disabled: Disable DHCP server pre 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.

Note that in order to use DHCP on the SM24DP4XA management port, the default PVLAN config must be changed at Configuration > Private VLANs > Membership.

In order to obtain an address via DHCP, the port must be in PVLAN 1. The SM24DP4XA Management port 29 defaults to no PVLAN for port isolation. If you want to use DHCP on the Management port, you must add it to PVLAN 1 and then create another PVLAN if you need port isolation.

2-3.1.2 Excluded IP

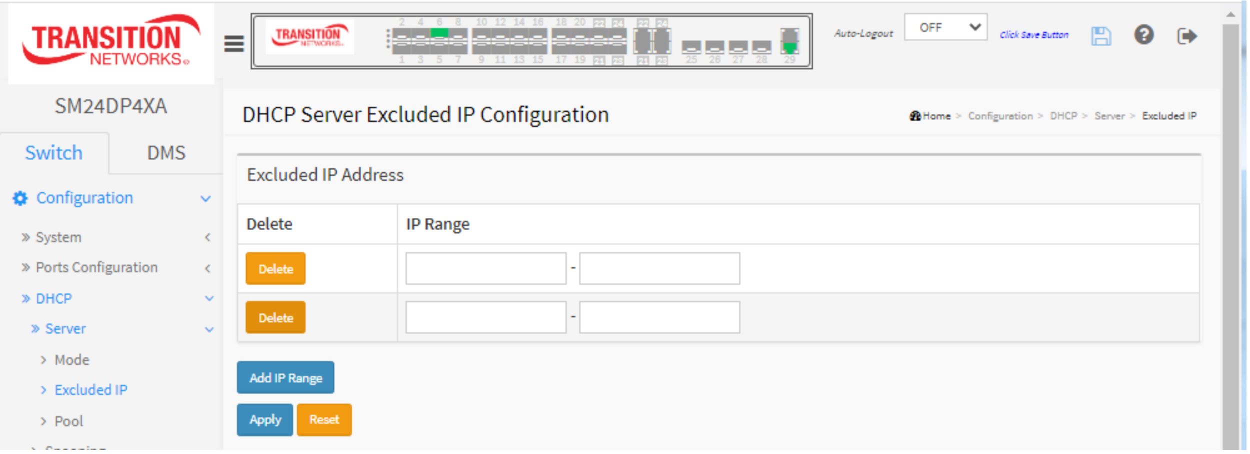
This page lets you configure excluded IP addresses. The DHCP server will not allocate these excluded IP addresses to a DHCP client.

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 2-3.1.2: DHCP Server Excluded IP Configuration



DHCP Server Excluded IP Configuration

Excluded IP Address

Delete	IP Range
Delete	-
Delete	-

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 the first or 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.

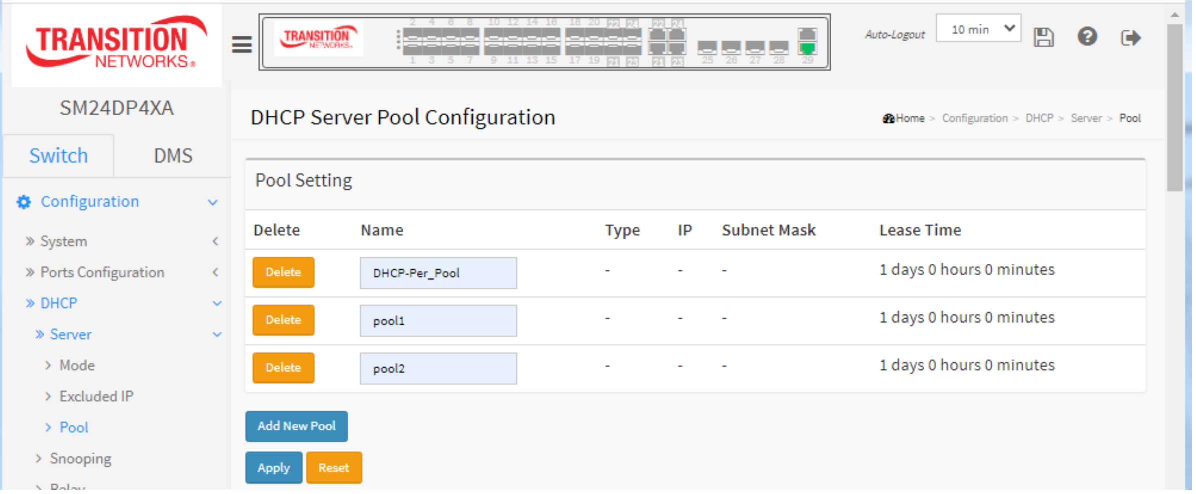
2-3.1.3 Pool

This page lets you manage DHCP pools. Based on the DHCP pool, a DHCP server will allocate IP address and deliver configuration parameters to DHCP client.

To configure DHCP server pool in the web interface:

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

Figure 2-3.1.3: DHCP Server Pool Configuration



DHCP Server Pool Configuration

Pool Setting

Delete	Name	Type	IP	Subnet Mask	Lease Time
Delete	DHCP-Per_Pool	-	-	-	1 days 0 hours 0 minutes
Delete	pool1	-	-	-	1 days 0 hours 0 minutes
Delete	pool2	-	-	-	1 days 0 hours 0 minutes

Parameter descriptions:

<u>**Pool Setting**</u> : 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 : Displays lease time of the pool in days, hours, and minutes.

Buttons

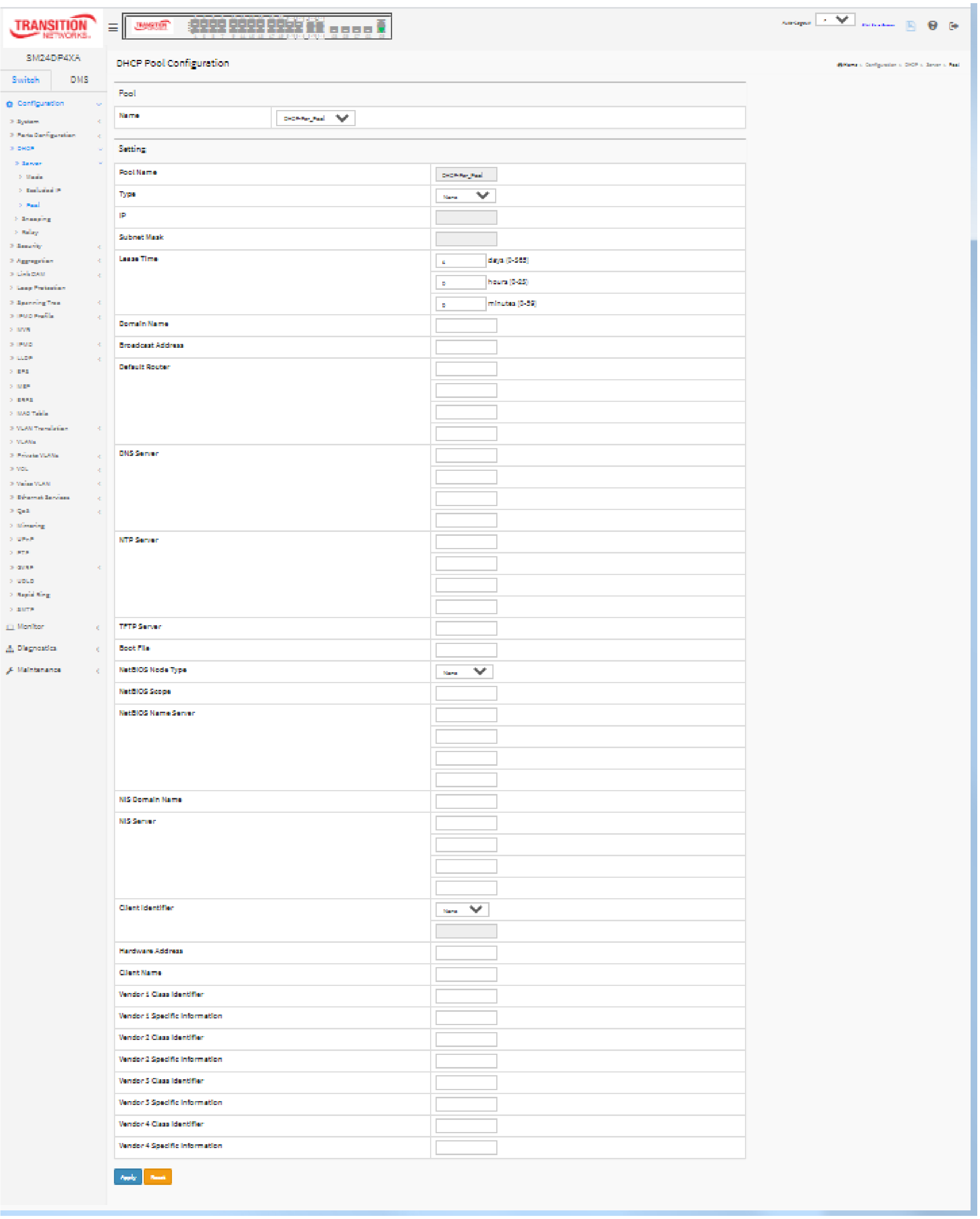
Add New Pool - Click to add a new DHCP pool.

Apply – Click to save changes.

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

DHCP Pool Configuration page

After you click Apply, this page displays to let you configure DHCP Pool parameters.



DHCP Pool Configuration

Pool

Name	DHCPSer_Pool

Setting

Pool Name	DHCPSer_Pool
Type	None
IP	
Subnet Mask	
Lease Time	1 days (0-365) 0 hours (0-23) 0 minutes (0-59)
Domain Name	
Broadcast Address	
Default Router	
DNS Server	
NTP Server	
TFTP Server	
Boot File	
NetBIOS Node Type	None
NetBIOS Scope	
NetBIOS Name Server	
NIS Domain Name	
NIS Server	
Client Identifier	None
Hardware Address	
Client Name	
Vendor 1 Class Identifier	
Vendor 1 Specific Information	
Vendor 2 Class Identifier	
Vendor 2 Specific Information	
Vendor 3 Class Identifier	
Vendor 3 Specific Information	
Vendor 4 Class Identifier	
Vendor 4 Specific Information	

Pool: Select a pool to configure the settings.

Name: Select a pool by pool name.

Setting: Configure pool settings.

Name: Display the selected pool name.

Type: Specify 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.

IP: Specify network number of the DHCP address pool.

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

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

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

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

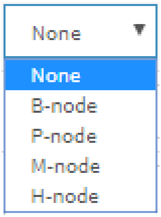
Default Router: DHCP option 3. Specify a list of IP addresses for routers on the client's subnet.

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

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

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

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



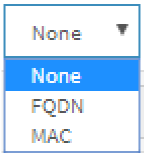
NetBIOS Node Type: DHCP option 46. Specify NetBIOS node type option to allow Netbios over TCP/IP clients which are configurable to be configured as described in RFC 1001/1002.

NetBIOS Scope: DHCP option 47. Specify the NetBIOS over TCP/IP scope parameter for the client as specified in RFC 1001/1002.

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

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

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



Client Identifier: DHCP option 61. Specify client's unique identifier to be used when the pool is the type of host.

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

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

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

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

Buttons

Apply: Click to save changes.

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

2-3.2 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.

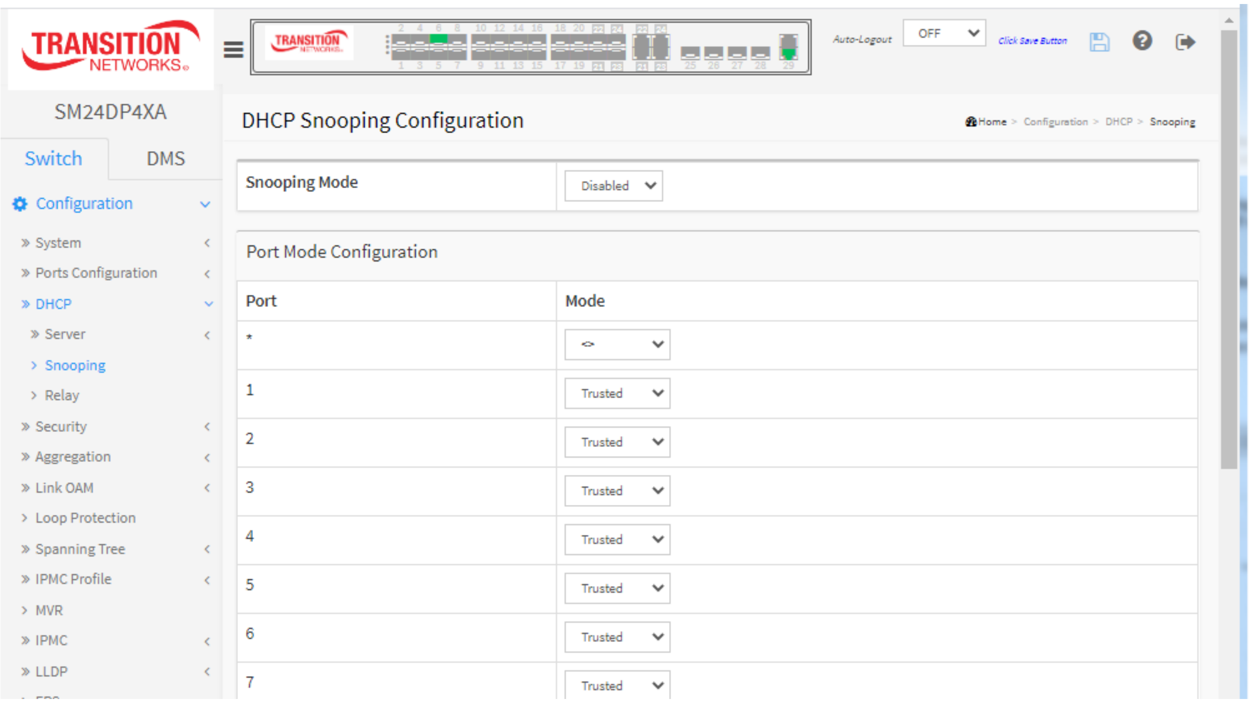
This page lets you configure the DHCP Snooping parameters of the switch. The DHCP Snooping can prevent attackers from adding their own DHCP servers to the network.

Web Interface

To configure DHCP snooping in the web interface:

1. Click Configuration, DHCP, Snooping.
2. Select “Enabled” at the Snooping Mode dropdown.
3. Select “Trusted” of the specific port at the Mode dropdown in the Port Mode Configuration section.
4. Click Apply.

Figure 2-3.2: DHCP Snooping Configuration



DHCP Snooping Configuration

Snooping Mode	Disabled

Port Mode Configuration

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 port modes are:

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

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

Buttons

Apply – Click to save changes.

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

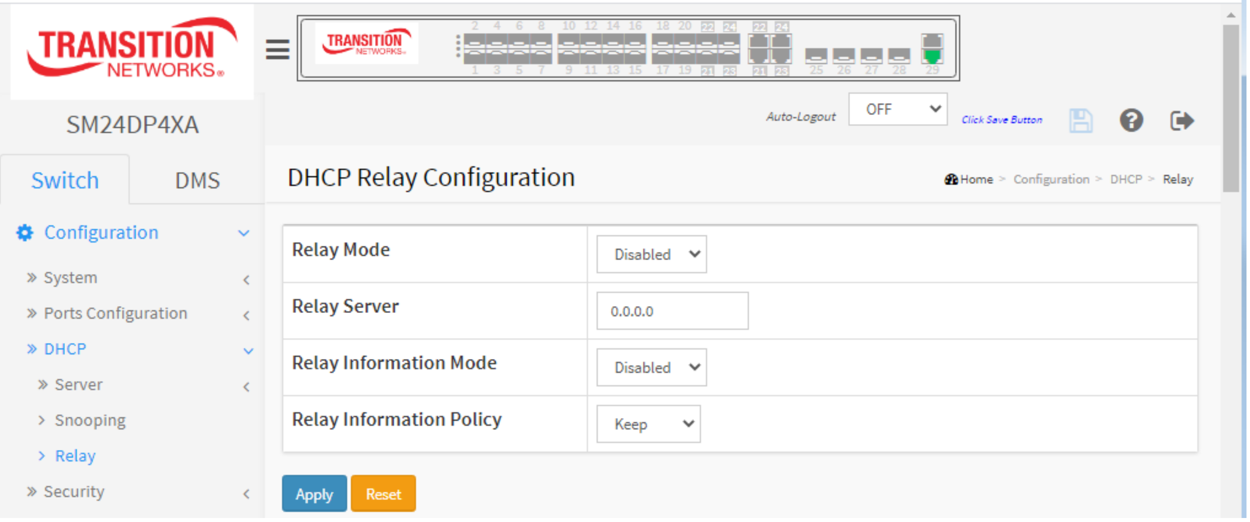
2-3.3 Relay

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.

To configure DHCP Relay in the web interface:

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

Figure 2-3.3: DHCP Relay Configuration



DHCP Relay Configuration

Relay Mode	Disabled
Relay Server	0.0.0.0
Relay Information Mode	Disabled
Relay Information Policy	Keep

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 receive form VLAN ID 3, switch ID 1, port No 8. And the option 82 remote ID value is equal the switch MAC address.

Possible modes are:

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

Disabled: Disable DHCP relay information mode operation.

Relay Information Policy : 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.

2-4 Security

This section lets you configure the switch security settings. You can use the switch security features to restrict input s.

2-4.1 Switch

2-4.1.1 Users

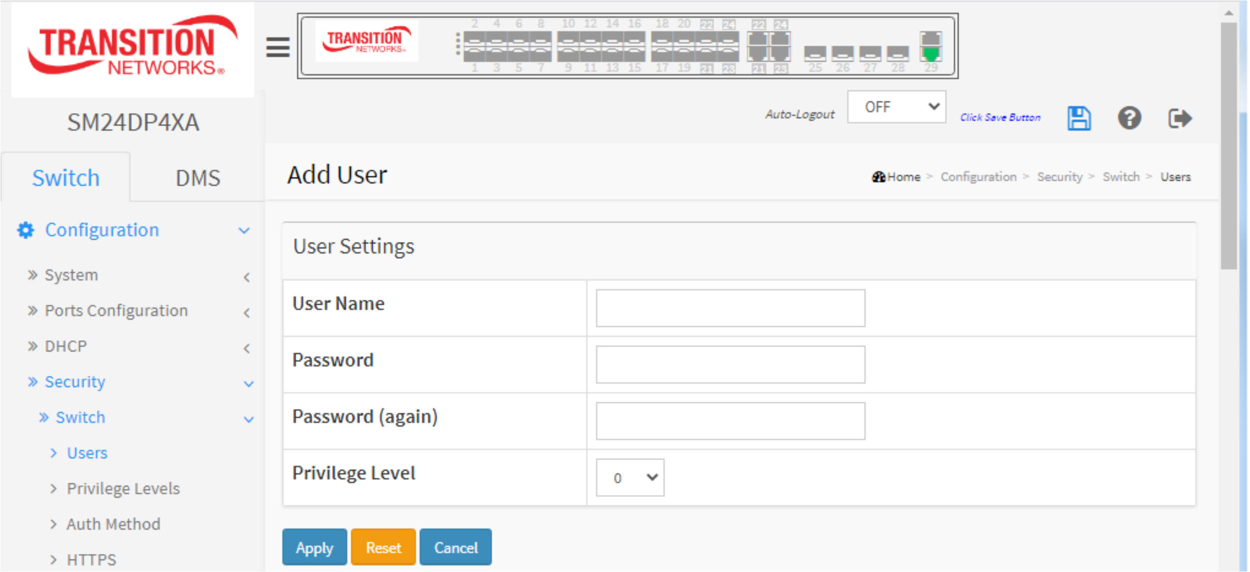
This page provides an overview of the current users. Currently the only way to login as another user on the web server is to close and reopen the browser.

Web Interface

To configure Account in the web interface:

1. Click Configuration, Security, Switch, Users. The default Users Configuration page displays.
2. Click Add New User to display the Add User table.
3. Specify the User Settings parameters.
4. Click Apply.

Figure 2-4.1.1: Add User



Add User

User Settings	
User Name	
Password	
Password (again)	
Privilege Level	0

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 characters and the allowed content is ASCII characters 32 - 126.

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

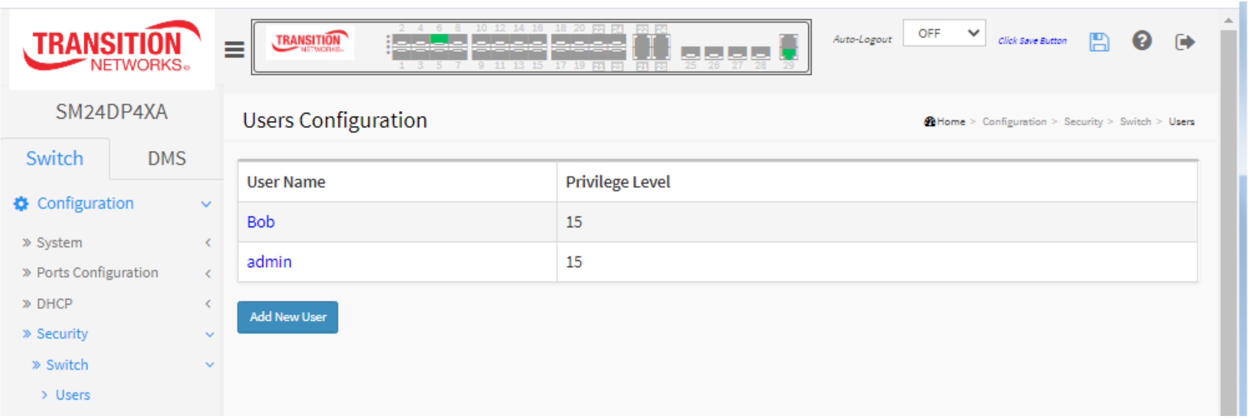
Privilege Level : The privilege level of the user. The allowed range is 0 - 15. If the privilege level value is 15, it can access all groups, i.e. that is granted the fully control of the device. Other values refer to other group privilege level. User's privilege should be same or greater than the group privilege level to have the access of that group. By default, most group's privilege level 5 has the read-only access and privilege level 10 has the read-write access. The system maintenance (software upload, factory defaults and etc.) need user privilege level 15. Generally, privilege level 15 can be used for an administrator account, privilege level 10 for a standard user account and privilege level 5 for a guest account.

Buttons

Add New User: Click to display the Add User table.
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: Delete the current user. This button is not available for new configurations (Add New User).

Edit User Settings

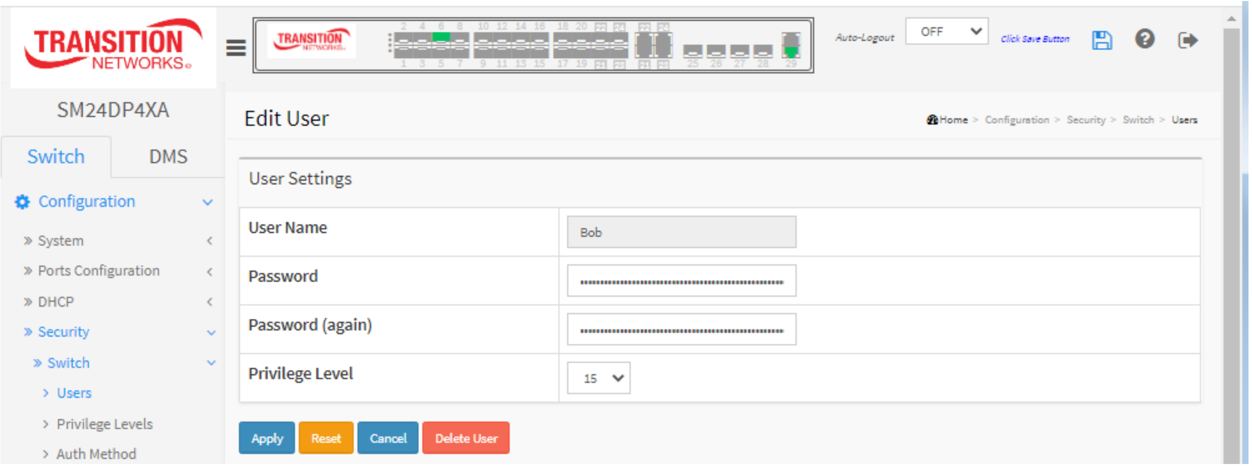
1. Navigate to the Users Configuration page:



Users Configuration

User Name	Privilege Level
Bob	15
admin	15

2. Click a linked User Name to display the Edit User Settings page:



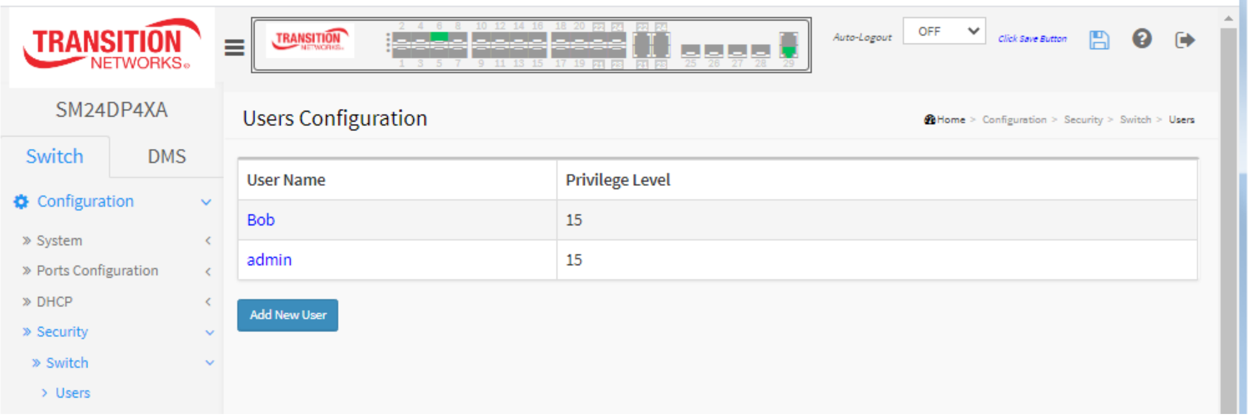
Edit User

User Settings	
User Name	Bob
Password	••
Password (again)	••
Privilege Level	15

3. Edit the Password and Privilege Level parameters.
4. Click the Apply button to save the changes.

Delete a User

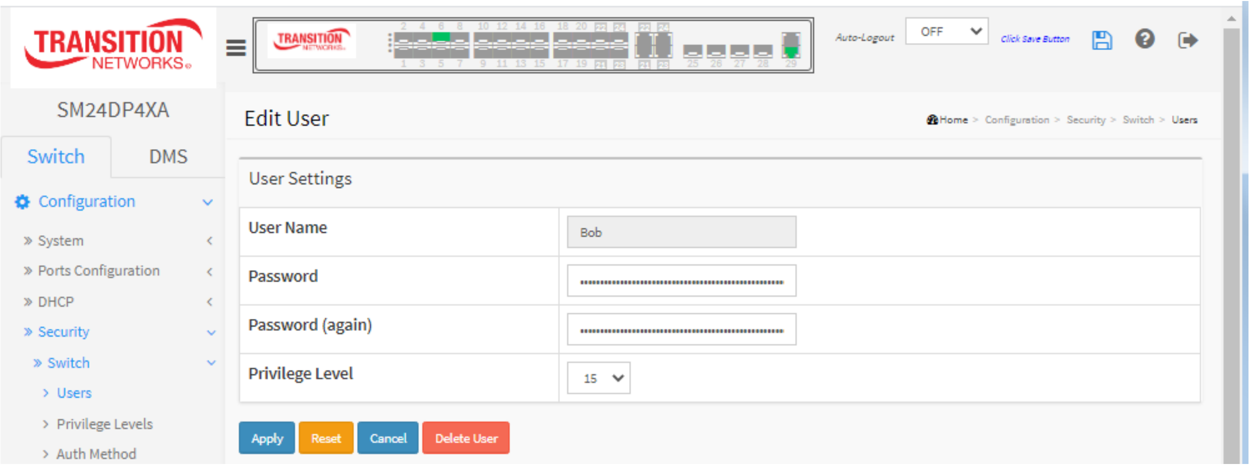
1. Navigate to the Users Configuration page:



Users Configuration

User Name	Privilege Level
Bob	15
admin	15

2. Click a linked User Name to display the Edit User Settings page:



Edit User

User Settings	
User Name	Bob
Password	••
Password (again)	••
Privilege Level	15

3. Click the Delete User button.

4. At the confirmation prompt click the OK button to delete the user.

2-4.1.2 Privilege Levels

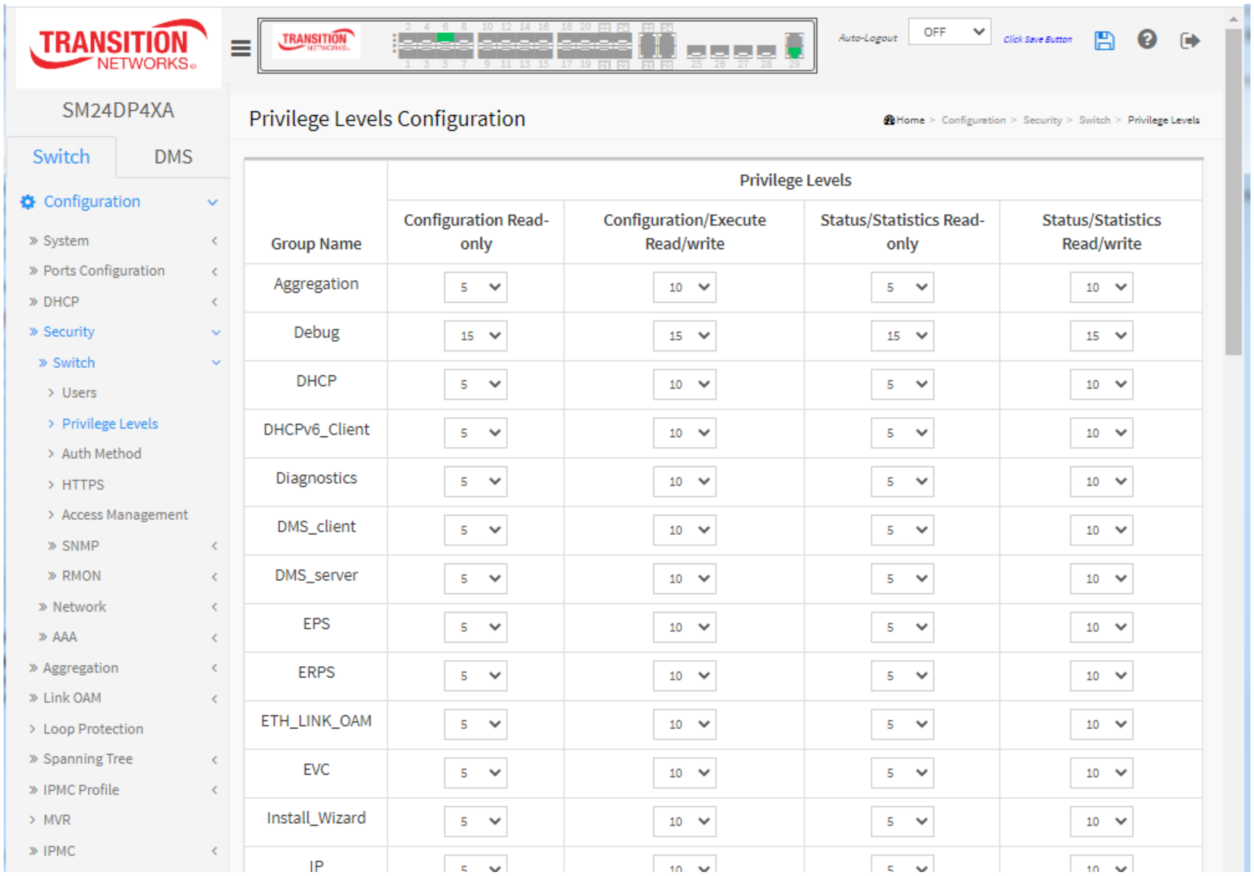
This page provides an overview of the privilege levels. The Group Privilege Levels are:

CRO (Configuration Read-only),
CRW (Configuration/Execute Read/write),
SRO (Status/Statistics Read-only) and
SRW (Status/Statistics Read/write).

To configure Privilege Levels via the web UI:

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

Figure2-4.1.2: Privilege Levels Configuration



Privilege Levels Configuration

	Privilege Levels			
Group Name	Configuration Read-only	Configuration/Execute Read/write	Status/Statistics Read-only	Status/Statistics Read/write
Aggregation	5	10	5	10
Debug	15	15	15	15
DHCP	5	10	5	10
DHCPv6_Client	5	10	5	10
Diagnostics	5	10	5	10
DMS_client	5	10	5	10
DMS_server	5	10	5	10
EPS	5	10	5	10
ERPS	5	10	5	10
ETH_LINK_OAM	5	10	5	10
EVC	5	10	5	10
Install_Wizard	5	10	5	10
IP	5	10	5	10

Parameter descriptions:

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

> ***System***: Contact, Name, Location, Timezone, Daylight Saving Time, Log.
>
> ***Security***: Authentication, System Access Management, Port (contains Dot1x port, MAC based and the MAC Address Limit), ACL, HTTPS, SSH, ARP Inspection and IP source guard.
>
> ***IP***: Everything except 'ping'.
>
> ***Port***: Everything except Cable Diagnostics.

Diagnostics: 'ping' and Cable Diagnostics.

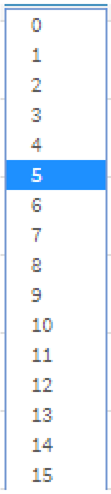
Maintenance: CLI- System Reboot, System Restore Default, System Password, Configuration Save, Configuration Load and Firmware Load. Web- Users, Privilege Levels and everything in Maintenance.

Debug: Only present in CLI.

Privilege Levels : Every group has an authorization Privilege level for these sub groups:

CRO (Configuration Read-only), **CRW** (Configuration/Execute Read/write), **SRO** (Status/Statistics Read-only) and **SRW** (Status/Statistics Read/write).

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.

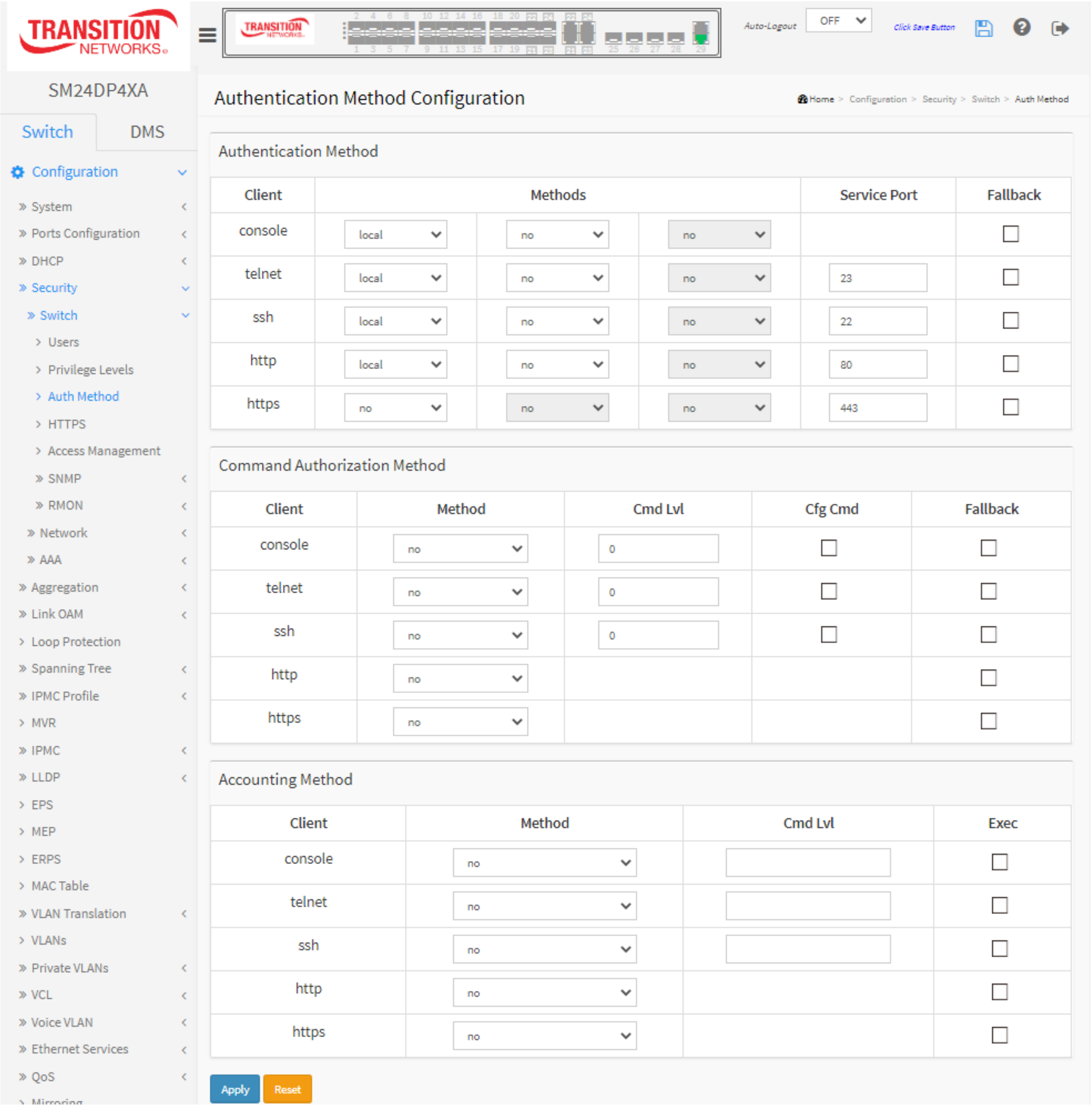
Reset - Click to undo any changes made locally and revert to previously saved values.

2-4.1.3 Authentication Method

This page lets you configure how a user is authenticated when they log in to the switch via one of the management client interfaces. To configure Authentication Method Configuration via the web UI:

1. Click Configuration, Security, Switch, Auth Method.
2. Specify which Clients (console, telnet, ssh, web) you want to monitor.
3. Set Authentication Method, Command Authorization Method, and Accounting Method parameters.
4. Check Fallback.
5. Click Apply.

Figure 2-4.1.3: Authentication Method Configuration



Authentication Method Configuration

Authentication Method

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

Command Authorization Method

Client	Method	Cmd Lvl	Cfg Cmd	Fallback
console	no	0	□	□
telnet	no	0	□	□
ssh	no	0	□	□
http	no			□
https	no			□

Accounting Method

Client	Method	Cmd Lvl	Exec
console	no		□
telnet	no		□
ssh	no		□
http	no		□
https	no		□

Parameter descriptions:

Authentication Method: The Authentication Method section allows you configure how a user is authenticated when he logs into the switch via one of the management client interfaces.

Client : The management client for which the configuration below applies. The set of Clients (console, telnet, ssh, http, and https) can be set to no, local, radius, or tacacs. The http client has an additional selection (redirect) which automatically changes http authentication to https (HTTPS Redirect).

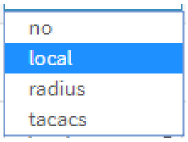
Authentication Methods : Authentication Method can be set to one of the following values:

none : authentication is disabled and login is not possible.

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

radius : use a remote RADIUS server for authentication.

tacacs+ : use a remote TACACS+ server for authentication.



Service Port : The TCP port for each client service. The valid port number is 1 ~ 65534.

Fallback : Enable fallback to local authentication by checking this box. If none of the configured authentication servers are alive, the local user database is used for authentication. This is only possible if the Authentication Method is set to a value other than 'none' or 'local'.

Command Authorization Method: The Command Authorization Method section lets you limit the CLI commands available to a user.

Client : The management client for which the configuration below applies.

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

no: Command authorization is disabled. User is granted access to CLI commands according to their privilege level.
tacacs: Use remote TACACS+ server(s) for command authorization. If all remote servers are offline, the user is granted access to CLI commands according to their privilege level.

Cmd Lvl : Authorize all commands with a privilege level higher than or equal to this level. Valid values are 0 - 15.

Cfg Cmd : Authorize configuration commands.

Accounting Method: The Accounting Method section lets you configure command and exec (login) accounting.

Client : The management client for which the configuration below applies.

Client : Method can be set to one of the following values:

no: Accounting is disabled.
tacacs: Use remote TACACS+ server(s) for accounting.

Cmd Lvl : Enable accounting of all commands with a privilege level higher than or equal to this level. Valid values are 0 - 15. Leave the field empty to disable command accounting.

Exec : Enable executive (login) accounting.

Buttons:

Apply – Click to save changes.

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

2-4.1.4 HTTPs

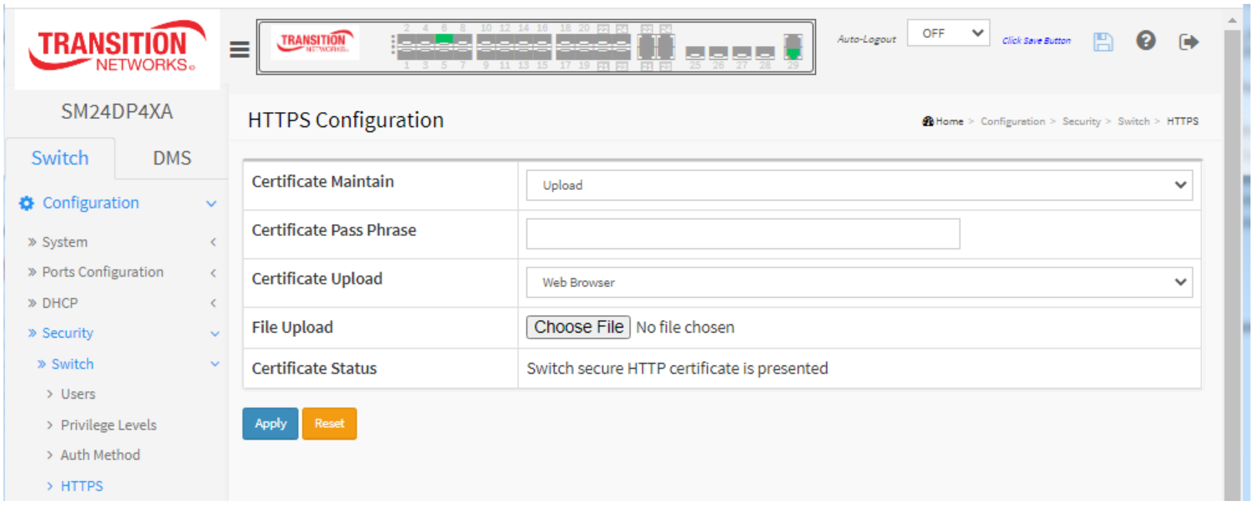
This page lets you set HTTPS parameters and maintain the current certificate on the switch. HTTPS is a secure communication protocol that combines authentication and data encryption to provide secure encrypted communication via the web browser.

Web Interface

To configure a HTTPS Configuration in the web interface:

1. Click Configuration, Security, Switch, HTTPS
2. Select a "Certificate Maintain" parameter.
3. Enter a "Certificate Pass Phrase".
4. Select a "Certificate Upload" method.
5. Choose a file to upload.
6. Click Apply and view the Certificate Status displayed.

Figure 2-4.1.5: HTTPS Configuration



HTTPS Configuration

Certificate Maintain	Upload
Certificate Pass Phrase	
Certificate Upload	Web Browser
File Upload	Choose File No file chosen
Certificate Status	Switch secure HTTP certificate is presented

Parameter descriptions:

Certificate Maintain : This field only can be configured when HTTPS is disabled. It is used to maintain the certification. Possible actions are:

> ***Upload***: To upload certification, there are two kind of upload method can be selected: Web Browser or URL.
>
> ***Generate***: To generate certification.

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

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

Possible Certificate Upload 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 the desired file to upload.

Certificate Status : Display the current status of certificate on the switch. Possible statuses are:

Switch secure HTTP certificate is presented: The certification is stored in HTTPS' database.

Switch secure HTTP certificate is not presented: No certification is stored in HTTPS' database.

Switch secure HTTP certificate is generating ...: The certification is generating.

Buttons

Apply : Click to save changes.

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

2-4.1.6 Access Management

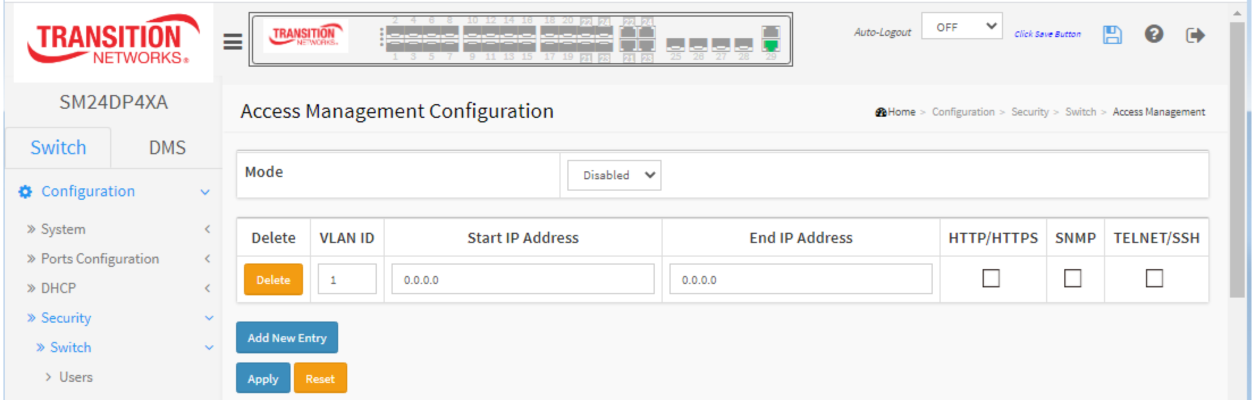
This section lets you configure access management table of the Switch including HTTP/HTTPS, SNMP, and TELNET/SSH. You can manage the Switch over an Ethernet LAN, or over the Internet.

Web Interface

To configure Access Management via the web interface:

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

Figure 2-4.1.6: Access Management Configuration



Access Management Configuration

Mode	Disabled

Delete	VLAN ID	Start IP Address	End IP Address	HTTP/HTTPS	SNMP	TELNET/SSH
Delete	1	0.0.0.0	0.0.0.0	□	□	□

Parameter descriptions:

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

> ***Enabled***: Enable access management mode operation.
>
> ***Disabled***: Disable access management mode operation.

Delete : Check to delete the entry.

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

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.

2-4.1.7 SNMP

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

The SNMP module is passive except for issuing trap information. The switch lets you turn the SNMP agent on (Enable) or off (Disable). If you set the field SNMP to “Enable”, the SNMP agent will start up. All supported MIB OIDs, including RMON MIB, can be accessed via SNMP manager. If the field 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.

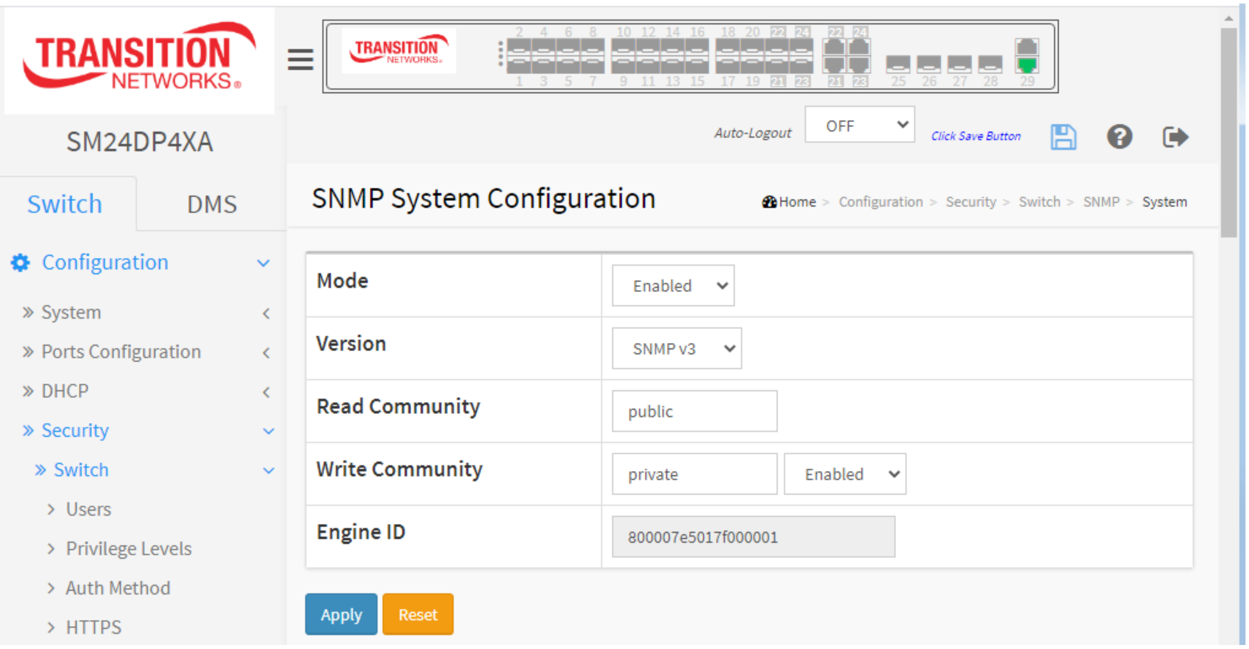
2-4.1.7.1 System

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

Web Interface

To configure SNMP System in the web interface:

1. Click Configuration, SNMP, System.
2. At the Mode dropdown select Enabled.
3. Specify the Version, Read Community, Write Community, and Engine ID.
4. Click Apply.



SNMP System Configuration

Mode	Enabled
Version	SNMP v3
Read Community	public
Write Community	private Enabled
Engine ID	800007e5017f000001

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 – 255 characters, and the allowed content is the ASCII characters 33 - 126.

This 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. SNMPv3 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 - 255 characters, and the allowed content is the ASCII characters 33 to 126.

Enabled: Enable SNMP write community operation.

Disabled: Disable SNMP write community operation.

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.

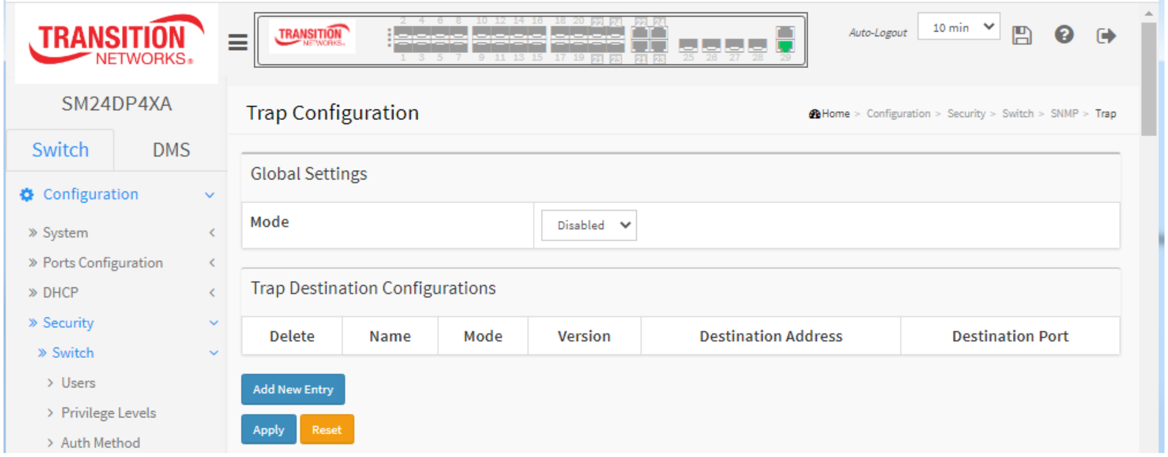
2-4.1.7.2 Trap

Configure SNMP traps on this page.

Web Interface

To configure SNMP Traps via the web interface:

1. Click Configuration, Security, Switch, SNMP, Trap to display the Trap Configuration page:



Trap Configuration

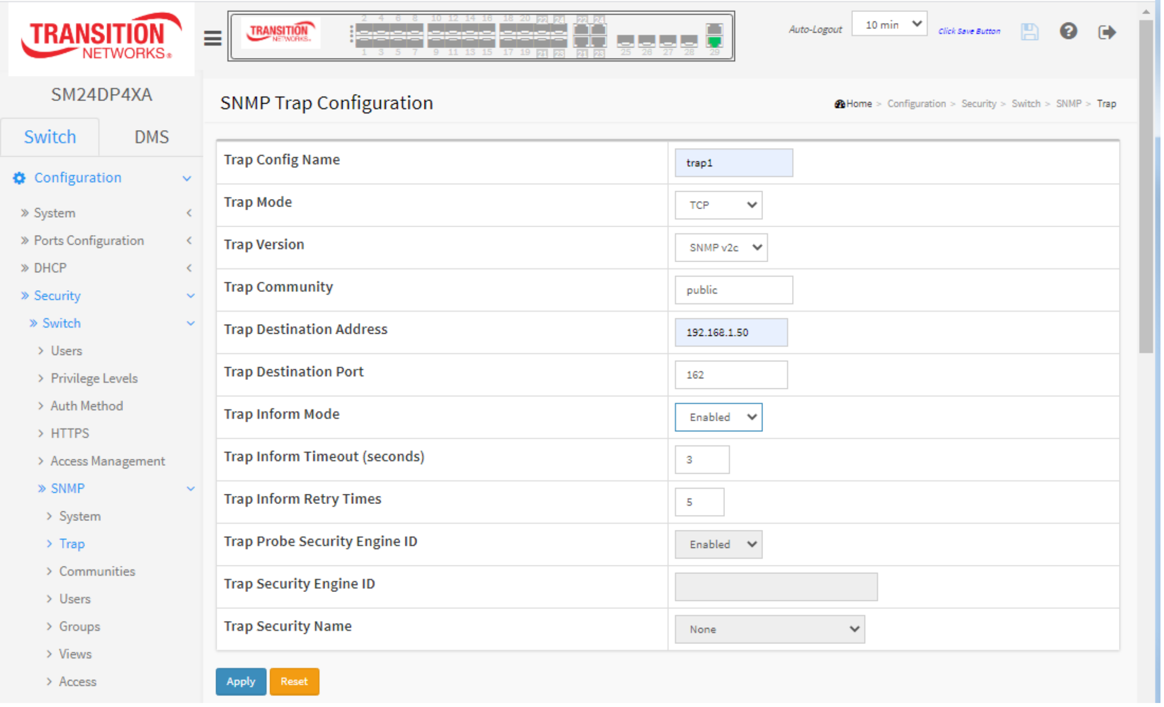
Global Settings

Mode	Disabled

Trap Destination Configurations

Delete	Name	Mode	Version	Destination Address	Destination Port

2. At the Mode dropdown select Enabled and click the Add New Entry button to display the SNMP Trap Configuration page.



SNMP Trap Configuration

Trap Config Name	trap1
Trap Mode	TCP
Trap Version	SNMP v2c
Trap Community	public
Trap Destination Address	192.168.1.50
Trap Destination Port	162
Trap Inform Mode	Enabled
Trap Inform Timeout (seconds)	3
Trap Inform Retry Times	5
Trap Probe Security Engine ID	Enabled
Trap Security Engine ID	
Trap Security Name	None

3. Enter the SNMP Trap Configuration parameters.
4. Click the Apply button.

Parameter descriptions:

Trap Config Name Enter the trap Configuration's name (the trap destination's name). The allowed string length is 1 – 32 characters, and the allowed content is ASCII characters 33 - 126.

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

Disabled: Disable SNMP trap mode operation (default).

UDP: Enable UDP SNMP trap mode operation.

TCP: Enable TCP SNMP trap mode operation.

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

SNMPv1: Set SNMP trap support to SNMP version 1.

SNMPv2c: Set SNMP trap support to SNMP version 2c (default).

SNMPv3: Set SNMP trap support to SNMP version 3.

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

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

This field also allows a valid hostname. A valid hostname is a string using the alphabet (A-Za-z), digits (0-9), dot (.), and dash (-) characters. 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.

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

Trap Destination Port : Indicates the SNMP trap destination port. SNMP Agent will send SNMP message via this port, the port range is 1~65535. The default is port 162.

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 (default).

Trap Inform Timeout (seconds): Indicates the SNMP trap inform timeout. The allowed range is 0 to 2147. The default is 3.

Trap Inform Retry Times: Indicates the SNMP trap inform retry times. The allowed range is 0 to 255. The default is 5.

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

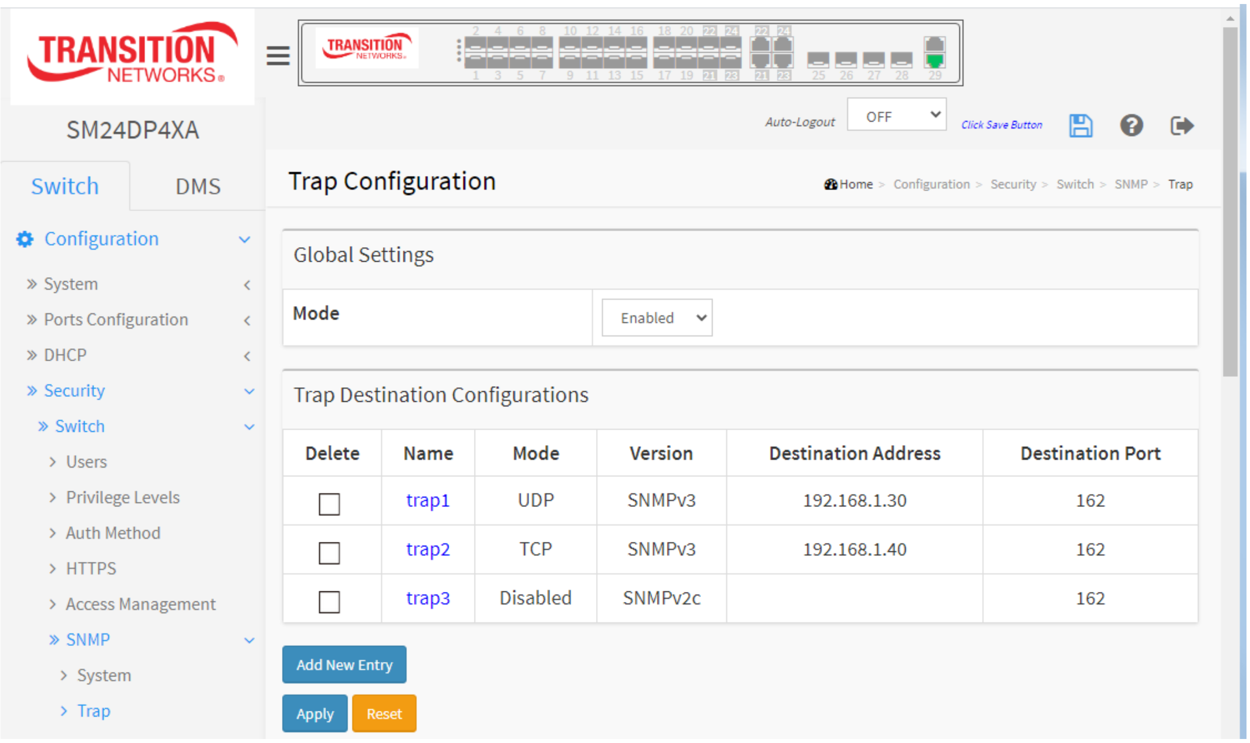
Enabled: Enable SNMP trap probe security engine ID mode of operation.

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.

After you have entered SNMP Trap Configuration parameters and have clicked the Apply button, the Trap Configuration page displays again.



Auto-Logout: OFF

Trap Configuration

Global Settings

Mode: Enabled

Trap Destination Configurations

Delete	Name	Mode	Version	Destination Address	Destination Port
□	trap1	UDP	SNMPv3	192.168.1.30	162
□	trap2	TCP	SNMPv3	192.168.1.40	162
□	trap3	Disabled	SNMPv2c		162

You can click the linked Name entry to display its SNMP Trap Configuration page again in case you want to make changes.

Buttons

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

Apply : Click to save changes.

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

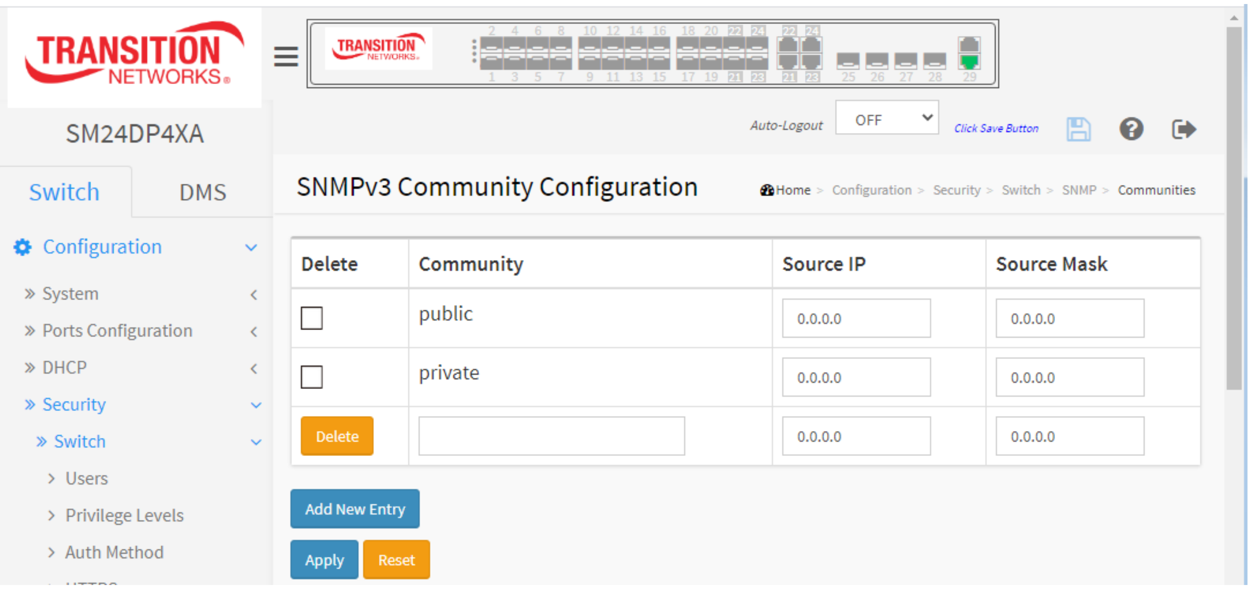
2-4.1.7.3 **Communities**

This page lets you configure SNMPv3 communities. The Community and User Name are unique.
To create a new community account, click the Add New Entry button, enter the account information, and then click Apply. The maximum number of Communities supported is 4.

To configure SNMP Communities via the web UI:

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

Figure 2-4.1.7.3: SNMPv3 Communities Security Configuration



SNMPv3 Community Configuration

Delete	Community	Source IP	Source Mask
□	public	0.0.0.0	0.0.0.0
□	private	0.0.0.0	0.0.0.0
Delete		0.0.0.0	0.0.0.0

Parameter descriptions:

Delete : Check to delete the entry.

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

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

Source Mask : Indicates the SNMP access source address mask.

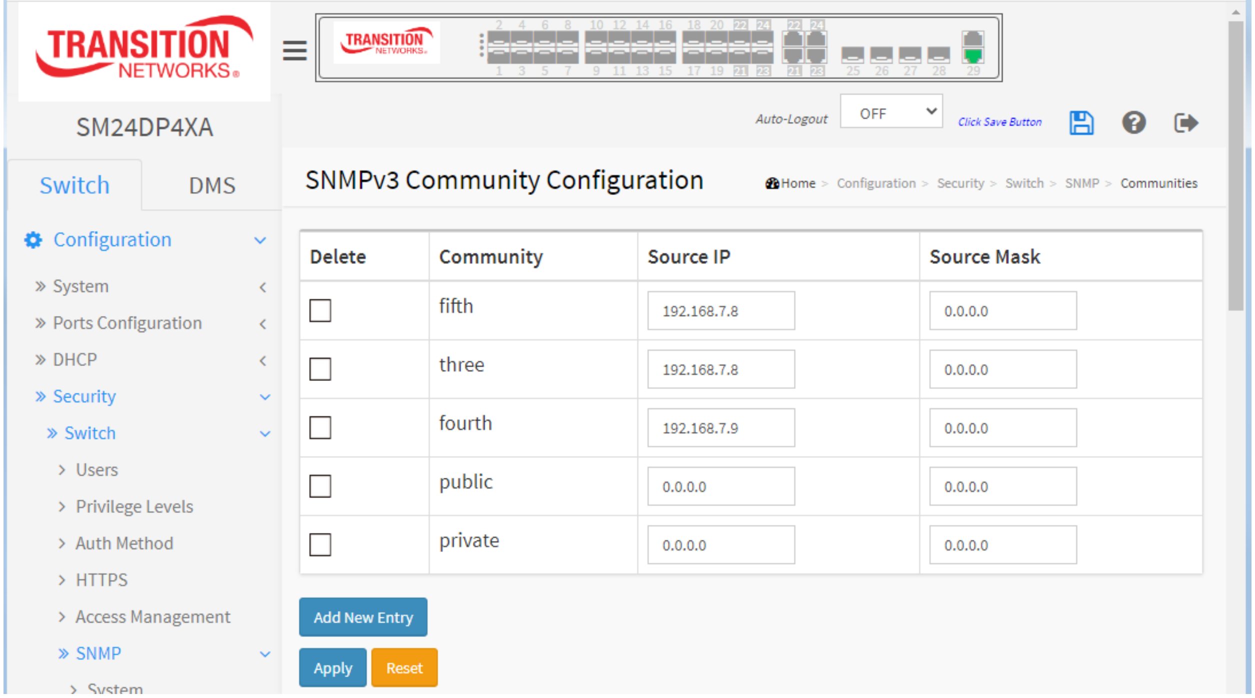
Buttons

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

Apply : Click to save changes.

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

Example:



SNMPv3 Community Configuration

Delete	Community	Source IP	Source Mask
□	fifth	192.168.7.8	0.0.0.0
□	three	192.168.7.8	0.0.0.0
□	fourth	192.168.7.9	0.0.0.0
□	public	0.0.0.0	0.0.0.0
□	private	0.0.0.0	0.0.0.0

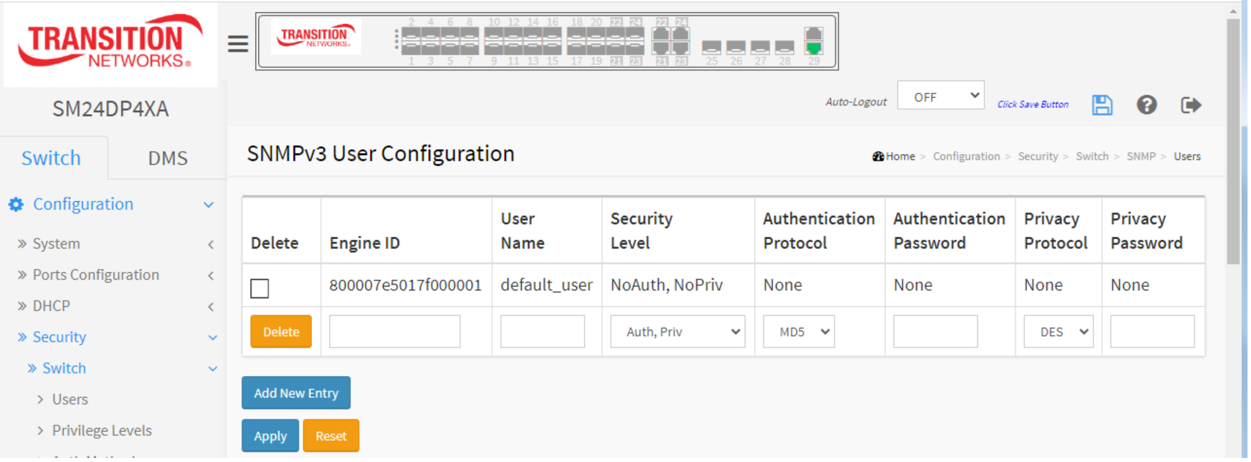
2-4.1.7.4 Users

This page lets you configure SNMPv3 users. The entry index keys are *Engine ID* and *User Name*. The maximum number of Users is 10.

To configure SNMP Users in the web interface:

1. Click Configuration, Security, Switch, SNMP, Users.
2. Specify the SNMPv3 parameters.
3. Click Apply.

Figure 2-4.1.7.4: SNMPv3 User Configuration



SNMPv3 User Configuration

Delete	Engine ID	User Name	Security Level	Authentication Protocol	Authentication Password	Privacy Protocol	Privacy Password
□	800007e5017f000001	default_user	NoAuth, NoPriv	None	None	None	None
Delete			Auth, Priv	MD5		DES	

Parameter descriptions:

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

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

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

Security Level : Indicates the security model that this entry should belong to. Valid values are:

NoAuth, NoPriv: No authentication and no privacy.

Auth, NoPriv: Authentication and no privacy.

Auth, Priv: Authentication and privacy.

This value cannot be modified on an existing entry. 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. Valid values are:

None: No authentication protocol (default instance only).

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.

This value cannot be modified on an existing entry. That means you must first ensure that the value is set correctly. See Term definitions below.

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

Privacy Protocol : Indicates the privacy protocol that this entry should belong to. Valid values are:

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

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

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

Buttons

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

Apply : Click to save changes.

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

Term definitions :

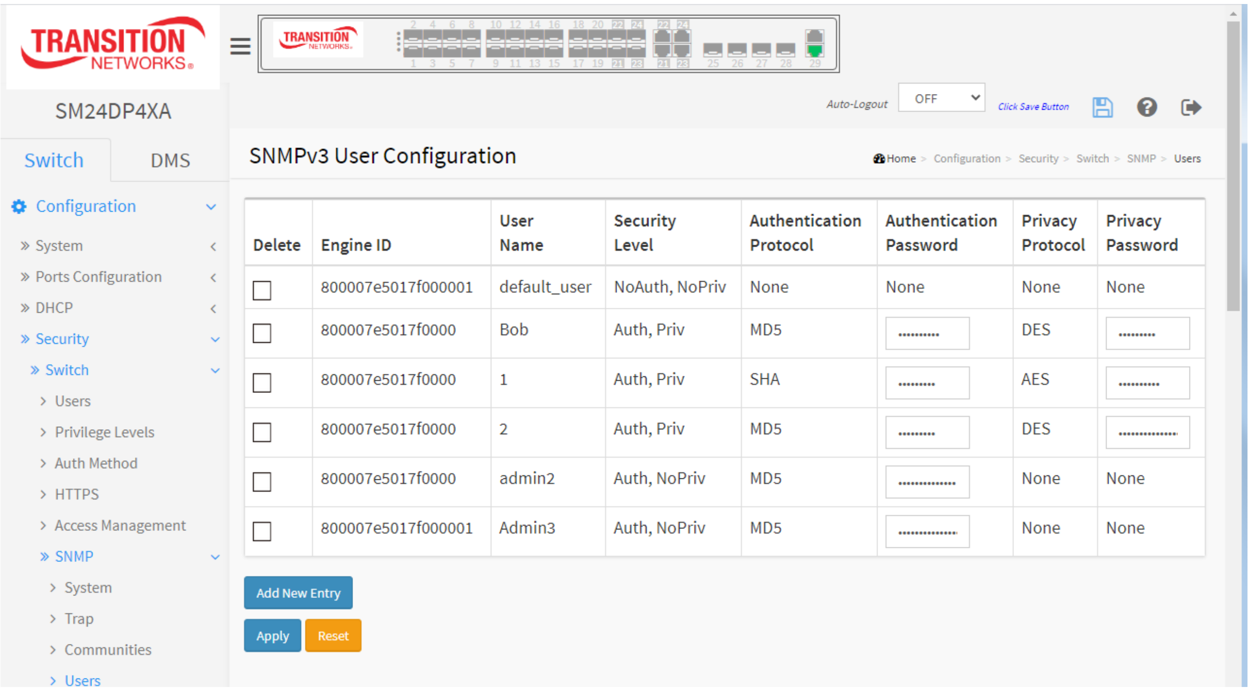
MD5 (Message-Digest algorithm 5) is a message digest algorithm, used cryptographic hash function with a 128-bit hash value. It was designed by Ron Rivest in 1991. MD5 is officially defined in RFC 1321 - The MD5 Message-Digest Algorithm.

SHA (Secure Hash Algorithm) was designed by the National Security Agency (NSA) and published by the NIST as a U.S. Federal Information Processing Standard. Hash algorithms compute a fixed-length digital representation (known as a message digest) of an input data sequence (the message) of any length.

DES (Data Encryption Standard) provides a complete description of a mathematical algorithm for encrypting (enciphering) and decrypting (deciphering) binary coded information. Encrypting data converts it to an unintelligible form called cipher. Decrypting cipher converts the data back to its original form called plaintext. The algorithm described in this standard specifies both enciphering and deciphering operations which are based on a binary number called a key.

AES (Advanced Encryption Standard)is the encryption key protocol applied in the IEEE 802.1i standard to improve WLAN security. It is an encryption standard by the U.S. government, which will replace DES and 3DES. AES has a fixed block size of 128 bits and a key size of 128, 192, or 256 bits.

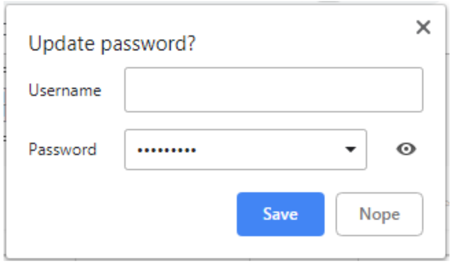
Example:



SNMPv3 User Configuration

Delete	Engine ID	User Name	Security Level	Authentication Protocol	Authentication Password	Privacy Protocol	Privacy Password
□	800007e5017f000001	default_user	NoAuth, NoPriv	None	None	None	None
□	800007e5017f0000	Bob	Auth, Priv	MD5	••••••••••	DES	••••••••••
□	800007e5017f0000	1	Auth, Priv	SHA	•••••••••	AES	••••••••••
□	800007e5017f0000	2	Auth, Priv	MD5	•••••••••	DES	••••••••••••••••
□	800007e5017f0000	admin2	Auth, NoPriv	MD5	•••••••••••••••	None	None
□	800007e5017f000001	Admin3	Auth, NoPriv	MD5	•••••••••••••••	None	None

Messages: After you click the Apply button your browser may display a confirmation prompt asking if you want to change the Username / Password (the text and format are browser dependent).


Update password?

Username:

Password: •••••••••

2-4.1.7.5 Groups

This page lets you configure SNMPv3 groups. The Entry index keys are Security Model and Security Name. To create a new group account, click the Add New Group button, enter the group information, and then click Apply. The maximum number of Groups is: v1: 2, v2c: 2, v3:10.

Web Interface

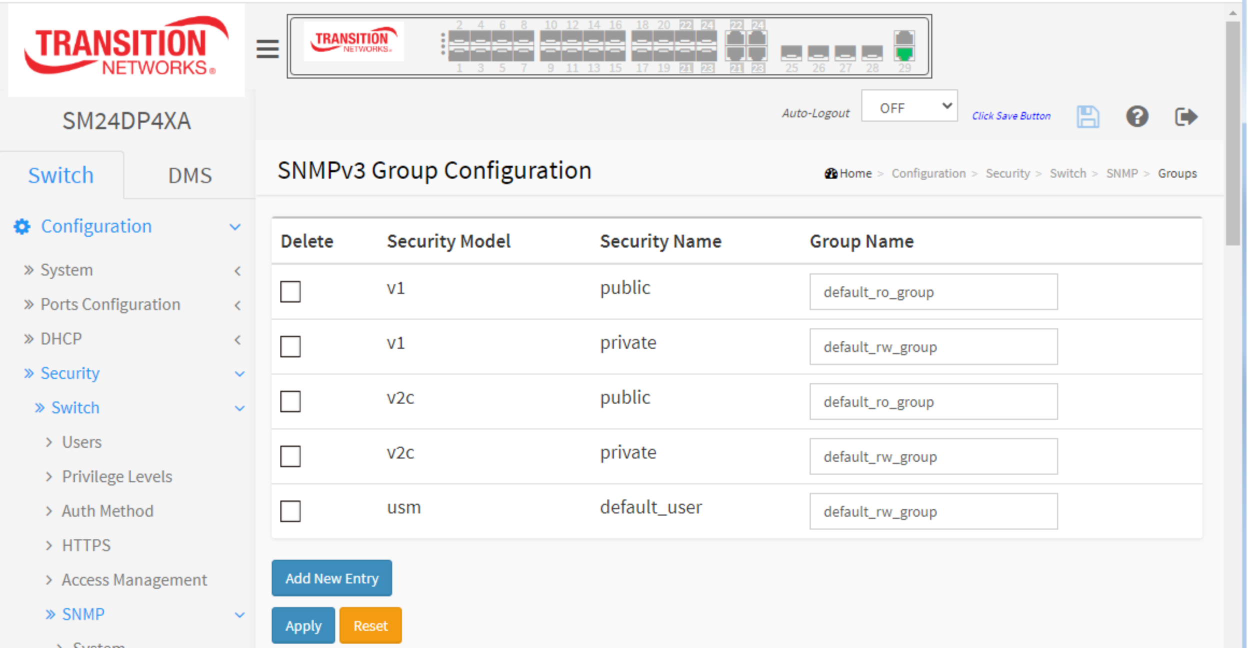
To configure SNMP Groups in the web interface:

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

Click the Add New Entry button and specify Security Model, Security Name, and Group Name.

3. Click Apply.

Figure 2-4.1.7.5: SNMPv3 Group Configuration



SNMPv3 Group Configuration

Delete	Security Model	Security Name	Group Name
□	v1	public	default_ro_group
□	v1	private	default_rw_group
□	v2c	public	default_ro_group
□	v2c	private	default_rw_group
□	usm	default_user	default_rw_group

Parameter descriptions:

Delete : Check to delete the entry.

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

For Security Models ***v1*** and ***v2c***, the Security Name dropdown options are ***public*** or ***private***.
For Security Model ***USM***, the Security Name dropdown option is ***default_user***.

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

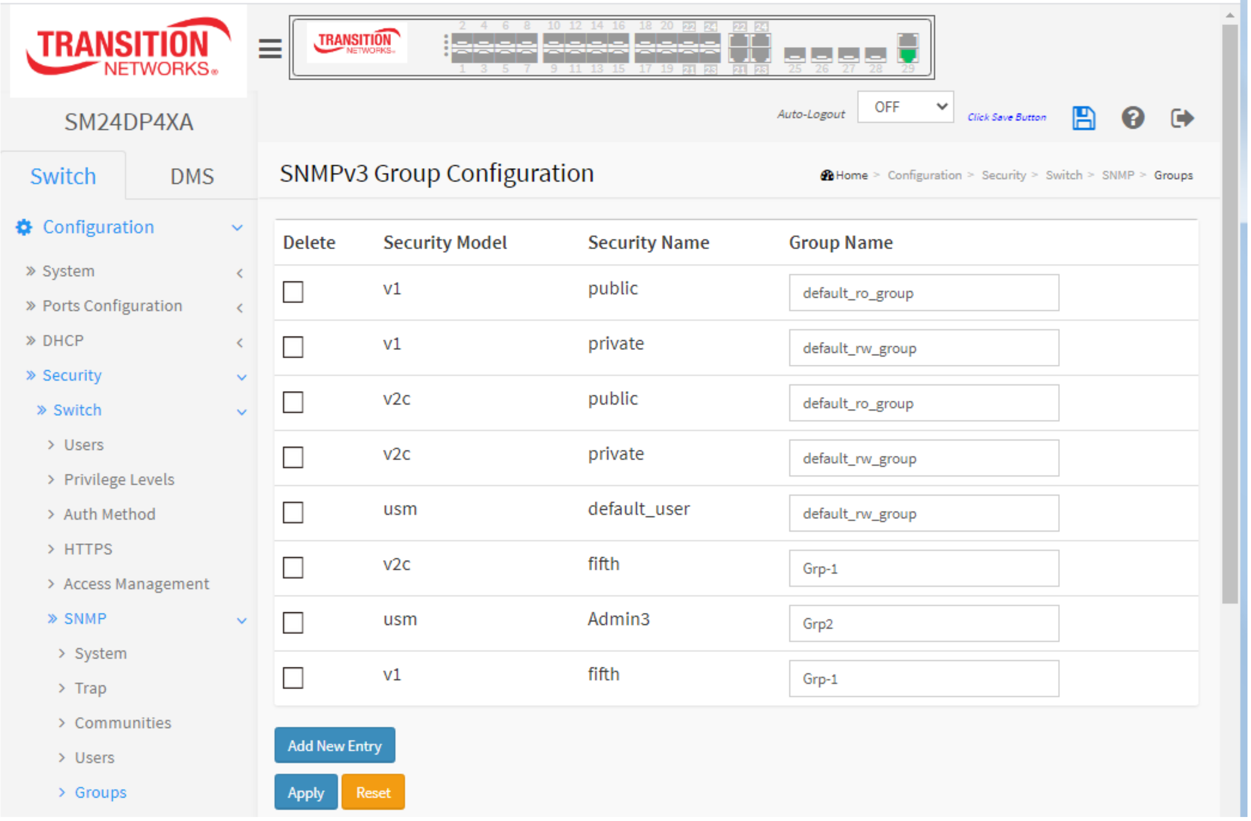
Buttons

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

Apply : Click to save changes.

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

Example:



SNMPv3 Group Configuration

Delete	Security Model	Security Name	Group Name
□	v1	public	default_ro_group
□	v1	private	default_rw_group
□	v2c	public	default_ro_group
□	v2c	private	default_rw_group
□	usm	default_user	default_rw_group
□	v2c	fifth	Grp-1
□	usm	Admin3	Grp2
□	v1	fifth	Grp-1

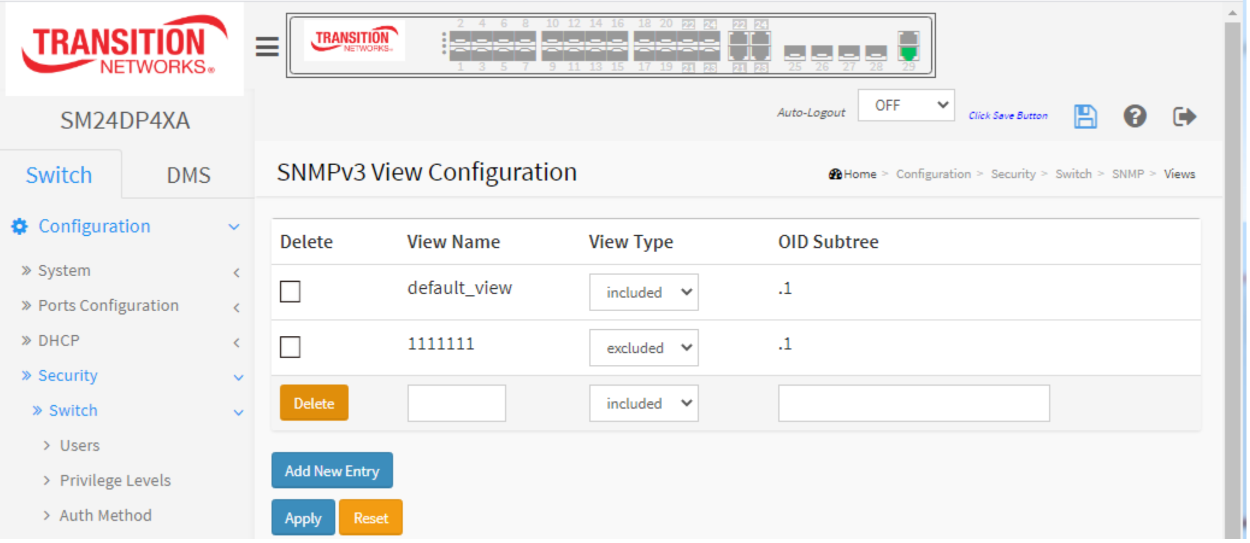
2-4.1.7.6 Views

This page lets you configure SNMPv3 view. The Entry index keys are OID Subtree and View Name.
To create a new view account, click the Add New Entry button, enter the view information, and then click Apply. The maximum number of Views is 28.

Web Interface

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

Figure 2-4.1.7.6: SNMP Views Configuration



SNMPv3 View Configuration

Delete	View Name	View Type	OID Subtree
□	default_view	included	.1
□	1111111	excluded	.1
Delete		included	

Parameter descriptions:

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

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

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

> ***included***: An optional flag to indicate that this view subtree should be included.
>
> ***excluded***: An optional flag to indicate that this view subtree should be excluded. In general, if a view entry's view type is 'excluded', there should be another view entry existing with view type as 'included' and its OID subtree should overstep the 'excluded' view entry.

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

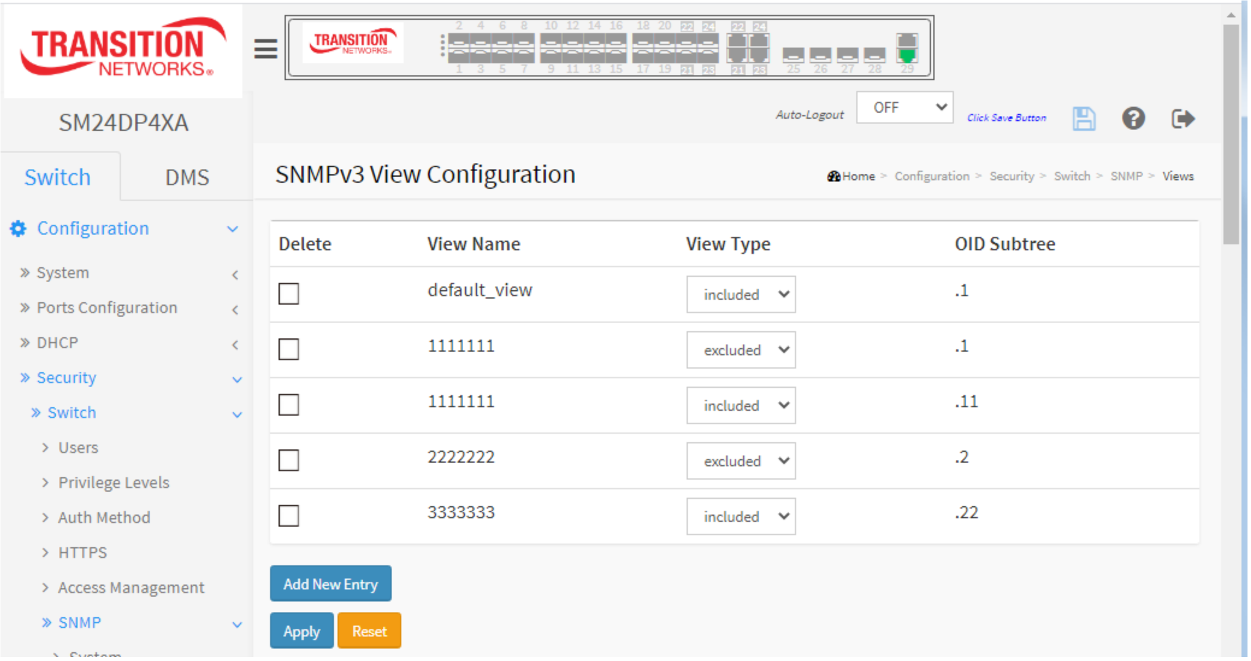
Buttons

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

Apply : Click to save changes.

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

Example:



SNMPv3 View Configuration

Delete	View Name	View Type	OID Subtree
□	default_view	included	.1
□	1111111	excluded	.1
□	1111111	included	.11
□	2222222	excluded	.2
□	3333333	included	.22

2-4.1.7.7 Access

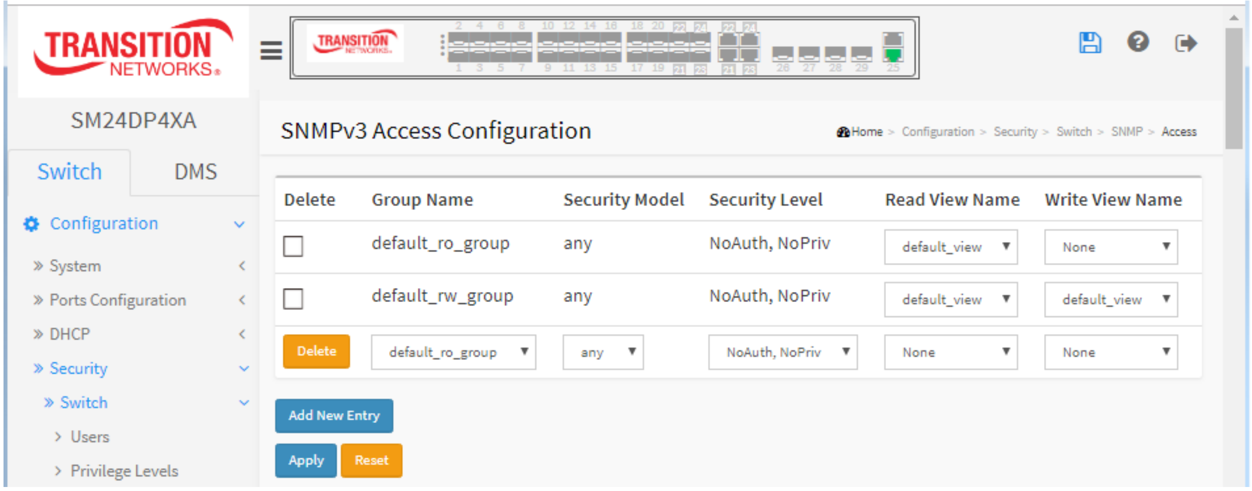
This page lets you configure SNMPv3 accesses. The Entry index key are Group Name, Security Model and Security level. To create a new access account, click the Add New Entry button, enter the access information, and then click Apply. The maximum number of Access Groups is 14.

Web Interface

To configure SNMP Access in the web interface:

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

Figure 2-4.1.7.7: SNMP Accesses Configuration



SNMPv3 Access Configuration

Delete	Group Name	Security Model	Security Level	Read View Name	Write View Name
□	default_ro_group	any	NoAuth, NoPriv	default_view ▼	None ▼
□	default_rw_group	any	NoAuth, NoPriv	default_view ▼	default_view ▼
Delete	default_ro_group ▼	any ▼	NoAuth, NoPriv ▼	None ▼	None ▼

Parameter descriptions:

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

Group Name : At the dropdown select the group name that this entry should belong to.

default_ro_group : Select to add the Group to the default read-only group.

default_rw_group : Select to add the Group to the default read-write group.

Security Model : Indicates the security model that this entry should belong to. Valid values 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. Valid values 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. Select ***None*** or ***default_view***.

Write View Name : The name of the MIB view defining the MIB objects for which this request may potentially set new values. Select ***None*** or ***default_view***.

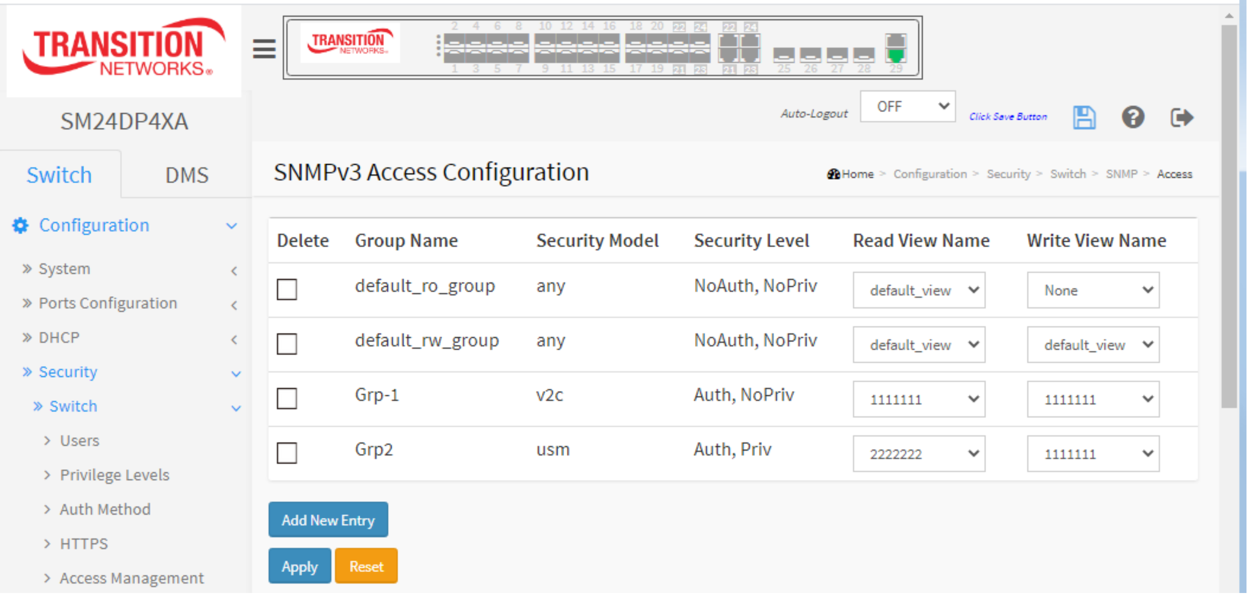
Buttons

Add New Entry : Click to add a new Group Access entry.

Apply : Click to save changes.

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

Example:



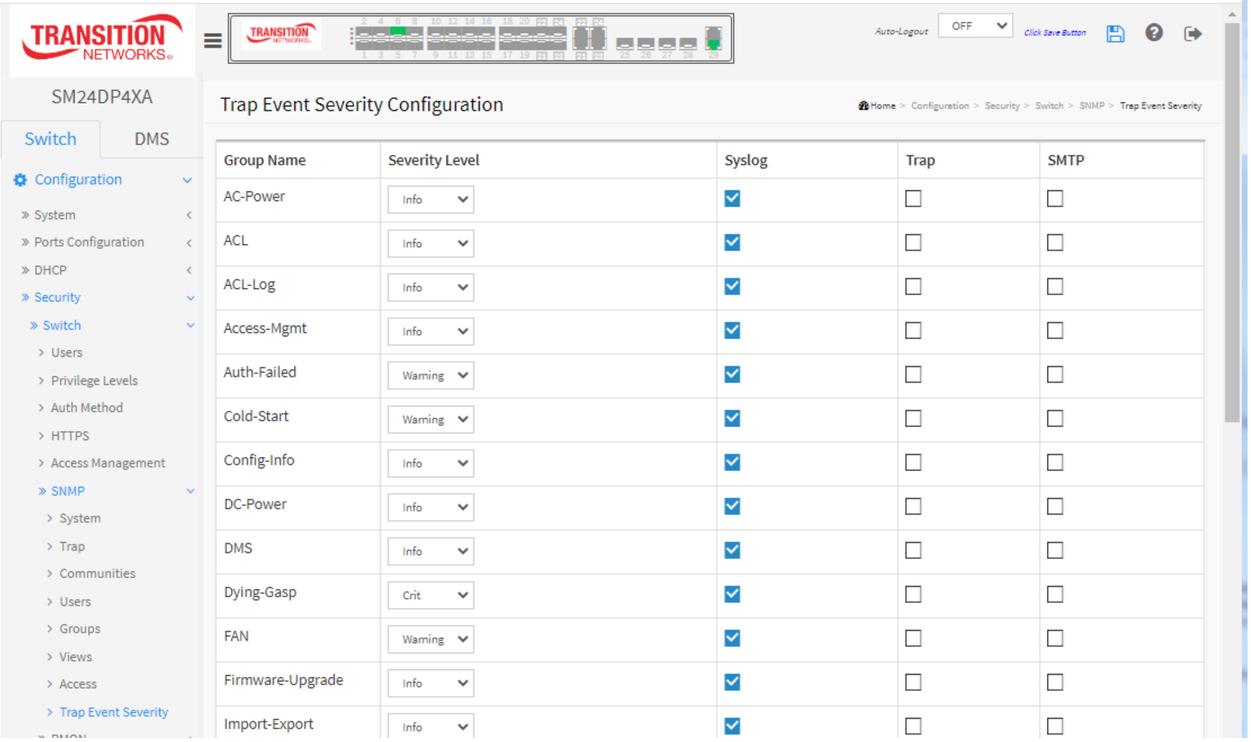
SNMPv3 Access Configuration

Auto-Logout: OFF

Delete	Group Name	Security Model	Security Level	Read View Name	Write View Name
□	default_ro_group	any	NoAuth, NoPriv	default_view	None
□	default_rw_group	any	NoAuth, NoPriv	default_view	default_view
□	Grp-1	v2c	Auth, NoPriv	1111111	1111111
□	Grp2	usm	Auth, Priv	2222222	1111111

2-4.1.7.8 Trap Event Severity

This page lets you set set Trap Event Severity parameters.



Trap Event Severity Configuration

Group Name	Severity Level	Syslog	Trap	SMTP
AC-Power	Info	☑	□	□
ACL	Info	☑	□	□
ACL-Log	Info	☑	□	□
Access-Mgmt	Info	☑	□	□
Auth-Failed	Warning	☑	□	□
Cold-Start	Warning	☑	□	□
Config-Info	Info	☑	□	□
DC-Power	Info	☑	□	□
DMS	Info	☑	□	□
Dying-Gasp	Crit	☑	□	□
FAN	Warning	☑	□	□
Firmware-Upgrade	Info	☑	□	□
Import-Export	Info	☑	□	□

Parameter descriptions:

Group Name: The name identifying the severity group.

Severity Level: Every group has an severity level. The following level types are supported:

<0> ***Emerg***ency: System is unusable.

<1> ***Alert***: Action must be taken immediately.

<2***>*** ***Crit***ical: Critical conditions.

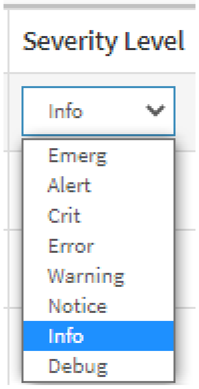
<3> ***Error***: Error conditions.

<4> ***Warning***: Warning conditions.

<5> ***Notice***: Normal but significant conditions.

<6> ***Info***rmation: Information messages.

<7> ***Debug***: Debug-level messages.



Syslog: Enable - Select this Group Name in Syslog.

Trap: Enable - Select this Group Name in Trap.

SMTP: Enable - Select this Group Name in SMTP.

Buttons

Apply: Click to apply changes.

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

2-4.1.8 RMON

An RMON implementation typically operates in a client/server model, monitoring devices that 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.

2-4.1.8.1 Statistics

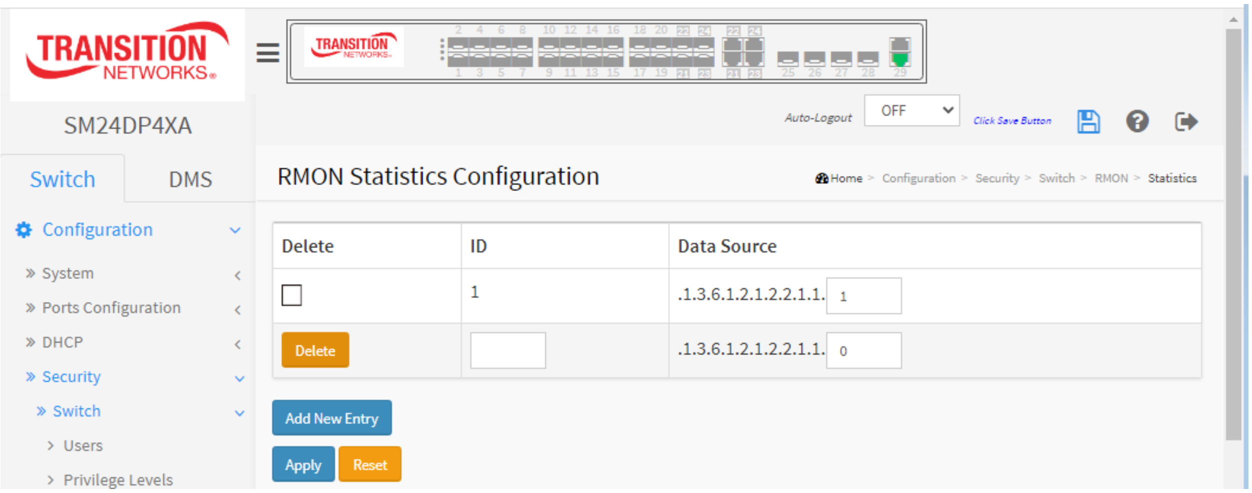
Configure RMON Statistics table on this page. The entry index key is **ID.**

Web Interface

To configure RMON parameters via the web interface:

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

Figure 2-4.1.8.1: RMON Statics Configuration



RMON Statistics Configuration

Delete	ID	Data Source
☐	1	.1.3.6.1.2.1.2.2.1.1. 1
Delete		.1.3.6.1.2.1.2.2.1.1. 0

Parameter descriptions:

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.

Buttons

Add New Entry: Click to add a new RMON statistics entry.

Apply : Click to save changes.

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

2-4.1.8.2 History

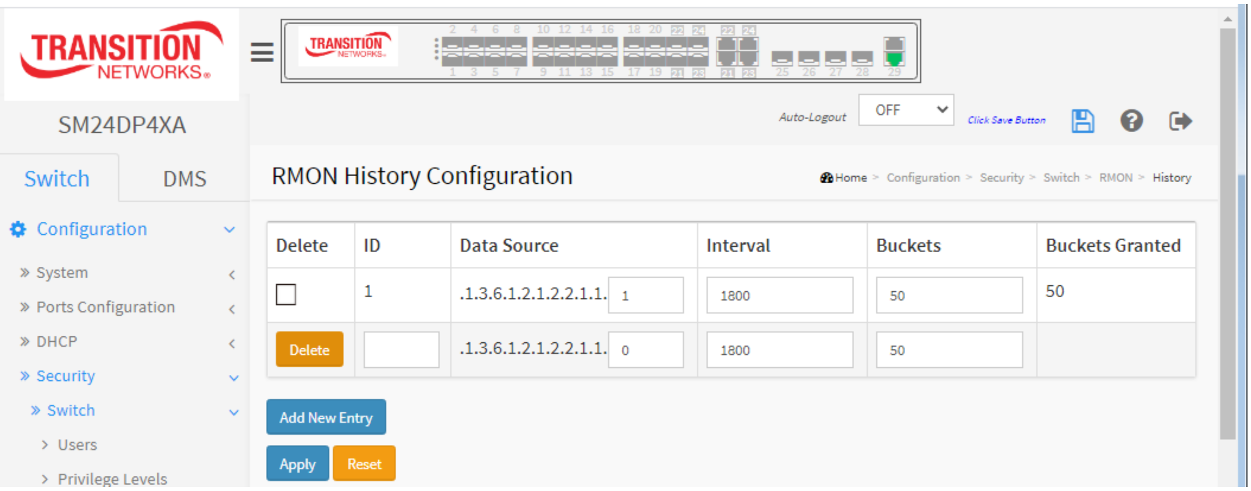
Configure RMON History table on this page. The entry index key is **ID.**

Web Interface

To 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 2-4.1.8.2: RMON History Configuration



RMON History Configuration

Delete	ID	Data Source	Interval	Buckets	Buckets Granted
□	1	.1.3.6.1.2.1.2.2.1.1. 1	1800	50	50
Delete		.1.3.6.1.2.1.2.2.1.1. 0	1800	50	

Parameter descriptions:

Delete : Check to delete the entry.

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

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

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

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

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

Buttons

Add New Entry: Click to add a new RMON history entry.

Apply : Click to save changes.

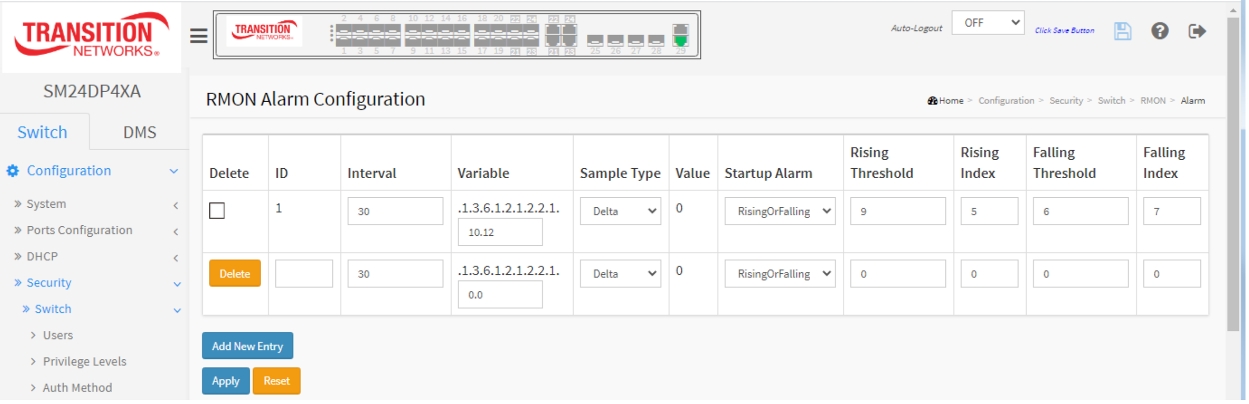
Reset : Click to undo any changes made locally and revert to previously saved values.

2-4.1.8.3 Alarm

Configure RMON Alarm table on this page. The entry index key is **ID.** To configure RMON Alarm via the web interface:

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

Figure 2-4.1.8.3: RMON Alarm Configuration



RMON Alarm Configuration

Delete	ID	Interval	Variable	Sample Type	Value	Startup Alarm	Rising Threshold	Rising Index	Falling Threshold	Falling Index
□	1	30	.1.3.6.1.2.1.2.2.1. 10.12	Delta	0	RisingOrFalling	9	5	6	7
Delete		30	.1.3.6.1.2.1.2.2.1. 0.0	Delta	0	RisingOrFalling	0	0	0	0

Add New Entry

Apply Reset

Parameter descriptions:

Delete : Check to delete the entry immediately.

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

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

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

> ***InOctets***: The total number of octets received on the interface, including framing characters.
>
> ***InUcastPkts***: The number of uni-cast packets delivered to a higher-layer protocol.
>
> ***InNUcastPkts***: The number of broad-cast and multi-cast packets delivered to a higher-layer protocol.
>
> ***InDiscards***: The number of inbound packets that are discarded even the packets are normal.
>
> ***InErrors***: The number of inbound packets that contained errors preventing them from being deliverable to a higher-layer protocol.
>
> ***InUnknownProtos***: the number of the inbound packets that were discarded because of the unknown or un-support protocol.
>
> ***OutOctets***: The number of octets transmitted out of the interface , including framing characters.
>
> ***OutUcastPkts***: The number of uni-cast packets that request to transmit.
>
> ***OutNUcastPkts***: The number of broad-cast and multi-cast packets that request to transmit.
>
> ***OutDiscards***: The number of outbound packets that are discarded event the packets is normal.
>
> ***OutErrors***: The number of outbound packets that could not be transmitted because of errors.
>
> ***OutQLen***: The length of the output packet queue (in packets).

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

Absolute: Get the sample directly.

Delta: Calculate the difference between samples (default).

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

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

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

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

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

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

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

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

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

Buttons

Add New Entry: Click to add a new RMON alarm entry.

Apply : Click to save changes.

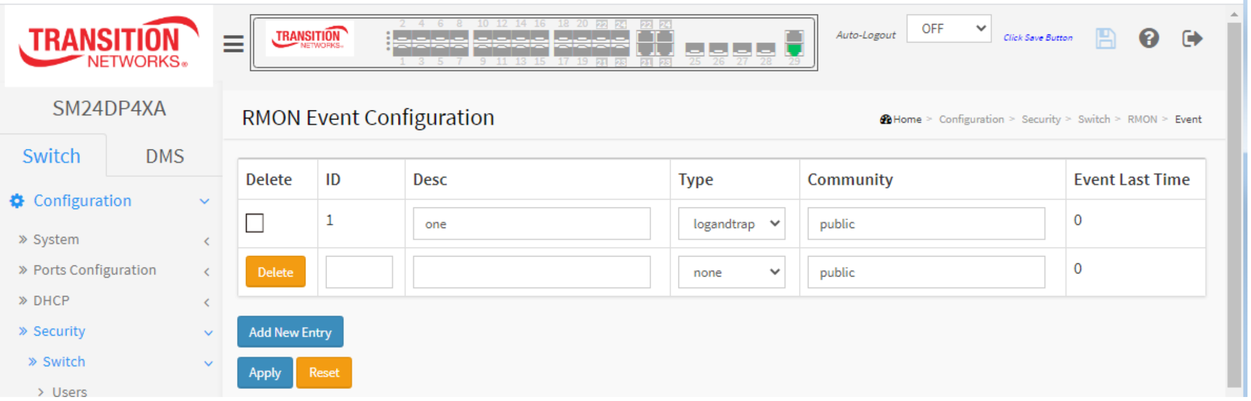
Reset : Click to undo any changes made locally and revert to previously saved values.

2-4.1.8.4 Event

Configure RMON Event table on this page. The entry index key is **ID.** To configure RMON Event via the web UI:

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

Figure 2-4.1.8.4: RMON Event Configuration



RMON Event Configuration

Delete	ID	Desc	Type	Community	Event Last Time
□	1	one	logandtrap	public	0
Delete			none	public	0

Add New Entry

Apply Reset

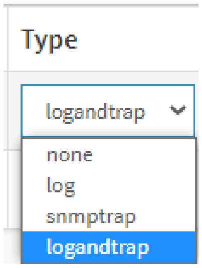
Parameter descriptions:

Delete : Check to delete the entry immediately.

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

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

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



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

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

logandtrap: The number of inbound packets that are discarded even the packets are normal (default) .

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

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

2-4.2 Network

2-4.2.1 Limit Control

This section shows you 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.

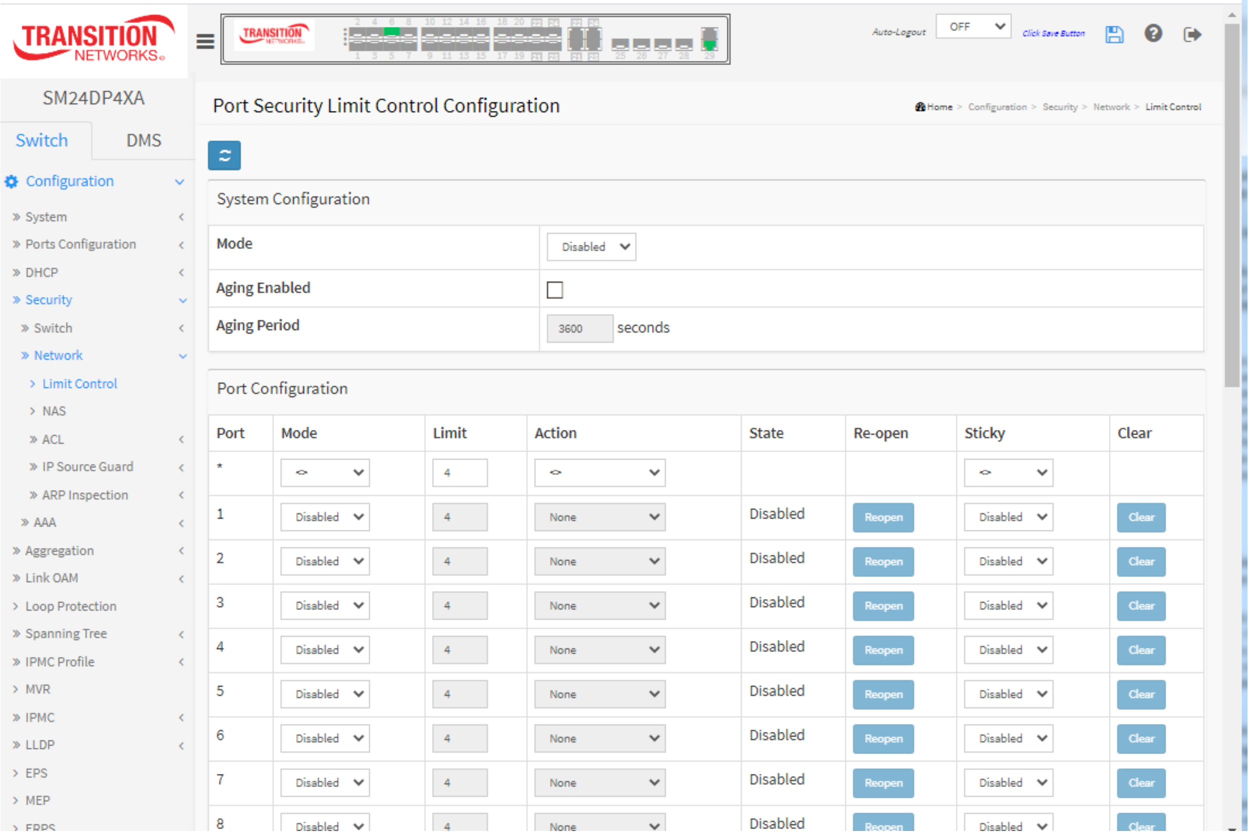
To configure a Configuration of Limit Control via the web UI:

1. Select “Enabled” at the Mode dropdown in the System Configuration section.
2. Check Aging Enabled.
3. Set Aging Period (default is 3600 seconds).

To configure a Port Configuration of Limit Control via the web interface:

1. Select “Enabled” in the Mode column 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 2-4.2.1: Port Security Limit Control Configuration



Port Security Limit Control Configuration

System Configuration

Mode	Disabled
Aging Enabled	□
Aging Period	3600 seconds

Port Configuration

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

Parameter descriptions:

System Configuration

Mode : Indicates if Limit Control is globally enabled or disabled on the switch. If globally disabled, other modules may still use the underlying functionality, but limit checks and 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 : The table has one row for each port and a number of columns:

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 is 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. The three ways to re-open the port:
>
> * Boot the switch,
>
> * Disable and re-enable Limit Control on the port or the switch, or
>
> * Click the Reopen button.

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

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

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

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

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

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

Re-open button : If a port is shut down by this module, you may reopen it by clicking this button, which will only be enabled if this is the case. For other methods, refer to Shutdown in the Action section above. **NOTE**: Clicking the Re-open button causes the page to be refreshed, so non-committed changes will be lost.

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

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

Buttons:

Refresh: Click to immediately refresh the page manually.

Apply – Click to save changes.

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

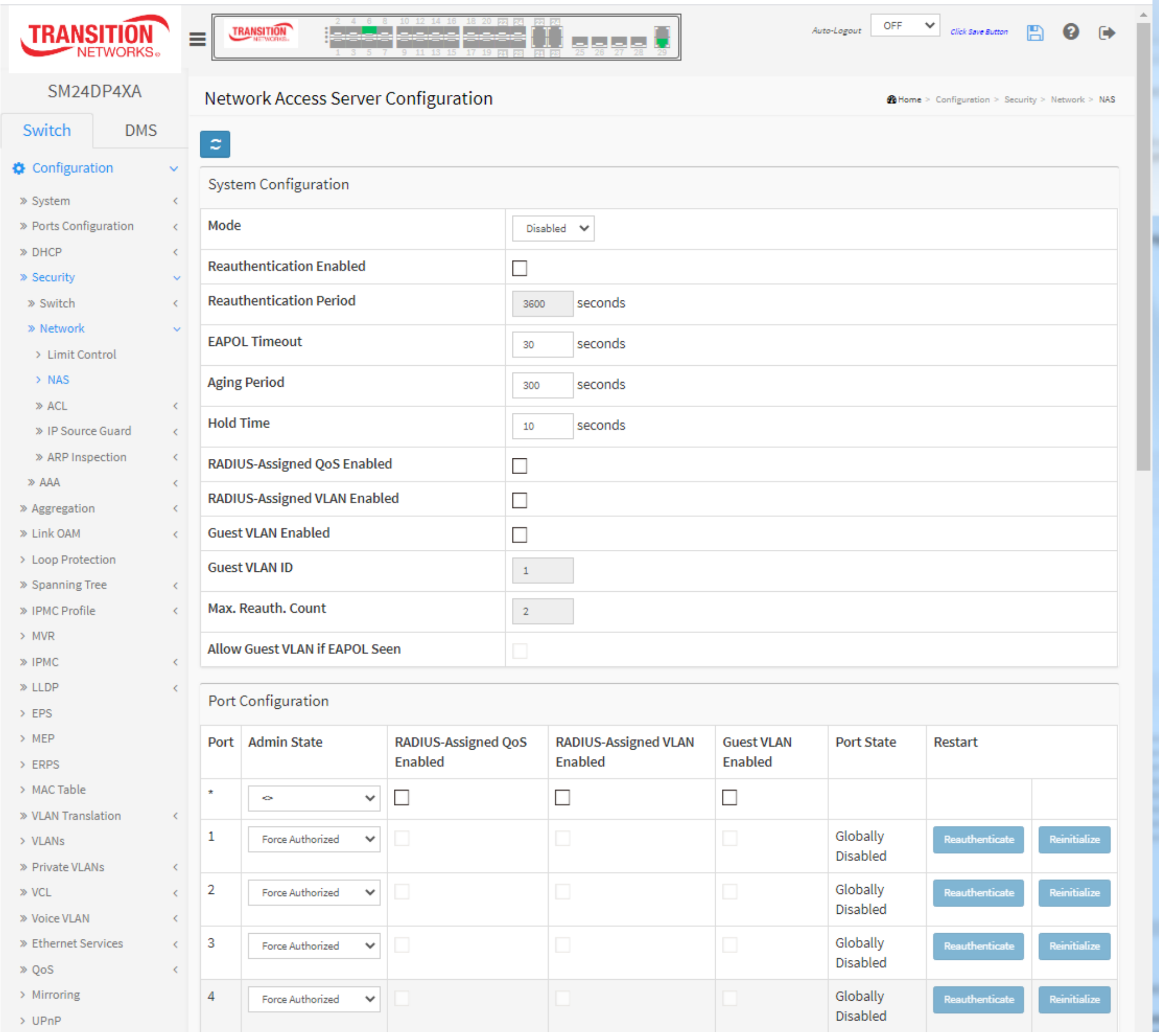
2-4.2.2 NAS

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

To configure a Network Access Server via the web UI:

1. Select “Enabled” in the Mode column of the Network Access Server Configuration section.
2. Set the System Configuration parameters.
3. Set the Port Configuration parameters.
4. Click Apply.

Figure 2-4.2.2: Network Access Server Configuration



Network Access Server Configuration

System Configuration

Mode	Disabled
Reauthentication Enabled	□
Reauthentication Period	3600 seconds
EAPOL Timeout	30 seconds
Aging Period	300 seconds
Hold Time	10 seconds
RADIUS-Assigned QoS Enabled	□
RADIUS-Assigned VLAN Enabled	□
Guest VLAN Enabled	□
Guest VLAN ID	1
Max. Reauth. Count	2
Allow Guest VLAN if EAPOL Seen	□

Port Configuration

Port	Admin State	RADIUS-Assigned QoS Enabled	RADIUS-Assigned VLAN Enabled	Guest VLAN Enabled	Port State	Restart	
*	<>	□	□	□			
1	Force Authorized	□	□	□	Globally Disabled	Reauthenticate	Reinitialize
2	Force Authorized	□	□	□	Globally Disabled	Reauthenticate	Reinitialize
3	Force Authorized	□	□	□	Globally Disabled	Reauthenticate	Reinitialize
4	Force Authorized	□	□	□	Globally Disabled	Reauthenticate	Reinitialize

Parameter descriptions:

<u>System Configuration</u>

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 determines whether RADIUS-assigned QoS Class is enabled on that port. When unchecked, RADIUS-server assigned QoS Class is disabled on all ports.

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

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

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

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

Guest VLAN ID : This is the value that a port's Port VLAN ID is set to if a port is moved into the Guest VLAN. It is only changeable if the Guest VLAN option is globally enabled. Valid values are in the range [1; 4095].

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

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

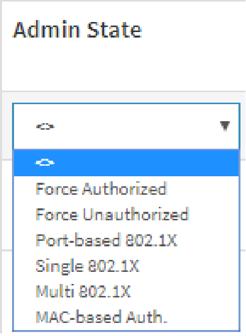
The value can only be changed if the Guest VLAN option is globally enabled.

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

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

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

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



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

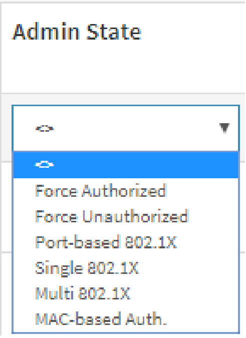
Port-based 802.1X **:** In the 802.1X-world, the user is called the supplicant, the switch is the authenticator, and the RADIUS server is the authentication server. The authenticator acts as the man-in-the-middle, forwarding requests and responses between the supplicant and the authentication server.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

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

NOTE: Suppose two backend servers are enabled and that the server timeout is configured to X seconds (using the AAA configuration page), and suppose that the first server in the list is currently down (but not considered dead). Now, if the supplicant retransmits EAPOL Start frames at a rate faster than X seconds, then it will never get authenticated, because the switch will cancel on-going backend authentication server requests whenever it receives a new EAPOL Start frame from the supplicant. And since the server hasn't yet failed (because the X seconds haven't expired), the same server will be contacted upon the next backend authentication server request from the switch. This scenario will loop forever. Therefore, the server timeout should be smaller than the supplicant's EAPOL Start frame retransmission rate.

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

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



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

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

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

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

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

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

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

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

- Port-based 802.1X
- 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 or Single 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.

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 these 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.

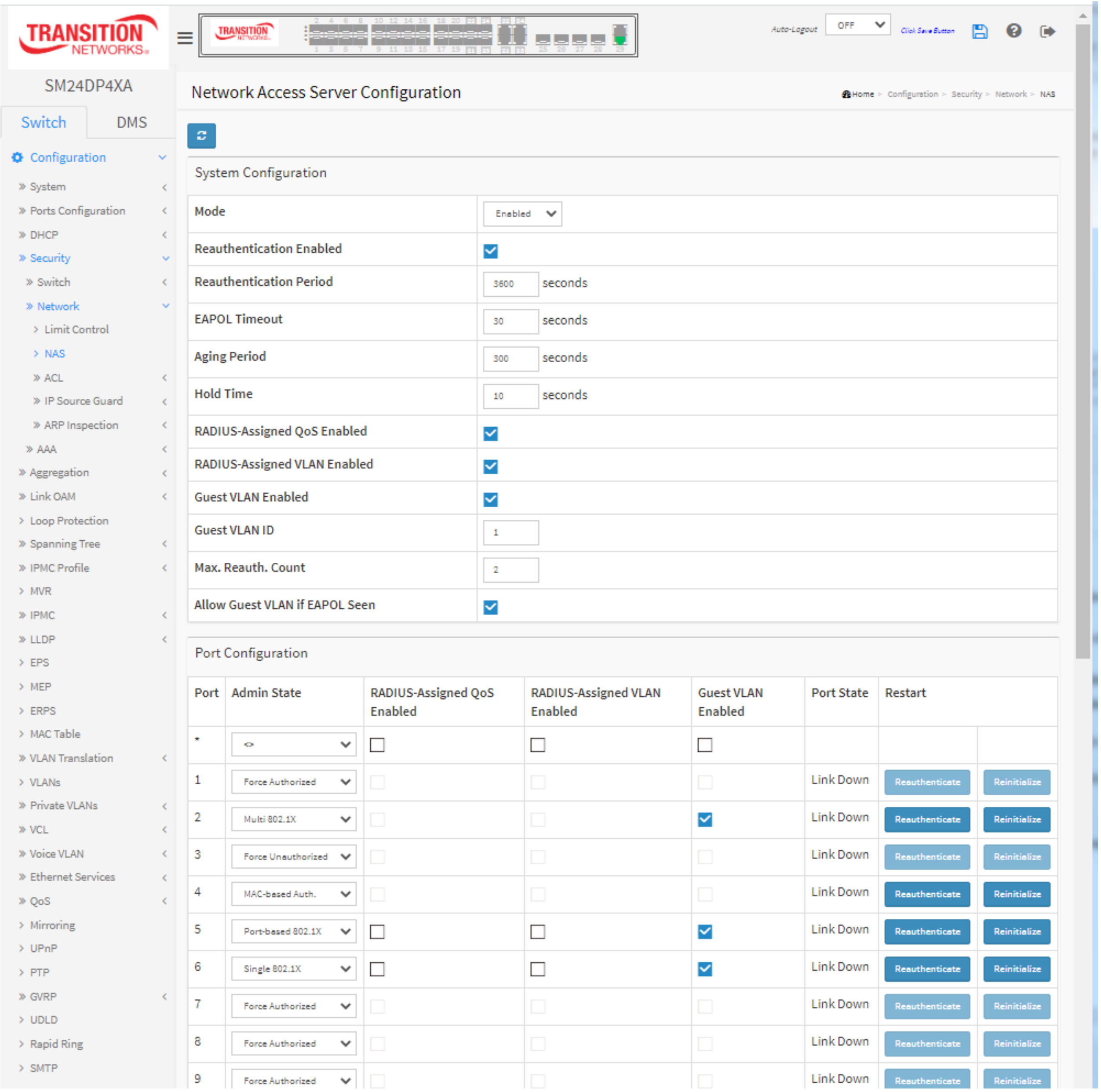
X Auth/Y Unauth: The port is in a multi-supplicant mode. Currently X clients are authorized and Y are unauthorized.

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.

Example:



Network Access Server Configuration

System Configuration

Mode	Enabled
Reauthentication Enabled	☑
Reauthentication Period	3600 seconds
EAPOL Timeout	30 seconds
Aging Period	300 seconds
Hold Time	10 seconds
RADIUS-Assigned QoS Enabled	☑
RADIUS-Assigned VLAN Enabled	☑
Guest VLAN Enabled	☑
Guest VLAN ID	1
Max. Reauth. Count	2
Allow Guest VLAN if EAPOL Seen	☑

Port Configuration

Port	Admin State	RADIUS-Assigned QoS Enabled	RADIUS-Assigned VLAN Enabled	Guest VLAN Enabled	Port State	Restart	
*	<>	□	□	□			
1	Force Authorized	□	□	□	Link Down	Reauthenticate	Reinitialize
2	Multi 802.1X	□	□	☑	Link Down	Reauthenticate	Reinitialize
3	Force Unauthorized	□	□	□	Link Down	Reauthenticate	Reinitialize
4	MAC-based Auth.	□	□	□	Link Down	Reauthenticate	Reinitialize
5	Port-based 802.1X	□	□	☑	Link Down	Reauthenticate	Reinitialize
6	Single 802.1X	□	□	☑	Link Down	Reauthenticate	Reinitialize
7	Force Authorized	□	□	□	Link Down	Reauthenticate	Reinitialize
8	Force Authorized	□	□	□	Link Down	Reauthenticate	Reinitialize
9	Force Authorized	□	□	□	Link Down	Reauthenticate	Reinitialize

Buttons:

Apply : Click to save changes.

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

Refresh : Click to manually refresh the webpage immediately.

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

Recovery: **1.** Click the Previous button. **2.** Disable Spanning Tree at Configuration > Spanning Tree > CIST Port. **3.** Continue operation.

2-4.2.3 ACL

The switch 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 EtherTypes (IPv4, ARP protocol, MAC and VLAN parameters, etc.). Here we will cover standard and extended access lists for TCP/IP. As you create ACEs for ingress classification, you can assign a policy for each port, the policy number is 1-8; however, each policy can be applied to any port. This makes it very easy to determine what type of ACL policy you will be working with.

2-4.2.3.1 Ports

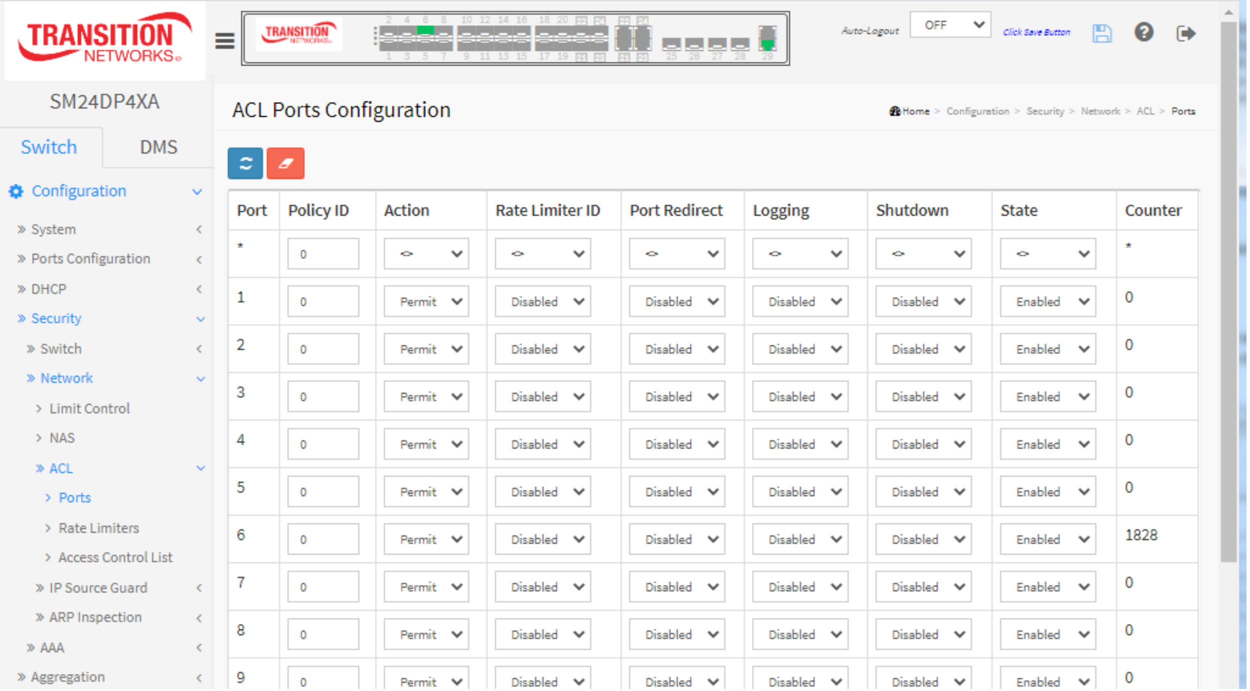
This page lets you to configure the ACL parameters (ACE) of each switch port. These parameters will affect frames received on a port unless the frame matches a specific ACE

Web Interface

To configure the ACL Ports Configuration in the web interface:

1. Click Configuration, Security, Network, ACL, Ports.
2. Specify the parameters for port ACL settings.
3. Click Apply to save the settings.
4. To cancel the settings click the Reset button to revert to previously saved values.
5. View the port Counters and click Refresh to update the counter or click Clear to clear the page.

Figure 2-4.2.3.1: ACL Ports Configuration



ACL Ports Configuration

Port	Policy ID	Action	Rate Limiter ID	Port Redirect	Logging	Shutdown	State	Counter
*	0	<>	<>	<>	<>	<>	<>	*
1	0	Permit	Disabled	Disabled	Disabled	Disabled	Enabled	0
2	0	Permit	Disabled	Disabled	Disabled	Disabled	Enabled	0
3	0	Permit	Disabled	Disabled	Disabled	Disabled	Enabled	0
4	0	Permit	Disabled	Disabled	Disabled	Disabled	Enabled	0
5	0	Permit	Disabled	Disabled	Disabled	Disabled	Enabled	0
6	0	Permit	Disabled	Disabled	Disabled	Disabled	Enabled	1828
7	0	Permit	Disabled	Disabled	Disabled	Disabled	Enabled	0
8	0	Permit	Disabled	Disabled	Disabled	Disabled	Enabled	0
9	0	Permit	Disabled	Disabled	Disabled	Disabled	Enabled	0

Parameter descriptions:

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

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

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

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

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

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

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

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

Save – Click to save changes.

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

Clear : Click to clear parameters manually.

Refresh: Click to manually refresh the webpage immediately.

