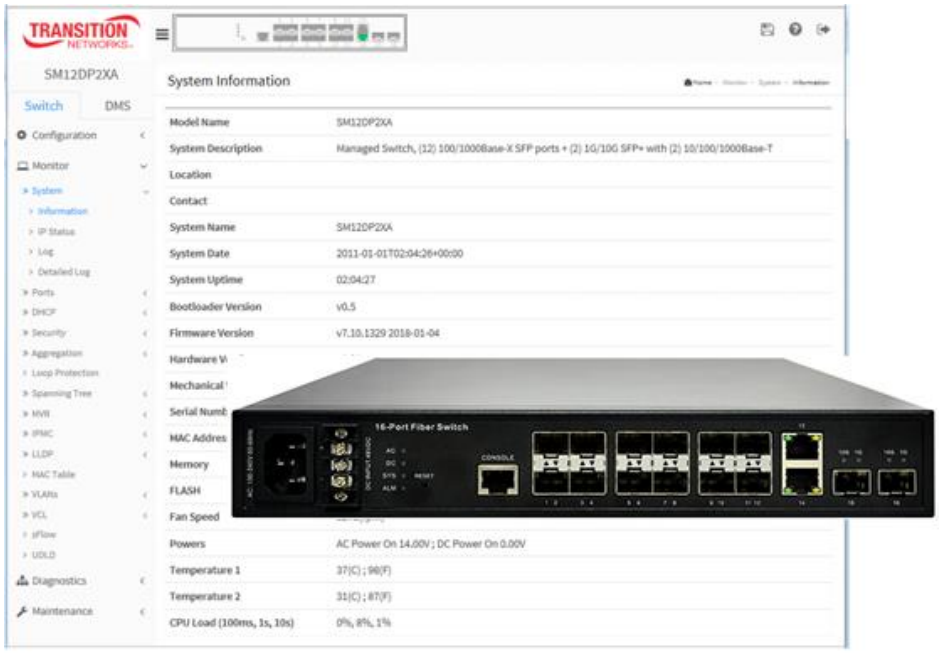
SM12DP2XA

Managed Gigabit Ethernet Fiber Switch

(12) 100/1000Base-X SFP Slots + (2) 1G/10G SFP+ slots + (2) 10/100/1000Base-T



Web User Guide

33752 Rev. C

Trademarks

All trademarks and registered trademarks are the property of their respective owners.

Copyright Notice/Restrictions

SM12DP2XA L2+ Managed GbE Fiber Switch Web User Guide 33752 Rev. C

Contact Information

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

Revision History

Rev	Date	Description
A	6/19/18	Initial release at FW v7.10.1423 2018-01-04 and HW v1.01.
B	1/20/20	Update for FW v7.10.2064; add "SNMP Server location" command and add Traffic Monitor back to DMS. Update for FW v7.10.2307; change DMS disable behavior and improve password encoding.
C	6/15/20	FW v7.10.2544: add Rapid Ring and Auto-logout features.

Cautions and Warnings

Definitions

Cautions indicate that there is the possibility of poor equipment performance or potential damage to the equipment. **Warnings** indicate that there is the possibility of injury to person.
Cautions and Warnings appear here and may appear throughout this manual where appropriate. Failure to read and understand the information identified by this symbol could result in poor equipment performance, damage to the equipment, or injury to persons.

Cautions

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

Warnings

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

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

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

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

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

See Electrical Safety Warnings on page 30 for Electrical Safety Warnings translated into multiple languages.

Table of Contents

Introduction

The SM12DP2XA Managed Gigabit Ethernet Fiber Switch is a next-generation Fiber Switch offering full suite of L2 features and additional 10GbE uplink connections. Advanced L3 features such as Static Route deliver better cost performance and lower total cost of ownership in Enterprise networks or backbone via fiber or copper connections.

The SM12DP2XA provides 12 GbE SFP ports, 2 RJ45 ports, 2 10GbE SFP+ ports and RJ45 Console port with built-in AC and DC dual power supply. The SM12DP2XA provides front panel access to the power, data, and management port in a compact form factor that allows desktop, wall-mount, or rack-mount installation.

The SM12DP2XA is ideal to deliver management simplicity, better user experience, and lowest total cost of ownership. The embedded Device Managed System is designed to be extremely easy-to-use, manage, and install IP Phones, IP Cameras, or WAPs for enterprise applications. Features include:

- Device Management System (DMS)
- IPv4 and IPv6 management
- Support Jumbo Frame up to 9K bytes
- Authentication – RADIUS, TACACS+
- IEEE 802.1X: RADIUS authentication, authorization and accounting, MD5 hash, guest VLAN, single/multiple host mode and single/multiple sessions
- DHCP Relay, DHCP Option 82, DHCP Snooping, DHCP Server, DHCP Per Port
- L2/L3/L4 ACLs support MAC, VLAN ID or IP, protocol, port, DSCP/IP precedence/TCP.UDP, Ether Type, ICMP, TCP flag
- LLDP (Link Layer Discovery Protocol)
- IP Source Guard, Port Security
- Port Mirroring
- Firmware update through TFTP/HTTP and console
- Syslog
- 1RU high, compact form factor
- Extended operating temperature: -20°C to + 60°C
- Rapid Ring and Spanning Tree (MSTP, RSTP, STP)

About this Manual

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

Related Manuals

SM12DP2XA Quick Start Guide, 33750
SM12DP2XA Install Guide, 33751
SM12DP2XA Web User Guide, 33752 (this manual)
SM12DP2XA CLI Reference, 33753
Release Notes

For More Information

A printed Quick Start Guide is shipped with each unit.

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.

Note: Information in this document is subject to change without notice. Note that this manual provides links to third party web sites for which Transition Networks is not responsible.

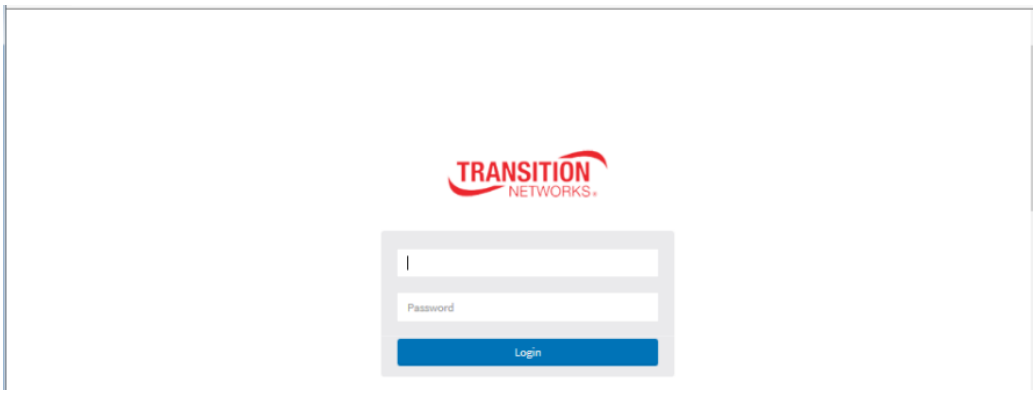
Chapter 1 - Web-based Management Operation

1-1 Initial Login and Web UI Description

This chapter describes how to configure and manage the SM12DP2XA via the web interface. With the Web UI, you can easily configure and monitor, from any port of the switch, all switch parameters and status, including port activity, Spanning tree status, port aggregation status, multicast traffic, VLAN and priority status, etc. The SM12DP2XA default values are:

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

After the SM12DP2XA has been configured for the interface, you can browse it. For instance, type 192.168.1.77 in the address row in a browser. The login page displays, prompting for a Username and Password.



The default username is **admin** and password is **admin**. For the first time to use, enter the default username and password, and then click the **Login** button. The login process now is complete.
The login menu requires you have to enter the complete username and password respectively.
The SM12DP2XA will not give you a shortcut to username automatically. This looks inconvenient but is safer.

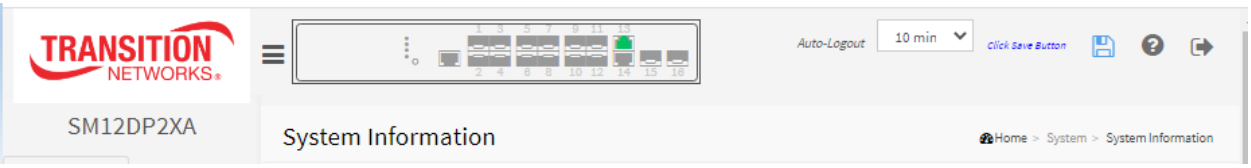
The SM12DP2XA allows two or more users using administrator's identity to manage this switch; whichever administrator does the last setting will be the available configuration to affect the system.

Note: When you log in to the SM12DP2XA Web UI, you can use either IPv4 or IPv6 login to manage. To optimize the display effect, we recommend you use Microsoft IE 6.0 or above, Netscape V7.1 or above, or FireFox V1.00 or above with resolution set to 1024x768. The switch supports neutral web browser interface.

Note: The SM12DP2XA default is DHCP disabled, so if you do not have DHCP server to provide an IP addresses to the switch, the switch default IP address is 192.168.1.77.

Webpage Controls

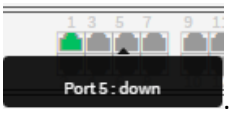
After Login, the System Information page displays by default. The webpage controls are shown and described below.



Click the Transition Networks logo to return to the Switch > System > System Information page.

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

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

or 

.

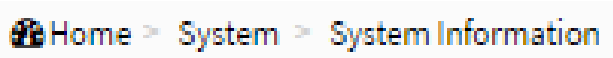
Click on any port to display its current Detailed Port Statistics page.

Top right corner icons: 

Save Configuration: Click to save parameter changes to the running-config file. Click OK when the message "*Please confirm to save current running-config file as startup-config file?*" displays.

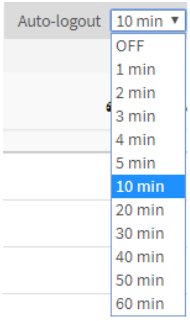
Help: Displays the Help page for the current webpage.

Logout: Logs you out and displays the Login prompt.



Displays the current webpage path.

: Auto-logout dropdown lets you set the amount of time after a successful login before an automatic log out occurs. The selections are OFF, 1, 2, 3, 4, 5, 10, 20, 30, 40, and 60 minutes (added at FW 7.10.2544). The default is 10 minutes.
When set to OFF, no Auto-logout occurs.



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

When the Auto-Logout timeout setting is changed, it directly writes to running-config.
To save the timeout change to start-up config, you must execute a save to startup-config.
To examine the running-config, you can run the CLI command "showing running-config" or in the Web UI just log out and log back in again.
To save the timeout change into startup-config, you must do a save to startup-config and then reboot the switch.

In other words:

- 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.

Chapter 2 - System Configuration

2-1 Initial Configuration

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

2-1 *System*

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

2-1.1 Information

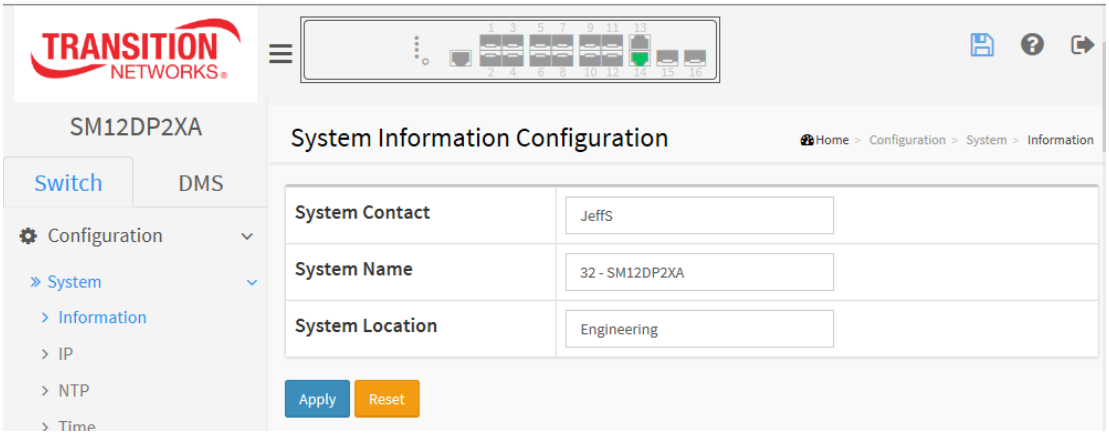
The switch system contact information is provided here.

Web interface

To configure System Information in the web interface:

1. Click Configuration, System, Information.
2. Enter System Contact, System Name, and System Location in the entry fields.
3. Click Apply.

Figure 2-1.1: System Information Configuration



Parameter descriptions:

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

System name: An administratively assigned name for this managed node. By convention, this is the node's fully-qualified domain name. A domain name is a text string drawn from the alphabet (A-Za-z), digits (0-9), minus sign (-).The allowed string length is 0 to 128. The field displays SM12DP2XA by default.

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

Buttons

Apply: Click to save changes.

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

2-1.2 IP

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

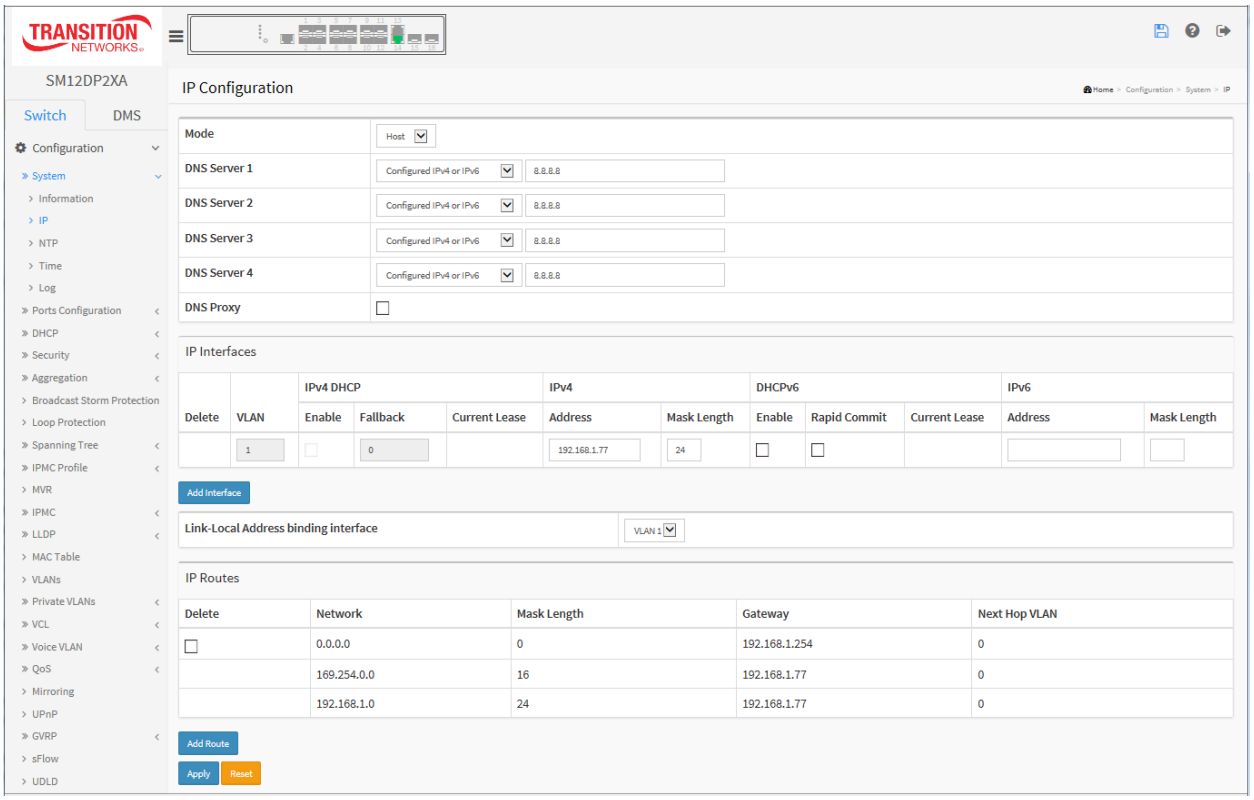
Configure the switch-managed IP information on this page (IP basic settings, control IP interfaces and IP routes). The maximum number of interfaces supported is 128 and the max number of routes is 32.

Web Interface

To configure an IP address via the web interface:

1. Click Configuration, System, IP.
2. Select the IP Configuration Mode (Host or Router).
3. Configure DNS Server 1 -4 as required.
4. Click Add Interface and enter the parameters to create a new Interface on the switch.
5. Click Add Route and enter the parameters to create a new Route on the switch.
6. Click Apply.

Figure2-1.2: IP configuration

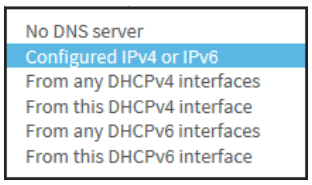


Parameter descriptions:

<u>IP Configuration</u>

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

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



No DNS server: No DNS server will be used.

Configured IPv4 or IPv6: Explicitly provide the IPv4 or IPv6 address of the DNS Server in dotted decimal notation (default).

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

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

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

IP Interfaces

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

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

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

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

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

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

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

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

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

Link-Local Address binding interface: At the dropdown select the binding interface (e.g., 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 8 interfaces is supported.

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

Apply: Click to save changes.

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

2-1.3 NTP

NTP (Network Time Protocol) is used to sync with the network time based Greenwich Mean Time (GMT). It use the NTP mode and you can select a built-in NTP time server or manually specify an NTP server as well as Time Zone. The switch will sync the time shortly after pressing the **Apply** button. Though it synchronizes the time automatically, NTP does not update the time periodically without user interaction.

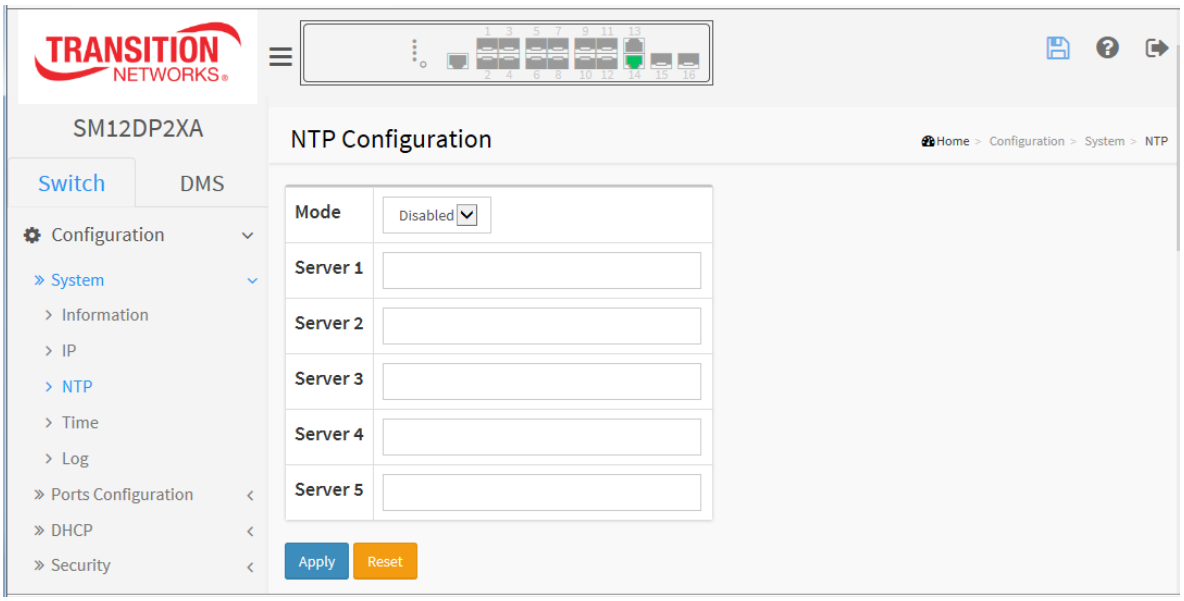
Time Zone is an offset time off GMT. You must select the time zone first and then perform time sync via NTP, since the switch will combine this time zone offset and updated NTP time to come out the local time, otherwise, you will not able to get the correct time. The switch supports configurable time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

Web Interface

To configure NTP in the web interface:

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

Figure 2-1.3: NTP Configuration



Parameter descriptions:

Mode : Sets the NTP mode operation. Possible modes are:

Enabled: Enable NTP client mode operation.

Disabled: Disable NTP client mode operation.

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

Buttons

Apply: Click to save changes.

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

2-1.4 Time

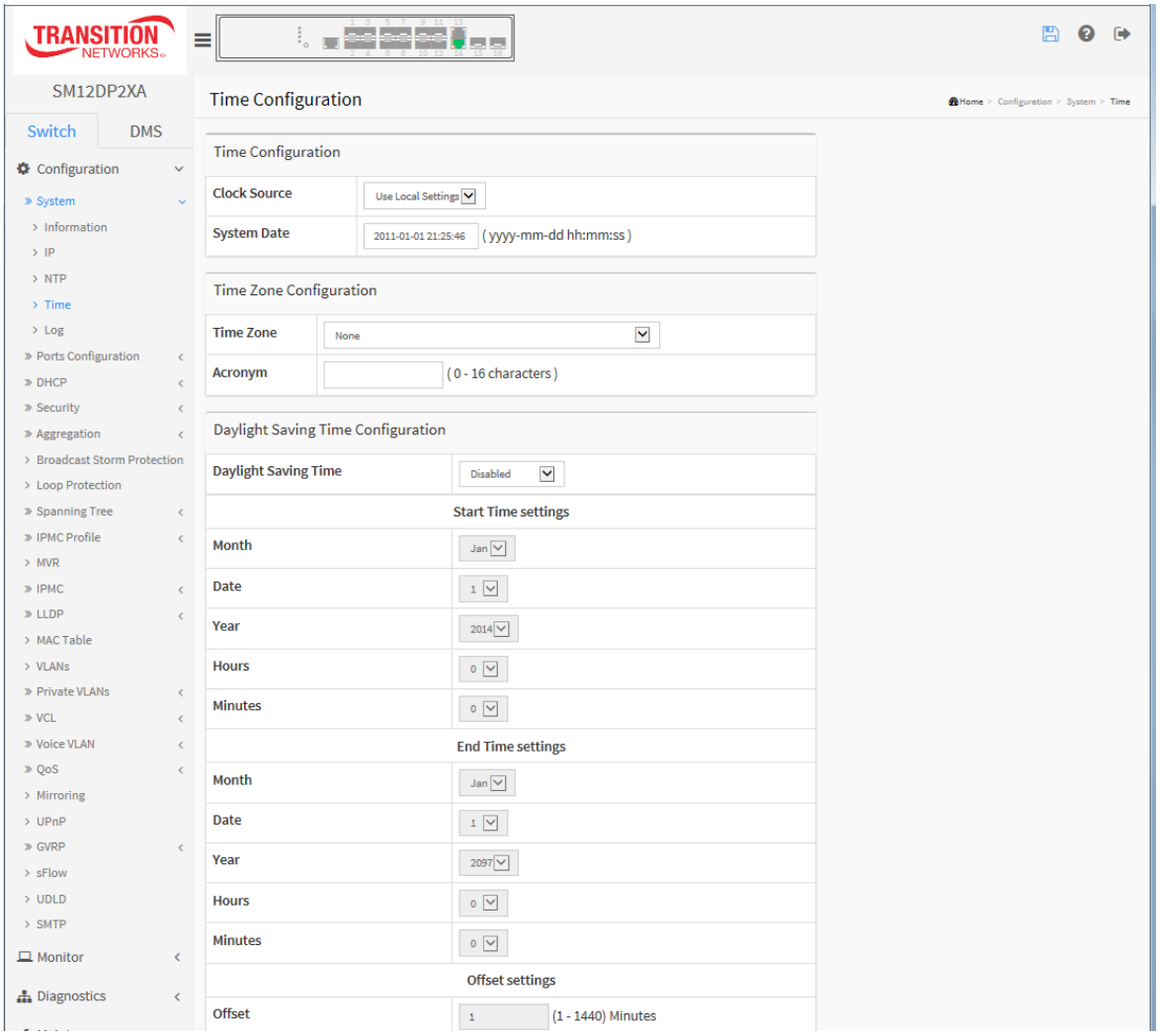
The switch provides manual and automatic ways to set the system time via NTP. Manual setting is simple; just enter “Year”, “Month”, “Day”, “Hour” and “Minute” within the valid value range indicated for each parameter.

Web Interface

To configure Time in the web interface:

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

Figure 2-1.4: Time Configuration



Parameter descriptions:

Time Configuration

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

System Date: Show the current time of the system. The year of system date limits between 2011 and 2037.

Time Zone Configuration

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

Acronym: Set the acronym of the time zone. This is a User configurable acronym to identify the time zone. (Range : Up to 16 characters)

Daylight Saving Time Configuration

Daylight Saving Time:

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

Recurring Configuration

Start time settings:

Week - Select the starting week number.

Day - Select the starting day.

Month - Select the starting month.

Hours - Select the starting hour.

Minutes - Select the starting minute.

End time settings:

Week - Select the ending week number.

Day - Select the ending day.

Month - Select the ending month.

Hours - Select the ending hour.

Minutes - Select the ending minute.

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

Note: The “Start Time Settings” and “End Time Settings” display what you set in the “Start Time Settings” and “End Time Settings” fields.

Buttons

Apply – Click to save changes.

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

2-1.5 Log

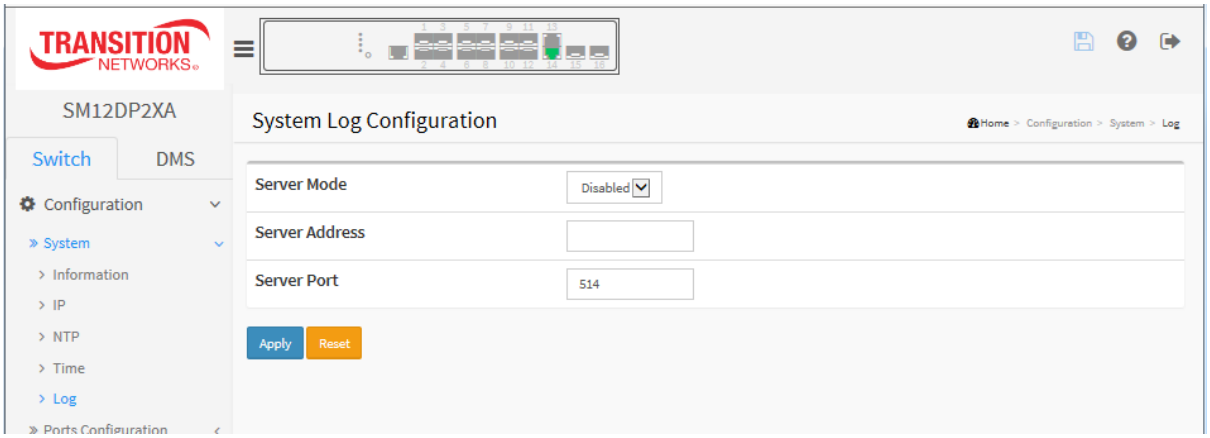
Syslog is a standard for logging program messages . It allows separation of the software that generates messages from the system that stores them and the software that reports and analyzes them. It can be used as well a generalized informational, analysis and debugging messages. Syslog is supported by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

Web Interface

To configure log parameters v the web interface:

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

Figure2-1.5: System Log Configuration



Parameter descriptions:

Server Mode : Indicate the server mode operation. When the mode operation is enabled, the syslog message is sent to the 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. A syslog packet will still be sent 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 provide DNS feature, it also can be a host name.

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

Buttons :

Apply – Click to save changes.

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

2-3 Ports Configuration

This page lets you view and configure the Port detail parameters of the switch (e.g., enable or disable switch Ports, monitor ports' content and status).

2-3.1 Ports

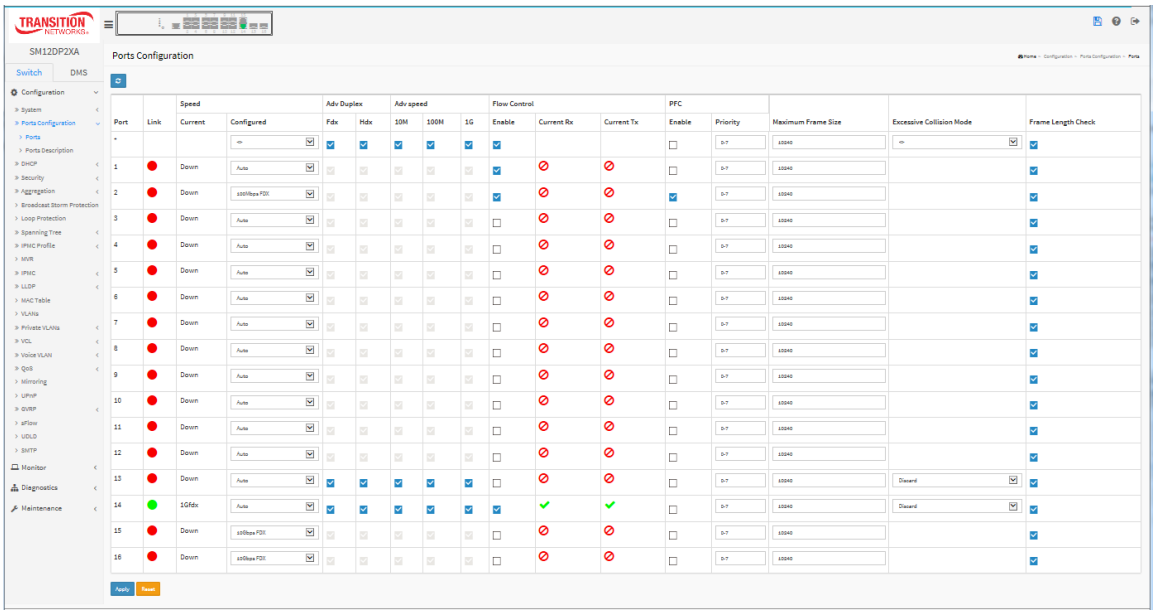
This page lets you view and configure current port settings.

Web Interface

To configure a Current Port Configuration in the web interface:

1. Click Configuration, Ports Configuration, Ports.
2. Specify Speed, Duplex, Flow Control, Max Frame size, Excessive Collision mode and Power Control.
3. Click Apply.

Figure 2-3.1: Port Configuration



Parameter descriptions:

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

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

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

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

Disabled - Disables the switch port operation.

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

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

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

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

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

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

10Gbps FDX - Forces the port in 10Gbps full duplex mode (ports 15 and 16 only).

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

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

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

PFC: When PFC (802.1Qbb Priority Flow Control) is enabled on a port then flow control on a priority level is enabled. Through the Priority field, a range (one or more) of priorities can be configured (e.g., '0-3,7) which equals '0,1,2,3,7'. PFC is not supported with auto negotiation. **Note**: Both PFC and Flow control cannot both be enabled for the same port.

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

Excessive Collision Mode: Configure port transmit collision behavior (ports 13 and 14 only).

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 will 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).

Enabled **:** frames with payload size less than 1536 bytes are dropped if the EtherType/Length field doesn't match the actual payload length.

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.

Message: *Both PFC and Flow Control cannot be enabled for the same port.*
Recovery: Click the **OK** button and disable either PFC or Flow Control.

2-3.2 Ports Description

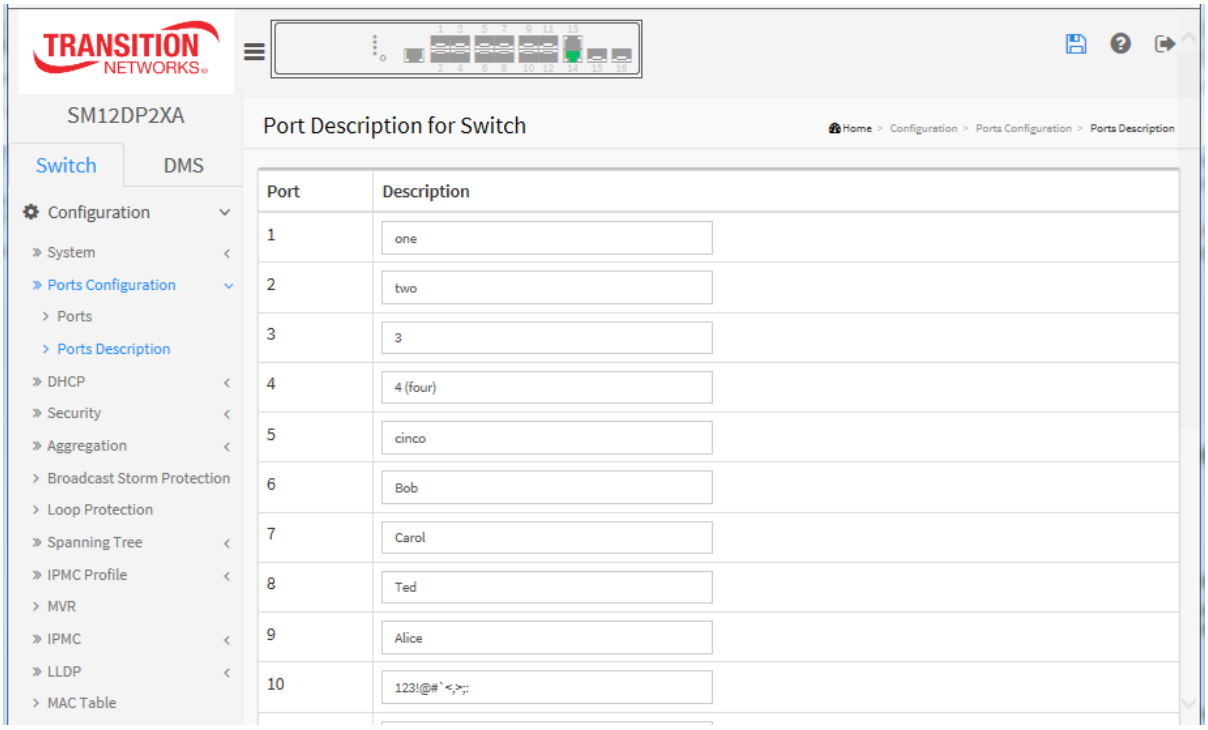
This page lets you enter descriptions for the Ports. You can enter an alphanumeric string with the name or version identification for the system's hardware type, software version, application, etc.

Web Interface

To configure a Port Description in the web interface:

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

Figure 2-3.2: Port Description



Parameter descriptions:

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

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

Buttons

Apply – Click to save changes.

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

2-4 DHCP

A DHCP Server is used to allocate network addresses and deliver configuration parameters to dynamically configured hosts called DHCP client.

2-4.1 Server

2-4.1.1 Mode

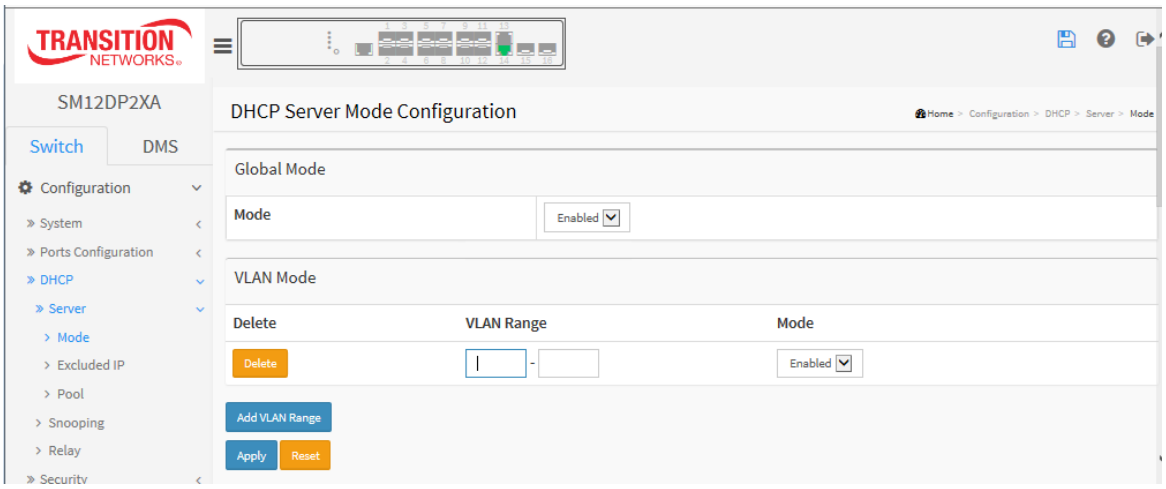
This page lets you configure global mode and VLAN mode to enable/disable DHCP server per system and per VLAN.

Web Interface

To configure DHCP server mode in the web interface:

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

Figure 2-4.1.1: DHCP Server Mode Configuration



Parameter descriptions:

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

> ***Enabled***: Enable DHCP server per system.
> ***Disabled***: Disable DHCP server pre system.

VLAN Range : Indicate the VLAN range in which DHCP server is enabled or disabled. The first VLAN ID must be smaller than or equal to the second VLAN ID. BUT, if the VLAN range contains only 1 VLAN ID, then you can just input it into either one of the first and second VLAN ID or both.

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

1. Press “Add VLAN Range” to add a new VLAN range.
2. Enter the VLAN range that you want to disable.
3. Choose Mode to be Disabled.
4. Press Apply to save the changes.

The disabled VLAN range is removed from the DHCP Server Mode configuration page.

Mode : Indicates the operating 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.

2-4.1.2 Excluded IP

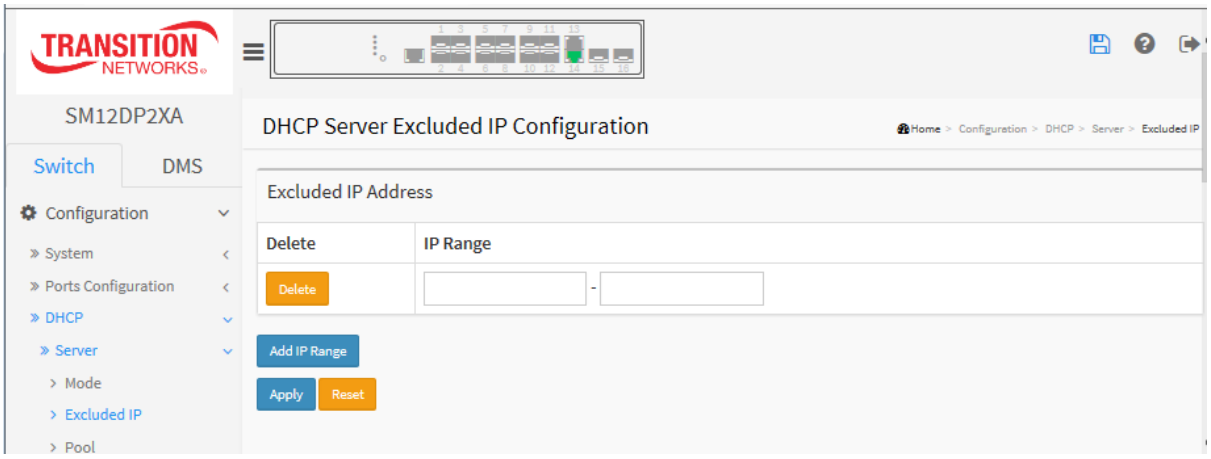
This page lets you configure excluded IP addresses. A DHCP server will not allocate these excluded IP addresses to a DHCP client.

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 enter the IP Range on the switch.
3. Click Apply.

Figure 2-4.1.2: DHCP Server Excluded IP



Parameter descriptions:

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

Buttons

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

Apply – Click to save changes.

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

2-4.1.3 Pool

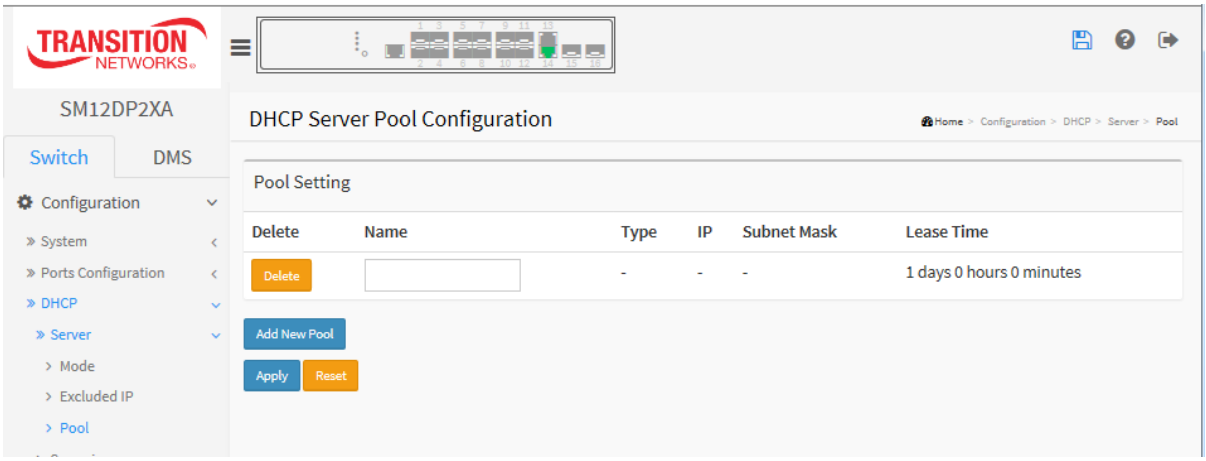
This page lets you manage DHCP pools. Based on the DHCP pool, a DHCP server will allocate IP address and deliver configuration parameters to the DHCP client.

Web Interface

To configure DHCP server pool in the web interface:

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

Figure 2-4.1.3 DHCP Server Pool



Parameter descriptions:

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

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

Type : Displays which type the pool is.

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

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

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

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

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

Lease Time : Displays lease time of the DHCP server pool.

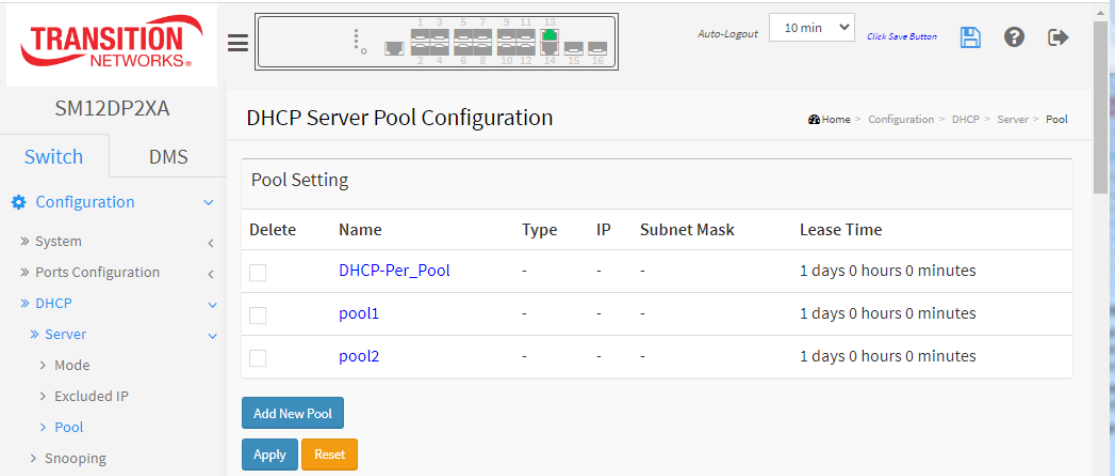
Buttons

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

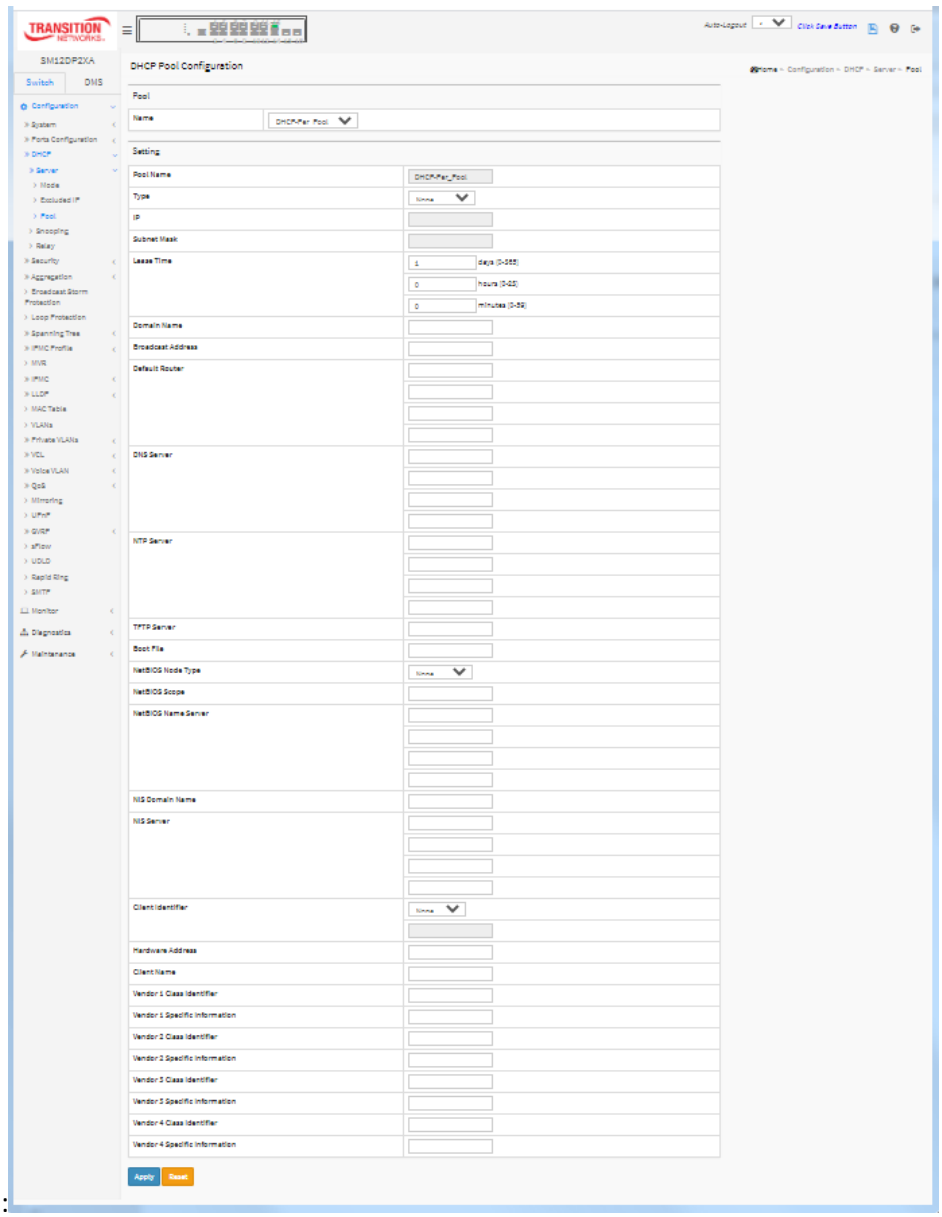
Apply – Click to save changes.

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

After you add pools and click Apply, the DHCP Server Pool Configuration page displays.



You can click a linked pool to display its specific DHCP Pool Configuration page:



:

Parameter descriptions:

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 that client should use when resolving hostname via DNS.

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

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

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

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.

Messages:

Pool type is defined so IP must be inputted.

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

2-4.2 Snooping

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

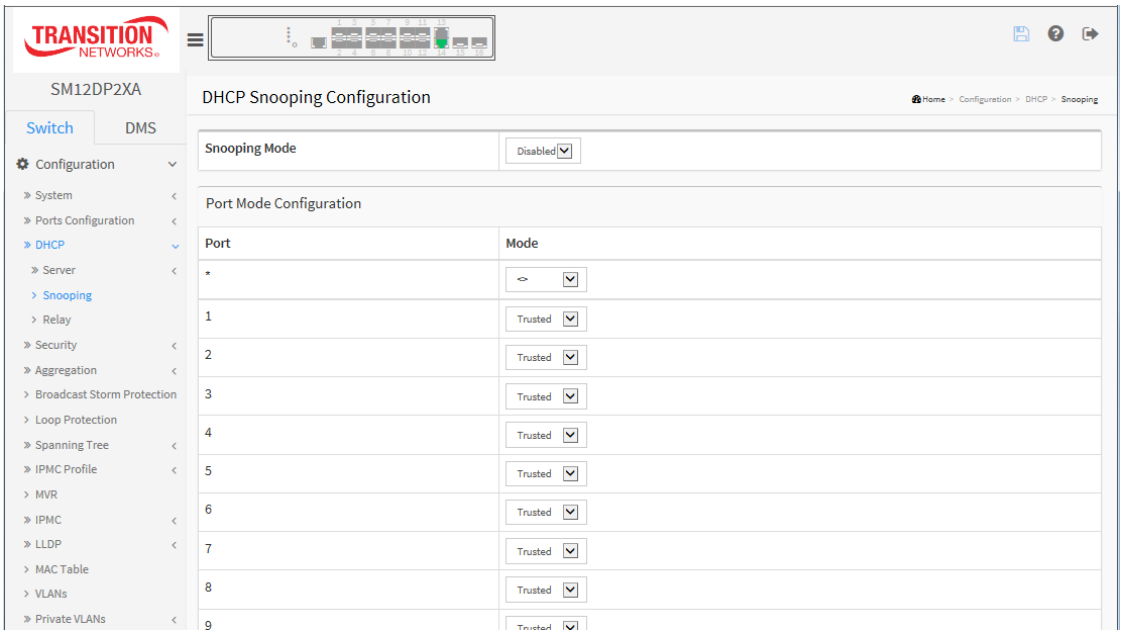
This page lets you configure the DHCP Snooping parameters of the switch. DHCP Snooping can prevent attackers from adding their own DHCP servers to the network.

Web Interface

To configure DHCP snooping in the web interface:

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

Figure 2-4.2: DHCP Snooping Configuration



Parameter descriptions:

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

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

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

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

Buttons

Apply – Click to save changes.

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

2-4.3 Relay

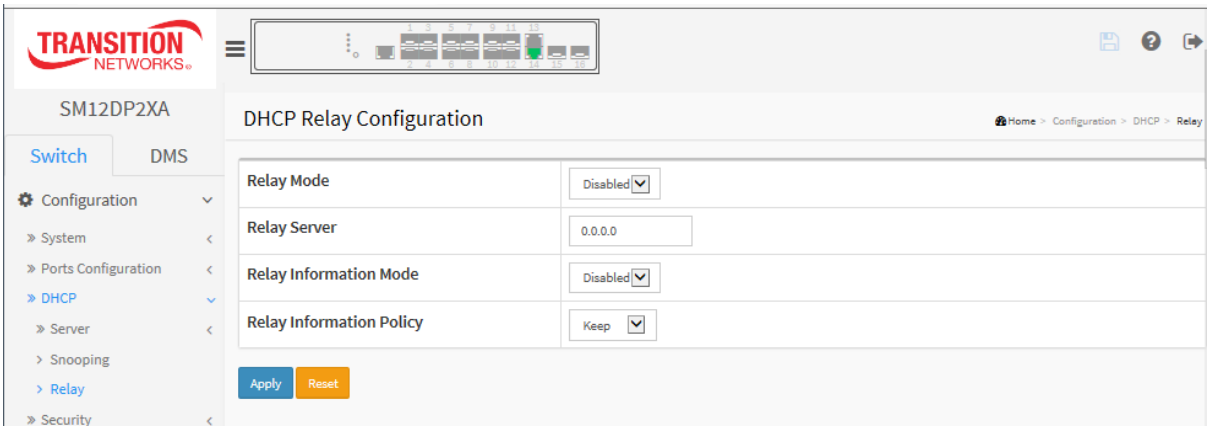
A DHCP relay agent is used to forward and to transfer DHCP messages between the clients and the server when they are not in the same subnet domain. It stores the incoming interface IP address in the GIADDR field of the DHCP packet. The DHCP server can use the value of GIADDR field to determine the assigned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

Web Interface

To configure DHCP Relay in the web interface:

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

Figure 2-4.3: DHCP Relay Configuration



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), and the last two characters are the port number. For example, "00030108" means the DHCP message was received from VLAN ID 3, switch ID 1, port No 8. The option 82 remote ID value is equal to the switch MAC address.

Possible modes are:

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

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

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

Buttons

Apply – Click to save changes.

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

2-5 Security

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

2-5.1 Switch

2-5.1.1 Users

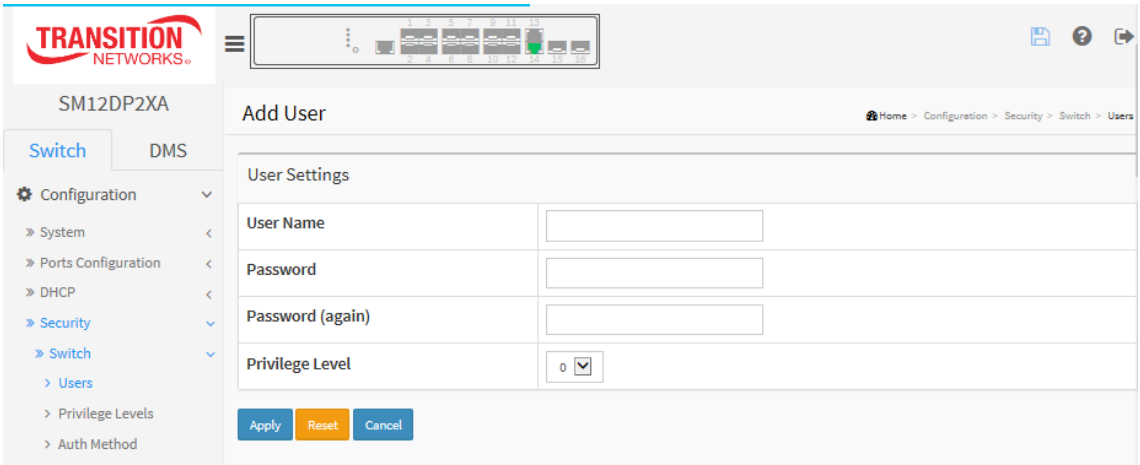
This page provides an overview of the current users. Currently the only way to login as another user on the web server is to close and reopen the web browser.

Web Interface

To configure User in the web interface:

1. Click Configuration, Security, Switch, Users.
2. Click Add new user
3. Specify the User Name parameter.
4. Click Apply.

Figure 2-5.1.1: Users Configuration – Add User



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 to 255, and the allowed content is the ASCII characters from 32 to 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 to 15. If the privilege level value is 15, it can access all groups, i.e. that is granted the fully control of the device. But others value need to refer to each group privilege level. User's privilege should be same or greater than the group privilege level to have the access of that group. By default setting, most groups' privilege level 5 has the read-only access and privilege level 10 has the read-write access. And the system maintenance (software upload, factory defaults and etc.) need user privilege level 15. Generally, the privilege level 15 can be used for an administrator account, privilege level 10 for a standard user account and privilege level 5 for a guest account. The default is 0.

Buttons

Apply – Click to save changes.

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

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

Delete User - Delete the current user; button not available for new configurations (Add New User).

2-5.1.2 Privilege Level

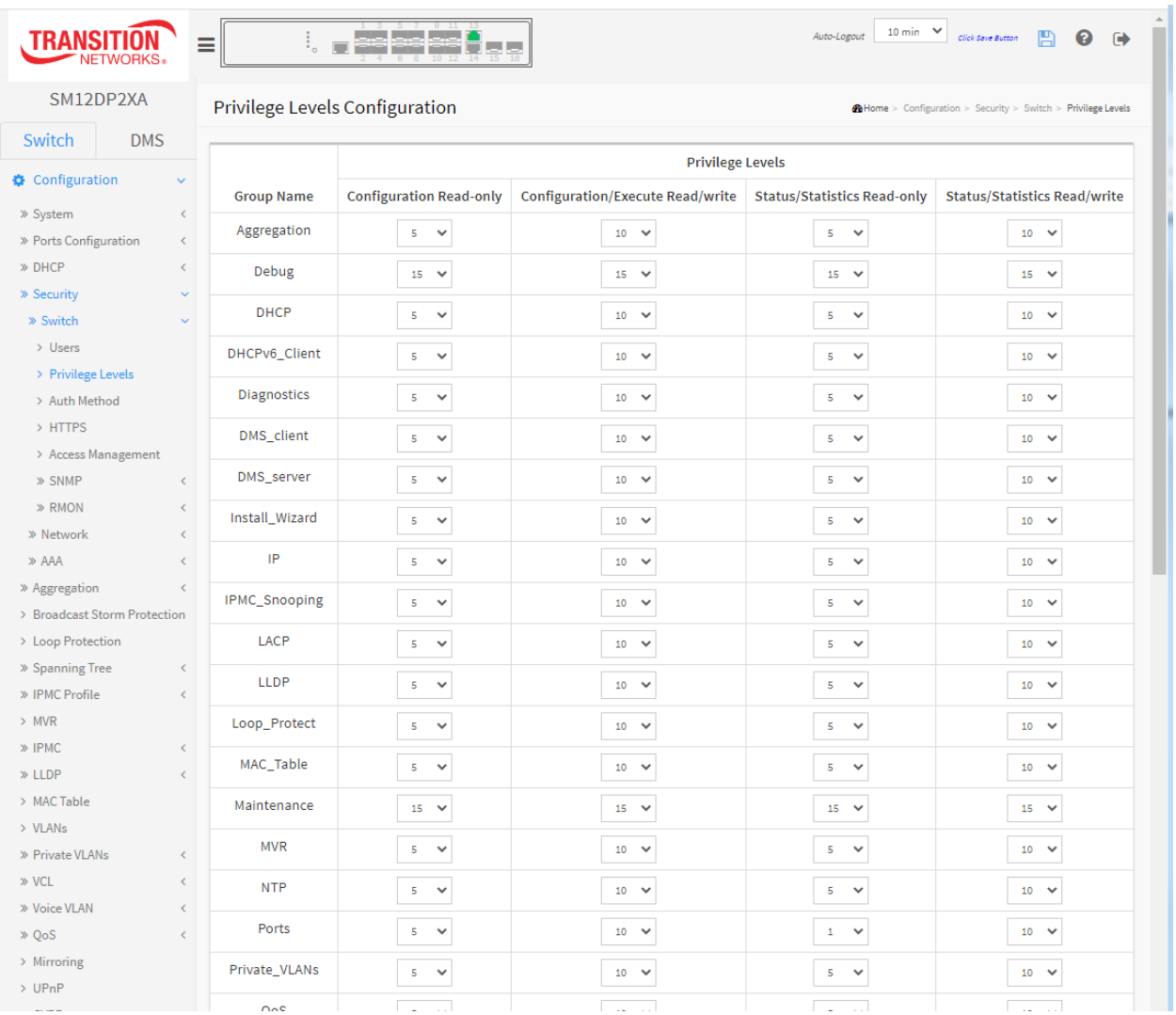
This page lets you set privilege levels for the various switch functions. The switch lets you set ACTIVATE, Aggregation, Debug, DHCP, DHCPv6_Client, Diagnostics, DMS_client, DMS_server, Install_Wizard, IP, IPMC_Snooping, LACP, LLDP, Loop_Protect, MAC_Table, Maintenance, MVR, NTP, Ports, Private_VLANs, QoS, RMirror, Security, sFlow, SMTP, Spanning_Tree, System, Trap_Event, Trouble_Shooting, TS_client, TS_server, UDLD, UPnP, VCL, VLANs, Voice_VLAN, VTUN, and XXRP at Privilege Levels 1 to 15.

Web Interface

To configure Privilege Level in the web interface:

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

Figure2-5.1.2: Privilege Level Configuration



Parameter descriptions:

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

The following descriptions define these privilege level groups in detail:

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

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

IP: Everything except 'ping'.

Port: Everything except 'Cable Diagnostics'.

Diagnostics: 'ping' and 'Cable Diagnostics'.

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

Debug: Only present in CLI.

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

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

Buttons

Apply – Click to save changes.

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

2-5.1.3 Authentication Method

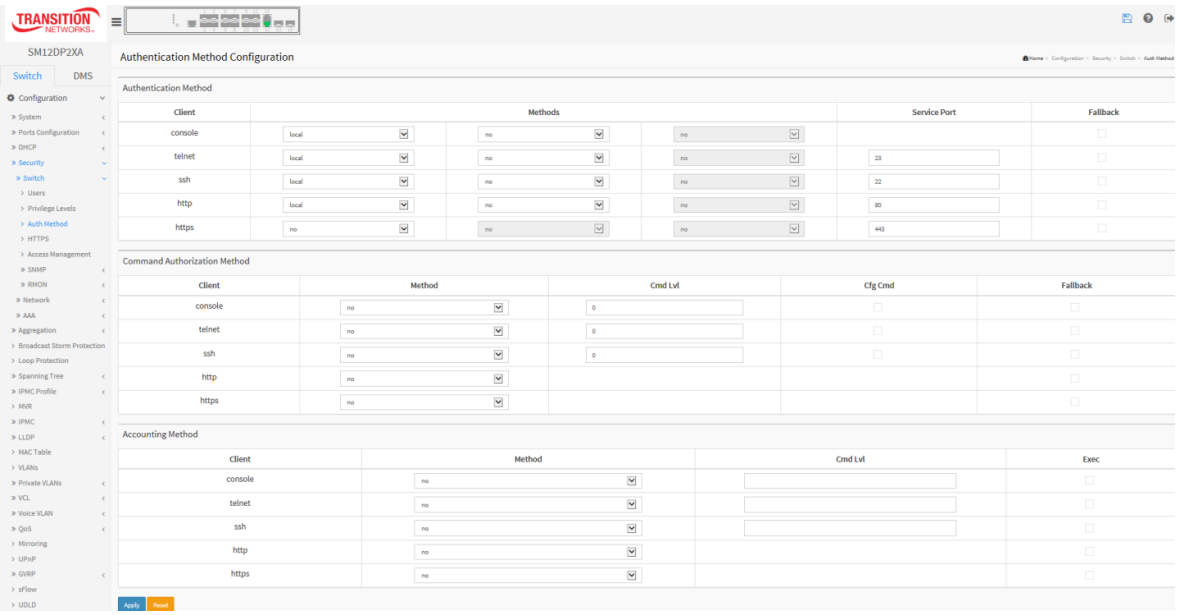
This page lets you configure a user with the authentication used when they log into the switch via one of the management client interfaces.

Web Interface

To configure an Authentication Method Configuration in the web interface:

1. Navigate to Configuration > Security > Switch > Auth Method.
2. Specify the Client (console, telnet, ssh, web) which you want to monitor.
3. Specify the Authentication Method (none, local, radius, tacacs+).
4. Check Fallback.
5. Click Apply.

Figure 2-5.1.3: Authentication Method Configuration



Parameter descriptions:

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

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

> ***none*** : authentication is disabled and login is not possible.
>
> ***local*** : use the local user database on the switch for authentication.
>
> ***radius*** : use a remote RADIUS server for authentication.
>
> ***tacacs+*** : use a remote TACACS+ server for authentication.

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

Buttons

Apply – Click to save changes.

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

2-5.1.4 HTTPs

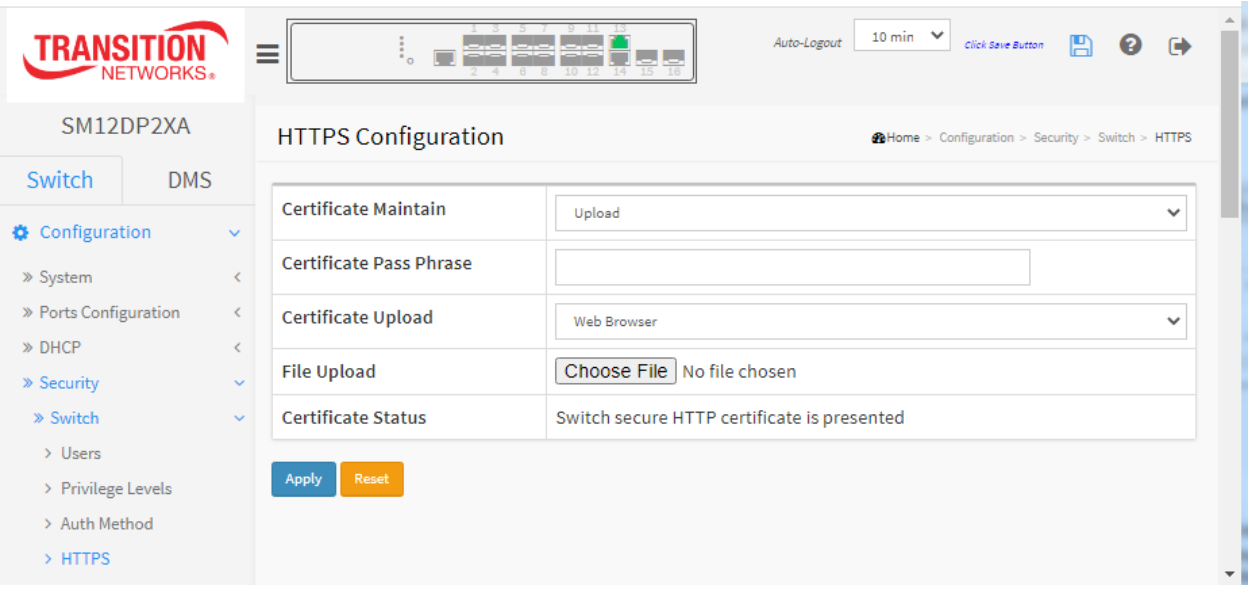
This page lets you configure the HTTPS (secure HTTP) settings and maintain the current certificate on the switch.

Web Interface

To configure a HTTPS Configuration in the web interface:

1. Navigate to Configuration > Security > Switch > HTTPS.
2. Select “Enabled” in the Mode of HTTPS Configuration.
3. Select “Enabled” in the Automatic Redirect of HTTPS Configuration.
4. Click Apply.

Figure 2-5.1.5: HTTPS Configuration



Parameter descriptions:

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

Upload: Upload a certificate PEM file. Possible methods are: Web Browser or URL.
Generate: Generate a new self-signed RSA certificate.

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

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

```
cat my.cert my.key > my.pem
```

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

Web Browser: Upload a certificate via Web browser.

URL: Upload a certificate via URL, the supported protocols are HTTP, HTTPS, TFTP and FTP.
The URL format is:

```
<protocol>://[<username>[:<password>]@]< host>[:<port>][/<path>]/<file_name>
```

For example:

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

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

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

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

Switch secure HTTP certificate is presented.
Switch secure HTTP certificate is not presented.
Switch secure HTTP certificate is generating ....

Buttons

Apply: Click to save changes.

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

2-5.1.6 Access Management

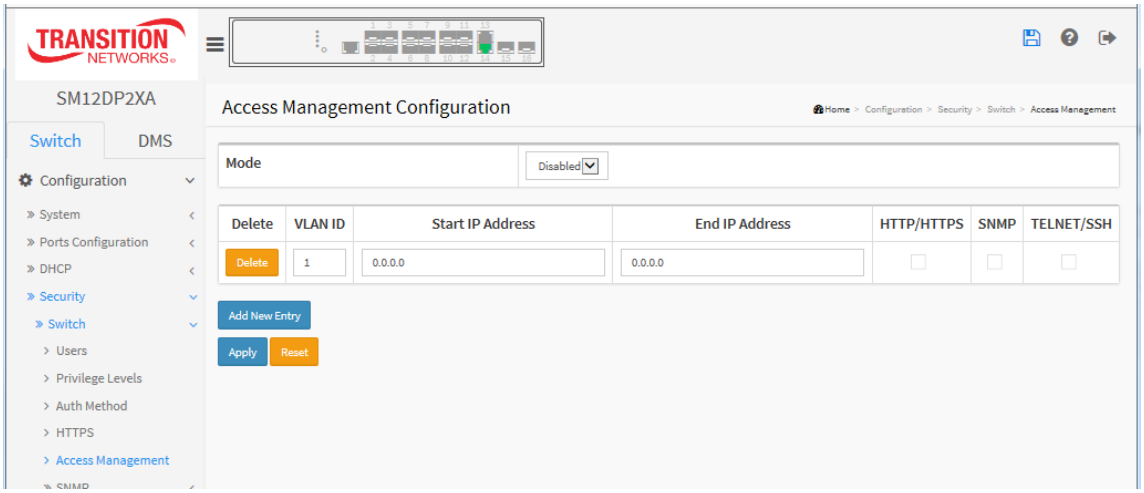
This page lets you configure access management table of the Switch including HTTP/HTTPS, SNMP, and TELNET/SSH. You can manage the switch over an Ethernet LAN or over the Internet.

Web Interface

To configure an Access Management Configuration in the web interface:

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

Figure 2-5.1.6: Access Management Configuration



Parameter descriptions:

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

Enabled: Enable access management mode operation.

Disabled: Disable access management mode operation.

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

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

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

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

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

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

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

Buttons:

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

Apply – Click to save changes.

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

2-5.1.7 SNMP

Any Network Management System (NMS) running the Simple Network Management Protocol (SNMP) can manage the Managed devices equipped with SNMP agent, provided that the Management Information Base (MIB) is installed correctly on the managed devices. The SNMP 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. SNMP agent is running on the switch to response the request issued by SNMP manager.

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

2-5.1.7.1 System

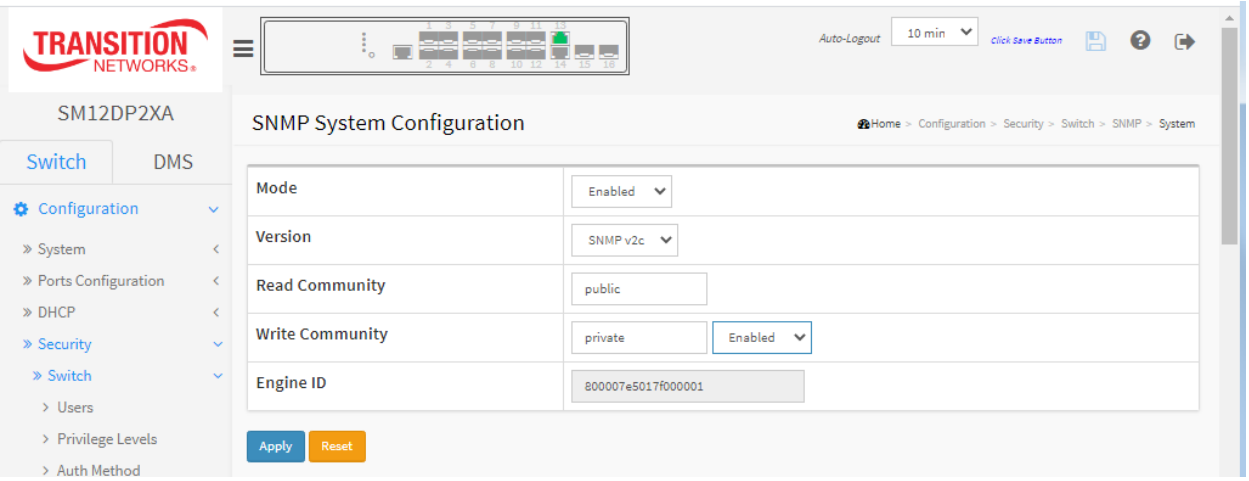
This page lets you configure SNMP settings, community name, trap host and public traps as well as the throttle of SNMP. An SNMP manager must pass the authentication by identifying both community names, then it can access the MIB information of the target device. So, both parties must have the same community name. Once completing the setting, click the **Apply** button, the setting takes effect.

Web Interface

To display the configure SNMP System in the web interface:

1. Click Configuration, Security, Switch, SNMP, System.
2. Set SNMP Mode, Version, Read Community and Write Community.
3. Specify the Engine ID.
4. Click Apply.

Figure2-5.1.7.1: SNMP System Configuration



Parameter descriptions:

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

Enabled: Enable the SNMP mode of operation.

Disabled: Disable the SNMP mode of operation.

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

SNMP v1: Set SNMP support to version 1.

SNMP v2c: Set SNMP support to version 2c.

SNMP v3: Set SNMP support to version 3.

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

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

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

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.

Messages:

The input value 'Trap Destination IPv6 Address' (::) is not a valid IPv6 address.

2-5.1.7.2 Trap

Configure SNMP traps on this page.

Global Settings

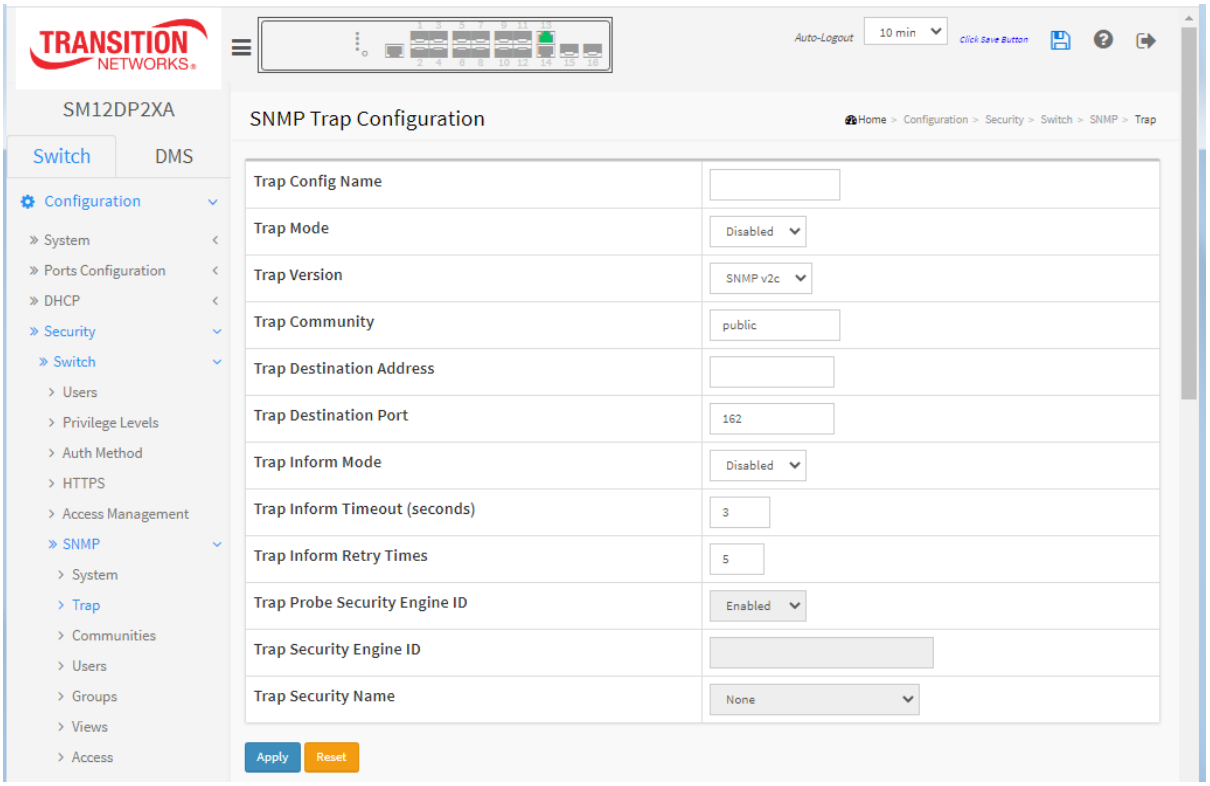
Configure an SNMP trap on this page.

Web Interface

To display the configure SNMP Trap Configuration in the web interface:

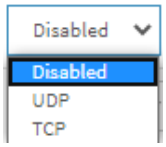
1. Click Configuration, Security, Switch, SNMP, Trap.
2. At the Mode dropdown select Enabled.
3. Click Add New Entry to create a new SNMP Trap.
4. Enter the SNMP Trap parameters.
5. Click Apply.

Figure2-5.1.7.2: SNMP Trap Configuration



Trap Config Name: Indicates the trap Configuration's name. Indicates the trap destination's name.

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

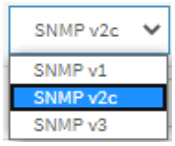


Disabled: Disable SNMP trap mode operation (default).

TCP: Enable TCP SNMP mode operation.

UDP: Enable UDP SNMP mode operation.

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



SNMPv1: Set SNMP trap supported version 1.
SNMPv2c: Set SNMP trap supported version 2c (default).
SNMPv3: Set SNMP trap supported version 3.

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

Trap Destination Address: Indicates the SNMP trap destination address. It allows a valid IP address in dotted decimal notation ('x.y.z.w'). It also allows a valid hostname. A valid hostname is a string drawn from the alphabet (A-Za-z), digits (0-9), dot (.), dash (-). Spaces are not allowed, the first character must be an alpha character, and the first and last characters must not be a dot or a dash.

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

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

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

> ***Enabled***: Enable SNMP trap inform mode operation.
> ***Disabled***: Disable SNMP trap inform mode operation.

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

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

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

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

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

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

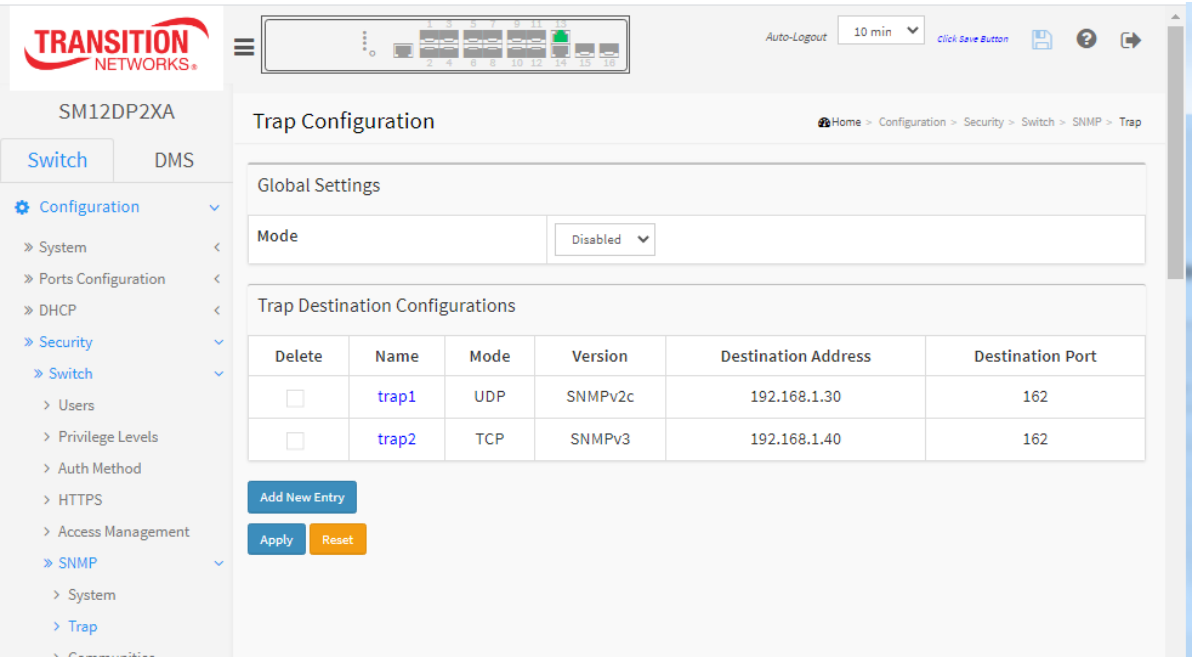
Buttons

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

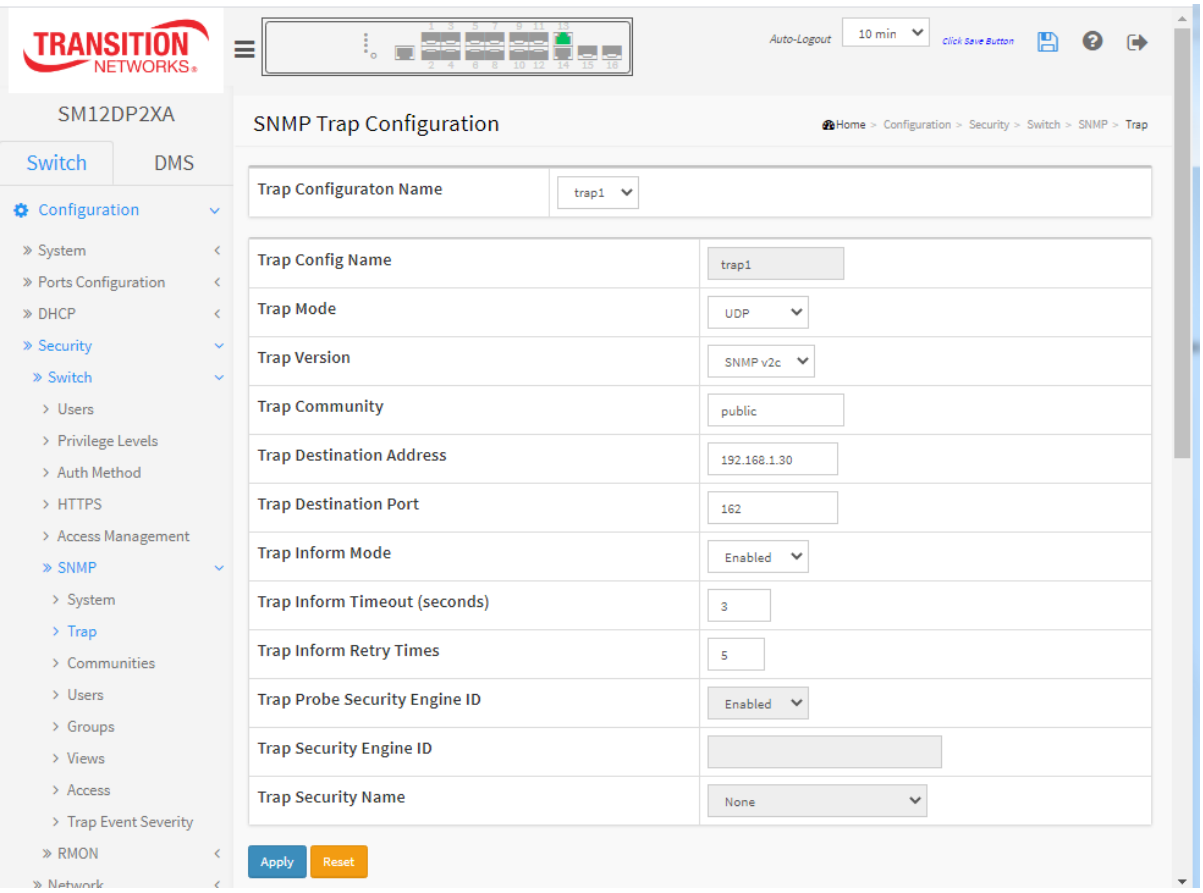
Apply : Click to save changes.

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

After you enter the screen parameters and click Apply, the Trap Configuration page displays with your new entries.



You can click a linked Name to display a page with additional SNMP Trap Configuration parameters. The page parameters displayed vary between SNMP v12, v2c, and v3.



2-5.1.7.3 **Communities**

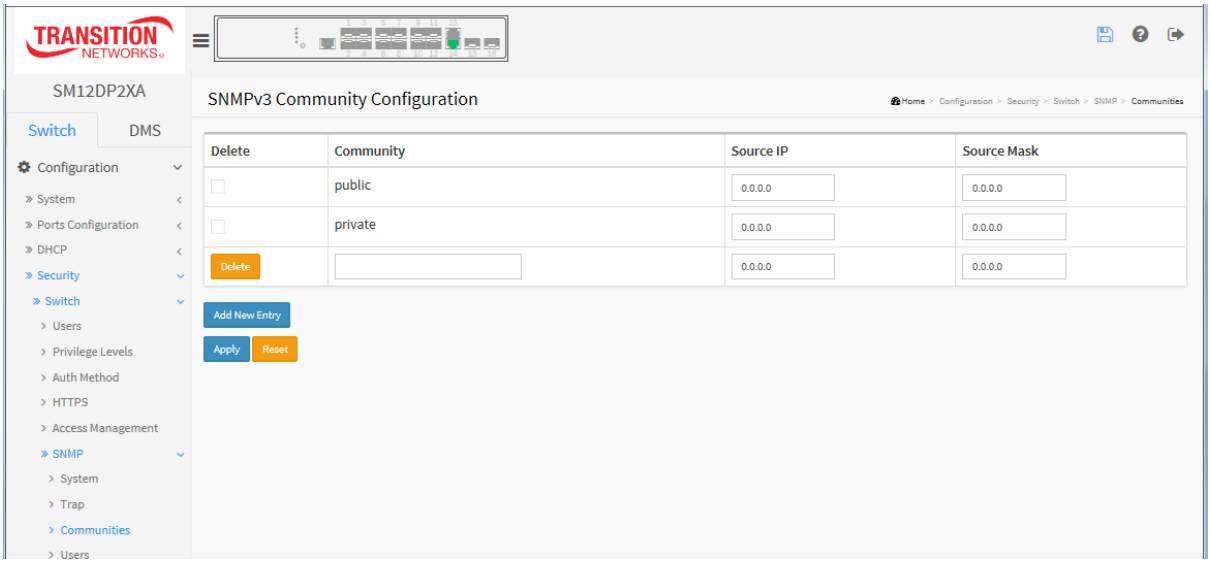
This page lets you configure SNMPv3 communities. The Community and User Name are unique.
To create a new community account, click the **Add New Community** button, and enter the account information then click Apply. The max number of Communities is 4.

Web Interface

To display the configure SNMP Communities in the web interface:

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

Figure2-5.1.7.3: SNMP Community Configuration



Parameter descriptions:

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

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

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

Source Mask : Indicates the SNMP access source address mask.

Buttons

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

Apply : Click to save changes.

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

2-5.1.7.4 Users

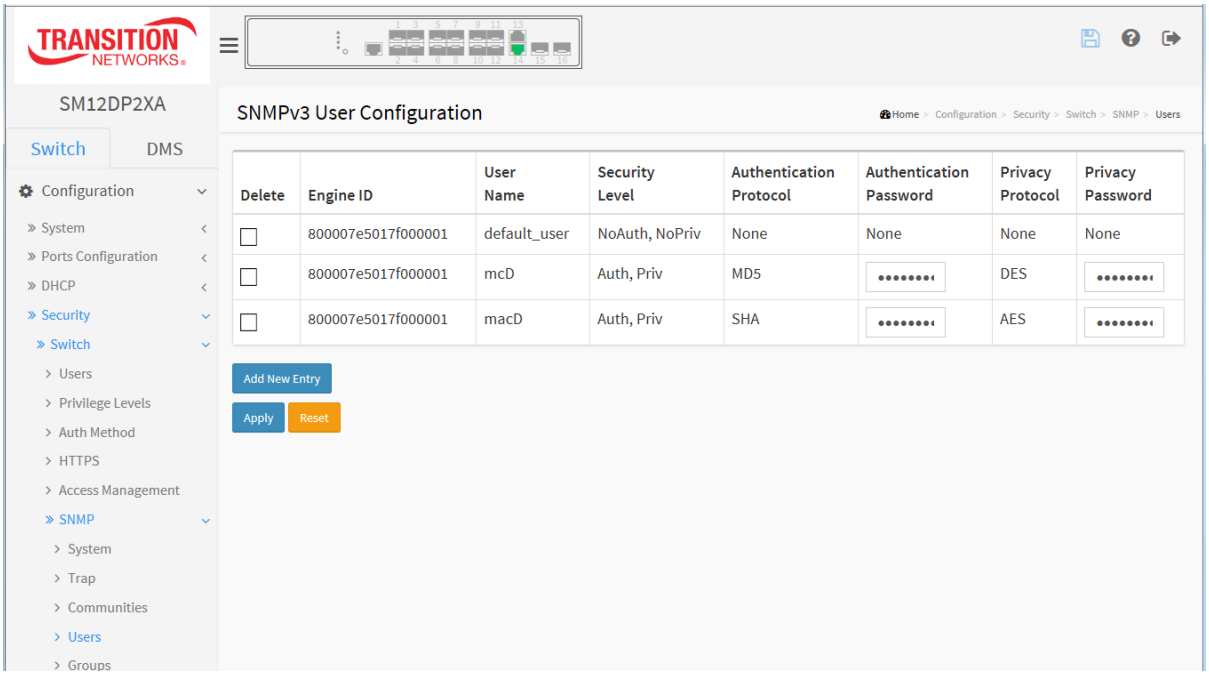
This page lets you configure SNMPv3 users. The Entry index key is User Name. The max number of SNMP v3 users is 10.

Web Interface

To display the configure SNMP Users in the web interface:

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

Figure 2-5.1.7.4: SNMP User Configuration



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

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

NoAuth, NoPriv: No authentication and no privacy.

Auth, NoPriv: Authentication but no privacy.

Auth, Priv: Authentication and privacy.

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

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

None: No authentication protocol.

MD5: An optional flag to indicate that this user uses MD5 authentication protocol. MD5 (Message-Digest algorithm 5) is a message digest algorithm that uses 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: An optional flag to indicate that this user uses SHA authentication protocol. 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.

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

Authentication Password : A string identifying the authentication password phrase.

For **MD5** authentication protocol, the allowed string length is 8 - 32. The allowed content is ASCII characters 33 - 126.

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. Possible privacy protocols are:

None: No privacy protocol.

DES: An optional flag to indicate that this user uses DES authentication protocol. 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: An optional flag to indicate that this user uses AES authentication protocol. AES (Advanced Encryption Standard) is the encryption key protocol applied in the 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.

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

2-5.1.7.5 Group

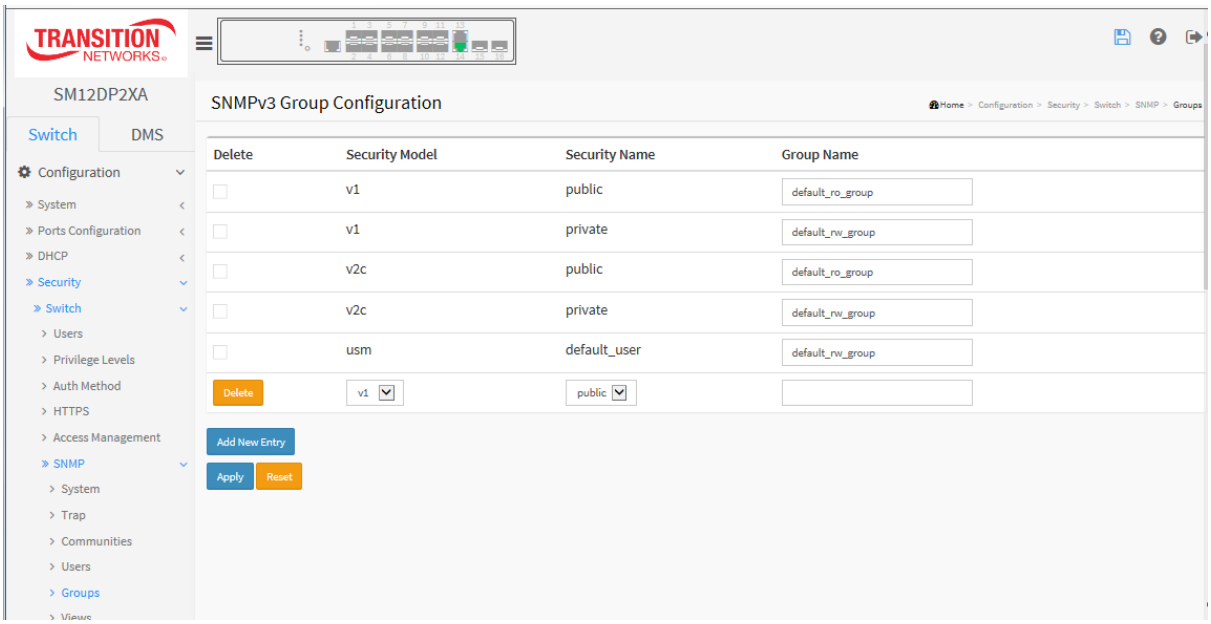
This page lets you configure SNMPv3 groups. The Entry index keys are Security Model and Security Name. To create a new group account, click the Add New Group button and enter the group information then click the Save button. The maximum number of Groups is v1: two, v2: two, v3: three.

Web Interface

To display the configure SNMP Groups in the web interface:

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

Figure 2-5.1.7.5: SNMP Groups Configuration



Parameter descriptions:

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

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

> ***v1***: Reserved for SNMPv1.
>
> ***v2c***: Reserved for SNMPv2c.
>
> ***usm***: User-based Security Model (USM).

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

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

2-5.1.7.6 Views

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

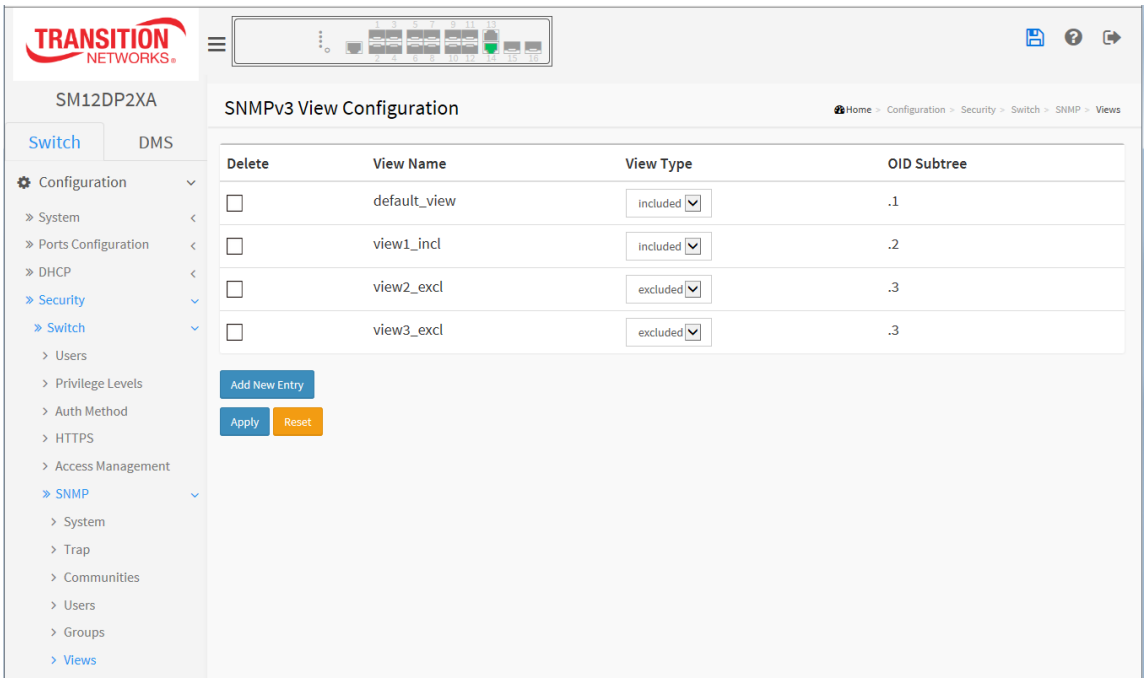
Configure SNMPv3 view table on this page. The entry index keys are View Name and OID Subtree.

Web Interface

To configure an SNMP view in the 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 2-5.1.7.6: SNMP Views Configuration



Parameter descriptions:

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

View Name : A string identifying the view name that this entry should belong to. The allowed string length is 1 - 32, 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 to 128. The allowed string content is digital number or asterisk (*).

2-5.1.7.7 Access

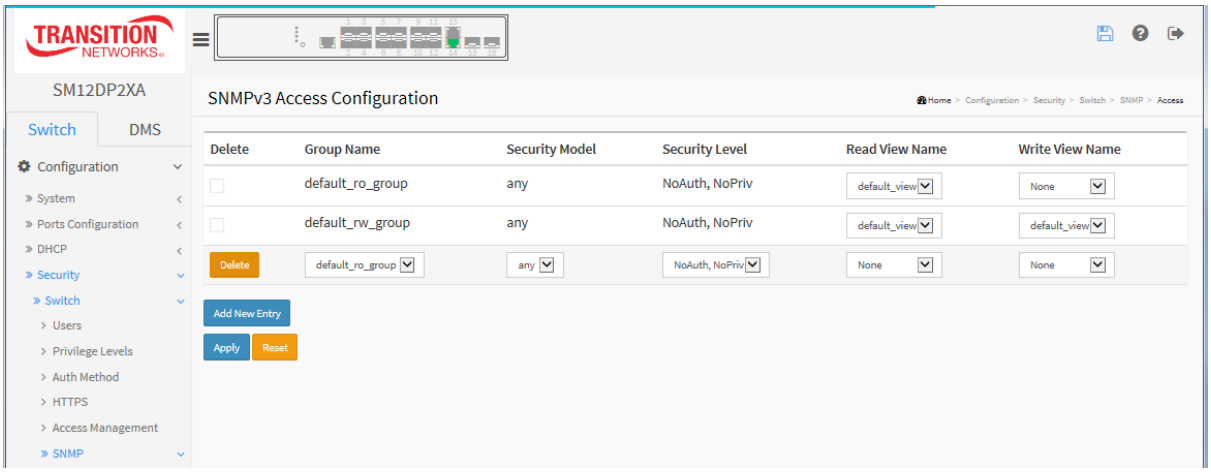
This page lets you configure SNMPv3 access. The Entry index key are Group Name, Security Model and Security level. To create a new access account, click the Add New Access button, and enter the access information then click Apply. The maximum number of Groups is 14.

Web Interface

To display the configure SNMP Access in the web interface:

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

Figure 2-5.1.7.7: SNMP Accesses Configuration



Parameter descriptions:

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

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

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

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

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

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

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

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

Buttons

Apply: Click to save changes.

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

Add New Entry: Click to add a new line to the table and enter parameters.

2-5.1.7.8 Trap Event Severity

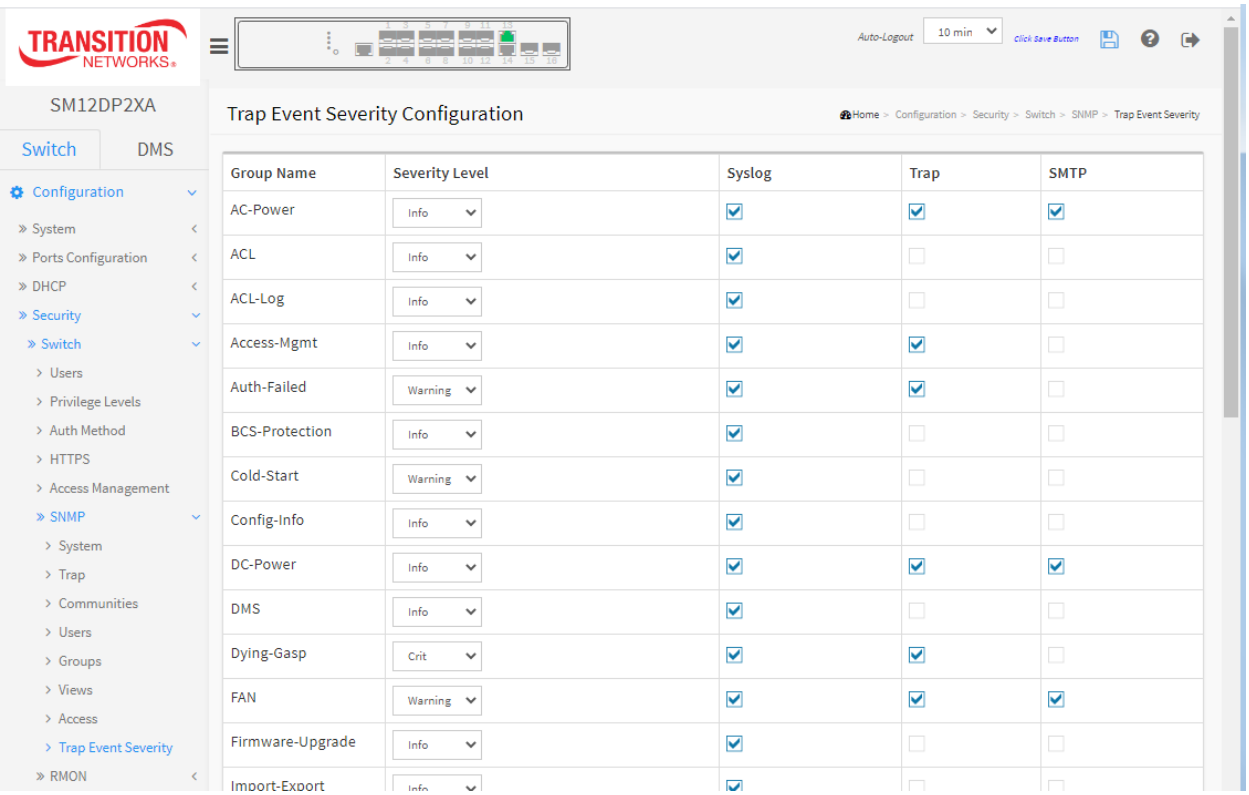
This page lets you view and configure current trap event severity levels and trap reporting methods (Syslog, Trap, SMTP) for the various user groups.

Web Interface

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

1. Click Configuration, Security, Switch, SNMP, Trap Event Severity.
2. For each Group Name select a Severity Level and check or uncheck the Syslog, Trap, and SMTP.
3. Click the Apply to save the settings.
4. To cancel the settings, click the Reset button to revert to previously saved values.

Figure 2-5.1.7.8: Trap Event Severity Configuration

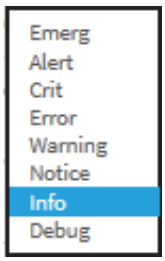


Parameter descriptions:

Group Name : The name identifying the severity group (e.g., ACL, Access-Mgmt, Auth-Failed, BCS-Protection, Cold-Start, Config-Info, DMS, Dying-Gasp, FAN).

Severity Level : Each group has a severity level. These levels are supported:

Emergency: System is unusable.
Alert: Action must be taken immediately.
Critical: Critical conditions.
Error: Error conditions.
Warning: Warning conditions.
Notice: Normal but significant conditions.
Information: Information messages.
Debug: Debug-level messages.



Syslog : 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 save changes.

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

2-5.1.8 RMON

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

2-5.1.8.1 Statistics

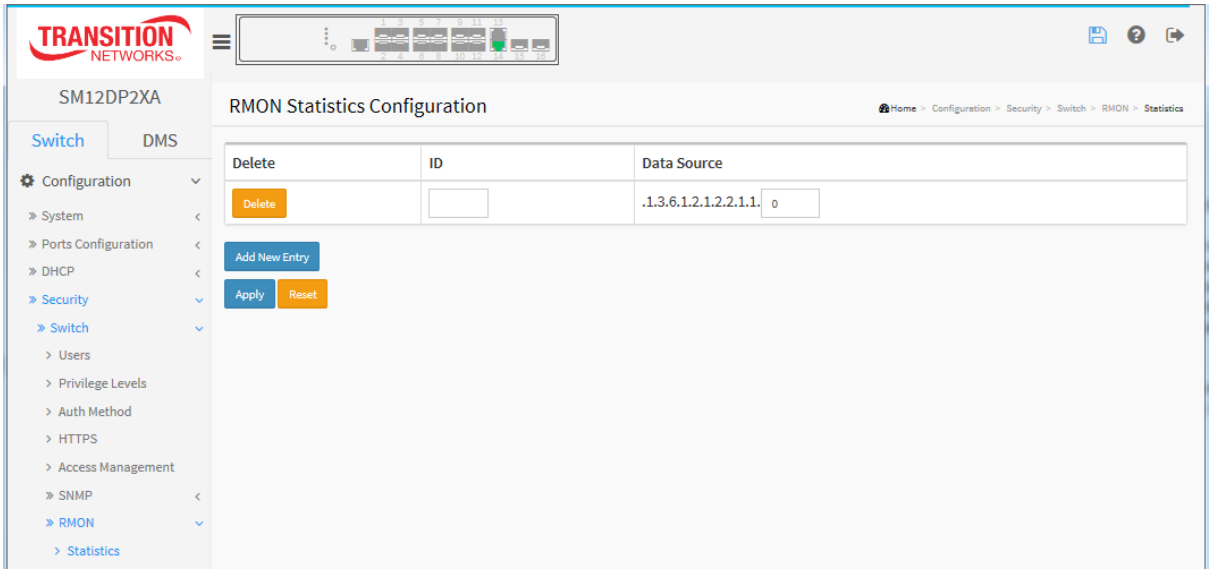
Configure RMON Statistics table on this page. The entry index key is **ID.**

Web Interface

To display the configure RMON configuration in the web interface:

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

Figure 2-5.1.8.1: RMON Statics Configuration



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

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

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

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

Buttons

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

Apply: Click to save changes.

