SISGM1040-284-LRT

Managed Hardened Gigabit Ethernet Switch

(8) 10/100/1000Base-T Ports + (4) 100/1000Base-X SFP Slots

Web User Guide

Part Number 33809
Revision F October 2023

Intellectual Property

Warranty

For details on the Lantronix warranty policy, see http://www.lantronix.com/support/warranty.

Contacts

Lantronix Corporate Headquarters
48 Discovery, Suite 250
Irvine, CA 92618, USA
Toll Free: 800-526-8766
Phone: 949-453-3990
Fax: 949-453-3995

Technical Support
Online: https://www.lantronix.com/technical-support/

Sales Offices
For a current list of our domestic and international sales offices, go to www.lantronix.com/about/contact.

Disclaimer

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

Revision History

Date	Rev	Notes
7/26/21	D	FW v7.20.0063: fix Web UI Help page reference to ‘Facility’, fix LLDP TX interval reporting and add new and modify existing API commands and response structures.
9/28/22	E	FW v7.20.0121: add API commands. Add ‘Set reboot system when DI changes to abnormal’ and fix DDM info update issue. Fix port link up when inserting TN-EOT-CO / -RT copper module. Update Radius server. Initial Lantronix rebrand. Add DHCP Option 229 and First Time Wizard. Add DHCP per port IP interface. Change default settings for SNMP mode and Auth Method. Add ConsoleFlow Cloud and LPM support.
10/11/23	F	FW v7.20.0190: Change ConsoleFlow to Percepxion. Add API in HTTPS. Fix issues with DeviceKey, FirmwareVersion, Serial # for Percepxion and MAC address for LPM. Update SSH and fix FW upgrade and DMS issues. Add PoE Status to Device Telemetry Data. Update to TLSv1.2 ciphers. Add two public OIDs. Remove invalid file name "mach10_combined.crt" from Config Download, Upload, Activate, and Delete pages. Automatically save configuration changes to Startup Config in Percepxion server. Update LACP on Air description.

Contents

Product Description

The SISGM1040-284-LRT industrial L2+ managed GbE switch is a next generation industrial grade Ethernet switch offering powerful L2 and basic L3 features with better functionality and usability. In addition to the extensive management features, the SISGM1040-284-LRT also provides carrier Ethernet features such as OAM/CF, ERPS/EPS, and PTPv2, making it suitable for industrial and carrier Ethernet applications.

The SISGM1040-284-LRT delivers eight 10M/100M/1G RJ45 ports, four GbE SFP ports and one RJ45 console port. SISGM1040-284-LRT provides high hardware performance and environment flexibility for industrial and carrier Ethernet applications.

The embedded Device Managed System (DMS) features provides the benefits of ease-of-use, configuration, installation, and troubleshooting in video surveillance, wireless access, and other industrial applications. The SISGM1040-284-LRT delivers management simplicity, great user experience, and low total cost of ownership.

About This Manual

This manual describes how to install, configure, and troubleshoot the SISGM1040-284-LRT switch via the Web UI, including how to:

- Configure switch parameters.
- Monitor switch information, status, and statistics.
- Run diagnostics.
- Perform maintenance (reboot, firmware upgrades, etc.).

Related Manuals

SISGM1040-284-LRT Quick Start Guide, 33807

SISGM1040-284-LRT Install Guide, 33808

SISGM1040-284-LRT CLI Referrnce, 33810

SISGM1040-284-LRT API User Guide, 33827

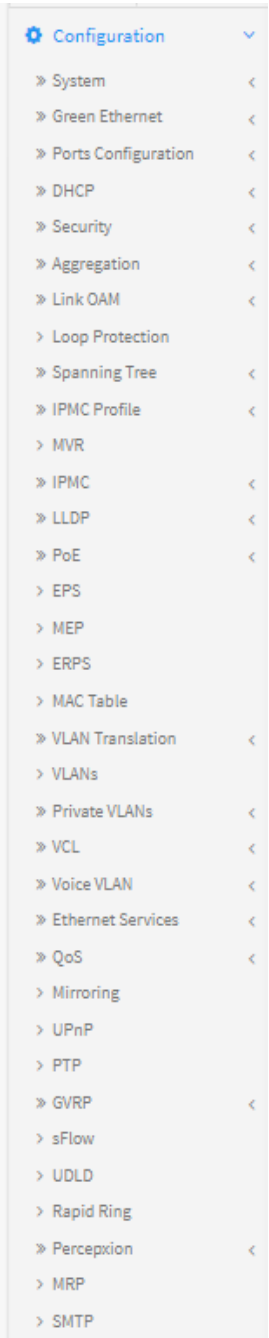
Release Notes (version specific)

For Lantronix Documentation, Firmware, App Notes, etc. go to https://www.lantronix.com/technical-support/
Note that this manual provides links to third party web sites for which Lantronix is not responsible.

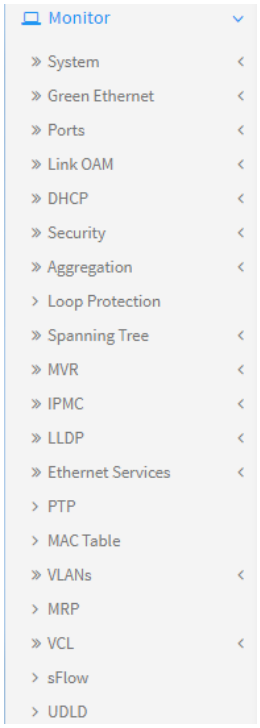
Web UI

The web user interface (Web UI) provides five main menu selections and related sub-menus:

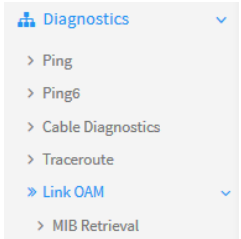
Main Menus



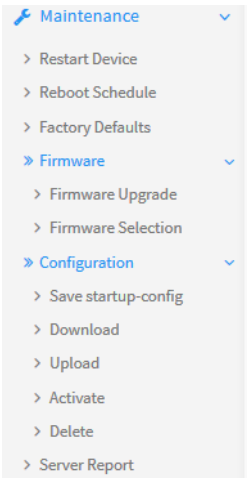
Configuration



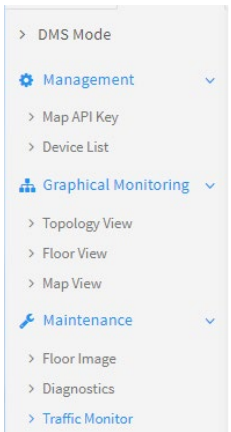
Monitor



Diagnostics



Maintenance

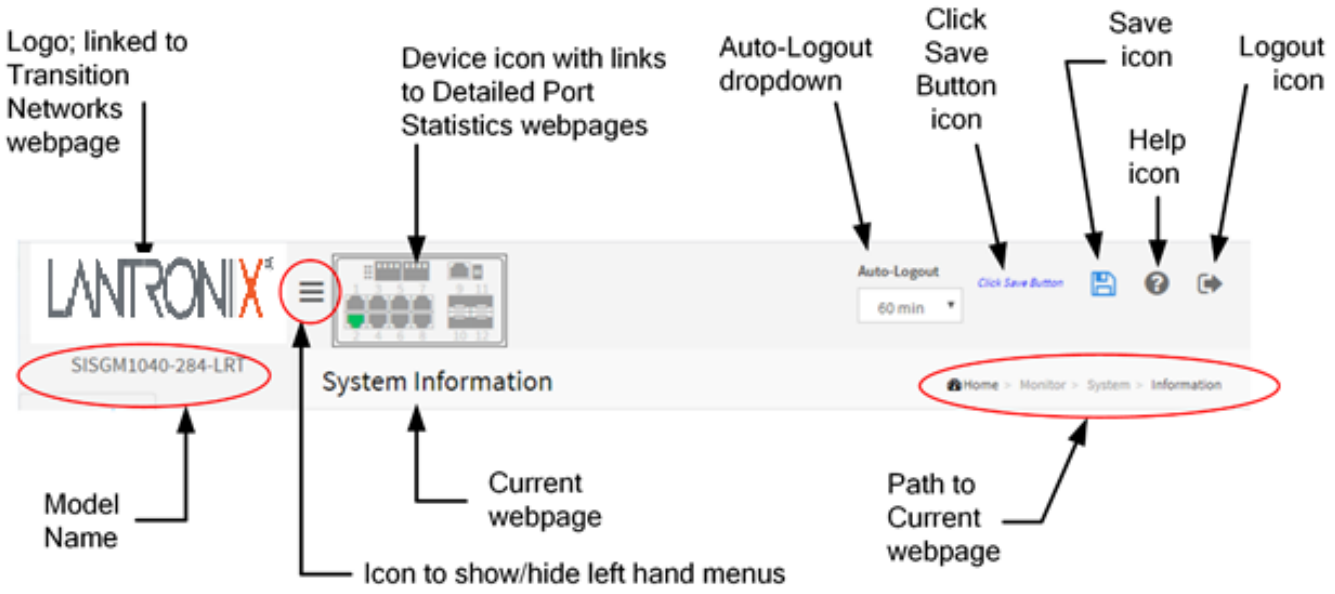


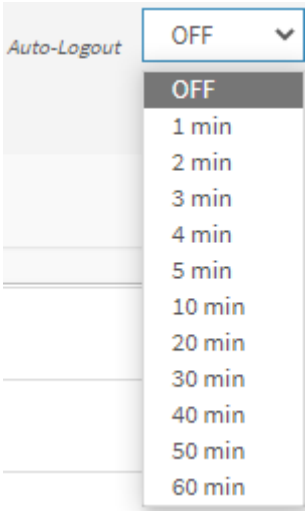
DMS Mode

Each of the main menu items and their sub-menus are described in the following sections.

Webpage Navigation

The Web UI navigation controls and icons are shown below.





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 (default), 20, 30, 40, and 60 minutes (added at FW v v7.10.2496).

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

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

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

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

Auto-Logout Timeout Summary

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

Webpage Messages

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

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

Message: *Are you sure you want to save running configuration to startup-config?*
Recovery: Click the OK button if you want to save the changes.

Message: *Update success!*

Initial Login and Configuration

The Web UI lets you easily configure and monitor from any port of the switch all switch modules and parameters. The default values are listed below:

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

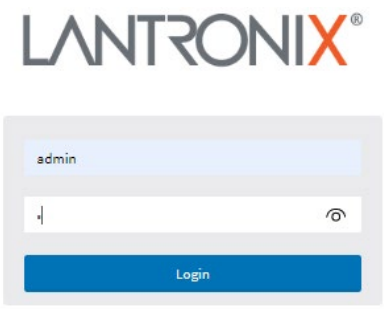
After the switch has been configured, you can browse it. For instance, type 192.168.1.77 in the address row in a browser, it will show the following screen and ask you for a username and password in order to login.

The default username is "admin" and the default password is "admin". For first time use, enter the default username and password, and then click the Login button. The login process now is completed.

Note: To optimize the display effect, we recommend you use Microsoft IE 10 above, Chrome V.39 above, Firefox V.33 above, or Microsoft Edge and have the resolution 1920x1080.

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

The Login page is shown below.



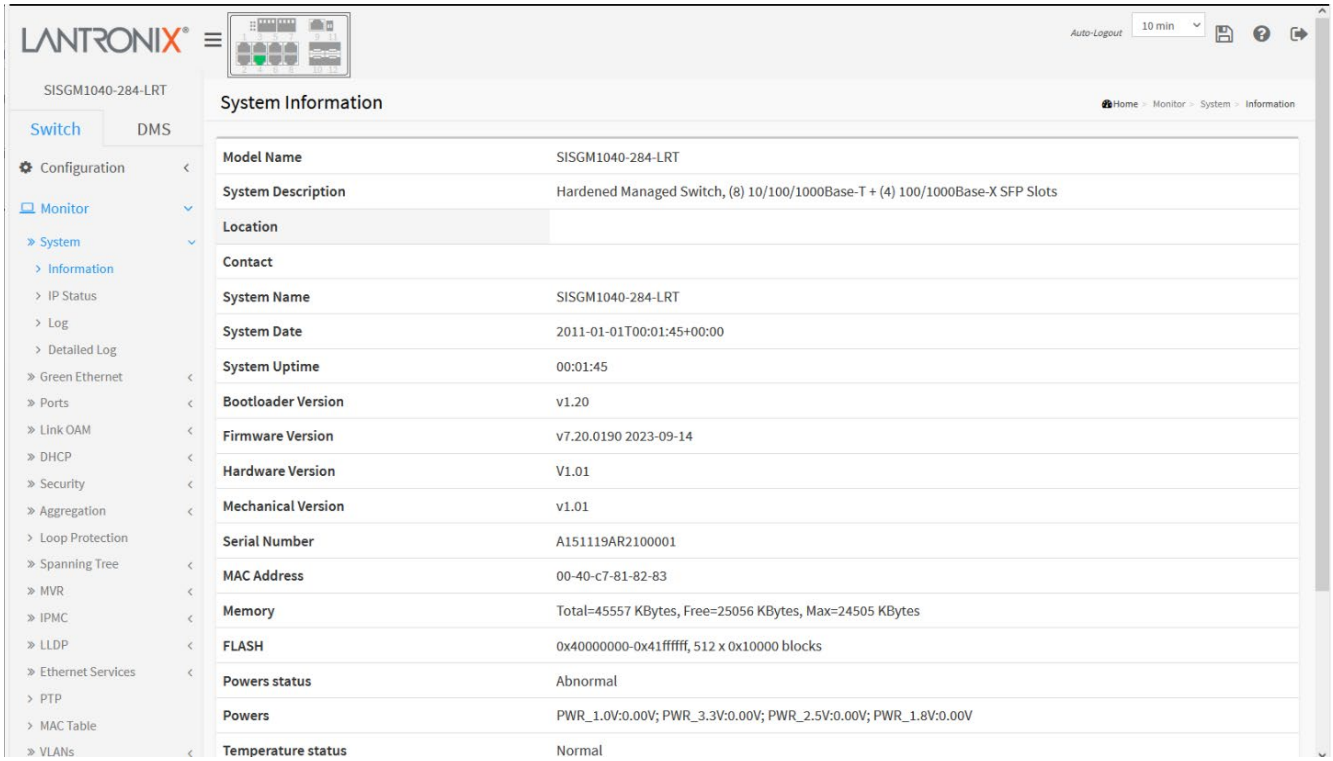
After Login the startup page displays at Switch > Monitor > System > Information (see below).

: Click to Show the Password text as you enter it. Added at FW VB7.20.0121.

: Click to Hide the Password text as you enter it. Added at FW VB7.20.0121.

Note: After initial login, change the Username and Password per your organization's security policy on the Users Configuration page at Switch > Configuration > Security > Switch > Users.

Startup page (Switch > Monitor > System > Information):

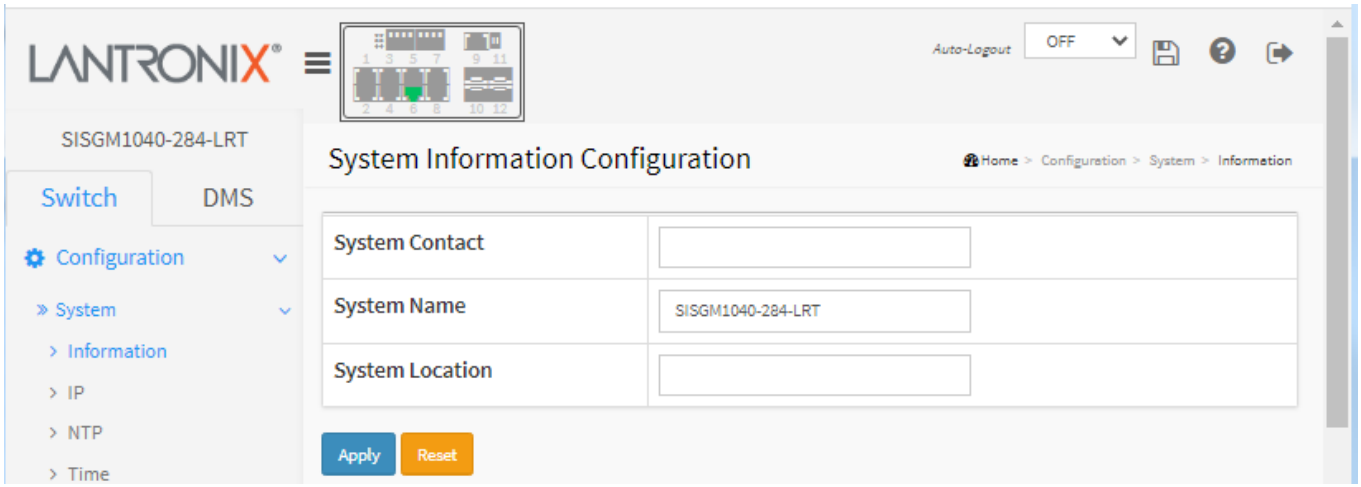


1. Configuration

The Configuration menu items let you set switch parameters which you can view in the Monitor sub-menus.

Configuration > System > Information

Navigate to the Configuration > System > Information menu path to display the System Information Configuration page. You can view and configure switch system parameters here. Information entered here displays at the Monitor > System > Information page.



Parameter descriptions:

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

System Name: An administratively assigned name for this managed node. By convention, the system name may be the node's fully qualified domain name (FQDN). The allowed string length is 0-128 characters.

System Location: The physical location of this node(e.g., telephone closet, 3rd floor). The allowed string length is 0 – 128 characters.

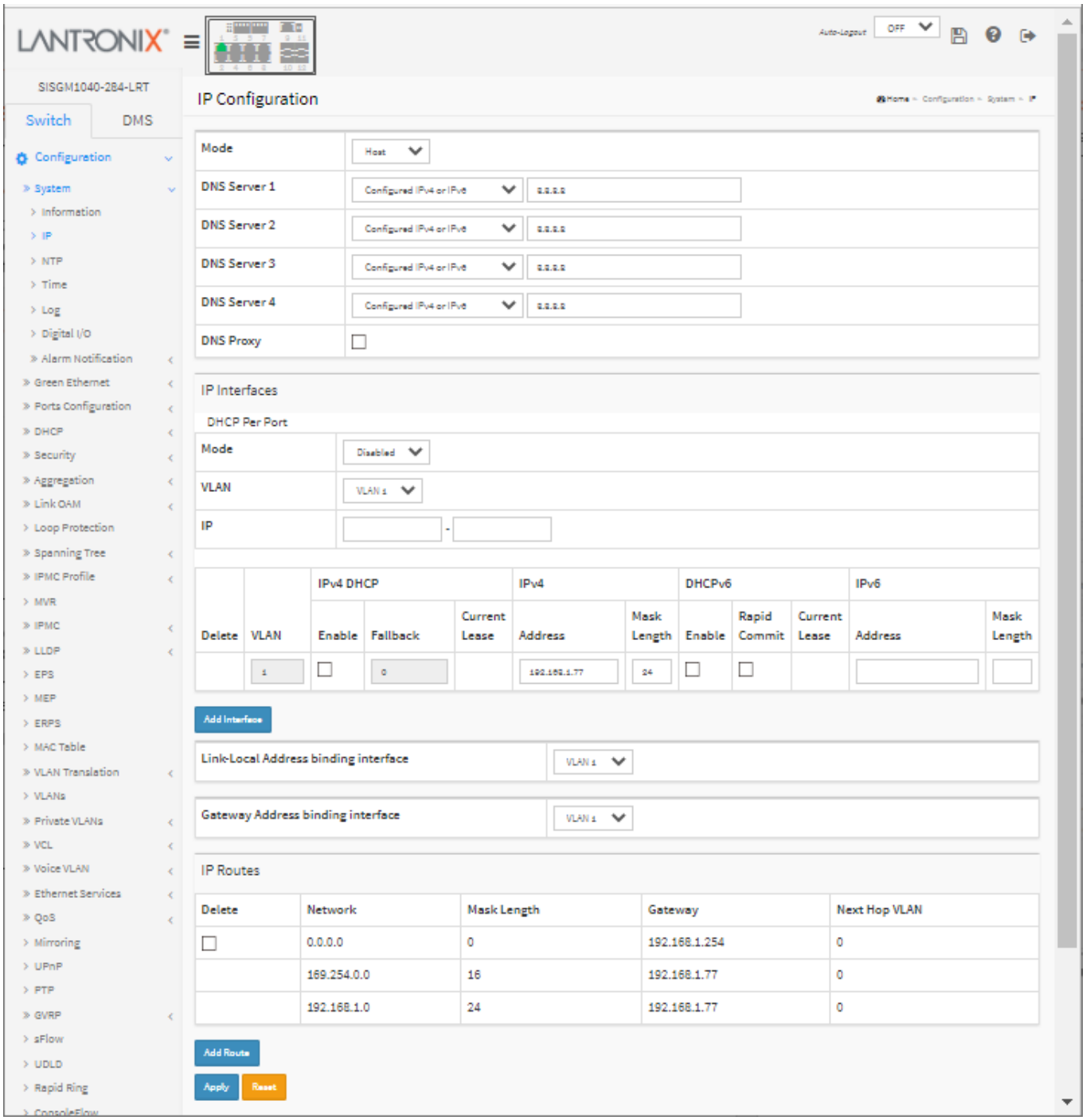
Buttons

Apply: Click to save changes.

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

Configuration > System > IP

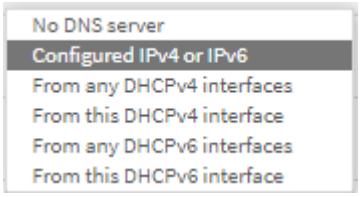
Navigate to the Configuration > System > Information menu path to display the IP Configuration page. You can view and configure switch IP parameters here. Information entered here displays at the Monitor > System > IP Status page.



Parameter descriptions:

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

DNS Server 1-4: This setting controls the DNS name resolution done by the switch. There are four servers available for configuration, and the index of the server presents the preference (less index has higher priority) in doing DNS name resolution. The switch selects the active DNS server from configuration in turn if the preferred server does not respond in five attempts. These modes are supported:



No DNS server: No DNS server will be used.

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

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

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

Configured IPv6: Explicitly provide the valid Ipv6 unicast (except linklocal) address of the DNS Server. Make sure the configured DNS server is reachable (e.g. via PING6) for activating DNS service.

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

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

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

IP Interfaces

DHCP Per Port Mode: Enable or Disable DHCP per port. The default is Disabled. See Appendix A – DHCP Per Port Configuration on page 413 for more information.

DHCP Per Port VLAN: Set DHCP per port VLAN.

DHCP Per Port IP: Define the IP range for DHCP per port.

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

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

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

IPv4 Address: The IPv4 address of the interface in dotted decimal notation. If DHCP is enabled, this field configures the fallback address. The field may be left blank if IPv4 operation on the interface is not desired - or no DHCP fallback address is desired.

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

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

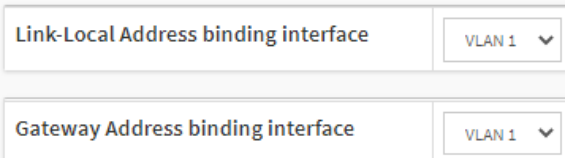
DHCPv6 Rapid Commit: Enable the DHCPv6 Rapid-Commit option by checking this box. If this option is enabled, the DHCPv6 client terminates the waiting process as soon as a Reply message with a Rapid Commit option is received. This option is only manageable when DHCPv6 client is enabled.

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

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

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

Link-Local Address binding interface: At the dropdown select the VLAN to be used. The default is VLAN1.



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

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. The Gateway and the 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 4095 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, the 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.

Messages:

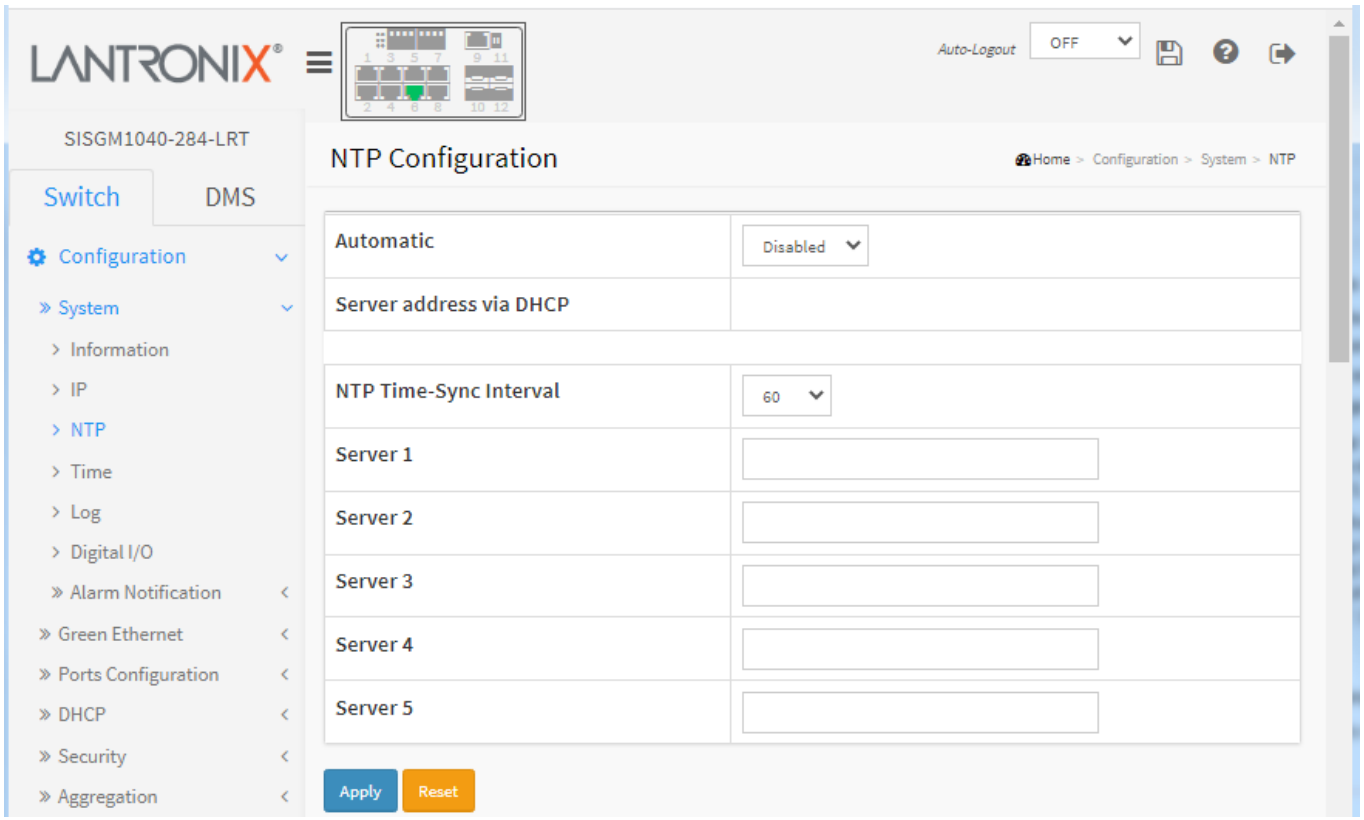
Subnet of VLAN 2 overlaps VLAN 1

Invalid route - address bits outside mask: 0.0.3.44

Invalid IPv4 Address: rt_net_2

Configuration > System > NTP

This page lets you set Network Time Protocol parameters. NTP is a network protocol for synchronizing computer system clocks. NTP uses UDP (datagrams) as its transport layer.



Parameter descriptions:

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

Enabled: NTP servers available from the DHCP.

Disabled: NTP servers available from the config.

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

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

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

Buttons

Apply: Click to save changes.

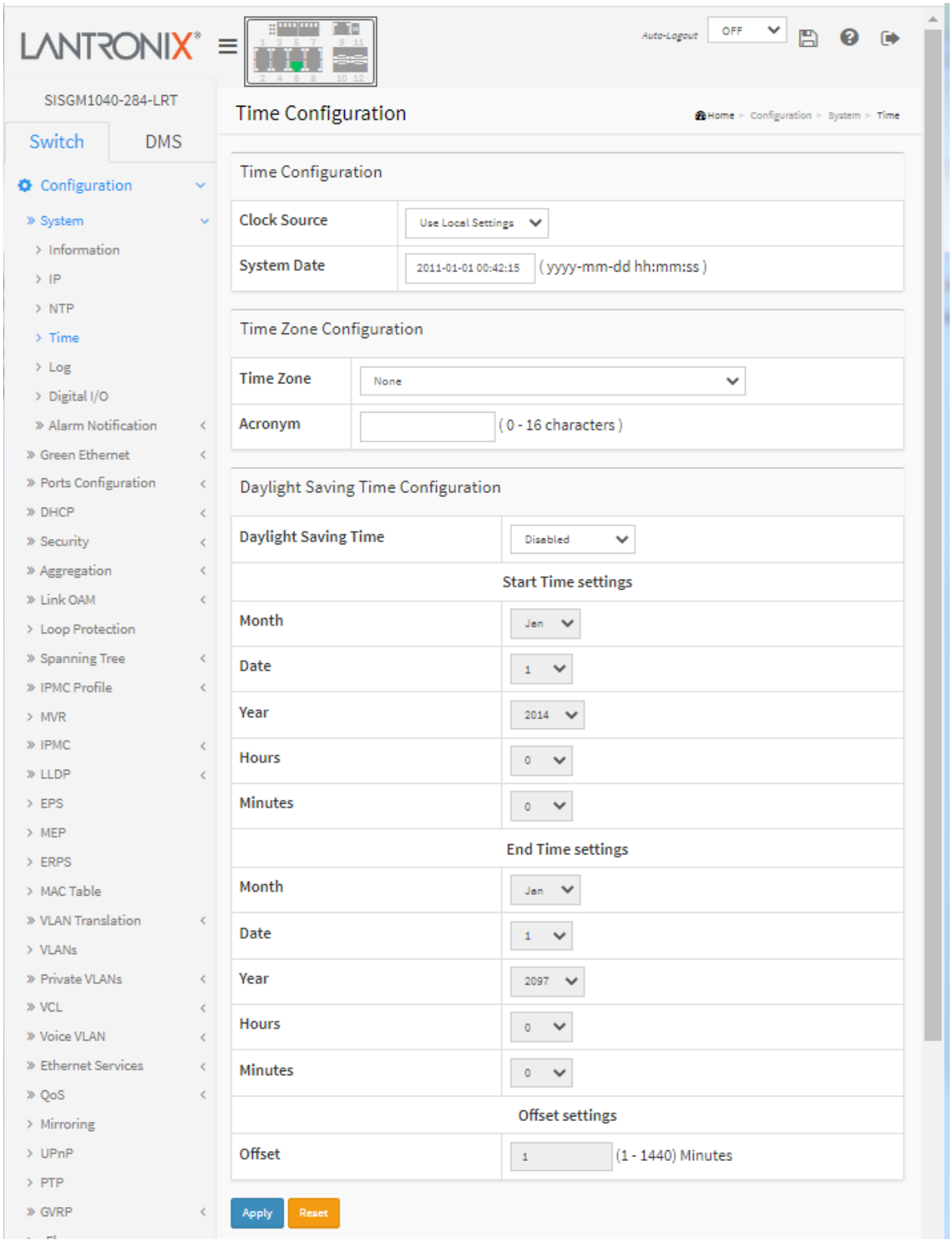
Reset: Click to undo any changes made locally and revert to previously saved values.

Message: *The value of 'Server 1 Address' (https://www.ntppool.org/en/) must be a valid IPv6 address in 128-bit records represented as eight fields of up to four hexadecimal digits with a colon (:) separating each field.*

Message: *The format of Server 1 Address' is invalid. It must be either a valid IP address in dotted decimal notation ('x.y.z.w') or a valid hostname. A valid hostname is a string drawn from the alphabet (A-Z a-z), digits (0-9), dot (.), or hyphen (-). Spaces are not allowed, the first character must be an alphanumeric character, and the first and last characters must not be a hyphen or a dot.*

Configuration > System > Time

This page lets you set system time parameters.



Parameter descriptions:

Time Configuration

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

System Date – Lets you set the current date and time of the system. The year of can be 2011 - 2037.

Time Zone Configuration

Time Zone - Lists various Time Zones worldwide. Select an appropriate Time Zone from the drop down.

Acronym - Set the acronym of the time zone. This is a 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 'Disabled' 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. The default is Disabled.

Recurring Configurations

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 minutes).

Non Recurring Configurations

Start time settings

Month - Select the starting month.
Date - Select the starting date.
Year - Select the starting year.
Hours - Select the starting hour.
Minutes - Select the starting minute.

End time settings

Month - Select the ending month.
Date - Select the ending date.
Year - Select the ending year.
Hours - Select the ending hour.
Minutes - Select the ending minute.

Offset settings

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

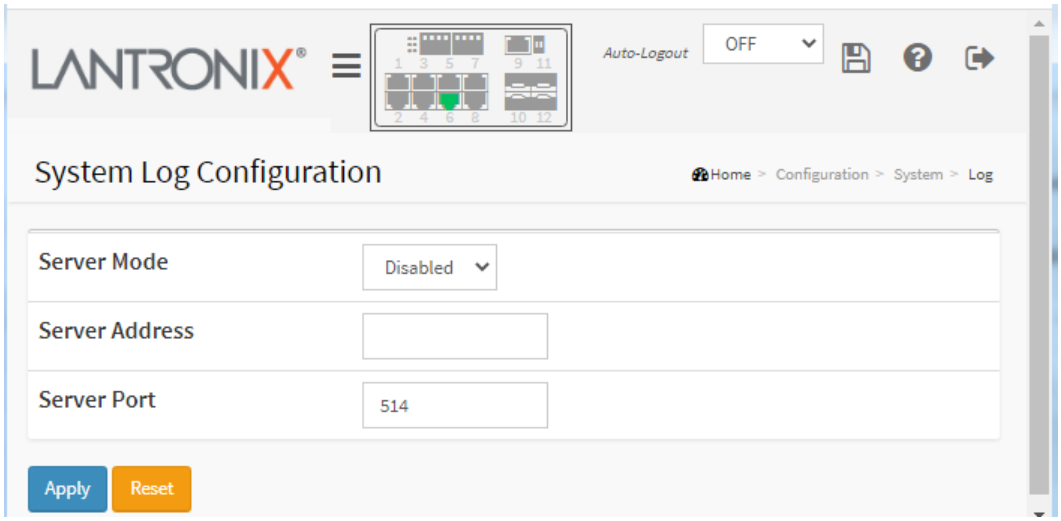
Buttons

Apply: Click to save changes.

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

Configuration > System > Log

This page lets you set syslog server parameters.



Parameter descriptions:

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

Enabled: Enable server mode operation.

Disabled: Disable server mode operation (default).

Server Address: Indicates the IPv4 host address of syslog server. If the switch has the DNS feature enabled, this can also be a domain name.

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

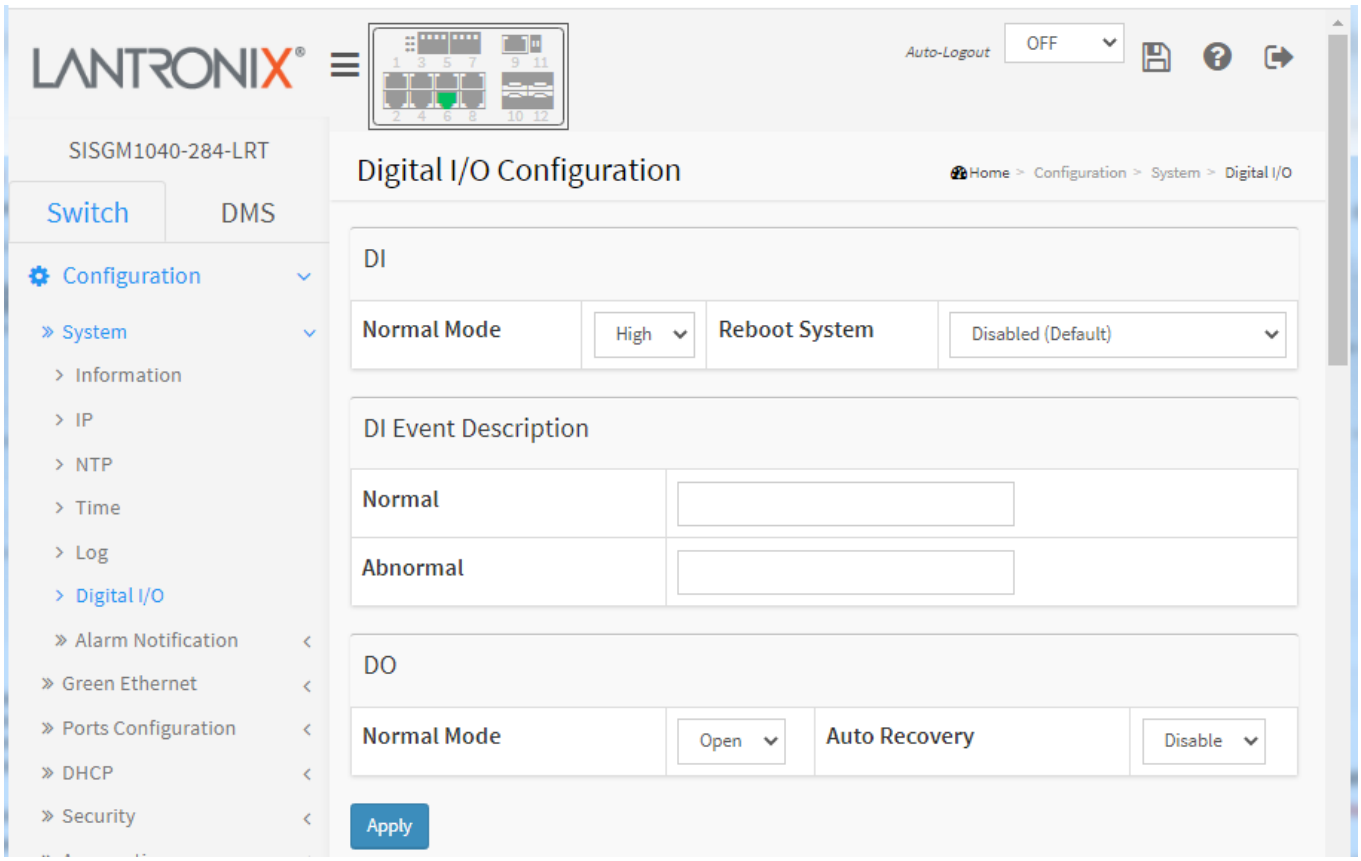
Buttons

Apply: Click to save changes.

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

Configuration > System > Digital I/O

The Digital I/O Configuration page lets you set digital input/output (DI/DO) modes. See the *Install Guide* for more information.



Parameter descriptions:

DI Normal Mode: Set the normal mode of the digital input (DI). You can set it to High or Low. The default is High.

Reboot System : Set the reboot system of the digital input (DI). You can set it to 'Disabled' or 'When DI was changed to abnormal'. The default is Disabled.

DI Event Description: Customize event message. You can describe the Normal and Abnormal events in detail.

DO Normal Mode: Set the normal mode of the digital output (DO). You can set it to Open or Close. The default is Open.

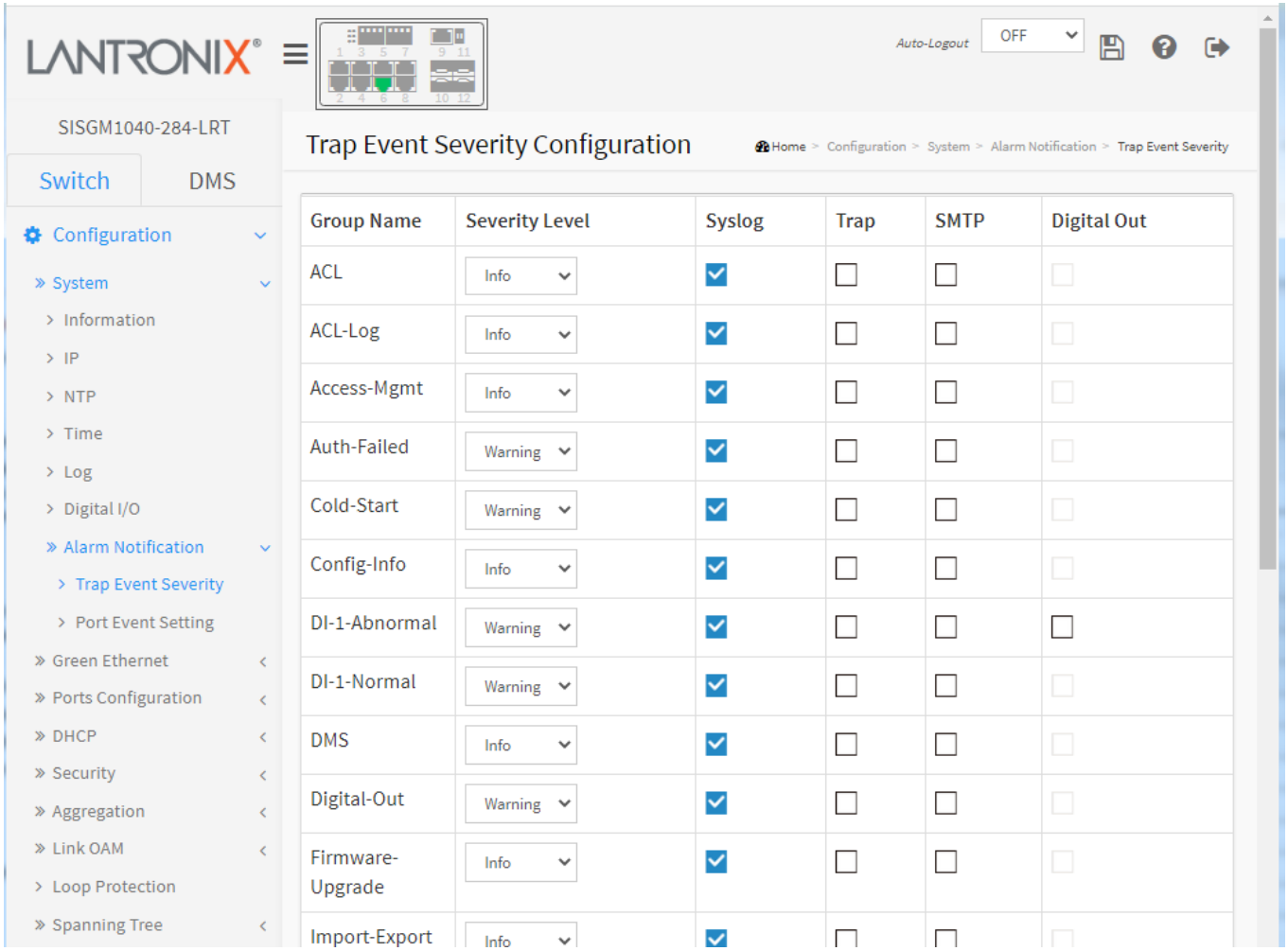
Auto Recovery: Enable the function of Auto Recovery for Digital Output to automatically go back to Normal mode when Digital Input changes back to Normal mode. The default is Disable.

Buttons

Apply: Click to apply changes immediately.

Configuration > System > Alarm Notification > Trap Event Severity

The Trap Event Severity Configuration page lets you set trap event severity levels and methods.



Parameter descriptions:

Group Name: The name identifying the severity group.

Severity Level: Every group has a configurable severity level. These seven levels are supported:

<0> ***Emergency***: System is unusable.

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

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

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

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

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

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

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

Syslog: Enable - Select this Group Name in Syslog.

Trap: Enable - Select this Group Name in Trap.

SMTP: Enable - Select this Group Name in SMTP.

Digital out: Enable - Select this Group Name in Digital Out.

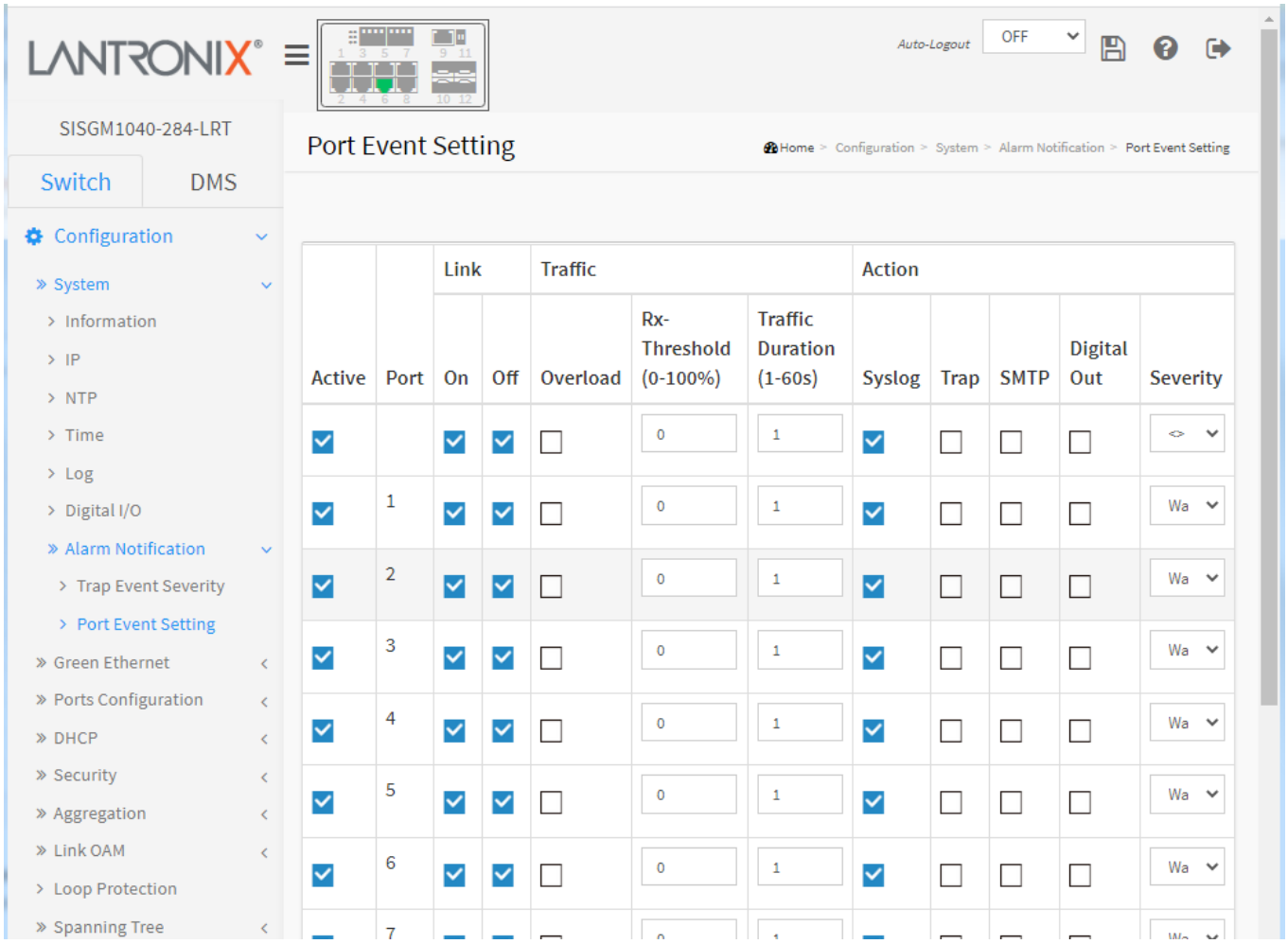
Buttons

Apply: Click to save changes.

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

Configuration > System > Alarm Notification > Port Event Setting

This page lets you set port Link, Traffic, and Action event parameters.



Parameter descriptions:

Active: To active the event handler of this port.

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

Link On: Event is triggered when link on.

Link Off: Event is triggered when link off.

Traffic Overload: Event is triggered when the traffic is overload.

Traffic Rx-Threshold (0-100%): Event is triggered when Rx reach this threshold.

Traffic Duration (0-60s): Event is triggered when the traffic duration reaches this value.

Action Syslog: Enable this port for Syslog.

Action Trap: Enable this port for Trap.

Action SMTP: Enable this port for SMTP.

Action Digital Out: Enable this port for Digital Out.

Severity: Every port has a configurable severity level. These seven levels are supported:

<0> ***Emergency***: System is unusable.

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

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

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

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

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

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

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

Buttons

Apply: Click to save changes.

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

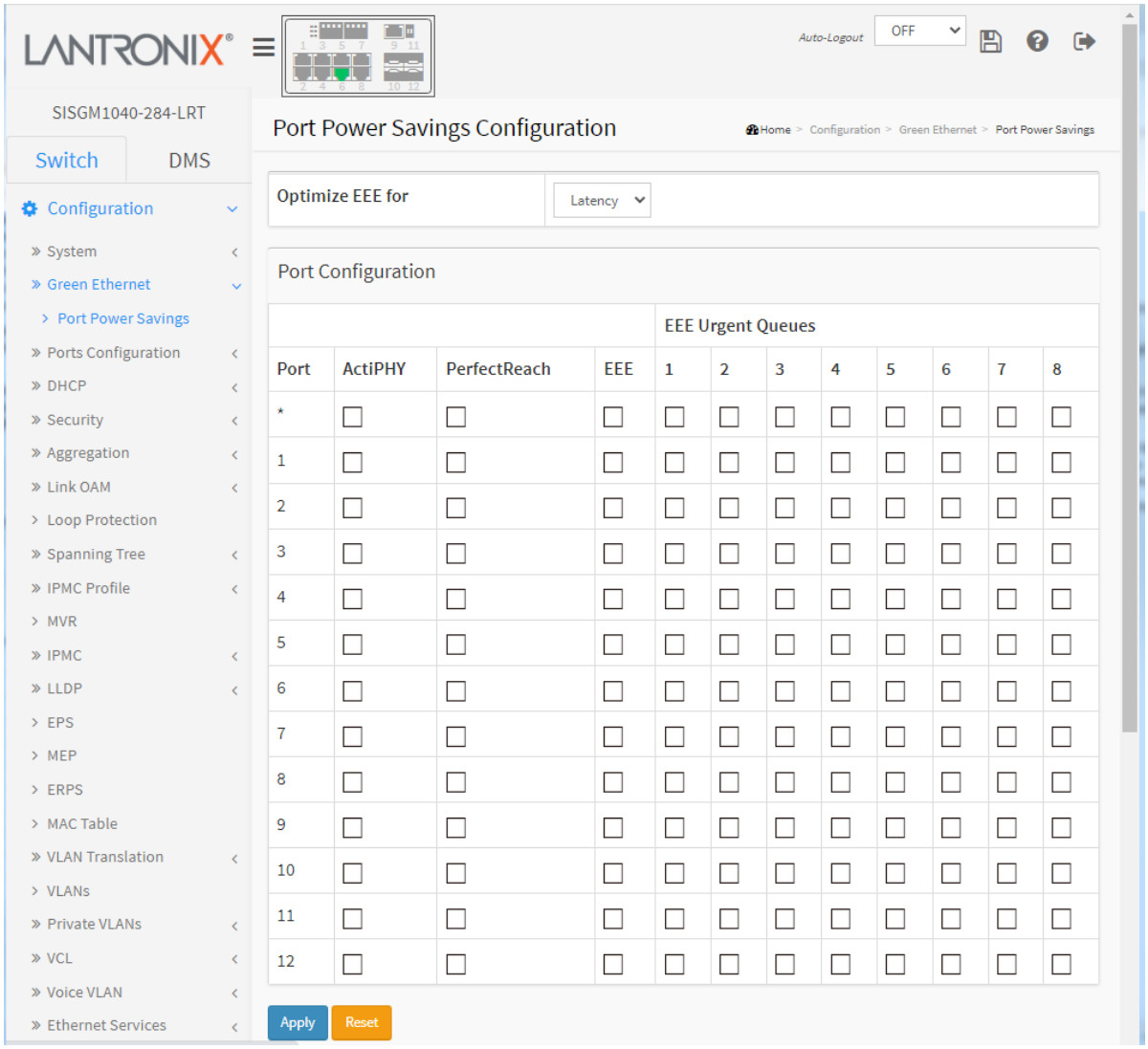
Configuration > Green Ethernet > Port Power Savings

The Port Power Savings Configuration page lets you set the port power savings parameters.

EEE (Energy Efficient Ethernet) is a power saving option that reduces the power usage when there is low or no traffic utilization. EEE works by powering down circuits when there is no traffic. When a port gets data to be transmitted all circuits are powered up. The time it takes to power up the circuits is named wakeup time. The default wakeup time is 17 us for 1Gbit links and 30 us for other link speeds. EEE devices must agree on the value of the wakeup time in order to make sure that both the receiving and transmitting device has all circuits powered up when traffic is transmitted. The devices can exchange wakeup time information using LLDP.

EEE works for ports in auto-negotiation mode, where the port is negotiated to either 1G or 100 Mbit full duplex mode. For ports that are not EEE-capable, the corresponding EEE checkboxes are grayed out and thus impossible to enable EEE for.

When a port is powered down for saving power, outgoing traffic is stored in a buffer until the port is powered up again. Because there is some overhead in turning the port down and up, more power can be saved if the traffic can be buffered up until a large burst of traffic can be transmitted. Buffering traffic will give some latency in the traffic.



Parameter descriptions:

Optimize EEE for: The switch can be set to optimize EEE (Energy Efficient Ethernet) for either:

Power: best power saving.

Latency: least traffic latency (default).

Port Configuration

Port: The switch port number of the logical port.

ActiPHY: Link down power savings enabled. ActiPHY works by lowering the power for a port when there is no link. The port is power up for short moment in order to determine if cable is inserted.

PerfectReach: Cable length power savings enabled. PerfectReach works by determining the cable length and lowering the power for ports with short cables.

EEE: Controls whether EEE is enabled for this switch port. For maximizing power savings, the circuit isn't started at once transmit data is ready for a port but is instead queued until a burst of data is ready to be transmitted. This will give some traffic latency.

If desired it is possible to minimize the latency for specific frames, by mapping the frames to a specific queue (done with QOS), and then mark the queue as an urgent queue. When an urgent queue gets data to be transmitted, the circuits will be powered up at once and the latency will be reduced to the wakeup time.

EEE Urgent Queues: Queues set will activate transmission of frames as soon as data is available. Otherwise the queue will postpone transmission until a burst of frames can be transmitted.

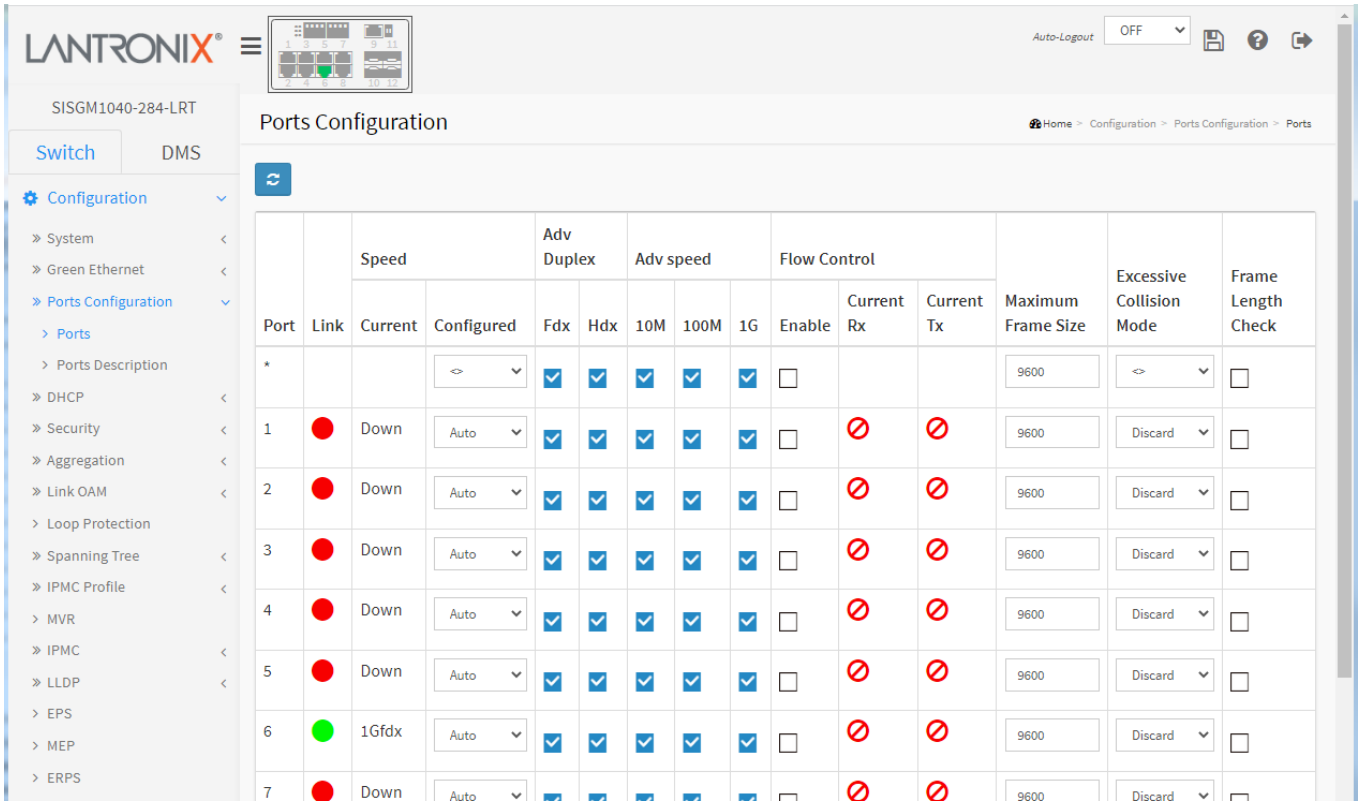
Buttons

Apply: Click to save changes.

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

Configuration > Ports Configuration > Ports

This page lets you set port parameters such as Duplex, Speed, Flow Control, MTU, etc.



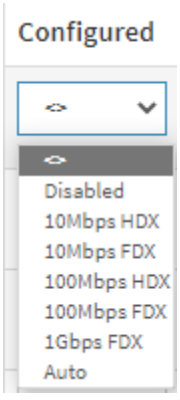
Parameter descriptions:

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 is shown. Possible speeds are:



Disabled - Disables the switch port operation.

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

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

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

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

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

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

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

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

Maximum Frame Size: Enter the maximum frame size allowed for the switch port, including FCS. The range is 1518-9600 bytes.

Excessive Collision Mode: Configure port transmit collision behavior:

Discard: Discard frame after 16 collisions (default).

Restart: Restart backoff algorithm after 16 collisions.

Frame Length Check: Configures if frames with incorrect frame length in the EtherType/Length field 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). If "frame length check" is enabled, frames with payload size less than 1536 bytes are dropped, if the EtherType/Length field doesn't match the actual payload length. If "frame length check" is disabled, frames are not dropped due to frame length mismatch. **Note**: No drop counters count frames dropped due to frame length mismatch

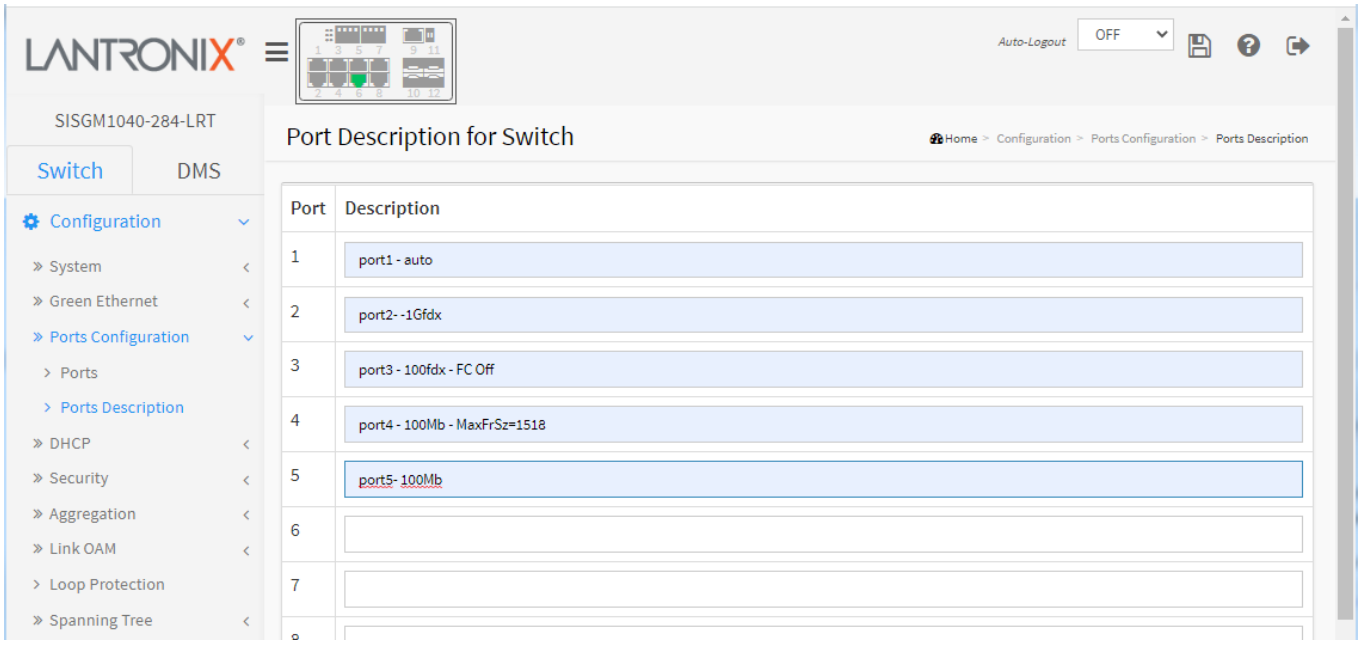
Buttons

Apply: Click to save changes.

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

Configuration > Ports Configuration > Ports Description

This page lets you describe each port.



Parameter descriptions:

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

Description: Enter up to 128 characters as a descriptive name to identify this port.

Buttons

Apply: Click to save changes.

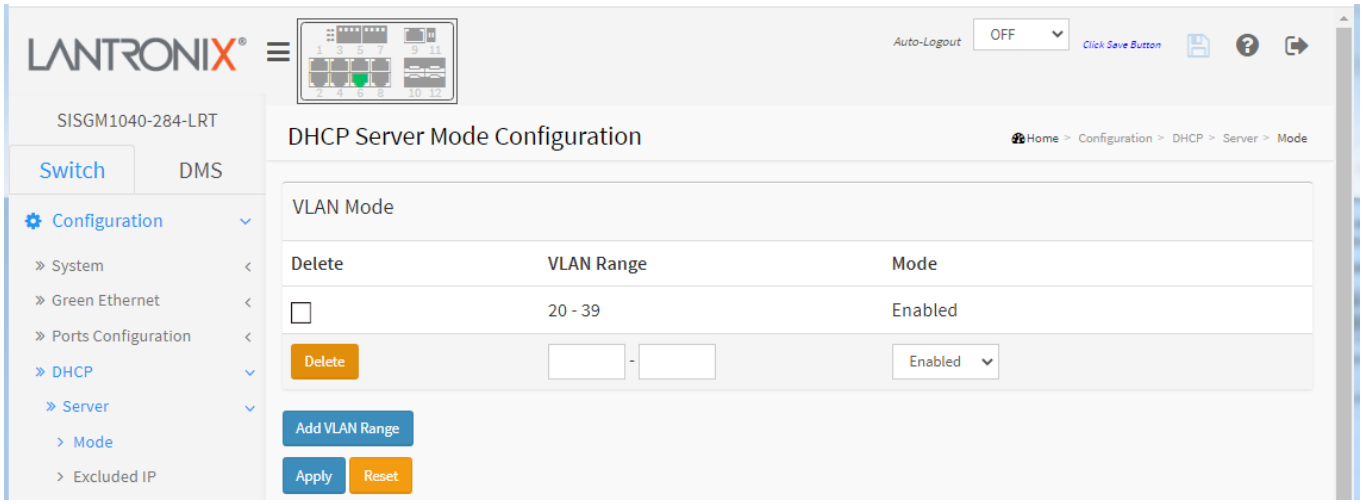
Reset: Click to undo any changes made locally and revert to previously saved values.

Configuration > DHCP > Server > Mode

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

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

From the default page, click the Add VLAN Range button to display the DHCP Server Mode Configuration table:



Parameter descriptions:

VLAN Mode: Configure operation mode to enable/disable DHCP server per VLAN.

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, to disable existed VLAN range, follow the steps.

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

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

Enabled: Enable DHCP server per VLAN.

Disabled: Disable DHCP server per VLAN.

Buttons

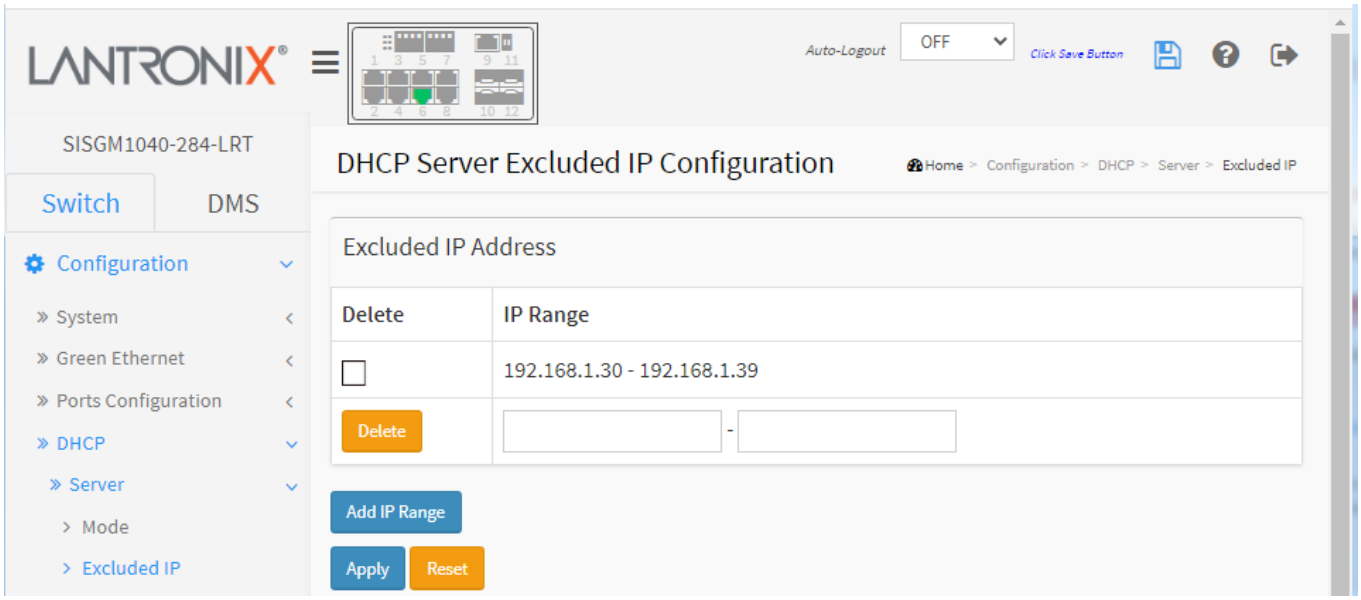
Add VLAN Range: Click to add a new VLAN range.

Apply: Click to save changes.

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

Configuration > DHCP > Server > Excluded IP

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



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 address or both.

Buttons

Delete : Click to immediately remove the entry from the table.

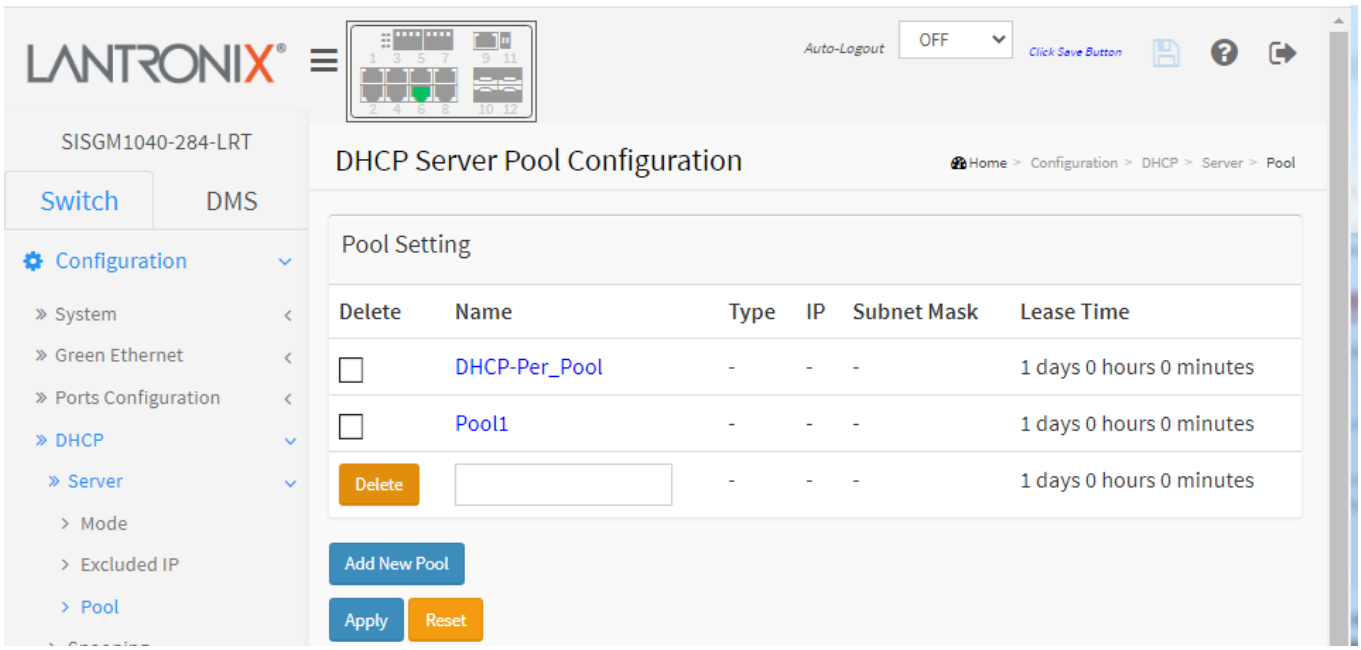
Add IP Range: Click to add a new excluded IP range.

Apply: Click to save changes.

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

Configuration > DHCP > Server > Pool

This page lets you configure DHCP pools. According to the DHCP pool, a DHCP server will allocate an IP address and deliver configuration parameters to a DHCP client.



Parameter descriptions:

Pool Setting: Add or delete pools. Adding a pool and giving a name creates a new pool with "default" configuration. To configure all settings including type, IP subnet mask and lease time, click the pool name to go to the configuration page (see below).

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

Type: Display which type of the pool is.

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

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

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

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

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

Lease Time: Display lease time of the pool. The default is 1 days 0 hours 0 minutes.

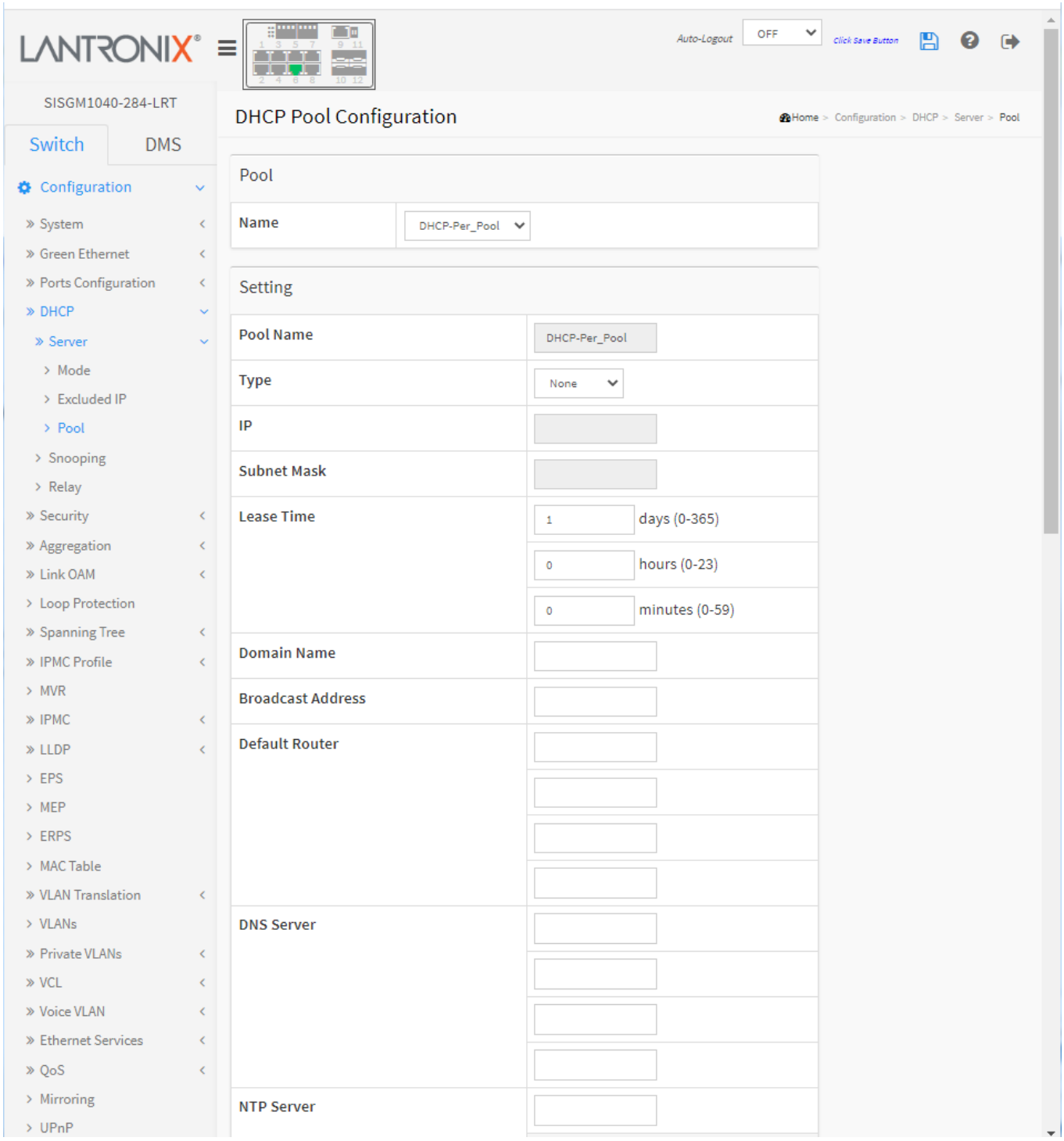
Buttons

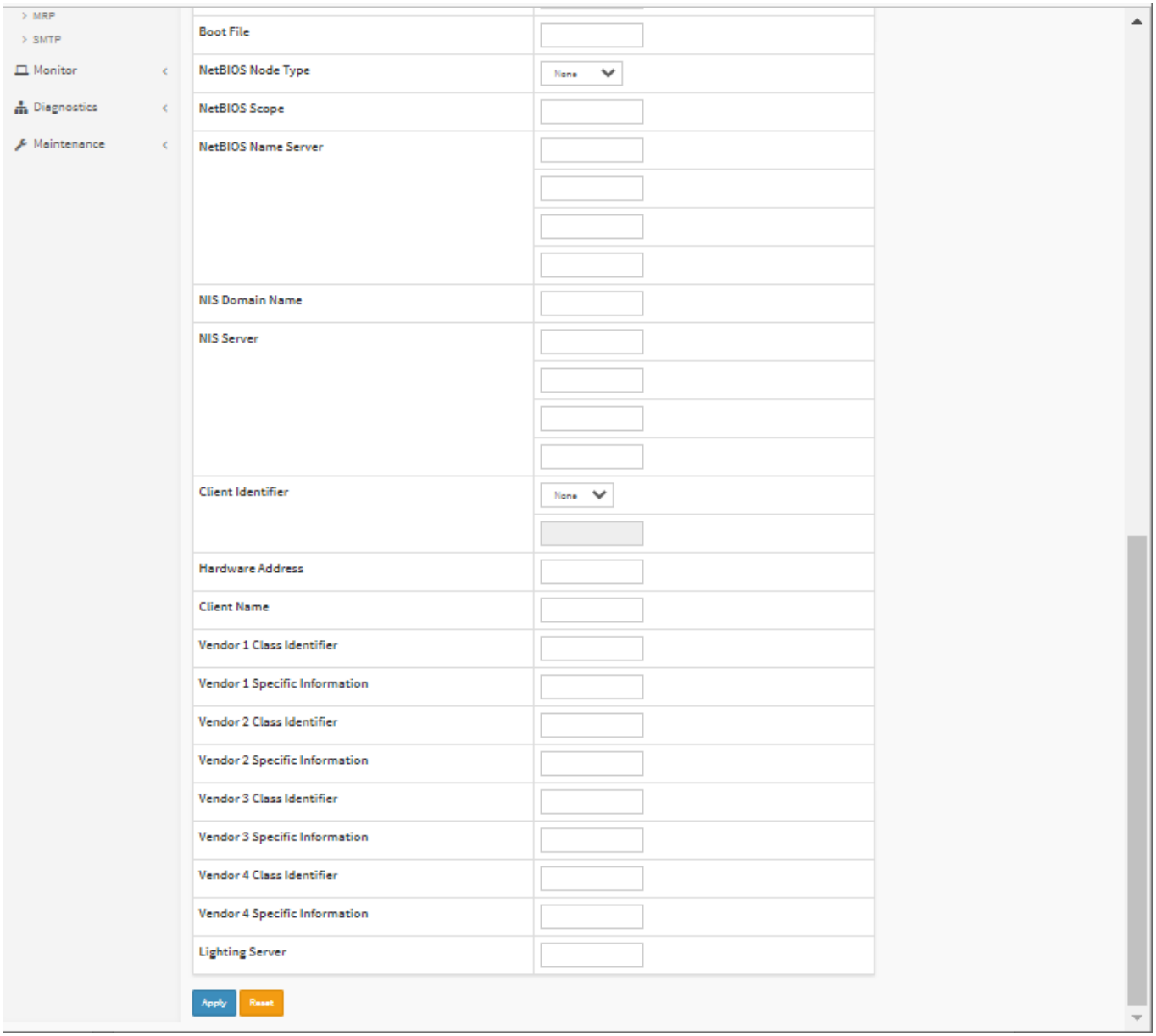
Add New Pool: Click to add a new excluded IP range.

Apply: Click to save changes.

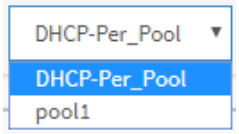
Reset: Click to undo any changes made locally and revert to previously saved values.

Click on a linked Pool Name to display its DHCP Pool Configuration page to configure all DHCP pool parameters.





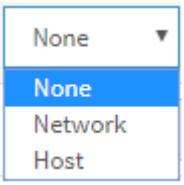
Parameter descriptions:



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 the pool is (None, Network, or Host).

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.

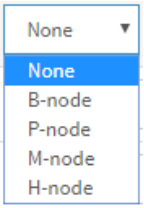
Default Router: DHCP option 3. Specify a list of IP addresses for routers on the client's subnet.

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 IETF RFC 1001/1002.

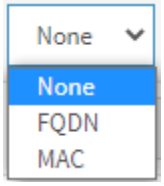
NetBIOS Scope: DHCP option 47. Specify the NetBIOS over TCP/IP scope parameter for the client as specified in RFC 1001/1002.

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. At the dropdown select None, FQDN, or MAC. The default is None.



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

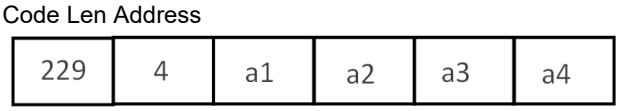
Lighting Server: DHCP option 229. Specify a lighting server available to the client. (Added at FW v7.20.0106.)

This feature should be enabled for any ports used for lighting nodes as it significantly reduces the delay time between when a lighting node is connected to a port and when the switch allows network communication from the lighting node to the lighting gateway.

Note: If multicast traffic is not allowed on your network, you can configure the network DHCP server to pass the lighting gateway server IP address in DHCP Option 229 (added at FW v7.20.0106).

With the switch acting as DHCP Server, it will insert operation 229 into DHCP offer packets and DHCP ACK packets. After receiving DHCP discover packets, it will insert option 229 for all DHCP clients as long as the DHCP Server is configured with Option 229. This option is configurable via the Web UI, SNMP, and CLI.

The code for this option is 229, and its length is 4 octets:



For DHCP packet content, Option 229 is inserted between the last and before option 255.

Buttons

Apply: Click to save changes.

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

Messages:

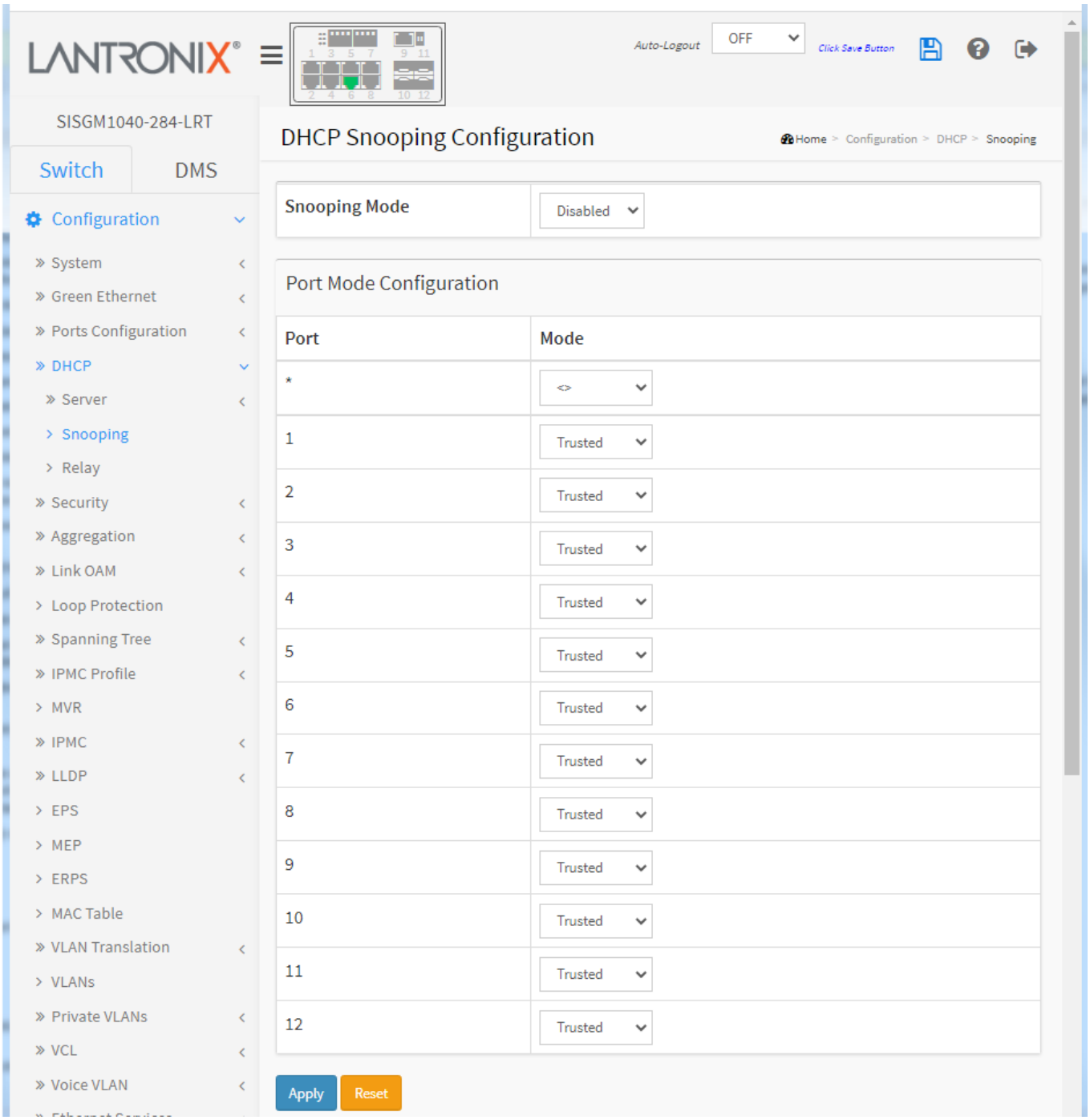
Pool type is defined so subnet mask must be inputted.

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

Invalid Vendor 1 Specific Information. It must be a HEX string and begin with '0x' or '0X'.

Configuration > DHCP > Snooping

This page lets you set DHCP Snooping parameters. DHCP Snooping is used to block intruder on the untrusted ports of the switch device when it tries to intervene by injecting a bogus DHCP reply packet into a legitimate conversation between the DHCP client and server.



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

Enabled: Enable DHCP snooping mode operation. When DHCP snooping mode 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

Mode: 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.

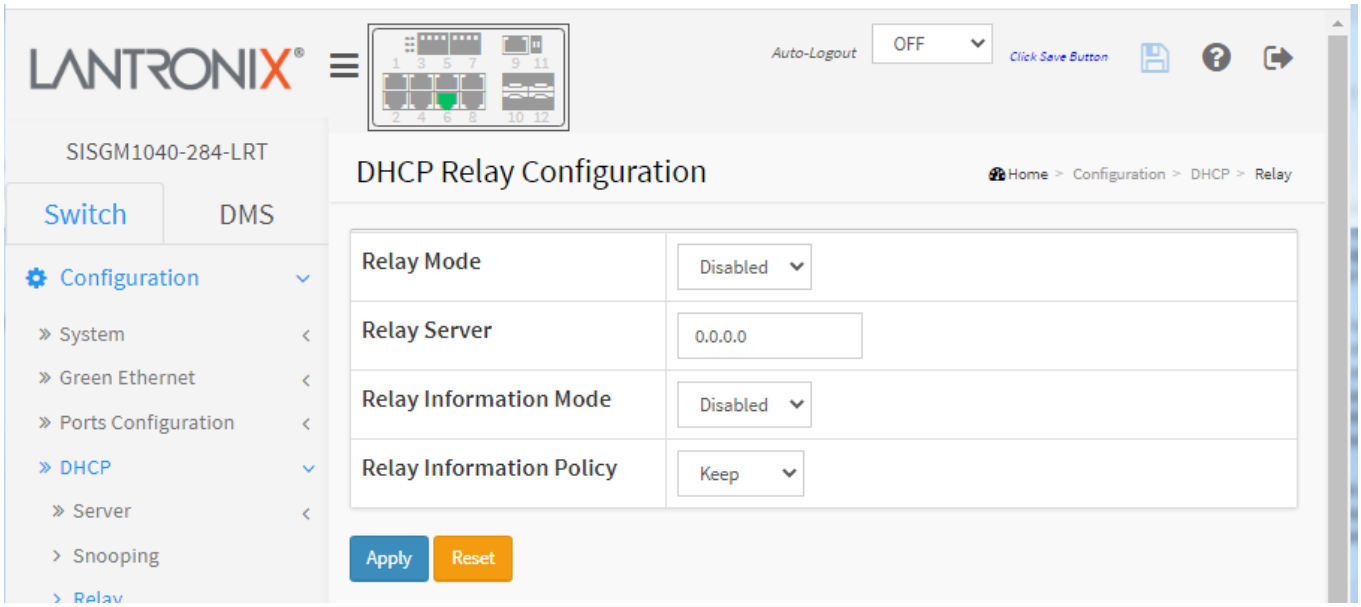
Configuration > DHCP > Relay

This page lets you set DHCP Relay parameters.

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.

DHCP option 82 enables a DHCP relay agent to insert specific information into a DHCP request packets when forwarding client DHCP packets to a DHCP server and remove the specific information from a DHCP reply packets when forwarding server DHCP packets to a DHCP client. The DHCP server can use this information to implement IP address or other assignment policies. Specifically, the option works by setting two sub-options: Circuit ID (option 1) and Remote ID (option2). The Circuit ID sub-option is supposed to include information specific to which circuit the request came in on. The Remote ID sub-option was designed to carry information relating to the remote host end of the circuit.

A Circuit ID is 4 bytes in length and the format is "vlan_id" "module_id" "port_no". The parameter of "vlan_id" is the first two bytes represent the VLAN ID. The parameter of "module_id" is the third byte for the module ID (always 0). The parameter of "port_no" is the fourth byte and it means the port number. The Remote ID is 6 bytes in length, and the value is equal the DHCP relay agents MAC address.



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 as "[vlan_id][module_id][port_no]". The first four characters represent the VLAN ID, the fifth and sixth characters are the module ID (always 0), and the last two characters are the port number. For example, "00030108" means the DHCP message receive form VLAN ID 3, switch ID 1, port No 8. And the option 82 remote ID value is equal the switch MAC address.

Possible modes are:

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

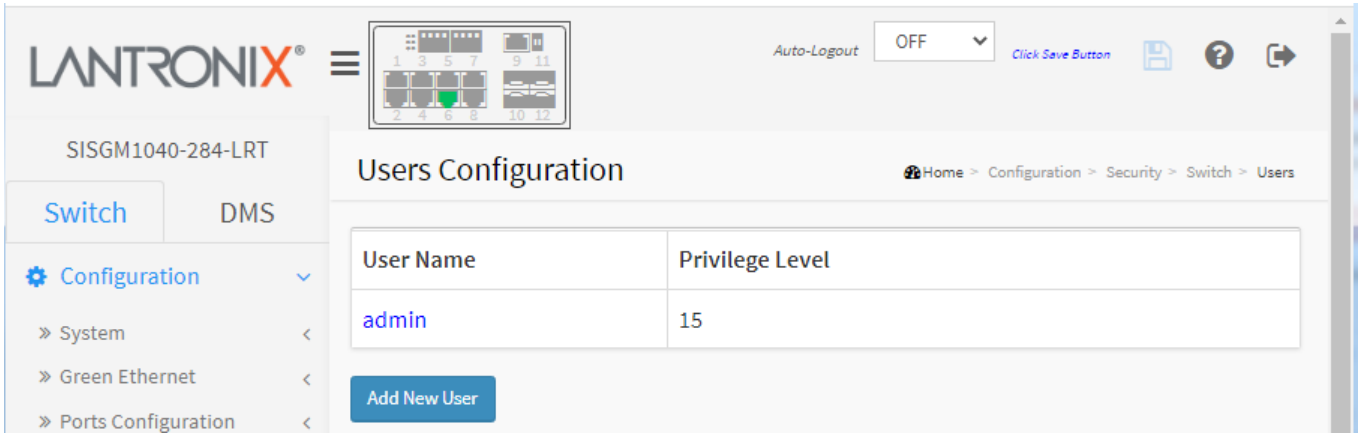
Apply: Click to save changes.

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

Messages: *Please make sure the DHCP server connected on trust port?*

Configuration > Security > Switch > Users

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



Parameter descriptions:

User Name: The name identifying the user. This is also a link to Add a new user or Edit an existing User.

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 other values must refer to each group privilege level. User's privilege should be same as or greater than the group privilege level to have the access of that group. By default setting, most groups privilege level 5 has read-only access, and privilege level 10 has read-write access. System maintenance (software upload, factory defaults etc.) needs user privilege level 15.

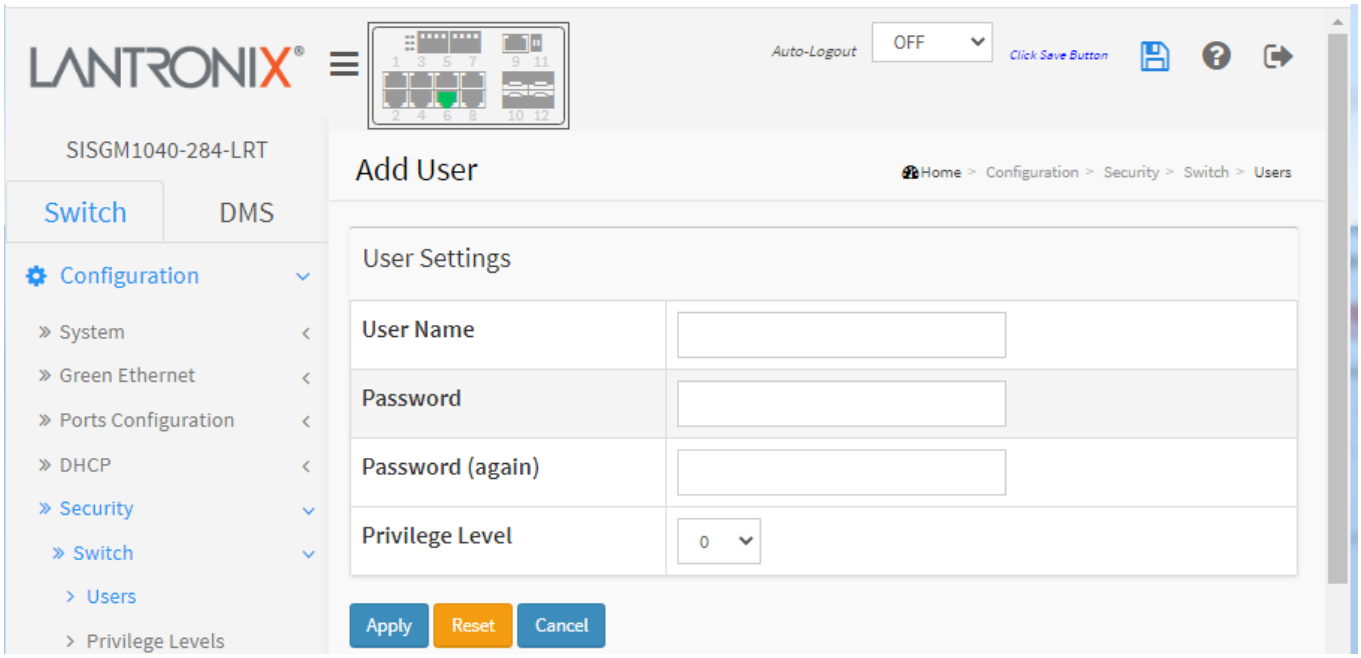
Generally, the privilege level 15 can be used for an administrator account, privilege level 10 for a standard user account and privilege level 5 for a guest account.

Buttons

Add New User: Click to add a new user (see below).

Add a User

Click the Add New User button to display the Add User page where you can set a new user's parameters.



User Name: A string identifying the user name that this entry should belong to. The allowed string length is 1 to 31 characters. The valid user name allows letters, numbers and underscores.

Password: The password of the user. The allowed string length is 0 to 31 characters. Any printable characters including space are accepted.

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 other values must refer to each group privilege level. User's privilege should be same or greater than the group privilege level to have the access of that group. By default setting, most groups privilege level 5 has read-only access, and privilege level 10 has read-write access. And the system maintenance (software upload, factory defaults 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 Privilege Level 0.

Buttons

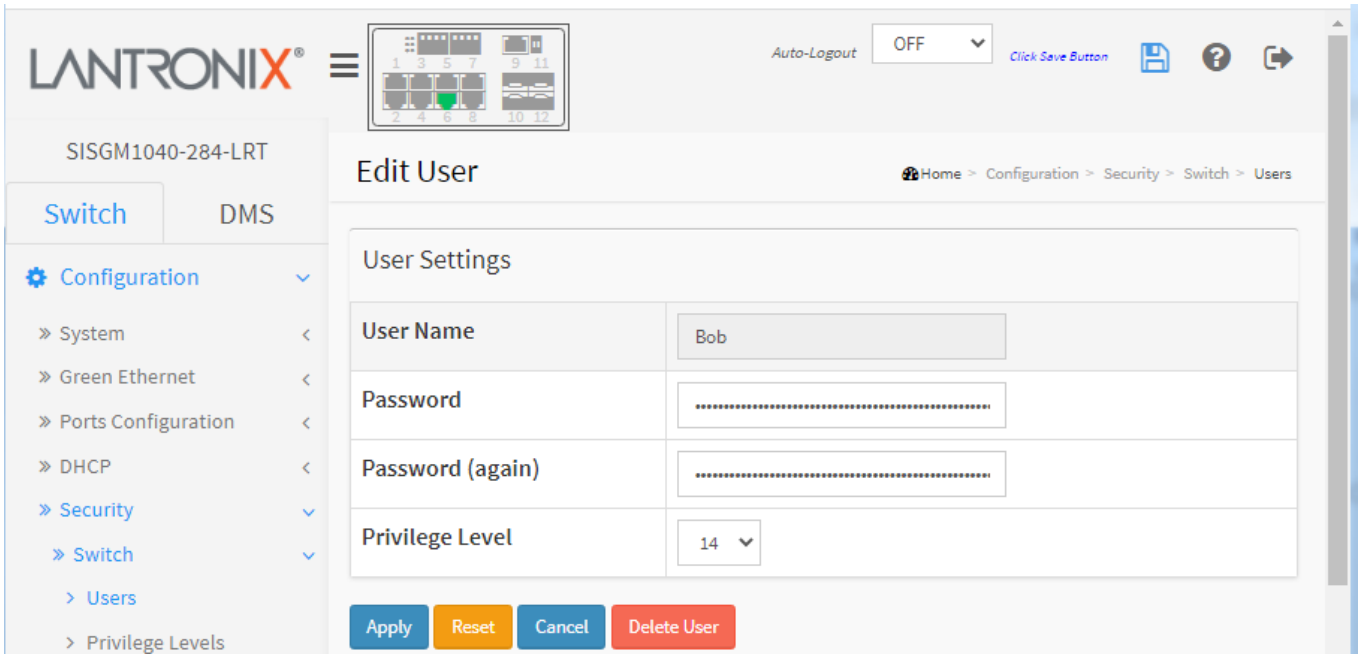
Apply: Click to save changes.

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 page.

Edit / Delete User

Click on a linked User Name to display the Edit User page. This page lets you configure a user's parameters.



User Name: A string identifying the user name that this entry should belong to. The allowed string length is 1 - 31 characters. The valid user name allows letters, numbers and underscores.

Password: The password of the user. The allowed string length is 0 to 31 characters. Any printable characters including the space character are accepted.

Password (again): The password of the user. Must match the previous Password entry.

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 other values must refer to each group privilege level. User's privilege should be same or greater than the group privilege level to have the access of that group. By default setting, most groups privilege level 5 has read-only access, and privilege level 10 has read-write access. And the system maintenance (software upload, factory defaults 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 Privilege Level 15.

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

Buttons

Apply: Click to save changes.

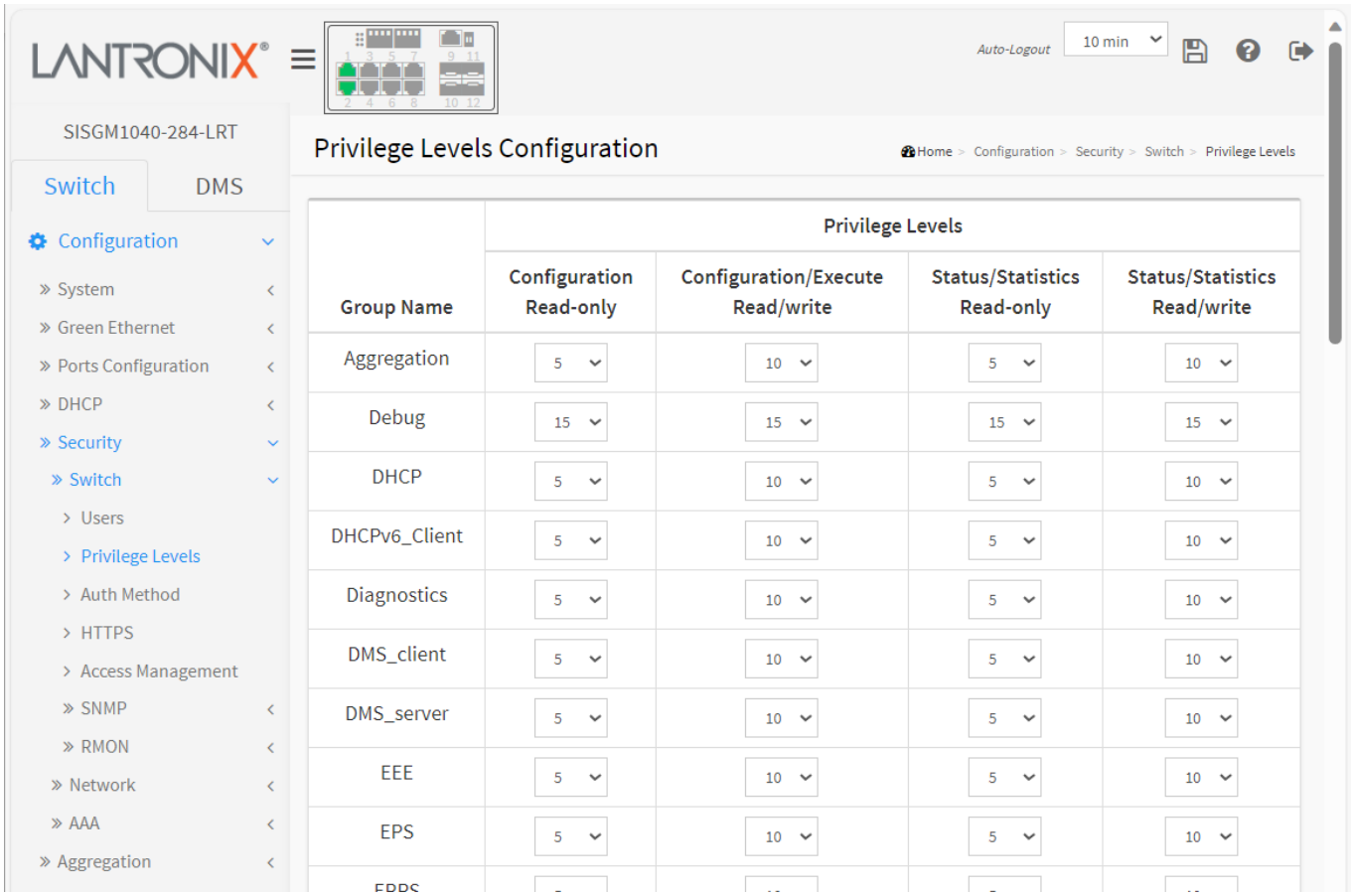
Reset: Click to undo any changes made locally and revert to previously saved values.

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

Delete User: Delete the current user. This button is not available for new configurations (Add new user).

Configuration > Security > Switch > Privilege Levels

This page lets you set the privilege levels for modules/groups of modules.



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

System: Contact, Name, Location, 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 levels are listed below in order of most to least privileges:

- Configuration/Execute Read/write
- Configuration Read-only
- Status/Statistics Read/write
- Status/Statistics Read-only

Buttons

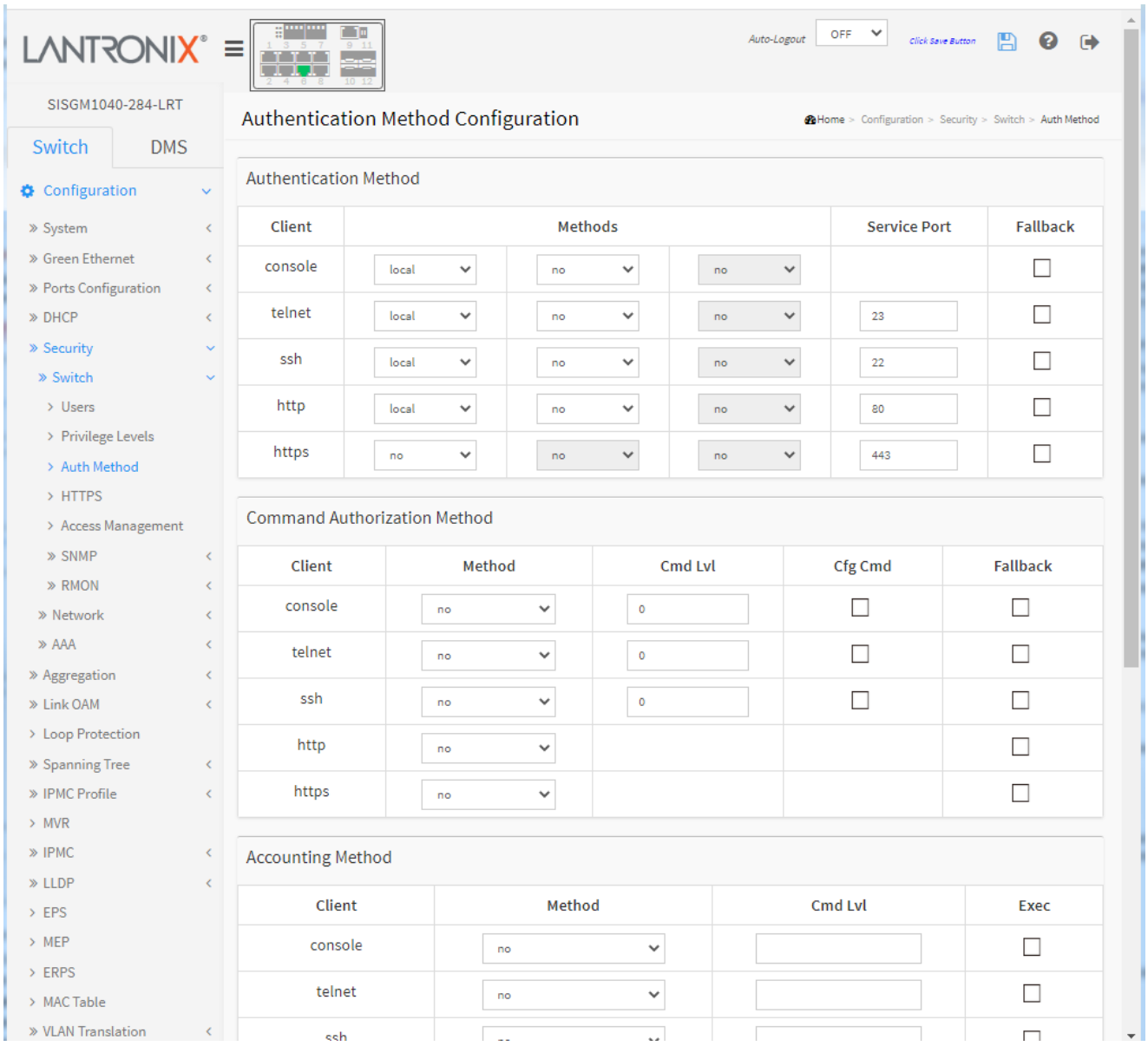
Apply: Click to save changes.

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

Message: *Insufficient Privilege Level The web page is non-accessible. Please use the valid privilege level*.
Meaning: Insufficient Privilege Level Help: The privilege level is insufficient.
Recovery: Please use the valid privilege level at Configuration > Security > Switch > Users.

Configuration > Security > Switch > Auth Method

This page lets you configure how a user is authenticated when they log into the switch via one of the management client interfaces. The table has one row for each client type and several columns.



Authentication Method:

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

Methods: Set to one of these values:

no: Authentication is disabled and login is not possible.

redirect: When HTTPS is enabled, enable HTTPS automatic redirect on the switch.

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

radius: Use remote RADIUS server(s) for authentication.

tacacs: Use remote TACACS+ server(s) for authentication.

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

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

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

Command Authorization Method: This section lets you limit the CLI commands available to a user. The table has one row for each client type and several columns:

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

Method: Set to one of these values:

no: Command authorization is disabled. User has access to CLI commands according to his privilege level.

tacacs: Use remote TACACS+ server(s) for command authorization. If all remote servers are offline, the user is granted access to CLI commands according to his privilege level.

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

Cfg Cmd: Also authorize configuration commands.

Fallback: This function is an auxiliary function of Authorization. When the device cannot communicate with a TACACS+ Server normally, it will check for the right permission level of the Local Account to execute the Authorization.

Accounting Method: This section lets you configure command and exec (login) accounting. The table has one row for each client type and several columns:

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

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

no: Accounting is disabled.

tacacs: Use remote TACACS+ server(s) for accounting.

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

Exec: Enable exec (login and logout) accounting.

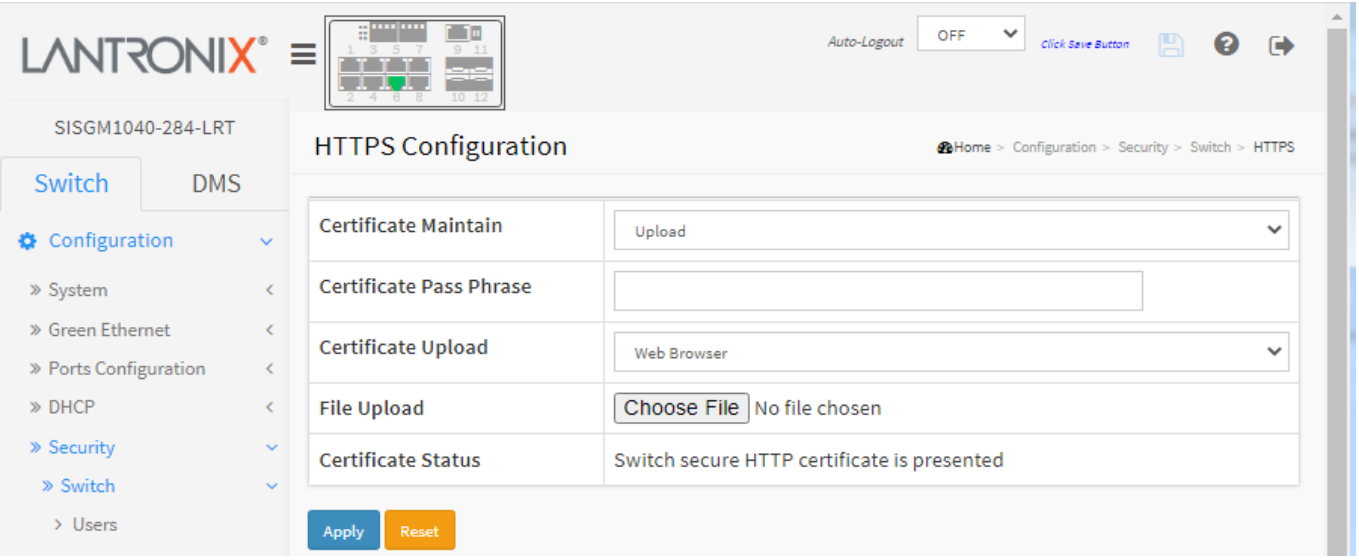
Buttons

Apply: Click to save changes.

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

Configuration > Security > Switch > HTTPS

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



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

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

Generate: Generate a new self-signed RSA certificate.

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

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

Web Browser: Upload a certificate via a 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 (-), and underscore (_). The maximum length is 63 and hyphen must not be first character. The file name content that only contains '.' is not allowed.

File Upload: Click the Choose File button and browse to and select the desired file.

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

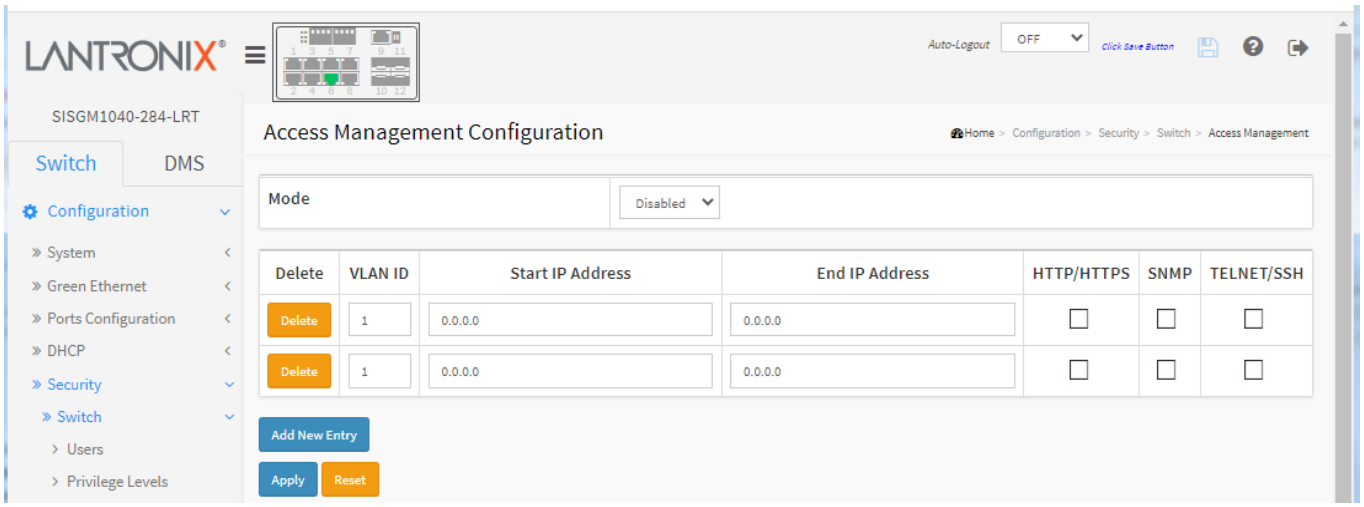
Switch secure HTTP certificate is presented.

Switch secure HTTP certificate is not presented.

Switch secure HTTP certificate is generating ....

Configuration > Security > Switch > Access Management

Configure access management table parameters on this page. The maximum number of entries is 16. If the application's type matches any one of the access management entries, it will allow access to the switch.



Parameter descriptions:

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

Enabled: Enable access management mode operation.

Disabled: Disable access management mode operation.

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

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

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

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

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

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

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

Buttons

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

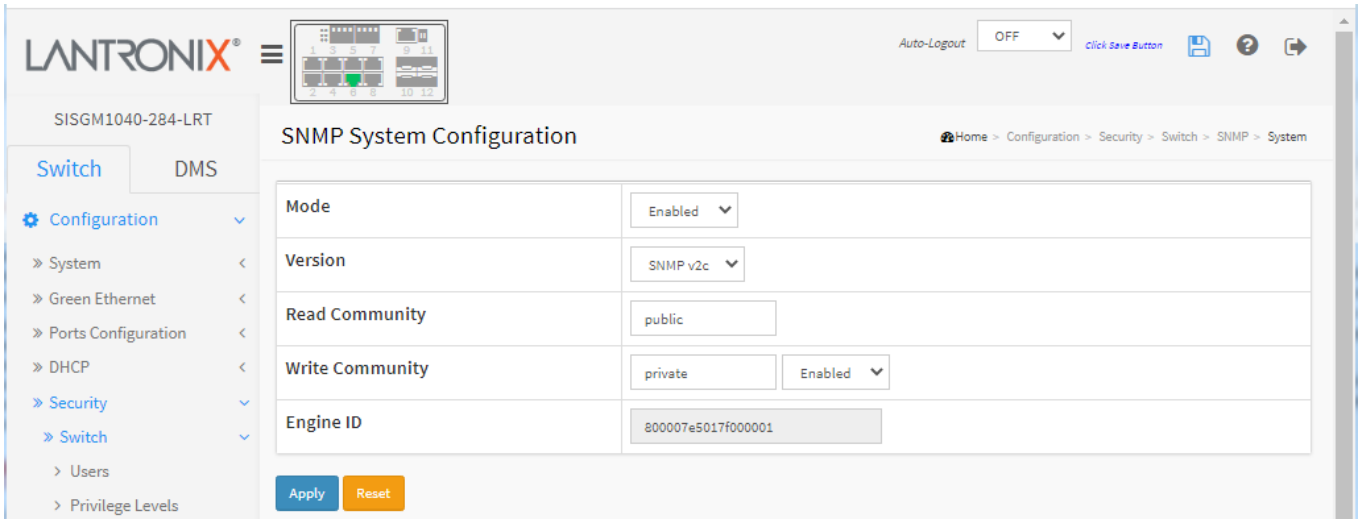
Apply: Click to apply changes immediately.

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

Configuration > Security > Switch > SNMP > System

This page lets you configure SNMP mode, version, community names, and engine ID. 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.

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 is a protocol that is used to govern the transfer of information between SNMP manager and agent and traverses the Object Identifier (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.



Parameter descriptions:

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

Enabled: Enable SNMP mode operation.

Disabled: Disable SNMP mode operation.

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

SNMP v1: Set SNMP supported version 1.

SNMP v2c: Set SNMP supported version 2c.

SNMP v3: Set SNMP supported version 3.

Read Community: Indicates the community read access string to permit access to SNMP agent. The allowed string length is 0 – 255 characters, and the allowed content is the ASCII characters 33 - 126. This field is applicable only when SNMP version is SNMPv1 or SNMPv2c. If SNMP version is SNMPv3, the community string will be associated with SNMPv3 communities table. 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 – 255 characters, and the allowed content is ASCII characters 33 - 126.

Enabled: Enable SNMP write community operation.

Disabled: Disable SNMP write community operation. This field is applicable only when SNMP version is SNMPv1 or SNMPv2c. If SNMP version is SNMPv3, the community string will be associated with SNMPv3 communities table. 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. Changing the Engine ID will clear all original local users.

Buttons

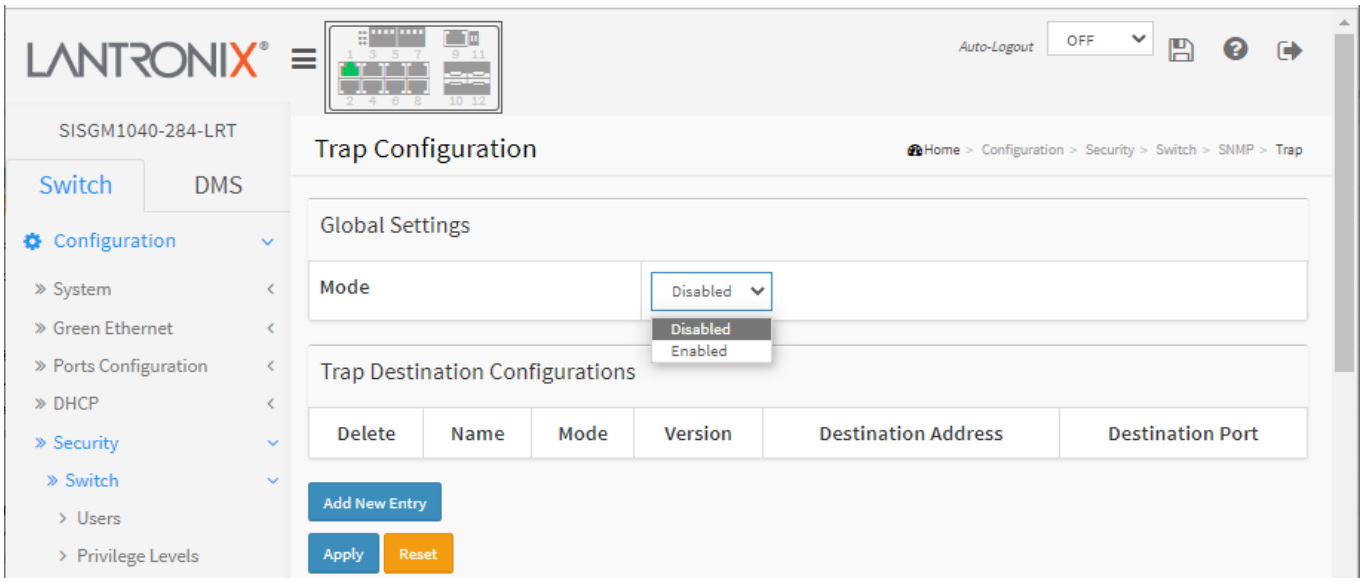
Add New Entry: Click to add a new access management entry.

Apply: Click to apply changes immediately.

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

Configuration > Security > Switch > SNMP > Trap

Configure SNMP traps on this page.



Global Settings: Configure SNMP trap on this page.

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

Enabled: Enable SNMP trap mode operation.

Disabled: Disable SNMP trap mode operation.

Trap Destination Configurations: Configure trap destinations on this page.

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

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

TCP: Enable TCP SNMP trap mode operation.

UDP: Enable UDP SNMP trap mode operation.

Disabled: Disable SNMP trap mode operation (default).

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

SNMPv1: Set SNMP trap supported version 1.

SNMPv2c: Set SNMP trap supported version 2c.

SNMPv3: Set SNMP trap supported version 3.

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'.

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

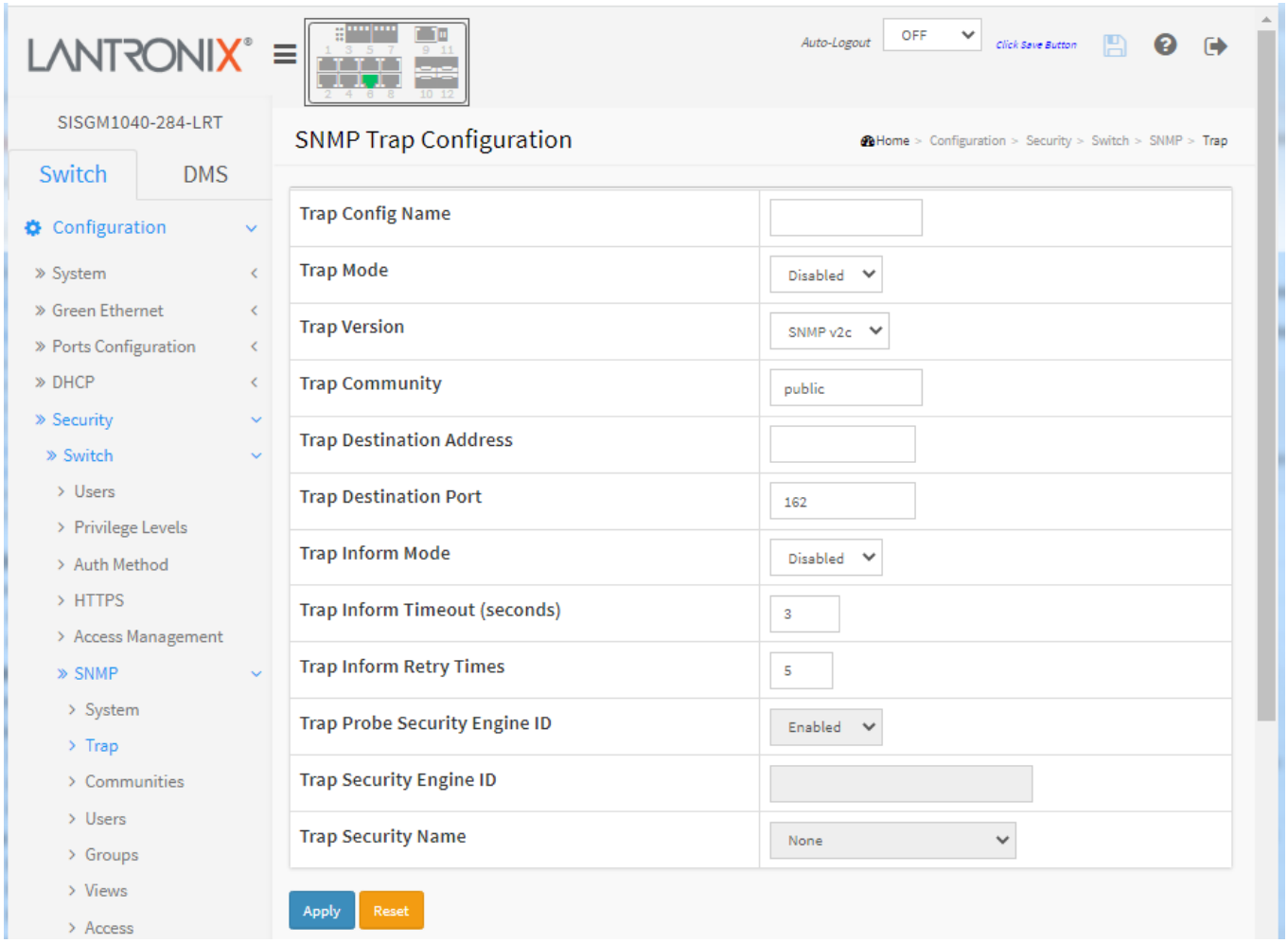
Buttons

Add New Entry: Click to add a new trap.

Apply: Click to apply changes immediately.

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

From the default page select Mode = Enabled and then click the Add New Entry button to display the SNMP Trap Configuration page:



Trap Config Name: Indicates which trap Configuration's name for configuring. The allowed string length is 1-32 characters, and the allowed content is ASCII characters 33-126.

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

Disabled: Disable SNMP trap mode operation (default).

UDP: Enable UDP SNMP trap mode operation.

TCP: Enable TCP SNMP trap mode operation.

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

SNMPv1: Set SNMP trap 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 - 255 characters, and the allowed content is ASCII characters 33 - 126.

Trap Destination Address: Indicates the SNMP trap destination address. It allows a valid IP address in dotted decimal notation ('x.y.z.w'). 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. The default is port 162.

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

Enabled: Enable SNMP trap inform mode operation.

Disabled: Disable SNMP trap inform mode operation (default).

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

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 the number of digits between 10 and 64, but all-zeros and all-'F's are not allowed.

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

Buttons

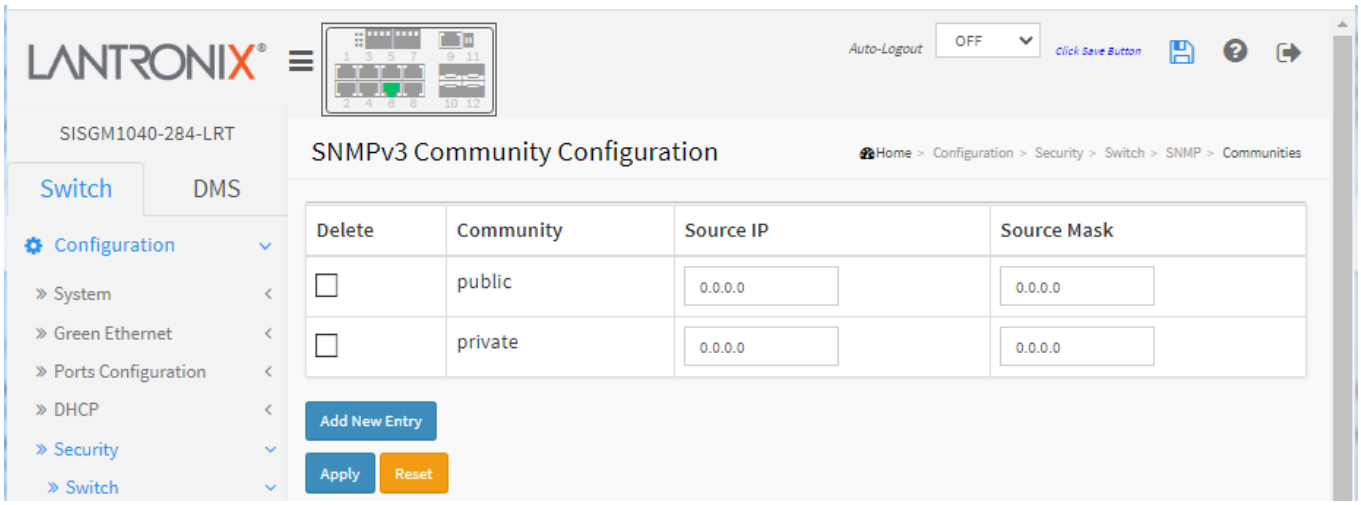
Add New Entry: Click to add a new user.

Apply: Click to apply changes immediately.

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

Configuration > Security > Switch > SNMP > Communities

Configure SNMPv3 community table on this page. The entry index key is Community.



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 characters, and the allowed content is ASCII characters 33-126. The community string will be treated as security name and map a SNMPv1 or SNMPv2c community string.

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

Source Mask: Indicates the SNMP access source address mask.

Buttons

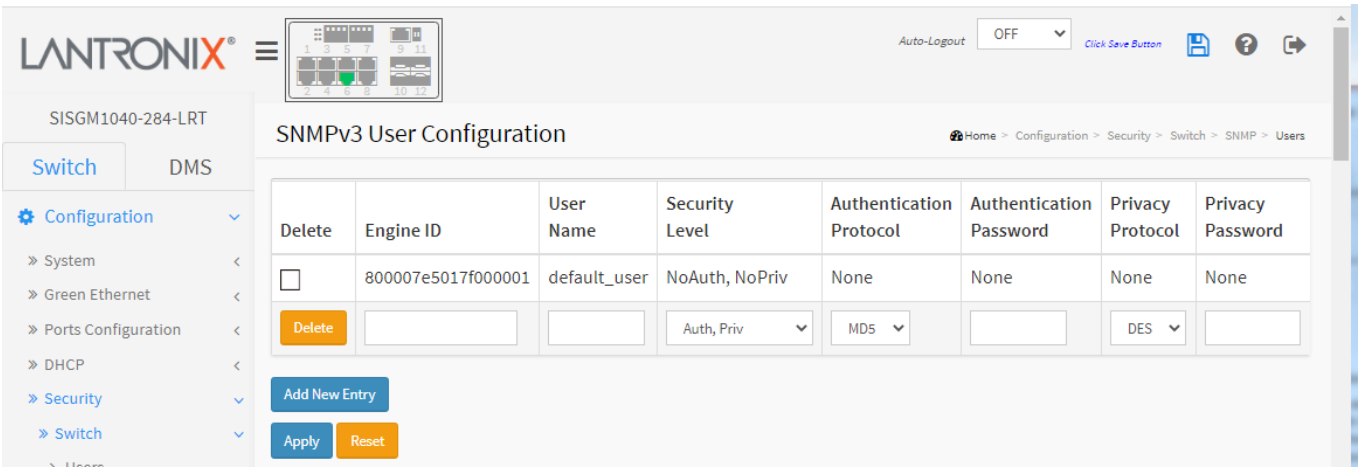
Add New Entry: Click to add a new community entry.

Apply: Click to apply changes immediately.

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

Configuration > Security > Switch > SNMP > Users

Configure SNMPv3 user table on this page. The entry index keys are Engine ID and User Name.



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 equals system engine ID then it is local user; otherwise it's remote user.

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

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

NoAuth, NoPriv: No authentication and no privacy (default).

Auth, NoPriv: Authentication and no privacy.

Auth, Priv: Authentication and privacy.

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

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

None: No authentication protocol.

MD5: An optional flag to indicate that this user uses MD5 authentication protocol (default).

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

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

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

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

None: No privacy protocol.

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

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

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

Buttons

Add New Entry: Click to add a new user.

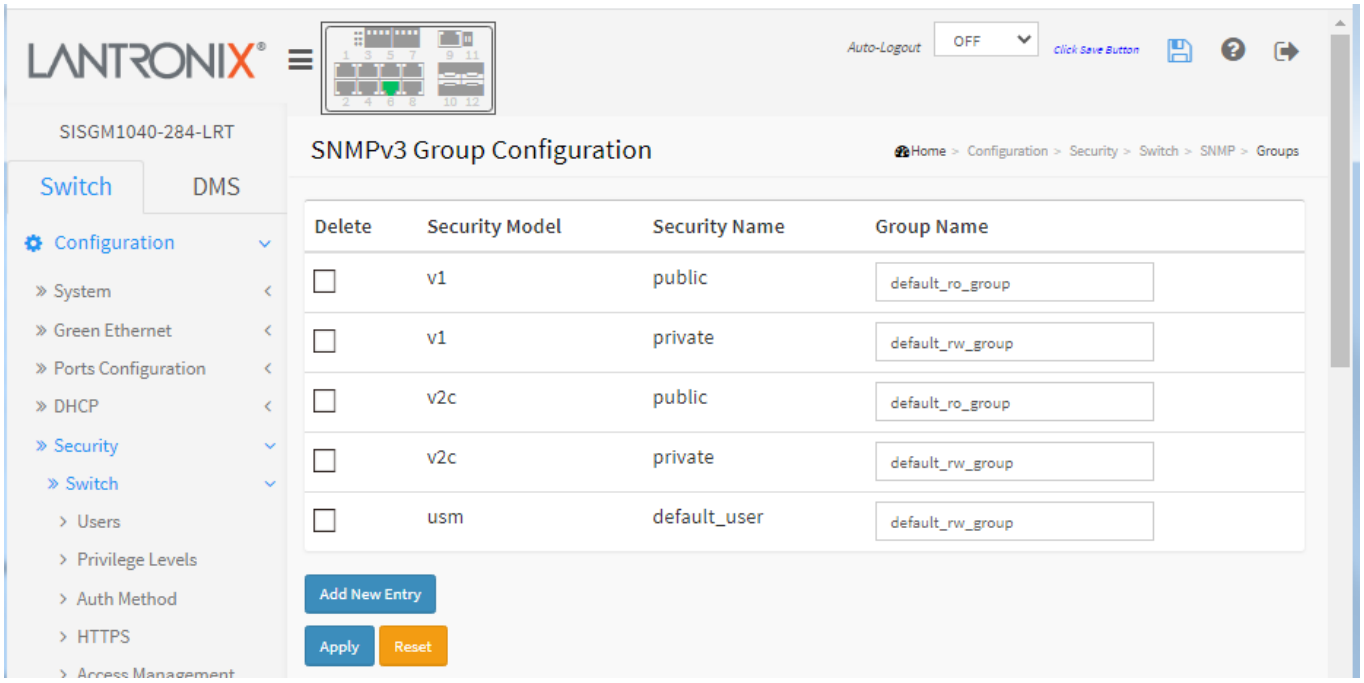
Apply: Click to apply changes immediately.

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

Example:

Configuration > Security > Switch > SNMP > Groups

Configure SNMPv3 group table on this page. The entry index keys are Security Model and Security Name.



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 1-32 characters, and the allowed content is ASCII characters 33-126.

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

Buttons

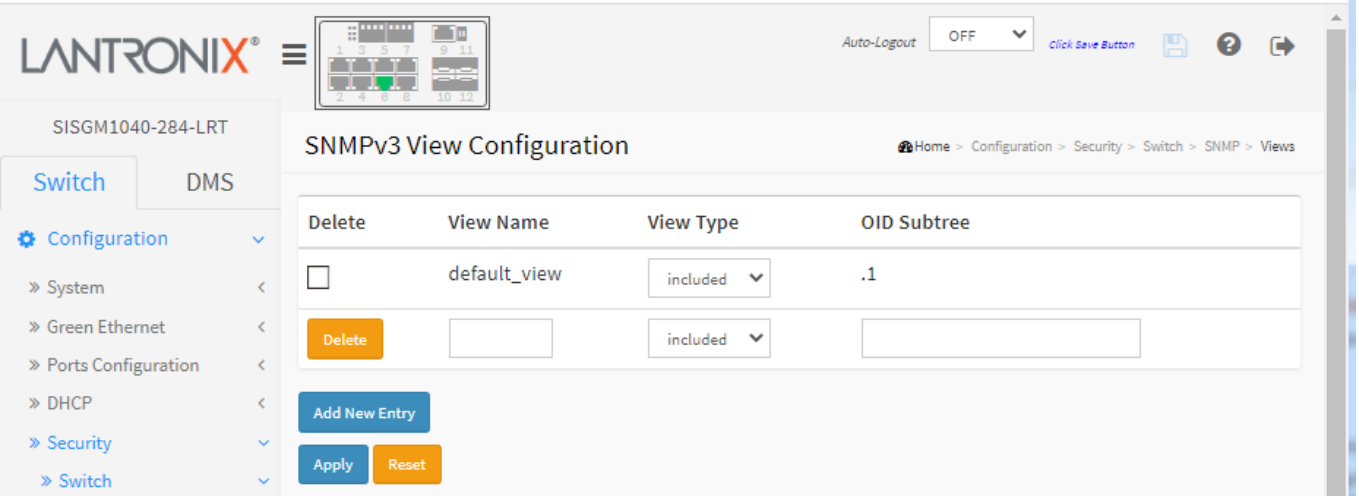
Add New Entry: Click to add a new group.

Apply: Click to apply changes immediately.

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

Configuration > Security > Switch > SNMP > Views

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



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

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

included: An optional flag to indicate that this view subtree should be included (default).

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

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

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

Buttons

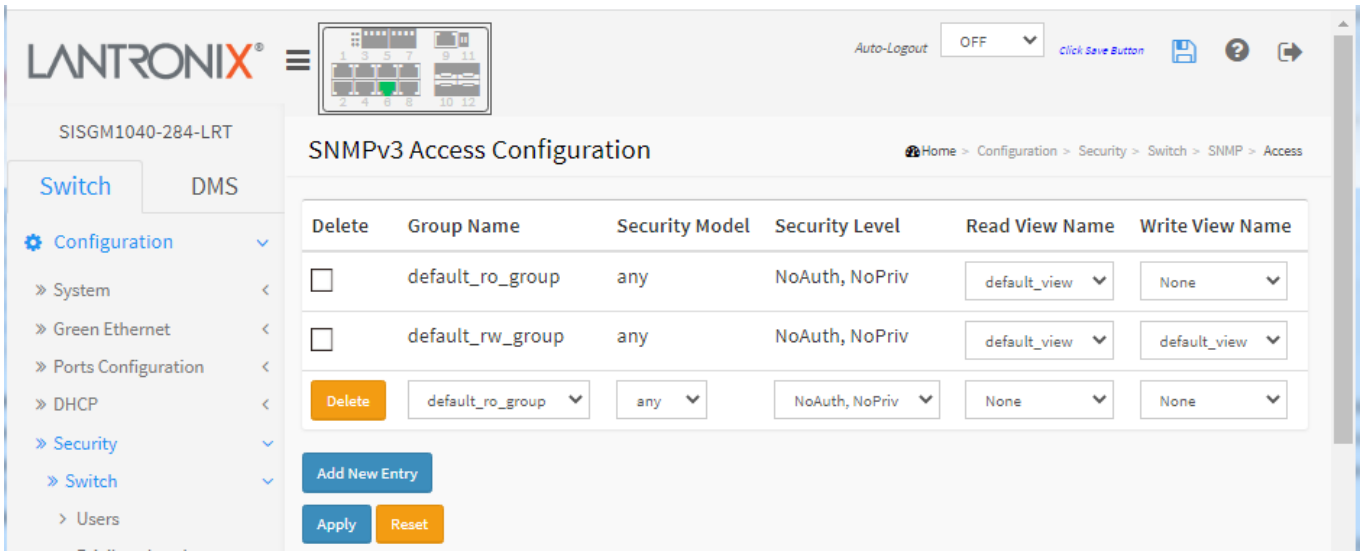
Add New Entry: Click to add a new view.

Apply: Click to apply changes immediately.

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

Configuration > Security > Switch > SNMP > Access

Configure SNMPv3 access table on this page. The entry index keys are Group Name, Security Model and Security Level.



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 1-32 characters, and the allowed content is ASCII characters 33-126.

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

any: Any security model accepted (v1, v2c, or usm) (default).

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 (default).

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 1-32 characters, and the allowed content is ASCII characters 33-126.

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

Buttons

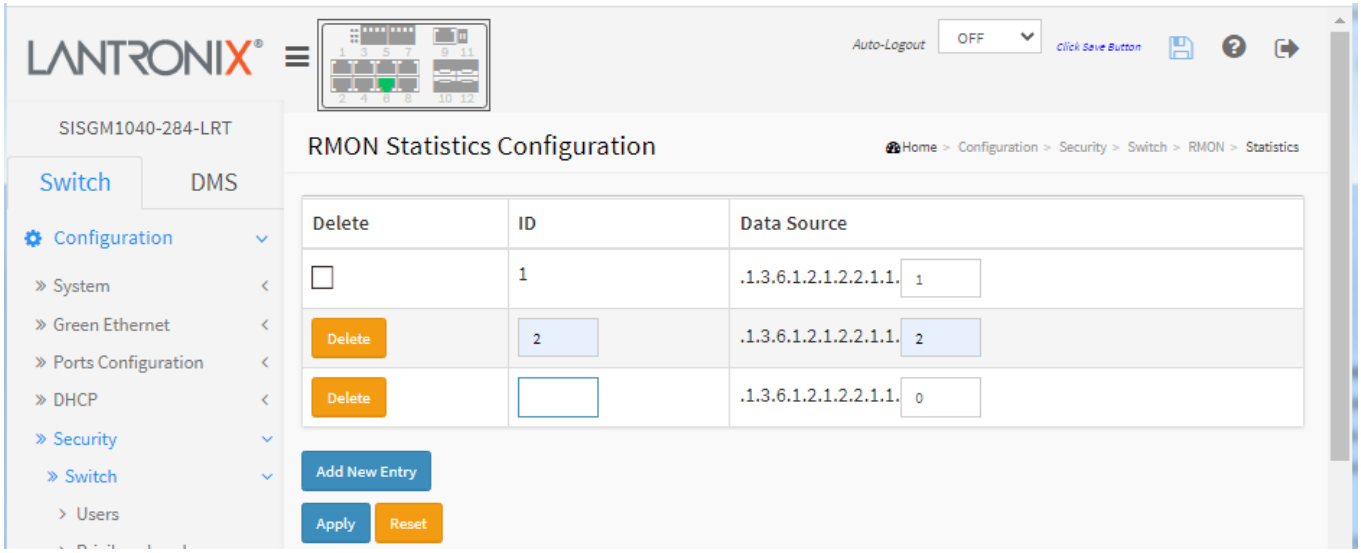
Add New Entry: Click to add a new access group.

Apply: Click to apply changes immediately.

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

Configuration > Security > Switch > RMON > Statistics

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



Parameter descriptions:

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

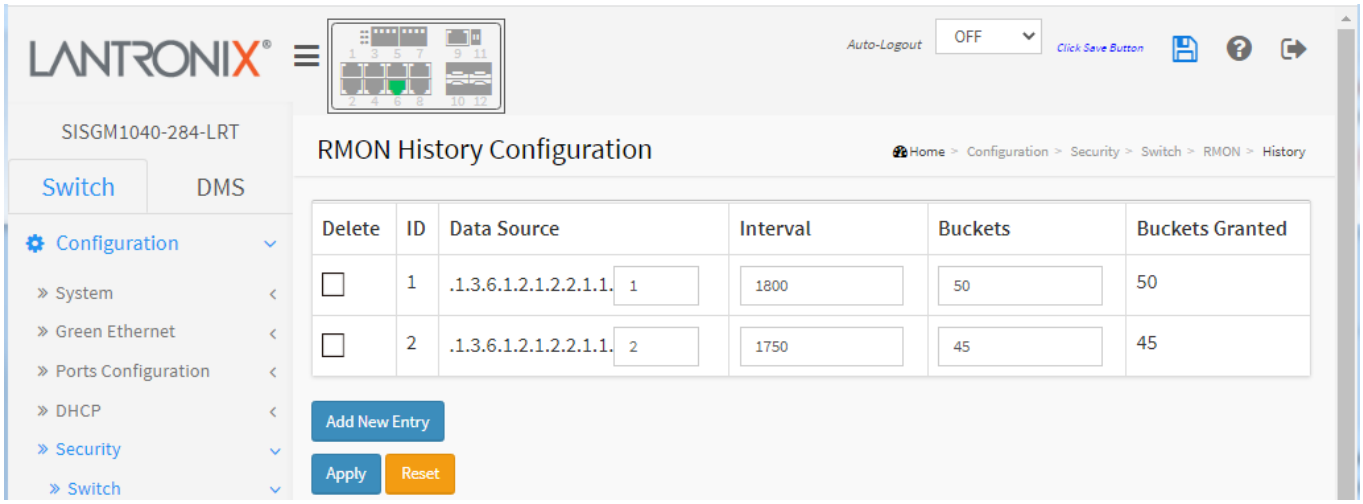
Add New Entry: Click to add a new RMON Statistics Data Source.

Apply: Click to apply changes immediately.

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

Configuration > Security > Switch > RMON > History

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



Parameter descriptions:

Delete: Check to delete the entry at 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.

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

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

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

Buttons

Add New Entry: Click to add a new instance.

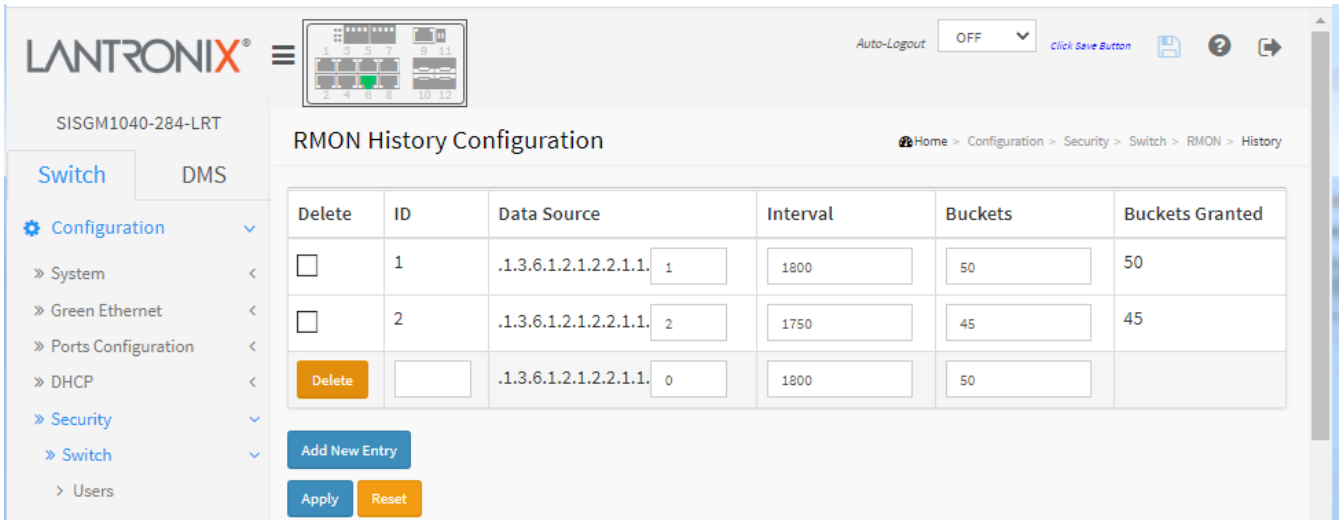
Apply: Click to apply changes immediately.