2-4.2.3.2 Rate Limiters

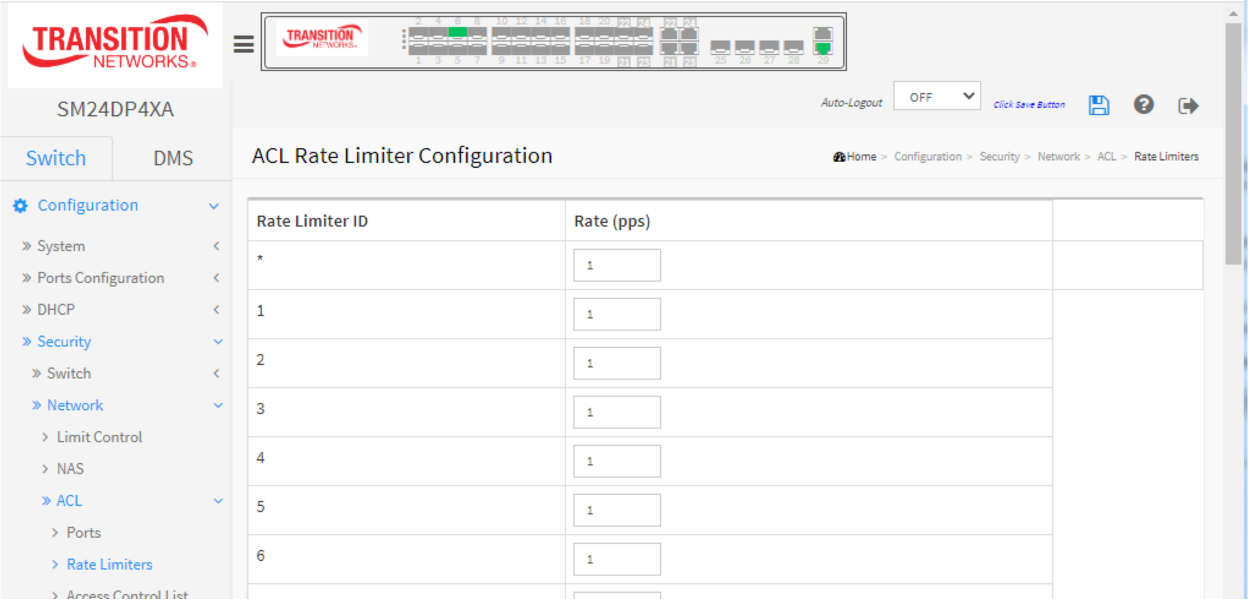
This page lets you configure the switch's ACL Rate Limiter parameters. The Rate Limiter Level (1 – 16) lets you set a Rate limit value in pps (packets per second).

Web Interface

To configure ACL Rate Limiter in the web interface:

1. Click Configuration, Security, Network, ACL, Rate Limiters.
2. Specify the Rate (pps) field.
3. Click the Apply button to save the settings.
5. To cancel the settings click the Reset button to revert to previously saved values.

Figure 2-4.2.3.2: ACL Rate Limiter Configuration



Auto-Logout: OFF

ACL Rate Limiter Configuration

Rate Limiter ID	Rate (pps)
*	1
1	1
2	1
3	1
4	1
5	1
6	1

Parameter descriptions:

Rate Limiter ID : The rate limiter ID for the settings contained in the same row (1 – 16).

Rate : The valid rate 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.

2-4.2.3.3 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.

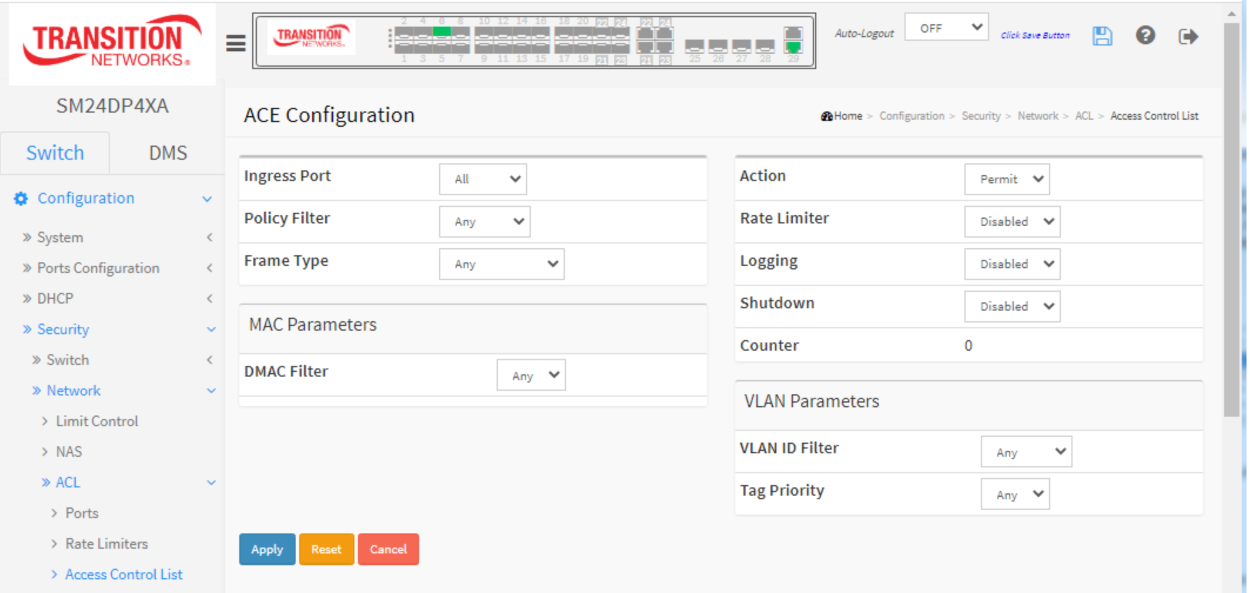
This page shows the Access Control List (ACL), which is made up of the ACEs defined on this switch. Each row describes the ACE that is defined. The maximum number of ACEs is 256 on each switch. Click on the lowest plus sign to add a new ACE to the list. The reserved ACEs used for internal protocol cannot 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 (i.e., edit, delete, or move the relative position of an entry in the list).
3. Specify the ACE parameters.
4. Click the Apply button to save the settings.
5. To cancel the settings click the reset button. It will revert to previously saved values.
6. When editing an entry on the ACE Configuration page, note that the Items displayed depend on various selections, such as Frame Type and IP Protocol Type. Specify the relevant criteria to be matched for this rule and set the actions to take when a rule is matched (such as Rate Limiter, Port Copy, Logging, and Shutdown).

Figure 2-4.2.3.3: ACL Rate Limiter Configuration (Frame Type = *Any*)



ACE Configuration

Ingress Port	All
Policy Filter	Any
Frame Type	Any

MAC Parameters

DMAC Filter	Any

Action	Permit
Rate Limiter	Disabled
Logging	Disabled
Shutdown	Disabled
Counter	0

VLAN Parameters

VLAN ID Filter	Any
Tag Priority	Any

Auto-Logout: OFF

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 Filter : Specify the policy number filter for this ACE.

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

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

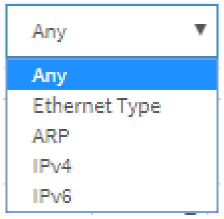
Policy Value : When "Specific" is selected for the policy filter, you can enter a specific policy value. The allowed range is 0 - 255.

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

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

Any: Any frame can match this ACE.

Ethernet Type: Only Ethernet Type frames can match this ACE. The IEEE 802.3 describes the value of Length/Type Field specifications to be greater than or equal to 1536 decimal (equal to 0600 hexadecimal) and the value should not be equal to 0x800(IPv4), 0x806(ARP) or 0x86DD(IPv6).



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

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

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

Action : Indicates the forwarding action of the ACE.

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

Deny: Frames matching the ACE are dropped.

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.

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.

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 : Indicates the number of times the ACE was hit by a frame.

Modification Buttons : Modify each ACE (Access Control Entry) in the table using these buttons:

⊕: Inserts a new ACE before the current row.

ⓔ: Edits the ACE row.

↑: Moves the ACE up the list.

↓: Moves the ACE down the list.

⊗: Deletes the ACE.

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

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. Notice the invalid IP address configuration is acceptable too, for example, 0.0.0.0. Normally, an ACE with invalid IP address will explicitly adding deny action.

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

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

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

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

Target IP Address : When "Host" or "Network" is selected for the target IP filter, you can enter a specific target IP address in dotted decimal notation. Notice the invalid IP address configuration is acceptable too, for example, 0.0.0.0. Normally, an ACE with invalid IP address will explicitly adding deny action.

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

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

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

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

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

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

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

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

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

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

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

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

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

IP : 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").

Ethernet : 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 section.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

SIP Address : When "Host" or "Network" is selected for the source IP filter, you can enter a specific SIP address in dotted decimal notation. Notice the invalid IP address configuration is acceptable too, for example, 0.0.0.0. Normally, an ACE with invalid IP address will explicitly adding deny action.

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

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

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

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

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

DIP Address : When "Host" or "Network" is selected for the destination IP filter, you can enter a specific DIP address in dotted decimal notation. Notice the invalid IP address configuration is acceptable too, for example, 0.0.0.0. Normally, an ACE with invalid IP address will explicitly adding deny action.

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

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

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

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

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

ICMP: Select ICMP to filter IPv6 ICMP protocol frames. Extra fields for defining ICMP parameters will appear. These fields are explained later in this 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 supports last 32 bits for IPv6 address.

SIP Bit Mask : When "Specific" is selected for the source IPv6 filter, you can enter a specific SIPv6 mask. The field only supports 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 0xFFFFFFFE(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 - 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 - 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 : These 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").

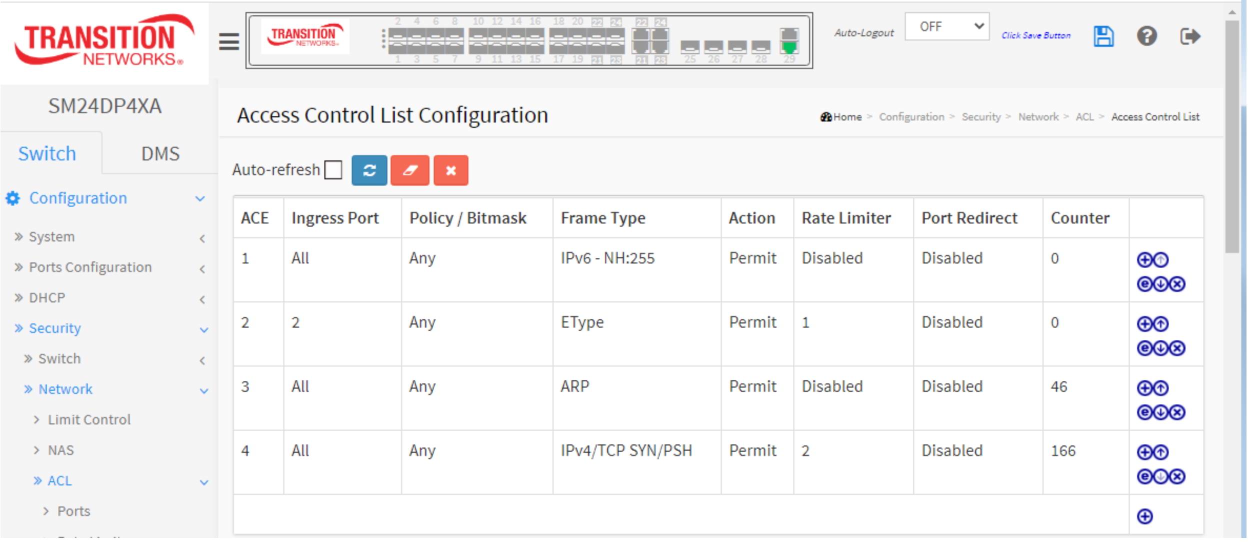
Specific: If you want to filter a specific EtherType filter with this ACE, you can enter a specific EtherType value. A field for entering a EtherType value appears.

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 cancel any unsaved changes.

Example:



Access Control List Configuration

Home > Configuration > Security > Network > ACL > Access Control List

Auto-refresh □

ACE	Ingress Port	Policy / Bitmask	Frame Type	Action	Rate Limiter	Port Redirect	Counter
1	All	Any	IPv6 - NH:255	Permit	Disabled	Disabled	0
2	2	Any	EType	Permit	1	Disabled	0
3	All	Any	ARP	Permit	Disabled	Disabled	46
4	All	Any	IPv4/TCP SYN/PSH	Permit	2	Disabled	166

2-4.2.5 IP Source Guard

This page lets you configure the IP Source Guard detail parameters of the switch. The IP Source Guard security feature is used to restrict IP traffic on DHCP snooping untrusted ports by filtering traffic based on the DHCP Snooping Table or manually configured IP Source Bindings. It helps prevent IP spoofing attacks when a host tries to spoof and use the IP address of another host.

2-4.2.5.1 Configuration

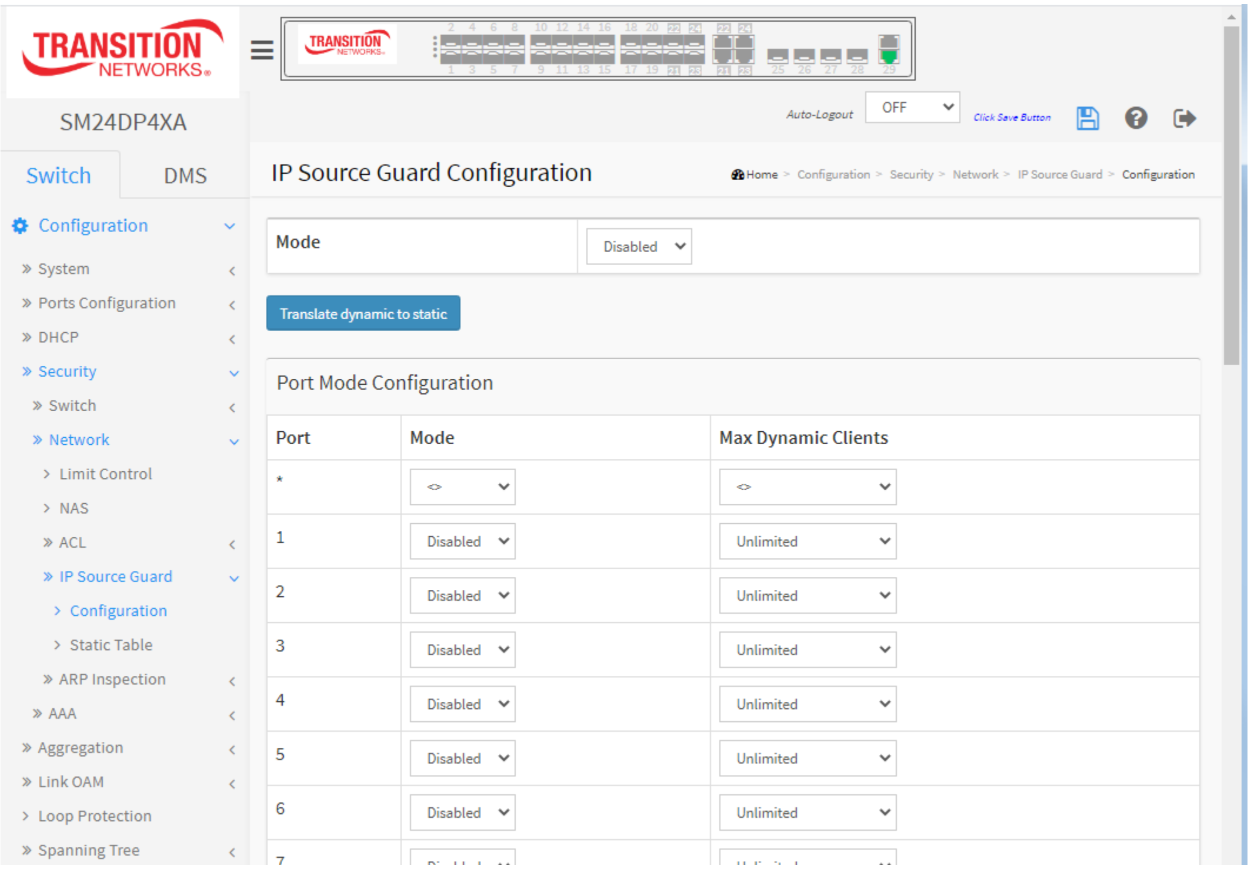
This page lets you to configure IP Source Guard setting including Mode (Enabled and Disabled) and Max Dynamic Clients (0, 1, 2, Unlimited).

Web Interface

To configure an IP Source Guard Configuration in the web interface:

1. Select Configuration, Security, Network, IP Source Guard, Configuration.
2. Select “Enabled” in the Mode of IP Source Guard Configuration.
3. Select “Enabled” for specific port(s) in the Mode column of the Port Mode Configuration section.
4. Select Maximum Dynamic Clients for the specific port in the Maximum Dynamic Clients column of the Port Mode Configuration section.
5. Click Apply.

Figure 2-4.2.5. 1: IP Source Guard Configuration



IP Source Guard Configuration

Mode	Disabled

Port Mode Configuration

Port	Mode	Max Dynamic Clients
*	<>	<>
1	Disabled	Unlimited
2	Disabled	Unlimited
3	Disabled	Unlimited
4	Disabled	Unlimited
5	Disabled	Unlimited
6	Disabled	Unlimited
7	Disabled	Unlimited

Parameter descriptions:

Mode of IP Source Guard Configuration **:** At the dropdown, enable or disable Global IP Source Guard globally. 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 Clients is 0, then the switch only allows forwarding IP packets that are matched in static entries on the specific port.

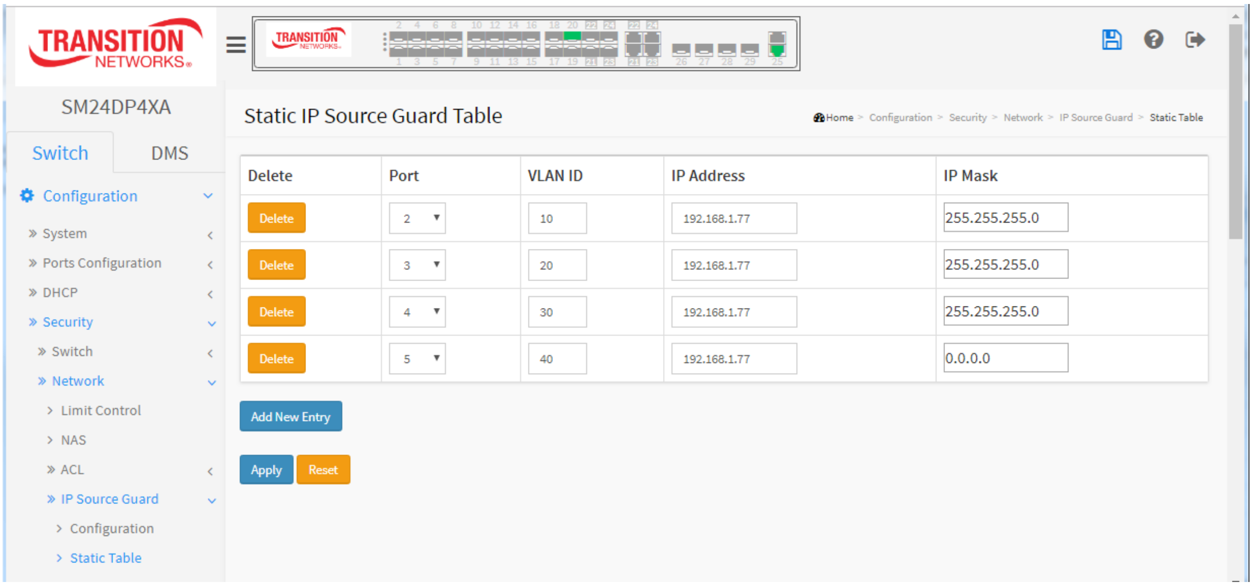
Buttons:

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.

Example:



Static IP Source Guard Table

Delete	Port	VLAN ID	IP Address	IP Mask
Delete	2	10	192.168.1.77	255.255.255.0
Delete	3	20	192.168.1.77	255.255.255.0
Delete	4	30	192.168.1.77	255.255.255.0
Delete	5	40	192.168.1.77	0.0.0.0

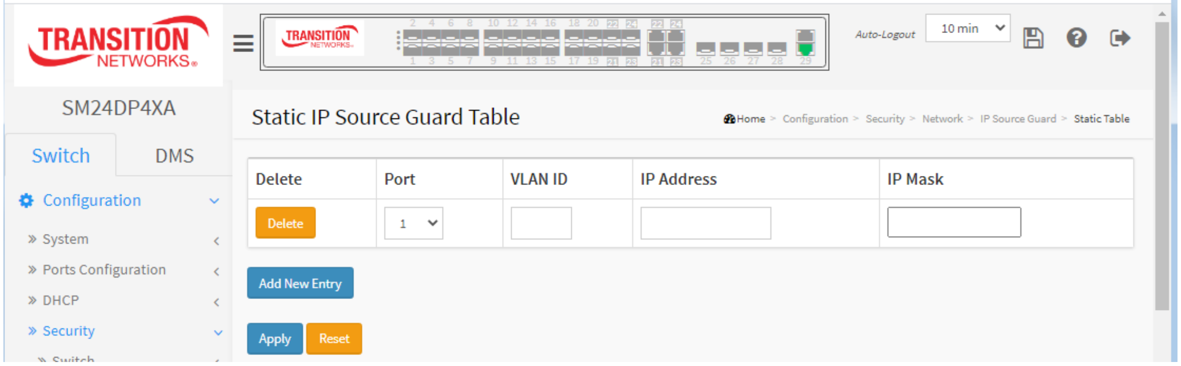
2-4.2.5.2 Static Table

This page lets you configure the Static IP Source Guard Table parameters of the switch. You can use the Static IP Source Guard Table configure to manage the entries.

To configure Static IP Source Guard Table parameters in the web UI:

1. Click Configuration, Security, Network, IP Source Guard, Static Table.
2. Click Add New Entry.
2. Specify the Port, VLAN ID, IP Address, and IP Mask for the entry.
3. Click Apply.

Figure 2-4.2.5.2: Static IP Source Guard Table



Static IP Source Guard Table

Delete	Port	VLAN ID	IP Address	IP Mask
Delete	1			

Add New Entry

Apply Reset

Delete : Check to delete the entry immediately.

Port : The logical port for the settings.

VLAN ID : The VLAN ID (VID) for the settings.

IP Address : Allowed Source IP address.

IP Mask : It can be used for calculating the allowed network with IP address.

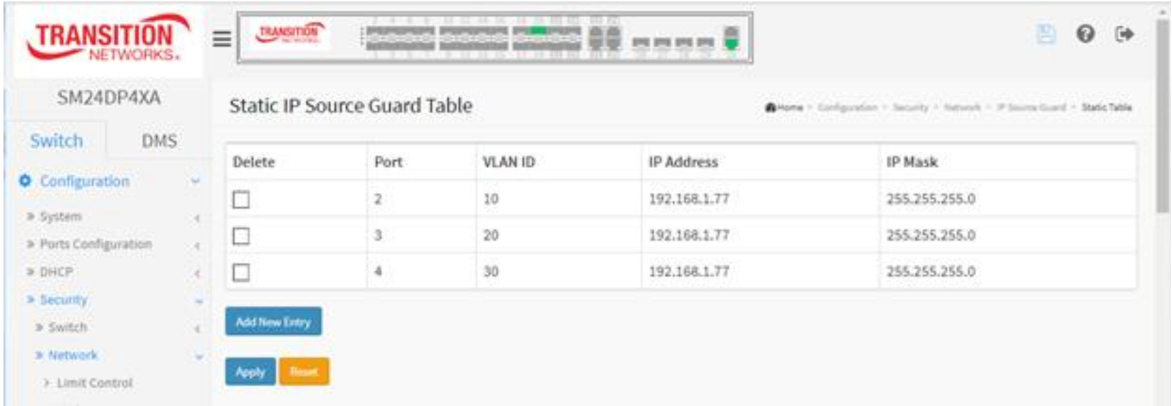
Add New Entry : Click to add a new entry to the Static IP Source Guard table. Specify the Port, VLAN ID, IP address, and IP Mask for the new entry.

Buttons:

Apply – Click to save changes.

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

Example:



Static IP Source Guard Table

Delete	Port	VLAN ID	IP Address	IP Mask
□	2	10	192.168.1.77	255.255.255.0
□	3	20	192.168.1.77	255.255.255.0
□	4	30	192.168.1.77	255.255.255.0

Add New Entry

Apply Reset

2-4.2.6 ARP Inspection

This page lets you configure the ARP Inspection parameters of the switch. You can use the ARP Inspection configure to manage the ARP table.

2-4.2.6.1 Configuration

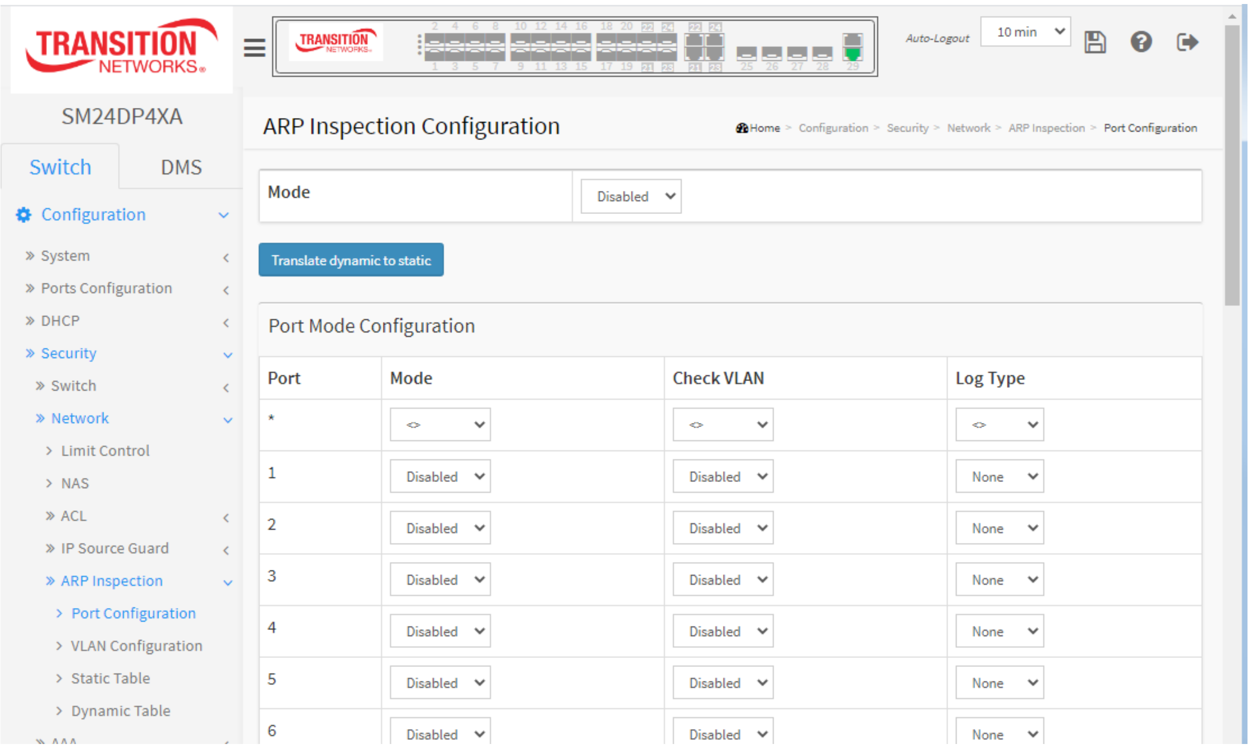
This page lets you to configure ARP Inspection setting including Mode (Enabled and Disabled) and Port (Enabled and Disabled).

Web Interface

To configure an ARP Inspection Configuration in the web interface:

1. Select Configuration, Security, Network, ARP Inspection, Port Configuration.
2. Select “Enabled” at the Mode dropdown of the ARP Inspection Configuration.
3. Select “Enabled” of the specific port at the Mode dropdown of the Port Mode Configuration section.
4. Click Apply.

Figure 2-4.2.6.1: ARP Inspection Configuration



ARP Inspection Configuration

Mode	Disabled

Translate dynamic to static

Port Mode Configuration

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 **:** at the dropdown enable or disable ARP Inspection globally.

Port Mode Configuration : Specify ARP Inspection is enabled on which ports. Only when both Global Mode and Port Mode on a given port are enabled, ARP Inspection is enabled on this given port. Possible modes are:

> ***Enabled***: Enable ARP Inspection operation.
>
> ***Disabled***: Disable ARP Inspection operation.

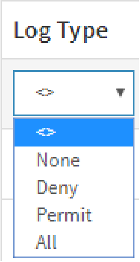
Check VLAN : To inspect the VLAN configuration, you must enable the setting of "Check VLAN". The default setting is disabled. When "Check VLAN" is disabled, the log type of ARP Inspection will refer to the port setting. When "Check VLAN" is enabled, the log type of ARP Inspection will refer to the VLAN setting. Possible setting of "Check VLAN" are:

Enabled: Enable check VLAN operation.

Disabled: Disable check VLAN operation.

The log type of ARP Inspection will refer to the port setting only when the Global Mode and Port Mode on a given port are enabled, and the setting of "Check VLAN" is disabled.

Log Type : Select one of the four log types:



None: Log nothing.

Deny: Log denied entries.

Permit: Log permitted entries.

Al: Log all entries.

Buttons:

Apply : Click to save changes.

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

Translate dynamic to static: Click to translate all dynamic entries to static entries.

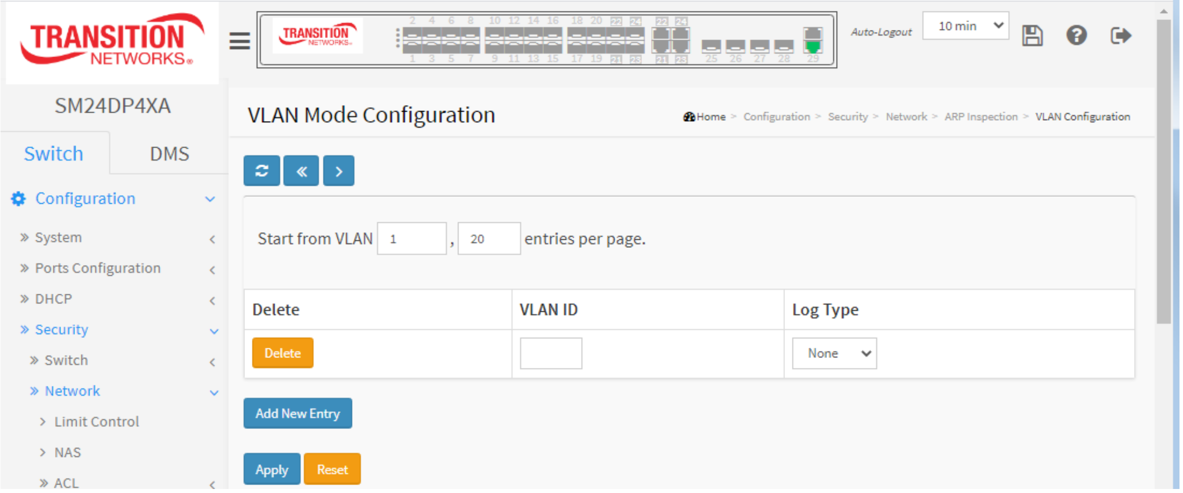
2-4.2.6.2 VLAN Mode Configuration

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 allow the user to select the starting point in the VLAN Table. Clicking the Refresh button will update the displayed table starting from that or the closest next VLAN Table match. The Next Entry (**>**) button will use the next entry of the currently displayed VLAN entry as a basis for the next lookup. When the end is reached the warning message is shown in the displayed table. Use the First Entry (**<<**) button to start over.

To configure a VLAN Mode Configuration in the web interface:

1. Click Configuration, Security, Network, ARP Inspection, Dynamic Table.
2. Click “Add New Entry”.
3. Specify the VLAN ID and Log Type.
4. Click Apply.

Figure 2-4.2.6.2: VLAN Mode Configuration



VLAN Mode Configuration

Start from VLAN 1 , 20 entries per page.

Delete	VLAN ID	Log Type
Delete		None

Add New Entry

Apply Reset

Parameter descriptions:

VLAN Mode Configuration : Specify ARP Inspection is enabled on which VLANs. First, you must enable the port setting on Port mode configuration web page. Only when both Global Mode and Port Mode on a given port are enabled, ARP Inspection is enabled on this given port. Second, you can specify which VLAN will be inspected on VLAN mode configuration web page. The log type also can be configured on a per-VLAN basis. Possible Log Types are:

None: Log nothing.

Deny: Log denied entries.

Permit: Log permitted entries.

ALL: Log all entries.

Buttons

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

Apply: Click to save changes.

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

2-4.2.6.3 Static Table

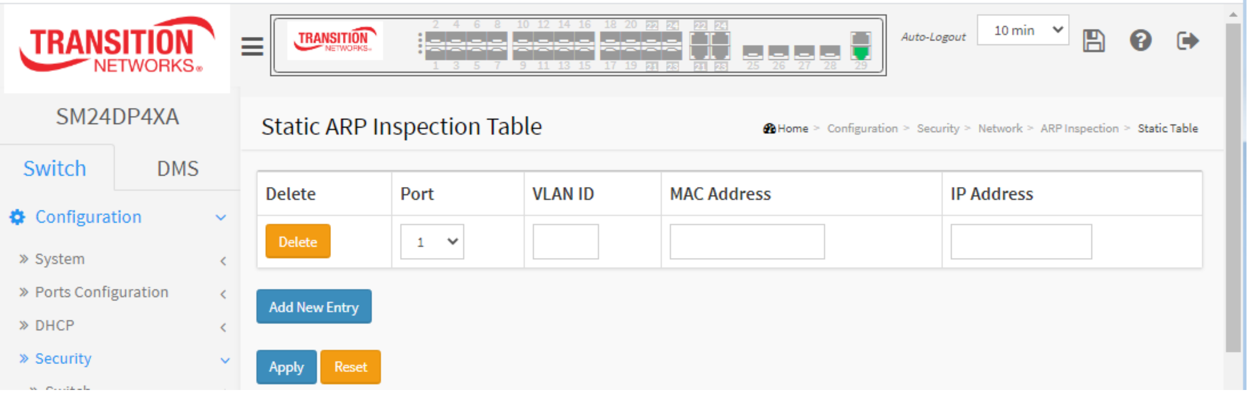
This page lets you configure the Static ARP Inspection Table parameters of the switch. You can use the Static ARP Inspection Table configure to manage the ARP entries.

Web Interface

To configure a Static ARP Inspection Table Configuration in the web interface:

1. Click Configuration, Security, Network, ARP Inspection, Static Table.
2. Click the Add New Entry button.
3. Specify the Port, VLAN ID, MAC address, and IP Address for the entry.
4. Click Apply.

Figure 2-4.2.6.3: Static ARP Inspection Table



Static ARP Inspection Table

Delete	Port	VLAN ID	MAC Address	IP Address
Delete	1			

Parameter descriptions:

Delete : Check to delete the entry immediately.

Port : The logical port for the settings.

VLAN ID : The VLAN ID (VID) for the settings.

MAC Address : Allowed Source MAC address in ARP request packets.

IP Address : Allowed Source IP address in ARP request packets.

Buttons:

Add New Entry : Click to add a new entry to the Static ARP Inspection table. Specify the Port, VLAN ID, MAC address, and IP address for the new entry. Click "Apply".

Save – Click to save changes.

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

2-4.2.6.4 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 Dynamic 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 **Refresh** button will update the displayed table starting from that or the closest next Dynamic ARP Inspection Table match. In addition, the two input fields will - upon a **Refresh** button click - assume the value of the first displayed entry, allowing for continuous refresh with the same start address.

The **>** button will use the last entry of the currently displayed table as a basis for the next lookup.
The last entry of the currently displayed table is used as the basis for the next lookup. When the end is reached the text "*No more entries*" is displayed. Use the **<<** button to start over.

Web Interface

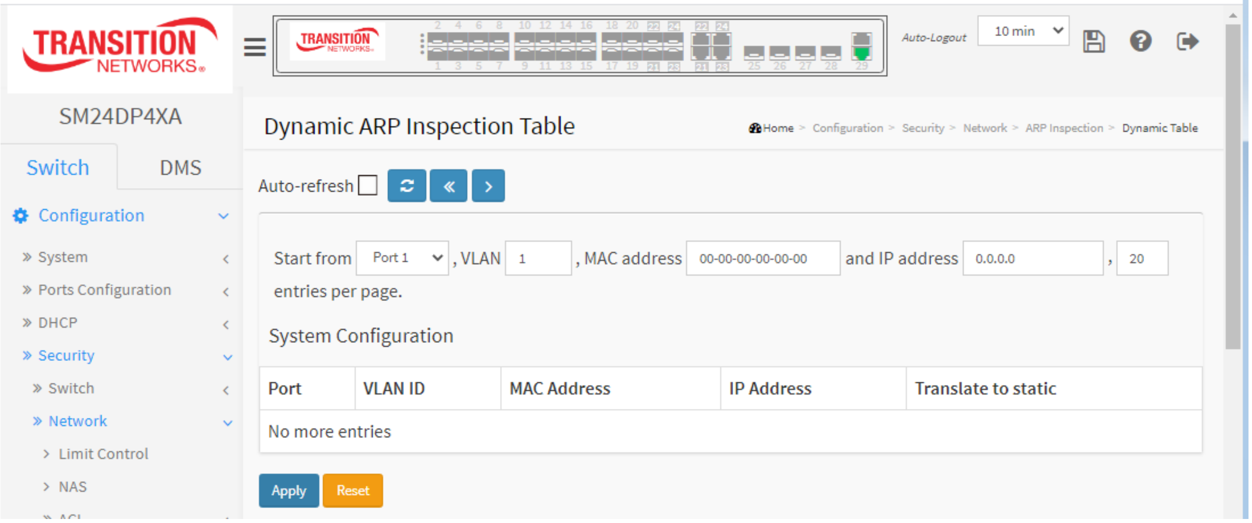
To configure a Dynamic ARP Inspection Table Configuration in the web interface:

1. Click Configuration, Security, Network, ARP Inspection, Dynamic Table.

2. Select the Start from , VLAN , MAC address and IP address, and entries per page parameters.

3. View the table entries.

Figure 2-4.2.6.3: Dynamic ARP Inspection Table



Dynamic ARP Inspection Table

Auto-refresh ☐ « >

Start from Port 1, VLAN 1, MAC address 00-00-00-00-00-00 and IP address 0.0.0.0, 20 entries per page.

System Configuration

Port	VLAN ID	MAC Address	IP Address	Translate to static
No more entries				

Apply Reset

Parameter descriptions:

ARP Inspection Table Columns

Port : Switch Port Number for which the entries are displayed.

VLAN ID : VLAN-ID in which the ARP traffic is permitted.

MAC Address : User MAC address of the entry.

IP Address : User IP address of the entry.

Translate to static : Select the checkbox to translate the entry to static entry.

Buttons:

Apply : Click to save changes.

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

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

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

<< : 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

2-4.3 AAA

This section shows you to use an 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.

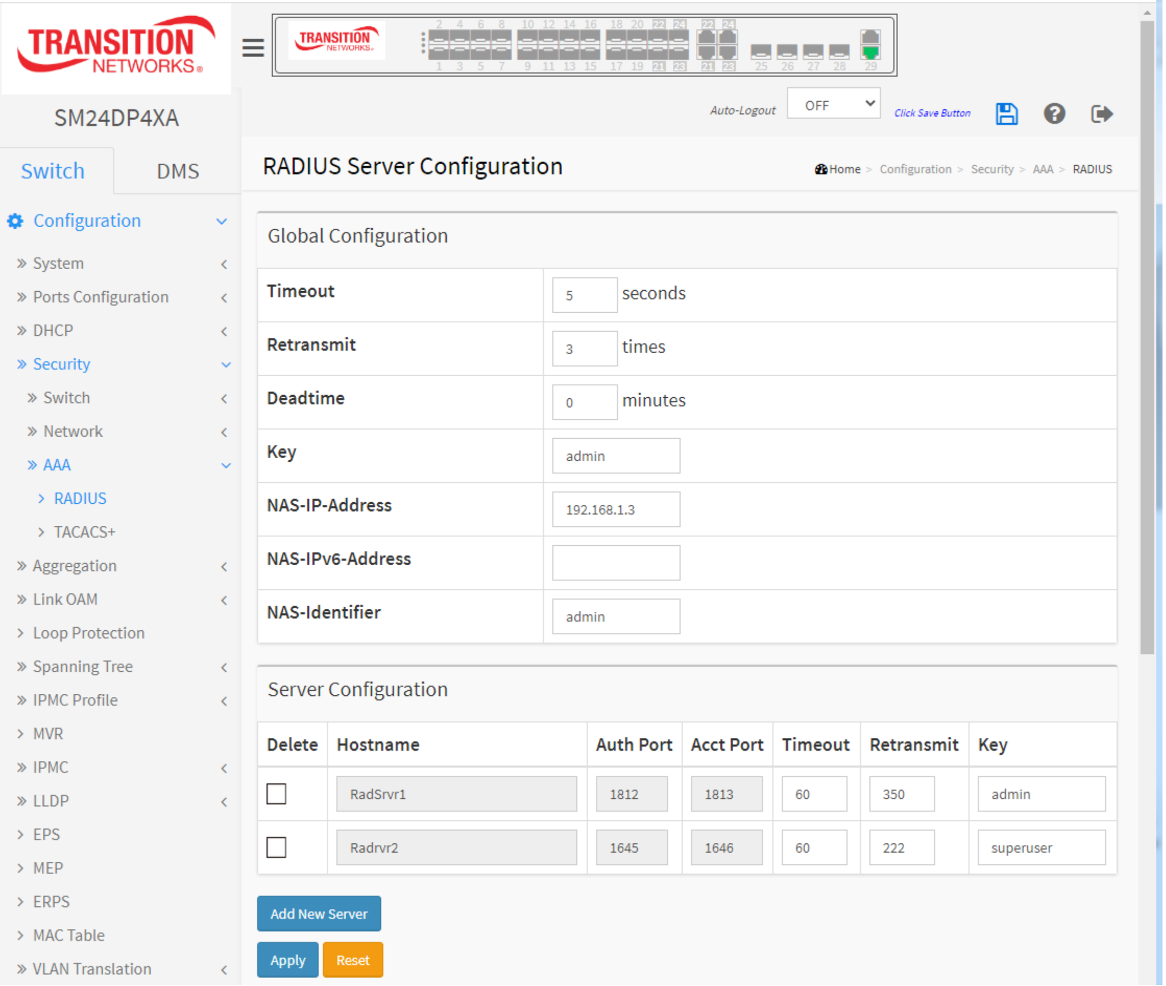
2-4.3.1 RADIUS

Web Interface

To configure a RADIUS in the web UI:

1. Click Configuration, Security, AAA, RADIUS.
2. Enter the Global Configuration section parameters.
3. Click the Add New Server button and enter the Server Configuration section parameters.
4. Click the Apply button to save the changes to the running-config file.

Figure 2-4.3.1: RADIUS Server Configuration



RADIUS Server Configuration

Global Configuration

Timeout	5 seconds
Retransmit	3 times
Deadtime	0 minutes
Key	admin
NAS-IP-Address	192.168.1.3
NAS-IPv6-Address	
NAS-Identifier	admin

Server Configuration

Delete	Hostname	Auth Port	Acct Port	Timeout	Retransmit	Key
□	RadSrvr1	1812	1813	60	350	admin
□	Radrvr2	1645	1646	60	222	superuser

<u>**Global Configuration**</u> : These setting 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 (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 several columns:

Delete : To delete a RADIUS server entry, check this box.

Hostname : The IP address or hostname of the RADIUS server. Hostname must be a valid hostname, unicast IPv4, or unicast IPv6 address.

Auth Port : The UDP port to use on the RADIUS server for authentication. The officially assigned port number for RADIUS Accounting is 1812. Note: by default, many access servers use port 1645 for authentication requests.

> **Note**: For Windows Server information on how to configure ports that Network Policy Server (NPS) uses for Remote Authentication Dial-In User Service (RADIUS) authentication and accounting traffic see https://docs.microsoft.com/en-us/windows-server/networking/technologies/nps/nps-udp-ports-configure#:~:text=The%20port%20values%20of%201812,and%201646%20for%20accounting%20requests

Acct Port : The UDP port to use on the RADIUS server for accounting. The officially assigned port number for RADIUS Accounting is 1813. Note: by default, many access servers use port 1646 for accounting requests.

Timeout : This optional setting overrides the global timeout value. Leaving it blank will use the global timeout value.

Retransmit : This optional setting overrides the global retransmit value. Leaving it blank will use the global retransmit value.

Key : This optional setting overrides the global key. Leaving it blank will use the global key.

Buttons

Add New 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.

Delete : Click the button to undo the addition of the new server.

Apply : Click to save changes.

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

2-4.3.2 TACACS+

Up to 5 servers are supported. TACACS+ (Terminal Access Controller Access Control System Plus) is a networking protocol which provides access control for routers, network access servers and other networked computing devices via one or more centralized servers. TACACS+ provides separate authentication, authorization and accounting services.

Web Interface

To configure a TACACS+ via the web interface:

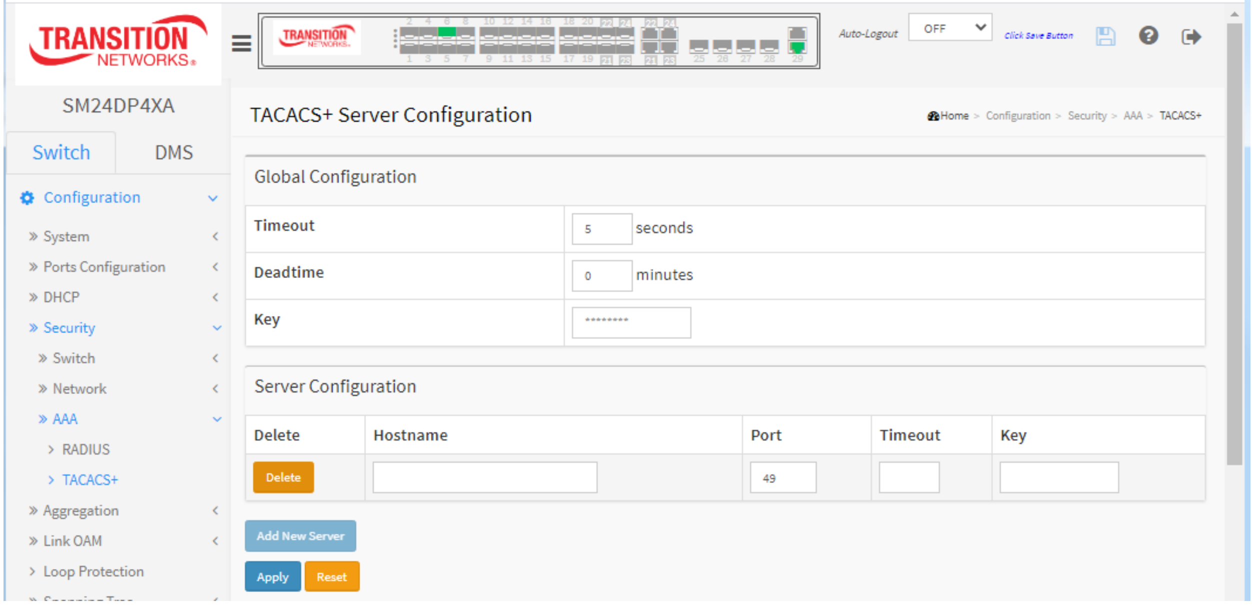
1. Click Configuration, Security, AAA, TACACS+.

2. Enter the Global Configuration parameters.

3. Click the Add New Server button and enter the Server Configuration parameters.

4. Click the Apply button to save the settings to the running-config file.

Figure 2-4.3.2: TACACS+ Server Configuration



TACACS+ Server Configuration

Global Configuration

Timeout	5 seconds
Deadtime	0 minutes
Key	••••••••

Server Configuration

Delete	Hostname	Port	Timeout	Key
Delete		49		

Add New Server

Apply Reset

Parameter descriptions:

Global Configuration : These setting are common for all TACACS+ servers.

Timeout : Timeout is the number of seconds, in the range 1 - 1000, to wait for a reply from a TACACS+ server before it is considered to be dead.

Deadtime : Deadtime (0 - 1440 minutes) is the period during which the switch will not send new requests to a server that has failed to respond to a previous request. This will stop the switch from continually trying to contact a server that it has already determined as dead. Setting the Dead time 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 several columns:

Delete : To delete a TACACS+ server entry immediately, check this box.

Hostname : The IP address or hostname of the TACACS+ server.

Port : The TCP port to use on the TACACS+ server for authentication.

Timeout : This optional setting overrides the global timeout value. Leaving it blank will use the global timeout value.

Key : This optional setting overrides the global key. Leaving it blank will use the global key.

Buttons

Add New Server : Click to add a new TACACS+ server. An empty row is added to the table, and the TACACS+ server can be configured as needed. Up to 5 servers are supported.

Delete : Click the button to undo the addition of the new server.

Apply: Click to save changes.

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

2-5 Aggregation

The 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.

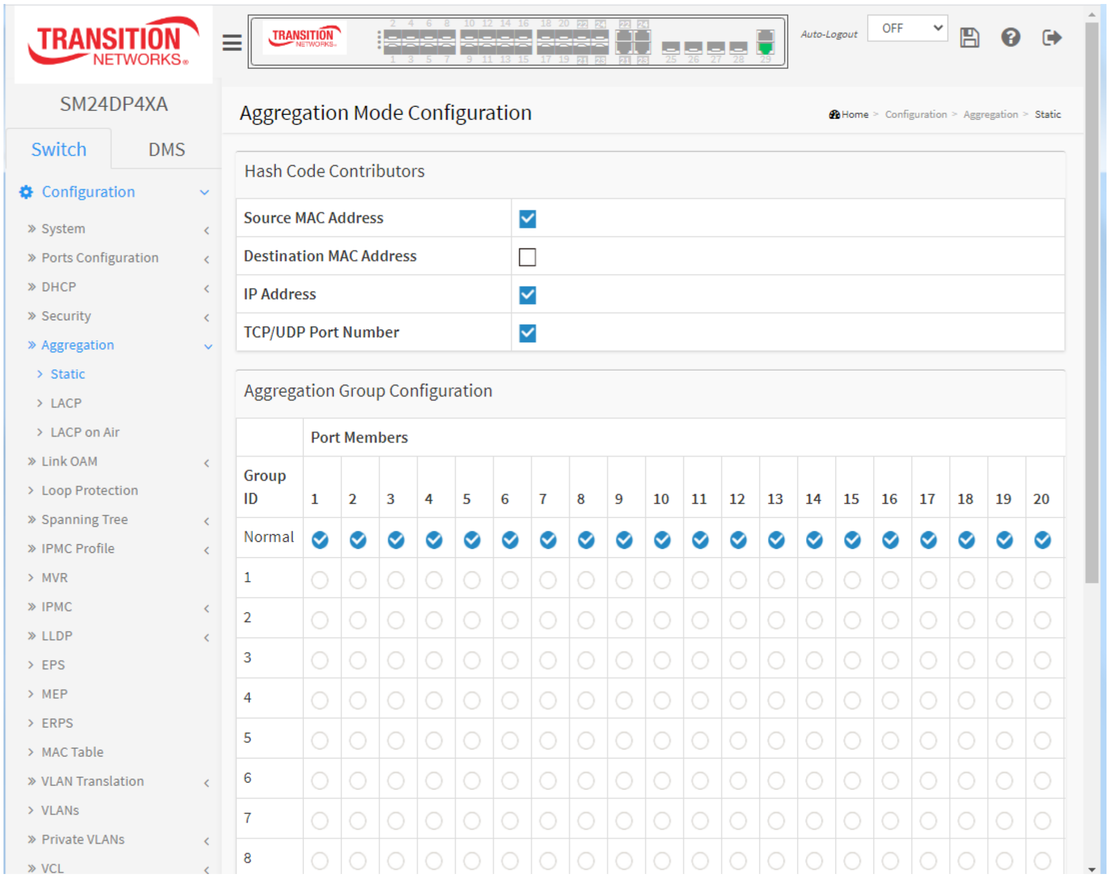
2-5.1 Static

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 ends of a link is strongly recommended. Please also note that low speed links will stay in "not ready" state when using static trunk to aggregate with high speed links.

To configure the Trunk Aggregation Hash mode and Aggregation Group via the web UI:

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

Figure 2-5.1: Aggregation Mode Configuration



Aggregation Mode Configuration

Hash Code Contributors

Source MAC Address	☑
Destination MAC Address	☐
IP Address	☑
TCP/UDP Port Number	☑

Aggregation Group Configuration

	Port Members																			
Group ID	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
Normal	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●
1	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○
2	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○
3	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○
4	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○
5	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○
6	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○
7	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○
8	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○

Parameter descriptions:

<u>Hash Code Contributors</u>

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.

<u>Aggregation Group Configuration</u>

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

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

Buttons

Save – Click to save changes.

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

Message: *The aggregation must include 2-8 ports*

2-5.2 LACP

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

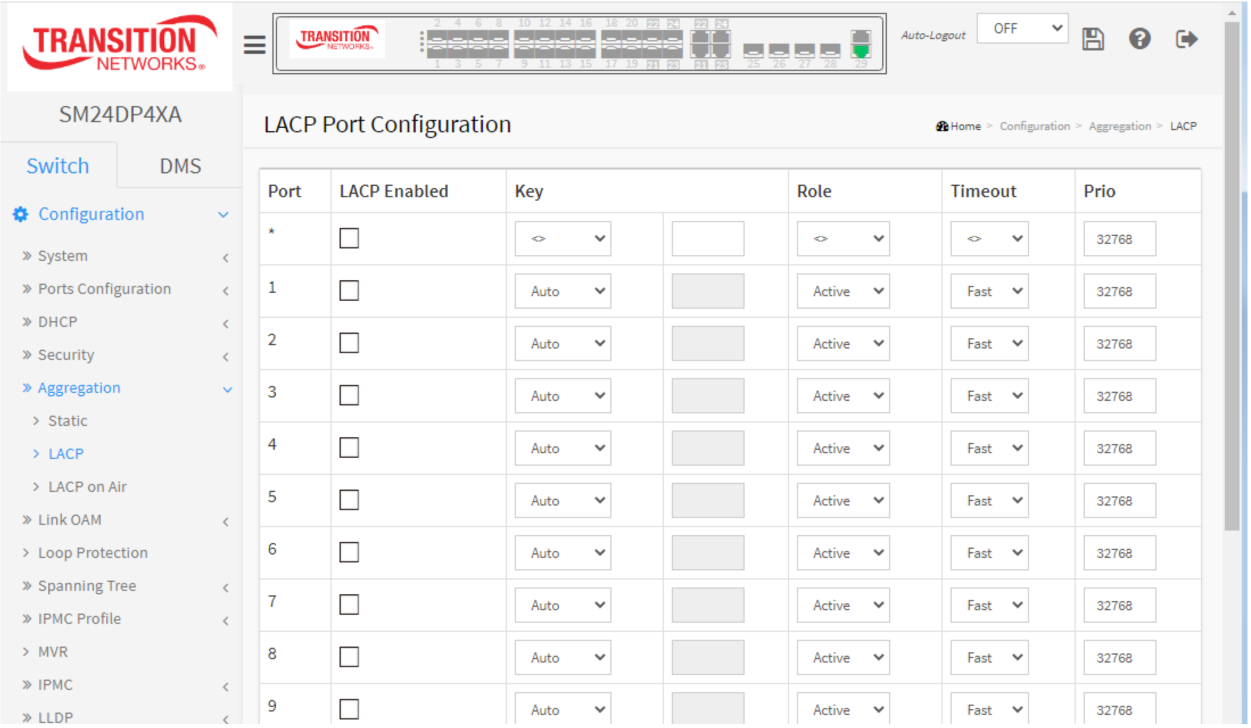
LACP is an IEEE 802.3ad standard protocol. The Link Aggregation Control Protocol allows bundling several physical ports together to form a single logical port. An LACP trunk group with more than one ready member port is a “real trunked” group. An LACP trunk group with only one or less than one ready member port is not a “real trunked” group.

Web Interface

To configure the Trunk Aggregation LACP parameters via the web UI:

1. Click Configuration, Aggregation, LACP.
2. Enable LACP on the switch ports.
3. Select the Key parameter (Auto or Specific). The default is Auto.
4. Select the Role (Active or Passive). The default is Active.
5. Click the Apply button to save the settings.
6. To cancel the settings click the Reset button. It will revert to previously saved values.

Figure 2-5.2: LACP Port Configuration



LACP Port Configuration

Port	LACP Enabled	Key		Role	Timeout	Prio
*	□	<>		<>	<>	32768
1	□	Auto		Active	Fast	32768
2	□	Auto		Active	Fast	32768
3	□	Auto		Active	Fast	32768
4	□	Auto		Active	Fast	32768
5	□	Auto		Active	Fast	32768
6	□	Auto		Active	Fast	32768
7	□	Auto		Active	Fast	32768
8	□	Auto		Active	Fast	32768
9	□	Auto		Active	Fast	32768

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, in the range 1-65535. The ***Auto*** setting will set the key according to the physical link speed: 10Mb = 1, 100Mb = 2, 1 Gb= 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 : Shows the LACP activity status. ***Active*** will transmit LACP packets each second, while ***Passive*** will wait for a LACP packet from a partner (speak if spoken to).

Timeout : Controls the period between BPDU transmissions.

Fast will transmit LACP packets each second.

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

Prio : Controls the priority of the port. If the LACP partner wants to form a larger group than is supported by this device then this parameter will control which ports will be active and which ports will be in a backup role. A lower number means greater priority.

Buttons

Save – Click to save changes.

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

Previous : Click to clear an LACP Error.

Message:

LACP Error *LACP cannot be enabed on ports whose 802.1X Admin State is not Authorized*

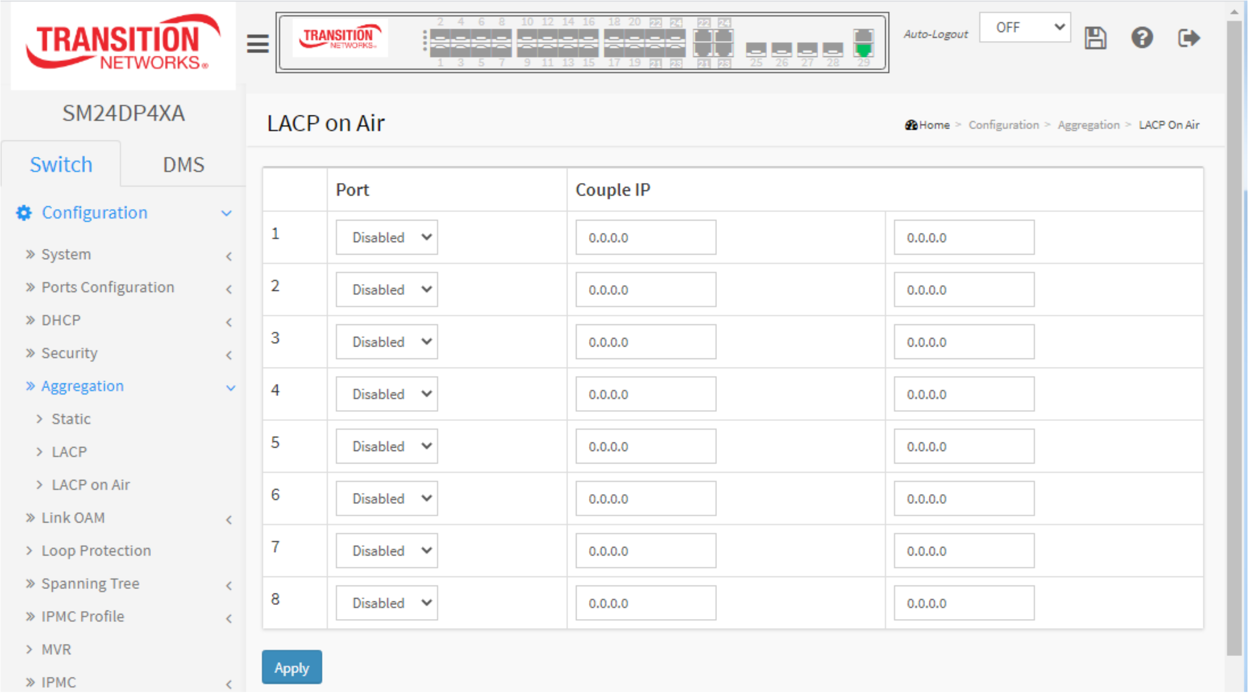
2-5.3 LACP on Air

This page lets you view and configure the current LACP on Air ports, and the Couple IP address for the access management.

To configure the LACP on Air parameters via the web interface:

1. Click Configuration, Aggregation, LACP.
2. Enable LACP on Air for the desired switch ports.
3. Enter Couple IP addresses.
4. Click the Apply button to save the settings.

Figure 2-5.3: LACP on Air Configuration



LACP on Air

	Port	Couple IP	
1	Disabled	0.0.0.0	0.0.0.0
2	Disabled	0.0.0.0	0.0.0.0
3	Disabled	0.0.0.0	0.0.0.0
4	Disabled	0.0.0.0	0.0.0.0
5	Disabled	0.0.0.0	0.0.0.0
6	Disabled	0.0.0.0	0.0.0.0
7	Disabled	0.0.0.0	0.0.0.0
8	Disabled	0.0.0.0	0.0.0.0

Parameter descriptions:

Port : Select which switch port(s) should have access to Couple IP device management.

Couple IP : Specify the connected partners for access management.

Buttons

Apply: Click to save changes.

2-6 Link OAM

2-6.1 Port Settings

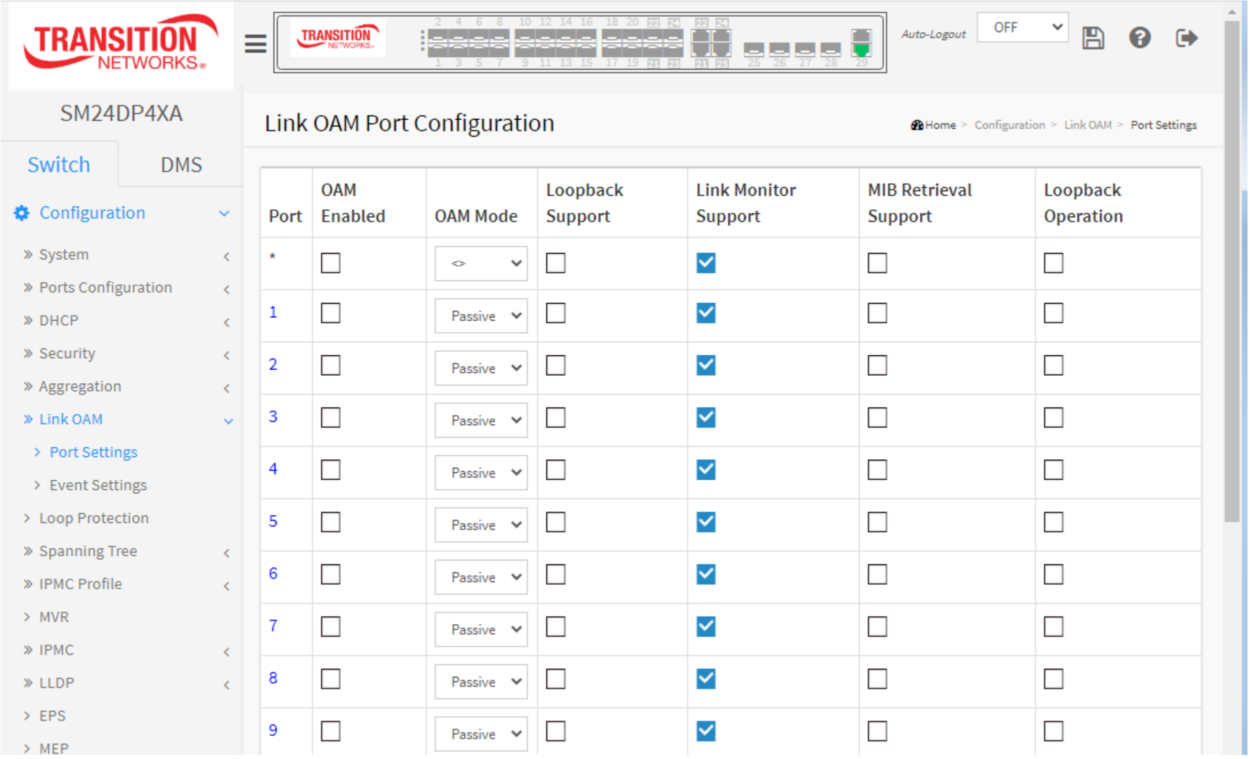
This page lets you view and configure the current Link OAM port parameters. Link OAM (Operation Administration and Maintenance is a protocol described in ITU-T Y.1731 used to implement Carrier Ethernet functionality. MEP functions such as CC and RDI are based on OAM.

Web Interface

To configure the Link OAM Port Configuration via the web interface:

1. Click Configuration, Link OAM, Port Settings.
2. Select the OAM Enabled and OAM Mode parameters.
3. Enable or disable Loopback Support, Link Monitor Support, MIB Retrieval Support, and Loopback Operation.

Figure 2-6.1: Link OAM Port Configuration



Link OAM Port Configuration

Port	OAM Enabled	OAM Mode	Loopback Support	Link Monitor Support	MIB Retrieval Support	Loopback Operation
*	☐	<>	☐	☑	☐	☐
1	☐	Passive	☐	☑	☐	☐
2	☐	Passive	☐	☑	☐	☐
3	☐	Passive	☐	☑	☐	☐
4	☐	Passive	☐	☑	☐	☐
5	☐	Passive	☐	☑	☐	☐
6	☐	Passive	☐	☑	☐	☐
7	☐	Passive	☐	☑	☐	☐
8	☐	Passive	☐	☑	☐	☐
9	☐	Passive	☐	☑	☐	☐

Parameter descriptions:

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

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

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

> ***Active***: DTE's configured in Active mode initiate the exchange of Information OAMPDUs as defined by the Discovery process. Once the Discovery process completes, Active DTE's are permitted to send any OAMPDU while connected to a remote OAM peer entity in Active mode.

Active DTE's operate in a limited respect if the remote OAM entity is operating in Passive mode. Active devices should not respond to OAM remote loopback commands and variable requests from a Passive peer.

Passive: DTE's configured in Passive mode do not initiate the Discovery process. Passive DTE's react to the initiation of the Discovery process by the remote DTE. This eliminates the possibility of passive to passive links. Passive DTE's shall not send Variable Request or Loopback Control OAMPDUs.

Loopback Support : Controls whether the loopback support is enabled for the switch port. Link OAM remote loopback can be used for fault localization and link performance testing. Enabling the loopback support will allow the DTE to execute the remote loopback command that helps in the fault detection.

Link Monitor Support : Controls whether the Link Monitor support is enabled for the switch port. On enabling the Link Monitor support, the DTE supports event notification that permits the inclusion of diagnostic information.

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

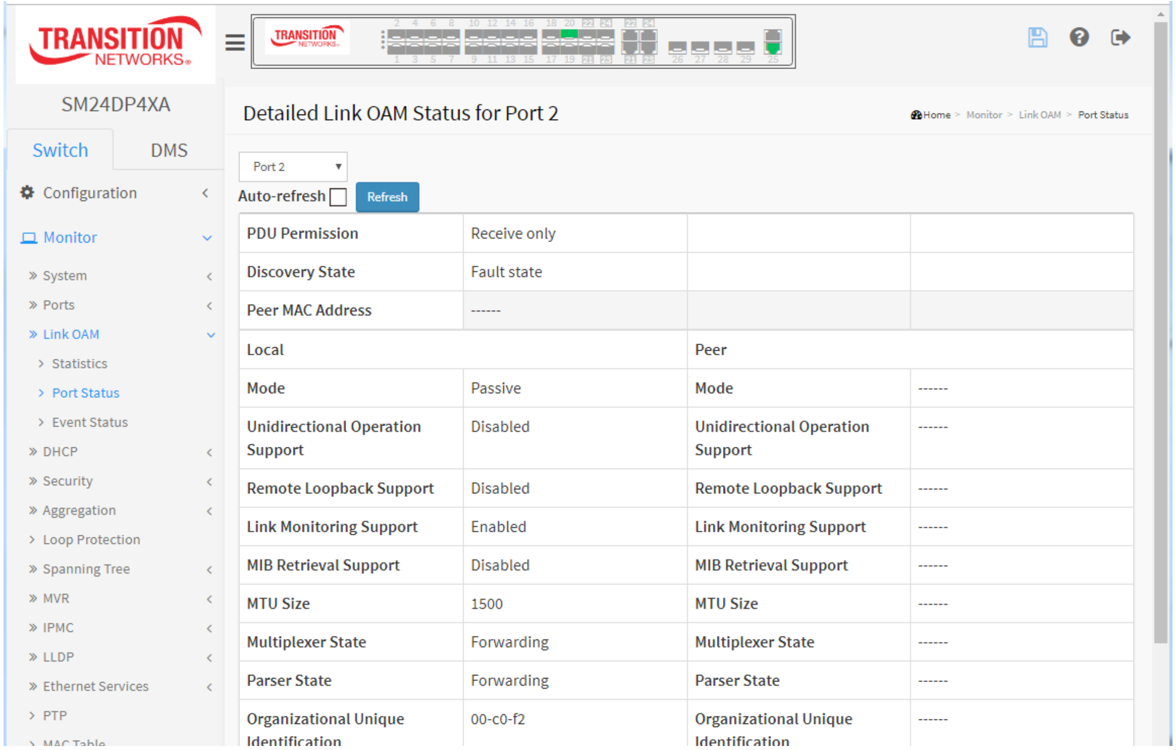
Loopback Operation : If the Loopback support is enabled, enabling this field will start a loopback operation for the port.

Buttons

Save – Click to save changes.

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

Detailed Link OAM Status:



Detailed Link OAM Status for Port 2

PDU Permission	Receive only		
Discovery State	Fault state		
Peer MAC Address	------		
Local		Peer	
Mode	Passive	Mode	------
Unidirectional Operation Support	Disabled	Unidirectional Operation Support	------
Remote Loopback Support	Disabled	Remote Loopback Support	------
Link Monitoring Support	Enabled	Link Monitoring Support	------
MIB Retrieval Support	Disabled	MIB Retrieval Support	------
MTU Size	1500	MTU Size	------
Multiplexer State	Forwarding	Multiplexer State	------
Parser State	Forwarding	Parser State	------
Organizational Unique Identification	00-c0-f2	Organizational Unique Identification	------

2-6.2 Event Settings

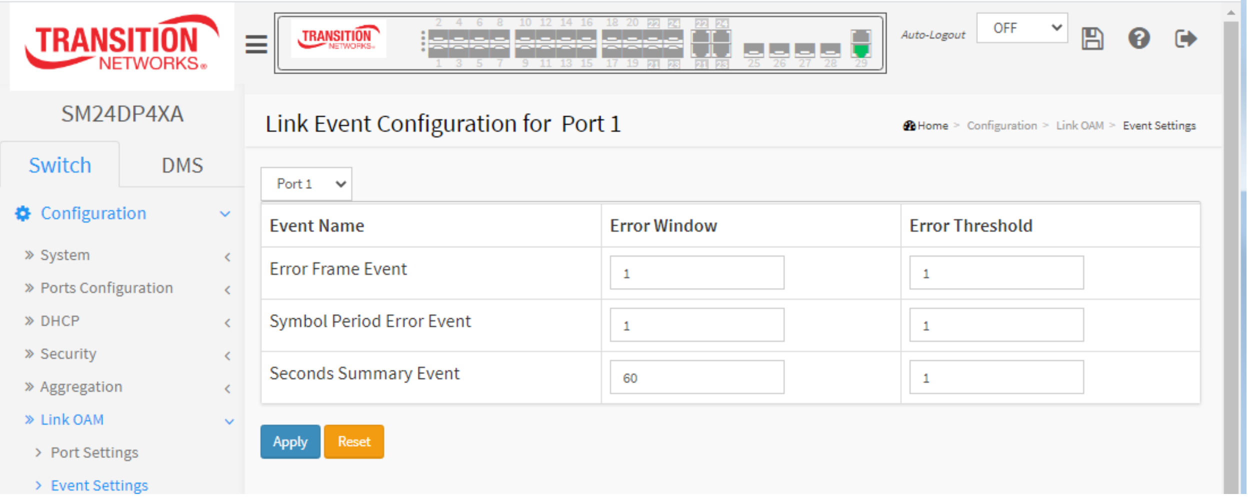
This page lets you view and configure the current Link OAM Link Event parameters.

Web Interface

To configure Link OAM Event parameters via the web interface:

1. Click Configuration, Link OAM, Event Settings.
2. Select a Port at the port select box.
3. For each Event Name, enter an Error Window and Error Threshold parameter.
4. Click the Apply button to save the settings.

Figure 2-6.2: Link OAM Event Configuration



Link Event Configuration for Port 1

Port 1

Event Name	Error Window	Error Threshold
Error Frame Event	1	1
Symbol Period Error Event	1	1
Seconds Summary Event	60	1

Parameter descriptions:

Port : The switch port number.

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

Error Window : Represents the window period in the order of 1 sec for the observation of various link events.

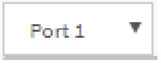
Error Threshold : Represents the threshold value for the window period for the appropriate Link event so as to notify the peer of this error.

Error Frame Event : The errored Frame Event counts the number of errored frames detected during the specified period. The period is specified by a time interval (Window in order of 1 sec). This event is generated if the errored frame count is equal to or greater than the specified threshold for that period (Period Threshold). Errored frames are frames that had transmission errors as detected at the Media Access Control sublayer. The Error Window for 'Error Frame Event' must be an integer 1-60 and its default value is '1'. The Error Threshold must be 0-0xffffffff and its default value is '0'.

Symbol Period Error Event : The Errored Symbol Period Event counts the number of symbol errors that occurred during the specified period. The period is specified by the number of symbols that can be received in a time interval on the underlying physical layer. This event is generated if the symbol error count is equal to or greater than the specified threshold for that period. Error Window for 'Symbol Period Error Event' must be an integer value between 1- 60 and its default value is '1'. Whereas Error Threshold must be between 0-0xffffffff and its default value is '0'.

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

Buttons



The port select box determines which port’s event information is displayed.

Apply : Click to save changes.

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

2-7 Loop Protection

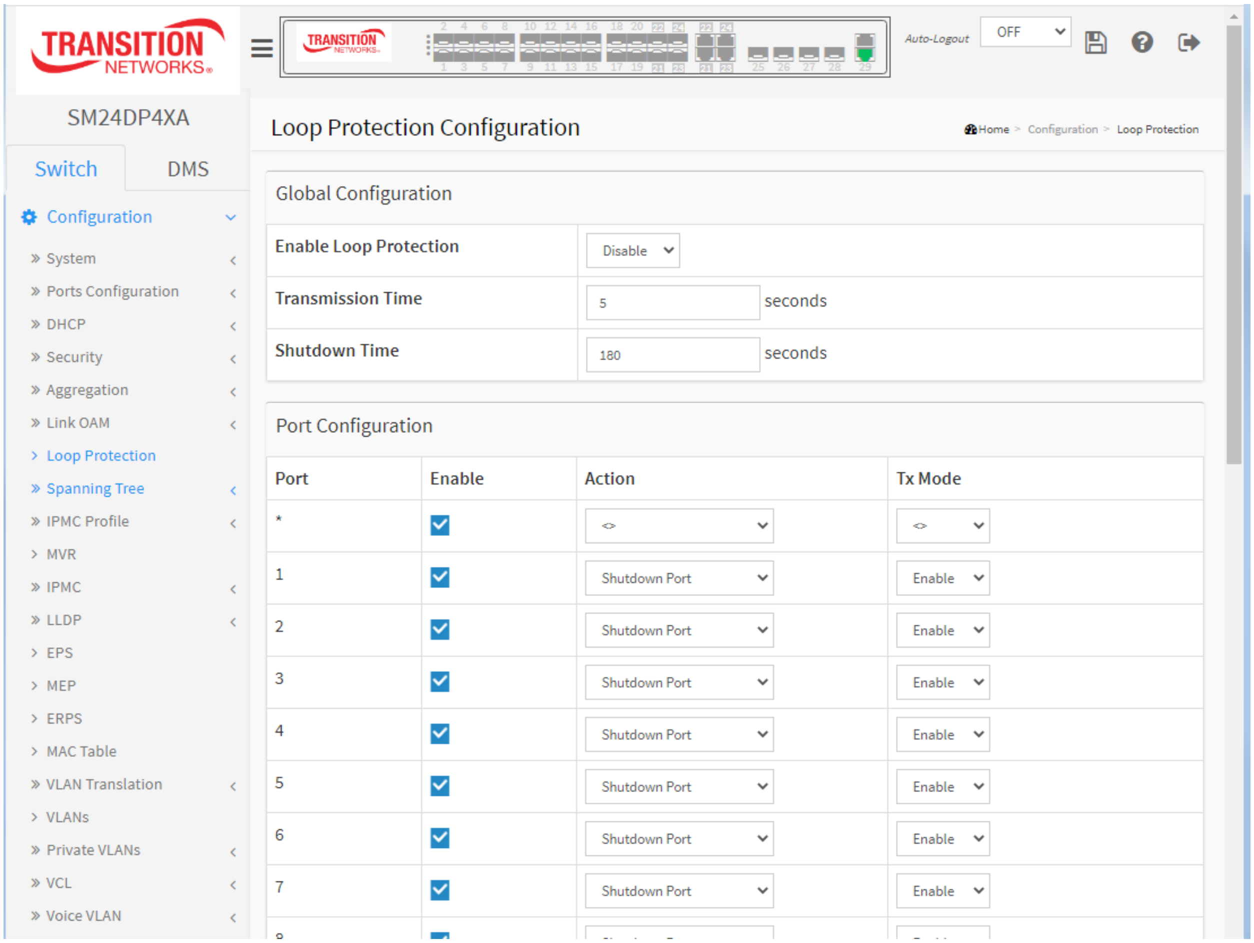
Loop Protection is used to detect the presence of traffic. When the switch receives packets (looping detection frame) from a MAC address the same as itself from a port, Loop Protection occurs.
The port will be locked when it receives the looping Protection frames. To resume the locked port, determine the looping path and remove 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 Loop Protection on the desired switch ports. The default is Disabled.
4. Select the Action and Tx Mode parameters.
5. Click the Apply button to save the settings.
6. To cancel the settings click the Reset button. It will revert to previously saved values.

Figure 2-7: Loop Protection Configuration



Loop Protection Configuration

Global Configuration

Enable Loop Protection	Disable
Transmission Time	5 seconds
Shutdown Time	180 seconds

Port Configuration

Port	Enable	Action	Tx Mode
*	☑	<>	<>
1	☑	Shutdown Port	Enable
2	☑	Shutdown Port	Enable
3	☑	Shutdown Port	Enable
4	☑	Shutdown Port	Enable
5	☑	Shutdown Port	Enable
6	☑	Shutdown Port	Enable
7	☑	Shutdown Port	Enable

Parameter descriptions:

Enable Loop Protection: Controls whether loop protections is enabled (globally).

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

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

Port No: 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:

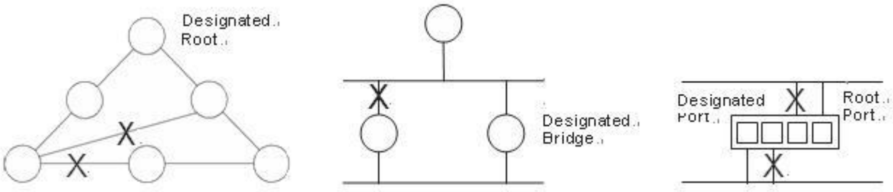
Apply : Click to save changes.

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

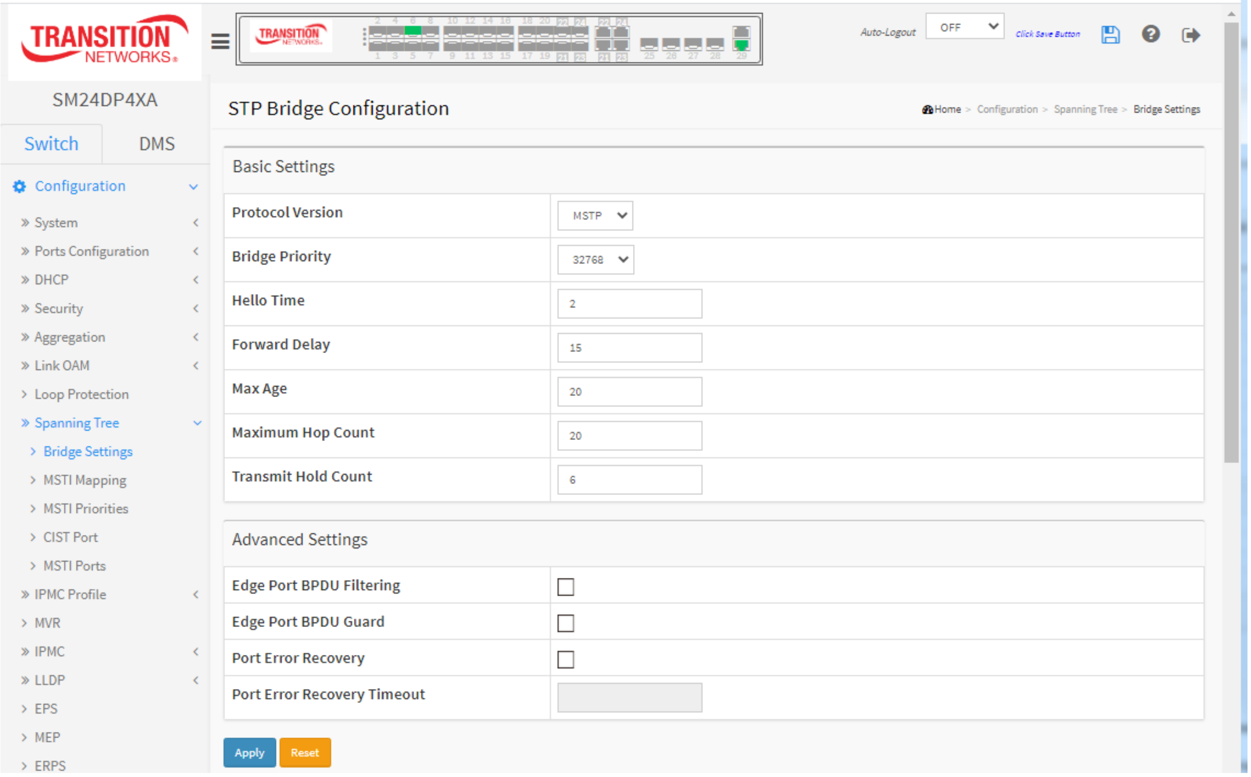
This page lets you configure the Spanning Tree Bridge and STP System settings. It allows you to configure STP System settings used by all STP Bridge instance in the switch.

Web Interface

To configure the Spanning Tree Bridge Settings parameters in the web interface:

1. Click Configuration, Spanning Tree, Bridge Settings.
2. Select and enter parameters in the Basic Settings fields.
3. Enable or disable the parameters and enter parameters in the Advanced Settings fields.
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



STP Bridge Configuration

Basic Settings

Protocol Version	MSTP
Bridge Priority	32768
Hello Time	2
Forward Delay	15
Max Age	20
Maximum Hop Count	20
Transmit Hold Count	6

Advanced Settings

Edge Port BPDU Filtering	☐
Edge Port BPDU Guard	☐
Port Error Recovery	☐
Port Error Recovery Timeout	

Parameter descriptions:

Basic Settings

Protocol Version : The STP protocol version setting. Valid values are STP, RSTP and MSTP.

> ***STP*** : The original Spanning Tree Protocol is an OSI layer-2 protocol which ensures a loop free topology for any bridged LAN. The original STP protocol is now obsolete by RSTP.
>
> In 1998, the IEEE with document 802.1w introduced an evolution of STP: the Rapid Spanning Tree Protocol, which provides for faster spanning tree convergence after a topology change. Standard IEEE 802.1D-2004 now incorporates RSTP and obsoletes STP, while at the same time being backwards-compatible with STP.
>
> ***RSTP*** : In 1998, the IEEE with document 802.1w introduced an evolution of STP: the Rapid Spanning Tree Protocol, which provides for faster spanning tree convergence after a topology change. Standard IEEE 802.1D-2004 now incorporates RSTP and obsoletes STP, while at the same time being backwards-compatible with STP.
>
> ***MSTP*** : In 2002, the IEEE introduced an evolution of RSTP: the Multiple Spanning Tree Protocol. The MSTP protocol provides for multiple spanning tree instances, while ensuring RSTP and STP compatibility. The standard was originally defined by IEEE 802.1s, but was later incorporated in IEEE 802.1D-2005.

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 - 40 seconds, and MaxAge must be <= (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 a Spanning Tree protocol on the switch that the bridge instance. The CIST is not available for explicit mapping, as it will receive the VLANs not explicitly mapped. Due to the reason that you need to set the list of VLANs mapped to the MSTI. The VLANs must be separated with comma and/or space. A VLAN can only be mapped to one MSTI. An unused MSTI should just be left empty (i.e., not have any VLANs mapped to it).

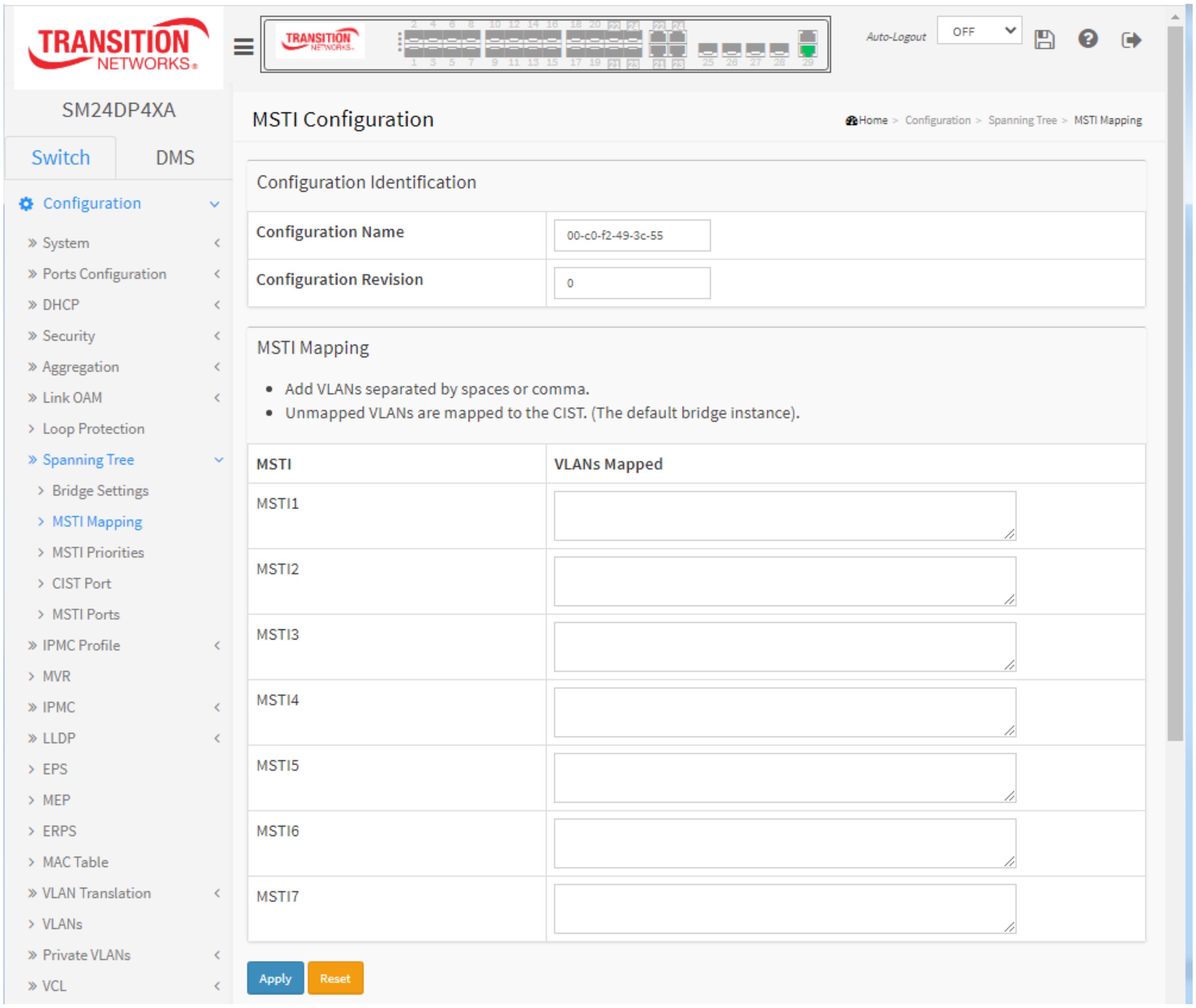
This page lets you view and configure the current STP MSTI bridge instance priority parameters.

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 in the fields.
3. Specify the VLANs Mapped blank field.
4. Click the Apply button to save the settings.
5. To cancel the settings click the Reset button. It will revert to previously saved values.

Figure 2-8.2: MSTI Configuration



MSTI Configuration

Configuration Identification

Configuration Name	00-c0-f2-49-3c-55
Configuration Revision	0

MSTI Mapping

- Add VLANs separated by spaces or comma.
- Unmapped VLANs are mapped to the CIST. (The default bridge instance).

MSTI	VLANs Mapped
MSTI1	
MSTI2	
MSTI3	
MSTI4	
MSTI5	
MSTI6	
MSTI7	

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

Buttons

Apply : Click to save changes.

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

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. The Priority (0-61440) controls the bridge priority. Lower numeric values have better priority. The bridge priority plus the MSTI instance number, concatenated with the 6-byte MAC address of the switch, forms a Bridge Identifier.

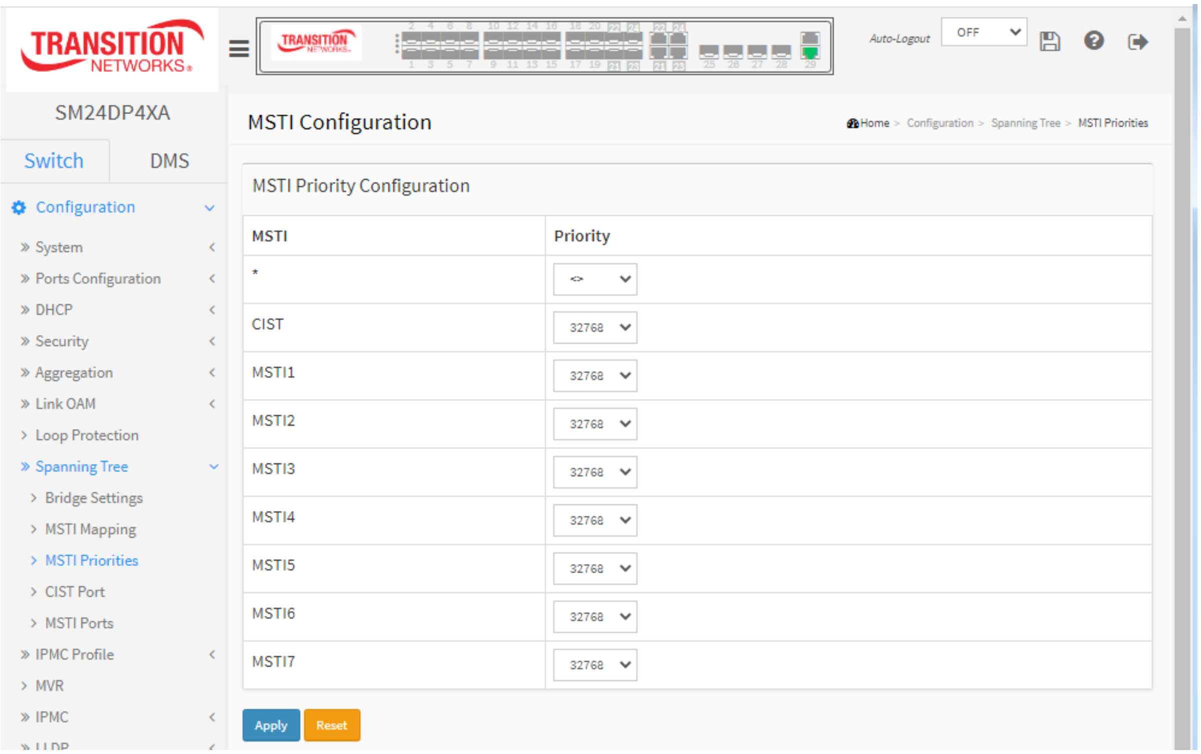
This page lets you view and configure the current STP MSTI bridge instance priority configurations.

Web Interface

To configure the Spanning Tree MSTI Priorities parameters via the web interface:

1. Click Configuration, Spanning Tree, MSTI Priorities
2. Set the Priority maximum. The default is 32768.
3. Click the Apply button to save the settings.
4. To cancel the settings click the Reset button. It will revert to previously saved values.

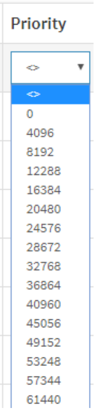
Figure 2-8.3: MSTI Priority Configuration



MSTI Configuration

MSTI Priority Configuration

MSTI	Priority
*	<>
CIST	32768
MSTI1	32768
MSTI2	32768
MSTI3	32768
MSTI4	32768
MSTI5	32768
MSTI6	32768
MSTI7	32768



Priority

<>

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

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

Save – Click to save changes.

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

2-8.4 CIST Ports

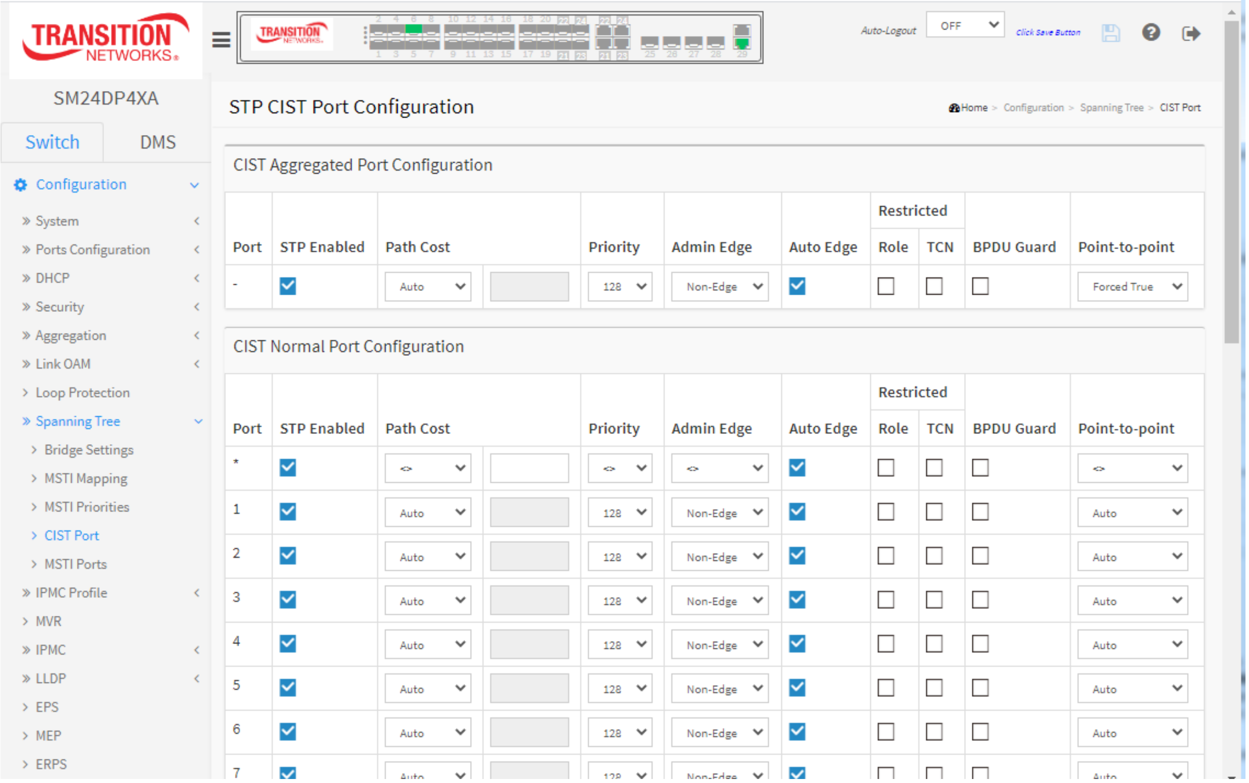
When you implement a Spanning Tree protocol on the switch that is the bridge instance, you must configure the CIST Ports. This page lets you view and configure the current STP CIST port parameters.

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 in the CIST Aggregated Port Configuration section.
3. Enable or disable the STP, then set all parameters in the CIST Normal Port Configuration section.
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



STP CIST Port Configuration

CIST Aggregated Port Configuration

							Restricted			
Port	STP Enabled	Path Cost		Priority	Admin Edge	Auto Edge	Role	TCN	BPDU Guard	Point-to-point
-	☑	Auto		128	Non-Edge	☑	□	□	□	Forced True

CIST Normal Port Configuration

							Restricted			
Port	STP Enabled	Path Cost		Priority	Admin Edge	Auto Edge	Role	TCN	BPDU Guard	Point-to-point
*	☑	<>		<>	<>	☑	□	□	□	<>
1	☑	Auto		128	Non-Edge	☑	□	□	□	Auto
2	☑	Auto		128	Non-Edge	☑	□	□	□	Auto
3	☑	Auto		128	Non-Edge	☑	□	□	□	Auto
4	☑	Auto		128	Non-Edge	☑	□	□	□	Auto
5	☑	Auto		128	Non-Edge	☑	□	□	□	Auto
6	☑	Auto		128	Non-Edge	☑	□	□	□	Auto
7	☑	Auto		128	Non-Edge	☑	□	□	□	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 in the range 1 to 200000000.

Priority : Controls the port priority. This can be used to control priority of ports having identical port cost. (See above.)

AdminEdge : Controls whether the operEdge flag should start as set or cleared. (The initial operEdge state when a port is initialized).

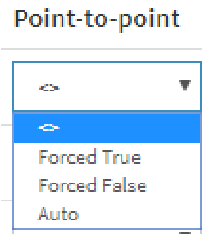
AutoEdge : Controls whether the bridge should enable automatic edge detection on the bridge port. This allows operEdge to be derived from whether BPDU's are received on the port or not.

Restricted Role : If enabled, causes the port not to be selected as Root Port for the CIST or any MSTI, even if it has the best spanning tree priority vector. Such a port will be selected as an Alternate Port after the Root Port has been selected. If set, it can cause lack of spanning tree connectivity. It can be set by a network administrator to prevent bridges external to a core region of the network influence the spanning tree active topology, possibly because those bridges are not under the full control of the administrator. This feature is also known as Root Guard.

Restricted TCN : If enabled, causes the port not to propagate received topology change notifications and topology changes to other ports. If set it can cause temporary loss of connectivity after changes in a spanning tree's active topology as a result of persistently incorrect learned station location information. It is set by a network administrator to prevent bridges external to a core region of the network, causing address flushing in that region, possibly because those bridges are not under the full control of the administrator or the physical link state of the attached LANs transits frequently.

BPDU Guard : If enabled, causes the port to disable itself upon receiving valid BPDU's. Contrary to the similar bridge setting, the port Edge status does not affect this setting. A port entering error-disabled state due to this setting is subject to the bridge Port Error Recovery setting as well.

Point to Point : Controls whether the port connects to a point-to-point LAN rather than to a shared medium. This can be automatically determined, or forced either true or false. Transition to the forwarding state is faster for point-to-point LANs than for shared media.



Buttons

Save – Click to save changes.

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

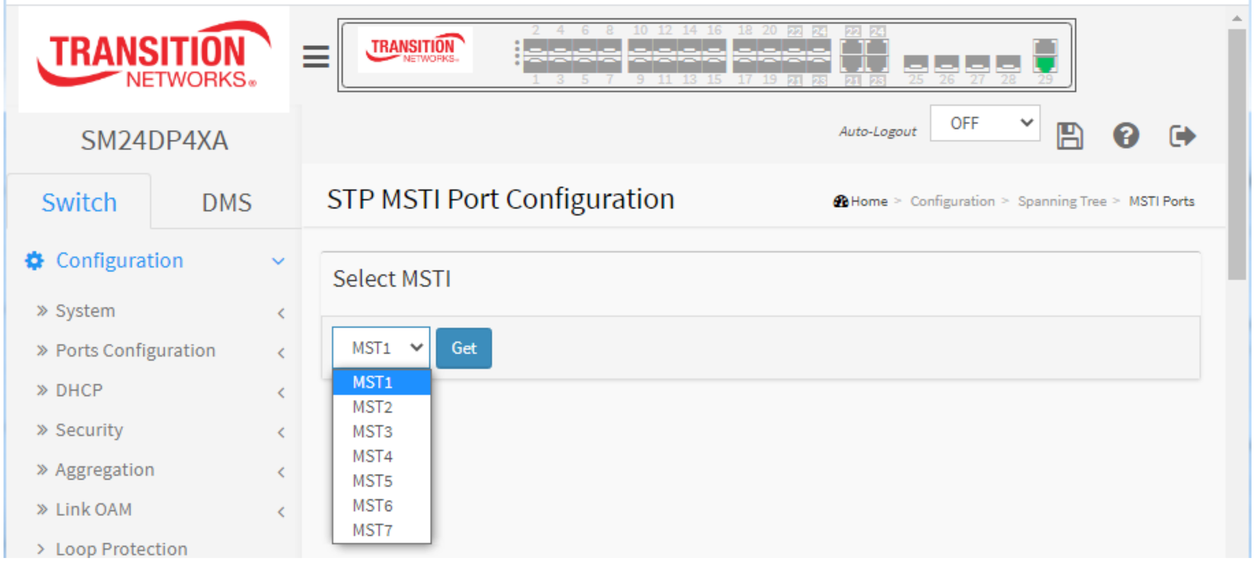
2-8.5 MSTI Ports

This page lets you view and configure the current STP MSTI port configurations. 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 Configuration parameters in the web interface:

1. Click Configuration, Spanning Tree, MSTI Ports.
2. At the dropdown select the MST1 or another MSTI Port.



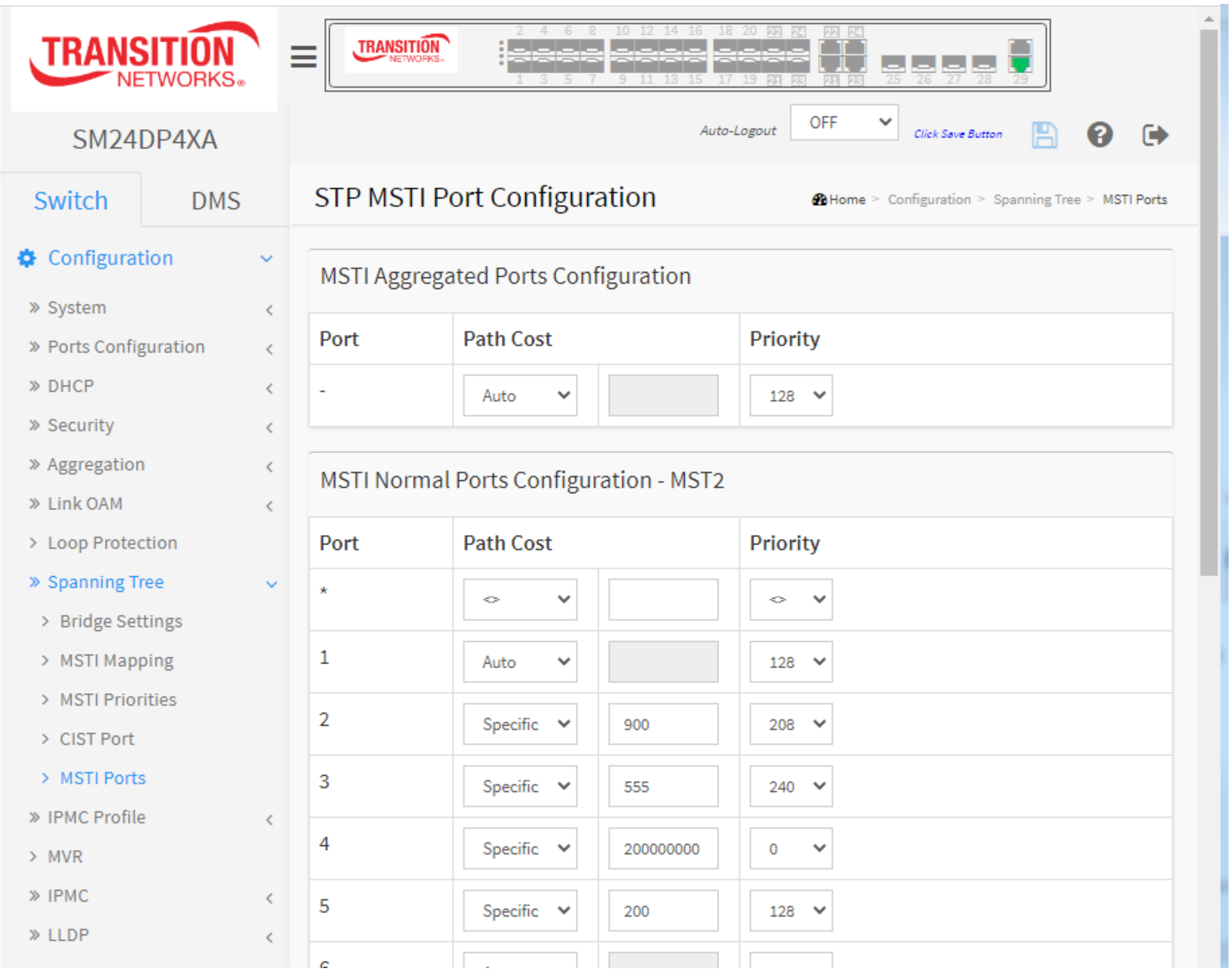
STP MSTI Port Configuration

Select MSTI

MST1

3. Click the Get button to display the detailed parameters on the STP MSTI Port Configuration page.
4. Set all parameters on the STP CIST Port Configuration page.
5. Click the Apply button to save the settings.
6. To cancel the settings click the Reset button to revert to previously saved values.

Figure 2-8.5: STP MSTI Port Configuration



STP MSTI Port Configuration

MSTI Aggregated Ports Configuration

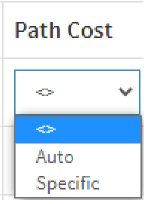
Port	Path Cost		Priority
-	Auto		128

MSTI Normal Ports Configuration - MST2

Port	Path Cost		Priority
*	<>		<>
1	Auto		128
2	Specific	900	208
3	Specific	555	240
4	Specific	200000000	0
5	Specific	200	128
6			

Parameter descriptions:

MSTI Aggregated Ports Configuration



Port : The switch port number of the corresponding STP CIST (and MSTI) port.

Path Cost : Controls the path cost incurred by the port.

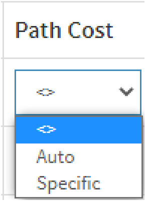
Auto : Set the path cost as appropriate by the physical link speed, using the 802.1D recommended values. This is the default setting.

Specific : 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.

MSTI Normal Ports Configuration - MSTx

Port : The switch port number of the corresponding STP CIST (and MSTI) port.

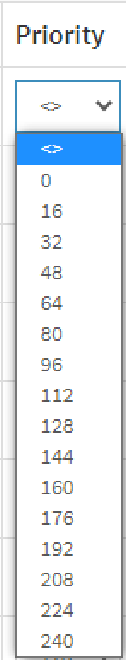


Path Cost : Controls the path cost incurred by the port.

Auto : Set the path cost as appropriate by the physical link speed, using the 802.1D recommended values. This is the default setting.

Specific : 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. The default is 128.

Priority : Controls the port priority. This can be used to control priority of ports having identical port cost.



Buttons

Save – Click to save changes.

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

2-9 IPMC Profile

2-9.1 Profile Table

This page provides IPMC Profile related configurations. The IPMC profile is used to deploy the access control on IP multicast streams. You can create up to 64 Profiles, with a maximum of 128 corresponding rules for each.

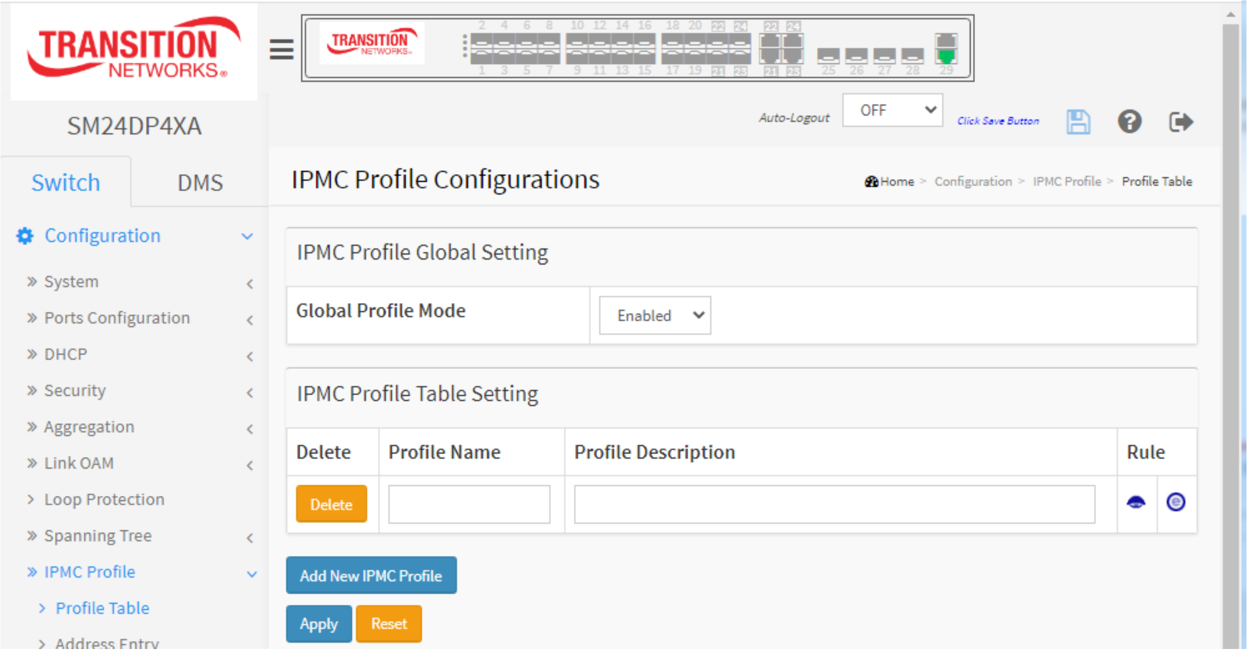
IPMC (IP MultiCast) supports IPv4 and IPv6 multicasting. IPMCv4 denotes multicast for IPv4. IPMCv6 denotes multicast for IPv6. An IPMC Profile (IP MultiCast Profile) is used to deploy the access control on IP multicast streams.

To configure the IPMC Profile Configuration in the web UI:

1. Click Configuration, IPMC Profile, Profile Table.
2. At the Global Profile Mode dropdown select Enabled.
3. Click the Add New IPMC Profile button.
4. Enter a Profile Name and Profile Description.
5. Click the Apply button.
6. In the Rule column click the edit button to enter the rule setting page.
7. Continue to the IPMC Profile Rule Settings Table section below.

Web Interface

Figure 2-9.1: IPMC Profile Configuration



IPMC Profile Configurations

IPMC Profile Global Setting

Global Profile Mode	Enabled

IPMC Profile Table Setting

Delete	Profile Name	Profile Description	Rule
Delete			

Parameter descriptions:

Port : The switch port number of the corresponding STP CIST (and MSTI) port.

Global Profile Mode : Enable/Disable the Global IPMC Profile.
System starts to do filtering based on profile settings only when the global profile mode is enabled.

Delete : Check to delete the entry immediately.

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 alpha character must be entered.

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 view the rules of the designated profile by using these buttons:

👁 : **Navigate**: List the rules associated with the designated profile.

ⓔ: **Edit**: Adjust the rules associated with the designated profile.

Buttons

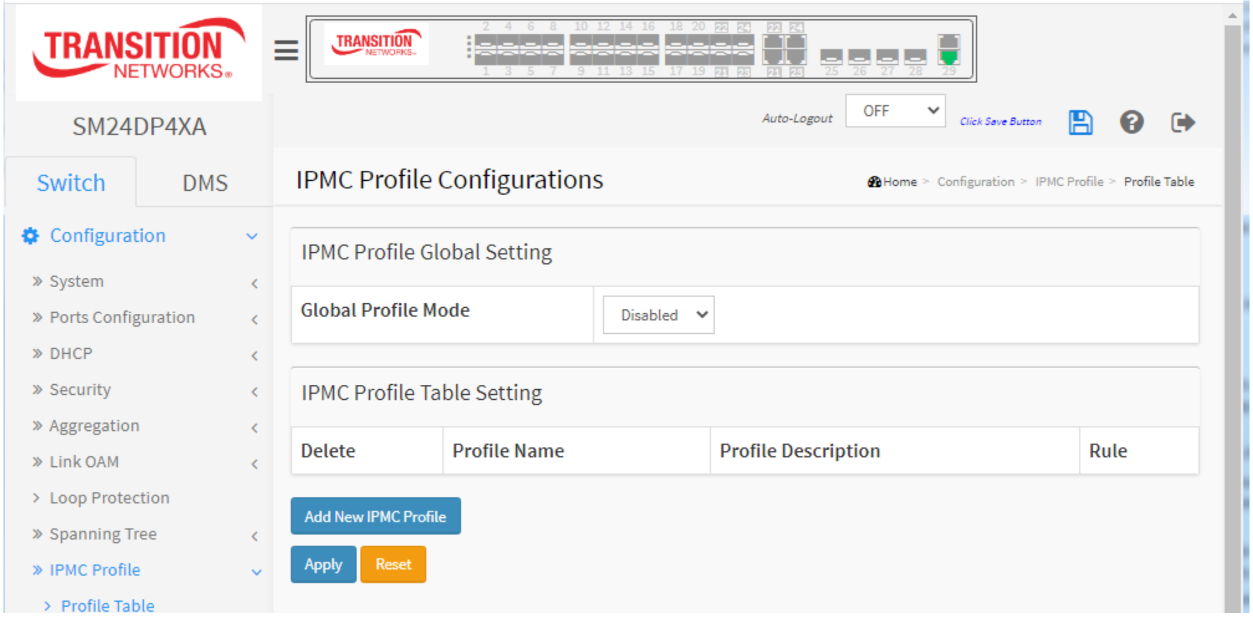
Add New IPMC Profile – Click to add new IPMC profile. Specify the name and configure the new entry. Click "Apply".

Save – 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.



IPMC Profile Configurations

IPMC Profile Global Setting

Global Profile Mode: Disabled

IPMC Profile Table Setting

Delete	Profile Name	Profile Description	Rule

Profile Name : The name of the designated profile to be associated. This field is not editable.

Entry Name : The name used in specifying the address range used for this rule.
Only the existing profile address entries will be chosen in the selected box. This field is not allowed to be selected as none ("-") while the Rule Settings Table is committed.

Address Range : The corresponding address range of the selected profile entry. This field is not editable and will be adjusted automatically according to the selected profile entry.

Action : Indicates the learning action upon receiving the Join/Report frame that has the group address matches the address range of the rule.

> ***Permit***: Group address matches the range specified in the rule will be learned.
>
> ***Deny***: Group address matches the range specified in the rule will be dropped.

Log : Indicates the logging preference upon receiving the Join/Report frame that has the group address matches the address range of the rule.

> ***Enable***: Corresponding information of the group address, that matches the range specified in the rule, will be logged.
>
> ***Disable***: Corresponding information of the group address, that matches the range specified in the rule, will not be logged.

Rule Management buttons : You can manage rules and the corresponding precedence order by using these buttons:

> ⊕: Insert a new rule before the current entry of rule.
>
> ⊗: Delete the current entry of rule.
>
> ↑: Moves the current entry of rule up in the list.
>
> ↓: Moves the current entry of rule down in the list.

Buttons

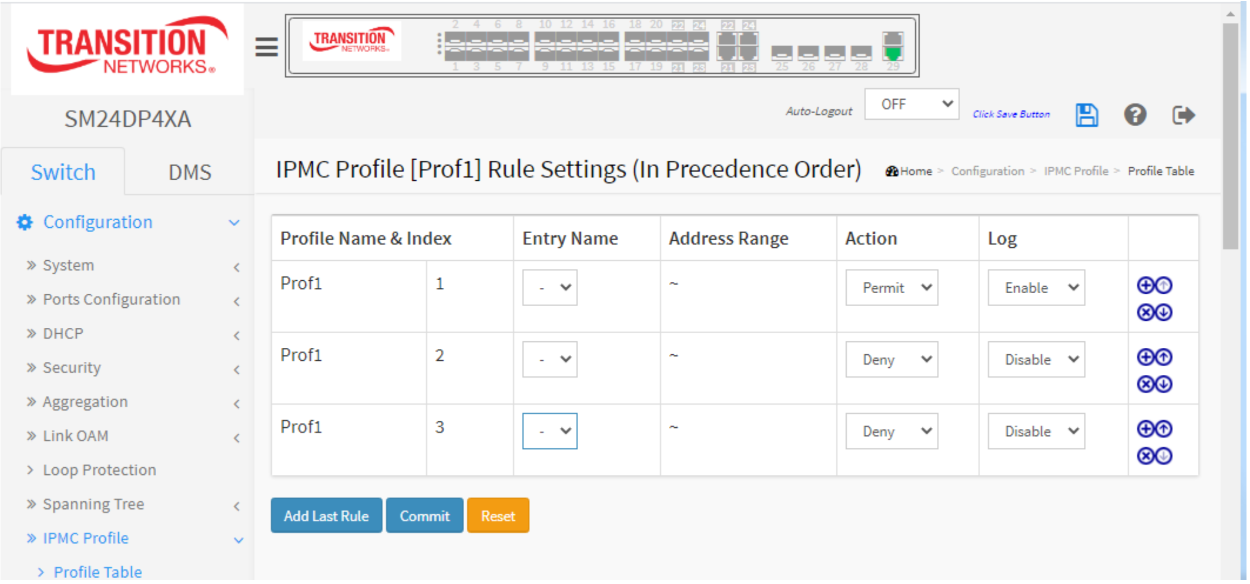
Add Last Rule – Click to add a new rule in the end of the specific profile's rule list. Specify the address entry and configure the new entry. Click "Commit"

Commit – Click to commit rule changes for the designated profile.

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

IPMC Profile Configurations Example

IPMC Profile [Prof1] Rule Settings (In Precedence Order):



IPMC Profile [Prof1] Rule Settings (In Precedence Order)

Profile Name & Index		Entry Name	Address Range	Action	Log	
Prof1	1	-	~	Permit	Enable	
Prof1	2	-	~	Deny	Disable	
Prof1	3	-	~	Deny	Disable	

Parameter descriptions:

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 character 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. A summary of the designated profile will be shown by clicking the Navigate button. You can manage or inspect the rules of the designated profile by using these buttons:

Navigate Profile Rule : List the rules associated with the designated profile.

Edit Profile Rule : Adjust the rules associated with the designated profile.

Messages:

Duplicated entry used in the 2nd rule.

Please select the Entry Name for the 2nd rule.

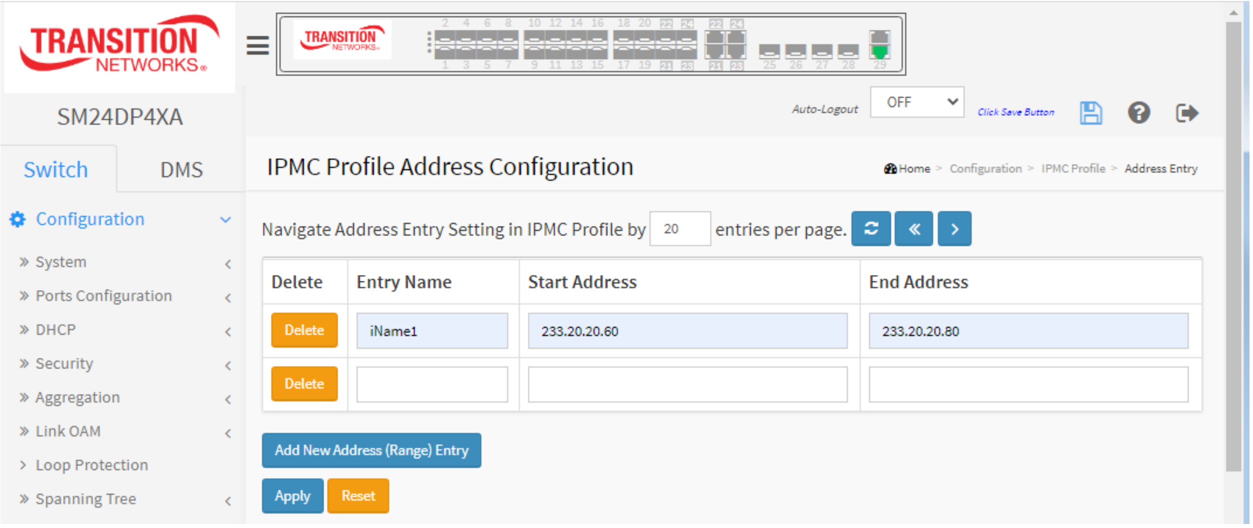
2-9.2 Address Entry

This page provides address range settings used in an 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.

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 page parameters.
4. Click the Apply button.

Figure 2-9.2: IPMC Profile Address Configuration



IPMC Profile Address Configuration

Navigate Address Entry Setting in IPMC Profile by 20 entries per page.

Delete	Entry Name	Start Address	End Address
Delete	iName1	233.20.20.60	233.20.20.80
Delete			

Add New Address (Range) Entry

Apply Reset

Parameter descriptions:

Delete : Check to immediately delete the entry.

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 alpha character must be present.

Start Address : The starting IPv4/IPv6 Multicast Group Address that will be used as an address range.

End Address : The ending IPv4/IPv6 Multicast Group Address that will be used as an address range.

Buttons

Add New Address (Range) Entry : Click to add new address range. Specify the name and configure the addresses. Click Apply

Apply : Click to save changes.

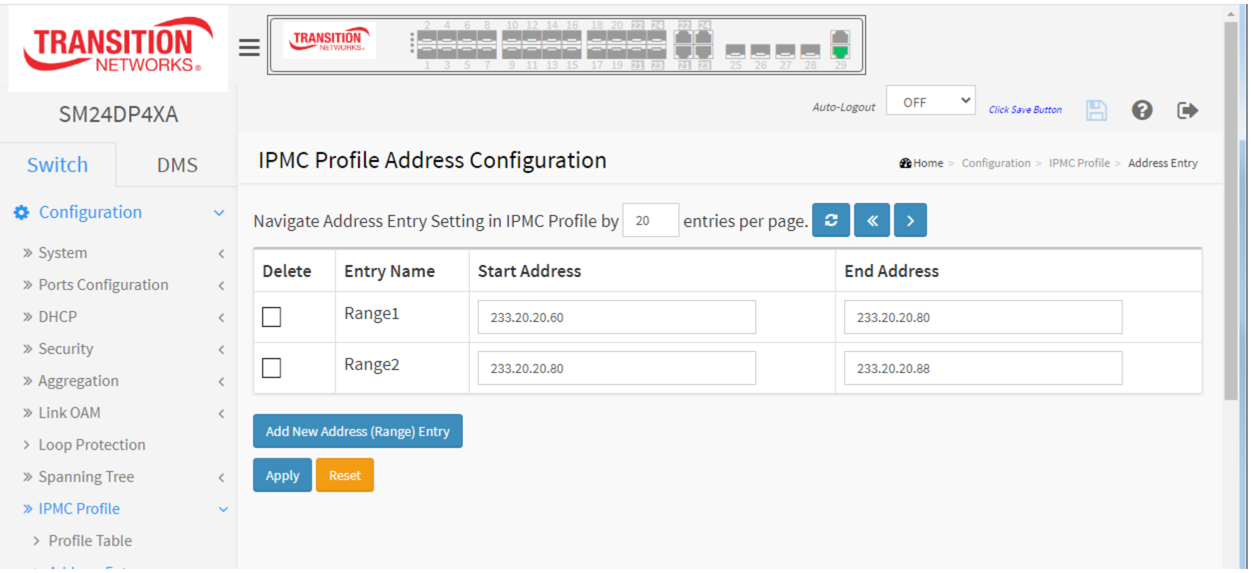
Reset : Click to undo any changes made locally and revert to previously saved values.

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

<< : Updates the table starting from the first entry in the IPMC Profile Address Configuration.

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

IPMC Profile Address Configuration Example:



IPMC Profile Address Configuration

Navigate Address Entry Setting in IPMC Profile by 20 entries per page.

Delete	Entry Name	Start Address	End Address
□	Range1	233.20.20.60	233.20.20.80
□	Range2	233.20.20.80	233.20.20.88

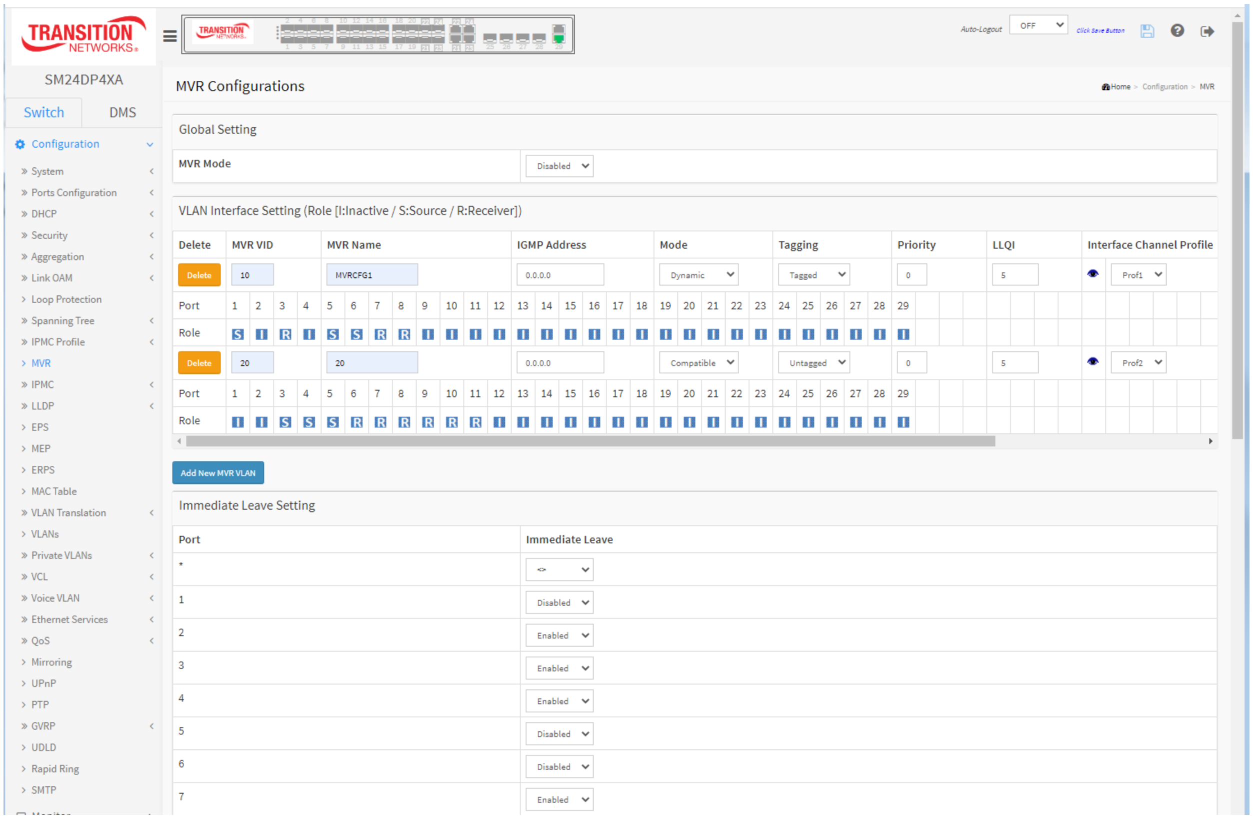
2-10 MVR

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 Switch A to join the appropriate multicast. Uplink ports that send and receive multicast data to and from the multicast VLAN are called MVR source ports.

To configure the MVR Configuration in the web interface:

1. Click Configuration, MVR, Configuration.
2. At the MVR Mode dropdown select Enabled.
3. Click the Add New MVR VLAN button and set the VLAN Interface Setting parameters.
4. Select the Immediate Leave Settings for the ports.
5. Click the Apply button to save the settings.

Figure 2-10: MVR Configuration



MVR Configurations

Global Setting

MVR Mode	Disabled

VLAN Interface Setting (Role [I:Inactive / S:Source / R:Receiver])

Delete	MVR VID	MVR Name	IGMP Address	Mode	Tagging	Priority	LLQI	Interface Channel Profile
Delete	10	MVRCFG1	0.0.0.0	Dynamic	Tagged	0	5	Prof1
Delete	20	20	0.0.0.0	Compatible	Untagged	0	5	Prof2

MVR VID 10:

Port	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29
Role	S	I	R	I	S	S	R	R	I	I	I	I	I	I	I	I	I	I	I	I	I	I	I	I	I	I	I	I	I

MVR VID 20:

Port	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29
Role	I	I	S	S	S	R	R	R	R	R	R	I	I	I	I	I	I	I	I	I	I	I	I	I	I	I	I	I	I

Add New MVR VLAN

Immediate Leave Setting

Port	Immediate Leave
*	<>
1	Disabled
2	Enabled
3	Enabled
4	Enabled
5	Disabled
6	Disabled
7	Enabled

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.

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.

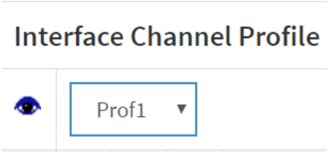
Mode : Specify the MVR mode of operation. In Dynamic mode, MVR allows dynamic MVR membership reports on source ports. In Compatible mode, MVR membership reports are forbidden on source ports. The default is Dynamic mode.

Tagging : Specify whether the traversed IGMP/MLD control frames will be sent as Untagged or Tagged with MVR VID. The default is Tagged.

Priority : Specify how the traversed IGMP/MLD control frames will be sent in prioritized manner. The default Priority is 0.

LLQI : Define the maximum time to wait for IGMP/MLD report memberships on a receiver port before removing the port from multicast group membership. The value is in units of tenths of a second. The range is 0 - 31744. The default LLQI is 5 tenths of a second (one-half second).

Interface Channel Profile : 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.



Profile Management button: You can inspect the rules of the designated profile by using the button:

Navigate: List the rules associated with the designated profile.

Port : The logical port for the settings.

Port Role : Configure an MVR port of the designated MVR VLAN as one of the following roles.

Inactive: The designated port does not participate in MVR operations.

Source: Configure uplink ports that receive and send multicast data as source ports. Subscribers cannot be directly connected to source ports.

Receiver: Configure a port as a receiver port if it is a subscriber port and should only receive multicast data. It does not receive data unless it becomes a member of the multicast group by issuing IGMP/MLD messages.

Caution: MVR source ports are not recommended to be overlapped with management VLAN ports. Select the port role by clicking the Role symbol to switch the setting:

I indicates Inactive; the default Role is Inactive (default setting).

S indicates Source;

R indicates Receiver.

Immediate Leave : Check to 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.

Apply: Click to save changes.

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

2-11 IPMC

ICMP (Internet Control Message Protocol) generates error responses for 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 is used to establish the multicast groups to forward the multicast packet to the member ports, and, in nature, avoids wasting the bandwidth while IP multicast packets are running over the network. This is because a switch that does not support IGMP or IGMP Snooping cannot tell the multicast packet from the broadcast packet, so it can only treat them all as the broadcast packet. Without IGMP Snooping, the multicast packet forwarding function is plain and nothing is different from broadcast packet.

A switch supports IGMP Snooping with the functions of query, report and leave, a type of packet exchanged between IP Multicast Router/Switch and IP Multicast Host, can update the information of the Multicast table when a member (port) joins or leaves an IP Multicast Destination Address. With this function, once a switch receives an IP multicast packet, it will forward the packet to the members who joined in a specified IP multicast group before.