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

2-5.1.8.2 History

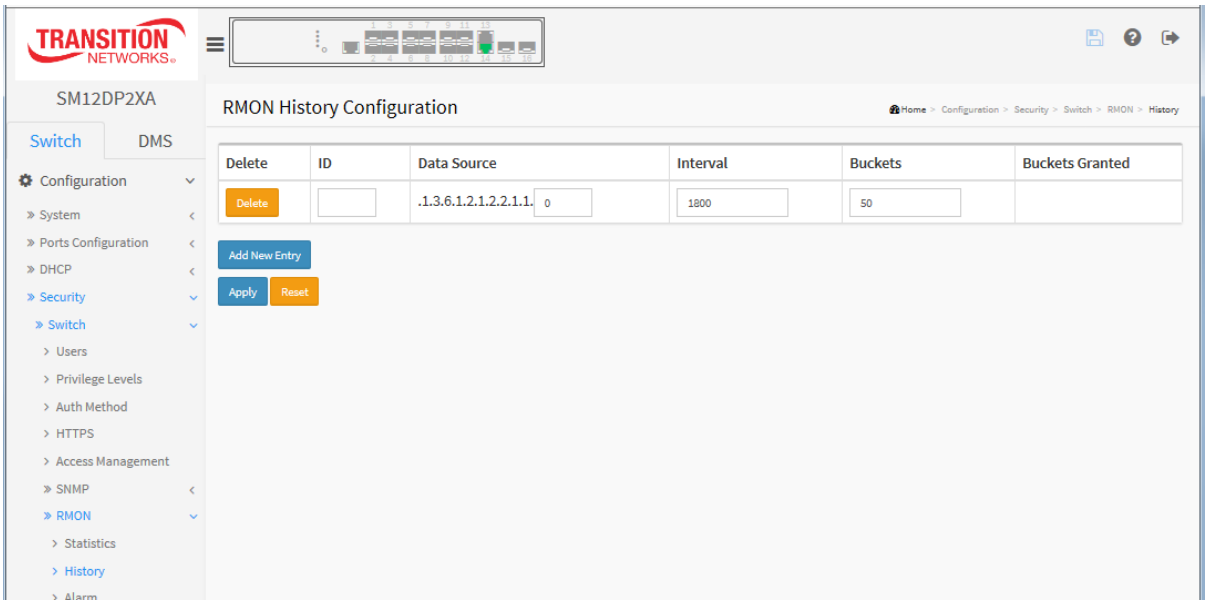
Configure the RMON History table on this page. The entry index key is **ID.**

Web Interface

To display the configure RMON History in the web interface:

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

Figure 2-5.1.8.2: RMON History Configuration



Parameter descriptions:

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

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

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

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

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

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

Buttons

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

Apply: Click to save changes.

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

2-5.1.8.3 Alarm

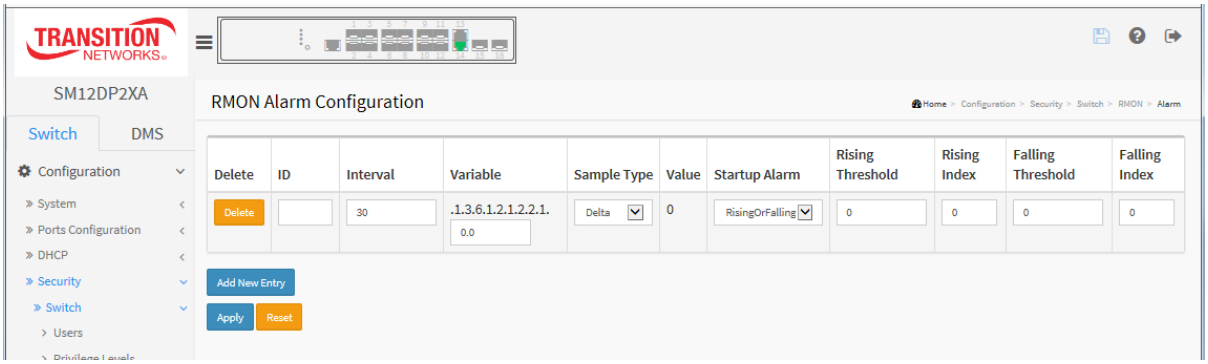
Configure the RMON Alarm table on this page. The entry index key is **ID.**

Web Interface

To display the configure RMON Alarm in the web interface:

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

Figure 2-5.1.8.3: RMON Alarm Configuration



Parameter descriptions:

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

ID : Indicates the index of the entry. The range is 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 alarm entry.

Apply: Click to save changes.

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

2-5.1.8.4 Event

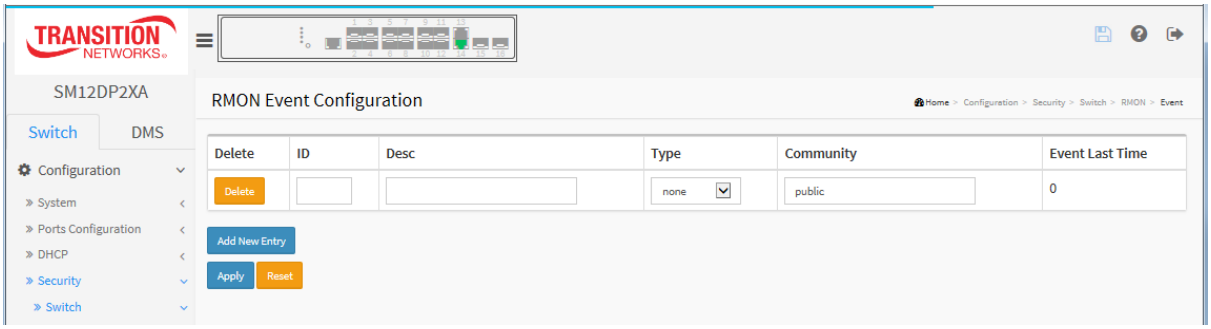
Configure RMON Event parameters on this page. The entry index key is **ID.**

Web Interface

To display the configure RMON Event in the web interface:

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

Figure 2-5.1.8.4: RMON Event Configuration



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

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

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

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

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

> ***none***: No SNMP log is created, no SNMP trap is sent.
>
> ***log***: Create SNMP log entry when the event is triggered.
>
> ***snmptrap***: Send SNMP trap when the event is triggered.
>
> ***logandtrap***: Create SNMP log entry and sent SNMP trap when the event is triggered.

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

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

Buttons

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

Apply: Click to save changes.

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

2-5.2 Network

2-5.2.1 Limit Control

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

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

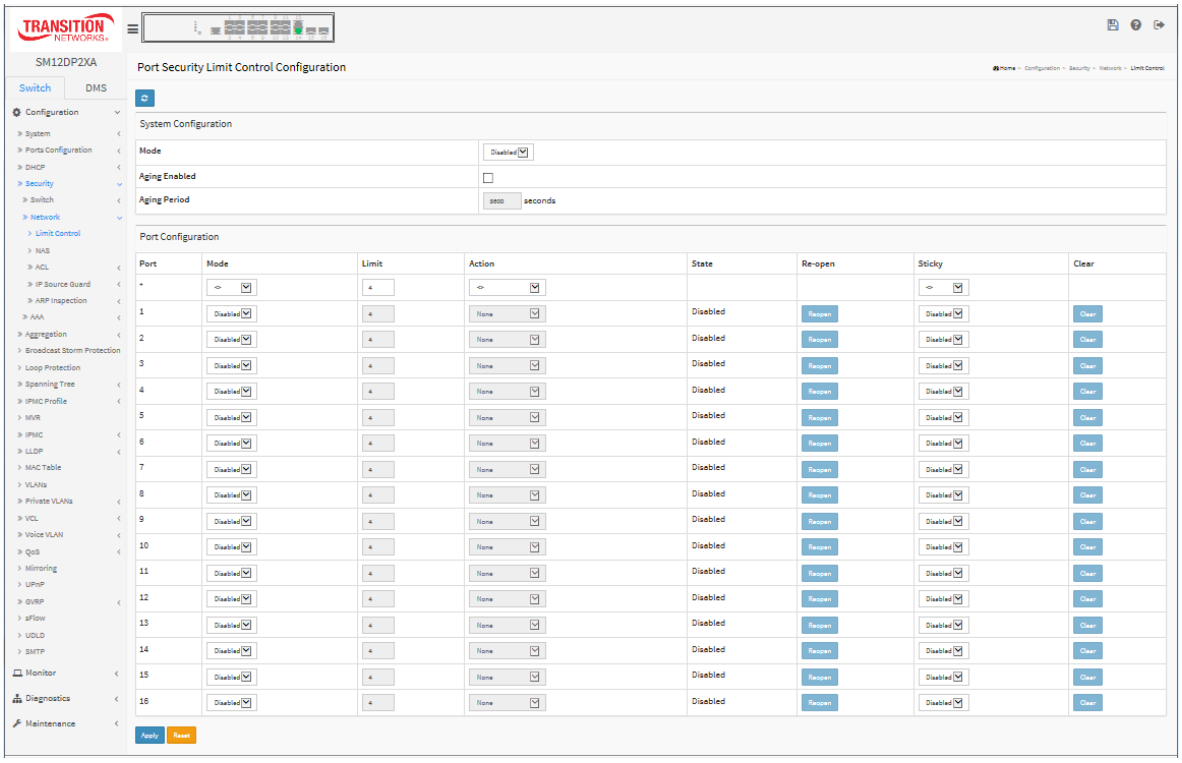
The Limit Control module utilizes a lower-layer module, Port Security module, which manages MAC addresses learned on the port.

Web Interface

To configure Limit Control via the web UI:

1. Navigate to Configuration > Security > Network > Limit Control.
2. In the System Configuration section, select “Enabled” in the Mode of System Configuration.
3. Check Aging Enabled.
4. Set the Aging Period (default is 3600 seconds).
5. In the Port Configuration section, select “Enabled” in the Mode of Port Configuration.
6. Specify the maximum number of MAC addresses in the Limit of Port Configuration.
7. Set the Action (Trap, Shutdown, or Trap & Shutdown).
8. At the Sticky dropdown, select Enable for the desired ports.
9. Click Apply.

Figure 2-5.2.1: Port Security Limit Control Configuration



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 a number between 10 and 10,000,000 seconds.

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

Port Configuration : The table has one row for each port on the switch and some columns, which are:

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

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

Limit : The maximum number of MAC addresses that can be secured on this port (1-1024). 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. There are three ways to re-open the port:

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

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

State : This column shows the current state of the port 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.

Sticky : If running config has a sticky MAC address, then these MAC addresses are automatically made to be static MAC address on the MAC Table. When you enable port security on a port it writes it to the MAC table. For example, when Port mode = Enable , Sticky mode = Enable, Action = shutdown:

- If the existing number of static MAC entries at the port = the configured limit quantity, the new learned MAC will cause the port to shut down.
- If the existing number of static MAC entry at the port < the configured limit quantity ,only the remaining number of limit can be added to the static MAC table.

To recover this sticky port, change Sticky mode to " Disable" and manually delete the static MAC entries at the port at MAC Address Table Configuration.

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

Buttons:

Refresh: You can click them for refresh the Port Security information manually.

Re-open : 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 that clicking the Re-open button causes the page to be refreshed, so non-committed changes will be lost.

Apply – Click to save changes.

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

2-5.2.2 NAS

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

This page lets you configure the IEEE 802.1X and MAC-based authentication system and port settings.

The IEEE 802.1X standard defines a port-based access control procedure that prevents unauthorized access to a network by requiring users to first submit credentials for authentication. One or more central servers, the backend servers, determine whether the user is allowed access to the network. These backend (RADIUS) servers are configured on the Configuration > Security > AAA page. The IEEE802.1X standard defines port-based operation.

MAC-based authentication allows for authentication of more than one user on the same port, and doesn't require the user to have special 802.1X supplicant software installed on his system. The switch uses the user's MAC address to authenticate against the backend server. Intruders can create counterfeit MAC addresses, which makes MAC-based authentication less secure than 802.1X authentication.

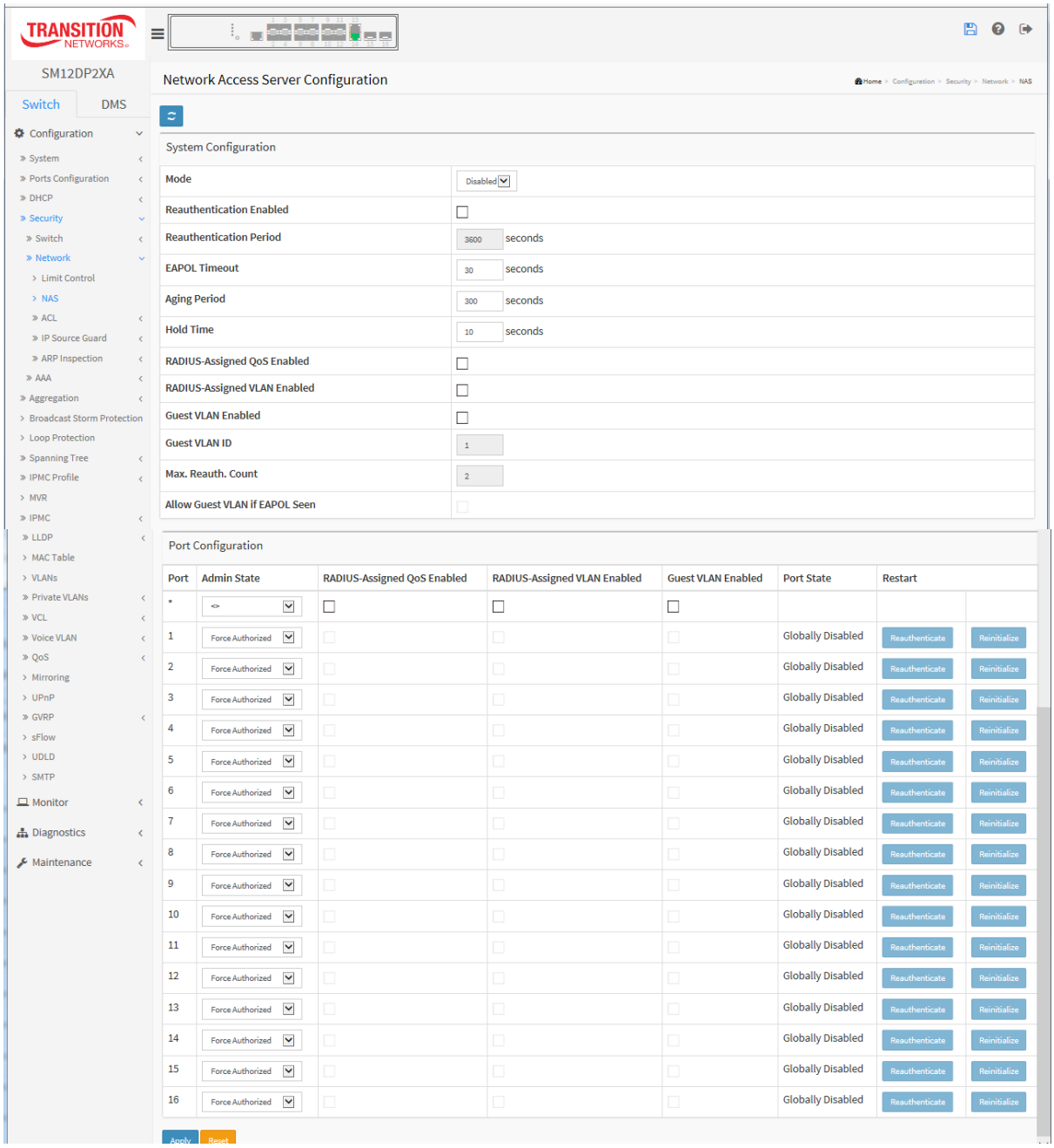
The NAS configuration consists of two sections, a system configuration and a port configuration.

Web Interface

To configure a Network Access Server in the web interface:

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

Figure 2-5.2.2: Network Access Server Configuration



System Configuration:

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

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

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

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

EAPOL Timeout : Determines the time for retransmission of Request Identity EAPOL frames. Valid values are in the range 1 to 255 seconds. This has no effect for MAC-based ports.

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

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

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

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

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

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

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

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

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

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

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

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

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

below for a detailed description).

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

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

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

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

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

Max. Reauth. Count : The number of times the switch transmits an EAPOL Request Identity frame without response before considering entering the Guest VLAN is adjusted with this setting. The value can only be changed if the Guest VLAN option is globally enabled.

Valid values are in the range [1; 255].

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

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

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

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

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

Force Authorized : In this mode, the switch will send one EAPOL Success frame when the port link comes up, and any client on the port will be allowed network access without authentication.
Note: The 802.1X Admin State must be set to Authorized for ports that are enabled for Spanning Tree or LACP.

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 but can be used by anyone. Also, only the MD5-Challenge method is supported. The maximum number of clients that can be attached to a port can be limited using the Port Security Limit Control functionality.

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

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

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

RADIUS attributes used in identifying a QoS Class:

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

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

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

RADIUS-Assigned VLAN Enabled : When RADIUS-Assigned VLAN is both globally enabled and enabled (checked) for a given port, the switch reacts to VLAN ID information carried in the RADIUS Access-Accept

packet transmitted by the RADIUS server when a supplicant is successfully authenticated. If present and valid, the port's Port VLAN ID will be changed to this VLAN ID, the port will be set to be a member of that VLAN ID, and the port will be forced into VLAN unaware mode. Once assigned, all traffic arriving on the port will be classified and switched on the RADIUS-assigned VLAN ID.

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

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

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

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

RADIUS attributes used in identifying a VLAN ID:

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

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

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

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

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

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

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

Once in the Guest VLAN, the port is considered authenticated, and all attached clients on the port are

allowed access on this VLAN. The switch will not transmit an EAPOL Success frame when entering the Guest VLAN.

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

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

Globally Disabled: NAS is globally disabled.

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

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

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

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

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

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

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

Buttons:

Apply – Click to save changes.

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

Refresh) Click to refresh the NAS Configuration manually.

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

Recovery: 1. Click the **Previous** button. 2. Either disable LACP or set 802.1X Admin State to Authorized for each port.

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. Either disable Spanning Tree or set 802.1X Admin State to Authorized for each port.

2-5.2.3 ACL

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

2-5.2.3.1 Ports

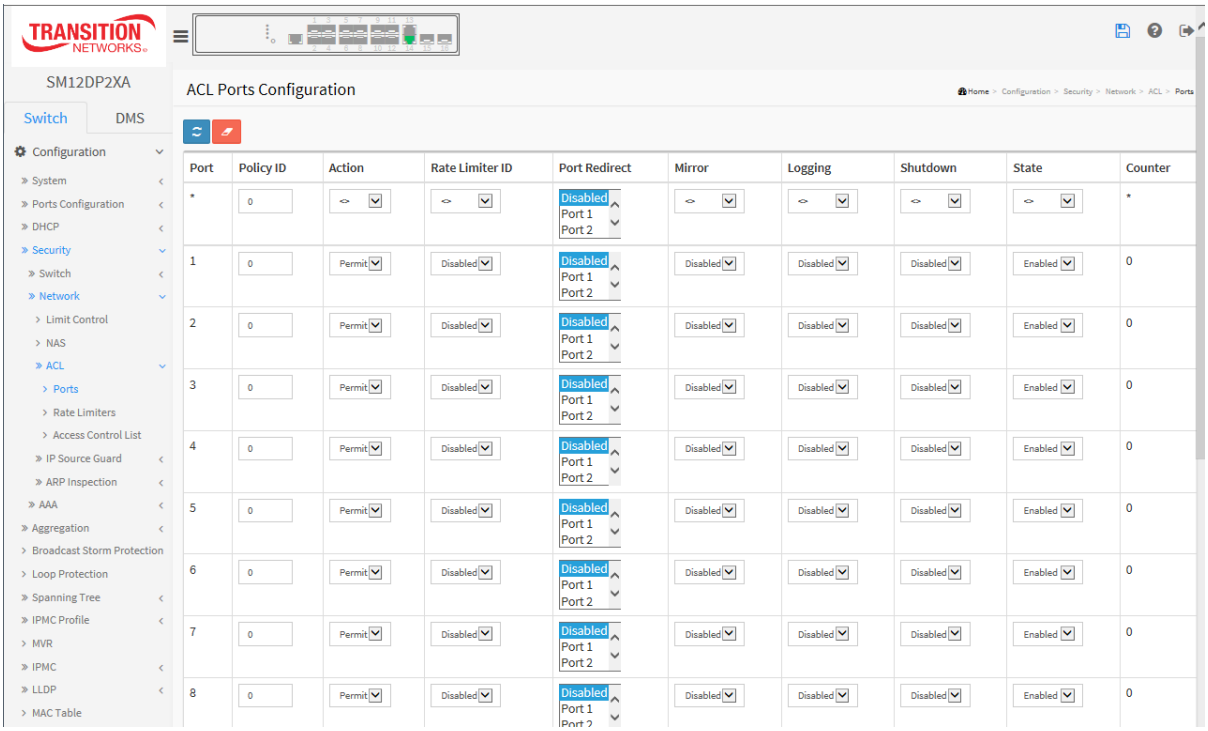
This page lets you configure the ACL parameters (ACE) of the each switch port. These parameters will affect frames received on a port unless the frame matches a specific ACE

Web Interface

To configure the ACL Ports Configuration in the web interface:

1. Click Configuration > Security > Network > ACL > Ports.
2. Set the parameter values as required for port ACL setting.
3. Click Apply to save the settings.
4. To cancel the settings, click the Reset button to revert to previously saved values.
5. After configuration is complete you can view the port Counters, click Refresh to update the counters, or click Clear to clear the information.

Figure 2-5.2.3.1: ACL Ports Configuration



Parameter descriptions:

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

Policy ID : Select the policy to apply to this port. Valid values are 1 through 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 through 16. The default value is "Disabled".

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

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

Enabled: Frames received on the port are mirrored.

Disabled: Frames received on the port are not mirrored.

The default value is "Disabled".

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

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

Disabled: Frames received on the port are not logged.

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

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

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

Disabled: Port shut down is disabled.

The default value is "Disabled".

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

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

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

The default value is "Enabled"

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

Buttons

Apply – Click to save changes.

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

Refresh: You can click to refresh the ACL Port Configuration page.

Clear : You can click to manually clear the ACL Port Configuration parameters.

2-5.2.3.2 Rate Limiters

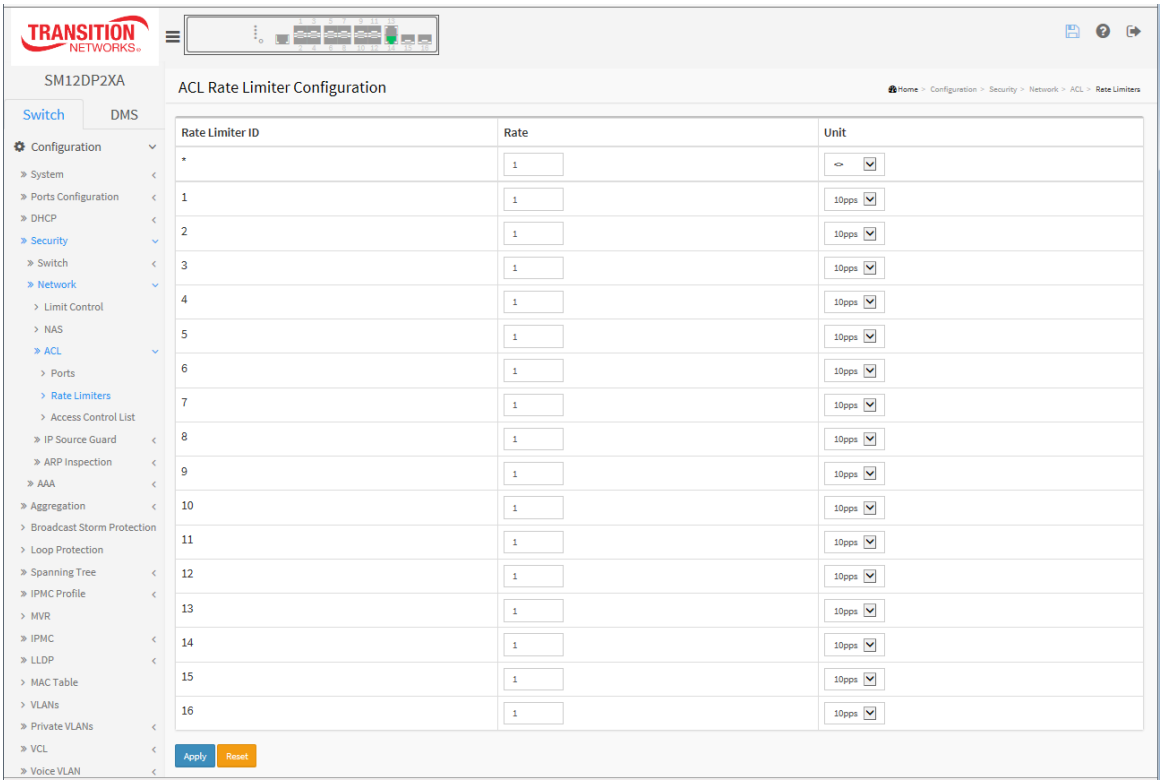
This page lets you configure the switch's ACL Rate Limiter parameters. The Rate Limiter table lets you set the rate limiter value and unit of measure.

Web Interface

To configure ACL Rate Limiter in the web interface:

1. Click Configuration, ACL, Rate Limiter.
2. For each Rate Limiter ID, specify the Rate and the Unit of measure.
3. Click Apply to save the settings.
4. To cancel the settings, click the Reset button to revert to previously saved values.

Figure 2-5.2.3.2: ACL Rate Limiter Configuration



Parameter descriptions:

Rate Limiter ID : The rate limiter ID for the settings contained in the same row and its range is 1 to 16.

Rate : Valid rates are 0, 1, 2, 3, ..., 500000 in 10pps or 0, 1, 2, 3, ..., 400000 in 25kbps.

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

10pps: 10 packets per second.

25kbps: 25 kbits per second.

Buttons

Apply – Click to save changes.

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

2-5.2.3.3 Access Control List

This page lets you configure Access Control List rule. An Access Control List (ACL) is a sequential list of permit or deny conditions that apply to IP addresses, MAC addresses, or other more specific criteria. This switch tests ingress packets against the conditions in an ACL one by one. A packet will be accepted as soon as it matches a permit rule or dropped as soon as it matches a deny rule.

If no rules match, the frame is accepted. Other actions can also be invoked when a matching packet is found, including rate limiting, copying matching packets to another port or to the system log, or shutting down a port.

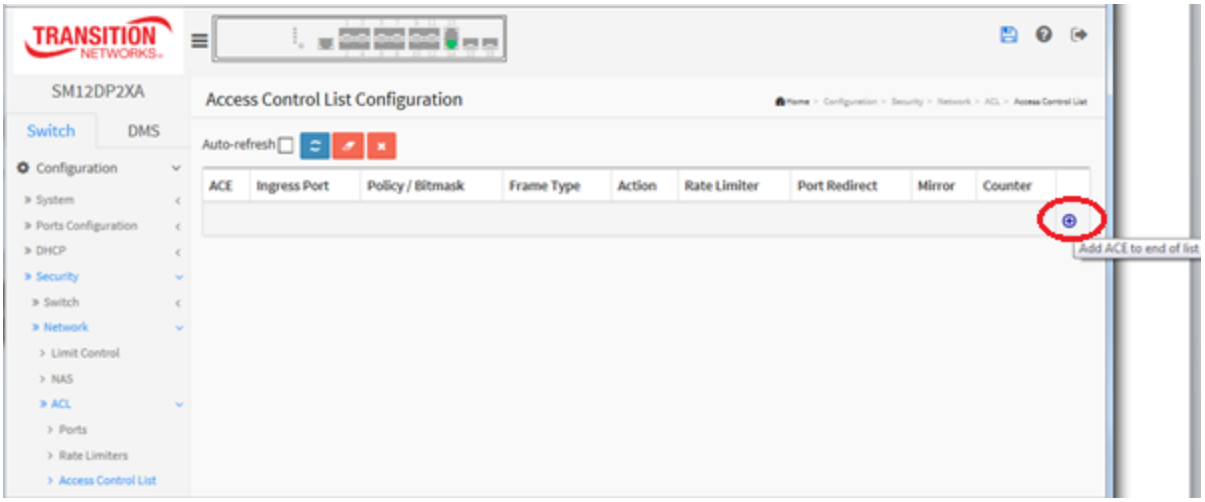
This page shows the Access Control List (ACL), which is made up of the ACEs (Access Control Entries) defined on this switch. Each row describes the ACE that is defined. The maximum number of ACEs is 512 on each switch. Click on the lowest plus sign to add a new ACE to the list. The reserved ACEs used for internal protocol, cannot be edited or deleted, the order sequence cannot be changed, and the priority is highest.

Web Interface

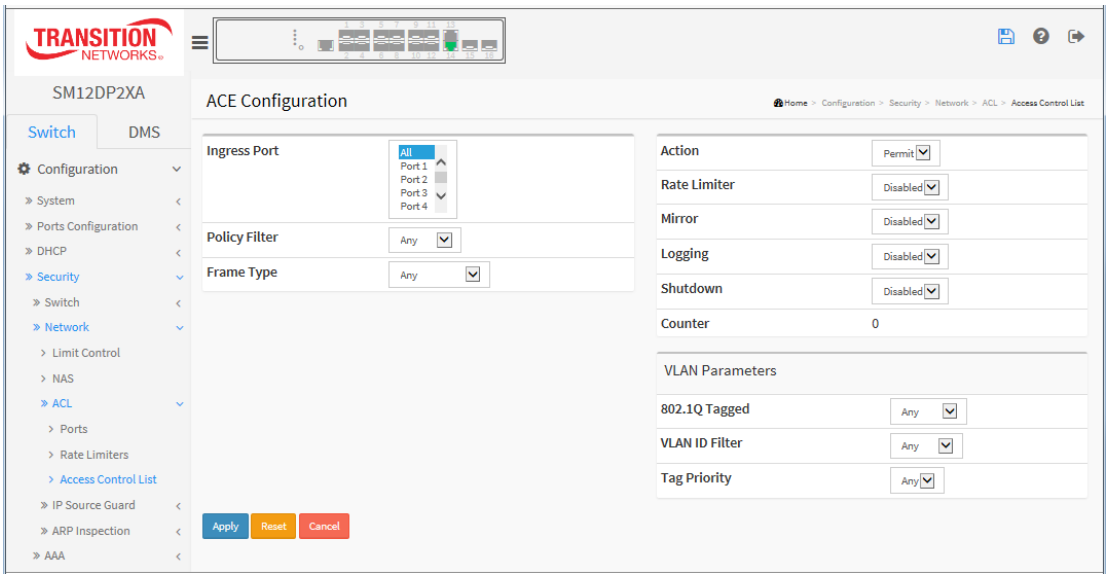
To configure Access Control List in the web interface:

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

Figure 2-5.2.3.3: Access Control List Configuration



When you click the button the ACE Configuration page displays.



Parameter descriptions:

Ingress Port : Select 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 : Indicates the policy number and bitmask of the ACE.

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

Any: The ACE will match any frame type.

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

ARP: The ACE will match ARP/RARP frames.

IPv4: The ACE will match all IPv4 frames.

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

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

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

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

IPv6: The ACE will match all IPv6 standard frames.

Action : Indicates the forwarding action of the ACE.

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

Deny: Frames matching the ACE are dropped.

Filter: Frames matching the ACE are filtered.

Filter Port : Select All ports or Port 1 – Port 16.

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

Port Copy : Indicates the port copy operation of the ACE. Frames matching the ACE are copied to the

port number. The allowed values are Disabled or a specific port number. When Disabled is displayed, the port copy operation is disabled.

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

Enabled: Frames received on the port are mirrored.

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

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

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

Disabled: Frames matching the ACE are not logged.

Note that the System Log memory size and logging rate are limited.

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

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

Disabled: Port shut down is disabled for the ACE.

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

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

: Insert a new ACE before the current row.

: Edit the ACE row.

: Move the ACE up the list.

: Move the ACE down the list.

: Delete 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.

IP Parameters:

IP Protocol Filter: Select Any, ICMP, UDP, TCP, or Specific.

IP TTL : Select Any, Non-zero, or Zero.

IP Fragment : Select Any, Yes, or No.

IP Option: Select Any, Yes, or No.

SIP Filter : Select Any, Host, or Network.

DIP Filter : Select Any, Host, or Network.

VLAN Parameters:

802.1Q Tagged : Select Any, Disabled, or Enabled.

VLAN ID Filter : Select Any or Specific.

VLAN ID : Enter a valid VLAN ID (if "VLAN ID Filter" was set to "Specific")

Tag Priority : Select tag priority 0, 1, 2, 3, 4, 5, 6, 7, 0-1, 2-3, 4-5, 6-7, 0-3, 4-7, or Any.

ARP Parameters:

ARP/RARP : Select Any, ARP, RARP, or Other.

Request/Reply : Select Any, Request, or Reply.

Sender IP Filter : Select Any, Host, or Network.

Target IP Filter : Select Any, Host, or Network.

Target IP Address : Enter the IP address of the target.

Sender IP Address : Enter the IP address of the sender.

Sender IP Mask : Enter the IP mask of the Sender (e.g., 255.255.255.0).

Target IP Filter : Select Any, Host, or Network.

ARP Sender MAC Match : Select Any, 0, or 1.

RARP Target MAC Match : Select Any, 0, or 1.

IP/Ethernet Length : Select Any, 0, or 1.

IP : Select Any, 0, or 1.

Ethernet : Select Any, 0, or 1.

IPv6 Parameters:

Next Header Filter : Select Any, ICMP, UDP, TCP, or Specific.

Next Header Value : Enter a value for the next header (e.g., 255).

SIP Filter : Select Any or Specific.

SIP Address (32 bits) : Enter after the "::" prefix.

SIP Bitmask (32 bits) : Enter after the "0x" prefix.

Hop Limit : Select Any, 0, or 1.

ICMPv6 Parameters:

ICMP Type Filter : Select Any or Specific.

ICMP Code Filter : Select Any or Specific.

UDPv6 Parameters:

Source Port Filter : Select Any, Specific, or Range.

Dest. Port Filter : Select Any, Specific, or Range.

TCPv6 Parameters:

Source Port Filter : Select Any, Specific, or Range.

Dest. Port Filter : Select Any, Specific, or Range.

TCP FIN : Select Any, 0, or 1.

TCP SYN : Select Any, 0, or 1.

TCP RST : Select Any, 0, or 1.

TCP PSH : Select Any, 0, or 1.

TCP ACK : Select Any, 0, or 1.

TCP URG : Select Any, 0, or 1.

Buttons:

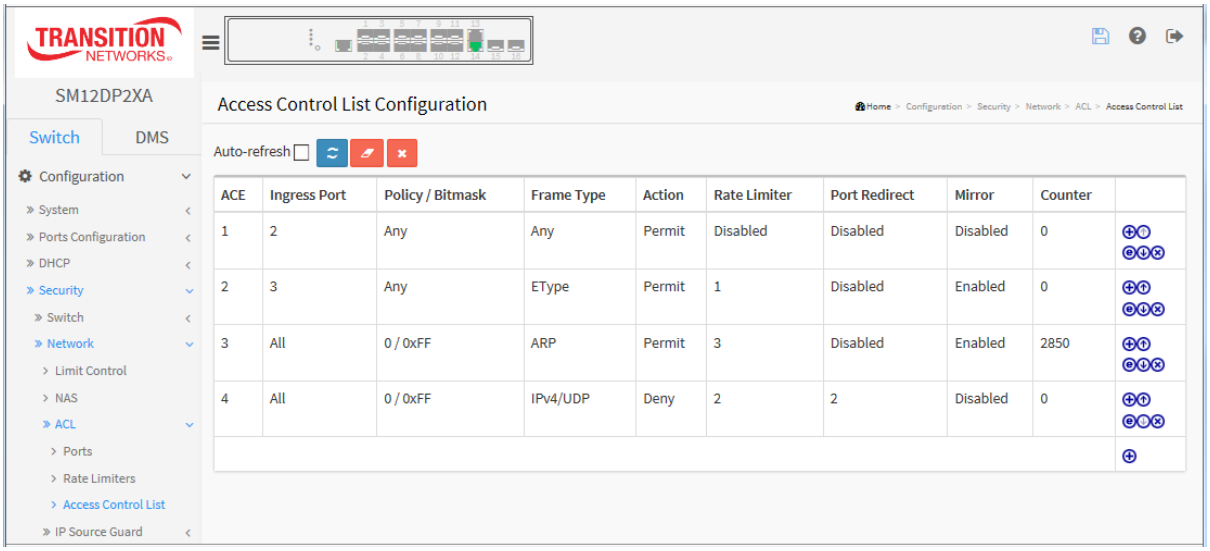
Apply – Click to save changes.

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

Auto-refresh: Check to automatically refresh the information every 3 minutes.

Access Control List Configuration Example

The sample ACL page below shows four ACEs configured with various Ingress Port, Policy / Bitmask, Frame Type, Action, Rate Limiter, Port Redirect, Mirror, and Counter settings.



2-5.2.4 IP Source Guard

This page lets you configure IP Source Guard detail parameters. You can use the IP Source Guard configure to enable or disable the switch port.

2-5.2.4.1 Configuration

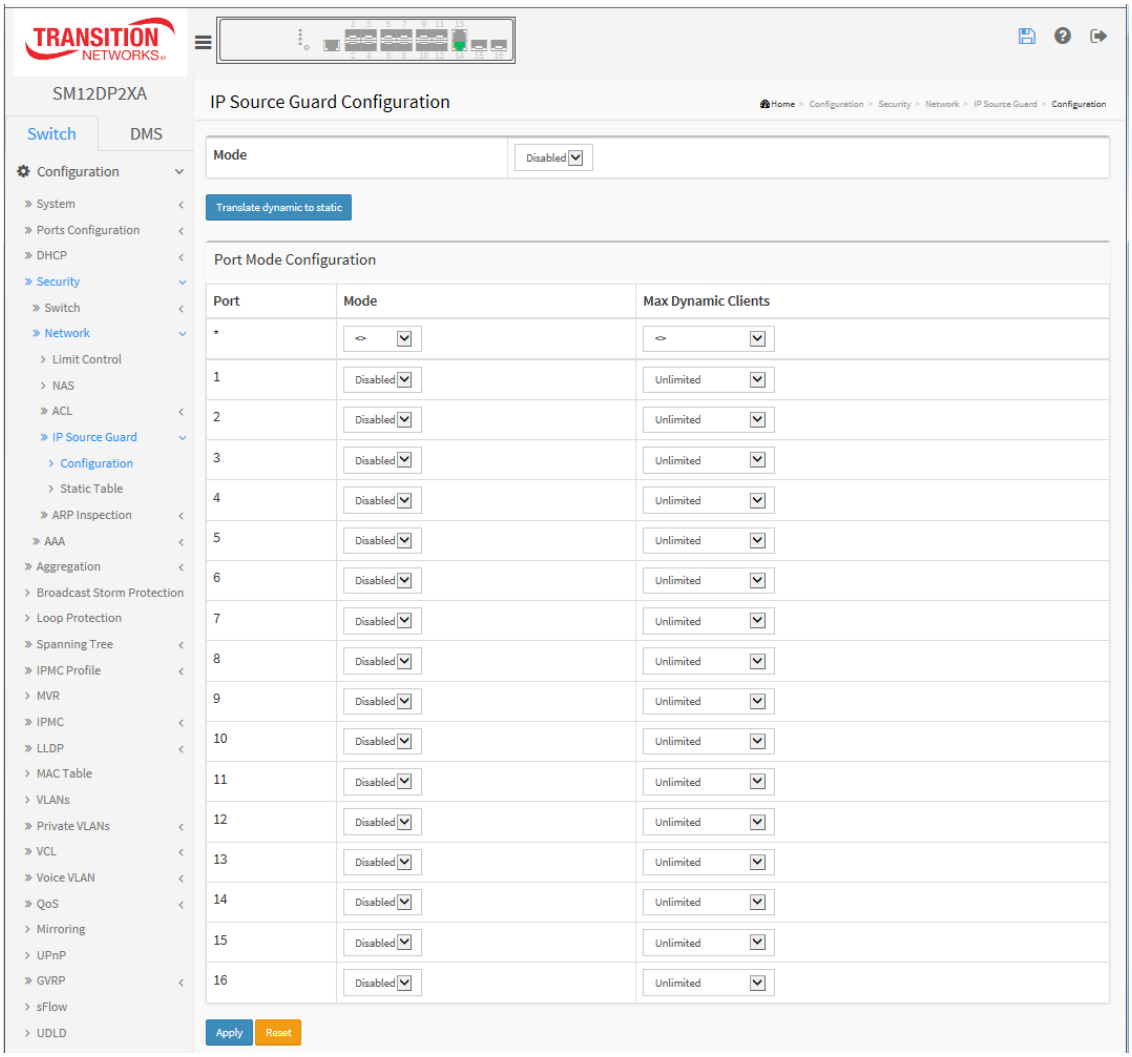
This page lets you configure IP Source Guard setting including Mode (Enabled or Disabled) and Maximum Dynamic Clients (0, 1, 2, or Unlimited).

Web Interface

To configure IP Source Guard in the web interface:

1. Navigate to Configuration > Security > Network > IP Source Guard > Configuration.
2. Select “Enabled” in the Mode of IP Source Guard Configuration.
3. Select “Enabled” of the specific port in the Mode of Port Mode Configuration.
4. Select Maximum Dynamic Clients (0, 1, 2, Unlimited) of the specific port at Mode of Port Mode Configuration.
5. Click Apply.

Figure 2-5.2.4. 1: IP Source Guard Configuration



Parameter descriptions:

Mode of IP Source Guard Configuration : Enable the Global IP Source Guard or disable the Global IP Source Guard. All configured ACEs will be lost when the mode is enabled.

Port Mode Configuration : Specify IP Source Guard is enabled on which ports. Only when both Global Mode and Port Mode on a given port are enabled, IP Source Guard is enabled on this given port.

Max Dynamic Clients : Specify the maximum number of dynamic clients that can be learned on given port. This value can be 0, 1, 2 or unlimited. If the port mode is enabled and the value of max dynamic client is equal to 0, it means only allow the IP packets forwarding that are matched in static entries on the specific port.

Buttons

Apply: Click to save changes.

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

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

2-5.2.4.2 Static Table

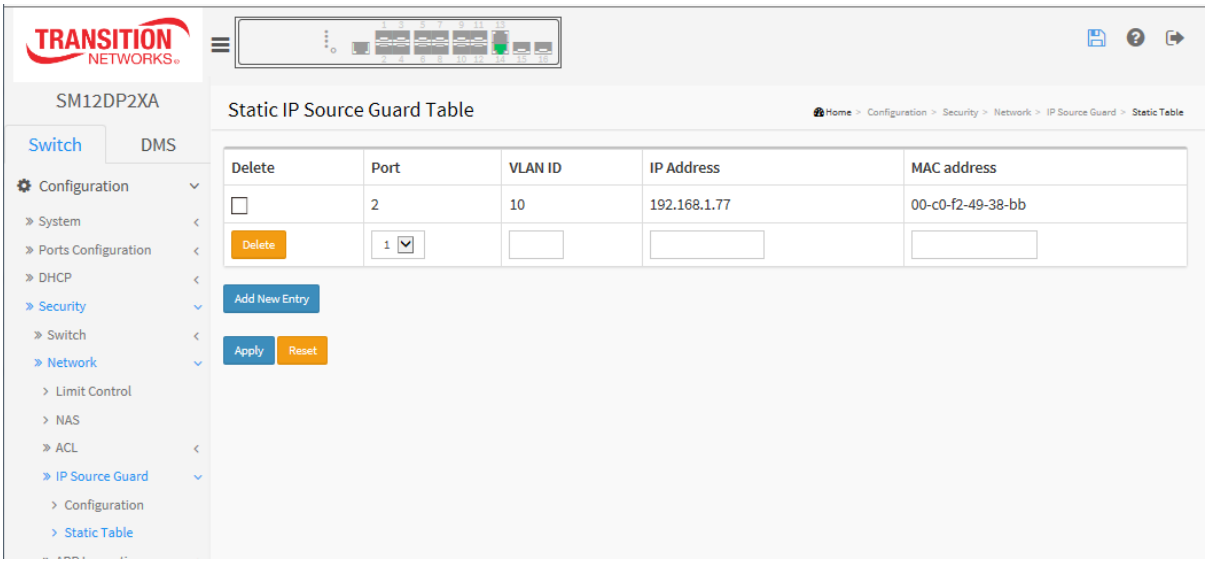
This page lets you configure switch Static IP Source Guard Table parameters.

Web Interface

To configure a Static IP Source Guard Table Configuration in the web interface:

1. Navigate to Configuration > Security > Network > IP Source Guard > Static Table.
2. Click “Add New Entry”.
3. Specify the Port, VLAN ID, IP Address, and MAC address of the entry.
4. Click Apply.

Figure 2-5.2.5.2: Static IP Source Guard Table



Parameter descriptions:

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

Port : The logical port for the settings.

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

IP Address : Allowed Source IP address.

MAC address : Allowed Source MAC address.

Buttons:

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

Apply – Click to save changes.

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

2-5.2.5 ARP Inspection

This page lets you configure the ARP Inspection parameters of the switch.

2-5.2.5.1 Configuration

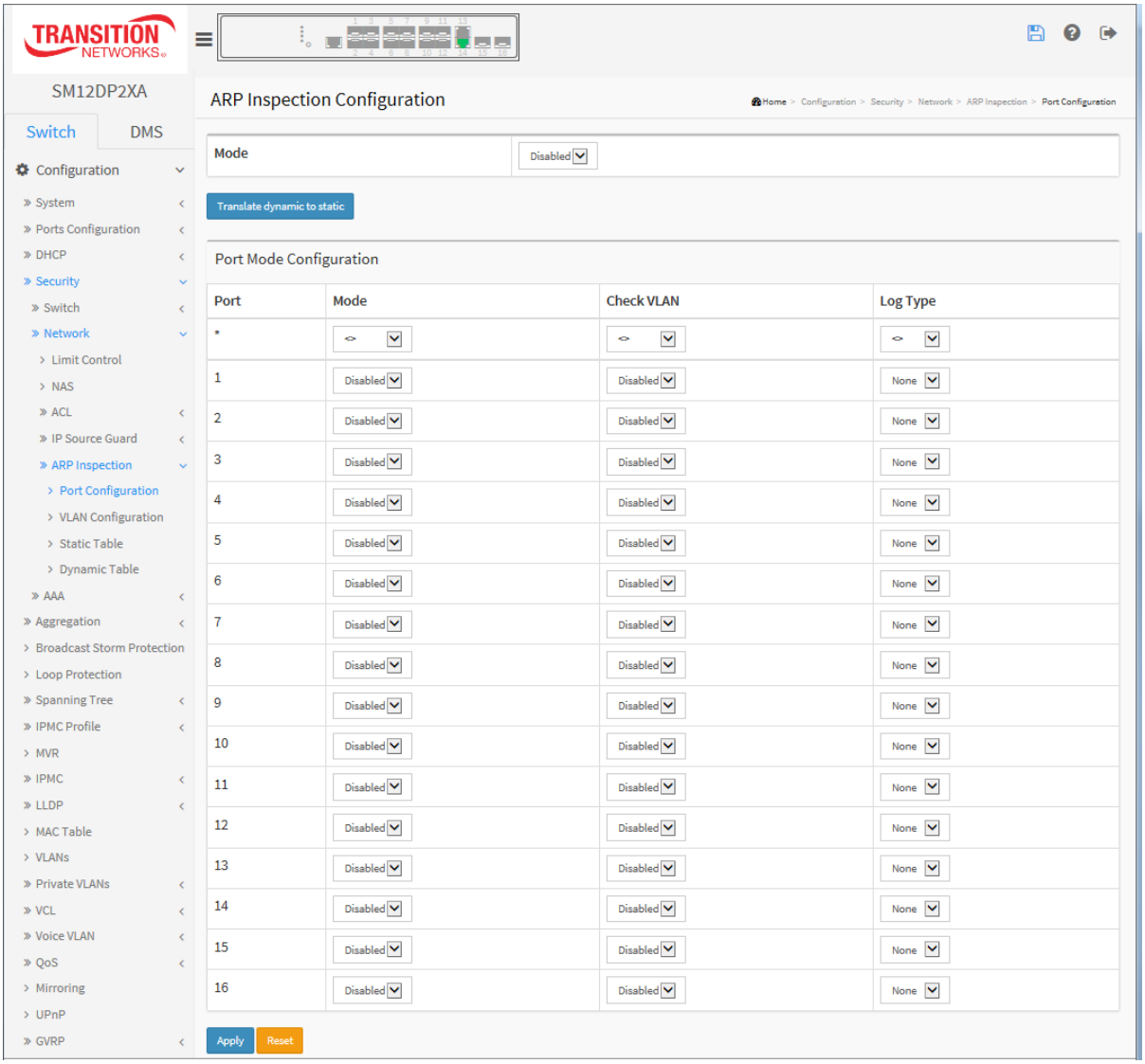
This page lets you configure ARP Inspection setting including Mode (Enabled and Disabled) and Port (Enabled and Disabled).

Web Interface

To configure an ARP Inspection Configuration in the web interface:

1. Navigate to Configuration > Security > Network > ARP Inspection > Port Configuration.
2. Select “Enabled” in the Mode of ARP Inspection Configuration.
3. Select “Enabled” of the specific port in the Mode of Port Mode Configuration.
4. Click Apply.

Figure 2-5.2.5.1: ARP Inspection Configuration



Parameter descriptions:

Mode of ARP Inspection Configuration : Enable or disable Global ARP Inspection.

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

Mode: Possible modes are:

Enabled: Enable ARP Inspection operation.

Disabled: Disable ARP Inspection operation.

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

Enabled: Enable check VLAN operation.
Disabled: Disable check VLAN operation.

Only the Global Mode and Port Mode on a given port are enabled, and the setting of "Check VLAN" is disabled, the log type of ARP Inspection will refer to the port setting. There are four log types and possible types are:

None: Log nothing.

Deny: Log denied entries.

Permit: Log permitted entries.

ALL: Log all entries.

Buttons:

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

Apply – Click to save changes.

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

2-5.2.5.2 VLAN Mode Configuration

This page provides ARP Inspection related configuration.

ARP Inspection is a secure feature. Several types of attacks can be launched against a host or devices connected to Layer 2 networks by "poisoning" the ARP caches. This feature is used to block such attacks. Only valid ARP requests and responses can go through the switch device.

Each page shows up to 9999 entries from the VLAN table (default is 20) selected with the "entries per page" input field. When first visited, the web page shows the first 20 entries from the beginning of the VLAN Table. The first displayed will be the one with the lowest VLAN ID found in the VLAN Table.

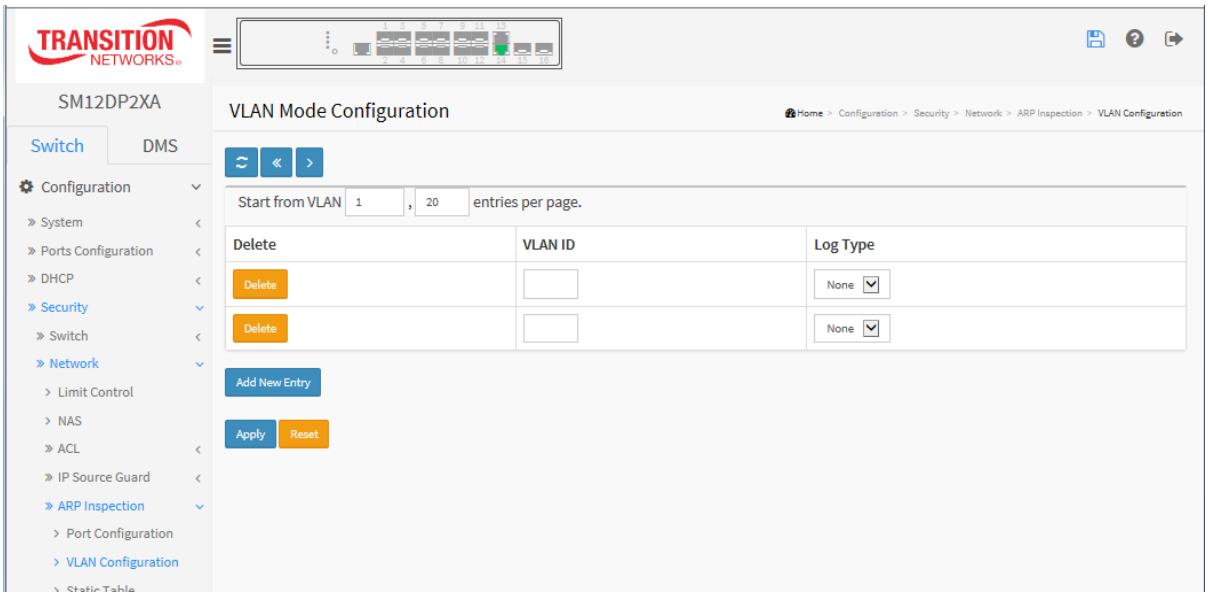
The "VLAN" input fields let you select the starting point in the VLAN Table. Clicking the **Refresh** button will update the displayed table starting from that or the closest next VLAN Table match. Clicking the **>** button will use the next entry of the currently displayed VLAN entry as the basis for the next lookup. When the end is reached the warning message is shown in the displayed table.
Use the **<<** button to start over.

Web Interface

To configure a VLAN Mode Configuration in the web interface:

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

Figure 2-5.2.5.2: VLAN Mode Configuration



Parameter descriptions:

<u>VLAN Mode Configuration</u>

VLAN ID : Specify on which VLANs ARP Inspection is enabled. First, you must enable the port setting on the Port mode configuration web page. Only when <u>both</u> Global Mode and Port Mode on a given port are enabled, ARP Inspection is enabled on this given port. Second, in the **VLAN ID** fields, specify which VLANs will be inspected on the VLAN mode configuration web page.

Log Type can be configured per VLAN setting. Possible types are:

None: Log nothing.

Deny: Log denied entries.

Permit: Log permitted entries.

ALL: Log all entries.

Buttons

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

Apply: Click to save changes.

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

2-5.2.5.3 Static Table

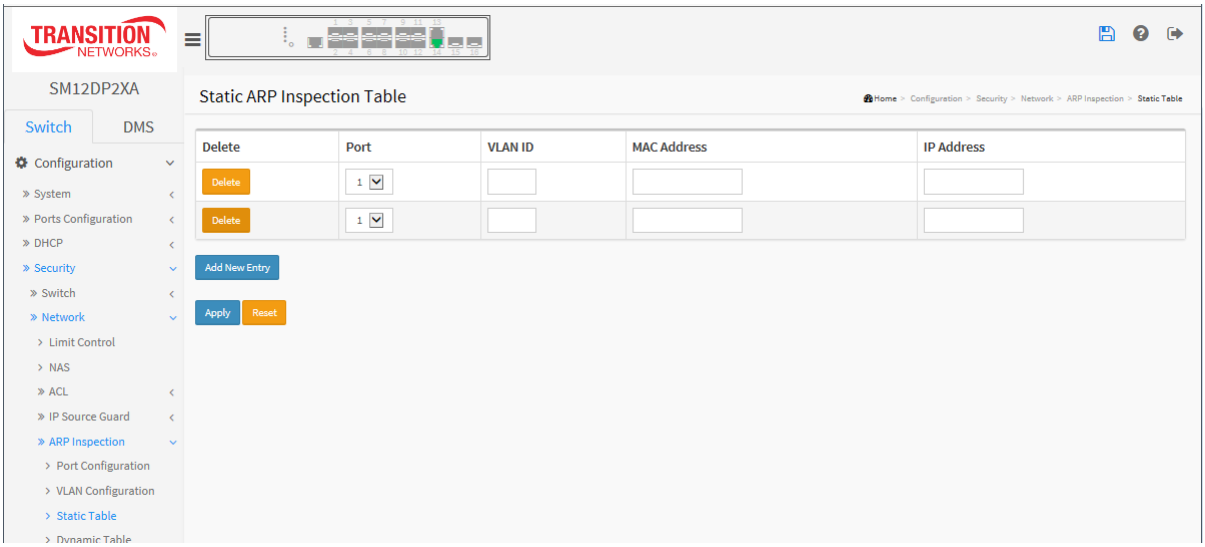
This page lets you configure the Static ARP Inspection Table parameters of the switch. You can use the Static ARP Inspection Table to manage the ARP entries.

Web Interface

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

1. Navigate to Configuration > Security > Network > ARP Inspection > Static Table.
2. Click “Add New Entry”.
3. Specify the Port, VLAN ID, IP Address, and MAC address in the entry.
4. Click Apply.

Figure 2-5.2.5.3: Static ARP Inspection Table



Parameter descriptions:

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

Port : The logical port for the settings.

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

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

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

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.

Apply – Click to save changes.

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

2-5.2.5.4 Dynamic Table

Entries in the Dynamic ARP Inspection Table are shown on this page. The Dynamic ARP Inspection Table contains up to 1024 entries, and is sorted first by port, then by VLAN ID, then by MAC address, and then by IP address.

Each page shows up to 99 entries from the Dynamic ARP Inspection table, default being 20, selected through the "entries per page" input field. When first visited, the web page will show the first 20 entries from the beginning of the Dynamic ARP Inspection Table.

The "Start from port address", "VLAN", "MAC address" and "IP address" input fields 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.

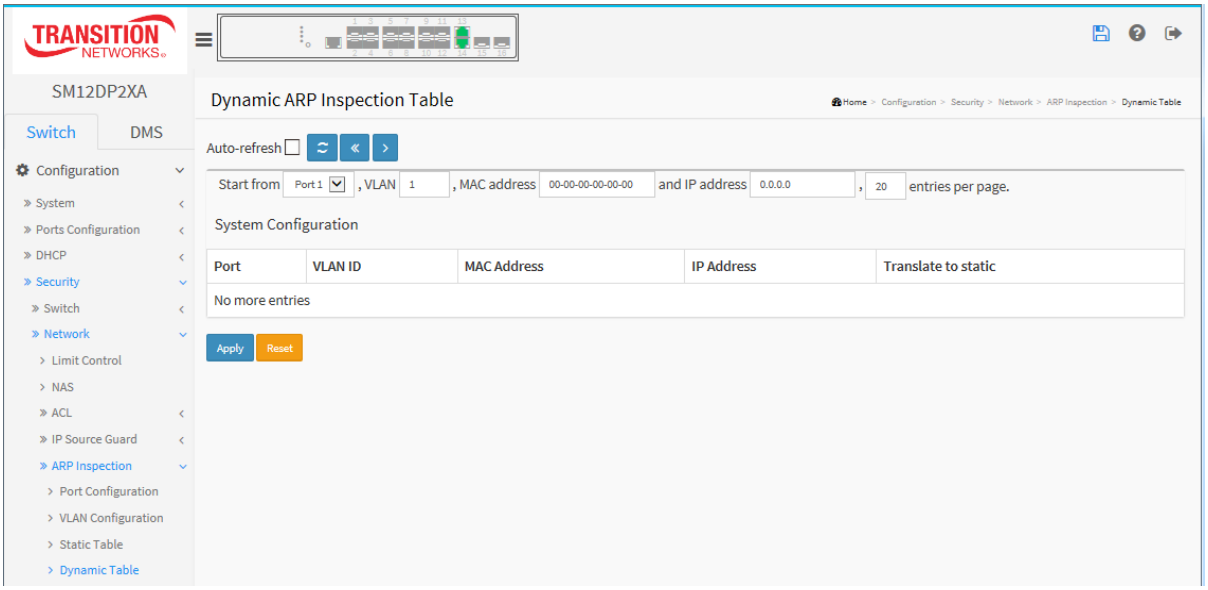
The << button will use the last entry of the currently displayed table as the basis for the next lookup. When the end is reached the text "*No more entries*" is shown in the displayed table. Use the > button to start over.

Web Interface

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

1. Navigate to Configuration > Security > Network > ARP Inspection > Dynamic Table.
2. Select the Start from port, VLAN, MAC address, IP address, and entries per page.
3. Click the Apply button.
4. View the table entries. If no entries are found, the message "*No more entries*" displays.

Figure 2-5.2.5.4: Dynamic ARP Inspection Table



Parameter descriptions:

ARP Inspection Table Columns

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

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

MAC Address : User MAC address of the entry.

IP Address : User IP address of the entry.

Buttons:

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.

Apply: Click to save changes.

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

2-5.3 AAA

This page lets you 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.

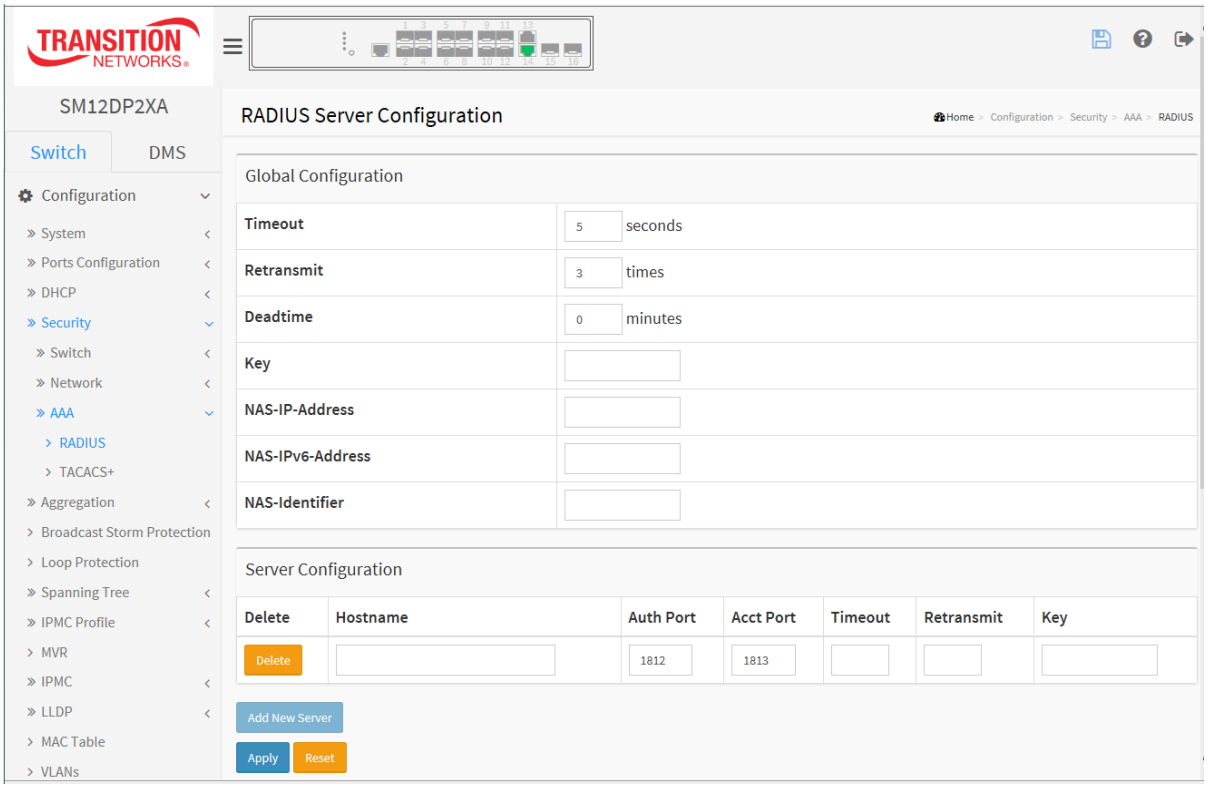
2-5.3.1 RADIUS

Web Interface

To configure a Common Configuration of AAA, RADIUS in the web interface:

1. Navigate to Configuration > Security > AAA > RADIUS.
2. Enter the Global Configuration parameters.
3. Click the Add New Server button.
4. Enter the Server Configuration parameters and click Apply.

Figure 2-5.3.1: RADIUS Authentication Server Configuration



Parameter descriptions:

Global Configuration : 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, which can be set to a number between 0 to 1440 minutes, is the period during which the switch will not send new requests to a server that has failed to respond to a previous request. This will stop the switch from continually trying to contact a server that it has already determined as

dead. Setting the Deadtime to a value greater than 0 (zero) will enable this feature, but only if more than one server has been configured.

Key : The secret key - up to 63 characters long - shared between the RADIUS server and the switch.

NAS-IP-Address (Attribute 4) : The IPv4 address to be used as attribute 4 in RADIUS Access-Request packets. If this field is left blank, the IP address of the outgoing interface is used.

NAS-IPv6-Address (Attribute 95) : The IPv6 address to be used as attribute 95 in RADIUS Access-Request packets. If this field is left blank, the IP address of the outgoing interface is used.

NAS-Identifier (Attribute 32) : The identifier - up to 255 characters long - to be used as attribute 32 in RADIUS Access-Request packets. If this field is left blank, the NAS-Identifier is not included in the packet.

Server Configuration : The table has one row for each RADIUS server and a number of columns, which are:

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

Hostname : The IP address or hostname of the RADIUS server.

Auth Port : The UDP port to use on the RADIUS server for authentication.

Acct Port : The UDP port to use on the RADIUS server for accounting.

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

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

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

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 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.

2-5.3.2 TACACS+

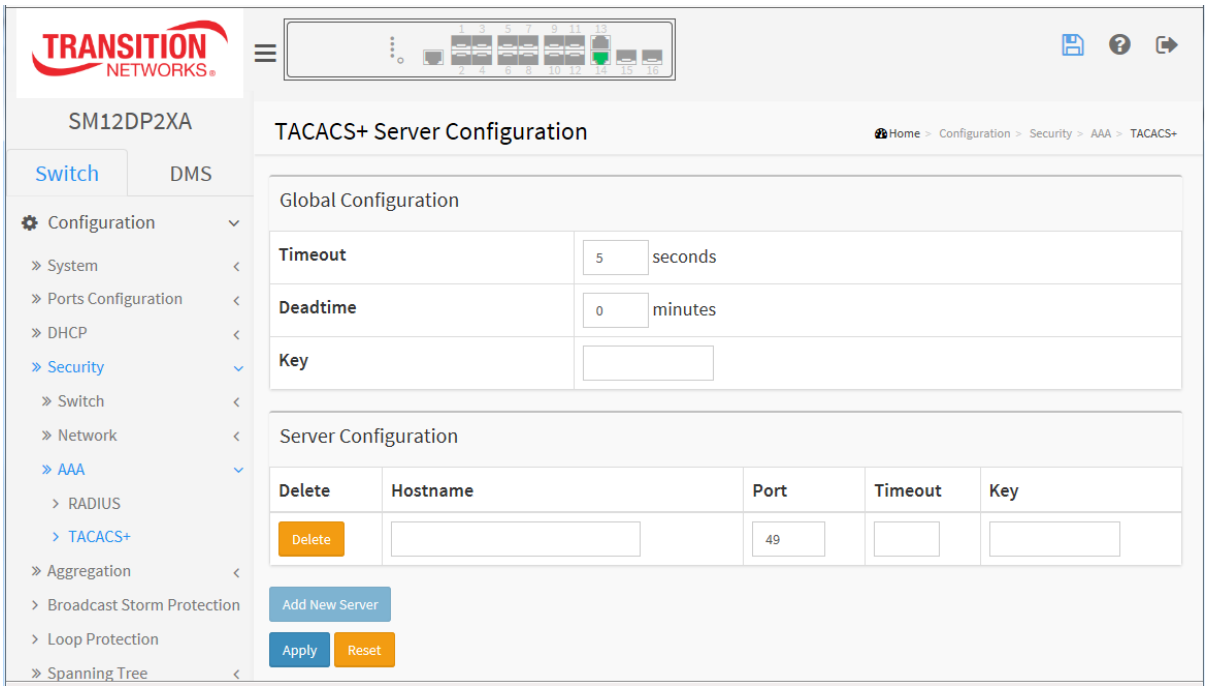
TACACS+ (Terminal Access Controller Access Control System Plus) is a networking protocol which provides access control for routers, network access servers and other networked computing devices via one or more centralized servers. TACACS+ provides separate authentication, authorization and accounting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

Web Interface

To configure a Common Configuration of AAA, TACACS+ in the web interface:

1. Navigate to Configuration > Security > AAA > TACACS+.
2. Enter the Global Configuration parameters.
3. Click the Add New Server button.
4. Enter the Server Configuration parameters.

Figure 2-5.3.2: TACACS+ Authentication Server Configuration



Parameter descriptions:

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

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

Deadtime : 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. Valid values are 0 - 1440 minutes. Setting 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 shared between the TACACS+ server and the switch (up to 63 characters).

Server Configuration : The table has one row for each TACACS+ server and a number of columns, which are:

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

Port : The TCP port to use on the TACACS+ server for authentication; the default is commonly-used port 49.

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.

2-6 Aggregation

Aggregation is used to configure the settings of Link Aggregation. You can bundle more than one port with the same speed, full duplex and the same MAC to be a single logical port, thus the logical port aggregates the bandwidth of these ports. This means you can apply your current Ethernet equipment's to build the bandwidth aggregation. For example, if there are three Fast Ethernet ports aggregated in a logical port, then this logical port has bandwidth three times as high as a single Fast Ethernet port has.

2-6.1 Static

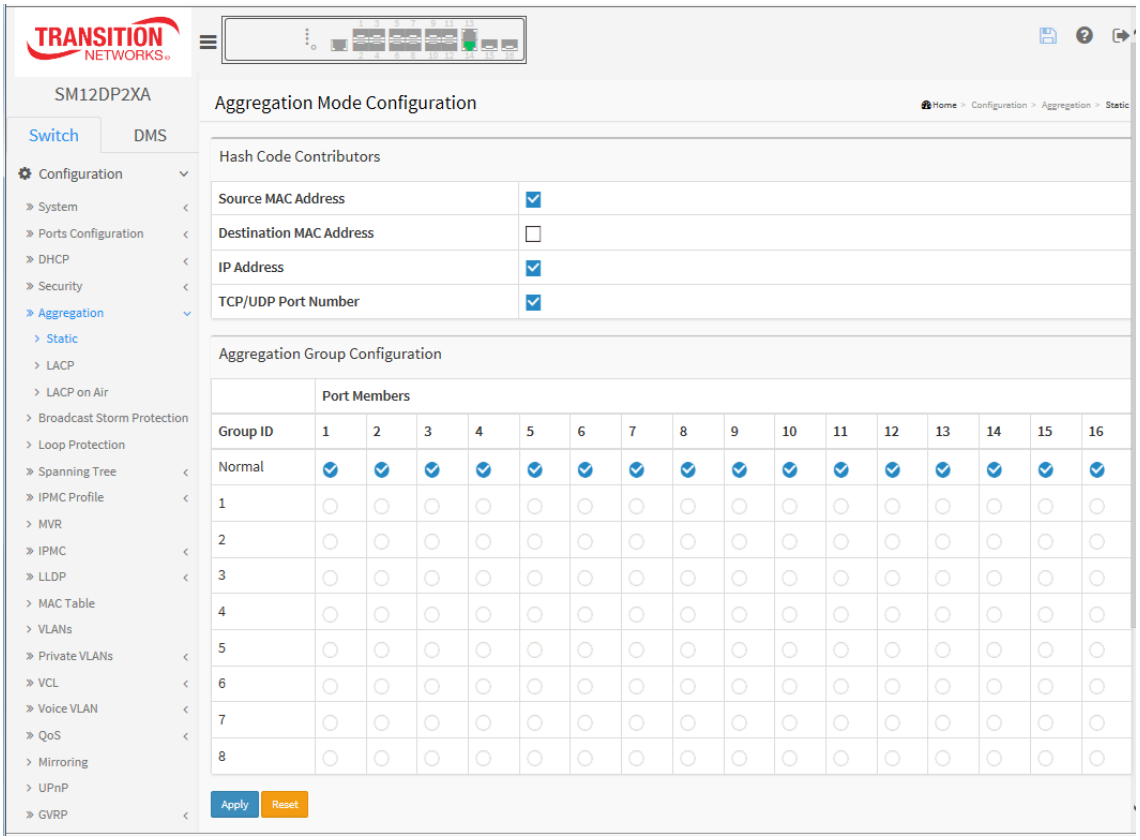
Ports using Static Trunk as their trunk method can choose their unique Static Group ID to form a logic "trunked port". The benefit of using Static Trunk method is that a port can immediately become a member of a trunk group without any handshaking with its peer port. This is also a disadvantage because the peer ports of your static trunk group may not know that they should be aggregate together to form a "logic trunked port". Using Static Trunk on both end of a link is strongly recommended. Please also note that low speed links will stay in "not ready" state when using static trunk to aggregate with high speed links.

Web Interface

To configure the Trunk Aggregation Hash mode and Aggregation Group in the web interface:

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

Figure 2-6.1: Aggregation Mode Configuration



Parameter descriptions:

Hash Code Contributors

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

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

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

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

Aggregation Group Configuration

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

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

Buttons

Apply – Click to save changes.

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

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

2-6.2 LACP

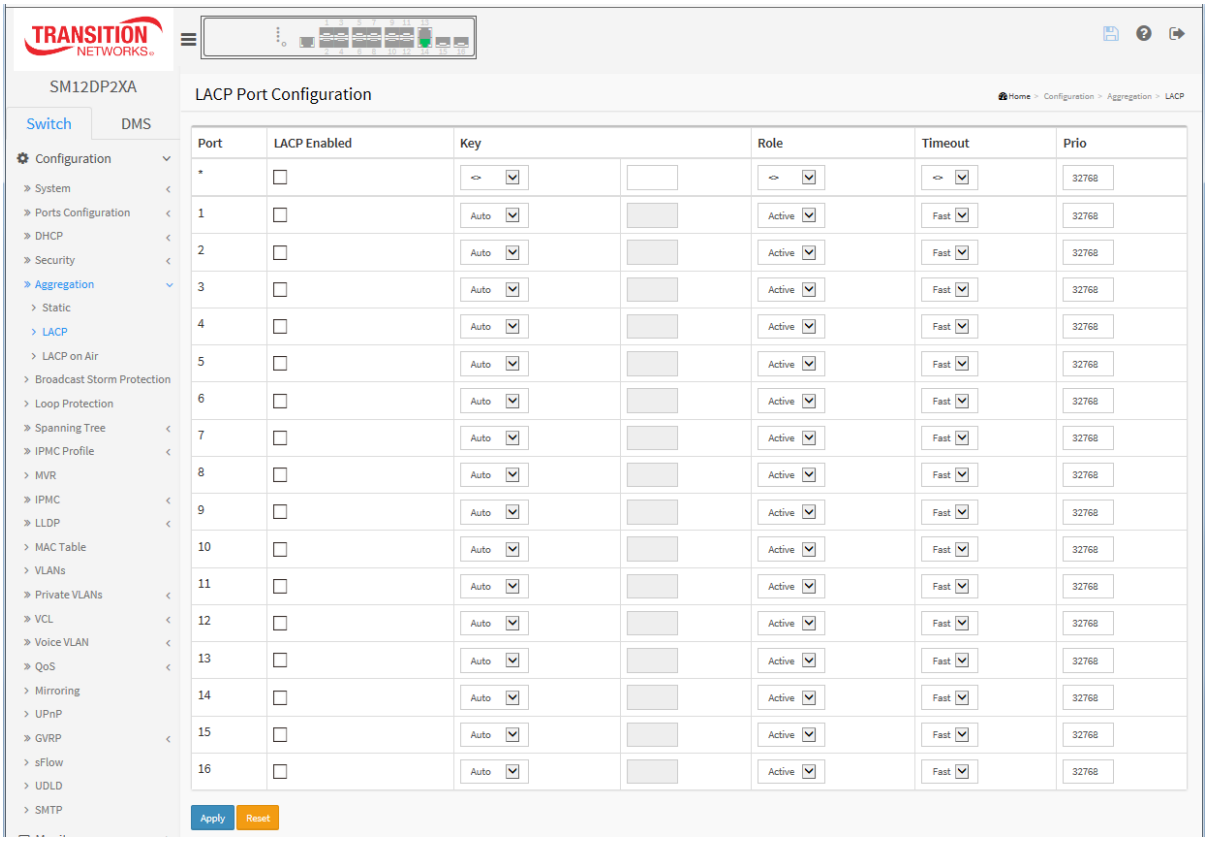
This page lets you view and configure the current LACP port configuration parameters. LACP (Link Aggregation Control Protocol) is an IEEE 802.3ad standard protocol that allows bundling several physical ports together to form a single logical port. An LACP trunk group with more than one ready member ports is a “real trunked” group. An LACP trunk group with only one or no ready member ports is not a “real trunked” group.

Web Interface

To configure the Trunk Aggregation LACP parameters in the web interface:

1. Click Configuration, LACP, Configuration.
2. Enable or disable the LACP on the port of the switch.
3. Scroll the Key parameter with Auto or Specific. The default is Auto.
4. Scroll the Role with Active or Passive. The default is Active.
5. Click Apply to save the settings.
6. To cancel the settings, click the Reset button to revert to previously saved values.

Figure 2-6.2: LACP Port Configuration



Parameter descriptions:

Port : The switch port number.

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

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

Role : The Role shows the LACP activity status. The Active will transmit LACP packets each second, while Passive will wait for a LACP packet from a partner (speak if spoken to).

Timeout : The Timeout controls the period between BPDU transmissions. Fast will transmit LACP packets each second, while Slow will wait for 30 seconds before sending a LACP packet.

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

Buttons

Apply – Click to save changes.

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

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

2-7 LACP on Air

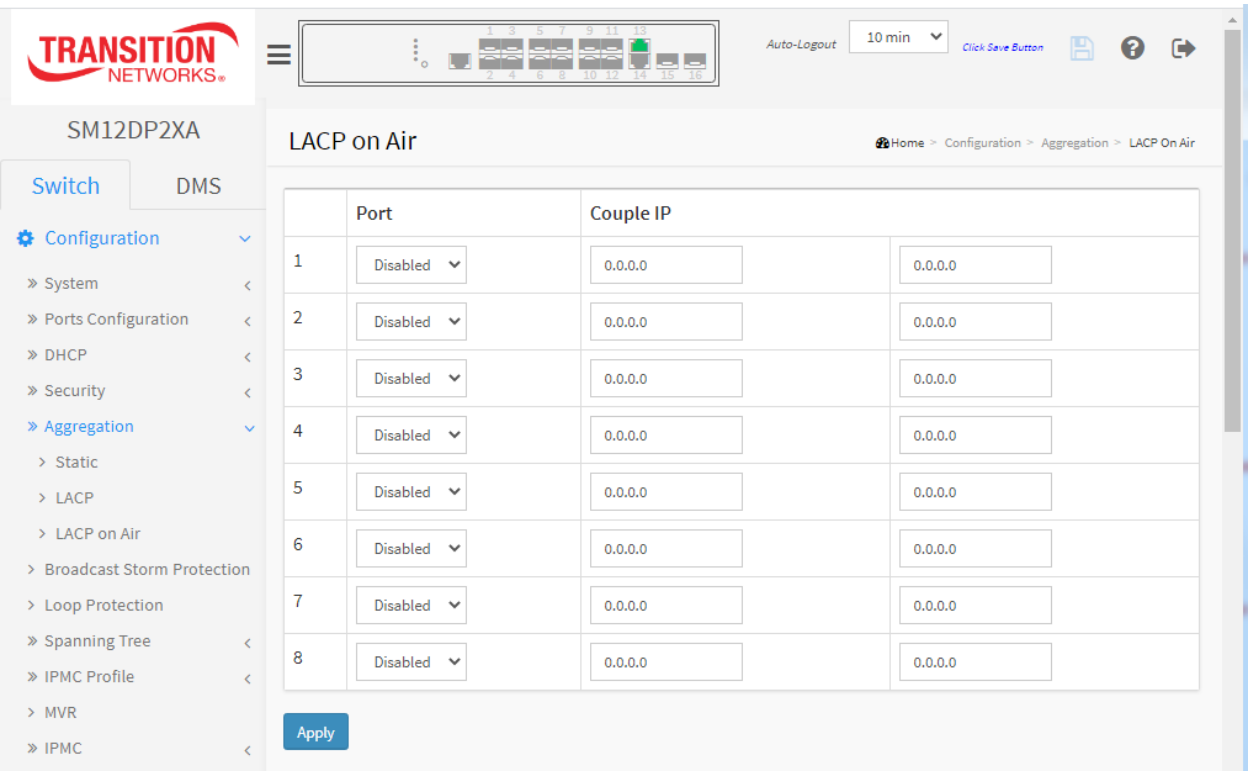
This page lets you view and configure the current LACP on Air ports and the Couple IP address for access management.

Web Interface

To configure LACP on Air parameters via the web interface:

1. Click Switch > Configuration > Aggregation > LACP On Air.
2. Enable or disable the Port(s).
3. Enter the Couple IP addresses.
4. Click Apply to save the settings.

Figure 2-7: LACP on Air



Parameter descriptions:

Port: Select the switch port should led the access of Couple IP device management.

Couple IP: Specify the connected partners for access management.

Buttons

Apply: Click to save changes.

2-8 Broadcast Storm Protection

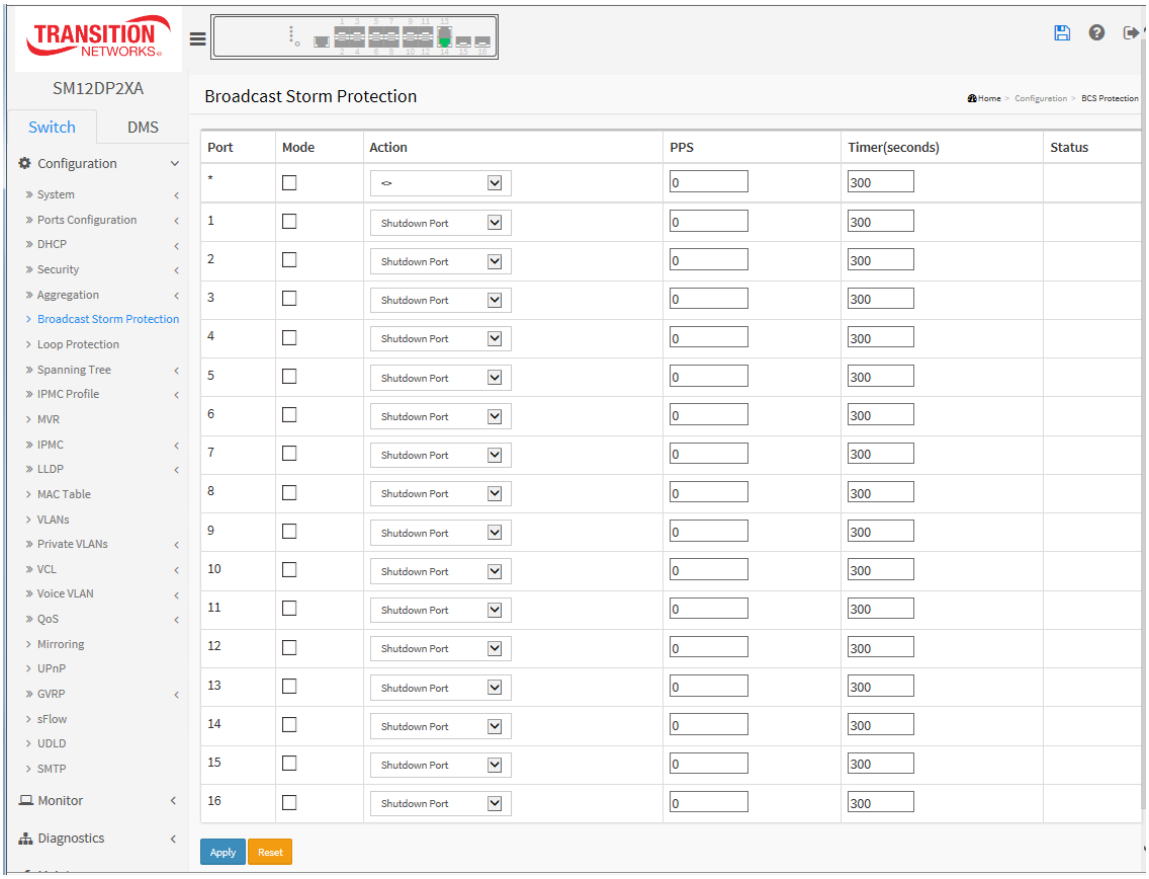
This page lets you view and configure the current Broadcast Storm Protection parameter settings.

Web Interface

To configure the Broadcast Storm Protection parameters in the web interface:

1. Click Configuration, Broadcast Storm Protection.
2. Enable or disable the Broadcast Storm Protection mode for each port.
3. Click Apply to save the settings.
4. To cancel the settings, click the Reset button to revert to previously saved values.

Figure 2-8: Broadcast Storm Protection



Parameter descriptions:

Port: The switch port number of the port.

Enable: Controls whether Broadcast Storm Protection is enabled on this switch port.

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

PPS: Broadcast Storm Protection threshold.

Timer: The period (in seconds) for which a port will be kept disabled in the event of a broadcast storm is detected (and the port action shuts down the port). Valid values are 0 to 65535 seconds.

Status: The current broadcast storm protection status of the port.

2-9 Loop Protection

Loop Protection is used to detect the presence of traffic. When the switch receives a packet's (looping detection frame) MAC address the same as itself from a port, Loop Protection occurs.

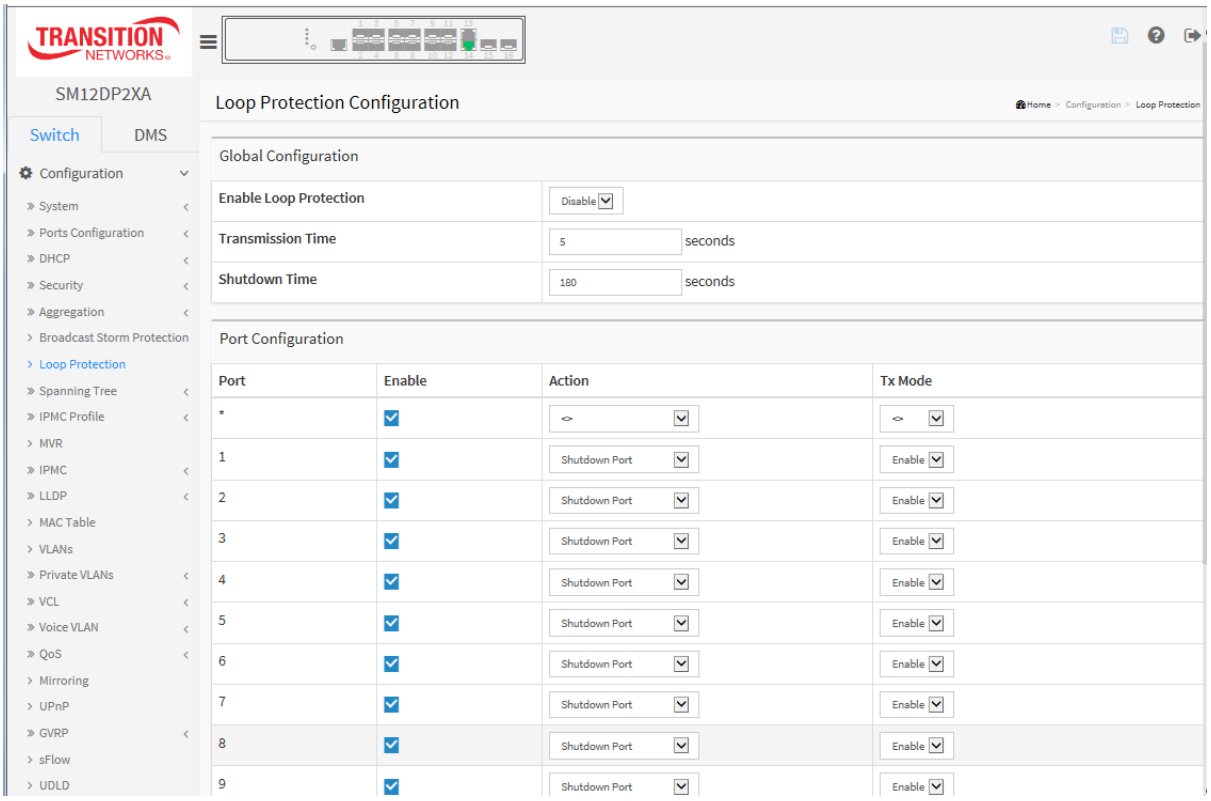
The port will be locked when it receives the loop Protection frames. If you want to resume the locked port, find out the looping path and take off the looping path, then select the resume the locked port and click "Resume" to turn on the locked ports.

Web Interface

To configure the Loop Protection parameters in the web interface:

1. Click Configuration, Loop Protection.
2. Enable or disable port Loop Protection for each port.
3. Enter the Global Configuration parameters.
4. Enter the Port Configuration parameters.
5. Click Apply to save the settings.
6. To cancel the setting, click the Reset button to revert to previously saved values.

Figure 2-9: Loop Protection Configuration.



Parameter descriptions:

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

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

Shutdown Time: The period (in seconds) for which a port will be kept disabled in the event of a loop is detected (and the port action shuts down the port). Valid values are 0 to 604800 seconds (7 days). A value of zero will keep a port disabled (until next device restart). The default value is 180 seconds.

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:

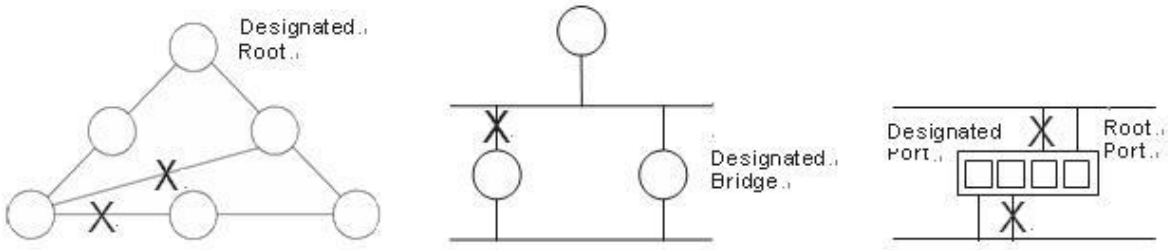
Apply – Click to save changes.

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

2-10 Spanning Tree

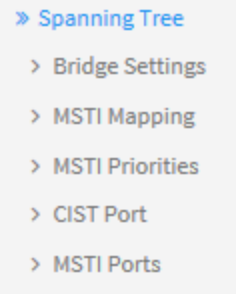
The Spanning Tree Protocol (STP) can be used to detect and disable network loops, and to provide backup links between switches, bridges or routers. This allows the switch to interact with other bridging devices (that is, an STP-compliant switch, bridge or router) in your network to ensure that only one 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.

Navigate to the Configuration > Spanning Tree menu path to display the Spanning Tree sub-tabs (Bridge Settings, MSTI Mapping, MSTI Priorities, CIST Port, and MSTI Ports).



2-10.1 Bridge Setting

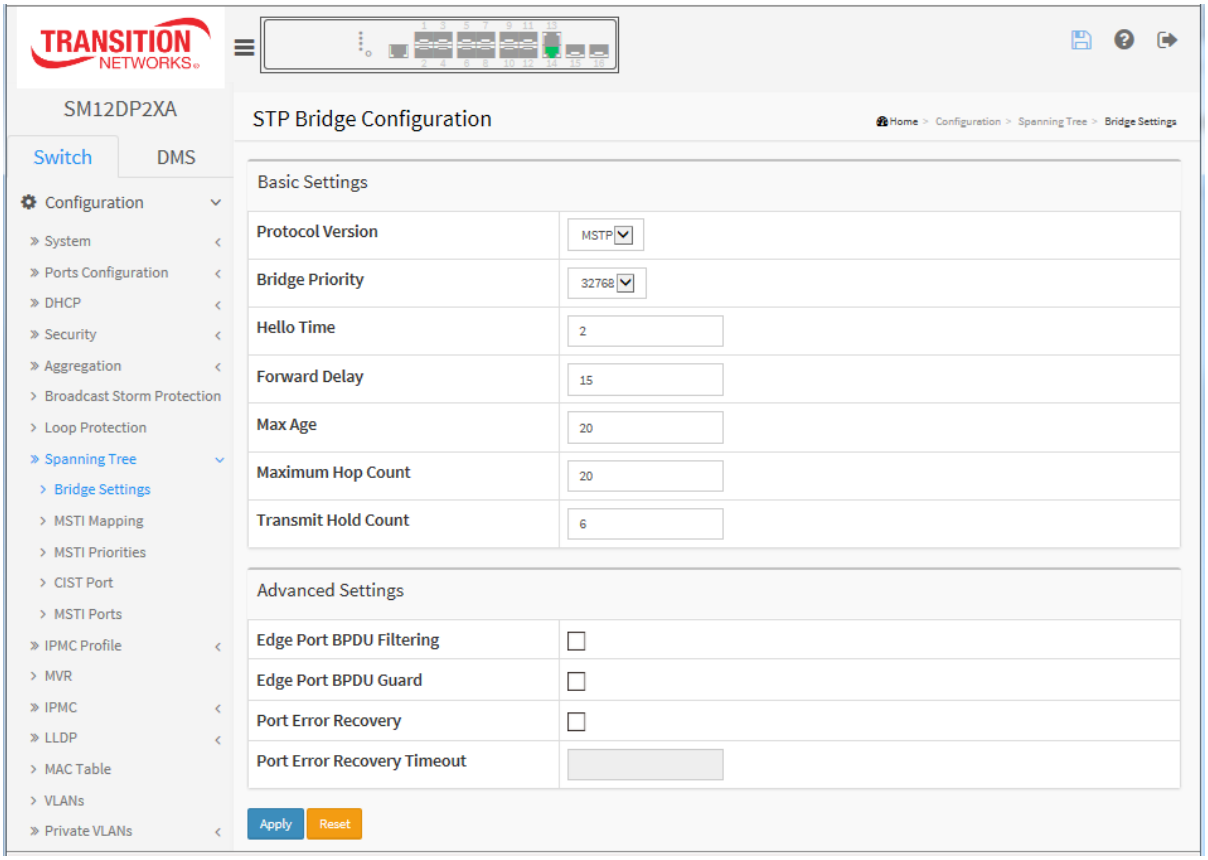
This page lets you configure the Spanning Tree Bridge and STP System settings. It allows you to configure STP System settings are used by all STP Bridge instance in the switch.

Web Interface

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

1. Click Configuration, Spanning Tree, Bridge Settings.
2. Set the Basic Settings and Advanced Settings parameters.
3. Click the Apply button to save the settings
4. To cancel the settings, click the Reset button to revert to previously saved values.

Figure 2-10.1: STP Bridge Configuration



Parameter descriptions:

Basic Settings

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

Bridge Priority : Controls the bridge priority. Lower numeric values have better priority. The bridge priority plus the MSTI instance number, concatenated with the 6-byte MAC address of the switch forms a Bridge Identifier. For MSTP operation, this is the priority of the CIST. Otherwise, this is the priority of the STP/RSTP bridge.

Forward Delay : The delay used by STP Bridges to transit Root and Designated Ports to Forwarding (used in STP compatible mode). Valid values are in the range 4 to 30 seconds.

Max Age : The maximum age of the information transmitted by the Bridge when it is the Root Bridge. Valid values are in the range 6 to 40 seconds, and MaxAge must be <= (FwdDelay-1)*2.

Maximum Hop Count : This defines the initial value of remaining Hops for MSTI information generated at the boundary of an MSTI region. It defines how many bridges a root bridge can distribute its BPDU information to. Valid values are in the range 6 to 40 hops.

Transmit Hold Count : The number of BPDU's a bridge port can send per second. When exceeded, transmission of the next BPDU will be delayed. Valid values are in the range 1 to 10 BPDU's per second.

Advanced Settings

Edge Port BPDU Filtering : Control whether a port explicitly configured as Edge will transmit and receive BPDUs.

Edge Port BPDU Guard : Control whether a port explicitly configured as Edge will disable itself upon reception of a BPDU. The port will enter the error-disabled state, and will be removed from the active topology.

Port Error Recovery : Control whether a port in the error-disabled state automatically will be enabled after a certain time. If recovery is not enabled, ports have to be disabled and re-enabled for normal STP operation. The condition is also cleared by a system reboot.

Port Error Recovery Timeout : The time to pass before a port in the error-disabled state can be enabled. Valid values are between 30 and 86400 seconds (24 hours).

Buttons

Apply – Click to save changes.

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

2-10.2 MSTI Mapping

When you implement a Spanning Tree Protocol on the switch that is the bridge instance. The CIST is not available for explicit mapping, as it will receive the VLANs not explicitly mapped. For that reason you must set the list of VLANs mapped to the MSTI. The VLANs must be separated with a 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).

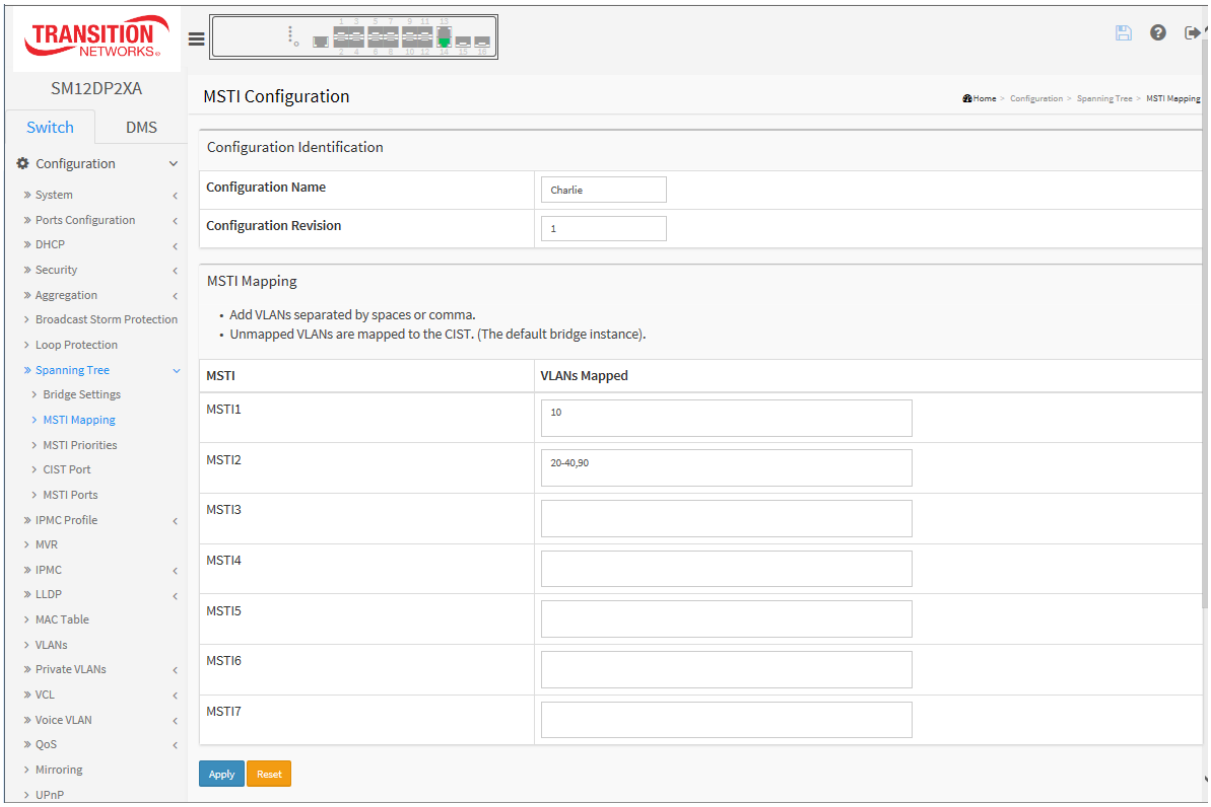
This page lets you view and configure the current STP MSTI bridge instance priority.

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

Figure 2-10.2: MSTI Configuration



Parameter descriptions:

Configuration Identification

Configuration Name : The name identifying the VLAN to MSTI mapping. Bridges must share the name and revision (see below), as well as the VLAN-to-MSTI mapping configuration in order to share spanning trees for MSTI's (Intra-region). The name is at most 32 characters.

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

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

MSTI : The bridge instance. The CIST is not available for explicit mapping, as it will receive the VLANs not explicitly mapped.

VLANs Mapped : The list of VLANs mapped to the MSTI. The VLANs can be given as a single (xx, xx being between 1 and 4094) VLAN, or a range (xx-yy), each of which must be separated with comma and/or space. A VLAN can only be mapped to one MSTI. An unused MSTI should just be left empty. (I.e. not having any VLANs mapped to it.) Example: 2,5,20-40.

Buttons

Apply – Click to save changes.

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

2-10.3 MSTI Priorities

When you implement a Spanning Tree protocol on the switch that the bridge instance. The CIST is the default instance which is always active. For controls the bridge priority. Lower numeric values have better priority. The bridge priority plus the MSTI instance number, concatenated with the 6-byte MAC address of the switch forms a Bridge Identifier.

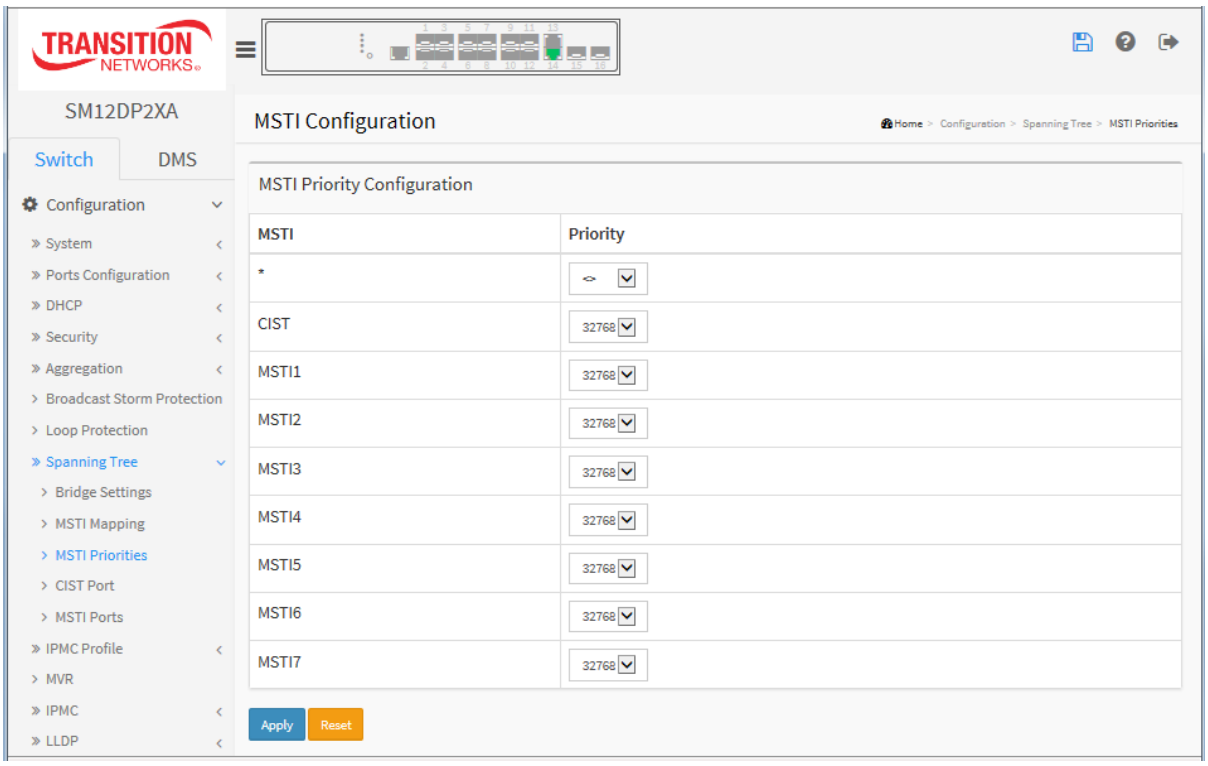
This page lets you view and configure current STP MSTI bridge instance priority parameters.