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

Messages: *invalid 'datasource', invalid llag*

Configuration > Security > Switch > RMON > Alarm

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



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 1-65535.

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 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 instance.

Apply: Click to apply changes immediately.

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

Messages:

Variable value is xxx.yyy, xxx is 10-21, yyy is 1-65535

'Rising threshold' must be an integer value between 1 and 2147483647

'Rising Index' must be an integer value between 1 and 65535

'Falling threshold' must be an integer value between 1 and 2147483647

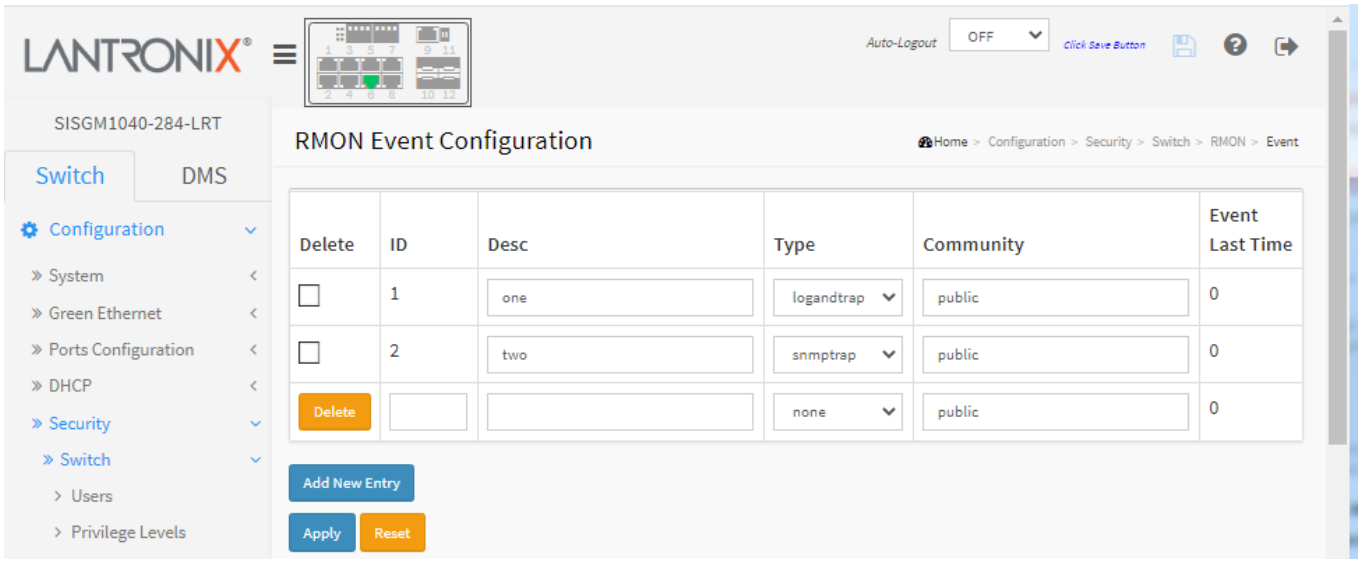
'Falling Index' must be an integer value between 1 and 65535

'Rising threshold' must be larger than 'Falling threshold'

'Falling Index' must be an integer value between 1 and 65535

Configuration > Security > Switch > RMON > Event

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



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 1-65535.

Desc: Describe this event; the string length is 0-127, 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 0- 127; the default is "public".

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

Buttons

Add New Entry: Click to add a new instance.

Apply: Click to apply changes immediately.

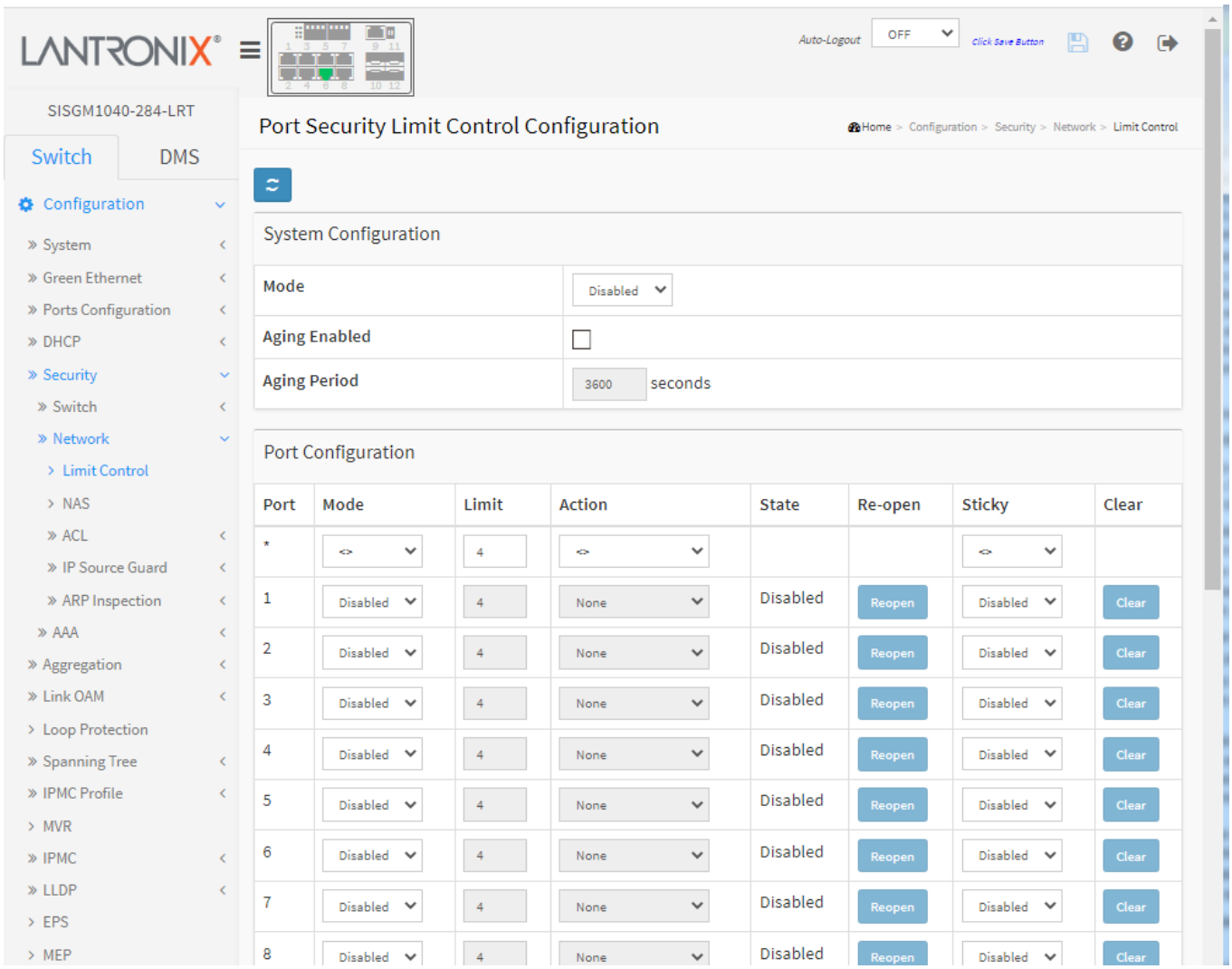
Reset: Click to undo any changes made locally and revert to previously saved values.

Configuration > Security > Network > Limit Control

This page allows you to configure the Port Security Limit Control system and port settings.

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

The Limit Control consists of two sections, a system-configuration and a port- configuration section.



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 several columns:

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

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

Limit: The maximum number of MAC addresses that can be secured on this port. The 'Limit' must be an integer value between 1 and 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:

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

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

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

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

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

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

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

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

Note that clicking the Reopen button causes the page to be refreshed, so non-committed changes will be lost.

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

Clear button: To clear the static MAC addresses be added by sticky function.

Buttons

Refresh: Click to refresh the page. Note that non-committed changes will be lost.

Apply: Click to save changes.

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

Example:

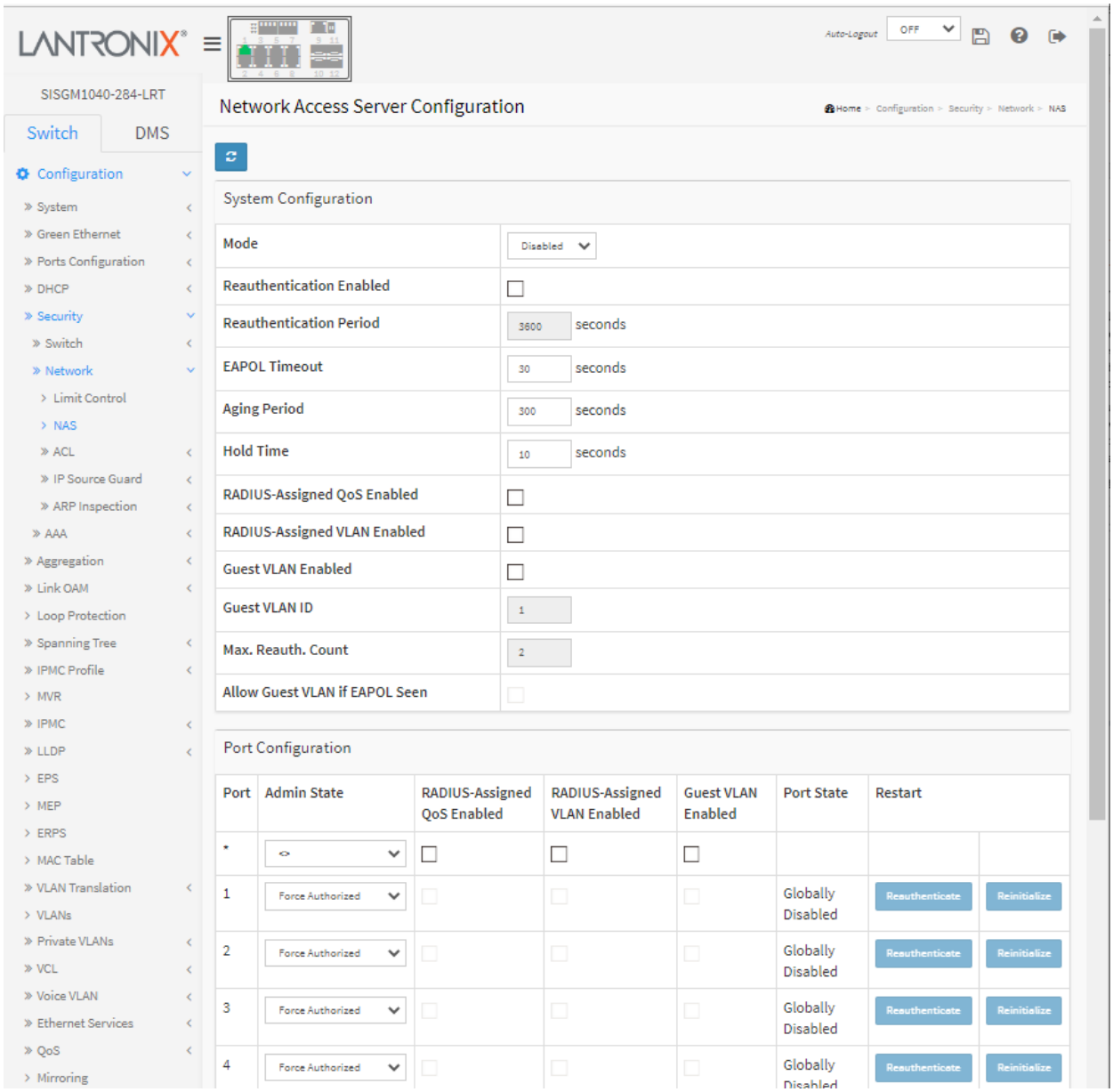
Configuration > Security > Network > NAS

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, but non-standard variants overcome security limitations as discussed below.

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 section and a Port Configuration section.



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 (Extensible Authentication Protocol (EAP) over LAN (EAPoL)) frames. Valid values are in the range 1 to 65535 seconds. This has no effect for MAC-based ports.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

> ***Force Authorized***: In this mode, the switch will send one EAPOL Success frame when the port link comes up, and any client on the port will be allowed network access without authentication.
>
> ***Force Unauthorized***: In this mode, the switch will send one EAPOL Failure frame when the port link comes up, and any client on the port will be disallowed network access.
>
> ***Port-based 802.1X***: In the 802.1X-world, the user is called the supplicant, the switch is the authenticator, and the RADIUS server is the authentication server. The authenticator acts as the man-in-the-middle, forwarding requests and responses between the supplicant and the authentication server. Frames sent between the supplicant and the switch are special 802.1X frames, known as EAPOL (EAP Over LANs) frames. EAPOL frames encapsulate EAP PDUs (RFC3748). Frames sent between the switch and the RADIUS server are RADIUS packets. RADIUS packets also encapsulate EAP PDUs together with other attributes like the switch's IP address, name, and the supplicant's port number on the switch. EAP is very

flexible, in that it allows for different authentication methods, like MD5-Challenge, PEAP, and TLS. The important thing is that the authenticator (the switch) doesn't need to know which authentication method the supplicant and the authentication server are using, or how many information exchange frames are needed for a particular method. The switch simply encapsulates the EAP part of the frame into the relevant type (EAPOL or RADIUS) and forwards it.

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

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

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

Single 802.1X is really not an IEEE standard, but features many of the same characteristics as does port-based 802.1X. In Single 802.1X, at most one supplicant can get authenticated on the port at a time. Normal EAPOL frames are used in the communication between the supplicant and the switch. If more than one supplicant is connected to a port, the one that comes first when the port's link comes up will be the first one considered. If that supplicant doesn't provide valid credentials within a certain amount of time, another supplicant will get a chance. Once a supplicant is successfully authenticated, only that supplicant will be allowed access. This is the most secure of all the supported modes. In this mode, the Port Security module is used to secure a supplicant's MAC address once successfully authenticated.

Multi 802.1X: 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 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 802.1X-based authentication is that the clients don't need special supplicant software to authenticate. The disadvantage is that MAC addresses can be spoofed by malicious users - equipment whose MAC address is a valid RADIUS user can be used by anyone. Also, only the MD5-Challenge method is supported. The maximum number of clients that can be attached to a port can be limited using the Port Security Limit Control functionality.

Note: The 802.1X Admin State must be set to Authorized for ports that are enabled for Spanning Tree. Other 802.1X Admin States require Spanning Tree to be disabled at Configuration > Spanning Tree > CIST Port.

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

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

- Port-based 802.1X
- Single 802.1X

RADIUS attributes used in identifying a QoS Class: The User-Priority-Table attribute defined in RFC4675 forms the basis for identifying the QoS Class in an Access-Accept packet. Only the first occurrence of the attribute in the packet will be considered, and to be valid, it must follow this rule:

- All 8 octets in the attribute's value must be identical and consist of ASCII characters in the range '0' - '7', which translates into the desired QoS Class in the range [0; 7].

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

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

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

- Port-based 802.1X
- Single 802.1X

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

RADIUS attributes used in identifying a VLAN ID: 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

Refresh: Click to refresh the page. Note that non-committed changes will be lost.

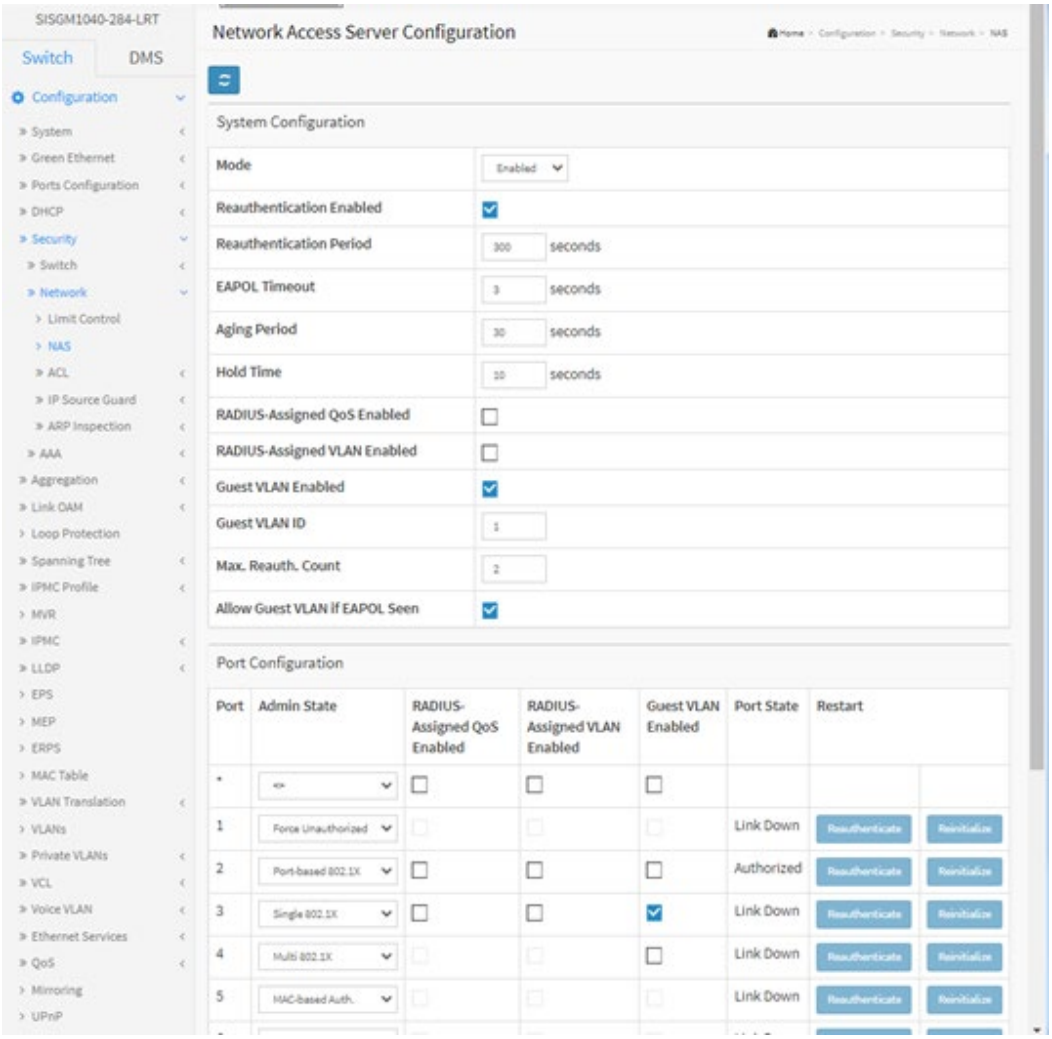
Apply: Click to save changes.

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

Messages:

The 802.1X Admin State must be set to Authorized for ports that are enabled for Spanning Tree

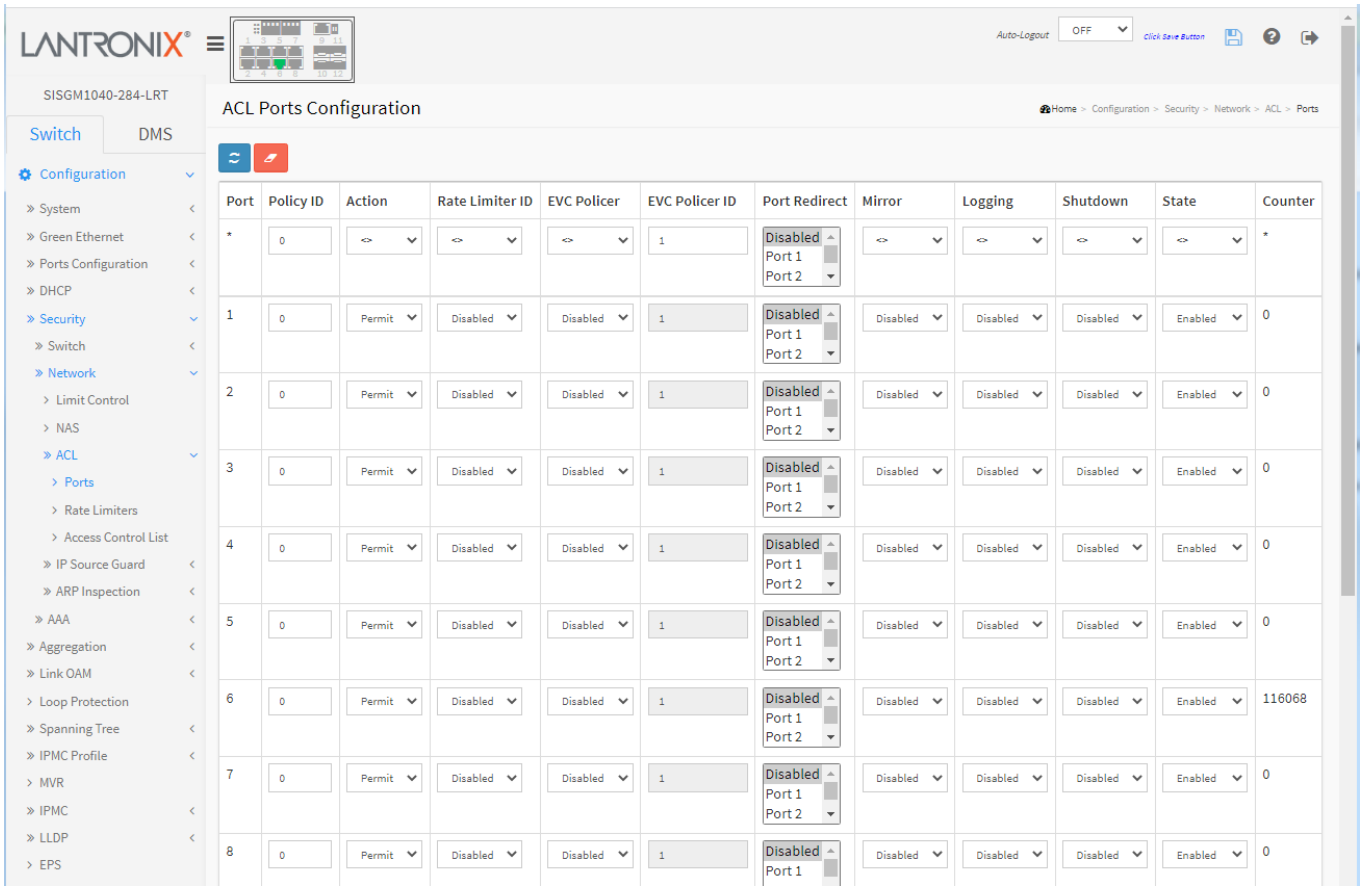
Example:



Configuration > Security > Network > ACL > Ports

Configure the ACL (Access Control List) parameters (ACE) of each switch port. These parameters will affect frames received on a port unless the frame matches a specific ACE.

An ACE (Access Control Entry) describes access permission associated with a specific ACE ID. There are three ACE frame types (Ethernet Type, ARP, and IPv4) and two ACE actions (permit and deny). The ACE also contains many detailed, different parameter options that are available for individual application.



Parameter descriptions:

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

Policy ID: Select the policy to apply to this port. The allowed values are 0 - 255. The default value is 0.

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

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

EVC Policer: Select whether EVC policer is enabled or disabled. The default value is "Disabled". Note that ACL rate limiter and EVC policer cannot both be enabled.

EVC Policer ID: Select which EVC policer ID to apply on this port. The allowed values are Disabled or the values 1 - 256.

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 (default).

Logging: Specify the logging operation of this port. Notice that the logging message doesn't include the 4 bytes CRC. 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 (default).

Note: The logging feature only works when the packet length is less than 1518 (without VLAN tags) and the System Log memory size and logging rate is limited.

Shutdown: Specify the port shut down operation of 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".

Note: The shutdown feature only works when the packet length is less than 1518 (without VLAN tags).

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 (default).

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

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

Buttons

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

Clear: Click to clear the counters.

Apply: Click to save changes.

Reset: Click to refresh the page; any changes made locally will be undone.

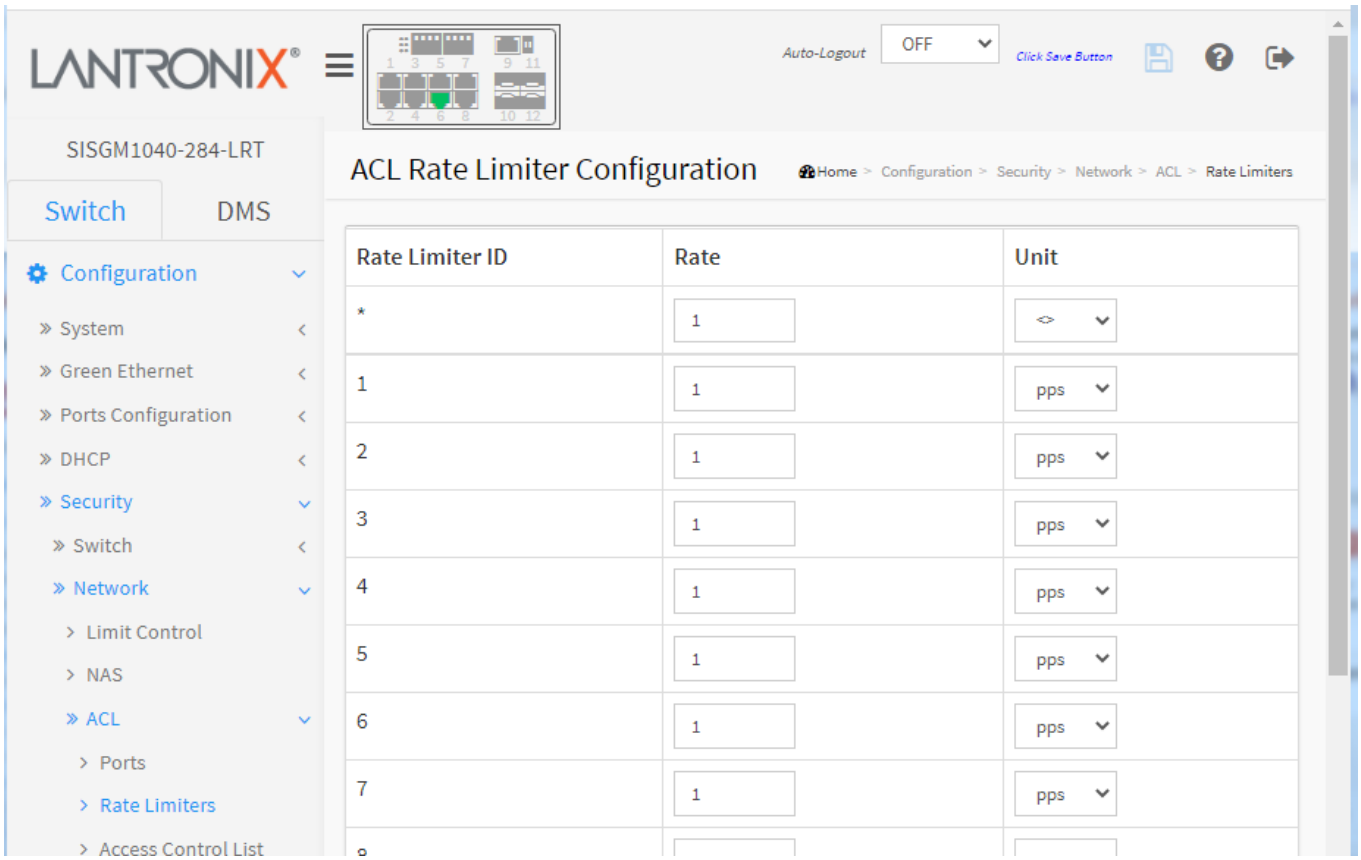
Messages:

The ACL rate limiter and EVC policer can not both be enabled.

The parameter of 'Port Redirect' can't be set when action is permitted

Configuration > Security > Network > ACL > Rate Limiters

Configure the rate limiter for the ACL of the switch on this page.



Parameter descriptions:

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

Rate: The valid rate is 0-3276700 in pps, or 0, 100, 200, 300, ..., 1000000 in kbps.

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

pps: packets per second.

kbps: Kbits per second.

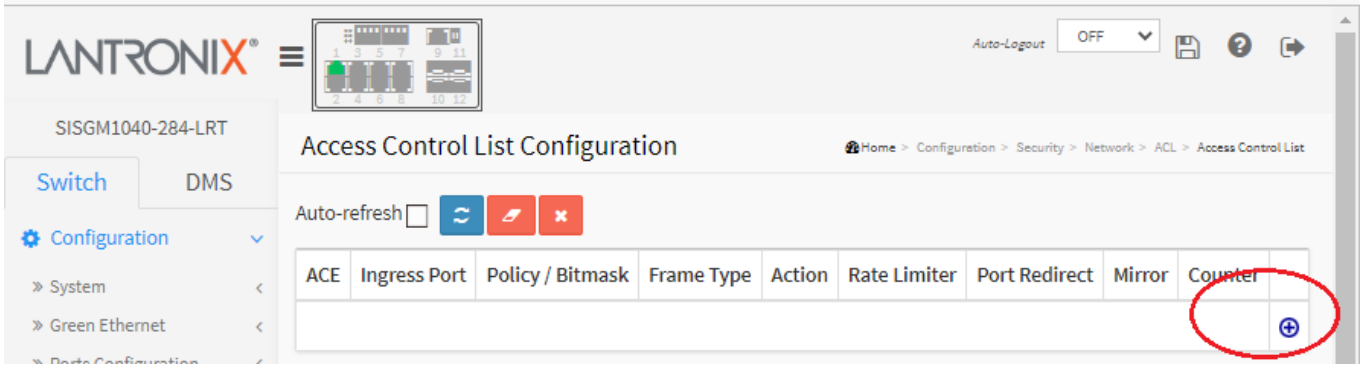
Buttons

Apply: Click to apply changes immediately.

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

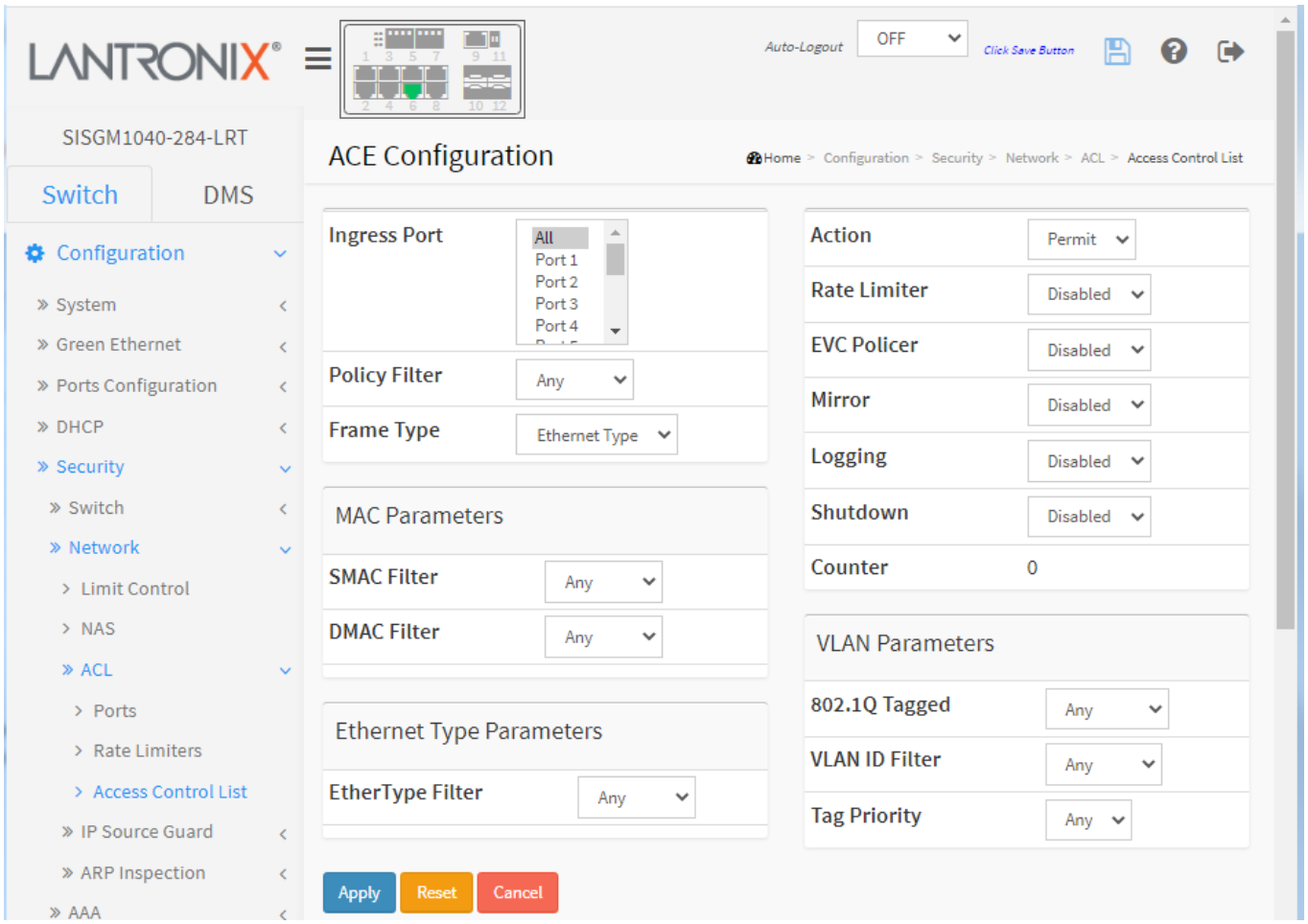
Configuration > Security > Network > ACL > Access Control List

Configure an ACE (Access Control Entry) on this page. From the initial ACL Configuration page click the ⊕ icon to display the ACE Configuration page.



An ACE consists of several parameters. These parameters vary according to the frame type that you select. First select the ingress port for the ACE, and then select the frame type. Different parameter options are displayed depending on the Frame Type selected.

A frame that hits this ACE matches the configuration that is defined here.



Parameter descriptions:

Ingress Port : Select the ingress port for which this ACE applies.

All: The ACE applies to all port.

Port n: The ACE applies to this port number, where *n* is the number of the switch port.

Policy Filter : Specify the policy number filter for this ACE.

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

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

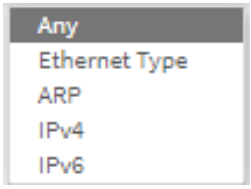
Policy Value : When "Specific" is selected for the Policy Filter, you can enter a specific policy value.
The allowed range is 0 to 255.

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

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

Any: Any frame can match this ACE.

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



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

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

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

Action : Specify the action to take with a frame that hits this ACE.

Permit: The frame that hits this ACE is granted permission for the ACE operation.

Deny: The frame that hits this ACE is dropped.

Filter: Frames matching the ACE are filtered.

Filter Port : When Action is set to 'Filter' select All port filters or select a specific port.

Rate Limiter : Specify the rate limiter in number of base units. The allowed range is 1 - 16. Disabled indicates that the rate limiter operation is disabled.

EVC Policer : Select whether EVC policer is enabled or disabled. The default value is "Disabled". Note that the ACL rate limiter and EVC policer cannot both be enabled.

EVC Policer ID : Select which EVC policer ID to apply on this ACE. The allowed values are Disabled or the values 1 - 256.

Port Redirect : Frames that hit the ACE are redirected to the port number specified here. The rate limiter will affect these ports. The allowed range is the same as the switch port number range.

Disabled indicates that the port redirect operation is disabled and the specific port number of 'Port Redirect' can't be set when action is permitted.

Mirror : Specify the mirror operation of this port. Frames matching the ACE are mirrored to the destination mirror port. The rate limiter will not affect frames on the mirror port. The allowed values are:

Enabled: Frames received on the port are mirrored.

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

Logging : Specify the logging operation of the ACE. Notice that the logging message doesn't include the 4 bytes CRC information. The allowed values are:

Enabled: Frames matching the ACE are stored in the System Log.
Disabled: Frames matching the ACE are not logged.

Note: The logging feature only works when the packet length is less than 1518(without VLAN tags) and the System Log memory size and logging rate is limited.

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

Enabled: If a frame matches the ACE, the ingress port will be disabled.
Disabled: Port shut down is disabled for the ACE.

Note: The shutdown feature only works when the packet length is less than 1518(without VLAN tags).

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

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

: Inserts a new ACE before the current row.

: Edits the ACE row.

: Moves the ACE up the list.

: Moves the ACE down the list.

: Deletes the ACE.

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

VLAN Parameters

802.1Q Tagged : Specify whether frames can hit the action according to the 802.1Q tagged. The allowed values are:

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

Enabled: Tagged frame only.

Disabled: Untagged frame only.

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

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

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

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

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

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

ARP/RARP : Specify the available ARP/RARP opcode (OP) flag for this ACE.
Any: No ARP/RARP OP flag is specified. (OP is "don't-care".)
ARP: Frame must have ARP opcode set to ARP.
RARP: Frame must have RARP opcode set to RARP.
Other: Frame has unknown ARP/RARP Opcode flag.

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

Any: No Request/Reply OP flag is specified. (OP is "don't-care".)
Request: Frame must have ARP Request or RARP Request OP flag set.
Reply: Frame must have ARP Reply or RARP Reply OP flag.

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

Any: No sender IP filter is specified. (Sender IP filter is "don't-care".)
Host: Sender IP filter is set to Host. Specify the sender IP address in the SIP Address field that appears.
Network: Sender IP filter is set to Network. Specify the sender IP address and sender IP mask in the SIP Address and SIP Mask fields that appear.

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

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

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

Any: No target IP filter is specified. (Target IP filter is "don't-care".)
Host: Target IP filter is set to Host. Specify the target IP address in the Target IP Address field that appears.
Network: Target IP filter is set to Network. Specify the target IP address and target IP mask in the Target IP Address and Target IP Mask fields that appear.

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

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

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

0: ARP frames where SHA is not equal to the SMAC address.
1: ARP frames where SHA is equal to the SMAC address.
Any: Any value is allowed ("don't-care").

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

0: RARP frames where THA is not equal to the target MAC address.
1: RARP frames where THA is equal to the target MAC address.
Any: Any value is allowed ("don't-care").

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

0: ARP/RARP frames where the HLN is not equal to Ethernet (0x06) or the (PLN) is not equal to IPv4 (0x04).
1: ARP/RARP frames where the HLN is equal to Ethernet (0x06) and the (PLN) is equal to IPv4 (0x04).
Any: Any value is allowed ("don't-care").

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

0: ARP/RARP frames where the HLD is not equal to Ethernet (1).
1: ARP/RARP frames where the HLD is equal to Ethernet (1).
Any: Any value is allowed ("don't-care").

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

0: ARP/RARP frames where the PRO is not equal to IP (0x800).
1: ARP/RARP frames where the PRO is equal to IP (0x800).
Any: Any value is allowed ("don't-care").

MAC Parameters:

SMAC Filter : Only displayed when 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: 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: To filter a specific destination MAC address with this ACE. 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 : The IP parameters can be configured when Frame Type "IPv4" is selected.

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

Any: No IP protocol filter is specified ("don't-care").
Specific: If you want to filter a specific IP protocol filter with this ACE, choose this value. A field for entering an IP protocol filter appears.
ICMP: Select ICMP to filter IPv4 ICMP protocol frames. Extra fields for defining ICMP parameters will appear. These fields are explained later in this manual.
UDP: Select UDP to filter IPv4 UDP protocol frames. Extra fields for defining UDP parameters will appear. These fields are explained later in this manual.
TCP: Select TCP to filter IPv4 TCP protocol frames. Extra fields for defining TCP parameters will appear. These fields are explained later in this manual.

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

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

zero: IPv4 frames with a Time-to-Live field greater than zero must not be able to match this entry.
non-zero: IPv4 frames with a Time-to-Live field greater than zero must be able to match this entry.
Any: Any value is allowed ("don't-care").

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

No: IPv4 frames where the MF bit is set or the FRAG OFFSET field is greater than zero must not be able to match this entry.
Yes: IPv4 frames where the MF bit is set or the FRAG OFFSET field is greater than zero must be able to match this entry.
Any: Any value is allowed ("don't-care").

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

No: IPv4 frames where the options flag is set must not be able to match this entry.
Yes: IPv4 frames where the options flag is set must be able to match this entry.
Any: Any value is allowed ("don't-care").

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

Any: No source IP filter is specified. (Source IP filter is "don't-care".)
Host: Source IP filter is set to Host. Specify the source IP address in the SIP Address field that appears.
Network: Source IP filter is set to Network. Specify the source IP address and source IP mask in the SIP Address and SIP Mask fields that appear.

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

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

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

Any: No destination IP filter is specified. (Destination IP filter is "don't-care".)
Host: Destination IP filter is set to Host. Specify the destination IP address in the DIP Address field that appears.
Network: Destination IP filter is set to Network. Specify the destination IP address and destination IP mask in the DIP Address and DIP Mask fields that appear.

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

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

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

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

Any: No IPv6 next header filter is specified ("don't-care").
Specific: If you want to filter a specific IPv6 next header filter with this ACE, choose this value. A field for entering an IPv6 next header filter appears.
ICMP: Select ICMP to filter IPv6 ICMP protocol frames. Extra fields for defining ICMP parameters will appear. These fields are explained later in this manual.

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

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

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

Any: No source IPv6 filter is specified. (Source IPv6 filter is "don't-care".)
Specific: Source IPv6 filter is set to Network. Specify the source IPv6 address and source IPv6 mask in the SIP Address fields that appear.

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

SIP BitMask : When "Specific" is selected for the source IPv6 filter, you can enter a specific SIPv6 mask. The field only supported last 32 bits for IPv6 address. Notice the usage of bitmask, if the binary bit value is "0", it means this bit is "don't-care". The real matched pattern is [sipv6_address & sipv6_bitmask] (last 32 bits). For example, if the SIPv6 address is 2001::3 and the SIPv6 bitmask is 0xFFFFFFFE(bit 0 is "don't-care" bit), then SIPv6 address 2001::2 and 2001::3 are applied to this rule.

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

zero: IPv6 frames with a hop limit field greater than zero must not be able to match this entry.
non-zero: IPv6 frames with a hop limit field greater than zero must be able to match this entry.
Any: Any value is allowed ("don't-care").

ICMP Parameters

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

Any: No ICMP filter is specified (ICMP filter status is "don't-care").
Specific: If you want to filter a specific ICMP filter with this ACE, you can enter a specific ICMP value. A field for entering an ICMP value appears.

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

ICMP Code Filter : Specify the ICMP code filter for this ACE.
Any: No ICMP code filter is specified (ICMP code filter status is "don't-care").
Specific: If you want to filter a specific ICMP code filter with this ACE, you can enter a specific ICMP code value. A field for entering an ICMP code value appears.

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

TCP/UDP Parameters

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

Any: No TCP/UDP source filter is specified (TCP/UDP source filter status is "don't-care").
Specific: If you want to filter a specific TCP/UDP source filter with this ACE, you can enter a specific TCP/UDP source value. A field for entering a TCP/UDP source value appears.
Range: If you want to filter a specific TCP/UDP source range filter with this ACE, you can enter a specific TCP/UDP source range value. A field for entering a TCP/UDP source value appears.

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

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

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

Any: No TCP/UDP destination filter is specified (TCP/UDP destination filter status is "don't-care").
Specific: If you want to filter a specific TCP/UDP destination filter with this ACE, you can enter a specific TCP/UDP destination value. A field for entering a TCP/UDP destination value appears.
Range: If you want to filter a specific range TCP/UDP destination filter with this ACE, you can enter a specific TCP/UDP destination range value. A field for entering a TCP/UDP destination value appears.

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

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

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

0: TCP frames where the FIN field is set must not be able to match this entry.
1: TCP frames where the FIN field is set must be able to match this entry.
Any: Any value is allowed ("don't-care").

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

0: TCP frames where the SYN field is set must not be able to match this entry.
1: TCP frames where the SYN field is set must be able to match this entry.
Any: Any value is allowed ("don't-care").

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

0: TCP frames where the RST field is set must not be able to match this entry.
1: TCP frames where the RST field is set must be able to match this entry.
Any: Any value is allowed ("don't-care").

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

0: TCP frames where the PSH field is set must not be able to match this entry.
1: TCP frames where the PSH field is set must be able to match this entry.
Any: Any value is allowed ("don't-care").

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

0: TCP frames where the ACK field is set must not be able to match this entry.
1: TCP frames where the ACK field is set must be able to match this entry.
Any: Any value is allowed ("don't-care").

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

0: TCP frames where the URG field is set must not be able to match this entry.
1: TCP frames where the URG field is set must be able to match this entry.
Any: Any value is allowed ("don't-care").

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

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

Any: No EtherType filter is specified (EtherType filter status is "don't-care").
Specific: If you want to filter a specific EtherType filter with this ACE, you can enter a specific EtherType value. A field for entering an EtherType value appears.

Ethernet Type Value : When "Specific" is selected for the EtherType filter, you can enter a specific EtherType value. The allowed range is **0x600** to **0xFFFF** but excluding 0x800(IPv4), 0x806(ARP) and 0x86DD(IPv6). A frame that hits this ACE matches this EtherType value.

ACE Configuration Buttons

Apply: Click to save changes.

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

Cancel: Return to the previous page.

Access Control List Configuration Buttons

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

Refresh : Click to refresh the page; any changes made locally will be undone.

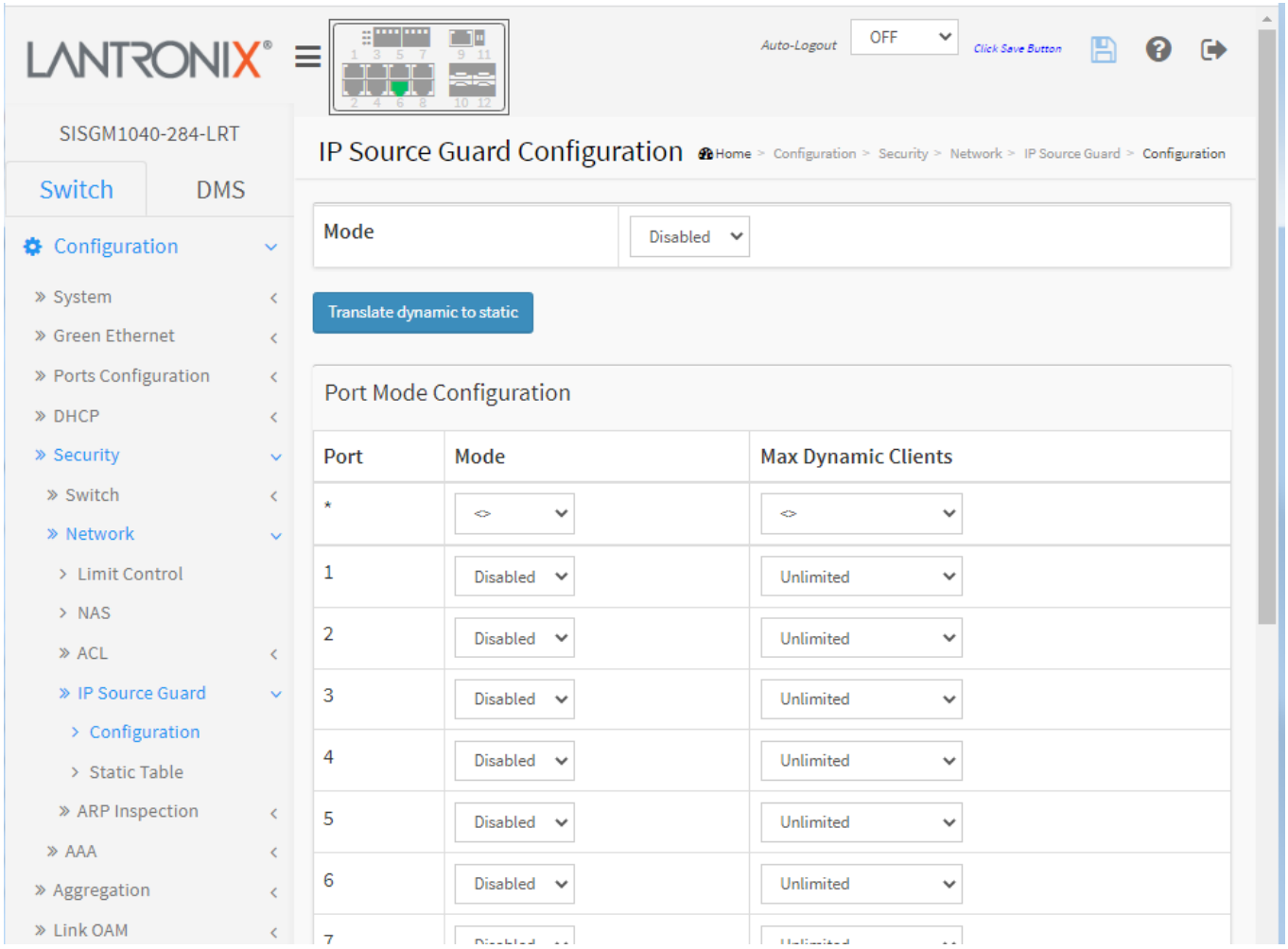
Clear : Click to clear the counters.

Remove All : Click to remove all ACEs.

Messages: *The ACL rate limiter and EVC policer can not both be enabled.*

Configuration > Security > Network > IP Source Guard > Configuration

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



Parameter descriptions:

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

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

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

Buttons

Apply: Click to save changes.

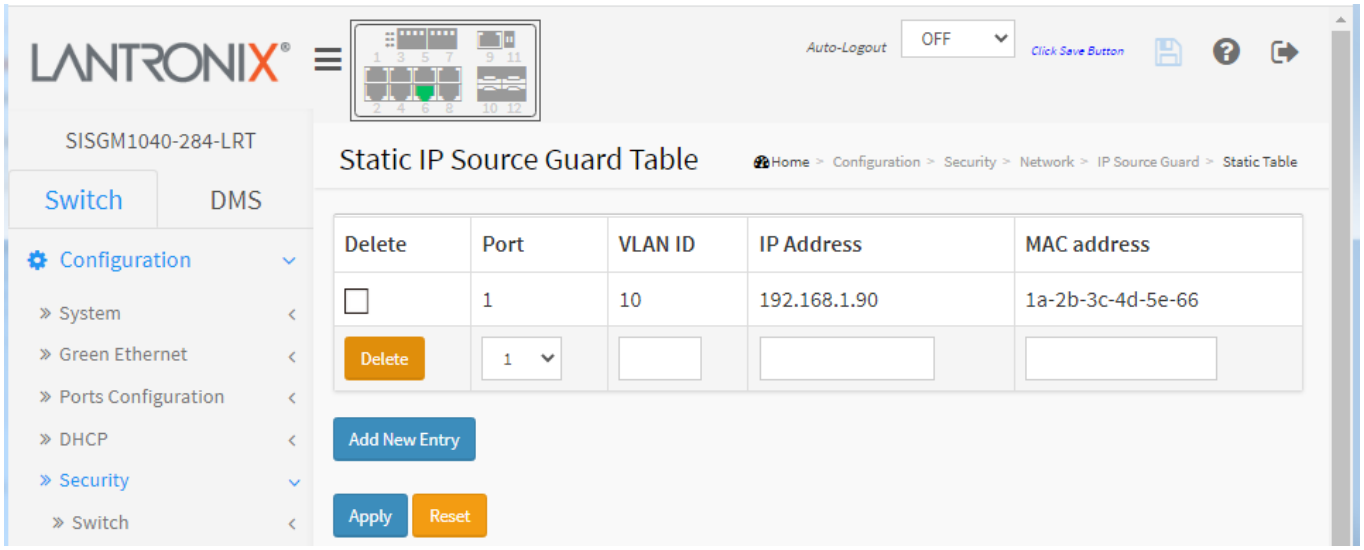
Reset: Click to undo any changes made locally and revert to previously saved values.

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

Configuration > Security > Network > IP Source Guard > Static Table

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

This page shows the static IP Source Guard rules. The maximum number of rules is 112 on the switch.



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 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 MAC Address for the new entry. Click the Apply button.

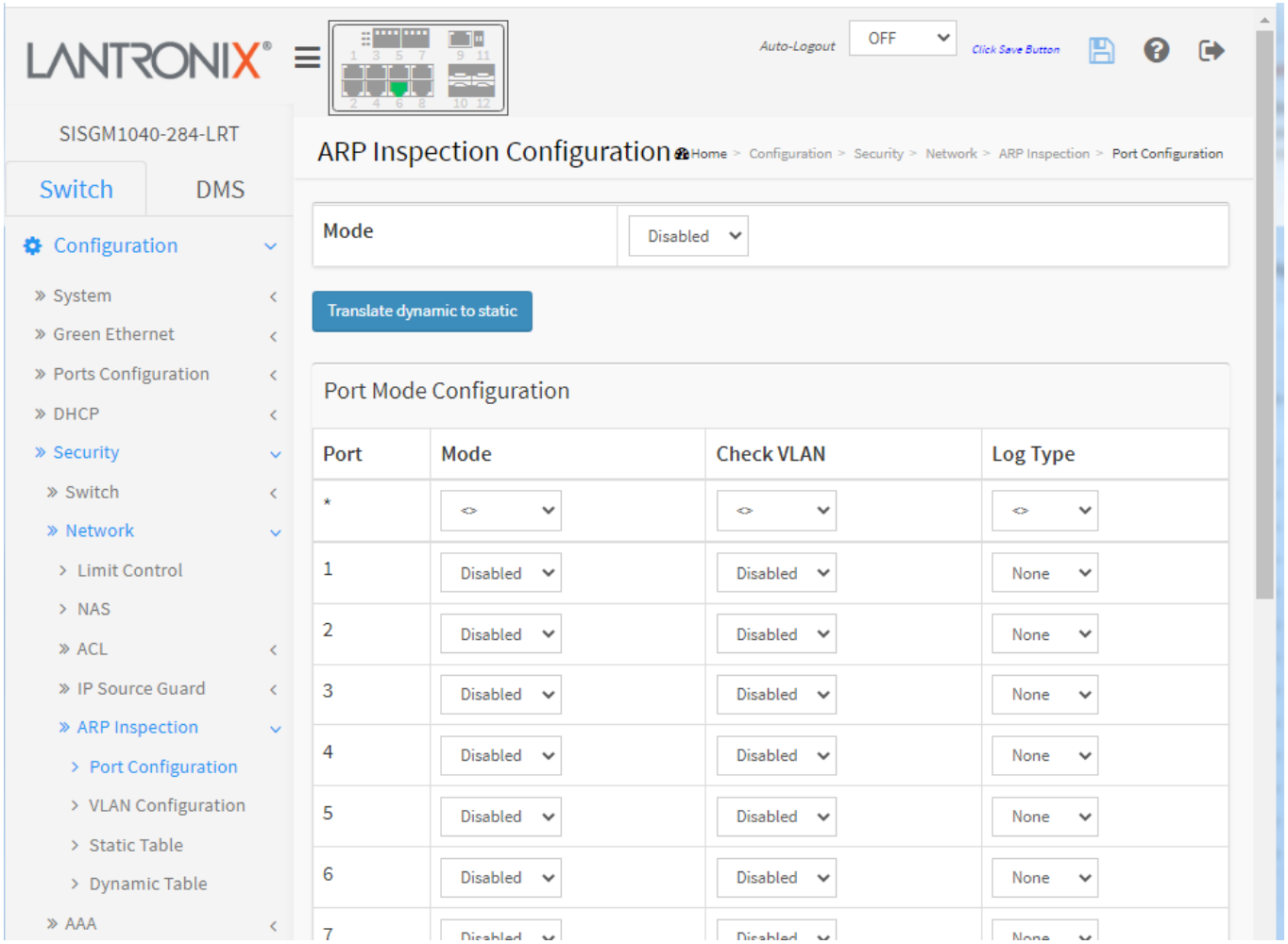
Apply – Click to save changes.

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

Configuration > Security > Network > ARP Inspection > Port Configuration

This page provides ARP Inspection related configuration.

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



Parameter descriptions:

Mode : Enable the Global ARP Inspection or disable the Global ARP Inspection.

Port Mode Configuration

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

Enabled: Enable ARP Inspection operation.

Disabled: Disable ARP Inspection operation.

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

Enabled: Enable check VLAN operation.

Disabled: Disable check VLAN operation.

Log Type : 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:

None: Log nothing.

Deny: Log denied entries.

Permit: Log permitted entries.

ALL: Log all entries.

Buttons

Apply: Click to save changes.

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

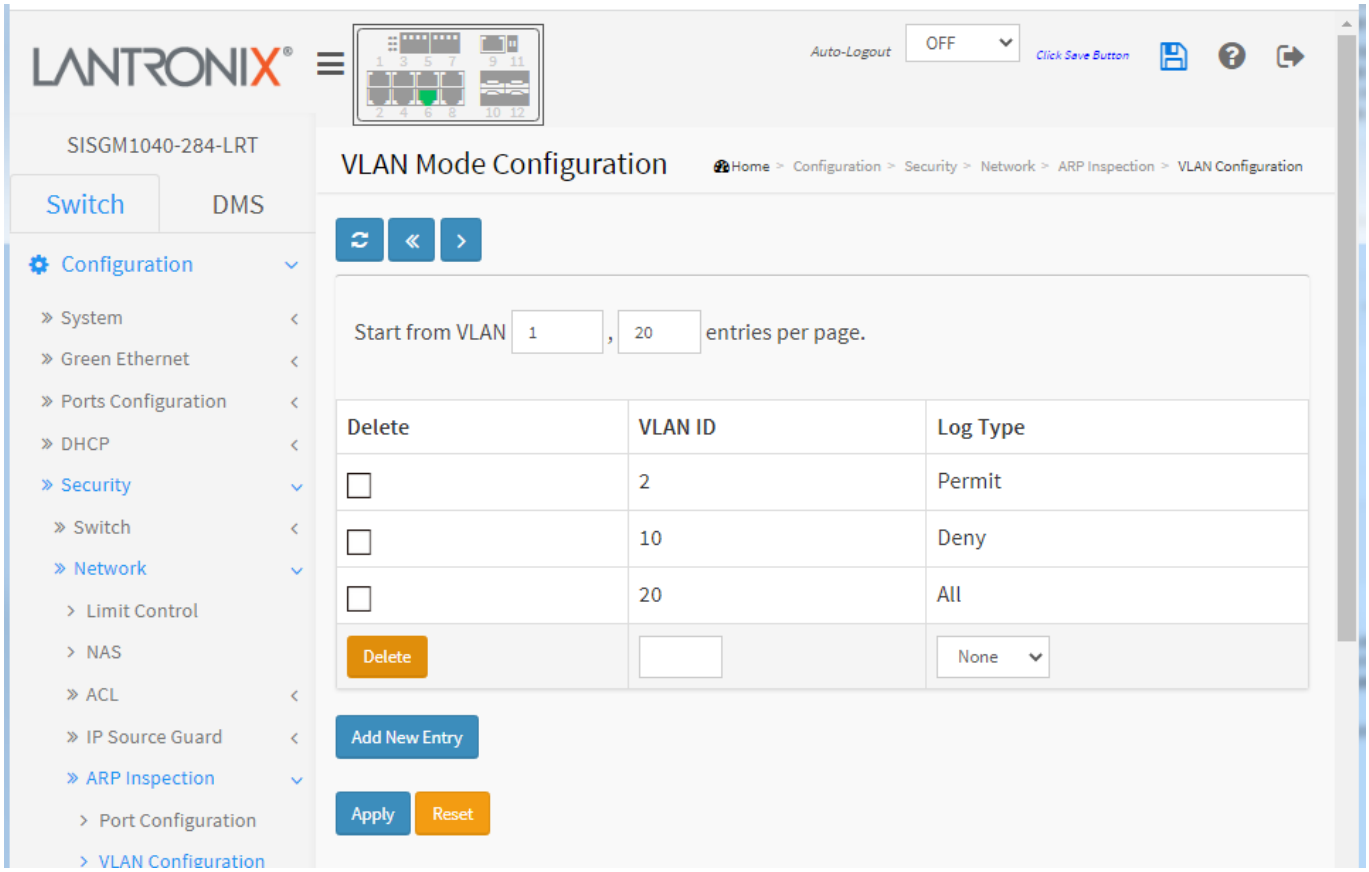
Translate dynamic to static: Click to translate all dynamic entries to static entries.

Configuration > Security > Network > ARP Inspection > VLAN Configuration

The VLAN Mode Configuration page provides ARP Inspection related configuration.

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

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



Parameter descriptions:

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

Log Type: The log type also can be configured on a per VLAN basis. Possible types are:

None: Log nothing.

Deny: Log denied entries.

Permit: Log permitted entries.

ALL: Log all entries.

Buttons

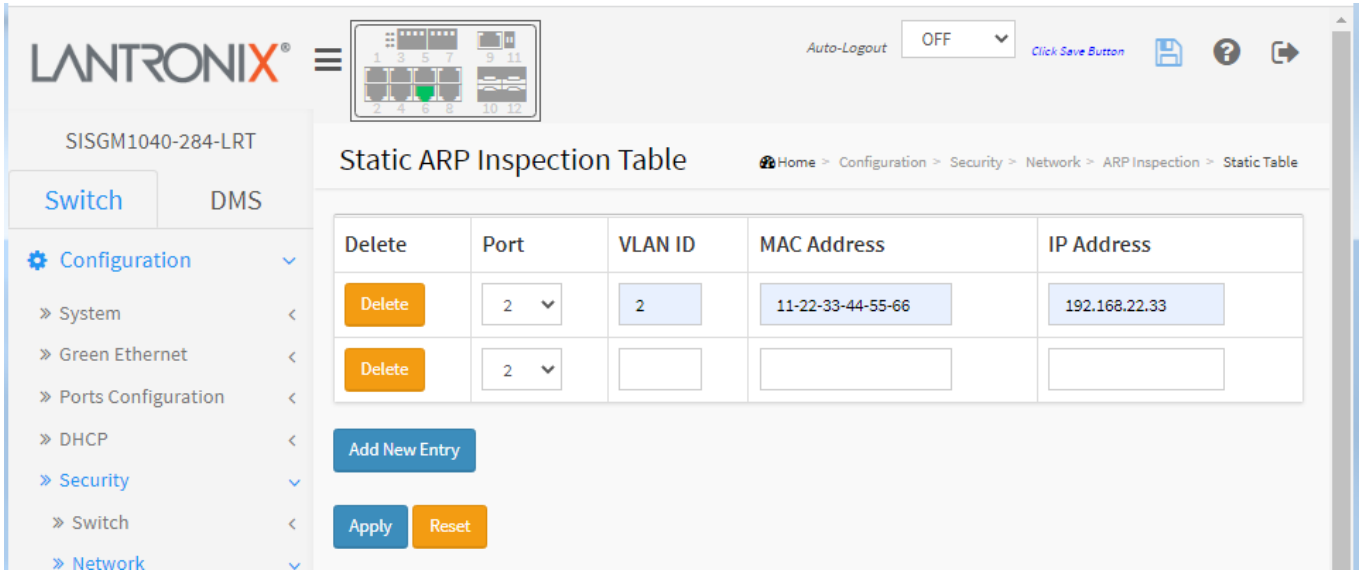
Add New Entry: Click to add a new VLAN to the ARP Inspection VLAN table.

Apply: Click to save changes.

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

Configuration > Security > Network > ARP Inspection > Static Table

This page shows the static ARP Inspection rules. The maximum number of rules is 256 on the switch.



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 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.

Apply: Click to save changes.

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

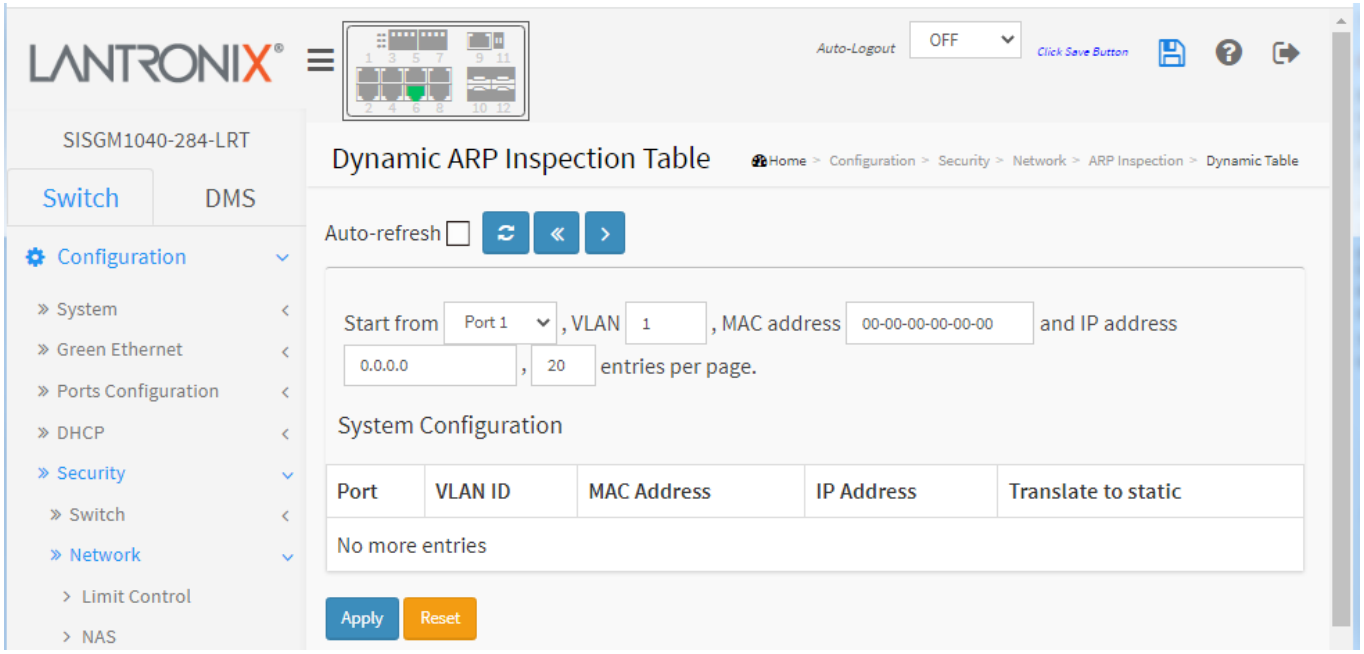
Configuration > Security > Network > ARP Inspection > Dynamic Table

Entries in the Dynamic ARP Inspection Table are shown on this page. The Dynamic ARP Inspection Table contains up to 256 entries, and is sorted first by port, then by VLAN ID, then by MAC address, and then by IP address. All dynamic entries are learning from DHCP Snooping.

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

The "Start from port address", "VLAN", "MAC address" and "IP address" input fields let you select the starting point in the Dynamic ARP Inspection Table. Clicking the Refresh button will update the displayed table starting from that or the closest next Dynamic ARP Inspection Table match. In addition, the two input fields will - upon a Refresh button click - assume the value of the first displayed entry, allowing for continuous refresh with the same start address.

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

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

Apply: Click to save changes.

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

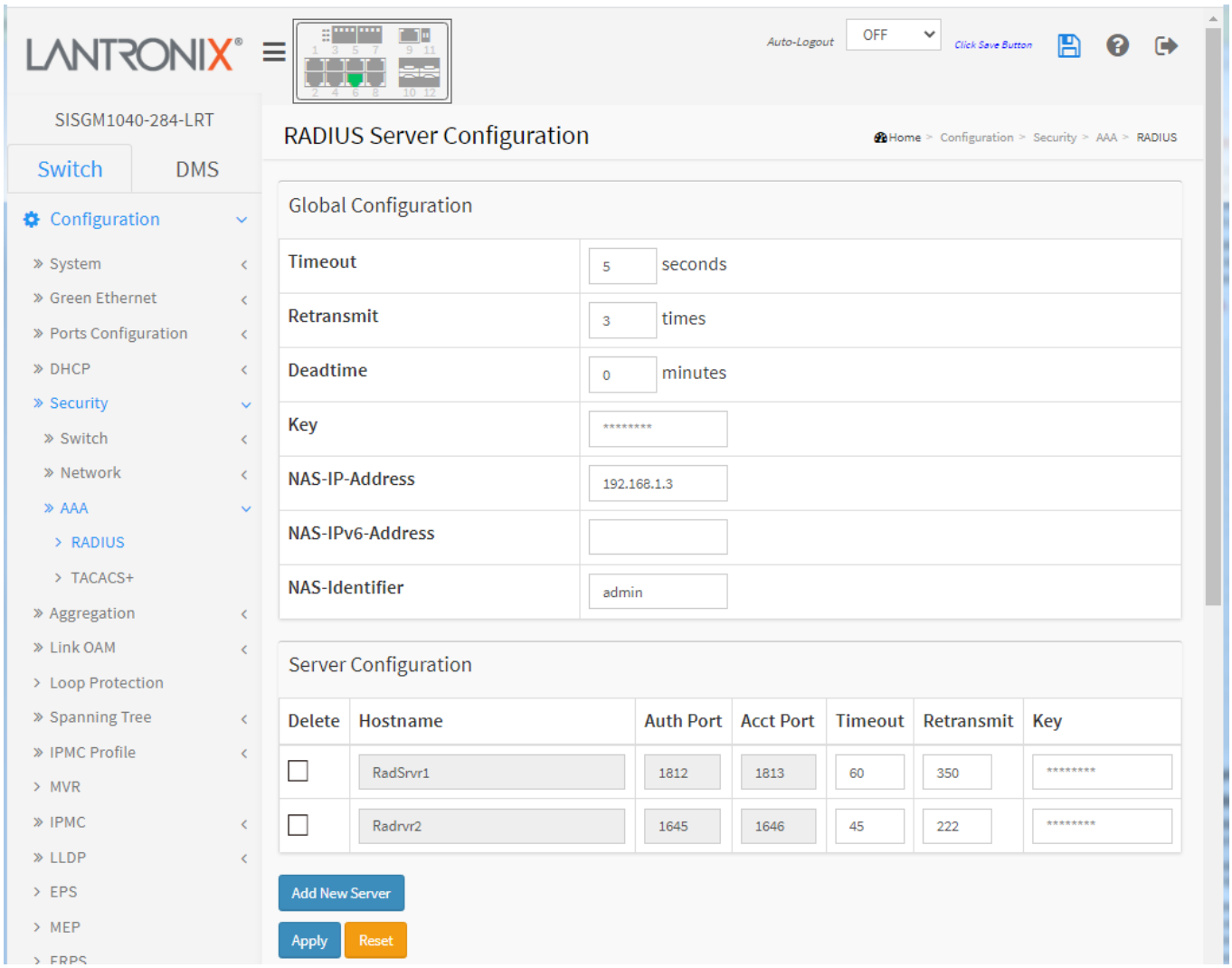
<< : Updates the table starting from the first entry in the Dynamic ARP Inspection Table.

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

Configuration > Security > AAA > RADIUS

This page lets you configure up to five RADIUS servers. RADIUS (Remote Authentication Dial In User Service) is a networking protocol that provides centralized Authentication, Authorization, and Accounting '(AAA' or 'Triple A') management for users who connect and use a network service. The RADIUS server is usually a background process running on a UNIX or Microsoft Windows Server.

RADIUS uses two packet types to manage the full AAA process: Access-Request, which manages authentication and authorization; and Accounting-Request, which manages accounting. Authentication and authorization are defined in IETF RFC 2865 and accounting is described by IETF RFC 2866.



Parameter descriptions:

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

Timeout: The number of seconds, in the range 1 to 1000, to wait for a reply from a RADIUS server before retransmitting the request.

Retransmit: 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 0 - 1440 minutes, is the period during which the switch will not send new requests to a server that has failed to respond to a previous request. This will stop the switch from continually trying to contact a server that it has already determined as dead. Setting the Deadtime to a value greater than 0 (zero) will enable this feature, but only if more than one server has been configured.

Key: The secret key - up to 63 characters long - shared between the 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 253 characters long - to be used as attribute 32 in RADIUS Access-Request packets. If this field is left blank, the NAS-Identifier is not included in the packet.

Server Configuration: The table has one row for each RADIUS server and several columns:

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

Hostname: The IPv4/IPv6 address or hostname of the RADIUS server.

Auth Port : The UDP port to use on the RADIUS server for authentication. Set to 0 to disable authentication. The officially assigned port number for RADIUS Accounting is 1812. **Note**: by default, many access servers use port 1645 for authentication requests.

> **Note:** For Windows Server information on how to configure ports that Network Policy Server (NPS) uses for Remote Authentication Dial-In User Service (RADIUS) authentication and accounting traffic see the MS Windows webpage.

Acct Port : The UDP port to use on the RADIUS server for accounting. Set to 0 to disable authentication. The officially assigned port number for RADIUS Accounting is 1813. **Note**: by default, many access servers use port 1646 for accounting requests.

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

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

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

Buttons

Add New Server: Click to add a new RADIUS server. An empty row is added to the table, and the RADIUS server can be configured as needed. Up to 5 servers are supported. The Reset button can be used to undo the addition of the new server.

Apply: Click to save changes.

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

Messages: *The input value NAS-IPv6-Address (111111111) is not a valid IPv6 address.*

The value of NAS-IP-Address must be a valid IP address in dotted decimal notation (x.y.z.w), where x, y, z, and w are decimal number between 0 and 255.

RADIUS Attributes

Value	Description	Data Type	Reference
4	NAS-IP-Address	ipv4addr	IETF RFC2865
32	NAS-Identifier	text	IETF RFC2865
95	NAS-IPv6-Address	ipv6addr	IETF RFC3162

The RADIUS Accounting protocol provides a protocol for carrying accounting information between a Network Access Server and a shared Accounting Server per IETF RFC 2866.

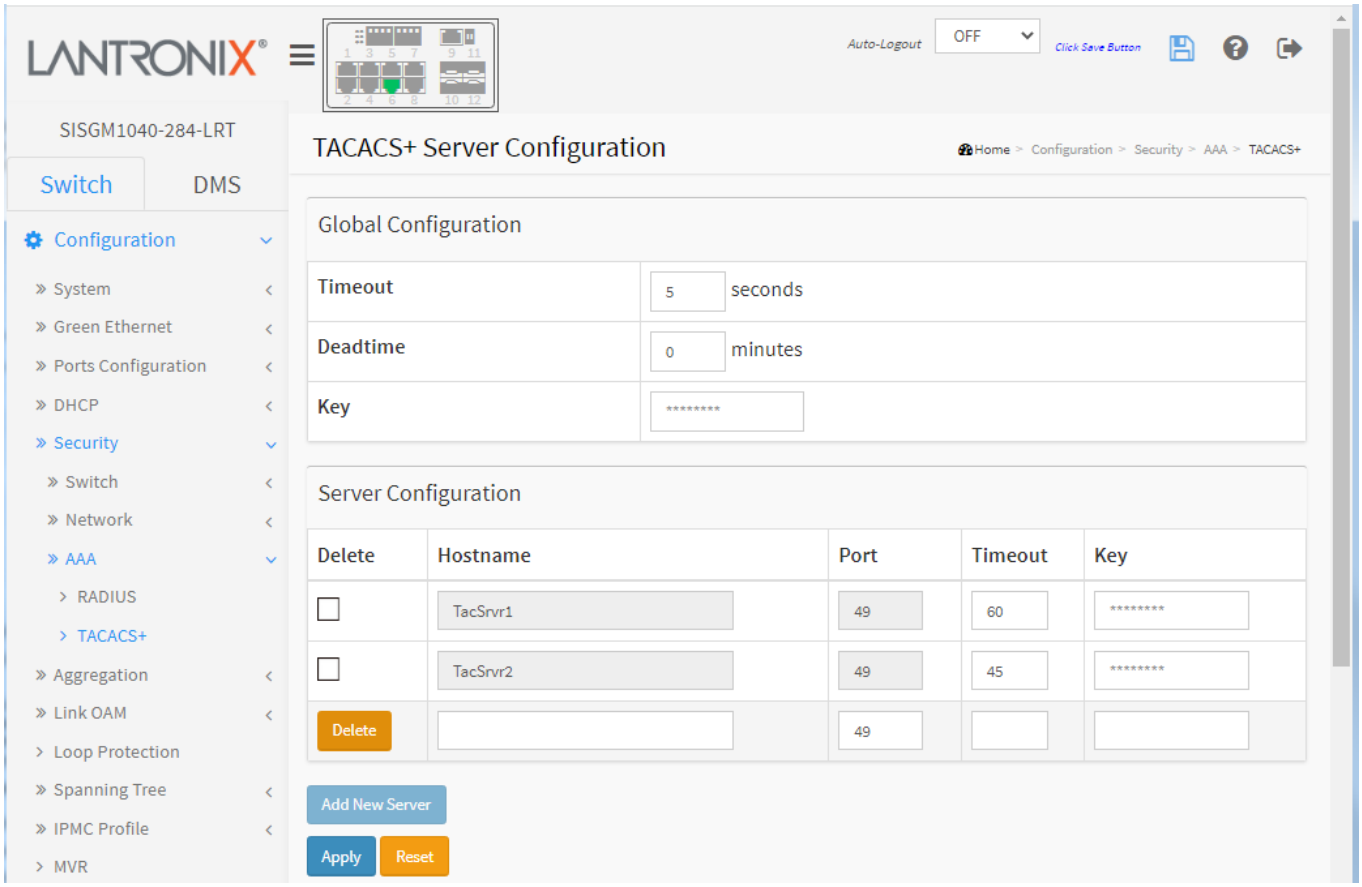
See the IANA Considerations for guidance regarding IANA registration of values related to RADIUS as defined in RFC2865.

See your RADIUS server documents for more information.

Configuration > Security > AAA > TACACS+

This page lets you configure up to five TACACS+ servers.

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.



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: Deadtime, which can be set to 0 to 1440 minutes, is the period during which the switch will not send new requests to a server that has failed to respond to a previous request. This will stop the switch from continually trying to contact a server that it has already determined as dead. Setting the Deadtime to a value greater than 0 (zero) will enable this feature, but only if more than one server has been configured.

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

Server Configuration: The table has one row for each TACACS+ server and several columns:

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

Hostname: The IPv4/IPv6 address or hostname of the TACACS+ server.

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

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

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

Buttons

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

Apply: Click to save changes.

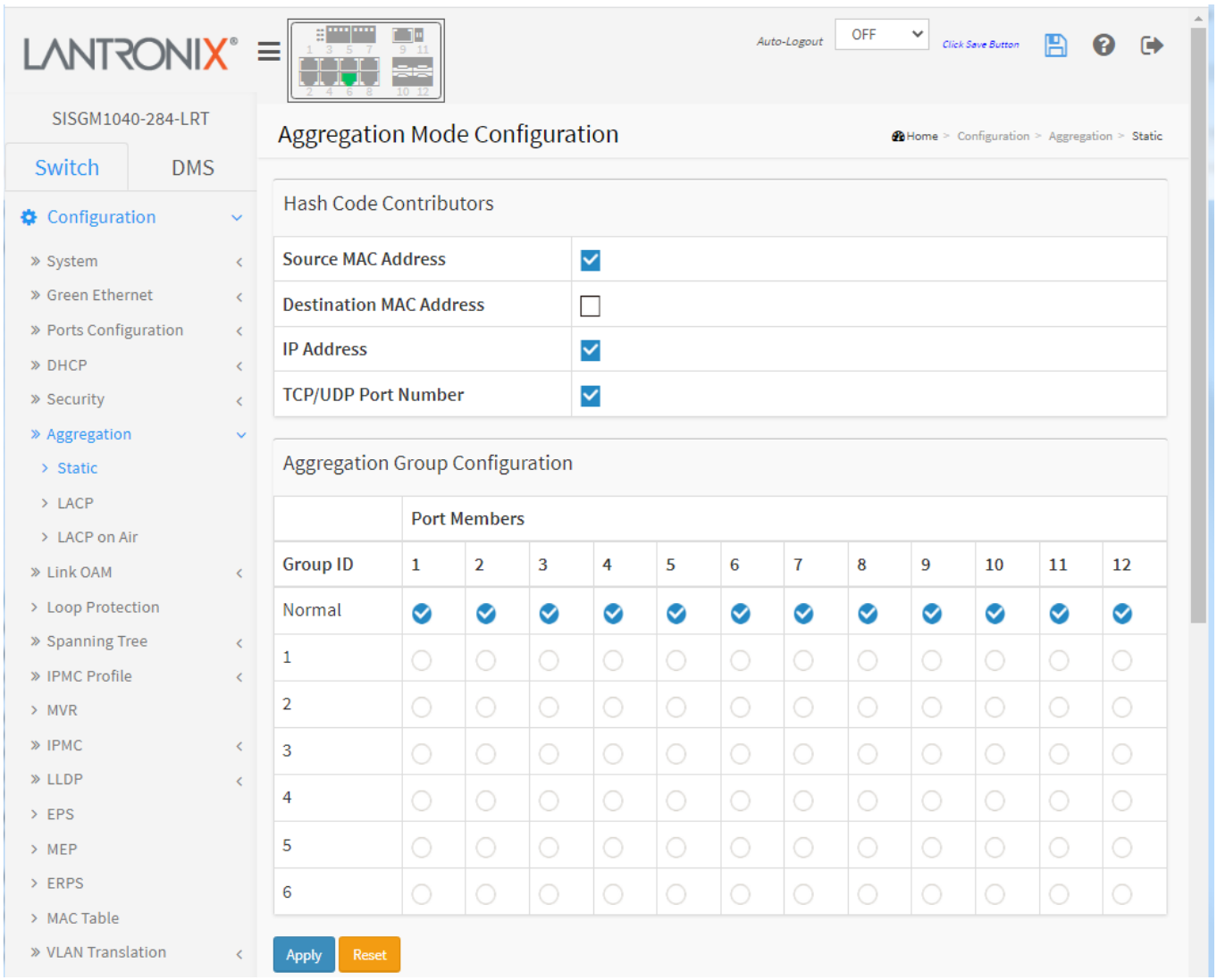
Reset: Click to undo any changes made locally and revert to previously saved values.

Message: *Authentication Error HTTPD cache has no valid entry*

Recovery: **1**. Click the Previous button. **2**. Re-enter the misconfigured TACACS+ Server parameter(s). **3**. Continue operation.

Configuration > Aggregation > Static

This page lets you configure Aggregation hash mode and aggregation groups. Aggregation uses multiple ports in parallel to increase the link speed beyond the limits of a port and to increase redundancy for higher availability.



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.

Messages:

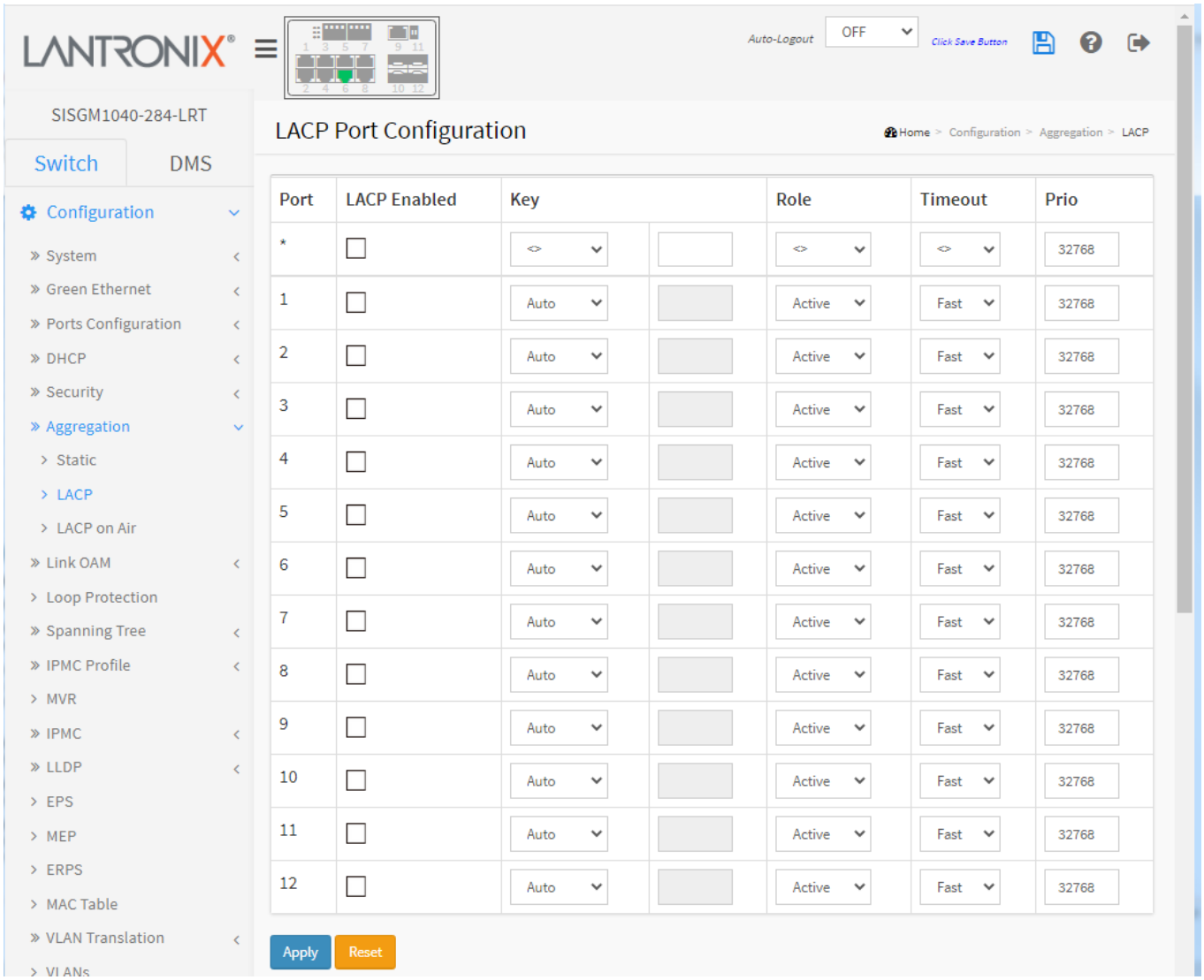
Group 1 member counts error!! Local aggregation must include 2-16 ports

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

Configuration > Aggregation > LACP

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

LACP is an IEEE 802.3ad standard protocol. The Link Aggregation Control Protocol allows bundling several physical ports together to form a single logical port. Note that LACP and Static aggregation cannot both be enabled on the same ports at the same time.



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: Controls the priority of the port, in the range 1-65535. 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.

Configuration > Aggregation > LACP on Air

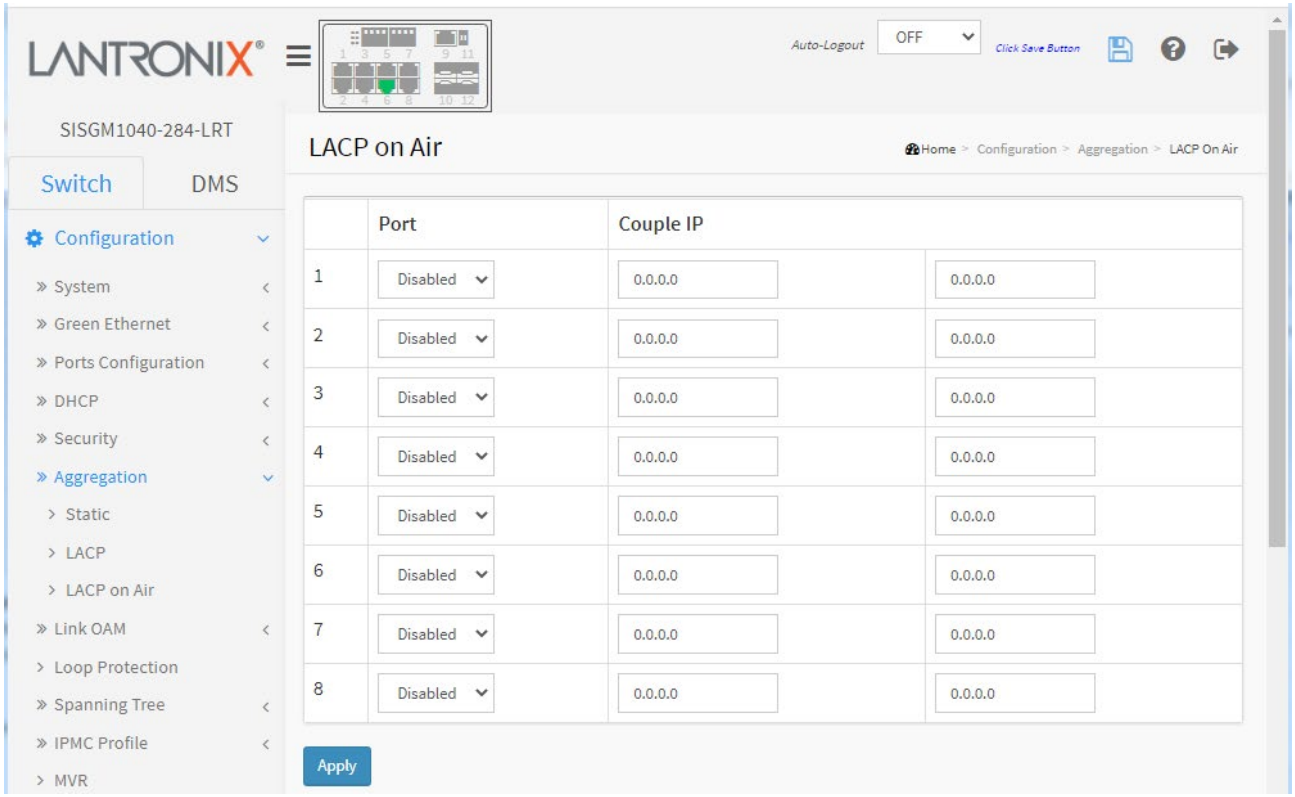
This page lets you set up the LACP on Air ports and the Couple IP address for access management. This feature provides LACP link aggregation via a wireless AP.

In order to achieve LACP load balancing, the switch uses a link aggregation hash algorithm (Source MAC, Destination MAC, and either an IP address or a TCP/UDP port number) to determine the forwarding path within a Link Aggregation Group (LAG). This means packets are forwarded on a path over the link aggregation, but the device may be located on another path. All switches have the same behavior when using the LACP protocol with this kind of application.

LACP on AIR can help to redirect packets to the corresponding path of a device.

To configure LACP on Air parameters in the web UI:

1. Navigate to Configuration > Aggregation > LACP On Air to display the LACP on Air webpage.
2. Enable or disable the LACP on Air for each switch port.
3. In the Couple IP fields enter the IP addresses of the connected partner devices for access management for each port.
4. Click the Apply button.



Parameter descriptions:

Port: To control which switch port should led the access of Couple IP device management.

Couple IP: Specify the connected partners for access management. The Couple IP parameters will be the individual IP addresses of Wireless3 and Wireless4 devices in the example below.

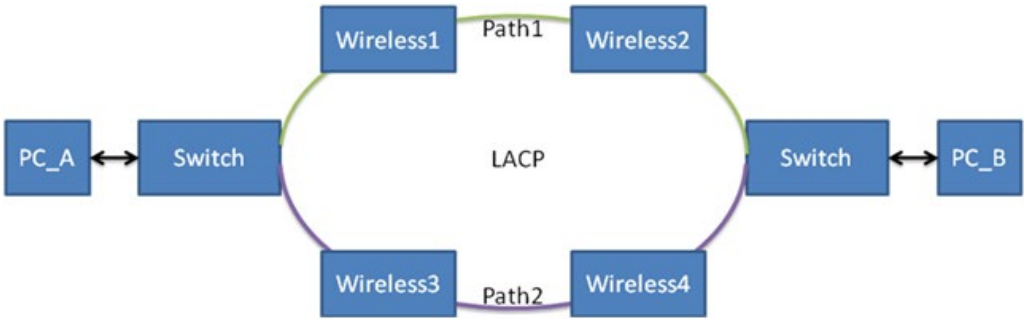
Buttons

Apply: Click to save changes.

Message: *LACP Error - LACP and Static aggregation can not both be enabled on the same ports*
Meaning: Two forms of aggregation cannot be enabled at the same time.
Recovery: **1.** Click the Previous button to clear the error message. **2.** Disable either static aggregation or LACP on Air.

Example:

Suppose PC_A wants to ping to Wireless4, due to link aggregation hash algorithm, ARP and ICMP packets from PC_A will be forwarded on the Path1, but since Wireless4 is located on the Path2, it will cause the ping to fail.

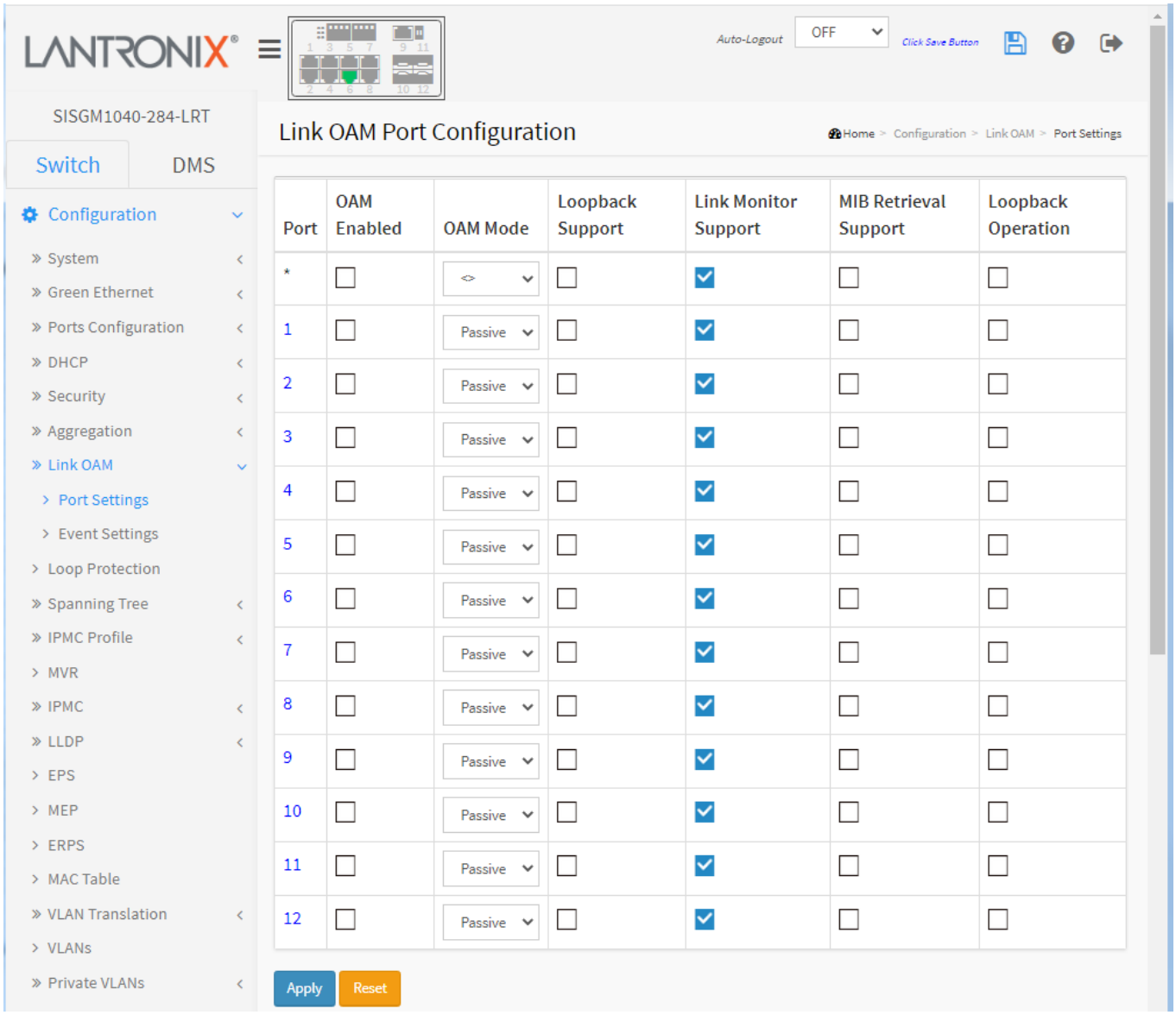


After configuring LACP on AIR, PC_A can ping Wireless4 successfully, since ARP and ICMP packets will be forwarded to Path2.

Configuration > Link OAM > Port Settings

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

OAM (Operation Administration and Maintenance) is a protocol described in ITU-T Y.1731 that is used to implement Carrier Ethernet functionality. MEP functionality such as CC and RDI is based on this.



Parameter descriptions:

Port: The switch port number.

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

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

Active: DTE's configured in Active mode initiate the exchange of Information OAMPDUs as defined by the Discovery process. Once the Discovery process completes, Active DTE's are permitted to send any OAMPDU while connected to a remote OAM peer entity in Active mode. Active DTE's operate in a limited respect if the remote OAM entity is operating in Passive mode. Active devices should not respond to OAM remote loopback commands and variable requests from a Passive peer.

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

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

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

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

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

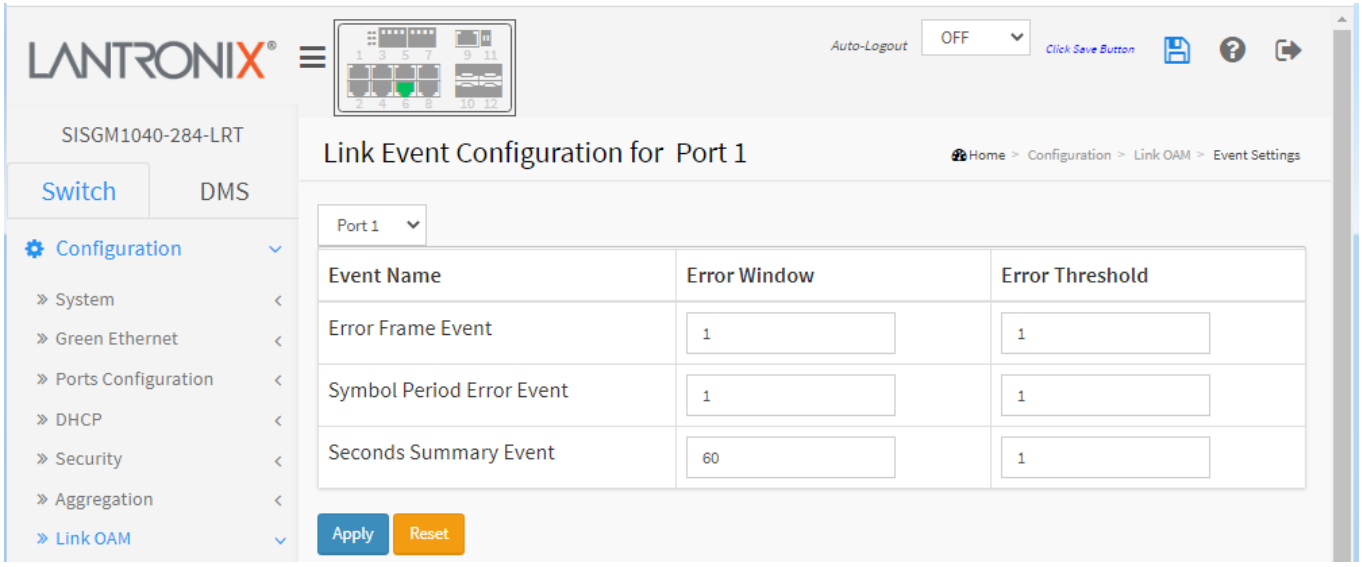
Buttons

Apply: Click to save changes.

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

Configuration > Link OAM > Event Settings

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



Parameter descriptions:

Port: The switch port number.

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

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

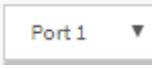
Error Threshold: Represents the threshold value for the window period for the appropriate Link event so as to notify the peer of this error.

Error Frame Event: The Errored Frame Event counts the number of errored frames detected during the specified period. The period is specified by a time interval (Window in order of 1 sec). This event is generated if the errored frame count is equal to or greater than the specified threshold for that period (Period Threshold). Errored frames are frames that had transmission errors as detected at the Media Access Control sublayer. Error Window for 'Error Frame Event' must be an integer value between 1-60 and its default value is '1'. Whereas Error Threshold must be 0-4294967295 and its default value is '0'.

Symbol Period Error Event: The Errored Symbol Period Event counts the number of symbol errors that occurred during the specified period. The period is specified by the number of symbols that can be received in a time interval on the underlying physical layer. This event is generated if the symbol error count is equal to or greater than the specified threshold for that period. Error Window for 'Symbol Period Error Event' must be an integer value of 1-60 and its default value is '1'. Whereas Error Threshold must be 0-4294967295 and its default value is '0'.

Seconds Summary Event: The Errored Frame Seconds Summary Event TLV counts the number of errored frame seconds that occurred during the specified period. The period is specified by a time interval. This event is generated if the number of errored frame seconds is equal to or greater than the specified threshold for that period. An errored frame second is a one second interval wherein at least one frame error was detected. Errored frames are frames that had transmission errors as detected at the Media Access Control sublayer. Error Window for 'Seconds Summary Event' must be an integer value between 10-900 and its default value is '60'. Whereas Error Threshold must be 0-65535 and its default value is '1'.

Buttons



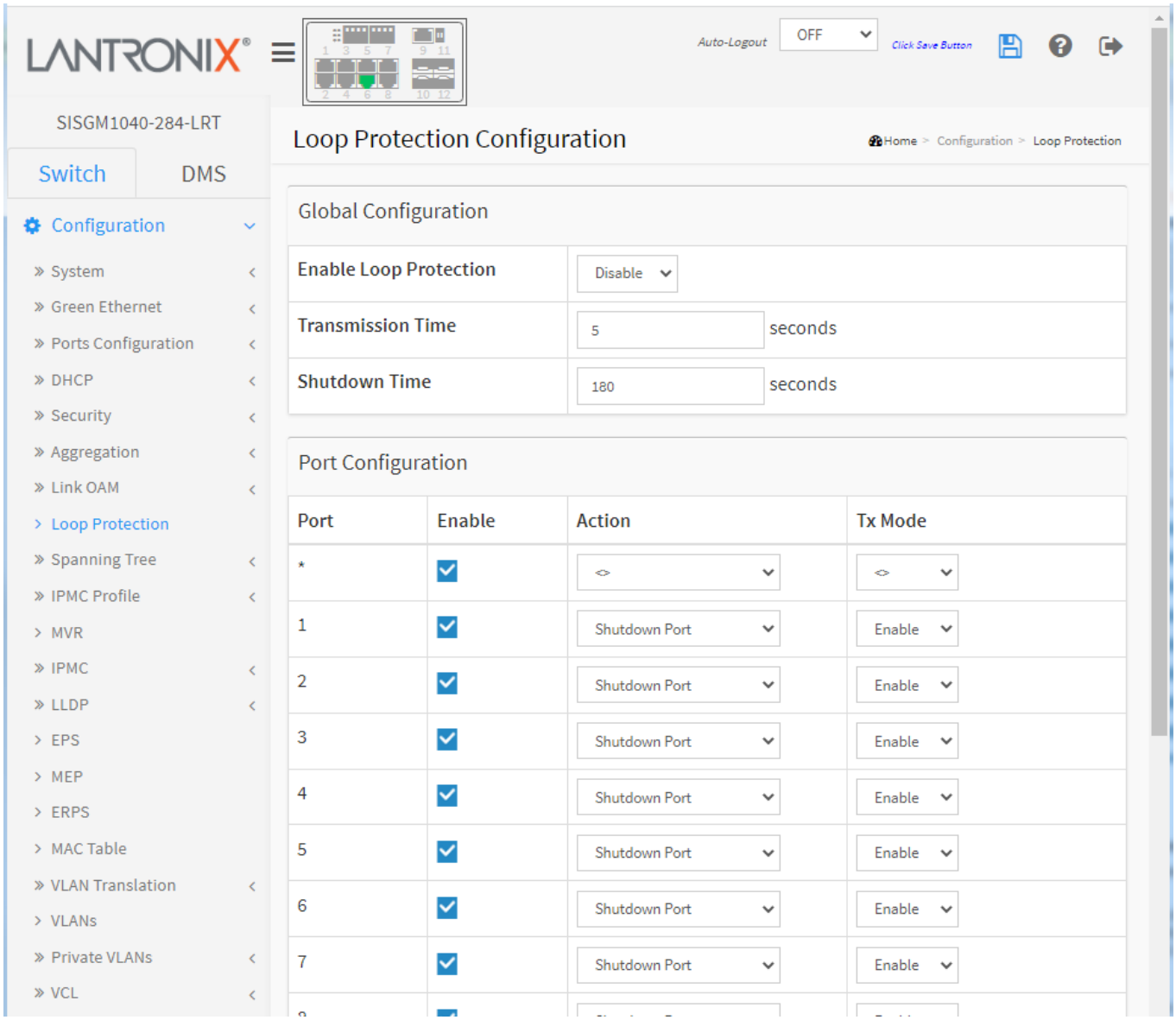
: The port select box determines which port is affected by clicking the buttons.

Apply: Click to save changes.

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

Configuration > Loop Protection

This page lets you view and configure Loop Protection parameters.



Parameter descriptions:

Global Configuration

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

Transmission Time: The interval between each loop protection PDU sent on each port. Valid values are 1 to 10 seconds. Default value is 5 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 is 180 seconds.

Port Configuration

Port: The switch port number of the port.

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

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

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

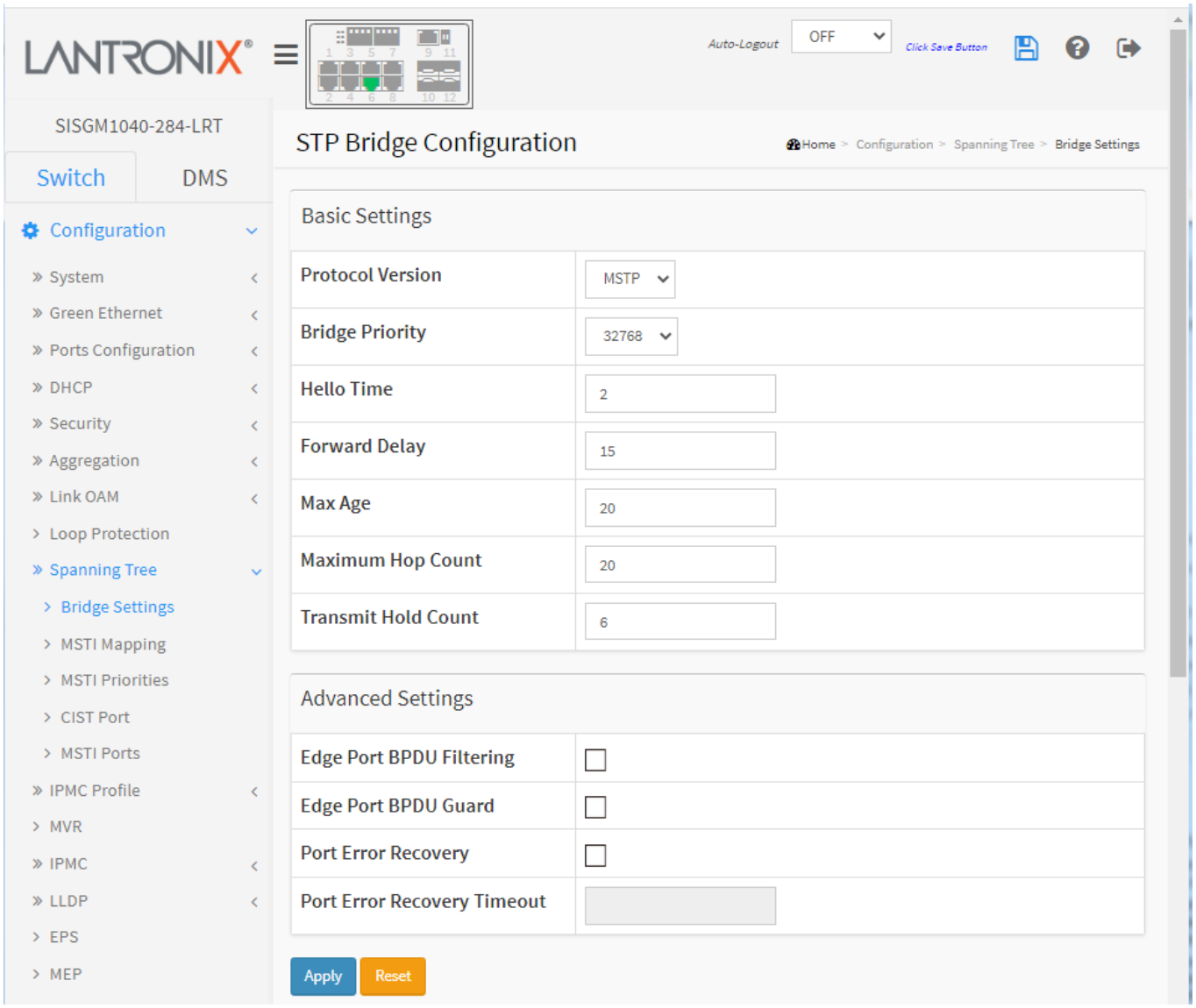
Buttons

Apply: Click to save changes.

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

Configuration > Spanning Tree > Bridge Settings

This page lets you configure STP system settings. The settings are used by all STP Bridge instances in the Switch .



Parameter descriptions:

Basic Settings

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

STP: Spanning Tree Protocol is an OSI layer-2 protocol which ensures a loop free topology for any bridged LAN. The original STP protocol is now obsolete by RSTP.

MSTP: In 2002, the IEEE introduced an evolution of RSTP: the Multiple Spanning Tree Protocol. The MSTP protocol provides for multiple spanning tree instances, while ensuring RSTP and STP compatibility. The standard was originally defined by IEEE 802.1s, but was later incorporated in IEEE 802.1D-2005.

RSTP: In 1998, the IEEE with document 802.1w introduced an evolution of STP: the Rapid Spanning Tree Protocol, which provides for faster spanning tree convergence after a topology change. Standard IEEE 802.1D-2004 now incorporates RSTP and obsoletes STP, while at the same time being backwards-compatible with STP.

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

Hello Time: The interval between sending STP BPDU's. Valid values are in the range 1 to 10 seconds, default is 2 seconds. Note: Changing this parameter from the default value is not recommended and may have adverse effects on your network.

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

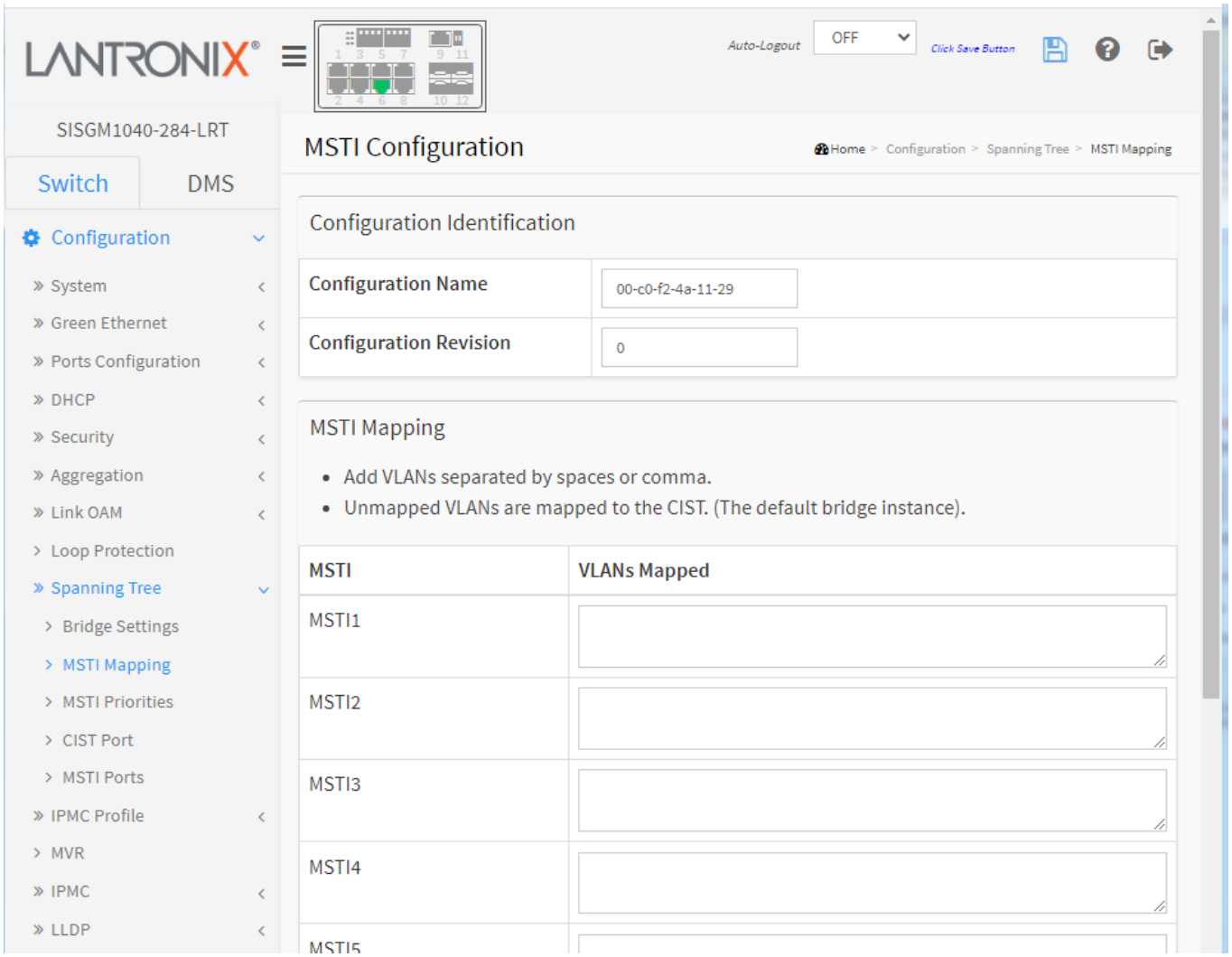
Buttons

Apply: Click to save changes.

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

Configuration > Spanning Tree > MSTI Mapping

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



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

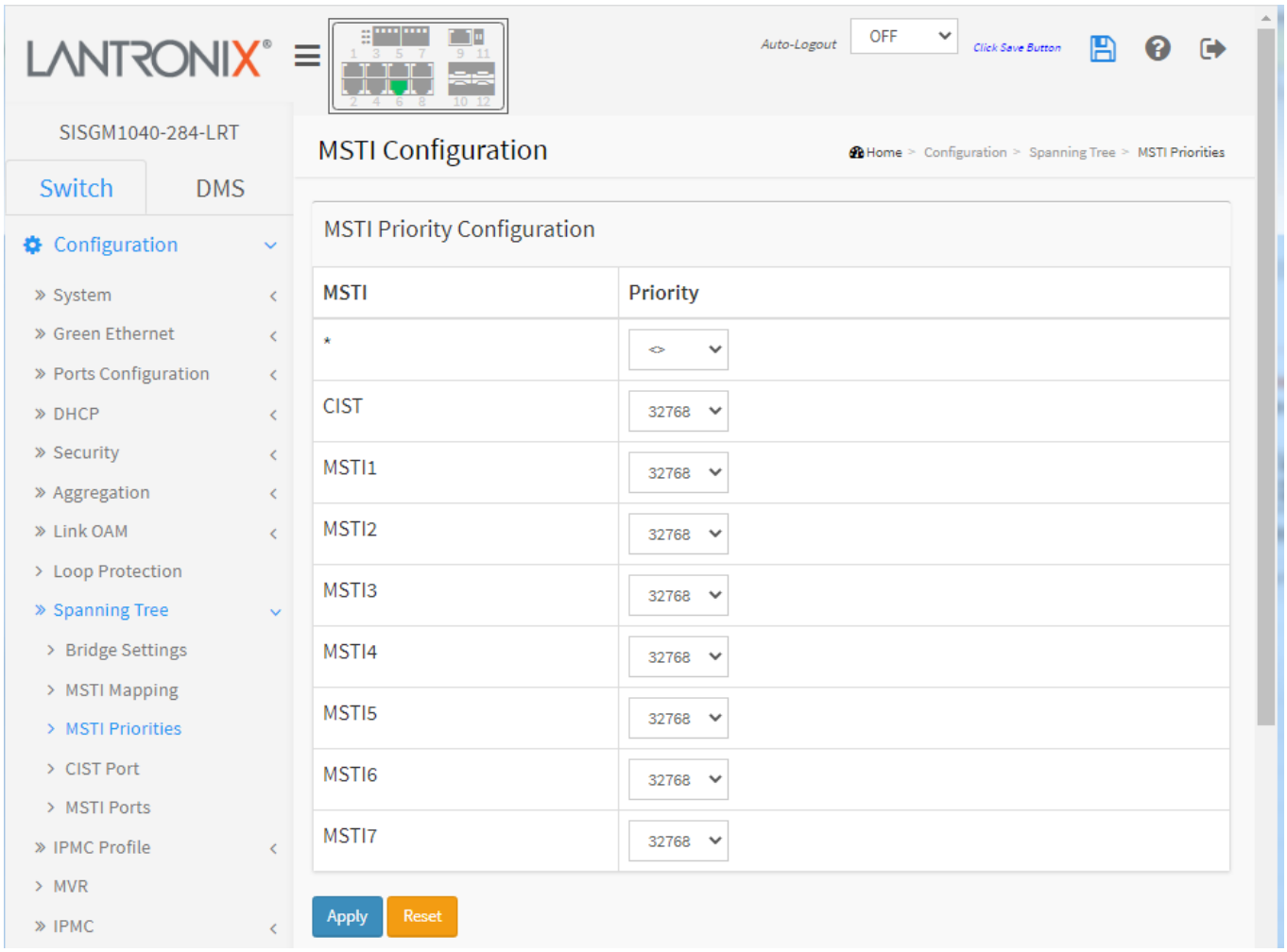
Apply: Click to save changes.

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

Messages: *MST2: VLAN '20' is already mapped to MST1*

Configuration > Spanning Tree > MSTI Priorities

This page lets you view and configure STP MSTI bridge instance priority parameters in the MSTI Priority Configuration table.



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. The valid range is 0-61440. The default is 32768.

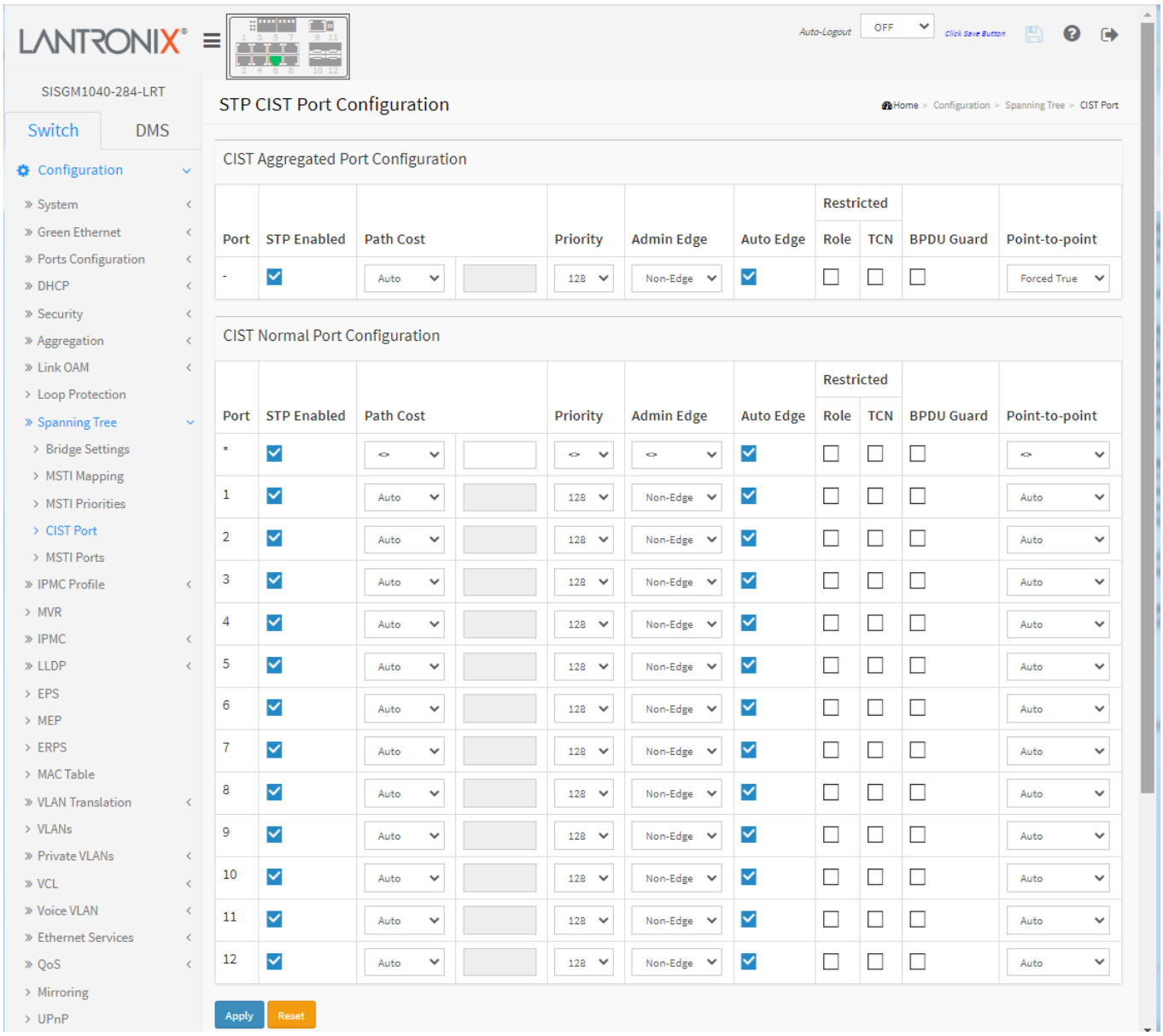
Buttons

Apply: Click to save changes.

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

Configuration > Spanning Tree > CIST Port

This page lets you view and configure STP CIST port parameters. This page contains settings for physical and aggregated ports.



Parameter descriptions:

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

STP Enabled: Controls whether STP is enabled on this switch port. This field will be read only if Voice VLAN feature is enabled. The Voice VLAN port mode will be read only if this field be Enabled.

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

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

operEdge (state flag): Operational flag describing whether the port is connecting directly to edge devices. (No Bridges attached). Transition to the forwarding state is faster for edge ports (having operEdge true) than for other ports. The value of this flag is based on AdminEdge and AutoEdge fields. This flag is displayed as Edge in Monitor->Spanning Tree -> STP Detailed Bridge Status.

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.

Configuration > Spanning Tree > MSTI Ports

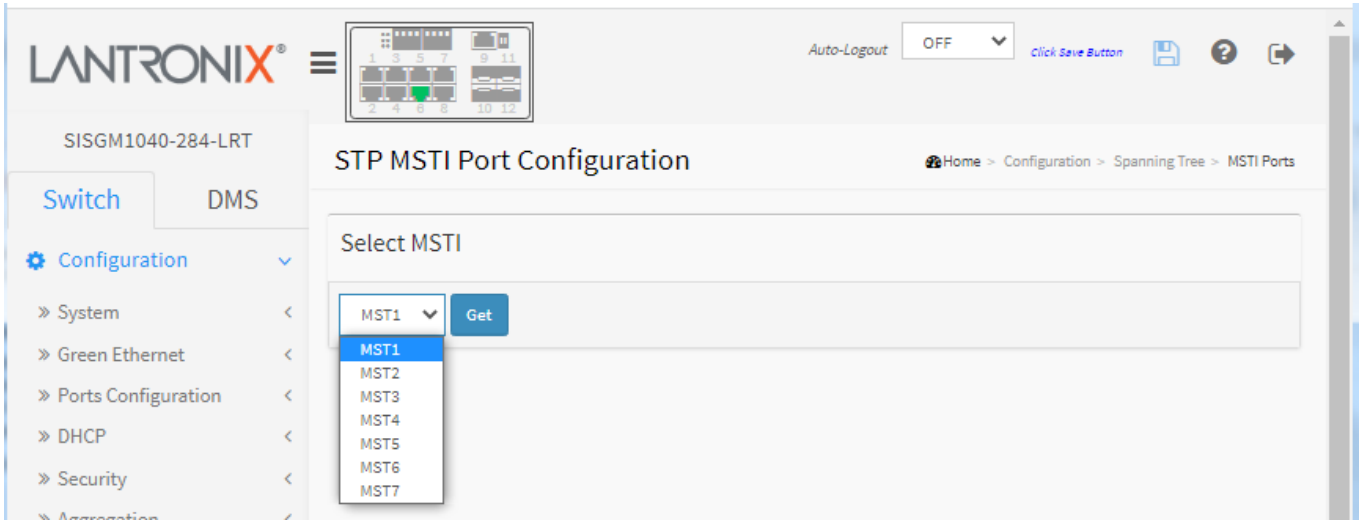
This page lets you configure STP MSTI port parameters.

An MSTI port is a virtual port, which is instantiated separately for each active CIST (physical) port for each MSTI instance configured on and applicable to the port. The MSTI instance must be selected before displaying actual MSTI port configuration options.

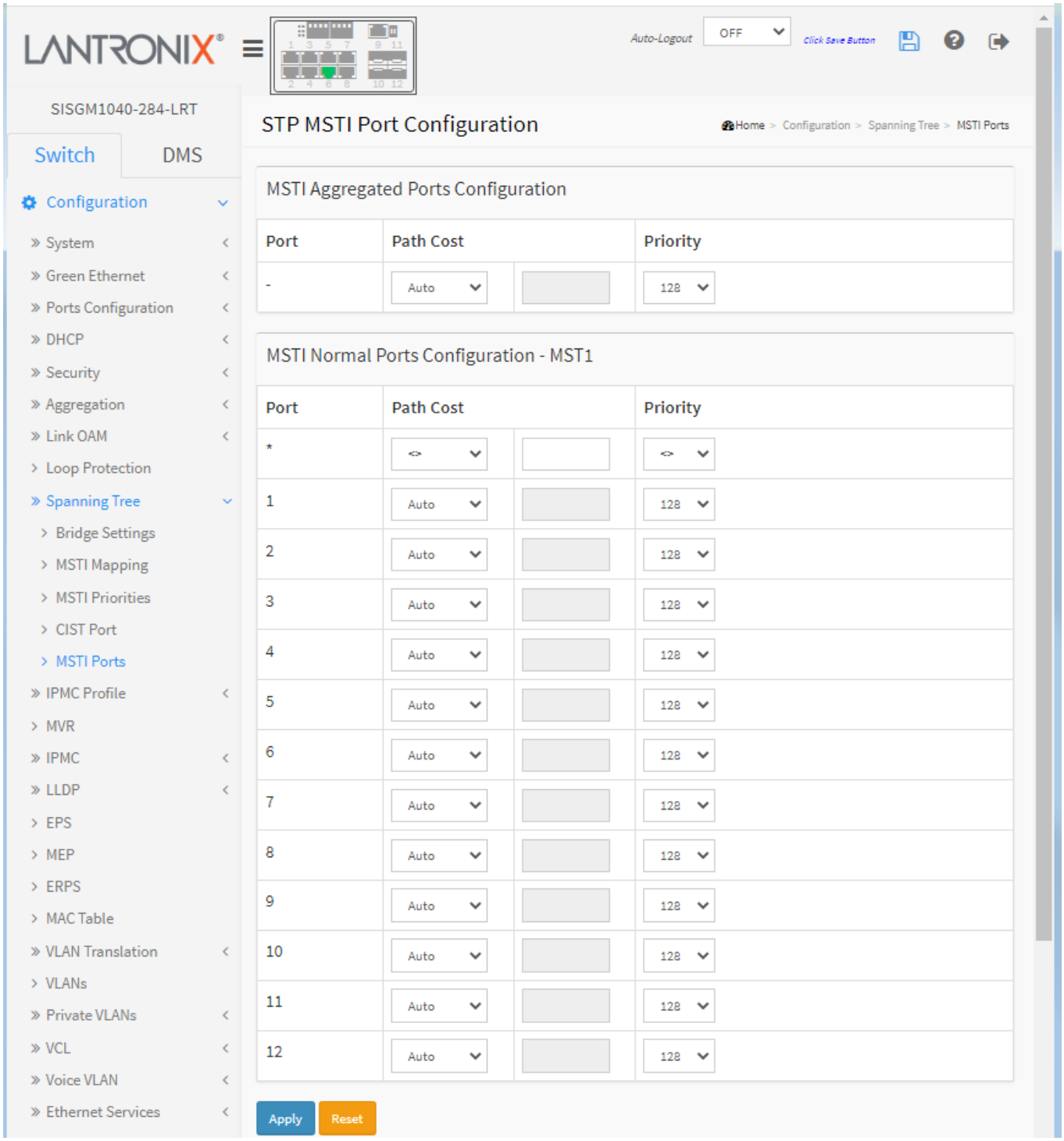
This page contains MSTI port settings for physical and aggregated ports.

The Multiple Spanning Tree Protocol (MSTP) and algorithm, provides both simple and full connectivity assigned to any given VLAN throughout a Bridged Local Area Network. MSTP uses BPDUs to exchange information between spanning-tree compatible devices, to prevent loops in each MSTI (Multiple Spanning Tree Instance) and in the CIST (Common and Internal Spanning Tree), by selecting active and blocked paths.

From the default page dropdown select an MSTI and click the Get button:



At the STP MSTI Port Configuration page enter the parameters as shown and described below.



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 (0-240 in increments of 16). This can be used to control priority of ports having identical port cost (see Path Cost above).

Buttons

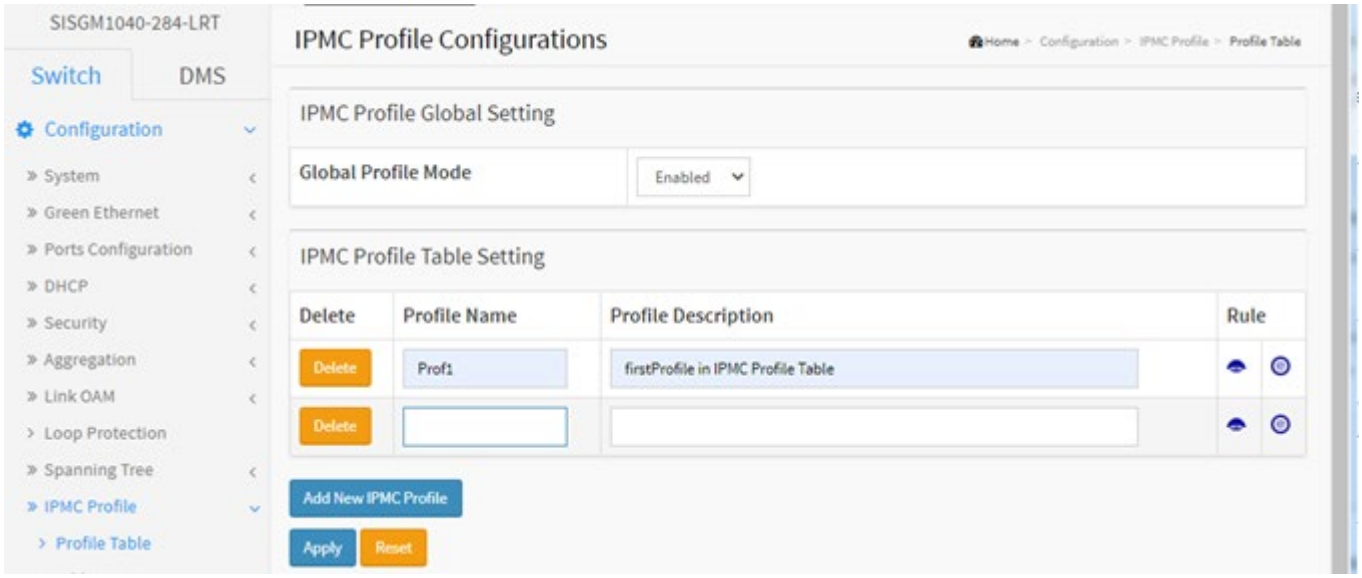
Get: Click to retrieve settings for a specific MSTI.

Apply: Click to save changes.

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

Configuration > IPMC Profile > Profile Table

This page provides IPMC Profile related configurations. An IPMC Profile (IP Multicast Profile) is used to deploy the access control on IP multicast streams. You can create up to 64 Profiles with up to 128 corresponding rules for each Profile.



Parameter descriptions:

Global Profile Mode: Enable/Disable the Global IPMC Profile. The switch 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 these buttons:

: Navigate (List) the rules associated with the designated profile.

: Edit the rules associated with the designated profile.

Buttons

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

Apply: Click to save changes.

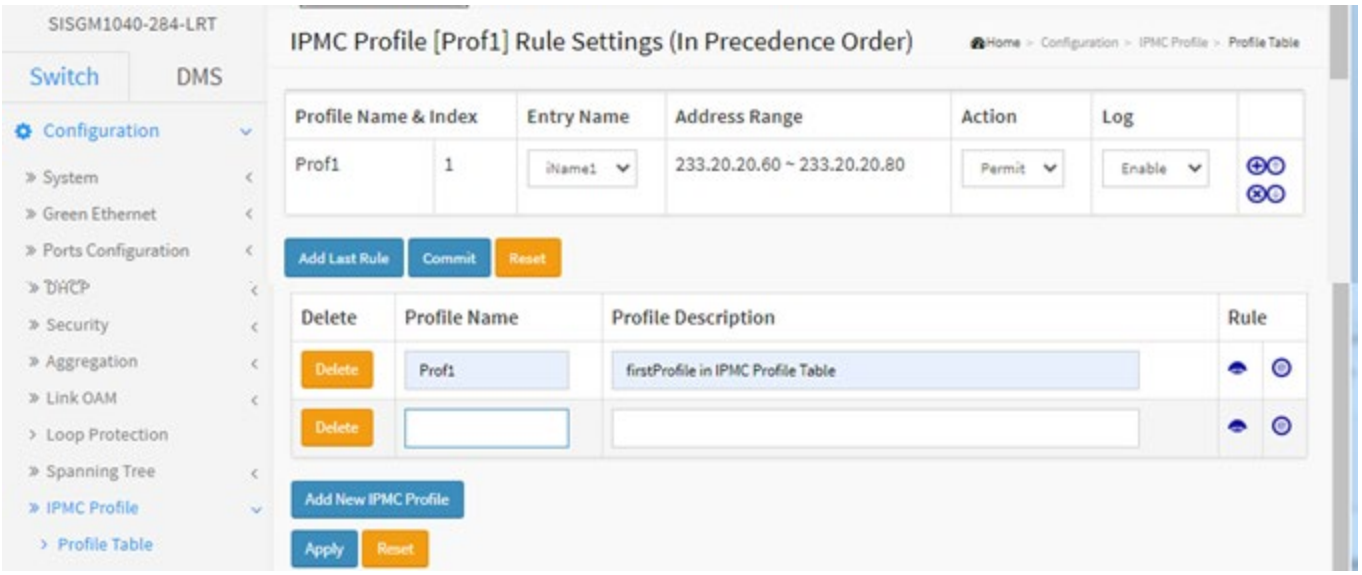
Reset: Click to undo any changes made locally and revert to previously saved values.

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.

1. Click the Edit button ( ) to display the IPMC Profile [Prof1] Rule Settings (In Precedence Order) page.

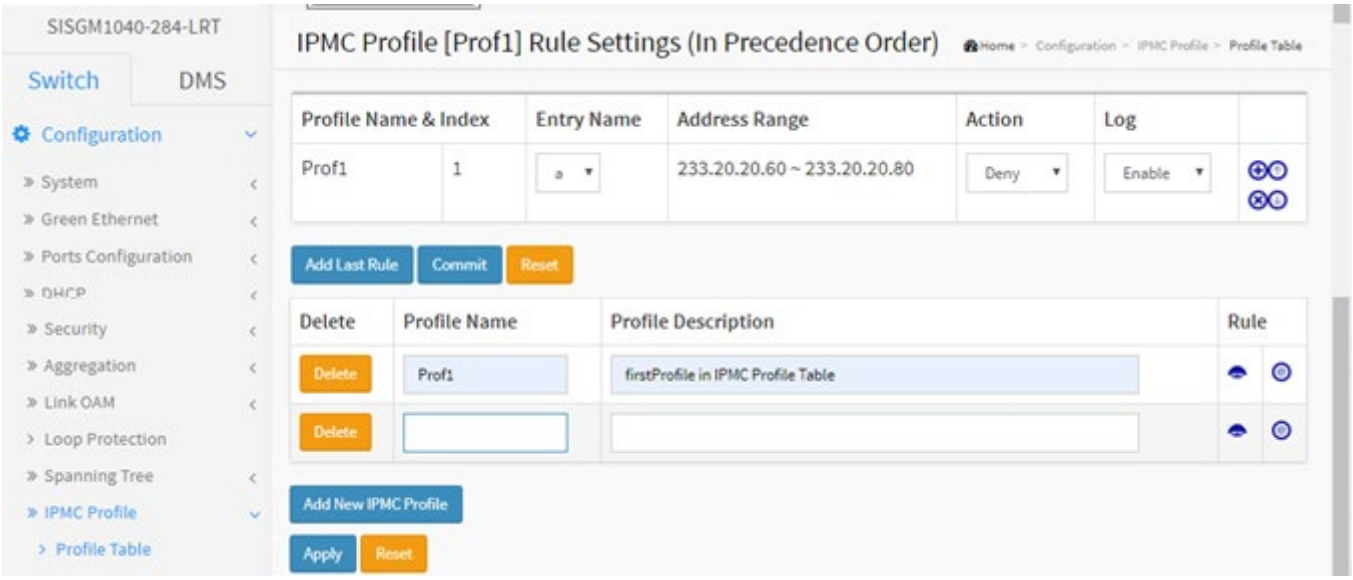
2. Click the Add Last Rule button to display the Rule Settings table:



3. Edit the parameters; see parameter descriptions below.

4. Create an IPMC Profile Address Entry (see next page).

4. Click the Commit button to apply the changes.



Parameter descriptions:

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

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

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

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

Permit: Group address matches the range specified in the rule will be learned.

Deny: Group address matches the range specified in the rule will be dropped.

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

Enable: Corresponding information of the group address, that matches the range specified in the rule, will be logged.

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

Rule Management Buttons: Manage rules and the corresponding precedence order using these buttons:

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

 : **Delete** the current entry of rule.

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

 : **Down**: 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.

Messages:

Please create the Address Entry at first!

Duplicated entry used in the 2nd rule.

Configuration > IPMC Profile > 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.

Parameter descriptions:

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

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

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

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

Buttons

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

Apply: Click to save changes.

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

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

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

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

Messages: *Please input valid IPv4/IPv6 multicast start address for Entry a.*

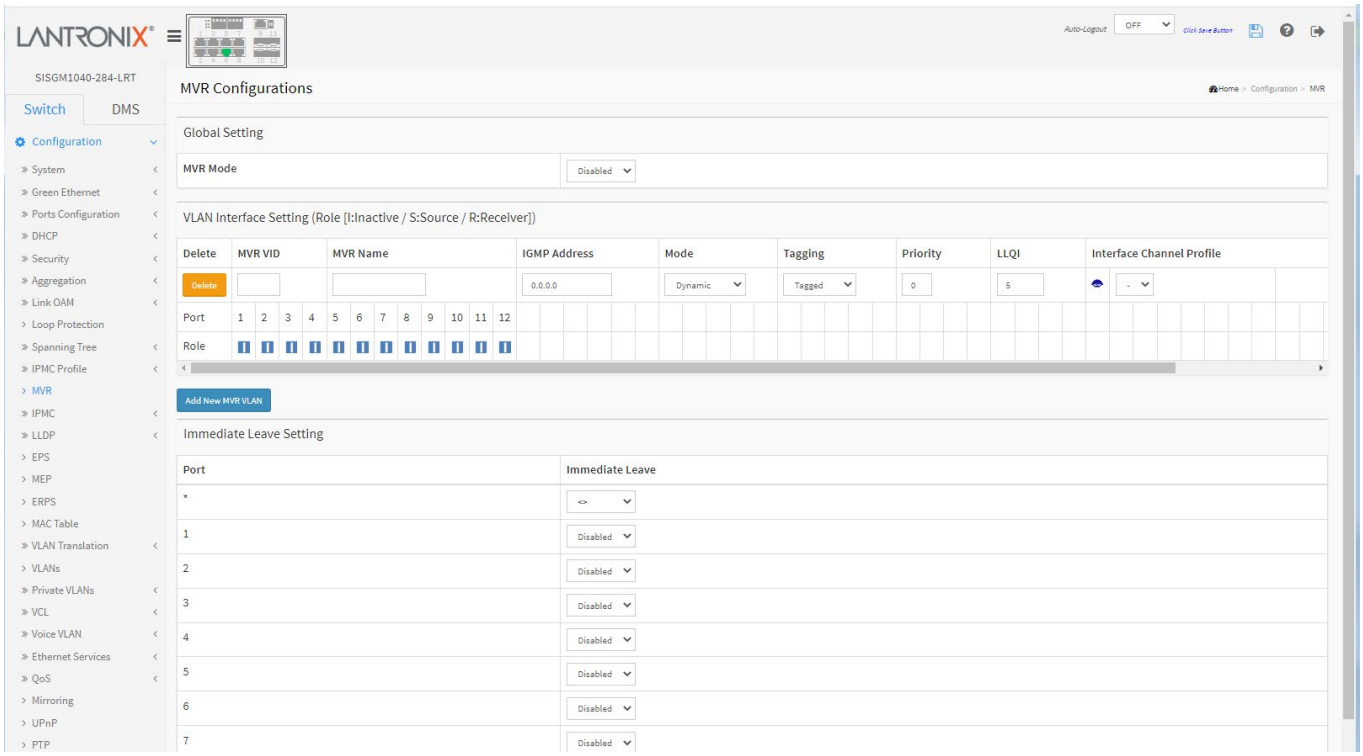
Configuration > MVR

This page provides MVR related configurations. The MVR feature enables multicast traffic forwarding on the Multicast VLANs.

In a multicast television application, a PC or a network television or 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/MLD report message to Switch A to join the appropriate multicast group address. Uplink ports that send and receive multicast data to and from the multicast VLAN are called MVR source ports.

You can create up to four MVR VLANs with corresponding channel profile for each Multicast VLAN.

The channel profile is defined by the IPMC Profile which provides the filtering conditions.



Parameter descriptions:

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

Delete: Check to delete the entry. The designated entry is deleted immediately.

MVR VID: Specify the Multicast VLAN ID. **Caution**: Do not overlap MVR source ports 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 16. MVR VLAN Name can only contain alphabets or numbers. When the optional MVR VLAN name is given, it should contain at least one alphabet. MVR VLAN name can be edited for the existing MVR VLAN entries or it can be added to the new entries.

IGMP Address: Define the IPv4 address as source address used in IP header for IGMP control frames. The default IGMP address is not set (0.0.0.0). When the IGMP address is not set, system uses IPv4 management address of the IP interface associated with this VLAN. When the IPv4 management address is not set, system uses the first available IPv4 management address. Otherwise, system uses a pre-defined value. By default, this is 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 prioritized. 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 Profile: When the MVR VLAN is created, select the IPMC Profile as the channel filtering condition for the specific MVR VLAN. Summary about the Interface Channel Profiling (of the MVR VLAN) will be shown by clicking the view button. Profile selected for designated interface channel is not allowed to have overlapped permit group address.

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

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

Port: The logical port for the settings.

Port Role: Select the port role by clicking the Role symbol to switch the setting. Set an MVR port of the designated MVR VLAN as one of these roles.

Inactive: The designated port does not participate MVR operations. **I** indicates Inactive role (default).

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

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. **R** indicates Receiver role.

Caution: MVR **S**ource ports are not recommended to be overlapped with Management VLAN ports.

Immediate Leave: Enable the fast leave on the port.