The packets will be discarded by the IGMP Snooping if the user transmits multicast packets to the multicast group that had not been built up in advance. IGMP mode enables the switch to issue IGMP function that you enable IGMP proxy or snooping on the switch, which connects to a router closer to the root of the tree. This interface is the upstream interface. The router on the upstream interface should be running IGMP.

2-11.1.1 Basic Configuration

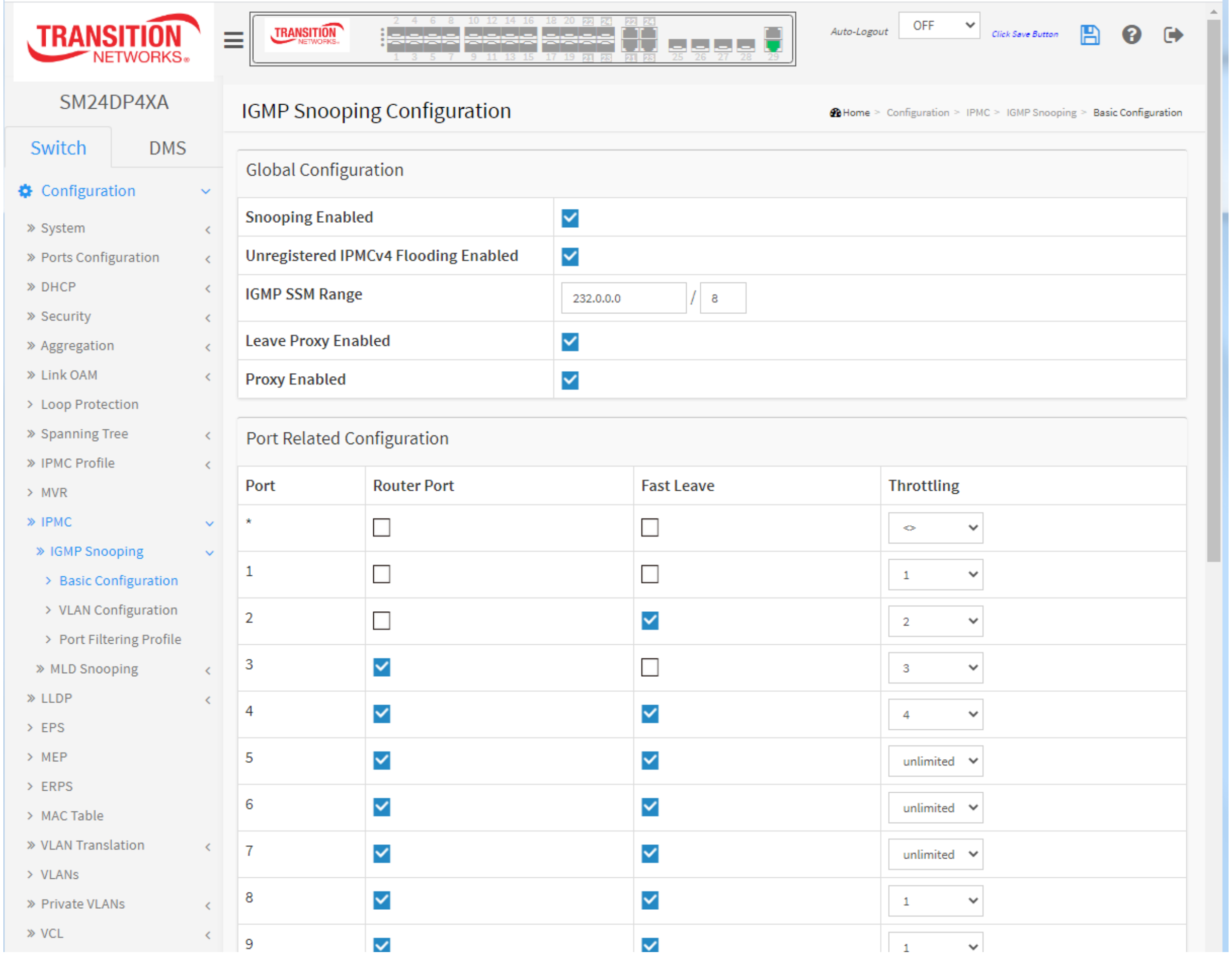
This page lets you set the basic IGMP snooping on the switch, which connects to a router closer to the root of the tree. This interface is the upstream interface. The router on the upstream interface should be running IGMP.

Web Interface

To configure the IGMP Snooping parameters in the web interface:

1. Click Configuration, IPMC,IGMP Snooping, Basic Configuration.
2. Set the Global Configuration section parameters.
3. Set the Port Related Configuration parameters.
4. Click the Apply button to save the settings.

Figure 2-11.1.1: IGMP Snooping Configuration



IGMP Snooping Configuration

Global Configuration

Snooping Enabled	☑
Unregistered IPMCv4 Flooding Enabled	☑
IGMP SSM Range	232.0.0.0 / 8
Leave Proxy Enabled	☑
Proxy Enabled	☑

Port Related Configuration

Port	Router Port	Fast Leave	Throttling
*	□	□	<>
1	□	□	1
2	□	☑	2
3	☑	□	3
4	☑	☑	4
5	☑	☑	unlimited
6	☑	☑	unlimited
7	☑	☑	unlimited
8	☑	☑	1
9	☑	☑	1

Parameter descriptions:

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/ subnet mask)

Proxy Enabled : Enable IGMP Proxy. This feature can be used to avoid forwarding unnecessary join and leave messages to the router side.

Port : It shows the physical Port index of 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 : Check to enable the fast leave on the port. Multicast snooping Fast Leave processing allows the switch to remove an interface from the forwarding-table entry without first sending out group specific queries to the interface. The VLAN interface is pruned from the multicast tree for the multicast group specified in the original leave message. Fast-leave processing ensures optimal bandwidth management for all hosts on a switched network, even when multiple multicast groups are in use simultaneously. This processing applies to IGMP and MLD.

Throttling : Enable to limit the number of multicast groups to which a switch port can belong. Select Unlimited or 1-10.

Buttons

Apply: Click to save changes.

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

2-11.1.2 VLAN Configuration

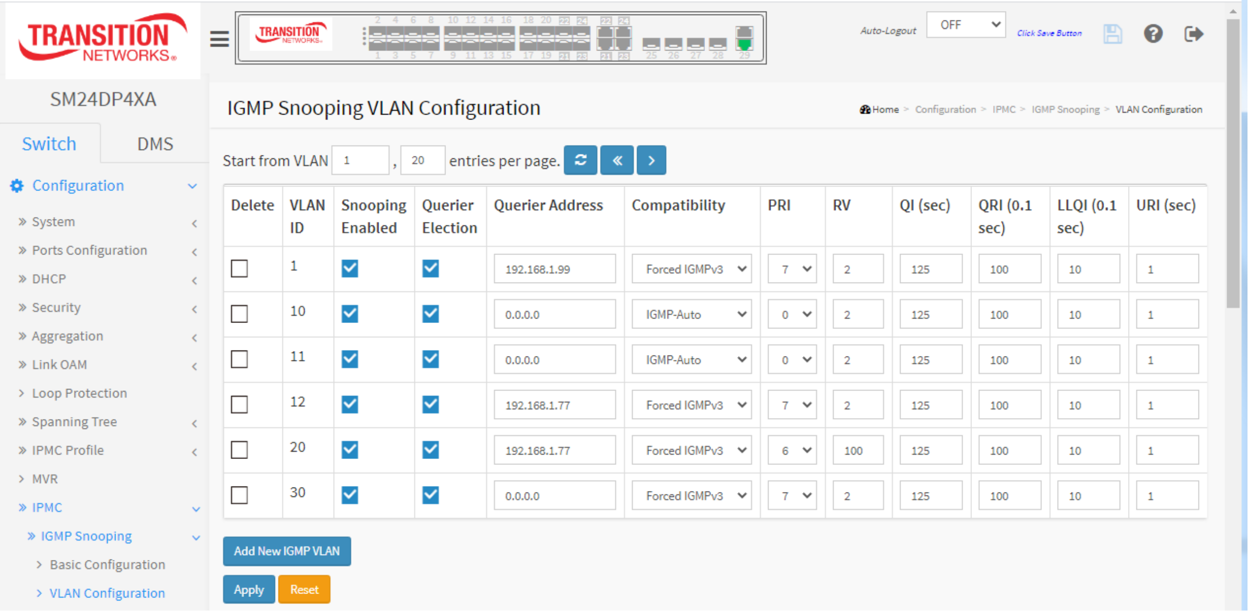
This page lets you set the VLAN configuration parameters integrated with the IGMP Snooping function. Each page shows up to 99 entries from the VLAN table, default being 20, selected through the "entries per page" input field. When first visited, the web page will show the first 20 entries from the beginning of the VLAN table. The first entry displayed is 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 IGMP Snooping VLAN via the web UI:

1. Click Configuration, IPMC, IGMP Snooping, VLAN Configuration.
2. Click the Add New IGMP VLAN button to add a row to the table.
3. Enter a VLAN ID.
4. Enable or disable Snooping and Querier Election.
5. Specify the parameters in the blank fields.
6. Click the Refresh button to update the data or click << or > to display previous entry or next entry.
7. Click the Apply button to save the settings.
8. To cancel the settings click the Reset button to revert to previously saved values.

Figure 2-11.1.2: IGMP Snooping VLAN Configuration



IGMP Snooping VLAN Configuration

Start from VLAN 1 , 20 entries per page.

Delete	VLAN ID	Snooping Enabled	Querier Election	Querier Address	Compatibility	PRI	RV	QI (sec)	QRI (0.1 sec)	LLQI (0.1 sec)	URI (sec)
□	1	☑	☑	192.168.1.99	Forced IGMPv3	7	2	125	100	10	1
□	10	☑	☑	0.0.0.0	IGMP-Auto	0	2	125	100	10	1
□	11	☑	☑	0.0.0.0	IGMP-Auto	0	2	125	100	10	1
□	12	☑	☑	192.168.1.77	Forced IGMPv3	7	2	125	100	10	1
□	20	☑	☑	192.168.1.77	Forced IGMPv3	6	100	125	100	10	1
□	30	☑	☑	0.0.0.0	Forced IGMPv3	7	2	125	100	10	1

Parameter descriptions:

Delete : Check to delete the entry. The designated entry will be deleted at the next save.

VLAN ID : The VLAN ID of the entry.

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 to be used as the source address in the 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, the system uses a pre-defined value. The default value is 192.0.2.1.

Compatibility : Compatibility is maintained by hosts and routers taking appropriate actions depending on the versions of IGMP operating on hosts and routers within a network. The allowed selections are ***IGMP-Auto***, ***Forced IGMPv1***, ***Forced IGMPv2***, and ***Forced IGMPv3***. The default compatibility value is ***IGMP-Auto***. See https://tools.ietf.org/html/rfc1112 or https://tools.ietf.org/html/rfc3376 or https://tools.ietf.org/html/rfc2236.

PRI : Priority of Interface. It indicates the IGMP control frame priority level generated by the system. These values can be used to prioritize different classes of traffic. The allowed range is 0 (best effort) to 7 (highest priority); the default interface priority is 0.

Rv : 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; the default query response interval is 100 in tenths of a second (10 seconds).

LLQI (LMQI for IGMP) : Last Member Query Interval. The Last Member Query Time is the time value represented by the Last Member Query Interval, multiplied by the Last Member Query Count. The allowed range is 0 to 31744 in tenths of seconds; the default last member query interval is 10 in tenths of a second (1 second).

URI : Unsolicited Report Interval; the time between repetitions of a host's initial report of membership in a group. The allowed range is 0 to 31744 seconds; the default URI is 1 second.

Buttons

Add New IGMP VLAN : Click the button to add a row to the IGMP Snooping VLAN Configuration table.

Apply : Click to save changes.

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

Refresh : Click to refreshes the table parameters starting.

|<< : 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

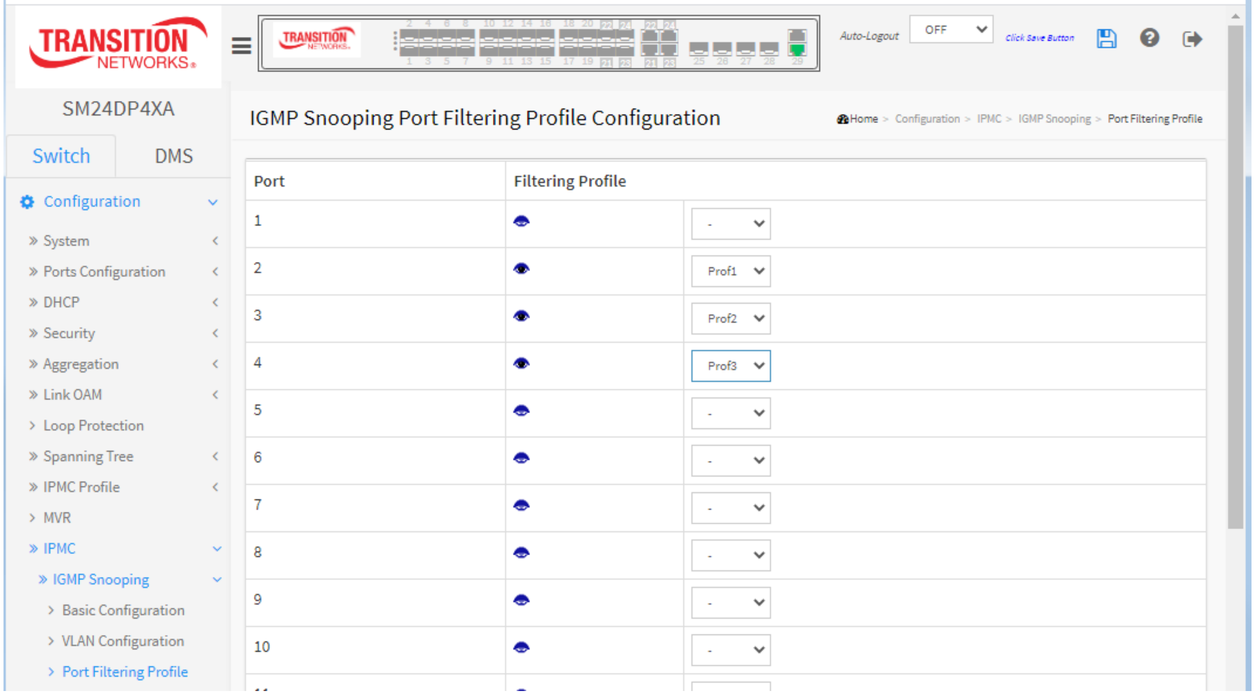
IPMC Profile (IP Multicast Profile) is used to deploy the access control on IP multicast streams.

Web Interface

To configure the IGMP Snooping Port Group Configuration in the web interface:

1. Click Configuration, IPMC, IGMP Snooping, Port Filtering Profile.
2. For each port, select a Profile at the dropdown and click the 👁 button.
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 2-11.1.3: IGMP Snooping Port Group Filtering Profile Configuration.



IGMP Snooping Port Filtering Profile Configuration

Port	Filtering Profile	
1	👁	-
2	👁	Prof1
3	👁	Prof2
4	👁	Prof3
5	👁	-
6	👁	-
7	👁	-
8	👁	-
9	👁	-
10	👁	-

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:

👁 : Navigate the Profile: List the rules associated with the designated profile.

Buttons:

Save – Click to save changes.

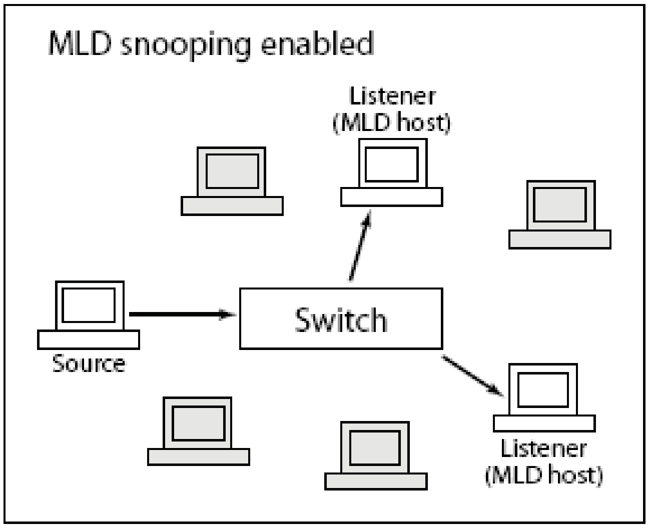
Reset- Click to undo any changes made locally and revert to previously saved values.

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.



2-11.2.1 Basic Configuration

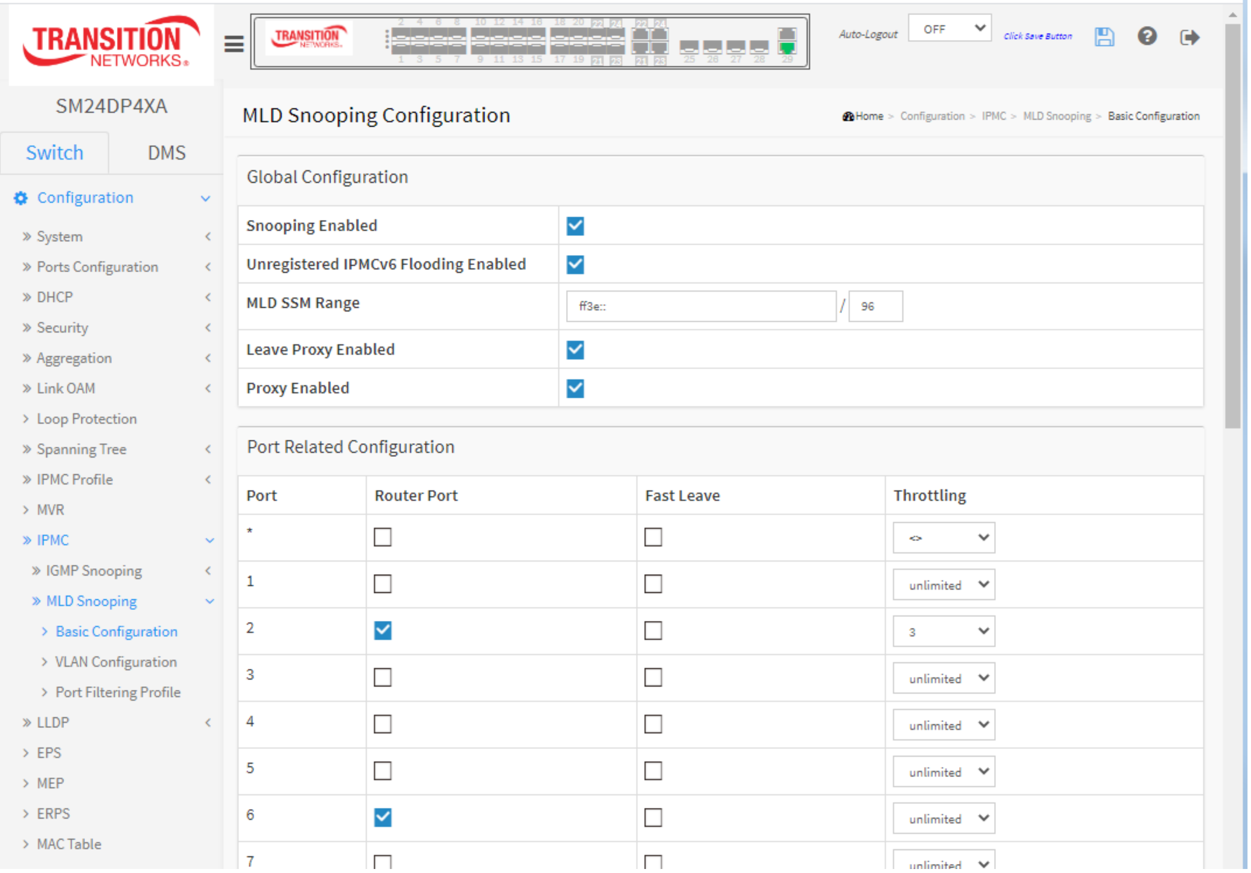
This page lets you to configure the MLD Snooping basic configuration and parameters.

Web Interface

To configure the MLD Snooping Configuration in the web interface:

1. Click Configuration, IPMC, MLD Snooping, Basic Configuration.
2. Enable the Global configuration parameter.
1. Set the port to join Router port and Fast Leave.
2. Select the Throttling mode (unlimited or 1 to 10).
3. Click the Apply button to save the settings.
4. To cancel the settings click the Reset button. It will revert to previously saved values.

Figure 2-11.2.1: MLD Snooping Basic Configuration.



MLD Snooping Configuration

Global Configuration

Snooping Enabled	☑
Unregistered IPMCv6 Flooding Enabled	☑
MLD SSM Range	ff3e:: / 96
Leave Proxy Enabled	☑
Proxy Enabled	☑

Port Related Configuration

Port	Router Port	Fast Leave	Throttling
*	☐	☐	<>
1	☐	☐	unlimited
2	☑	☐	3
3	☐	☐	unlimited
4	☐	☐	unlimited
5	☐	☐	unlimited
6	☑	☐	unlimited
7	☐	☐	unlimited

Parameter descriptions:

Snooping Enabled : Enable the Global MLD Snooping.

Unregistered IPMCv6 Flooding Enabled : Enable unregistered IPMCv6 traffic flooding. Note that disabling unregistered IPMCv6 traffic flooding may lead to failure of Neighbor Discovery.

MLD SSM Range : SSM (Source-Specific Multicast) Range allows the SSM-aware hosts and routers run the SSM service model for the groups in the address (using IPv6 Address) range.

Proxy Enabled : Enable MLD Proxy to avoid forwarding unnecessary join and leave messages to the router side.

Port: The Port index where you enable or disable the MLD Snooping function.

Fast Leave : Check to enable 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 : Enable to limit the number of multicast groups to which a switch port can belong.

Buttons:

Save – 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.

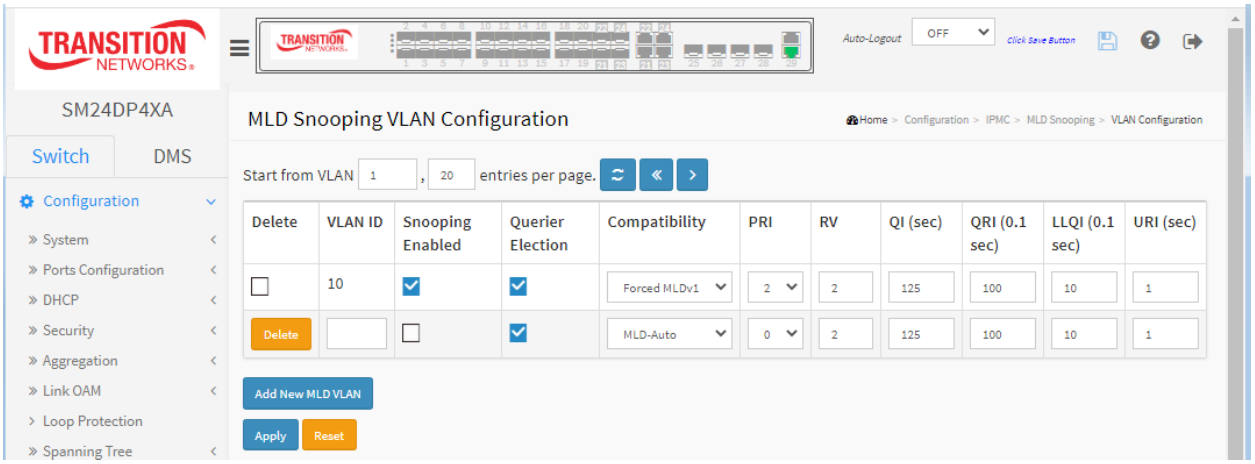
The **>** button will use the last entry of the currently displayed entry as a basis for the next lookup. When the end is reached the text "No more entries" is shown in the displayed table. Use the **<<** button to start over.

Web Interface

To configure the MLD Snooping VLAN Configuration in the web interface:

1. Click Configuration, IPMC, MLD Snooping, VLAN Configuration.
2. Specify the entries per page.
3. Click Refresh to refresh the page immediately.
4. Enter the VLAN Configuration parameters.
5. Click << or > to move to the previous or next entry.

Figure 2-11.2.2: MLD Snooping VLAN Configuration



MLD Snooping VLAN Configuration

Start from VLAN 1 , 20 entries per page.

Delete	VLAN ID	Snooping Enabled	Querier Election	Compatibility	PRI	RV	QI (sec)	QRI (0.1 sec)	LLQI (0.1 sec)	URI (sec)
□	10	☑	☑	Forced MLDv1	2	2	125	100	10	1
Delete		□	☑	MLD-Auto	0	2	125	100	10	1

Add New MLD VLAN

Apply Reset

Parameter descriptions:

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

VLAN ID : The VLAN ID of the entry.

Snooping Enabled : Enable the per-VLAN MLD Snooping. Up to 32 VLANs can be selected for MLD Snooping.

Querier Election : Enable to join MLD Querier election in the VLAN. Disable to act as a MLD Non-Querier.

Compatibility : Compatibility is maintained by hosts and routers taking appropriate actions depending on the versions of MLD operating on hosts and routers within a network. The allowed selections are MLD-Auto, Forced MLDv1, Forced MLDv2, default Compatibility value is MLD-Auto.

PRI: Priority of Interface. It indicates the MLD control frame priority level generated by the system. These values can be used to prioritize different classes of traffic. The allowed range is 0 (best effort) to 7 (highest), default PRI value is 0.

Rv : Robustness Variable; allows tuning for the expected packet loss on a network. The allowed range is 1 to 255; default RV value is 2.

QI : Query Interval; the interval between General Queries sent by the Querier. The allowed range is 1 to 31744 seconds; default QI is 125 seconds.

QRI : Query Response Interval. The Maximum Response Delay used to calculate the Maximum Response Code inserted into the periodic General Queries. The allowed range is 0 to 31744 in tenths of seconds; the default QRI is 100 in tenths of seconds (10 seconds). .

LLQI (LMQI for IGMP) : Last Listener Query Interval. The Last Listener Query Interval is the Maximum Response Delay used to calculate the Maximum Response Code inserted into Multicast Address Specific Queries sent in response to Version 1 Multicast Listener Done messages. It is also the Maximum Response Delay used to calculate the Maximum Response Code inserted into Multicast Address and Source Specific Query messages. The allowed range is 0 to 31744 in tenths of seconds, the default LLQI is 10 in tenths of seconds (1 second).

URI : Unsolicited Report Interval. The Unsolicited Report Interval is the time between repetitions of a node's initial report of interest in a multicast address. The allowed range is 0 to 31744 seconds; the default URI is 1 second.

Buttons:

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

<< : Updates the table starting from the first entry in the VLAN Table, i.e. the entry with the lowest VLAN ID.

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

Add New MLD VLAN : Click to add new MLD VLAN. Specify the VID and configure the new entry. Click "Apply". The specific MLD VLAN starts working after the corresponding static VLAN is also created.

Apply : Click to save changes.

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

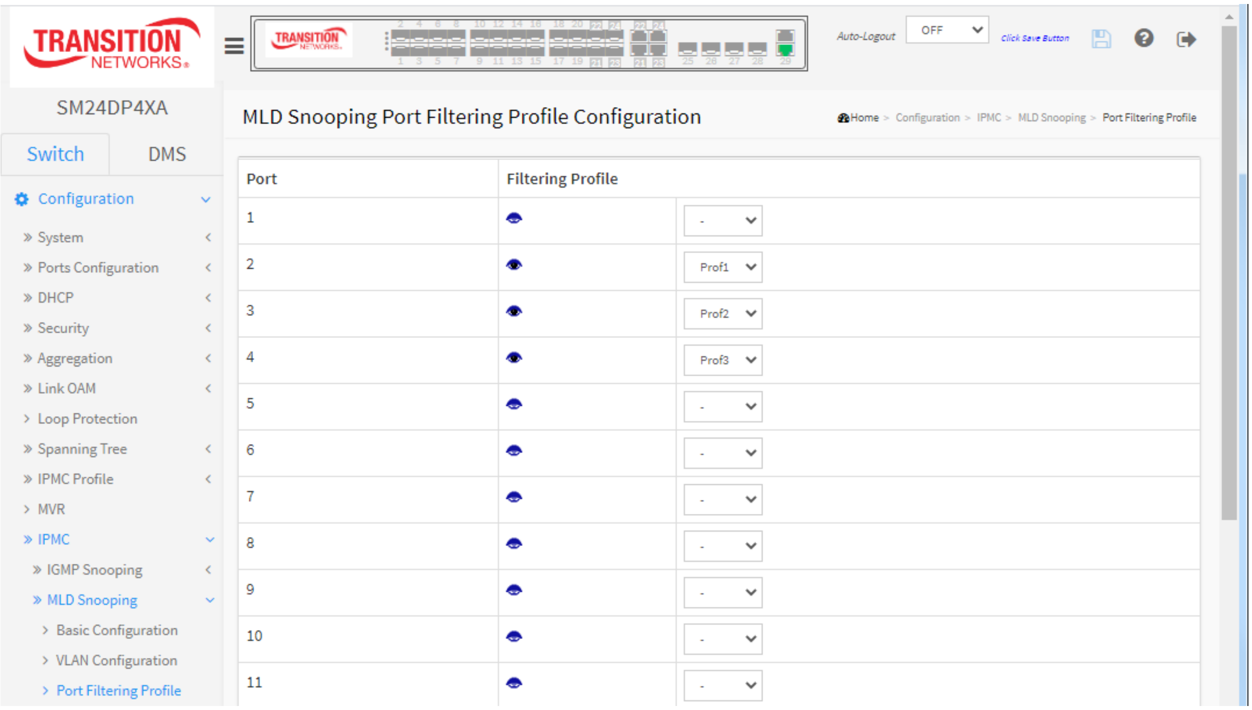
2-11.2.3 Port Group Filtering Profile

Web Interface

To configure MLD Snooping Port Group in the web interface:

1. Click Configuration, IPMC, MLD Snooping, Port Group Filtering Configuration.
2. Click the Apply button to save the settings.
3. If you want to cancel the setting then you need to click the Reset button.
4. It will revert to previously saved values.

Figure 2-11.2.3: MLD Snooping Port Filtering Configuration



MLD Snooping Port Filtering Profile Configuration

Port	Filtering Profile	
1	👁	-
2	👁	Prof1
3	👁	Prof2
4	👁	Prof3
5	👁	-
6	👁	-
7	👁	-
8	👁	-
9	👁	-
10	👁	-
11	👁	-

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 Navigate Profile button:

👁 : List the rules associated with the designated profile.

Buttons:

Save – 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. The Link Layer Discovery Protocol (LLDP) provides a standards-based method for enabling switches to advertise themselves to adjacent devices and to learn about adjacent LLDP devices. 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

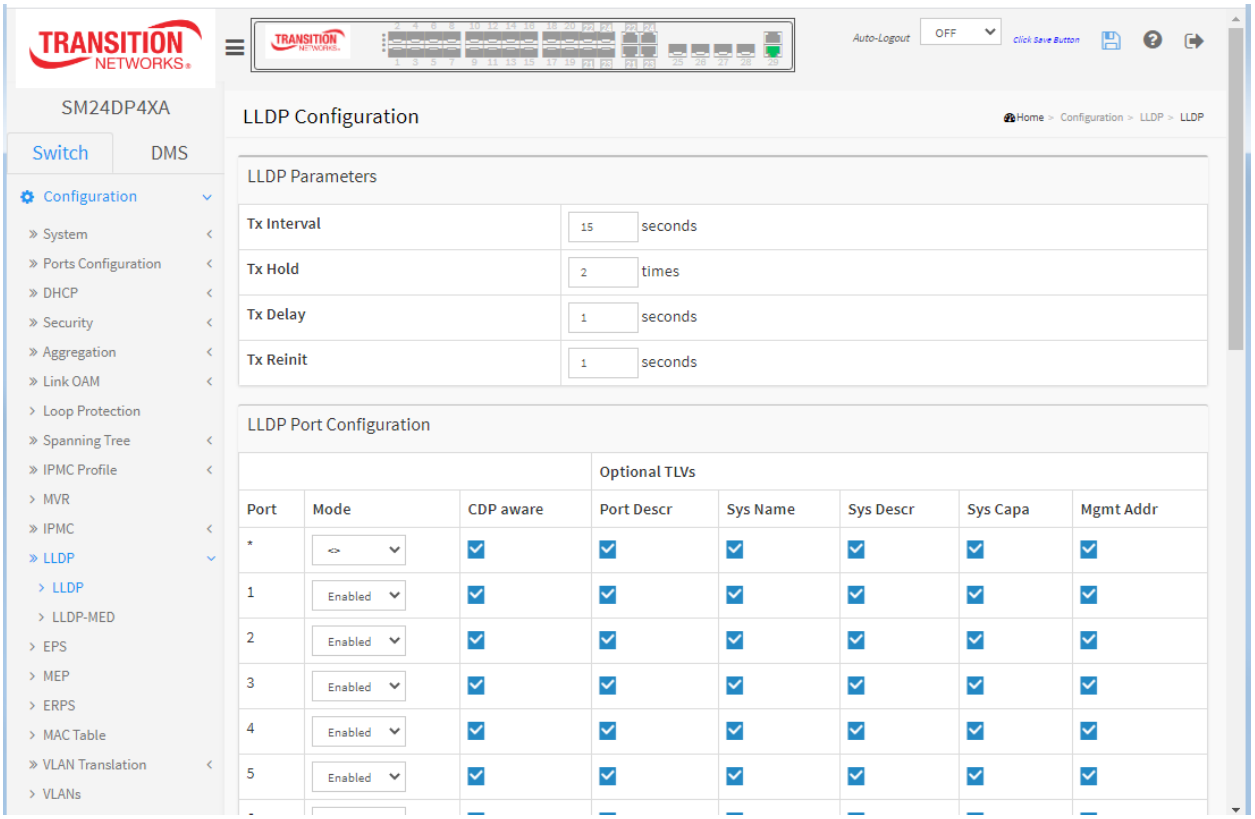
You can per port to do the LLDP configuration and the detail parameters, the settings will take effect immediately. This page lets you view and configure the current LLDP port settings.

Web Interface

To configure LLDP:

1. Click Configuration, LLDP, LLDP.
2. Set the 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 the Apply button.

Figure 2-12.1: LLDP Configuration



LLDP Configuration

LLDP Parameters

Tx Interval	15	seconds
Tx Hold	2	times
Tx Delay	1	seconds
Tx Reinit	1	seconds

LLDP Port Configuration

			Optional TLVs				
Port	Mode	CDP aware	Port Descr	Sys Name	Sys Descr	Sys Capa	Mgmt Addr
*	<>	☑	☑	☑	☑	☑	☑
1	Enabled	☑	☑	☑	☑	☑	☑
2	Enabled	☑	☑	☑	☑	☑	☑
3	Enabled	☑	☑	☑	☑	☑	☑
4	Enabled	☑	☑	☑	☑	☑	☑
5	Enabled	☑	☑	☑	☑	☑	☑

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 5 - 32768 seconds.

Tx Hold : Each LLDP frame contains information about how long the information in the LLDP frame will be considered valid. The LLDP information valid period is set to Tx Hold multiplied by Tx Interval seconds. Valid values are 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 number of seconds between the shutdown frame and a new LLDP initialization. Valid values are 1 - 10 seconds.

LLDP Port Configuration

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

Mode : Select LLDP mode:

> ***Rx only*** : The switch will not send out LLDP information, but LLDP information from neighbor units is analyzed.
> ***Tx only*** : The switch will drop LLDP information received from neighbors but will send out LLDP information.
> ***Disabled*** : The switch will not send out LLDP information and will drop LLDP information received from neighbors.
> ***Enabled*** : The switch will send out LLDP information and will analyze LLDP information received from neighbors.

CDP Aware : Select CDP awareness. CDP (Cisco Discovery Protocol) 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:

Save – 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).

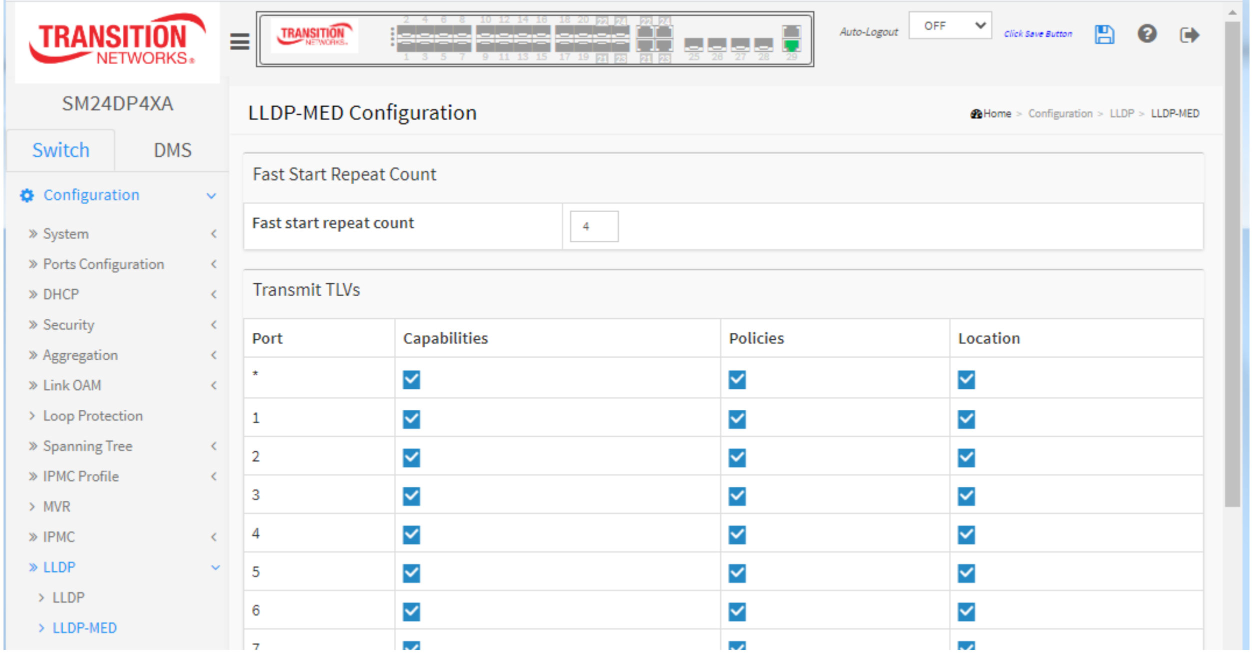
This page lets you configure the LLDP-MED. This function applies to devices that support LLDP-MED.

Web Interface

To configure LLDP-MED:

1. Click Configuration, 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 the Add New Policy button and set policy parameters.
6. Click the Apply button, the Policy Port Configuration page displays (see below).
7. Select a Policy ID for each port.
8. Click Apply.

Figure 2-12.2: LLDP-MED Configuration



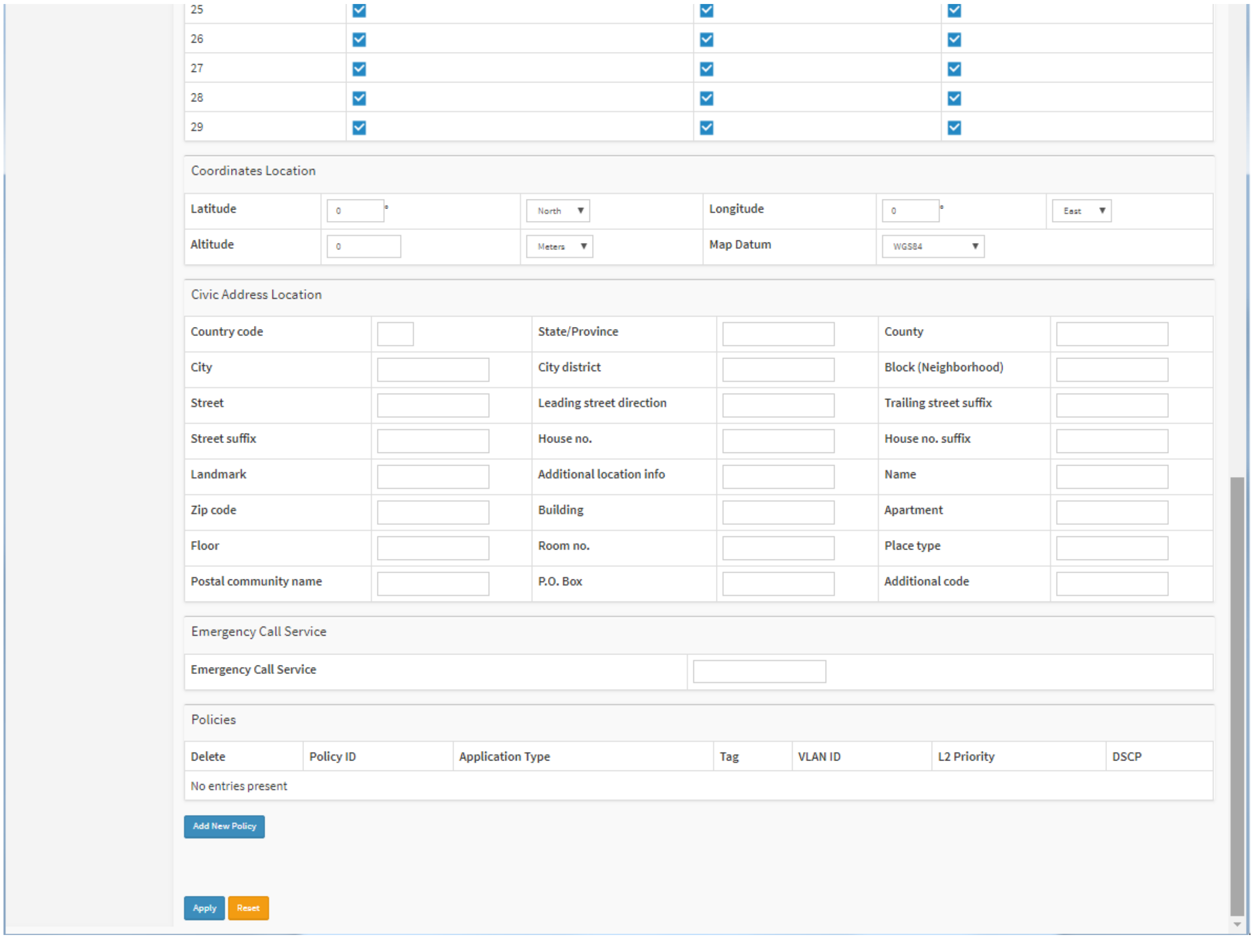
LLDP-MED Configuration

Fast Start Repeat Count

Fast start repeat count	4

Transmit TLVs

Port	Capabilities	Policies	Location
*	☑	☑	☑
1	☑	☑	☑
2	☑	☑	☑
3	☑	☑	☑
4	☑	☑	☑
5	☑	☑	☑
6	☑	☑	☑
7	☑	☑	☑



25	☑	☑	☑
26	☑	☑	☑
27	☑	☑	☑
28	☑	☑	☑
29	☑	☑	☑

Coordinates Location

Latitude	0 °	North	Longitude	0 °	East
Altitude	0	Meters	Map Datum	WGS84	

Civic Address Location

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

Emergency Call Service

Emergency Call Service	

Policies

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

Parameter descriptions:

Fast Start Repeat Count

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

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

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

Note that LLDP-MED and the LLDP-MED Fast Start mechanism is only intended to run on links between

LLDP-MED Network Connectivity Devices and Endpoint Devices, and as such does not apply to links between LAN infrastructure elements, including Network Connectivity Devices, or other types of links.

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

Interface : The interface name to which the configuration applies.

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

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

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

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

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 - Example: DK, DE or US.

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

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

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

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

Block (Neighbourhood) : 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.

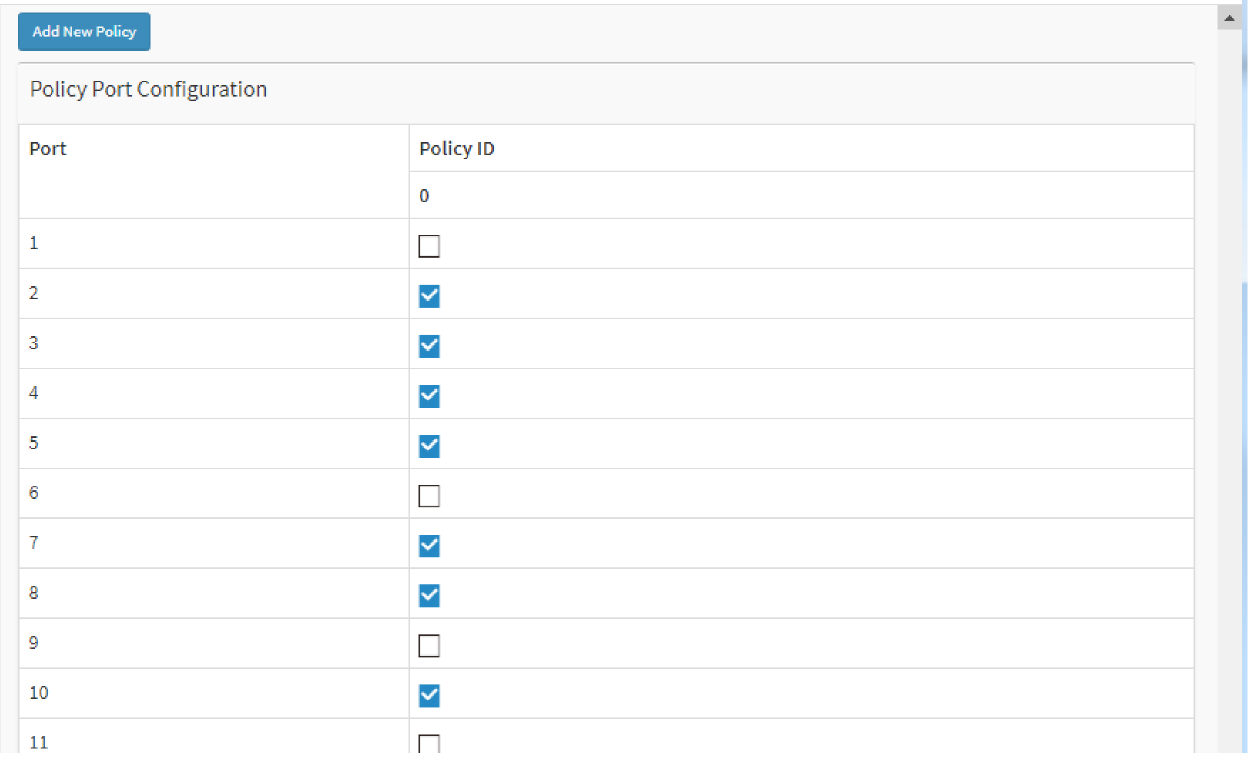
P.O. Box : Post office box (P.O. BOX) - Example: 12345.

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.

Policy Port Configuration:



Policy Port Configuration

Port	Policy ID
	0
1	□
2	☑
3	☑
4	☑
5	☑
6	□
7	☑
8	☑
9	□
10	☑
11	□

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

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

The network policy attributes advertised are:

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

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

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

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

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

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

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

Application Type : Intended use of the application types:

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

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

Buttons:

Save – Click to save changes.

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

2-13 EPS

Ethernet (Linear) Protection Switch instances are configured here. This linear protection switching mechanisms are applied to VLAN-based Ethernet networks. Protection switching is a fully allocated survivability mechanism.

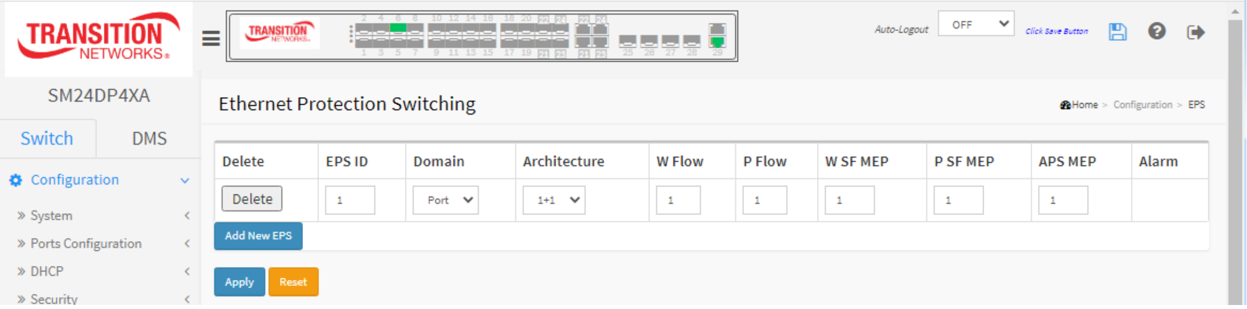
It is fully allocated in the sense that the route and bandwidth of the protection entity are reserved for a selected working entity. It provides a fast and simple survivability mechanism. It is easier for the network operator to grasp the status of the network (e.g., active network topology) with protection switching than with other survivability mechanisms, such as RSTP.

The switch supports linear 1+1 protection switching architecture and linear 1:1 protection switching architecture. The linear 1+1 protection switching architecture operates with either unidirectional or bidirectional switching. The linear 1:1 protection switching architecture operates with bidirectional switching.

Web Interface

To configure Ethernet Protection Switching in the web interface:

1. Click Configuration, EPS.
2. Click the Add New EPS button.
3. Set the page parameters.
4. Click the Apply button when done to save the settings to the running-config file.



Ethernet Protection Switching

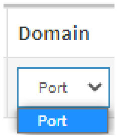
Delete	EPS ID	Domain	Architecture	W Flow	P Flow	W SF MEP	P SF MEP	APS MEP	Alarm
Delete	1	Port	1+1	1	1	1	1	1	

Parameter descriptions:

Delete : Check this box is used to mark an EPS for deletion in next Save operation.

EPS ID : The ID of the EPS. Click on the ID of an EPS to enter the configuration page.

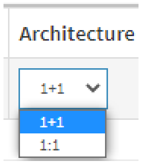
Domain : Port: This will create an EPS in the Port Domain. 'W/P Flow' is a Port.



Architecture : At the dropdown select 1+1 or 1:1.

1+1: This will create a 1+1 EPS.

1:1: This will create a 1:1 EPS.



W Flow : The working flow for the EPS - See 'Domain'.

P Flow : The protecting flow for the EPS - See 'Domain'.

W SF MEP : The working Signal Fail reporting MEP.

P SF MEP : The protecting Signal Fail reporting MEP.

APS MEP : The APS PDU handling MEP.

Alarm : There is an active alarm on the EPS.

Buttons

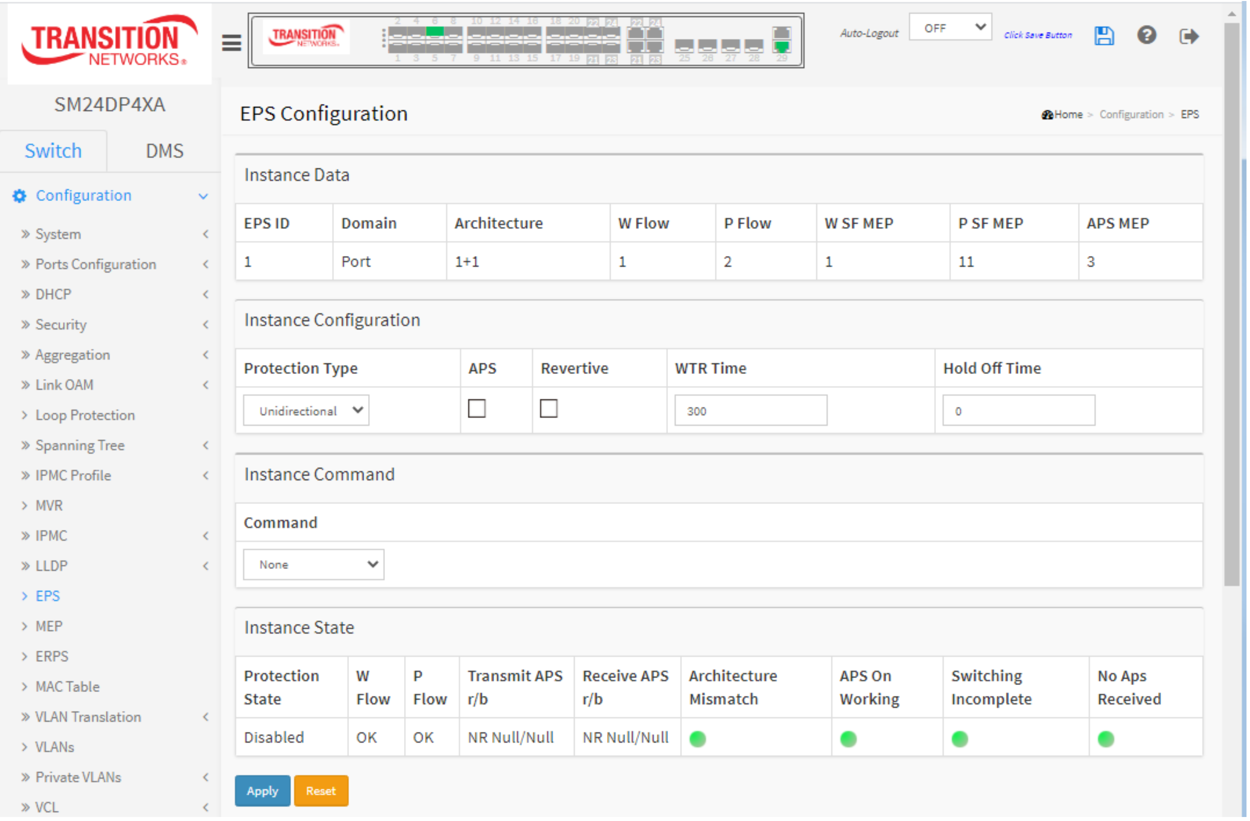
Add New EPS – Click to add a new EPS entry.

Apply : Click to save changes.

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

EPS Configuration

Click on a linked EPS ID to display the EPS Configuration page for the selected EPS instance:



EPS Configuration

Instance Data

EPS ID	Domain	Architecture	W Flow	P Flow	W SF MEP	P SF MEP	APS MEP
1	Port	1+1	1	2	1	11	3

Instance Configuration

Protection Type	APS	Revertive	WTR Time	Hold Off Time
Unidirectional	□	□	300	0

Instance Command

Command
None

Instance State

Protection State	W Flow	P Flow	Transmit APS r/b	Receive APS r/b	Architecture Mismatch	APS On Working	Switching Incomplete	No Aps Received
Disabled	OK	OK	NR Null/Null	NR Null/Null	●	●	●	●

Parameter descriptions:

Instance Data

EPS ID : The ID of the EPS.

Domain : ***Port***: The EPS in the Port Domain. 'W/P Flow' is a Port.

Architecture : See help on EPS create WEB.

W Flow : The working flow for the EPS - See 'Domain'.

P Flow : The protecting flow for the EPS - See 'Domain'.

W SF MEP : The working Signal Fail reporting MEP.

P SF MEP : The protecting Signal Fail reporting MEP.

APS MEP : The APS PDU handling MEP.

Instance Configuration

Configured : Red: This EPS is only created and has not yet been configured - is not active. **Green:** This EPS is configured - is active.

Protection Type : Unidirectional: EPS in the two ends can select traffic from different working/protecting flow. This is only possible in case of 1+1.

Bidirectional: EPS in the two ends is selecting traffic from the same working/protecting flow. This requires APS enabled. This is mandatory for 1:1

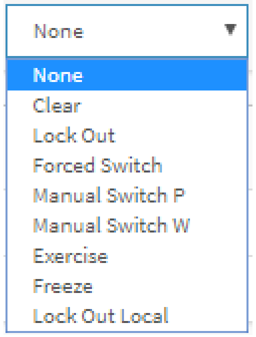
APS : The Automatic Protection Switching protocol can be enabled/disabled. This is mandatory for 1:1.

Revertive : The revertive switching to working flow can be enabled/disabled.

WTR Time : The Wait To Restore timing value to be used in revertive switching. Range is 1 to 720 seconds.

Hold Off Time : The timing value to be used to make persistent check on Signal Fail before switching. This is in 100 ms. and the max value is 100 ms (10 sec).

Instance Command



Command : At the dropdown select:

None: There is no active local command on this instance.

Clear: The active local command will be cleared.

Lock Out: This EPS is locked to working (not active). In case of 1:N (more than one EPS with same protecting flow) - when one EPS switch to protecting flow, other EPS is enforced this command

Forced Switch: Forced switch to protecting.

Manual Switch P: Manual switch to protecting.

Manual Switch W: Manual switch to working. This is only allowed in case of 'non-revertive' mode

Exercise: Exercise of the protocol - not traffic effecting. This is only allowed in case of 'Bidirectional' protection type

Freeze: This EPS is locally frozen - ignoring all input.

Lock Out Local: This EPS is locally "locked out" - ignoring local SF detected on working.

Instance State

Protection State : EPS state according to State Transition Tables in G.8031.

W Flow : The State of the Working flow:

OK: State of working flow is ok

SF: State of working flow is Signal Fail

SD: State of working flow is Signal Degrade (for future use)

P Flow : The State of the Protection flow:

OK: State of protecting flow is ok

SF: State of protecting flow is Signal Fail

SD: State of protecting flow is Signal Degrade (for future use)

Transmit APS r/b : The transmitted APS according to State Transition Tables in G.8031.

Receive APS r/b : The received APS according to State Transition Tables in G.8031.

Architecture Mismatch : The architecture indicated in the received APS does not match the locally configured architecture.

APS on working : APS is received on the working flow.

Switching Incomplete : Traffic is not selected from the same flow instance in the two ends.

No APS Received : APS PDU is not received from the other end.

Buttons

Apply : Click to save changes.

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

Messages:

The working and protection flows are equal

Working MEP and protecting SF MEP is same instance

The working flow is used by other EPS instance

2-14 MEP

Maintenance association End Point (MEP); points at the edge of the domain, define the boundary for the domain. A MEP sends and receives CFM frames through the relay function, drops all CFM frames of its level or lower that come from the wire side.

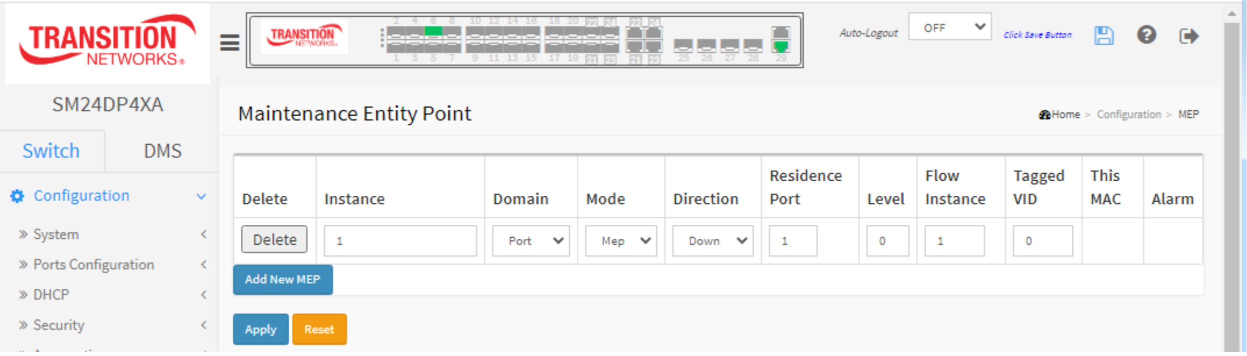
2-14.1 Configuration

Configure Maintenance Entity Point instances here.

Web Interface

To configure Maintenance Entity Point in the web interface:

1. Click Configuration, MEP.
2. Click the Add New MEP button.
3. Enter the MEP instance parameters.
4. Click the Apply button.



Maintenance Entity Point

Delete	Instance	Domain	Mode	Direction	Residence Port	Level	Flow Instance	Tagged VID	This MAC	Alarm
Delete	1	Port	Mep	Down	1	0	1	0		

Parameter descriptions:

Delete : This box is used to mark a MEP for deletion in next Save operation.

Instance : The ID of the MEP. Click on the ID of a MEP to enter the configuration page.

Domain : Select the MEP domain:

Port: This is a MEP in the Port Domain. 'Flow Instance' is a Port.

Evc: This is a MEP in the EVC Domain. 'Flow Instance' is a EVC

Mode : Select MEP or MIP:

MEP: This is a Maintenance Entity End Point.

MIP: This is a Maintenance Entity Intermediate Point.

Direction : Select the MEP direction:

Up: This is a Down MEP - monitoring ingress OAM and traffic on 'Residence Port'.

Down: This is a Up MEP - monitoring egress OAM and traffic on 'Residence Port'.

Residence Port : The port where MEP is monitoring - see 'Direction'.

Level : The MEG level of this MEP (0-7).

Flow Instance : The MEP is related to this flow - See 'Domain'.

Tagged VID : Select:

Port MEP: An outer C/S-tag (depending on VLAN Port Type) is added with this VID. Entering '0' means no TAG added.

EVC MIP: On Serval, this is the Subscriber VID that identifies the subscriber flow in this EVC where the MIP is active.

This MAC : The MAC of this MEP - can be used by other MEP when unicast is selected (Info only).

Alarm : 🔴 Red: There is an active alarm on the MEP. 🟢 Green: No alarm condition exists.

Buttons

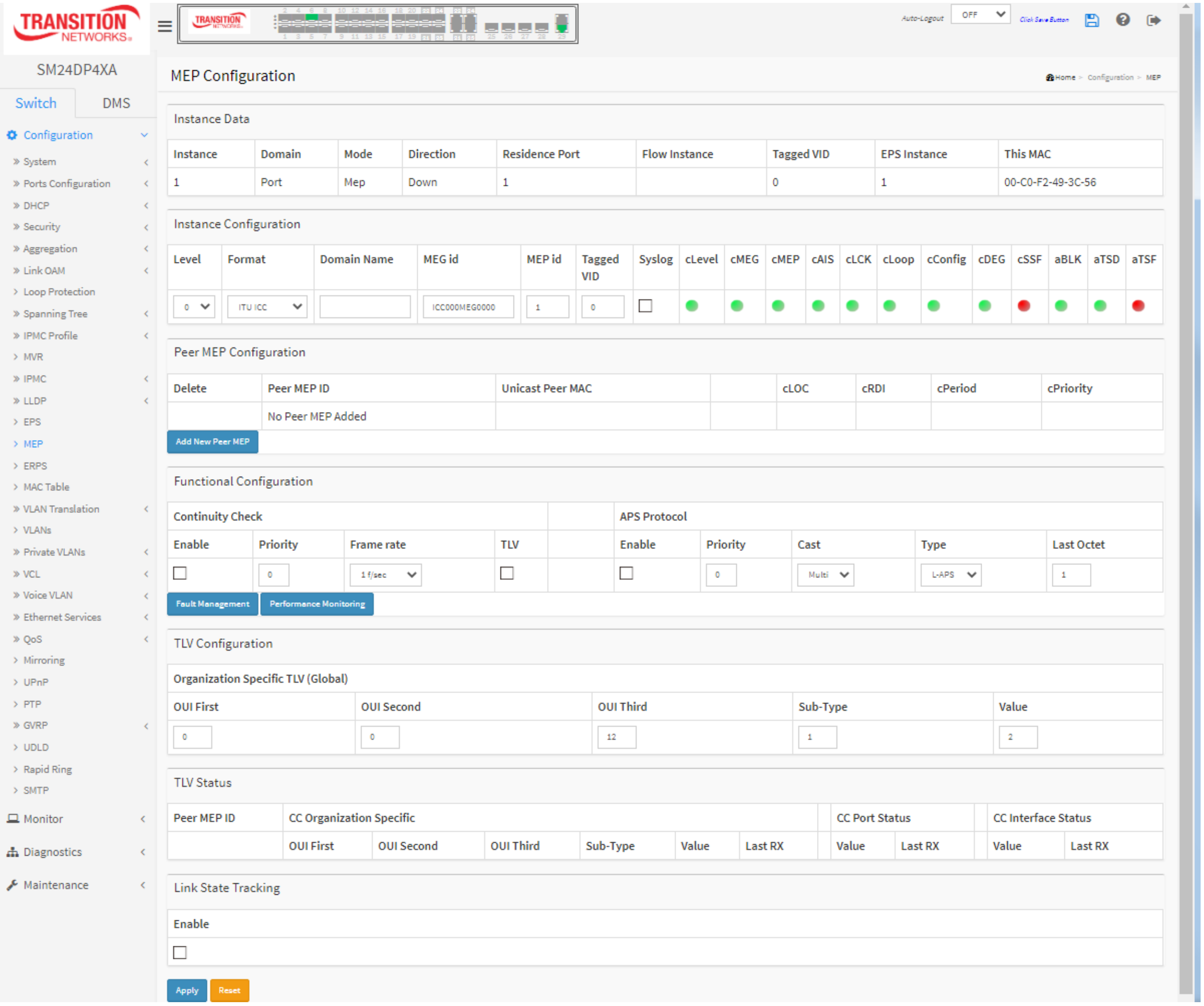
Add New MEP – Click to add a new MEP entry.

Apply – Click to save changes.

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

MEP Configuration page

Click a linked instance to display the MEP Configuration page for the selected MEP instance. This page lets you view and configure the current MEP Instance.



MEP Configuration

Instance Data

Instance	Domain	Mode	Direction	Residence Port	Flow Instance	Tagged VID	EPS Instance	This MAC
1	Port	Mep	Down	1		0	1	00-C0-F2-49-3C-56

Instance Configuration

Level	Format	Domain Name	MEG id	MEP id	Tagged VID	Syslog	cLevel	cMEG	cMEP	cAIS	cLCK	cLoop	cConfig	cDEG	cSSF	aBLK	aTSD	aTSF
0	ITU ICC		ICC000MEG0000	1	0	□	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🔴	🟢	🟢	🔴

Peer MEP Configuration

Delete	Peer MEP ID	Unicast Peer MAC		cLOC	cRDI	cPeriod	cPriority
	No Peer MEP Added						

Add New Peer MEP

Functional Configuration

Continuity Check					APS Protocol				
Enable	Priority	Frame rate	TLV		Enable	Priority	Cast	Type	Last Octet
□	0	1 f/sec	□		□	0	Multi	L-APS	1

Fault Management | Performance Monitoring

TLV Configuration

Organization Specific TLV (Global)

OUI First	OUI Second	OUI Third	Sub-Type	Value
0	0	12	1	2

TLV Status

Peer MEP ID	CC Organization Specific						CC Port Status		CC Interface Status	
	OUI First	OUI Second	OUI Third	Sub-Type	Value	Last RX	Value	Last RX	Value	Last RX

Link State Tracking

Enable
□

Apply | Reset

Parameter descriptions:

Instance Data

Instance : The ID of the MEP.

Domain: e.g., Port.

Mode : MEP or MIP.

Direction : Up or Down.

Residence Port : e.g., 1.

Flow Instance : See help on MEP create WEB.

Tagged VID : See help on MEP create WEB.

This MAC : See help on MEP create WEB.

Instance Configuration

EVC Policy ID : This is the Policy number of the relevant ECE. Policy ID is used to assure that received OAM PDU is able to hit a IS2 entry. If this value is '0' IS2 rules will be created on classified VID. If this is NOT '0' IS2 rules will be created on this Policy (PAG). This must be equal to ECE Policy Number if OAM PDU will hit the ECE IS0. This is the case if an ECE is created with 'tag_type' as 'any'.

Level : The MEG level of this MEP (0-7).

Format : The configuration of the two possible Maintenance Association Identifier formats.

ITU ICC: Defined by ITU (Y1731 Fig. A3). 'Domain Name' is not used. 'MEG id' must be max. 13 char.

IEEE String: This is defined by IEEE (802.1ag Section 21.6.5). 'Domain Name' can be max. 16 char. 'MEG id' (Short MA Name) can be max. 16 char.

ITU CC ICC: This is defined by ITU (Y1731 Fig. A5). 'Domain Name' is not used. 'MEG id' must be max. 15 char.

Domain Name : This is the IEEE Maintenance Domain Name and is only used in case of 'IEEE String' format. This string can be empty giving Maintenance Domain Name Format 1 - Not present. This can be max 16 char.

MEG Id : This is either ITU MEG ID or IEEE Short MA Name - depending on 'Format'. See 'Format'. In case of ITU ICC format this must be 13 char. In case of ITU CC ICC format this must be 15 char. In case of IEEE String format this can be max 16 char.

MEP Id : This value will become the transmitted two byte CCM MEP ID.

Tagged VID : This value will be the VID of a TAG added to the OAM PDU.

VOE : This will attempt to utilize VOE HW for MEP implementation. Not all platforms support VOE.

cLevel : Fault Cause indicating that a CCM is received with a lower level than the configured for this MEP.

cMEG : Fault Cause indicating that a CCM is received with a MEG ID different from configured for this MEP.

cMEP : Fault Cause indicating that a CCM is received with a MEP ID different from all 'Peer MEP ID' configured for this MEP.

cAIS : Fault Cause indicating that AIS PDU is received.

cLCK : Fault Cause indicating that LCK PDU is received.

cDEG : Fault Cause indicating that server layer is indicating Signal Degraded.

cSSF : Fault Cause indicating that server layer is indicating Signal Fail.

aBLK : The consequent action of blocking service frames in this flow is active.

aTSD : The consequent action of indicating Trail Signal Degrade is calculated.

aTSF : The consequent action of indicating Trail Signal Fail towards protection is active.

Delete : This box is used to mark a Peer MEP for deletion in next Save operation.

Peer MEP ID : This value will become an expected MEP ID in a received CCM - see 'cMEP'.

Unicast Peer MAC : This MAC will be used when unicast is selected with this peer MEP. Also this MAC is used to create HW checking of receiving CCM PDU (LOC detection) from this MEP.

cLOC : Fault Cause indicating that no CCM has been received (in 3,5 periods) - from this peer MEP.

cRDI : Fault Cause indicating that a CCM is received with Remote Defect Indication - from this peer MEP.

cPeriod : Fault Cause indicating that a CCM is received with a period different what is configured for this MEP - from this peer MEP.

cPriority : Fault Cause indicating that a CCM is received with a priority different what is configured for this MEP - from this peer MEP.

Buttons

Add New Peer MEP: Click to add a new peer MEP.

Functional Configuration

Continuity Check

Enable : Continuity Check based on transmitting/receiving CCM PDU can be enabled/disabled. The CCM PDU is always transmitted as Multi-cast Class 1.

Priority : The priority to be inserted as PCP bits in TAG (if any). In case of enable of Continuity Check and Loss Measurement both implemented on SW based CCM, 'Priority' has to be the same.

Frame rate : Selecting the frame rate of CCM PDU. This is the inverse of transmission period as described in Y.1731. This value has the following uses:

***** The transmission rate of the CCM PDU.

***** Fault Cause cLOC is declared if no CCM PDU has been received within 3.5 periods - see 'cLOC'.

***** Fault Cause cPeriod is declared if a CCM PDU has been received with different period - see 'cPeriod'.

Selecting 300f/sec or 100f/sec will configure HW based CCM (if possible). Selecting other frame rates will configure SW based CCM. In case of enable of Continuity Check and Loss Measurement both implemented on SW based CCM, 'Frame Rate' has to be the same.

TLV : Enable/disable of TLV insertion in the CCM PDU.

APS Protocol

Enable : Automatic Protection Switching protocol information transportation based on transmitting / receiving R-APS/L-APS PDU can be enabled/disabled. Must be enabled to support ERPS/ELPS with APS. This is only valid with one Peer MEP configured.

Priority : The priority to be inserted as PCP bits in TAG (if any).

Cast : Selection of APS PDU transmitted unicast or multi-cast. The unicast MAC will be taken from the 'Unicast Peer MAC' configuration. Unicast is only valid for L-APS - see 'Type'. The R-APS PDU is always transmitted with multi-cast MAC described in G.8032.

Type : Either:

R-APS: APS PDU is transmitted as R-APS - this is for ERPS.

L-APS: APS PDU is transmitted as L-APS - this is for ELPS.

Last Octet : This is the last octet of the transmitted and expected RAPS multi-cast MAC. In G.8031 (03/2010) a RAPS multi-cast MAC is defined as 01-19-A7-00-00-XX. In current standard the value for this last octet is '01' and the usage of other values is for further study.

TLV Configuration : Configuration of the OAM PDU TLV. Currently only TLV in the CCM is supported.

Organization Specific - OUI First : The transmitted first value in the OS TLV OUI field.

Organization Specific - OUI Second : The transmitted second value in the OS TLV OUI field.

Organization Specific - OUI Third : The transmitted third value in the OS TLV OUI field.

Organization Specific - Sub-Type : The transmitted value in the OS TLV Sub-Type field.

Organization Specific – Value : The transmitted value in the OS TLV Value field.

TLV Status : Display of the last received TLV. Currently only TLV in the CCM is supported.

CC Organization Specific - OUI First : The last received first value in the OUI field.

CC Organization Specific - OUI Second : The last received second value in the OS TLV OUI field.

CC Organization Specific - OUI Third : The last received third value in the OS TLV OUI field.

CC Organization Specific - Sub-Type : The last received value in the OS TLV Sub-Type field.

CC Organization Specific – Value : The last received value in the OS TLV Value field.

CC Organization Specific - Last RX : OS TLV was received in the last received CCM PDU.

CC Port Status – Value : The last received value in the PS TLV Value field.

CC Port Status - Last RX : PS TLV was received in the last received CCM PDU.

CC Interface Status – Value : The last received value in the IS TLV Value field.

CC Interface Status - Last RX : IS TLV was received in the last received CCM PDU.

Link State Tracking

Enable : When LST is enabled in an instance, Local SF or received 'isDown' in CCM Interface Status TLV, will bring down the residence port. Only valid in Up-MEP. The CCM rate must be 1 f/s or faster.

Buttons

Fault Management: Click to go to the Fault Management page.

Performance Monitor: Click to go to the Performance Monitor page.

Apply: Click to save changes.

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

2-15 ERPS

ERPS (Ethernet Ring Protection Switching) specifies protection switching mechanisms and a protocol for Ethernet layer network (ETH) rings. Ethernet Rings can provide wide-area multipoint connectivity more economically due to their reduced number of links. The mechanisms and protocol defined in this Recommendation achieve highly reliable and stable protection; and never form loops, which would fatally affect network operation and service availability. See Appendix B – G.8032 Major and Sub Rings Configuration on page 421 for more information.

Each Ethernet Ring Node is connected to adjacent Ethernet Ring Nodes participating in the same Ethernet Ring, using two independent links. A ring link is bounded by two adjacent Ethernet Ring Nodes, and a port for a ring link is called a ring port. The minimum number of Ethernet Ring Nodes in an Ethernet Ring is two.

The fundamentals of this ring protection switching architecture are:

- The principle of loop avoidance.
- The utilization of learning, forwarding, and Filtering Database (FDB) mechanisms defined in the Ethernet flow forwarding function (ETH_FF).

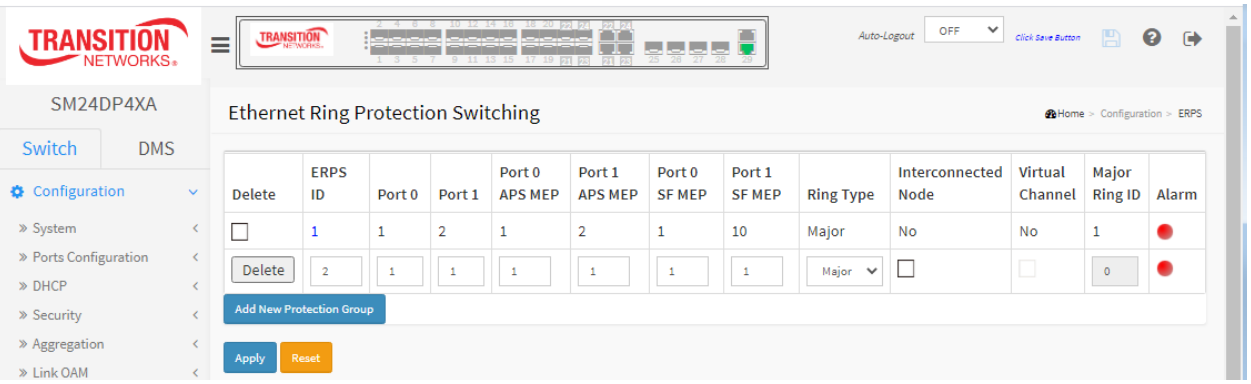
Loop avoidance in an Ethernet Ring is achieved by guaranteeing that, at any time, traffic may flow on all but one of the ring links. This particular link is called the Ring Protection Link (RPL), and under normal conditions this ring link is blocked, i.e. not used for service traffic. One designated Ethernet Ring Node, the RPL Owner Node, is responsible for blocking traffic at one end of the RPL. Under an Ethernet ring failure condition, the RPL Owner Node is responsible for unblocking its end of the RPL (unless the RPL has failed) allowing the RPL to be used for traffic. The other Ethernet Ring Node adjacent to the RPL, the RPL Neighbor Node, may also participate in blocking or unblocking its end of the RPL.

The event of an Ethernet Ring failure results in protection switching of the traffic. This is achieved under the control of the ETH_FF functions on all Ethernet Ring Nodes. An APS protocol is used to coordinate the protection actions over the ring.

Web Interface

To configure Ethernet Ring Protection Switching in the web interface:

1. Click Configuration, ERPS.
2. Click the Add New Protection Group button.
3. Enter and select the ERPS parameters.
4. Click the Apply button.



Ethernet Ring Protection Switching

Delete	ERPS ID	Port 0	Port 1	Port 0 APS MEP	Port 1 APS MEP	Port 0 SF MEP	Port 1 SF MEP	Ring Type	Interconnected Node	Virtual Channel	Major Ring ID	Alarm
□	1	1	2	1	2	1	10	Major	No	No	1	●
Delete	2	1	1	1	1	1	1	Major	□	□	0	●

Add New Protection Group

Apply Reset

Parameter descriptions:

Delete : This box is used to mark an ERPS for deletion in next Save operation.

Protection group ID : The ID of the created Protection group. Click on the ID of a Protection group to enter the configuration page.

Port 0 : This will create a Port 0 of the switch in the ring.

Port 1 : This will create "Port 1" of the switch in the Ring. As interconnected sub-ring will have only one ring port, "Port 1" is configured as "0" for interconnected sub-ring. "0" in this field indicates that no "Port 1" is associated with this instance

Port 0 SF MEP : The Port 0 Signal Fail reporting MEP.

Port 1 SF MEP : The Port 1 Signal Fail reporting MEP. As only one SF MEP is associated with interconnected sub-ring without virtual channel, it is configured as "0" for such ring instances. "0" in this field indicates that no Port 1 SF MEP is associated with this instance.

Port 0 APS MEP : The Port 0 APS PDU handling MEP.

Port 1 APS MEP : The Port 1 APS PDU handling MEP. As only one APS MEP is associated with interconnected sub-ring without virtual channel, it is configured as "0" for such ring instances. "0" in this field indicates that no Port 1 APS MEP is associated with this instance.

Ring Type : Type of Protecting ring. It can be either major ring or sub-ring.

Interconnected Node : Interconnected Node indicates that the ring instance is interconnected. Click on the checkbox to configure this. "Yes" indicates it is an interconnected node for this instance. "No" indicates that the configured instance is not interconnected.

Virtual Channel : Sub-rings can either have virtual channel or not on the interconnected node. This is configured using "Virtual Channel" checkbox. "Yes" indicates it is a sub-ring with virtual channel. "No" indicates, sub-ring doesn't have virtual channel.

Major Ring ID : Major ring group ID for the interconnected sub-ring. It is used to send topology change updates on major ring. If ring is major, this value is same as the protection group ID of this ring.

Alarm : Red 🔴 There is an active alarm on the ERPS. Green 🟢 No alarm condition exists.

Buttons

Add New Protection Group – Click to add a new Protection group entry.

Refresh – Click to refresh the page immediately.

Apply – Click to save changes.

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

Messages:
'Port 0' and 'Port 1' can not be same
'Port 0 APS MEP' and 'Port 1 APS MEP' can not be same
Port 0 SF MEP and Port 1 SF MEP can not be same

2-16 MAC Table

Switching of frames is based on the DMAC address contained in the frame. The switch builds a table that maps MAC addresses to switch ports for knowing which ports the frames should go to (based on the DMAC address in the frame). This table contains both static and dynamic entries. The static entries are configured by the network administrator if the administrator wants to do a fixed mapping between the DMAC address and switch ports.

The frames also contain a MAC address (SMAC address), which shows the MAC address of the device sending the frame. The SMAC address is used by the switch to automatically update the MAC table with these dynamic MAC addresses. Dynamic entries are removed from the MAC table if no frame with the corresponding SMAC address was seen after a configurable age time.

To configure MAC Address Table in the web interface:

Aging Configuration

1. Click configuration.
2. Specify the Disable Automatic Aging and Aging Time.
3. Click Apply.

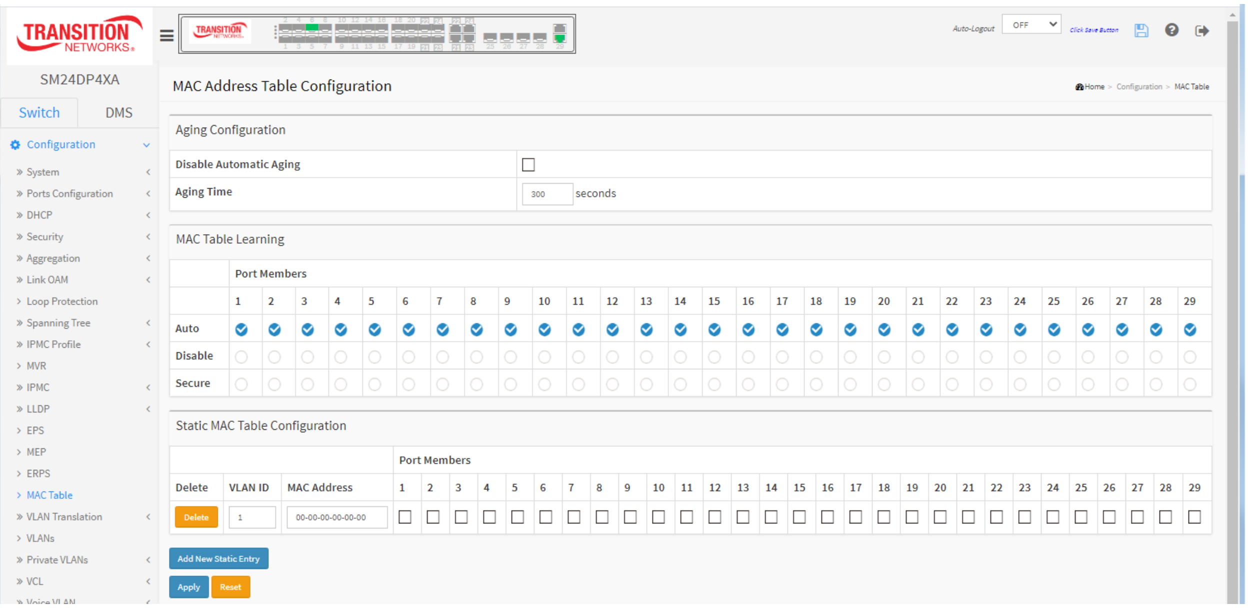
MAC Table Learning

1. Click configuration.
2. Specify the Port Members (Auto, Disable, Secure).
3. Click Apply.

Static MAC Table Configuration

1. Click configuration and Add new Static entry.
2. Specify the VLAN IP and Mac address, Port Members.
3. Click Apply.

Figure 2-16: MAC Address Table Configuration



Auto-Logout OFF

MAC Address Table Configuration

Aging Configuration

Disable Automatic Aging	☐
Aging Time	300 seconds

MAC Table Learning

	Port Members																												
	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29
Auto	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●
Disable	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○
Secure	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○

Static MAC Table Configuration

			Port Members																												
Delete	VLAN ID	MAC Address	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29
Delete	1	00-00-00-00-00-00	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐

Add New Static Entry

Apply Reset

Parameter descriptions:

Aging Configuration : By default, dynamic entries are removed from the MAC table after 300 seconds. This removal is also called aging. Configure aging time by entering a value here in seconds. The allowed range is 10 - 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 MAC table is sorted first by VLAN ID and then by MAC address.

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

VLAN ID : The VLAN ID of the entry.

MAC Address : The MAC address of the entry.

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

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:

Error: mac address:00-00-00-00-00-00 is not multicast mac address, support only one port.

2-17 VLAN Translation

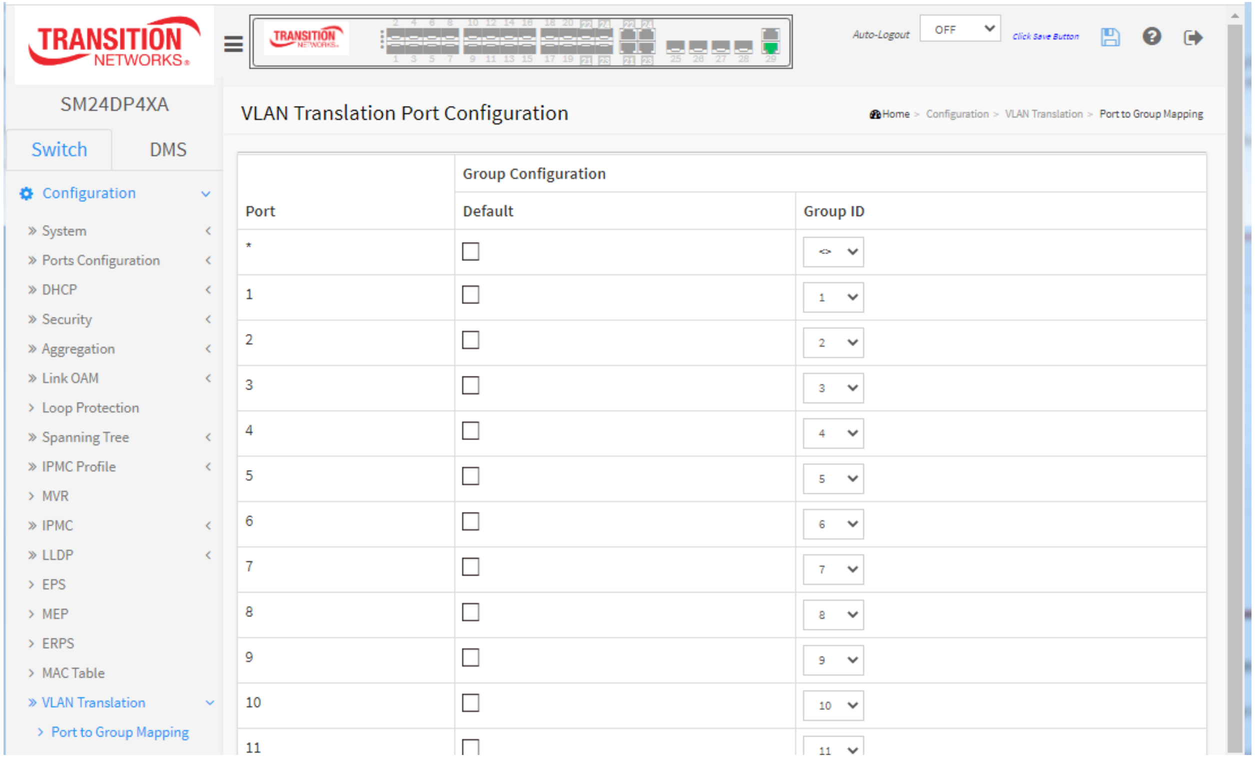
2-17.1 Port to Group Configuration

This page lets you configure switch Ports to use a given VLAN Translation Mapping Group. This will enable all VLAN Translation mappings of that group (if any) on the selected switch port.

Web Interface

To configure VLAN Translation, Port to Group Configuration Table in the web interface:

1. Click Configuration, VLAN Translation, Port to Group Mapping.
2. For each port check the Default checkbox and assign a Group ID as desired.
3. Click the Apply button.



Auto-Logout OFF

VLAN Translation Port Configuration

Port	Group Configuration	
	Default	Group ID
*	□	<>
1	□	1
2	□	2
3	□	3
4	□	4
5	□	5
6	□	6
7	□	7
8	□	8
9	□	9
10	□	10
11	□	11

Parameter descriptions:

Port : The Port column shows the list of ports for which you can configure the VLAN Translation Mapping Group.

Default : To set the switch port to use the default VLAN Translation Group click the checkbox and click Apply.

Group ID : The VLAN Translation mappings are organized into Groups, identified by the Group ID. This way a port is configured to use a number of VLAN Translation mappings easily by simply configuring it to use a given group. The number of possible groups in a switch is equal to the number of ports present in this switch. A port can be configured to use any of the groups, but only one at any given time. Multiple ports can be configured to use the same group. A valid Group ID is an integer value of 1 - 4.
Note: By default, each port is set to use the group with Group ID equal to the port number. For example, port #1 is by default set to use group with GID = 1.

Buttons

Apply : Click to save changes.

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

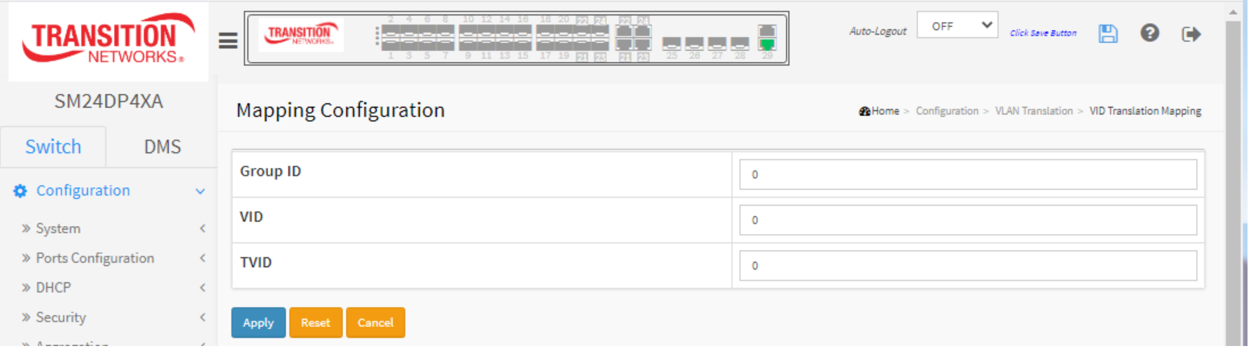
2-17.2 VID Translation Mapping

This page lets you create mappings of VLANs -> Translated VLANs and organize these mappings into global Groups.

Web Interface

To configure VLAN Translation Mapping via the web interface:

1. Click Configuration, VLAN Translation, VID Translation Mapping.
2. Click the Add New Mapping icon (⊕).
3. Enter the Group ID, VID, and TVID parameters.
4. Click the Apply button to save the settings.



Mapping Configuration

Group ID	0
VID	0
TVID	0

Parameter descriptions:

Group ID : The VLAN Translation mappings are organized into Groups, identified by the Group ID. This way a port is configured to use a number of VLAN Translation mappings easily by simply configuring it to use a given group. Then number of possible groups in a switch is equal to the number of ports present in this switch. A port can be configured to use any of the groups, but only one at any given time. Multiple ports can be configured to use the same group. A valid Group ID is an integer value 1 to 29.

Note: By default, each port is set to use the group with Group ID equal to the port number. For example, port #1 is by default set to use group with GID = 1.

VID : Indicates the VLAN of the mapping (i.e. 'source' VLAN). A valid VLAN ID is 1 - 4095.

TVID : Indicates the VLAN ID to which VLAN ID of an ingress frame will be translated to (granted that the mapping is enabled on the ingress port that the frame arrived at). A valid VLAN ID is 1 - 4095.

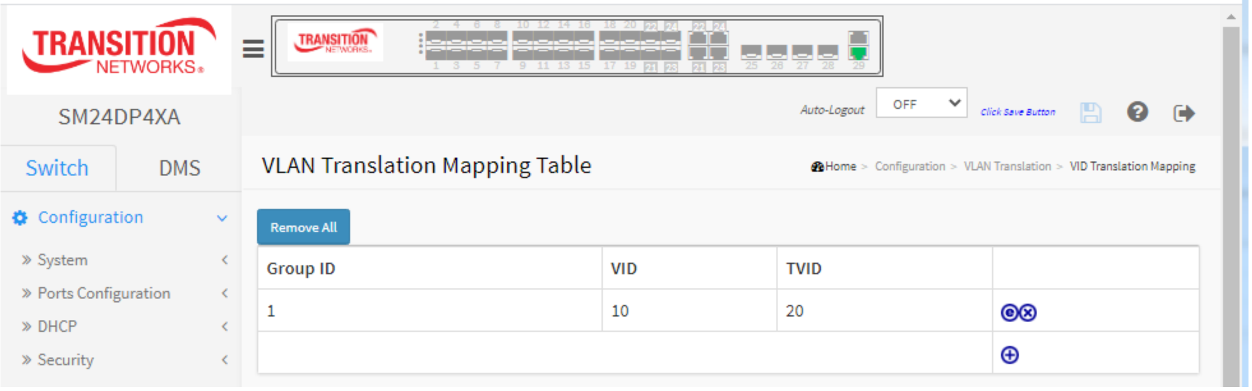
Buttons

Apply : Click to save changes.

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

Cancel : Click to cancel the settings.

After you make entries and click Apply, the VLAN Translation Mapping Table displays:



VLAN Translation Mapping Table

Group ID	VID	TVID	
1	10	20	ⓔ⊗
			⊕

Modification Buttons

You can modify each VLAN Translation mapping in the table using the following buttons:

ⓔ Edit: Edits the mapping row.

⊗ Delete: Deletes the mapping.

⊕ Add: Adds a new mapping.

Buttons

Remove All: Click to remove all VLAN Translation mappings.

2-18 VLANs

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

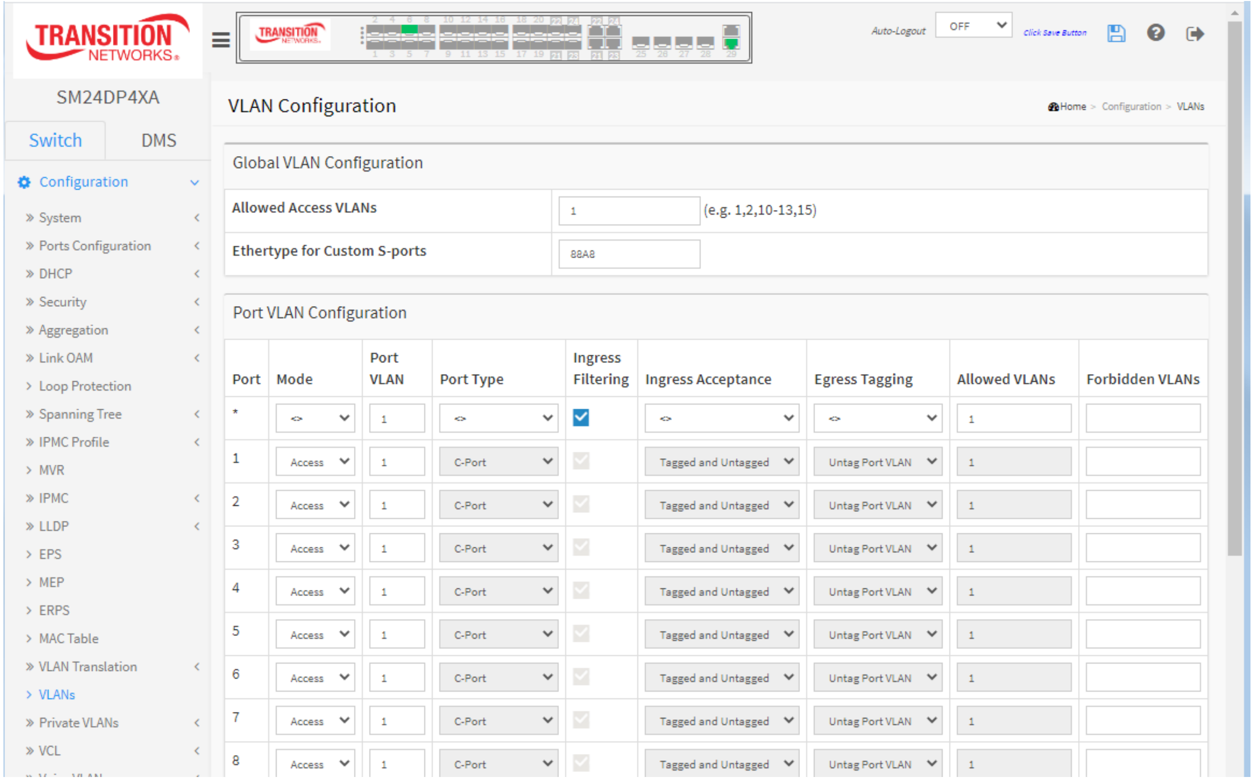
When you specify a new management VLAN, your HTTP connection to the old management VLAN is lost. For this reason, you should have a connection between your management station and a port in the new management VLAN or connect to the new management VLAN through a multi-VLAN route.

Web Interface

To configure VLAN membership configuration in the web interface:

1. Click Configuration, VLANs.
2. Specify the *Global* VLAN Configuration parameters.
3. Specify the *Port* VLAN Configuration parameters.
4. Click Apply.

Figure 2-18.1: VLAN Configuration



VLAN Configuration

Global VLAN Configuration

Allowed Access VLANs	1 (e.g. 1,2,10-13,15)
Ethertype for Custom S-ports	88A8

Port VLAN Configuration

Port	Mode	Port VLAN	Port Type	Ingress Filtering	Ingress Acceptance	Egress Tagging	Allowed VLANs	Forbidden VLANs
*	<>	1	<>	☑	<>	<>	1	
1	Access	1	C-Port	☑	Tagged and Untagged	Untag Port VLAN	1	
2	Access	1	C-Port	☑	Tagged and Untagged	Untag Port VLAN	1	
3	Access	1	C-Port	☑	Tagged and Untagged	Untag Port VLAN	1	
4	Access	1	C-Port	☑	Tagged and Untagged	Untag Port VLAN	1	
5	Access	1	C-Port	☑	Tagged and Untagged	Untag Port VLAN	1	
6	Access	1	C-Port	☑	Tagged and Untagged	Untag Port VLAN	1	
7	Access	1	C-Port	☑	Tagged and Untagged	Untag Port VLAN	1	
8	Access	1	C-Port	☑	Tagged and Untagged	Untag Port VLAN	1	

Parameter descriptions:

Global VLAN Configuration

Allowed Access VLANs: This field shows the allowed Access VLANs (i.e., it only affects ports configured as Access ports). Ports in other modes are members of all VLANs specified in the Allowed VLANs field. By default, only VLAN 1 exists. More VLANs may be created by using a list syntax where the individual elements are separated by commas. Ranges are specified with a dash separating the lower and upper bound. The following example will create VLANs 1, 10, 11, 12, 13, 200, and 300: 1,10-13,200,300. Spaces are allowed in between the delimiters.

Ethertype for Custom S-ports : This field specifies the ethertype/TPID (specified in hexadecimal) used for Custom S-ports. The setting is in force for all ports whose Port Type is set to S-Custom-Port.

Port VLAN Configuration

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

Mode : The port mode (default is Access) determines the fundamental behavior of the port in question. A port can be in one of three modes as described below.
Whenever a particular mode is selected, the remaining fields in that row will be either grayed out or made changeable depending on the mode in question.
Grayed out fields show the value that the port will get when the mode is applied.

> ***Access*:** Access ports are normally used to connect to end stations. Dynamic features like Voice VLAN may add the port to more VLANs behind the scenes. Access ports have the following characteristics:
> - Member of exactly one VLAN, the Port VLAN (a.k.a. Access VLAN), which by default is 1,
> - accepts untagged frames and C-tagged frames,
> - discards all frames that are not classified to the Access VLAN,
> - on egress all frames are transmitted untagged.
>
> ***Trunk*:** Trunk ports can carry traffic on multiple VLANs simultaneously and are normally used to connect to other switches. Trunk ports have the following characteristics:
> - By default, a trunk port is member of all existing VLANs. This may be limited by the use of Allowed VLANs,
> - unless VLAN Trunking is enabled on the port, frames classified to a VLAN that the port is not a member of will be discarded,
> - by default, all frames but frames classified to the Port VLAN (a.k.a. Native VLAN) get tagged on egress. Frames classified to the Port VLAN do not get C-tagged on egress,
> - egress tagging can be changed to tag all frames, in which case only tagged frames are accepted on ingress,
> - VLAN trunking may be enabled.
>
> ***Hybrid*:** Hybrid ports resemble trunk ports in many ways but adds additional port configuration features. In addition to the characteristics described for trunk ports, hybrid ports have these abilities:
> - Can be configured to be VLAN tag unaware, C-tag aware, S-tag aware, or S-custom-tag aware,
> - ingress filtering can be controlled,
> - ingress acceptance of frames and configuration of egress tagging can be configured independently.

Port VLAN : Determines the port's VLAN ID (a.k.a. PVID). Allowed VLANs are in the range 1 – 4095; the default is 1.
On ingress, frames get classified to the Port VLAN if the port is configured as VLAN unaware, the frame is untagged, or VLAN awareness is enabled on the port, but the frame is priority tagged (VLAN ID = 0).
On egress, frames classified to the Port VLAN do not get tagged if Egress Tagging configuration is set to untag Port VLAN.

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

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

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

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

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

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

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

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 Allowed Access VLANs field. By default, a port may become a 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 a member of any of the existing VLANs, but if it is configured for VLAN Trunking it will still be able to carry all unknown VLANs.

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

Buttons

Apply : Click to save changes.

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

2-19 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.

2-19.1 VLAN Membership

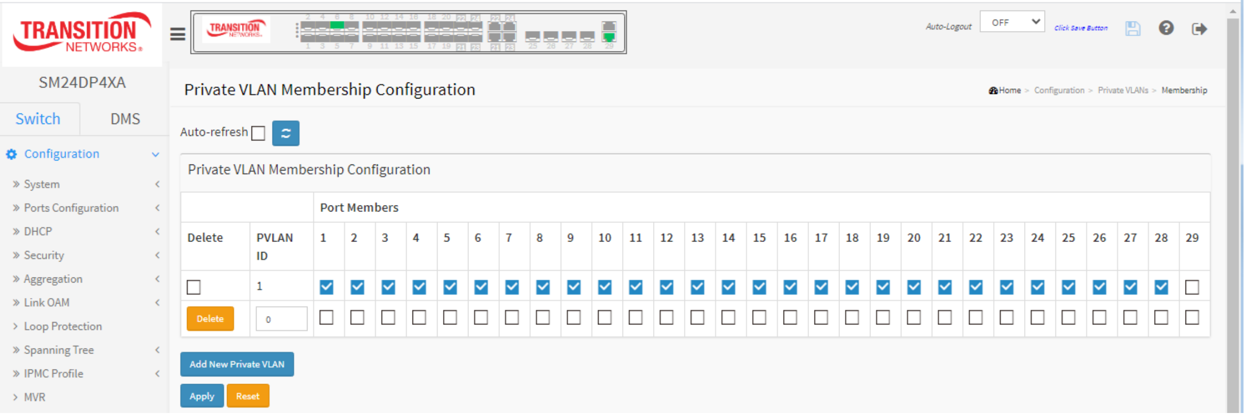
The VLAN membership configuration for the switch can be monitored and modified here. Up to 4096 VLANs are supported. This page allows for adding and deleting VLANs as well as adding and deleting port members of each VLAN.

Web Interface

To configure VLAN membership configuration in the web interface:

1. Click Configuration, Private VLANs, Membership.
2. Click the Add New Private VLAN button.
3. Specify Management VLAN ID (0~ 4094).
4. Click Apply.

Figure 2-19.1: VLAN Membership Configuration



Private VLAN Membership Configuration

Auto-refresh □

Private VLAN Membership Configuration

		Port Members																												
Delete	PVLAN ID	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29
□	1	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	□
Delete	0	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□

Add New Private VLAN

Apply Reset

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.

Add New Private VLAN : Click to add a new private 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 Apply. A VLAN without any port members will be deleted when you click Apply.

The **Delete** button can be used to undo the addition of new VLANs.

Buttons:

Apply – Click to save changes.

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

Note that in order to use DHCP on the SM24DP4XA Management port, the default PVLAN configuration must be changed at Configuration > Private VLANs > Membership.

In order to obtain an address via DHCP, the port must be in PVLAN 1. SM24DP4XA Management port 29 defaults to no PVLAN for port isolation. If you want to use DHCP on the Management port, you must add it to PVLAN 1 and then create another PVLAN if you need port isolation.

2-19.2 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 a data packet is matched with a physical address on said layer 2 switch and a forwarding map is generated for the data packet based upon the destination address on the data packet. The data packet is then sent to the plurality of ports pursuant to the forwarding map generated based upon whether the ingress port was configured as a protected or non-protected port.

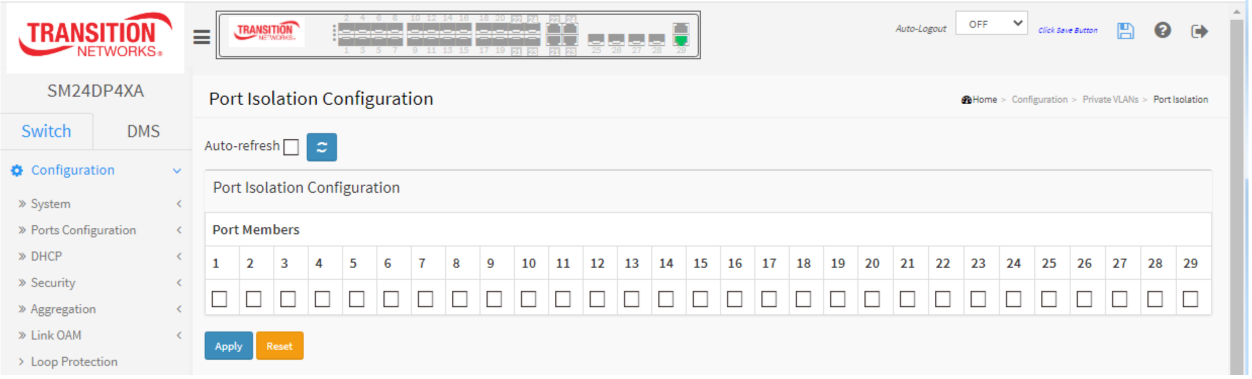
This page is used for enabling or disabling port isolation on ports in a Private VLAN.A port member of a VLAN can be isolated to other isolated ports on the same VLAN and Private VLAN.

Web Interface

To configure Port Isolation configuration in the web interface:

1. Click Configuration, Private VLAN, Port Isolation.
2. Evoke which port want to enable Port Isolation
3. Click Apply.

Figure 2-19.2: Port Isolation Configuration



Port Isolation Configuration

Auto-refresh □

Port Isolation Configuration

Port Members

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29
□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□

Apply Reset

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.

2-20 VCL

2-20.1 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.

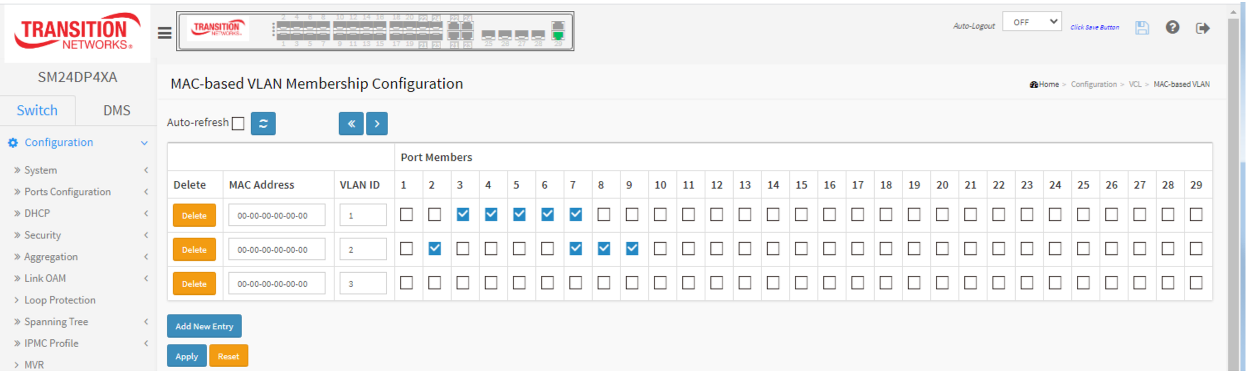
MAC-based VLANs group VLAN members by MAC address. With MAC-based VLAN configured, the device adds a VLAN tag to an untagged frame according to its source MAC address. MAC-based VLANs are mostly used in conjunction with security technologies such as 802.1X to provide secure, flexible network access for 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 2-20.1: MAC-based VLAN Membership Configuration



MAC-based VLAN Membership Configuration

Auto-refresh □

			Port Members																												
Delete	MAC Address	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	25	26	27	28	29
Delete	00-00-00-00-00-00	1	□	□	☑	☑	☑	☑	☑	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□
Delete	00-00-00-00-00-00	2	□	☑	□	□	□	□	☑	☑	☑	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□
Delete	00-00-00-00-00-00	3	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□

Add New Entry

Apply Reset

Parameter descriptions:

Delete : Click to delete a MAC-based VLAN entry.

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.

Buttons:

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

The MAC-based VLAN entry is enabled on the selected switch when you click Apply. A MAC-based VLAN without any port members will be deleted when you click Apply. The **Reset** button can be used to undo the addition of new MAC-based VLANs.

Apply – Click to save changes.

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

2-20.2 Protocol -based VLAN

This section describes Protocol -based VLANs; switch protocol support includes Ethernet, LLC, and SNAP Protocols.

LLC : The Logical Link Control (LLC) data communication protocol layer is the upper sub-layer of the Data Link Layer (which is itself layer 2, just above the Physical Layer) in the seven-layer OSI reference model. It provides multiplexing mechanisms that make it possible for several network protocols (IP, IPX, Decnet and AppleTalk) to coexist within a multipoint network and to be transported over the same network media, and can also provide flow control and automatic repeat request (ARQ) error management mechanisms.

SNAP : The Subnetwork Access Protocol (SNAP) is a mechanism for multiplexing, on networks using IEEE 802.2 LLC, more protocols than can be distinguished by the 8-bit 802.2 Service Access Point (SAP) fields. SNAP supports identifying protocols by Ethernet type field values; it also supports vendor-private protocol identifier spaces. It is used with IEEE 802.3, IEEE 802.4, IEEE 802.5, IEEE 802.11 and other IEEE 802 physical network layers, as well as with non-IEEE 802 physical network layers such as FDDI that use 802.2 LLC.

2-20.2.1 Protocol to Group

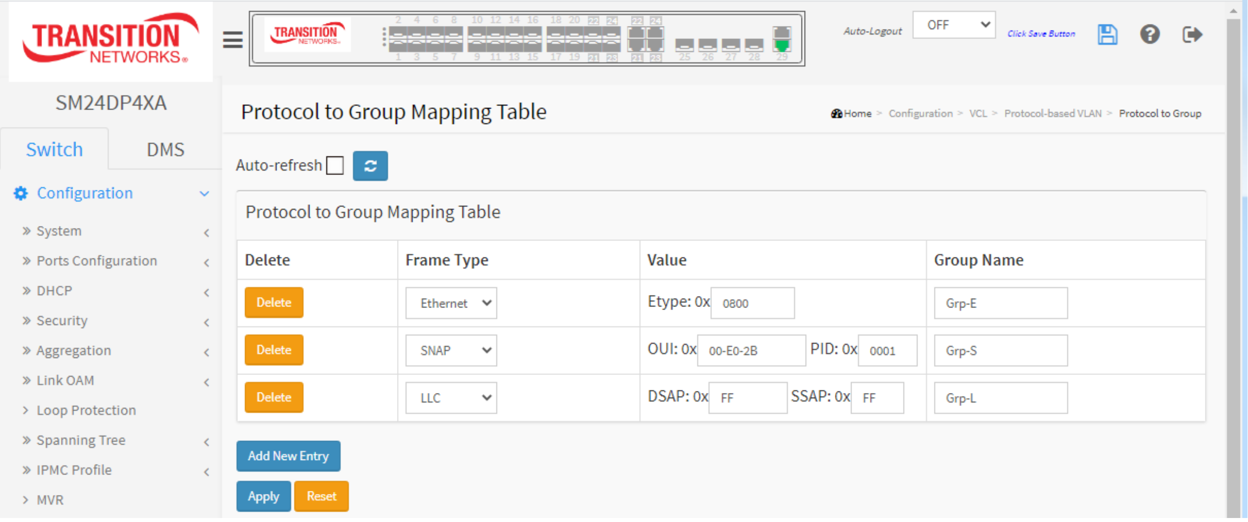
This page allows you to add new protocols to Group Name (unique for each Group) mapping entries as well as allow you to see and delete already mapped entries for the selected switch.

Web Interface

To configure Protocol -based VLAN configuration in the web interface:

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

Figure 2-20.2.1: Protocol to Group Mapping Table



Auto-Logout: OFF

Protocol to Group Mapping Table

Auto-refresh □

Protocol to Group Mapping Table

Delete	Frame Type	Value	Group Name
Delete	Ethernet	Etype: 0x 0800	Grp-E
Delete	SNAP	OUI: 0x 00-E0-2B PID: 0x 0001	Grp-S
Delete	LLC	DSAP: 0x FF SSAP: 0x FF	Grp-L

Add New Entry

Apply Reset

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 : Frame Type can have one of the following values: **Ethernet**, **LLC**, or **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 are 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 string for every entry which consists of a combination of alpha characters (a-z or A-Z) and numeric characters (0-9).

NOTE: Special characters and underscore (_) are not allowed.

Add New Entry : Click to add a new entry in mapping table. An empty row is added to the table; Frame Type, Value and the Group Name can be configured as needed.

The **Delete** button can be used to undo the addition of new entry.

Buttons:

Save – Click to save changes.

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

Refresh : Click them for refresh webpage information manually.

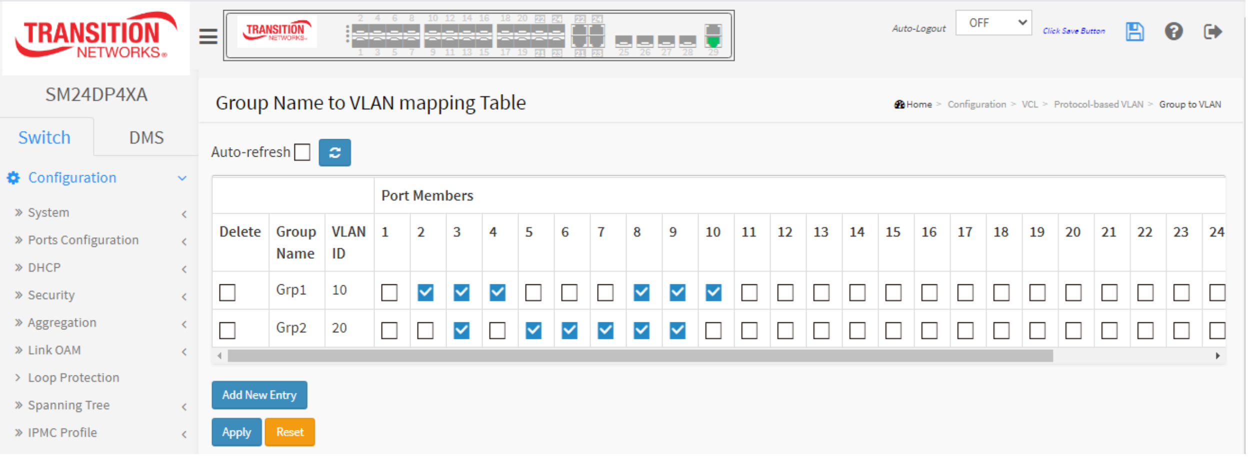
2-20.2.2 Group to VLAN

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

To configure the Group Name to VLAN mapping table configured 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. Check the desired Port Members checkboxes.
5. Click Apply.

Figure 2-20.2.2: Group Name to VLAN mapping Table



Group Name to VLAN mapping Table

Auto-refresh □

			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
□	Grp1	10	□	☑	☑	☑	□	□	□	☑	☑	☑	□	□	□	□	□	□	□	□	□	□	□	□	□	□
□	Grp2	20	□	□	☑	□	☑	☑	☑	☑	☑	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□

Add New Entry

Apply Reset

Parameter descriptions:

Delete : To delete a Group Name to VLAN map entry, check this box.

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 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:

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 - 4095. The Reset button can be used to undo the addition of new entry.

Apply – Click to save changes.

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

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

Refresh: Click to immediately refresh the page.

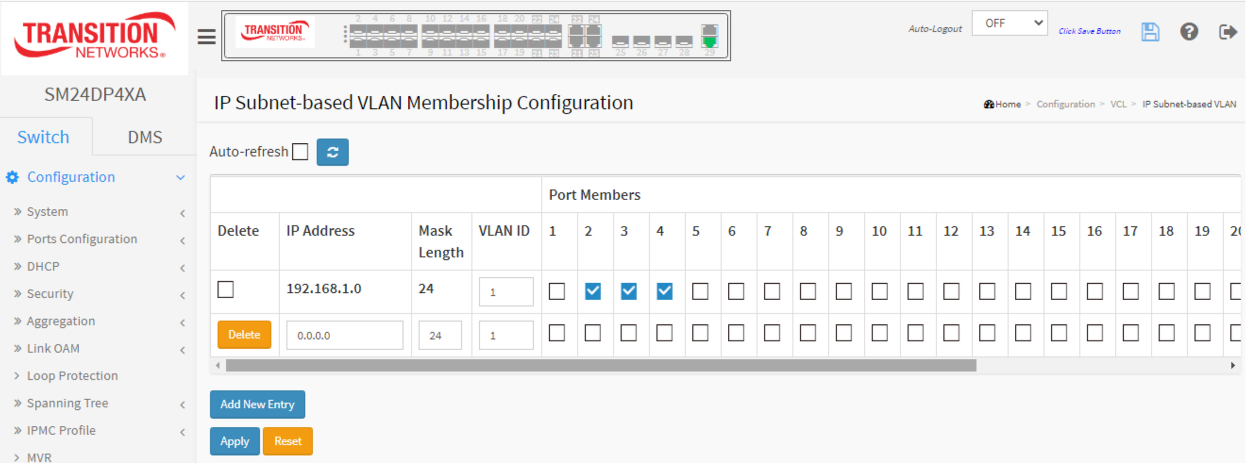
2-20.3 IP Subnet-based VLAN

The IP subnet-based VLAN entries can be configured here. This page allows for adding, updating and deleting IP subnet-based VLAN entries and assigning the entries to different ports. This page shows only static entries.

To 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.
3. Specify the IP Address, Mask Length, and VLAN ID.
4. Select Port Members.
5. Click Apply.

Figure 2-20.3: IP Subnet-based VLAN Membership Configuration



IP Subnet-based VLAN Membership Configuration

Auto-refresh □

				Port Members																			
Delete	IP Address	Mask Length	VLAN ID	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
□	192.168.1.0	24	1	□	☑	☑	☑	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□
Delete	0.0.0.0	24	1	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□

Add New Entry

Apply Reset

Delete : To delete an IP subnet-based VLAN entry, click this button.

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:

Add New Entry : Click to add a new IP subnet-based VLAN entry. An empty row is added to the table, and the IP subnet-based VLAN entry can be configured as needed. Any IP address/mask can be configured for the IP subnet-based VLAN entry. Valid values for VLAN ID are 1 - 4095. The IP subnet-based VLAN entry is enabled when you click Apply. The “Delete” button can be used to undo the addition of new IP subnet-based VLANs. You can enter up to 128 IP subnet-based VLAN entries.

Apply – Click to save changes.

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

Message : *Subnet 0.0.0.0/x is not valid. Please use a non-zero subnet.*

2-21 VOICE VLAN

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

2-21.1 Configuration

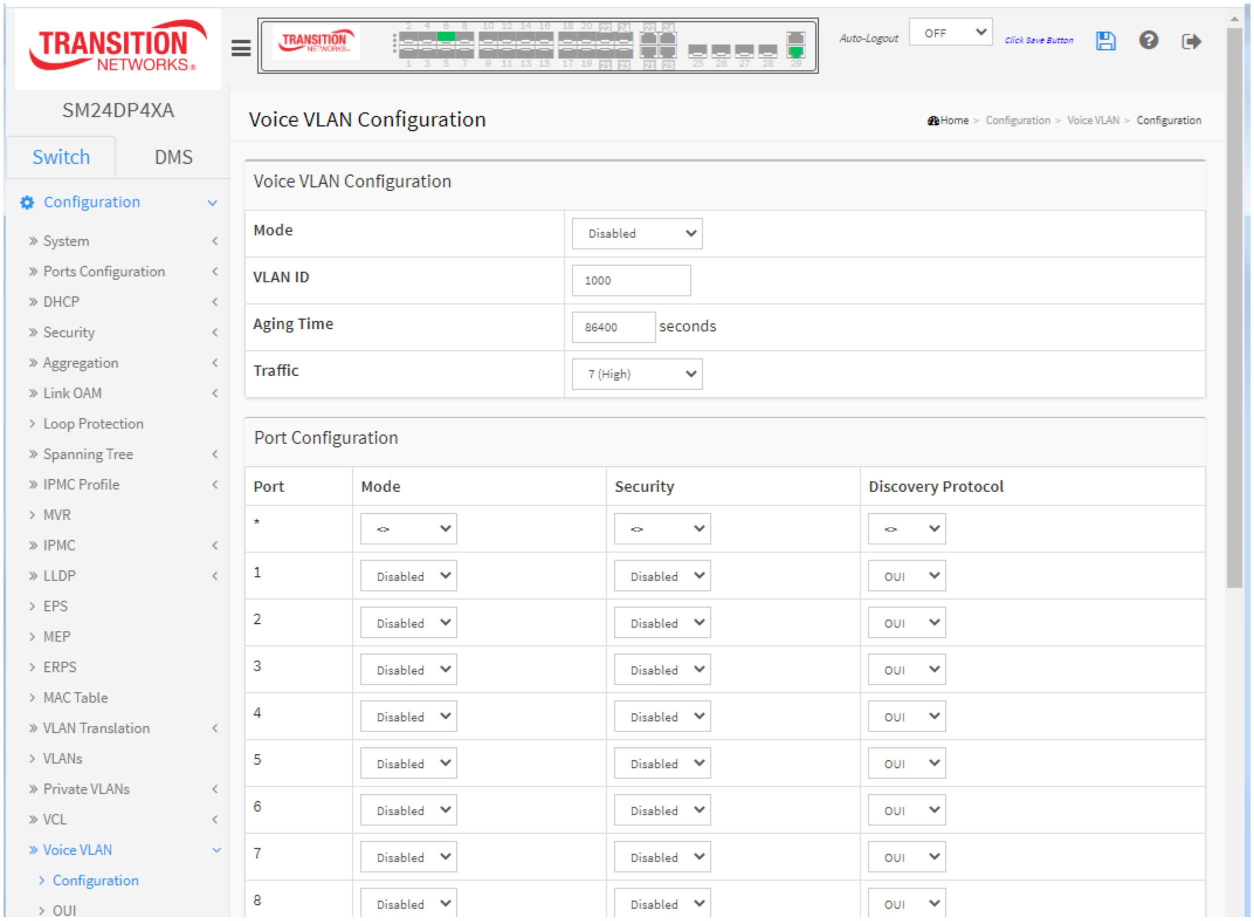
The Voice VLAN feature enables voice traffic forwarding on the Voice VLAN, then the switch can classify and schedule network traffic. It is recommended that there be two VLANs on a port - one for voice, one for data. Before connecting the IP device to the switch, the IP phone should configure the voice VLAN ID correctly. It should be configured through its own GUI.

Web Interface

To configure Voice VLAN via the web interface:

1. Click Configuration, Voice VLAN, Configuration.
2. Select “Enabled” at the Mode dropdown in the Voice VLAN Configuration section.
3. Specify VLAN ID, Aging Time, and Traffic Class.
4. Specify (Mode, Security, and Discovery Protocol) in the Port Configuration section.
5. Click Apply.

Figure 2-21.1: Voice VLAN Configuration



Voice VLAN Configuration

Voice VLAN Configuration

Mode	Disabled
VLAN ID	1000
Aging Time	86400 seconds
Traffic	7 (High)

Port Configuration

Port	Mode	Security	Discovery Protocol
*	<>	<>	<>
1	Disabled	Disabled	OUI
2	Disabled	Disabled	OUI
3	Disabled	Disabled	OUI
4	Disabled	Disabled	OUI
5	Disabled	Disabled	OUI
6	Disabled	Disabled	OUI
7	Disabled	Disabled	OUI
8	Disabled	Disabled	OUI

Parameter descriptions:

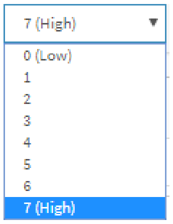
Mode : Sets the Voice VLAN mode operation. You must disable MSTP feature before we enable Voice VLAN. It can avoid the conflict of ingress filtering. Possible modes are:

Enabled: Enable Voice VLAN mode operation.

Disabled: Disable Voice VLAN mode operation.

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

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



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

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 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 the auto detect process. Possible discovery protocols are:

OUI: Detect telephony device by OUI address.

LLDP: Detect telephony device by LLDP.

Both: Both OUI and LLDP.

Buttons:

Save – Click to save changes.

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

2-21.2 OUI

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

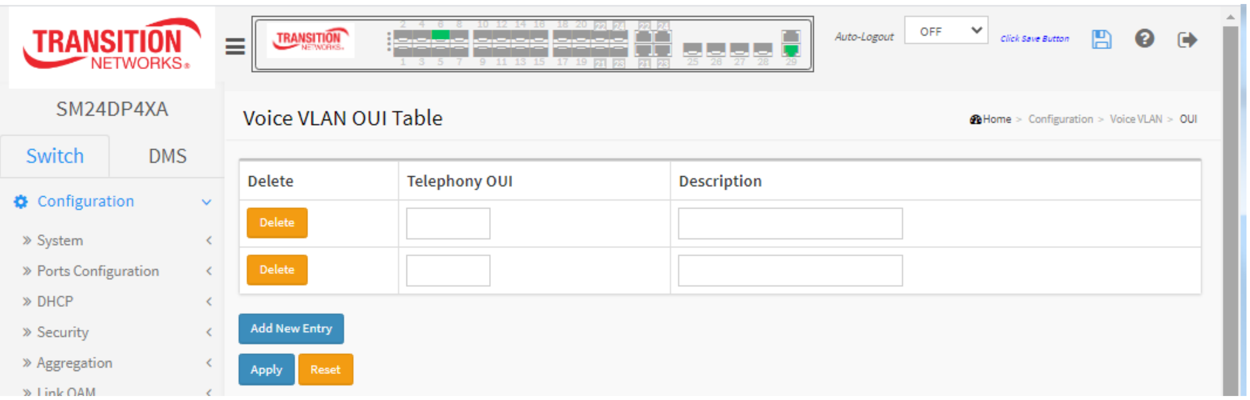
Voice VLAN is VLAN configured specially for voice traffic. By adding ports with voice devices attached to voice VLAN, you can perform QoS-related configuration for voice data, ensuring the transmission priority of voice traffic and voice quality.

Web Interface

To configure the Voice VLAN OUI Table via the web interface:

1. Click Configuration, Voice VLAN, OUI.
2. Click the Add New Entry button.
3. Specify the Telephony OUI and Description parameters.
4. Click Apply.

Figure 2-21.2: Voice VLAN OUI Table



Voice VLAN OUI Table

Delete	Telephony OUI	Description
Delete		
Delete		

Add New Entry

Apply Reset

Parameter descriptions:

Delete : Click to delete the entry.

Telephony OUI : A telephony OUI address is a globally unique identifier assigned to a vendor by IEEE. It must be 6 characters long and the input format is "xx-xx-xx" (where x is a hexadecimal digit).

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

Buttons:

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

Apply : Click to save changes.

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

2-22 Ethernet Services

Ethernet Virtual Connection (EVC) can utilize dedicated policers and shapers, statistics, queues, and tagging/marking schemes. Further, each connection may use built-in service activation testing when first provisioned; dedicated OAM functions ensure fault-free and SLA-compliant operation.

An EVC (Ethernet Virtual Connection) is a MEF standard that describes services provided to customers at User Network Interfaces (UNIs). Inside provider networks, nodes are connected using Internal Network-to-Network Interfaces (I-NNIs). Connections between service providers are done using External Network-to-Network Interfaces (E-NNIs). An Ethernet Virtual Connection is an association of two or more UNIs.

2-22.1 Port Configuration

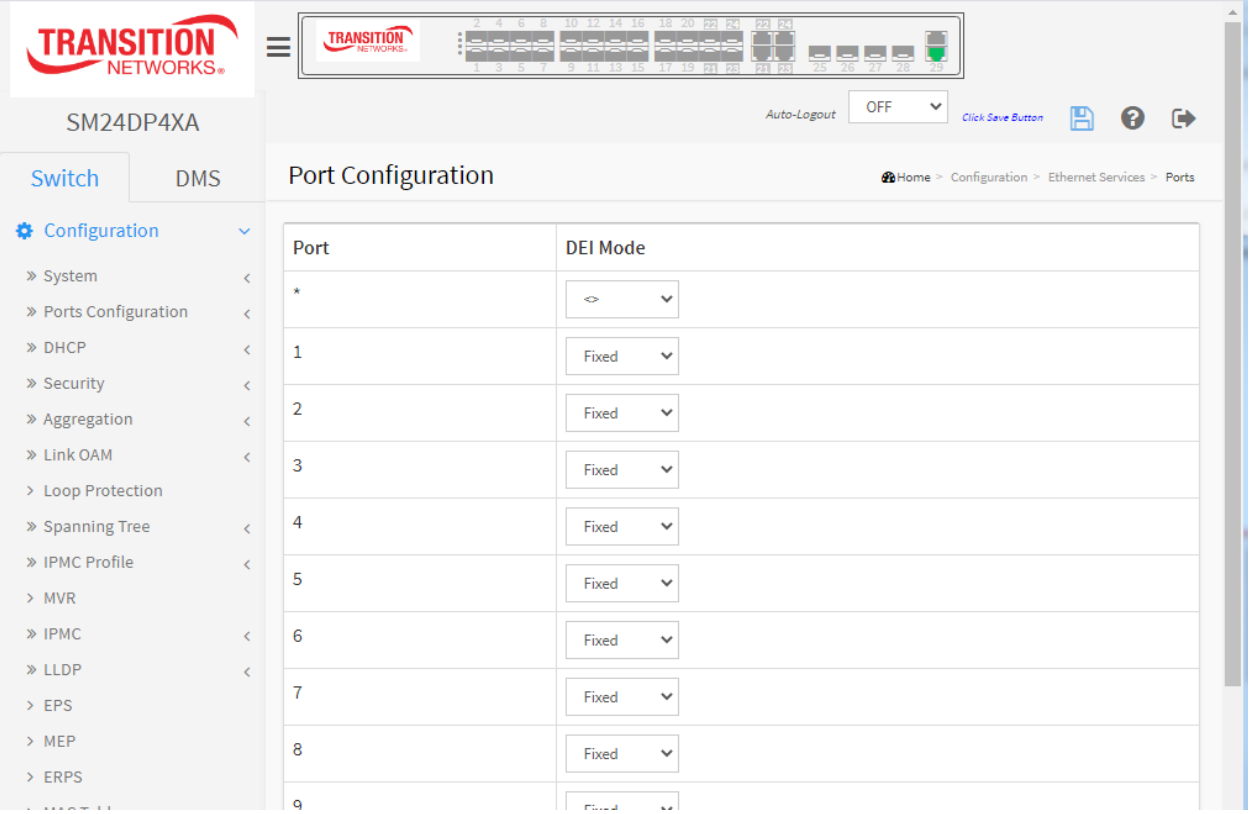
This page lets you view and configure current EVC port parameters.

Web Interface

To configure EVC Port Configuration in the web interface:

1. Click Configuration, Ethernet Services, Ports.
2. Select a DEI Mode for each port.
3. Click the Apply button to save the settings.