Web Interface

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

1. Click Configuration, Spanning Tree, MSTI Priorities
2. Select the Priority, the maximum is 240. The default is 128.
3. Click Apply to save the settings.
4. To cancel the settings, click the Reset button to revert to previously saved values.

Figure 2-10.3: MSTI Configuration



Parameter descriptions:

MSTI : The bridge instance. The CIST is the default instance, which is always active.

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

Buttons

Apply – Click to save changes.

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

2-10.4 CIST Ports

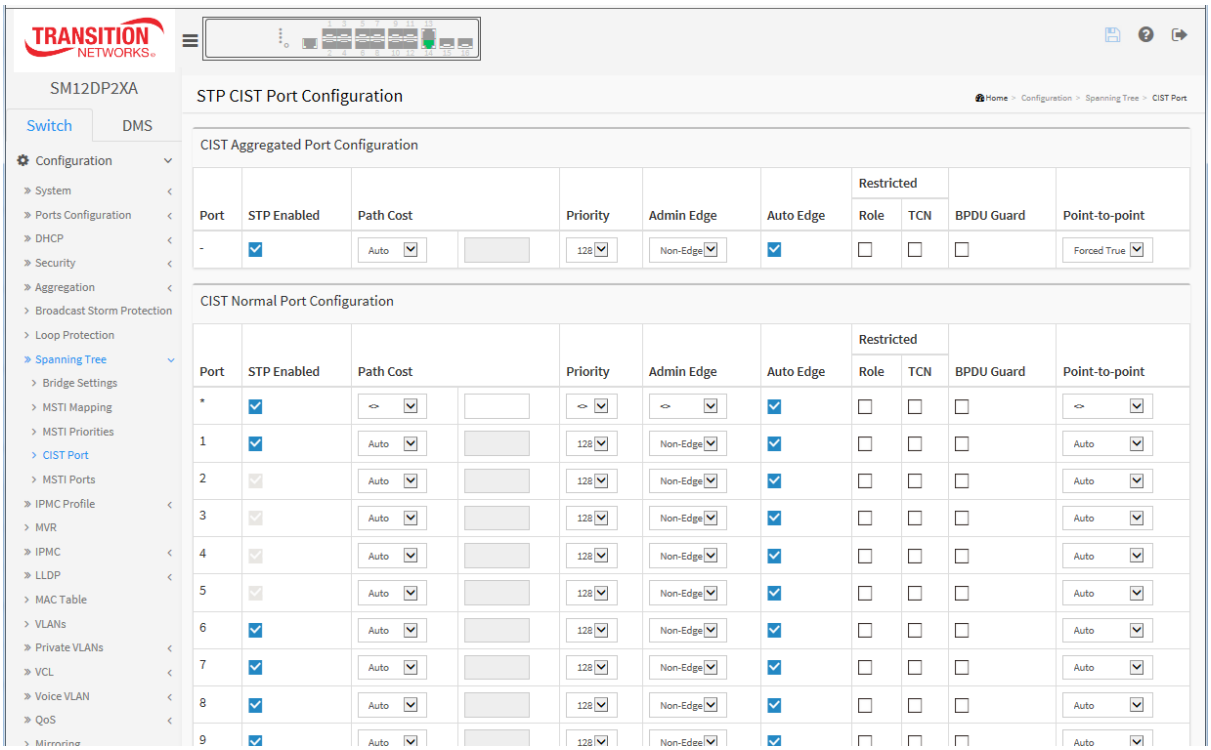
When you implement a Spanning Tree protocol on the switch that the bridge instance, you must configure the CIST Ports. This page lets you view and configure the current STP CIST port settings.

Web Interface

To configure the Spanning Tree CIST Ports parameters in the web interface:

1. Click Configuration, Spanning Tree, CIST Ports.
2. Scroll to and set all parameters of CIST Aggregated Port Configuration.
3. Enable or disable the STP, then scroll and set all CIST normal Port configuration parameters.
4. Click Apply to save the settings.
5. To cancel the settings, click the Reset button to revert to previously saved values.

Figure 2-10.4: CIST Aggregated Port Configuration



Parameter descriptions:

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

STP Enabled : Controls whether STP is enabled on this switch port.

Path Cost : Controls the path cost incurred by the port. The Auto setting will set the path cost as appropriate by the physical link speed, using the 802.1D recommended values. Using the Specific setting, a user-defined value can be entered. The path cost is used when establishing the active topology of the network. Lower path cost ports are chosen as forwarding ports in favor of higher path cost ports. Valid values are in the range 1 to 200000000.

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

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

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

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

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

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

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

Buttons

Apply – Click to save changes.

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

2-10.5 MSTI Ports

This page lets you view and configure the current STP MSTI port configurations.

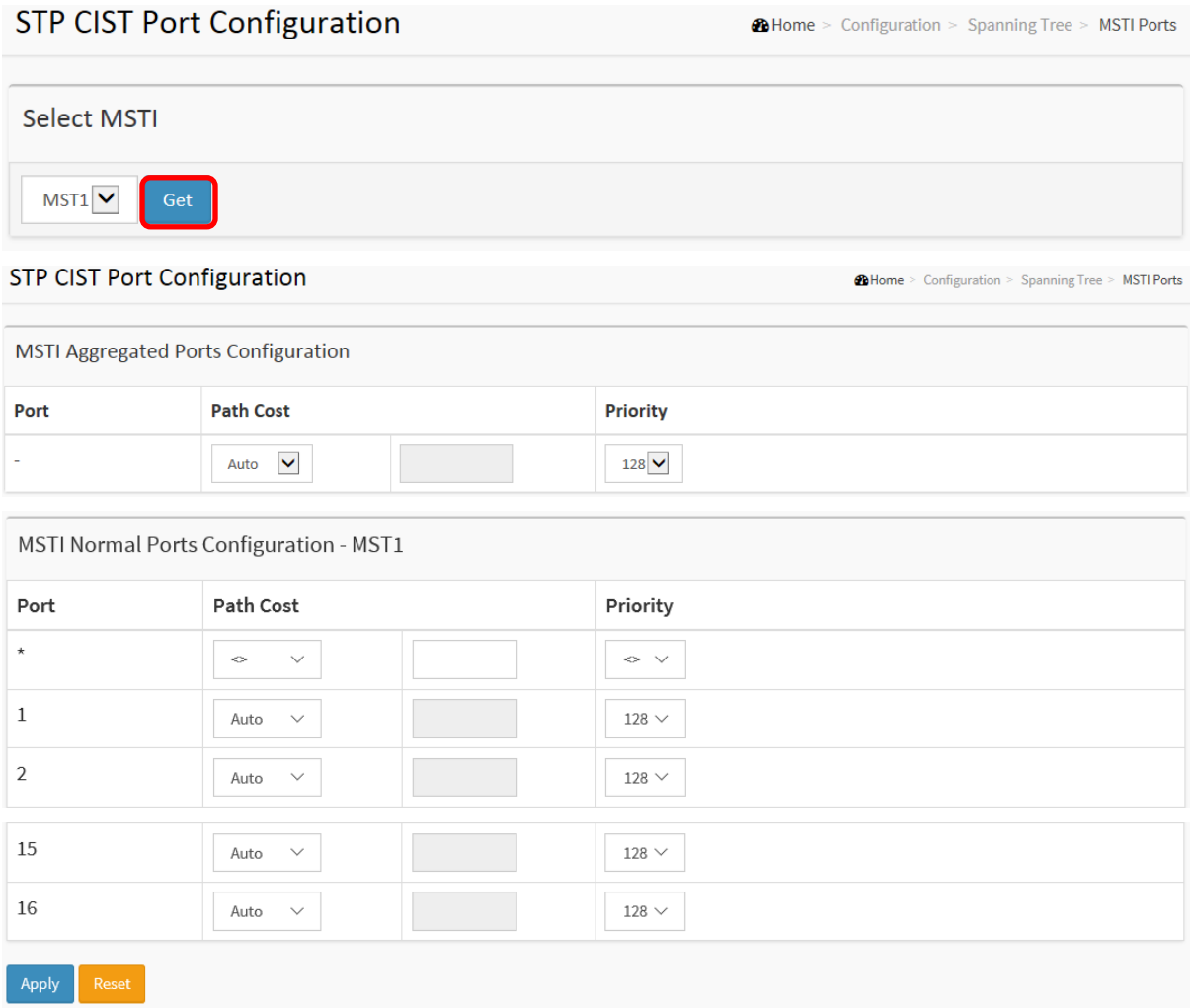
An MSTI port is a virtual port, which is instantiated separately for each active CIST (physical) port for each MSTI instance configured on and applicable to the port. The MSTI instance must be selected before displaying actual MSTI port configuration options. It contains MSTI port settings for physical 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. Select the MST1 or other MSTI Port.
3. Click **Get** to set the detail parameters of the MSTI Ports.
4. Set all parameters of the MSTI Port configuration.
5. Click **Apply** to save the settings.
6. To cancel the settings, click the **Reset** button to revert to previously saved values.

Figure 2-10.5: MSTI Port Configuration



Parameter descriptions:

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

Path Cost : Controls the path cost incurred by the port. The Auto setting will set the path cost as

appropriate by the physical link speed, using the 802.1D recommended values. Using the Specific setting, a user-defined value can be entered. The path cost is used when establishing the active topology of the network. Lower path cost ports are chosen as forwarding ports in favor of higher path cost ports. Valid values are 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).

Buttons

Get : Click to retrieve settings for a specific MSTI.

Apply : Click to save changes.

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

2-11 IPMC Profile

This page provides IPMC Profile related configurations. IPMC (IP MultiCast) supports IPv4 and IPv6 multicasting (IPMCv4 and IPMCv6).

2-11.1 Profile Table

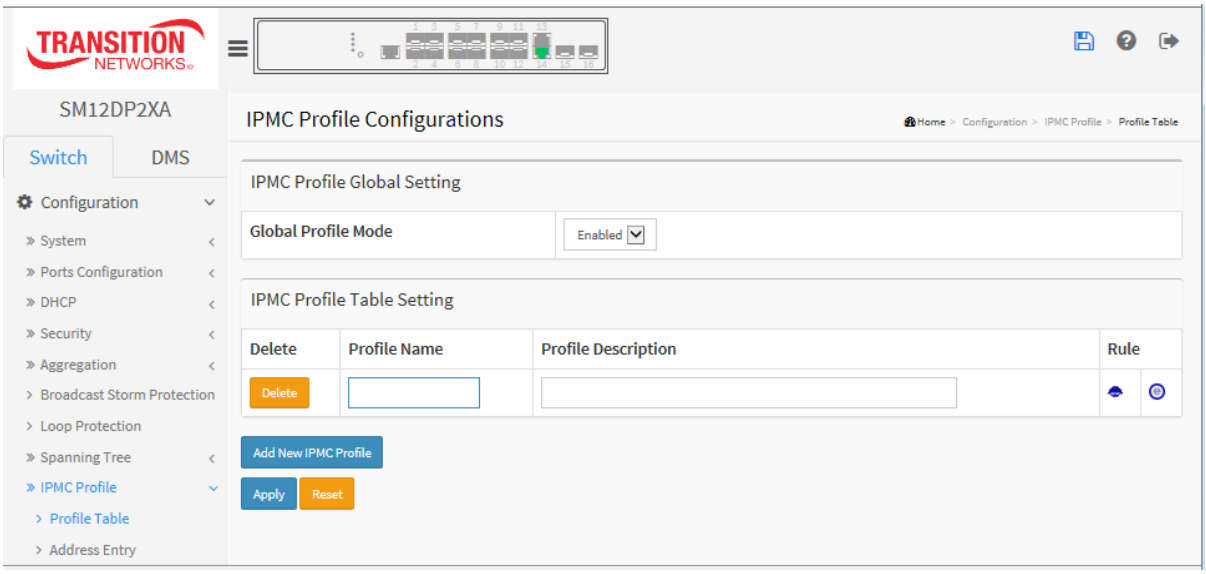
The IPMC profile is used to deploy the access control on IP multicast streams. It is allowed to create at maximum 64 Profiles with at maximum 128 corresponding rules for each.

Web Interface

To configure the IPMC Profile Configuration in the web interface:

1. Navigate to Configuration > IPMC Profile > Profile Table.
2. Set Global Profile Mode to Enabled.
3. Click the Add New Profile button.
4. Enter a Profile Name and a Profile Description.
5. Click the Apply button.
6. List ( ) and Adjust ( ) the Profile rule.
7. Click the Add Last Rule button.
8. Click the Apply button to save the changes

Figure 2-11.1: IPMC Profile Configuration



Parameter descriptions:

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

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

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

Profile Name : The name used for indexing the profile table.
Each entry has the unique name which is composed of 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. Summary about the designated profile will be shown by clicking the view button. You can manage or inspect the rules of the designated profile by using the following buttons:

: List the rules associated with the designated profile.

: Adjust the rules associated with the designated profile.

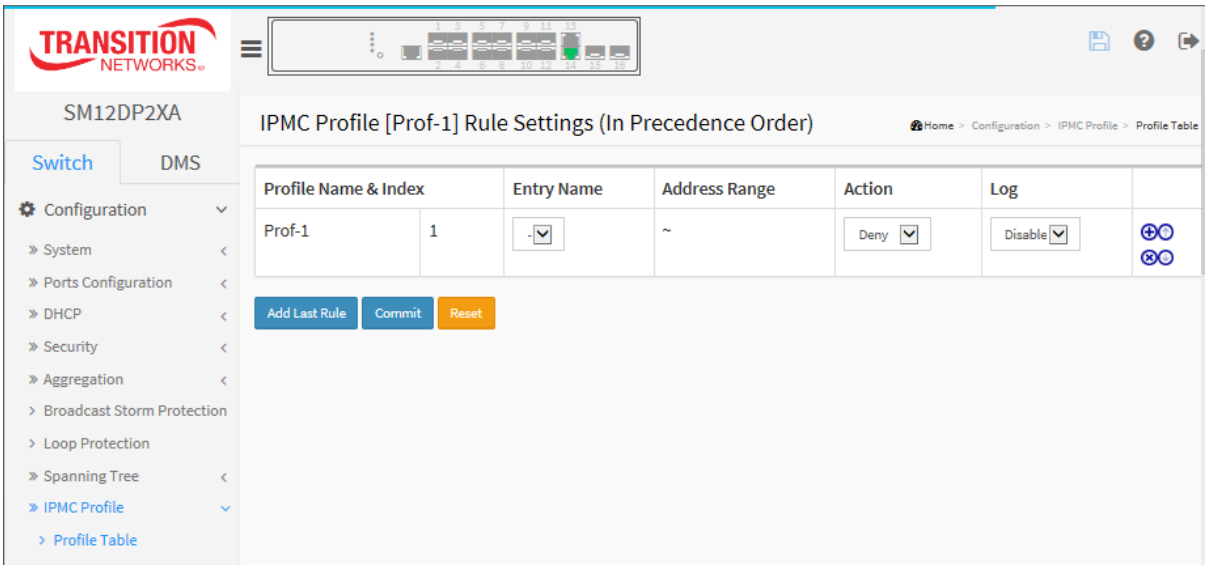
Buttons

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

Apply – Click to save changes.

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

Click the **Add Last Rule** button to display the newly-created IPMC Profile [Prof-1] Rule Settings (In Precedence Order):



Create an Address Entry and click the **Commit** button.

Buttons

Rule Management buttons : Manage rules and their precedence order using these buttons:

: **Insert**: Insert a new rule before this rule.

: **Delete**: Delete this rule.

: **Up**: Move this rule up in the list.

: **Down**: Moves this rule down in the list.

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.

2-11.1.1 IPMC Profile Rule Settings Table

This page provides the filtering rule settings for a specific IPMC profile. It displays the configured rule entries in precedence order. First rule entry has highest priority in lookup, while the last rule entry has lowest priority in lookup.

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

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

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

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

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

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

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

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

: Insert a new rule before the current entry of rule.

: Delete the current entry of rule.

: Moves the current entry of rule up in the list.

: Moves the current entry of rule down in the list.

Buttons

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

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

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

2-11.2 Address Entry

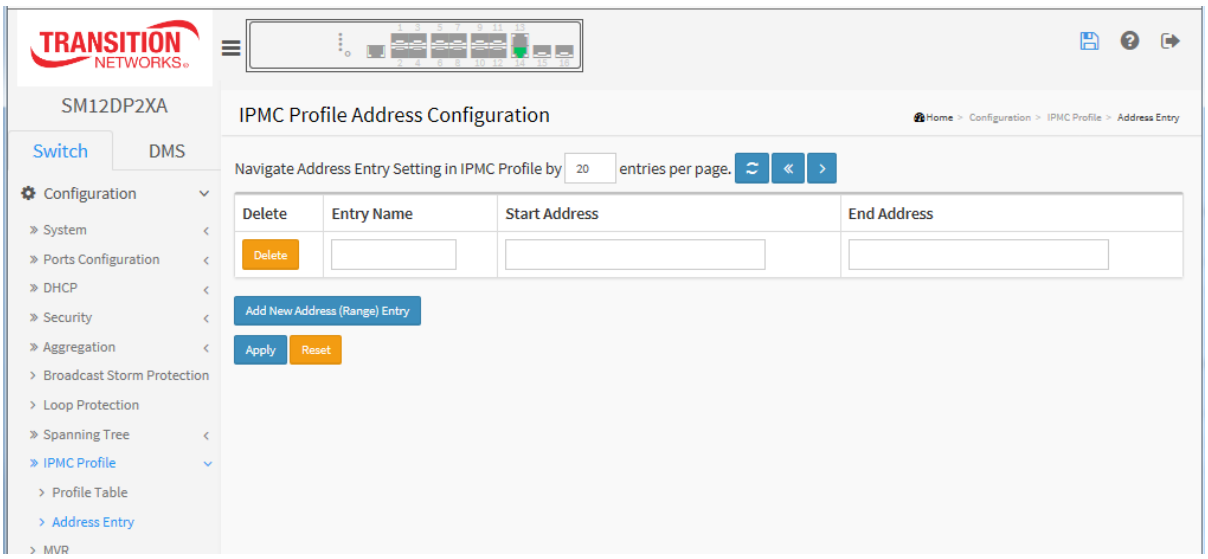
This page provides address range settings used in IPMC profile. The address entry is used to specify the address range that will be associated with IPMC Profile. You can create up to 128 address entries in the system.

Web Interface

To configure the IPMC Profile Address Configuration in the web interface:

1. Navigate to Configuration > IPMC Profile > Address Entry.
2. Click the **Add New Address (Range)** button.
3. Enter a new Entry Name, Start Address, and End Address.
4. Click the **Apply** button to save the changes.

Figure 2-11.2: IPMC Profile Address Configuration



Parameter descriptions:

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

Entry Name : The name used for indexing the address entry table.
Each entry has the unique name which is composed of a maximum of 16 alphabetic and numeric characters. At least one alphabet must be present.

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

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

Buttons

Add New Address (Range) Entry : Click the button to add a new address range.

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.

<< : First entry; updates the table starting from the first entry in the IPMC Profile Address Configuration.

> : Next entry; updates the table, starting with the entry after the last entry currently displayed.

2-12 MVR

The MVR feature enables multicast traffic forwarding on the Multicast VLAN.

The MVR (Multicast VLAN Registration) protocol for Layer 2 (IP)-networks enables multicast-traffic from a source VLAN to be shared with subscriber-VLANs. The main reason for using MVR is to save bandwidth by preventing duplicate multicast streams being sent in the core network, instead the stream(s) are received on the MVR-VLAN and forwarded to the VLANs where hosts have requested it/them.

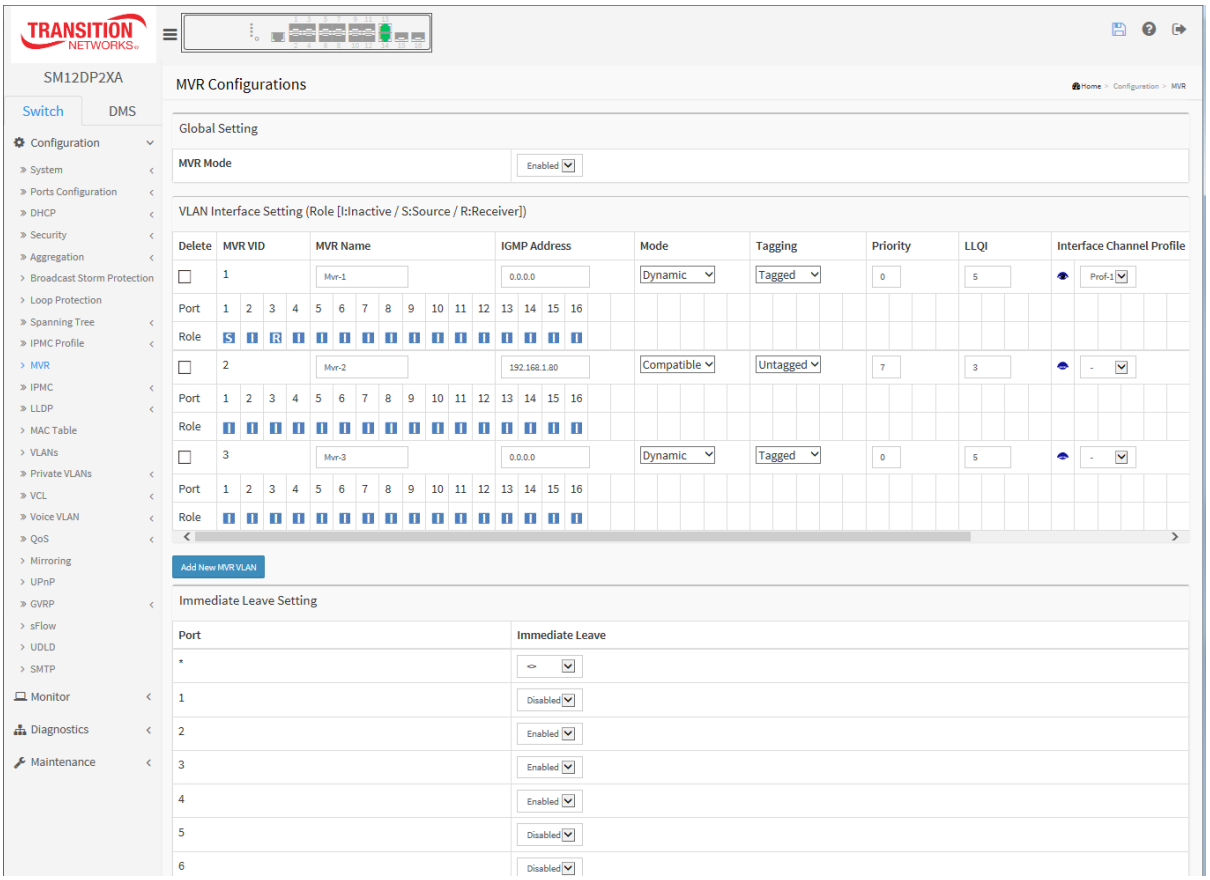
In a multicast television application, a PC or a television with a set-top box can receive the multicast stream. Multiple set-top boxes or PCs can be connected to one subscriber port, which is a switch port configured as an MVR receiver port. When a subscriber selects a channel, the set-top box or PC 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.

Web Interface

To configure the MVR Configuration in the web interface:

1. Click Configuration, MVR.
2. Set the MVR mode to enable or disable and set all parameters.
3. Click Apply to save the settings.
4. To cancel the settings, click the Reset button to revert to previously saved values.

Figure 2-12: MVR Configuration



Parameter descriptions:

Global Setting :

MVR Mode : Enable/Disable MVR globally. The Unregistered Flooding control depends on the current configuration in IGMP/MLD Snooping. It is suggested to enable Unregistered Flooding control when the MVR group table is full.

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

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

MVR VID : Specify the Multicast VLAN ID. **Caution:** MVR source ports are not recommended to be overlapped with Management VLAN ports.

MVR Name : MVR Name is an optional attribute to indicate the name of the specific MVR VLAN. Maximum length of the MVR VLAN Name string is 32. MVR VLAN Name can only contain alphabets or numbers. When the optional MVR VLAN name is given, it should contain at least one alphabet. MVR VLAN name can be edited for the existing MVR VLAN entries or it can be added to the new entries.

IGMP Address : Define the IPv4 address as source address used in IP header for IGMP control frames. The default IGMP address is not set (0.0.0.0). When the IGMP address is not set, the system uses IPv4 management address of the IP interface associated with this VLAN. When the IPv4 management address is not set, the system uses the first available IPv4 management address. Otherwise, the system uses a pre-defined value; by default, this value will be 192.0.2.1.

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

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

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

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

Interface Channel Setting : When the MVR VLAN is created, click the Edit symbol to expand the corresponding multicast channel settings for the specific MVR VLAN. Summary about the Interface Channel Setting (of the MVR VLAN) will be shown besides the Edit symbol.

Port : The logical port for the settings.

Port Role : Configure an MVR port of the designated MVR VLAN as one of these roles: **S**, **I** or **R**.

> ***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; **S** indicates Source; **R** indicates Receiver. The default Role is **I**nactive.

Immediate Leave : Enable the fast leave on the port.

Buttons

Add New MVR VLAN : Click to add new MVR VLAN. Specify the VID and configure the new entry, then click "Save".

Apply : Click to save changes.

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

Message: *MVR Interface Configuration Error Failure in SET MVR VLAN VID 2*
Recovery: **1.** Click the Previous button to clear the error message. **2.** Re-configure the MVR VLAN.

2-13 IPMC

ICMP (Internet Control Message Protocol) is a protocol that generated the error response, diagnostic or routing purposes. ICMP messages generally contain information about routing difficulties or simple exchanges such as time-stamp or echo transactions.

2-12.1 IGMP Snooping

This function 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 supported 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 multicast packets are transmitted to a 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.

2-13.1.1 Basic Configuration

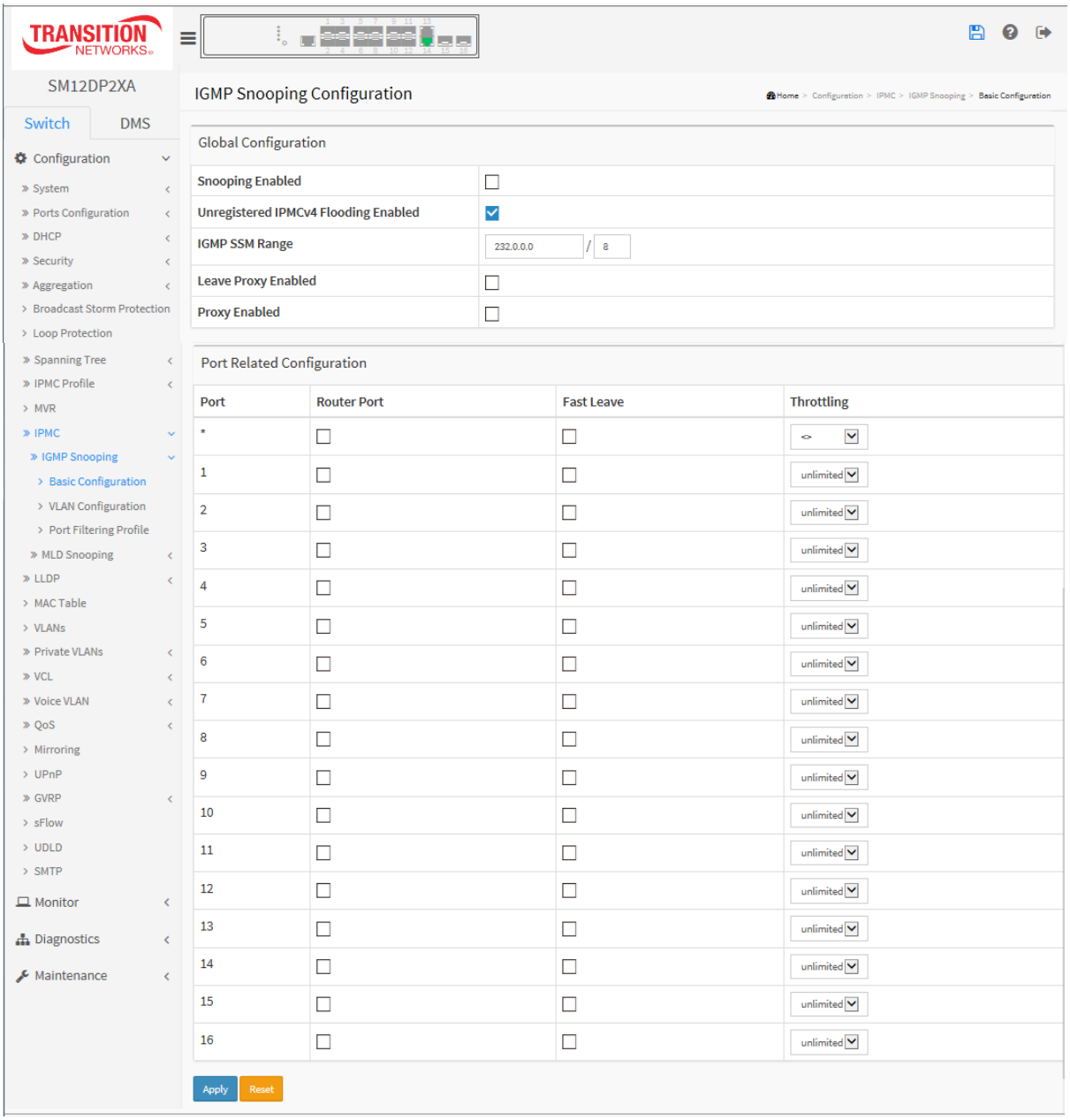
This page lets you set the basic IGMP snooping on the switch, which connects to a router closer to the root of the tree. This interface is the upstream interface. The router on the upstream interface should be running IGMP.

Web Interface

To configure the IGMP Snooping parameters in the web interface:

1. Click Configuration, IPMC, IGMP Snooping, Basic Configuration.
2. Evoke to select enable or disable which Global configuration.
3. Evoke which port wants to become a Router Port or enable/ disable the Fast Leave function.
4. Scroll to set the Throttling parameter.
5. Click Apply to save the settings.
6. To cancel the settings, click the Reset button to revert to previously saved values

Figure 2-13.1.1: IGMP Snooping Configuration



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/ sub mask)

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

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

Port : It shows the physical Port index of switch.

Router Port : Specify which ports act as router ports. A router port is a port on the Ethernet switch that leads towards the Layer 3 multicast device or IGMP querier.

If an aggregation member port is selected as a router port, the whole aggregation will act as a router port.

Fast Leave : Enable the fast leave on the port.

Throttling : Enable to limit the number of multicast groups to which a switch port can belong (unlimited or 0-10).

2-13.1.2 VLAN Configuration

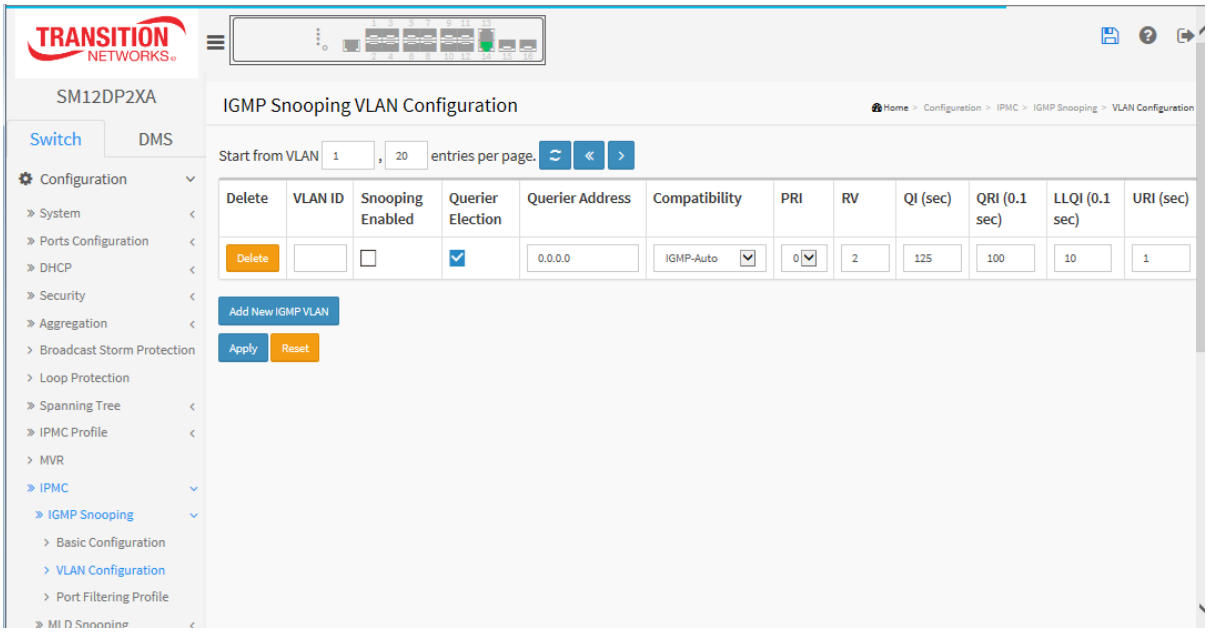
The section describes the VLAN configuration setting process integrated with IGMP Snooping function. For each setting page shows up to 99 entries from the VLAN table (default is 20) selected through the "entries per page" input field. When first visited, the web page will show the first 20 entries from the beginning of the VLAN table. The first displayed will be the one with the lowest VLAN ID found in the VLAN Table. The "VLAN" input fields let you select the starting point in the VLAN Table.

Web Interface

To configure the IGMP Snooping VLAN Configuration in the web interface:

1. Click Configuration, IPMC, IGMP Snooping, VLAN Configuration.
2. Enable or disable Snooping, IGMP Querier.
3. Specify the parameters in the blank field.
4. Click Refresh to update the data or click << or > to display previous entry or next entry.
5. Click Apply to save the settings.
6. To cancel the settings, click the Reset button to revert to previously saved values.

Figure 2-12.1.2: IGMP Snooping VLAN Configuration



Parameter descriptions:

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

VLAN ID : Displays the VLAN ID of the entry.

IGMP Snooping Enabled : Enable the per-VLAN IGMP Snooping. Only up to 32 VLANs can be selected.

Querier Election : Enable to join IGMP Querier election in the VLAN. Disable to act as an IGMP Non-Querier.

Querier Address : Define the IPv4 address as source address used in IP header for IGMP Querier election. When the Querier address is not set, the system uses IPv4 management address of the IP interface associated with this VLAN. When the IPv4 management address is not set, system uses the first available IPv4 management address.
Otherwise, the system uses a pre-defined value. By default, this value will be 192.0.2.1.

Compatibility : Compatibility is maintained by hosts and routers taking appropriate actions depending on the versions of IGMP operating on hosts and routers within a network. The allowed selection is IGMP-Auto, Forced IGMPv1, Forced IGMPv2, Forced IGMPv3, default compatibility value is IGMP-Auto.

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

Rv : Robustness Variable. The Robustness Variable allows tuning for the expected packet loss on a network. The allowed range is 1 to 255; default robustness variable value is 2.

QI : Query Interval. The Query Interval is the interval between General Queries sent by the Querier. The allowed range is 1 to 31744 seconds; default query interval is 125 seconds.

QRI : Query Response Interval. The Max Response Time used to calculate the Max Resp Code inserted into the periodic General Queries. The allowed range is 0 to 31744 in tenths of seconds; default query response interval is 100 in tenths of seconds (10 seconds).

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

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

Buttons :

Apply – Click to save changes.

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

Upper right icon (Refresh, <<, >) : You can click them Refreshes the displayed table starting from the "VLAN" input fields. Or click “<<” to update the table starting from the first entry in the VLAN table, i.e. the entry with the lowest VLAN ID. Others click “> “ to update the table, starting with the entry after the last entry currently displayed.

2-13.1.3 Port Filtering Profile

This page lets you set the IGMP Port Group Filtering. In some network application environments, such as metropolitan or multiple-dwelling unit (MDU) installations, a user might want to control the multicast groups to which a user on a switch port can belong. This feature lets you control the distribution of multicast services, such as IP/TV, based on some type of subscription or service plan.

With this feature you can filter multicast joins on a per-port basis by configuring IP multicast profiles and associating them with individual switch ports. An IGMP profile can contain one or more multicast groups and specifies whether access to the group is permitted or denied. If an IGMP profile denying access to a multicast group is applied to a switch port, the IGMP join report requesting the stream of IP multicast traffic is dropped, and the port is not allowed to receive IP multicast traffic from that group. If the filtering action permits access to the multicast group, the IGMP report from the port is forwarded for normal processing.

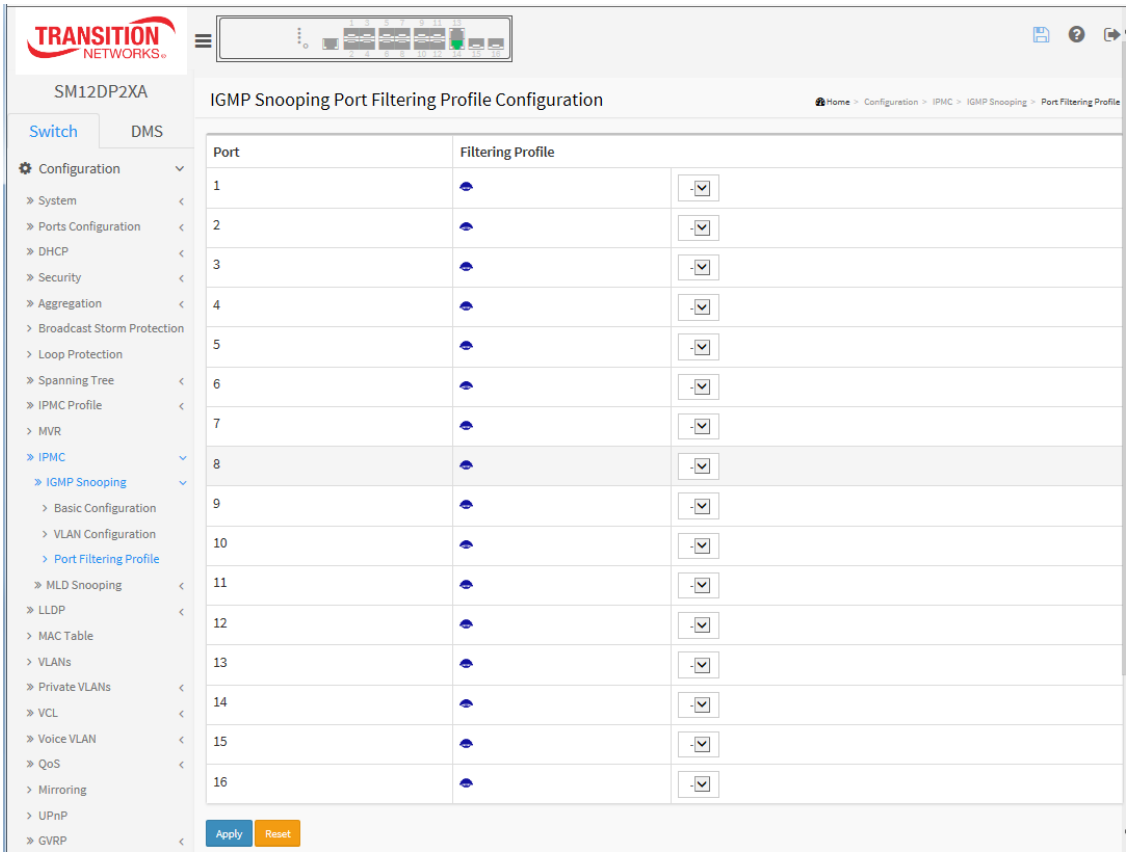
IGMP filtering controls only IGMP membership join reports and has no relationship to the function that directs the forwarding of IP multicast traffic.

Web Interface

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

1. Click Configuration, IPMC, IGMP Snooping, Port Group Filtering.
2. Click the Add New Filtering Group button.
3. Scroll the Port to enable the Port Group Filtering. Specify the Filtering Groups in the blank field.
4. Click Apply to save the settings.
5. To cancel the settings, click the Reset button to revert to previously saved values.

Figure 2-13.1.3: IGMP Snooping Port Filtering Profile Configuration



Parameter descriptions:

Port : The logical port for the settings.

Filtering Profile : Select the IPMC Profile as the filtering condition for the specific port. A summary of the designated profile will be shown by clicking the View button.

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

 : List the rules associated with the designated profile.

Buttons:

Apply – Click to save changes.

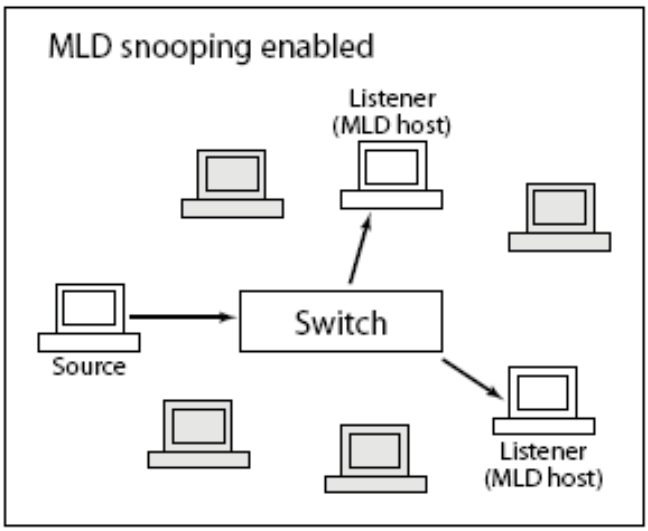
Reset- Click to undo any changes made locally and revert to previously saved values.

2-13.2 MLD Snooping

Curiously enough, a network node that acts as a source of IPv6 multicast traffic is only an indirect participant in MLD snooping—it just provides multicast traffic, and MLD doesn't interact with it. (Note, however, that in an application like desktop conferencing a network node may act as both a source and an MLD host; but MLD interacts with that node only in its role as an MLD host.)

A source node creates multicast traffic by sending packets to a multicast address. In IPv6, addresses with the first eight bits set (that is, "FF" as the first two characters of the address) are multicast addresses, and any node that listens to such an address will receive the traffic sent to that address. Application software running on the source and destination systems cooperates to determine what multicast address to use. (Note that this is a function of the application software, not of MLD.)

When MLD snooping is enabled on a VLAN, the switch acts to minimize unnecessary multicast traffic. If the switch receives multicast traffic destined for a given multicast address, it forwards that traffic only to ports on the VLAN that have MLD hosts for that address. It drops that traffic for ports on the VLAN that have no MLD hosts.



2-13.2.1 Basic Configuration

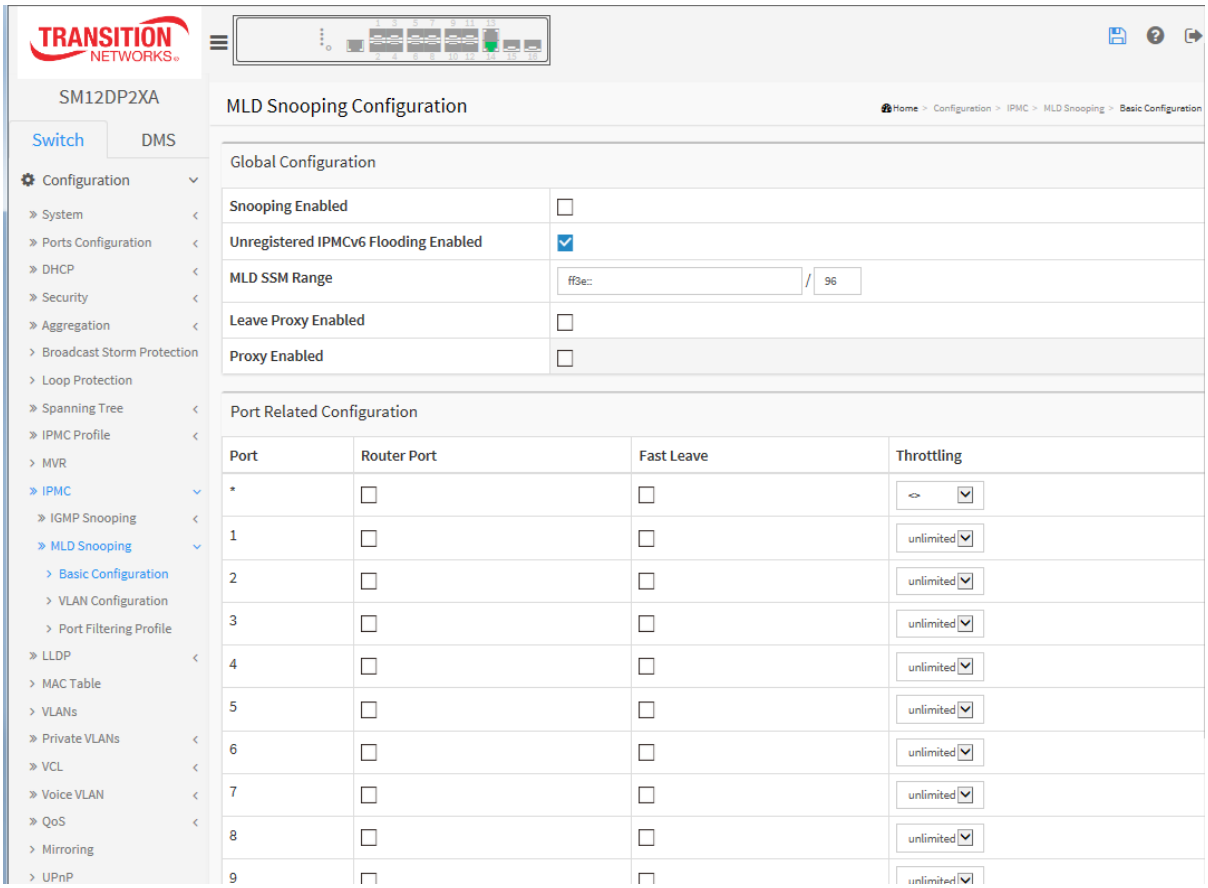
The section describes how to configure MLD Snooping basic configuration and parameters.

Web Interface

To configure the MLD Snooping Configuration in the web interface:

1. Click Configuration, MLD Snooping, Basic Configuration.
2. Set the Global configuration parameters.
3. Set the Port Related Configuration parameters.
4. Click Apply to save the settings.
5. To cancel the settings, click the Reset button to revert to previously saved values.

Figure 2-13.2.1: MLD Snooping Basic Configuration



Parameter descriptions:

Snooping Enabled : Enable the Global MLD Snooping.

Unregistered IPMCv6 Flooding Enabled : Enable unregistered IPMCv6 traffic flooding. The flooding control takes effect only when MLD Snooping is enabled. When MLD Snooping is disabled, unregistered IPMCv6 traffic flooding is always active in spite of this setting.

MLD SSM Range : SSM (Source-Specific Multicast) Range allows the SSM-aware hosts and routers run the SSM service model for the groups in the address (Using IPv6 Address) range.

Leave Proxy Enabled : Enable MLD Leave Proxy. This feature can be used to avoid forwarding unnecessary leave messages to the router side.

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

Router Port : Specify which ports act as router ports. A router port is a port on the Ethernet switch that leads towards the Layer 3 multicast device or MLD querier. If an aggregation member port is selected as a router port, the whole aggregation will act as a router port.

Fast Leave : Check to enable the Fast Leave on the port.

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

2-13.2.2 VLAN Configuration

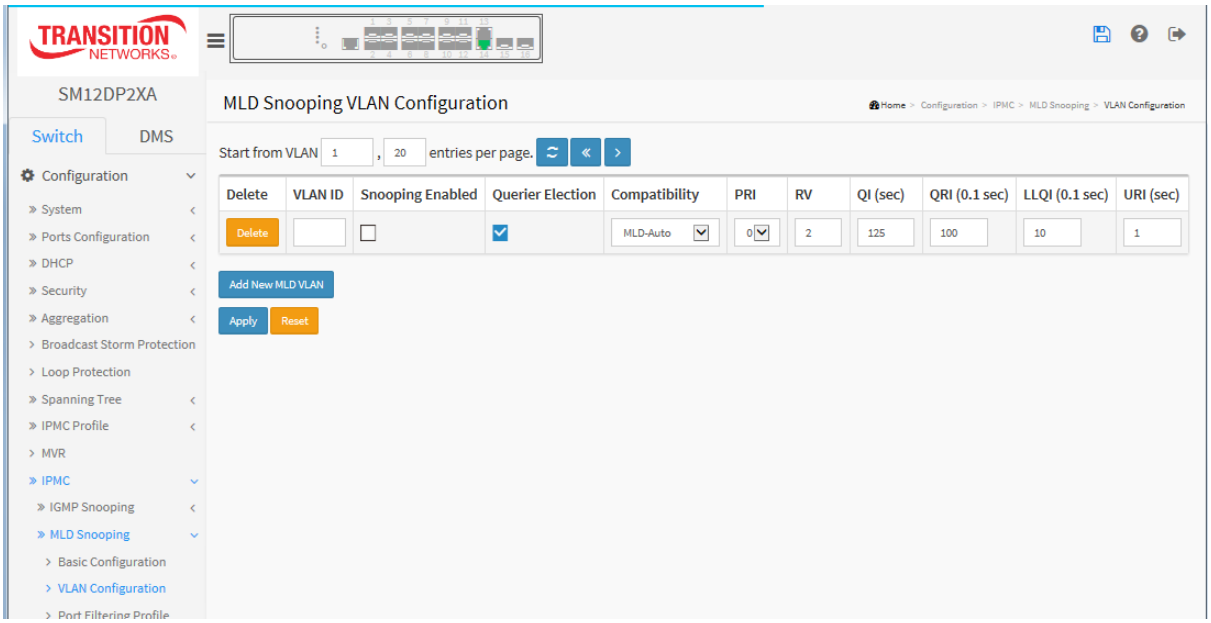
When MLD snooping is enabled on a VLAN, the switch acts to minimize unnecessary multicast traffic. If the switch receives multicast traffic destined for a given multicast address, it forwards that traffic only to ports on the VLAN that have MLD hosts for that address. It drops that traffic for ports on the VLAN that have no MLD hosts

Web Interface

To configure the MLD Snooping VLAN Configuration via the web interface:

1. Click Configuration, IPMC, MLD Snooping, VLAN Configuration.
2. Click the Add New MLD VLAN button.
3. Specify the VLAN ID, Snooping Enabled, Querier Election, Compatibility, PRI, RV, QI, QRI, LLQI, and URI parameters.
4. Click Refresh to refresh the MLD Snooping VLAN Configuration information.
5. Click << or > to move to the previous or next entry.

Figure 2-13.2.2: MLD Snooping VLAN Configuration.



Parameter descriptions:

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

VLAN ID : It displays the VLAN ID of the entry.

IGMP Snooping Enabled : Enable the per-VLAN IGMP Snooping. Only up to 32 VLANs can be selected. .

Querier Election : Enable to join IGMP Querier election in the VLAN. Disable to act as an IGMP Non-Querier.

Querier Address : Define the IPv4 address as source address used in IP header for IGMP Querier election. When the Querier address is not set, system uses IPv4 management address of the IP interface associated with this VLAN. When the IPv4 management address is not set, system uses the first available IPv4 management address. Otherwise, system uses a pre-defined value. By default, this value will be 192.0.2.1.

Compatibility : Compatibility is maintained by hosts and routers taking appropriate actions depending on the versions of IGMP operating on hosts and routers within a network. The allowed selection is IGMP-Auto, Forced IGMPv1, Forced IGMPv2, Forced IGMPv3, default compatibility value is IGMP-Auto.

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

Rv : Robustness Variable. The Robustness Variable allows tuning for the expected packet loss on a network. The allowed range is 1 to 255; default robustness variable value is 2.

QI : Query Interval. The Query Interval is the interval between General Queries sent by the Querier. The allowed range is 1 to 31744 seconds; default query interval is 125 seconds.

QRI : Query Response Interval. The Max Response Time used to calculate the Max Resp Code inserted into the periodic General Queries. The allowed range is 0 to 31744 in tenths of seconds; default query response interval is 100 in tenths of seconds (10 seconds).

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

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

Buttons :

Apply – Click to save changes.

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

Upper right icon (Refresh, <<, >) : Click to Refresh the displayed table starting from the "VLAN" input fields. Or click “<<” to update the table starting from the first entry in the VLAN table, i.e. the entry with the lowest VLAN ID. Otherwise click “> “ to update the table, starting with the entry after the last entry currently displayed.

2-13.2.3 Port Group Filtering

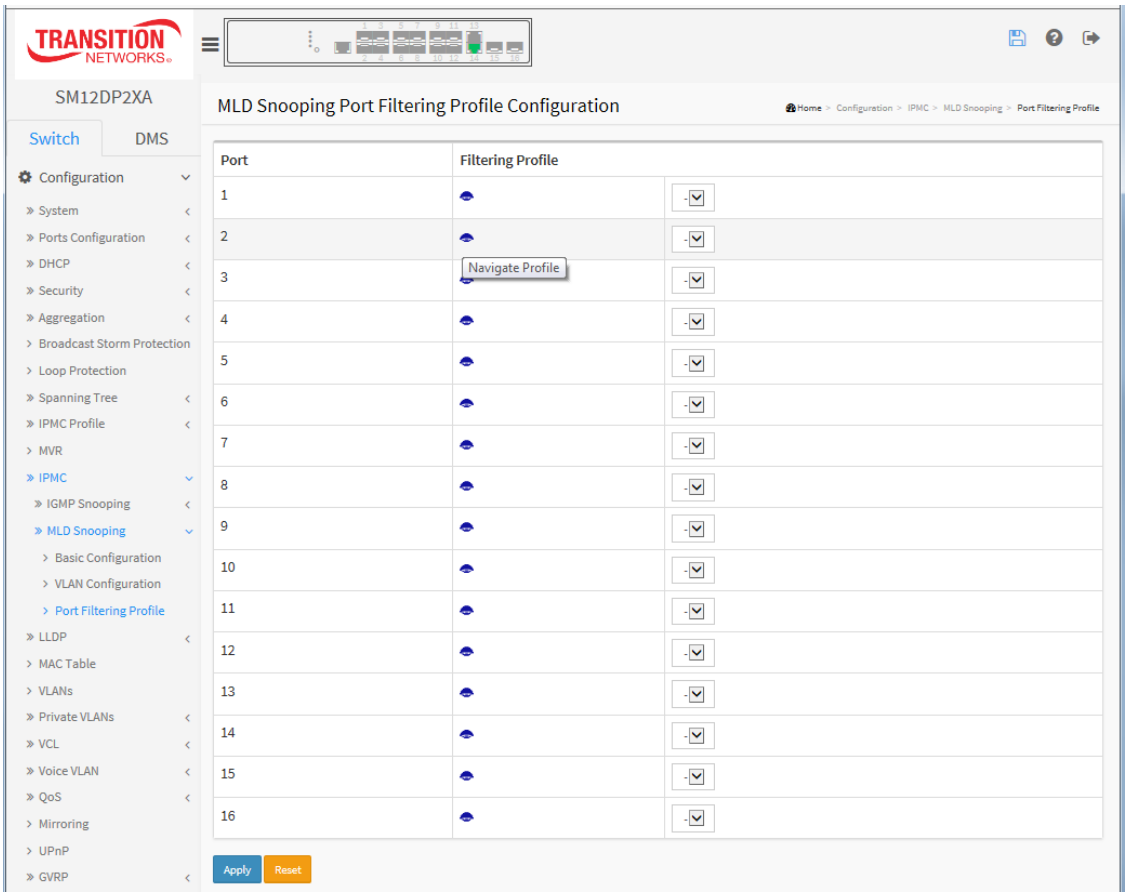
The section describes how to set Port Group Filtering in the MLD Snooping function and add new filtering group and safety policy.

Web Interface

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

1. Click Configuration, IPMC, MLD Snooping, Port Filtering Profile.
2. Specify the Filtering Profile entries per page.
3. Click the Apply to save the settings.
4. To cancel the settings, click the Reset button to revert to previously saved values.

Figure 2-13.2.3: MLD Snooping Port Filtering Profile Configuration



Parameter descriptions:

Port : The logical port for the settings.

Filtering Profile : Select the IPMC Profile as the filtering condition for the specific port. A summary of the designated profile will be shown by clicking the View button.

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


: List the rules associated with the designated profile.

Buttons:

Apply – Click to save changes.

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

2-14 LLDP

The switch supports the 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. The Link Layer Discovery Protocol (LLDP) is a vendor-neutral Link Layer protocol in the Internet Protocol Suite used by network devices for advertising their identity, capabilities, and neighbors on an 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.

2-14.1 LLDP Configuration

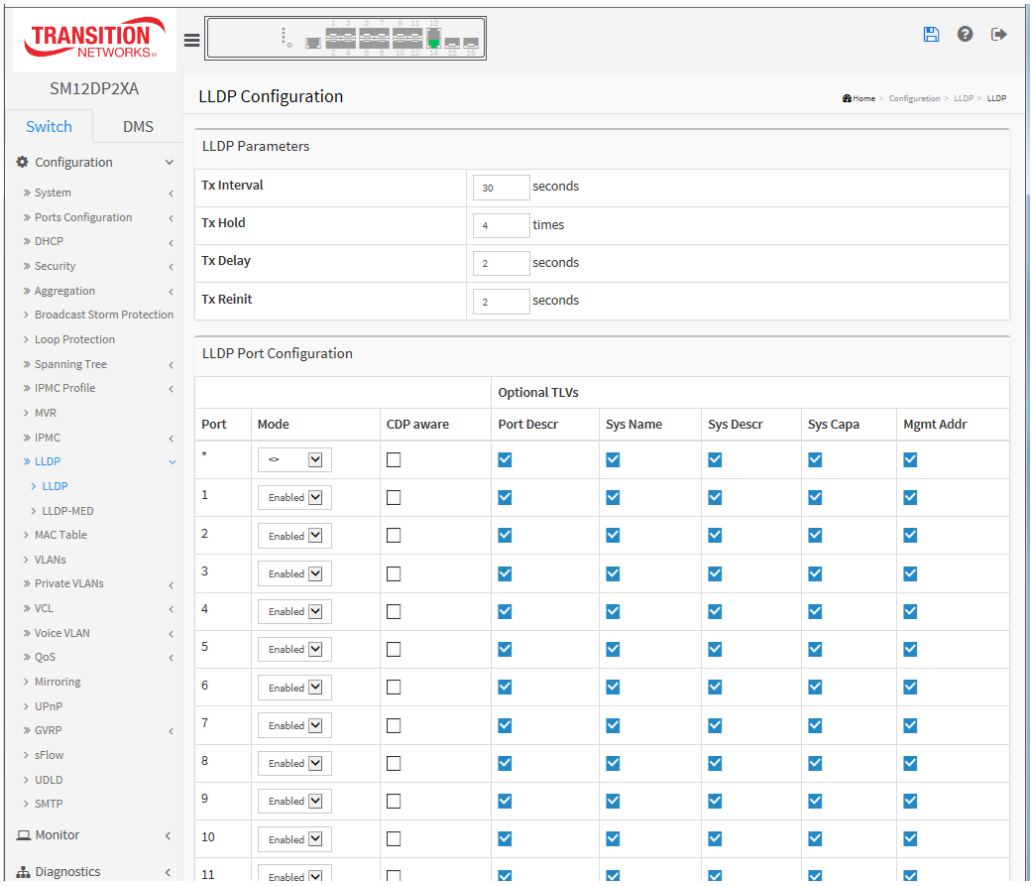
You can set the LLDP configuration and the detail parameters on a per-port basis; the settings will take effect immediately. This page lets you view and configure the current LLDP port settings.

Web Interface

To configure LLDP:

1. Click Configuration, LLDP, LLDP to display the LLDP Configuration table.
2. Set the LLDP timing parameters.
3. Set the required Mode for transmitting or receiving LLDP messages.
4. Specify the optional information to include in the TLV field of advertised messages.
5. Click Apply.

Figure 2-14.1: LLDP Configuration



Parameter descriptions:

LLDP Parameters

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

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

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

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

LLDP Port Configuration

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

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

Mode : Select the LLDP mode.

> ***Rx only***: The switch will not send out LLDP information, but LLDP information from neighbor units is analyzed.
>
> ***Tx only***: The switch will drop LLDP information received from neighbors, but will send out LLDP information.
>
> ***Disabled***: The switch will not send out LLDP information, and will drop LLDP information received from neighbors.
>
> ***Enabled***: The switch will send out LLDP information, and will analyze LLDP information received from neighbors.

CDP Aware : Select CDP awareness. The CDP operation is restricted to decoding incoming CDP frames (The switch doesn't transmit CDP frames). CDP frames are only decoded if LLDP on the port is enabled. Only CDP TLVs that can be mapped to a corresponding field in the LLDP neighbors' table are decoded. All other TLVs are discarded (Unrecognized CDP TLVs and discarded CDP frames are not shown in the LLDP statistics.). CDP TLVs are mapped onto LLDP neighbors' table as shown below.

> CDP TLV "Device ID" is mapped to the LLDP "Chassis ID" field.
>
> CDP TLV "Address" is mapped to the LLDP "Management Address" field. The CDP address TLV can contain multiple addresses, but only the first address is shown in the LLDP neighbors' table.
>
> CDP TLV "Port ID" is mapped to the LLDP "Port ID" field.
>
> CDP TLV "Version and Platform" is mapped to the LLDP "System Description" field.

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

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

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

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

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

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

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

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

Buttons:

Apply – Click to save changes.

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

2-14.2 LLDP-MED Configuration

Media Endpoint Discovery is an enhancement of LLDP, known as LLDP-MED that provides:

- Auto-discovery of LAN policies (such as VLAN, Layer 2 Priority and Differentiated services (Diffserv) settings) enabling plug and play networking.
- Device location discovery to allow creation of location databases and, in the case of Voice over Internet Protocol (VoIP), Enhanced 911 services.
- Extended and automated power management of Power over Ethernet (PoE) end points.
- Inventory management, allowing network administrators to track their network devices, and determine their characteristics (manufacturer, software and hardware versions, serial or asset number).

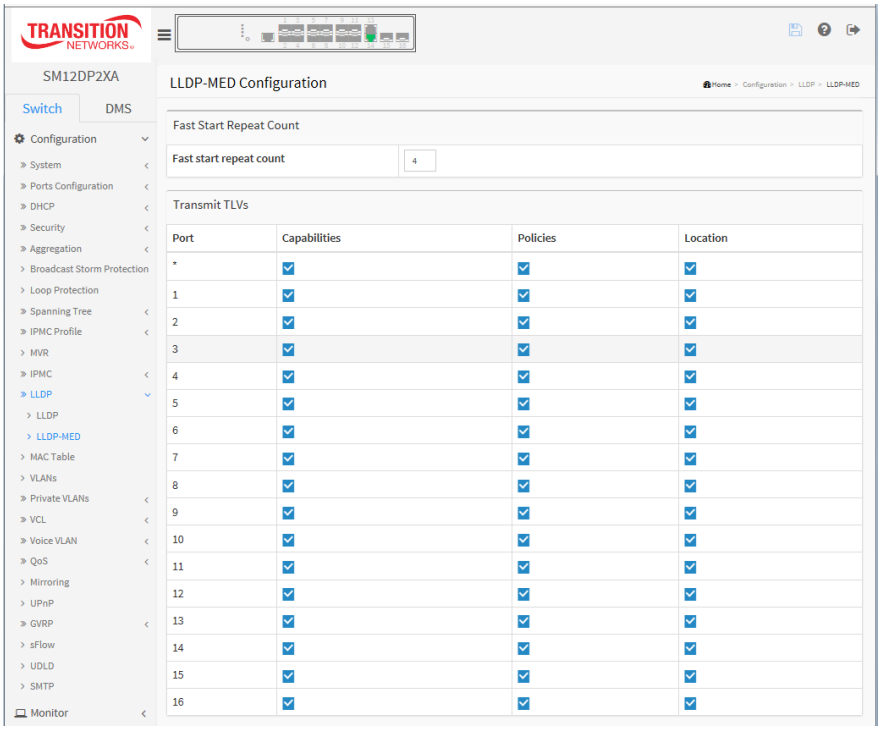
This page lets you configure LLDP-MED parameters that apply to VoIP devices supporting LLDP-MED.

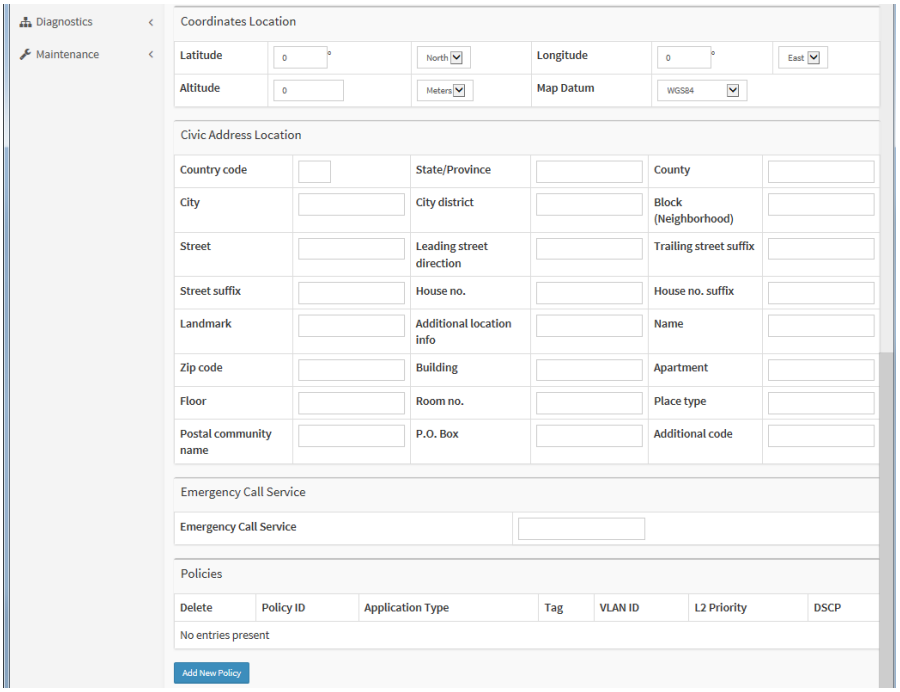
Web Interface

To configure LLDP-MED via the Web UI:

1. Click Configuration, LLDP, LLDP-MED.
2. Set the Fast start repeat count parameter; the default is 4.
3. In the Transmit TLVs section specify the Capabilities, Policies, and Location for each port.
4. Set the Coordinates Location parameters.
5. Enter the Civic Address Location parameters.
6. Enter the Emergency Call Service parameters.
7. Click the Add New Policy button.
8. In the Policies section, enter the Policy ID, Application Type, Tag, VLAN ID, L2 Priority, and DSCP parameters.
9. Click the Apply button to display the Policy Port Configuration table.
10. For each port check or uncheck the Policy ID checkbox.
11. Click the Apply button to save the changes.

Figure 2-14.2: LLDP-MED Configuration





Parameter descriptions:

Fast start repeat count

Rapid startup and Emergency Call Service Location Identification Discovery of endpoints is a critically important aspect of VoIP systems in general. In addition, it is best to advertise only those pieces of information which are specifically relevant to 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 will be transmitted to the neighbors. When the checkbox is checked the information is included in the frame transmitted to the neighbor.

Port : The interface port number 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.

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 media types above)

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

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

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

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

Application Type : At the dropdown select Voice, Voice Signaling, Guest Voice, Guest Voice Signaling, Softphone Voice, Video Conferencing, Streaming Video, or Video Signaling.

Intended use of the application types:

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Port : The port number to which the configuration applies.

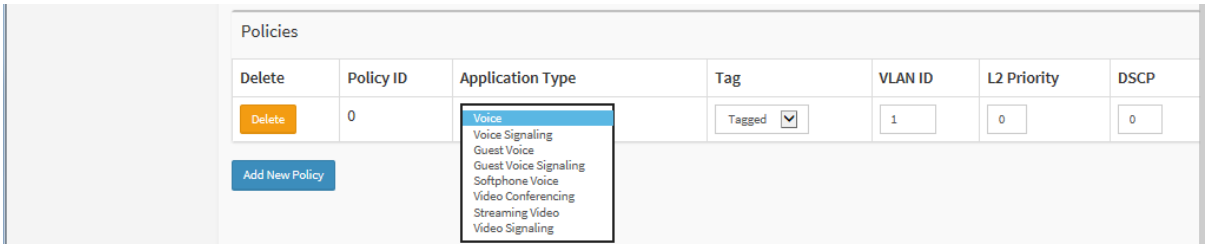
Policy Id : The set of policies that will apply to a given port. The set of policies is selected by check marking the checkboxes that corresponds to the policies.

Buttons:

Apply – Click to save changes.

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

Add New Policy : Click to add a new policy. Specify the Application type, Tag, VLAN ID, L2 Priority and DSCP for the new policy. Click Apply.



2-15 MAC Table

Switching of frames is based upon the DMAC address contained in the frame. The switch builds up a table that maps MAC addresses to switch ports for knowing which ports the frames should go to (based on the DMAC address in the frame). This table contains both static and dynamic entries. The static entries are configured by the network administrator if the administrator wants to do a fixed mapping between the DMAC address and switch ports.

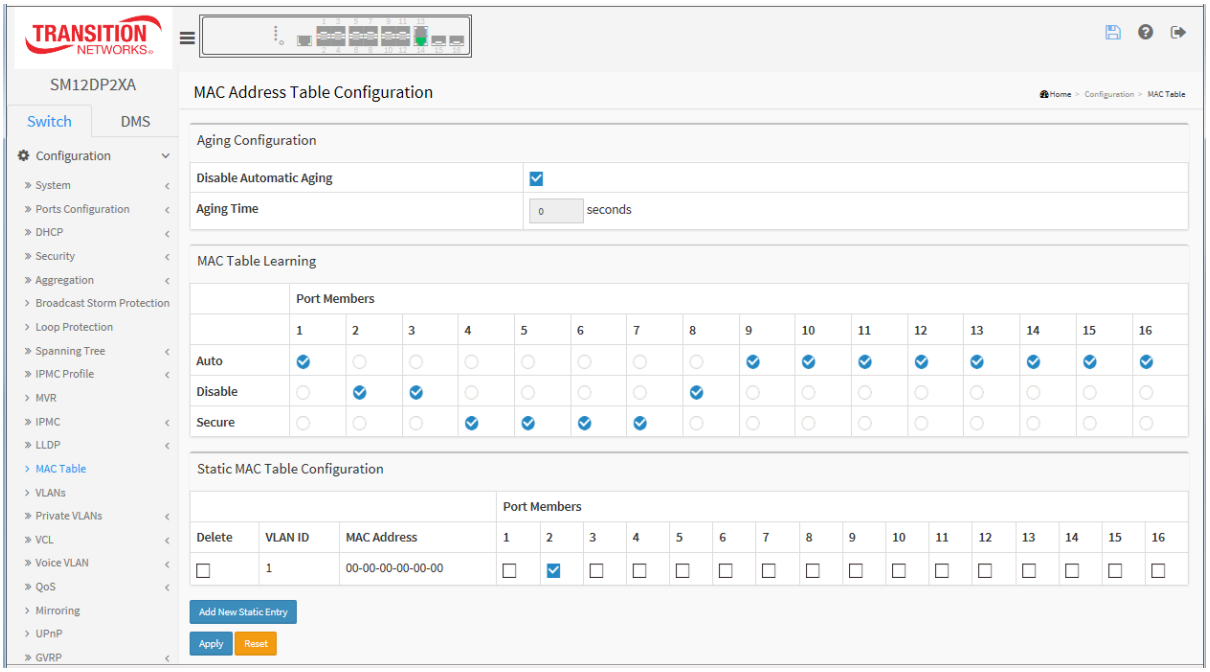
The frames also contain a MAC address (SMAC address), which shows the MAC address of the equipment sending the frame. The SMAC address is used by the switch to automatically update the MAC table with these dynamic MAC addresses. Dynamic entries are removed from the MAC table if no frame with the corresponding SMAC address has been seen after a configurable age time.

Web Interface

To configure MAC Address Table in the web interface:

1. Navigate to Configuration > MAC Table.
2. Enter the Aging Configuration parameters.
3. In the MAC Table Learning section, select Auto, Disable, or Secure for the Port Members.
4. Click the Add New Static Entry button and enter Static MAC Table Configuration parameters.
5. Click Apply.

Figure 2-15: MAC Address Table Configuration



Parameter descriptions:

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

MAC Table Learning : If the learning mode for a given port is greyed out, another module is in control of the mode, so that you cannot change it. 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.

Buttons:

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

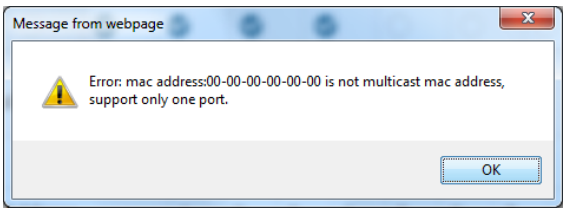
Apply – Click to save changes.

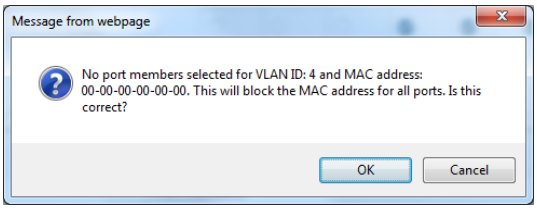
Reset- Click to undo any changes made locally and revert to previously-saved values.

Message: *Error: mac address:00-00-00-00-00-00 is not multicast mac address, support only one port.*

Recovery:

1. Click **OK** to close the webpage message.
2. Make sure you have checked a single Port Member in the Static MAC Table Configuration section.
3. Click Apply.





Message: *No port members selected for VLAN ID: 4 and MAC address 00-00-00-00-00-00. This will block the MAC address for all ports. Is this correct?*

Recovery:

1. Click **OK** to close the webpage message and continue or click **Cancel** and return to Static MAC Table Configuration.

2-16 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.

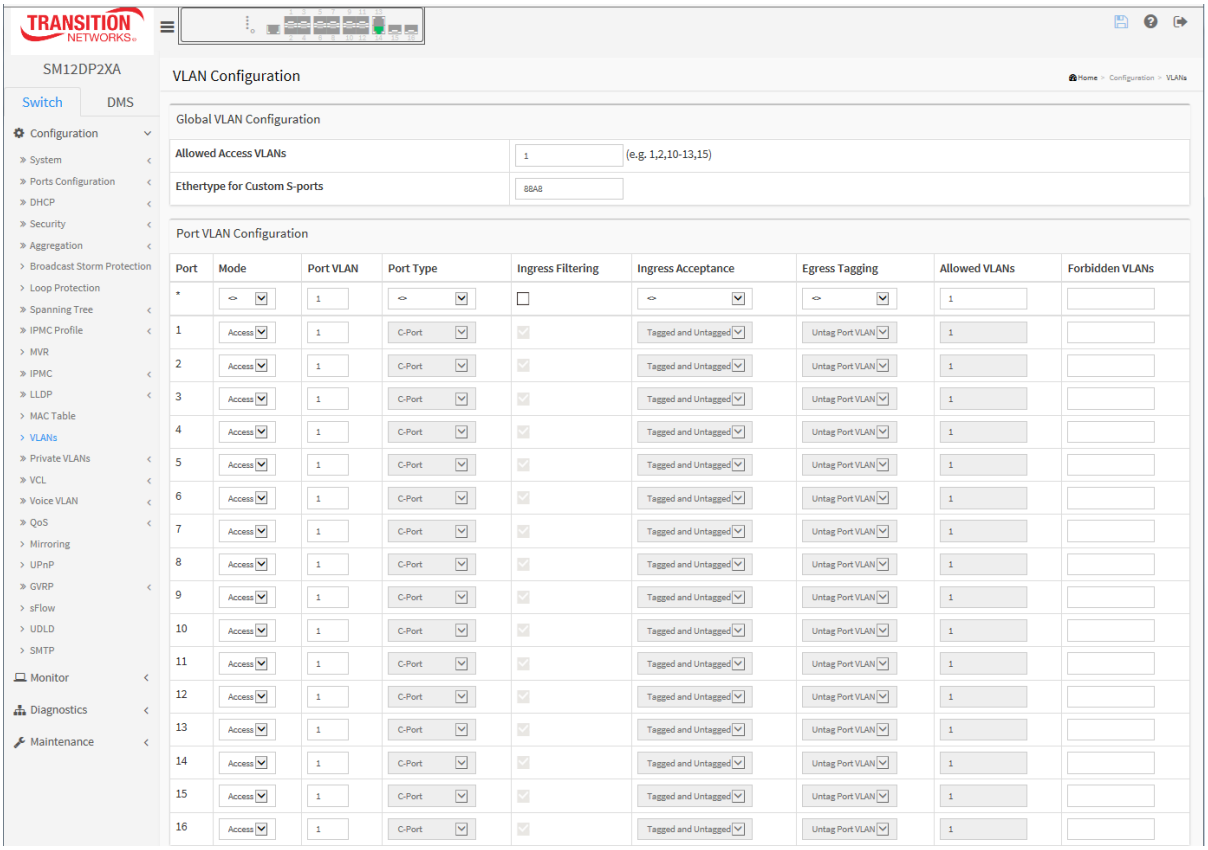
When you specify a new management VLAN, your HTTP connection to the old management VLAN is lost. For this reason, you should have a connection between your management station and a port in the new management VLAN or connect to the new management VLAN through a multi-VLAN route.

Web Interface

To configure VLANs in the web interface:

1. Click Configuration, VLANS.
2. Specify Allowed Access VLANs and Ethertype for Custom S-ports.
3. Specify the Port VLAN Configuration parameters.
4. Click Apply.

Figure 2-16.1: VLAN Configuration



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

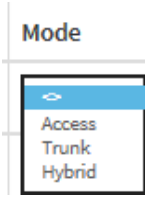
bound. The following example will create VLANs 1, 10, 11, 12, 13, 200, and 300: **1,10-13,200,300**. Spaces are allowed between the delimiters.

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 determines the fundamental behavior of the port in question. A port can be in one of three modes (***Access***, ***Port***, or ***Hybrid***) 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. The default is ***Access*** mode.



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.

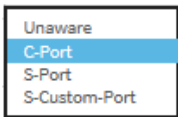
Hybrid: Hybrid ports resemble trunk ports in many ways, but adds additional port configuration features. In addition to the characteristics described for trunk ports, hybrid ports have these abilities:

- 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 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.



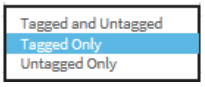
S-Port: On ingress, frames with a VLAN tag with TPID = 0x8100 or 0x88A8 get classified to the VLAN ID embedded in the tag. If a frame is untagged or priority tagged, the frame gets classified to the Port VLAN. If frames must be tagged on egress, they will be tagged with an S-tag.
S-Custom-Port: On ingress,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

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

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

Tagged and Untagged : Both tagged and untagged frames are accepted.
Tagged Only **:** Only tagged frames are accepted on ingress. Untagged frames are discarded.



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

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

Untag Port VLAN**:** Frames classified to the Port VLAN are transmitted untagged. Other frames are transmitted with the relevant tag.
Tag All**:** All frames, whether classified to the Port VLAN or not, are transmitted with a tag.

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

Allowed VLANs : Ports in Trunk and Hybrid mode may control which VLANs they are allowed to become members of. Access ports can only be member of one VLAN, the Access VLAN.
The field's syntax is identical to the syntax used in the Existing VLANs field. By default, a port may become member of all possible VLANs, and is therefore set to **1**-**4095**.

The field may be left empty, which means that the port will not be member of any of the existing VLANs, but if it is configured for VLAN Trunking it will still be able to carry all unknown VLANs.

Forbidden VLANs : A port may be configured to never be member of one or more VLANs. This is particularly useful when dynamic VLAN protocols like MVRP and GVRP must be prevented from dynamically adding ports to VLANs.
The trick is to mark such VLANs as forbidden on the port in question. The syntax is identical to the syntax used in the Existing VLANs field.
By default, the field is left blank, which means that the port may become a member of all possible VLANs.

Buttons:

Apply – Click to save changes.

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

2-17 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.

2-17.1 Private VLAN Membership

The VLAN membership configuration for the switch can be monitored and modified here. Up to 4096 VLANs are supported. This page lets you add and delete VLANs as well as add and delete port members of each VLAN.

Port members of each Private VLAN can be added or removed here. Private VLANs are based on the source port mask, and there are no connections to VLANs. This means that VLAN IDs and Private VLAN IDs can be identical.

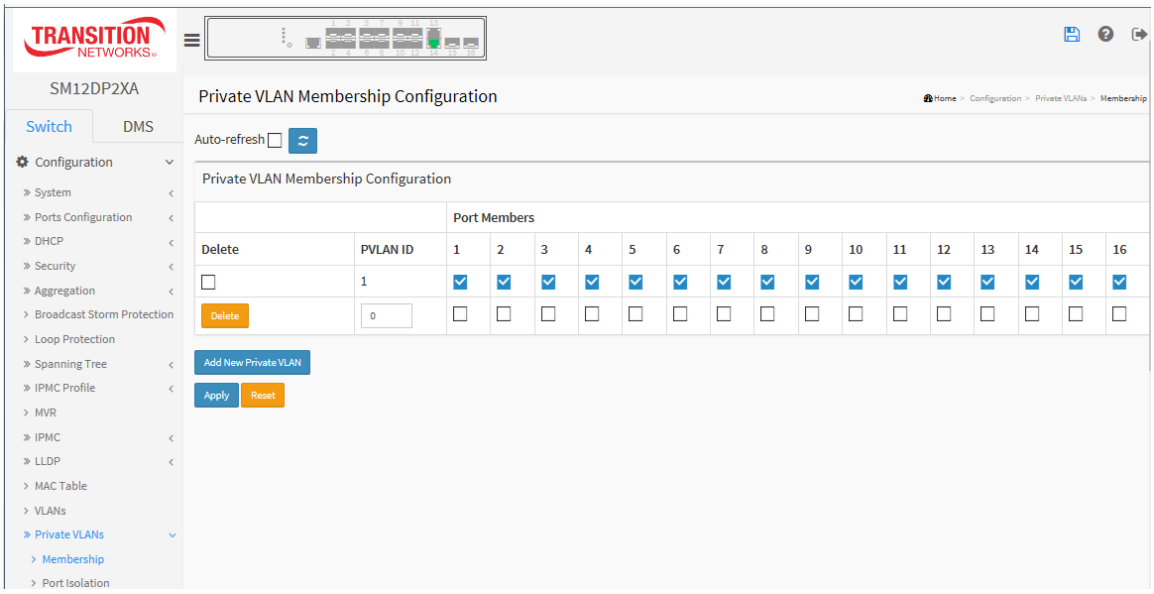
A port must be a member of both a VLAN and a Private VLAN to be able to forward packets.
By default, all ports are VLAN unaware and members of VLAN 1 and Private VLAN 1.
A VLAN unaware port can only be a member of one VLAN, but it can be a member of multiple Private VLANs.

Web Interface

To configure VLAN membership configuration in the web interface:

1. Click Configuration > Private VLANs > Membership.
2. Specify Management VLAN ID (2 – 4094).
3. Click Add New Private VLAN.
4. Select the desired Port Members.
5. Click Apply.

Figure 2-17.1: VLAN Membership Configuration



Parameter descriptions:

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

PVLAN ID : Enter the ID of this particular private VLAN (1-16).

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.

Buttons:

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

Apply – Click to save changes.

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

2-17.2 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.

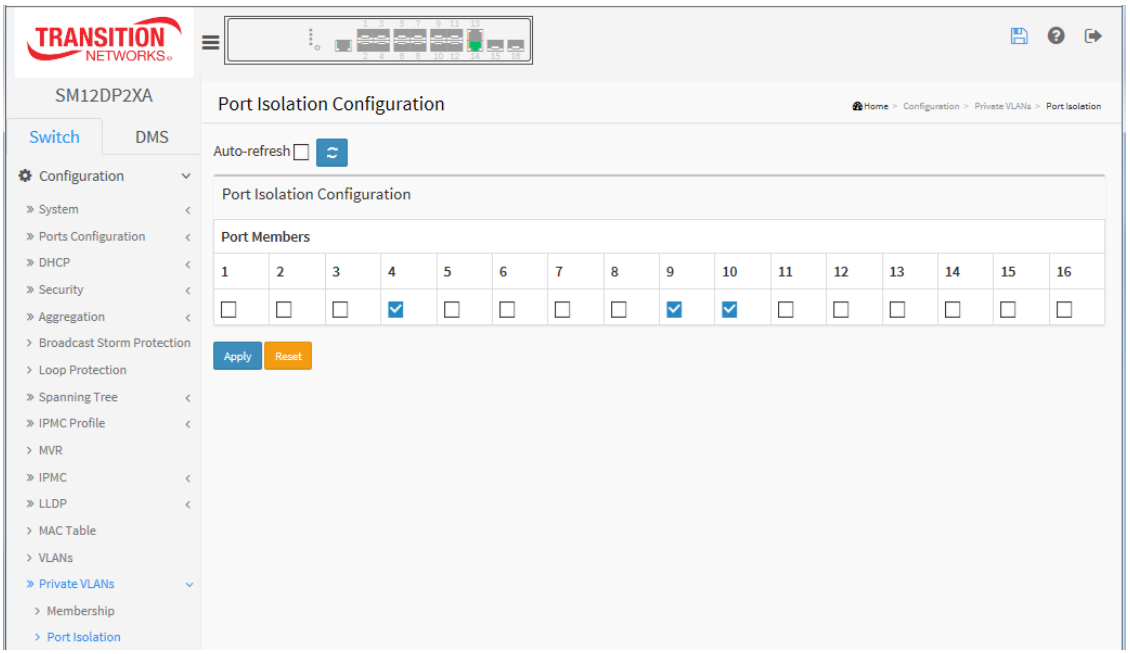
This page is used for enabling or disabling port isolation on ports in a Private VLAN. A port member of a VLAN can be isolated to other isolated ports on the same VLAN and Private VLAN.

Web Interface

To configure Port Isolation configuration in the web interface:

1. Click Configuration, Private VLANs, Port Isolation.
2. Select the ports you want to enable Port Isolation.
3. Click Apply.

Figure 2-17.2: Port Isolation Configuration



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.

2-18 VCL

The switch supports three types of VCLs (VLAN Control Lists): MAC-based, Protocol-based, and IP Subnet-based VCLs.

2-18.1 MAC-based VLAN

A 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. To provide user access and ensure data security in the meantime, the MAC-based VLAN technology was developed.

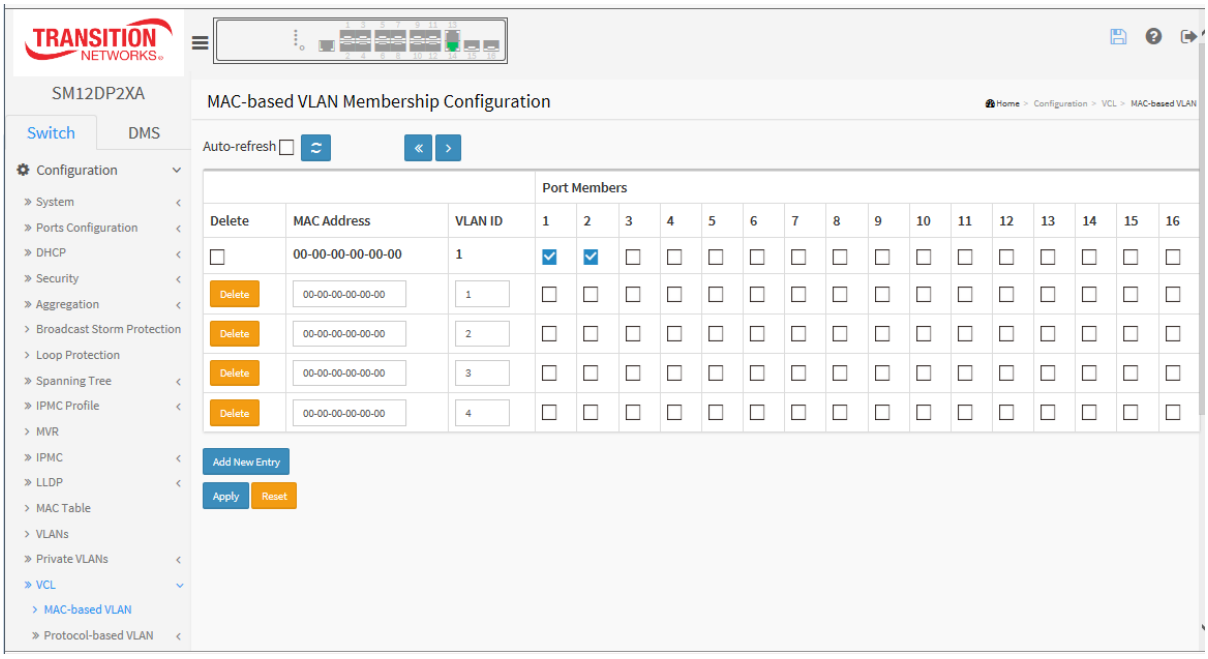
MAC-based VLANs group VLAN members by MAC address. With MAC-based VLAN configured, the device adds a VLAN tag to an untagged frame according to its source MAC address. MAC-based VLANs are mostly used in conjunction with security technologies such as 802.1X to provide secure, flexible network access for terminal devices.

Web Interface

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

1. Click Configuration, VLC, MAC-based VLAN.
2. Click Add New Entry.
3. Specify the MAC address and VLAN ID.
4. Check the desired Port Member checkboxes.
5. Click Apply.

Figure 2-18.1: MAC-based VLAN Membership Configuration



Parameter descriptions:

Delete : To delete a MAC-based VLAN entry, check this box and click Apply. The entry will be deleted on the switch.

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:

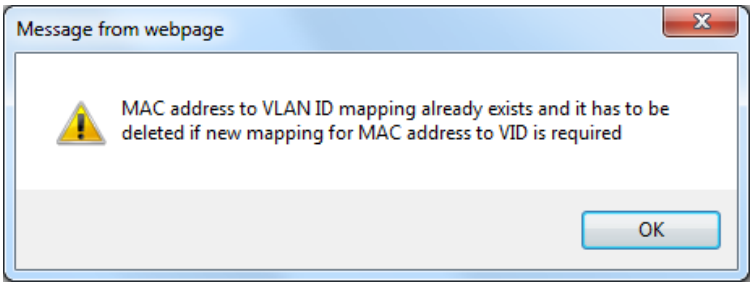
Add New Entry : Click to add a new MAC-based VLAN entry. An empty row is added to the table, and the MAC-based VLAN entry can be configured as needed. Any unicast MAC address can be configured for the MAC-based VLAN entry. No broadcast or multicast MAC addresses are allowed. Legal values for a VLAN ID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

Apply – Click to save changes.

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

Message: *MAC address to VLAN ID mapping already exists and it has to be deleted if new mapping for MAC address to VID is required.*

Recovery: Click **OK** and re-select port members.



2-18.2 Protocol -based VLAN

This page lets you select the Protocol-based VLAN parameters. Switch protocol support includes Ethernet, LLC, and SNAP protocols.

LLC : The Logical Link Control (LLC) data communication protocol layer is the upper sub-layer of the Data Link Layer (which is itself layer 2, just above the Physical Layer) in the seven-layer OSI reference model. It provides multiplexing mechanisms that make it possible for several network protocols (IP, IPX, Decnet and Appletalk) to coexist within a multipoint network and to be transported over the same network media, and can also provide flow control and automatic repeat request (ARQ) error management mechanisms.

SNAP : The Subnetwork Access Protocol (SNAP) is a mechanism for multiplexing, on networks using IEEE 802.2 LLC, more protocols than can be distinguished by the 8-bit 802.2 Service Access Point (SAP) fields. SNAP supports identifying protocols by Ethernet type field values; it also supports vendor-private protocol identifier spaces. It is used with IEEE 802.3, IEEE 802.4, IEEE 802.5, IEEE 802.11 and other IEEE 802 physical network layers, as well as with non-IEEE 802 physical network layers such as FDDI that use 802.2 LLC.

2-17.2.1 Protocol to Group

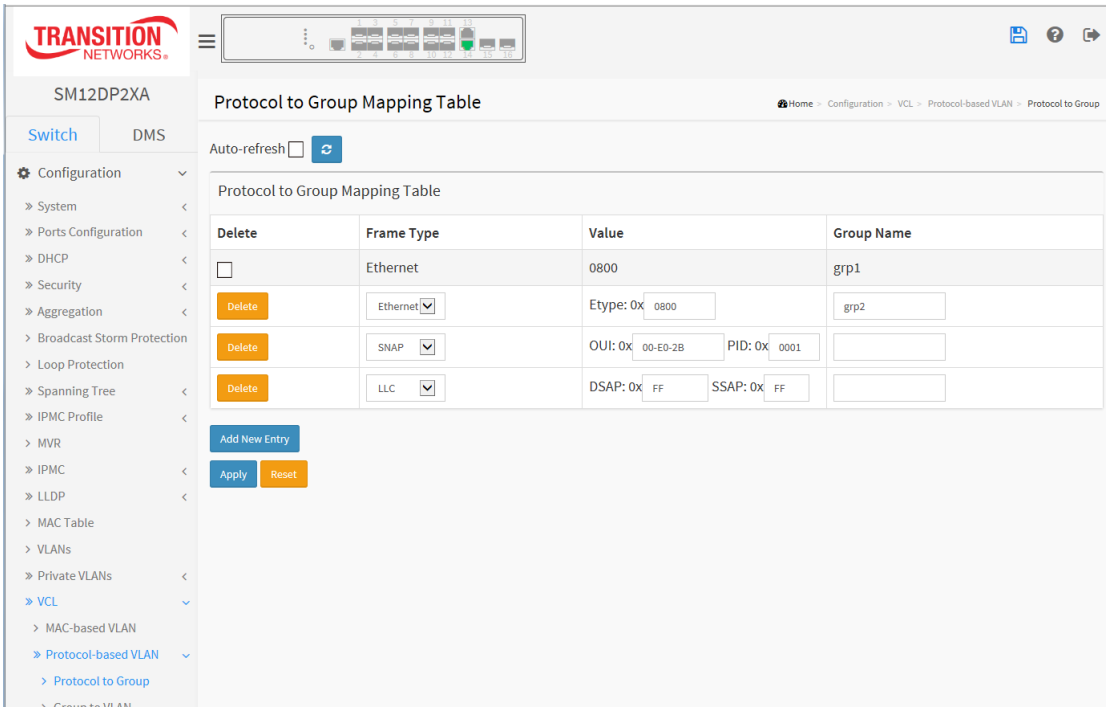
This page allows you to add new protocols to Group Name (unique for each Group) mapping entries as well as allow you to see and delete already mapped entries for the switch.

Web Interface

To configure Protocol-based VLAN parameters via the web interface:

1. Click Configuration > VCL > Protocol-based VLAN > Protocol to Group.
2. Click Add New Entry.
2. Specify the Frame Type, Value, and Group Name.
3. Click Apply.

Figure 2-17.2.1: Protocol to Group Mapping Table



Parameter descriptions:

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

Frame Type : At Frame Type select **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 ranges from 0x00-0xff.
   b. PID: If the OUI is hexadecimal 000000, the protocol ID is the Ethernet type (EtherType) field value for the protocol running on top of SNAP; if the OUI is an OUI for a particular organization, the protocol ID is a value assigned by that organization to the protocol running on top of SNAP. In other words, if value of OUI field is 00-00-00 then value of PID will be etype (0x0600-0xffff) and if value of OUI is other than 00-00-00 then valid value of PID will be any value from 0x0000 to 0xffff.

Group Name : A valid Group Name is a unique 16-character long string for every entry which consists of a combination of alphabets (a-z or A-Z) and integers(0-9).

NOTE: Special character and underscore (_) are not allowed.

Buttons:

Add New Entry : Click to add a new entry in mapping table. An empty row is added to the table; Frame Type, Value and the Group Name can be configured as needed. The Reset button can be used to undo the addition of new entry.

Apply – Click to save changes.

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

Refresh: Click to refresh the Protocol Group Mapping information manually.

2-18.2.2 Group to VLAN

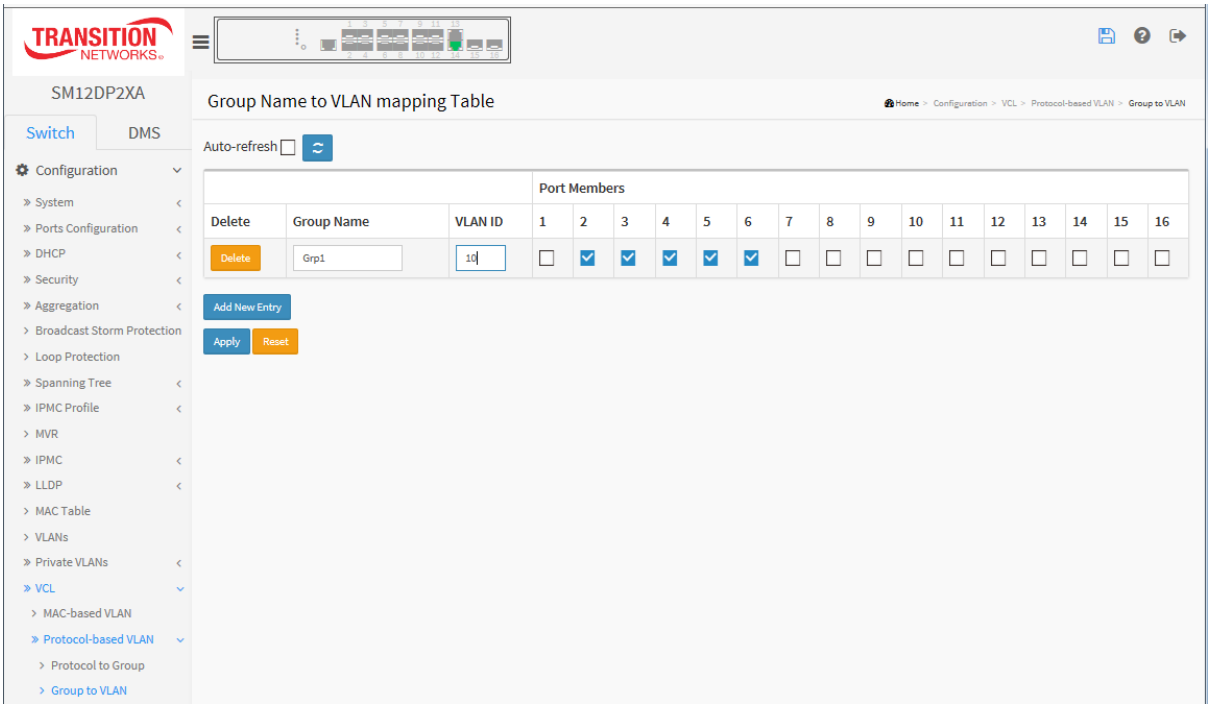
This page lets you map an already configured Group Name to a VLAN for the switch .

Web Interface

To display Group Name to VLAN mapping table configured in the web interface:

1. Click Configuration > VCL > Protocol-based VLAN > Group to VLAN.
2. Click Add New Entry.
3. Specify the Group Name and VLAN ID and check Port Members.
4. Click Apply.

Figure 2-18.2.2: Group Name of VLAN Mapping Table



Parameter descriptions:

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

Group Name : A valid Group Name is a string of at most 16 characters which consists of a combination of alphabet characters (a-z or A-Z) and numbers (0-9), no special characters are allowed. Whichever Group name you try map to a VLAN must be present in Protocol to Group mapping table and must not be already used by any other existing mapping entry on this page.

VLAN ID : Indicates the ID to which Group Name will be mapped. A valid VLAN ID is 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 : Click and the device will refresh the information automatically every 3 seconds.

Refresh : Click to refresh the Protocol Group Mapping information manually.

2-18.3 IP Subnet-based VLAN

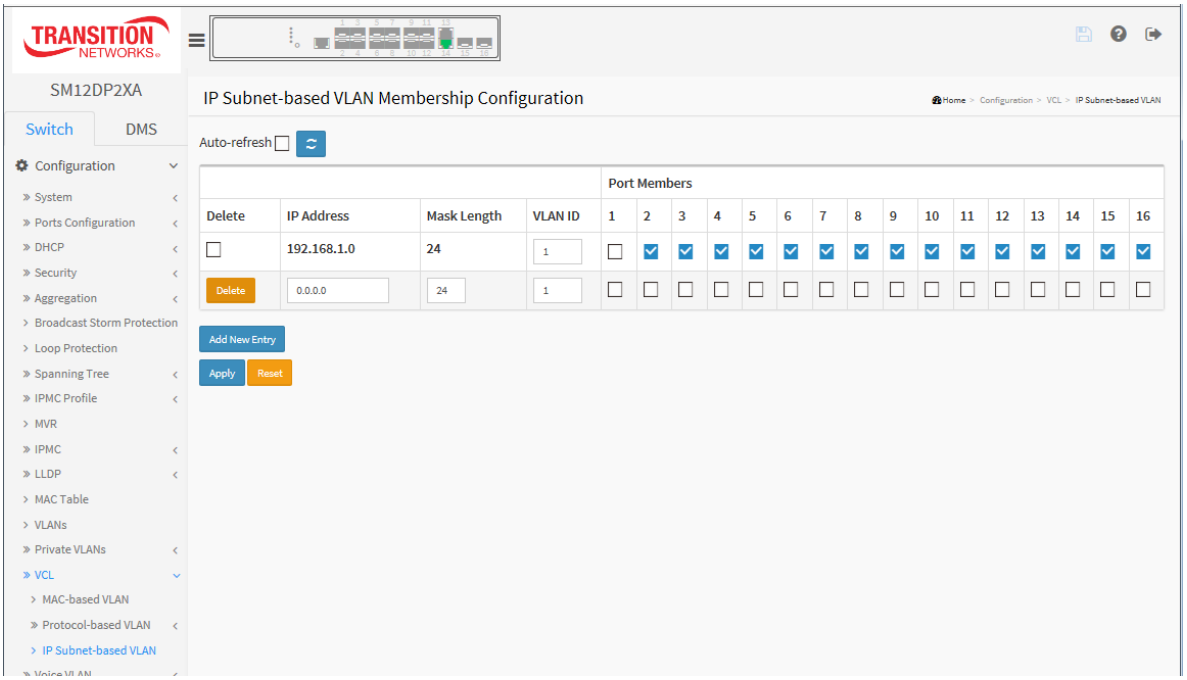
The IP subnet-based VLAN entries can be configured here. This page lets you add, update and delete IP subnet-based VLAN entries and assign the entries to different ports. This page shows only static entries.

Web Interface

To display IP subnet-based VLAN Membership to configured in the web interface:

1. Click Configuration > VCL > IP Subnet-based VLAN.
2. Click Add New Entry.
3. Specify the IP Address, Mask Length, and VLAN ID and select Port Members.
4. Click Apply.

Figure 2-18.3: IP Subnet-based VLAN Membership Configuration



Parameter descriptions:

Delete : To delete an IP subnet-based VLAN entry, check this box and press save. The entry will be deleted on the selected switch.

IP Address : Indicates the IP address.

Mask Length : Indicates the network mask length.

VLAN ID : Indicates the VLAN ID. VLAN ID can be changed for the existing entries.

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

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

The IP subnet-based VLAN entry is enabled on the switch when you click on Save. The Delete button can be used to undo the addition of new IP subnet-based VLANs. The maximum possible IP subnet-based VLAN entries are limited to 128.