Buttons

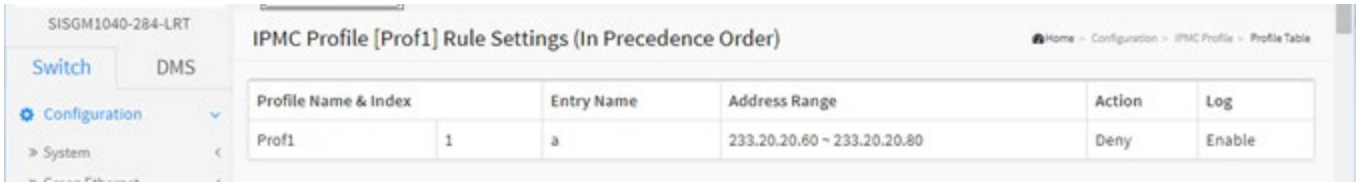
Add New MVR VLAN: Click to add a new MVR VLAN. Specify the VID and configure the new entry.

Apply: Click to save changes.

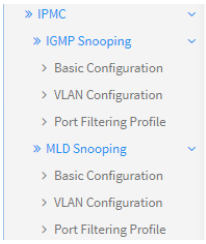
Reset: Click to undo any changes made locally and revert to previously saved values.

Messages: *Failure in SET MVR VLAN VID 30*

Example:

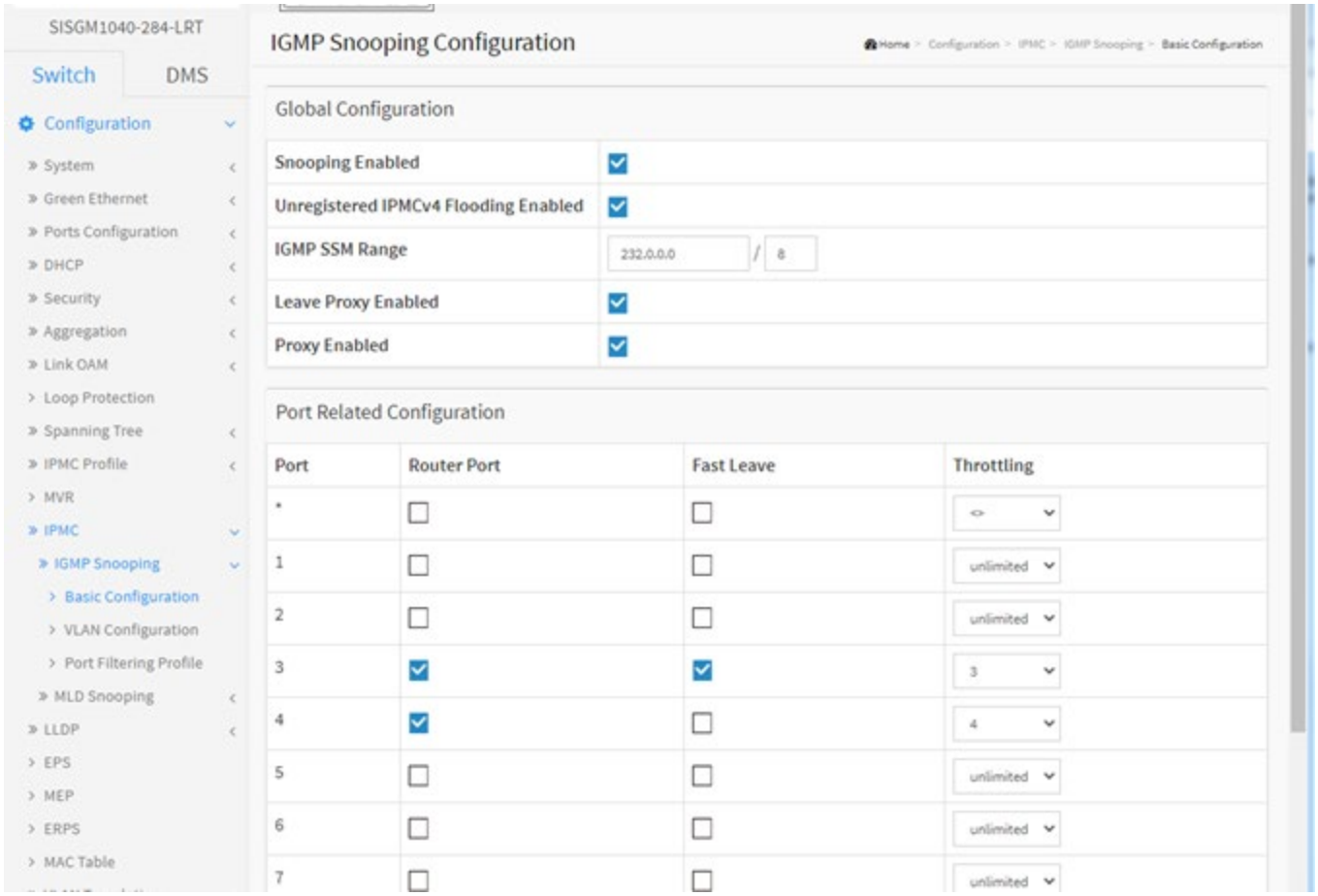

SISGM1040-284-LRT
Switch
DMS
Configuration
System
IPMC Profile [Prof1] Rule Settings (In Precedence Order)
Home > Configuration > IPMC Profile > Profile Table
Profile Name & Index
Entry Name
Address Range
Action
Log
Prof1
1
a
233.20.20.60 ~ 233.20.20.80
Deny
Enable

Configuration > IPMC > IGMP Snooping > Basic Configuration



This page provides IGMP Snooping related configuration.

IGMP (Internet Group Management Protocol) is a communications protocol used to manage the membership of Internet Protocol multicast groups. IGMP is used by IP hosts and adjacent multicast routers to establish multicast group memberships. It is an integral part of the IP multicast specification, like ICMP for unicast connections. IGMP can be used for online video and gaming, and allows more efficient use of resources when supporting these uses.



Global Configuration

Snooping Enabled: Check to enable IGMP Snooping globally.

Unregistered IPMCv4 Flooding Enabled: Check to enable unregistered IPMCv4 traffic flooding. The flooding control takes effect only when IGMP Snooping is enabled. When IGMP Snooping is disabled, unregistered IPMCv4 traffic flooding is always active despite this setting.

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. Assign a valid IPv4 multicast address as prefix with a prefix length (from 4 to 32) for the range.

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

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

Port Related Configuration

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

Buttons

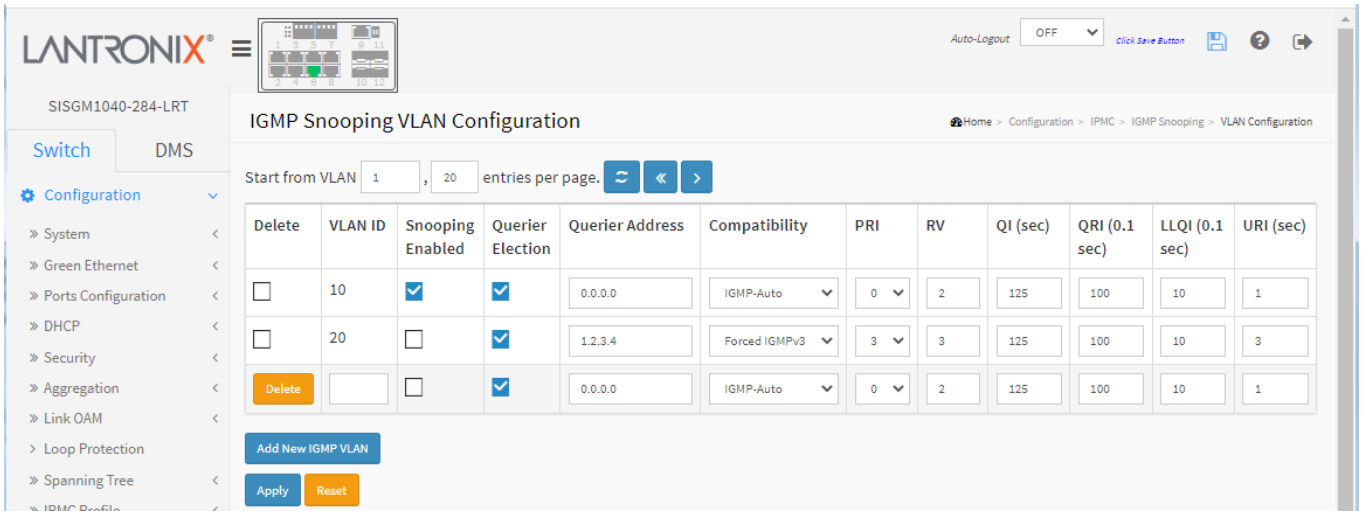
Apply: Click to apply changes immediately.

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

Configuration > IPMC > IGMP Snooping > VLAN Configuration

Each page shows up to 99 entries from the VLAN table, default being 20, selected through the "entries per page" input field. When first visited, the web page will show the first 20 entries from the beginning of the VLAN table. The first displayed will be the one with the lowest VLAN ID found in the VLAN table.

The "VLAN" input fields let you select the starting point in the VLAN table.



Parameter descriptions:

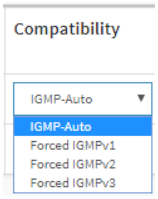
Delete: Check to delete the entry. The designated entry will be deleted during the next save.

VLAN ID: The VLAN ID of the entry.

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

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

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



Compatibility: Compatibility is maintained by hosts and routers taking appropriate actions depending on the versions of IGMP operating on hosts and routers within a network.
The allowed selections are IGMP-Auto, Forced IGMPv1, Forced IGMPv2, and Forced IGMPv3.
The 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); the 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 and the default robustness variable value is 2.

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

QRI (0.1 sec): Query Response Interval. The Maximum Response Delay used to calculate the Maximum Response Code inserted into the periodic General Queries. The allowed range is 0 to 31744 in tenths of seconds; the default query response interval is 100 in tenths of seconds (10 seconds).

LLQI (0.1 sec): (LMQI for IGMP): Last Member Query Interval; the time value represented by the Last Member Query Interval, multiplied by the Last Member Query Count. The allowed range is 0 to 31744 in tenths of seconds, default last member query interval is 10 in tenths of seconds (1 second).

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

Buttons

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

<< : Updates the table starting from the first entry in the VLAN Table, i.e. the entry with the lowest VLAN ID.

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

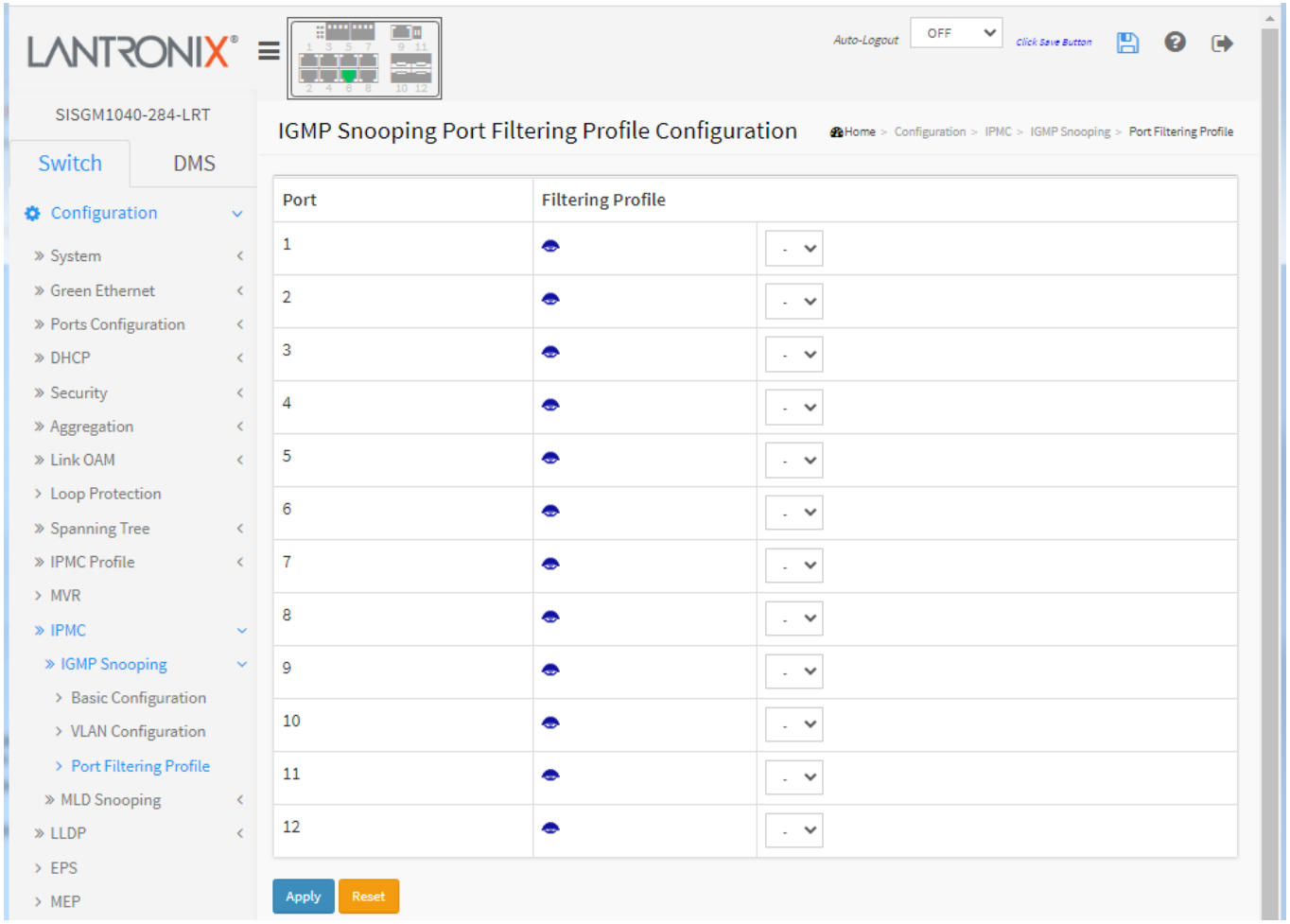
Add New IGMP VLAN: : Click to add new IGMP VLAN. Specify the VID and configure the new entry. The specific IGMP VLAN starts working after the corresponding static VLAN is also created.

Apply: Click to save changes.

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

Configuration > IPMC > IGMP Snooping > Port Filtering Profile

This page lets you set an IPMC filtering profile on a per-port basis.



Parameter descriptions:

Port: The logical port for the settings.

Filtering Profile: Select the IPMC Profile as the filtering condition for the specific port. Summary about the designated profile will be shown by clicking the view button.

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

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

Buttons

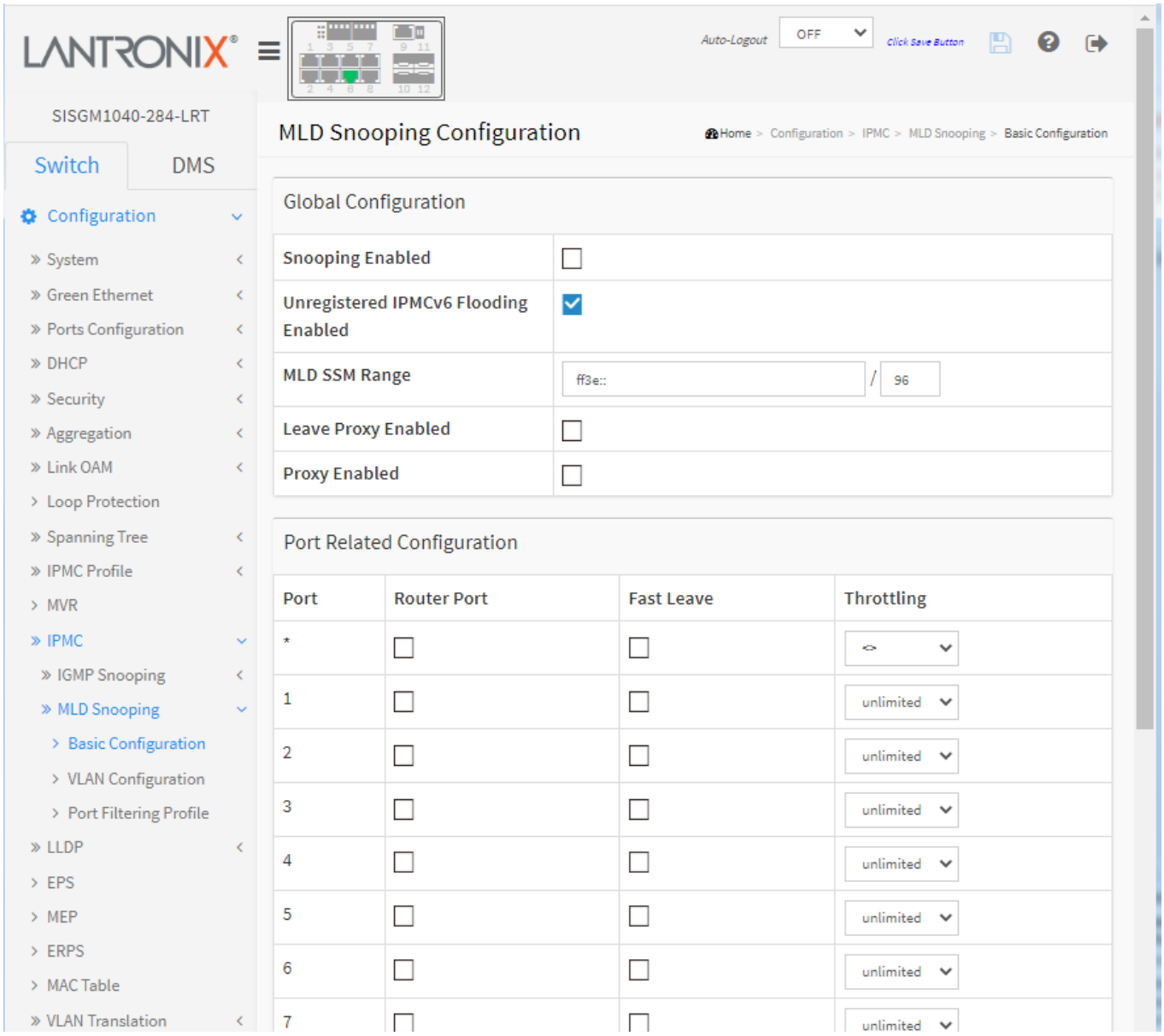
Apply: Click to apply changes immediately.

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

Configuration > IPMC > MLD Snooping > Basic Configuration

This page provides MLD Snooping related configuration.

MLD (Multicast Listener Discovery for IPv6) is used by IPv6 routers to discover multicast listeners on a directly attached link, much as IGMP is used in IPv4. The protocol is embedded in ICMPv6 instead of using a separate protocol.



Parameter descriptions:

Snooping Enabled: Enable the Global MLD Snooping.

Unregistered IPMCv6 Flooding Enabled: Check the box to 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 despite 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 range. Assign valid IPv6 multicast address as prefix with a prefix length (from 8 to 128) for the range.

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

Proxy Enabled: Check to 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 fast leave on the port.

Throttling: At the dropdown select the number of multicast groups to which a switch port can belong (Unlimited or 1-10).

Buttons

Apply: Click to apply changes immediately.

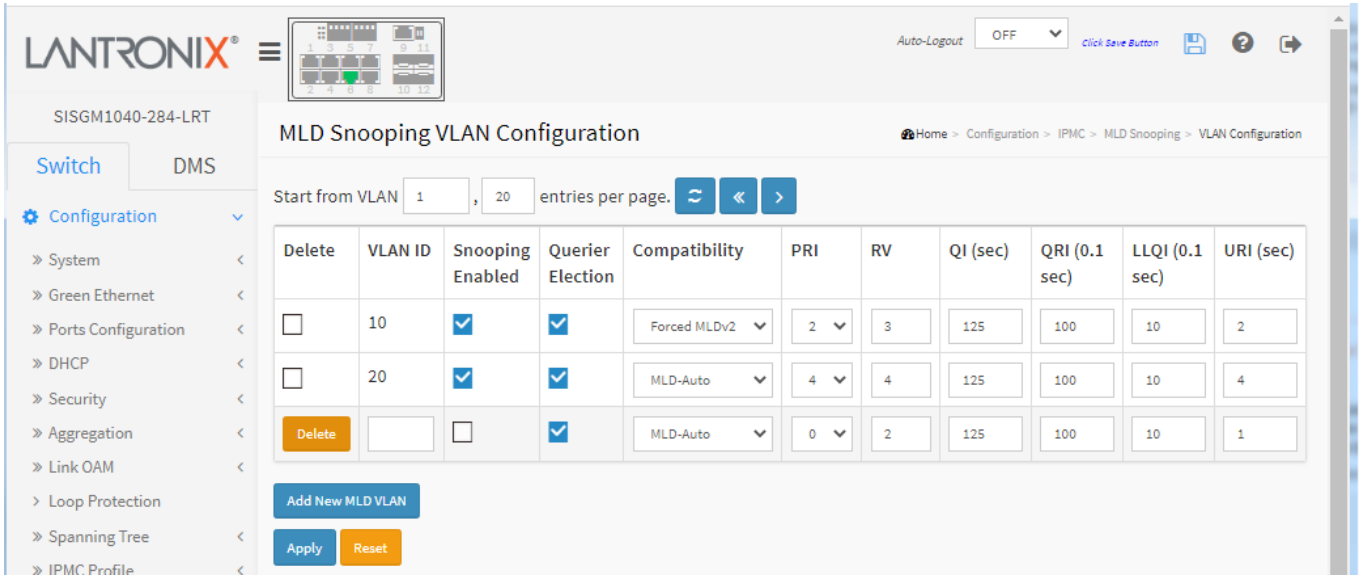
Reset: Click to undo any changes made locally and revert to previously saved values.

Configuration > IPMC > MLD Snooping > VLAN Configuration

This page lets you set MLD Snooping VLAN parameters.

Each page shows up to 99 entries from the VLAN table, default being 20, selected through the "entries per page" input field. When first visited, the web page will show the first 20 entries from the beginning of the VLAN table. The first displayed will be the one with the lowest VLAN ID found in the VLAN Table.

The "VLAN" input fields let you select the starting point in the VLAN table.



Parameter descriptions:

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

VLAN ID: The VLAN ID of the entry.

Snooping Enabled: Check to enable the per-VLAN MLD Snooping. Up to 32 VLANs can be selected for MLD Snooping.

Querier Election: Check to enable to join MLD Querier election in the VLAN. Disable to act as a MLD Non-Querier.

Compatibility: Compatibility is maintained by hosts and routers taking appropriate actions depending on the versions of MLD operating on hosts and routers within a network. The allowed selections are MLD-Auto, Forced MLDv1, and Forced MLDv2; the default compatibility value is MLD-Auto.

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

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

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

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

LLQI: Last Listener Query Interval is the Maximum Response Delay used to calculate the Maximum Response Code inserted into Multicast Address Specific Queries sent in response to Version 1 Multicast Listener Done messages. It is also the Maximum Response Delay used to calculate the Maximum Response Code inserted into Multicast Address and Source Specific Query messages. The allowed range is 0 to 31744 in tenths of seconds; the default last listener query interval is 10 in tenths of seconds (1 second).

URI: Unsolicited Report Interval is the time between repetitions of a node's initial report of interest in a multicast address. The allowed range is 0 to 31744 seconds; the default unsolicited report interval is 1 second.

Buttons

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

<< : Updates the table starting from the first entry in the VLAN Table, i.e. the entry with the lowest VLAN ID.

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

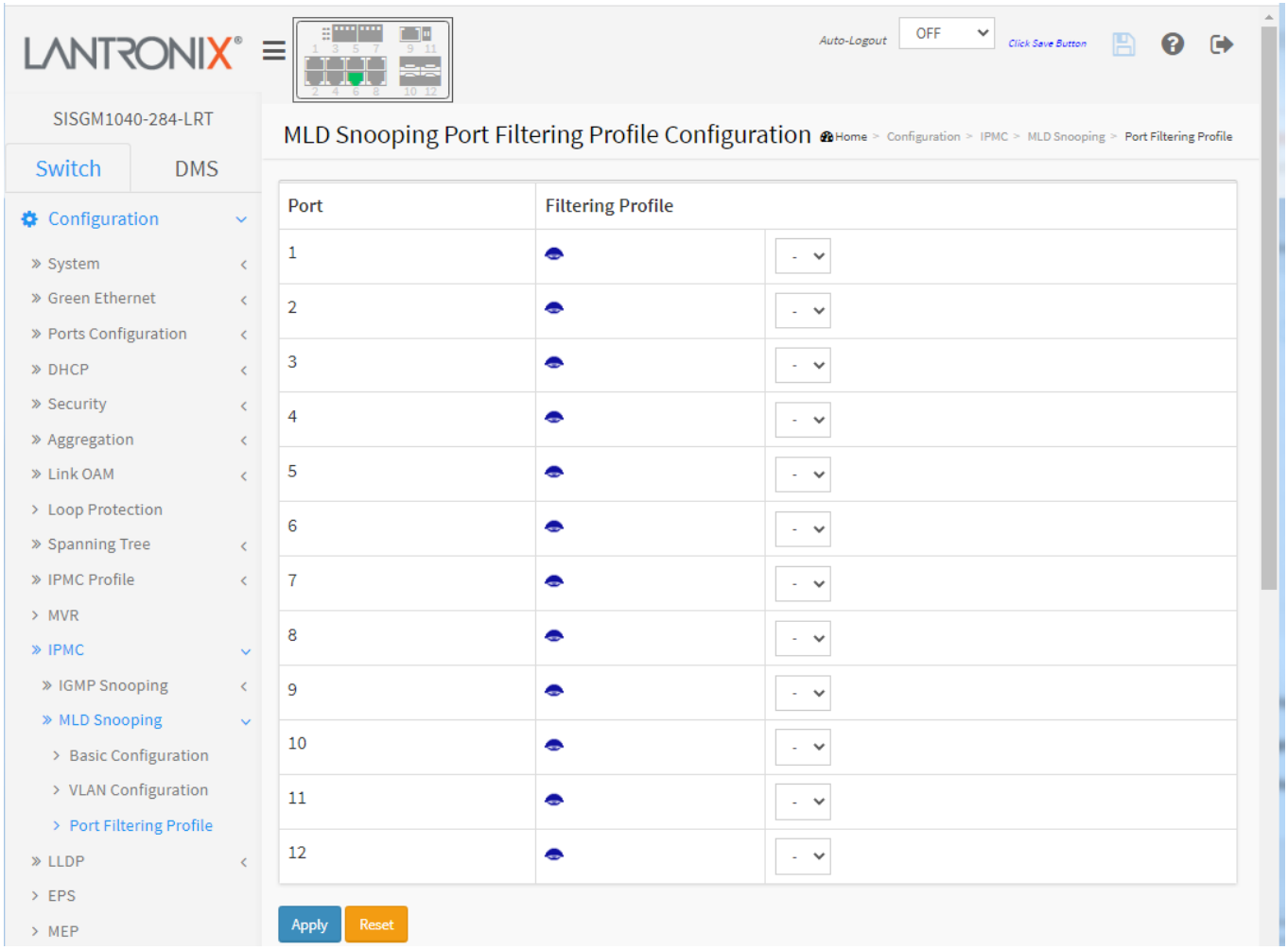
Add New MLD VLAN : Click to add new MLD VLAN. Specify the VID and configure the new entry. Click "Apply". The specific MLD VLAN starts working after the corresponding static VLAN is also created.

Apply: Click to save changes.

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

Configuration > IPMC > MLD Snooping > Port Filtering Profile

This page lets you select the IPMC Profile as the filtering condition for each port.



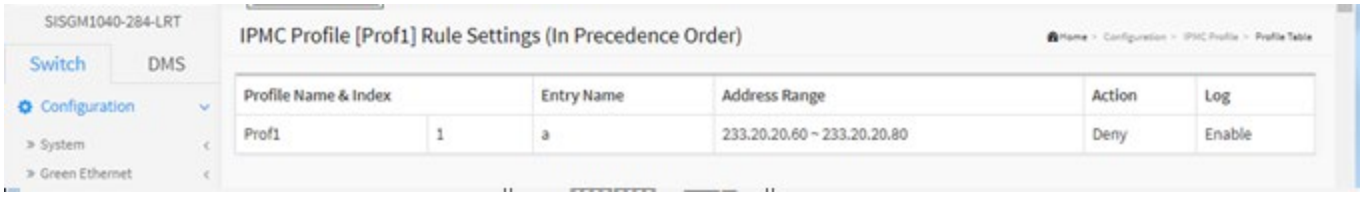
Port: The logical port for the settings.

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

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

Navigate: List the rules associated with the designated profile.

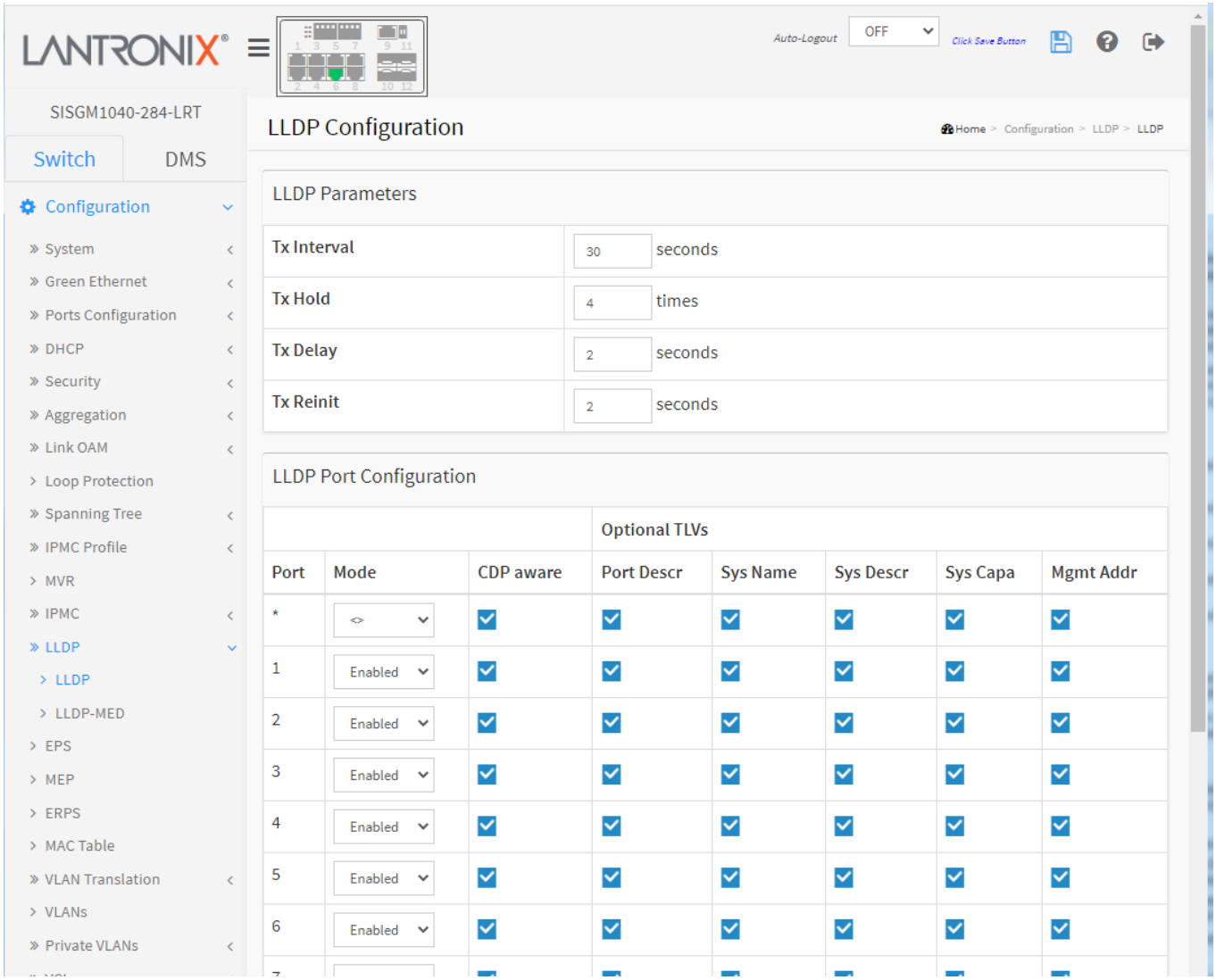
Example:



Configuration > LLDP > LLDP

This page lets you view and configure LLDP interface parameters.

LLDP is an IEEE 802.1ab standard protocol. The Link Layer Discovery Protocol (LLDP) specified in this standard allows stations attached to an IEEE 802 LAN to advertise, to other stations attached to the same IEEE 802 LAN, the major capabilities provided by the system incorporating that station, the management address or addresses of the entity or entities that provide management of those capabilities, and the identification of the stations point of attachment to the IEEE 802 LAN required by those management entity or entities. The information distributed via this protocol is stored by its recipients in a standard Management Information Base (MIB), making it possible for the information to be accessed by a Network Management System (NMS) using a management protocol such as the Simple Network Management Protocol (SNMP).



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 time the information in the LLDP frame will be considered valid. The LLDP information valid period is set to Tx Hold multiplied by Tx Interval seconds. Valid values are 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 an interface is disabled, LLDP is disabled or the switch is rebooted, a LLDP shutdown frame is transmitted to the neighboring units, signaling that the LLDP information isn't valid anymore. Tx Reinit controls the number of seconds between the shutdown frame and a new LLDP initialization. Valid values are restricted to 1 - 10 seconds.

LLDP Port Configuration

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

Mode: Select LLDP mode:

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

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

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

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

Optional TLVs

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

Note: When CDP awareness on an interface is disabled the CDP information isn't removed immediately, but gets removed 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.

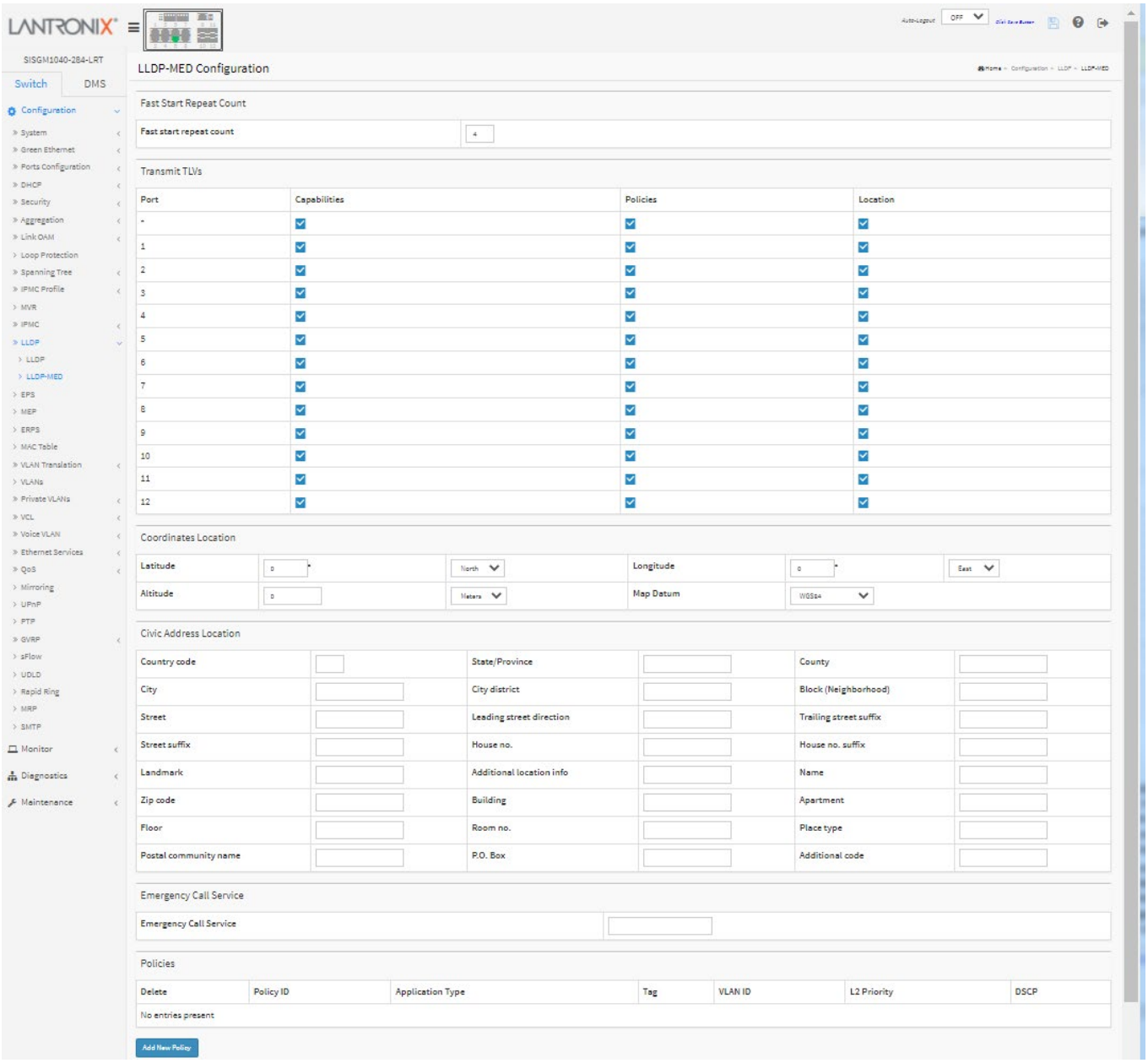
Buttons

Apply: Click to save changes.

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

Configuration > LLDP > LLDP-MED

This page allows you to configure the LLDP-MED. This function applies to VoIP devices which support LLDP-MED. LLDP-MED is an extension of IEEE 802.1ab defined by the Telecommunication Industry Association (TIA-1057).



Parameter descriptions:

Fast start repeat count

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.

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 interface. The LLDP-MED application will temporarily speed up the transmission of the LLDPDU to start within a second, when a new LLDP-MED neighbor has been detected in order share LLDP-MED information as fast as possible to new neighbors.

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

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

Transmit TLVs: It is possible to select which LLDP-MED information that 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.

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 -2097151.9 to 2097151.9 with a maximum of 1 digit. 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 of 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). The total number of characters for the combined civic address information must not exceed 250 characters. A couple of notes to the limitation of 250 characters.

1) A non-empty civic address location will use 2 extra characters in addition to the civic address location text.

2) The 2 letter country code is not part of the 250 characters limitation.

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

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

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

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

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

Block (Neighborhood): Neighborhood, block.

Street: Street - Example: Poppelvej.

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

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

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

House no.: House number - Example: 21.

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

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

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

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

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

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

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

Floor: Floor - Example: 4.

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

Place type: Place type - Example: Office.

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

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

Additional code: Additional code - Example: 1320300003.

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

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

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

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

The network policy attributes advertised are:

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

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

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

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

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

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

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

Application Type: Intended use of the application types:

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

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

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

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

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

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

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

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

Tag: Indicates 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 interface 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: 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.

Adding a new policy: Click Add New Policy to add a new policy. Specify the Application type, Tag, VLAN ID, L2 Priority and DSCP for the new policy. Click "Apply". The number of policies supported is 32

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

Interface: The interface name to which the configuration applies.

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

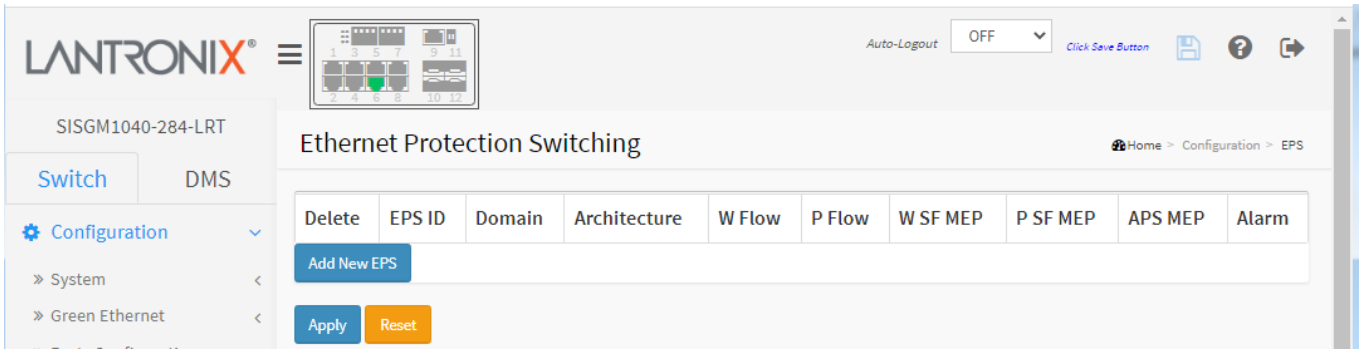
Buttons

Apply: Click to apply changes immediately.

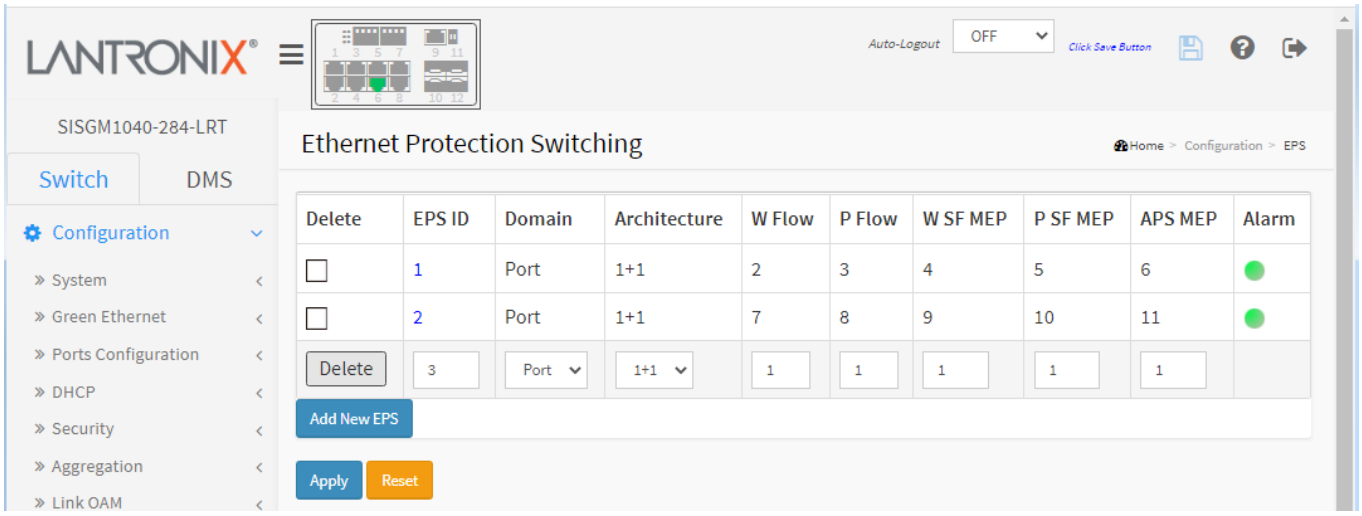
Reset: Click to undo any changes made locally and revert to previously saved values.

Configuration > EPS

The Ethernet (Linear) Protection Switch instances are configured here. EPS (Ethernet Protection Switching) is defined in ITU-T G.8031. From the default page click the Add New EPS button to display the EPS config table:



↓↓↓↓



Parameter descriptions:

Delete: This box is used to mark an EPS for deletion in next Save operation.

EPS ID: The ID of the EPS. Click on the ID of an EPS to enter the EPS Configuration page (see below). The valid range is 1-100.

Domain: Port: This will create a EPS in the Port Domain. 'W/P Flow' is a Port.

Architecture: Port: This will create a 1+1 EPS.

Port: This will create a 1:1 EPS.

W Flow: The working flow for the EPS - See 'Domain'.

P Flow: The protecting flow for the EPS - See 'Domain'.

W SF MEP: The working Signal Fail reporting MEP.

P SF MEP: The protecting Signal Fail reporting MEP.

APS MEP: The APS PDU handling MEP.

Alarm: There is an active alarm on the EPS.

Buttons

Add New EPS: Click to add a new EPS entry.

Apply: Click to save changes.

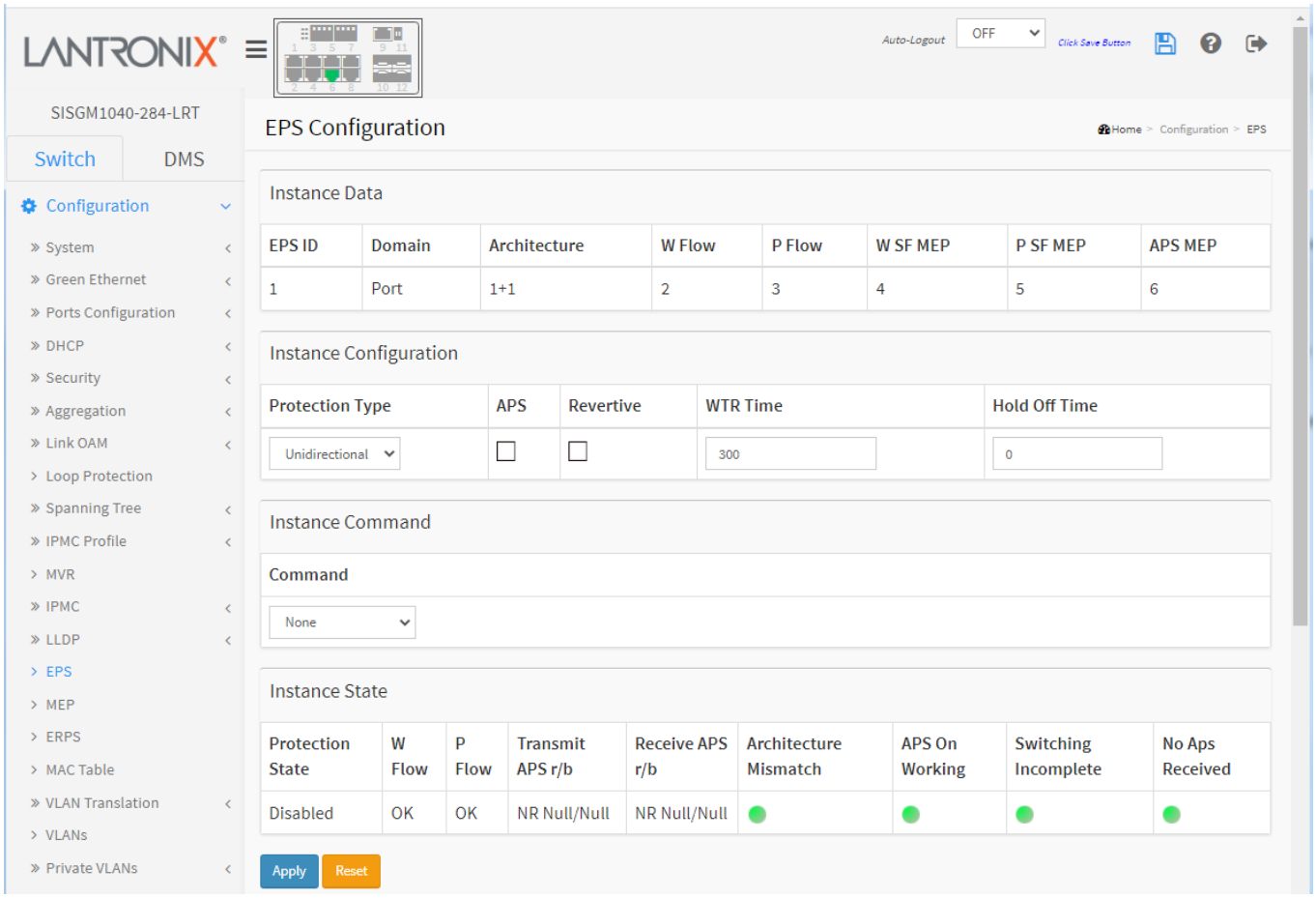
Reset: Click to undo any changes made locally and revert to previously saved values.

Messages:

Only one EPS can be added for each Apply operation
The working and protection flows are equal
Working MEP and protecting SF MEP is same instance

EPS Configuration page

On the Ethernet Protection Switching page, click on the ID of an EPS to enter its configuration page:



Parameter descriptions:

Instance Data:

EPS ID: The ID of the EPS. Click on the ID of an EPS to enter the configuration page. The range is 1-100.

Domain: Port: This will create a EPS in the Port Domain. 'W/P Flow' is a Port.

Architecture: Port: This will create a 1+1 EPS.

W Flow: The working flow for the EPS - See 'Domain'.

P Flow: The protecting flow for the EPS - See 'Domain'.

W SF MEP: The working Signal Fail reporting MEP.

P SF MEP: The protecting Signal Fail reporting MEP.

APS MEP: The APS PDU handling MEP.

Instance Configuration

Protection Type:

Unidirectional: EPS in the two ends can select traffic from different working/protecting flow. This is only possible in case of 1+1.

Bidirectional: EPS in the two ends is selecting traffic from the same working/protecting flow. This requires APS enabled. This is mandatory for 1:1.

APS: The Automatic Protection Switching protocol can be enabled/disabled. This is mandatory for 1:1.

Revertive: The revertive switching to working flow can be enabled/disabled.

WTR Time: The Wait To Restore timing value to be used in revertive switching. Range is 1 to 720 seconds.

Hold Off Time: The timing value to be used to make persistent check on Signal Fail before switching. This is in 100 ms. and the max value is 100 (10 sec).

Instance Command

Command:

None: There is no active local command on this instance.

Clear: The active local command will be cleared.

Lock Out: This EPS is locked to working (not active). In case of 1:N (more than one EPS with same protecting flow) - when one EPS switch to protecting flow, other EPS is enforced this command

Forced Switch: Forced switch to protecting.

Manual Switch P: Manual switch to protecting.

Manual Switch W: Manual switch to working. This is only allowed in case of 'non-revertive' mode

Exercise: Exercise of the protocol - not traffic effecting. This is only allowed in case of 'Bidirectional' protection type

Freeze: This EPS is locally frozen - ignoring all input.

Lock Out Local: This EPS is locally "locked out" - ignoring local SF detected on working.

Instance State

Protection State: EPS state according to State Transition Tables in G.8031.

W Flow: OK: State of working flow is ok

SF: State of working flow is Signal Fail

SD: State of working flow is Signal Degrade (for future use)

P Flow: OK: State of protecting flow is ok

SF: State of protecting flow is Signal Fail

SD: State of protecting flow is Signal Degrade (for future use)

Transmit APS r/b: The transmitted APS according to State Transition Tables in G.8031.

Receive APS r/b: The received APS according to State Transition Tables in G.8031.

Architecture Mismatch: The architecture indicated in the received APS does not match the locally configured.

APS on working: APS is received on the working flow.

Switching Incomplete: Traffic is not selected from the same flow instance in the two ends.

No APS Received: APS PDU is not received from the other end.

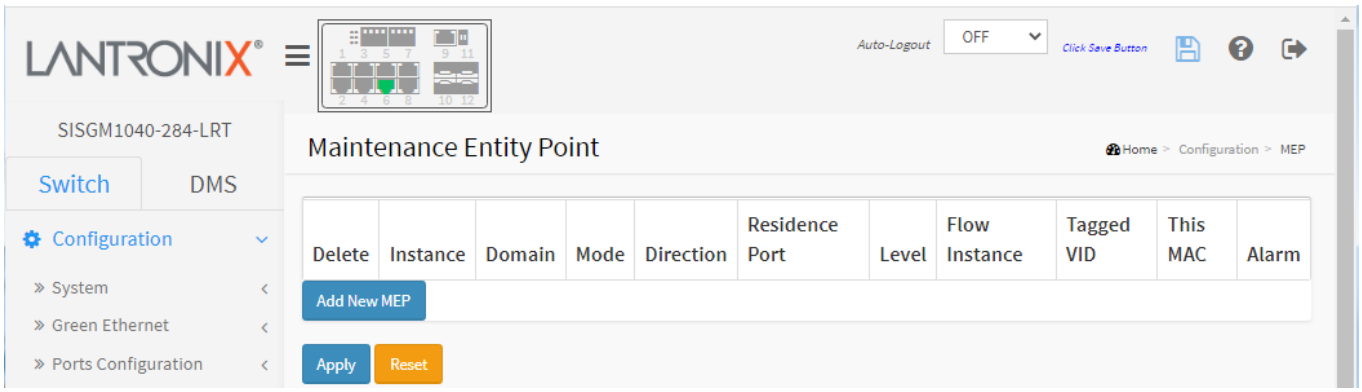
Buttons

Apply: Click to save changes.

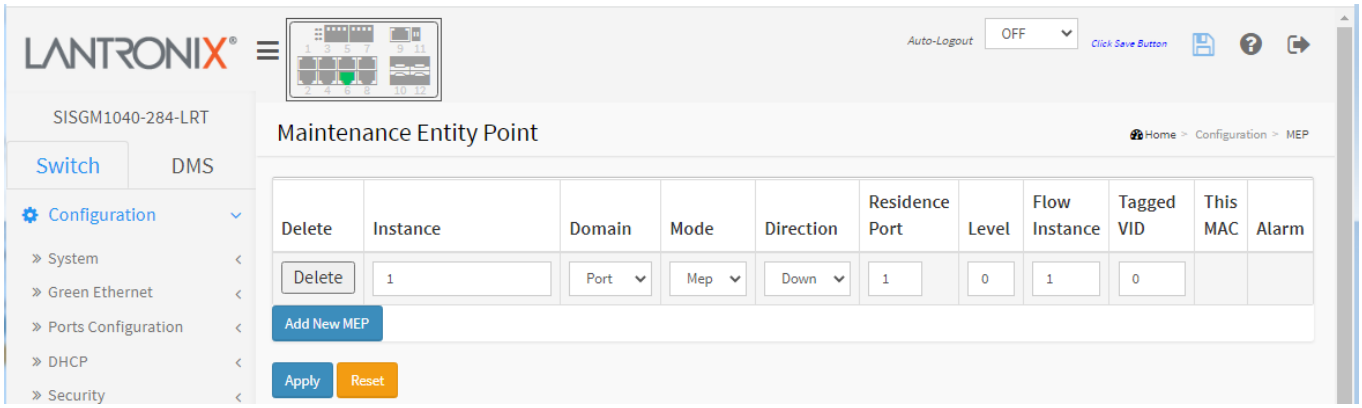
Reset: : Click to undo any changes made locally and revert to previously saved values.

Configuration > MEP

Maintenance Entity Point instances are configured here. A MEP (Maintenance Entity Endpoint) is an endpoint in a Maintenance Entity Group (ITU-T Y.1731). From the default page click the Add New MEP button to display the MEP config table:



↓↓↓↓



Parameter descriptions:

Delete: This box is used to mark a MEP for deletion in next Save operation.

Instance: The ID of the MEP. Click on the ID of a MEP to enter the configuration page. The range is 1 -100.

Domain: The domain of the MEP.

Port: This is a MEP in the Port Domain.

EVC: This is a MEP in the EVC Domain. 'Flow Instance' is an EVC. The EVC must be created

VLAN: This is a MEP in the VLAN Domain. 'Flow Instance' is a VLAN. For an Up-MEP, the VLAN must be created.

Mode: Select MEP or MIP:

MEP: This is a Maintenance Entity End Point.

MIP: This is a Maintenance Entity Intermediate Point.

Direction: The MEP direction (Up or Down):

Down: This is a Down MEP - monitoring ingress OAM and traffic on 'Residence Port'.

Up: This is a Up MEP - monitoring egress OAM and traffic on 'Residence Port'.

Residence Port: The port where MEP is monitoring - see 'Direction'. For an EVC MEP the port must be a port in the EVC. For a VLAN MEP the port must be a VLAN member.

Level: The MEG level of this MEP.

Flow Instance: The MEP is related to this flow - See 'Domain'. This is not relevant and not shown in case of Port MEP.

Tagged VID: Port MEP: An outer C-tag or S-tag (depending on VLAN Port Type) is added with this VID. Entering '0' means no TAG added.

EVC MEP: This is not used.

VLAN MEP: This is not used.

EVC MIP: On Serval, this is the Subscriber VID that identify the subscriber flow in this EVC where the MIP is active.

This MAC: The MAC of this MEP - can be used by other MEP when unicast is selected (Info only).

Alarm: There is an active alarm on the MEP.

Buttons

Add New MEP: Click to add a new MEP entry.

Apply: Click to save changes.

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

Messages:

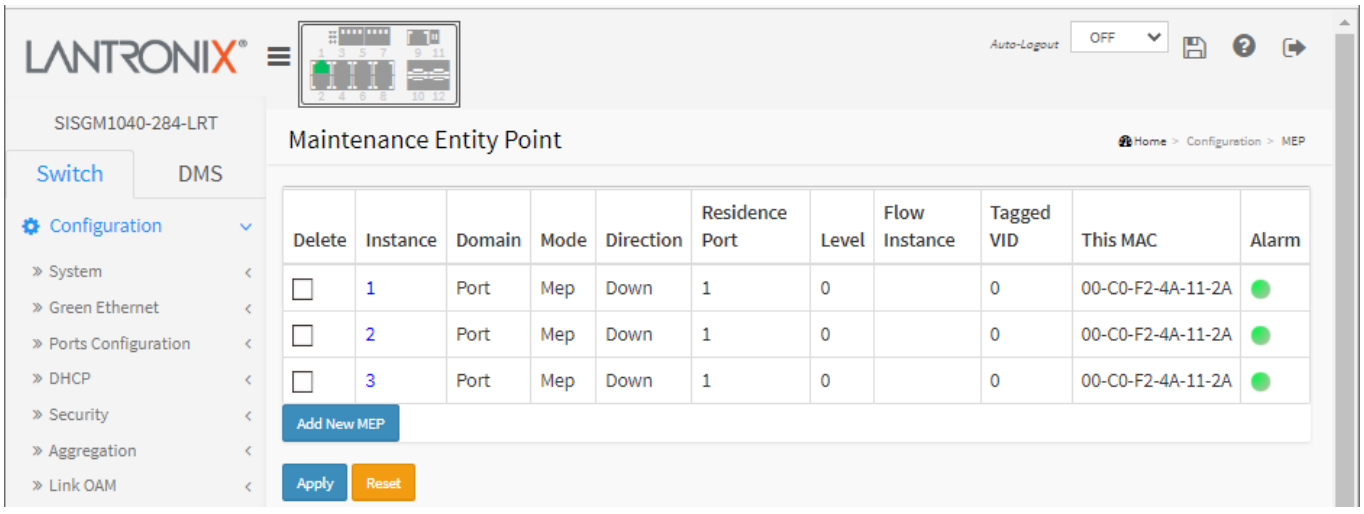
Warning! The configuration is invalid. EVC flow was found invalid

Warning! The configuration is invalid. VLAN domain is not supported

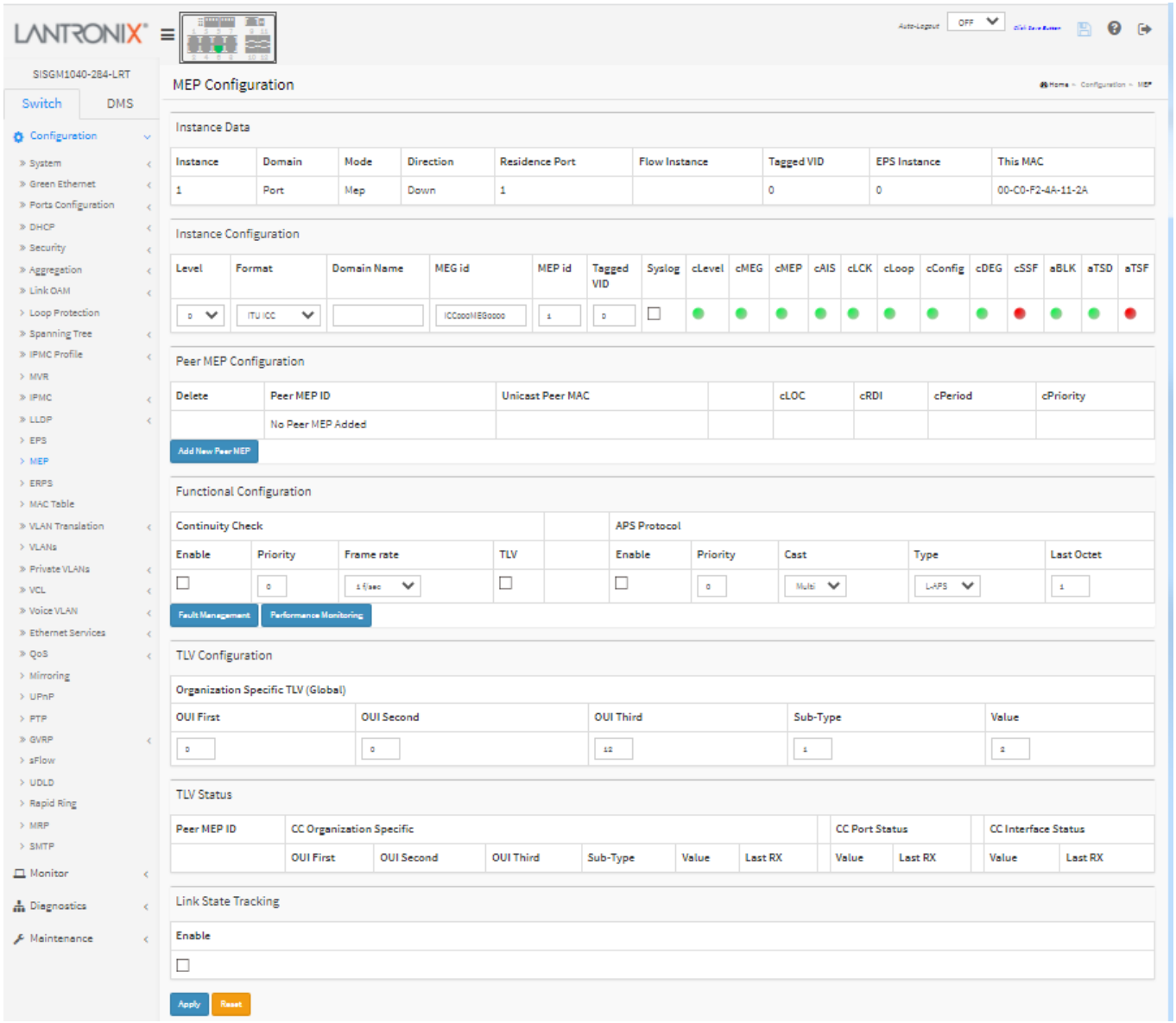
Warning! The configuration is invalid. VLAN is not created for this VID

Warning! The configuration is invalid. This MIP is not supported

Example:



Click a linked MEP Instance to display its MEP Configuration page. This page lets you view and configure the current MEP Instance.



Parameter descriptions:

Instance Data

MEP Instance: The ID of the MEP. Click on the ID of a MEP to enter the configuration page. The valid range is 1 - 100.

Domain: **Port**: This is a MEP in the Port Domain.

Mode: Select MEP or MIP:

Direction: The MEP direction (Up or Down):

Down: This is a Down MEP - monitoring ingress OAM and traffic on 'Residence Port'.

Up: This is a Up MEP - monitoring egress OAM and traffic on 'Residence Port'.

Residence Port: The port where MEP is monitoring - see 'Direction'. For a EVC MEP the port must be a port in the EVC. For a VLAN MEP the port must be a VLAN member.

Flow Instance: The MEP is related to this flow - See 'Domain'. This is not relevant and not shown in case of Port MEP.

Tagged VID: Port MEP: An outer C-tag or S-tag (depending on VLAN Port Type) is added with this VID. Entering '0' means no TAG added.

This MAC: The MAC of this MEP - can be used by other MEP when unicast is selected (Info only).

Instance Configuration

EVC QoS: This is only relevant for a EVC MEP. This is the Qos of the EVC and used for getting QoS counters for Loss Measurement.

Level: The MEG level of this MEP (0-7).

Format: This is the configuration of the two possible Maintenance Association Identifier formats.

ITU ICC: This is defined by ITU (Y1731 Fig. A3). 'Domain Name' is not used. 'MEG id' must be max. 13 char.

IEEE String: This is defined by IEEE (802.1ag Section 21.6.5). 'Domain Name' can be max. 16 char. 'MEG id' (Short MA Name) can be max. 16 char.

ITU CC ICC: This is defined by ITU (Y1731 Fig. A5). 'Domain Name' is not used. 'MEG id' must be max. 15 char.

Domain Name: This is the IEEE Maintenance Domain Name and is only used in case of 'IEEE String' format. This string can be empty giving Maintenance Domain Name Format 1 - Not present. This can be max 16 char.

MEG Id: This is either ITU MEG ID or IEEE Short MA Name - depending on 'Format'. See 'Format'. In case of ITU ICC format this must be 13 char. In case of ITU CC ICC format this must be 15 char. In case of IEEE String format this can be max 16 char.

MEP Id**:** This value will become the transmitted two byte CCM MEP ID.

Tagged VID: This value will be the VID of a TAG added to the OAM PDU.

VOE: This will attempt to utilize VOE HW for MEP implementation. Not all platforms support VOE.

cLevel: Fault Cause indicating that a CCM is received with a lower level than the configured for this MEP.

cMEG: Fault Cause indicating that a CCM is received with a MEG ID different from configured for this MEP.

cMEP: Fault Cause indicating that a CCM is received with a MEP ID different from all 'Peer MEP ID' configured for this MEP.

cAIS: Fault Cause indicating that AIS PDU is received.

cLCK: Fault Cause indicating that LCK PDU is received.

cDEG: Fault Cause indicating that server layer is indicating Signal Degraded.

cSSF: Fault Cause indicating that server layer is indicating Signal Fail.

aBLK: The consequent action of blocking service frames in this flow is active.

aTSD: The consequent action of indicating Trail Signal Degrade is calculated.

aTSF: The consequent action of indicating Trail Signal Fail to-wards protection is active.

Delete: This box is used to mark a Peer MEP for deletion in next Save operation.

Peer MEP ID: This value will become an expected MEP ID in a received CCM - see 'cMEP'.

Unicast Peer MAC: This MAC will be used when unicast is selected with this peer MEP. Also this MAC is used to create HW checking of receiving CCM PDU (LOC detection) from this MEP.

cLOC: Fault Cause indicating that no CCM has been received (in 3,5 periods) - from this peer MEP.

cRDI: Fault Cause indicating that a CCM is received with Remote Defect Indication - from this peer MEP.

cPeriod: Fault Cause indicating that a CCM is received with a period different what is configured for this MEP - from this peer MEP.

cPriority: Fault Cause indicating that a CCM is received with a priority different what is configured for this MEP - from this peer MEP.

Buttons

Add New Peer MEP: Click to add a new peer MEP.

Functional Configuration

Continuity Check: Enable. Continuity Check based on transmitting/receiving CCM PDU can be enabled/disabled. The CCM PDU is always transmitted as Multi-cast Class 1.

Priority: The priority to be inserted as PCP bits in TAG (if any). In case of enable of Continuity Check and Loss Measurement both implemented on SW based CCM, 'Priority' has to be the same.

Frame rate: Selecting the frame rate of CCM PDU. This is the inverse of transmission period as described in Y.1731. This value has these uses:

- The transmission rate of the CCM PDU.
- Fault Cause cLOC is declared if no CCM PDU has been received within 3.5 periods - see 'cLOC'.
- Fault Cause cPeriod is declared if a CCM PDU has been received with different period - see 'cPeriod'.

Selecting 300f/sec or 100f/sec will configure HW based CCM (if possible). Selecting other frame rates will configure SW based CCM. In case of enable of Continuity Check and Loss Measurement both implemented on SW based CCM, 'Frame Rate' has to be the same.

TLV: Enable/disable of TLV insertion in the CCM PDU.

APS Protocol Enable: Automatic Protection Switching protocol information transportation based on transmitting/receiving R-APS/L-APS PDU can be enabled/disabled. Must be enabled to support ERPS/ELPS implementing APS. This is only valid with one Peer MEP configured.

Priority: The priority to be inserted as PCP bits in TAG (if any).

Cast: Selection of APS PDU transmitted unicast or multi-cast. The unicast MAC will be taken from the 'Unicast **Peer** MAC' configuration. Unicast is only valid for L-APS - see 'Type'. The R-APS PDU is always transmitted with multi-cast MAC described in G.8032.

Type: Select R-APS or L-APS:

***R-APS**:* APS PDU is transmitted as R-APS - this is for ERPS.

L-APS: APS PDU is transmitted as L-APS - this is for ELPS.

Last Octet: This is the last octet of the transmitted and expected RAPS multi-cast MAC. In G.8031 (03/2010) a RAPS multi-cast MAC is defined as 01-19-A7-00-00-XX. In current standard the value for this last octet is '01' and the usage of other values is for further study.

TLV Configuration: Configuration of the OAM PDU TLV. Currently only TLV in the CCM is supported.

Organization Specific - OUI First: The transmitted first value in the OS TLV OUI field.

Organization Specific - OUI Second: The transmitted second value in the OS TLV OUI field.

Organization Specific - OUI Third: The transmitted third value in the OS TLV OUI field.

Organization Specific - Sub-Type: The transmitted value in the OS TLV Sub-Type field.

Organization Specific – Value: The transmitted value in the OS TLV Value field.

TLV Status: Display of the last received TLV. Currently only TLV in the CCM is supported.

CC Organization Specific - OUI First: The last received first value in the OUI field.

CC Organization Specific - OUI Second: The last received second value in the OS TLV OUI field.

CC Organization Specific - OUI Third: The last received third value in the OS TLV OUI field.

CC Organization Specific - Sub-Type: The last received value in the OS TLV Sub-Type field.

CC Organization Specific – Value: The last received value in the OS TLV Value field.

CC Organization Specific - Last RX: OS TLV was received in the last received CCM PDU.

CC Port Status – Value: The last received value in the PS TLV Value field.

CC Port Status - Last RX: PS TLV was received in the last received CCM PDU.

CC Interface Status – Value: The last received value in the IS TLV Value field.

CC Interface Status - Last RX: IS TLV was received in the last received CCM PDU.

Link State Tracking

Enable: When LST is enabled in an instance, Local SF or received 'isDown' in CCM Interface Status TLV, will bring down the residence port. Only valid in Up-MEP. The CCM rate must be 1 f/s or faster.

Buttons

Fault Management: Click to go to the Fault Management page.

Performance Monitor: Click to go to the Performance Monitor page.

Apply: Click to save changes.

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

Messages:

'Port 0' and 'Port 1' can not be same

'Port 0 APS MEP' and 'Port 1 APS MEP' can not be same

Port 0 SF MEP and Port 1 SF MEP can not be same

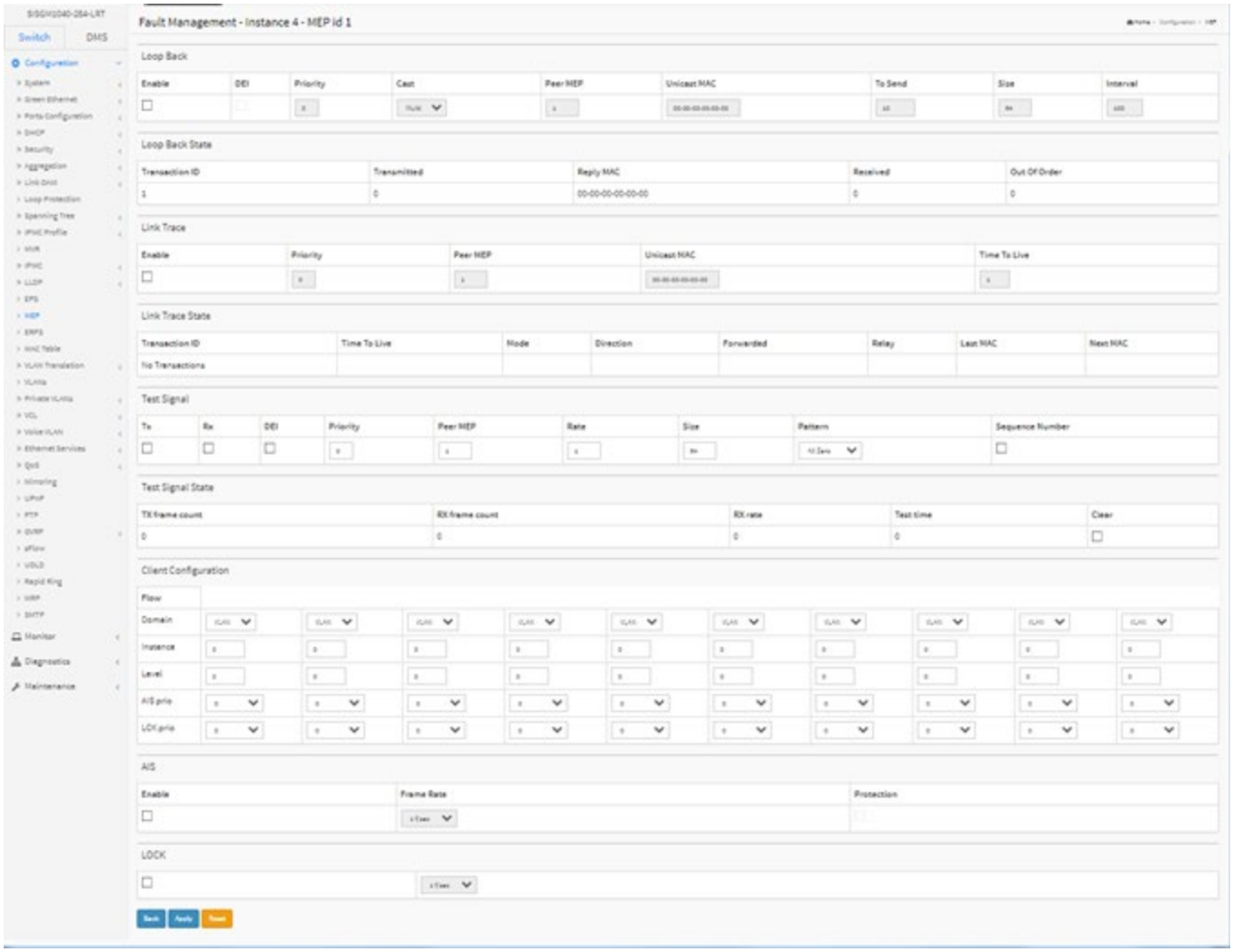
Invalid peer MEP ID

Invalid number of peer's for this configuration

Only one MEP can be added for each Apply operation

Fault Management page

This page lets you view and configure the Fault Management of the current MEP Instance.



Parameter descriptions:

Loop Back

Enable: Loop Back based on transmitting/receiving LBM/LBR PDU can be enabled/disabled. Loop Back is automatically disabled when all 'To Send' LBM PDU has been transmitted - waiting 5 sec. for all LBR from the end.

DEI: The DEI to be inserted as PCP bits in TAG (if any).

Priority: The priority to be inserted as PCP bits in TAG (if any).

Cast: Selection of LBM PDU transmitted unicast or multi-cast. The unicast MAC will be configured through 'Peer MEP' or 'Unicast Peer MAC'. To-wards MIP only unicast Loop Back is possible.

Peer MEP: This is only used if the 'Unicast MAC' is configured to all zero. The LBM unicast MAC will be taken from the 'Unicast Peer MAC' configuration of this peer.

Unicast MAC: This is only used if NOT configured to all zero. This will be used as the LBM PDU unicast MAC. This is the only way to configure Loop Back to-wards a MIP.

To Send: The number of LBM PDU to send in one loop test. The value 0 indicate infinite transmission (test behavior). This is HW based LBM/LBR and Requires VOE.

Size: The LBM frame size. This is entered as the wanted size (in bytes) of an un-tagged frame containing LBM OAM PDU - including CRC (four bytes).

Example when 'Size' = 64 => Un-tagged frame size = DMAC(6) + SMAC(6) + TYPE(2) + LBM PDU LENGTH(46) + CRC(4) = 64 bytes

The transmitted frame will be four bytes longer for each tag added - 8 bytes in case of a tunnel EVC.

There are two frame MAX sizes to consider.

Switch RX frame MAX size: The MAX frame size (all inclusive) accepted on the switch port of 9600 Bytes.

CPU RX frame MAX size: The MAX frame size (all inclusive) possible to copy to CPU of 1526 Bytes.

Consider that the Peer MEP must be able to handle the selected frame size. Consider that In case of SW based MEP, the received LBR PDU must be copied to CPU.

A Warning will be given if selected frame size exceeds the CPU RX frame MAX size Frame MIN Size is 64 Bytes.

Interval: The interval between transmitting LBM PDU. In 10ms. in case 'To Send' != 0 (max 100 - '0' is as fast as possible) In 1us. in case 'To Send' == 0 (max 10.000)",

Loop Back State:

Transaction ID: The transaction id of the first LBM transmitted. For each LBM transmitted the transaction id in the PDU is incremented.

Transmitted: The total number of LBM PDU transmitted.

Reply MAC: The MAC of the replying MEP/MIP. In case of multi-cast LBM, replies can be received from all peer MEP in the group. This MAC is not shown in case of 'To Send' == 0.

Received: The total number of LBR PDU received from this 'Reply MAC'.

Out Of Order: The number of LBR PDU received from this 'Reply MAC' with incorrect 'Transaction ID'.

Link Trace

Enable: Link Trace based on transmitting/receiving LTM/LTR PDU can be enabled/disabled. Link Trace is automatically disabled when all 5 transactions are done with 5 sec. interval - waiting 5 sec. for all LTR in the end. The LTM PDU is always transmitted as Multi-cast Class 2.

Priority: The priority to be inserted as PCP bits in TAG (if any).

Peer MEP: This is only used if the 'Unicast MAC' is configured to all zero. The Link Trace Target MAC will be taken from the 'Unicast Peer MAC' configuration of this peer.

Unicast MAC: This is only used if NOT configured to all zero. This will be used as the Link Trace Target MAC. This is the only way to configure a MIP as Target MAC.

Time To Live: This is the LTM PDU TTL value as described in Y.1731. This value is decremented each time forwarded by a MIP. Will not be forwarded reaching zero.

Link Trace State

Transaction ID: The transaction id is incremented for each LTM send. This value is inserted the transmitted LTM PDU and is expected to be received in the LTR PDU. Received LTR with wrong transaction id is ignored. There are five transactions in one Link Trace activated.

Time To Live: This is the TTL value taken from the LTM received by the MIP/MEP sending this LTR - decremented as if forwarded.

Mode: Indicating if is a MEP/MIP sending this LTR.

Direction: Indicating if MEP/MIP sending this LTR is ingress/egress.

Forwarded: Indicates if MEP/MIP sending this LTR has forwarded the LTM.

Relay: The Relay action can be one of the following

MAC: The was a hit on the LT Target MAC

FDB: LTM is forwarded based on hit in the Filtering DB

MFDB: LTM is forwarded based on hit in the MIP CCM DB

Last MAC: The MAC identifying the last sender of the LBM causing this LTR - initiating MEP or previous MIP forwarding.

Next MAC: The MAC identifying the next sender of the LBM causing this LTR - MIP forwarding or terminating MEP.

Test Signal

Enable: Test Signal based on transmitting TST PDU can be enabled/disabled.

DEI: The DEI to be inserted as PCP bits in TAG (if any).

Priority: The priority to be inserted as PCP bits in TAG (if any).

Peer MEP: The TST frame destination MAC will be taken from the 'Unicast Peer MAC' configuration of this peer.

Rate: The TST frame transmission bit rate - in Megabits per second. Limit is 400 Mbps. This is the bit rate of a standard frame without any encapsulation. If 1 Mbps rate is selected in a EVC MEP, the added tag will give a higher bitrate on the wire.

Size: The TST frame size. This is entered as the wanted size (in bytes) of a un-tagged frame containing TST OAM PDU - including CRC (four bytes).

Example when 'Size' = 64 => Un-tagged frame size = DMAC(6) + SMAC(6) + TYPE(2) + TST PDU LENGTH(46) + CRC(4) = 64 bytes

The transmitted frame will be four bytes longer for each tag added - 8 bytes in case of a tunnel EVC.

There are two frame MAX sizes to consider:

Switch RX frame MAX size: The MAX frame size (all inclusive) accepted on the switch port of 9600 Bytes.

CPU RX frame MAX size: The MAX frame size (all inclusive) possible to copy to CPU of 1526 Bytes.

Consider that the Peer MEP must be able to handle the selected frame size. Consider that in order to calculate the 'RX rate' a received TST PDU must be copied to CPU. A Warning will be given if selected frame size exceeds the CPU RX frame MAX size. Frame MIN Size is 64 Bytes.

Pattern: The 'empty' TST PDU has the size of 12 bytes. In order to achieve the configured frame size a data TLV will be added with a pattern. Example when 'Size' = 64 => Un-tagged frame size = DMAC(6) + SMAC(6) + TYPE(2) + TST PDU LENGTH(46) + CRC(4) = 64 bytes

The TST PDU must be 46 bytes so a pattern of 46-12=34 bytes will be added.

All Zero: Pattern will be '00000000'

All One: Pattern will be '11111111'

10101010: Pattern will be '10101010'

Test Signal State

TX frame count: The number of transmitted TST frames since last 'Clear'.

RX frame count: The number of received TST frames since last 'Clear'.

RX rate: The current received TST frame bit rate in Kbps. This is calculated on a 1 s. basis, starting when first TST frame is received after 'Clear'. The frame size used for this calculation is the first received after 'Clear'

Test time: The number of seconds passed since first TST frame received after last 'Clear'.

Clear: This will clear all Test Signal State. Transmission of TST frame will be restarted. Calculation of 'Rx frame count', 'RX rate' and 'Test time' will be started when receiving first TST frame.

Client Configuration: Only a Port MEP can be a server MEP with flow configuration. The Priority in the client flow is always the highest priority configured in the EVC.

Domain: The domain of the client layer flow.

Instance: Client layer flow instance numbers.

Level: Client layer level - AIS and LCK PDU transmitted in this client layer flow will be on this level.

AIS Prio: The priority to be used when transmitting AIS in each client flow. Priority resulting in highest possible PCP can be selected.

LCK Prio: The priority to be used when transmitting LCK in each client flow. Priority resulting in highest possible PCP can be selected.

AIS

Enable: Insertion of AIS signal (AIS PDU transmission) in client layer flows, can be enable/disabled.

Frame Rate: Selecting the frame rate of AIS PDU. This is the inverse of transmission period as described in Y.1731.

Protection: Selecting this means that the first 3 AIS PDU is transmitted as fast as possible - in case of using this for protection in the end point.

LOCK

Enable: Insertion of LOCK signal (LCK PDU transmission) in client layer flows, can be enable/disabled.

Frame Rate: Selecting the frame rate of LCK PDU. This is the inverse of transmission period as described in Y.1731.

Buttons

Back: Click to go back to this MEP instance main page.

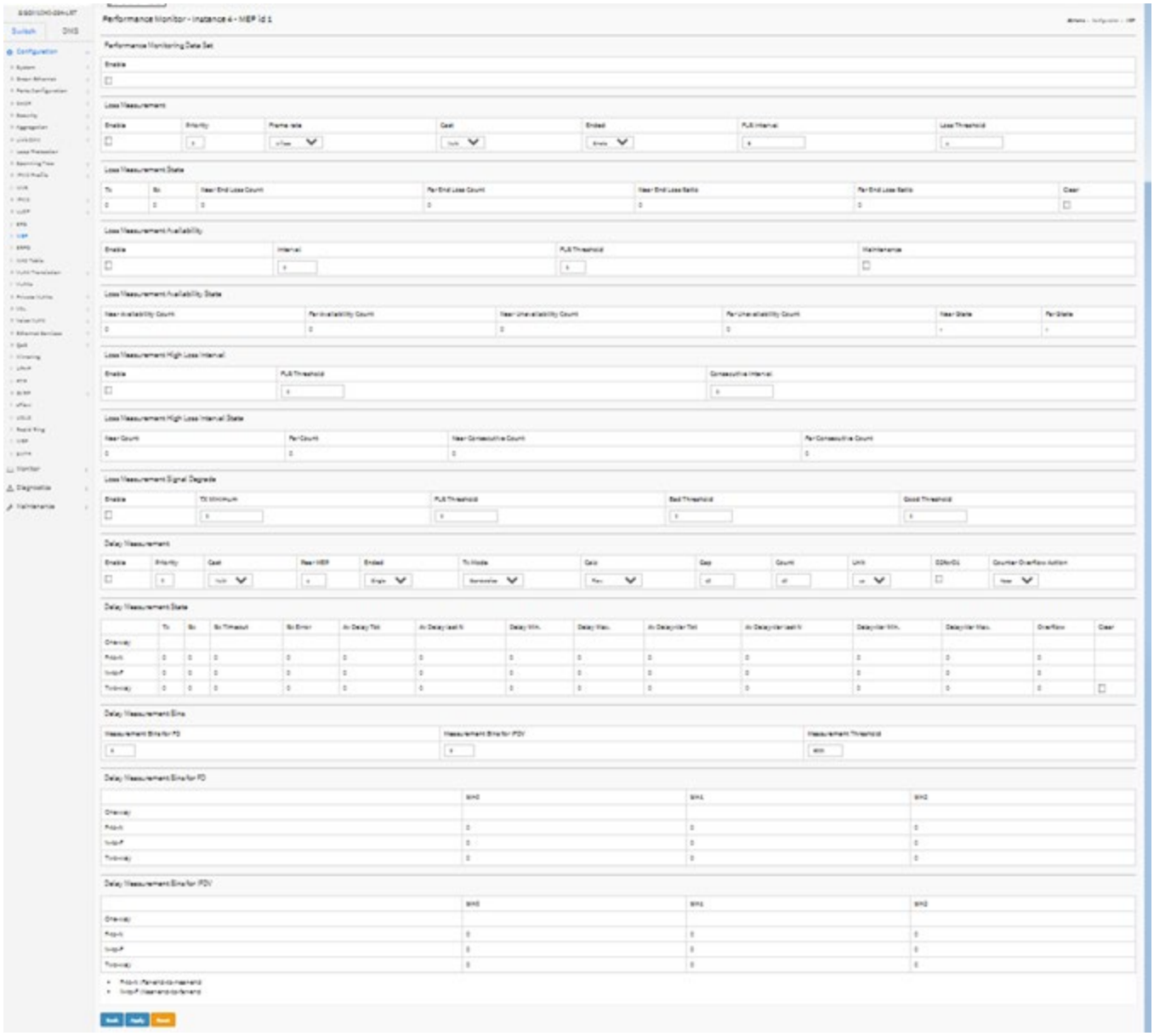
Apply: Click to save changes.

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

Message: Warning! The configuration is invalid. Some parameters are not allowed to change on an enabled instance.

Performance Monitor page

This page lets you view and configure the performance monitor of the current MEP Instance.



Parameter descriptions:

Performance Monitoring Data Set

Enable: When enabled this MEP instance will contribute to the 'PM Data Set' gathered by the PM Session.

Loss Measurement

Enable: Loss Measurement based on transmitting/receiving CCM or LMM/LMR PDU can be enabled/disabled - see 'Ended'. This is only valid with one Peer MEP configured.

Priority: The priority to be inserted as PCP bits in TAG (if any). In case of enable of Continuity Check and Loss Measurement both implemented on SW based CCM, 'Priority' has to be the same.

Frame rate: Selecting the frame rate of CCM/LMM PDU. This is the inverse of transmission period as described in Y.1731. Selecting 300f/sec or 100f/sec is not valid. In case of enable of Continuity Check and Loss Measurement both implemented on SW based CCM, 'Frame Rate' has to be the same.

Cast: Selection of CCM or LMM PDU transmitted unicast or multicast. The unicast MAC will be taken from the 'Unicast Peer MAC' configuration. In case of enable of Continuity Check and dual ended Loss Measurement both implemented on SW based CCM, 'Cast' has to be the same.

Ended: Single or Dual ended:

Single: Single ended Loss Measurement implemented on LMM/LMR.

Dual: Dual ended Loss Measurement implemented on SW based CCM.

FLR Interval: This is the interval in seconds where the Frame Loss Ratio is calculated.

Loss Threshold: Far end loss threshold count is incremented if a loss measurement is above this threshold.

Loss Measurement State

Near End Loss Count: The accumulated near end frame loss count - since last 'clear'.

Far End Loss Count: The accumulated far end frame loss count - since last 'clear'.

Near End Loss Ratio: The near end frame loss ratio calculated based on the near end frame loss count and far end frame transmitted - in the latest 'FLR Interval'. The result is given in percent.

Far End Loss Ratio: The far end frame loss ratio calculated based on the far end frame loss count and near end frame transmitted - in the latest 'FLR Interval'. The result is given in percent.

Clear: Set of this check and save will clear the accumulated counters and restart ratio calculation.

Loss Measurement Availability

Enable: Enable/disable of loss measurement availability.

Interval: Availability interval - number of measurements with same availability in order to change availability state.

FLR Threshold: Availability frame loss ratio threshold in per mille.

Maintenance: Enable/disable of loss measurement availability maintenance.

Loss Measurement Availability Status

Near Avail Count: Near end availability count.

Far Avail Count: Far end availability count.

Near Unavail Count: Near end unavailability count.

Far Unavail Count: Far end unavailability count.

Near State: Near end availability state.

Far State: Far end availability state.

Loss Measurement High Loss Interval

Enable: Enable/disable of loss measurement high loss interval.

FLR Threshold: High Loss Interval frame loss ratio threshold in per mille.

Consecutive Interval: High Loss Interval consecutive interval (number of measurements).

Loss Measurement High Loss Interval Status

Near Count: Near end high loss interval count (number of measurements where availability state is available and FLR is above high loss interval FLR threshold.

Far Count: Far end high loss interval count (number of measurements where availability state is available and FLR is above high loss interval FLR threshold.

Near Consecutive Count: Near end high loss interval consecutive count.

Far Consecutive Count: Far end high loss interval consecutive count.

Loss Measurement Signal Degrade

Enable: Enable/disable of loss measurement signal degrade.

TX Minimum: Minimum number of frames that must be transmitted in a measurement before frame loss ratio is tested against loss ratio threshold.

FLR Threshold: Signal Degraded frame loss ratio threshold in per mille.

Bad Threshold: Number of consecutive bad interval measurements required to set degrade state.

Good Threshold: Number of consecutive good interval measurements required to clear degrade state.

Delay Measurement

Enable: Delay Measurement based on transmitting 1DM/DMM PDU can be enabled/disabled. Delay Measurement based on receiving and handling 1DM/DMR PDU is always enabled.

Priority: The priority to be inserted as PCP bits in TAG (if any).

Cast: Selection of 1DM/DMM PDU transmitted unicast or multicast. The unicast MAC will be configured through 'Peer MEP'.

Peer MEP: This is only used if the 'Cast' is configured to Uni. The 1DM/DMR unicast MAC will be taken from the 'Unicast Peer MAC' configuration of this peer.

Way: Select One-Way or Two-Way:

One-Way: One-Way Delay Measurement implemented on 1DM.

Two-Way: Two-Way Delay Measurement implemented on DMM/DMR.

Tx Mode: Standardize: Y.1731 standardize way to transmit 1DM/DMR.

Proprietary: Vitesse proprietary way with follow-up packets to transmit 1DM/DMR.

Calc: This is only used if the 'Way' is configured to Two-way.

Round trip: The frame delay calculated by the transmitting and receiving timestamps of initiators. Frame Delay = RxTimeb-TxTimeStampf

Flow: The frame delay calculated by the transmitting and receiving timestamps of initiators and remotes. Frame Delay = (RxTimeb-TxTimeStampf)-(TxTimeStampb-RxTimeStampf)

Gap: The gap between transmitting 1DM/DMM PDU in 10ms. The range is 10 to 65535.

Count: The number of last records to calculate. The range is 10 to 2000.

Unit: The time resolution.

D2forD1: Enable to use DMM/DMR packet to calculate one-way DM. If the option is enabled, the following action will be taken. When DMR is received, two-way delay (roundtrip or flow) and both near-end-to-far-end and far-end-to-near-end one-way delay are calculated. When DMM or 1DM is received, only far-end-to-near-end one-way delay is calculated.

Counter Overflow Action: The action to counter when overflow happens.

Delay Measurement State

Tx: The accumulated transmit count - since last 'clear'.

Rx: The accumulated receive count - since last 'clear'.

Rx Timeout: The accumulated receive timeout count for two-way only - since last 'clear'.

Rx Error: The accumulated receive error count - since last 'clear'. This is counting if the frame delay is larger than 1 second or if far end residence time is larger than the round trip time.

Av Delay Tot: The average total delay - since last 'clear'.

Av Delay last N: The average delay of the last n packets - since last 'clear'.

Delay Min.: The minimum delay - since last 'clear'.

Delay Max.: The maximum delay - since last 'clear'.

Av Delay-Var Tot: The average total delay variation - since last 'clear'.

Av Delay-Var last N: The average delay variation of the last n packets - since last 'clear'.

Delay-Var Min.: The minimum delay variation - since last 'clear'.

Delay-Var Max.: The maximum delay variation - since last 'clear'.

Overflow: The number of counter overflow - since last 'clear'.

Clear: Set of this check and save will clear the accumulated counters.

Far-end-to-near-end one-way delay: The one-way delay is from remote devices to the local devices. Here are the conditions to calculate this delay. 1. 1DM received. 2. DMM received with D2forD1 enabled. 3. DMR received with D2forD1 enabled.

Near-end-to-far-end one-way delay: The one-way delay is from the local devices to remote devices. The only case to calculate this delay is below. DMR received with D2forD1 enabled.

Delay Measurement Bins: A Measurement Bin is a counter that stores the number of delay measurements falling within a specified range, during a Measurement Interval.

Measurement Bins for FD: Configurable number of Frame Delay Measurement Bins per Measurement Interval.

The minimum number of FD Measurement Bins per Measurement Interval supported is 2.

The maximum number of FD Measurement Bins per Measurement Interval supported is 10.

The default number of FD Measurement Bins per Measurement Interval supported is 3.

Measurement Bins for IFDV: Configurable number of Inter-Frame Delay Variation Measurement Bins per Measurement Interval.

The minimum number of FD Measurement Bins per Measurement Interval supported is 2.

The maximum number of FD Measurement Bins per Measurement Interval supported is 10.

The default number of FD Measurement Bins per Measurement Interval supported is 2.

Measurement Threshold: Configurable the Measurement Threshold for each Measurement Bin.

The unit for a measurement threshold is in microseconds (us).

The default configured measurement threshold for a Measurement Bin is an increment of 5000 us.

Delay Measurement Bins for FD: A Measurement Bin is a counter that stores the number of delay measurements falling within a specified range, during a Measurement Interval.

If the measurement threshold is 5000 us and the total number of Measurement Bins is four. For example:

Bin	Threshold	Range
bin0	0 us	0 us <= measurement < 5,000 us
bin1	5,000 us	5,000 us <= measurement < 10,000 us
bin2	10,000 us	10,000 us <= measurement < 15,000 us
bin3	15,000 us	15,000 us <= measurement < infinite us

Delay Measurement Bins for IFDV: A Measurement Bin is a counter that stores the number of delay measurements falling within a specified range, during a Measurement Interval. If the measurement threshold is 5000 us and the total number of Measurement Bins is four; For example:

Bin	Threshold	Range
bin0	0 us	0 us <= measurement < 5,000 us
bin1	5,000 us	5,000 us <= measurement < 10,000 us
bin2	10,000 us	10,000 us <= measurement < 15,000 us
bin3	15,000 us	15,000 us <= measurement < infinite us

Buttons

Back: Click to go back to this MEP instance main page.

Apply: Click to save changes.

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

Messages:

Invalid number of peer's for this configuration

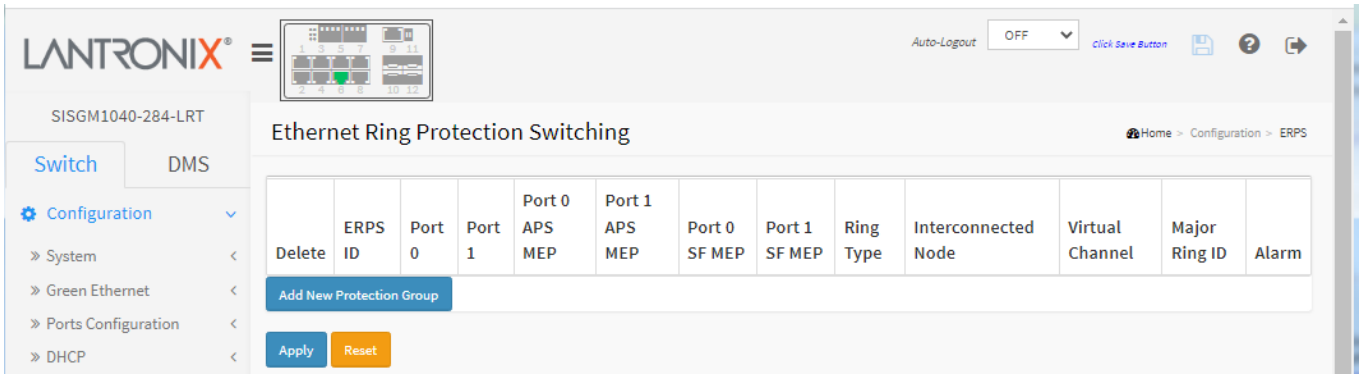
Warning! The configuration is invalid. Invalid peer MEP ID

For a non-MPLS MEP, the client flow domain can not be mixed VLAN and EVC.

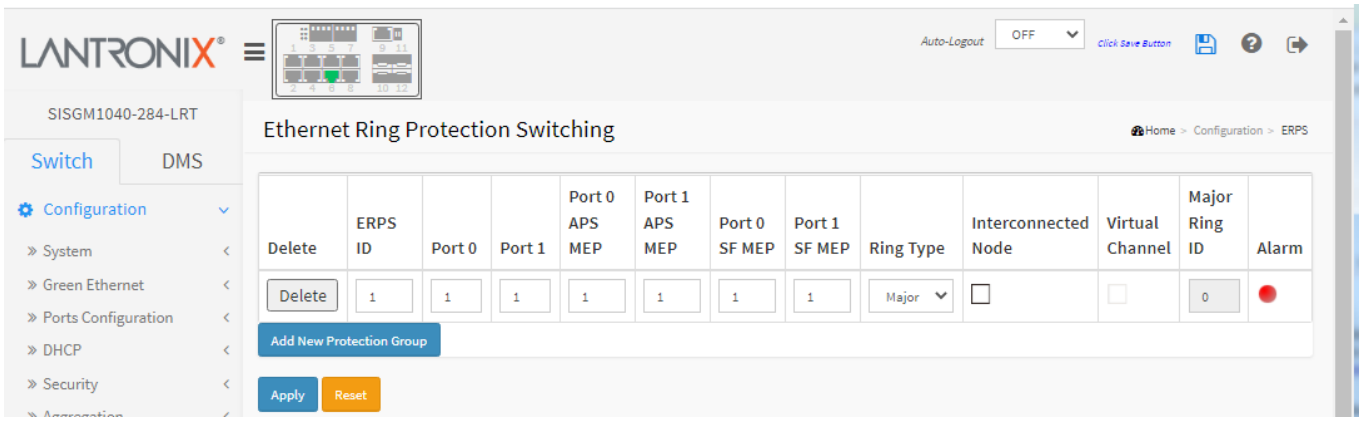
Configuration > ERPS

ERPS instances are configured here. ERPS (Ethernet Ring Protection Switching) is defined in ITU/T G.8032. ERPS provides fast protection and recovery switching for Ethernet traffic in a ring topology while also ensuring that the Ethernet layer remains loop-free. See “Appendix C – MRP Operation and Examples” on page 424 for more information.

Navigate to the Switch > Configuration ERPS menu path to display the default Ethernet Ring Protection Switching page:



Click the Add New Protection Group button to add a new Protection group entry to the table:



Parameter descriptions:

Delete: This box is used to mark an ERPS for deletion in next Save operation.

ERPS ID: The ID of the created Protection group, It must be an integer value of 1 - 64. The maximum number of ERPS Protection Groups that can be created are 64. Click on the ID of a Protection group to enter the configuration page (see below).

Port 0: This will create a Port 0 of the switch in the ring.

Port 1: This will create "Port 1" of the switch in the Ring. As interconnected sub-ring will have only one ring port, "Port 1" is configured as "0" for interconnected sub-ring. "0" in this field indicates that no "Port 1" is associated with this instance

Port 0 SF MEP: The Port 0 Signal Fail reporting MEP.

Port 1 SF MEP: The Port 1 Signal Fail reporting MEP. As only one SF MEP is associated with interconnected sub-ring without virtual channel, it is configured as "0" for such ring instances. "0" in this field indicates that no Port 1 SF MEP is associated with this instance.

Port 0 APS MEP: The Port 0 APS PDU handling MEP.

Port 1 APS MEP: The Port 1 APS PDU handling MEP. As only one APS MEP is associated with interconnected sub-ring without virtual channel, it is configured as "0" for such ring instances. "0" in this field indicates that no Port 1 APS MEP is associated with this instance.

Ring Type: Type of Protecting ring. It can be either major ring or sub-ring.

Interconnected Node: Interconnected Node indicates that the ring instance is interconnected. Click on the checkbox to configure this. "Yes" indicates it is an interconnected node for this instance. "No" indicates that the configured instance is not interconnected.

Virtual Channel: Sub-rings can either have virtual channel or not on the interconnected node. This is configured using "Virtual Channel" checkbox. "Yes" indicates it is a sub-ring with virtual channel. "No" indicates, sub-ring doesn't have virtual channel.

Major Ring ID: Major ring group ID for the interconnected sub-ring. It is used to send topology change updates on major ring. If ring is major, this value is same as the protection group ID of this ring.

Alarm: Indicates there is an active alarm on the ERPS.

Buttons

Add New Protection Group: Click to add a new Protection group entry.

Apply: Click to save changes.

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

Messages:

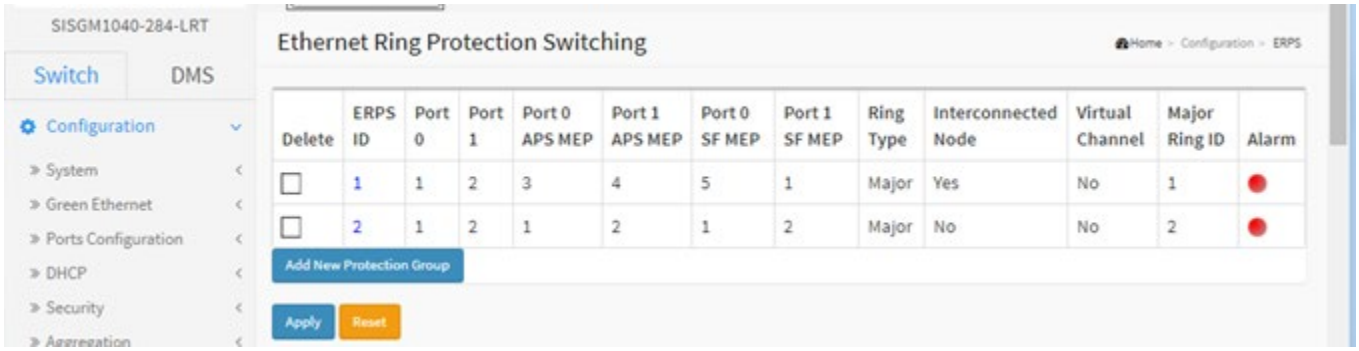
Only one ERPS can be added for each Apply operation

'Port 0' and 'Port 1' can not be same

'Port 0 APS MEP' and 'Port 1 APS MEP' can not be same

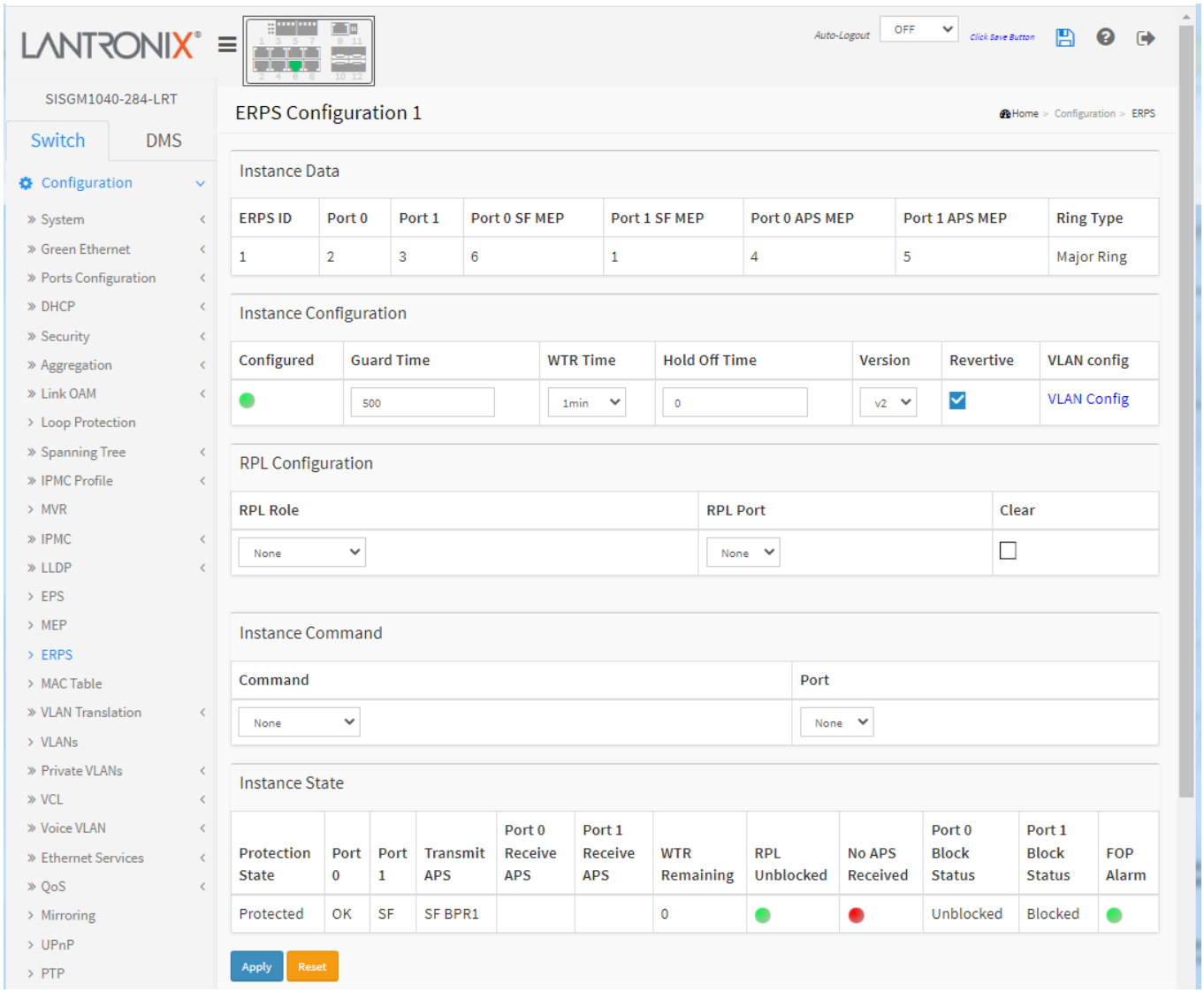
Port 0 SF MEP and Port 1 SF MEP can not be same

Example:



ERPS Configuration

Click a linked ERPS ID to display its Configuration page. This page lets you view and configure an ERPS Instance.



Parameter descriptions:

Instance Data

ERPS ID: The ID of the Protection group.

Port 0: This will create a Port 0 of the switch in the ring.

Port 1: This will create "Port 1" of the switch in the Ring. As interconnected sub-ring will have only one ring port, "Port 1" is configured as "0" for interconnected sub-ring. "0" in this field indicates that no "Port 1" is associated with this instance

Port 0 SF MEP: The Port 0 Signal Fail reporting MEP.

Port 1 SF MEP: The Port 1 Signal Fail reporting MEP. As only one SF MEP is associated with interconnected sub-ring without virtual channel, it is configured as "0" for such ring instances. "0" in this field indicates that no Port 1 SF MEP is associated with this instance.

Port 0 APS MEP: The Port 0 APS PDU handling MEP.

Port 1 APS MEP: The Port 1 APS PDU handling MEP. As only one APS MEP is associated with interconnected sub-ring without virtual channel, it is configured as "0" for such ring instances. "0" in this field indicates that no Port 1 APS MEP is associated with this instance.

Ring Type: Type of Protecting ring. It can be either major ring or sub-ring.

Instance Configuration

Configured:

Red: This ERPS is only created and has not yet been configured - is not active.

Green: This ERPS is configured - is active.

Guard Time: Guard timeout value to be used to prevent ring nodes from receiving outdated R-APS messages. The period of the guard timer can be configured in 10 ms steps between 10 ms and 2 seconds, with a default value of 500 ms

WTR Time: The Wait To Restore timing value to be used in revertive switching. The period of the WTR time can be configured by the operator in 1 minute steps between 5 and 12 minutes with a default value of 5 minutes.

Hold Off Time: The timing value to be used to make persistent check on Signal Fail before switching. The range of the hold off timer is 0 to 10 seconds in steps of 100 ms

Version: ERPS Protocol Version - v1 or v2

Revertive: In Revertive mode, after the conditions causing a protection switch has cleared, the traffic channel is restored to the working transport entity, i.e., blocked on the RPL.

In Non-Revertive mode, the traffic channel continues to use the RPL, if it is not failed, after a protection switch condition has cleared.

VLAN config: VLAN configuration of the Protection Group. Click on the "VLAN Config" link to configure VLANs for this protection group.

RPL Configuration

RPL Role: It can be either RPL owner or RPL Neighbor.

RPL Port: This allows to select the east port or west port as the RPL block.

Clear: If the owner has to be changed, then the clear check box allows to clear the RPL owner for that ERPS ring.

Sub-Ring Configuration

Topology Change: Clicking this checkbox indicates that the topology changes in the sub-ring are propagated in the major ring.

Instance Command

Command: Administrative command. A port can be administratively configured to be in either manual switch or forced switch state.

Forced Switch: Forced Switch command forces a block on the ring port where the command is issued.

Manual Switch: In the absence of a failure or FS, Manual Switch command forces a block on the ring port where the command is issued.

Clear: The Clear command is used for clearing an active local administrative command (e.g., Forced Switch or Manual Switch).

Port: Port selection - Port0 or Port1 of the protection Group on which the command is applied.

Instance State

Protection State: ERPS state according to State Transition Tables in G.8032.

Port 0: OK or SF:

OK: State of East port is ok

SF: State of East port is Signal Fail

Port 1: OK or SF:

OK: State of West port is ok

SF: State of West port is Signal Fail

Transmit APS: The transmitted APS according to State Transition Tables in G.8032.

Port 0 Receive APS: The received APS on Port 0 according to State Transition Tables in G.8032.

Port 1 Receive APS: The received APS on Port 1 according to State Transition Tables in G.8032.

WTR Remaining: Remaining WTR timeout in milliseconds.

RPL Un-blocked: APS is received on the working flow.

No APS Received: RAPS PDU is not received from the other end.

Port 0 Block Status: Block status for Port 0 (Both traffic and R-APS block status). R-APS channel is never blocked on sub-rings without virtual channel.

Port 1 Block Status: Block status for Port 1 (Both traffic and R-APS block status). R-APS channel is never blocked on sub-rings without virtual channel.

FOP Alarm: Failure of Protocol Defect (FOP) status. If FOP is detected, red LED glows; else green LED glows.

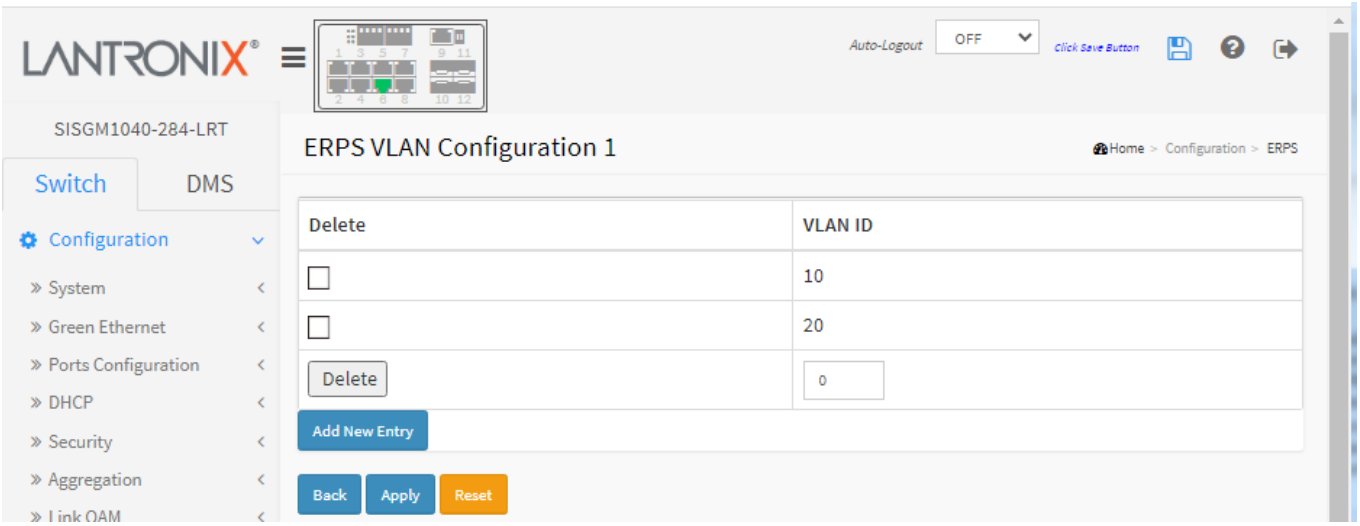
Buttons

Apply: Click to apply changes immediately.

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

ERPS VLAN Configuration

1. At the ERPS Configuration page click the linked text "VLAN Config" to display the ERPS VLAN Configuration page.
2. Click the Add New Entry button to display the ERPS VLAN Config table:



3. Enter a VLAN ID.
4. Click the Apply button.
5. Click the Back button to return to the ERPS Configuration page.

Parameter descriptions:

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

VLAN ID: Indicates the ID of this particular VLAN.

Buttons

Add New Entry: Click the Add New Entry button to add a new VLAN ID. Legal values for VLAN ID are 1-4095. The maximum number of VLANs is 63.

The VLAN is enabled when you click on "Apply" to save. A VLAN without any port members will be deleted when you click "Apply". The Reset button can be used to undo the addition of new VLANs.

Apply: Click to save changes.

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

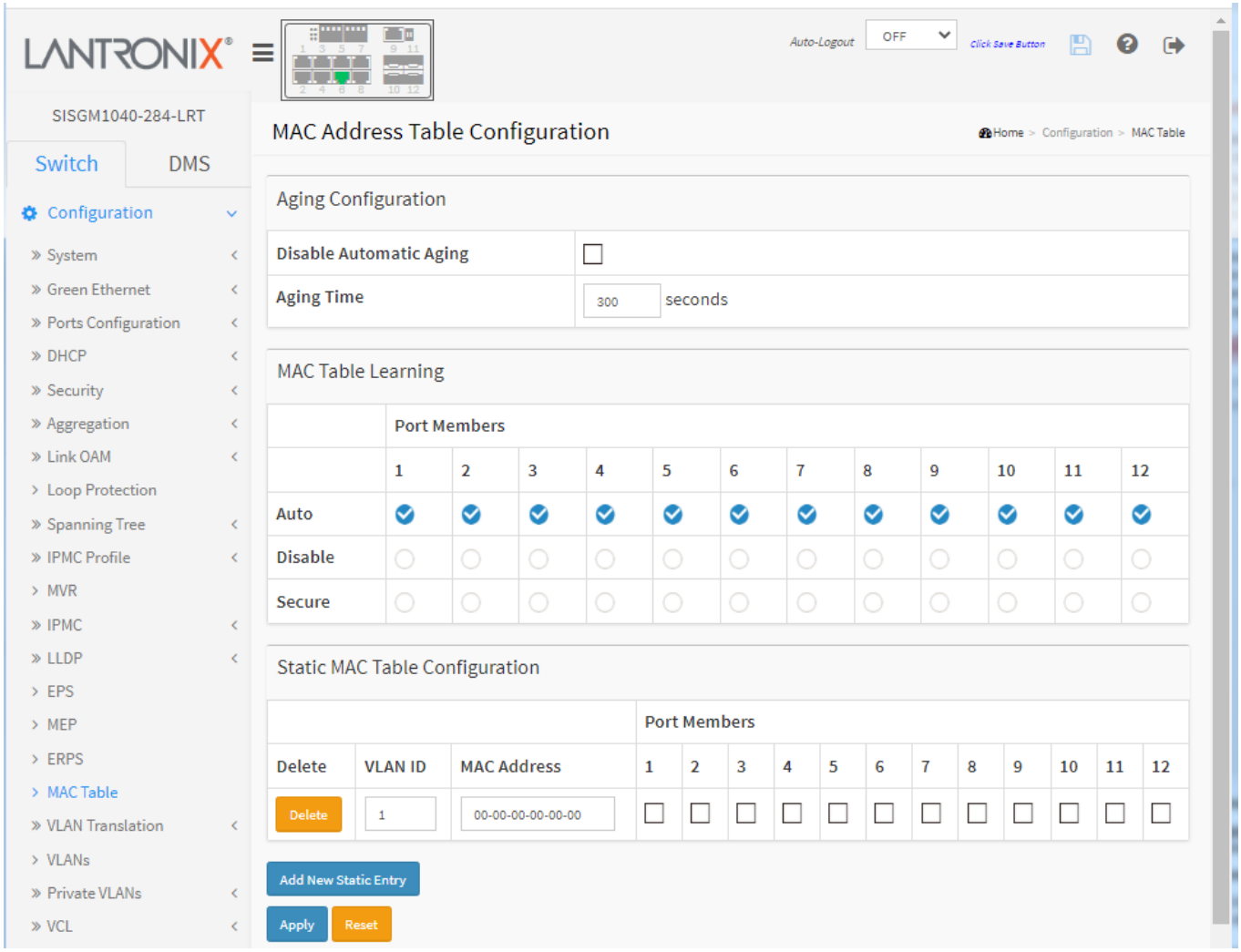
Back: Click to go back to this MEP instance main page.

Configuration > MAC Table

The MAC Address Table is configured on this page. Set timeouts for entries in the dynamic MAC Table and configure the static MAC table here.

Switching of frames is based on the DMAC address contained in the frame. The switch builds up a table that maps MAC addresses to switch ports for knowing which ports the frames should go to (based on the DMAC address in the frame). This table contains both static and dynamic entries. The static entries are configured by the network administrator if the administrator wants to do a fixed mapping between the DMAC address and switch ports.

The frames also contain a MAC address (SMAC address) which shows the MAC address of the equipment sending the frame. The SMAC address is used by the switch to automatically update the MAC table with these dynamic MAC addresses. Dynamic entries are removed from the MAC table if no frame with the corresponding SMAC address have been seen after a configurable age time.



Parameter descriptions:

Aging Configuration: By default, dynamic entries are removed from the MAC table after 300 seconds. This removal is called ‘aging’.

Disable Automatic Aging: Check the box to disable the automatic aging of dynamic entries.

Aging Time: Configure aging time by entering a value here in seconds. The allowed range is 10 - 1000000 seconds. The default is 300 seconds.

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

Apply: Click to save changes.

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

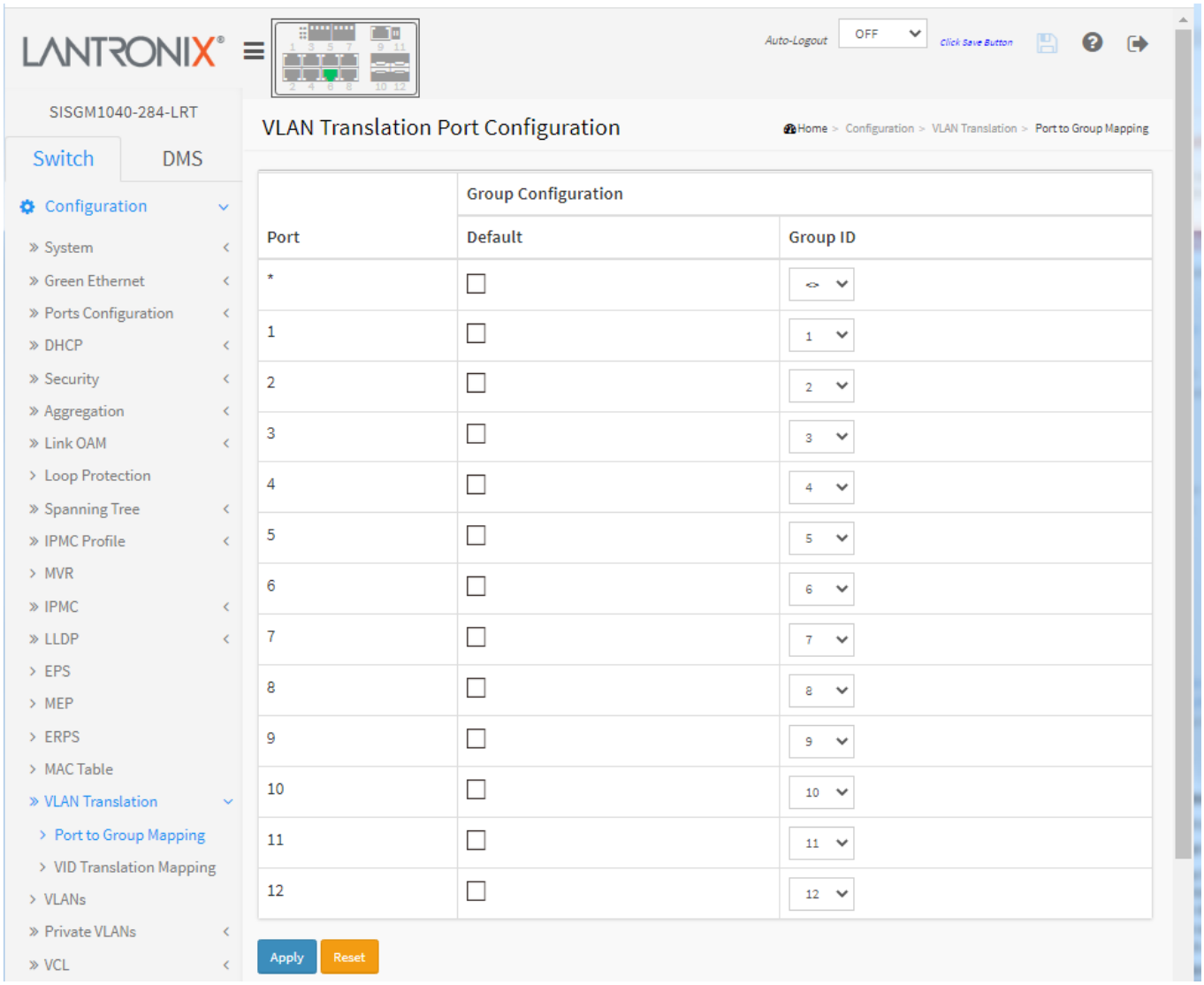
Messages:

Error: mac address:00-00-00-00-00-00 is not multicast mac address, support only one port.

No port members selected for VLAN ID: 1000 and MAC address: 00-00-00-00-00-00. This will block the MAC address for all ports. Is this correct?

Configuration > VLAN Translation > Port to Group Mapping

This page lets you configure switch Ports to use a given VLAN Translation Mapping Group. This will enable all VLAN Translation mappings of that group (if any) on the selected switch port.



Parameter descriptions:

Port: The Port column shows the list of ports for which you can configure the VLAN Translation Mapping Groups.

Default: To set the switch port to use the default VLAN Translation Group click the checkbox.

Group ID: The VLAN Translation mappings are organized into Groups, identified by the Group ID. This way a port is configured to use several VLAN Translation mappings easily by simply configuring it to use a given group. Then number of possible groups in a switch is equal to the number of ports present in this switch. A port can be configured to use any of the groups, but only one at any given time. Multiple ports can be configured to use the same group. A valid Group ID is an integer value of 1 - 12.

Note: By default, each port is set to use the group with Group ID equal to the port number. For example, port #1 is by default set to use group with GID = 1.

Buttons

Apply: Click to save changes.

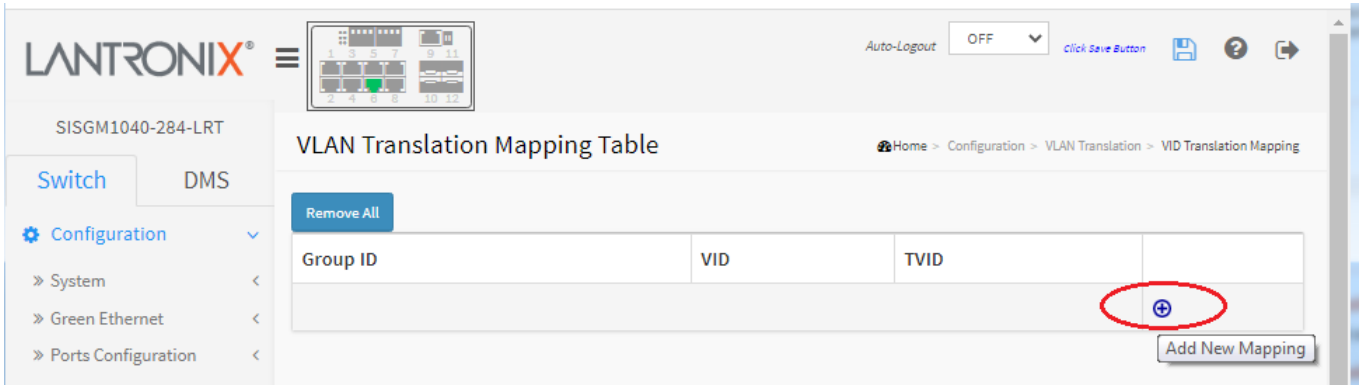
Reset: Click to undo any changes made locally and revert to previously saved values.

Configuration > VLAN Translation > VID Translation Mapping

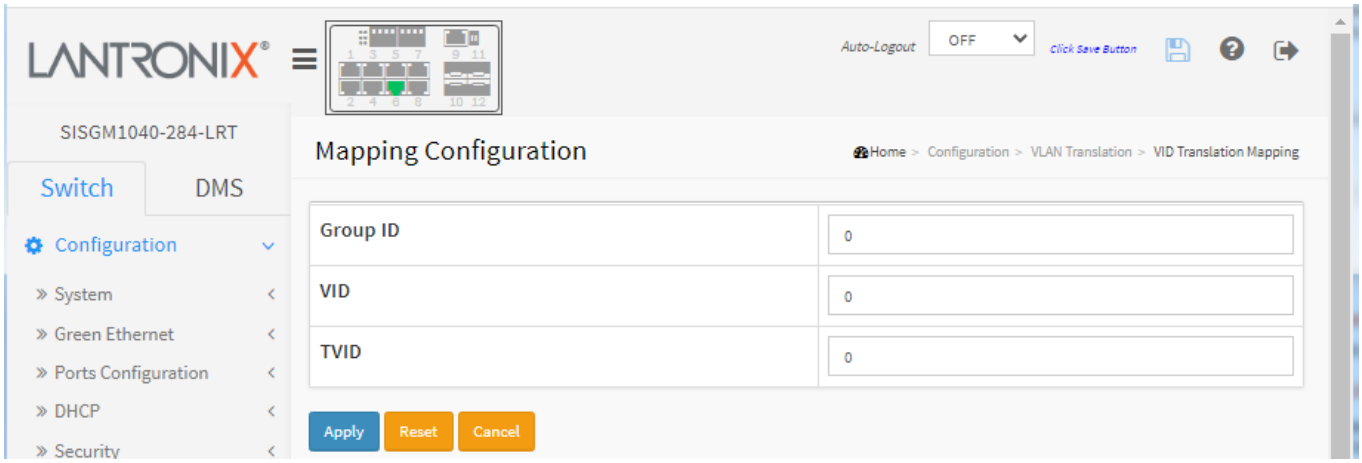
This page lets you set VLAN Translation mapping parameters.

VLAN Translation Mapping Table

After you click the Apply button the VLAN Translation Mapping Table displays. This page lets you create mappings of VLANs > Translated VLANs and organize these mappings into global Groups. Here you can Add, Edit or delete table entries. From the default page click the Add New Mapping (⊕) icon to display the "Mapping Configuration" page.



↓↓↓↓



Parameter descriptions:

Group ID: The VLAN Translation mappings are organized into Groups, identified by the Group ID. This way a port is configured to use several VLAN Translation mappings easily by simply configuring it to use a given group. The number of possible groups in a switch is equal to the number of ports present in this switch. A port can be configured to use any of the groups, but only one at any given time. Multiple ports can be configured to use the same group. A valid Group ID is an integer value from 1 to 12.

Note: By default, each port is set to use the group with Group ID equal to the port number. For example, port #1 is by default set to use group with GID = 1.

VID: Indicates the VLAN of the mapping (i.e., 'source' VLAN). A valid VLAN ID ranges from 1 to 4095.

TVID: Indicates the VLAN ID to which VLAN ID of an ingress frame will be translated to (granted that the mapping is enabled on the ingress port that the frame arrived at). A valid VLAN ID ranges from 1 to 4095.

Modification Buttons

You can modify each VLAN Translation mapping in the table using these buttons:

: Edits the mapping row.

: Deletes the mapping.

: Adds a new mapping.

Buttons

Apply: Click to save changes.

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

Cancel: Return to the previous page; any changes made locally will be undone.

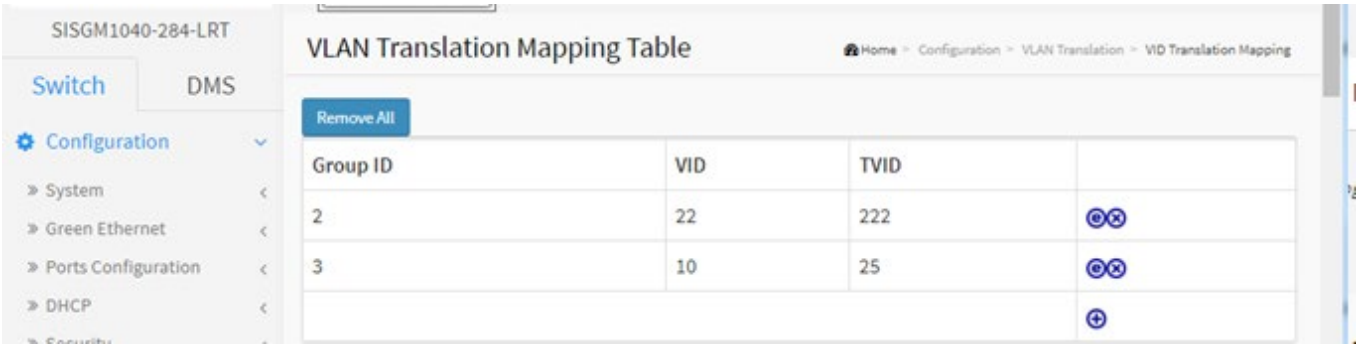
Remove All: Click to remove all VLAN Translation mappings.

Messages:

'Group ID' must be an integer value between 1 and 12

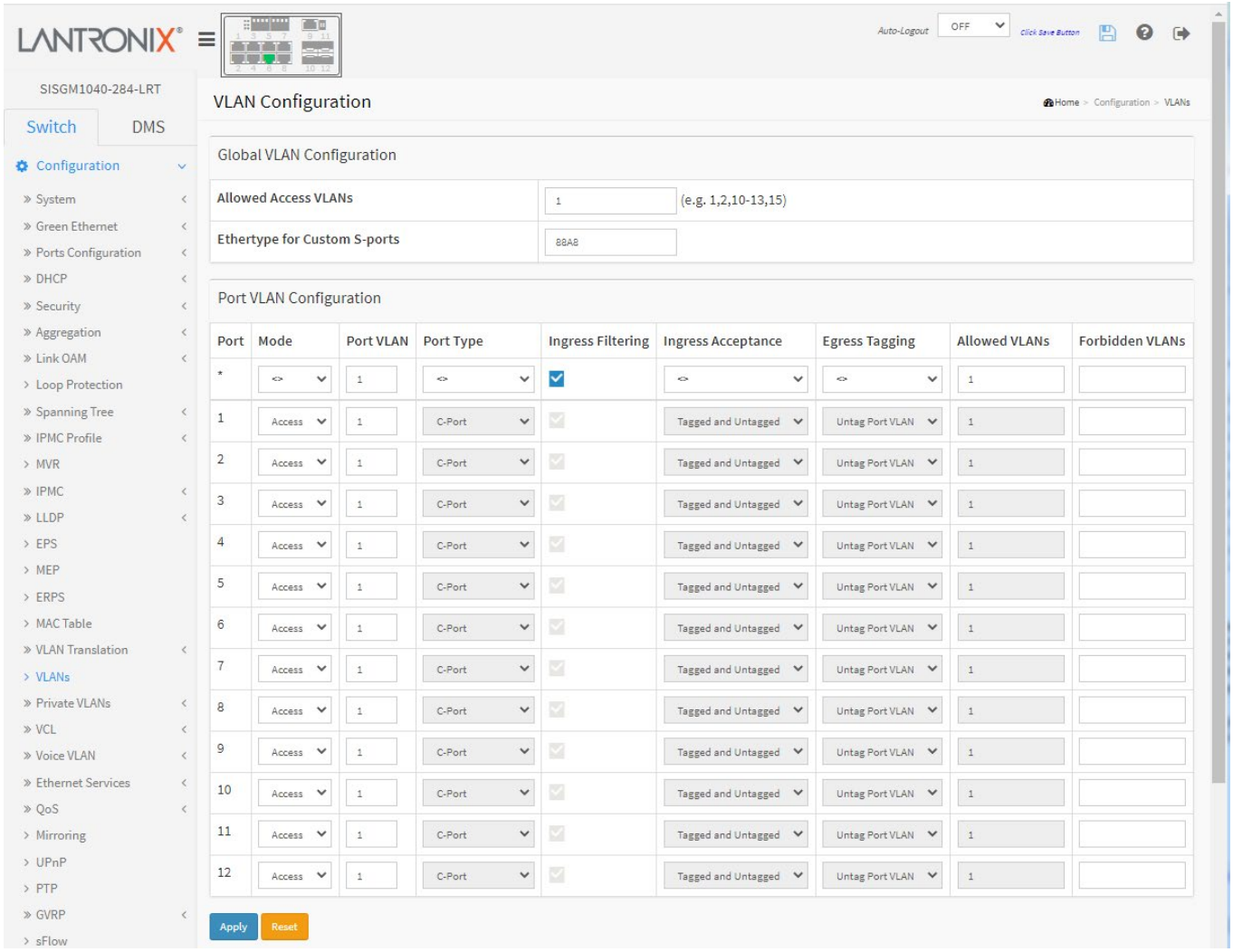
VLAN ID and Translated VLAN ID cannot be same.

Example:



Configuration > VLANs

This page allows for controlling VLAN configuration on the switch. The page is divided into a global section and a per-port configuration section.



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 is enabled. More VLANs may be created by using a list syntax where the individual elements are separated by commas. Ranges are specified with a dash separating the lower and upper bound.

The following example will create VLANs 1, 10, 11, 12, 13, 200, and 300: 1,10-13,200,300. Spaces are allowed in between the delimiters.

Ethertype for Custom S-ports: This field specifies the ethertype/TPID (specified in hexadecimal) used for Custom S-ports. The setting is in force for all ports whose Port Type is set to S-Custom-Port.

Port VLAN Configuration

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

Mode: The port mode (default is Access) determines the fundamental behavior of the port in question. A port can be in one of three modes as described below.

Whenever a particular mode is selected, the remaining fields in that row will be either grayed out or made changeable depending on the mode in question.

Grayed out fields show the value that the port will get when the mode is applied.

Access: Access ports are normally used to connect to end stations. Dynamic features like Voice VLAN may add the port to more VLANs behind the scenes. Access ports have the following characteristics:

Member of exactly one VLAN, the Port VLAN (a.k.a. Access VLAN), which by default is 1.

Accepts untagged 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 VLANs (1-4095)

The VLANs that a trunk port is member of may be limited by the use of Allowed VLANs

Frames classified to a VLAN that the port is not a member of are 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.

Hybrid: Hybrid ports resemble trunk ports in many ways but adds additional port configuration features. In addition to the characteristics described for trunk ports, hybrid ports have these abilities:

Can be configured to be VLAN tag unaware, C-tag aware, S-tag aware, or S-custom-tag aware

Ingress filtering can be controlled

Ingress acceptance of frames and configuration of egress tagging can be configured independently.

Port VLAN: Determines the port's VLAN ID (a.k.a. PVID). Allowed VLANs are in the range 1 - 4095, default being 1.

On ingress, frames get classified to the Port VLAN if the port is configured as VLAN unaware, the frame is untagged, or VLAN awareness is enabled on the port, but the frame is priority tagged (VLAN ID = 0).

On egress, frames classified to the Port VLAN do not get tagged if Egress Tagging configuration is set to untag Port VLAN.

The Port VLAN is called an "Access VLAN" for ports in Access mode and Native VLAN for ports in Trunk or Hybrid mode.

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

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

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

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

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

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

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

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

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

Tagged and Untagged: Both tagged and untagged frames are accepted.

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

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

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

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

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

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

Allowed VLANs: Ports in Trunk and Hybrid mode may control which VLANs they can 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 Enabled VLANs field. By default, a Trunk or Hybrid port will become member of all VLANs and is therefore set to 1-4095.

The field may be left empty, which means that the port will not become member of any VLANs.

Forbidden VLANs: A port may be configured to never be member of one or more VLANs. This is particularly useful when dynamic VLAN protocols like MVRP and GVRP must be prevented from dynamically adding ports to VLANs.

The trick is to mark such VLANs as forbidden on the port in question. The syntax is identical to the syntax used in the Enabled VLANs field.

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

Buttons

Apply: Click to apply changes immediately.

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

Configuration > Private VLANs > Membership

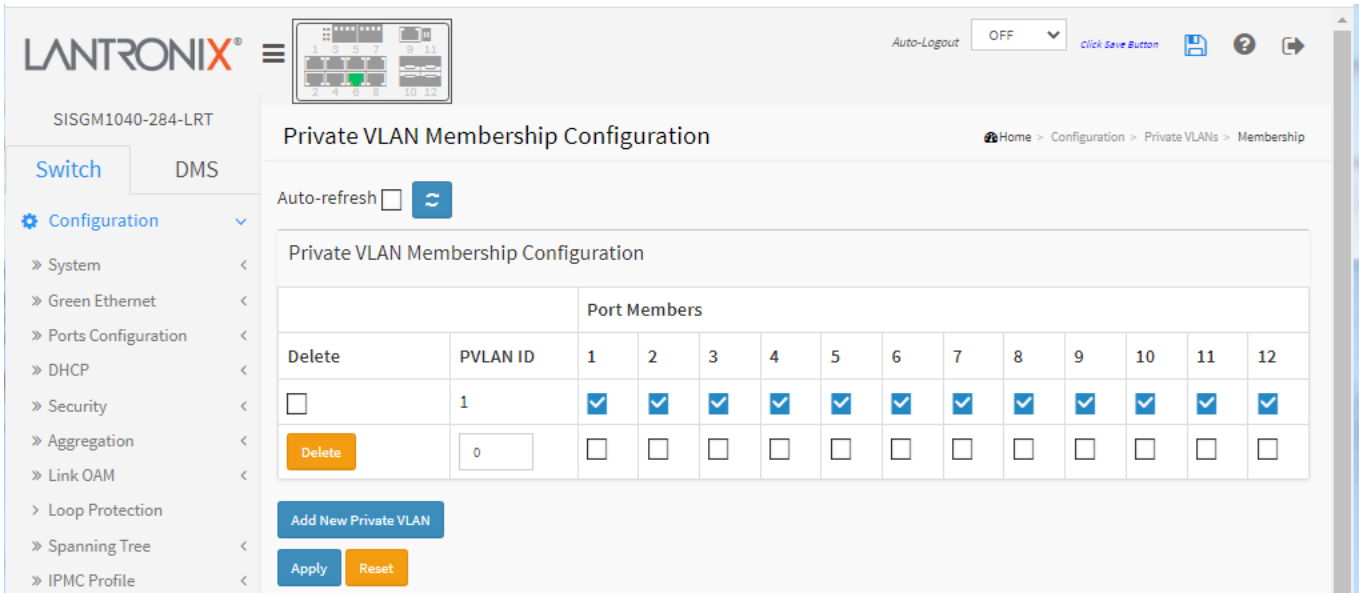
The Private VLAN membership configurations for the switch can be monitored and modified here. Private VLANs can be added or deleted here. Port members of each Private VLAN can be added or removed here.

Private VLANs are based on the source port mask, and there are no connections to VLANs. This means that VLAN IDs and Private VLAN IDs can be identical.

A port must be a member of both a VLAN and a Private VLAN to be able to forward packets. By default, all ports are VLAN unaware and members of VLAN 1 and Private VLAN 1.

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

In a private VLAN, PVLANs provide layer 2 isolation between ports within the same broadcast domain. Isolated ports configured as part of PVLAN cannot communicate with each other. Member ports of a PVLAN can communicate with each other.



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

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

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

Buttons

Add New Private VLAN: Click to add a new private VLAN ID. An empty row is added to the table, and the private VLAN can be configured as needed. The allowed range for a private VLAN ID is the same as the switch port number range (1-12). Any values outside this range are not accepted, and a warning message displays.

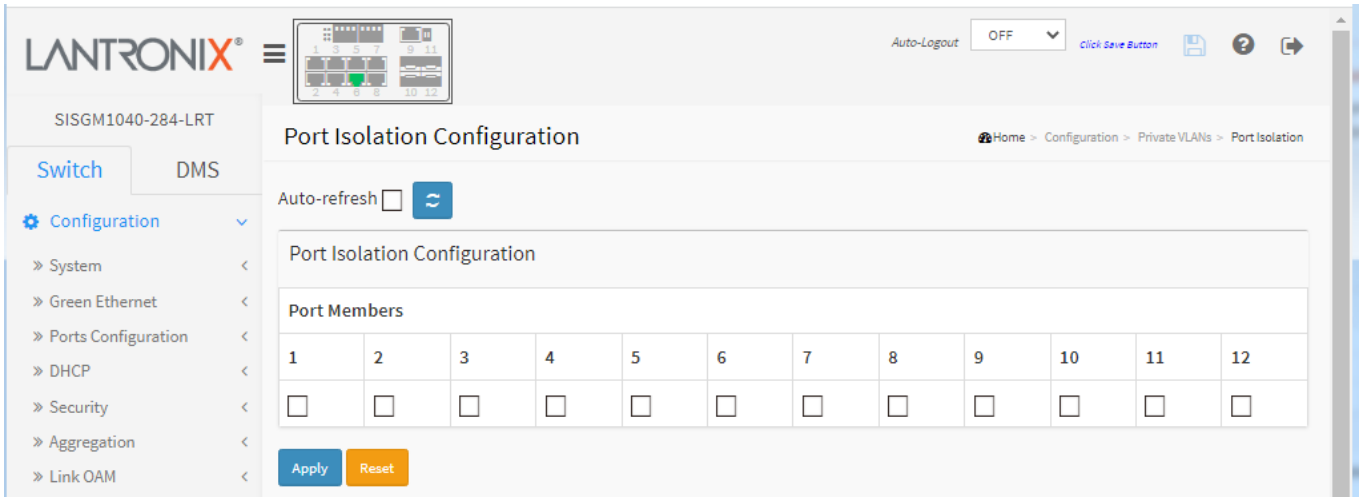
Apply: The Private VLAN is enabled when you click "Apply".

Reset: Click the button to undo the addition of new Private VLANs.

Configuration > Private VLANs > Port Isolation

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.