Figure 2-22.1: Ethernet Services Port Configuration



Port	DEI Mode
*	<>
1	Fixed
2	Fixed
3	Fixed
4	Fixed
5	Fixed
6	Fixed
7	Fixed
8	Fixed
9	Fixed

Parameter descriptions:

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

DEI Mode : The DEI mode for an NNI port determines whether frames transmitted on the port will have the DEI field in the outer tag marked based on the color of the frame. The allowed values are:

Coloured: The DEI is 1 for yellow frames and 0 for green frames.

Fixed: The DEI value is determined by ECE rules.

Buttons:

Apply : Click to save changes.

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

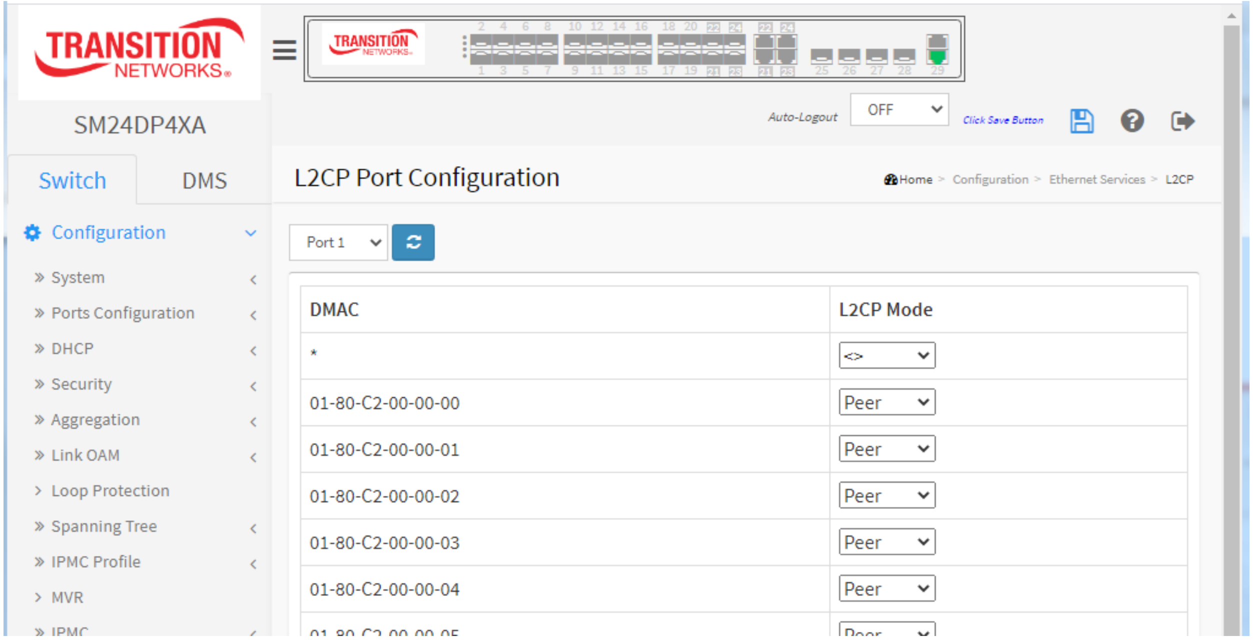
2-22.2 L2CP

This page lets you view and configure current EVC L2CP parameters.

To configure L2CP Configuration in the web interface:

1. Click Configuration, Ethernet Services, L2CP.
2. Select a port at the port select dropdown.
3. Select an L2CP Mode for each DMAC (Destination MAC).
4. Click the Apply button to save the settings.

Figure 2-22.1: Ethernet Service L2CP Configuration



L2CP Port Configuration

DMAC	L2CP Mode
*	<>
01-80-C2-00-00-00	Peer
01-80-C2-00-00-01	Peer
01-80-C2-00-00-02	Peer
01-80-C2-00-00-03	Peer
01-80-C2-00-00-04	Peer
01-80-C2-00-00-05	Peer

Parameter descriptions:

DMAC : The destination BPDU MAC addresses (01-80-C2-00-00-0X) and GARP (01-80-C2-00-00-2X) MAC addresses for the settings contained in the same row.

L2CP Mode : The L2CP mode for the specific port. The possible values are:

Peer : Allow to peer L2CP frames.

Forward : Allow to forward L2CP frames.

Buttons

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

Refresh : Click to refresh the page.

Apply : Click to save changes.

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

2-22.2 Bandwidth Profiles

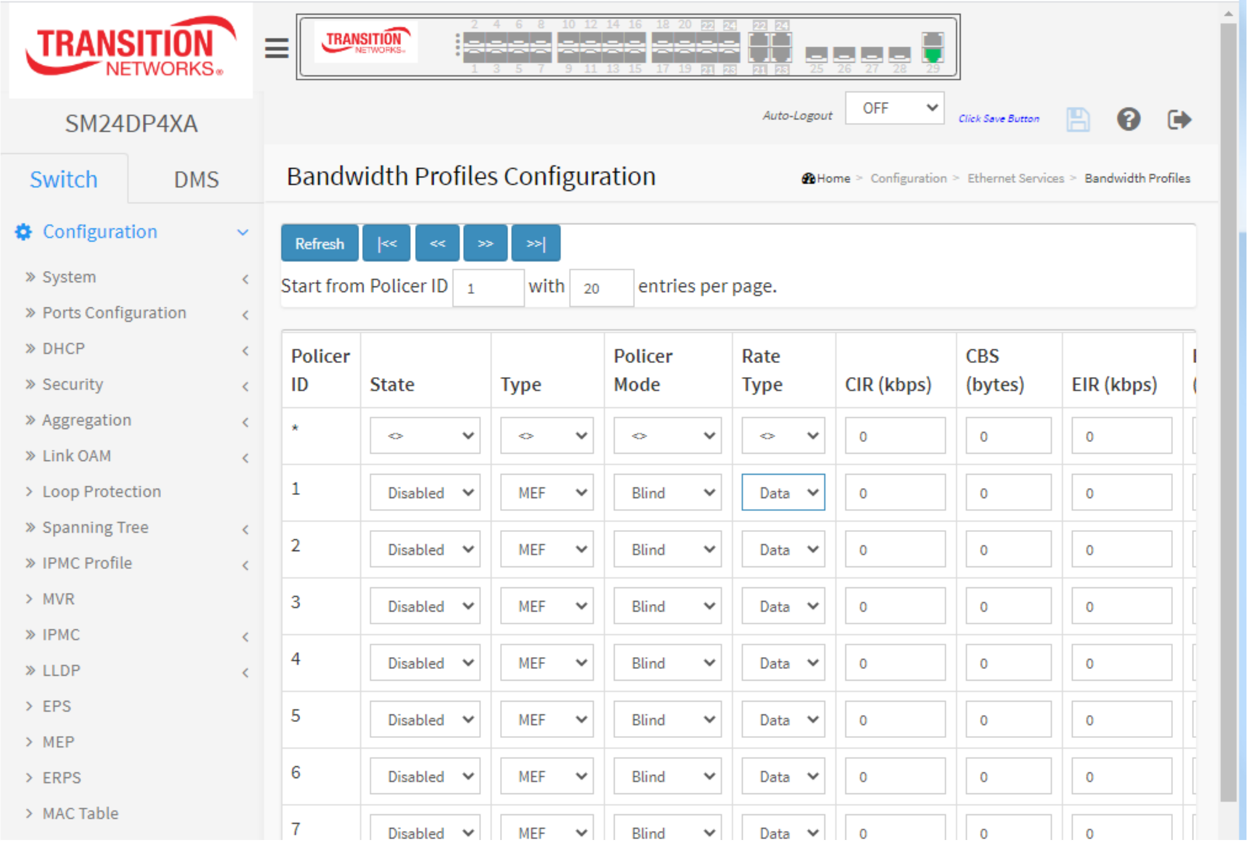
This page lets you view and configure current EVC ingress bandwidth profile configurations. These policers may be used to limit the traffic received on UNI ports.

Web Interface

To configure EVC Bandwidth Profiles Configuration in the web interface:

1. Click Configuration, Ethernet Services, Bandwidth Profiles.
2. Set the Start from Policer ID and entries per page.
3. For each desired Policer ID set the State, Type, Policer Mode, Rate Type, CIR, CBS, EIR, and EBS parameters.
4. Click the Apply button to save the settings.

Figure 2-22.1: Bandwidth Profiles Configuration



Bandwidth Profiles Configuration

Start from Policer ID 1 with 20 entries per page.

Policer ID	State	Type	Policer Mode	Rate Type	CIR (kbps)	CBS (bytes)	EIR (kbps)
*	<>	<>	<>	<>	0	0	0
1	Disabled	MEF	Blind	Data	0	0	0
2	Disabled	MEF	Blind	Data	0	0	0
3	Disabled	MEF	Blind	Data	0	0	0
4	Disabled	MEF	Blind	Data	0	0	0
5	Disabled	MEF	Blind	Data	0	0	0
6	Disabled	MEF	Blind	Data	0	0	0
7	Disabled	MEF	Blind	Data	0	0	0

Parameter descriptions:

Start from Policer ID : The start Policer ID for displaying the table entries. The allowed range is 1 - 2048.

entries per page : The number of entries per page. The allowed range is 2 - 2048.

Policer ID : The Policer ID is used to identify one of the 2048 policers.

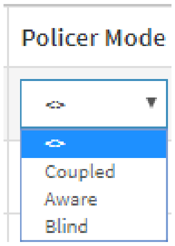
State : The administrative state of the bandwidth profile. The allowed values are:

> ***Enabled***: The bandwidth profile enabled.
>
> ***Disabled***: The bandwidth profile is disabled.

Type : The policer type of the bandwidth profile. The allowed values are:

MEF: MEF ingress bandwidth profile.

Single: Single bucket policer.



Policer Mode : The colour mode of the bandwidth profile. The allowed values are:

Coupled: Colour-aware mode with coupling enabled.

Aware: Colour-aware mode with coupling disabled.

Blind: Colour-blind mode (the default).

Rate Type : The rate type of the bandwidth profile. The allowed values are:

Data: Specify that this bandwidth profile operates on data rate.

Line: Specify that this bandwidth profile operates on line rate.

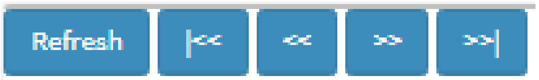
CIR : The Committed Information Rate of the bandwidth profile. The allowed range is 0 - 10000000 kilobit per second (Kbps).

CBS : The Committed Burst Size of the bandwidth profile. The allowed range is 0 - 100000 bytes.

EIR : The Excess Information Rate for MEF type bandwidth profile. The allowed range is 0 - 10000000 kilobit per second.

EBS : The Excess Burst Size for MEF type bandwidth profile. The allowed range is 0 - 100000 bytes.

Buttons



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

|<< **:** First page: Updates the table, starting with the first entry in the table.

<< : Previous page : Updates the table, ending at the entry before the first entry currently displayed.

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

>**|** **: Last page :** Updates the table, ending at the last entry in the table.

Apply : Click to save changes.

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

2-22.3 EVCs

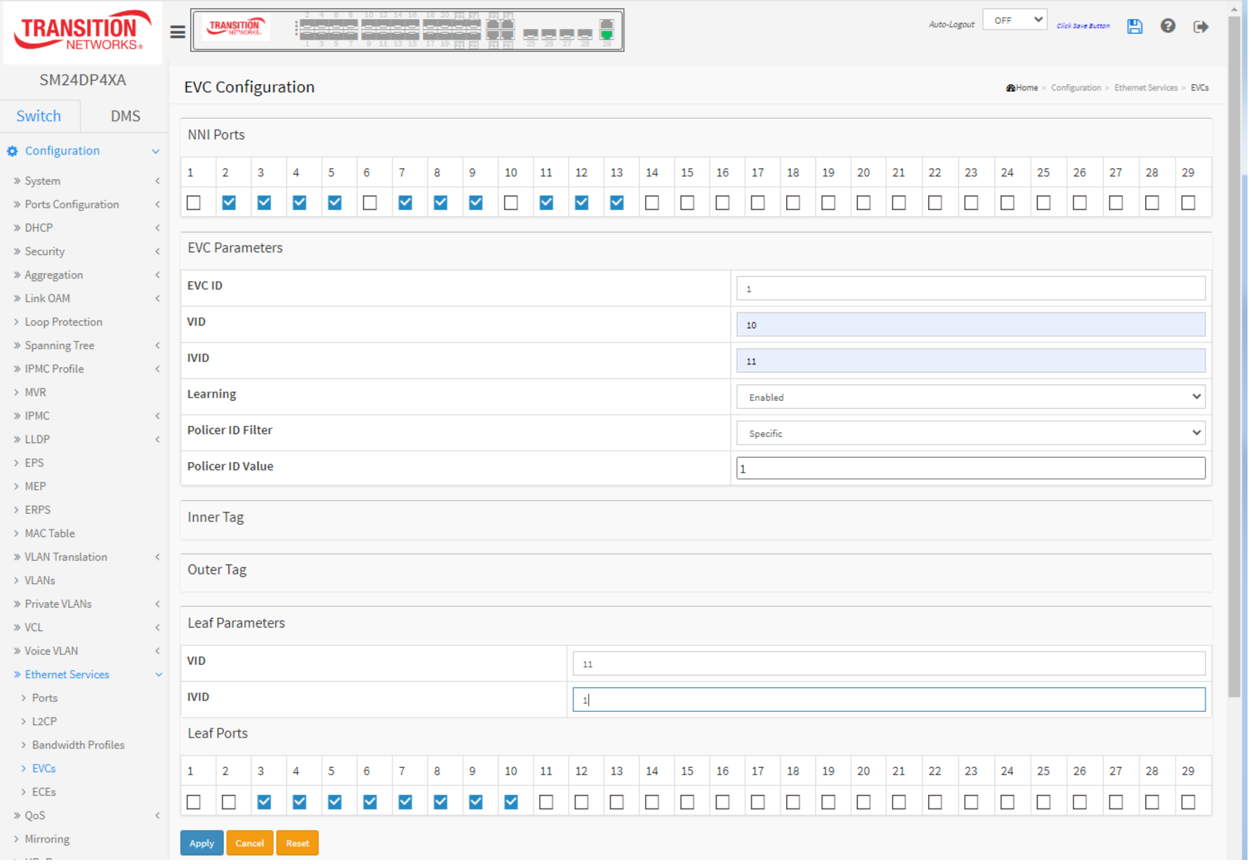
This page lets you view and configure the current EVC Control Entries. AN EVC (Ethernet Virtual Connection) is a MEF standard that describes services provided to customers at User Network Interfaces (UNIs). Inside provider networks, nodes are connected using Internal Network-to-Network Interfaces (I-NNIs). Connections between service providers are done using External Network-to-Network Interfaces (E-NNIs). An Ethernet Virtual Connection is an association of two or more UNIs.

Web Interface

To configure EVC Control Entries in the web interface:

1. Click Configuration, Ethernet Services, EVCs to display the EVC Control List Configuration page.
2. Click the Add New EVC icon (⊕) to display the EVC Configuration page.
3. Enter the EVC Configuration parameters.
4. Click the Apply button.
5. Set the EVC Configuration parameters.
6. Use the Modification buttons as required.
7. Click the Apply button to save the entries.

Figure 2-22.3: EVC Configuration



EVC Configuration

NNI Ports

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29
□	☑	☑	☑	☑	□	☑	☑	☑	□	☑	☑	☑	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□

EVC Parameters

EVC ID	1
VID	10
IVID	11
Learning	Enabled
Policer ID Filter	Specific
Policer ID Value	1

Inner Tag

Outer Tag

Leaf Parameters

VID	11
IVID	1

Leaf Ports

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29
□	□	☑	☑	☑	☑	☑	☑	☑	☑	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□

Parameter descriptions:

NNI Ports: The list of Network to Network Interfaces for the EVC.

<u>EVC Parameters:</u>

EVC ID : The EVC ID identifies the EVC. The range is 1 - 256.

VID : The VLAN ID in the PB network. It may be inserted in a C-tag, S-tag or S-custom tag depending on the NNI port VLAN configuration. The range is 0 - 4095.

IVID : The Internal/classified VLAN ID in the PB network. The range is 1 - 4095.

Learning : The learning mode for the EVC controls whether source MAC addresses are learned for frames matching the EVC. Learning may be disabled if the EVC only includes two UNI/NNI ports. Valid values are:

Enabled: Learning is enabled (MAC addresses are learned).

Disabled: Learning is disabled (MAC addresses are not learned).

Policer ID Filter: The ingress bandwidth profile mode for the EVC. Valid values are:

Specific: The range is from 1 through 256.

Discard: All received frames are discarded for the EVC.

None: None bandwidth profile for the EVC.

Leaf Parameters:

Leaf VID : The leaf VLAN ID used in the outer tag for the EVC. The allowed range is 0 - 4095.

Leaf IVID : The leaf internal classified VLAN ID for the EVC. The allowed range is 0-4095.

Leaf Ports : The list of leaf ports for the EVC. Check the boxes as required. EVC internal VID and Leaf internal VID must be different.

Buttons

Refresh : Click to refresh the page.

Remove All : Click to remove all ECEs. At the confirmation prompt click OK.

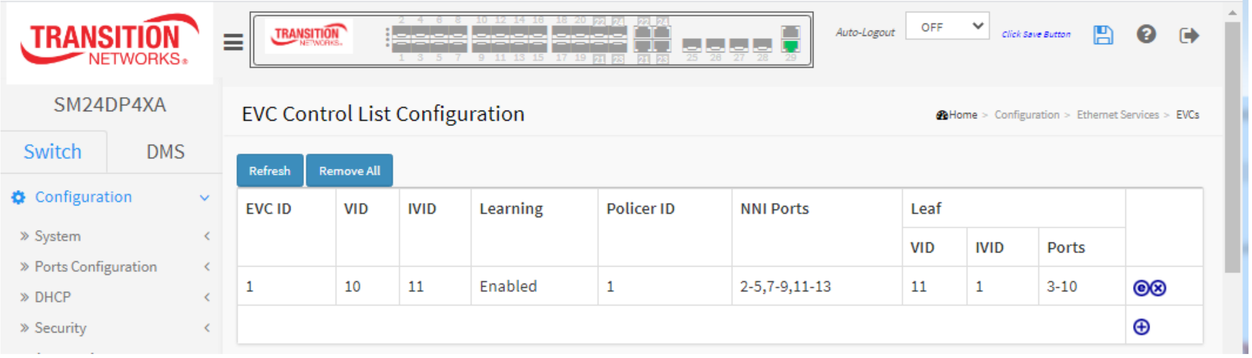
Apply : Click to save changes.

Cancel : Return to the previous page; any changes made locally will be undone.

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

EVC Control List Configuration

This page displays current EVC configurations. Only Provider Bridge based EVCs are supported.



EVC Control List Configuration

EVC ID	VID	IVID	Learning	Policer ID	NNI Ports	Leaf			
						VID	IVID	Ports	
1	10	11	Enabled	1	2-5,7-9,11-13	11	1	3-10	ⓔⓧ
									⊕

Parameter descriptions:

EVC ID : The EVC ID identifies the EVC. The range is 1 - 4096.

VID : The VLAN ID in the PB network. It may be inserted in a C-tag, S-tag or S-custom tag depending on the NNI port VLAN configuration. The range is 1 - 4095.

IVID : The Internal/classified VLAN ID in the PB network. The valid range is 1 - 4095.

Learning : The learning mode for the EVC controls whether source MAC addresses are learned for frames matching the EVC. Learning may be disabled if the EVC only includes two UNI/NNI ports. Valid values are:

Enabled: Learning is enabled (MAC addresses are learned).

Disabled: Learning is disabled (MAC addresses are not learned).

Policer ID : The ingress bandwidth profile mode for the EVC. Valid values are:

Specific: The range is 1 - 256.

Discard: All received frames are discarded for the EVC.

None: None bandwidth profile for the EVC.

NNI Ports : The list of Network to Network Interfaces for the EVC.

Leaf VID : The leaf VLAN ID used in the outer tag for the EVC.

Leaf IVID : The leaf internal classified VLAN ID for the EVC.

Leaf Ports : The list of leaf ports for the EVC.

Modification Buttons

You can modify each EVC in the table using the following buttons:

⊕: Add new EVC.

ⓔ: Edit the EVC row.

ⓧ: Delete the EVC.

2-22.4 ECEs

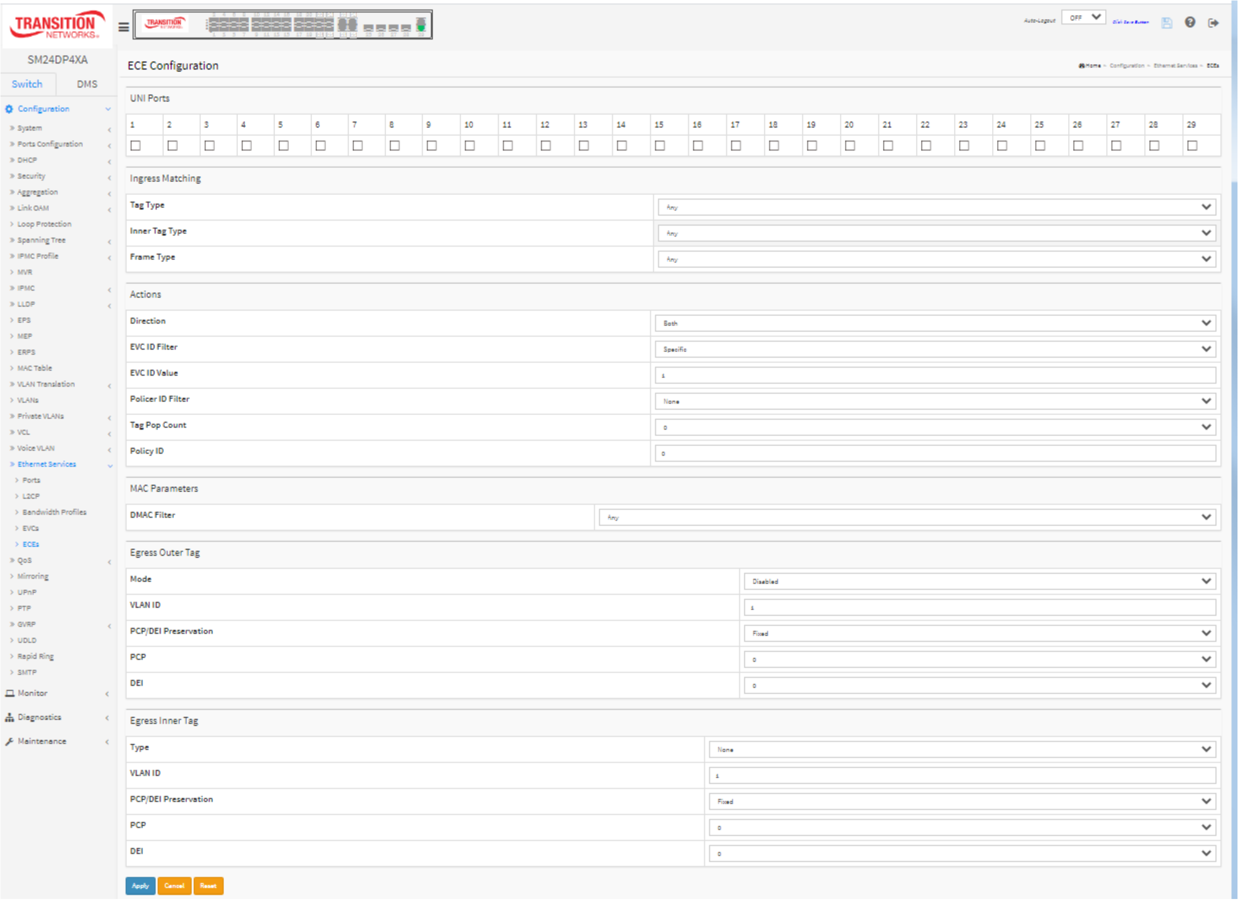
This page lets you view and configure current ECE configurations.

Web Interface

To configure ECE Control Entries in the web interface:

1. Click Configuration, Ethernet Services, ECEs to display the ECE Control List Configuration page.
2. Click the ⊕ modification button to add a new entry at the bottom of the ECE Configuration table.
3. Select the UNI Ports.
4. Select the Ingress Matching parameters.
5. Set the Action parameters and the MAC parameters.
6. Set the Egress Outer Tag parameters and the Egress Inner Tag parameters.
7. Click the Apply button to save the settings.

Figure 2-22.4: ECE Configuration



Auto-Logout: OFF

ECE Configuration

UNI Ports

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29
□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□

Ingress Matching

Tag Type	Any
Inner Tag Type	Any
Frame Type	Any

Actions

Direction	Both
EVC ID Filter	Specific
EVC ID Value	1
Policer ID Filter	None
Tag Pop Count	0
Policy ID	0

MAC Parameters

DMAC Filter	Any

Egress Outer Tag

Mode	Disabled
VLAN ID	1
PCP/DEI Preservation	Fixed
PCP	0
DEI	0

Egress Inner Tag

Type	None
VLAN ID	1
PCP/DEI Preservation	Fixed
PCP	0
DEI	0

Parameter descriptions:

UNI Ports : The list of User Network Interfaces for the ECE. Check the checkbox to include the desired ports.

Ingress Matching

Tag Type : The tag type for matching the ECE. The possible values are:

Any: The ECE will match both tagged and untagged frames.

Untagged: The ECE will match untagged frames only.

C-Tagged: The ECE will match custom tagged frames only.

S-Tagged: The ECE will match service tagged frames only.

Tagged: The ECE will match tagged frames only.

VLAN ID Filter : The VLAN ID filter for matching the ECE. It is only significant if tag type 'Tagged' is selected. The possible values are:

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 value with this ECE, choose this value. A field for entering a specific value appears.

Range: If you want to filter a specific VLAN ID range filter with this ECE, choose this value. A field for entering a range appears.

VLAN ID Value : When "Specific" is selected for the VLAN ID filter, you can enter a specific value. The allowed value is 0 - 4095.

VLAN ID Range : When "Range" is selected for the VLAN ID filter, you can enter a specific range. The allowed range is 0 - 4095.

PCP : The PCP value for matching the ECE. Only significant if tag type 'Tagged' is selected. Valid values:

Any: The ECE will match any PCP value.

Specific: The ECE will match a specific PCP in the range 0 - 7.

Range: The ECE will match PCP values in the selected range 0-1, 2-3, 4-5, 6-7, 0-3 or 4-7.

DEI : The DEI value for matching the ECE. It only significant if tag type 'Tagged' is selected. The allowed values are: 0, 1 or Any.

Inner Tag Type : The inner tag type for matching the ECE. The possible values are:

Any: The ECE will match both tagged and untagged frames.

Untagged: The ECE will match untagged frames only.

Tagged: The ECE will match tagged frames only.

Inner VLAN ID Filter : The inner VLAN ID filter for matching the ECE. It only significant if tag type 'Tagged' is selected. The possible values are:

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

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

Range: If you want to filter a specific inner VLAN ID range filter with this ECE, choose this value. A field for entering a range appears.

Inner VLAN ID Value : When "Specific" is selected for the VLAN ID filter, you can enter a specific value. The allowed values are 0 - 4095.

Inner VLAN ID Range : When "Range" is selected for the VLAN ID filter, you can enter a specific range. The allowed range is 0 - 4095.

Inner Tag PCP : The inner PCP value for matching the ECE. It only significant if inner tag type 'Tagged' is selected. The possible values are:

> ***Any***: The ECE will match any PCP value.
>
> ***Range***: The ECE will match PCP values in the selected range 0-1, 2-3, 4-5, 6-7, 0-3 or 4-7.
>
> ***Specific***: The ECE will match a specific PCP in the range 0 - 7.

Inner Tag DEI : The inner DEI value for matching the ECE. It only significant if inner tag type 'Tagged' is selected. The allowed value is: 0, 1 or Any.

Frame Type : The frame type for the ECE. The possible values are:

> ***Any***: The ECE will match any frame type.
>
> ***IPv4***: The ECE will match IPv4 frames only.
>
> ***IPv6***: The ECE will match IPv6 frames only.

SMAC Filter : The source MAC address for matching the ECE. The possible values are:

> ***Any***: No SMAC filter is specified. (SMAC filter status is "don't-care".)
>
> ***Specific***: If you want to filter a specific SMAC value with this ECE, choose this value. A field for entering a specific value appears.

SMAC Value : When "Specific" is selected for the SMAC filter, you can enter a specific value. The legal format is "xx-xx-xx-xx-xx-xx" or "xx.xx.xx.xx.xx.xx" or "xxxxxxxxxxxx" (x is a hexadecimal digit).

DMAC Filter : The destination MAC address for matching the ECE. The possible values are:

> ***Any***: No DMAC filter is specified (DMAC filter status is "don't-care").
>
> ***Unicast***: Frame must be unicast.
>
> ***Multicast***: Frame must be multicast.
>
> ***Broadcast***: Frame must be broadcast.
>
> ***Specific***: If you want to filter a specific DMAC value with this ECE, choose this value. A field for entering a specific value appears.

DMAC Value : When "Specific" is selected for the DMAC filter, you can enter a specific value. The legal format is "xx-xx-xx-xx-xx-xx" or "xx.xx.xx.xx.xx.xx" or "xxxxxxxxxxxx" (x is a hexadecimal digit).

Protocol Filter : The IP protocol for matching the ECE. The possible values are:

> ***Any***: No protocol filter is specified (Protocol filter status is "don't-care").
>
> ***UDP***: Specify the UDP for matching the ECE.
>
> ***TCP***: Specify the TCP for matching the ECE.
>
> ***Specific***: If you want to filter a specific protocol value with this ECE, choose this value. A field for entering a specific value appears.

Protocol Value : When "Specific" is selected for the protocol filter, you can enter a specific value.
The allowed value is 0 255.

SIP Filter : The source IP address for matching the ECE. The possible values are:

> ***Any***: No SIP filter is specified. (SIP filter status is "don't-care".)
>
> ***Host***: When "IPv4" is selected for the Frame Type, if you want to filter a specific host address with this ECE, choose this value. A field for entering a host address appears.
>
> ***Network***: When "IPv4" is selected for the Frame Type, if you want to filter a specific network address with this ECE, choose this value. Two fields for entering a specific network address and network mask appears.
>
> ***Specific***: When "IPv6" is selected for the Frame Type, if you want to filter a specific network address with this ECE, choose this value. Two fields for entering a specific network address and network mask appears.

SIP Address : When "Host" or "Network" is selected for the SIP filter, you can enter a specific host or network address. When "IPv6" is selected for the Frame Type, the field only supports 32 bits for IPv6 address.

SIP Mask : When "Host" or "Network" is selected for the SIP filter, you can enter a specific network mask. When "IPv6" is selected for the Frame Type, the field only supports 32 bits for IPv6 address mask.

DIP Filter : The destination IP address for matching the ECE. The possible values are:

> ***Any***: No DIP filter is specified. (DIP filter status is "don't-care".)
>
> ***Host***: When "IPv4" is selected for the Frame Type, if you want to filter a specific host address with this ECE, choose this value. A field for entering a host address appears.
>
> ***Network***: When "IPv4" is selected for the Frame Type, if you want to filter a specific network address with this ECE, choose this value. Two fields for entering a specific network address and network mask appears.
>
> ***Specific***: When "IPv6" is selected for the Frame Type, if you want to filter a specific network address with this ECE, choose this value. Two fields for entering a specific network address and network mask appears.

DIP Address : When "IPv4" is selected for the Frame Type and "Host" or "Network" is selected for the DIP filter, you can enter a specific host or network address. When "IPv6" is selected for the Frame Type, the field only supports 32 bits for IPv6 address.

DIP Mask : When "IPv4" is selected for the Frame Type and "Host" or "Network" is selected for the DIP filter, you can enter a specific network mask. When "IPv6" is selected for the Frame Type, the field only supports 32 bits for IPv6 address mask.

DSCP Filter : The DSCP filter for matching the ECE. The possible values are:

> ***Any***: No DSCP filter is specified. (DSCP filter status is "don't-care".)
>
> ***Specific***: If you want to filter a specific DSCP value with this ECE, choose this value. A field for entering a specific value appears.
>
> ***Range***: If you want to filter a specific DSCP range filter with this ECE, choose this value. A field for entering a range appears.

DSCP Value : When "Specific" is selected for the DSCP filter, you can enter a specific value. The allowed value is 0 - 63.

DSCP Range : When "Range" is selected for the DSCP filter, you can enter a specific range. The allowed range is 0 - 63.

Fragment : The IPv4 Fragment for matching the ECE. This involves the settings for the More Fragments (MF) bit and the Fragment Offset (FRAG OFFSET) field for an IPv4 frame. The possible values are:

Any: The ECE will match any MF bit.

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

Non-Fragment: 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.

Source Port Filter : The TCP/UDP source port for matching the ECE. It only significant if protocol filter 'UDP' or 'TCP' is selected. The possible values are:

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

Specific: If you want to filter a specific TCP/UDP source port No. with this ECE, choose this value. A field for entering a specific No. appears.

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

Source Port No. : When "Specific" is selected for the source port filter, you can enter a specific value. The allowed value is 0 - 65535.

Source Port Range : When "Range" is selected for the source port filter, you can enter a specific range. The allowed range is 0 - 65535.

Destination Port Filter : The TCP/UDP destination port for matching the ECE. It only significant if protocol filter 'UDP' or 'TCP' is selected. The possible values are:

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

Specific: If you want to filter a specific TCP/UDP destination port No. with this ECE, choose this value. A field for entering a specific No. appears.

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

Destination Port No. : When "Specific" is selected for the destination port filter, you can enter a specific value. The allowed value is 0 - 65535.

Destination Port Range : When "Range" is selected for the destination port filter, you can enter a specific range. The allowed range is 0 - 65535.

Actions

Direction : The EVCs and ECEs are used to setup flows in one or both directions as determined by the ECE Direction parameter. If the ECE is bidirectional, the ingress rules of the NNI ports will be setup to match the traffic being forwarded to NNI ports. The possible values are:

Both: Bidirectional.

UNI-to-NNI: Unidirectional from UNI to NNI.

NNI-to-UNI: Unidirectional from NNI to UNI.

Rule Type : The rule type for the ECE. The possible values are:

Both: Ingress and egress rule.

RX: Ingress rule.

TX: Egress rule.

TX Lookup : The TX lookup for the ECE. The possible values are:

VID lookup: The TX lookup is based on VID.

VID-PCP: The TX lookup is based on VID and PCP.

ISDX: The TX lookup is based on ISDX.

EVC ID Filter : The EVC ID for the ECE. The ECE is only active when mapping to an existing EVC. The possible values are:

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

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

EVC ID Value : When "Specific" is selected for the VLAN ID filter, you can enter a specific value. The allowed value is 1 - 1024.

Policer ID Filter : The policer ID filter for matching the ECE. The possible values are:

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

Discard: All received frames are discarded for the ECE.

None: All received frames are forwarded for the ECE.

EVC: The bandwidth profile for the specified EVC ID is used.

Policer ID Value : When "Specific" is selected for the policer ID filter, you can enter a specific value. The value is from 1 - 1022.

Tag Pop Count : The ingress tag pop count for the ECE. The allowed range is 0 - 2.

Policy ID : The ACL Policy ID for the ECE for matching ACL rules. The allowed range is 0 - 63.

Class : The traffic class for the ECE. The allowed range is 0 - 8 or disabled.

Drop Precedence : The drop precedence for the ECE. The allowed range is 0, 1 or disabled.

Egress Outer Tag

Outer Tag Mode : The outer tag for nni-to-uni direction for the ECE. The possible values are:
Enable: Enable outer tag for nni-to-uni direction for the ECE.
Disable: Disable outer tag for nni-to-uni direction for the ECE.

Outer Tag VID : The EVC outer tag VID for UNI ports. The allowed value is 0 - 4095.

Outer Tag PCP Mode : The outer tag PCP mode for the ECE. The possible values are:

Classified: The outer tag PCP Mode is classified.

Fixed: The outer tag PCP Mode is classified.

Mapped: The outer tag PCP Mode is based on mapped (QOS, DP).

Outer Tag PCP : The outer tag PCP value for the ECE. The allowed range is 0 - 7.

Outer Tag DEI Mode : The outer tag DEI mode for the ECE. The possible values are:

Classified: The outer tag DEI mode is classified.

Fixed: The outer tag DEI mode is fixed.

Drop Precedence: The outer tag DEI mode is drop precedence.

Outer Tag DEI : The outer tag DEI value for the ECE. The allowed value is 0 or 1.

Egress Inner Tag

Inner Tag Type : The inner type for the ECE determines whether an inner tag is inserted in frames forwarded to NNI ports. The possible values are:

> ***None***: An inner tag is not inserted.
>
> ***C-tag***: An inner C-tag is inserted.
>
> ***S-tag***: An inner S-tag is inserted.
>
> ***S-custom-tag***: An inner tag is inserted and the tag type is determined by the VLAN port configuration of the NNI.

Inner Tag VLAN ID : The inner tag VLAN ID for the ECE. The allowed range is 0 - 4095.

Inner Tag PCP Mode : The inner tag PCP mode for the ECE. The possible values are:

> ***Classified***: The inner tag PCP Mode is classified.
>
> ***Fixed***: The inner tag PCP Mode is classified.
>
> ***Mapped***: The inner tag PCP Mode is based on mapped (QOS, DP).

Inner Tag PCP : The inner tag PCP value for the ECE. The allowed range is 0 - 7.

Inner Tag DEI Mode : The inner tag DEI mode for the ECE. The possible values are:

> ***Classified***: The inner tag DEI mode is classified.
>
> ***Fixed***: The inner tag DEI mode is fixed.
>
> ***Drop Precedence***: The inner tag DEI mode is drop precedence.

Inner Tag DEI : The inner tag DEI value for the ECE. The allowed value is 0 or 1.

Buttons

Apply - Click to save changes.

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

Cancel - Return to the previous page; any changes made locally will be undone.

Modification Buttons

You can modify each ECE (EVC Control Entry) in the table using the following buttons:

⊕ : Inserts a new ECE before the current row.

ⓔ : Edits the ECE row.

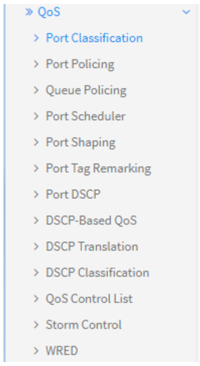
↑ : Moves the ECE up the list.

↓ : Moves the ECE down the list.

⊗ : Deletes the ECE.

⊕ : The lowest plus sign adds a new entry at the bottom of the ECE

2-24 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.

The switch provides flexibility in the classification of incoming frames to a QoS class. QoS classification looks for information up to Layer 4, including IPv4 and IPv6 DSCP, IPv4 TCP/UDP port numbers, and user priority of tagged frames. This QoS classification mechanism is implemented in a QoS control list (QCL). The QoS class assigned to a frame is used throughout the device for providing queuing, scheduling, and congestion control guarantees to the frame according to what was configured for that specific QoS class.

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

2-24.1 Port Classification

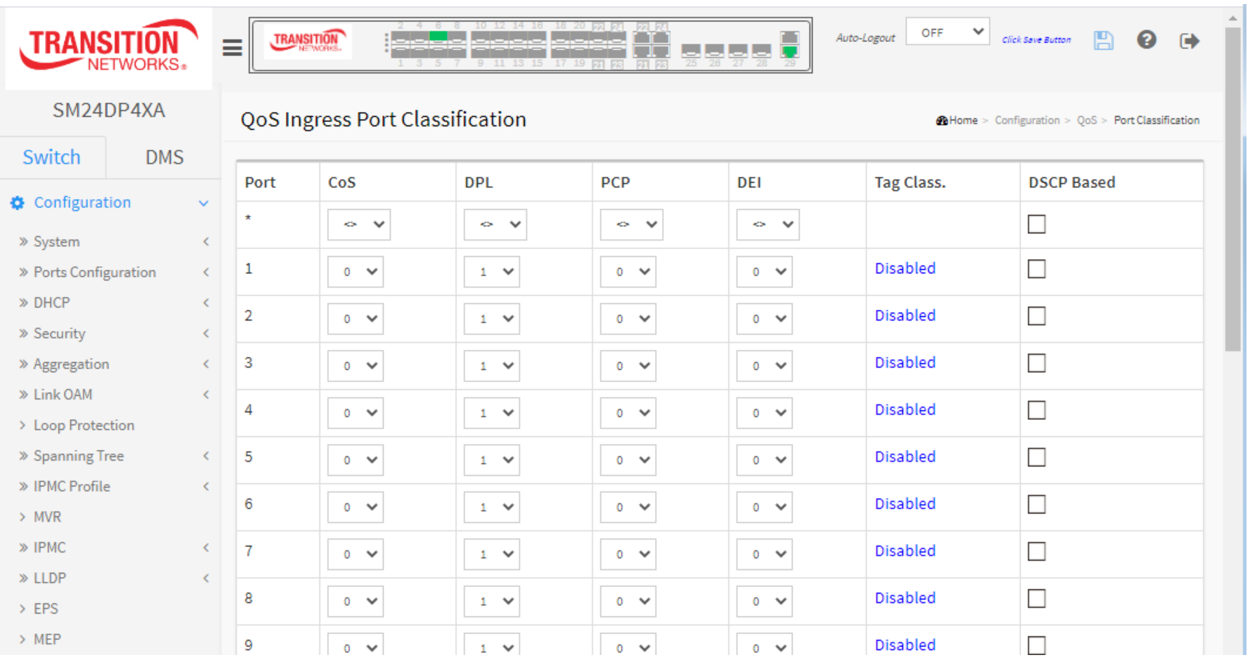
This page lets you configure basic QoS Ingress Classification settings for all switch ports.

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 the Apply button to save the settings. To cancel the settings click the Reset button.

Figure 2-24.1: QoS Ingress Port Classification



QoS Ingress Port Classification

Port	CoS	DPL	PCP	DEI	Tag Class.	DSCP Based
*	<>	<>	<>	<>		□
1	0	1	0	0	Disabled	□
2	0	1	0	0	Disabled	□
3	0	1	0	0	Disabled	□
4	0	1	0	0	Disabled	□
5	0	1	0	0	Disabled	□
6	0	1	0	0	Disabled	□
7	0	1	0	0	Disabled	□
8	0	1	0	0	Disabled	□
9	0	1	0	0	Disabled	□

Parameter descriptions:

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

CoS : Controls the default class of service. All frames are classified to a CoS. There is a one to one mapping between CoS, queue and priority. A CoS of 0 (zero) has the lowest priority. If the port is VLAN aware, the frame is tagged and Tag Class. is enabled, then the frame is classified to a CoS that is mapped from the PCP and DEI value in the tag. Otherwise the frame is classified to the default CoS. The classified CoS can be overruled by a QCL entry. **Note**: If the default CoS has been dynamically changed, then the actual default CoS is shown in parentheses after the configured default CoS.

DPL : Controls the default drop precedence level. All frames are classified to a drop precedence level. If the port is VLAN aware, the frame is tagged and Tag Class. is enabled, then the frame is classified to a DPL that is mapped from the PCP and DEI value in the tag. Otherwise the frame is classified to the default DPL. The classified DPL can be overruled by a QCL entry.

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 CoS and DPL for tagged frames.

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

Click on the mode in order to configure the mode and/or mapping.

Note: This setting has no effect if the port is VLAN unaware. Tagged frames received on VLAN unaware ports are always classified to the default CoS and DPL.

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

Buttons:

Save – Click to save changes.

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

2-24.2 Port Policing

This page lets you view and 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 used for data flows and voice or video flows because voice and video usually maintains a steady rate of traffic.

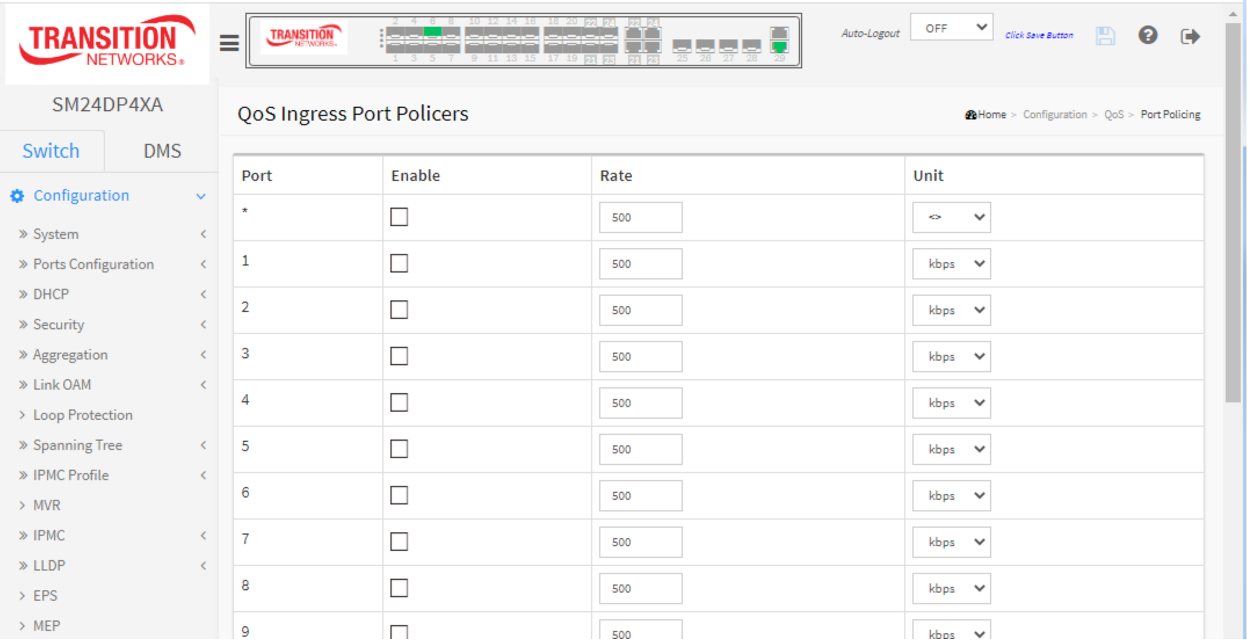
A policer can limit the bandwidth of received frames. It is located in front of the ingress queue.

Web Interface

To display the QoS Port Schedulers in the web interface:

1. Click Configuration, QoS, Port Policing.
2. Enable the port(s) you want as QoS Ingress Port Policers and type the Rate limit condition.
3. Select the Rate limit Unit of measure.
4. Click the Apply button to save the settings.

Figure 2-24.2: QoS Ingress Port Policers Configuration



QoS Ingress Port Policers

Port	Enable	Rate	Unit
*	☐	500	<>
1	☐	500	kbps
2	☐	500	kbps
3	☐	500	kbps
4	☐	500	kbps
5	☐	500	kbps
6	☐	500	kbps
7	☐	500	kbps
8	☐	500	kbps
9	☐	500	kbps

Parameter descriptions:

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

Enable : To enable the Port(s) you want to enable the QoS Ingress Port Policers function.

Rate : Controls the rate for the port policer. This value is restricted to 100-13128072 when "Unit" is kbps, 1-13128 when "Unit" is mbps, 1-131071 when "Unit" is fps, and 1-131 when "Unit" is kfps. The rate is internally rounded up to the nearest value supported by the port policer.

Unit : Select the unit of measure for the rate (kbps, Mbps, fps or kfps).

Buttons:

Save – Click to save changes.

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

2-24.3 Queue Policing

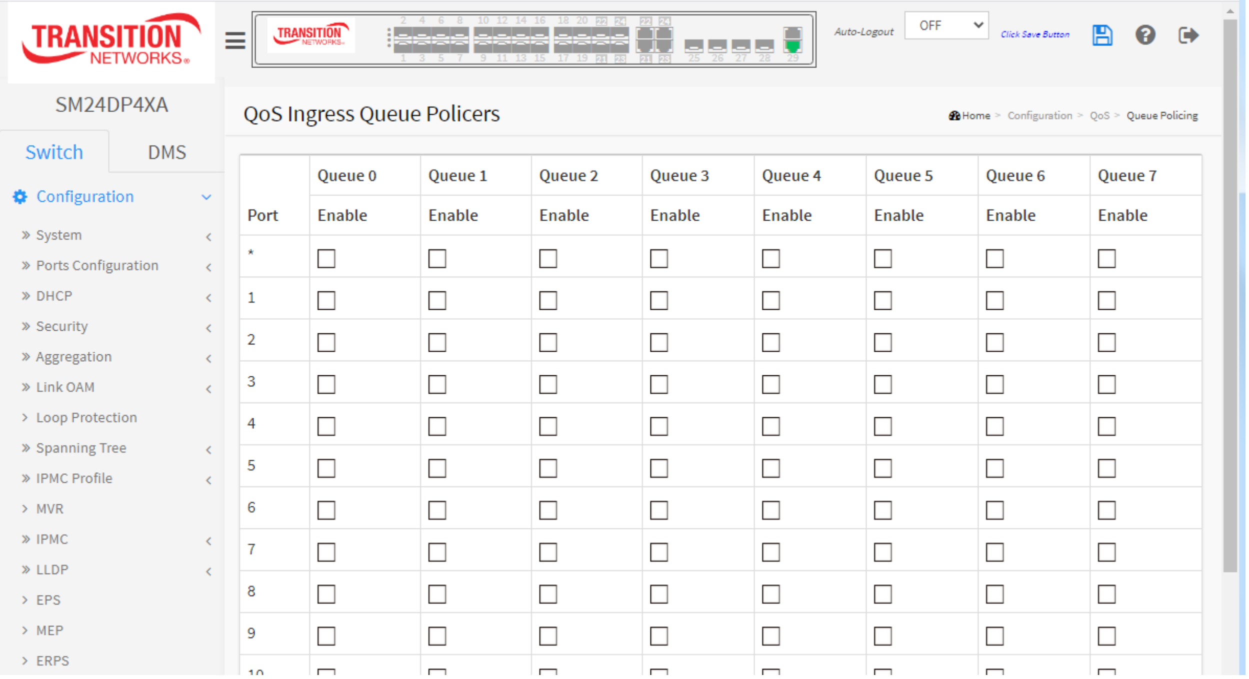
This section provides an overview of f QoS Ingress Port Policers for all switch ports The Port Policing is useful in constraining traffic flows and marking frames above specific rates. Policing is primarily useful for data flows and voice or video flows because voice and video usually maintains a steady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

Web Interface

To display the QoS Port Schedulers in the web interface:

1. Click Configuration, QoS, Queue Policing.
2. Enable the QoS Ingress Queue Policers and enter the Rate limit condition.
3. Click Apply to save the configuration.

Figure 2-24.3: QoS Ingress Queue Policers



QoS Ingress Queue Policers

	Queue 0	Queue 1	Queue 2	Queue 3	Queue 4	Queue 5	Queue 6	Queue 7
Port	Enable	Enable	Enable	Enable	Enable	Enable	Enable	Enable
*	□	□	□	□	□	□	□	□
1	□	□	□	□	□	□	□	□
2	□	□	□	□	□	□	□	□
3	□	□	□	□	□	□	□	□
4	□	□	□	□	□	□	□	□
5	□	□	□	□	□	□	□	□
6	□	□	□	□	□	□	□	□
7	□	□	□	□	□	□	□	□
8	□	□	□	□	□	□	□	□
9	□	□	□	□	□	□	□	□
10	□	□	□	□	□	□	□	□

Parameter descriptions:

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

Enabled : Checkboxes to control whether the queue policer is enabled on this switch port.

Buttons:

Save – Click to save changes.

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

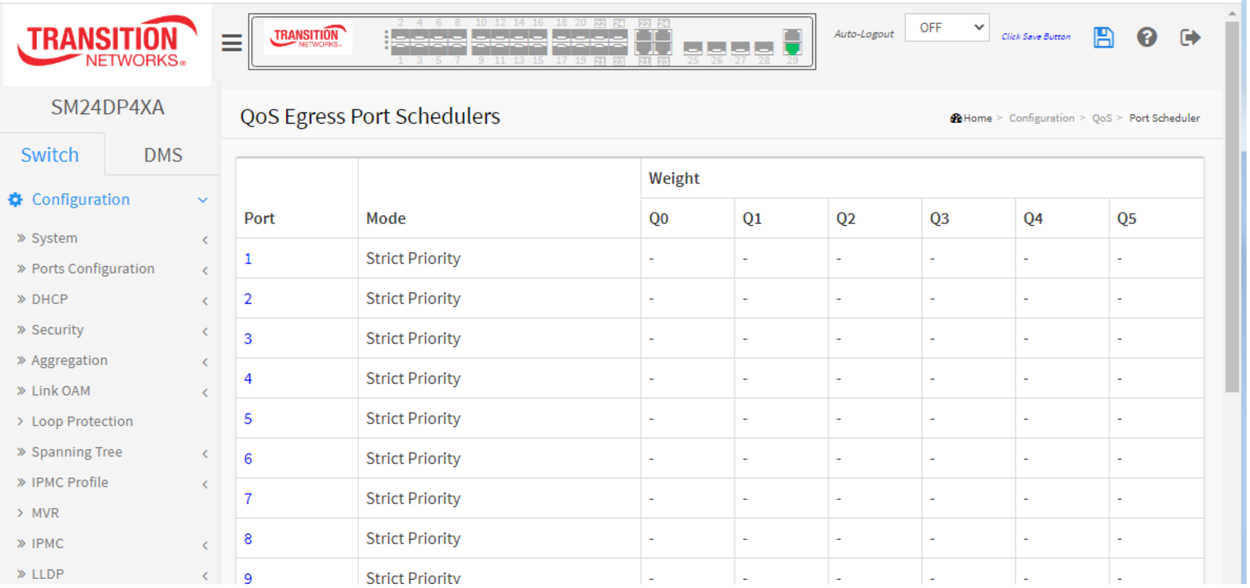
2-24.4 Port Schedulers

This page lets you view and configure QoS Egress Port Schedulers for all switch ports.

Web Interface

To display the QoS Port Schedulers in the web interface:

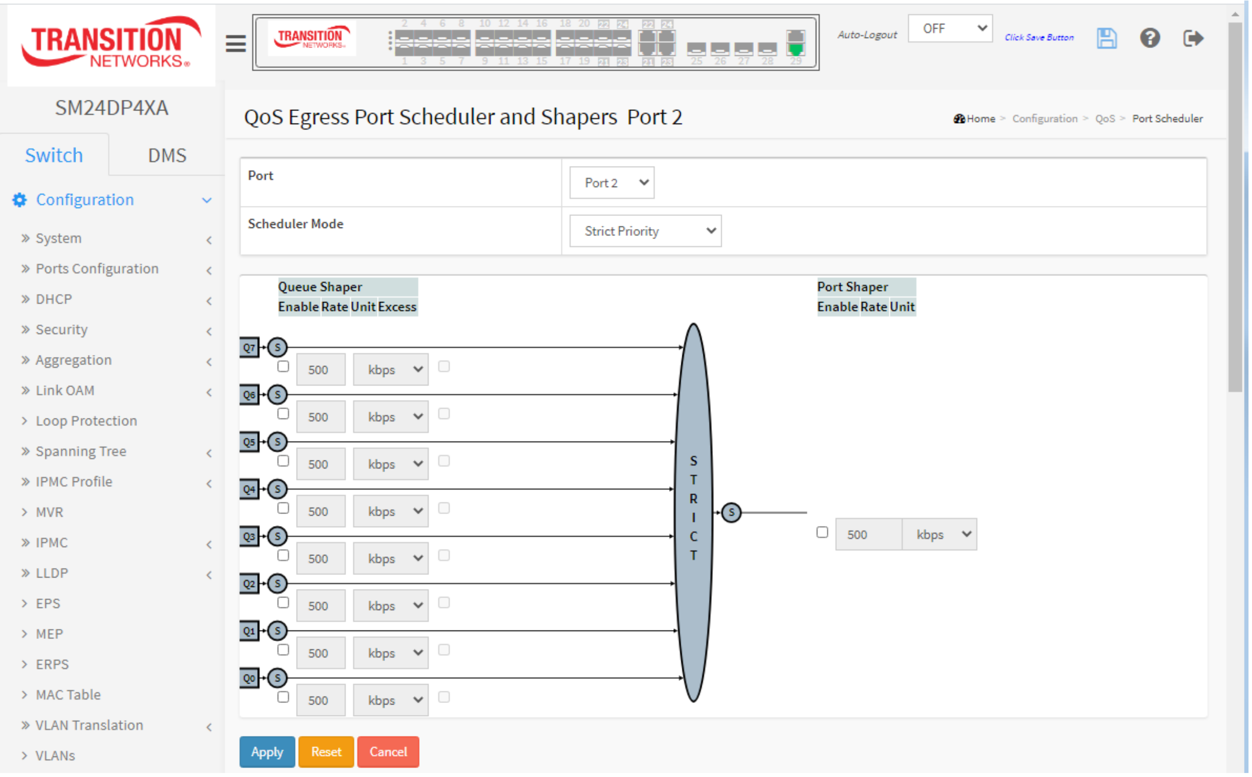
1. Click Configuration, QoS, Port Schedulers to display the QoS Egress Port Schedulers page:



QoS Egress Port Schedulers

Port	Mode	Weight					
		Q0	Q1	Q2	Q3	Q4	Q5
1	Strict Priority	-	-	-	-	-	-
2	Strict Priority	-	-	-	-	-	-
3	Strict Priority	-	-	-	-	-	-
4	Strict Priority	-	-	-	-	-	-
5	Strict Priority	-	-	-	-	-	-
6	Strict Priority	-	-	-	-	-	-
7	Strict Priority	-	-	-	-	-	-
8	Strict Priority	-	-	-	-	-	-
9	Strict Priority	-	-	-	-	-	-

2. Click a linked port number in the Port column to display its QoS Egress Port Scheduler and Shapers page:



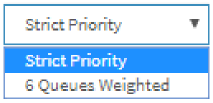
QoS Egress Port Scheduler and Shapers Port 2

Port	Port 2
Scheduler Mode	Strict Priority

Queue	Queue Shaper Enable	Rate	Unit	Excess
Q7	□	500	kbps	□
Q6	□	500	kbps	□
Q5	□	500	kbps	□
Q4	□	500	kbps	□
Q3	□	500	kbps	□
Q2	□	500	kbps	□
Q1	□	500	kbps	□
Q0	□	500	kbps	□

Port Shaper Enable	Rate	Unit
□	500	kbps

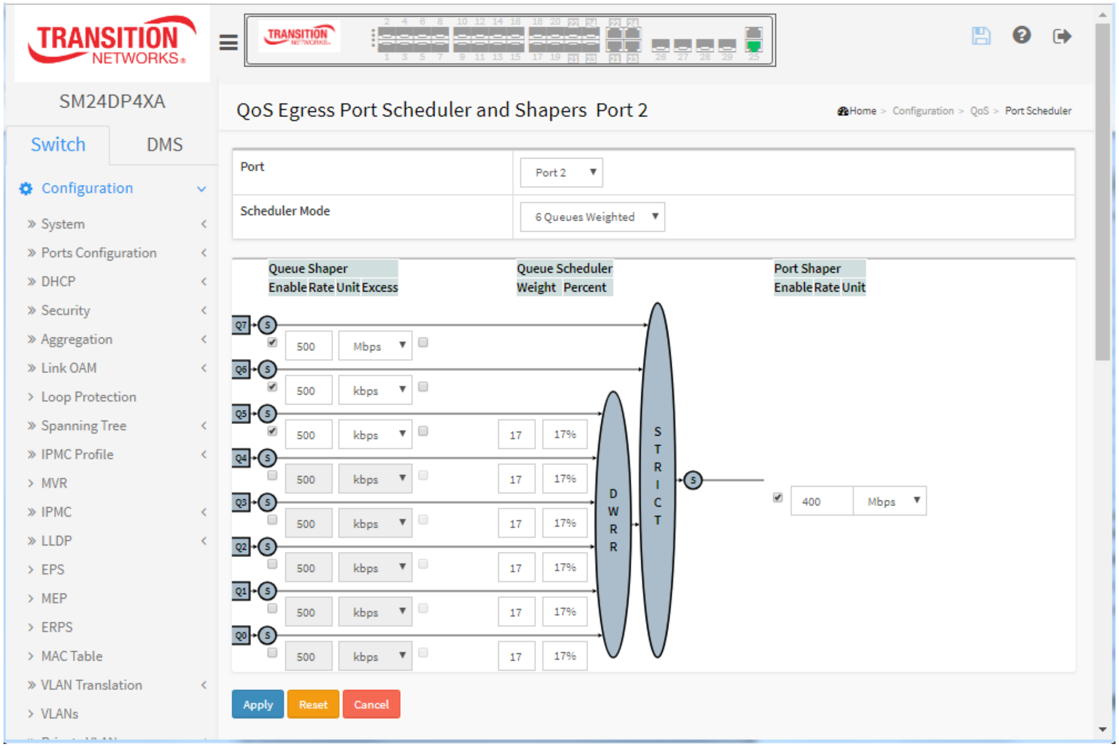
3. Select a different port if desired, and at the Schedule Mode dropdown select Strict Priority (default) or 6 Queues Weighted.



4. In the Queue Shaper column set Enable, Rate, Unit, and Excess.

5. In the Port Shaper column set Enable, Rate, Unit, and Excess.

6. If you selected 6 Queues Weighted in step 4, in the Queue Scheduler column set Weight and Percent as shown below.



QoS Egress Port Scheduler and Shapers Port 2

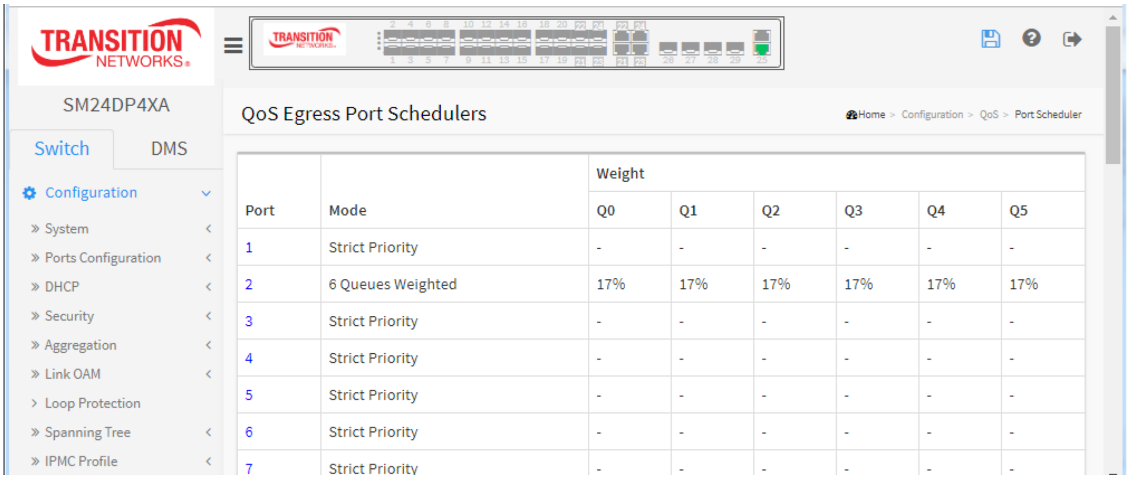
Port: Port 2

Scheduler Mode: 6 Queues Weighted

	Queue Shaper Enable	Rate	Unit	Excess	Queue Scheduler Weight	Percent
Q7	☑	500	Mbps	□		
Q6	☑	500	kbps	□		
Q5	☑	500	kbps	□	17	17%
Q4	□	500	kbps	□	17	17%
Q3	□	500	kbps	□	17	17%
Q2	□	500	kbps	□	17	17%
Q1	□	500	kbps	□	17	17%
Q0	□	500	kbps	□	17	17%

Port Shaper Enable Rate Unit: ☑ 400 Mbps

7. Click the Apply button to save the settings. The QoS Egress Port Schedulers page displays again with the changed settings:



QoS Egress Port Schedulers

		Weight					
Port	Mode	Q0	Q1	Q2	Q3	Q4	Q5
1	Strict Priority	-	-	-	-	-	-
2	6 Queues Weighted	17%	17%	17%	17%	17%	17%
3	Strict Priority	-	-	-	-	-	-
4	Strict Priority	-	-	-	-	-	-
5	Strict Priority	-	-	-	-	-	-
6	Strict Priority	-	-	-	-	-	-
7	Strict Priority	-	-	-	-	-	-

Parameter descriptions:

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

Mode : Shows the scheduling mode for this port (Strict Priority or 6 Queues Weighted).

Weight (Qn) : Shows the weight for this queue and port.

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

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

Queue Shaper Rate : Controls the rate for the queue shaper. This value is restricted to 100-13128072 when "Unit" is kbps, and 1-13128 when "Unit" is Mbps. The rate is internally rounded up to the nearest value supported by the queue shaper.

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 cancel the settings.

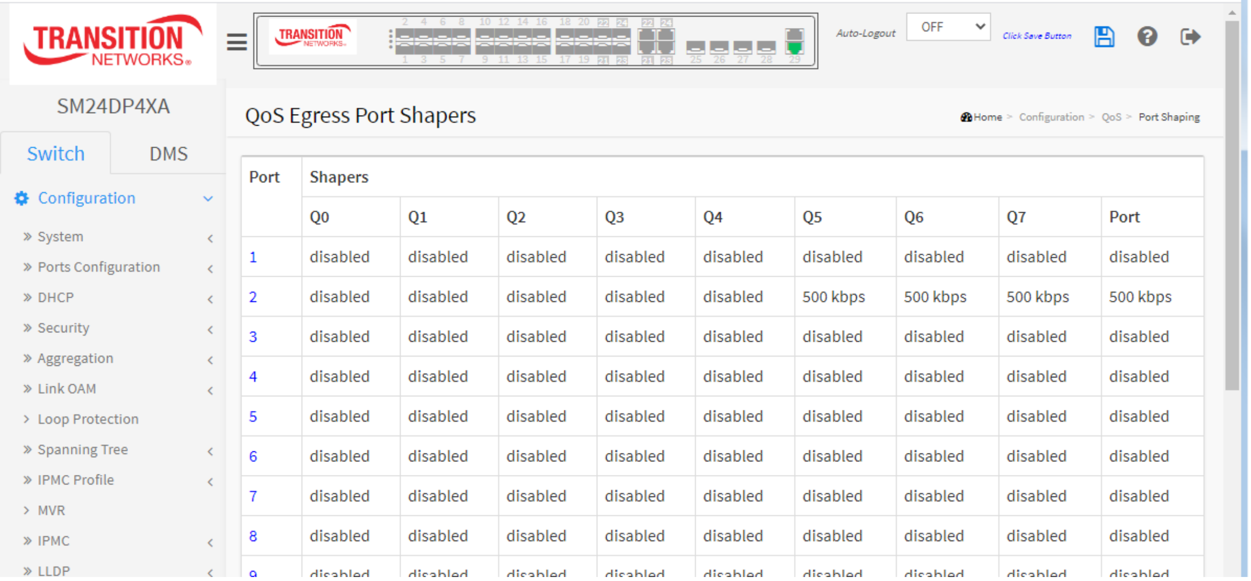
2-24.5 Port Shaping

This section provides an overview of QoS Egress Port Shapers for all switch ports.

Web Interface

To display the QoS Port Shapers in the web interface:

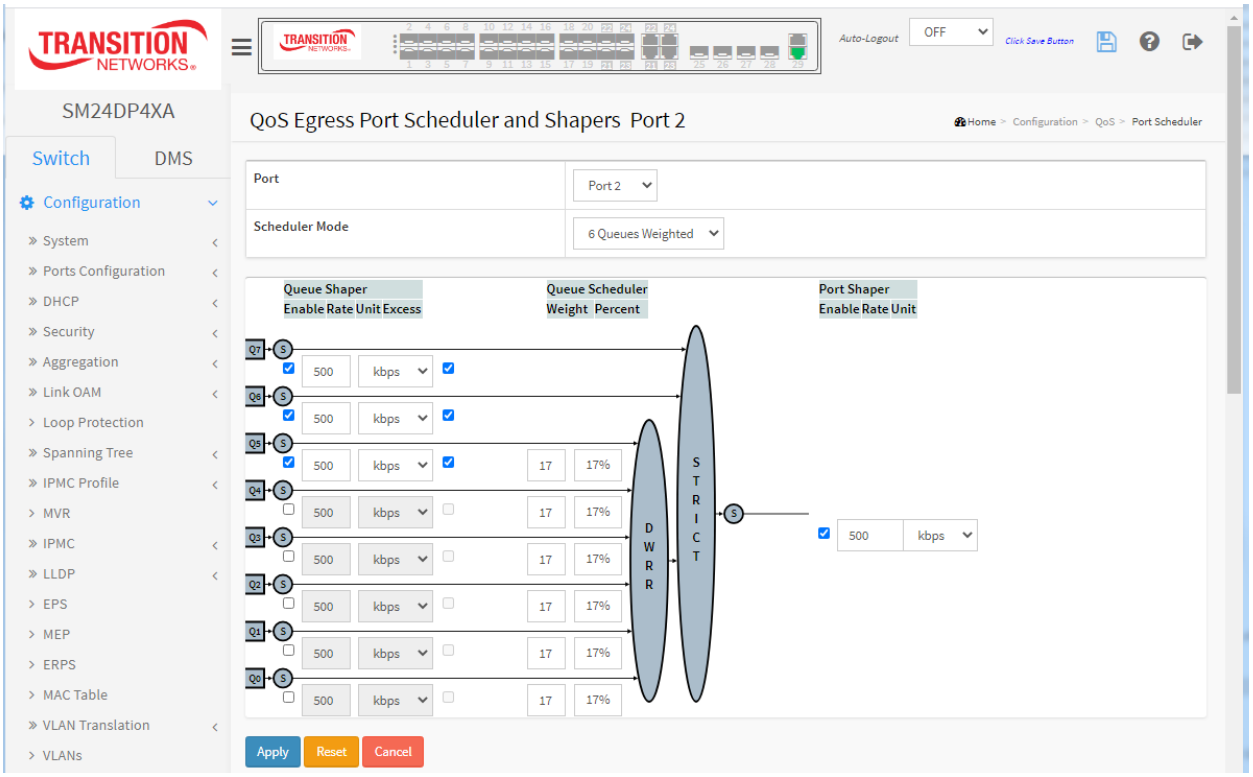
1. Click Configuration, QoS, Port Shaping to display the **QoS Egress Port Shapers page:**



QoS Egress Port Shapers

Port	Shapers								
	Q0	Q1	Q2	Q3	Q4	Q5	Q6	Q7	Port
1	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled
2	disabled	disabled	disabled	disabled	disabled	500 kbps	500 kbps	500 kbps	500 kbps
3	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled
4	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled
5	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled
6	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled
7	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled
8	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled
9	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled

2. Click a linked port number to display its QoS Egress Port Scheduler and Shapers page.



QoS Egress Port Scheduler and Shapers Port 2

Port	Port 2
Scheduler Mode	6 Queues Weighted

	Queue Shaper Enable	Rate	Unit	Excess	Queue Scheduler Weight	Percent
Q7	☑	500	kbps	☑		
Q6	☑	500	kbps	☑		
Q5	☑	500	kbps	☑	17	17%
Q4	□	500	kbps	□	17	17%
Q3	□	500	kbps	□	17	17%
Q2	□	500	kbps	□	17	17%
Q1	□	500	kbps	□	17	17%
Q0	□	500	kbps	□	17	17%

Port Shaper Enable	Rate	Unit
☑	500	kbps

3. Continue configuring the page parameters as described in the previous section.

Parameter descriptions:

Scheduler Mode : Controls how many of the queues are scheduled as strict and how many are scheduled as 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. This value is restricted to 100-13128072 when "Unit" is kbps, and 1-13128 when "Unit" is Mbps. The rate is internally rounded up to the nearest value supported by the queue shaper.

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

Queue Shaper Excess : Controls whether the queue is allowed to use excess bandwidth.

Queue Scheduler Weight : Controls the weight for this queue. 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. This value is restricted to 100-13128072 when "Unit" is kbps, and 1-13128 when "Unit" is Mbps. The rate is internally rounded up to the nearest value supported by the port shaper.

Port Shaper Unit : Controls the unit of measure for the port shaper rate as kbps or Mbps.

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.

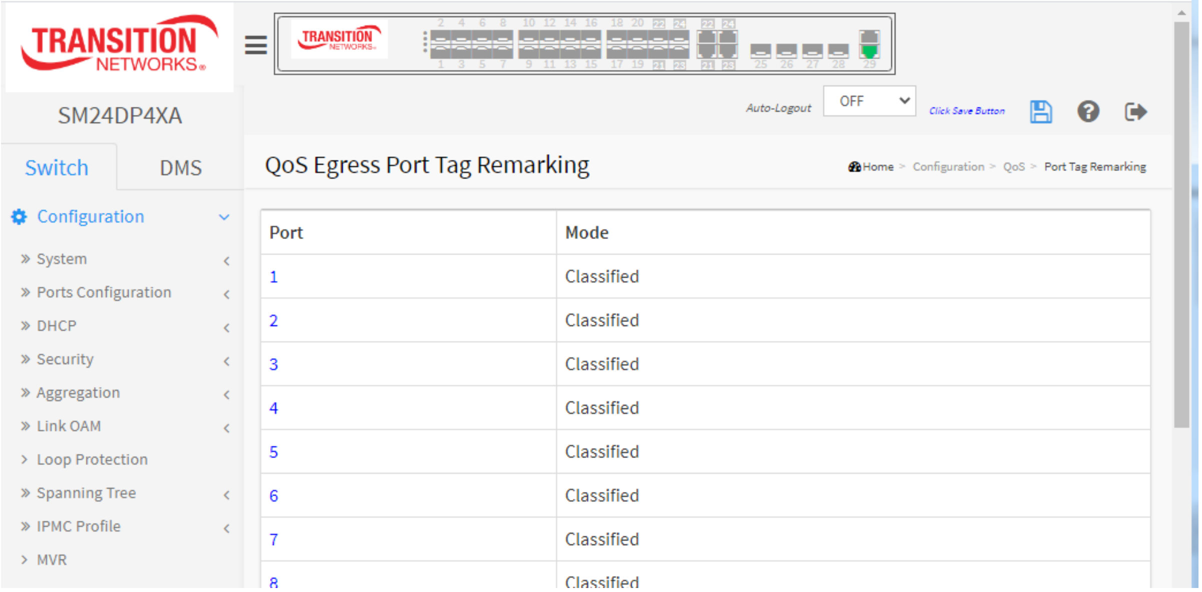
2-24.6 Port Tag Remarking

This page provides an overview of QoS Egress Port Tag Remarking for all switch ports.

Web Interface

To display the QoS Port Tag Remarking in the web interface:

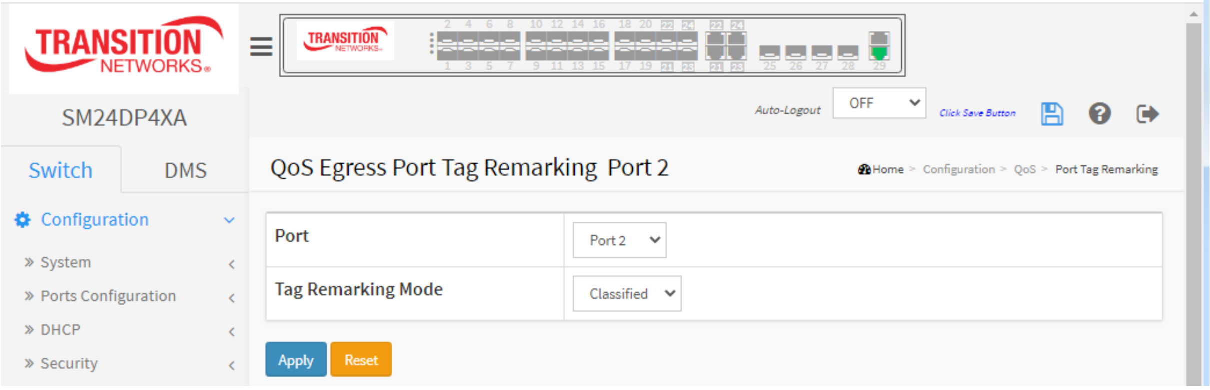
1. Click Configuration, QoS, Port Tag Remarking to display the QoS Egress Port Tag Remarking page:



QoS Egress Port Tag Remarking

Port	Mode
1	Classified
2	Classified
3	Classified
4	Classified
5	Classified
6	Classified
7	Classified
8	Classified

2. Click a linked port number to display its QoS Egress Port Tag Remarking page:



QoS Egress Port Tag Remarking Port 2

Port	Port 2
Tag Remarking Mode	Classified

3. Set the page parameters as described below.

Parameter descriptions:

Port : The logical port for the settings contained in the same row. Click on the port number to configure tag remarking for the desired ports.

Mode : Shows 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.

Tag Remarking Mode : Select 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.

Buttons:

Apply – Click to save changes.

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

2-24.7 Port DSCP

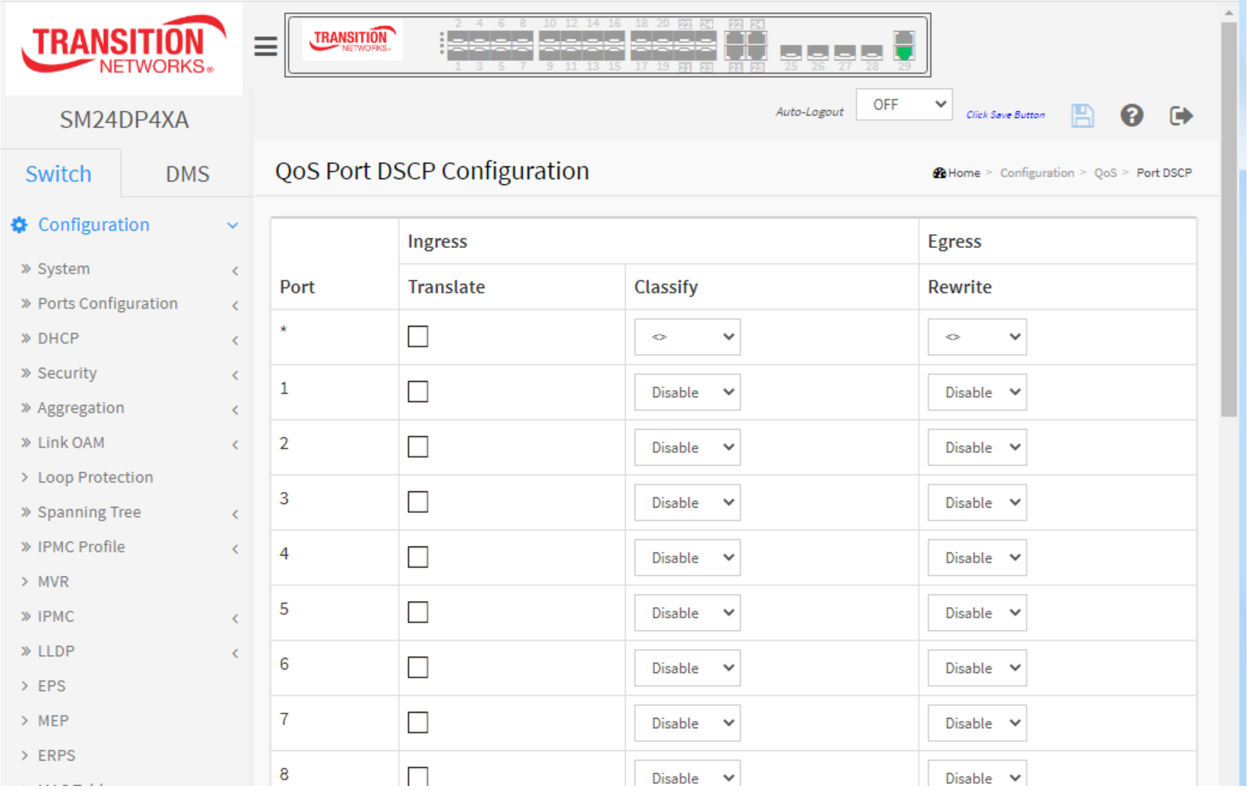
This page lets you set the QoS Port DSCP configuration that was allowed when you configured the basic QoS Port DSCP Configuration settings for all switch ports.

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 set the Classify Parameter parameters.
3. Select Egress Rewrite parameters.
4. Click the Apply button to save the settings.
5. To cancel the settings click the Reset button to revert to previously saved values.

Figure 2-24.7: QoS Port DSCP Configuration



QoS Port DSCP Configuration

	Ingress		Egress
Port	Translate	Classify	Rewrite
*	□	<>	<>
1	□	Disable	Disable
2	□	Disable	Disable
3	□	Disable	Disable
4	□	Disable	Disable
5	□	Disable	Disable
6	□	Disable	Disable
7	□	Disable	Disable
8	□	Disable	Disable

Parameter descriptions:

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

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

Translate **:** To enable Ingress Translation click the checkbox.

Classify: Classification for a port can have one of these 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.

2-24.8 DSCP-Based QoS

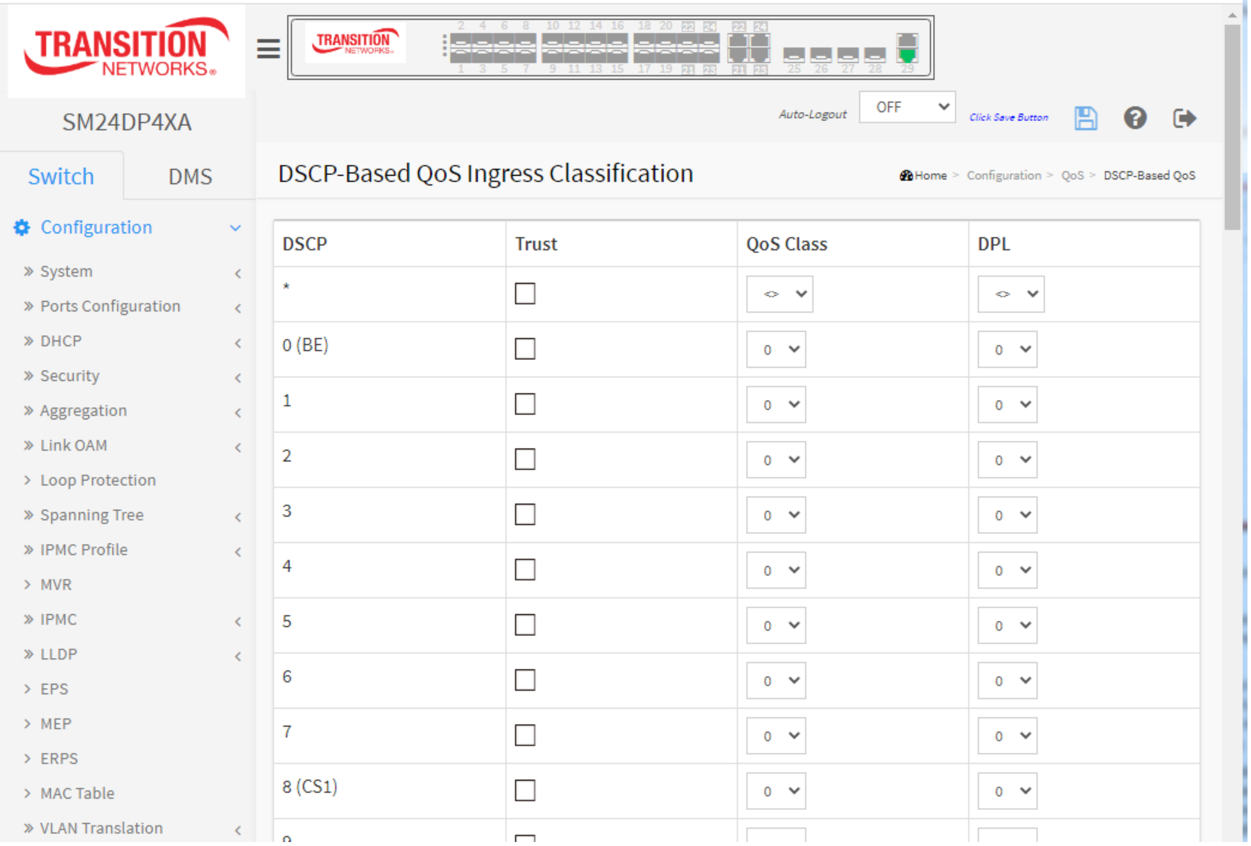
This page lets you configure the DSCP-Based QoS mode and basic QoS DSCP based QoS Ingress Classification settings for the switch.

Web Interface

To configure the DSCP-Based QoS Ingress Classification parameters via the web interface:

1. Click Configuration, QoS, DSCP-Based QoS.
2. Enable or disable the DSCP for Trust.
3. Select QoS Class and DPL 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 2-24.8: DSCP-Based QoS Ingress Classification



DSCP-Based QoS Ingress Classification

DSCP	Trust	QoS Class	DPL
*	□	<>	<>
0 (BE)	□	0	0
1	□	0	0
2	□	0	0
3	□	0	0
4	□	0	0
5	□	0	0
6	□	0	0
7	□	0	0
8 (CS1)	□	0	0

Parameter descriptions:

DSCP : Maximum number of supported DSCP values are 64. DSCP (Differentiated Services Code Point) is a field in the header of IP packets that is used for packet classification purposes.

Trust : Check if the DSCP value is to be trusted. Controls whether a specific DSCP value is trusted. Only frames with trusted DSCP values are mapped to a specific QoS class and Drop Precedence Level. Frames with untrusted DSCP values are treated as non-IP frames.

QoS Class : QoS Class value can be any of (0-7). Every incoming frame is classified to a QoS class, which 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. There is a one to one mapping between QoS class, queue and priority. A QoS class of 0 (zero) has the lowest priority.

DPL : Drop Precedence Level (0-3). Every incoming frame is classified to a Drop Precedence Level (DP level), which is used throughout the device for providing congestion control guarantees to the frame according to what was configured for that specific DP level. A DP level of 0 (zero) corresponds to 'Committed' (Green) frames and a DP level of 1 or higher corresponds to 'Discard Eligible' (Yellow) frames.

Buttons:

Apply – Click to save changes.

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

2-24.9 DSCP Translation

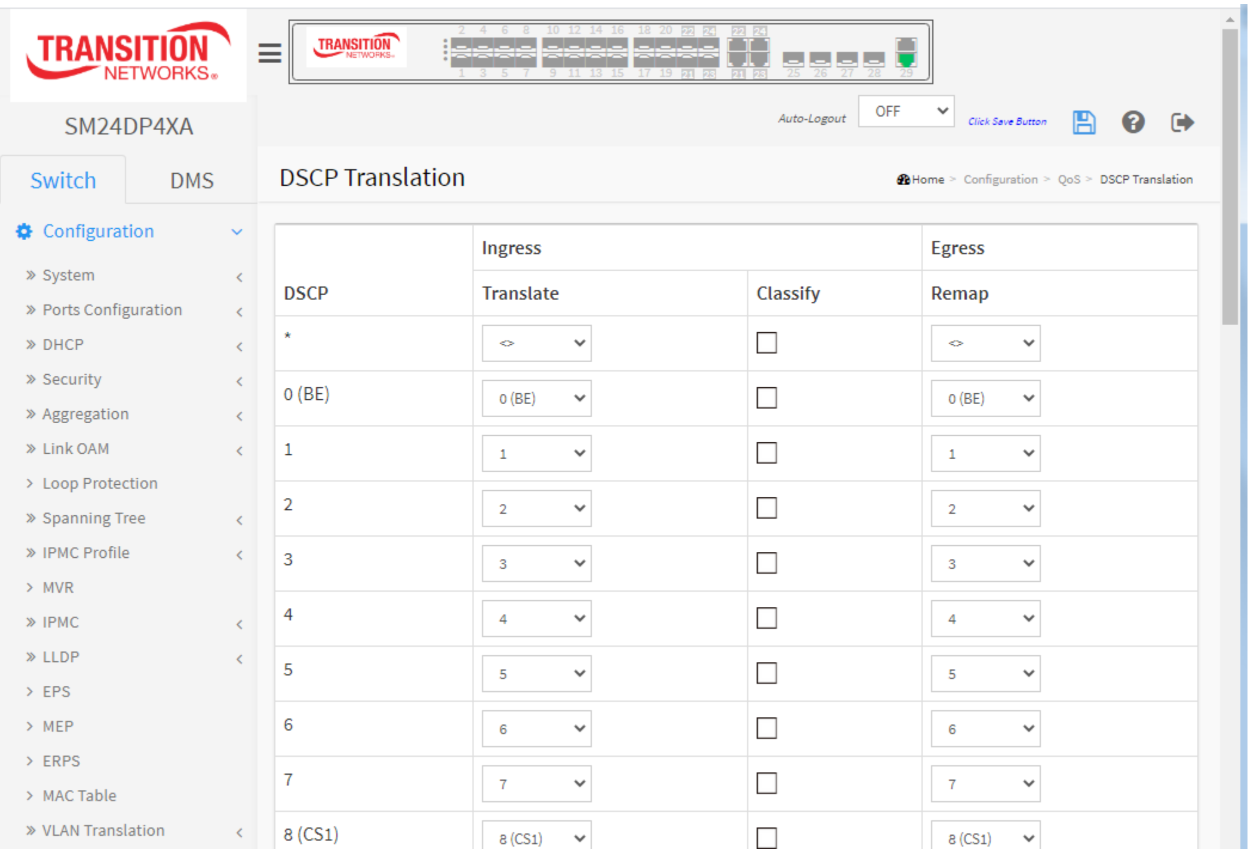
This page lets you configure the basic QoS DSCP Translation settings for the switch. DSCP translation can be done in Ingress or Egress.

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 the Apply button to save the settings.
5. To cancel the settings click the Reset button. It will revert to previously saved values.

Figure 2-24.9: DSCP Translation



DSCP Translation

	Ingress		Egress
DSCP	Translate	Classify	Remap
*	<>	□	<>
0 (BE)	0 (BE)	□	0 (BE)
1	1	□	1
2	2	□	2
3	3	□	3
4	4	□	4
5	5	□	5
6	6	□	6
7	7	□	7
8 (CS1)	8 (CS1)	□	8 (CS1)

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.

2-24.10 DSCP Classification

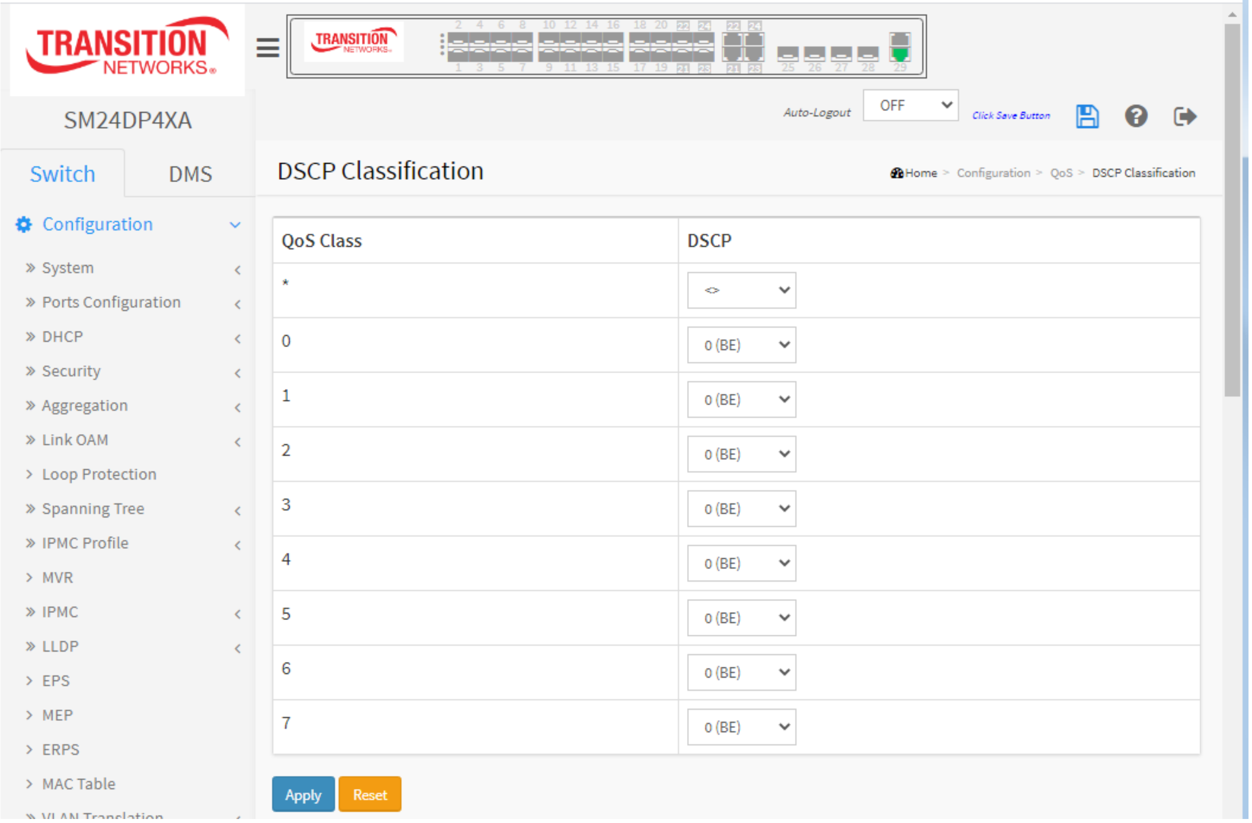
This page lets you configure the mapping of QoS class and Drop Precedence Level to DSCP value.

Web Interface

To configure the DSCP Classification parameters in the web interface:

1. Click Configuration, QoS, DSCP Translation.
2. Select the DSCP parameters.
3. Click the Apply button to save the settings.
4. To cancel the settings click the Reset button. It will revert to previously saved values.

Figure 2-24.10: DSCP Classification Configuration



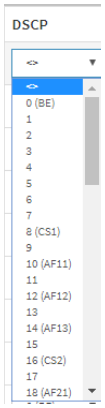
DSCP Classification

QoS Class	DSCP
*	<>
0	0 (BE)
1	0 (BE)
2	0 (BE)
3	0 (BE)
4	0 (BE)
5	0 (BE)
6	0 (BE)
7	0 (BE)

Parameter descriptions:

QoS Class : Actual QoS Class value ranges from 0 to 7.

DSCP : Select the classified DSCP value (0-63).



Buttons:

Save – Click to save changes.

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

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

Refresh: Click to immediately refresh the page manually.

2-24.11 QoS Control List Configuration

This page lets you configure the QoS Control List (QCL), which is made up of the QCEs. Each row describes a QCE that is defined. The maximum number of QCEs is 256 per switch. Click on the lowest plus sign to add a new QCE to the list.

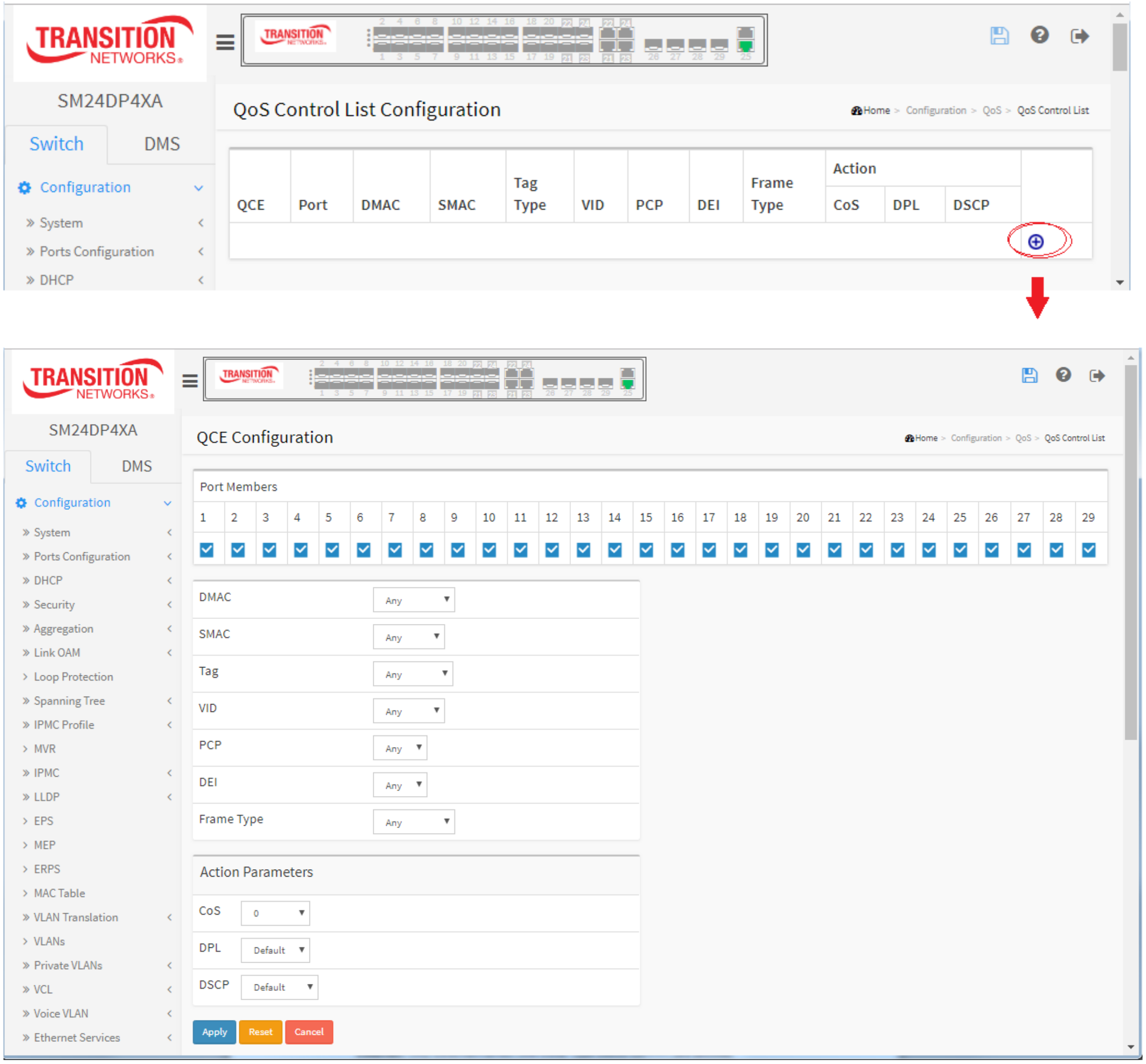
This page lets you edit/insert a single QoS Control Entry at a time. A QCE consists of several parameters. These parameters vary according to the Frame Type that you select.

Web Interface

To configure the QoS Control List parameters in the web interface:

1. Click Configuration, QoS, QoS Control List.
2. Click the ⊕ icon to add a new QoS Control List.
3. Set all parameters and enable the Port Member to join the QCE rules.
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 2-24.11: QoS Control List Configuration



QoS Control List Configuration

QCE	Port	DMAC	SMAC	Tag Type	VID	PCP	DEI	Frame Type	Action		
									CoS	DPL	DSCP
											⊕

QCE Configuration

Port Members

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29
☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑

DMAC	Any
SMAC	Any
Tag	Any
VID	Any
PCP	Any
DEI	Any
Frame Type	Any

Action Parameters

CoS	0
DPL	Default
DSCP	Default

Parameter descriptions:

QCE : Indicates the QCE id.

Port : Indicates the list of ports configured with the QCE or 'Any'.

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

Any: Match any DMAC. The default value is 'Any'.

Unicast: Match unicast DMAC.

Multicast: Match multicast DMAC.

Broadcast: Match broadcast DMAC.

SMAC : Match OUI field of source MAC address, i.e. first three octets (bytes) of MAC address or 'Any'.

Tag Type : Indicates tag type. Possible values are:

Any: Match tagged and untagged frames. The default value is 'Any'.

Untagged: Match untagged frames.

Tagged: Match tagged frames.

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. Possible values are:

Any: Match any frame type.

Ethernet: Match EtherType frames.

LLC: Match (LLC) frames.

SNAP: Match (SNAP) frames.

IPv4: Match IPv4 frames.

IPv6: Match IPv6 frames.

Action : Indicates the classification action taken on ingress frame if parameters configured are matched with the frame's content. Possible actions are:

CoS: Classify Class of Service.

DPL: Classify Drop Precedence Level.

DSCP: Classify DSCP value.

Modification Buttons :

You can modify each QCE (QoS Control Entry) in the table using the following buttons:

⊕: Add: 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 what to make any port member of the QCL entry. By default all ports will be checked

Key Parameters : Key configuration are described below:

DMAC Destination MAC address: Possible values are 'Unicast', 'Multicast', 'Broadcast' or 'Any'.

SMAC Source MAC address: xx-xx-xx (24 MS bits OUI) or 'Any'.

Tag Value of Tag field can be 'Untagged', 'Tagged', 'C-Tagged', 'S-Tagged' or 'Any'.

VID Valid value of VLAN ID can be any value in the range 1-4095 or 'Any'; user can enter either a specific value or a range of VIDs.

PCP Valid value PCP are specific (0, 1, 2, 3, 4, 5, 6, 7) or range (0-1, 2-3, 4-5, 6-7, 0-3, 4-7) or 'Any'.

DEI Valid value of DEI can be '0', '1' or 'Any'.

Frame Type Frame Type can have any of these values: 1. Any, 2. EtherType, 3. LLC, 4. SNAP, 5. IPv4, or 6. IPv6. These Frame Types are described below.

Any : Allow all types of frames.

EtherType : Valid Ether Type can be 0x600-0xFFFF excluding 0x800(IPv4) and 0x86DD(IPv6) or 'Any'.

LLC : Can be:

DSAP Address Valid DSAP(Destination Service Access Point) can vary from 0x00 to 0xFF or 'Any'.

SSAP Address Valid SSAP(Source Service Access Point) can vary from 0x00 to 0xFF or 'Any'.

Control Valid Control field can vary from 0x00 to 0xFF or 'Any'.

SNAP : **PID** Valid PID (a.k.a Ether Type) can be 0x0000-0xFFFF or 'Any'.

IPv4 : Select:

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.

IP Fragment : IPv4 frame fragmented option: 'Yes', 'No' or 'Any'.

DSCP : Diffserv Code Point value (DSCP): It can be a specific value, range of values or 'Any'. DSCP values are in the range 0-63 including BE, CS1-CS7, EF or AF11-AF43.
Sport : Source TCP/UDP port:(0-65535) or 'Any', specific or port range 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 : Select:

Protocol : IP protocol number: (0-255, 'TCP' or 'UDP') or 'Any'.

Source IP : 32 LS bits of IPv6 source address in value/mask format or 'Any'.

DSCP : Diffserv Code Point value (DSCP): It can be a specific value, range of values or 'Any'. DSCP values are in the range 0-63 including BE, CS1-CS7, EF or AF11-AF43.

Sport : Source TCP/UDP port :(0-65535) or 'Any', specific or port range applicable for IP protocol UDP/TCP.

Dport : Destination TCP/UDP port :(0-65535) or 'Any', specific or port range applicable for IP protocol UDP/TCP.

Action Parameters

CoS : Class of Service: (0-7) or 'Default'.

DP : Drop Precedence Level: (0-3) or 'Default'.

DSCP : (0-63, BE, CS1-CS7, EF or AF11-AF43) or 'Default'.

Default : means that the default classified value is not modified by this QCE.

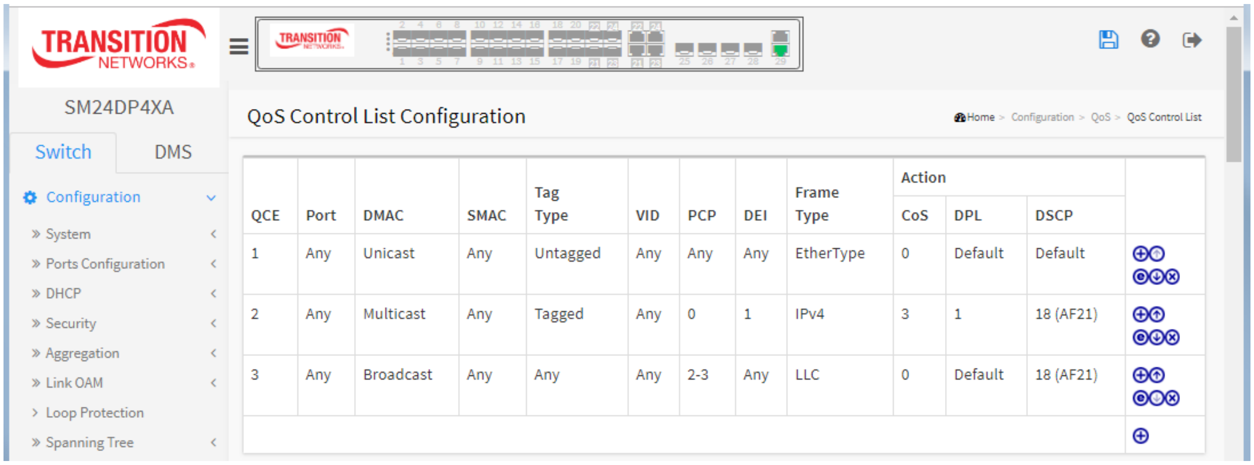
Buttons

Apply : Click to save the configuration and move to main QCL page.

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

Cancel : Return to the previous page without saving the configuration change.

Example



QoS Control List Configuration

QCE	Port	DMAC	SMAC	Tag Type	VID	PCP	DEI	Frame Type	Action			
									CoS	DPL	DSCP	
1	Any	Unicast	Any	Untagged	Any	Any	Any	EtherType	0	Default	Default	⊕⊕ ⊕⊕⊗
2	Any	Multicast	Any	Tagged	Any	0	1	IPv4	3	1	18 (AF21)	⊕⊕ ⊕⊕⊗
3	Any	Broadcast	Any	Any	Any	2-3	Any	LLC	0	Default	18 (AF21)	⊕⊕ ⊕⊕⊗
												⊕

2-24.12 Storm Control

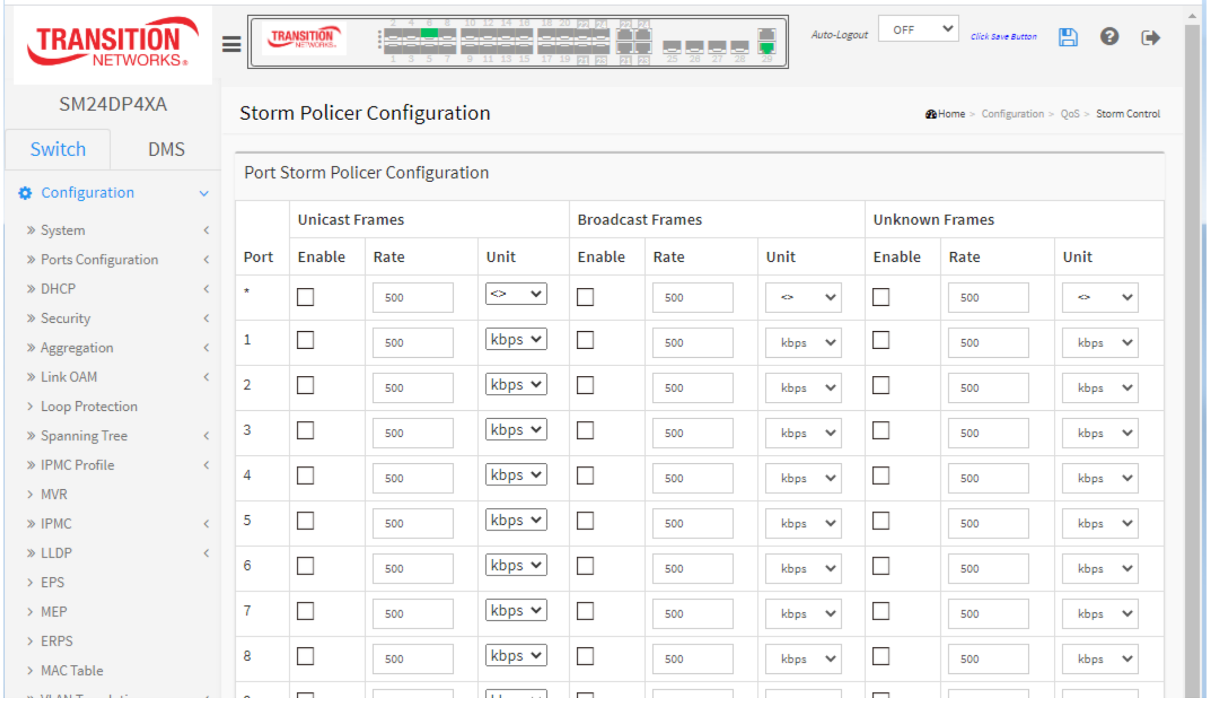
This page lets you configure Storm control for the switch. There is a unicast storm rate control, multicast storm rate control, and a broadcast storm rate control. These only affect flooded frames, i.e. frames with a (VLAN ID, DMAC) pair not present on the MAC Address table. The configuration indicates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

Web Interface

To configure the Storm Control Configuration parameters in the web interface:

1. Click Configuration, QoS, Storm Control Configuration
2. Select the frame type to enable storm control
3. Set the Rate 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 2-24.12: Port Storm Policer Configuration



Storm Policer Configuration

Port Storm Policer Configuration

	Unicast Frames			Broadcast Frames			Unknown Frames		
Port	Enable	Rate	Unit	Enable	Rate	Unit	Enable	Rate	Unit
*	□	500	<>	□	500	<>	□	500	<>
1	□	500	kbps	□	500	kbps	□	500	kbps
2	□	500	kbps	□	500	kbps	□	500	kbps
3	□	500	kbps	□	500	kbps	□	500	kbps
4	□	500	kbps	□	500	kbps	□	500	kbps
5	□	500	kbps	□	500	kbps	□	500	kbps
6	□	500	kbps	□	500	kbps	□	500	kbps
7	□	500	kbps	□	500	kbps	□	500	kbps
8	□	500	kbps	□	500	kbps	□	500	kbps

Frame Type : The settings in a particular row apply to the frame type listed here: 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.

Buttons:

Apply : Click to save changes.

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

2-24.13 Storm Policer

This page lets you configure Port Storm Policer parameters for all switch ports.

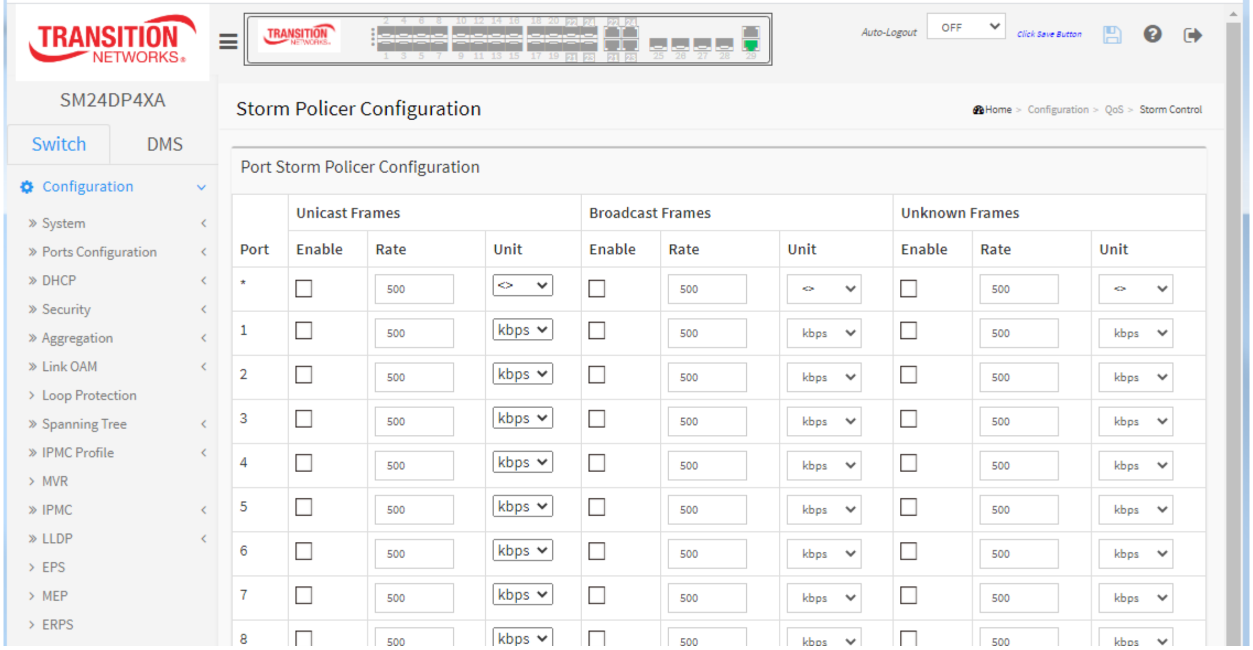
There is a storm policer for unicast frames, broadcast frames and unknown (flooded) frames.

Web Interface

To configure the WRED Configuration parameters in the web interface:

1. Navigate to Switch > Configuration > QoS > Storm Control.
2. Set and select the desired parameters for each port.
3. Click the Apply button to save changes.

Figure 2-24.13: Storm Policer Configuration



Storm Policer Configuration

Port Storm Policer Configuration

	Unicast Frames			Broadcast Frames			Unknown Frames		
Port	Enable	Rate	Unit	Enable	Rate	Unit	Enable	Rate	Unit
*	□	500	<>	□	500	<>	□	500	<>
1	□	500	kbps	□	500	kbps	□	500	kbps
2	□	500	kbps	□	500	kbps	□	500	kbps
3	□	500	kbps	□	500	kbps	□	500	kbps
4	□	500	kbps	□	500	kbps	□	500	kbps
5	□	500	kbps	□	500	kbps	□	500	kbps
6	□	500	kbps	□	500	kbps	□	500	kbps
7	□	500	kbps	□	500	kbps	□	500	kbps
8	□	500	kbps	□	500	kbps	□	500	kbps

Parameter descriptions:

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

Enable: Enable or disable the storm policer for this switch port.

Rate: Controls the rate for the port storm policer. This value is restricted to 1-13128072 when "Unit" is fps or kbps, and 1-13128 when "Unit" is kfps or Mbps. The rate is internally rounded up to the nearest value supported by the port storm policer.

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

Buttons:

Apply : Click to save changes.

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

2-24.14 WRED

This page lets you configure the WRED function for the switch. Here you can configure the Random Early Detection (RED) settings for queues 0 to 5. RED cannot be applied to queues 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.

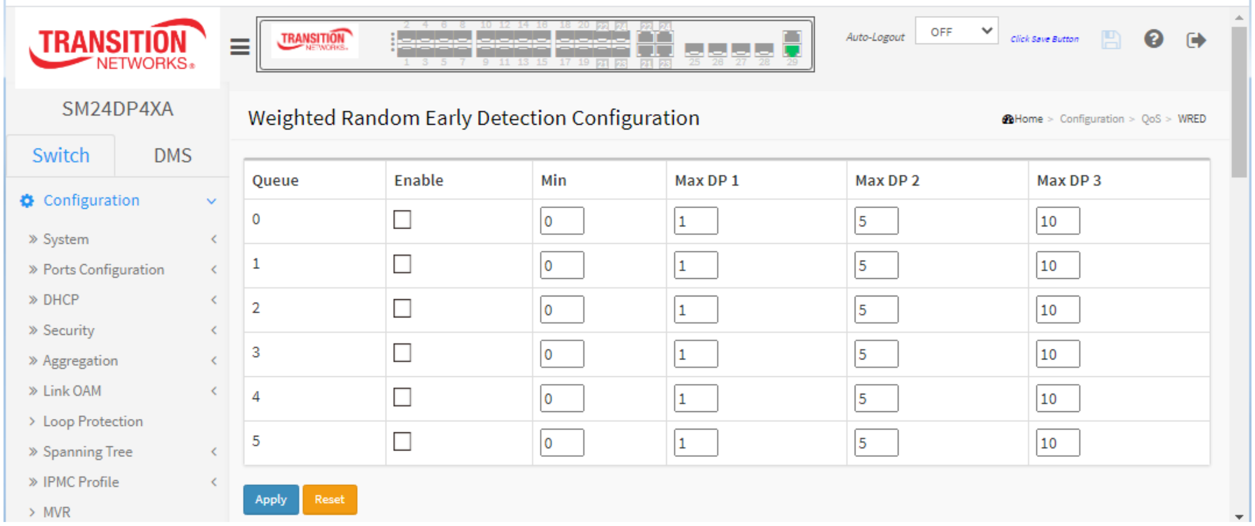
The settings are global for all ports in the switch.

Web Interface

To configure the WRED Configuration parameters in the web interface:

4. Click Configuration, QoS, WRED.
5. Enable or disable WRED.
6. Enter each parameter value.
7. Click the Apply button to save the settings.
8. To cancel the settings click the Reset button. It will revert to previously saved values.

Figure 2-24.13: WRED Configuration



Weighted Random Early Detection Configuration

Queue	Enable	Min	Max DP 1	Max DP 2	Max DP 3
0	□	0	1	5	10
1	□	0	1	5	10
2	□	0	1	5	10
3	□	0	1	5	10
4	□	0	1	5	10
5	□	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.

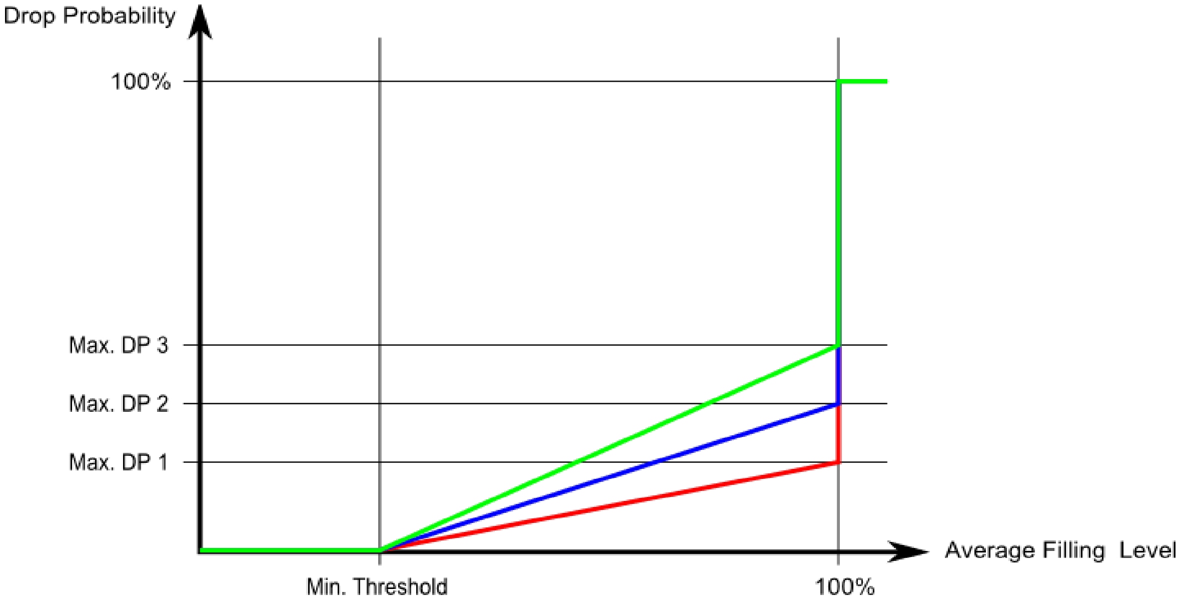
Max DP1 : Controls the drop probability for frames marked with Drop Precedence Level 1 when the average queue filling level is 100%. This value is restricted to 0-100.

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.

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).

Buttons:

Apply : Click to save changes.

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

2-25 Mirroring & Remote Mirroring Configuration

Mirroring is a feature for switched port analyzer. The administrator can use Mirroring to debug network problems. The selected traffic can be mirrored or copied on a destination port where a network analyzer can be attached to analyze the network traffic.

Remote Mirroring is an extended function of Mirroring. It can extend the destination port in another switch. So the administrator can analyze the network traffic on the other switches.

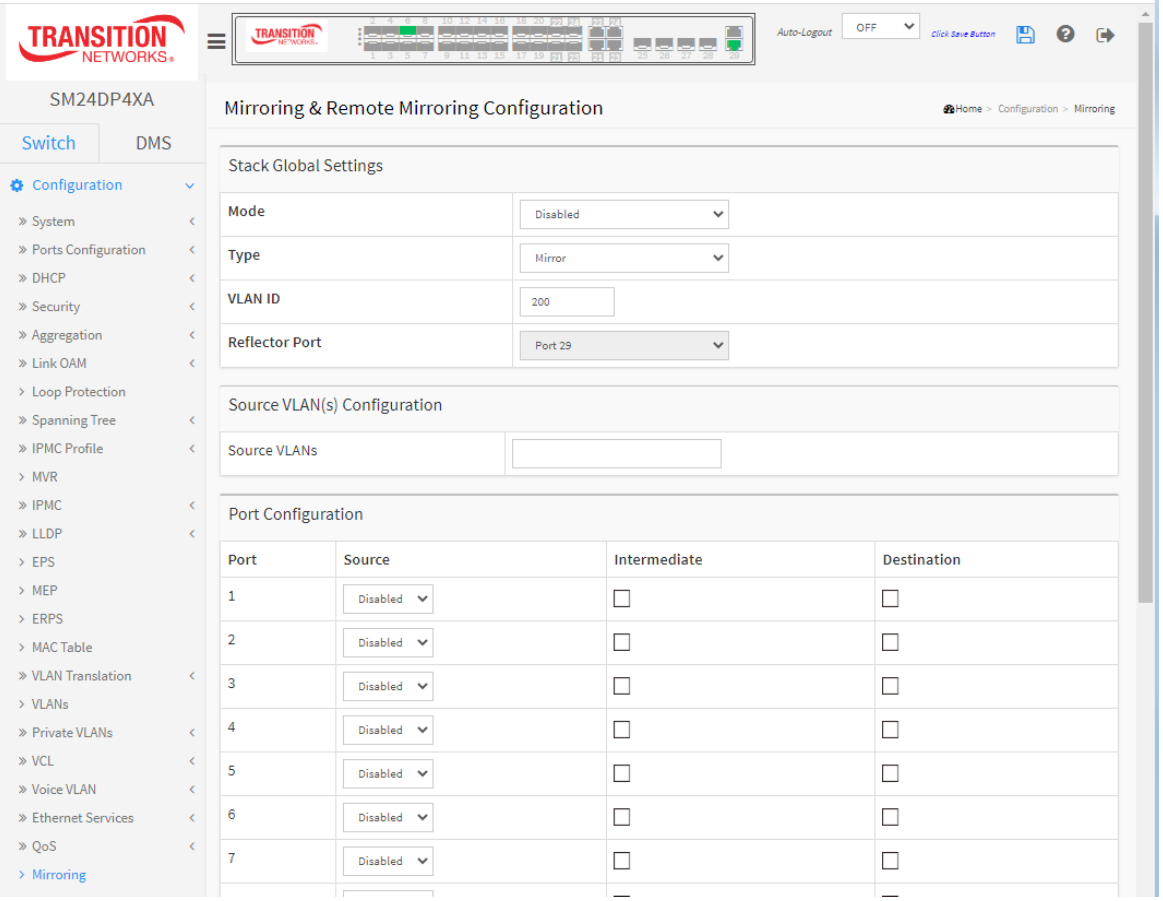
If you want to get the tagged mirrored traffic, you must set VLAN egress tagging as "Tag All" on the reflector port. Otherwise, to get untagged mirrored traffic you must set VLAN egress tagging as "Untag ALL" on the reflector port.

Web Interface

To configure Mirroring via the web interface:

1. Click Configuration, Mirroring.
2. Select the Port to mirror on which port.
3. Select disabled, enable, TX Only and RX Only to set the Port mirror mode.
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 2-26: Mirroring & Remote Mirroring Configuration



Mirroring & Remote Mirroring Configuration

Stack Global Settings

Mode	Disabled
Type	Mirror
VLAN ID	200
Reflector Port	Port 29

Source VLAN(s) Configuration

Source VLANs	

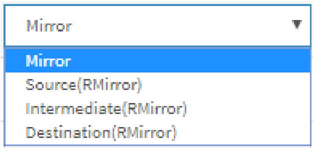
Port Configuration

Port	Source	Intermediate	Destination
1	Disabled	□	□
2	Disabled	□	□
3	Disabled	□	□
4	Disabled	□	□
5	Disabled	□	□
6	Disabled	□	□
7	Disabled	□	□

Parameter descriptions:

Mode : Select Enabled or Disabled as the mirror or Remote Mirroring function. The default is Disabled.

Type : Select switch type:



Mirror : The switch is running in mirror mode. The source port(s) and destination port are located on this switch.

Source(RMirror) : The switch is a source node for monitor flow. The source port(s), reflector port and intermediate port(s) are located on this switch.

Intermediate(RMirror) : The switch is a forwarding node for monitor flow and the switch is an option node. The object is to forward traffic from source switch to destination switch. The intermediate ports are located on this switch.

Destination(RMirror) : The switch is an end node for monitor flow. The destination port(s) and intermediate port(s) are located on this switch.

VLAN ID : Points to where the monitor packet will copy to. The default VLAN ID is 200.

Reflector Port : A method to redirect the traffic to Remote Mirroring VLAN. Any device connected to a port set as a reflector port loses connectivity until the Remote Mirroring is disabled.
If you shut down a port, it cannot be a candidate for reflector port.
If you shut down the port which is a reflector port, the remote mirror function cannot work.

Note 1: The reflector port needs to select only on Source switch type.
Note 2: The reflector port needs to disable MAC Table learning and STP.
Note 3: The reflector port only supports on pure copper ports.

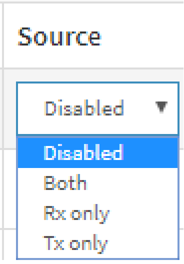
<u>Source VLAN(s) Configuration</u> : The switch can support VLAN-based Mirroring. To monitor some VLANs on the switch, you can set the selected VLANs on this field.
Note1: The Mirroring session must have either ports or VLANs as sources, but not both.

<u>Port Configuration</u> : The table is used for port role selecting.

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

Source : Select mirror mode.

Disabled : Neither frames transmitted nor frames received are mirrored.
Both : Frames received and frames transmitted are mirrored on the Intermediate/Destination **port**.
Rx only : Frames received on this port are mirrored on the Intermediate/Destination port. Frames transmitted are not mirrored.
Tx only : Frames transmitted on this port are mirrored on the Intermediate/Destination port. Frames received are not mirrored.



Intermediate : Select intermediate port. This checkbox is designed for Remote Mirroring. The intermediate port is a switched port to connect to other switch. **Note**: The intermediate port requires MAC Table learning to be disabled.

Destination : Select destination port. This checkbox is designed for mirror or Remote Mirroring. The destination port is a switched port that you receive a copy of traffic from the source port.
Note1: In mirror mode, the device only supports one destination port.
Note2: The destination port needs to disable MAC Table learning.

Configuration Guideline for All Features

When the switch is running in Remote Mirroring mode, the administrator must check if other features are enabled or disabled. For example, the administrator has not disabled MSTP on a reflector port. All monitor traffic will be blocked on a reflector port. All recommended settings are described below.

	Impact	source port	reflector port	intermediate port	destination port	Remote Mirroring VLAN
arp_inspection	High		* disabled	* disabled		
acl	Critical		* disabled	* disabled	* disabled	
dhcp_relay	High		* disabled	* disabled		
dhcp_snooping	High		* disabled	* disabled		
ip_source_guard	Critical		* disabled	* disabled	* disabled	
ipmc/igmpsnp	Critical					un-conflict
ipmc/mldsnp	Critical					un-conflict
lacp	Low				o disabled	
lldp	Low				o disabled	
mac learning	Critical		* disabled	* disabled	* disabled	
mstp	Critical		* disabled		o disabled	
mvr	Critical					un-conflict
nas	Critical		* authorized	* authorized	* authorized	
psec	Critical		* disabled	* disabled	* disabled	
qos	Critical		* unlimited	* unlimited	* unlimited	
upnp	Low				o disabled	
mac-based vlan	Critical		* disabled	* disabled		
protocol-based vlan	Critical		* disabled	* disabled		
vlan_translation	Critical		* disabled	* disabled	* disabled	
voice_vlan	Critical		* disabled	* disabled		

mrp	Low				o disabled	
mvrp	Low				o disabled	
Note:						
* -- must						
o -- optional						
Impact: Critical/High/Low						
Critical	5 packets -> 0 packet					
High	5 packets -> 4 packets					
Low	5 packets -> 6 packets					

Buttons

Apply : Click to save changes.

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

2-26 UPnP

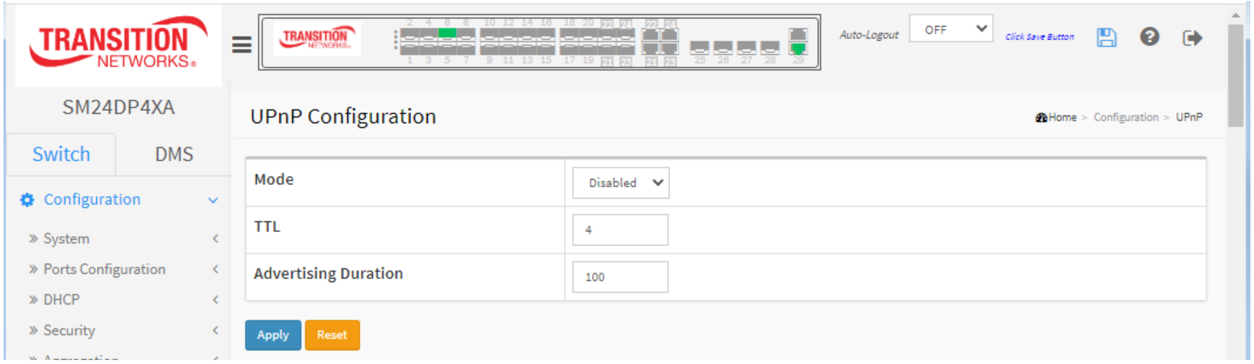
UPnP (Universal Plug and Play) helps allow devices to connect seamlessly and to simplify the implementation of networks in the home (data sharing, communications, and entertainment) and in corporate environments for simplified installation of computer components.

Web Interface

To configure the UPnP via the web interface:

1. Click Configuration, UPnP.
2. Select the mode (enable or disable).
3. Specify the parameters in each blank field.
4. Click the Apply button to save the settings.
5. To cancel the settings click the Reset button to revert to previously saved values.

Figure 2-27: UPnP Configuration



UPnP Configuration

Mode	Disabled
TTL	4
Advertising Duration	100

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:

Save – Click to save changes.

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

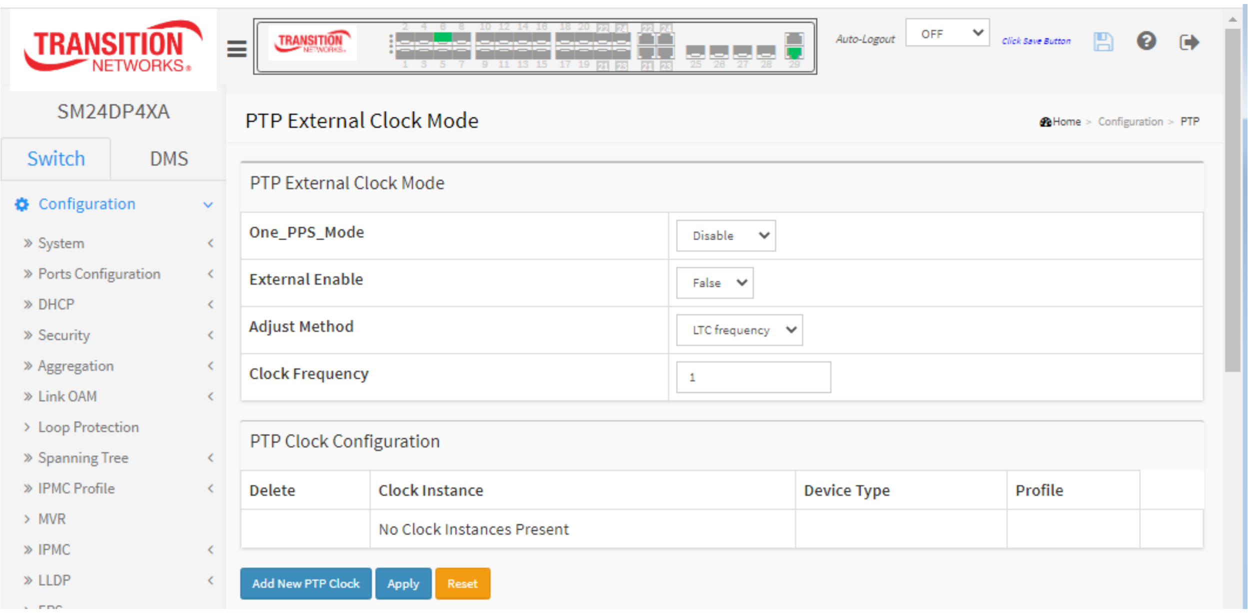
2-27 PTP

The Precision Time Protocol (PTP) is a protocol used to synchronize clocks throughout a computer network. It achieves clock accuracy in the sub-microsecond range, making it suitable for measurement and control systems. A maximum of 4 clock instances can be created.