2-19 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.

2-18.1 Configuration

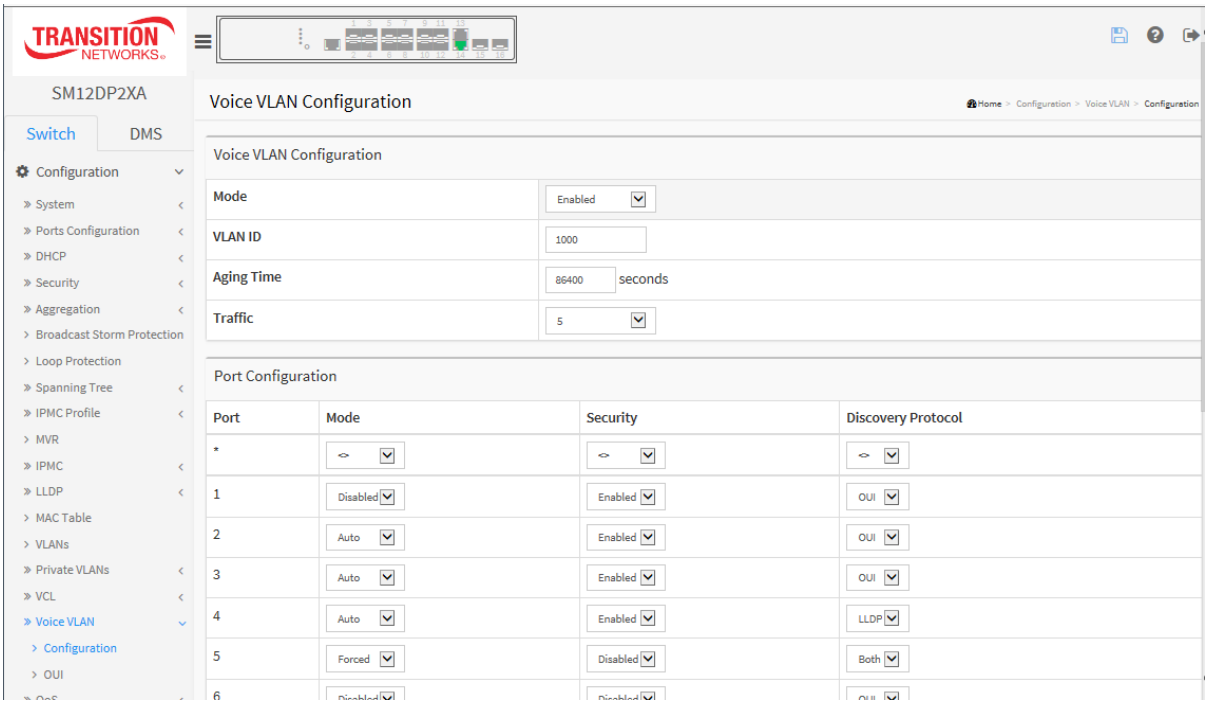
The Voice VLAN feature enables voice traffic forwarding on the Voice VLAN, then the switch can classify and schedule network traffic. It is recommended that there be two VLANs on a port - one for voice, one for data. Before connecting the IP device to the switch, the IP phone should configure the voice VLAN ID correctly. It should be configured via its own GUI.

Web Interface

To configure Voice VLAN in the web interface:

1. Click Configuration > Voice VLAN > Configuration.
2. In the Voice VLAN Configuration section specify Mode (Enabled), VLAN ID, Aging Time, and Traffic Class.
3. In the Port Configuration section specify Mode, Security, and Discovery Protocol for each port.
4. Click Apply.

Figure 2-19.1: Voice VLAN Configuration



Parameter descriptions:

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

Enabled: Enable Voice VLAN mode operation.

Disabled: Disable Voice VLAN mode operation.

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

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

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

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

Disabled: Disjoin from Voice VLAN.

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

Forced: Force join to Voice VLAN.

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

Enabled: Enable Voice VLAN security mode operation.

Disabled: Disable Voice VLAN security mode operation.

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

OUI: Detect telephony device by OUI (Organizationally Unique Identifier.

LLDP: Detect telephony device by LLDP.

Both: Both OUI and LLDP.

Buttons:

Apply – Click to save changes.

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

2-19.2 OUI

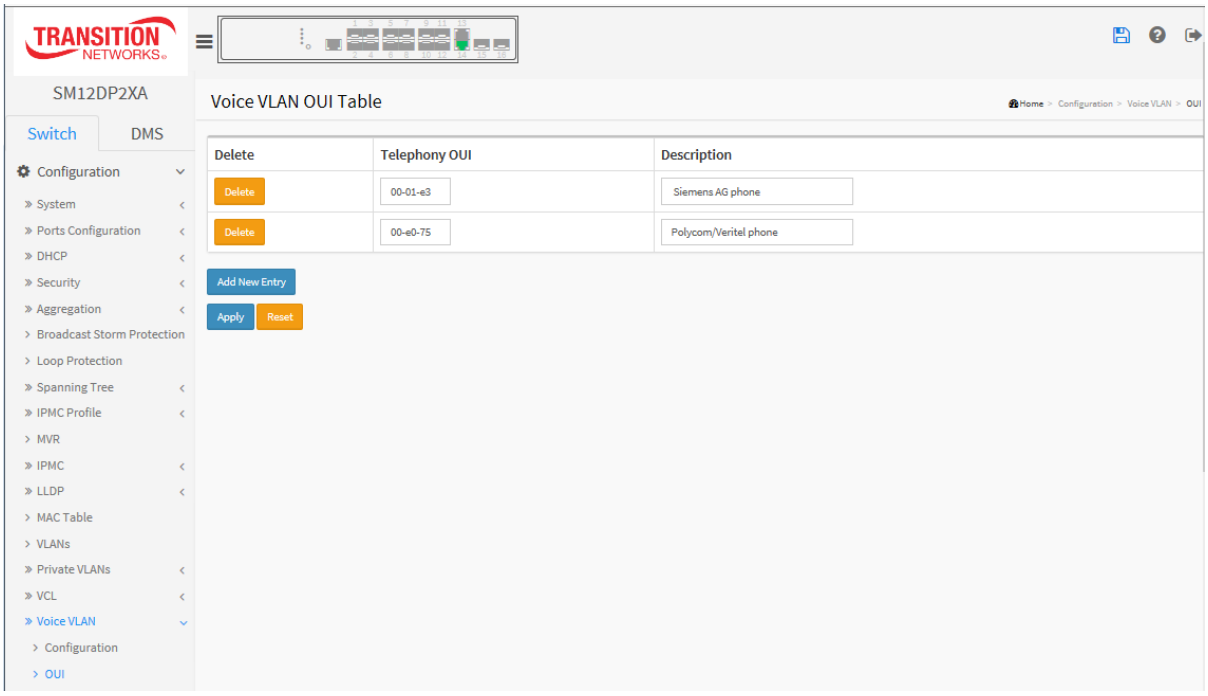
You can configure Voice VLAN OUI parameters on this page. The maximum number of entries is 16. Modifying the OUI table will restart auto detection of the OUI process. An OUI (organizationally unique identifier) address is a globally unique identifier assigned to a vendor by IEEE. You can determine which vendor a device belongs to according to the OUI address which forms the first 24 bits of a MAC address.

Web Interface

To configure Voice VLAN OUI Table in the web interface:

1. Click Configuration > Voice VLAN > OUI.
2. Click Add New Entry.
3. Specify the Telephony OUI and Description in the Voice VLAN OUI table.
4. Click Apply.

Figure 2-19.2: Voice VLAN OUI Table



Parameter descriptions:

Delete : Check to delete the entry during the next save.

Telephony OUI : A telephony OUI address is a globally unique identifier assigned to a vendor by the IEEE. It must be 6 characters long and the input format is "xx-xx-xx" (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.

Buttons:

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

Apply – Click to save changes.

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

2-20 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 a high flexibility in the classification of incoming frames to a QoS class. The QoS classification looks for information up to Layer 4, including IPv4 and IPv6 DSCP, IPv4 TCP/UDP port numbers, and user priority of tagged frames. This QoS classification mechanism is implemented in a QoS control list (QCL). The QoS class assigned to a frame is used throughout the device for providing queuing, scheduling, and congestion control guarantees to the frame according to what was configured for that specific QoS class.

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

2-20.1 Port Classification

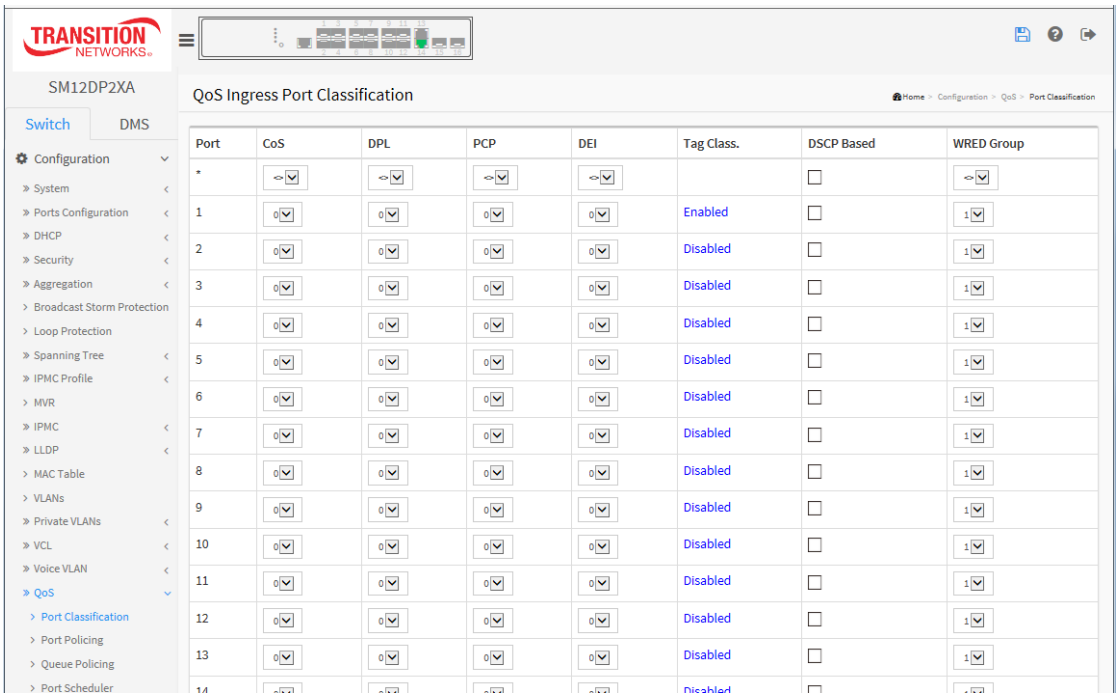
This page lets you configure basic QoS Ingress Classification settings for all switch ports.

Web Interface

To configure the QoS Port Classification parameters in the web interface:

1. Click Configuration, QoS, Port Classification.
2. Select the CoS, DPL, PCP, DEI, Tag Class., DSCP Based, and WRED Group parameters.
3. Click Apply to save the settings.
4. To cancel the settings, click the Reset button to revert to previously saved values.

Figure 2-20.1: QoS Ingress Port Classification



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 QoS class and DP level for tagged frames.

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

Click on the linked Tag Class. mode in order to configure the mode and/or mapping on the Tagged Frames Settings page.

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.

WRED Group : Controls the WRED group membership. Valid values are 1, 2, and 3.

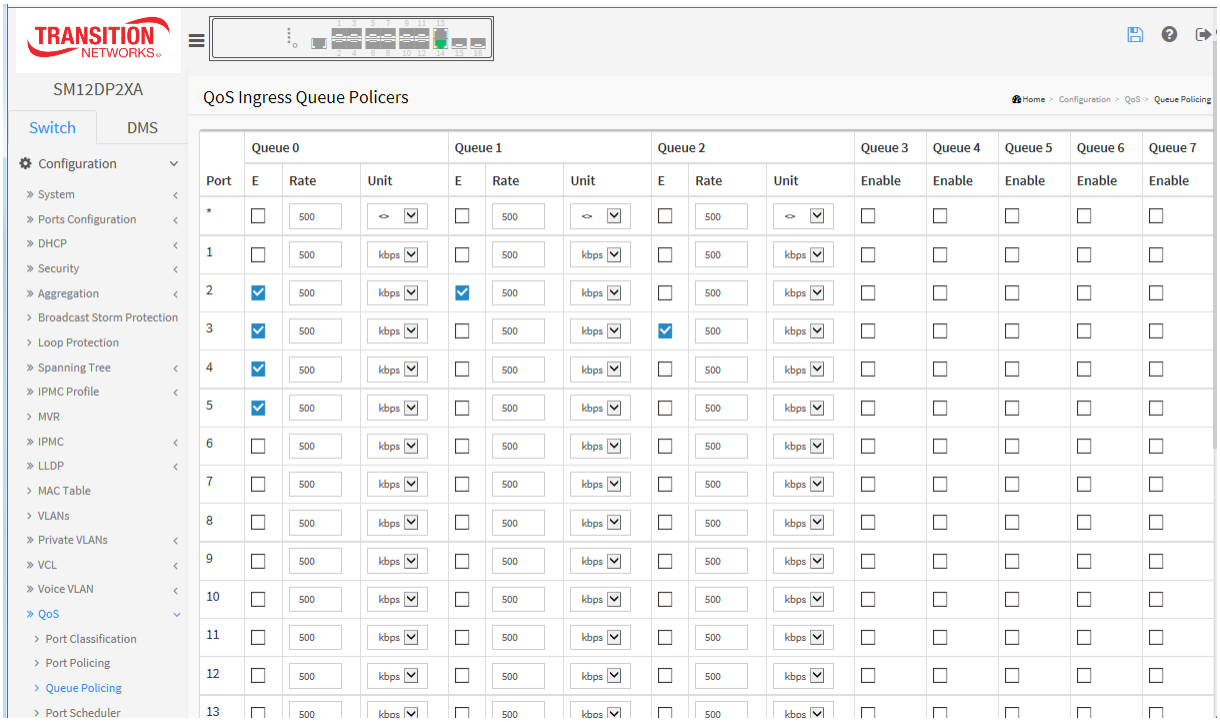
Buttons:

Apply – Click to save changes.

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

At Configuration > QoS > Port Classification click on the linked Tag Class. mode in order to configure the mode and/or mapping on the Tagged Frames Settings page.

Additional fields display only if at least one of the queue policers is enabled on the QoS Ingress Queue Policers page:



2-20.3 Port Policing

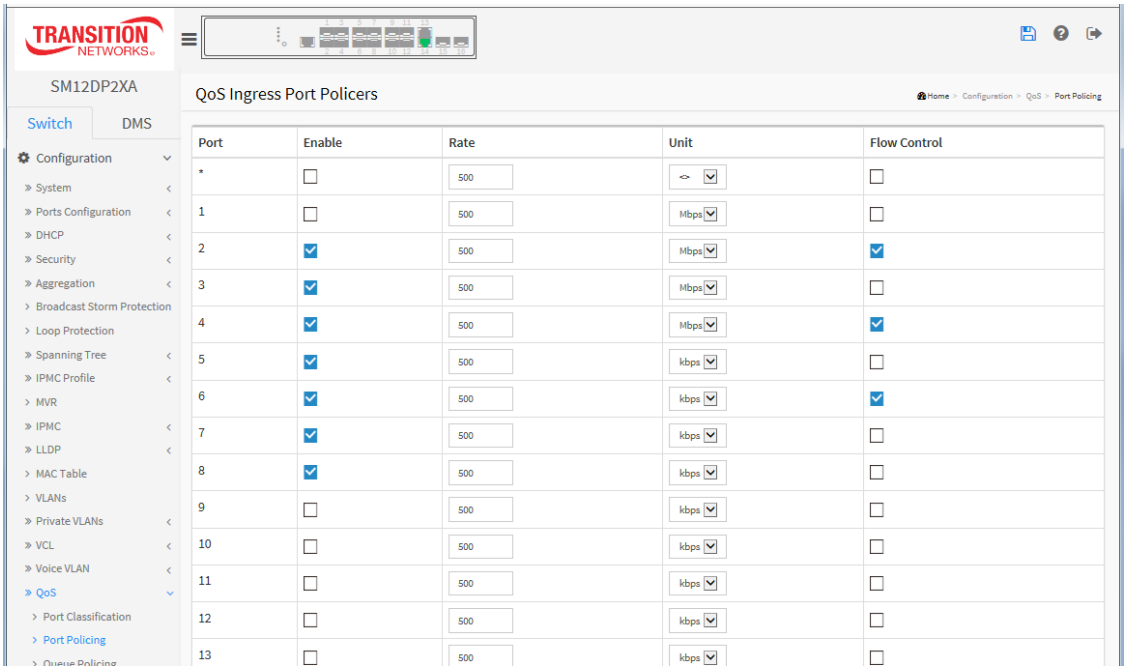
This page provides an overview of QoS Ingress Port Policers for all switch ports. Port Policing is useful in constraining traffic flows and marking frames above specific rates. Policing is primarily useful for data flows and voice or video flows because voice and video usually maintains a steady rate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

Web Interface

To configure the QoS Ingress Port Schedulers via the web interface:

1. Click Configuration, QoS, Port Policing.
2. Enable the QoS Ingress Port Policers and enter the Rate limit.
3. Select the Rate limit Unit with kbps, Mbps, fps and kfps.
4. Click Apply to save the configuration.

Figure 2-20.3: QoS Ingress Port Policers Configuration



Parameter descriptions:

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

Enable : Check the Port(s) on which you want to enable the QoS Ingress Port Policers function.

Rate : Controls the rate for the port policer. This value is restricted to 25-13128147 when "Unit" is kbps , 1-13128 when "Unit" is mbps , 10-5242870 when "Unit" is fps, and 1-5242 when "Unit" is kfps. The rate is internally rounded up to the nearest value supported by the port policer.

Unit : Select the rate unit of measure (kbps, Mbps, fps and kfps). The default is kbps.

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

Buttons:

Apply – Click to save changes.

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

2-20.4 Port Schedulers

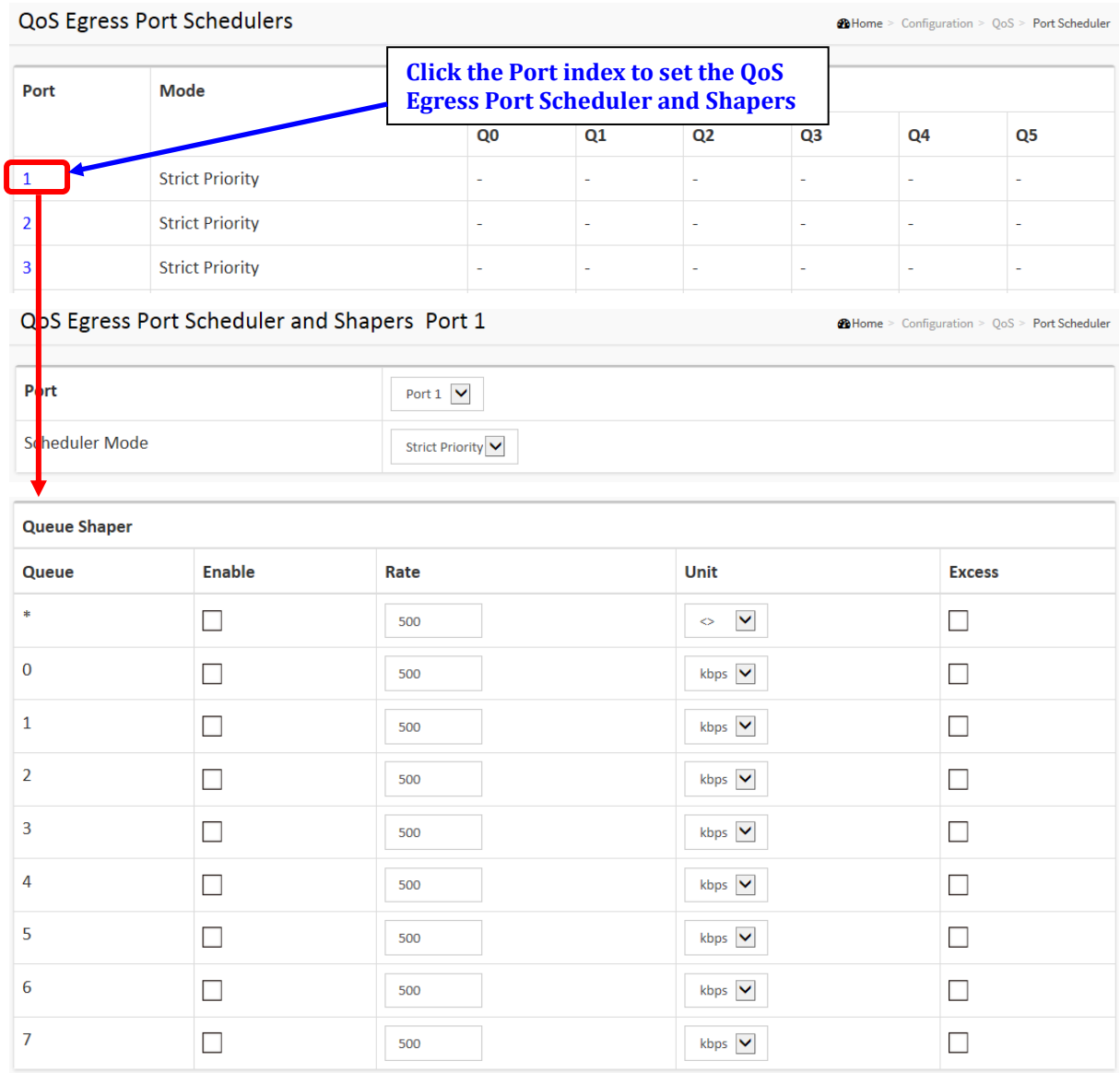
This page provides an overview of QoS Egress Port Schedulers for all switch ports.

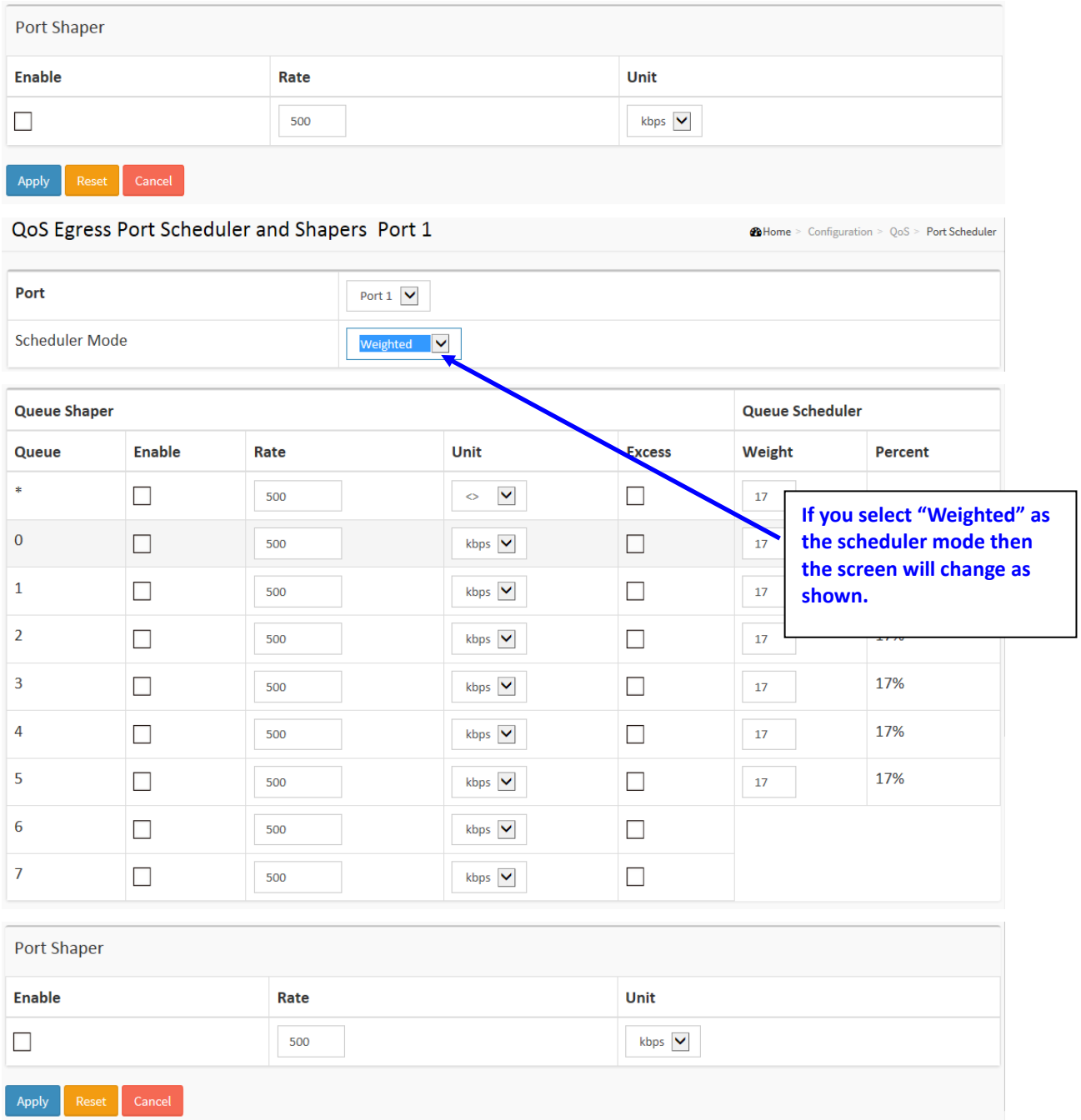
Web Interface

To display and configure the QoS Port Schedulers in the web interface:

1. Click Configuration, QoS, Port Schedulers to display the QoS Egress Port Schedulers table.
2. Click a linked port number to display the QoS Egress Port Scheduler and Shapers table for the selected port.
3. Select the Scheduler Mode and configure the Queue Shaper parameters.
4. Click the Apply button.

Figure 2-20.4: QoS Egress Port Schedulers



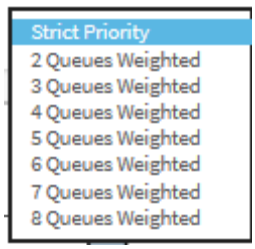


Parameter descriptions:

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

Mode : Shows the scheduling mode for this port.

Weight (Qn) : Shows the weight for this queue and port.



Scheduler Mode : Select the scheduler mode is "Strict Priority" or a number of queues "Weighted" for this switch port.

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

Queue Shaper Rate : Controls the rate for the queue shaper. The default value is 500. This value is

restricted to 100-13107100 when the "Unit" is "kbps", and it is restricted to 1-13107 when the "Unit" is "Mbps.

Queue Shaper Unit : Controls the unit of measure for the queue shaper rate as "kbps" or "Mbps". The default value is "kbps".

Queue Shaper Excess : Controls whether the queue is allowed to use excess bandwidth.

Queue Scheduler Weight : Controls the weight for this queue. The default value is "17". This value is restricted to 1-100. This parameter is only shown if "Scheduler Mode" is set to "Weighted".

Queue Scheduler Percent : Shows the weight in percent for this queue. This parameter is only shown if "Scheduler Mode" is set to "Weighted"

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

Port Shaper Rate : Controls the rate for the port shaper. The default value is 500. This value is restricted to 100-13107100 when the "Unit" is "kbps", and it is restricted to 1-13107 when the "Unit" is "Mbps".

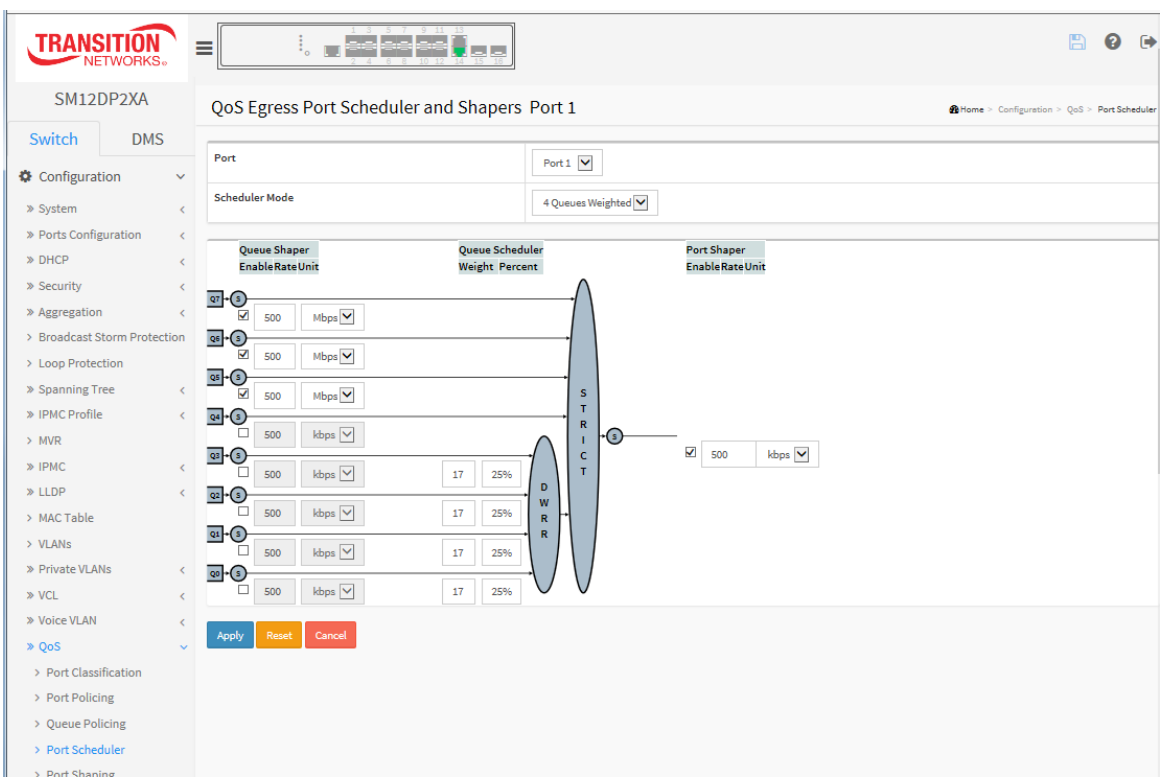
Port Shaper Unit : Controls the unit of measure for the port shaper rate as "kbps" or "Mbps". The default value is "kbps".

Buttons:

Apply – Click to save changes.

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

The example below shows QoS Egress Port Scheduler and Shapers for Port 1, with Scheduler Mode set to "4 Queues Weighted".



2-20.5 Port Shaping

This page provides an overview of QoS Egress Port Shapers for all switch ports.

Web Interface

To display and configure the QoS Port Shapers in the web interface:

1. Click Configuration, QoS, Port Shaping.
2. Click a Port number in the Port column to go to the QoS Egress Port Scheduler and Shapers page for the selected port.
3. Configure the Scheduler Mode, Queue Shaper, Queue Scheduler, and Port Shaper parameters.

Figure 2-20.5: QoS Egress Port Shapers (Strict Priority Mode)

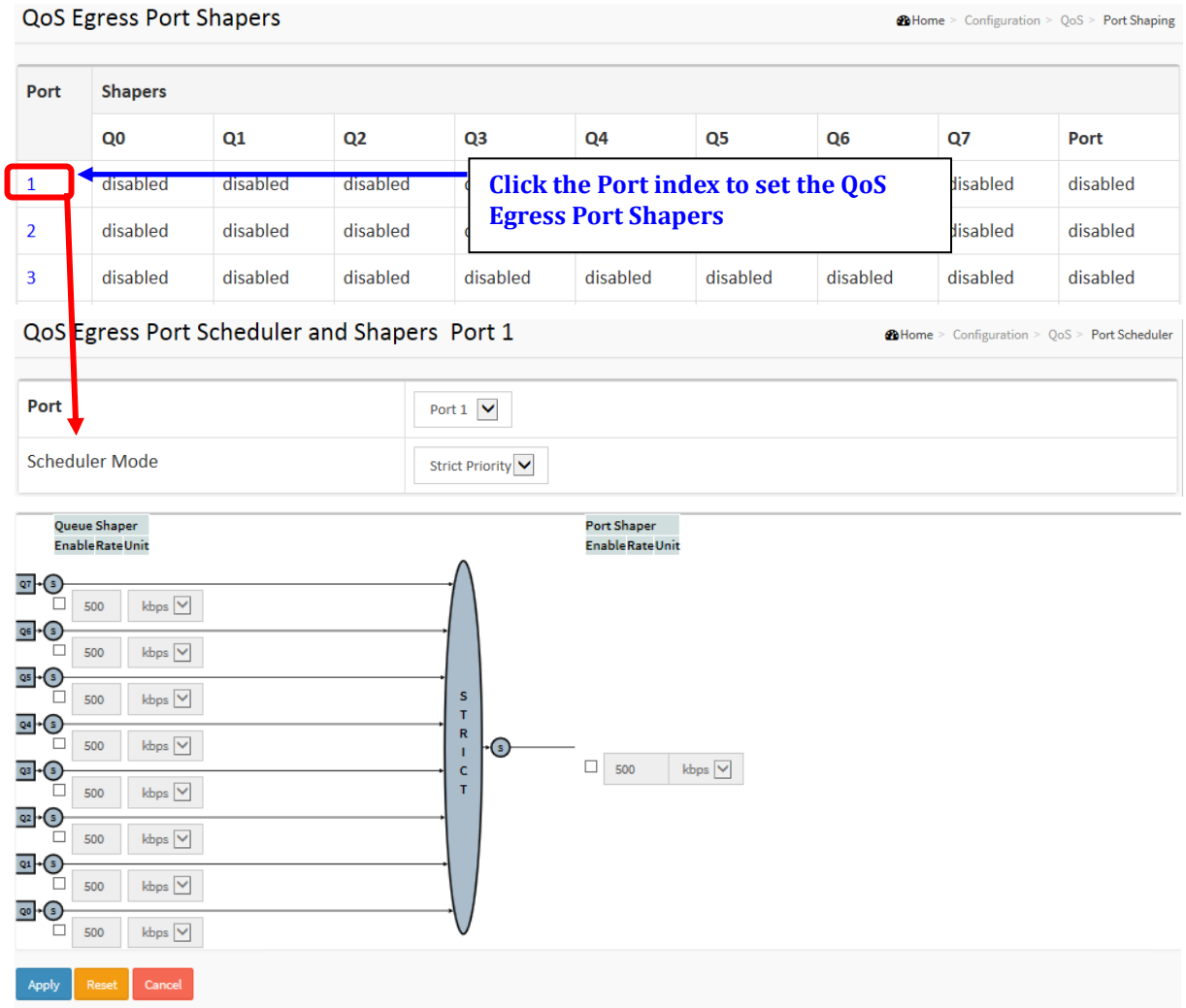
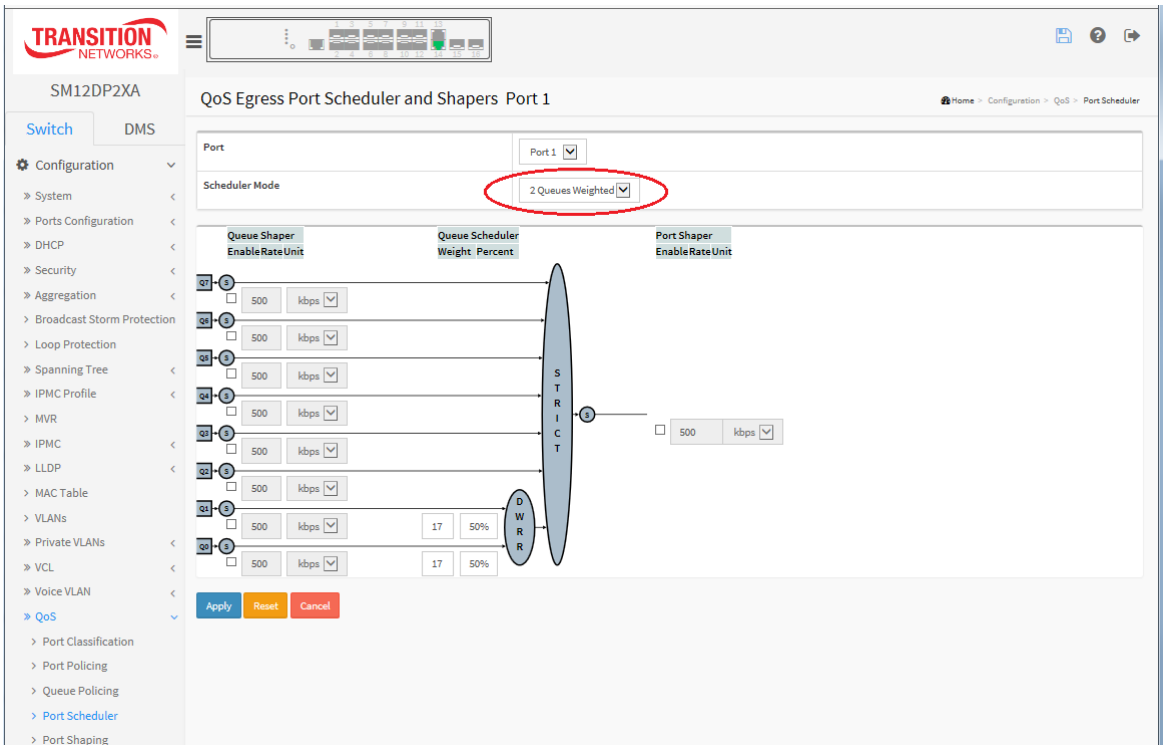


Figure 2-20.5: QoS Egress Port Shapers (2 Queues Weighted Mode)



Parameter descriptions:

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

Scheduler Mode : Lets you select the scheduling mode for this port (Strict Priority, 2 Queues Weighted, 3 Queues Weighted, 4 Queues Weighted, 5 Queues Weighted, 6 Queues Weighted, 7 Queues Weighted, or 8 Queues Weighted).

Queue Shaper

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 100-13107100 when "Unit" is kbps, and 1-13107 when "Unit" is Mbps. The rate is internally rounded up to the nearest value supported by the queue shaper.

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

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

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.

2-20.6 Port Tag Remarking

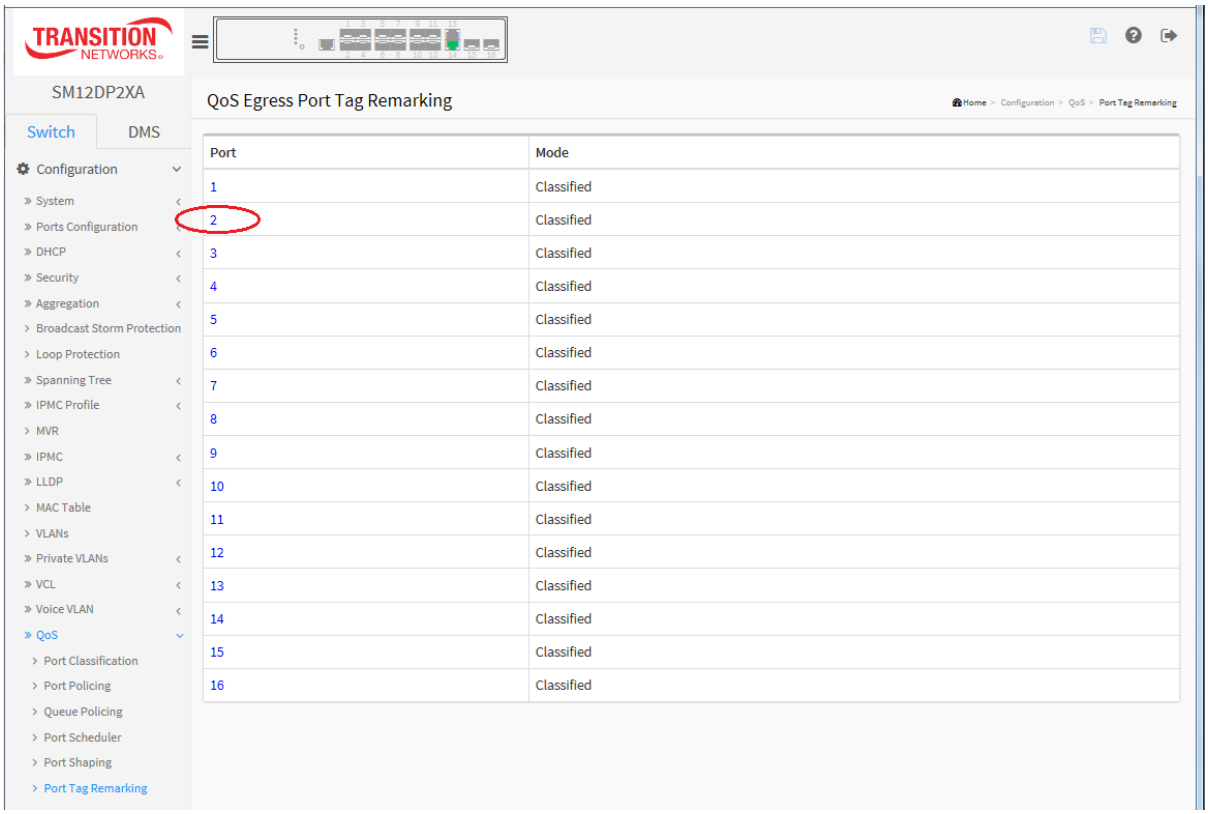
The QoS Egress Port Tag Remarking for a specific port are configured on this page.

Web Interface

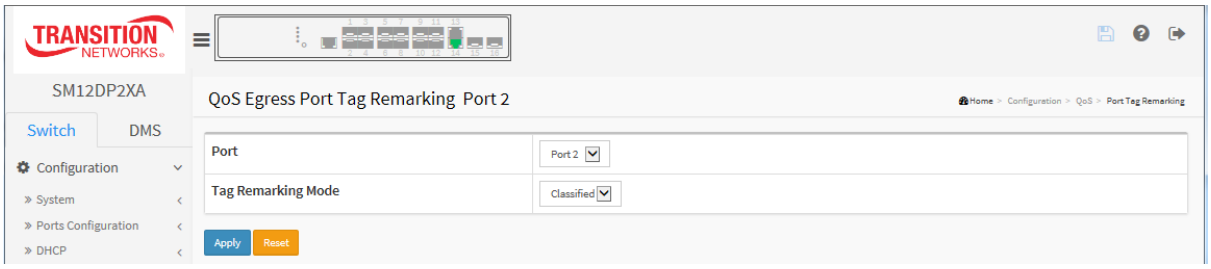
To display the QoS Port Tag Remarking in the web interface:

1. Click Configuration, QoS, Port Tag Remarking.
2. Click the linked Port index to display the QoS Port Tag Remarking page.

Figure 2-20.6: Port Tag Remarking



3. Set the QoS Port Tag Remarking parameters for the selected port (port 2 below).
4. Click the Apply button when done.



Parameter descriptions:

Port : The logical port for the settings contained in the same row. Select the port number in order to configure it.

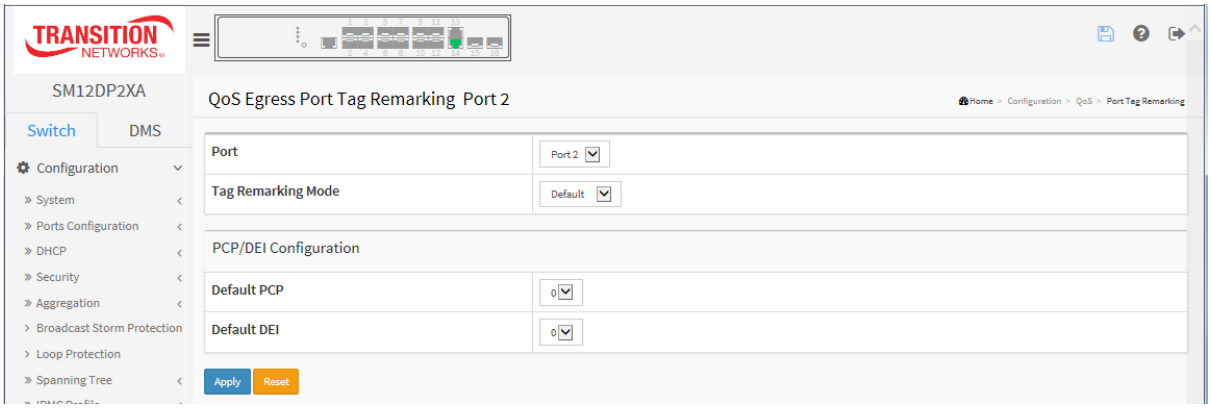
Tag Remarking Mode : Sets the tag remarking mode for this port. The selections are:

Classified: Use classified PCP/DEI values (shown in screen above).

Default: Use default PCP/DEI values.

Mapped: Use mapped versions of QoS class and DP level.

Tag Remarking Mode = Default:

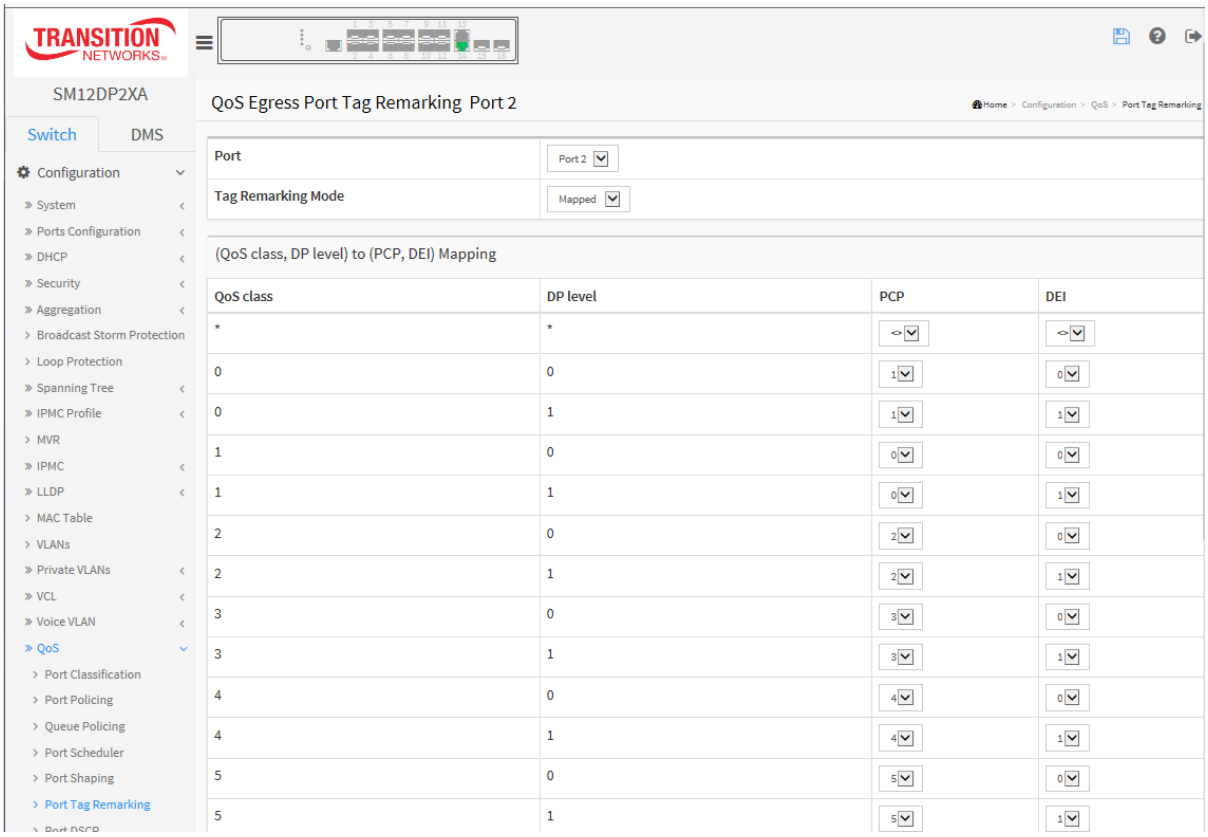


PCP/DEI Configuration :

Default PCP : At the dropdown select 0, 1, 2, 3, 4, 5, 6, or 7 .

Default DEI 01 : At the dropdown select 0 or 1.

Tag Remarking Mode = Mapped:



Port : Select Port 1 - Port 16.
Tag Remarking Mode : Select Classified, Default, or Mapped.

(QoS class, DP level) to (PCP, DEI) Mapping

QoS class : Displays the QoS class (0-7) for this port.

DP level : Displays the DP level (0 or 1) for this port.

PCP : At the dropdown select the PCP (0-7) for this port.

DEI : At the dropdown select the DEI (0 or 1) for this port.

.

2-20.7 Port DSCP

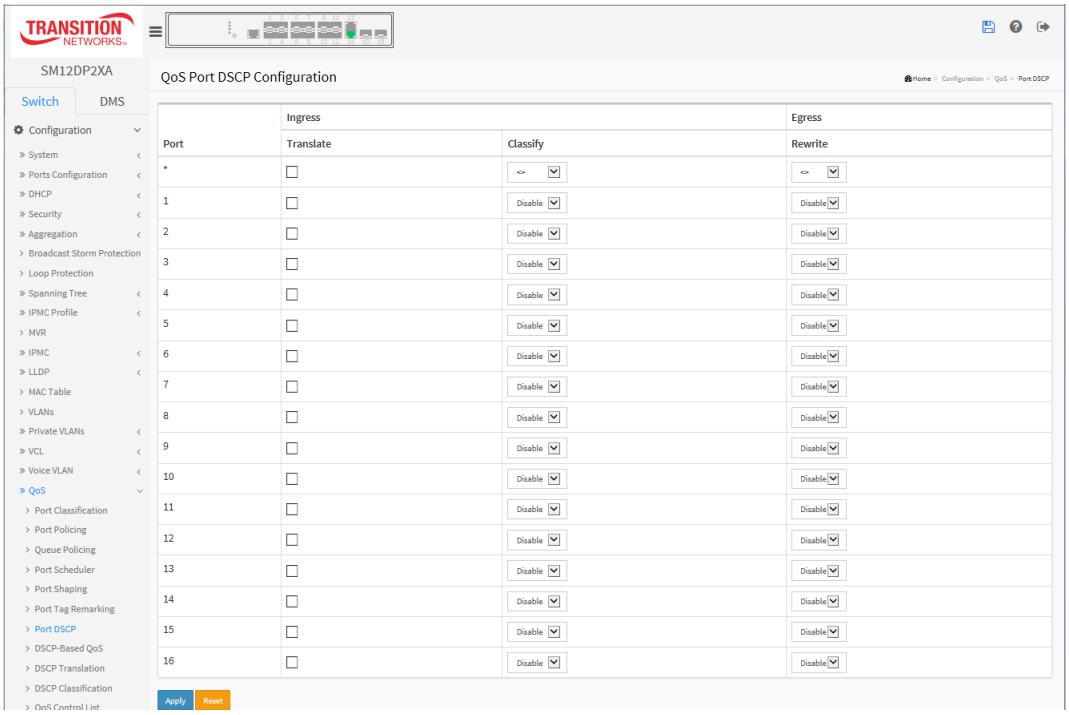
This page lets you configure basic QoS Port DSCP configuration settings for all switch ports.

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.
3. Select Egress Rewrite parameters.
4. Click Apply to save the settings.
5. To cancel the settings, click the Reset button to revert to previously saved values.

Figure 2-20.7: QoS Port DSCP Configuration



Parameter descriptions:

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

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

***Translate* :** To Enable the Ingress Translation click the checkbox

***Classify*:** Classification for a port; one of four different values:

Disable: No Ingress DSCP Classification.

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

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

All: Classify all DSCP.

Egress : Port Egress Rewriting can be one of below 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.

2-20.8 DSCP-Based QoS

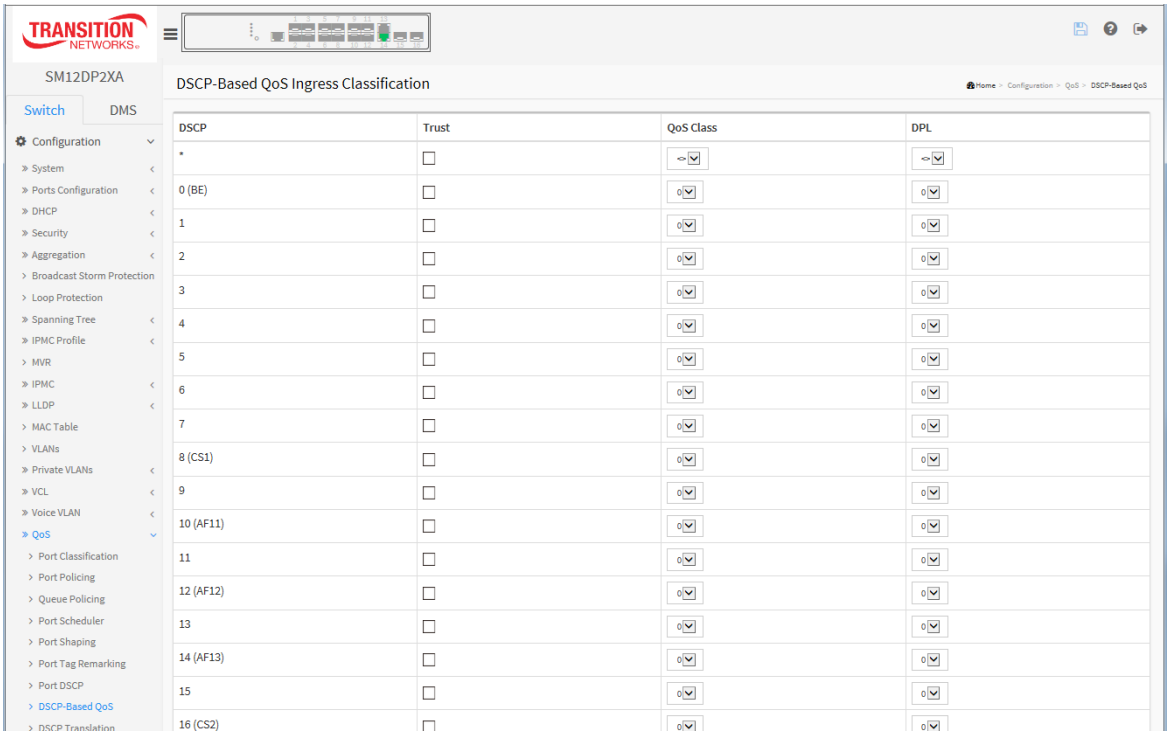
This page lets you configure the basic QoS DSCP based QoS Ingress Classification settings for the switch. DSCP (Differentiated Services Code Point) is a field in the header of IP packets for packet classification purposes.

Web Interface

To configure the DSCP-based QoS Ingress Classification parameters in the web interface:

1. Click Configuration, QoS, DSCP-based QoS.
2. Check or uncheck the Trust checkbox to enable or disable the DSCP for Trust.
3. Select QoS Class and DPL parameters.
4. Click Apply to save the settings,
5. To cancel the settings, click the Reset button to revert to previously saved values.

Figure 2-20.8: DSCP-Based QoS Ingress Classification



Parameter descriptions:

DSCP : Maximum number of supported DSCP values are 64.

Trust : 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 0-7.

DPL : Drop Precedence Level (0-3).

Buttons:

Apply – Click to save changes.

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

2-20.9 DSCP Translation

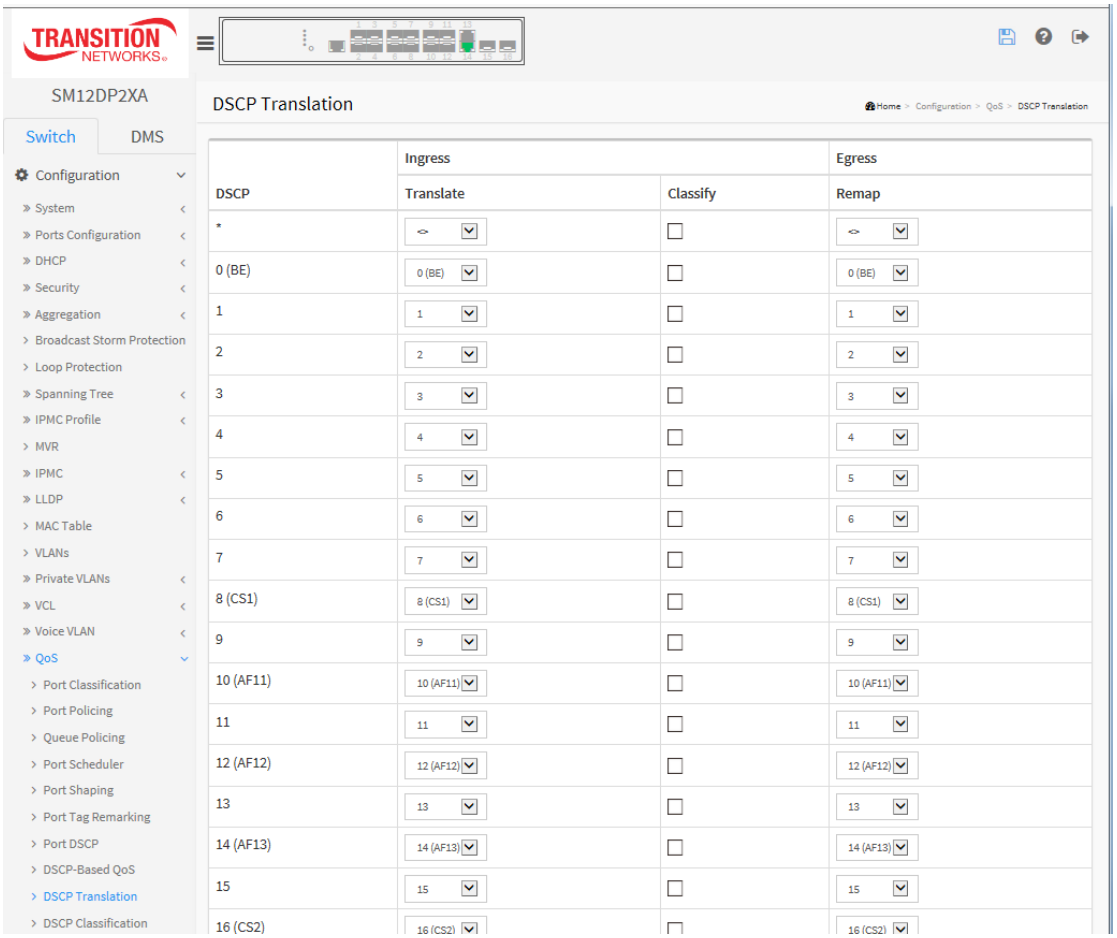
This page lets you configure basic QoS DSCP Translation settings for the switch. DSCP translation can be done at Ingress or Egress.

Web Interface

To configure the DSCP Translation parameters in the web interface:

1. Click Configuration, QoS, DSCP Translation.
2. Select the Ingress Translate and Classify parameters.
3. Select the Egress Remap parameters.
4. Click Apply to save the settings.
5. To cancel the settings, click the Reset button to revert to previously saved values.

Figure 2-20.9: DSCP Translation



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 is one parameters for the Egress side: **Remap**.

Buttons:

Apply – Click to save changes.

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

2-20.10 DSCP Classification

This page lets you configure mapping of QoS class and Drop Precedence Level to DSCP value.

QoS Class : 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) : Every incoming frame is classified to a Drop Precedence Level (DP level), which is used throughout the device for providing congestion control guarantees to the frame according to what was configured for that specific DP level. A DP level of 0 (zero) corresponds to 'Committed' (Green) frames and a DP level of 1 corresponds to 'Discard Eligible' (Yellow) frames.

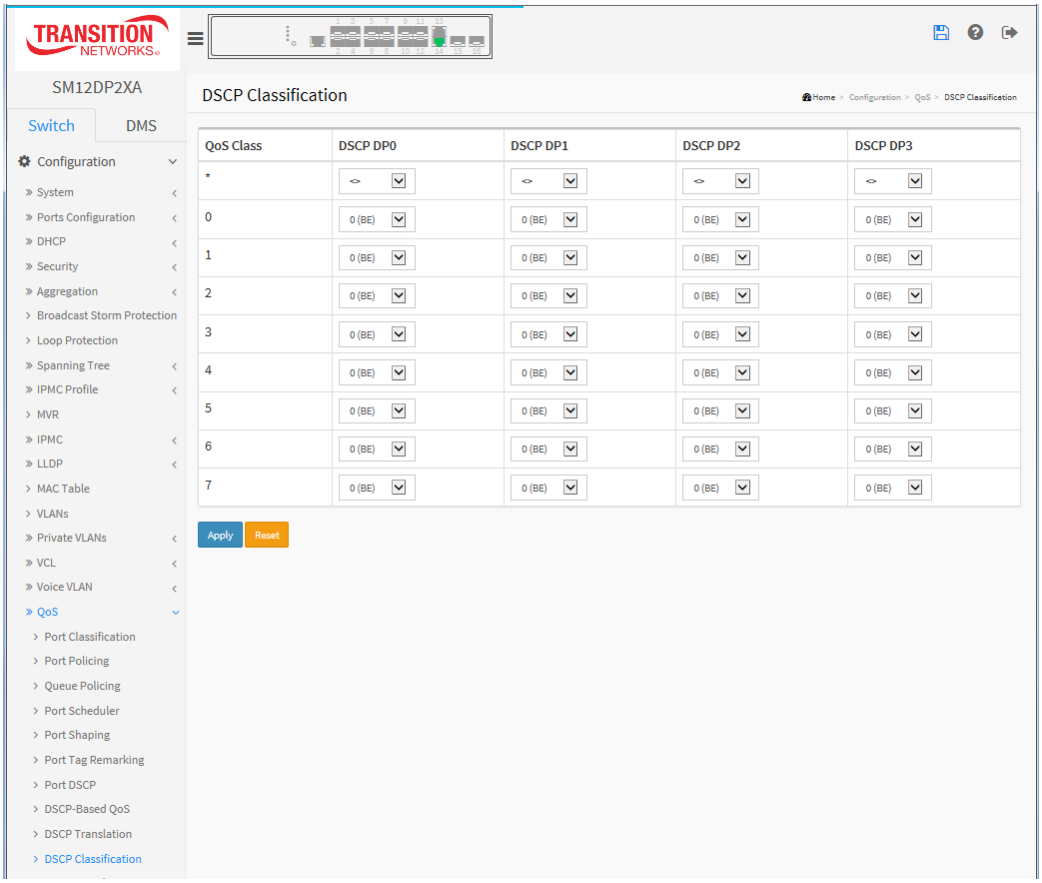
DSCP (Differentiated Services Code Point) is a field in the header of IP packets for packet classification purposes.

Web Interface

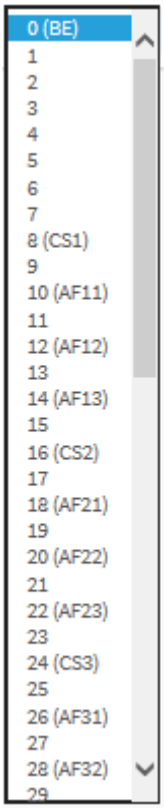
To configure the DSCP Classification parameters in the web interface:

1. Click Configuration, QoS, DSCP Classification.
2. Set the DSCP parameters.
3. Click Apply to save the settings.
4. To cancel the settings click the Reset button to revert to previously saved values.

Figure 2-20.9: DSCP Classification



Parameter descriptions:



QoS Class : The actual QoS class (0-7).

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

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

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

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

Buttons:

Apply – Click to save changes.

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

.

2-20.11 QoS Control List Configuration

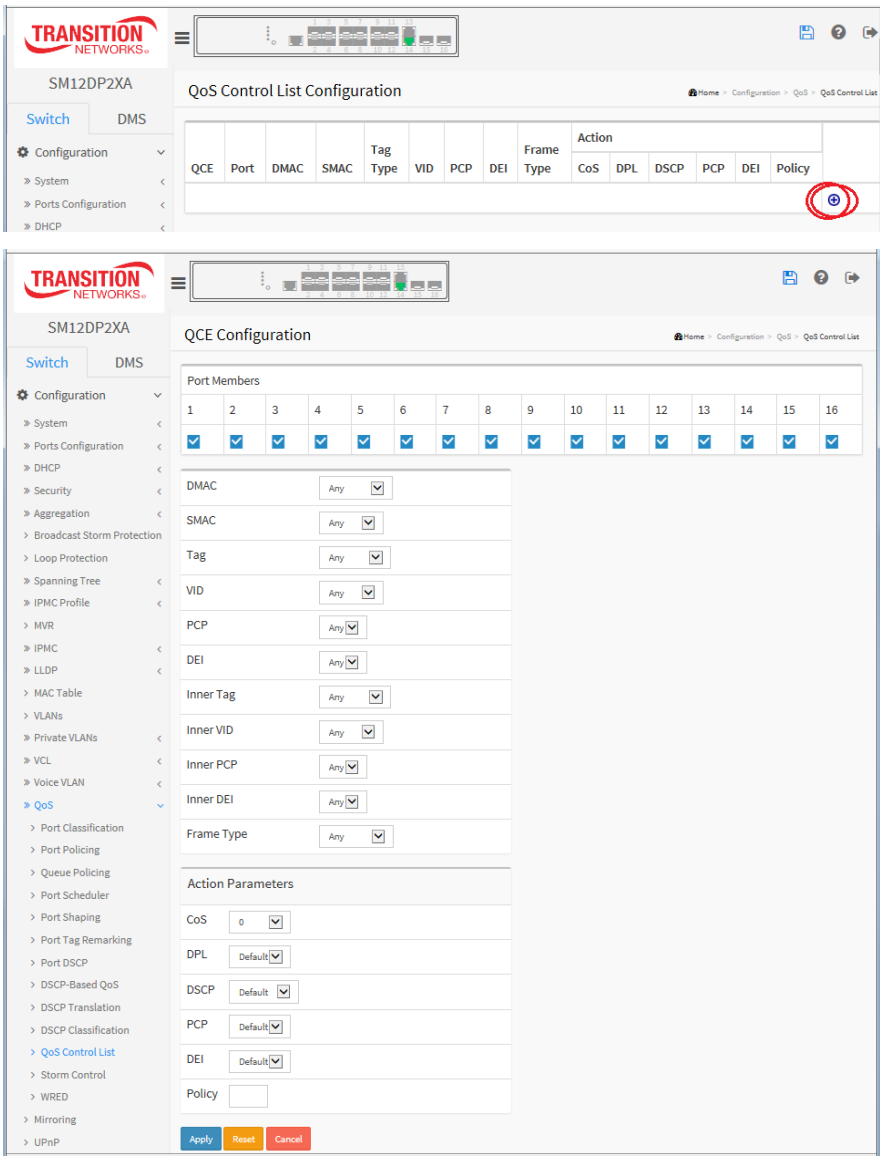
This page lets you configure the QoS Control List (QCL), which is made up of QCEs. Each row describes a defined QCE. The maximum number of QCEs is 256 per switch. Click on the lowest plus sign ( ) to add a new QCE to the list.

Web Interface

To configure the QoS Control List parameters in the web interface:

1. Click Configuration, QoS, QoS Control List.
2. Click the icon to add a new QoS Control List instance.
3. Select the Port Member to join the QCE rules.
4. Select all parameters.
5. Click Apply to save the settings.
6. To cancel the settings, click the Reset button to revert to previously saved values.

Figure 2-20.11: QoS Control List Configuration



Parameter descriptions:

QCE : Indicates the QCE ID.

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

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

Any: Match any DMAC. The default value is 'Any'.

Unicast: Match unicast DMAC.

Multicast: Match multicast DMAC.

Broadcast: Match broadcast DMAC.

<MAC>: Match specific DMAC.

SMAC : Match specific source MAC address or 'Any'. If a port is configured to match on DMAC/DIP, this field indicates the DMAC.

Tag Type : Indicates tag type. Possible values are:

Any: Match tagged and untagged frames. The default value is 'Any'.

Untagged: Match untagged frames.

Tagged: Match tagged frames.

C-Tagged: Match C-tagged frames.

S-Tagged: Match S-tagged frames.

VID : Indicates VLAN ID, either a specific VID or range of VIDs. VID can be in the range 1-4095 or 'Any'

PCP : Priority Code Point: Valid values of PCP are specific(0, 1, 2, 3, 4, 5, 6, 7) or range(0-1, 2-3, 4-5, 6-7, 0-3, 4-7) or 'Any'.

DEI : Drop Eligible Indicator: Valid value of DEI are 0, 1 or 'Any'.

Frame Type : Indicates the type of frame to look for incoming frames. Possible frame types are:

Any: The QCE will match all frame type.

Ethernet: Only Ethernet frames (with Ether Type 0x600-0xFFFF) are allowed.

LLC: Only (LLC) frames are allowed.

SNAP: Only (SNAP) frames are allowed

IPv4: The QCE will match only IPV4 frames.

IPv6: The QCE will match only IPV6 frames.

Action : Indicates the classification action taken on ingress frame if parameters configured are matched with the frame's content. 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.

Modification Buttons : You can modify each QCE in the table using these buttons:

: Inserts a new QCE before the current row.

: Edits the QCE.

: Moves the QCE up the list.

: Moves the QCE down the list.

: Deletes the QCE.

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

Port Members : Check the checkbox button in case you what to make any port member of the QCL entry. By default all ports are checked.

Key Parameters : Key configuration are described as below:

Tag: Value of Tag field can be 'Any', 'Untag' or 'Tag'

VID: Valid value of VLAN ID can be any value in the range 1-4095 or 'Any'; enter either a specific value or a range of VIDs

PCP: Priority Code Point valid values are specific (0, 1, 2, 3, 4, 5, 6, 7) or range (0-1, 2-3, 4-5, 6-7, 0-3, 4-7) or 'Any'.

DEI Drop Eligible Indicator: Valid value of DEI can be any of values between 0, 1 or 'Any'.

SMAC Source MAC address: 24 MS bits (OUI) or 'Any'.

DMAC Type: Destination MAC type: possible values are unicast (UC), multicast (MC), broadcast(BC) or 'Any'.

Frame Type: Frame Type can be Any, Ethernet, LLC, SNAP, IPv4 or IPv6.

Note: The frame types are explained below:

1. *Any* : Allow all types of frames.

2. *Ethernet* : Ethernet Type Valid Ethernet type can have value within 0x600-0xFFFF or 'Any', default value is 'Any'.

3. *LLC*: SSAP Address Valid SSAP(Source Service Access Point) can vary from 0x00 to 0xFF or 'Any', the default value is 'Any'
DSAP Address Valid DSAP(Destination Service Access Point) can vary from 0x00 to 0xFF or 'Any', the default value is 'Any'
Control Address Valid Control Address can vary from 0x00 to 0xFF or 'Any', the default value is 'Any'

4. *SNAP* : PID Valid PID (Ethernet type) can have value within 0x00-0xFFFF or 'Any', default value is 'Any'

5. *IPv4* : Protocol IP protocol number: (0-255, TCP or UDP) or 'Any' Source IP Specific Source IP address in value/mask format or 'Any'. IP and Mask are in the format x.y.z.w where x, y, z, and w are decimal numbers between 0 and 255. When Mask is converted to a 32-bit binary string and read from left to right, all bits following the first zero must also be zero DSCP Diffserv Code Point value (DSCP): It can be specific value, range of value or 'Any'. DSCP values are in the range 0-63 including BE, CS1-CS7, EF or AF11-AF43

IP Fragment IPv4 frame fragmented option: yes|no|any.

Sport Source TCP/UDP port:(0-65535) or 'Any', specific or port range applicable for IP protocol UDP/TCP .

Dport Destination TCP/UDP port:(0-65535) or 'Any', specific or port range applicable for IP protocol UDP/TCP .

6. *IPv6* :Protocol IP protocol number: (0-255, TCP or UDP) or 'Any'.
Source IP IPv6 source address: (a.b.c.d) or 'Any', 32 LS bits .

DSCP Diffserv Code Point value (DSCP): It can be specific value, range of value or 'Any'. DSCP values are in the range 0-63 including BE, CS1-CS7, EF or AF11-AF43 .

Sport Source TCP/UDP port:(0-65535) or 'Any', specific or port range applicable for IP protocol UDP/TCP.

Dport Destination TCP/UDP port:(0-65535) or 'Any', specific or port range applicable for IP protocol UDP/TCP.

Action Configuration : Class QoS Class: "class (0-7)", default- basic classification. DP: Valid DP Level can be (0-3)", default- basic classification. DSCP: Valid DSCP value can be (0-63, BE, CS1-CS7, EF or AF11-AF43).

Buttons:

Apply : Click to save changes. This will save the configuration and move to the 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.

2-20.12 Storm Control

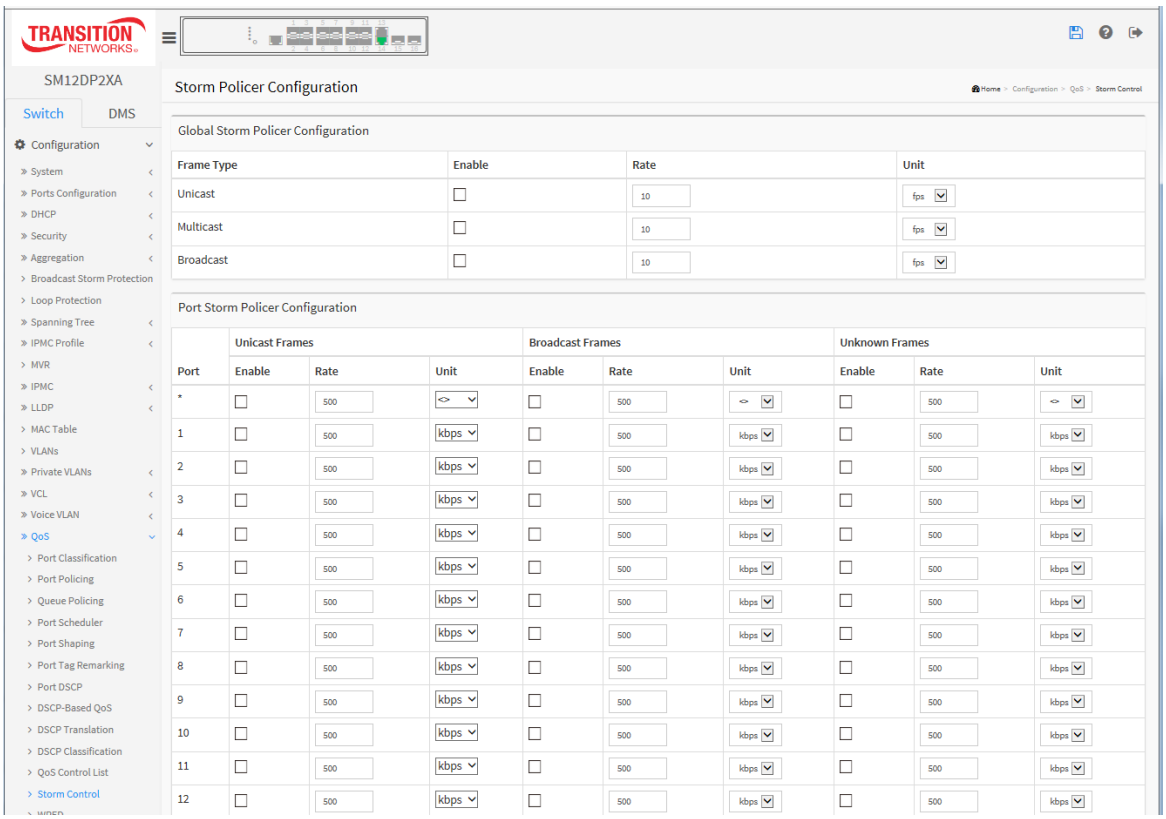
This page lets you configure Storm control for the switch. There are Global storm policers and Port storm policers that can be configured here.

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 and Unit parameters.
4. Click Apply to save the settings.
5. To cancel the settings, click the Reset button to revert to previously saved values.

Figure 2-20.11: Storm Control Configuration



Parameter descriptions:

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

Frame Type : The frame type for which the configuration below applies (Unicast, Multicast or Broadcast).

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

Rate : Controls the rate for the global storm policer. This value is restricted to 10-13128147 when "Unit" is fps or kbps, and 1-13128 when "Unit" is kfps or Mbps. The rate is internally rounded up to the nearest value supported by the global storm policer.

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

Port Storm Policer Configuration: Port storm policers for all switch ports are configured in this section. There is a storm policer for unicast frames, broadcast frames and unknown (flooded) frames. The displayed settings are:

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 10-13128147 when "Unit" is fps or kbps, and 1-13128 when "Unit" is kfps or Mbps. The rate is internally rounded up to the nearest value supported by the 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.

2-20.13 WRED

This page lets you configure the WRED function for the switch and configure Random Early Detection (RED) settings for queue 0 to 5. RED cannot be applied to queue 6 and 7. Through different RED configuration for the queues (QoS classes) it is possible to obtain Weighted Random Early Detection (WRED) operation between queues. The settings are global for all ports.

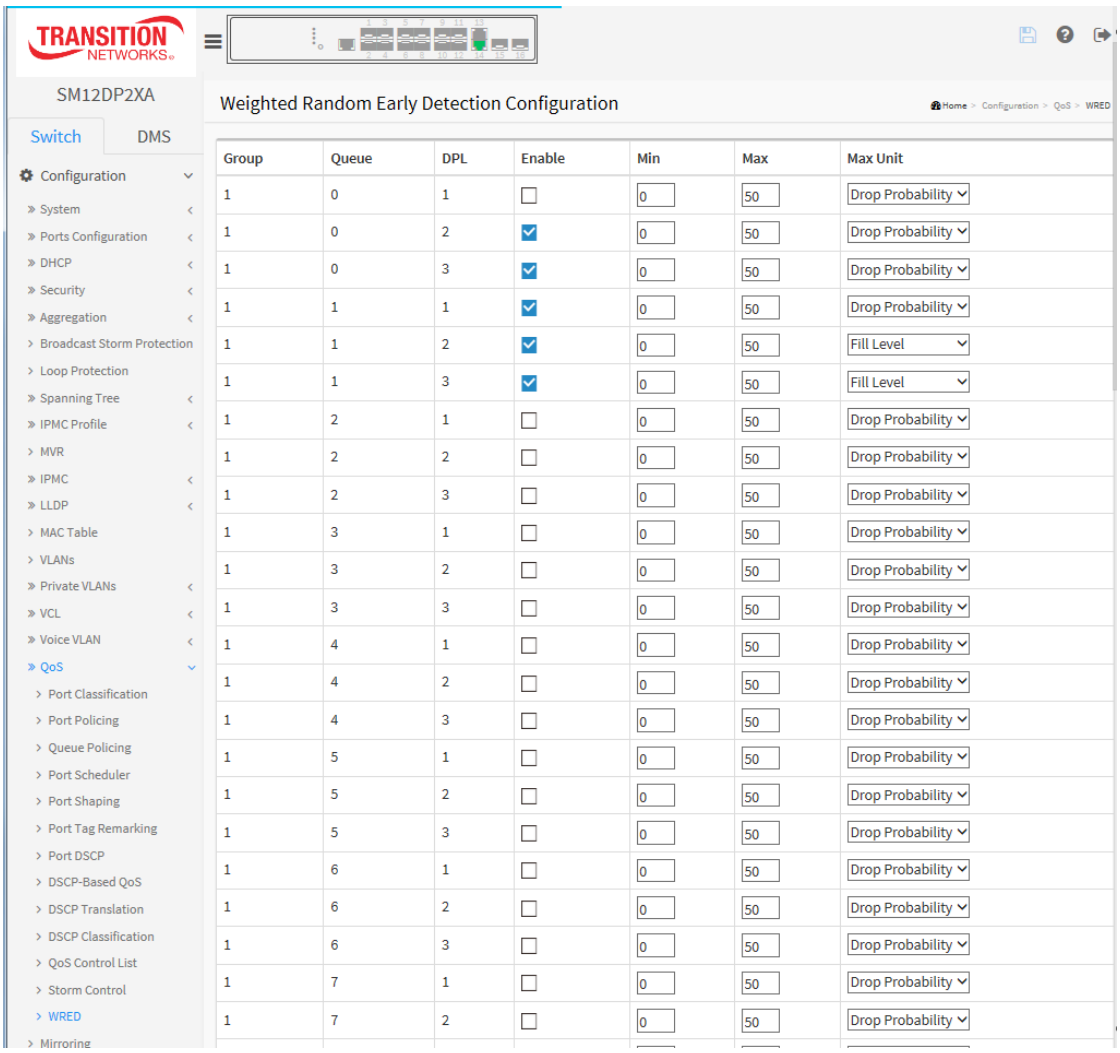
WRED (Weighted Random Early Detection) is an active queue management mechanism that provides preferential treatment of higher priority frames when traffic builds up within a queue. A frame's DP level is used as input to WRED. A higher DP level assigned to a frame results in a higher probability that the frame is dropped during times of congestion.

Web Interface

To configure the WRED Configuration parameters in the web interface:

1. Click Configuration, QoS, WRED.
2. Enable or disable WRED.
3. Enter each parameter value.
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 2-20.13: WRED Configuration



Group	Queue	DPL	Enable	Min	Max	Max Unit
1	0	1	☐	0	50	Drop Probability
1	0	2	☑	0	50	Drop Probability
1	0	3	☑	0	50	Drop Probability
1	1	1	☑	0	50	Drop Probability
1	1	2	☑	0	50	Fill Level
1	1	3	☑	0	50	Fill Level
1	2	1	☐	0	50	Drop Probability
1	2	2	☐	0	50	Drop Probability
1	2	3	☐	0	50	Drop Probability
1	3	1	☐	0	50	Drop Probability
1	3	2	☐	0	50	Drop Probability
1	3	3	☐	0	50	Drop Probability
1	4	1	☐	0	50	Drop Probability
1	4	2	☐	0	50	Drop Probability
1	4	3	☐	0	50	Drop Probability
1	5	1	☐	0	50	Drop Probability
1	5	2	☐	0	50	Drop Probability
1	5	3	☐	0	50	Drop Probability
1	6	1	☐	0	50	Drop Probability
1	6	2	☐	0	50	Drop Probability
1	6	3	☐	0	50	Drop Probability
1	7	1	☐	0	50	Drop Probability
1	7	2	☐	0	50	Drop Probability

Parameter descriptions:

Group: The WRED group number for which the configuration below applies.

Queue: The queue number (QoS class) for which the configuration below applies.

DPL: The Drop Precedence Level for which the configuration below applies.

Enable: Controls whether RED is enabled for this entry.

Min: Controls the lower RED fill level threshold. If the queue filling level is below this threshold, the drop probability is zero. This value is restricted to 0-100%.

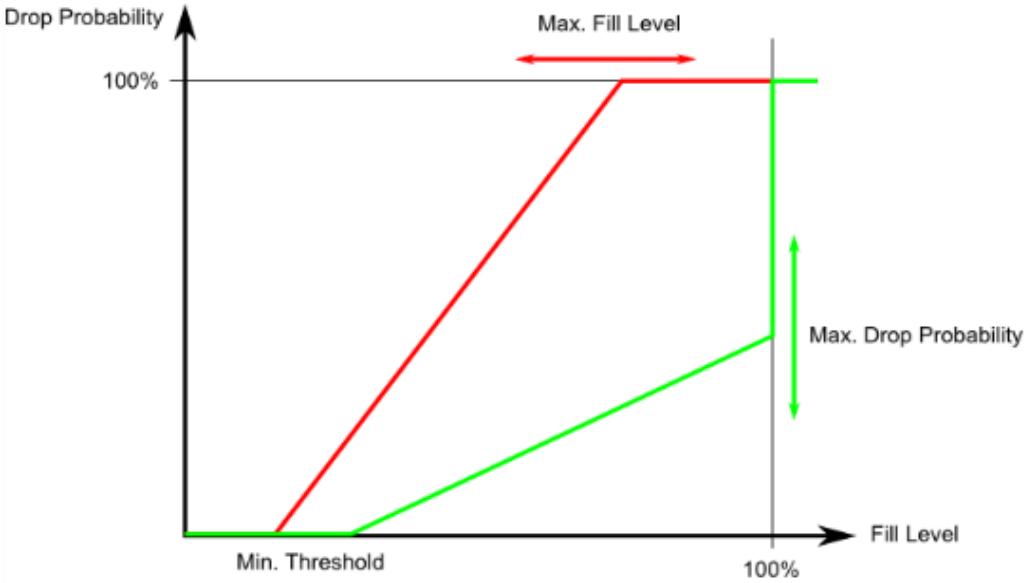
Max: Controls the upper RED drop probability or fill level threshold for frames marked with Drop Precedence Level > 0 (yellow frames). This value is restricted to 1-100%.

Max Unit: Selects the unit for Max. Possible values are:

> ***Drop Probability***: Max controls the drop probability just below 100% fill level.
>
> ***Fill Level***: Max controls the fill level where drop probability reaches 100%.

RED Drop Probability Function

The figure below shows the drop probability versus fill level function with associated parameters.



Min is the fill level where the queue randomly start dropping frames marked with Drop Precedence Level > 0 (yellow frames).

If Max Unit is 'Drop Probability' (the green line), Max controls the drop probability when the fill level is just below 100%.

If Max Unit is 'Fill Level' (the red line), Max controls the fill level where drop probability reaches 100%. This configuration makes it possible to reserve a portion of the queue exclusively for frames marked with Drop Precedence Level 0 (green frames). The reserved portion is calculated as (100 - Max) %.

Frames marked with Drop Precedence Level 0 (green frames) are never dropped.

The drop probability for frames increases linearly from zero (at Min average queue filling level) to Max Drop Probability or Fill Level.

Buttons:

Apply : Click to save changes.

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

2-21 Mirroring & Remote Mirroring

Mirroring is a feature for switched port analyzer. The administrator can use the Mirroring to debug network problems. The selected traffic can be mirrored (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 to another switch, so the administrator can analyze the network traffic on the other switches.

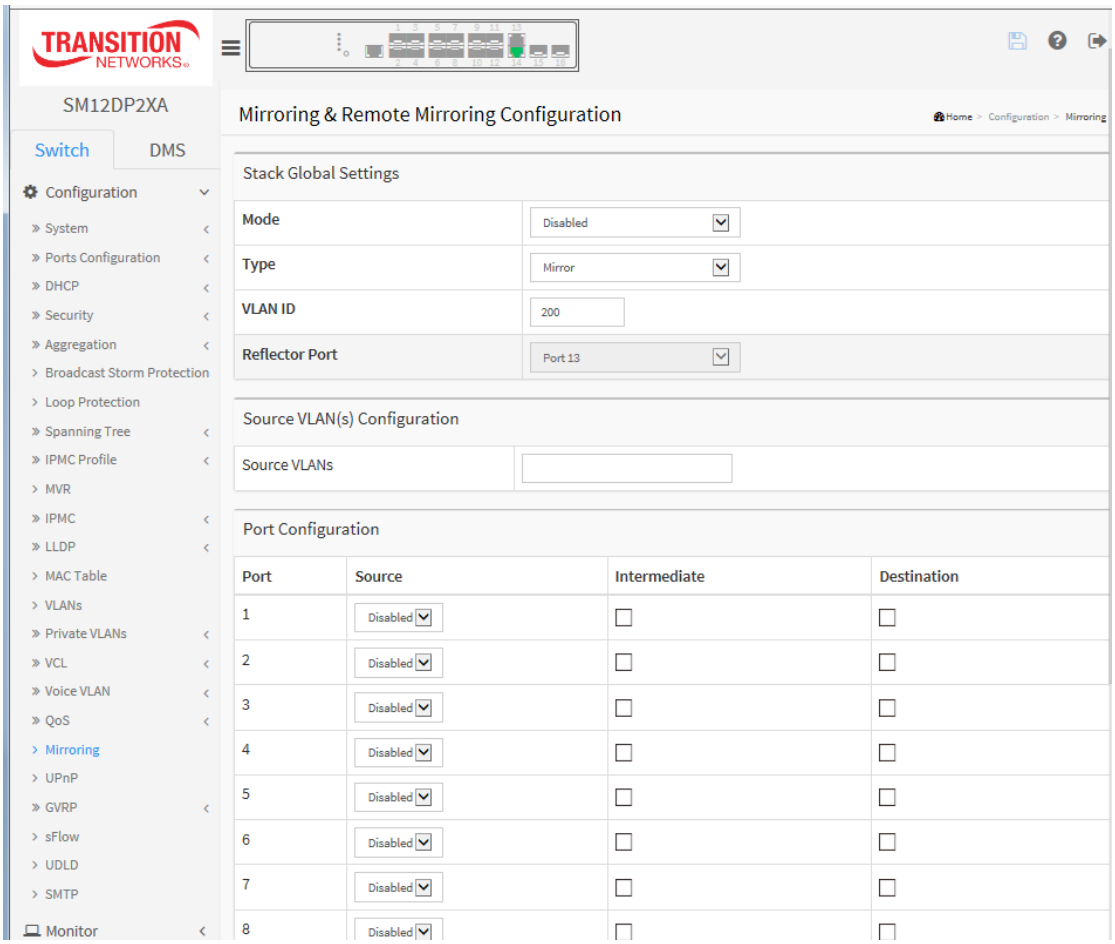
To get tagged mirrored traffic, you must set VLAN egress tagging as "Tag All" on the reflector port.
To get untagged mirrored traffic, you must set VLAN egress tagging as "Untag ALL" on the reflector port.

Web Interface

To configure Mirroring & Remote Mirroring via the web interface:

1. Click Configuration, Mirroring.
2. Select the Mode and Type.
3. If Type was set to other than “Mirror”, select VLAN ID and Reflector Port.
4. Enter the desired Source VLANs.
5. For each Port, select Source, Intermediate, and Destination.
6. Click Apply to save the settings.
7. To cancel the settings, click the Reset button to revert to previously saved values.

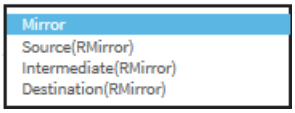
.Figure 2-21: Mirror Configuration



Parameter descriptions:

Mode : Select Enabled/Disabled for the mirror or Remote Mirroring function.

Type : Select switch type.



Mirror: The switch is running in mirror mode. The source port(s) and destination port are on this switch.

Source : 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 : 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 : The switch is an end node for monitor flow. The destination port(s) and intermediate port(s) are located on this switch.

VLAN ID : The VLAN ID points out where the monitor packet will copy to. By default VLAN ID 200 displays.

Reflector Port : The reflector port is a method to redirect the traffic to Remote Mirroring VLAN. Any device connected to a port set as a Reflector port loses connectivity until Remote Mirroring is disabled. Only configurable (for ports 13 and 14) when "Type" is set to "Source(RMirror)".

If you shut down a port, it cannot be a candidate for reflector port.

If you shut down the 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 pure copper ports.

Source VLAN(s) Configuration : The switch supports VLAN-based Mirroring. If you want to monitor some VLANs on the switch, you can set the selected VLANs on this field.
Note: The Mirroring session will have either ports or VLANs as sources, but not both.

Remote Mirroring Port Configuration : The table on the next page describes port role selection for each feature.

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 needs to disable MAC Table learning.

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.

Note 1: In Mirror mode, the device only supports one destination port.

Note 2: The destination port must have MAC Table Learning disabled.

Configuration Guideline for All Features

When the switch is running in Remote Mirroring mode, you must also check if other features are enabled or disabled. For example, if MSTP is not disabled on the Reflector port, all monitor traffic will be blocked on the Reflector port.

All recommended settings are described below.

Feature	Impact	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:

* -- required

o -- optional

Impact: Critical/High/Low

Critical

High

Low

2-22 UPnP

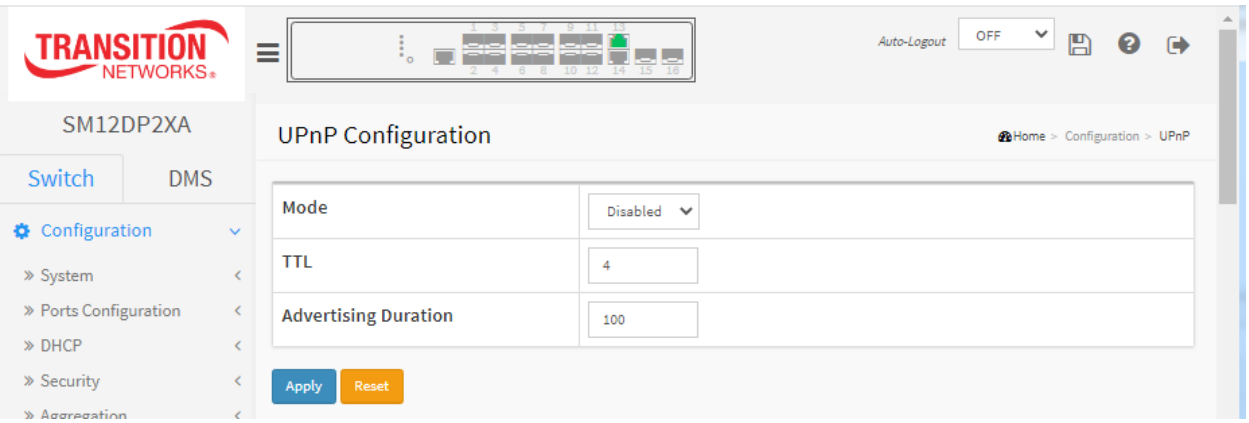
UPnP (Universal Plug and Play) allows devices to connect seamlessly and to simplify network implementation in the home (data sharing, communications, entertainment) and in corporate environments.

Web Interface

To configure the UPnP Configuration in the web interface:

1. Click Configuration, UPnP.
2. Set the Mode to Enabled or Disabled.
3. Specify the parameters in each blank field.
4. Click Apply to save the settings.
5. To cancel the settings, click the Reset button to revert to previously saved values.

Figure 2-22: UPnP Configuration



Parameter descriptions: These parameters are displayed on the UPnP Configuration page:

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

Enabled: Enable UPnP mode operation.

Disabled: Disable UPnP mode operation.

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

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

Advertising Duration : The duration, carried in SSDP packets, is used to inform a control point or control points how often it or they should receive an SSDP advertisement message from this switch.
If a control point does not receive any message within the duration, it will think that the switch no longer exists. Due to the unreliable nature of UDP, in the standard it is recommended that such refreshing of advertisements 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 66- 86400.

Buttons:

Apply – Click to save changes.

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

2-23. GVRP

GVRP (GARP VLAN Registration Protocol) is used for dynamically registering VLANs on ports, as specified in IEEE 802.1Q-2005, clause 11. GVRP uses GARP, hence the G in GVRP.

2-23.1 GVRP Configuration

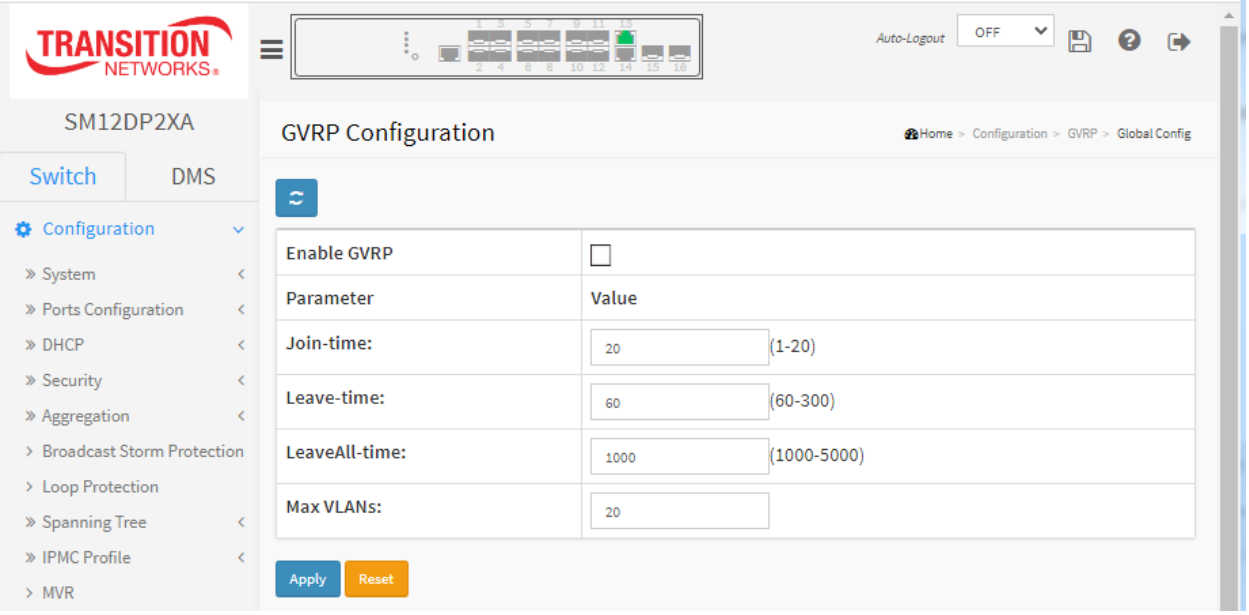
This page lets you configure the global GVRP configuration settings that are commonly applied to all GVRP enabled ports.

Web Interface

To configure the GVRP in 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 2-23.1: GVRP Configuration



Enable GVRP : Check the checkbox to enable GVRP globally.

GVRP protocol timers : GARP implementation consists of three state machines (tables) along with three timers. The three state machines are applicant state, registrar state, and LeaveAll. The timers are Join, Leave and LeaveAll.

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. **Note**: this number can only be changed when GVRP is disabled globally.

Buttons:

 **Refresh: Click to manually update the webpage manually.**

Apply – Click to save changes.

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

2-23.2 Port Config

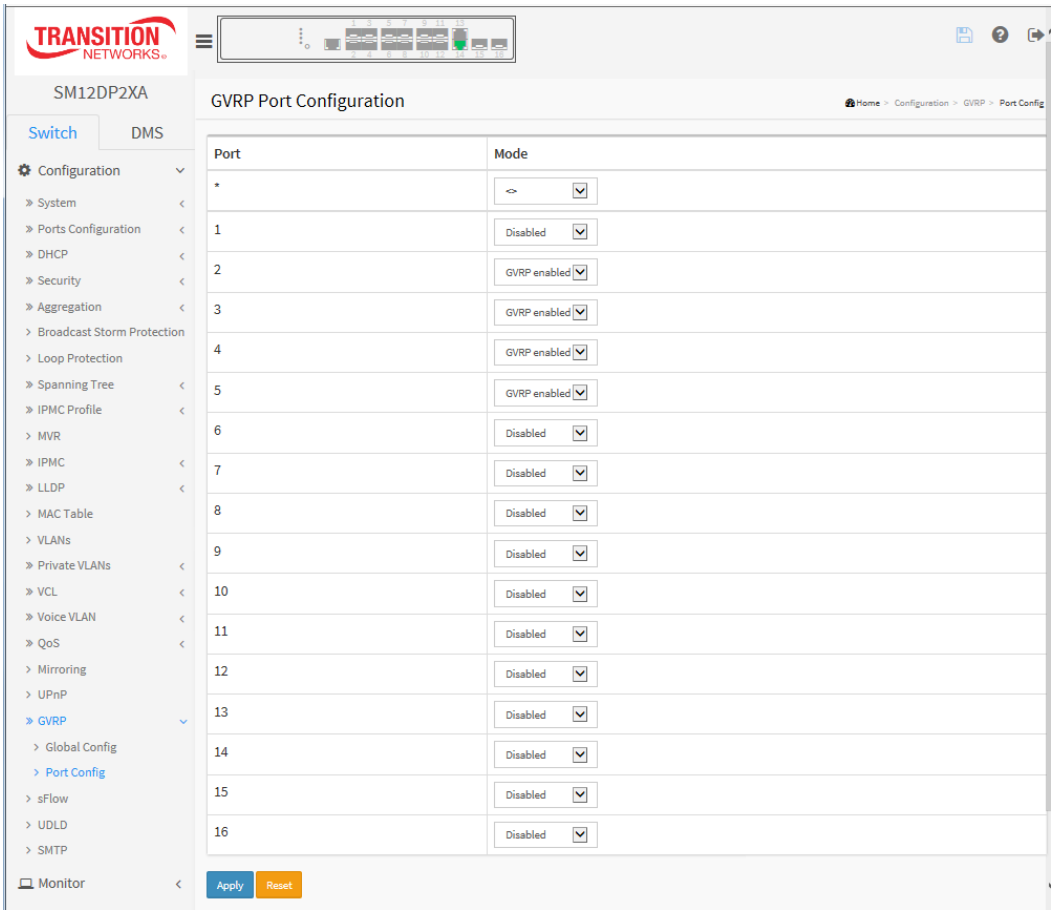
This page lets you enable or disable a port for GVRP operation. This configuration can be performed either before or after GVRP is configured globally; the protocol operation will be the same.

Web Interface

To configure the GVRP port parameters in the web interface:

1. Click Configuration, GVRP, Port Config.
2. For each port, select the Mode (either Disabled or GVRP enabled).
3. Click Apply.

Figure 2-23.2: GVRP Configuration



Parameter descriptions:

Port : The logical port that is to be configured.

Mode : Select either 'Disabled' or 'GVRP enabled'. These values turn the GVRP feature off or on respectively for the port in question.

> ***Disabled***: Select to Disable GVRP mode on this port. This is the default setting.
> ***GVRP enabled***: Select to Enable GVRP mode on this port.

Buttons:

Apply – Click to save changes.

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

2-24. sFlow

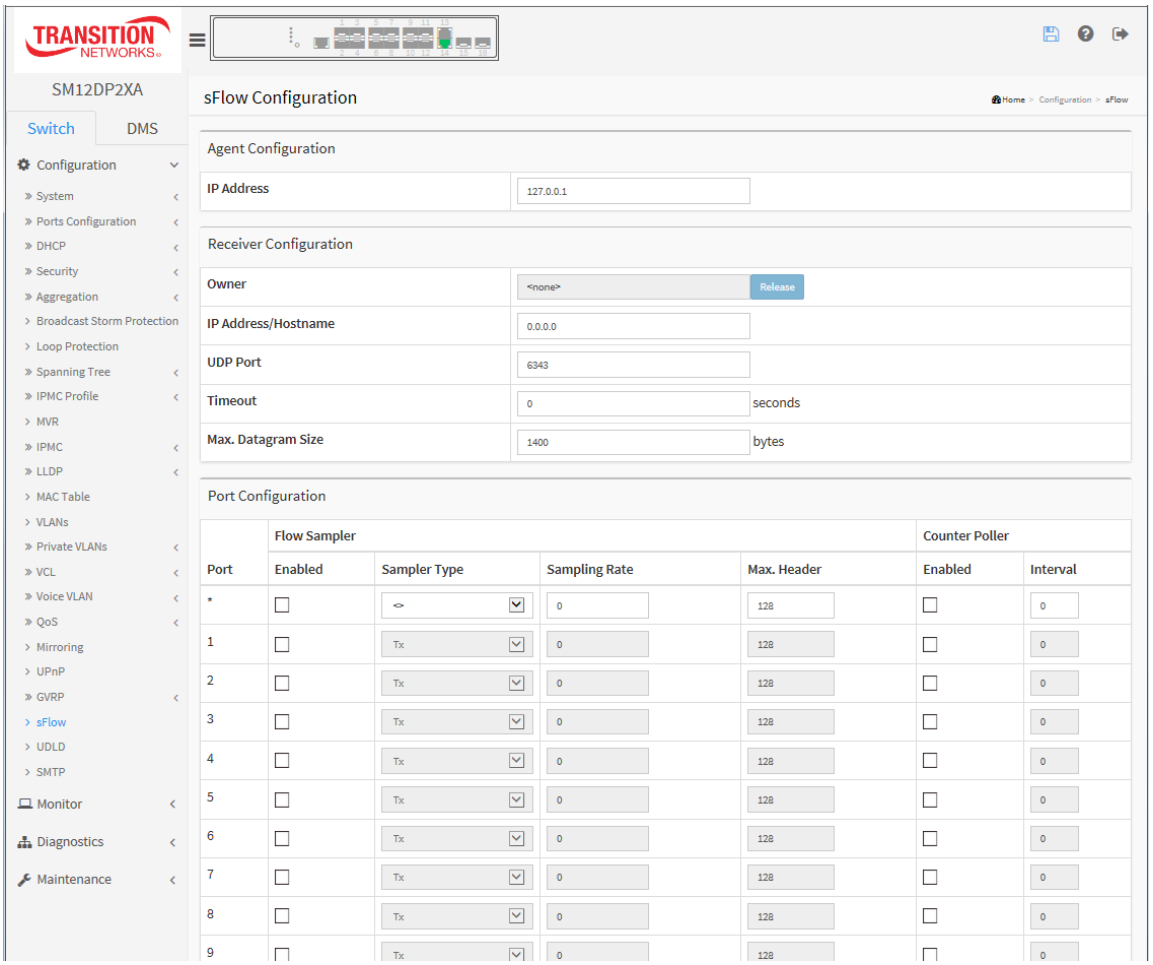
This page lets you configure sFlow Collector for the switch. The sFlow configuration is divided into two parts: configuration of the sFlow receiver (sFlow collector) and configuration of per-port flow and counter samplers. The sFlow configuration is not persisted to non-volatile memory, so a reboot or master change will disable sFlow sampling.