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

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

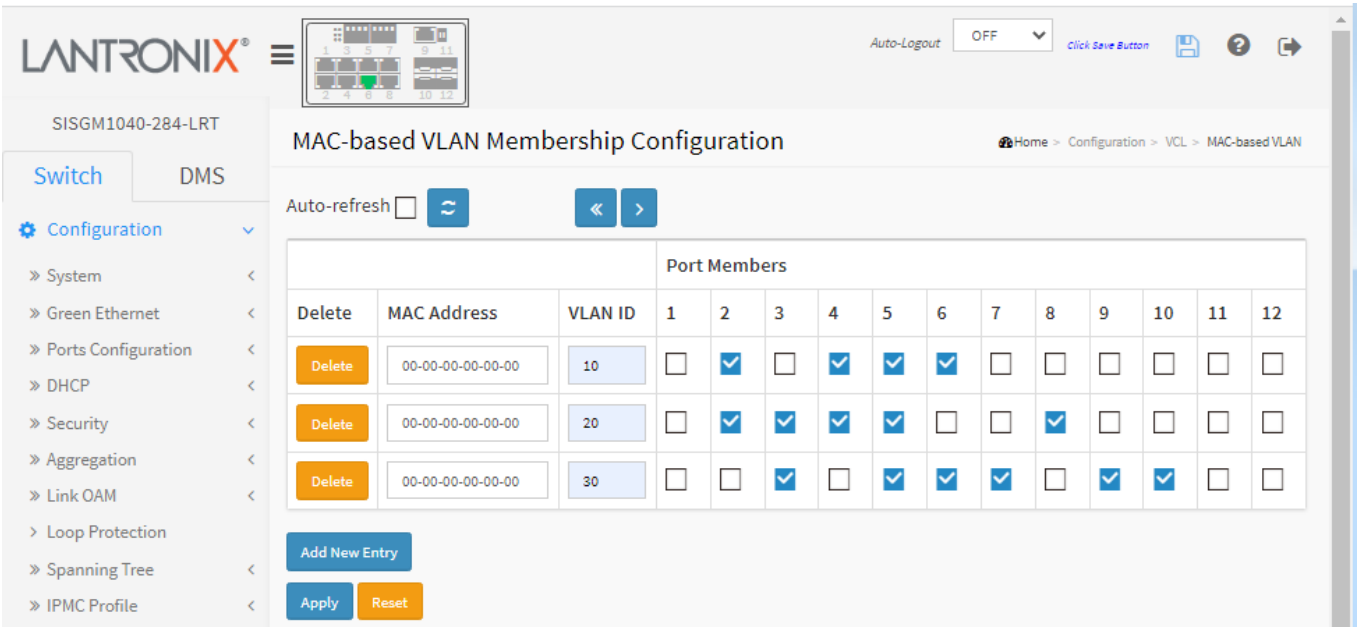
Refresh: Click to refresh the page immediately.

Apply: Click to save changes.

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

Configuration > VCL > MAC-based VLAN

The MAC address to VLAN ID mappings can be configured here. This page allows adding and deleting MAC-based VLAN Classification List entries and assigning the entries to different ports. The maximum possible MAC to VLAN ID mapping entries is 256.



Delete: To delete a MAC to VLAN ID mapping entry, check this box and click Apply. The entry will be deleted.

MAC Address: Indicates the MAC address of the mapping.

VLAN ID: Indicates the VLAN ID the above MAC will be mapped to.

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

Buttons

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

The MAC to VLAN ID entry is enabled when you click on "Apply". A mapping without any port members will not be added when you click "Apply". The Reset button can be used to undo the addition of new mappings.

Apply: Click to save changes.

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

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

Refresh: Refreshes the displayed table.

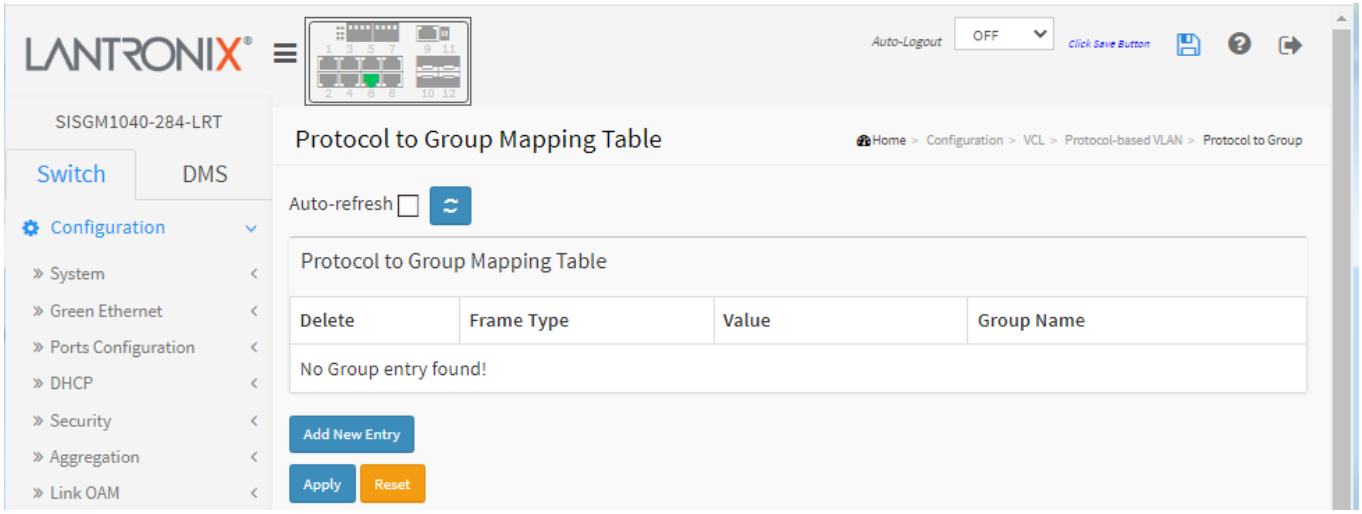
First page: Click to go to the initial page.

 **Next page**: Click to go to the next sequential page if there is one.

Messages: *MAC address to VLAN ID mapping already exists and it has to be deleted if new mapping for MAC address to VID is required*

Configuration > VCL > Protocol-based VLAN > Protocol to Group

This page allows you to view, add and delete new Protocol to Group Name mapping entries. Each protocol can be part of only one Group.



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

Frame Type: Frame Type can have one of these values: ***Ethernet***, ***LLC***, or ***SNAP***. **Note**: When changing the Frame Type field, the valid value of the following text field will vary depending on the new frame type you selected.

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

Ethernet: The value in the text field when Ethernet is selected as a Frame Type is called etype. Valid values for etype range between 0x0600 and 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 is also comprised of two different sub-values.

OUI: OUI (Organizationally Unique Identifier) is a parameter in the format of xx-xx-xx where each pair (xx) in the string is a hexadecimal value ranging between 0x00 and 0xff.

PID: PID (Protocol ID). If OUI is hexadecimal 000000, then the protocol ID is the Ethernet type (EtherType) field value for the protocol running on top of SNAP; if 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 valid values of PID will be any value between 0x0000 and 0xffff.

Group Name: A valid Group Name is a 16-character long string, unique for every entry, which consists of a combination of alphabets (a-z or A-Z) and integers(0-9). **Note**: Special characters and underscores (_) are not allowed.

Buttons

Add New Group Entry: Click to add a new entry in the mapping table. An empty row is added to the table, where 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. The maximum possible Protocol to Group mappings are limited to 128.

Apply: Click to save changes.

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

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

Refresh: Click to refresh the page immediately.

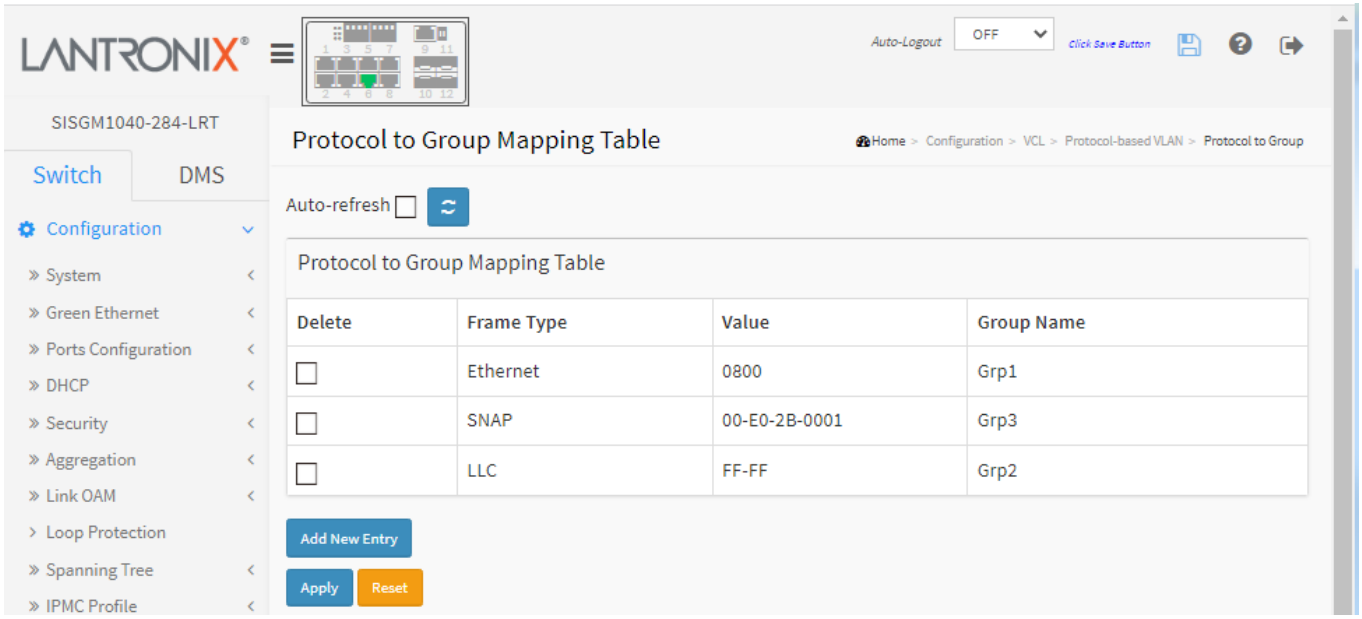
Messages:

Invalid characters found. Please check help page for correct Group name format.

Group Name field can not be empty. Please check help page for correct Group name format.

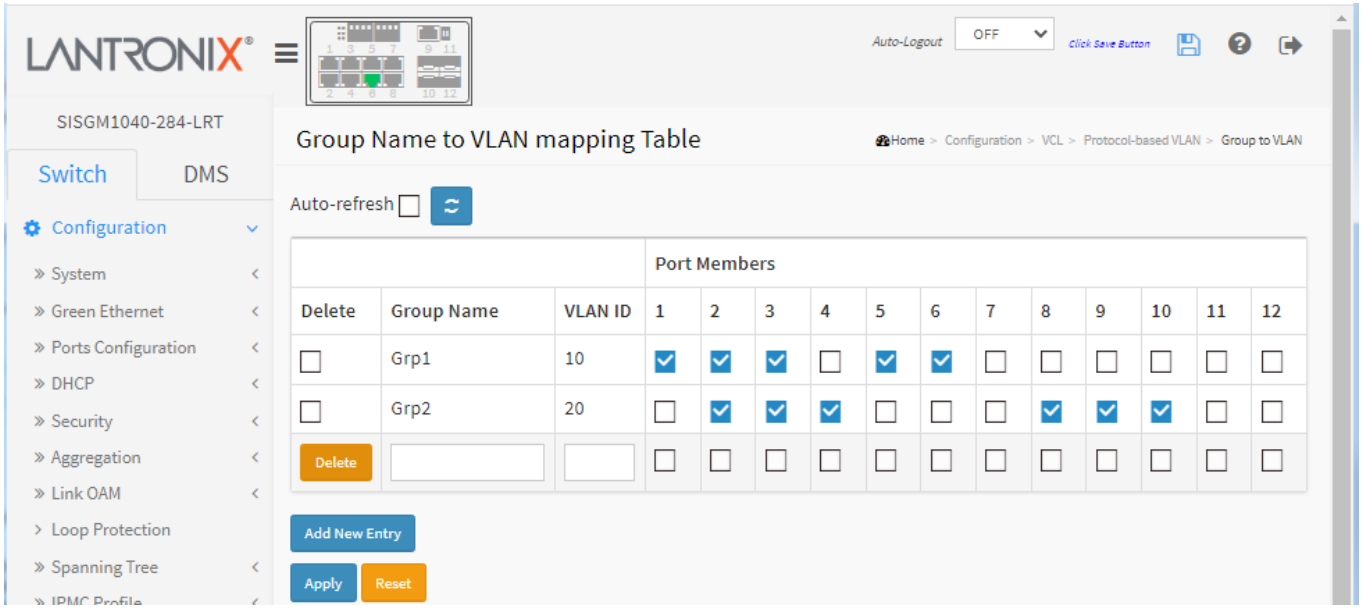
Frame type: 1 and value: 0800 is already mapped to Group ID: 'Grp1'!

Example:



Configuration > VCL > Protocol-based VLAN > Group to VLAN

This page allows you to map a Group Name (already configured or to be configured in the future) to a VLAN for the switch.



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

Group Name: A valid Group Name is a string, at the most 16 characters long, which consists of a combination of alphabets (a-z or A-Z) and integers (0-9) with no special characters allowed. You may either use a Group that already includes one or more protocols (see Protocol to Group mappings) or create a Group to VLAN ID mapping that will become active the moment you add one or more protocols inside that Group. Furthermore, the Group to VLAN ID mapping is not unique, as long as the port lists of these mappings are mutually exclusive (e.g. Group1 can be mapped to VID 1 on port#1 and to VID 2 on port#2).

VLAN ID: Indicates the VLAN ID to which the Group Name will be mapped. A valid VLAN ID ranges from 1 to 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 the mapping, check the box. To remove or exclude the port from the mapping, make sure the box is unchecked. By default, no ports are members, and all boxes are unchecked.

Buttons

Add New Entry: Click to add a new entry in the mapping table. An empty row is added to the table and the Group Name, VLAN ID and port members can be configured as needed. Valid values for a VLAN ID are 1 - 4095. The Reset button can be used to undo the addition of new entry. The maximum possible Group to VLAN mappings is limited to 256.

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

Refresh: Click to refresh the page immediately.

Apply: Click to save changes.

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

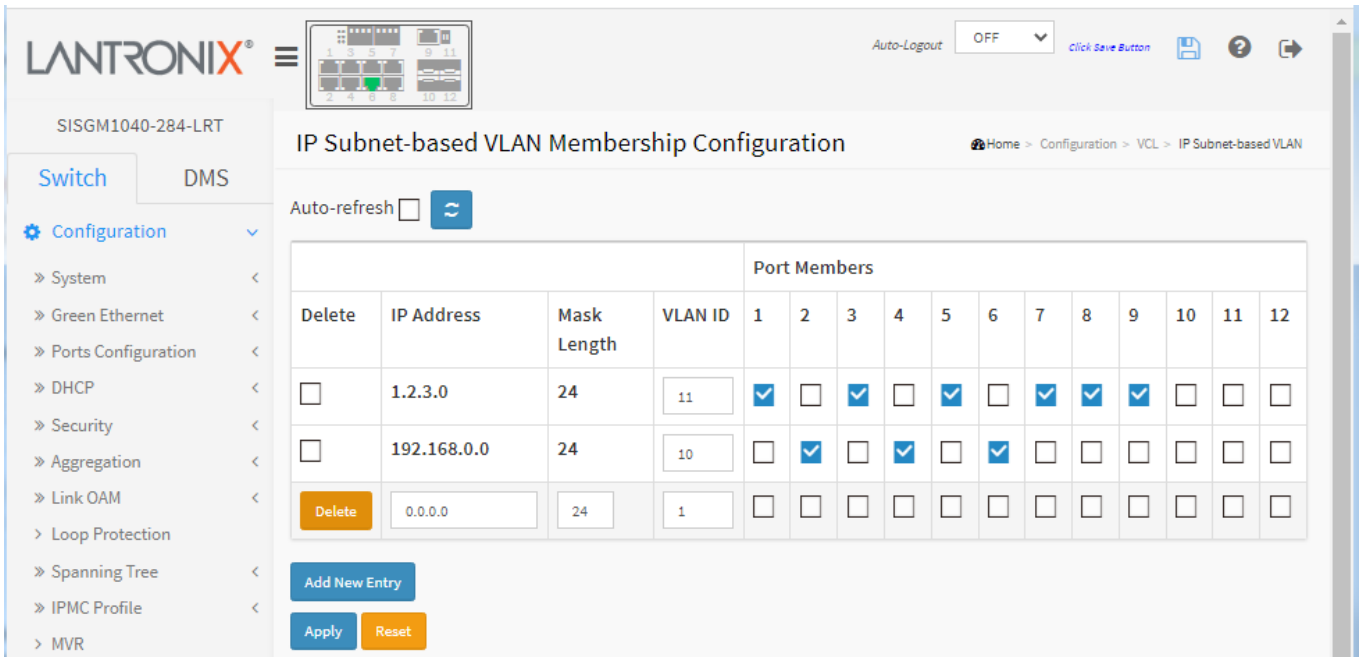
Message: *Invalid characters found. Please check help page for correct Group name format.*

Meaning: You entered one or more invalid characters in the Group Name.

Recovery: Correct the invalid Group Name entry (e.g., do not start a Group Name with a numeric value).

Configuration > VCL > IP Subnet-based VLAN

The IP subnet to VLAN ID mappings can be configured here. This page allows adding, updating and deleting IP subnet to VLAN ID mapping entries and assigning them to different ports. The table initially displays the message "*Currently no entries present*".



Delete: To delete a mapping, check this box and click Apply. The entry will be deleted in the stack.

IP Address: Indicates the subnet's IP address (Any of the subnet's host addresses can be also provided here, the application will convert it automatically).

Mask Length: Indicates the subnet's mask length.

VLAN ID: Indicates the VLAN ID the subnet will be mapped to. IP Subnet to VLAN ID is a unique matching.

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

Buttons

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

The IP subnet to VLAN ID mapping entry is enabled when you click on "Apply". The Reset button can be used to undo the addition of new mappings. The maximum possible IP subnet to VLAN ID mappings are limited to 128.

Apply: Click to save changes.

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

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

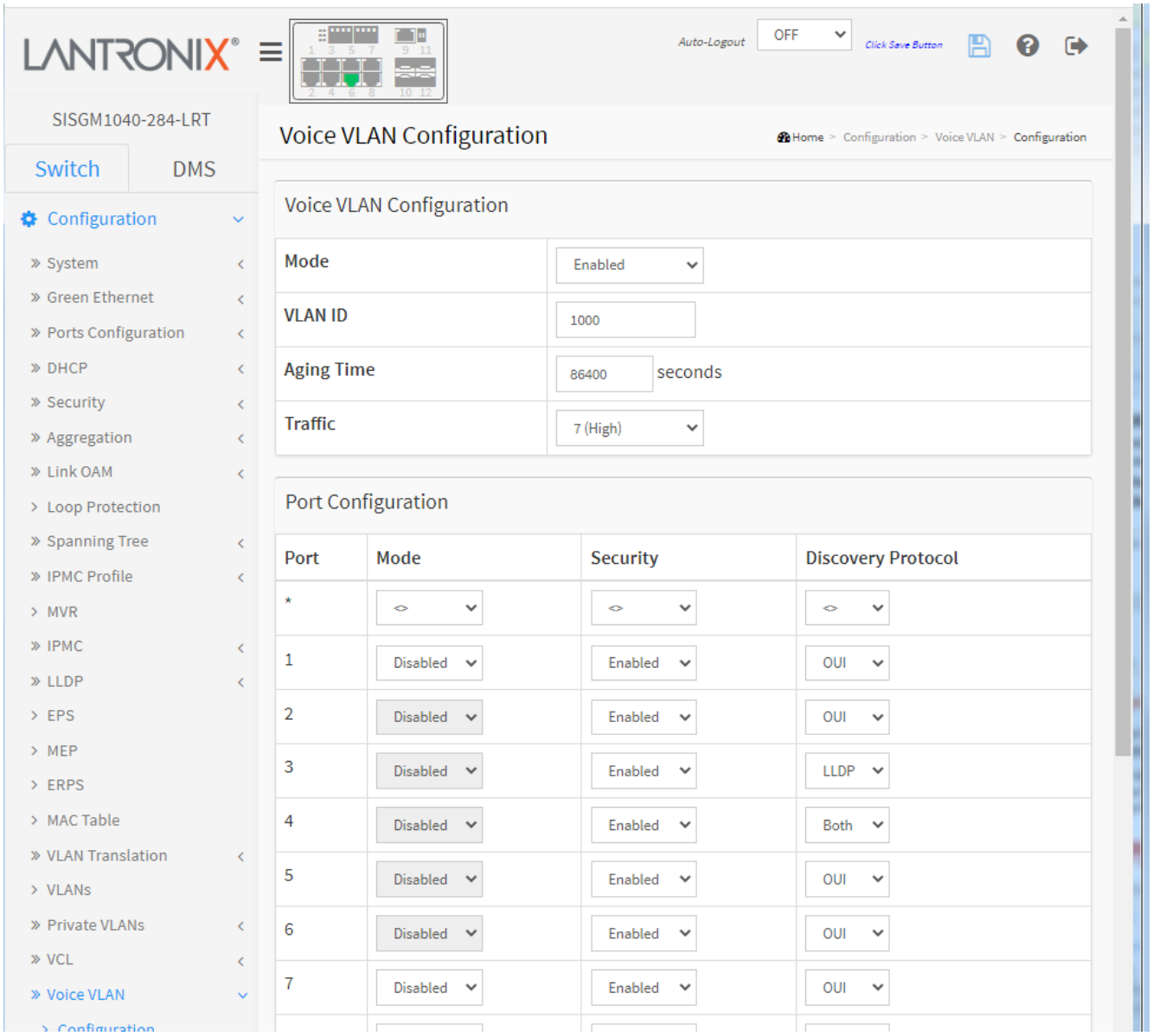
Refresh: Refreshes the displayed table.

Messages: *Subnet 0.0.0.0/x is not valid. Please use a non-zero subnet.*

Configuration > Voice VLAN > 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 with its own GUI.

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



Voice VLAN Configuration section:

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

Enabled: Enable Voice VLAN mode operation (default).

Disabled: Disable Voice VLAN mode operation.

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

Aging Time: Indicates the Voice VLAN secure learning aging time. The allowed range is 10 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. The default is 86400 seconds.

Traffic: Indicates the Voice VLAN traffic class (0 (Low) – 7 (High). All traffic on the Voice VLAN will apply this class.

Port Configuration section:

Port : A row displays for each port 1-12.

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

Disabled: Disjoin from Voice VLAN.

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

Forced: Force join to Voice VLAN.

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

Enabled: Enable Voice VLAN security mode operation.

Disabled: Disable Voice VLAN security mode operation.

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

OUI: Detect telephony device by OUI address.

LLDP: Detect telephony device by LLDP.

Both: Both OUI and LLDP.

Buttons

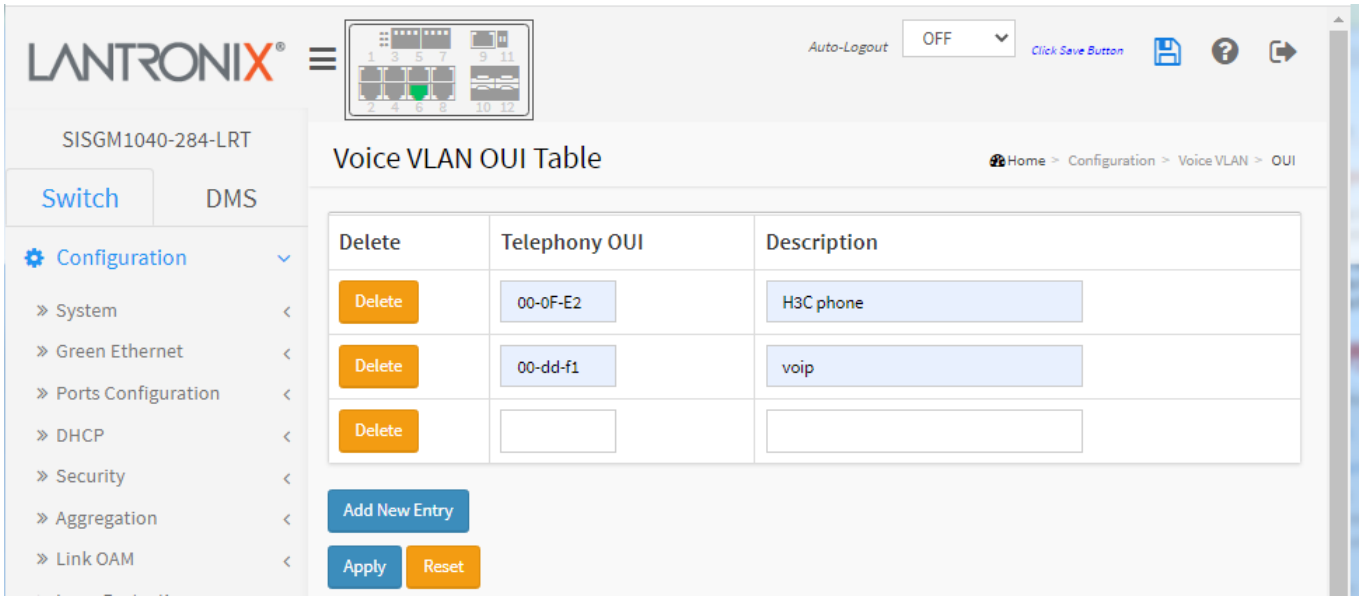
Apply: Click to apply changes immediately.

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

Configuration > Voice VLAN > OUI

Configure VOICE VLAN OUI table on this page. The maximum number of entries is 16. Modifying the OUI table will restart auto detection of the OUI process.

An OUI is an Organizationally Unique Identifier. An OUI address is a globally unique identifier assigned to a vendor by the 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.



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

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

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

Buttons

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

Apply: Click to save changes.

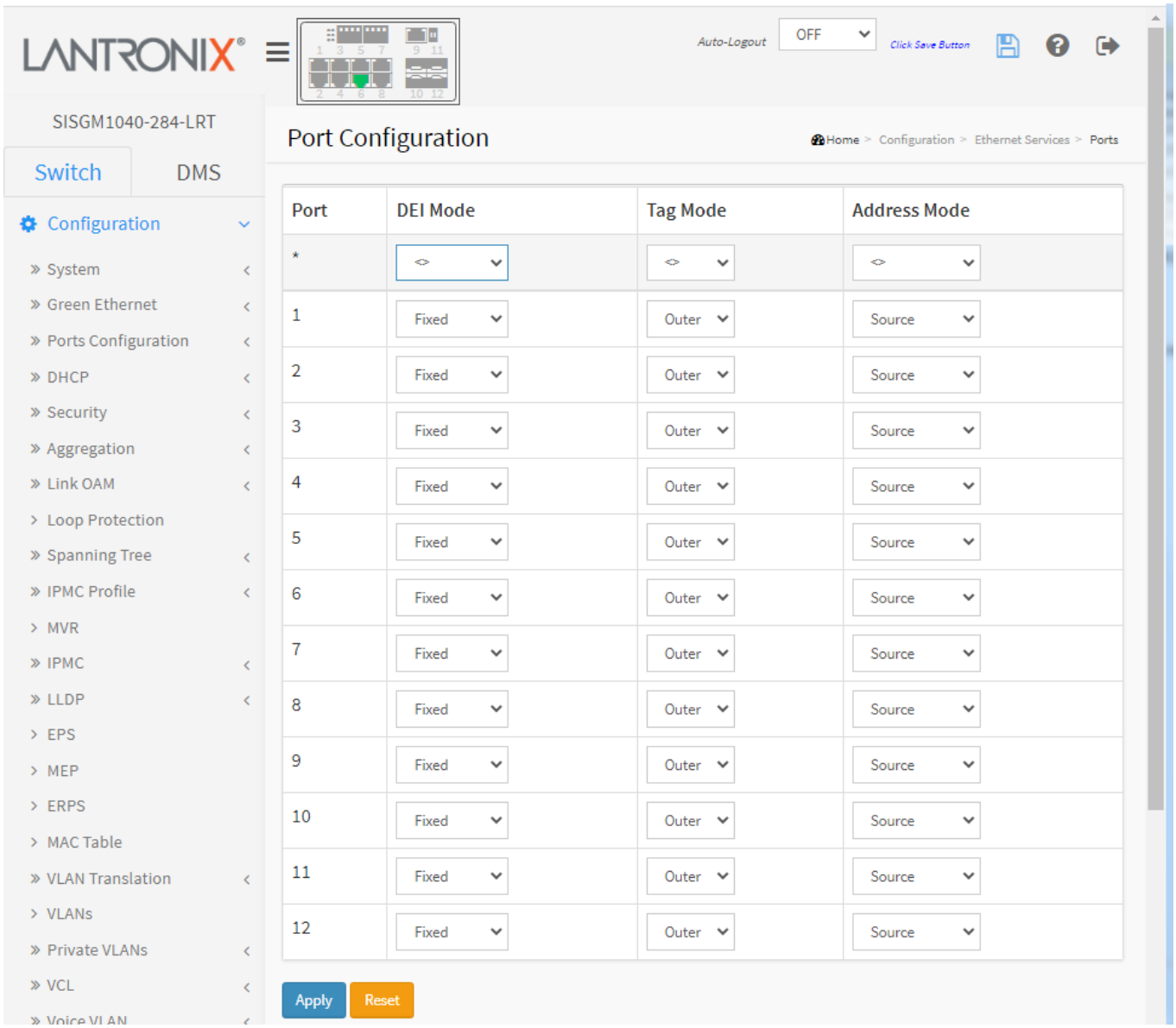
Reset: Click to undo any changes made locally and revert to previously saved values.

Messages: *The same entry already exists.*

Configuration > Ethernet Services > Ports

This page lets you view and configure EVC port parameters.

An EVC (Ethernet Virtual Connection) is a MEF standard that describe services provided to customers at User Network Interfaces (UNIs). Inside provider networks, nodes are connected using Internal Network-to-Network Interfaces (I-NNIs). Connections between service providers are done using External Network-to-Network Interfaces (E-NNIs). An Ethernet Virtual Connection is an association of two or more UNIs.



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

DEI Mode: The DEI mode for an NNI port determines whether frames transmitted on the port will have the DEI field in the outer tag marked based on the colour of the frame. The allowed values are:

Coloured: The DEI is 1 for yellow frames and 0 for green frames.

Fixed: The DEI value is determined by ECE rules.

Tag Mode: The tag mode specifying whether the EVC classification must be based on the outer or inner tag. This can be used on NNI ports connected to another service provider, where an outer "tunnel" tag is added together with the inner tag identifying the EVC. The allowed values are:

Inner: Enable inner tag in EVC classification.

Outer: Enable outer tag in EVC classification.

Address Mode: The IP/MAC address mode specifying whether the EVC classification must be based on source (SMAC/SIP) or destination (DMAC/DIP) addresses. The allowed values are:

Source: Enable SMAC/SIP matching.

Destination: Enable DMAC/DIP matching.

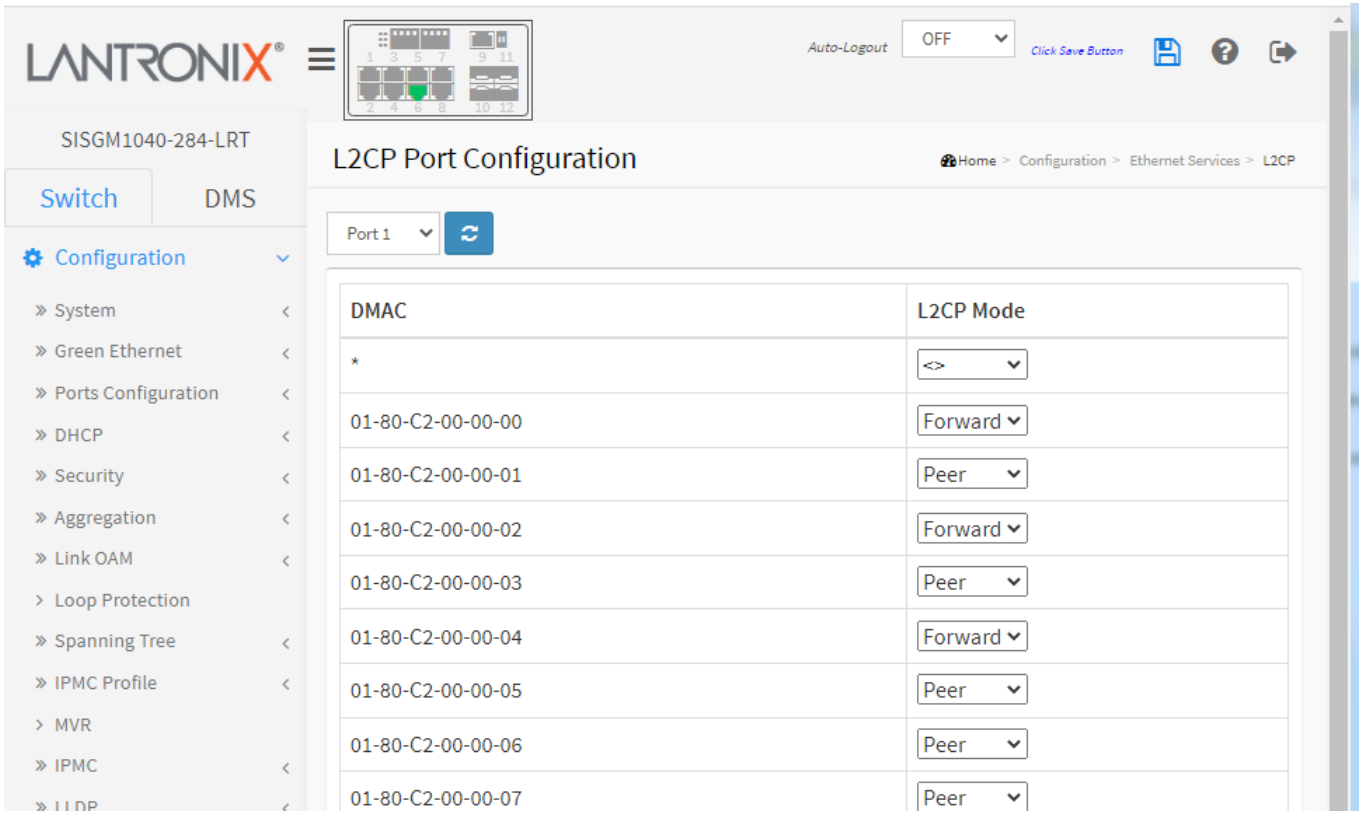
Buttons

Apply: Click to save changes.

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

Configuration > Ethernet Services > L2CP

This page displays current EVC L2CP configurations. The settings can also be configured here.



DMAC: The destination BPDU MAC addresses (01-80-C2-00-00-0X) and GARP (01-80-C2-00-00-2X) MAC addresses for the settings contained in the same row.

L2CP Mode: The L2CP mode for the specific port. Possible values are:

Peer: Allow to peer L2CP frames.

Forward: Allow to forward L2CP frames.

Buttons

The port select box lets you select which port's information is displayed.

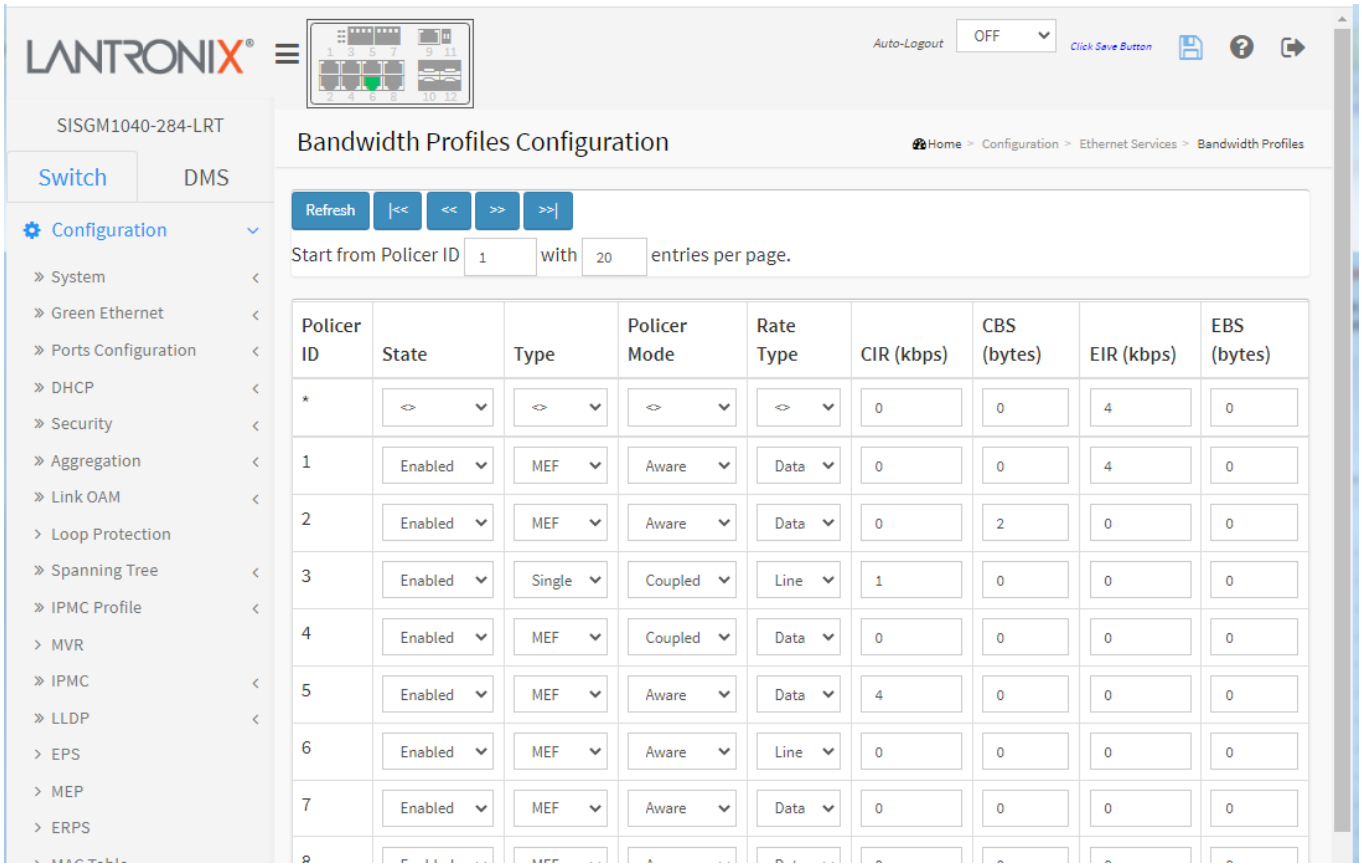
Refresh: Click to refresh the page.

Apply: Click to save changes.

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

Configuration > Ethernet Services > Bandwidth Profiles

This page lets you view and configure EVC ingress bandwidth profile parameters. Policers may be used to limit the traffic received on UNI ports. A policer can limit the bandwidth of received frames. It is located in front of the ingress queue.



Start Policer ID: The start Policer ID for displaying the table entries. The allowed range is from 1 - 256.

Number of Entries: The number of entries per page. The allowed range is 2 - 256.

Policer ID: The Policer ID is used to identify one of the 256 policers.

State: The administrative state of the bandwidth profile. The allowed values are:

Enabled: The bandwidth profile enabled.

Disabled: The bandwidth profile is disabled.

Type: The policer type of the bandwidth profile. The allowed values are:

MEF: MEF ingress bandwidth profile.

Single: Single bucket policer.

Policer Mode: The color mode of the bandwidth profile. The allowed values are:

Coupled: Color-aware mode with coupling enabled.

Aware: Color-aware mode with coupling disabled.

Rate Type: The rate type of the bandwidth profile. The allowed values are:

Data: Specify that this bandwidth profile operates on data rate.

Line: Specify that this bandwidth profile operates on line rate.

CIR: The Committed Information Rate of the bandwidth profile. The allowed range is 0 - 10000000 kilobits per second.

CBS: The Committed Burst Size of the bandwidth profile. The allowed range is 0 - 100000 bytes.

EIR: The Excess Information Rate for MEF type bandwidth profile. The allowed range is 0 - 10000000 kilobits per second.

EBS: The Excess Burst Size for MEF type bandwidth profile. The allowed range is 0 - 100000 bytes.

Buttons

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

|<<: First page. Updates the table, starting with the first entry in the table.

<<: Previous page. Updates the table, ending at the entry before the first entry currently displayed.

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

>>|: Last page. Updates the table, ending at the last entry in the table.

Apply: Click to save changes.

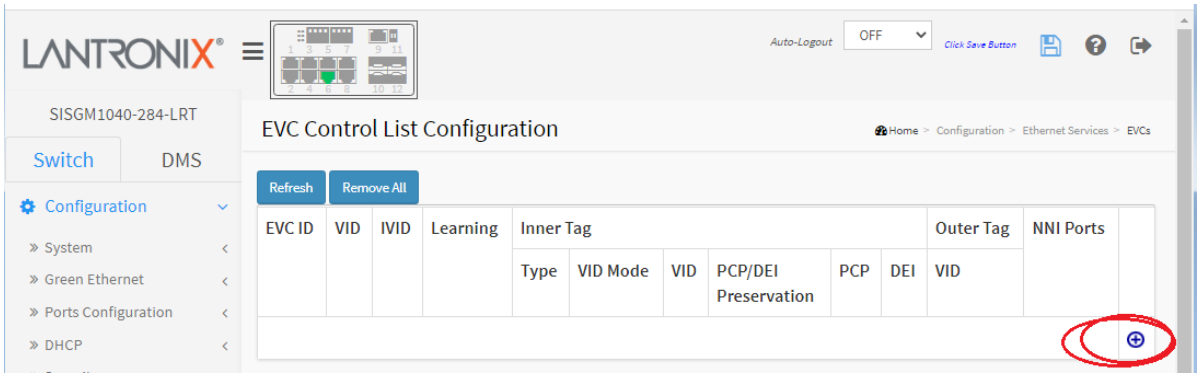
Reset: Click to undo any changes made locally and revert to previously saved values.

Configuration > Ethernet Services > EVCs

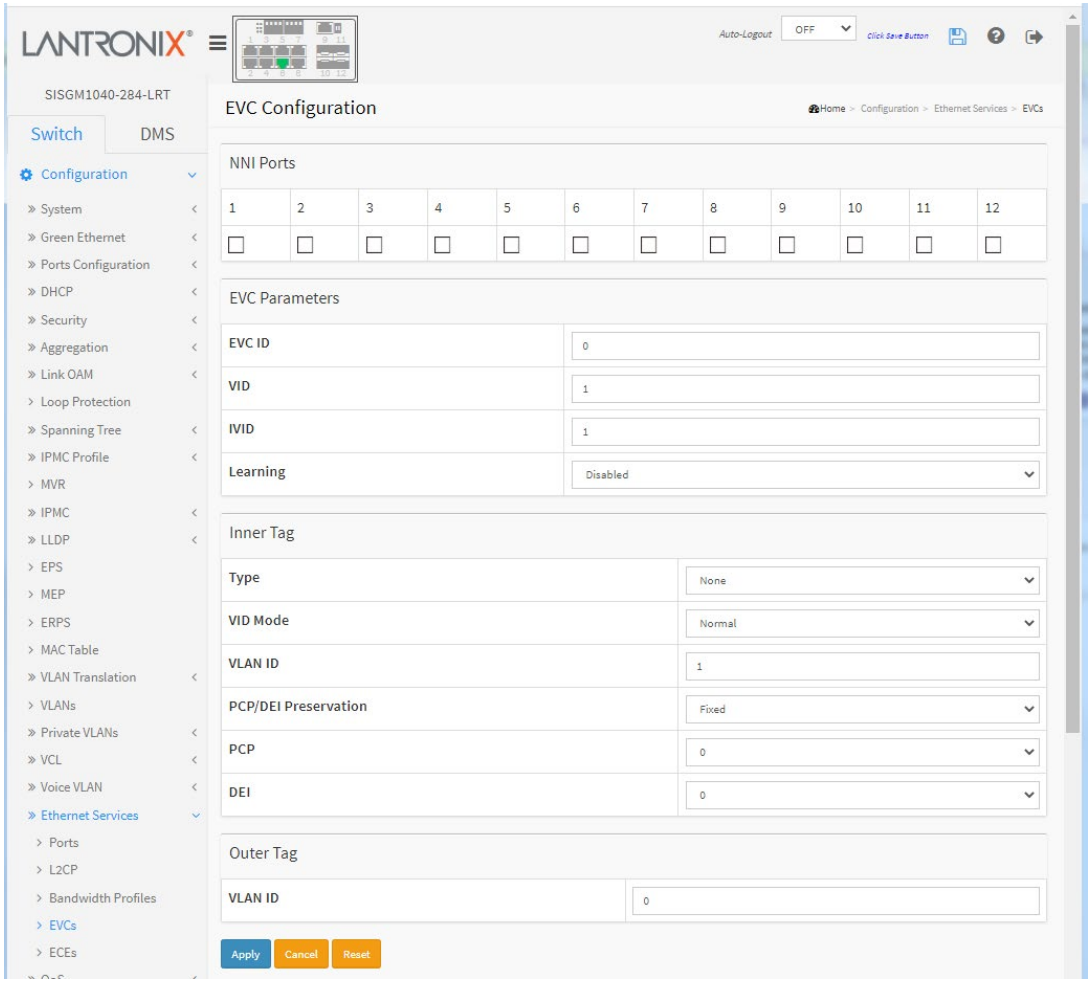
This page displays current EVC configurations. Currently only Provider Bridge based EVCs are supported.

MEF EVC (Ethernet Virtual Connection) standards describe services provided to customers at User Network Interfaces (UNIs). Inside provider networks, nodes are connected using Internal Network-to-Network Interfaces (I-NNIs). Connections between service providers are done using External Network-to-Network Interfaces (E-NNIs). An Ethernet Virtual Connection is an association of two or more UNIs.

Initially, from the default page, click the Add New EVC button ( ).



Enter the parameters at the EVC Configuration page:



NNI Ports: Checkboxes for the port(s) list of Network to Network Interfaces for the EVC.

EVC Parameters

EVC ID: The EVC ID identifies the EVC. The allowed range is 1 - 256.

VID: The VLAN ID in the PB network. It may be inserted in a C-tag, S-tag or S-custom tag depending on the NNI port VLAN configuration. The allowed range is from 1 - 4095.

IVID: The Internal/classified VLAN ID in the PB network. The allowed range is 1 - 4095.

Learning: The learning mode for the EVC controls whether source MAC addresses are learned for frames matching the EVC. Learning may be disabled if the EVC only includes two UNI/NNI ports. Possible values are:

Enabled: Learning is enabled (MAC addresses are learned).

Disabled: Learning is disabled (MAC addresses are not learned).

Inner Tag

Type: The inner tag type is used to determine whether an inner tag is inserted in frames forwarded to NNI ports. Possible values are:

None: An inner tag is not inserted.

C-tag: An inner C-tag is inserted.

S-tag: An inner S-tag is inserted.

S-custom-tag: An inner tag is inserted and the tag type is determined by the VLAN port configuration of the NNI.

Inner VID Mode: The inner VID Mode affects the VID in the inner and outer tag. Possible values are:

Normal: The VID of the two outer tags aren't swapped.

Tunnel: The VID of the two outer tags are swapped, so that the VID of the outer tag is taken from the Inner Tag configuration and the VID of the inner tag is the EVC VID. In this mode, the NNI ports are normally configured to do EVC classification based on the inner tag.

Inner Tag VID: The Inner tag VLAN ID. The allowed range is from 1 - 4095.

Inner Tag PCP/DEI Preservation: The inner tag PCP and DEI preservation. Possible values are:

Preserved: The inner tag PCP and DEI is preserved.

Fixed: The inner tag PCP and DEI is fixed.

Inner Tag PCP: The inner tag PCP value. The allowed range is from 0 - 7.

Inner Tag DEI: The inner tag DEI value. The allowed value is 0 or 1.

Outer Tag

VID: The EVC outer tag VID for UNI ports. The allowed range is from 1 - 4095.

Buttons

Apply: Click to save changes.

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

Cancel: Return to the previous page; any changes made locally will be undone.

Modification Buttons

You can modify each EVC in the table using these buttons:

: Edits the EVC row.

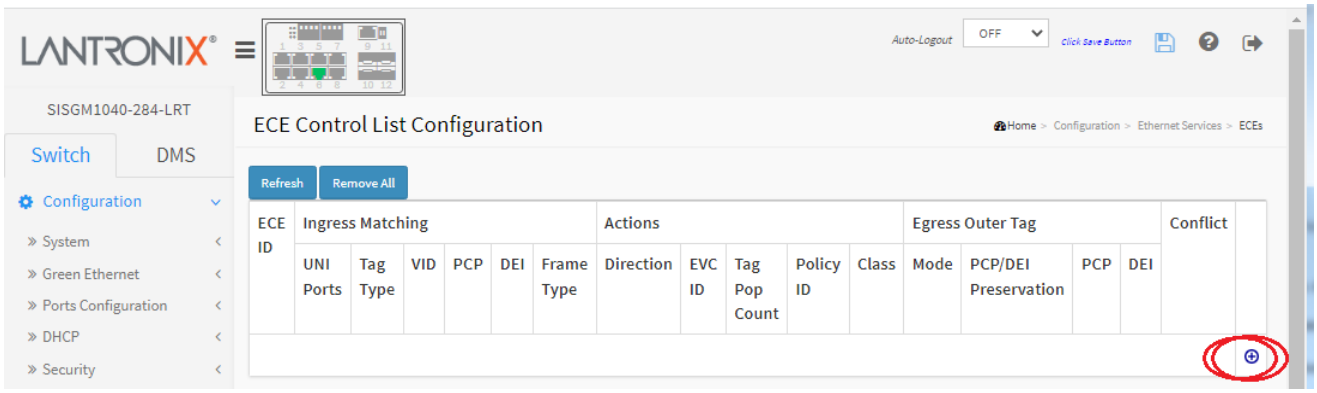
: Deletes the EVC.

: Adds new EVC.

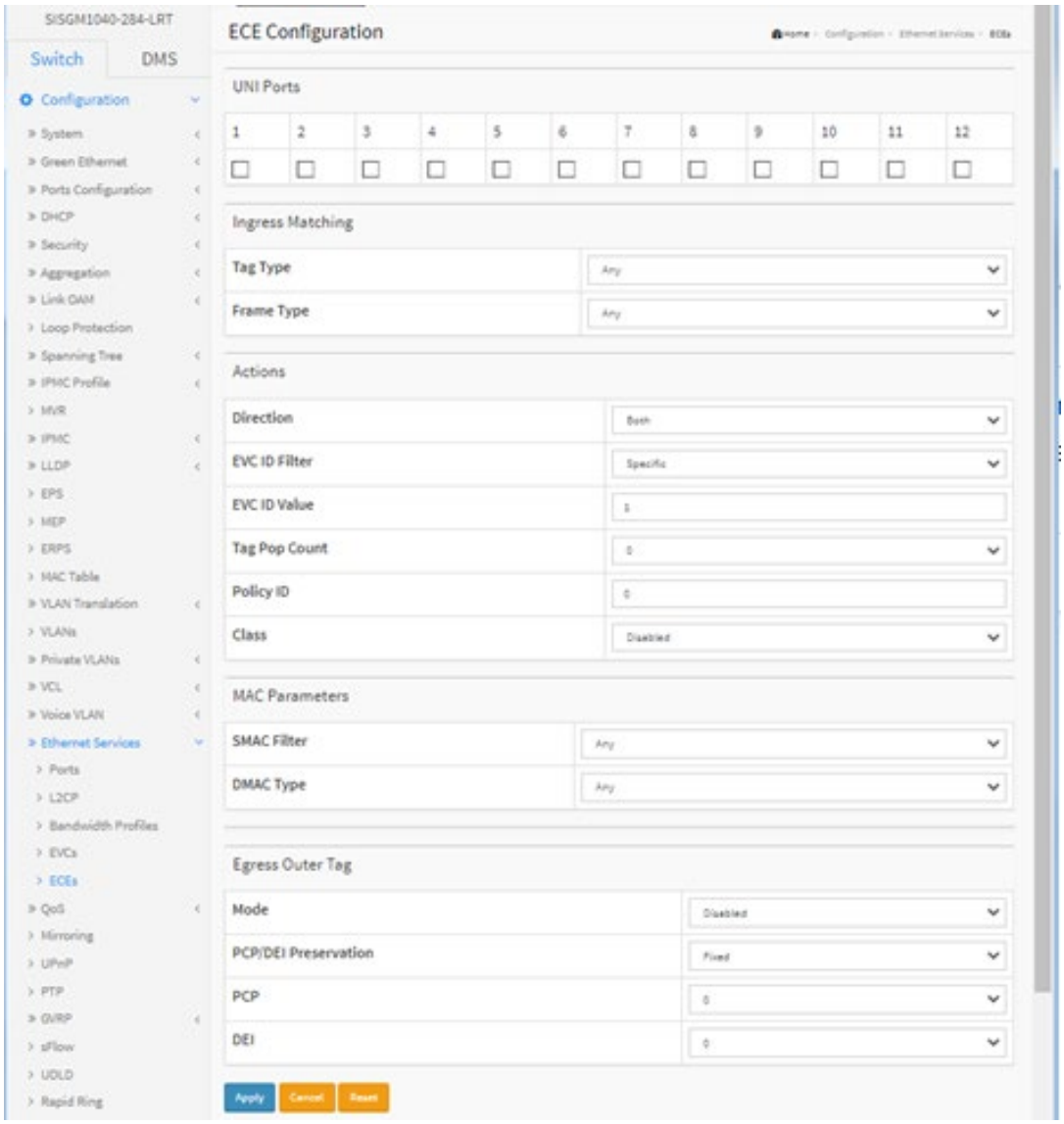
Example:

Configuration > Ethernet Services > ECEs

This page lets you view and set ECE parameters. ECE (EVC Control Entry) rules are ordered in a list to control the preferred classification. Initially, from the default page, click the Add New EVC button (⊕).



Enter the parameters at the EVC Configuration page:



UNI Ports: The list of User Network Interfaces for the ECE.

UNI Matching

Tag Type: The tag type for matching the ECE. Possible values are:

Any: The ECE will match both tagged and untagged frames.

Untagged: The ECE will match untagged frames only.

C-Tagged: The ECE will match custom tagged frames only.

S-Tagged: The ECE will match service tagged frames only.

Tagged: The ECE will match tagged frames only.

VLAN ID Filter: The VLAN ID filter for matching the ECE. It only significant if tag type 'Tagged' is selected. Possible values are:

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

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

Range: If you want to filter a specific VLAN ID range filter with this ECE, choose this value. A field for entering a range appears.

VLAN ID Value: When "Specific" is selected for the VLAN ID filter, you can enter a specific value. The allowed value is 0 - 4095.

VLAN ID Range: When "Range" is selected for the VLAN ID filter, you can enter a specific range. The allowed range is 0 - 4095.

PCP: The PCP value for matching the ECE. It only significant if tag type 'Tagged' is selected. Possible values are:

Any: The ECE will match any PCP value.

Specific: The ECE will match a specific PCP in the range 0 through 7.

Range: The ECE will match PCP values in the selected range 0-1, 2-3, 4-5, 6-7, 0-3 or 4-7.

DEI: The DEI value for matching the ECE. It only significant if tag type 'Tagged' is selected. The allowed value is: 0, 1 or Any.

Frame Type: The frame type for the ECE. Possible values are:

Any: The ECE will match any frame type.

IPv4: The ECE will match IPv4 frames only.

IPv6: The ECE will match IPv6 frames only.

IP Parameters

Protocol Filter: The IP protocol for matching the ECE. Possible values are:

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

UDP: Specify the UDP for matching the ECE.

TCP: Specify the TCP for matching the ECE.

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

Protocol Value: When "Specific" is selected for the protocol filter, you can enter a specific value. The allowed value is from 0 through 255.

SIP/DIP Filter: The source/destination IP address for matching the ECE. It depends on by the port address mode, when port address mode is set to 'Source' then the field is used for source address. Similarly, when port address mode is set to 'Destination' then the field is used for destination address. Possible values are:

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

Host: When "IPv4" is selected for the Frame Type, if you want to filter a specific host address with this ECE, choose this value. A field for entering a host address appears.

Network: When "IPv4" is selected for the Frame Type, if you want to filter a specific network address with this ECE, choose this value. Two fields for entering a specific network address and network mask appears.

Specific: When "IPv6" is selected for the Frame Type, if you want to filter a specific network address with this ECE, choose this value. Two fields for entering a specific network address and network mask appears.

SIP/DIP Address: When "IPv4" is selected for the Frame Type and "Host" or "Network" is selected for the SIP/DIP filter, you can enter a specific host or network address. When "IPv6" is selected for the Frame Type, the field only supported 32 bits for IPv6 address.

SIP/DIP Mask: When "IPv4" is selected for the Frame Type and "Host" or "Network" is selected for the SIP/DIP filter, you can enter a specific network mask. When "IPv6" is selected for the Frame Type, the field only supported 32 bits for IPv6 address mask.

DSCP Filter: The DSCP filter for matching the ECE. Possible values are:

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

Specific: If you want to filter a specific DSCP value with this ECE, choose this value. A field for entering a specific value appears.

Range: If you want to filter a specific DSCP range filter with this ECE, choose this value. A field for entering a range appears.

DSCP Value: When "Specific" is selected for the DSCP filter, you can enter a specific value. The allowed value is 0 - 63.

DSCP Range: When "Range" is selected for the DSCP filter, you can enter a specific range. The allowed range is 0 - 63.

Fragment: The IPv4 Fragment for matching the ECE. This involves the settings for the More Fragments (MF) bit and the Fragment Offset (FRAG OFFSET) field for an IPv4 frame. Possible values are:

Any: The ECE will match any MF bit.

Non-Fragment: IPv4 frames where the MF bit is set or the FRAG OFFSET field is greater than zero must not be able to match this entry.

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

UDP/TCP Parameters

Source Port Filter: The TCP/UDP source port for matching the ECE. It only significant if protocol filter 'UDP' or 'TCP' is selected. Possible values are:

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

Specific: If you want to filter a specific TCP/UDP source port No. with this ECE, choose this value. A field for entering a specific No. appears.

Range: If you want to filter a specific TCP/UDP source port range filter with this ECE, choose this value. A field for entering a range appears.

Source Port No.: When "Specific" is selected for the source port filter, you can enter a specific value. The allowed value is 0 - 65535.

Source Port Range: When "Range" is selected for the source port filter, you can enter a specific range. The allowed range is 0 - 65535.

Destination Port Filter: The TCP/UDP destination port for matching the ECE. It only significant if protocol filter 'UDP' or 'TCP' is selected. Possible values are:

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

Specific: If you want to filter a specific TCP/UDP destination port No. with this ECE, choose this value. A field for entering a specific No. appears.

Range: If you want to filter a specific TCP/UDP destination port range filter with this ECE, choose this value. A field for entering a range appears.

Destination Port No.: When "Specific" is selected for the destination port filter, you can enter a specific value. The allowed value is 0 - 65535.

Destination Port Range: When "Range" is selected for the destination port filter, you can enter a specific range. The allowed range is 0 - 65535.

MAC Parameters

SMAC Filter: The source MAC address for matching the ECE. Possible values are:

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

Specific: If you want to filter a specific SMAC value with this ECE, choose this value. A field for entering a specific value appears.

SMAC Value: When "Specific" is selected for the SMAC filter, you can enter a specific value. The legal format is "xx-xx-xx-xx-xx-xx" or "xx.xx.xx.xx.xx.xx" or "xxxxxxxxxxxx" (x is a hexadecimal digit).

DMAC Type: The destination MAC address type for matching the ECE. Possible values are:

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

Unicast: Frame must be unicast.

Multicast: Frame must be multicast.

Broadcast: Frame must be broadcast.

Actions

Direction: The EVCs and ECEs are used to setup flows in one or both directions as determined by the ECE Direction parameter. If the ECE is bidirectional, the ingress rules of the NNI ports will be setup to match the traffic being forwarded to NNI ports. Possible values are:

Both: Bidirectional.

UNI-to-NNI: Unidirectional from UNI to NNI.

NNI-to-UNI: Unidirectional from NNI to UNI.

EVC ID Filter: The EVC ID for the ECE. The ECE is only active when mapping to an existing EVC. Possible values are:

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

Specific: If you want to filter a specific EVC ID with this ECE, choose this value. A field for entering a specific value appears.

EVC ID Value: When "Specific" is selected for the VLAN ID filter, you can enter a specific value. The allowed value is 1 - 256.

Tag Pop Count: The ingress tag pop count for the ECE. The allowed range is 0 - 2.

Policy ID: The ACL Policy ID for the ECE for matching ACL rules. The allowed range is 0 - 255.

Class: The traffic class for the ECE. The allowed range is 0 - 7 or disabled.

Egress Outer Tag

Outer Tag Mode: The outer tag for nni-to-uni direction for the ECE. Possible values are:

Enable: Enable outer tag for nni-to-uni direction for the ECE.

Disable: Disable outer tag for nni-to-uni direction for the ECE.

Outer Tag PCP/DEI Preservation: The outer tag PCP and DEI preservation for the ECE. Possible values are:

Preserved: The outer tag PCP and DEI is preserved.

Fixed: The outer tag PCP and DEI is fixed.

Outer Tag PCP: The outer tag PCP value for the ECE. The allowed range is 0 - 7.

Outer Tag DEI: The outer tag DEI value for the ECE. The allowed value is 0 or 1.

Buttons

Apply: Click to save changes.

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

Cancel: Return to the previous page; any changes made locally will be undone.

Modification Buttons

You can modify each ECE (EVC Control Entry) in the table using these buttons:

: Inserts a new ECE before the current row.

: Edits the ECE row.

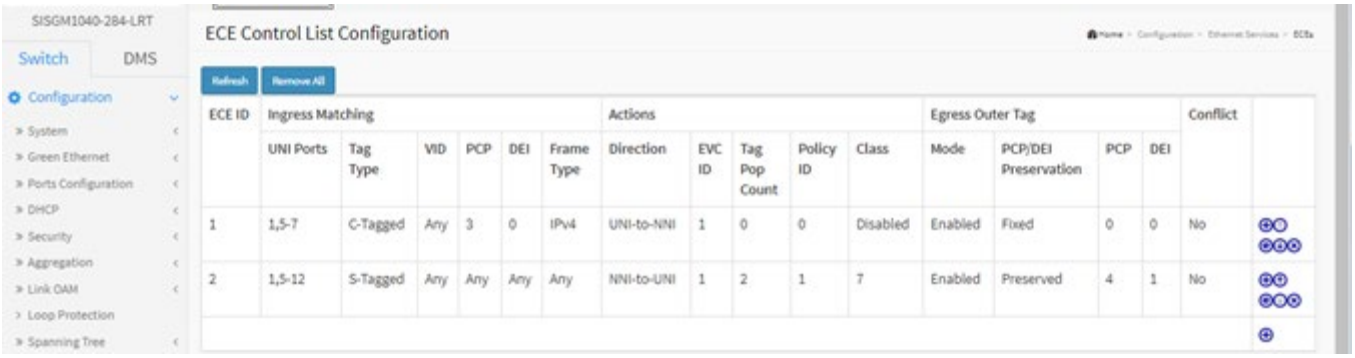
: Moves the ECE up the list.

: Moves the ECE down the list.

: Deletes the ECE.

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

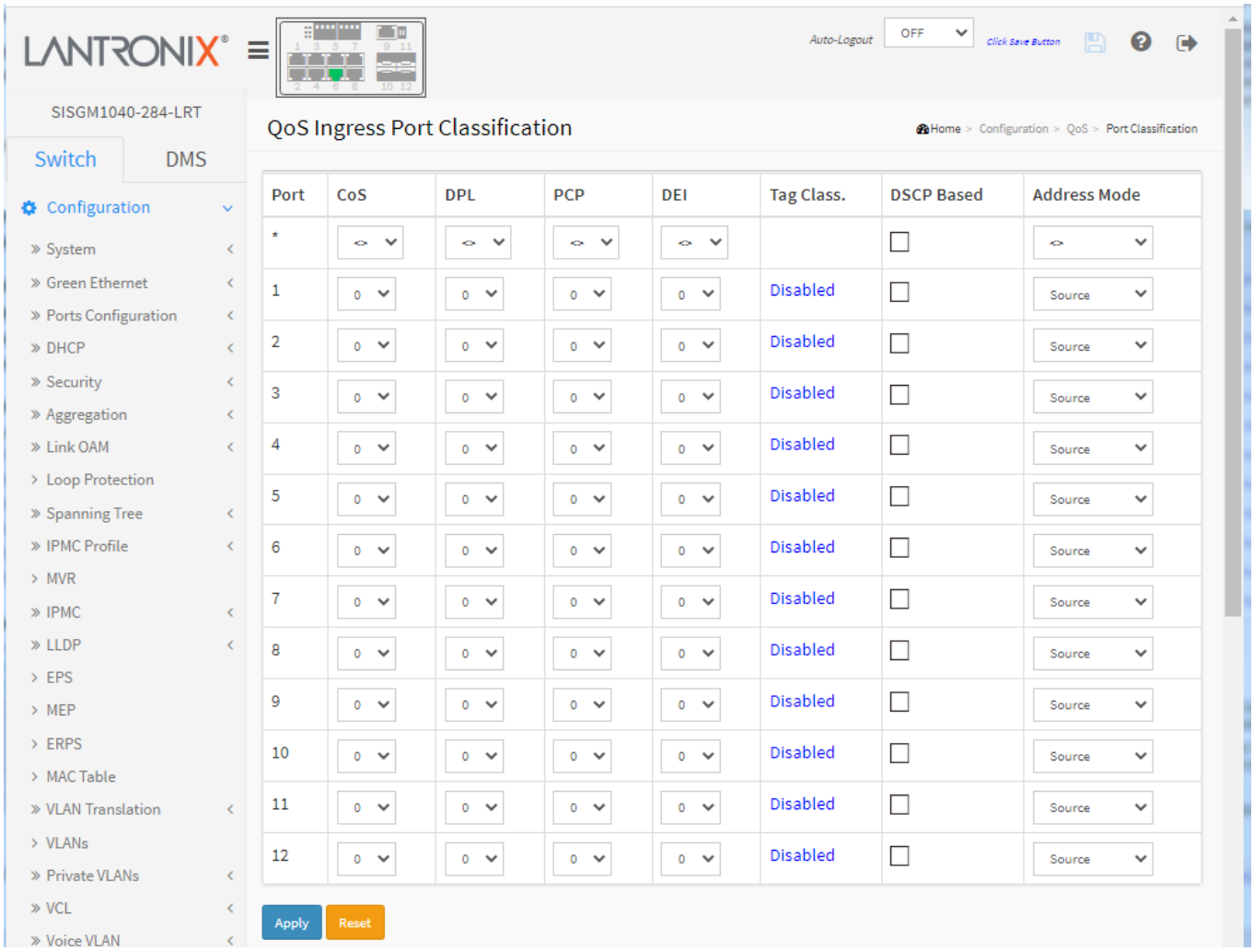
Example:



Configuration > QoS > Port Classification

This page lets you configure basic QoS Ingress Classification settings for all switch ports.

QoS (Quality of Service) is a method to guarantee a bandwidth relationship between individual applications or protocols. A communications network transports a multitude of applications and data, including high-quality video and delay-sensitive data such as real-time voice. Networks must provide secure, predictable, measurable, and sometimes guaranteed services. Achieving the required QoS becomes the secret to a successful end-to-end business solution. Therefore, QoS is the set of techniques to manage network resources.



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

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

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

The classified CoS can be overruled by a QCL entry.

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

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

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

The classified DPL can be overruled by a QCL entry.

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

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

Tag Class.: Shows the classification mode for tagged frames on this port.

Disabled: Use default CoS and DPL for tagged frames (default).

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

Click on the linked Mode in order to configure the mode and/or mapping (see below). **Note**: This setting has no effect if the port is VLAN unaware. Tagged frames received on VLAN unaware ports are always classified to the default CoS and DPL.

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

Address Mode: The IP/MAC address mode specifying whether the QCL classification must be based on source (SMAC/SIP) or destination (DMAC/DIP) addresses on this port. The allowed values are:

Source: Enable SMAC/SIP matching.

Destination: Enable DMAC/DIP matching.

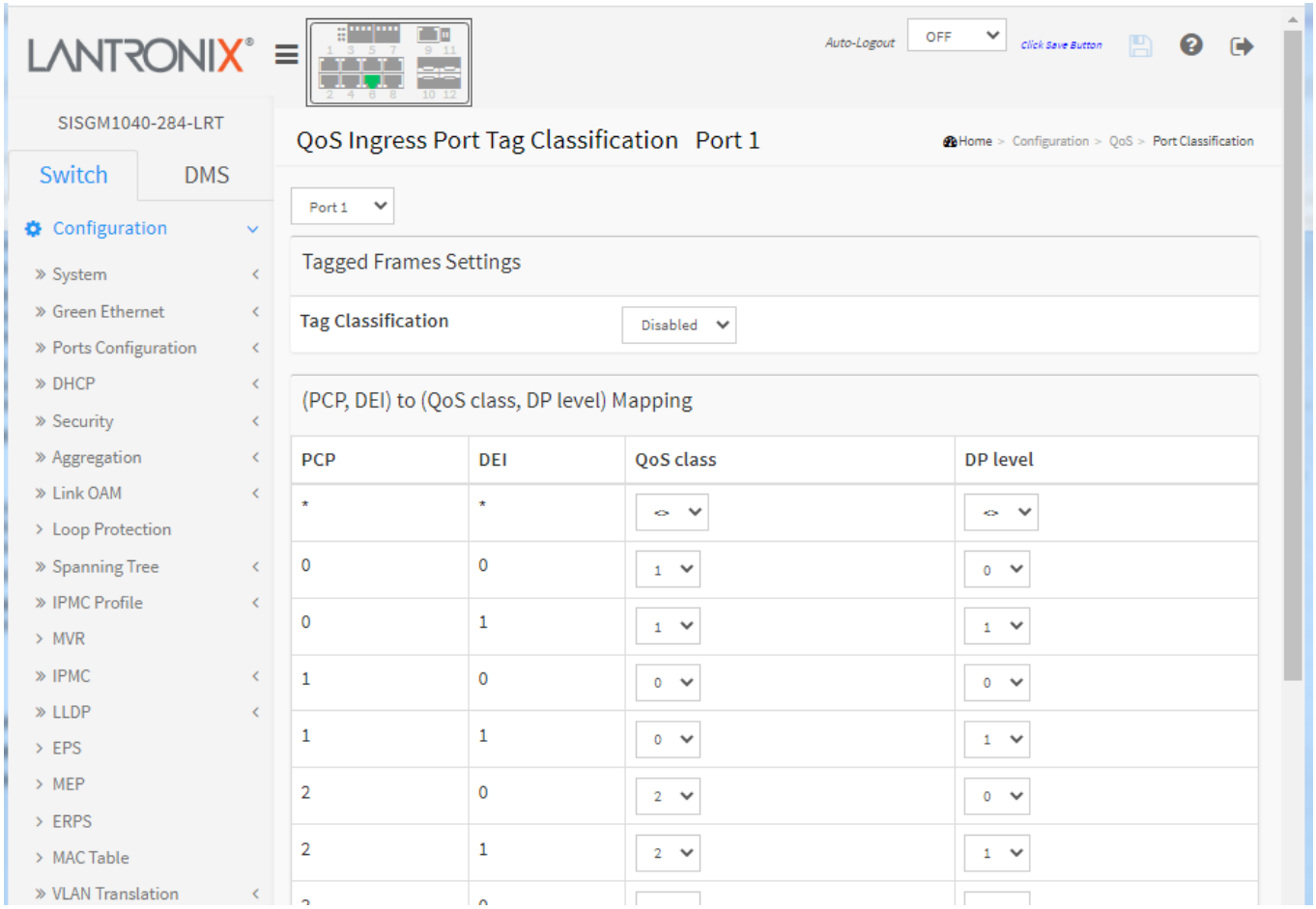
Buttons

Apply: Click to save changes.

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

QoS Ingress Port Tag Classification page: Click on the linked Mode in order to configure the mode and/or mapping for the selected port. The classification mode for tagged frames are configured on this page.

At the port dropdown select the port to be viewed.



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

Disabled: Use default QoS class and Drop Precedence Level for tagged frames.

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

(PCP, DEI) to (QoS class, DP level) Mapping : Controls the mapping of the classified (PCP, DEI) to (QoS class = 0-7, DP level = 0 or 1) values when Tag Classification is set to Enabled.

Buttons

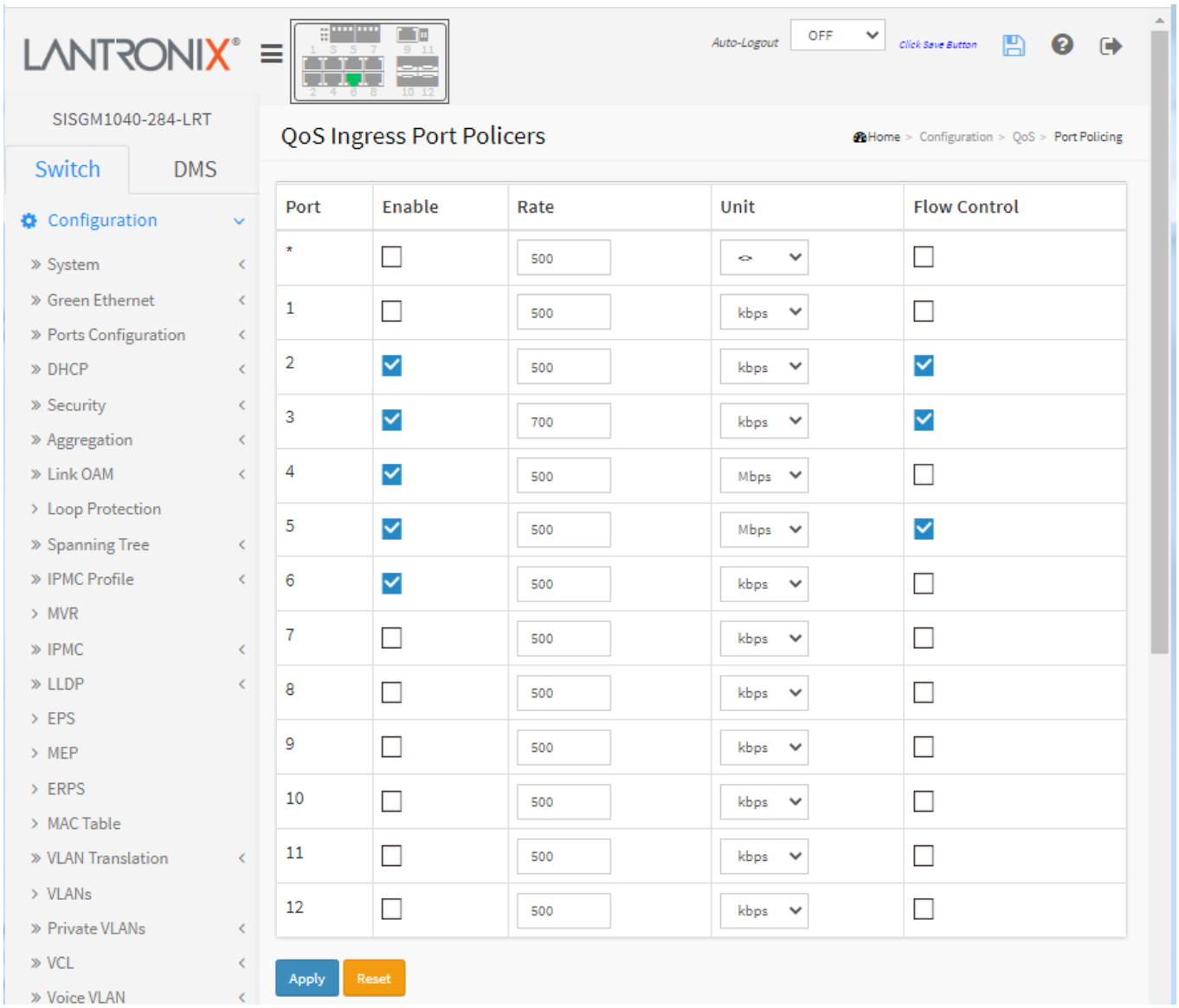
Apply : Click to save changes.

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

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

Configuration > QoS > Port Policing

Navigate to the Switch > Configuration > QoS > Port Policing menu path to display the QoS Ingress Port Policers page. This page lets you configure the Policer settings for all switch ports. A policer can limit the bandwidth of received frames. It is located in front of the ingress queue.



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

Enable: Enable or disable the port policer for this switch port.

Rate: Controls the rate for the port policer. This value is restricted to 100-3276700 when "Unit" is kbps , 1-3276 when "Unit" is mbps , 100-3276700 when "Unit" is fps, and 1-3276 when "Unit" is kfps. The rate is internally rounded up to the nearest value supported by the port policer.

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

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

Buttons

Apply: Click to save changes.

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

Messages:

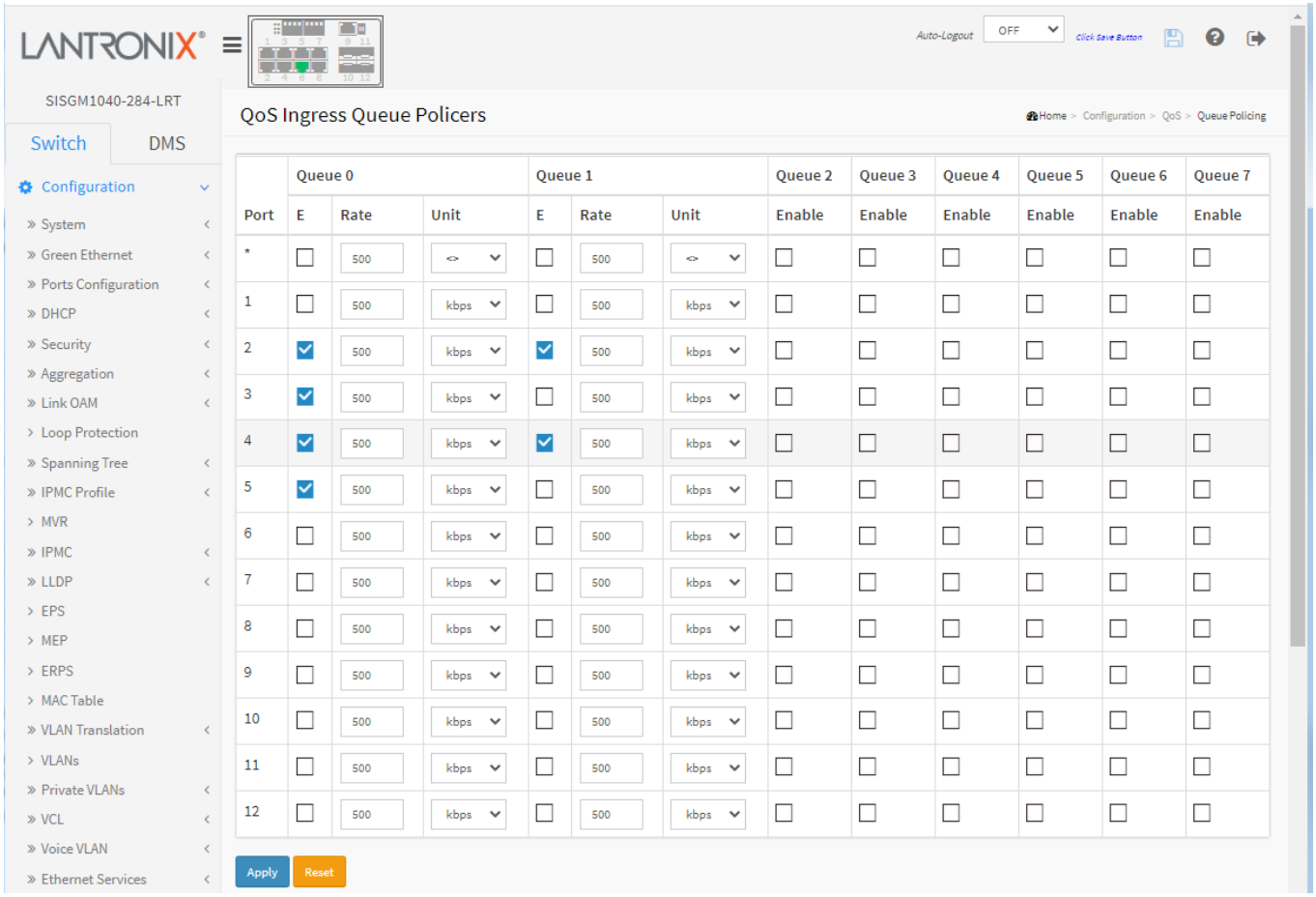
'Rate' must be an integer value between 1 and 3276 Mbps.

'Rate' must be an integer value between 100 and 3276700 kbps.

Configuration > QoS > Queue Policing

This page allows you to configure the Queue Policer settings for all switch ports.

From the default page, enable queues and set the queue parameters:



Port: The port number for which the parameters below apply.

Enable (E): Enable or disable the queue policer for this switch port.

Rate: Controls the rate for the queue policer. This value is restricted to 100-3276700 when "Unit" is kbps, and 1-3276 when "Unit" is Mbps. The rate is internally rounded up to the nearest value supported by the queue policer. This field is only shown if at least one of the queue policers are enabled.

Unit: Controls the unit of measure for the queue policer rate as kbps or Mbps. This field is only shown if at least one of the queue policers are enabled.

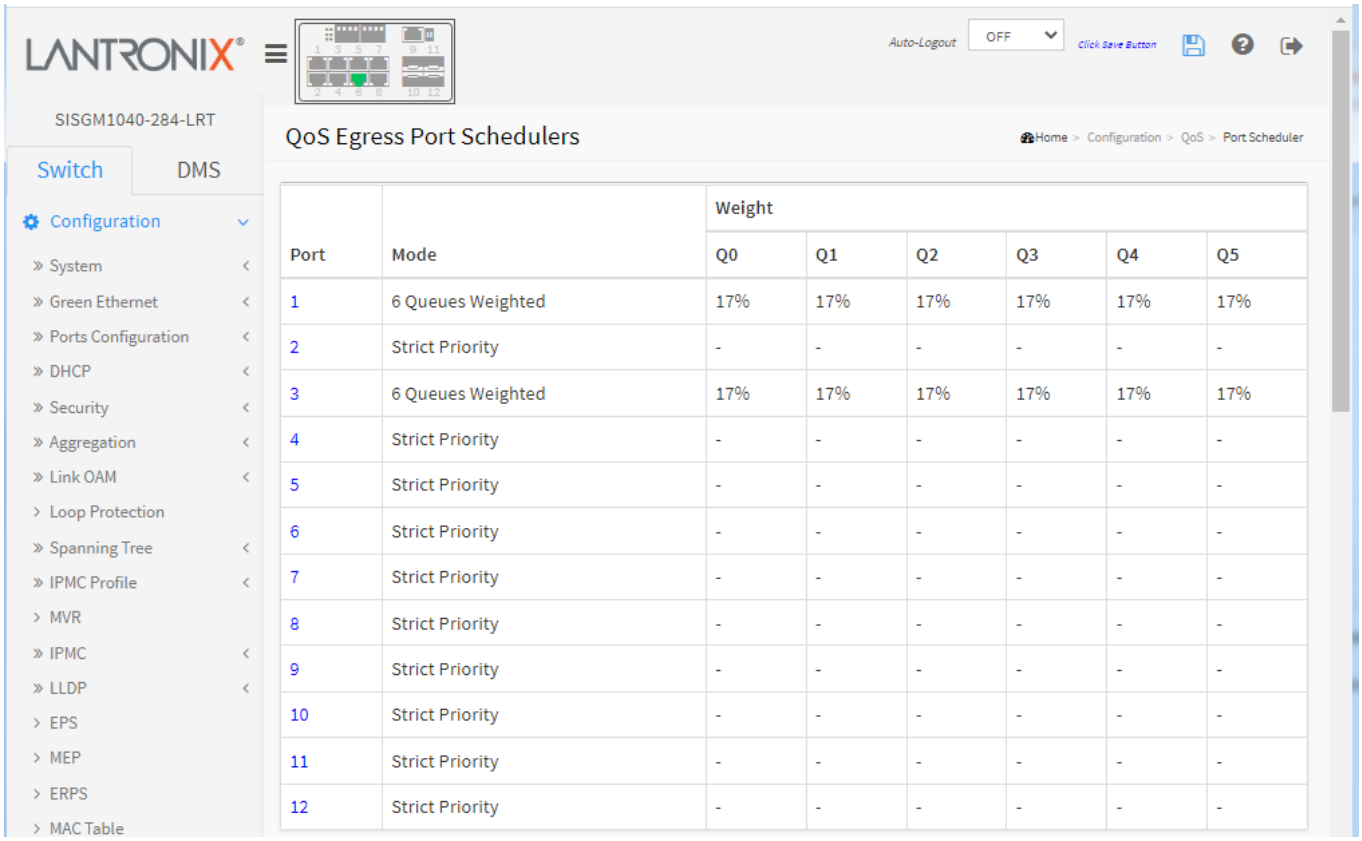
Buttons

Apply: Click to save changes.

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

Configuration > QoS > Port Scheduler

This page provides an overview of QoS Egress Port Schedulers for all switch ports.



Port	Mode	Weight					
		Q0	Q1	Q2	Q3	Q4	Q5
1	6 Queues Weighted	17%	17%	17%	17%	17%	17%
2	Strict Priority	-	-	-	-	-	-
3	6 Queues Weighted	17%	17%	17%	17%	17%	17%
4	Strict Priority	-	-	-	-	-	-
5	Strict Priority	-	-	-	-	-	-
6	Strict Priority	-	-	-	-	-	-
7	Strict Priority	-	-	-	-	-	-
8	Strict Priority	-	-	-	-	-	-
9	Strict Priority	-	-	-	-	-	-
10	Strict Priority	-	-	-	-	-	-
11	Strict Priority	-	-	-	-	-	-
12	Strict Priority	-	-	-	-	-	-

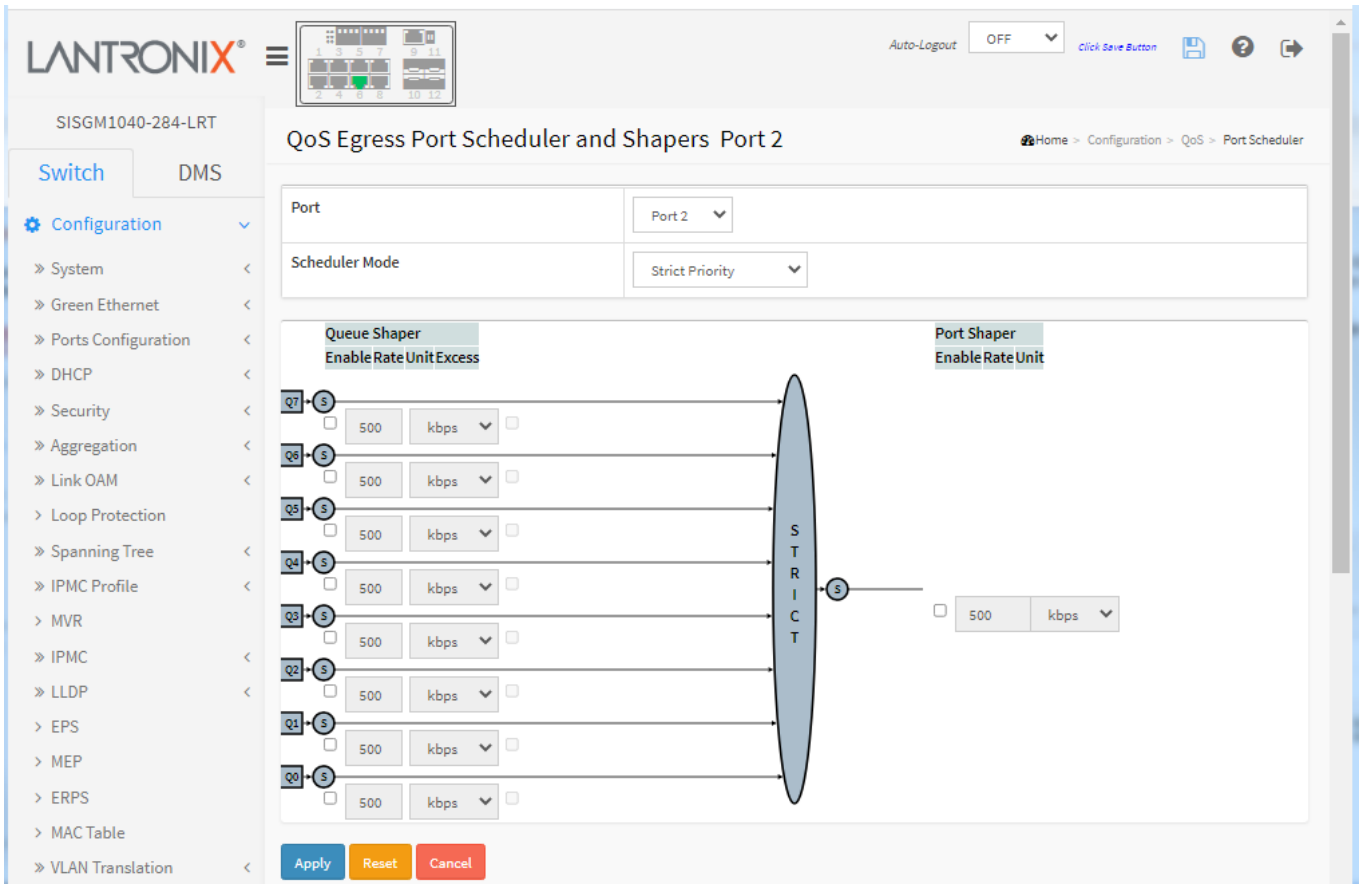
Port: The logical port for the settings contained in the same row. Click on the port number in order to configure the schedulers (see below).

Mode: Shows the scheduling mode for this port (Strict Priority or 6 Queues Weighted).

Qn: Shows the weight for this queue and port.

QoS Egress Port Scheduler and Shapers

This page allows you to configure the Scheduler and Shapers for a specific port. Scheduler Mode “Strict Priority” displays by default:



Scheduler Mode: Controls how many of the queues are scheduled as Strict and how many are scheduled as Weighted on this switch port.

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

Queue Shaper Rate: Controls the rate for the queue shaper. This value is restricted to 100-3281943 when "Unit" is kbps, and 1-3281 when "Unit" is Mbps. The rate is internally rounded up to the nearest value supported by the queue shaper.

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

Queue Shaper Excess: Controls whether the queue is allowed to use excess bandwidth.

Queue Scheduler Weight: Controls the weight for this queue. This value is restricted to 1-100. This parameter is only shown if "Scheduler Mode" is set to "Weighted".

Queue Scheduler Percent: Shows the weight in percent for this queue. This parameter is only shown if "Scheduler Mode" is set to "Weighted".

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

Port Shaper Rate: Controls the rate for the port shaper. This value is restricted to 100-3281943 when "Unit" is kbps, and 1-3281 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.

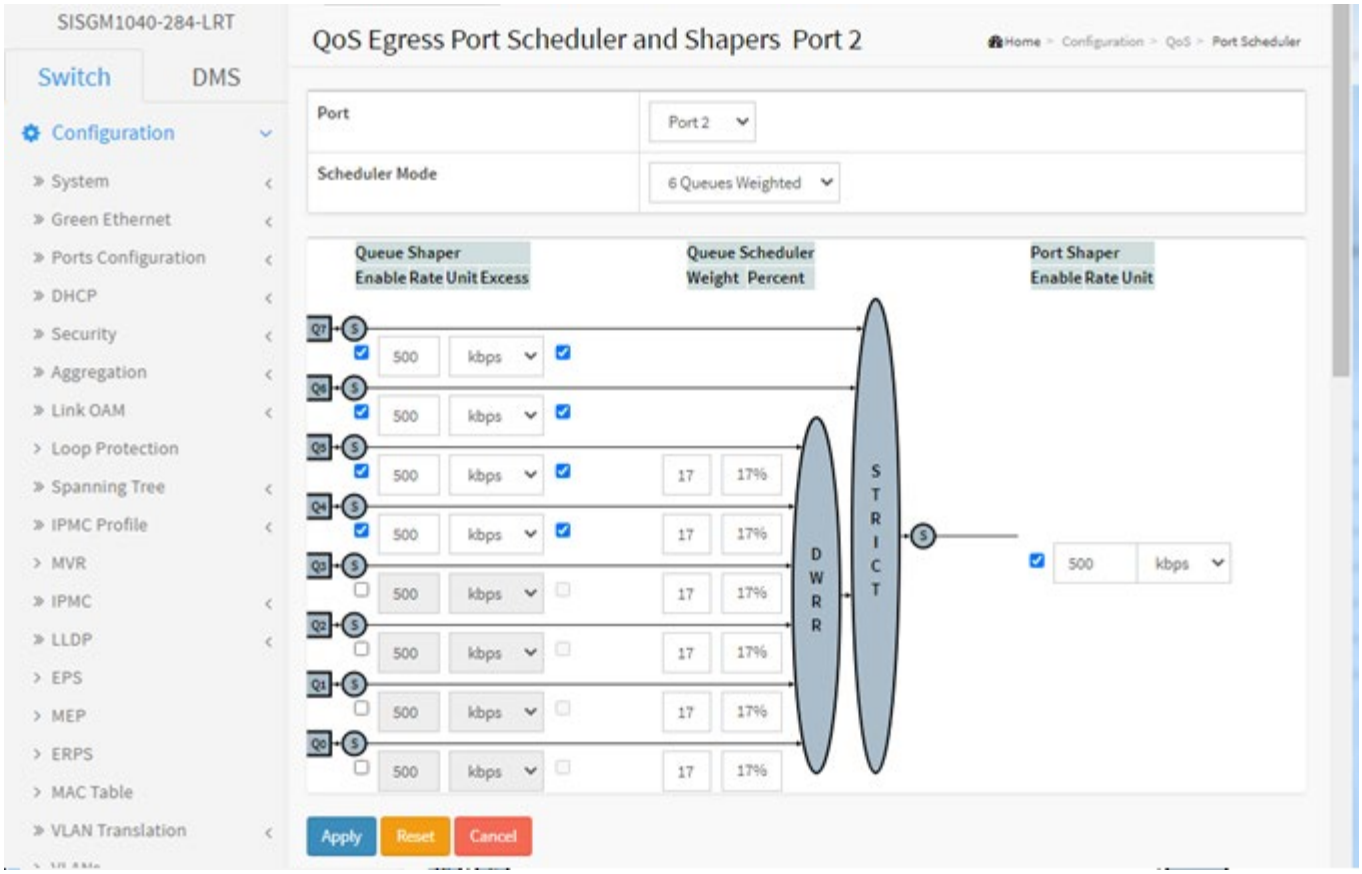
Buttons

Apply: Click to save changes.

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

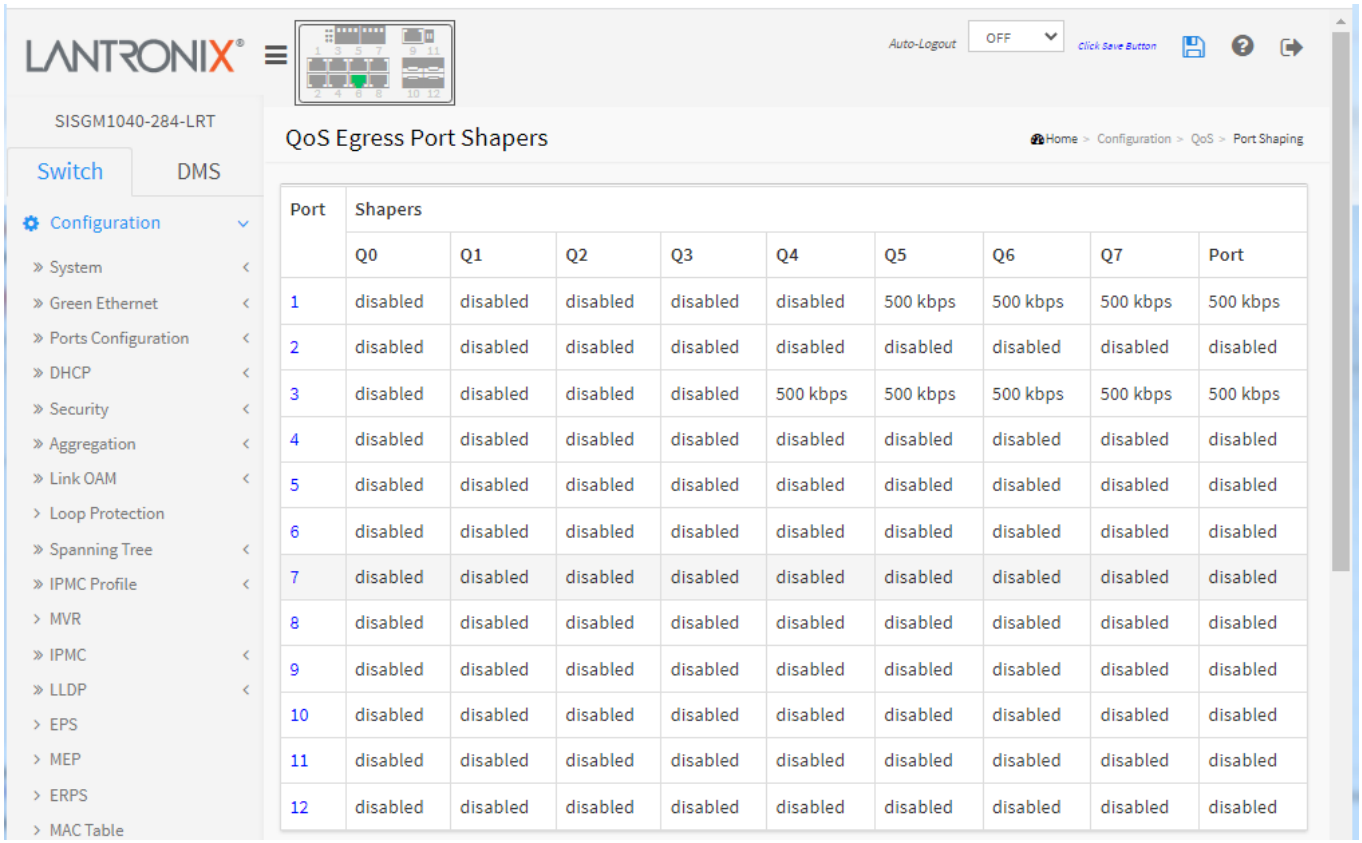
Cancel: Click to undo any changes made locally and return to the previous page.

Scheduler Mode "6 Queues Weighted":



Configuration > QoS > Port Shaping

This page provides an overview of QoS Egress Port Shapers for all switch ports.



Port	Shapers								
	Q0	Q1	Q2	Q3	Q4	Q5	Q6	Q7	Port
1	disabled	disabled	disabled	disabled	disabled	500 kbps	500 kbps	500 kbps	500 kbps
2	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled
3	disabled	disabled	disabled	disabled	500 kbps	500 kbps	500 kbps	500 kbps	500 kbps
4	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled
5	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled
6	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled
7	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled
8	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled
9	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled
10	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled
11	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled
12	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled

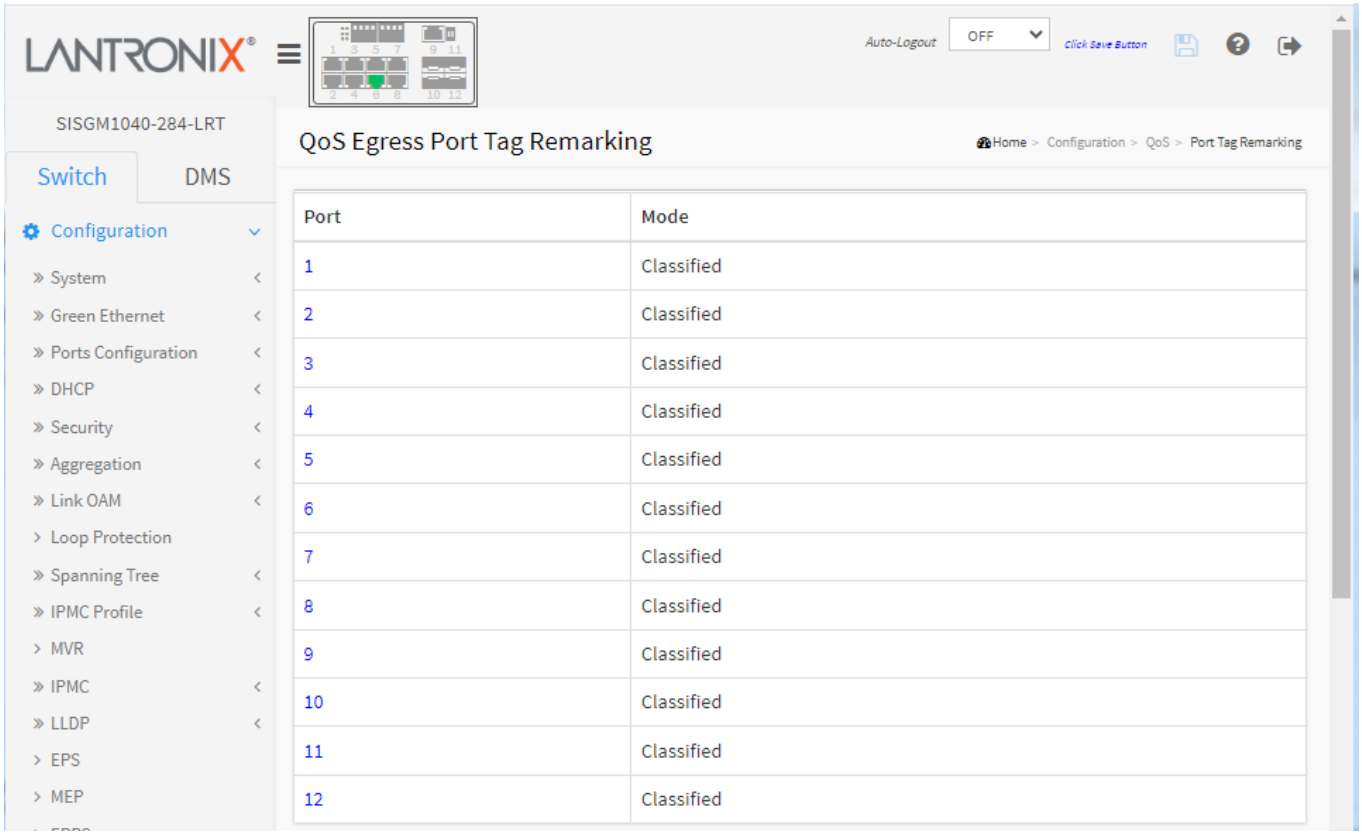
Port: The logical port for the settings contained in the same row. Click on a linked port number to configure the shapers. See “QoS Egress Port Scheduler and Shapers” above for details.

Shapers Qn: Shows "**-**" for disabled or actual queue shaper rate (e.g. "800 Mbps").

Shapers Port: Shows "**-**" for disabled or actual port shaper rate (e.g. "800 Mbps").

Configuration > QoS > Port Tag Remarking

This page provides an overview of QoS Egress Port Tag Remarking for all switch ports.



Port: The logical port for the settings contained in the same row. Click on a linked port number to configure tag remarking.

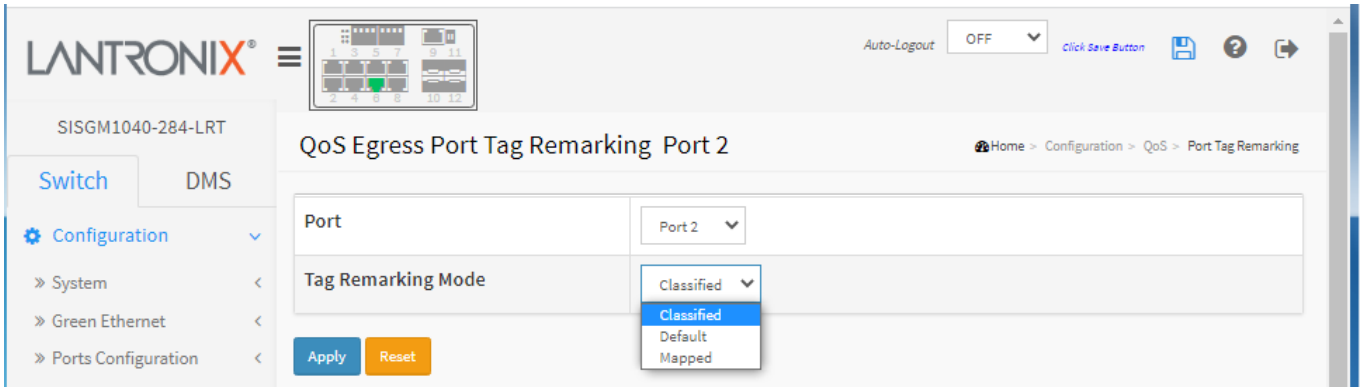
Mode: Shows the tag remarking mode for this port.

Classified: Use classified PCP/DEI values.

Default: Use default PCP/DEI values.

Mapped: Use mapped versions of QoS class and DP level.

The "QoS Egress Port Tag Remarking " page is shown below. The QoS Egress Port Tag Remarking for a specific port are configured on this page.



Port: The logical port for the settings contained in the same row. Select the port number in order to configure it.

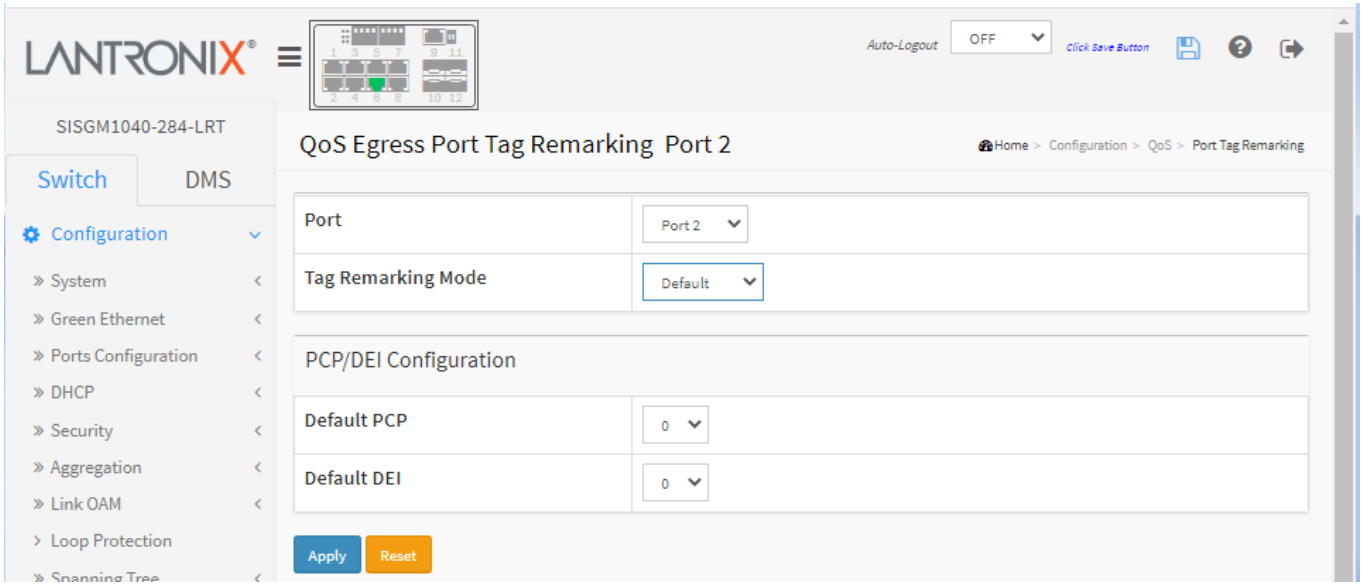
Tag Remarking Mode: Controls the tag remarking mode for this port.

Classified: Use classified PCP/DEI values.

Default: Use default PCP/DEI values.

Mapped: Use mapped versions of QoS class and DP level.

Select a different "Tag Remarking Mode" to display its PCP/DEI Configuration options:



Default PCP : Select 0-7; the default is 0.

Default DEI : Select 0 or 1; the default is 0.

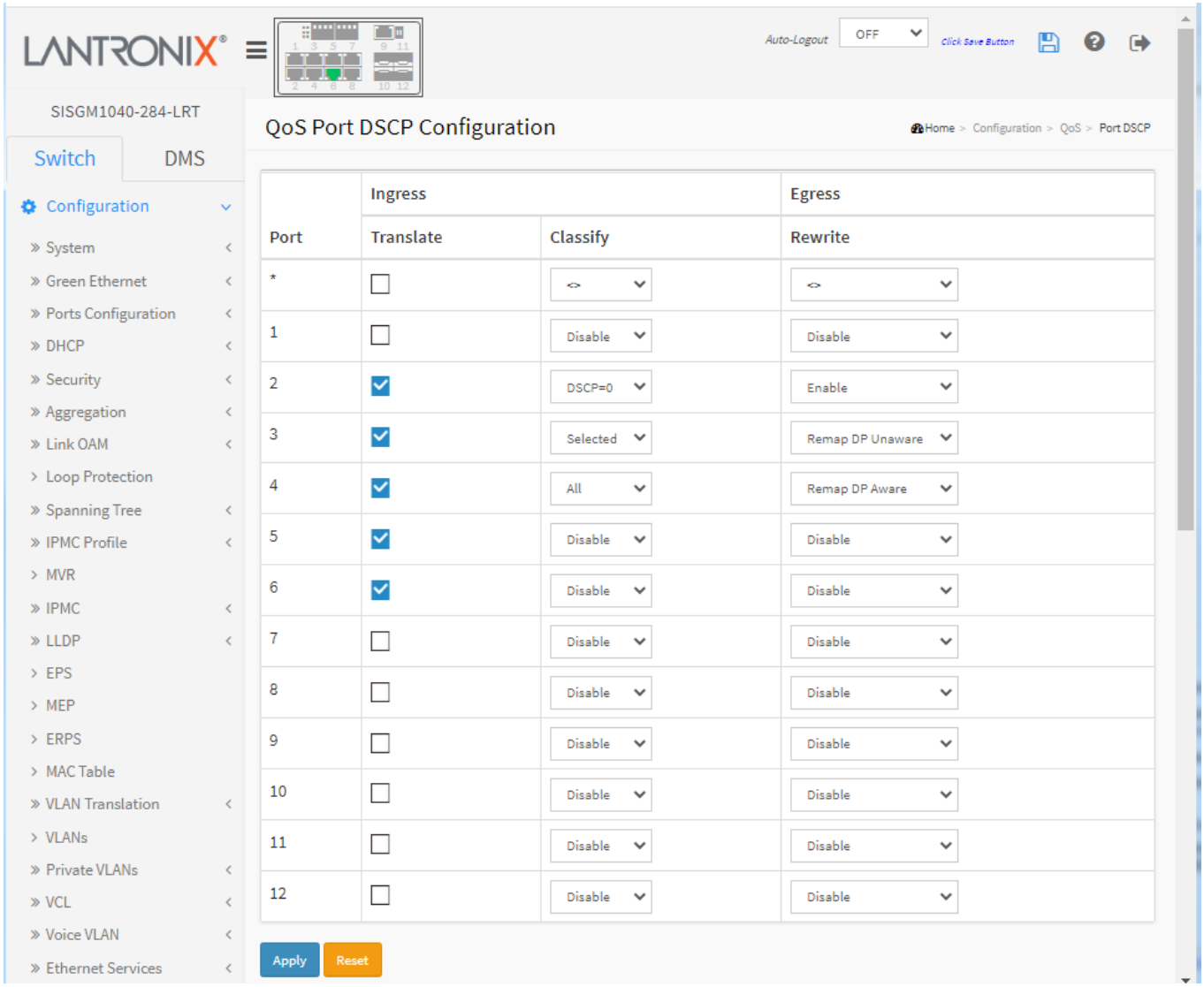
Buttons

Apply: Click to save changes.

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

Configuration > QoS > Port DSCP

This page lets you configure the basic QoS Port DSCP Configuration settings for all switch ports.

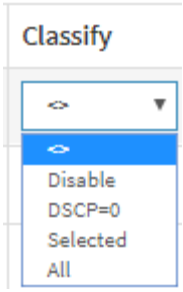


Port: The Port column shows the list of ports for which you can configure DSCP ingress and egress settings.

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

Translate: To Enable the Ingress Translation, click the checkbox.

Classify: Classification for a port have 4 different values.



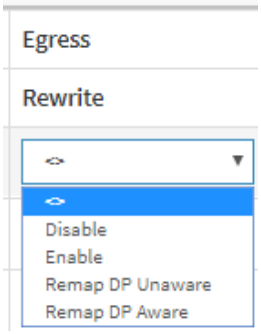
Disable: No Ingress DSCP Classification.

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

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

All: Classify all DSCP.

Egress: Port Egress Rewriting can be:



Disable: No Egress rewrite.

Enable: Rewrite enabled without remapping.

Remap DP Unaware: DSCP from analyzer is remapped and frame is remarked with remapped DSCP value. The remapped DSCP value is always taken from the 'DSCP Translation->Egress Remap DP0' table.

Remap DP Aware: DSCP from analyzer is remapped and frame is remarked with remapped DSCP value. Depending on the DP level of the frame, the remapped DSCP value is either taken from the 'DSCP Translation > Egress Remap DP0' table or from the 'DSCP Translation > Egress Remap DP1' table.

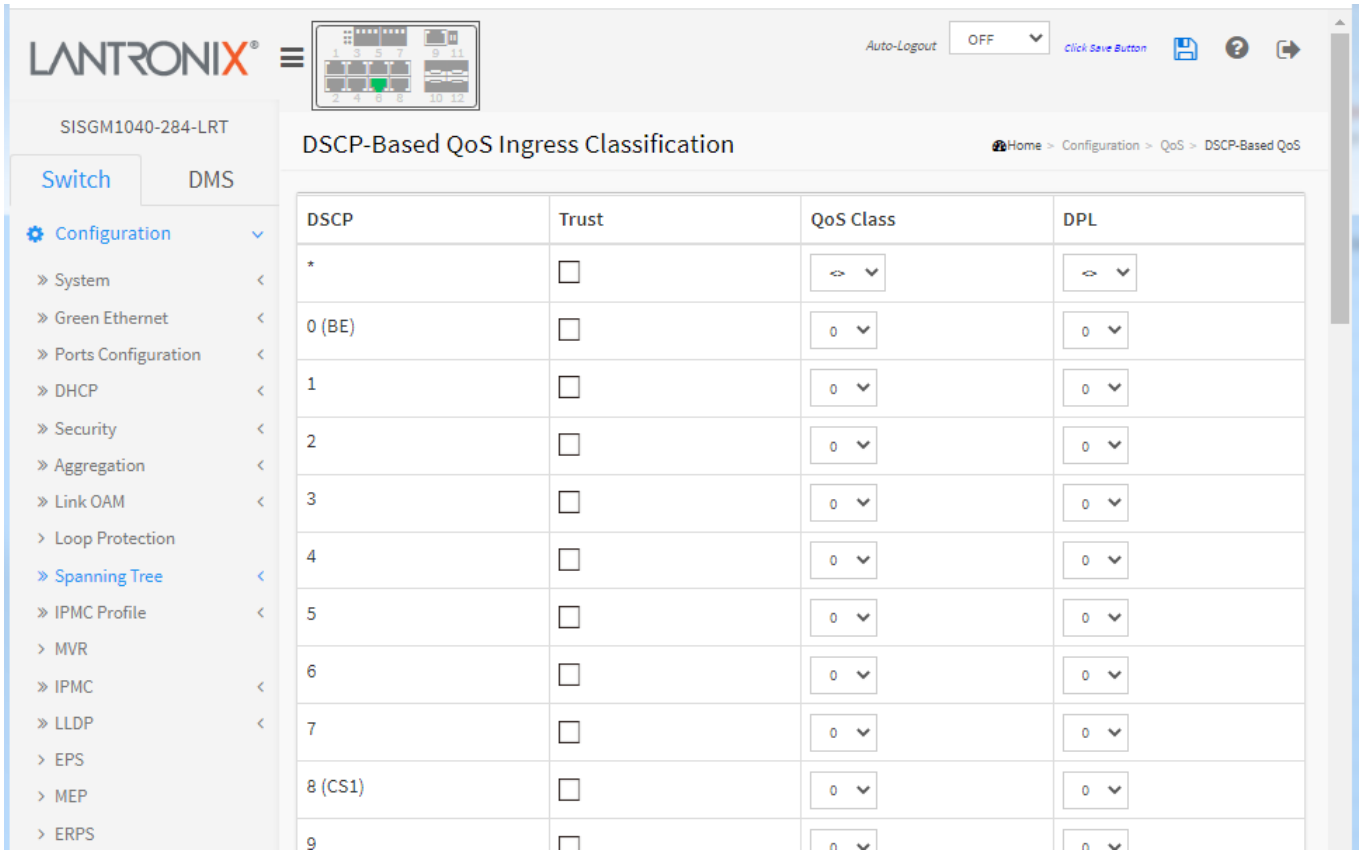
Buttons

Apply: Click to save changes.

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

Configuration > QoS > DSCP-Based QoS

This page allows you to configure the basic QoS DSCP based QoS Ingress Classification settings for all switches.



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 a non-IP frame.

QoS Class: QoS class value can be 0-7.

DPL: Drop Precedence Level (0-1).

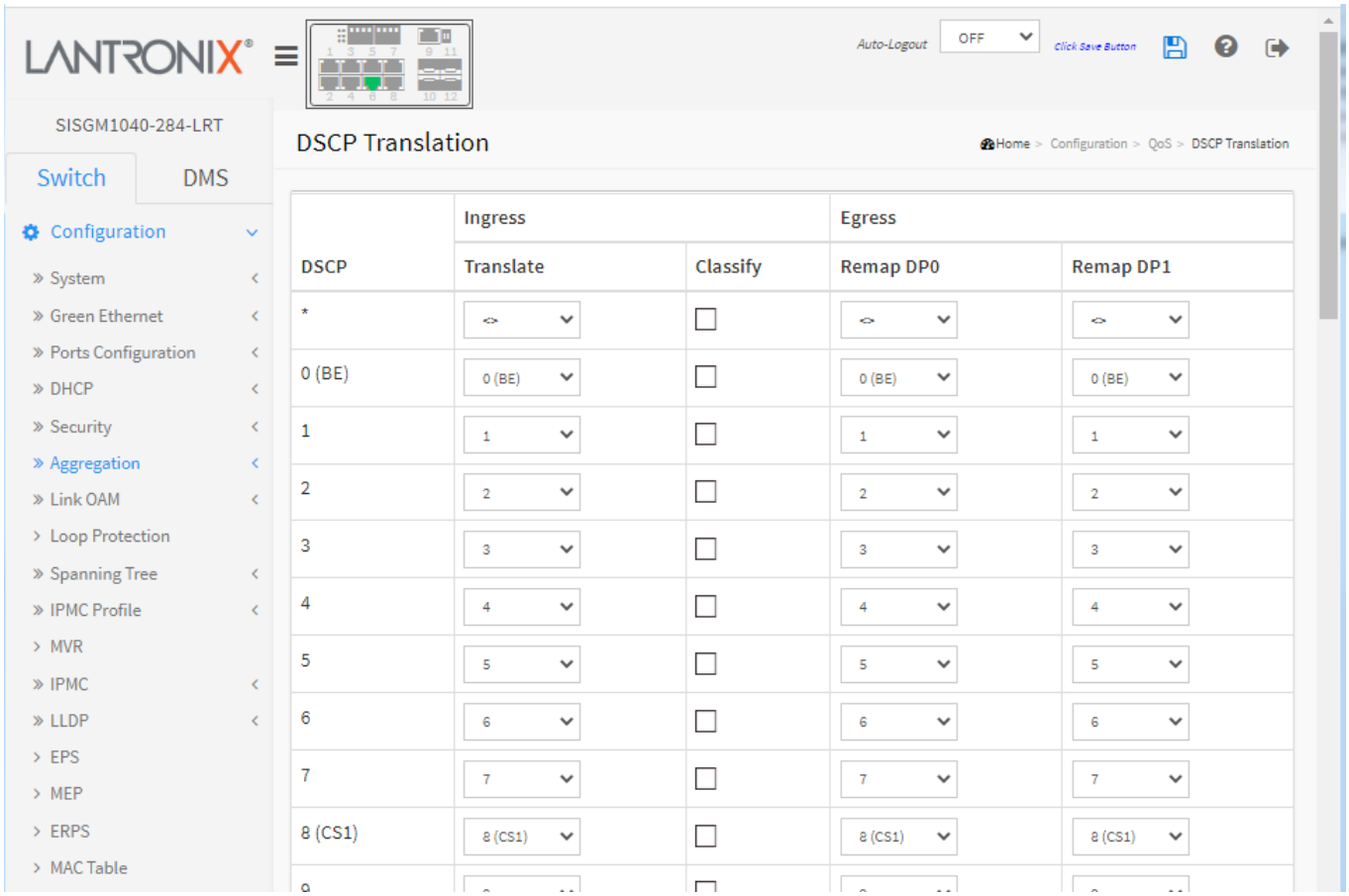
Buttons

Apply: Click to save changes.

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

Configuration > QoS > DSCP Translation

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



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: These parameters are configurable for the Egress side:

Remap DP0: Controls the remapping for frames with DP level 0. Select the DSCP value from select menu to which you want to remap. DSCP value ranges from 0 to 63.

Remap DP1: Controls the remapping for frames with DP level 1. Select the DSCP value from select menu to which you want to remap. DSCP value ranges from 0 to 63.

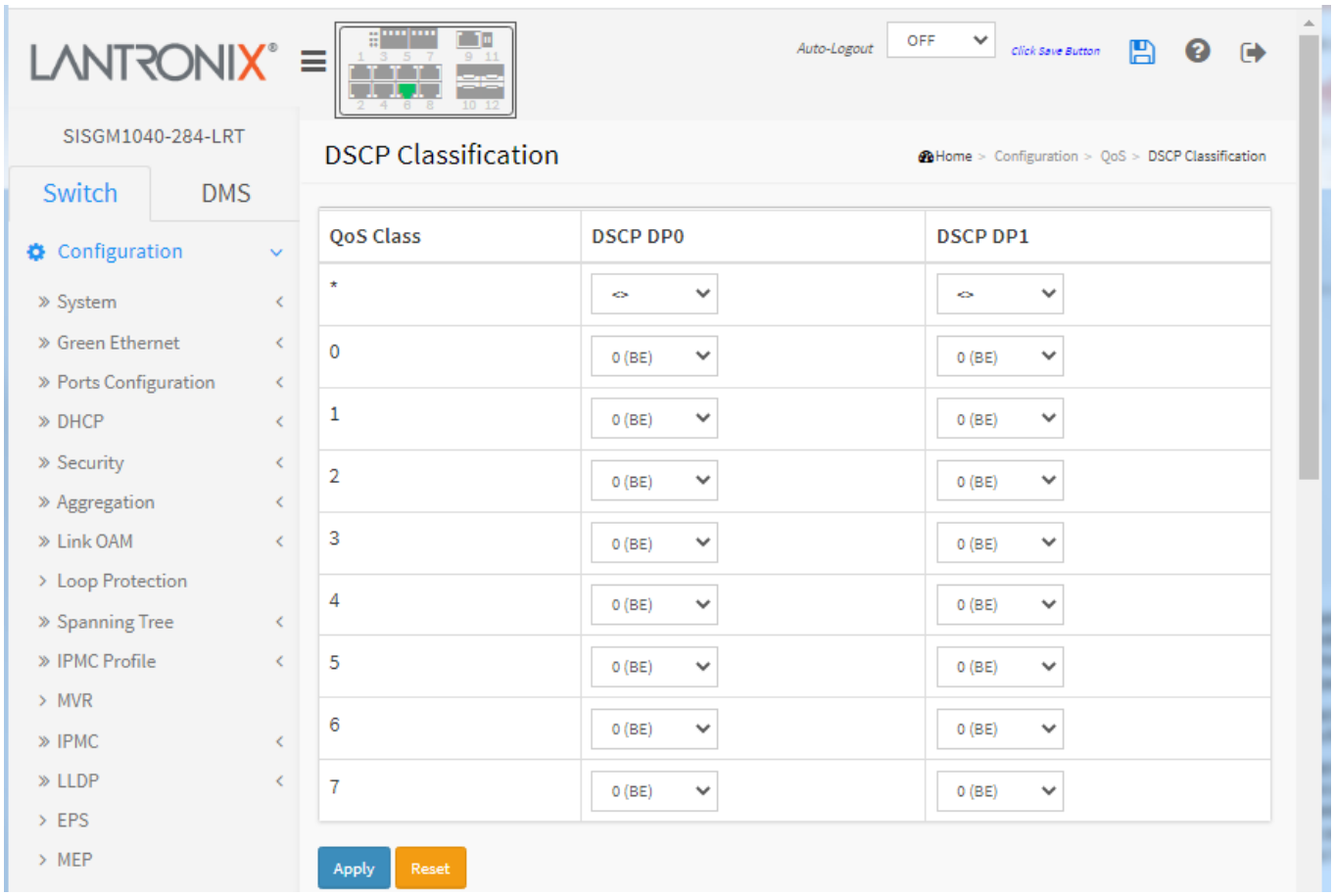
Buttons

Apply: Click to save changes.

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

Configuration > QoS > DSCP Classification

This page allows you to configure the mapping of QoS class and Drop Precedence Level to DSCP value.



QoS Class: Actual 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.

DSCP DP0: Select the classified DSCP value (0-63) for Drop Precedence Level 0. *DSCP* (Differentiated Services Code Point) is a field in the header of IP packets for packet classification purposes.

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

Buttons

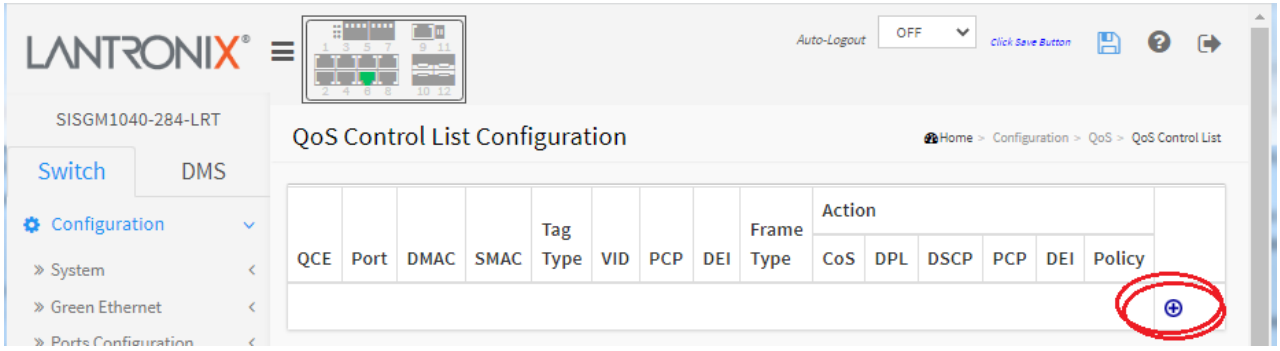
Apply: Click to save changes.

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

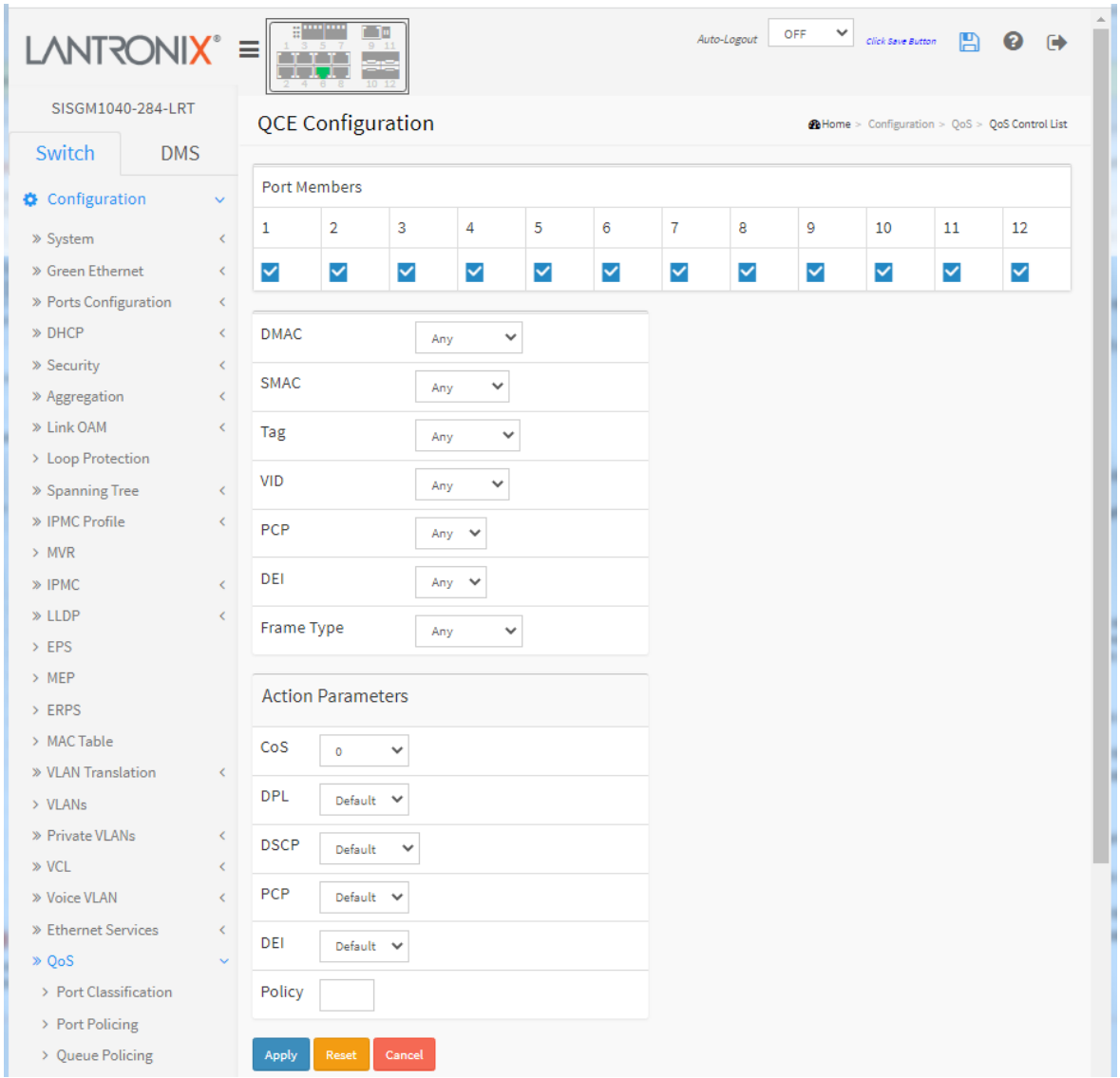
Configuration > QoS > QoS Control List

This page shows the QoS Control List (QCL) which is made up of the QCEs. Each row describes a QCE that is defined. The maximum number of QCEs is 256 on each switch.

Click on the lowest plus sign (⊕) to add a new QCE to the list.



On the “QCE Configuration” page enter the page parameters.



This page lets you create and edit one QoS Control Entry at a time. A QCE consists of several parameters. These parameters vary according to the Frame Type that you select.

Port Members: Check the checkbox button to include the port in the QCL entry. By default all ports are included.

Key Parameters

DMAC: Destination MAC address: Possible values are 'Unicast', 'Multicast', 'Broadcast' or 'Any'.

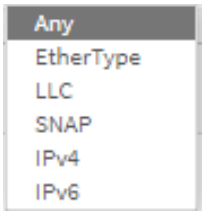
SMAC: Source MAC address: xx-xx-xx-xx-xx-xx or 'Any'. If a port is configured to match on DMAC/DIP, this field is the Destination MAC address.

Tag: Value of Tag field can be 'Untagged', 'Tagged', 'C-Tagged', 'S-Tagged' or 'Any'.

VID: Valid value of VLAN ID can be any value in the range 1-4095 or 'Any'; user can enter either a specific value or a range of VIDs.

PCP: Valid value PCP are specific (0, 1, 2, 3, 4, 5, 6, 7) or range (0-1, 2-3, 4-5, 6-7, 0-3, 4-7) or 'Any'.

DEI: Valid value of DEI can be '0', '1' or 'Any'.



Frame Type: Can have be Any, EtherType, LLC, SNAP, IPv4, or IPv6 as described below.

Any: Allow all types of frames.

EtherType: Valid Ether Type can be 0x600-0xFFFF excluding 0x800(IPv4) and 0x86DD(IPv6) or 'Any'.

LLC: parameters:

DSAP Address; Valid DSAP (Destination Service Access Point) can be 0x00 to 0xFF or 'Any'.

SSAP Address: Valid SSAP (Source Service Access Point) can vary from 0x00 to 0xFF or 'Any'.

Control: Valid Control field can be 0x00 to 0xFF or 'Any'.

SNAP: ***PID***: Valid PID (a.k.a Ether Type) can be Specific (0x0000-0xFFFF) or 'Any'.

IPv4: parameters:

Protocol: IP protocol number: (0-255, 'TCP' or 'UDP') or 'Any'.

SIP: 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. If a port is configured to match on DMAC/DIP, this field is the Destination IP address.

IP Fragment: IPv4 frame fragmented option: 'Yes', 'No' or 'Any'.

DSCP: Diffserv Code Point value (DSCP): It can be a Specific value, a Range of values, or 'Any'. DSCP values are in the range 0-63 including BE, CS1-CS7, EF or AF11-AF43.

Sport: Source TCP/UDP port:(0-65535) or 'Any', specific or port range applicable for IP protocol UDP/TCP.

Dport: Destination TCP/UDP port:(0-65535) or 'Any', specific or port range applicable for IP protocol UDP/TCP.

IPv6: parameters:

Protocol: IP protocol number: (Other 0-255, 'TCP' or 'UDP') or 'Any'.

SIP (32 LSB) : 32 LS bits of IPv6 source address in value/mask format or 'Any'. If a port is configured to match on DMAC/DIP, this field is the Destination IP address.

DSCP: Diffserv Code Point value (DSCP): It can be a specific value, range of values or 'Any'. DSCP values are in the range 0-63 including BE, CS1-CS7, EF or AF11-AF43.

Sport: Source TCP/UDP port:(0-65535) or 'Any', specific or port range applicable for IP protocol UDP/TCP.

Dport: Destination TCP/UDP port:(0-65535) or 'Any', specific or port range applicable for IP protocol UDP/TCP.

Action Parameters

CoS: Class of Service: (0-7) or 'Default'.

DP: Drop Precedence Level: (0-1) or 'Default'.

DSCP Differentiated Services Code Point: (0-63, BE, CS1-CS7, EF or AF11-AF43) or 'Default'.

PCP: Priority Code Point: (0-7) or 'Default'. Note: PCP and DEI cannot be set individually.

DEI: Drop Eligible Indicator: (0-1) or 'Default'.

Policy: ACL Policy number: (0-255) or 'Default' (empty field).

Note: 'Default' means that the default classified value is not modified by this QCE.

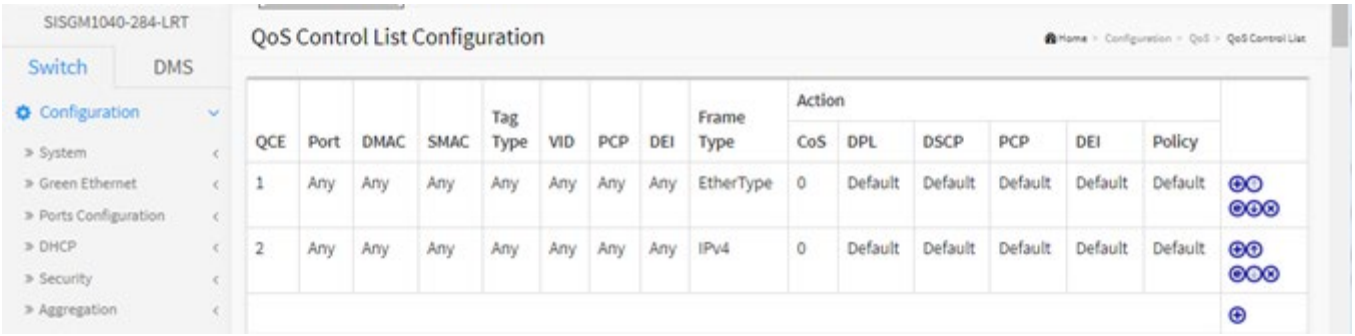
Buttons

Apply: Click to save the configuration and move to main QCL page.

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

Cancel: Return to the previous page without saving the configuration change.

Example:



Messages:

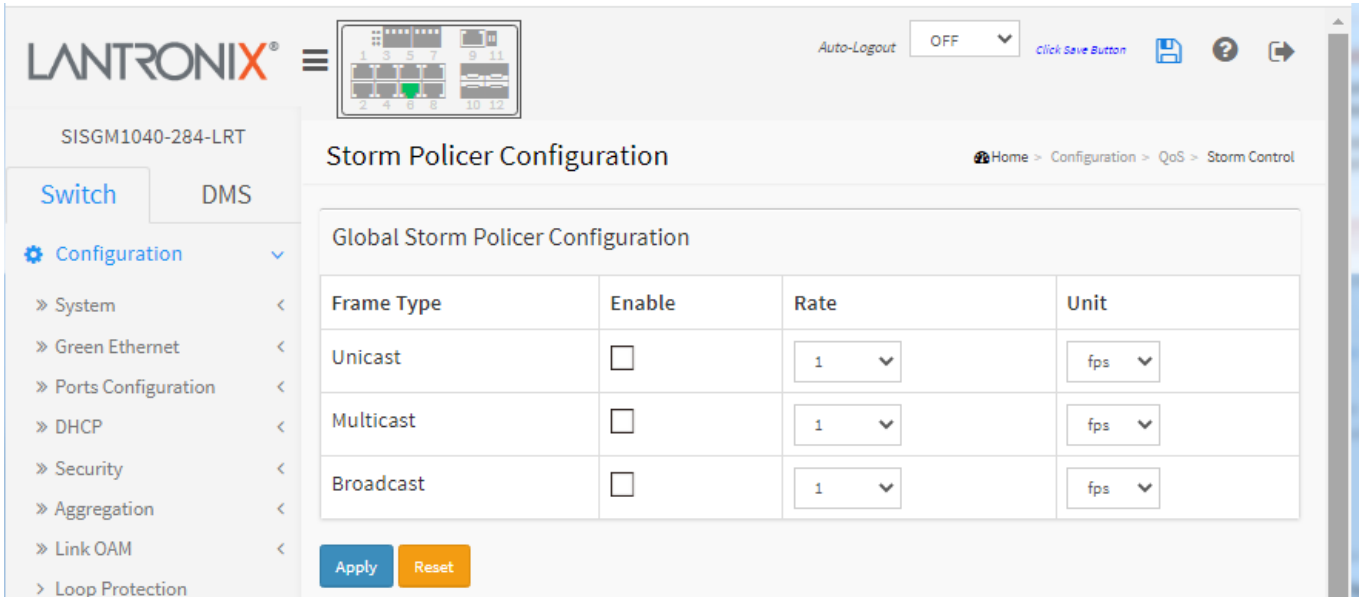
PCP and DEI cannot be set individually!

'Dport' must be an integer value between 0 and 65535

Configuration > Storm Control

Navigate to Configuration > QoS > Storm Control to display the Storm Policing webpage. This page lets you configure Global storm policers for the switch.

There is a unicast storm policer, multicast storm policer, and a broadcast storm policer. These only affect flooded frames, i.e. frames with a (VLAN ID, DMAC) pair not present in the MAC Address table.



Frame Type: The frame type for which the configuration below applies (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 1-1024000 when "Unit" is fps, and 1-1024 when "Unit" is kfps. The rate is internally rounded up to the nearest value supported by the global storm policer. Valid values are: 1, 2, 4, 8, 16, 32, 64, 128, 256, 512, 1K, 2K, 4K, 8K, 16k, 32k, 64k, 128k, 256K, 512K or 1024K.

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

Buttons

Apply: Click to save changes.

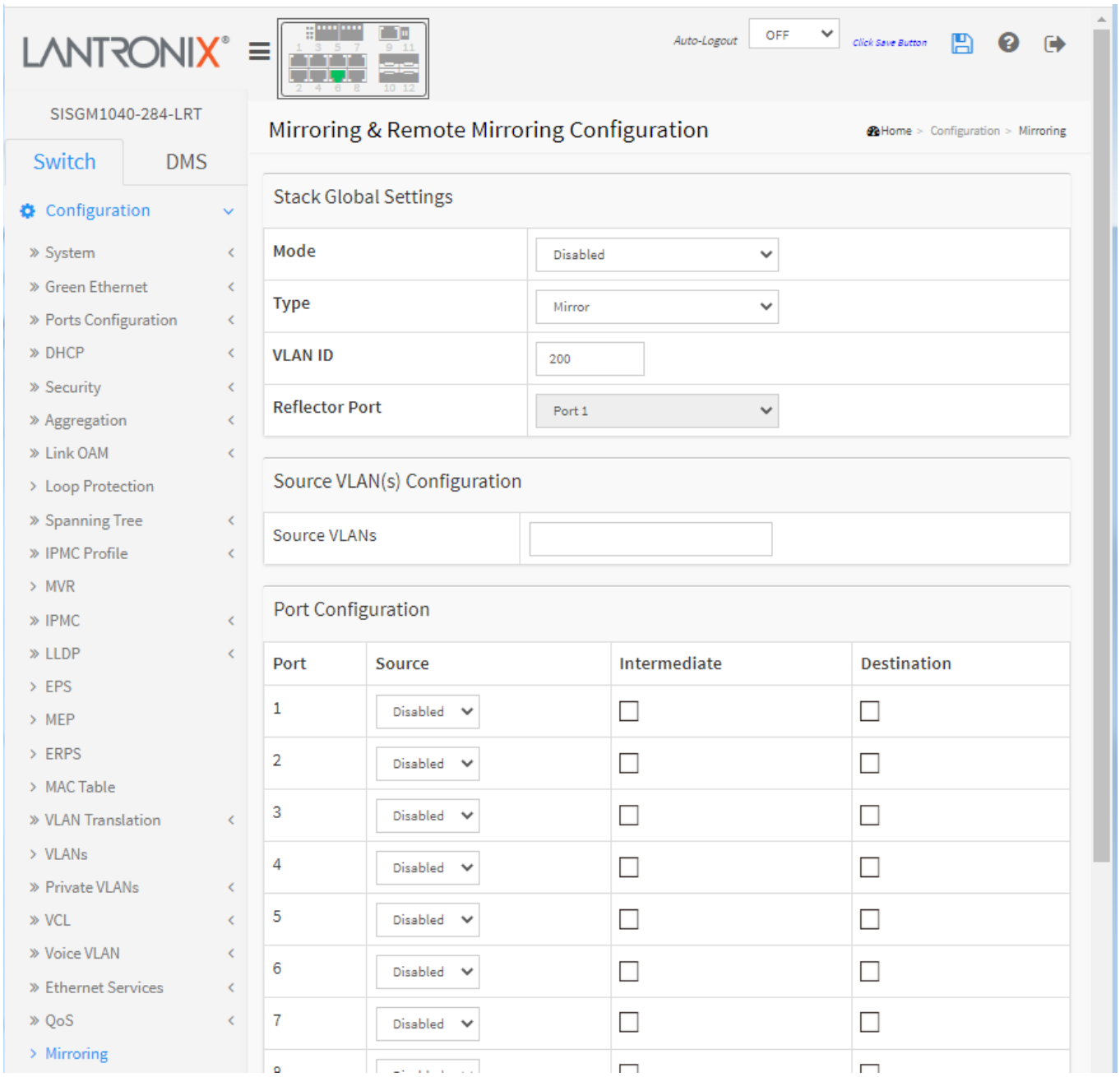
Reset: Click to undo any changes made locally and revert to previously saved values.

Configuration > Mirroring

Mirroring is a feature for use with a switched port analyzer. The administrator can use the Mirroring to debug network problems. The selected traffic can be mirrored or copied on a destination port where a network analyzer can be attached to analyze the network traffic.

Remote Mirroring is an extended function of Mirroring. It can extend the destination port in another switch. The administrator can then analyze the network traffic on other switches.

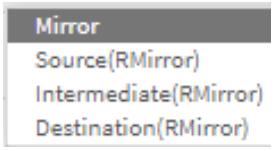
To get the tagged mirrored traffic, you must set VLAN egress tagging as "Tag All" on the reflector port. Otherwise, to get untagged mirrored traffic, you must set VLAN egress tagging as "Untag ALL" on the reflector port.



Stack Global Settings

Mode: Enable or Disable the mirror or Remote Mirroring function. The default is Disabled.

Type: Select switch type:



Mirror: The switch is running on mirror mode. The source port(s) and destination port are located 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. The default VLAN ID is 200.

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 the Remote Mirroring is disabled.

If you shut down a port, it cannot be a candidate for reflector port.

If you shut down the port which is a reflector port, the remote mirror function cannot work.

Note 1: The reflector port needs to select only on Source switch type.

Note 2: The reflector port needs to disable MAC Table learning and STP.

Note 3: The reflector port only supports on pure copper ports.

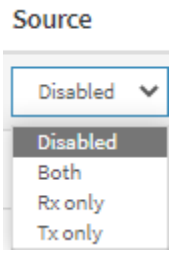
Source VLAN(s) Configuration: The switch can support VLAN-based Mirroring. To monitor some VLANs on the switch, you can set the selected VLANs on this field.