Web Interface

To configure the PTP Clock Configuration in the web interface:

1. Click Configuration, PTP to display the PTP External Clock Mode page.



PTP External Clock Mode

PTP External Clock Mode

One_PPS_Mode	Disable
External Enable	False
Adjust Method	LTC frequency
Clock Frequency	1

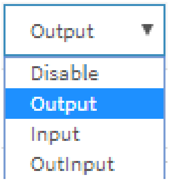
PTP Clock Configuration

Delete	Clock Instance	Device Type	Profile
	No Clock Instances Present		

2. Enter the PTP External Clock Mode parameters.
3. Click the Add New PTP Clock button.
4. Enter the PTP Clock Configuration parameters.
5. Click the Apply button to save the settings. The PTP External Clock Mode page displays again with the new Clock Instance.
6. Click the linked Clock Instance number (instance 0 circled above) to display the PTP Clock's Configuration and Status page (shown below).

PTP External Clock Mode

One_pps_mode : This selection box lets you select the One_pps_mode parameter. Valid values are:



Output : Enable the 1 pps clock output.

Input : Enable the 1 pps clock input.

OutInput : Enable the 1 pps clock output and Input.

Disable : Disable the 1 pps clock in/out-put.

External Enable : This selection box lets you configure the External Clock output:

True : Enable the external clock output.

False : Disable the external clock output.

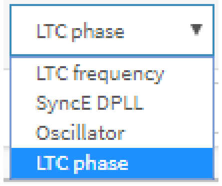
Adjust Method : Selection box lets you configure the Frequency adjustment setting:

LTC frequency : Select Local Time Counter (LTC) frequency control.

SyncE DPLL : Select SyncE DPLL frequency control, if allowed by SyncE.

Oscillator : Select an oscillator independent of SyncE for frequency control, if supported by the hardware.

LTC phase : Select Local Time Counter (LTC) phase control (assumes that the frequency is locked by means of SyncE).



Clock Frequency : Lets you set the Clock Frequency. Valid values are 1 –25000000 (1 - 25MHz).

PTP Clock Configuration

Delete : Check the box to delete the instance.

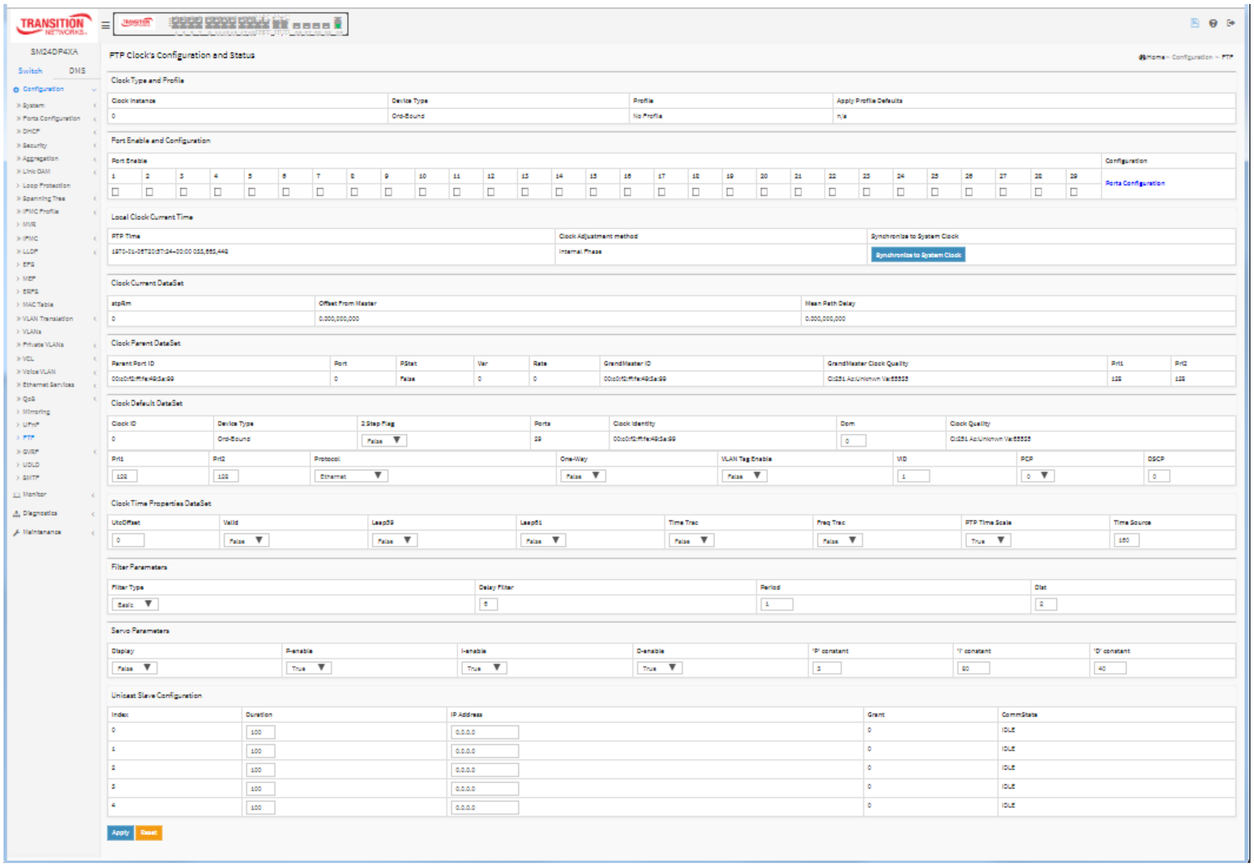
Clock Instance: 0-3.

Device Type : e.g., Ord-Bound

Profile : e.g., 0-3 or No Profile.

On the PTP External Clock Mode page when you click the linked Clock Instance number (e.g., instance 0) the PTP Clock's Configuration and Status page displays as shown below.

PTP Clock's Configuration and Status page (Clock Instance 0)



PTP Clock's Configuration and Status

Clock Type and Profile

Clock Instance	Device Type	Profile	Apply Profile Defaults
0	Ord-Bound	No Profile	n/a

Port Enable and Configuration

Port Enable																													Configuration
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	Ports Configuration
□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	

Local Clock Current Time

PTP Time	Clock Adjustment method	Synchronize to System Clock
1970-01-08T20:37:24+00:00 055,665,449	Internal Phase	Synchronize to System Clock

Clock Current DataSet

stpRm	Offset From Master	Mean Path Delay
0	0.000,000,000	0.000,000,000

Clock Parent DataSet

Parent Port ID	Port	PStat	Var	Rate	GrandMaster ID	GrandMaster Clock Quality	Pri1	Pri2
00:c0:f2:ff:fe:49:5a:99	0	False	0	0	00:c0:f2:ff:fe:49:5a:99	Cl:251 Ac:Unknown Va:65535	128	128

Clock Default DataSet

Clock ID	Device Type	2 Step Flag	Ports	Clock Identity	Dom	Clock Quality
0	Ord-Bound	False ▼	29	00:c0:f2:ff:fe:49:5a:99	0	Cl:251 Ac:Unknown Va:65535

Pri1	Pri2	Protocol	One-Way	VLAN Tag Enable	VID	PCP	DSCP
128	128	Ethernet ▼	False ▼	False ▼	1	0 ▼	0

Clock Time Properties DataSet

UtcOffset	Valid	Leap59	Leap61	Time Trac	Freq Trac	PTP Time Scale	Time Source
0	False ▼	False ▼	False ▼	False ▼	False ▼	True ▼	160

Filter Parameters

Filter Type	Delay Filter	Period	Dist
Basic ▼	6	1	2

Servo Parameters

Display	P-enable	I-enable	D-enable	'P' constant	'I' constant	'D' constant
False ▼	True ▼	True ▼	True ▼	3	80	40

Unicast Slave Configuration

Index	Duration	IP Address	Grant	CommState
0	100	0.0.0.0	0	IDLE
1	100	0.0.0.0	0	IDLE
2	100	0.0.0.0	0	IDLE
3	100	0.0.0.0	0	IDLE
4	100	0.0.0.0	0	IDLE

Apply Reset

Parameter descriptions:

PTP Clock's Configuration and Status

Clock Type and Profile (read only)

Clock Instance : Indicates the Instance of a particular Clock Instance [0..3]. Click on the Clock Instance number to edit the Clock details.

Device Type : Indicates the Type of the Clock Instance. There are five Device Types.

Ord-Bound - clock's Device Type is Ordinary-Boundary Clock.

P2p Transp - clock's Device Type is Peer to Peer Transparent Clock.

E2e Transp - clock's Device Type is End to End Transparent Clock.

Master Only - clock's Device Type is Master Only.

Slave Only - clock's Device Type is Slave Only.

Profile : Displays the Profile number if one exists, otherwise displays No Profile.

Apply Profile Defaults : e.g., n/a.

Port Enable and Configuration

Port Enable : Check or uncheck the box for each port.

Configuration : Linked text Ports Configuration ; click to go to the PTP Clock's Port Data Set Configuration page.

Local Clock Current Time (read only): Show/update local clock data:

PTP Time : Shows the actual PTP time with nanosecond resolution (e.g., 1970-01-06T21:57:43+00:00 278,504,528)

Clock Adjustment method : Shows the actual clock adjustment method. The method depends on the available hardware (e.g., Software).

Synchronize to System Clock : Click the button to synchronize the System Clock to PTP Time.

Ports Configuration : Click to edit the port data set for the ports assigned to this clock instance.

Clock Current DataSet

stpRm : e.g., 0.

Offset From Master : e.g., 0.000,000,000.

Mean Path Delay : e.g., 0.000,000,000.

Clock Parent DataSet

Parent Port ID: e.g., 00:c0:f2:ff:fe:49:3a:9a

Port : e.g., 0.

PStat : e.g., False.

Var : e.g., 0.

Rate : e.g., 0.

GrandMaster ID : e.g., 00:c0:f2:ff:fe:49:3a:9a.

GrandMaster Clock Quality : e.g., Cl:251 Ac:Unknwn Va:65535.

Pri1 : e.g., 128.

Pri2 : e.g., 128.

<u>Clock Default DataSet</u>: The clock default data set is defined in the IEEE 1588 Standard. It holds three groups of data: the static members defined at clock creation time, the Dynamic members defined by the system, and the configurable members which can be set here.

Clock ID: An internal instance id (0..3).

Device Type : Indicates the Type of the Clock Instance. There are five Device Types.

Ord-Bound - Clock's Device Type is Ordinary-Boundary Clock.

P2p Transp - Clock's Device Type is Peer to Peer Transparent Clock.

E2e Transp - Clock's Device Type is End to End Transparent Clock.

Master Only - Clock's Device Type is Master Only.

Slave Only - Clock's Device Type is Slave Only.

2 Step Flag : At the dropdown select True or False. True if two-step Sync events and Pdelay_Resp events are used.

Ports : The total number of physical ports in the node (e.g., 29).

Clock Identity : Displays a unique clock identifier (e.g., 00:c0:f2:ff:fe:49:3a:9a).

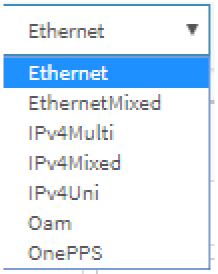
Dom : Domain; Clock domain [0..127].

Clock Quality : Determined by the system, and holds 3 parts: Clock Class, Clock Accuracy and OffsetScaledLog Variance as defined in IEEE1588. The Clock Accuracy values are defined in IEEE1588 table 6 (Currently the clock Accuracy is set to 'Unknown' as default). (E.g., Cl:251 Ac:Unknwn Va:65535).

Pri1 : Clock priority 1 [0..255] used by the BMC master select algorithm; the default is 128.

Pri2 : Clock priority 2 [0..255] used by the BMC master select algorithm; the default is 128.

Protocol : at the dropdown select Ethernet (default), EthernetMixed, IPv4Multi, IPv6Mixed, IPv4Uni, Oam, or OnePPS. This is the Transport protocol used by the PTP protocol engine:



Ethernet PTP over Ethernet multicast

EthernetMixed PTP using a combination of Ethernet multicast and unicast

IPv4Multi PTP over IPv4 multicast

IPv4Mixed PTP using a combination of IPv4 multicast and unicast

IPv4Uni PTP over IPv4 unicast

One-Way : Select True or False. The default is False. If true, one way measurements are used. This parameter applies only to a slave. In one-way mode no delay measurements are performed, i.e. this is applicable only if frequency synchronization is needed. The master always responds to delay requests.

VLAN Tag Enable : Select True or False. The default is False. The VLAN Tag Enable parameter is ignored, because the tagging is controlled by the VLAN configuration.

VID : VLAN Identifier used for tagging the VLAN packets. The default is 0.

PCP : Priority Code Point value used for PTP frames. Select 0-7.

DSCP : The default is 0.

Clock Time Properties DataSet : The clock time properties data set is defined in the IEEE 1588 Standard. The data set is both configurable and dynamic, i.e. the parameters can be configured for a grandmaster. In a slave clock the parameters are overwritten by the grandmasters timing properties.
Note: These parameters are not used in the current PTP implementation. The valid values for the Time Source parameter are:

16 (0x10) ATOMIC_CLOCK
32 (0x20) GPS
48 (0x30) TERRESTRIAL_RADIO
64 (0x40) PTP
80 (0x50) NTP
96 (0x60) HAND_SET
144 (0x90) OTHER
160 (0xA0) INTERNAL_OSCILLATOR

UtcOffset : enter a number; 0 is the default.

Valid : select True or False; False is the default.
Leap59 : select True or False; False is the default.

Leap61 : select True or False; False is the default.

Time Trac : select True or False; False is the default.

Freq Trac : select True or False; False is the default.

PTP Time Scale : select True or False; True is the default.

Time Source : e.g., 160

Filter Parameters : The default delay filter is a low pass filter, with a time constant of 2**DelayFilter*DelayRequestRate.
If the DelayFilter parameter is set to 0, the delay filter uses the same algorithm as the offset filter.
The default offset filter uses a minimum offset or a mean filter method (i.e., the minimum measured offset during Period samples is used in the calculation). The distance between two calculations is Dist periods. **Note**: In configurations with Timestamp enabled PHYs, the period is automatically increased, if (period*dist < SyncPackets pr sec/4), i.e. max 4 adjustments are made pr sec.

If Dist is 1 the offset is averaged over the Period,

If Dist is >1 the offset is calculated using 'min' offset.

Filter Type: Shows the filter type used which can be either the basic filter or an advanced filter that can be configured to use only a fraction of the packets received (i.e. the packets that have experienced the least latency) (e.g., Basic).

Delay Filter : See above (e.g., 6).

Period : e.g., 1. See above.

Dist : e.g., 2. See above.

Servo Parameters : The default clock servo uses a PID regulator to calculate the current clock rate. i.e.

clockAdjustment =
OffsetFromMaster/ P constant +
Integral(OffsetFromMaster)/ I constant +
Differential OffsetFromMaster)/ D constant

Display : Select True or False. The default is False. If true then Offset From Master, MeanPathDelay and clockAdjustment are logged on the debug terminal

P-enable : Select True or False. The default is True. If true the P part of the algorithm is included.

I-enable : Select True or False. The default is True. If true the I part of the algorithm is included.

D-enable : Select True or False. The default is True. If true the D part of the algorithm is included.

'P' constant: [1..1000] see above. The default is 3.

'I' constant : [1..1000] see above. The default is 80.

'D' constant : [1..1000] see above. The default is 40.

Unicast Slave Configuration : When operating in IPv4 Unicast mode, the slave is configured up to 5 master IP addresses. The slave then requests Announce messages from all the configured masters. The slave uses the BMC algorithm to select one as master clock, the slave then request Sync messages from the selected master.

Index : Instances (0-4).

Duration : The number of seconds a master is requested to send Announce/Sync messages. The request is repeated from the slave each Duration/4 seconds. The default is 100.

IP Address : The IPv4 Address of the Master clock. The default is 0.0.0.0.

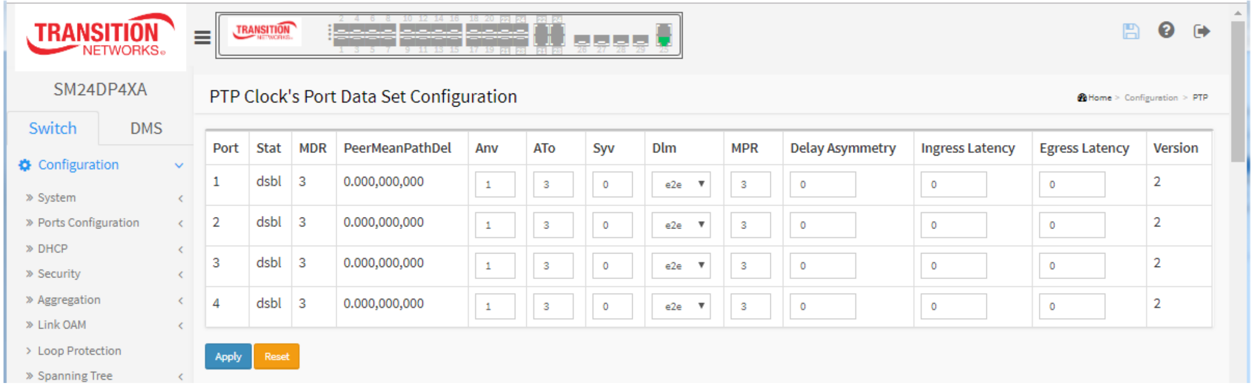
Grant : The granted repetition period for the sync message (e.g., 0).

CommState : The state of the communication with the master, possible values are:

- ***IDLE*** : The entry is not in use.
- ***INIT*** : Announce is sent to the master (Waiting for a response).
- ***CONN*** : The master has responded.
- ***SELL*** : The assigned master is selected as current master.
- ***SYNC*** : The master is sending Sync messages.

PTP Clock's Port Data Set Configuration

At the PTP Clock's Configuration and Status page if you have Port Enabled in the Port Enable and Configuration section, you can click on the linked Ports Configuration text in the Configuration column to display the PTP Clock's Port Data Set Configuration page:



PTP Clock's Port Data Set Configuration

Port	Stat	MDR	PeerMeanPathDel	Anv	ATo	Syv	Dlm	MPR	Delay Asymmetry	Ingress Latency	Egress Latency	Version
1	dsbl	3	0.000,000,000	1	3	0	e2e ▼	3	0	0	0	2
2	dsbl	3	0.000,000,000	1	3	0	e2e ▼	3	0	0	0	2
3	dsbl	3	0.000,000,000	1	3	0	e2e ▼	3	0	0	0	2
4	dsbl	3	0.000,000,000	1	3	0	e2e ▼	3	0	0	0	2

Parameter descriptions:

Port : Static member port Identity : Port number [1..max port no]

Stat : Dynamic member portState: Current state of the port (e.g., dsbl).

MDR : Dynamic member log Min Delay Req Interval: The delay request interval announced by the master.

Peer Mean Path Del : The path delay measured by the port in P2P mode. In E2E mode this value is 0.

Anv : The interval for issuing announce messages in master state. Range is -3 to 4.

ATo : The timeout for receiving announce messages on the port. Range is 1 to 10.

Syv : The interval for issuing sync messages in master. Range is -7 to 4.

Dlm : Configurable member delayMechanism: The delay mechanism used for the port:

e2e : End to end delay measurement

p2p : Peer to peer delay measurement.

Can be defined per port in an Ordinary/Boundary clock. In a transparent clock all ports use the same delay mechanism, determined by the clock type.

MPR : The interval for issuing Delay_Req messages for the port in E2e mode. This value is announced from the master to the slave in an announce message. The value is reflected in the MDR field in the Slave

The interval for issuing Pdelay_Req messages for the port in P2P mode. Range is -7 to 5.

Note: The interpretation of this parameter has changed from release 2.40. In earlier versions the value was interpreted relative to the Sync interval, this was a violation of the standard, so now the value is interpreted as an interval. I.e. MPR = 0 => 1 Delay_Req pr sec, independent of the Sync rate.

Delay Asymmetry : If the transmission delay for a link in not symmetric, the asymmetry can be configured here, see IEEE 1588 Section 7.4.2 Communication path asymmetry. Range is -100000 to 100000.

Version : The current implementation only supports PTP version 2.

Ingress latency : Ingress latency measured in ns, as defined in IEEE 1588 Section 7.3.4.2.
Range is -100000 to 100000.

Egress Latency : Egress latency measured in ns, as defined in IEEE 1588 Section 7.3.4.2.
Range is -100000 to 100000.

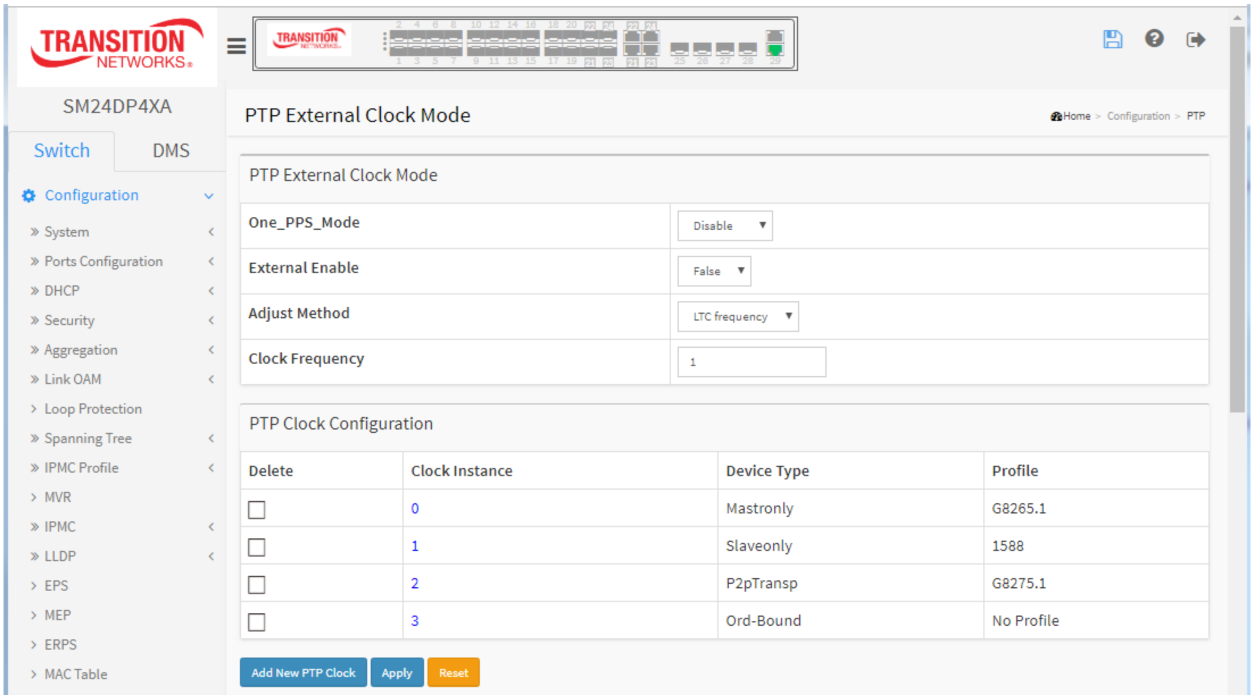
Buttons

Add New PTP Clock : Click to create a new clock instance.

Apply : Click to save the page immediately.

Reset : Click to reset the page immediately.

Example : Four PTP Clock instances configured:



PTP External Clock Mode

PTP External Clock Mode

One_PPS_Mode	Disable ▾
External Enable	False ▾
Adjust Method	LTC frequency ▾
Clock Frequency	1

PTP Clock Configuration

Delete	Clock Instance	Device Type	Profile
□	0	Mastronly	G8265.1
□	1	Slaveonly	1588
□	2	P2pTransp	G8275.1
□	3	Ord-Bound	No Profile

2-28 GVRP

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.

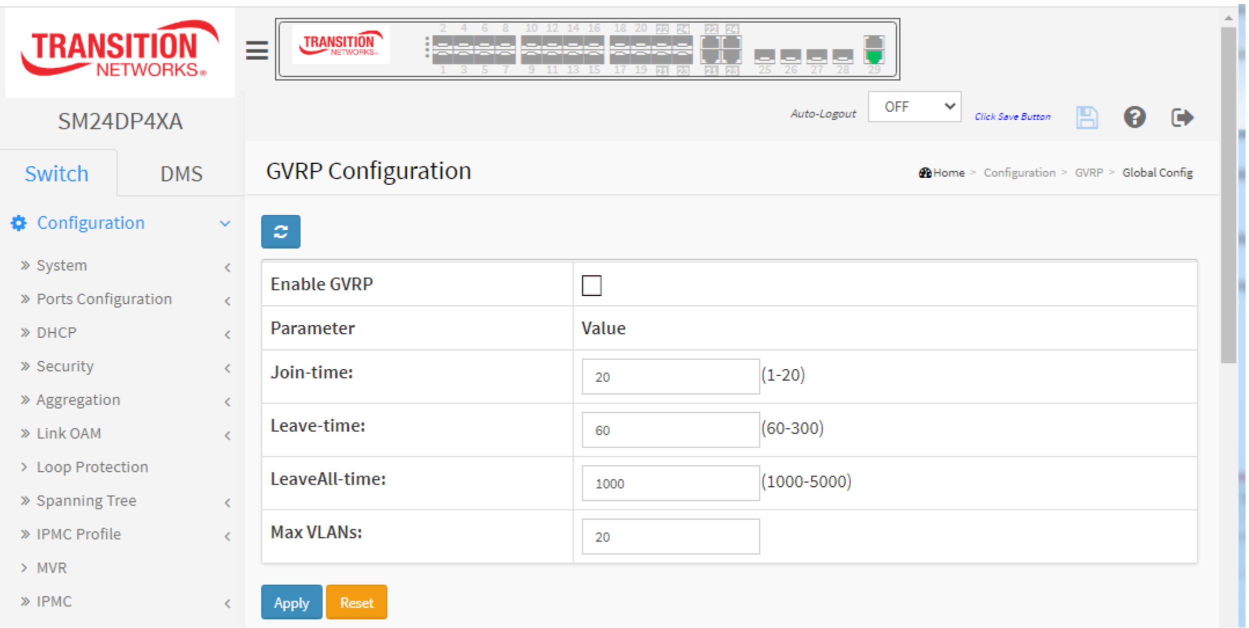
GVRP (GARP VLAN Registration Protocol) is used for dynamically registering VLANs on ports as specified in IEEE 802.1Q-2005, clause 11. GVRP is an example of the use of GARP, hence the G in GVRP.

2-28.1 Global Config

To configure GVRP via the web interface:

1. Click Configuration, GVRP, Global Config.
2. Check the “Enable GVRP” checkbox.
3. Specify Join-time, Leave-time, Leave All-time, and Max VLANs.
4. Click Apply.

Figure 2-29.1: GVRP Configuration



GVRP Configuration

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

Parameter descriptions:

Enable GVRP : The GVRP feature is enabled globally by setting the check mark in the checkbox named Enable GVRP.

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

Refresh: Click to refresh the page immediately.

Apply : Click to save the page immediately.

Reset : Click to reset the page immediately.

2-28.2 Port Config

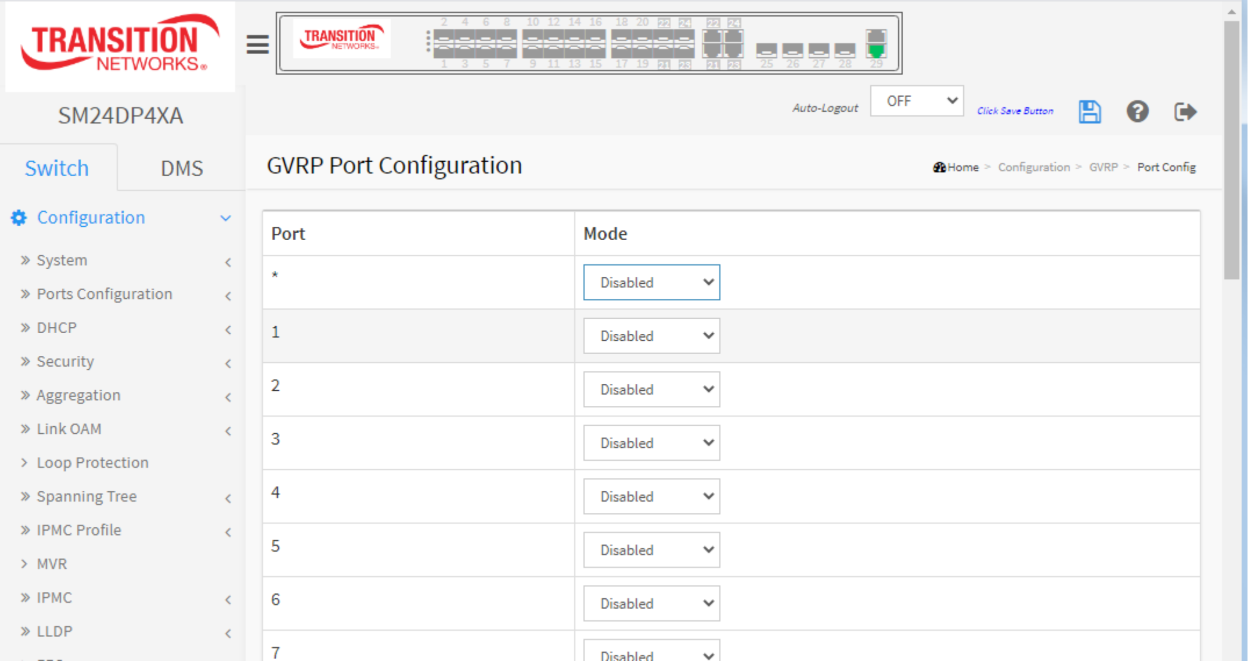
This page allows you to configure the basic GVRP Configuration settings for all switch ports.
This configuration can be performed either before or after GVRP is configured globally; the protocol operation will be the same either way.

Web Interface

To configure GVRP via the web interface:

1. Click Configuration, GVRP, Port Config.
2. Specify Port mode.
3. Click Apply.

Figure 2-29.2: GVRP Port Configuration



Auto-Logout OFF

GVRP Port Configuration

Port	Mode
*	Disabled
1	Disabled
2	Disabled
3	Disabled
4	Disabled
5	Disabled
6	Disabled
7	Disabled

Parameter descriptions:

Port : The logical port that is to be configured.

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

Disabled **:** Select to Disable GVRP mode on this port.

GVRP Enabled **:** Select to Enable GVRP mode on this port.

Buttons

Apply : Click to save the page immediately.

Reset : Click to reset the page immediately.

2-29 UDLD

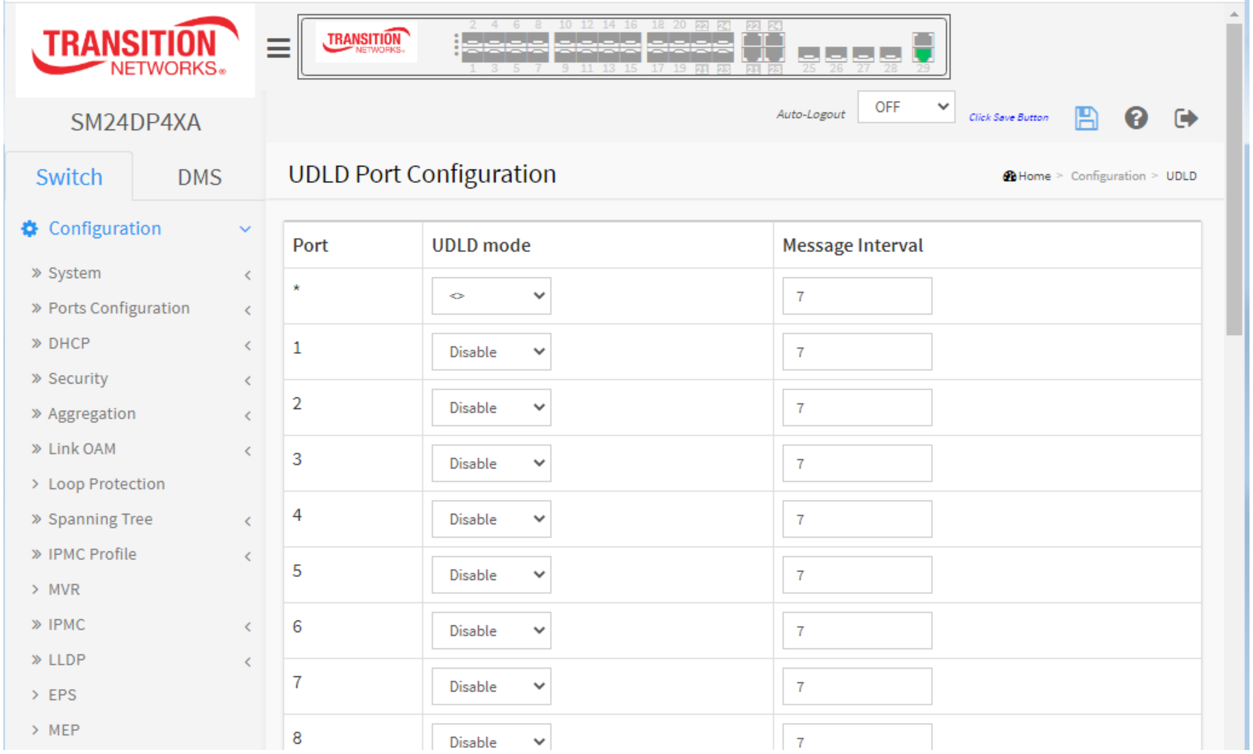
The UDLD (Uni Directional Link Detection) protocol monitors the physical configuration of the links between devices and ports that support UDLD. It detects the existence of unidirectional links.
UDLD provides mechanisms useful for detecting one way connections before they create a loop or other protocol malfunction. IETF RFC 5171 specifies a way at data link layer to detect Uni directional link.

Web Interface

To configure the UPnP Configuration in the web interface:

1. Click Configuration, UDLD.
2. Set the UDLD mode and Message Interval.
3. Click the Apply button to save the settings.
4. To cancel the settings click the Reset button. It will revert to previously saved values.

Figure 2-33: UDLD Port Configuration



UDLD Port Configuration

Port	UDLD mode	Message Interval
*	<>	7
1	Disable	7
2	Disable	7
3	Disable	7
4	Disable	7
5	Disable	7
6	Disable	7
7	Disable	7
8	Disable	7

Parameter descriptions:

Port : Port number of the switch.

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

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

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

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

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

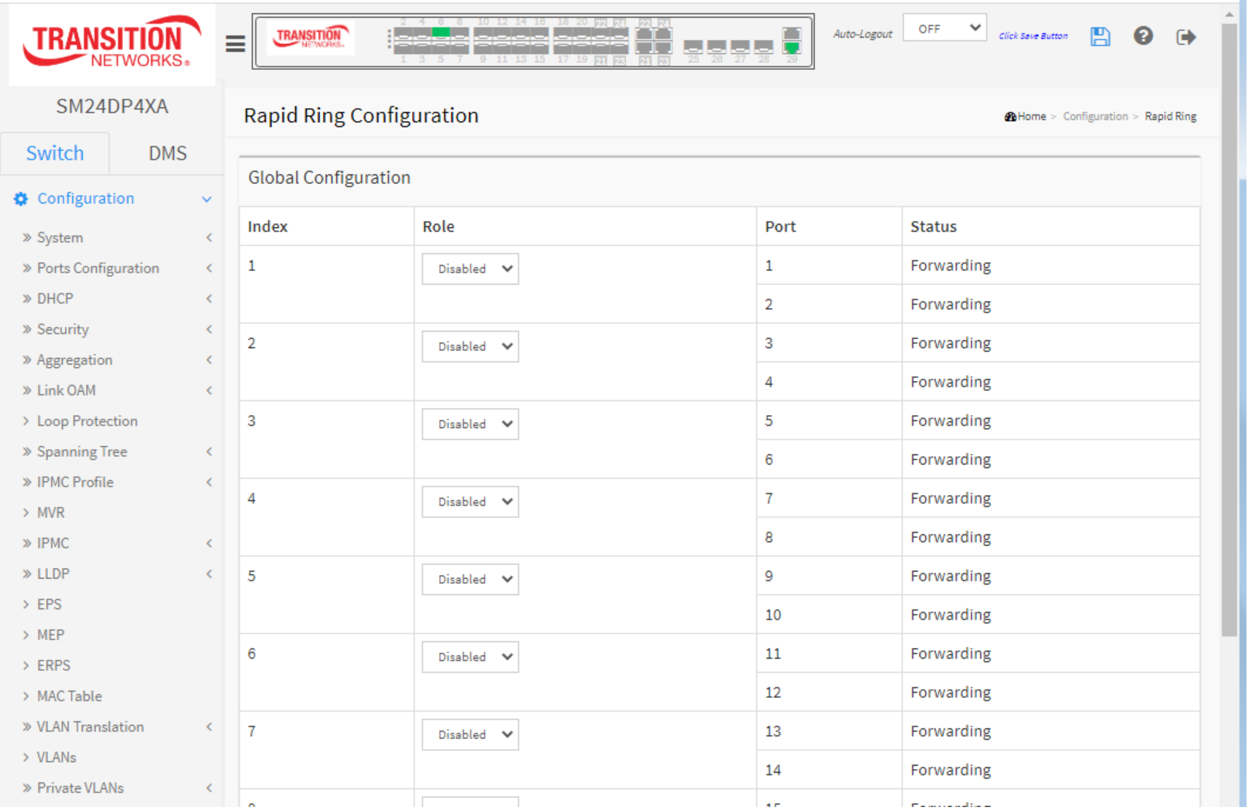
Buttons

Apply : Click to save the page immediately.

Reset : Click to reset the page immediately.

2-30 Rapid Ring

Configure Rapid Ring Global Configuration parameters at Switch > Configuration > Rapid Ring.



Rapid Ring Configuration

Global Configuration

Index	Role	Port	Status
1	Disabled	1	Forwarding
		2	Forwarding
2	Disabled	3	Forwarding
		4	Forwarding
3	Disabled	5	Forwarding
		6	Forwarding
4	Disabled	7	Forwarding
		8	Forwarding
5	Disabled	9	Forwarding
		10	Forwarding
6	Disabled	11	Forwarding
		12	Forwarding
7	Disabled	13	Forwarding
		14	Forwarding
8		15	Forwarding

Parameter descriptions:

Index: The Rapid Ring instance number (1-14).

Role: Select a Rapid Ring role (*Disabled*, *Master*, or *Member*). The default is *Disabled*. **Note**: Rapid Ring Role cannot be returned to Disabled using the Web UI. The roles can be disabled using the CLI command interface. See the CLI Reference.

Port: The switch port number of the port.

Status: The current Rapid Ring status of the port (e.g., *Forwarding*, *Discarding*).

Buttons

Apply: Click to apply changes.

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

Messages:

Message: *Rapid Ring Configuration Error*
Error in port 3, STP is enable
Meaning: Spanning Tree and Rapid Ring cannot both be enabled at the same time.
Recovery: Click the Previous button, disable Spanning Tree at Configuration > Spanning Tree > CIST Port, and continue operation.

2-31 SMTP

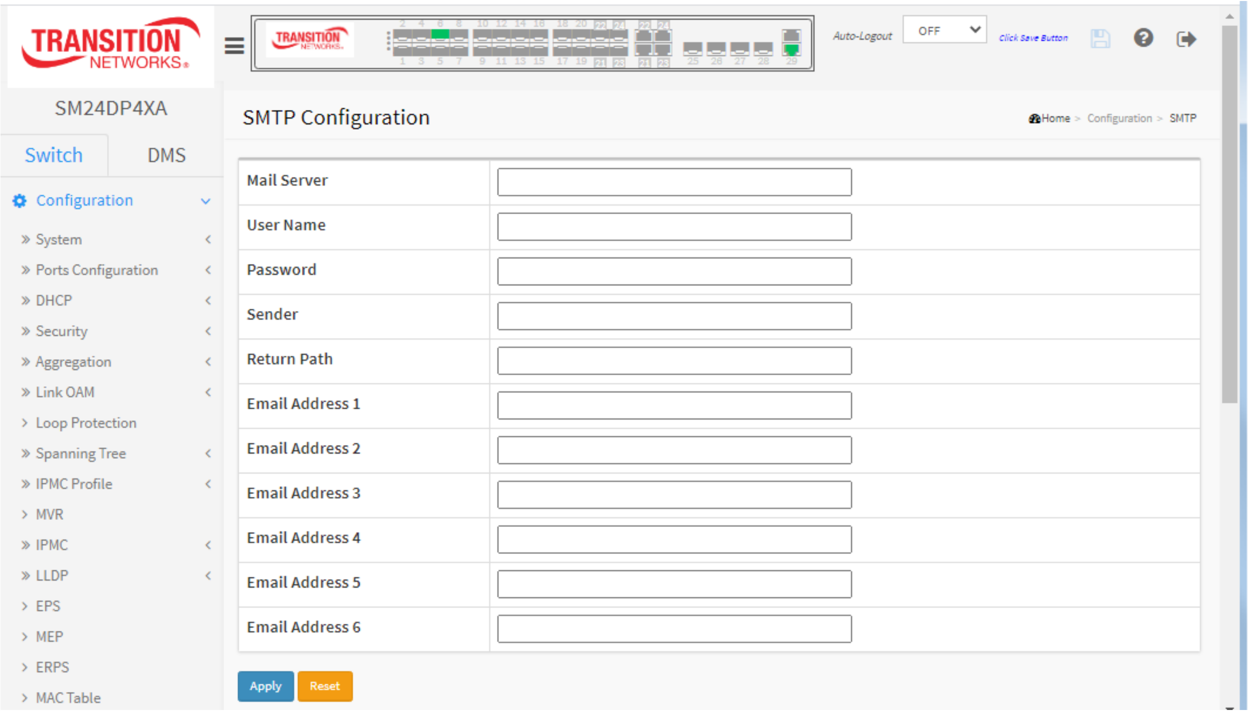
Configure SMTP (Simple Mail Transfer Protocol) on this page. Simple Mail Transfer Protocol is the message-exchange standard for the Internet. The Switch is to be configured as a client of SMTP while the server is a remote device that will receive messages from the switch that alarm events occurred.

Web Interface

To configure the UPnP Configuration via the web interface:

1. Click Configuration, SMTP.
2. Enter the User Name, Password, Sender and Return Path parameters.
3. Enter Email Address 1-6 as required.
4. Click the Apply button to save the settings.
5. To cancel the settings click the Reset button. It will revert to previously saved values.

Figure 2-34: SMTP Configuration



SMTP Configuration

Mail Server	
User Name	
Password	
Sender	
Return Path	
Email Address 1	
Email Address 2	
Email Address 3	
Email Address 4	
Email Address 5	
Email Address 6	

Parameter descriptions:

Mail Server : The IP address or hostname of the mail server. IP address is expressed in dotted decimal notation. This will be the device that sends out the mail.

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 (up to six).

Buttons

Apply : Click to apply changes.

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

3. Monitor

This chapter describes the monitor sub-menus (e.g., System, Ports, Link OAM, DHCP, Security, PTP, etc.).

3-1 System

After you login, the switch displays system information. This page is the default (startup) page that displays after you log in.

3-1.1 Information

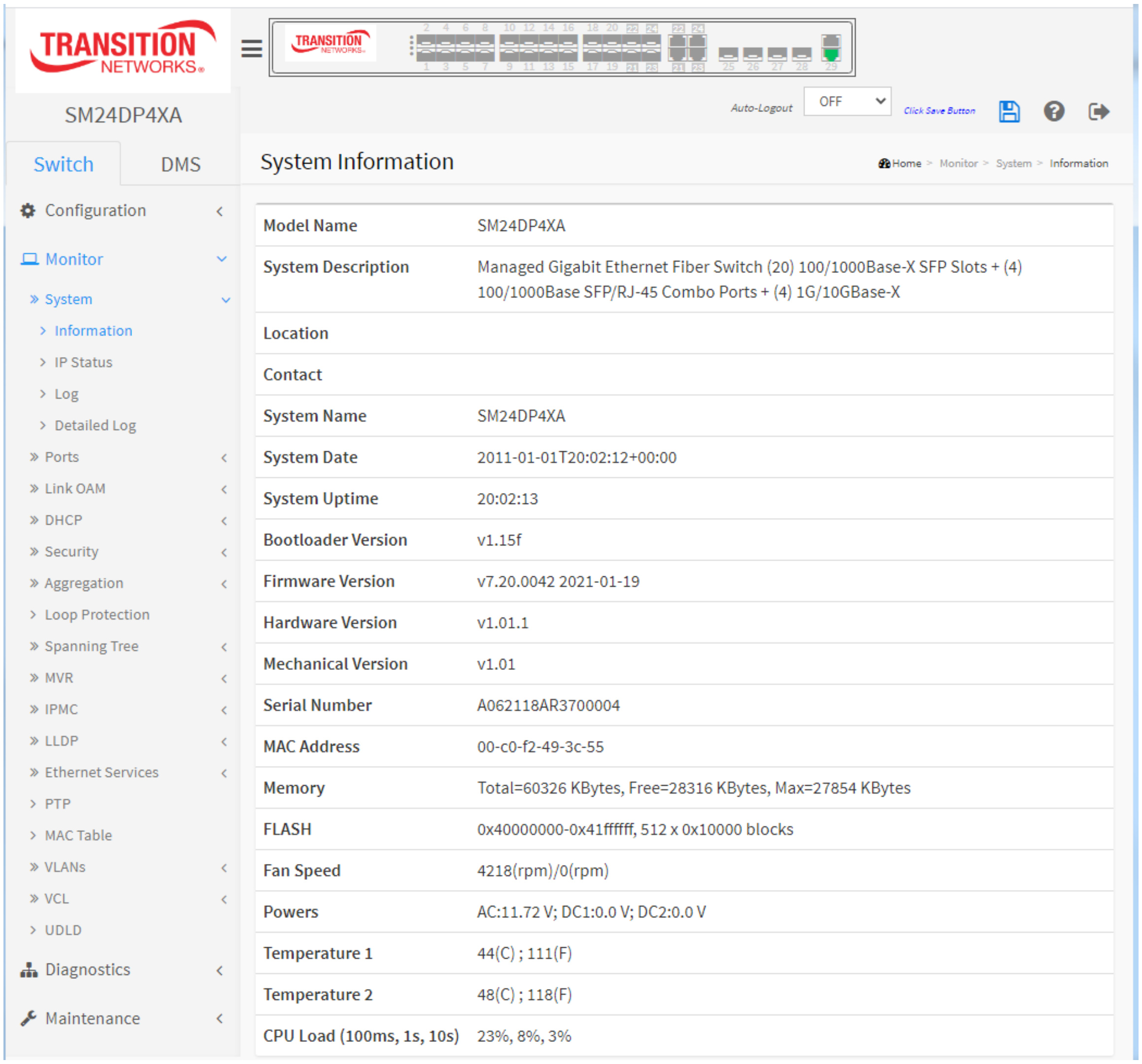
This page displays switch system information, such as Model Name, System Description, System Uptime, Firmware Version, Serial Number, MAC Address, Fan Speed, etc.

Web interface

To configure System Information in the web interface:

1. Click Monitor, System, and Information.
2. View the system and contact information.

Figure 3-1.1: System Information



System Information

Model Name	SM24DP4XA
System Description	Managed Gigabit Ethernet Fiber Switch (20) 100/1000Base-X SFP Slots + (4) 100/1000Base SFP/RJ-45 Combo Ports + (4) 1G/10GBase-X
Location	
Contact	
System Name	SM24DP4XA
System Date	2011-01-01T20:02:12+00:00
System Uptime	20:02:13
Bootloader Version	v1.15f
Firmware Version	v7.20.0042 2021-01-19
Hardware Version	v1.01.1
Mechanical Version	v1.01
Serial Number	A062118AR3700004
MAC Address	00-c0-f2-49-3c-55
Memory	Total=60326 KBytes, Free=28316 KBytes, Max=27854 KBytes
FLASH	0x40000000-0x41ffffff, 512 x 0x10000 blocks
Fan Speed	4218(rpm)/0(rpm)
Powers	AC:11.72 V; DC1:0.0 V; DC2:0.0 V
Temperature 1	44(C) ; 111(F)
Temperature 2	48(C) ; 118(F)
CPU Load (100ms, 1s, 10s)	23%, 8%, 3%

Parameter descriptions:

Model Name : Model Name (*SM24DP4XA*).

System Description : System Description (*Managed Fiber Switch, 24-port 100/1000Base-X SFP + (4) 1G/10G SFP+*).

Location : The system location configured in Configuration > System > Information > System Location.

Contact : The system contact configured in Configuration > System > Information > System Contact.

System Name : The system name (*SM24DP4XA*).

System Date : The current (GMT) system time and date. The system time is obtained through the Timing server running on the switch, if any. The default is *2011-01-06T21:41:32+00:00*.

System Uptime : The period of time the device has been operational (e.g., *5d 21:41:33*).

Bootloader Version : The boot code version of this switch (e.g., *v1.33* or *v 1.15f*).

Firmware Version : The software version and date of this switch (e.g., *v7.20.0042 2021-01-19*).

Hardware Version : The hardware version of this switch (e.g., *v1.01.1 or v1.01.1*).

Mechanical Version : The mechanical version of this switch (e.g., *v1.01*).

Serial Number : The serial number of this switch (e.g., *A062118AR3700002*).

MAC Address : The MAC address of this switch (e.g., *06-c3-f2-49-3a-99*).

Memory : Displays the memory size of the system (e.g., *Total=62772 KBytes, Free=31253 KBytes, Max=30662 Kbytes*).

FLASH : Displays the flash size of the system (e.g., *0x40000000-0x41ffffff, 512 x 0x10000 blocks*).

Fan Speed : Displays the fan speed (rpm) of the system (e.g., *5273(rpm)/5273(rpm)*).

Powers: Displays the AC and DC input power levels (e.g., *AC:0.00 V; DC:11.54 V* or *AC:11.90 V; DC:11.54 V*).

Temperature 1 : Detect and show temperature sensor 1 in both Celsius and Fahrenheit. For example : *36(C) ; 96(F)*.

Temperature 2 : Detect and show temperature sensor 2 in both Celsius and Fahrenheit. For example: *40(C) ; 104(F)*.

CPU Load : Displays the CPU loading(100ms, 1s, 10s) of the system (e.g., *1%, 6%, 4%*). The CPU load is measured as averaged over the last 100ms, 1sec and 10 seconds intervals. The last 120 samples are graphed, and the last numbers are displayed as text as well. In order to display the SVG graph, your browser must support the SVG format. Consult the SVG Wiki for more information on browser support. Specifically, at the time of writing, Microsoft Internet Explorer will need to have a plugin installed to support SVG.

3-1.3 IP Status

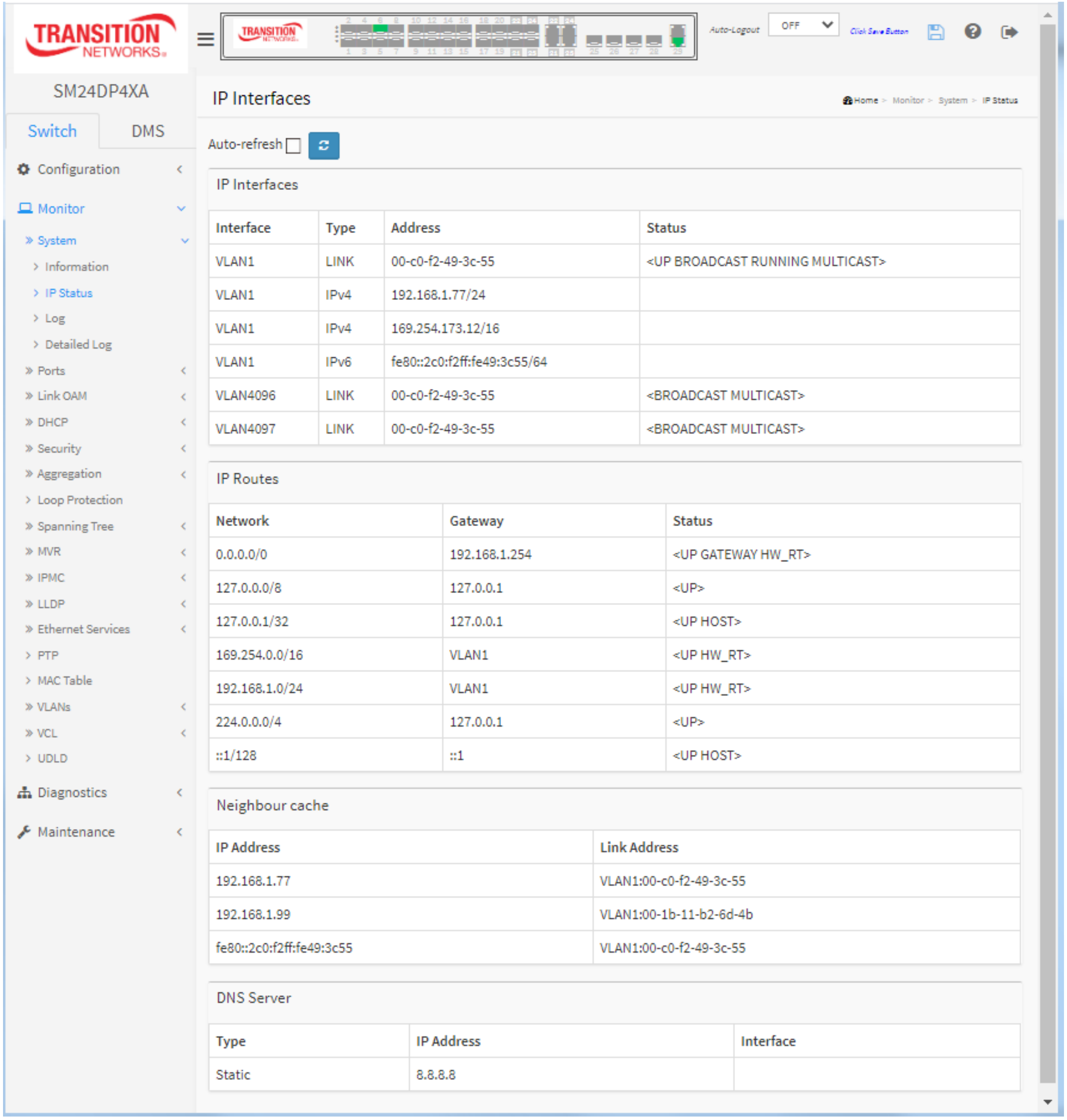
This page displays the status of the IP protocol layer. The status is defined by the IP interfaces, the IP routes and the neighbor cache (ARP cache) status.

Web Interface

To display the log configuration in the web interface:

1. Click Monitor, System and IP Status.
2. View the IP address information.

Figure 3- 1.3: IP Status



IP Interfaces

Auto-refresh □

IP Interfaces

Interface	Type	Address	Status
VLAN1	LINK	00-c0-f2-49-3c-55	<UP BROADCAST RUNNING MULTICAST>
VLAN1	IPv4	192.168.1.77/24	
VLAN1	IPv4	169.254.173.12/16	
VLAN1	IPv6	fe80::2c0:f2ff:fe49:3c55/64	
VLAN4096	LINK	00-c0-f2-49-3c-55	<BROADCAST MULTICAST>
VLAN4097	LINK	00-c0-f2-49-3c-55	<BROADCAST MULTICAST>

IP Routes

Network	Gateway	Status
0.0.0.0/0	192.168.1.254	<UP GATEWAY HW_RT>
127.0.0.0/8	127.0.0.1	<UP>
127.0.0.1/32	127.0.0.1	<UP HOST>
169.254.0.0/16	VLAN1	<UP HW_RT>
192.168.1.0/24	VLAN1	<UP HW_RT>
224.0.0.0/4	127.0.0.1	<UP>
::1/128	::1	<UP HOST>

Neighbour cache

IP Address	Link Address
192.168.1.77	VLAN1:00-c0-f2-49-3c-55
192.168.1.99	VLAN1:00-1b-11-b2-6d-4b
fe80::2c0:f2ff:fe49:3c55	VLAN1:00-c0-f2-49-3c-55

DNS Server

Type	IP Address	Interface
Static	8.8.8.8	

Parameter descriptions:

<u>**IP Interfaces**</u>

Interface : Shows the name of the interface.

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).

<u>**IP Routes**</u>

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

Gateway : Shows the gateway address of this route.

Status : Show the status flags of the route.

<u>**Neighbour cache**</u>

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 exists.

<u>**DNS Server**</u>

Type : The configuration type of DNS server.

IP Address : The IP address of the DNS server.

Interface : The name of the interface.

Buttons

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

Refresh: Click to manually refresh the page immediately.

3-1.4 Log

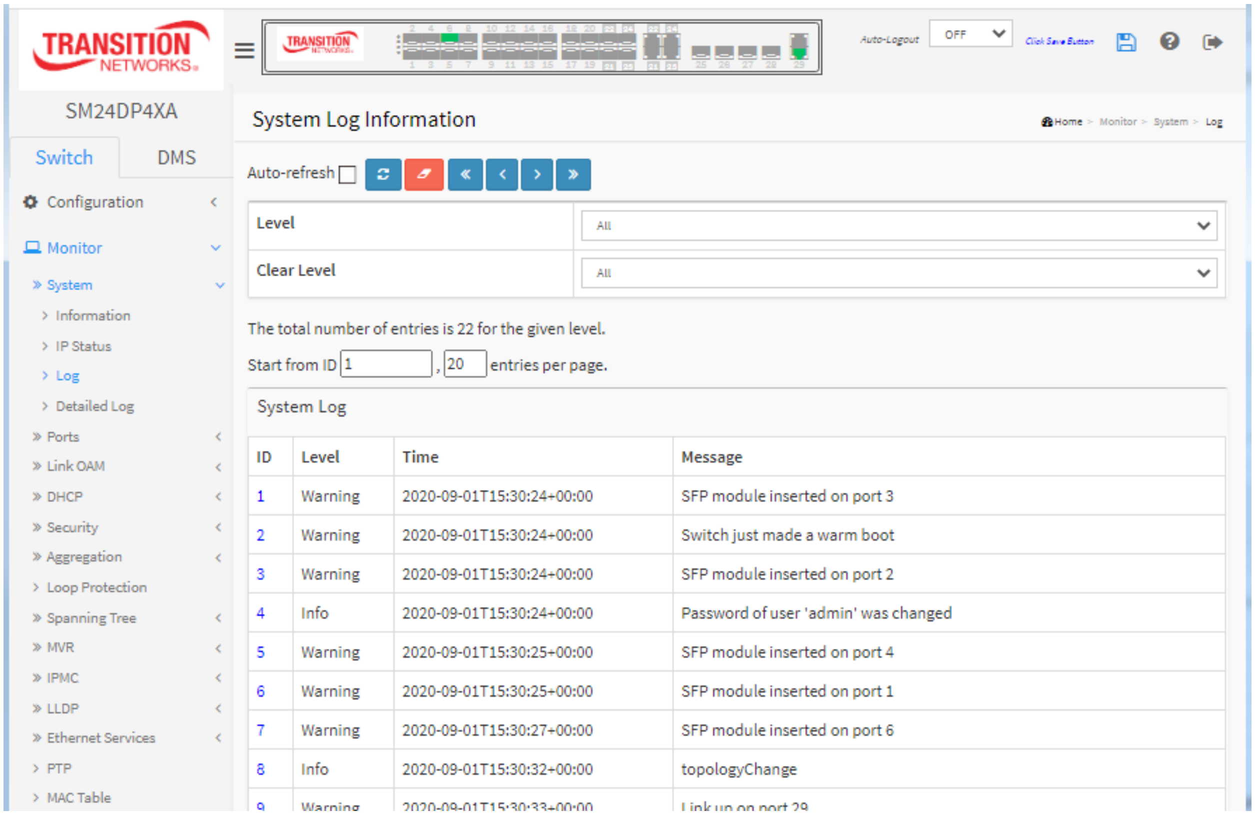
This page displays the system log information of the switch.

Web Interface

To display the log configuration in the web interface:

1. Click Monitor, System and Log.
2. Display the log information.

Figure 3- 1.4: System Log Information



System Log Information

Auto-refresh □

Level	All
Clear Level	All

The total number of entries is 22 for the given level.

Start from ID 1 , 20 entries per page.

System Log

ID	Level	Time	Message
1	Warning	2020-09-01T15:30:24+00:00	SFP module inserted on port 3
2	Warning	2020-09-01T15:30:24+00:00	Switch just made a warm boot
3	Warning	2020-09-01T15:30:24+00:00	SFP module inserted on port 2
4	Info	2020-09-01T15:30:24+00:00	Password of user 'admin' was changed
5	Warning	2020-09-01T15:30:25+00:00	SFP module inserted on port 4
6	Warning	2020-09-01T15:30:25+00:00	SFP module inserted on port 1
7	Warning	2020-09-01T15:30:27+00:00	SFP module inserted on port 6
8	Info	2020-09-01T15:30:32+00:00	topologyChange
9	Warning	2020-09-01T15:30:33+00:00	Link up on port 29

Parameter descriptions:

Level : Select the level of the system log entry. The following level types are supported:

Emerg: The system log entry is emergency level.

Alert: The system log entry is alert level.

Crit: The system log entry is critical level.

Error: The system log entry is error level.

Warning: The system log entry is warning level.

Notice: The system log entry is notice level.

Info: The system log entry is information level.

Debug: The system log entry is debug level.

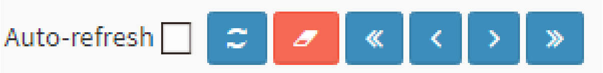
Clear Level :Select the level to clear at a Clear button operation. See Level description above.

ID : ID (instance number) of the system log entry.

Time : Displays the log record by device time. The date and time of the system log entry.

Message : It will display the log detail message. The message of the system log entry.

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. See “Clear Level” above.

<< : First entry; updates the system log entries, starting from the first available entry ID.

< : Previous entry; updates the system log entries, ending at the last entry currently displayed.

> : Next entry; updates the system log entries, starting from the last entry currently displayed.

>>: Last entry; updates the system log entries, ending at the last available entry ID.

Sample System Log Messages

ID	Level	Time	Message
2	Notice	2011-01-01T00:00:11+00:00	LINK-UPDOWN: Interface Vlan 1, changed state to down.
3	Warning	2011-01-01T00:00:12+00:00	SFP module inserted on port 20
4	Warning	2011-01-01T00:00:13+00:00	Switch just made a warm boot
5	Warning	2011-01-01T00:00:13+00:00	Link up on port 25
7	Warning	2011-01-01T00:00:14+00:00	Link up on port 20
10	Notice	2011-01-01T00:00:18+00:00	LINK-UPDOWN: Interface Vlan 1, changed state to up.
11	Warning	2011-01-01T00:00:22+00:00	FAN No: #2 FAN Failed, 0RPM
12	Warning	2011-01-01T00:00:25+00:00	FAN No: #2 FAN Recovered, 5273RPM

3-1.5 Detailed Log

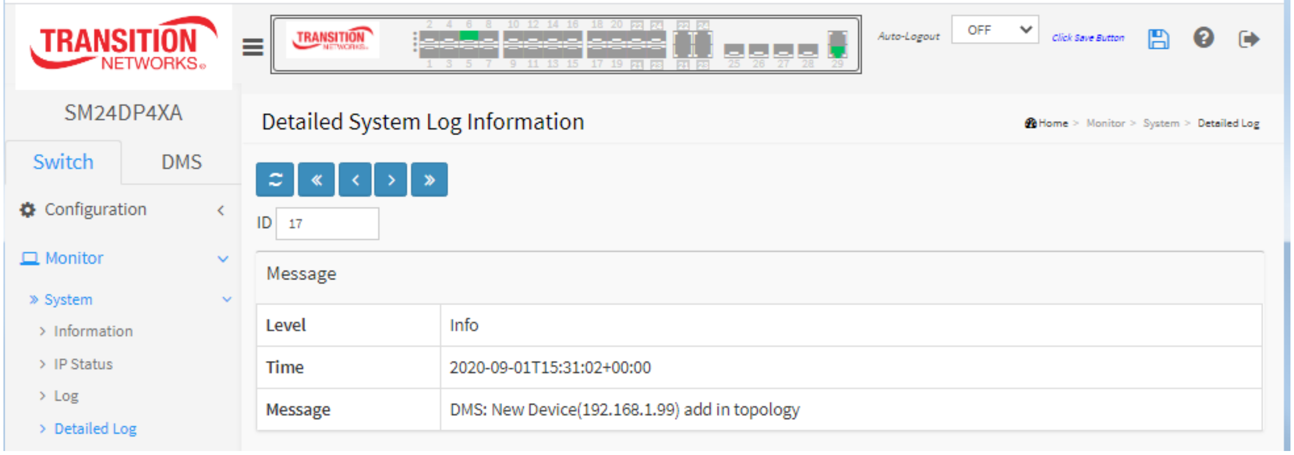
This page displays the detailed log information of the switch.

Web Interface

To display the detailed System Log via the web UI:

1. Click Monitor, System and Detailed Log.
2. View the log information.

Figure 3- 1.5: Detailed System Log Information



Detailed System Log Information

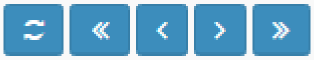
ID 17

Message	
Level	Info
Time	2020-09-01T15:31:02+00:00
Message	DMS: New Device(192.168.1.99) add in topology

Parameter descriptions:

ID : The ID (>= 1) of the system log entry.

Message : The detailed message of the system log entry.



Buttons

Refresh: Updates the system log entries, starting from the current entry ID.

<< : First entry; updates the system log entries, starting from the first available entry ID.

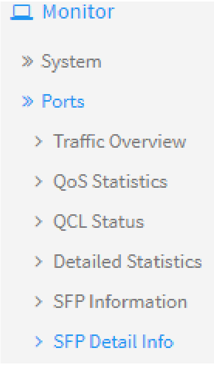
< : Previous entry; updates the system log entries, ending at the last entry currently displayed.

> : Next entry; updates the system log entries, starting from the last entry currently displayed.

>>: Last entry; updates the system log entries, ending at the last available entry ID.

3-2 Ports

This section lets you monitor various ports content or status information.



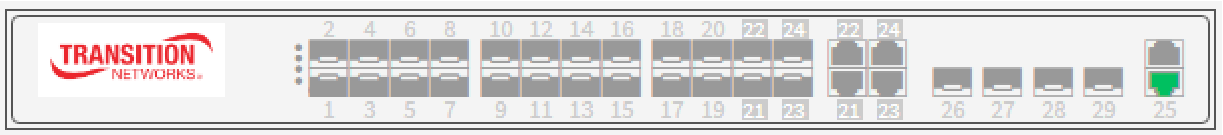
3-2.3.1 State

Each page provides an overview of the current switch port states.

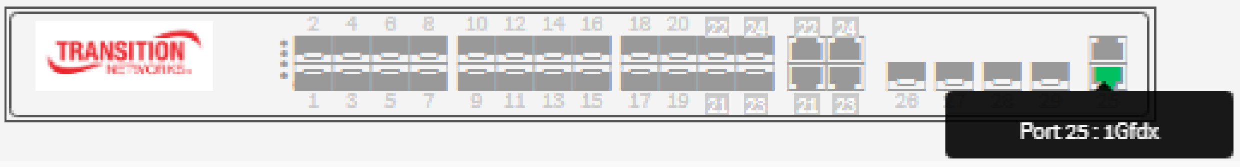
Web Interface

To display the Ports State in the Web UI:

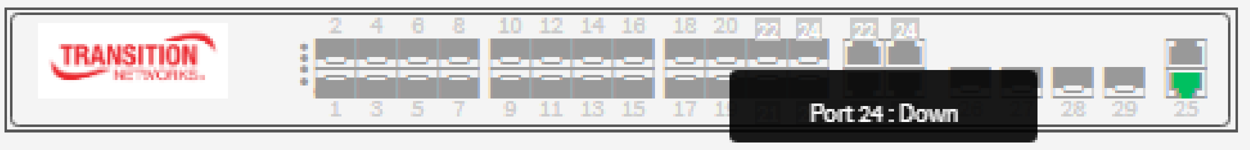
1. Click any page.
2. View the Port state overview.



3. Hover the cursor over any port to display its speed (if up) or status (if down).



Port 25 : 1Gfdx



Port 24 : Down

4. Right click an SFP port to display its specific SFP Information page.
5. Left click a copper port to display its Detailed Port Statistics page.
6. Click the browser back button to go back to the starting page.

The port states are shown below:

RJ45 ports	□	■	🟩
SFP ports	◻◻	◼◼	🟦🟦
State	Disabled	Down	Link

3-2.2 Traffic Overview

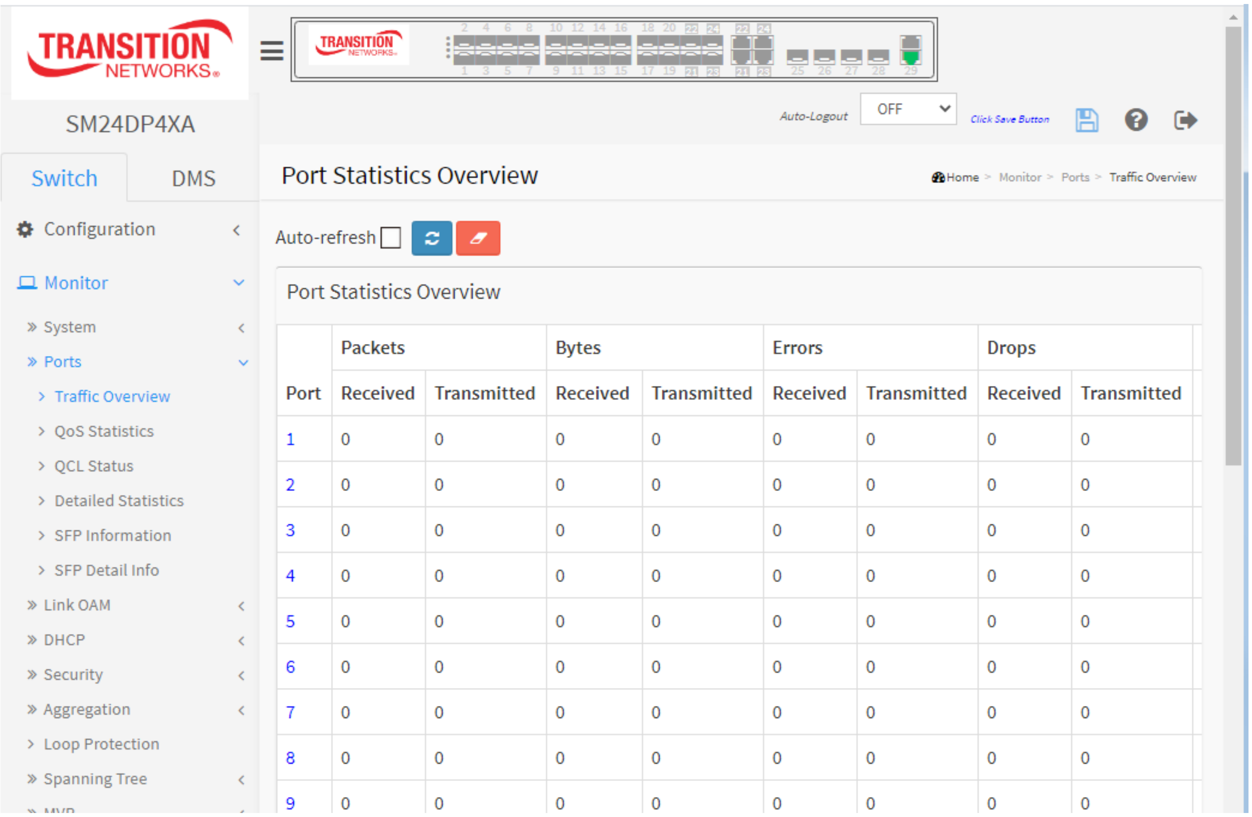
This page displays Port statistics information and an overview of traffic statistics for all switch ports.

Web Interface

To display the Port Statistics Overview in the web interface:

1. Click Monitor, Port, Traffic Overview.
2. Click Refresh to refresh the page immediately or clear all table information when you click Clear.
3. You can click a linked port number to display its Detailed Port Statistics page.

Figure 3-2.2: Port Statistics Overview



Port Statistics Overview

Auto-refresh □

Port Statistics Overview

	Packets		Bytes		Errors		Drops	
Port	Received	Transmitted	Received	Transmitted	Received	Transmitted	Received	Transmitted
1	0	0	0	0	0	0	0	0
2	0	0	0	0	0	0	0	0
3	0	0	0	0	0	0	0	0
4	0	0	0	0	0	0	0	0
5	0	0	0	0	0	0	0	0
6	0	0	0	0	0	0	0	0
7	0	0	0	0	0	0	0	0
8	0	0	0	0	0	0	0	0
9	0	0	0	0	0	0	0	0

Parameter descriptions:

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

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

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

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

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

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

Buttons

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

Refresh: Click to immediately refresh the page.

Clear : Click to clear the displayed statistics.

3-2.3 QoS Statistics

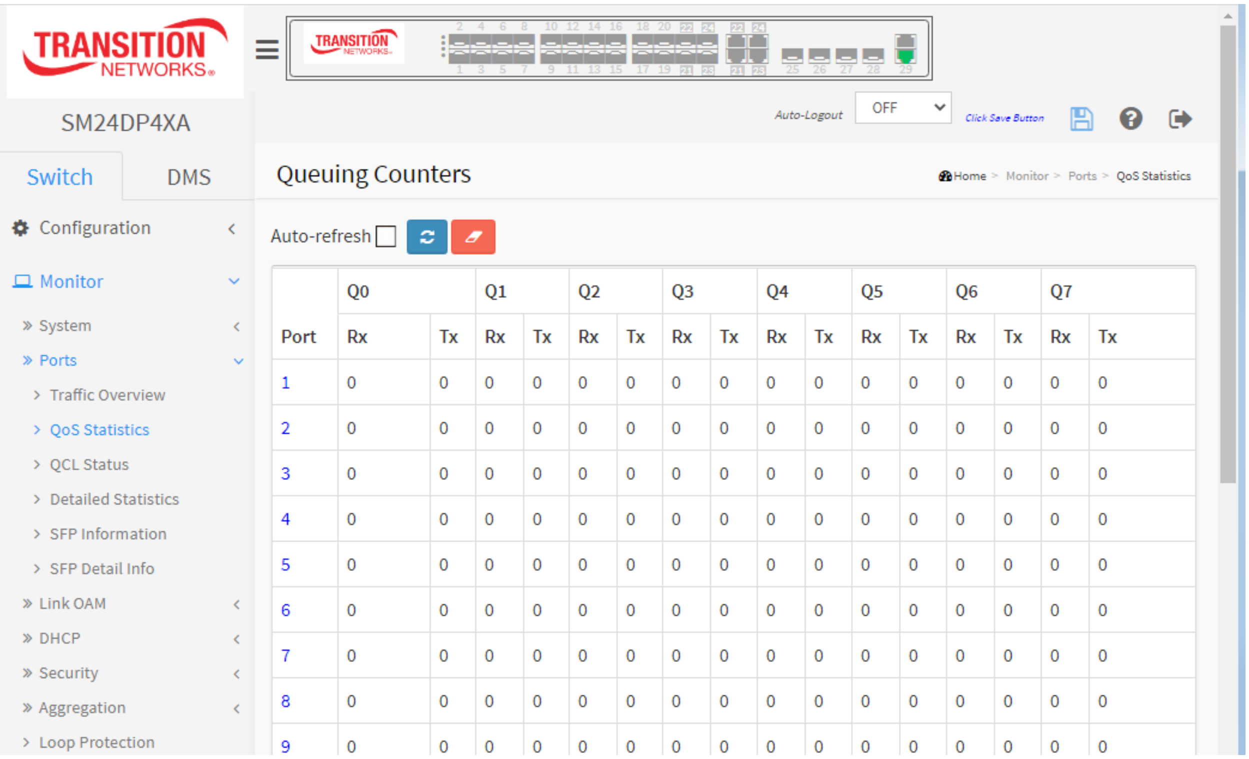
This page displays detailed QoS Queuing counters for the different queues for all switch ports.

Web Interface

To display the Queuing Counters via the web interface:

1. Click Monitor, Ports, then QoS Statistics.
2. View the displayed information.
3. Click Refresh to refresh the page or clear all information when you click Clear.

Figure 3-2.3: Queuing Counters Overview



Auto-Logout OFF

Queuing Counters

Auto-refresh □

	Q0		Q1		Q2		Q3		Q4		Q5		Q6		Q7	
Port	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

Parameter descriptions:

Port : The logical port for the settings contained in the same row. Click a linked port number to display its Detailed Statistics page.

Qn : Qn is the Queue number; there are 8 QoS queues per port. Q0 is the lowest priority queue.

Rx/Tx : The number of received and transmitted packets per queue.

Buttons

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

Refresh: Click to refresh the page.

Clear: Clears the counters for all ports.

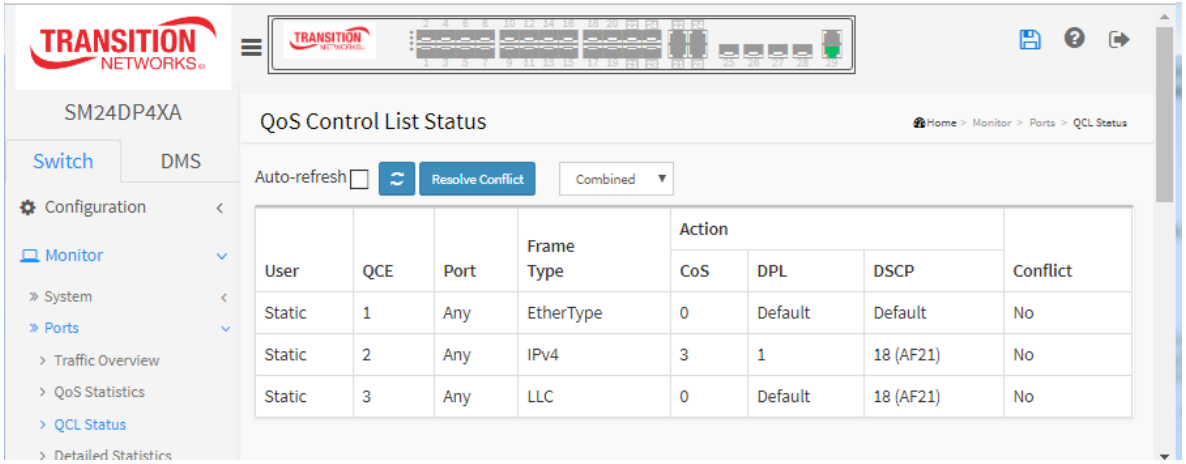
3-2.4 QCL Status

This page shows the QCL status by different QCL users. Each row describes the QCE that is defined. It is a conflict if a specific QCE is not applied to the hardware due to hardware limitations. The maximum number of QCEs is 256 on each switch.

To display the QoS Control List Status in the web interface:

1. Click Monitor, Ports, QCL Status.
2. At the User Select box, select the set of users to display (Static, Voice VLAN, DMS, Conflict, Combined).
3. Click the buttons as required.

Figure 3-2.4: QoS Control List Status



QoS Control List Status

Auto-refresh □ Combined

User	QCE	Port	Frame Type	Action			Conflict
				CoS	DPL	DSCP	
Static	1	Any	EtherType	0	Default	Default	No
Static	2	Any	IPv4	3	1	18 (AF21)	No
Static	3	Any	LLC	0	Default	18 (AF21)	No

User : Indicates the QCL user (e.g., Static).

QCE : Indicates the QCE ID.

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

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

Any: Match any frame type.

Ethernet: Match EtherType frames.

LLC: Match (LLC) frames.

SNAP: Match (SNAP) frames.

IPv4: Match IPv4 frames.

IPv6: Match IPv6 frames.

Action : Indicates the classification action taken on ingress frame if parameters configured are matched with the frame's content. Possible actions are:

CoS: Classify Class of Service.

DPL: Classify Drop Precedence Level.

DSCP: Classify DSCP value.

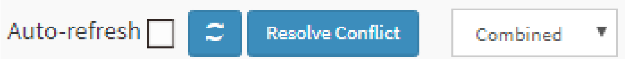
PCP: Classify PCP value.

DEI: Classify DEI value.

Policy: Classify ACL Policy number.

Conflict : Displays Conflict status of QCL entries. As H/W resources are shared by multiple applications. It may happen that resources required to add a QCE may not be available, in that case it shows conflict status as 'Yes', otherwise it is always 'No'. **Note** that conflict can be resolved by releasing the hardware resources required to add QCL entry on pressing 'Resolve Conflict' button.

Buttons

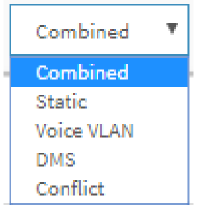


Auto-refresh: Check this box to refresh the page automatically every 3 seconds.

Resolve Conflict: Click to release the resources required to add QCL entry, incase conflict status for any QCL entry is 'yes'.

Refresh: Click to refresh the page.

User Select box : Select the set of users for which you want to view information on (Static, Voice VLAN, DMS, Conflict, or Combined).



3-2.5 Detailed Statistics

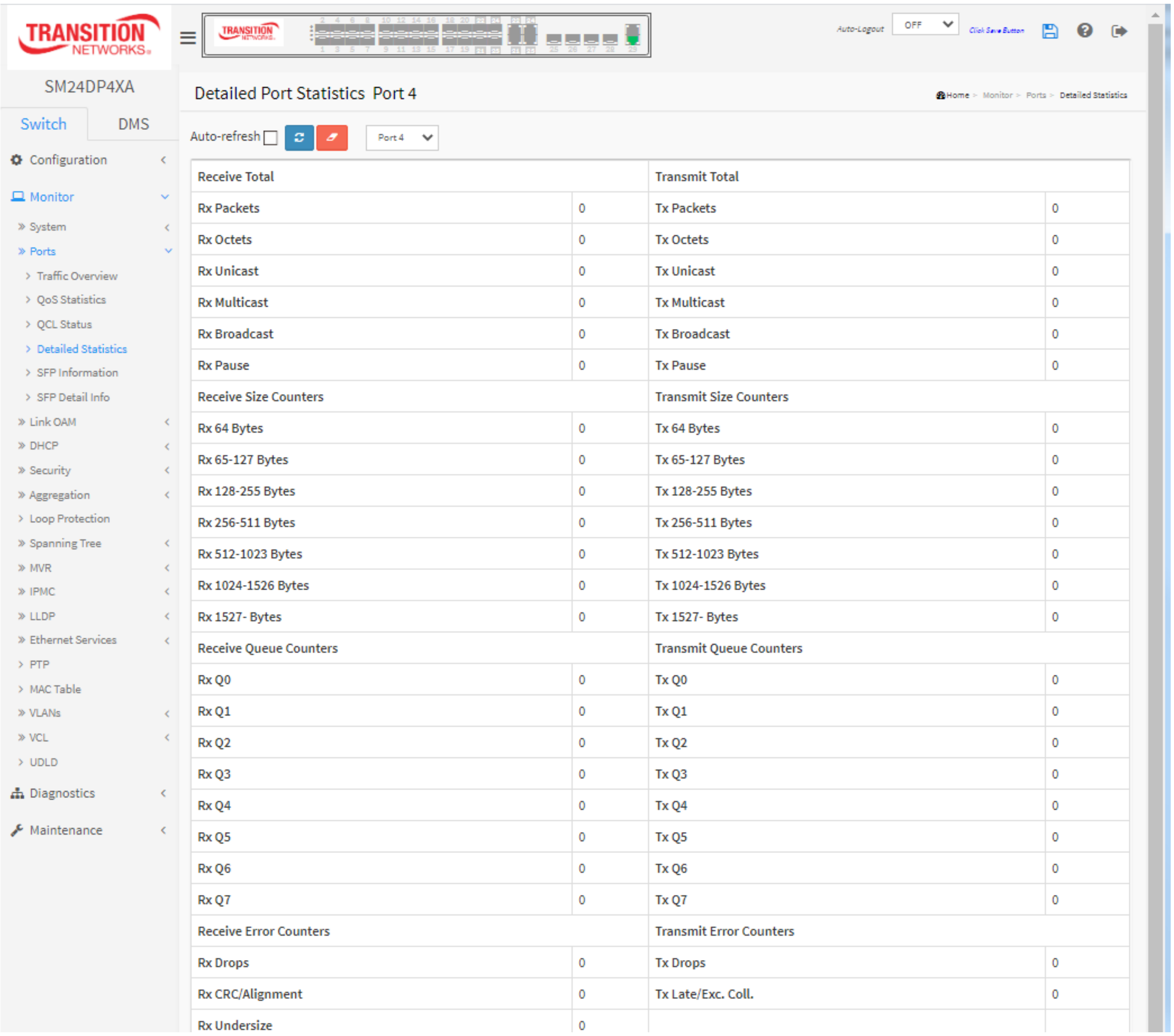
This page shows detailed traffic statistics for a specific switch port. Use the port select box to select which switch port details to display. The displayed counters are the totals for receive and transmit, the size counters for receive and transmit, and the error counters for receive and transmit.

Web Interface

To display the per-port detailed Statistics Overview in the web interface:

1. Click Monitor, Ports, then Detailed Statistics.
2. Scroll the Port Index to select which port you want to show the detailed Port statistics overview.
3. Click Refresh to refresh the port detailed statistics or clear all information when you click Clear.

Figure 3-2.5: Detailed Port Statistics



Detailed Port Statistics Port 4

Auto-refresh □ Port 4

Receive Total		Transmit Total	
Rx Packets	0	Tx Packets	0
Rx Octets	0	Tx Octets	0
Rx Unicast	0	Tx Unicast	0
Rx Multicast	0	Tx Multicast	0
Rx Broadcast	0	Tx Broadcast	0
Rx Pause	0	Tx Pause	0
Receive Size Counters		Transmit Size Counters	
Rx 64 Bytes	0	Tx 64 Bytes	0
Rx 65-127 Bytes	0	Tx 65-127 Bytes	0
Rx 128-255 Bytes	0	Tx 128-255 Bytes	0
Rx 256-511 Bytes	0	Tx 256-511 Bytes	0
Rx 512-1023 Bytes	0	Tx 512-1023 Bytes	0
Rx 1024-1526 Bytes	0	Tx 1024-1526 Bytes	0
Rx 1527- Bytes	0	Tx 1527- Bytes	0
Receive Queue Counters		Transmit Queue Counters	
Rx Q0	0	Tx Q0	0
Rx Q1	0	Tx Q1	0
Rx Q2	0	Tx Q2	0
Rx Q3	0	Tx Q3	0
Rx Q4	0	Tx Q4	0
Rx Q5	0	Tx Q5	0
Rx Q6	0	Tx Q6	0
Rx Q7	0	Tx Q7	0
Receive Error Counters		Transmit Error Counters	
Rx Drops	0	Tx Drops	0
Rx CRC/Alignment	0	Tx Late/Exc. Coll.	0
Rx Undersize	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.

Buttons

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

Clear: Clears the counters for the selected port.

Refresh: Click to refresh the page.

3-2.6 SFP Information

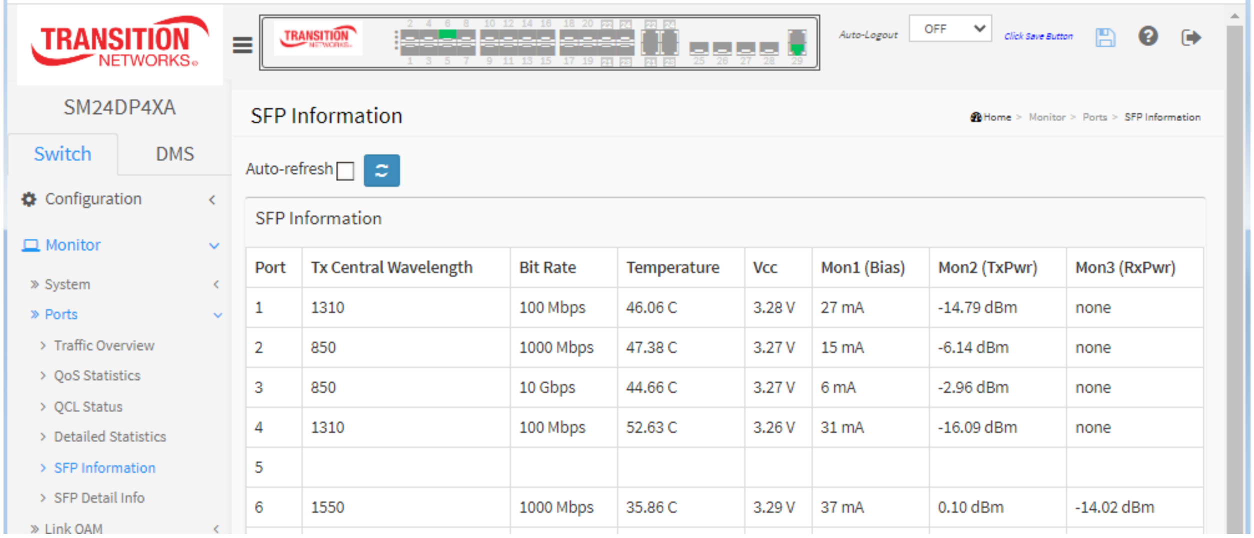
This page shows Information on SFPs in the system. This page displays general SFP information and monitoring information.

Web Interface

To display the per-port detailed Statistics Overview via the web interface:

1. Click Monitor, Ports, SFP Information.
2. View the displayed SFP information.
3. Click Auto-refresh or Refresh as required.

Figure 3-2.6: SFP Information



SFP Information

Auto-refresh □

SFP Information

Port	Tx Central Wavelength	Bit Rate	Temperature	Vcc	Mon1 (Bias)	Mon2 (TxPwr)	Mon3 (RxPwr)
1	1310	100 Mbps	46.06 C	3.28 V	27 mA	-14.79 dBm	none
2	850	1000 Mbps	47.38 C	3.27 V	15 mA	-6.14 dBm	none
3	850	10 Gbps	44.66 C	3.27 V	6 mA	-2.96 dBm	none
4	1310	100 Mbps	52.63 C	3.26 V	31 mA	-16.09 dBm	none
5							
6	1550	1000 Mbps	35.86 C	3.29 V	37 mA	0.10 dBm	-14.02 dBm

Parameter descriptions:

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

Tx Central Wavelength : Displays the nominal transmitter output wavelength in nm (e.g., *1550, 1310,* or *850* nanometers (nm).

Bit rate : Displays the nominal bit rate of the transceiver (e.g., *10 Gbps, 100 Mbps, 1000 Mbps, 10 Gbps*).

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 (e.g., *31.08 C*).

Vcc : Displays the internally measured transceiver supply voltage (e.g., *3.27 V*). Accuracy is vendor specific but must be better than 3% 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 spec for more detail.

Mon1 (Bias) : Displays the measured TX bias current in mA (e.g., *15 mA*). 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 dBm (e.g., *-6.82 dBm*). 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

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

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

3-2.7 SFP Detailed Info

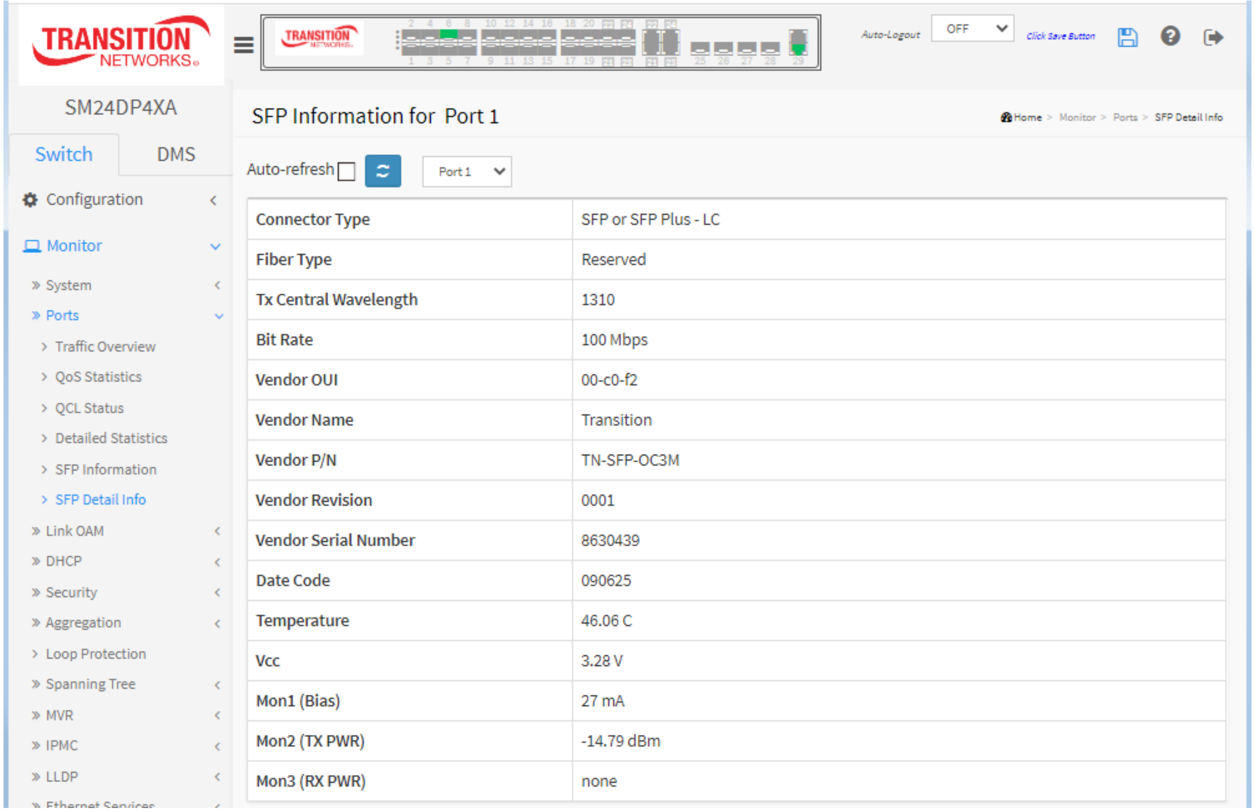
This page shows the details of a specified SFP. This page displays general SFP information and monitoring information.

Web Interface

To display the per-port detailed Statistics Overview via the web interface:

1. Click Monitor, Ports, SFP Information.
2. Use the port select box to select the desired SFP port number.
3. View the displayed SFP information.
4. Click Auto-refresh or Refresh as required.

Figure 3-2.7: SFP Information for Port 2



SFP Information for Port 1

Auto-refresh □ Port 1

Connector Type	SFP or SFP Plus - LC
Fiber Type	Reserved
Tx Central Wavelength	1310
Bit Rate	100 Mbps
Vendor OUI	00-c0-f2
Vendor Name	Transition
Vendor P/N	TN-SFP-OC3M
Vendor Revision	0001
Vendor Serial Number	8630439
Date Code	090625
Temperature	46.06 C
Vcc	3.28 V
Mon1 (Bias)	27 mA
Mon2 (TX PWR)	-14.79 dBm
Mon3 (RX PWR)	none

Parameter descriptions:

Connector Type : Displays the external optical or electrical cable connector provided as the media interface (e.g., *SFP or SFP Plus – LC*).

Fiber Type : Displays the fiber channel transmission media (e.g., *Reserved* or *Single Mode (SM)* or *Multi-mode (MM)*.

Tx Central Wavelength : Displays the nominal transmitter output wavelength in nm (e.g., *1550, 1310,* or *850* nanometers (nm).

Bit rate : Displays the nominal bit rate of the transceiver (e.g., *10 Gbps, 100 Mbps, 1000 Mbps, 10 Gbps*).

Vendor OUI : Displays the vendor IEEE company ID (e.g., *00-c0-f2*).

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-SFP-OC3S*, or *TN-10GSFP-LR8M*).

Vendor Revision : Displays the vendor¡¦s product revision (e.g., *1.0*)

Vendor Serial Number : Displays the vendor serial number for the transceiver (e.g., *TWFXPZ000*).

Date Code : Displays the vendor's manufacturing date code (e.g., *170508*).

Temperature : Displays the internally measured transceiver temperature (e.g., *31.08 C*). 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 (e.g., *3.27 V*). Accuracy is vendor specific but must be better than 3 % 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 spec for details.

Mon1 (Bias) : Displays the measured TX bias current in mA (e.g., *82 mA*). Accuracy is vendor specific but must be better than 10 % of the manufacturer's nominal value over specified operating temperature and voltage.

Mon2 (TX PWR) : Displays the measured coupled TX output power in mW (e.g., **1.86 dBm**). 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 (e.g., *none*). 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

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

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

Port select box : Select the port to display its SFP details.

3-3 Link OAM

3-3.1 Detailed Link OAM Statistics

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

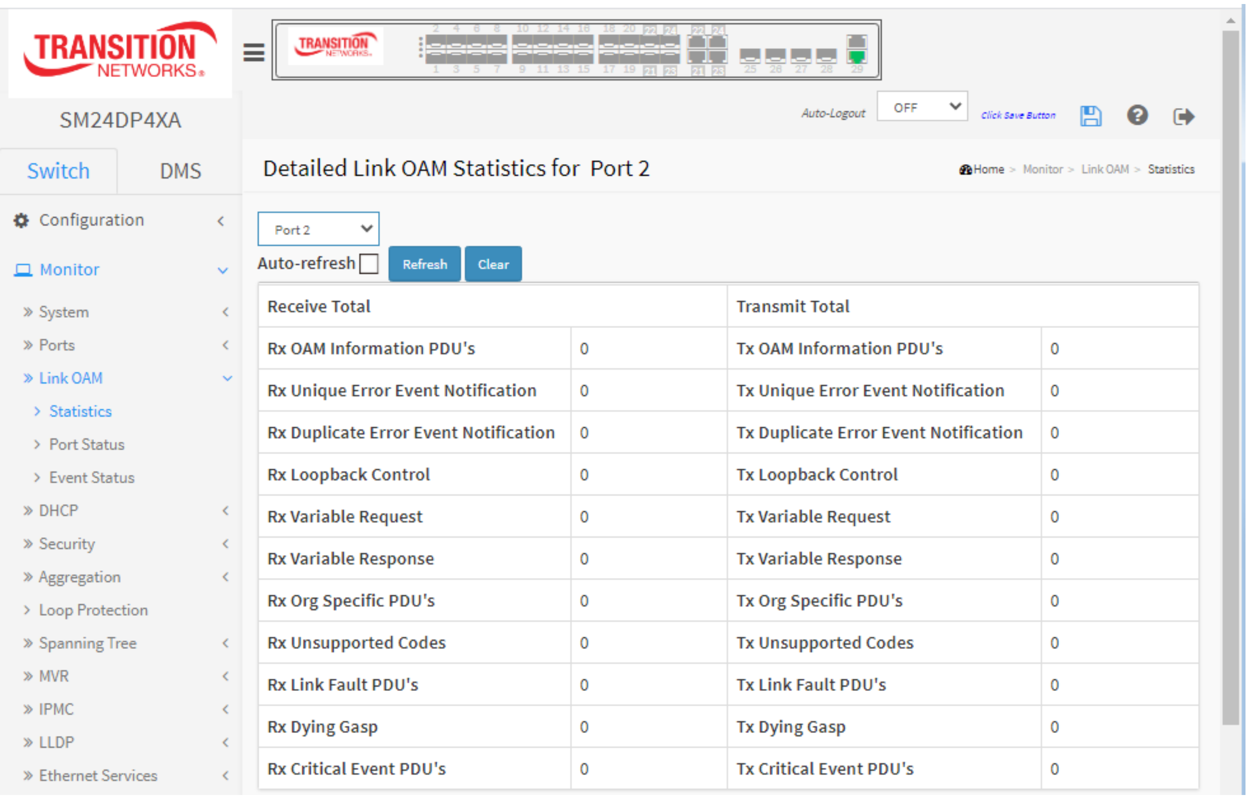
The displayed counters represent the total number of OAM frames received and transmitted for the selected port. Discontinuities of these counters can occur at re-initialization of the management system.

Web Interface

To display the per Port detailed Statistics Overview in the web interface:

1. Click Monitor, Link OAM, and Statistics.
2. Use the Port select dropdown to select the Port to show detailed LOAM statistics on.
3. View the displayed statistics.
4. Click Auto-refresh, Refresh, or Clear as required.

Figure 3-3.1: Detailed Link OAM Statistics for Port 2



Detailed Link OAM Statistics for Port 2

Port 2

Auto-refresh □ Refresh Clear

Receive Total		Transmit Total	
Rx OAM Information PDU's	0	Tx OAM Information PDU's	0
Rx Unique Error Event Notification	0	Tx Unique Error Event Notification	0
Rx Duplicate Error Event Notification	0	Tx Duplicate Error Event Notification	0
Rx Loopback Control	0	Tx Loopback Control	0
Rx Variable Request	0	Tx Variable Request	0
Rx Variable Response	0	Tx Variable Response	0
Rx Org Specific PDU's	0	Tx Org Specific PDU's	0
Rx Unsupported Codes	0	Tx Unsupported Codes	0
Rx Link Fault PDU's	0	Tx Link Fault PDU's	0
Rx Dying Gasp	0	Tx Dying Gasp	0
Rx Critical Event PDU's	0	Tx Critical Event PDU's	0

Receive Total and Transmit Total

Rx and Tx OAM Information PDU's : The number of received and transmitted OAM Information PDU's. Discontinuities of this counter can occur at re-initialization of the management system.

Rx and Tx Unique Error Event Notification : A count of the number of unique Event OAMPDUs received and transmitted on this interface. Event Notifications may be sent in duplicate to increase the probability of successfully being received, given the possibility that a frame may be lost in transit. Duplicate Event Notification transmissions are counted by Duplicate Event Notification counters for Tx and Rx respectively. A unique Event Notification OAMPDU is indicated as an Event Notification OAMPDU with a

Sequence Number field that is distinct from the previously transmitted Event Notification OAMPDU Sequence Number.

Rx and Tx Duplicate Error Event Notification : A count of the number of duplicate Event OAMPDUs received and transmitted on this interface. Event Notification OAMPDUs may be sent in duplicate to increase the probability of successfully being received, given the possibility that a frame may be lost in transit. A duplicate Event Notification OAMPDU is indicated as an Event Notification OAMPDU with a Sequence Number field that is identical to the previously transmitted Event Notification OAMPDU Sequence Number.

Rx and Tx Loopback Control : A count of the number of Loopback Control OAMPDUs received and transmitted on this interface.

Rx and Tx Variable Request : A count of the number of Variable Request OAMPDUs received and transmitted on this interface.

Rx and Tx Variable Response : A count of the number of Variable Response OAMPDUs received and transmitted on this interface.

Rx and Tx Org Specific PDU's : A count of the number of Organization Specific OAMPDUs transmitted on this interface.

Rx and Tx Unsupported Codes : A count of the number of OAMPDUs transmitted on this interface with an unsupported op-code.

Rx and Tx Link fault PDU's : A count of the number of Link fault PDU's received and transmitted on this interface.

Rx and Tx Dying Gasp : A count of the number of Dying Gasp events received and transmitted on this interface.

Rx and Tx Critical Event PDU's : A count of the number of Critical event PDU's received and transmitted on this interface.

Buttons

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

Refresh: Click to refresh the page.

Clear: Clears the counters for the selected port.

3-3.2 Detailed Link OAM Status

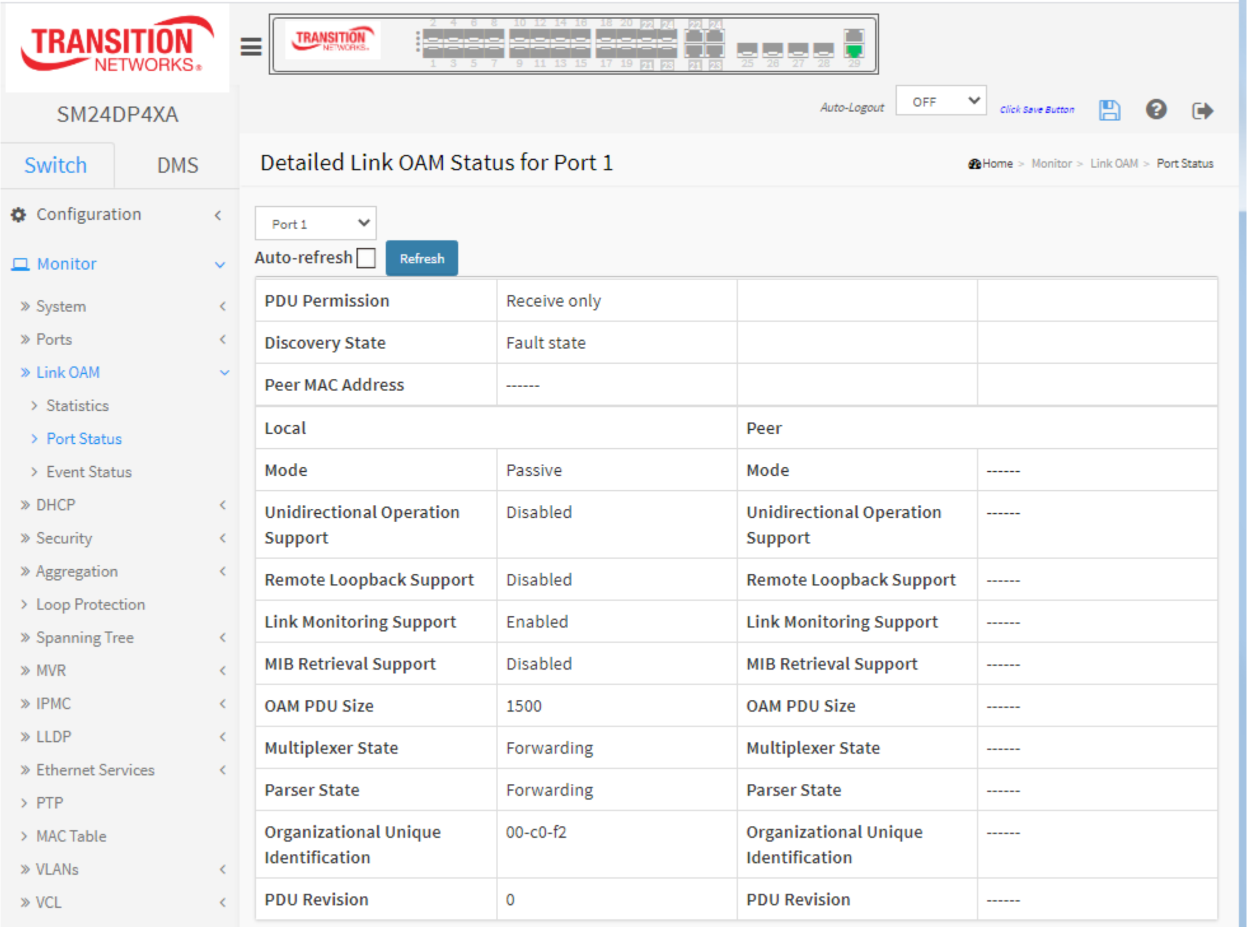
This page provides Link OAM configuration operational status. The displayed fields show the active configuration status for the selected port.

Web Interface

To display the per-port detailed Statistics Overview in the web interface:

1. Click Monitor, Link OAM, and Port Status.
2. Select the Port for which you want to show the status.
3. View the displayed status.
4. Click Auto-refresh, Refresh, or Clear as required.

Figure 3-3.2: Detailed Link OAM Status for Port 1



Detailed Link OAM Status for Port 1

Port 1

Auto-refresh □ Refresh

PDU Permission	Receive only		
Discovery State	Fault state		
Peer MAC Address	------		
Local		Peer	
Mode	Passive	Mode	------
Unidirectional Operation Support	Disabled	Unidirectional Operation Support	------
Remote Loopback Support	Disabled	Remote Loopback Support	------
Link Monitoring Support	Enabled	Link Monitoring Support	------
MIB Retrieval Support	Disabled	MIB Retrieval Support	------
OAM PDU Size	1500	OAM PDU Size	------
Multiplexer State	Forwarding	Multiplexer State	------
Parser State	Forwarding	Parser State	------
Organizational Unique Identification	00-c0-f2	Organizational Unique Identification	------
PDU Revision	0	PDU Revision	------

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

Discovery State : Displays the current state of the discovery process. Possible states are Fault state, Active state, Passive state,SEND_LOCAL_REMOTE_STATE, SEND_ANY_STATE, SEND_LOCAL_REMOTE_OK_STATE.

Peer MAC Address : Displays the MAC address of the peer device or “------” if none is available.

Local and Peer

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

Unidirectional Operation Support : This feature is not available to be configured by the user. The status of this configuration is retrieved from the PHY.

Remote Loopback Support : If status is enabled, DTE is capable of OAM remote loopback mode.

Link Monitoring Support : If status is enabled, DTE supports interpreting Link Events.

MIB Retrieval Support : If status is enabled DTE supports sending Variable Response OAMPDUs.

OAM PDU Size : Represents the largest OAMPDU, in octets, supported by the DTE. This value is compared to the remotes Maximum PDU Size and the smaller of the two is used.

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

Parser State : When in forwarding state, Device is forwarding non-OAMPDUs to higher sublayer. When in loopback, Device is looping back non-OAMPDUs to the lower sublayer. When in discarding state, Device is discarding non-OAMPDUs.

Organizational Unique Identification : 24-bit Organizationally Unique Identifier of the vendor.

PDU Revision : It indicates the current revision of the Information TLV. The value of this field shall start at zero and be incremented each time something in the Information TLV changes. Upon reception of an Information TLV from a peer, an OAM client may use this field to decide if it needs to be processed (an Information TLV that is identical to the previous Information TLV doesn't need to be parsed as nothing in it has changed).

Buttons

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

Refresh: Click to refresh the page immediately.

3-3.3 Detailed Link OAM Link (Event) Status

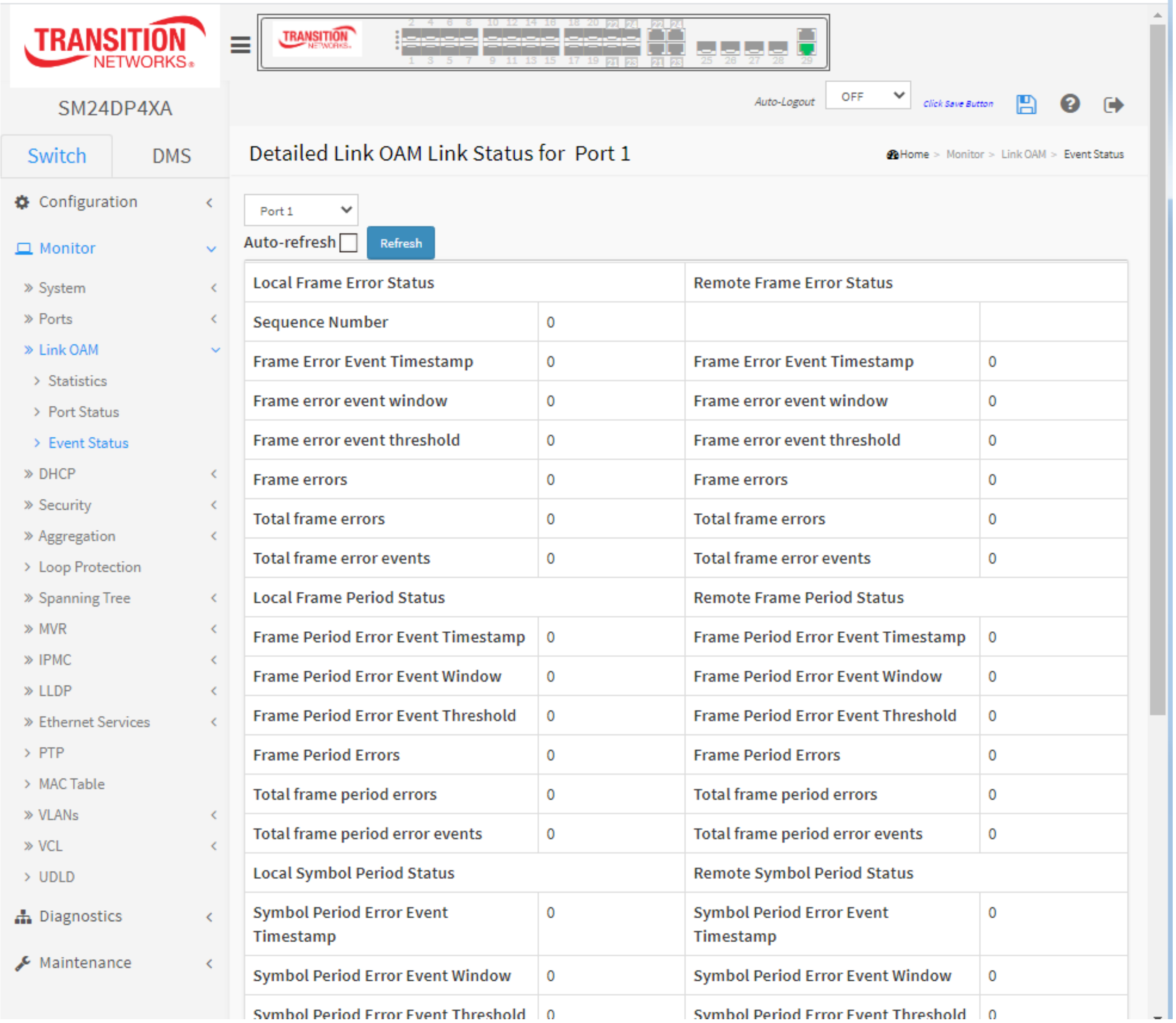
This page displays the current Link OAM Link Event parameters. The left pane displays the Event status for the Local OAM unit while the right pane displays the status for the Peer for the respective port.

Web Interface

To display the per-port detailed Status via the web interface:

1. Click Monitor, Link OAM, Event Status.
2. At the port select box, select the Port for which you want to view the detailed status.
3. View the displayed status.
4. Click Auto-refresh, Refresh, or Clear as required.

Figure 3-3.3: Detailed Link OAM Link Status for Port 1



Detailed Link OAM Link Status for Port 1

Local Frame Error Status		Remote Frame Error Status	
Sequence Number	0		
Frame Error Event Timestamp	0	Frame Error Event Timestamp	0
Frame error event window	0	Frame error event window	0
Frame error event threshold	0	Frame error event threshold	0
Frame errors	0	Frame errors	0
Total frame errors	0	Total frame errors	0
Total frame error events	0	Total frame error events	0
Local Frame Period Status		Remote Frame Period Status	
Frame Period Error Event Timestamp	0	Frame Period Error Event Timestamp	0
Frame Period Error Event Window	0	Frame Period Error Event Window	0
Frame Period Error Event Threshold	0	Frame Period Error Event Threshold	0
Frame Period Errors	0	Frame Period Errors	0
Total frame period errors	0	Total frame period errors	0
Total frame period error events	0	Total frame period error events	0
Local Symbol Period Status		Remote Symbol Period Status	
Symbol Period Error Event Timestamp	0	Symbol Period Error Event Timestamp	0
Symbol Period Error Event Window	0	Symbol Period Error Event Window	0
Symbol Period Error Event Threshold	0	Symbol Period Error Event Threshold	0

<u>**Local Frame Error Status and Remote Frame Error Status**</u>

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

Frame Error Event Timestamp : Two-octet field indicates the time reference when the event was generated, in 100 ms intervals.

Frame error event window : This two-octet field indicates the duration of the period in 100 ms intervals.

1) The default value is one second.
2) The lower bound is one second.
3) The upper bound is one minute.

Frame error event threshold : This four-octet field indicates the number of detected errored frames in the period is required to be equal to or greater than in order for the event to be generated.

1) The default value is one frame error.
2) The lower bound is zero frame errors.
3) The upper bound is unspecified.

Frame errors : This four-octet field indicates the number of detected errored frames in the period.

Total frame errors : This eight-octet field indicates the sum of errored frames that have been detected since the OAM sublayer was reset.

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

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

Frame Period Error Event Window : This four-octet field indicates the duration of period in terms of frames.

Frame Period Error Event Threshold : This four-octet field indicates the number of errored frames in the period is required to be equal to or greater than in order for the event to be generated.

Frame Period Errors : This four-octet field indicates the number of frame errors in the period.

Total frame period errors : This eight-octet field indicates the sum of frame errors that have been detected since the OAM sublayer was reset.

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

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

Symbol Period Error Event Window : This eight-octet field indicates the number of symbols in the period.

Symbol Period Error Event Threshold : This eight-octet field indicates the number of errored symbols in the period is required to be equal to or greater than in order for the event to be generated.

Symbol Period Errors : This eight-octet field indicates the number of symbol errors in the period.

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

Symbol frame period error events : This two-octet field indicates the number of errored frame seconds in the period, encoded as a 16-bit unsigned integer.

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

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

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

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

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

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

Buttons

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

Refresh: Click to refresh the page.

3-4 DHCP

3-4.1 Server

A DHCP Server is used to allocate network addresses and deliver configuration parameters to dynamically configured hosts called DHCP clients.

3-4.1.1 Statistics

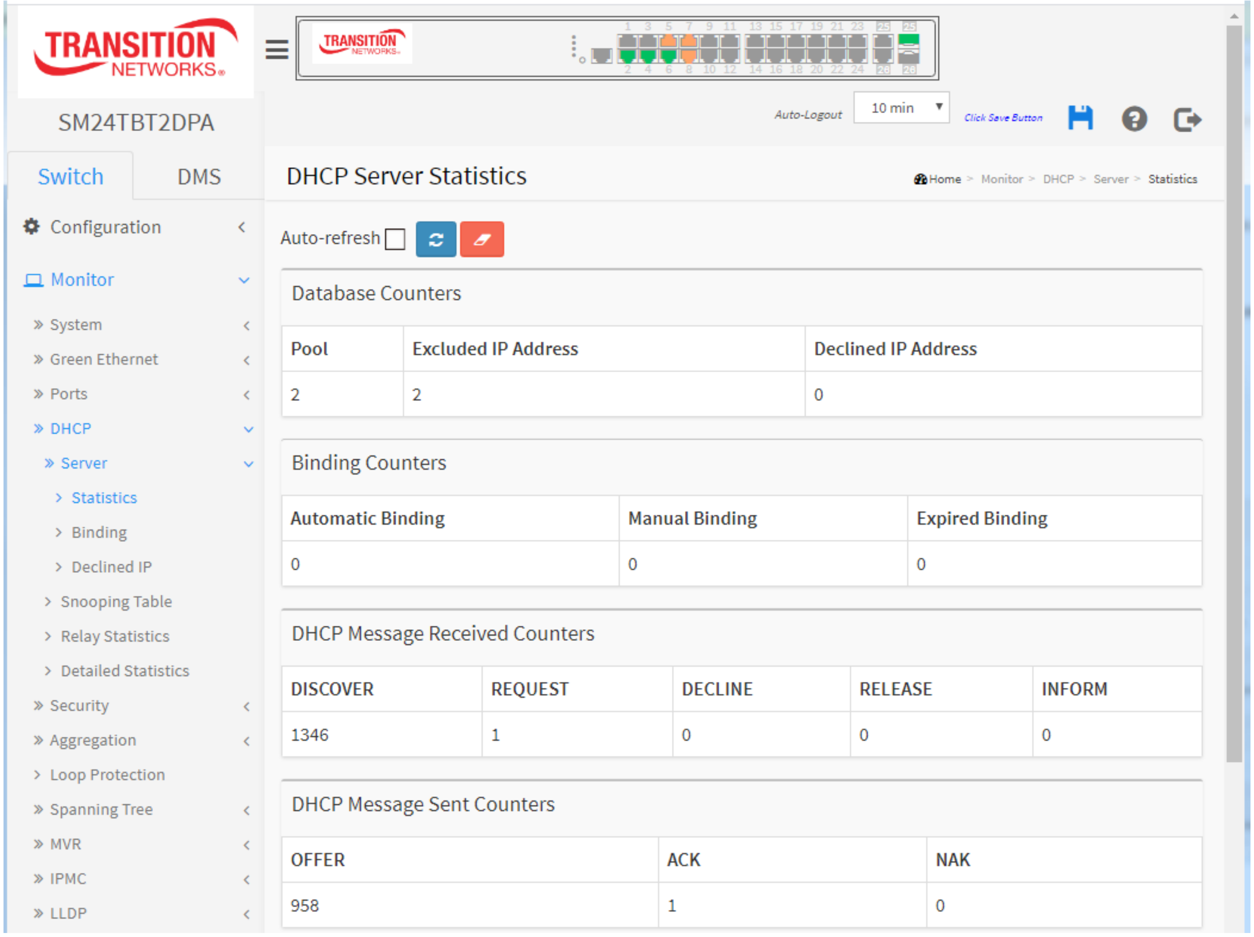
This page displays the database counters and the number of DHCP messages sent and received by the DHCP server.

Web Interface

To display the DHCP server Statistics Overview in the web interface:

1. Click Monitor, DHCP, Server, Statistics.
2. View the displayed statistics.
3. Use the Auto-refresh, Refresh, and Clear icons as desired.

Figure 3-4.1.1: DHCP Server Statistics



DHCP Server Statistics

Database Counters

Pool	Excluded IP Address	Declined IP Address
2	2	0

Binding Counters

Automatic Binding	Manual Binding	Expired Binding
0	0	0

DHCP Message Received Counters

DISCOVER	REQUEST	DECLINE	RELEASE	INFORM
1346	1	0	0	0

DHCP Message Sent Counters

OFFER	ACK	NAK
958	1	0

Parameter descriptions:

Database Counters

Pool : Number of pools.

Excluded IP Address : Number of excluded IP address ranges.

Declined IP Address : Number of sec lined 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.

Clear : Click to clear the DHCP Message Received Counters and DHCP Message Sent Counters.

3-4.1.2 Binding

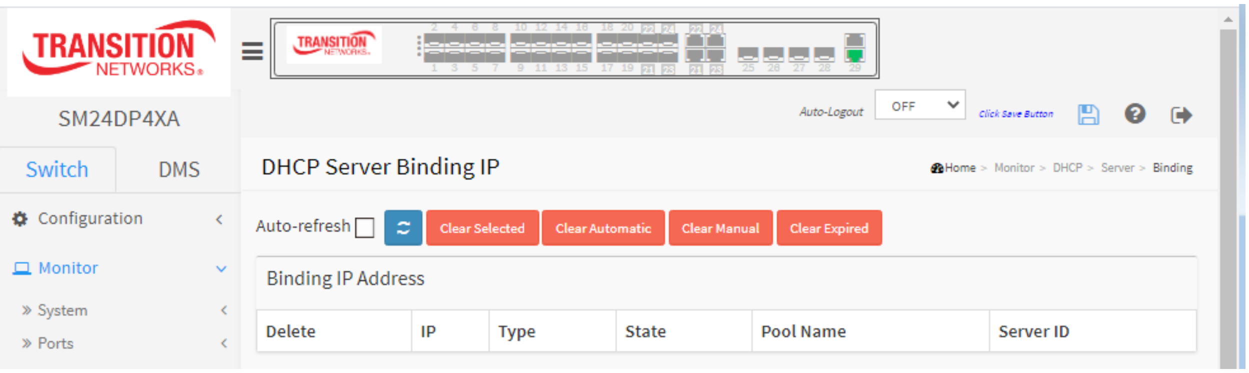
This page displays bindings generated for DHCP clients. A binding is a collection of configuration parameters, including at least an IP address, associated with or "bound to" a DHCP client. Bindings are managed by DHCP servers.

Web Interface

To display DHCP Server Binding IP in the web interface:

1. Click Monitor, DHCP, Server, and Binding.
2. View the displayed information.
3. Use the various buttons as required.

Figure 3-4.1.2: DHCP Server Binding IP



Binding IP Address

Delete	IP	Type	State	Pool Name	Server ID

Parameter descriptions:

IP : IP address allocated to DHCP client.

Type : Type of binding (Automatic, Manual, or Expired).

State : State of binding (Committed, Allocated, or Expired).

Pool Name : The pool that generated 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.

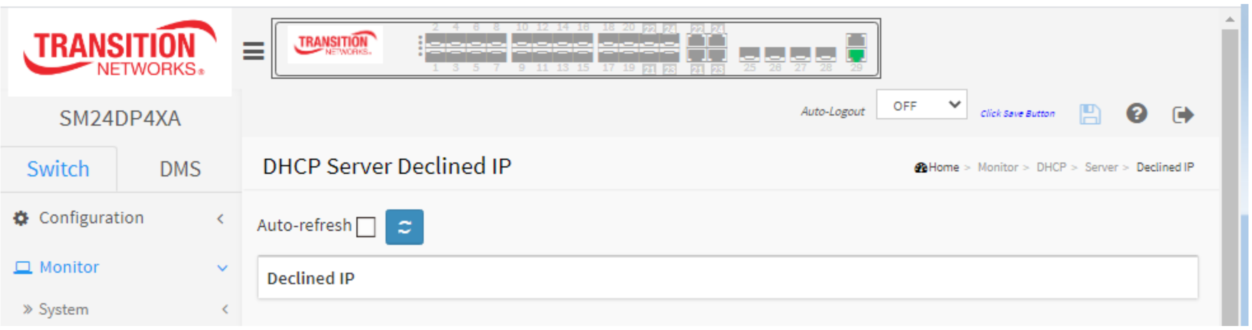
3-4.1.3 Declined IP

This page displays IP addresses declined by DHCP clients.

Web Interface

To display DHCP Server Declined IP in the web interface:

1. Click Monitor, DHCP, Server and Declined IP.
2. View the displayed information.
3. Click the Auto-refresh and Refresh buttons as required.



DHCP Server Declined IP

Auto-refresh □

Declined IP

Figure 3-4.1.3: Declined IP

Parameter descriptions:

Declined IP : List of IP addresses declined.

Buttons

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

Refresh : Click to refresh the page immediately.

3-4.2 Snooping Table

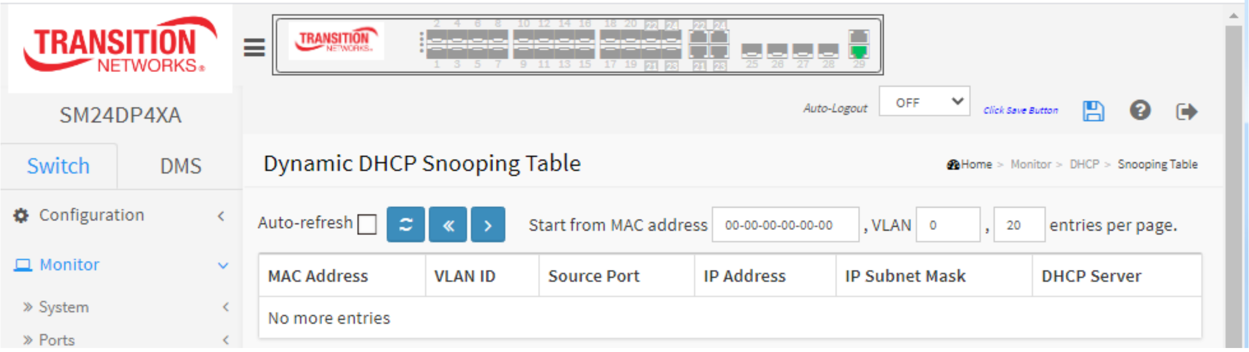
This page display the dynamic IP assigned information after DHCP Snooping mode is disabled. All DHCP clients obtained the dynamic IP address from the DHCP server will be listed in this table except for local VLAN interface IP addresses. Entries in the Dynamic DHCP Snooping Table are shown on this page.

Web Interface

To monitor the DHCP snooping table via the web interface:

1. Click Monitor, DHCP, and Snooping table.
2. Set the Start from MAC address, VLAN, and entries per page.
3. Use the various buttons as required.

Figure 3-4.2: Dynamic DHCP Snooping Table



Dynamic DHCP Snooping Table

Auto-refresh □ Start from MAC address 00-00-00-00-00-00 , VLAN 0 , 20 entries per page.

MAC Address	VLAN ID	Source Port	IP Address	IP Subnet Mask	DHCP Server
No more entries					

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: 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.

3-4.3 Relay Statistics

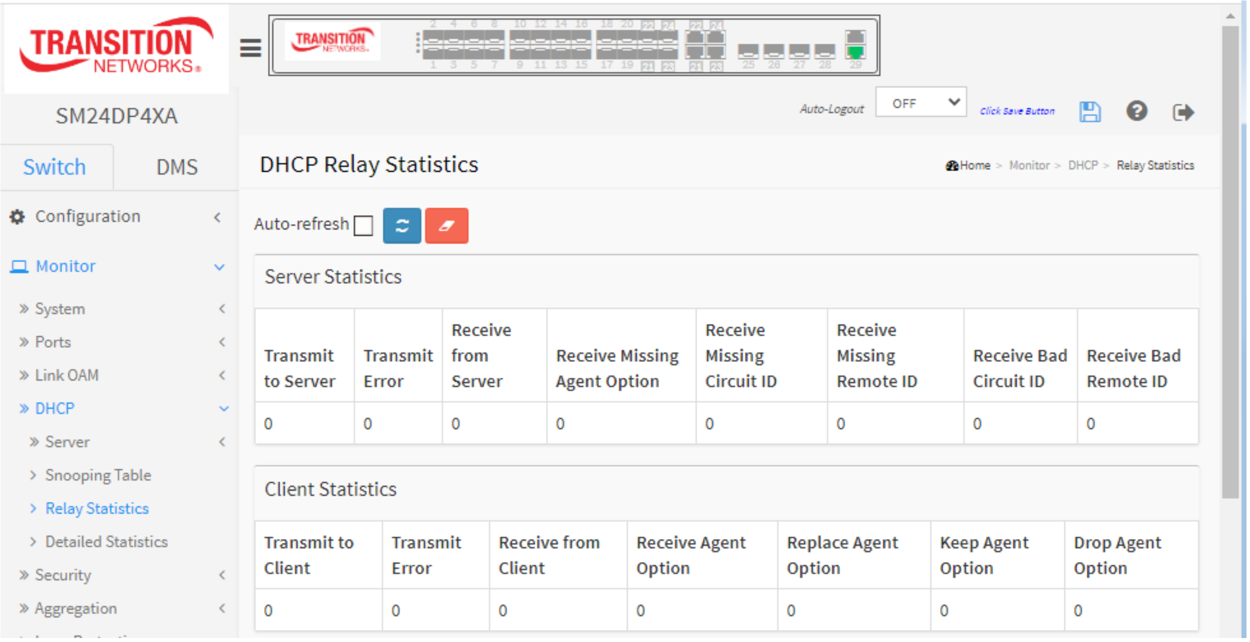
This page provides statistics for DHCP relay.

Web Interface

To monitor a DHCP Relay statistics in the web interface:

1. Click Monitor, DHCP, Relay Statistics.
2. View the displayed information.
3. Use the various buttons as required.

Figure 3-4.3: DHCP Relay Statistics



DHCP Relay Statistics

Auto-refresh □

Server Statistics

Transmit to Server	Transmit Error	Receive from Server	Receive Missing Agent Option	Receive Missing Circuit ID	Receive Missing Remote ID	Receive Bad Circuit ID	Receive Bad Remote ID
0	0	0	0	0	0	0	0

Client Statistics

Transmit to Client	Transmit Error	Receive from Client	Receive Agent Option	Replace Agent Option	Keep Agent Option	Drop Agent Option
0	0	0	0	0	0	0

Parameter descriptions:

<u>**Server Statistics**</u>

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.