Web Interface

To configure the sFlow Agent in the web interface:

1. Click Configuration, sFlow.
2. Set the parameters.
3. Click Apply to save the settings.
4. To cancel the settings, click the Reset button to revert to previously saved values.

Figure 2-24: sFlow Configuration



Parameter descriptions:

Agent Configuration

IP Address : The IP address used as Agent IP address in sFlow datagrams. It serves as a unique key that will identify this agent over extended periods of time. Both IPv4 and IPv6 addresses are supported.

Receiver Configuration

Owner : Basically, sFlow can be configured in two ways: Through local management using the Web or CLI interface or through SNMP. This read-only field shows the owner of the current sFlow configuration and assumes values as follows:

• If sFlow is currently unconfigured/unclaimed, Owner contains <*none*>.

• If sFlow is currently configured through Web or CLI, Owner contains <*Configured through local management*>.

• If sFlow is currently configured through SNMP, Owner contains a string identifying the sFlow receiver. If sFlow is configured through SNMP, all controls (except for the Release button) are disabled to avoid inadvertent reconfiguration.

The **Release** button allows for releasing the current owner and disable sFlow sampling. The **Release** button is disabled if sFlow is currently unclaimed. If configured via SNMP, the release must be confirmed (a confirmation request will display).

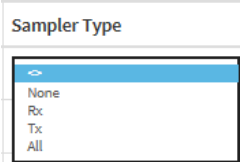
IP Address/Hostname : The IP address or hostname of the sFlow receiver. Both IPv4 and IPv6 addresses are supported.

UDP Port : The UDP port on which the sFlow receiver listens to sFlow datagrams. If set to 0 (zero), the default port (6343) is used.

Timeout : The number of seconds remaining before sampling stops and the current sFlow owner is released. While active, the current time left can be updated with a click on the Refresh-button.
If locally managed, the timeout can be changed on the fly without affecting any other settings.

Max. Datagram Size : The maximum number of data bytes that can be sent in a single sample datagram. This should be set to a value that avoids fragmentation of the sFlow datagrams. Valid range is 200 to 1468 bytes with default being 1400 bytes.

Port Configuration



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

Flow Sampler Enabled : Enables/disables flow sampling on this port.

Sampler Type: At the dropdown select None, Rx, Tx, or All.

Sampler Rate : The statistical sampling rate for packet sampling. Set to N to sample on average 1/Nth of the packets transmitted/received on the port. Not all sampling rates (1 – 4294967295) are achievable. If an unsupported sampling rate is requested, the switch will automatically adjust it to the closest achievable. This will be reported back in this field.

Flow Sampler Max. Header : The maximum number of bytes that should be copied from a sampled packet to the sFlow datagram. Valid range is 14 to 200 bytes with default being 128 bytes. If the maximum datagram size does not take into account the maximum header size, samples may be dropped.

Counter Poller Enabled : Enables/disables counter polling on this port.

Counter Poller Interval : With counter polling enabled, this specifies the interval - in seconds - between counter poller samples.

Buttons:

Apply : Click to save changes.

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

Release : Allows for releasing the current owner and disable sFlow sampling. The Release button is disabled if sFlow is currently unclaimed. If configured via SNMP, the release must be confirmed (a confirmation request will display).

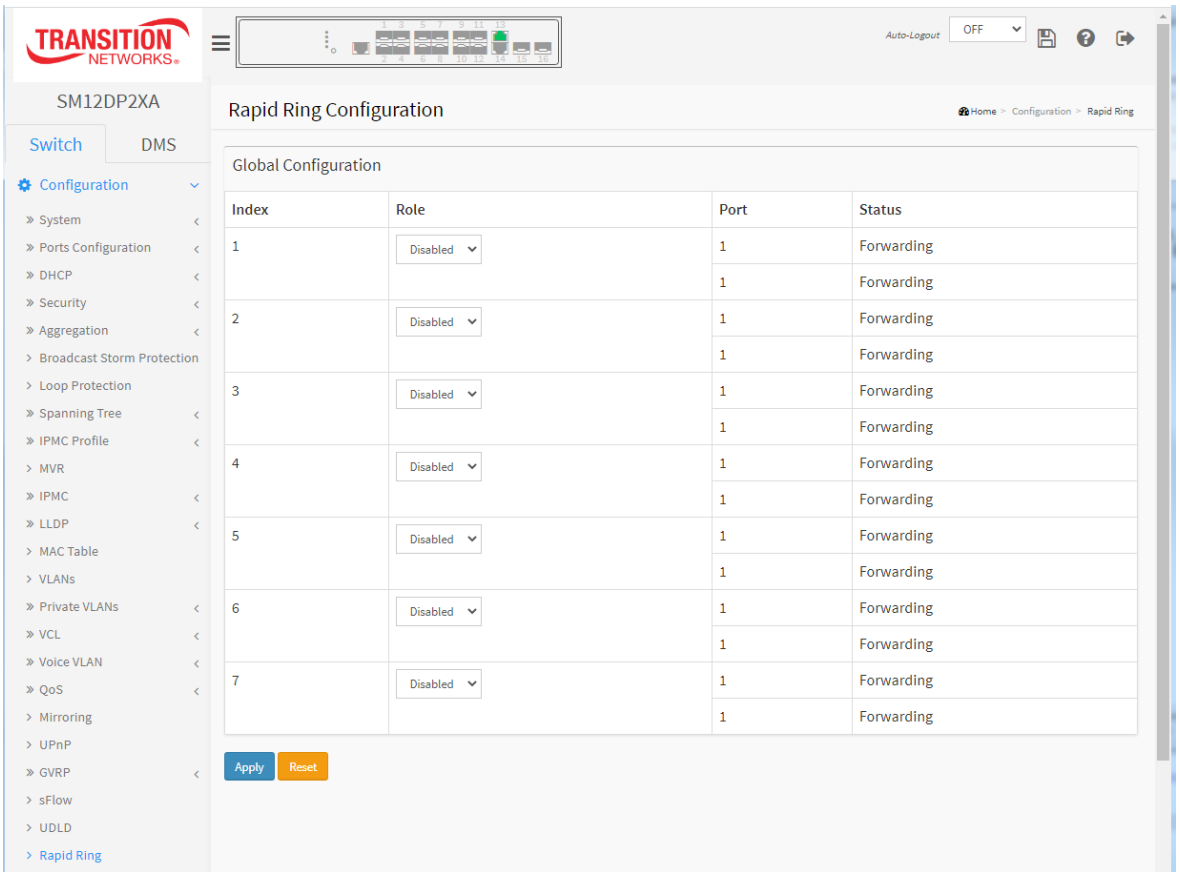
2-25 Rapid Ring

Rapid Ring is a redundancy proprietary protocol that runs on your network; it can be used to recover the network system from critical link failures to protect from network loops (added at FW v7.10.2544).

Many redundant or network recovery protocols defined by IEEE, such as spanning tree (STP, RSTP, MSTP) were developed to recover the network system for the connection failure, but the recovery time of Rapid Ring is can be less than 20ms for up to 250 switches, which is much less than the other redundancy protocols.

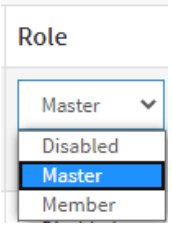
Note that Rapid Ring roles cannot be returned to Disabled using the Web UI. The roles can be disabled using a CLI command. Note that other Ring technologies (e.g., STP) must be disabled.

Navigate to Switch > Configuration > Rapid Ring to display the Rapid Ring Configuration webpage.



Parameter descriptions:

<u>Global Configuration</u>



Index: The Rapid Ring instance number (1-7).

Role: Set Ring role value to Master, Member, or Disabled. The default is Disabled.

Port: The switch port number of the port.

Status: The current Rapid Ring status of the port (e.g., Forwarding, Discarding).

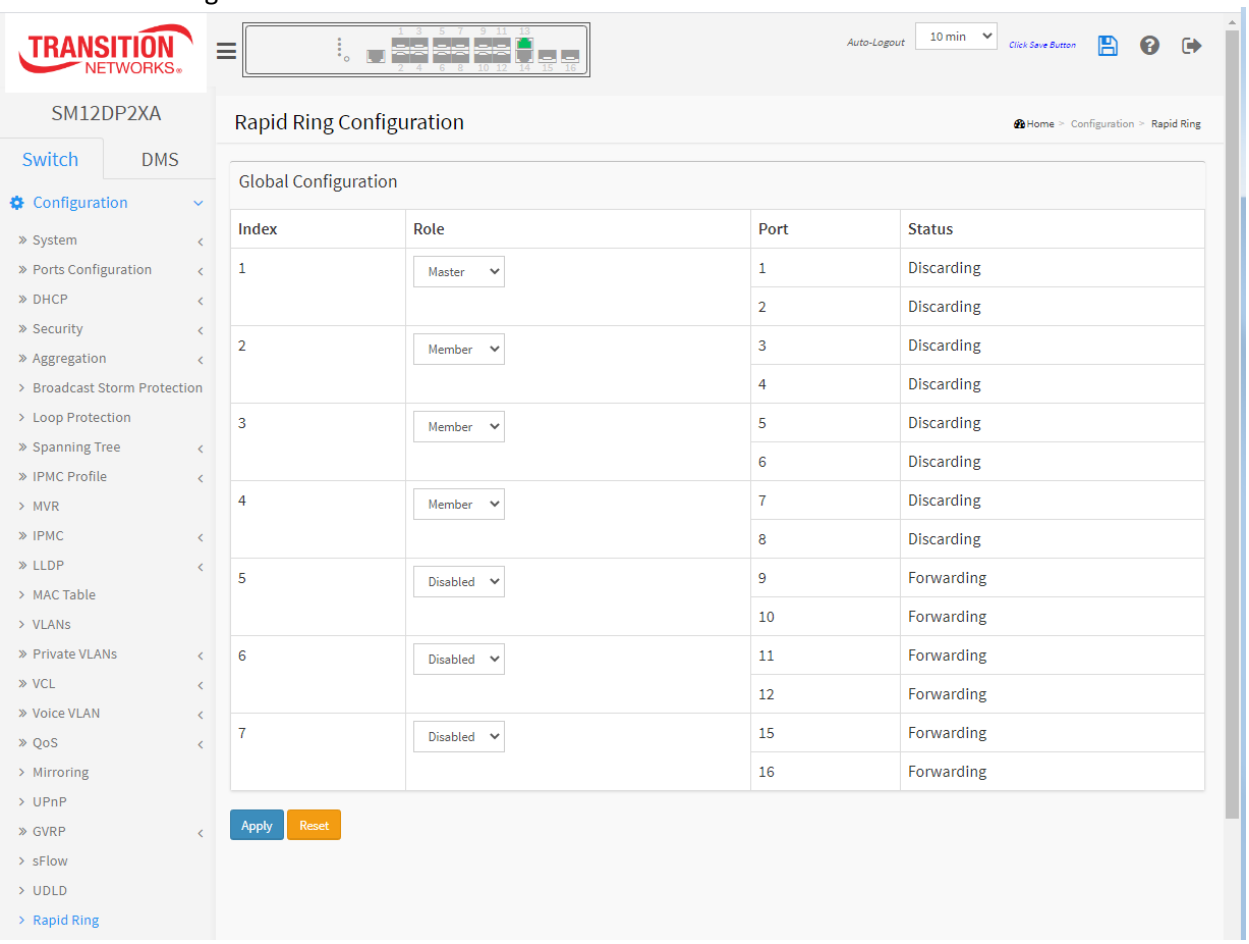
Buttons:

Apply : Click to save changes.

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

Message: *Error in port 1, STP is enable*
Meaning: Another Ring technology id currently enabled.
Recovery: **1**. Click the **Previous** button. **2**. At Switch > Configuration > Spanning Tree > CIST Port disable Spanning Tree. **3**. Continue Rapid Ring configuration.

Example: Port 1 is set as the Ring Master, ports 3-8 are set as Ring Members, and ports 9-12 are left at the default setting of Disabled.



Index	Role	Port	Status
1	Master	1	Discarding
		2	Discarding
2	Member	3	Discarding
		4	Discarding
3	Member	5	Discarding
		6	Discarding
4	Member	7	Discarding
		8	Discarding
5	Disabled	9	Forwarding
		10	Forwarding
6	Disabled	11	Forwarding
		12	Forwarding
7	Disabled	15	Forwarding
		16	Forwarding

2-26 UDLD

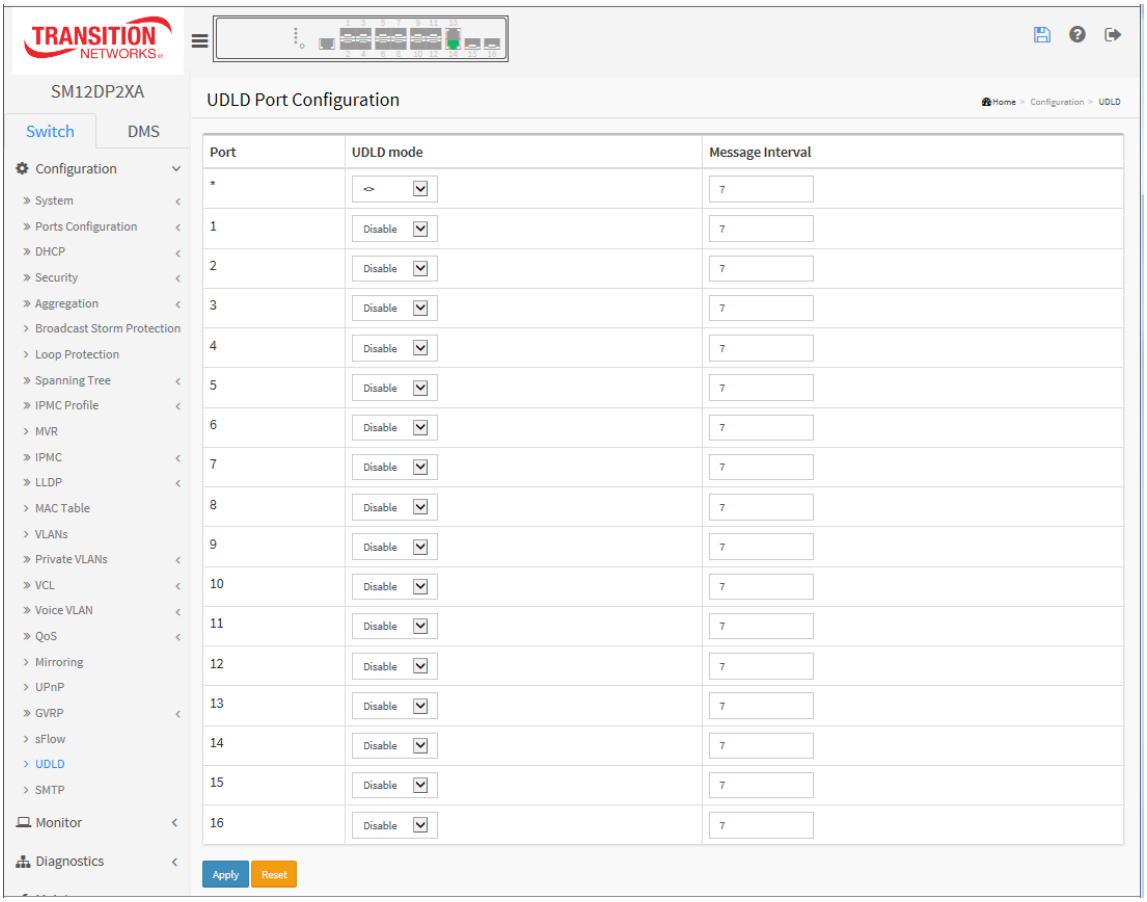
UDLD (Uni Directional Link Detection) is a protocol that monitors the physical configuration of the links between devices and ports that support UDLD. It detects the existence of unidirectional links.
It provides mechanisms useful for detecting one way connections before they create a loop or other protocol malfunction. IETF RFC 5171 specifies a way to detect Uni-directional links at the data link layer.

Web Interface

To configure the UPnP Configuration in the web interface:

1. Click Configuration, UDLD.
2. Set the UDP mode to Enable or Disable.
3. Specify the parameter in each blank field.
4. Click Apply to save the settings.
5. To cancel the settings, click the Reset button to revert to previously saved values.

Figure 2-26: UDLD Configuration



Parameter descriptions: These parameters are displayed on the UPnP Configuration page:

Port : Port number of the switch.

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

Disable : In disabled mode, UDLD functionality doesn't 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 back up, you must 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 range is 7 - 90 seconds (the default is 7 seconds). Currently the default time interval is supported, due to lack of detailed information in IETF RFC 5171.

Buttons:

Apply – Click to apply changes.

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

2-27 SMTP Configuration

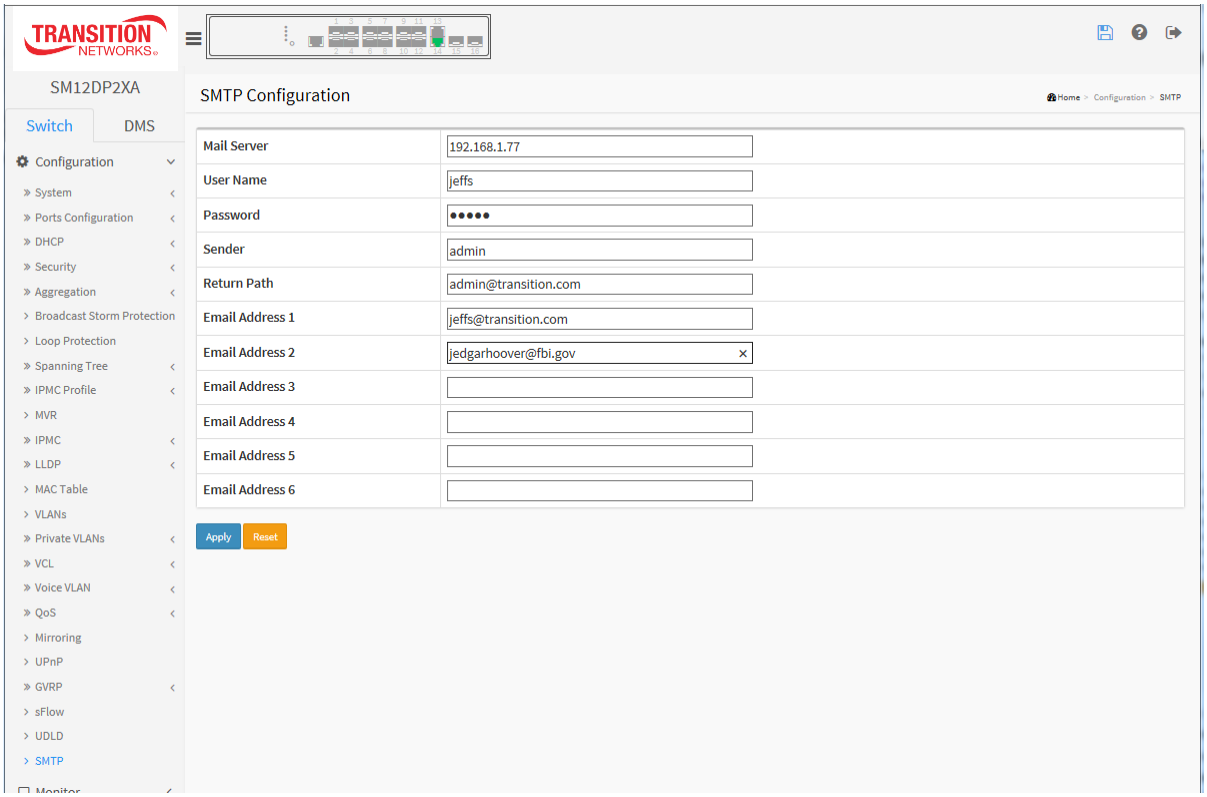
Configure SMTP (Simple Mail Transfer Protocol) on this page. SMTP is the Internet message-exchange standard. The switch is to be configured as a client of SMTP, while the server is a remote device that will receive messages from the switch indicating that alarm events occurred.

Web Interface

To configure the SMTP Configuration in the web interface:

1. Click Configuration, SMTP.
2. Specify the parameter in each blank field.
3. Click Apply to save the settings.
4. To cancel the settings, click the Reset button to revert to previously saved values.

Figure 2-27: SMTP Configuration



Parameter descriptions:

Mail Server : Specify the IP Address of the server transferring your email.

User Name : Specify the username on the mail server.

Password : Specify the password on the mail server.

Sender : Specify the mail sender name.

Return-Path : Set the mail return-path as sender mail address.

Email Address 1-6 : Enter the e-mail address(es) to receive the alarm message.

Buttons:

Apply : Click to apply changes.

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

Chapter 3. Monitor

This chapter describes the functions that you can monitor (e.g., System, Ports, DHCP, Security).

3-1 System

After you login, the switch displays the System Information page. This page is the startup page displaying basic system information, as described below.

3-1.1 Information

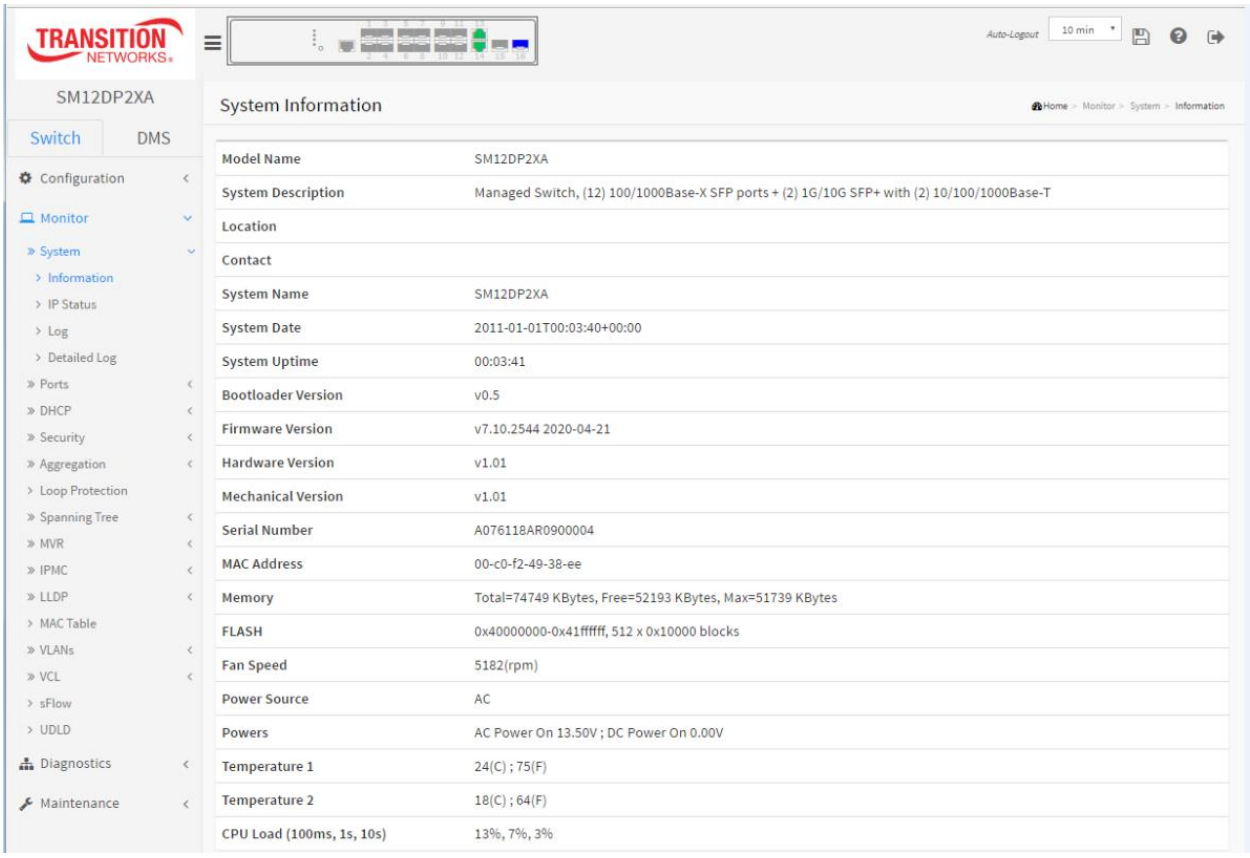
The switch system information is provided here.

Web interface

To configure System Information in the web interface:

1. Click Monitor, System, Information.
2. View the various parameters (described below).

Figure 3-1.1: System Information



Parameter descriptions:

Model Name : Displays the factory-defined model name for identification purposes (*SM12DP2XA*).

System Description : Displays the system description (*Managed Switch, (12) 100/1000Base-X SFP ports + (2) 1G/10G SFP+ with (2) 10/100/1000Base-T*).

Location : Displays the system location configured at Configuration > System > Information > System Location.

Contact : The system contact configured at Configuration > System > Information > System Contact.

System Name : Displays the user-defined system name that is configured at System > System Information > Configuration > System Name (*SM12DP2XA*).

System Date : The current (GMT) system time and date. The system time is obtained via the Timing server running on the switch, if any. The format is "*2018-06-12T13:00:39-06:00*".

System Uptime : The period of time the device has been operational, in the format *4d 22:19:16*.

Bootloader Version : Displays the current boot loader version number (e.g., *v0.5*).

Firmware Version : Displays the current firmware version number (e.g., *v7.10.2544*).

Hardware Version : The hardware version of this switch (e.g., *v1.01*).

Mechanical Version : The mechanical version of this switch (e.g., *v1.01*).

Serial Number : The serial number of this switch (e.g., *A076118AR0900001*).

MAC Address : The MAC Address of this switch in the format *11-22-33-44-55-66*.

Memory : Displays the memory size of the system. For example: *Total=77700 KBytes, Free=55148 KBytes, Max=54643 Kbytes*.

FLASH : Displays the flash size of the system (e.g., *0x40000000-0x41ffffff, 512 x 0x10000 blocks*).

Fan Speed : Displays the fan speed of the system in the format *7031(rpm)*.

Powers : Displays the power source of the system (e.g., *AC Power On 14.00V ; DC Power On 0.00V* or *AC Power On 0.00V ; DC Power On 11.80V* or *AC Power On 14.00V ; DC Power On 11.80V*).

Temperature 1: Displays the temperature of temperature sensor 1 (e.g., *36(C) ; 96(F))*.

Temperature 2: Displays the temperature of temperature sensor 2 (e.g., *30(C) ; 86(F)* .

CPU Load (100ms, 1s, 10s): Displays the current CPU loading (e.g., *11%, 10%, 5%)*.

3-1.2 IP Status

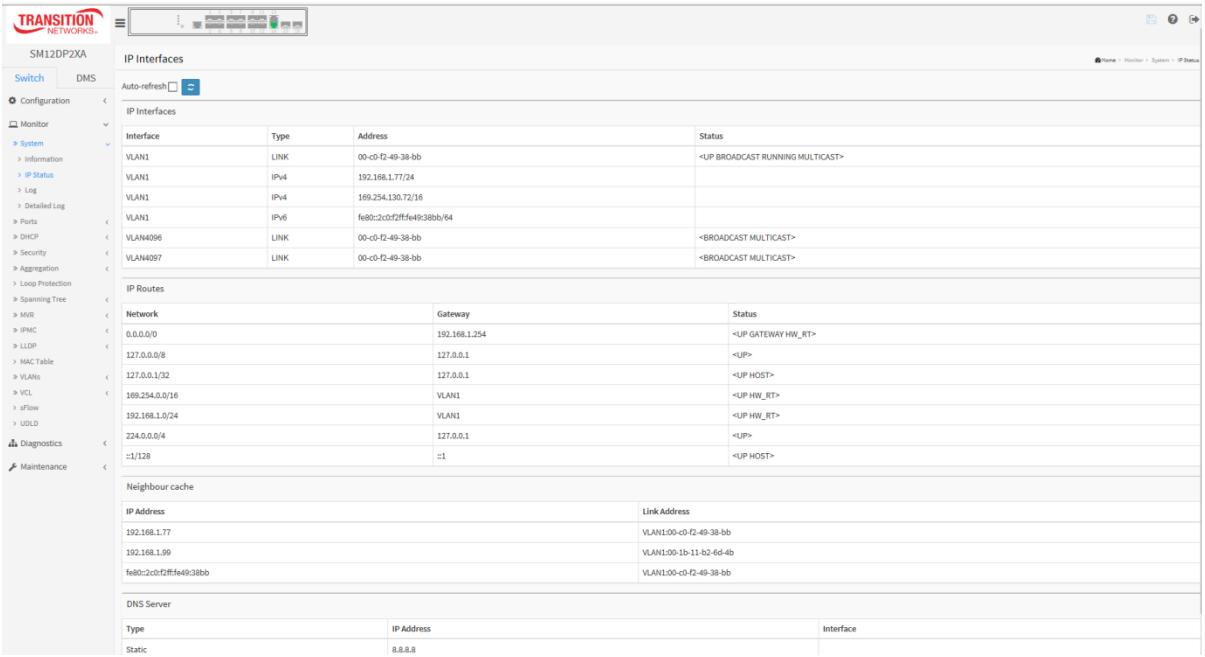
This page displays the status of the IP protocol layer. The status is displayed for the IP interfaces, the IP routes, neighbor cache (ARP cache), and DNS Server.

Web Interface

To display the log configuration in the web interface:

1. Click Monitor, System, IP Status.
2. View the IP address information.

Figure 3- 1.2: IP Status



Parameter descriptions:

IP Interfaces

Interface : Displays the name of the interface.

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

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

Status : Displays the status flags of the interface and/or address (e.g., <UP BROADCAST RUNNING MULTICAST> or <BROADCAST MULTICAST>).

IP Routes

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

Gateway : Displays the gateway address of this route.

Status : Displays the status flags of the route (e.g., <UP>, <UP HOST>, or <UP GATEWAY HW_RT>).

Neighbour cache

IP Address : Displays the IP address of the entry.

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

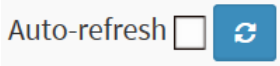
DNS Server

Type: The configuration type of DNS server (e.g., Static).

IP Address: The IP address of the DNS server (e.g., 8.8.8.8).

Interface: blank or the DNS Server interface type.

Buttons



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

Refresh: Click to refresh the page immediately.

3-1.3 Log

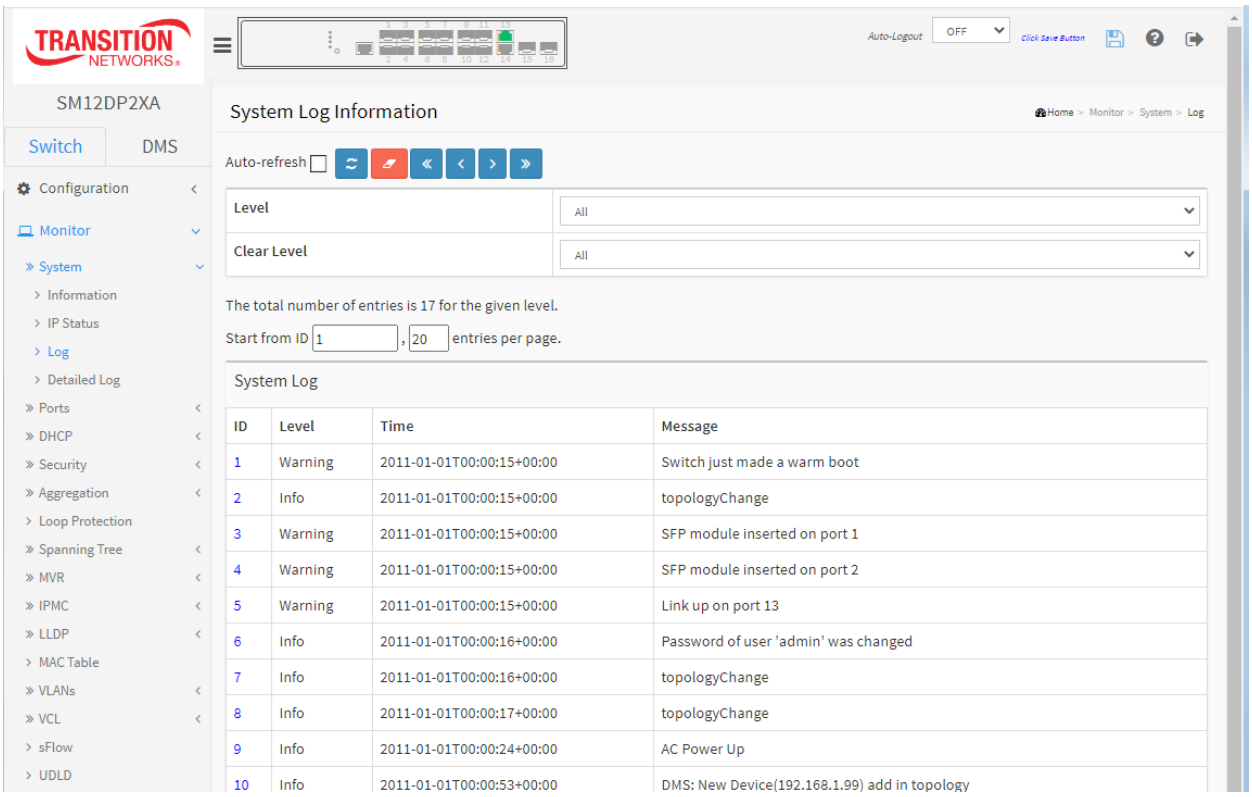
This page displays the system log (Syslog) information.

Web Interface

To display the log configuration in the web interface:

1. Click Monitor, System, Log.
2. View the log information.

Figure 3- 1.3: System Log Information



Parameter descriptions:

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

Level : The relative system log entry level. These levels 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.

All : The system log entry includes all of the above.

Clear Level : Specify which system log entries are to be cleared. To clear specific system log entries, select the clear level first then click the Clear button.

ID : The ID of the system log entry for this line of the table. Click the linked ID number to display its Detailed System Log Information.

Time : Displays the log record by device time of the system log entry.

Message :Displays the log detail 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.

<<: Updates the system log entries, starting from the first available entry ID.

< : Updates the system log entries, ending at the last entry currently displayed.

> : Updates the system log entries, starting from the last entry currently displayed.

>> : Updates the system log entries, ending at the last available entry ID.

System Log Message Examples

Level	Message
Notice	LINK-UPDOWN: Interface Vlan 1, changed state to down.
Warning	Link up on port 14
Info	Password of user 'admin' was changed
Warning	Switch just made a warm boot
Info	topologyChange
Warning	Link down on port 14
Info	Login passed for user 'admin'
Info	DMS: New Device(192.168.1.99) add in topology
Info	User 'admin' logout
Warning	SFP module inserted on port 15 (also displays the SFP Connector Type, Fiber Type, etc.
Info	DMS: New Device(192.168.0.99) add in topology
Info	DMS: Device(192.168.0.99) Off-line is caused by network disconnection.

3-1.4 Detailed Log

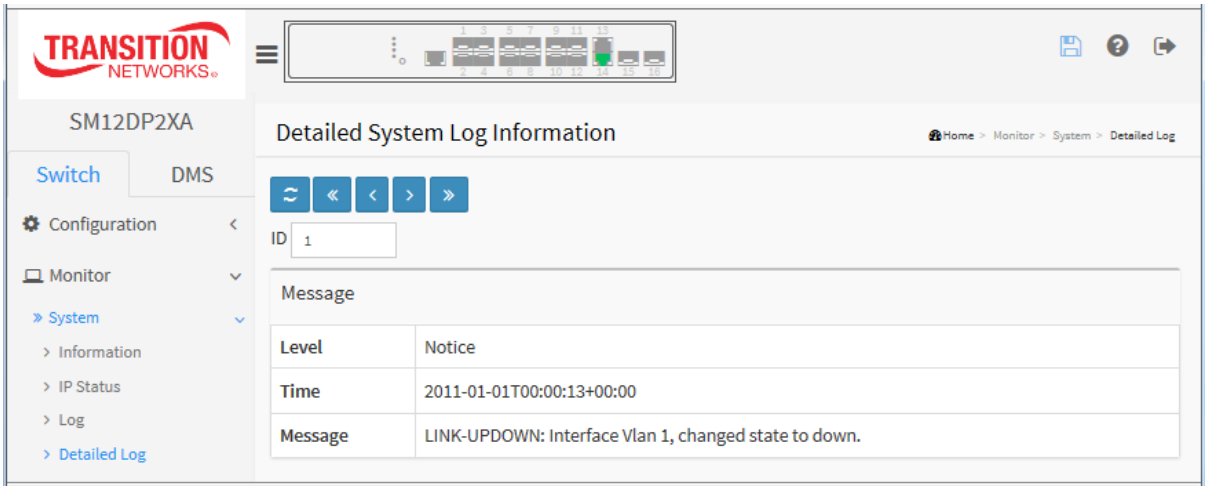
This page displays the detailed log information.

Web Interface

To display the detailed log configuration in the web interface:

1. Click Monitor, System, Detailed Log.
2. View the detailed log information.
3. Enter another log ID or use the buttons to display different log message data.

Figure 3- 1.4: Detailed System Log Information



Parameter descriptions:

ID : The ID of the system log entry. Displays entry 1 by default. You can enter the ID of any existing log message to display its data. If an entry ID number does not exist, the message "*No system log entry*" displays.

Level: The level of the system log entry.

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.

Time : The occurred time of the system log entry in the format *2011-01-01T00:00:13+00:00*.

Message : The detailed message of the specified system log entry (e.g., *Link up on port 14*).

Buttons

Refresh: Updates the system log entries, starting from the current entry ID.

<< : Updates the system log entries to the first available entry ID

< : Updates the system log entry to the previous available entry ID

> : Updates the system log entry to the next available entry ID

> : Updates the system log entry to the last available entry ID.

3-2 Ports

This page displays the Port detail parameters of the switch.

3-2.1 Traffic Overview

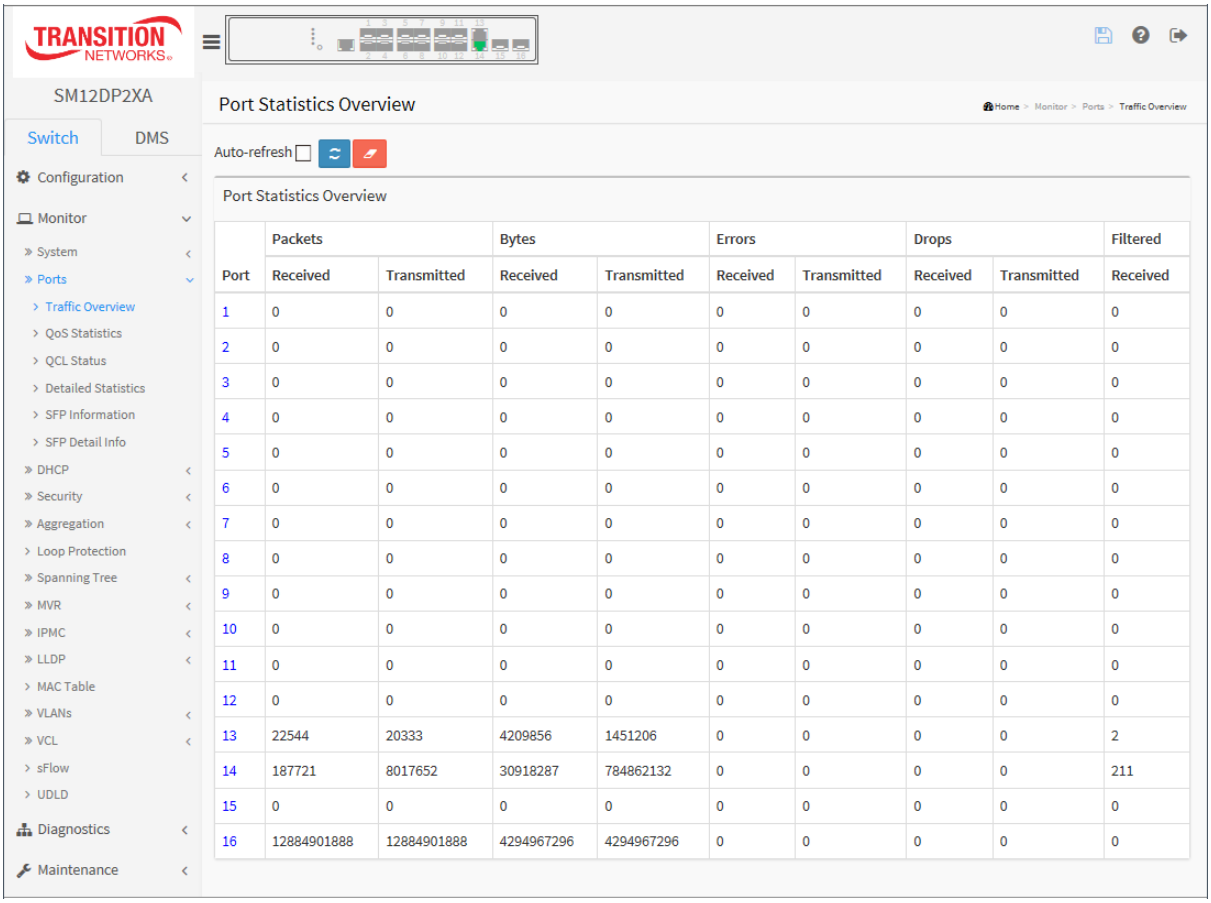
This page lets you configure the Port statistics information and provides overview of general traffic statistics for all switch ports.

Web Interface

To display the Port Statistics Overview in the web interface:

1. Click Monitor, Port, Traffic Overview.
2. To automatically refresh the page click the Auto-refresh button.
3. Click Refresh to refresh the port statistics, or click Clear to clear all page information.
4. Click a linked port number in the Port column to display the port's Detailed Port Statistics.

Figure 3-2.1: Port Statistics Overview



	Packets		Bytes		Errors		Drops		Filtered
Port	Received	Transmitted	Received	Transmitted	Received	Transmitted	Received	Transmitted	Received
1	0	0	0	0	0	0	0	0	0
2	0	0	0	0	0	0	0	0	0
3	0	0	0	0	0	0	0	0	0
4	0	0	0	0	0	0	0	0	0
5	0	0	0	0	0	0	0	0	0
6	0	0	0	0	0	0	0	0	0
7	0	0	0	0	0	0	0	0	0
8	0	0	0	0	0	0	0	0	0
9	0	0	0	0	0	0	0	0	0
10	0	0	0	0	0	0	0	0	0
11	0	0	0	0	0	0	0	0	0
12	0	0	0	0	0	0	0	0	0
13	22544	20333	4209856	1451206	0	0	0	0	2
14	187721	8017652	30918287	784862132	0	0	0	0	211
15	0	0	0	0	0	0	0	0	0
16	12884901888	12884901888	4294967296	4294967296	0	0	0	0	0

Parameter descriptions: The displayed counters are:

Port : The logical port for the settings contained in the same row. Click a linked port number in this column to display the port's Detailed Port Statistics.

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

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

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

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

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

Buttons

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

Refresh: Click to refresh the page.

Clear: Clears the counters for all ports.

3-3.2 QoS Statistics

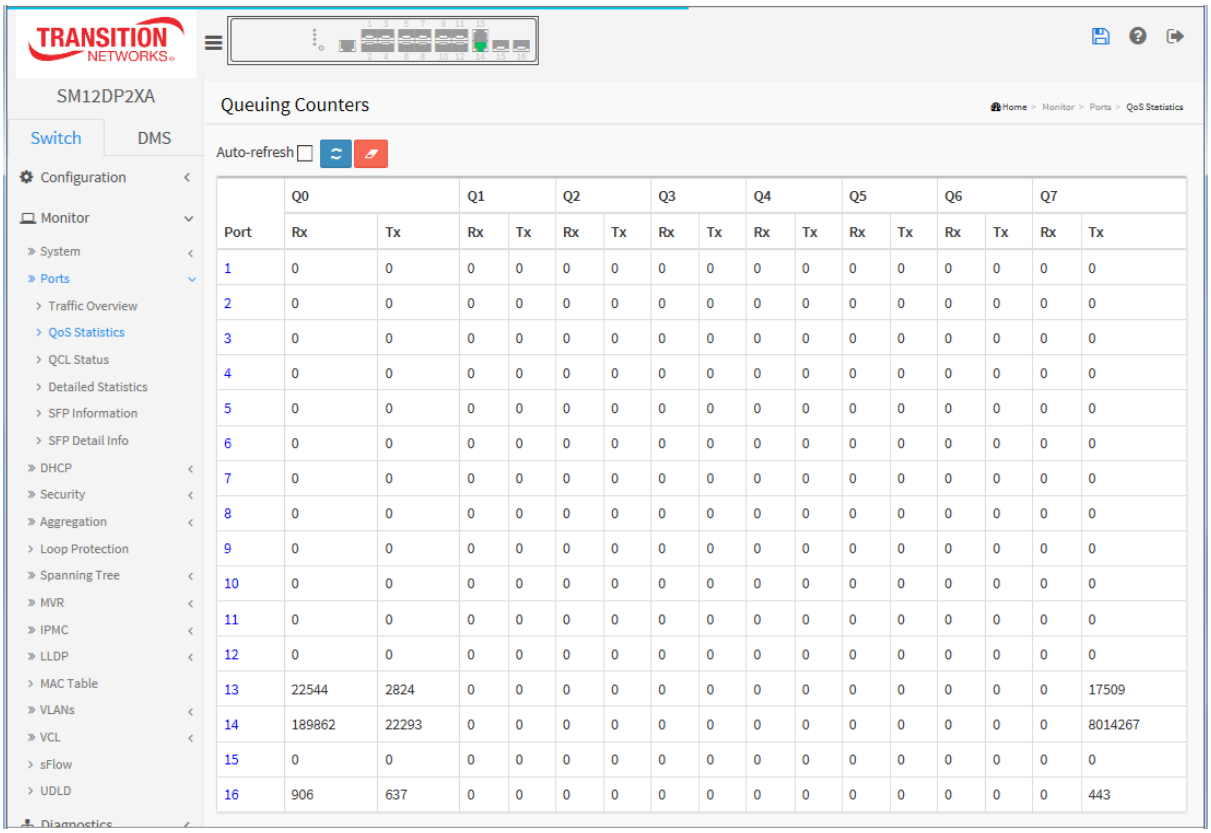
This page displays statistics for the different queues for all switch ports.

Web Interface

To display the Queuing Counters in the web interface:

1. Click Monitor, Ports, QoS Statistics.
2. To automatically refresh the page information, check the Auto-refresh checkbox.
3. Click Refresh to refresh the Queuing Counters or click Clear to clear all page information.
4. Click a linked port number in the Port column to display the port's Detailed Port Statistics.

Figure 3-3.2: Queuing Counters



	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
10	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
11	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
12	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
13	22544	2824	0	0	0	0	0	0	0	0	0	0	0	0	0	17509
14	189862	22293	0	0	0	0	0	0	0	0	0	0	0	0	0	8014267
15	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
16	906	637	0	0	0	0	0	0	0	0	0	0	0	0	0	443

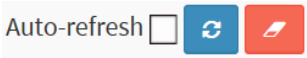
Parameter descriptions:

Port : The logical port for the settings contained in the same row. Click a linked port number in this column to display the port's Detailed Port Statistics.

Qn : Qn is the Queue number, there are eight QoS queues per port. Q0 is the lowest priority queue.

Rx/Tx : The number of received and transmitted packets per queue.

Buttons



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

Refresh: Click to refresh the page.

Clear: Clears the counters for all ports.

3-3.3 QCL Status

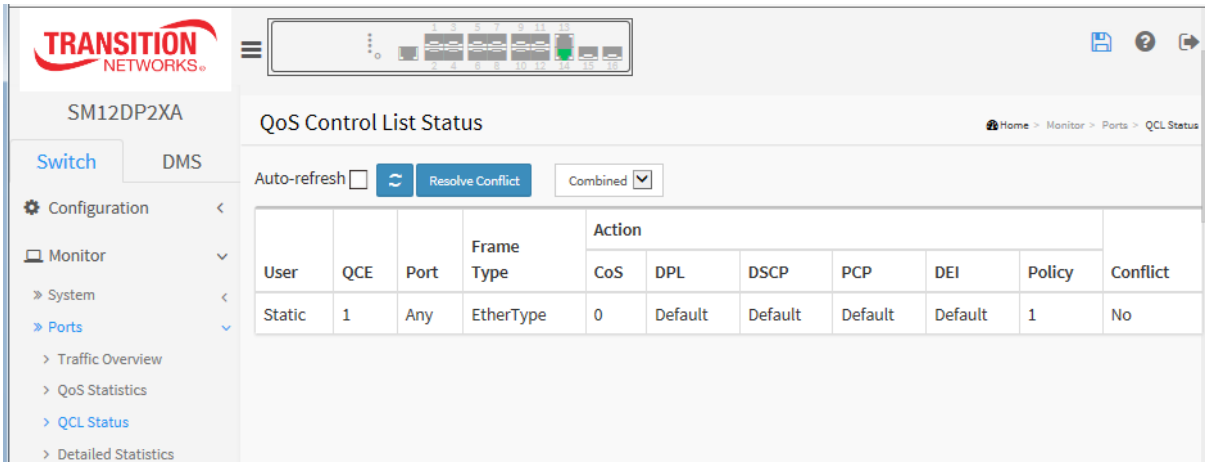
This page displays the QCL status of different QCL users. Each row describes the QCE that is defined. A “conflict” exists if a specific QCE is not applied to the hardware due to hardware limitations. The maximum number of QCEs is 256 on each switch.

Web Interface

To display the QoS Control List Status in the web interface:

1. Click Monitor, Ports, QCL Status.
2. Select Combined, Static, Voice VLAN, DMS, or Conflict at the dropdown.
3. To automatically refresh the page every 3 seconds check the Auto-refresh checkbox.
4. Click the Refresh button to immediately refresh the page data.

Figure 3-3.3: QoS Control List Status



Parameter descriptions:

User : Displays the QCL user. Displays “*No entries*” if there are no users to display.

QCE : Displays the index of QCE.

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

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

Any: Match any frame type.

EtherType: Match EtherType frames.

LLC: Match (LLC) frames.

SNAP: Match (SNAP) frames.

IPv4: Match IPv4 frames.

IPv6: Match IPv6 frames.

Action : Displays the classification action taken on an 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.

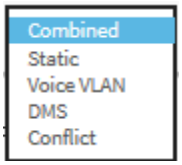
Conflict : Displays Conflict status of QCL entries. It may happen that resources required to add a QCE may not available, in that case it shows conflict status as 'Yes', otherwise it is always 'No'.
Note that conflict can be resolved by releasing the H/W resources required to add QCL entry on pressing 'Resolve Conflict' button.

Buttons

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

Resolve Conflict: Click to release the resources required to add QCL entry, in case conflict status for any QCL entry is 'yes'.

Refresh: Click to immediately refresh the page manually.



QCL status drop down: Select the QCL status to be displayed from this drop down list. The selections are Combined, Static, Voice VLAN, DMS, and Conflict.

3-3.4 Detailed Statistics

The section describes how to provide detailed traffic statistics for a specific switch port. Use the port select box to select which switch port details to display.

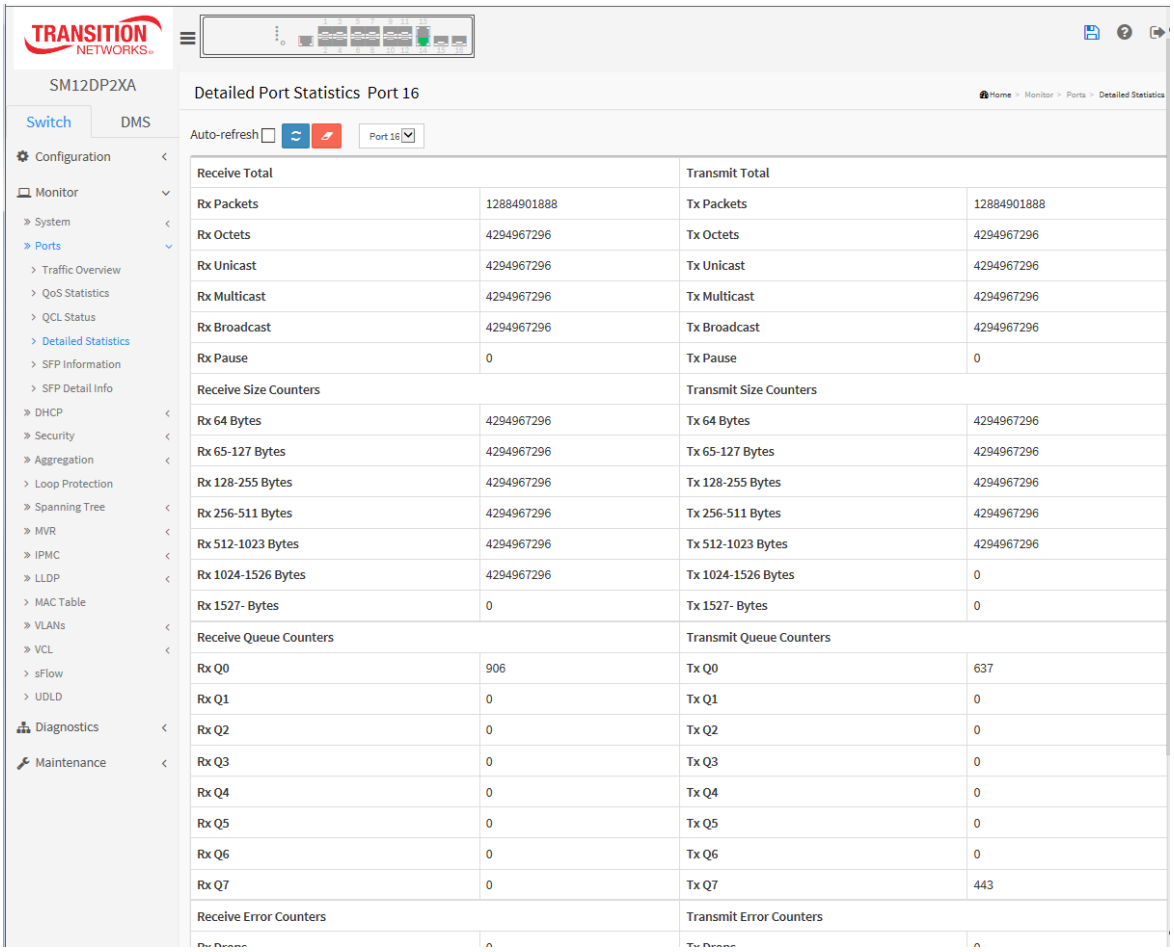
The displayed counters are the totals for receive and transmit, the size counters for receive and transmit, and the error counters for receive and transmit.

Web Interface

To display the per-port detailed Statistics Overview in the web interface:

1. Click Monitor, Ports, Detailed Statistics.
2. Scroll the Port select box to select which port you want to show the detailed port statistics.
3. To automatically refresh page information every 3 seconds check the Auto-refresh checkbox.
4. Click Refresh to refresh the port detailed statistics or click Clear to clear all page information.

Figure 3-3.4: Detailed Port Statistics



Receive Total		Transmit Total	
Rx Packets	12884901888	Tx Packets	12884901888
Rx Octets	4294967296	Tx Octets	4294967296
Rx Unicast	4294967296	Tx Unicast	4294967296
Rx Multicast	4294967296	Tx Multicast	4294967296
Rx Broadcast	4294967296	Tx Broadcast	4294967296
Rx Pause	0	Tx Pause	0
Receive Size Counters		Transmit Size Counters	
Rx 64 Bytes	4294967296	Tx 64 Bytes	4294967296
Rx 65-127 Bytes	4294967296	Tx 65-127 Bytes	4294967296
Rx 128-255 Bytes	4294967296	Tx 128-255 Bytes	4294967296
Rx 256-511 Bytes	4294967296	Tx 256-511 Bytes	4294967296
Rx 512-1023 Bytes	4294967296	Tx 512-1023 Bytes	4294967296
Rx 1024-1526 Bytes	4294967296	Tx 1024-1526 Bytes	0
Rx 1527- Bytes	0	Tx 1527- Bytes	0
Receive Queue Counters		Transmit Queue Counters	
Rx Q0	906	Tx Q0	637
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	443
Receive Error Counters		Transmit Error Counters	

Parameter descriptions:

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

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.

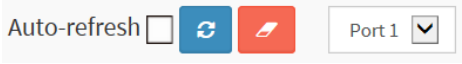
Long frames are frames that are longer than the configured maximum frame length for this port.

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.

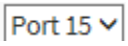
Buttons



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

Refresh: Click to refresh the page.

Clear: Clears the counters for the selected port.



: The port select box lets you select which port's data you want displayed.

3-3.5 SFP Information

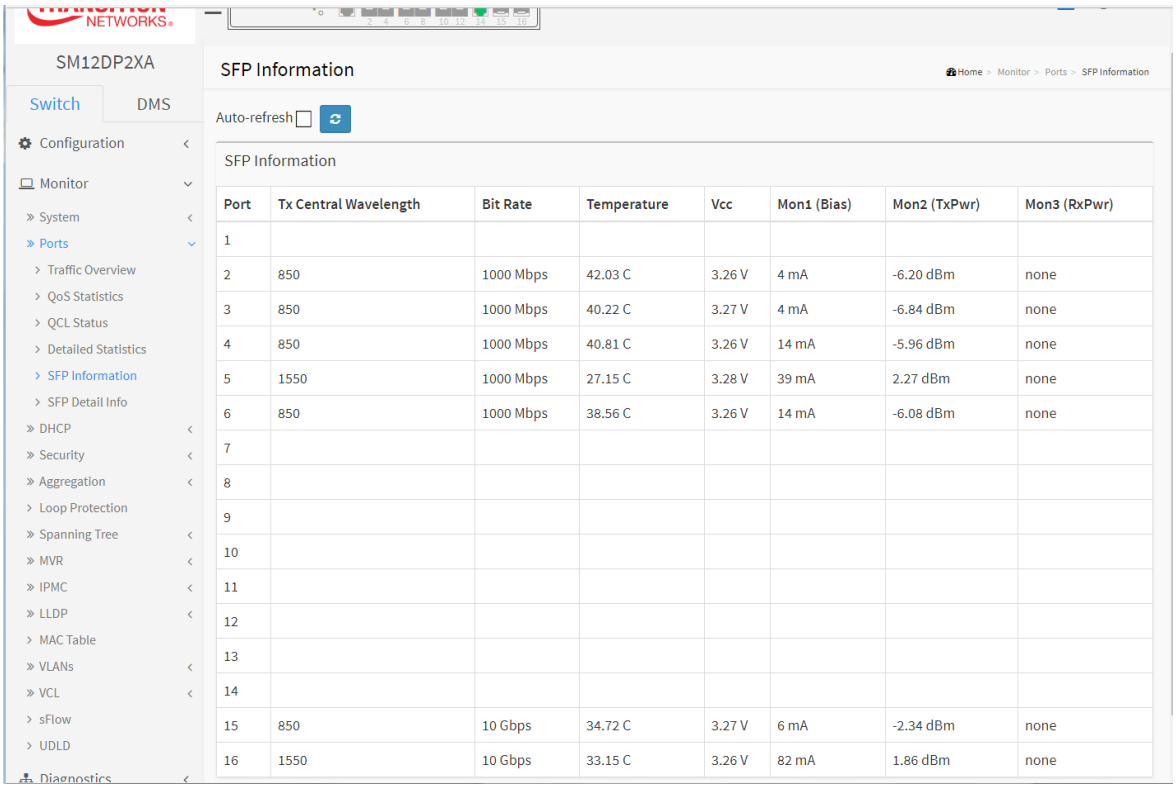
This page displays general SFP information and monitoring information. The information includes Connector type, Fiber type, wavelength, Bit Rate, Vendor OUI, etc.

Web Interface

To display the SFP information in the web interface:

1. Click Monitor, Ports, SFP Information.
2. View the displayed SFP Information.

Figure 3-3.5: SFP Information Overview



Port	Tx Central Wavelength	Bit Rate	Temperature	Vcc	Mon1 (Bias)	Mon2 (TxPwr)	Mon3 (RxPwr)
1							
2	850	1000 Mbps	42.03 C	3.26 V	4 mA	-6.20 dBm	none
3	850	1000 Mbps	40.22 C	3.27 V	4 mA	-6.84 dBm	none
4	850	1000 Mbps	40.81 C	3.26 V	14 mA	-5.96 dBm	none
5	1550	1000 Mbps	27.15 C	3.28 V	39 mA	2.27 dBm	none
6	850	1000 Mbps	38.56 C	3.26 V	14 mA	-6.08 dBm	none
7							
8							
9							
10							
11							
12							
13							
14							
15	850	10 Gbps	34.72 C	3.27 V	6 mA	-2.34 dBm	none
16	1550	10 Gbps	33.15 C	3.26 V	82 mA	1.86 dBm	none

Parameter descriptions:

Tx Central Wavelength : Displays the fiber optical transmitting central wavelength (e.g., 850 nm, 1310 nm, 1550 nm, etc.).

Bit Rate: Displays the nominal bit rate of the transceiver (e.g., 1000 Mbps or 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.

Vcc : Displays the internally measured transceiver supply voltage. Accuracy is vendor-specific but must be better than 3 percent of the manufacturer's nominal value over specified operating temperature and voltage. Note that in some transceivers, transmitter supply voltage and receiver supply voltage are isolated. In that case, only one supply is monitored. Refer to the SFP device documentation for details.

Mon1 (Bias) : Displays the measured TX bias current in 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. 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 enable an automatic refresh of the page at regular intervals.

Refresh : Click to refresh the page. Any changes made locally will be undone.

3-3.6 SFP Detail Information

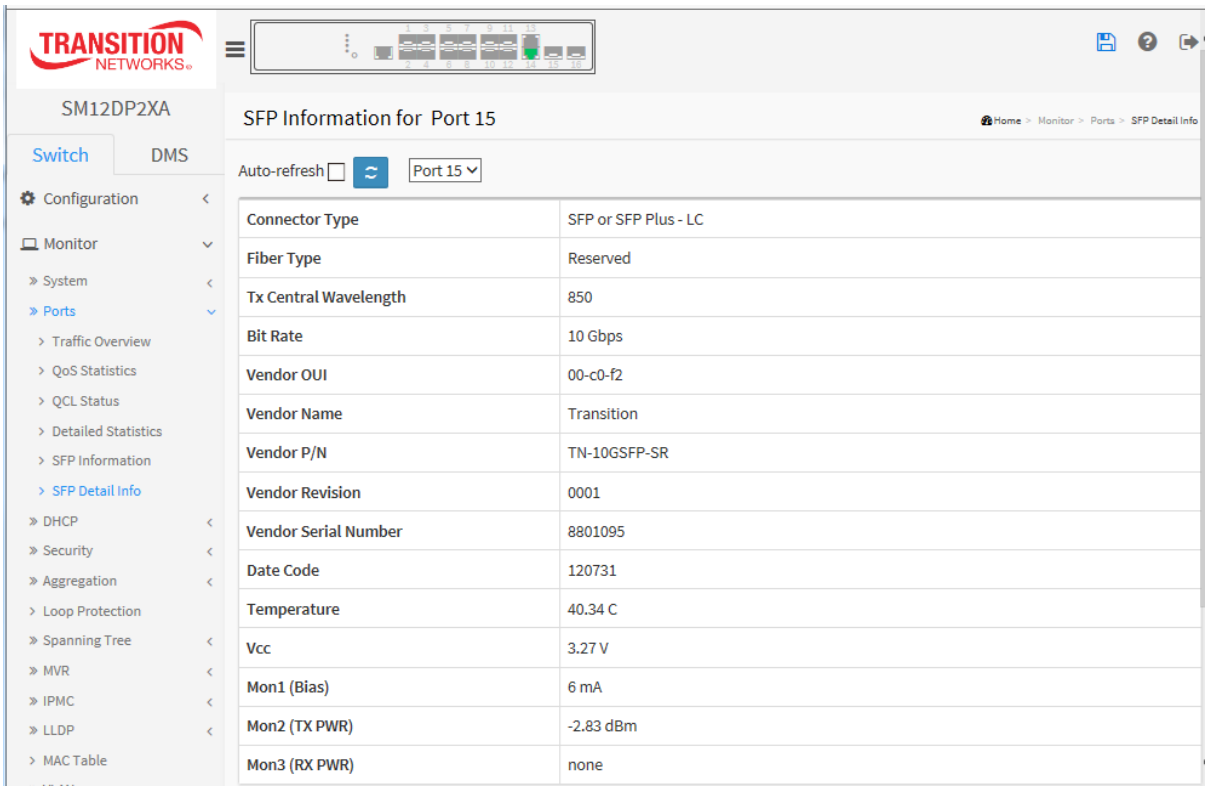
This page displays detailed SFP module information for SFP modules /ports of the switch.
The information includes Connector type, Fiber Type, Wavelength, Bit Rate, Vendor OUI, etc.

Web Interface

To display the SFP information in the web interface:

1. Click Monitor, Ports, SFP Detail Info.
2. Select the SFP port (port 1-12, 15, or 16).
3. View the displayed SFP Information details for the selected SFP.

Figure 3-3.6: SFP Detail Information



Parameter descriptions:

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

Fiber Type: Displays the fiber mode (e.g., Multi-Mode, Single-Mode, Reserved, Multi-mode (MM), etc.).

Tx Central Wavelength: Displays the fiber optical transmitting central wavelength (e.g., 850 nm, 1310 nm, 1550 nm, etc.).

Baud Rate: Displays the maximum baud rate of the fiber module supported (e.g., 1 Gbps, 10 Gbps).

Vendor OUI: Displays the Manufacturer's OUI code which is assigned by IEEE (e.g., 00-c0-f2).

Vendor Name: Displays the company name of the module manufacturer (e.g., Transition).

Vendor P/N: Displays the product name given by the module manufacturer (e.g., TN-10GSFP-SR, TN-SFP-OC3S, TN-10GSFP-LR8M, or TN-SFP-OC3M).

Vendor Rev (Revision): Displays the module revision (e.g., 0001).

Vendor SN (Serial Number): Displays the serial number assigned by the manufacturer (e.g., 8631044).

Date Code: Displays the date this SFP module was made (e.g., 120731 or 070410).

Temperature: Displays the current temperature of SFP module (e.g., 42.06 C).

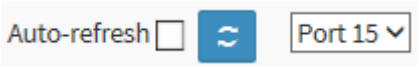
Vcc: Displays the working DC voltage of SFP module (e.g., 3.27 V).

Mon1 (Bias) mA: Displays the Bias current of SFP module (e.g., 6 mA).

Mon2 (TX PWR): Displays the transmit power of SFP module (e.g., -2.81 dBm).

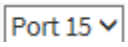
Mon3 (RX PWR): Displays the receiver power of SFP module (e.g., none).

Buttons



Auto-refresh: Check this box to enable an automatic refresh of the page at regular intervals.

Refresh : Click to refresh the page. Any changes made locally will be undone.



: The port select box determines which port is affected by clicking the buttons.

3-4 DHCP

3-4.1 Server

DHCP Server is used to allocate network addresses and deliver configuration parameters to dynamically configured hosts called DHCP client.

3-4.1.1 Statistics

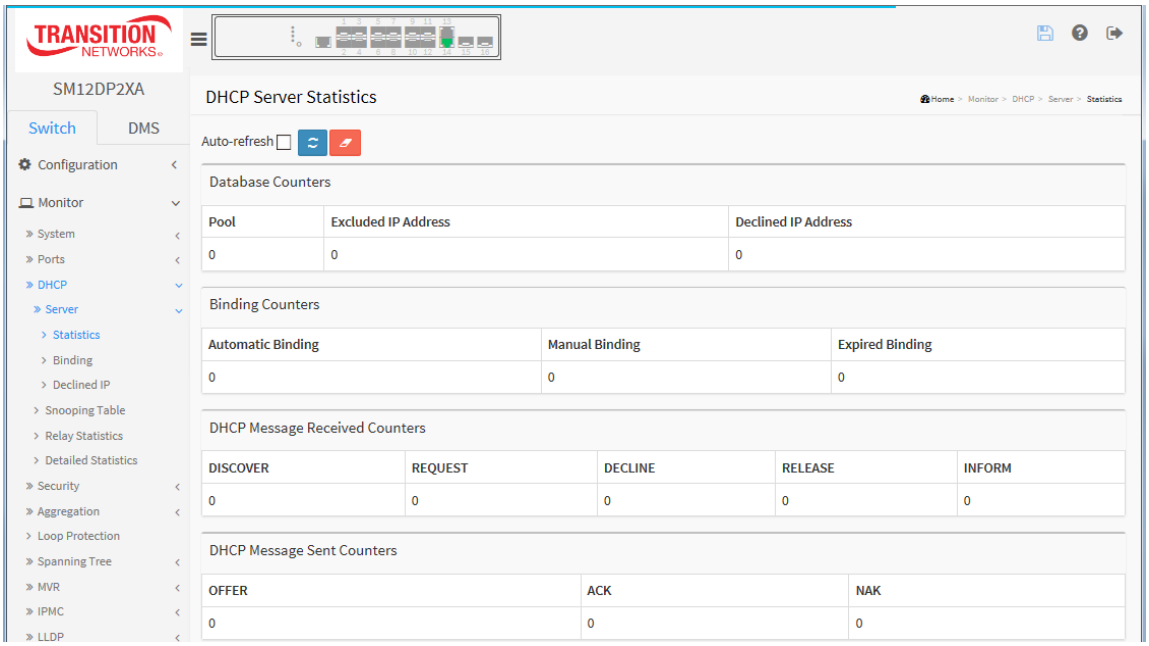
This page displays the database counters and the number of DHCP messages sent and received by DHCP server.

Web Interface

To display DHCP Server statistics in the web interface:

1. Navigate to Monitor > DHCP > Server > Statistics.
2. View the DHCP Server Statistics in the web interface:

Figure 3-4.1.1: DHCP Server Statistics



Parameter descriptions:

Database Counters

Pool : Number of DHCP pools.

Excluded IP Address : Number of excluded IP address ranges.

Declined IP Address : Number of declined IP addresses.

Binding Counters

Automatic Binding : Number of bindings with network-type pools.

Manual Binding : Number of bindings that administrator assigns an IP address to a client. That is, the pool is of host type.

Expired Binding : Number of bindings that their lease time expired or they are cleared from Automatic/Manual type bindings.

DHCP Message Received Counters

DISCOVER : Number of DHCP DISCOVER messages received.

REQUEST : Number of DHCP REQUEST messages received.

DECLINE : Number of DHCP DECLINE messages received.

RELEASE : Number of DHCP RELEASE messages received.

INFORM : Number of DHCP INFORM messages received.

DHCP Message Sent Counters

OFFER : Number of DHCP OFFER messages sent.

ACK : Number of DHCP ACK (Acknowledge) messages sent.

NAK : Number of DHCP NAK (Negative Acknowledge) messages sent.

Buttons:

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

Clear: Clears the counters for the selected port.

Refresh: Click to refresh the page immediately.

3-4.1.2 Binding

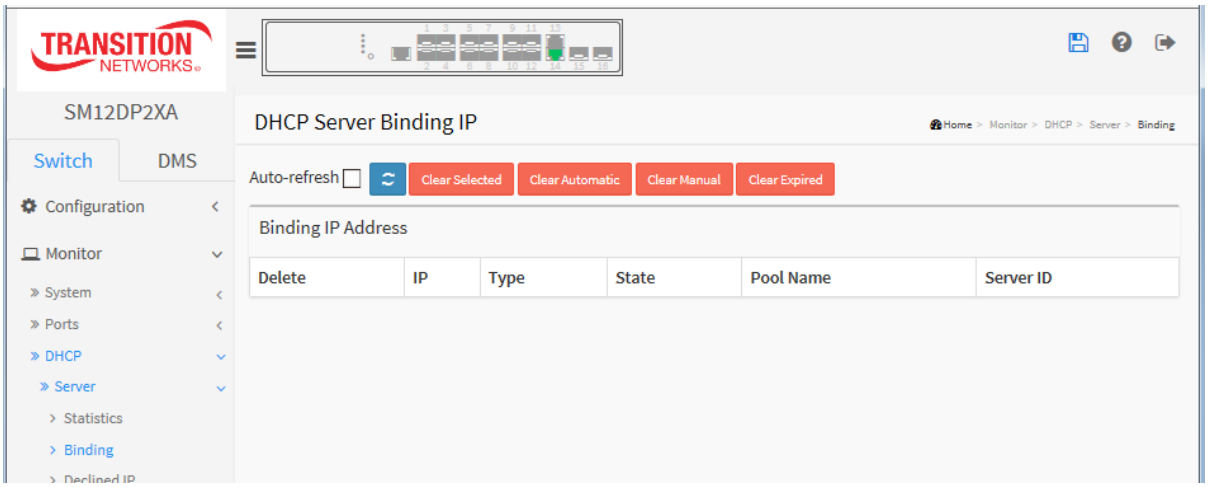
This page displays bindings generated for DHCP clients.

Web Interface

To display DHCP Server Binding IP in the web interface:

1. Click Monitor, DHCP, Server, Binding.
2. View the DHCP Server Binding IP table information.

Figure 3-4.1.2: DHCP Server Binding IP Table



Parameter descriptions:

IP : IP address allocated to DHCP client.

Type : Type of binding. Possible types are Automatic, Manual, Expired.

State : State of binding. Possible states are Committed, Allocated, Expired.

Pool Name : The pool that generates the binding.

Server ID : Server IP address to service the binding.

Buttons:

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

Refresh: Click to refresh the page immediately.

Clear Selected: Click to clear selected bindings. If the selected binding is Automatic or Manual, then it is changed to be Expired. If the selected binding is Expired, then it is freed.

Clear Automatic: Click to clear all Automatic bindings and Change them to Expired bindings.

Clear Manual: Click to clear all Manual bindings and Change them to Expired bindings.

Clear Expired: Click to clear all Expired bindings and free them.

3-4.1.3 Declined IP

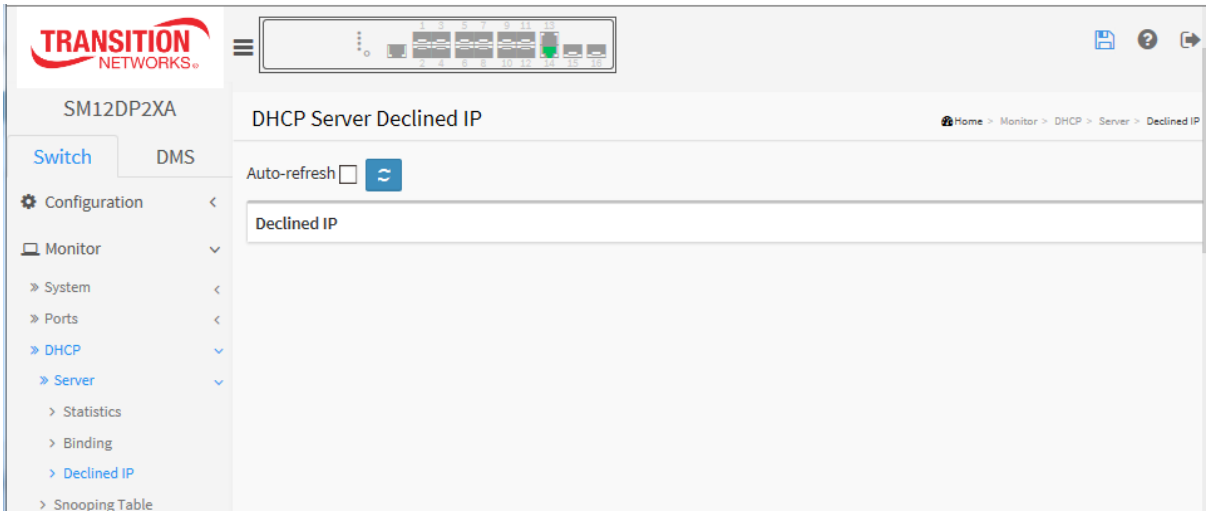
This page displays declined IP addresses.

Web Interface

To display DHCP Server Declined IP in the web interface:

1. Click Monitor, DHCP, Server, Declined IP.
2. Observe the DHCP Server Declined IP table data.

Figure 3-4.1.3: Declined IP



Parameter descriptions:

IP : IP address allocated to DHCP client.

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

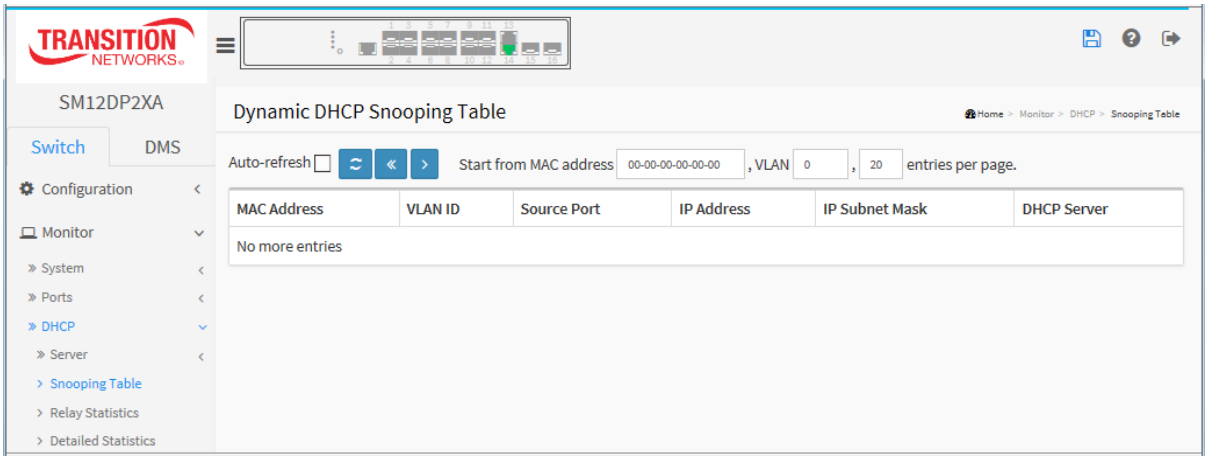
This page displays the dynamic IP assigned information after DHCP Snooping mode is disabled.
All DHCP clients obtained the dynamic IP address from the DHCP server will be listed in this table except for local VLAN interface IP addresses. Entries in the Dynamic DHCP snooping Table are shown on this page.

Web Interface

To monitor a DHCP Snooping Table via the web interface:

1. Click Monitor, DHCP, Snooping Table.
2. Select “Start from MAC address”, “VLAN”, and “entries per page”.
3. View the Dynamic DHCP Snooping Table parameters.

Figure 3-4.2: Dynamic DHCP Snooping Table



Parameter descriptions:

MAC Address : Displays the user MAC address of the entry.

VLAN ID : Displays the VLAN-ID in which the DHCP traffic is permitted.

Source Port : Displays the Switch Port number for which the entries are displayed.

IP Address : Displays the User IP address of the entry.

IP Subnet Mask : Displays the User IP subnet mask of the entry.

DHCP Server : Displays the 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

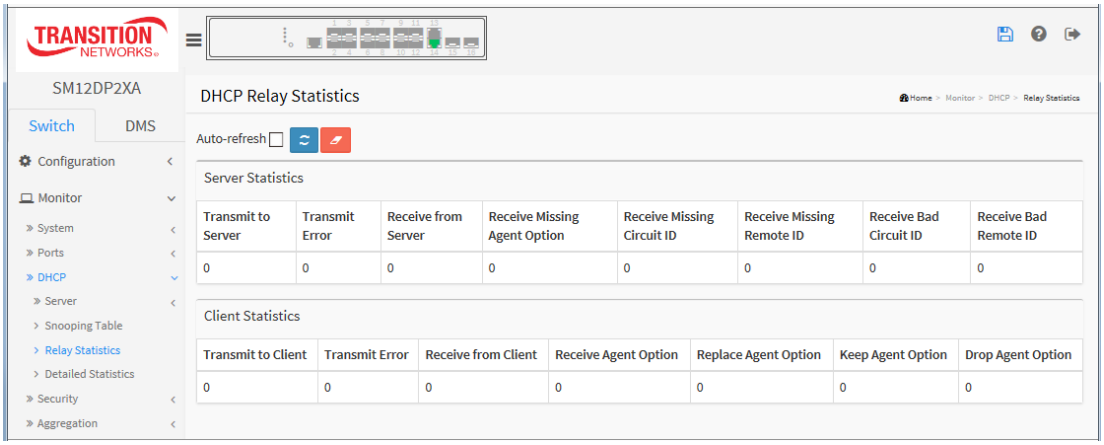
This page displays DHCP relay server and client statistics.

Web Interface

To monitor a DHCP Relay statistics in the web interface:

1. Click Monitor, DHCP, Relay Statistics.
2. View the displayed parameters.

Figure 3-4.3: DHCP Relay Statistics



Parameter descriptions:

Server Statistics

Transmit to Server : The number of packets that are relayed from client to server.

Transmit Error : The number of packets that resulted in errors while being sent to clients.

Receive from Server : The number of packets received from server.

Receive Missing Agent Option: The number of packets received without agent information options.

Receive Missing Circuit ID : The number of packets received with the Circuit ID option missing.

Receive Missing Remote ID : The number of packets received with the Remote ID option missing.

Receive Bad Circuit ID: The number of packets whose Circuit ID option did not match known circuit ID.

Receive Bad Remote ID : The number of packets whose Remote ID option did not match known Remote ID.

Client Statistics

Transmit to Client : The number of relayed packets from server to client.

Transmit Error : The number of packets that resulted in error while being sent to servers.

Receive from Client : The number of received packets from server.

Receive Agent Option : The number of received packets with relay agent information option.

Replace Agent Option : The number of packets which were replaced with relay agent information option.

Keep Agent Option : The number of packets whose relay agent information was retained.

Drop Agent Option : The number of packets that were dropped which were received with relay agent information.

3-4.4 Detailed Statistics

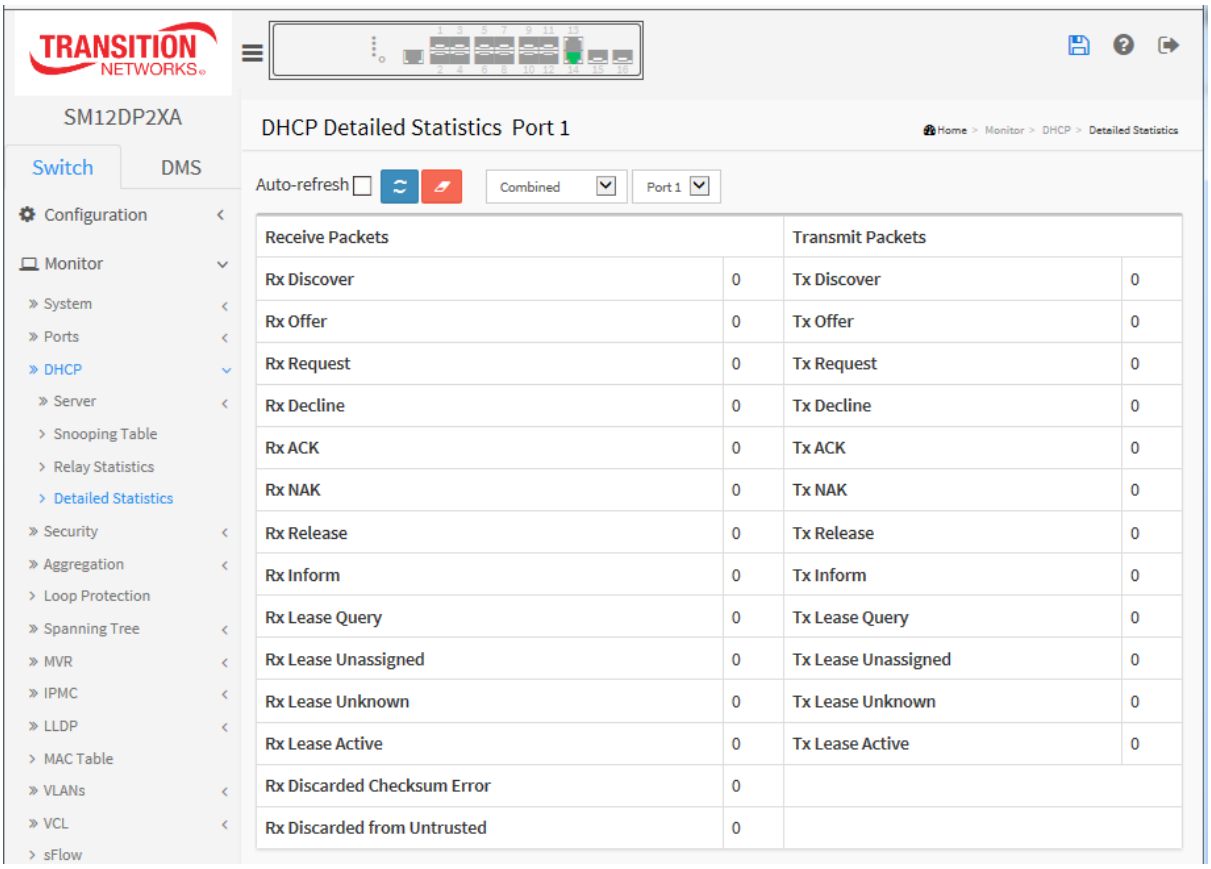
This page displays detailed DHCP statistics for a selected DHCP port. Note that the normal forward per-port TX statistics is not increased if the incoming DHCP packet is done by the L3 forwarding mechanism. Clearing the statistics on a specific port may not take effect on global statistics since it gathers the different layer overview.

Web Interface

To monitor DHCP Relay Statistics via the web interface:

1. Click Monitor, DHCP, Detailed Statistics.
2. Select a DHCP User and Port and view the displayed parameters.

Figure 3-4.4: DHCP Detailed Statistics



Parameter descriptions:

Server Statistics

Rx and Tx Discover : The number of discover (option 53 with value 1) packets received and transmitted.

Rx and Tx Offer : The number of offer (option 53 with value 2) packets received and transmitted.

Rx and Tx Request : The number of request (option 53 with value 3) packets received and transmitted.

Rx and Tx Decline: The number of decline (option 53 with value 4) packets received and transmitted.

Rx and Tx ACK: The number of ACK (option 53 with value 5) packets received and transmitted.

Rx and Tx NAK: The number of NAK (option 53 with value 6) packets received and transmitted.

Rx and Tx Release: The number of release (option 53 with value 7) packets received and transmitted.

Rx and Tx Inform: The number of inform (option 53 with value 8) packets received and transmitted.

Rx and Tx Lease Query: The number of lease query (option 53 with value 10) packets received and transmitted.

Rx and Tx Lease Unassigned: The number of lease unassigned (option 53 with value 11) packets received and transmitted.

Rx and Tx Lease Unknown: The number of lease unknown (option 53 with value 12) packets received and transmitted. Rx and Tx Lease Active

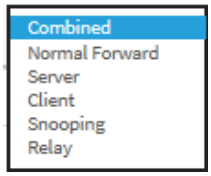
Rx and Tx Lease Active: The number of lease active (option 53 with value 13) packets received and transmitted.

Rx Discarded checksum error: The number of discard packet that IP/UDP checksum is error.

Rx Discarded from Untrusted: The number of discarded packets coming from untrusted port.

Buttons

: The DHCP user select box determines which DHCP user is affected by clicking the buttons. Select Combined, Normal Forward, Server, Client, Snooping, or Relay).



: The port select box determines which port is affected by clicking the 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.

3-5 Security

3-5.1 Access Management Statistics

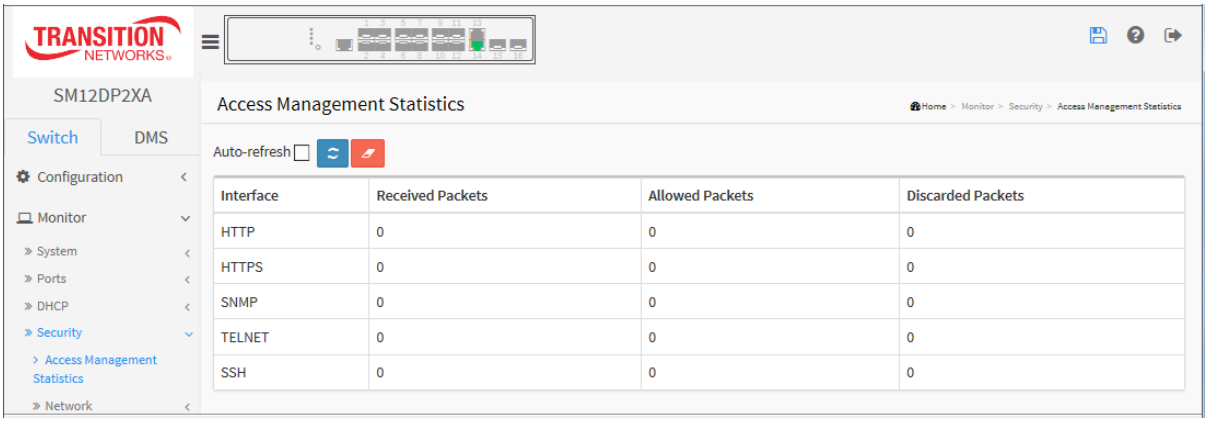
This page displays detailed statistics of the Access Management methods (HTTP, HTTPS, SNMP, TELNET, and SSH).

Web Interface

To view Access Management Statistics in the web interface:

1. Click Monitor, Security, Access Management Statistics.
2. Check Auto-refresh.
3. Click Refresh to refresh the port detailed statistics or click Clear to clear all page information.

Figure 3-5.1: Access Management Statistics



Parameter descriptions:

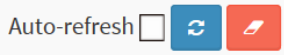
Interface : The interface type through which the remote host can access the switch.

Received Packets : Number of received packets from the interface when access management mode is enabled.

Allowed Packets : Number of allowed packets from the interface when access management mode is enabled

Discarded Packets. : Number of discarded packets from the interface when access management mode is enabled.

Buttons



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

Refresh: Click to refresh the page immediately.

Clear: Clears the counters for the selected port.

3-5.2 Network

3-5.2.1 Port Security

3-5.2.1.1 Switch

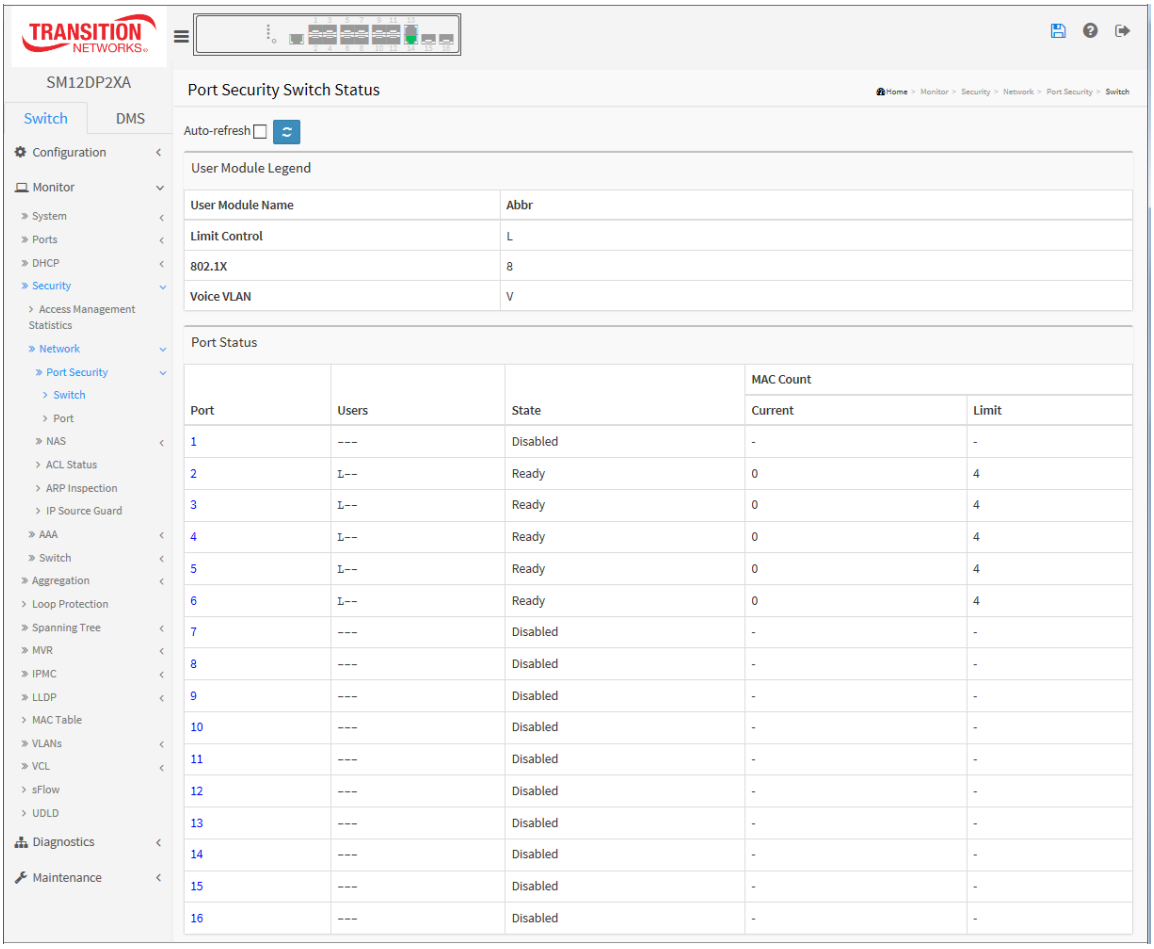
This page displays the Port Security status. Port Security is a module with no direct configuration. Configuration comes indirectly from other modules (the user modules). When a user module has enabled port security on a port, the port is set up for software-based learning. In this mode, frames from 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 user module chooses to block it, it will be blocked until that user module decides otherwise. The status page is divided into two sections; one with a legend of user modules and one with the actual port status.

Web Interface

To configure a Port Security Switch Status Configuration in the web interface:

1. Click Monitor > Security > Network > Port Security > Switch.
2. Check the Auto-refresh checkbox.
3. Click Refresh to refresh the port detailed statistics.

Figure 3-5.2.1.1: Port Security Switch Status



Parameter descriptions:

User Module Legend : This section displays all user modules that may request Port Security services.

User Module Name : The full name of a module that may request Port Security services.

Abbr : A one-letter abbreviation of the user module. This is used in the Users column in the port status table. The user module names are abbreviated as Limit Control = L, 802.1X = 8, and Voice VLAN = V.

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 link 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. 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 (**-**).

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

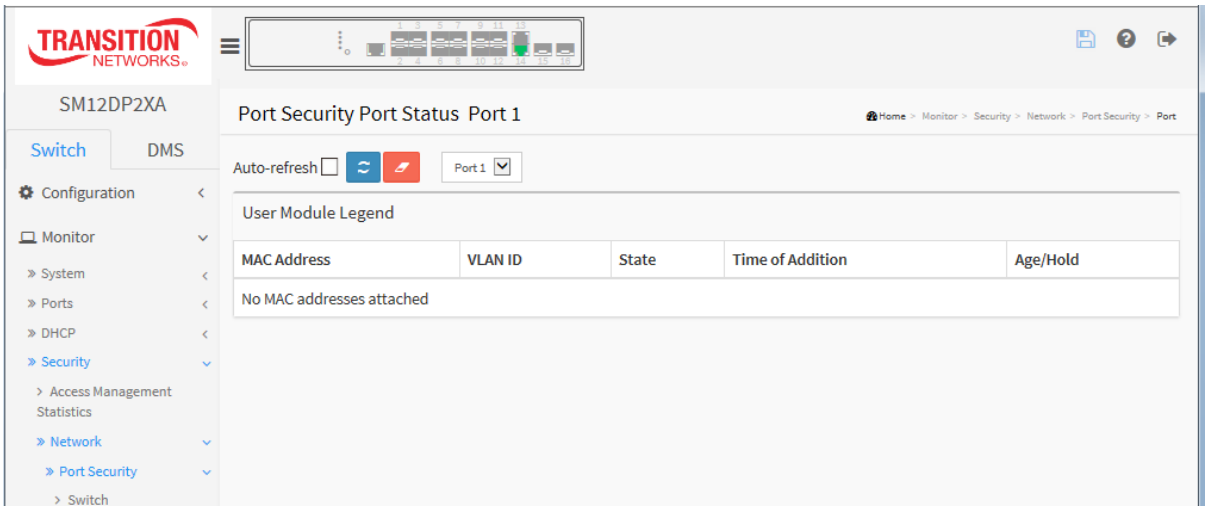
This page displays the MAC addresses secured by the Port Security module. Port Security is a module with no direct configuration. Configuration comes indirectly from other modules (the user modules). When a user module has enabled port security on a port, the port is set up for software-based learning. In this mode, frames from unknown MAC addresses are passed on to the port security module, which in turn asks all user modules whether to allow this new MAC address to forward or block it. For a MAC address to be set in the forwarding state, all enabled user modules must unanimously agree on allowing the MAC address to forward. If only one user module chooses to block it, it will be blocked until that user module decides otherwise.

Web Interface

To configure a Port Security Switch Status Configuration in the web interface:

1. Click Monitor, Security, Network, Port Security, Port.
2. Specify the Port which you want to monitor.
3. Check the Auto-refresh checkbox.
4. Click Refresh to refresh the port detailed statistics.

Figure 3-5.2.1.2: Port Security Port Status



Parameter descriptions:

MAC Address and **VLAN ID :** The MAC address and VLAN ID that is seen on this port. If no MAC addresses are learned, a single row stating "*No MAC addresses attached*" displays.

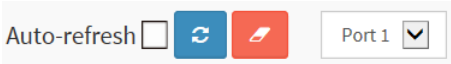
State : Indicates whether the corresponding MAC address is blocked (B) or forwarding (F). In the blocked state, it will not be allowed to transmit or receive traffic.

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



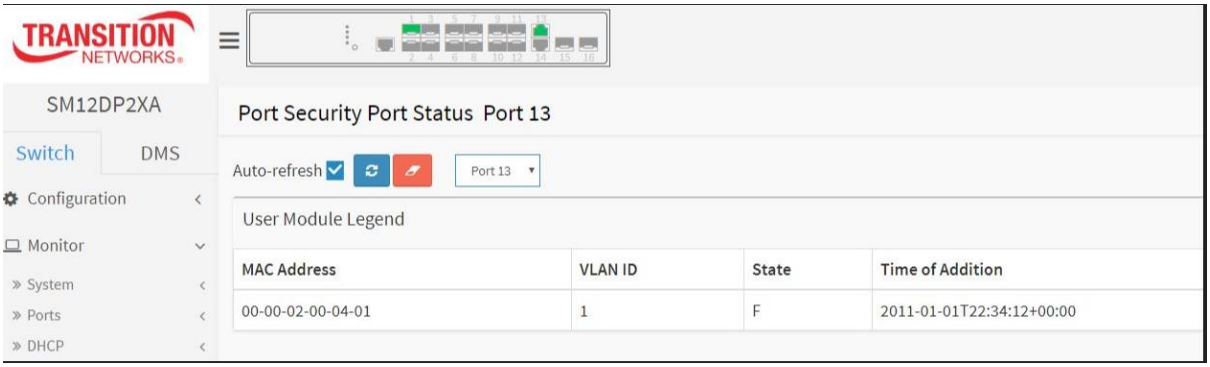
Auto-refresh: Check this box to refresh the page automatically every 3 seconds.

Refresh: Click to refresh the page.

Clear: Clears the page data for the selected port.

: The port select box determines which port is affected by clicking the buttons.

Figure 3-5.2.1.2: Port Security Port Status



3-5.2.2 NAS

3-5.2.2.1 Switch

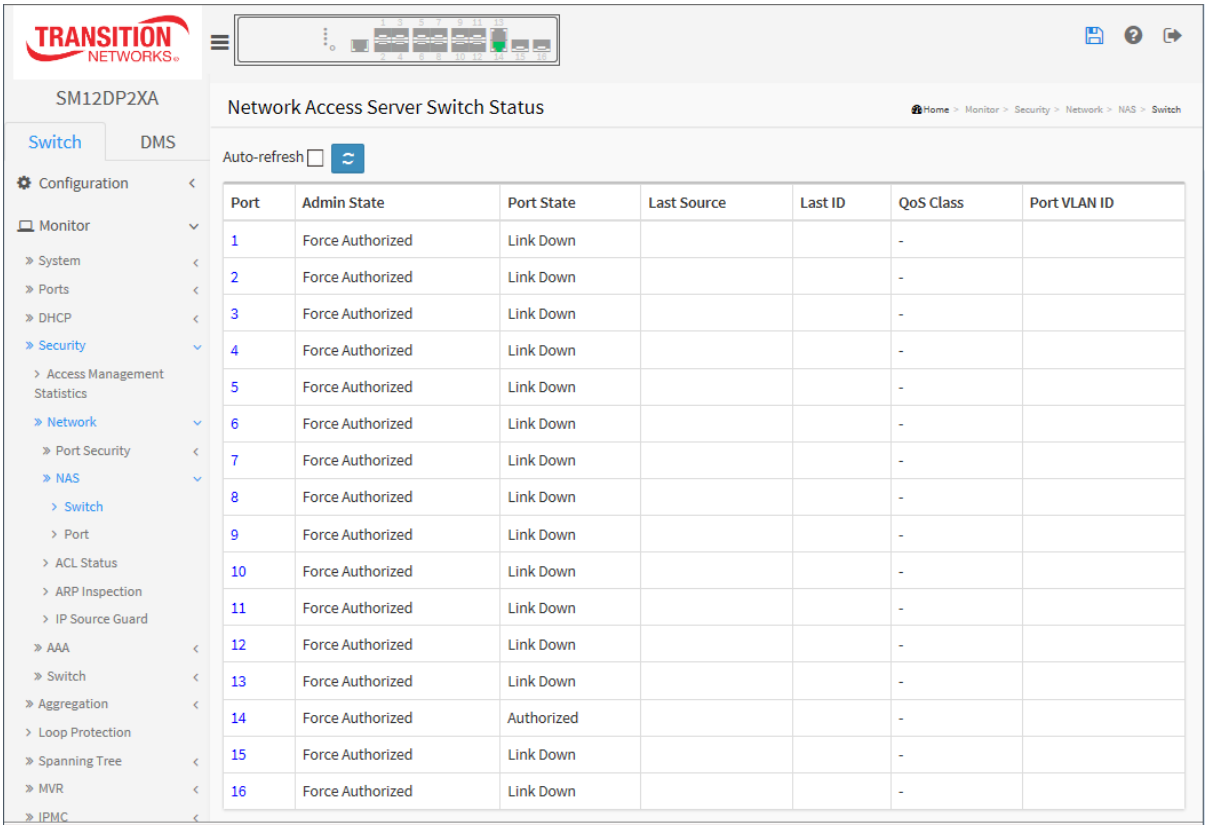
The page displays the switch NAS status information for each port. The status includes Admin State Port State, Last Source, Last ID, QoS Class, and Port VLAN ID.