Note 1: The Mirroring session can have either ports or VLANs as sources, but not both.

Port Configuration: The following table is used for Remote Mirroring port role selections.

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 (default).

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 another switch. Note: The intermediate port needs to have MAC Table learning disabled.

Destination: Select destination port. This checkbox is designed for mirror or Remote Mirroring. The destination port is a switched port that you receive a copy of traffic from the source port. Note1: In mirror mode, the device only supports one destination port. Note2: The destination port needs to have MAC Table learning disabled.

Configuration Guideline for All Features: When the switch is running on Remote Mirroring mode, the administrator also needs to check whether or not other features are enabled or disabled. For example, the administrator is not disabled the MSTP on reflector port. All monitor traffic will be blocked on reflector port.

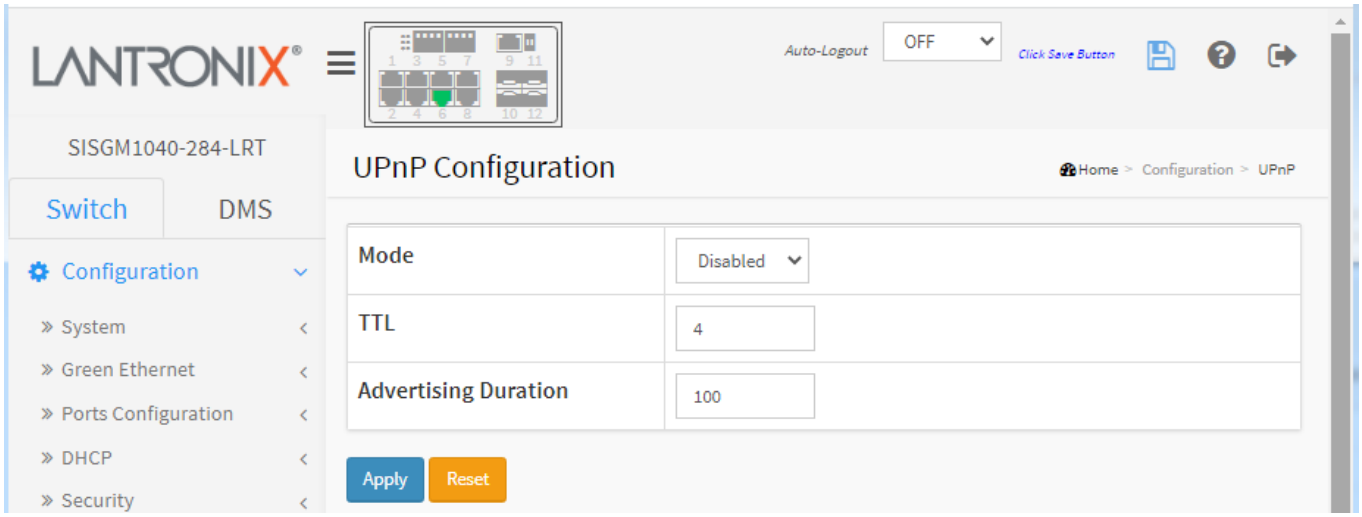
All recommended settings are described below.

	Impact	Source port	Reflector port	Intermediate port	Destination port	Remote Mirroring VLAN
arp_inspection	High		* disabled	* disabled		
acl	Critical		* disabled	* disabled	* disabled	
dhcp_relay	High		* disabled	* disabled		
dhcp_snooping	High		* disabled	* disabled		
ip_source_guard	Critical		* disabled	* disabled	* disabled	
ipmc/igmpsnp	Critical					un-conflict
ipmc/mldsnp	Critical					un-conflict
lacp	Low				o disabled	
lldp	Low				o disabled	
mac learning	Critical		* disabled	* disabled	* disabled	
mstp	Critical		* disabled		o disabled	
mvr	Critical					un-conflict
nas	Critical		* authorized	* authorized	* authorized	
psec	Critical		* disabled	* disabled	* disabled	
qos	Critical		* unlimited	* unlimited	* unlimited	
upnp	Low				o disabled	
mac-based vlan	Critical		* disabled	* disabled		
protocol-based vlan	Critical		* disabled	* disabled		
vlan_translation	Critical		* disabled	* disabled	* disabled	
voice_vlan	Critical		* disabled	* disabled		
mrp	Low				o disabled	
mvrp	Low				o disabled	
Note:						
* -- must						
o -- optional						
Impact: Critical/High/Low						
Critical	5 packets -> 0 packet					
High	5 packets -> 4 packets					
Low	5 packets -> 6 packets					

Configuration > UPnP

Configure UPnP (Universal Plug and Play) on this page.

The goals of UPnP are to allow devices to connect seamlessly and to simplify the implementation of networks in the home (data sharing, communications, and entertainment) and in corporate environments for simplified installation of computer components. The Universal Plug and Play Forum was formed to standardize discovery and control of networked devices. See the Open Connectivity Foundation webpage.



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

Enabled: Enable UPnP mode operation.

Disabled: Disable UPnP mode operation (default).

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

TTL: The TTL value is used by UPnP to send SSDP advertisement messages. Valid values are in the range 1 to 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 be done at less than one-half of the advertising duration. In the implementation, the switch sends SSDP messages periodically at the interval one-half of the advertising duration minus 30 seconds. Valid values are in the range 66 to 86400.

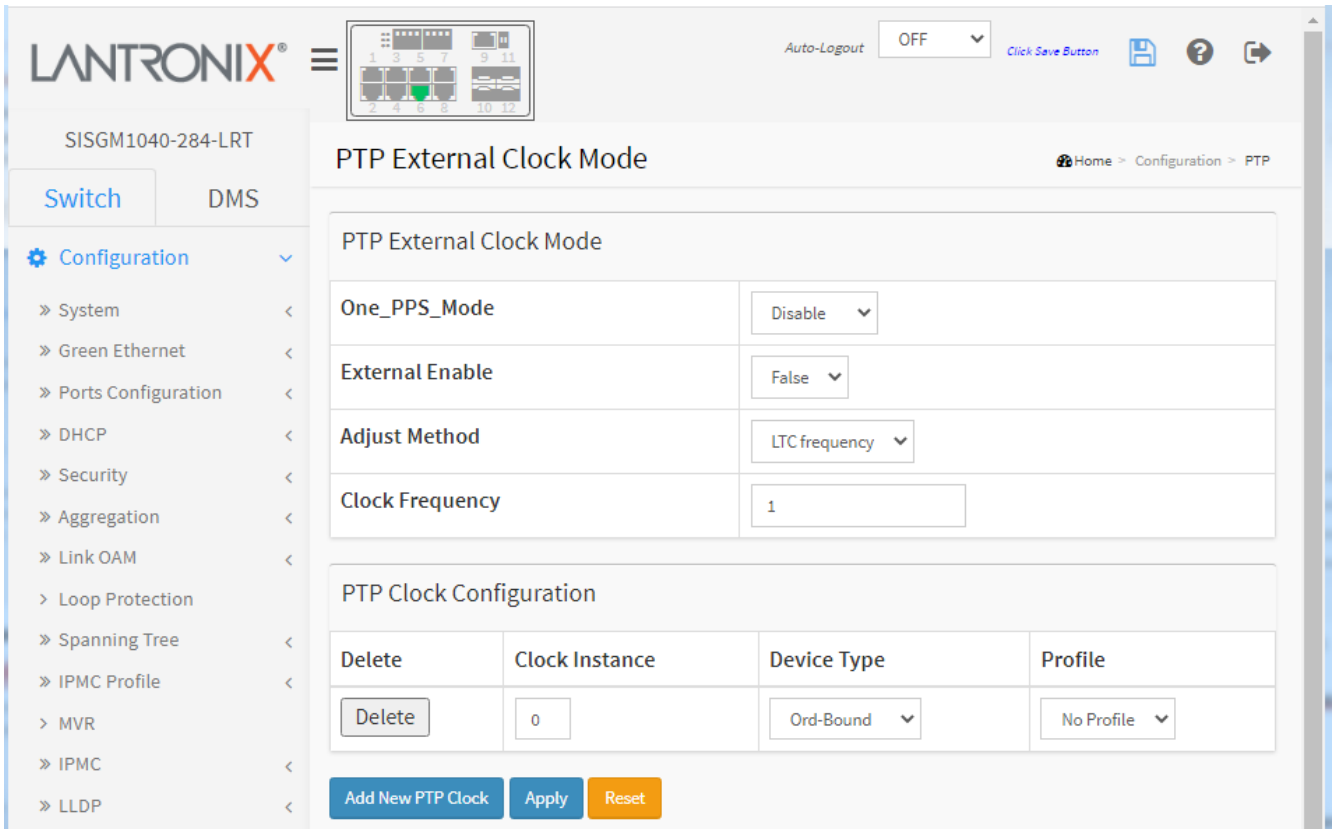
Buttons

Apply: Click to save changes.

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

Configuration > PTP

This page lets you view and configure current PTP clock parameters. PTP (Precision Time Protocol) is a network protocol for synchronizing the clocks of computer systems. The initial PTP page is shown with “No Clock Instances Present” displayed. Click the **Add New PTP Clock** button to display the instances configuration table:



PTP External Clock Configuration

One_PPS_Mode: This Selection box will allow you to select the One_pps_mode configuration. These values are possible:

Output : Enable the 1 pps clock output

Input : Enable the 1 pps clock input

Disable : Disable the 1 pps clock in/out-put

External Enable: This Selection box will allow you to configure the External Clock output. The following values are possible:

True : Enable the external clock output

False : Disable the external clock output

Adjust Method: This Selection box will allow you to configure the Frequency adjustment configuration.

LTC frequency : Select Local Time Counter (LTC) frequency control.

SyncE-DPLL : Select SyncE DPLL frequency control, if allowed by SyncE.

Oscillator : Select an oscillator independent of SyncE for frequency control, if supported by the HW.

LTC phase : Select Local Time Counter (LTC) phase control (assumes that the frequency is locked by means of SyncE).

Clock Frequency: This will allow to set the Clock Frequency. The possible range of values are 1 - 25000000 (1 - 25MHz).

PTP Clock Configuration

Delete: Check this box and click the Apply button to delete the clock instance.

Clock Instance: The PTP Clock instance number for this line (e.g., 0-3).

Device Type: The PTP Clock device type (e.g., Master Only, Slave only, P2pTransp, Ord-Bound).

Profile: The PTP Clock device profile selected (e.g., 1588, G8265.1, G8275.1, No Profile).

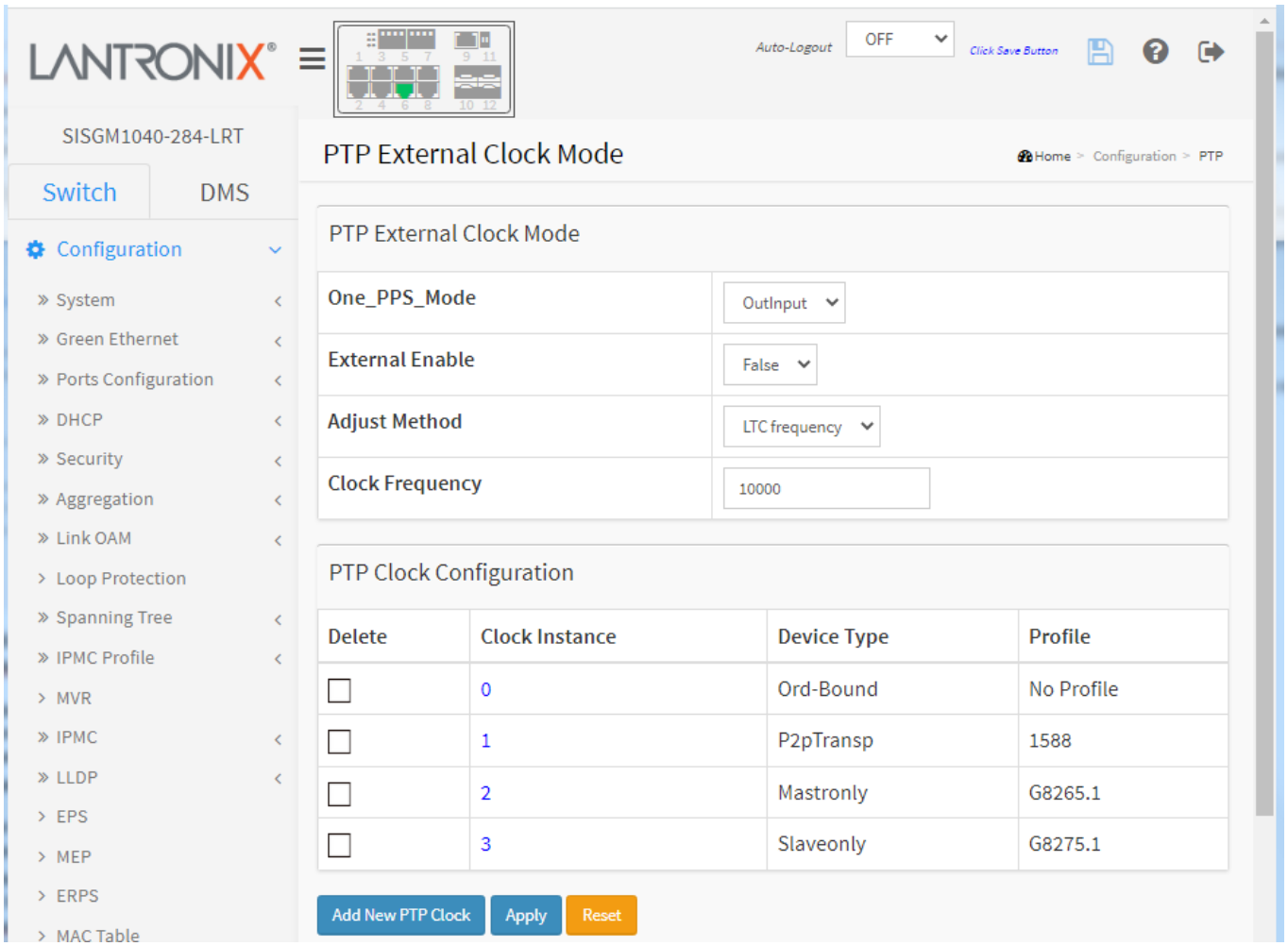
Buttons:

Add New PTP Clock: Click to add and configure a new PTP Clock instance.

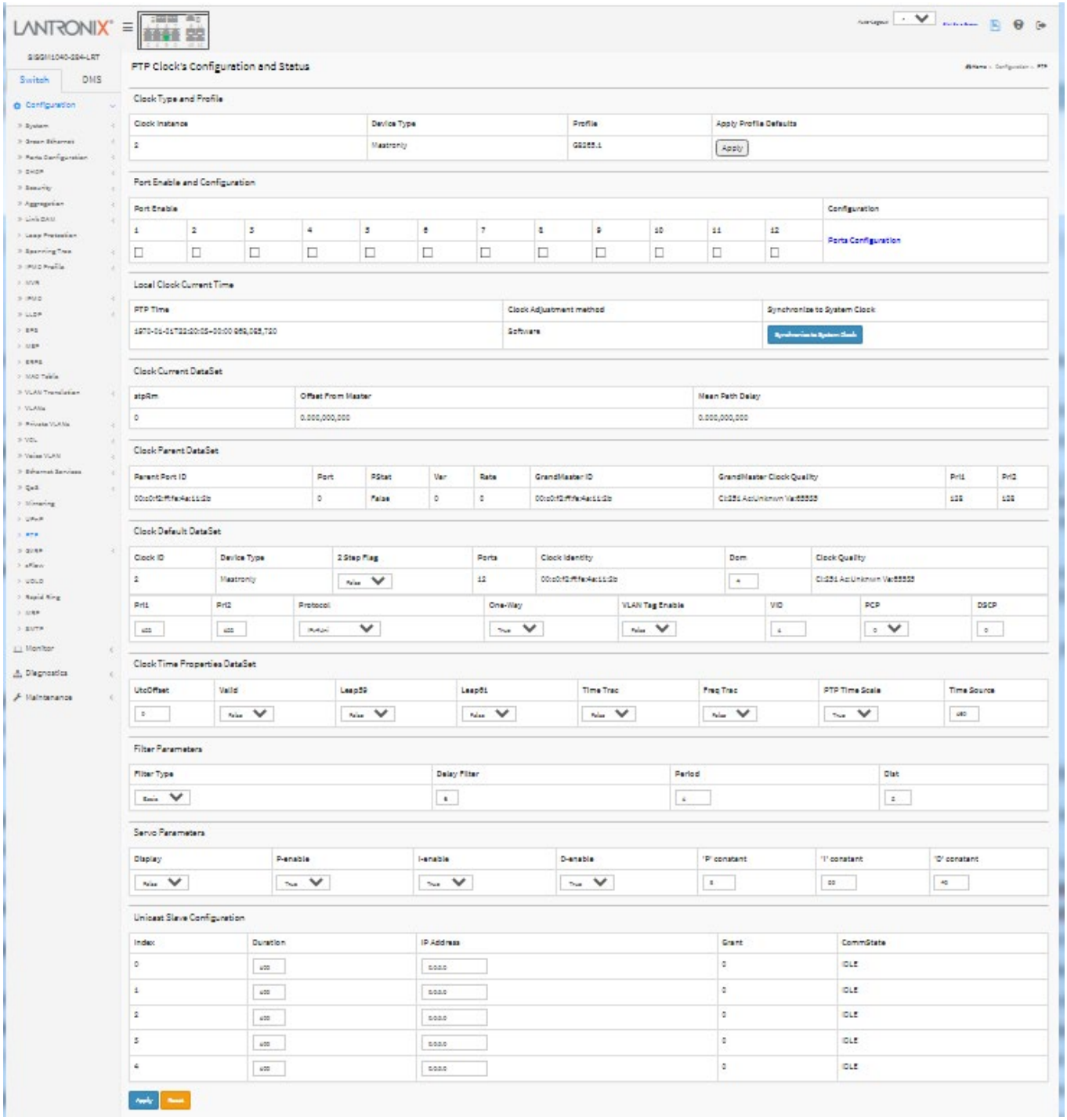
Apply: Click to save changes.

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

Example: Four PTP Clock instances created (Clock Instances 0-3):



Click a linked Clock Instance number (e.g., 0 above) to display its “PTP Clock's Configuration and Status” page:



This page lets you view and configure current PTP clock settings.

Clock Type and Profile

Clock Instance: The instance number selected (e.g., 0).

Device Type: The device type selected (e.g., Mastronly or Ord-Bound).

Profile: The Profile number (e.g., 1588 or No Profile).

Apply Profile Defaults: The Apply button; click to make these parameter selections the defaults.

Port Enable and Configuration

Port Enable: Check the port number boxes to enable PTP.

Configuration: Click the linked "Ports Configuration" text to display the "PTP Clock's Port Data Set Configuration" page.

Local Clock Current Time

PTP Time: The local clock current time in the format *1970-01-01T00:29:41+00:00 487,362,920*.

Clock Adjustment method: The method of clock adjustment (e.g., Internal Timer)

Synchronize to System Clock: Button to synchronize this clock instance to the System Clock.

Clock Current Data Set: The clock current data set is defined in the IEEE 1588 Standard. The current data set is dynamic.

stpRm: Steps Removed : It is the number of PTP clocks traversed from the grandmaster to the local slave clock.

Offset from Master: Time difference between the master clock and the local slave clock, measured in ns.

Mean Path Delay: The mean propagation time for the link between the master and the local slave.

Clock Parent Data Set: The clock parent data set is defined in the IEEE 1588 standard. The parent data set is dynamic.

Parent Port Identity: Clock identity for the parent clock, if the local clock is not a slave, the value is the clocks own id.

Port: Port Id for the parent master port

PStat: Parents Stats (always false).

Var: It is observed parent offset scaled log variance

Change Rate: Observed Parent Clock Phase Change Rate. i.e. the slave clocks rate offset compared to the master. (unit = ns per s).

Grand Master Identity: Clock identity for the grand master clock, if the local clock is not a slave, the value is the clocks own id.

Grand Master Clock Quality: The clock quality announced by the grand master (See description of Clock Default DataSet:Clock Quality)

Pri1: Clock priority 1 announced by the grand master

Pri2: Clock priority 2 announced by the grand master.

Clock Time Properties Data Set: The clock time properties data set is defined in the IEEE 1588 Standard. The data set is both configurable and dynamic, i.e. the parameters can be configured for a grandmaster. In a slave clock the parameters are overwritten by the grandmasters timing properties. The parameters are not used in the current PTP implementation.

Valid values for the Time Source parameter are:

16 (0x10) ATOMIC_CLOCK

32 (0x20) GPS

48 (0x30) TERRESTRIAL_RADIO

64 (0x40) PTP

80 (0x50) NTP

96 (0x60) HAND_SET

144 (0x90) OTHER

160 (0xA0) INTERNAL_OSCILLATOR

Servo Parameters: The default clock servo uses a PID regulator to calculate the current clock rate. i.e.

clockAdjustment =
OffsetFromMaster/ P constant +
Integral(OffsetFromMaster)/ I constant +
Differential OffsetFromMaster)/ D constant

Display: If true then Offset From Master, MeanPathDelay and clockAdjustment are logged on the debug terminal.

P-enable: If true the P part of the algorithm is included

I-Enable: If true the I part of the algorithm is included

D-enable: If true the D part of the algorithm is included

'P' constant: [1..1000] see above

'I' constant: [1..10000] see above

'D' constant: [1..10000] see above

Unicast Slave Configuration: When operating in IPv4 Unicast mode, the slave is configured up to 5 master IP addresses. The slave then requests Announce messages from all the configured masters. The slave uses the BMC algorithm to select one as master clock, the slave then request Sync messages from the selected master.

Duration: The number of seconds a master is requested to send Announce/Sync messages. The request is repeated from the slave each Duration/4 seconds.

IP Address: IPv4 Address of the Master clock

Grant: The granted repetition period for the sync message

CommState: The state of the communication with the master, possible values are:

IDLE : The entry is not in use.

INIT : Announce is sent to the master (Waiting for a response).

CONN : The master has responded.

SELL : The assigned master is selected as current master.

SYNC : The master is sending Sync messages.

Buttons

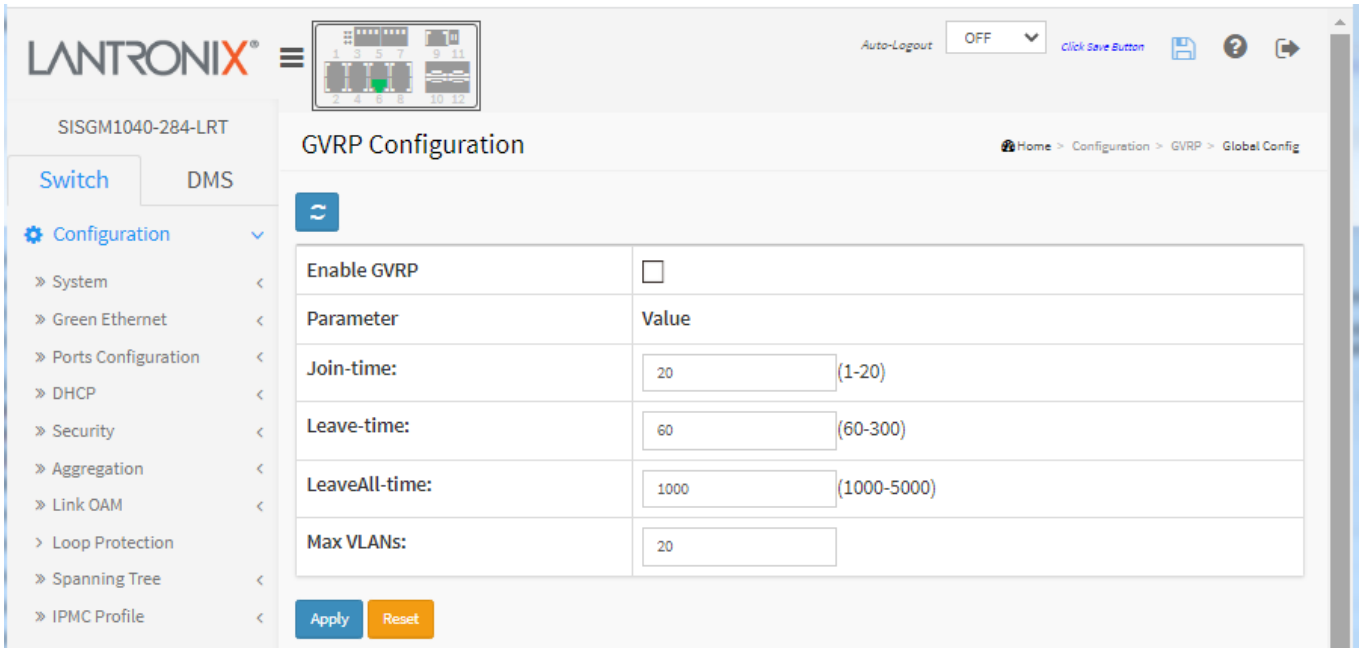
Apply: Click to save the page immediately.

Reset: Click to reset the page immediately.

Configuration > GVRP > Global Config

This page allows you to configure the global GVRP parameters commonly applied to all GVRP enabled ports.

GVRP (GARP VLAN Registration Protocol) is a protocol for dynamically registering VLANs on ports, as specified in IEEE 802.1Q-2005, clause 11. GVRP is an example of the use of GARP, hence the G in GVRP.



Enable GVRP globally: The GVRP feature is globally enabled by setting the check mark in the checkbox named Enable GVRP and pressing the Apply button.

GVRP protocol timers:

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

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

LeaveAll-time is a value in the range of 1000-5000cs, i.e. in units of one hundredth of a second. The default is 1000cs.

Max VLANs: When GVRP is enabled, a maximum number of VLANs supported by GVRP is specified. The valid range is 1-4094 VLANs. The default is 20 VLANs max. This number can only be changed when GVRP is turned off.

Buttons

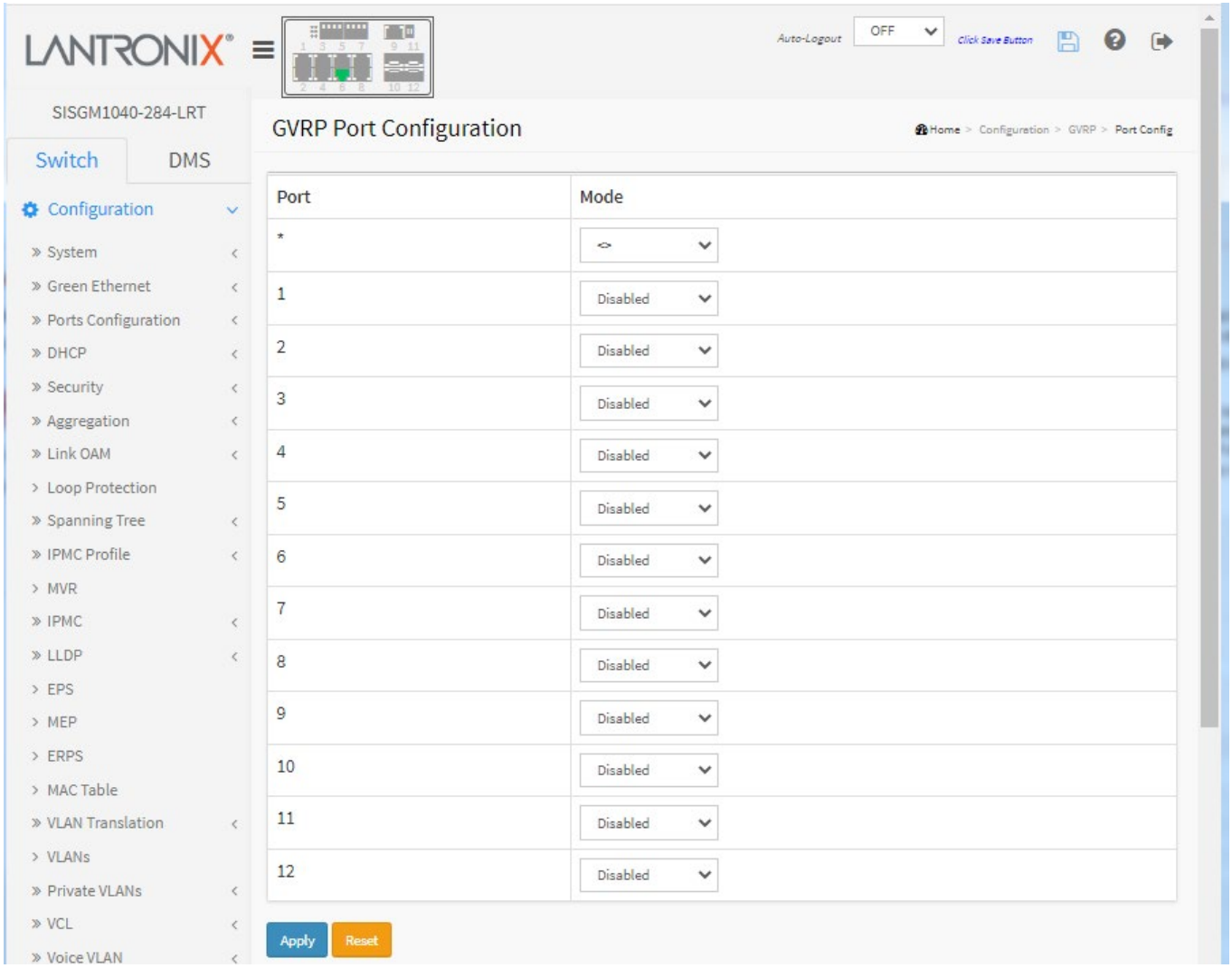
Apply: Click to save the page immediately.

Reset: Click to reset the page immediately.

Configuration > GVRP > Port Config

This page allows you to enable or disable a port for GVRP operation.

This configuration can be performed either before or after GVRP is configured globally - the protocol operation will be the same.



Port: The logical port that is to be configured.

Mode: Mode can be either 'Disabled' or 'GVRP enabled'. These values turn the GVRP feature off or on respectively for the port in question.

Buttons

Apply: Click to save the page immediately.

Reset: Click to reset the page immediately.

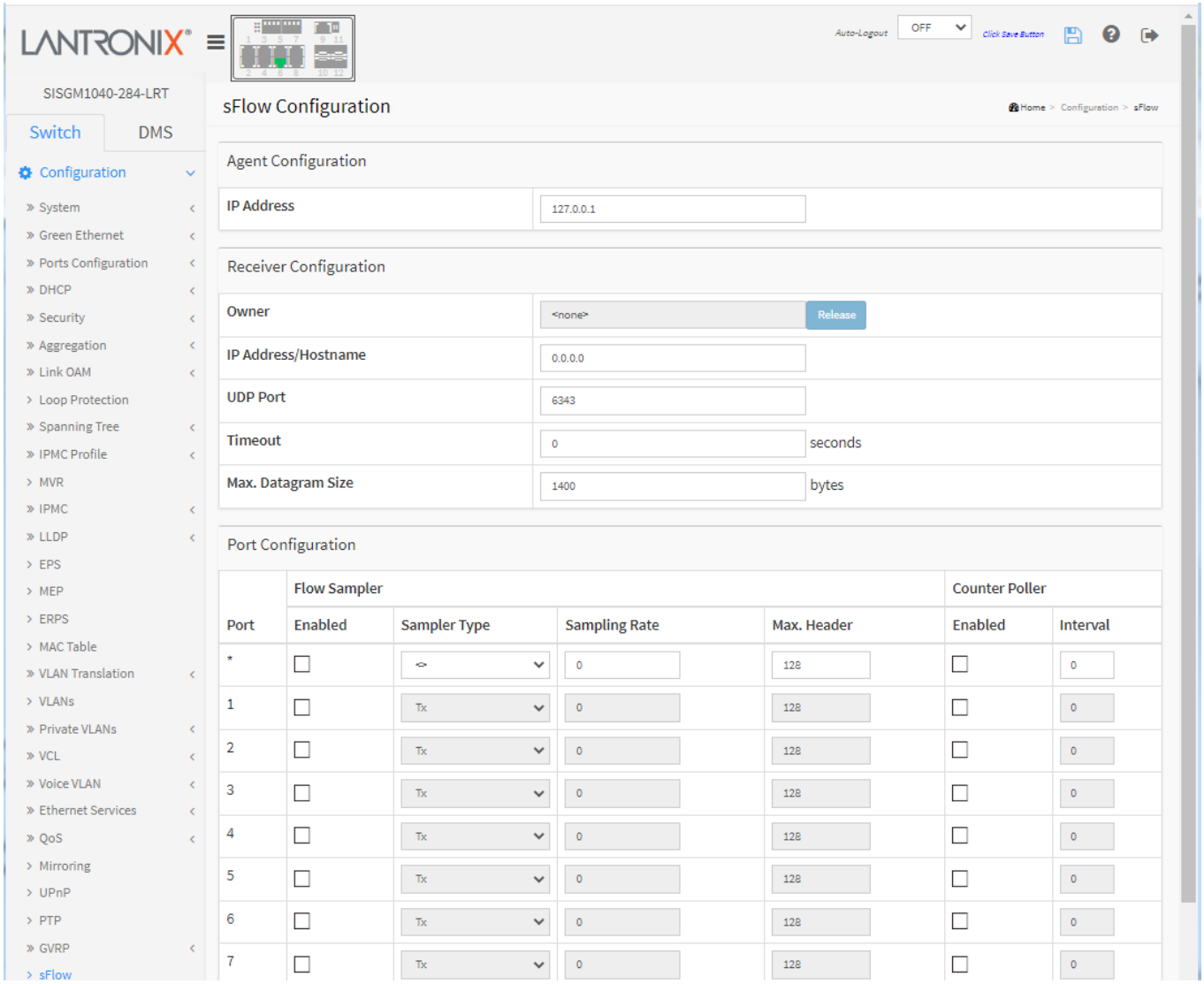
Configuration > sFlow

This page allows for configuring sFlow. The configuration is divided into two parts: configuration of the sFlow receiver (a.k.a. sFlow collector) and configuration of per-port flow and counter samplers.

sFlow configuration is not persisted to non-volatile memory, which means that a reboot will disable sFlow sampling.

sFlow is an industry standard technology for monitoring switched networks through random sampling of packets on switch ports and time-based sampling of port counters. The sampled packets and counters (referred to as flow samples and counter samples, respectively) are sent as sFlow UDP datagrams to a central network traffic monitoring server. This central server is called an sFlow receiver or sFlow collector.

Additional information can be found at http://sflow.org.



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 button is disabled if sFlow is currently unclaimed. If configured through SNMP, the release must be confirmed (a confirmation request will appear).

IP Address/Hostname: The IP address or hostname of the sFlow receiver. Both IPv4 and IPv6 addresses are supported.

UDP Port: The UDP port on which the sFlow receiver listens to sFlow datagrams. If set to 0 (zero), the default port (6343) is used.

Timeout: The number of seconds remaining before sampling stops and the current sFlow owner is released. While active, the current time left can be updated with a click on the Refresh button. If locally managed, the timeout can be changed on the fly without affecting any other settings. Valid range is 0 to 2147483647 seconds.

Max. Datagram Size: The maximum number of data bytes that can be sent in a single sample datagram. This should be set to a value that avoids fragmentation of the sFlow datagrams. Valid range is 200 to 1468 bytes with default being 1400 bytes.

Port Configuration

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

Flow Sampler Enabled: Enables/disables flow sampling on this port.

Flow Sampler Sampling Rate: The statistical sampling rate for packet sampling. Set to N to sample on average 1/Nth of the packets transmitted/received on the port. Not all sampling rates are achievable. If an unsupported sampling rate is requested, the switch will automatically adjust it to the closest achievable. This will be reported back in this field. Valid range is 1 to 4294967295.

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. Valid range is 1 to 3600 seconds.

Buttons

Release: allows for releasing the current owner and disable sFlow sampling. The button is disabled if sFlow is currently unclaimed. If configured through SNMP, the release must be confirmed (a confirmation request will appear).

Refresh: Click to refresh the page. Note that unsaved changes will be lost.

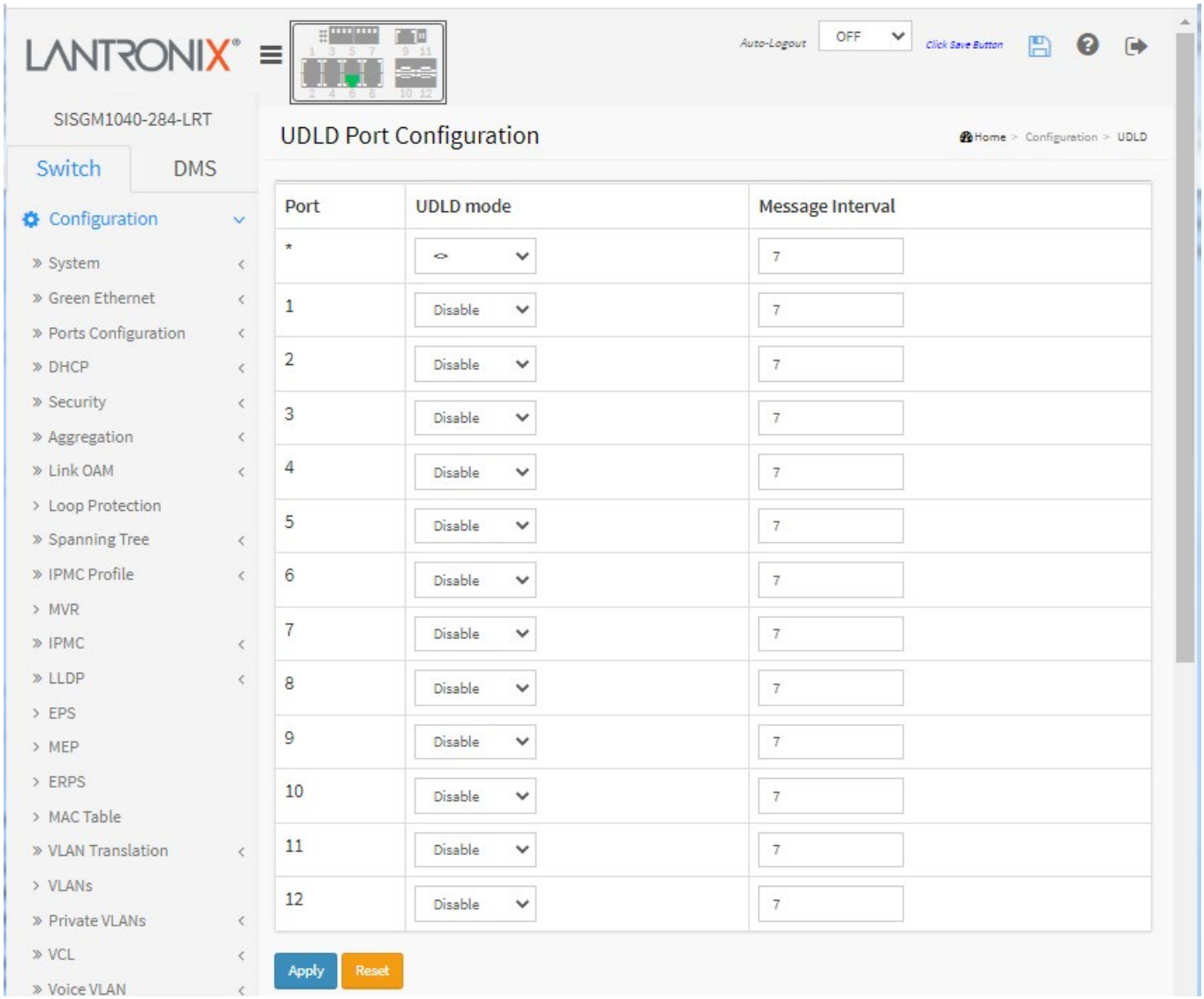
Apply: Click to save changes. Note that sFlow configuration is not persisted to non-volatile memory.

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

Configuration > UDLD

This page lets you view and configure UDLD parameters.

UDLD (Uni Directional Link Detection) monitors the physical configuration of the links between devices and ports that support UDLD. It detects the existence of unidirectional links. Its functionality is to provide mechanisms useful for detecting one way connections before they create a loop or other protocol malfunction. IETF RFC 5171 specifies a way at data link layer to detect Uni directional link.



Port: Port number of the switch.

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

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

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

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

Message Interval: Sets 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 from 7 to 90 seconds(Default value is 7 seconds)(Currently default time interval is supported, due to lack of detailed information in IETF RFC 5171).

Buttons

Release: allows for releasing the current owner and disable sFlow sampling. The button is disabled if sFlow is currently unclaimed. If configured through SNMP, the release must be confirmed (a confirmation request will appear).

Refresh: Click to refresh the page. Note that unsaved changes will be lost.

Apply: Click to save changes. Note that sFlow configuration is not persisted to non-volatile memory.

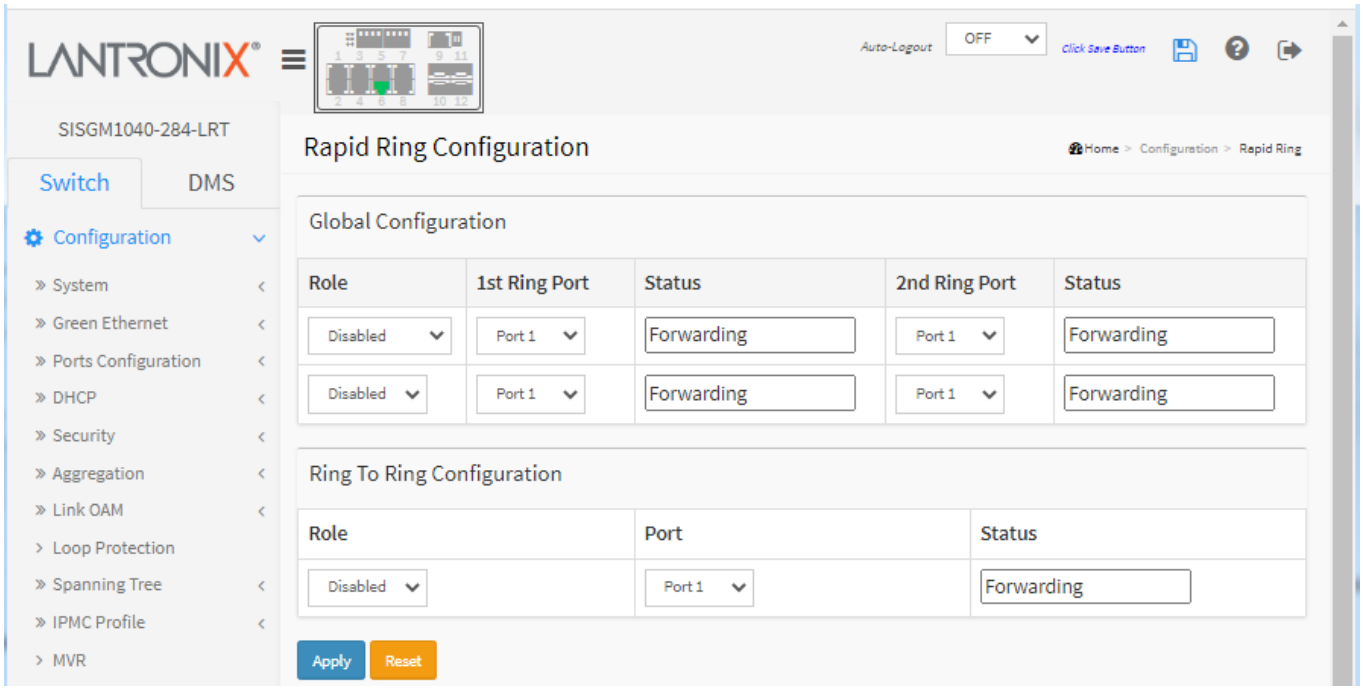
Reset: Click to undo any changes made locally and revert to previously saved values.

Configuration > Rapid Ring Configuration

This page lets you view and configure current Rapid Ring parameters. **Note**: STP must be disabled (at Configuration > Spanning Tree > CIST Port) to enable and configure Rapid Ring. See Appendix B - Rapid Ring on page 417 for more information on Rings support.

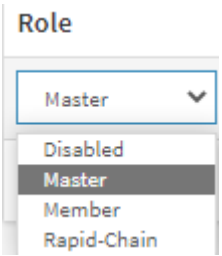
To configure Rapid Ring via the web UI:

1. Click Configuration, Rapid Ring.
2. Specify the Roles, Ports, and Status.
3. Click Apply.



Parameter descriptions:

Global Configuration



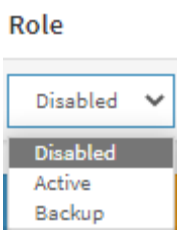
Role : Select a role value.

Disabled: Rapid Ring configuration is disabled globally.
Master: Sets the role to ring master.
Member: Sets the role to ring member.
Rapid-Chain: Sets the role to failover.

Port : Select the switch port number of the port. The ports should not be the same.

Status : Displays the current Rapid Ring status of the port (Forwarding, Discarding, …).

Ring To Ring Configuration



Role : Select a role value.

Disabled: Rapid Ring configuration is disabled for ring-to-ring.
Active: Sets the role to active ring member.
Backup: Sets the role to backup ring member.

Port : Select the switch port number of the port. The ports should not be the same in Global Configuration.

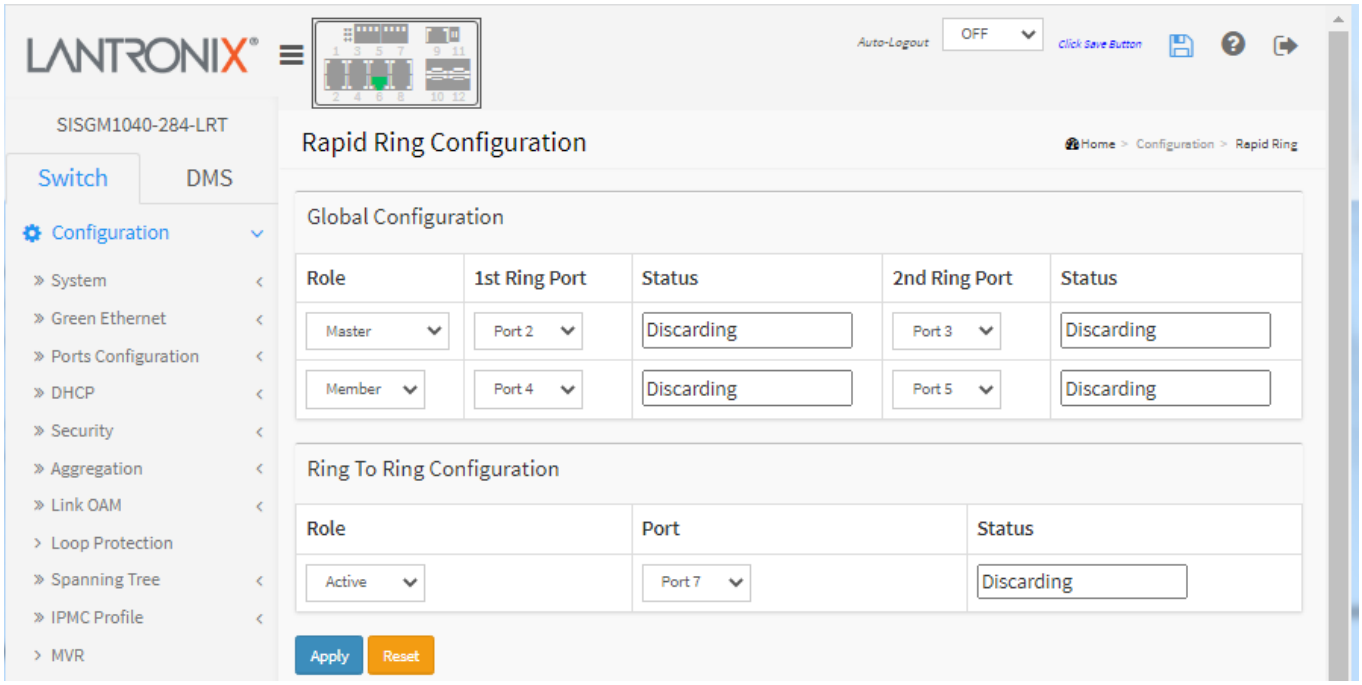
Status : Displays the current Rapid Ring status of the port (e.g., Forwarding, Discarding, etc.).

Buttons:

Apply – Click to save changes.

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

Example:



Messages

Message: *Rapid Ring Configuration Error Error in port 2, STP is enable*

Meaning: You mis-configured Rapid Rings setup.

Recovery: **1.** Click the **Previous** button. **2.** Re-configure rapid ring with valid selections. **3.** Disable STP globally and per-port at Configuration > Spanning Tree > CIST Port. **4**. Continue operation.

Message: *The ports should not be same.*

Meaning: You configured at least one port for multiple Roles.

Recovery: **1.** Click the OK button to clear the webpage message. **2**. Change the port role selections. **3.** Click the **Apply** button. **4.** Continue operation.

Configuration > Percepxion and LPM

This page lets you configure Percepxion parameters. This page has four sections: the Status, Configuration, Percepxion Connection 1, and Connection 2 sections as shown and described below.

Percepxion is Lantronix cloud-hosted or on-premise management platform that provides a single pane of glass for centralized management and automated monitoring of deployed Lantronix devices, along with real-time notifications, managed APIs and data dashboards. For more information see https://www.lantronix.com/percepxion/.

Lantronix Provisioning Manager (LPM) is a software application that provisions, configures and updates Lantronix Console Managers and IoT Gateways for local site installations and deployments. LPM discovery is enabled by default and is not configurable. For more LPM information see https://www.lantronix.com/products/lantronix-provisioning-manager/.

There are three pieces of information that the Percepxion client needs to complete registration and to publish data and configuration to the Percepxion server: Serial Number, Device ID, and Device Key. The Serial Number is always preprogrammed on the device (typically derived from the MAC address of the first Ethernet port). A new device would also be preprogrammed with the Device ID and Key.

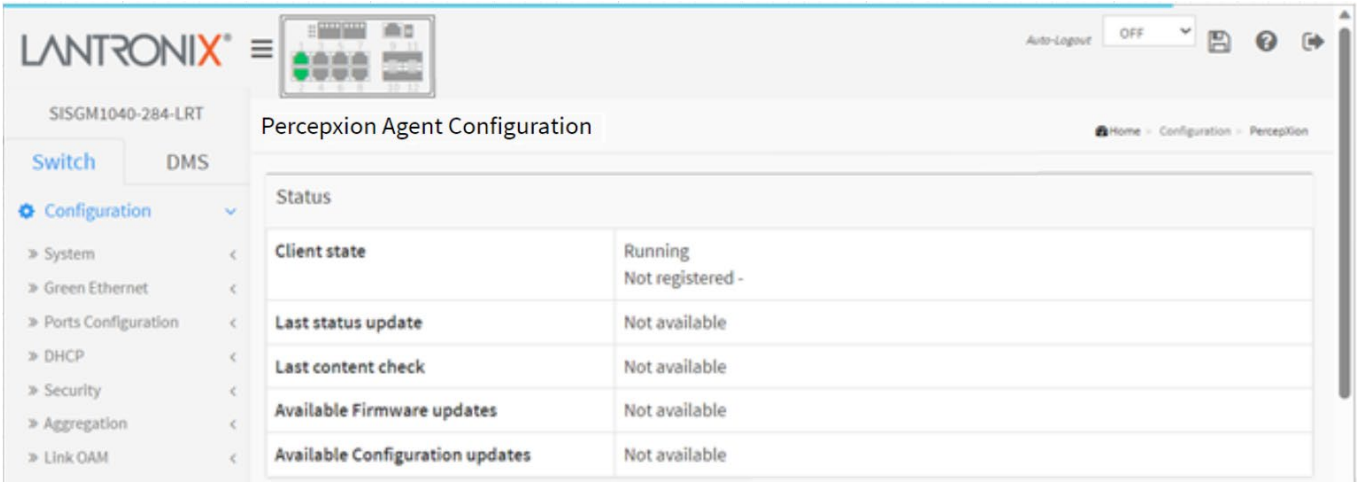
For existing devices where the ID and Key are not pre-programmed, LPM uses Lantronix proprietary search and query protocol to get the device serial number, and then uses the switch REST API interface to set the Device ID and Device Key.

Supported Firmware Versions

Devices must meet firmware requirements in order to work with Percepxion and LPM. SISPM1040--284-LRT requires firmware v 7.20.0190 or above.

Percepxion Agent Configuration

Navigate to Configuration > Percepxion > Percepxion Config to display the Percepxion Agent Configuration page:



Parameter descriptions:

Status:

Client state: Displays the existing Percepxion client state (e.g., *Exited*, *Active, Inactive, Running,* or *Not Registered*) .

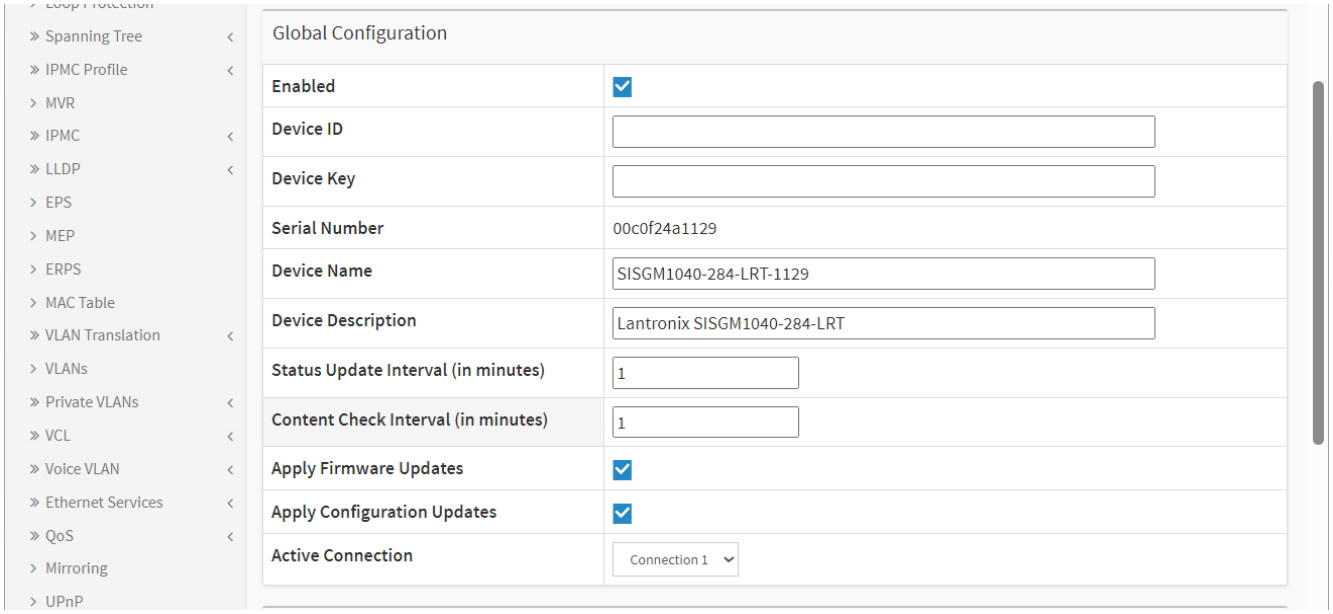
Last status update: Displays the amount of time in minutes between status updates (1-1440 minutes or *<Not Available>.*

Last content check: Displays the amount of time in minutes between content checks; 1 minute to 90 days (in minutes) or *<Not Available>.*

Available Firmware updates: Displays a list of firmware that is available on the server. Select the firmware from this list and click Update now to upgrade or downgrade the firmware. Displays *<Not available>* if no Firmware updates are currently available.

Available Configuration updates: Displays a list of configuration that is available on the server.
Select the configuration from this list and click Update now to upgrade or downgrade the firmware. Displays *<Not available>* if no configuration updates are currently available.

Global Configuration:



Enabled : Check the box to enable Percepxion globally. The default is disabled (unchecked).

Device ID: Displays the switch Device ID (read only). The Device ID may be provisioned through Lantronix Provisioning manager (LPM). **Note**: The Device ID can only be provisioned once. It will persist across resets.

Device Key: Enter the key for the device; 32 alphanumeric characters. **Note**: Device Key may be configured via the Lantronix Provision Manager (LPM). The entry field shows two icons:

 : Click to Show the Device Key text as you enter it.

 : Click to Hide the Device Key text as you enter it.

Serial Number : Displays the serial number of the switch in the format *11-22-33-44-55-66*. Read only.

Device Name : Enter a Percepxion Device Name for the switch of up to 32 alphanumeric characters (e.g., *SISPM1040-384-SAAS*). Device Name can have only alphanumeric (a-z, A-Z, 0-9) characters, hyphens (-), and underscores (_). Device Name must begin and end with an alphanumeric character.

Device Description : Enter a Percepxion Device Description for the switch of up to 32 alphanumeric characters (e.g., *SISGM1040-284-LRT*).

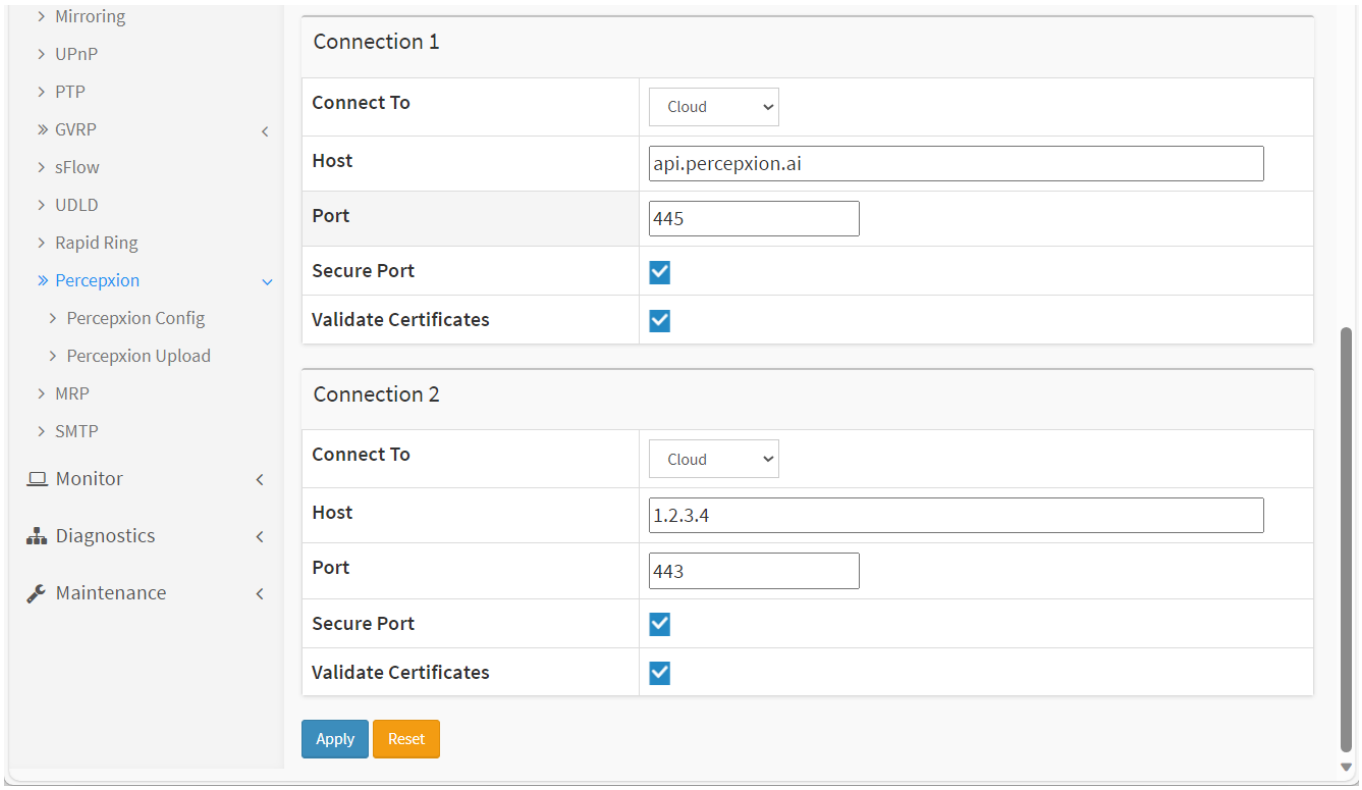
Status Update Interval : Select the amount of time in minutes between updates (1-1440 minutes). The default is 1 minute. This is the frequency that the switch updates the device status to Percepxion.

Content Check Interval : Select the amount of time in minutes between content checks (1-56160 minutes). The default is 1 minute. This is the frequency that the switch checks Percepxion for updates to configuration or firmware. The valid range is 1 hour – 2160 hours (90 days).

Apply Firmware Updates : Check the box to enable automatic switch firmware upgrades via Percepxion. The default is enabled.

Apply Configuration Updates : Check the box to enable automatic switch configuration upgrades via Percepxion. The default is enabled.

Active Connection: At the dropdown select the configuration you want to be active (i.e., *Connection 1* or *Connection 2*. The default is *Connection 1*. This is the connection to use when connecting to Percepxion. The configurable parameters for Connection 1 and Connection 2 are shown and described below.



Connection 1 :

Connect To : At the dropdown, select Cloud (default) or On Premise as the Percepxion connection type for Connection 1. Percepxion is available in cloud or on-premise installation. Choose cloud or on-premise setup according to the determination of your organization. See the Percepxion Help page for more information.

> ***Cloud*** setup connects you directly to the Percepxion server URL, allowing you to access your devices through internet.
>
> ***On-premise*** setup connects you to Percepxion through your organization's network. This means you need to be physically "on-premises" to access your organization's network via Wi-Fi, or may need to use a VPN connection. You may later view and update on-premise setup.

Host : Enter the IP address or host name of the Percepxion server for Connection 1. This is used by Percepxion to register the switch.

Port : Enter the port number for Connection 1. The default is port 443.

Secure Port : Check the box to make the selected port a secure port for Connection 1. The default is enabled.

Validate Certificates : Check the box to force using certificate validation for Connection 1. The default is enabled. To validate certificates, Secure Port must be enabled.

Connection 2 :

Connect To : At the dropdown, select Cloud (default) or On Premise as the Percepxion connection type for Connection 2. Percepxion is available in cloud or on-premise installation. Choose cloud or on-premise setup according to the determination of your organization. See the Percepxion Help page for more information.

> ***Cloud*** setup connects you directly to the Percepxion server URL, allowing you to access your devices through internet.
>
> ***On-premise*** setup connects you to Percepxion through your organization's network. This means you need to be physically "on-premises" to access your organization's network via Wi-Fi, or may need to use a VPN connection. You may later view and update on-premise setup.

Host : Enter the IP address of the Percepxion Host for Connection 2.

Port : Enter the port number for Connection 2. The default is port 443.

Secure Port : Check the box to make the selected port a secure port for Connection 2. The default is enabled.

Validate Certificates : Check the box to enable using certificate validation of the Percepxion server certificates. To validate certificates, Secure Port must be enabled. The default is enabled.

Buttons

Apply : Click to apply changes.

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

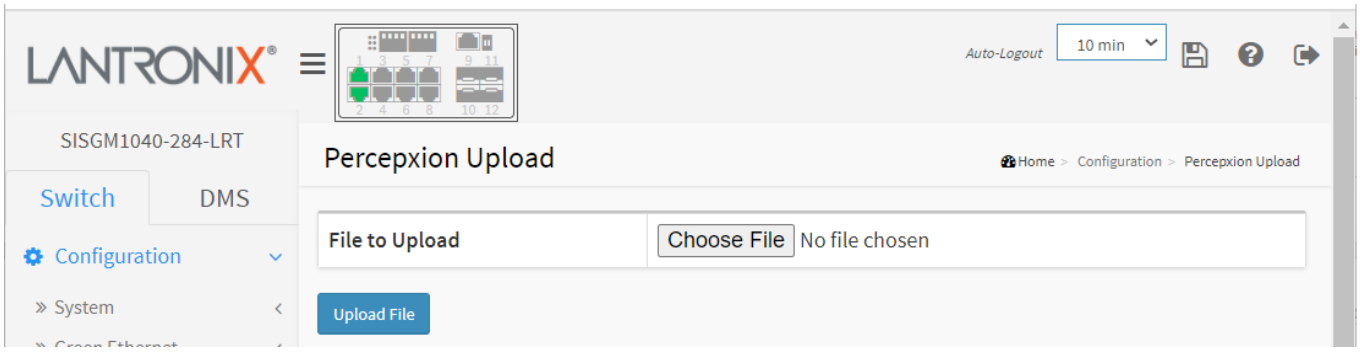
Messages:

device id : 32 alphanumeric characters

5

Percepxion Upload

Navigate to Configuration > Percepxion > Percepxion Upload to display the Percepxion Upload page. This page lets you navigate to and select a file to upload.



Parameter descriptions:

File to Upload: Click the Choose File button to navigate to and select a file to upload.

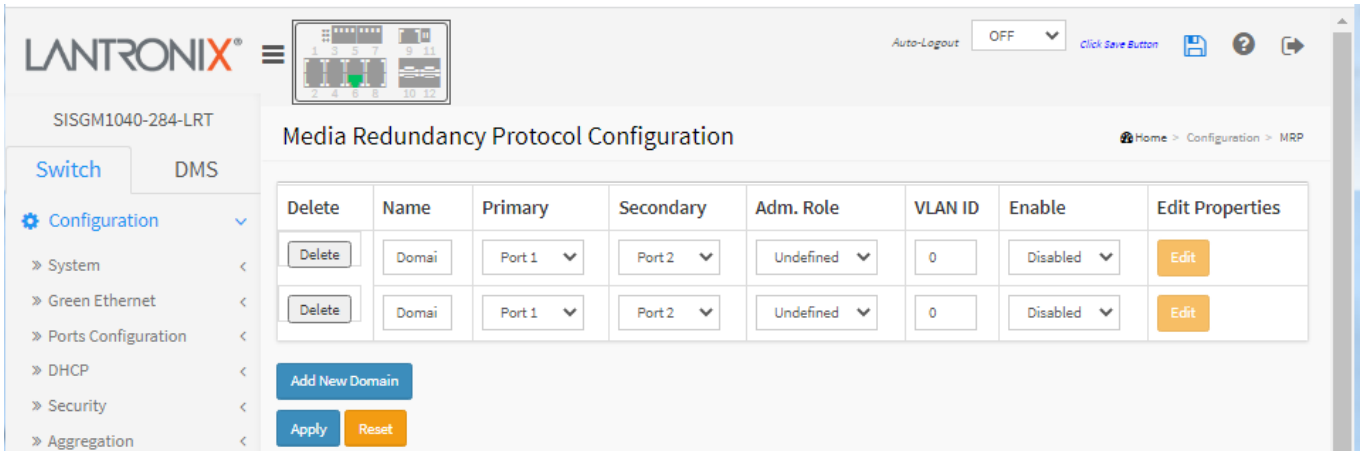
Upload File: Click the button to upload the selected file. The message "*Upload successfully completed.*" displays.

Configuration > MRP

This page lets you configure MRP (Media Redundancy Protocol) parameters (added at FW v7.10.2465).
The maximum number of MRP entries is 2.

MRP is a data network protocol standardized by the International Electrotechnical Commission as IEC 62439-2. It allows rings of Ethernet switches to overcome any single failure with recovery time much faster than achievable with Spanning Tree Protocol. See the IETF website at for more information. See Appendix C – MRP Operation and Examples on page 424 for MRP setup examples.

Note: You must disable Spanning Tree at Configuration > Spanning Tree > CIST Port before you can configure MRP on this page.



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

Name: A logical name for the MRP domain to easy the management of MRP domains.

Primary: The index of the layer 2 interface which is used as ring port 1.

Secondary: The index of the layer 2 interface which is used as ring port 2.

Adm. Role: If the value is set to ***Client*** the entity will be set to the role of a Media Redundancy Client (***MRC***). If the value is set to ***Manager***, the entity will be set to the role of a Media Redundancy Manager (***MRM***). The MRM monitors the ring topology. During normal ring operation (i.e., without ring interruption due to an error) the MRM disconnects one of its ring ports so that the ring topology becomes 'loop free' from a communication point of view. As soon as the ring is open due to the failure of a node and the data communication is broken, the MRM reconfigures the data paths within 200ms. It enables the disconnected ring port and creates a new loop free topology. Multiple MRMs in a single ring is not supported.

VLAN ID: The VLAN ID assigned to the MRP protocol. The allowed range is 0 to 4094.

Enable: Enable/Disable MRP protocol.

Edit Properties: Click to edit domain properties (see below).

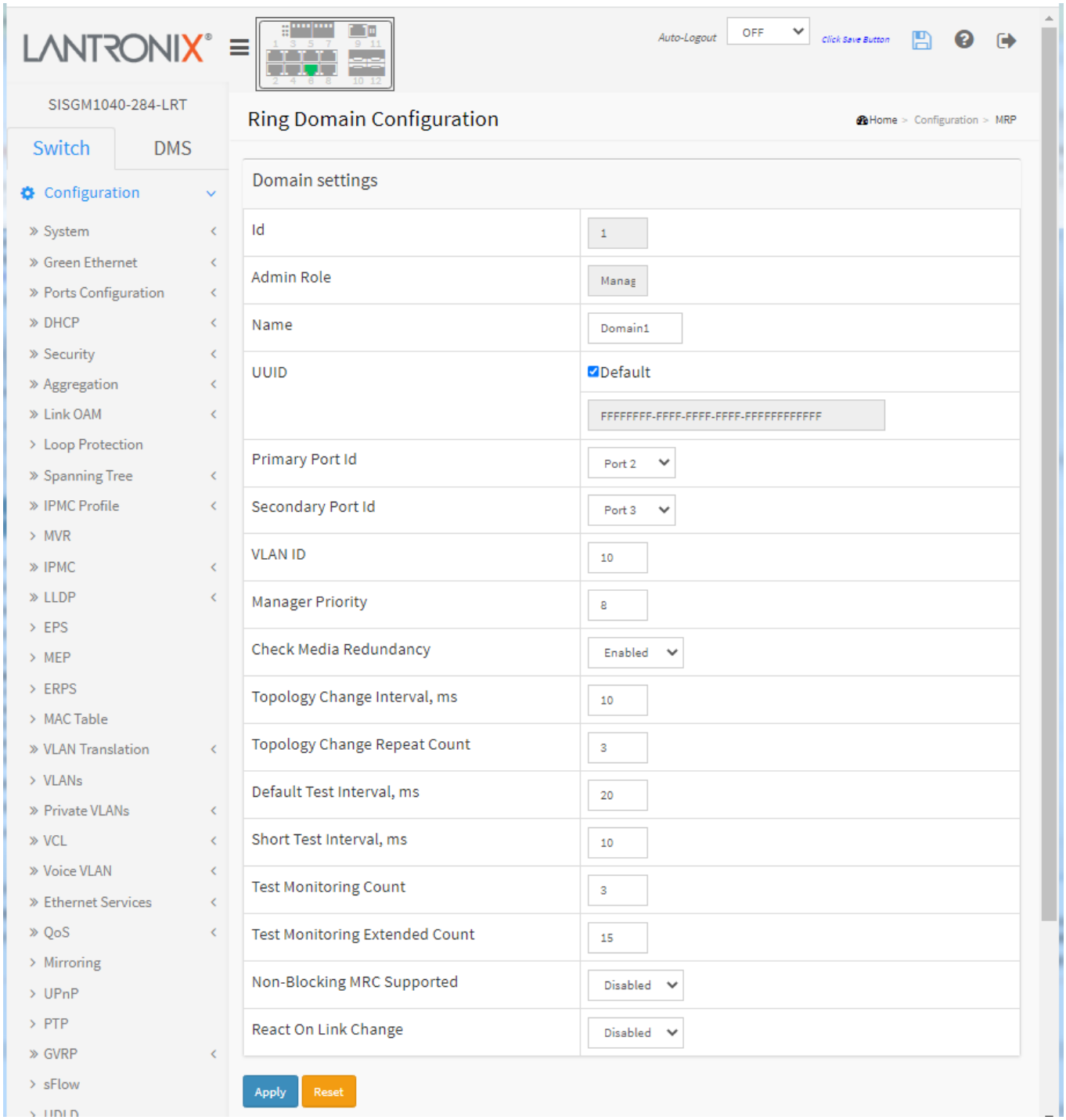
Buttons

Add New Domain: Click to add a new domain row.

Apply: Click to save changes.

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

Click the **Edit Properties** button to display the Ring Domain Configuration page where you can edit domain properties. Note that some parameters appear only in the Media Redundancy Client (MRC) role or only in the Media Redundancy Manager (MRM) role. The Media Redundancy Manager (MRM) Admin Role page is shown below:



ID: The index of the entry.

Admin Role: If the value is set to Client, the entity will be set to the role of a Media Redundancy Client (MRC). If the value is set to Manager the entity will be set to the role of a Media Redundancy Manager (MRM).

Name: A logical name for the MRP domain to easy the management of MRP domains.

UUID: Universally Unique Identifier belongs to the MRP domain which represents a ring.

Primary Port ID: The index of the layer 2 interface which is used as ring port 1.

Secondary Port ID: The index of the layer 2 interface which is used as ring port 2.

VLAN ID: The VLAN ID assigned to the MRP protocol. The allowed range is 0 to 4094.

Manager Priority: This parameter contains the value for the manager priority.

Check Media Redundancy: This parameter selects whether monitoring of MRM state is enabled or disabled. Only MRM.

Topology Change Interval, ms: This parameter contains the value of the interval for sending MRP_TopologyChange frames. The allowed range is 1 to 20. Only MRM.

Topology Change Repeat Count: This parameter contains the value of the interval count which controls repeated transmissions of MRP_TopologyChange frames. The allowed range is 1 to 5. Only MRM.

Default Test Interval, ms: This parameter contains the value of the default interval for sending MRP_Test frames on ring ports. The allowed range is 1 to 50. Only MRM.

Short Test Interval, ms: This parameter contains the value of the short interval for sending MRP_Test frames on ring ports after link changes in the ring. The allowed range is 1 to 30. Only MRM.

Test Monitoring Count: This parameter contains the value of the interval count for monitoring the reception of MRP_Test frames. The allowed range is 1 to 15. Only MRM.

Test Monitoring Extended Count: This optional parameter contains the value of the extended interval count for monitoring the reception of MRP_Test frames. The allowed range is 1 to 30. Only MRM.

Non-Blocking MRC Supported: This parameter specifies the ability of the MRM to support MRCs without BLOCKED port state support in the ring. Only MRM.

React On Link Change: This optional parameter specifies whether the MRM reacts on MRP_LinkChange frames or not. Only MRM.

Link Down Interval, ms: This parameter contains the value of the interval for sending MRP_LinkDown frames on ring ports. The allowed range is 1 to 50. Only MRC.

Link Up Interval, ms: This parameter contains the value of the interval for sending MRP_LinkUp frames on ring ports. The allowed range is 1 to 50. Only MRC.

Link Change Count: This parameter contains the value of the MRP_LinkChange frame count which controls repeated transmissions of MRP_LinkUp or MRP_LinkDown frames. The allowed range is 1 to 10. Only MRC.

BLOCKED State Supported: This parameter specifies whether the MRC supports BLOCKED state at its ring ports or not. Only MRC.

Buttons

Apply: Click to save changes.

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

Messages

Message: *VLAN ID is used in other ring domain*

Message: *Domain is enabled*

Message: *The maximum number of entries is 2*

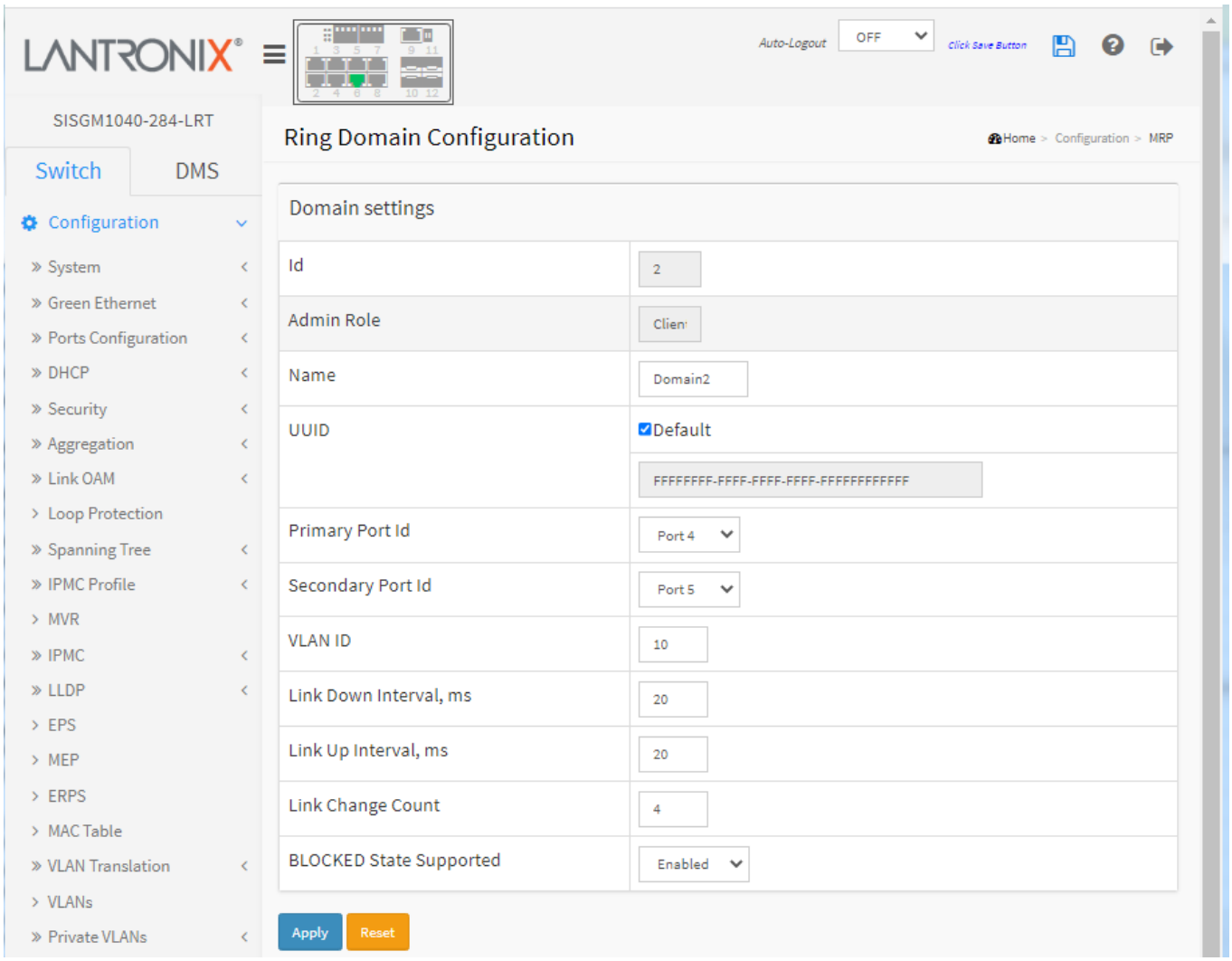
Message: *Role is undefined*

Message: *Invalid ring port*

Message: *Ring port is used*

Message: *Domain is enabled*

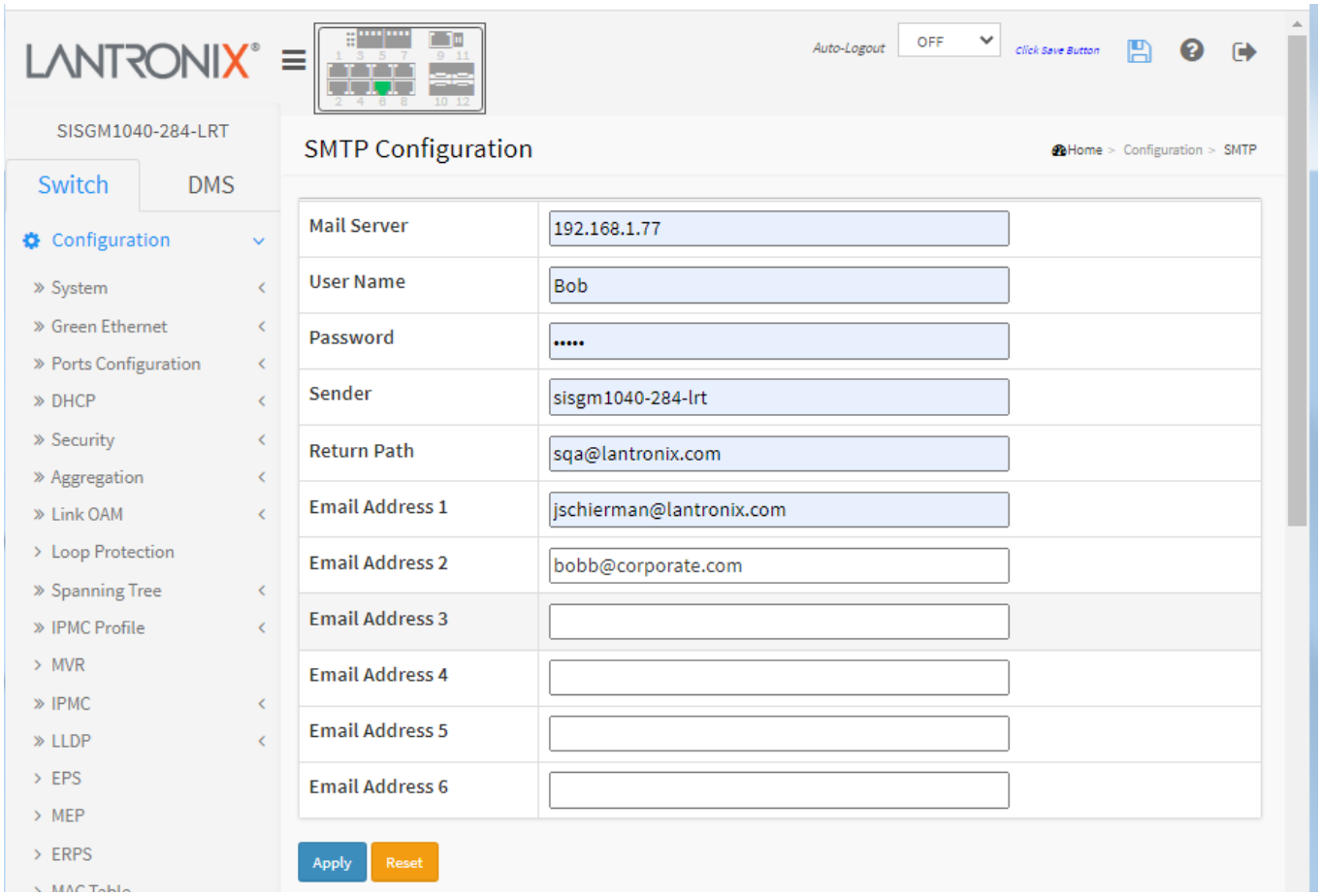
The Media Redundancy Client (MRC) Admin Role page is shown below:



Configuration > SMTP

Configure SMTP (Simple Mail Transfer Protocol) on this page. Simple Mail Transfer Protocol is the message-exchange standard for the Internet.

The switch is to be configured as a client of SMTP while the server is a remote device that will receive messages from the switch that alarm events occurred.



Mail Server: The IP address or hostname of the mail server. IP address is expressed in dotted decimal notation. This will be the device that sends out the mail for you

User Name: Specify the username on the mail server.

Password: Specify the password of the user on the mail server.

Sender: Specify the sender name of the alarm mail.

Return Path: Specify the sender email address of the alarm mail. This address will be the "from" address on the email message.

Email Address #: Specify the email address of the receiver.

Buttons

Apply: Click to apply changes immediately.

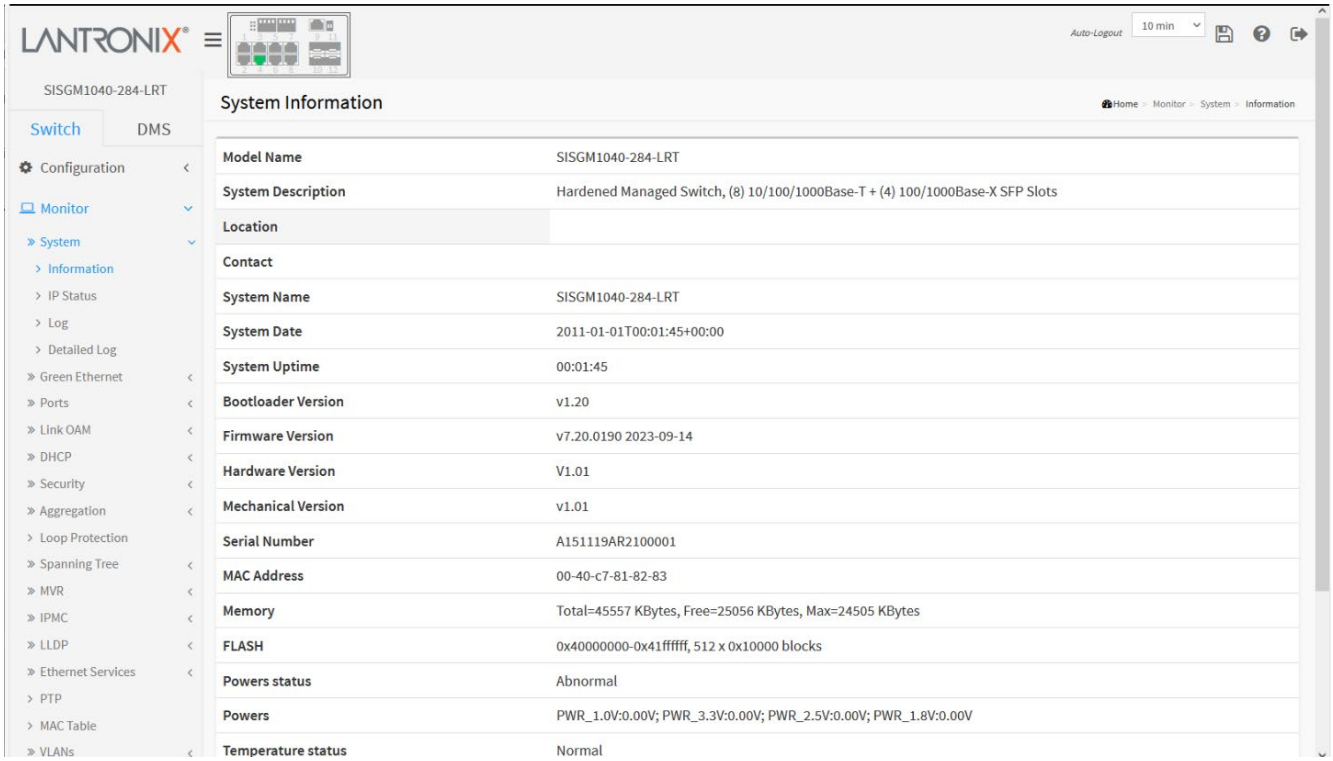
Reset: Click to undo any changes made locally and revert to previously saved values.

2. Monitor

The Monitor menu items let you view the parameters that are currently configured via the Configuration sub-menus.

Monitor > System > Information

Switch system information is provided here. This is the startup page; when you log in to the system this page displays. All fields are read only.



Parameter descriptions:

Model Name: Displays the factory defined model name for identification purposes (e.g., *SISGM1040-284-LRT*).

System Description: the system description (e.g., *Hardened Managed Switch, (8) 10/100/1000Base-T + (4) 100/1000Base-X SFP Slots).*

Location: The system location configured at Configuration > System > Information > System Location.

Contact: The system contact configured at Configuration > System > Information > System Contact.

System Name: Displays the user-defined system name configured at System > System Information > Configuration > System Name (e.g., *SISGM1040-284-LRT*).

System Date: The current (GMT) system time and date. The system time is obtained from the Timing server running on the switch, if any (the default is *2011-01-01T00:56:26+00:00*).

System Uptime: The amount of time the device has been operational.

Bootloader Version: Displays the current boot loader version number (e.g., *v1.20*).

Firmware Version: Displays the current firmware version number and date (e.g., *v7.20.0190 2023-09-14*)

Hardware Version: Displays the hardware version of the device (e.g., *v1.01*).

Mechanical Version: Displays the mechanical version of the device (e.g., *v1.01*).

Serial Number: Displays the unique serial number that is assigned to the device (e.g., *A088119AR2500002*).

MAC Address: The MAC Address of this switch (in the format *00-11-22-33-44-55*).

Memory: Displays the memory size of the system (e.g., *Total=49801 KBytes, Free=30364 KBytes, Max=30210 KBytes*).

FLASH: Displays the flash size of the system (e.g., *0x40000000-0x41ffffff, 512 x 0x10000 blocks*).

Powers status: Displays the powers status of the system (e.g., *Normal* or *Abnormal*).

Powers: Displays the powers of the system (e.g., *PWR_1.0V:0.98V; PWR_3.3V:3.28V; PWR_2.5V:2.60V; PWR_1.8V:1.93V*).

Temperature status: Displays the temperature status of the system (e.g., *Normal*).

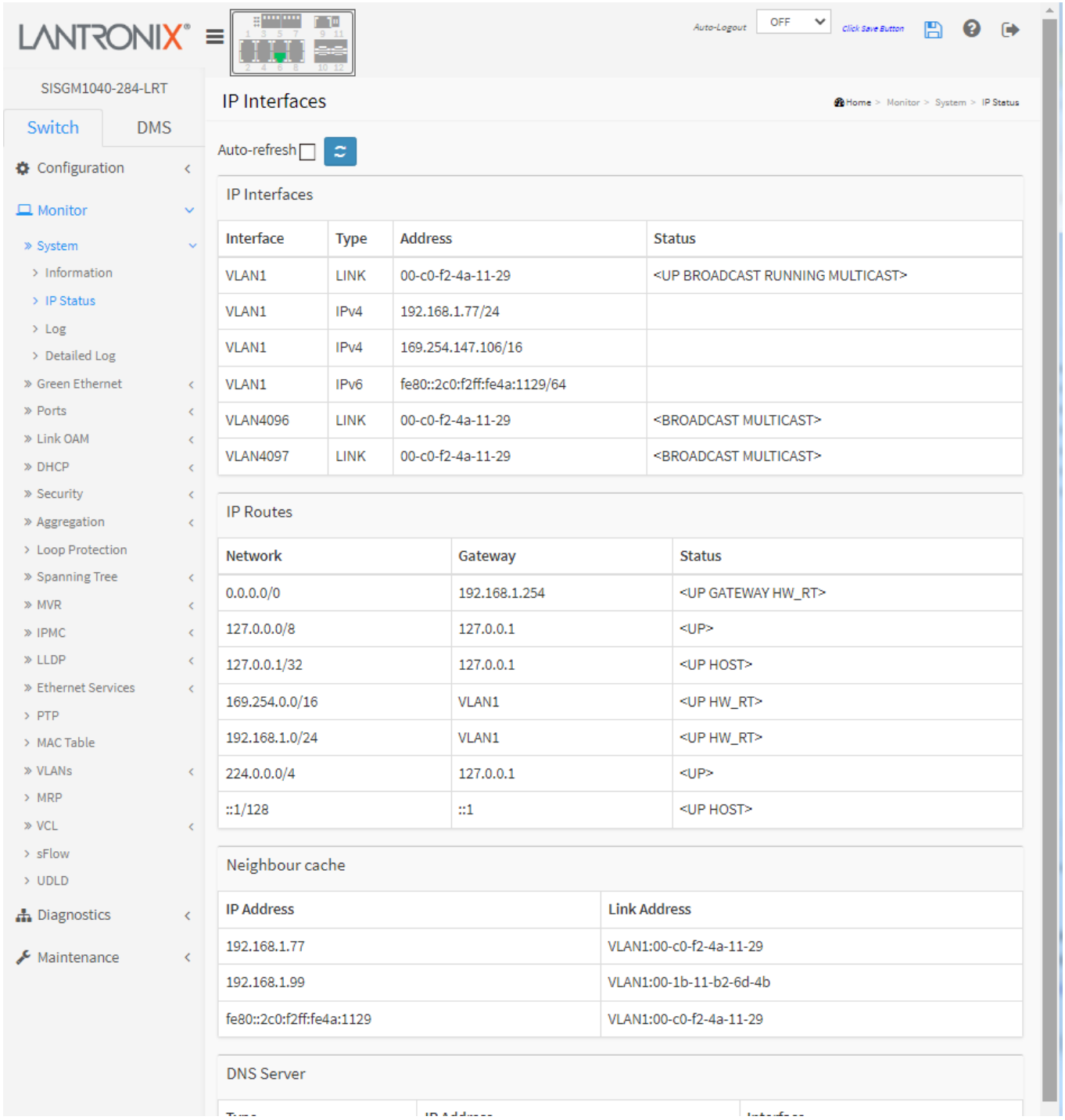
Temperature 1: Displays the temperature of system sensor 1 (e.g., *41(C) ; 105(F)*).

Temperature 2: Displays the temperature of system sensor 2 (e.g., *45(C) ; 113(F)*).

CPU Load (100ms, 1s, 10s): Displays the cpu loading (100ms, 1s, 10s) of the system (e.g., *15%, 12%, 10%).*

Monitor > System > IP Status

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



IP Interfaces

Interface: The name of the interface.

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

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

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

IP Routes

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

Gateway: The gateway address of this route.

Status: The status flags of the route.

Neighbour cache

IP Address: The IP address of the entry.

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

DNS Server

Type: The configuration type of DNS server.

IP Address: The IP address of the DNS server.

Interface: The name of the interface.

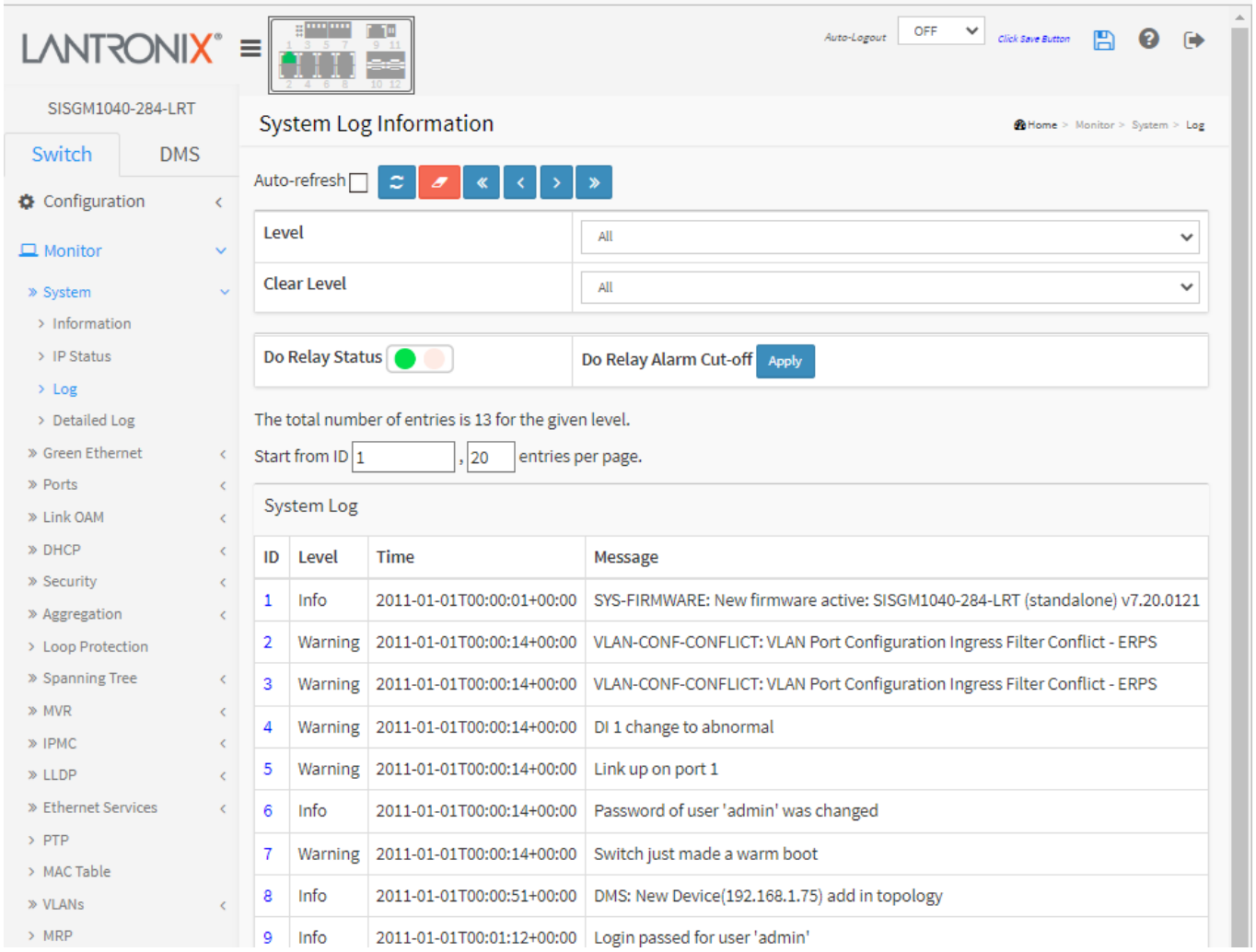
Buttons

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

Refresh: Click to refresh the page immediately.

Monitor > System > Log

The switch system log information is provided here.



Level: The level of the system log entry. The "Level" input field is used to filter the display system log entries.

Emerg: The system log entry is belonged emergency level.

Alert: The system log entry is belonged alert level.

Crit: The system log entry is belonged critical level.

Error: The system log entry is belonged error level.

Warning: The system log entry is belonged warning level.

Notice: The system log entry is belonged notice level.

Info: The system log entry is belonged information level.

Debug: The system log entry is belonged debug level.

Clear Level: input field is used to specify which system log entries will be cleared.

Do Relay Status: shows the status of digital-out relay contact. See the Install Guide for hardware information.

Do Relay Alarm Cut-off: force cut off the digital-out relay contact. See the Install Guide for hardware information.

System Log

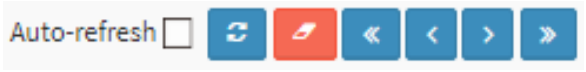
ID : The entry number.

Level : The level of the system log entry. See description above.

Time: The date and time that the system log entry occurred.

Message: The detail message of the system log entry.

Buttons



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

Refresh: Updates the table entries, starting from the current entry.

Clear: Flushes the selected entries.

<< : Updates the table entries, starting from the first available entry.

< : Updates the table entries, ending at the last entry currently displayed.

>> : Updates the table entries, starting from the last entry currently displayed.

> : Updates the table entries, ending at the last available entry.

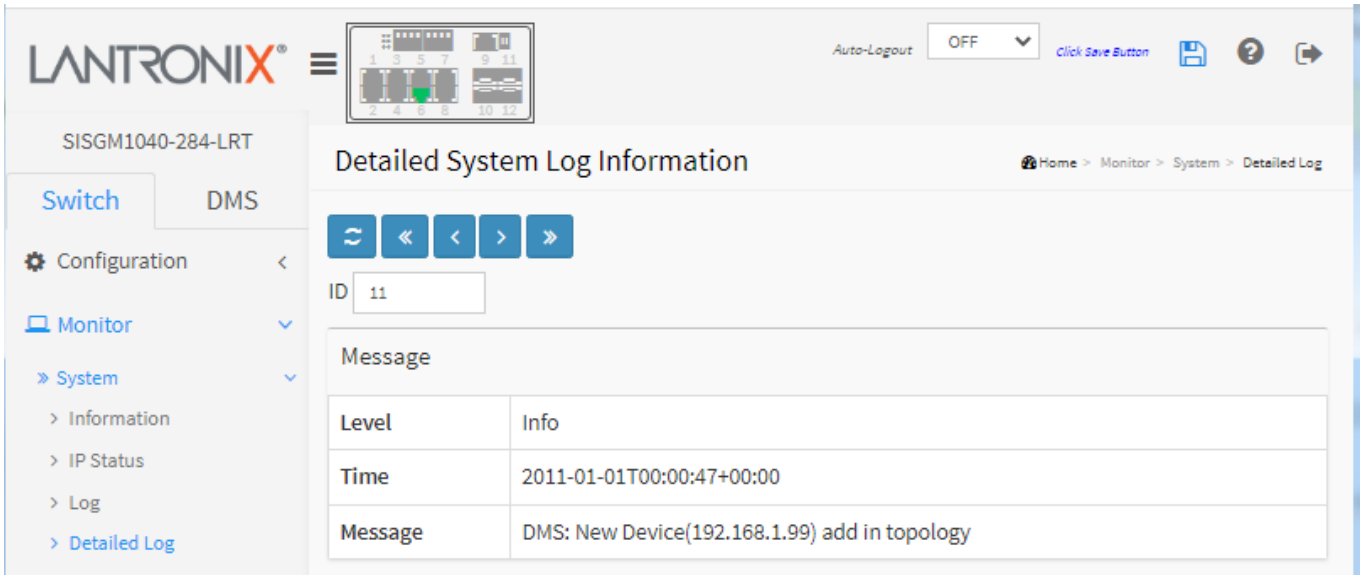
Example

System Log

ID	Level	Time	Message
1	Warning	2011-01-01T00:00:11+00:00	SFP module inserted on port 12
2	Warning	2011-01-01T00:00:11+00:00	DI 1 change to abnormal
3	Warning	2011-01-01T00:00:11+00:00	Link up on port 2
4	Warning	2011-01-01T00:00:11+00:00	SFP module inserted on port 9
5	Info	2011-01-01T00:00:11+00:00	Password of user 'admin' was changed
6	Warning	2011-01-01T00:00:11+00:00	Switch just made a cold boot
7	Warning	2011-01-01T00:00:11+00:00	SFP module inserted on port 10
8	Info	2011-01-01T00:00:11+00:00	topologyChange

Monitor > System > Detailed Log

The switch system detailed log information is provided here.



Level: The level of the system log entry. The "Level" field displays system log entries.

Emerg: The system log entry is belonged emergency level.

Alert: The system log entry is belonged alert level.

Crit: The system log entry is belonged critical level.

Error: The system log entry is belonged error level.

Warning: The system log entry is belonged warning level.

Notice: The system log entry is belonged notice level.

Info: The system log entry is belonged information level.

Debug: The system log entry is belonged debug level.

Time: The occurred time of the system log entry.

Message: The detail message of the system log entry.

Buttons

Refresh: Updates the table entries, starting from the current entry.

<< : Updates the table entries, starting from the first available entry.

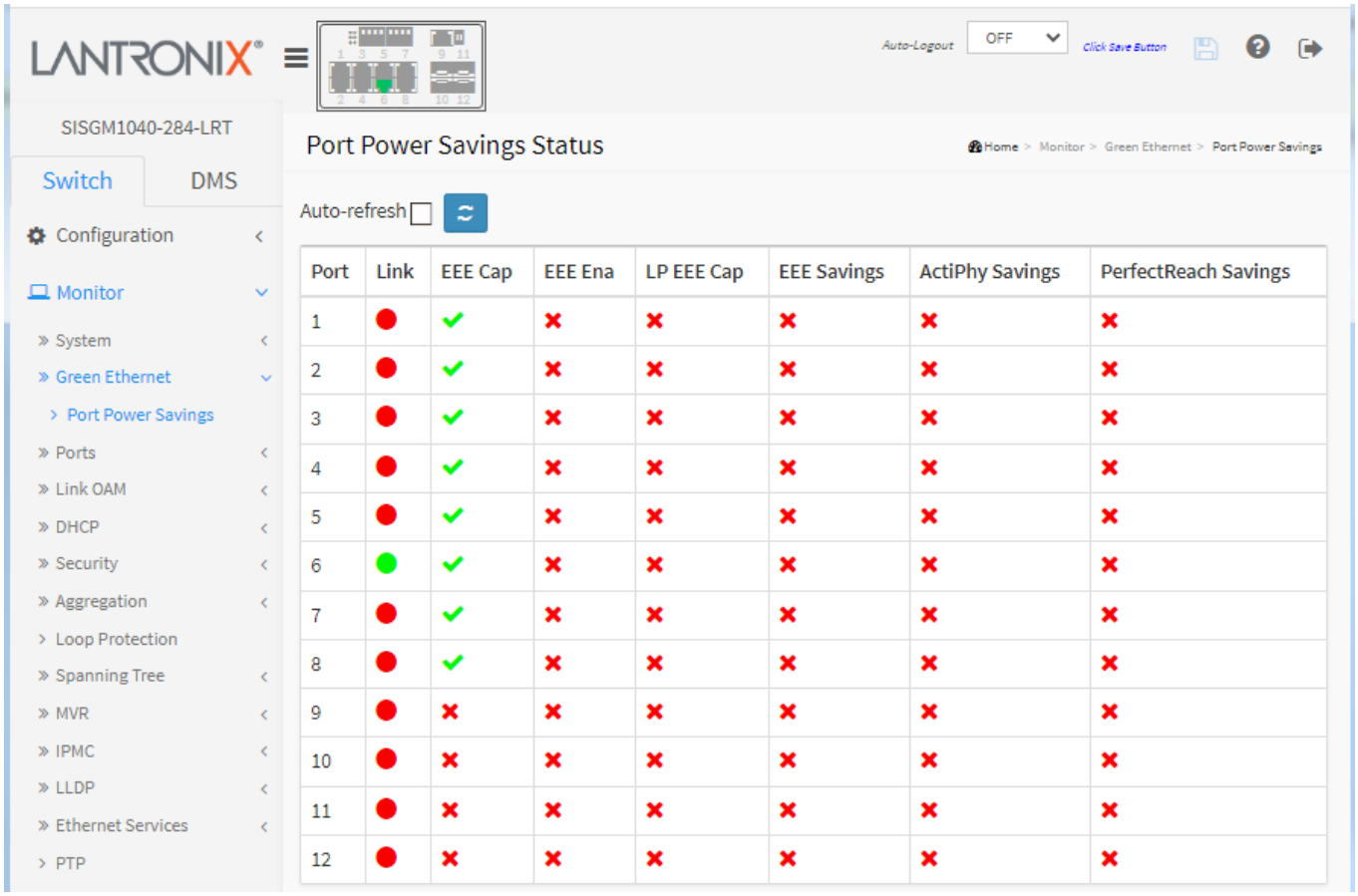
< : Updates the table entries, ending at the last entry currently displayed.

>> : Updates the table entries, starting from the last entry currently displayed.

> : Updates the table entries, ending at the last available entry.

Monitor > Green Ethernet > Port Power Savings

This page provides the current status for EEE (Energy Efficient Ethernet) as defined in IEEE 802.3az.



Port	Link	EEE Cap	EEE Ena	LP EEE Cap	EEE Savings	ActiPhy Savings	PerfectReach Savings
1	●	✓	✗	✗	✗	✗	✗
2	●	✓	✗	✗	✗	✗	✗
3	●	✓	✗	✗	✗	✗	✗
4	●	✓	✗	✗	✗	✗	✗
5	●	✓	✗	✗	✗	✗	✗
6	●	✓	✗	✗	✗	✗	✗
7	●	✓	✗	✗	✗	✗	✗
8	●	✓	✗	✗	✗	✗	✗
9	●	✗	✗	✗	✗	✗	✗
10	●	✗	✗	✗	✗	✗	✗
11	●	✗	✗	✗	✗	✗	✗
12	●	✗	✗	✗	✗	✗	✗

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

Link: Shows if the link is up for the port (green = link up, red = link down).

EEE cap: Shows if the port is EEE capable.

EEE Ena: Shows if EEE is enabled for the port (reflects the settings at the Port Power Savings configuration page).

LP EEE cap: Shows if the link partner is EEE capable.

EEE Savings: Shows if the system is currently saving power due to EEE. When EEE is enabled, the system will power down if no frame has been received or transmitted in 5 usecond increments.

ActiPhy Savings: Shows if the system is currently saving power due to ActiPhy.

PerfectReach Savings: Shows if the system is currently saving power due to PerfectReach.

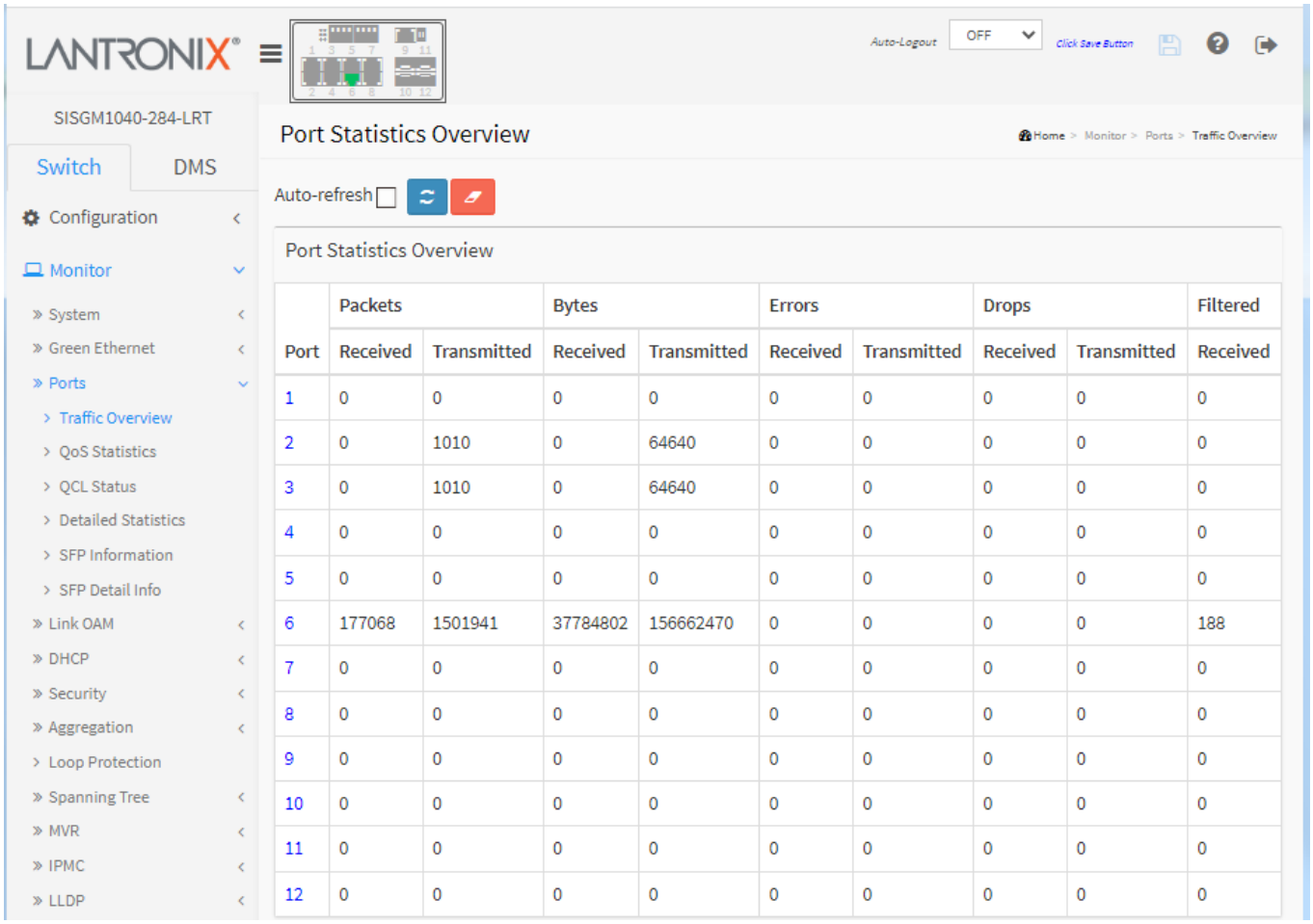
Buttons

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

Refresh: Click to refresh the page.

Monitor > Ports > Traffic Overview

This page provides an overview of general traffic statistics for all switch ports.



Port: The logical port for the settings contained in the same row. Click a linked Port # to display its detailed statistics.

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

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

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

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

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

Buttons

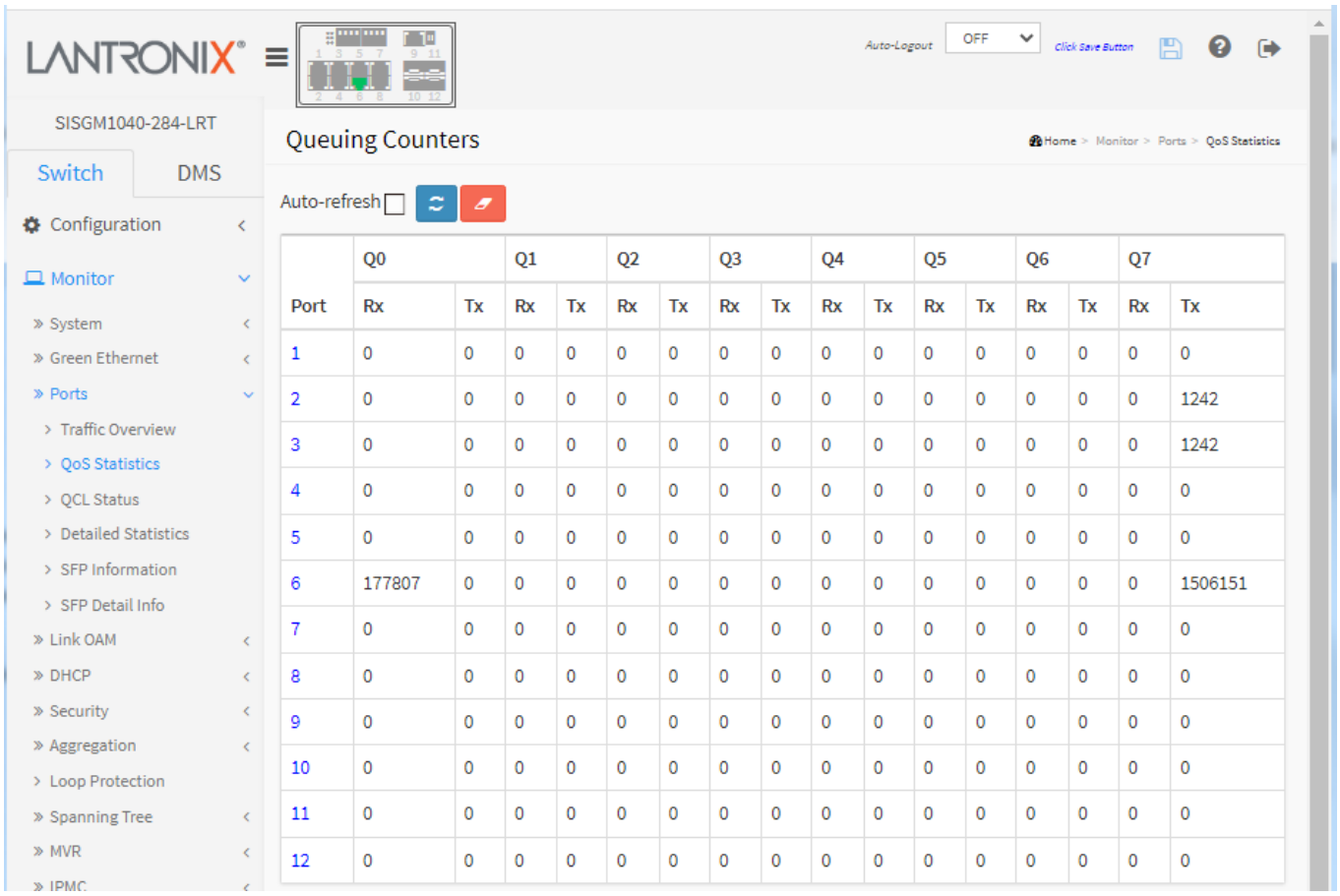
Auto-refresh: Check this box to refresh the page automatically every 3 seconds.

Refresh: Click to refresh the page immediately.

Clear: Clears the counters for all ports.

Monitor > Ports > QoS Statistics

This page provides statistics for the different queues for all switch ports.



	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	1242
3	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1242
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	177807	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1506151
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

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

Qn: There are 8 QoS queues per port. Q0 is the lowest priority queue.

Rx/Tx: The number of received and transmitted packets per queue.

Buttons

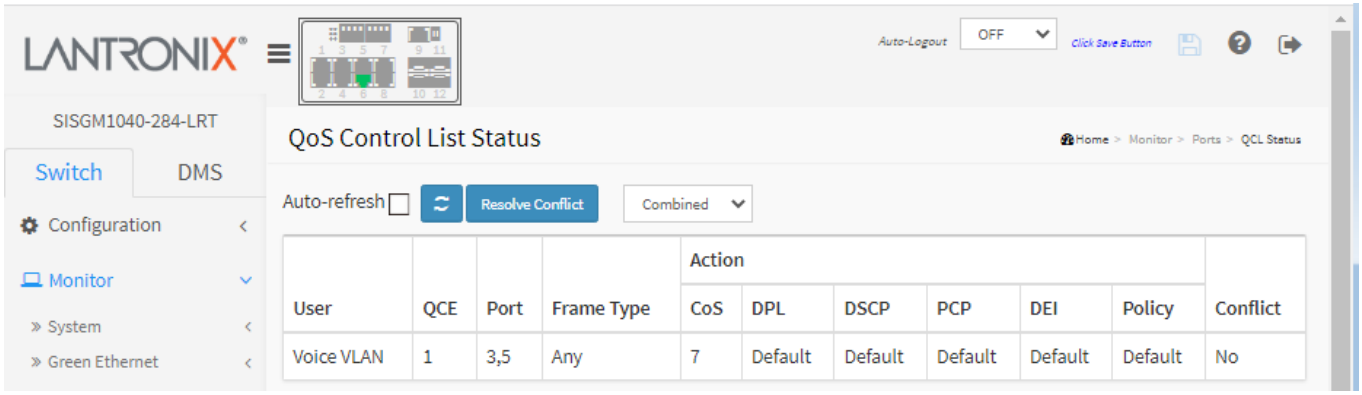
Auto-refresh: Check this box to refresh the page automatically every 3 seconds.

Refresh: : Click to refresh the page immediately.

Clear: Clears the counters for all ports.

Monitor > Ports > QCL Status

This page shows the QCL status by different QCL users. Each row describes the QCE that is defined. It is a conflict if a specific QCE is not applied to the hardware due to hardware limitations. The maximum number of QCEs is 256 on each switch.



User: Indicates the QCL user.

QCE: Indicates the QCE id.

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

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

Any: Match any frame type.

Ethernet: Match EtherType frames.

LLC: Match (LLC) frames.

SNAP: Match (SNAP) frames.

IPv4: Match IPv4 frames.

IPv6: Match IPv6 frames.

Action: Indicates the classification action taken on ingress frame if parameters configured are matched with the frame's content. Possible actions are:

CoS: Classify Class of Service.

DPL: Classify Drop Precedence Level.

DSCP: Classify DSCP value.

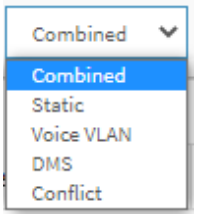
PCP: Classify PCP value.

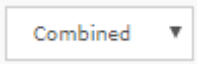
DEI: Classify DEI value.

Policy: Classify ACL Policy number.

Conflict: Displays Conflict status of QCL entries. As H/W resources are shared by multiple applications. It may happen that resources required to add a QCE may not be available, in that case it shows conflict status as 'Yes', otherwise it is always 'No'. Please note that conflict can be resolved by releasing the H/W resources required to add QCL entry on pressing the 'Resolve Conflict' button.

Buttons





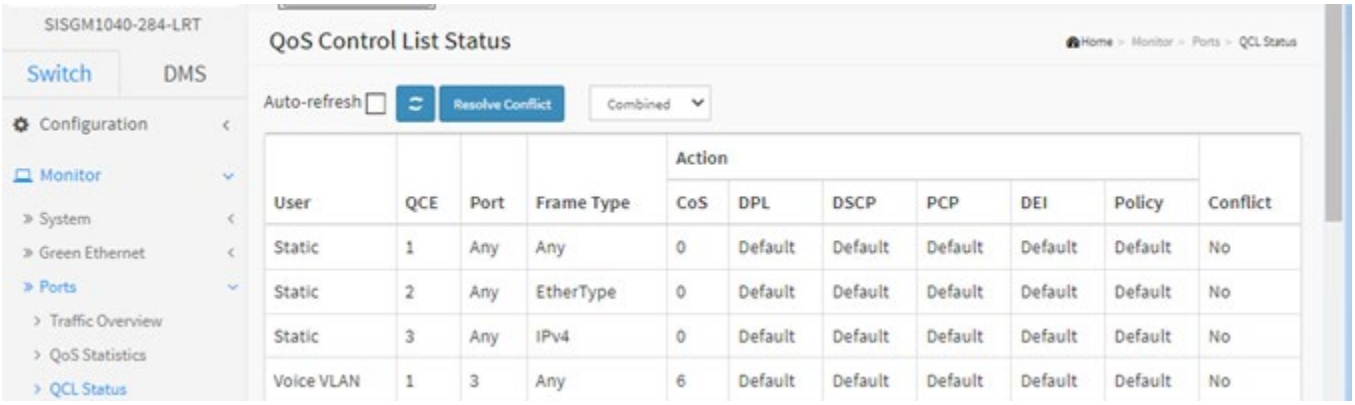
Users : Select the QCL status from this drop down list (Combined, Static, Voice VLAN, DMS, Conflict).

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 the conflict status for any QCL entry is 'yes'.

Refresh: Click to refresh the page.

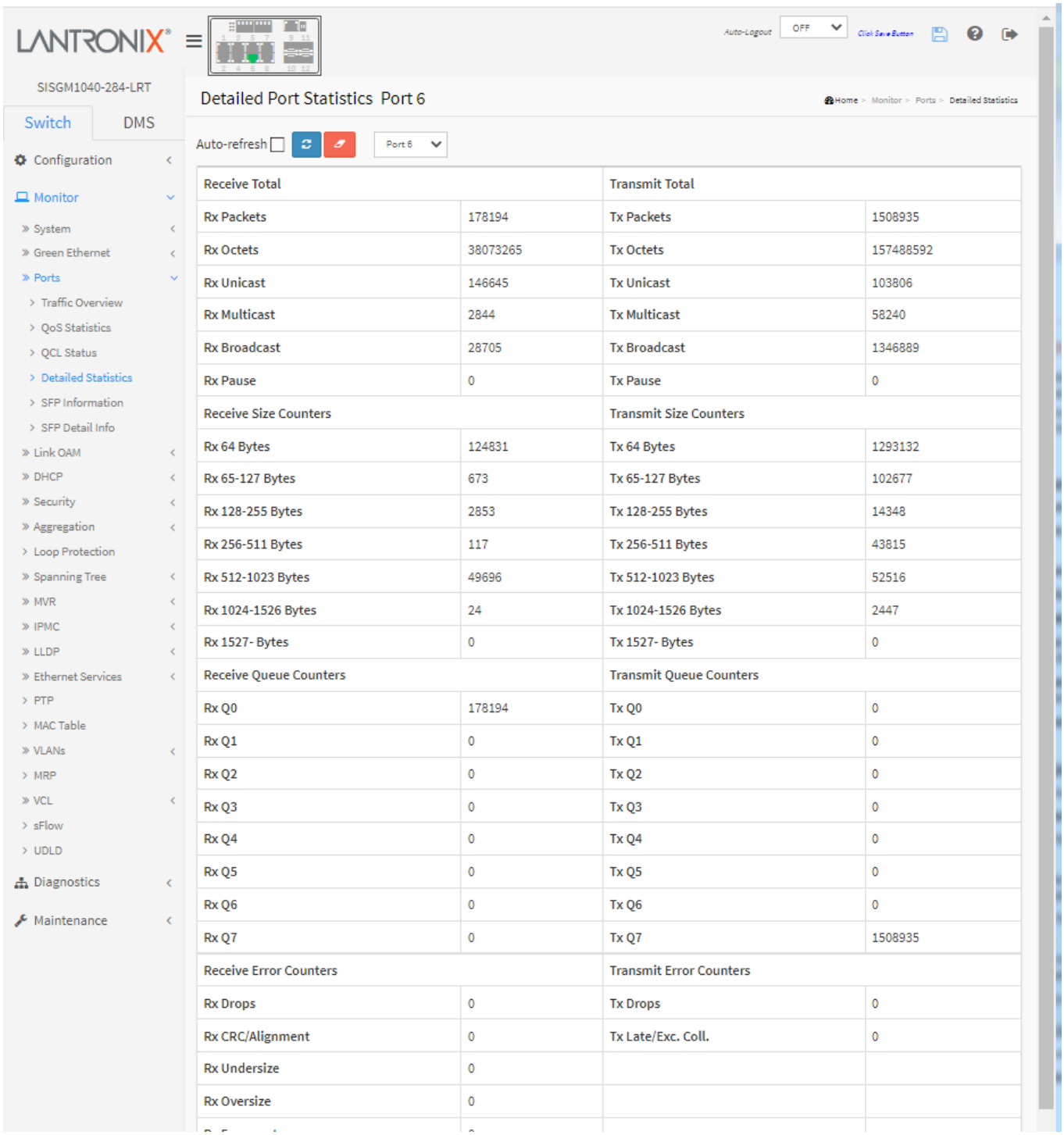
Example:



Monitor > Ports > Detailed Statistics

This page provides 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.



Receive Total		Transmit Total	
Rx Packets	178194	Tx Packets	1508935
Rx Octets	38073265	Tx Octets	157488592
Rx Unicast	146645	Tx Unicast	103806
Rx Multicast	2844	Tx Multicast	58240
Rx Broadcast	28705	Tx Broadcast	1346889
Rx Pause	0	Tx Pause	0
Receive Size Counters		**Transmit Size Counters**	
Rx 64 Bytes	124831	Tx 64 Bytes	1293132
Rx 65-127 Bytes	673	Tx 65-127 Bytes	102677
Rx 128-255 Bytes	2853	Tx 128-255 Bytes	14348
Rx 256-511 Bytes	117	Tx 256-511 Bytes	43815
Rx 512-1023 Bytes	49696	Tx 512-1023 Bytes	52516
Rx 1024-1526 Bytes	24	Tx 1024-1526 Bytes	2447
Rx 1527- Bytes	0	Tx 1527- Bytes	0
Receive Queue Counters		**Transmit Queue Counters**	
Rx Q0	178194	Tx Q0	0
Rx Q1	0	Tx Q1	0
Rx Q2	0	Tx Q2	0
Rx Q3	0	Tx Q3	0
Rx Q4	0	Tx Q4	0
Rx Q5	0	Tx Q5	0
Rx Q6	0	Tx Q6	0
Rx Q7	0	Tx Q7	1508935
Receive Error Counters		**Transmit Error Counters**	
Rx Drops	0	Tx Drops	0
Rx CRC/Alignment	0	Tx Late/Exc. Coll.	0
Rx Undersize	0		
Rx Oversize	0		

Parameter descriptions:

Receive Total and Transmit Total

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

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

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

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

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

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

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

Receive and Transmit Queue Counters: The number of received and transmitted packets per input and output queue.

Receive Error Counters

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

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

Rx Undersize: The number of short frames received with valid CRC. Short frames are frames that are smaller than 64 bytes.

Rx Oversize: The number of long frames received with valid CRC. Long frames are frames that are longer than the configured maximum frame length for this port.

Rx Fragments: The number of short frames received with invalid CRC. Short frames are frames that are smaller than 64 bytes.

Rx Jabber: The number of long frames received with invalid CRC. Long frames are frames that are longer than the configured maximum frame length for this port.

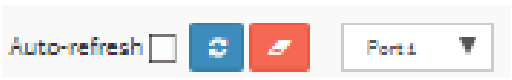
Rx Filtered: The number of received frames filtered by the forwarding process.

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.

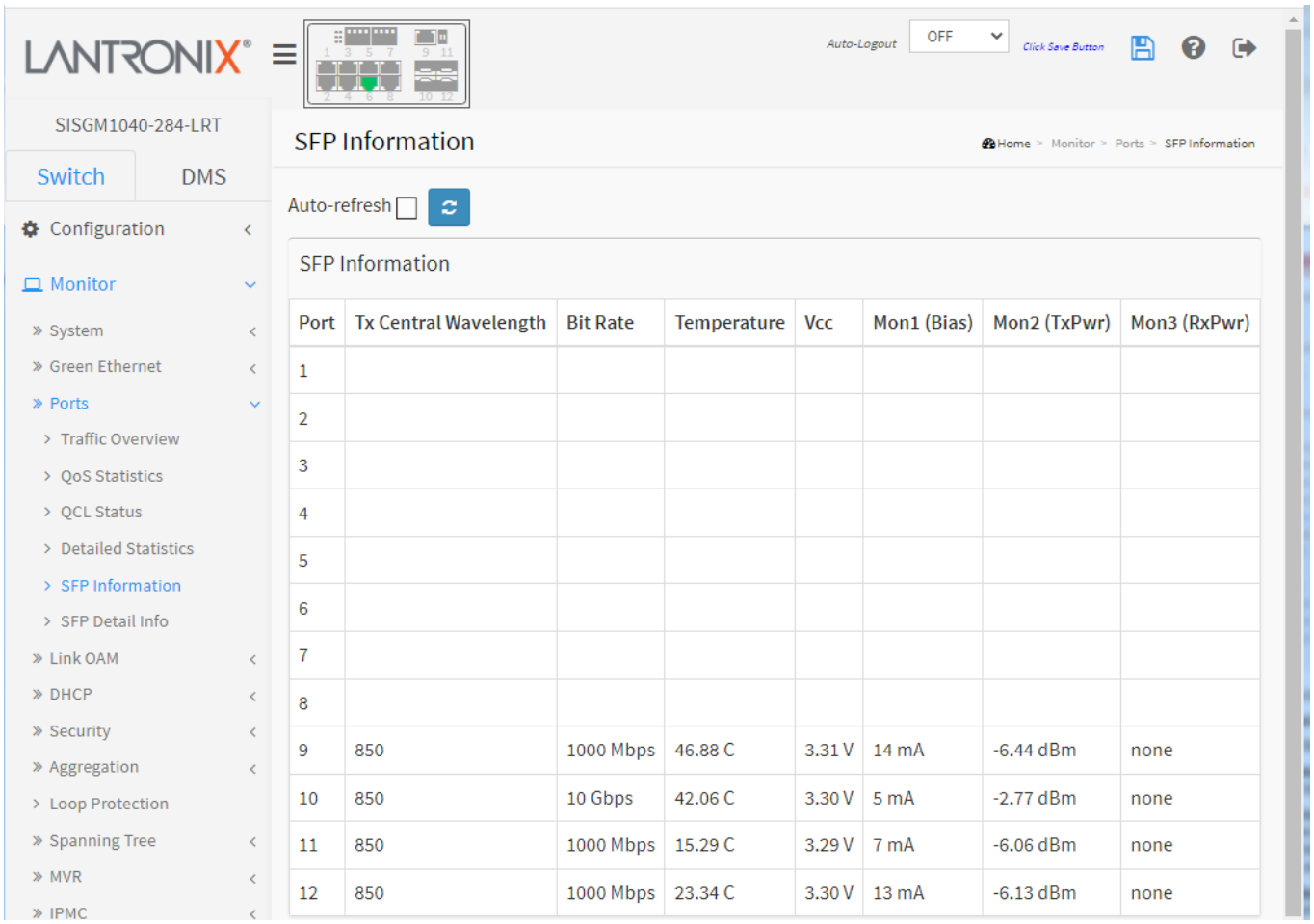
Refresh: Click to refresh the page immediately.

Clear: Clears the counters for the selected port.

: Port select box determines which port is affected by clicking the buttons.

Monitor > Ports > SFP Information

This page displays general SFP information and monitoring information.



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

Tx Central Wavelength: Displays the nominal transmitter output wavelength in nm.

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

Temperature: Displays the internally measured transceiver temperature. Temperature accuracy is vendor specific but must be better than 3 degrees Celsius over specified operating temperature and voltage.

Vcc: Displays the internally measured transceiver supply voltage. Accuracy is vendor specific but must be better than 3 percent of the manufacturer's nominal value over specified operating temperature and voltage. Note that in some transceivers, transmitter supply voltage and receiver supply voltage are isolated. In that case, only one supply is monitored. Refer to the device specification for more detail.

Mon1 (Bias): Displays the measured TX bias current in uA. Accuracy is vendor specific but must be better than 10 percent of the manufacturer's nominal value over specified operating temperature and voltage.

Mon2 (TX PWR): Displays the measured coupled TX output power in mW. Accuracy is vendor specific but must be better than 3dB over specified operating temperature and voltage. Data is assumed to be based on measurement of a laser monitor photodiode current. Data is not valid when the transmitter is disabled.

Mon3 (RX PWR): Displays the measured received optical power in mW. Absolute accuracy is dependent upon the exact optical wavelength. For the vendor specified wavelength, accuracy should be better than 3dB over specified temperature and voltage. This accuracy should be maintained for input power levels up to the lesser of maximum transmitted or maximum received optical power per the appropriate standard. It should be maintained down to the minimum transmitted power minus cable plant loss (insertion loss or passive loss) per the appropriate standard. Absolute accuracy beyond this minimum required received input optical power range is vendor specific.

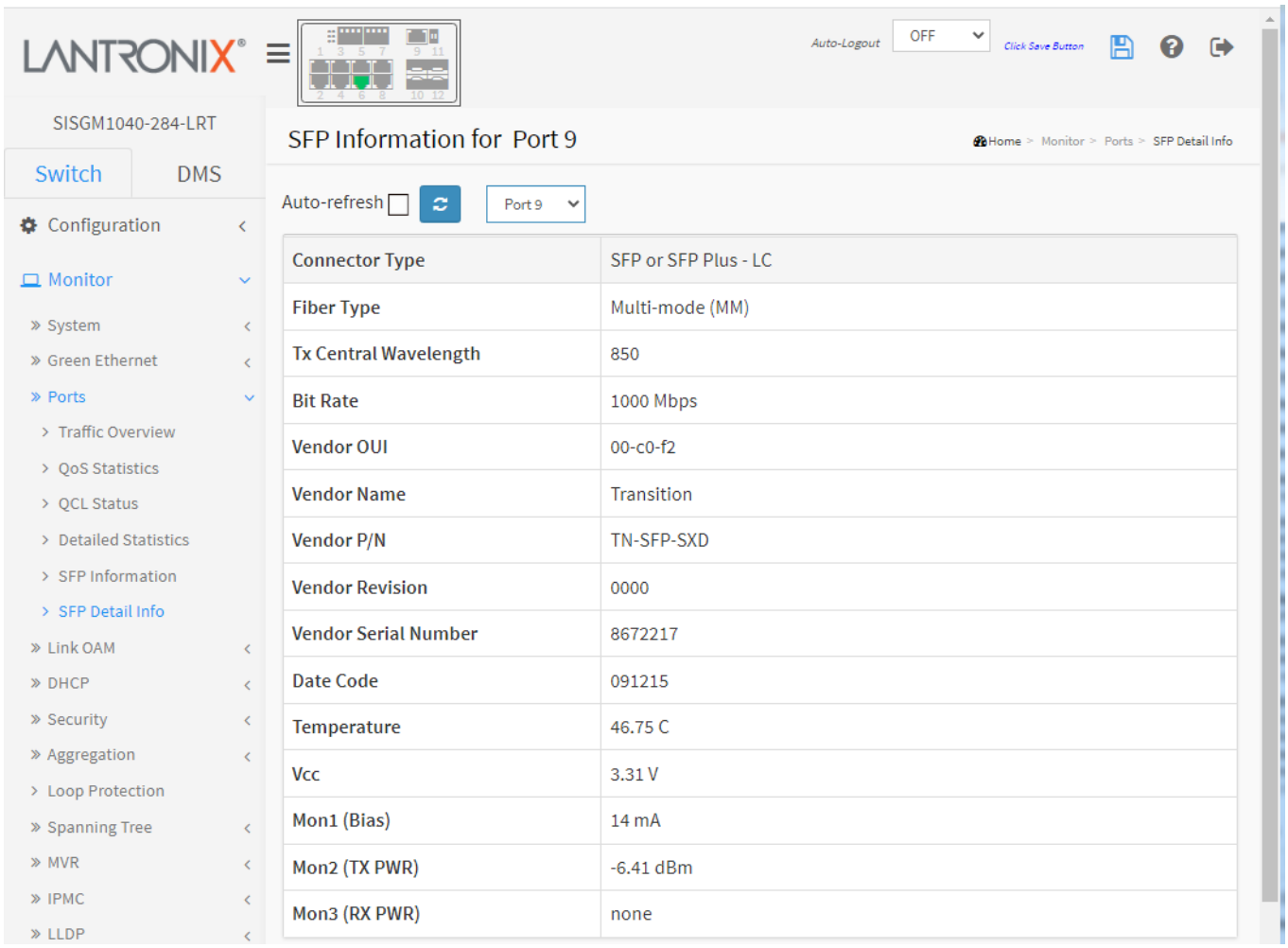
Buttons

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.

Monitor > Ports > SFP Detail Info

This page displays detailed SFP information and monitoring information.



Connector Type: Displays the external optical or electrical cable connector provided as the media interface.

Fiber Type: Displays the fiber channel transmission media.

Tx Central Wavelength: Displays the nominal transmitter output wavelength in nm.

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

Vendor OUI: Displays the vendor IEEE company ID (Organizationally Unique Identifier).

Vendor Name: Displays the vendor name.

Vendor P/N: Displays the vendor part number or product name.

Vendor Revision: Displays the vendor's product revision.

Vendor Serial Number: Displays the vendor serial number for the transceiver.

Date Code: Displays the vendor's manufacturing date code.

Temperature: Displays the internally measured transceiver temperature. Temperature accuracy is vendor specific but must be better than 3 degrees Celsius over specified operating temperature and voltage.

Vcc: Displays the internally measured transceiver supply voltage. Accuracy is vendor specific but must be better than 3 percent of the manufacturer's nominal value over specified operating temperature and voltage. Note that in some transceivers, transmitter supply voltage and receiver supply voltage are isolated. In that case, only one supply is monitored. Refer to the device specification for more detail.

Mon1 (Bias): Displays the measured TX bias current in uA. Accuracy is vendor specific but must be better than 10 percent of the manufacturer's nominal value over specified operating temperature and voltage.

Mon2 (TX PWR): Displays the measured coupled TX output power in mW. Accuracy is vendor specific but must be better than 3dB over specified operating temperature and voltage. Data is assumed to be based on measurement of a laser monitor photodiode current. Data is not valid when the transmitter is disabled.

Mon3 (RX PWR): Displays the measured received optical power in mW. Absolute accuracy is dependent upon the exact optical wavelength. For the vendor specified wavelength, accuracy should be better than 3dB over specified temperature and voltage. This accuracy should be maintained for input power levels up to the lesser of maximum transmitted or maximum received optical power per the appropriate standard. It should be maintained down to the minimum transmitted power minus cable plant loss (insertion loss or passive loss) per the appropriate standard. Absolute accuracy beyond this minimum required received input optical power range is vendor specific.

Buttons

: **Port select box** determines which port is affected by clicking the buttons.

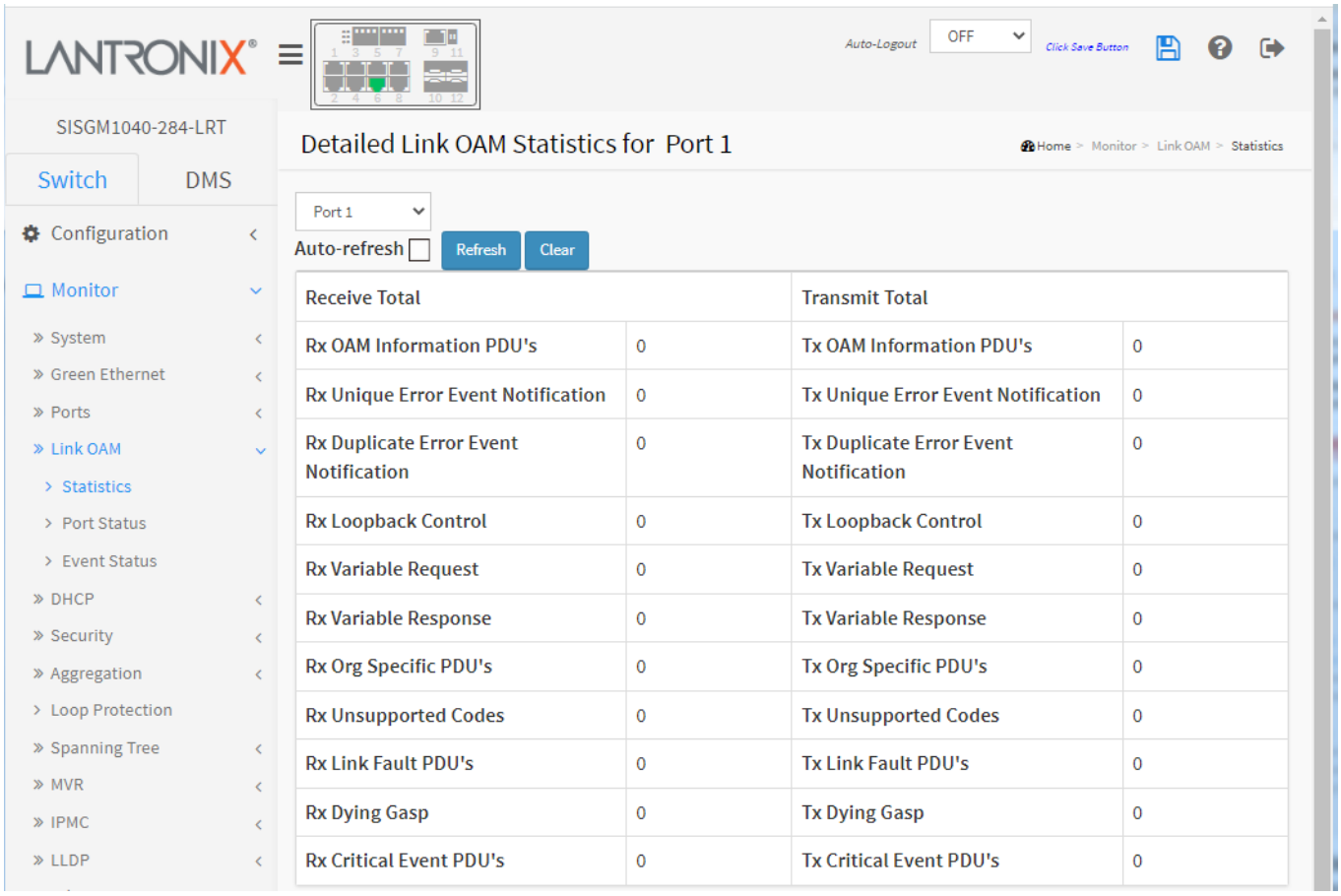
Refresh: Click to refresh the page. Any changes made locally will be undone.

Auto-refresh: Check this box to enable an automatic refresh of the page at regular intervals.

Monitor > Link OAM > Statistics

This page provides detailed OAM traffic statistics for a specific switch port. Use the port select box to select which switch port details to display.

The displayed counters represent the total number of OAM frames received and transmitted for the selected port. Discontinuities of these counter can occur at re-initialization of the management system.



Receive Total and Transmit Total

Rx and Tx OAM Information PDU's: The number of received and transmitted OAM Information PDU's. Discontinuities of this counter can occur at re-initialization of the management system.

Rx and Tx Unique Error Event Notification: A count of the number of unique Event OAMPDUs received and transmitted on this interface. Event Notifications may be sent in duplicate to increase the probability of successfully being received, given the possibility that a frame may be lost in transit. Duplicate Event Notification transmissions are counted by Duplicate Event Notification counters for Tx and Rx respectively. A unique Event Notification OAMPDU is indicated as an Event Notification OAMPDU with a Sequence Number field that is distinct from the previously transmitted Event Notification OAMPDU Sequence Number.

Rx and Tx Duplicate Error Event Notification: A count of the number of duplicate Event OAMPDUs received and transmitted on this interface. Event Notification OAMPDUs may be sent in duplicate to increase the probability of successfully being received, given the possibility that a frame may be lost in transit. A duplicate Event Notification OAMPDU is indicated as an Event Notification OAMPDU with a Sequence Number field that is identical to the previously transmitted Event Notification OAMPDU Sequence Number.

Rx and Tx Loopback Control: A count of the number of Loopback Control OAMPDUs received and transmitted on this interface.

Rx and Tx Variable Request: A count of the number of Variable Request OAMPDUs received and transmitted on this interface.

Rx and Tx Variable Response: A count of the number of Variable Response OAMPDUs received and transmitted on this interface.

Rx and Tx Org Specific PDU's: A count of the number of Organization Specific OAMPDUs transmitted on this interface.

Rx and Tx Unsupported Codes: A count of the number of OAMPDUs transmitted on this interface with an unsupported op-code.

Rx and Tx Link fault PDU's: A count of the number of Link fault PDU's received and transmitted on this interface.