<u>**Client Statistics**</u>

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: Refreshes the displayed table starting from the input fields.

Clear : Flushes all dynamic entries.

3-4.4 Detailed Statistics

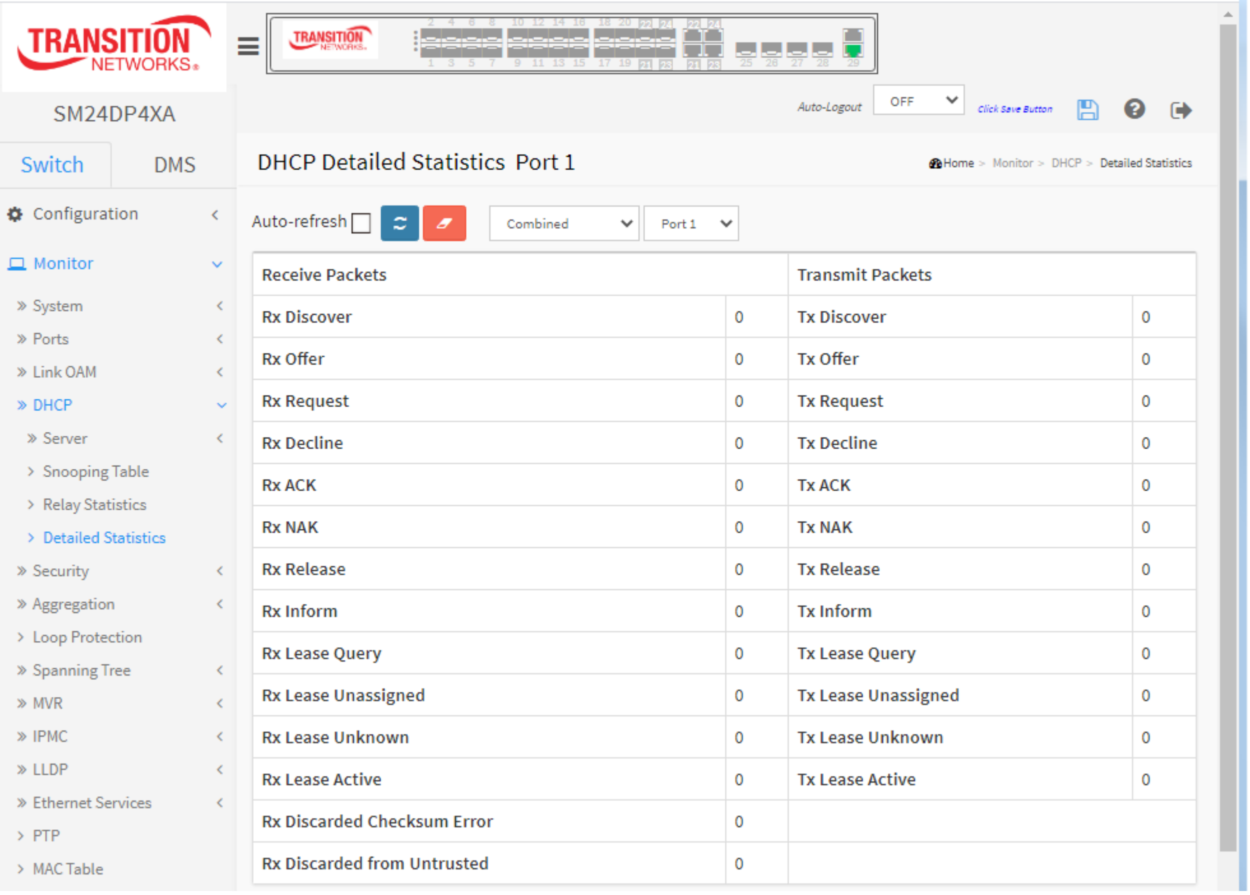
This page provides statistics for DHCP snooping. Notice that the normal forward per-port TX statistics isn't increased if the incoming DHCP packet is done by L3 forwarding mechanism. And clear the statistics on specific port may not take effect on global statistics since it gathers the different layer overview.

Web Interface

To monitor a DHCP Relay statistics in the web interface:

1. Click Monitor, DHCP, Detailed Statistics.
2. View the displayed information.
3. Use the various buttons as required.

Figure 3-4.4: DHCP Detailed Statistics for Port 1



DHCP Detailed Statistics Port 1

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.

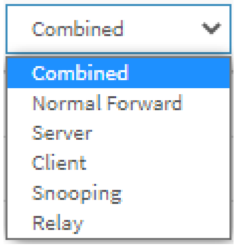
Rx and Tx Lease Active: The number of lease active (option 53 with value 13) packets received and transmitted.

Rx Discarded checksum error: The number of discard packet that IP/UDP checksum is error.

Rx Discarded from Untrusted: The number of discarded packets that are coming from untrusted port.

Buttons

: DHCP user select box lets you select which user’s statistics to display.



: Port select box set which port’s statistics are to be displayed.

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.

3-5 Security

3-5.1 Access Management Statistics

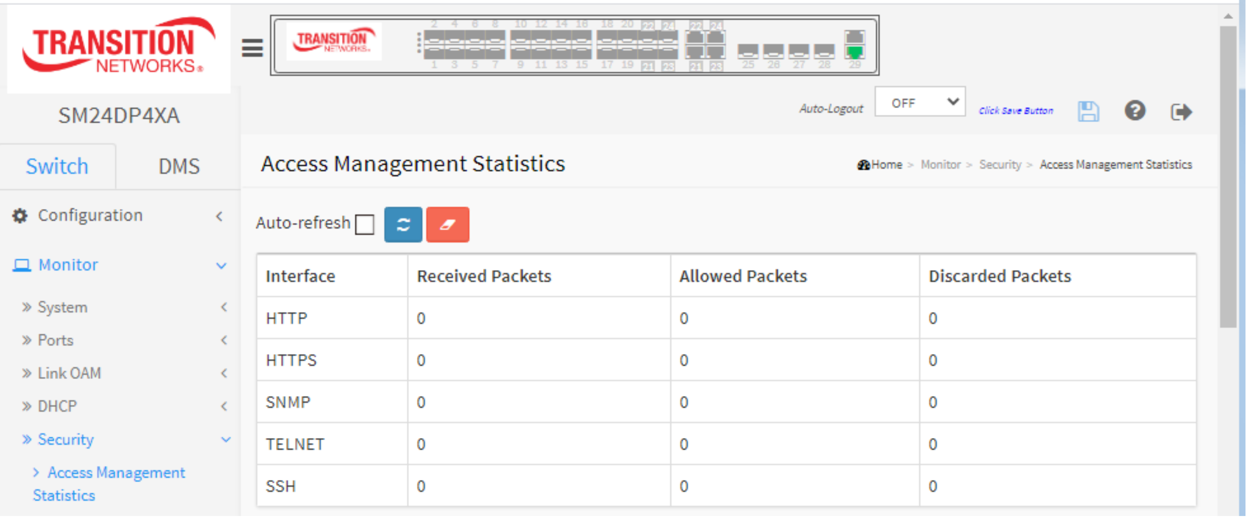
This page shows detailed statistics of the Access Management interfaces, including HTTP, HTTPS, SNMP, TELNET, and SSH.

Web Interface

To configure an Assess Management Statistics in the web interface:

1. Click Monitor, Security, Access Management Statistics.
2. View the displayed information.
3. Use the various buttons as required.

Figure 3-5.1: Access Management Statistics



Access Management Statistics

Interface	Received Packets	Allowed Packets	Discarded Packets
HTTP	0	0	0
HTTPS	0	0	0
SNMP	0	0	0
TELNET	0	0	0
SSH	0	0	0

Parameter descriptions:

Interface : The interface type through which the remote host can access the switch (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 refresh the page.

Clear: Clears the counters for the selected port.

3-5.2 Network

3-5.2.1 Port Security

3-6.2.1.1 Switch

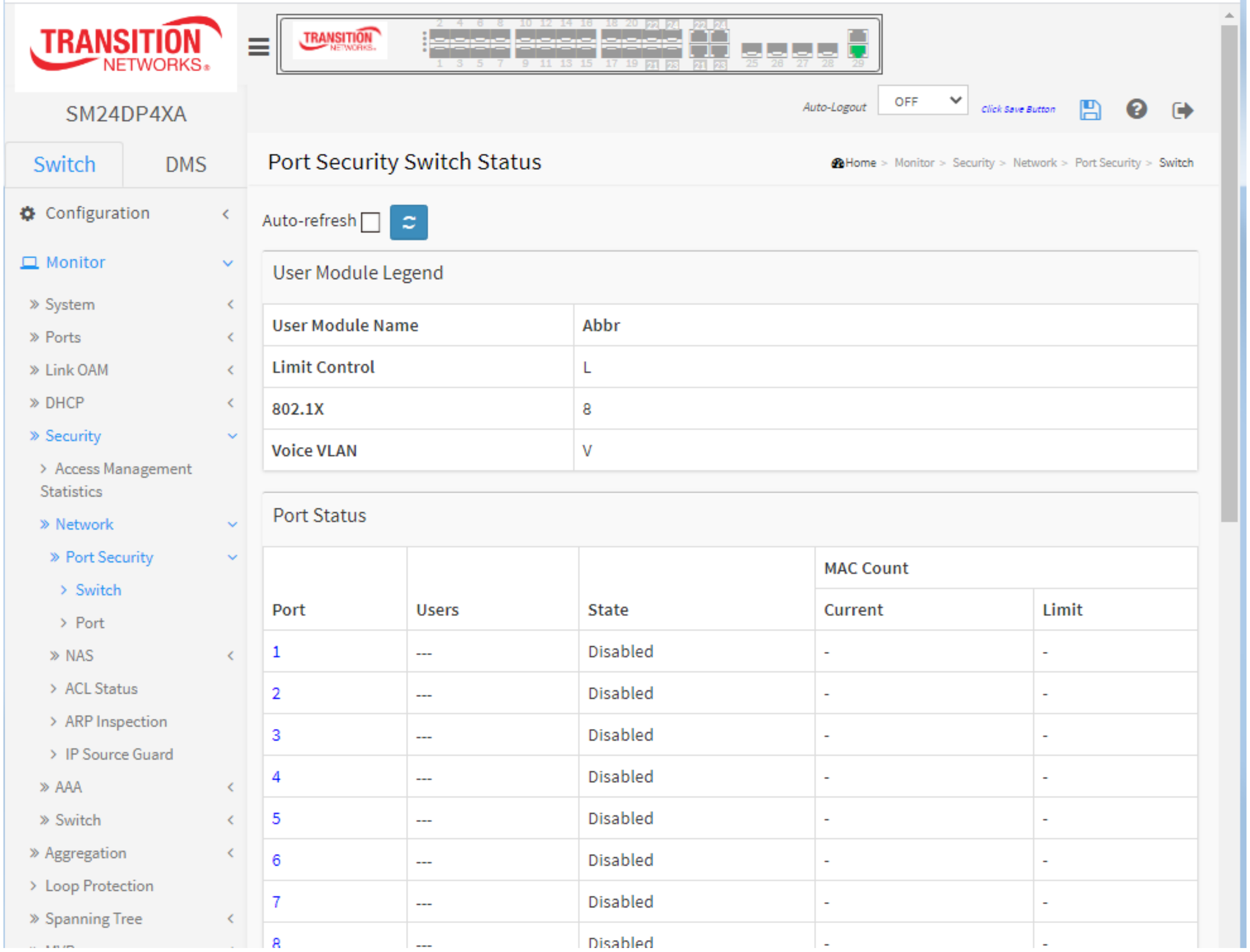
This page shows the Port Security status. Port Security is a module with no direct configuration. Configuration comes indirectly from other modules - the user modules. When a user module has enabled port security on a port, the port is set-up for software-based learning. In this mode, frames from unknown 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. View the displayed information.
3. Use the various buttons as required.

Figure 3-5.2.1.1: Port Security Switch Status



Port Security Switch Status

Auto-refresh □

User Module Legend

User Module Name	Abbr
Limit Control	L
802.1X	8
Voice VLAN	V

Port Status

			MAC Count	
Port	Users	State	Current	Limit
1	---	Disabled	-	-
2	---	Disabled	-	-
3	---	Disabled	-	-
4	---	Disabled	-	-
5	---	Disabled	-	-
6	---	Disabled	-	-
7	---	Disabled	-	-
8	---	Disabled	-	-

Parameter descriptions:

User Module Legend : The legend shows all user modules that may request Port Security services.

User Module Name : The full name of a module that may request Port Security services (Limit Control, 802.1X, Voice VLAN).

Abbr : A one-letter abbreviation (L, 8, V) of the User Module Name. This is used in the Users column in the port status table.

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

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 '-' 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.

Refresh: Click to refresh the page.

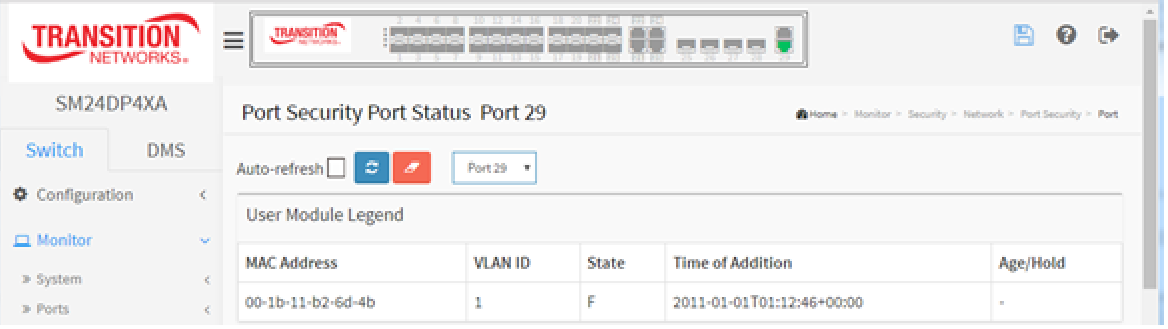
3-5.2.1.2 Port

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.

To configure a Port Security Switch Status Configuration in the web interface:

1. Click Monitor, Security, Network, Port Security, Port.
2. Use the port select box to select which port to show status for.
3. View the displayed information.
4. Use the various buttons as required.

Figure 3-5.2.1.2: Port Security Port Status for Port 29



Port Security Port Status Port 29

Auto-refresh □ Port 29 ▾

User Module Legend

MAC Address	VLAN ID	State	Time of Addition	Age/Hold
00-1b-11-b2-6d-4b	1	F	2011-01-01T01:12:46+00:00	-

MAC Address & VLAN ID : The MAC address and VLAN ID seen on this port. If no MAC addresses are learned, a single row stating "*No MAC addresses attached*" is displayed.

State : Indicates whether the corresponding MAC address is **B** (blocked) or **F** (forwarding). In the blocked state, it will not be allowed to transmit or receive traffic.

Time of Addition : Shows the date and time when this MAC address was first seen on the port.

Age/Hold : If at least one user module has decided to block this MAC address, it will stay in the blocked state until the hold time (measured in seconds) expires. If all user modules have decided to allow this MAC address to forward, and aging is enabled, the Port Security module will periodically check that this MAC address still forwards traffic. If the age period (measured in seconds) expires and no frames have been seen, the MAC address will be removed from the MAC table. Otherwise a new age period will begin. If aging is disabled or a user module has decided to hold the MAC address indefinitely, a dash (-) will be shown.

Buttons

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

Refresh: Click to refresh the page.

Clear : Click to clear table parameters.

3-5.2.2 NAS

3-6.2.2.1 Switch

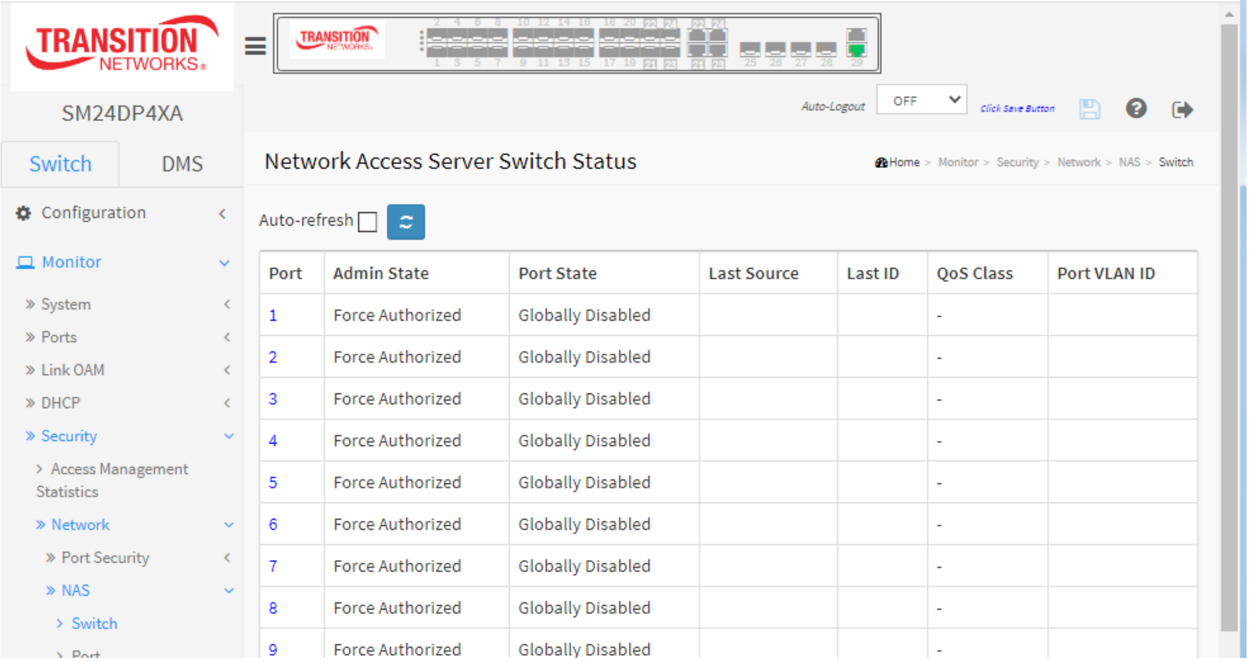
This page shows each port's NAS status information. The status includes Admin State Port State, Last Source, Last ID, QoS Class, and Port VLAN ID.

Web Interface

To configure a NAS Switch Status Configuration in the web interface:

1. Click Monitor, Security, Network, NAS, Switch.
2. View the displayed information.
3. Use the Auto-refresh and Refresh buttons as required.
4. You can click a linked Port number to display its details.

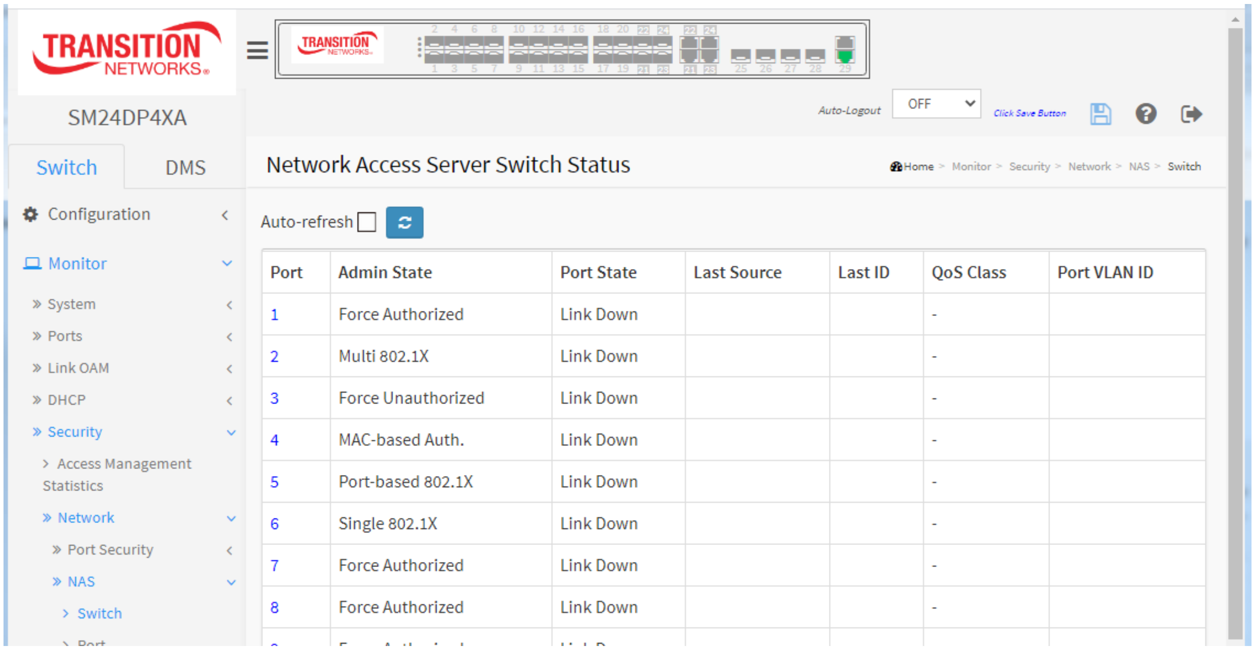
Figure 3-5.2.2.1: Network Access Server Switch Status



Network Access Server Switch Status

Auto-refresh □

Port	Admin State	Port State	Last Source	Last ID	QoS Class	Port VLAN ID
1	Force Authorized	Globally Disabled			-	
2	Force Authorized	Globally Disabled			-	
3	Force Authorized	Globally Disabled			-	
4	Force Authorized	Globally Disabled			-	
5	Force Authorized	Globally Disabled			-	
6	Force Authorized	Globally Disabled			-	
7	Force Authorized	Globally Disabled			-	
8	Force Authorized	Globally Disabled			-	
9	Force Authorized	Globally Disabled			-	



Network Access Server Switch Status

Auto-refresh □

Port	Admin State	Port State	Last Source	Last ID	QoS Class	Port VLAN ID
1	Force Authorized	Link Down			-	
2	Multi 802.1X	Link Down			-	
3	Force Unauthorized	Link Down			-	
4	MAC-based Auth.	Link Down			-	
5	Port-based 802.1X	Link Down			-	
6	Single 802.1X	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 to navigate to detailed NAS statistics for this port.

Admin State : The port's current administrative state. Force Authorized, Force Unauthorized, Port-based 802.1X, Single 802.1X, Multi 802.1X, or MAC-based Auth. See Configuration > Security > Network > NAS for full descriptions.

Port State : The current state of the port. It can have one of these 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.

Last Source : The source MAC address carried in the most recently received EAPOL frame for EAPOL-based authentication, and the most recently received frame from a new client for MAC-based authentication.

Last ID : The user name (supplicant identity) carried in the most recently received Response Identity EAPOL frame for EAPOL-based authentication, and the source MAC address from the most recently received frame from a new client for MAC-based authentication.

QoS Class : QoS Class assigned to the port by the RADIUS server if enabled.

Port VLAN ID : The VLAN ID that NAS has put the port in. The field is blank if the Port VLAN ID is not overridden by NAS.

If the VLAN ID is assigned by the RADIUS server, "(RADIUS-assigned)" is appended to the VLAN ID.
See the online Help for more about RADIUS-assigned VLANs.

If the port is moved to the Guest VLAN, "(Guest)" is appended to the VLAN ID. See the online Help or see Configuration > Security > Network > NAS for more about Guest VLANs.

Buttons

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

Refresh: Click to refresh the page.

3-5.2.2.2 Port

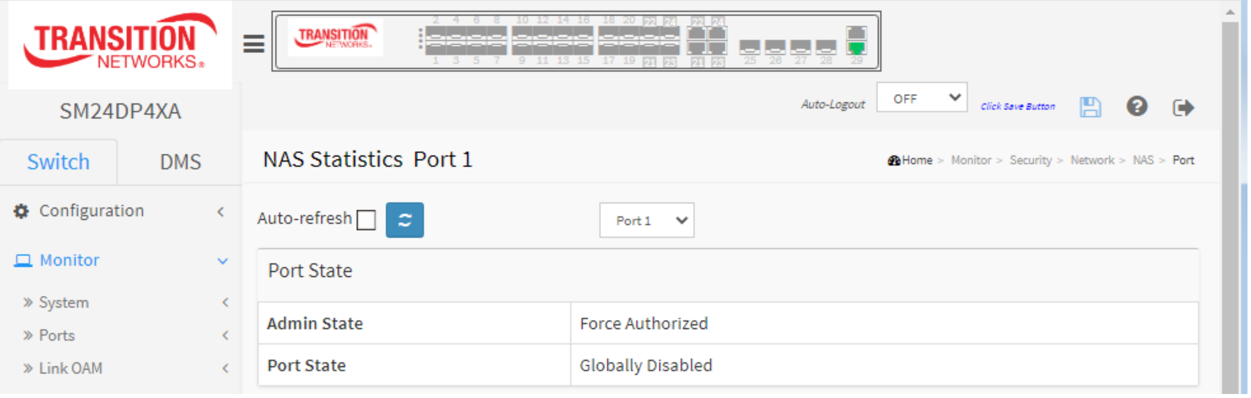
This page provides detailed NAS statistics for a specific switch port running EAPOL-based IEEE 802.1X authentication. For MAC-based ports, it shows selected backend server (RADIUS Authentication Server) statistics only.

Web Interface

To configure a NAS Port Status Configuration in the web interface:

1. Click Monitor, Security, Network, NAS, Port.
2. At the port select box choose a port.
3. View the displayed information.
4. Use the buttons as required.

Figure 3-5.2.2.2: NAS Statistics



NAS Statistics Port 1

Auto-refresh □ Port 1

Port State

Admin State	Force Authorized
Port State	Globally Disabled

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.
For more about RADIUS-assigned VLANs see the online Help or see Configuration > Security > Network > NAS.

If the port is moved to the Guest VLAN, "(Guest)" is appended to the VLAN ID. For more about Guest VLANs see the online Help or see Configuration > Security > Network > NAS.

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: 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).

Clear: This button is available in the following modes:

- Force Authorized
- Force Unauthorized
- Port-based 802.1X
- Single 802.1X

Clear All: Click to clear the counters for the selected port. This button is available in the following 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 the following modes:

- Multi 802.1X
- MAC-based Auth.X

Click to clear only the currently selected client's counters.

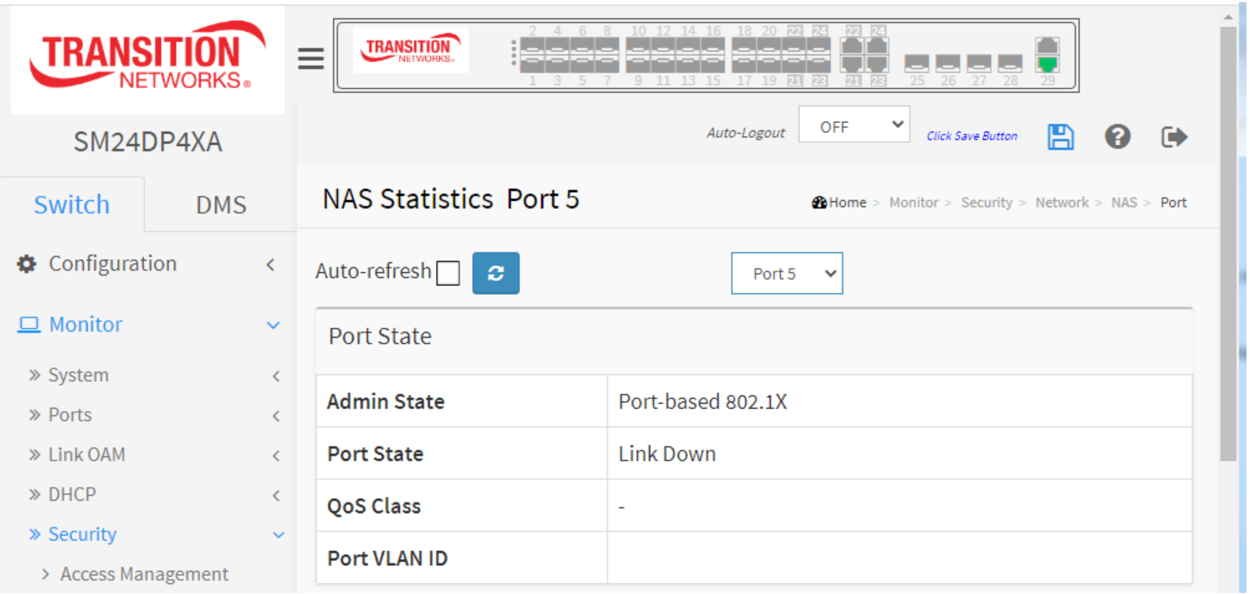
Buttons

Port select box: At the dropdown choose a port.

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

Refresh: Click to refresh the page immediately.

Example:



NAS Statistics Port 5

Port State	
Admin State	Port-based 802.1X
Port State	Link Down
QoS Class	-
Port VLAN ID	

3-5.2.3 ACL Status

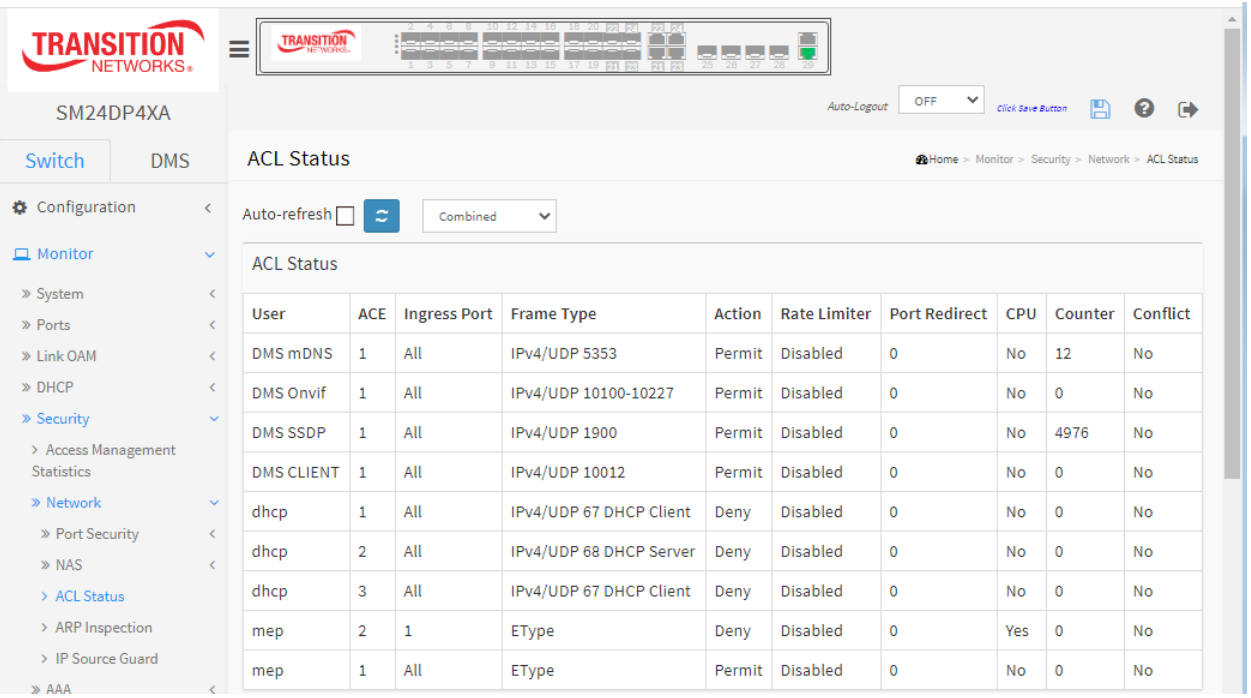
This page lets you shows the ACL status by different ACL users. Each row describes the ACE that is defined. It is a conflict if a specific ACE is not applied to the hardware due to hardware limitations. The maximum number of ACEs is 512 on each switch.

Web Interface

To display the ACL status in the web interface:

1. Click Monitor, Security, Network, ACL Status.
2. At the user select dropdown select the desired user.
3. View the displayed information.
4. Use the buttons as required.

Figure 3-5.2.3: ACL Status



ACL Status

ACL Status

User	ACE	Ingress Port	Frame Type	Action	Rate Limiter	Port Redirect	CPU	Counter	Conflict
DMS mDNS	1	All	IPv4/UDP 5353	Permit	Disabled	0	No	12	No
DMS Onvif	1	All	IPv4/UDP 10100-10227	Permit	Disabled	0	No	0	No
DMS SSDP	1	All	IPv4/UDP 1900	Permit	Disabled	0	No	4976	No
DMS CLIENT	1	All	IPv4/UDP 10012	Permit	Disabled	0	No	0	No
dhcp	1	All	IPv4/UDP 67 DHCP Client	Deny	Disabled	0	No	0	No
dhcp	2	All	IPv4/UDP 68 DHCP Server	Deny	Disabled	0	No	0	No
dhcp	3	All	IPv4/UDP 67 DHCP Client	Deny	Disabled	0	No	0	No
mep	2	1	EType	Deny	Disabled	0	Yes	0	No
mep	1	All	EType	Permit	Disabled	0	No	0	No

Parameter descriptions:

User : Indicates the ACL user.

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 - 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.

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

Enabled: Frames received on the port are mirrored.

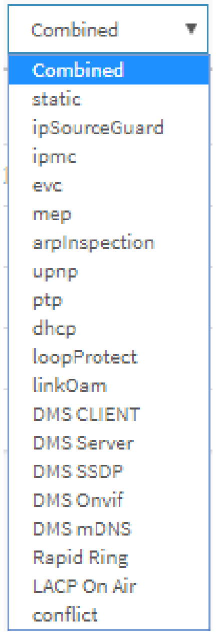
Disabled: Frames received on the port are not mirrored. The default value is "Disabled".

CPU : Forward packet that matched the specific ACE to CPU.

CPU Once : Forward first packet that matched the specific ACE to CPU.

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

Conflict : Indicates the hardware status of the specific ACE. The specific ACE is not applied to the hardware due to hardware limitations.



Buttons

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

Refresh: Click to refresh the page immediately.

User select box: At the dropdown select the desired user (Combined, static, evc, mep, ptp, dhcp, conflict, etc.).

3-5.2.5 ARP Inspection

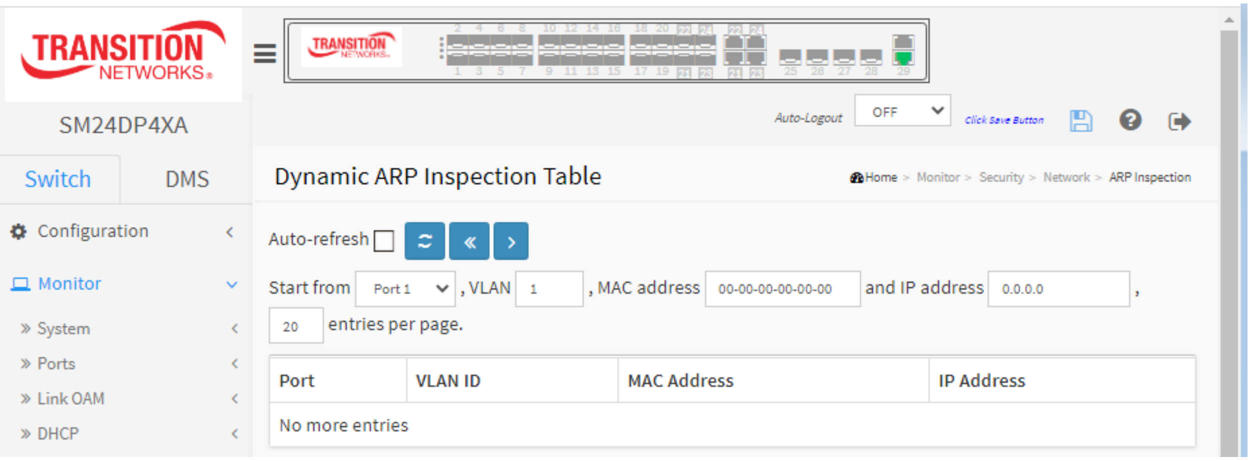
This page lets you configure the Dynamic ARP Inspection Table parameters of the switch. The Dynamic ARP Inspection Table contains up to 1024 entries, and is sorted first by port, then by VLAN ID, then by MAC address, and then by IP address.

Web Interface

To configure a Dynamic ARP Inspection Table Configuration in the web interface:

1. Click Monitor, Security, Network, ARP Inspection.
2. Set the Start from, VLAN, MAC address, IP address, and entries per page.
3. View the displayed information.
4. Use the buttons as required.

Figure 3-5.2.5: Dynamic ARP Inspection Table



Dynamic ARP Inspection Table

Auto-refresh □

Start from Port 1, VLAN 1, MAC address 00-00-00-00-00-00 and IP address 0.0.0.0,

20 entries per page.

Port	VLAN ID	MAC Address	IP Address
No more entries			

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 allow the user to select the starting point in the Dynamic ARP Inspection Table. Clicking the Refresh button will update the displayed table starting from that or the closest next Dynamic ARP Inspection Table match. In addition, the two input fields will - upon a Refresh button click - assume the value of the first displayed entry, allowing for continuous refresh with the same start address.

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

Parameter descriptions:

Port : Switch Port Number for which the entries are displayed.

VLAN ID : VLAN-ID in which the ARP traffic is permitted.

MAC Address : User MAC address of the entry.

IP Address : User IP address of the entry.

Buttons

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

Refresh: Click to refresh the page immediately.

<<: Updates the system log entries to the first available entry ID.

> : Updates the system log entry to the next available entry ID.

3-5.2.6 IP Source Guard

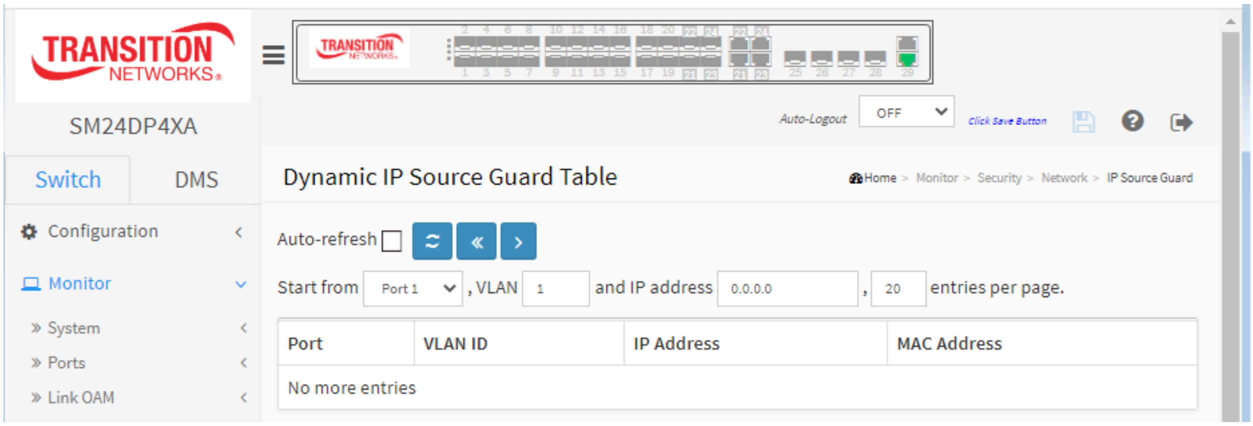
This page displays entries in the Dynamic IP Source Guard Table. The Dynamic IP Source Guard Table is sorted first by port, then by VLAN ID, then by IP address, and then by MAC address.

Web Interface

To configure a Dynamic IP Source Guard Table Configuration in the web interface:

1. Click Monitor, Security, Network, IP Source Guard.
2. Specify the Start from port, VLAN ID, IP Address, and entries per page.
3. View the displayed information.
4. Use the buttons as required.

Figure 3-5.2.6: Dynamic IP Source Guard Table



Dynamic IP Source Guard Table

Auto-refresh □

Start from Port 1 , VLAN 1 and IP address 0.0.0.0 , 20 entries per page.

Port	VLAN ID	IP Address	MAC Address
No more entries			

Parameter descriptions:

Port : Switch Port Number for which the entries are displayed.

VLAN ID : VLAN-ID in which the IP traffic is permitted.

IP Address : User IP address of the entry.

MAC Address : Source MAC address.

Buttons

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

Refresh: Click to refresh the page.

<<: 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

3-6.3.1 RADIUS Overview

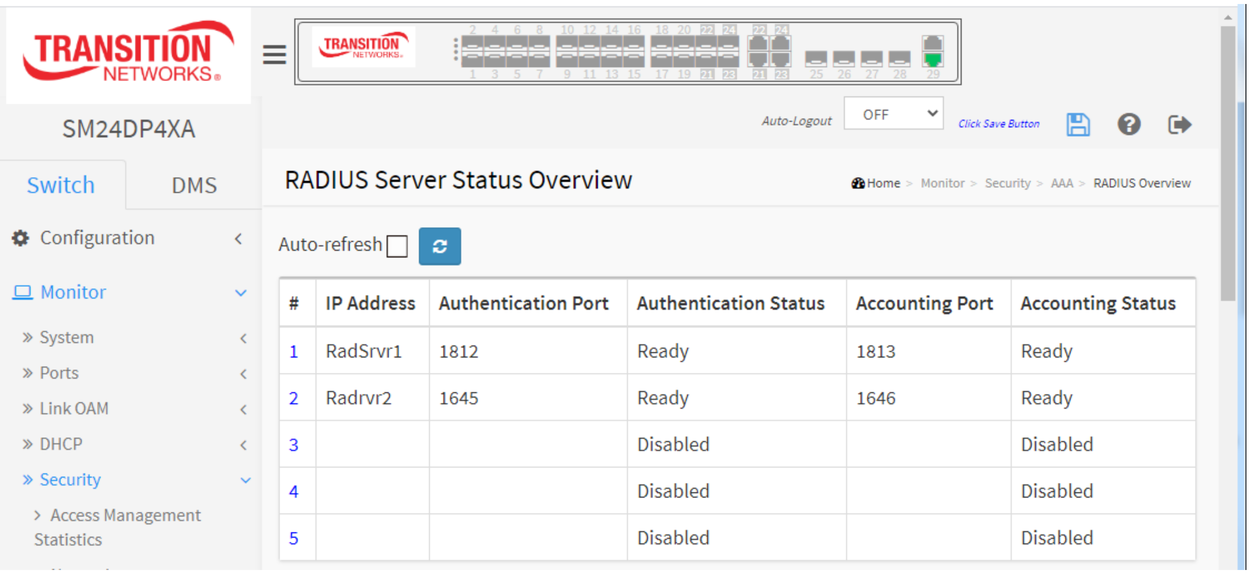
This page shows an overview of the RADIUS Authentication and Accounting servers’ status.

Web Interface

To configure a RADIUS Overview Configuration in the web interface:

1. Click Monitor, Security, AAA, RADIUS Overview.
2. View the displayed information.
3. Use the buttons as required.
4. You can click a linked number in the # column to display the selected server’s details.

Figure 3-5.3.1: RADIUS Server Status Overview



RADIUS Server Status Overview

Auto-refresh □

#	IP Address	Authentication Port	Authentication Status	Accounting Port	Accounting Status
1	RadSrvr1	1812	Ready	1813	Ready
2	Radrvr2	1645	Ready	1646	Ready
3			Disabled		Disabled
4			Disabled		Disabled
5			Disabled		Disabled

Parameter descriptions:

# : The RADIUS server number. Click to navigate to the detailed statistics for this server.

IP Address : The IP address of this server.

Authentication Port : The Auth Port; the UDP port number for authentication. The UDP port to use on the RADIUS server for authentication. The officially assigned port number for RADIUS Accounting is 1812. By default, many access servers use port 1645 for authentication requests.

Authentication Status : The current status of the server. This field takes one of these values:

Disabled: The server is disabled.

Not Ready: The server is enabled, but IP communication is not yet up and running.

Ready: The server is enabled, IP communication is up and running, and the RADIUS module is ready to accept access attempts.

Dead (X seconds left): Access attempts were made to this server, but it did not reply within the configured timeout. The server has temporarily been disabled, but will get re-enabled when the dead-time expires. The number of seconds left before this occurs is displayed in parentheses. This state is only reachable when more than one server is enabled.

Accounting Port : UDP port number for accounting. The Acct Port; the UDP port to use on the RADIUS server for accounting. The officially assigned port number for RADIUS Accounting is 1813. By default, many access servers use port 1646 for accounting requests.

Accounting Status : The current status of the server. This field takes one of these values:

Disabled: The server is disabled.

Not Ready: The server is enabled, but IP communication is not yet up and running.

Ready: The server is enabled, IP communication is up and running, and the RADIUS module is ready to accept access attempts.

Dead (X seconds left): Access attempts were made to this server, but it did not reply within the configured timeout. The server has temporarily been disabled but will get re-enabled when the dead-time expires. The number of seconds left before this occurs is displayed in parentheses. This state is only reachable when more than one server is enabled.

Buttons

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

Refresh: Click to refresh the page.

3-5.3.2 RADIUS Details

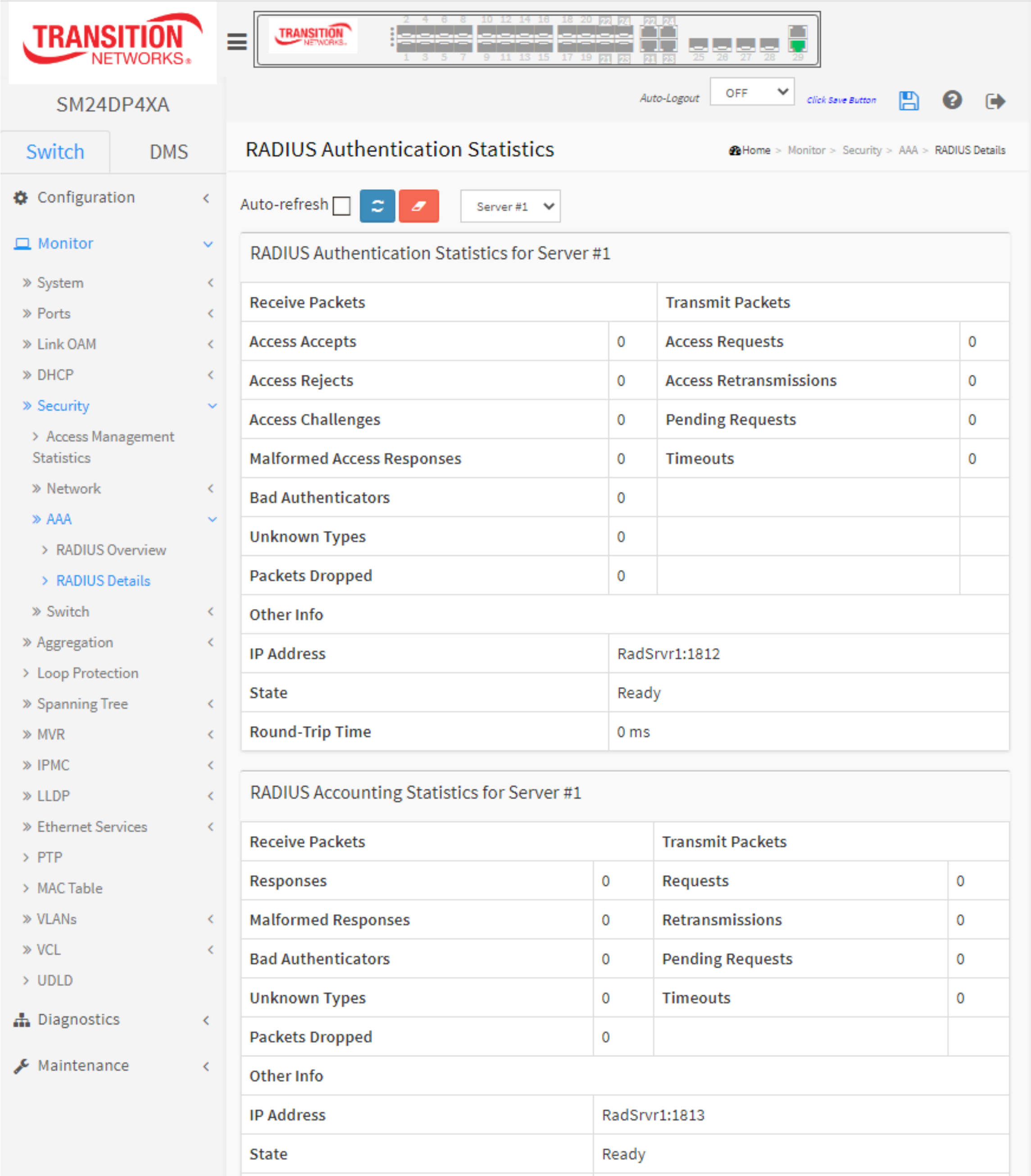
This page shows detailed statistics for a specified RADIUS server.

Web Interface

To view RADIUS Details via the web interface:

1. Click Security, AAA, RADIUS Overview.
2. Use the server select dropdown to select the Server you want to check.
3. View the displayed information.
4. Use the buttons as required.

Figure 3-5.3.2: RADIUS Authentication Statistics for Server #1



RADIUS Authentication Statistics

RADIUS Authentication Statistics for Server #1

Receive Packets		Transmit Packets	
Access Accepts	0	Access Requests	0
Access Rejects	0	Access Retransmissions	0
Access Challenges	0	Pending Requests	0
Malformed Access Responses	0	Timeouts	0
Bad Authenticators	0		
Unknown Types	0		
Packets Dropped	0		

Other Info	
IP Address	RadSrvr1:1812
State	Ready
Round-Trip Time	0 ms

RADIUS Accounting Statistics for Server #1

Receive Packets		Transmit Packets	
Responses	0	Requests	0
Malformed Responses	0	Retransmissions	0
Bad Authenticators	0	Pending Requests	0
Unknown Types	0	Timeouts	0
Packets Dropped	0		

Other Info	
IP Address	RadSrvr1:1813
State	Ready

Parameter descriptions:

RADIUS Authentication Statistics : The statistics map closely to those specified in IETF RFC4668 - RADIUS Authentication Client MIB.

Packet Counters : RADIUS authentication server packet counter. There are seven receive and four transmit counters.

Other Info : This section contains information about the state of the server and the latest round-trip time.

Packet Counters : RADIUS authentication server packet counter. There are seven receive and four transmit counters.

RADIUS Accounting Statistics : The statistics map closely to those specified in IETF RFC4670 - RADIUS Accounting Client MIB.
Use the server select box to switch between the backend servers to show details for.

Packet Counters : RADIUS authentication server packet counter. There are seven receive and four transmit counters.

Other Info : This section contains information about the state of the server and the latest round-trip time.

See the online Help for more information.

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.

Server #1 ▼ **Server select box** : lets you select which server's statistics to display.

3-5.4 Switch

3-5.4.1 RMON

3-5.4.1.1 Statistics

This section 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 entry displayed will be the one with the lowest ID found in the Statistics table.

The "Start from Control Index" allows the user to select the starting point in the Statistics table. Click the **Refresh** button to update the displayed table starting from that or the next closest Statistics table match.

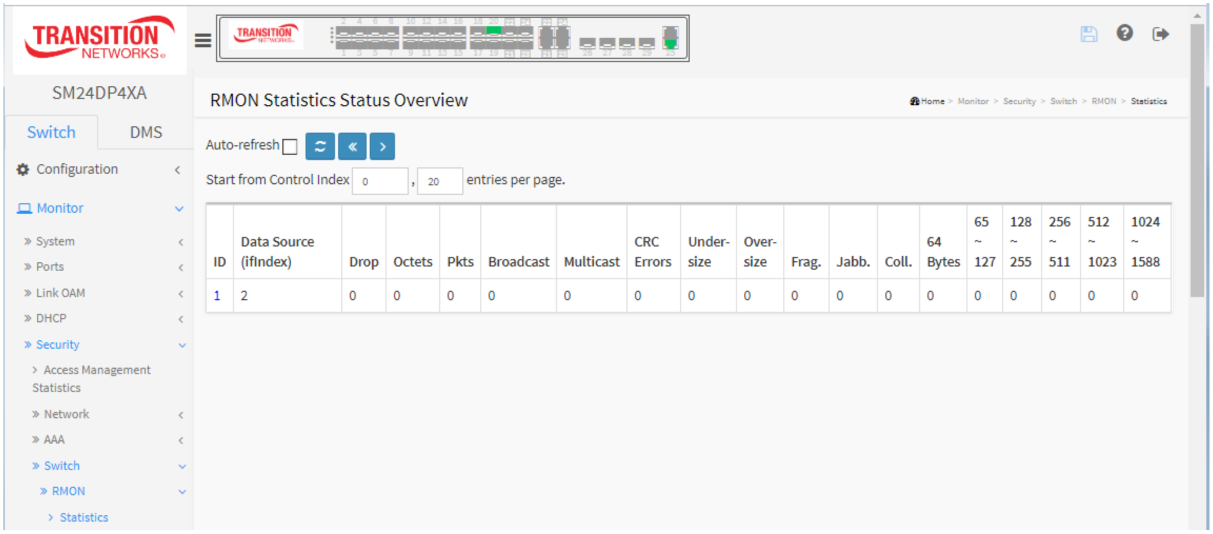
Click the **>** button to use the last entry of the currently displayed entry as a basis for the next lookup. When the end is reached the text "*No more entries*" displays. Use the **<<** button to start over.

Web Interface

To configure a RMON Statistics in the web interface:

1. Click Monitor, Security, Switch, RMON, Statistics.
2. Specify the Start from Control Index and entries per page.
3. Use the buttons as required.

Figure 3-5.4.1.1: RMON Statistics Status Overview



RMON Statistics Status Overview

Auto-refresh □ ⟳ « ›

Start from Control Index 0 , 20 entries per page.

ID	Data Source (ifIndex)	Drop	Octets	Pkts	Broadcast	Multicast	CRC Errors	Under-size	Over-size	Frag.	Jabb.	Coll.	64 Bytes	65 ~ 127	128 ~ 255	256 ~ 511	512 ~ 1023	1024 ~ 1588
1	2	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0

Parameter descriptions:

ID : Indicates the index of Statistics entry. Click the linked ID number to display its Detailed RMON Statistics (see below)

Data Source (ifIndex) : The port ID which you want to be monitored.

Drop : The total number of events in which packets were dropped by the probe due to lack of resources.

Octets : The total number of octets of data (including those in bad packets) received on the network.

Pkts : The total number of packets (including bad packets, broadcast packets, and multicast packets) received.

Broadcast : The total number of good packets received that were directed to the broadcast address.

Multicast : The total number of good packets received that were directed to a multicast address.

CRC Errors : The total number of packets received that had a length (excluding framing bits, but including FCS octets) of between 64 and 1518 octets, inclusive, but had either a bad Frame Check Sequence (FCS) with an integral number of octets (FCS Error) or a bad FCS with a non-integral number of octets (Alignment Error).

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 long.

65~127 : The total number of packets (including bad packets) received that were 65 - 127 octets long.

128~255 : The total number of packets (including bad packets) received that were 128 - 255 octets long.

256~511 : The total number of packets (including bad packets) received that were 256 - 511 octets long.

512~1023 : The total number of packets (including bad packets) received that were 512 - 1023 octets long.

1024~1588 : The total number of packets (including bad packets) received that were 1024 - 1588 octets long.

Buttons

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

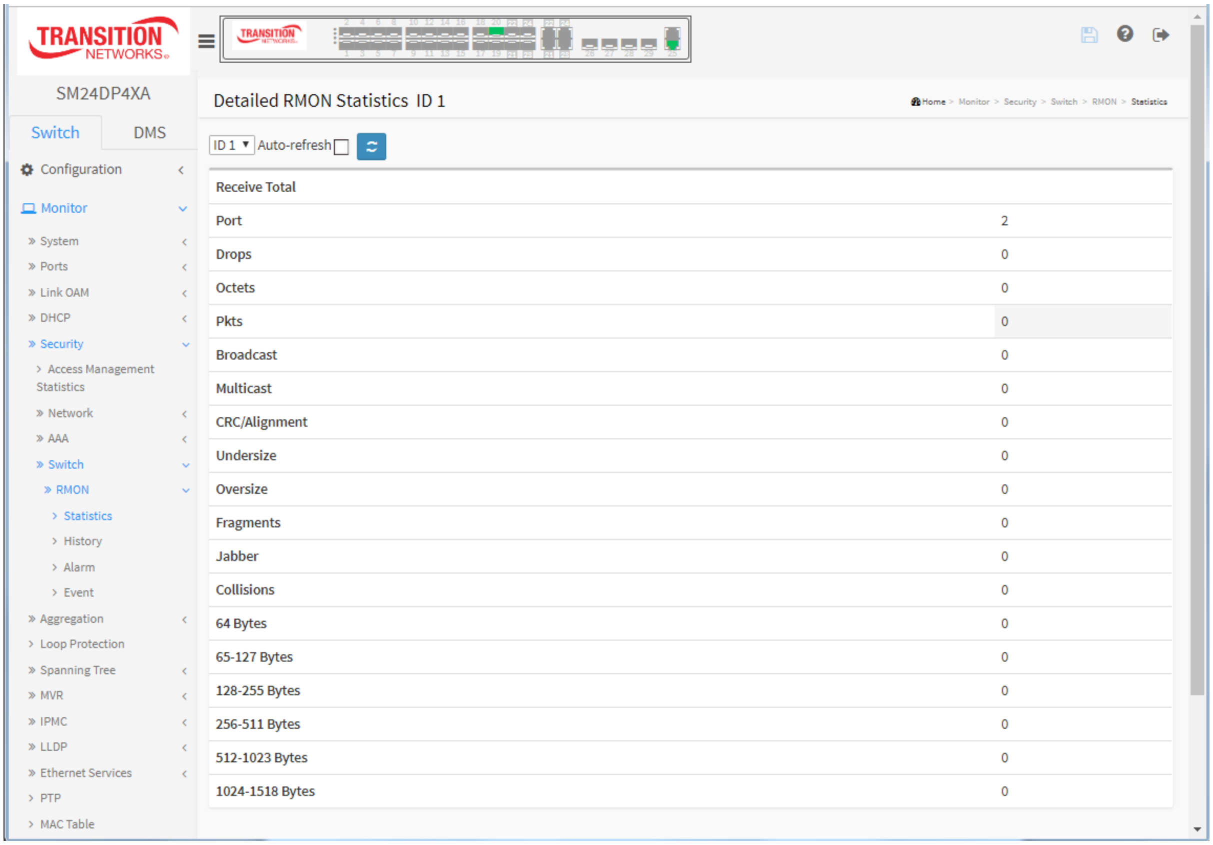
Refresh: Click to refresh the page immediately.

<< : Updates the table starting from the first entry in the Statistics table (the entry with the lowest ID).

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

Detailed RMON Statistics

When you click a linked ID number its Detailed RMON Statistics displays. The parameters are described above.



Detailed RMON Statistics ID 1

ID 1 ▾ Auto-refresh □

Receive Total	
Port	2
Drops	0
Octets	0
Pkts	0
Broadcast	0
Multicast	0
CRC/Alignment	0
Undersize	0
Oversize	0
Fragments	0
Jabber	0
Collisions	0
64 Bytes	0
65-127 Bytes	0
128-255 Bytes	0
256-511 Bytes	0
512-1023 Bytes	0
1024-1518 Bytes	0

3-5.4.1.2 History

This page provides an overview of RMON History entries. Each page shows up to 99 entries from the History table, default being 20, selected through the "entries per page" input field. When first visited, the web page will show the first 20 entries from the beginning of the History table. The first entry displayed will be the one with the lowest History Index and Sample Index found in the History table. The "Start from History Index and Sample Index" allows the user to select the starting point in the History table.

The "Start from History Index and Sample Index" lets you select the starting point in the History table. Clicking the **Refresh** button will update the displayed table starting from that or the next closest History table match.

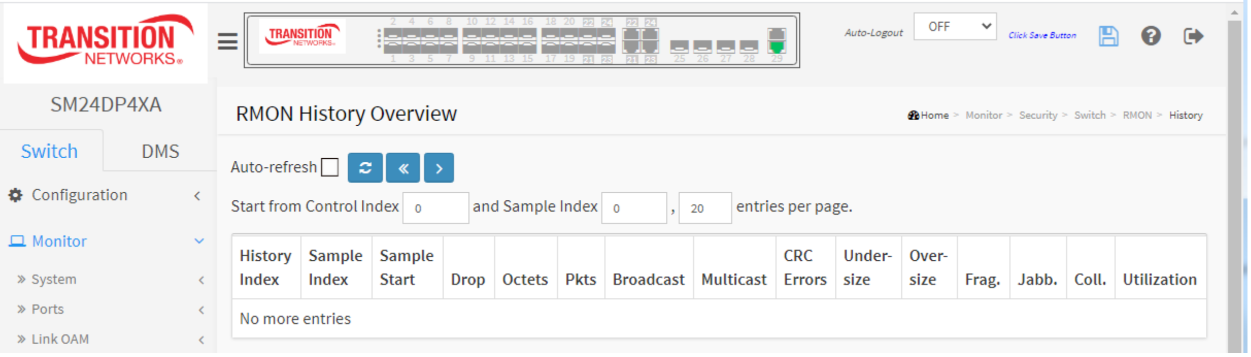
The **>** button will use the last entry of the currently displayed entry as a basis for the next lookup. When the end is reached the text "*No more entries*" displays in the table. Use the **<<** button to start over.

Web Interface

To configure a RMON history Configuration in the web interface:

1. Click Monitor, Security, Switch, RMON, History.
2. Set the Start from Control Index, Sample Index, and entries per page.
3. Use the buttons as required.

Figure 3-5.4.1.2: RMON History Overview



RMON History Overview

Auto-refresh □ ⟳ « ›

Start from Control Index 0 and Sample Index 0 , 20 entries per page.

History Index	Sample Index	Sample Start	Drop	Octets	Pkts	Broadcast	Multicast	CRC Errors	Under-size	Over-size	Frag.	Jabb.	Coll.	Utilization
No more entries														

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.

CRCErrors : 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 (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" allows the user to select the starting point in the Alarm table.

Clicking the **Refresh** button will update the displayed table starting from that or the next closest Alarm table match.

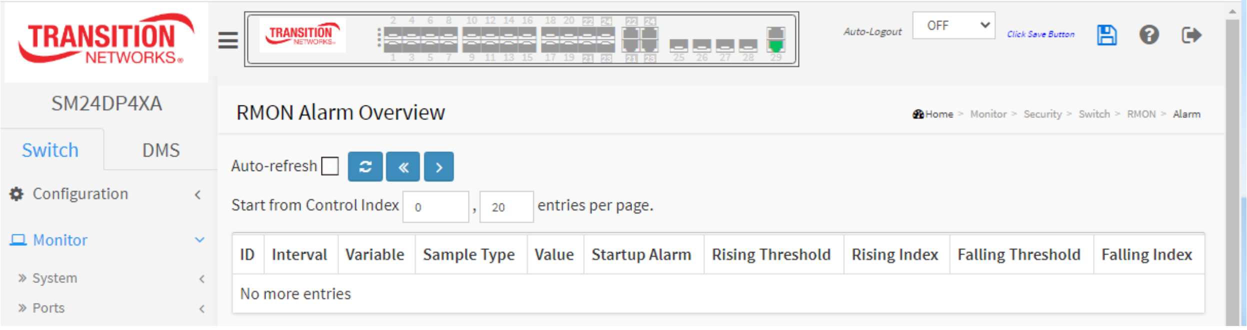
The **>** button will use the last entry of the currently displayed entry as a basis for the next lookup. When the end is reached the text "No more entries" displays in the table. Use **<<** the button to start over.

Web Interface

To configure a RMON Alarm Overview in the web interface:

1. Click Monitor, Security, Switch, RMON, Alarm.
2. Set the Start from Control Index and entries per page.
3. View the displayed information. If none exists, the table displays *No more entries*.
4. Use the buttons as required.

Figure 3-5.4.1.3: RMON Alarm Overview



RMON Alarm Overview

Auto-refresh □ ⟳ « ›

Start from Control Index 0 , 20 entries per page.

ID	Interval	Variable	Sample Type	Value	Startup Alarm	Rising Threshold	Rising Index	Falling Threshold	Falling Index
No more entries									

Parameter descriptions:

ID : 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 (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 entry displayed will be the one with the lowest Event Index and Log Index found in the Event table.

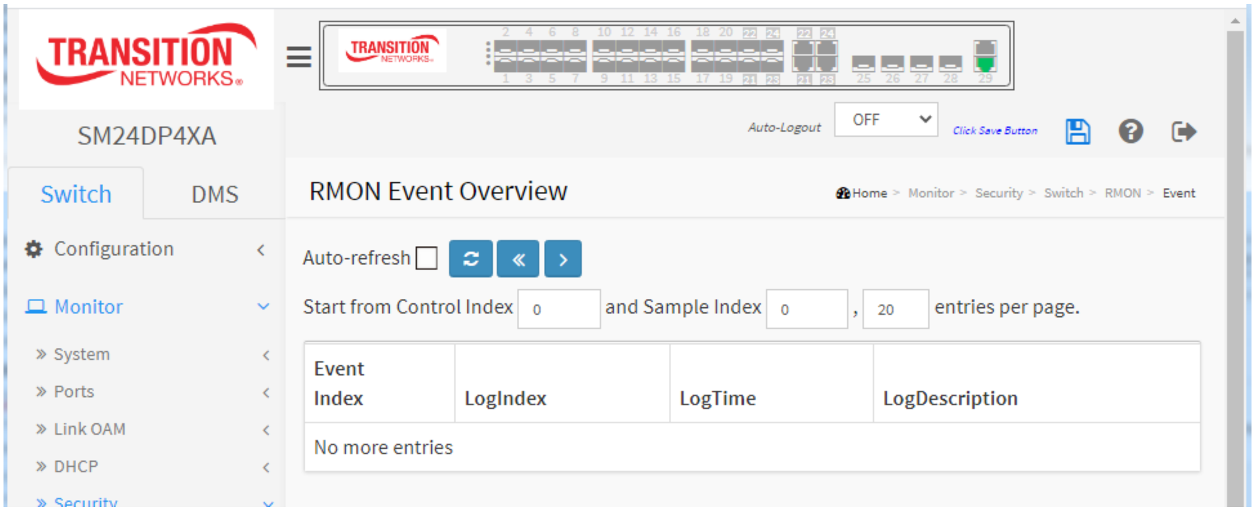
The "Start from Event Index and Log Index" allows the user to select the starting point in the Event table. Clicking the **Refresh** button will update the displayed table starting from that or the next closest Event table match. The **>** button will use the last entry of the currently displayed entry as a basis for the next lookup.
When the end is reached the text "No more entries" displays in the table. Use the **<<** button to start over.

Web Interface

To view the RMON Events via the web interface:

1. Click Monitor, Security, Switch, RMON, Event.
2. Set the Start from Control Index, Sample Index, and entries per page.
3. View the displayed information. If none exists, the table displays *No more entries*.

Figure 3-5.4.1.4: RMON Event Overview



RMON Event Overview

Auto-refresh □

Start from Control Index 0 and Sample Index 0 , 20 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: 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 (the entry with the lowest Event Index and Log Index).

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

3-6 Aggregation

3-6.1 Aggregation Status

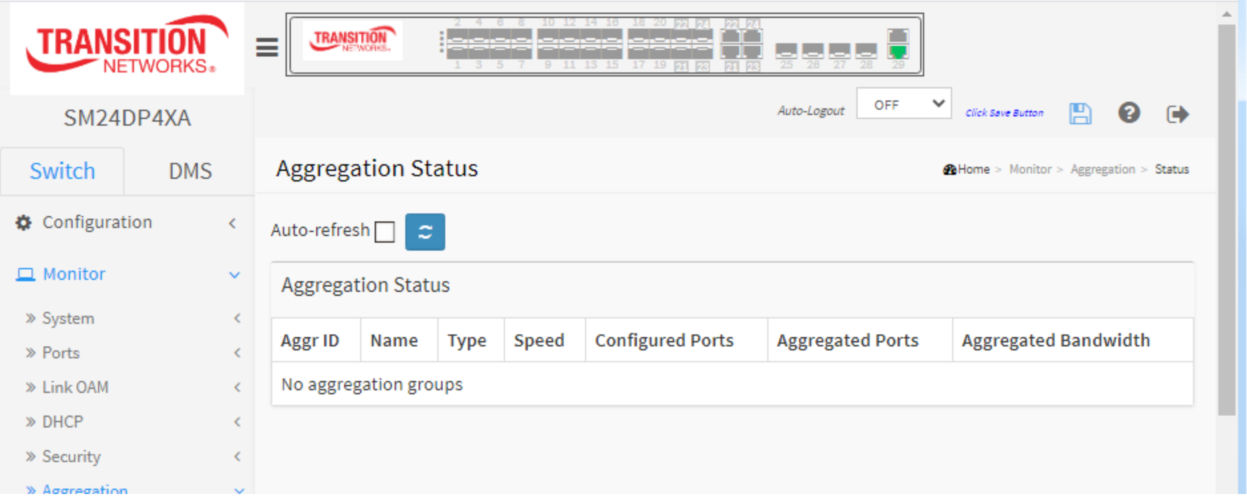
This page displays the status of ports in Aggregation group.

Web Interface

To display the Aggregation Status in the web interface:

1. Click Monitor, Aggregation, Status.
2. View the displayed information. If none exists, the table displays *No aggregation groups*.
3. Use the buttons as required.

Figure 3-6.1 Aggregation Status



Aggregation Status

Auto-refresh □

Aggregation Status

Aggr ID	Name	Type	Speed	Configured Ports	Aggregated Ports	Aggregated Bandwidth
No aggregation groups						

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.

Buttons

Refresh : Click to refresh the page immediately.

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

3-7 LACP

3-7.1 System Status

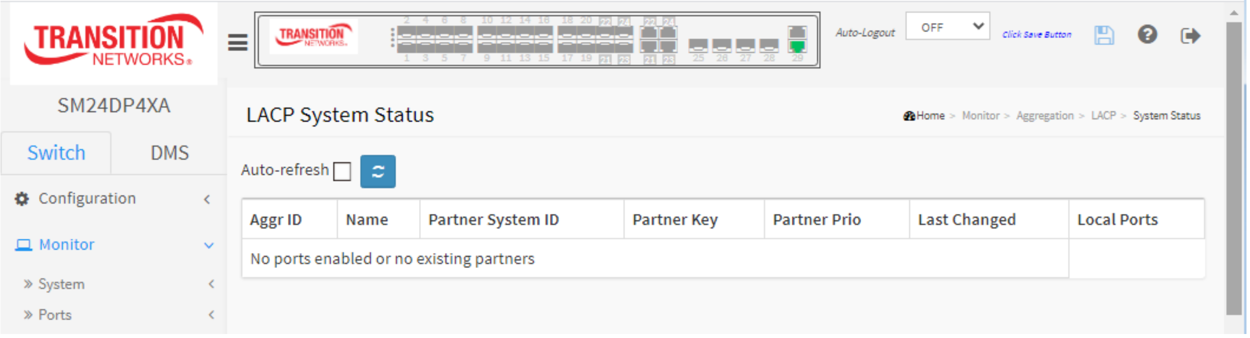
This page displays a status overview for all LACP instances.

Web Interface

To display the LACP System status in the web interface:

1. Click Monitor, Aggregation, LACP, System Status.
2. View the displayed information. If none exists, the table displays *No ports enabled or no existing partners*.
3. Use the buttons as required.

Figure 3-7.1 LACP System Status



LACP System Status

Auto-refresh □

Aggr ID	Name	Partner System ID	Partner Key	Partner Prio	Last Changed	Local Ports
No ports enabled or no existing partners						

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'.

Name : The name of the Aggregation group ID.

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

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

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.

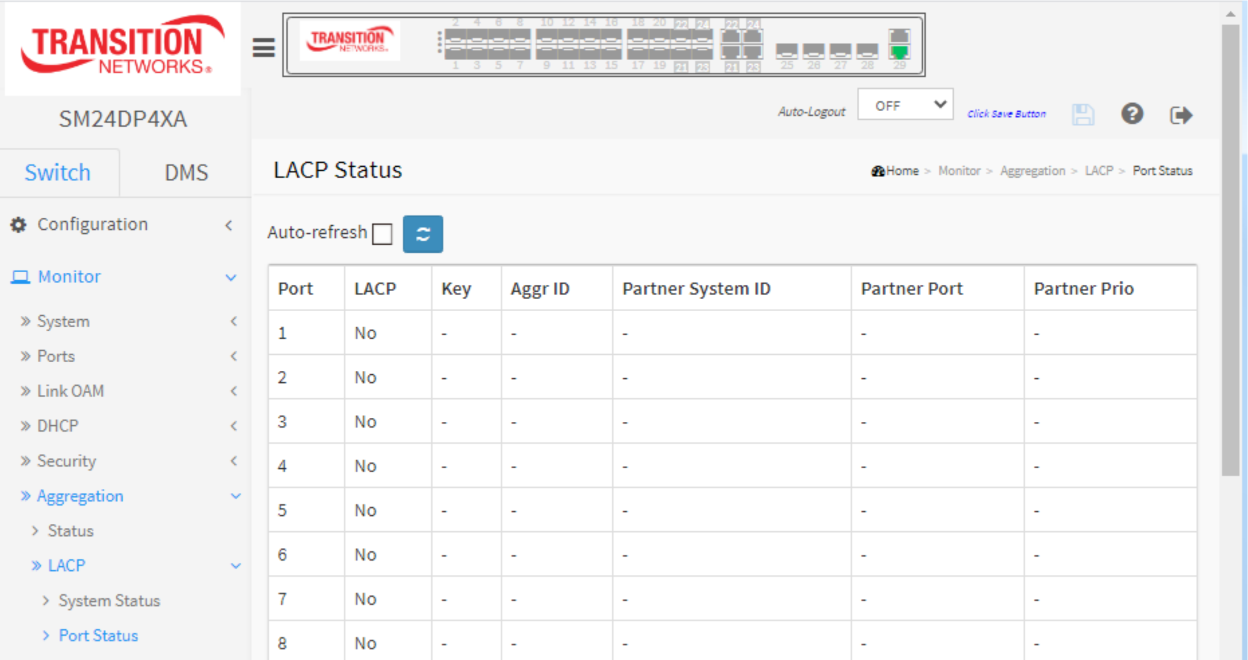
3-7.2 Port Status

This page provides an LACP Status overview for all LACP instances.

To display the LACP Port status in the web interface:

1. Click Monitor, Aggregation, LACP, Port Status.
2. View the displayed information.
3. Use the buttons as required.

Figure 3-7.2: LACP Status



LACP Status

Auto-refresh □

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	-	-	-	-	-

Parameter descriptions:

Port : The switch port number.

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

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

Aggr ID : The Aggregation ID 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.

Buttons

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

Refresh: Click to refresh the page immediately.

3-7.3 Port Statistics

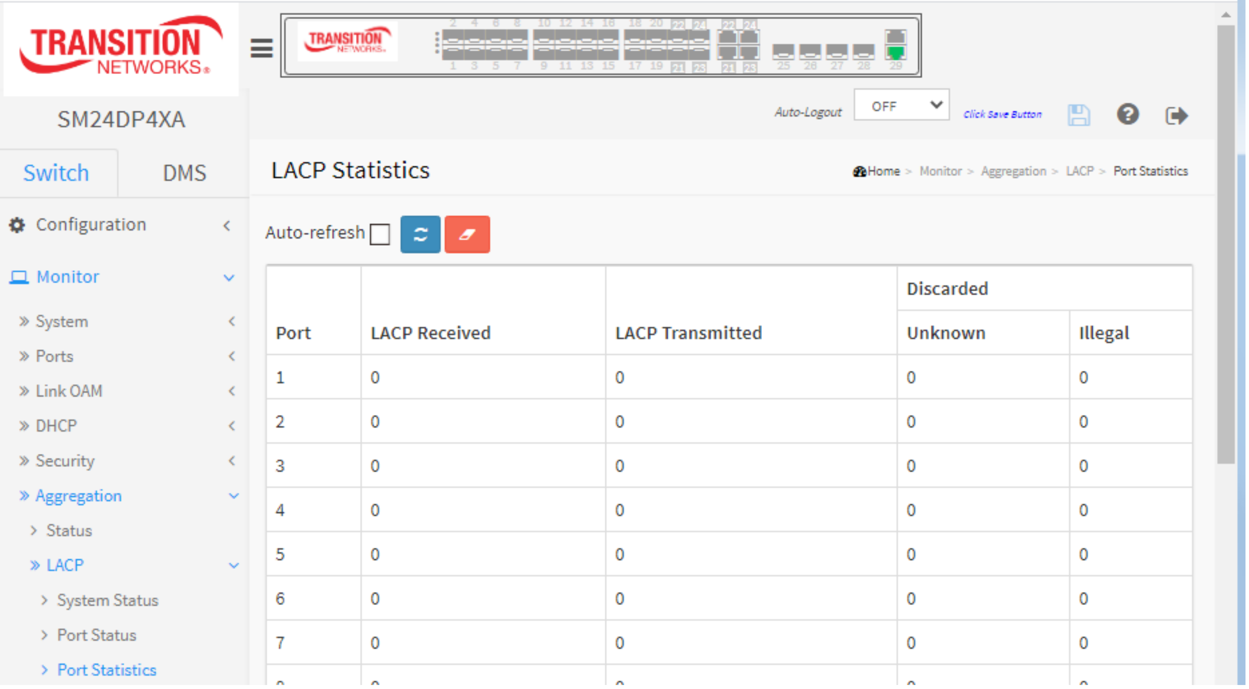
This page provides a Port Statistics overview of all LACP instances.

Web Interface

To display the LACP Port status in the web interface:

1. Click Monitor, Aggregation, LACP, Port Statistics.
2. View the displayed information.
3. Use the buttons as required.

Figure 3-6.3: LACP Statistics



LACP Statistics

Auto-refresh □

Port	LACP Received	LACP Transmitted	Discarded	
			Unknown	Illegal
1	0	0	0	0
2	0	0	0	0
3	0	0	0	0
4	0	0	0	0
5	0	0	0	0
6	0	0	0	0
7	0	0	0	0

Parameter descriptions:

Port : The switch port number.

LACP Received : Shows how many LACP frames have been received at each port.

LACP Transmitted : Shows how many LACP frames have been sent from each port.

Discarded : Shows how many Unknown 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 refresh the page immediately.

Clear: Clears the counters for the selected port.

3-8 Loop Protection

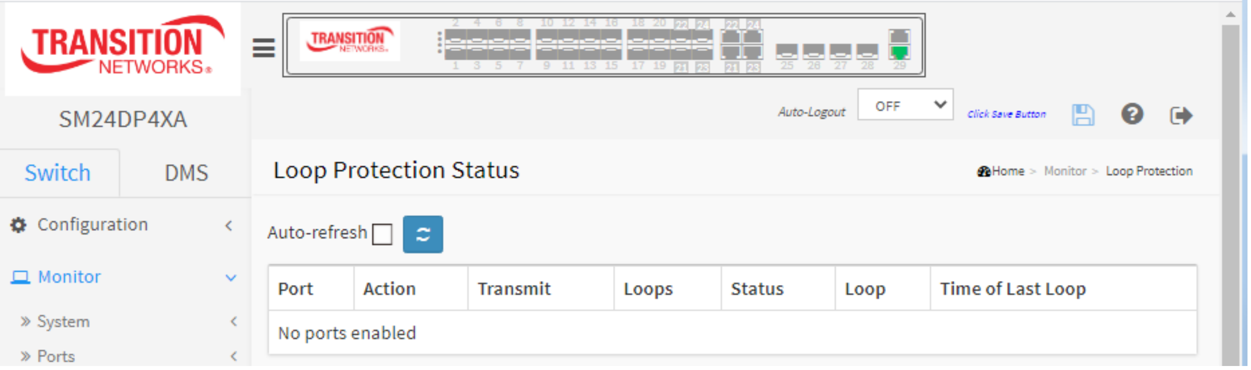
This page displays the loop protection port status.

Web Interface

To display the Loop Protection status in the web interface:

1. Click Monitor, Loop Protection.
2. View the displayed information. If none exists, the table displays *No ports enabled*.
3. Use the buttons as required.

Figure 3-8: Loop Protection Status



Loop Protection Status

Auto-refresh □

Port	Action	Transmit	Loops	Status	Loop	Time of Last Loop
No ports enabled						

Parameter descriptions:

Port : The switch port number of the logical port.

Action : The currently configured port action.

Transmit : The currently configured port transmit mode.

Loops : The number of loops detected on this port.

Status : The current loop protection status of the port.

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

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

Buttons

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

Refresh: Click to refresh the page immediately.

3-9 Spanning Tree

3-9.1 Bridge Status

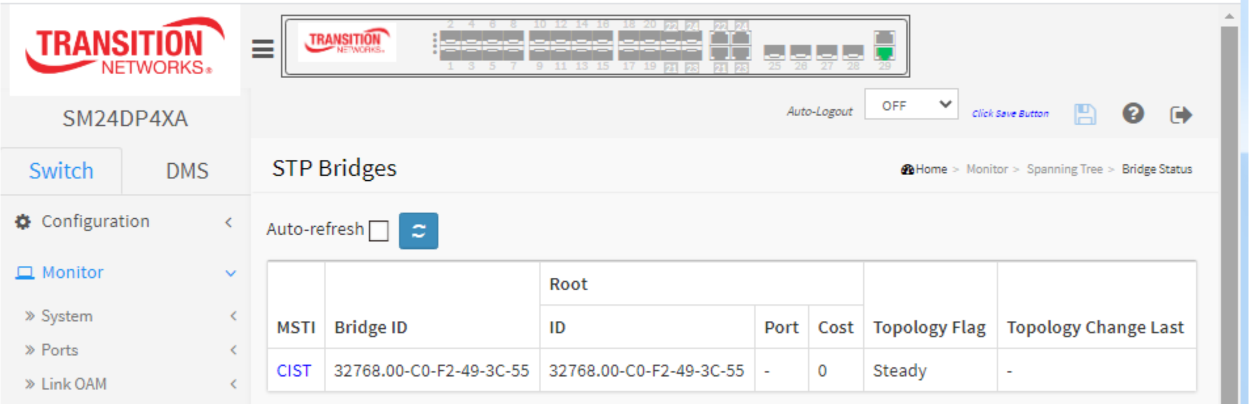
This page provides a status overview of all STP bridge instances. The displayed table contains a row for each STP bridge instance.

Web Interface

To display the STP Bridges status in the web interface:

1. Click Monitor, Spanning Tree, Bridge Status.
2. View the displayed information.
3. Use the buttons as required.
4. You can click CIST to display the STP Detailed Bridge Status page (see below).

Figure 3-9.1: STP Bridges



		Root				
MSTI	Bridge ID	ID	Port	Cost	Topology Flag	Topology Change Last
CIST	32768.00-C0-F2-49-3C-55	32768.00-C0-F2-49-3C-55	-	0	Steady	-

Parameter descriptions:

MSTI : The Bridge Instance. This is also a link to the STP Detailed Bridge Status (see below).

Bridge ID : The Bridge ID of this Bridge instance.

Root ID : The Bridge ID of the currently elected root bridge.

Root Port : The switch port currently assigned the root port role.

Root Cost : Root Path Cost. For the Root Bridge it is zero. For all other Bridges, it is the sum of the Port Path Costs on the least cost path to the Root Bridge.

Topology Flag : The current state of the Topology Change Flag of this Bridge instance.

Topology Change Last : The time since last Topology Change occurred.

Buttons

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

Refresh: Click to refresh the page immediately.

3-9.1.1 STP Detailed Bridge Status

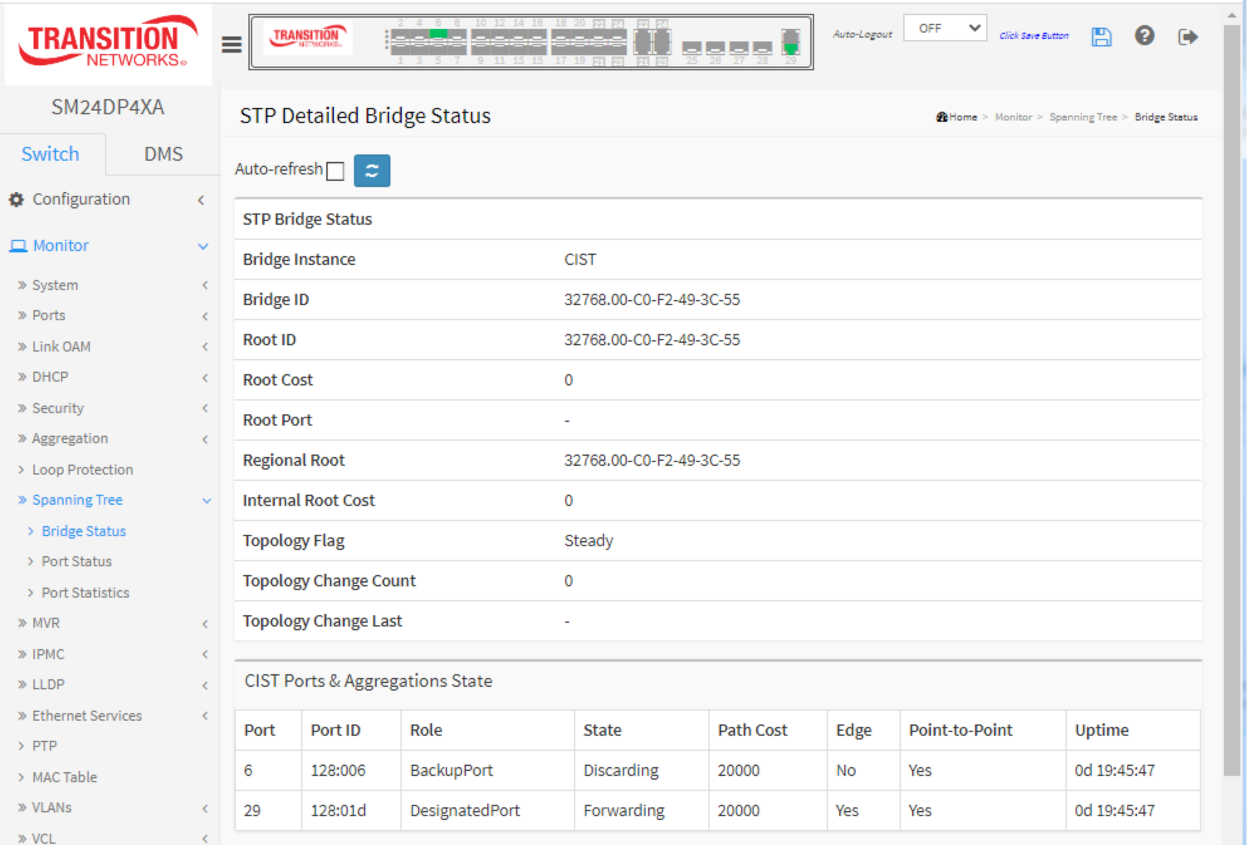
This page provides detailed information on a single STP bridge instance, along with port state for all active ports associated. At the STP Bridges page, when you click CIST, the STP Detailed Bridge Status page displays as shown below.

Web Interface

To display the STP Bridges status in the web interface:

1. Click Monitor, Spanning Tree, Bridge Status.
2. Click CIST to display the STP Detailed Bridge Status page.
3. View the page information.
4. Use the buttons as required.

Figure 3-9.1.1: STP Detailed Bridge Status



STP Detailed Bridge Status

Auto-refresh □

STP Bridge Status	
Bridge Instance	CIST
Bridge ID	32768.00-C0-F2-49-3C-55
Root ID	32768.00-C0-F2-49-3C-55
Root Cost	0
Root Port	-
Regional Root	32768.00-C0-F2-49-3C-55
Internal Root Cost	0
Topology Flag	Steady
Topology Change Count	0
Topology Change Last	-

CIST Ports & Aggregations State

Port	Port ID	Role	State	Path Cost	Edge	Point-to-Point	Uptime
6	128:006	BackupPort	Discarding	20000	No	Yes	0d 19:45:47
29	128:01d	DesignatedPort	Forwarding	20000	Yes	Yes	0d 19:45:47

Parameter descriptions:

STP Bridge Status

Bridge Instance : The Bridge instance (e.g., CIST, MST1, etc.).

Bridge ID : The Bridge ID of this Bridge instance.

Root ID : The Bridge ID of the currently elected root bridge.

Root Port : The switch port currently assigned the root port role.

Root Cost : Root Path Cost. For the Root Bridge 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.

Regional Root : The Bridge ID of the currently elected regional root bridge, inside the MSTP region of this bridge. *(For the CIST instance only)*.

Internal Root Cost : The Regional Root Path Cost. For the Regional Root Bridge this is zero. For all other CIST instances in the same MSTP region, it is the sum of the Internal Port Path Costs on the least cost path to the Internal Root Bridge. *(For the CIST instance only)*.

Topology Flag : The current state of the Topology Change Flag of this Bridge instance.

Topology Change Count : The number of times where the topology change flag has been set (during a one-second interval).

Topology Change Last : The time passed since the Topology Flag was last set.

CIST Ports & Aggregations State

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

Port ID : The port id as used by the STP protocol. This is the priority part and the logical port index of the bridge port.

Role : The current STP port role; can be Alternate Port, Backup Port , Root Port , or Designated Port.

State : The current STP port state. The port state can be Discarding, Learning, or Forwarding.

Path Cost : The current STP port path cost. This will either be a value computed from the Auto setting, or any explicitly configured value.

Edge : The current STP port (operational) Edge Flag. An Edge Port is a switch port to which no Bridges are attached. The flag may be automatically computed or explicitly configured. Each Edge Port transits directly to the Forwarding Port State, since there is no possibility of it participating in a loop.

Point-to-Point : The current STP port point-to-point flag. A point-to-point port connects to a non-shared LAN media. The flag may be automatically computed or explicitly configured. The point-to-point properties of a port affect how fast it can transit to STP state.

Uptime : The time since the bridge port was last initialized.

Buttons

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

Refresh: Click to refresh the page immediately.

3-9.2 Port Status

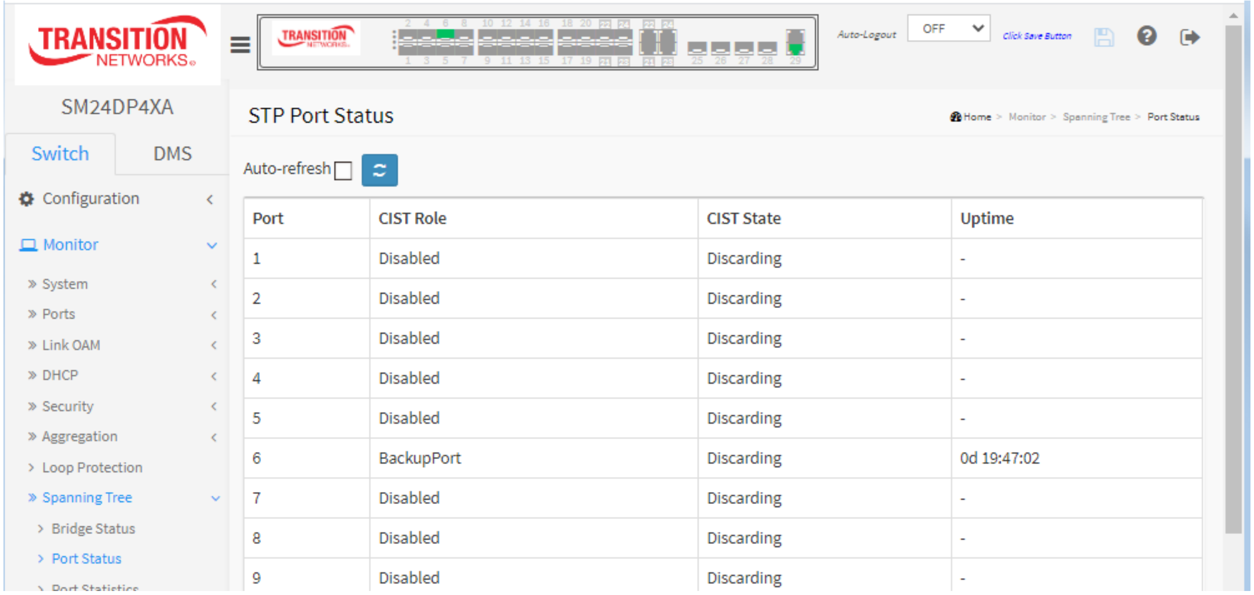
This page displays the STP CIST port status for physical ports of the switch.

Web Interface

To display the STP Port status in the web interface:

1. Click Monitor, Spanning Tree, STP Port Status.
2. View the displayed information.
3. Use the buttons as required.

Figure 3-9.2: STP Port Status



STP Port Status

Auto-refresh □

Port	CIST Role	CIST State	Uptime
1	Disabled	Discarding	-
2	Disabled	Discarding	-
3	Disabled	Discarding	-
4	Disabled	Discarding	-
5	Disabled	Discarding	-
6	BackupPort	Discarding	0d 19:47:02
7	Disabled	Discarding	-
8	Disabled	Discarding	-
9	Disabled	Discarding	-

Parameter descriptions:

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

CIST Role : The current STP port role of the CIST port. The port role can be one of these values: 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 these 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 refresh the page immediately.

3-9.3 Port Statistics

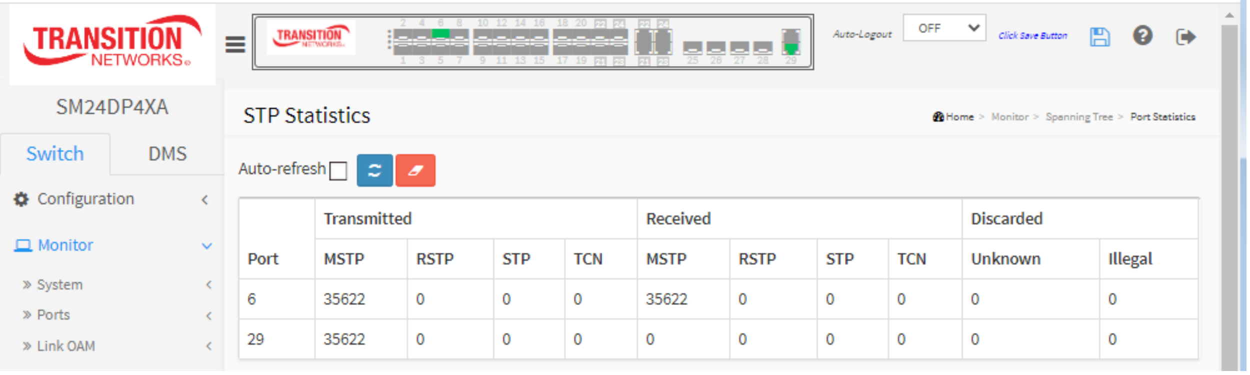
This page displays the STP Statistics detail counters of bridge ports in the currently selected switch.

Web Interface

To display the STP Port status in the web interface:

1. Click Monitor, Spanning Tree, Port Statistics.
2. View the displayed STP statistics.
3. Use the buttons as required.

Figure 3-8.3: STP Statistics



STP Statistics

Auto-refresh □

	Transmitted				Received				Discarded	
Port	MSTP	RSTP	STP	TCN	MSTP	RSTP	STP	TCN	Unknown	Illegal
6	35622	0	0	0	35622	0	0	0	0	0
29	35622	0	0	0	0	0	0	0	0	0

Parameter descriptions:

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

MSTP : The number of MSTP Configuration BPDU's received/transmitted on the port.

RSTP : The number of RSTP Configuration BPDU's received/transmitted on the port.

STP : The number of legacy STP Configuration BPDU's received/transmitted on the port.

TCN : The number of (legacy) Topology Change Notification BPDU's received/transmitted on the port.

Discarded Unknown : The number of unknown Spanning Tree BPDU's received (and discarded) on the port.

Discarded Illegal : The number of illegal Spanning Tree BPDU's received (and discarded) on the port.

Buttons

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

Clear: Clears the counters for the selected port.

Refresh: Click to refresh the page immediately.

3-10 MVR

3-10.1 Statistics

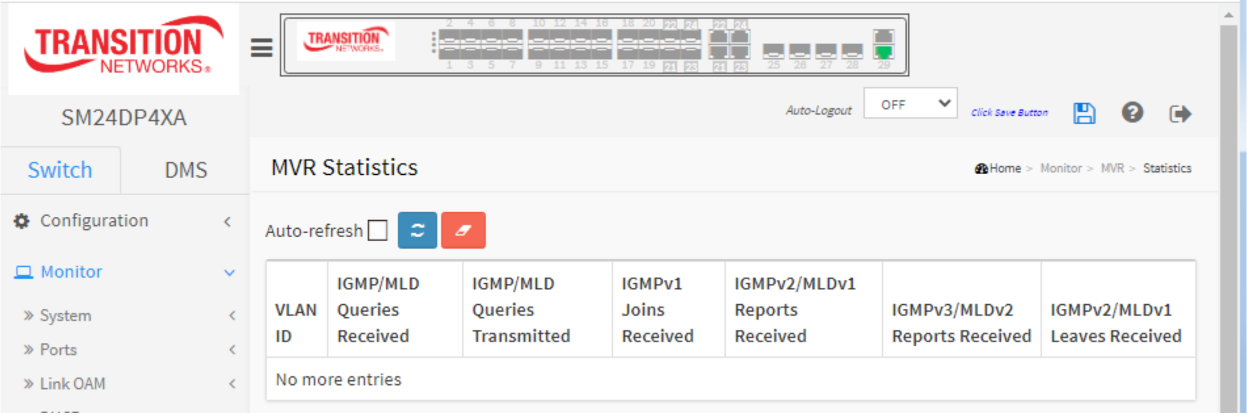
This page displays detailed MVR Statistics Information.

Web Interface

To display the MVR Statistics information in the web interface:

1. Click Monitor, MVR, Statistics.
2. View the displayed statistics.
3. Use the buttons as required.

Figure 3-10.1: MVR Statistics



MVR Statistics

VLAN ID	IGMP/MLD Queries Received	IGMP/MLD Queries Transmitted	IGMPv1 Joins Received	IGMPv2/MLDv1 Reports Received	IGMPv3/MLDv2 Reports Received	IGMPv2/MLDv1 Leaves Received
No more entries						

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.

Clear: Clears the counters for the selected port.

3-10.2 MVR Channels Groups

This page displays entries in the MVR Group table. 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.

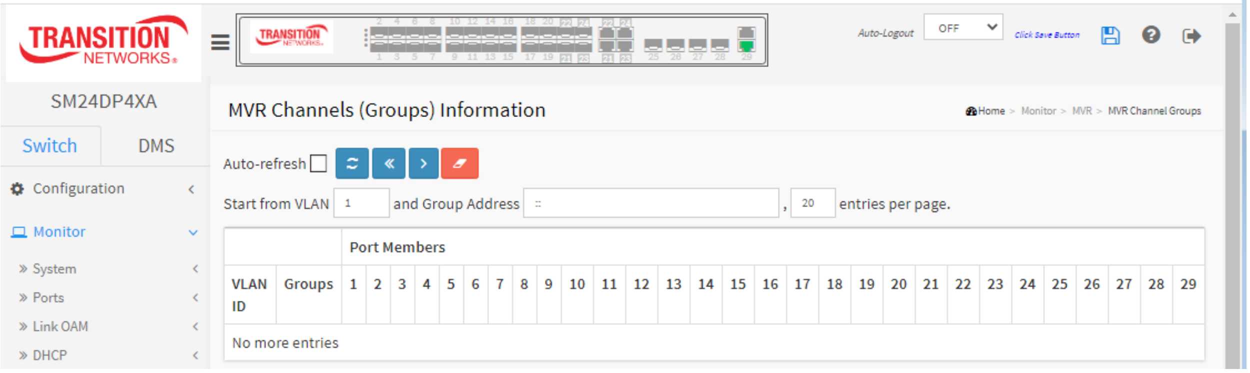
The "Start from VLAN", and "Group Address" input fields allow the user to select the starting point in the MVR Channels (Groups) Information Table. Clicking the **Refresh** button will update the displayed table starting from that or the closest next MVR Channels (Groups) Information Table match. In addition, the two input fields will - upon a **Refresh** button click - assume the value of the first displayed entry, allowing for continuous refresh with the same start address.

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

To display the MVR Groups Information in the web interface:

1. Click Monitor, MVR, MVR Channel Groups.
2. View the displayed information.
3. Use the buttons as required.

Figure 3-10.2: MVR Channels (Groups) Information



MVR Channels (Groups) Information

Auto-refresh □

Start from VLAN 1 and Group Address :: , 20 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	25	26	27	28	29
No more entries																														

Parameter descriptions:

VLAN ID : VLAN ID of the group.

Groups : Group ID of the group displayed.

Port Members : Ports under this group.

Buttons

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

Refresh: Click to refresh the page immediately.

<: Updates the system log entries to the first available entry ID.

> : Updates the system log entry to the next available entry ID.

Clear : Clears the statistics.

3-10.3 MVR SFM Information

The MVR SFM (Source-Filtered Multicast) Information table contains the SSM (Source-Specific Multicast) information. This table is sorted first by VLAN ID, then by group, and then by Port. Different source addresses that belong to the same group are treated as single entry.

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 allow the user to select the starting point in the MVR SFM Information Table. Clicking the **Refresh** button will update the displayed table starting from that or the closest next MVR SFM Information Table match. In addition, the two input fields will - upon a **Refresh** button click - assume the value of the first displayed entry, allowing for continuous refresh with the same start address.

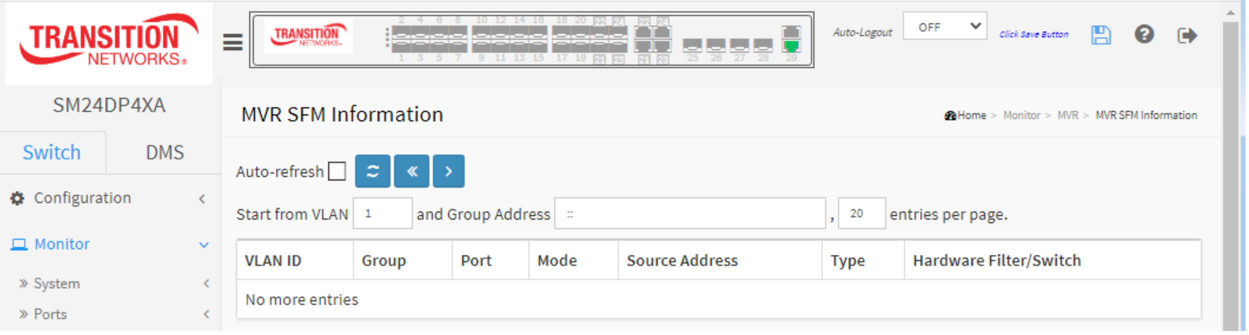
The **>** button will use the last entry of the currently displayed table as a basis for the next lookup. When the end is reached the text "*No more entries*" is shown in the displayed table. Use the **<<** button to start over.

Web Interface

To display the MVR SFM Information in the web interface:

1. Click Monitor, MVR, MVR SFM Information.
2. View the displayed information. If none exists, the table displays *No more entries*.
3. Use the buttons as required.

Figure 3-10.3: MVR SFM Information



MVR SFM Information

Auto-refresh □

Start from VLAN 1 and Group Address :: , 20 entries per page.

VLAN ID	Group	Port	Mode	Source Address	Type	Hardware Filter/Switch
No more entries						

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 chip.

Buttons

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

Refresh: Click to refresh the page.

<<: 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

3-11.1 IGMP Snooping

3-11.1.1 Status

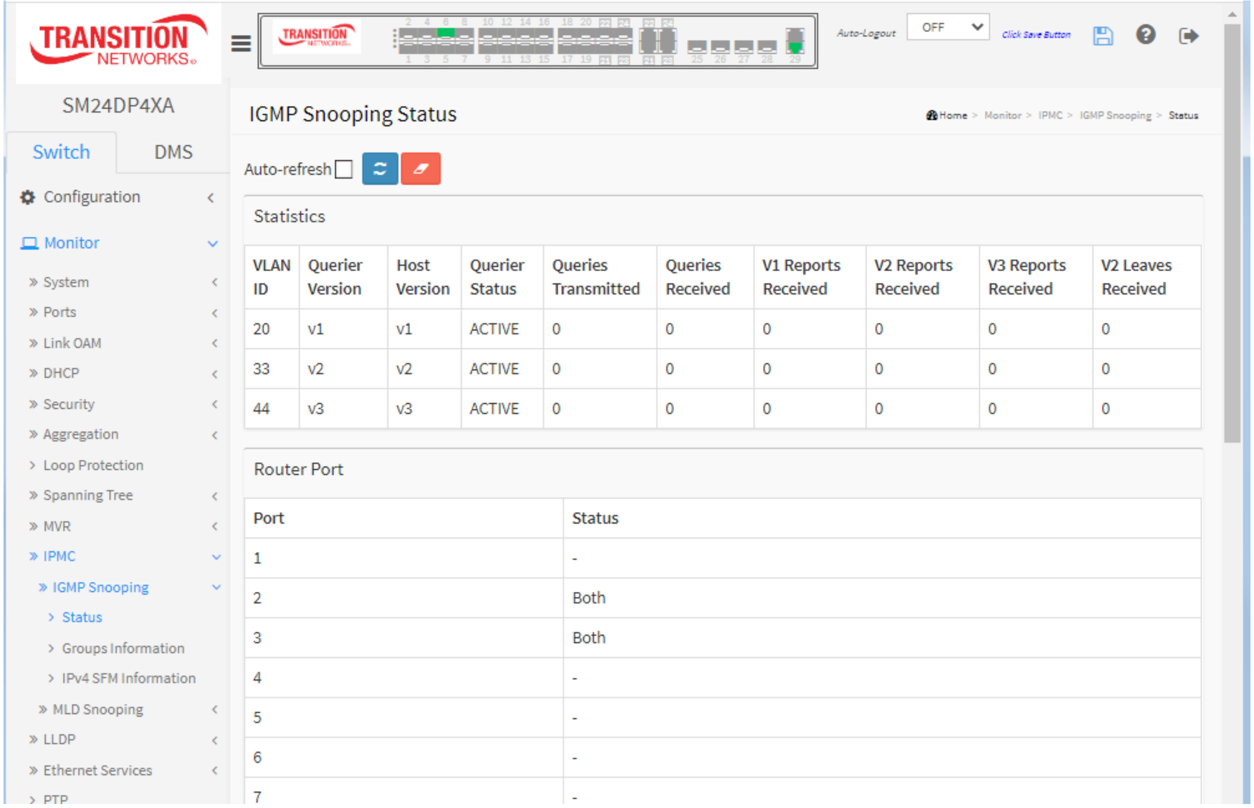
This page displays the IGMP Snooping detail status.

Web Interface

To display the IGMP Snooping status in the web interface:

1. Click Monitor, IPMC, IGMP Snooping, Status.
2. View the displayed information.
3. Use the buttons as required.

Figure 3-10.1.1: IGMP Snooping Status



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
20	v1	v1	ACTIVE	0	0	0	0	0	0
33	v2	v2	ACTIVE	0	0	0	0	0	0
44	v3	v3	ACTIVE	0	0	0	0	0	0

Router Port

Port	Status
1	-
2	Both
3	Both
4	-
5	-
6	-
7	-

Parameter descriptions:

VLAN ID : The VLAN ID of the entry.

Querier Version : Working Querier Version.

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.

Clear: Clears the counters for the selected port.

Refresh: Click to refresh the page immediately.

3-11.1.2 Group Information

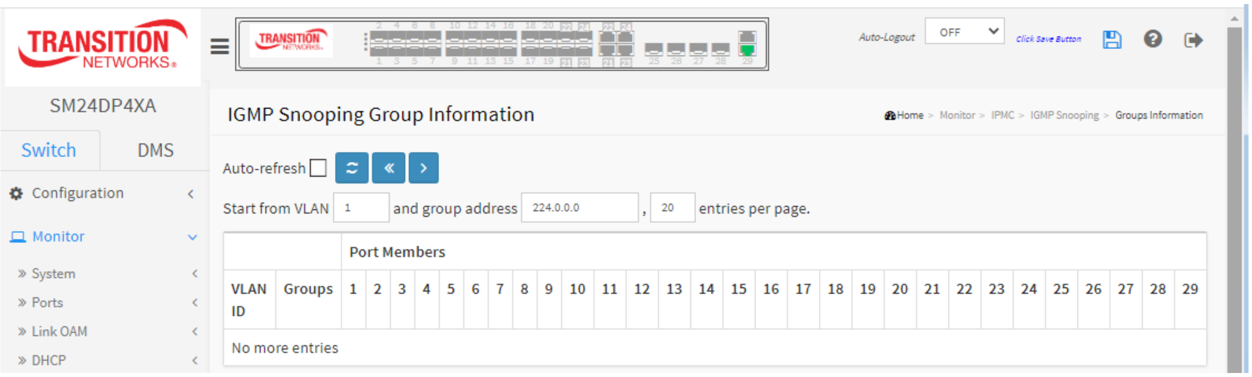
Entries in the IGMP Group Table are shown on this page. The IGMP Group Table is sorted first by VLAN ID, and then by group. The **>** button will use the last entry of the currently displayed table as a basis for the next lookup. When the end is reached the text "*No more entries*" is shown in the displayed table. Use the **<<** button to start over.

Web Interface

To display the IGMP Snooping Group Information in the web interface:

1. Click Monitor, IGMP Snooping, Group Information.
2. View the displayed information.
3. Use the buttons as required.

Figure 3-11.1.2: IGMP Snooping Group Information



IGMP Snooping Group Information

Auto-refresh □ ⟳ « ›

Start from VLAN 1 and group address 224.0.0.0 , 20 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	25	26	27	28	29
No more entries																														

Parameter descriptions:

VLAN ID : VLAN ID of the group.

Groups : Group address of the group displayed.

Port Members : Ports under this group.

Buttons

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

Refresh: Click to refresh the page.

<<: Updates the system log entries to the first available entry ID

> : Updates the system log entry to the next available entry ID

3-11.1.3 IPv4 SFM Information

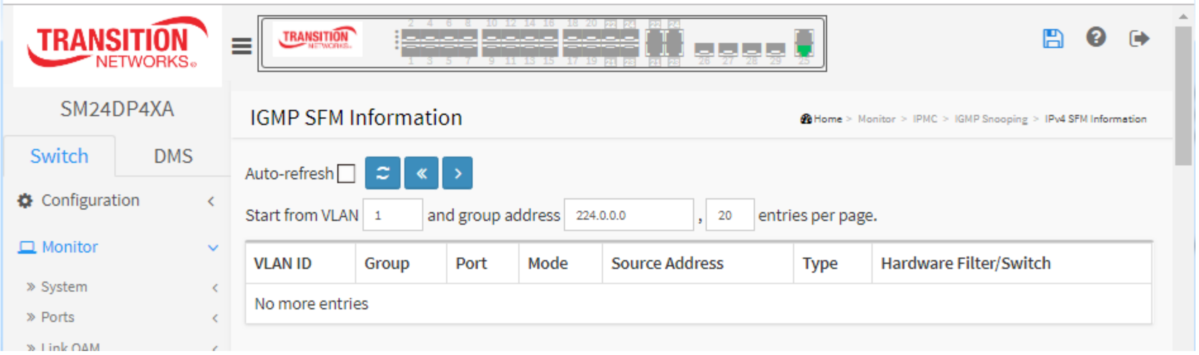
Entries in the IGMP SFM Information Table are shown on this page. The IGMP SFM (Source-Filtered Multicast) Information Table also contains the SSM (Source-Specific Multicast) information. This table is sorted first by VLAN ID, then by group, and then by Port. Different source addresses belong to the same group are treated as single entry.

Web Interface

To display the IPv4 SSM Information in the web interface:

1. Click Monitor, IPMC, IGMP Snooping, IPv4 SSM Information.
2. View the displayed information.
3. Use the buttons as required.

Figure 3-11.1.3: IPv4 SFM Information.



IGMP SFM Information

Auto-refresh □

Start from VLAN 1 and group address 224.0.0.0 , 20 entries per page.

VLAN ID	Group	Port	Mode	Source Address	Type	Hardware Filter/Switch
No more entries						

Parameter descriptions:

VLAN ID : VLAN ID of the group.

Group : Group address of the group displayed.

Port : Switch port number.

Mode : Indicates the filtering mode maintained per (VLAN ID, port number, Group Address) basis. It can be either Include or Exclude.

Source Address : IP Address of the source. Currently, system limits the total number of IP source addresses for filtering to be 128.

Type : Indicates the Type. It can be either Allow or Deny.

Hardware Filter/Switch : Indicates whether data plane destined to the specific group address from the source IPv4 address could be handled by the chip.

Buttons

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

Refresh: Click to refresh the page immediately.

<<: Updates the system log entries to the first available entry ID.

> : Updates the system log entry to the next available entry ID.

3-11.2 MLD Snooping

3-11.2.1 Status

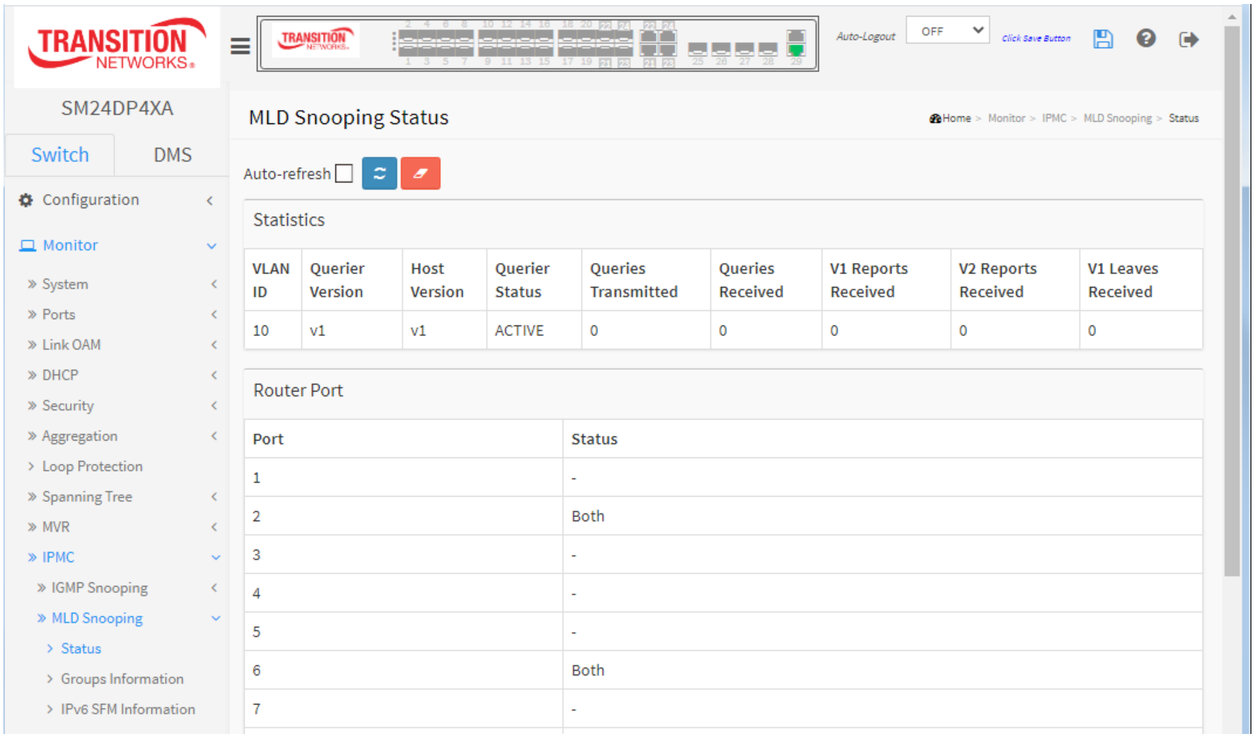
This page displays the MLD Snooping Status and Statistics information.

Web Interface

To display the MLD Snooping Status in the web interface:

1. Click Monitor, IPMC, MLD Snooping, Status.
2. View the displayed information.
3. Use the buttons as required.

Figure 3-11.2.1: MLD Snooping Status



MLD Snooping Status

Auto-refresh □

Statistics

VLAN ID	Querier Version	Host Version	Querier Status	Queries Transmitted	Queries Received	V1 Reports Received	V2 Reports Received	V1 Leaves Received
10	v1	v1	ACTIVE	0	0	0	0	0

Router Port

Port	Status
1	-
2	Both
3	-
4	-
5	-
6	Both
7	-

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.

Buttons

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

Clear: Clears the counters for the selected port.

Refresh: Click to refresh the page immediately.

3-11.2.2 Group Information

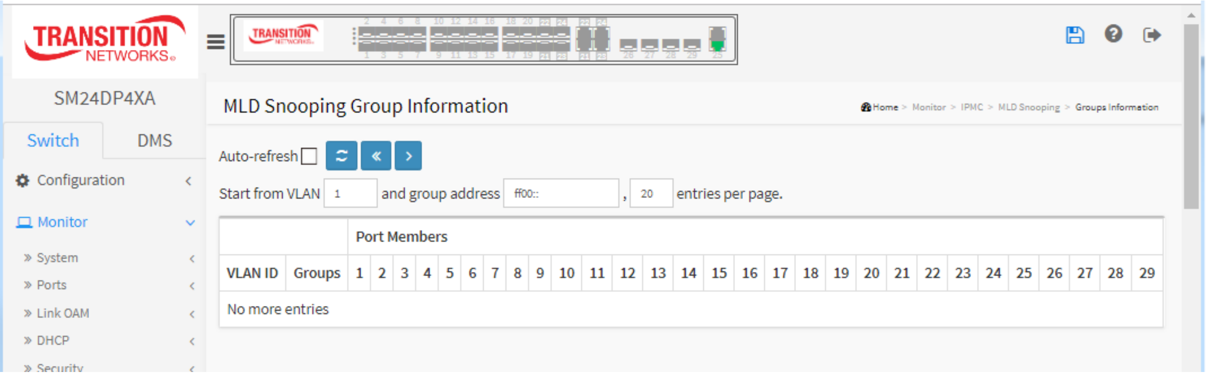
This page displays the MLD Snooping Groups Information.

Web Interface

To display the MLD Snooping Group information in the web interface:

1. Click Monitor, IPMC, MLD Snooping, Group Information
2. View the displayed information.
3. Use the buttons as required.

Figure 3-11.2.2: MLD Snooping Group Information



MLD Snooping Group Information

Auto-refresh □

Start from VLAN 1 and group address ff00:: , 20 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	25	26	27	28	29
No more entries																														

Parameter descriptions:

VLAN ID : VLAN ID of the group.

Groups : Group address of the group displayed.

Port Members : Ports under this group.

Buttons

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

Refresh: Click to refresh the page immediately.

<<: Updates the system log entries to the first available entry ID.

> : Updates the system log entry to the next available entry ID.

3-11.2.3 IPv6 SFM Information

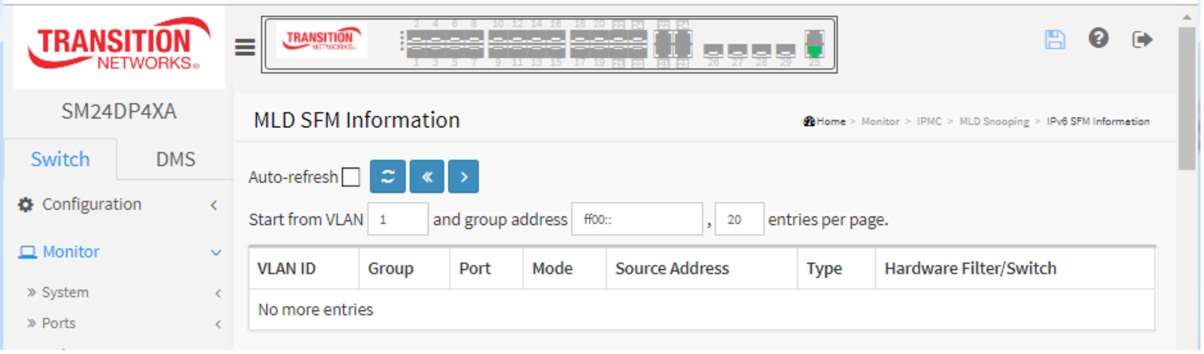
This page displays entries in the MLD SFM Information table. The MLD SFM (Source-Filtered Multicast) Information Table also contains the SSM (Source-Specific Multicast) information. This table is sorted first by VLAN ID, then by group, and then by Port. Different source addresses belong to the same group are treated as single entry.

Web Interface

To display the MLDv2 IPv6 SSM Information in the web interface:

1. Click Monitor, IPMC, MLD Snooping, IPv6 SFM Information.
2. View the displayed information.
3. Use the buttons as required.

Figure 3-11.2.3: IPv6 SFM Information



MLD SFM Information

Auto-refresh □

Start from VLAN 1 and group address ff00:: , 20 entries per page.

VLAN ID	Group	Port	Mode	Source Address	Type	Hardware Filter/Switch
No more entries						

Parameter descriptions:

VLAN ID : VLAN ID of the group.

Group : Group address of the group displayed.

Port : Switch port number.

Mode : Indicates the filtering mode maintained per (VLAN ID, port number, Group Address) basis. It can be either Include or Exclude.

Source Address : IP Address of the source. Currently, system limits the total number of IP source addresses for filtering to be 128.

Type : Indicates the Type. It can be either Allow or Deny.

Hardware Filter/Switch : Indicates whether data plane destined to the specific group address from the source IPv6 address could be handled by chip or not.

Buttons

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

Refresh: Click to refresh the page immediately.

<<: Updates the system log entries to the first available entry ID.

> : Updates the system log entry to the next available entry ID.

3-12 LLDP

3-12.1 Neighbor

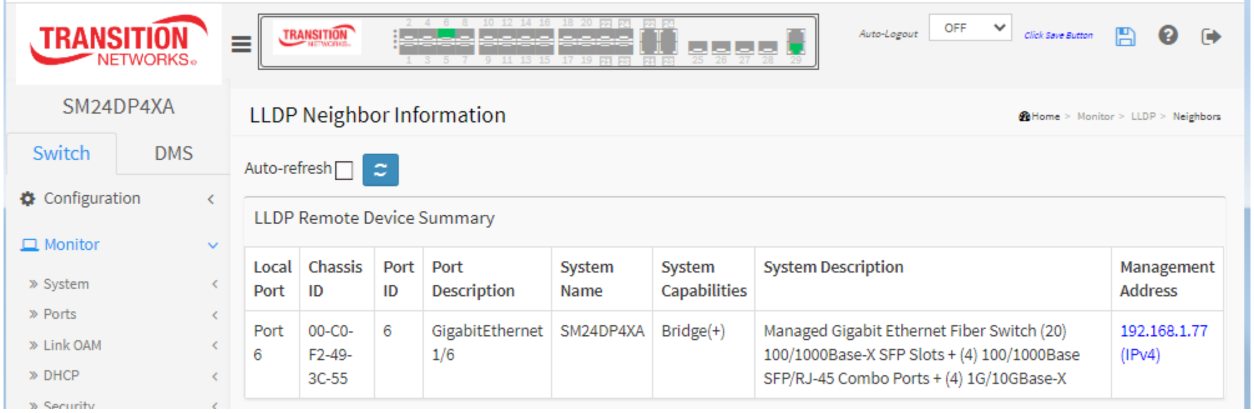
This page provides a status overview for all LLDP neighbors. The displayed table contains a row for each port on which an LLDP neighbor is detected. If your network has no devices that support LLDP then the table will show “*No neighbor information found*”.

Web Interface

To show LLDP neighbors:

1. Click Monitor, LLDP, Neighbors.
2. View the displayed information.
3. Use the buttons as required.

Figure 3-12.1: LLDP Neighbors information



LLDP Neighbor Information

Auto-refresh □

LLDP Remote Device Summary

Local Port	Chassis ID	Port ID	Port Description	System Name	System Capabilities	System Description	Management Address
Port 6	00-C0-F2-49-3C-55	6	GigabitEthernet 1/6	SM24DP4XA	Bridge(+)	Managed Gigabit Ethernet Fiber Switch (20) 100/1000Base-X SFP Slots + (4) 100/1000Base SFP/RJ-45 Combo Ports + (4) 1G/10GBase-X	192.168.1.77 (IPv4)

Parameter descriptions:

Local Interface : 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, including:

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

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

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

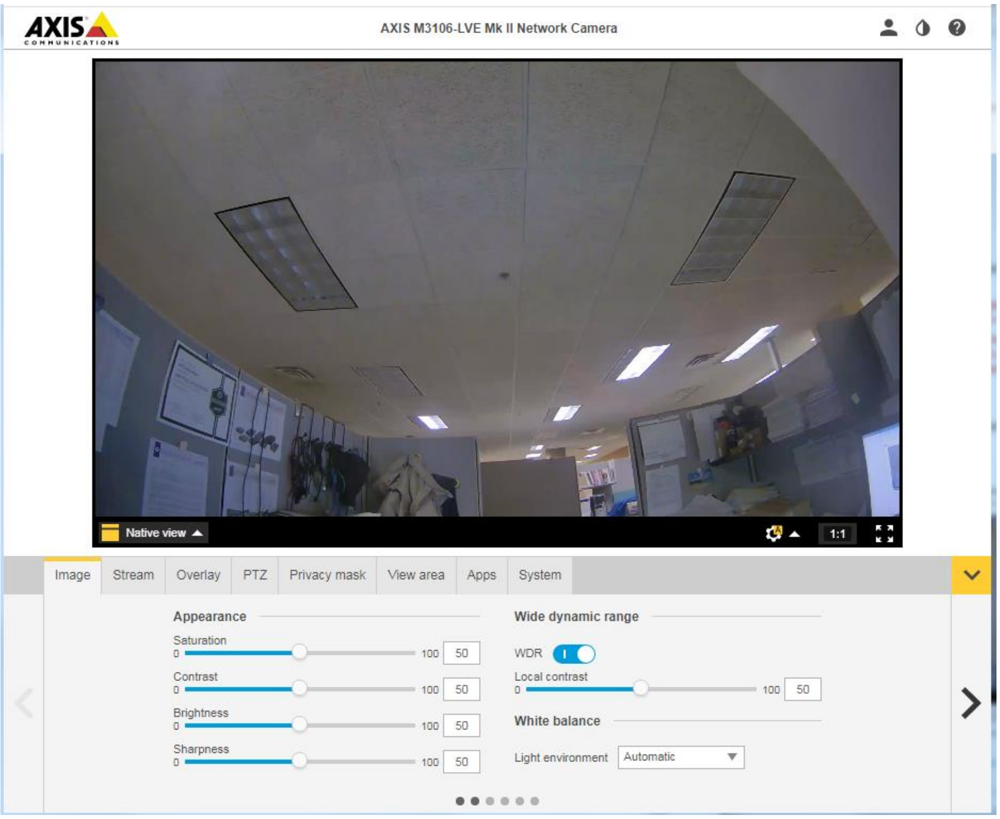
Management Address : The neighbor unit's address that is used for higher layer entities to assist discovery by the network management. This could for instance hold the neighbors' IP address. Click the linked IP address to display its related information. Click the linked IP address to display neighbor unit information (see below).

Buttons

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

Refresh: Click to refresh the page immediately.

You can click a linked IP address in the Management Address column to display neighbor unit information:



Appearance

Saturation 0 100 50

Contrast 0 100 50

Brightness 0 100 50

Sharpness 0 100 50

Wide dynamic range

WDR I

Local contrast 0 100 50

White balance

Light environment Automatic

3-12.2 LLDP-MED Neighbor

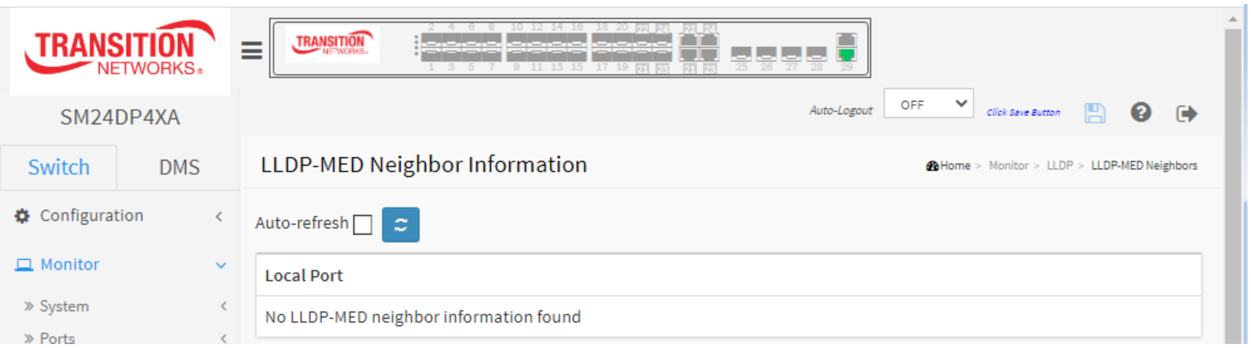
This page provides a status overview of all LLDP-MED neighbors. The displayed table contains a row for each port on which an LLDP neighbor is detected. This function applies to devices that support LLDP-MED.

Web Interface

To show LLDP-MED neighbor information:

1. Click Monitor, LLDP, LLDP-MED Neighbor.
2. View the displayed information.
3. Use the buttons as required.

Figure 3-12.2: LLDP-MED Neighbor information



LLDP-MED Neighbor Information

Auto-refresh □

Local Port
No LLDP-MED neighbor information found

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:

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

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

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

Each LLDP-MED Endpoint Device Class is defined to build upon the capabilities defined for the previous Endpoint Device Class. For-example will any LLDP-MED Endpoint Device claiming compliance as a Media

Endpoint (Class II) also support all aspects of TIA-1057 applicable to Generic Endpoints (Class I), and any LLDP-MED Endpoint Device claiming compliance as a Communication Device (Class III) will also support all aspects of TIA-1057 applicable to both Media Endpoints (Class II) and Generic Endpoints (Class I).

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Buttons

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

Refresh: Click to refresh the page immediately.

3-12.3 Port Statistics

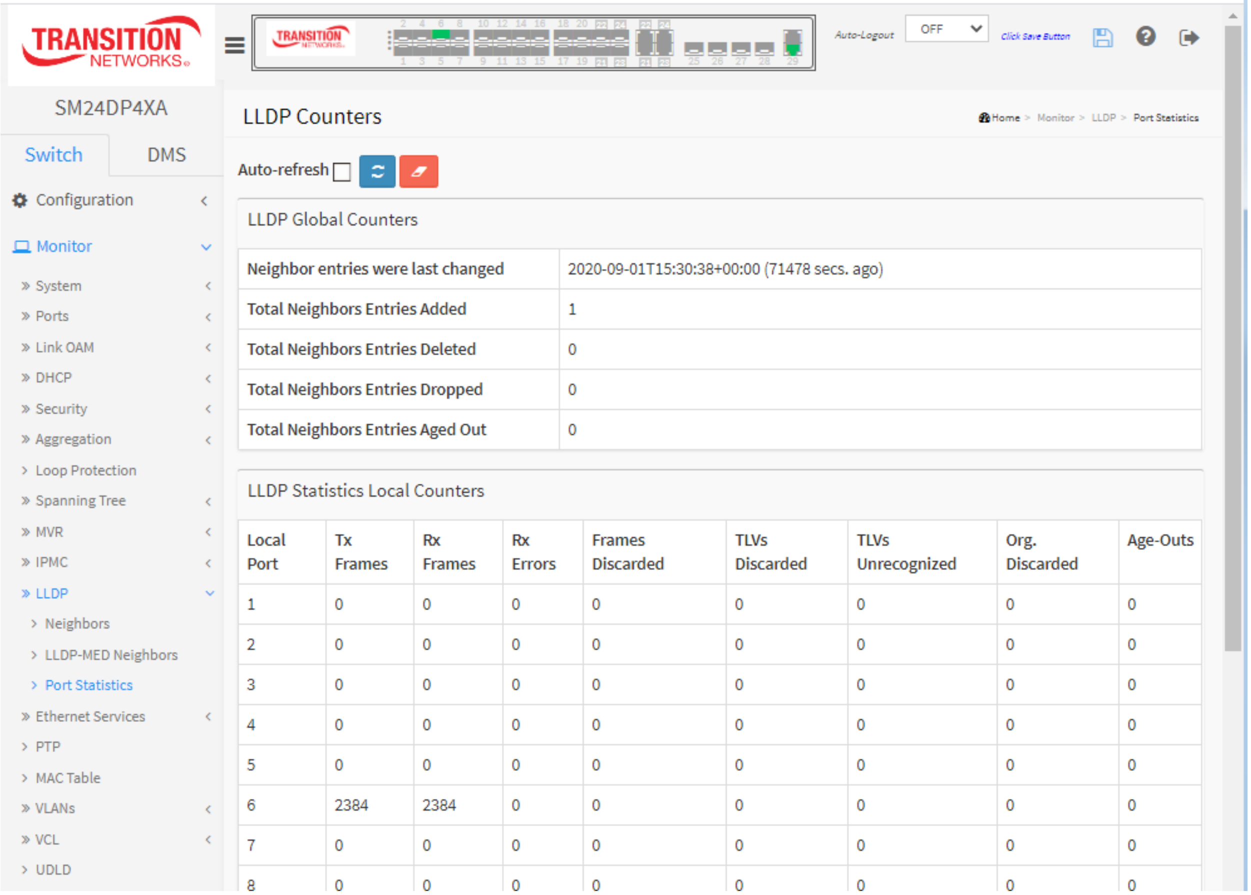
Two types of counters are shown. *Global* counters are counters that refer to the whole switch, while *Local* counters refer to per port counters for the currently selected switch

Web Interface

To show LLDP Statistics:

1. Click Monitor, LLDP, Port Statistics.
2. View the displayed information.
3. Use the buttons as required.

Figure 3-12.3: LLDP Port Statistics information



LLDP Counters

Auto-refresh □

LLDP Global Counters

Neighbor entries were last changed	2020-09-01T15:30:38+00:00 (71478 secs. ago)
Total Neighbors Entries Added	1
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
5	0	0	0	0	0	0	0	0
6	2384	2384	0	0	0	0	0	0
7	0	0	0	0	0	0	0	0
8	0	0	0	0	0	0	0	0

Parameter descriptions:

Global Counters

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

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

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

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

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

Local Counters : The displayed table contains a row for each port. The columns 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 Neighbours" 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.