Web Interface

To configure a NAS Switch Status Configuration in the web interface:

1. Click Monitor, Security, Network, NAS, Switch.
2. Check the Auto-refresh checkbox.
3. Click Refresh to refresh the NAS switch status.

Figure 3-5.2.2.1: Network Access Server Switch Status



Port	Admin State	Port State	Last Source	Last ID	QoS Class	Port VLAN ID
1	Force Authorized	Link Down			-	
2	Force Authorized	Link Down			-	
3	Force Authorized	Link Down			-	
4	Force Authorized	Link Down			-	
5	Force Authorized	Link Down			-	
6	Force Authorized	Link Down			-	
7	Force Authorized	Link Down			-	
8	Force Authorized	Link Down			-	
9	Force Authorized	Link Down			-	
10	Force Authorized	Link Down			-	
11	Force Authorized	Link Down			-	
12	Force Authorized	Link Down			-	
13	Force Authorized	Link Down			-	
14	Force Authorized	Authorized			-	
15	Force Authorized	Link Down			-	
16	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. Refer to NAS Admin State for a description of possible values.

Port State : The current state of the port (ink Down, Authorized, Globally Disabled). Refer to NAS Port State for a description of the individual states.

Last Source : The source MAC address carried in the most recently received EAPOL frame for EAPOL-based authentication, and the most recently received frame from a new client for MAC-based authentication.

Last ID : The user name (supplicant identity) carried in the most recently received Response Identity EAPOL frame for EAPOL-based authentication, and the source MAC address from the most recently

received frame from a new client for MAC-based authentication.

QoS Class : QoS Class assigned to the port by the RADIUS server if enabled.

Port VLAN ID : The VLAN ID that NAS has put the port in. The field is blank if the Port VLAN ID is not overridden by NAS.

If the VLAN ID is assigned by the RADIUS server, "(RADIUS-assigned)" is appended to the VLAN ID.

If the port is moved to the Guest VLAN, "(Guest)" is appended to the VLAN ID.

Buttons

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

Refresh: Click to refresh the page.

3-5.2.2.2 Port

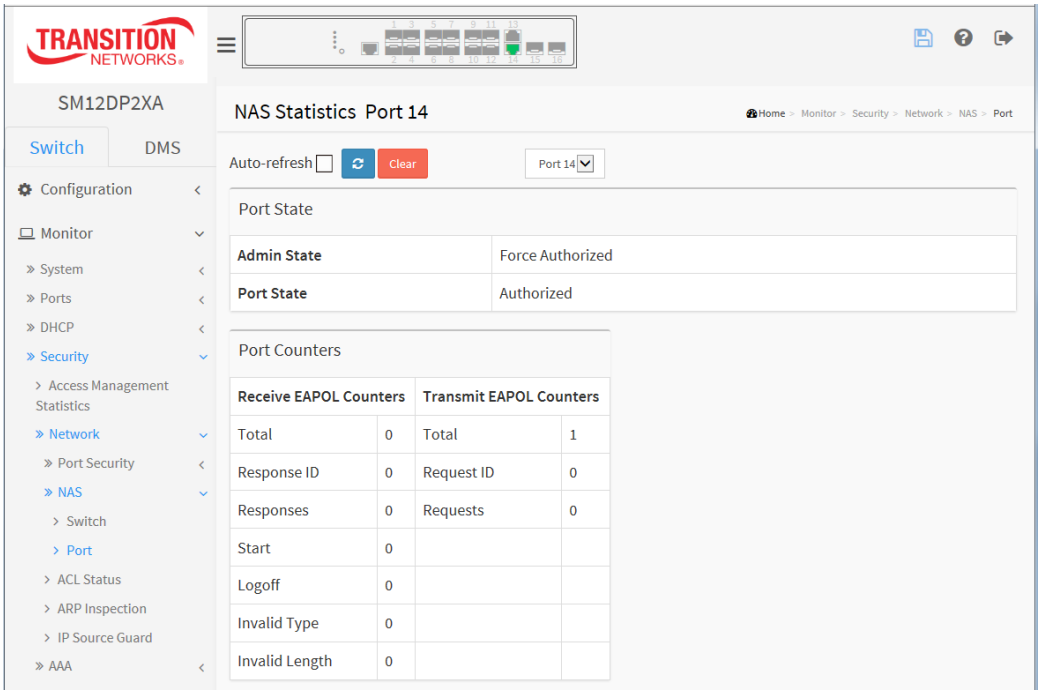
This page displays the detailed NAS statistics for a specific switch port running EAPOL-based IEEE 802.1X authentication. For MAC-based ports, this page shows selected backend server (RADIUS Authentication Server) statistics only.

Web Interface

To configure a NAS Port Status Configuration in the web interface:

1. Click Monitor, Security, Network, NAS, Port.
2. Select a Port number from the dropdown (e.g., Port 14 shown below).
3. View the Port Counters data.
4. Check the Auto-refresh checkbox to automatically refresh the page every 3 seconds.
5. Click Refresh to immediately refresh the statistics.

Figure 3-5.2.2.2: NAS Statistics



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.
If the port is moved to the Guest VLAN, "(Guest)" is appended to the VLAN ID.

Port Counters

EAPOL Counters : These supplicant frame counters are available for the following administrative states:

- Force Authorized
- Force Unauthorized
- Port-based 802.1X
- Single 802.1X
- Multi 802.1X

Direction	Name	IEEE Name	Description
Rx	Total	dot1xAuthEapolFramesRx	The number of valid EAPOL frames of any type that have been received by the switch.
Rx	Response ID	dot1xAuthEapolRespIdFramesRx	The number of valid EAPOL Response Identity frames that have been received by the switch.
Rx	Responses	dot1xAuthEapolRespFramesRx	The number of valid EAPOL response frames (other than Response Identity frames) that have been received by the switch.
Rx	Start	dot1xAuthEapolStartFramesRx	The number of EAPOL Start frames that have been received by the switch.
Rx	Logoff	dot1xAuthEapolLogoffFramesRx	The number of valid EAPOL Logoff frames that have been received by the switch.
Rx	Invalid Type	dot1xAuthInvalidEapolFramesRx	The number of EAPOL frames that have been received by the switch in which the frame type is not recognized.
Rx	Invalid Length	dot1xAuthEapLengthErrorFramesRx	The number of EAPOL frames that have been received by the switch in which the Packet Body Length field is invalid.
Tx	Total	dot1xAuthEapolFramesTx	The number of EAPOL frames of any type that have been transmitted by the switch.
Tx	Request ID	dot1xAuthEapolReqIdFramesTx	The number of EAPOL Request Identity frames that have been transmitted by the switch.
Tx	Requests	dot1xAuthEapolReqFramesTx	The number of valid EAPOL Request frames (other than Request Identity frames) that have been transmitted by the switch.

Backend Server Counters : These backend (RADIUS) frame counters are available for these administrative states:

- Port-based 802.1X
- Single 802.1X
- Multi 802.1X
- MAC-based Auth.

Direction	Name	IEEE Name	Description
Rx	Access Challenges	dot1xAuthBackendAccess Challenges	**802.1X-based**: Counts the number of times that the switch receives the first request from the backend server following the first response from the supplicant. Indicates that the backend server has communication with the switch. **MAC-based**: Counts all Access Challenges received from the backend server for this port (left-most table) or client (right-most table).
Rx	Other Requests	dot1xAuthBackendOther RequestsToSupplicant	**802.1X-based**: Counts the number of times that the switch sends an EAP Request packet following the first to the supplicant. Indicates that the backend server chose an EAP-method. **MAC-based**: Not applicable.
Rx	Auth. Successes	dot1xAuthBackendAuth Successes	**802.1X- and MAC-based**: Counts the number of times that the switch receives a success indication. Indicates that the supplicant/client has successfully authenticated to the backend server.
Rx	Auth. Failures	dot1xAuthBackendAuthFails	**802.1X- and MAC-based**: Counts the number of times that the switch receives a failure message. This indicates that the supplicant/client has not authenticated to the backend server.
Tx	Responses	dot1xAuthBackendResponses	**802.1X-based:** Counts the number of times that the switch attempts to send a supplicant's first response packet to the backend server. Indicates the switch attempted communication with the backend server. Possible retransmissions are not counted. **MAC-based:** Counts all the backend server packets sent from the switch towards the backend server for a given port (left-most table) or client (right-most table). Possible retransmissions are not counted.

Last Supplicant/Client Info : Information about the last supplicant/client that attempted to authenticate. This information is available for the following administrative states:

- Port-based 802.1X
- Single 802.1X
- Multi 802.1X
- MAC-based Auth.

Name	IEEE Name	Description
MAC Address	dot1xAuthLastEapolFrameSource	The MAC address of the last supplicant/client.
VLAN ID	-	The VLAN ID on which the last frame from the last supplicant/client was received.
Version	dot1xAuthLastEapolFrameVersion	**802.1X-based**: The protocol version number carried in the most recently received EAPOL frame. **MAC-based**: Not applicable.
Identity	-	**802.1X-based**: The user name (supplicant identity) carried in the most recently received Response Identity EAPOL frame. **MAC-based**: Not applicable.

Selected Counters : The Selected Counters table is visible when the port is in one of the following 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 above.

Attached MAC Addresses

Identity : Shows the identity of the supplicant, as received in the Response Identity EAPOL frame. Clicking the link causes the supplicant's EAPOL and Backend Server counters to be shown in the Selected Counters table. If no supplicants are attached, it shows No supplicants attached.

This column is not available for MAC-based Auth.

MAC Address : For Multi 802.1X, this column holds the MAC address of the attached supplicant. For MAC-based Auth., this column holds the MAC address of the attached client.

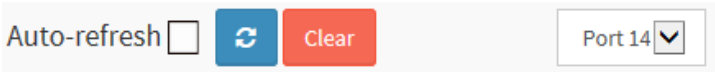
Clicking the link causes the client's Backend Server counters to be shown in the Selected Counters table. If no clients are attached, it shows No clients attached.

VLAN ID : This column holds the VLAN ID that the corresponding client is currently secured through the Port Security module.

State : The client can either be authenticated or unauthenticated. In the authenticated state, it is allowed to forward frames on the port, and in the unauthenticated state, it is blocked. As long as the backend server hasn't successfully authenticated the client, it is unauthenticated. If an authentication fails for one or the other reason, the client will remain in the unauthenticated state for Hold Time seconds.

Last Authentication : Shows the date and time of the last authentication of the client (successful as well as unsuccessful).

Buttons



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

Refresh: Click to refresh the page.

Clear: This button is available in these modes:

- Force Authorized
- Force Unauthorized
- Port-based 802.1X
- Single 802.1X

Clear All: Click to clear the counters for the selected port.

This button is available in these modes:

- Multi 802.1X
- MAC-based Auth.X

Clear This: Click to clear both the port counters and all of the attached client's counters. The "Last Client" will not be cleared, however.

This button is available in these modes:

- Multi 802.1X
- MAC-based Auth.X

Click to clear only the currently selected client's counters.

3-5.2.3 ACL Status

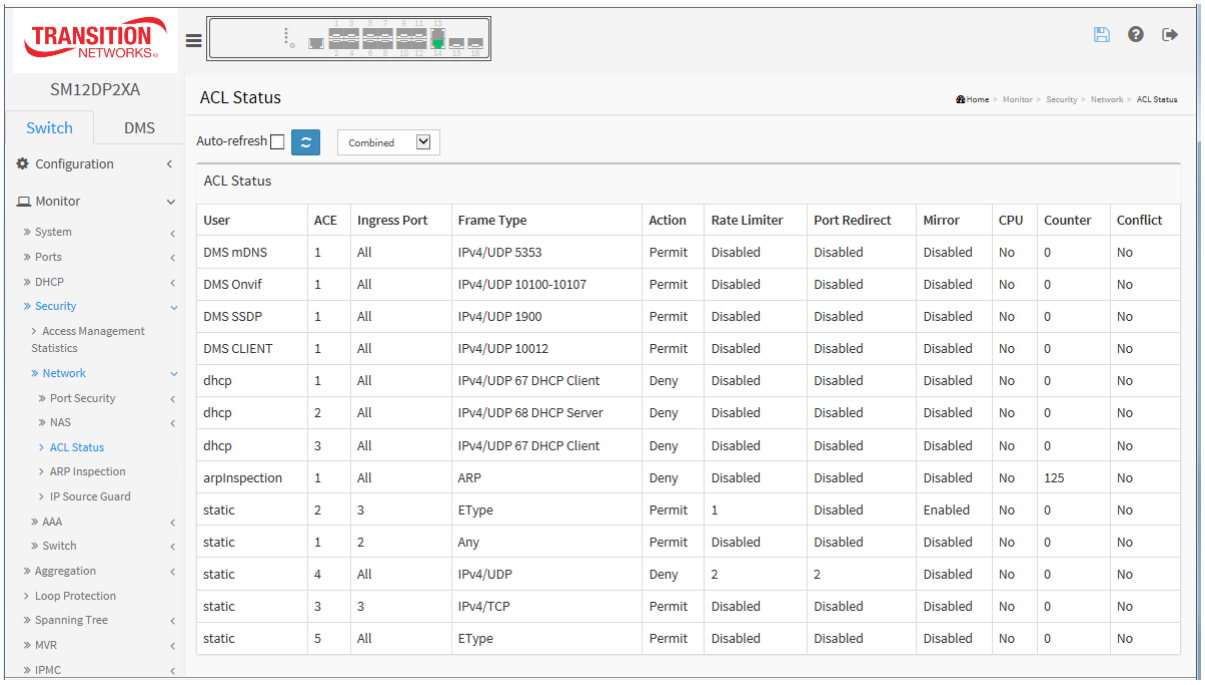
This page shows the ACL status by different ACL users. Each row describes the ACE that is defined. It is a conflict if a specific ACE is not applied to the hardware due to hardware limitations. The maximum number of ACEs is 512 on each switch.

Web Interface

To display the ACL status in the web interface:

1. Click Monitor > Security > Network > ACL Status.
2. To automatically refresh the information, check the Auto-refresh checkbox.
3. Click Refresh to immediately refresh the ACL Status.

Figure 3-5.2.3: ACL Status



User	ACE	Ingress Port	Frame Type	Action	Rate Limiter	Port Redirect	Mirror	CPU	Counter	Conflict
DMS mDNS	1	All	IPv4/UDP 5353	Permit	Disabled	Disabled	Disabled	No	0	No
DMS Onvif	1	All	IPv4/UDP 10100-10107	Permit	Disabled	Disabled	Disabled	No	0	No
DMS SSDP	1	All	IPv4/UDP 1900	Permit	Disabled	Disabled	Disabled	No	0	No
DMS CLIENT	1	All	IPv4/UDP 10012	Permit	Disabled	Disabled	Disabled	No	0	No
dhcp	1	All	IPv4/UDP 67 DHCP Client	Deny	Disabled	Disabled	Disabled	No	0	No
dhcp	2	All	IPv4/UDP 68 DHCP Server	Deny	Disabled	Disabled	Disabled	No	0	No
dhcp	3	All	IPv4/UDP 67 DHCP Client	Deny	Disabled	Disabled	Disabled	No	0	No
arpInspection	1	All	ARP	Deny	Disabled	Disabled	Disabled	No	125	No
static	2	3	EType	Permit	1	Disabled	Enabled	No	0	No
static	1	2	Any	Permit	Disabled	Disabled	Disabled	No	0	No
static	4	All	IPv4/UDP	Deny	2	2	Disabled	No	0	No
static	3	3	IPv4/TCP	Permit	Disabled	Disabled	Disabled	No	0	No
static	5	All	EType	Permit	Disabled	Disabled	Disabled	No	0	No

Parameter descriptions:

User : Indicates the ACL user (e.g., static, dhcp, DMS CLIENT, arpInspection, etc.).

ACE: Indicates the ACE ID on the local switch.

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

All: The ACE will match any ingress port.

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

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

Any: The ACE will match any frame type.

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

ARP: The ACE will match ARP/RARP frames.

IPv4: The ACE will match all IPv4 frames.

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

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

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

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

IPv6: The ACE will match all IPv6 standard frames.

Action : Indicates the forwarding action of the ACE.

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

Deny: Frames matching the ACE are dropped.

Filter: Frames matching the ACE are filtered.

Rate Limiter : Indicates the rate limiter number of the ACE. The allowed range is 1 - 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.

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.

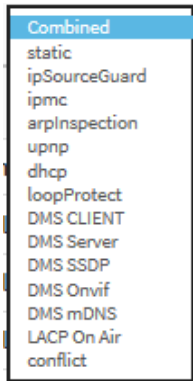
Buttons

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

Refresh: Click to refresh the page.

: User select dropdown to select the user to display.

At the dropdown you can select Combined, static, ipSourceGuard, ipmc, arpInspection, upnp, dhcp, loopProtect, DMS CLIENT, DMS Server, DMS SSDP, DMS Onvif, DMS mDNS, LACP On Air, or conflict.



3-5.2.4 ARP Inspection

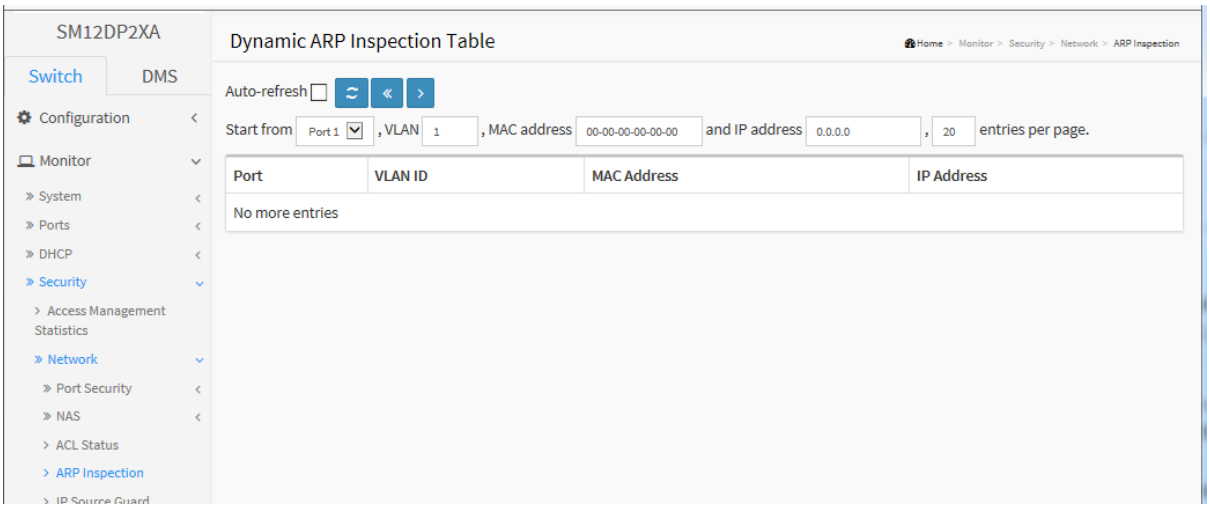
The section describes the Dynamic ARP Inspection Table parameters of the switch. The Dynamic ARP Inspection Table contains up to 1024 entries, and is sorted first by port, then by VLAN ID, then by MAC address, and then by IP address.

Web Interface

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

1. Click Monitor, Security, Network, ARP Inspection.
2. Specify the Start from port, VLAN ID, MAC address, IP Address, and entries per page.
3. Check the Auto-refresh checkbox to refresh the page automatically every 3 seconds.
4. Click Refresh to refresh the page data immediately.

Figure 3-5.2.4: Dynamic ARP Inspection Table



Navigating the ARP Inspection Table

Each page shows up to 99 entries from the Dynamic ARP Inspection table, default being 20, selected through the "entries per page" input field. When first visited, the web page will show the first 20 entries from the beginning of the Dynamic ARP Inspection Table.

The "Start from port address", "VLAN", "MAC address" and "IP address" input fields let you select the starting point in the Dynamic ARP Inspection Table. Clicking the 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 the 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.

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: 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 ARP Inspection Table.

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

3-5.2.5 IP Source Guard

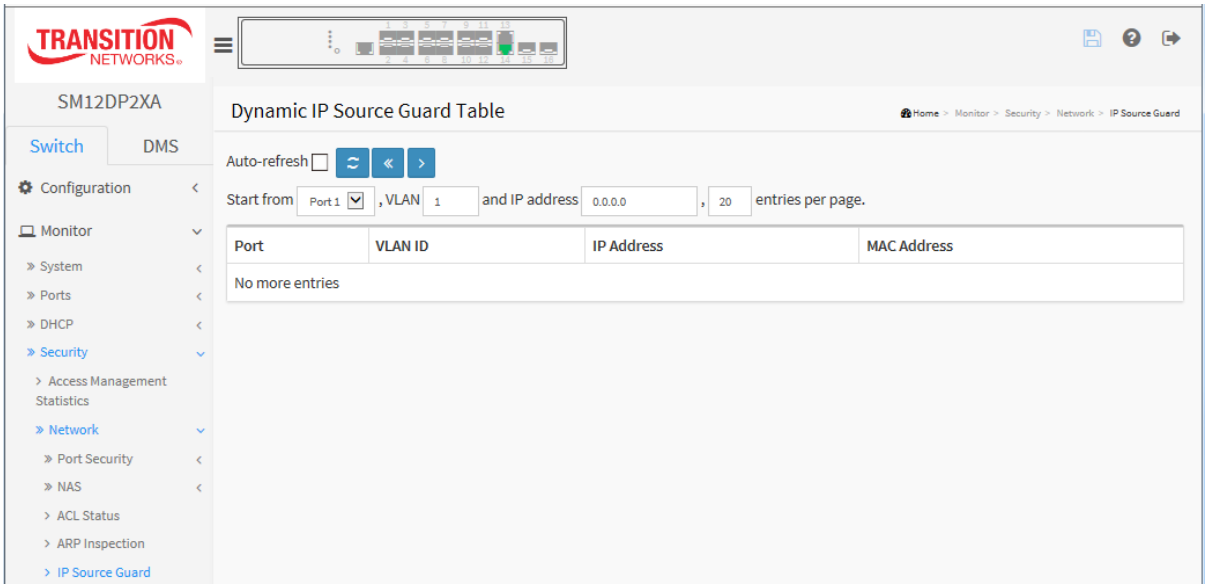
This page displays entries in the Dynamic IP Source Guard Table. The Dynamic IP Source Guard Table is sorted first by port, then by VLAN ID, then by IP address, and then by MAC address.

Web Interface

To view 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. Check the Auto-refresh checkbox.
4. Click Refresh to refresh the port detailed statistics.

Figure 3-5.2.5: Dynamic IP Source Table



Parameter descriptions:

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

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

IP Address : User IP address of the entry.

MAC Address : Source MAC address.

Buttons

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

Refresh: Click to 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

3-5.3.1 RADIUS Overview

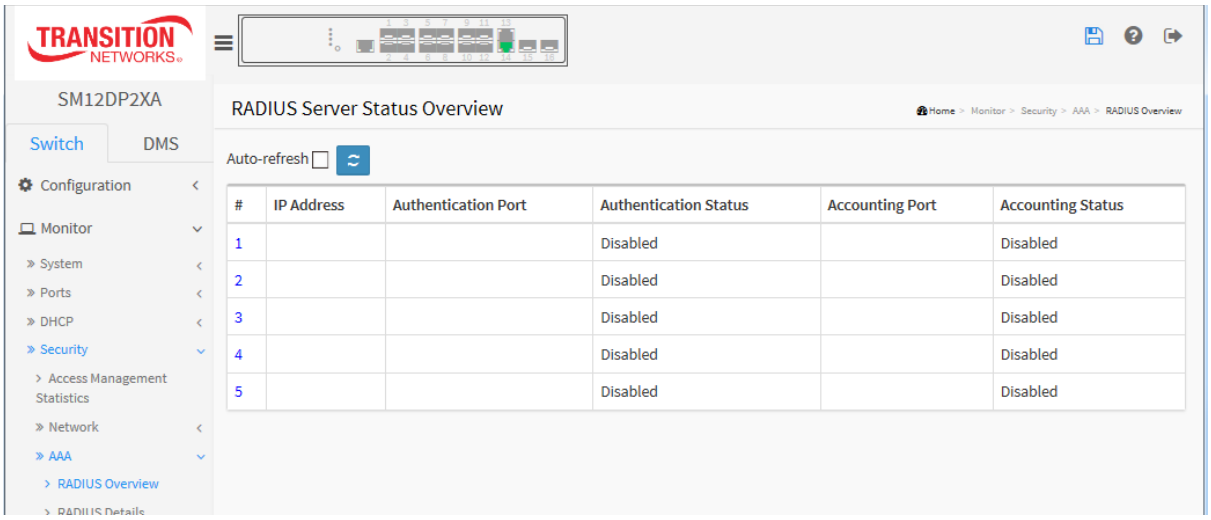
This page displays an overview of the RADIUS Authentication and Accounting status.

Web Interface

To view a RADIUS Overview Configuration in the web interface:

1. Click Monitor, Security, AAA, RADIUS Overview.
2. Check the Auto-refresh checkbox.
3. Click Refresh to refresh the port detailed statistics.

Figure 3-5.3.1: RADIUS Server Status Overview



Parameter descriptions:

 # : The RADIUS server number. Click to navigate to detailed statistics for this server.

IP Address : The IP address and UDP port number (in <IP Address>:<UDP Port> notation) of this server.

Authentication Port: The UDP port number for authentication.

Authentication Status : The current status of the server. This field takes one of the following values:

> ***Disabled***: The 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: The UDP port number for accounting.

Accounting Status: The current status of the server. This field takes one of the following values:

> ***Disabled***: The server is disabled.
>
> ***Not Ready***: The server is enabled, but IP communication is not yet up and running.

Ready: The server is enabled, IP communication is up and running, and the RADIUS module is ready to accept access attempts.

Dead (X seconds left): Access attempts were made to this server, but it did not reply within the configured timeout. The server has temporarily been disabled, but will get re-enabled when the dead-time expires. The number of seconds left before this occurs is displayed in parentheses. This state is only reachable when more than one server is enabled.

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

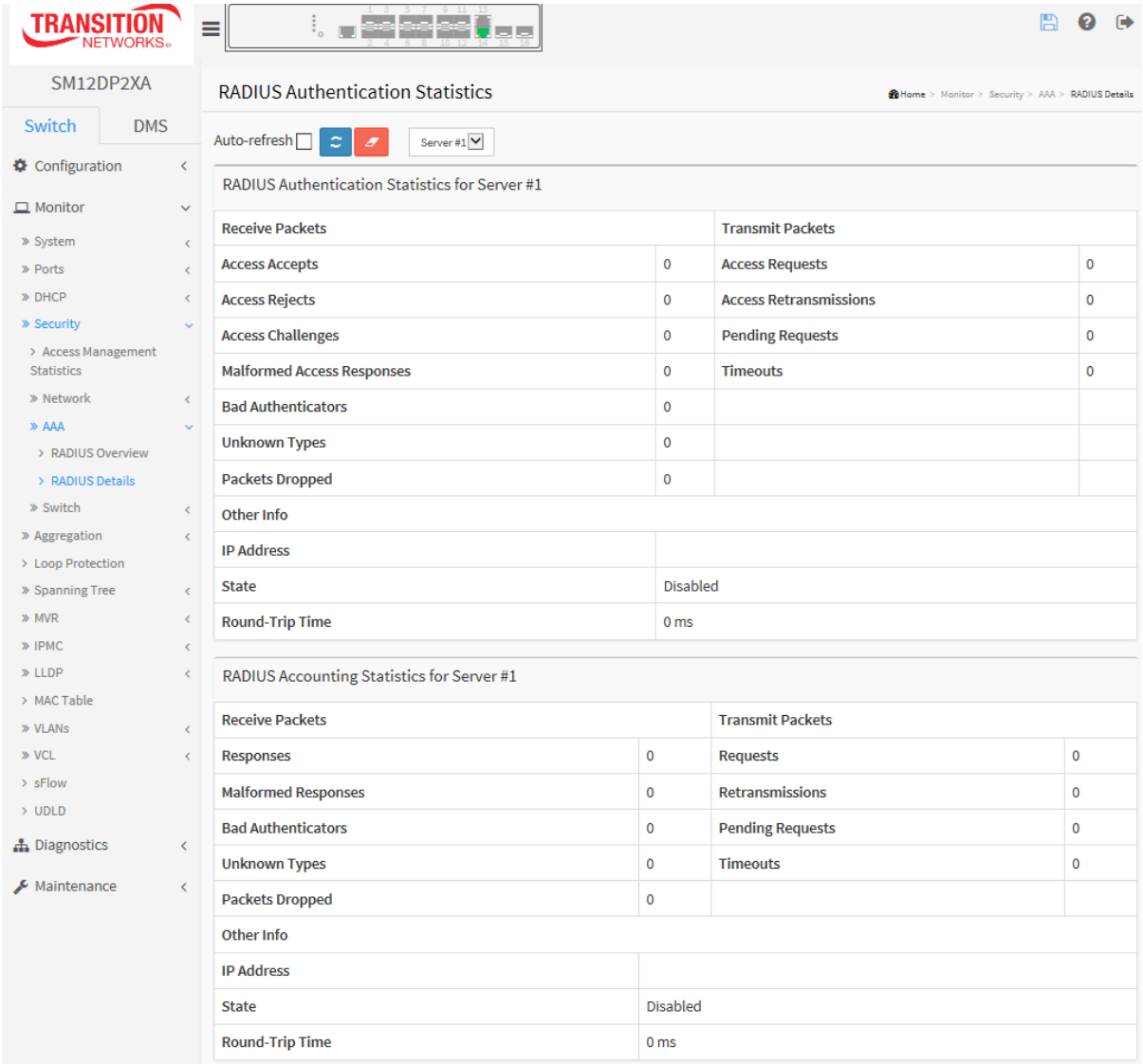
This page displays a detailed statistics for a particular RADIUS server.

Web Interface

To view the RADIUS Details via the web interface:

1. Click Monitor, Security, AAA, RADIUS Details.
2. Specify the Server # which you want to check.
3. View the Authentication and Accounting Statistics for the selected Server.
4. Check the Auto-refresh checkbox to refresh the page automatically every 3 seconds.
5. Click Refresh to refresh the statistics or click Clear to clear all information.

Figure 3-5.3.2: RADIUS Authentication Statistics



Parameter descriptions:

RADIUS Authentication Statistics

The statistics map closely to those specified in IETF RFC4668 - RADIUS Authentication Client MIB.
Use the server select box to switch between the backend servers to show details for.

Packet Counters

RADIUS authentication server packet counter. There are seven receive and four transmit counters.

Direction	Name	RFC4668 Name	Description
Rx	**Access Accepts**	radiusAuthClientExtAccessAccepts	The number of RADIUS Access-Accept packets (valid or invalid) received from the server.
Rx	**Access Rejects**	radiusAuthClientExtAccessRejects	The number of RADIUS Access-Reject packets (valid or invalid) received from the server.
Rx	**Access Challenges**	radiusAuthClientExtAccessChallenges	The number of RADIUS Access-Challenge packets (valid or invalid) received from the server.
Rx	**Malformed Access Responses**	radiusAuthClientExtMalformedAccessResponses	The number of malformed RADIUS Access-Response packets received from the server. Malformed packets include packets with an invalid length. Bad authenticators or Message Authenticator attributes or unknown types are not included as malformed access responses.
Rx	**Bad Authenticators**	radiusAuthClientExtBadAuthenticators	The number of RADIUS Access-Response packets containing invalid authenticators or Message Authenticator attributes received from the server.
Rx	**Unknown Types**	radiusAuthClientExtUnknownTypes	The number of RADIUS packets that were received with unknown types from the server on the authentication port and dropped.
Rx	**Packets Dropped**	radiusAuthClientExtPacketsDropped	The number of RADIUS packets that were received from the server on the authentication port and dropped for some other reason.
Tx	**Access Requests**	radiusAuthClientExtAccessRequests	The number of RADIUS Access-Request packets sent to the server. This does not include retransmissions.
Tx	**Access Retransmissions**	radiusAuthClientExtAccessRetransmissions	The number of RADIUS Access-Request packets retransmitted to the RADIUS authentication server.
Tx	**Pending Requests**	radiusAuthClientExtPendingRequests	The number of RADIUS Access-Request packets destined for the server that have not yet timed out or received a response. This variable is incremented when an Access-Request is sent and decremented due to receipt of an Access-Accept, Access-Reject, Access-Challenge, timeout, or retransmission.
Tx	**Timeouts**	radiusAuthClientExtTimeouts	The number of authentication timeouts to the server. After a timeout, the client may retry to the same server, send to a different server, or give up. A retry to the same server is counted as a retransmit as well as a timeout. A send to a different server is counted as a Request as well as a timeout.

Other Info

This section contains information about the state of the server and the latest round-trip time.

Name	RFC4668 Name	Description
IP Address	-	IP address and UDP port for the authentication server in question.
State	-	Shows the state of the server. It takes one of the following values: Disabled: The selected server is disabled. Not Ready: The server is enabled, but IP communication is not yet up and running. Ready: The server is enabled, IP communication is up and running, and the RADIUS module is ready to accept access attempts. Dead (X seconds left): Access attempts were made to this server, but it did not reply within the configured timeout. The server has temporarily been disabled, but will get re-enabled when the dead-time expires. The number of seconds left before this occurs is displayed in parentheses. This state is only reachable when more than one server is enabled.
Round-Trip Time	radiusAuthClientExtRoundTrip Time	The time interval (measured in milliseconds) between the most recent Access-Reply/Access-Challenge and the Access-Request that matched it from the RADIUS authentication server. The granularity of this measurement is 100 ms. A value of 0 ms indicates that there hasn't been round-trip communication with the server yet.

RADIUS Accounting Statistics

The statistics map closely to those specified in RFC4670 - RADIUS Accounting Client MIB. Use the server select box to switch between the backend servers to show details for.

Packet Counters

RADIUS accounting server packet counter. There are five receive and four transmit counters.

Direction	Name	RFC4670 Name	Description
Rx	**Responses**	radiusAccClientExtResponses	The number of RADIUS packets (valid or invalid) received from the server.
Rx	**Malformed Responses**	radiusAccClientExtMalformedRe sponses	The number of malformed RADIUS packets received from the server. Malformed packets include packets with an invalid length. Bad authenticators or unknown types are not included as malformed access responses.
Rx	**Bad Authenticators**	radiusAcctClientExtBadAuthentic ators	The number of RADIUS packets containing invalid authenticators received from the server.
Rx	**Unknown Types**	radiusAccClientExtUnknownType s	The number of RADIUS packets of unknown types that were received from the server on the accounting port.
Rx	**Packets Dropped**	radiusAccClientExtPacketsDropp ed	The number of RADIUS packets that were received from the server on the accounting port and dropped for some other reason.
Tx	**Requests**	radiusAccClientExtRequests	The number of RADIUS packets sent to the server. This does not include retransmissions.
Tx	**Retransmissions**	radiusAccClientExtRetransmissio ns	The number of RADIUS packets retransmitted to the RADIUS accounting server.
Tx	**Pending Requests**	radiusAccClientExtPendingRequ ests	The number of RADIUS packets destined for the server that have not yet timed out or received a response. This variable is

			incremented when a Request is sent and decremented due to receipt of a Response, timeout, or retransmission.
Tx	**Timeouts**	radiusAccClientExtTimeouts	The number of accounting timeouts to the server. After a timeout, the client may retry to the same server, send to a different server, or give up. A retry to the same server is counted as a retransmit as well as a timeout. A send to a different server is counted as a Request as well as a timeout.

Other Info

This section contains information about the state of the server and the latest round-trip time.

Name	RFC4670 Name	Description
IP Address	-	IP address and UDP port for the accounting server in question.
State	-	Shows the state of the server. It takes one of the following values: Disabled: The selected server is disabled. Not Ready: The server is enabled, but IP communication is not yet up and running. Ready: The server is enabled, IP communication is up and running, and the RADIUS module is ready to accept accounting attempts. Dead (X seconds left): Accounting attempts were made to this server, but it did not reply within the configured timeout. The server has temporarily been disabled, but will get re-enabled when the dead-time expires. The number of seconds left before this occurs is displayed in parentheses. This state is only reachable when more than one server is enabled.
Round-Trip Time	radiusAccClientExtRoundTripTime	The time interval (measured in milliseconds) between the most recent Response and the Request that matched it from the RADIUS accounting server. The granularity of this measurement is 100 ms. A value of 0 ms indicates that there hasn't been round-trip communication with the server yet.

Buttons:

Auto-refresh : Check this box to enable an automatic refresh of the page at regular intervals.

Refresh : Click to refresh the page immediately.

Clear : Clears the counters for the selected server. The "Pending Requests" counter will not be cleared by this operation.

3-5.4 Switch

3-5.4.1 RMON

3-5.4.1.1 Statistics

This page provides an overview of RMON Statistics entries. Each page shows up to 99 entries from the Statistics table, default being 20, selected through the "entries per page" input field. When first visited, the web page will show the first 20 entries from the beginning of the Statistics table. The first displayed will be the one with the lowest ID found in the Statistics table.

The "Start from Control Index" lets you select the starting point in the Statistics table. Clicking the **Refresh** button will update the displayed table starting from that or the next closest Statistics table match.

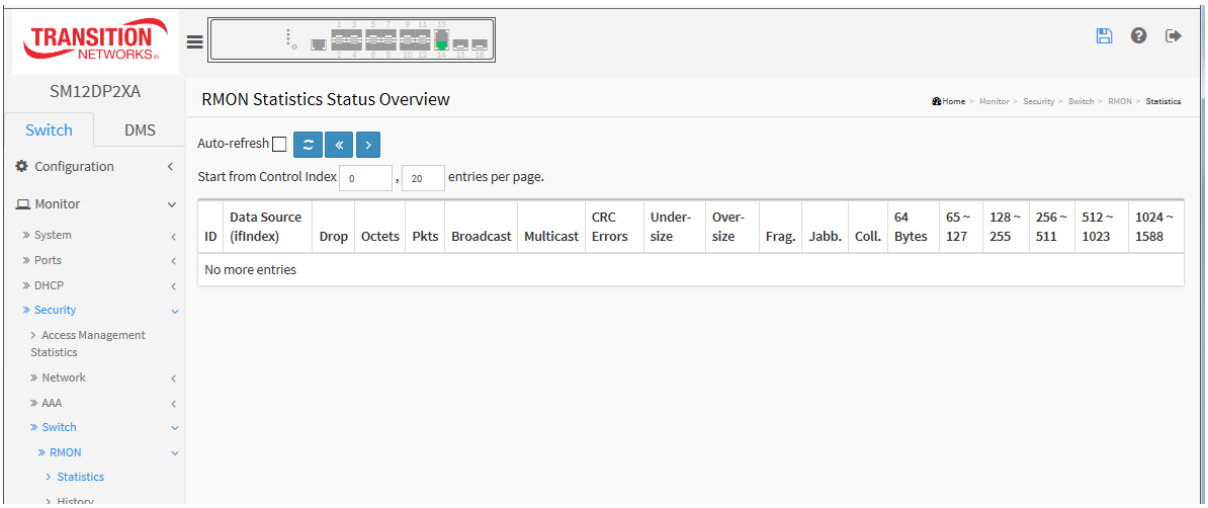
The **>** button will use the last entry of the currently displayed entry as the basis for the next lookup. When the end is reached the text "*No more entries*" is shown in the displayed table. Use the **<<** button to start over.

Web Interface

To configure a RMON Statistics in the web interface:

1. Click Monitor, Security, Switch, RMON, Statistics.
2. Specify the “Start from Control Index”.
3. Check the Auto-refresh checkbox.
4. Click Refresh to manually refresh the port detailed statistics.

Figure 3-5.4.1.1: RMON Statistics Status Overview



Parameter descriptions:

ID : Indicates the index of Statistics entry.

Data Source(ifIndex) : The port ID which wants to be monitored.

Drop : The total number of events in which packets were dropped by the probe due to lack of resources.

Octets : The total number of octets of data (including those in bad packets) received on the network.

Pkts : The total number of packets (including bad packets, broadcast packets, and multicast packets) received.

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 in length.

65~127 : The total number of packets (including bad packets) received that were between 65 to 127 octets in length.

128~255 : The total number of packets (including bad packets) received that were between 128 to 255 octets in length.

256~511 : The total number of packets (including bad packets) received that were between 256 to 511 octets in length.

512~1023 : The total number of packets (including bad packets) received that were between 512 to 1023 octets in length.

1024~1588 : The total number of packets (including bad packets) received that were between 1024 to 1588 octets in length.

Buttons

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

Refresh: Click to refresh the page immediately.

<< : Updates the table starting from the first entry in the Statistics table, i.e. the entry with the lowest ID.

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

3-5.4.1.2 History

This page provides an overview of RMON History entries. Each page shows up to 99 entries from the History table, default being 20, selected through the "entries per page" input field. When first visited, the web page will show the first 20 entries from the beginning of the History table. The first displayed will be the one with the lowest History Index and Sample Index found in the History table.
The "Start from History Index and Sample Index" lets you 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.

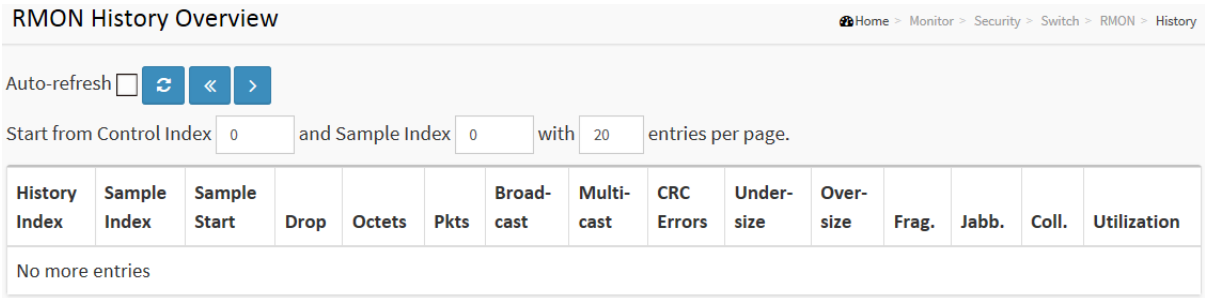
The **>** button will use the last entry of the currently displayed entry as the basis for the next lookup. When the end is reached the text "No more entries" is shown in the displayed table. Use **<<** the button to start over.

Web Interface

To configure a RMON history Configuration in the web interface:

1. Click Monitor, Security, Switch, RMON, History.
2. Specify Port which you want to check.
3. Check the Auto-refresh checkbox.
4. Click Refresh to refresh the statistics or click Clear to clear all information.

Figure 3-5.4.1.2: RMON History Overview



Parameter descriptions:

History Index : The index of History control entry.

Sample Index : 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, i.e., the entry with the lowest History Index and Sample Index

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

3-5.4.1.3 Alarm

This page provides an overview of RMON Alarm entries. Each page shows up to 99 entries from the Alarm table, default being 20, selected through the "entries per page" input field. When first visited, the web page will show the first 20 entries from the beginning of the Alarm table. The first displayed will be the one with the lowest ID found in the Alarm table.

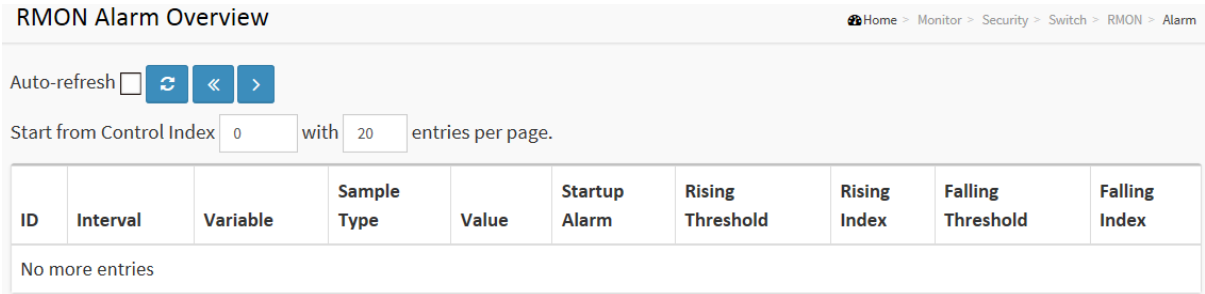
The "Start from Control Index" lets you select the starting point in the Alarm table. Clicking the **Refresh** button will update the displayed table starting from that or the next closest Alarm table match. The > will use the last entry of the currently displayed entry as the basis for the next lookup. When the end is reached the text "*No more entries*" is shown in the displayed table. Use the **<<** button to start over.

Web Interface

To configure a RMON Alarm Overview in the web interface:

1. Click Monitor, Security, Switch, RMON, Alarm.
2. Specify the “Start from Control Index” and “entries per page” .
3. Check the Auto-refresh checkbox.
4. Click Refresh to refresh the port detailed statistics.

Figure 3-5.4.1.3: RMON Alarm Overview



Parameter descriptions:

ID : The index of Alarm control entry.

Interval : 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 displayed will be the one with the lowest Event Index and Log Index found in the Event table .

The "Start from Event Index and Log Index" lets you select the starting point in the Event table. Clicking the Refresh button will update the displayed table starting from that or the next closest Event table match.

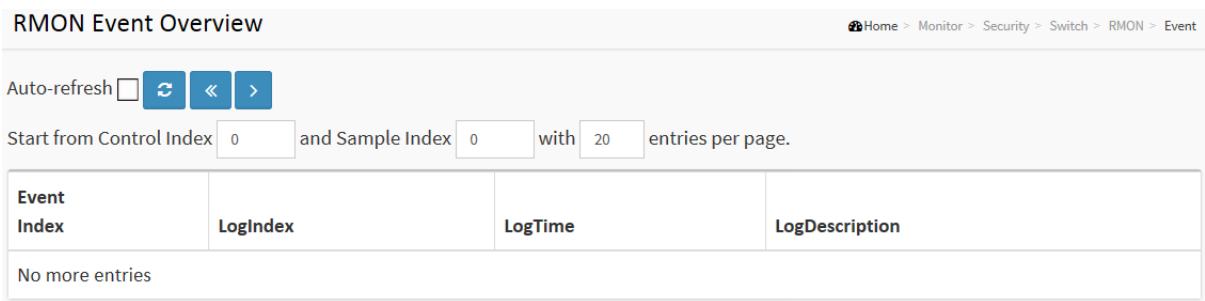
The **>** button will use the last entry of the currently displayed entry as the basis for the next lookup. When the end is reached the text "*No more entries*" is shown in the displayed table. Use the **<<** button to start over.

Web Interface

To configure a RMON Event Overview in the web interface:

1. Click Monitor, Security, Switch, RMON, Event.
2. Specify the Start from Control Index and the Sample Index.
3. Check the Auto-refresh checkbox.
4. Click Refresh to refresh the page data.

Figure 3-5.4.1.4: RMON Event Overview



Parameter descriptions:

Event Index : Indicates the index of the event entry.

LogIndex : 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, i.e. the entry with the lowest Event Index and Log Index.

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

3-6 Aggregation

3-6.1 Status

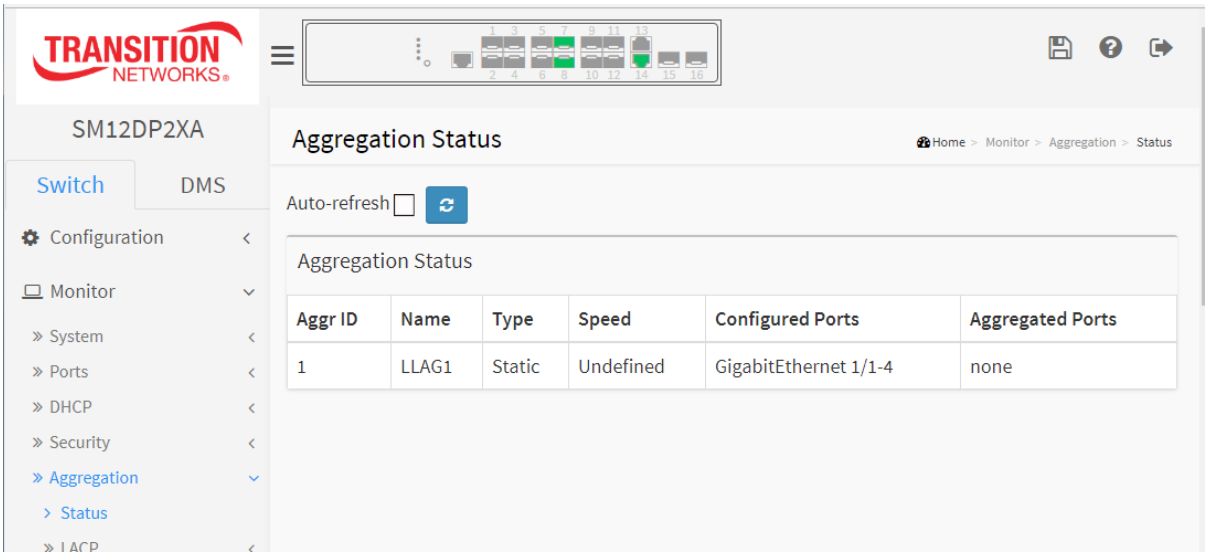
This page displays the status of ports in an Aggregation group.

Web Interface

To display the Aggregation status in the web interface:

1. Click Monitor, Aggregation, Status.
2. Check the Auto-refresh checkbox.
3. Click Refresh to refresh the Aggregation Status details.

Figure 3-6.1 Aggregation Status



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.

3-7 LACP

3-7.1 System Status

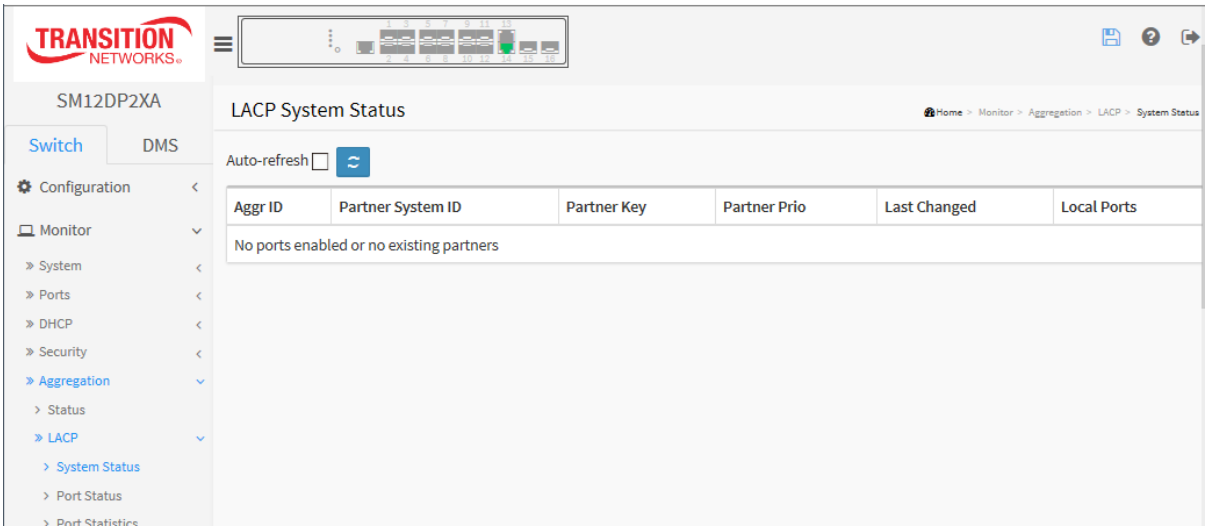
This page provides a status overview for all LACP instances.

Web Interface

To display the LACP System status in the web interface:

1. Click Monitor, Aggregation, LACP, System Status.
2. Check the Auto-refresh checkbox.
3. Click Refresh to refresh the port detailed statistics.

Figure 3-7.1 LACP System Status



Parameter descriptions:

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

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

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

Last Changed : The time since this aggregation changed.

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

Buttons

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

Refresh: Click to refresh the page.

3-7.2 Port Status

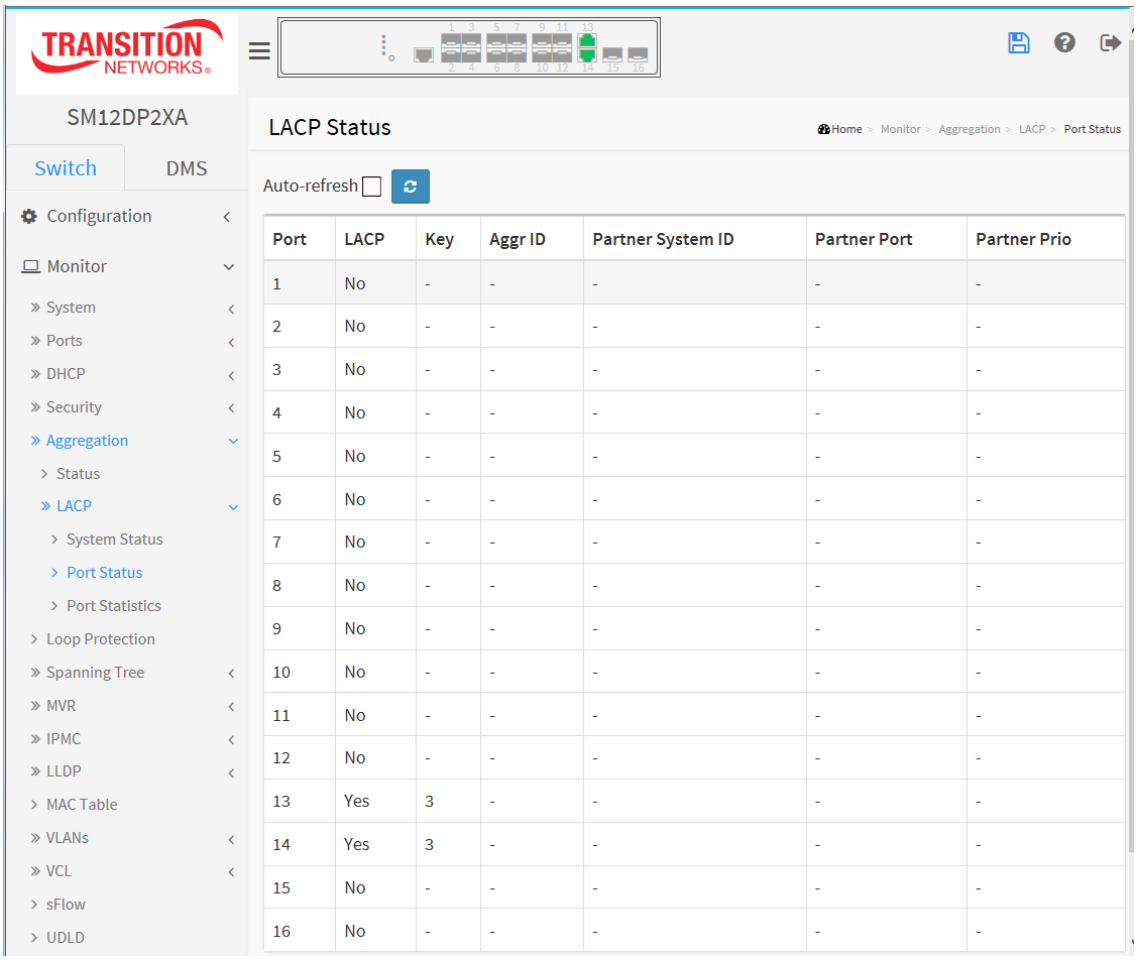
This page provides a status overview for LACP status for all ports.

Web Interface

To display the LACP Port status in the web interface:

1. Click Monitor, Aggregation, LACP, Port Status.
2. Check the Auto-refresh checkbox to automatically refresh the information every 3 seconds.
3. Click Refresh to refresh the LACP Port Status.

Figure 3-7.2: LACP Status



Port	LACP	Key	Aggr ID	Partner System ID	Partner Port	Partner Prio
1	No	-	-	-	-	-
2	No	-	-	-	-	-
3	No	-	-	-	-	-
4	No	-	-	-	-	-
5	No	-	-	-	-	-
6	No	-	-	-	-	-
7	No	-	-	-	-	-
8	No	-	-	-	-	-
9	No	-	-	-	-	-
10	No	-	-	-	-	-
11	No	-	-	-	-	-
12	No	-	-	-	-	-
13	Yes	3	-	-	-	-
14	Yes	3	-	-	-	-
15	No	-	-	-	-	-
16	No	-	-	-	-	-

Parameter descriptions:

Port : The switch port number.

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

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

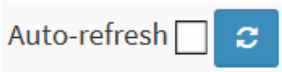
Aggr ID : The Aggregation ID assigned to this aggregation group. IDs 1 and 2 are GLAGs while IDs 3-14 are LLAGs.

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

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

Partner Prio: The partner's port priority.

Buttons



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

Refresh: Click to refresh the page immediately.

3-7.3 Port Statistics

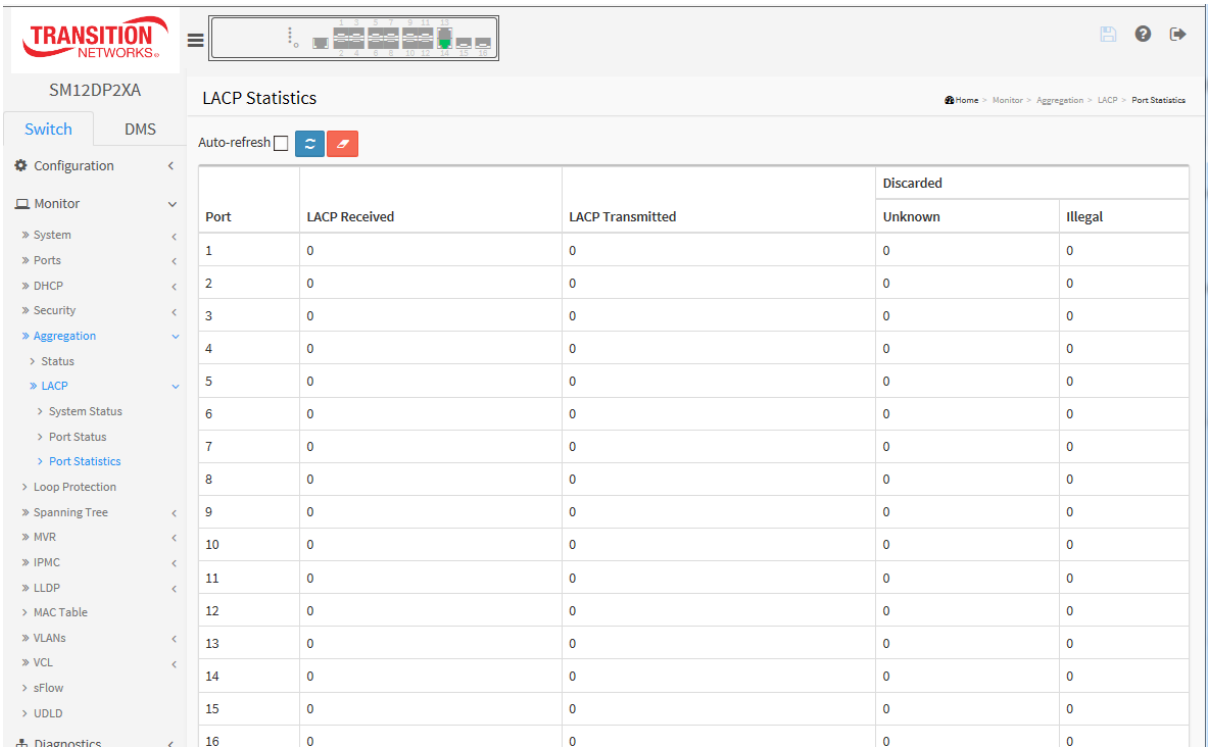
This page provides an overview of LACP statistics for all ports.

Web Interface

To display the LACP Port status in the web interface:

1. Click Monitor, Aggregation, LACP, Port Statistics.
2. To automatically refresh the information check the Auto refresh checkbox.
3. Click Refresh to refresh the LACP Statistics.

Figure 3-7.3: LACP Statistics



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
8	0	0	0	0
9	0	0	0	0
10	0	0	0	0
11	0	0	0	0
12	0	0	0	0
13	0	0	0	0
14	0	0	0	0
15	0	0	0	0
16	0	0	0	0

Parameter descriptions:

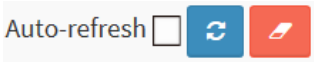
Port : The switch port number.

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.

Clear: Clears the counters for the selected port.

Refresh: Click to refresh the page.

3-8 Loop Protection

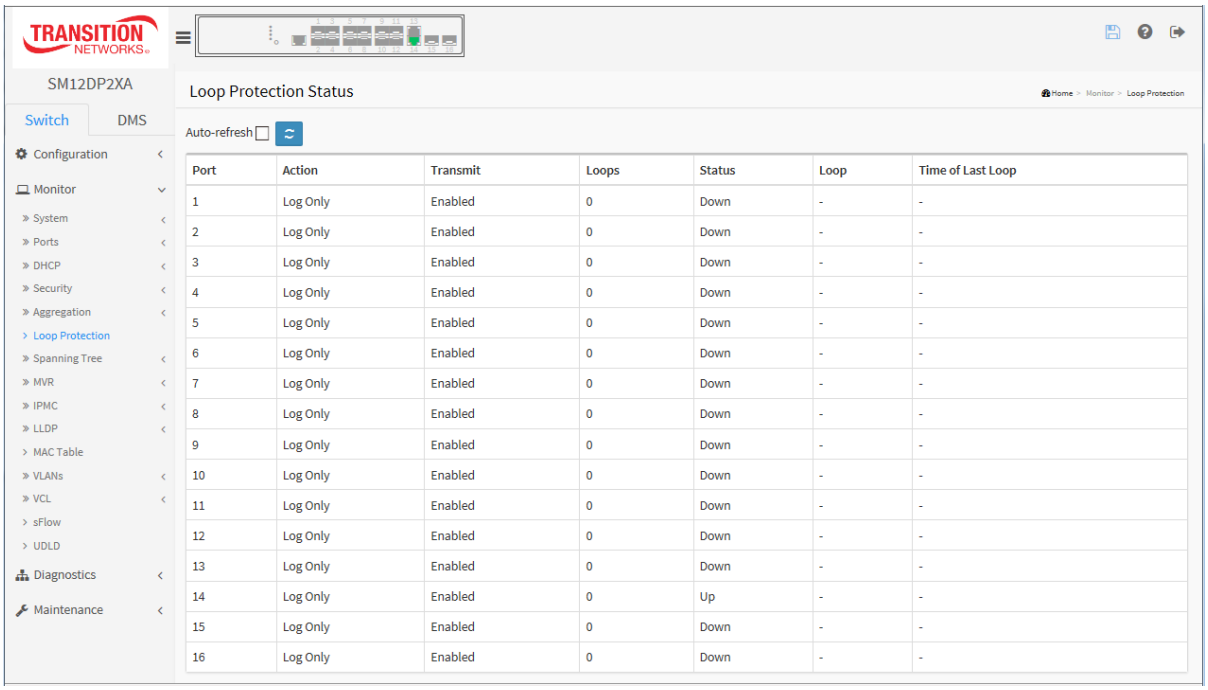
This page displays the loop protection port status the ports of the currently selected switch.

Web Interface

To display the Loop Protection status in the web interface:

1. Click Monitor, Loop Protection.
2. To automatically refresh the information every 3 seconds check the Auto refresh checkbox.
3. Click Refresh to refresh the LACP Statistics.

Figure 3-8: Loop Protection Status



Port	Action	Transmit	Loops	Status	Loop	Time of Last Loop
1	Log Only	Enabled	0	Down	-	-
2	Log Only	Enabled	0	Down	-	-
3	Log Only	Enabled	0	Down	-	-
4	Log Only	Enabled	0	Down	-	-
5	Log Only	Enabled	0	Down	-	-
6	Log Only	Enabled	0	Down	-	-
7	Log Only	Enabled	0	Down	-	-
8	Log Only	Enabled	0	Down	-	-
9	Log Only	Enabled	0	Down	-	-
10	Log Only	Enabled	0	Down	-	-
11	Log Only	Enabled	0	Down	-	-
12	Log Only	Enabled	0	Down	-	-
13	Log Only	Enabled	0	Down	-	-
14	Log Only	Enabled	0	Up	-	-
15	Log Only	Enabled	0	Down	-	-
16	Log Only	Enabled	0	Down	-	-

Parameter descriptions:

Port : The switch port number of the logical port.

Action : The currently configured port action.

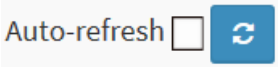
Transmit : The currently configured port transmit mode.

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 enable an automatic refresh of the page every 3 seconds.

Refresh: Click to refresh the page immediately.

3-9 Spanning Tree

3-9.1 Bridge Status

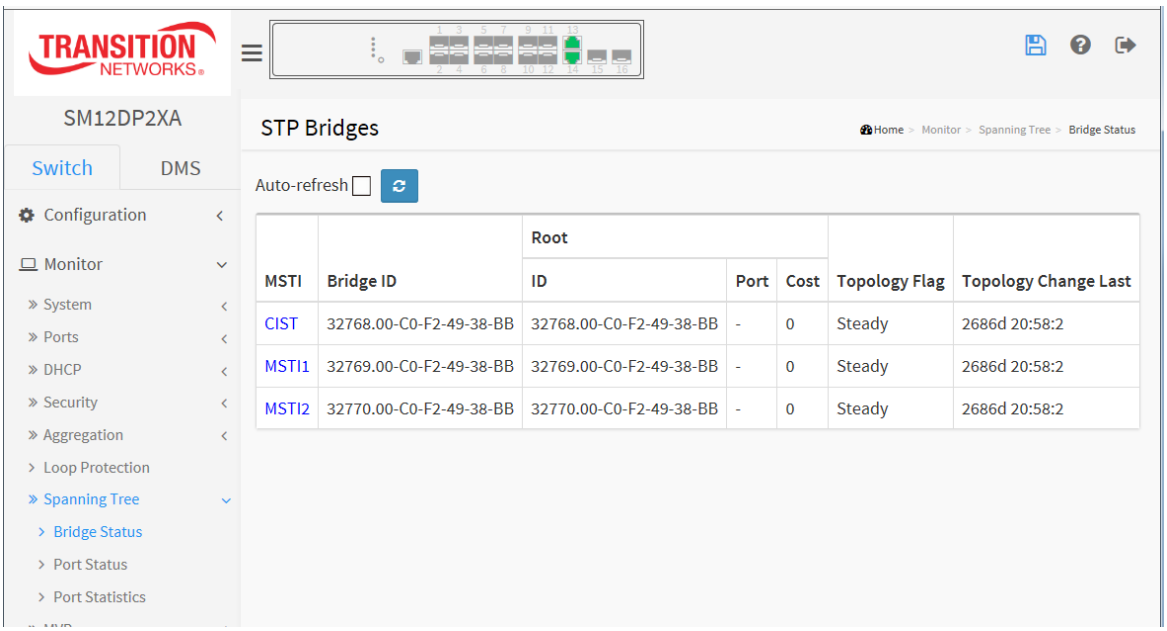
After you complete the MSTI Port configuration then you can have the switch display the Bridge Status. This page provides a status overview of all STP bridge instances. The displayed table contains a row for each STP bridge instance, where the column displays the information below.

Web Interface

To display the STP Bridges status in the web interface:

1. Click Monitor, Spanning Tree, Bridge Status.
2. To automatically refresh the information check the Auto-refresh checkbox.
3. Click Refresh to refresh the STP Bridges table data immediately.
4. Click the linked instance in the MSTI column (e.g., CIST) to go to the "STP Detailed Bridge Status" page.

Figure 3-9.1: STP Bridges Status



Parameter descriptions:

MSTI : The Bridge Instance. This is also a link to the STP Detailed Bridge Status.

Bridge ID : The Bridge ID of this Bridge instance.

Root ID : The Bridge ID of the currently elected root bridge.

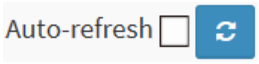
Root Port : The switch port currently assigned the root port role.

Root Cost : Root Path Cost. For the Root Bridge it is zero. For all other Bridges, it is the sum of the Port Path Costs on the least cost path to the Root Bridge.

Topology Flag : The current state of the Topology Change Flag of this Bridge instance.

Topology Change Last : The time since last Topology Change occurred.

Buttons

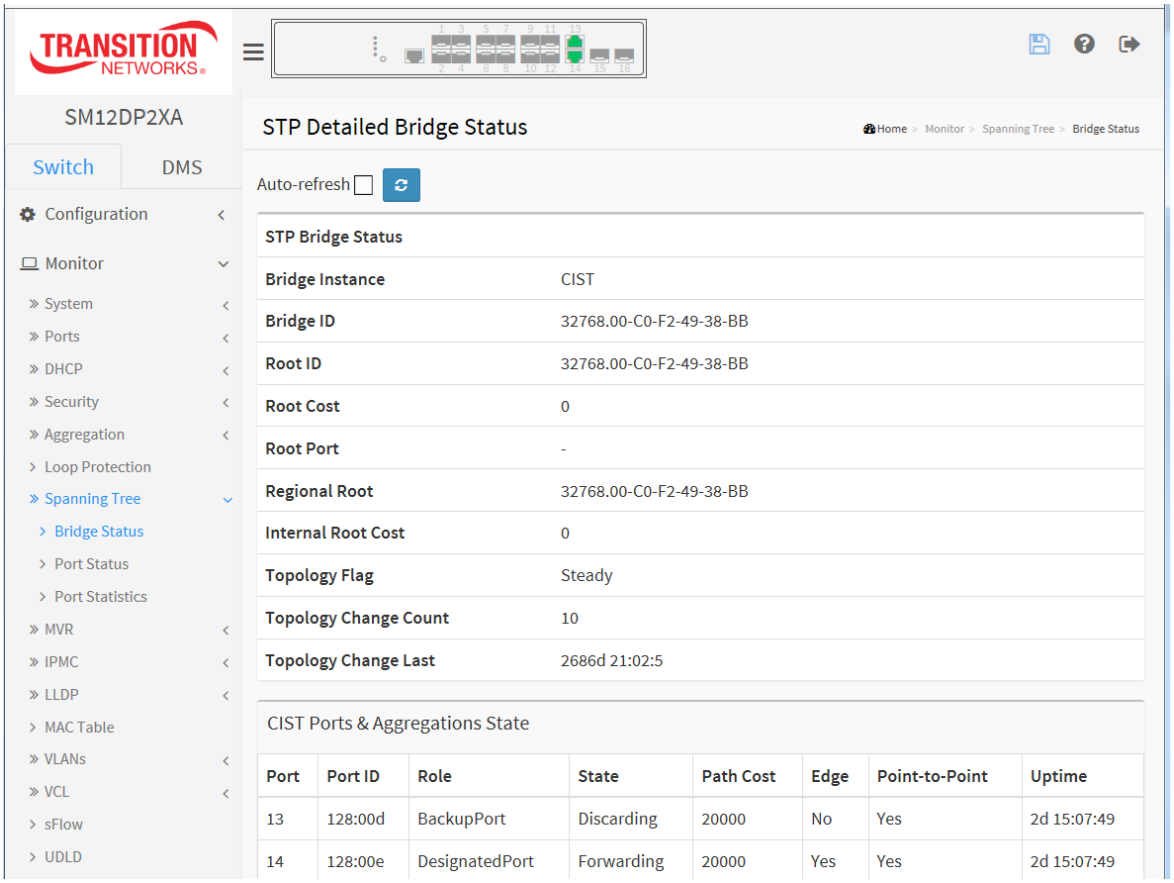


Auto-refresh: Check this box to refresh the page automatically every 3 seconds.

Refresh: Click to refresh the page.

When you click a linked instance in the MSTI column (e.g., CIST) the STP Detailed Bridge Status page displays. This page provides detailed information on a single STP bridge instance, along with port state for all active ports associated.

The page contains two tables with the following information:



Parameter descriptions:

STP Bridge Status

Bridge Instance : The Bridge instance (e.g., *CIST*, *MST1*, etc.).

Bridge ID : The Bridge ID of this Bridge instance (e.g., *32768.00-C0-F2-49-38-BB*).

Root ID : The Bridge ID of the currently elected root bridge.

Root Port : The switch port currently assigned the root port role.

Root Cost : Root Path Cost. For the Root Bridge this is zero. For all other Bridges, it is the sum of the Port Path Costs on the least cost path to the Root Bridge.

Regional Root : The Bridge ID of the currently elected regional root bridge, inside the MSTP region of this bridge. (For the CIST instance only).

Internal Root Cost : The Regional Root Path Cost. For the Regional Root Bridge this is zero. For all other

CIST instances in the same MSTP region, it is the sum of the Internal Port Path Costs on the least cost path to the Internal Root Bridge. (For the CIST instance only).

Topology Flag : The current state of the Topology Change Flag of this Bridge instance (e.g., *Steady*).

Topology Change Count : The number of times that the topology change flag was set (during a one-second interval) (e.g., *10*).

Topology Change Last : The time passed since the Topology Flag was last set (e.g., *2686d 21:12:1*).

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 (e.g., *128:00d*). This is the priority part and the logical port index of the bridge port.

Role : The current STP port role. The port role can be *AlternatePort*, *BackupPort*, *RootPort*, or *DesignatedPort*.

State : The current STP port state. The port state can be *Blocking*, *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 (e.g., *20000*).

Edge : The current STP port (operational) Edge Flag (*Yes* or *No*). An Edge Port is a switch port to which no Bridges are attached. The flag may be automatically computed or explicitly configured. Each Edge Port transits directly to the Forwarding Port State, since there is no possibility of it participating in a loop.

Point-to-Point : The current STP port point-to-point flag (*Yes* or *No*). A point-to-point port connects to a non-shared LAN media. The flag may be automatically computed or explicitly configured.
The point-to-point properties of a port affect how fast it can transit to STP state.

Uptime : The time since the bridge port was last initialized (e.g., *2d 15:17:06*).

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

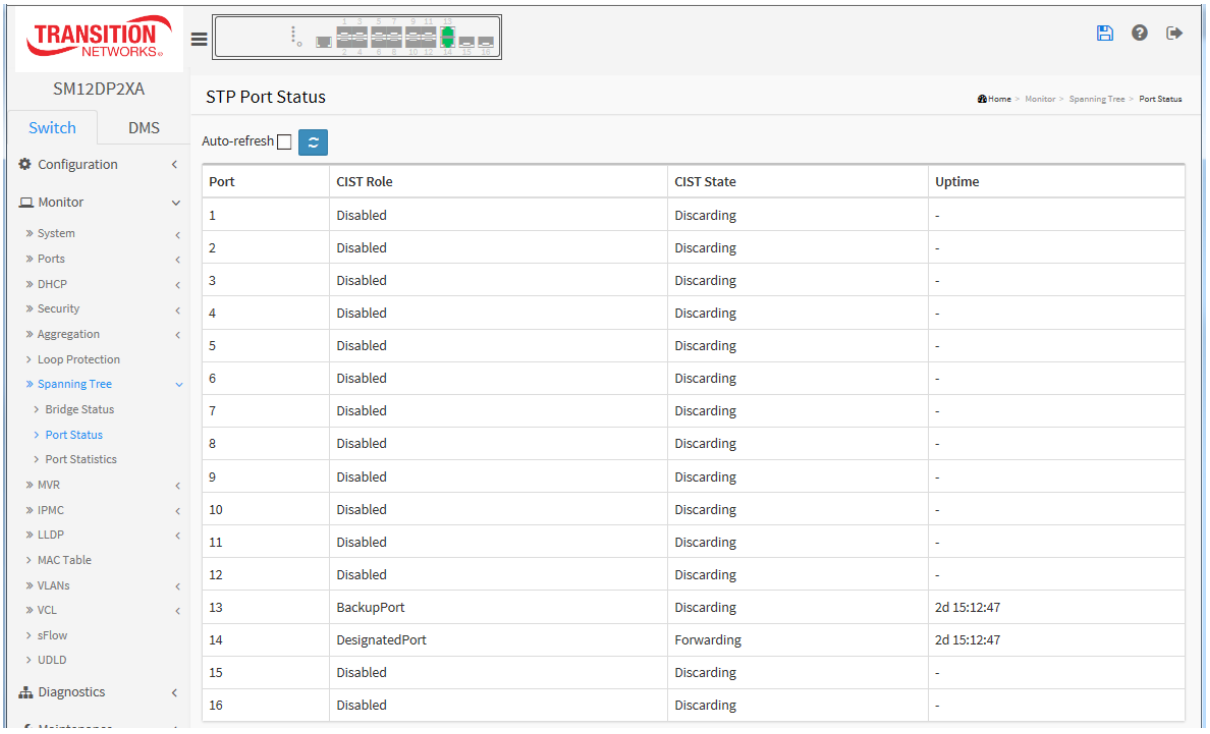
After you complete the STP configuration you can display the STP Port Status. This page describes the STP CIST port status for physical ports of the switch.

Web Interface

To display the STP Port status in the web interface:

1. Click Monitor, Spanning Tree, Port Status.
2. To automatically refresh the information, check the Auto-refresh checkbox.
3. Click Refresh to refresh the STP Bridges.

Figure 3-9.2: STP Port Status



Port	CIST Role	CIST State	Uptime
1	Disabled	Discarding	-
2	Disabled	Discarding	-
3	Disabled	Discarding	-
4	Disabled	Discarding	-
5	Disabled	Discarding	-
6	Disabled	Discarding	-
7	Disabled	Discarding	-
8	Disabled	Discarding	-
9	Disabled	Discarding	-
10	Disabled	Discarding	-
11	Disabled	Discarding	-
12	Disabled	Discarding	-
13	BackupPort	Discarding	2d 15:12:47
14	DesignatedPort	Forwarding	2d 15:12:47
15	Disabled	Discarding	-
16	Disabled	Discarding	-

Parameter descriptions:

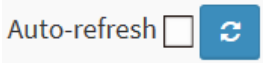
Port : The switch port number of the logical STP port.

CIST Role : The current STP port role of the CIST port. The port role can be *AlternatePort*, *Backup Port*, *RootPort*, *DesignatedPort*, or *Disabled*.

CIST State : The current STP port state of the CIST port. The port state can be *Blocking*, *Learning*, *Discarding*, or *Forwarding*.

Uptime : The time since the bridge port was last initialized (e.g., *5d 21:27:42*).

Buttons



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

Refresh: Click to refresh the page.

3-9.3 Port Statistics

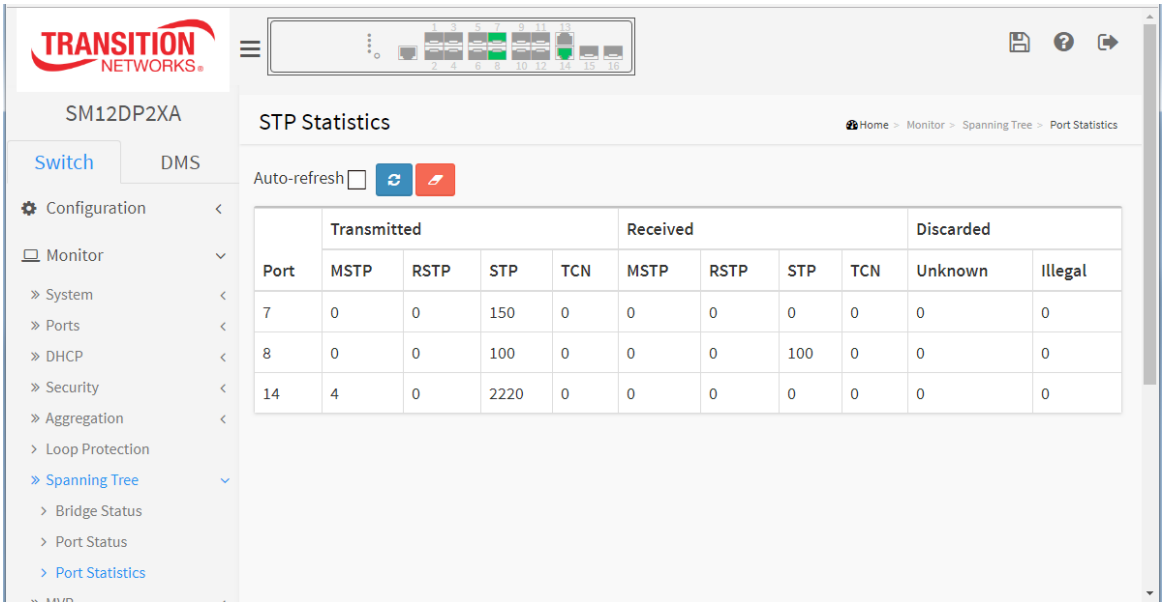
After you complete the STP configuration you can have the switch display the STP Statistics. This page displays the STP Statistics detail counters of bridge ports in the currently selected switch.

Web Interface

To display the STP Port status in the web interface:

1. Click Monitor, Spanning Tree, Port Statistics.
2. To automatically refresh the page, check the Auto-refresh checkbox.
3. Click Refresh to refresh the STP Bridges.

Figure 3-9.3: STP Statistics



	Transmitted				Received				Discarded	
Port	MSTP	RSTP	STP	TCN	MSTP	RSTP	STP	TCN	Unknown	Illegal
7	0	0	150	0	0	0	0	0	0	0
8	0	0	100	0	0	0	100	0	0	0
14	4	0	2220	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.

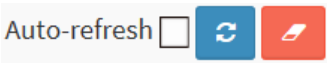
STP : The number of legacy STP Configuration BPDU's received/transmitted on the port.

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.

Refresh: Click to refresh the page immediately.

Clear: Clears the counters for the selected port.

3-10 MVR

3-10.1 Statistics

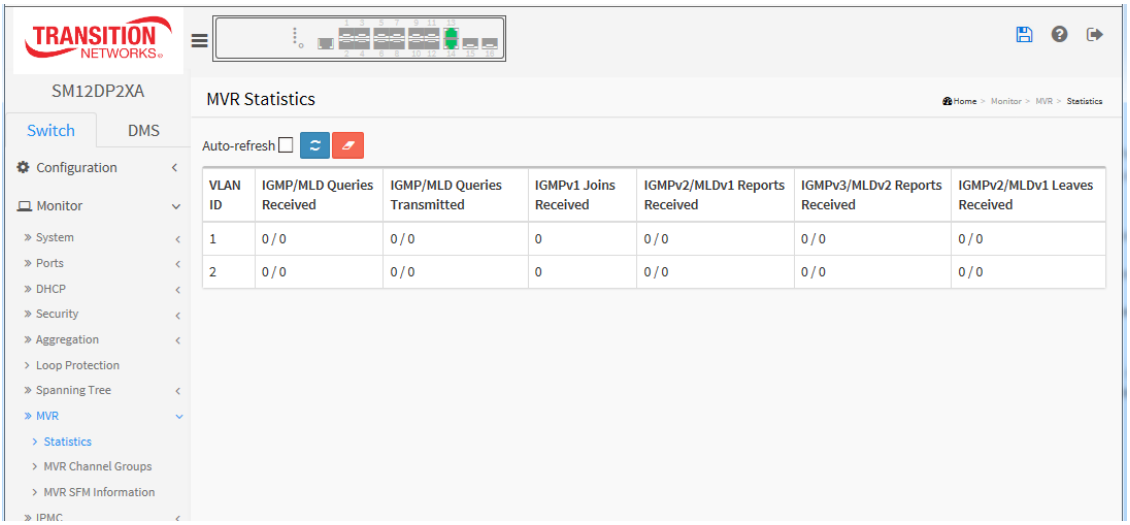
The section describes the MVR detail Statistics displayed after you have configured MVR on the switch. It provides detailed MVR Statistics Information.

Web Interface

To display the MVR Statistics Information in the web interface:

1. Click Monitor, MVR, Statistics.
2. To automatically refresh the information, check the Auto-refresh checkbox.
3. Click Refresh to refresh an entry of the MVR Statistics Information.

Figure 3-10.1: MVR Statistics



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.

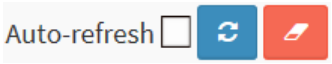
IGMPv1 Joins Received : The number of Received IGMPv1 Joins.

IGMPv2/MLDv1 Report's Received : The number of Received IGMPv2 Joins and MLDv1 Reports, respectively.

IGMPv3/MLDv2 Report's Received : The number of Received IGMPv1 Joins and MLDv2 Report's, respectively.

IGMPv2/MLDv1 Leave's Received : The number of Received IGMPv2 Leaves and MLDv1 Dones, respectively.

Buttons



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

Refresh: Click to refresh the page.

Clear: Clears the counters for the selected port.

3-10.2 MVR Channels Groups

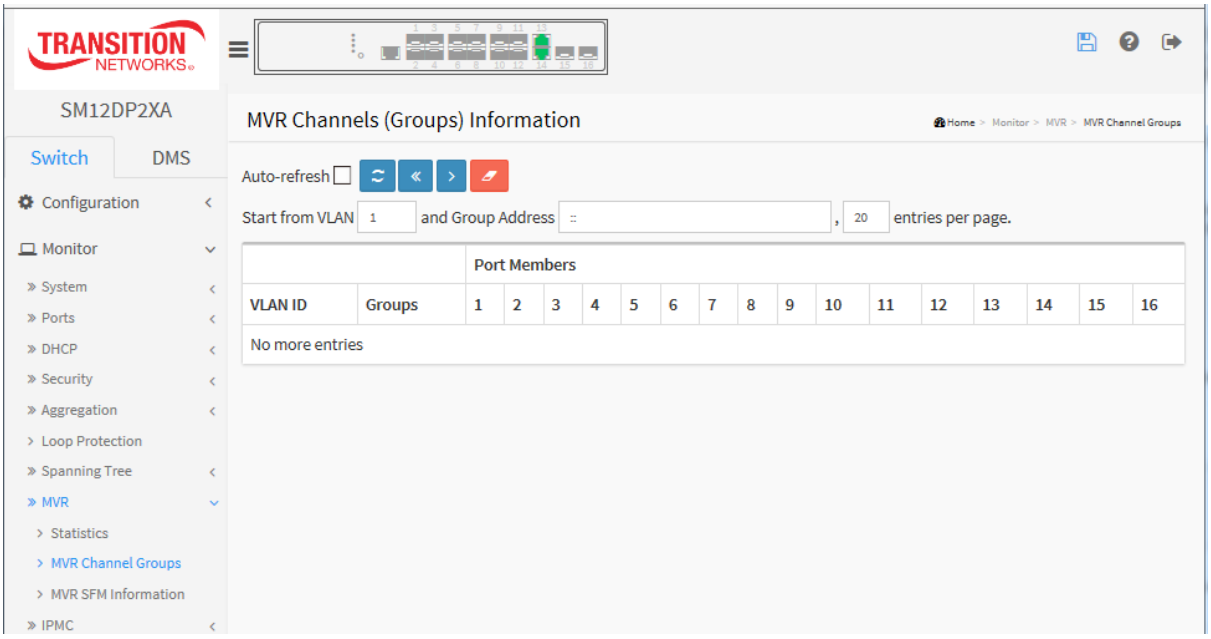
The section describes user could display the MVR Groups detail information on the switch. Entries in the MVR Group Table are shown on this page. The MVR Group Table is sorted first by VLAN ID, and then by group.

Web Interface

To display the MVR Groups Information in the web interface:

1. Click Monitor, MVR, MVR Channel Groups.
2. To automatically refresh the information, check the Auto-refresh checkbox.
3. Click the Refresh button to immediately refresh an entry of the MVR Groups Information.
4. Click **<<** or **>** to move to the previous or next entry.

Figure 3-10.2: MVR Channels (Groups) Information



Navigating the MVR Channels (Groups) Information Table

Each page shows up to 99 entries from the MVR Group table, default being 20, selected through the "entries per page" input field. When first visited, the web page will show the first 20 entries from the beginning of the MVR Channels (Groups) Information Table.

The "Start from VLAN", and "Group Address" input fields let you select the starting point in the MVR Channels (Groups) Information Table. Clicking **Refresh** the button will update the displayed table starting from that or the closest next MVR Channels (Groups) Information Table match.
In addition, the two input fields will - upon a **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 the 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.

MVR Channels (Groups) Information Table Columns

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.

<<: Updates the system log entries to the first available entry ID

> : Updates the system log entry to the next available entry ID.

3-10.3 MVR SFM Information

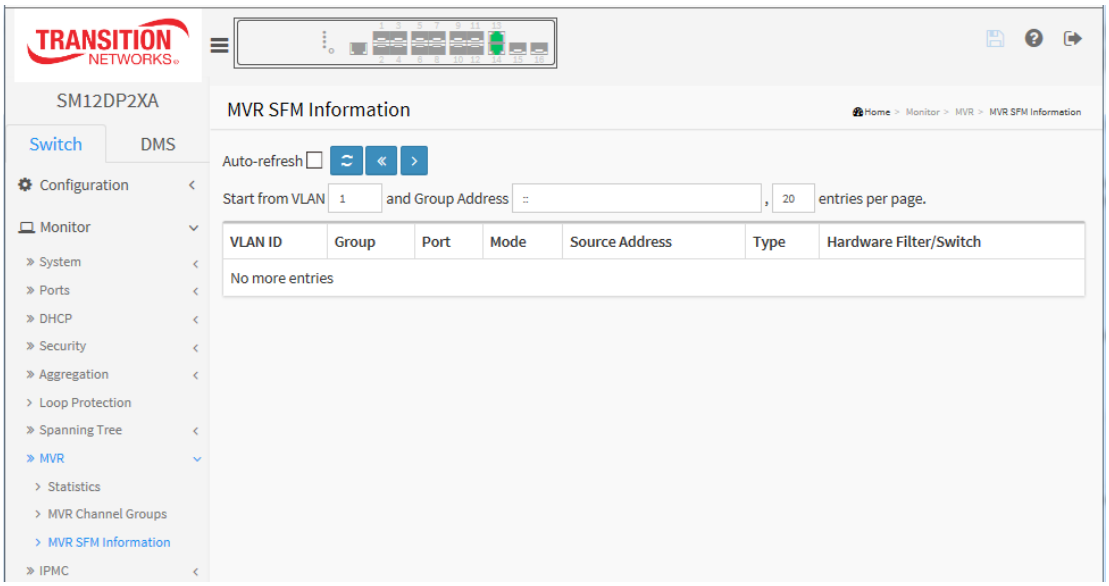
The MVR SFM (Source-Filtered Multicast) Information Table also contains the SSM (Source-Specific Multicast) information. This table is sorted first by VLAN ID, then by group, and then by Port. Different source addresses belong to the same group are treated as single entry.

Web Interface

To display the MVR SFM Information in the web interface:

1. Click Monitor, MVR, MVR SFM Information.
2. To auto-refresh the information check the Auto-refresh checkbox.
3. Click the Refresh button to immediately refresh an entry.
4. Click << or > to move to previous or next entry.

Figure 3-10.2: MVR SFM Information



Parameter descriptions:

Navigating the MVR SFM Information Table

Each page shows up to 99 entries from the MVR SFM Information Table, default being 20, selected through the "entries per page" input field. When first visited, the web page will show the first 20 entries from the beginning of the MVR SFM Information Table.

The "Start from VLAN", and "Group Address" input fields let you select the starting point in the MVR SFM Information Table. Clicking the **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 the 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.

VLAN ID : VLAN ID of the group.

Group : Group address of the group displayed.

Port : Switch port number.

Mode : Indicates the filtering mode maintained per (VLAN ID, port number, Group Address) basis. It can

be either Include or Exclude.

Source Address : IP Address of the source. Currently, system limits the total number of IP source addresses for filtering to be 128. When there is no any source filtering address, the text "None" is shown in the Source Address field.

Type : Indicates the Type. It can be either Allow or Deny.

Hardware Filter/Switch : Indicates whether data plane destined to the specific group address from the source IPv4/IPv6 address could be handled by the chip.

Buttons

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

Refresh: Click to 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

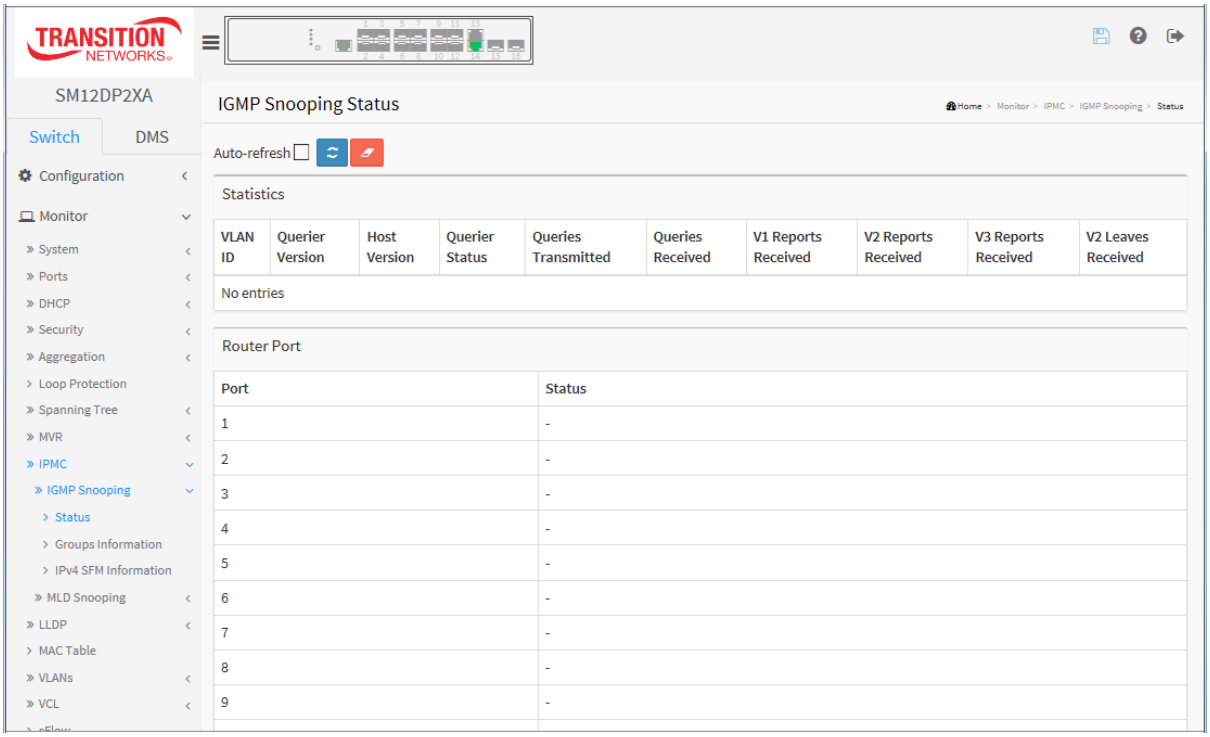
After you complete the IGMP Snooping configuration, the switch can display the IGMP Snooping Status. This page displays the IGMP Snooping detail status.

Web Interface

To display the IGMP Snooping status in the web interface:

1. Click Monitor, IPMC, IGMP Snooping, Status.
2. To automatically refresh the information, check the Auto-refresh box.
3. Click Refresh to refresh the IGMP Snooping Status.
4. Click Clear to clear the IGMP Snooping Status.

Figure 3-11.1.1: IGMP Snooping Status.



Parameter descriptions:

VLAN ID : The VLAN ID of the entry.

Querier Version : Working Querier Version currently.

Host Version : Working Host Version currently.

Querier Status : 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.

3-11.1.2 Group Information

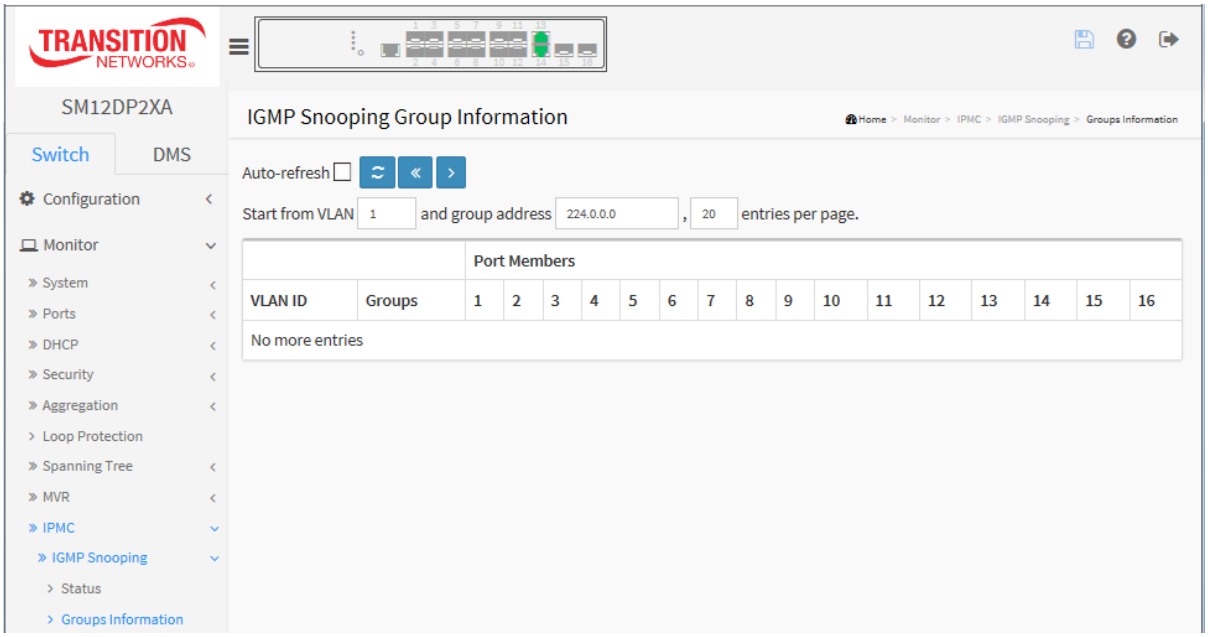
After you complete to set the IGMP Snooping function then you can let the switch to display the IGMP Snooping Group Information. Entries in the IGMP Group Table are shown on this page.
The IGMP Group Table is sorted first by VLAN ID, and then by group. The > button will use the last entry of the currently displayed table as the 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 > IPMC > IGMP Snooping > Groups Information.
2. To auto-refresh the information check the “Auto-refresh box.
3. Click “Refresh” to refresh an entry of the IGMP Snooping Groups Information.
4. Click << or > to move to the previous or next entry.

Figure 3-11.1.2: IGMP Snooping Groups Information



Navigating the IGMP Group Table

Each page shows up to 99 entries from the IGMP Group table, default being 20, selected through the "entries per page" input field. When first visited, the web page will show the first 20 entries from the beginning of the IGMP Group Table. The "Start from VLAN", and "group" input fields let you select the starting point in the IGMP Group Table. Clicking the **Refresh** button will update the displayed table starting from that or the closest next IGMP Group Table match. In addition, the two input fields will - upon a **Refresh** button click - assume the value of the first displayed entry, allowing for continuous refresh with the same start address. The **>** button will use the last entry of the currently displayed table as the 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.

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

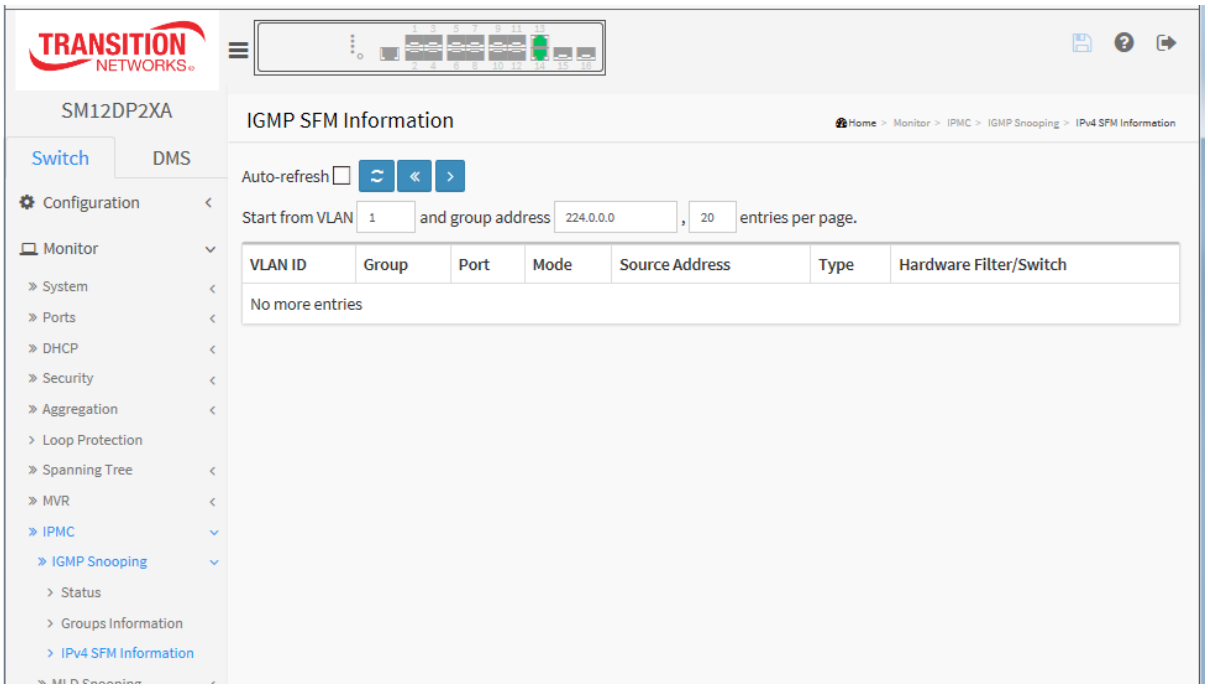
Entries in the IGMP SFM Information Table are shown on this page. The IGMP SFM (Source-Filtered Multicast) Information Table also contains the SSM (Source-Specific Multicast) information. This table is sorted first by VLAN ID, then by group, and then by Port. Different source addresses belonging to the 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. To automatically refresh the information, check the Auto-refresh box.
3. Click Refresh to refresh an entry of the IPv4 SFM Information.
4. Click << or > to move to the previous or next entry.

Figure 3-11.1.3: IPv4 SFM Information



Navigating the IGMP SFM Information Table

Each page shows up to 99 entries from the IGMP SFM Information table, default being 20, selected through the "entries per page" input field. When first visited, the web page will show the first 20 entries from the beginning of the IGMP SFM Information Table.

The "Start from VLAN", and "group" input fields let you select the starting point in the IGMP SFM Information Table. Clicking the **Refresh** button will update the displayed table starting from that or the closest next IGMP SFM Information Table match. In addition, the two input fields will - upon a **Refresh** button click - assume the value of the first displayed entry, allowing for continuous refresh with the same start address.

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

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.