Rx and Tx Dying Gasp: A count of the number of Dying Gasp events received and transmitted on this interface.

Rx and Tx Critical Event PDU's: A count of the number of Critical event PDU's received and transmitted on this interface.

Buttons

: **Port select box** determines which port is affected by clicking the buttons.

Auto-refresh: Check this box to enable an automatic refresh every 3 seconds.

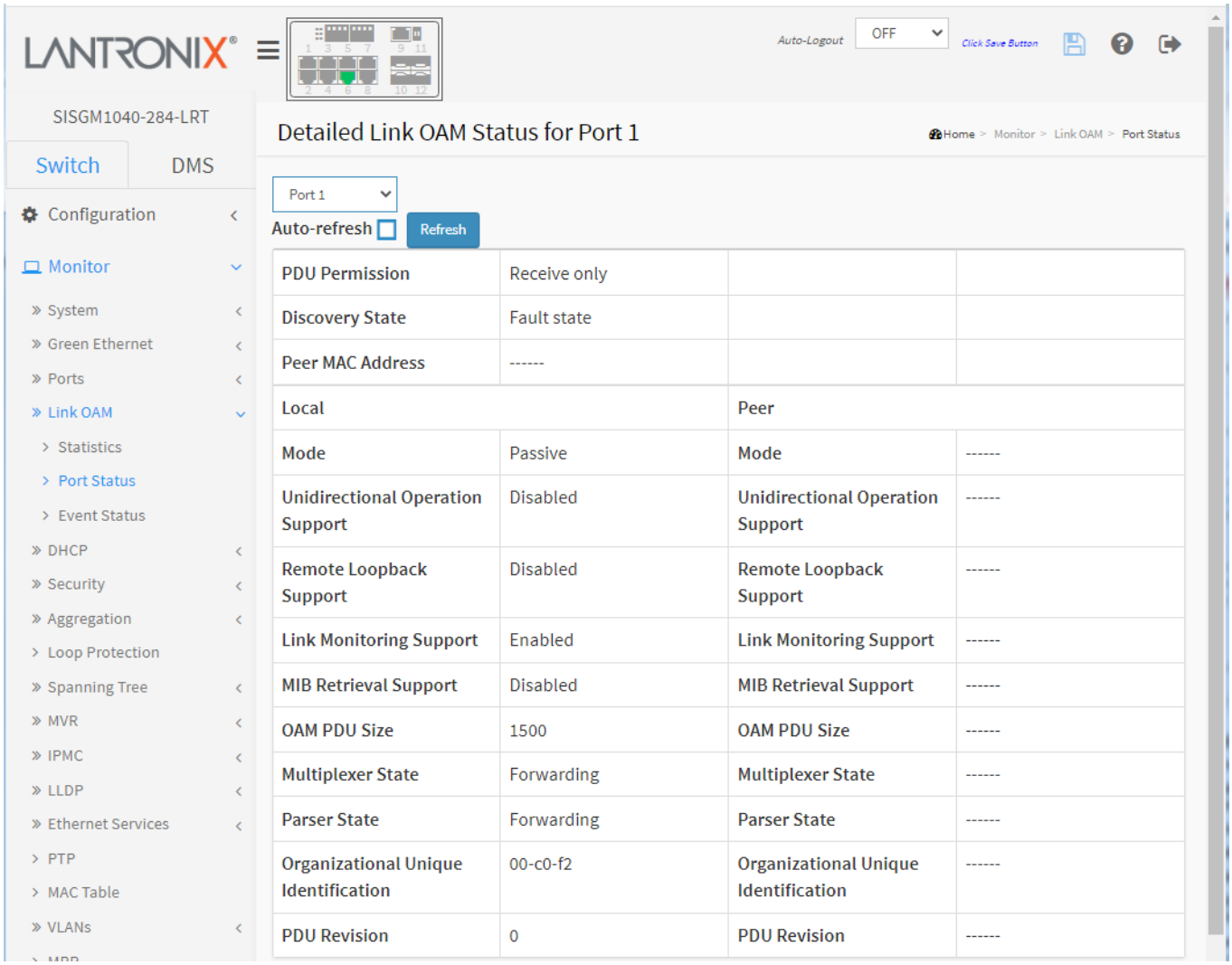
Refresh: Click to refresh the page immediately.

Clear: Clears the counters for the selected port.

Monitor > Link OAM > Port Status

This page provides Link OAM configuration operational status.

The displayed fields shows the active configuration status for the selected port.



PDU Permission: This field is available only for the Local DTE. It displays the current permission rules set for the local DTE. Possible values are "Link fault", "Receive only", "Information exchange only", or "ANY".

Discovery State: Displays the current state of the discovery process. Possible states are Fault state, Active state, Passive state, SEND_LOCAL_REMOTE_STATE, SEND_LOCAL_REMOTE_OK_STATE, SEND_ANY_STATE.

Peer MAC Address: The MAC address of the peer device if known, otherwise displays ----- .

Local and Peer

Mode: The Mode in which the Link OAM is operating, Active or Passive.

Unidirectional Operation Support: This feature is not available to be configured by the user. The status of this configuration is retrieved from the PHY.

Remote Loopback Support: If status is enabled, DTE is capable of OAM remote loopback mode.

Link Monitoring Support: If status is enabled, DTE supports interpreting Link Events.

MIB Retrieval Support: If status is for example enabled, DTE supports sending Variable Response OAMPDUs.

OAM PDU Size: It represents the largest OAMPDU, in octets, supported by the DTE. This value is compared to the remotes Maximum PDU Size and the smaller of the two is used.

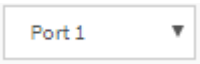
Multiplexer State: When in forwarding state, the Device is forwarding non-OAMPDUs to the lower sublayer. Incase of discarding, the device discards all the non-OAMPDU's.

Parser State: When in forwarding state, Device is forwarding non-OAMPDUs to higher sublayer. When in loopback, Device is looping back non-OAMPDUs to the lower sublayer. When in discarding state, Device is discarding non-OAMPDUs.

Organizational Unique Identification: 24-bit Organizationally Unique Identifier (OUI) of the vendor.

PDU Revision: It indicates the current revision of the Information TLV. The value of this field will start at zero and be incremented each time something in the Information TLV changes. On reception of an Information TLV from a peer, an OAM client may use this field to decide if it needs to be processed (an Information TLV that is identical to the previous Information TLV doesn't need to be parsed as nothing in it has changed).

Buttons



: **Port select box** determines which port is affected by clicking the buttons.

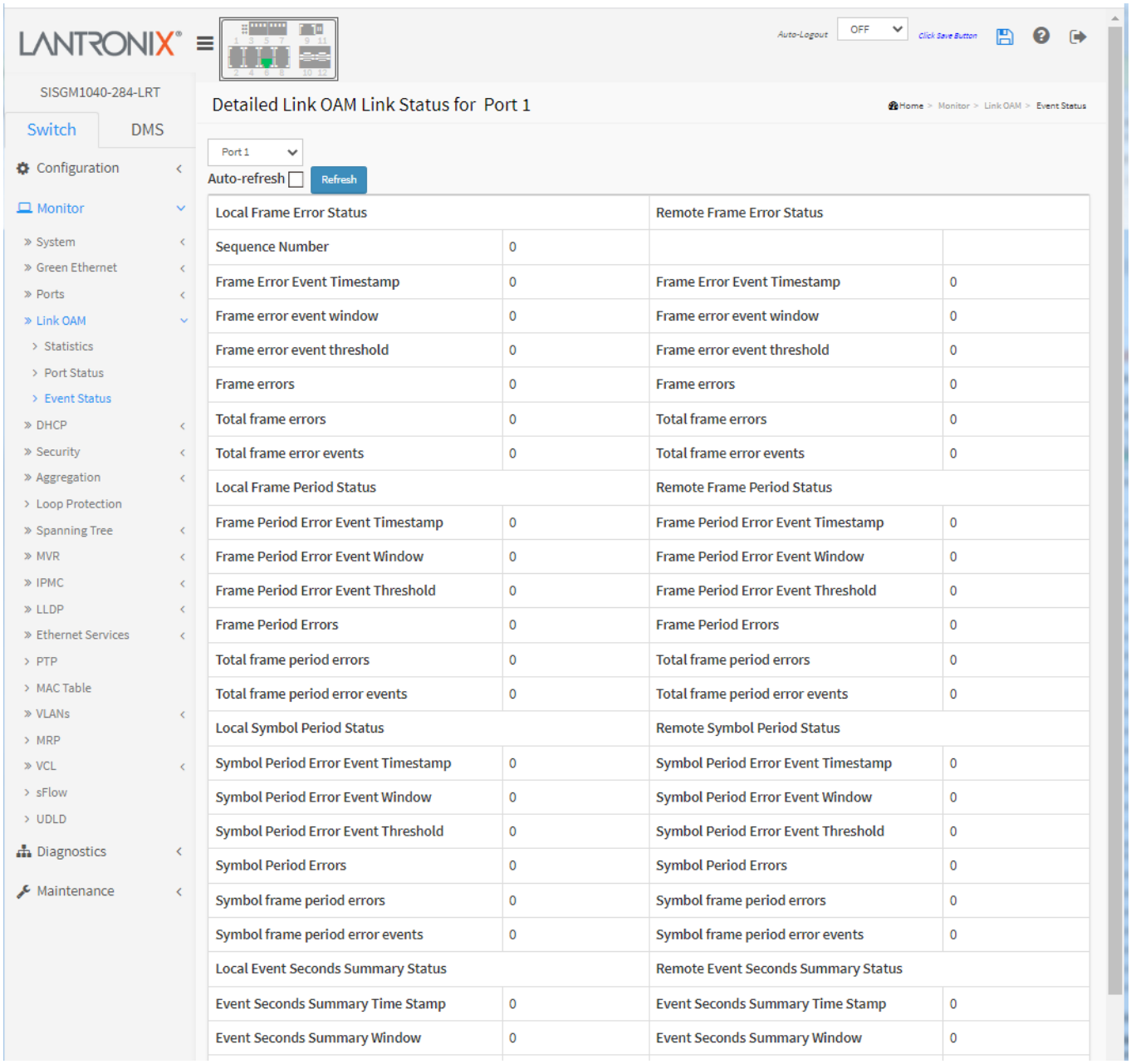
Refresh: Click to refresh the page immediately.

Auto-refresh: Check this box to enable an automatic refresh every 3 seconds.

Monitor > Link OAM > Event Status

This page lets you view the current Link OAM Link Event configurations.

The left pane displays the Event status for the Local OAM unit while the right pane displays the status for the Peer for the respective port.



Local Frame Error Status		Remote Frame Error Status	
Sequence Number	0		
Frame Error Event Timestamp	0	Frame Error Event Timestamp	0
Frame error event window	0	Frame error event window	0
Frame error event threshold	0	Frame error event threshold	0
Frame errors	0	Frame errors	0
Total frame errors	0	Total frame errors	0
Total frame error events	0	Total frame error events	0
Local Frame Period Status		Remote Frame Period Status	
Frame Period Error Event Timestamp	0	Frame Period Error Event Timestamp	0
Frame Period Error Event Window	0	Frame Period Error Event Window	0
Frame Period Error Event Threshold	0	Frame Period Error Event Threshold	0
Frame Period Errors	0	Frame Period Errors	0
Total frame period errors	0	Total frame period errors	0
Total frame period error events	0	Total frame period error events	0
Local Symbol Period Status		Remote Symbol Period Status	
Symbol Period Error Event Timestamp	0	Symbol Period Error Event Timestamp	0
Symbol Period Error Event Window	0	Symbol Period Error Event Window	0
Symbol Period Error Event Threshold	0	Symbol Period Error Event Threshold	0
Symbol Period Errors	0	Symbol Period Errors	0
Symbol frame period errors	0	Symbol frame period errors	0
Symbol frame period error events	0	Symbol frame period error events	0
Local Event Seconds Summary Status		Remote Event Seconds Summary Status	
Event Seconds Summary Time Stamp	0	Event Seconds Summary Time Stamp	0
Event Seconds Summary Window	0	Event Seconds Summary Window	0

Sequence Number: This two-octet field indicates the total number of events occurred at the remote end.

Frame Error Event Timestamp: This two-octet field indicates the time reference when the event was generated, in terms of 100 ms intervals.

Frame error event window: This two-octet field indicates the duration of the period in terms of 100 ms intervals. 1) The default value is one second. 2) The lower bound is one second. 3) The upper bound is one minute.

Frame error event threshold: This four-octet field indicates the number of detected errored frames in the period is required to be equal to or greater than in order for the event to be generated. 1) The default value is one frame error. 2) The lower bound is zero frame errors. 3) The upper bound is unspecified.

Frame errors: This four-octet field indicates the number of detected errored frames in the period.

Total frame errors: This eight-octet field indicates the sum of errored frames that have been detected since the OAM sublayer was reset.

Total frame error events: This four-octet field indicates the number of Errored Frame Event TLVs that have been generated since the OAM sublayer was reset.

Frame Period Error Event Timestamp: This two-octet field indicates the time reference when the event was generated, in terms of 100 ms intervals.

Frame Period Error Event Window: This four-octet field indicates the duration of period in terms of frames.

Frame Period Error Event Threshold: This four-octet field indicates the number of errored frames in the period is required to be equal to or greater than in order for the event to be generated.

Frame Period Errors: This four-octet field indicates the number of frame errors in the period.

Total frame period errors: This eight-octet field indicates the sum of frame errors that have been detected since the OAM sublayer was reset.

Total frame period error events: This four-octet field indicates the number of Errored Frame Period Event TLVs that have been generated since the OAM sublayer was reset.

Symbol Period Error Event Timestamp: This two-octet field indicates the time reference when the event was generated, in terms of 100 ms intervals.

Symbol Period Error Event Window: This eight-octet field indicates the number of symbols in the period.

Symbol Period Error Event Threshold: This eight-octet field indicates the number of errored symbols in the period is required to be equal to or greater than in order for the event to be generated.

Symbol Period Errors: This eight-octet field indicates the number of symbol errors in the period.

Symbol frame period errors: This eight-octet field indicates the sum of symbol errors since the OAM sublayer was reset.

Symbol frame period error events: This four-octet field indicates the number of Errored Symbol Period Event TLVs that have been generated since the OAM sublayer was reset.

Event Seconds Summary Time Stamp: This two-octet field indicates the time reference when the event was generated, in terms of 100 ms intervals, encoded as a 16-bit unsigned integer.

Event Seconds Summary Window: This two-octet field indicates the duration of the period in terms of 100 ms intervals, encoded as a 16-bit unsigned integer.

Event Seconds Summary Threshold: This two-octet field indicates the number of errored frame seconds in the period is required to be equal to or greater than in order for the event to be generated, encoded as a 16-bit unsigned integer.

Event Seconds Summary Events: This two-octet field indicates the number of errored frame seconds in the period, encoded as a 16-bit unsigned integer.

Event Seconds Summary Error Total: This four-octet field indicates the sum of errored frame seconds that have been detected since the OAM sublayer was reset.

Event Seconds Summary Event Total: This four-octet field indicates the number of Errored Frame Seconds Summary Event TLVs that have been generated since the OAM sublayer was reset, encoded as a 32bit unsigned integer.

Buttons

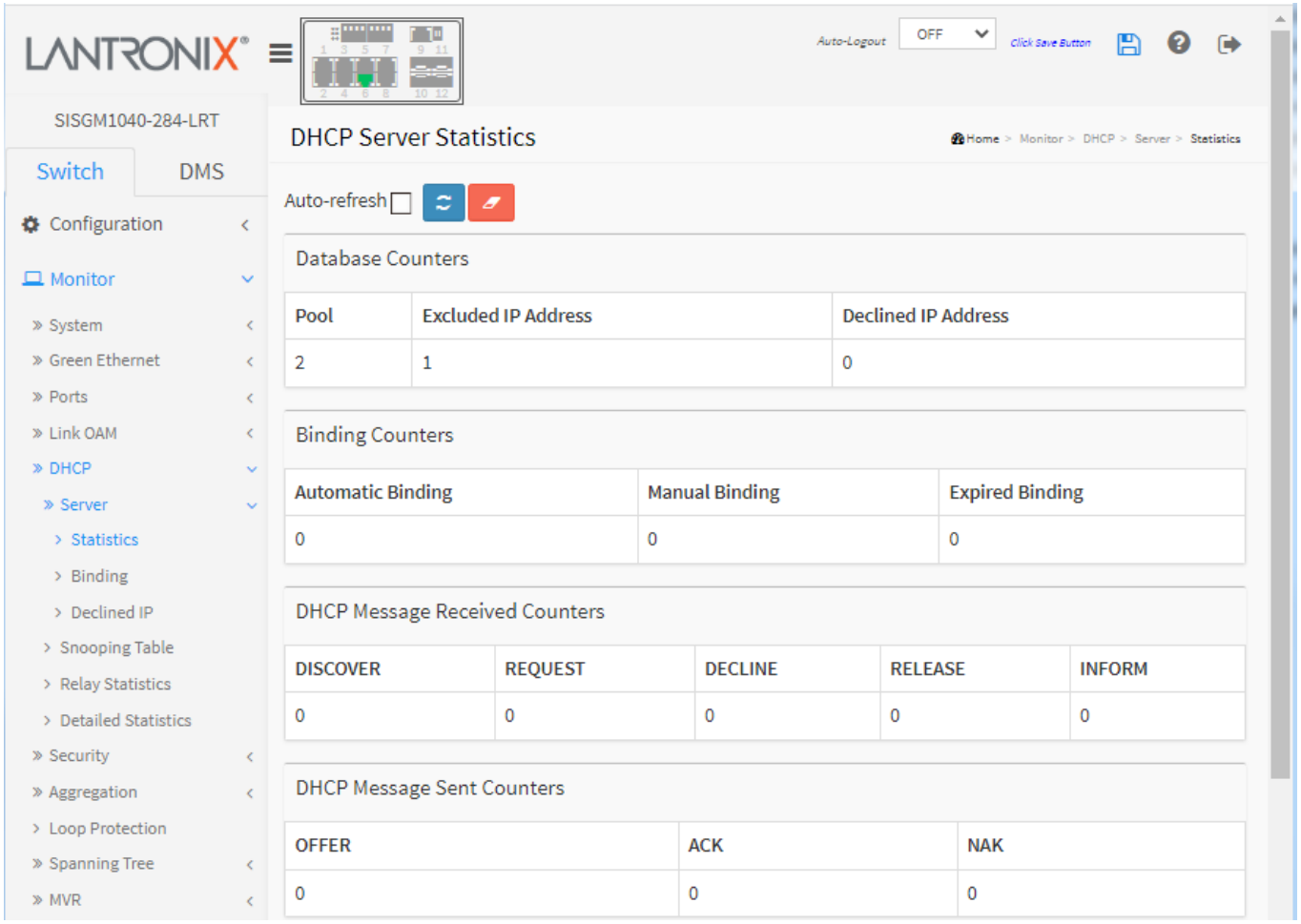
: **Port select box** determines which port is affected by clicking the buttons.

Auto-refresh: Check this box to enable an automatic refresh every 3 seconds.

Refresh: Click to refresh the page.

Monitor > DHCP > Server > Statistics

This page displays the database counters and the number of DHCP messages sent and received by DHCP server.



Database Counters: Display counters of various databases.

Pool: Number of pools.

Excluded IP Address: Number of excluded IP address ranges.

Declined IP Address: Number of declined IP addresses.

Binding Counters: Display counters of various databases.

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: Display counters of DHCP messages received by a DHCP server.

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: Display counters of DHCP messages sent by DHCP server.

OFFER: Number of DHCP OFFER messages sent.

ACK: Number of DHCP ACK messages sent.

NAK: Number of DHCP NAK messages sent.

Buttons

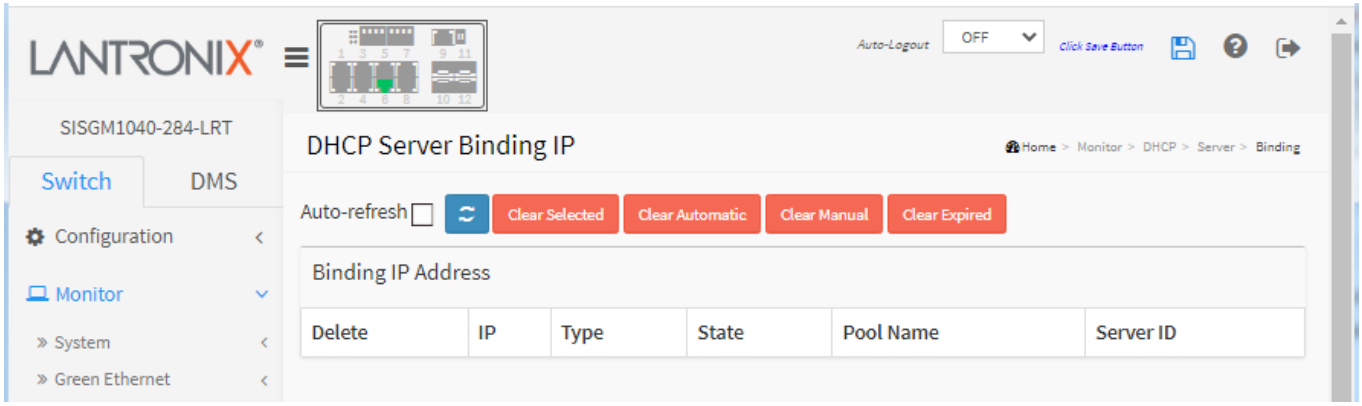
Auto-refresh: Check this box to refresh the page automatically every 3 seconds.

Refresh: Click to refresh the page immediately.

Clear: Click to Clears DHCP Message Received Counters and DHCP Message Sent Counters.

Monitor > DHCP > Server > Binding

This page displays bindings generated for DHCP clients.



Binding IP Address: Display all bindings.

IP: IP address allocated to DHCP client.

Type: Type of binding. Possible types are Automatic, Manual, Expired.

State: State of binding. Possible states are Committed, Allocated, Expired.

Pool Name: The pool that generates the binding.

Server ID: Server IP address to service the binding.

Buttons

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

Refresh: Click to refresh the page immediately.

Clear Selected: Click to clear selected bindings. If the selected binding is Automatic or Manual, then it is changed to be Expired. If the selected binding is Expired, then it is freed.

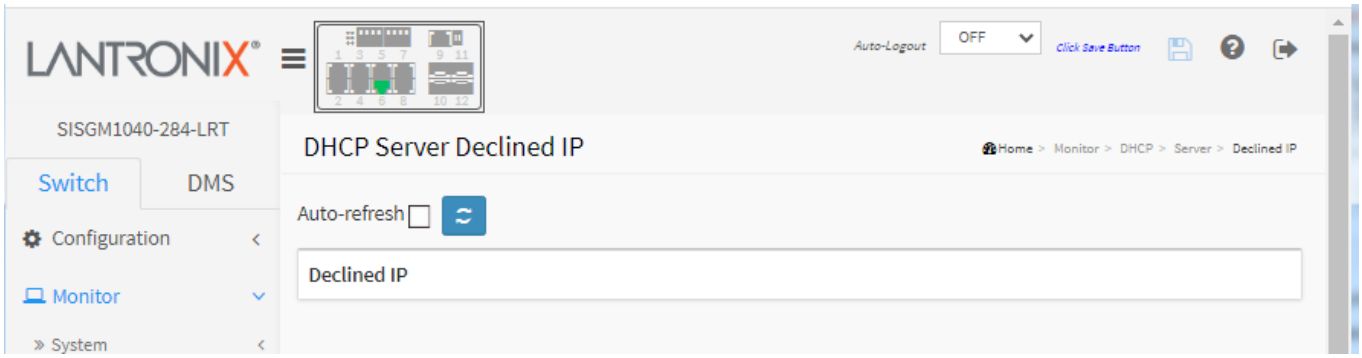
Clear Automatic: Click to clear all Automatic bindings and Change them to Expired bindings.

Clear Manual: Click to clear all Manual bindings and change them to Expired bindings.

Clear Expired: Click to clear all Expired bindings and free them.

Monitor > DHCP > Server > Declined IP

This page displays declined IP addresses.



DHCP Server Declined IP: Display IP addresses declined by DHCP clients.

Declined IP: List of IP addresses declined.

Buttons

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

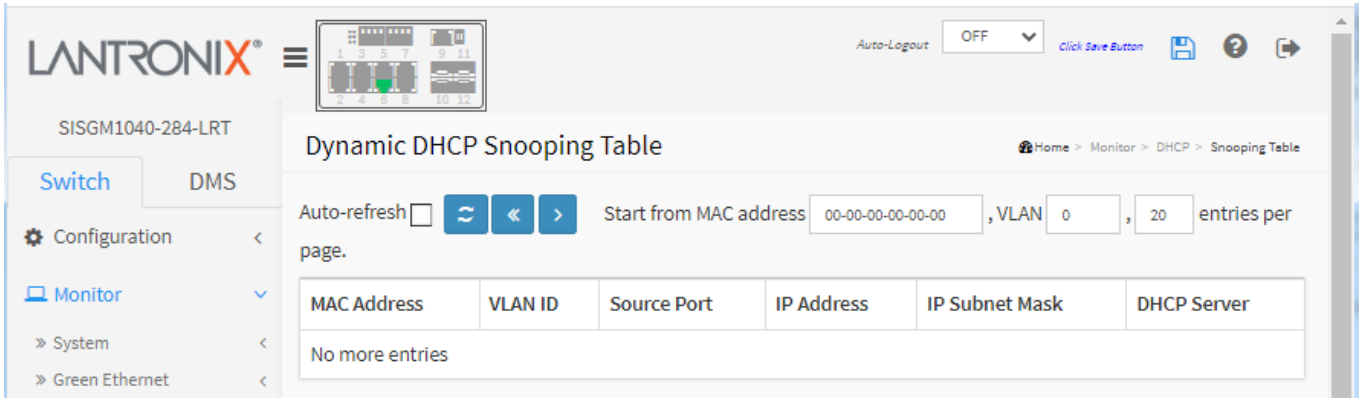
Refresh: Click to refresh the page immediately.

Monitor > DHCP > Snooping Table

This page display the dynamic IP assigned information after DHCP Snooping mode is disabled. All DHCP clients obtained the dynamic IP address from the DHCP server will be listed in this table except for local VLAN interface IP addresses. Entries in the Dynamic DHCP snooping Table are shown on this page.

Each page shows up to 99 entries from the Dynamic DHCP snooping 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 DHCP snooping Table.

The "MAC address" and "VLAN" input fields allows the user to select the starting point in the Dynamic DHCP snooping Table.



MAC Address: User MAC address of the entry.

VLAN ID: The VLAN ID in which the DHCP traffic is permitted.

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

IP Address: User IP address of the entry.

IP Subnet Mask: User IP subnet mask of the entry.

DHCP Server Address: DHCP Server address of the entry.

Buttons

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

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

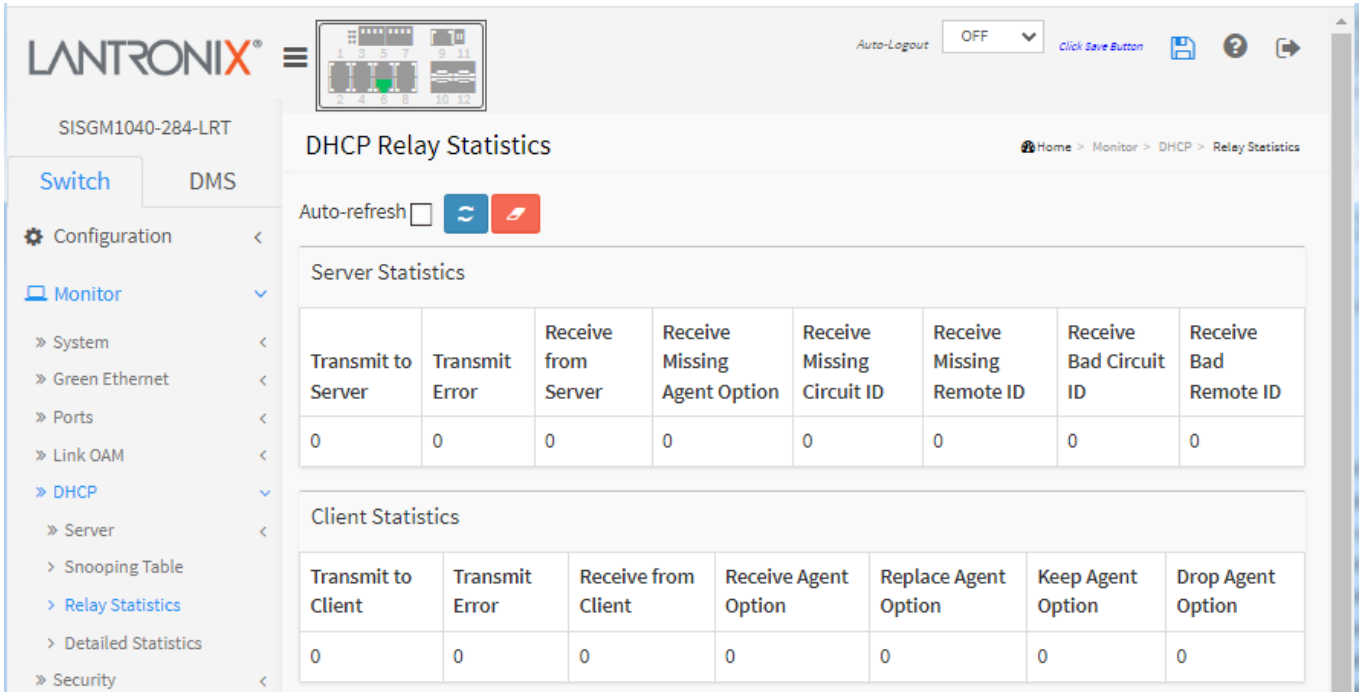
Clear: Flushes all dynamic entries.

<< : Updates the table starting from the first entry in the Dynamic DHCP Snooping Table.

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

Monitor > DHCP > Relay Statistics

This page provides statistics for DHCP relay.



Server Statistics

Transmit to Server: The number of packets that are relayed from client to server.

Transmit Error: The number of packets that resulted in errors while being sent to clients.

Receive from Server: The number of packets received from server.

Receive Missing Agent Option: The number of packets received without agent information options.

Receive Missing Circuit ID: The number of packets received with the Circuit ID option missing.

Receive Missing Remote ID: The number of packets received with the Remote ID option missing.

Receive Bad Circuit ID: The number of packets whose Circuit ID option did not match known circuit ID.

Receive Bad Remote ID: The number of packets whose Remote ID option did not match known Remote ID.

Client Statistics

Transmit to Client: The number of relayed packets from server to client.

Transmit Error: The number of packets that resulted in error while being sent to servers.

Receive from Client: The number of received packets from server.

Receive Agent Option: The number of received packets with relay agent information option.

Replace Agent Option: The number of packets which were replaced with relay agent information option.

Keep Agent Option: The number of packets whose relay agent information was retained.

Drop Agent Option: The number of packets that were dropped which were received with relay agent information.

Buttons

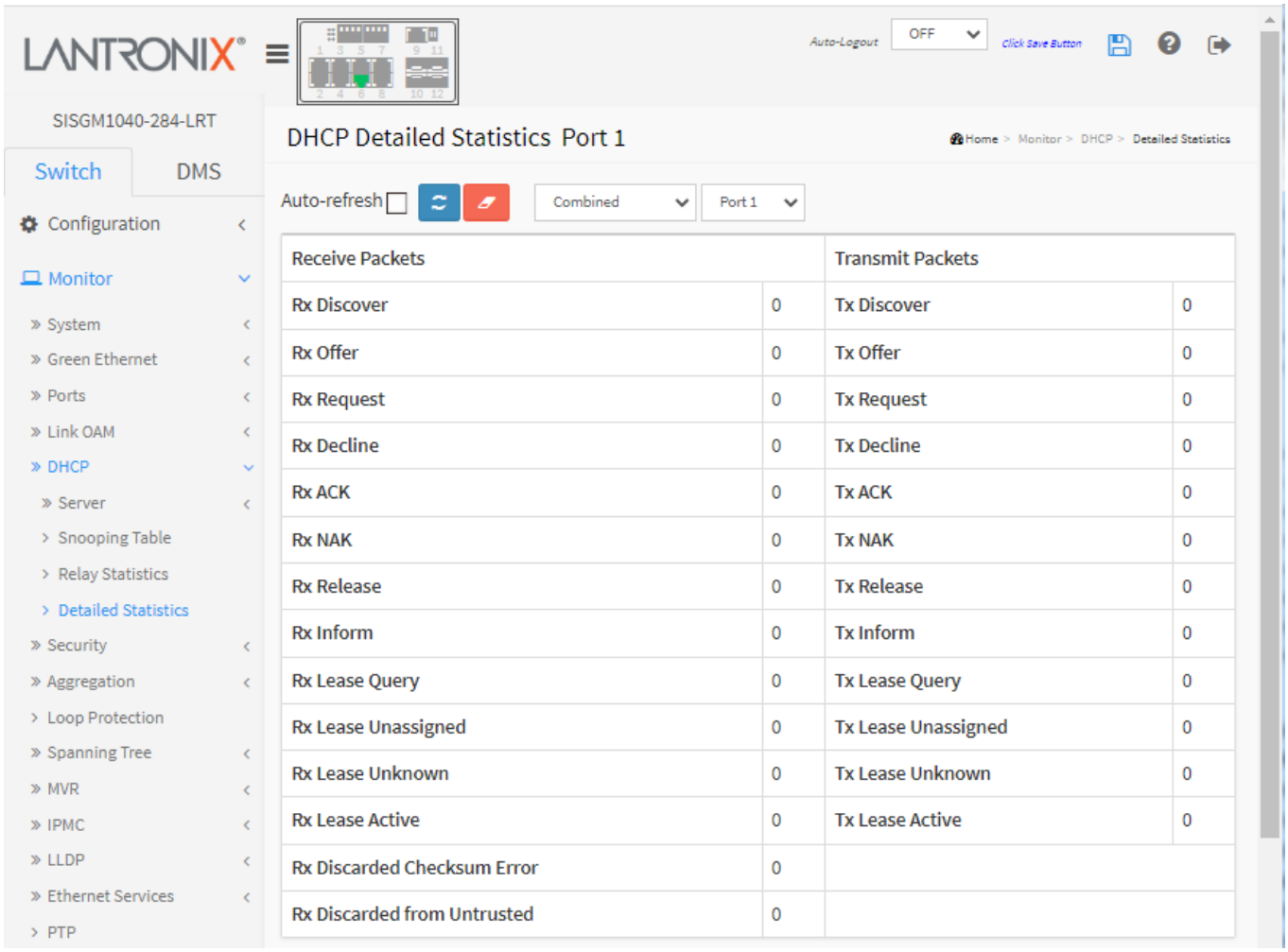
Auto-refresh: Check this box to refresh the page automatically every 3 seconds.

Refresh: Click to refresh the page immediately.

Clear: Clear all statistics.

Monitor > DHCP > Detailed Statistics

This page provides statistics for DHCP snooping. Notice that the normal forward per-port TX statistics isn't increased if the incoming DHCP packet is done by L3 forwarding mechanism. Any clear of the statistics on a specific port may not take effect on global statistics since it gathers the different layer overview.



Receive and Transmit Packets

Rx and Tx Discover: The number of discover (option 53 with value 1) packets received and transmitted.

Rx and Tx Offer: The number of offer (option 53 with value 2) packets received and transmitted.

Rx and Tx Request: The number of request (option 53 with value 3) packets received and transmitted.

Rx and Tx Decline: The number of decline (option 53 with value 4) packets received and transmitted.

Rx and Tx ACK: The number of ACK (option 53 with value 5) packets received and transmitted.

Rx and Tx NAK: The number of NAK (option 53 with value 6) packets received and transmitted.

Rx and Tx Release: The number of release (option 53 with value 7) packets received and transmitted.

Rx and Tx Inform: The number of inform (option 53 with value 8) packets received and transmitted.

Rx and Tx Lease Query: The number of lease query (option 53 with value 10) packets received and transmitted.

Rx and Tx Lease Unassigned: The number of lease unassigned (option 53 with value 11) packets received and transmitted.

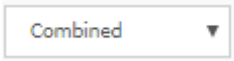
Rx and Tx Lease Unknown: The number of lease unknown (option 53 with value 12) packets received and transmitted.

Rx and Tx Lease Active: The number of lease active (option 53 with value 13) packets received and transmitted.

Rx Discarded checksum error: The number of discard packet that IP/UDP checksum is error.

Rx Discarded from Untrusted: The number of discarded packets that are coming from untrusted port.

Buttons



: **DHCP user select box** determines which user is affected by clicking the buttons.

: **Port select box** determines which port is affected by clicking the buttons.

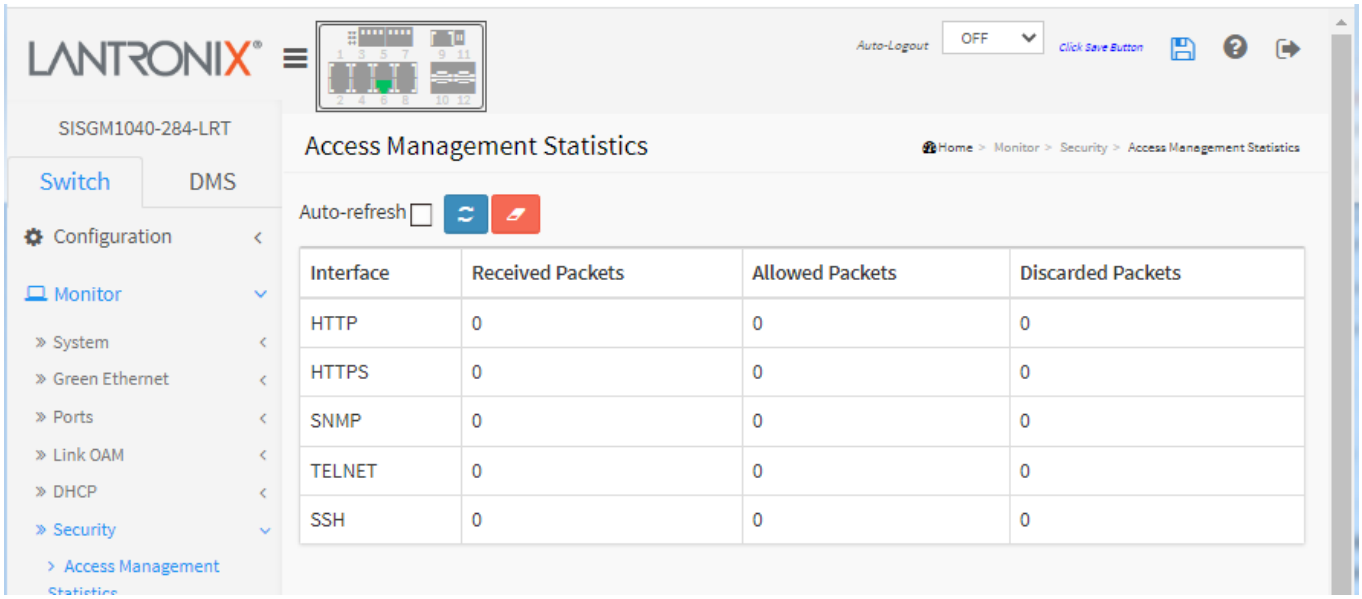
Auto-refresh: Check this box to refresh the page automatically every 3 seconds.

Refresh: Click to refresh the page immediately.


: **Clears** the counters for the selected port.

Monitor > Security > Access Management Statistics

This page provides statistics for access management.



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.

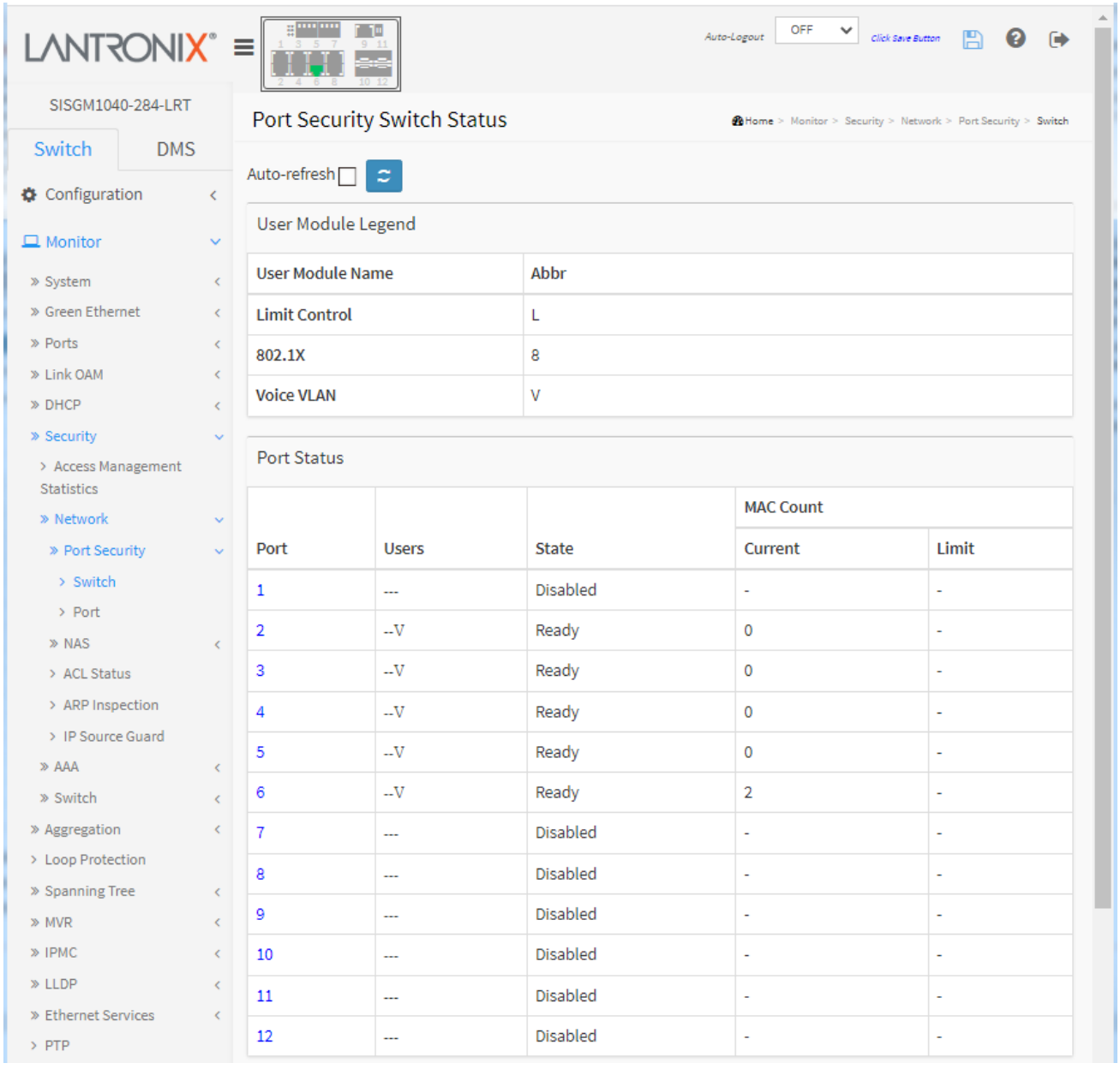
Refresh: Click to refresh the page immediately.

Clear: Clear all statistics.

Monitor > Security > Network > Port Security > Switch

This page shows the Port Security status. Port Security is a module with no direct configuration. Configuration comes indirectly from other modules - the user modules. When a user module has enabled port security on a port, the port is set-up for software-based learning. In this mode, frames from unknown MAC addresses are passed on to the port security module, which in turn asks all user modules whether to allow this new MAC address to forward or block it. For a MAC address to be set in the forwarding state, all enabled user modules must unanimously agree on allowing the MAC address to forward. If only one chooses to block it, it will be blocked until that user module decides otherwise.

The status page is divided into two sections - one with a legend of user modules and one with the actual port status.



User Module Legend: The legend shows all user modules that may request Port Security services.

User Module Name: The full name of a module that may request Port Security services.

Abbr: A one-letter abbreviation of the user module. This is used in the Users column in the port status table.

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

Port: The port number for which the status applies. Click the port number to see the status for this port.

Users: Each of the user modules has a column that shows whether that module has enabled Port Security or not. A '-' means that the corresponding user module is not enabled, whereas a letter indicates that the user module abbreviated by that letter (see “Abbr” above) 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 webpage.

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 (-).

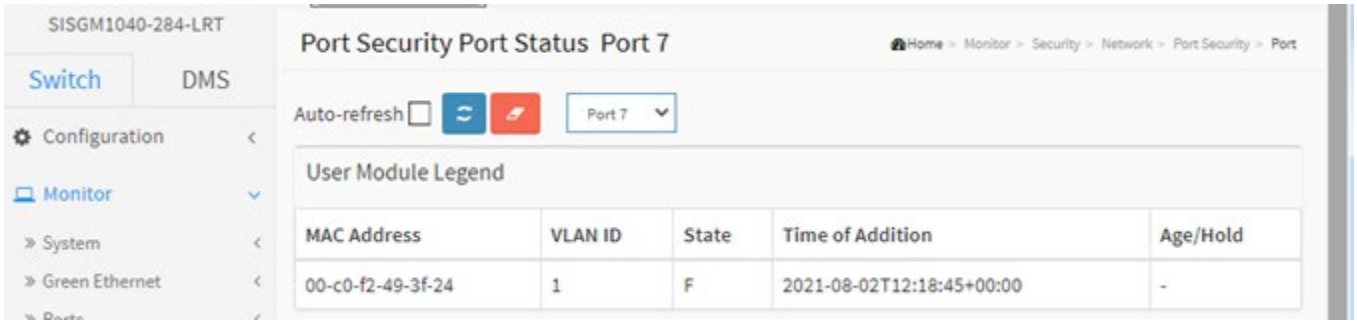
Buttons

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

Refresh: Click to refresh the page immediately.

Monitor > Security > Network > Port Security > Port

This page shows the MAC addresses secured by the Port Security module. Port Security is a module with no direct configuration. Configuration comes indirectly from other modules - the user modules. When a user module has enabled port security on a port, the port is set-up for software-based learning. In this mode, frames from unknown MAC addresses are passed on to the port security module, which in turn asks all user modules whether to allow this new MAC address to forward or block it. For a MAC address to be set in the forwarding state, all enabled user modules must unanimously agree on allowing the MAC address to forward. If only one chooses to block it, it will be blocked until that user module decides otherwise.



MAC Address & **VLAN ID**: The MAC address and VLAN ID that is seen on this port. If no MAC addresses are learned, a single row stating "*No MAC addresses attached*" is displayed.

State: Indicates whether the corresponding MAC address is blocked or forwarding. In the blocked state, it will not be allowed to transmit or receive traffic.

Time of Addition: Shows the date and time when this MAC address was first seen on the port.

Age/Hold: If at least one user module has decided to block this MAC address, it will stay in the blocked state until the hold time (measured in seconds) expires. If all user modules have decided to allow this MAC address to forward, and aging is enabled, the Port Security module will periodically check that this MAC address still forwards traffic. If the age period (measured in seconds) expires and no frames have been seen, the MAC address will be removed from the MAC table. Otherwise a new age period will begin.

If aging is disabled or a user module has decided to hold the MAC address indefinitely, a dash (-) will be shown.

Buttons

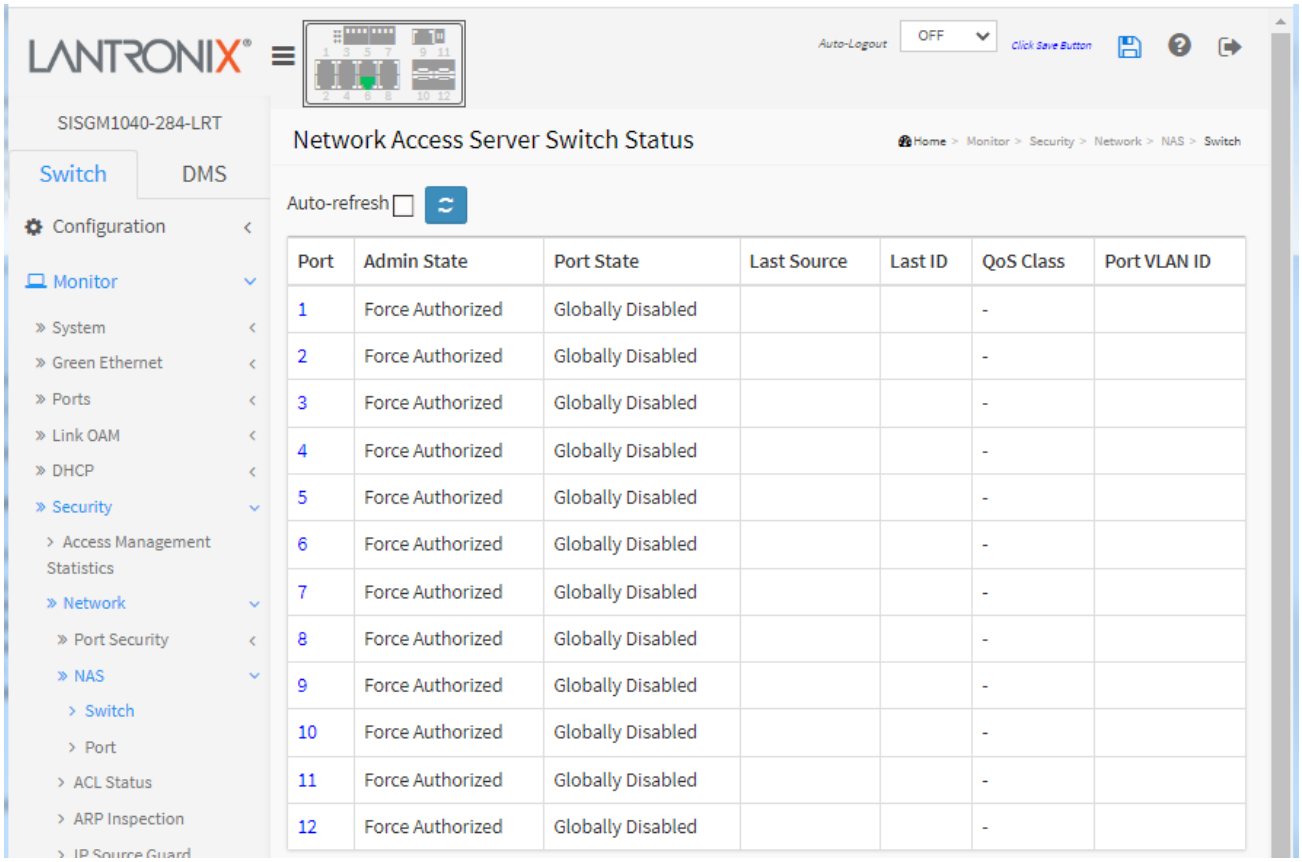
Port select box: Use to select which port to show status for.

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

Refresh: Click to refresh the page immediately.

Monitor > Security > Network > NAS > Switch

This page provides an overview of the current NAS port states.



Port: The switch port number. Click to navigate to detailed NAS statistics for this port.

Admin State: The port's current administrative state. See NAS Admin State for a description of possible values.

Port State: The current state of the port. Refer to NAS Port State for a description of the individual states.

Last Source: The source MAC address carried in the most recently received EAPOL frame for EAPOL-based authentication, and the most recently received frame from a new client for MAC-based authentication.

Last ID: The user name (supplicant identity) carried in the most recently received Response Identity EAPOL frame for EAPOL-based authentication, and the source MAC address from the most recently received frame from a new client for MAC-based authentication.

QoS Class: QoS Class assigned to the port by the RADIUS server if enabled.

Port VLAN ID: The VLAN ID that NAS has put the port in. The field is blank if the Port VLAN ID is not overridden by NAS. If the VLAN ID is assigned by the RADIUS server, "(RADIUS-assigned)" is appended to the VLAN ID. Read more about RADIUS-assigned VLANs here. If the port is moved to the Guest VLAN, "(Guest)" is appended to the VLAN ID. Read more about Guest VLANs here.

Buttons

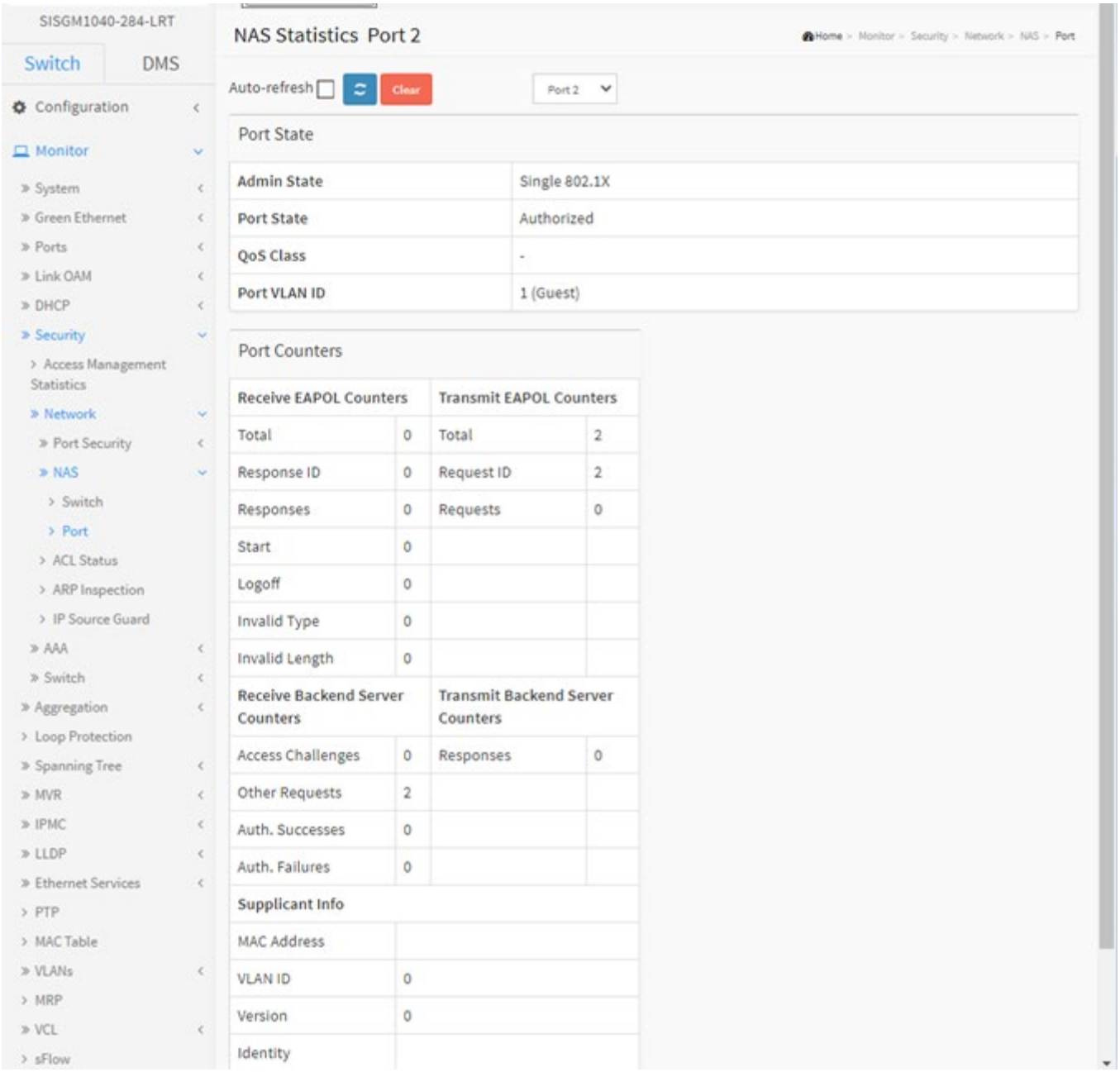
Auto-refresh: Check this box to refresh the page automatically every 3 seconds.

Refresh: Click to refresh the page immediately.

Monitor > Security > Network > NAS > Port

This page provides detailed NAS statistics for a specific switch port running EAPOL-based IEEE 802.1X authentication. For MAC-based ports, it shows selected backend server (RADIUS Authentication Server) statistics, only .

Use the port select box to select which port details to be displayed.



Port State

Admin State: The port's current administrative state. Refer to NAS Admin State for a description of possible values.

Port State: The current state of the port. Refer to NAS Port State for a description of the individual states.

QoS Class: The QoS class assigned by the RADIUS server. The field is blank if no QoS class is assigned.

Port VLAN ID: The VLAN ID that NAS has put the port in. The field is blank, if the Port VLAN ID is not overridden by NAS.

If the VLAN ID is assigned by the RADIUS server, "(RADIUS-assigned)" is appended to the VLAN ID. Read more about RADIUS-assigned VLANs here.

If the port is moved to the Guest VLAN, "(Guest)" is appended to the VLAN ID. Read more about Guest VLANs here.

Port Counters

EAPOL Counters

These supplicant frame counters are available for these administrative states: Force Authorized, Force Unauthorized, Port-based 802.1X, Single 802.1X, Multi 802.1X.

EAPOL Counters			
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.

Backend Server Counters			
Direction	**Name**	**IEEE Name**	**Description**
Rx	Access Challenges	dot1xAuthBackendAccessChallenges	**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	dot1xAuthBackendOtherRequestsToSupplicant	**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	dot1xAuthBackendAuthSuccesses	**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 these administrative states: Port-based 802.1X, Single 802.1X, Multi 802.1X, MAC-based Auth.

Last Supplicant/Client Info		
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 either Multi 802.1X or MAC-based Auth. admin state. The table is identical to and is placed next to the Port Counters table and will be empty if no MAC address is currently selected. To populate the table, select one of the attached MAC Addresses from the table below.

Attached MAC Addresses

Identity: Shows the identity of the supplicant, as received in the Response Identity EAPOL frame.
Clicking the link causes the supplicant's EAPOL and Backend Server counters to be shown in the Selected Counters table. If no supplicants are attached, it shows No supplicants attached.
This column is not available for MAC-based Auth.

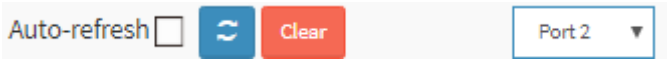
MAC Address: For Multi 802.1X, this column holds the MAC address of the attached supplicant.
For MAC-based Auth., this column holds the MAC address of the attached client.
Clicking the link causes the client's Backend Server counters to be shown in the Selected Counters table. If no clients are attached, it shows No clients attached.

VLAN ID: This column holds the VLAN ID that the corresponding client is currently secured through the Port Security module.

State: The client can either be authenticated or unauthenticated. In the authenticated state, it is allowed to forward frames on the port, and in the unauthenticated state, it is blocked. As long as the backend server hasn't successfully authenticated the client, it is unauthenticated. If an authentication fails for one or the other reason, the client will remain in the unauthenticated state for Hold Time seconds.

Last Authentication: Shows the date and time of the last authentication of the client (successful as well as unsuccessful).

Buttons



Port select box: determines which port is affected when clicking the buttons.

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

Refresh: Click to refresh the page immediately.

Clear: Click to clear the counters for the selected port. This button is available in the following modes:

- Force Authorized
- Force Unauthorized
- Port-based 802.1X
- Single 802.1X

Clear All: Click to clear both the port counters and all of the attached client's counters. The "Last Client" will not be cleared, however. This button is available in the following modes:

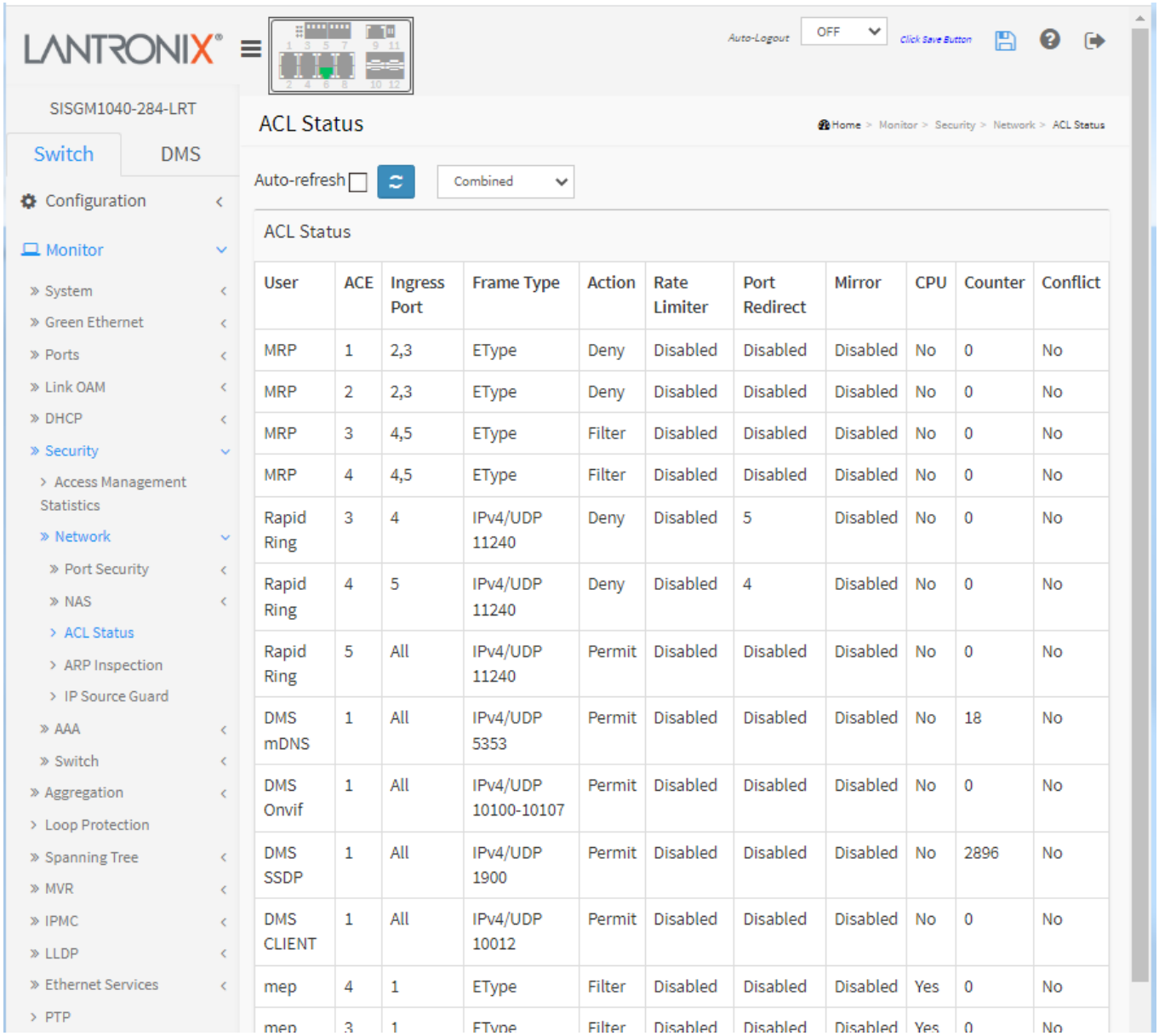
- Multi 802.1X
- MAC-based Auth.X

Clear This: Click to clear only the currently selected client's counters. This button is available in the following modes:

- Multi 802.1X
- MAC-based Auth.X

Monitor > Security > Network > ACL Status

This page shows the ACL status of different ACL users. Each row describes an ACE that is defined. It is a 'Conflict' if a specific ACE is not applied to the hardware due to hardware limitations. The maximum number of ACEs is 256 per switch.



User	ACE	Ingress Port	Frame Type	Action	Rate Limiter	Port Redirect	Mirror	CPU	Counter	Conflict
MRP	1	2,3	EType	Deny	Disabled	Disabled	Disabled	No	0	No
MRP	2	2,3	EType	Deny	Disabled	Disabled	Disabled	No	0	No
MRP	3	4,5	EType	Filter	Disabled	Disabled	Disabled	No	0	No
MRP	4	4,5	EType	Filter	Disabled	Disabled	Disabled	No	0	No
Rapid Ring	3	4	IPv4/UDP 11240	Deny	Disabled	5	Disabled	No	0	No
Rapid Ring	4	5	IPv4/UDP 11240	Deny	Disabled	4	Disabled	No	0	No
Rapid Ring	5	All	IPv4/UDP 11240	Permit	Disabled	Disabled	Disabled	No	0	No
DMS mDNS	1	All	IPv4/UDP 5353	Permit	Disabled	Disabled	Disabled	No	18	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	2896	No
DMS CLIENT	1	All	IPv4/UDP 10012	Permit	Disabled	Disabled	Disabled	No	0	No
mep	4	1	EType	Filter	Disabled	Disabled	Disabled	Yes	0	No
mep	3	1	EType	Filter	Disabled	Disabled	Disabled	Yes	0	No

User: Indicates the ACL user (e.g., MEP, DMS CLIENT, Rapid Ring, etc.).

ACE: Indicates the ACE ID on local switch.

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

All: The ACE will match all ingress port.

Port: The ACE will match a specific ingress port 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 redirect operation of the ACE. Frames matching the ACE are redirected to the port number. The allowed values are Disabled or a specific port number. When Disabled is displayed, the port redirect operation is disabled.

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

Enabled: Frames received on the port are mirrored.

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

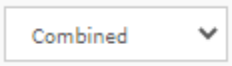
CPU: Forward packet that matched the specific ACE to CPU.

CPU Once: Forward first packet that matched the specific ACE to CPU.

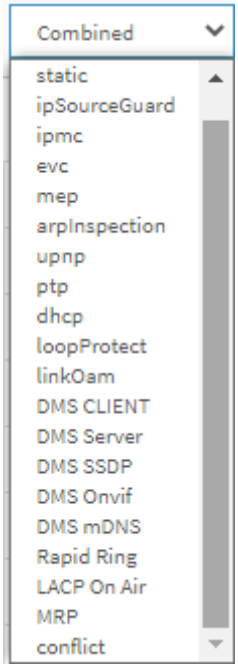
Counter: The counter indicates the number of times the ACE was hit by a frame.

Conflict: Indicates the hardware status of the specific ACE. The specific ACE is not applied to the hardware due to hardware limitations.

Buttons



User select box: determines which ACL user (e.g., static, Combined, ipmc, mep, etc.) has its information displayed on the page. The default is 'Combined' (all user's information displayed together).



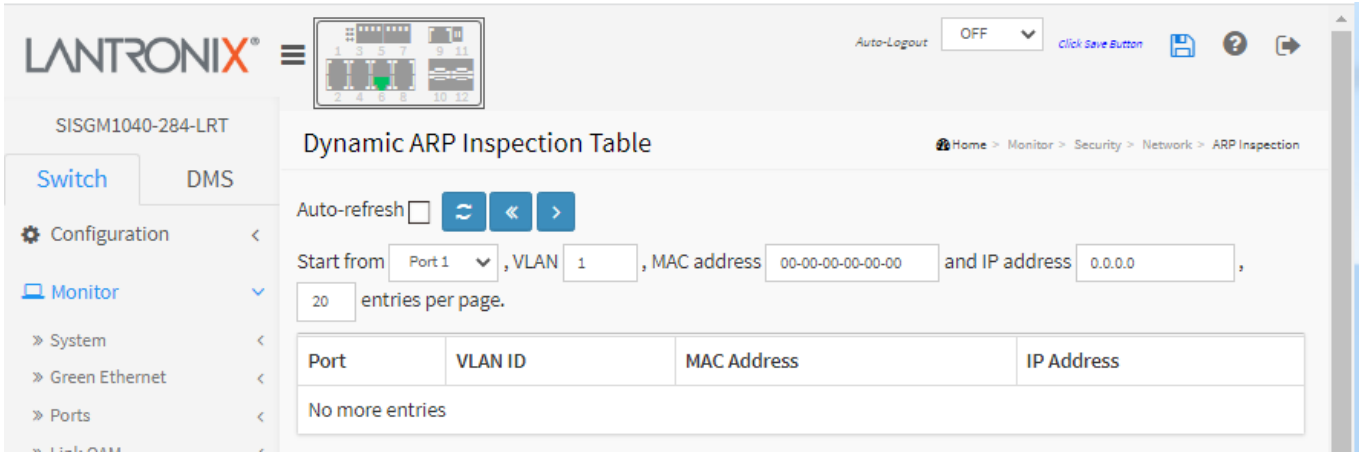
Auto-refresh: Check this box to refresh the page automatically every 3 seconds.

Refresh: Click to refresh the page.

Monitor > Security > Network > ARP Inspection

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.



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.

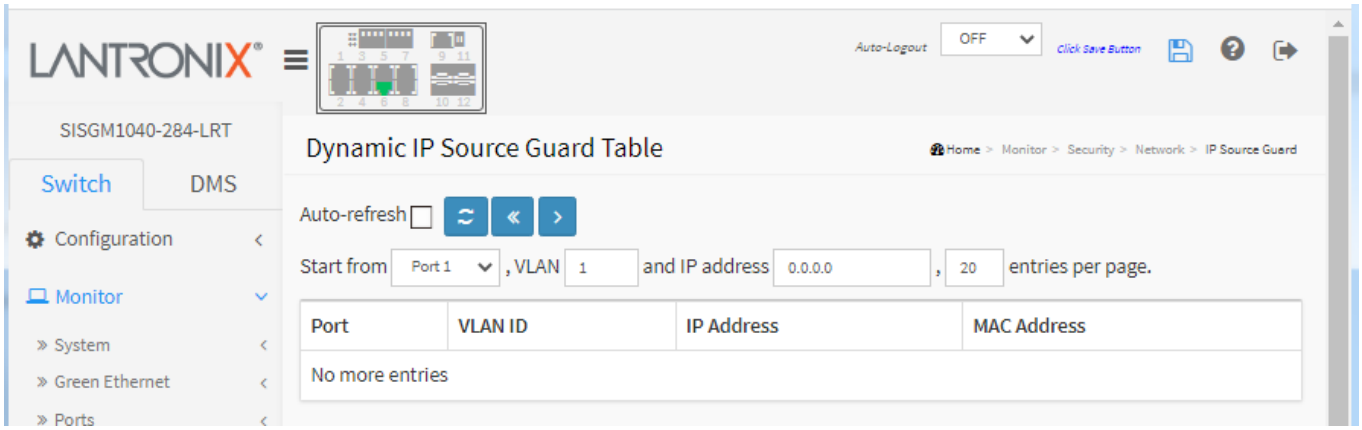
<< : Updates the table starting from the first entry in the Dynamic ARP Inspection Table.

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

Monitor > Security > Network > IP Source Guard

Entries in the Dynamic IP Source Guard Table are shown on this page. The Dynamic IP Source Guard Table is sorted first by port, then by VLAN ID, then by IP address, and then by MAC address.

Each page shows up to 99 entries from the Dynamic IP Source Guard 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 IP Source Guard Table.



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: Refreshes the displayed table starting from the input fields.

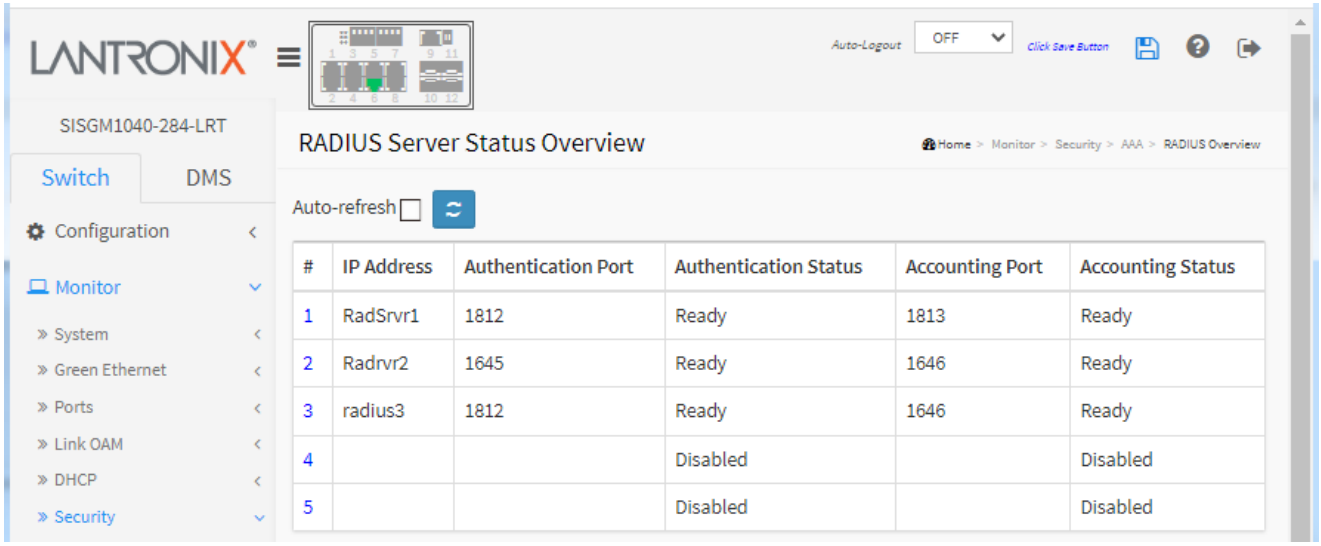
Clear: Flushes all dynamic entries.

<< : Updates the table starting from the first entry in the Dynamic IP Source Guard Table.

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

Monitor > Security > AAA > RADIUS Overview

This page provides an overview of the status of the RADIUS servers configured on the RADIUS Server Configuration page at Configuration > Security > AAA > RADIUS.



: The RADIUS server number. Click to navigate to detailed statistics for this RADIUS server.

IP Address: The IP address of this server.

Authentication Port: UDP port number for authentication.

Authentication Status: The current status of the server. This field has one of these values:

Disabled: The server is disabled.

Not Ready: The server is enabled, but IP communication is not yet up and running.

Ready: The server is enabled, IP communication is up and running, and the RADIUS module is ready to accept access attempts.

***Dead (X seconds left)*:** Access attempts were made to this server, but it did not reply within the configured timeout. The server has temporarily been disabled but will get re-enabled when the dead-time expires. The number of seconds left before this occurs is displayed in parentheses. This state is only reachable when more than one server is enabled.

Accounting Port: UDP port number for accounting.

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.

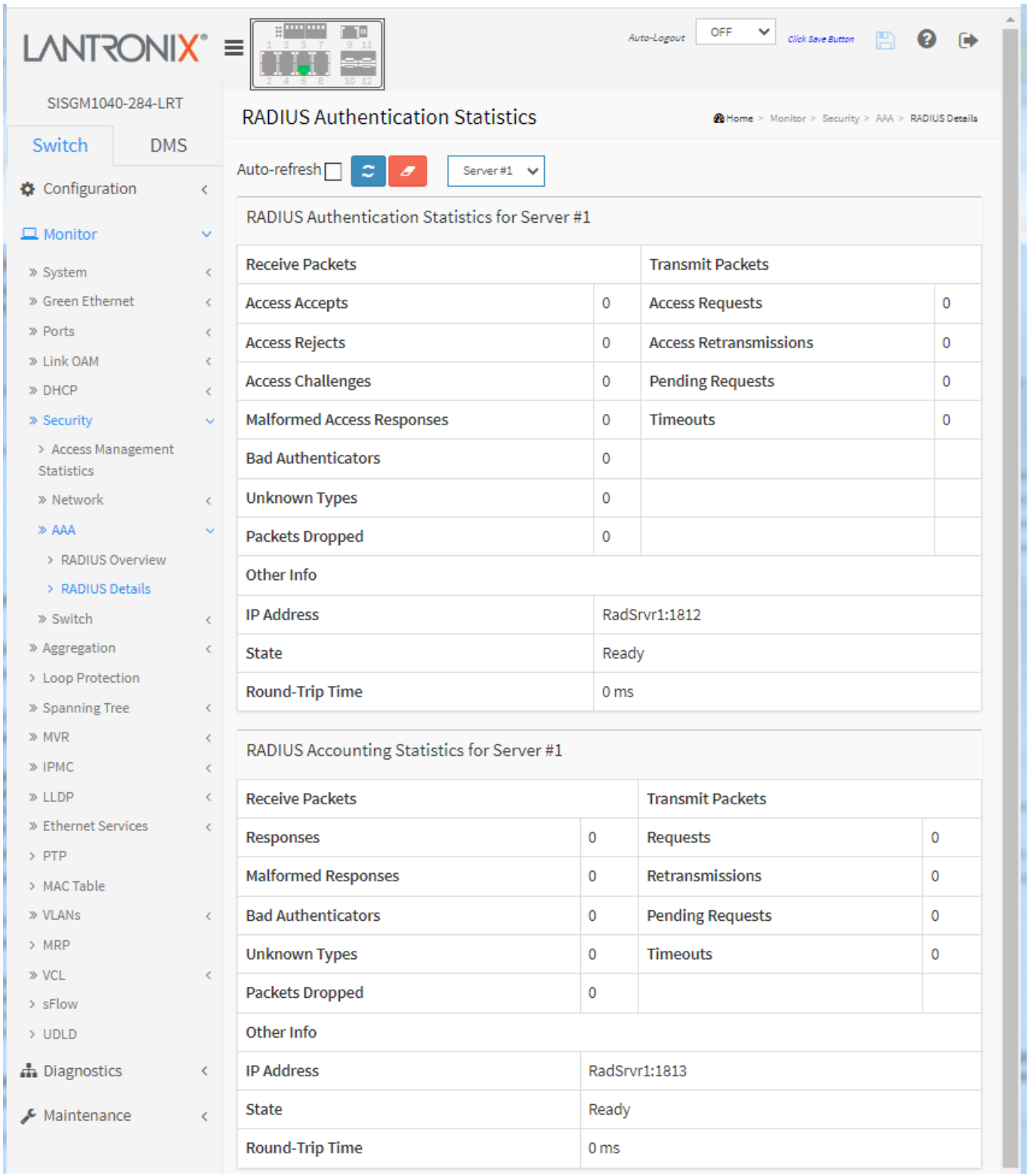
Buttons

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

Refresh: Click to refresh the page immediately.

Monitor > Security > AAA > RADIUS Details

This page provides detailed statistics for a selected RADIUS server.



RADIUS Authentication Statistics: The statistics map closely to those specified in RFC4668 - RADIUS Authentication Client MIB. Use the server select box to switch between the backend servers to show details for.

Packet Counters: RADIUS authentication server packet counter. There are seven receive and four transmit counters.

Direction	Name	RFC4668 Name	Description
Rx	**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	radiusAuthClientExtRoundTripTime	The time interval (measured in milliseconds) between the most recent Access-Reply/Access-Challenge and the Access-Request that matched it from the RADIUS authentication server. The granularity of this measurement is 100 ms. A value of 0 ms indicates that there hasn't been round-trip communication with the server yet.

RADIUS Accounting Statistics: The statistics map closely to those specified in RFC4670 - RADIUS Accounting Client MIB. Use the server select box to switch between the backend servers to show details for.

Packet Counters: RADIUS accounting server packet counter. There are five receive and four transmit counters.

Direction	Name	RFC4670 Name	Description
Rx	**Responses**	radiusAccClientExtResponses	The number of RADIUS packets (valid or invalid) received from the server.
Rx	**Malformed Responses**	radiusAccClientExtMalformedResponses	The number of malformed RADIUS packets received from the server. Malformed packets include packets with an invalid length. Bad authenticators or unknown types are not included as malformed access responses.
Rx	**Bad Authenticators**	radiusAcctClientExtBadAuthenticators	The number of RADIUS packets containing invalid authenticators received from the server.
Rx	**Unknown Types**	radiusAccClientExtUnknownTypes	The number of RADIUS packets of unknown types that were received from the server on the accounting port.
Rx	**Packets Dropped**	radiusAccClientExtPacketsDropped	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**	radiusAccClientExtRetransmissions	The number of RADIUS packets retransmitted to the RADIUS accounting server.
Tx	**Pending Requests**	radiusAccClientExtPendingRequests	The number of RADIUS packets destined for the server that have not yet timed out or received a response. This variable is incremented when a Request is sent and decremented due to receipt of a Response, timeout, or retransmission.
Tx	**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

Server select box: determines which server is affected by clicking the buttons.

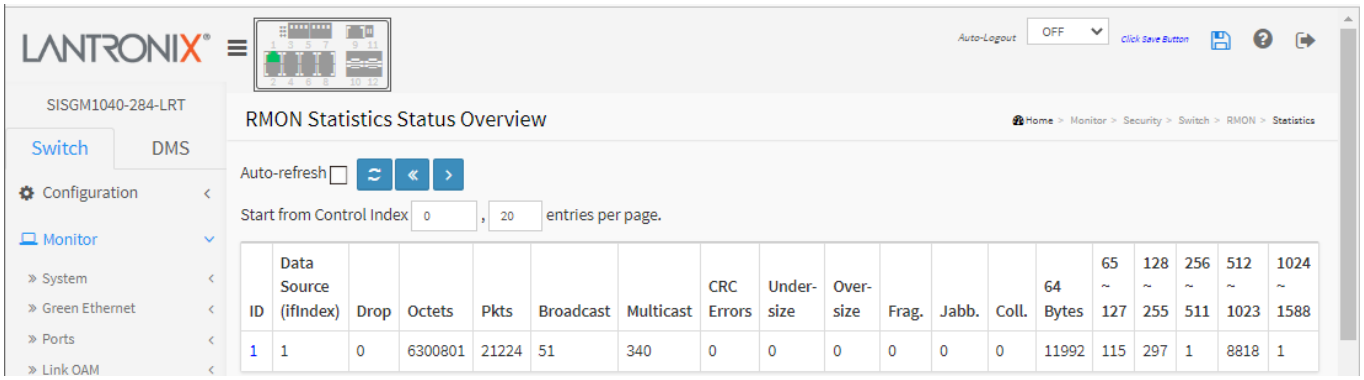
Auto-refresh: Check this box to refresh the page automatically every 3 seconds.

Refresh: Click to refresh the page immediately.

Clear: Clears the counters for the selected server. The "Pending Requests" counter will not be cleared by this operation.

Monitor > Security > Switch > RMON > 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 entry displayed will be the one with the lowest ID found in the Statistics table.



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.

Multi-cast: The total number of good packets received that were directed to a multicast address.

CRC Errors: The total number of packets received that had a length (excluding framing bits, but including FCS octets) of between 64 and 1518 octets, inclusive, but had either a bad Frame Check Sequence (FCS) with an integral number of octets (FCS Error) or a bad FCS with a non-integral number of octets (Alignment Error).

Under-size: The total number of packets received that were less than 64 octets.

Over-size: The total number of packets received that were longer than 1518 octets.

Frag.: The number of frames which size is less than 64 octets received with invalid CRC.

Jabb.: The number of frames which size is larger than 64 octets received with invalid CRC.

Coll.: The best estimate of the total number of collisions on this Ethernet segment.

64 Bytes: The total number of packets (including bad packets) received that were 64 octets in length.

65~127: The total number of packets (including bad packets) received that were 65 to 127 octets in length.

128~255: The total number of packets (including bad packets) received that were 128 to 255 octets in length.

256~511: The total number of packets (including bad packets) received that were 256 to 511 octets in length.

512~1023: The total number of packets (including bad packets) received that were 512 to 1023 octets in length.

1024~1588: The total number of packets (including bad packets) received that were 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.

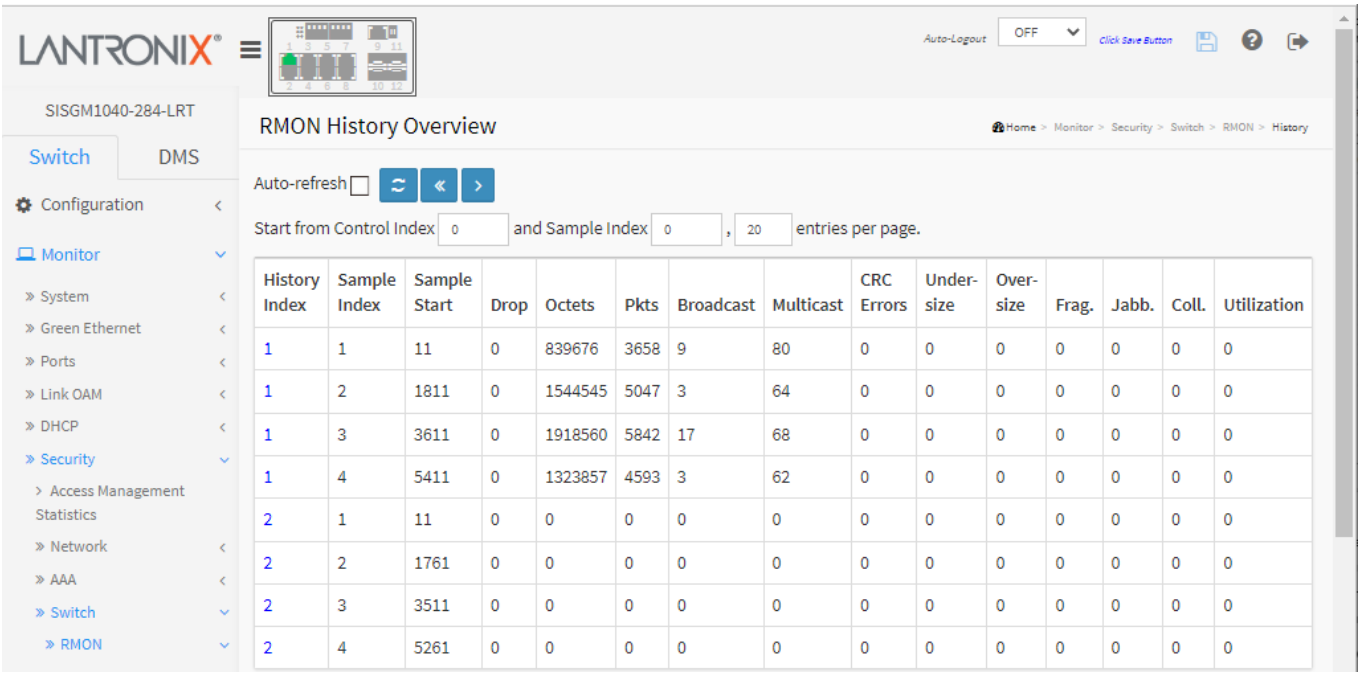
<< : Updates the table starting from the first entry in the Statistics table, i.e. the entry with the lowest ID.

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

Messages: *No more entries*

Monitor > Security > Switch > RMON > History

This page provides an overview of RMON History entries. Each page shows up to 99 entries from the History table, selected through the "entries per page" input field. When first visited, the web page will show the first 20 entries from the beginning of the History table. The first entry displayed will be the one with the lowest History Index and Sample Index found in the History table.



History Index	Sample Index	Sample Start	Drop	Octets	Pkts	Broadcast	Multicast	CRC Errors	Under-size	Over-size	Frag.	Jabb.	Coll.	Utilization
1	1	11	0	839676	3658	9	80	0	0	0	0	0	0	0
1	2	1811	0	1544545	5047	3	64	0	0	0	0	0	0	0
1	3	3611	0	1918560	5842	17	68	0	0	0	0	0	0	0
1	4	5411	0	1323857	4593	3	62	0	0	0	0	0	0	0
2	1	11	0	0	0	0	0	0	0	0	0	0	0	0
2	2	1761	0	0	0	0	0	0	0	0	0	0	0	0
2	3	3511	0	0	0	0	0	0	0	0	0	0	0	0
2	4	5261	0	0	0	0	0	0	0	0	0	0	0	0

History Index: Indicates the index of History control entry.

Sample Index: Indicates the index of the data entry associated with the control entry.

Sample Start: The value of sysUpTime at the start of the interval over which this sample was measured.

Drop: The total number of events in which packets were dropped by the probe due to lack of resources.

Octets: The total number of octets of data (including those in bad packets) received on the network.

Pkts: The total number of packets (including bad packets, broadcast packets, and multicast packets) received.

Broadcast: The total number of good packets received that were directed to the broadcast address.

Multicast: The total number of good packets received that were directed to a multicast address.

CRCErrors: The total number of packets received that had a length (excluding framing bits, but including FCS octets) of between 64 and 1518 octets, inclusive, but had either a bad Frame Check Sequence (FCS) with an integral number of octets (FCS Error) or a bad FCS with a non-integral number of octets (Alignment Error).

Undersize: The total number of packets received that were less than 64 octets.

Oversize: The total number of packets received that were longer than 1518 octets.

Frag.: The number of frames which size is less than 64 octets received with invalid CRC.

Jabb.: The number of frames which size is larger than 64 octets received with invalid CRC.

Coll.: The best estimate of the total number of collisions on this Ethernet segment.

Utilization: The best estimate of the mean physical layer network utilization on this interface during this sampling interval, in hundredths of a percent.

Buttons

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

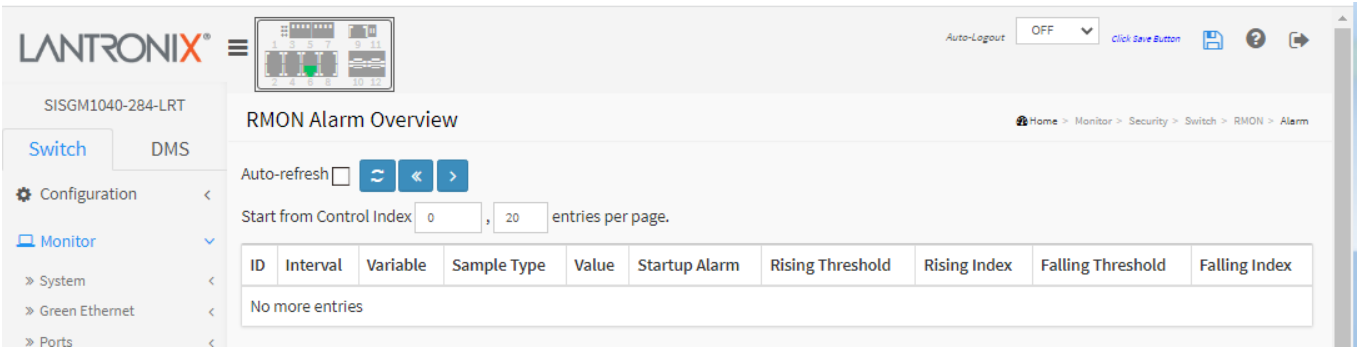
Refresh: Click to refresh the page immediately.

<< : Updates the table starting from the first entry in the History table, 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.

Monitor > Security > Switch > RMON > 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.



ID: Indicates the index of Alarm control entry.

Interval: Indicates the interval in seconds for sampling and comparing the rising and falling threshold.

Variable: Indicates the particular variable to be sampled

Sample Type: The method of sampling the selected variable and calculating the value to be compared against the thresholds.

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

Startup Alarm: The alarm that may be sent when this entry is first set to valid.

Rising Threshold: Rising threshold value.

Rising Index: Rising event index.

Falling Threshold: Falling threshold value.

Falling Index: Falling event index.

Buttons

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

Refresh: Click to refresh the page immediately.

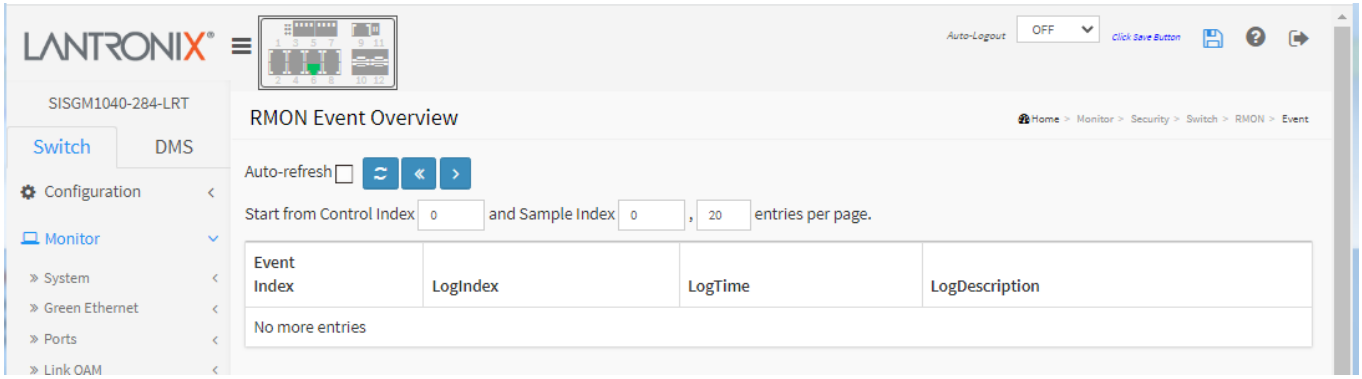
<< : Updates the table starting from the first entry in the Alarm Table, i.e. the entry with the lowest ID.

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

Messages: *No more entries*

Monitor > Security > Switch > RMON > 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.



Event Index: Indicates the index of the event entry.

Log Index: Indicates the index of the log entry.

LogTime: Indicates Event log time

LogDescription: Indicates the Event description.

Buttons

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

Refresh: Click to refresh the page immediately.

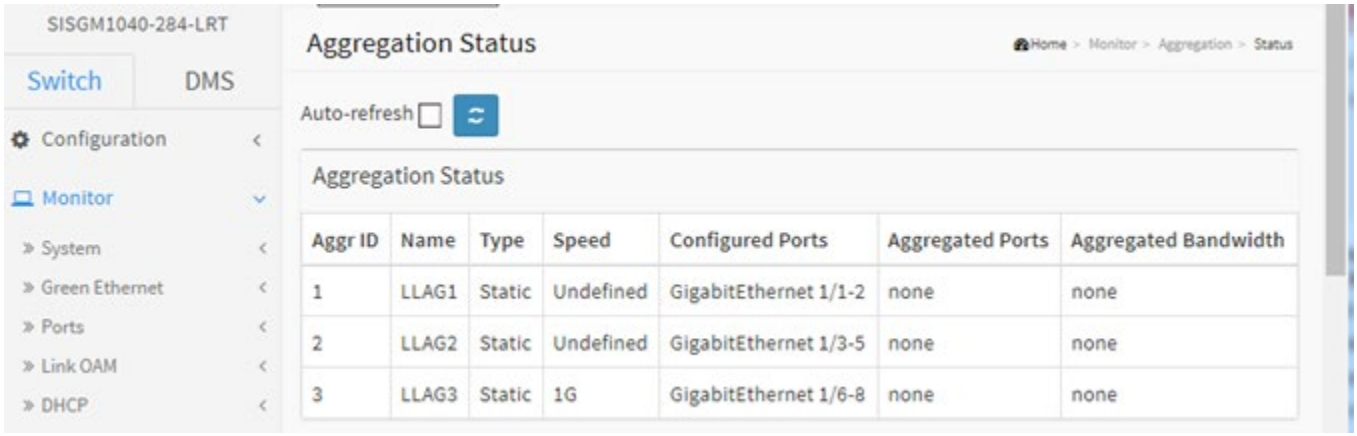
<< : Updates the table starting from the first entry in the Event Table, i.e. the entry with the lowest Event Index and Log Index.

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

Messages: *No more entries*

Monitor > Aggregation > Status

This page displays the status of ports in Aggregation group.



Aggregation Group Status

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

Name: Name of the Aggregation group ID.

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

Speed: Speed of the Aggregation group.

Configured ports: Configured member ports of the Aggregation group.

Aggregated ports: Aggregated member ports of the Aggregation group.

Aggregated Bandwidth: Aggregated Bandwidth of the Aggregation group.

Buttons

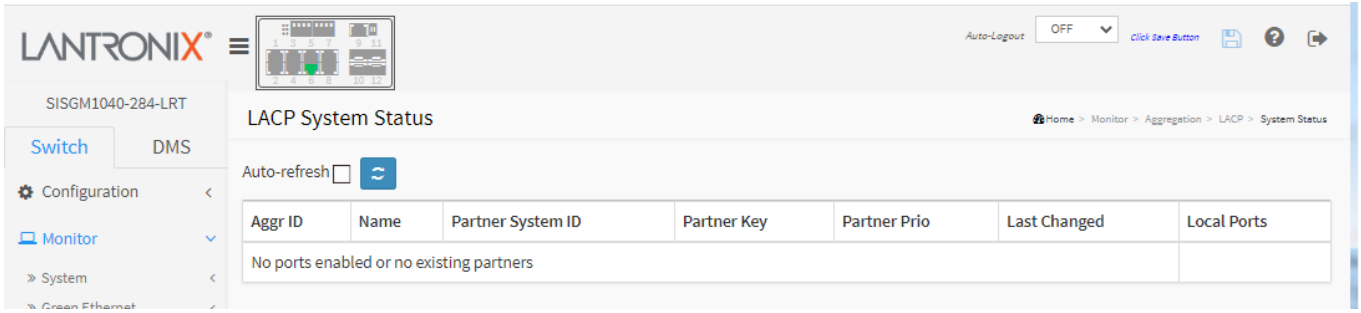
Auto-refresh: Automatic refresh occurs every 3 seconds.

Refresh: Click to refresh the page immediately.

Messages: *No aggregation groups*

Monitor > Aggregation > LACP > System Status

This page displays a status overview for all LACP instances.



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.

Partner Prio: The priority of this partner.

Last Changed: The time since this aggregation changed.

Local Ports: Shows which ports are a part of this aggregation for this switch.

Buttons

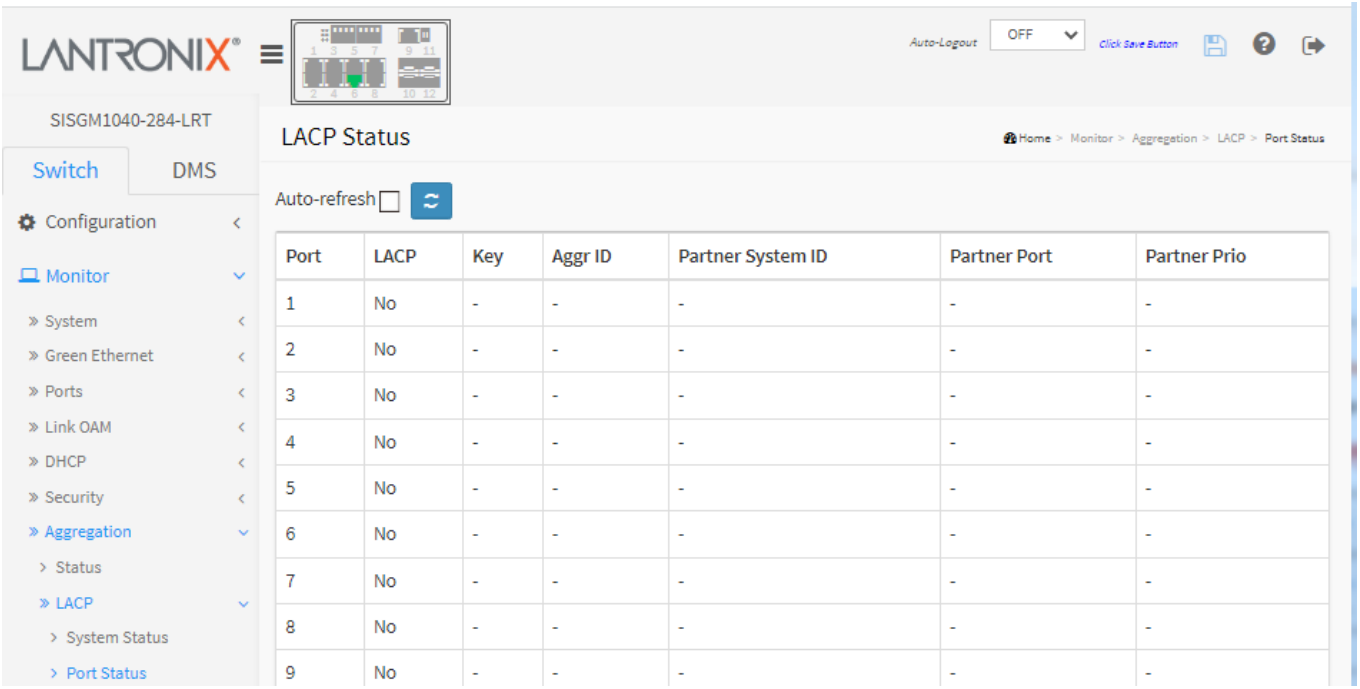
Auto-refresh: Automatic refresh occurs every 3 seconds.

Refresh: Click to refresh the page immediately.

Messages: *No ports enabled or no existing partners*

Monitor > Aggregation > LACP > Port Status

This page provides a status overview for LACP status for all ports.



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 it's LACP status is disabled.

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

Aggr ID: The Aggregation ID assigned to this aggregation group.

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.

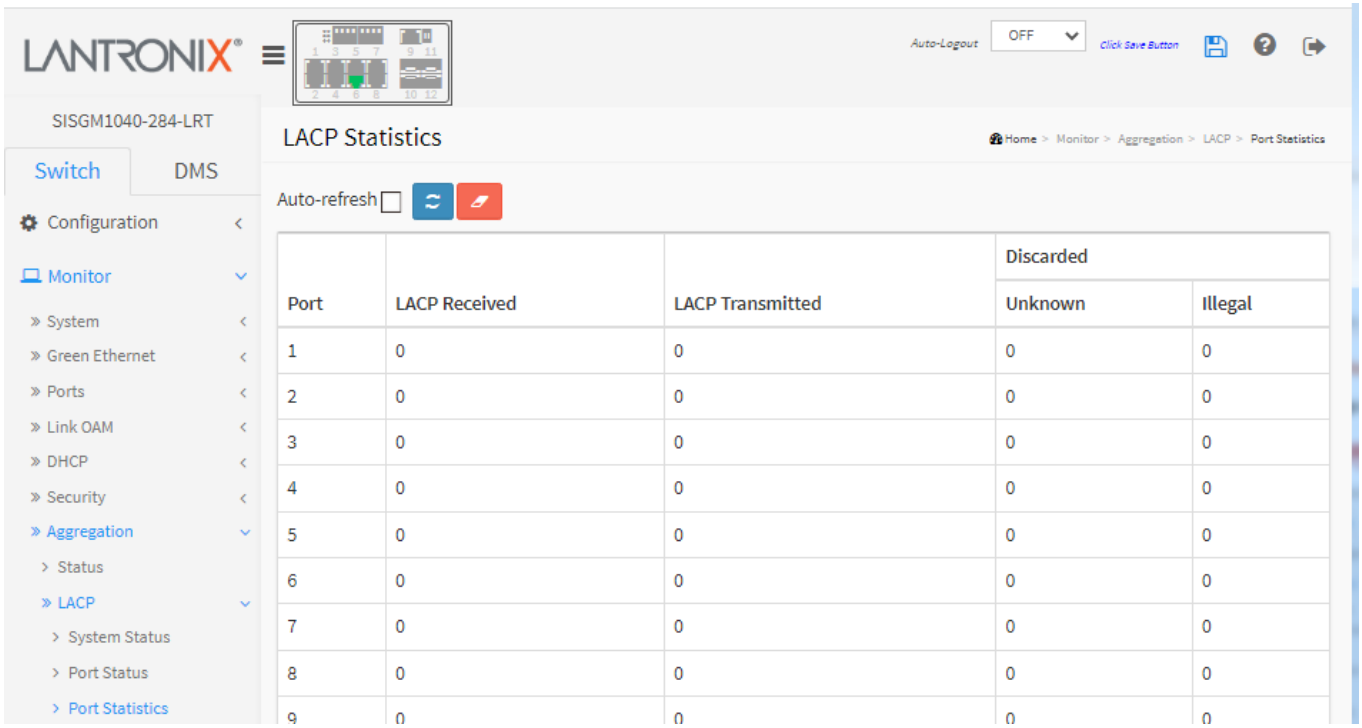
Buttons

Auto-refresh: Automatic refresh occurs every 3 seconds.

Refresh: Click to refresh the page immediately.

Monitor > Aggregation > LACP > Port Statistics

This page provides an overview for LACP statistics for all ports.



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 and illegal LACP frames have been discarded at each port.

Buttons

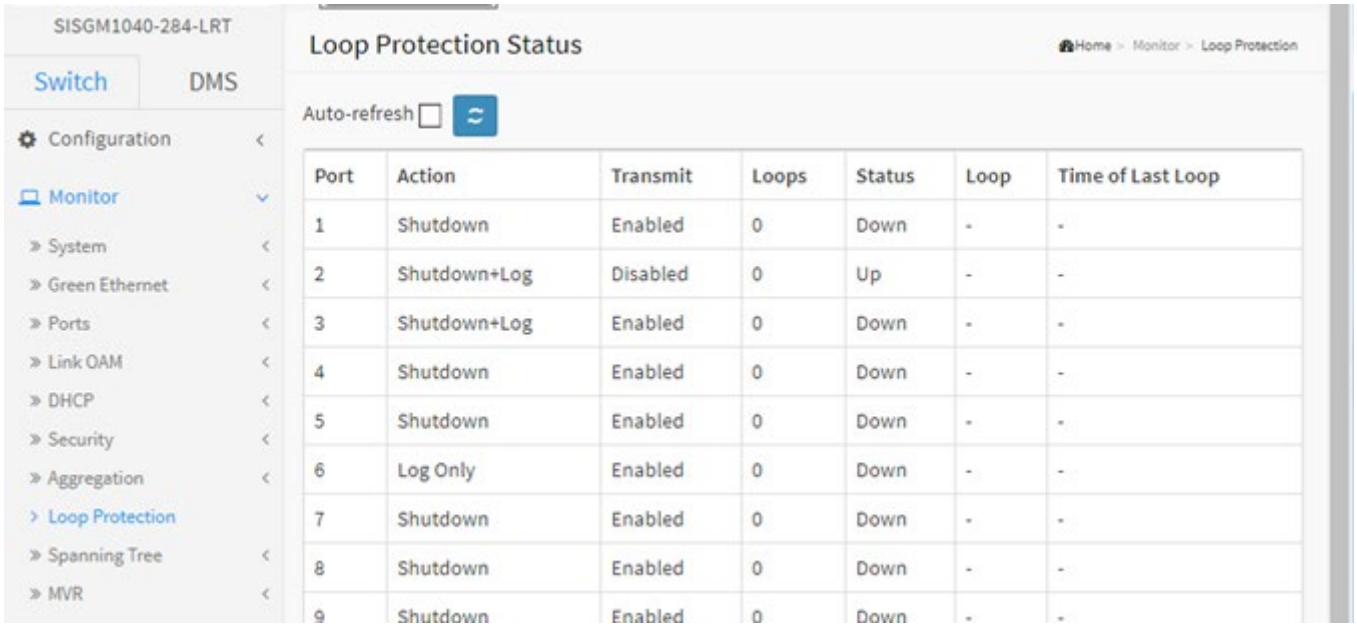
Auto-refresh: Automatic refresh occurs every 3 seconds.

Refresh: Click to refresh the page immediately.

Clear: Clears the counters for all ports.

Monitor > Loop Protection

This page displays the loop protection status of the switch ports.



Port: The switch port number of the logical port.

Action: The currently configured port action (Shutdown , Log, or Shutdown+Log).

Transmit: The currently configured port transmit mode (Enabled or Disabled).

Loops: The number of loops detected on this port.

Status: The current loop protection status of the port (Up or Down).

Loop: The loops currently detected on each port.

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

Buttons

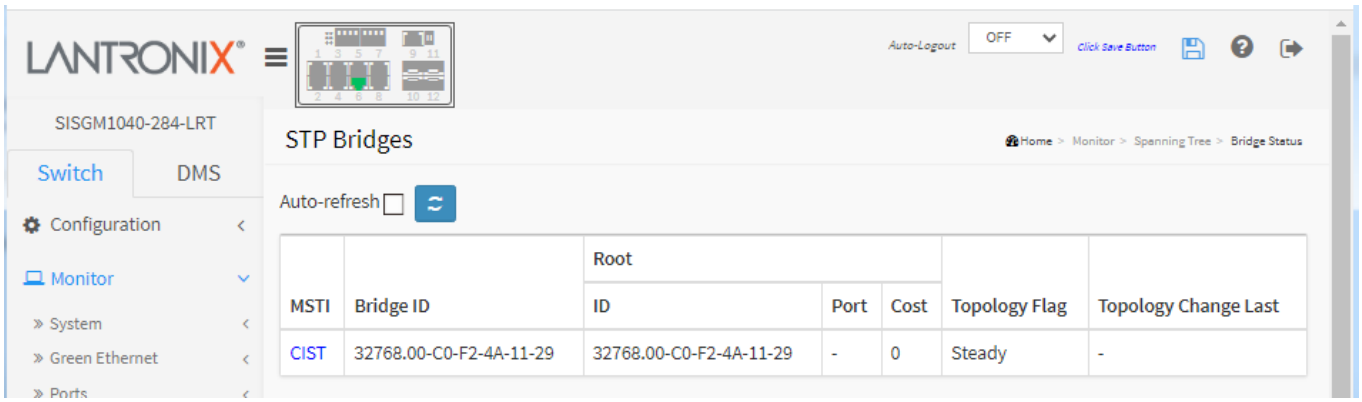
Auto-refresh: Check this box to enable an automatic refresh every 3 seconds.

Refresh: Click to refresh the page immediately.

Messages: *No ports enabled*

Monitor > Spanning Tree > Bridge Status

This page provides a status overview of all STP bridge instances. The displayed table contains a row for each STP bridge instance.



MSTI: The Bridge Instance. This is also a link to the STP Detailed Bridge Status (see example below).

Bridge ID: The Bridge ID of this Bridge instance.

Root ID: The Bridge ID of the currently elected root bridge.

Root Port: The switch port currently assigned the root port role.

Root Cost: Root Path Cost. For the Root Bridge it is zero. For all other Bridges, it is the sum of the Port Path Costs on the least cost path to the Root Bridge.

Topology Flag: The current state of the Topology Change Flag of this Bridge instance.

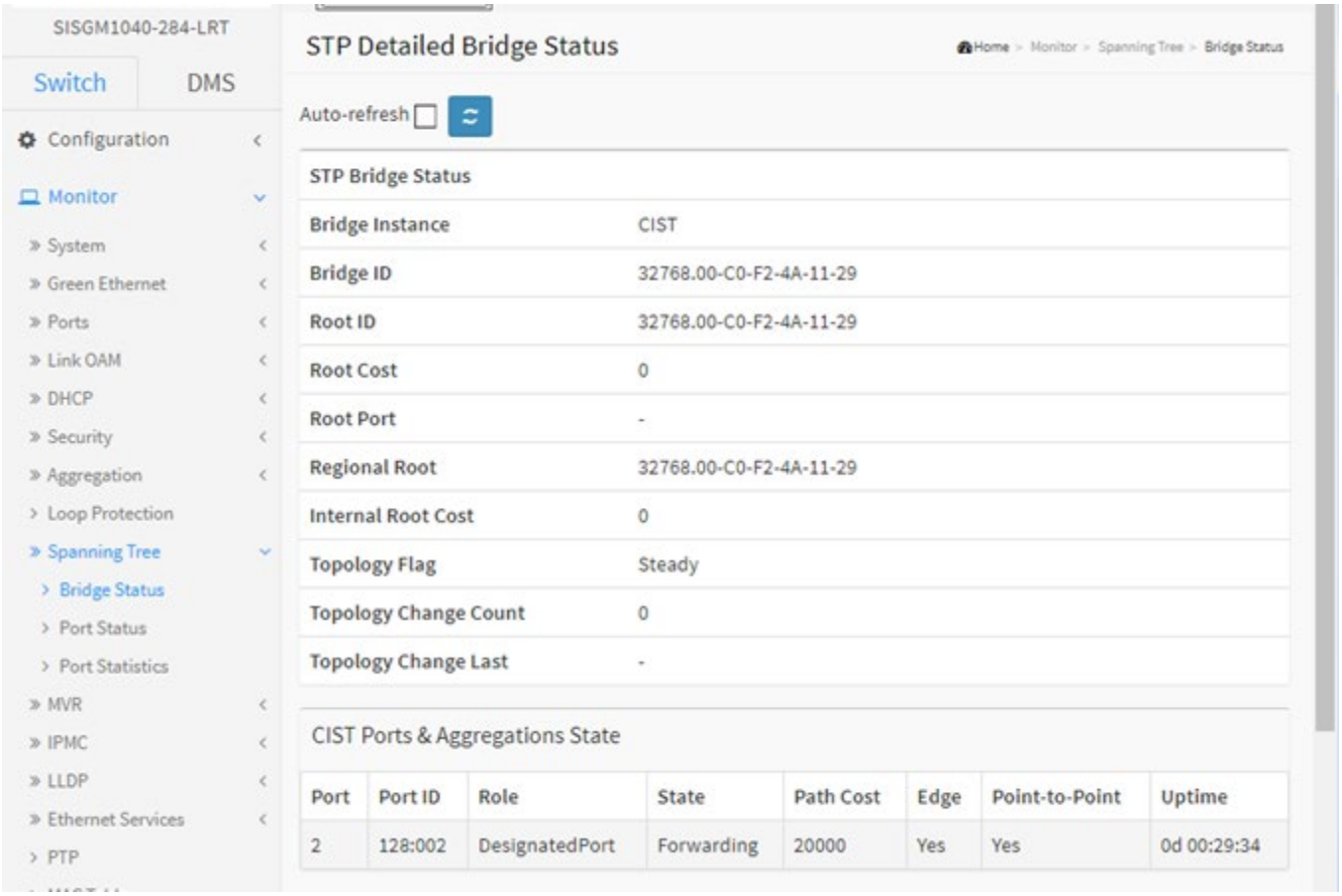
Topology Change Last: The time since last Topology Change occurred.

Buttons

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

Refresh: Click to refresh the page immediately.

STP Detailed Bridge Status : Click a link in the MSTI column of the STP Bridge Status page to display the STP Detailed Bridge Status page. This page provides detailed information on a single STP bridge instance, along with port state for all active ports associated.



Parameter descriptions:

Bridge Instance : The Bridge instance (e.g., CIST, MST1, MIST2, etc.).

Bridge ID : The Bridge ID of this Bridge instance in the format 32768.00-C0-F2-4A-11-29.

Root ID : The Bridge ID of the currently elected root bridge in the format 32768.00-C0-F2-4A-11-29).

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 where the topology change flag has been set (during a one-second interval).

Topology Change Last : The time passed since the Topology Flag was last set.

CIST Ports & Aggregations State

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

Port ID : The port id as used by the STP protocol. This is the priority part and the logical port index of the bridge port.

Role : The current STP port role. The port role can be one of these values: AlternatePort, BackupPort, RootPort, and DesignatedPort.

State : The current STP port state. The port state can be one of these values: Discarding, Learning, or Forwarding.

Path Cost : The current STP port path cost. This will either be a value computed from the Auto setting, or any explicitly configured value.

Edge : The current STP port (operational) Edge Flag (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.

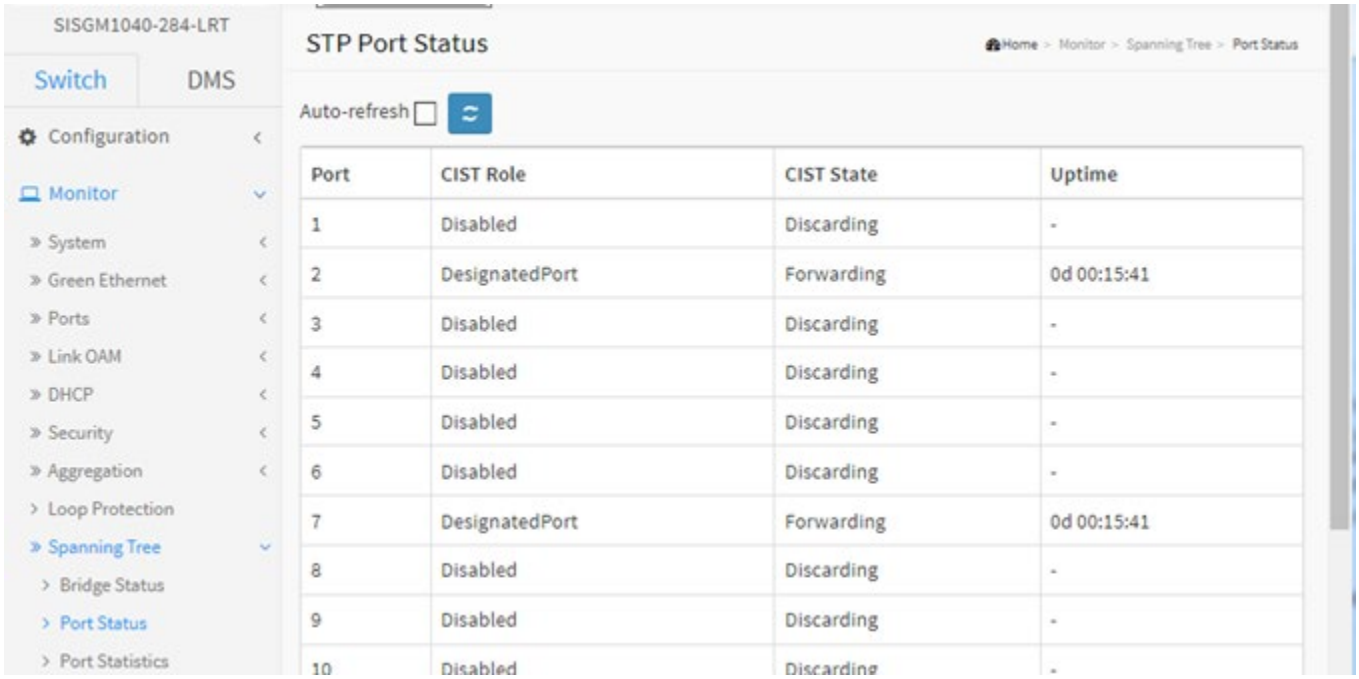
Buttons

Refresh : Click to refresh the page immediately.

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

Monitor > Spanning Tree > Port Status

This page displays the STP CIST port status for physical ports of the switch.



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 a value of AlternatePort, BackupPort, RootPort, DesignatedPort, Non-STP, or Disabled.

CIST State: The current STP port state of the CIST port. The port state can be Discarding, Learning, or Forwarding.

Uptime: The time since the bridge port was last initialized.

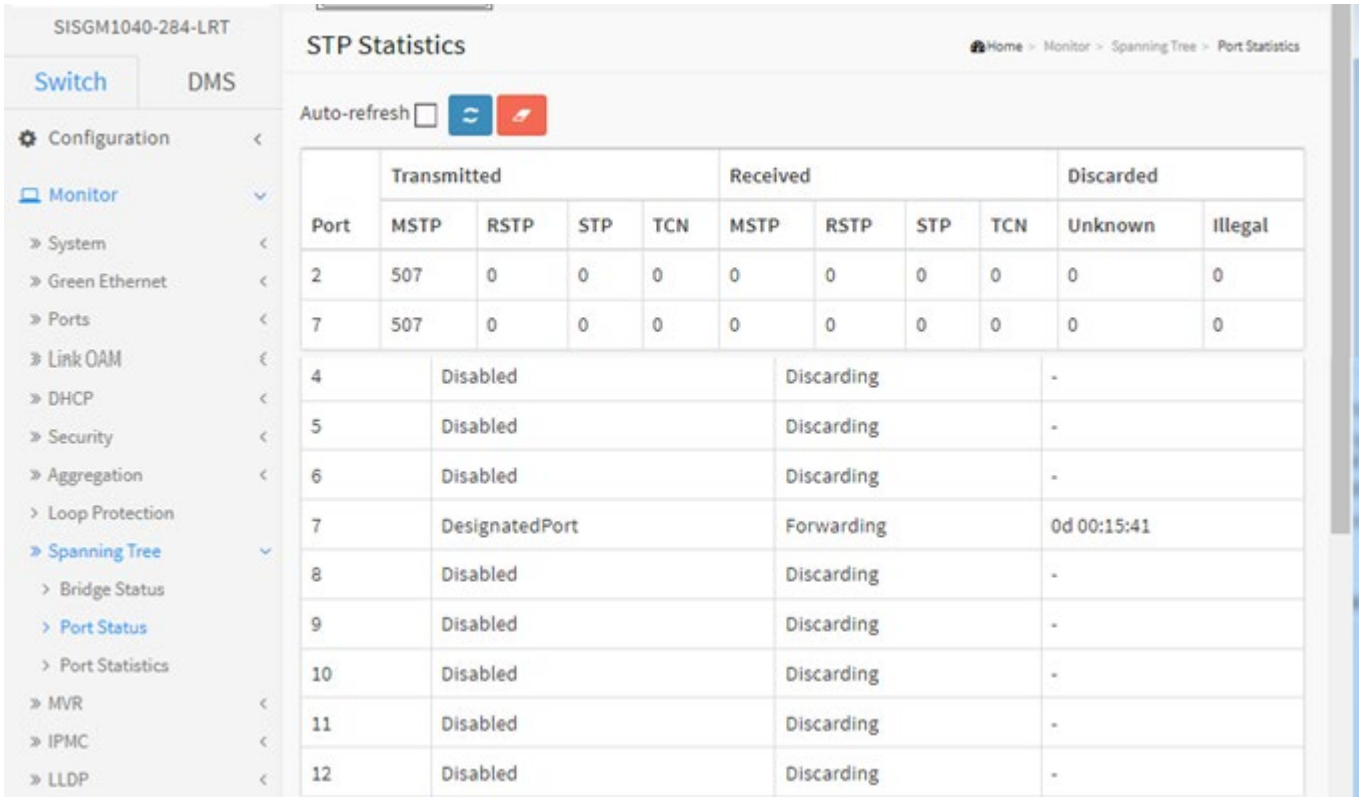
Buttons

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

Refresh: Click to refresh the page immediately.

Monitor > Spanning Tree > Port Statistics

This page displays the STP Port Statistics counters of bridge ports in the switch.



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

MSTP: The number of MSTP BPDU's received/transmitted on the port.

RSTP: The number of RSTP 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

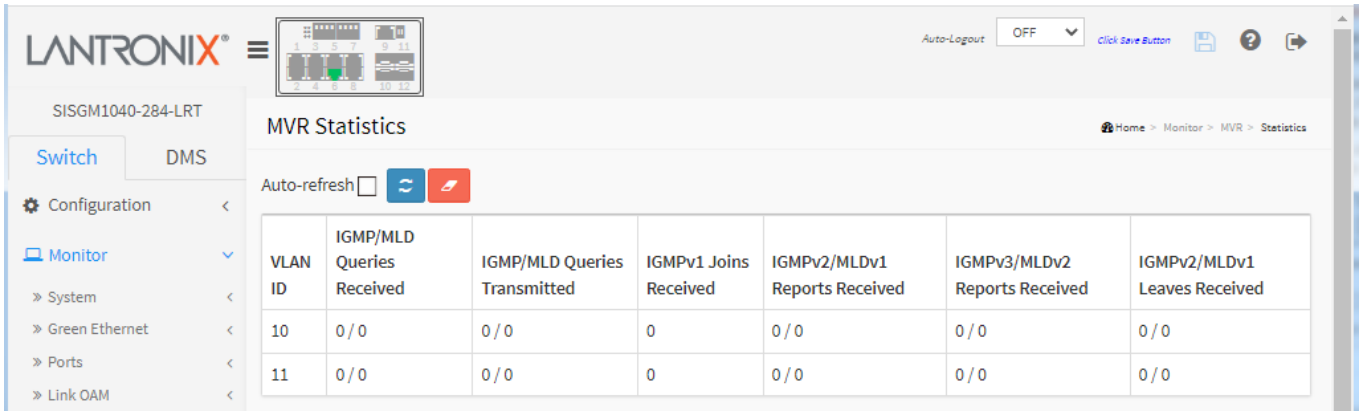
Auto-refresh: Check this box to refresh the page automatically every 3 seconds.

Refresh: Click to refresh the page immediately.

Clear: Click to reset the counters.

Monitor > MVR > Statistics

This page provides MVR Statistics information.



VLAN ID: The Multicast VLAN ID.

IGMP/MLD Queries Received: The number of Received Queries for IGMP and MLD, respectively.

IGMP/MLD Queries Transmitted: The number of Transmitted Queries for IGMP and MLD, respectively.

IGMPv1 Joins Received: The number of Received IGMPv1 Join's.

IGMPv2/MLDv1 Report's Received: The number of Received IGMPv2 Join's and MLDv1 Report's, respectively.

IGMPv3/MLDv2 Report's Received: The number of Received IGMPv1 Join's and MLDv2 Report's, respectively.

IGMPv2/MLDv1 Leave's Received: The number of Received IGMPv2 Leave's and MLDv1 Done's, respectively.

Buttons

Auto-refresh : Automatic refresh occurs every 3 seconds.

Refresh: Click to refresh the page immediately.

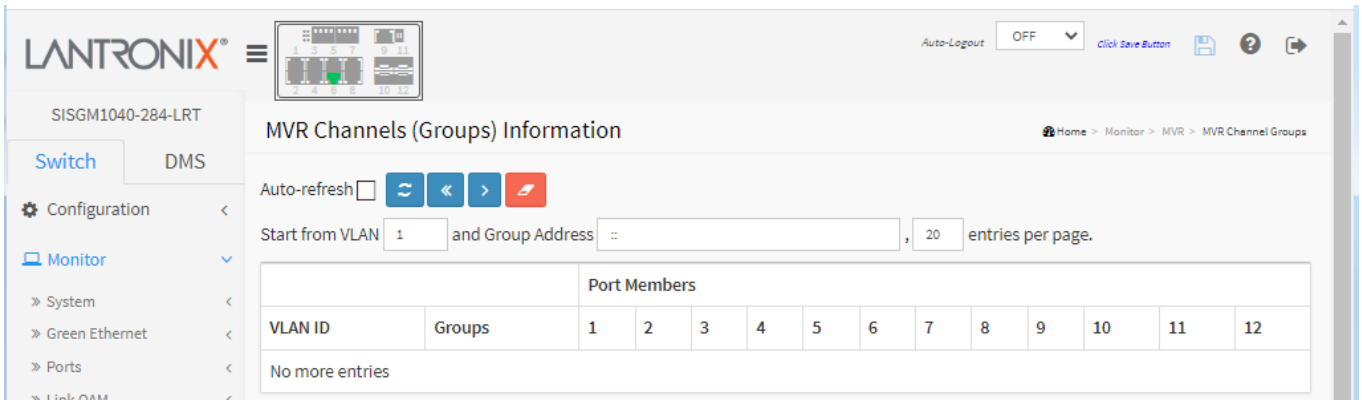
Clear: Clears all Statistics counters.

Monitor > MVR > MVR Channel Groups

Entries in the MVR Channels (Groups) Information Table are shown on this page. The MVR Channels (Groups) Information Table is sorted first by VLAN ID, and then by group.

Each page shows up to 99 entries from the MVR Group table, default being 20, selected through the "entries per page" input field. When first visited, the web page will show the first 20 entries from the beginning of the MVR Channels (Groups) Information Table.

The "Start from VLAN", and "Group Address" input fields allow the user to select the starting point in the MVR Channels (Groups) Information Table.



VLAN ID: VLAN ID of the group.

Groups: Group ID of the group displayed.

Port Members: Ports under this group.

Buttons

Auto-refresh : Automatic refresh occurs every 3 seconds.

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

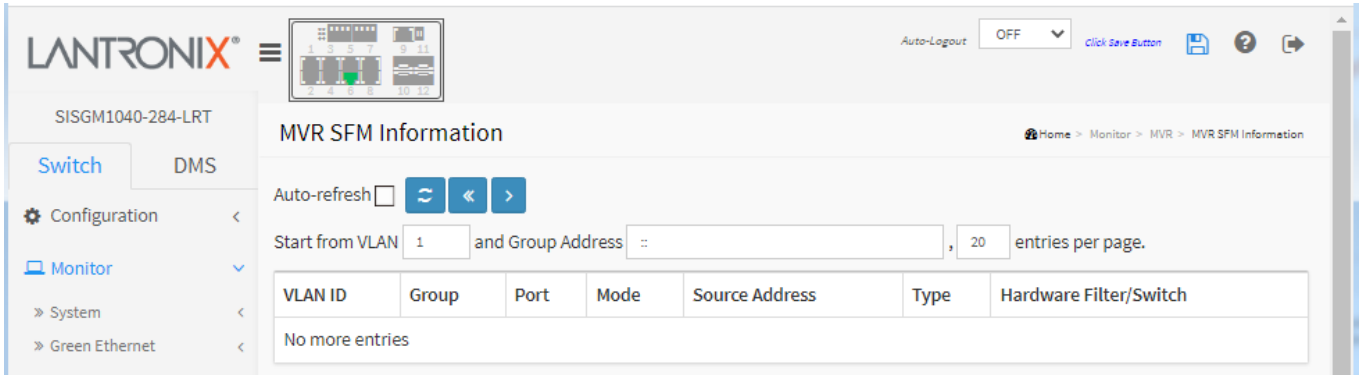
<< : Updates the table starting from the first entry in the MVR Channels (Groups) Information Table.

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

Clear: Clears all table entries.

Monitor > MVR > MVR SFM Information

Entries in the MVR SFM Information Table are shown on this page. 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.



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. The maximum number of IP source address for filtering (per group) is 8.
When there is not any source filtering address, the text "None" is shown in the Source Address field.

Type: Indicates the Type. It can be either Allow or Deny.

Hardware Filter/Switch: Indicates whether data plane destined to the specific group address from the source IPv4/IPv6 address could be handled by chip or not.

Buttons

Auto-refresh : Automatic refresh occurs every 3 seconds.

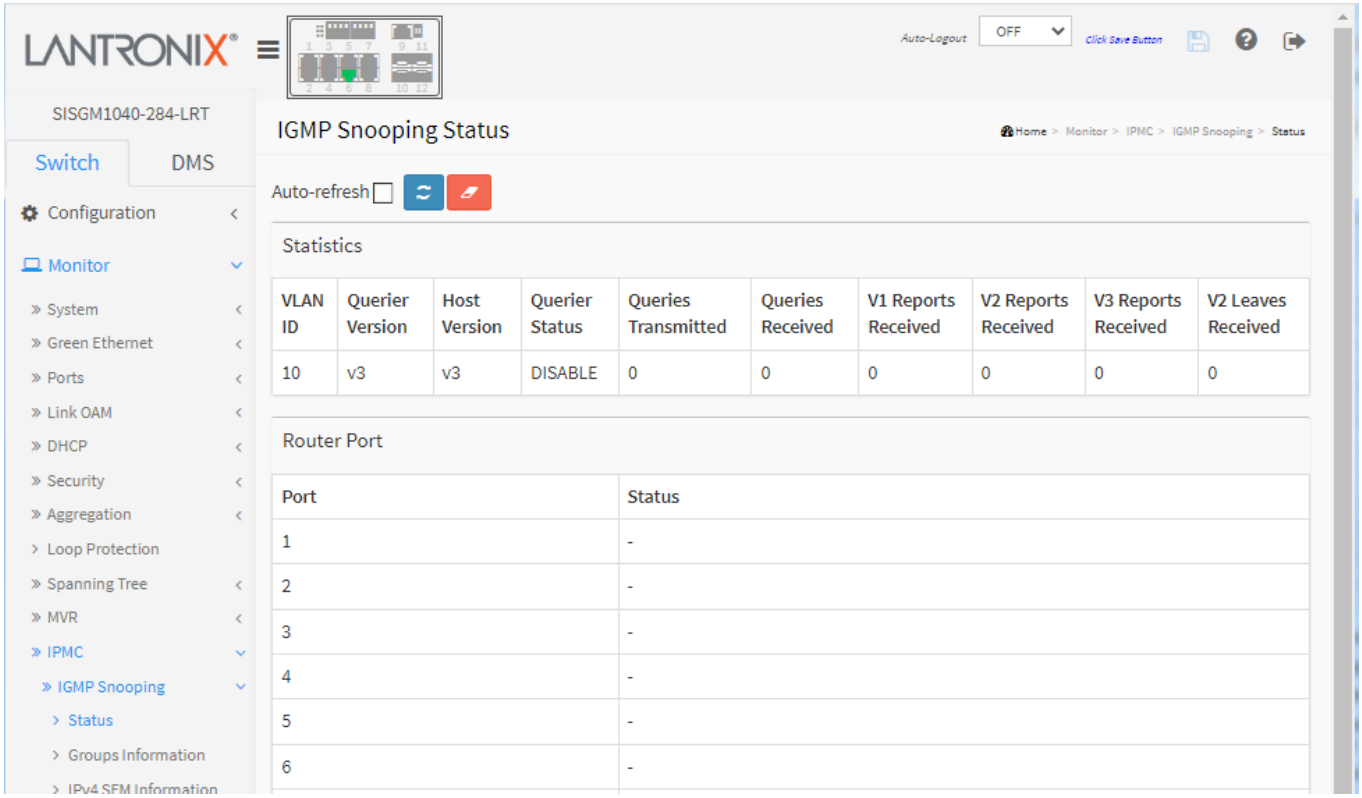
Refresh: Refreshes the displayed table starting from the input fields.

<< : Updates the table starting from the first entry in the MVR SFM Information Table.

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

Monitor > IPMC > IGMP > Snooping Status

This page provides IGMP Snooping status.



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

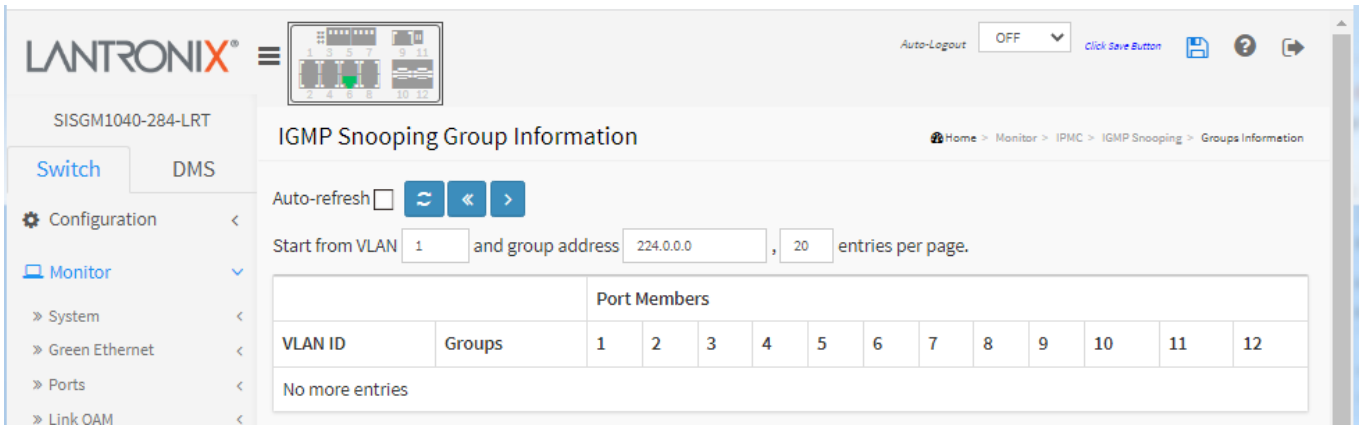
Auto-refresh : Automatic refresh occurs every 3 seconds.

Refresh: Click to refresh the page immediately.

Clear: Clears all Statistics counters.

Monitor > IPMC > IGMP Snooping > Groups 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.



VLAN ID: VLAN ID of the group.

Groups: Group address of the group displayed.

Port Members: Ports under this group.

Buttons

Auto-refresh : Automatic refresh occurs every 3 seconds.

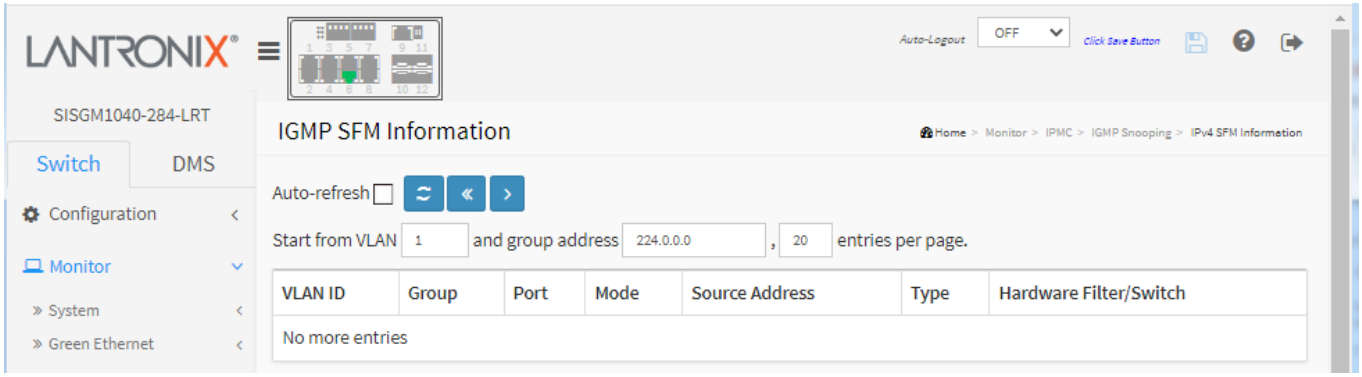
Refresh: Refreshes the displayed table starting from the input fields.

<< : Updates the table, starting with the first entry in the IGMP Group Table.

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

Monitor > IPMC > IGMP Snooping > IPv4 SFM Information

Entries in the IGMP SFM Information Table are shown on this page. The IGMP SFM (Source-Filtered Multicast) Information Table also contains the SSM (Source-Specific Multicast) information. This table is sorted first by VLAN ID, then by group, and then by Port. Different source addresses belong to the same group are treated as single entry.



VLAN ID: VLAN ID of the group.

Group: Group address of the group displayed.

Port: Switch port number.

Mode: Indicates the filtering mode maintained per (VLAN ID, port number, Group Address) basis. It can be either Include or Exclude.

Source Address: IP Address of the source. Currently, system limits the total number of IP source addresses for filtering to be 128.

Type: Indicates the Type. It can be either Allow or Deny.

Hardware Filter/Switch: Indicates whether data plane destined to the specific group address from the source IPv4 address could be handled by chip or not.

Buttons

Auto-refresh : Automatic refresh occurs every 3 seconds.

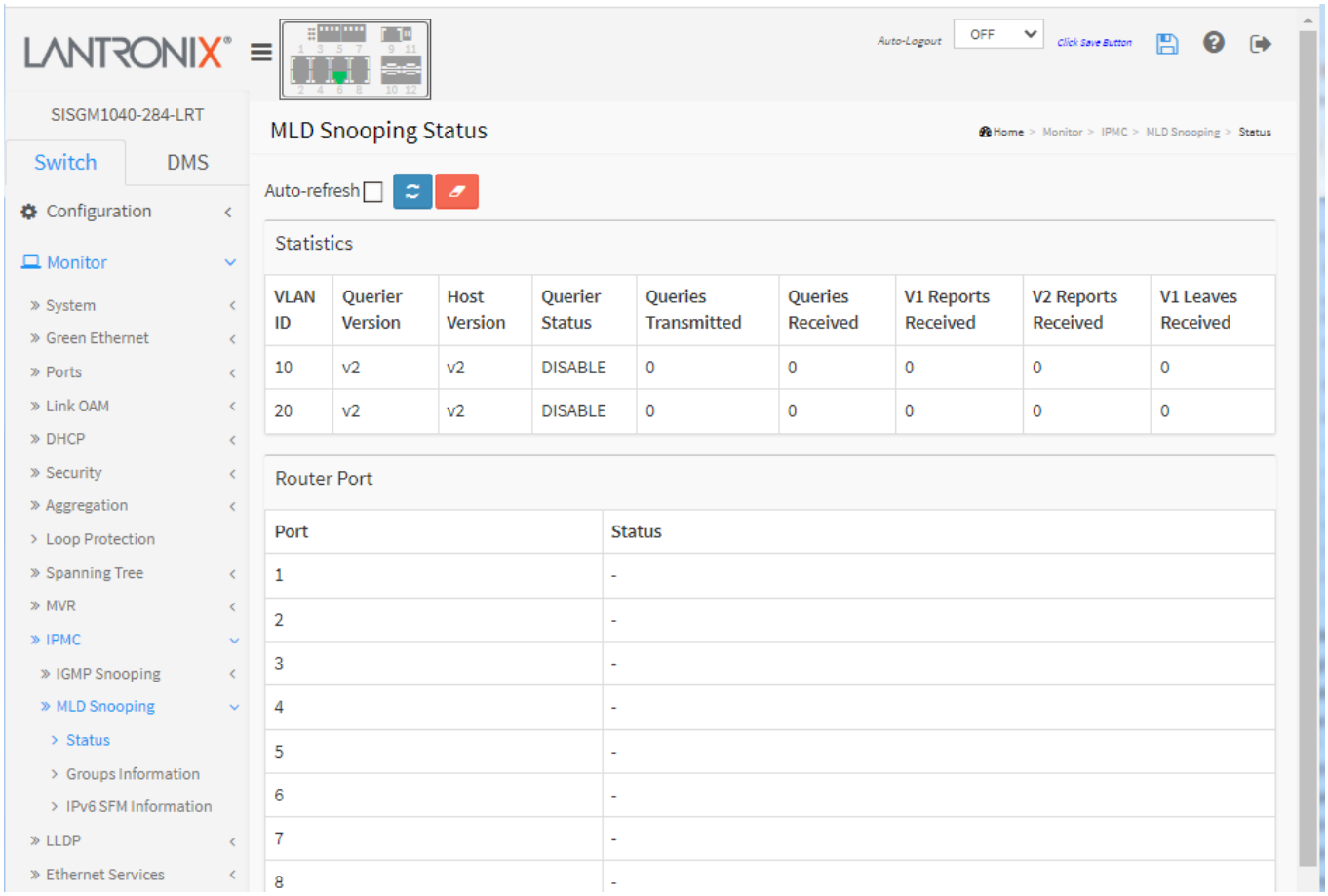
Refresh: Refreshes the displayed table starting from the input fields.

<< : Updates the table starting from the first entry in the IGMP SFM Information Table.

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

Monitor > IPMC > MLD Snooping > Status

This page provides MLD Snooping status.



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". Displays "DISABLE" if 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

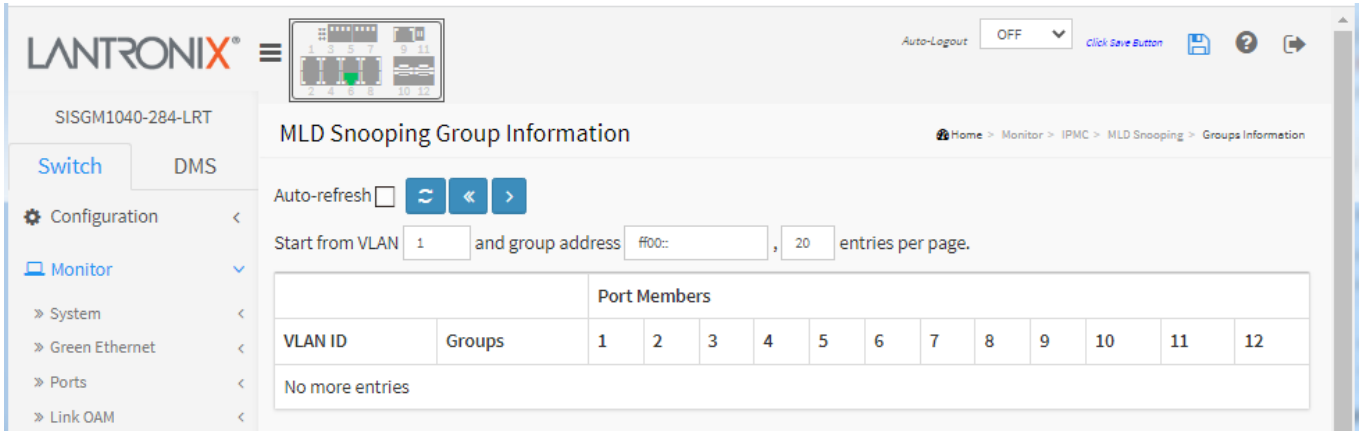
Auto-refresh : Automatic refresh occurs every 3 seconds.

Refresh: Click to refresh the page immediately.

Clear: Clears all Statistics counters.

Monitor > IPMC > MLD Snooping > Groups Information

Entries in the MLD Group Table are shown on this page. The MLD Group Table is sorted first by VLAN ID, and then by group.



VLAN ID: VLAN ID of the group.

Groups: Group address of the group displayed.

Port Members: Ports under this group.

Buttons

Auto-refresh : Automatic refresh occurs every 3 seconds.