Clear: Clears the counters for the selected port.

Refresh: Click to refresh the page immediately.

3-13 Ethernet Services

3-13.1 EVC Statistics

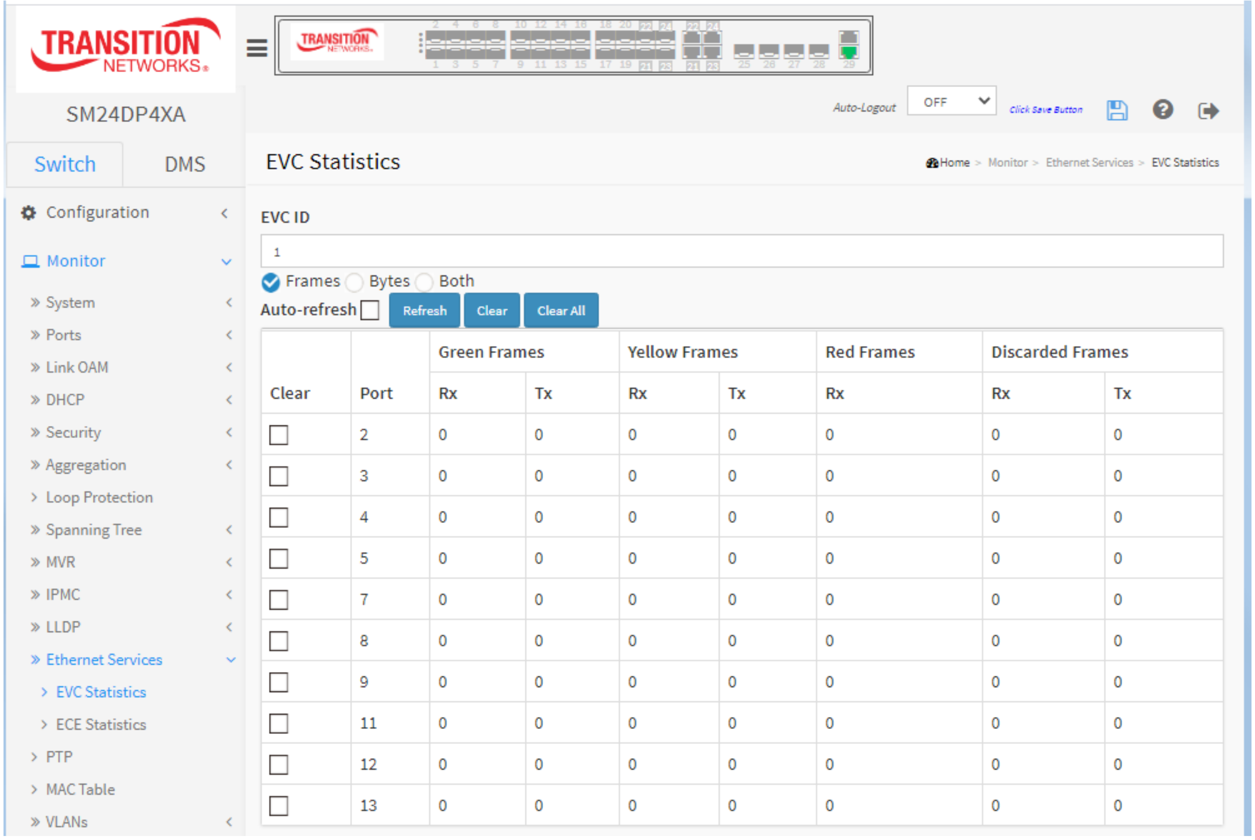
This page provides NNI port traffic statistics for the selected EVC. It also shows counters for UNI ports of ECEs mapping to the EVC.

Web Interface

To display EVC Statistics in the web interface:

1. Click Monitor, Ethernet Services, EVC Statistics.
2. View the displayed information.
3. Use the buttons and radio buttons as required.

Figure 3-13.1: EVC Statistics



EVC Statistics

EVC ID: 1

● Frames ○ Bytes ○ Both

Auto-refresh □

		Green Frames		Yellow Frames		Red Frames	Discarded Frames	
Clear	Port	Rx	Tx	Rx	Tx	Rx	Rx	Tx
□	2	0	0	0	0	0	0	0
□	3	0	0	0	0	0	0	0
□	4	0	0	0	0	0	0	0
□	5	0	0	0	0	0	0	0
□	7	0	0	0	0	0	0	0
□	8	0	0	0	0	0	0	0
□	9	0	0	0	0	0	0	0
□	11	0	0	0	0	0	0	0
□	12	0	0	0	0	0	0	0
□	13	0	0	0	0	0	0	0

Parameter descriptions:

Clear : This box is used to mark a port for clearance in next Clear operation.

Port : The UNI/NNI port for the EVC.

Rx Green : The number of green frames received.

Tx Green : The number of green frames transmitted.

Rx Yellow : The number of yellow frames received.

Tx Yellow : The number of yellow frames transmitted.

Rx Red : The number of red frames received.

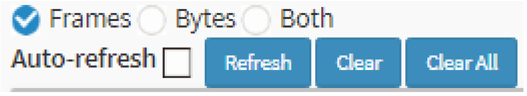
Rx Discarded : The number of discarded frames in the ingress queue system.

Tx Discarded : The number of discarded frames in the egress queue system.

Rx Discarded : The number of discarded frames in the ingress queue system.

Tx Discarded : The number of discarded frames in the egress queue system.

Buttons



Frames: Show frames statistics only.

Bytes: Show bytes statistics only.

Both: Show both frames and bytes statistics.

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

Refresh: Click to refresh the page immediately.

Clear: Clears the counters for the selected port.

Clear All: Clears the counters for all ports.

3-13.2 ECE Statistics

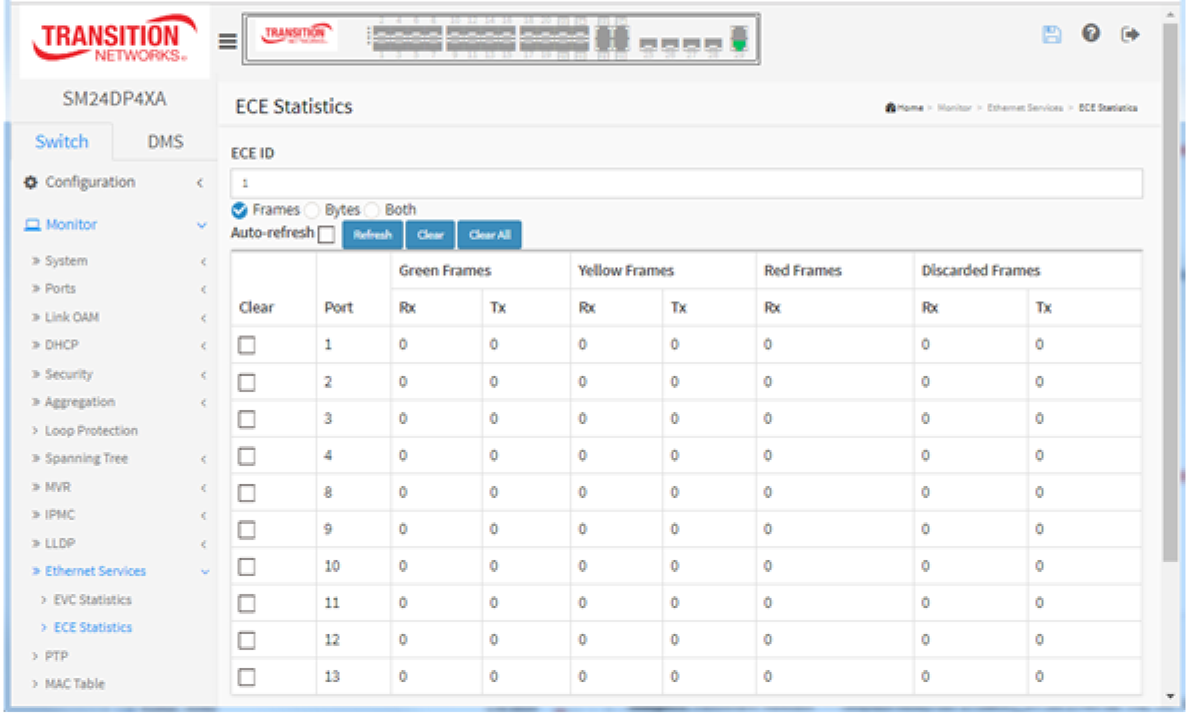
This page provides UNI port traffic statistics for available ECEs. It also shows counters for NNI ports of the EVC to which the ECE is mapped.

Web Interface

To display ECE Statistics in the web interface:

1. Click Monitor, Ethernet Services, ECE Statistics.
2. Enter the desired ECE ID.
3. Select Frames, Bytes, or Both .
4. Click the buttons as required.

Figure 3-13.2: ECE Statistics



ECE Statistics

ECE ID

1

● Frames ○ Bytes ○ Both

Auto-refresh □ Refresh Clear Clear All

		Green Frames		Yellow Frames		Red Frames	Discarded Frames	
Clear	Port	Rx	Tx	Rx	Tx	Rx	Rx	Tx
□	1	0	0	0	0	0	0	0
□	2	0	0	0	0	0	0	0
□	3	0	0	0	0	0	0	0
□	4	0	0	0	0	0	0	0
□	8	0	0	0	0	0	0	0
□	9	0	0	0	0	0	0	0
□	10	0	0	0	0	0	0	0
□	11	0	0	0	0	0	0	0
□	12	0	0	0	0	0	0	0
□	13	0	0	0	0	0	0	0

Parameter descriptions:

ECE ID : Displays the available ECE ID.

Clear : Check this box to mark a port for statistics to be cleared in next Clear operation.

Port : The UNI/NNI port for the EVC.

Rx Green Frames and Bytes : The number of green bytes and frames received.

Tx Green Frames and Bytes : The number of green bytes and frames transmitted.

Rx Yellow Frames and Bytes : The number of yellow bytes and frames received.

Tx Yellow Frames and Bytes : The number of yellow bytes and frames transmitted.

Rx Red Frames and Bytes : The number of red bytes and frames received.

Rx Discarded Frames and Bytes : The number of bytes and frames discarded in the ingress queue system.

Tx Discarded Frames and Bytes : The number of bytes and frames discarded in the egress queue system.

Buttons

Frames: Show frames statistics only.

Bytes: Show bytes statistics only.

Both: Show both frames and bytes statistics.

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

Refresh: Click to refresh the page.

Clear: Clears the counters for the selected port.

Clear All: Clears the counters for all ports.

3-14 PTP

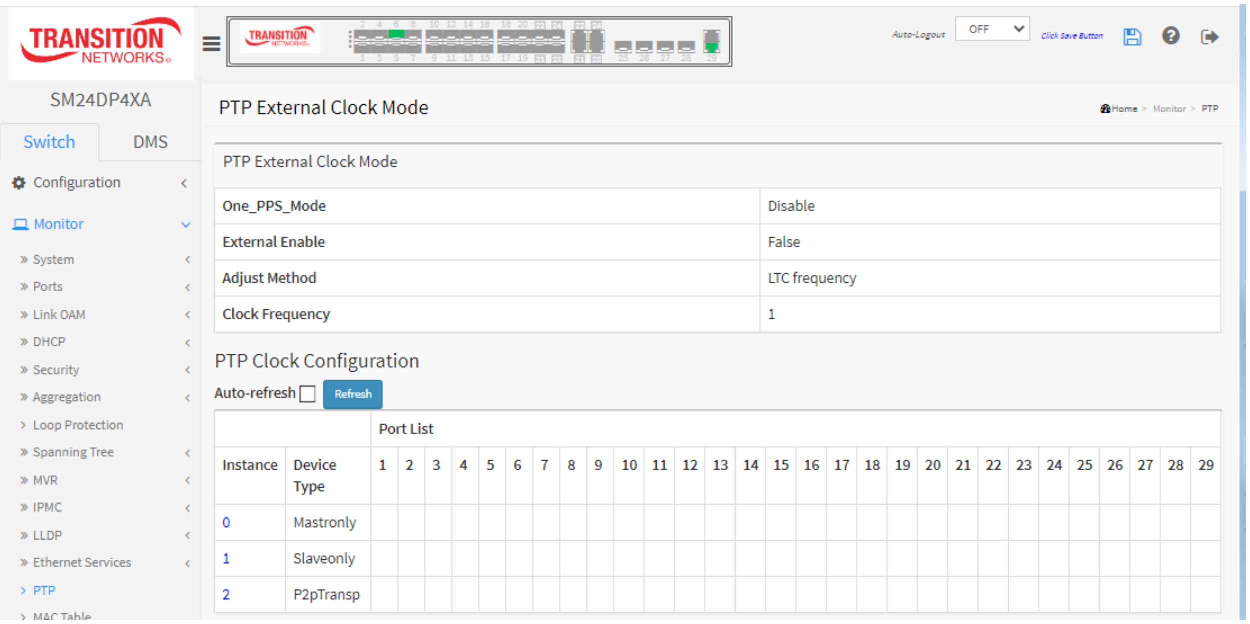
This page lets you view the current PTP clock settings.

Web Interface

To view PTP External Clock Mode via the web interface:

1. Click Monitor, PTP.
2. View the displayed information.
3. Click the linked instance numbers and/or buttons as required.

Figure 3-14: PTP External Clock Mode



PTP External Clock Mode

PTP External Clock Mode	
One_PPS_Mode	Disable
External Enable	False
Adjust Method	LTC frequency
Clock Frequency	1

PTP Clock Configuration

Auto-refresh □ Refresh

		Port List																												
Instance	Device Type	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29
0	Mastronly																													
1	Slaveonly																													
2	P2pTransp																													

Parameter descriptions:

<u>PTP External Clock Description</u>

One_pps_mode : Shows the current One_pps_mode configured.

Output : Enable the 1 pps clock output

Input : Enable the 1 pps clock input

Disable : Disable the 1 pps clock in/out-put

External Enable : Shows the current External clock output configuration.

True : Enable the external clock output

False : Disable the external clock output

VCXO_Enable : Shows the current VCXO rate adjustment configuration.

True : Enable the external VCXO rate adjustment

False : Disable the external VCXO rate adjustment

Clock Frequency : Shows the current clock frequency used by the External Clock. The possible values are 1 - 25000000 (1 - 25MHz).

PTP Clock Description

Clock Instance : Indicates the Instance of a particular Clock Instance [0..3]. Click on the linked Clock Instance number to display the Clock details. See below.

Device Type : Indicates the Type of the Clock Instance. There are five Device Types.

Ord-Bound - Clock's Device Type is Ordinary-Boundary Clock.

P2p Transp - Clock's Device Type is Peer to Peer Transparent Clock.

E2e Transp - Clock's Device Type is End to End Transparent Clock.

Master Only - Clock's Device Type is Master Only.

Slave Only - Clock's Device Type is Slave Only.

Displays "*No Clock Instances Present*" if no PTP clock instances are currently configured.

Port List : Shows the ports configured for that Clock Instance.

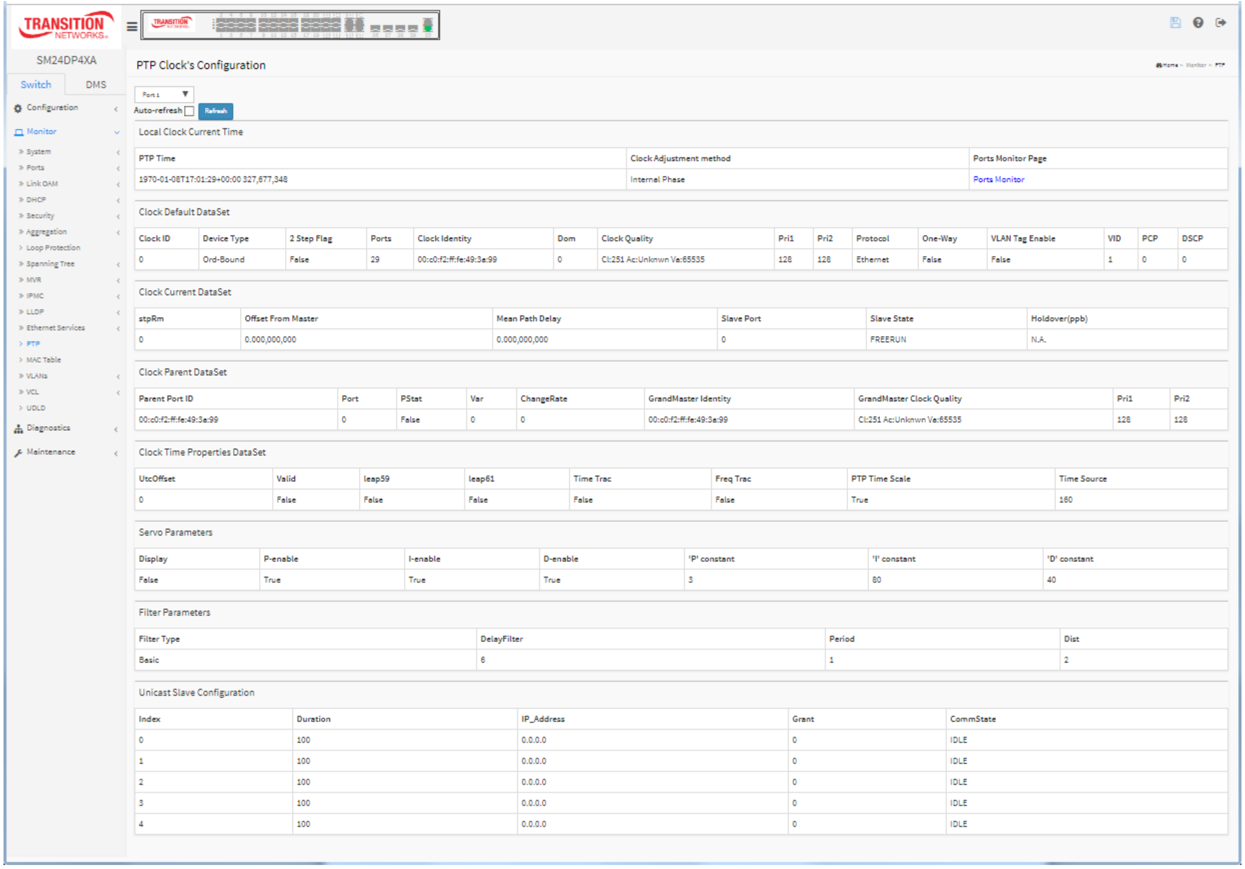
Buttons

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

Refresh: Click to refresh the page immediately.

PTP Clock's Configuration

When you click on the Clock Instance number the Clock details display. This page allows the user to inspect the current PTP clock settings.



PTP Clock's Configuration

Auto-refresh □

Local Clock Current Time

PTP Time	Clock Adjustment method	Ports Monitor Page
1970-01-08T17:01:29+00:00 327,677,348	Internal Phase	Ports Monitor

Clock Default DataSet

Clock ID	Device Type	2 Step Flag	Ports	Clock Identity	Dom	Clock Quality	Pri1	Pri2	Protocol	One-Way	VLAN Tag Enable	VID	PCP	DSCP
0	Ord-Bound	False	29	00:c0:f2:ff:fe:49:3a:99	0	Cl:251 Ac:Unknwn Va:65535	128	128	Ethernet	False	False	1	0	0

Clock Current DataSet

stpRm	Offset From Master	Mean Path Delay	Slave Port	Slave State	Holdover(ppb)
0	0.000,000,000	0.000,000,000	0	FREERUN	N.A.

Clock Parent DataSet

Parent Port ID	Port	PStat	Var	ChangeRate	GrandMaster Identity	GrandMaster Clock Quality	Pri1	Pri2
00:c0:f2:ff:fe:49:3a:99	0	False	0	0	00:c0:f2:ff:fe:49:3a:99	Cl:251 Ac:Unknwn Va:65535	128	128

Clock Time Properties DataSet

UtcOffset	Valid	leap59	leap61	Time Trac	Freq Trac	PTP Time Scale	Time Source
0	False	False	False	False	False	True	160

Servo Parameters

Display	P-enable	I-enable	D-enable	'P' constant	'I' constant	'D' constant
False	True	True	True	3	80	40

Filter Parameters

Filter Type	DelayFilter	Period	Dist
Basic	6	1	2

Unicast Slave Configuration

Index	Duration	IP_Address	Grant	CommState
0	100	0.0.0.0	0	IDLE
1	100	0.0.0.0	0	IDLE
2	100	0.0.0.0	0	IDLE
3	100	0.0.0.0	0	IDLE
4	100	0.0.0.0	0	IDLE

Parameter descriptions:

Local Clock Current time : Show local clock data

PTP Time : Shows the actual PTP time with nanosecond resolution.

Clock Adjustment Method : Shows the actual clock adjustment method. The method depends on the available hardware.

Ports Monitor Page : Click to monitor the port data set for the ports assigned to this clock instance.

Clock Default Dataset : The clock default data set is defined in the IEEE 1588 Standard. It holds three groups of data: the static members defined at clock creation time, the dynamic members defined by the system, and configurable members which can be set here.

Clock ID : An internal instance id (0..3)

Device Type : Indicates the Type of the Clock Instance. There are five Device Types.

Ord-Bound - Clock's Device Type is Ordinary-Boundary Clock.

P2p Transp - Clock's Device Type is Peer to Peer Transparent Clock.

E2e Transp - Clock's Device Type is End to End Transparent Clock.

Master Only - Clock's Device Type is Master Only.

Slave Only - Clock's Device Type is Slave Only.

2 Step Flag : True if two-step Sync events and Pdelay_Resp events are used

Ports : The total number of physical ports in the node

Clock Identity : It shows unique clock identifier

Dom : Clock domain [0..127].

Clock Quality : The clock quality is determined by the system, and holds 3 parts: Clock Class, Clock Accuracy and OffsetScaledLog Variance as defined in IEEE1588. The Clock Accuracy values are defined in IEEE1588 table 6 (Currently the clock Accuracy is set to 'Unknown' as default).

Pri1 : Clock priority 1 [0..255] used by the BMC master select algorithm.

Pri2 : Clock priority 2 [0..255] used by the BMC master select algorithm.

Protocol : Transport protocol used by the PTP protocol engine

Ethernet PTP over Ethernet multicast
ip4multi PTP over IPv4 multicast
ip4uni PTP over IPv4 unicast

Note : IPv4 unicast protocol only works in Master only and Slave only clocks. See parameter Device Type.

In a unicast Slave only clock you also need configure which master clocks to request Announce and Sync messages from. See: Unicast Slave Configuration

One-Way : If true, one-way measurements are used. This parameter applies only to a slave. In one-way mode no delay measurements are performed, i.e. this is applicable only if frequency synchronization is needed. The master always responds to delay requests.

VLAN Tag Enable : Enables the VLAN tagging for the PTP frames. **Note**: Packets are only tagged if the port is configured for VLAN tagging for the configured VLAN (i.e., the VLAN Tag Enable parameter is ignored).

VID : VLAN Identifier used for tagging the PTP frames.

PCP : Priority Code Point value used for PTP frames.

Clock current Data Set : The clock current data set is defined in the IEEE 1588 Standard. The current data set is dynamic

stpRm : Steps Removed : It is the number of PTP clocks traversed from the grandmaster to the local slave clock.

Offset from master : Time difference between the master clock and the local slave clock, measured in ns.

mean Path Delay : The mean propagation time for the link between the master and the local slave

Slave Port : Shows which port is in slave mode. The value is 0 if no ports are in slave mode.

Slave State : Shows synchronization state of the slave.

Holdover(pbb) : After the slave has been in Locked mode during the stabilization period, this value shows the actual clock offset between the freerun and the actual holdover frequency, the value is shown in parts pr billion (ppb). During the stabilization period, the value is shown as N.A. The stabilization period is 60 sec as default, it can be changed from the CLI interface.

Clock Parent Data Set : The clock parent data set is defined in the IEEE 1588 standard. The parent data set is dynamic.

Parent Port ID : Clock identity for the parent clock, if the local clock is not a slave, the value is the clocks own id.

Port : Port Id for the parent master port

PStat : Parents Stats (always false).

Var : It is observed parent offset scaled log variance

Change Rate : Observed Parent Clock Phase Change Rate. i.e. the slave clocks rate offset compared to the master. (unit = ns per s).

Grand Master Identity : Clock identity for the grand master clock, if the local clock is not a slave, the value is the clocks own id.

Grand Master Clock Quality : The clock quality announced by the grand master (See description of Clock Default DataSet:Clock Quality)

Pri1 : Clock priority 1 announced by the grand master

Pri2 : Clock priority 2 announced by the grand master.

Clock Time Properties Data Set : The clock time properties data set is defined in the IEEE 1588 Standard. The data set is both configurable and dynamic, i.e. the parameters can be configured for a grandmaster. In a slave clock the parameters are overwritten by the grandmasters timing properties. The parameters are not used in the current PTP implementation.

The valid values for the Time Source parameter are:

16 (0x10) ATOMIC_CLOCK
32 (0x20) GPS
48 (0x30) TERRESTRIAL_RADIO
64 (0x40) PTP
80 (0x50) NTP
96 (0x60) HAND_SET
144 (0x90) OTHER
160 (0xA0) INTERNAL_OSCILLATOR

Servo Parameters : The default clock servo uses a PID regulator to calculate the current clock rate. i.e.
clockAdjustment =
OffsetFromMaster/ P constant +
Integral(OffsetFromMaster)/ I constant +
Differential OffsetFromMaster)/ D constant

Display : If true then Offset From Master, MeanPathDelay and clockAdjustment are logged on the debug terminal.

P-enable : If true the P part of the algorithm is included.

I-Enable : If true the I part of the algorithm is included.

D-enable : If true the D part of the algorithm is included.

'P' constant : [1..1000] see above.

'I' constant : [1..10000] see above.

'D' constant : [1..10000] see above.

Filter Parameters : The default delay filter is a low pass filter, with a time constant of 2***DelayFilter***DelayRequestRate.

If the DelayFilter parameter is set to 0, the delay filter uses the same algorithm as the offset filter. The default offset filter uses a minimum offset or a mean filter method i.e. The minimum measured offset during **Period** samples is used in the calculation. The distance between two calculations is **Dist** periods.
If **Dist** is 1 the offset is averaged over the **Period**,
If **Dist** is >1 the offset is calculated using 'min' offset.

DelayFilter : See above

Filter Type : Shows the filter type used which can be either the basic filter or an advanced filter that can be configured to use only a fraction of the packets received (i.e. the packets that have experienced the least latency).

Period : See above

dist : See above

Height : The height of the sample window measured in microseconds (only applicable to advanced offset filter).

Percentage : The percentage of sync packets (with smallest delay) used by the offset filter (only applicable to advanced offset filter).

Reset Threshold : The threshold in micro seconds at which the offset filter will be reset and the slave clock synchronized to the master.

Unicast Slave Configuration : When operating in IPv4 Unicast mode, the slave is configured with up to five master IP addresses. The slave then requests Announce messages from all the configured masters. The slave uses the BMC algorithm to select one as master clock, the slave then request Sync messages from the selected master.

Duration : The number of seconds a master is requested to send Announce/Sync messages. The request is repeated from the slave each Duration/4 seconds.

IP_address : IPv4 Address of the master clock.

grant : The granted repetition period for the sync message

CommState : The state of the communication with the master; possible values are:

IDLE : The entry is not in use.

INIT : Announce is sent to the master (Waiting for a response).

CONN : The master has responded.

SELL : The assigned master is selected as current master.

SYNC : The master is sending Sync messages.

Buttons

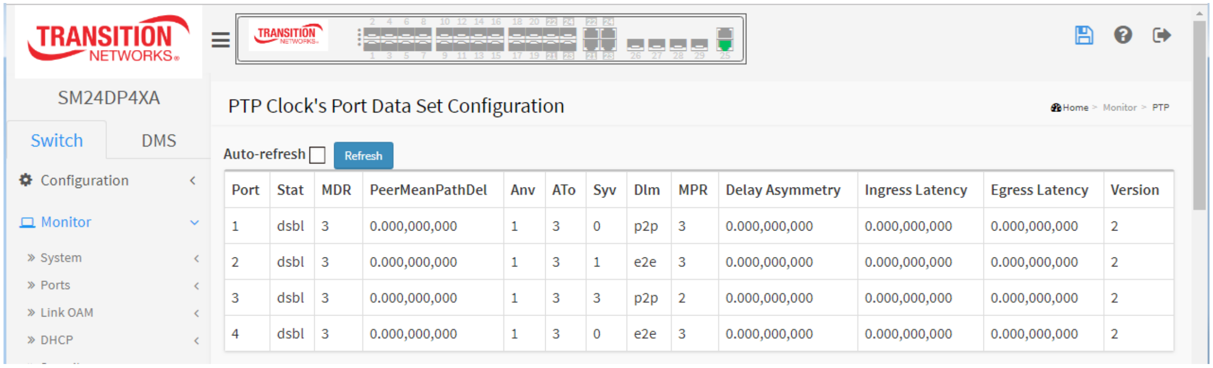
Auto-refresh□ : Check this box to refresh the page automatically every 3 seconds.

Refresh : Click to refresh the page immediately.

: **Port select box** : At the dropdown select the port to be displayed.

PTP Clock's Port Data Set Configuration page

At the PTP Clock's Configuration page, click the linked Ports Monitor text to display the PTP Clock's Port Data Set Configuration page. The port data set is defined in the IEEE 1588 Standard.



PTP Clock's Port Data Set Configuration

Auto-refresh □ Refresh

Port	Stat	MDR	PeerMeanPathDel	Anv	ATo	Syv	Dlm	MPR	Delay Asymmetry	Ingress Latency	Egress Latency	Version
1	dsbl	3	0.000,000,000	1	3	0	p2p	3	0.000,000,000	0.000,000,000	0.000,000,000	2
2	dsbl	3	0.000,000,000	1	3	1	e2e	3	0.000,000,000	0.000,000,000	0.000,000,000	2
3	dsbl	3	0.000,000,000	1	3	3	p2p	2	0.000,000,000	0.000,000,000	0.000,000,000	2
4	dsbl	3	0.000,000,000	1	3	0	e2e	3	0.000,000,000	0.000,000,000	0.000,000,000	2

Parameter descriptions:

Port : Port number [1..max port no].

Stat : Current state of the port.

MDR : log Min Delay Req Interval: The delay request interval announced by the master.

Peer Mean Path Del : The path delay measured by the port in P2P mode. In E2E mode this value is 0.

Anv : The interval for issuing announce messages in master state.

ATo : The timeout for receiving announce messages on the port.

Syv : The interval for issuing sync messages in master.

Dlm : delayMechanism: The delay mechanism used for the port:

- ***e2e*** : End to end delay measurement.
- ***p2p*** : Peer to peer delay measurement.

MPR : The interval for issuing Delay_Req messages for the port in E2e mode. This value is announced from the master to the slave in an announce message. The value is reflected in the MDR field in the Slave

The interval for issuing Pdelay_Req messages for the port in P2P mode.

Note: The interpretation of this parameter has changed from release 2.40. In earlier versions the value was interpreted relative to the Sync interval, this was a violation of the standard, so now the value is interpreted as an interval. I.e. MPR = 0 => 1 Delay_Req pr sec, independent of the Sync rate.

Delay Asymmetry : The transmission delay asymmetry for a link. See IEEE 1588 Section 7.4.2 Communication path asymmetry.

Version : The current implementation only supports PTP version 2.

Ingress latency : Ingress latency measured in ns, as defined in IEEE 1588 Section 7.3.4.2.

Egress Latency : Egress latency measured in ns, as defined in IEEE 1588 Section 7.3.4.2.

Buttons

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

Refresh : Click to refresh the page immediately.

3-15 MAC Table

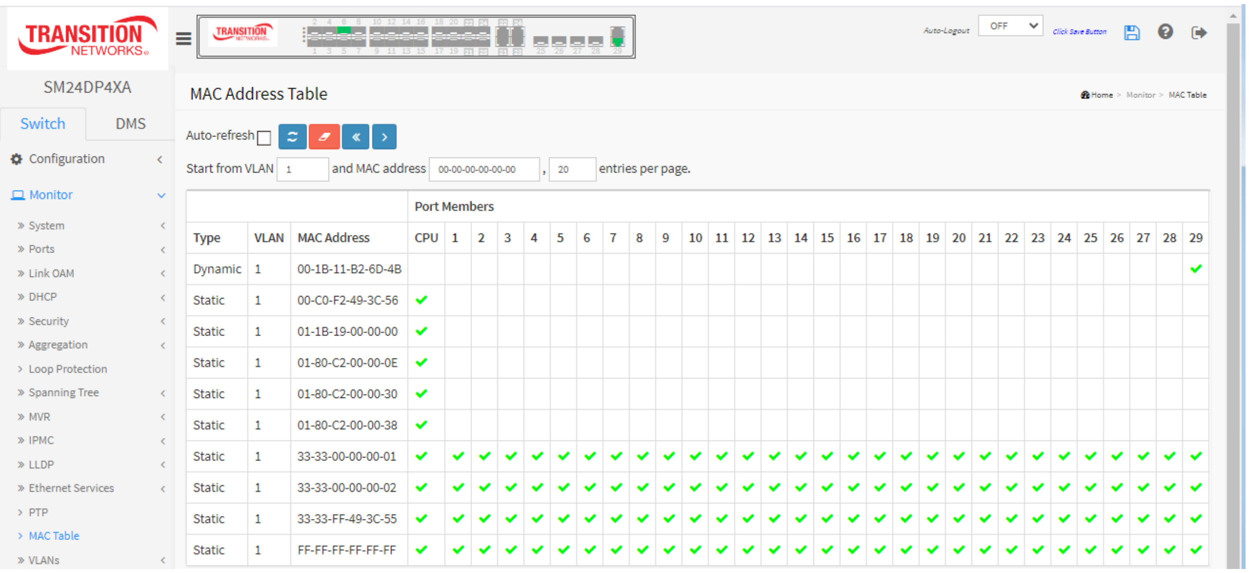
Entries in the MAC Table are shown on this page. The MAC Table contains up to 8192 entries, and is sorted first by VLAN ID, then by MAC address.

Web Interface

To display MAC Address Table in the web interface:

1. Click Monitor, Dynamic MAC Table.
2. Specify the Start from VLAN and MAC Address.
3. View the MAC Address Table.
4. Use the buttons as required.

Figure 3- 15: MAC Address Table



MAC Address Table

Auto-refresh □

Start from VLAN 1 and MAC address 00-00-00-00-00-00 , 20 entries per page.

			Port Members																													
Type	VLAN	MAC Address	CPU	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29
Dynamic	1	00-1B-11-B2-6D-4B																														✓
Static	1	00-C0-F2-49-3C-56	✓																													
Static	1	01-1B-19-00-00-00	✓																													
Static	1	01-80-C2-00-00-0E	✓																													
Static	1	01-80-C2-00-00-30	✓																													
Static	1	01-80-C2-00-00-38	✓																													
Static	1	33-33-00-00-00-01	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Static	1	33-33-00-00-00-02	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Static	1	33-33-FF-49-3C-55	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Static	1	FF-FF-FF-FF-FF-FF	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓

Parameter descriptions:

Type : Indicates whether the entry is a static or a dynamic entry.

VLAN : The VLAN ID of the entry.

MAC address : The MAC address of the entry.

Port Members : The ports that are members of the entry.

Buttons

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

Clear: Clears the counters for the selected port.

Refresh: Click to refresh the page immediately.

<<: 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)

33-33-00-00-00-01 : Destination MAC (for IPv6 Router Advertisement) (reference IPv6 RA.JPG)

33-33-00-00-00-02 : Destination MAC (for IPv6 Router Solicitation) (reference IPv6 RS.JPG)

33-33-FF-73-01-29 : Destination MAC (for IPv6 Neighbor Solicitation) (reference IPv6 DAD.JPG)

33-33-FF-A8-01-01: your switch MAC address (for IPv6 global IP)

FF-FF-FF-FF-FF-FF: for Broadcast.

3-16 VLANs

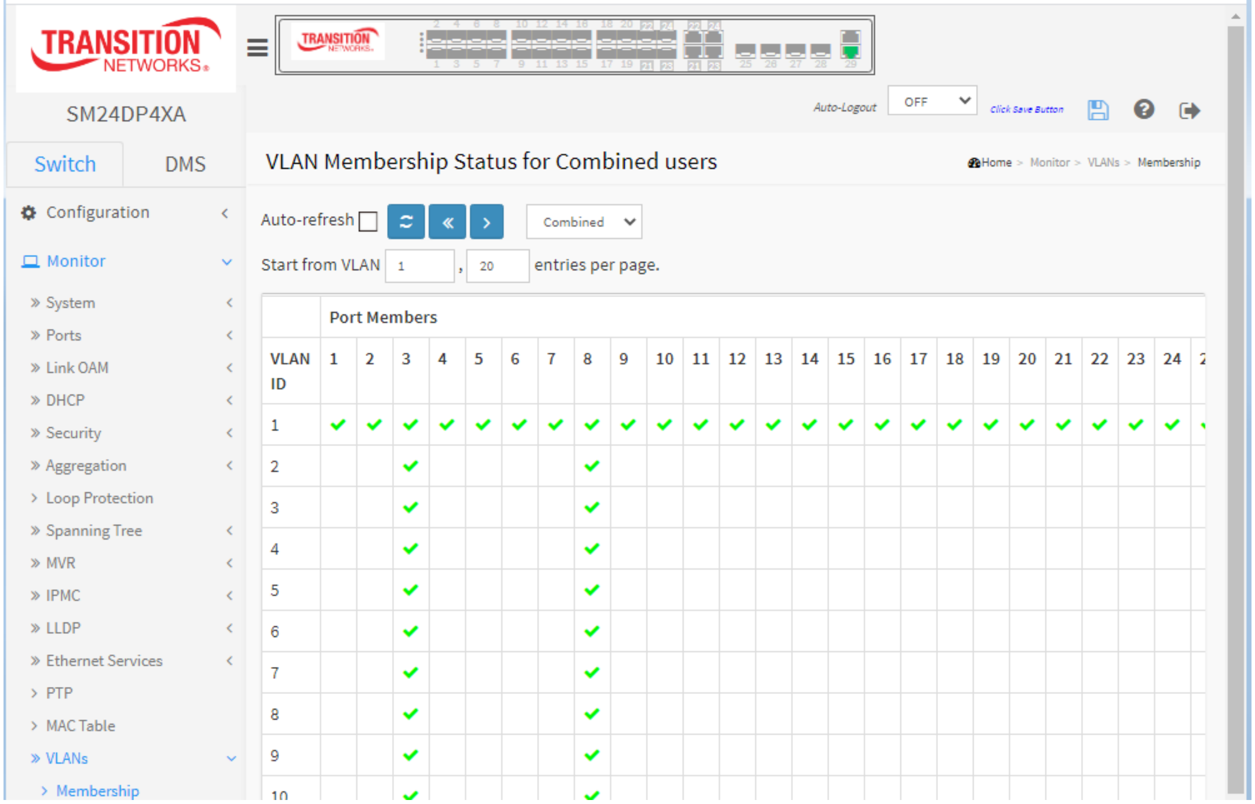
3-16.1 VLAN Membership

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

To view VLAN membership status via the web UI:

1. Click Monitor, VLANs, VLAN membership.
2. Set the Start from VLAN and entries per page.
3. At the User select box, select which set of VLAN users to display.
4. Use the buttons as required.

Figure 3-16.1: VLAN Membership Status for Combined users



VLAN Membership Status for Combined users

Auto-refresh □ Combined

Start from VLAN 1 , 20 entries per page.

	Port Members																								
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	2
1	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
2			✓					✓																	
3			✓					✓																	
4			✓					✓																	
5			✓					✓																	
6			✓					✓																	
7			✓					✓																	
8			✓					✓																	
9			✓					✓																	
10			✓					✓																	

Parameter descriptions:

VLAN USER : VLAN User module uses services of the VLAN management functionality to configure VLAN memberships and VLAN port configs such as PVID and UVID. These VLAN user types are supported:

***CLI/Web/SNMP* :** These are referred to as static.

***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* : U**sed 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.

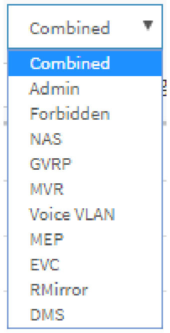
If a port is included in a Forbidden port list and dynamic VLAN user register VLAN on same Forbidden port, then conflict port will be displayed as ✗c.

Buttons

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

Refresh : Click to refresh the page immediately.

User select box: Lets you select which set of user's information is to be displayed in the table. Select VLAN Users from this drop down list.



3-16.2 VLAN Port

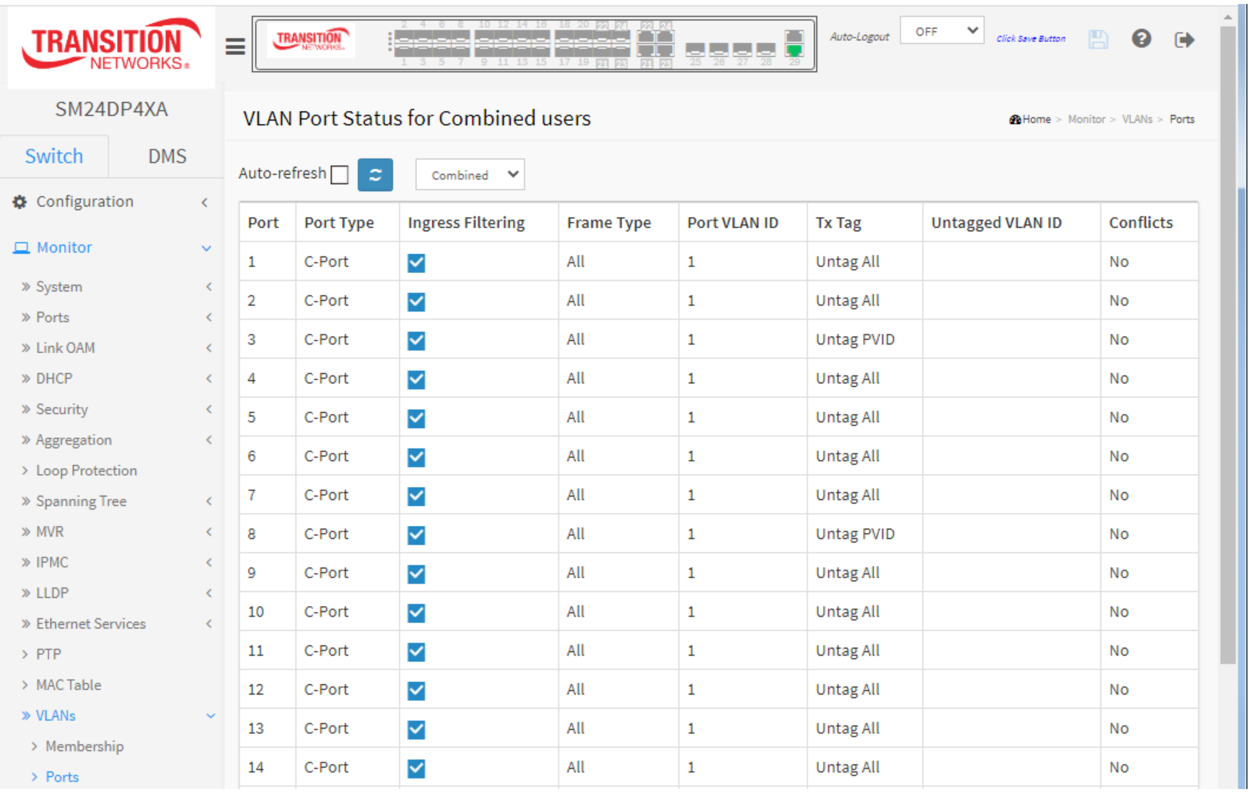
This page shows Port Status of all VLAN users and reports it in the order of Static, NAS, MVRP, MVP, Voice VLAN, MSTP, GVRP, Combined.

Web Interface

To display VLAN Port Status in the web interface:

1. Click Monitor, VLAN Port Status.
2. At the User select box, select the set of users to be displayed.
3. View the displayed information.
4. Click the buttons as required.

Figure 3-16.2: VLAN Port Status for Combined users



VLAN Port Status for Combined users

Auto-refresh □ Combined

Port	Port Type	Ingress Filtering	Frame Type	Port VLAN ID	Tx Tag	Untagged VLAN ID	Conflicts
1	C-Port	☑	All	1	Untag All		No
2	C-Port	☑	All	1	Untag All		No
3	C-Port	☑	All	1	Untag PVID		No
4	C-Port	☑	All	1	Untag All		No
5	C-Port	☑	All	1	Untag All		No
6	C-Port	☑	All	1	Untag All		No
7	C-Port	☑	All	1	Untag All		No
8	C-Port	☑	All	1	Untag PVID		No
9	C-Port	☑	All	1	Untag All		No
10	C-Port	☑	All	1	Untag All		No
11	C-Port	☑	All	1	Untag All		No
12	C-Port	☑	All	1	Untag All		No
13	C-Port	☑	All	1	Untag All		No
14	C-Port	☑	All	1	Untag All		No

Parameter descriptions:

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

CLI/Web/SNMP **:** These are referred to as static.

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

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.

PVID : Shows the VLAN identifier for that port. The allowed values are 1 - 4095. The default value is 1.

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.

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.

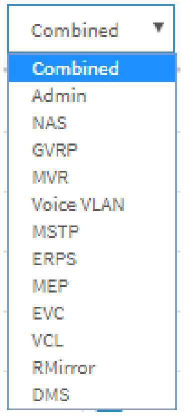
Frame Type : Shows whether the port accepts all frames or only tagged frames. This parameter affects VLAN ingress processing. If the port only accepts tagged frames, untagged frames received on that port are discarded.

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 box : Select a VLAN User from this drop down list.

3-17 VCL

3-17.1 MAC-based VLAN

This page displays the VCL (VLAN Control List) status of the ports. This page shows MAC-based VLAN entries configured by various MAC-based VLAN users. These VLAN User types are supported:

Static : CLI/Web/SNMP are referred to as static.

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

DMS : The Device Management System provides device-level Graphical Monitoring, Traffic Monitoring, and Troubleshooting.

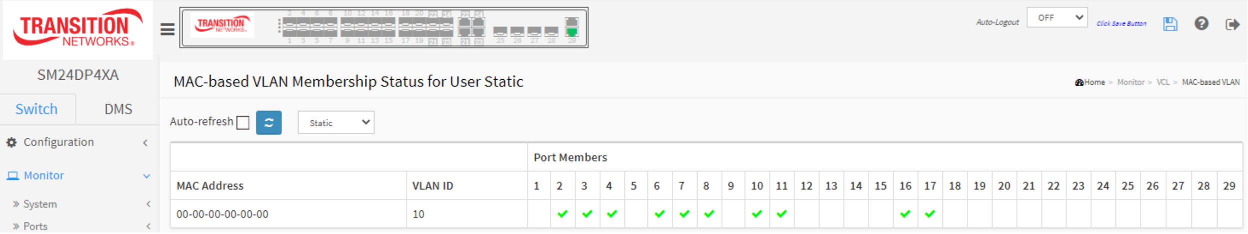
Combined : The combined set of Static, NAS and DMS users.

Web Interface

To display VCL status via the web interface:

1. Click Monitor, VCL, MAC-based VLAN.
2. At the User select box, select the set of users to display statistics for.
3. View the displayed information.
4. Use the buttons as required.

Figure 3-17: MAC-based VLAN Membership Status



MAC-based VLAN Membership Status for User Static

Auto-refresh □ Static

		Port Members																											
MAC Address	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	25	26	27	28	29
00-00-00-00-00-00	10		✓	✓	✓		✓	✓	✓		✓	✓					✓	✓												

Parameter descriptions:

MAC Address : Indicates the MAC address.

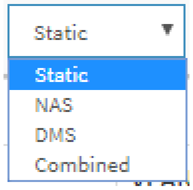
VLAN ID : Indicates the VLAN ID.

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 : Refreshes the displayed table.



User select box: At the dropdown, select the set of VLAN users to display.

3-17.2 Protocol-based VLAN

This section provides Protocol-based VLAN and IP Subnet-based VLAN support.

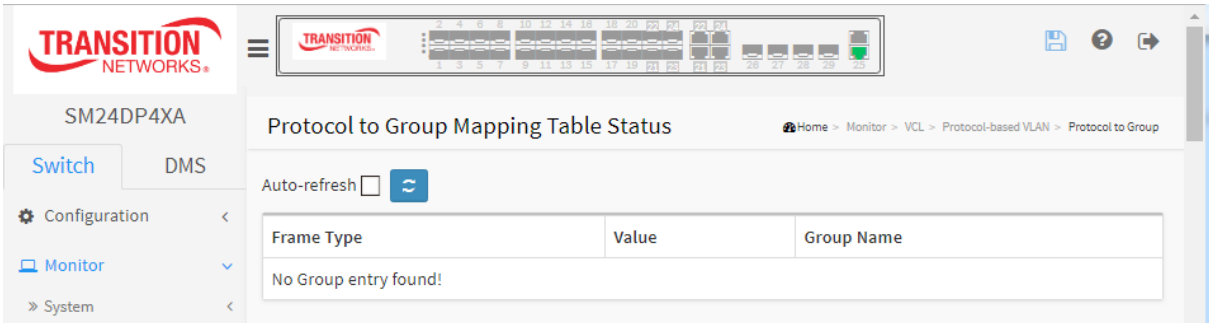
3-19.2.1 Protocol to Group

This page displays the protocols to Group Name (unique for each Group) mapping entries for the switch.

Web Interface

To display VCL status via the web interface:

1. Click Monitor, VCL, Protocol-based VLAN, Protocol to Group.
2. View the displayed information.
3. Use the buttons as required.



Protocol to Group Mapping Table Status

Auto-refresh □

Frame Type	Value	Group Name
No Group entry found!		

Parameter descriptions:

Frame Type : Frame Type can have one of these values: Ethernet, LLC, or 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:

1. **For 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

2. **For 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)

3. **For 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 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.

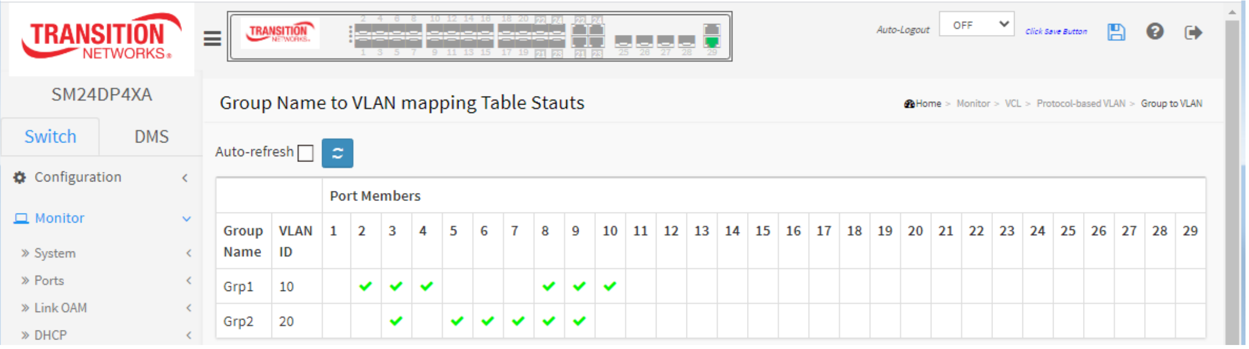
3-17.2.2 Group to VLAN

This page displays the configured Group Name to a VLAN for the switch.

Web Interface

To display VCL status via the web interface:

1. Click Monitor, VCL, Protocol-based VLAN, Group to VLAN.
2. View the displayed information.
3. Use the buttons as required.



Group Name to VLAN mapping Table Stauts

Auto-refresh □

		Port Members																												
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	25	26	27	28	29
Grp1	10		✓	✓	✓				✓	✓	✓																			
Grp2	20			✓		✓	✓	✓	✓	✓																				

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.

Refresh : Refreshes the displayed table.

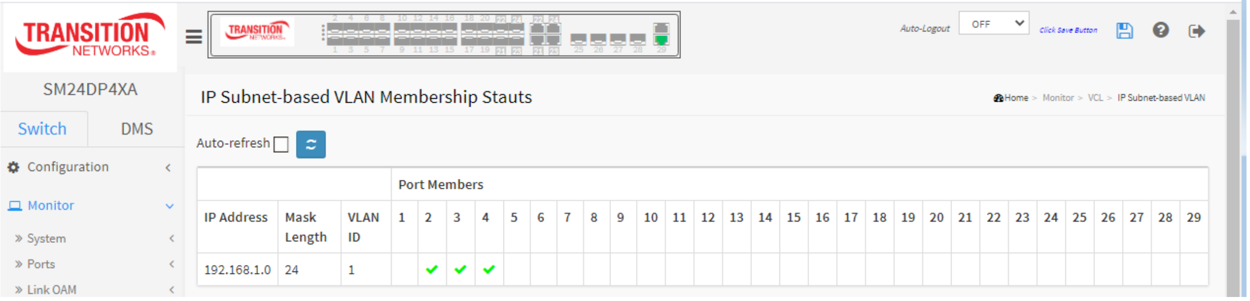
3-17.3 IP Subnet-based VLAN

This page displays IP subnet-based VLAN entries. This page shows only static entries.

Web Interface

To display VCL status via the web interface:

1. Click Monitor, VCL, IP Subnet-based VLAN.
2. View the displayed information.
3. Use the buttons as required.



IP Subnet-based VLAN Membership Stauts

Home > Monitor > VCL > IP Subnet-based VLAN

Auto-refresh □

			Port Members																												
IP Address	Mask Length	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	25	26	27	28	29
192.168.1.0	24	1		✓	✓	✓																									

Parameter descriptions:

IP Address : Indicates the IP address.

Mask Length : Indicates the network mask length.

VLAN ID : Indicates the VLAN ID. VLAN ID can be changed for the existing entries.

Port Members : A row of check boxes for each port is displayed for each IP subnet-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 : Refreshes the displayed table.

3-18 UDLD

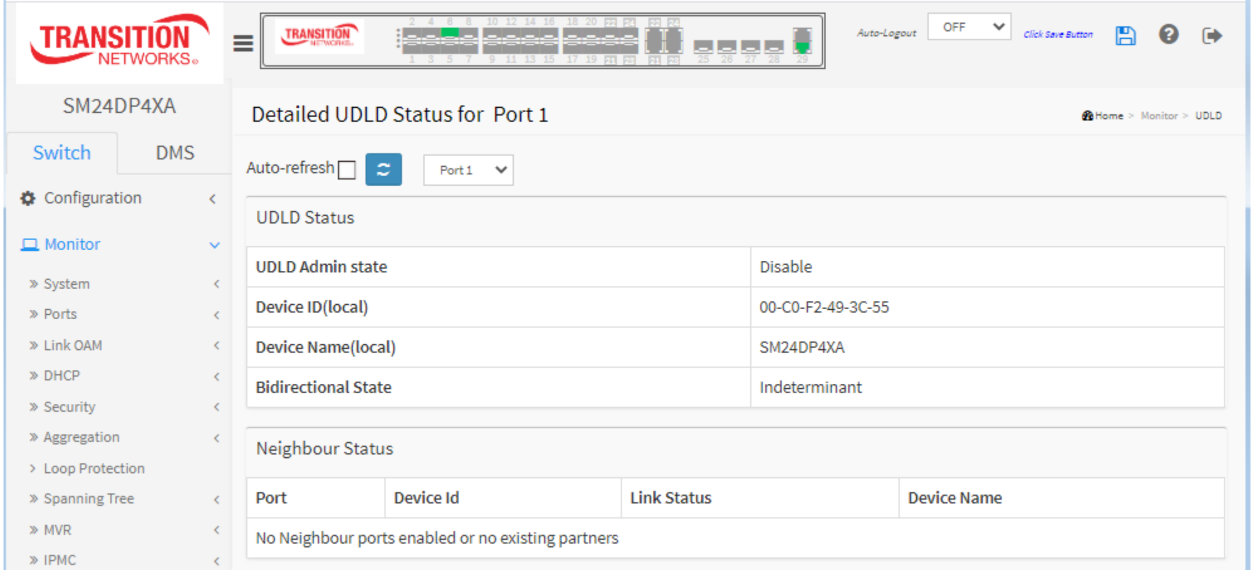
This page displays the UDLD (Unidirectional Link Detection) status of the ports. UDLD protocol monitors the physical configuration of the links between devices and ports that support UDLD. It detects the existence of unidirectional links. Its functionality is to provide mechanisms useful for detecting one way connections before they create a loop or other protocol malfunction. RFC 5171 specifies a way at data link layer to detect Uni directional link.

Web Interface

To display UDLD in the web interface:

1. Click Monitor, UDLD.
2. At the Port select box select the desired port.
3. View the displayed information.
4. Use the buttons as required.

Figure 3-18: UDLD Status



Detailed UDLD Status for Port 1

Auto-refresh □ Port 1

UDLD Status

UDLD Admin state	Disable
Device ID(local)	00-C0-F2-49-3C-55
Device Name(local)	SM24DP4XA
Bidirectional State	Indeterminant

Neighbour Status

Port	Device Id	Link Status	Device Name
No Neighbour ports enabled or no existing partners			

Parameter descriptions:

__UDLD Status__

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

Device ID(local) : The ID of Device.

Device Name(local) : Name of the Device.

Bidirectional State : The current state of the port.

__Neighbour Status__

Port : The current port of neighbour device.

Device ID : The current ID of neighbour device.

Link Status : The current link status of neighbour port.

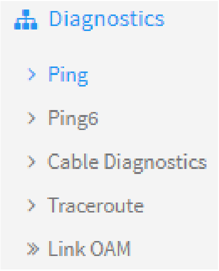
Device Name : Name of the Neighbour Device.

Buttons

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

Refresh : Refreshes the displayed table.

4. Diagnostics



This chapter describes the system diagnostics, including Ping, Ping6, Cable Diagnostics, Traceroute, and Link OAM.

4-1 Ping

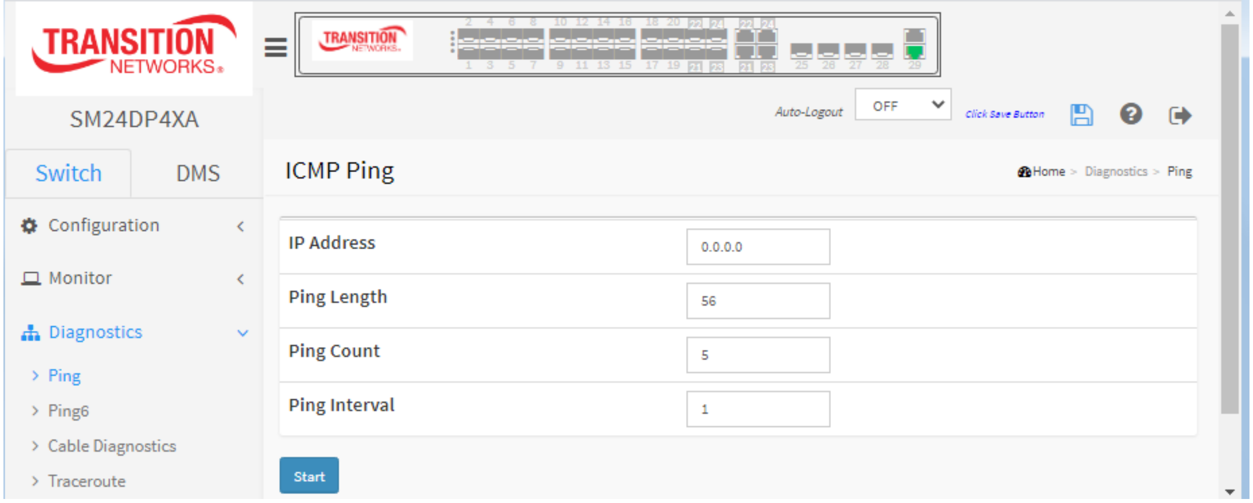
This page lets you issue ICMP PING packets to troubleshoot IPv4 connectivity issues.

Web Interface

To configure an ICMP Ping via the web interface:

1. Click Diagnostics, Ping.
2. Specify an IP Address.
3. Specify Ping Length, Count, and Interval.
4. Click Start.

Figure 4-1: ICMP Ping



ICMP Ping

IP Address	0.0.0.0
Ping Length	56
Ping Count	5
Ping Interval	1

Start

Parameter descriptions:

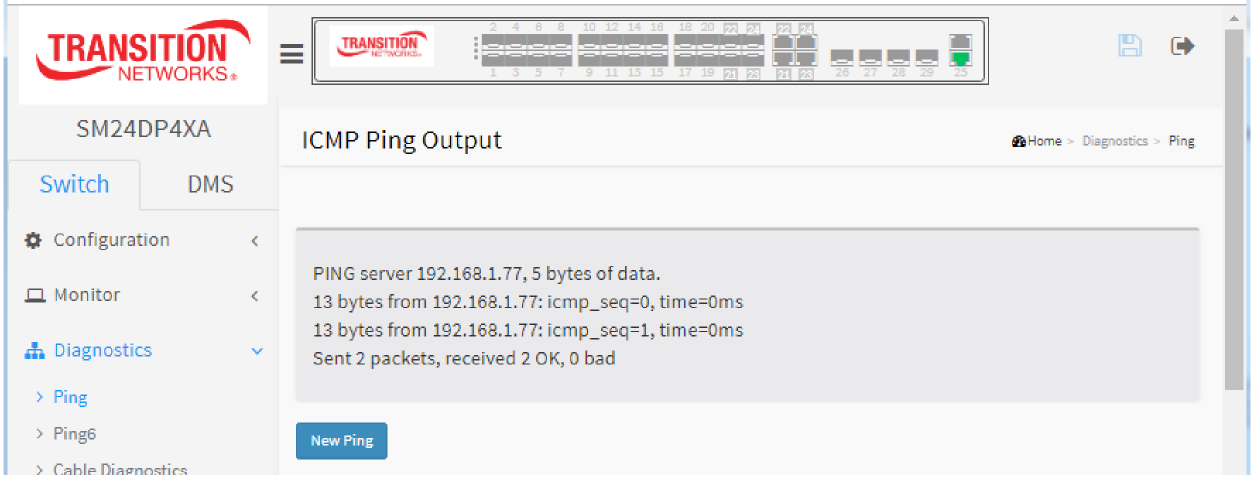
IP Address : To set the IP Address of device what you want to ping it.

Ping Size: To set the ICMP Packet size to ping the other device.

Start: Click the button then the switch will start to ping the device using the selected ICMP packet size. After you click the **Start** button, five ICMP packets are transmitted, and the sequence number and roundtrip time are displayed upon reception of a reply. The page refreshes automatically until responses to all packets are received, or until a timeout occurs.

```
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
```

A sample ICMP Ping Output is shown below:



```
PING server 192.168.1.77, 5 bytes of data.
13 bytes from 192.168.1.77: icmp_seq=0, time=0ms
13 bytes from 192.168.1.77: icmp_seq=1, time=0ms
Sent 2 packets, received 2 OK, 0 bad
```

Buttons

Start : Click to start transmitting ICMP packets.

New Ping : Click to re-start diagnostics with PING.

4-2 Ping6

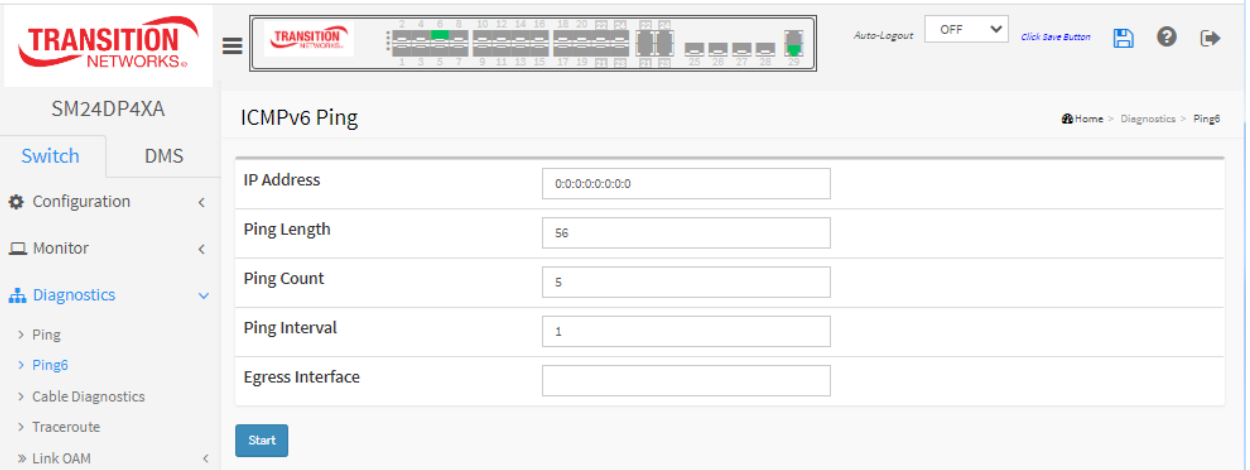
This page lets you issue ICMPv6 PING packets to troubleshoot IPv6 connectivity issues.

Web Interface

To configure an ICMP Ping via the web interface:

1. Click Diagnostics, Ping6.
2. Specify an IP Address.
3. Specify Ping Length, Count, Interval, and Egress Interface.
4. Click Start.

Figure 4-1: ICMP Ping6



ICMPv6 Ping

IP Address	0:0:0:0:0:0:0:0
Ping Length	56
Ping Count	5
Ping Interval	1
Egress Interface	

Parameter descriptions:

IP Address : The destination IP Address.

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 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

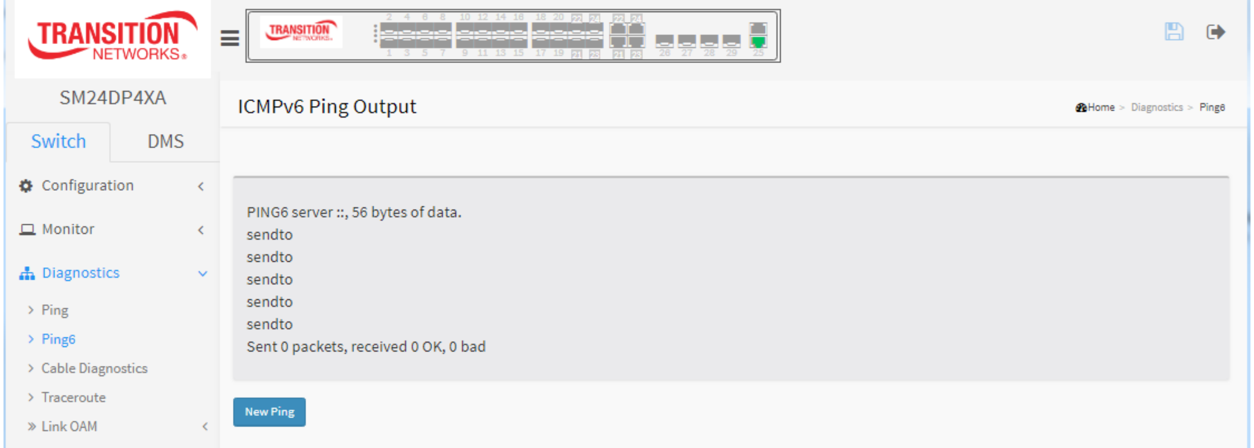
Start : Click to start transmitting ICMP packets.

New Ping : Click to re-start diagnostics with PING.

After you press **Start**, ICMPv6 packets are transmitted, and the sequence number and round trip time are displayed upon reception of a reply. The page refreshes automatically until responses to all packets are received, or until a timeout occurs.

```
PING6 server ff02::2, 56 bytes of data.
64 bytes from fe80::219:5bff:fe2f:b47: icmp_seq=0, time=10ms
64 bytes from fe80::215:58ff:feed:69dd: icmp_seq=0, time=10ms
64 bytes from fe80::219:5bff:fe2f:b47: icmp_seq=1, time=0ms
64 bytes from fe80::215:58ff:feed:69dd: icmp_seq=1, time=0ms
64 bytes from fe80::219:5bff:fe2f:b47: icmp_seq=2, time=0ms
64 bytes from fe80::215:58ff:feed:69dd: icmp_seq=2, time=0ms
64 bytes from fe80::219:5bff:fe2f:b47: icmp_seq=3, time=0ms
64 bytes from fe80::215:58ff:feed:69dd: icmp_seq=3, time=0ms
64 bytes from fe80::219:5bff:fe2f:b47: icmp_seq=4, time=0ms
64 bytes from fe80::215:58ff:feed:69dd: icmp_seq=4, time=0ms
Sent 5 packets, received 10 OK, 0 bad
```

A sample ICMPv6 Ping Output is shown below:



```
PING6 server ::, 56 bytes of data.
sendto
sendto
sendto
sendto
sendto
Sent 0 packets, received 0 OK, 0 bad
```

4-3 Cable Diagnostics

This page is used for running the Cable Diagnostics for 10/100 and 1G copper ports.

Select a port and click the **Start** button to run the diagnostics. This will take approximately 5 seconds. When completed, the page refreshes automatically, and you can view the cable diagnostics results in the cable status table. Note that Cable Diagnostics is only accurate for cables of length 7 - 120 meters with 5-meter accuracy.

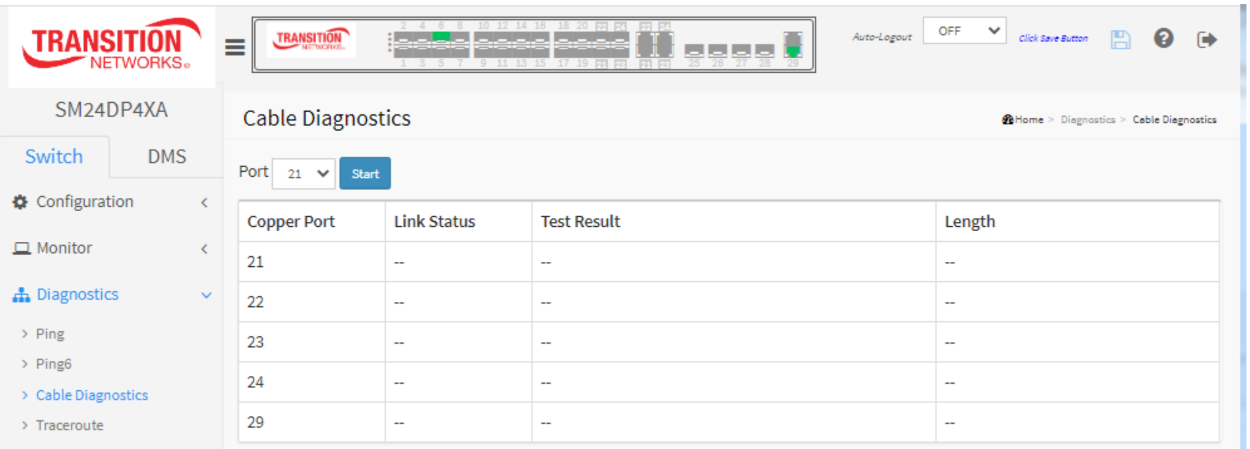
10 and 100 Mbps ports will be linked down while running Cable Diagnostics. Therefore, running Cable Diagnostics on a 10 or 100 Mbps management port will cause the switch to stop responding until Cable Diagnostics is complete.

Web Interface

To configure a Cable Diagnostic via the web interface:

1. Click Diagnostics, Cable Diagnostics.
2. At the Port select dropdown, specify the Port to diagnose.
3. Click Start. At the confirmation prompt, click OK to continue.

Figure 4-3: Cable Diagnostics



Cable Diagnostics

Port 21

Copper Port	Link Status	Test Result	Length
21	--	--	--
22	--	--	--
23	--	--	--
24	--	--	--
29	--	--	--

Parameter descriptions:

Port : 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.

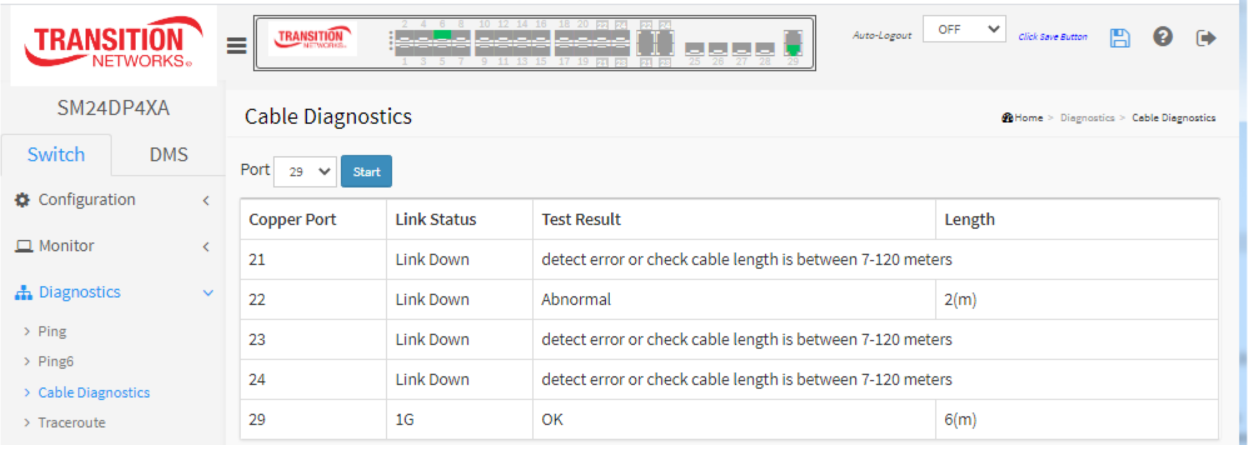
Test Result : Test Result of the cable.

***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 follow, the length has different definition.

1G : The length is the minimum value of 4-pair.
10M/100M : The length is the minimum value of 2-pair.
Link Down : The length is the minimum value of non-zero of 4-pair.

Example:



Cable Diagnostics

Port 29 Start

Copper Port	Link Status	Test Result	Length
21	Link Down	detect error or check cable length is between 7-120 meters	
22	Link Down	Abnormal	2(m)
23	Link Down	detect error or check cable length is between 7-120 meters	
24	Link Down	detect error or check cable length is between 7-120 meters	
29	1G	OK	6(m)

Messages: *Switch is currently not responding. Please wait...*

4-4 Traceroute

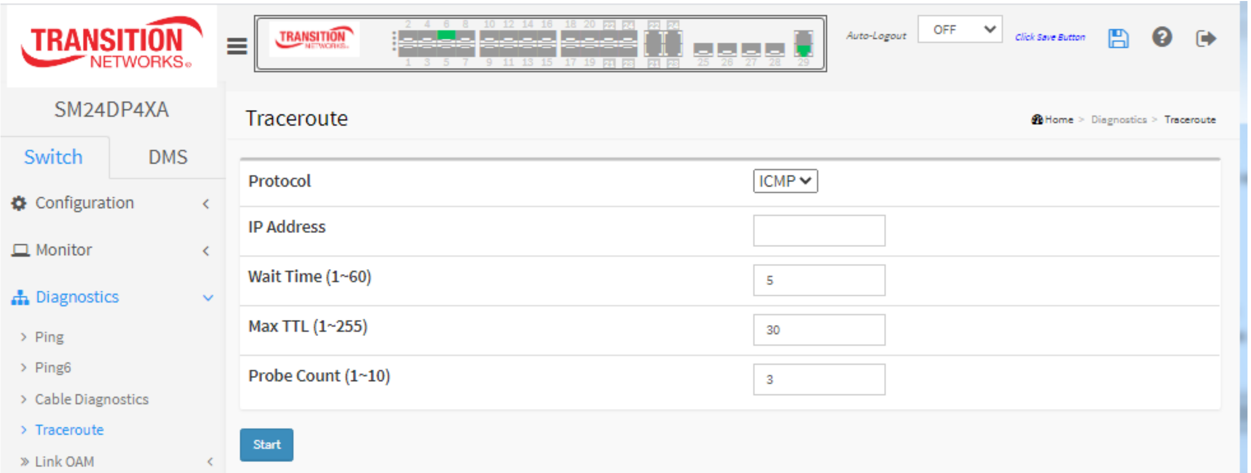
This page lets you issue ICMP, TCP, or UDP packets to diagnose network connectivity issues.

Web Interface

To configure a Cable Diagnostic via the web interface:

1. Click Diagnostics, Traceroute.
2. Select a Protocol.
3. Enter an IP Address, Wait Time, Max TTL, and Probe Count
4. Click Start. At the confirmation prompt, click OK to continue.

Figure 4-4: Traceroute



Traceroute

Protocol	ICMP
IP Address	
Wait Time (1~60)	5
Max TTL (1~255)	30
Probe Count (1~10)	3

Start

Parameter descriptions:

Protocol : The protocol (ICMP, UDP, or TCP) packets to send.

IP Address : The destination IP Address.

Wait Time : Set the time (in seconds) to wait for a response to a probe (default 5.0 sec). Valid values are 1 - 60.

Max TTL : Specifies the maximum number of hops (max time-to-live value) traceroute will probe. Valid values are 1 - 255. The default is 30 hops.

Probe Count : Sets the number of probe packets per hop. Valid values are 1 - 10. The default is 3.

Buttons

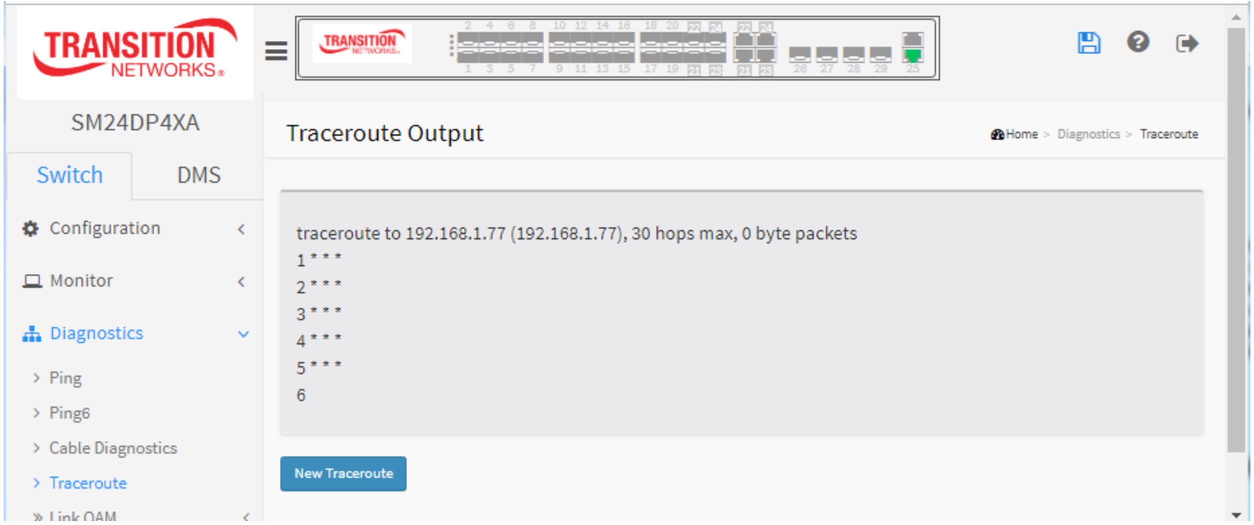
Start : Click to start issuing ICMP, TCP, or UDP packets.

New Traceroute : Click to start a new 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.

```
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
```

Sample Traceroute Output



```
traceroute to 192.168.1.77 (192.168.1.77), 30 hops max, 0 byte packets
1 * * *
2 * * *
3 * * *
4 * * *
5 * * *
6
```

4-5 Link OAM

4-5.1 MIB Retrieval

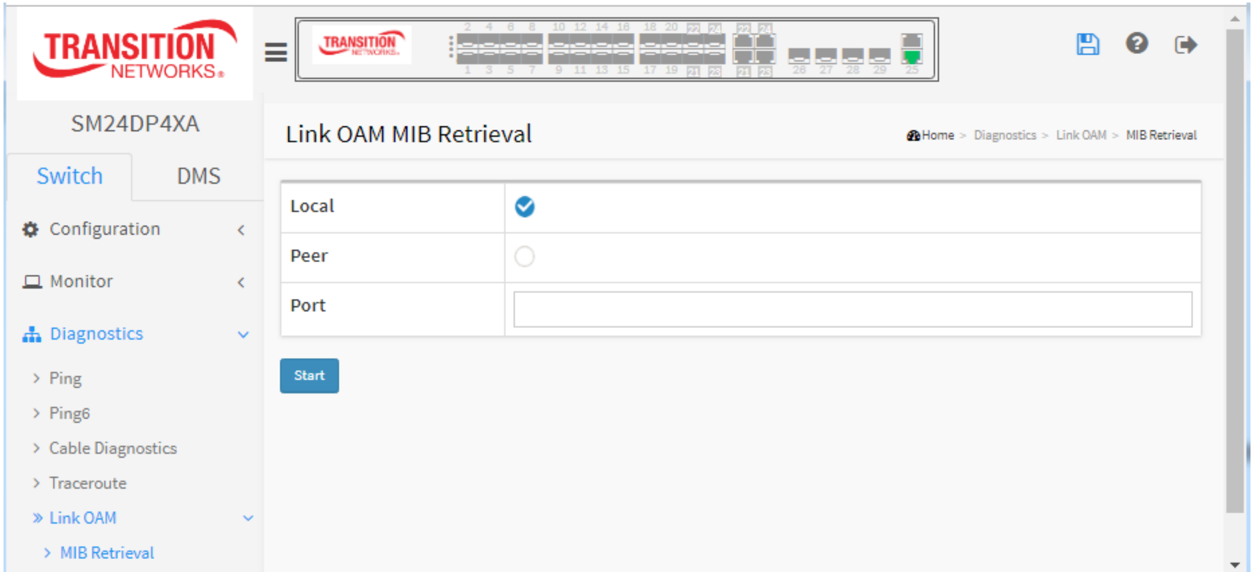
This page lets you retrieve the local or remote OAM MIB variable data on a particular port. Select the appropriate radio button and enter the port number of the switch to retrieve the content of interest. Click **Start** to retrieve the content. Click **Previous** to retrieve another content of interest.

Web Interface

To configure a Link OAM MIB Retrieval in the web interface:

1. Specify Local or Peer.
2. Specify a Port number.
3. Click Start.

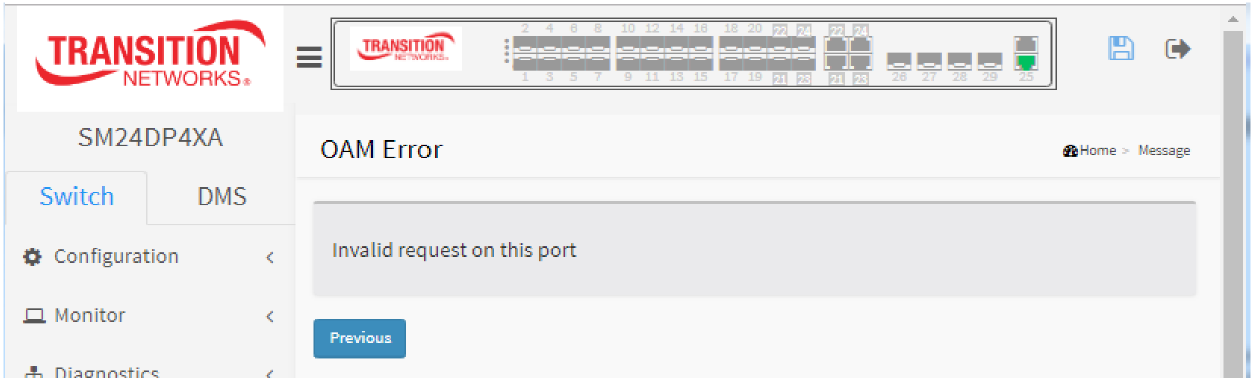
Figure 4-2.1: Link OAM MIB Retrieval



Link OAM MIB Retrieval

Local	●
Peer	○
Port	

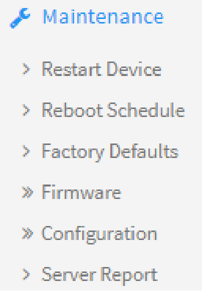
Messages : *OAM Error Invalid request on this port.*



OAM Error

Invalid request on this port

5. Maintenance



This chapter describes the available Maintenance tasks, including Restart Device, Reboot Schedule, Factory Defaults, Firmware Upgrade / Selection, Configuration Save/Download/Upload/Activate/Delete, and Server Report.

5-1 Restart Device

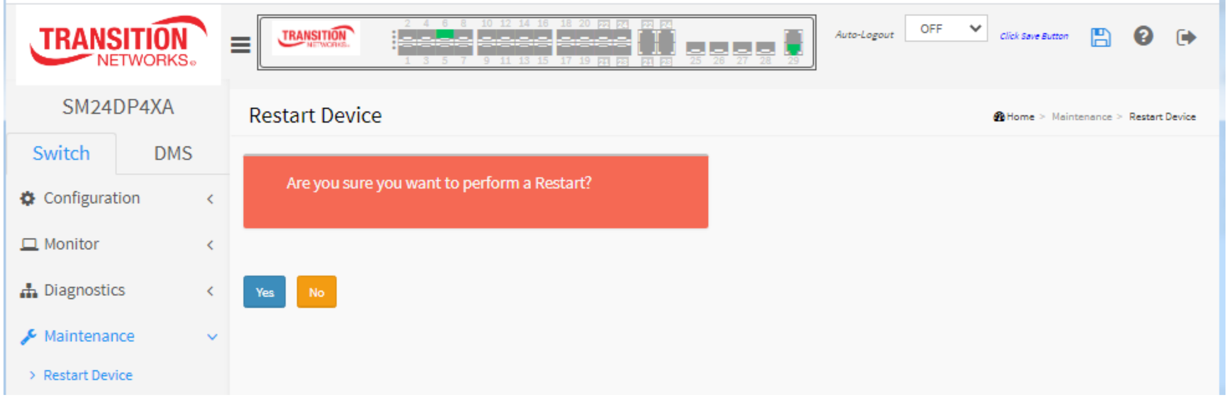
This page lets you restart switch for any maintenance needs. Any configuration files or scripts that you saved in the switch should still be available afterwards.

Web Interface

To configure a Restart Device Configuration in the web interface:

1. Click Maintenance, Restart Device.
2. Check or uncheck Force Cool Restart.
3. At the "*Are you sure…*" prompt click Yes.

Figure 5-1: Restart Device



Are you sure you want to perform a Restart?

Parameter descriptions:

Restart Device : You can restart the switch on this page. After restart, the switch will boot normally.

Buttons:

Yes – Click to start the device.

No- Click to undo any restart action.

5-2 Switch Reboot Schedule

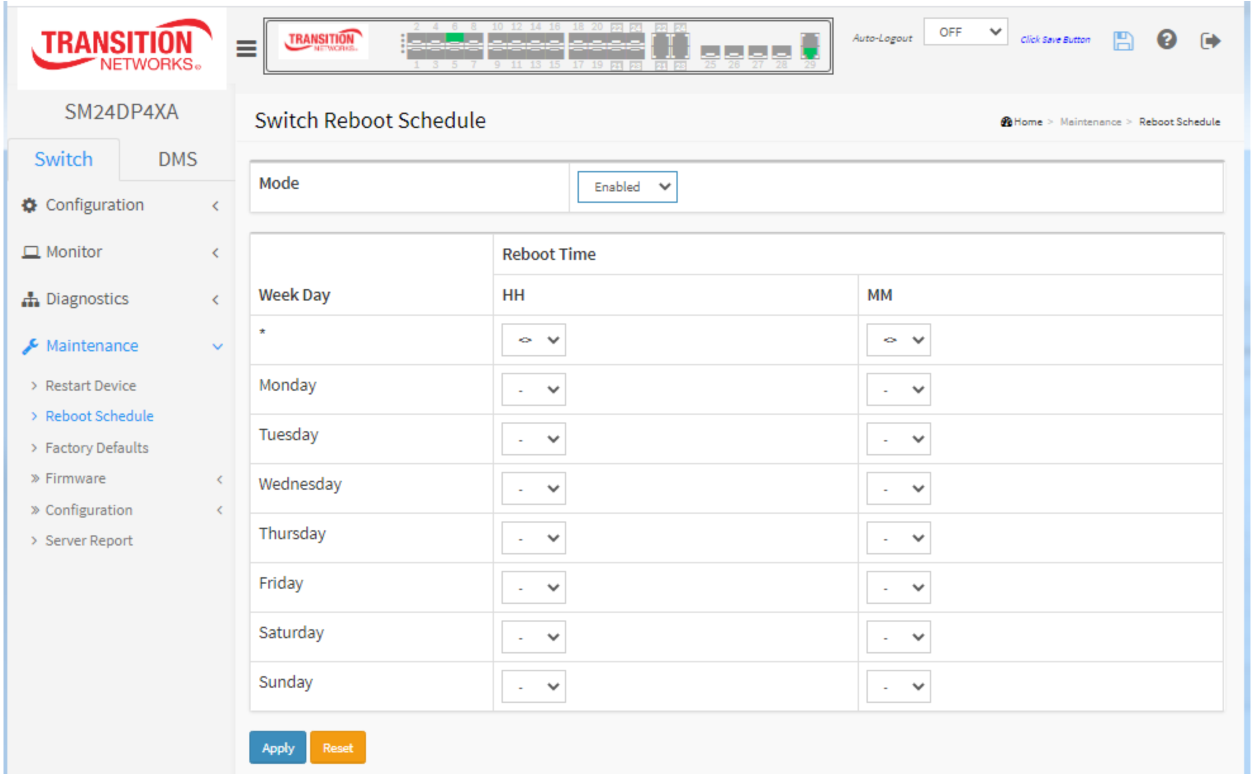
This page lets you set a Reboot Schedule for the switch.

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 reboot schedule parameters.
3. Enter the Reboot Day(s) and Time(s).
4. Click the Apply button.

Figure 5-1: Switch Reboot Schedule



Switch Reboot Schedule

Mode	Enabled

	Reboot Time	
Week Day	HH	MM
*	<>	<>
Monday	-	-
Tuesday	-	-
Wednesday	-	-
Thursday	-	-
Friday	-	-
Saturday	-	-
Sunday	-	-

Parameter descriptions:

Mode : Indicates the reboot scheduling mode operation. Possible modes are:

Enabled: Enable switch reboot scheduling.
Disabled: Disable switch reboot scheduling.

Week Day : The day(s) to reboot this switch.

Reboot Time : The time(s) to reboot the switch in hours (HH) and minutes (MM).

Buttons

Apply : Click to save changes.

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

5-3 Factory Defaults

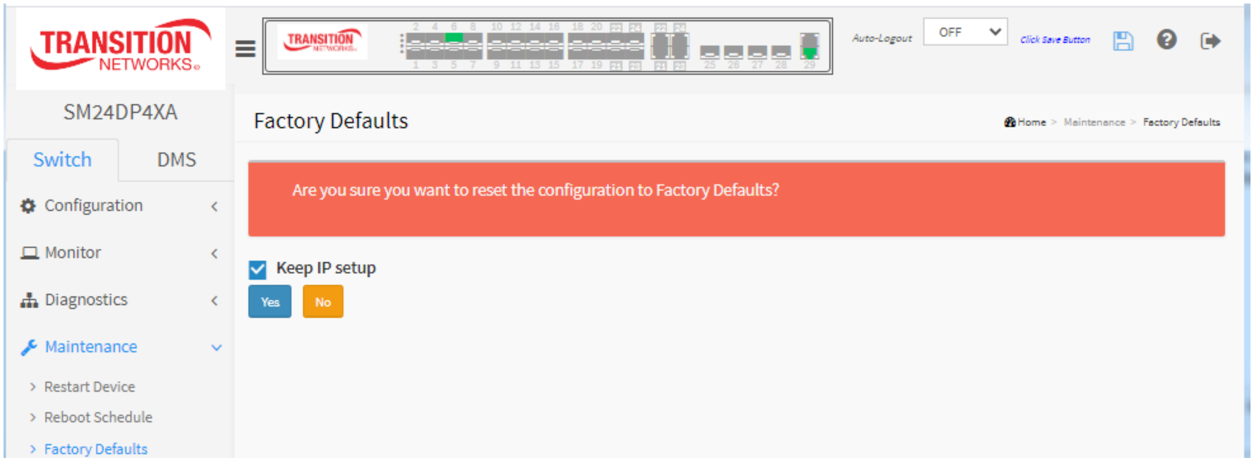
This page lets you to reset the Switch configuration to Factory Defaults. Any configuration files or scripts will reset to factory default values. Only the IP configuration is retained. The new configuration is available immediately, which means that no restart is necessary.

Web Interface

To configure a reset to Factory Defaults via 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



Factory Defaults

Are you sure you want to reset the configuration to Factory Defaults?

☑ Keep IP setup

Yes No

Parameter descriptions:

Keep IP setup : Check if you want to keep the current IP settings.

Yes : Click the button to reset the configuration to Factory Defaults.

No : Click to return to the Port State page without resetting the configuration.

Note: Restoring factory defaults can also be performed by making a physical loopback between port 1 and port 2 within the first minute from switch reboot. In the first minute after boot, 'loopback' packets will be transmitted at port 1. If a 'loopback' packet is received at port 2 the switch will do a restore to factory defaults.

5-4 Firmware

This section lets you upgrade / select firmware. The switch can be enhanced with more value-added functions by installing firmware upgrades.

5-4.1 Software Upload

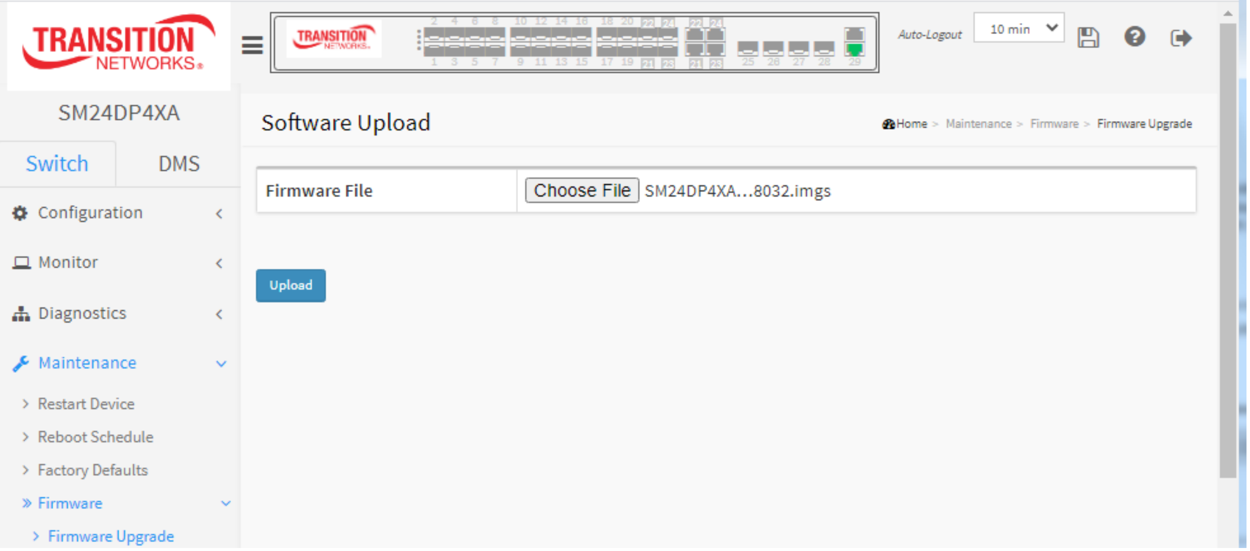
This page facilitates an update of the firmware controlling the switch.

Web Interface

To upgrade firmware via the web interface:

1. Click Maintenance, Firmware, Firmware Upgrade.
2. Click the Choose File button and navigate to and open a firmware file (.IMGS format).
3. Check or uncheck the Force Cool Restart checkbox.
4. Click the Upload button.

Figure 5-4.1 Software Upload



Software Upload

Firmware File	Choose File SM24DP4XA…8032.imgs

Parameter descriptions:

Choose File : Click the button to search for the Firmware file.

Upload: Click to make the switch start uploading the firmware from the selected location.

NOTE: This page facilitates an update of the firmware controlling the switch. Uploading software will update all managed switches to the location of a software image and click. After the software image is uploaded, a page announces that the firmware update is initiated. After about a minute, the firmware is updated and the switch restarts.

WARNING: While the firmware is being updated, Web access appears to be defunct. The front LED flashes Green/Off with a frequency of 10 Hz while the firmware update is in progress. Do not restart or power off the device at this time or the switch may fail to function afterwards.

Messages:

Firmware/EZCM Upgrade Result

The EZCM files are successfully updated.

Do not need to upgrade firmware due to version is the same.

Rebooting system!

Meaning: You tried to upgrade firmware to the current version.

Recovery: None; wait for the reboot to finish and then continue operation.

Messages:

Firmware upgrade in progress

The system will restart after the update.

Until then, do not reset or power off the device!

Erasing, please stand by…

When the Firmware upgrade is done, the last line of the message changes to "*Completed*!".

You may need to refresh the web page to clear the "*Completed*!" message.

5-4.2 Software Image Select

This page lets you select the active and alternate (backup) firmware images in the device and allows you to revert to the alternate image. The webpage displays two tables with information about the active and alternate firmware images.

Note:

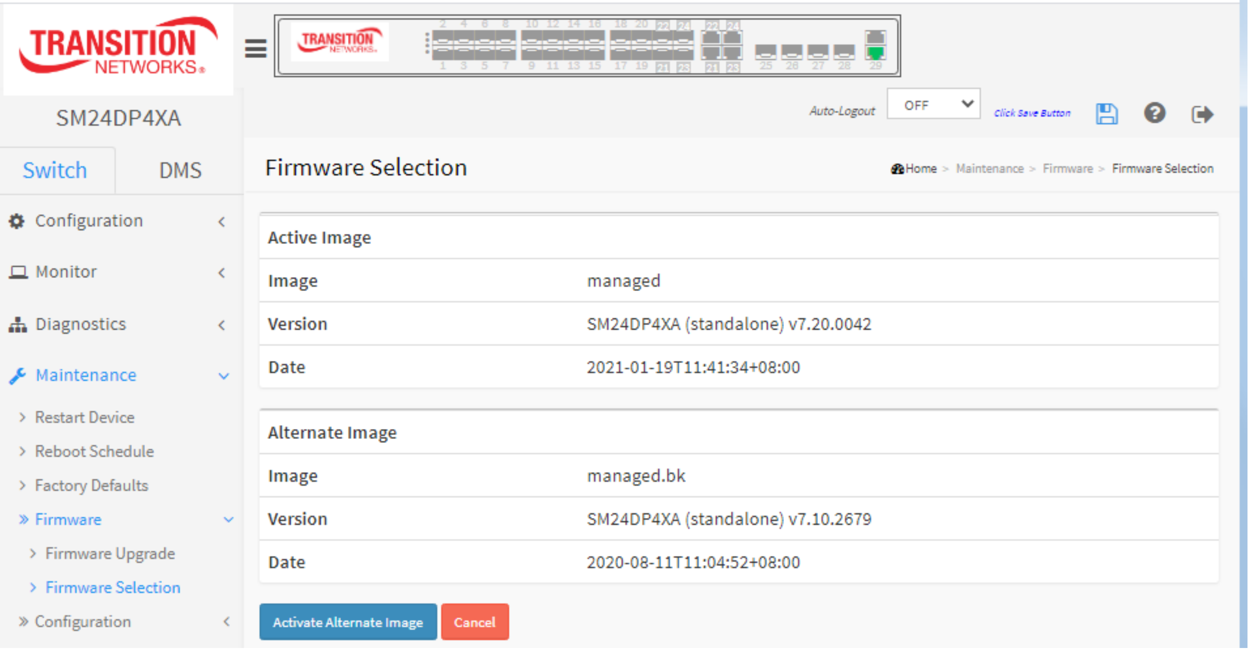
1. If the active firmware image is the alternate image, only the "Active Image" table is shown. In this case, the Activate Alternate Image button is also disabled.
2. If the alternate image is active (due to primary image corruption or manual intervention), uploading a new firmware image to the device will automatically use and activate the primary image.
3. The firmware version and date information may be empty for older firmware releases. This does not constitute an error.

Web Interface

To upgrade firmware via the web interface:

1. Click Maintenance, Firmware, Firmware Selection.
2. Verify the image version and date information.
3. Click the **Activate Alternate Image** button.

Figure 5-4.2 Firmware Selection



Firmware Selection

Active Image	
Image	managed
Version	SM24DP4XA (standalone) v7.20.0042
Date	2021-01-19T11:41:34+08:00

Alternate Image	
Image	managed.bk
Version	SM24DP4XA (standalone) v7.10.2679
Date	2020-08-11T11:04:52+08:00

Parameter Descriptions:

Image : The flash index name of the firmware image. The name of Active (primary or preferred) Image is *managed*; the Alternate Image is named *managed.bk*.

Version : The version of the firmware image (e.g., *SM24DP4XA (standalone) v7.20.0042*).

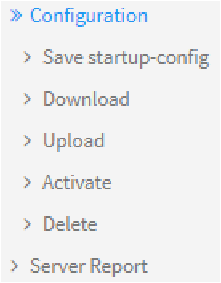
Date : The date and time when the firmware was produced (e.g., *2021-01-19T11:41:34+08:00*).

Buttons

Activate Alternate Image: Click to use the “Alternate Image”. This button may be disabled depending on system state.

Cancel: Cancel activating the backup image. Navigates away from this page.

5-5 Configuration



This section describes the Configuration menu selections, including Save startup-config, Download, Upload, Activate, Delete, and Server Report.

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.

5-5.1 Save startup-config

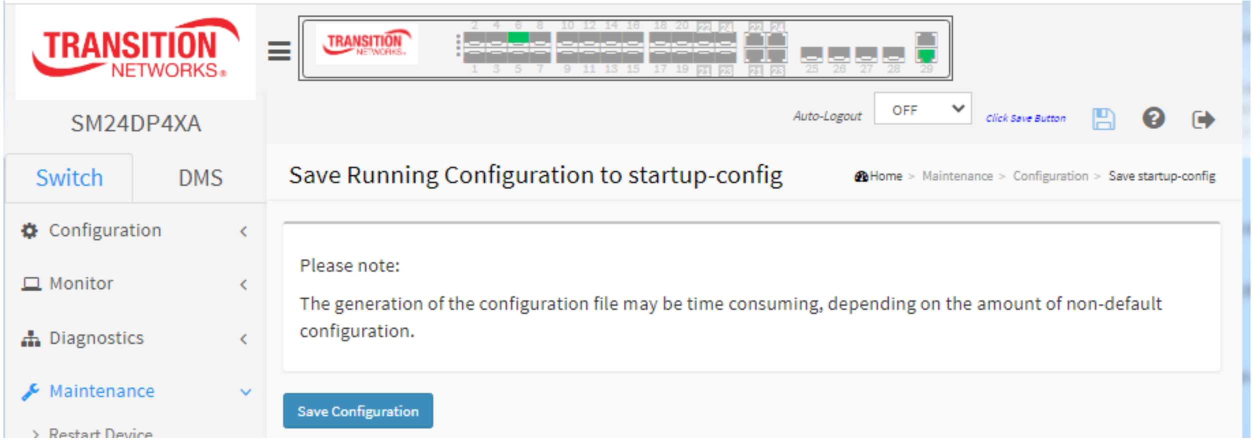
This copies running-config to startup-config, so the currently active configuration will be used at the next reboot.

Web Interface

To save the running configuration in the web interface:

1. Click Maintenance, Configuration, Save startup-config.
2. **Note** that the generation of the configuration file may be time consuming, depending on the amount of non-default configuration.
3. Click the Save Configuration button. When successfully completed, the message "*Save Running Configuration to startup-config startup-config saved successfully.*" displays.

Figure 5-5.1: Save Running Configuration to startup-config startup-config



Save Running Configuration to startup-config

Please note:

The generation of the configuration file may be time consuming, depending on the amount of non-default configuration.

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.

5-5.2 Download

The configuration download function will be backed up and saved configuration from the switch's configuration into the running web browser PC.

It is possible to download any of the files on the switch to the web browser. Select the file and click Download of running-config may take a little while to complete, as the file must be prepared for download.

There are three system files:

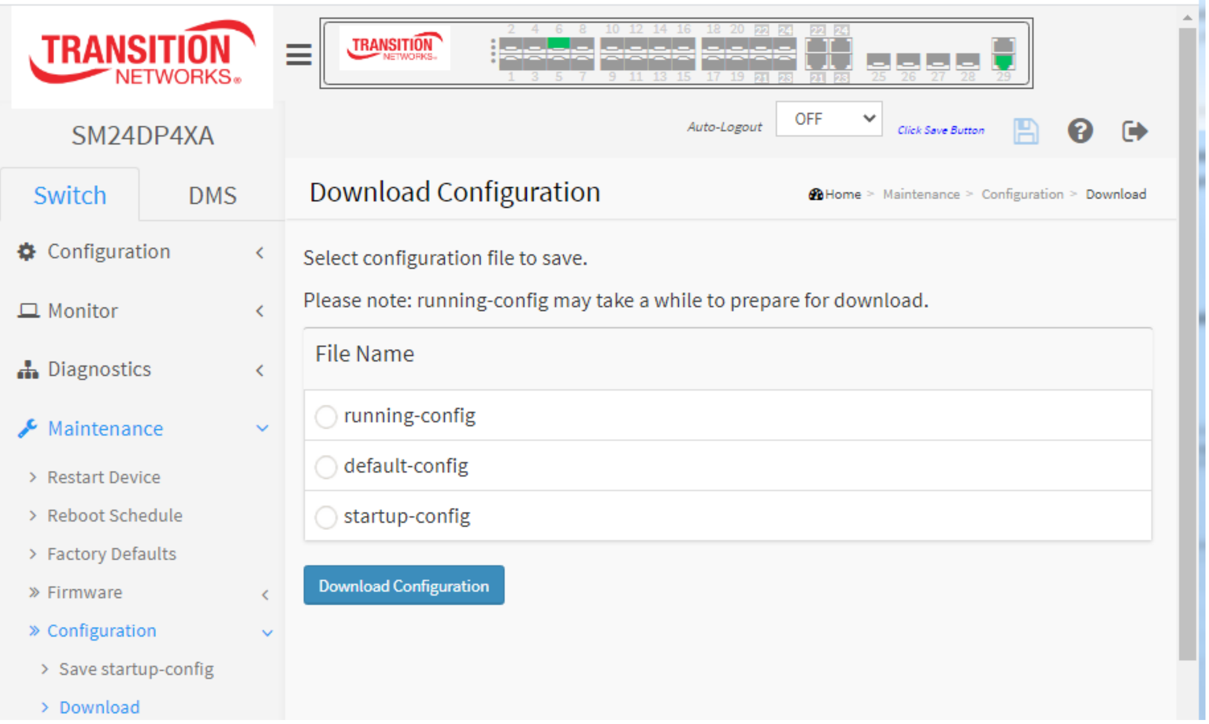
1. **running-config**: A virtual file that represents the currently active configuration on the switch. This file is volatile.
2. **startup-config**: The startup configuration for the switch, read at boot time.
3. **default-config**: A read-only file with vendor-specific configuration. This file is read when the system is restored to default settings.

Web Interface

To download configuration in the web interface:

1. Click Maintenance, Configuration, Download.
2. Select a config file to save. **Note** that running-config may take a while to prepare for download.
3. Click the Download Configuration button.
4. Save or view the file folder location.

Figure 5-5.2: Configuration Download



Download Configuration

Select configuration file to save.

Please note: running-config may take a while to prepare for download.

File Name
○ running-config
○ default-config
○ startup-config

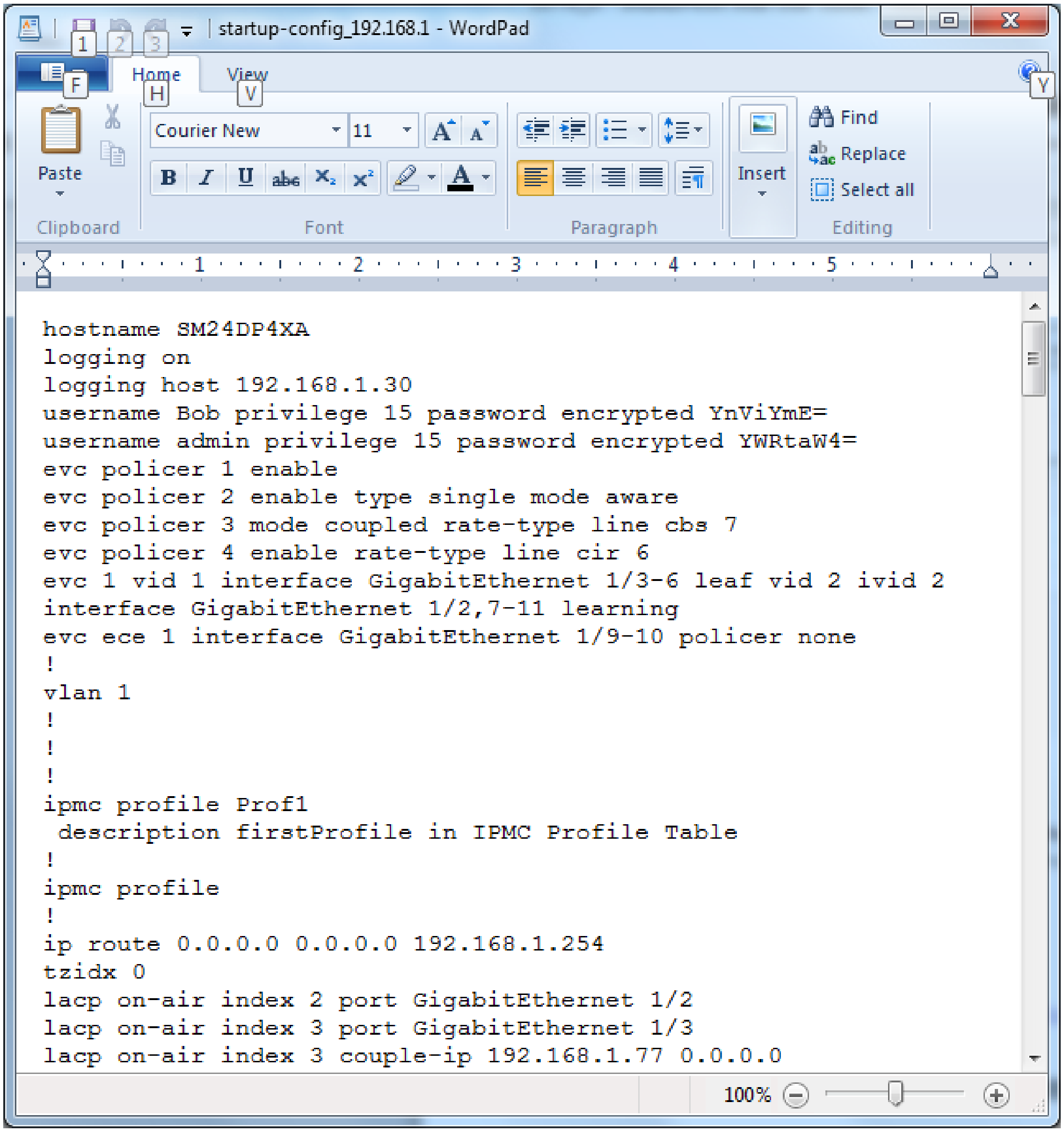
Download Configuration

Buttons :

Download Configuration: Click the "Download" button then the running web management PC will start to download the configuration from the managed switch configuration into the specified location.

Filename examples:

- default-config_192.168.1.77_20110108
- startup-config_192.168.1.77_20110108 (example shown below in WordPad)



```
hostname SM24DP4XA
logging on
logging host 192.168.1.30
username Bob privilege 15 password encrypted YnViYmE=
username admin privilege 15 password encrypted YWRtaW4=
evc policer 1 enable
evc policer 2 enable type single mode aware
evc policer 3 mode coupled rate-type line cbs 7
evc policer 4 enable rate-type line cir 6
evc 1 vid 1 interface GigabitEthernet 1/3-6 leaf vid 2 ivid 2
interface GigabitEthernet 1/2,7-11 learning
evc ece 1 interface GigabitEthernet 1/9-10 policer none
!
vlan 1
!
!
!
ipmc profile Prof1
 description firstProfile in IPMC Profile Table
!
ipmc profile
!
ip route 0.0.0.0 0.0.0.0 192.168.1.254
tzidx 0
lacp on-air index 2 port GigabitEthernet 1/2
lacp on-air index 3 port GigabitEthernet 1/3
lacp on-air index 3 couple-ip 192.168.1.77 0.0.0.0
```

5-5.3 Upload

This page lets you export the switch configuration for maintenance needs. Any current configuration files will be exported as text format.

It is possible to upload a file from the web browser to all the files on the switch, except default-config, which is read-only.

Select the file to upload, select the destination file on the target, then click Upload Configuration.

If the destination is running-config, the file will be applied to the switch configuration. This can be done in two ways:

- **Replace**: The current configuration is fully replaced with the configuration in the uploaded file.
- **Merge**: The uploaded file is merged into running-config.

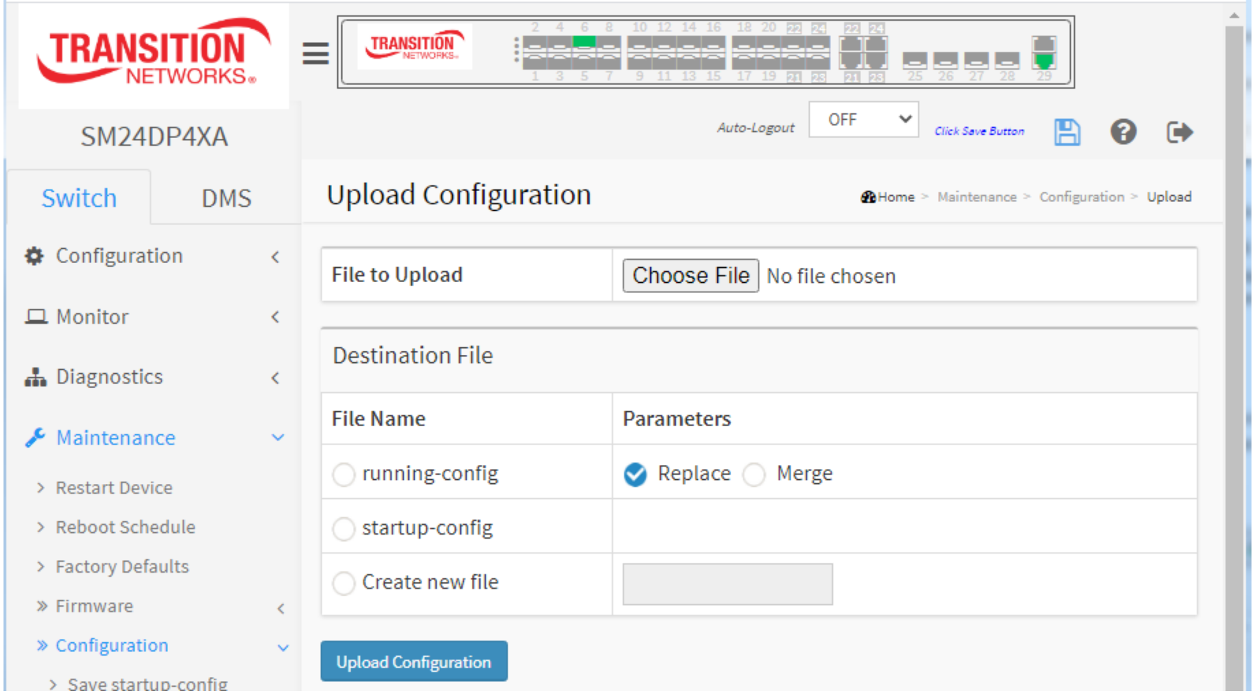
If the file system is full (i.e. contains the three system files mentioned above plus two other files), it is not possible to create new files, but an existing file must be overwritten or another deleted first.

Web Interface

To upload configuration in the web interface:

1. Click Maintenance, Configuration, Upload.
2. Click the Choose File button and navigate to and select the desired .IMGS file.
3. Select a Destination File. If you select "running-config", also select Replace or Merge.
4. Click the Upload Configuration button.

Figure 5-5.3: Upload Configuration



Upload Configuration

File to Upload	Choose File No file chosen

Destination File

File Name	Parameters
○ running-config	● Replace ○ Merge
○ startup-config	
○ Create new file	

Upload Configuration

Choose File : Click the button to search for and select the configuration filename.

Upload Configuration: Click the button then the switch will start to upload the configuration from its stored location.

5-5.4 Activate

It is possible to activate any of the configuration files present on the switch, except for running-config which represents the currently active configuration.

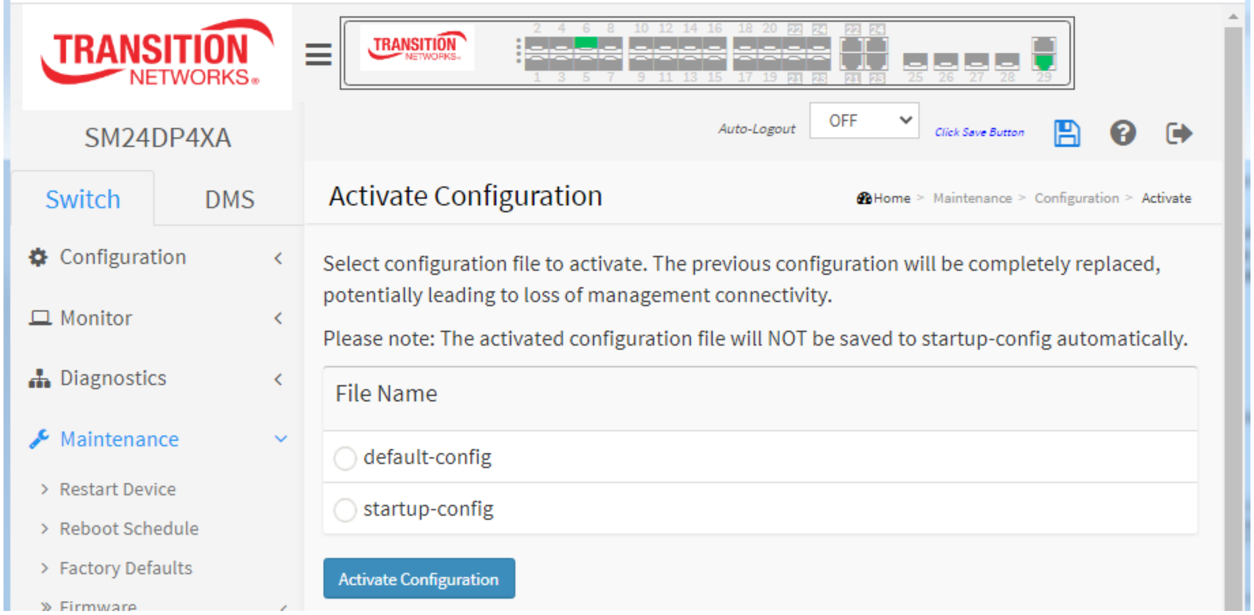
Select the file to activate and click Activate Configuration. This will initiate the process of completely replacing the existing configuration with that of the selected file. Please note: The activated configuration file will NOT be saved to startup-config automatically. The message "*No files available for activation*." displays if no files are available to activate.

Web Interface

To activate configuration in the web interface:

1. Click Maintenance, Configuration, Activate.
2. Select the desired filename (e.g., default-config or startup-config).
3. Click the Activate Configuration button.

Figure 5-5.4: Activate Configuration



Activate Configuration

Select configuration file to activate. The previous configuration will be completely replaced, potentially leading to loss of management connectivity.

Please note: The activated configuration file will NOT be saved to startup-config automatically.

File Name
○ default-config
○ startup-config

Activate Configuration

Parameter descriptions:

There are two system files:

1. **default-config**: A read-only file with vendor-specific configuration. This file is read when the system is restored to default settings.
2. **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.

5-5.5 Delete

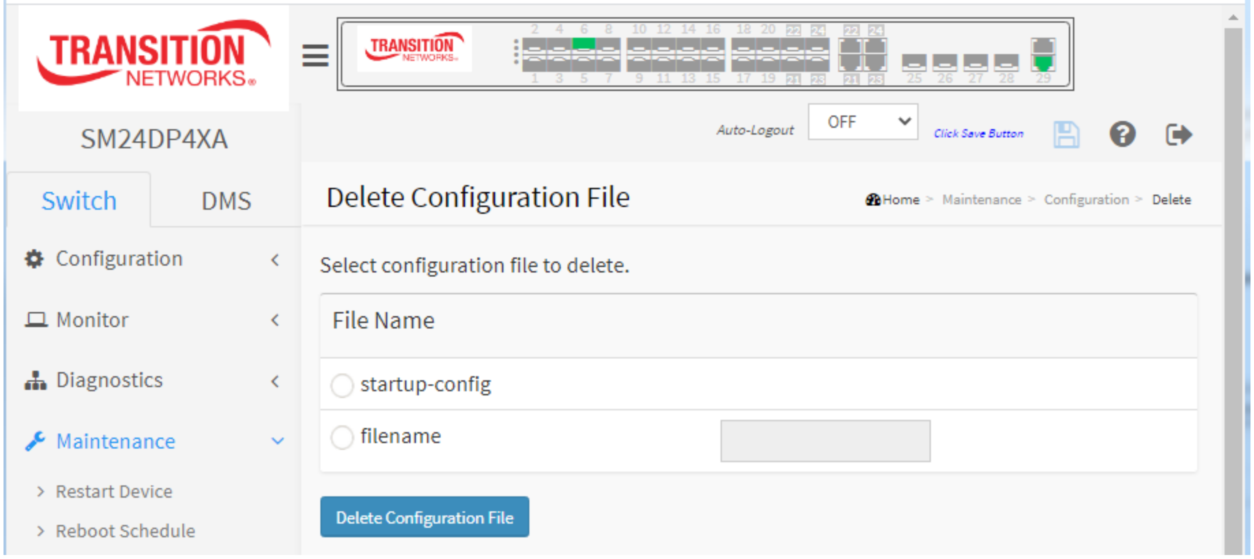
It is possible to delete any of the writable files stored in flash, including startup-config. If this is done and the switch is rebooted without a prior Save operation, this effectively resets the switch to default configuration.

Web Interface

To delete configuration in the web interface:

1. Click Maintenance, Configuration, Delete.
2. Select the desired file (e.g., startup-config). If none are available, the message "*No files available for deletion.*" displays.
3. Click the Delete Configuration File button.

Figure 5-4.5: Delete Configuration File



Delete Configuration File

Select configuration file to delete.

File Name
○ startup-config
○ filename

Parameter descriptions:

startup-config: The startup configuration for the switch, which is read at boot time.

Buttons :

Delete Configuration: Click the "Delete" button then the startup-config file will be deleted; this effectively resets the switch to default configuration.

5-5.6 Server Report

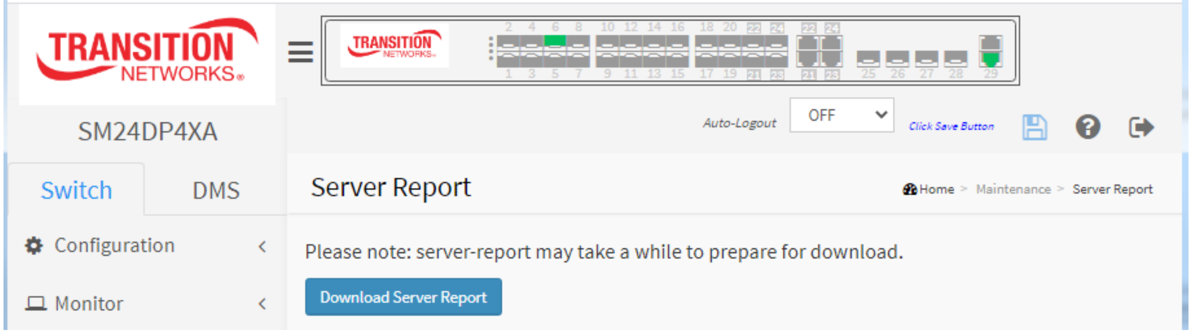
It is possible to download server report file on the switch to the web browser. Download of a Server Report may take a little while to complete, as the file must be prepared for download.

Web Interface

To download a server report file via the web interface:

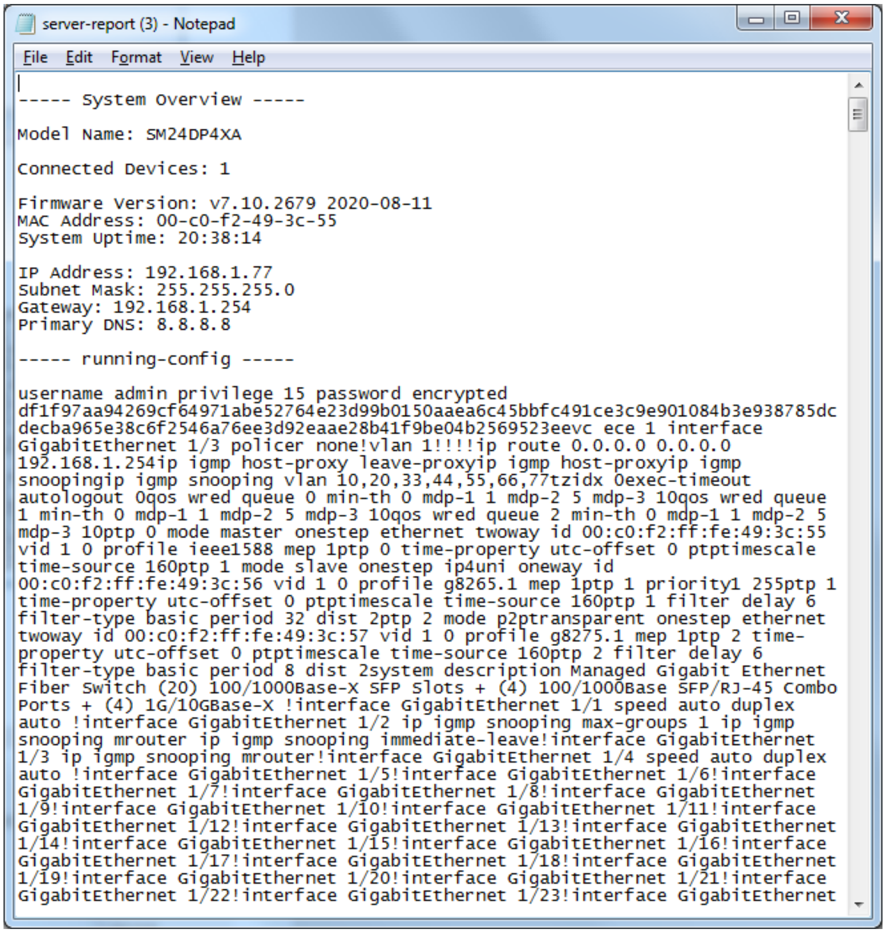
1. Click Maintenance, Server Report.
2. Open or save the report.

Figure 5-5.6: Server Report



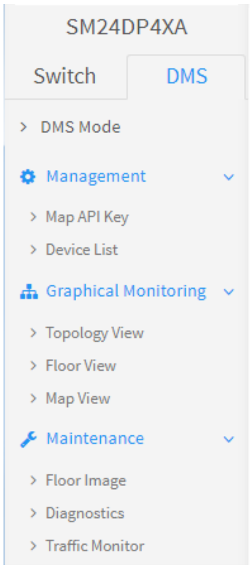
Please note: server-report may take a while to prepare for download.

A sample Server Report is shown below.



```
----- System Overview -----

Model Name: SM24DP4XA

Connected Devices: 1

Firmware Version: v7.10.2679 2020-08-11
MAC Address: 00-c0-f2-49-3c-55
System Uptime: 20:38:14

IP Address: 192.168.1.77
Subnet Mask: 255.255.255.0
Gateway: 192.168.1.254
Primary DNS: 8.8.8.8

----- running-config -----

username admin privilege 15 password encrypted
df1f97aa94269cf64971abe52764e23d99b0150aaea6c45bbfc491ce3c9e901084b3e938785dc
decba965e38c6f2546a76ee3d92eaae28b41f9be04b2569523eevc ece 1 interface
GigabitEthernet 1/3 policer none!vlan 1!!!!ip route 0.0.0.0 0.0.0.0
192.168.1.254ip igmp host-proxy leave-proxyip igmp host-proxyip igmp
snoopingip igmp snooping vlan 10,20,33,44,55,66,77tzidx 0exec-timeout
autologout 0qos wred queue 0 min-th 0 mdp-1 1 mdp-2 5 mdp-3 10qos wred queue
1 min-th 0 mdp-1 1 mdp-2 5 mdp-3 10qos wred queue 2 min-th 0 mdp-1 1 mdp-2 5
mdp-3 10ptp 0 mode master onestep ethernet twoway id 00:c0:f2:ff:fe:49:3c:55
vid 1 0 profile ieee1588 mep 1ptp 0 time-property utc-offset 0 ptptimescale
time-source 160ptp 1 mode slave onestep ip4uni oneway id
00:c0:f2:ff:fe:49:3c:56 vid 1 0 profile g8265.1 mep 1ptp 1 priority1 255ptp 1
time-property utc-offset 0 ptptimescale time-source 160ptp 1 filter delay 6
filter-type basic period 32 dist 2ptp 2 mode p2ptransparent onestep ethernet
twoway id 00:c0:f2:ff:fe:49:3c:57 vid 1 0 profile g8275.1 mep 1ptp 2 time-
property utc-offset 0 ptptimescale time-source 160ptp 2 filter delay 6
filter-type basic period 8 dist 2system description Managed Gigabit Ethernet
Fiber Switch (20) 100/1000Base-X SFP Slots + (4) 100/1000Base SFP/RJ-45 Combo
Ports + (4) 1G/10GBase-X !interface GigabitEthernet 1/1 speed auto duplex
auto !interface GigabitEthernet 1/2 ip igmp snooping max-groups 1 ip igmp
snooping mrouter ip igmp snooping immediate-leave!interface GigabitEthernet
1/3 ip igmp snooping mrouter!interface GigabitEthernet 1/4 speed auto duplex
auto !interface GigabitEthernet 1/5!interface GigabitEthernet 1/6!interface
GigabitEthernet 1/7!interface GigabitEthernet 1/8!interface GigabitEthernet
1/9!interface GigabitEthernet 1/10!interface GigabitEthernet 1/11!interface
GigabitEthernet 1/12!interface GigabitEthernet 1/13!interface GigabitEthernet
1/14!interface GigabitEthernet 1/15!interface GigabitEthernet 1/16!interface
GigabitEthernet 1/17!interface GigabitEthernet 1/18!interface GigabitEthernet
1/19!interface GigabitEthernet 1/20!interface GigabitEthernet 1/21!interface
GigabitEthernet 1/22!interface GigabitEthernet 1/23!interface GigabitEthernet
```

6. DMS (Device Management System)



6.1 Introduction to DMS

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 SM24DP4XA main menu pane on the left, navigate to the DMS tab to display the main DMS features: DMS Mode, Management, Graphical Monitoring, and Maintenance.