<<: 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

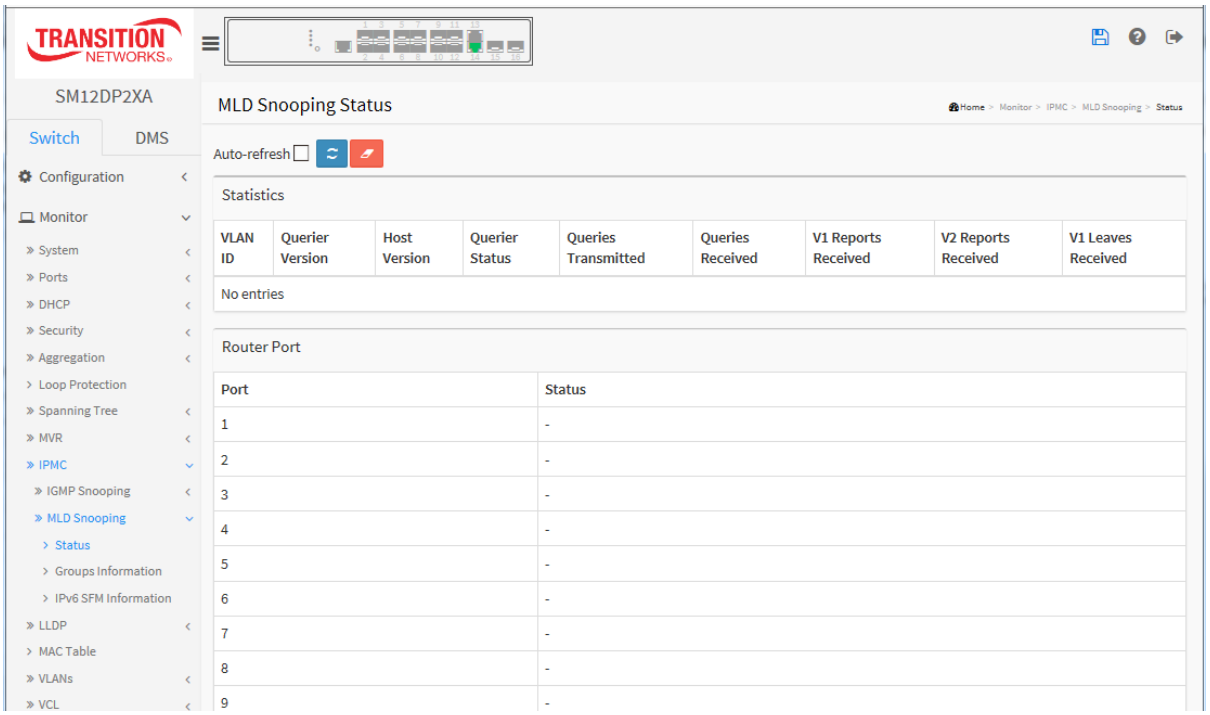
The page describes how to display the configured MLD Snooping Status and detail information.

Web Interface

To display the MLD Snooping Status in the web interface:

1. Click Monitor, IPMC, MLD Snooping, Status.
2. To automatically refresh the information check the Auto-refresh box.
3. Click Refresh to refresh an entry of the MLD Snooping Status Information.
4. Click Clear to clear the MLD Snooping Status.

Figure 3-11.2.1: MLD Snooping Status



Parameter descriptions:

VLAN ID : The VLAN ID of the entry.

Querier Version : Working Querier Version currently.

Host Version : Working Host Version currently.

Querier Status : Show the Querier status is "ACTIVE" or "IDLE". "DISABLE" denotes the specific interface is administratively disabled.

Queries Transmitted : The number of Transmitted Queries.

Queries Received : The number of Received Queries.

V1 Reports Received : The number of Received V1 Reports.

V2 Reports Received : The number of Received V2 Reports.

V1 Leaves Received : The number of Received V1 Leaves.

Router Port : Display which ports act as router ports. A router port is a port on the Ethernet switch that leads towards the Layer 3 multicast device or MLD querier.

Static denotes the specific port is configured to be a router port.

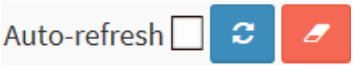
Dynamic denotes the specific port is learnt to be a router port.

Both denote the specific port is configured or learnt to be a router port.

Port : Switch port number.

Status : Indicate whether specific port is a router port or not.

Buttons



Auto-refresh: Check 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.

3-11.2.2 Group Information

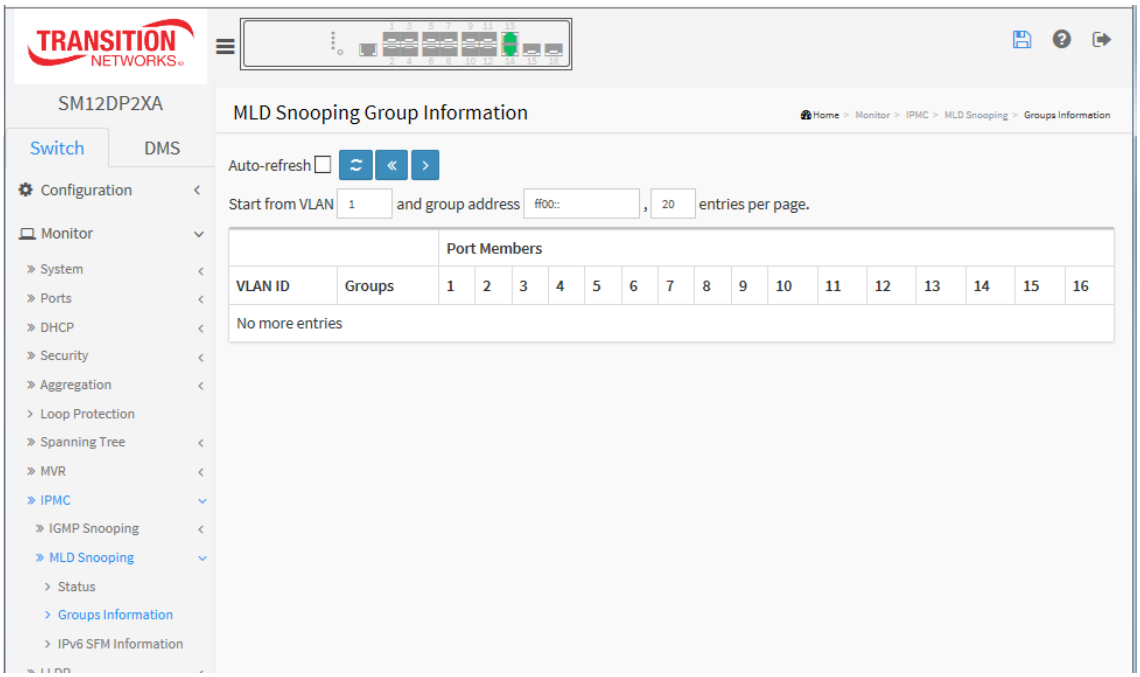
The page describes the MLD Snooping Groups Information. The "Start from VLAN", and "group" input fields let you select the starting point in the MLD Group table.

Web Interface

To display the MLD Snooping Group information in the web interface:

1. Click Monitor, MLD Snooping, Groups Information.
2. To automatically refresh the information, check the Auto-refresh box.
3. Click Refresh to refresh an entry of the MLD Snooping Group Information.
4. Click Clear to clear the MLD Snooping Groups information.

Figure 3-11.2.2: MLD Snooping Group Information



Navigating the MLD Group Table

Each page shows up to 99 entries from the MLD Group table (the default is 20) selected through the "entries per page" input field. When first visited, the web page will show the first 20 entries from the beginning of the MLD Group Table.

The "Start from VLAN", and "group" input fields let you select the starting point in the MLD Group Table. Clicking the **Refresh** button will update the displayed table starting from that or the closest next MLD Group Table match. In addition, the two input fields will - upon a **Refresh** button click - assume the value of the first displayed entry, allowing for continuous refresh with the same start address.

The **>** button will use the last entry of the currently displayed table as the 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.

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.

3-11.2.3 IPv6 SFM Information

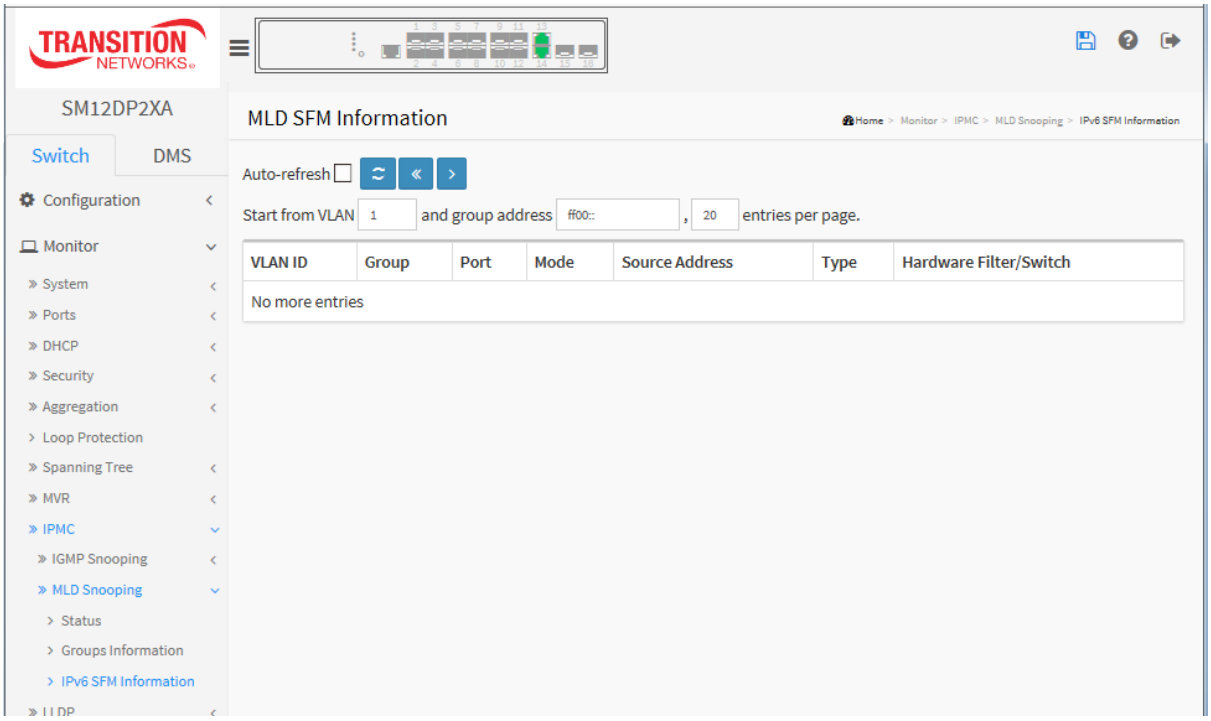
Entries in the MLD SFM Information table are shown on this page. The MLD SFM (Source-Filtered Multicast) Information table also contains the SSM (Source-Specific Multicast) information. This table is sorted first by VLAN ID, then by group, and then by Port. Different source addresses belonging to the 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. To automatically refresh the information, check the Auto-refresh checkbox.
3. Click **Refresh** to refresh an entry of the MLDv2 IPv6 SSM Information.
4. Click **<<** or **>** to move to previous or next entry.

Figure 3-11.2.3: IPv6 SFM Information



Navigating the MLD SFM Information Table

Each page shows up to 99 entries from the MLD SFM Information table, default being 20, selected through the "entries per page" input field. When first visited, the web page will show the first 20 entries from the beginning of the MLD SFM Information table.

The "Start from VLAN", and "group" input fields let you select the starting point in the MLD SFM Information Table. Clicking the **Refresh** button will update the displayed table starting from that or the closest next MLD SFM Information table match. In addition, the two input fields will - upon a **Refresh** button click - assume the value of the first displayed entry, allowing for continuous refresh with the same start address.

The **>** button will use the last entry of the currently displayed table as the 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.

Parameter descriptions:

VLAN ID : VLAN ID of the group.

Group : Group address of the group displayed.

Port : Switch port number.

Mode : Indicates the filtering mode maintained per (VLAN ID, port number, Group Address) basis. It can be either Include or Exclude.

Source Address : IP Address of the source. Currently, system limits the total number of IP source addresses for filtering to be 128.

Type : Indicates the Type. It can be either Allow or Deny.

Hardware Filter/Switch : Indicates whether data plane destined to the specific group address from the source IPv6 address could be handled by the chip.

Buttons

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

Refresh: Click to refresh the page.

<<: 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 Neighbors

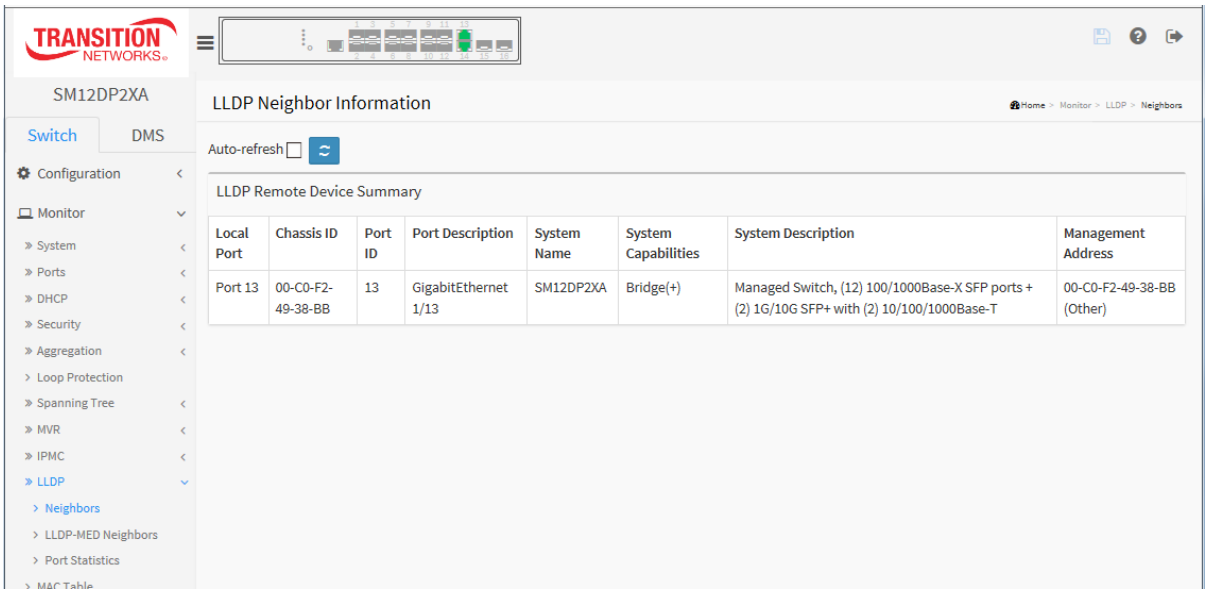
This page provides details of LLDP neighbors. The displayed table contains a row for each port on which an LLDP neighbor is detected. If your network without any device supports LLDP then the table will show "*No LLDP neighbor information found*".

Web Interface

To show LLDP neighbors:

1. Click Monitor, LLDP, Neighbors.
2. Click Refresh to manually update the web page immediately.
3. Click Auto-refresh to automatically update the web page every 3 seconds.

Figure 3-12.1: LLDP Neighbor information



Parameter descriptions:

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

Chassis ID : The identification of the neighbors' LLDP frames (e.g., *00-C0-F2-49-38-BB*).

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

Port Description : the port description advertised by the neighbor unit (e.g., *GigabitEthernet 1/13*).

System Name : the name advertised by the neighbor unit.

System Capabilities : describes the neighbor unit's capabilities, including:

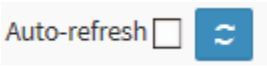
1. Other
2. Repeater
3. Bridge
4. WLAN Access Point
5. Router
6. Telephone
7. DOCSIS cable device
8. Station only
9. Reserved

When a capability is enabled, the capability is followed by a (**+**).

If the capability is disabled, the capability is followed by a (**-**).

Management Address : Management Address is the neighbor unit's address that is used for higher layer entities to assist discovery by the network management. This could for instance hold the neighbors' IP address (e.g., *192.168.1.77 (IPv4)*) or MAC address (e.g., *00-C0-F2-49-38-BB (Other)*).

Buttons



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

Refresh: Click to refresh the page immediately.

3-12.2 LLDP-MED Neighbor

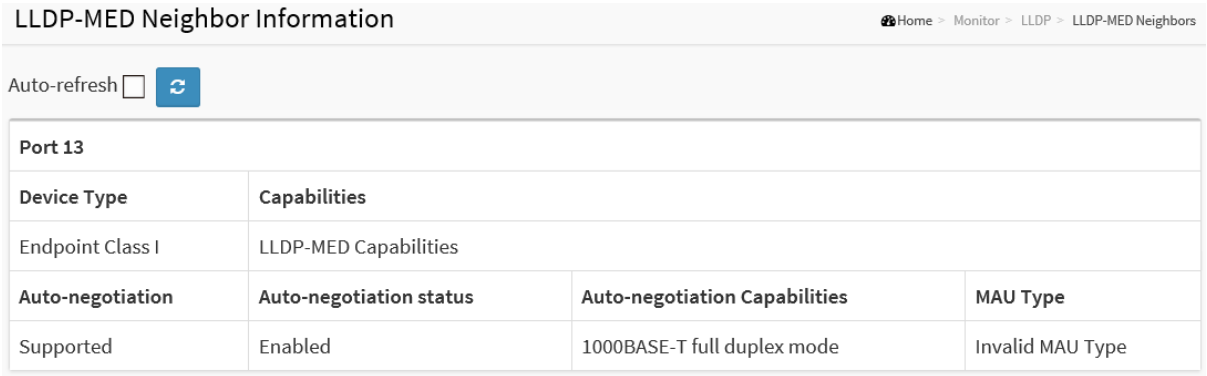
This page provides a status overview of all LLDP-MED neighbors. The displayed table contains a row for each port on which an LLDP neighbor is detected. This function applies to VoIP devices which support LLDP-MED. If your network has no devices that support LLDP-MED, the table will display "*No LLDP-MED neighbor information found*".

Web Interface

To show LLDP-MED neighbor:

1. Click Monitor, LLDP, LLDP-MED Neighbors.
2. Click Refresh to manually update the web page.
3. Click Auto-refresh to automatically update the web page every 3 seconds.

Figure 3-12.2: LLDP-MED Neighbors information



Port 13			
Device Type	**Capabilities**		
Endpoint Class I	LLDP-MED Capabilities		
Auto-negotiation	**Auto-negotiation status**	**Auto-negotiation Capabilities**	**MAU Type**
Supported	Enabled	1000BASE-T full duplex mode	Invalid MAU Type

Parameter descriptions:

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

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

LLDP-MED Network Connectivity Device Definition

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

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

LLDP-MED Endpoint Device Definition

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

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

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

LLDP-MED 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.

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

2. Voice Signalling - for use in network topologies that require a different policy for the voice signaling than for the voice media.

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

4. Guest Voice Signalling - for use in network topologies that require a different policy for the guest voice signaling than for the guest voice media.

5. Softphone Voice - for use by softphone applications on typical data centric devices, such as PCs or laptops.

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

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

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

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

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

Auto-negotiation : **I**dentifies 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.

3-12.3 Port Statistics

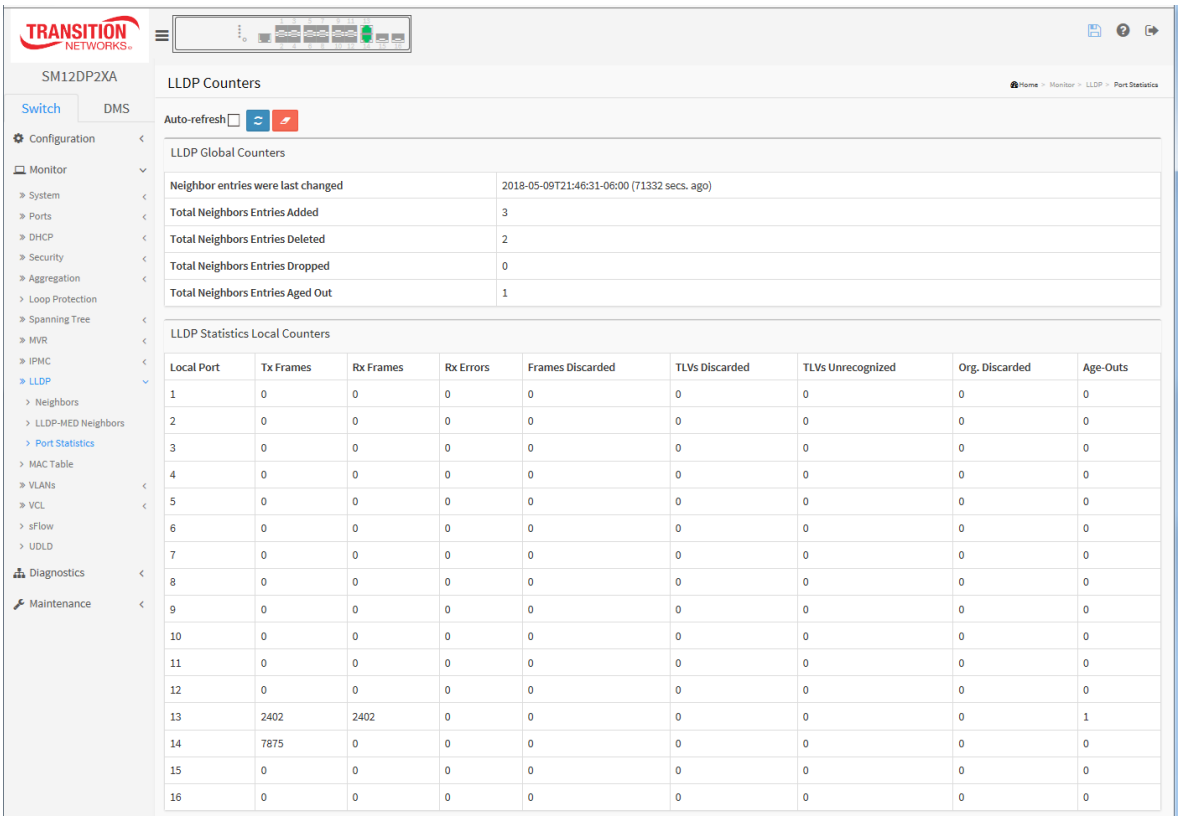
Two types of LLDP counters are shown. *Global* counters are counters that refer to the whole switch. *Local* counters refer to per-port counters.

Web Interface

To show LLDP Statistics:

1. Click Monitor, LLDP, Port Statistics to show the LLDP counters page.
2. Click Refresh to manually update the web page.
3. Click Auto-refresh for auto-update the web page.
4. Click Clear to clear all counters.

Figure 3-12.4: LLDP Port Statistics



Parameter descriptions:

LLDP Global Counters

Neighbour entries were last changed: Shows the time when the last entry was last deleted or added. It also shows the time elapsed since the last change was detected in the format: *2010-12-31T23:59:59+00:00 (339039 secs. ago)*.

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

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

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

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

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

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

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

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

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

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

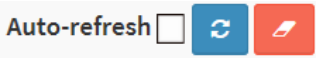
TLVs Discarded : Each LLDP frame can contain multiple pieces of information, known as TLVs (TLV is short for "Type Length Value"). If a TLV is malformed, it is counted and discarded.

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

Org. Discarded : The number of organizationally received TLVs.

Age-Outs : Each LLDP frame contains information about how long time the LLDP information is valid (age-out time). If no new LLDP frame is received within the age out time, the LLDP information is removed, and the Age-Out counter is incremented.

Buttons



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

Refresh: Click to refresh the page.

Clear: Clears the counters for the selected port.

3-13 MAC Table

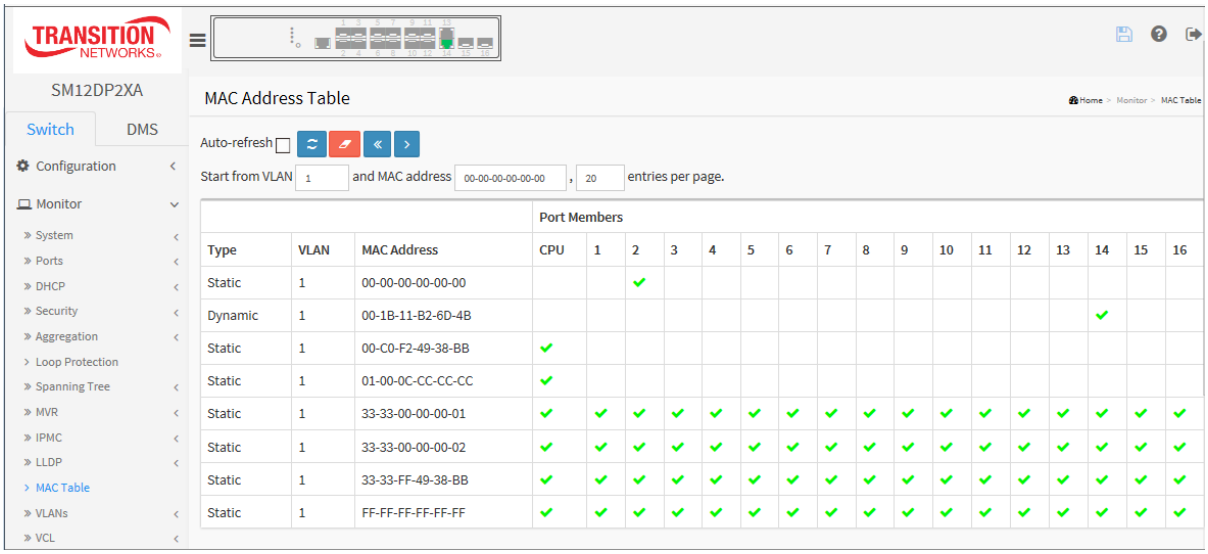
Entries in the MAC Table are shown on this page. The MAC Table contains up to 8192 entries, and is sorted first by VLAN ID, then by MAC address.

Web Interface

To display MAC Address Table in the web interface:

1. Click Monitor, MAC Table to display the MAC Address Table.
2. View the Type, VLAN, MAC Address, and Port Members information.
3. Navigate the MAC Address Table as described below.

Figure 3- 13: MAC Address Table



Each page shows up to 999 entries from the MAC table (default is 20 entries) selected through the "entries per page" input field. When first visited, the web page will show the first 20 entries from the beginning of the MAC Table. The first displayed will be the one with the lowest VLAN ID and the lowest MAC address found in the MAC Table.

The "Start from MAC address" and "VLAN" input fields let you select the starting point in the MAC Table. Clicking the **Refresh** button will update the displayed table starting from that or the closest next MAC Table match. In addition, the two input fields will - upon a **Refresh** button click - assume the value of the first displayed entry, allowing for continuous refresh with the same start address.

The **>** button will use the last entry of the currently displayed VLAN/MAC address pairs as the 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.

Parameter descriptions:

MAC Address Table Columns

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 are checked (✔).

Buttons

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

Refresh: Click to refresh the page immediately.

Clear: Clears the counters for the selected port.

<<: Updates the system log entries to the first available entry ID.

> : Updates the system log entry to the next available entry ID.

NOTE:

00-40-C7-73-01-29 : your switch MAC address (for IPv4).

33-33-00-00-00-01 : Destination MAC (for IPv6 Router Advertisement) (reference IPv6 RA.JPG).

33-33-00-00-00-02 : Destination MAC (for IPv6 Router Solicitation) (reference IPv6 RS.JPG).

33-33-FF-73-01-29 : Destination MAC (for IPv6 Neighbor Solicitation) (reference IPv6 DAD.JPG).

33-33-FF-A8-01-01: your switch MAC address (for IPv6 global IP).

FF-FF-FF-FF-FF-FF: for Broadcast.

3-14 VLANs

3-14.1 VLAN Membership

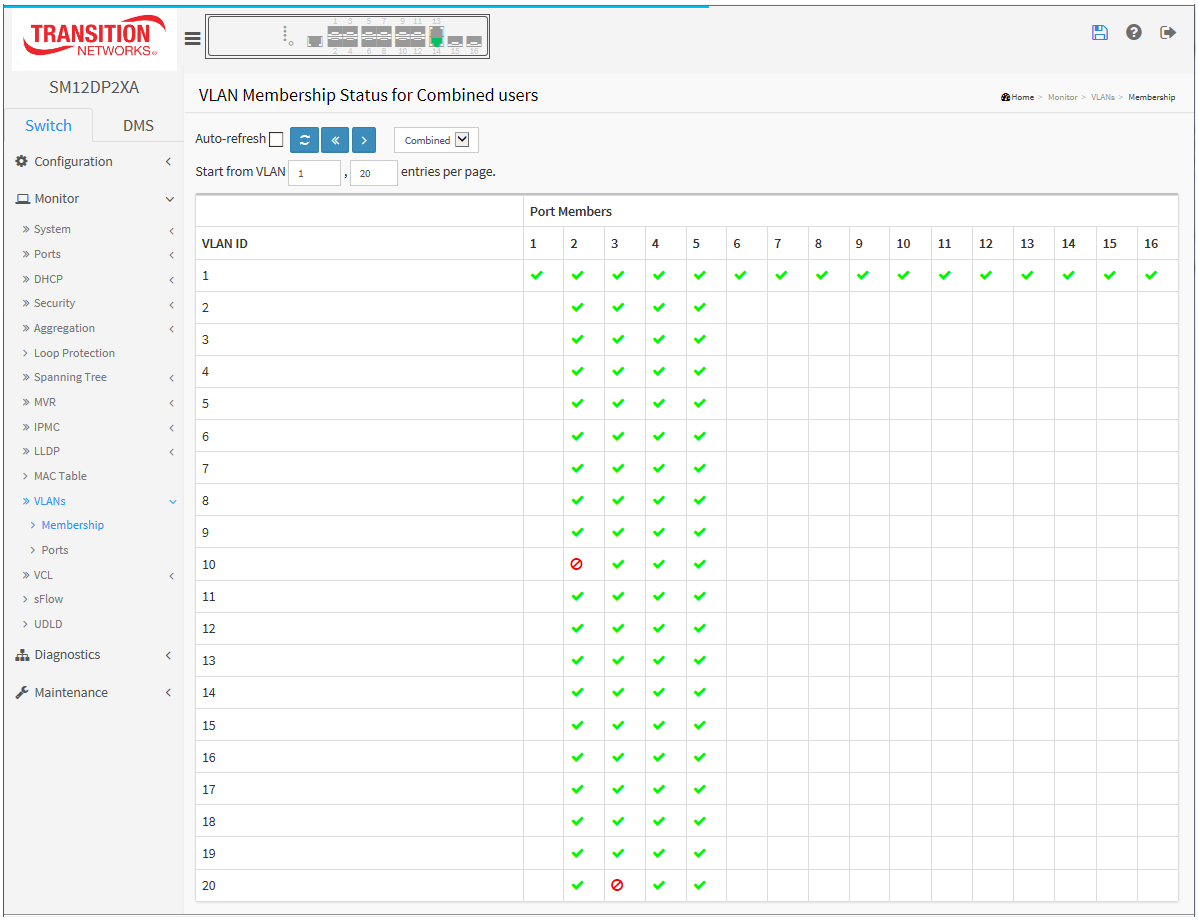
This page provides an overview of membership status of VLAN users. The VLAN Membership Status page shows the current VLAN port members for all VLANs configured by a selected VLAN User (selection allowed by the VLAN users combo box). When ALL VLAN Users are selected, it shows this information for all the VLAN users, and this is by default. VLAN membership allows the frames classified to the VLAN ID to be forwarded on the respective VLAN member ports.

Web Interface

To configure VLAN membership configuration in the web interface:

1. Click Monitor, VLANs, Membership.
2. View the VLAN IDs and related Port Members.
3. Filter the view using the VLAN Users dropdown (Combined).
4. Click Refresh to update the status.

Figure 3-14.1: VLAN Membership Status for Combined users



Each page shows up to 99 entries from the VLAN table, default being 20, selected through the "entries per page" input field. When first visited, the web page will show the first 20 entries from the beginning of the VLAN Table. The first displayed will be the one with the lowest VLAN ID found in the VLAN Table.

The "Start from VLAN" input field let you select the starting point in the VLAN table. The “entries per page” input field let you set the number of table entries displayed per webpage. Clicking the **“Refresh”** button will update the displayed table starting from that or the closest next VLAN Table match.

The **>** button will use the last entry of the currently displayed VLAN entry as the 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.

Parameter descriptions:

VLAN users : Various internal software modules may use VLAN services to configure VLAN memberships on the fly. The drop-down list on the right allows for selecting between showing VLAN memberships as configured by an administrator (Admin) or as configured by one of these internal software modules. The "Combined" entry shows a combination of the administrator and internal software modules configuration, and basically reflects what is actually configured in hardware.

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

Port Members : A row of check boxes for each port is displayed for each VLAN ID.
If a port is included in a VLAN, an image ✓ will be displayed.
If a port is included in a Forbidden port list, an image ⊘ will be displayed.
If a port is included in a Forbidden port list and dynamic VLAN user register VLAN on same Forbidden port, then conflict port will be displayed as ✕.

Buttons

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

Refresh: Click to refresh the page immediately.

<< : Click to use the last entry of the currently displayed VLAN entry as the basis for the next lookup.

> : Updates the table with the last entry.

Select VLAN users from this drop down list (Combined, Admin, various internal software modules).

3-14.2 VLAN Port

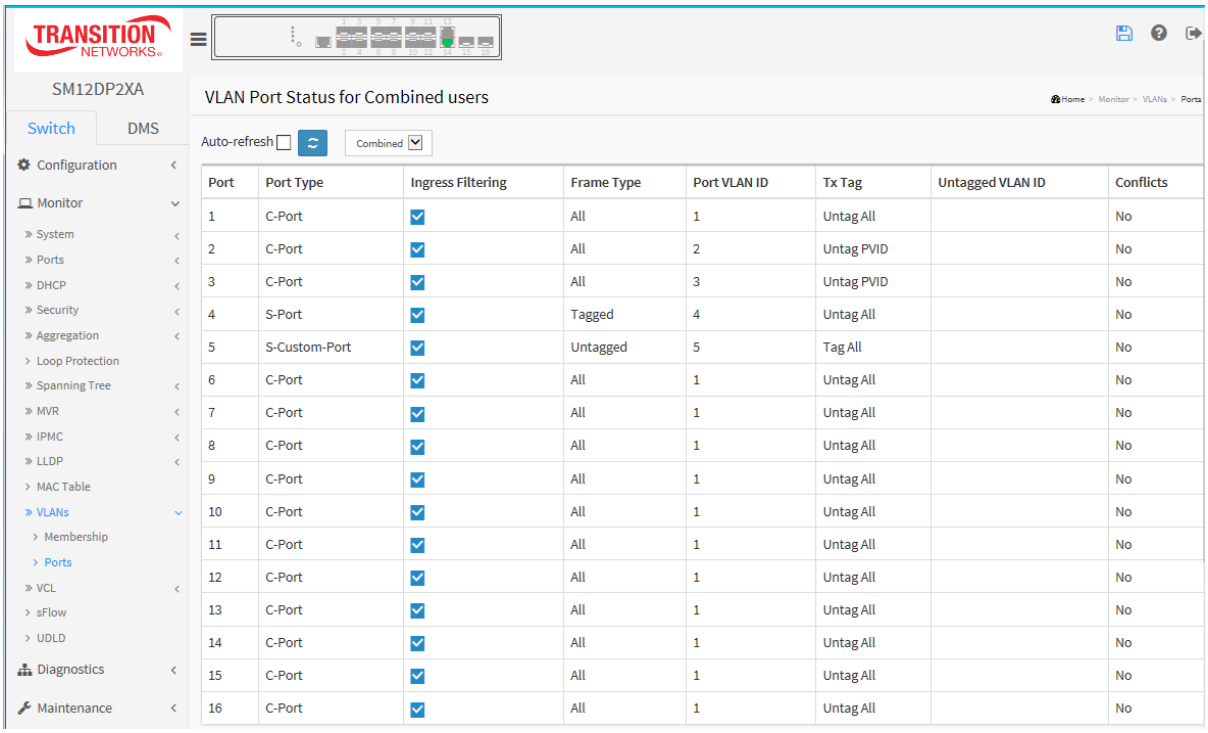
The VLAN Port Status page displays the information of all VLAN status and reports it by the order of Static, NAS, MVRP, MVP, Voice VLAN, MSTP, GVRP, and Combined.

Web Interface

To display VLAN Port Status in the web interface:

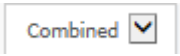
1. Click Monitor, VLANs, Ports.
2. Specify the VLAN users to be displayed (Combined, Admin, NAS, GVRP, MVR, etc.).
3. View the displayed Port Status information.

Figure 3-14.2: VLAN Port Status for Combined users



Port	Port Type	Ingress Filtering	Frame Type	Port VLAN ID	Tx Tag	Untagged VLAN ID	Conflicts
1	C-Port	☑	All	1	Untag All		No
2	C-Port	☑	All	2	Untag PVID		No
3	C-Port	☑	All	3	Untag PVID		No
4	S-Port	☑	Tagged	4	Untag All		No
5	S-Custom-Port	☑	Untagged	5	Tag All		No
6	C-Port	☑	All	1	Untag All		No
7	C-Port	☑	All	1	Untag All		No
8	C-Port	☑	All	1	Untag All		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
15	C-Port	☑	All	1	Untag All		No
16	C-Port	☑	All	1	Untag All		No

Parameter descriptions:



VLAN user : Various internal software modules may use VLAN services to configure VLAN port configuration on the fly. The drop-down list on the right allows for selecting between showing VLAN memberships as configured by an administrator (Admin) or as configured by one of these internal software modules. The "Combined" entry will show a combination of the administrator and internal software modules configuration, and basically reflects what is actually configured in hardware. If a given software modules hasn't overridden any of the port settings, the text "No data exists for the selected user" is shown in the table.

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

Port Type : Shows the Port Type (Unaware, C-Port, S-Port, or S-Custom-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. S-Custom-Port is S-port with a Custom TPID.

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

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

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

Tx Tag : Shows egress filtering frame status (Tag All, Untag All, or Untag PVID).

Untagged VLAN ID : Shows UVID (Untagged VLAN ID). A port's UVID determines the packet's behavior at the egress side.

Conflicts : Shows whether Conflicts exist (Yes or No). 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 immediately refresh the page.

3-15 VCL

3-15.1 MAC-based VLAN

This page shows MAC-based VLAN entries configured by various MAC-based VLAN users. Current support includes these VLAN User types:

CLI/Web/SNMP : These are referred to as static.

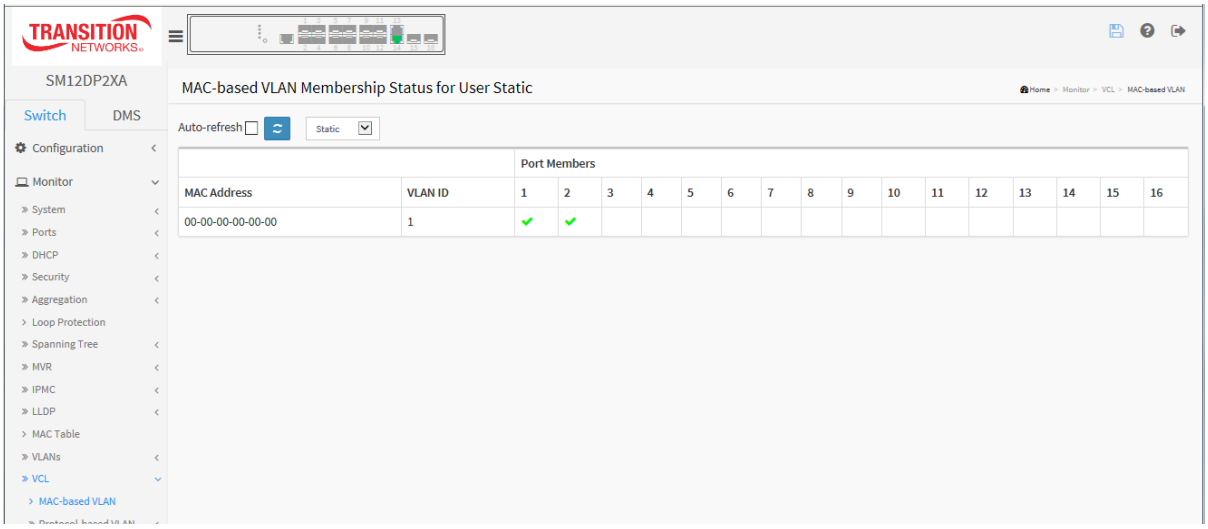
NAS : NAS provides port-based authentication, which involves communications between a Supplicant, Authenticator, and an Authentication Server.

Web Interface

To display MAC-based VLAN configuration in the web interface:

1. Click Monitor, VCL, MAC-based VLAN Status.
2. Specify the Static, NAS, Combined.
3. Display MAC-based information.

Figure 3-15.1: MAC-based VLAN Membership Status for User Static



Parameter descriptions:

MAC Address : Indicates the MAC address.

VLAN ID : Indicates the VLAN ID.

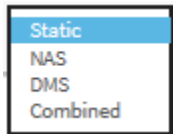
Port Members : Port members of the MAC-based VLAN entry.

Buttons

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

Refresh: Click to refresh the page.

VLAN user select box: lets you filter the set of displayed VLAN users.



3-15.2 Protocol-based VLAN

3-15.2.1 Protocol to Group

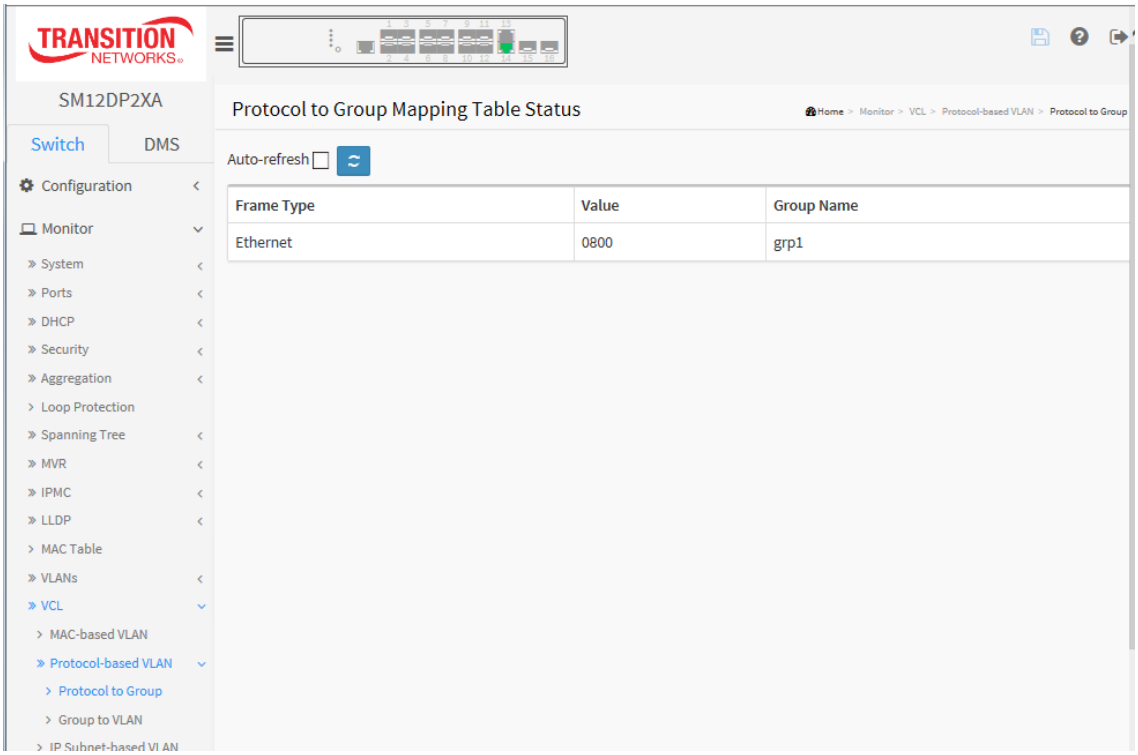
This page displays the protocols to Group Name (unique for each Group) mapping entries for the switch .

Web Interface

To display Protocol-based VLAN configuration in the web interface:

1. Click Monitor, VCL, > Protocol-based VLAN, Protocol to Group.
2. Check “Auto-refresh”.
3. Click “Refresh“ to refresh the port detailed statistics.

Figure 3-15.1: Protocol to Group Mapping Table Status



Parameter descriptions:

Frame Type : Frame Type can be 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 ranges from 0x0600-0xffff

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

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

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

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

OUI: OUI (Organizationally Unique Identifier) is value in format of xx-xx-xx where each pair (xx) in string is a hexadecimal value ranges from 0x00-0xff.

PID: If the OUI is hexadecimal 000000, the protocol ID is the Ethernet type (EtherType) field value for the protocol running on top of SNAP; if the OUI is an OUI for a particular organization, the protocol ID is a value assigned by that organization to the protocol running on top of SNAP.

In other words, if the value of OUI field is 00-00-00 then the value of PID will be etype (0x0600-0xffff) and if the value of OUI is other than 00-00-00 then the 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 alphabet characters (a-z or A-Z) and integers (0-9).

NOTE: special characters and underscore (_) are not allowed.

Buttons

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

Refresh: Click to refresh the page.

3-15.2.2 Group to VLAN

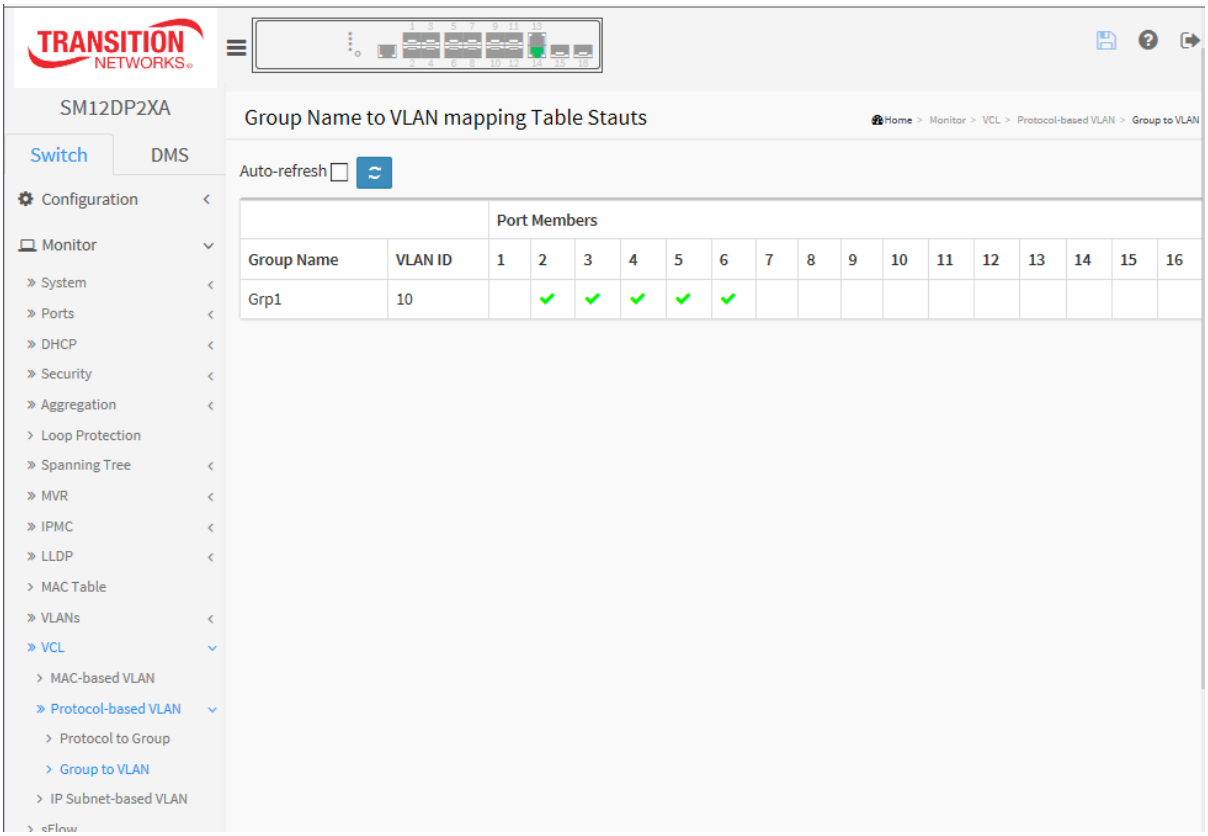
This page displays the configured Group Name to a VLAN for the switch.

Web Interface

To display Group to VLAN configuration in the web interface:

1. Click Monitor, VCL, Protocol-based VLAN, Group to VLAN.
2. Check Auto-refresh to refresh the status every 3 seconds.
3. Click Refresh to refresh the status immediately.

Figure 3-15.2.2: Group Name to VLAN mapping Table Status



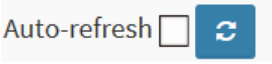
Parameter descriptions:

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 the Protocol to Group mapping table and must not be pre-used by any other existing mapping entry on this page.

VLAN ID : Indicates the ID to which Group Name will be mapped. A valid VLAN ID from 1-4095.

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

Buttons



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

Refresh: Click to refresh the page.

3-15.3 IP Subnet-based VLAN

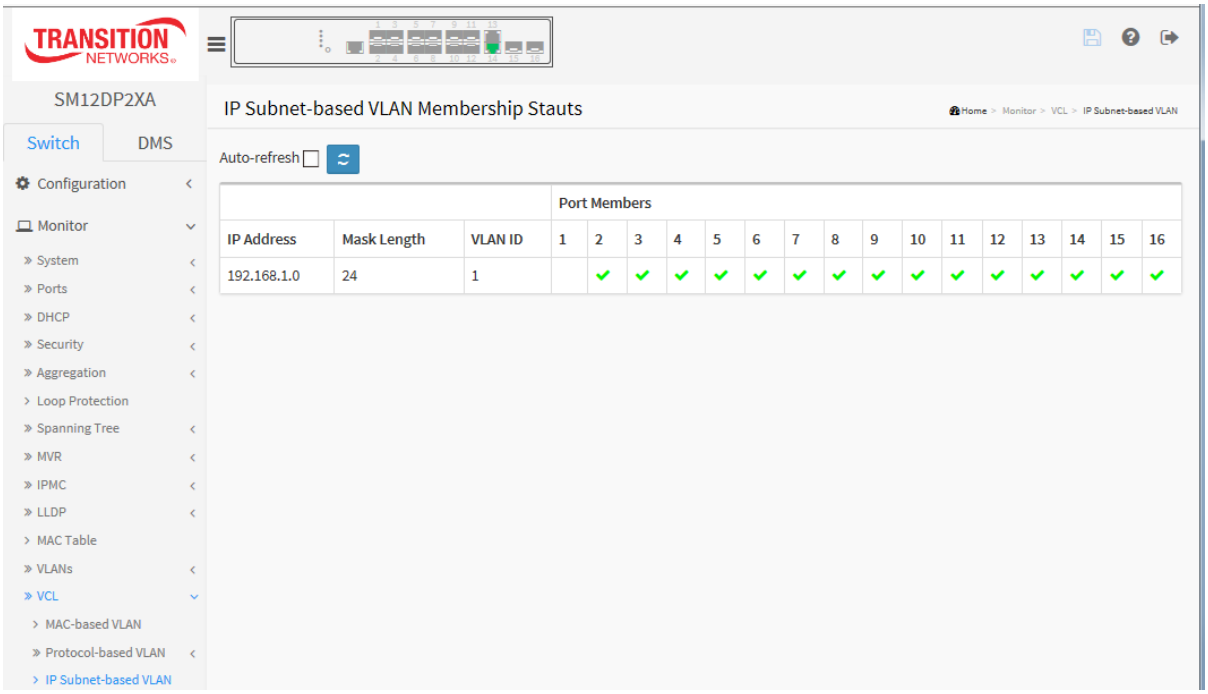
This page shows IP subnet-based VLAN entries. This page shows only static entries.

Web Interface

To display MAC-based VLAN configuration in the web interface:

1. Click Monitor, VCL, IP Subnet-based VLAN.
2. Check Auto-refresh.
3. Click Refresh to refresh the port detailed statistics immediately.

Figure 3-15.3: IP Subnet-based VLAN Membership Status



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: Click to refresh the page.

3-16 sFlow

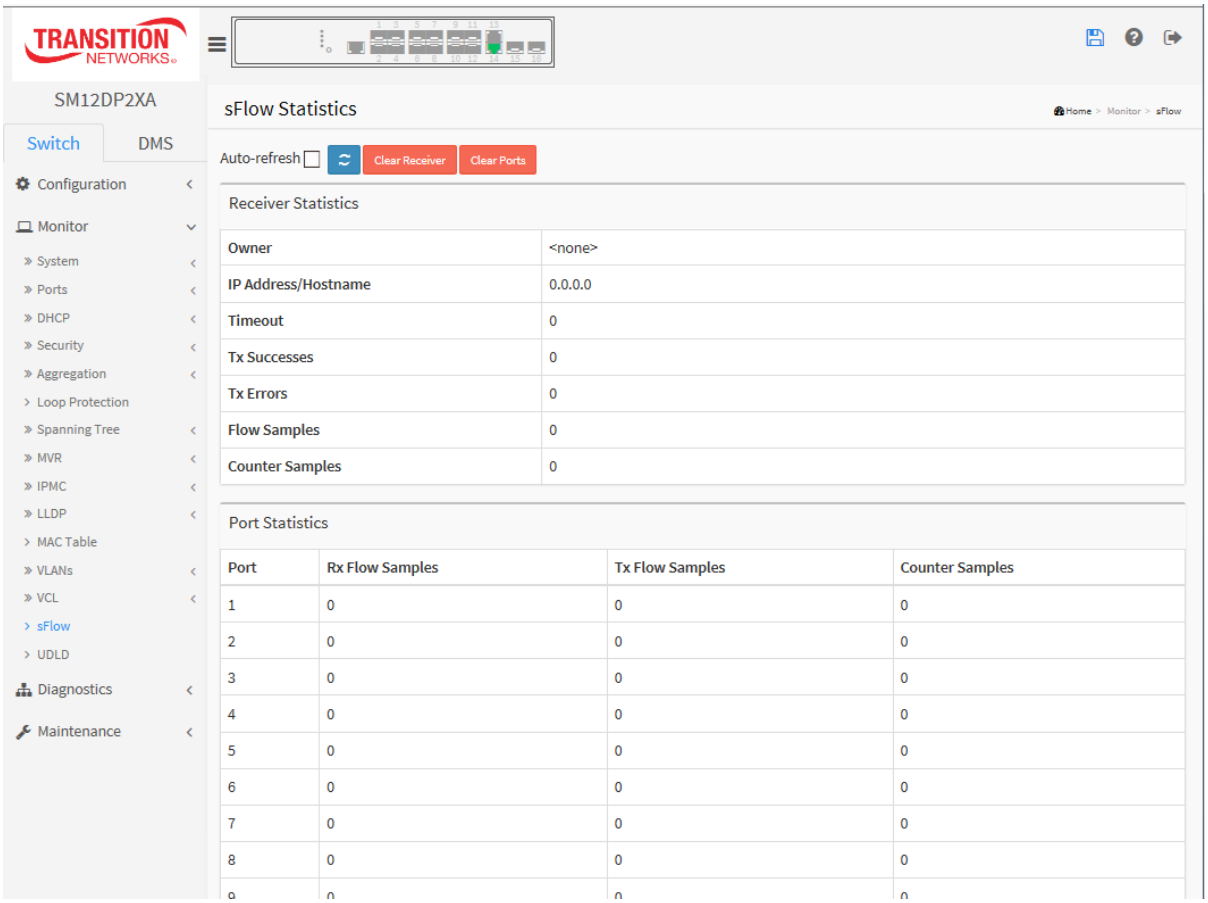
This page shows receiver and per-port sFlow statistics.

Web Interface

To display MAC-based VLAN configuration in the web interface:

1. Click Monitor, sFlow.
2. View the displayed sFlow information.

Figure 3-16: sFlow Statistics



Parameter descriptions:

Owner : This field shows the current owner of the sFlow configuration. It assumes one of these values:

<none> : Displays if sFlow is currently unconfigured/unclaimed, Owner contains *<none>*.

<Configured through local management> : Displays if sFlow is currently configured through Web or CLI, Owner.

<string> : Displays if sFlow is currently configured through SNMP, the Owner field contains a string identifying the sFlow receiver.

IP Address/Hostname : The IP address or hostname of the sFlow receiver.

Timeout : The number of seconds remaining before sampling stops and the current sFlow owner is released.

Tx Successes : The number of UDP datagrams successfully sent to the sFlow receiver.

Tx Errors : The number of UDP datagrams that has failed transmission. The most common source of errors is invalid sFlow receiver IP/hostname configuration. To diagnose, paste the receiver's IP address/hostname into the Ping Web page (Diagnostics > Ping/Ping6).

Flow Samples : The total number of flow samples sent to the sFlow receiver.

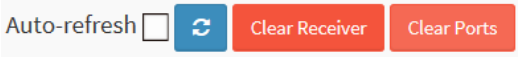
Counter Samples : The total number of counter samples sent to the sFlow receiver.

Port Statistics

Port : The port number for which the following statistics applies.

Rx and Tx Flow Samples : The number of flow samples sent to the sFlow receiver originating from this port. Here, flow samples are divided into Rx and Tx flow samples, where Rx flow samples contains the number of packets that were sampled upon reception (ingress) on the port and Tx flow samples contains the number of packets that were sampled upon transmission (egress) on the port.

Counter Samples : The total number of counter samples sent to the sFlow receiver originating from this port.



Buttons

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

Refresh: Click to refresh the page.

Clear Receiver: Clears the sFlow receiver counters.

Clear Ports: Clears the per-port counters.

3-17 UDLD

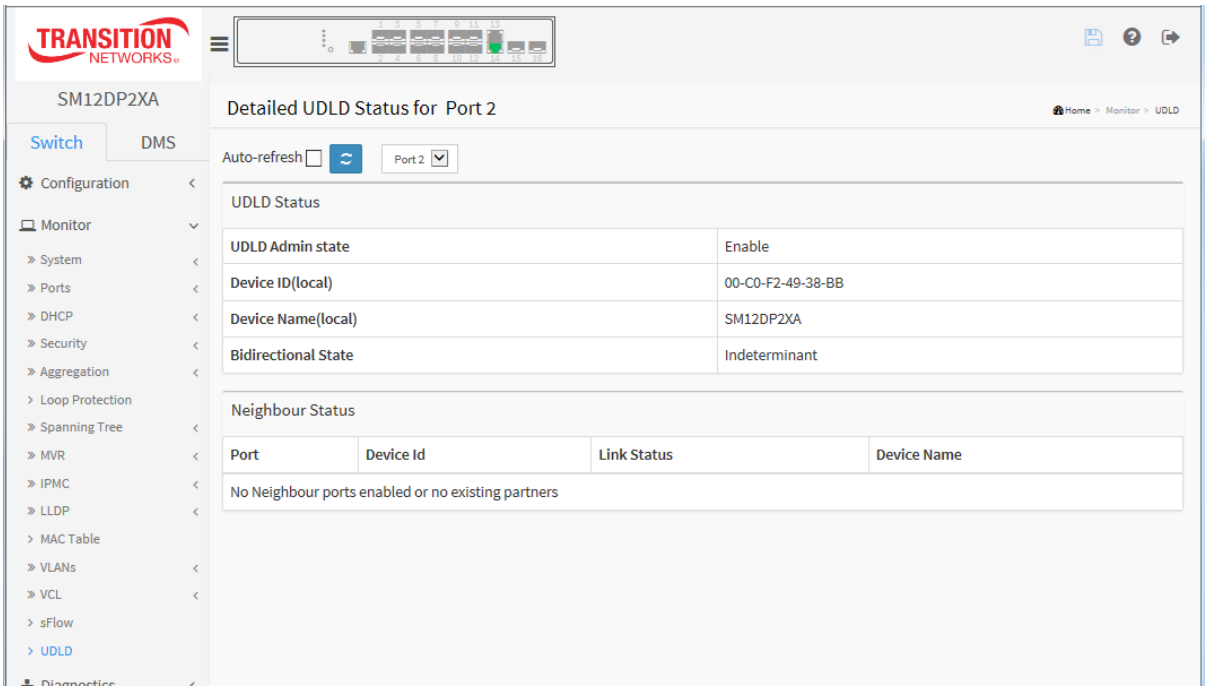
This page displays the UDLD status and Neighbor status of the ports.

Web Interface

To display UDLD status in the web interface:

1. Click Monitor, UDLD
2. View the displayed UDLD information.

Figure 3-17: Detailed UDLD Status



Parameter descriptions:

UDLD Status

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

Device ID(local) : The ID of Device.

Device Name(local) : The name of the Device (SM12DP2XA).

Bidirectional State : The current state of the port.

Neighbour Status

Port : The current port of neighbor device.

Device ID : The current ID of neighbor device.

Link Status : The current link status of neighbor port.

Device Name : The name of the Neighbor Device.

Chapter 4. Diagnostics

This page provides a set of basic system diagnostics, including ICMP Ping, Link OAM, ICMPv6 Ping, and Cable Diagnostics.

4-1 Ping

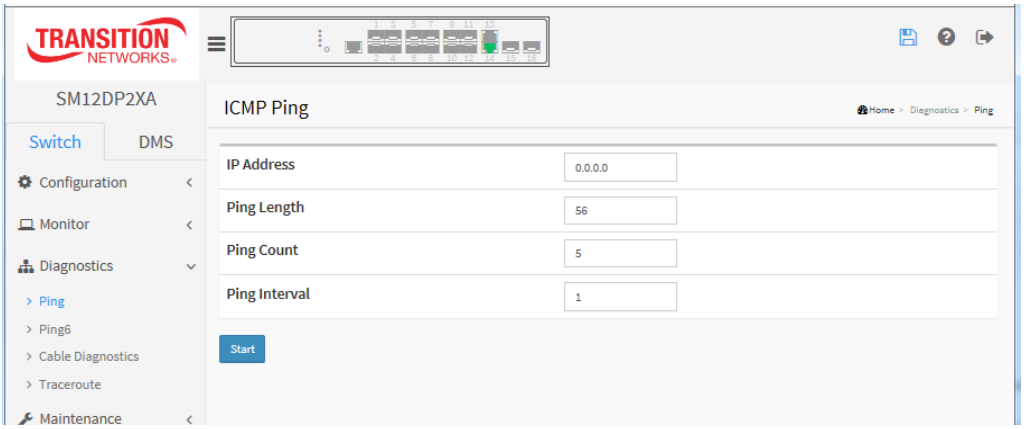
This page lets you issue ICMP PING packets to troubleshoot IPv4 connectivity issues.

Web Interface

To configure an ICMP PING Configuration in the web interface:

1. Specify the ICMP PING IP Address.
2. Specify the ICMP PING Size.
3. Click Start.

Figure 4-1: ICMP Ping



Parameter descriptions:

IP Address : To set the IP Address of device what you want to ping it.

Ping Length: The payload size of the ICMP packet. Values range from 2 bytes to 1452 bytes.

Ping Count: The count of the ICMP packet. Values range from 1 time to 60 times.

Ping Interval: The interval of the ICMP packet. Values range from 0 second to 30 seconds.

Start: Click the “Start” button then the switch will start to ping the device using the ICMP packet size set on the switch.

After you press Start, five ICMP packets are transmitted, and the sequence number and roundtrip time are displayed upon reception of a reply. The page refreshes automatically until responses to all packets are received, or until a timeout occurs.

```
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
```

4-2 Ping6

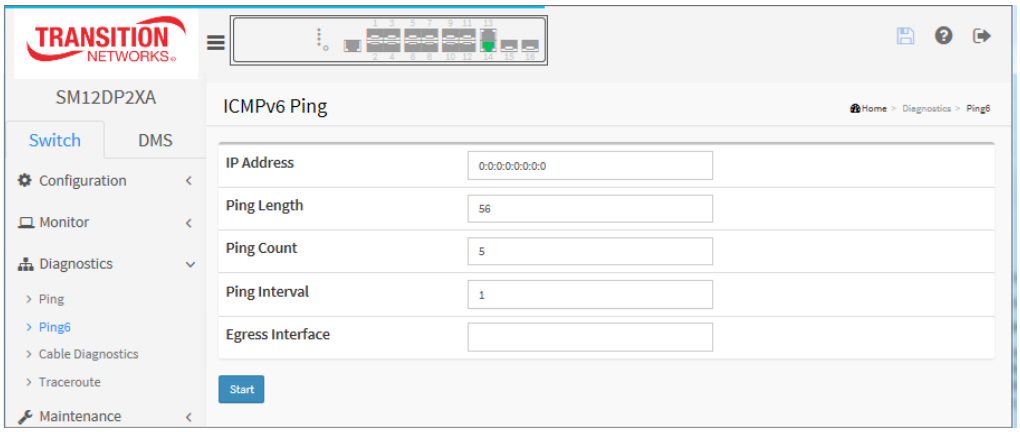
This page lets you issue ICMPv6 PING packets to troubleshoot IPv6 connectivity issues.

Web Interface

To configure an ICMPv6 PING Configuration in the web interface:

1. Specify the ICMPv6 PING IP Address.
2. Specify the ICMPv6 PING Size.
3. Click Start.

Figure 4-2: ICMPv6 Ping



Parameter descriptions: You can configure the following properties of the issued ICMPv6 packets:

IP Address : The destination IP Address with IPv6

Ping Length : The payload size of the ICMP packet. Values range from 2 bytes to 1452 bytes.

Ping Count : The count of the ICMP packet. Values range from 1 time to 60 times.

Ping Interval : The interval of the ICMP packet. Values range from 0 second to 30 seconds.

Egress Interface : The VLAN ID (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.

Start: Click the "Start" button then the switch will start to ping the device using ICMPv6 packet size what set on the switch. After you press Start, five ICMPv6 packets are transmitted, and the sequence number and roundtrip time are displayed upon reception of a reply. The page refreshes automatically until responses to all packets are received, or until a timeout occurs.

```
PING server 10.10.132.20
64 bytes from 10.10.132.20: icmp_seq=0, time=0ms
64 bytes from 10.10.132.20: icmp_seq=1, time=0ms
64 bytes from 10.10.132.20: icmp_seq=2, time=0ms
64 bytes from 10.10.132.20: icmp_seq=3, time=0ms
64 bytes from 10.10.132.20: icmp_seq=4, time=0ms
Sent 5 packets, received 5 OK, 0 bad
```

4-3 Cable Diagnostics

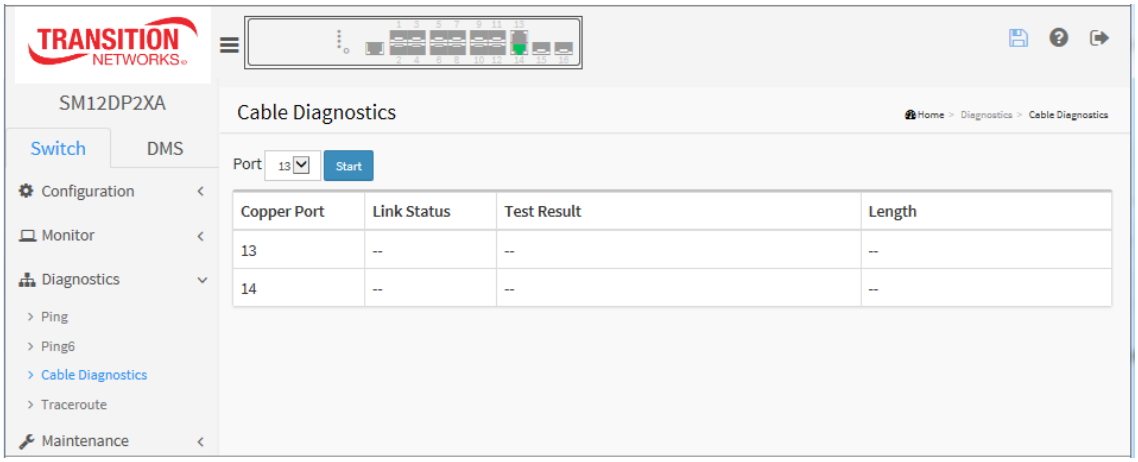
This page lets you run the built-in Cable Diagnostics. This will take approximately 5 - 15 seconds. When completed, the page refreshes automatically, and you can view the cable diagnostics results in the cable status table. Note that Cable Diagnostics is only accurate for cables of length 7 -140 meters. The 10 and 100 Mbps ports will be linked down while running Cable Diagnostics. Therefore, running Cable Diagnostics on a 10 or 100 Mbps management port will cause the switch to stop responding until Cable Diagnostics is complete.

Web Interface

To run a Cable Diagnostics in the web interface:

1. Specify the Port which you want to check.
2. Click Start.

Figure 4-3: Cable Diagnostics



Parameter descriptions:

Port : At the dropdown, select the port (13 or 14) to run the Cable Diagnostics.

Copper Port : Copper port number (13 or 14).

Link Status : The status of the cable.

10M: Cable is link up and correct. Speed is 10 Mbps.

100M: Cable is link up and correct. Speed is 100 Mbps.

1G : Cable is link up and correct. Speed is 1 Gbps.

10G : Cable is link up and correct. Speed is 10 Gbps.

Link Down: Link down or cable is not correct.

Cable Diagnostic is running...: the test is in progress.

Test Result: Test Result of the cable.

OK: Correctly terminated pair.

Abnormal: Incorrectly terminated pair or link down.

detect error or check cable length is between 7-120 meters

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.

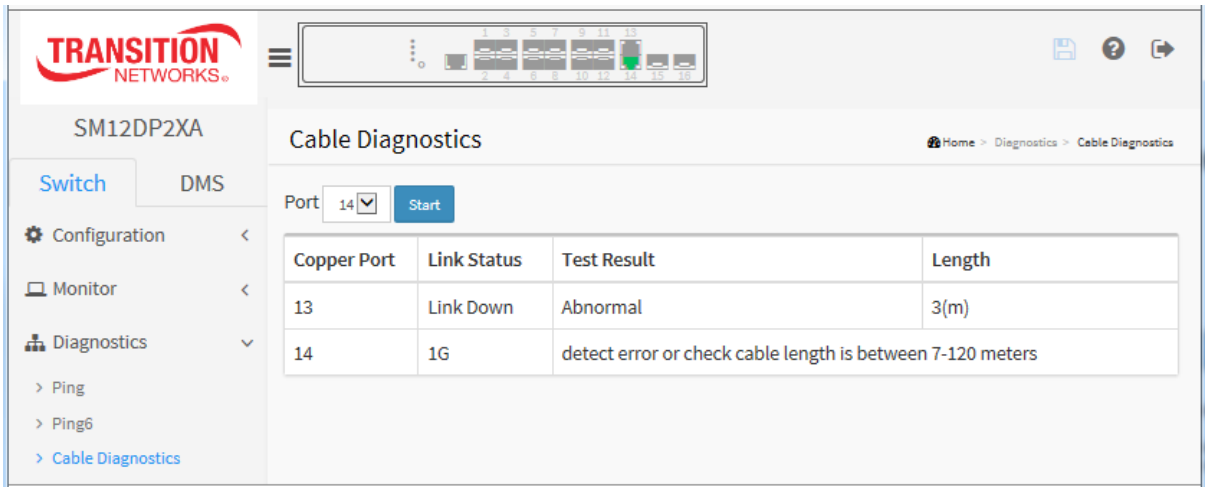
1G: The length is the minimum value of 4-pair.

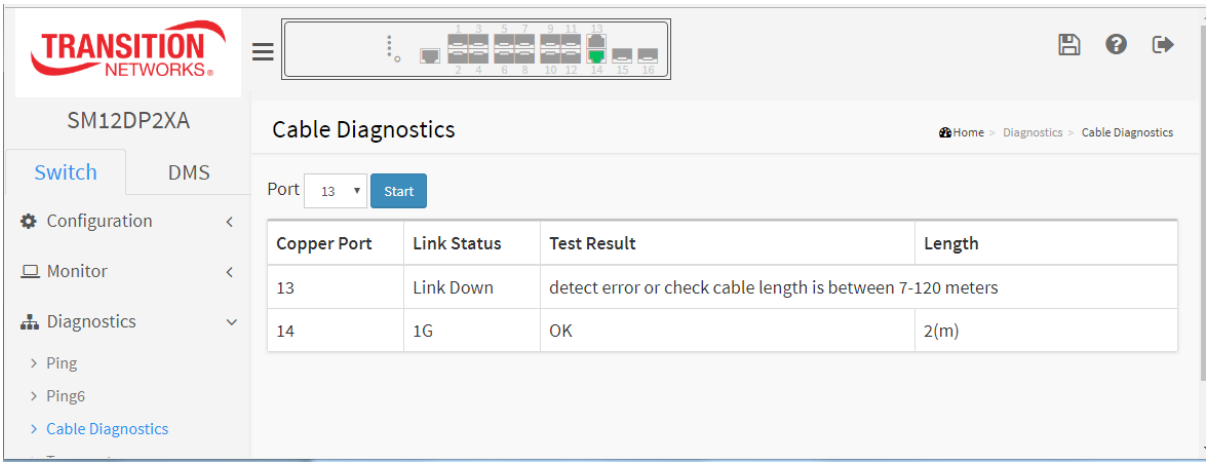
10M/100M: The length is the minimum value of 2-pair.

Link Down: The length is the minimum value of non-zero of 4-pair.

2(m): The length is OK at the length listed.

Sample completed cable diagnostics are shown below:





Message: *Cable Diagnostic is running…* displays while the diagnostic is running. No action required.

Message: *10 and 100 Mbps ports will be linked down and lost connection while running Cable Diagnostics.*
Are you sure you want to continue?
Note that Diagnostics is only accurate for cable of length 7-120 meters.
Recovery: Click the **OK** button to clear the webpage message and continue operation.

Message: *detect error or check cable length is between 7-12 meters*

4-4 Traceroute

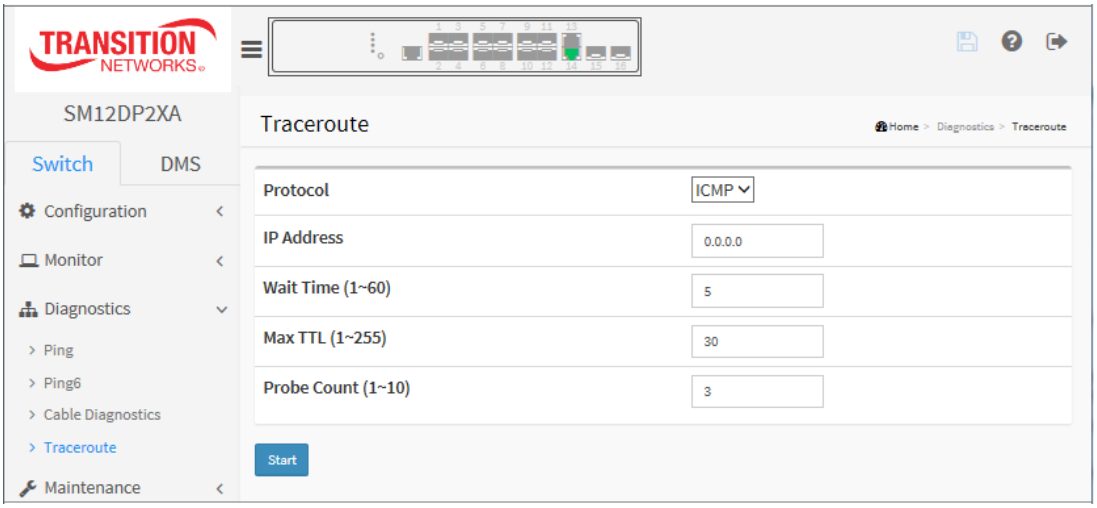
This page lets you issue ICMP, TCP, or UDP packets to diagnose network connectivity issues.

Web Interface

To configure an ICMPv6 PING Configuration in the web interface:

1. Specify traceroute IP Address.
2. Specify traceroute Size.
3. Click Start.

Figure 4-4: Traceroute



Parameter descriptions:

Protocol : Select the protocol (ICMP, UDP, 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). Values range from 1 to 60. The payload size of the ICMP packet. Valid values are 2 - 1452 bytes.

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. Values range from 1 to 10. The default is 3.

After you press **Start**, Traceroute sends packets with gradually increasing TTL value, starting with TTL value of 1. The first router receives the packet, decrements the TTL value and drops the packet because it then has TTL value zero. The router sends an ICMP Time Exceeded message back to the source. The next set of packets are given a TTL value of 2, so the first router forwards the packets, but the second router drops them and replies with ICMP Time Exceeded. Proceeding in this way, traceroute uses the returned ICMP Time Exceeded messages to build a list of routers that packets traverse, until the destination is reached and returns an ICMP Echo Reply message. For example:

```
traceroute to 202.39.253.11 (202.39.253.11), 30 hops max, 40 byte packets
1 192.168.10.254 ae-2-3508.edge4.Atlanta2.Level3.net. (192.168.10.254) 10 ms 10 ms 10 ms
2 59-125-13-254.HINET-IP.hinet.net. (59.125.13.254) 20 ms 20 ms 20 ms
3 h146.s228.ts.hinet.net. (168.95.228.146) 20 ms 10 ms 20 ms
4 tchn-3011.hinet.net. (220.128.16.194) 20 ms TCHN-3112.hinet.net. (220.128.17.142) 20 ms
tchn-3011.hinet.net. (220.128.16.202) 20 ms
5 TPDT-3012.hinet.net. (220.128.17.6) 20 ms TPDT-3011.hinet.net. (220.128.16.10) 20 ms TPDT-
3012.hinet.net. (220.128.17.6) 40 ms
```

```
6 CHCH-3112.hinet.net. (220.128.2.13) 20 ms tchn-3011.hinet.net. (220.128.1.9) 10 ms CHCH-
3112.hinet.net. (220.128.2.13) 30 ms
7 211.22.41.237 CHCH-3112.hinet.net. (211.22.41.237) 20 ms 30 ms 30 ms
8 202-39-253-11.HINET-IP.hinet.net. (202.39.253.11) 10 ms 10 ms
```

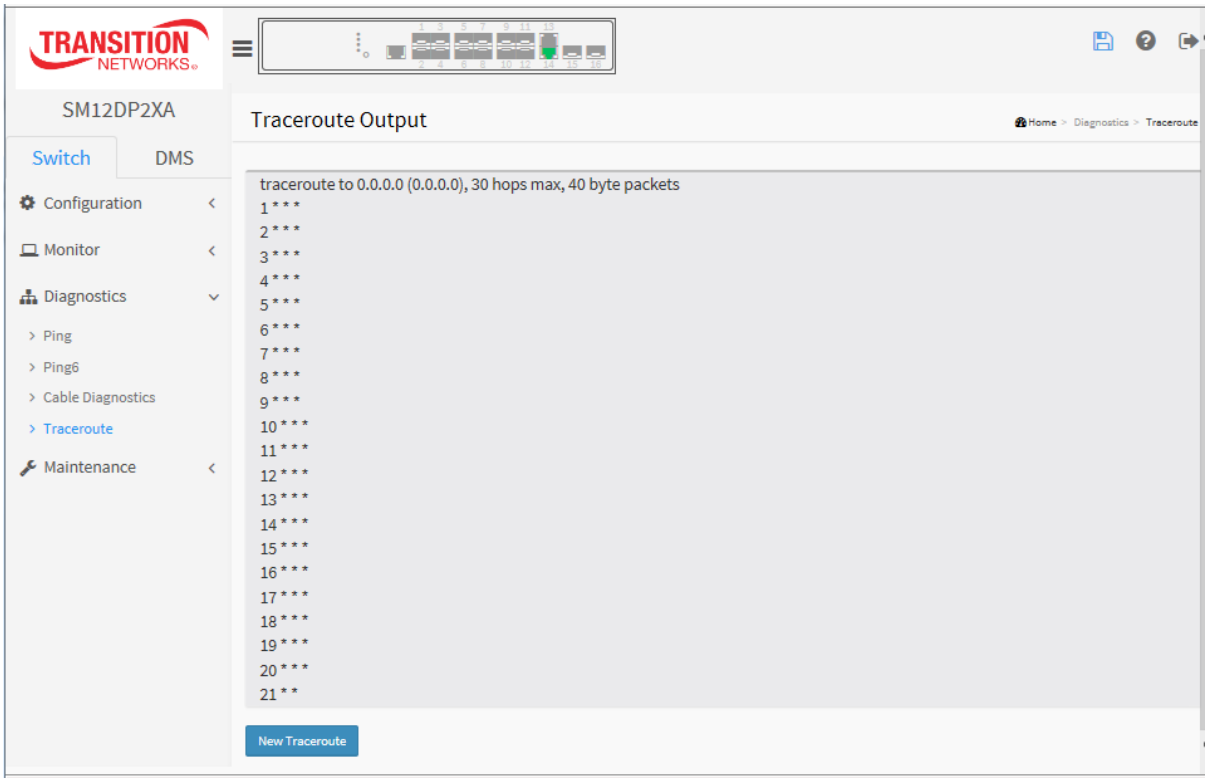
Buttons:

Start: Click to start transmitting ICMP packets.

New Traceroute: The button displays after a failed or successful Traceroute attempt to allow you to try another Traceroute with different parameters. Click to re-start diagnostics.

Message: *traceroute: unknown host 0.0.0.0192.168.1.77* displays if traceroute fails. Enter a different destination IP Address.

A successful Traceroute is shown below:



Chapter 5. Maintenance

This chapter describes the switch Maintenance configuration tasks to enhance the performance, including Restart Device, Firmware upgrade, Save/Restore, Import/Export.

5-1 Restart Device

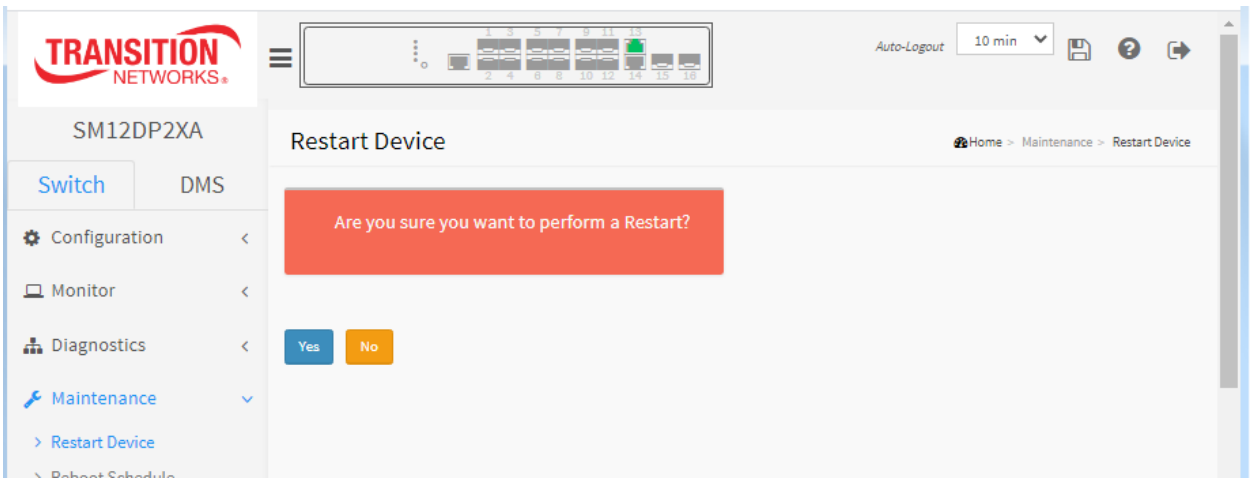
This page lets you restart the switch for maintenance needs. Any configuration files or scripts that you saved in the switch should still be available afterwards.

Web Interface

To perform a Restart Device in the web interface:

1. Click Restart Device.
2. Click Yes.

Figure 5-1: Restart Device



Buttons:

Yes : Click “Yes” and the device will restart.

No : Click to undo any restart action.

***Messages**:*

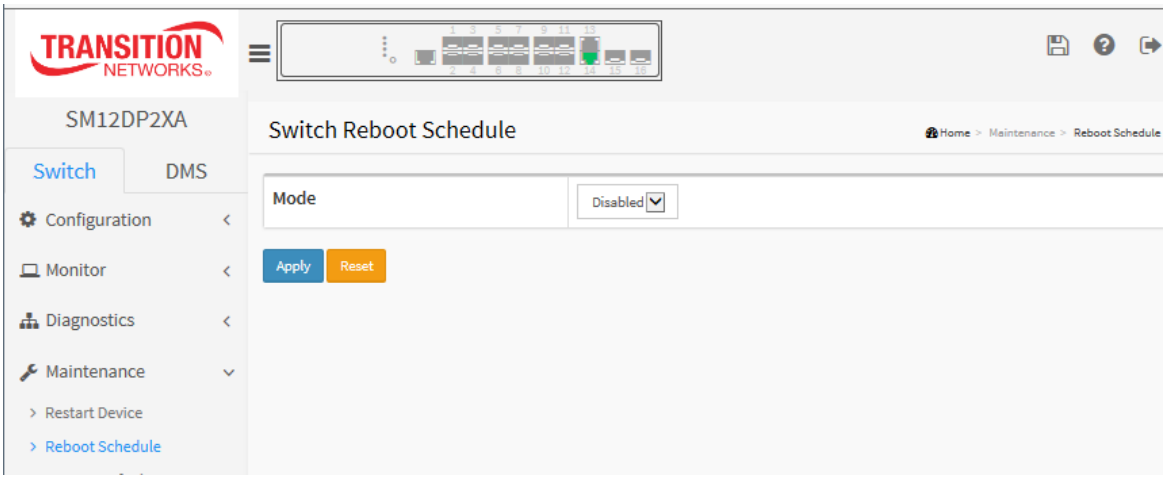
System restart is in progress… displays while the restart takes place. The login prompt then displays.

Are you sure you want to perform a Restart? displays so you can verify that you want to continue.

5-2 Reboot Schedule

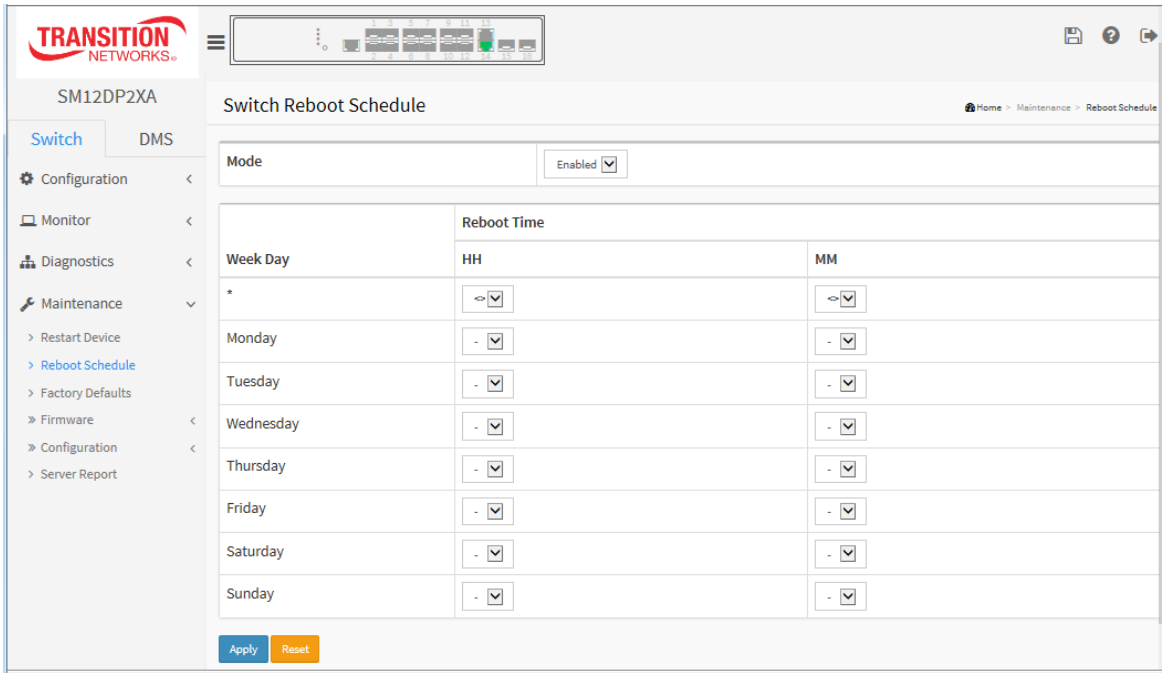
This page lets you schedule the time to reboot the switch from Maintenance > Reboot Schedule.

By default the Switch Reboot Schedule age displays with Mode Disabled.



1. At the default page, select **Enable**.

2. When the schedule page displays, enter the **Reboot Time** for the desired days.



3. Click the **Apply** button.

Mode : Indicates the reboot scheduling mode operation. Possible modes are:

Enabled: Enable switch reboot scheduling.

Disabled: Disable switch reboot scheduling.

Week Day: The day to reboot this switch.

Reboot Time: The time to reboot the switch (HH = Hour from 0-23) and MM = Minute from 0-55).

Buttons

Apply : Click to save changes.

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

5-3 Factory Defaults

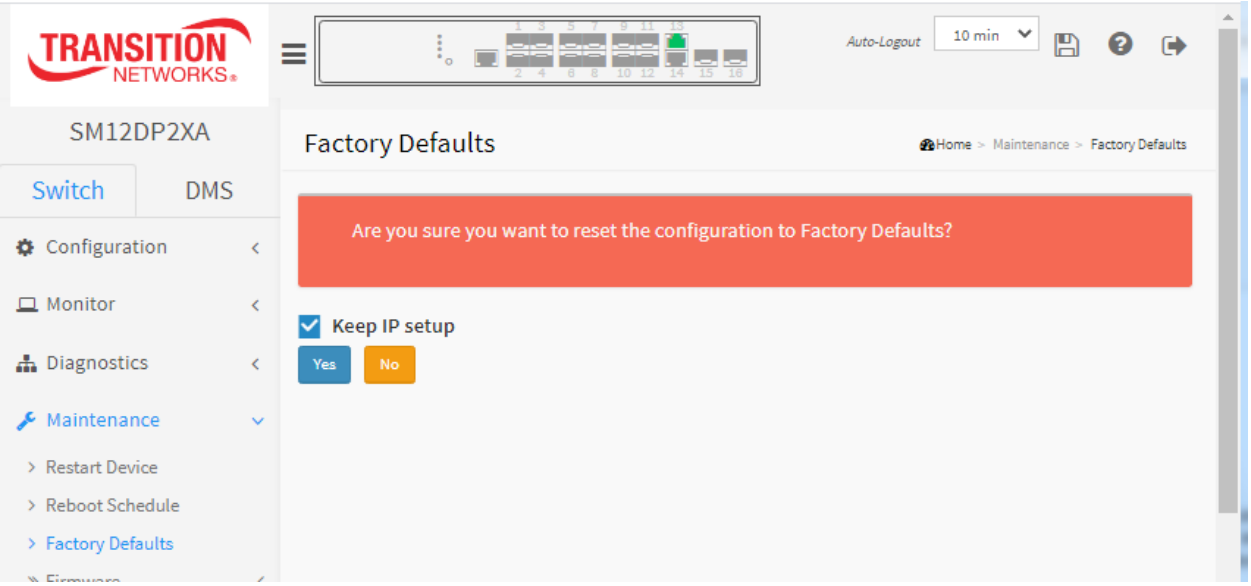
You can reset the configuration of the switch on this page. Any configuration files or scripts will recover to factory default values. Only the IP configuration is retained. The new configuration is available immediately, which means that no restart is necessary.

Web Interface

To configure a Factory Defaults Configuration in the web interface:

1. Click Maintenance, Factory Defaults.
2. Uncheck or check the Keep IP setup checkbox.
3. Click Yes.

Figure 5-3.1: Factory Defaults



Parameter descriptions:

Keep IP setup : Check "Keep IP setup" if you want to keep the current IP address settings.

Buttons:

Yes : Click to reset the configuration to Factory Defaults.

No : Click to return to Monitor > System > Information without resetting the configuration.

Note: Restoring factory default can also be performed by making a physical loopback between port 1 and port 2 within the first minute from switch reboot. In the first minute after boot, 'loopback' packets will be transmitted at port 1. If a 'loopback' packet is received at port 2 the switch will do a restore to default.

5-4 Firmware

This page lets you upgrade switch Firmware. The switch can be enhanced with value-added functions by installing firmware upgrades. For Transition Networks Firmware, etc. go to the Product Support webpage (logon required).

5-4.1 Firmware upgrade

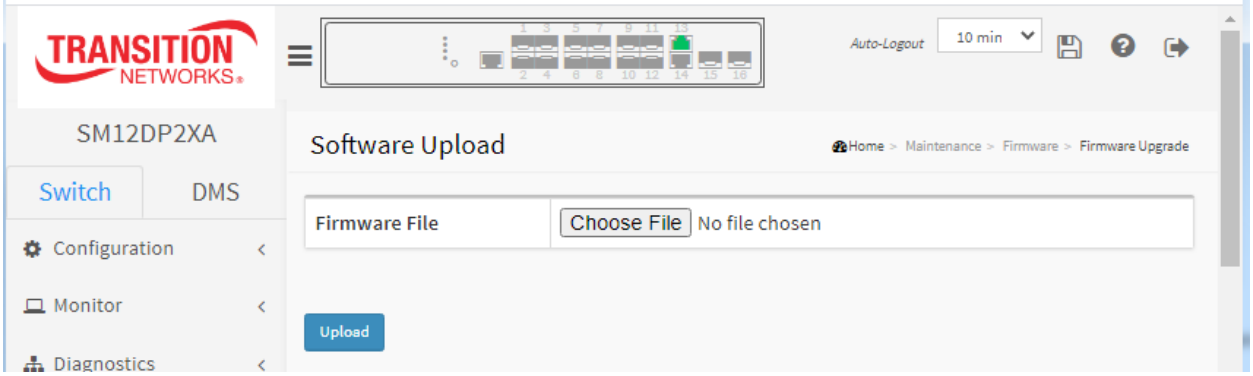
This page facilitates an update of the firmware controlling the switch.

Web Interface

To perform a Firmware Upgrade via the web UI:

1. Click Maintenance > Firmware > Firmware Upgrade to display the Software Upload page.
2. Click Browse… to browse to and select a Firmware File, then click Open.
3. Check the Force Cool Restart checkbox if desired.
4. Click the Upload button.

Figure 5-4.1 Software Upload



Parameter descriptions:

Browse : Click the "**Browse...**" button to search the Firmware URL and filename. **Browse** to the location of a software image and click Open, then click **Upload**.

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 all managed switches restart. 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:

Invalid Firmware Image The uploaded firmware image is invalid. Please use a correct firmware image. displays if you selected an invalid firmware file / format.

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.

5-3.2 Firmware Selection

This page provides information about the active and alternate (backup) firmware images in the device, and allows you to revert to the alternate image. The web page displays two tables with information about the active and alternate firmware images.

Note:

1. If the active firmware image is the alternate image, only the "Active Image" table is shown. In this case, the Activate Alternate Image button is disabled.
2. If the alternate image is active (due to a corruption of the primary image or manual intervention), uploading a new firmware image to the device will automatically use the primary image slot and activate this.
3. The firmware version and date information may be empty for older firmware releases. This does not constitute an error.

Web Interface

To configure a Firmware Upgrade Configuration in the web interface:

1. Navigate to Maintenance > Firmware > Firmware Selection.
2. Click Activate Alternate Image.

Figure 5-3.2 Firmware Selection

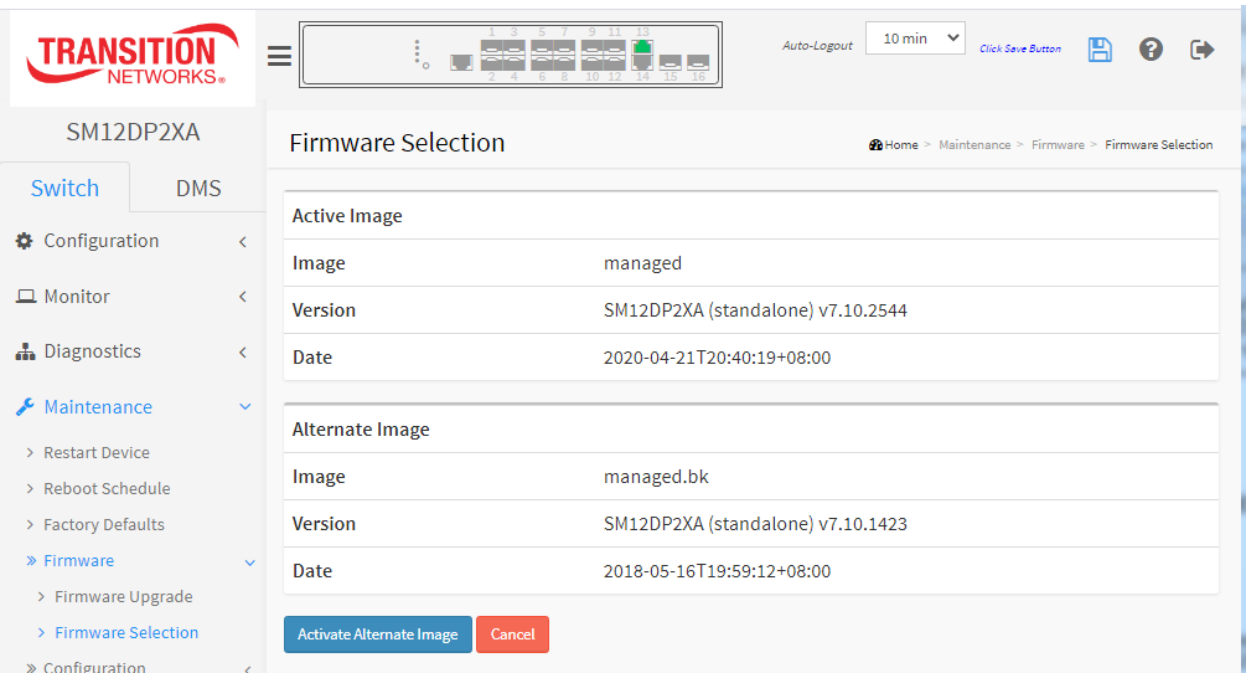


Image Information

Image : The flash index name of the firmware image. The name of primary (preferred) image is *managed*, the alternate image is named *managed.bk*.

Version : The version of the firmware image (e.g., *SM12DP2XA (standalone) v7.10.2544*).

Date : The date where the firmware was produced, in the format *2020-04-21T20:40:19+08:00*.

Buttons

Activate Alternate Image: Click to use the “Alternate Image” if one exists. This button may be disabled depending on system state. This button is inactive if no alternate image exists.

Cancel: Cancel activating the backup image. Navigates away from this page.

5-5 Configuration

The switch stores its configuration in a number of text files in CLI format. The files are either virtual (RAM-based) or stored in flash on the switch. There are three system files:

running-config: A virtual file that represents the currently active configuration on the switch. This file is volatile.

startup-config: The startup configuration for the switch, read at boot time.

default-config: A read-only file with vendor-specific configuration. This file is read when the system is restored to default settings. The default configuration file is read and applied immediately after the system configuration is reset to default. The file is read-only and cannot be modified.

It is also possible to store up to two other files and apply them to running-config, thereby switching configuration. **Note**: The generation of the configuration file may be time consuming, depending on the amount of non-default configuration.

5-5.1 Save startup-config

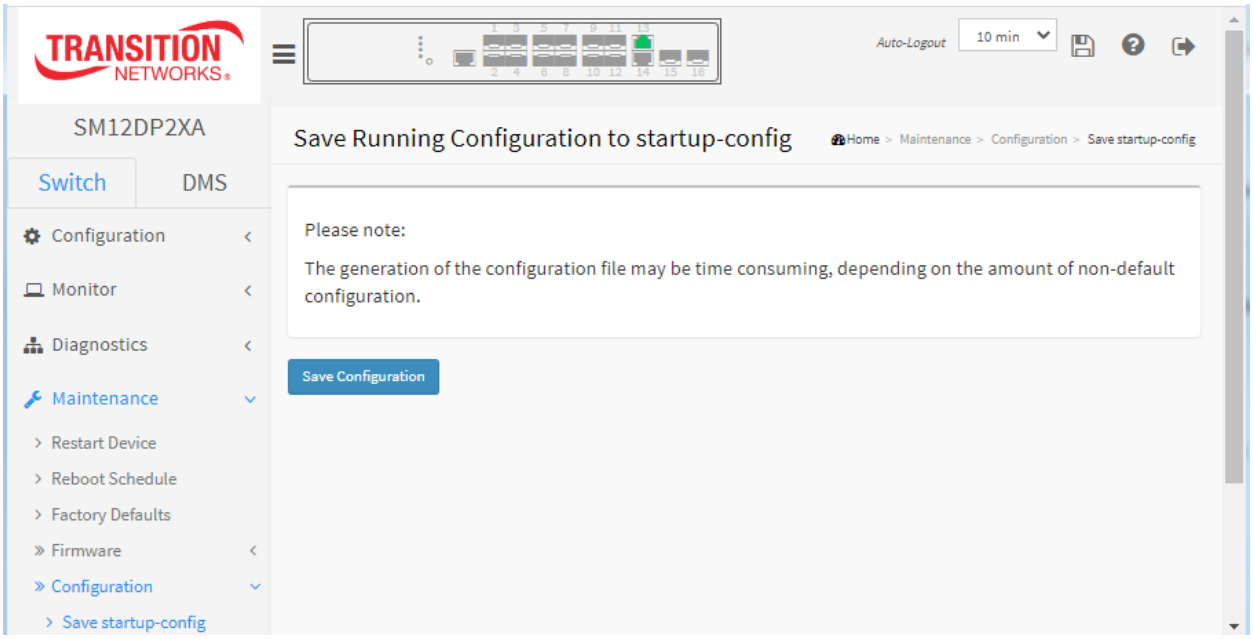
This will copy running-config to startup-config, thereby ensuring that the currently active configuration will be used at the next reboot.

Web Interface

To save the running configuration in the web interface:

1. Click Maintenance, Configuration, Save startup-config.
2. Click Save Configuration. If successful, the message "*Save Running Configuration to startup-config startup-config saved successfully.*" displays.

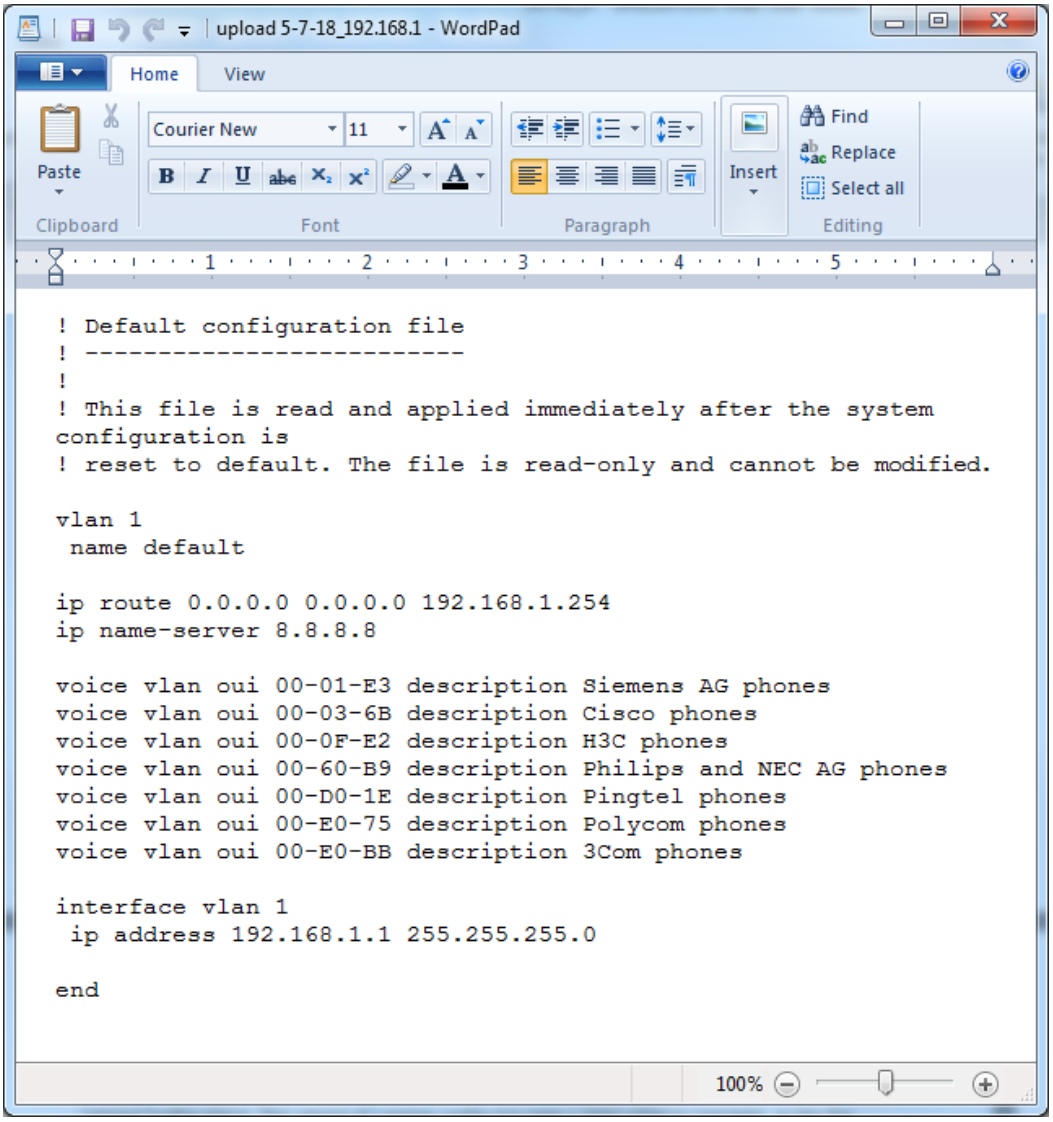
Figure 5-5.1: Save Running Configuration to startup-config



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.