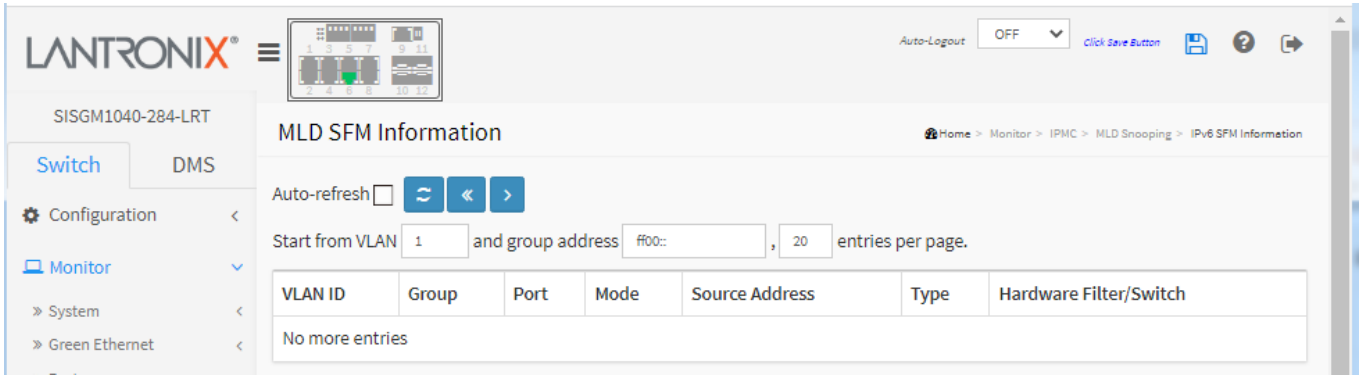
Refresh: Refreshes the displayed table starting from the input fields.

<< : Updates the table, starting with the first entry in the MLD Group Table.

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

Monitor > IPMC > MLD Snooping > IPv6 SFM Information

Entries in the MLD SFM Information Table are shown on this page. The MLD SFM (Source-Filtered Multicast) Information Table also contains the SSM (Source-Specific Multicast) information. This table is sorted first by VLAN ID, then by group, and then by Port. Different source addresses belong to the same group are treated as single entry.



VLAN ID: VLAN ID of the group.

Group: Group address of the group displayed.

Port: Switch port number.

Mode: Indicates the filtering mode maintained per (VLAN ID, port number, Group Address) basis. It can be either Include or Exclude.

Source Address: IP Address of the source. Currently, system limits the total number of IP source addresses for filtering to be 128.

Type: Indicates the Type. It can be either Allow or Deny.

Hardware Filter/Switch: Indicates whether data plane destined to the specific group address from the source IPv6 address could be handled by chip or not.

Buttons

Auto-refresh : Automatic refresh occurs every 3 seconds.

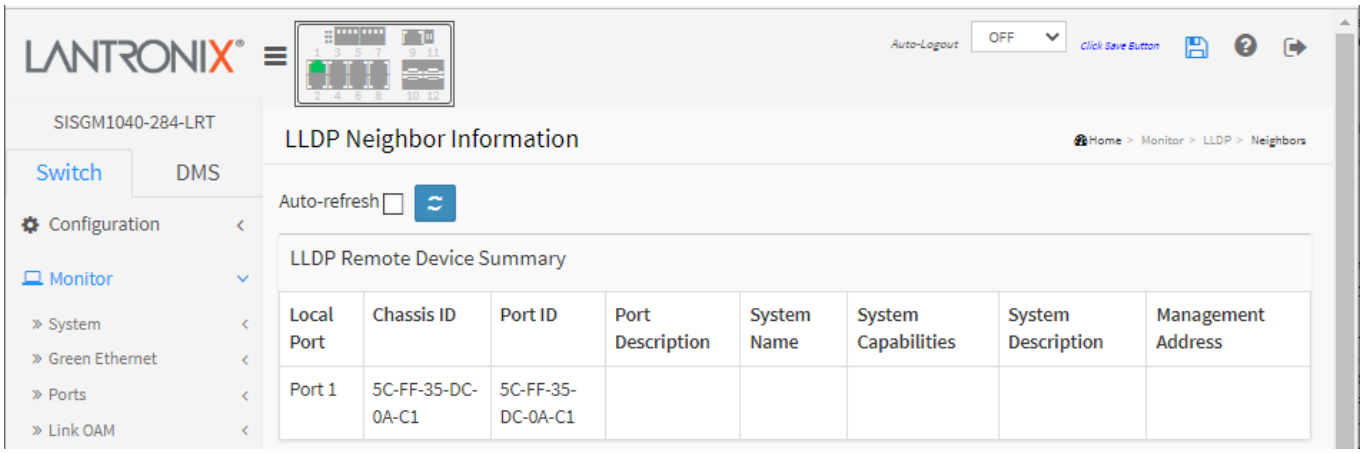
Refresh: Refreshes the displayed table starting from the input fields.

<< : Updates the table starting from the first entry in the MLD SFM Information Table.

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

Monitor > LLDP > LLDP Neighbor

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



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

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

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

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

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

System Capabilities: System Capabilities describes the neighbor unit's capabilities. The possible capabilities are:

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

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

System Description: System Description is the description advertised by the neighbor unit.

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

Buttons

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

Refresh: Click to immediately refresh the page.

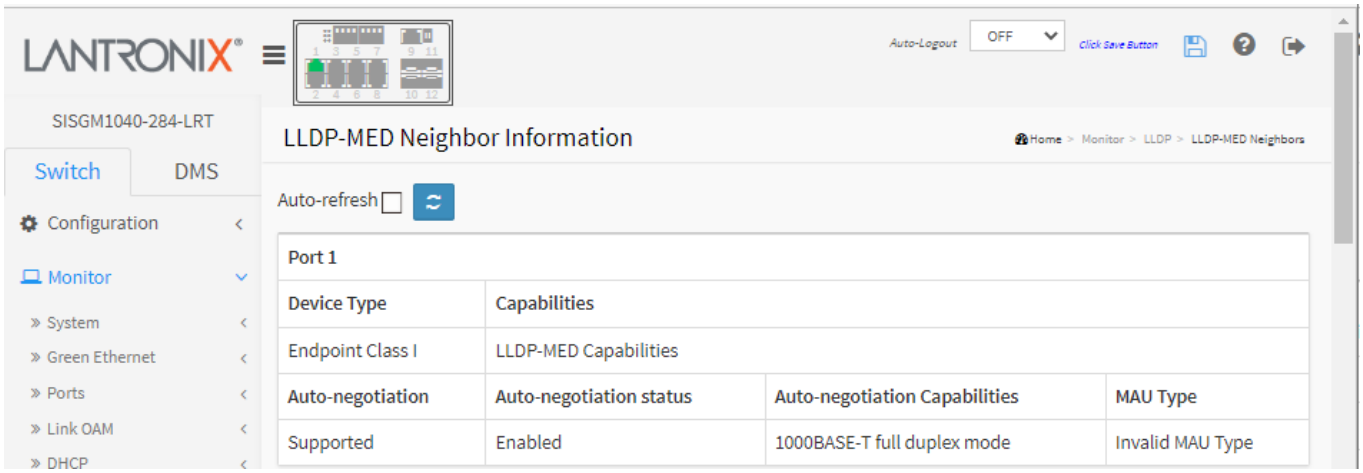
Messages:

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

'Tx Hold' must be an integer value between 2 and 10 times

Monitor > LLDP > LLDP-MED Neighbors

This page provides a status overview of all LLDP-MED neighbors. The displayed table contains a row for each port on which an LLDP neighbor is detected. This function applies to VoIP devices which support LLDP-MED.



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: Describes the neighbor 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:

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

Voice Signalling - for use in network topologies that require a different policy for the voice signalling than for the voice media.

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

Guest Voice Signalling - for use in network topologies that require a different policy for the guest voice signalling than for the guest voice media.

Softphone Voice - for use by softphone applications on typical data centric devices, such as PCs or laptops.

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

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

Video Signalling - for use in network topologies that require a separate policy for the video signalling than for the video media.

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

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

Defined: The network policy is defined.

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

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

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

VLAN ID: VLAN ID is the VLAN identifier (VID) for the port as defined in IEEE 802.1Q-2003. A value of 1 - 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 - 63).

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

Auto-negotiation status: 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 (Physical Medium Dependent) operating mode will be determined by the operational MAU type field value rather than by auto-negotiation.

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

MAU Type: Displays the discovered type of MAU (Medium Attachment Unit) or the message” Invalid MAU Type”.

Buttons

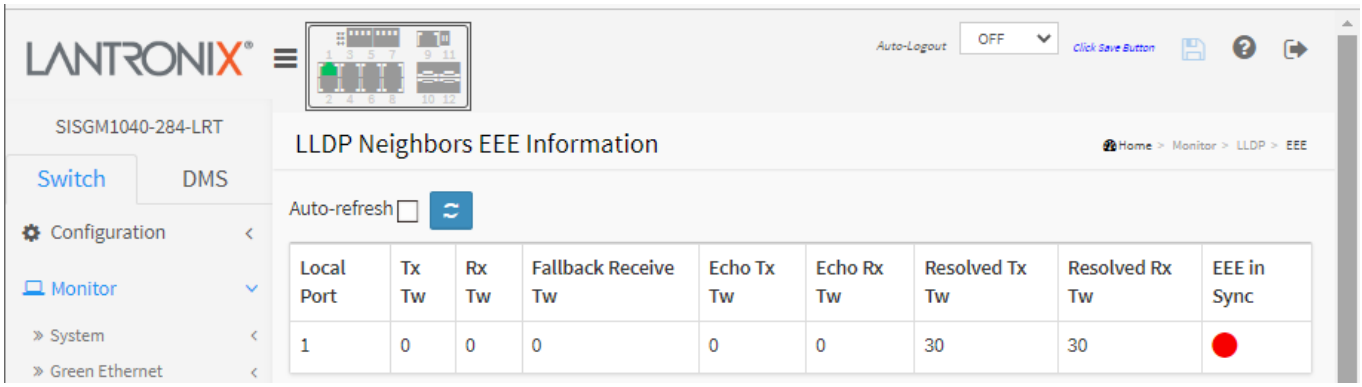
Auto-refresh: Check this box to refresh the page automatically every 3 seconds.

Refresh: Click to manually refresh the page immediately.

Monitor > LLDP > EEE

This page provides an overview of EEE information exchanged by LLDP.

By using EEE power savings can be achieved at the expense of traffic latency. This latency occurs due to that the circuits EEE turn off to save power, need time to boot up before sending traffic over the link. This time is called "wakeup time". To achieve minimal latency, devices can use LLDP to exchange information about their respective TX and RX "wakeup time " as a way to agree on the minimum wakeup time they need.



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

Tx Tw: The link partner's maximum time that transmit path can hold-off sending data after deassertion of LPI (Low Power Idle). EEE saves energy by cycling between Active and Low Power Idle.

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

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

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

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

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

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

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

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

Green - Switch and link partner have agreed on wakeup time

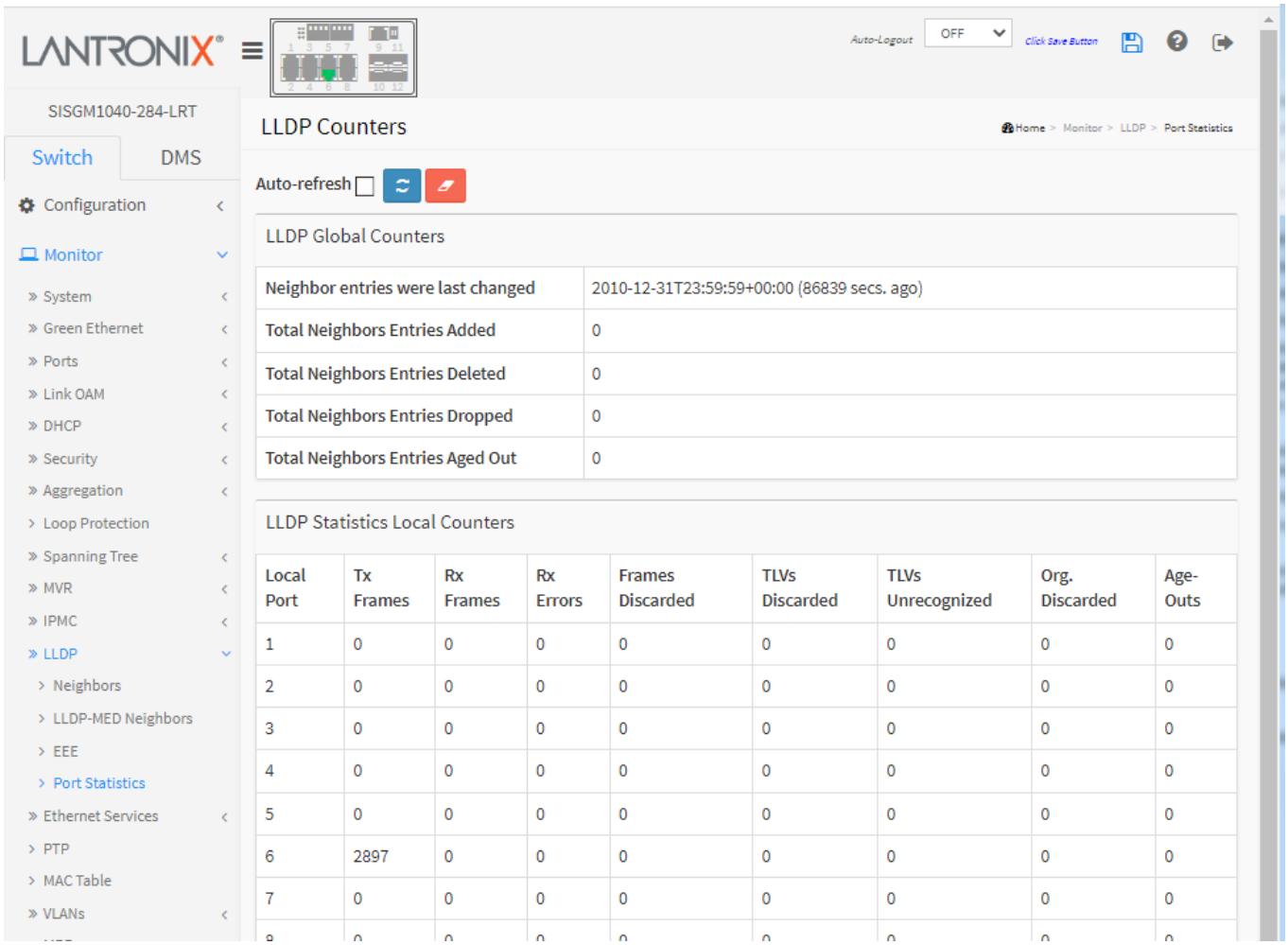
Buttons

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

Refresh: Click to refresh the page.

Monitor > LLDP > Port Statistics

This page provides an overview of all LLDP traffic. Two types of counters are shown. Global counters are counters that refer to the whole switch, while Local counters refer to per port counters for the currently selected switch.



LLDP Global Counters:

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

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

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

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

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

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

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

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

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

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

Frames Discarded: If a 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: If LLDP frame is received with an organizationally TLV, but the TLV is not supported the TLV is discarded and counted.

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

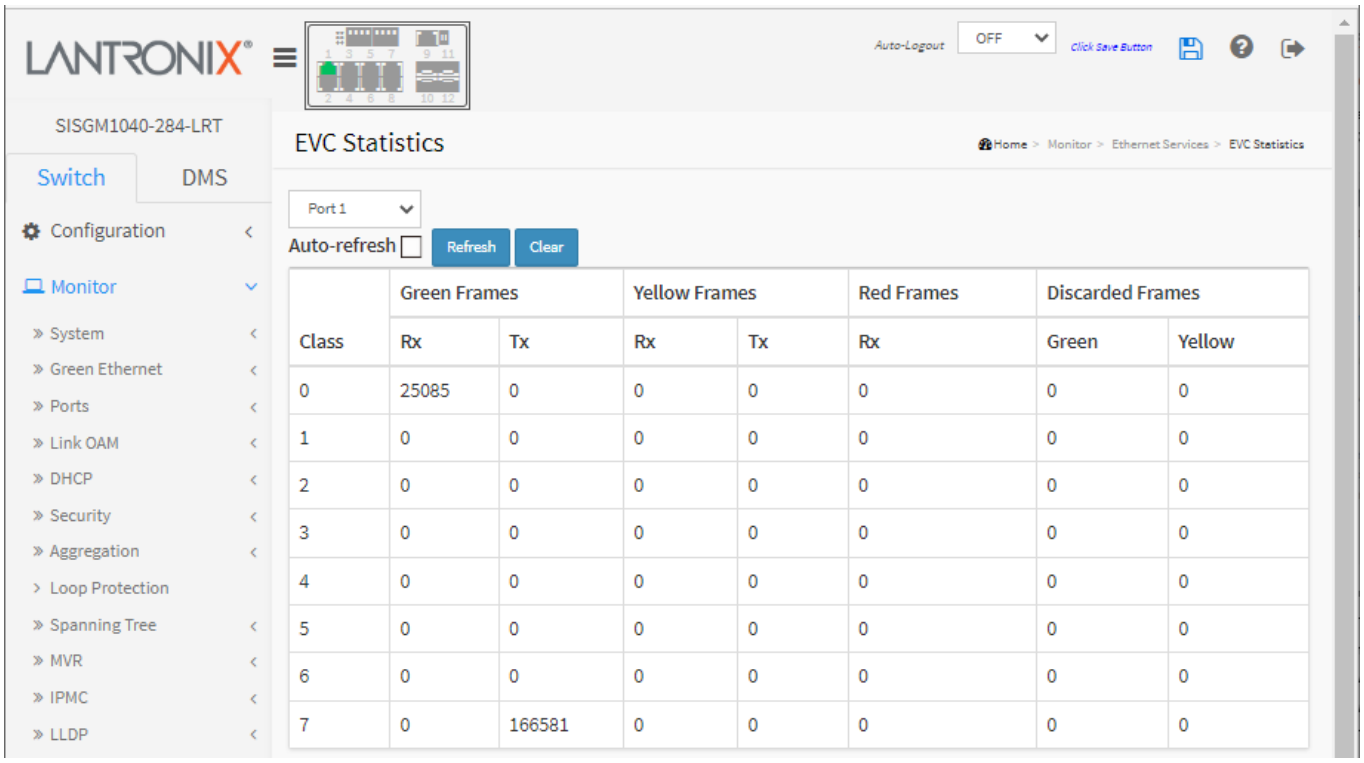
Auto-refresh: Check this box to refresh the page automatically every 3 seconds.

Refresh: Click to refresh the page.

Clear: Clears the local counters. All counters (including global counters) are cleared upon reboot.

Monitor > Ethernet Services > EVC Statistics

This page provides NNI port traffic statistics for the selected EVC. It also shows counters for UNI ports of ECEs mapping to the EVC. And the MPLS Pseudo-Wires counters are included when the PW ID is attached to the selected EVC.



Class: The traffic class for the EVC.

Rx Green: The number of green frames received.

Tx Green: The number of green frames transmitted.

Rx Yellow: The number of yellow frames received.

Tx Yellow: The number of yellow frames transmitted.

Rx Red: The number of red frames received.

Green Discarded: The number of discarded green frames.

Yellow Discarded: The number of discarded yellow frames.

Buttons

Port select box: determines which port's statistics are displayed.

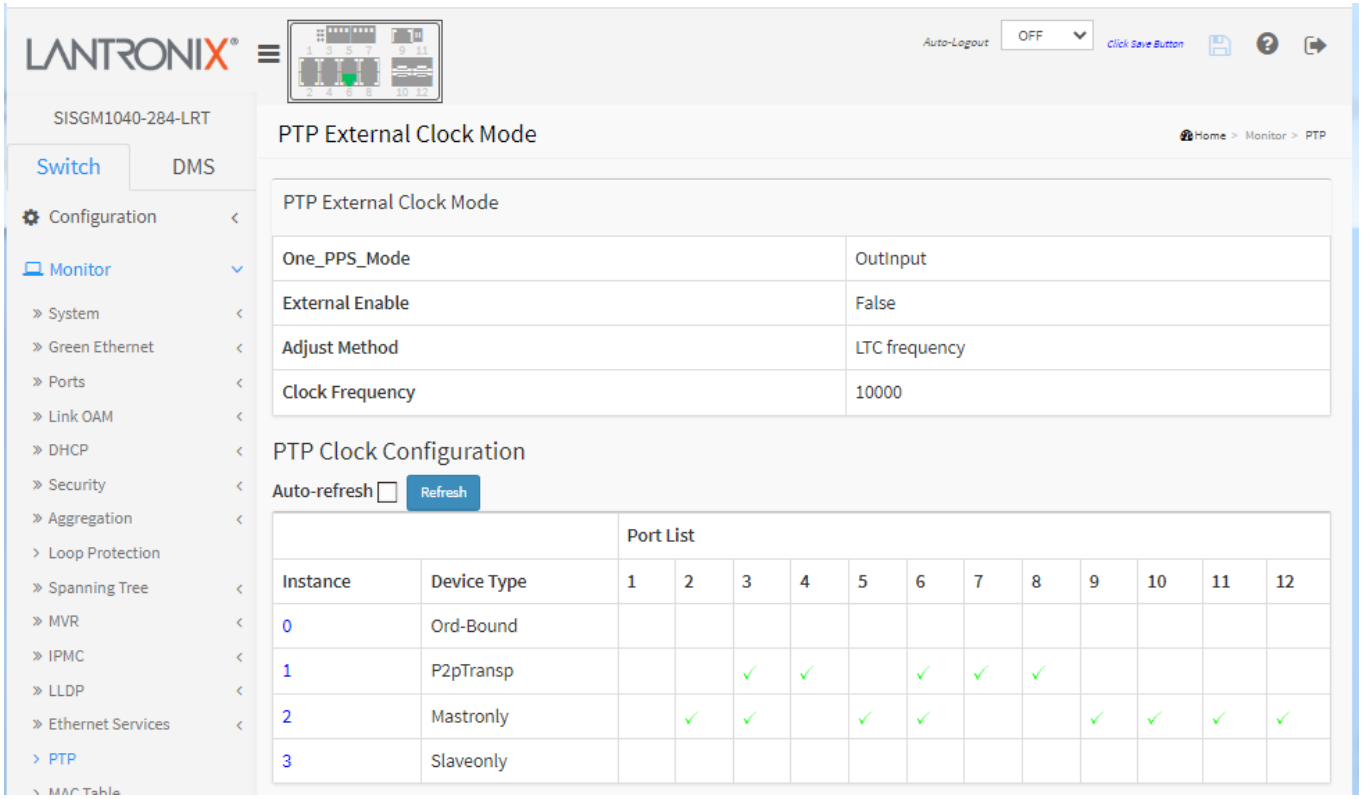
Auto-refresh: Check this box to refresh the page automatically every 3 seconds.

Refresh: Click to refresh the page immediately.

Clear: Clears the counters for selected ports.

Monitor > PTP

This page lets you view current PTP clock settings. Displays "*No Clock Instances Present*" if no PTP clocks are configured.



PTP External Clock Mode

One_PPS_Mode: Shows the current One_pps_mode settings.

Output : Enable the 1 pps clock output.

Input : Enable the 1 pps clock input.

Disable : Disable the 1 pps clock in/output.

External Enable: Shows the current External clock output configuration.

True : Enable the external clock output.

False : Disable the external clock output.

Adjust Method: Shows the current Frequency adjustment configuration.

LTC frequency : Local Time Counter (LTC) frequency control.

SyncE-DPLL : SyncE DPLL frequency control, if allowed by SyncE.

Oscillator : Oscillator independent of SyncE for frequency control, if supported by the HW.

LTC phase : Local Time Counter (LTC) phase control (assumes that the frequency is locked by means of SyncE).

Clock Frequency: Shows the current clock frequency used by the External Clock. The possible range of values is 1 Hz - 25000000 (1 - 25MHz).

PTP Clock Configuration

Instance: Indicates the Instance of a particular Clock Instance [0..3]. Click on the Clock Instance number to view the PTP Clock's Configuration details (see below).

ClkDom: Indicates the Clock domain used by the Instance of a particular Clock Instance [0..3].

Device Type: Indicates the Type of the Clock Instance. There are five Device Types.

Ord-Bound - Clock's Device Type is Ordinary-Boundary Clock.

P2p Transp - Clock's Device Type is Peer to Peer Transparent Clock.

E2e Transp - Clock's Device Type is End to End Transparent Clock.

Master Only - Clock's Device Type is Master Only.

Slave Only - Clock's Device Type is Slave Only.

Port List: Shows the ports configured for that Clock Instance with a green checkmark.

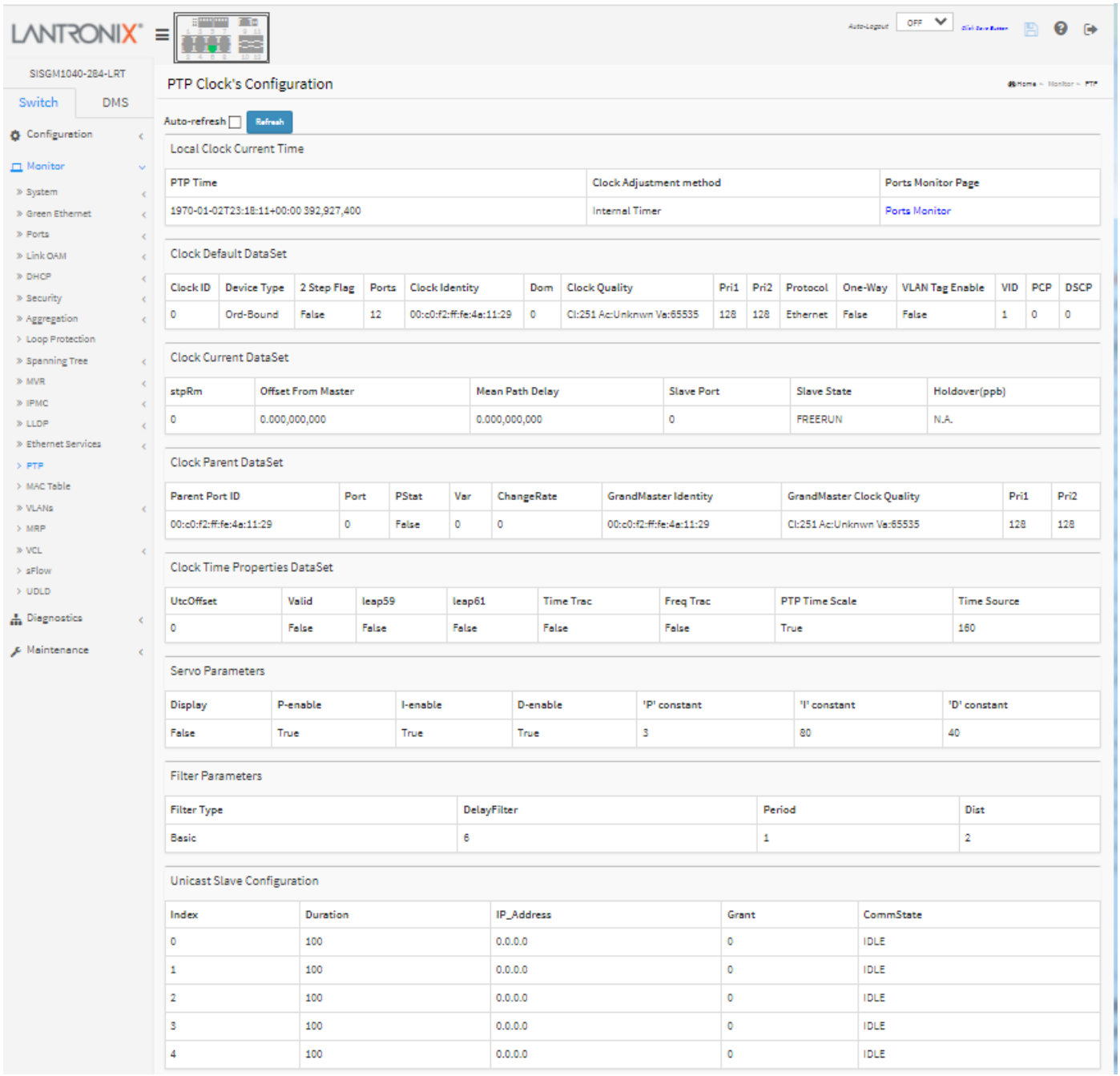
Buttons

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

Refresh: Click to refresh the page immediately.

PTP Clock's Configuration

This page lets you view current PTP clock settings



Local Clock Current Time

PTP Time: The local clock current time in the format *1970-01-01T00:29:41+00:00 487,362,920*.

Clock Adjustment method: The method of clock adjustment (e.g., Internal Timer)

Ports Monitor Page: Click the Ports Monitor link to display the “PTP Clock's Port Data Set Configuration” page (described below).

Clock Current Data Set: The clock current data set is defined in the IEEE 1588 Standard. The current data set is dynamic.

stpRm: Steps Removed : It is the number of PTP clocks traversed from the grandmaster to the local slave clock.

Offset from Master: Time difference between the master clock and the local slave clock, measured in ns.

Mean Path Delay: The mean propagation time for the link between the master and the local slave.

Clock Parent Data Set: The clock parent data set is defined in the IEEE 1588 standard. The parent data set is dynamic.

Parent Port Identity: Clock identity for the parent clock, if the local clock is not a slave, the value is the clocks own id.

Port: Port Id for the parent master port

PStat: Parents Stats (always false).

Var: It is observed parent offset scaled log variance

Change Rate: Observed Parent Clock Phase Change Rate. i.e. the slave clocks rate offset compared to the master. (unit = ns per s).

Grand Master Identity: Clock identity for the grand master clock, if the local clock is not a slave, the value is the clocks own id.

Grand Master Clock Quality: The clock quality announced by the grand master (See description of Clock Default DataSet:Clock Quality)

Pri1: Clock priority 1 announced by the grand master

Pri2: Clock priority 2 announced by the grand master.

Clock Time Properties Data Set: The clock time properties data set is defined in the IEEE 1588 Standard. The data set is both configurable and dynamic, i.e. the parameters can be configured for a grandmaster. In a slave clock the parameters are overwritten by the grandmasters timing properties. The parameters are not used in the current PTP implementation.

Valid values for the Time Source parameter are:

16 (0x10) ATOMIC_CLOCK
32 (0x20) GPS
48 (0x30) TERRESTRIAL_RADIO
64 (0x40) PTP
80 (0x50) NTP
96 (0x60) HAND_SET
144 (0x90) OTHER
160 (0xA0) INTERNAL_OSCILLATOR

Servo Parameters: The default clock servo uses a PID regulator to calculate the current clock rate. i.e.

clockAdjustment =
OffsetFromMaster/ P constant +
Integral(OffsetFromMaster)/ I constant +
Differential OffsetFromMaster)/ D constant

Display: If true then Offset From Master, MeanPathDelay and clockAdjustment are logged on the debug terminal.

P-enable: If true the P part of the algorithm is included

I-Enable: If true the I part of the algorithm is included

D-enable: If true the D part of the algorithm is included

'P' constant: [1..1000] see above

'I' constant: [1..10000] see above

'D' constant: [1..10000] see above

Unicast Slave Configuration: When operating in IPv4 Unicast mode, the slave is configured up to 5 master IP addresses. The slave then requests Announce messages from all the configured masters. The slave uses the BMC algorithm to select one as master clock, the slave then request Sync messages from the selected master.

Duration: The number of seconds a master is requested to send Announce/Sync messages. The request is repeated from the slave each Duration/4 seconds.

IP Address: IPv4 Address of the Master clock

Grant: The granted repetition period for the sync message

CommState: The state of the communication with the master, possible values are:

IDLE : The entry is not in use.

INIT : Announce is sent to the master (Waiting for a response).

CONN : The master has responded.

SELL : The assigned master is selected as current master.

SYNC : The master is sending Sync messages.

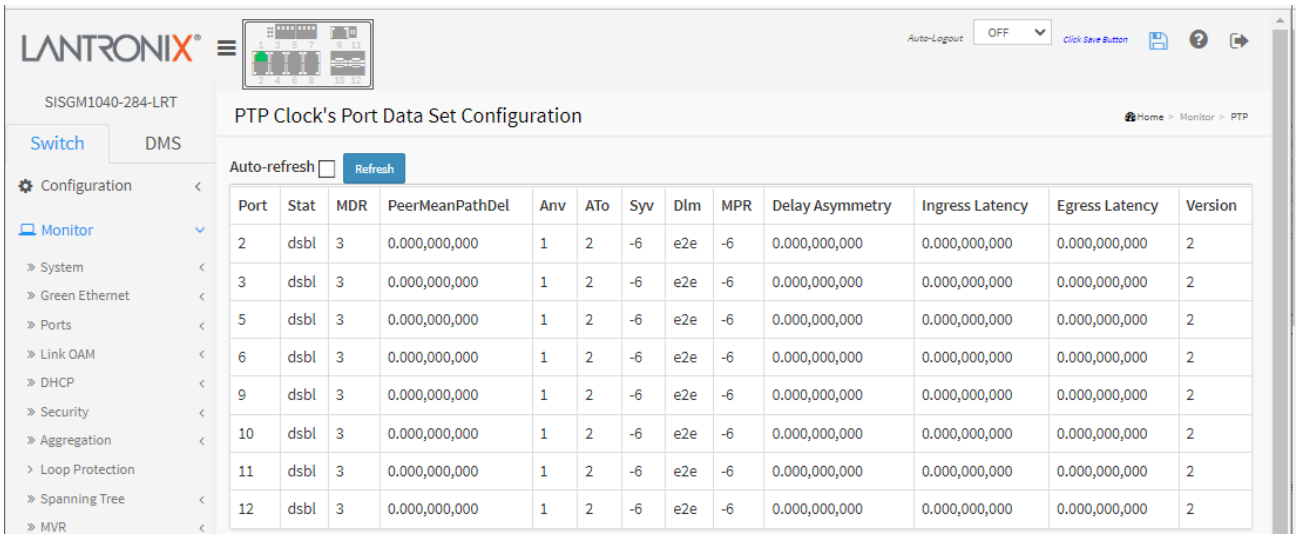
Buttons

Apply: Click to save the page immediately.

Reset: Click to reset the page immediately.

PTP Clock's Port Data Set Configuration page

The port data set is defined in the IEEE 1588 Standard.



Port	Stat	MDR	PeerMeanPathDel	Anv	ATo	Syv	Dlm	MPR	Delay Asymmetry	Ingress Latency	Egress Latency	Version
2	dsbl	3	0.000,000,000	1	2	-6	e2e	-6	0.000,000,000	0.000,000,000	0.000,000,000	2
3	dsbl	3	0.000,000,000	1	2	-6	e2e	-6	0.000,000,000	0.000,000,000	0.000,000,000	2
5	dsbl	3	0.000,000,000	1	2	-6	e2e	-6	0.000,000,000	0.000,000,000	0.000,000,000	2
6	dsbl	3	0.000,000,000	1	2	-6	e2e	-6	0.000,000,000	0.000,000,000	0.000,000,000	2
9	dsbl	3	0.000,000,000	1	2	-6	e2e	-6	0.000,000,000	0.000,000,000	0.000,000,000	2
10	dsbl	3	0.000,000,000	1	2	-6	e2e	-6	0.000,000,000	0.000,000,000	0.000,000,000	2
11	dsbl	3	0.000,000,000	1	2	-6	e2e	-6	0.000,000,000	0.000,000,000	0.000,000,000	2
12	dsbl	3	0.000,000,000	1	2	-6	e2e	-6	0.000,000,000	0.000,000,000	0.000,000,000	2

Port: Port number [1..max port no].

Stat: Current state of the port.

MDR: log Min Delay Req Interval: the delay request interval announced by the master.

Peer Mean Path Del: The path delay measured by the port in P2P mode. In E2E mode this value is 0.

Anv: The interval for issuing announce messages in master state.

ATo: The timeout for receiving announce messages on the port.

Syv: The interval for issuing sync messages in master.

Dlm: delayMechanism: The delay mechanism used for the port:

e2e End to end delay measurement.

p2p Peer to peer delay measurement.

MPR: The interval for issuing Delay_Req messages for the port in E2e mode. This value is announced from the master to the slave in an announce message. The value is reflected in the MDR field in the Slave. The interval for issuing Pdelay_Req messages for the port in P2P mode.

Note: The interpretation of this parameter has changed from release 2.40. In earlier versions the value was interpreted relative to the Sync interval, this was a violation of the standard, so now the value is interpreted as an interval. I.e. MPR = 0 => 1 Delay_Req pr sec, independent of the Sync rate.

Delay Asymmetry: The transmission delay asymmetry for a link. See IEEE 1588 Section 7.4.2 Communication path asymmetry.

Version: The current implementation only supports PTP version 2.

Ingress latency: Ingress latency measured in ns, as defined in IEEE 1588 Section 7.3.4.2.

Egress Latency: Egress latency measured in ns, as defined in IEEE 1588 Section 7.3.4.2.

Buttons

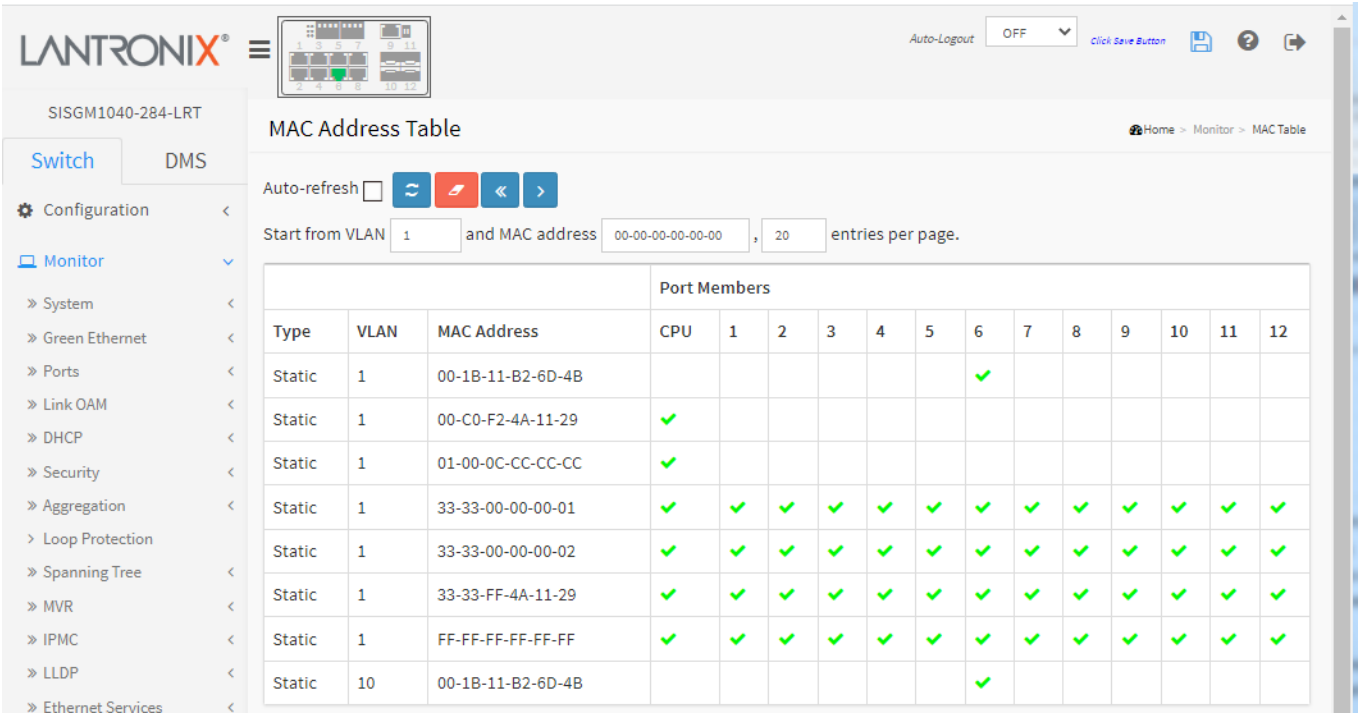
Auto-refresh: Check this box to refresh the page automatically every 3 seconds.

Refresh: Click to manually refresh the page immediately.

Monitor > MAC Table

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

Each page shows up to 999 entries from the MAC 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 MAC Table. The first entry displayed is the one with the lowest VLAN ID and the lowest MAC address found in the MAC Table.



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: A green checkmark indicates the ports that are members of the entry (CPU and ports 1-12).

Buttons

Auto-refresh : Click for an automatic page refresh every 3 seconds.

Refresh: Refreshes the displayed table starting from the "Start from MAC address" and "VLAN" input fields.

: Flushes all dynamic entries.

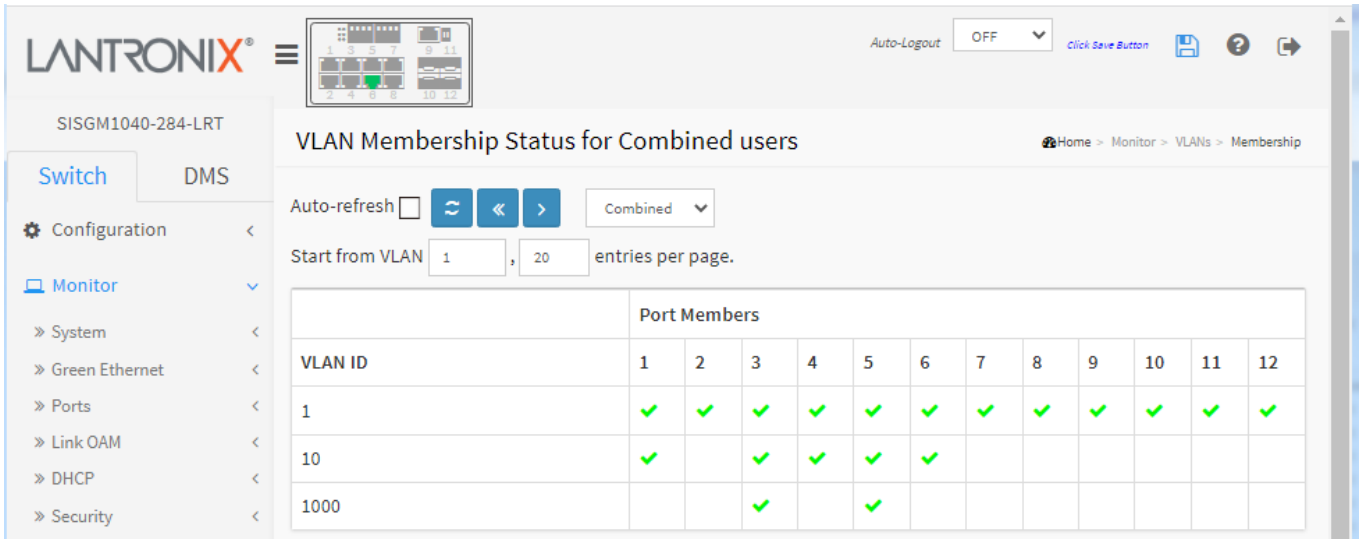
<< : **First page**: Updates the table starting from the first entry in the MAC Table (i.e., the entry with the lowest VLAN ID and MAC address).

< : **Next page**: Updates the table, starting with the entry after the last entry currently displayed.

Monitor > VLANs > Membership

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

Each page shows up to 99 entries from the VLAN table (the default is 20), selected via 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.



VLAN User: Various internal software modules may use VLAN services to configure VLAN memberships on the fly.

The drop-down list on the right allows for selecting between showing VLAN memberships as configured by an administrator (Admin) or as configured by one of these internal software modules.

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

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

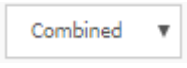
Port Members: A row of check boxes for each port is displayed for each VLAN ID.

 : If a port is included in a VLAN, this image displays (port).

 : If a port is in the forbidden port list, this image displays (forbid).

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

Buttons



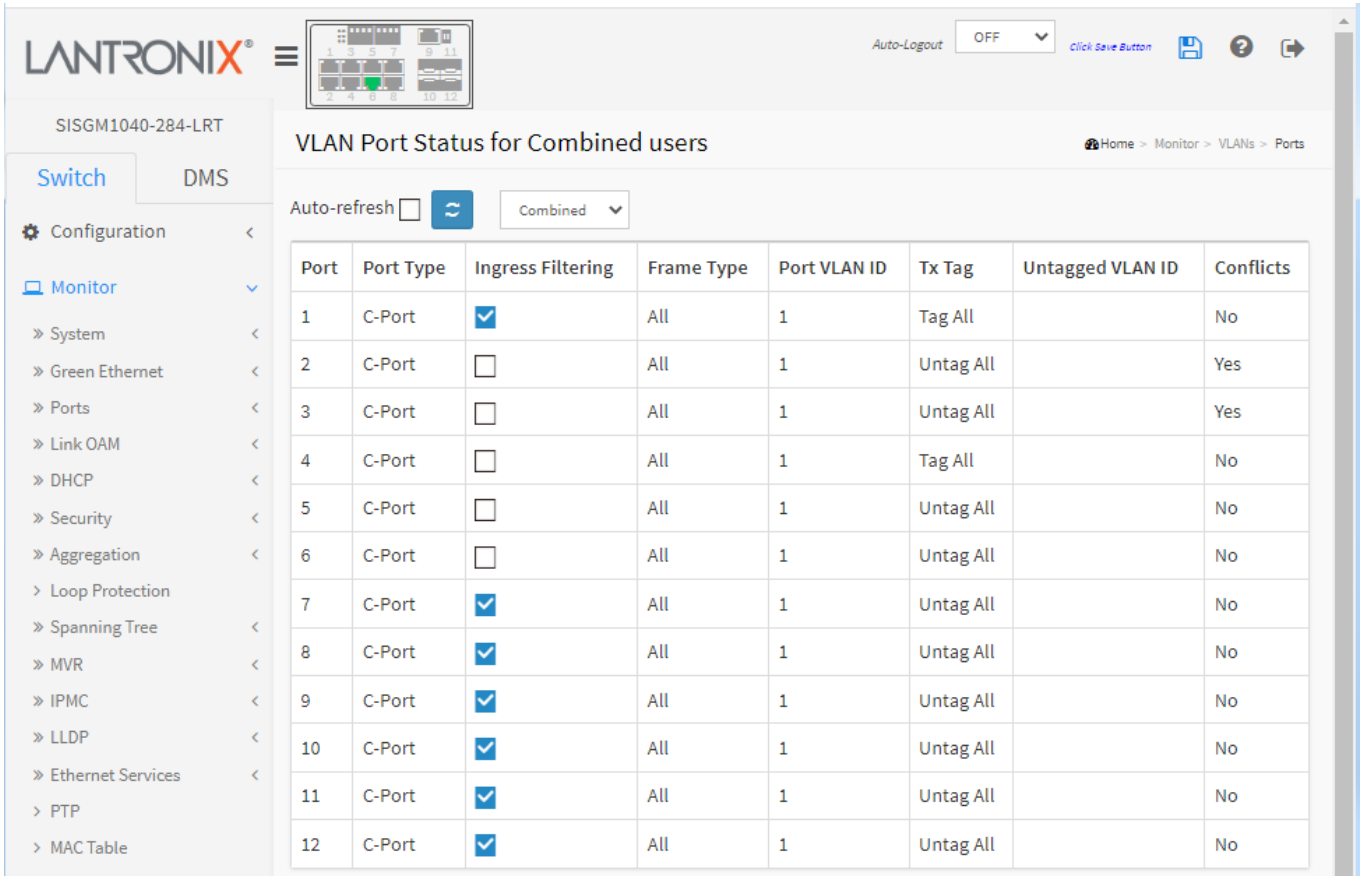
User dropdown list: Select VLAN Users from this drop down list.

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

Refresh: Click to refresh the page immediately.

Monitor > VLANs > Ports

This page provides VLAN Port Status.



VLAN User: Various internal software modules may use VLAN services to configure VLAN port configuration on the fly. The drop-down list lets you select 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*" displays 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, S-Custom-Port.) that a given user wants to configure on the port. The field is empty if not overridden by the selected user.

Ingress Filtering: Shows whether a given user wants ingress filtering enabled or not. The field is empty if not overridden by the selected user.

Frame Type: Shows the acceptable frame types (All, Tagged, Untagged) that a given user wants to configure on the port. The field is empty if not overridden by the selected user.

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 the Tx Tag requirements (Tag All, Tag PVID, Tag UVID, Untag All, Untag PVID, Untag UVID) that a given user has on a port. The field is empty if not overridden by the selected user.

Untagged VLAN ID: If Tx Tag is overridden by the selected user and is set to Tag or Untag UVID, then this field will show the VLAN ID the user wants to tag or untag on egress. The field is empty if not overridden by the selected user.

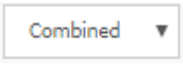
Conflicts: Two users may have conflicting requirements to a port's configuration. For instance, one user may require all frames to be tagged on egress while another requires all frames to be untagged on egress.

Since both users cannot win, this gives rise to a conflict, which is solved in a prioritized way. The Administrator has the least priority. Other software modules are prioritized according to their position in the drop-down list: The higher in the list, the higher priority.

If conflicts exist, it will be displayed as "Yes" for the "Combined" user and the offending software module.

The "Combined" user reflects what is actually configured in hardware.

Buttons



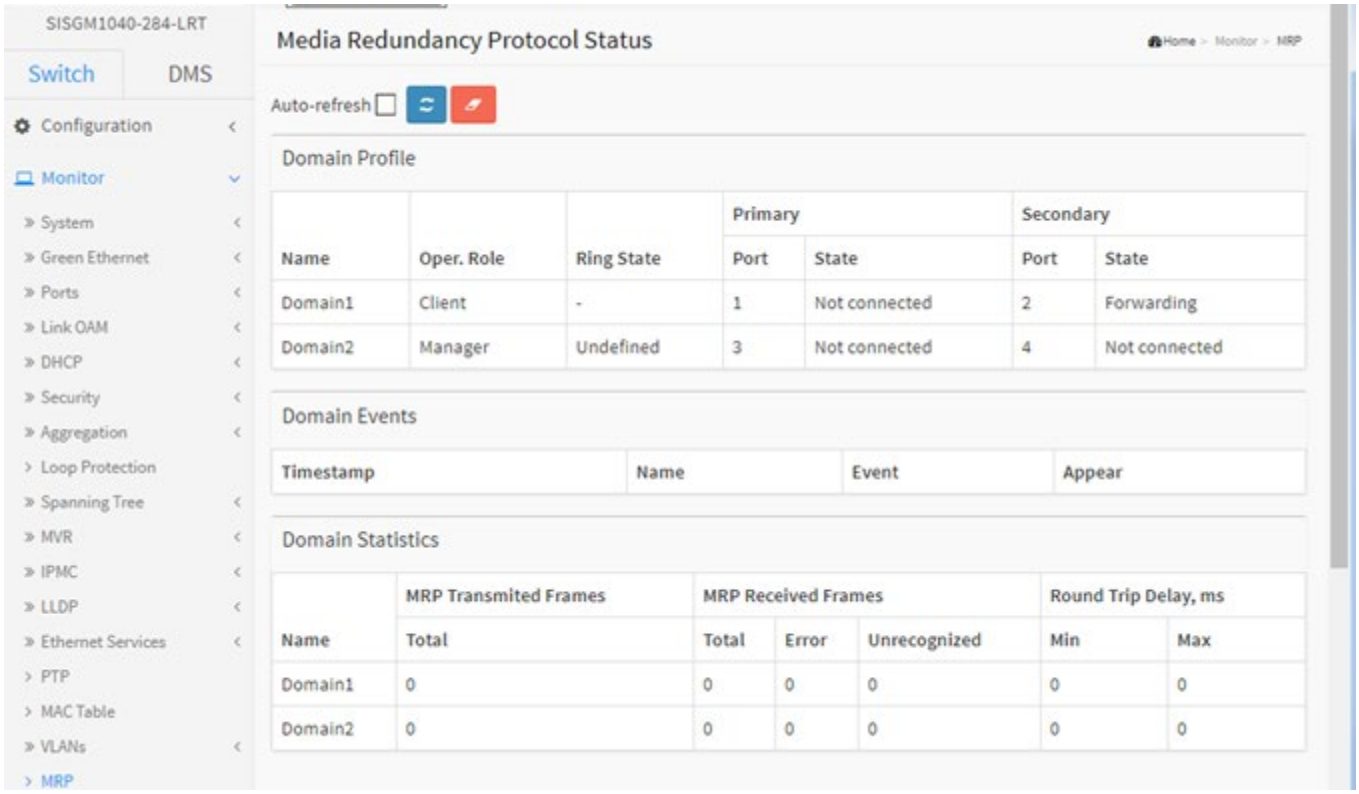
User dropdown list: Select VLAN Users from this drop down list.

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

Refresh: Click to refresh the page immediately.

Monitor > MRP

This page displays MRP (Media Redundancy Protocol) status. See “Appendix C – MRP Operation and Examples” on page 424 for more information.



Domain Profile

Name: A logical name for the MRP domain to help manage MRP domains.

Oper. Role: The operational role of an MRP entity per domain (e.g., Client or Manager).

Ring State: Ring status of the MRP entity (e.g., - or Closed or Undefined).

Primary Port: The Port number (ifIndex) of the layer 2 interface which is used as ring port 1.

Primary State: The State (ifIndex) of the layer 2 interface which is used as ring port 1 (e.g., Forwarding, Blocked, Not Connected).

Secondary Port: The Port number (ifIndex) of the layer 2 interface which is used as ring port 2.

Secondary State: The State (ifIndex) of the layer 2 interface which is used as ring port 2 (e.g., Forwarding, Blocked, Not Connected).

Domain Events

Timestamp: The date and time of the logged event.

Name: A logical name for the MRP domain.

Event: Event type e.g., Ring Open).

Appear: Event appear (true) or disappear (false).

Domain Statistics

Name: The logical name of the MRP domain.

MRP Transmitted Frames – Total: The total transmitted frames.

MRP Received Frames: The total received frames (Total, Error, and Unrecognized frames).

Round Trip Delay (ms): Round-Trip-Delay (in milliseconds) which was measured since startup. Minimum and maximum values.

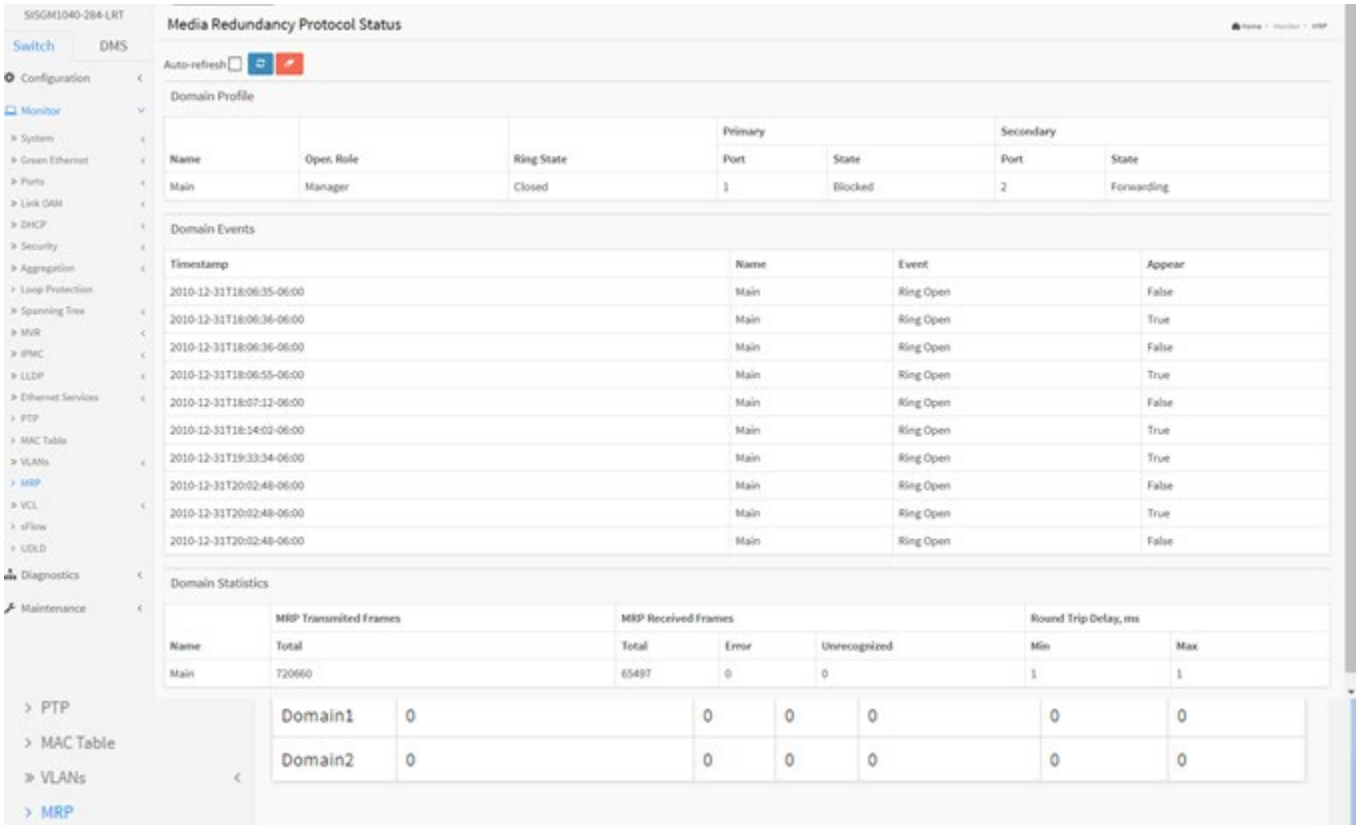
Buttons:

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

Refresh: Click to manually refresh the page immediately.

Clear: Clears the stratus parameters.

Example:

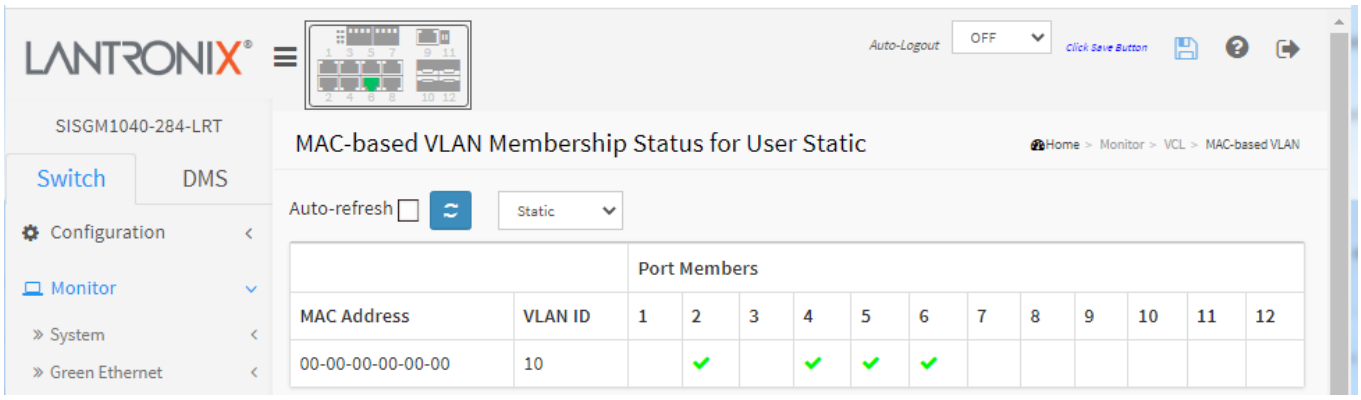


Monitor > VCL > MAC-based VLAN

This page shows MAC-based VLAN entries configured by various MAC-based VLAN users. The following VLAN User types are supported:

CLI/Web/SNMP : These are referred to as static.

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



MAC Address: Indicates the MAC address.

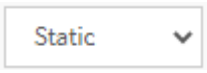
VLAN ID: Indicates the VLAN ID.

Port Members: Port members of the MAC-based VLAN entry.

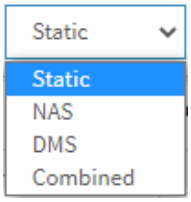
Buttons

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

Refresh: Refreshes the displayed table.

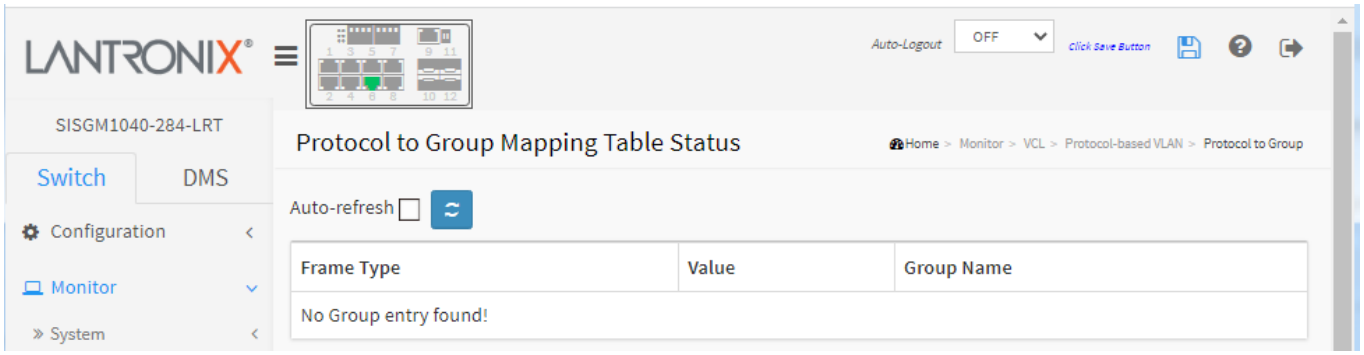


: **User Select dropdown** : select the set of users that you want statistics displayed for.



Monitor > VCL > Protocol-based VLAN > Protocol to Group

This page shows you the protocols to Group Name (unique for each Group) mapping entries for the switch .



Frame Type: Frame Type can have one of these values: ***Ethernet***. ***LLC***, or ***SNAP*** as described below.

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

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

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

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 the string is a hexadecimal value in the ranges 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 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.

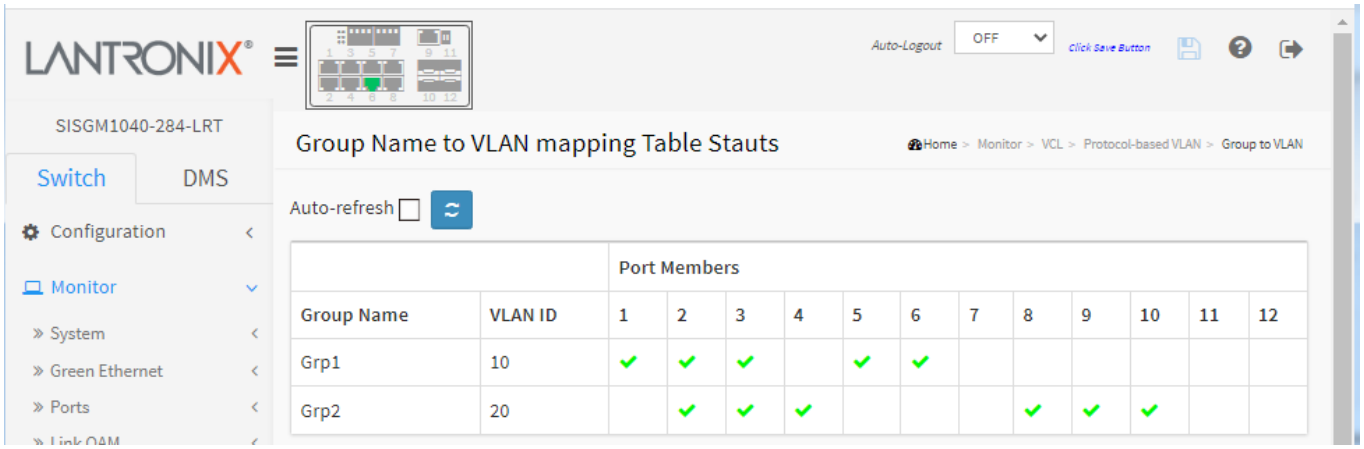
Buttons

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

Refresh: Refreshes the displayed table.

Monitor > VCL > Protocol-based VLAN > Group to VLAN

This page displays the configured Group Name to a VLAN for the switch.



Group Name: A valid Group Name is a string of up to 16 characters which consists of a combination of alphabets (a-z or A-Z) and integers (0-9). No special character is allowed. whichever Group name you try map to a VLAN must be present in Protocol to Group mapping table and must not be pre-used by any other existing mapping entry on this page.

VLAN ID: Indicates the ID to which Group Name will be mapped. A valid VLAN ID ranges from 1-4095.

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

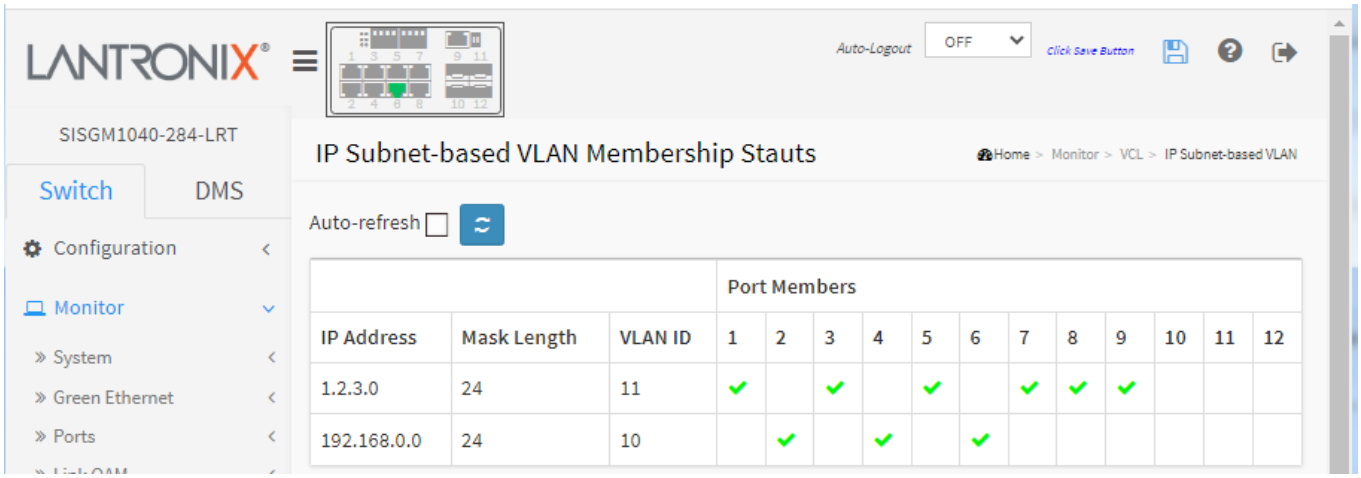
Buttons

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

Refresh: Refreshes the displayed table.

Monitor > VCL > IP Subnet-based VLAN

The page shows IP subnet-based VLAN entries. This page shows only static entries.



IP Address: Indicates the IP address.

Mask Length: Indicates the network mask length.

VLAN ID: Indicates the VLAN ID. VLAN ID can be changed for the existing entries.

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

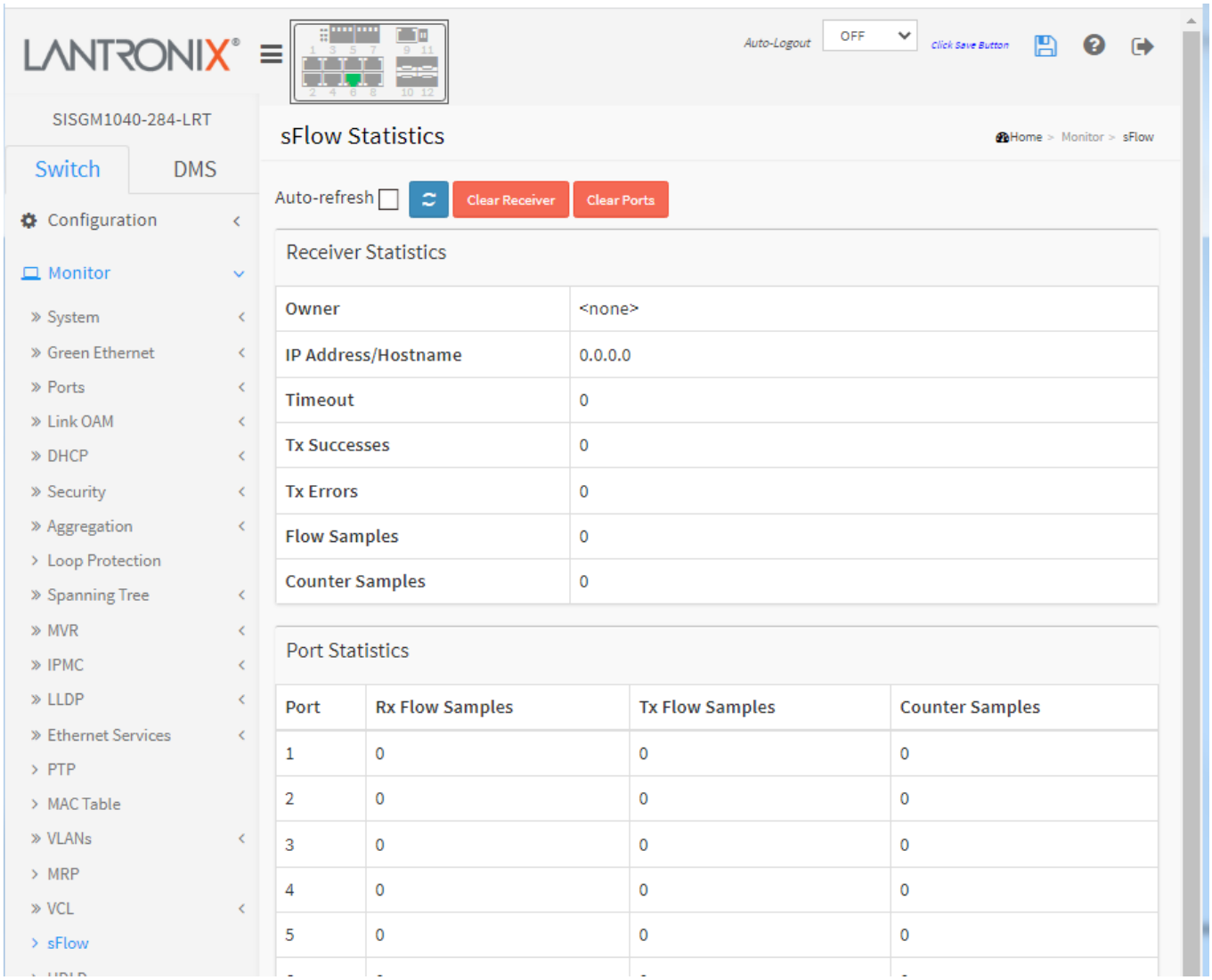
Buttons

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

Refresh: Refreshes the displayed table.

Monitor > sFlow

This page shows receiver and per-port sFlow statistics.



Receiver Statistics

Owner: This field shows the current owner of the sFlow configuration. It assumes one of three values as follows:

- If sFlow is currently unconfigured/unclaimed, Owner contains <none>.
- If sFlow is currently configured through Web or CLI, Owner contains <Configured through local management>.
- If sFlow is currently configured through SNMP, Owner contains a string identifying the sFlow receiver.

IP Address/Hostname: The IP address or hostname of the sFlow receiver.

Timeout: The number of seconds remaining before sampling stops and the current sFlow owner is released.

Tx Successes: The number of UDP datagrams successfully sent to the sFlow receiver.

Tx Errors: The number of UDP datagrams that has failed transmission. **Note**: 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.

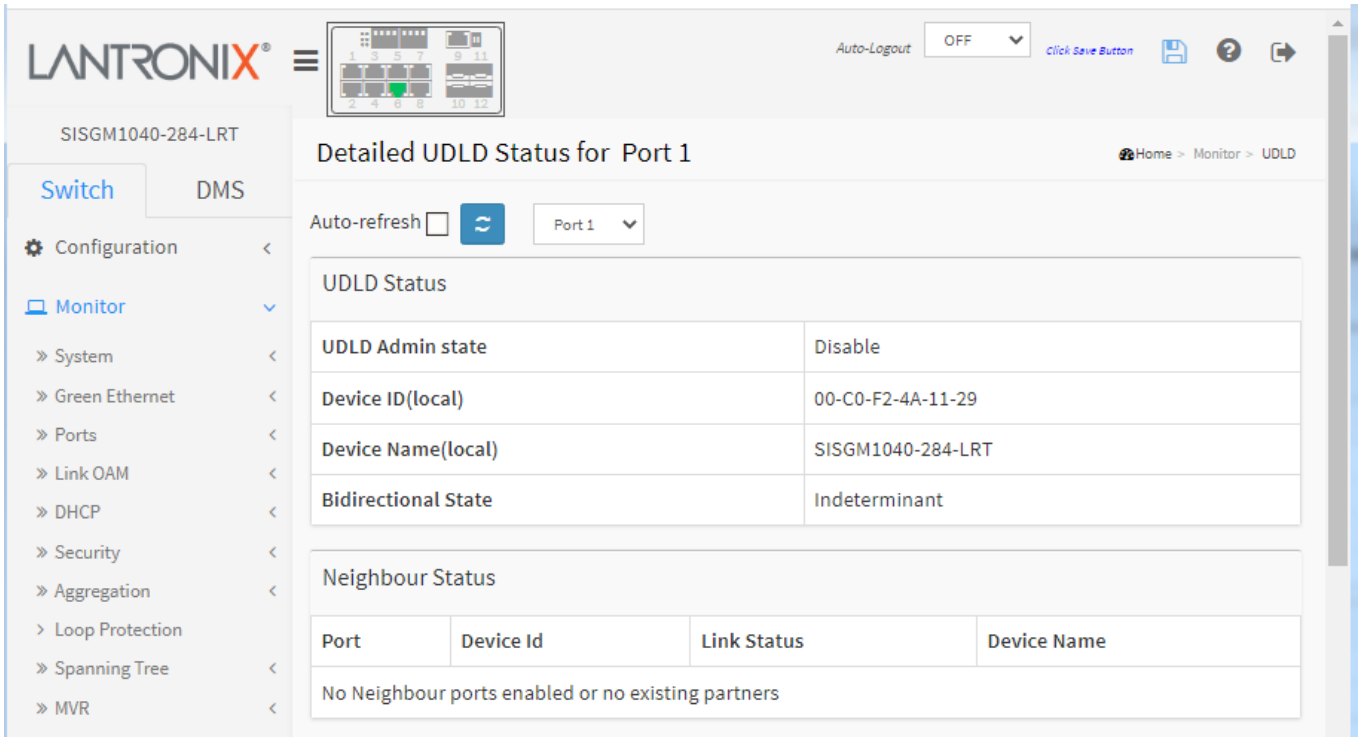
Refresh: Click to refresh the page.

Clear Receiver: Clears the sFlow receiver counters.

Clear Ports: Clears the per-port counters.

Monitor > UDLD

This page displays the UDLD status of the ports.



UDLD Status

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

Device ID(local): The ID of Device.

Device Name(local): Name of the Device.

Bidirectional State: The current state of the port (e.g., *Indeterminant*).

Neighbour Status: Displays "*No Neighbour ports enabled or no existing partners*" if none discovered.

Port: The current port of neighbour device.

Device ID: The current ID of neighbour device.

Link Status: The current link status of neighbour port.

Device Name: Name of the Neighbour Device.

Buttons

Auto-refresh: Check this box to enable an automatic refresh of the page at regular intervals.

Refresh: Click to refresh the page immediately.

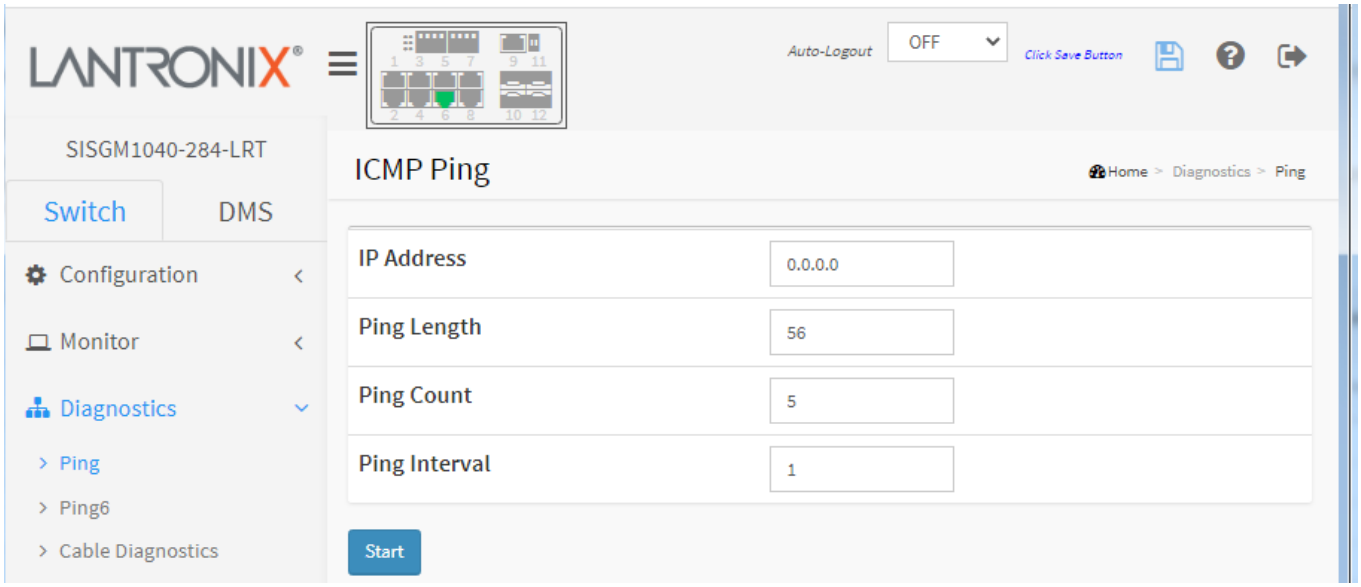
Port select box: At the dropdown list select which port's UDLD information to display.

3. Diagnostics

This menu section lets you configure ICMP Ping, ICMPv6 Ping, Cable Diagnostics, Traceroute, and Link OAM MIB Retrieval.

Diagnostics > Ping

This page allows you to issue ICMP PING packets to troubleshoot IP connectivity issues.



IP Address: The destination IP Address.

Ping Length: The payload size of the ICMP packet. Values range from 2 bytes to 1452 bytes.

Ping Count: The count of the ICMP packet. Values range from 1 time to 60 times.

Ping Interval: The interval of the ICMP packet. Values range from 0 second to 30 seconds.

Buttons:

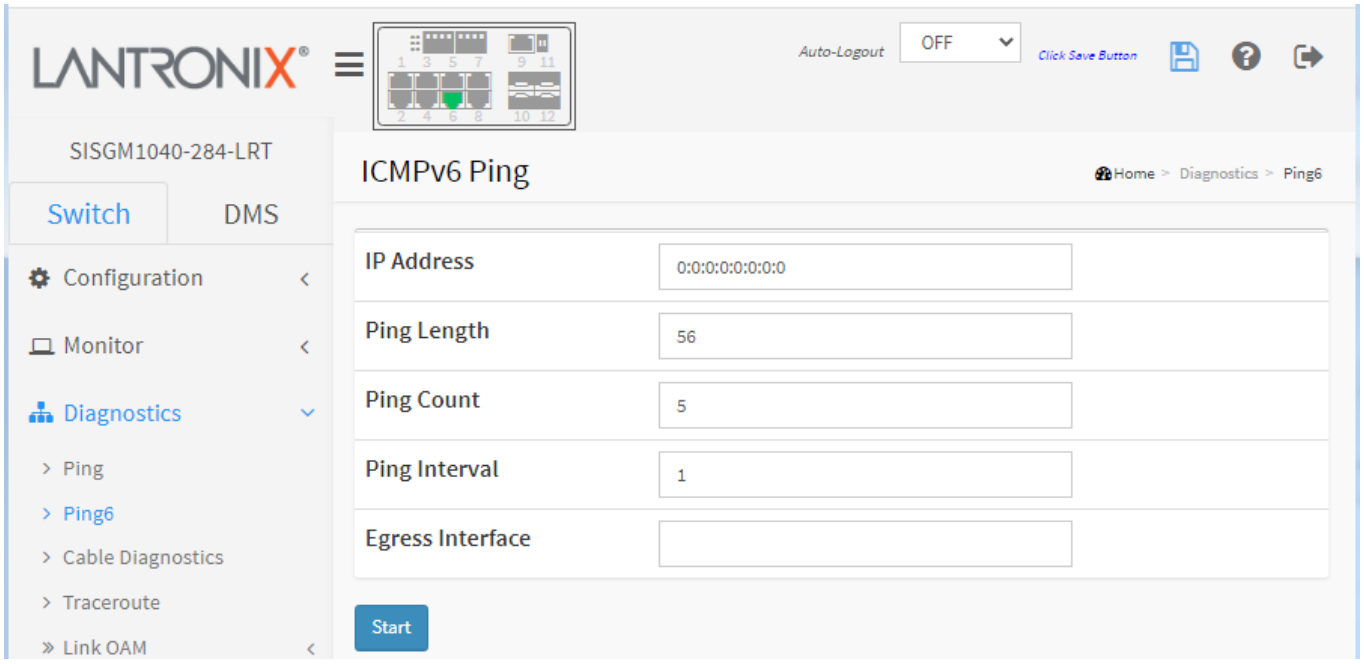
Start: After you click the Start button, ICMP packets are transmitted, and the sequence number and round trip time are displayed upon reception of a reply. The amount of data received inside of an IP packet of type ICMP ECHO_REPLY will always be 8 bytes more than the requested data space (the ICMP header). The page refreshes automatically until responses to all packets are received, or until a timeout occurs.

Example:

```
PING server 10.10.132.20, 56 bytes of data.
64 bytes from 10.10.132.20: icmp_seq=0, time=10ms
64 bytes from 10.10.132.20: icmp_seq=1, time=10ms
64 bytes from 10.10.132.20: icmp_seq=2, time=10ms
64 bytes from 10.10.132.20: icmp_seq=3, time=10ms
64 bytes from 10.10.132.20: icmp_seq=4, time=10ms
Sent 5 packets, received 5 OK, 0 bad
```

Diagnostics > Ping6

This page lets you issue ICMPv6 PING packets to troubleshoot IPv6 connectivity issues.



IP Address: The destination IP Address.

Ping Length: The payload size of the ICMP packet. Values range from 2 bytes to 1452 bytes.

Ping Count: The count of the ICMP packet. Values range from 1 time to 60 times.

Ping Interval: The interval of the ICMP packet. Values range from 0 second to 30 seconds.

Egress Interface (Only for IPv6): The VLAN ID (VID) of the specific egress IPv6 interface which ICMP packet goes. The given VID ranges from 1 to 4094 and will be effective only when the corresponding IPv6 interface is valid. When the egress interface is not given, PING6 finds the best match interface for destination. Do not specify egress interface for loopback address. Do specify egress interface for link-local or multicast address.

Buttons:

Start: After you press Start, ICMPv6 packets are transmitted, and the sequence number and round trip time are displayed upon reception of a reply. The page refreshes automatically until responses to all packets are received, or until a timeout occurs.

Example:

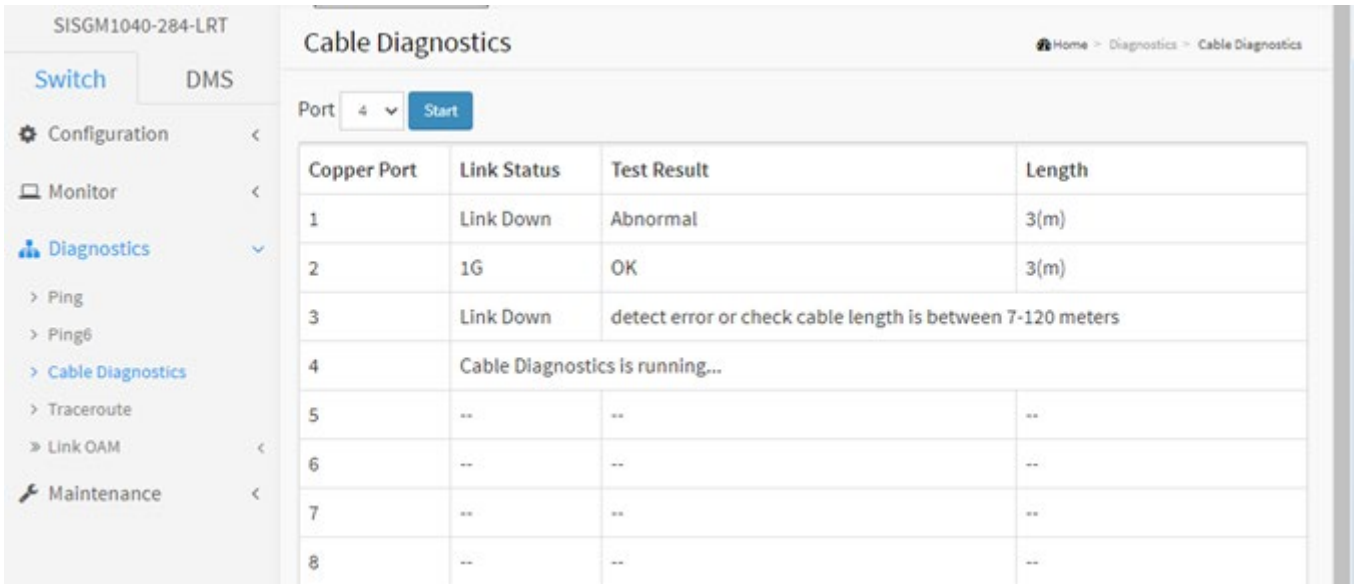
```
PING6 server ff02::2, 56 bytes of data.
64 bytes from fe80::219:5bff:fe2f:b47: icmp_seq=0, time=10ms
64 bytes from fe80::215:58ff:feed:69dd: icmp_seq=0, time=10ms
64 bytes from fe80::219:5bff:fe2f:b47: icmp_seq=1, time=10ms
64 bytes from fe80::215:58ff:feed:69dd: icmp_seq=1, time=10ms
64 bytes from fe80::219:5bff:fe2f:b47: icmp_seq=2, time=10ms
64 bytes from fe80::215:58ff:feed:69dd: icmp_seq=2, time=10ms
64 bytes from fe80::219:5bff:fe2f:b47: icmp_seq=3, time=10ms
64 bytes from fe80::215:58ff:feed:69dd: icmp_seq=3, time=10ms
64 bytes from fe80::219:5bff:fe2f:b47: icmp_seq=4, time=10ms
64 bytes from fe80::215:58ff:feed:69dd: icmp_seq=4, time=10ms
Sent 5 packets, received 10 OK, 0 bad
```

Diagnostics > Cable Diagnostics

This page is used for running the Cable Diagnostics for 10/100 and 1G copper ports.

Select a Port and press the **Start** button to run the diagnostics. This will take approximately 5 seconds. When completed, the page refreshes automatically, and you can view the cable diagnostics results in the cable status table. Note that Cable Diagnostics is only accurate for cables of length 7 - 120 meters with 5-meter accuracy.

The 10 and 100 Mbps ports will be linked down while running Cable Diagnostics, so running Cable Diagnostics on a 10 or 100 Mbps management port will cause the switch to stop responding until Cable Diagnostics is complete.



Port: Dropdown list to select the port on which you are requesting Cable Diagnostics.

Copper Port: Copper port number.

Link Status: The status of the cable.

Cable Diagnostics is running…: The test is in process.

10M: Cable is link up and correct. Speed is 10Mbps.

100M: Cable is link up and correct. Speed is 100Mbps.

1G : Cable is link up and correct. Speed is 1Gbps.

Link Down: Link down or cable is not correct.

Test Result: Test Result of the cable.

OK: Correctly terminated pair.

Abnormal: Incorrectly terminated pair or link down.

detect error or check cable length is between 7-120 meters: A specific error and length.

Length: The length (in meters) of the cable pair. The resolution is 3 meters. When Link Status is shown as follows, the length has different definition.

1G: The length is the minimum value of 4-pair.

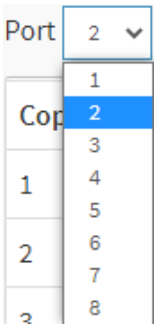
10M/100M: The length is the minimum value of 2-pair.

Link Down: The length is the minimum value of non-zero of 4-pair.

Buttons:

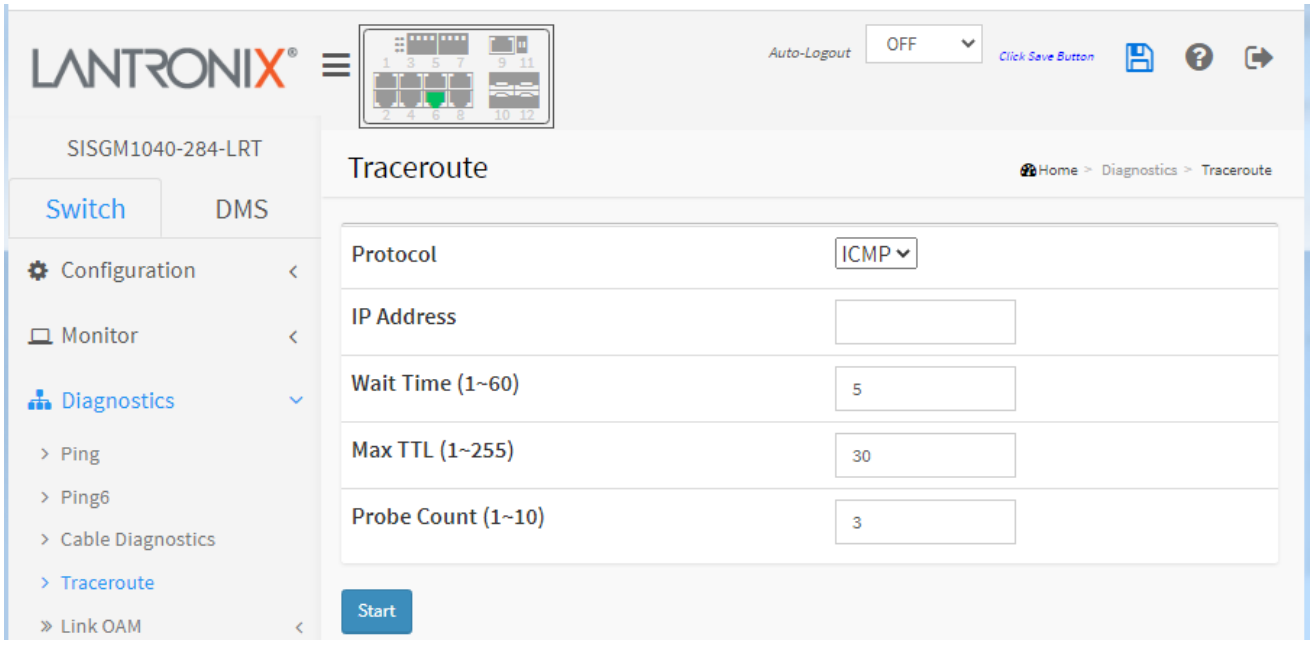
Port select : At the dropdown select the port number to test.

Start: Press to begin the diagnostics.



Diagnostics > Traceroute

This page lets you issue ICMP, TCP, or UDP packets to diagnose network connectivity issues.



Protocol: The protocol (ICMP, UDP, TCP) to use to send packets.

IP Address: The destination IP Address.

Wait Time: Set the time (in seconds) to wait for a response to a probe (the default is **5**.0 sec). Valid values are 1-60 seconds. The payload size of the ICMP packet. Valid values are 2 -1452 bytes.

Max TTL: Specifies the maximum number of hops (maximum time-to-live value) traceroute will probe. Valid values are 1-255 hops. The default is 30 hops.

Probe Count: Sets the number of probe packets per hop. Valid values are 1-10. The default is 3.

Buttons

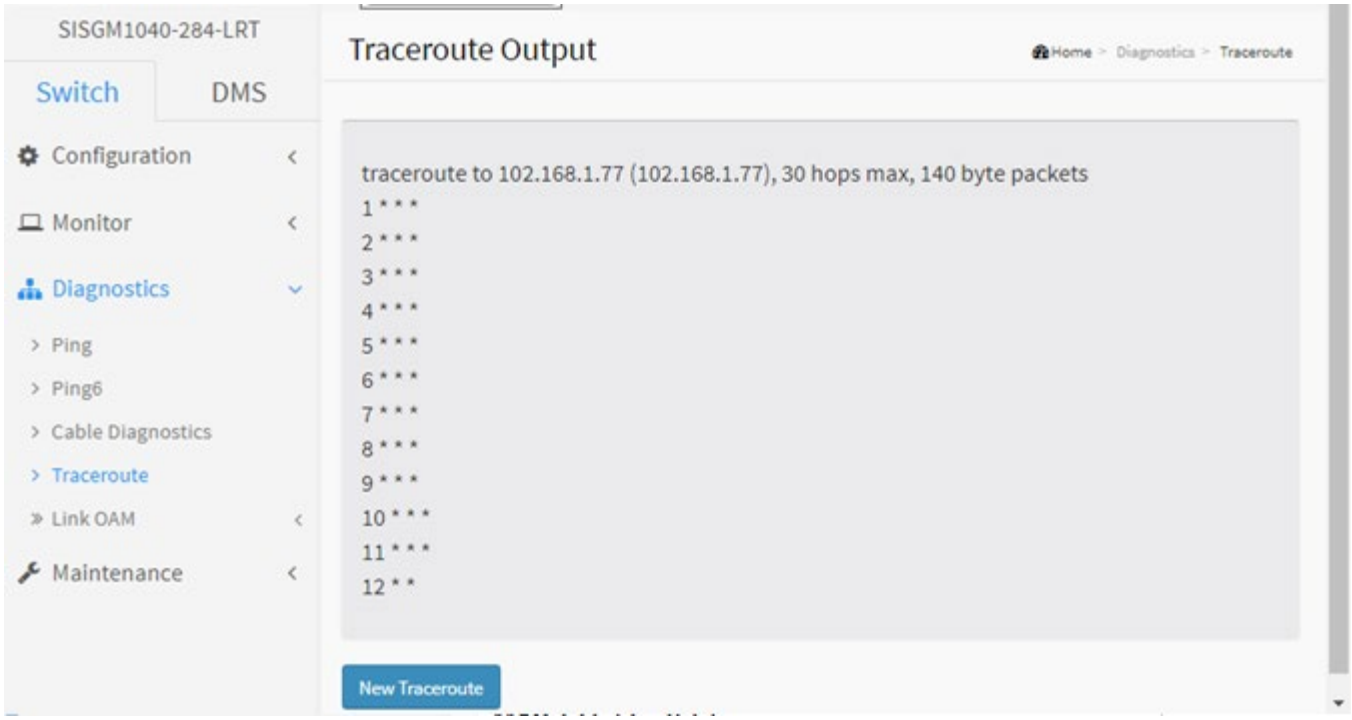
Start: Click to start transmitting the selected Protocol packets.

New Traceroute: Click to re-start Traceroute diagnostics.

After you press **Start**, Traceroute sends packets with gradually increasing TTL values, 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.

Example:

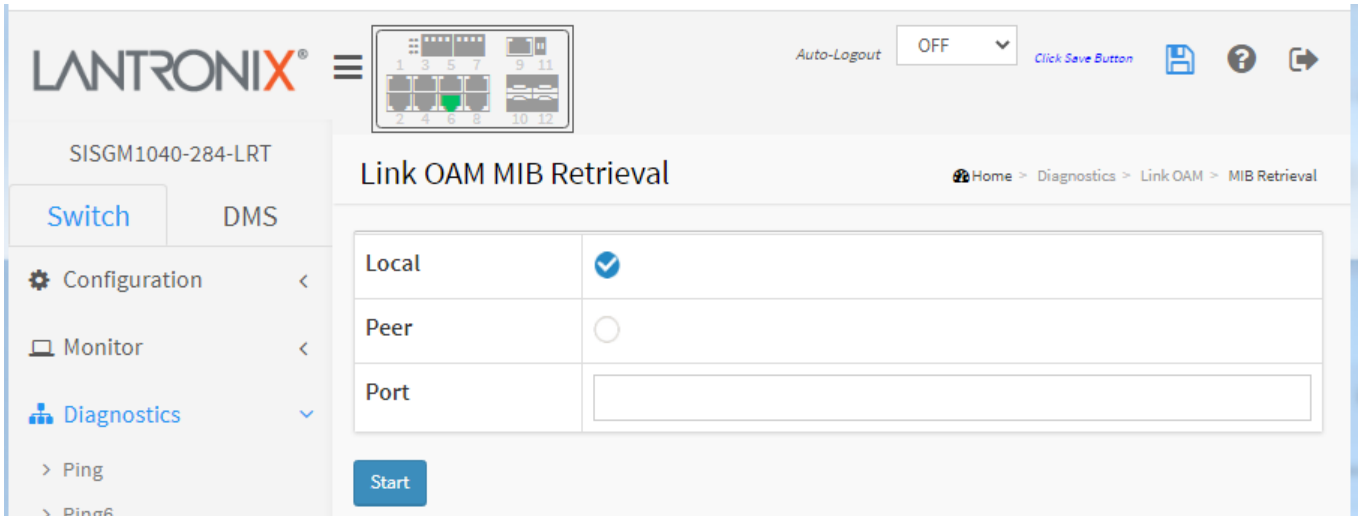
```
traceroute to 202.39.253.11 (202.39.253.11), 30 hops max, 40 byte packets
1 192.168.10.254 ae-2-3508.edge4.Atlanta2.Level3.net. (192.168.10.254) 10 ms 10 ms 10 ms
2 59-125-13-254.HINET-IP.hinet.net. (59.125.13.254) 20 ms 20 ms 20 ms
3 h146.s228.ts.hinet.net. (168.95.228.146) 20 ms 10 ms 20 ms
4 tchn-3011.hinet.net. (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
```



Messages: *traceroute: unknown host*

Diagnostics > Link OAM > MIB Retrieval

This page lets you retrieve the local or remote OAM MIB variable data on a particular port.



Select the appropriate radio button and enter the port number of the switch to retrieve the content of interest. Click on **Start** to retrieve the content. Click the **Previous** button to retrieve other content of interest.

Messages:

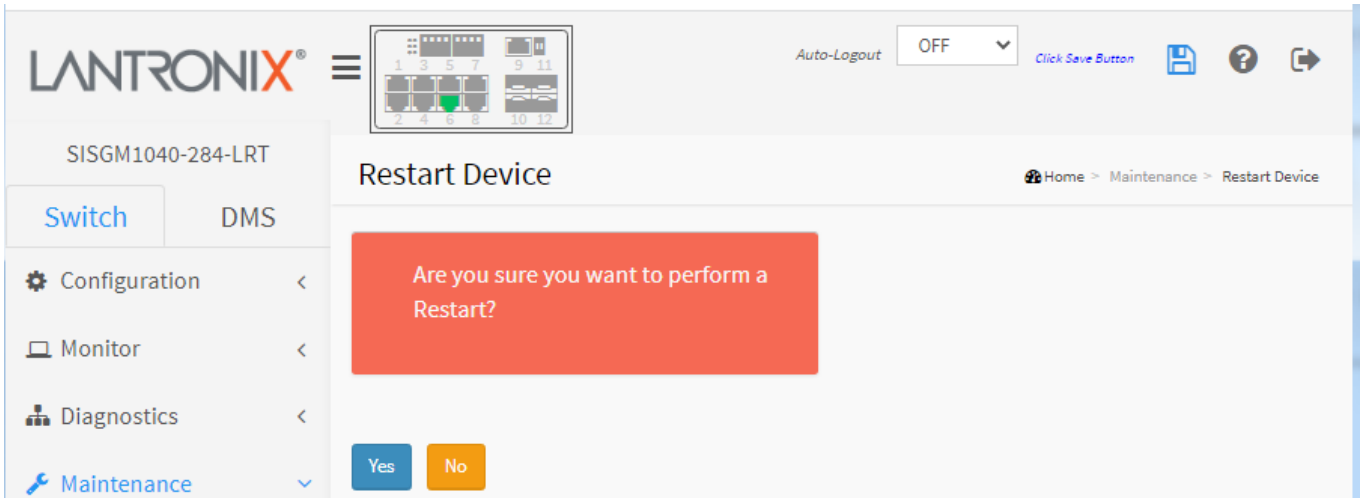
OAM Error *Invalid request on this port*

4. Maintenance

This section lets you perform a Restart Device, Reboot Schedule, Factory Defaults, Firmware Upgrade, Firmware Swap, several Configuration actions and run a Server Report.

Maintenance > Restart Device

You can restart the switch on this page. After restart, the switch will boot normally.



At the prompt "*Are you sure you want to perform a Restart?*" select ***Yes*** or ***No***:

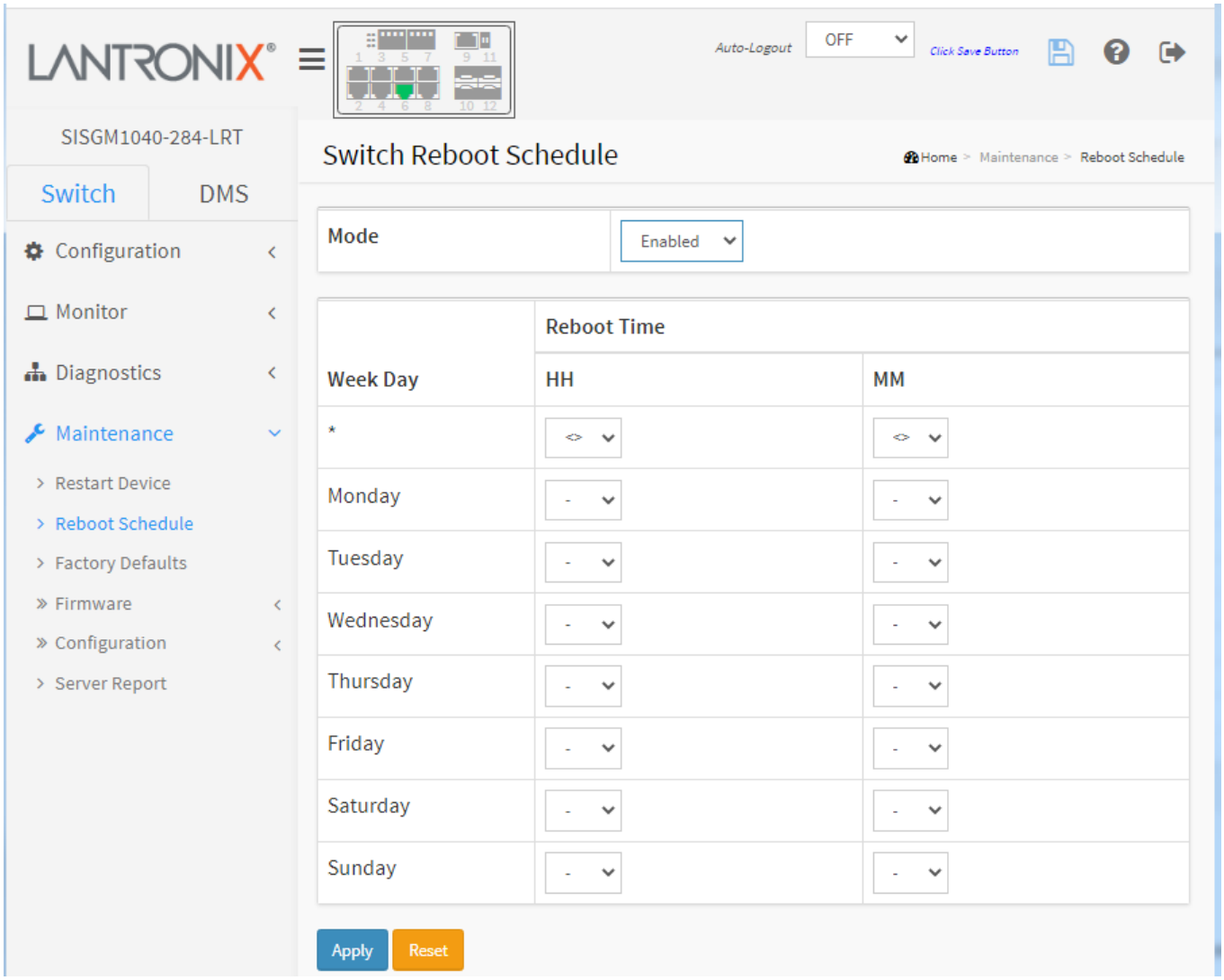
Yes: Click to restart device.

No: Click to return to the startup page at Monitor > System > Information without restarting.

Maintenance > Reboot Schedule

This page lets you schedule the day and time to reboot the switch.

On the default page, at the Mode dropdown, click **Enabled** to display the Switch Reboot Schedule:



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: For one or more schedule days, select the time in hours (HH) and Minutes (MM) to reboot the switch.

Buttons

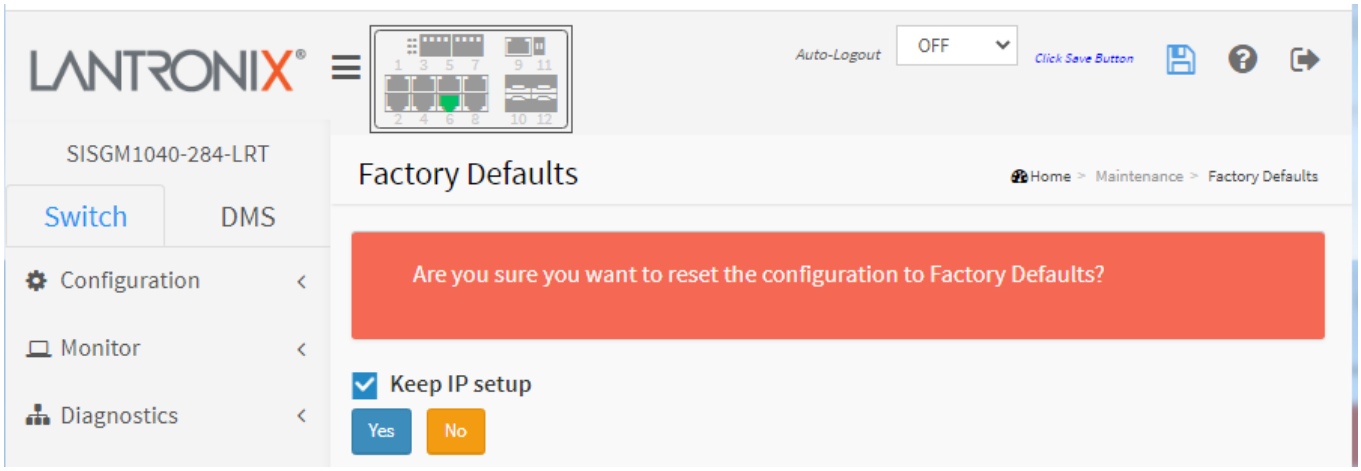
Apply: Click to save changes.

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

Maintenance > Factory Defaults

You can reset the configuration of the switch back to its factory default settings on this page. Only the IP configuration is retained (if selected).

The new configuration is available immediately, which means that no restart is necessary.



Keep IP setup: Check the checkbox if you want to keep the current IP settings.

At the prompt "*Are you sure you want to reset the configuration to Factory Defaults?*", select ***Yes*** or ***No***:

Yes: Click to reset the configuration to Factory Defaults.

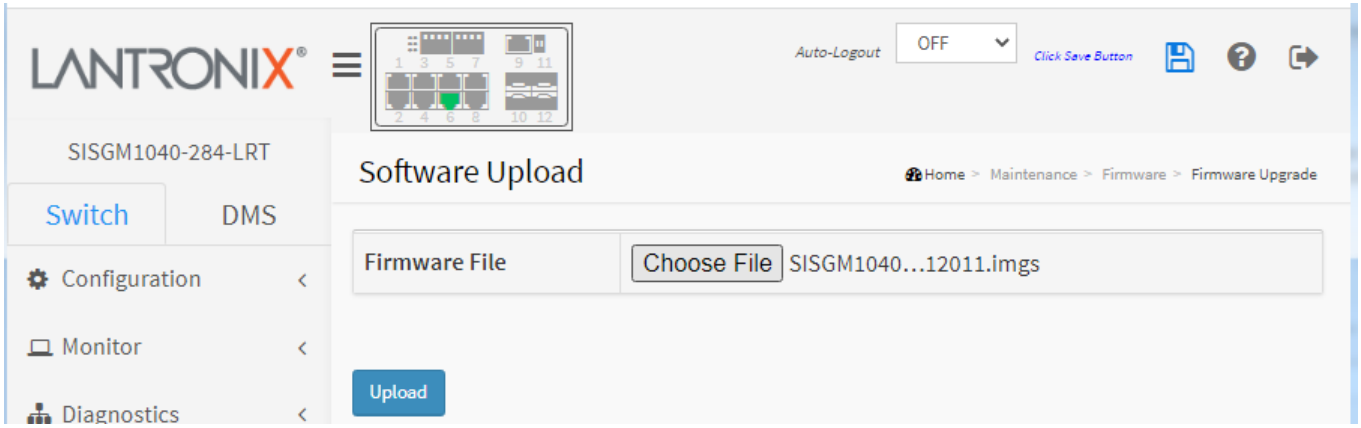
No: Click to return to the Monitor > System > Information page without resetting the configuration.

Note: Restoring factory default can also be performed by making a physical loopback between port 1 and port 2 within the first minute from switch reboot. In the first minute after boot, 'loopback' packets will be transmitted at port 1. If a 'loopback' packet is received at port 2 the switch will do a restore to defaults.

Maintenance > Firmware > Firmware Upgrade

The Software Upload page lets you update the firmware controlling the switch.

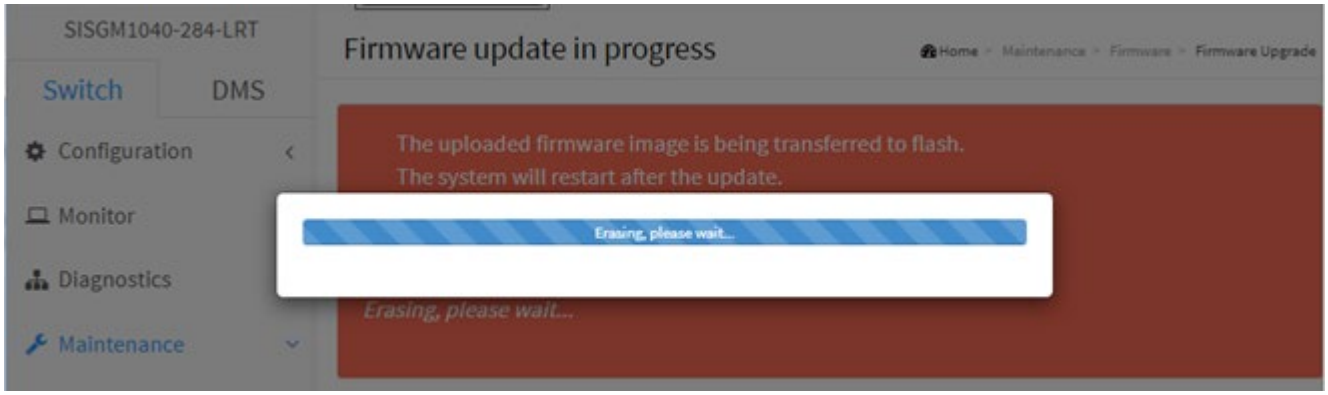
Warning: While the firmware is being updated, Web UI access appears to be defunct. The switch front panel LED flashes Green/Off with a frequency of 10 Hz while the firmware update is in progress. **Do not** restart or power off the device at this time or the switch may fail to function afterwards.



Choose File: Click and browse to the location of a software image (e.g., LTRX-SISGM1040-284-LRT_7.20.0.0170.dat).

Upload: With a proper Firmware File chosen and displayed, click the Upload button.

After the software image is uploaded, a page announces that the firmware update is in progress. After about a minute, the firmware is updated and the switch restarts.



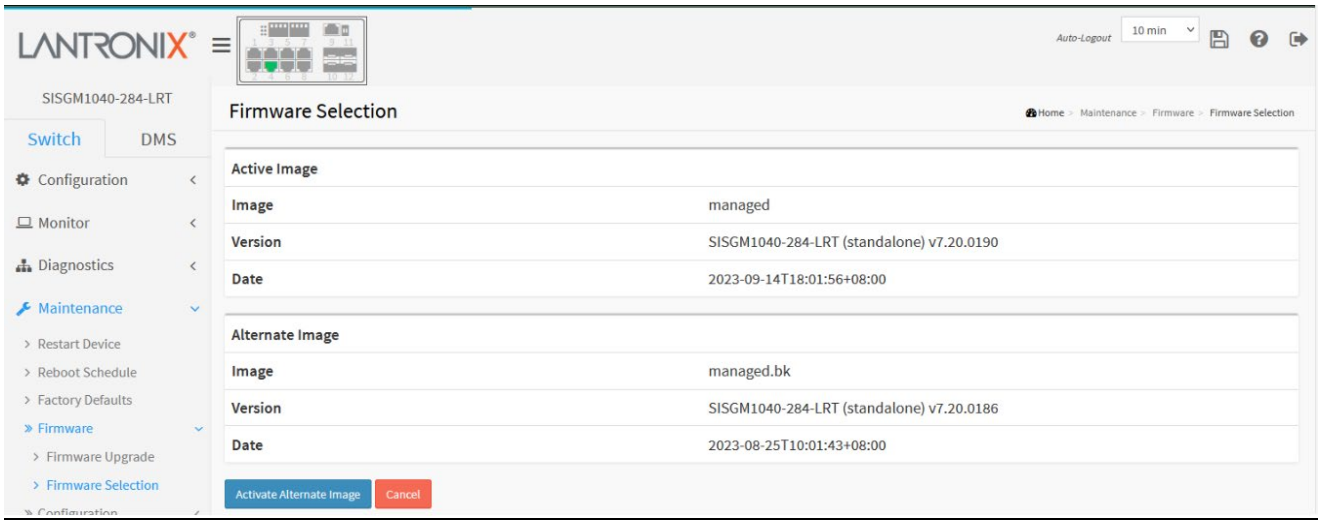
Messages: *Firmware/EZCM Upgrade Result*
The uploaded firmware image is invalid. Please use a correct firmware image.

Maintenance > Firmware > Firmware Selection

This page provides information about the Active and Alternate (backup) firmware versions in the device and lets you revert to the alternate image. This web page displays two tables with information about the active and alternate firmware images.

Note:

1. In case the active firmware image is the alternate image, only the "Active Image" table is shown. In this case, the **Activate Alternate Image** button is also disabled.
2. If the alternate image is active (due to a corruption of the primary image or by 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.



Active Image

Image: The flash index name of the Active firmware image. The name of Active (current) image is *managed*.

Version: The version of the Active firmware image (e.g., *SISGM1040-284-LRT (standalone) v7.20.0190*).

Date: The date when the Active firmware was produced (e.g., *2023-04-16T17:01:57+08:00*).

Alternate Image

Image: The name of Alternate (backup) image is *managed.bk*.

Version: The version of the Alternate firmware image (e.g., *SISGM1040-284-LRT (standalone) v7.20. 0186)*.

Date: The date when the Alternate firmware was produced (e.g., *2023-03-16T12:51:31+08:00*).

Buttons

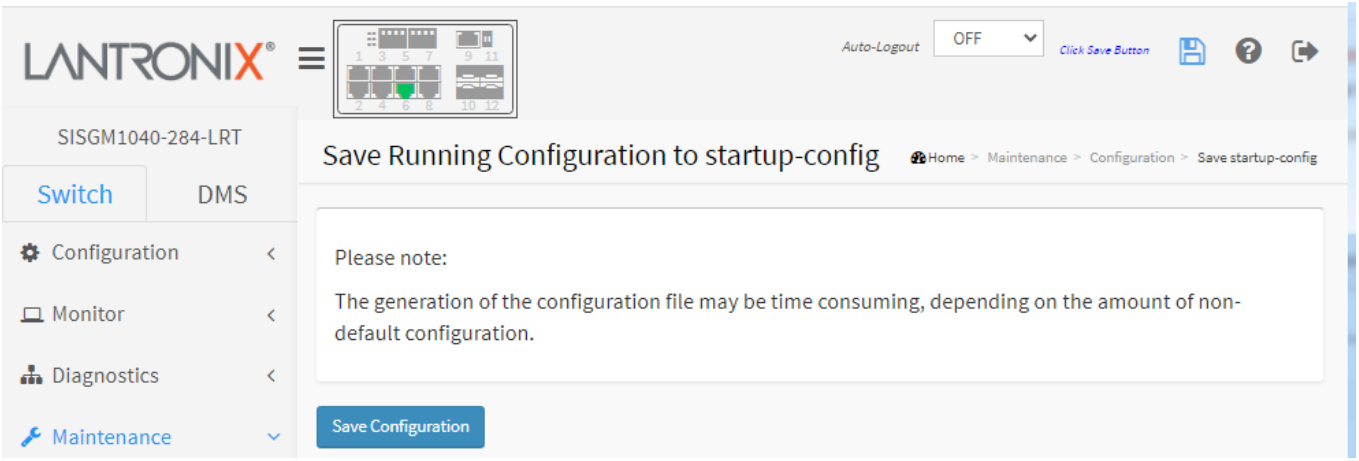
Activate Alternate Image: Click to use the Alternate image. This button may be disabled depending on system state. At the confirmation message "*Are you sure you want to activate the alternate software image?*" click the OK button to continue.

Cancel: Cancel activating the backup image. Navigates away from this page to the startup page at Monitor > System > Information.

Maintenance > Configuration > Save startup-config

This copies running-config to startup-config, thereby ensuring that the currently active configuration will be used at the next reboot.

Please note: The generation of the configuration file may be time consuming, depending on the amount of non-default configuration.



Buttons:

Save Configuration: Click to save the running-config file to the startup-config file.

Messages:

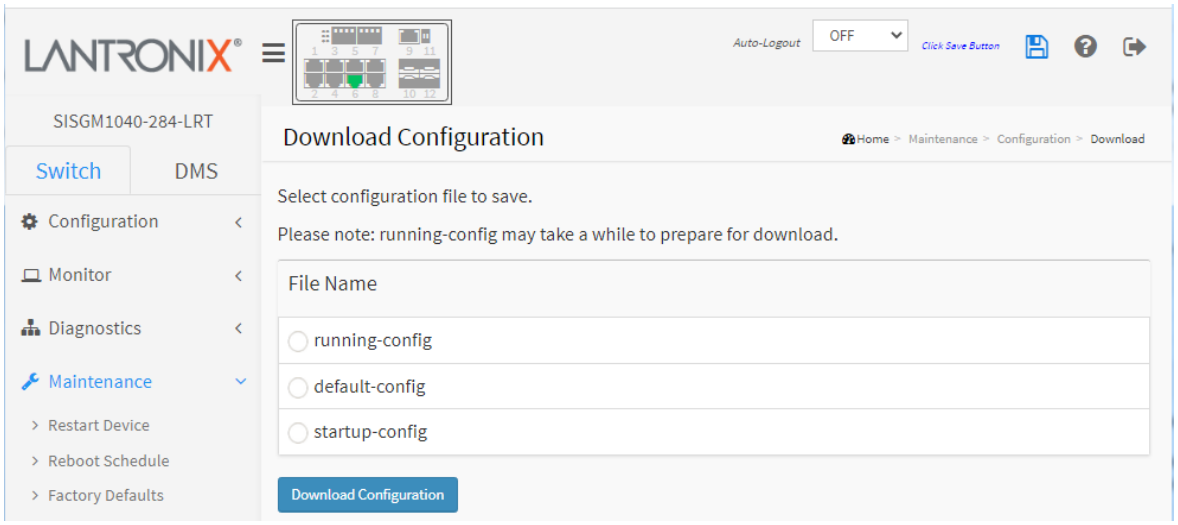
Save Running Configuration to startup-config

startup-config saved successfully.

Maintenance > Configuration > Download

This page lets you save any of the config files on the switch to the web browser.

Download of running-config may take a little while to complete, as the file must be prepared for download.



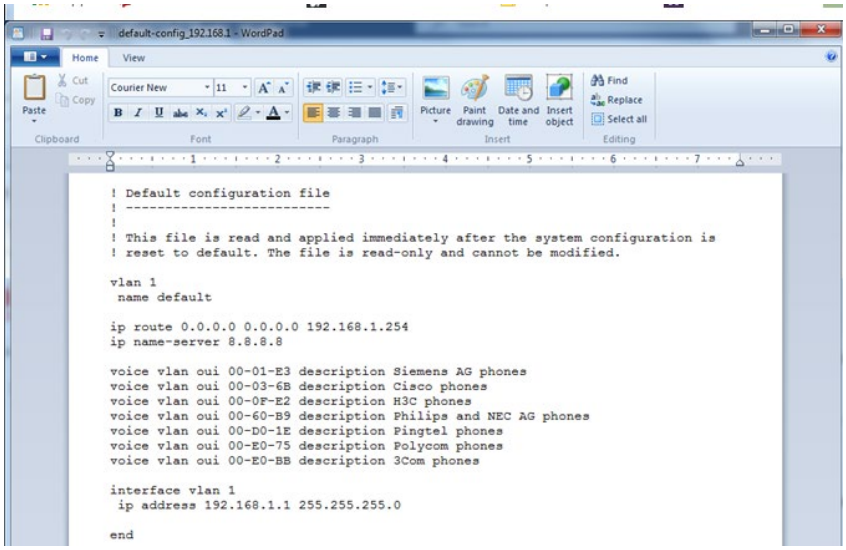
File Name: Select a configuration file to save. Please note: running-config may take a while to prepare for download.

- **running-config**: Save the current configuration that is currently running on the switch.
- **default-config**: Save the factory default configuration that the switch shipped with from the factory.
- **startup-config**: Save the configuration that was last used.

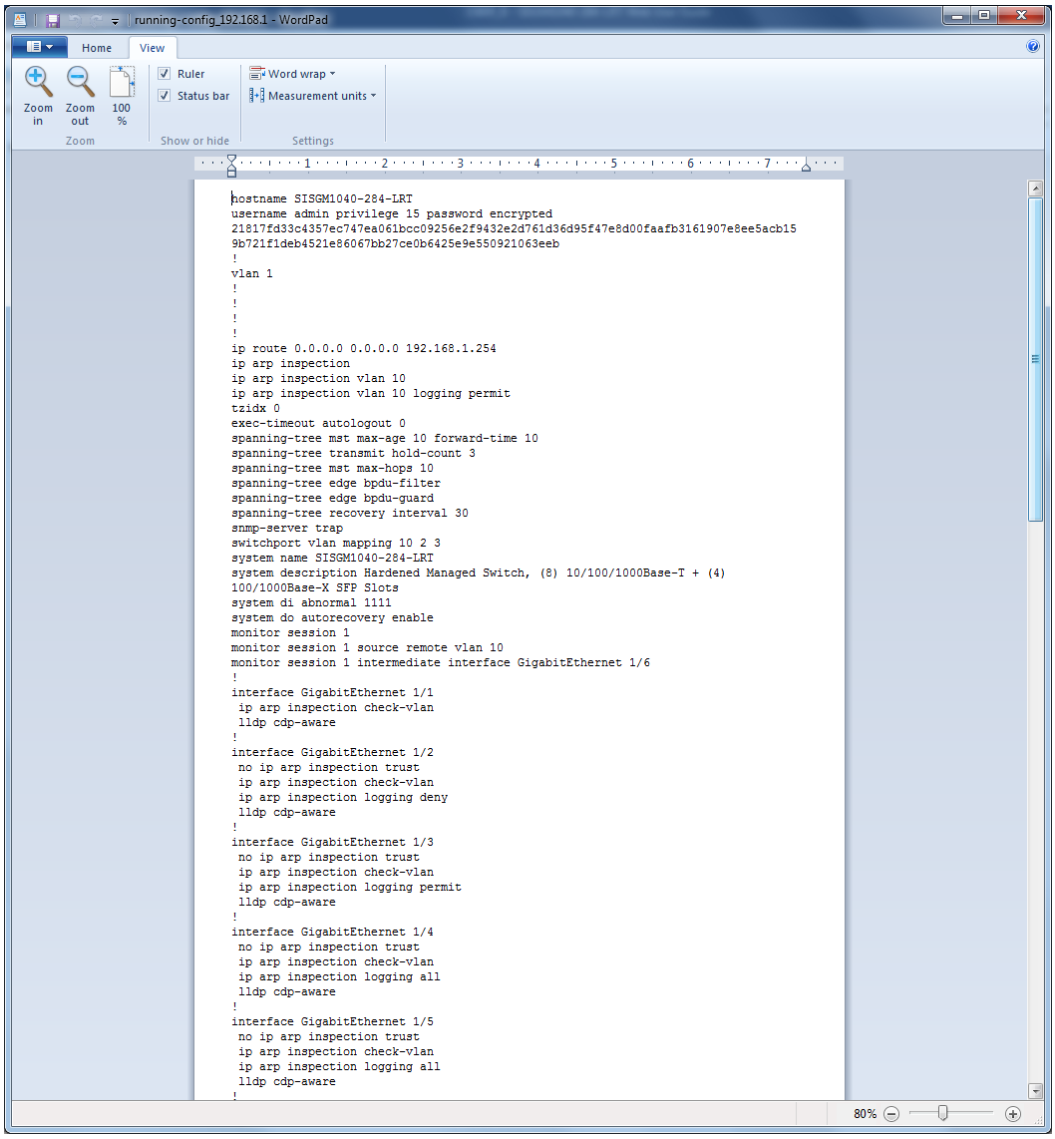
Buttons:

Download Configuration: Click to download the selected file. You can then Open the file or Show its folder location.

Sample Default Config file:



Sample running-config file:



Maintenance > Configuration > Upload

It is possible to upload a file from the web browser to all the files on the switch, except default-config which is read-only.

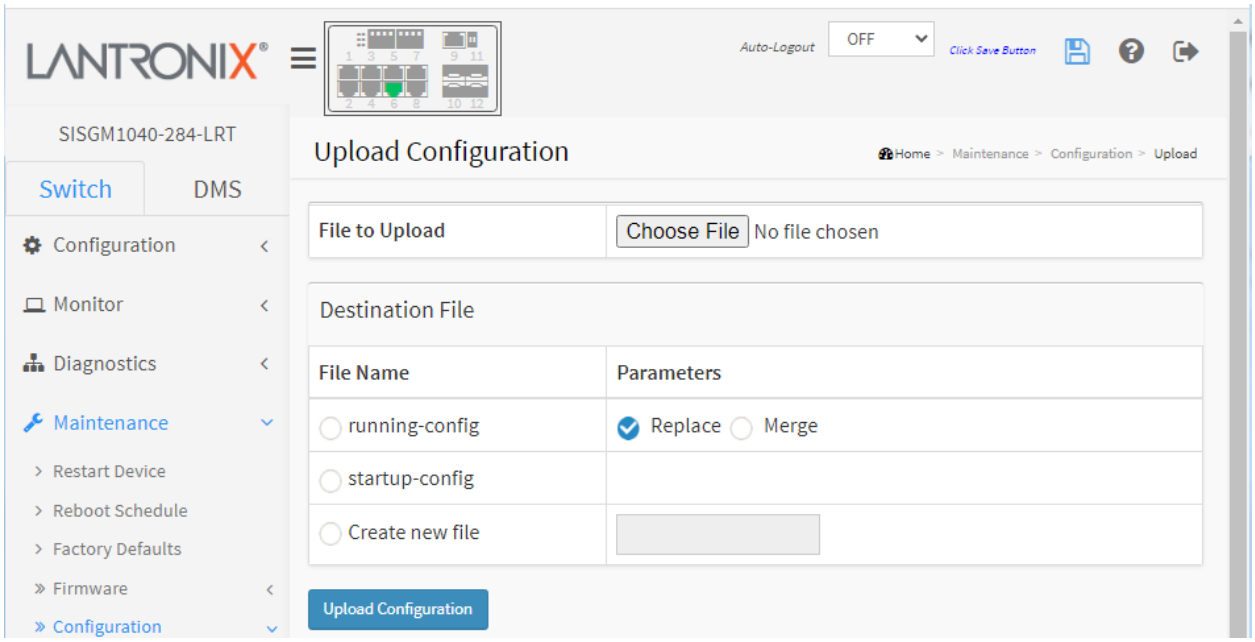
Click the Choose File button and select the file to upload, select the destination file on the target, then click the Upload Configuration button.

If the destination is running-config, the file will be applied to the switch configuration. This can be done in one of two ways:

Replace mode: The current configuration is fully replaced with the configuration in the uploaded file.

Merge mode: The uploaded file is merged into running-config.

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.



Destination File:

File Name: Select a radio button:

- **running-config**: The current configuration that is currently running on the switch.
- **default-config**: The factory default configuration that the switch shipped with from the factory.
- **Create new file**: Radio button to let you enter a enter a new destination filename.

Parameters: For the running-config destination, select Replace or Merge:

Replace mode: The current configuration is fully replaced with the configuration in the uploaded file. This is the default setting.

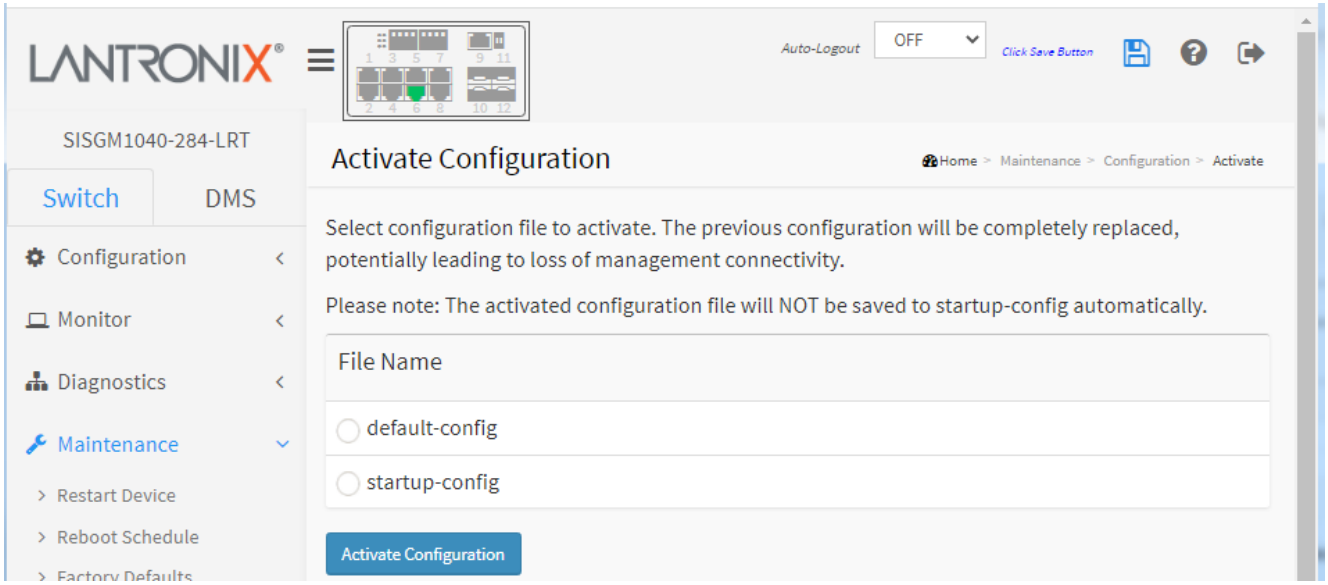
Merge mode: The uploaded file is merged into running-config.

Message: *Upload successfully completed.*

Maintenance > Configuration > 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.

Please note: The activated configuration file will NOT be saved to startup-config automatically.



File Name: Select a configuration file to activate. The previous configuration will be completely replaced, potentially leading to loss of management connectivity.

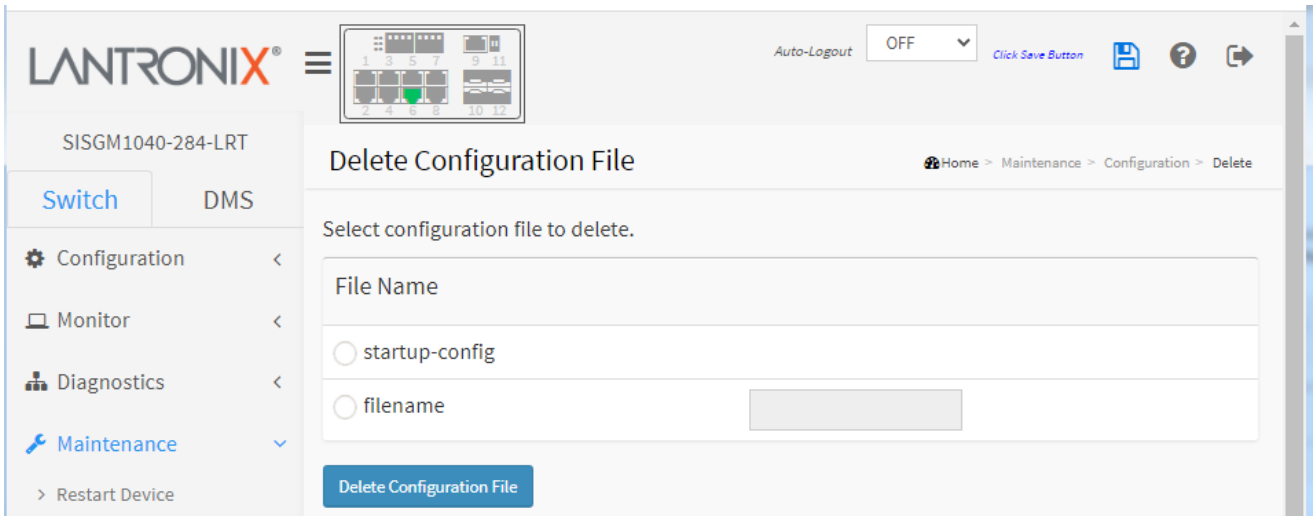
- **default-config**: The factory default configuration that the switch shipped with from the factory.
- **startup-config**: The configuration that was last used.
- **startup-config_192.168.1**: a new destination filename created at Maintenance > Configuration > Upload.

Buttons:

Activate Configuration: Click to initiate the process of completely replacing the existing configuration with that of the selected file.

Maintenance > Configuration > 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 Apply (save) operation, this effectively resets the switch to its default configuration.



File Name: Select the name of the Configuration file to be deleted:

- **startup-config**: Select to delete the startup-config file.
- **filename**: Select and enter the name of the file to delete that was created at Maintenance > Configuration > Upload.

Buttons:

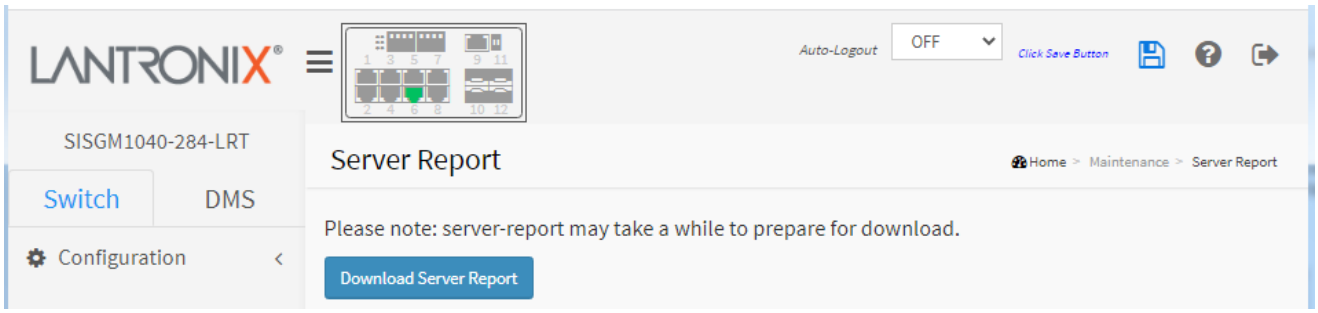
Messages: *Are you sure you want to delete startup-config_192.168.1?*

Click to confirm that you want to delete the selected file.

The message "*Delete Configuration File Successfully deleted.*" displays when successfully completed.

Maintenance > Server Report

It is possible to download server report file on the switch to the web browser. Download of server-report may take a little while to complete, as the file must be prepared for download.



Buttons:

Download Server Report: Click to download a server report file on the switch to the web browser. The report is downloaded and you can Open or Show in file. Server Report sections include System Overview, running-config, System log, System info, Port status, and Port statistics.

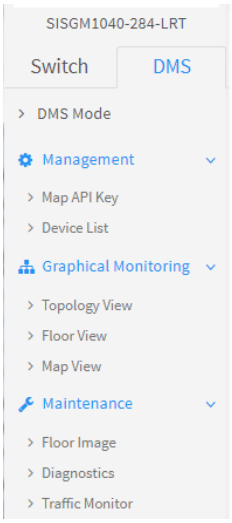
Example: server-report.txt:

server-report (1) - Notepad

File Edit Format View Help

```
----- System Overview -----

Model Name: SISGM1040-284-LRT

Connected Devices: 1

Firmware Version: v7.20.0102 2022-01-05
MAC Address: 00-c0-f2-4a-11-29
System Uptime: 2d 14:22:04

IP Address: 192.168.1.77
Subnet Mask: 255.255.255.0
Gateway: 192.168.1.254
Primary DNS: 8.8.8.8

----- running-config -----

hostname SISGM1040-284-LRTip dhcp excluded-address 192.168.1.30
192.168.1.39evc policer 1 enable eir 4evc policer 2 enable cbs 2evc policer
3 enable type single mode coupled rate-type line cir 1evc policer 4 enable
mode coupledevc policer 5 enable cir 4evc policer 6 enable rate-type lineevc
policer 7 enableevc policer 8 enableevc policer 9 enableevc policer 10
enableevc policer 11 enableevc policer 12 enableevc policer 13 enableevc
policer 14 enableevc policer 15 enableevc policer 16 enableevc policer 17
enableevc policer 18 enableevc policer 19 enableevc policer 20 enable!vlan
1!!ipmc range iName1 233.20.20.80 233.20.20.99!!ip route 0.0.0.0 0.0.0.0
192.168.1.254mvrmvr vlan 10 name MVRCFG1mvr vlan 11 name MVRCFG1234567891mvr
name MVRCFG1234567891 mode compatiblemvr name MVRCFG1234567891 frame
priority 1no mvr name MVRCFG1234567891 frame taggedmvr name MVRCFG1234567891
last-member-query-interval 6ip igmp snooping vlan 10,20ipv6 mld snooping
vlan 10,20ip arp inspection vlan 2ip arp inspection vlan 10ip arp inspection
vlan 20ip arp inspection vlan 2 logging permitip arp inspection vlan 10
logging denyip arp inspection vlan 20 logging allip source binding interface
GigabitEthernet 1/1 10 192.168.1.90 1a-2b-3c-4d-5e-66tzidx 0exec-timeout
autologout 0rapid-ring entry 1 role master port1 GigabitEthernet 1/2 port2
GigabitEthernet 1/3rapid-ring entry 2 role member port1 GigabitEthernet 1/4
port2 GigabitEthernet 1/5ring-to-ring role backup port GigabitEthernet 1/7
radius-server attribute 4 192.168.1.3radius-server attribute 32 admin
radius-server host RadSrvr1 timeout 60 retransmit 350 key encrypted
52e182b84d44b1fd8221681a043bd1f5b7dec5b26295110dc0d38a16e8db61f7e3c9f9fe3999
ce76807bad28cb99f9a12bf00d1a3a384e83fc5b8ae82672b59dradius-server host
Radrvr2 auth-port 1645 acct-port 1646 timeout 45 retransmit 222 key
encrypted
005233c78c2c0a8974dc66c513005849fceeea018b0d7eb2bb61b9644438df4e87f345bdd55c
cfd54037733c2884d3fea52b1c4e3d574a33f369bf57f4f9864cradius-server host
radius3 acct-port 1646 timeout 1 retransmit 99 key encrypted
bcb10efe1d96439cd3fe8b8f656b79de1f773f825f3419eaec0041a5d3f705f9ed8a290428e2
ebcaf37d9249188904c45b4916a0fbeceb112d057f7148a56795tacacs-server host
TacSrvr1 timeout 60 key encrypted
eb63bfb914ccf06f45282d7842e79a95d22737986fd10c293f31cde4f2bdb205e79ef675882f
81354855abdcf43c35c89b21d0c4f5b15eb6bf95bd8b24ce3588tacacs-server host
TacSrvr2 timeout 45 key encrypted
8c0f86c965557dcac68a1ba228d6d8f9d9b52a218bd73056a94be8b7baf5d62fe20fa1a5192d
712469ba5a0f808cbb37a5ef7b5cf73fbee8682a38733bf68ef3voice vlanptp 0 mode
boundary onestep ethernet twoway id 00:c0:f2:ff:fe:4a:11:29 vid 1 0 mep 1ptp
0 time-property utc-offset 0 ptptimescale time-source 160ptp 1 mode
p2ptransparent onestep ethernet twoway id 00:c0:f2:ff:fe:4a:11:2a vid 1 0
profile ieee1588 mep 1ptp 1 time-property utc-offset 0 ptptimescale time-
```

5. DMS (Device Management System)



Lantronix Device Management System (DMS) capability built into the switch provides time-saving features enabling security integrators or network administrators to establish and document a baseline deployment, and automatically discover and remotely configure attached IP-powered devices (PDs). DMS can automatically discover all IP devices and display the devices in a graphic networking topology view.

DMS Functions

DMS Mode: Lets you enable or disable DMS operation and set Controller Priority.

Management: Provides Map API Key and Device List.

Graphical Monitoring: Provides Topology View, Floor View, and Map View.

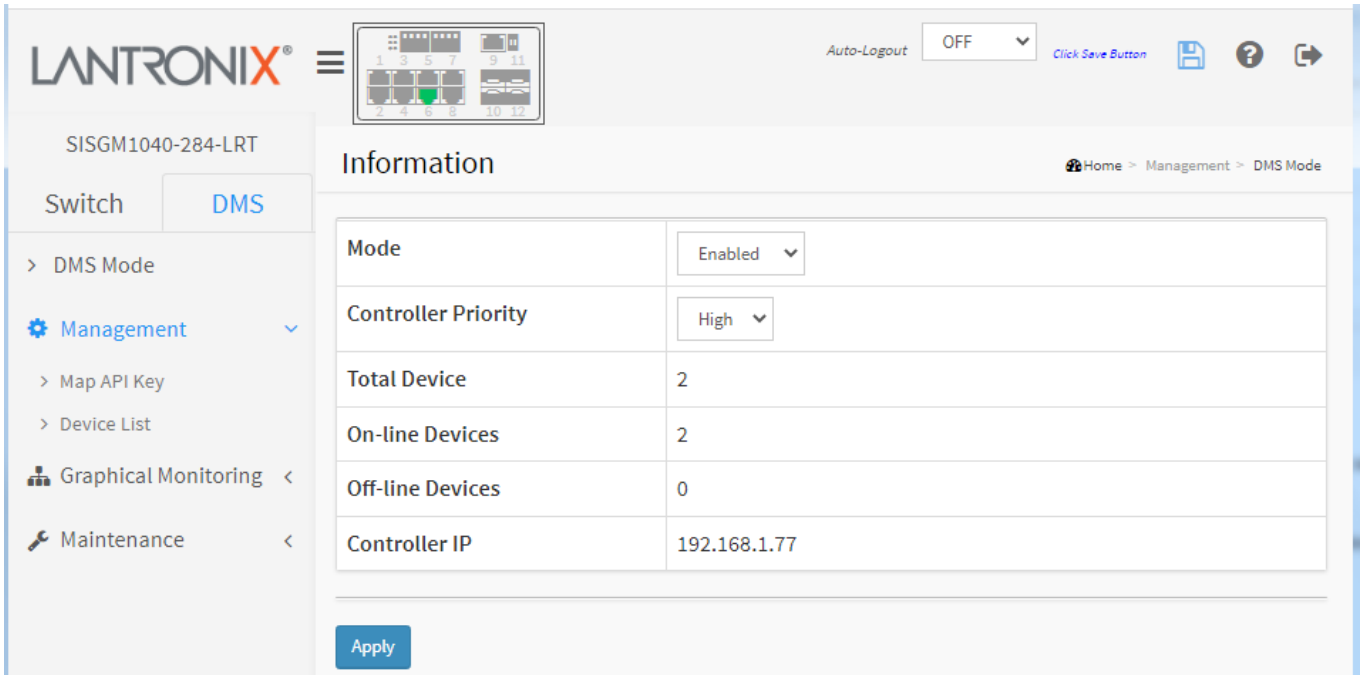
Maintenance: Provides Floor Image, Diagnostics, and Traffic Monitor.

DMS Advanced Features

- Automatically discover and remotely configure attached IP addressable powered devices (PD)
- Establish and document a baseline deployment
- Graphical topology view for device management
- Floor view for device management (import JPEG design drawings)
- Google Maps™ view for device management
- Auto Power Reset (APR) monitors and automatically restarts edge devices
- Troubleshoot cable and IP connection issues
- Monitor and analyze traffic by Day/Week/Port/Device
- Perform health checks with thresholds
- Auto-Alarm on error conditions

DMS > Management > DMS Mode

This page lets you enable or disable the DMS function, set Controller Priority, and view device information.