DMS features include:

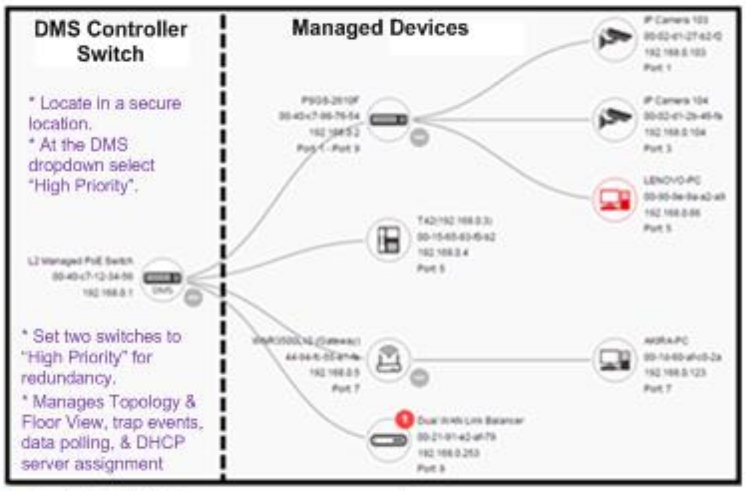
- DMS automatically discovers and displays all devices connected to the switch using standard networking protocols such as LLDP, UPnP, ONVIF, etc.
- DMS supports up to 256 devices within four subnets.
- DMS operates via an intuitive web GUI to allow you to:
  - Power down the IP cameras, NVRs, or any PoE devices.
  - Remotely identify the exact cable break location.
  - Detect abnormal traffic issues on IP cameras/NVR.
  - Monitor devices' status (e.g., link up, PoE power, traffic, etc.).
  - Configure VLAN/QoS intuitively for better solution quality/reliability.

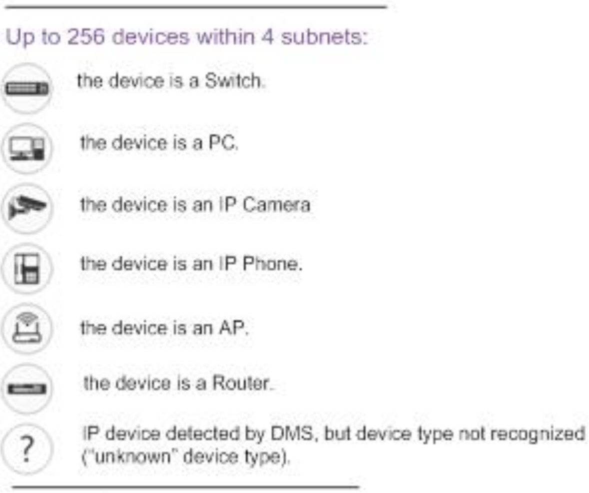
6.2 DMS Controller Switch

Configure DMS mode and monitor device numbers/ DMS Controller switch IP.

DMS is controlled by the DMS Controller switch, as specified by DMS Mode selection.

The DMS Controller switch is in charge of syncing DMS information in order to manage Topology View, Floor View, and trap event / data polling / DHCP server assignment.


DMS Controller Switch
* Locate in a secure location.
* At the DMS dropdown select "High Priority".
L2 Managed PoE Switch
DMS
* Set two switches to "High Priority" for redundancy.
* Manages Topology & Floor View, trap events, data polling, & DHCP server assignment
Managed Devices
IP Camera 103
IP Camera 104
LENOVO-PC
Dual WAN Link Balancer


Up to 256 devices within 4 subnets:

the device is a Switch.

the device is a PC.

the device is an IP Camera.

the device is an IP Phone.

the device is an AP.

the device is a Router.

? IP device detected by DMS, but device type not recognized ("unknown" device type).

6.3 DMS Controller Switch and Managed Devices

If there are more than two switches set as High-priority or no High-priority mode switch, the switch with the longer system uptime will be selected as the DMS Controller switch. If two switches have the same up time, the switch with the smaller MAC address will be assigned as the DMS Controller switch.

You can set two switches to High priority for Controller switch redundancy.

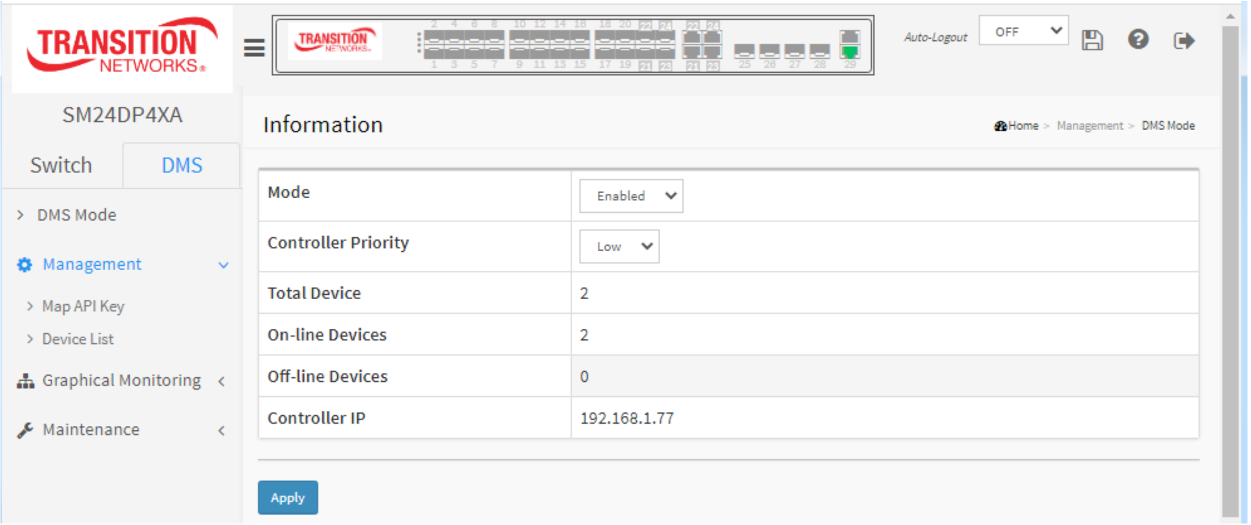
The DMS Controller Switch should be put in a secure location such as a server room, with access/authority limited to IT staff.

The DMS Controller Switch is the center of IP / Event management to operate the DMS:

- When enabled DHCP Server mode in DMS network, the DMS Controller switch is responsible for assigning IP address for all devices.
- The DMS Controller Switch will collect, poll, and sync DMS information, and act as the Event Notification control center to manage all device information.

6.4 DMS > DMS Mode

This page lets you set the DMS Mode and displays the discovered device and Controller IP information.



Information

Mode	Enabled
Controller Priority	Low
Total Device	2
On-line Devices	2
Off-line Devices	0
Controller IP	192.168.1.77

Parameter descriptions:

Mode : Enable or Disable the DMS function. The default is Enabled.

Controller Priority: Choose "Controller Priority" when DMS is enabled:

High: This switch will become the DMS Controller (Master) switch.

Mid: This switch will have medium level priority.

Low: This switch will have low level priority (default).

Non: This switch will never become the DMS 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 are on-line in Topology view.

Off-Line Devices : Shows how many IP devices are off-line in Topology view.

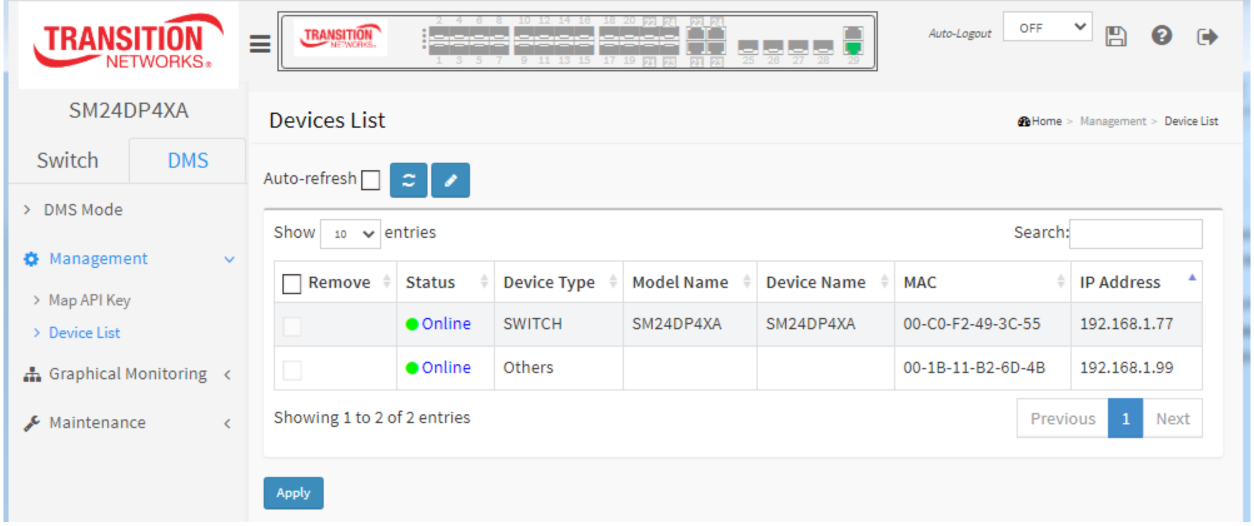
Controller IP : Shows the IP address of the DMS Controller (Master) device.

Buttons

Apply : Click to save changes.

6.5 DMS > Management > Device List

This page provides an overview of the devices in the DMS system.



Devices List

Auto-refresh □

Show 10 entries Search:

□ Remove	Status	Device Type	Model Name	Device Name	MAC	IP Address
□	● Online	SWITCH	SM24DP4XA	SM24DP4XA	00-C0-F2-49-3C-55	192.168.1.77
□	● Online	Others			00-1B-11-B2-6D-4B	192.168.1.99

Showing 1 to 2 of 2 entries Previous 1 Next

Apply

Parameter descriptions:

Remove : Check the box to remove off-line device from the list.

Status : Device Online or Offline. Click a linked status to display its Diagnostics page (see below).

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.

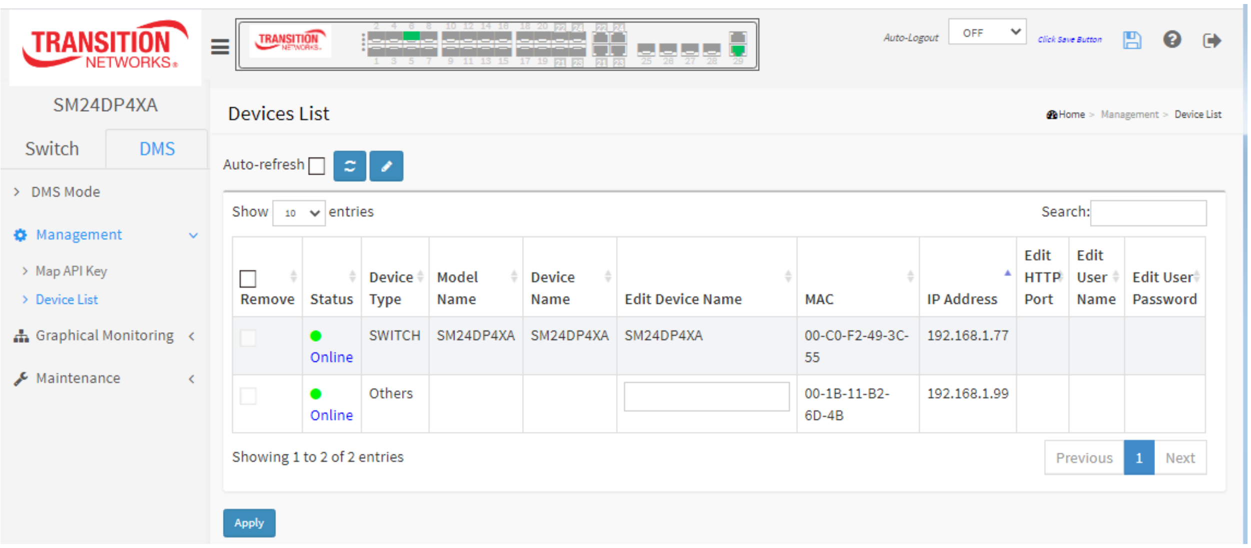
Refresh: Refreshes the displayed table starting from the input fields.

: **Edit device name** : Add the input fields for editing the device names and the HTTP ports. See below.

Apply : Click to save changes.

Editing Device Name

On the Devices List page you can click the **Edit Device Name** button (✎) to add an input field for editing the Device names. The HTTP port, User Name, and Password fields display.



Devices List

Auto-refresh □

Show 10 entries Search:

□ Remove	Status	Device Type	Model Name	Device Name	Edit Device Name	MAC	IP Address	Edit HTTP Port	Edit User Name	Edit User Password
□	● Online	SWITCH	SM24DP4XA	SM24DP4XA	SM24DP4XA	00-C0-F2-49-3C-55	192.168.1.77			
□	● Online	Others				00-1B-11-B2-6D-4B	192.168.1.99			

Showing 1 to 2 of 2 entries

Previous 1 Next

Apply

When you click the **Edit Device Name** button four new fields display:

Edit Device Name : Enter the type of the network connectivity device (PC, SWITCH, AP, IP Cam, IP Phone or Others).

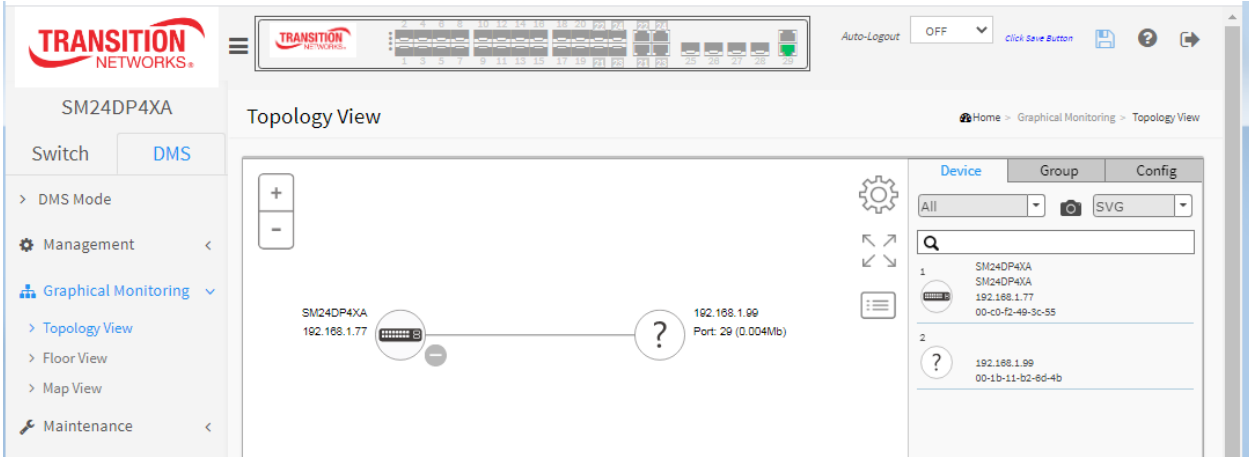
Edit Http Port : Shows the discovered HTTP port assigned.

Edit User Name : Shows the discovered login user name for the device.

Edit Password : Shows the discovered login password for the device.

6.6 DMS > Graphical Monitoring > Topology View

DMS automatically discovers all IP devices and displays the devices in graphic network Topology View. You can manage and monitor devices in the Topology View, such as to remotely diagnose the cable connection status, auto alarm notifications on critical events, remotely reboot PoE device when it's not alive. You can use the DMS platform to solve the abnormal issues anytime and anywhere by tablet or smart phone, and keep the network working smoothly.



Parameter descriptions:

Click **DMS** > **Graphical Monitoring** -> **Topology View** to view the network topology. The control icons are show and described below:

+ − : Plus and Minus icons: Zoom in and zoom out of Topology view; you can scroll up and down with mouse to achieve the same purpose.

⚙ : Click to alternately show/hide the Setting functions (Device, Group, Config tabs). Click the upper right corner "Setting icon" to pop up Device, Group, and Config tabs, with the export topology view and advanced search functions for Topology view, as described below.

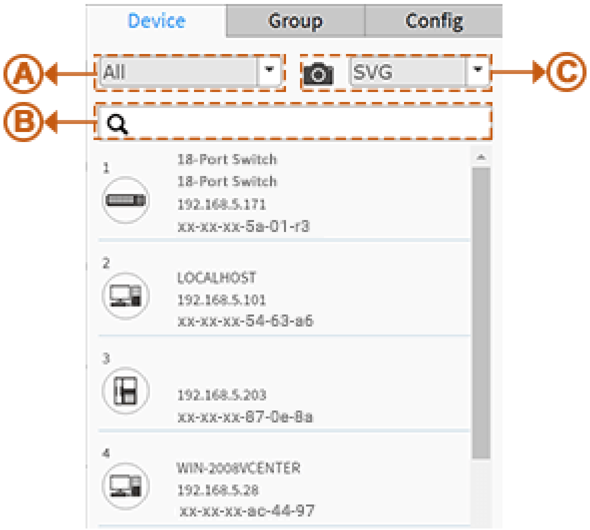
↖↗↙↘ ↘↙↗↖ : Click to alternately show full screen / partial screen. Icon with screen view type; click it to change to Full screen or return to the Normal View of Topology.

☑ Device Name
☑ Model Name
□ Mac
☑ IP
□ PoE

☰ : Click to alternately display and hide the "Device parameters " icon which lets you select the set of device parameters to display (Device Name, Model Name, Mac, IP, PoE). Not all parameters can be selected at the same time.

Setting icon (⚙) Functions (Device, Group, Config tabs)

1. Device Search Console



1
18-Port Switch
18-Port Switch
192.168.5.171
xx-xx-xx-5a-01-r3

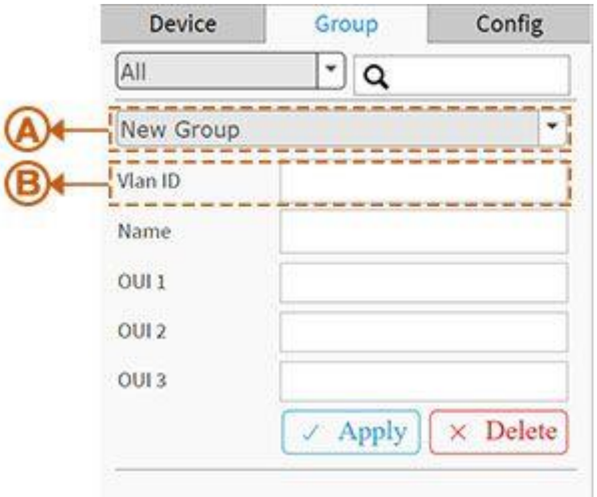
2
LOCALHOST
192.168.5.101
xx-xx-xx-54-63-a6

3
192.168.5.203
xx-xx-xx-87-0e-8a

4
WIN-2008VCENTER
192.168.5.28
xx-xx-xx-ac-44-97

Function	
A.	Filter devices by Device Type.
B.	Search devices by key words full text search.
C.	Save the whole View to SVG, PNG or PDF.

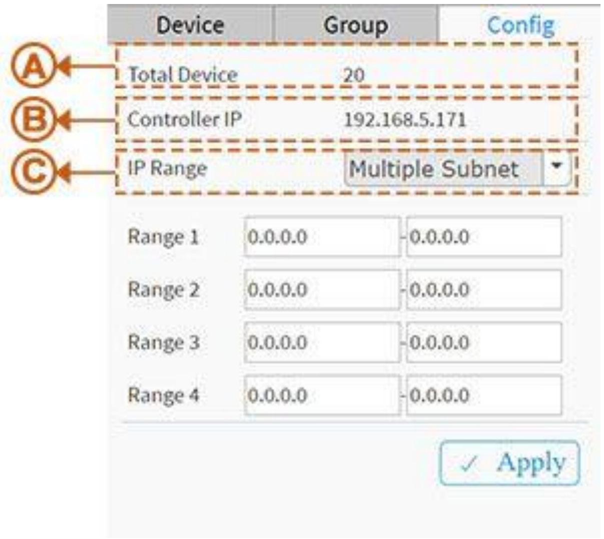
2. Group Setting Console



- Using Mac Based VLAN to isolate groups.
- One IP device only can join one VLAN group.

Function	
A.	Group devices by filtering, searching, clicking device icons, or specifying OUI.
B.	Assign VLAN ID or Name to Group.

3. System Setting Console



Device | Group | Config

Total Device 20

Controller IP 192.168.5.171

IP Range Multiple Subnet

Range 1 0.0.0.0 - 0.0.0.0

Range 2 0.0.0.0 - 0.0.0.0

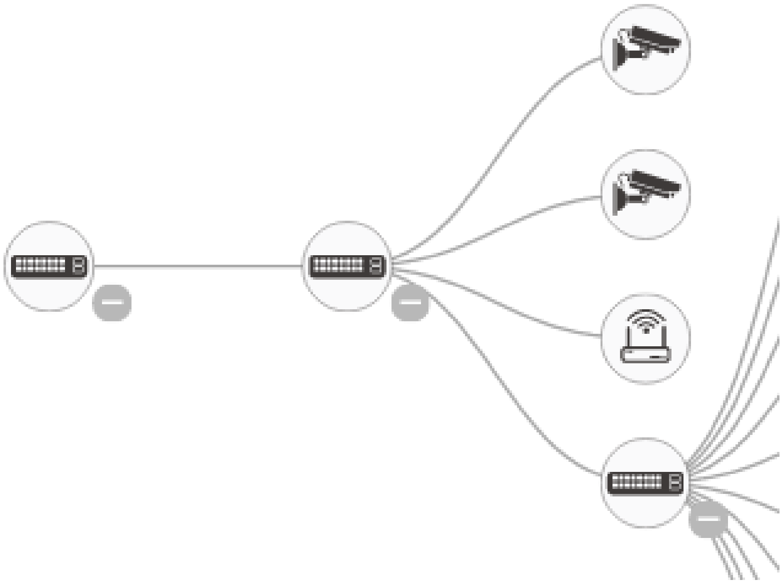
Range 3 0.0.0.0 - 0.0.0.0

Range 4 0.0.0.0 - 0.0.0.0

✓ Apply

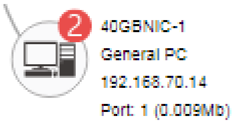
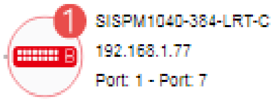
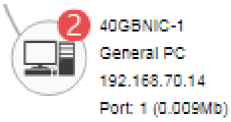
	Function
A.	Shows how many IP devices are detected and displayed in the topology view.
B.	Shows the Master IP.
C.	**Single Subnet:** DMS will base on the master switch's IP address. Here the subnet means "255.255.255.0" **Multiple Subnet:** To provide 4 ranges for inputting manually. (In this case, we suggest you also adjust the switch's subnet mask to "255.255.0.0" to avoid IP devices that can't be recognized.)

Device Tree View

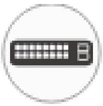
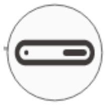
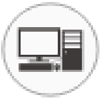
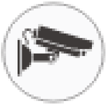
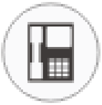
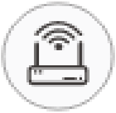


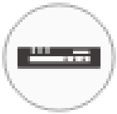
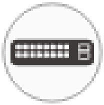
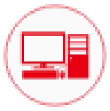
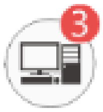
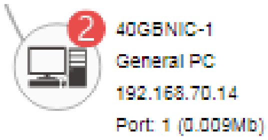
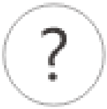
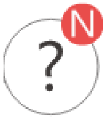
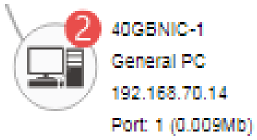
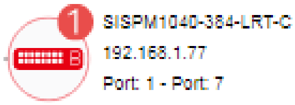
Topology View Icons / Controls

Click anywhere and drag to move the display area up /down/ left /right.

+ -	Click “+” or “-” to zoom in or zoom out the display area.
 2 40GBNIC-1 General PC 192.168.70.14 Port: 1 (0.009Mb)	A Black device icon indicates device is operating normally. Click a device icon to show its device console.
 1 SISPM1040-384-LRT-C 192.168.1.77 Port: 1 - Port: 7	A Red device icon indicates the device is operating abnormally.
 2 40GBNIC-1 General PC 192.168.70.14 Port: 1 (0.009Mb)	A Red circled device number shows the number of alarm notifications for the device.
☰	Click this icon to select the set of information to be displayed (MAC, IP, PoE power, etc.).
Config	Click this icon to sort, filter, or configure basic settings (e.g., VLAN, QoS).

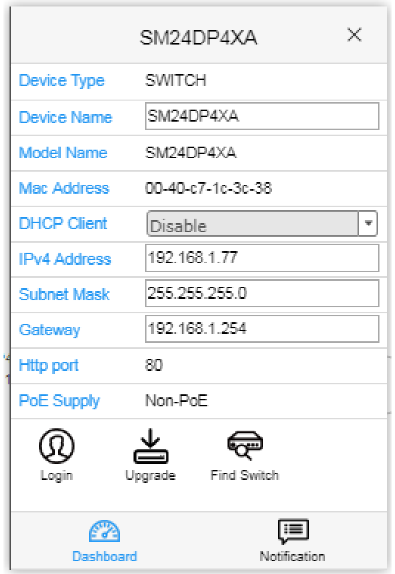
Device Categories and Statuses

	The device is a Switch.
	The device is a General switch.
	The device is a PC.
	The device is an IP Cam.
	The device is an IP Phone.
	The device is a Wireless Access Point (WAP).

	The device is a Router.
	Black icon: Device link up. You can select a function and check for issues.
	Red icon: Device link down. You can diagnose the link status.
	Icon with number: indicates some event has occurred (e.g. Device Off-line, IP Duplicate, etc.) on the IP device; you can click on the device icon to check events in Notification.
 2 40GBNIC-1 General PC 192.168.70.14 Port: 1 (0.009Mb)	A Red circled device number shows the number of alarm notifications for the device.
	Icon with question mark: Unknown Device; the IP device is detected by DMS, but the device type can't be recognized which will be classified as an unknown device type.
	Icon with question mark and red N:indicates the device is unknown and id not connected.
 2 40GBNIC-1 General PC 192.168.70.14 Port: 1 (0.009Mb)	A Black device icon indicates device is operating normally. Click device icon to show its device console.
 1 SISPM1040-384-LRT-C 192.168.1.77 Port: 1 - Port: 7	A Red device icon indicates the device is operating abnormally.

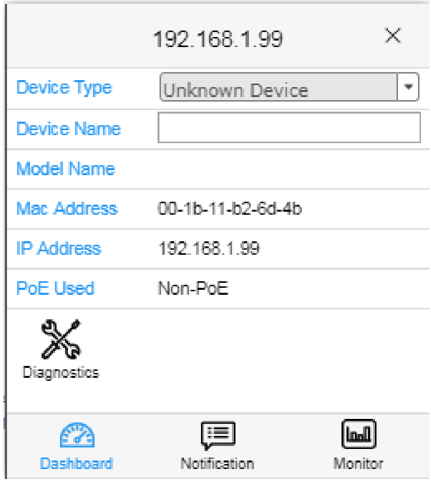
Device Consoles

Left-click any device icon to display the device consoles for further actions:



SM24DP4XA ×

Device Type	SWITCH
Device Name	SM24DP4XA
Model Name	SM24DP4XA
Mac Address	00-40-c7-1c-3c-38
DHCP Client	Disable
IPv4 Address	192.168.1.77
Subnet Mask	255.255.255.0
Gateway	192.168.1.254
Http port	80
PoE Supply	Non-PoE



192.168.1.99 ×

Device Type	Unknown Device
Device Name	
Model Name	
Mac Address	00-1b-11-b2-6d-4b
IP Address	192.168.1.99
PoE Used	Non-PoE

Dashboard Console: Displays device info and related actions for the device. Different device types support different functions:

- If an IP device is recognized as DMS switch, it will support "Upgrade" and "Find Switch" function.
- If an IP device is recognized as PoE device, it will support more "Reboot" function in addition to "Upgrade".
- If an IP device is recognized as IP Cam via ONVIF protocol, it will support "Streaming" function.

Device Type: Displays automatically. If an unknown type is detected, you can still select type from a pre-defined list.

Device Name: Create your own Device Name or alias for easy management (e.g., 1F_Lobby_Cam1).

Model Name, MAC Address, IP Address, Subnet Mask, Gateway, PoE Supply and PoE Used are displayed automatically by DMS.

Http Port: Re-assign HTTP port number to the device for better security.

Login

Login: Click the Login Action Icon to log in the device via HTTP for further configuration or status monitoring.

Upgrade

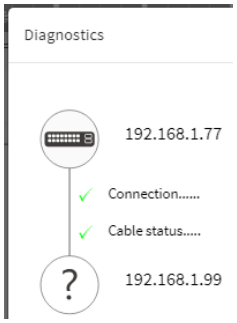
Upgrade: Click to upgrade the device’s software version. The current device Name, IP address, Version, and Status display. Enter a Tftp Server IP address and firmware File name, then click the Apply (✓ Apply) button.

Find Switch

Find Switch: When this feature is activated, the switch LED all flicker for 15 seconds.

Diagnostics

Diagnostics: Click Diagnostic Action Icon to perform the cable diagnostics, to exam where the broken cable is, and, check if the device connection is alive by ping.



Cable Status:

- **Green icon:** Cable is connected correctly.
- **Red icon:** Cable is not connected correctly. User can check the distance info (XX meters) to identify the broken cable location.

Connection:

- **Green icon:** Device is pinged correctly.
- **Red icon:** Device is not transmitted /receiving data correctly, which means it might not be pinged successfully.

Reboot

Reboot: Click Reboot Action Icon to reboot the device remotely so as recover the device back to its normal operation.

Streaming

Streaming: Click Streaming Action Icon to display the video images streaming, if the device supports this feature.

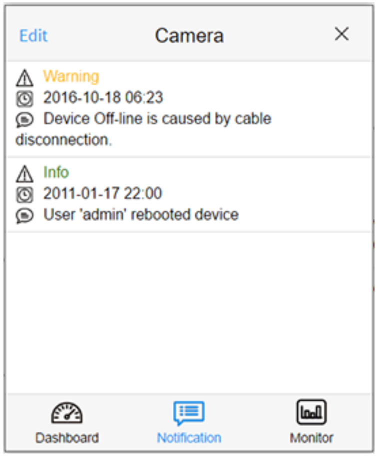
Parent Node

Parent Node: When DMS switch detects more than two IP devices from the same port, switch can't resolve this IP device's layout, instead, it will show a blank node to present this situation. User can use "Parent Node" function to adjust layout in Dashboard.

PoE Config

PoE Config: Click it to configure the PoE function, enable/disable PoE Auto Checking and enable/disable PoE mode for per port.

Notification Console: Displays alarms and logs triggered by events.



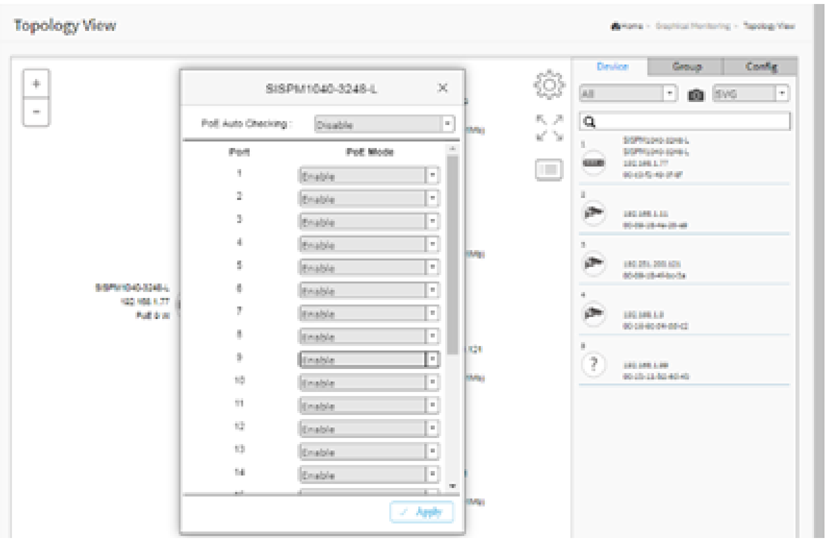
Warning
2016-10-18 06:23
Device Off-line is caused by cable disconnection.

Info
2011-01-17 22:00
User 'admin' rebooted device

PoE Auto Checking “AutoFill” Feature

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

1. Configure the “PoE Auto Checking” parameter at Switch > PoE Management > PoE Auto Checking. The default value of the “Failure Action” parameter is “Reboot Remote PD”. Note that “PoE Auto Checking” is called “PoE Auto Power Reset” in earlier firmware versions.
2. Configure PoE parameters at DMS > Graphical Monitoring > Topology View. Left click on the switch icon to display its device configuration popup. Click the PoE Config (PoE Config) icon to display the PoE Auto Checking pane:



Topology View

SISPM1040-3248-L

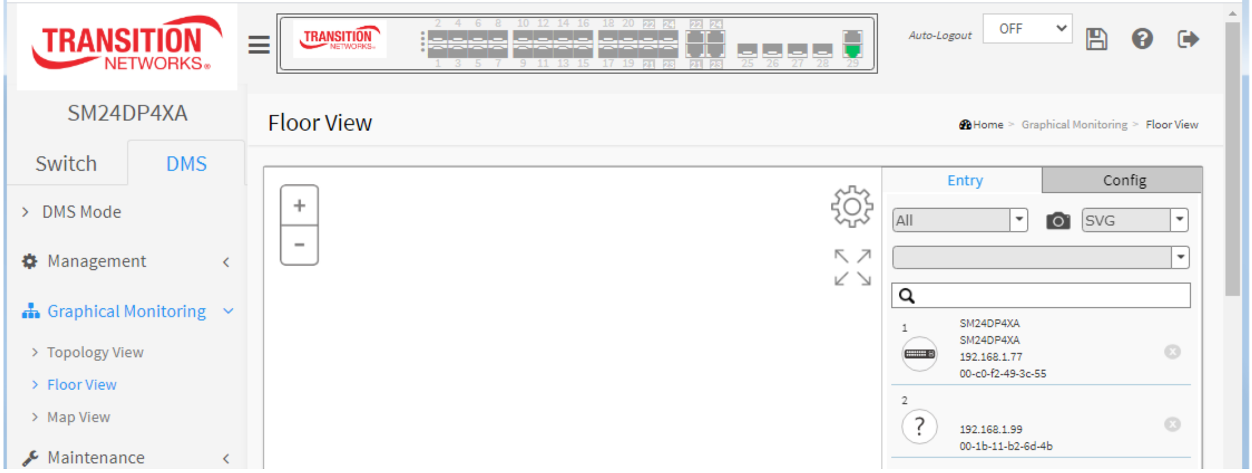
PoE Auto Checking : Disable

Port	PoE Mode
1	Enable
2	Enable
3	Enable
4	Enable
5	Enable
6	Enable
7	Enable
8	Enable
9	Enable
10	Enable
11	Enable
12	Enable
13	Enable
14	Enable

6.7 DMS > Graphical Monitoring > Floor View

This page lets you plan IP devices installation location onto the custom uploaded floor images. You must first add the images at DMS > Maintenance > Floor Image. Floor View functions include:

- Anchor Devices onto Floor Maps
- Find Device location instantly
- 10 Maps can be stored in each Switch
- IP Surveillance/VoIP/Wi-Fi applications
- Other features the same as Topology View
- To place and remove a device icon:
    - Select a device and click its icon from the device list. The device icon will show on the floor image's default location.
    - Click and hold left mouse by dragging-and-dropping the icon to the correct location on the floor view.
    - Click cross sign on the right side of device icon to remove a device from all floor view images.



1
SM24DP4XA
SM24DP4XA
192.168.1.77
00-c0-f2-49-3c-55

2
?
192.168.1.99
00-1b-11-b2-6d-4b

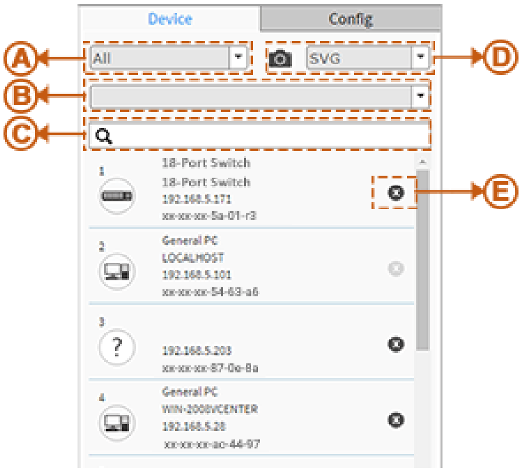
Parameter descriptions:

+ − : Plus and Minus icons: Zoom in and zoom out of Topology view; you can scroll up and down with mouse to achieve the same purpose.

⚙ : Click the upper right corner "Setting icon" to pop up Device, Group, and Config tabs, with the export topology view and advanced search functions for Topology view, as described below.

↖↗↙↘ ↘↙↗↖ : Click to alternately show full screen / partial screen. Icon with screen view type; click it to change to Full screen or return to the Normal View of Topology.

1. Device Search Console



1
18-Port Switch
18-Port Switch
192.168.5.171
xx-xx-xx-5a-01-r3

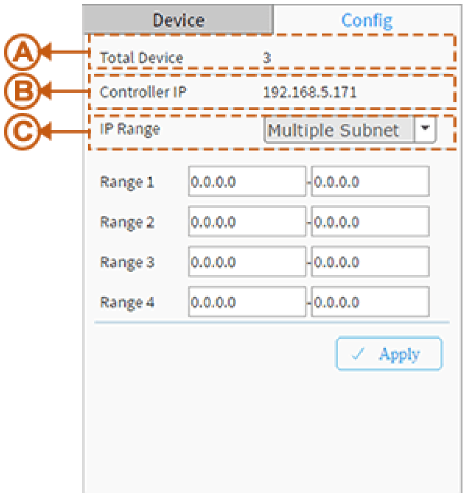
2
General PC
LOCALHOST
192.168.5.101
xx-xx-xx-54-63-a6

3
192.168.5.203
xx-xx-xx-87-0e-8a

4
General PC
WIN-2008VCENTER
192.168.5.28
xx-xx-xx-ac-44-97

Function	
A.	Filter devices by Device Type
B.	Select floor images
C.	Search devices by key words full text search
D.	Save the whole View to SVG, PNG or PDF
E.	Remove a device from all floor view images

2. System Setting Console



Total Device 3
Controller IP 192.168.5.171
IP Range Multiple Subnet
Range 1 0.0.0.0 - 0.0.0.0
Range 2 0.0.0.0 - 0.0.0.0
Range 3 0.0.0.0 - 0.0.0.0
Range 4 0.0.0.0 - 0.0.0.0

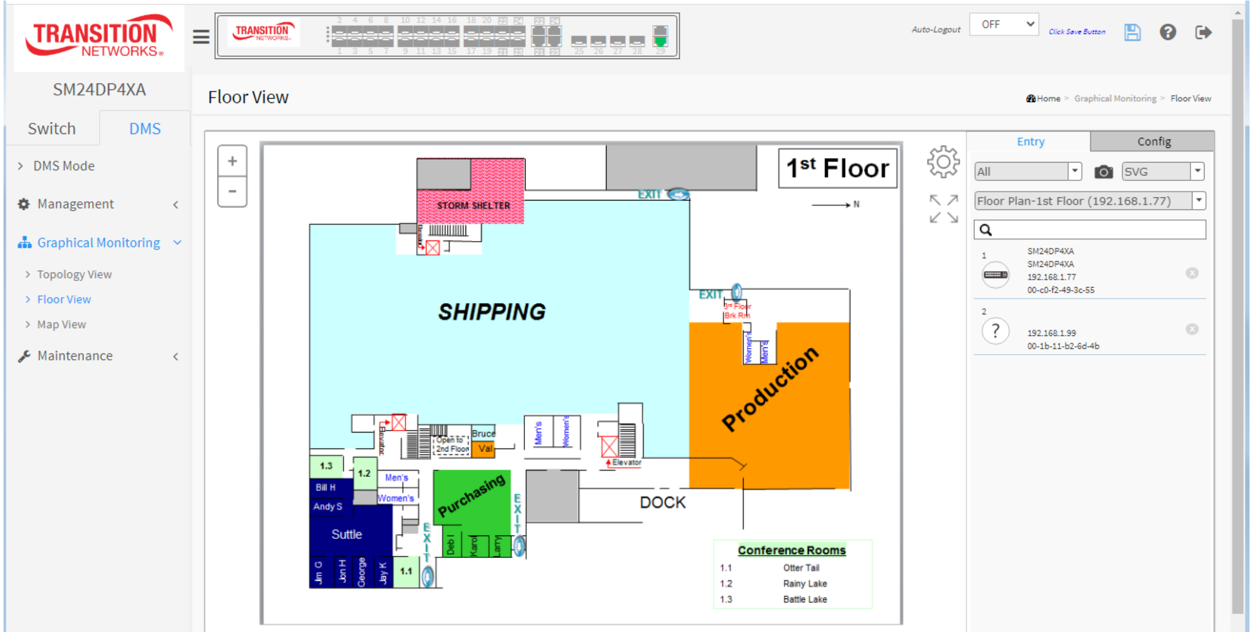
Function	
A.	Shows how many IP devices are detected and displayed in the topology view.
B.	Shows the Master IP.
C.	**Single Subnet:** DMS will base on the master switch's IP address. Here the subnet means "255.255.255.0".
	Multiple Subnet: To provide 4 ranges for inputting manually. (In the case, we suggest you adjust the switch's subnet mask to "255.255.0.0" to avoid IP devices can't be recognized.)

Device Status

Icon with black mark: Device link up. You can select function and check issues.

Icon with red mark: Device link down. You can diagnose the link status.

Example



SM24DP4XA

Switch | DMS

- DMS Mode
- Management
- Graphical Monitoring
  - Topology View
  - Floor View
  - Map View
- Maintenance

Auto-Logout: OFF

Click Save Button

Floor View

Home > Graphical Monitoring > Floor View

Entry | Config

All | SVG

Floor Plan-1st Floor (192.168.1.77)

1
SM24DP4XA
SM24DP4XA
192.168.1.77
00-c0-f2-49-3c-55

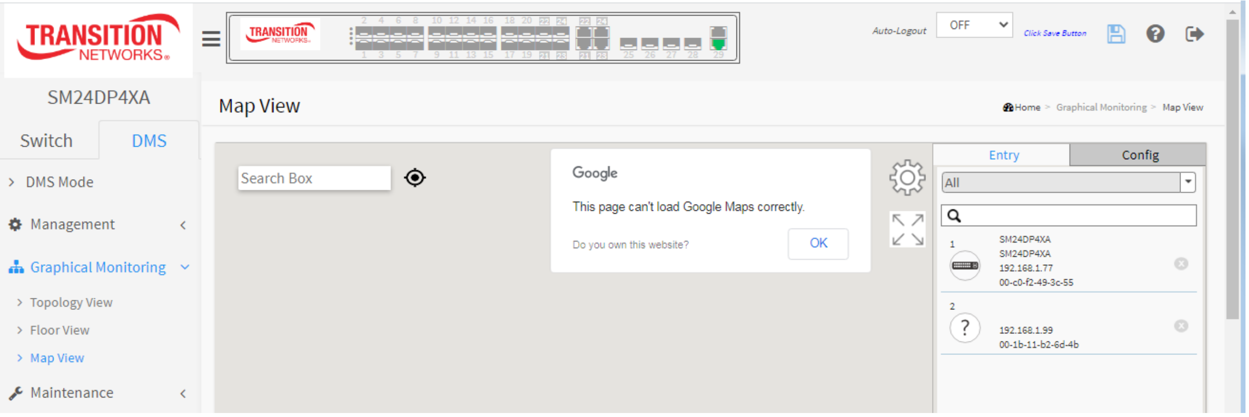
2
192.168.1.99
00-1b-11-b2-6d-4b

6.8 DMS > Graphical Monitoring > Map View

This page lets you find the location of the devices even they are installed in different building. You can place devices icon on the Map View where you can navigate using Google Maps.

Map View Functions

- Anchor devices onto Google Maps.
- Find devices Instantly from Map.
- On-Line search company/address.
- Outdoor IP Cam/Wi-Fi Applications.
- Other features the same as Topology view
- To place and remove a device icon:
    - Select a device and click its icon in the device list. The device icon will show on the map's default location.
    - Click and hold left mouse to drag-and-drop the icon to the correct location on the Map view.
    - Click the cross sign on the right side of a device icon to remove it from Map view.



Google

This page can't load Google Maps correctly.

Do you own this website?

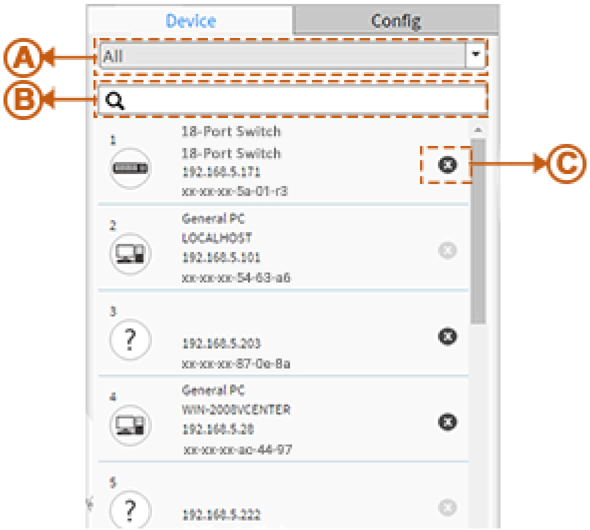
1 SM24DP4XA SM24DP4XA 192.168.1.77 00-c0-f2-49-3c-55

2 192.168.1.99 00-1b-11-b2-6d-4b

Parameter descriptions:

⚙ Click the upper right corner "Setting icon" to pop-up Device and Config tabs, and advanced search functions for the device.

1. Device Search Console



All

1
18-Port Switch
18-Port Switch
192.168.5.171
xx-xx-xx-5a-01-r3

2
General PC
LOCALHOST
192.168.5.101
xx-xx-xx-54-63-a6

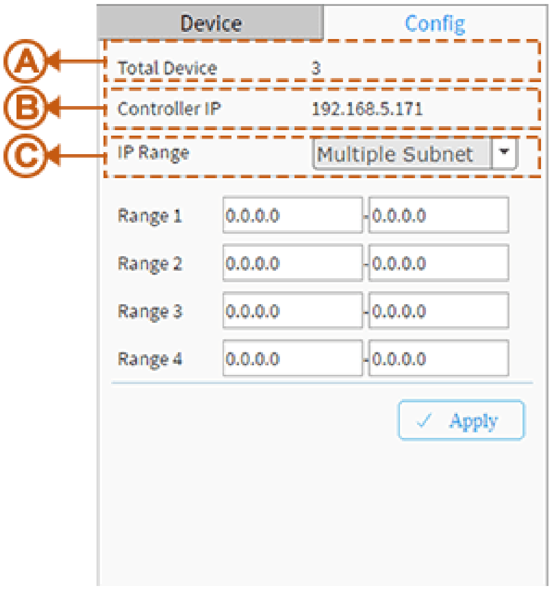
3
?
192.168.5.203
xx-xx-xx-87-0e-8a

4
General PC
WIN-2008VCENTER
192.168.5.28
xx-xx-xx-ac-44-97

5
?
192.168.5.222

Function	
A.	Filter devices by Device Type
B.	Search devices by key words full text search
C.	Remove a device from map view

2. System Setting Console



Total Device 3

Controller IP 192.168.5.171

IP Range Multiple Subnet

Range 1 0.0.0.0 - 0.0.0.0

Range 2 0.0.0.0 - 0.0.0.0

Range 3 0.0.0.0 - 0.0.0.0

Range 4 0.0.0.0 - 0.0.0.0

Function	
A.	Shows how many IP devices are detected and displayed in the topology view.
B.	Shows the Master IP.
C.	**Single Subnet:** DMS will base on the master switch's IP address. Here the subnet means "255.255.255.0"
	Multiple Subnet: To provide 4 ranges for inputting manually (in the case, we suggest you adjust the switch's subnet mask to "255.255.0.0" also to avoid IP devices can't be recognized.)

Icon with screen view type: Click it to change to Full Screen View of Map or return to the Normal View.

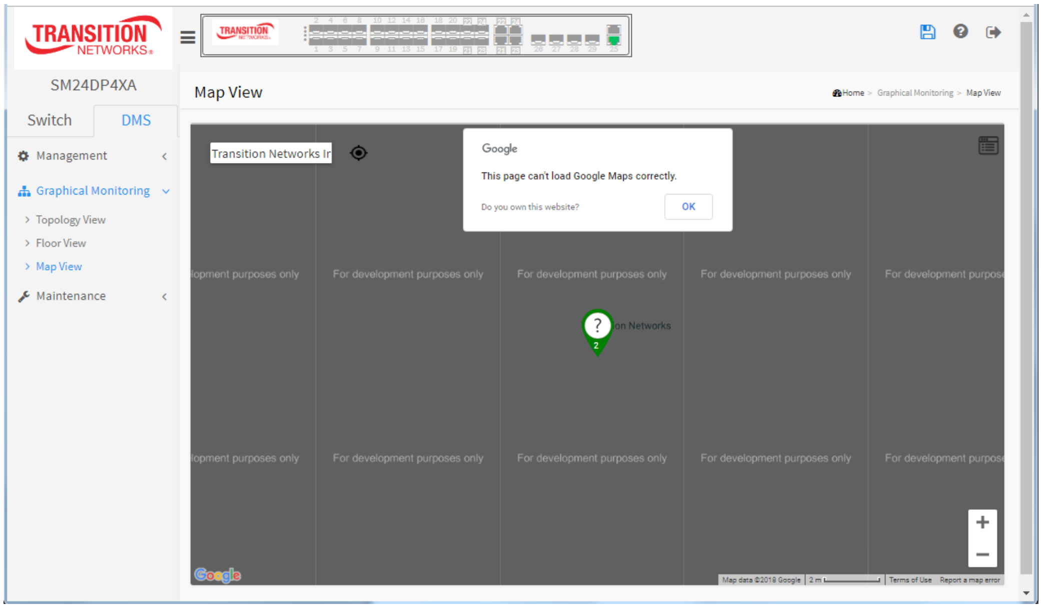
Device Status

Icon with black mark: Device link up. You can select function and check issues.

Icon with red mark: Device link down. You can diagnose the link status.

Message: *This page can't load Google Maps correctly.*

Message: *Oops! Something went wrong. This page didn't load Google Maps correctly. See the JavaScript console for technical details.*



Google

This page can't load Google Maps correctly.

Do you own this website?

OK

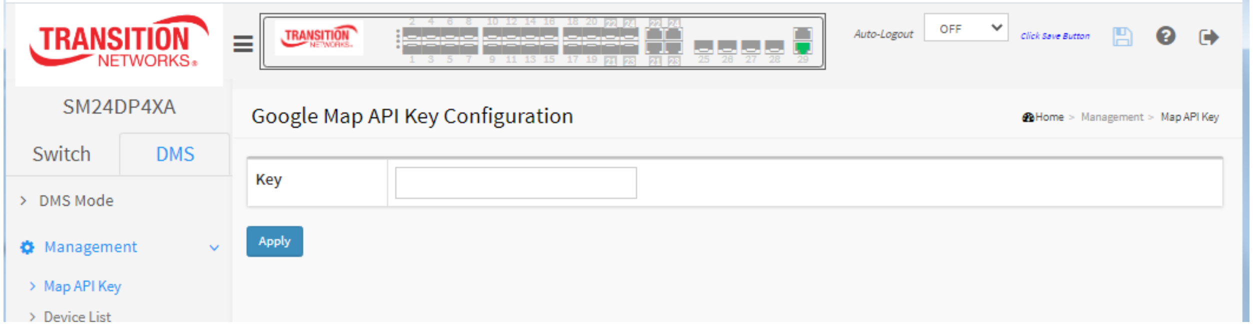
Meaning :

Recovery : **1.** Click the **OK** button to clear the webpage message. **2.** Continue with the Map API Key section below.

6.9 DMS > Management > Map API Key

This page lets you set up the Google Map API Key. You will need a valid API key and a Google Cloud Platform billing account to access Google core product. If not, DMS Map View will not be able to load Google Maps correctly. Visit the Google website below and follow the directions to get an API key:

https://developers.google.com/maps/documentation/directions/get-api-key



Google Map API Key Configuration

Key	

Parameter descriptions:

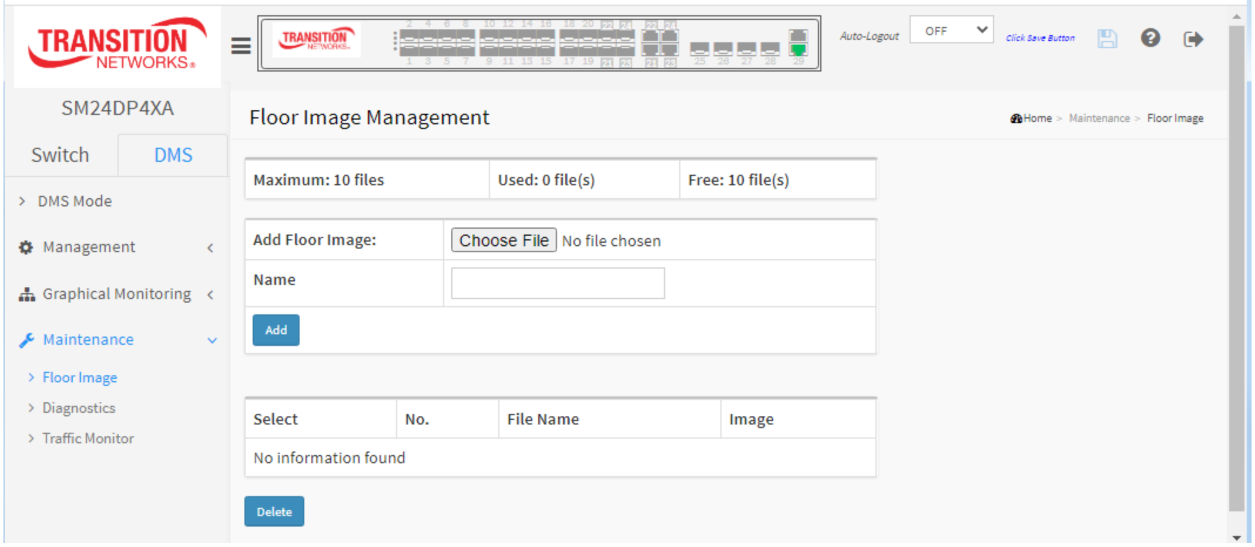
Key : Enter the Google API Key.

Buttons

Apply : Click to save changes.

6.10 DMS > Maintenance > Floor Image

Navigate to DMS > Maintenance > Floor Image to display the Floor Image Management page:



Floor Image Management

Maximum: 10 files	Used: 0 file(s)	Free: 10 file(s)

Add Floor Image:	Choose File No file chosen
Name	

Select	No.	File Name	Image
No information found			

Parameter descriptions:

Maximum: x files: By default this field displays "Maximum: 10 files". With each switch added and discovered, the maximum value increases by 10. For example, if only two switches are connected to each other, the maximum number of files will increase from 10 to 20 (on both switches). But once the connection is removed and after an approximate 1 minute wait, the maximum number of files will restore to 10.

The maximum number of images displayed is additive. When the switch is stand alone with no connections to other DMS switches, the number displayed is 10. As other DMS switches are added, the field is incremented by 10 for each one.

Used: x file(s): The number of files that have already been uploaded.

Free: x file(s): The number of files that can be uploaded before reaching the maximum number of images.

Choose File : Select the checkbox to select an image from the list.

Name : Shows file name selected; only jpg and png files are allowed. Special Characters are not allowed in Name.

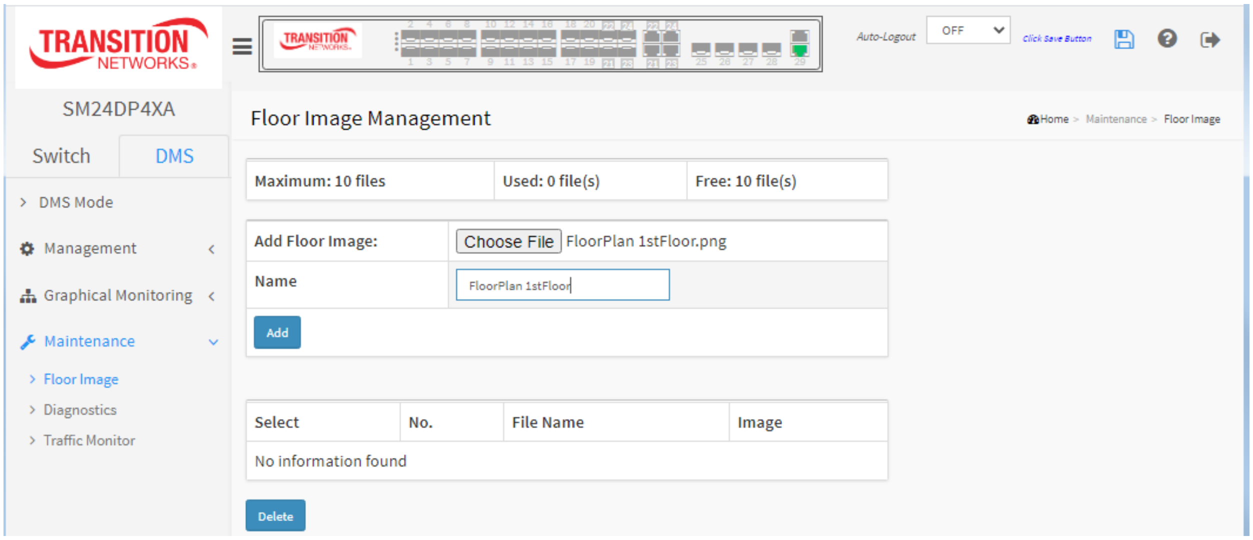
Buttons

Add: Click Add to upload. When done, a snapshot will be available on screen.

Delete: To remove an existing floor map, select its checkbox and click Delete to remove.

Examples:

A Floor Image file selected:



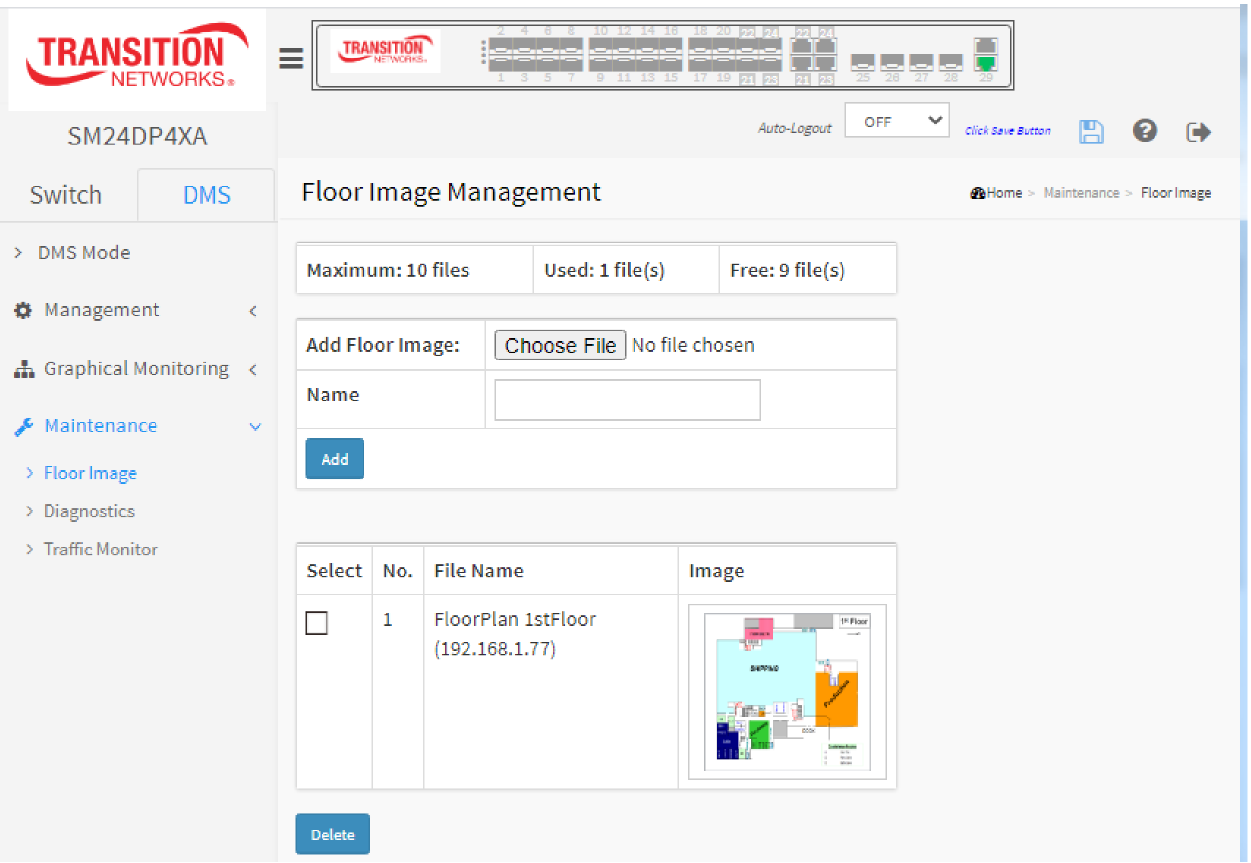
Floor Image Management

Maximum: 10 files	Used: 0 file(s)	Free: 10 file(s)

Add Floor Image:	Choose File FloorPlan 1stFloor.png
Name	FloorPlan 1stFloor

Select	No.	File Name	Image
No information found			

A Floor Image file added:



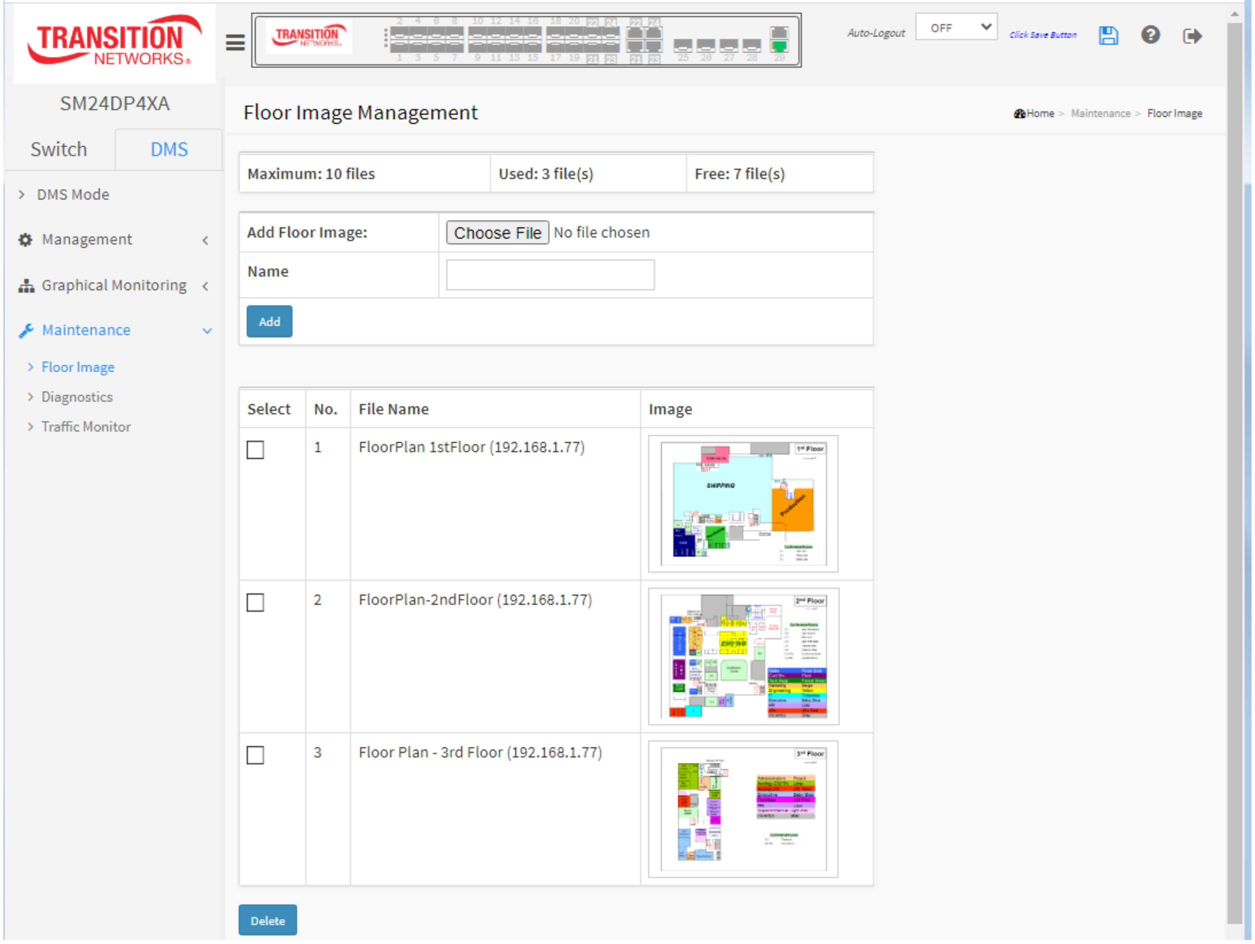
Floor Image Management

Maximum: 10 files	Used: 1 file(s)	Free: 9 file(s)

Add Floor Image:	Choose File No file chosen
Name	

Select	No.	File Name	Image
□	1	FloorPlan 1stFloor (192.168.1.77)	

Three Floor Image files added:



Floor Image Management

Maximum: 10 files	Used: 3 file(s)	Free: 7 file(s)

Add Floor Image:	Choose File No file chosen
Name	

Select	No.	File Name	Image
□	1	FloorPlan 1stFloor (192.168.1.77)	
□	2	FloorPlan-2ndFloor (192.168.1.77)	
□	3	Floor Plan - 3rd Floor (192.168.1.77)	

Message: *192.168.1.77 says: Insufficient Space. Only x files available.*

Meaning: The file is too large or no file exists.

Recovery: Click the **OK** button to clear the message and choose a new File Name to add.

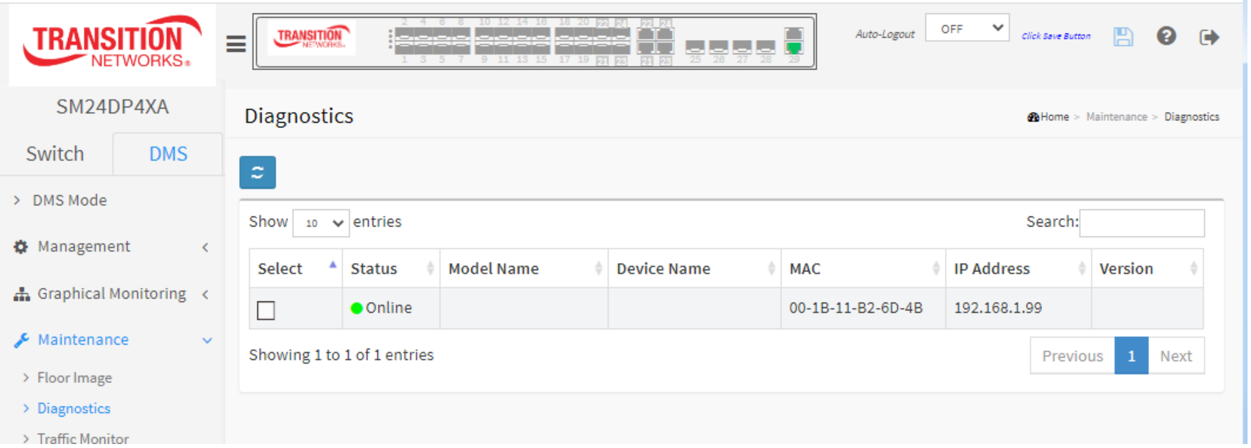
Message: Special Characters are not allowed in Name.

Meaning: The Floor Image filename has special characters (dash, space, numbers, etc.) which are not allowed.

Recovery: Click the **OK** button to clear the message and choose a File Name with no special characters.

6.11 DMS > Maintenance > Diagnostics

This page provides an overview of the Diagnostics.



Diagnostics

Auto-Logout: OFF

Show 10 entries   Search:

Select	Status	Model Name	Device Name	MAC	IP Address	Version
□	● Online			00-1B-11-B2-6D-4B	192.168.1.99	

Showing 1 to 1 of 1 entries   Previous 1 Next

Parameter descriptions:

Select : Check the box to select a device on which to run its Connection and Cable status diagnostic.

Status : Device Online or Offline.

Model Name : The model name of the network connectivity devices.

Device Name : The device name of the network connectivity devices.

MAC : The mac address of the device.

IP Address : The IP address of the network connectivity devices.

Version : The Version of the network connectivity devices.

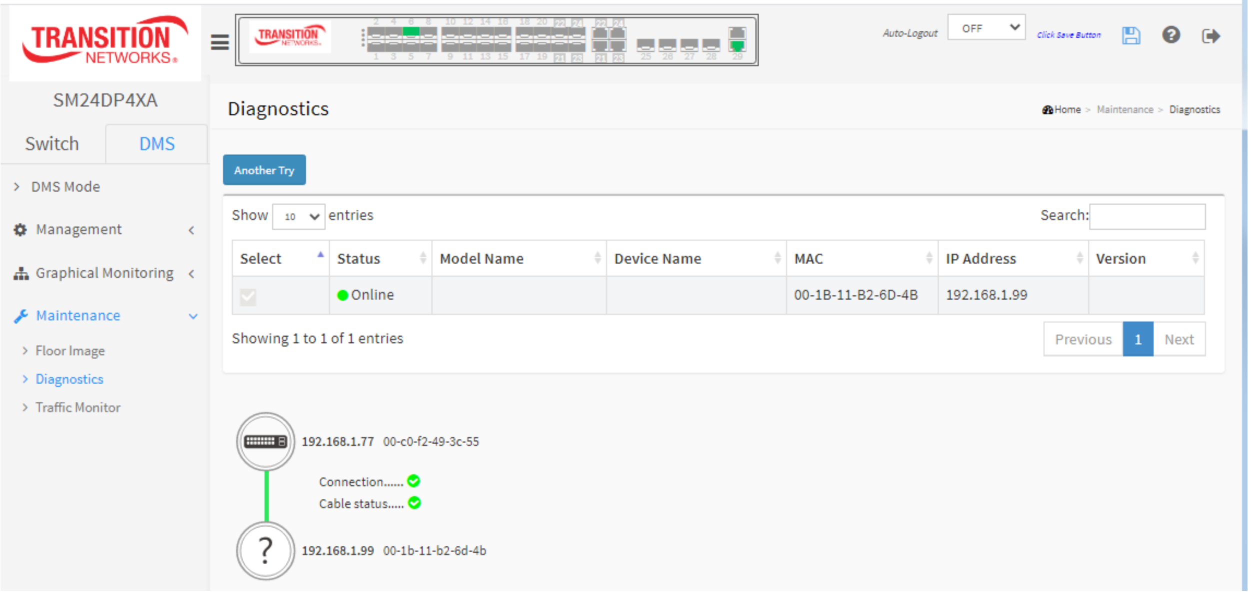
Buttons

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

Search : Search for any key word you want.

Another try : Click leave the Diagnostics result page and go back to the DMS > Maintenance > Diagnostics page.

At DMS > Maintenance > Diagnostics, check the **Select** checkbox to run a Connection and Cable status diagnostic:



Diagnostics

Show 10 entries Search:

Select	Status	Model Name	Device Name	MAC	IP Address	Version
☑	● Online			00-1B-11-B2-6D-4B	192.168.1.99	

Showing 1 to 1 of 1 entries

192.168.1.77 00-c0-f2-49-3c-55

Connection...... ✓
Cable status..... ✓

192.168.1.99 00-1b-11-b2-6d-4b

Click the **Another try** button to the DMS > Maintenance > Diagnostics page.

Diagnostics Results:

Connection...... ● : The connection diagnostic was successful (green dot).

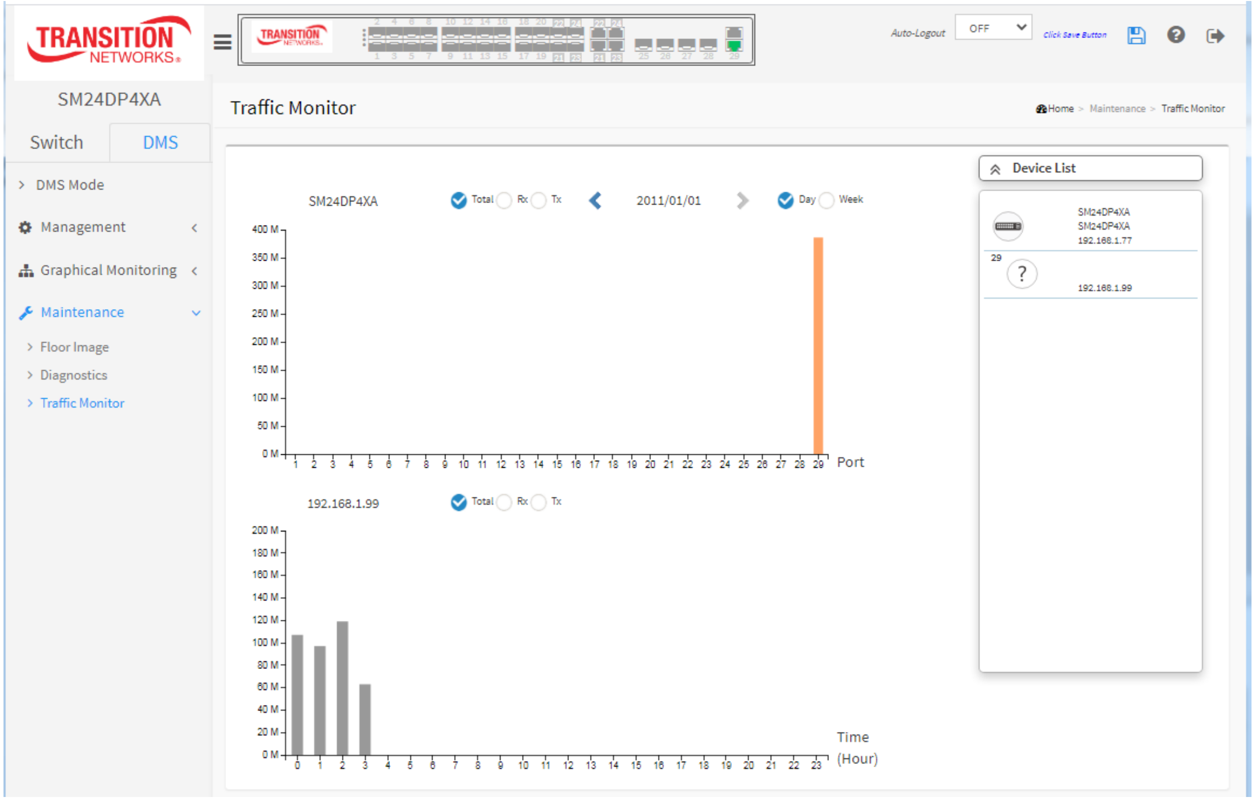
Connection...... ● : The connection diagnostic was unsuccessful (red dot).

Cable status..... ● : The cable status diagnostic was successful (green dot).

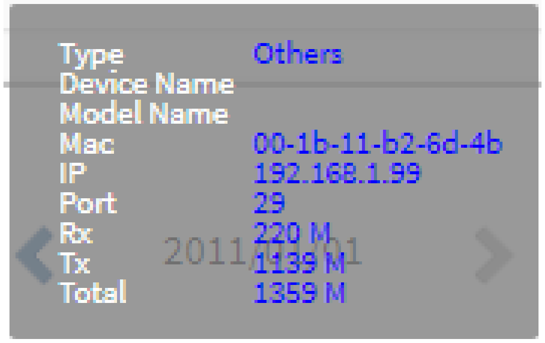
Cable status..... ● : The cable status diagnostic was unsuccessful (red dot).

6.12 DMS > Maintenance > Traffic Monitor

This page displays a visual chart of network traffic of all the devices. Numbers are shown in Mbit/s. You can view the traffic through all the ports or a specific port. Click on a specific port on the traffic chart to reveal its traffic during the day. You can select to display a summary of a day's or a week's traffic by selecting the check circle on top. The same applies to the selection of Rx Tx traffic. A single port's traffic is shown at the lower half of the screen. Note: Traffic Monitor feature is only available on the DMS Controller (Master) switch.



Hover the cursor over a chart bar to display its details:



Type	Others
Device Name	
Model Name	
Mac	00-1b-11-b2-6d-4b
IP	192.168.1.99
Port	29
Rx	220 M
Tx	1139 M
Total	1359 M

6.13 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 the 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 and make sure Mode = Enabled, Controller Priority = High, and 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 TN Technical Support. See Contact Us below.

Problem: DMS will discover the device type, name and model of some cameras and hosts but others are displayed as *Unknown*.

Description: When a device is detected by DMS, the device’s information (such as type, model name…etc.) can be recognized via LLDP (e.g. Switch), UPnP (e.g. AP), ONVIF (e.g. IP cam), NBNS (e.g. PC) packets if the device supports these protocols. So if the device display as *Unknown*, that means this device do not issue above mentioned protocol for DMS to recognize.

Resolution: You can manually assign and configure the device type and name for the unknown devices. See the Topology View > Dashboard or the Topology View section.

Message: *This page can’t load Google Maps correctly.*

Recovery:

1. Click the **OK** button to clear the message.
2. Navigate to DMS > Management > Map API Key.
3. See “6.9.1 How to Get the Google Map API Key on page 381.
4. Click the linked text “*Do you own this website?*” to display the Google API Key and Billing Errors Troubleshooting page.
5. For help on finding error messages, see the section on checking errors in your browser.
6. See the Google Maps Platform FAQ for more information.

For More DMS Information

See the online DMS Video. See the online DMS Overview.

7. Service, Warranty, Support, Contact, & Compliance Information

See the SM24DP4XA Install Guide for related information.

Appendix A – DHCP Per Port

You can configure DHCP Per Port via the Web UI as described below. The DHCP Per Port factory default mode is Disabled. See the *SM24TBT2DPA CLI Reference* for CLI mode operation.

The switch's DHCP server assigns IP addresses. Clients get IP addresses in sequence and the switch assigns IP addresses on a per-port basis starting from the configured IP range. For example, if the IP address range is configured as 192.168.10.20 - 192.168.10.37 with one DHCP device connected to port 1, the client will always get IP address 192.168.10.20, then port 3 is always distributed IP address 192.168.10.22, even if port 2 is an empty port (because port 2 is always distributed IP address 192.168.10.21).

The switch does not allow a DHCP per Port pool to include the switch's address.

IP address assigned range and VLAN 1 should stay in the same subnet mask.

The configurable IP address range is allowed to configure over 18 IP addresses, but the switch always assigns one IP address per port connecting device.

The DHCP Per Port function is only supported on VLAN 1.

When the DHCP Per Port function is enabled, the switch software will automatically create the related DHCP pool named "DHCP_Per_Port".

Once the DHCP Per Port function is enabled on one switch, IPv4 DHCP client at VLAN1 mode (DMS DHCP mode), DHCP server mode are all limited to be enabled at the same time (an error message displays if attempted).

If the DHCP server pool has been configured, once you enable the DHCP Per Port function, then that DHCP server pool configuration will be overwritten.

Only for VLAN 1, clients issued DHCP packets will not be broadcast/forwarded to other ports. DHCP packets in others VLANs will be broadcast/forwarded to other ports.

The DHCP Per Port function allows the switch to connect only one DHCP client device.

DHCP-Per-Port is configured entirely on the **Switch** > **Configuration** > **System** > **IP** page, IP Interfaces window.

The feature is enabled here and an IP range (pool) is entered. The "automatic" results of this action can be displayed in:

- **Switch** > **Configuration** > **System** > **DHCP** > **Server** > **Mode** (Global Mode – Enabled, VLAN Mode - VLAN 1 created)
- **Switch** > **Configuration** > **System** > **DHCP** > **Excluded** (Excluded range created based on range entered)
- **Switch** > **Configuration** > **System** > **DHCP** > **Pool** (Pool "DHCP_Per_Port" created based on range entered)

Actual DHCP operation is monitored as normal under **System** > **Monitor** > **DHCP**.

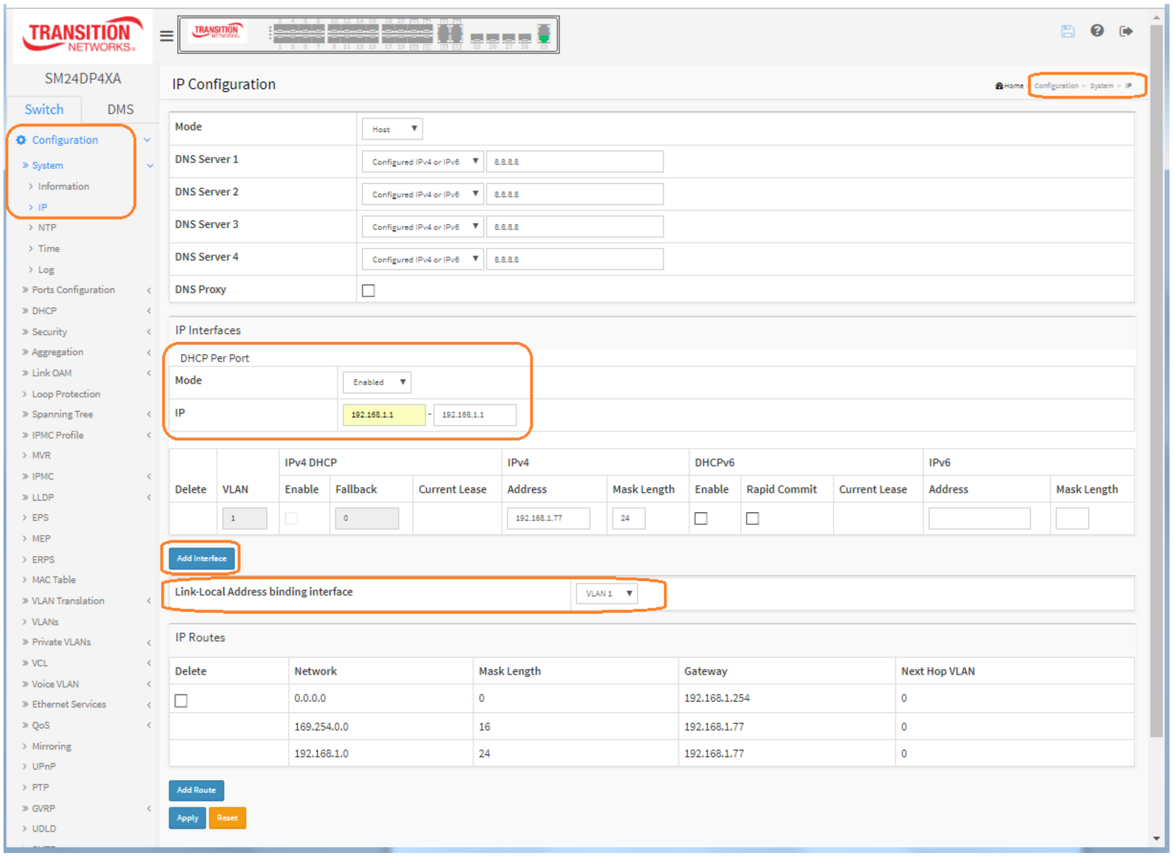
The DHCP Per Port pages and parameters are described below.

DHCP per Port Mode Configuration

The DHCP per Port function lets you assign an IP address based on the switch port the device is connected to. This will speed up installation of IP cameras, as the cameras can be configured after they are on the network. The DHCP Per Port assignment lets you know which IP was assigned to which camera.

Note: to prevent IP conflict, each switch can be allocated a different IP range.

To configure DHCP Per Port via the Web UI, navigate to the **Configuration** > **System** > **IP** menu path.



IP Configuration

Mode	Host ▼	
DNS Server 1	Configured IPv4 or IPv6 ▼	8.8.8.8
DNS Server 2	Configured IPv4 or IPv6 ▼	8.8.8.8
DNS Server 3	Configured IPv4 or IPv6 ▼	8.8.8.8
DNS Server 4	Configured IPv4 or IPv6 ▼	8.8.8.8
DNS Proxy	□	

IP Interfaces

DHCP Per Port

Mode	Enabled ▼
IP	192.168.1.1 - 192.168.1.1

		IPv4 DHCP			IPv4		DHCPv6			IPv6	
Delete	VLAN	Enable	Fallback	Current Lease	Address	Mask Length	Enable	Rapid Commit	Current Lease	Address	Mask Length
	1	□	0		192.168.1.77	24	□	□			

Add Interface

Link-Local Address binding interface	VLAN 1 ▼

IP Routes

Delete	Network	Mask Length	Gateway	Next Hop VLAN
□	0.0.0.0	0	192.168.1.254	0
	169.254.0.0	16	192.168.1.77	0
	192.168.1.0	24	192.168.1.77	0

Add Route

Apply Reset

Parameter descriptions: The **DHCP Per Port** parameters and buttons are described below.

Mode: at the dropdown select **Enable** or **Disable** the DHCP Per Port function globally. The default is **Disabled**.

IP: enter the IPv4 IP address range to be used when the DHCP Per Port function is enabled (e.g., 192.168.10.20 - 192.168.10.37). The DHCP Per Port IP range must be within the interface subnet. Note that DHCP Per Port with IPv6 is not supported at this time. The DHCP Per Port IP range must equal the switch port number excluding uplink ports (16).

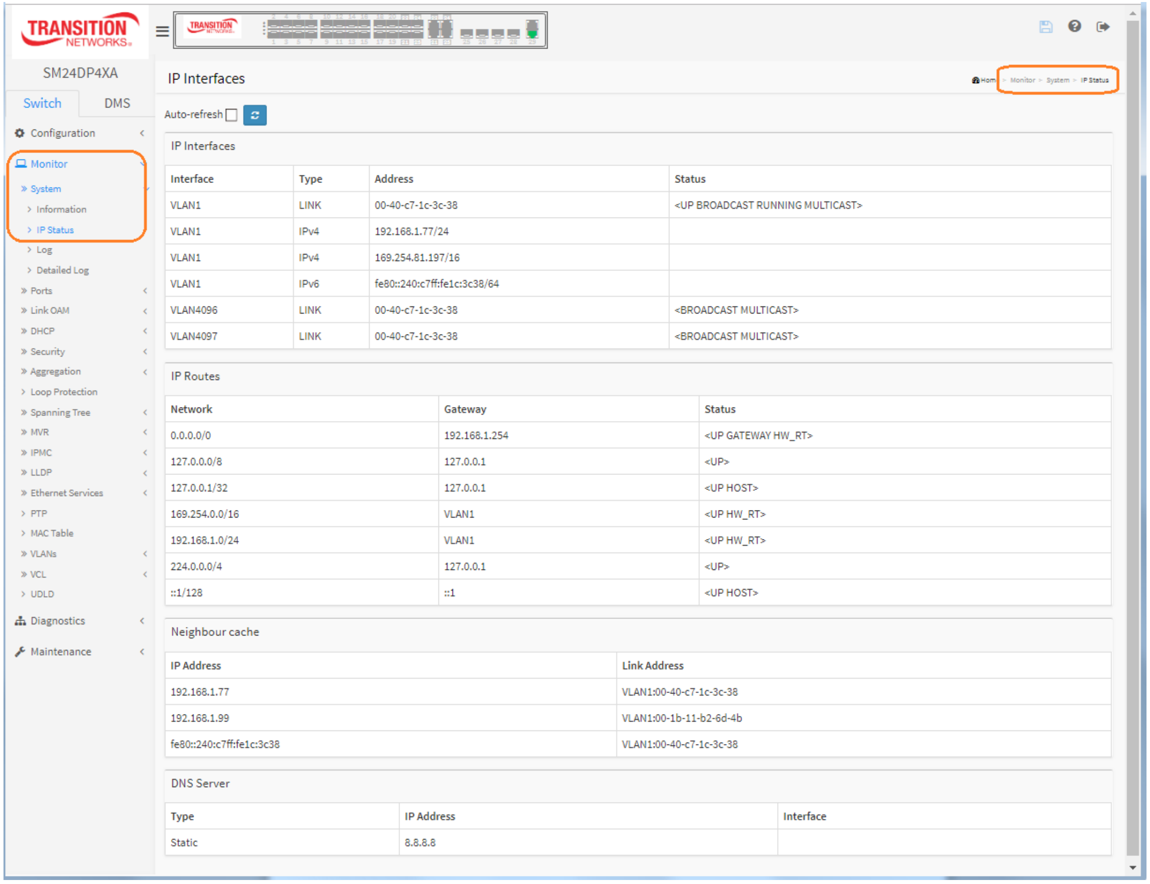
Apply: Click to save changes to the entries. If the entries are valid, the webpage message "*Update success!*" displays. Click the **OK** button to clear the message. If any entries are invalid, an error message displays. Click the **OK** button to clear the message and enter valid values, then click the **Apply** button again.

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

DHCP Server Mode Configuration

When DHCP Per Port is enabled and configured at **Configuration** > **System** > **IP**, the checkbox and selection in the DHCP Server Mode Configuration section at **Configuration** > **DHCP** > **Server** > **Mode** will become gray (cannot be selected):

To monitor DHCP Per Port status, navigate to the **Monitor** > **System** > **IP Status** menu path.



IP Interfaces

IP Interfaces

Interface	Type	Address	Status
VLAN1	LINK	00-40-c7-1c-3c-38	<UP BROADCAST RUNNING MULTICAST>
VLAN1	IPv4	192.168.1.77/24	
VLAN1	IPv4	169.254.81.197/16	
VLAN1	IPv6	fe80::240:c7ff:fe1c:3c38/64	
VLAN4096	LINK	00-40-c7-1c-3c-38	<BROADCAST MULTICAST>
VLAN4097	LINK	00-40-c7-1c-3c-38	<BROADCAST MULTICAST>

IP Routes

Network	Gateway	Status
0.0.0.0/0	192.168.1.254	<UP GATEWAY HW_RT>
127.0.0.0/8	127.0.0.1	<UP>
127.0.0.1/32	127.0.0.1	<UP HOST>
169.254.0.0/16	VLAN1	<UP HW_RT>
192.168.1.0/24	VLAN1	<UP HW_RT>
224.0.0.0/4	127.0.0.1	<UP>
::1/128	::1	<UP HOST>

Neighbour cache

IP Address	Link Address
192.168.1.77	VLAN1:00-40-c7-1c-3c-38
192.168.1.99	VLAN1:00-1b-11-b2-6d-4b
fe80::240:c7ff:fe1c:3c38	VLAN1:00-40-c7-1c-3c-38

DNS Server

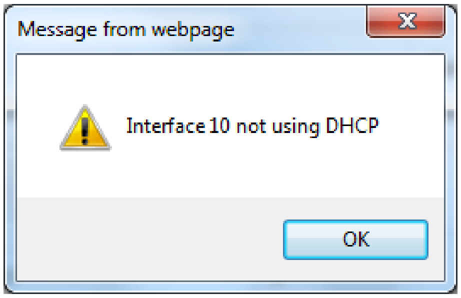
Type	IP Address	Interface
Static	8.8.8.8	

DHCP per Port Mode Web UI Messages

Message: *Interface xx not using DHCP*

Meaning: The Interface being configured does not have DHCP enabled and configured.

Recovery: **1**. Click the **OK** button to clear the webpage message. **2**. Enable and configure DHCP for the interface being configured. See "DHCP Server Mode Configuration" on page 303.

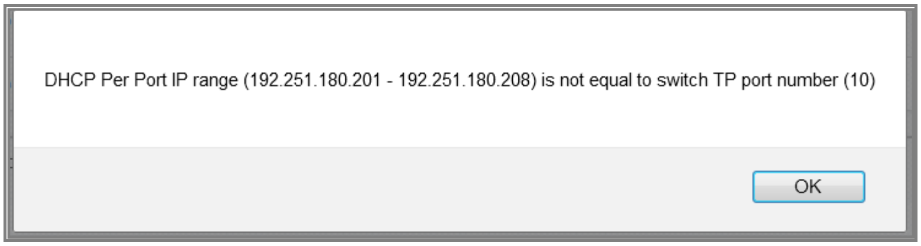


Interface 10 not using DHCP

Message: *'DHCP Per Port IP range (192-168-1.80 - 192-168-1.99*) is not equal to switch port number excluding uplink ports (10)

Meaning: The IPv4 IP address range entered for the DHCP Per Port function was invalid.

Recovery: **1**. Click the **OK** button to clear the webpage message. **2**. Re-configure DHCP Per Port. See the DHCP Per Port Mode Configuration section above.

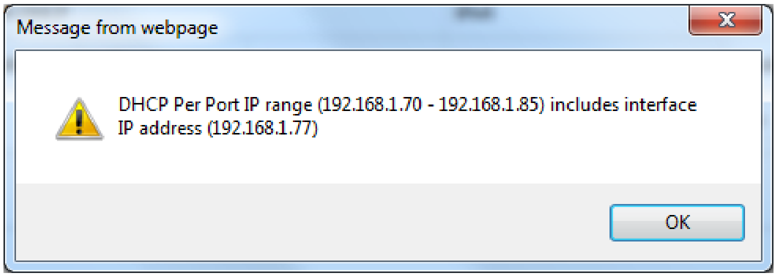


DHCP Per Port IP range (192.251.180.201 - 192.251.180.208) is not equal to switch TP port number (10)

Message: *'DHCP Per Port IP range (192-168-1.70 - 192-168-1.85*) *includes interface IP Address (192.168.1.77)*

Meaning: The IPv4 IP address range entered for the DHCP Per Port function was invalid.

Recovery: **1**. Click the **OK** button to clear the webpage message. **2**. Re-configure DHCP Per Port. See the DHCP Per Port Mode Configuration section above. On the screen below, the range should be something like 192-168-1.80 - 192-168-1.85 to be valid.

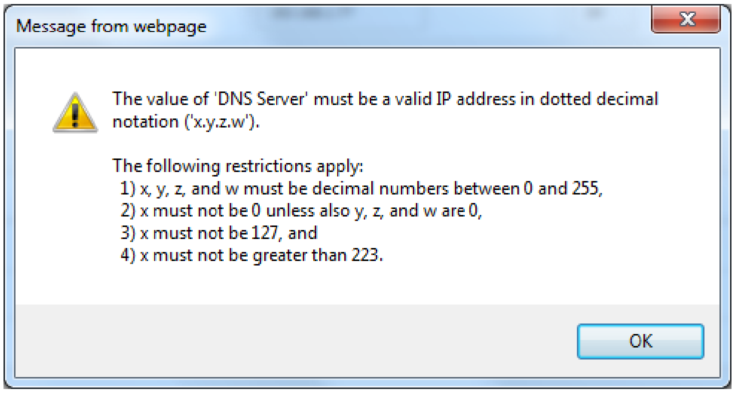


DHCP Per Port IP range (192.168.1.70 - 192.168.1.85) includes interface IP address (192.168.1.77)

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

Meaning: You entered an invalid IP address for the DNS Server being configured.

Recovery: **1**. Click the **OK** button to clear the webpage message. **2**. Enter a valid IP address in the format x.y.z.w per the on-screen restrictions. See "DHCP Server Mode Configuration" on page 303.



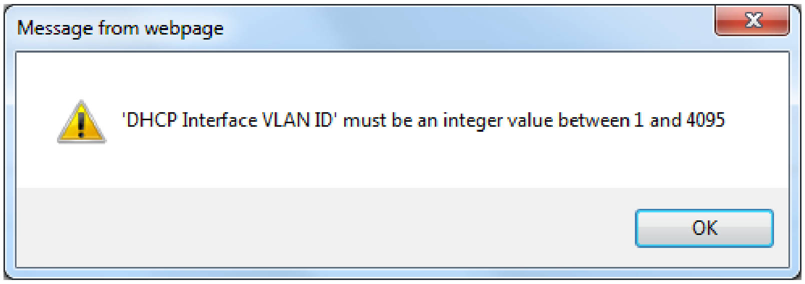
The value of 'DNS Server' must be a valid IP address in dotted decimal notation ('x.y.z.w').

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

Message: *'DHCP Interface VLAN ID' must be an integer value between 1 and 4095.*

Meaning: You entered an invalid VLAN ID for the DHCP Interface.

Recovery: **1**. Click the **OK** button to clear the webpage message. **2**. Enter a valid VLAN ID for the DHCP Interface (1-4095). See "DHCP Server Mode Configuration" on page 301.

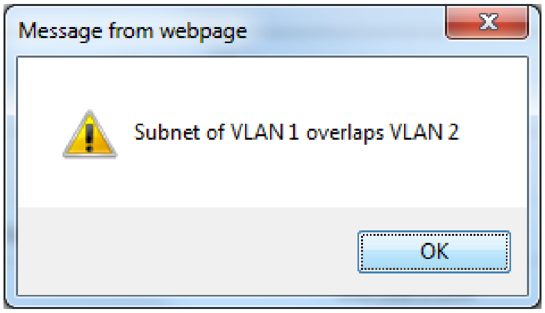


'DHCP Interface VLAN ID' must be an integer value between 1 and 4095

Message: *Subnet of VLAN 1 overlaps VLAN 2*

Meaning: The IPv4 IP address range entered for the DHCP Per Port function was invalid.

Recovery: **1**. Click the **OK** button to clear the webpage message. **2**. Re-configure DHCP Per Port. See the DHCP Per Port Mode Configuration section above.



Subnet of VLAN 1 overlaps VLAN 2

Appendix B – G.8032 Major and Sub Rings Configuration

Introduction

Ethernet Ring Protection Switching (ERPS) is a protocol defined by the International Telecommunication Union - Telecommunication Standardization Sector (ITU-T) to prevent loops at Layer 2. With the standard number is ITU-T G.8032, and ERPS is also called G.8032. Generally, redundant links are used on a network to provide link backup and enhance network reliability. The use of redundant links, however, may produce loops, causing broadcast storms and rendering the MAC address table unstable. These can affect the network, where the communication quality is not good enough, and communication services might be interrupted.

ERPS provides advantages of traditional ring network technologies such as STP/RSTP/MSTP and optimizes detection mechanism to provide faster convergence. For example, the ERPS-enabled switch provides 50-ms convergence for broadcast packets.

See section 2-15 ERPS on page 165 for more information.

Basic Concepts

There are some basic concepts that support ERPS Ring:

- **Ring Protection Link (RPL)** – Link designated by mechanism that is blocked during Idle state to prevent loop on Bridged ring.
- **RPL Owner node** – Node connected to RPL that blocks traffic on RPL during Idle state and unblocks during Protection state.
- **RPL Neighbor node** – Node connected to RPL that blocks traffic on RPL during Idle state and unblocks during Protection state (v2).
- **Link Monitoring** – Links of ring are monitored using standard ETH CC OAM messages (CFM) • Signal Fail (SF) – Signal Fail is declared when signal fail condition is detected.
- **No Request (NR)** – No Request is declared when there are no outstanding conditions (e.g., SF, etc.) on the node.
- **Ring APS (R-APS) Messages** – Protocol messages defined in Y.1731 and G.8032.
- **Automatic Protection Switching (APS) Channel** - Ring-wide VLAN used exclusively for transmission of OAM messages including R-APS messages.

IP Addresses

The sample configurations below use these IP addresses:

SISPM1040-582-LRT : 192.168.1.85

SISPM1040-384-LRT-C : 192.168.1.95

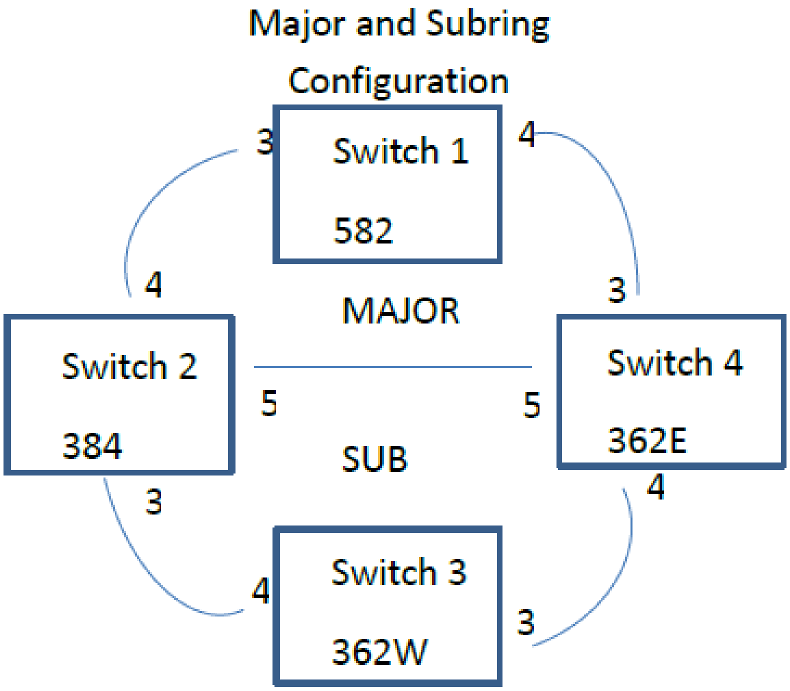
362W : 192.168.1.125

362E : 192.168.1.135

Sample Configuration

Major Ring and Sub Ring : 4 Switches

Major : SW#1, SW#2, SW#4; **Sub** : SW#2, SW#3, SW#4



VLANs	APS Data
10,20	5

RPL Mode	Major	Sub	Major	Sub	Major	Sub
	Owner Switch #1	Owner Switch #3	Neighbor Switch #2	Neighbor Switch #2	None Switch #4	None Switch #4

Switch 1 Configuration (SISPM1040-582-LRT)

VLANs	Port 3	Trunk	Tag All	5,10
	Port 4	Trunk	Tag All	5,10
STP	Port 3	Disable		
	Port 4	Disable		

MEPs	Instance	Port	VLAN	MAC	MEP ID	Peer MAC	Peer MEP ID
	1	3	10	00-C0-F2-49-39-5F	1	00-40-C7-1C-C7-30	4
	2	4	10	00-C0-F2-49-39-60	5	00-C0-F2-53-EF-FC	5

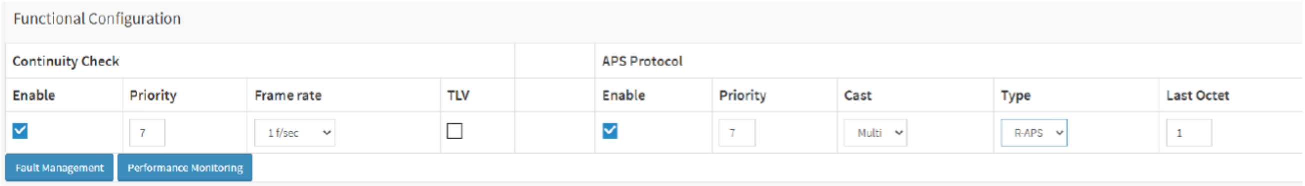
Note: All MEPs are programed the same under the Functional Configuration

Continuity Check

Check Enable – Priority: 7 – Frame rate: 1f/sec

APS Protocol

Check Enable – Priority: 7 – Cast: Multi – Type: R-APS



Functional Configuration

Continuity Check				APS Protocol				
Enable	Priority	Frame rate	TLV	Enable	Priority	Cast	Type	Last Octet
☑	7	1 f/sec	□	☑	7	Multi	R-APS	1

ERPS

ERPS ID	Port 0	Port 1	Port 0 SF	Port 1 SF	Port 0 APS	Port 1 APS	Ring	RPL	Port	VLAN
1	1	2	1	2	1	2	Major	Owner	0	5

Switch 2 Configuration (SISPM1040-384-LRT-C)

VLANs	Port 3	Trunk	Tag All	5,20
	Port 4	Trunk	Tag All	5,10
	Port 5	Trunk	Tag All	5,10,20
STP	Port 3	Disable		
	Port 4	Disable		
	Port 5	Disable		

MEPs	Instance	Port	VLAN	MAC	MEP ID	Peer MAC	Peer MEP ID
	1	3	20	00-40-C7-1C-C7-2F	3	00-C0-F2-53-F0-BA	8
	2	4	10	00-C0-F2-49-39-60	4	00-C0-F2-49-39-5F	1
	3	5	10	00-40-C7-1C-C7-31	9	00-C0-F2-53-EF-FE	10

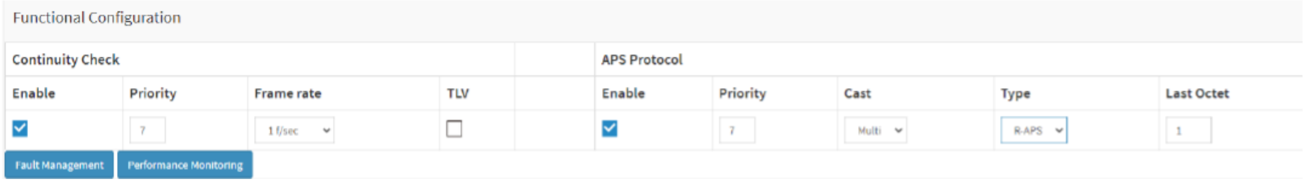
Note: All MEPs are programed the same under the Functional Configuration

Continuity Check

Check Enable – Priority: 7 – Frame rate: 1f/sec

APS Protocol

Check Enable – Priority: 7 – Cast: Multi – Type: R-APS



Functional Configuration

Continuity Check				APS Protocol				
Enable	Priority	Frame rate	TLV	Enable	Priority	Cast	Type	Last Octet
☑	7	1 f/sec	☐	☑	7	Multi	R-APS	1

ERPS

ERPS ID	Port 0	Port 1	Port 0 SF	Port 1 SF	Port 0 APS	Port 1 APS	Ring	RPL	Port	VLAN
1	3	2	3	2	3	2	Major	Neighbor	1	5
2	1	0	1	0	1	0	Sub	Neighbor	0	5

Interconnect Yes, Major 1

Switch 3 Configuration (SISPM1040-362-LRT[W])

VLANs	Port 3	Trunk Tag All 5,20
	Port 4	Trunk Tag All 5,20
STP	Port 3	Disable
	Port 4	Disable

MEPs	Instance	Port	VLAN	MAC	MEP ID	Peer MAC	Peer MEP ID
	1	3	20	00-C0-F2-53-F0-B9	7	00-C0-F2-53-EF-FD	6
	2	4	20	00-C0-F2-53-F0-BA	8	00-40-C7-1C-C7-2F	3

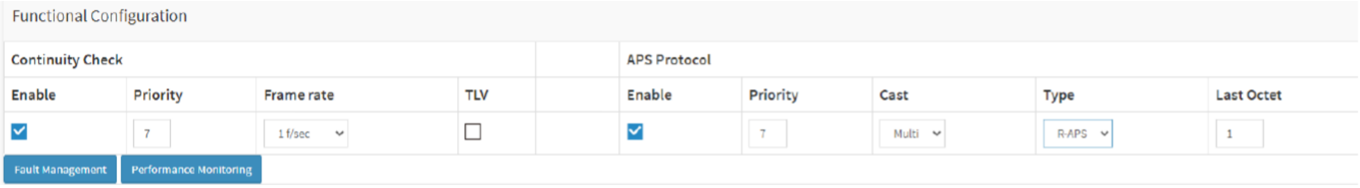
Note: All MEPs are programed the same under the Functional Configuration

Continuity Check

Check Enable – Priority: 7 – Frame rate: 1f/sec

APS Protocol

Check Enable – Priority: 7 – Cast: Multi – Type: R-APS



Functional Configuration

Continuity Check					APS Protocol				
Enable	Priority	Frame rate	TLV		Enable	Priority	Cast	Type	Last Octet
☑	7	1 f/sec	□		☑	7	Multi	R-APS	1

ERPS

ERPS ID	Port 0	Port 1	Port 0 SF	Port 1 SF	Port 0 APS	Port 1 APS	Ring	RPL	Port	VLAN
1	1	2	1	2	1	2	Sub	Owner	1	5

Switch 4 Configuration (SISPM1040-362-LRT[E])

VLANs	Port 3	Trunk	Tag All	5,10
	Port 4	Trunk	Tag All	5,20
	Port 5	Trunk	Tag All	5,10,20
STP	Port 3	Disable		
	Port 4	Disable		
	Port 5	Disable		

MEPs	Instance	Port	VLAN	MAC	MEP ID	Peer MAC	Peer MEP ID
	1	3	10	00-C0-F2-53-EF-FC	5	00-C0-F2-49-39-60	2
	2	4	20	00-C0-F2-53-EF-FD	6	00-C0-F2-53-F0-B9	7
	3	5	10	00-C0-F2-53-EF-FE	10	00-40-C7-1C-C7-31	9

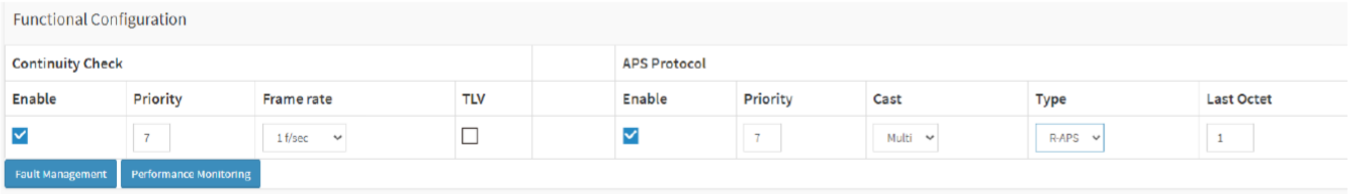
Note: All MEPs are programed the same under the Functional Configuration

Continuity Check

Check Enable – Priority: 7 – Frame rate: 1f/sec

APS Protocol

Check Enable – Priority: 7 – Cast: Multi – Type: R-APS



Functional Configuration

Continuity Check					APS Protocol				
Enable	Priority	Frame rate	TLV		Enable	Priority	Cast	Type	Last Octet
☑	7	1 f/sec	☐		☑	7	Multi	R-APS	1

ERPS

ERPS ID	Port 0	Port 1	Port 0 SF	Port 1 SF	Port 0 APS	Port 1 APS	Ring	RPL	Port VLAN
1	1	3	1	3	1	3	Major	None	5
2	2	0	2	0	2	0	Sub	None	5

Interconnect Yes, Major 1

Testing

Testing Pings from Switch 4 to Switch 1 – Major Ring

Failing Major ring, No lost pings

```
C:\Users\dennist>ping 192.168.1.85 -t
Pinging 192.168.1.85 with 32 bytes of data:
Reply from 192.168.1.85: bytes=32 time<1ms TTL=64
Reply from 192.168.1.85: bytes=32 time<1ms TTL=64
Reply from 192.168.1.85: bytes=32 time<1ms TTL=64
Reply from 192.168.1.85: bytes=32 time<1ms TTL=64
Reply from 192.168.1.85: bytes=32 time<1ms TTL=64
Reply from 192.168.1.85: bytes=32 time<1ms TTL=64
Reply from 192.168.1.85: bytes=32 time<1ms TTL=64
Reply from 192.168.1.85: bytes=32 time<1ms TTL=64
Reply from 192.168.1.85: bytes=32 time<1ms TTL=64
Reply from 192.168.1.85: bytes=32 time<1ms TTL=64
Reply from 192.168.1.85: bytes=32 time<1ms TTL=64
Reply from 192.168.1.85: bytes=32 time<1ms TTL=64
Reply from 192.168.1.85: bytes=32 time<1ms TTL=64
Reply from 192.168.1.85: bytes=32 time<1ms TTL=64
Reply from 192.168.1.85: bytes=32 time<1ms TTL=64
Reply from 192.168.1.85: bytes=32 time<1ms TTL=64
Reply from 192.168.1.85: bytes=32 time<1ms TTL=64
Reply from 192.168.1.85: bytes=32 time<1ms TTL=64
Reply from 192.168.1.85: bytes=32 time=1ms TTL=64
Reply from 192.168.1.85: bytes=32 time<1ms TTL=64
Reply from 192.168.1.85: bytes=32 time<1ms TTL=64
Reply from 192.168.1.85: bytes=32 time<1ms TTL=64
Reply from 192.168.1.85: bytes=32 time<1ms TTL=64
Reply from 192.168.1.85: bytes=32 time<1ms TTL=64
Reply from 192.168.1.85: bytes=32 time<1ms TTL=64
Reply from 192.168.1.85: bytes=32 time<1ms TTL=64
Reply from 192.168.1.85: bytes=32 time<1ms TTL=64
Reply from 192.168.1.85: bytes=32 time<1ms TTL=64
Reply from 192.168.1.85: bytes=32 time<1ms TTL=64
Reply from 192.168.1.85: bytes=32 time=5ms TTL=64    ←---------------------
Reply from 192.168.1.85: bytes=32 time<1ms TTL=64    Cable Disconnect
Reply from 192.168.1.85: bytes=32 time=3ms TTL=64    ←---------------------
Reply from 192.168.1.85: bytes=32 time<1ms TTL=64
Reply from 192.168.1.85: bytes=32 time=1ms TTL=64
Reply from 192.168.1.85: bytes=32 time<1ms TTL=64
Reply from 192.168.1.85: bytes=32 time<1ms TTL=64
Reply from 192.168.1.85: bytes=32 time=1ms TTL=64
Reply from 192.168.1.85: bytes=32 time<1ms TTL=64
Reply from 192.168.1.85: bytes=32 time<1ms TTL=64
Ping statistics for 192.168.1.85:
Packets: Sent = 45, Received = 45, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 0ms, Maximum = 5ms, Average = 0ms
```

Testing Pings from Switch 4 to Switch 3 – Sub Ring

Fail Subring, No lost pings

```
C:\Users\dennist>ping 192.168.1.125 -t

Pinging 192.168.1.125 with 32 bytes of data:
Reply from 192.168.1.125: bytes=32 time=1ms TTL=64
Reply from 192.168.1.125: bytes=32 time<1ms TTL=64
Reply from 192.168.1.125: bytes=32 time<1ms TTL=64
Reply from 192.168.1.125: bytes=32 time<1ms TTL=64
Reply from 192.168.1.125: bytes=32 time<1ms TTL=64
Reply from 192.168.1.125: bytes=32 time<1ms TTL=64
Reply from 192.168.1.125: bytes=32 time<1ms TTL=64
Reply from 192.168.1.125: bytes=32 time<1ms TTL=64
Reply from 192.168.1.125: bytes=32 time<1ms TTL=64
Reply from 192.168.1.125: bytes=32 time<1ms TTL=64
Reply from 192.168.1.125: bytes=32 time<1ms TTL=64
Reply from 192.168.1.125: bytes=32 time<1ms TTL=64
Reply from 192.168.1.125: bytes=32 time<1ms TTL=64
Reply from 192.168.1.125: bytes=32 time=1ms TTL=64
Reply from 192.168.1.125: bytes=32 time<1ms TTL=64
Reply from 192.168.1.125: bytes=32 time<1ms TTL=64
Reply from 192.168.1.125: bytes=32 time<1ms TTL=64
Reply from 192.168.1.125: bytes=32 time<1ms TTL=64
Reply from 192.168.1.125: bytes=32 time<1ms TTL=64
Reply from 192.168.1.125: bytes=32 time<1ms TTL=64
Reply from 192.168.1.125: bytes=32 time<1ms TTL=64
Reply from 192.168.1.125: bytes=32 time=7ms TTL=64    ←--------------------
Reply from 192.168.1.125: bytes=32 time<1ms TTL=64     Cable Disconnect
Reply from 192.168.1.125: bytes=32 time<1ms TTL=64
Reply from 192.168.1.125: bytes=32 time<1ms TTL=64
Reply from 192.168.1.125: bytes=32 time<1ms TTL=64
Reply from 192.168.1.125: bytes=32 time<1ms TTL=64
Reply from 192.168.1.125: bytes=32 time<1ms TTL=64
Reply from 192.168.1.125: bytes=32 time<1ms TTL=64
Reply from 192.168.1.125: bytes=32 time=1ms TTL=64
Reply from 192.168.1.125: bytes=32 time<1ms TTL=64
Reply from 192.168.1.125: bytes=32 time=1ms TTL=64
Reply from 192.168.1.125: bytes=32 time<1ms TTL=64
Reply from 192.168.1.125: bytes=32 time<1ms TTL=64
Reply from 192.168.1.125: bytes=32 time<1ms TTL=64
Reply from 192.168.1.125: bytes=32 time<1ms TTL=64
Reply from 192.168.1.125: bytes=32 time<1ms TTL=64
Reply from 192.168.1.125: bytes=32 time<1ms TTL=64
Reply from 192.168.1.125: bytes=32 time<1ms TTL=64
Ping statistics for 192.168.1.125:
Packets: Sent = 41, Received = 41, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 0ms, Maximum = 7ms, Average = 0ms
```

Config files

running-config_192.168.1

```
hostname SISPM1040-362-LRT-E
username admin privilege 15 password encrypted
feec1d1085ff075fd03b1d2d5ab4c0befbff0917079c8abb3a77338041bf5d6e1771bdbbd1a317ea2f42fc
2aacc8c50a8e667456d7c04099f74f8ef9dcc0fbd4
!
vlan 1
!
!
!
!
ip route 0.0.0.0 0.0.0.0 192.168.1.254
tzidx 0
exec-timeout autologout 0
snmp-server location DT Lab Ring
system name SISPM1040-362-LRT-E
system location DT Lab Ring
system description Managed Hardened PoE+ Switch, (4) 10/100/1000Base-T PoE+ Ports +
(2) 10/100/1000Base-T Ports + (2) 100/1000Base-X SFP Ports
!
interface GigabitEthernet 1/1
!
interface GigabitEthernet 1/2
!
interface GigabitEthernet 1/3
 no spanning-tree
 switchport trunk allowed vlan 5,10
 switchport trunk vlan tag native
 switchport mode trunk
 poe mode disable
!
interface GigabitEthernet 1/4
 no spanning-tree
 switchport trunk allowed vlan 5,20
 switchport trunk vlan tag native
 switchport mode trunk
 poe mode disable
!
interface GigabitEthernet 1/5
 no spanning-tree
 switchport trunk allowed vlan 5,10,20
 switchport trunk vlan tag native
 switchport mode trunk
!
interface GigabitEthernet 1/6
!
interface GigabitEthernet 1/7
!
interface GigabitEthernet 1/8
!
interface vlan 1
 ip address 192.168.1.135 255.255.255.0
 ip dhcp server
!
mep 1 down domain port level 4 interface GigabitEthernet 1/3
mep 1 mep-id 5
mep 1 vid 10
mep 1 peer-mep-id 2 mac 00-C0-F2-49-39-60
mep 1 cc 7
mep 1 aps 7 raps
mep 2 down domain port level 4 interface GigabitEthernet 1/4
mep 2 mep-id 6
mep 2 vid 20
mep 2 peer-mep-id 7 mac 00-C0-F2-53-F0-B9
mep 2 cc 7
mep 2 aps 7 raps
mep 3 down domain port level 4 interface GigabitEthernet 1/5
mep 3 mep-id 10
mep 3 vid 10
mep 3 peer-mep-id 9 mac 00-40-C7-1C-C7-31
mep 3 cc 7
mep 3 aps 7 raps
erps 1 major port0 interface GigabitEthernet 1/3 port1 interface GigabitEthernet 1/5
erps 1 mep port0 sf 1 aps 1 port1 sf 3 aps 3
erps 1 vlan 5
erps 2 sub port0 interface GigabitEthernet 1/4 interconnect 1
erps 2 mep port0 sf 2 aps 2
erps 2 vlan 5
!
spanning-tree aggregation
 spanning-tree link-type point-to-point
!
!
line console 0
!
line vty 0
!
line vty 1
!
line vty 2
!
line vty 3
!
line vty 4
!
line vty 5
!
line vty 6
!
line vty 7
!
line vty 8
!
line vty 9
!
line vty 10
!
line vty 11
!
line vty 12
!
line vty 13
!
line vty 14
!
line vty 15
!
!
end
```

running-config_192.168.1

hostname SISPM1040-582-LRT

```
logging on
logging host 192.168.1.253
username admin privilege 15 password encrypted
7073dec86c15b8a9907bb4106ef783adde46bd5b5969cc68fb55b430336bd7c80d5ded65d2fdb39abe81cc
9caa5a93620f270c21bca86e776cee9c5588bfb8c7
username superuser privilege 15 password encrypted
4643fdc71f39fd4cb955943fcaf89faca81bc650fbaeebe25a796662d5c225bf0d5ded65d2fdb39abe81cc
9c514497e27799560e488713aabaac4f167e7732ca
!
vlan 1
!
!
!
!
ip route 0.0.0.0 0.0.0.0 192.168.1.254
ntp automatic
ntp server 1 ip-address ntp1.transition.com
ntp server 2 ip-address ntp2.transition.com
clock timezone '' 9
tzidx 0
exec-timeout autologout 0
poe ping-check enable
snmp-server contact DTroxel
snmp-server location DT Office
system contact DTroxel
system name SISPM1040-582-LRT
system location DT Office
system description Managed Hardened PoE++ Switch (8) 10/100/1000Base-T PoE++ Ports +
(2) 100/1000Base-X SFP Slot
!
interface GigabitEthernet 1/1
 no spanning-tree
 poe ping-ip-addr 192.168.1.70
 poe failure-action reboot-Remote-PD
!
interface GigabitEthernet 1/2
 no spanning-tree
 switchport forbidden vlan add 3,5
!
interface GigabitEthernet 1/3
 no spanning-tree
 switchport trunk allowed vlan 5,10
 switchport trunk vlan tag native
 switchport mode trunk
 poe mode disable
!
interface GigabitEthernet 1/4
 no spanning-tree
 switchport trunk allowed vlan 5,10
 switchport trunk vlan tag native
 switchport mode trunk
 poe mode disable
 poe ping-ip-addr 192.168.1.200
!
interface GigabitEthernet 1/5
 no spanning-tree
!
interface GigabitEthernet 1/6
 no spanning-tree
!
interface GigabitEthernet 1/7
!
interface GigabitEthernet 1/8
```

```
 poe mode disable
!
interface GigabitEthernet 1/9
 no spanning-tree
!
interface GigabitEthernet 1/10
 no spanning-tree
!
interface vlan 1
 ip address 192.168.1.85 255.255.255.0
 ip dhcp server
!
mep 1 down domain port level 4 interface GigabitEthernet 1/3
mep 1 vid 10
mep 1 peer-mep-id 4 mac 00-40-C7-1C-C7-30
mep 1 cc 7
mep 1 aps 7 raps
mep 2 down domain port level 4 interface GigabitEthernet 1/4
mep 2 mep-id 2
mep 2 vid 10
mep 2 peer-mep-id 5 mac 00-C0-F2-53-EF-FC
mep 2 cc 7
mep 2 aps 7 raps
erps 1 major port0 interface GigabitEthernet 1/3 port1 interface GigabitEthernet 1/4
erps 1 mep port0 sf 1 aps 1 port1 sf 2 aps 2
erps 1 rpl owner port0
erps 1 vlan 5
!
spanning-tree aggregation
 no spanning-tree
 spanning-tree link-type point-to-point
!
!
line console 0
!
line vty 0
!
line vty 1
!
line vty 2
!
line vty 3
!
line vty 4
!
line vty 5
!
line vty 6
!
line vty 7
!
line vty 8
!
line vty 9
!
line vty 10
!
line vty 11
!
line vty 12
!
line vty 13
!
line vty 14
!
line vty 15
```

```
!
map-api-key AIzaSyBItuM0hDtK6nJeZPEk7jnrcoGGi92EpFM
!
end
```

running-config_192.168.1

hostname SISPM1040-384-LRT-C

```
username admin privilege 15 password encrypted
6593186b999f348becd63b8612ac561c114250a1a00bd38f6afb5378acb6d08c1864c59b092b0e2b29ba4f
1d559166800846cbc52c4558a90e4cdf95d3cfcbf4
username dennis privilege 5 password encrypted
a92a5dbf4fcd2e13d35adb36d2418476e907de19a641fa7baf80b1abb2bacd8ee5dbdd44e246b88be1636d
f6b8769af790aa8721622481085e33c32e6e119dbd
!
vlan 1
!
!
!
!
ip route 0.0.0.0 0.0.0.0 192.168.1.254
tzidx 0
exec-timeout autologout 0
poe ping-check enable
access-list ace 2 ingress interface GigabitEthernet 1/2 action deny
access-list ace 1 next 2 ingress interface GigabitEthernet 1/2 frame-type ipv4-tcp
dport 443
system name SISPM1040-384-LRT-C
system description Managed Hardened PoE+ Switch, (8) 10/100/1000Base-T PoE+ Ports +
(4) 100/1000Base-X SFP
!
interface GigabitEthernet 1/1
 no spanning-tree
 lldp cdp-aware
 poe ping-ip-addr 192.168.1.100
 poe failure-action reboot-Remote-PD
!
interface GigabitEthernet 1/2
 no spanning-tree
 lldp cdp-aware
 speed 1000
 duplex full
!
interface GigabitEthernet 1/3
 no spanning-tree
 switchport trunk allowed vlan 5,20
 switchport trunk vlan tag native
 switchport mode trunk
 lldp cdp-aware
 poe mode disable
!
interface GigabitEthernet 1/4
 no spanning-tree
 switchport trunk allowed vlan 5,10
 switchport trunk vlan tag native
 switchport mode trunk
 lldp cdp-aware
 poe mode disable
!
interface GigabitEthernet 1/5
 no spanning-tree
 switchport trunk allowed vlan 5,10,20
 switchport trunk vlan tag native
 switchport mode trunk
 lldp cdp-aware
 poe mode disable
!
interface GigabitEthernet 1/6
 no spanning-tree
 lldp cdp-aware
!
```

```
interface GigabitEthernet 1/7
 lldp cdp-aware
!
interface GigabitEthernet 1/8
 lldp cdp-aware
!
interface GigabitEthernet 1/9
 no spanning-tree
 switchport trunk allowed vlan 1,50,100
 switchport trunk vlan tag native
 lldp cdp-aware
!
interface GigabitEthernet 1/10
 no spanning-tree
 lldp cdp-aware
!
interface GigabitEthernet 1/11
 no spanning-tree
 lldp cdp-aware
!
interface GigabitEthernet 1/12
 no spanning-tree
 lldp cdp-aware
!
interface vlan 1
 ip address 192.168.1.95 255.255.255.0
 ip dhcp server
!
mep 1 down domain port level 4 interface GigabitEthernet 1/3
mep 1 mep-id 3
mep 1 vid 20
mep 1 peer-mep-id 8 mac 00-C0-F2-53-F0-BA
mep 1 cc 7
mep 1 aps 7 raps
mep 2 down domain port level 4 interface GigabitEthernet 1/4
mep 2 mep-id 4
mep 2 vid 10
mep 2 peer-mep-id 1 mac 00-C0-F2-49-39-5F
mep 2 cc 7
mep 2 aps 7 raps
mep 3 down domain port level 4 interface GigabitEthernet 1/5
mep 3 mep-id 9
mep 3 vid 10
mep 3 peer-mep-id 10 mac 00-C0-F2-53-EF-FE
mep 3 cc 7
mep 3 aps 7 raps
erps 1 major port0 interface GigabitEthernet 1/5 port1 interface GigabitEthernet 1/4
erps 1 mep port0 sf 3 aps 3 port1 sf 2 aps 2
erps 1 rpl neighbor port1
erps 1 vlan 5
erps 2 sub port0 interface GigabitEthernet 1/3 interconnect 1
erps 2 mep port0 sf 1 aps 1
erps 2 rpl neighbor port0
erps 2 vlan 5
!
spanning-tree aggregation
 no spanning-tree
 spanning-tree link-type point-to-point
!
!
line console 0
!
line vty 0
!
line vty 1
!
```

```
line vty 2
!
line vty 3
!
line vty 4
!
line vty 5
!
line vty 6
!
line vty 7
!
line vty 8
!
line vty 9
!
line vty 10
!
line vty 11
!
line vty 12
!
line vty 13
!
line vty 14
!
line vty 15
!
map-api-key AIzaSyBItuM0hDtK6nJeZPEk7jnrcoGGi92EpFM
!
end
```

running-config_192.168.1

```
hostname SISPM1040-362-LRT-W
username admin privilege 15 password encrypted
6158ed7daf39d06ded0e7c4828c3b15bb4c40673bd445afcd643295925ae425d9611d1cbe872708237571a
acc7b9237f33b01ae6866e2484009edfe1fa0bf56f
!
vlan 1
!
!
!
!
ip route 0.0.0.0 0.0.0.0 192.168.1.254
tzidx 0
exec-timeout autologout 0
snmp-server location DT Lab Ring
system name SISPM1040-362-LRT-W
system location DT Lab Ring
system description Managed Hardened PoE+ Switch, (4) 10/100/1000Base-T PoE+ Ports +
(2) 10/100/1000Base-T Ports + (2) 100/1000Base-X SFP Ports
!
interface GigabitEthernet 1/1
!
interface GigabitEthernet 1/2
!
interface GigabitEthernet 1/3
 no spanning-tree
 switchport trunk allowed vlan 5,20
 switchport trunk vlan tag native
 switchport mode trunk
 poe mode disable
!
interface GigabitEthernet 1/4
 no spanning-tree
 switchport trunk allowed vlan 5,20
 switchport trunk vlan tag native
 switchport mode trunk
 poe mode disable
!
interface GigabitEthernet 1/5
!
interface GigabitEthernet 1/6
!
interface GigabitEthernet 1/7
!
interface GigabitEthernet 1/8
!
interface vlan 1
 ip address 192.168.1.125 255.255.255.0
 ip dhcp server
!
mep 1 down domain port level 4 interface GigabitEthernet 1/3
mep 1 mep-id 7
mep 1 vid 20
mep 1 peer-mep-id 6 mac 00-C0-F2-53-EF-FD
mep 1 cc 7
mep 1 aps 7 raps
mep 2 down domain port level 4 interface GigabitEthernet 1/4
mep 2 mep-id 8
mep 2 vid 20
mep 2 peer-mep-id 3 mac 00-40-C7-1C-C7-2F
mep 2 cc 7
mep 2 aps 7 raps
erps 1 sub port0 interface GigabitEthernet 1/3 port1 interface GigabitEthernet 1/4
erps 1 mep port0 sf 1 aps 1 port1 sf 2 aps 2
erps 1 rpl owner port1
erps 1 vlan 5
!
spanning-tree aggregation
 spanning-tree link-type point-to-point
!
!
line console 0
!
line vty 0
!
line vty 1
!
line vty 2
!
line vty 3
!
line vty 4
!
line vty 5
!
line vty 6
!
line vty 7
!
line vty 8
!
line vty 9
!
line vty 10
!
line vty 11
!
line vty 12
!
line vty 13
!
line vty 14
!
line vty 15
!
!
end
```

Transition Networks
10900 Red Circle Drive
Minnetonka, MN 55343 USA
tel: +1.952.941.7600 | toll free: 1.800.526.9267 | fax: 952.941.2322

SM24DP4XA Web User Guide, 33770 Rev. D