A sample default-config file is shown below:



The basic default-config content is shown below:

```
! Default configuration file
! --------------------------
!
! This file is read and applied immediately after the system configuration is
! reset to default. The file is read-only and cannot be modified.

vlan 1
 name default

ip route 0.0.0.0 0.0.0.0 192.168.1.254
ip name-server 8.8.8.8

voice vlan oui 00-01-E3 description Siemens AG phones
voice vlan oui 00-03-6B description Cisco phones
voice vlan oui 00-0F-E2 description H3C phones
voice vlan oui 00-60-B9 description Philips and NEC AG phones
voice vlan oui 00-D0-1E description Pingtel phones
voice vlan oui 00-E0-75 description Polycom phones
voice vlan oui 00-E0-BB description 3Com phones

interface vlan 1
 ip address 192.168.1.1 255.255.255.0

end
```

A sample running-config file is shown below:

```
hostname SM12DP2XA
username admin privilege 15 password encrypted YWRtaW4=
!
vlan 1
!
!
!
!
ip route 0.0.0.0 0.0.0.0 192.168.1.254
tzidx 0
system name SM12DP2XA
system description Managed Switch, (12) 100/1000Base-X SFP ports
+ (2) 1G/10G SFP+ with (2) 10/100/1000Base-T
!
interface GigabitEthernet 1/1
 flowcontrol on
!
interface GigabitEthernet 1/2
!
interface GigabitEthernet 1/3
!
interface GigabitEthernet 1/4
!
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
 flowcontrol on
!
interface 10GigabitEthernet 1/1
!
interface 10GigabitEthernet 1/2
!
interface vlan 1
 ip address 192.168.1.77 255.255.255.0
!
```

5-5.2 Upload

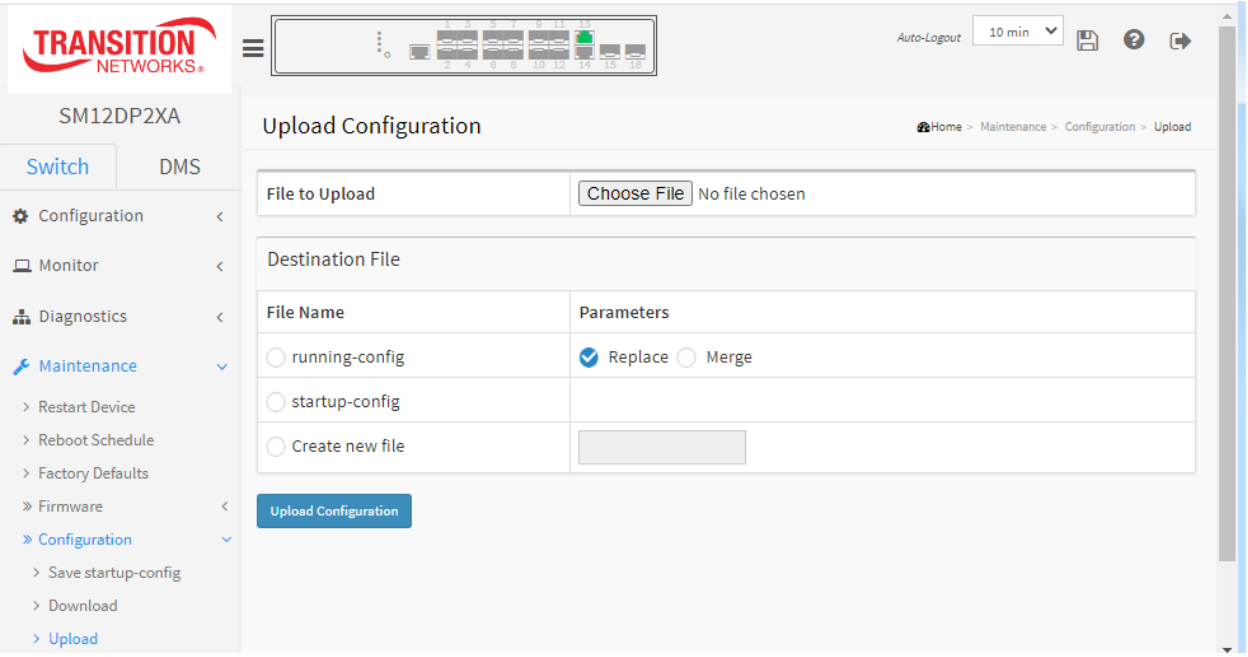
It is possible to upload any of the files on the switch to the web browser. Select the file and click Upload Configuration. The upload of running-config may take a little while to complete, as the file must be prepared for upload. If the flash file system is full (i.e., contains default-config and 100 other files, usually including startup-config), it is not possible to create new files. Instead an existing file must be overwritten or another file must be deleted.

Web Interface

To upload configuration in the web interface:

1. Click Maintenance > Configuration > Upload.
2. Browse to and select the file to upload.
3. Select the destination file name.
4. Click Upload Configuration. If successful, the message "*Upload successfully completed.*" displays.

Figure 5-5.2: Upload Configuration



Parameter descriptions:

File to Upload : Click the **Browse…** button and select the desired file.

File Name: Select one of the three system files:

running-config: A volatile file representing the currently active switch configuration.

startup-config: The startup configuration for the switch, read at boot time.

Create new file: You can create up to 99 other files, typically used for configuration backups or alternative configurations.

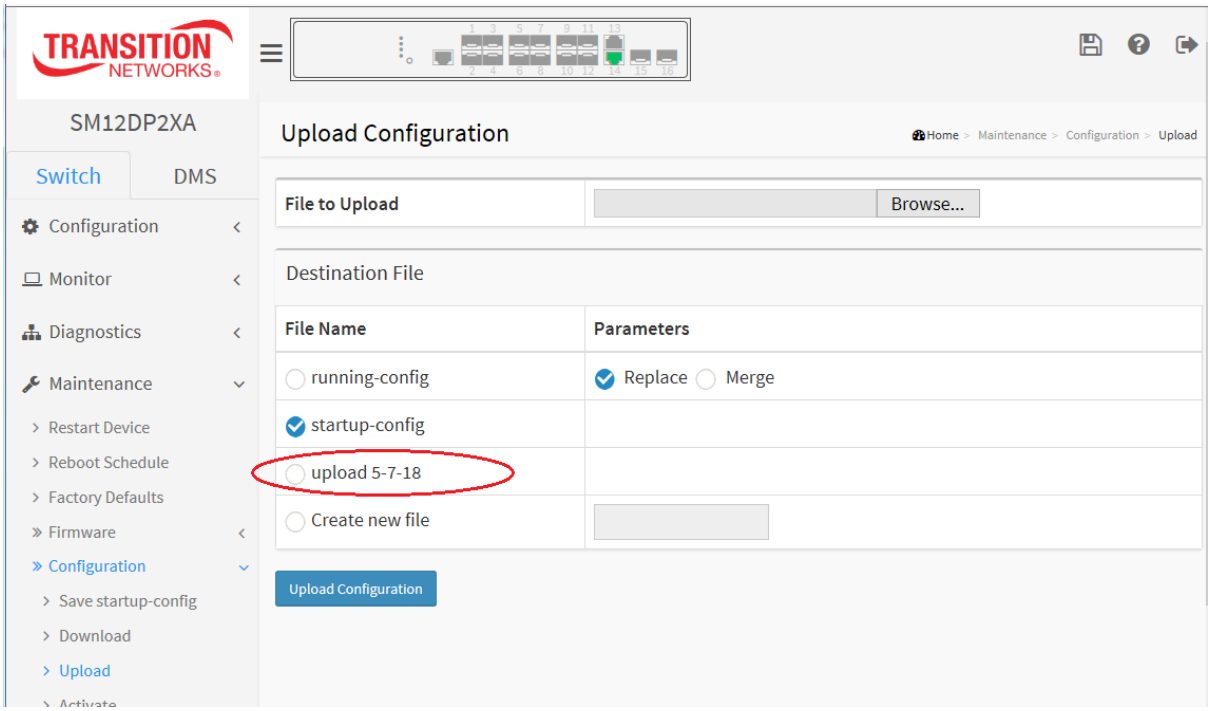
Parameters: Select ***Replace*** or ***Merge***. If the destination is running-config, the file will be applied to the switch configuration. This can be done in two ways:

Replace mode: The current configuration is fully replaced with the configuration in the uploaded file.

Merge mode: The uploaded file is merged into running-config.

Buttons:

Upload Configuration: Click the button then the running web management PC will start to upload the configuration from the managed switch configuration into the specified PC location and display it on the page. In the example below, the file “upload 5-7-18” was uploaded.



5-5.3 Download

This page lets you export the switch configuration for maintenance needs. Any current configuration files will be exported in text format.

It is possible to download a file from the web browser to all the files on the switch, except default-config, which is read-only.

Select the file to download, select the destination file on the target, then click Download Configuration.

If the destination is running-config, the file is applied to the switch config in one of two ways:

Replace mode: The current config is fully replaced with the config in the downloaded file.

Merge mode: The downloaded file is merged into running-config.

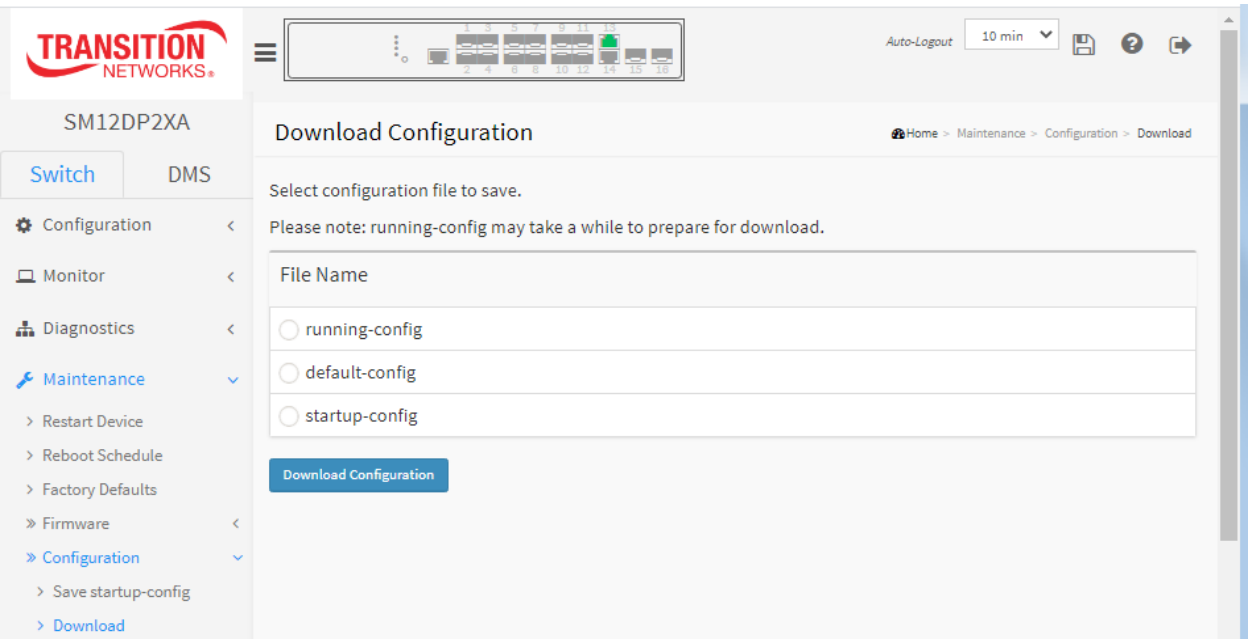
If the file system is full (i.e. contains the three system files mentioned above plus two other files), it will not be possible to create new files, but an existing file must be overwritten or another deleted first. **Note**: running-config may take a while to prepare for download.

Web Interface

To download configuration in the web interface:

1. Click Maintenance > Configuration > Download.
2. Select the configuration file to save.
3. Click Download Configuration.

Figure 5-5.3: Configuration Download

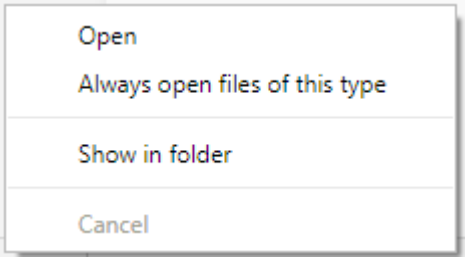


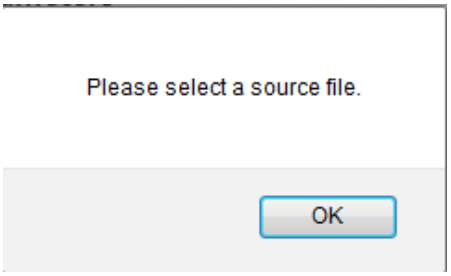
Parameter descriptions:

File Name : Select which configuration file to save (running-config, default-config, or startup-config).

Download Configuration: Click the button then the switch will start to download the configuration from stored location on the PC or Server. A webpage message displays, giving you options to open or save the downloaded file. Select the desired option (typically “Save” or “Save as”).

Examples of various options to open or save the downloaded file:





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. The previous configuration will be completely replaced, potentially leading to loss of management connectivity.

Note: The activated configuration file will NOT be saved to startup-config automatically.

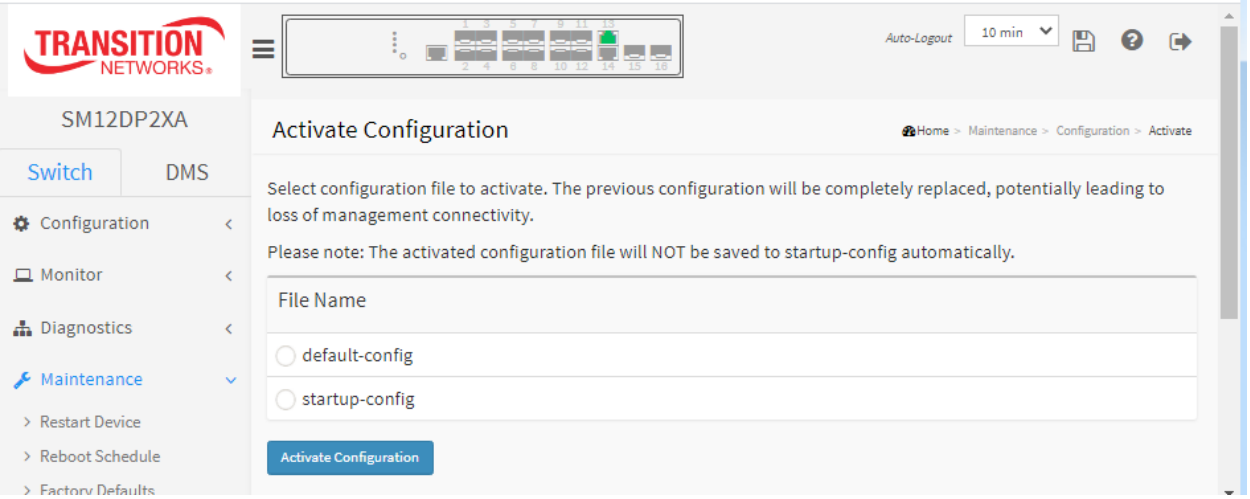
Note: If the configuration changes the IP settings, management connectivity may be lost.

Web Interface

To activate a configuration in the web interface:

1. Click Maintenance > Configuration > Activate.
2. Select the configuration file to activate.
3. Click Activate Configuration.

Figure 5-5.4: Activation Configuration



Parameter descriptions:

File Name: There are two system files:

default-config: A read-only file with vendor-specific information. This file is read when the system is restored to default settings.

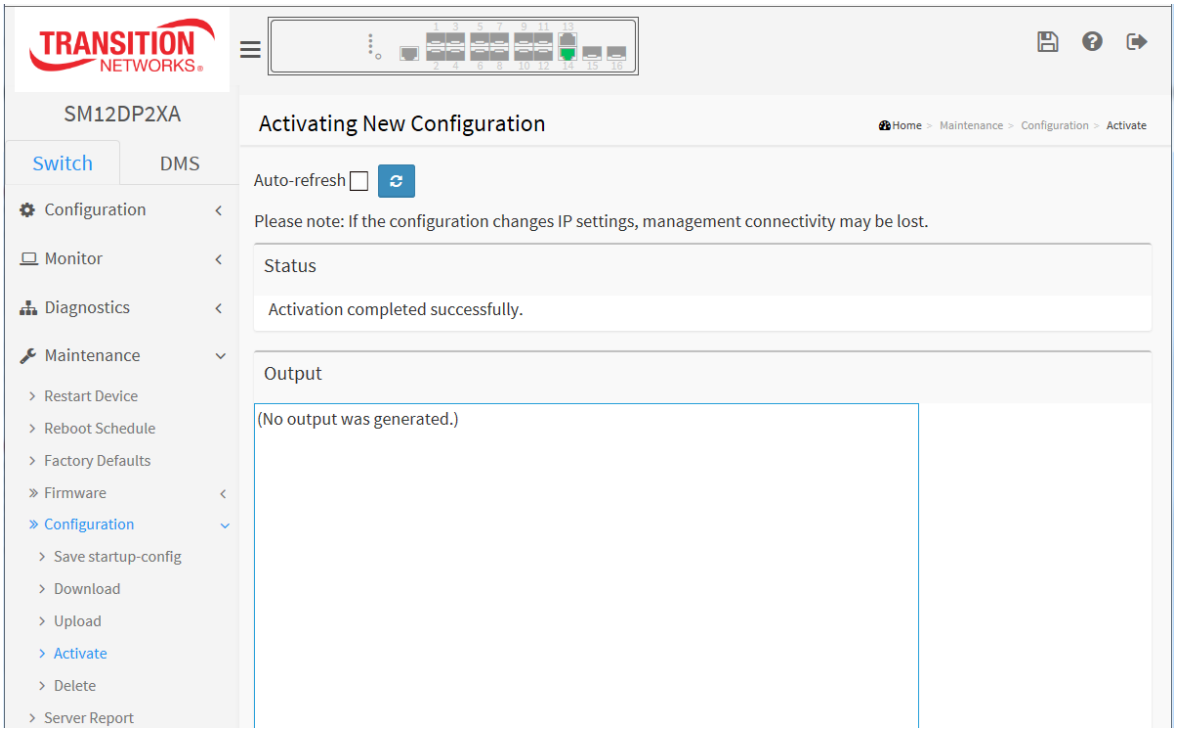
startup-config: The startup configuration for the switch, read at boot time.

Buttons :

Activate Configuration: Click the button then the selected file will be activated and will become this switch's running configuration.

If the Activation was successful, the page displays "***Status**: Activation completed successfully*.".

If the Activation was not successful, the page displays "***Output**: (No output was generated*.)".



5-5.5 Delete

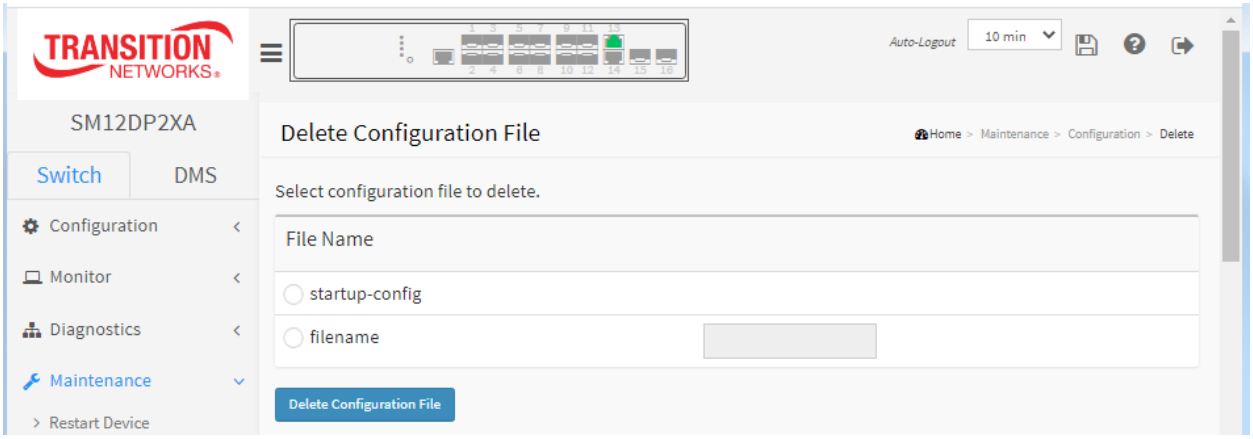
It is possible to delete any of the writable files stored in flash, including startup-config. If this is done and the switch is rebooted without a prior Save operation, this effectively resets the switch to its default configuration.

Web Interface

To delete configuration in the web interface:

1. Click Maintenance > Configuration > Activate.
2. Select the configuration file to delete.
3. Click Activate Configuration.

Figure 5-5.5: Delete Configuration File



Parameter descriptions:

File Name: There is one system file and one optional file entry:

startup-config: The startup configuration for the switch, read at boot time.

filename: Click the radio button and enter the name of the file to be deleted.

Buttons :

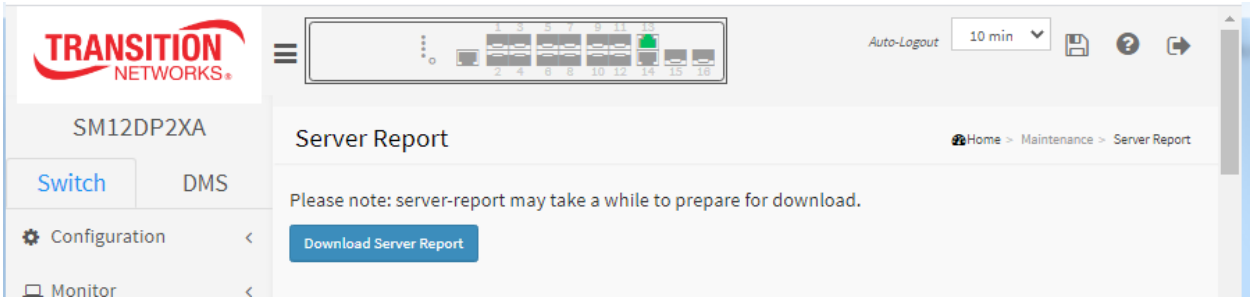
Delete Configuration: Click the button then the startup-config or selected file will be deleted.

Messages: *Are you sure you want to delete <filename>?*

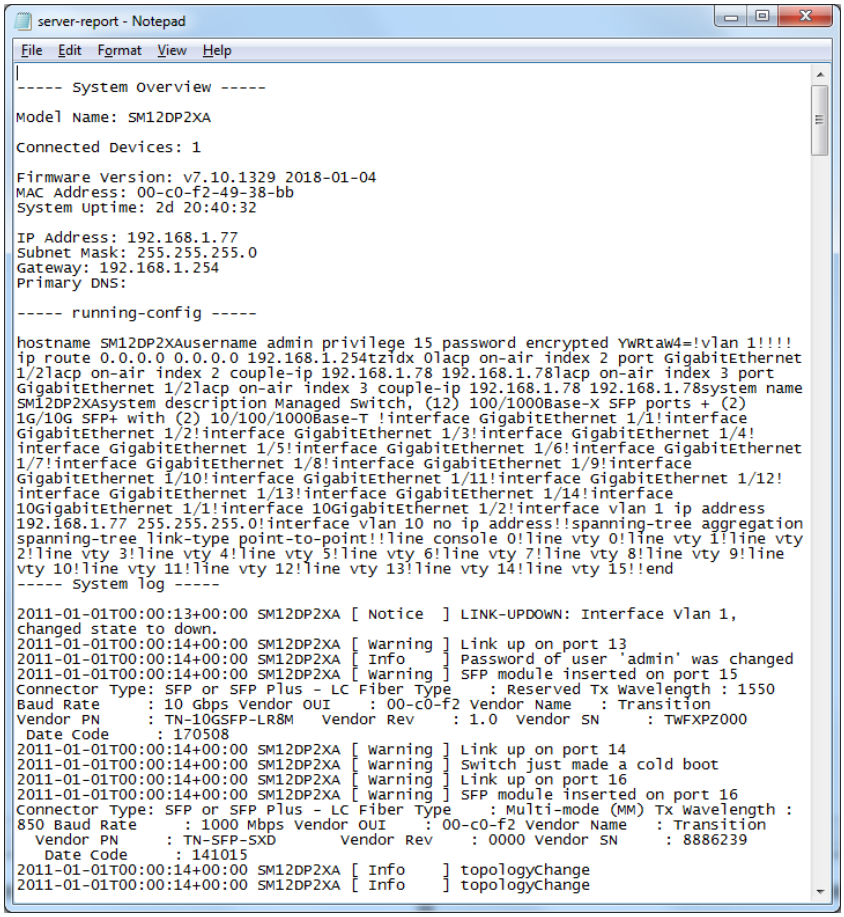
5-6 Server Report

This page lets you download a server report file on the switch to the web browser.

1. Select Maintenance > Server Report.
2. Click the Download Server Report button.
3. At the prompt "*Do you want to open or save …*" select Open, Save, Save as, Save and open, or Cancel. **Note**: The server report may take a while to prepare for download.



4. View the Server Report.



The Server Report provides a text file with System Overview, running-config, System log, System info, Port status, and Port statistics.

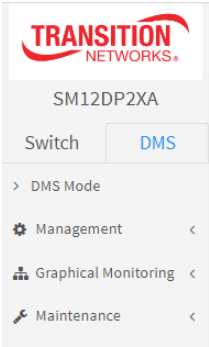
Messages:


Do you want to open or save server-report.txt (40.8 KB) from 192.168.1.77?
Open
Save
Cancel

or


server-report (1).txt
Show all

Chapter 6. DMS



The DMS tab provides the Management, Graphical Monitoring, and Maintenance sub-tabs as described in the following sections.

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:

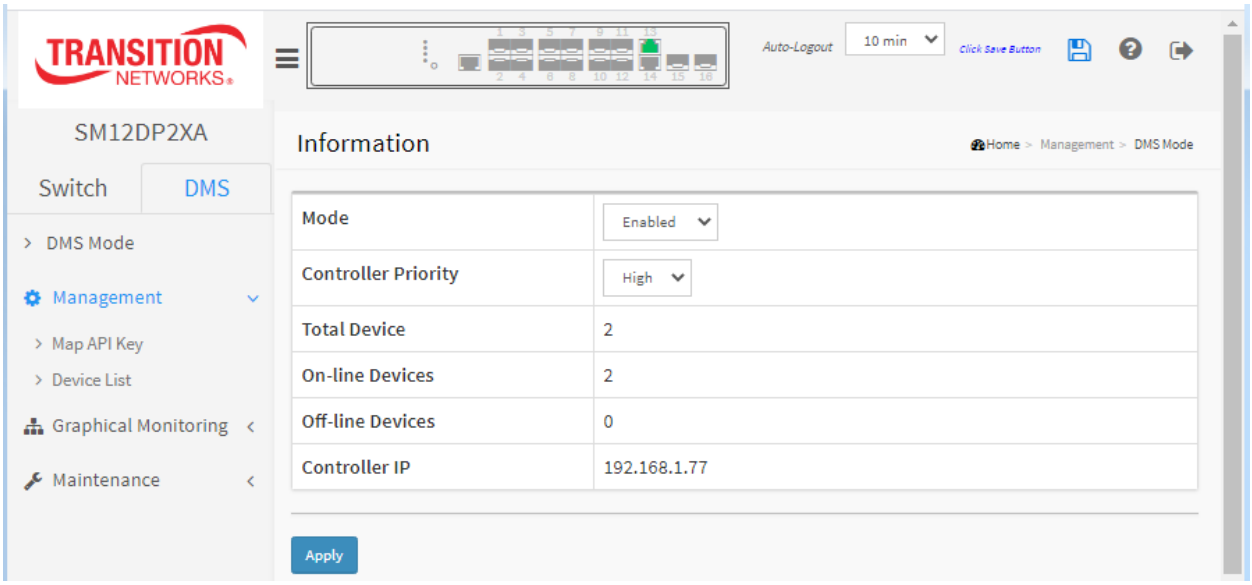
- Power down the IP cameras, NVRs, or any PoE devices.
- Remotely identify the exact cable break location.
- Detect abnormal traffic issues on IP cameras/NVR.
- Monitor devices' status (e.g., link up, PoE power, traffic, etc.).
- Configure VLAN/QoS intuitively for better solution quality/reliability.

6-1 DMS > DMS Mode

At DMS > DMS Mode you can select DMS Mode information parameters.

6-1.1 DMS > DMS Mode

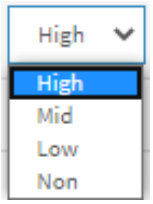
The DMS Information table, displayed at the DMS > Management > DMS Mode menu path, provides DMS Mode selection and displays device information.



Parameter descriptions:

Mode: Enable or Disable the DMS function on this switch. The default is Enabled.

Controller Priority: Choose "Controller Priority" when DMS is enabled:



High: This switch will become the Master (Controller) switch.

Mid: Middle level priority.

Low: Low level priority (default).

Non: If you choose "None", this switch will never become the Master (Controller) switch.

Total Device: Displays the total number of IP devices discovered and displayed in Topology view.

On-Line Devices: Displays the number of IP devices that are on-line in Topology view.

Off-Line Devices: Displays the number of IP devices that are off-line in Topology view.

Controller IP: Displays the Master (Controller) switch's IP address. If there are more than two Switches set as High-priority or no High-priority mode switch, the switch with the longer system uptime will be selected as the DMS Controller switch. If two Switches have same up time, the Switch with the smaller MAC address will be assigned as the DMS Controller 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. When enabled DHCP Server mode in DMS network, the DMS Controller switch will be responsible for assigning IP address for all devices. The DMS Controller Switch will collect, poll, and sync DMS information, and act as the Event Notification control center to manage all device information.

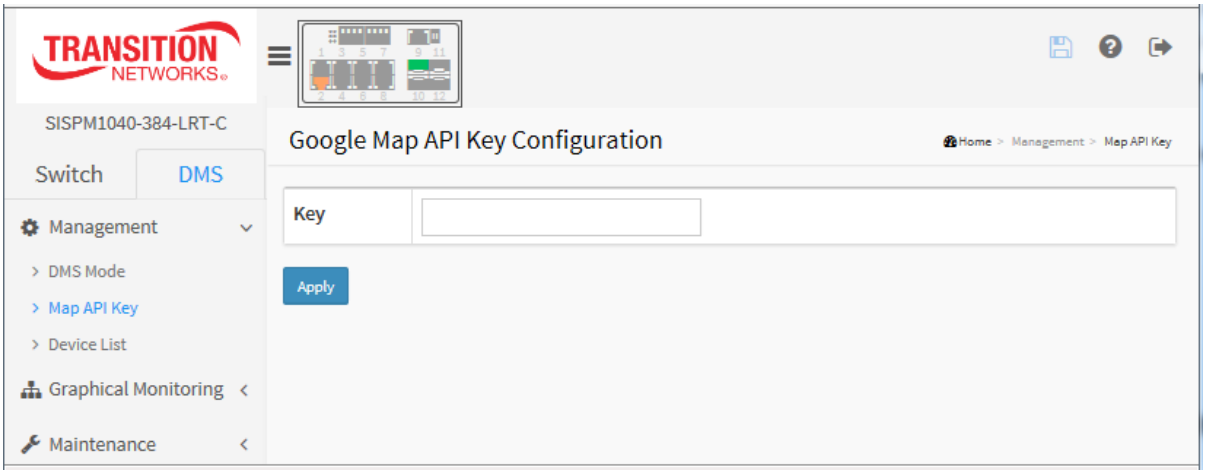
Buttons

Apply: Click to save changes.

6-1.2 Map API Key

You need a valid API key and a Google Cloud Platform billing account to access Google product. If no key is entered, DMS Map View will not be able to load Google Maps correctly. See the Google website and follow the steps to get an API key:
https://developers.google.com/maps/documentation/directions/get-api-key

6.6.1 Google Map API Key Configuration



Parameters:

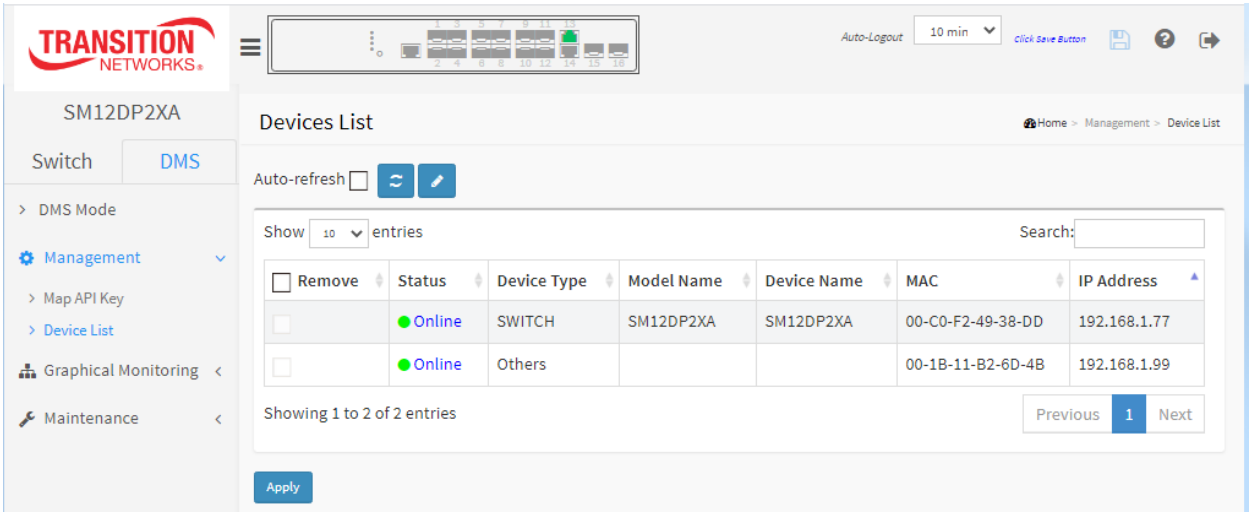
Key : Specify the Google Map API Key.

Buttons

Apply: Click to save changes.

6-1.2 DMS > Management > Device List

This page provides an overview of the DMS devices in the Devices List table. By default seven coulumns display:



Parameter descriptions:

Remove: Check to remove off-line device from the list.

Status: Device is Online or Offline. You can click on the linked Online Status column in a row to go to the DMS > Maintenance > Diagnostics page.

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

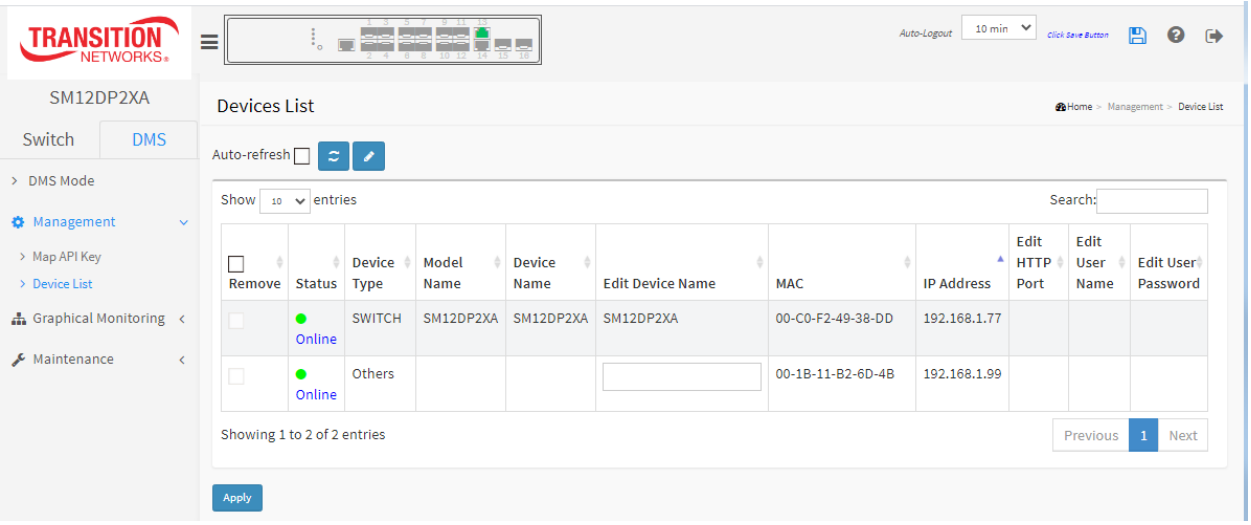
Auto-refresh: Check this box to refresh the page automatically every 3 seconds.

 Refresh: Click to refresh the displayed table starting from the input fields.

 : Click to add an input field for editing the device names and the http ports.

Apply: Click to save changes.

Example: Click the Edit button to display additional columns:



Additional Parameters:

Edit Device Name: Entry field for changing the current device name.

Edit HTTP Port: Entry field for changing the current HTTP port number.

Edit User Name: Entry field for changing the current login Username.

Edit User Password: Entry field for changing the current login password.

6-2 DMS > Graphical Monitoring

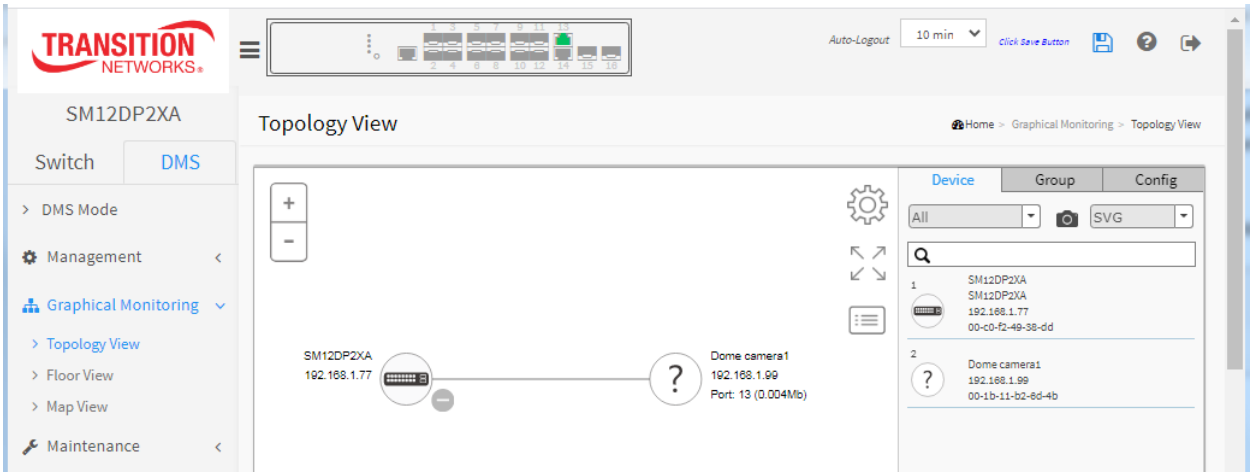
At DMS > Graphical Monitoring you can select Topology View, Floor View, or Map View submenus.

6-2.1 DMS > Graphical Monitoring > Topology View

DMS can automatically discover all IP devices and display the devices by graphic networking topology view.

You can manage and monitor them by the Topology View, such as to remotely diagnose cable connection status, auto alarm notifications on critical events, remotely reboot PoE device when it's not alive. Therefore, you can apply DMS platform to solve abnormal issues anytime and anywhere via tablet or smart phone to keep the network running smoothly.

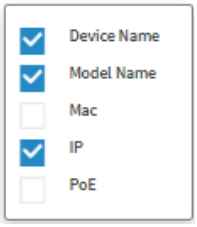
Click **Graphical Monitoring** -> **Topology View** to view the network topology.



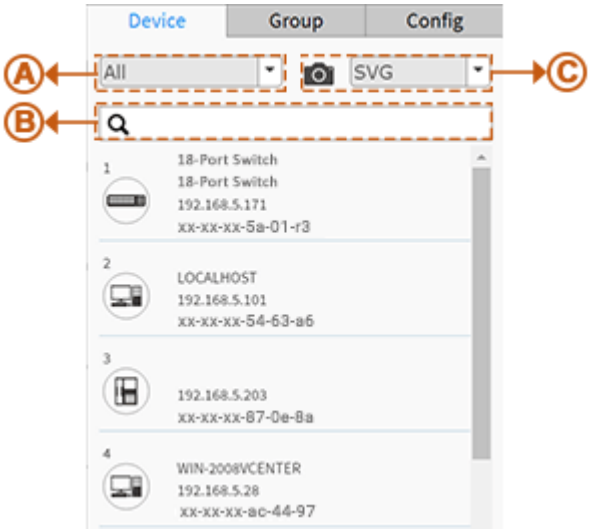
Plus and minus icons: Zoom in and zoom out of Topology view; you can scroll up/down you're your mouse to achieve the same purpose.

In the upper right corner, there is a "Setting icon". When user clicks the icon, it will pop-up Device, Group, Config, export topology view and advanced search functions for the topology.

Click to display a pop-up that lets you select which parameters to display for each device icon. Select three of the five parameters available: Device Name, Model Name, Mac, IP, and/or PoE.

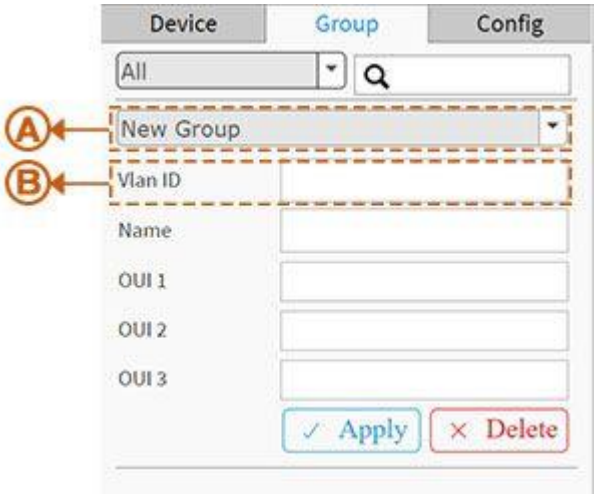


Device Search Console



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

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.

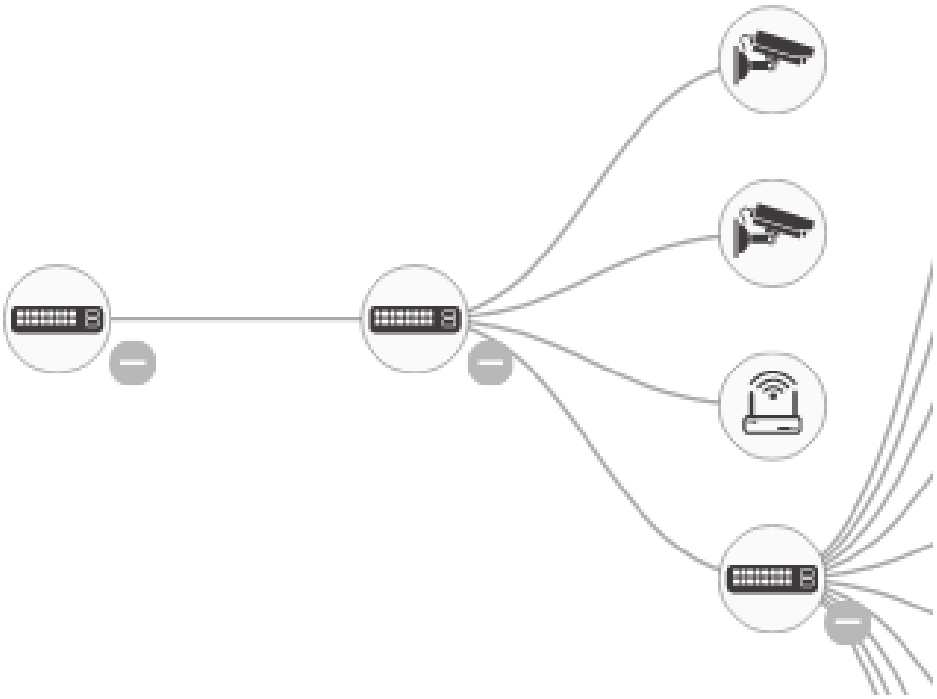
System Setting Console

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 will suggest user to adjust 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 Topology or return to the Normal View.


Icon with information list: You can select the kind of information to be shown on the topology view of each device. Up to 3 items can be selected.

Device Tree View



Device categories

The full set of Device Types includes PC (General PC), IP Camera (General IP Camera), IP Phone General IP Phone or Cisco SPA303), AP (General AP), Others (Mobile Device, General Switch, Internet Gateway, IP PBX, NAS, Printer, NVR, VMS, Unknown Device). The device type icons are described below:

 means the device is a Switch.

 means the device is a PC.

 means the device is an IP Camera.

 means the device is an IP Phone.

 means the device is an AP (Wireless Access Point or WAP).

 means the device is a Router.

 Icon with question mark means the IP device is detected by DMS, but the device type can't be recognized which will be classified as an unknown device type.

Device Status

 Icon with black mark: Device link up. Select a function and check issues.

 Icon with red mark: Device link down. Diagnose the link status.

 Icon with numbers: Indicates some events occurred (e.g. Device Off-line, IP Duplicate...etc.) on the IP device; click on the device icon to check events in Notification.

Device consoles

Left-click any device icon to display the device consoles for further actions:

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: Can be displayed 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 such as "*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: Click the Icon to log in the device via http for further configuration or status monitoring.

Upgrade: Click it to upgrade software version.

Find Switch: When this feature is activated, the front panel LEDs will flash for 15 seconds.

Diagnostics: Click to perform the cable diagnostics, to exam where the broken cable is, and, check if the device connection is alive or not by ping.

Cable Status:

-**Green icon:** Cable is connected correctly.

-**Red icon:** Cable is not connected correctly. You can check the distance info (XX meters) to identify the broken cable location.

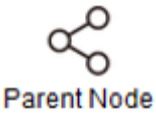
Connection:

-**Green icon:** Device is pinged correctly.

-**Red icon:** Device is not transmitting /receiving data correctly, which means it might not be pinging successfully.

Reboot: Click to reboot the device remotely so as recover the device back to its normal operation.

Streaming: Click to display the video images streaming, if the device supports this feature.



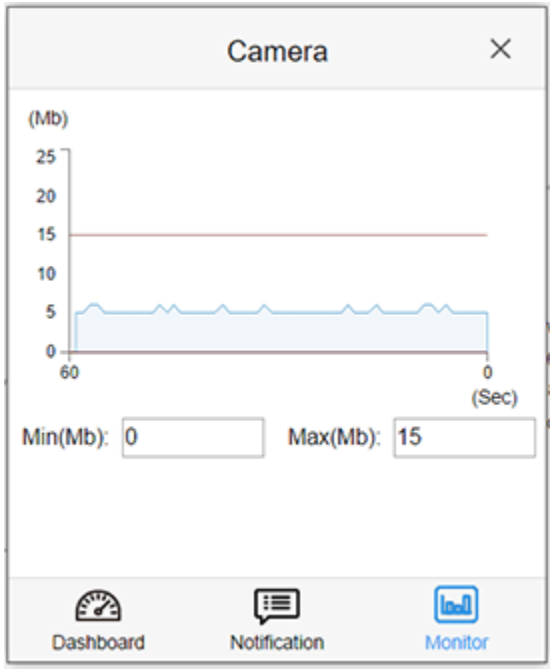
Parent Node: When DMS switch detects more than two IP devices from the same port, the switch can't resolve this IP device's layout, instead, it will show a blank node to present this situation. You can use the "Parent Node" function to adjust the Dashboard layout.

PoE Config: Click 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.

Monitor Console: Displays the traffics for device health check purpose.

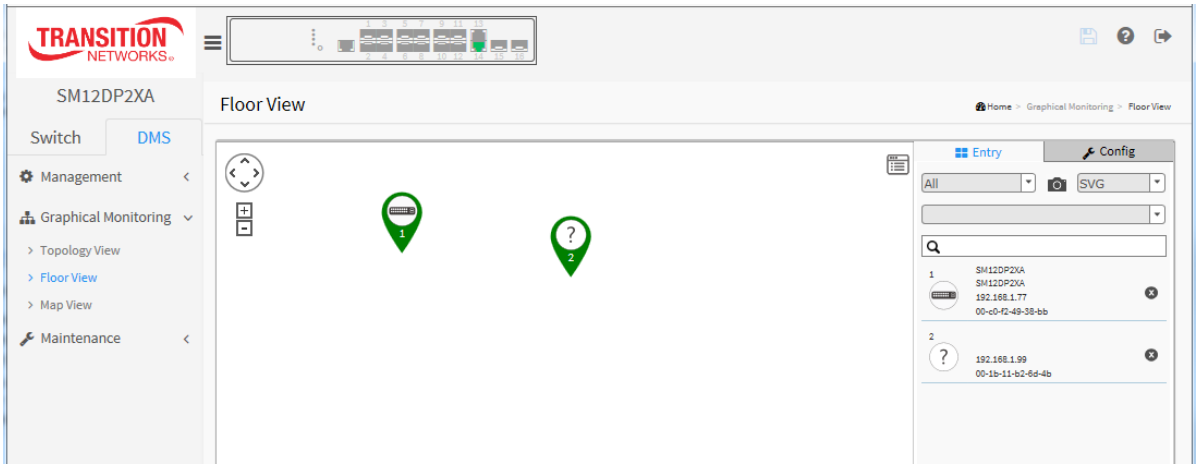
- For each IP device except DMS switches; set a threshold of throughput for IP devices, and get notification when throughput is lower or higher than settings.
- If both values are "0", it means the function is disabled.
- Polling interval is 1 second, when the page is closed, the Polling interval will change to about 5 seconds.



6-2.2 DMS > Graphical Monitoring > Floor View

Here you can easily plan IP devices installation locations onto a custom uploaded floor image.
This page lets you upload and manage floor map images. Due to flash memory limitations, up to 20 JPEG or PNG images, each of a max. of 256KB size, can be uploaded to the switch.

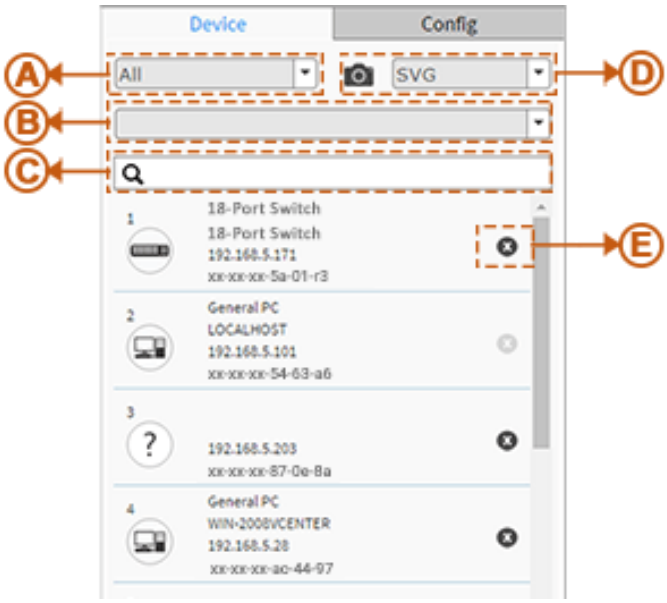
The DMS > Maintenance > Floor Image page lets you upload and manage floor map images in order for you to view them here.



 The Plus and Minus marks let you zoom in and zoom out the floor view; you can scroll up/down with mouse to achieve the same purpose.

 In the upper right corner, click the "Setting icon" to alternately display or hide the Entry and Config tabs with Device, Config, export floor view and advanced search functions for the device.

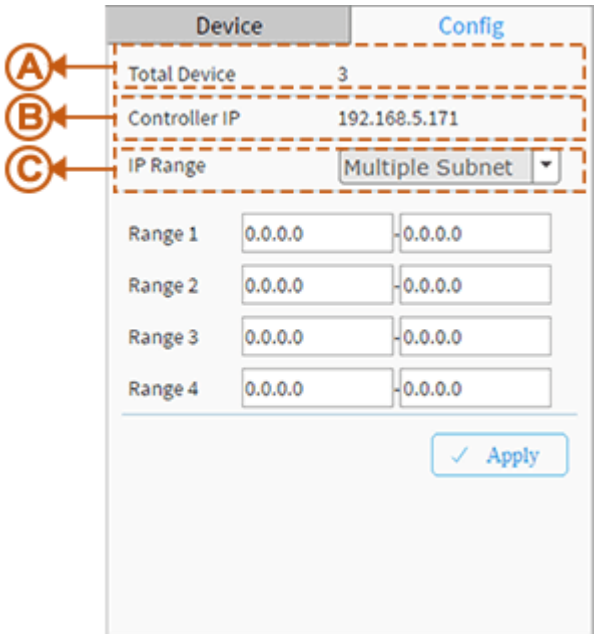
Device Search Console



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

System Setting Console



Function

A.	Shows how many IP devices are detected and displayed in the topology view.
B.	Show the Master IP address.
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 will suggest user to adjust 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 Floor or return to the Normal View.

Floor View

The DMS > > Graphical Monitoring > Floor View lets you:

- Anchor Devices onto Floor Maps
- Find Device locations Instantly
- Store 10 Maps in each Switch
- Provide IP Surveillance/VoIP/WiFi applications
- Place and remove a device icon:
  - To select a device click its icon from the device list. The device icon will show on the floor image's default location.
  - Click and hold left mouse to drag-and-drop the icon to the correct location on the floor view.
  - Click the cross sign on the right side of device icon to remove a device from all floor view images.

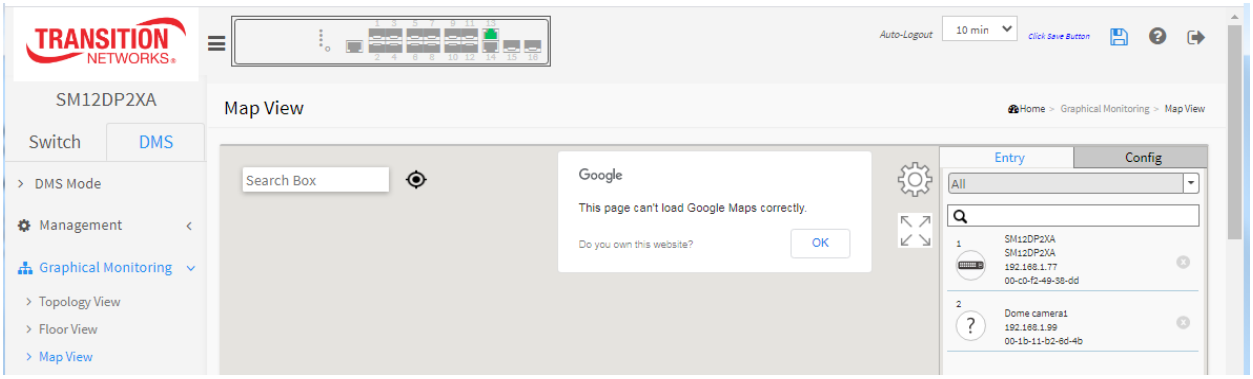
Device Status


Icon with black mark: Device link up. You can select the device / function and check issues.

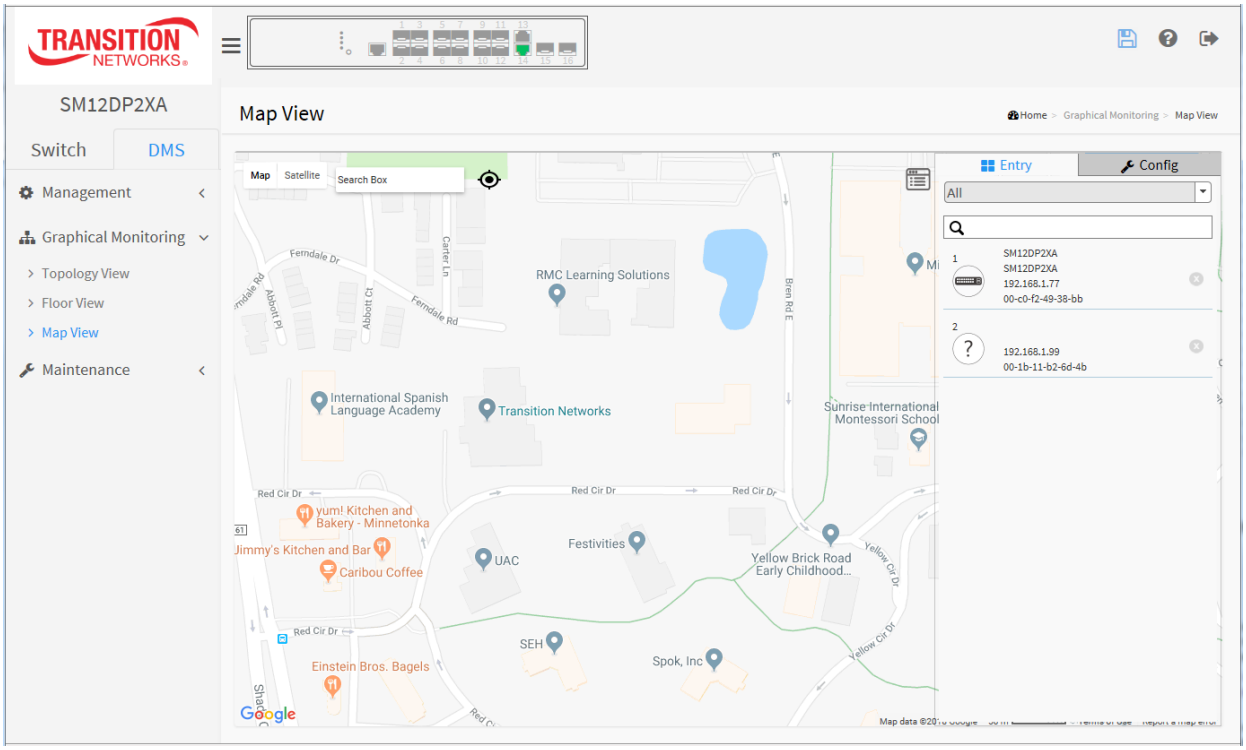

Icon with red mark: Device link down. You can diagnose the link status.

6-2.3 DMS > Graphical Monitoring > Map View

The Map View can help find the location of the devices even they are installed in different building. You can place the device icon on the Map View and navigate by Google Maps.

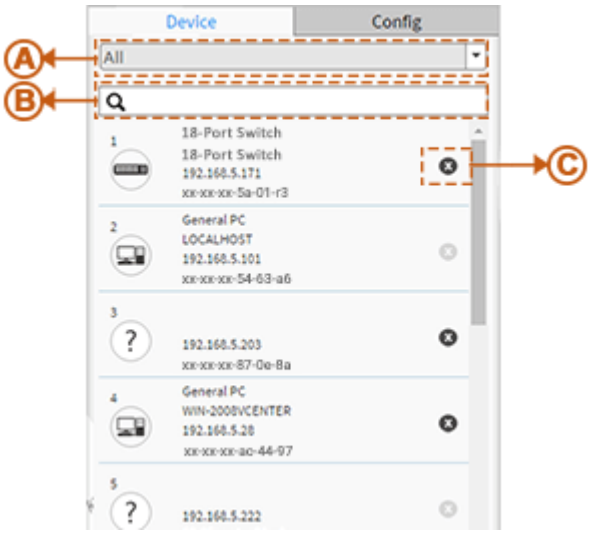


See Get the Google Map API Key on page 418.



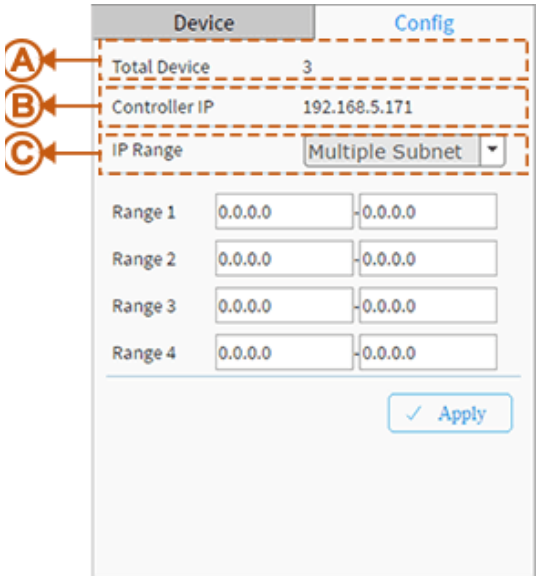
Click the  Setting icon in the upper right corner to alternately display and hide the Entry and Config tabs with Device, Config, and advanced search functions for the device.

1. Device Search Console



Function	
A.	Filter devices by Device Type
B.	Search devices by key words full text search
C.	Remove a device from map view

System Setting Console



Function	
A.	Shows how many IP devices are detected and displayed in the topology view.
B.	Shows the Master IP.
C.	**Single Subnet:** DMS base on master switch IP address. Here the subnet is "255.255.255.0" **Multiple Subnet:** To provide 4 ranges for inputting manually. (In this case we suggest that you adjust the switch's subnet mask to "255.255.0.0" to avoid IP devices that can't be recognized.)

Click the  Setting icon in the upper right corner to alternately display and hide the Entry and Config tabs with Device, Config, and advanced search functions for the device.

Map View lets you:

- Anchor Devices onto Google Map.
- Find Devices Instantly from the Map.
- Perform On-line search for a Company/Address.
- Run Outdoor IP Cam/WiFi Applications.
- Place and remove a device icon: Select a device and click its icon from the device list. The device icon will show on the map's default location. Click and hold left mouse by dragging-and-dropping the icon to the correct location on the map view. Click the cross sign on the right side of device icon to remove a device from map view.

Device Status

 Icon with black mark: Device link up. Click to select functions and check issues.

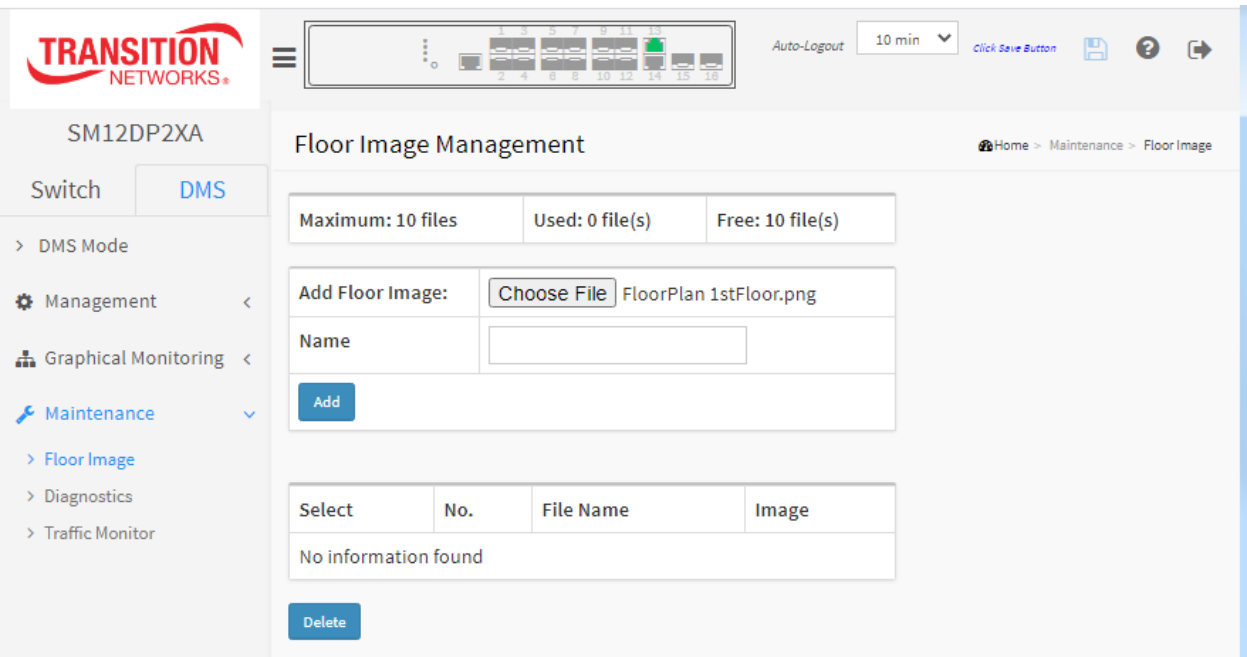
 Icon with red mark: Device link down. Click to diagnose the link status.

6-3 DMS > Maintenance

At DMS > Maintenance you can select Floor Image, Diagnostics, or Traffic Monitor.

6-3.1 DMS > Maintenance > Floor Image

This page lets you upload and manage floor map images. Up to 20 JPEG or PNG images of up to 256KB each can be uploaded to the switch.



Parameter descriptions:

Add Floor Image : Select the checkbox to select an image from the list.

Name: Displays the selected file name.

Select: Displays "*No information found*" until a floor image is added (screen above). After a filename is added, check the checkbox in the Select column to select an image from the list so it can be deleted. When checked, check the box again to de-select it.

No.: Displays the instance, starting at 1; up to 20 file instances are allowed. Up to 20 JPEG images of 256 Kb each can be uploaded to the switch.

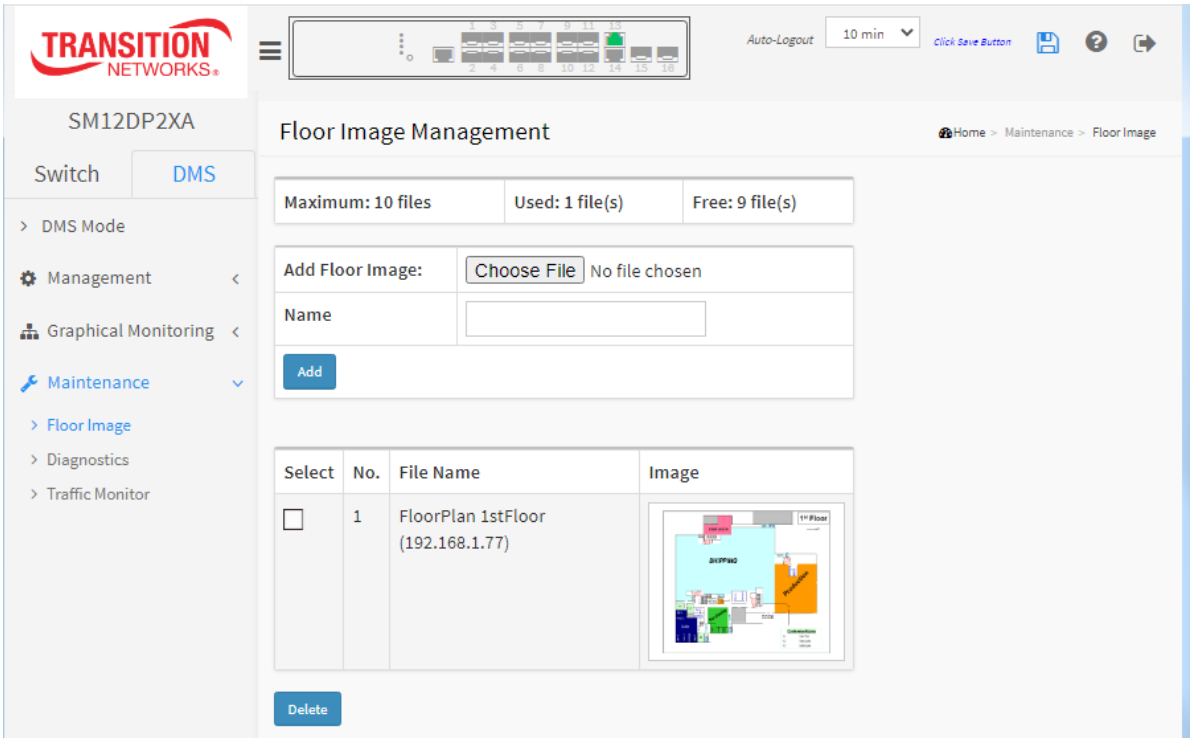
File Name: the floor image filename.

Image: a thumbnail of the floor image.

Buttons

Browse…: Click to select an image from the list. Only .jpg and .png file formats are allowed.
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 the selected floor map.

Example: One Floor Plan added:



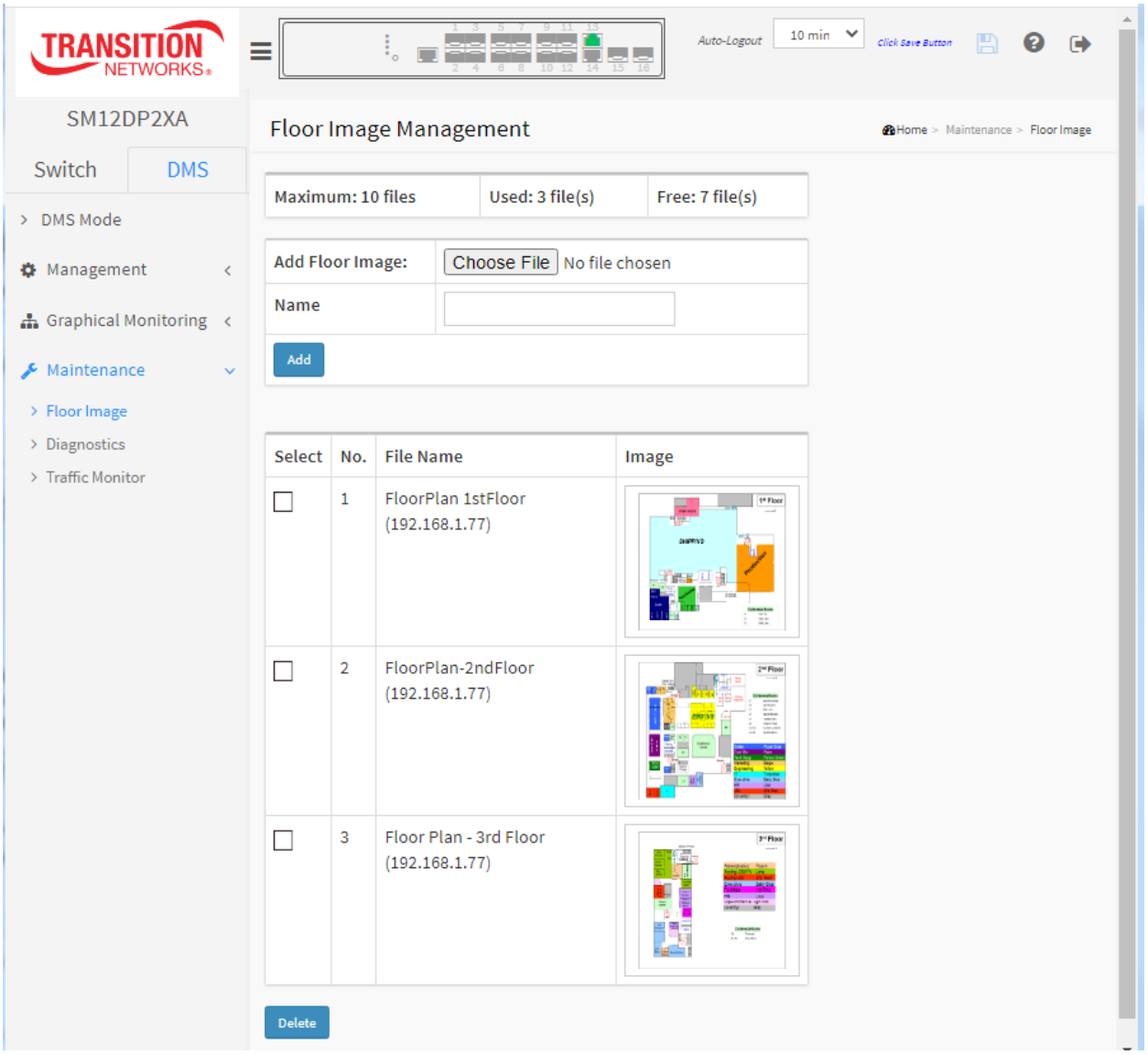
Messages:

Processing… displays temporarily when loading or deleting a file.

Only jpg, png are allowed displays if you select an unsupported graphics file format.

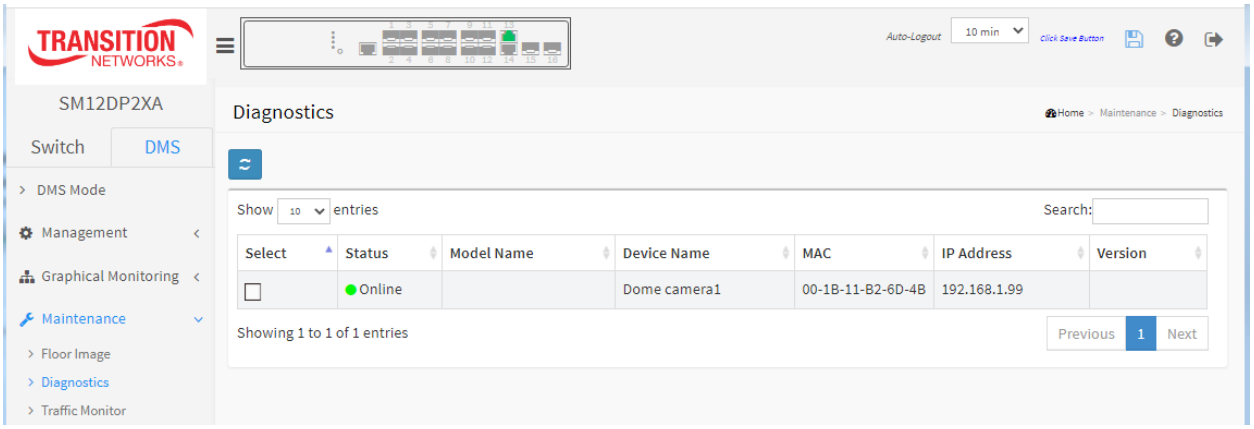
File size is too big. Only 524152 bytes is available.

Example: Three Floor Plans added:



6-3.2 DMS > Maintenance > Diagnostics

This page provides an overview of the DMI Diagnostics. This page displays when you click on an On-line entry in the Status column at the DMS > Management > Device List menu path.



Parameter descriptions:

Show *xx* entries: at the dropdown, select 10, 25, 50, or 100 entries per page. The default is 10.

Select: Select off-line device from the list.

Status: Device Online or Offline.

Model Name: The model name of the network connected devices.

Device Name: The device name of the network connected devices.

MAC: The mac address of the device.

IP Address: The IP address of the network connected devices.

Version: The Version of the network connected devices.

Buttons

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

Search: Search any key word you want.

Previous: Click to display the prior page of table data.

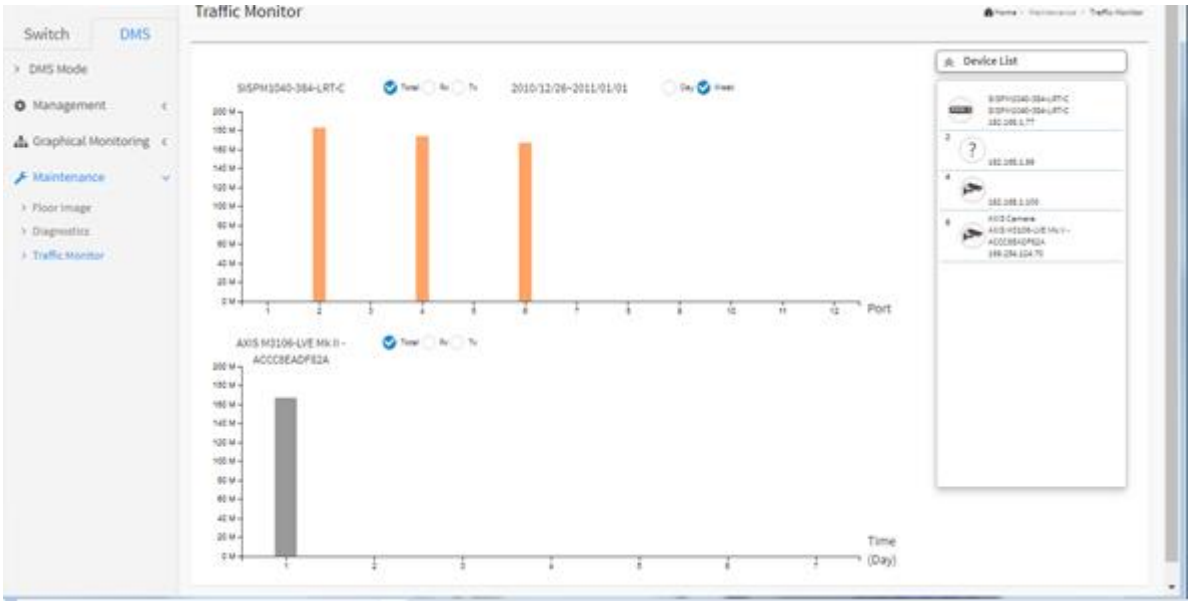
Current page: Displays the page number of the currently-displayed page.

Next: Click to display the following page of table data.

6-3.3 DMS > Maintenance > Traffic Monitor

DMS supports traffic monitoring of each port and keeps a one-week record that can be used to compare and analyze through visual charts. The page displays two different graphs for a selected device.

This page displays a chart of network traffic of all the devices. You can view the traffic of all ports or a specific port. Click on specific port on the traffic chart to reveal its traffic during the day. You can select to display a summary of one day or a week of traffic by selecting the check circle on top. The same applies to the selection of Tx, or Rx traffic, or a total of both. A single port's traffic is shown at the lower half of the screen.



Parameter descriptions:

Total / Rx / Tx: Select the set of data to be displayed.

< yy/mm/dd >: Select the date of data displayed. This is the time set at Switch > Configuration > System > Time or at Switch > Configuration > System > NTP.

Day / Week: Select a day's worth of data or a week's worth of data to be displayed.

Device List: Displays the set of discovered devices.

Throughput: Vertical axis shows throughput (e.g., 0 M – 18000 M or 0 M-1200 M). The unit of measure is Mbps.

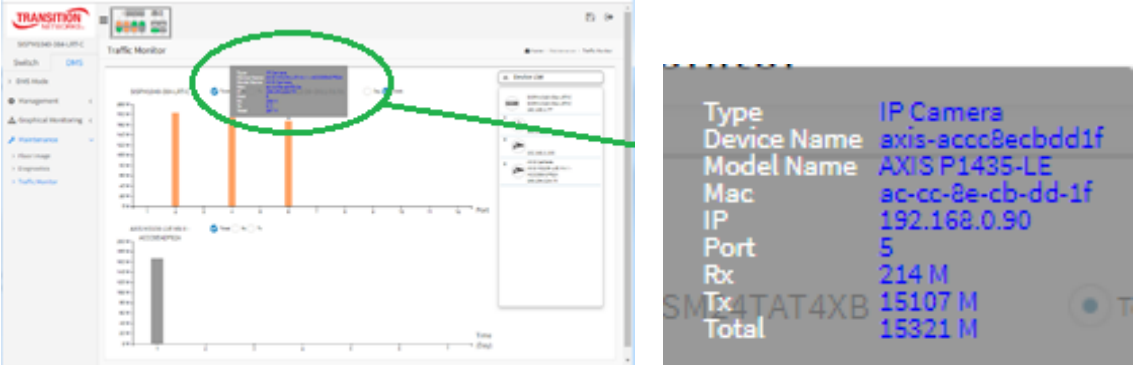
Port: Horizontal axis shows the switch port numbers.

Time (Hour): Horizontal axis shows the time elapsed in hours (0-23).

The graph's vertical axis shows throughput and the unit of measure is Mbps.

DMS Traffic Monitor

1. Navigate to DMS > Maintenance > Traffic Monitor.
2. Select a device to monitor.
3. Hover the cursor over a column in the graph to view its details.



4. Click the graph column to display its axis information in the lower graph table.

Message: *Traffic Monitor feature is only available on master controller.*

Current master controller IP Address:0.0.0.0

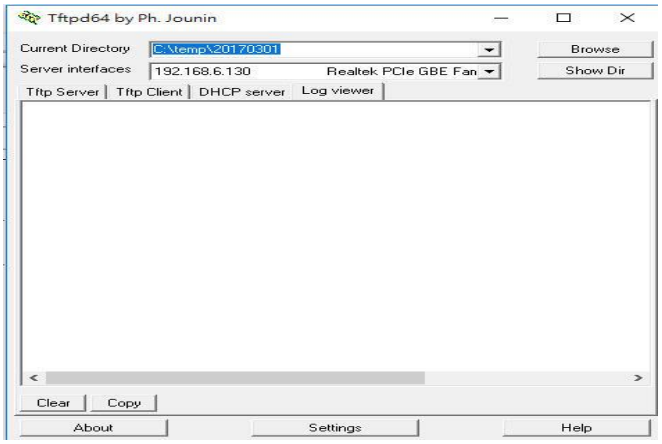
Meaning: The switch must be the Master (Controller) switch (added at FW v 7.10.2307).

Recovery: Click the OK button and make this switch the Master (Controller) switch. See 6-1.1 DMS > DMS Mode on page **342.**

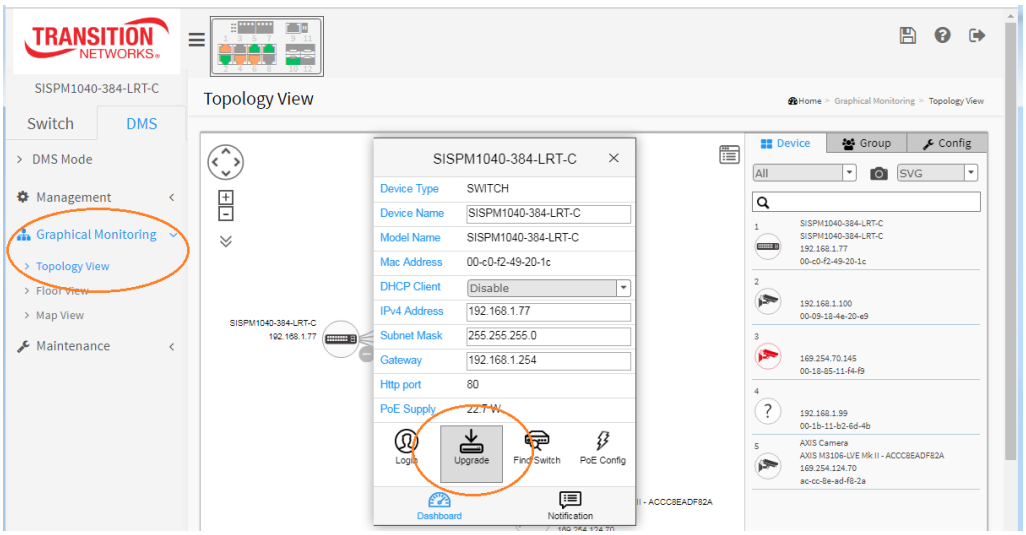
6-3.4 DMS Firmware Upgrade Procedure

1. Navigate to the DMS > Graphical Monitoring > Topology View menu path.
2. Click the button to display the right pane menu tabs (Device, Group, and Config).
3. Connect all switches and make sure DMS discovers and displays them.
4. Set all switches with different IP addresses and in the same IP segment.
5. Make sure gateway IP address is configured.
6. Left-click any device icon to display the device consoles for further actions:

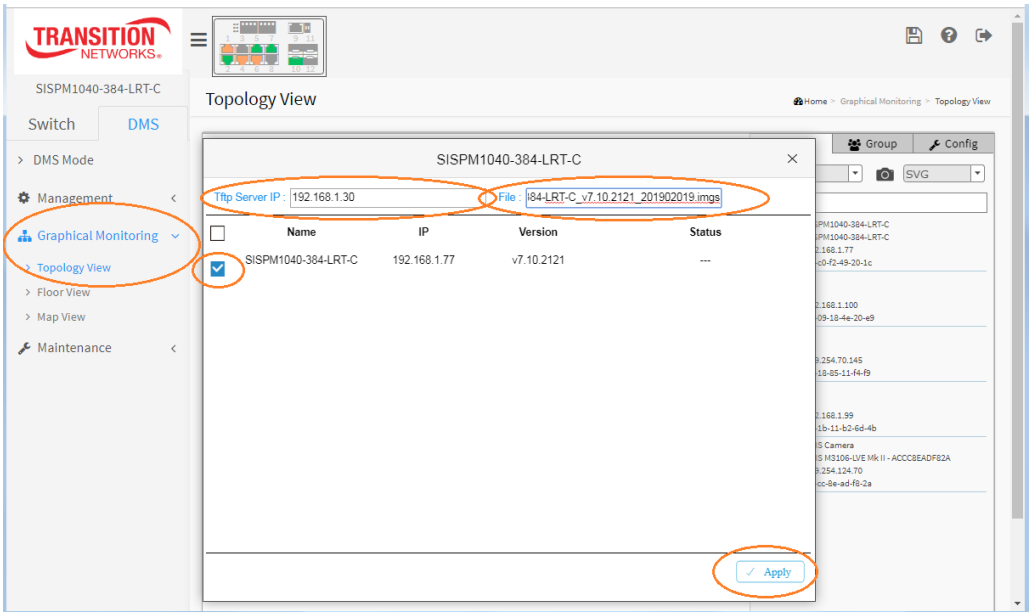
7. Click the Upgrade (**Upgrade)** button to upgrade the software version.
8. Enable the TFTP server and set the correct image path.



9. Click the switch icon, and then click the “Upgrade” button in the Dashboard.

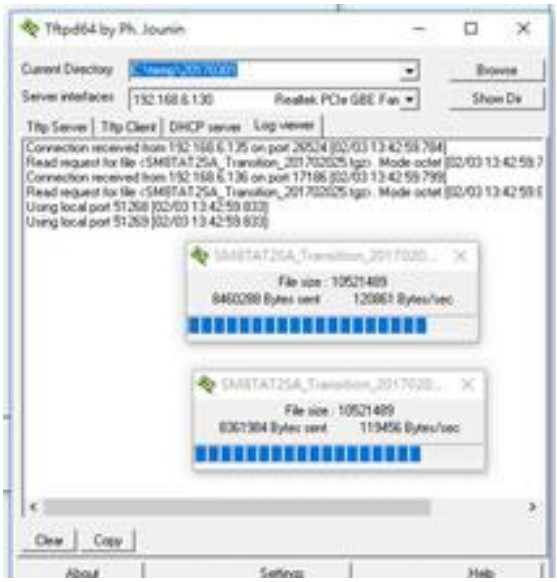


10. Enter the TFTP server IP address and FW file name and select the switch on which you want to upgrade the FW.



11. Click “Apply” to start the FW upgrade and save to Running-config.

12. Observe the upgrade status until completion.



Messages

Starting, please wait...

Error : Firmware download fail

6-4 DMS Troubleshooting

Problem: The switch lists itself as the only device in DMS Topology View.
Problem: In DMS, the Local image shows the IP address of another switch.

Description: The switch is listed as only device in DMS Topology View in DMS; all devices are listed in DMS device list. This is usually because the switch's gateway is not configured appropriately.

Resolution: An IP Route must be configured manually. For example, a switch IP address of 192.168.1.77 should have the following IP route configured: ip route 0.0.0.0 0.0.0.0 192.168.1.x. Without the IP route configured, you may be unable to view all devices on the network in DMS.

1. Go to DMS > Management > DMS Mode to check if the controller IP is correct.
2. Verify that the gateway of this switch is correctly configured.
3. Verify that all connected devices are displayed in DMS Topology View.

Problem: DMS Connectivity diagnostics fails to ICMP reachable device.
Description: DMS displays a device which is reachable via ICMP ping as failing the connection status in diagnostics. Cable status displays as *OK*.
Resolution: Contact 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* displays at DMS > Graphical Monitoring > Map View.

Resolution: 1. Click the OK button to clear the message. 2. See Get the Google Map API Key on page 418.

6-5 For More DMS Information

See the online DMS Video.

See the online DMS Overview.

Chapter 7 - Troubleshooting

Most problems are caused by the following situations. Check for these items first when you start troubleshooting:

1. Verify the install procedures were performed correctly. See the related Install Guide.

2. Check if the POWER LED is Off:
   - Check connections between the switch, the power cord and the wall outlet.
   - Contact your dealer for assistance.

3. Check if the Link LED is Off:
   - Verify that the switch and attached device are powered on.
   - Be sure the cable is plugged into the switch and corresponding device.
   - If the switch is installed in a rack, check the connections to the punch-down block and patch panel.
   - Verify that the proper cable type is used and its length does not exceed specified limits.
   - Check the adapter on the attached device and cable connections for possible defects. Replace the defective adapter or cable if necessary.
   - Use the **RESET** button to change LED mode, reset the switch, or restore to defaults. See the Install Guide for details.

4. Make sure all devices connected to the SM12DP2XA are configured to auto negotiate, or are configured to connect at half duplex (all hubs are configured this way, for example).

5. Check the cabling:
   - Look for faulty or loose cables.
   - Look for non-standard and mis-wired cables.

6. Make sure you have a valid network topology:
   - Check for improper Network Topologies.
   - Make sure that your network topology contains no data path loops.

7. Check the port configuration.
   - Make sure ports have not been put into a “blocking” state by Spanning Tree, GVRP, or LACP. The normal operation of the Spanning Tree, GVRP, and LACP features may put the port in a blocking state.
   - Verify that the port has not been configured as disabled via software.

8. Record any related error messages, conditions, and configurations for your Tech Support Specialist to consider.

9. Contact Transition Networks Tech Support. See Contact Us below.

Contact Us

Call us at 800-526-9267 or +1-952-941-7600. Telephone: +1-952-941-7600.

Toll Free: 800-526-9267 Fax: 952-941-2322 Web: https://www.transition.com

Address: 10900 Red Circle Drive, Minnetonka, MN 55343 USA

Email Us: customerservice@transition.com or techsupport@transition.com or sales@transition.com or info@transition.com.

Appendix A – DHCP Per Port

You can configure DHCP Per Port via the Web UI and CLI as described below. The DHCP Per Port factory default mode is Disabled. See the *SM12DP2XA CLI Reference* for CLI mode operation.

Configure DHCP Per Port via the Web UI

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**.

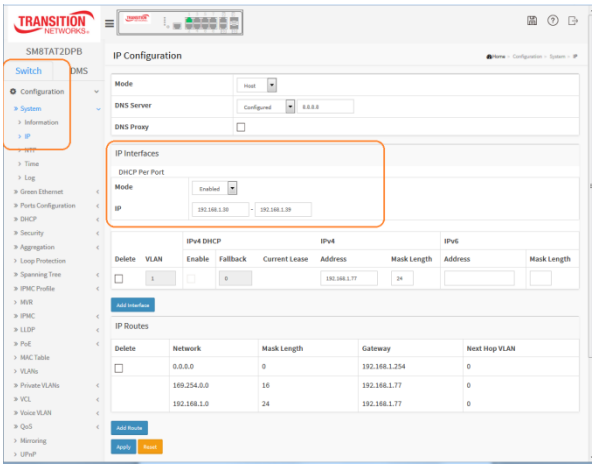
The DHCP Per Port pages and parameters are described below.

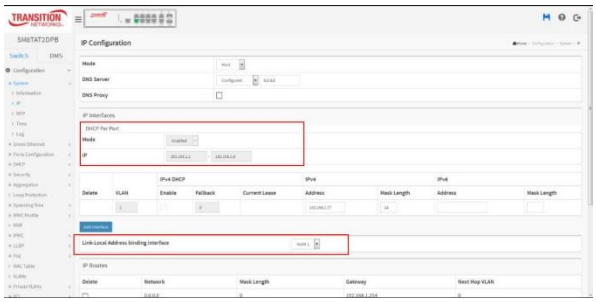
DHCP per Port Mode Configuration

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.





Parameter descriptions: The DHCP Per Port parameters and buttons are described below.

DHCP Per Port Mode: at the dropdown select **Enable** or **Disable** the DHCP Per Port function globally. The default is **Disabled**.

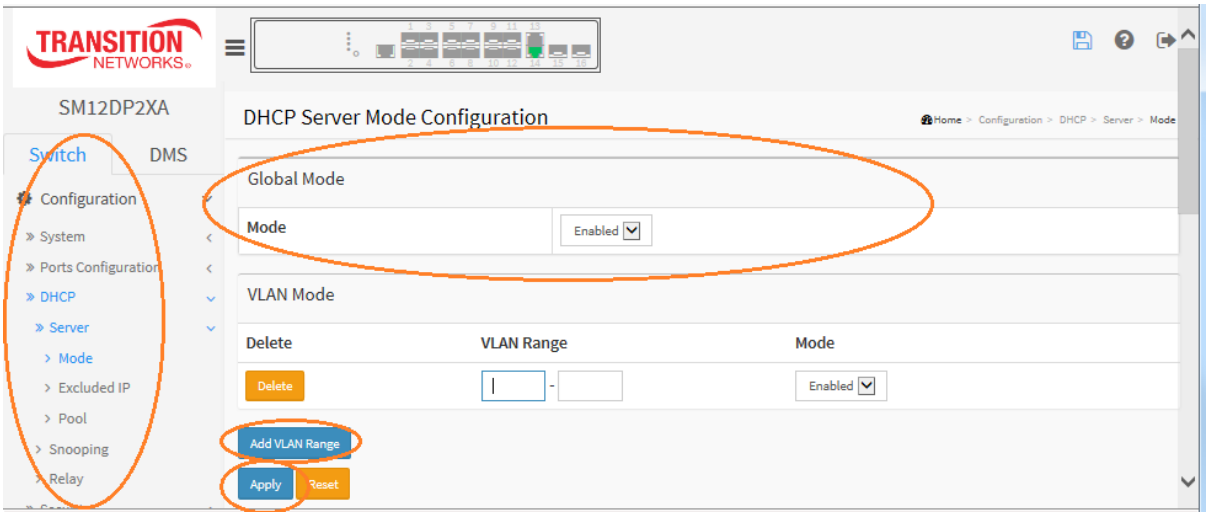
IP: enter the IPv4 IP address range to be used when the DHCP Per Port function is enabled (e.g., 192.168.10.20 - 192.168.10.37). The DHCP Per Port IP range must be within the interface subnet. Note that DHCP Per Port with IPv6 is not supported at this time. The DHCP Per Port IP range must equal the switch port number excluding uplink ports (16).

Apply: Click to save changes to the entries. If the entries are valid, the webpage message "*Update success!*" displays. Click the **OK** button to clear the message. If any entries are invalid, an error message displays. Click the **OK** button to clear the message and enter valid values, then click the **Apply** button again.

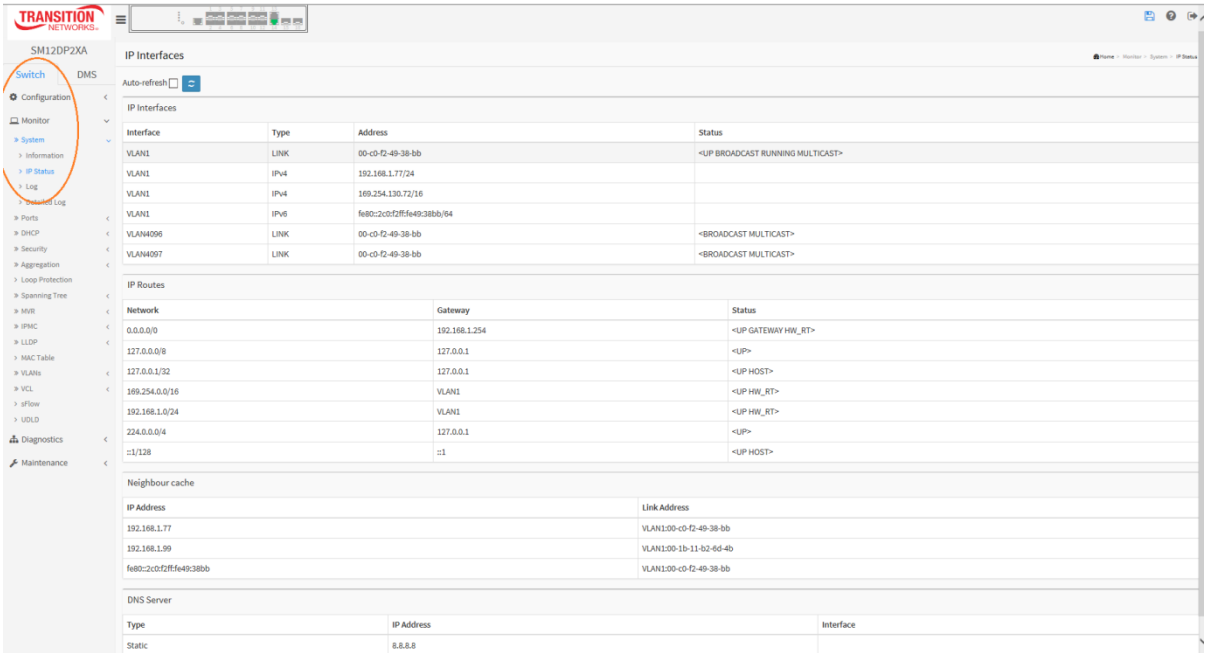
Reset: Click to undo any changes made locally and revert to previously saved values.

DHCP Server Mode Configuration

When DHCP Per Port is enabled and configured at **Configuration** > **System** > **IP**, the checkbox and selection in the DHCP Server Mode Configuration section at **Configuration** > **DHCP** > **Server** > **Mode** will become gray (cannot be selected):



To monitor DHCP Per Port status, navigate to the **Monitor** > **System** > **IP Status** menu path.

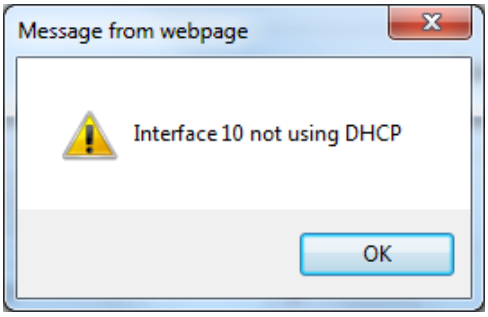


DHCP per Port Mode Web UI Messages

Message: *Interface xx not using DHCP*

Meaning: The Interface being configured does not have DHCP enabled and configured.

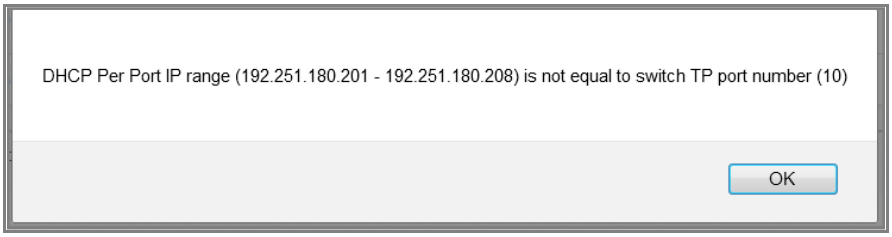
Recovery: **1**. Click the **OK** button to clear the webpage message. **2**. Enable and configure DHCP for the interface being configured. See "DHCP Server Mode Configuration" on page 303.



Message: *'DHCP Per Port IP range (192-168-1.80 - 192-168-1.99*) is not equal to switch port number excluding uplink ports (10)

Meaning: The IPv4 IP address range entered for the DHCP Per Port function was invalid.

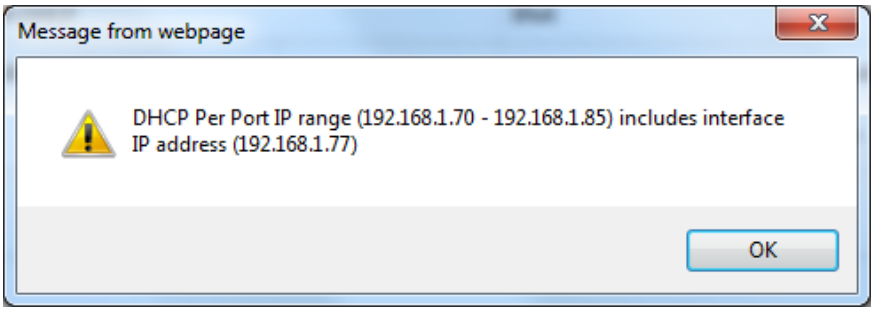
Recovery: **1**. Click the **OK** button to clear the webpage message. **2**. Re-configure DHCP Per Port. See the DHCP Per Port Mode Configuration section above.



Message: *'DHCP Per Port IP range (192-168-1.70 - 192-168-1.85*) *includes interface IP Address (192.168.1.77)*

Meaning: The IPv4 IP address range entered for the DHCP Per Port function was invalid.

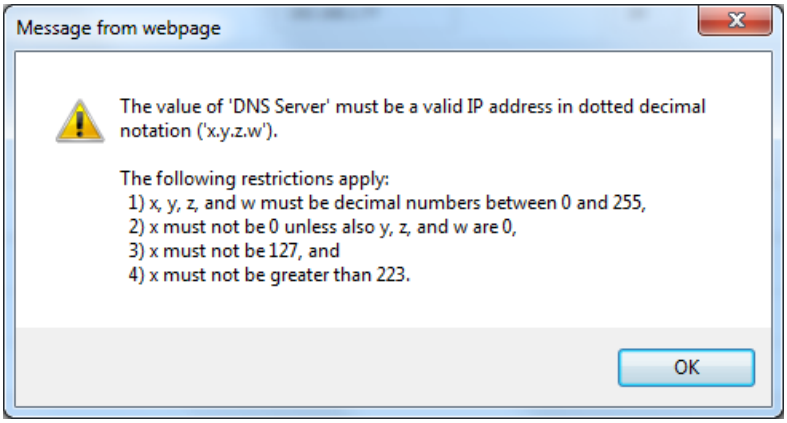
Recovery: **1**. Click the **OK** button to clear the webpage message. **2**. Re-configure DHCP Per Port. See the DHCP Per Port Mode Configuration section above. On the screen below, the range should be something like 192-168-1.80 - 192-168-1.85 to be valid.



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

Meaning: You entered an invalid IP address for the DNS Server being configured.

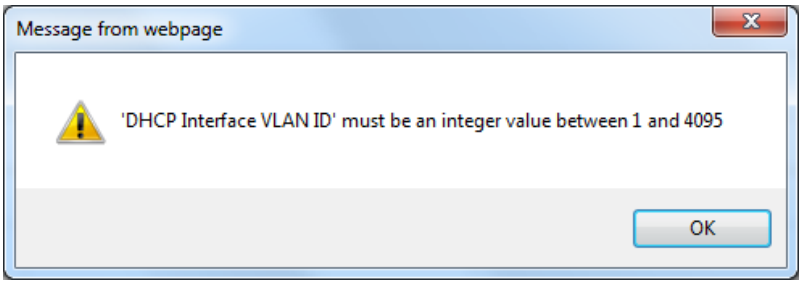
Recovery: **1**. Click the **OK** button to clear the webpage message. **2**. Enter a valid IP address in the format x.y.z.w per the on-screen restrictions. See "DHCP Server Mode Configuration" on page 303.



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.



Appendix B – Service, Warranty, and Tech Support

See the *SM12DP2XA Install Guide* for related information.

Appendix C – Compliance Information

See the *SM12DP2XA Install Guide* for related information.

Transition Networks
10900 Red Circle Drive
Minnetonka, MN 55343, U.S.A.
tel: +1.952.941.7600 | toll free: 1.800.526.9267 | fax: 952.941.2322
sales@transition.com | techsupport@transition.com | customerservice@transition.com

SM12DP2XA Web User Guide, 33752 Rev. C