Mode: Enable/Disable the DMS function. The default is Enabled.

Controller Priority: Set the "Controller Priority" when enabling DMS:

High: This switch will be the Controller (Master) switch. This setting is required for Traffic Monitoring.

Mid: Sets the switch DMS to middle level priority.

Low: Sets the switch DMS to low level priority.

Non: This switch will never become the Controller (Master) switch. This is the default setting.

Total Device: Shows how many IP devices are detected and displayed in the Topology view.

On-Line Devices: Shows how many IP devices on-line in the Topology view.

Off-Line Devices: Shows how many IP devices off-line in the Topology view.

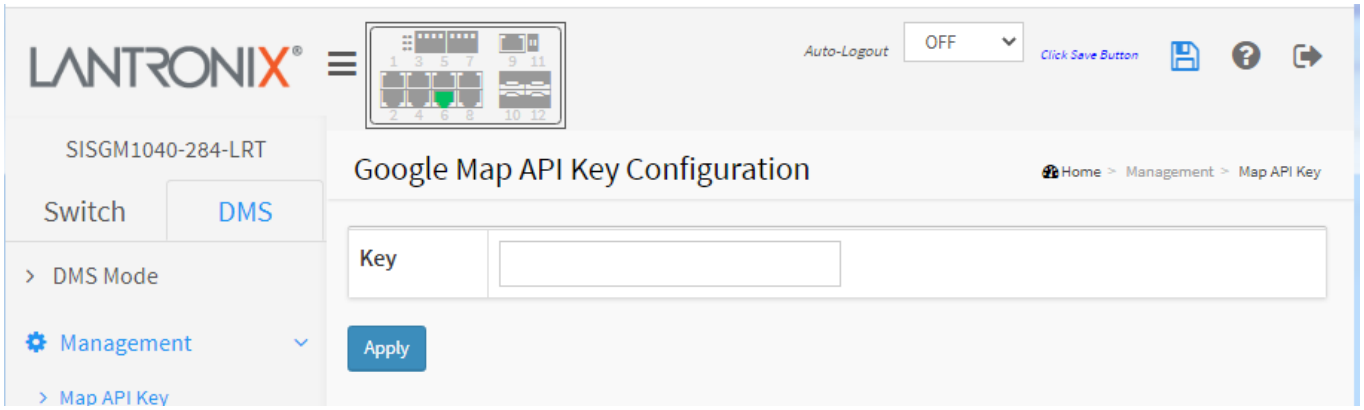
Controller IP: Show the IP address of the Controller (Master) switch.

Buttons

Apply: Click to save changes.

DMS > Management > Map API Key

You need a valid API key and a Google Cloud Platform billing account to access Google core product. If not, DMS Map View will not be able to load Google Maps correctly. Please visit the Google website below and follow the directions to get an API key: https://developers.google.com/maps/documentation/directions/get-api-key.



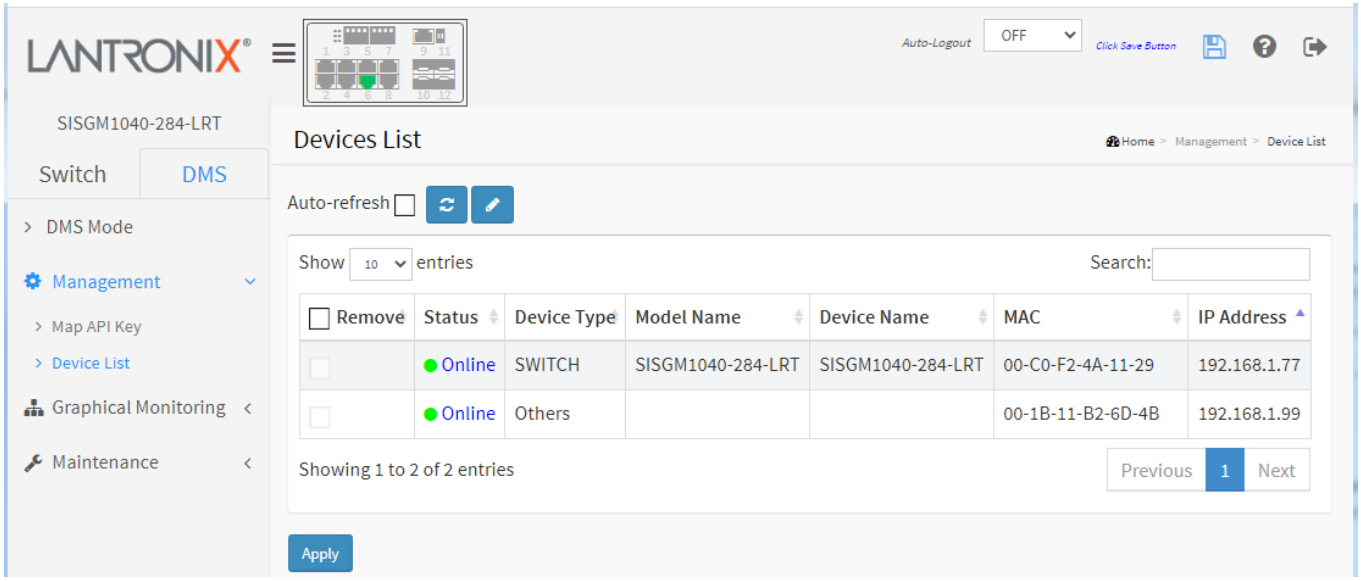
Key: Enter the downloaded Google Maps API Key.

Buttons

Apply: Click to save changes.

DMS > Management > Device List

This page provides an overview of the device list.



Remove: Remove off-line device from the list.

Status: Device Online or Offline. Click the linked Online text to run a diagnostic on the device (see below).

Device Type: The type of the network connectivity devices such as PC, SWITCH, AP, IP Cam, IP Phone or Others.

Model Name: The model name of the network connectivity devices.

Device Name: The device name of the network connectivity devices.

MAC: The mac address of the device.

IP Address: The IP address of the network connectivity devices.

Buttons

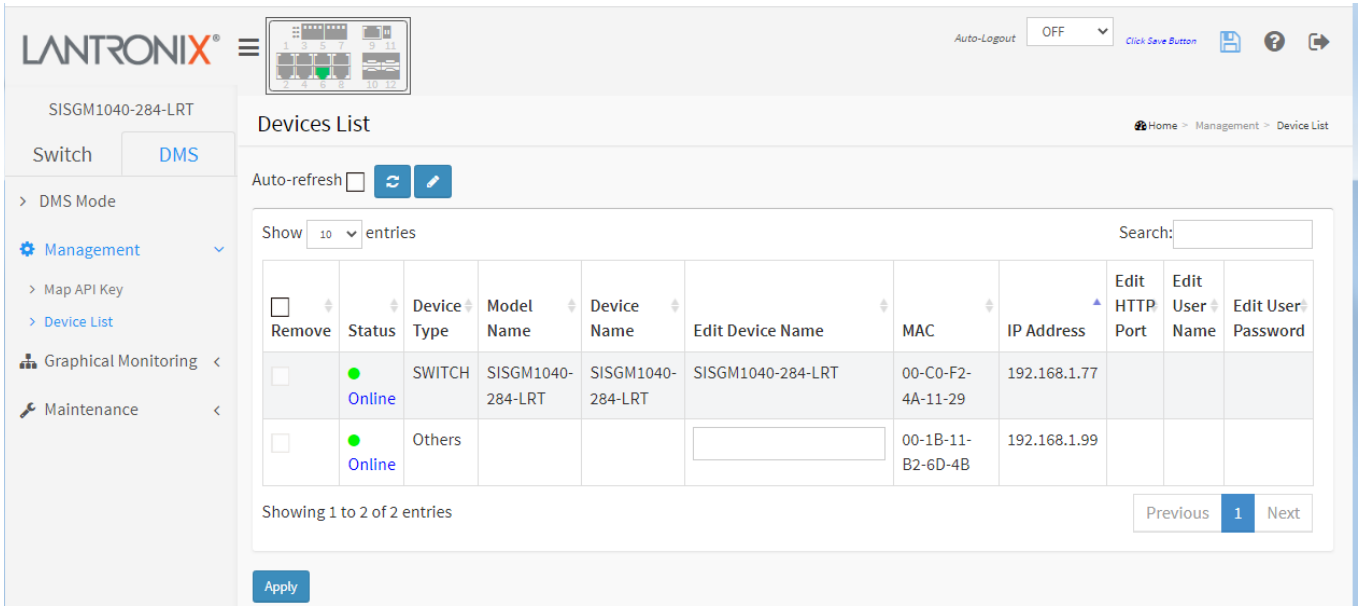
Auto-refresh: Check this box to refresh the page automatically every 3 seconds.

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

 **Edit**: Add the input fields for editing additional fields (see below).

Apply: Click to save changes.

Click the Edit ( ) button to display four additional input fields for editing.



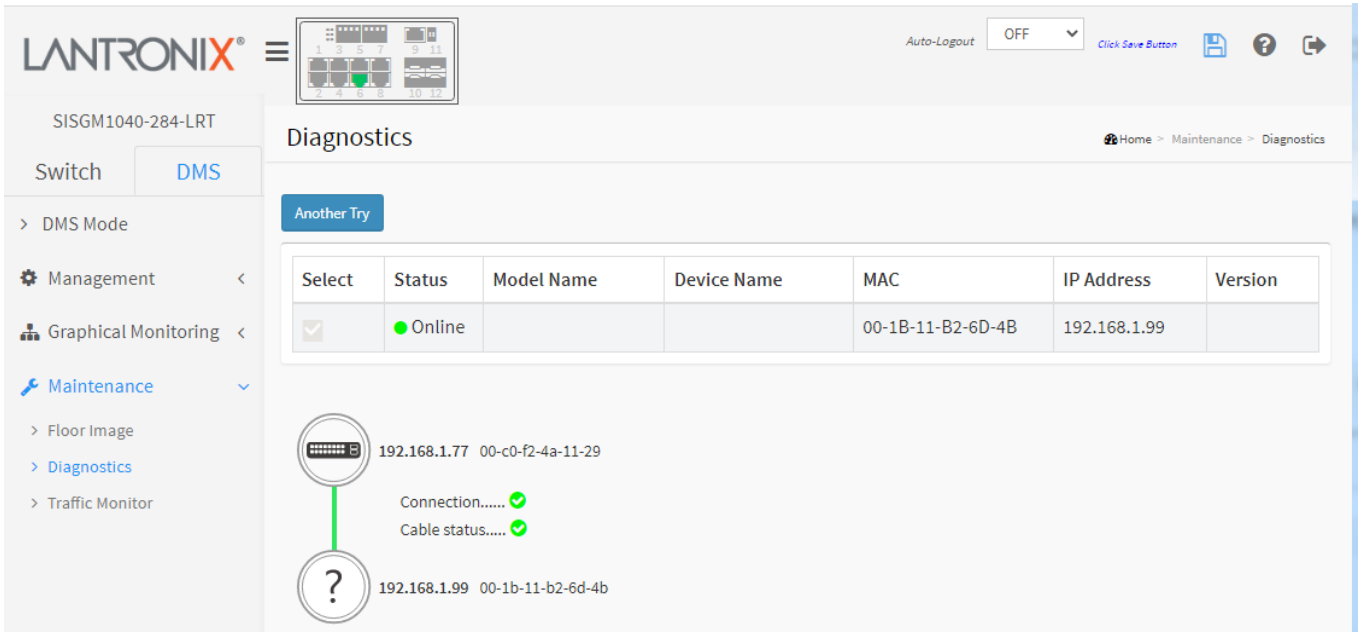
Edit Device Name: Edit the type of network connectivity device (e.g., PC, SWITCH, AP, SISGM1040-284-LRT).

Edit HTTP Port: Change the HTTP port number.

Edit User Name: Edit the User's name.

Edit User Password: Edit the user's password.

Click the linked Online text to run a diagnostic on the device from DMS > Maintenance > Diagnostics:



Another Try: Click the button to run diagnostics again.

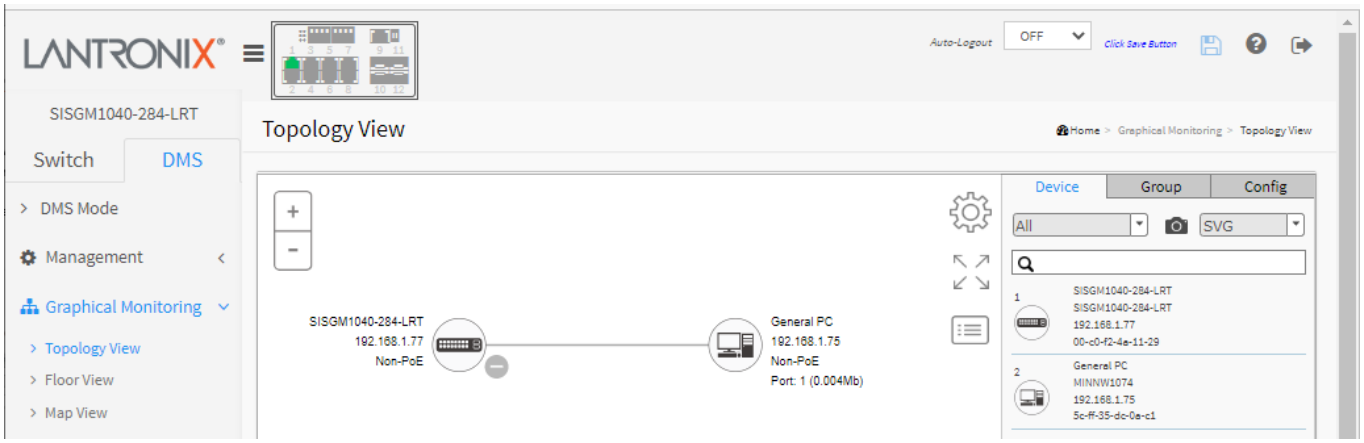
DMS > Graphical Monitoring > Topology View

DMS can automatically discover all IP devices and display the devices by graphic networking topology view.

You can manage and monitor devices in Topology View, such as to remotely diagnose the cable connection status, auto alarm notifications on critical events, and remotely reboot PoE device when it's not alive.

You can apply the DMS platform to solve abnormal issues anytime and anywhere by tablet or smart phone, and keep the network works smoothly.

Click Graphical Monitoring -> Topology View to view the network topology:



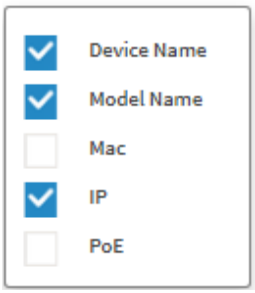
Parameter descriptions:

: Icon with plus and minus marks; zoom in and zoom out Topology view or scroll up/down with mouse to achieve the same purpose.

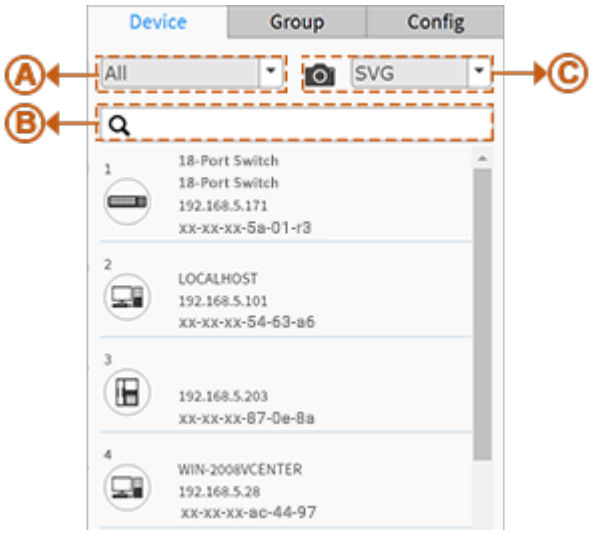
:There is a "Setting icon" in the upper right corner. Click the icon to pop-up Device, Group, Config, export topology view and advanced search functions for the topology.

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: User can select what kind of information should be shown on the topology view of each device. Up to 3 items can be selected at a time. The options are Device Name, Model Name, Mac, IP, and PoE.

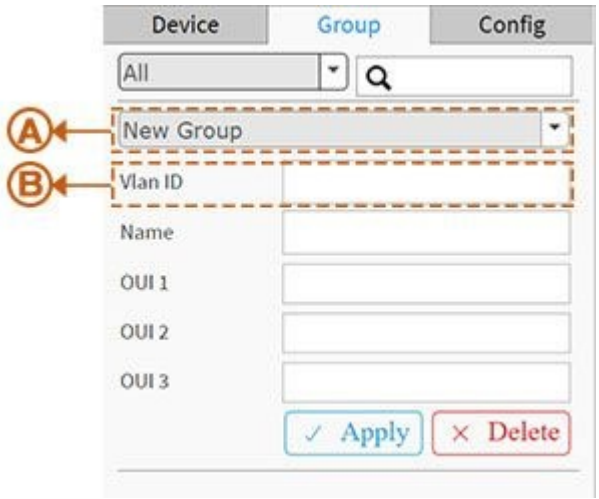


1. Device Search Console



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

2. Group Setting Console



- Using MAC Based VLAN to isolate groups.
- One IP device only can join one VLAN group.

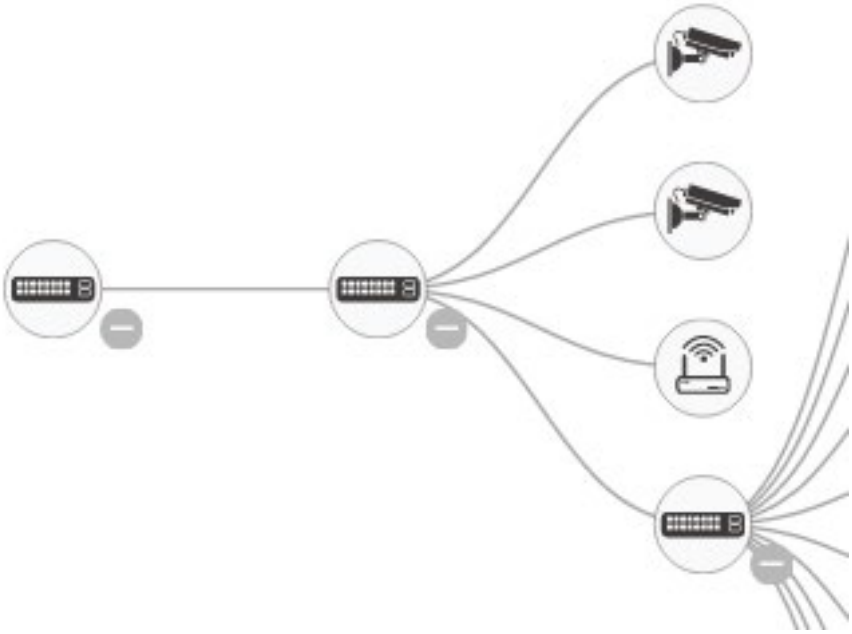
Function	
A.	Group devices by filtering, searching, clicking device icons, or specifying OUI.
B.	Assign VLAN ID or Name to Group.

3. System Setting Console

Function

A.	Shows how many IP devices are detected and displayed in the topology view.
B.	Show 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.)

Device Tree View



Device category


Means the device is a Switch.


Means the device is a PC.


Means the device is an IP Cam.


Means the device is an IP Phone.


Means the device is an AP.


Means the device is a Router.


Icon with question: It means the IP device is detected by DMS, but the device type can't be recognized; it will be classified as an “unknown” device type.

Device Status

- Icon with black mark: Device link up. You can select function and check issues.
- Icon with red mark: Device link down. You can diagnose the link status.
- Icon with numbers: Means some event has happened (e.g. Device Off-line, IP Duplicate, etc.) on the IP device; you can click on the device icon to check events in Notification.

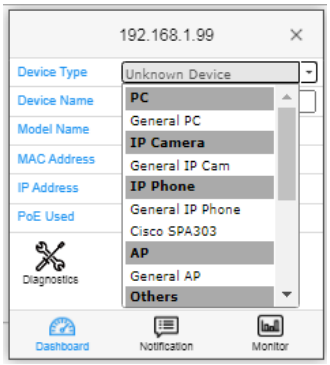
Device consoles

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: It can be displayed automatically. If an unknown type is detected, you can select a type from the dropdown: **PC** (General PC), **IP Camera** (General IP Cam), **IP Phone** (General IP Phone, Cisco SPA303), **AP** (General AP), **Others** (Mobile Device, General Switch, General Gateway, IP PBX, NAS, Printer, NVR, VMS, Unknown Device).

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.
Device Type (e.g., SWITCH), Device Name (e.g., SISGM1040-284-LRT), Model Name (e.g., SISGM1040-284-LRT), MAC Address (e.g., 00-c0-f2-4a-11-29), DHCP Client Enable/Disable), IPv4 Address, Subnet Mask,Gateway, HTTP port, and PoE Supply (i.e., Non-PoE).

HTTP Port: Re-assign HTTP port number to the device for better security.

Icons:

Login: Click the Login Action 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 switch LED will all lighten up and flicker for 15 seconds.

Diagnostics: Click Diagnostic Action Icon to perform the cable diagnostics, to exam where the broken cable is, and, check if the device connection is alive or not by ping.

Cable Status:

Green icon: Cable is connected correctly.

Red icon: Cable is not connected correctly. User can check the distance info (XX meters) to identify the broken cable location.

Connection:

Green icon: Device is pinged correctly.

Red icon: Device is not transmitted /receiving data correctly. Which means it might not be pinged successfully.

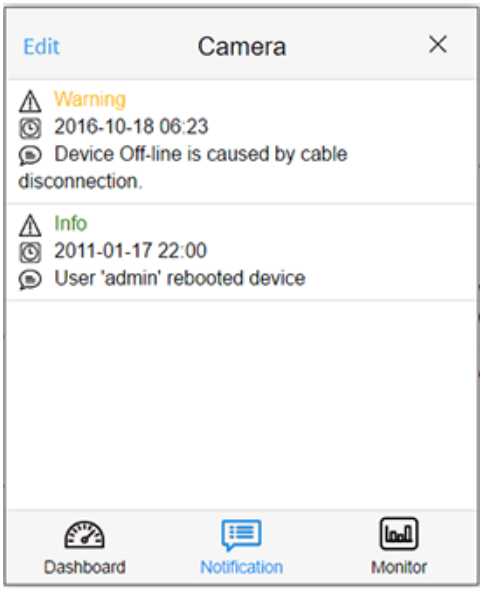
Reboot: Click Reboot Action Icon to reboot the device remotely so as recover the device back to its normal operation.

Streaming: Click Streaming Action Icon 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, switch can't resolve this IP device's layout, instead, it will show a blank node to present this situation. User can use "Parent Node" function to adjust layout in Dashboard.

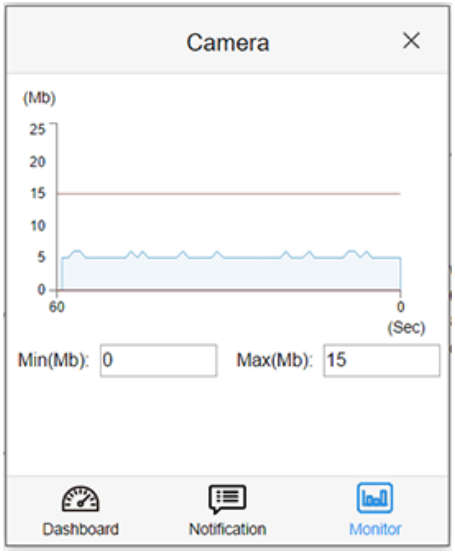
PoE Config: Click it to configure the PoE function, enable/disable PoE Auto Checking and enable/disable PoE mode for per port.

Notification Console: displays alarms and logs triggered by events.



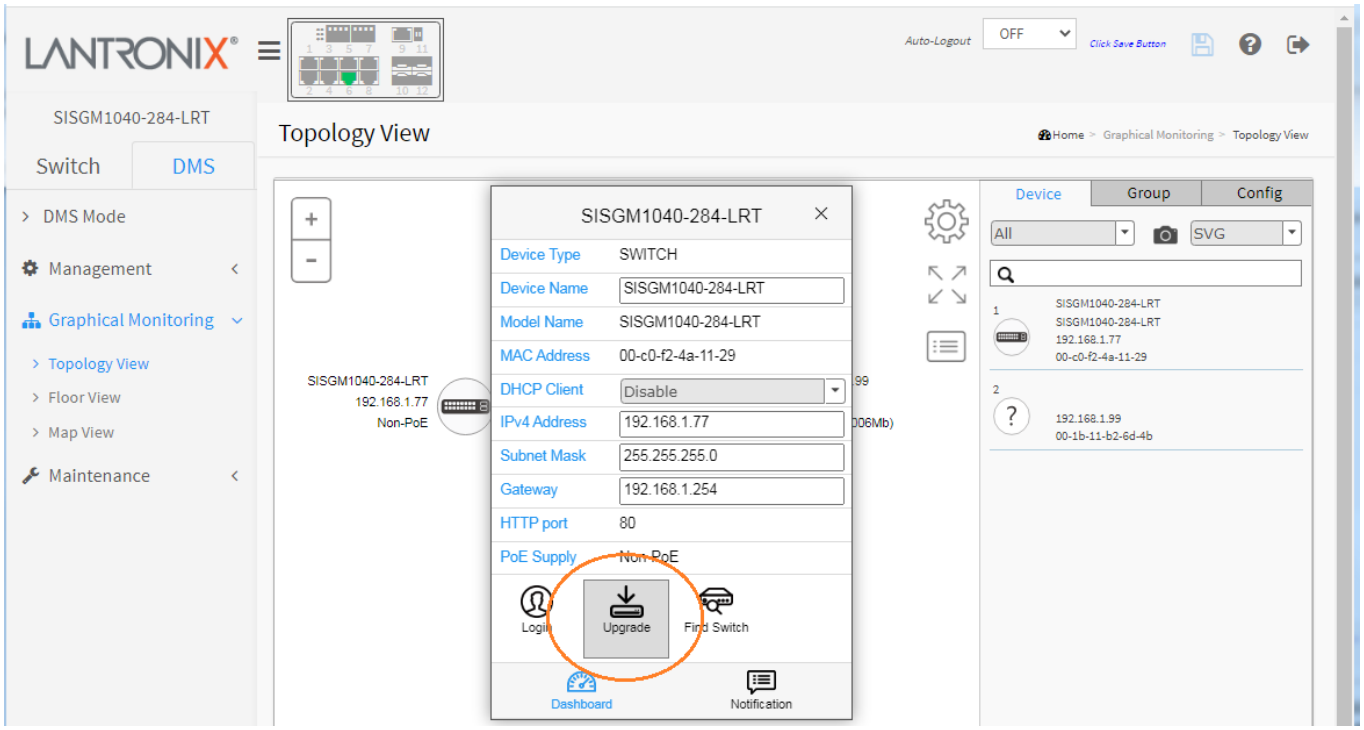
Monitor Console: displays the traffics for device health check purpose.

- For each IP device except DMS switches, User can 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.

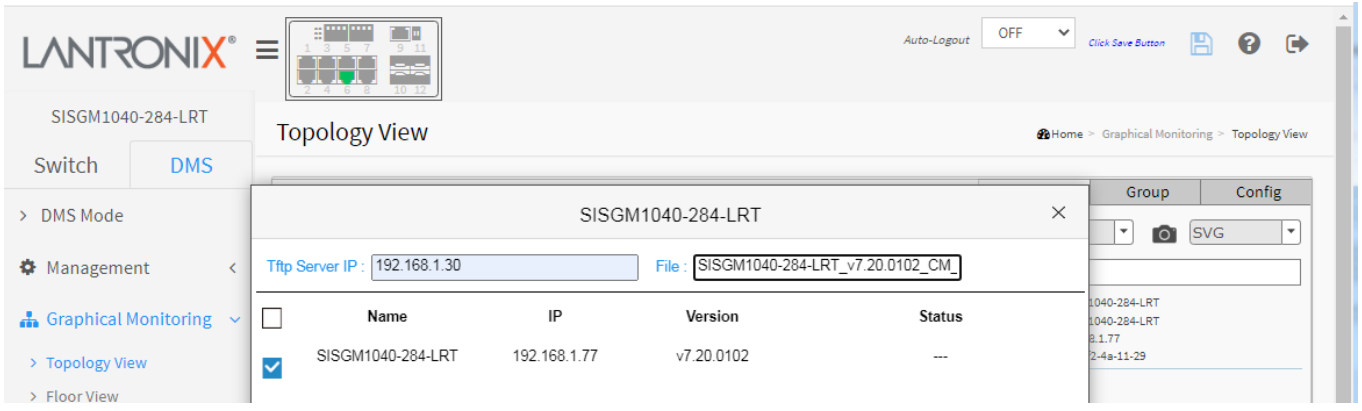


Upgrade Firmware from Topology View

1. Navigate to DMS > Graphical Monitoring > Topology View.
2. Left mouse click the switch icon to display its options:

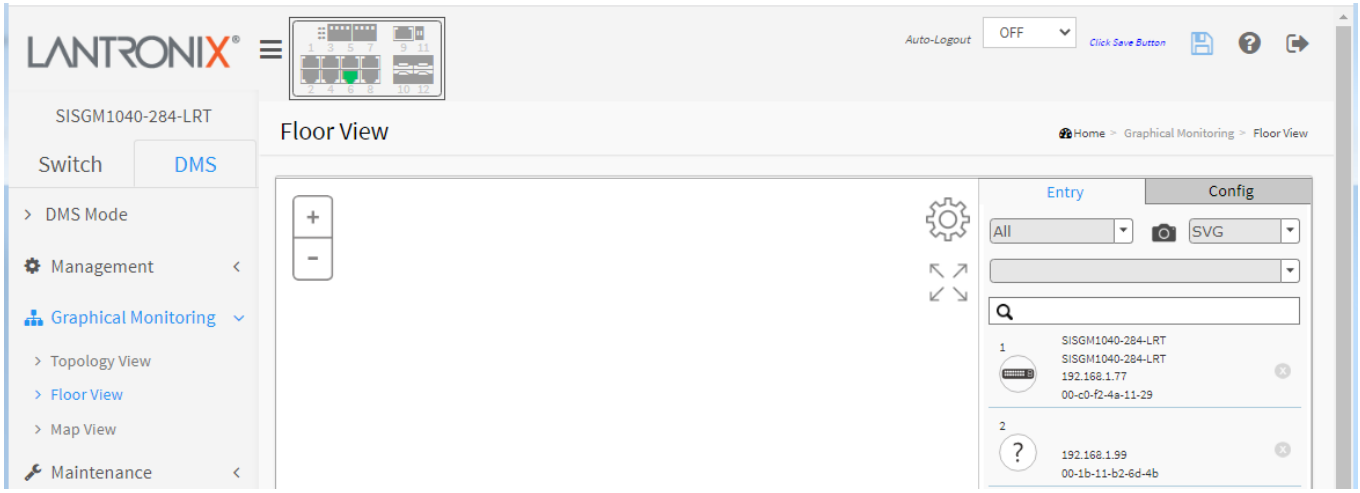


3. Click the Upgrade icon.
4. Enter the Tftp Server IP (e.g., 192.168.1.300).
5. Enter the File name (e.g., SISGM1040-284-LRT_v7.20.0063_CM_201905009).
6. Check an instance checkbox and click the Apply button.

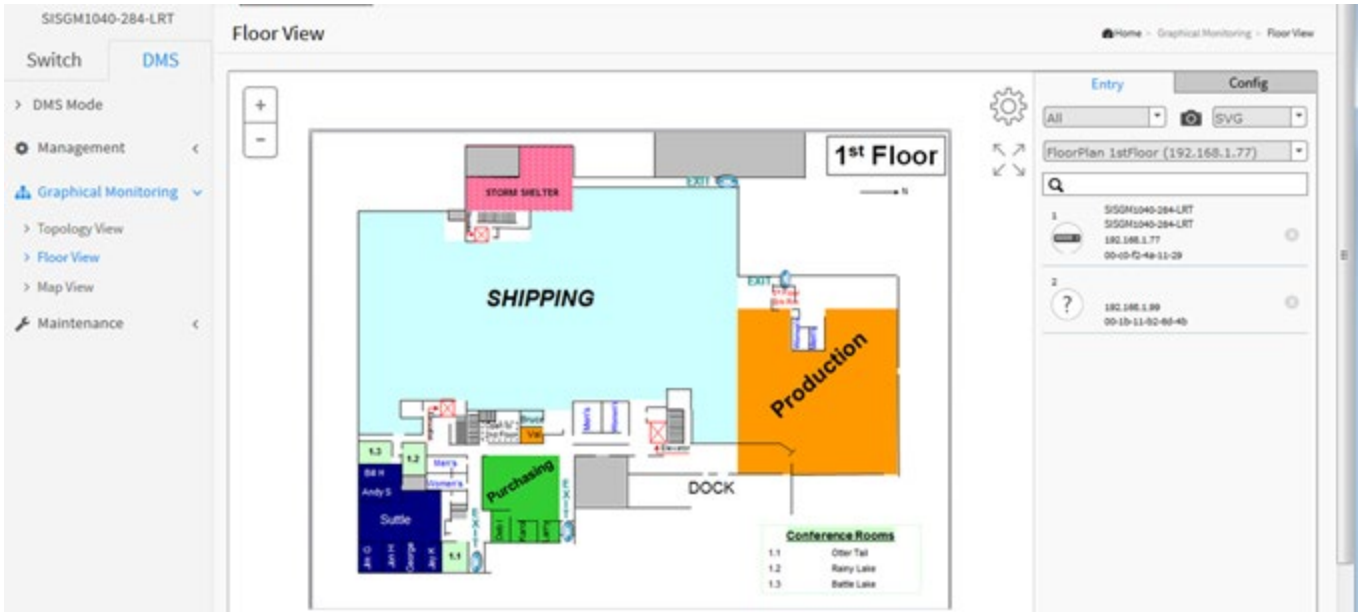


DMS > Graphical Monitoring > Floor View

This page lets you plan IP devices installation locations onto the custom uploaded floor images.



You must first add one or more floor images from DMS > Maintenance > Floor Image.

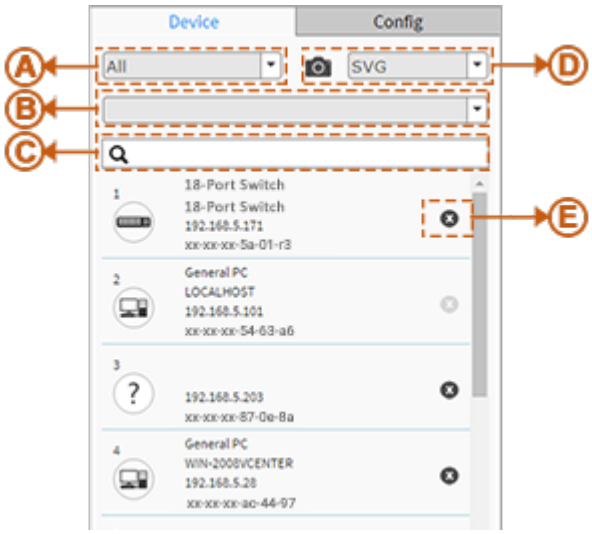


Parameter descriptions:

Icon with plus and minus marks: Zoom in and zoom out the floor view, user can scroll up/down with mouse to achieve the same purpose.

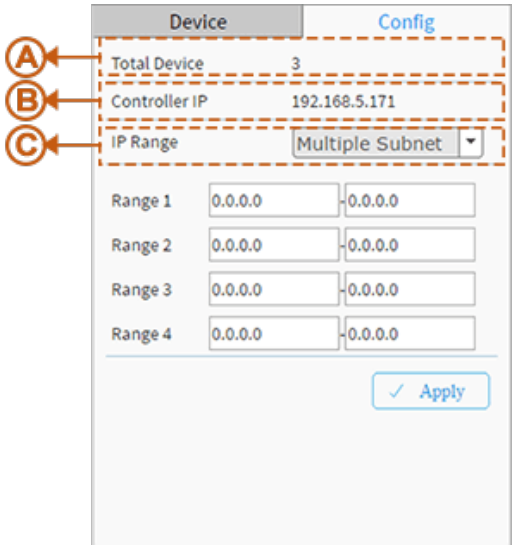
In the upper right corner, there is a "Setting icon". When you click the icon, it will pop-up Device, Config, export floor view and advanced search functions for the device.

1. 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

2. System Setting Console



Function
A. Shows how many IP devices are detected and displayed in Topology view.
B. Shows the Master IP.

C.
Single Subnet: DMS will base on the master switch's IP address. Here the subnet means "255.255.255.0"

Multiple Subnet: To provide 4 ranges for inputting manually. In the case, we suggest 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 Normal View.

Floor View

- Anchor Devices onto Floor Maps
- Find Device Location Instantly
- 10 Maps can be Stored in Each Switch
- IP Surveillance/VoIP/WiFi Applications
- Other features same as Topology View
- To place and remove a device icon:
  i. Select a device and click its icon from the device list.
  ii. The device icon will show on the floor image's default location.
  iii. Click and hold left mouse by dragging-and-dropping the icon to the correct location on the floor view.
  iv. Click 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 function and check issues.

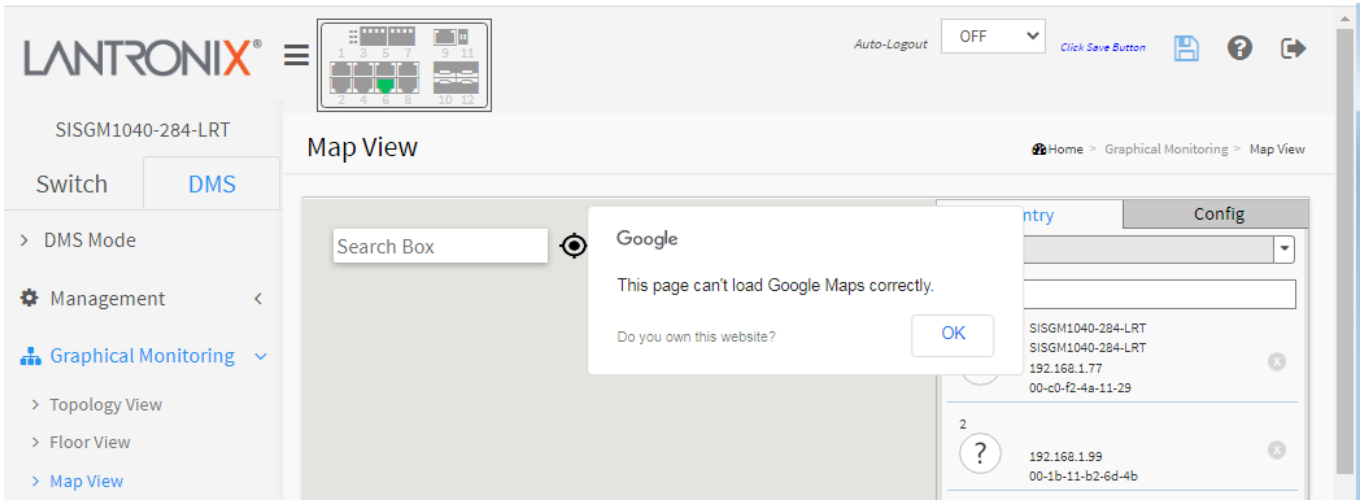

Icon with red mark: Device link down. You can diagnose the link status.

Icon with a question mark; Unknown device type.

DMS > Graphical Monitoring > Map View

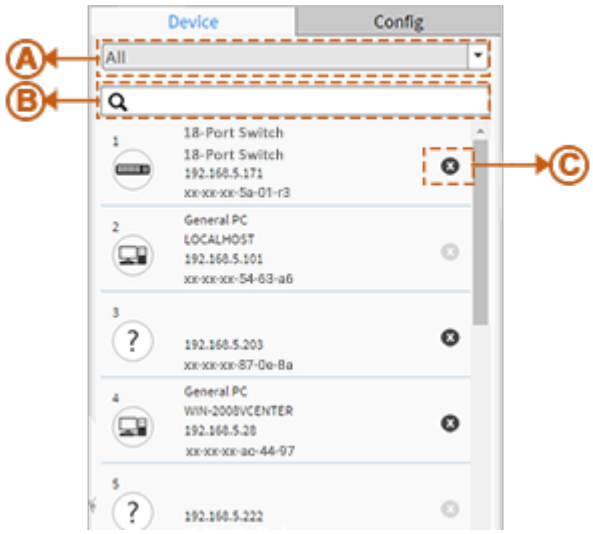
This page helps to find the location of the devices even they are installed in different building. You can place device icons on the Map View of which navigated by Google Maps.

If the message "*This page can't load Google Maps correctly.*" displays, click the OK button to clear the message and see DMS > Management > Map API Key on page 391.



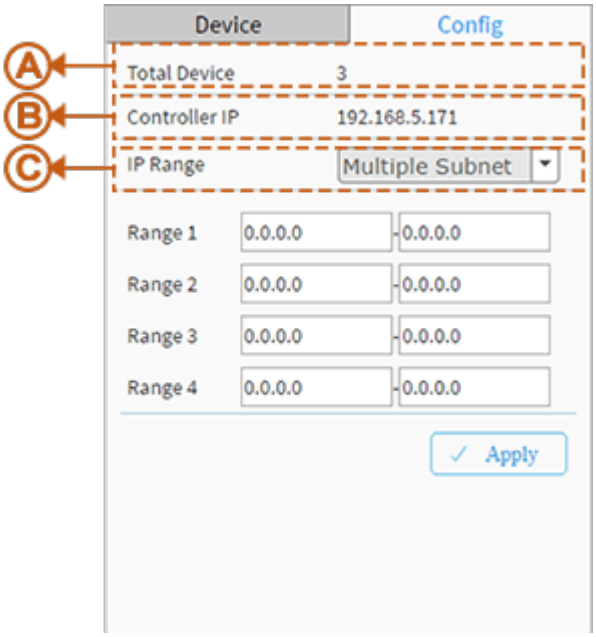
In the upper right corner, there is a "Setting icon". When you click the icon, it will pop-up Device, Config, and advanced search functions for the device.

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

2. 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 Map or return to the Normal View.

Map View

- Anchor Devices onto Google Map.
- Find Devices Instantly from Map.
- On-Line Search Company/Address.
- Outdoor IP Cam/WiFi Applications.
- Other Feature same as Topology View
- To place and remove a device icon
  - To 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 and drag-and-drop the icon to the correct location on the Map view.
  - Click the cross sign on the right side of a device icon to remove the device from Map view.

Device Status

Icon with black mark: Device link up. You can select function and check issues.

Icon with red mark: Device link down. You can diagnose the link status.

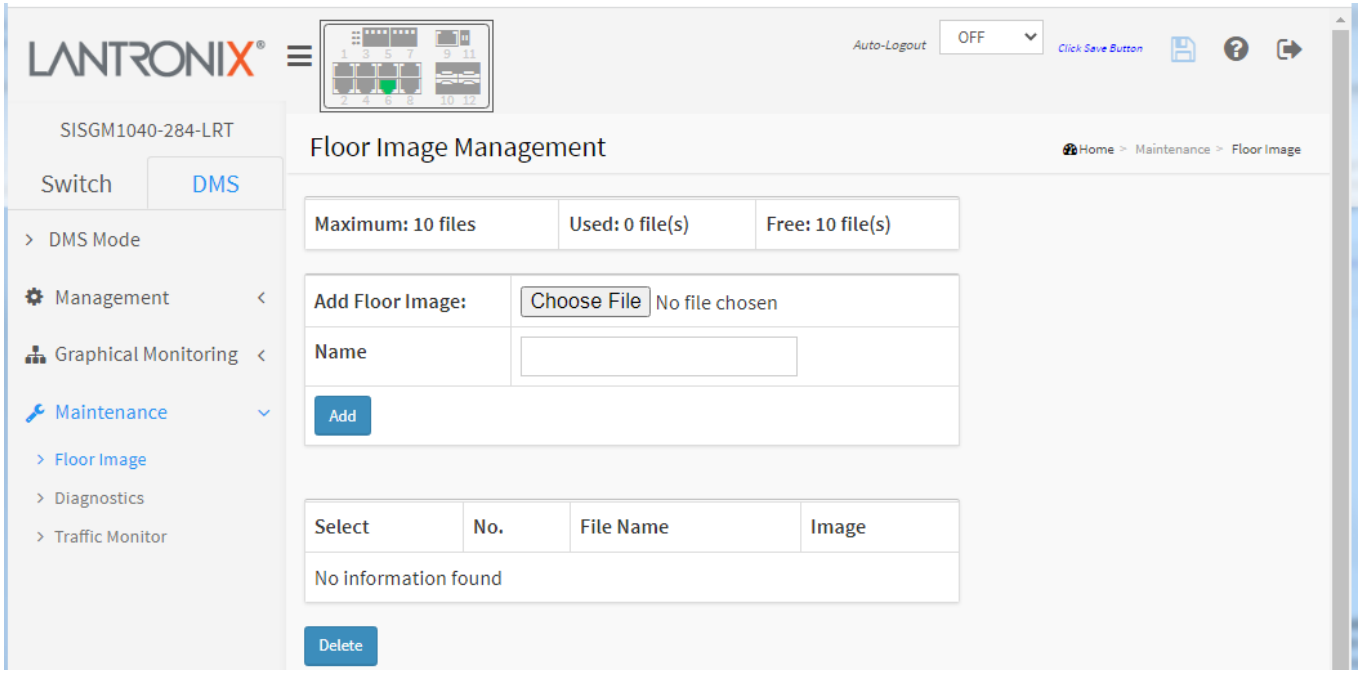
Icon with a question mark; Unknown device type.

Message:
This page can't load Google Maps correctly.
Do you own this website?

Click the OK button to clear the message, or click “Do you own this website?” to go to the Google Developers webpage.

DMS > Maintenance > Floor Image

Navigate to the DMS > Maintenance > Floor Image menu path to display the Floor Image Management page. This page lets you upload and manage floor map images. You can then plan IP devices' installation location onto the custom uploaded floor images at DMS > Graphical Monitoring > Floor View. Up to 10 floor images, each of a max. of 524152B size, can be uploaded to the switch.



Parameter Descriptions:

Maximum: *x* files: By default this field displays "Maximum: 10 files". With each switch added and discovered, the maximum value increases by 10. For example, if only two switches are connected to each other, the maximum number of files will increase from 10 to 20 (on both switches). But once the connection is removed and after an approximate 1 minute wait, the maximum number of files will restore to 10. The maximum number of images displayed is additive. When the switch is stand alone with no connections to other DMS switches, the number displayed is 10. As other DMS switches are added, the field is incremented by 10 for each one.

Used: x file(s): The number of files that have already been uploaded.

Free: *x* file(s): The number of files that can be uploaded before reaching the maximum number of images.

Name: Displays the chosen filename.

Buttons

Choose File: Click to browse to and select a Floor Image file.

Add: Click Add to upload. When done, a snapshot will be available on screen.

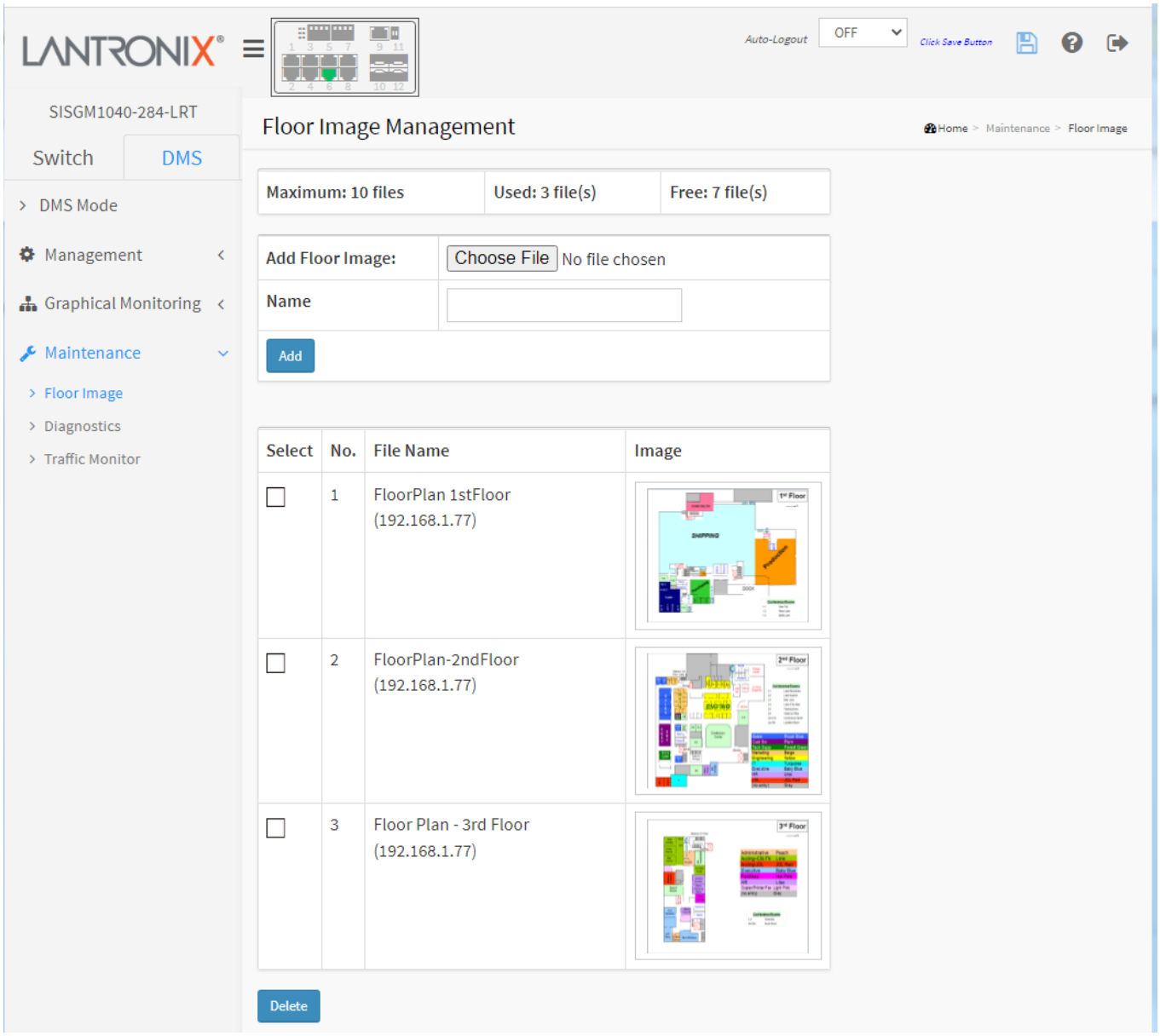
Delete: To remove an existing Floor Map image, select its checkbox and click Delete to remove.

Messages:

Only jpg, png are allowed Click the OK button and select a different file.

Add file fail, file name already exist! Click the Previous button and continue operation.

Example: Floor Image Management page with three images:



Select: Check the checkbox to select an image from the list.

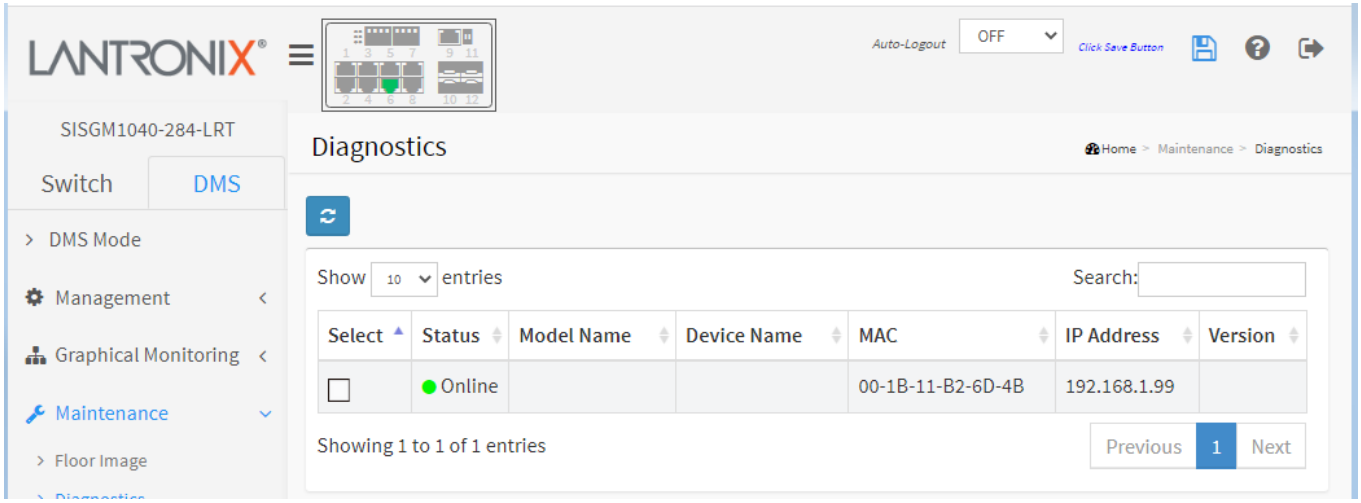
No.: The image number

File Name: Displays the selected Floor Image file name.

Image: Displays the added image(s).

DMS > Maintenance > Diagnostics

This page lets you run Diagnostic and provides Connection and Cable status.



Select: Check a checkbox of an on-line device to run a diagnostic on.

Status: Displays device Status; either Online or Offline.

Model Name: The model name of the network connectivity device.

Device Name: The device name of the network connectivity device.

MAC: The MAC address of the device.

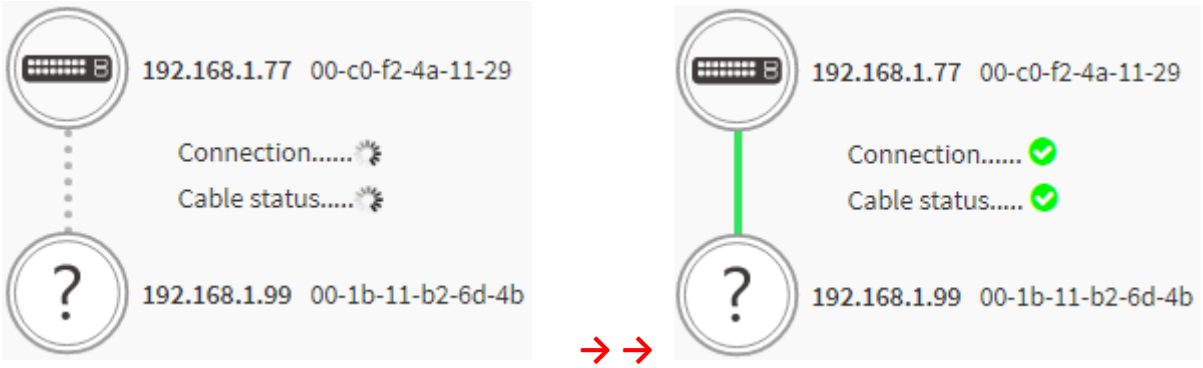
IP Address: The IP address of the network connectivity device.

Version: The Version of the network connectivity device.

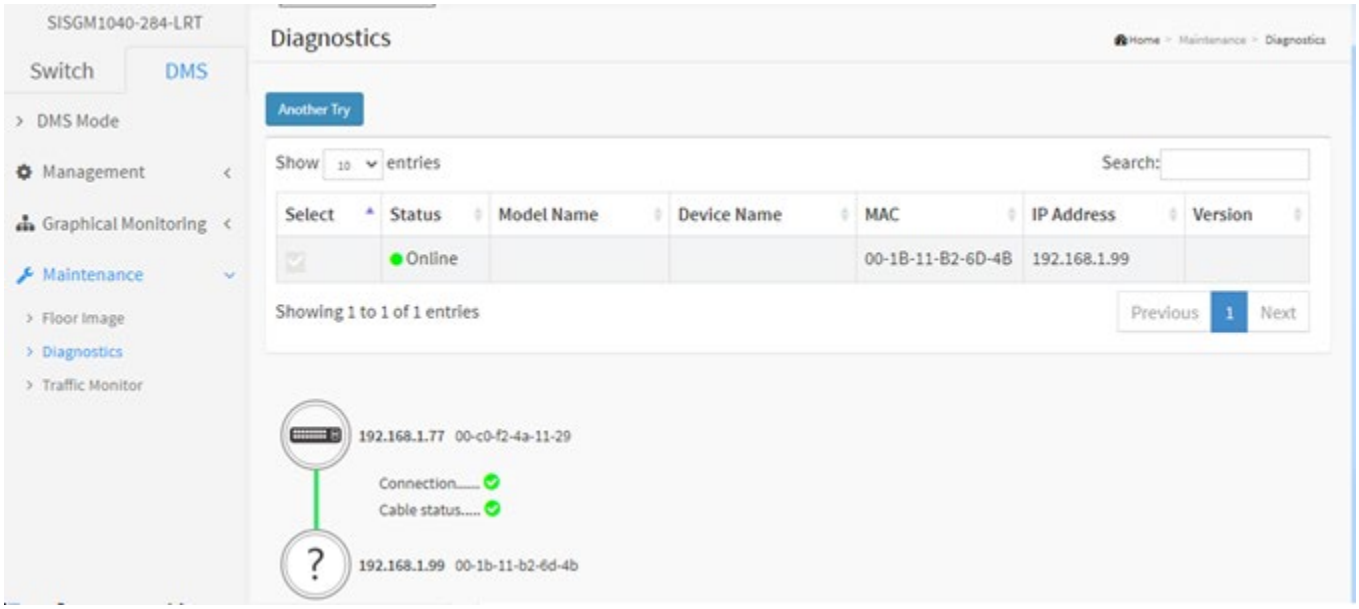
Buttons

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

Search: Enter text to search for any key word you want.



Example: Diagnostic run with Connection and Cable status passed (OK).



Connection.....● : Connection diagnostic passed.

Cable status.....● : Cable diagnostic passed.

Connection.....● : Connection diagnostic failed.

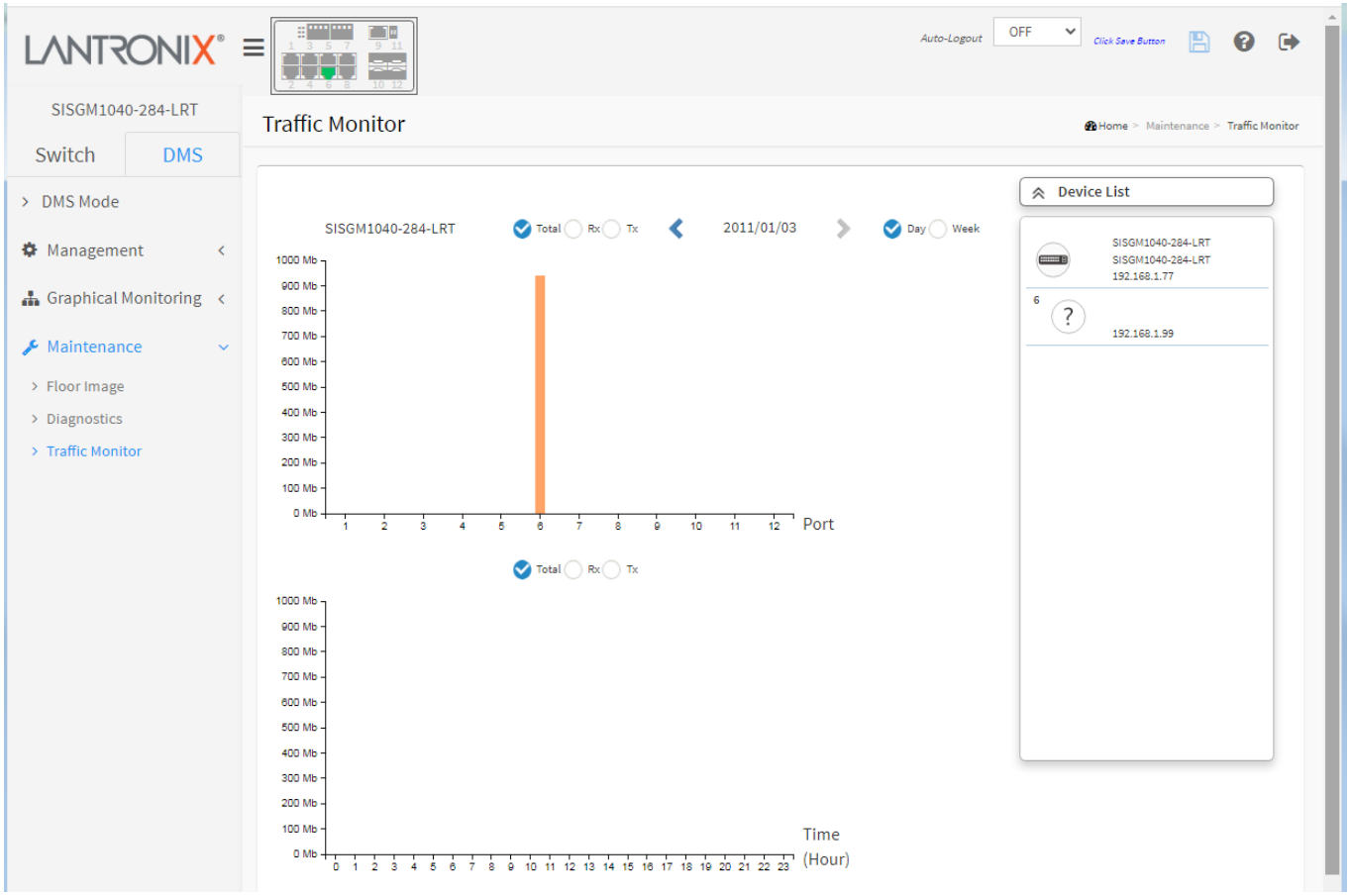
Cable status.....● : Cable diagnostic failed.

Buttons

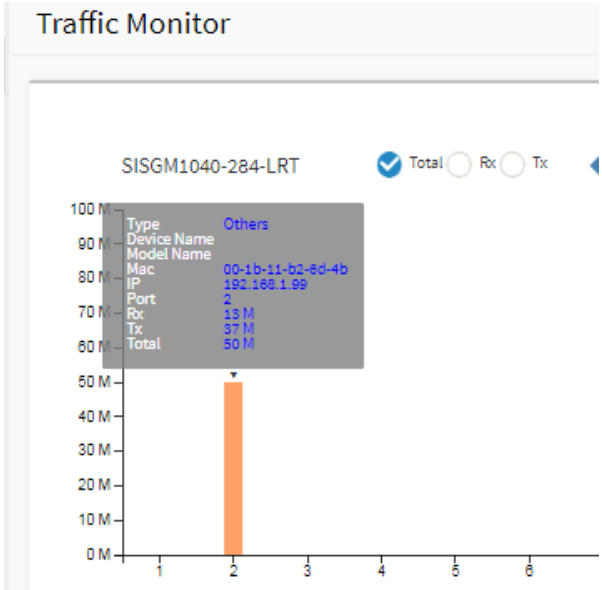
Another Try: Click to return to the previous page.

DMS > Maintenance > Traffic Monitor

This page displays a visual chart of network traffic of all the devices. Numbers are shown in Mbps. To view the traffic through a specific port click on a specific port on the traffic chart to reveal its traffic during the day. You can select to display a summary of a day's or a week's traffic by selecting the check circle on top. The same applies to the selection of Rx Tx traffic. A single port's traffic is shown at the lower half of the screen.



Hover the cursor over a chart column to display device information.



DMS Troubleshooting

Problem: The switch lists itself as the only device in Topology View of DMS.

Problem: In DMS, the Local image shows the IP address of another switch.

Description: The switch is listed as only device in DMS Topology View in DMS; all devices are listed in DMS device list. This is usually because the switch's gateway is not configured appropriately.

Resolution: An IP Route must be configured manually. For example, a switch IP address of 192.168.1.77 should have the following IP route configured: ip route 0.0.0.0 0.0.0.0 192.168.1.x. Without the IP route configured, you may be unable to view all devices on the network in DMS.

1. Go to DMS > Management > DMS Mode to check if the controller IP is correct.
2. Verify that the gateway of this switch is correctly configured.
3. Verify that all connected devices are displayed in DMS Topology View.

Problem: DMS Connectivity diagnostics fails to ICMP reachable device.

Description: DMS displays a device which is reachable via ICMP ping as failing the connection status in diagnostics. Cable status displays as *OK*.

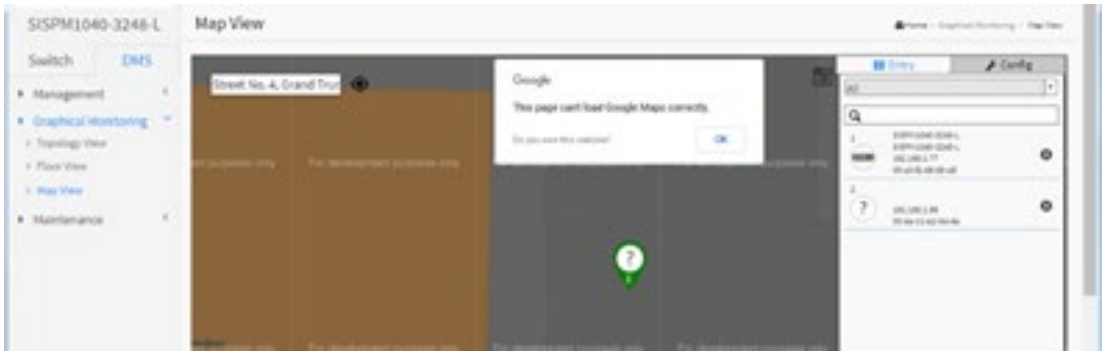
Resolution: Contact TN Technical Support.

Problem: DMS will discover the device type, name and model of some cameras and hosts but others are displayed as *Unknown*.

Description: When a device is detected by DMS, the device's information (such as type, model name…etc.) can be recognized via LLDP (e.g. Switch), UPnP (e.g. AP), ONVIF (e.g. IP cam), NBNS (e.g. PC) packets if the device supports these protocols. So if the device display as *Unknown*, that means this device do not issue above mentioned protocol for DMS to recognize.

Resolution: You can manually assign and configure the device type and name for the unknown devices. See the Topology View > Dashboard or the Topology View section.

Message: *This page can't load Google Maps correctly.* See DMS > Management > Map API Key on page 391.



Appendix A – DHCP Per Port Configuration

You can configure DHCP Per Port via the Web UI as described below.

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.

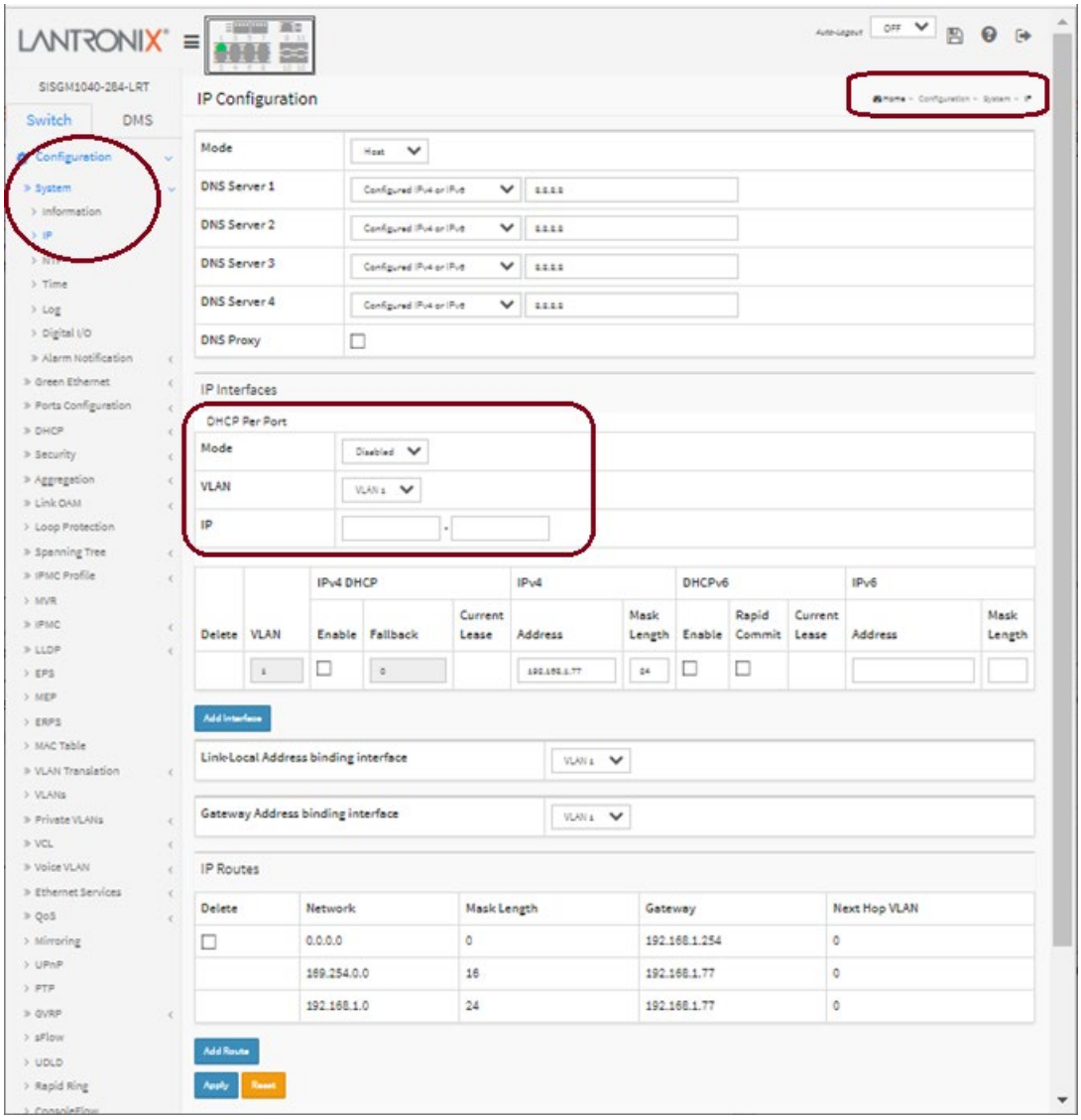
The DHCP Per Port pages and parameters are described below.

DHCP Per Port 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 and monitor DHCP Per Port via the Web UI, navigate to the Switch > System > IP Address > Advanced Settings menu path.



DHCP Per Port Mode: at the dropdown select Enable or Disable the DHCP Per Port function globally. The default is Disabled.

DHCP Per Port VLAN: The DHCP Per Port VLAN function lets you have an IP address from a DHCP pool on a switch be statically assigned to a switchport, such that whichever device plugs into the switchport it will always be assigned that specific IP address. The IP address is configured in the interface config settings. Note that this is binding an IP address to an interface, not to a MAC address, which is the classic binding technique found on most switches. 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. (Added at FW VB7.20.0140.) See “Configuration > System > IP” on page 15 for more information.

DHCP Per Port IP: enter the IPv4 IP address range to be used when the DHCP Per Port function is enabled (e.g., 192.168.1.78 - 192.168.1.101). 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.

Buttons

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.

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”.

Message: *DHCP Per Port IP range (192.168.1.1 - 192.168.1.10) is not equal to switch TP port number (8)*

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 34.

Message: *DHCP per Port range (192.168.1.50 - 192.168.1.66) is not equal to switch TP port number (8).*

Message: *Update success!*

Appendix B - Rapid Ring Operation

Rapid Ring Operation

Rapid Ring is a proprietary redundancy network ring protocol. It can be used to recover the network from critical link failure to provide fault failover protection.

Many redundant or network recovery protocols are defined by IEEE, such as spanning tree (STP, RSTP, MSTP) are available to recover the network from link failures. But the recovery time to propagate broadcast packets to the failover port can take several seconds, depending on the amount of network traffic. Rapid Ring recovery is less than 20ms for up to 250 switches.

The SISGM1040-284-LRT supports four types of ring topology:

- Single Ring
- Ring to Ring
- Dual Ring
- Rapid Chain

The four types of Rapid Ring and how to configure them is described below.

Note: Only one redundant protocol can be used at the same time. Before you enable Rapid Ring, you must disable Spanning Tree.

Single Ring

Single Ring can be used to recover the network if a critical link failure occurs. With Single Ring, one of the switches must be configured as the “Master” and the other switches as Members of the single ring. Each switch will have a forwarding path and a backup path on the Ring Master. If one link fails, the ring will automatically activate the backup path within 20ms.

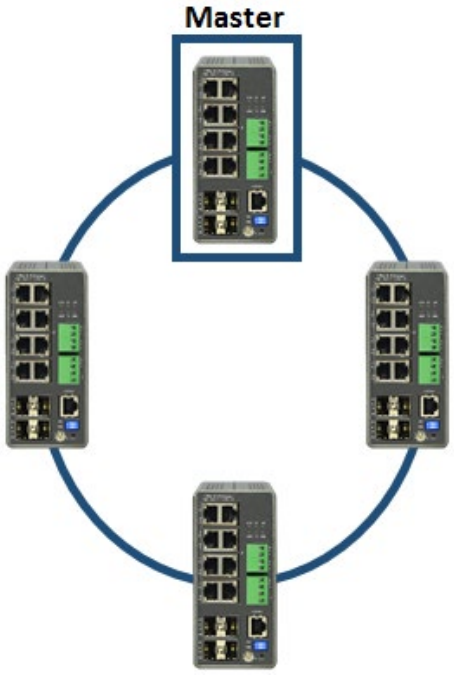


Figure 1: Single Ring

Single Ring configuration is shown and described below.

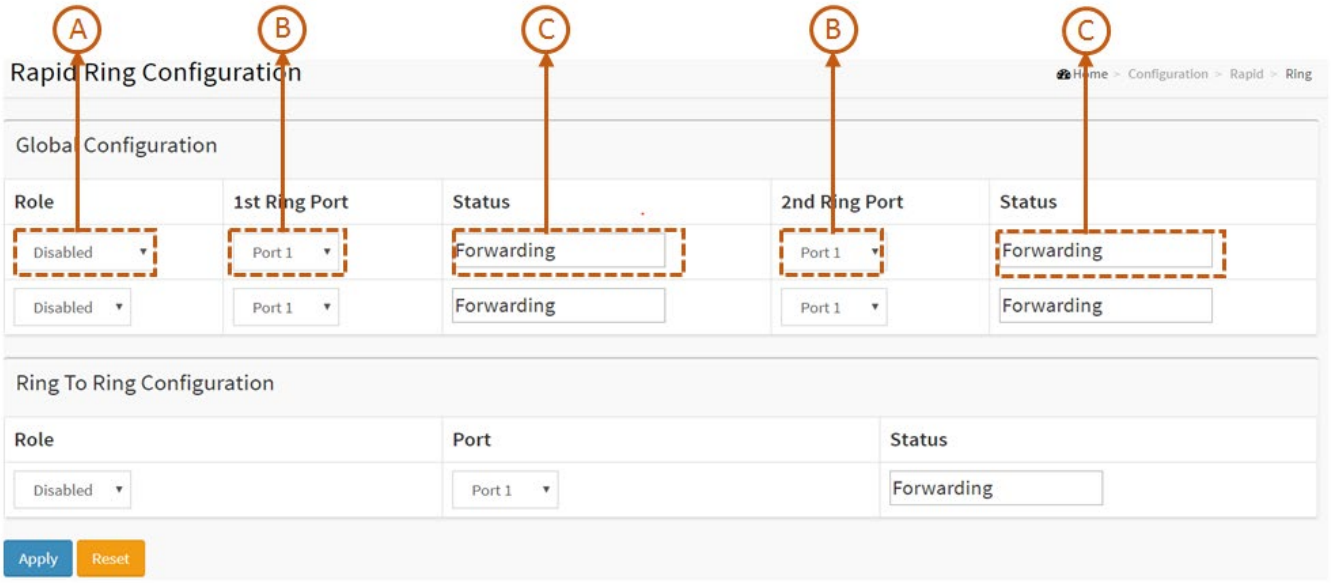


Figure 2: Single Ring Configuration

A. Configure the Role as **Master** or **Member**. Only one switch in the single ring can be the Master and rest of the switches must be set as Members of the single ring.

B. Configure 1st Ring Port and 2nd Ring Port as link ports.

C. If it is Master, by default 1st Ring Port will be the active path and 2nd Ring Port will be the backup path.

D. If it is a Member, 1st Ring Port and 2nd Ring Port is used to connect the link partner of the Single Ring.

E. Indicates port status (e.g., Forwarding, Discarding, etc.).

Ring to Ring

Ring to Ring is a flexible application that connects several single rings together. Since some devices could be located in a remote area, it may not be convenient to connect all devices in the system to create a single ring. Ring to Ring can be used to connect the devices into different single rings. They can still communicate with each other. If any path fails, it can recover the network system within 20ms.

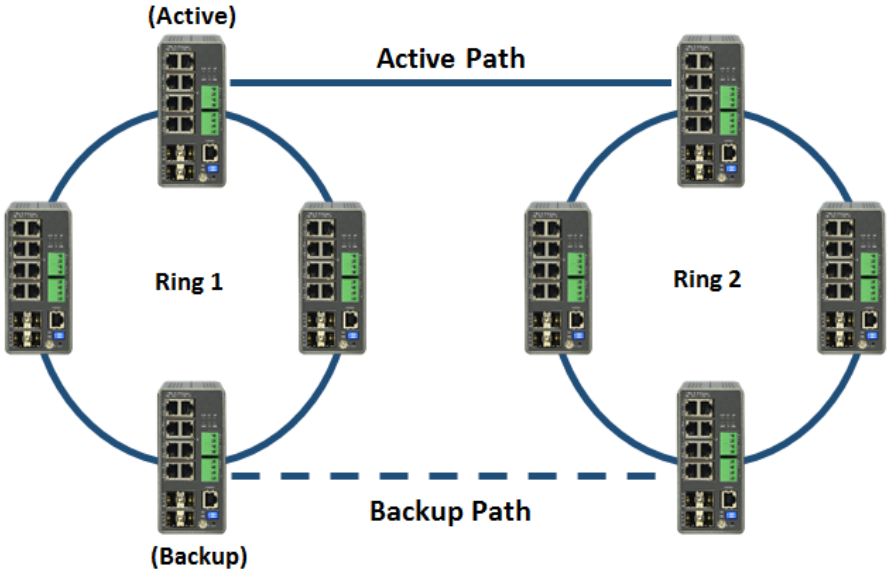


Figure 3: Ring to Ring Overview

Ring to Ring configuration is shown and described below.

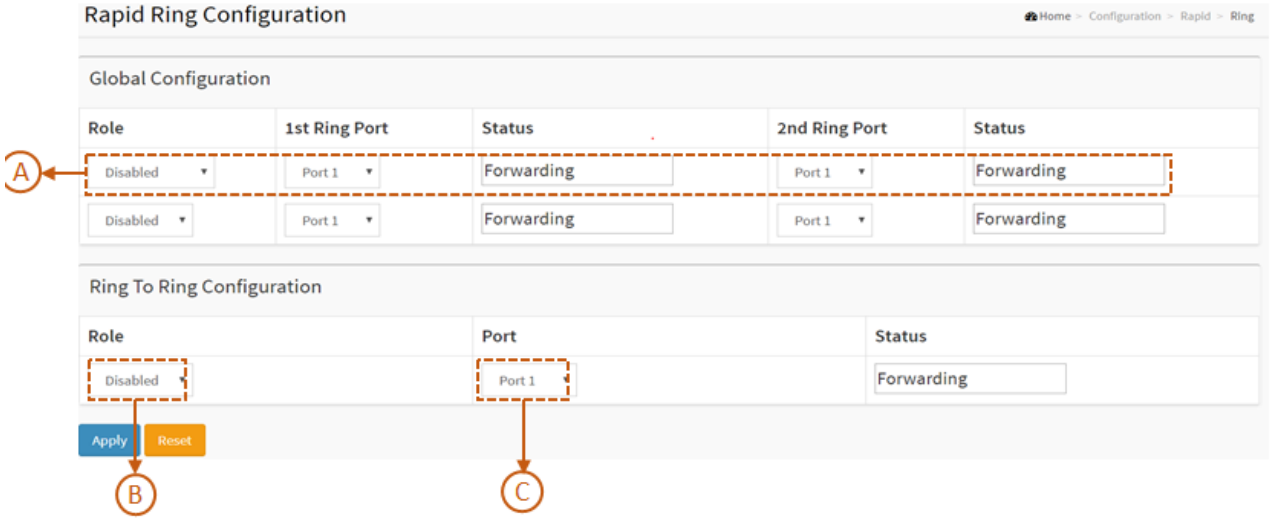


Figure 4: Ring to Ring Configuration

A. Set up Single Ring for Ring 1 and Ring 2, setting can refer to 2-1.2.
B. Configure the Role as **Active** or **Backup** or **Disabled**. Choose one specific Ring (Ring 1 or Ring 2) to set up ring-to-ring configuration. Remember to configure Active and Backup Switch connected to another ring. Only one switch can be set to be the Active/ Backup, and the rest of the switches should be configured as Disabled.
C. Configure Active/ Backup link port. This port should not be same as above 1st Ring Port and 2nd Ring Port.

Dual Ring

Dual Ring is a more economical application, which uses only one switch between the two rings. This mode is ideal for applications that have inherent cabling difficulties and saves costs.

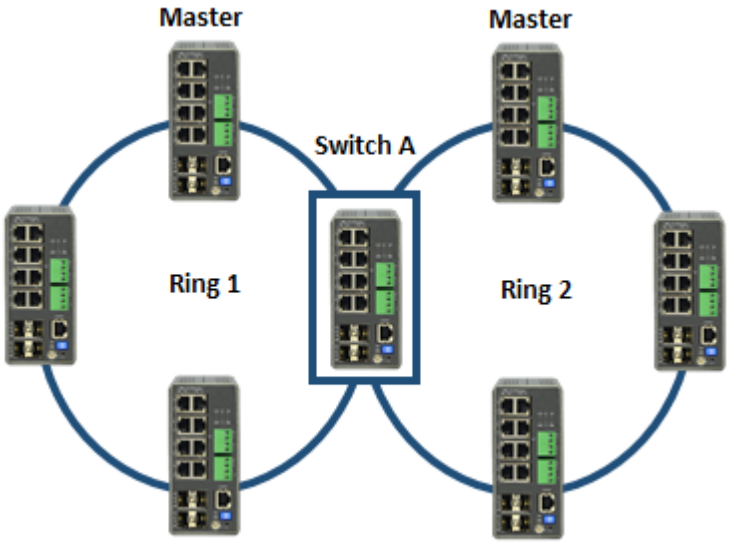


Figure 5: Dual Ring Overview

Dual Ring configuration is shown and described below.

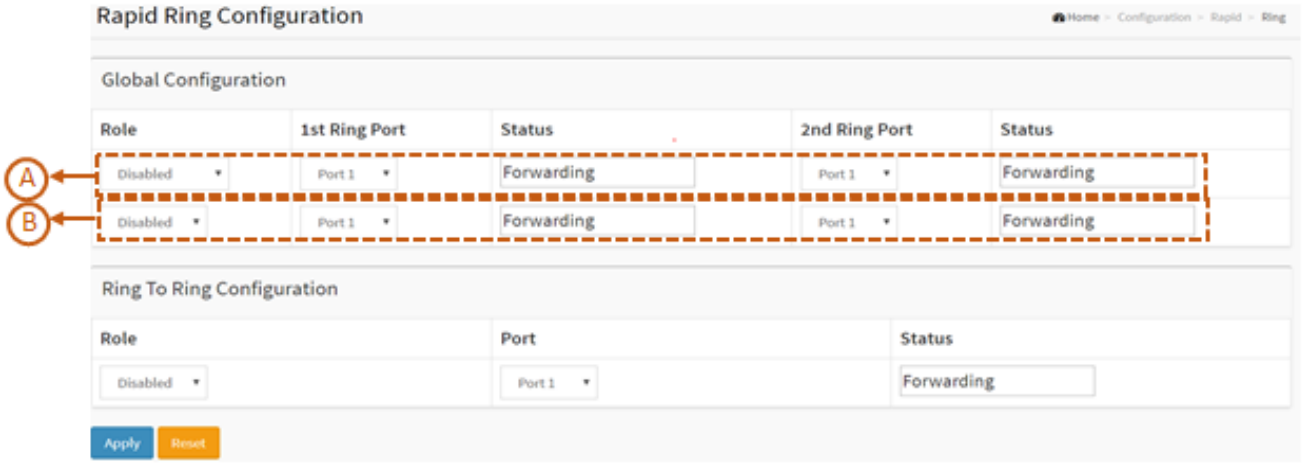


Figure 6: Dual Ring Configuration

A. Set up Single Ring for Ring 1 and Ring 2; refer to Single Ring above.

B. Setup second ring for switch A; refer to Single Ring above.

Note: Switch A is not suggested to be the Master for Ring 1 or Ring 2.

Rapid Chain

Rapid Chain is a highly flexible application for complex industrial networks. It allows the switches to be quickly and easily deployed in any type of complex redundant network with a fast recovery time.

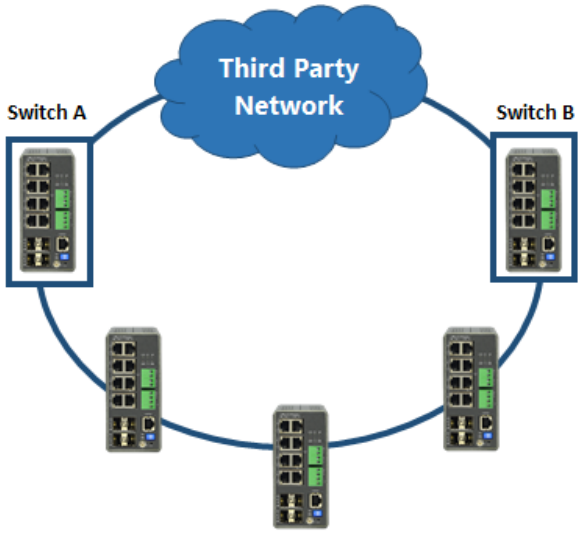


Figure 7: Rapid Chain Overview

Rapid Chain configuration is shown and described below.

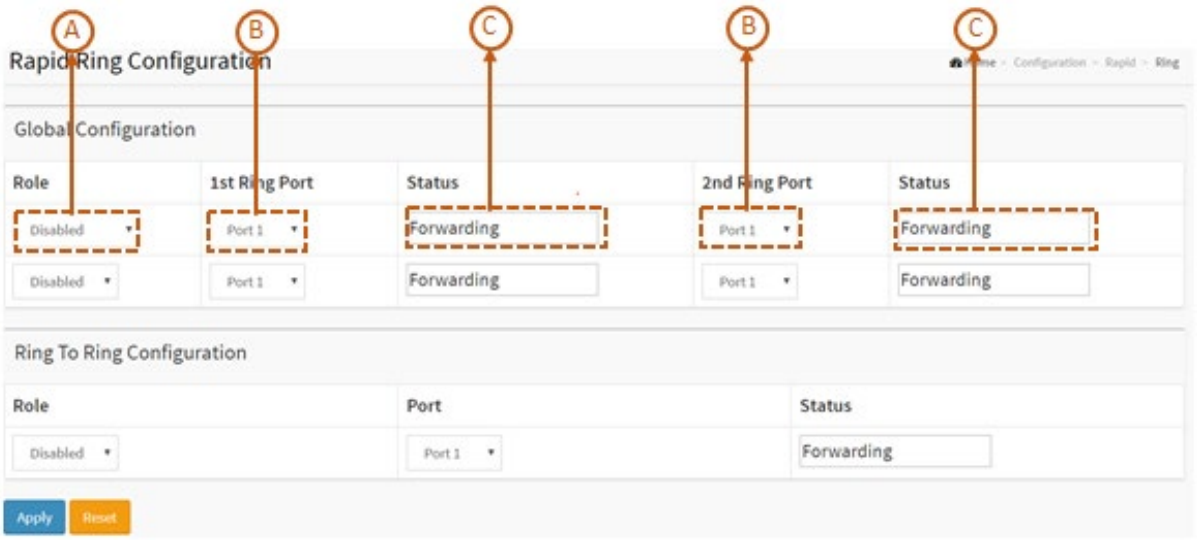


Figure 8: Rapid Chain Configuration

A. Configure the Role as **Rapid-Chain** or **Member**. Only two switches (Switch A & B) have to be set as Rapid-Chain, and the rest of the switches should be set as the Member of Rapid Chain.

B. Configure 1st Ring Port and 2nd Ring Port as link port.

C. If it is Rapid-Chain, 2nd Ring Port has to connect to Third Party Network.

D. If it is Member, 1st Ring Port and 2nd Ring Port is connected to link partner of the Rapid Chain.

E. Indicates Port status (e.g., Forwarding, Discarding).

Note: If it is Rapid-Chain, one of Switch A & Switch B's 2nd port will be the backup path chosen by the smaller MAC address.

Hardware Setting and Status for Ring

Ring Setting by DIP Switch

The front panel DIP switch settings are shown and described below. Note that **RM** indicates Ring Master and **RC** indicates Rapid Chain.

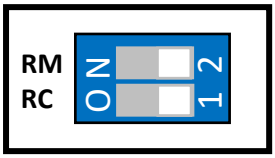


Figure 9: DIP Switch

Configure Rapid Ring by hardware DIP Switch as shown in the table below:

Table 1: DIP Switch Settings

Mode	RM	RC	Rapid Ring Status	1st Port	2nd Port	RM LED	RC LED
HW Control	OFF	OFF	Single Ring Member	The largest Odd Port Number	The largest Even Port Number	Lit Amber	Off
HW Control	ON	OFF	Single Ring Master	The largest Odd Port Number	The largest Even Port Number	Lit Green	Off
HW Control	OFF	ON	Rapid Chain	The largest Odd Port Number	The largest Even Port Number	Off	Lit Green (Active Path); Lit Amber (Backup Path)
SW Control	ON	ON	Rapid Ring Settings by Software	--	--	--	--

Note:

1. DIP Switch default settings are ON/ON (SW Control).
2. In HW mode, all Rapid Ring and Spanning Tree SW configuration from Web, Telnet, and Console is "deactivated".
3. Only Single Ring and Rapid Chain are configurable by DIP Switch.
4. The largest Even/Odd ports include both fiber and copper ports. For a Combo port, either fiber or copper can be used as the Ring connecting port.

RM and RC LED Descriptions

The table below describes the front panel **RM** (Ring Master) and **RC** (Rapid Chain) LED status:

Table 2: LED Status

LED	Color	State	Description
RM (Ring Master)	Green	On	Ring Master has been detected in the switch.
	Amber	On	Ring Member has been detected in the switch.
	--	Off	Disabled
RC (Rapid Chain)	Green	On	Rapid Chain has been detected in the switch (Active path).
	Amber	On	Rapid Chain has been detected in the switch (Backup path).
		Blinking	Error: *There is no correspondent Rapid Chain Switch found.*
	--	Off	Disabled

Appendix C – MRP Operation and Examples

You can configure Media Redundancy Protocol (MRP) parameters via the Web UI at Configuration > MRP and monitor them at Monitor > MRP, and via the CLI. See the *CLI Reference* for Command Line operation.

According to ANSI, IEC 62439-2 Ed. 1.0 b:2010 is applicable to high-availability automation networks based on ISO/IEC 8802-3 / IEEE 802.3 Ethernet technology. It specifies a recovery protocol based on a ring topology, designed to react deterministically on a single failure of an inter-switch link or switch in the network, under the control of a dedicated Media Redundancy Manager (MRM) node.

Media Redundancy Protocol per IEC 62439-2 is an interoperable ring technology designed to allow a switch to connect onto a universal redundant high speed ring. MRP is self-healing and self-adjusting, requiring no operator interaction. MRP is based on the concept of standby connections for seamless redundancy.

MRP Description

1. MRP operates at the MAC Layer of the Ethernet Switch.
2. The Ring Manager is called the Media Redundancy Manager (MRM).
3. Ring Clients are called Media Redundancy Clients (MRCs).
4. MRM and MRC ports support three Status Types:
   a. *Disabled* ring ports drop all the received frames.
   b. *Blocked* ring ports drop all the received frames except the MRP control frames.
   c. *Forwarding* ring ports forward all the received frames.
5. Ring Reconfiguration speed is 200 ms for 50 switches on average.
6. The MRM continuously sends Watchdog Packets into the ring network to verify communication between ring points.
7. During normal operation, no packets are transmitted over the redundant link.
8. When the MRM no longer receives the Watchdog Packets it sent out, the redundant path is immediately activated, and it becomes the primary layer 2 packet path.
9. When the failed link is restored:
   a. The MRM switches back to normal operation and the first Path becomes the primary path again.
   b. You can configure a period of time before the MRM switches back to the primary path (to prevent the circuit from flapping if it is not stable).

MRP Operation

Normal operation: the network works in the *Ring-Closed* status. In this status, one of the MRM ring ports is blocked, while the other is forwarding. Conversely, both ring ports of all MRCs are forwarding. Loops are avoided because the physical ring topology is reduced to a logical stub topology.

Failure mode: the network works in the *Ring-Open* status. For instance, in case of failure of a link connecting two MRCs, both ring ports of the MRM are forwarding. The MRCs adjacent to the failure have a blocked and a forwarding ring port; the other MRCs have both ring ports forwarding. The physical ring topology is also a logical stub topology in the Ring-Open status.

Note that multiple MRMs in a single ring is not supported. If there are two MRMs in one ring, then both MRMs are generated by the event MULTIPLE_MANAGERS. Having multiple active MRMs cause the ring to an incorrect state. The fix is to change all active MRMs except one to the MRC state.

Related Devices

MRP is implemented on Lantronix SISPM1040-384-LRT-C, SISPM1040-362-LRT, SISPM1040-582-LRT, and SISGM1040-284-LRT switches.

MRP Sample Setup

The example below shows SISPM1040-384-LRT-C switches (one MRM and five MRCs).

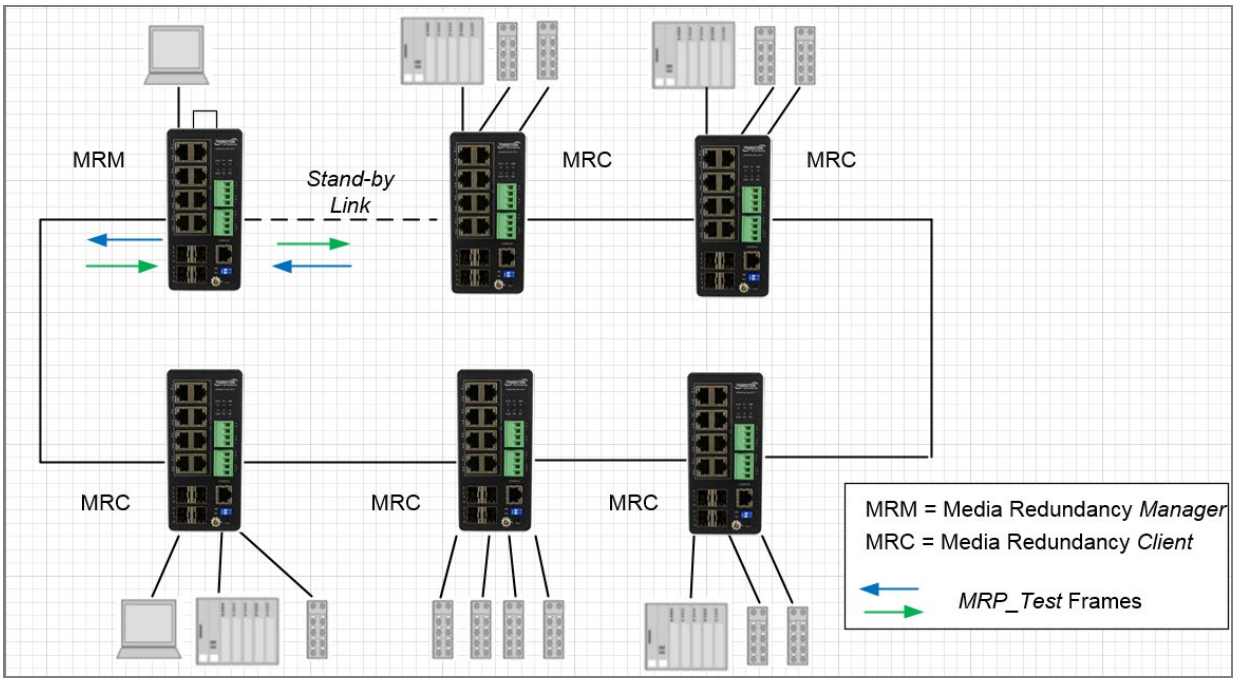


Figure: MRP Sample Setup

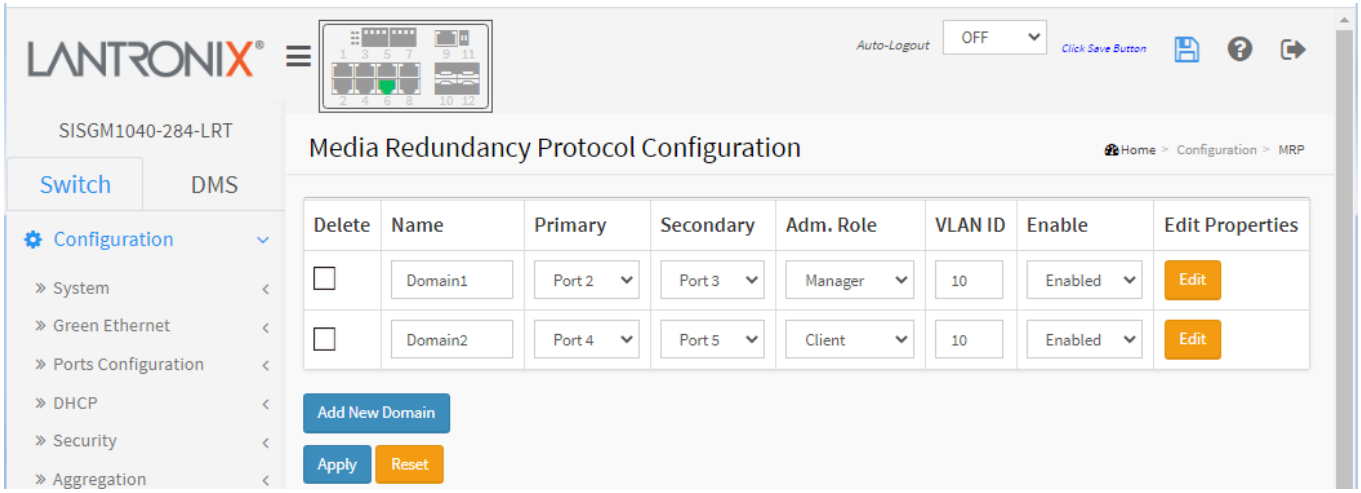
MRP Pre-Requisites (General)

The following are required to perform MRP setups.

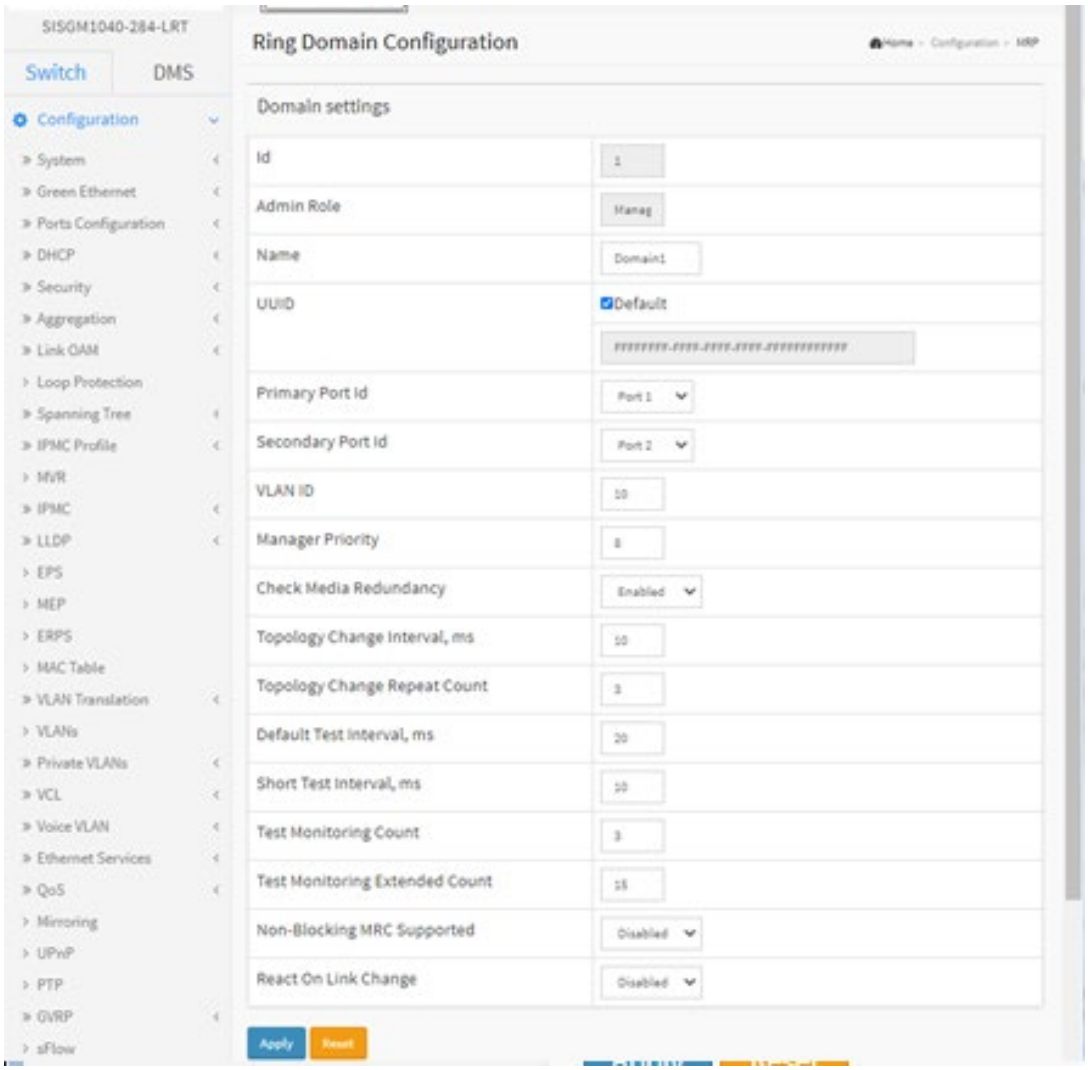
1. Spanning Tree must be disabled at Configuration > Spanning Tree > CIST Port.
2. Other Ring technologies must be disabled (G.8031 EPS, G.8032 ERPS, Rapid-Ring, Ring-To-Ring, etc.).
3. Multiple MRMs in a single ring is not supported. If there are two MRMs in one ring, then both MRMs are generated by the event MULTIPLE_MANAGERS. The multiple active MRMs cause the ring to an incorrect state. Fix: change all active MRMs except one to the MRC state.
4. Other pre-requisites may apply to the specific examples below.

MRP Web UI Configuration

1. Navigate to Switch > Configuration > MRP to initially configure two MRP Domains:

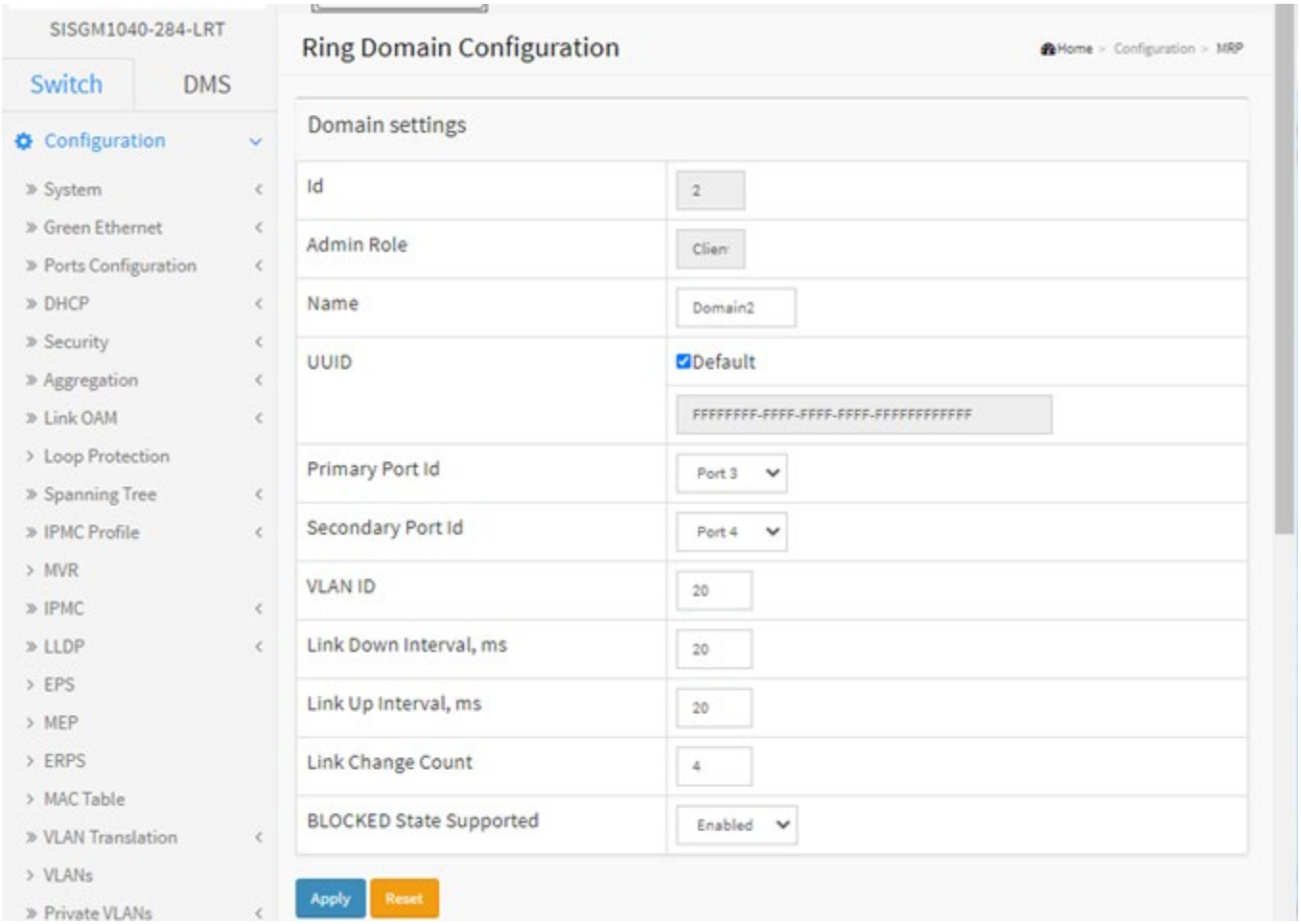


2. Click Apply to save, and then click the Edit button to configure the first MRP Domain (Domian1).



3. Edit the Domain Settings as required. Click Apply to save; the message "*Domain is enabled*" displays. Click OK to clear the webpage message. The "Media Redundancy Protocol Configuration" page displays again.

4. Click the Edit button to display the second MRP Domain (Domian2).



5. Edit the Domain Settings as required. Click Apply to save; the message "*Domain is enabled*" displays. Click OK to clear the webpage message.

6. When the "Media Redundancy Protocol Configuration" page displays again, verify the settings.

Example 1: MRP Manager Re-Config (Web UI)

This application example shows the MRP Manager reconfiguring the traffic path based on the client state.

Sample Setup: This setup includes one device with MRP enabled and has an admin role set as Manager and three clients connected in a ring topology. See the MRP Sample Setup diagram below.

Procedure:

1. Disable any other Ring technologies and disable Spanning-tree at Configuration > Spanning Tree > CIST Port.
2. For the device acting as MRM click 'Add New Domain' button to configure the MRP instance in the 'Media Redundancy Protocol Configuration' page.
3. Assign the first ring port under 'Primary' and the second ring port under 'Secondary'.
4. Set the Administrative Role to 'Manager' under 'Adm. Role'. Assign any VLAN ID from 2-4094.
5. Set the instance to 'enable'.
6. Go to the 'Ring Domain Configuration (Manager Role)' page and set a Domain name.
7. Tick the Default box for UUID.
8. Select the Primary and Secondary Port IDs.
9. Enable 'Check Media Redundancy'.
10. Leave other settings as default.
11. For the devices acting as MRCs in the 'Ring Domain Configuration (Client Role)' page assign the first Primary and Secondary Port IDs for the ring ports.
12. Enter the same VLAN ID as in step 4 above.
13. Link Down Interval should be 20ms. Link Up Interval should be 20ms. Link change count should be 4.
14. 'BLOCKED State Supported' must be enabled. By default, one ring port will be disabled for loop-free communication.
15. Configure ring ports to Hybrid mode on the VLAN Configuration page. Assign the VLAN ID as configured in step 4.
16. Send bi-directional traffic tagged with the VLAN ID set in step 4 above.
17. Create a failure on any one of the client ring ports by disconnecting the cable. The MRM should reconfigure the path within 200<500ms. The Redundancy manager will send test frames marked with a unique MAC with OUI of 00-15-4E and forwarded by the MRCs to the opposite ring ports per the interval specified.
    The disabled ring port should now be enabled, creating a new loop-free topology.
18. There should be no traffic loss after path reconfiguration.

Example 2: Non-Blocking MRC State Recognized by MRM (Web UI)

This application example shows a Non-blocking MRC state is recognized by the MRM.

Setup: This setup and steps 1-18 in Example 1 above are required.

Procedure:

1. Disable any other Ring technologies and disable Spanning-tree at Configuration > Spanning Tree > CIST Port.
2. Disable 'BLOCKED State Supported'.
3. Configure ring ports to Hybrid mode on the VLAN Configuration page. Assign the VLAN ID as configured in step 4 of Example 1.
4. Send bi-directional traffic tagged with the VLAN ID set in the previous step.
5. Create a failure on any one of the client ring ports by disconnecting the cable. The client ring ports will be in a forwarding state instead of blocking. The MRM should reconfigure the path within 200<500ms. The MRM will send test frames marked with a unique MAC with OUI of 00-15-4E and forwarded by the MRCs to the opposite ring ports per the interval specified.
6. Verify the MRC reacts to the reconfiguration frames as received by the MRM. The link down on the client ring port should be detected by the MRC.
7. There should be no traffic loss after path reconfiguration.

Example 3: MRP Roles Set in Web UI

Setup: This setup shows that the MRP can have both Manager and Undefined roles.

Procedure:

1. Disable any other Ring technologies and disable Spanning-tree at Configuration > Spanning Tree > CIST Port.
2. 'BLOCKED State Supported' should be enabled. By default, one ring port will be disabled for loop-free communication.
3. Configure ring ports to Hybrid mode on the VLAN Configuration page. Assign the VLAN ID as set in step 4 of Example 1.
4. Send bi-directional traffic tagged with the VLAN ID set in the previous step.
5. Create a failure on any one of the client ring ports by disconnecting the cable. The MRM should reconfigure the path within 200<500ms. The Redundancy manager will send test frames marked with a unique MAC with OUI of 00-15-4E and forwarded by the MRCs to the opposite ring ports per the interval specified.
   The disabled ring port should now be enabled and creates a new loop-free topology.
6. There should be no traffic loss after path reconfiguration.
7. On a second client set the 'BLOCKED State Supported' option to disable. The ring port will now be in a forwarding state. Cause a failure on the ring port of another device that has its blocked state disabled.
8. Verify that frames are forwarded and received by the MRC with blocking enabled. There should be no traffic loss after path reconfiguration.

Appendix D – G.8032 Major and Sub Rings Configuration

Introduction

Ethernet Ring Protection Switching (ERPS) is a protocol defined by the International Telecommunication Union - Telecommunication Standardization Sector (ITU-T) to prevent loops at Layer 2. With the standard number is ITU-T G.8032, and ERPS is also called G.8032. Generally, redundant links are used on a network to provide link backup and enhance network reliability. The use of redundant links, however, may produce loops, causing broadcast storms and rendering the MAC address table unstable. These can affect the network, where the communication quality is not good enough, and communication services might be interrupted.

ERPS provides advantages of traditional ring network technologies such as STP/RSTP/MSTP and optimizes detection mechanism to provide faster convergence. For example, the ERPS-enabled switch provides 50-ms convergence for broadcast packets. See “Configuration > ERPS” on page 172 for general G.8032 ERPS configuration information.

Basic Concepts

There are some basic concepts that support ERPS Ring:

- **Ring Protection Link (RPL)** – Link designated by mechanism that is blocked during Idle state to prevent loop on Bridged ring.
- **RPL Owner node** – Node connected to RPL that blocks traffic on RPL during Idle state and unblocks during Protection state.
- **RPL Neighbor node** – Node connected to RPL that blocks traffic on RPL during Idle state and unblocks during Protection state (v2).
- **Link Monitoring** – Links of ring are monitored using standard ETH CC OAM messages (CFM) • Signal Fail (SF) – Signal Fail is declared when signal fail condition is detected.
- **No Request (NR)** – No Request is declared when there are no outstanding conditions (e.g., SF, etc.) on the node.
- **Ring APS (R-APS) Messages** – Protocol messages defined in Y.1731 and G.8032.
- **Automatic Protection Switching (APS) Channel** - Ring-wide VLAN used exclusively for transmission of OAM messages including R-APS messages.

IP Addresses

The sample configurations below use these IP addresses:

SISPM1040-582-LRT : 192.168.1.85

SISPM1040-384-LRT-C : 192.168.1.95

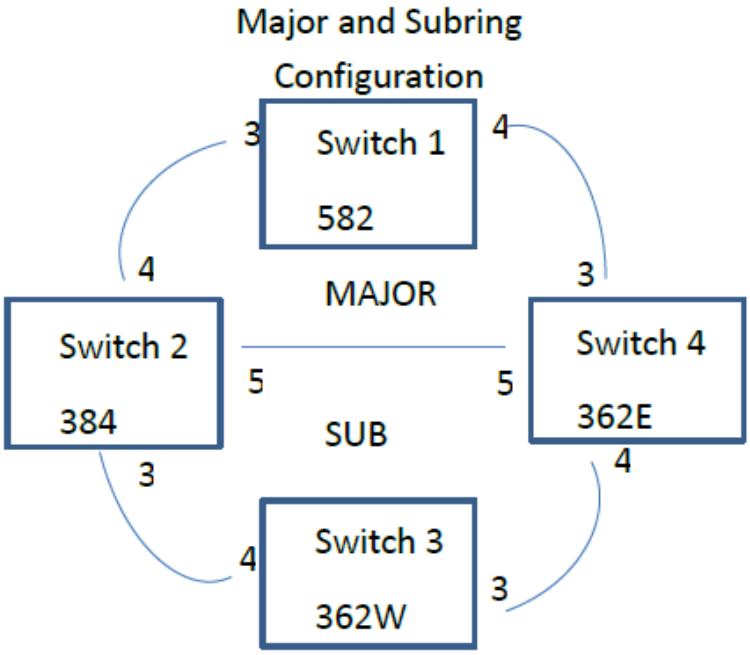
SISPM1040-362-LRT-W: 192.168.1.125

SISPM1040-362-LRT [E]): 192.168.1.135

Sample Configuration

Major Ring and Sub Ring : 4 Switches

Major : SW#1, SW#2, SW#4; **Sub** : SW#2, SW#3, SW#4



VLANs		APS	Data
		10,20	5

RPL Mode	Major	Sub	Major	Sub	Major	Sub
	Owner Switch #1	Owner Switch #3	Neighbor Switch #2	Neighbor Switch #2	None Switch #4	None Switch #4

Switch 1 Configuration (SISPM1040-582-LRT)

VLANs	Port 3	Trunk	Tag All	5,10
	Port 4	Trunk	Tag All	5,10
STP	Port 3	Disable		
	Port 4	Disable		

MEPs	Instance	Port	VLAN	MAC	MEP ID	Peer MAC	Peer MEP ID
	1	3	10	00-C0-F2-49-39-5F	1	00-40-C7-1C-C7-30	4
	2	4	10	00-C0-F2-49-39-60	5	00-C0-F2-53-EF-FC	5

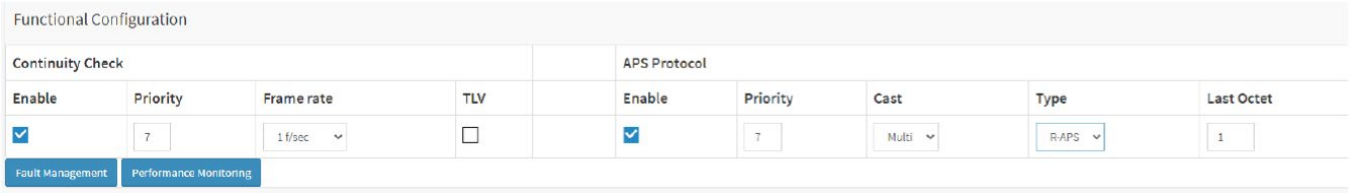
Note: All MEPs are programed the same under the Functional Configuration

Continuity Check

Check Enable – Priority: 7 – Frame rate: 1f/sec

APS Protocol

Check Enable – Priority: 7 – Cast: Multi – Type: R-APS



ERPS

ERPS ID	Port 0	Port 1	Port 0 SF	Port 1 SF	Port 0 APS	Port 1 APS	Ring	RPL	Port	VLAN
1	1	2	1	2	1	2	Major	Owner	0	5

Switch 2 Configuration (SISPM1040-384-LRT-C)

VLANs	Port 3	Trunk	Tag All	5,20
	Port 4	Trunk	Tag All	5,10
	Port 5	Trunk	Tag All	5,10,20
STP	Port 3	Disable		
	Port 4	Disable		
	Port 5	Disable		

MEPs	Instance	Port	VLAN	MAC	MEP ID	Peer MAC	Peer MEP ID
	1	3	20	00-40-C7-1C-C7-2F	3	00-C0-F2-53-F0-BA	8
	2	4	10	00-C0-F2-49-39-60	4	00-C0-F2-49-39-5F	1
	3	5	10	00-40-C7-1C-C7-31	9	00-C0-F2-53-EF-FE	10

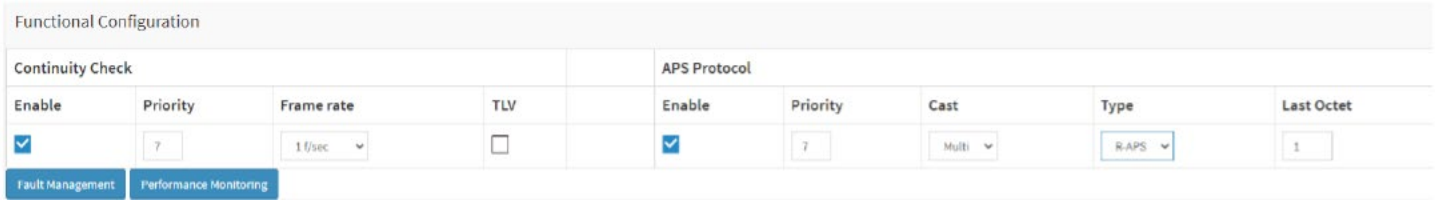
Note: All MEPs are programed the same under the Functional Configuration

Continuity Check

Check Enable – Priority: 7 – Frame rate: 1f/sec

APS Protocol

Check Enable – Priority: 7 – Cast: Multi – Type: R-APS



ERPS

ERPS ID	Port 0	Port 1	Port 0 SF	Port 1 SF	Port 0 APS	Port 1 APS	Ring	RPL Port	VLAN
1	3	2	3	2	3	2	Major	Neighbor	1 5
2	1	0	1	0	1	0	Sub	Neighbor	0 5

Interconnect Yes, Major 1

Switch 3 Configuration (SISPM1040-362-LRT [W])

VLANs	Port 3	Trunk Tag All 5,20
	Port 4	Trunk Tag All 5,20
STP	Port 3	Disable
	Port 4	Disable

MEPs	Instance	Port	VLAN	MAC	MEP ID	Peer MAC	Peer MEP ID
	1	3	20	00-C0-F2-53-F0-B9	7	00-C0-F2-53-EF-FD	6
	2	4	20	00-C0-F2-53-F0-BA	8	00-40-C7-1C-C7-2F	3

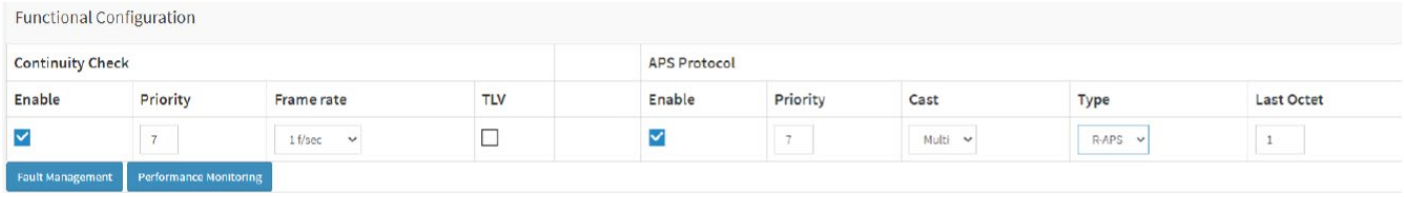
Note: All MEPs are programed the same under the Functional Configuration

Continuity Check

Check Enable – Priority: 7 – Frame rate: 1f/sec

APS Protocol

Check Enable – Priority: 7 – Cast: Multi – Type: R-APS



ERPS

ERPS ID	Port 0 Port	Port 0 VLAN	Port 1	Port 0 SF	Port 1 SF	Port 0 APS	Port 1 APS	Ring	RPL
1	1	2	1	2	1	2	Sub	Owner	1
5									

Switch 4 Configuration (SISPM1040-362-LRT [E])

VLANs	Port 3	Trunk	Tag All	5,10
	Port 4	Trunk	Tag All	5,20
	Port 5	Trunk	Tag All	5,10,20
STP	Port 3	Disable		
	Port 4	Disable		
	Port 5	Disable		

MEPs	Instance	Port	VLAN	MAC	MEP ID	Peer MAC	Peer MEP ID
	1	3	10	00-C0-F2-53-EF-FC	5	00-C0-F2-49-39-60	2
	2	4	20	00-C0-F2-53-EF-FD	6	00-C0-F2-53-F0-B9	7
	3	5	10	00-C0-F2-53-EF-FE	10	00-40-C7-1C-C7-31	9

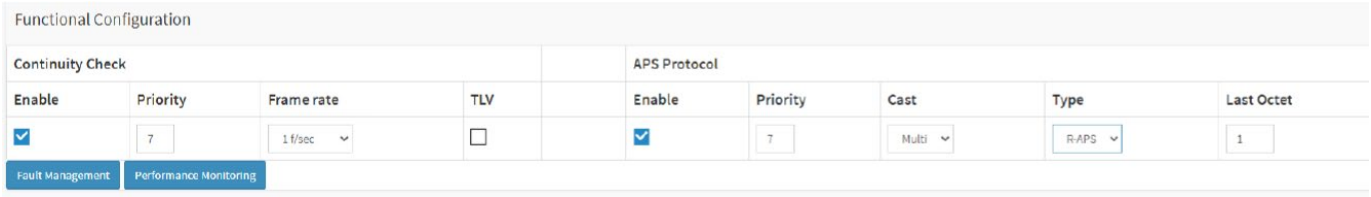
Note: All MEPs are programed the same under the Functional Configuration

Continuity Check

Check Enable – Priority: 7 – Frame rate: 1f/sec

APS Protocol

Check Enable – Priority: 7 – Cast: Multi – Type: R-APS



ERPS

ERPS ID	Port 0	Port 1	Port 0 SF	Port 1 SF	Port 0 APS	Port 1 APS	Ring	RPL	Port VLAN
1	1	3	1	3	1	3	Major	None	5
2	2	0	2	0	2	0	Sub	None	5

Interconnect Yes, Major 1

Testing

Testing Pings from Switch 4 to Switch 1 – Major Ring

Failing Major ring, No lost pings

C:\Users\dennist>ping 192.168.1.85 -t

Pinging 192.168.1.85 with 32 bytes of data:
Reply from 192.168.1.85: bytes=32 time<1ms TTL=64
Reply from 192.168.1.85: bytes=32 time<1ms TTL=64
Reply from 192.168.1.85: bytes=32 time<1ms TTL=64
Reply from 192.168.1.85: bytes=32 time<1ms TTL=64
Reply from 192.168.1.85: bytes=32 time<1ms TTL=64
Reply from 192.168.1.85: bytes=32 time<1ms TTL=64
Reply from 192.168.1.85: bytes=32 time<1ms TTL=64
Reply from 192.168.1.85: bytes=32 time<1ms TTL=64
Reply from 192.168.1.85: bytes=32 time<1ms TTL=64
Reply from 192.168.1.85: bytes=32 time<1ms TTL=64
Reply from 192.168.1.85: bytes=32 time<1ms TTL=64
Reply from 192.168.1.85: bytes=32 time<1ms TTL=64
Reply from 192.168.1.85: bytes=32 time<1ms TTL=64
Reply from 192.168.1.85: bytes=32 time<1ms TTL=64
Reply from 192.168.1.85: bytes=32 time<1ms TTL=64
Reply from 192.168.1.85: bytes=32 time<1ms TTL=64
Reply from 192.168.1.85: bytes=32 time<1ms TTL=64
Reply from 192.168.1.85: bytes=32 time<1ms TTL=64
Reply from 192.168.1.85: bytes=32 time<1ms TTL=64
Reply from 192.168.1.85: bytes=32 time=1ms TTL=64
Reply from 192.168.1.85: bytes=32 time<1ms TTL=64
Reply from 192.168.1.85: bytes=32 time<1ms TTL=64
Reply from 192.168.1.85: bytes=32 time<1ms TTL=64
Reply from 192.168.1.85: bytes=32 time<1ms TTL=64
Reply from 192.168.1.85: bytes=32 time<1ms TTL=64
Reply from 192.168.1.85: bytes=32 time<1ms TTL=64
Reply from 192.168.1.85: bytes=32 time<1ms TTL=64
Reply from 192.168.1.85: bytes=32 time<1ms TTL=64
Reply from 192.168.1.85: bytes=32 time<1ms TTL=64
Reply from 192.168.1.85: bytes=32 time=5ms TTL=64 ←----------
Reply from 192.168.1.85: bytes=32 time<1ms TTL=64 **Cable Disconnect**
Reply from 192.168.1.85: bytes=32 time=3ms TTL=64 ←----------
Reply from 192.168.1.85: bytes=32 time<1ms TTL=64
Reply from 192.168.1.85: bytes=32 time=1ms TTL=64
Reply from 192.168.1.85: bytes=32 time<1ms TTL=64
Reply from 192.168.1.85: bytes=32 time<1ms TTL=64
Reply from 192.168.1.85: bytes=32 time=1ms TTL=64
Reply from 192.168.1.85: bytes=32 time<1ms TTL=64
Reply from 192.168.1.85: bytes=32 time<1ms TTL=64
Ping statistics for 192.168.1.85:
Packets: Sent = 45, Received = 45, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 0ms, Maximum = 5ms, Average = 0ms

Testing Pings from Switch 4 to Switch 3 – Sub Ring

Fail Subring, No lost pings

C:\Users\dennist>ping 192.168.1.125 -t

Pinging 192.168.1.125 with 32 bytes of data:
Reply from 192.168.1.125: bytes=32 time=1ms TTL=64
Reply from 192.168.1.125: bytes=32 time<1ms TTL=64
Reply from 192.168.1.125: bytes=32 time<1ms TTL=64
Reply from 192.168.1.125: bytes=32 time<1ms TTL=64
Reply from 192.168.1.125: bytes=32 time<1ms TTL=64
Reply from 192.168.1.125: bytes=32 time<1ms TTL=64
Reply from 192.168.1.125: bytes=32 time<1ms TTL=64
Reply from 192.168.1.125: bytes=32 time<1ms TTL=64
Reply from 192.168.1.125: bytes=32 time<1ms TTL=64
Reply from 192.168.1.125: bytes=32 time<1ms TTL=64
Reply from 192.168.1.125: bytes=32 time<1ms TTL=64
Reply from 192.168.1.125: bytes=32 time<1ms TTL=64
Reply from 192.168.1.125: bytes=32 time<1ms TTL=64
Reply from 192.168.1.125: bytes=32 time=1ms TTL=64
Reply from 192.168.1.125: bytes=32 time<1ms TTL=64
Reply from 192.168.1.125: bytes=32 time<1ms TTL=64
Reply from 192.168.1.125: bytes=32 time<1ms TTL=64
Reply from 192.168.1.125: bytes=32 time<1ms TTL=64
Reply from 192.168.1.125: bytes=32 time<1ms TTL=64
Reply from 192.168.1.125: bytes=32 time<1ms TTL=64
Reply from 192.168.1.125: bytes=32 time<1ms TTL=64
Reply from 192.168.1.125: bytes=32 time=7ms TTL=64 ←----------
Reply from 192.168.1.125: bytes=32 time<1ms TTL=64 Cable Disconnect
Reply from 192.168.1.125: bytes=32 time<1ms TTL=64
Reply from 192.168.1.125: bytes=32 time<1ms TTL=64
Reply from 192.168.1.125: bytes=32 time<1ms TTL=64
Reply from 192.168.1.125: bytes=32 time<1ms TTL=64
Reply from 192.168.1.125: bytes=32 time<1ms TTL=64
Reply from 192.168.1.125: bytes=32 time<1ms TTL=64
Reply from 192.168.1.125: bytes=32 time=1ms TTL=64
Reply from 192.168.1.125: bytes=32 time<1ms TTL=64
Reply from 192.168.1.125: bytes=32 time=1ms TTL=64
Reply from 192.168.1.125: bytes=32 time<1ms TTL=64
Reply from 192.168.1.125: bytes=32 time<1ms TTL=64
Reply from 192.168.1.125: bytes=32 time<1ms TTL=64
Reply from 192.168.1.125: bytes=32 time<1ms TTL=64
Reply from 192.168.1.125: bytes=32 time<1ms TTL=64
Reply from 192.168.1.125: bytes=32 time<1ms TTL=64
Reply from 192.168.1.125: bytes=32 time<1ms TTL=64
Ping statistics for 192.168.1.125:
Packets: Sent = 41, Received = 41, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 0ms, Maximum = 7ms, Average = 0ms

Config files

running-config_192.168.1

```
hostname SISPM1040-362-LRT-E
username admin privilege 15 password encrypted
feec1d1085ff075fd03b1d2d5ab4c0befbff0917079c8abb3a77338041bf5d6e1771bdbbd1a317ea2f42fc2aacc8c5
0a8e667456d7c04099f74f8ef9dcc0fbd4
!
vlan 1
!
!
!
!
ip route 0.0.0.0 0.0.0.0 192.168.1.254
tzidx 0
exec-timeout autologout 0
snmp-server location DT Lab Ring
system name SISPM1040-362-LRT-E
system location DT Lab Ring
system description Managed Hardened PoE+ Switch, (4) 10/100/1000Base-T PoE+ Ports + (2)
10/100/1000Base-T Ports + (2) 100/1000Base-X SFP Ports
!
interface GigabitEthernet 1/1
!
interface GigabitEthernet 1/2
!
interface GigabitEthernet 1/3
 no spanning-tree
 switchport trunk allowed vlan 5,10
 switchport trunk vlan tag native
 switchport mode trunk
 poe mode disable
!
interface GigabitEthernet 1/4
 no spanning-tree
 switchport trunk allowed vlan 5,20
 switchport trunk vlan tag native
 switchport mode trunk
 poe mode disable
!
interface GigabitEthernet 1/5
 no spanning-tree
 switchport trunk allowed vlan 5,10,20
 switchport trunk vlan tag native
 switchport mode trunk
!
interface GigabitEthernet 1/6
!
interface GigabitEthernet 1/7
!
interface GigabitEthernet 1/8
!
interface vlan 1
 ip address 192.168.1.135 255.255.255.0
 ip dhcp server
!
mep 1 down domain port level 4 interface GigabitEthernet 1/3
mep 1 mep-id 5
mep 1 vid 10
mep 1 peer-mep-id 2 mac 00-C0-F2-49-39-60
mep 1 cc 7
mep 1 aps 7 raps
mep 2 down domain port level 4 interface GigabitEthernet 1/4
```

```
mep 2 mep-id 6
mep 2 vid 20
mep 2 peer-mep-id 7 mac 00-C0-F2-53-F0-B9
mep 2 cc 7
mep 2 aps 7 raps
mep 3 down domain port level 4 interface GigabitEthernet 1/5
mep 3 mep-id 10
mep 3 vid 10
mep 3 peer-mep-id 9 mac 00-40-C7-1C-C7-31
mep 3 cc 7
mep 3 aps 7 raps
erps 1 major port0 interface GigabitEthernet 1/3 port1 interface GigabitEthernet 1/5
erps 1 mep port0 sf 1 aps 1 port1 sf 3 aps 3
erps 1 vlan 5
erps 2 sub port0 interface GigabitEthernet 1/4 interconnect 1
erps 2 mep port0 sf 2 aps 2
erps 2 vlan 5
!
spanning-tree aggregation
 spanning-tree link-type point-to-point
!
!
line console 0
!
line vty 0
!
line vty 1
!
line vty 2
!
line vty 3
!
line vty 4
!
line vty 5
!
line vty 6
!
line vty 7
!
line vty 8
!
line vty 9
!
line vty 10
!
line vty 11
!
line vty 12
!
line vty 13
!
line vty 14
!
line vty 15
!
!
end
```

running-config_192.168.1

```
hostname SISPM1040-582-LRT
logging on
logging host 192.168.1.253
username admin privilege 15 password encrypted
7073dec86c15b8a9907bb4106ef783adde46bd5b5969cc68fb55b430336bd7c80d5ded65d2fdb39abe81cc9caa5a93
620f270c21bca86e776cee9c5588bfb8c7
username superuser privilege 15 password encrypted
4643fdc71f39fd4cb955943fcaf89faca81bc650fbaeebe25a796662d5c225bf0d5ded65d2fdb39abe81cc9c514497
e27799560e488713aabaac4f167e7732ca
!
vlan 1
!
!
!
!
ip route 0.0.0.0 0.0.0.0 192.168.1.254
ntp automatic
ntp server 1 ip-address ntp1.transition.com
ntp server 2 ip-address ntp2.transition.com
clock timezone '' 9
tzidx 0
exec-timeout autologout 0
poe ping-check enable
snmp-server contact DTroxel
snmp-server location DT Office
system contact DTroxel
system name SISPM1040-582-LRT
system location DT Office
system description Managed Hardened PoE++ Switch (8) 10/100/1000Base-T PoE++ Ports + (2)
100/1000Base-X SFP Slot
!
interface GigabitEthernet 1/1
 no spanning-tree
 poe ping-ip-addr 192.168.1.70
 poe failure-action reboot-Remote-PD
!
interface GigabitEthernet 1/2
 no spanning-tree
 switchport forbidden vlan add 3,5
!
interface GigabitEthernet 1/3
 no spanning-tree
 switchport trunk allowed vlan 5,10
 switchport trunk vlan tag native
 switchport mode trunk
 poe mode disable
!
interface GigabitEthernet 1/4
 no spanning-tree
 switchport trunk allowed vlan 5,10
 switchport trunk vlan tag native
 switchport mode trunk
 poe mode disable
 poe ping-ip-addr 192.168.1.200
!
interface GigabitEthernet 1/5
 no spanning-tree
!
interface GigabitEthernet 1/6
 no spanning-tree
!
interface GigabitEthernet 1/7
!
```

```
interface GigabitEthernet 1/8
 poe mode disable
!
interface GigabitEthernet 1/9
 no spanning-tree
!
interface GigabitEthernet 1/10
 no spanning-tree
!
interface vlan 1
 ip address 192.168.1.85 255.255.255.0
 ip dhcp server
!
mep 1 down domain port level 4 interface GigabitEthernet 1/3
mep 1 vid 10
mep 1 peer-mep-id 4 mac 00-40-C7-1C-C7-30
mep 1 cc 7
mep 1 aps 7 raps
mep 2 down domain port level 4 interface GigabitEthernet 1/4
mep 2 mep-id 2
mep 2 vid 10
mep 2 peer-mep-id 5 mac 00-C0-F2-53-EF-FC
mep 2 cc 7
mep 2 aps 7 raps
erps 1 major port0 interface GigabitEthernet 1/3 port1 interface GigabitEthernet 1/4
erps 1 mep port0 sf 1 aps 1 port1 sf 2 aps 2
erps 1 rpl owner port0
erps 1 vlan 5
!
spanning-tree aggregation
 no spanning-tree
 spanning-tree link-type point-to-point
!
!
line console 0
!
line vty 0
!
line vty 1
!
line vty 2
!
line vty 3
!
line vty 4
!
line vty 5
!
line vty 6
!
line vty 7
!
line vty 8
!
line vty 9
!
line vty 10
!
line vty 11
!
line vty 12
!
line vty 13
!
line vty 14
```

```
!
line vty 15
!
map-api-key AIzaSyBItuM0hDtK6nJeZPEk7jnrcoGGi92EpFM
!
end
```

running-config_192.168.1

```
hostname SISPM1040-384-LRT-C
username admin privilege 15 password encrypted
6593186b999f348becd63b8612ac561c114250a1a00bd38f6afb5378acb6d08c1864c59b092b0e2b29ba4f1d559166
800846cbc52c4558a90e4cdf95d3cfcbf4
username dennis privilege 5 password encrypted
a92a5dbf4fcd2e13d35adb36d2418476e907de19a641fa7baf80b1abb2bacd8ee5dbdd44e246b88be1636df6b8769a
f790aa8721622481085e33c32e6e119dbd
!
vlan 1
!
!
!
!
ip route 0.0.0.0 0.0.0.0 192.168.1.254
tzidx 0
exec-timeout autologout 0
poe ping-check enable
access-list ace 2 ingress interface GigabitEthernet 1/2 action deny
access-list ace 1 next 2 ingress interface GigabitEthernet 1/2 frame-type ipv4-tcp dport 443
system name SISPM1040-384-LRT-C
system description Managed Hardened PoE+ Switch, (8) 10/100/1000Base-T PoE+ Ports + (4)
100/1000Base-X SFP
!
interface GigabitEthernet 1/1
 no spanning-tree
 lldp cdp-aware
 poe ping-ip-addr 192.168.1.100
 poe failure-action reboot-Remote-PD
!
interface GigabitEthernet 1/2
 no spanning-tree
 lldp cdp-aware
 speed 1000
 duplex full
!
interface GigabitEthernet 1/3
 no spanning-tree
 switchport trunk allowed vlan 5,20
 switchport trunk vlan tag native
 switchport mode trunk
 lldp cdp-aware
 poe mode disable
!
interface GigabitEthernet 1/4
 no spanning-tree
 switchport trunk allowed vlan 5,10
 switchport trunk vlan tag native
 switchport mode trunk
 lldp cdp-aware
 poe mode disable
!
interface GigabitEthernet 1/5
 no spanning-tree
 switchport trunk allowed vlan 5,10,20
 switchport trunk vlan tag native
 switchport mode trunk
 lldp cdp-aware
 poe mode disable
!
interface GigabitEthernet 1/6
 no spanning-tree
 lldp cdp-aware
!
```

```
interface GigabitEthernet 1/7
 lldp cdp-aware
!
interface GigabitEthernet 1/8
 lldp cdp-aware
!
interface GigabitEthernet 1/9
 no spanning-tree
 switchport trunk allowed vlan 1,50,100
 switchport trunk vlan tag native
 lldp cdp-aware
!
interface GigabitEthernet 1/10
 no spanning-tree
 lldp cdp-aware
!
interface GigabitEthernet 1/11
 no spanning-tree
 lldp cdp-aware
!
interface GigabitEthernet 1/12
 no spanning-tree
 lldp cdp-aware
!
interface vlan 1
 ip address 192.168.1.95 255.255.255.0
 ip dhcp server
!
mep 1 down domain port level 4 interface GigabitEthernet 1/3
mep 1 mep-id 3
mep 1 vid 20
mep 1 peer-mep-id 8 mac 00-C0-F2-53-F0-BA
mep 1 cc 7
mep 1 aps 7 raps
mep 2 down domain port level 4 interface GigabitEthernet 1/4
mep 2 mep-id 4
mep 2 vid 10
mep 2 peer-mep-id 1 mac 00-C0-F2-49-39-5F
mep 2 cc 7
mep 2 aps 7 raps
mep 3 down domain port level 4 interface GigabitEthernet 1/5
mep 3 mep-id 9
mep 3 vid 10
mep 3 peer-mep-id 10 mac 00-C0-F2-53-EF-FE
mep 3 cc 7
mep 3 aps 7 raps
erps 1 major port0 interface GigabitEthernet 1/5 port1 interface GigabitEthernet 1/4
erps 1 mep port0 sf 3 aps 3 port1 sf 2 aps 2
erps 1 rpl neighbor port1
erps 1 vlan 5
erps 2 sub port0 interface GigabitEthernet 1/3 interconnect 1
erps 2 mep port0 sf 1 aps 1
erps 2 rpl neighbor port0
erps 2 vlan 5
!
spanning-tree aggregation
 no spanning-tree
 spanning-tree link-type point-to-point
!
!
line console 0
!
line vty 0
!
line vty 1
```

```
!
line vty 2
!
line vty 3
!
line vty 4
!
line vty 5
!
line vty 6
!
line vty 7
!
line vty 8
!
line vty 9
!
line vty 10
!
line vty 11
!
line vty 12
!
line vty 13
!
line vty 14
!
line vty 15
!
map-api-key AIzaSyBItuM0hDtK6nJeZPEk7jnrcoGGi92EpFM
!
end
```

running-config_192.168.1

```
hostname SISPM1040-362-LRT-W
username admin privilege 15 password encrypted
6158ed7daf39d06ded0e7c4828c3b15bb4c40673bd445afcd643295925ae425d9611d1cbe872708237571aacc7b923
7f33b01ae6866e2484009edfe1fa0bf56f
!
vlan 1
!
!
!
!
ip route 0.0.0.0 0.0.0.0 192.168.1.254
tzidx 0
exec-timeout autologout 0
snmp-server location DT Lab Ring
system name SISPM1040-362-LRT-W
system location DT Lab Ring
system description Managed Hardened PoE+ Switch, (4) 10/100/1000Base-T PoE+ Ports + (2)
10/100/1000Base-T Ports + (2) 100/1000Base-X SFP Ports
!
interface GigabitEthernet 1/1
!
interface GigabitEthernet 1/2
!
interface GigabitEthernet 1/3
 no spanning-tree
 switchport trunk allowed vlan 5,20
 switchport trunk vlan tag native
 switchport mode trunk
 poe mode disable
!
interface GigabitEthernet 1/4
 no spanning-tree
 switchport trunk allowed vlan 5,20
 switchport trunk vlan tag native
 switchport mode trunk
 poe mode disable
!
interface GigabitEthernet 1/5
!
interface GigabitEthernet 1/6
!
interface GigabitEthernet 1/7
!
interface GigabitEthernet 1/8
!
interface vlan 1
 ip address 192.168.1.125 255.255.255.0
 ip dhcp server
!
mep 1 down domain port level 4 interface GigabitEthernet 1/3
mep 1 mep-id 7
mep 1 vid 20
mep 1 peer-mep-id 6 mac 00-C0-F2-53-EF-FD
mep 1 cc 7
mep 1 aps 7 raps
mep 2 down domain port level 4 interface GigabitEthernet 1/4
mep 2 mep-id 8
mep 2 vid 20
mep 2 peer-mep-id 3 mac 00-40-C7-1C-C7-2F
mep 2 cc 7
mep 2 aps 7 raps
erps 1 sub port0 interface GigabitEthernet 1/3 port1 interface GigabitEthernet 1/4
erps 1 mep port0 sf 1 aps 1 port1 sf 2 aps 2
```

```
erps 1 rpl owner port1
erps 1 vlan 5
!
spanning-tree aggregation
 spanning-tree link-type point-to-point
!
!
line console 0
!
line vty 0
!
line vty 1
!
line vty 2
!
line vty 3
!
line vty 4
!
line vty 5
!
line vty 6
!
line vty 7
!
line vty 8
!
line vty 9
!
line vty 10
!
line vty 11
!
line vty 12
!
line vty 13
!
line vty 14
!
line vty 15
!
!
end
```

Lantronix Corporate Headquarters
48 Discovery, Suite 250
Irvine, CA 92618, USA
Toll Free: 800-526-8766
Phone: 949-453-3990
Fax: 949-453-3995

Technical Support
Online: https://www.lantronix.com/technical-support/

Sales Offices
For a current list of our domestic and international sales offices, go to the Lantronix web site at www.lantronix.com/about/contact.